THE TAMIL NADU
Dr. AMBEDKAR LAW UNIVERSITY
(State University Established by Act No. 43 of 1997)
SCHOOL OF EXCELLENCE IN LAW
'Perungudi Campus', M.G.R. Salai, Perungudi, Chennai - 600 113.

INFORMATION SECURITY AND DIGITAL FORENSICS

COURSE MATERIAL FOR BCA LLB

SEMESTER VI

By

Tmt. Umashankari
Head of the Department,
Department of Computer Applications
Dr. M.G.R. Janaki Arts & Science College for Women,
Chennai - 600 028.

PREFACE

Information security processes and policies typically involve physical and digital security measures to protect data from unauthorized access, use, replication or destruction. These measures can include mantraps, encryption key management, network intrusion detection systems, password policies and regulatory compliance. A security audit may be conducted to evaluate the organization's ability to maintain secure systems against a set of established criteria.

Computers and other digital devices are becoming ubiquitous in our modern society. It was inevitable that they would begin to feature as heavily in crime and law. Since the late 1970s the amount of crime involving computers has been growing very quickly, creating a need for constantly developing forensic tools and practices.

From its inception in the 1980s the digital forensics field has grown in popularity and support. Digital evidence is being recognized much more easily in courts and companies are understanding the need for proper forensic processes when investigating employee malpractice. Digital forensics is, at root, a forensic science encompassing the recovery and investigation of material found in digital devices. This book aims to detail the practical, theoretical and legal aspect of a digital forensic investigations.

Information Security and Digital Forensics is an excellent introductory text for programs in computer science and computer engineering in law and police education. It is also a valuable reference for legal practitioners, police officers, investigators, and forensic practitioners seeking to gain a deeper understanding of digital forensics and cybercrime.

Tmt. Umashankari
Head of the Department,
Department of Computer Applications
Dr. M.G.R. Janaki Arts & Science College for Women,
Chennai - 600 028.

BCA. LL.B (HONS) DEGREE COURSE

Title of the Course/ Paper	**INFORMATION SECURITY AND DIGITAL FORENSICS**
Objective of the course	The use of computers, mobile phones and other digital devices across the globe has increased dramatically. These devices are most susceptible to information security attacks and the thus they also possess huge evidence which shall be used during crime scene investigation. This makes the course on digital forensic an inevitable one for the security professional which provides better understanding on information about cyber security and different forms of evidences in many digital devices, collection and interpretation of the same.
Sub.code	**HD6B**
Course outline	**UNIT-I :: Internet Crimes** – Introduction of IT laws and cyber crimes-Classifications of conventional and cyber crime- Malicious Code, Hacking, Cracking, Viruses, virus Attacks, Polymorphism, Steganography, Pornography, Hardware and software Piracy, intellectual Property, Legal Systems of information Technology, Social Engineering, Mail bombs, Bug Exploits, Operating System Attacks, Application Attacks, Reverse engineering and Cracking Techniques and Financial Frauds- money Laundering-Commercial Espionage and Commercial Extortion Online, Offences and Penalties under Information Technology Act and its Adjusting bodies, Offences Related with digital signature and electronic signature under Information Technology act – role of Certifying authorities – cyber Regulations Appellate Tribunal.
	UNIT-II : : Digital Forensics Introduction to Cyber Forensics – Investigation and Investigation Tools, E-Discovery, Digital Evidence Collection, Evidence Preservation, Evidential Potential of Digital Devices: Closed vs. Open systems, Evaluating Digital Evidence Potential –Device Handling: Seizure Issues, Device Identification. Networked Devices and Contamination- E-mail investigation, E-Mail Tracking, IP Tracking , E-Mail recovery, Encryption and Decryption Methods, search and Seizure of computers , Password Cracking- Digital forensics Examination of Principles: Previewing Imaging, Continuity, Hashing and Evidence Location- Seven Element security Model- developmental Interpretation- Data and Content and Context – Distributed System security-Public Key Cryptography – VPN- forensic Photography-Forensic Audio and Video analysis.
	UNIT-III:: Data and Evidence Recovery –Introduction to Deleted file Recovery, Formatted Partition, Data Recovery Tools, Data Recovery Procedures and Ethics, Preserve and Safety Handle Original Media, Complete Time Line analysis of computer Files based on File Creation, File Modification and File Access, recovery Internet Usage Data, Recover Swap Files- Temporary Files- Cache Files, forensic tool kit (FTK)-History Tracking, working on duplicate Media, working in Live Systems, Methods and Procedures, Presentation of Evidence.

	Unit IV – Wireless Technology and security – personal Area Network, Wireless Local area Network, Metropolitan Area Network, Wide area Network. Wireless Threats, vulnerabilities and Securities : War Driving , War chalking, War Flying, Common Wi-Fi security Recommendations, PDA Security, Cell Phones and security, Wireless Dos Attacks, GPs Jamming , identify theft- Voice ,SMS and Identification, Data Interpretation in GSM Network Service Code- Mobile Phone codes, Catalog Tricks and AT command Service, SMS Security Issues- Crime and mobile Phones, Evidence Forensic Procedure , files Present in SIM Card, device Data, External Memory dump, Evidence in Memory Card, Operating systems – android Forensic- Procedure for Handling Anan Android Devices , Imaging Android USB Mass storage devices, Logical and Physical Techniques.
	Unit V - Information Security and Management- Cyber security and its Problem – intervention Strategies Redundancy, Diversity and Autarchy-Private Ordering Solutions, Regulation and Jurisdiction for Global Cyber Security, Copy right-source of Risk, pirates, interne Infringement , fair use, Posting, Criminals Liability, Data Losing- security Management of IT Systems: Network security Management- firewalls, Intrusion Detection systems(IDS) and In-Plane Switching(IPS) Configuration Management-Web and Wireless security Management Security Management – General Server Configuration Guidelines And Maintenance Information Security Management Information Classification – Access Control Models, role Based and Lattice Models-Mandatory and Discretionary Access Controls – Linux and Windows Case Studies- Technical Controls for Authentication and Confidentiality – Password Management and key Management for users-case Studies of Kerberos.
Recommended Texts	• The Information Technology Act, 2000 and Its Amendment and Allied Rules • Ali Jahangiri- Live Hacking Techniques and Counter Measures for Ethical Hackers and IT Security Experts • Angus M. Marshall John – Digital Forensics: Digital Evidence in Criminal investigation. • Micki Krause, Harold F. Tripton- Information Security Management, Handbook • Dr.(Smt) Rukmani Krishnamurthy- introduction t0 forensic Science in Crime Investigation

CONTENTS

CHAPTER 1

1.1 INTRODUCTION TO CYBER LAW

The term 'Cyber Law' in general refers to all the legal and regulatory aspects of Internet. It means that anything concerned with, related to, or emanating from any legal aspects or issues concerning any activity of netizens and others in cyberspace comes within the ambit of cyber law. More specifically, cyber law can be defined as a law governing the use of computer and the Internet. Namely, it focuses on a combination of state and federal statutory, decisional and administrative laws arising out of the use of Internet.

The IT revolution resulted in a phenomenal increase in the number of cyberspace users all over the world. The birth of the Internet resulted in networking which helped millions of users to connect online, thus facilitating the sharing of information. In India also, there was an overwhelming increase in the number of internet-users. *Forrester Research*, a technology and market research Firm reported that the number of internet-users worldwide would touch the 2.2 billion mark by 2013 and that India would have the third highest number of internet-users at the same time. The government framed and announced Internet policy document in 1997 to promote and encourage internet-users in India. With economic activities like buying, selling, advertising, etcetera taking place online, the Internet indeed proved to be a boon for many. Little did anyone suspect that the uncontrolled manner in which online activities were carried on would give way to another category of computer related crimes. Cyber crime is a new type of criminal activity that started raising its ugly head in the early 1990s, as the Internet emerged as a virtual place for the users worldwide to meet and share various forms of Information. This development also paralleled with the entry of criminals to gain access to sensitive information if they have the necessary knowhow. Thus the Cyber space became vulnerable from the economic and social perspectives- driving companies and individuals to take costly steps to ensure their safety and exposure from those deviant acts in the cyber space.

1.2 CYBER LAW AND CYBER CRIME:

One of the early cyber crime, which had come to the public notice is the fraud relating to fund transfer online to the tune of USD 10 Million from Citibank. A Russian hacker group led by Vladimir Kevin, a renowned hacker, perpetrated the attack compromising the bank's security systems. Vladimir was allegedly using his office computer at AO Saturn, a computer firm in St. Petersburg, Russia, to break into Citibank computers to commit the cyber crime. He was finally arrested on Heathrow airport on his way to Switzerland.

Cyber Crimes increased by 22.7% in 2007 as compared to 2006 (from 453 in 2006 to 556 in 2007), Cyber Forgery 64.0% (217 out of total 339) and Cyber Fraud 21.5% (73 out of 339) were the main cases under IPC category for Cyber Crimes. In this 63.05% of the offenders under IT Act were in the age group 18-30 years (97 out of 154) and 55.2% of the offenders under IPC Sections were in the age group 30-45 years (237 out of 429) according to the latest data available with the National Crime Records Bureau of the Ministry of Home of Government of India.

The Information Technology Bill (1999) has defined the cybercrimes as:

Whoever knowingly or intentionally conceals, destroys, or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source document used for a computer, computer programme, computer system, or computer network, when computer source code is required to be kept or maintained by law for the time being in force [shall be punishable with a fine which may extend up to rupees two lakhs or with imprisonment up to three years, or with both].

DEFINITION OF CYBERCRIME

Defining cybercrimes, as "acts that are punishable by the Information Technology Act" would be unsuitable as the Indian Penal Code also covers many cybercrimes, such as email spoofing and cyber defamation, sending threatening emails etc. A simple yet sturdy definition of cybercrime would be "unlawful acts wherein the computer is either a tool or a target or both".

Let us examine the acts wherein the computer is a tool for an unlawful act. This kind of activity usually involves a modification of a conventional crime by using computers. Some examples are:

Financial crimes: This would include cheating, credit card frauds, money laundering etc. To cite a recent case, a website offered to sell Alphonso mangoes at a throwaway price. Distrusting such a transaction, very few people responded to or supplied the website with their credit card numbers. These people were actually sent the Alphonso mangoes. The word about this website now spread like wildfire. Thousands of people from all over the country responded and ordered mangoes by providing their credit card numbers. The owners of what was later proven to be a bogus website then fled taking the numerous credit card numbers and proceeded to spend huge amounts of money much to the chagrin of the card owners.

1.3 NEED FOR CYBER LAW

There are various reasons why it is extremely difficult for conventional law to cope with cyberspace. Some of these are discussed below.

1. Cyberspace is an intangible dimension that is impossible to govern and regulate using conventional law.

2. Cyberspace has complete disrespect for jurisdictional boundaries. A person in India could break into a banks electronic vault hosted on a computer in USA and transfer millions of Rupees to another bank in Switzerland, all within minutes. All he would need is a laptop computer and a cell phone.

3. Cyberspace handles gigantic traffic volumes every second. Billions of emails are crisscrossing the globe even as we read this, millions of websites are being accessed every minute and billions of dollars are electronically transferred around the world by banks every day.

4. Cyberspace offers enormous potential for anonymity to its members. Readily available encryption software and steganographic tools that seamlessly hide information within image and sound files ensure the confidentiality of information exchanged between cyber-citizens.

5. Cyberspace offers never-seen-before economic efficiency. Billions of dollars worth of software can be traded over the Internet without the need for any government licenses, shipping and handling charges and without paying any customs duty.

6. Electronic information has become the main object of cybercrime. It is characterized by extreme mobility, which exceeds by far the mobility of persons, goods or other services. International computer networks can transfer huge amounts of data around the globe in a matter of seconds.

7. A software source code worth crores of rupees or a movie can be pirated across the globe within hours of their release.

8. Theft of corporeal information (e.g. books, papers, CD ROMs, floppy disks) is easily covered by traditional penal provisions. However, the problem begins when electronic records are copied quickly, inconspicuously and often via telecommunication facilities.

1.4 JURISPRUDENCE OF INDIAN CYBER LAW:

The primary source of cyber law in India is the Information Technology Act, 2000 (IT Act) which came into force on 17 October 2000. The primary purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government. The IT Act also penalizes various cybercrimes and provides strict punishments (imprisonment terms upto 10 years and compensation up to Rs 1 crore).

An Executive Order dated 12 September 2002 contained instructions relating provisions of the Act with regard to protected systems and application for the issue of a Digital Signature Certificate. Minor errors in the Act were rectified by the Information Technology (Removal of Difficulties) Order, 2002 which was passed on 19 September 2002. The IT Act was amended by the Negotiable Instruments (Amendments and Miscellaneous Provisions) Act, 2002. This introduced the concept of electronic cheques and truncated cheques. Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004 has provided the necessary legal framework for filing of documents with the Government as well as issue of licenses by the Government.

It also provides for payment and receipt of fees in relation to the Government bodies. On the same day, the Information Technology (Certifying Authorities) Rules, 2000 also came into force. These rules prescribe the eligibility, appointment and working of Certifying Authorities (CA). These rules also lay down the technical standards, procedures and security methods to be used by a CA.

These rules were amended in 2003, 2004 and 2006.

Information Technology (Certifying Authority) Regulations, 2001 came into force on 9 July 2001. They provide further technical standards and procedures to be used by a CA. Two important guidelines relating to CAs were issued. The first are the Guidelines for submission of application for license to operate as a Certifying Authority under the IT Act. These guidelines were issued on 9th July 2001. Next were the Guidelines for submission of certificates and certification revocation lists to the Controller of Certifying Authorities for publishing in National

Repository of Digital Certificates. These were issued on 16thDecember 2002. The Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000 also came into force on 17th October 2000.

These rules prescribe the appointment and working of the Cyber Regulations Appellate Tribunal (CRAT) whose primary role is to hear appeals against orders of the Adjudicating Officers. The Cyber Regulations Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Presiding Officer) Rules, 2003 prescribe the salary, allowances and other terms for the Presiding Officer of the CRAT. Information Technology (Other powers of Civil Court vested in Cyber Appellate Tribunal) Rules 2003 provided some additional powers to the CRAT.

On 17th March 2003, the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003 were passed. These rules prescribe the qualifications required for Adjudicating Officers. Their chief responsibility under the IT Act is to adjudicate on cases such as unauthorized access, unauthorized copying of data, spread of viruses, denial of service attacks, disruption of computers, computer manipulation etc. These rules also prescribe the manner and mode of inquiry and adjudication by these officers.

The Government had not appointed the Adjudicating Officers or the Cyber Regulations Appellate Tribunal for almost 2 years after the passage of the IT Act. This prompted ASCL students to file a Public Interest Litigation (PIL) in the Bombay High Court asking for a speedy appointment of Adjudicating officers. The Bombay High Court, in its order dated 9th October 2002, directed the Central Government to announce the appointment of adjudicating officers in the public media to make people aware of the appointments. The division bench of the Mumbai High Court consisting of Honorable Justice A.P. Shah and Honorable Justice Ranjana Desai also ordered that the Cyber Regulations Appellate Tribunal be constituted within a reasonable time frame.

Following this the Central Government passed an order dated 23rd March 2003 appointing the Secretary of Department of Information Technology of each of the States or of Union Territories' of India as the adjudicating officers. The Information Technology (Security Procedure) Rules, 2004 came into force on 29th October 2004. They prescribe provisions relating to secure digital signatures and secure electronic records. Also relevant are the Information Technology (Other Standards) Rules, 2003.

An important order relating to blocking of websites was passed on 27th February, 2003. Computer Emergency Response Team (CERT-IND) can instruct Department of Telecommunications (DOT) to block a website. The Indian Penal Code (as amended by the IT Act) penalizes several cybercrimes. These include forgery of electronic records, cyber frauds, destroying electronic evidence etc. Digital Evidence is to be collected and proven in court as per the provisions of the Indian Evidence Act (as amended by the IT Act).

In case of bank records, the provisions of the Bankers Book Evidence Act (as amended by the IT Act) are relevant. Investigation and adjudication of cybercrimes is done in accordance with the provisions of the Code of Criminal Procedure and the IT Act.

The Reserve Bank of India Act was also amended by the IT Act.

1.5 CLASSIFICATION OF CYBER CRIMES:

Computer crime mainly consists of unauthorized access to computer systems data alteration, data destruction, and theft of intellectual properly. Cyber crime in the context of national security may involve hacking, traditional espionage, or information warfare and related activities.

Pornography, threatening email, assuming someone's identity, sexual harassment, defamation, SPAM and Phishing are some examples where computers are used to commit crime, whereas viruses, worms and industrial espionage, software piracy and hacking are examples where computers become target of crime.

Two classes of cyber crimes:

A. Computer Assisted Cyber Crimes: computer is instrumental in committing the crime.

Selling nonexistent, defective, substandard or counterfeit goods, theft of credit card, bank fraud, fake stock shares, intellectual property offences including unauthorized sharing of the copy righted content of movies, music, digitized books

- Selling obscene and prohibited sexual representations.

B. Computer Oriented Cyber Crimes: Computer is the target of the crime

- o Malicious Software: viruses, Trojans (which corrupt server)
- o Cyber terrorism:
- o Child pornography
- o Violent and extreme pornography
- o Internet inspired homicides and suicides

- ❖ *Worm: Self-replicating programmes, spread autonomously without a carrier.*
- ❖ *Trojan: installed during downloading some programme as a back ground activity causing irreparable damage*
- ❖ *Spyware: parasitic software-invades privacy-divulging details- through tracking cookies.*

Even though our basic understanding about cyber crime is that computer is necessary as one of the components of the offence, it is also interpreted that a crime committed by using any digital device is covered under the ambit of cyber crime. For example: Casio digital diary, Mobiles, Calculators, Pen drives, CDs.

At the onset, let us satisfactorily define "cybercrime" and differentiate it from "conventional Crime". Computer crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

Other Classification of Cyber Crime based on Individual, Organization and Society:

The subject of cybercrime may be broadly classified under the following three groups. They are:

1. *Against Individuals*
    a) Their person &
    b) Their property of an individual
2. *Against Organization*
    a) Government
    b) Firm, Company, Group of Individuals.
3. *Against Society at large*

The following are the crimes, which can be committed against the following groups

Against Individuals:

i. Harassment via e-mails.

ii. Cyber-stalking.

iii. Dissemination of obscene material.

iv. Defamation.

v. Unauthorized control/access over computer system.

vi. Indecent exposure

vii. Email spoofing

viii. Cheating & Fraud Against Individual Property:

i. Computer vandalism.

ii. Transmitting virus.

iii. Unauthorized control/access over computer system.

iv. Intellectual Property crimes

v. Internet time thefts Against Organization:

i. Unauthorized control/access over computer system

ii. Possession of unauthorized information.

iii. Cyber terrorism against the government organization.

iv. Distribution of pirated software etc. Against Society at large:

i. Pornography (basically child pornography).

ii. Polluting the youth through indecent exposure.

iii. Trafficking

iv. Financial crimes

v. Sale of illegal articles

vi. Online gambling

vii. Forgery

The Information Technology Act deals with the following cybercrimes along with others.

Cyber pornography

This would include pornographic websites; pornographic magazines produced using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc.). Recent Indian incidents revolving around cyber pornography include the Air Force Bal bharati School case. A student of the Air Force Bal bharati School, Delhi, was teased by all his classmates for having a pockmarked face. Tired of the cruel jokes, he decided to get back at history mentors. He scanned photographs of his classmates and teachers, morphed them with nude photographs and put them up on a website that he uploaded on to a free web hosting service. It was only after the father of one of the class girls featured on the website objected and lodged a complaint with the police that any action was taken.

Another incident, in Mumbai a Swiss couple would gather slum children and then would force them to appear for obscene photographs. They would then upload these photographs to websites specially designed for pedophiles. The Mumbai police arrested the couple for pornography.

Sale of illegal articles

This would include sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or 167 simply by using email communication. E.g. many of the auction sites even in India are believed to be selling cocaine in the name of 'honey'.

Online gambling

There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.

Intellectual Property crimes

These include software piracy, copyright infringement, trademarks violations, theft of computer source code etc.

Email spoofing

A spoofed email is one that appears to originate from one source but actually has been sent from another source.

Email spoofing can also cause monetary damage. In an American case, a teenager made millions of dollars by spreading false information about certain companies whose shares he had short sold. This misinformation was spread by sending spoofed emails, purportedly from news agencies like Reuters, to share brokers and investors who were informed that the companies were doing very badly. Even after the truth came out the values of the shares did not go back to the earlier levels and thousands of investors lost a lot of money.

Forgery

Counterfeit currency notes, postage and revenue stamps, mark sheets etc. can be forged using sophisticated computers, printers and scanners. Outside many colleges across India, one finds touts soliciting the sale of fake mark sheets or even certificates. These are made using computers, and high quality scanners and printers. In fact, this has becoming a booming business involving thousands of Rupees being given to student gangs in exchange for these bogus but authentic looking certificates.

Cyber Defamation

This occurs when defamation takes place with the help of computers and / or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

In a recent occurrence, Surekha (names of people have been changed), a young girl was about to be married to Suraj. She was really pleased because despite it being an arranged marriage, she had liked the boy. He had seemed to be open-minded and pleasant. Then, one day when she met Suraj, he looked worried and even a little upset. He was not really interested in talking to her. When asked he told her that, members of his family had been receiving e-mails that contained malicious things about Surekha's character. Some of them spoke of affairs, which she had had in the past. He told her that, his parents were justifiably very upset and were also considering breaking off the engagement. Fortunately, Suraj was able to prevail upon his parents and the other elders of his house to approach the police instead of blindly believing what was contained in the mails.

During investigation, it was revealed that the person sending those e-mails was none other than Surekha's stepfather. He had sent these e-mails so as to break up the marriage. The girl's marriage would have caused him to lose control of her property of which he was the guardian till she got married.

Another famous case of cyber defamation occurred in America. All friends and relatives of a lady were beset with obscene e-mail messages appearing to originate from her account. These mails were giving the lady in question a bad name among her friends. The lady was an activist against pornography. In reality, a group of people displeased with her views and angry with her for opposing they had decided to get back at her by using such underhanded methods. In addition to sending spoofed obscene e-mails they also put up websites about her, that basically maligned her character and sent e-mails to her family and friends containing matter defaming her.

Cyber stalking

The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc.

Email Bombing

Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing. In one case, a foreigner who had been residing in Shimla, India for almost thirty years wanted to avail of a scheme introduced by the Shimla Housing Board to buy land at lower rates. When he made an application it was rejected on the grounds that the schemes were available only for citizens of India. He decided to take his revenge. Consequently he sent thousands of mails to the Shimla Housing Board and repeatedly kept sending e-mails till their servers crashed.

Data Diddling

This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed. Electricity Boards in India have been victims to data diddling programs inserted when private parties were computerizing their systems.

Salami Attacks

These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount of money every month. To cite an example, an employee of a bank in USA was dismissed from his job. Disgruntled at having been supposedly mistreated by his employers the man first introduced a logic bomb into the bank's systems. Logic bombs are programmes, which are activated on the occurrence of a particular predefined event.

The logic bomb was programmed to take ten cents from all the accounts in the bank and put them into the account of the person whose name was alphabetically the last in the bank's rosters. Then he went and opened an account in the name of Ziegler. The amount being withdrawn from each of the accounts in the bank was so insignificant that neither any of the account holders nor the bank officials noticed the fault. It was brought to their notice when a person by the name of Zygler opened his account in that bank. He was surprised to find a sizable amount of money being transferred into his account every Saturday.

Denial Of Service Attack

This involves flooding a computer resource with more requests than it can handle. This causes the resource (e.g. a web server) to crash thereby denying authorized users the service offered by the resource. Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread. It is very difficult to control such attacks. The attack is initiated by sending excessive demands to the victim's computer(s), exceeding the limit that the victim's servers can support and making the servers crash. Denial-of-service attacks have had an impressive history having, in the past, brought down websites like Amazon, CNN, Yahoo and eBay!

Virus / Worm Attacks

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up the entire

available space on a computer's memory. The VBS_LOVELETTER virus (better known as the Love Bug or the ILOVEYOU virus) was reportedly written by a Filipino undergraduate. In May 2000, this deadly virus beat the Melissa virus hollow - it became the world's most prevalent virus. It struck one in every five personal computers in the world.

When the virus was brought under check the true magnitude of the losses was incomprehensible. Losses incurred during this virus attack were pegged at US

$ 10billion.The original VBS_LOVELETTER utilized the addresses in Microsoft Outlook and emailed itself to those addresses. The e-mail, which was sent out, had "ILOVEYOU" in its subject line. The attachment file was named "LOVE- LETTER-FORYOU. TXT.vbs". The subject line and those who had some knowledge of viruses did not notice the tiny .vbs extension and believed the file to be a text file conquered people wary of opening e-mail attachments. The message in the e-mail was "kindly check the attached LOVELETTER coming from me".

Since, the initial outbreak over thirty variants of the virus have been developed many of them following the original by just a few weeks. In addition, the Love Bug also uses the Internet Relay Chat (IRC) for its propagation. It e-mails itself to users in the same channel as the infected user. Unlike the Melissa virus this virus does have a destructive effect. Whereas the Melissa, once installed, merely inserts some text into the affected documents at a

particular instant during the day, VBS_LOVELETTER first selects certain files and then inserts its own code in lieu of the original data contained in the file. This way it creates ever- increasing versions of itself. Probably the world's most famous worm was the Internet worm let loose on the Internet by Robert Morris sometime in 1988. The Internet was, then, still in its developing years and this worm, which affected thousands of computers, almost brought its development to a complete halt. It took a team of experts almost three days to get rid of the worm and in the meantime many of the computers had to be disconnected from the network.

Logic bombs

These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

Trojan attacks

A Trojan as this program is aptly called is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing. There are many simple ways of installing a Trojan in someone's computer. To cite and example, two friends Rahul and Mukesh (names changed), had a heated argument over one girl, Radha (name changed) whom they both liked. When the girl, asked to choose, chose Mukesh over Rahul, Rahul decided to get even. On the14th of February, he sent Mukesh a spoofed e-card, which appeared to have come from Radha's mail account. The e-card actually contained a Trojan. As soon as Mukesh opened the card, the Trojan was installed on his computer. Rahul now had complete control over Mukesh's computer and proceeded to harass him thoroughly.

Internet time thefts

This connotes the usage by an unauthorized person of the Internet hours paid for by another person. In a case reported before the enactment of the Information Technology Act, 2000 Colonel Bajwa, a resident of New Delhi, asked a nearby net café owner to come and set up his Internet connection. For this purpose, the net café owner needed to know his username and password. After having set up the connection he went away with knowing the present username and password. He then sold this information to another net café. One week later Colonel Bajwa found that his Internet hours were almost over. Out of the 100 hours that he had bought, 94hours had been used up within the span of that week. Surprised, he reported the incident to the Delhi police. The police could not believe that time could be stolen. They were not aware of the concept of time-theft at all. Colonel Bajwa's report was rejected. He decided to approach The Times of India, New Delhi. They, in turn carried a report about the inadequacy of the New Delhi Police in handling cybercrimes. The Commissioner of Police, Delhi then took the case into his own hands and the police under his directions raided and arrested the net café owner under the charge of theft as defined by the Indian Penal Code. The net café owner spent several weeks locked up in Tihar jail before being granted bail.

Web jacking

This occurs when someone forcefully takes control of a website (by cracking the password and later changing it). The actual owner of the website does not have any more control over what appears on that website. In a recent incident reported in the USA the owner of a hobby website for children received an e-mail informing her that a group of hackers had gained control over her website. They demanded a ransom of 1 million dollars from her. The owner, a schoolteacher, did not take the threat seriously. She felt that it was just a scare tactic and ignored the e-mail. It was three days later that she came to know, following many telephone calls from all over the country, that the hackers had web jacked her website. Subsequently, they had altered a portion of the website which was entitled 'How to have fun with goldfish'. In all the places where it had been mentioned, they had replaced the word 'goldfish' with the word 'piranhas'. Piranhas are tiny but extremely dangerous flesh- eating fish.

Many children had visited the popular website and had believed what the contents of the website suggested. These unfortunate children followed the instructions, tried to play with piranhas, which they bought from pet shops, and were very seriously injured.

Theft of computer system

This type of offence involves the theft of a computer, some part(s) of a computer or peripheral attached to the computer.

1.6 CONVENTIONAL CRIME

Crime is a social and economic phenomena and is as old as the human society. Crime is legal concept and has the sanction of the law. Crime or an offence is a legal wrong that can be followed by criminal proceedings which may result into punishment. The hallmark of criminality is that, it is breach of the criminal law. Per Lord Atkin the criminal quality of an act cannot be discovered by reference to any standard but one: is the act prohibited with penal consequences'.

A crime may be said to be any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by penal consequences.

Cyber Crime:

Cybercrime is the latest and perhaps the most complicated problem in the cyber world. Cybercrime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime'. Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cybercrime'

A generalized definition of cybercrime may be unlawful acts wherein the computer is either a tool or target or both' The computer may be used as a tool in the following kinds of activity- financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking. The computer may however be target for unlawful acts in the following cases- unauthorized

access to computer/ computer system/ computer networks, theft of information contained in the electronic form, e-mail bombing, data didling, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system.

Difference between conventional crime and cyber crime

There is apparently no distinction between cyber and conventional crime. However on a deep introspection we may say that there exist a fine line of demarcation between the conventional and cybercrime, which is appreciable. The demarcation lies in the involvement of the medium in cases of cybercrime. The sine qua non for cybercrime is that there should be an involvement, at any stage, of the virtual cyber medium.

Capacity to store data in comparatively small space: The computer has unique characteristic

of storing data in a very small space. This affords to remove or derive information either through physical or virtual medium makes it much easier.

Easy to access : The problem encountered in guarding a computer system from unauthorized access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.

Complex : The computers work on operating systems and these operating systems in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.

Negligence: Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cybercriminal to gain access and control over the computer system.

Loss of evidence: Loss of evidence is a very common & obvious problem as all the data are routinely destroyed. Further collection of data outside the territorial extent also paralyzes this system of crime investigation.

1.7 CYBER CRIMINIALS

The cyber criminals constitute of various groups/ category. This division may be justified on the basis of the object that they have in their mind. The following are the category of cyber criminals-

Organized hackers

These kinds of hackers are mostly organised together to fulfil certain objective. The reason may be to fulfil their political bias, fundamentalism, etc. The Pakistanis are said to be one of the best quality hackers in the world. They mainly target the Indian government sites with the purpose to fulfil their political objectives. Further the NASA as well as the Microsoft sites is always under attack by the hackers.

Professional hackers / crackers

Their work is motivated by the colour of money. These kinds of hackers are mostly employed to hack the site of the rivals and get credible, reliable and valuable information. Further they are even employed to crack the system of the employer basically as a measure to make it safer by detecting the loopholes.

***Discontented employees*:** This group include those people who have been either sacked by their employer or are dissatisfied with their employer. To avenge they normally hack the system of their employee.

Tampering with computer Source document

A person who knowingly or intentionally, conceals (hides or keeps secret), destroys (demolishes or reduces), alters (change in characteristics) or causes another to conceal, destroy, and alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law is punishable.

For instance, hiding the C.D.ROM in which the source code files are stored, making a C File into a CPP File or removing the read only attributes of a file. Hacking is usually understood to be the unauthorized access of a computer system and networks. Originally, the term "hacker" describes any amateur computer programmer who discovered ways to make software run more efficiently. Hackers usually "hack" on a problem until they find a solution, and keep trying to make their equipment work in new and more efficient ways. A hacker can be a Code Hacker, Cracker or a Cyber Punk.

Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by means is said to commit hacking.

Publishing obscene material in electronic form

A person who publishes or transmits or causes to be published in the electronic form, any material which is lascivious, or if its effect is such as to tend to deprave and corrupt persons who are likely to read, see or hear the matter contained or embodied in it, is liable to punishment. The important ingredients of such an offence are publishing (make generally known or issue copies for sale to public), or transmitting (transfer or be a medium for), or causing to be published (to produce the effect of publishing), pornographic material in the electronic form.
Child Pornography

Child Pornography is a part of cyber pornography but it is such a grave offence that it is individually also recognized as a cybercrime. The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide. The Internet is very fast becoming a household commodity in India. Its explosion has made the children a viable victim to the cybercrime. As more homes have access to Internet, more children would be using the Internet and more are the chances of falling victim to the aggression of pedophiles. The pedophiles use their false identity to trap children and even contact them in various chat rooms where they befriend them and gain personal information

from the innocent preys. They even start contacting children on their e-mail addresses. These pedophiles drag children to the net for the purpose of sexual assault or so as to use them as a sex object.

Accessing protected system

Any unauthorized person who secures access or attempts to secure access to a protected system is liable to be punished with imprisonment and may also be liable to fine.

Breach of confidentiality and privacy

Any person who, secures access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned or discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be liable to be punished under the Information Technology Act.

1.8 INTELLECTUAL PROPERTY RIGHTS

Intellectual property rights are the legal rights that cover the privileges given to individuals who are the owners and inventors of a work, and have created something with their intellectual creativity. Individuals related to areas such as literature, music, invention, etc., can be granted such rights, which can then be used in the business practices by them.

The creator/inventor gets exclusive rights against any misuse or use of work without his/her prior information. However, the rights are granted for a limited period of time to maintain equilibrium.

The following list of activities which are covered by the intellectual property rights are laid down by the World Intellectual Property Organization (WIPO) "

- Industrial designs
- Scientific discoveries
- Protection against unfair competition
- Literary, artistic, and scientific works
- Inventions in all fields of human endeavor
- Performances of performing artists, phonograms, and broadcasts
- Trademarks, service marks, commercial names, and designations
- All other rights resulting from intellectual activity in the industrial, scientific, literary, or artistic fields

Types of Intellectual Property Rights

Intellectual Property Rights can be further classified into the following categories "

- Copyright
- Patent
- Patent
- Trade Secrets, etc.

Advantages of Intellectual Property Rights

Intellectual property rights are advantageous in the following ways "

- Provides exclusive rights to the creators or inventors.
- Encourages individuals to distribute and share information and data instead of keeping it confidential.
- Provides legal defense and offers the creators the incentive of their work.
- Helps in social and financial development.

Intellectual Property Rights in India

To protect the intellectual property rights in the Indian territory, India has defined the formation of constitutional, administrative and jurisdictive outline whether they imply the copyright, patent, trademark, industrial designs, or any other parts of the intellectual property rights.

Back in the year 1999, the government passed an important legislation based on international practices to safeguard the intellectual property rights. Let us have a glimpse of the same "

- The **Patents** (Amendment) Act, 1999, facilitates the establishment of the mail box system for filing patents. It offers exclusive marketing rights for a time period of five years.
- The **Trade Marks** Bill, 1999, replaced the Trade and Merchandise Marks Act, 1958
- The **Copyright** (Amendment) Act, 1999, was signed by the President of India.
- The ***sui generis*** legislation was approved and named as the Geographical Indications of Goods (Registration and Protection) Bill, 1999.
- The **Industrial Designs** Bill, 1999, replaced the Designs Act, 1911.
- The **Patents (Second Amendment)** Bill, 1999, for further amending the Patents Act of 1970 in compliance with the TRIPS.

Intellectual Property in Cyber Space

Every new invention in the field of technology experiences a variety of threats. Internet is one such threat, which has captured the physical marketplace and have converted it into a virtual marketplace.

To safeguard the business interest, it is vital to create an effective property management and protection mechanism keeping in mind the considerable amount of business and commerce taking place in the Cyber Space.

Today it is critical for every business to develop an effective and collaborative IP management mechanism and protection strategy. The ever-looming threats in the cybernetic world can thus be monitored and confined.

Various approaches and legislations have been designed by the law-makers to up the ante in delivering a secure configuration against such cyber-threats. However it is the duty of the intellectual property right (IPR) owner to invalidate and reduce such *mala fide* acts of criminals by taking proactive measures.

1.9 SOCIAL ENGINEERING

WHAT IS SOCIAL ENGINEERING?

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

Social engineering attack lifecycle

What makes social engineering especially dangerous is that it relies on human error, rather than vulnerabilities in software and operating systems. Mistakes made by legitimate users are much less predictable, making them harder to identify and thwart than a malware-based intrusion.

1.9 SOCIAL ENGINEERING ATTACK TECHNIQUES

Social engineering attacks come in many different forms and can be performed anywhere where human interaction is involved. The following are the five most common forms of digital social engineering assaults.

Baiting

As its name implies, baiting attacks use a false promise to pique a victim's greed or curiosity. They lure users into a trap that steals their personal information or inflicts their systems with malware.

The most reviled form of baiting uses physical media to disperse malware. For example, attackers leave the bait—typically malware-infected flash drives—in conspicuous areas where potential victims are certain to see

them (e.g., bathrooms, elevators, the parking lot of a targeted company). The bait has an authentic look to it, such as a label presenting it as the company's payroll list.

Victims pick up the bait out of curiosity and insert it into a work or home computer, resulting in automatic malware installation on the system.

Baiting scams don't necessarily have to be carried out in the physical world. Online forms of baiting consist of enticing ads that lead to malicious sites or that encourage users to download a malware-infected application.

Scareware

Scareware involves victims being bombarded with false alarms and fictitious threats. Users are deceived to think their system is infected with malware, prompting them to install software that has no real benefit (other than for the perpetrator) or is malware itself. Scareware is also referred to as deception software, rogue scanner software and fraudware.

A common scareware example is the legitimate-looking popup banners appearing in your browser while surfing the web, displaying such text such as, "Your computer may be infected with harmful spyware programs." It either offers to install the tool (often malware-infected) for you, or will direct you to a malicious site where your computer becomes infected.

Scareware is also distributed via spam email that doles out bogus warnings, or makes offers for users to buy worthless/harmful services.

Pretexting

Here an attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by a perpetrator pretending to need sensitive information from a victim so as to perform a critical task.

The attacker usually starts by establishing trust with their victim by impersonating co-workers, police, bank and tax officials, or other persons who have right-to-know authority. The pretexter asks questions that are ostensibly required to confirm the victim's identity, through which they gather important personal data.

All sorts of pertinent information and records is gathered using this scam, such as social security numbers, personal addresses and phone numbers, phone records, staff vacation dates, bank records and even security information related to a physical plant.

Phishing

As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.

An example is an email sent to users of an online service that alerts them of a policy violation requiring immediate action on their part, such as a required password change. It includes a link to an illegitimate website—nearly identical in appearance to its legitimate version—prompting the unsuspecting user to enter their current credentials and new password. Upon form submittal the information is sent to the attacker.

Given that identical, or near-identical, messages are sent to all users in phishing campaigns, detecting and blocking them are much easier for mail servers having access to threat sharing platforms.

Spear phishing

This is a more targeted version of the phishing scam whereby an attacker chooses specific individuals or enterprises. They then tailor their messages based on characteristics, job positions, and contacts belonging to their victims to make their attack less conspicuous. Spear phishing requires much more effort on behalf of the perpetrator and may take weeks and months to pull off. They're much harder to detect and have better success rates if done skillfully.

A spear phishing scenario might involve an attacker who, in impersonating an organization's IT consultant, sends an email to one or more employees. It's worded and signed exactly as the consultant normally does, thereby deceiving recipients into thinking it's an authentic message. The message prompts recipients to change their password and provides them with a link that redirects them to a malicious page where the attacker now captures their credentials.

1.10 SOCIAL ENGINEERING PREVENTION

Social engineers manipulate human feelings, such as curiosity or fear, to carry out schemes and draw victims into their traps. Therefore, be wary whenever you feel alarmed by an email, attracted to an offer displayed on a website, or when you come across stray digital media lying about. Being alert can help you protect yourself against most social engineering attacks taking place in the digital realm.

Moreover, the following tips can help improve your vigilance in relation to social engineering hacks.

1. **Don't open emails and attachments from suspicious sources** – If you don't know the sender in question, you don't need to answer an email. Even if you do know them and are suspicious about their message, cross-check and confirm the news from other sources, such as via telephone or directly from a service provider's site. Remember that email addresses are spoofed all of the time; even an email purportedly coming from a trusted source may have actually been initiated by an attacker.

2. **Use multifactor authentication** – One of the most valuable pieces of information attackers seek are user credentials. Using multifactor authentication helps ensure your account's protection in the event of system compromise. Imperva Incapsula Login Protect is an easy-to-deploy 2FA solution that can increase account security for your applications.

3. **Be wary of tempting offers** – If an offer sounds too enticing, think twice before accepting it as fact. Googling the topic can help you quickly determine whether you're dealing with a legitimate offer or a trap.

4. **Keep your antivirus/antimalware software updated** – Make sure automatic updates are engaged, or make it a habit to download the latest signatures first thing each day. Periodically check to make sure that the updates have been applied, and scan your system for possible infections.

1.11 Email Bomb

Email bombs, depending on the magnitude can be a form of prank or an actual denial of service attack. There are three ways to create an email bomb:

- Mass mailing - involves sending numerous duplicates of the same email to one email address. Because of the simplicity of this attack, it can be easily detected by spam filters. To be done on a massive scale, an attacker can use a bot net or zombie net, computers across the globe which are under the attacker's control due to some form of malware such as Trojans, and then instructing the bot net to send millions of emails to a single or a few addresses at once in order to perform a denial of service attack. This is harder for spam filters to detect since each email would be coming from a unique source.

- List linking - meant more to annoy rather than cause real trouble. The technique involves subscribing the address for attack to different email list subscriptions so it would always receive spam mail from these lists. The user then has to manually unsubscribe from each list. However, more legitimate lists require email verification which the user has to manually click and accept to be part of the email listing. To circumvent this, the attacker may register a new email account and subscribe that to all the lists and have it automatically forward all mail to the victim. The attacker can reply to the confirmation emails. But since the emails will be coming from a single forwarding source, it can simply be blocked by the user.

- ZIP bombing - the latest twist on email bombing using ZIP archived attachments. Mail servers always check email attachments for viruses, especially zip archives and .exe files. The idea here is to place a text file with millions or billions of arbitrary characters or even a single letter repeated millions of times so that the scanner would require a greater amount of processing power to read each one. Combining this with mass mailing techniques ups the potential for a denial of service attack to succeed.

1.12 SECURITY MEASURES

Security refers to providing a protection system to computer system resources such as CPU, memory, disk, software programs and most importantly data/information stored in the computer system. If a computer program is run by an unauthorized user, then he/she may cause severe damage to computer or data stored in it. So a computer system must be protected against unauthorized access, malicious access to system memory, viruses, worms etc. We're going to discuss following topics in this chapter.

- Authentication
- One Time passwords
- Program Threats
- System Threats
- Computer Security Classifications

Authentication

Authentication refers to identifying each user of the system and associating the executing programs with those users. It is the responsibility of the Operating System to create a protection system which ensures that a user who is running a particular program is authentic. Operating Systems generally identifies/authenticates users using following three ways "

- Username / Password " User need to enter a registered username and password with Operating system to login into the system.
- User card/key " User need to punch card in card slot, or enter key generated by key generator in option provided by operating system to login into the system.
- User attribute - fingerprint/ eye retina pattern/ signature " User need to pass his/her attribute via designated input device used by operating system to login into the system.

One Time passwords

One-time passwords provide additional security along with normal authentication. In One-Time Password system, a unique password is required every time user tries to login into the system. Once a one-time password is used, then it cannot be used again. One-time password are implemented in various ways.

- Random numbers " Users are provided cards having numbers printed along with corresponding alphabets. System asks for numbers corresponding to few alphabets randomly chosen.
- Secret key " User are provided a hardware device which can create a secret id mapped with user id. System asks for such secret id which is to be generated every time prior to login.
- Network password " Some commercial applications send one-time passwords to user on registered mobile/ email which is required to be entered prior to login.

Program Threats

Operating system's processes and kernel do the designated task as instructed. If a user program made these process do malicious tasks, then it is known asProgram Threats. One of the common example of program threat is a program installed in a computer which can store and send user credentials via network to some hacker. Following is the list of some well-known program threats.

- Trojan Horse " Such program traps user login credentials and stores them to send to malicious user who can later on login to computer and can access system resources.
- Trap Door " If a program which is designed to work as required, have a security hole in its code and perform illegal action without knowledge of user then it is called to have a trap door.
- Logic Bomb " Logic bomb is a situation when a program misbehaves only when certain conditions met otherwise it works as a genuine program. It is harder to detect.
- Virus " Virus as name suggest can replicate themselves on computer system. They are highly dangerous and can modify/delete user files, crash systems. A virus is generatlly a small code embedded in a program. As user accesses the program, the virus starts getting embedded in other files/ programs and can make system unusable for user

System Threats

System threats refers to misuse of system services and network connections to put user in trouble. System threats can be used to launch program threats on a complete network called as program attack. System threats creates such an environment that operating system resources/ user files are misused. Following is the list of some well-known system threats.

- Worm " Worm is a process which can choked down a system performance by using system resources to extreme levels. A Worm process generates its multiple copies where each copy uses system resources, prevents all other processes to get required resources. Worms processes can even shut down an entire network.
- Port Scanning " Port scanning is a mechanism or means by which a hacker can detects system vulnerabilities to make an attack on the system.
- Denial of Service " Denial of service attacks normally prevents user to make legitimate use of the system. For example, a user may not be able to use internet if denial of service attacks browser's content settings.

1.13 COMPUTER SECURITY CLASSIFICATIONS

As per the U.S. Department of Defense Trusted Computer System's Evaluation Criteria there are four security classifications in computer systems: A, B, C, and D. This is widely used specifications to determine and model the security of systems and of security solutions. Following is the brief description of each classification.

Classification Type Description
Type A Highest Level. Uses formal design specifications and verification techniques. Grants a high degree of assurance of process security.
Type B Provides mandatory protection system. Have all the properties of a class C2 system. Attaches a sensitivity label to each object. It is of three types. • B1 - Maintains the security label of each object in the system. Label is used for making decisions to access control. • B2 - Extends the sensitivity labels to each system resource, such as storage objects, supports covert channels and auditing of events. • B3 - Allows creating lists or user groups for access-control to grant access or revoke access to a given named object.
Type C Provides protection and user accountability using audit capabilities. It is of two types. • C1 - Incorporates controls so that users can protect their private information and keep other users from accidentally reading / deleting their data. UNIX versions are mostly Cl class. • C2 - Adds an individual-level access control to the capabilities of a Cl level system.
Type D Lowest level. Minimum protection. MS-DOS, Window 3.1 fall in this category.

CHAPTER 2

2.1 REVERSE ENGINEERING

Reverse engineering is the process of extracting the knowledge or design blueprints from anything man-made. The concept has been around since long before computers or modern technology, and probably dates back to the days of the industrial revolution. It is very similar to scientific research, in which a researcher is attempting to work out the "blueprint" of the atom or the human mind. The difference between reverse engineering and conventional scientific research is that with reverse engineering the artifact being investigated is manmade, unlike scientific research where it is a natural phenomenon.

Reverse engineering is usually conducted to obtain missing knowledge, ideas, and design philosophy when such information is unavailable. In some cases, the information is owned by someone who isn't willing to share them. In other cases, the information has been lost or destroyed. Traditionally, reverse engineering has been about taking shrink-wrapped products and physically dissecting them to uncover the secrets of their design. Such secrets were then typically used to make similar or better products. In many industries, reverse engineering involves examining the product under a microscope or taking it apart and figuring out what each piece does. Not too long ago, reverse engineering was actually a fairly popular hobby, practiced by a large number of people (even if it wasn't referred to as reverse engineering). Remember how in the early days of modern electronics, many people were so amazed by modern appliances such as the radio and television set that it became common practice to take them apart and see what goes on inside? That was reverse engineering. Of course, advances in the electronics industry have made this practice far less relevant. Modern digital electronics are so miniaturized that nowadays you really wouldn't be able to see much of the interesting stuff by just opening the box.

Software Reverse Engineering: Reversing

Software is one of the most complex and intriguing technologies around us nowadays, and software reverse engineering is about opening up a program's "box," and looking inside. Of course, we won't need any screwdrivers on this journey. Just like software engineering, software reverse engineering is a purely virtual process, involving only a CPU, and the human mind.

Software reverse engineering requires a combination of skills and a thorough understanding of computers and software development, but like most worthwhile subjects, the only real prerequisite is a strong curiosity and desire to learn. Software reverse engineering integrates several arts: code breaking, puzzle solving, programming, and logical analysis.

2.2 REVERSING APPLICATIONS

It would be fair to say that in most industries reverse engineering for the purpose of developing competing products is the most well-known application of reverse engineering. The interesting thing is that it really isn't as popular in the software industry as one would expect. There are several reasons for this, but it is primarily

because software is so complex that in many cases reverse engineering for competitive purposes is thought to be such a complex process that it just doesn't make sense financially.

So what are the common applications of reverse engineering in the software world? Generally speaking, there are two categories of reverse engineering applications: security-related and software development–related. The following sections present the various reversing applications in both categories.

2.3 SECURITY-RELATED REVERSING

For some people the connection between security and reversing might not be immediately clear. Reversing is related to several different aspects of computer security. For example, reversing has been employed in encryption research—a researcher reverses an encryption product and evaluates the level of security it provides. Reversing is also heavily used in connection with malicious software, on both ends of the fence: it is used by both malware developers and those developing the antidotes. Finally, reversing is very popular with crackers who use it to analyze and eventually defeat various copy protection schemes.

Malicious Software

The Internet has completely changed the computer industry in general and the security-related aspects of computing in particular. Malicious software, such as viruses and worms, spreads so much faster in a world where millions of users are connected to the Internet and use e-mail daily. Just 10 years ago, a virus would usually have to copy itself to a diskette and that diskette would have to be loaded into another computer in order for the virus to spread. The infection process was fairly slow, and defense was much simpler because the channels of infection were few and required human intervention for the program to spread. That is all ancient history—the Internet has created a virtual connection between almost every computer on earth. Nowadays modern worms can spread *automatically* to millions of computers without any human intervention.

Reversing is used extensively in both ends of the malicious software chain. Developers of malicious software often use reversing to locate vulnerabilities in operating systems and other software. Such vulnerabilities can be used to penetrate the system's defense layers and allow infection—usually over the Internet. Beyond infection, culprits sometimes employ reversing techniques to locate software vulnerabilities that allow a malicious program to gain access to sensitive information or even take full control of the system.

At the other end of the chain, developers of antivirus software dissect and analyze every malicious program that falls into their hands. They use reversing techniques to trace every step the program takes and assess the damage it could cause, the expected rate of infection, how it could be removed from infected systems, and whether infection can be avoided altogether.

Reversing Cryptographic Algorithms

Cryptography has always been based on secrecy: Alice sends a message to Bob, and encrypts that message using a secret that is (hopefully) only known to her and Bob. Cryptographic algorithms can be roughly divided

into two groups: restricted algorithms and key-based algorithms. Restricted algorithms are the kind some kids play with; writing a letter to a friend with each letter shifted several letters up or down. The secret in restricted algorithms is the algorithm itself. Once the algorithm is exposed, it is no longer secure.

Restricted algorithms provide very poor security because reversing makes it very difficult to maintain the secrecy of the algorithm. Once reversers get their hands on the encrypting or decrypting program, it is only a matter of time before the algorithm is exposed. Because the algorithm is the secret, reversing can be seen as a way to break the algorithm. On the other hand, in key-based algorithms, the secret is a key, some numeric value that is used by the algorithm to encrypt and decrypt the message.

In key-based algorithms users encrypt messages using keys that are kept private. The algorithms are usually made public, and the keys are kept private (and sometimes divulged to the legitimate recipient, depending on the algorithm). This almost makes reversing pointless because the algorithm is already known. In order to decipher a message encrypted with a key-based cipher, you would have to either:

- Obtain the key
- Try all possible combinations until you get to the key
- Look for a flaw in the algorithm that can be employed to extract the key or the original message

Still, there are cases where it makes sense to reverse engineer private implementations of key-based ciphers. Even when the encryption algorithm is well known, specific implementation details can often have an unexpected impact on the overall level of security offered by a program. Encryption algorithms are delicate, and minor implementation errors can sometimes completely invalidate the level of security offered by such algorithms. The only way to really know for sure whether a security product that implements an encryption algorithm is truly secure is to either go through its source code (assuming it is available), or to reverse it.

Digital Rights Management

Modern computers have turned most types of copyrighted materials into digital information. Music, films, and even books, which were once only available on physical analog mediums, are now available digitally. This trend is a mixed blessing, providing huge benefits to consumers, and huge complications to copyright owners and content providers. For consumers, it means that materials have increased in quality, and become easily accessible and simple to manage. For providers, it has enabled the distribution of high-quality content at low cost, but more importantly, it has made controlling the flow of such content an impossible mission. Digital information is incredibly fluid. It is very easy to move around and can be very easily duplicated. This fluidity means that once the copyrighted materials reach the hands of consumers, they can be moved and duplicated so easily that piracy almost becomes common practice. Traditionally, software companies have dealt with piracy by embedding copy protection technologies into their software. These are additional pieces of software embedded on top of the vendor's software product that attempt to prevent or restrict users from copying the program. In recent years, as digital media became a reality, media content providers have developed or acquired technologies that control the

distribution of content such as music, movies, etc. These technologies are collectively called digital rights management (DRM) technologies. DRM technologies are conceptually very similar to traditional software copy protection technologies discussed above. The difference is that with software, the thing which is being protected is active or "intelligent," and can decide whether to make itself available or not. Digital media is a passive element that is usually played or read by another program, making it more difficult to control or restrict usage.

Auditing Program Binaries

One of the strengths of open-source software is that it is often inherently more dependable and secure. Regardless of the real security it provides, it just *feels* much safer to run software that has often been inspected and approved by thousands of *impartial* software engineers. Needless to say, open-source software also provides some real, tangible quality benefits. With open-source software, having open access to the program's source code means that certain vulnerabilities and security holes can be discovered very early on, often before malicious programs can take advantage of them. With proprietary software for which source code is unavailable, reversing becomes a viable (yet admittedly limited) alternative for searching for security vulnerabilities.

2.3 Frauds can be categorized by the type of victim involved. The most common groups of victims encountered by Fraud Examiners include:

- Funders & Donors Creditors
- Businesses
- Banks or other financial institutions
- Central or local government
- Fraud by manipulating financial markets
- Frauds can also be categorized by the technique or activity used by the fraudster.

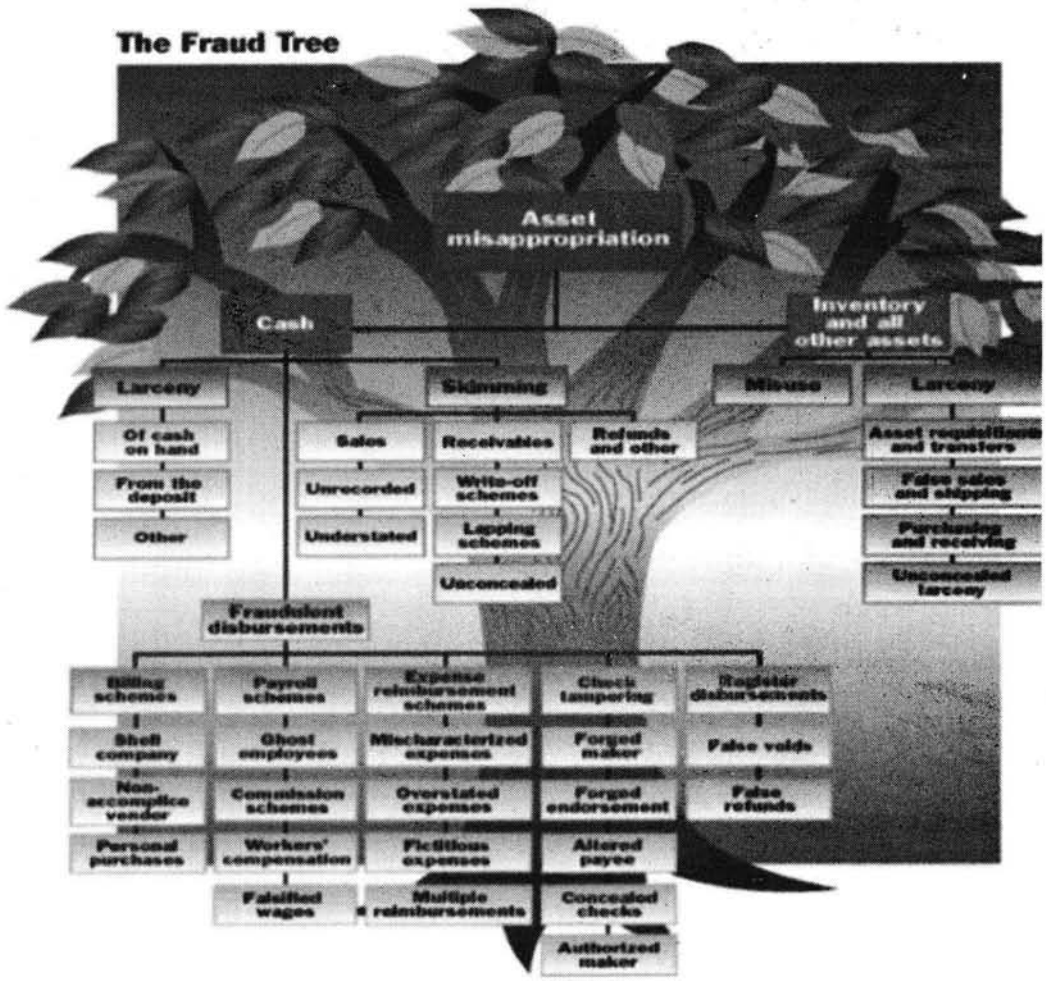
These include but not limited to: Advance fee frauds

- Bogus invoices
- Contract Procurement
- Computer hacking of information or property
- Conflict of Interest
- Corruption and bribery
- Counterfeiting, forgery
- Credit Card fraud
- False Accounting - manipulation of accounts, shares, accounting records
- Fraudulent bankruptcy - exploitation of cross-border corporate structures
- Financial Statement Fraud
- Fraud Risk Analysis

- Insurance fraud
- Internet online scams - auctions, credit card purchases, investment scams
- Investment fraud
- Misappropriation of assets
- Money laundering
- Payroll fraud - ghost employees
- Principal agents - failure of systems to restrict key individuals
- Pyramid schemes

2.4 THE FRAUD TREE – ASSET MISAPPROPRIATION

Over the years, the asset misappropriation chart has become known as the "fraud tree" for its numerous branches. The tree's trunk consists of two major asset types: cash, and inventory and all other assets. Crooked employees clearly favor misappropriating the former—nearly nine in 10 illegal schemes involve the cash account. The reasons should not be surprising: Cash is fungible, has a specific value and is easily transported. Inventory—except for consumer goods—has limited usefulness to a thief; an employee in a ball bearing plant can have a hard time converting the loot into cash. And of course, many business enterprises don't have a physical inventory at all.



Money laundering is a term used to describe a scheme in which criminals try to disguise the identity, original ownership, and destination of money that they have obtained through criminal conduct. The laundering is done with the intention of making it seem that the proceeds have come from a legitimate source. A simpler definition of money laundering would be a series of financial transactions that are intended to transform ill-gotten gains into legitimate money or other **assets**.

What is Money Laundering?

When money is obtained from criminal acts such as drug trafficking or illegal gambling, the money is considered "dirty" in that it may seem suspicious if deposited directly into a bank or other financial institution. Because the money's owner needs to create financial records ostensibly showing where the money came from, the money must be "cleaned," by running it through a number of legitimate businesses before depositing it, hence the term "money laundering." Because the act is specifically used to hide illegally obtained money, it too is unlawful.

Different jurisdictions, both foreign and domestic, have their own specific definitions of what acts constitute the crime of money laundering. Which enforcement agency has the authority to investigate money laundering, as well as punishments for the crime, are outlined in the statutes of each jurisdiction.

It has been estimated that at least $300 billion is laundered each year in the United States alone. According to a 2009 study published by the United States Sentencing Commission, more than 81,000 people are convicted of money laundering on some level each year in the United States.

Steps in Money Laundering

Money laundering is accomplished in many ways, though most include three common steps, including

1. Obtaining the money or introducing it into the financial system in some way
2. Transferring or concealing the source of the money through complex or multiple transactions
3. Returning the money back into the financial world so that it appears legitimate.

Of these steps, placement of the money into financial institutions is the most difficult. This is because the Bank Secrecy Act of 1970 requires financial institutions to report deposits over $10,000 in a single day. To circumvent this step then, launderers funnel cash through a legitimate high-cash business, such as a check cashing service, bar, nightclub, or convenience store.

Ways Criminals Avoid Detection

Large scale criminal groups may use complex money laundering techniques in order to avoid detection. However, smaller scale criminals or first time offenders often use simpler methods in their attempt avoid detection. Such money laundering techniques may include:

- Transferring money from bank to bank or from account to account
- Breaking up large amounts into smaller bank deposits
- Purchasing money orders in smaller money amounts
- Breaking the cash into small amounts and purchasing cashier's checks

For example, Sally steals a large amount of cash from her business. She wants the money to go undetected, so instead of making one large deposit into her savings or banking account, she breaks the money up and deposits one small amount each week. This ensures the bank does not look at her transaction suspiciously since it is uncommon for her to deposit large sums of money.

2.4 Money Laundering Techniques

There are many forms of money laundering though some are more common and profitable than others. Some of the more popular money laundering techniques include:

- **Bulk cash smuggling** involves literally smuggling cash into another country for deposit into offshore banks or other type of financial institutions that honor client secrecy.
- **Structuring**, also referred to as "smurfing," is a method in which cash is broken down into smaller amount, which are then used to purchase money orders or other instruments to avoid detection or suspicion.
- **Trade-based laundering** is similar to embezzlement in that invoices are altered to show a higher or lower amount in order to disguise the movement of money.
- **Cash-intensive business** occurs when a business that legitimately deals with large amounts of cash uses its accounts to deposit money obtained from both everyday business proceeds and money obtained through illegal means. Businesses able to claim all of these proceeds as legitimate income include those that provide services rather than goods, such as strip clubs, car washes, parking buildings or lots, and other businesses with low variable costs.
- **Shell companies** and trusts are used to disguise the true owner or agent of a large amount of money.
- **Bank capture** refers to the use of a bank owned by money launderers or criminals, who then move funds through the bank without fear of investigation.
- **Real estate laundering** occurs when someone purchases real estate with money obtained illegally, then sells the property. This makes it seem as if the profits are legitimate.
- **Casino laundering** involves an individual going into a casino with illegally obtained money. The individual purchases chips with the cash, plays for a while, then cashes out the chips, and claims the money as gambling winnings.

2.5 Anti-Money Laundering Laws

Anti-money laundering laws reflect an effort made the government to stop money laundering methods that involve financial institutions. Under the guidelines set forth by anti-money laundering, or "AML" financial institutions are required to verify large sums of money passing through the institution, and they are required to report suspicious transactions. It is estimated that money laundering is so prominent globally, that it is impossible for the Financial Action Task Force to produce estimates or figures as to its scope.

Financial Action Task Force

The Financial Action Task Force ("FATF") was formed in 1989 by a coalition of countries. This intergovernmental agency was designed to develop and promote international cooperation for combating money laundering. As of 2015, the FATF is comprised of 34 different countries, but the agency is always seeking to expand its membership to more regions. Headquartered in Paris, France, the FATF also works to combat the financing of terrorism. The FATF has developed recommendations to combat money laundering, and the agency has three functions in regards to this criminal activity:

1. Monitoring the progress of member countries in their anti-money laundering measures
2. Reviewing trends and techniques in money laundering, reporting these, as well as new countermeasures, to member countries
3. Promoting FATF anti-money laundering measures and standards globally

2.6 BANK SECRECY ACT

The Bank Secrecy Act (the "BSA") was enacted by Congress in 1970, as an effort to combat the use of financial institutions in money laundering crimes. The Act contains laws that require financial institutions to report certain transactions to the United States Department of Treasury, including transactions in excess of $10,000. The institutions must also file a Suspicious Activity Report, or "SAR," if they consider any financial transaction suspicious or believe the funds comes from unlawful activities. The Act is also responsible for the creation of the Financial Crimes Enforcement Network, which makes reports of money-laundering or suspicious activity available to criminal investigators around the world.

Other Anti-Money Laundering Regulations

Since the BSA was created, many other legislative acts and money laundering regulations have came about to strengthen the movement. These include:

- **The Money Laundering Control Act of 1986**, which prohibits engaging in any transactions involving proceeds generated from illegal activities.

- **The 1988 Anti-Drug Abuse Act**, which expanded the definition of "financial institution" to include car dealers and real estate personnel, requiring them to file reports on transactions involving large amounts of currency.
- **The 1992 Annunzio-Wylie Anti-Money Laundering Act**, which requires more strict sanctions for violations of the BSA, and requiring additional verifications, recordkeeping, and reporting for wire transfers.
- **The Money Laundering Suppression Act of 1994** requires banks to develop and institute training in anti money laundering examination procedures.
- **The Money Laundering and Financial Crimes Strategy Act of 1998** requires banking agencies to develop training for examiners.

Unfortunately, as these money laundering regulations are put into place, criminals work to find new methods to prevent their activity from becoming detected or considered suspicious.

The Role of Financial Institutions in Combating Money Laundering

In this age of electronic transactions to and from financial institutions around the globe, anti money laundering laws attempt to quell money laundering by requiring these institutions to identify and report suspicious activities. Technology has also paved the way for anti-money laundering software, detects large increases in account balances or large withdrawals, and which filters data and classifies it according to levels of suspicion. Software is also used to detect transactions with banking institutions in blacklisted or hostile countries. When such transactions are identified, the program alerts bank managers who then study the information and decide whether it should be reported to the government.

Penalties for Money Laundering

The penalties for money laundering vary greatly depending on the circumstance and the amount of funds involved. The penalties may also vary if the acts occurred in more than one jurisdiction. In addition to imprisonment, punishment for money laundering may include large fines, restitution, and community service. Typically, the more money involved, the harsher the punishment.

S.No.	Section	Offence Name	Description	Penalty
1.	65	Tampering with computer source document	Intentional concealment, destruction or alteration of the computer source code which is required to be kept or maintained by law	Imprisonment up to 3 years or with fine up to 2 lakh Rupees or with both.
2.	66	Hacking with Computer System	Destruction, deletion or alteration of any information residing in a computer resource, decreasing its value or utility or affecting it injuriously by whatever means intentionally or knowingly.	Imprisonment up to 3 years or with fine up to 2 lakh Rupees or with both.
3.	67	Publishing of information which is obscene in electronic form	Publication or transmission by a person or through someone else in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such which tends to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.	On first conviction with imprisonment up to 5 years and with fine up to 1 lakh Rupees and in the event of a second or subsequent conviction with imprisonment up to 10 years and also with fine up to 2 lakh Rupees.
4.	71	Misrepresentation to the Controller or the Certifying	Making any misrepresentation to,or suppression of any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be.	Imprisonment for a term which may extend to 2 years, or with fine up to 1 lakh Rupees, or with both
5.	72	Authority Penalty for breach of confidentiality and privacy Publishing	Any person, who, in pursuance of any of the powers conferred under IT Act, has secured access to any electronic record, book, register, correspondence, information or document without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document to any other person.	Imprisonment for a term which may extend to 2 years, or with fine up to 1 lakh Rupees, or with both.
6.	73	Digital Signature Certificate false in certain particulars	Publishing a Digital Signature Certificate or otherwise making it available to any other person with the knowledge that the Certifying Authority listed in the certificate has not issued it or the subscriber listed in the certificate has not accepted it or the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.	Imprisonment for a term which may extend to 2 years, or with fine which may extend to 1 lakh Rupees.
7.	74	Publication for fraudulent purpose	Creation, publication or otherwise making available a Digital Signature Certificate for any fraudulent or unlawful purpose.	Imprisonment for a term which may extend to 2 years, or with fine up to 1 lakh Rupees, or with both.

Cyber espionage

It is the act or practice of obtaining secrets from individuals, competitors, rivals, groups, governments, and enemies for military, political, or economic advantage using illegal exploitation methods on the internet.

Sabotage

Sabotage literally means willful damage to any machinery or materials or disruption of work. In the context of cyberspace, it is a threat to the existence of computers and satellites used by military activities

2.7 Information Technology Act, 2000

The introduction of the internet has brought the tremendous changes in our lives. People of all fields are increasingly using the computers to create, transmit and store information in the electronic form instead of the traditional papers, documents. Information stored in electronic forms has many advantages, it is cheaper, easier to store, easier to retrieve and for speedier to connection. Though it has many advantages, it has been misused by many people in order to gain themselves or for sake or otherwise to harm others. The high and speedier connectivity to the world from any place has developed many crimes and these increased offences led to the need of law for protection. Some countries have been rather been vigilant and formed some laws governing the net. In order to keep in pace with the changing generation, the Indian Parliament passed the law — Information Technology Act 2000. The IT Act 2000 has been conceptualized on the United Nations Commissions on International Trade Law (UNCITRAL) Model Law.

The increase rate of technology in computers has led to enactment of Information Technology Act 2000. The converting of the paper work into electronic records, the storage of the electronic data, has led tremendous changed the scenario of the country. The Act further amends the Indian Penal Code, 1860, The Evidence Act, 1872, The Bankers Books Evidence Act, 1891 and The Reserve Bank of India Act, 1934.

The salient features of the I.T Act are as follows "

- Digital signature has been replaced with electronic signature to make it a more technology neutral act.
- It elaborates on offenses, penalties, and breaches.
- It outlines the Justice Dispensation Systems for cyber-crimes.
- It defines in a new section that *cyber café is any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public.*
- It provides for the constitution of the Cyber Regulations Advisory Committee.
- It is based on The Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934, etc.
- It adds a provision to Section 81, which states that the provisions of the Act shall have overriding effect. The provision states that *nothing contained in the Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957.*

Section 65: Tampering with computer source documents Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network,

when the computer source code is required to be kept or maintained by law for the being time in force, shall be punishable with imprisonment up to three year, or with fine which may extend up to two lakh rupees, or with both.

Explanation: For the purpose of this section computer source code' means the

listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Object: The object of the section is to protect the intellectual property' invested in

the computer. It is an attempt to protect the computer source documents (codes) beyond what is available under the Copyright Law.

Essential ingredients of the section

1. Knowingly or intentionally concealing,
2. Knowingly or intentionally destroying,
3. Knowingly or intentionally altering,
4. Knowingly or intentionally causing others to conceal,
5. Knowingly or intentionally causing another to destroy,
6. Knowingly or intentionally causing another to alter.

This section extends towards the Copyright Act and helps the companies to protect their source code of their programmes.

Penalties: Section 65 is tried by any magistrate. This is cognizable and non-bailable offence.

Penalties: Imprisonment up to 3 years and / or Fine: Two lakh rupees.

Case Laws

i. Frios v/s State of Kerala

Facts: In this case it was declared that the FRIENDS application software as protected system. The author of the application challenged the notification and the constitutional validity of software under Section 70. The court upheld the validity of both.

It included tampering with source code. Computer source code the electronic form, it can be printed on paper.

Held: The court held that tampering with Source code are punishable with three years jail and or two lakh rupees fine of rupees two lakh rupees for altering, concealing and destroying the source code.

ii. Syed Asifuddin Case

Facts: In this case the Tata Indicom employees were arrested for manipulation of the electronic 32- bit number (ESN) programmed into cell phones theft were exclusively franchised to Reliance Infocom.

Held: Court held that Tampering with source code invokes Section 65 of the Information Technology Act.

iii. Parliament Attack Case

Facts: In this case several terrorist attacked on 13 December, 2001 Parliament House. In this the Digital evidence played an important role during their prosecution. The accused argued that computers and evidence can easily be tampered and hence should not be relied.

In Parliament case several smart device storage disks and devices, a Laptop were recovered from the truck intercepted at Srinagar pursuant to information given by two suspects. The laptop included the evidence of fake identity cards, video files containing clips of the political leaders with the background of Parliament in the background shot from T.V news channels. In this case design of Ministry of Home Affairs car sticker, there was game wolf pack36 with user name of ¯Ashiq . There was the name in one of the fake identity cards used by the terrorist. No back up was taken therefore it was challenged in the Court.

Held: Challenges to the accuracy of computer evidence should be established by the challenger. Mere theoretical and generic doubts cannot be cast on the evidence.

Section66: Hacking with the computer system

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both. *Explanation:* The section tells about the hacking activity.

Essential ingredients of the section:

1. Whoever with intention or knowledge.
2. Causing wrongful loss or damage to the public or any person.
3. Destroying or altering any information residing in a computer resource.
4. Or diminishes its value or utility or.
5. Affects it injuriously by any means.

Penalties: Punishment: Imprisoned up to three years and Fine: This may extend up to two lakh rupees or with both. Case Laws:

1. R v/s Gold & Schifreen

In this case it is observed that the accused gained access to the British telecom Prestly Gold computers networks file amount to dishonest trick and not criminal offence.

2. R v/s Whiteley.

In this case the accused gained unauthorized access to the Joint Academic Network (JANET) and deleted, added files and changed the passwords to deny access to the authorized users.

The perspective of the section is not merely protect the information but to protect the integrity and security of computer resources from attacks by unauthorized person seeking to enter such resource, whatever may be the intention or motive.

Cases Reported In India:

Official website of Maharashtra government hacked.

The official website of the government of Maharashtra was hacked by Hackers Cool Al- Jazeera, and claimed them they were from Saudi Arabia.

Section 67: Publishing of obscene information in electronic form

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstance, to read see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

Essential ingredients of this section:

Publishing or transmitting, or causing to be published, pornographic material in electronic form.

Penalties: Punishment:

On first conviction- imprisonment which may extend up to five years. Fine: up to on first conviction which may extend to one lakh rupees.

On second conviction- imprisonment up to which may extend to ten years and Fine which may extend up to two lakh rupees.

Case Laws

1. The State of Tamil Nadu v/s Suhas Katti.

Facts: This case is about posting obscene, defamatory and annoying message about a divorcee woman in the Yahoo message group. E-mails were forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. These postings resulted in annoying phone calls to the lady. Based on the complaint police nabbed the accused. He was a known family friend of the victim and was interested in marrying her. She married to another person, but that marriage ended in divorce and the accused started contacting her once again. And her reluctance to marry him he started harassing her through internet.

Held: The accused is found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000 and the accused is convicted and is sentenced for the offence to undergo RI for 2 years under 469 IPC and to pay fine of Rs.500/-and for the offence u/s 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay fine of Rs.500/- and for the offence u/s 67 of IT Act 2000 to undergo RI for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently.'

The accused paid fine amount and he was lodged at Central Prison, Chennai. This is considered the first case convicted under section 67 of Information Technology Act 2000 in India.

In a recent case, a groom's family received numerous emails containing defamatory information about the prospective bride. Fortunately, they did not believe the emails and chose to take the matter to the police. The sender of the emails turned out to be the girl's step-father, who did not want the girl to get married, as he would have lost control over her property, of which he was the legal guardian.

2. Avnish Bajaj (CEO of bazzee.com – now a part of the eBay group of companies) case.

Facts: There were three accused first is the Delhi school boy and IIT Kharagpur Ravi Raj and the service provider Avnish Bajaj.

The law on the subject is very clear. The sections slapped on the three accused were Section 292 (sale, distribution, public exhibition, etc., of an obscene object) and Section 294 (obscene acts, songs, etc., in a public place) of the Indian Penal Code (IPC), and Section 67 (publishing information which is obscene in electronic form) of the Information Technology Act 2000. In addition, the schoolboy faces a charge under Section 201 of the IPC (destruction of evidence), for there is apprehension that he had destroyed the mobile phone that he used in the episode. These offences invite a stiff penalty, namely, imprisonment ranging from two to five years, in the case of a first time conviction, and/or fines.

Held: In this case the Service provider Avnish Bajaj was later acquitted and the Delhi school boy was granted bail by Juvenile Justice Board and was taken into police charge and detained into Observation Home for two days.

3. DASKHINA Kannada police have solved the first case of cyber crime in the district.

A press release by Dakshina Kannada Police said here on Saturday that a Father at a Christian institution in the city had approached the Superintendent of Police with a complaint that he was getting offensive and obscene e-mails.

Police said that all the three admitted that they had done this to tarnish the image of the Father. As the three tendered an unconditional apology to the Father and gave a written undertaking that they would not repeat such act in future, the complainant withdrew his complaint. Following this, the police dropped the charges against the culprit.

The release said that sending of offensive and obscene e-mails is an offence under the Indian Information Technology Act 2000. If the charges are framed.

Section 68: Power of controller to give directions

- The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.
- Any person who fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding three years or to a fine not exceeding two lakh rupees or to both. *Explanation:* Any person who fails to comply with any order under sub section (1) of the above section, shall be guilty of an offence and shall be convicted for a term not less than three years or to a fine exceeding two lakh rupees or to both.

The under this section is non-bailable& cognizable.

Penalties:

Punishment: imprisonment up to a term not exceeding three years Fine: not exceeding two lakh rupees.

Section 69: Directions of Controller to a subscriber to extend

facilities to decrypt information

- If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence; for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.
- The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information.

- The subscriber or any person who fails to assist the agency referred to in sub section (2) shall be punished with an imprisonment for a term which may extend to seven years.

Penalties: Punishment: imprisonment for a term which may extend to seven years.

The offence is cognizable and non- bailable.

Section 70: Protected System

- The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.
- The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1).
- Any person who secures access or attempts to secure access to a protected system in contravention of the provision of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

Explanation: This section grants the power to the appropriate government to

declare any computer, computer system or computer network, to be a protected system. Only authorized person has the right to access to protected system.

Penalties: Punishment: the imprisonment which may extend to ten years and fine.

Section 71: Penalty for misrepresentation

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or which fine which may extend to one lakh rupees, or with both.

Penalties:

Punishment: imprisonment which may extend to two years

Fine: may extend to one lakh rupees or with both.

Section 72: Penalty for breach of confidentiality and privacy Save as otherwise provide in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulation made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Explanation: This section relates to any to any person who in pursuance of any of

the powers conferred by the Act or it allied rules and regulations has secured access to any: Electronic record, books, register, correspondence, information, document, or other material.

If such person discloses such information, he will be punished with punished. It would not apply to disclosure of personal information of a person by a website, by his email service provider.

Penalties:

Punishment: term which may extend to two years.

Fine: one lakh rupees or with both.

Section 73: Penalty for publishing Digital Signature Certificate false in certain particulars

1. No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that-

- ❒ The Certifying Authority listed in the certificate has not issued it; or
- ❒ The subscriber listed in the certificate has not accepted it; or
- ❒ The certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

2. Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Explanation: The Certifying Authority listed in the certificate has not issued it or,

The subscriber listed in the certificate has not accepted it or the certificate has been revoked or suspended.

The Certifying authority may also suspend the Digital Signature Certificate if it is of the opinion that the digital signature certificate should be suspended in public interest.

A digital signature may not be revoked unless the subscriber has been given opportunity of being heard in the matter. On revocation the Certifying Authority need to communicate the same with the subscriber. Such publication is not an offence it is the purpose of verifying a digital signature created prior to such suspension or revocation.

Penalties:

Punishment: imprisonment of a term of which may extend to two years.

Fine: fine may extend to 1 lakh rupees or with both Case Laws:

Bennett Coleman & Co. v/s Union of India.

In this case the publication has been stated that ¯publication means dissemination and circulation ¶–@ Ð–□. In the context of digital medium, the term publication includes and transmission of information or data in electronic form.

Section 74: Publication for fraudulent purpose

Whoever knowingly creates publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which extend to one lakh rupees, or with both.

Explanation: This section prescribes punishment for the following acts:

Knowingly creating a digital signature certificate for any

- ❒ Fraudulent purpose or,
- ❒ Unlawful purpose.

Knowingly publishing a digital signature certificate for any

- ❒ Fraudulent purpose or
- ❒ Unlawful purpose

Knowingly making available a digital signature certificate for any

- ❒ Fraudulent purpose or
- ❒ Unlawful purpose.

Penalties:

Punishment: imprisonment for a term up to two years. Fine: up to one lakh or both.

Section 75: Act to apply for offence or contravention **committed outside India**

1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.
2) For the purposes of sub-section (1), this Act shall apply to an offence or Contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

Explanation : This section has broader perspective including cybercrime, committed by cyber criminals, of any nationality, any territoriality.

Case Laws:

R v/s Governor of Brixton prison and another.

Facts: In this case the Citibank faced the wrath of a hacker on its cash management system, resulting in illegal transfer of funds from customers account in to the accounts of the hacker, later identified as Vladimir Levin and his accomplices. After Levin was arrested he was extradite to the United States. One of the most important issues was jurisdictional issue, the ¯place of origin ·–D-Ð–□ of the cybercrime.

Held: The Court held that the real- time nature of the communication link between Levin and Citibank computer meant that Levins keystrokes were actually occurring on the Citibank computer.

It is thus important that in order to resolve the disputes related to jurisdiction, the issue of territoriality and nationality must be placed by a much broader criteria embracing principles of reasonableness and fairness to accommodate overlapping or conflicting interests of states, in spirit of universal jurisdiction.

Section 76: Confiscation

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provisions of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation :

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit.

Explanation: The aforesaid section highlights that all devices whether computer,

computer system, floppies, compact disks, tape drives or any other storage, communication, input or output device which helped in the contravention of any provision of this Act, rules, orders, or regulations made under there under liable to be confiscated.

Section 77: Penalties or confiscation not to interfere with other punishments

No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

Explanation: The aforesaid section lays down a mandatory condition, which states the Penalties or confiscation not to interfere with other punishments to which the person affected thereby is liable under any other law for the time being in force.

Section 78: Power to investigate offences

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Deputy Superintendent of Police shall investigate any offence under this Act.

Explanation: The police officer not below the rank of Deputy Superintendent of

police shall investigate the offence.

Conclusion:

Due to the increase in the digital technology various offences has also increased. Since new-new technology come every day, the offences has also increased therefore the IT Act 2000 need to be amended in order to include those offences which are now not included in the Act.

In India cybercrime is of not of high rate therefore we have time in order to tighten the cyber laws and include the offences which are now not included in the IT Act 2000.

The following table shows the offence and penalties against all the mentioned sections of the I.T. Act "

Section	Offence	Punishment	Bailability and Congizability
65	Tampering with Computer Source Code	Imprisonment up to 3 years or fine up to Rs 2 lakhs	Offence is Bailable, Cognizable and triable by Court of JMFC
66	Computer Related Offences	Imprisonment up to 3 years or fine up to Rs 5 lakhs	Offence is Bailable, Cognizable and
66-A	Sending offensive messages through Communication service, etc...	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable and triable by Court of JMFC
66-B	Dishonestly receiving stolen computer resource or communication device	Imprisonment up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-C	Identity Theft	Imprisonment of either description up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-D	Cheating by Personation by using computer resource	Imprisonment of either description up to 3 years and /or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-E	Violation of Privacy	Imprisonment up to 3 years and /or fine up to Rs. 2 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-F	Cyber Terrorism	Imprisonment extend to imprisonment for Life	Offence is Non-Bailable, Cognizable and triable by Court of Sessions

Section	Offence	Punishment	Bailability and Congizability
67	Publishing or transmitting obscene material in electronic form	On first Conviction, imprisonment up to 3 years and/or fine up to Rs. 5 lakh On Subsequent Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh	Offence is Non-Bailable, Cognizable and triable by Court of JMFC
67-A	Publishing or transmitting of material containing sexually explicit act, etc... in electronic form	On first Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non-Bailable, Cognizable and triable by Court of JMFC
67-B	Publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form	On first Conviction imprisonment of either description up to 5 years and/ or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment of either description up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non Bailable, Cognizable and triable by Court of JMFC
67-C	Intermediary intentionally or knowingly contravening the directions about Preservation and retention of information	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.
68	Failure to comply with the directions given by Controller	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
69	Failure to assist the agency referred to in sub section (3) in regard interception or monitoring or decryption of any information through any computer resource	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.
69-A	Failure of the intermediary to comply with the direction issued for blocking for public access of any information through any computer resource	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.

Section	Offence	Punishment	Bailability and Congizability
69-B	Intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) in regard monitor and collect traffic data or information through any computer resource for cybersecurity	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.
70	Any person who secures access or attempts to secure access to the protected system in contravention of provision of Sec. 70	Imprisonment of either description up to 10 years and fine	Offence is Non-Bailable, Cognizable.
70-B	Indian Computer Emergency Response Team to serve as national agency for incident response. Any service provider, intermediaries, data centres, etc., who fails to prove the information called for or comply with the direction issued by the ICERT.	Imprisonment up to 1 year and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable
71	Misrepresentation to the Controller to the Certifying Authority	Imprisonment up to 2 years and/ or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
72	Breach of Confidentiality and privacy	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
72-A	Disclosure of information in breach of lawful contract	Imprisonment up to 3 years and/or fine up to Rs. 5 lakh.	Offence is Cognizable, Bailable
73	Publishing electronic Signature Certificate false in certain particulars	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
74	Publication for fraudulent purpose	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.

2.8 MISUSE OF THE TECHNOLOGY

Though it has many advantages, it has been misused by many people in order to gain themselves or for sake or otherwise to harm others. The high and speedier connectivity to the world from any place has developed many crimes and these increased offences led to the need of law for protection. Some countries have been rather been vigilant and formed some laws governing the net. In order to keep in pace with the changing generation, the Indian Parliament passed the law — Information Technology Act 2000. The IT Act 2000 has been conceptualized on the United Nations Commissions on International Trade Law (UNCITRAL) Model Law.

The Indian Penal Code, 1860

Normally referred to as the IPC, this is a very powerful legislation and probably the most widely used in criminal jurisprudence, serving as the main criminal code of India. Enacted originally in 1860 and amended many time since, it covers almost all substantive aspects of criminal law and is supplemented by other criminal provisions. In independent India, many special laws have been enacted with criminal and penal provisions which are often referred to and relied upon, as an additional legal provision in cases which refer to the relevant provisions of IPC as well.60

The Indian Penal Code was amended by inserting the word 'electronic' thereby treating the electronic records and documents on a par with physical records and documents. The Sections dealing with false entry in a record or false document etc (e.g. 192, 204, 463, 464, 464, 468 to 470, 471, 474, 476 etc) have since been amended as 'electronic record and electronic document' thereby bringing within the ambit of IPC. Now, electronic record and electronic documents has been treated just like physical records and documents during commission of acts of forgery or falsification of physical records in a crime. After the above amendment, the investigating agencies file the cases/ charge-sheet quoting the relevant sections from IPC under section 463,464, 468 and 469 read with the ITA/ITAA under Sections 43 and 66 in like offences to ensure the evidence and/or punishment can be covered and proved under either of these or under both legislation.61

Misuse of Information Technology under Indian Penal Code, 186062

S.No.	Section	Offence Name	Description	Penalty
1.	Various sections		The IT Act amends the IPC. The word document now includes an electronic record. The result is that anyone using forged electronic record or certificates is punishable under the IPC for offences related to false evidences and certificates.	Imprisonments for terms which may extend to 10 years or with fine or with both.
2.	120 A	Criminal Conspiracy	Two or more persons agree to do an illegal act or an act by illegal means themselves or through some other persons or means.	Depending on the object of Conspiracy imprisonment for term from 6 months to life imprisonment with or without fine.
3.	153 A (1)	Promoting enmity between different groups	By words spoken or written, signs, visible representations or otherwise attempting to promote or promotion of enmity between different groups on grounds of religion, race, domicile, residence, language etc.	Imprisonment for a term which may extend to 3 years, or with fine or with both.
4.	292	Sale, etc., of obscene books, etc.	Selling, hiring, distribution, public exhibition or putting into circulation of obscene material, taking part or receiving profits of such business, advertisement etc.	On first conviction imprisonment up to 2 years with fine of 2000 Rupees on second or sequent conviction imprisonment up to 5 years with fine of 5000 Rupees.
5.	295 A	Deliberate and malicious acts, intended to outrage religious feelings of any class	Using words, signs or visible representations with deliberate and malicious intention to outrage religious feelings of a religious class.	Imprisonment for a term which may extend to 3 years, or with fine or with both.
6.	463	Forgery	Making any false electronic record or a part of it with the intention to cause damage or injury to public or any person to commit any fraud or enter into any express or implied contract.	Imprisonment for a term which may extend to 2 years, or with fine or with both.
7.	416	Cheating by personation	Cheating by pretending to be some other person or by knowingly substituting one person for another person representing that he or any other person is a person other he or such other person really is. Person personated could be a real or imaginary person.	Imprisonment for a term which may extend to 2 years, or with fine or with both.

S.No.	Section	Offence Name	Description	Penalty
8.	499	Defamation	Whoever by words either spoken or intended to be read or by signs or by visible representations makes or publishes any imputation concerning any person intending to harm the reputation of such person is said to defame.	Imprisonment for a term which may extend to 2 years, or with fine or with both.
9.	501	Printing orengraving matter known to be defamatory	Printing or engraving any matter knowing or having good reason to believe that such matter is defamatory.	Imprisonment for a term which may extend to 2 years, or with fine or with both.
10.	503	Criminal Intimidation	Threatening another with any injury to his person, reputation or property or to some person in whom one is interested with the intention to cause alarm to that person or causing him to do any illegal act in order to avoid the threat.	Imprisonments for a term which may extend from 2 years till 7 years, with fine or with both depending on the kind of threat given.
11.	505(1), (2)	Statements conducing to public mischief	Making, publishing or circulating any rumour or false report about armed forces of India or with intention to create enmity, hatred or ill-will between classes.	Imprisonment for a term which may extend to 3 years, or with fine or with both.
12.	507	Criminal Intimidation by anonymous communication	Criminal Intimidation by anonymous communication or having taken precaution to conceal name and whereabouts of the person giving threat.	Imprisonments for a term which may extend from 2 years till 7 years, with fine or with both depending on the kind of threat given and 2 years additional imprisonment.
13.	509	Word, gesture or act intended to insult the modesty of a woman	Utterance of words, making of sound, gesture or exhibition of object in order to intrude the privacy or insult the modesty of a woman.	Imprisonment for a term which may extend to 1 year, or with fine or with both.

2.9 PENALTIES AND ADJUDICATION

Digital Signature

A digital signature is a technique to validate the legitimacy of a digital message or a document. A valid digital signature provides the surety to the recipient that the message was generated by a known sender, such that the sender cannot deny having sent the message. Digital signatures are mostly used for software distribution, financial transactions, and in other cases where there is a risk of forgery.

Electronic Signature

An electronic signature or e-signature, indicates either that a person who demands to have created a message is the one who created it.

A signature can be defined as a schematic script related with a person. A signature on a document is a sign that the person accepts the purposes recorded in the document. In many engineering companies digital seals are also required for another layer of authentication and security. Digital seals and signatures are same as handwritten signatures and stamped seals.

Digital Signature to Electronic Signature

Digital Signature was the term defined in the old I.T. Act, 2000. **Electronic Signature** is the term defined by the amended act (I.T. Act, 2008). The concept of Electronic Signature is broader than Digital Signature. Section 3 of the Act delivers for the verification of Electronic Records by affixing Digital Signature.

As per the amendment, verification of electronic record by electronic signature or electronic authentication technique shall be considered reliable.

According to the **United Nations Commission on International Trade Law (UNCITRAL),** electronic authentication and signature methods may be classified into the following categories "

- Those based on the knowledge of the user or the recipient, i.e., passwords, personal identification numbers (PINs), etc.
- Those bases on the physical features of the user, i.e., biometrics.
- Those based on the possession of an object by the user, i.e., codes or other information stored on a magnetic card.
- Types of authentication and signature methods that, without falling under any of the above categories might also be used to indicate the originator of an electronic communication (Such as a facsimile of a handwritten signature, or a name typed at the bottom of an electronic message).

According to the UNCITRAL MODEL LAW on Electronic Signatures, the following technologies are presently in use "

- Digital Signature within a public key infrastructure (PKI)
- Biometric Device
- PINs
- Passwords
- Scanned handwritten signature
- Signature by Digital Pen
- Clickable "OK" or "I Accept" or "I Agree" click boxes

The faster world-wide connectivity has developed numerous online crimes and these increased offences led to the need of laws for protection. In order to keep in stride with the changing generation, the Indian Parliament passed the Information Technology Act 2000 that has been conceptualized on the United Nations Commissions on International Trade Law (UNCITRAL) Model Law.

The law defines the offenses in a detailed manner along with the penalties for each category of offence.

Offences

Cyber offences are the illegitimate actions, which are carried out in a classy manner where either the computer is the tool or target or both.

Cyber-crime usually includes the following "

- Unauthorized access of the computers
- Data diddling
- Virus/worms attack
- Theft of computer system
- Hacking
- Denial of attacks
- Logic bombs
- Trojan attacks
- Internet time theft
- Web jacking
- Email bombing
- Salami attacks
- Physically damaging computer system.

The offences included in the I.T. Act 2000 are as follows "

- Tampering with the computer source documents.
- Hacking with computer system.
- Publishing of information which is obscene in electronic form.
- Power of Controller to give directions.
- Directions of Controller to a subscriber to extend facilities to decrypt information.
- Protected system.
- Penalty for misrepresentation.
- Penalty for breach of confidentiality and privacy.
- Penalty for publishing Digital Signature Certificate false in certain particulars.
- Publication for fraudulent purpose.
- Act to apply for offence or contravention committed outside India Confiscation.
- Penalties or confiscation not to interfere with other punishments.
- Power to investigate offences.

Example

Offences Under The It Act 2000

Section 65. Tampering with computer source documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the being time in force, shall be punishable with imprisonment up to three year, or with fine which may extend up to two lakh rupees, or with both.

Explanation " For the purpose of this section "computer source code" means the listing of programs, computer commands, design and layout and program analysis of computer resource in any form.

Object " The object of the section is to protect the "intellectual property" invested in the computer. It is an attempt to protect the computer source documents (codes) beyond what is available under the Copyright Law

Essential ingredients of the section

knowingly or intentionally concealing

knowingly or intentionally destroying

knowingly or intentionally altering

knowingly or intentionally causing others to conceal

knowingly or intentionally causing another to destroy

knowingly or intentionally causing another to alter.

This section extends towards the Copyright Act and helps the companies to protect their source code of their programs.

Penalties " Section 65 is tried by any magistrate.

This is cognizable and non-bailable offence.

Penalties " Imprisonment up to 3 years and / or

Fine " Two lakh rupees.

OTHER PENALTIES AND ADJUDICATION

1. Penalty of damage of computer, computer system, etc.

If any person without permission of the owner or any other person who is incharge of a computer, computer or computer network,-

(a) accesses or secures access to such computer, computer system or computer network;

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorised to access any computer, or computer network by any means ;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder ;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Explanation.- For the purpose of this section,-

(i) "computer contaminant" means any set of computer instructions that are designed-

(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed some other event takes place in that computer resource;

(iv) "damage " means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

2. Penalty for failure to furnish information, return, etc.

If any person who is required under this Act or any rules or regulations made thereunder to-

(a) furnish any document, return or report to the Controller or the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;

(b) file any return or furnish any information, books or other documents within the time specified therefor in the regulation fails to file return or furnish the same within the time specified therefor in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;

(c) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

3. Residuary penalty

Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

4. Power to adjudicate

(1) For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made thereunder the Central Government shall, subject to the provisions of sub-section (3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government.

(2) The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

(3) No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government.

(4) Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

(5) Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under sub-section (2) of section 58, and-

(6) all proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code;

(7) shall be deemed to be a civil court for the purpose of section 345 and .46 of the Code of Criminal Procedure, 1973.

5.Factors to be taken into account by the adjudicating officer

While adjudging the quantum of compensation under this Chapter, the adjudicating officer shall have due regard to the following factors, namely :-

(a) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;

(b) the amount of loss caused to any person as a result of the default;

(c) the repetitive nature of the default.

2.10 ESTABLISHMENT OF CYBER APPELLATE TRIBUNAL(1) The Central Government shall, by notification, establish one or more appellate tribunals to be knownas the Cyber Regulations Appellate Tribunal.(2) The Central Government shall also specify, in the notification referred to in sub-section (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction. **Composition of Cyber Appellate Tribunal** A Cyber Appellate Tribunal shall consist of one person only (hereinafter referred to as the

Presiding Officer of the Cyber Appellate Tribunal) to be appointed, by notification, by the Central Government. **Appeal to Cyber Appellate Tribunal** (1) Save as provided in sub-section (2), any person aggrieved by an order made by Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal jurisdiction in the matter.(2) No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.(3) Every appeal under sub-section (1) shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or theadjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed :Provided that the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficientcause for not filing it within that period.(4) On receipt of an appeal under sub-section (1), the Cyber Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.(5) The Cyber Appellate Tribunal shall send a copy or every order made by it to the parties to the appeal and to the concerned Controller or adjudicating officer.(6) The appeal filed before the Cyber Appellate Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal. **Procedure and powers of the Cyber Appellate Tribunal**(1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sitting.(2) The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely : -(a) summoning and enforcing the attendance of any person and examining him on oath;(b) requiring the discovery and production of documents or other electronic records;(c) receiving evidence on affidavits;(d) issuing commissions for the examination of witnesses of documents;(e) reviewing its decisions;(f) dismissing an application for default or deciding it ex parte;(g) any other matter which may be prescribed.(3) Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purpose of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.**Right to legal representation**The appellant may either appear in person or authorise one or more legalpractitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal. **Limitation**The provisions of the Limitation Act, 1963, shall, as far as may be, apply to an appeal made to the Cyber Appellate Tribunal.**Civil court not to have jurisdiction**No court shall have jurisdictions to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act. **Recovery of penalty**A penalty imposed under this Act, if it is pad, shall be recovered as an arrear or land revenue and the licence or the Digital Signature Certificate, as the case may be, shall be suspended till the penalty is paid.

CHAPTER 3

3.1 The Goal of the Forensic Investigation - An Overview

Any investigation has a purpose. With this chapter we will start with the reasons why one would need to conduct an investigation involving computers. When we understand the reason why we are conducting the investigation, then we can develop a plan of action on how to conduct that investigation, and where to look for evidence. The information gathered during the investigation can be used for the enforcement of Human Resources (HR) rules for disciplinary action and even legal action. Therefore, the reasons for the investigation are almost as important as the investigation itself.

This chapter reviews several reasons why an investigation is needed and the plan of that investigation, based on those reasons. It also reviews the impact of the action that resulted in the complaint. We first need to determine the impact or feasibility of conducting the investigation. For example, if the cost of the investigation outweighs the benefits, there might not be a reason to conduct the investigation. For the most part, the decision to conduct the investigation is up to management. However, it is the investigators' responsibility to provide the information on which to allow management to base the decision to proceed.

Why Investigate?

First we will need to consider the complaint or the initial reason for conducting an investigation.

Some typical reasons that may warrant an investigation include but are not limited to:

- Internet usage exceeds norm
- Using e"mail inappropriately
- Use of Internet, e"mail, or PC in a non"work"related manner
- Theft of information
- Violation of security policies or procedures
- Intellectual property infractions
- Electronic tampering

Internet Exceeds Norm

If the complaint is that someone's Internet usage is too high, we should first determine the basis for this complaint. It should also be determined whether the above normal Internet usage was identified through electronic monitoring or by personal observation. It is also appropriate to determine if the usage is out"of"line with company standards for the type of job responsibilities held by the individual under investigation. Equally important is to determine how those standards were determined and developed.

There are different questions to be asked, and answered, in order to investigate the claim, depending on the basis of the complaint.

If the usage was electronically monitored:

1. Did a firewall monitor the usage?

2. Was the usage monitored by Internet Protocol (IP) address or individual identification (ID)?

3. What exactly was monitored? (e.g., time, sites, keywords, etc.)

4. Can more than one person use this personal computer (PC) (or IP address)?

5. Can more than one person use this ID?

6. Can the usage times/dates be correlated to physical access by the individual under investigation? (If monitoring shows access was between 8 a.m. and 10 a.m., was the individual at work during this time?)

7. What was the pattern of access?

8. How does this compare with the individual's work schedule? Could the individual have logged in and then not logged out? (i.e., get to an Internet site and then go to another task on the PC, thus leaving the Internet site up and running?)

9.Are there timeouts set on the Internet access? On the PC login?

10.Are there security cameras, login sheets, key card access logs, or timecards that can verify that it was the individual who accessed the Internet via this PC?

11. Is there a pattern to the usage?

Once you obtain answers to these questions you will begin to see the outlines of a plan of the investigation forming. For example, if Joe Programmer is accused of exceeding Internet norms, based on a report generated from the firewall monitoring system, we can ask some additional questions to validate the concern/ complaint.

If the pattern of unusually high utilization was after"hours when Joe was not scheduled to be at work, then there might be a deeper issue that will require further investigating to uncover (i.e., who and how someone was using Joe's ID after"hours). However, if the case is simply that Joe is logging into the Internet first thing in the morning to check the latest news or stock quotes, and not logging out, this is a case where the monitoring or rules might need to be adjusted to account for the high usage. Alternatively, Joe may simply need a refresher course on the company's Internet usage policies. On the other hand, if the usage concern was based on a person's observation of Joe's actions, there is another, slightly different set of questions to ask, such as:

1. Who made the observation? Are logs available to support the observation? (e.g., login, logout, timecards, firewall access, etc.)

2. Are there other witnesses to support the observation?

3. What exactly was the individual under investigation observed doing?

4. What is the pattern of usage?

5. Are there security cameras, login sheets, time cards, or key card access logs that can verify the individual under investigation had access and was logged on to the Internet?

Again, once you obtain answers to these questions you will begin to formalize a plan of investigation. This plan will differ slightly from the plan based on electronic monitoring. With observation being the basis for a complaint, the ability to verify the usage is more difficult to substantiate — but not impossible.

The above"normal utilization should prompt the investigator and management to inquire about the impact (financial, physical, operational, etc.) of the so"called excessive usage. Several questions to help evaluate the impact include:

1. What damage (if any) did the excessive usage cause?

2. How can the damage be substantiated?

3. How can the damage be quantified?

4. Did the individual under investigation not meet his or her job responsibilities as a result of excessive Internet usage?

5. Did the individual under investigation interfere with another person's job performance as a result of the excessive utilization?

6. Was someone offended by the usage (e.g., inappropriate materials, games being played)?

7. Can you identify this person?

8. Is the person willing to state for the record that he or she she was offended by the usage?

9. Did fraud occur in the form of falsified timesheets — hours of work reported, or any other form, as a result?

The answers to these questions answers will not only help form the plan for this type of investigation, but will also help the investigator and management determine if the investigation should be (can be) pursued.

Inappropriate E"mail

Before performing any investigation on e"mail, you need to ensure that corporate policy allows it. New electronic privacy laws protect the privacy of electronic communications. If corporate policy specifically states that all

computers and data stored on them belong to the corporation, then you are probably on safe ground. Be sure that there is such a policy and that the employee under investigation has read the policy before proceeding. Although this is one of the easiest investigations, this type of investigation should be done strictly by the book. If the corporate policy does not contain the rights to the employee's e"mail, then you and your corporation could be subject to a lawsuit for invading the privacy of an employee.

If the reason for an investigation is that there was inappropriate use of e"mail, either through the act of sending offensive material or for personal and non"work"related use, there is yet another set of questions that should be asked. These questions will help determine if there was inappropriate utilization of the company's e"mail systems and if further investigative action is required.

1. What was sent?

2. Can you obtain a copy from the complainant or recipient?

3. Is a copy available from the automated e"mail archive system?

4. Was someone offended? (This could be an harassment issue and require HR involvement.)

5. Who if anyone else received the material?

6. Was the individual under investigation the originator of the e"mail, or was it someone else?

7. How were you able to (or can you) validate this?

8. Could someone else have sent the e"mail, using the ID of the individual under investigation?

9. Are screen"saver passwords used?

10. Could someone else use the PC of the individual under investigation?

11.Was the time that the e"mail was sent during the time the individual under investigation had access to e"mail?

12. Is auto"forwarding of e"mail used? Available? Activated?

13. Was a group list used?

14. Are there patterns or history to the e"mail usage?

15. Have there been previous warnings to the individual under investigation about the e"mailusage?

16. If so, are these warnings documented?

17. What was the intent of the e"mail?

Some of the questions listed in the section on abnormal Internet utilization can also be applied to this type of investigation. The real issue with this type of investigation is to determine whether it is an issue of harassment or

a case of violating company e"mail policies/procedures. Potential exposures to the company, which can result from the lack of a proactive response by management to a harassment omplaint, include a lawsuit filed against the company by the complainant, as well as multiple instances of harassment that can lead to multiple lawsuits. Furthermore, to make matters worse, the longer the company waits to investigate, the more likely it is that lawyers will have a field day and turn this into the company not caring, and thus higher rewards to the complainant. To alleviate the appearance of a non"proactive response to harassment complaints, the company should have anti"harassment policies and training programs. This training should be repeated annually for all employees. There should be documentation that is maintained in HR files stating that each employee has attended and signed a statement that he or she has read the company's policies against harassment. This is also documentation that should be gathered during the investigation.

3.2 COMPUTER FORENSIC TOOLKITS- An Overview

Computer forensics is a very important branch of computer science in relation to computer and Internet related crimes. Earlier, computers were only used to produce data but now it has expanded to all devices related to digital data. The goal of Computer forensics is to perform crime investigations by using evidence from digital data to find who was the responsible for that particular crime.

For better research and investigation, developers have created many computer forensics tools. Police departments and investigation agencies select the tools based on various factors including budget and available experts on the team.

These computer forensics tools can also be classified into various categories:

- Disk and data capture tools
- File viewers
- File analysis tools
- Registry analysis tools
- Internet analysis tools
- Email analysis tools
- Mobile devices analysis tools
- Mac OS analysis tools
- Network forensics tools
- Database forensics tools

1. Digital Forensics Framework

Digital Forensics Framework is another popular platform dedicated to digital forensics. The tool is open source and comes under GPL License. It can be used either by professionals or non-experts without any trouble. It can be used for digital chain of custody, to access the remote or local devices, forensics of Windows or Linux OS, recovery hidden of deleted files, quick search for files' meta data, and various other things.

2. Open Computer Forensics Architecture

Open Computer Forensics Architecture (OCFA) is another popular distributed open-source computer forensics framework. This framework was built on Linux platform and uses postgreSQL database for storing data.

3. CAINE

CAINE (Computer Aided Investigative Environment) is the Linux distro created for digital forensics. It offers an environment to integrate existing software tools as software modules in a user friendly manner. This tool is open source.

4. X-Ways Forensics

X-Ways Forensics is an advanced platform for digital forensics examiners. It runs on all available version of Windows. It claims to not be very resource hungry and to work efficiently. If we talk about the features, find the key features in the list below:

- Disk imaging and cloning
- Ability to read file system structures inside various image files
- It supports most of the file systems including FAT12, FAT16, FAT32, exFAT, TFAT, NTFS, Ext2, Ext3, Ext4, Next3®, CDFS/ISO9660/Joliet, UDF
- Automatic detection of deleted or lost hard disk partition
- Various data recovery techniques and powerful file carving
- Bulk hash calculation
- Viewing and editing binary data structures using templates
- Easy detection of and access NTFS ADS
- Well maintained file header
- Automated activity logging
- Data authenticity

- Complete case management
- Memory and RAM analysis
- Gallery view for pictures
- Internal viewer for Windows registry file
- Automated registry report
- Extracts metadata from various file types
- Ability to extract emails from various available email clients.
- And many more..

5. SANS Investigative Forensics Toolkit – SIFT

SANS Investigative Forensics Toolkit or SIFT is a multi-purpose forensic operating system which comes with all the necessary tools used in the digital forensic process. It is built on Ubuntu with many tools related to digital forensics.

6. EnCase

EnCase is another popular multi-purpose forensic platform with many nice tools for several areas of the digital forensic process. This tool can rapidly gather data from various devices and unearth potential evidence. It also produces a report based on the evidence.

7. Registry Recon

Registry Recon is a popular registry analysis tool. It extracts the registry information from the evidence and then rebuilds the registry representation. It can rebuild registries from both current and previous Windows installations.

8. The Sleuth Kit

The Sleuth Kit is a Unix and Windows based tool which helps in forensic analysis of computers. It comes with various tools which helps in digital forensics. These tools help in analyzing disk images, performing in-depth analysis of file systems, and various other things.

9. Llibforensics

Libforensics is a library for developing digital forensics applications. It was developed in Python and comes with various demo tools to extract information from various types of evidence.

10. Volatility

Volatility is the memory forensics framework. It used for incident response and malware analysis. With this tool, you can extract information from running processes, network sockets, network connection, DLLs and registry hives. It also has support for extracting information from Windows crash dump files and hibernation files. This tool is available for free under GPL license.

11. WindowsSCOPE

WindowsSCOPE is another memory forensics and reverse engineering tool used for analyzing volatile memory. It is basically used for reverse engineering of malwares. It provides the capability of analyzing the Windows kernel, drivers, DLLs, virtual and physical memory.

12. The Coroner's Toolkit

The Coroner's Toolkit or TCT is also a good digital forensic analysis tool. It runs under several Unix-related operating systems. It can be used to aid analysis of computer disasters and data recovery.

13. Oxygen Forensic Suite

Oxygen Forensic Suite is a nice software to gather evidence from a mobile phone to support your case. This tool helps in gathering device information (including manufacturer, OS, IMEI number, serial number), contacts, messages (emails, SMS, MMS), recover deleted messages, call logs and calendar information. It also lets you access and analyze mobile device data and documents. It generates easy to understand reports for better understanding.

14. Bulk Extractor

Bulk Extractor is also an important and popular digital forensics tool. It scans the disk images, file or directory of files to extract useful information. In this process, it ignores the file system structure, so it is faster than other available similar kinds of tools. It is basically used by intelligence and law enforcement agencies in solving cyber crimes.

15. Xplico

Xplico is an open source network forensic analysis tool. It is basically used to extract useful data from applications which use Internet and network protocols. It supports most of the popular protocols including HTTP, IMAP, POP, SMTP, SIP, TCP, UDP, TCP and others. Output data of the tool is stored in SQLite database of MySQL database. It also supports IPv4 and IPv6 both.

16. Mandiant RedLine

Mandiant RedLine is a popular tool for memory and file analysis. It collects information about running processes on a host, drivers from memory and gathers other data like meta data, registry data, tasks, services, network information and Internet history to build a proper report.

17. Computer Online Forensic Evidence Extractor (COFEE)

Computer Online Forensic Evidence Extractor or COFEE is a tool kit developed for computer forensic experts. This tool was developed by Microsoft to gather evidence from Windows systems. It can be installed on a USB pen drive or external hard disk. Just plug in the USB device in the target computer and it starts a live analysis. It comes with 150 different tools with a GUI based interface to command the tools. It is fast and can perform the whole analysis in as few as 20 minutes. To law enforcement agencies, Microsoft provides free technical support for the tool.

18. P2 eXplorer

P2 eXplorer is a forensic image mounting tool which aims to help investigating officers with examination of a case. With this image, you can mount forensic images as a read-only local and physical disc and then explore the contents of the image with file explorer. You can easily view deleted data and unallocated space of the image.

It can mount several images at a time. It supports most of the image formats including EnCasem, safeBack, PFR, FTK DD, WinImage, Raw images from Linux DD, and VMWare images. It supports both logical and physical image types.

19. PlainSight

PlainSight is another useful digital forensics tool. It is a CD based Knoppix which is a Linux distribution. Some of its uses include viewing Internet histories, data carving, checking USB device usage, memory dumps extracting password hashes, information gathering, examining Windows firewall configuration, seeing recent documents, and other useful tasks. For using this too, you only need to boot from the CD and the follow the instructions.

20. XRY

XRY is the mobile forensics tool developed by Micro Systemation. It is used to analyze and recover crucial information from mobile devices. This tool comes with a hardware device and software. Hardware connects mobile phones to PC and software performs the analysis of the device and extract data. It is designed to recover data for forensic analysis.

21. HELIX3

HELIX3 is a live CD-based digital forensic suite created to be used in incident response. It comes with many open source digital forensics tools including hex editors, data carving and password cracking tools.

This tool can collect data from physical memory, network connections, user accounts, executing processes and services, scheduled jobs, Windows Fegistry, chat logs, screen captures, SAM files, applications, drivers, environment variables and Internet history. Then it analyzes and reviews the data to generate the complied results based on reports.

22. Cellebrite UFED

Cellebrite's UFED solutions present a unified workflow to allow examiners, investigators and first responders to collect, protect and act decisively on mobile data with the speed and accuracy a situation demands – without ever compromising one for the other. The UFED Pro Series is designed for forensic examiners and investigators who require the most comprehensive, up-to-date mobile data extraction and decoding support available to handle the influx of new data sources. Platform agnostic, the UFED Field Series is designed to unify workflows between the field and lab, making it possible to view, access and share mobile data via in-car workstations, laptops, tablets or a secure, self-service kiosk located at a station.

3.3 Introduction and overview- Digital forensic

Digital forensic evidence consists of exhibits, each consisting of a sequence of bits, presented by witnesses in a legal matter, to help jurors establish the facts of the case and support or refute legal theories of the case. The exhibits should be introduced and presented and/or challenged by properly qualified people using a properly applied methodology that addresses the legal theories at issue. The tie between technical issues associated with the digital forensic evidence and the legal theories is the job of expert witnesses.

Exhibits are introduced as evidence by one side or another. In this introductory process, testimony is presented to establish the process used to identify, collect, preserve, transport, store, analyze, interpret, attribute, and/or reconstruct the information contained in the exhibits and to establish, to the standard of proof required by the matter at hand, that the evidence reflects a sequence of events that is asserted to have produced it. Evidence, to be admitted, must be shown by the party attempting to admit it, to be relevant, authentic, not the result of hearsay, original writing or the legal equivalent thereof, and more probative than prejudicial. Assuming that adequate facts can be established for the introduction of an exhibit, people involved in the chain of custody and processes used to create, handle, and introduce the evidence testify about how it came to be, how it came to court, and about the event sequences that may have produced it.

Digital forensic evidence is usually latent, in that it can only be seen by the trier of fact at the desired level of detail through the use of tools. In order for tools to be properly applied to a legal standard, it is normally required that the people who use these tools properly apply their scientific knowledge, skill, experience, training, and/or education to use a methodology that is reliable to within defined standards, to show the history, pedigree, and reliability of the tools, proper testing and calibration of those tools, and their application to functions they are reliable at performing within the limitations of their reliable application. Non- experts can introduce and make statement about evidence to the extent that they can clarify non-scientific issues by stating what they observed.

Digital forensic evidence is challenged by identifying that, by intent or accident, content, context, meaning, process, relationships, ordering, timing, location, corroboration, and/or consistency are made or missed by the other side, and that this produced false positives or false negatives in the results presented by the other side.

The trier of fact then must make determinations about how the evidence is applied to the matter at hand so as to weigh it against and in conjunction with all of the other evidence and to render judgments about the legal matters that the evidence applies to.

This context includes, without limit:

- The legal matter determines the jurisdictions involved and thus the applicable laws and legal processes, the legal theories, methodologies, and applications of those methodologies that will be accepted, the requirements for admissibility of evidence, the requirements for acceptance of expert witnesses, the standards of proof, and many other similar things that impact the digital forensic evidence and its use.
- The nature of the case, whether it is civil or criminal, and sub-distinctions within these broad categories, affects the standards of proof and admissibly, the rules of evidence, the rules for trials, and many other aspects of what can and cannot be used in the legal matter and supported or refuted through digital forensic evidence.
- Limitations on elements of the case such as searches and seizures, which may be real-time or after the fact, compulsory or permission, and limited in various ways so as to prevent them from becoming "fishing expeditions" are informed by and help to form the context within which the digital forensic examiner must operate.
- Procedural requirements of legal cases may constrain certain arguments and evidence so that it can only be used at particular times or in particular types of hearings.
- The calendar is often daunting in legal matters, and in many cases there is very little time to do the things that have to be done with regard to digital forensic evidence. The calendar of the case may also impact the sequence in which evidence is dealt with, and this may result in additional complexities relating to the ordering of activities undertaken.
- Cost is an important factor because only finite available financial resource is available. While there may be an enormous range of analysis that could be undertaken, much of it may not be undertaken because of cost constraints.
- Strategies and tactics of the case may limit the approaches that may be taken to the digital forensic evidence. For example, even though some sorts of analysis may be feasible, they may be potentially harmful to the side of the case the forensic examiner is involved in, and therefore not undertaken by that side.
- Availability of witnesses and evidence is often limited. In some cases evidence may only be examined in a specific location and under specific supervision, while in most cases, witnesses are only available to the attorneys during limited time frames and under limitedcircumstances.For the opposition to the party bringing the witness, these may be very limited and restricted to testimony under oath in depositions and elsewhere.

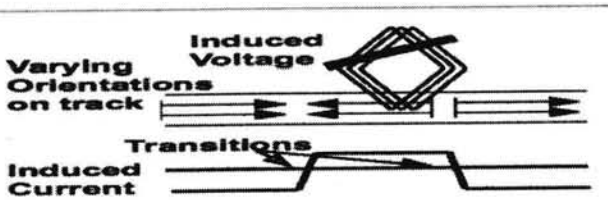
- Stipulations often limit the utility and applicability of digital forensic evidence. For example, if there is a stipulation as to a factual matter, even if the digital forensic evidence would seem to refute that stipulation, it can be given no weight because the stipulation is, legally speaking, a fact that is agreed to by all parties and therefore cannot be refuted.

- Prior statements of witnesses often create situations in which digital forensic evidence is applied to confirm or refute those statements. In these cases, the goal is to find evidence that would tend to refute the statements and thereby make the witness and their prior testimony incredible.

- Notes and other related materials are potentially subject to subpoena in legal matters, and therefore, conjectures on notes, FAXes, and drafts of expert reports as well as other similar material might be discoverable and used to refute the work of the experts. This tends to limit the manner in which the expert can work without endangering the case for their client.

There are many other similar legal contextual issues that drive the digital forensics process and the work of those who undertake those processes. And without this context, it is very difficult if not impossible to do the job properly. While it is the task of the lawyers to limit the efforts of the digital forensics evidence workers in these regards, it is the task of the workers to know what they are doing and how to do it properly within the legal context.

Figure 1 – The way floppy disks encode digital signals (from [2])



Digital forensic evidence consists of digital "bits", each of which is a '1' or a '0'; however, that evidence is realized in the physical world by physical mechanisms that, generally speaking, are not themselves digital. In some cases, the mechanisms by which the evidence was produced become part of the issue that must be addressed.

Those who engage in work related to digital forensic evidence must understand these issues at a rudimentary level in order to be useful to the legal process, and they must understand these issues and be willing to work within the context of the legal system and the specifics of the matter at hand in order to work in this area.

3.3 The processes involved with digital forensic evidence

While there are many other characterizations of the processes involved in dealing with digital forensic evidence (DFE), the perspective taken here will assume, without limit, the DFE must be identified, collected, preserved, transported, stored, analyzed, interpreted, attributed, perhaps reconstructed,presented, and, depending on court orders, destroyed. [1] All of these must be done in a manner that meets the legal standards of the jurisdiction and the case.

Identification

In order to be processed and applied, evidence must first, somehow, be identified as evidence. It is common for there to be an enormous amount of potential evidence available for a legal matter, and for the vast majority of the potential evidence to never be identified. To get a sense of this, consider that every sequence of events within a single computer might cause interactions with files and the file systems in which they reside, other processes and the programs they are executing and the files they produce and manage, and log files and audit trails of various sorts. In a networked environment, this

extends to all networked devices, potentially all over the world. Evidence of an activity that caused digital forensic evidence to come into being might be contained in a time stamp associated with a different program in a different computer on the other side of the world that was offset from its usual pattern of behavior by a few microseconds. If the evidence cannot be identified as relevant evidence, it may never be collected or processed at all, and it may not even continue to exist in digital form by the time it is discovered to have relevance.

Collection

In order to be considered for use in court, identified evidence must be collected in such a manner as to preserve its integrity throughout the process, including the preservation of information related to the chain of custody under which it was collected and preserved. Recent case law has established that there is a duty to preserve digital forensic evidence once the holder of that evidence is or reasonably should be aware that it has potential value in a legal matter. This duty is typically fulfilled by collecting and preserving a copy of the original evidence so that the actual original media need not be preserved, but rather, can continue to be used. Collection may involve many different technologies and techniques depending on the circumstance.

What is collected is driven by what is identified; however, a common practice in the digital forensics community has been to take forensically sound images of all bits contained within each media containing identified content. This provides the means to then identify further evidence contained within that media for subsequent analysis, assuming that the copy of the media was properly preserved along the way. The problem with this process today is that the volume of storage required has become very large in many cases, and this process tends to be highly disruptive of operating businesses that use these computers in a non-stop fashion. Consider the business impact on an Internet Service Provider if they have to cease operations of a computer that would otherwise be in use in order to preserve evidence.

Preservation of relevant log files and audit data is particularly important and should always be identified and preserved. This includes all logs associated with the servers used to send, receive, process, and store the evidence. Failure to do this becomes particularly problematic in cases when the purity of the evidence is at issue. For example, if an exhibit contains some corrupt content, the entire

exhibit becomes suspect. If original records are not available to rehabilitate relevant portions of the exhibit, all of the evidence contained in the exhibit may be inadmissible. If there is suspicion of spoliation, the additional log files and related records will be necessary in order to show that redundant information exists that is consistent with the actual creation of the content at issue. Even information such as system crashes and reboots may be critical to a case because corrupt file content may be produced by those sorts of events and without the logs to show what happened when, that corruption may not be able to be reconciled with the need for preservation of the purity of the evidence.

Transportation

Evidence must sometimes be transported from place to place. For example, when collected from a crime scene, the evidence must somehow be moved to a secure location or it may not be properly preserved through to a trial. Digital forensic evidence can generally be transported by making exact duplicates, at the level of bits, of the original content. This includes, without limit, the movement of the content over networks, assuming adequate precautions are taken to assure its purity during that transportation. Evidence is often copied and sent electronically, on compact disks, or in other media, from place to place. Original copies are normally kept in a secure location in order to act as the original evidence that is introduced into the legal proceedings. If there is any question about the bits contained in the evidence, it can be settled by returning to the original. Facsimile evidence, printouts, and other similar depictions of digital forensic evidence may also be transported, but they are not a good substitute for the original digital forensic evidence in most cases, among other reasons, because they make it far harder, if not impossible, to properly analyze what the original bits were. For example, many different bit sequences may produce the output depictions, and identical bit sequences may produce different output depictions. Care must be taken in transportation to prevent spoliation as well. For example, in a hot car, digital media tends to lose bits.

Increasingly evidence is transported electronically from place to place, and even the simplest errors can cause the data arriving to be incorrect or improperly authenticated for legal purposes. Care must be taken to preserve

chain of custody and assure that a witness can testify accurately about what took place, using and retaining contemporary notes, and taking proper precautions to assure that evidence is not spoliated and is properly treated along the way.

Storage

In storage, digital media must be properly maintained for the period of time required for the purposes of trial. Depending on the particular media, this may involve any number of requirements ranging from temperature and humidity controls to the need to supply additional power, or to reread media. Storage must be adequately secure to assure proper chain of custody, and typically, for evidence areas containing large volumes of evidence, paperwork associated with all actions related to the evidence must be kept to assure that evidence doesn't go anywhere without being properly traced. Many different sorts of things can go wrong in storage, including, without limit, decay over time, environmental changes resulting in the presence or absence of a necessary condition for preservation, direct environmental assault on the media, fires, floods, and other external events reaching the evidence, loss of power to batteries and other media-preserving mechanisms, and decay over time from other natural and artificial sources.

Analysis, interpretation, and attribution

Analysis, interpretation, and attribution of evidence are the most difficult aspects encountered by most forensic analysts. In the digital forensics arena, there are usually only a finite number of possible event sequences that could have produced evidence; however, the actual number of possible sequences may be almost unfathomably large. In essence, almost any execution of an instruction by the computing environment containing or generating the evidence may have an impact on the evidence.

Since it is infeasible to reconstruct every possible sequence to find all of the sequences that may have produced the actual evidence in a any particular case, analysts focus in on large sets of sequences of events and tend to characterize things in those terms. For example, if the evidence includes a log file that appears to be associated with a file transfer, the name of the file transfer program included in the log file will typically be associated with common behavior of that program and used as a basis for the analysis. The user identity indicated in the log file may be associated with a human or group, and this creates an initial attribution that can then be used as a basis for further efforts to attribute to the standard of proof required.

Of course the presence of this record in an audit trail doesn't mean that the program was ever run at all or that the thing the record indicates ever took place or that the user identified caused the events of interest. There are many possible sequences of events that could result in the presence of such a record. For example, and without limiting the totality of possible event sequences, the record could have been placed there maliciously, it could be a record produced by another program that looks similar to the program being considered, it could have been a record produced by the program even though the file transfer failed, the record could have been produced by a Trojan horse acting for the user, or the record could be there because of a failure in a disk write that produced a cross-link between disk blocks associated with different sorts of records.

The analyst seeking to interpret the evidence should seek to take into account the alternative explanations for evidence in trying to understand what actually took place and how certain they are of the assertions they make. It is fairly common for supposed experts to make leaps and draw conclusions that are not justified. For example, an analyst might write a report stating something like "X did Y producing Z" where X is an individual or program and Y is an action that produced some element of the evidence Z. But this is excessive in almost all cases. A more appropriate conclusion might be "Based on the evidence available to me at this time, it appears that X did Y producing Z". And of course it helps if some or many of the alternative explanations have been explored and shown to be inconsistent with the evidence. That's one of the reasons that seemingly irrelevant evidence might be very useful in a legal matter. For example, evidence from system logs might indicate that there were no detected disk errors, system crashes or reboots, or other anomalies reflected in the log files for the period in question, and that therefore, the explanations associated with these sorts of anomalies are inconsistent with the evidence. But without those log files or some other evidence, this conclusion cannot be reasonably drawn.

In networked environments, there are potentially far more sequences of bits that may be relevant to the issues in the matter at hand. As a result, there is potentially far more evidence available, and the analysis and interpretation of that larger body of evidence leads to many more potential analytical and interpretive processes and products. It could be argued that this increases the complexity of analysis exponentially, but in reality, the additional evidence tends to further restrict the number of histories that are feasible in order to retain consistency of interoperation across the evidence. As an example, the file transfer record identified above might be greatly bolstered or flatly refuted by corresponding records on remote systems from which the file was asserted to be downloaded and through which the transfer may have come.

Analysis, interpretation, and attribution of digital forensic evidence are also reconcilable with non-digital evidence and externally stipulated or demonstrated facts. As an example, if the digital forensic evidence appears to show that person X was present at the local console of a computer in Los Angeles, California two hours after they passed through customs and immigration in London, England, even though the network logs from distant systems show that the transfer took place, it is not a reasonable interpretation to assert that the individual was in Los Angeles. Clearly there is another explanation, whether it is two individuals, a remote control mechanism, alteration of multiple logs in multiple systems, alteration of customs and immigration logs, altered time clocks, or any of a long list of other possibilities. While in some venues, the "don't confuse me with the facts" approach may apply, in a legal setting, digital forensic evidence should reconcile with external reality.

Anchor facts that the analyst can testify to are a good example of the interaction between digital forensic evidence and physical reality. An example of an anchor fact is knowledge of time keeping mechanisms on systems that interact with evidence available in the matter at hand. For example, if the analyst operates a system that retains sound records and was synchronized to network time protocol during the period of time at issue, and that system has a record of an email passing through a relevant system that includes time and date stamps, then the time skew between the analysts system and the relevant system provides an anchor in facts that the analyst can use to make more definitive statements about what took place and when. Interpretation of the evidence can then more definitively

assert that, based on the personal knowledge of the witness and the records they have of facts relevant to the matter, a particular record is consistent with a time skew of 18 hours. This may even allow the analyst to explain how the individual could have appeared to have been in London at the same time they appeared to have been in Los Angeles.

3.4 DIGITAL EVIDENCE

Digital evidence is any information or data of value to an investigation that is stored on, received by, or transmitted by an electronic device. Text messages, emails, pictures and videos, and internet searches are some of the most common types of digital evidence.

Digital Trail

Most criminals now leave a digital trail; a suspect's e-mail or mobile phone files might contain critical information:

- Intent,
- Location and time of crime,
- Relationship with victim(s), and
- Relationship with other suspect(s)

On Scene

As the first responding officer, the collection and preservation of digital evidence begins with you.

Once the scene has been secured and legal authority to seize the evidence has been confirmed, devices can be collected. First responders must be cautious when handling digital devices in addition to normal evidence collection procedures the preventing the exposure to extreme temperatures, static electricity and moisture are a must.

3.4 Frequently seized devices – Smartphones and other mobile devices

Step 1 – Document the device and all collection procedures and information

- Photograph OR Video OR Sketch
- Notes
- Chain of custody

Step 2 – Determine if the device is on or off

- Look for lights
- Listen for sounds
- Feel for vibrations or heat

NOTE – Many mobile devices save power by turning off screens after a specified amount of time. Despite the screen status, the device is likely still active. Ask if the device is currently powered on. Where legal, pressing the power button quickly will activate the screen.

Step 3 – If the device is off, **do not turn it on**

- Collect and package (see Step 5)
- Ask for password/pass pattern
- Transport (see Step 6)

Step 4 – If the device is on, proceed with **CAUTION**

WARNING – The two most significant challenges for officers seizing mobile devices are: (1) isolating the device from cellular and Wi-Fi networks; and (2) obtaining security passwords or pass patterns for the device so the evidence can be examined forensically. Always ask if there is any security feature enabled on the phone. These can include passwords (simple or omplex), security/wiping apps, pass patterns, or biometrics (facial scan). Document (see the attached consent form for guidance) and confirm the password or pass pattern. Turning the device off could result in the loss of evidence. The best option is to keep the device powered, unlocked (if locked, collect any available passwords, PIN codes, or security unlock information), and in airplane mode until it is in the hands of an experience technician.

Step 5 – Collection and Package

WARNING – You may need to collect other forensic evidence including fingerprints, biological samples, DNA, etc. from smartphones and mobile devices. Work with crime scene technicians or trained forensic personnel to preserve such evidence without disturbing the integrity of the data on the device. Be sure to advise forensic examiners in advance of submission of the possible existence of hazardous material on the device.

- Secure data and power cables
- Consider collecting computers that may contain device backups
- Package the device so it will not be physically damaged or deformed
- Package the device in evidence bags or boxes

Step 6 – Transport

- Deliver evidence to a secure law enforcement facility or digital evidence laboratory as soon as possible
- Protect from temperature extremes and moisture

3.5 Frequently seized devices – Laptop and Desktop Computer Systems

Step 1 – Document the device and all collection procedures and information

- Photograph OR Video OR Sketch
- Notes
- Chain of custody

Step 2 – Determine if the device is on or off

- Look for lights
- Listen for sounds
- Feel for vibrations or heat

Step 3 – If the system is off, **do not turn it on**

- Disassemble (see Step 5)
- Transport (see Step 6)

Step 4 – If the system is on, proceed with **CAUTION**

- Do not type, click the mouse, or explore files or directories without advanced training or expert consultation
- Ask about passwords and/or encyption of the system
- Observe the screen, and look for any running programs that indicate access to internet-based accounts, open files, encryption, or the presence of files or data of potential evidentiary value
- If you see anything on the screen that concerns you or needs to be preserved, consult with an expert (if you don't know who to contact, call the number on the inside cover of this manual)
- Photograph the screen
- Once you are prepared to power down the system, pull the plug from the back of the computer system
- Remove the battery from a laptop system

Step 5 – Disassemble and package the system

WARNING – You may need to collect other forensic evidence including fingerprints, biological samples, DNA, etc. from computer systems, digital devices, and electronic media. Work with crime scene service technicians or trained forensic personnel to preserve such evidence without disturbing the integrity of the digital media.

- Photograph the system from all perspectives
- Clearly mark evidence and document chain of custody, location, and other important details about the seized item(s)
- Disconnect and secure cables

• Check media ports and cd/dvd trays for the presence of removable media
• Package the system, and peripheral devices, for transport using laptop bags (if applicable), boxes, or evidence bags

Step 6 – Transport
• Protect from temperature extremes and moisture
• Do not place evidence in the cruiser's trunk
• Protect from electro-static discharge
• Package evidence so it will not be physically damaged or deformed
• Deliver evidence to a secure law enforcement facility or digital evidence laboratory as soon as practicable

3.6 Other commonly seized devices that may store digital evidence

There are many other storage media and technical devices that may process and store digital evidence. Examples of these devices include media cards (ie. secure digital, SIM, flash, memory sticks), thumb drives, optical media (ie. CD, DVD, and Blu-ray), digital cameras, MP3 players, iPods, servers, surveillance systems, gaming stations (ie. Xbox, PlayStation, Wii), and GPS devices. Each of these devices is capable of holding significant digital evidence that will help your case. And each is handled in a separate way. Seizure of these items should be performed with special care. Consider working with an experienced digital evidence analyst to collect these items.

Step 1 – Document the device and all collection procedures and information
• Photograph OR Video OR Sketch
• Notes
• Chain of custody

Step 2 – Determine if the device is on or off
• Look for lights
• Listen for sounds
• Feel for vibrations or heat

Step 3 – Ask if there are any security features enabled on the device including passwords or encrypted file protection.

Step 4 – If the device is off, **do not turn it on**
• Collect and package (see Step 6)
• Transport (see Step 7)

Step 5 – While assessing, collecting, packaging, and transporting, follow these device-specific rules
• Only trained personnel should collect data from a server. If you don't know what you are doing, stop and call an expert. Be careful when asking for the assistance of information technology or other personnel on-site

• GPS devices, MP3 players, and digital cameras should be turned off to secure data. Be sure to ask for any passwords or security features
• If available, paper evidence bags, or static-free evidence bags, are best for the storage of media
• Media contained in binders or carriers should remain in the container
• Be careful not to scratch optical media during seizure.
• Gaming stations should be seized in the same manner as computers

WARNING – Collecting evidence from surveillance systems can be difficult. Time is of the essence as digital surveillance systems often have proprietary software and hardware needs for playback. Speak to your prosecutor or agency legal counsel when making a decision about the seizure of a digital surveillance system as opposed to footage or segments of video extracted from the system. Also, be sure to get the company and installer name and contact information for the person that installed or maintains the system.

Step 6 – Collection and Package
• Follow chain-of-custody procedures
• Secure data and power cables
• Label the evidence container(s), not the device(s)
• Package the device so it will not be physically damaged or deformed
• Package the device in evidence bags or boxes

Step 7 – Transport
• Deliver evidence to a secure law enforcement facility or digital evidence laboratory as soon as practicable
• Protect from temperature extremes and moisture

3.7 Tracing IP addresses

Internet Protocol (IP) addresses provide the basis for online communication, allowing devices to interface and communicate with one another as they are con- nected to the Internet. As was noted in Chapter 3, IP addresses provide investiga- tors a trail to discover and follow, which hopefully leads to the person(s) responsible for some online malfeasance. In Chapter 5 and 6, we discussed differ- ent tools that investigators can use to examine various parts of the Internet, including identifying the owners of domains and IP addresses. In this chapter, we are going to discuss tracing an IP address and the investigative advantages of this process. We have covered the tools to help us trace IP addresses in previous chap- ters, but here we want to walk through the process of identifying the IP to trace and who is behind that address.

Online tools for tracing an IP address

Tracing IP addresses and domains is a fundamental skill for any Internet investi- gator. There are many resources available on the Internet to assist in this process. Of primary importance are the entities responsible for the addressing system, namely, the Internet Assigned Number Authority (IANA) and its subordinate bod- ies the Regional Internet Registries (RIR). In addition to IANA and RIR, there are a multitude of other independent

online resources that can assist the investiga- tor in conducting basic IP identification. assign the top level domains, that is, .com, org, mil, edu. and coordinate the IP addresses and their allocation to the RIR. IANA established the RIR to allocate IP address in geographical regions.

The RIR system evolved over time, eventually dividing the world into the following five regions:

1. African Network Information Centre (AfriNIC) for Africa, http://www.afrinic. net/
2. American Registry for Internet Numbers (ARIN) for the United States, Canada, several parts of the Caribbean region, and Antarctica, https://www. arin.net/
3. Asia-Pacific Network Information Centre (APNIC) for Asia, Australia, New Zealand, and neighboring countries, http://www.apnic.net/
4. Latin America and Caribbean Network Information Centre (LACNIC) for Latin America and parts of the Caribbean region, http://www.lacnic.net/en/ web/lacnic/inicio
5. Re´seaux IP Europe´ens Network Coordination Centre (RIPE NCC) for Europe, Russia, http://http://www.ripe.net/

Each site has a search "Whois" function that allows the investigator to identify IP registration information. IANA and the RIR are the official registrars and own- ers of the domain records and IP addresses. An investigator wishing to verify the owner of an IP can use the RIR to locate the records.

Internet commercial and freeware tools:

There are also many Internet sites to look up IP and Domain registrations. Some provide the basic registration information and other sites combine additional tools that enable the investigator to identify an IP's physical location. The following websites, mentioned in Chapter 6, are easily accessible from the Vere Software Internet Investigators Toolbar, and are important utilities for the investigator:

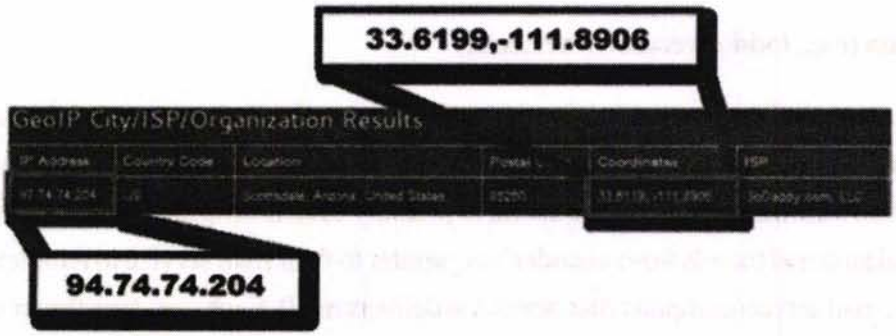
DNS Stuff (http://www.dnsstuff.com/tools/tools): This website has been around for a number of years. It offers both free and pay options for assisting in IP addresses identification and other online information.

Network-Tools.com (http://network-tools.com): Another website with a simple user interface to assist in IP tracing.

CentralOps.net (http://centralops.net/co/): This is another website that assists with your IP tracing. One of its features, Domain Dossier, does multiple lookups on an IP address or domain.

In some circumstances, the investigator may look up a domain or and IP address with these commercial tools and find the address concealed by the com- mercial registrar. In these cases, the investigator may need to go to the commer- cial registrar's site and use the Whois search located there to determine the domain registration records.

Each of the mentioned websites presents the domain registration information in a slightly different manner and may have additional tools useful to the investigator. Experience with each will provide the investigator with a better understanding of each site's features.



Geolocation of an IP address

Geolocation in general refers to the identification of the real geographical area of an electronic device, such as a cell phone, IP addresses, WiFi, and MAC addresses. Now that being said that does not mean an IP address can be traced directly to a house. Geolocation particularly for IP addresses is not an exact science. Unlike cell phones that can be traced via their GPS coordinates or cell tower triangulation, IP addresses use a common database of address locations maintained by different com- panies. One of the most commonly used databases is maintained by Maxmind, Inc. which can be found at www.maxmind.com. Maxmind provides a free service to geolocate an IP address to a state or city. Purchasing their services can give the Internet investigator access to a more precise location, up to and including physical addresses. There are other online services that provide geolocation identification of IP addresses such as IP2Location.com. Some investigative tools, such as Vere Software's WebCase, include access to the Maxmind database as a feature of its domain lookup. On Maxmind's website you can use their demo function to identify an IP addresses location. An example of a Maxmind search for the geolocation of IP address 97.74.74.204 is shown in the above figure. Along with identifying the geolocation of the address as Scottsdale, Arizona, website provides the latitude and longitude based on this location and the Internet Service Provider (ISP) hosting the IP address, in this case GoDaddy.com LLC.

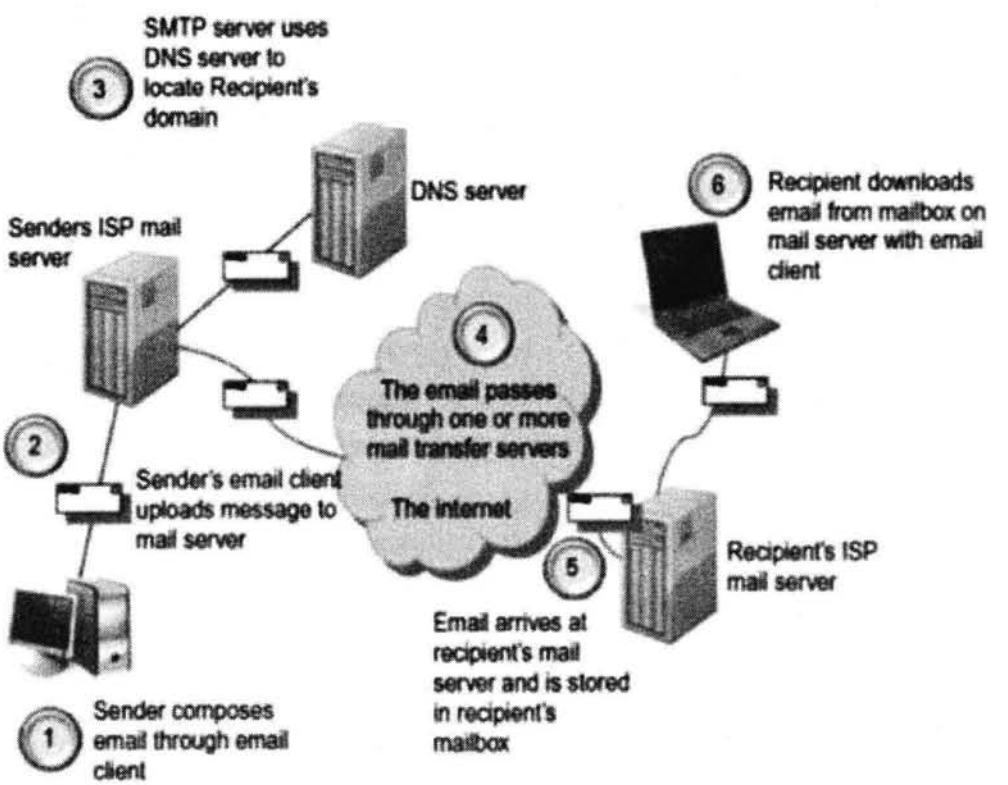
3.8 Tracing emails

Email is as ubiquitous as any of the IPs we have discussed. Other than the World Wide Web, this is one of the most used tools for communication. It is commonly employed for everything from personal communications to business use. Unfortunately, it is also a favorite tool for threats and harassment by criminals and stalkers. This section will explain the basic parts of an email and how to effectively identify the sender or identify the pieces of the email that can further the investigation through additional follow-up.

The email itself has several features that are unique and make identification possible. These features provide initial clues which may not identify a specific person or sender without additional investigative steps. To start email addresses, have the standard familiar format of the username, the @ symbol, the domain name used by the user and the top level domain associated with the domain name. For example:

***username*@domain (e.g., todd@veresoftware.com)**

The email we see in our email program generally shows only the sender, the receiver, and the subject line. As we discussed in Chapter 3, there is a significant amount of data in the unseen headers of the email that gives the investigator important information that can be useful in possibly establishing an email's sen- der's identity. We know that in general an email travels from a sender's computer to their mail service to recipient's mail service, where it resides on a mail server (computer that stores and delivers mail). Each next time the receiver logs into his or her account, the mail reader retrieves the message to his or PC/workstation. As the email travels through the Internet, from email server to email server, it gathers data from each processing server. Each of these servers gives the investigator an idea of how the email traveled from sender to receiver. In the following Figure 8 we have shown the process of the email traveling through the Internet.



Where is the Evidence?

In general about where evidence could be, it could be in numerous places along that path (Figure 8.4). However, that does not mean a copy of the email will exist on each location when you attempt to locate it. Depending on the jurisdiction, records of the email transfer may not be required to be kept by government regulations. In the United States, there are no specific record retention requirements for tracking email. Each service provider sets its own standards for logging information. What we can generally identify are the copies of a previously sent email messages that may be stored at accessible loca- tions. Those accessible locations include:

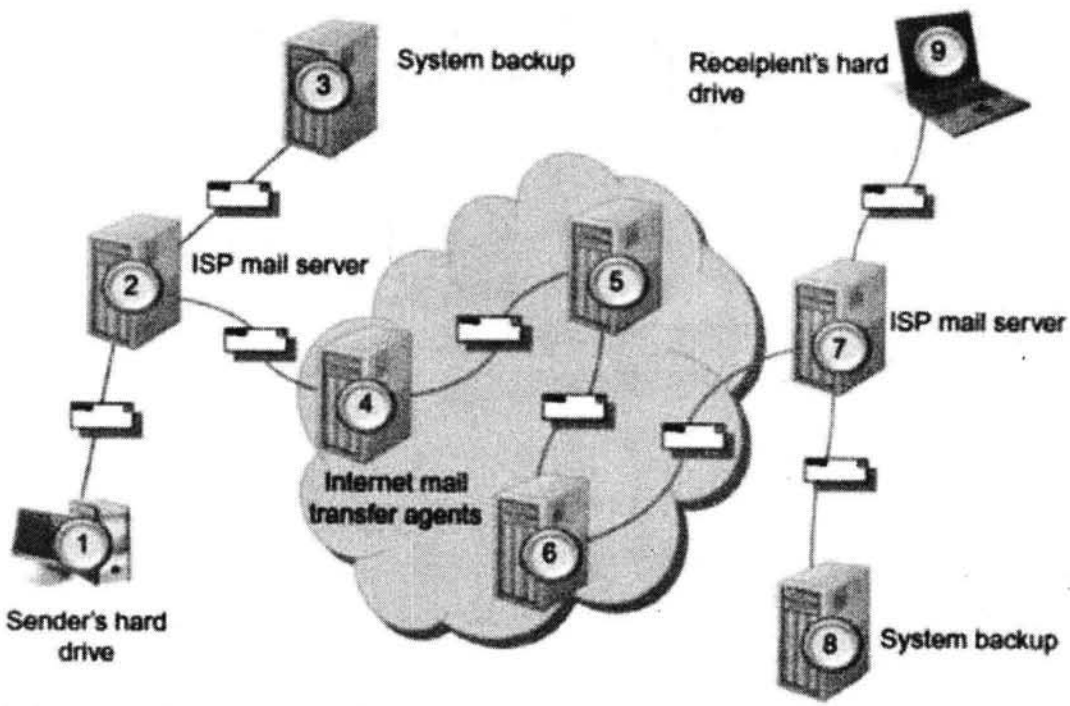
The sender's device

The sender's mail server

The recipient's mail server

The recipient's device.

A record of the email transmission (date, time, source, and destination) can reside in these same locations. Accessing these records can be done through the sender's device or through a forensic examination of the device. Before accessing data, be aware there are different legal requirements in play. Accessing data that resides on the sender's device requires consent or a tradi- tional search warrant. However, in the United States, data that resides on a server requires compliance with the Stored Communications Act (SCA) (see Chapter 4). Of course, accessing any of the records requires the proper legal authority which can include consent, a subpoena, or search warrant. Additionally, depending on the laws in the investigator's country, other legal options for access may be available.



Viewing email headers:

To determine the sender of an email, an investigator needs the email's header information. An email header is the information added to the beginning/top of the electronic message. Normally, email clients and web services only show an abbreviated form of the header. Email headers are created by the email servers that process the messages. Adding information depends on the email protocol used. Not every server adds detailed information to the header as it passes through the server. Viewing the email headers is different for each email pro- gram or service. In Chapter 4, we discussed using Spamcop from the Internet Investigators Toolbar to identify the specifics of accessing email headers for different email services and tools. From the Spamcop website, we can easily identify how to access full email headers to be reviewed for identifying information.

The information commonly displayed are the abbreviated headers. We normally see in an email:

From: To:

CC:

Subject:

Date:

For the investigator, the identifying information is the "From" line which is the email address the message purportedly came from, the "To" line which is where the message was sent, and the "CC" line is where other email addresses receiving the message are included. Is this information enough to properly trace an email? The answer is it certainly no. There is more information which can be used to effectively identify email movement through the Internet.

The full header provides the investigator with significantly more data with which to determine the veracity of the email as well as its origin. What the full headers can help the investigator identify are:

- Who sent the email
- Which network it originated from
- Which email servers processed it

CHAPTER 4

4.1 AUDIT TRAILS

Audit trails maintain a record of system activity both by system and application processes and by user activity of systems and applications. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications. This bulletin focuses on audit trails as a technical control and discusses the benefits and objectives of audit trails, the types of audit trails, and some common implementation issues.

An audit trail is a series of records of computer events, about an operating system, an application, or user activities. A computer system may have several audit trails, each devoted to a particular type of activity. Auditing is a review and analysis of management, operational, and technical controls. The auditor can obtain valuable information about

activity on a computer system from the audit trail. Audit trails improve the auditability of the computer system.

Audit trails may be used as either a support for regular system operations or a kind of insurance policy or as both of these. As insurance, audit trails are maintained but are not used unless needed, such as after a system outage. As a support for operations, audit trails are used to help system administrators ensure that the system or resources have not been

harmed by hackers, insiders, or technical problems.

4.2 BENEFITS AND OBJECTIVES

Audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events (actions that happen on a computer system), intrusion detection, and problem analysis.

Individual Accountability

Audit trails are a technical mechanism that help managers maintain individual accountability. By advising users that they are personally accountable for their actions, which are tracked by an audit trail that logs user activities, managers can help promote proper user behavior. Users are less likely to attempt to circumvent security policy if they know that their actions will be recorded in an audit log.

For example, audit trails can be used in concert with access controls to identify and provide information about users suspected of improper modification of data (e.g., introducing errors into a database). An audit trail may record "before" and "after" versions of records. (Depending upon the size of the file and the capabilities of the audit logging tools, this may be very resource-intensive.) Comparisons can then be made between the actual changes made to records and what was expected. This can help management determine if errors were made by the user, by the system or application software, or by some other source.

Audit trails work in concert with logical access controls, which restrict use of system resources. Granting users access to particular resources usually means that they need that access to accomplish their job. Authorized access, of course, can be misused, which is where audit trail analysis is useful. While users cannot be prevented from using resources to which they have legitimate access authorization, audit trail analysis is used to examine their actions. For example, consider a personnel office in which users have access to those personnel records for which they are responsible. Audit trails can reveal that an individual is printing far more records than the average user, which could indicate the selling of personal data. Another example may be an engineer who is using a computer for the design of a new product. Audit trail analysis could reveal that an outgoing modem was used extensively by the engineer the week before quitting. This could be used to investigate whether proprietary data files were sent to an unauthorized party.

Reconstruction of Events

Audit trails can also be used to reconstruct events after a problem has occurred. Damage can be more easily assessed by reviewing audit trails of system activity to pinpoint how, when, and why normal operations ceased. Audit trail analysis can often distinguish between operator-induced errors (during which the system may have performed exactly as instructed) or system-created errors (e.g., arising from a poorly tested piece of replacement code). If, for example, a system fails or the integrity of a file (either program or data) is questioned, an analysis of the audit trail can reconstruct the series of steps taken by the system, the users, and the application. Knowledge of the conditions that existed at the time of, for example, a system crash, can be useful in avoiding future outages. Additionally, if a technical problem occurs (e.g., the corruption of a data file) audit trails can aid in the recovery process (e.g., by using the record of changes made to reconstruct the file).

Intrusion Detection

Intrusion detection refers to the process of identifying attempts to penetrate a system and gain unauthorized access. If audit trails have been designed and implemented to record appropriate information, they can assist in intrusion detection. Although normally thought of as a real-time effort, intrusions can be detected in real time, by examining audit records as they are created (or through the use of other kinds of warning flags/notices), or after the fact (e.g., by examining audit records in a batch process).

Real-time intrusion detection is primarily aimed at outsiders attempting to gain unauthorized access to the system. It may also be used to detect changes in the system's performance indicative of, for example, a virus or worm attack (forms of malicious code). There may be difficulties in implementing real-time auditing, including unacceptable system performance.

After-the-fact identification may indicate that unauthorized access was attempted (or was successful). Attention can then be given to damage assessment or reviewing controls that were attacked.

Problem Analysis

Audit trails may also be used as on-line tools to help identify problems other than intrusions as they occur. This is often referred to as real-time auditing or monitoring. If a system or application is deemed to be critical to an organization's business or mission, real-time auditing may be implemented to monitor the status of these processes (although, as noted above, there can be difficulties with real-time analysis). An analysis of the audit trails may be able to verify that the system operated normally (i.e., that an error may have resulted from operator error, as opposed to a system-originated error). Such use of audit trails may be complemented by system performance logs. For example, a significant increase in the use of system resources (e.g., disk file space or outgoing modem use) could indicate a security problem.

4.3 AUDIT TRAILS AND LOGS

A system can maintain several different audit trails concurrently. There are typically two kinds of audit records,

(1) an event-oriented log and

(2) a record of every keystroke, often called keystroke monitoring. Event-based logs usually contain records describing system events, application events, or user events.

An audit trail should include sufficient information to establish what events occurred and who (or what) caused them. In general, an event record should specify when the event occurred, the user ID associated with the event, the program or command used to initiate the event, and the result. Date and time can help determine if the user was a masquerader or the actual person specified.

Keystroke Monitoring

Keystroke monitoring is the process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails. Examples of keystroke monitoring would include viewing characters as they are typed by users, reading users' electronic mail, and viewing other recorded information typed by users.

Some forms of routine system maintenance may record user keystrokes. This could constitute keystroke monitoring if the keystrokes are preserved along with the user identification so that an administrator could determine the keystrokes entered by specific users. Keystroke monitoring is conducted in an effort to protect systems and data from intruders who access the systems without authority or in excess of their assigned authority. Monitoring keystrokes typed by intruders can help administrators assess and repair damage caused by intruders.

Audit Trails and Verification

(1) Transactions that meet exception criteria shall be completely and accurately highlighted and reviewed by personnel independent of those that initiate the transaction.

(2) Adequate audit trails shall be captured and certain information needed to determine sensitive events and pattern analysis that would indicate possible fraudulent use of the system (e.g. repeated unsuccessful logons, access attempts over a series of days) shall be analyzed. This information includes such information as who, what, when, where, and any special information such as:

(i) Success or failure of the event

(ii) Use of authentication keys, where applicable

(3) Automated or manual procedures shall be used to monitor and promptly report all significant security events, such as accesses, which are out-of-pattern relative to time, volume, frequency, type of information asset, and redundancy. Other areas of analysis include:

(i) Significant computer system events (e.g. configuration updates, system crashes)

(ii) Security profile changes

(iii) Actions taken by computer operations, system administrators, system programmers, and/or security administrators

(4) The real time clock of the computer system shall be set accurately to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases.

(5) The real time clock of the computer or communications device shall be set to Indian Standard Time (IST). Further there shall be a procedure that checks and corrects drift in the real time clock.

(6) Computer system access records shall be kept for a minimum of two years, in either hard copy or electronic form. Records, which are of legal nature and necessary for any legal or regulation requirement or investigation of criminal behaviour, shall be retained as per laws of the land.

(7) Computer records of applications transactions and significant events must be retained for a minimum period of two years or longer depending on specific record retention requirements.

4.4 PUBLIC-KEY CRYPTOGRAPHY,

Public-key cryptography, or asymmetric cryptography, is an encryption scheme that uses two mathematically related, but not identical, keys - a public key and a private key. Unlike symmetric key algorithms that rely on one key to both encrypt and decrypt, each key performs a unique function. The public key is used to encrypt and the private key is used to decrypt.

It is computationally infeasible to compute the private key based on the public key. Because of this, public keys can be freely shared, allowing users an easy and convenient method for encrypting content and verifying digital signatures, and private keys can be kept secret, ensuring only the owners of the private keys can decrypt content and create digital signatures.

Since public keys need to be shared but are too big to be easily remembered, they are stored on digital certificates for secure transport and sharing. Since private keys are not shared, they are simply stored in the software or operating system you use, or on hardware (e.g., USB token, hardware security module) containing drivers that allow it to be used with your software or operating system.

Digital certificates are issued by entities known as Certificate Authorities (CAs).

The main business applications for public-key cryptography are:

- **Digital signatures** - content is digitally signed with an individual's private key and is verified by the individual's public key
- **Encryption** - content is encrypted using an individual's public key and can only be decrypted with the individual's private key

4.5 DIGITAL SIGNATURE

1. Authentication of electronic records

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record. Explanation- For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible-

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

Functions of Authority Controller

The Controller may perform all or any of the following functions, namely:-

(a) exercising supervision over the activities of the Certifying functions, namely :-

(b) certifying public keys of the Certifying Authorities;

(c) laying down the standards to be maintained by the Certifying Authorities;

(d) specifying the qualifications and experience which employees of the Certifying Authority should possess;

(e) specifying the conditions subject to which the Certifying Authorities shall conduct their business;

(f) specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key;

(g) specifying the form and content of a Digital Signature Certificate and the key;

(h) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;

(i) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;

(j) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;

(k) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;

(l) resolving any conflict of interests between the Certifying Authorities and the subscribers;

(m) laying down the duties of the Certifying Authorities;

(n) maintaining a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

Disclosure

(1) Every Certifying Authority shall disclose in the manner specified by regulations-

(a) its Digital Signature Certificate which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate;

(b) any certification practice statement relevant thereto;

(c) notice of the revocation or suspension of its Certifying Authority certificate, if any; and

(d) any other fact that materially and adversely affects either the reliability of a Digital Signature Certificate, which that Authority has issued, or the Authority's ability to perform its services.

(2) Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Digital Signature Certificate was granted, then, the Certifying Authority shall-

(a) use reasonable efforts to notify any person who is likely to be affected by that occurrence; or

(b) act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

4.6 Security Benefits of Digital Signatures

Assuming the private key has remained secret and the individual it was issued to is the only person with access to it, digitally signing documents and emails offers the following benefits.

- **Authentication** – since the individual's unique private key was used to apply the signature, recipients can be confident that the individual was the one to actually apply the signature
- **Non-repudiation** – since the individual is the only one with access to the private key used to apply the signature, he/she cannot later claim that it wasn't him/her who applied the signature
- **Integrity** - when the signature is verified, it checks that the contents of the document or message match what was in there when the signature was applied. Even the slightest change to the original document would cause this check to fail.

Security Benefits of Encryption

Assuming the individual's private key has not been compromised, encrypting data and messages offers the following security benefits.

- **Confidentiality** - because the content is encrypted with an individual's public key, it can only be decrypted with the individual's private key, ensuring only the intended recipient can decrypt and view the contents
- **Integrity** - part of the decryption process involves verifying that the contents of the original encrypted message and the new decrypted match, so even the slightest change to the original content would cause the decryption process to fail

3.15 Introduction to Forensic Photography

Photography of everything from landscapes to historical events has preserved and illustrated history for the past 200 years. When a photograph of a forged document was presented and allowed as courtroom evidence in 1851[1], photography as a forensic tool was born and soon became a boon to cases of identification and scene analysis. Crime scene photography became cutting edge in the 1870s and new technologies have expanded its use ever since.

Principles of Crime Scene Photography

There is no prescribed length of time it takes to photographically document a crime scene. The amount of time spent depends on the size and

complication in the crime scene, how much there is to document and environmental factors like weather or danger to the investigative team. It can consist of thousands of photographs and hours of work.

Crime scene photography should not just focus on the obvious. The purpose of crime scene photography is to document what is there and where it is in relationship to the scene, whether it is obviously connected to the crime or not. For example, a photographer in Florida shot the inside of every cabinet and the refrigerator at a homicide scene in a home, just as a matter of procedure. It was later discovered that the victim had a receipt for a six-pack of beer, matching the beer shown in the photograph of the refrigerator.

Relatives noted that the victim did not drink beer. Further investigation led the team to the convenience store where the beer was purchased and the surveillance tape showed the victim with an unknown person purchasing the beer. It turns out that the victim had picked up a hitchhiker, purchased beer for that person and come back to the house. The photograph of the refrigerator contents had created the link enabling the investigators to find the suspect.

Capturing the Scene

Photography, or "writing or drawing with light", is defined as the process or art of producing images of objects on sensitized surfaces by the chemical action of light or of other forms of radiant energy, such as X-rays, gamma rays or cosmic rays. Fixing an image permanently has been possible since the 1820s in a variety of ways from the daguerreotype, to silver plates, to film and now digitally.

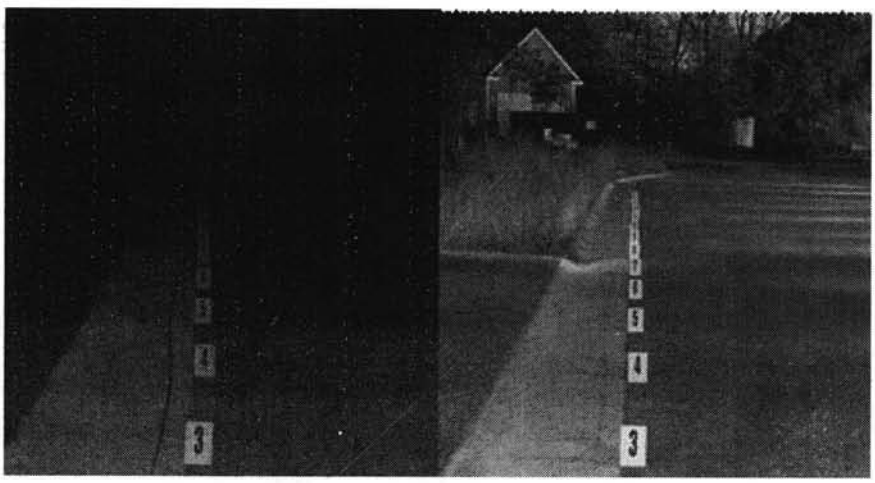
Some may consider photography more of an art than a science, but well-taken crime scene photographs can aid scientists, investigators and members of the court in their search for the truth. This makes photography a critical first responder skill. Larger agencies may have specially trained and certified crime scene photographers with high-end cameras and lighting to document crime scenes and evidence, but more often the first responder needs to do what they can with equipment assigned to them. That said, many of today's digital point-and-shoot cameras have a variety of settings that, with some basic operator training, allow for proper documentation.

Controlling the Light

Photographers use several means to tell the camera how to capture the image including aperture, shutter speed, depth of field and white balance. Aperture refers to the size of the opening that lets light into the camera and shutter speed is how long that opening, or shutter, remains open. Depth of field is the amount of area in front of (foreground) and behind (background) an object that remains in focus. Lastly, white balance allows the camera torecord the proper temperature of light, resulting in an accurate representation of the color tones of objects in the photograph.

Brightening the Darkness

Experienced photographers often use a technique called "painting with light" to expose image details in dark or near-dark conditions. In this technique, the shutter is held open for seconds or minutes and the photographer walks through the scene adding light from sources such as a flashlight or detached camera flash.



Crime scene at night & after using the painting with light technique. (Courtesy of Scott Campbell)

However the photographer chooses to capture the image, the main reason for crime scene photography is to thoroughly document the entire scene, the evidence, and any areas of special significance to the investigation.

4.7 Why and when is crime scene photography used?

Photography should be used as part of the documentation for all physical crime scenes, including traffic collisions, burglaries, homicides, or any number of crimes against people or property. Photographs, however, can be misleading and confusing to the viewer. Therefore, crime scene photographers must ensure their work is both ethical and honest while capturing as much accurate information and detail as possible. Documenting all elements of a crime scene is a major stepping stone when trying to piece together what happened, how it happened and who did it.

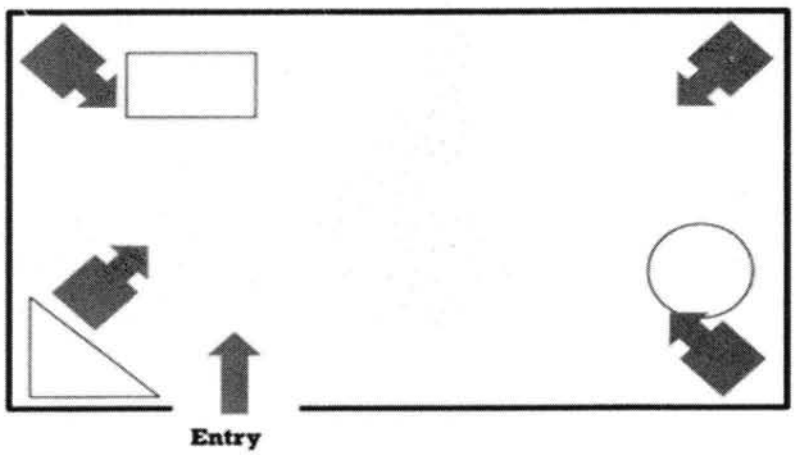
Crime scenes are typically full of activity and often unpredictable, with first responders assisting victims and investigators beginning their work. Even in the most ideal situation, capturing photographic evidence can be challenging. An experienced photographer will know to take photos at all stages of the investigation and that it is better to have too many than not enough images.

The following steps are taken to ensure proper photographic documentation:

1. **Secure the scene:** In all forensic investigations, the first step is to secure the crime scene.
2. **Evaluate conditions:** Next, the photographer should evaluate the available light and weather conditions and adjust camera settings appropriately. Crime scenes can be indoors, outside or both; they can be vehicles, include multiple rooms, or any combination of locations, therefore no single camera setting will work for all crime scenes.

3. **Shoot the scene:** The photographer should take photographs before anything is disturbed, progressively working through the scene from outside to close-up pictures. Many shots should be taken, from the entire scene, to medium shots to show the relationship of evidence to the overall scene.

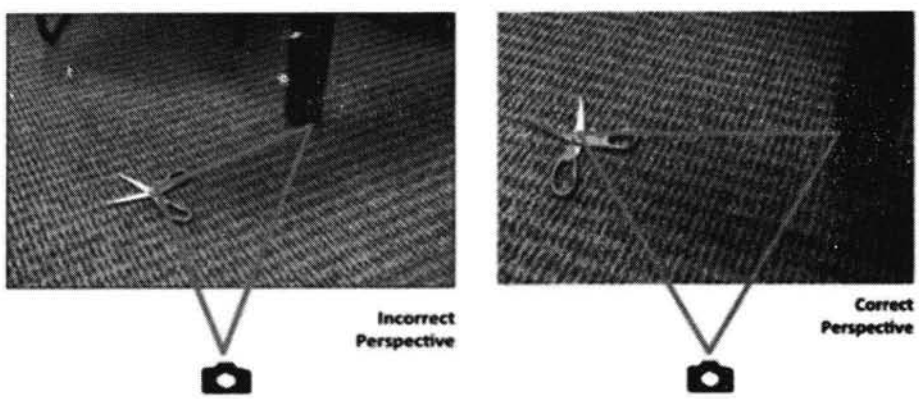
   Just like a television program will show the viewer the outside of a building to establish where the characters are going, the crime scene photographer should capture the whole scene first using wide-angle shots covering the entire scene from the approach and through every area. Close-up images of evidence can be taken out of context, so establishing the scene first with wide and medium shots is critical.



In addition, photographs should be taken looking up from the scene to capture evidence or environmental factors that may be above the scene.

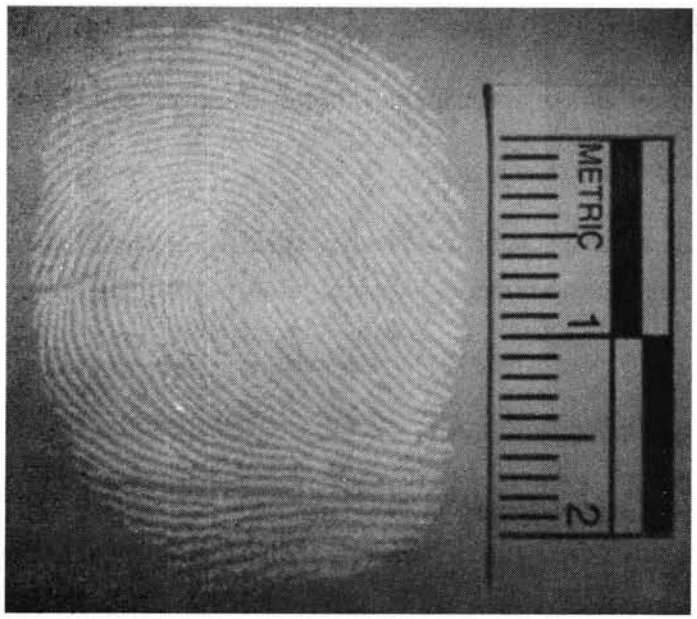
4. **Photograph the victims:** The next series of shots should include victims (if present) to show locations, injuries and condition.

5. **Photograph the evidence:** Then each piece of evidence should be photographed to illustrate where it was found. This establishes the relationships of the evidence to the victim, the victim to the room and so on. These photographs should be taken from straight above or straight on at right angles, eliminating potential distance distortions. Each piece of evidence should be photographed with a scale to indicate size and without a scale.

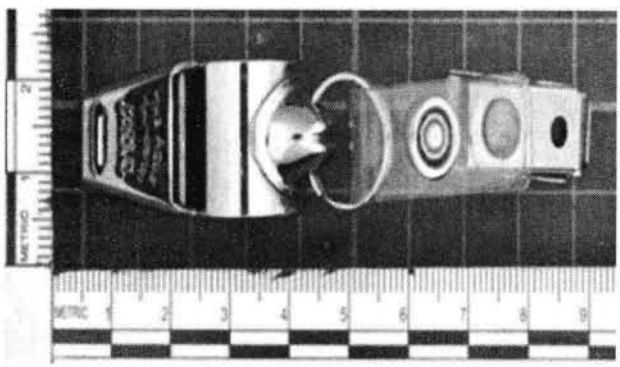


(Courte sy of Daniel Nichols, NFSTC)

6. **Evidence markers:** Photographs should be taken before evidence markers are placed, then again after. These initial shots are important to prove that no one has tampered with the crime scene.



7. **Re-shoot for new evidence:** If investigators mark new evidence, the whole series of shots should be repeated, including all evidence shots. These photos should include the entire piece of evidence and a scale to indicate size.



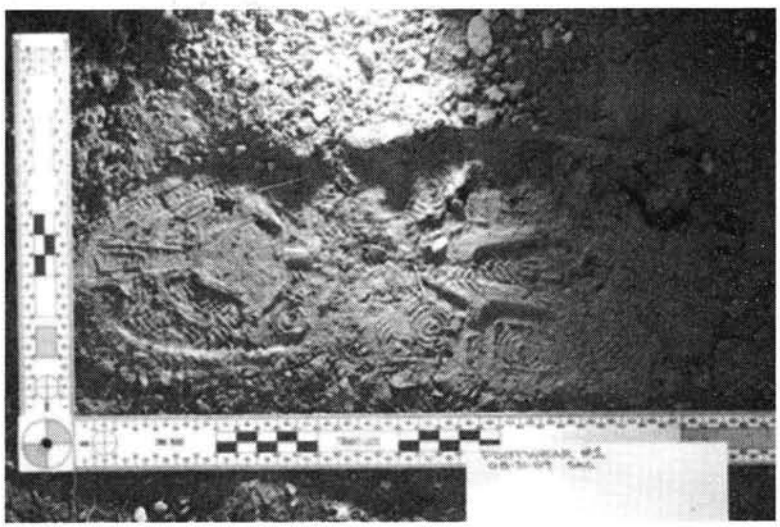
(Courtesy of Becky Carter, CEP, NFSTC)

Special imaging techniques and lighting should be used to capture things like fingerprints, indentations, shoe and tire track impressions, vehicle identification numbers (VIN) and very small pieces of evidence. Techniques may include:

- **Alternate light sources (ALS)** – such as lasers, blue or green lights and colored filters that help detect processed latent fingerprints or other hidden evidence and illuminate for photographing

Green light used to illuminate a latent fingerprint. (Courtesy of Scott Campbell)

- **Oblique angle lighting** -- using a flashlight, camera flash or ALS at a very low angle to cast shadows that allow an imprint or impression to be photographed



Oblique light used to add contrast to a footprint. (Courtesy of Scott Campbell)

Cartridge case details captured with macro lens. (Courtesy of Scott Campbell)

Photographs should accurately document the lighting conditions at the scene. After those photos are taken, if necessary, a photographer will add artificial light, like a flash, to compensate for a camera's limitations in capturing the visible range of light under certain conditions.

Shoot fast: Sometimes environmental factors such as rain, snow or traffic can make conditions difficult for photography. The photographer must work quickly to capture as much visual documentation as possible from a deteriorating scene.

Photograph the victim later: If a victim must be moved or requires treatment, the photographer can go back to document the victim's injuries. Various techniques using special lighting and colored filters can highlight injuries (bruising, scarring) and healing status.

4.8 Who Conducts the Photographic Analysis and Enhancements

Once working copies of all the photographs have been created, investigators can select images for analysis and enhancement. This is normally done by the photographer or, if available, within the audio/visual department in the laboratory. As with all evidence, detailed records should be kept regarding who accesses or works with the files and what techniques were used to enhance or otherwise modify the files.

4.9 How and Where Evidence Photographs are Processed

All photographs taken are saved as originally captured, entered into evidence inventory and tracked. Selected photographs of particular evidence or parts of a scene may need additional enhancement. This can be done within the department if the appropriate software is available or may be sent to a regional specialist. The most common enhancements include cropping, brightness and contrast adjustments and color processing.

Potential photographic enhancements follow the same rules as news journalism. An image may be lightened and darkened, cropped or the color enhanced. The white balance can be adjusted, but adding or removing information is unacceptable. When submitted for courtroom use, the original photograph must be available for comparison and the technician or examiner must be able to show and describe any enhancements that were done, and why.

When images are presented, they must be clearly identified as a working and/or enhanced version. The original camera sequential numbering system should be retained to show that images are in order and none have been removed. The working images should not be renamed until identified or selected for use, and original files should not be renamed at all.

4.10 Type of Equipment Used

Investigators and technicians photographing a crime scene should have access to a good quality camera that is capable of manual override and has interchangeable lenses, off-camera flash, cable release, and a tripod mount. With these tools and a widely attainable level of training and practice, good quality photographs can be taken in a broad range of scenarios including low light, highly reflective surfaces and tight spaces.

That said, many first responders are equipped with basic, consumer-level point-and-shoot cameras. Since they may be in the best position to capture important evidence, basic knowledge of how to capture an image and use the camera they have is very important. Even with simple equipment, a first responder with introductory photography training can produce images of sufficient quality to support an investigation.

Cell phones and other personal electronic devices with integrated cameras are not recommended unless their use is an operational necessity. An example would be if a muddy shoe print is found near a crime scene but it is raining. The shoe print may disappear quickly, so if a cell phone camera is the only camera available, then it would be operationally

4.11 INTRODUCTION - FORENSIC EVIDENCE, AUDIO AND VIDEO RECORDINGS

Unlike other forms of forensic evidence, audio and video recordings can provide a real-time, eyewitness account of a crime so investigators can watch or hear what transpired. For instance, a surveillance video captures a bank robbery in progress, or a hidden camera records an undercover sting operation. Over the past decade, sources of recorded audio and video that can assist in an investigation have increased exponentially. Closed circuit television systems (CCTV) and video and audio recorders can be found in businesses, at traffic intersections, parking lots, bank machines, on police-vehicle dashboards and of course, in cell phones.

For large-scale events or crimes, the sheer amount of recorded audio and video evidence can be massive. During the riots that occurred in Vancouver, British Columbia after the 2011 Stanley Cup Finals, more than 5,000 hours of recordings were captured. Law enforcement has since brought charges against more than a hundred rioters using video evidence and more charges are expected.

For most crimes, however, high-quality audio and/or video recordings are often not available. This is where forensic audio and video expertise can help. Forensic experts have many techniques to enhance recordings that can bring out details and provide a clearer picture of what occurred, or make an audio recording more audible. This in turn helps investigators, lawyers and jurors better conduct their duties.

Principles of Forensic Audio and Video Analysis

To assist in an investigation, forensic experts can repair, recover, enhance and analyze audio and video recordings using an array of scientific tools and techniques.

Repair and Recovery of Evidence

Before audio and video evidence can be analyzed, it may first need to be repaired or recovered from damaged media or a damaged recording device.

Repairing evidence is especially common for analog and digital magnetic tape. It may need to be spliced back together or put into a new audio/video housing in order to recover the audio or video. In today's digital world, CDs, DVDs, cell phones, portable cameras and other sources of digital media and recording devices can be damaged by heat, misuse, the environmental conditions of a crime scene, or simply on purpose by an offender. Even in these situations, the digital files can be recovered and used for analysis.

Evidence Enhancement

The most common function of forensic video and audio experts is to clarify a recording so that it is more apparent to investigators, attorneys and jurors what the evidence demonstrates.

To enhance a video recording, filters can be used to adjust the brightness and contrast, correct the color, crop and resize an image, enhance edge detail and reduce visual distortion. The speed of playback can also be adjusted to more accurately display the frame rate at which it was recorded.

To enhance an audio recording, filters can be employed to improve clarity. This may entail removal of unwanted noise or enhancing the intelligibility of speech.

Recordings will often be made in less than ideal circumstances, such as when someone is wearing a body wire. Utilizing audio engineering techniques may allow faint voices or events to be heard more clearly on playback.

Analysis, Interpretation and Identification

Authentication of recordings – In many criminal cases, the authenticity of the recording and the content of the recording may be called in to question. Forensic audio and video experts can examine a variety of characteristics of the audio or video recording to determine whether the evidence has been altered. This includes confirming the integrity (verification) of the recording, as well as authenticating that the content of the image or audio is what it purports to be.

If the ambient sound present on an audio recording changes abruptly, this could indicate that the environment where the recording took place suddenly changed. The volume and tone of a voice on the recording can provide clues as to distance and spatial relationships within a scene. Lighting conditions can be examined to estimate the time of day or environmental conditions at the time of the recording.

Technical details may also confirm information about a recording. For instance, an unnatural waveform present in the audio or video signal may indicate that an edit has been made. A physical identifier may be present in the signal on magnetic tape that can identify it as a copy or indicate that it was recorded on a particular device. Sometimes, a perpetrator will try to destroy audio or video evidence; however, using these methods, the recording can be analyzed to determine what occurred.

In the famous Watergate investigation, a great deal of effort was spent examining an 18½-minute gap in an audio recording of President Richard Nixon discussing the Watergate break in with his Chief of Staff. Analysis of the audio signature[1] left behind in this erased portion allowed investigators to determine which White House tape recorder made the erasure and how many different erasures were made. Examining the level of AC hum recorded to tape even provided details on whether the recording took place in Nixon's secretary's office or in another location.

And new techniques are constantly being developed. A unique approach employed in the United Kingdom examines the low-frequency hum captured when a recorder is plugged into an electrical outlet or near a strong electrical current. This frequency will alternate slightly depending on the power load experienced at that time of day. By examining minute fluctuations of this frequency, analysts can determine whether a recording took place at the stated time and whether the recording is continuous and unaltered. This technique has been in use in the UK for over eight years; in the United States, this technique is still being researched and databases are being built for comparison.

Identifying people or objects on a recording — Identifying a person or object from an image on a video or voice on an audio recording requires training in Image Content Analysis or speech science. These examinations are detailed comparisons of an unknown recording to a known recording, or an unknown object to a known object in an attempt to make a positive identification. For instance, an image of a hat at the crime scene may be

compared with a hat found on a suspect. The comparison techniques used in image analysis follow the same detailed comparison techniques as Fingerprint and Document examiners. The analysis and comparison of voices is an evolving area of practice that can be controversial in criminal cases.

Audio and Video Evidence That May Be Analyzed

Audio and video evidence can be found at more locations and from more diverse sources than ever before. From convenience stores to fast food restaurants, malls to banks, traffic intersections to parks, CCTV systems are virtually everywhere. And cell phone cameras extend a watchful eye to nearly every corner of every town. Audio evidence may be available from 911 calls, telephone answering machines, voicemail recordings, video cameras, cell phones and computer files.

4.12 How the Evidence Is Collected

Depending on the circumstance, the surroundings, and the witnesses who may have been present, several different recordings of an event may be available. The responding officers or crime scene investigators should first identify all video or audio evidence that may exist. In addition to surveillance cameras at the scene, surveillance systems nearby may provide valuable footage, such as recordings of a perpetrator approaching or fleeing a scene.

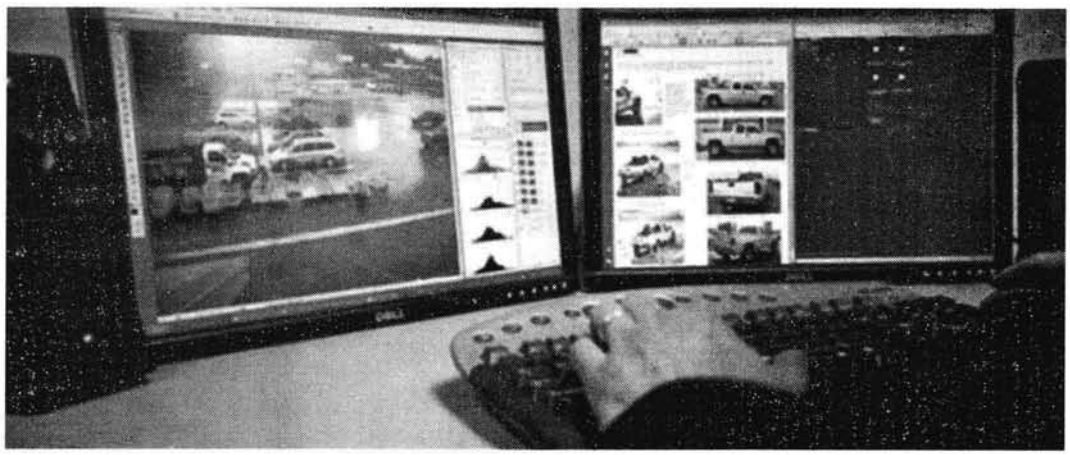
Even if the recording does not appear to be very clear or useful, all relevant footage should be collected. Forensic enhancement may recover details that aren't noticeable when viewing or listening to the unprocessed recording.

Digital video and audio - Well over half of all closed-circuit television evidence seized by police today is digital and file-based, although some systems can record to digital magnetic tape. Digital video recorders come in two general types: embedded stand-alone and PC-based. Both types generally record the audio and video to hard drives; however, some systems record to secure digital (SD) cards and other removable media.

Digital video and audio evidence from CCTV systems are generally proprietary in nature and require a special software player produced by the manufacturer to play back the collected recordings properly. When the video and audio is collected from the device it needs to be retrieved in a manner that produces the best quality possible, which is usually the proprietary recorded files. There are numerous types of digital video and audio recording devices, with a variety of methods of exporting these files. Some will have CD/DVD writing capabilities, some use USB for output, and some, although digital, may only have analog outputs. Find further information on proper collection methods at

Analog video and audio -- Analog video systems are rapidly becoming a recording technology of the past; however, many are still in use today. If a system uses analog tape, the investigator should bear in mind that every playback of the tape will degrade the recorded images. Prior to ejecting the tape, the investigator will make sure

the tape is stopped, document everything on the display, then eject the tape and remove the write protection tab to prevent it from being recorded over. A copy of the tape should then be made for all future viewing, preserving the original video evidence.



Courtesy of Target® Forensic Services

How the Analysis Is Performed

The first step of an analysis is for the examiner to simply listen to or view the recorded footage. The examiner will then begin to locate the area of interest to be enhanced and examined in closer detail using specialized devices and software.

Before processing audio and video evidence, a working copy of the evidence may be created. This assures that the original evidence is always available in its unaltered state. In addition, the original will always be available for comparison to the processed copy.

All examination procedures are carefully constructed so that the image or video is a true and accurate representation of the scene. Investigators never change the recorded data—they only enhance what is already present.

Video Enhancement Techniques --- A variety of enhancement techniques can be employed on video evidence. It is important that the best video recording be submitted to obtain the best enhancement results. Limitations on the enhancement process may exist if an analog copy or digital file that has undergone additional compression is submitted for analysis. Techniques can include:

Sharpening --- Makes edges of images in the recording become more clear and distinct.

Video stabilization --- Reduces the amount of movement in the video, producing the smoothest possible playback.

Masking --- Covers the face or areas of the video that may protect a witness, victim or law enforcement officer.

Interlacing --- In an analog system, interlaced scanning is used to record images (a technique of combining two television fields in order to produce a full frame of video). A process called de-interlacing may be used to retrieve the information in both fields of video.

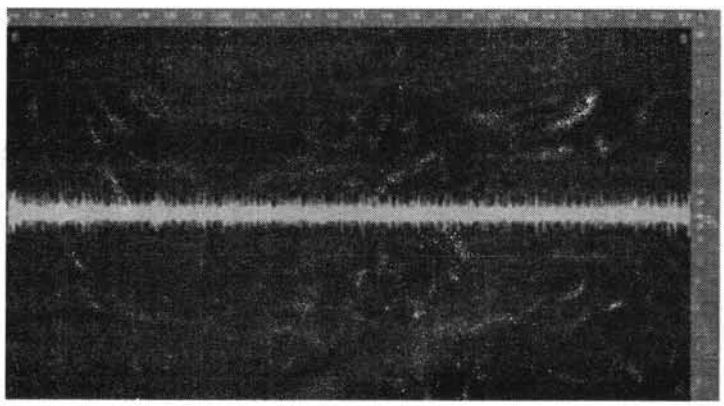
Demultiplexing --- Allows for isolation of each camera. In CCTV systems, a device called a multiplexer is used to combine multiple video signals into a single signal or separate a combined signal. These devices are frequently used in security and law enforcement applications for recording and/or displaying multiple camera images simultaneously or in succession.

Audio Enhancement Techniques --- For audio recordings, a variety of filters can be applied to enhance the material, bringing out specific aspects or events contained in the recording.

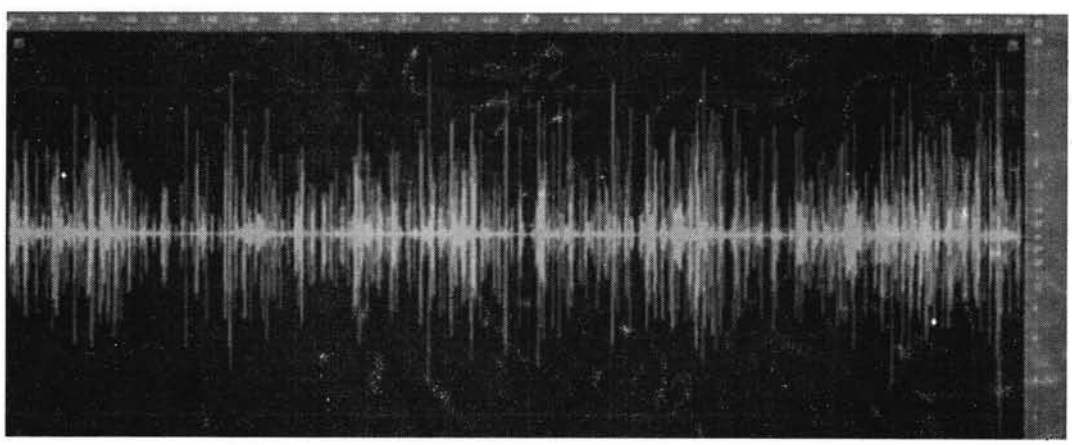
Frequency Equalization --- Highly precise equalizers can be used to boost or cut specific bands of frequencies. To help make speech more intelligible, the frequency band containing most speech content, 200Hz–5000Hz, can be amplified or isolated. If amplification is applied to a frequency range, other information residing in this frequency range will be boosted as well. If noise resides in this same range, this noise will also be increased, limiting the ability to clarify voices.

Loud background noises may be analyzed by a spectrum analyzer and the corresponding frequencies reduced so that these noises are less noticeable.

Compression --- Faint sounds in the recording can be boosted by compressing or leveling the signal so that the dynamic range of the material is reduced, making soft sounds more apparent.



Waveform of a recording made at a low volume with significantly loud ambient noise that is masking the speech content of the recording.



The same recording after enhancement. The noise is attenuated and the volume of the speech is increased.

CHAPTER 5

5.1 INTRODUCTION TO DATA LOSES AND RECOVERY

Data loss cases

Most common data loss causes include:

- **Accidental deletion of files or folders**

  Depending on the file system, each OS acts differently while deleting a file. For instance, in **Windows FAT** file system the OS marks file directory entries as "unused" and destroys file allocation information (except for the beginning of the file), in **NTFS** only the *file entry* is marked as *"unused"*, the record is deleted from the directory and the disk space is also marked as *"unused"*; in most **Linux/Unix** file systems the OS *destroys the file descriptor* (information about the file location, file type, file size etc.) and marks the disk space as *"free"*.

  The main purpose of file deletion is to release storage space used by the file for storing a new file. For performance reasons storage space is not wiped immediately, which makes the actual from the file remain on the disk until this storage space is reused for saving a new file.

- **File system formatting**

  File system formatting can be started by mistake, for example, by specifying a wrong disk partition or by mishandling a storage (e.g. NAS devices usually format the internal storage after an attempt to reconfigure RAID).

  The formatting procedure *creates empty file system structures* on the storage and *overwrites any information* after that. If the types of the file systems coincide, it destroys the existing file system structures by overwriting them with new ones; if the types of the file systems differ, the structures are written to different locations and may delete user's data.

- **Logical damage of a file system**

  This kind of failure may occur due to *blackouts* or *hardware failures*. Sometimes, logical damages are also caused by *software failures*. Modern file systems have a high level of protection against file system logical damages, yet, they remain helpless against hardware or software malfunctions.

  Even a small piece of wrong data written to a wrong location on the storage can cause the destruction of file system structures, breaking file system object links and making the file system non-readable.

- **Loss of information about partition**

  This failure may occur because of a failed *"fdisk"* operation or *user's errors*, which usually results in the loss of information about the partition location and size.

- **Storage failure**

  If you detect any *physical problems* on the storage (e.g. the storage is not running, making unusual noises, overheating or facing problems to read data etc.), **it is not recommended to take any actions by yourself**. You should take the storage to *a specialized data recovery laboratory*.

  If a failure has occurred to a **RAID** system (only one drive failure for RAID5, maximum two drives failure for RAID6 etc.), recovering data without the missing drive is possible, as the redundancy of RAID allows recovering data without a single storage.

5.2 Common Computer Problems

- Computer won't boot up
- Applications that are unable to run or load data
- Hard drive crashes
- Corrupt files or data
- Accidental reformatting of partitions
- Inaccessible drives and partitions
- Media surface contamination and damage

What Causes Data Loss?

- Sabotage
- Natural Disaster
- Hardware Error
- Virus Attack
- Human Error
  - Intentional deletion
  - Accidental overwriting of files
- Software Corruption

Cause	Example	Percentage
Hardware & System Problems	Disk drive crashes, electrical outages or power surges, manufacturer defects.	45%
Human Errors	Accidental deletions, overwriting files, causing trauma to desktop or laptop.	33%
Software Corruption or Application Error	Application displays an error message when a document is opened. Installing or removing a program corrupts another.	12%
Computer Viruses	i.e.: MyDoom.A MyDoom.B W32.Welchia.Worm W32.Blaster.Worm W32.Spybot.Worm Downloader.Trojan W32.Swen.A@mm	6%
Natural Disasters	Fires, floods, lightning, earthquakes.	4%

5.3 How to Prevent Data Loss

- Don't upgrade hardware or software without having a backup
- Physically secure your system from intruders
- Use firewalls and virus protection

Be prepared for physical disasters

Things to Know About Data Loss

- Data loss is disastrous at home, but for companies it causes setbacks in time and money.
- "93% of companies that experience data loss for more than 10 days file for bankruptcy within one year of the disaster."
- If the data loss recovery is dealt with quickly or the necessary precautions are taken prior to any problem, the company could retrieve the data more easily or not experience a problem at all.

5.4 Data Recovery

Data recovery is the process of retrieving or restoring digital information that is no longer accessible for some reason. A good example would be any file that has been mistakenly deleted, lost, or corrupted. The data recovery process varies based on the circumstances under which it was lost.

- The majority of data loss situations are recoverable.
- Computer storage systems may fail, but the data stored on them is not always completely lost.
- There are occasions when damage to data is permanent and complete data recovery is not possible.
- However, some data is usually always recoverable.
- Data recovery professionals can recover data from crashed hard drives, operating systems, storage devices,
- servers, desktops, and laptops using various proprietary data recovery tools and techniques.

How does recovery work?

The information remaining on the storage can be recovered to a safe location. Recovery chances depend greatly on the specific data loss situation, but you should keep in mind that *no information is recoverable after being overwritten*. For this reason, nothing should be written **into the storage until the last file is recovered**.

Data recovery software serves to get data back after its loss with the maximum result possible. Commonly, data recovery process is based on storage scan to find specific information (deleted files, lost file systems) and assemble structures of the damaged file system.

5.5 Data recovery chances

Data recovery chances strongly depend on the actual cause of data loss and further user's actions. To get the best possible data recovery result, it is strongly recommended to **prevent any possibility of anything being written** to the storage and **run data recovery software immediately**.

Chances for recovery

In the process of any file deletion, both intentional and accidental, the operating system aims at clearing storage space for new files marking the space used by previous files as "free". Fortunately, the storage space remains occupied by the previous file until it isoverwritten with a new one, thus leaving the possibility of retrieving deleted files.Chances to recover deleted files depend on the file system, as each file system conducts file deletion differently. In addition, users can increase data recovery chances by choosing efficient, safe and reliable data recovery software.

- **Data loss caused by file deletion**

  Any deleted file remains on the storage until the storage *space is reused by other data*. After file deletion, an OS may reuse disk space to store a new file. Thus, even a minor piece of information written to the storage can cause permanent data loss. Using a web browser might result in overwriting deleted files through caching or saving cookies to the storage. If you install any software to the same drive, your data can be overwritten as well.

Another factor that affects data recovery chances after file deletion is the *file deletion algorithm of a file system*. For Windows NTFS file system recovery chances are quite high: if the file descriptor remains on the disk, the software can easily find all the required information about the file. Unlike NTFS, BSD UFS file system destroys information about file start, location and size permanently and together with a high degree of file fragmentation (typical for this file system) leaves few chances for successful data recovery.

Other file systems (like FAT) provide average chances for data recovery. Here, the information is destroyed *partly* (like information about file fragments), but information about the file name, start and size remains on the disk. Heuristic algorithms allow "predicting" file fragments and recover undamaged files. Please, keep in mind, that due to the lack of real information about the allocation of file fragments any data recovery software may fail to detect the actual position of the file, especially if several fragmented files situated close to the same location on the storage weredeleted.

These factors determine using a set of *deterministic* and *heuristic algorithms* to predict the location of the deleted file. Please, consider that these algorithms differ from manufacturer to manufacturer and so do the recovery results.

- **Recovery after file system formatting**

After file system formatting, a part of information on the storage is destroyed due to overwriting the space with new information of a new file system. Again, data recovery chances after formatting *depend largely on the differences between the original and the new file systems.*.

For instance, if a file system is formatted with FAT, it overwrites huge amount of storage space on the disk *starting with zeros* (empty block allocation tables) and therefore destroying all the previous data. Even if the previous file system was FAT as well, the information about allocation of the previous files will be lost completely. Other file systems usually allocate more or fewer structures to different storage locations.

Sometimes, recovery chances are higher when the file system is *formatted with the same file system type*: in case of NTFS overwritten with NTFS data recovery chances are quite high, while FAT overwritten with FAT has worse recovery chances.

Efficient data recovery software usually gives a satisfying recovery result after file system formatting. Most file systems (except those like FAT) might keep file allocation information, directory records and file names allowing users to reconstruct the file system successfully. However, since new structures are written to the disk, *some user information can be damaged*and some files or folders can be lost.

- **Recovery after file system damage**

In this case, data recovery software applies the same techniques as in the case of a formatted file system. Data recovery chances depend on the actual file system damage (damage of user files, file folders, file location, file name).

- **Loss of information about partition**

  This data loss case is an extremely singular one. Working with this type of damage, data recovery software identifies the file system starting with the known file system structures while scanning the storage. If the loss didn't affect the file system itself, the data can be fully retrieved in its original form.

- **Hardware failure**

  Note: Never try to recover data from a failed or failing storage on your own. This can result in permanent data loss. The only exception is RAID systems where storage redundancy allows recovering data completely with the failed unit missing.

  RAID failure might also affect the file system. But if the file system remains intact, your RAID has relatively high data recovery chances. For further information concerning the specifics of data recovery from RAID please refer to RAID systems recovery.

- **Recovery of wiped/overwritten data**

  Recovery of wiped and then overwritten data is impossible due to the technology of writing data. The myth about the possibility to recover the lost files that were overwritten is the result of successful attempts to recover data from old floppy disks and hard drives. These devices with storage capacity from kilobytes to megabytes use very wide magnetic trace and simple digital encoding to store information. That is why it was possible to read *"traces of data"* after wiping or overwriting by calibrating read *"head"* sensitivity and position.

  Modern systems use very thin tracks, high precision of head calibration and extremely high signal frequency near to the top of technology limit. Performance of modern chips only allows picking a good discrete signal from a disk platter and never identifies any *'signal traces'*. This scheme is impossible for any digital device as discreet signal frequency to handle such data lies much beyond the theoretical limit of electronic circuits.

5.6 Data Recovery Tips

- **DO's**
  - Backup your data frequently.
  - If you believe there is something wrong with your computer shut it down,do not continue to power up because you may do more damage.
  - If you here a clunk, clunk sound when you power up the drive, shut down! Do not panic nor turn the power button on and off.
  - Package the drive properly when you send it in to a data recovery specialist. You can cause additional damage to the hard drive if it is poorly packaged.

- **DON'TS**

  - Do not ever assume that data recovery is impossible; even in the worst cases, such as natural disasters data recovery specialists have been able to retrieve valuable data.
  - Never remove the cover from the hard drive; this will only cause further damage.
  - Do not rest your computer on a moveable object or piece of furniture.

Shock and vibration can result in serious damage to the hard drive.

- Do not subject the drive to extreme temperatures changes both hot and cold.
- In the case where a drive has been exposed to water, fire or even smoke do not try to power up.

5.7 DATA RECOVERY TECHNIQUES

- Use of software to recover data
- Use of machines to recover data

Software Data Extraction

- Data extraction is the process of moving data off of the imaged drive to another destination location.
- Data extraction software scans sectors of the hard drive and restructures the file system either in memory or another hard drive. The software can be used to copy the recoverable data to a destination location

Software Recovery

- Data loss can occur because the hard drive may have problems accessing the data it contains at a software or logical level.
- By making a complete sector copy (an exact copy including all deleted information) of the hard drive, using a program such as Norton GHOST, most data recovery programs search for deleted MFT (Master File Table) entries to undelete files.
- If the MFT is corrupt or defective, this method will not work.

Some data recovery programs will ignore the MFT and search all of the unallocated clusters to try to find and recover files.

Data recovery techniques

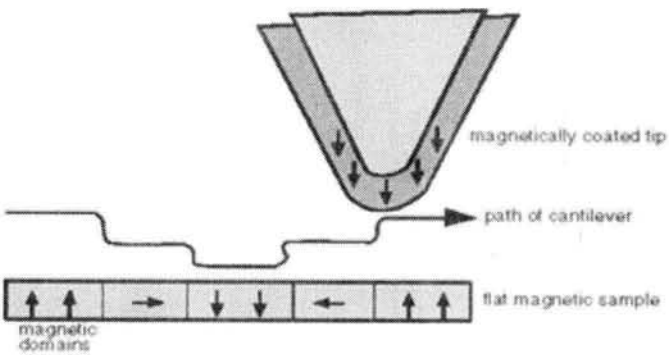
- **Scanning Probe Microscopy (SPM)**
- **Magnetic Force Microscopy (MFM)**
- **Scanning Tunneling Microscopy (STM)**

Scanning Probe Microscopy (SPM)

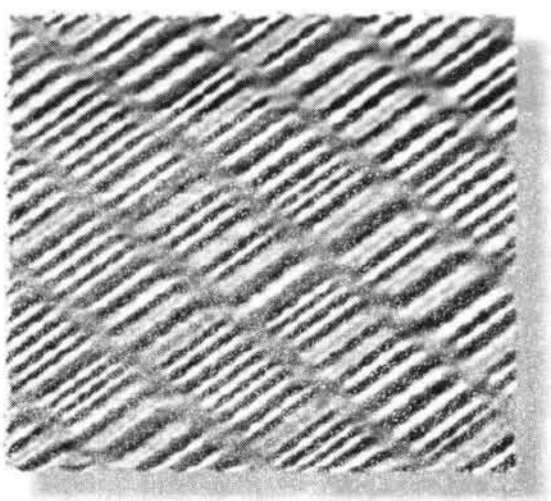
- A technique that is used to image and measure surfaces at the atomic level.
- Scans an atomically sharp probe over a surface which produces a 3D topographic image of the surface at the atomic scale.

Magnetic Force Microscopy (MFM)

- MFM (Magnetic Force Microscopy) is a new technique which images the spatial variation of magnetic forces on a sample surface.
- MFM is derived from scanning probe microscopy (SPM) and uses a sharp magnetic tip attached to a flexible cantilever for analysis.
- An image of the field at the surface is formed by moving the tip across the surface and measuring the force.
- Detectable old data will be present beside new data on the track which is usually ignored.
- Together with software, MFM can see past various kinds of data loss/removal.
- Each track contains an image of everything ever written to it, but each layer gets progressively smaller the earlier it was written.
- MFM looks at the minute sampling region to detect remnant magnetization at track edges.



MFM image showing the bits of a hard disk



Scanning Tunneling Microscopy (STM)

- STM (Scanning Tunneling Microscopy) is a more recent variation of MFM which uses a probe tip typically made by plating nickel onto a pre-patterned surface.
- The probe is scanned across the surface that is to be analyzed. STM measures a weak electrical current flowing between the tip and the sample. The image is then generated in the same way as MFM.

5.8 DATA RECOVERY TOOLS

The following are the data recovery tools for various operating systems:

1. **Recuva (Windows)**
2. **PhotoRec (Windows / Mac / Linux)**
3. **Puran File Recovery (Windows)**
4. **Pandora Recovery (Windows)**
5. **Glary Undelete (Windows)**
6. **SoftPerfect File Recovery (Windows)**
7. **Tokiwa Data Recovery (Windows)**
8. **Exif Untrasher (Mac OS X)**
9. **PC INSPECTOR File Recovery (Windows)**
10. **Wise Data Recovery (Windows)**
11. **UndeleteMyFiles Pro (Windows)**
12. **TestDisk (Windows / Mac / Linux)**
13. **Disk Drill (Windows)**
14. **Undelete360 (Windows)**
15. **CD Recovery Toolbox Free (Windows)**
16. **FreeUndelete (Windows)**
17. **ADRC Data Recovery (Windows)**
18. **Lazesoft Recovery Suite Home (Windows)**
19. **WinHex (Windows)**
20. **Paragon Rescue Kit Free (Windows)**

5.9 DATA RECOVERY PROCESS

Step 1 – Evaluation: The first step is to correctly diagnose the problem. This is a critical stage, because if the drive is handled incorrectly the chances of performing a successful data recovery are lessened. If you brought in a computer, laptop or external drive (including NAS or Apple Time Capsule etc) the hard drive is removed by opening the external enclosure; and then it is hooked up to specialized recovery equipment to diagnose the damaged components. At the end of this stage, the recovery level is determined, and this tells you the flat rate and time needed to recover your data.

Step 2 – Recovery: Once you approve the recovery level, we take the necessary steps to recover your data. If the drive failed mechanically Level 3 it is opened in a controlled environment called a clean-room (or class 100 environment) which is needed so that when your drive lid is opened, contaminants like dust and moisture cannot damage the drive platter permanently.

STEP ONE

Evaluation

Remove Drive from Device

Diagnose failure

Determine Level – 1,2 or 3

Notify Client of Results

STEP TWO

Recovery

Clone Hard Drive (L1-L2)

Clean-Room Service (L3)

Check / Repair Logical Errors

Create Recovery Image

STEP THREE

Extraction

Test Clients External Drive

Extract Recovery Image

Check File Structure

Notify Client of Pickup

CHAPTER 6

6.1 THE ETHICS OF COMPUTER-BASED ELECTRONIC EVIDENCE RECOVERY

Technology is present in every aspect of modern life. Information Technology is constantly growing & every new development gets a larger role in our lives. Criminals are exploiting the same technological advances which are driving forward the evolution of society.

Computers can be used in the commission of crime, they can contain evidence of crime and can even be targets of crime. Understanding the role and nature of electronic evidence that might be found, how to process a crime scene containing potential electronic evidence and how an agency might respond to such situations is crucial. It cannot be over emphasized that the rules of evidence apply equally to computer-based electronic evidence as much as they do to material obtained from other sources. It is always the responsibility of the case officer to ensure compliance with legislation and, in particular, to be sure that the procedures adopted in the seizure of any property are performed in accordance with statute and current case law.

Electronic evidence is valuable evidence and it should be treated in the same manner as traditional forensic evidence with respect and care. The recovery of evidence from electronic devices like computers, tapes, CD/ DVD, flash drives, is now firmly part of investigative activity in both public and private sector domains. The methods of recovering electronic evidence, whilst maintaining evidential continuity and integrity may seem complex and costly, but experience has shown that, if dealt with correctly, it will produce evidence that is both compelling and cost effective.

Computer-based electronic evidence is information and data of investigative value that is stored on or transmitted by a computer. As such, this evidence is latent evidence in the same sense that fingerprints or DNA (deoxyribonucleic acid) evidence is latent. Computer-based electronic evidence is very delicate. It can be easily altered, damaged, or destroyed if not handled properly or by improper examination, For this reason special precautions are taken to document, collect, preserve and examine this type of evidence. Failure to do so may make it unusable or lead to an inaccurate conclusion.

In its natural state, we cannot see what is contained in the physical object that holds our evidence. Equipment and software are required to make the evidence available. Testimony may be required to explain the examination and any process limitations.

FOUR PRINCIPLES ARE INVOLVED ELECTRONIC DATA EVIDENCE:

Principle 1:

No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

Principle 2:

In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3:

An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4:

The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

Explanation of the principles

Computer-based electronic evidence is subject to the same rules and laws that apply to documentary evidence. The principle of documentary evidence may be explained thus: the responsibility is on the prosecution to show to the court that the evidence produced is as it is since the first possession of police.

Sometimes Operating systems and other programs alter and add to the contents of electronic storage automatically even user may not aware of changes being made by such programs. Wherever practicable, an image should be made of the entire target device. If creating image of incomplete or selective file which is considered as an alternative in certain circumstances, investigators should be careful to ensure that all relevant evidence is captured.

In a some cases, it may not be possible to get an image using a recognized imaging device. In these conditions, its necessary to access original machine to recover the evidence. While doing this it is important that a witness, who is able to give evidence to a court of law makes any such access.

It is essential to display objectivity in a court, as well as the continuity and integrity of evidence. It is also necessary to demonstrate how evidence has been recovered, showing each process through which the evidence was obtained. Evidence should be preserved to such an extent that a third party is able to repeat the same process and arrive at the same result as that presented to a court.

6.2 Time-Frame Analysis

In situations where an individual is suspected of using a certain computer, time-frame analysis can contribute to associating the events that occurred on the computer with that individual.

Time-frame analysis can be performed using two methods:

1. The first involves reviewing the time stamps and date stamps that are found in the file system metadata (for example, when the files were last modified, last accessed, created, or changed status). These clues might provide useful details to further the investigation. An example of this analysis would be using the last modified date and time to establish when the contents of a file were last changed.

2. The second method involves reviewing the application logs that are found (the logs may include the error logs, installation logs, connection logs, and security logs). For example, examination of a security log may indicate when a user name/password combination was used to log in to a system.

Timeline Analysis

Timeline analysis is useful for a variety of investigation types and is often used to answer questions about when a computer is used or what events occurred before or after a given event. Autopsy contains an advanced timeline interface that was built with funding from DHS S&T. It pulls timestamp info from the following places:

- Files
- Web artifacts
- Other Autopsy extracted data, such as EXIF and GPS

It has two display modes. The first is a bar chart that answers questions about how much data occurred in a given time frame. This interface is less about details of what occurred, but rather how much occurred.

The following example gives the detail description of file creation from various sources of data, analysis and disseminate.

Prepare

The scope of the request determines the data to be collected, such as within a specific timeframe, and data of relevance such as specific documents, pictures or video. Can be from multiple computers, other digital data holdings, or other information sources.

Collect the relevant source files;

1. Event Logs
* Vista - windows\system32\winevt\logs*.evtx
* XP - windows\system32\config*.evt
Encase; run the event log parser script to export to csv
Event Log Explorer: allows you to view, merge, and export event logs with associated data descriptions

2. MFT/FAT Filetime Data (MACe)

* data for relevent files; inc. Modified, last Access, Created, MFT Entry modified

Encase: select items of interest and export data to csv or FTK Imager, FTK, X-Ways, ProDiscover, TSK, etc

3. Registry Files * C:\windows\system32\config\sam, system, software,

* C:\~username~\ntuser.dat security

- use Access Data Registry Viewer or RegRipper predefined reports to extract keys of interest, such as TypedURL, User account creation dates, etc.

- Manually enter data into a spreadsheet

4. Internet History

* index.dat files such as; ~username~\AppData\local\Microsoft\Windows\History\History.IE5\index.dat

* also Registry TypedURLs (date is for Key not URL)

Encase: Run the Search for Internet records and export

Mandiant Web Historian

MiTeC Windows File Analyzer / Pasco

5. Email Files

* eg Outlook dbx/pst files; EML Windows Mail files

Encase: Run the Search for Email records and export

ABC Amber Outlook

6. Recycle Bin\Recycler

* located in; C:\$recycler, C:\$Recycle.Bin, etc

Encase; sort by File Deleted date column and also export entries in Recycle folders (can be done at same time as Filetime Data (MACe))

MiTeC Windows File Analyzer: browse to folder with extracted INFO2 file and export report

7. thumbs.db

* thumbs.db files in folders with pictures

Encase: thumbs parser / view file structure

MiTeC Windows File Analyzer

8. Archive Files

* zip, rar, tar, etc files

Encase: view file structure

Izarc; File, Print File List to Text File

9. Link Files

*.lnk files

Encase script to parse link file data

MiTeC Windows File Analyzer

10. Prefetch

* located in; C:\Windows\Prefetch\

MiTEC Windows File Analyzer: exe, time, number

11. Logs

* look for log files from software, such as MSN Logs, AV scanners, CCleaner, Eraser, etc

* use Prefetch / Registry info to determine what software has been used and where log files may be

12. Restore Points

* located in; C:\ System Volume Information\

* also includes previous Registry Files in the RP folders

13. Documents/Spreadsheets/PDF metadata

* extract documents and metadata from documentsv * there may be information contained within the documents that will have to be manually entered into a spreadsheet, such as resume, financial transactions, etc

14. Chat Logs

* Internet Chat Logs MSN, Yahoo, etc

15. JPG Exif

*.jpg files which hold EXIF data

BR's EXIFextracter - extract EXIF data into a csv

* ALSO Information from photos, such as suspect photographed on holiday with date/time information (manually enter)

16. Phones

* Data extracted from mobile phones, such as; calls made and received, SMS, Photos, Video, etc

* use .XRY or Cellebrite to export to csv

17. Internet / Network Capture Files

* information from internet sources, such as dates of web site page creation or modification, wincap files

18. CCTV

* footage from CCTV showing activity of note

19. Financial Information

* information gleaned from spreadsheets or PDF files such as bank statements, or other external sources

20. Other Sources of information

* add any other source you have data for

Collate

For each source of data;

* Export / convert data to csv format
* Open csv in OpenOffice Spreadsheet / MS Excel
* Add columns for itemnumber, principaldate, realtime, source, comment
* Check time columns for accuracy and whether data is in UTC, Windows Filetime, Unix, or localtime
* if necessary use the realtime column to convert time columns to the correct localtime. This may entail calculating timezone offset for UTC, determining whether daylight savings (DST) was in effect, and how the OS is calculating dates/times around DST change
* sort by date columns, and highlight dates of interest
* you may need to do multiple sort and highlight processes for spreadsheets with multiple date columns (such as Filetime Data MACe spreadsheets)
* Copy highlighted dates to the principaldate column
* add data to the source column, such as AppEventLog
* add any comments to the comments column
* copy highlighted rows to a master timeline spreadsheet
* change font colour to color-code different source data

Do this for each source of data, adding selected data rows to a single master timeline spreadsheet

Analyse

* Sort by the principaldate column
* take some time to THINK about what is occuring
* add comments where relevant
* refine the data to what is relevant and remove rows which do not contribute information to the process
* copy the important information to a final spreadsheet

Disseminate

* refine the presentation spreadsheet to enable ease of reading and decide how best to present your findings; i2, spreadsheet, written report, etc

6.3 Digital Investigations and Evidence

A *digital investigation* is a process where we develop and test hypotheses that answer questions about digital events. This is done using the scientific method where we develop a hypothesis using evidence that we find and then test the hypothesis by looking for additional evidence that shows the hypothesis is impossible. *Digital evidence* is a digital object that contains reliable information that supports or refutes a hypothesis.

Consider a server that has been compromised. We start an investigation to determine how it occurred and who did it. During the investigation, we find data that were created by events related to the incident. We recover deleted log entries from the server, find attack tools, and find numerous vulnerabilities that existed on the server. Using this data, and more, we develop hypotheses about which vulnerability the attacker used to gain access and what she did afterwards. Later, we examine the firewall configuration and logs and determine that some of the scenarios in our hypotheses are impossible because that type of network traffic could not have existed, and we do not find the necessary log entries. Therefore, we have found evidence that refutes one or more hypotheses.

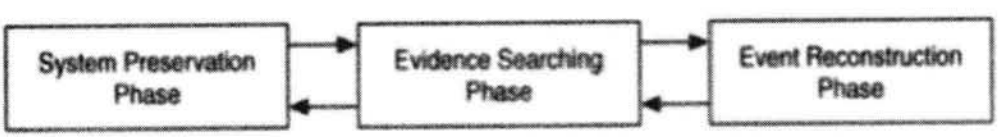
A *digital forensic investigation* is a process that uses science and technology to analyze digital objects and that develops and tests theories, which can be entered into a court of law, to answer questions about events that occurred. In other words, a digital forensic investigation is a more restricted form of digital investigation.

6.4 Digital Crime Scene Investigation Process

There is no single way to conduct an investigation. If you ask five people to find the person who drank the last cup of coffee without starting a new pot, you will probably see five different approaches. One person may dust the pot for fingerprints, another may ask for security camera tapes of the break room, and another may look for the person with the hottest cup of coffee. As long as we find the right person and do not break any laws in the process, it does not matter which process is used, although some are more efficient than others.

The approach used for a digital investigation is based on the physical crime sceneinvestigation process. In this case, we have a digital crime scene that includes the digital environment created by software and hardware. The process has three major phases, which are system preservation, evidence searching, and event reconstruction. These phases do not need to occur one after another, and the flow is shown in Figure 6.1.

Figure 6.1. The three major phases of a digital crime scene investigation.



This process can be used when investigating both live and dead systems. A *live analysis* occurs when you use the operating system or other resources of the system being investigated to find evidence. A *dead analysis* occurs when you are running trusted applications in a trusted operating system to find evidence. With a live analysis, you risk getting false information because the software could maliciously hide or falsify data. A dead analysis is more ideal, but is not possible in all circumstances.

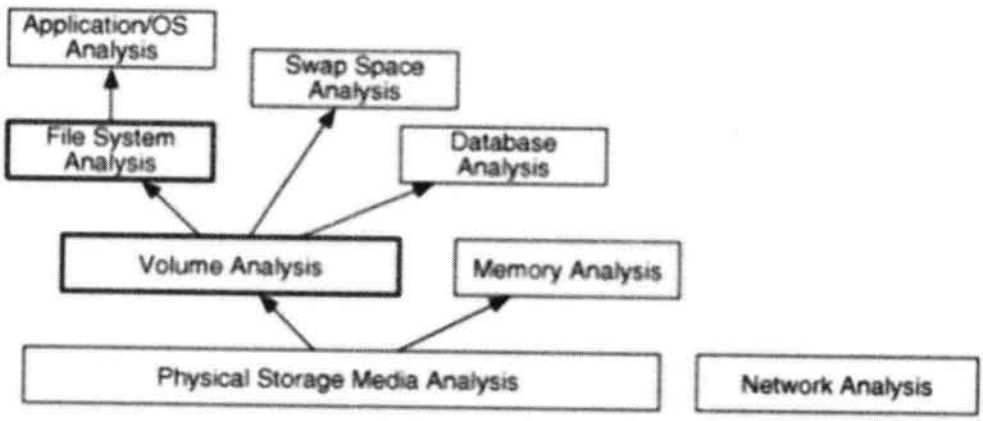
Data Analysis and Types

When analyzing digital data, we are looking at an object that has been designed by people. Further, the storage systems of most digital devices have been designed to be scalable and flexible, and they have a layered design. The following layered design to define the different analysis types.

If we start at the bottom of the design layers, there are two independent analysis areas. One is based on storage devices and the other is based on communication devices. This book is going to focus on the analysis of storage devices, specifically non-volatile devices, such as hard disks. The analysis of communication systems, such as IP networks, is not covered in this book,

Figure 6.2 shows the different analysis areas. The bottom layer is Physical Storage Media Analysis and involves the analysis of the physical storage medium. Examples of physical store mediums include hard disks, memory chips, and CD-ROMs. Analysis of this area might involve reading magnetic data from in between tracks or other techniques that require a clean room. For this book, we are going to assume that we have a reliable method of reading data from the physical storage medium and so we have a stream 1s and 0s that were previously written to the storage device.

Figure 6.2. Layers of analysis based on the design of digital data.



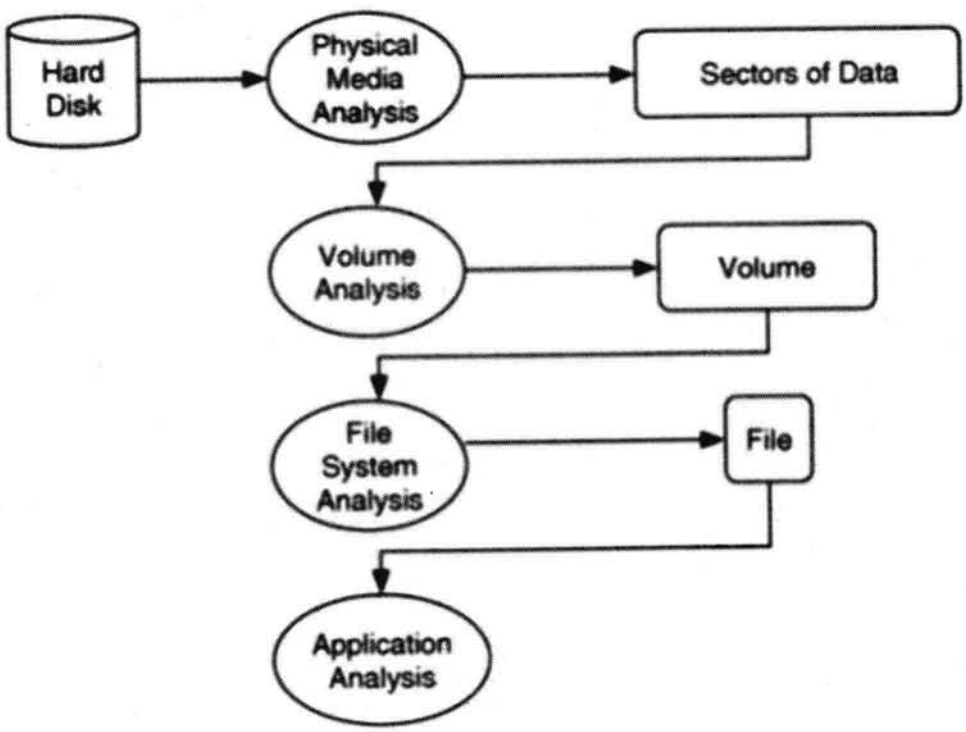
We now analyze the 1s and 0s from the physical medium. Memory is typically organized by processes and is out of the scope of this book. We will focus on non-volatile storage, such as hard disks and flash cards. Storage devices that are used for non-volatile storage are typically organized into volumes. A *volume* is a collection of storage locations that a user or application can write to and read from. There are two major concepts in this layer. One is partitioning, where we divide a single volume into multiple smaller volumes, and the other is assembly, where we combine multiple volumes into one larger volume, which may later be partitioned. Examples of this category include DOS partition tables, Apple partitions, and RAID arrays. Some media, such as floppy disks, do not have any data in this layer, and the entire disk is a volume. We will need to analyze data at the volume level to determine where the file system or other data are located and to determine where we may find hidden data.

Inside each volume can be any type of data, but the most common contents are file systems. Other volumes may contain a database or be used as a temporary swap space (similar to the Windows pagefile). F*ile systems*, which is a collection of data structures that allow an application to create, read, and write files. We analyze a file system to find files, to recover deleted files, and to find hidden data. The result of file system analysis could be file content, data fragments, and metadata associated with files.

To understand what is inside of a file, we need to jump to the application layer. The structure of each file is based on the application or OS that created the file. For example, from the file system perspective, a Windows registry file is no different from an HTML page because they are both files. Internally, they have very different structures and different tools are needed to analyze each. Application analysis is very important, and it is here where we would analyze configuration files to determine what programs were running or to determine what a JPEG picture is of. I do not discuss application analysis in this book because it requires multiple books of its own to cover in the same detail that file systems and volumes are covered.

We can see the analysis process in Figure 6.3. This shows a disk that is analyzed to produce a stream of bytes, which are analyzed at the volume layer to produce volumes. The volumes are analyzed at the file system layer to produce a file. The file is then analyzed at the application layer.

Figure 6.3. Process of analyzing data at the physical level to the application level.



Essential and Nonessential Data

All data in the layers previously discussed have some structure, but not all structure is necessary for the layer to serve its core purpose. For example, the purpose of the file system layer is to organize an empty volume so that we can store data and later retrieve them. The file system is required to correlate a file name with file content. Therefore, the name is essential and the on-disk location of the file content is essential. We can see this in Figure 6.4 where we have a file named miracle.txt and its content is located at address 345. If either the name or the address were incorrect or missing, then the file content could not be read. For example, if the address were set to 344, then the file would have different content.

Figure6.4. To find and read this file, it is essential for the name, size, and content location to be accurate, but it is not essential for the last accessed time to be accurate.

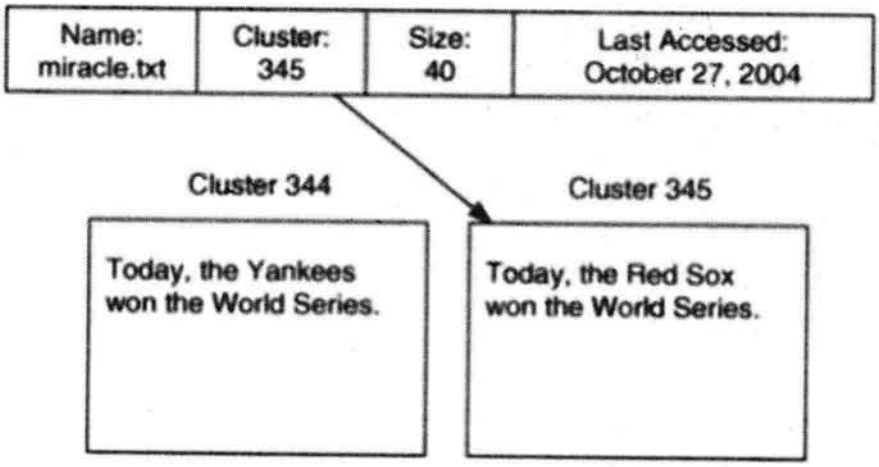


Figure 6.4 also shows that the file has a last accessed time. This value is not essential to the purpose of the file system, and if it were changed, missing, or incorrectly set, it would not affect the process of reading or writing file content.

We can trust that the file content address in a file is accurate because otherwise the person who used the system would not have been able to read the data. The last access time may or may not be accurate. The OS may not have updated it after the last access, the user may have changed the time, or the OS clock could have been off by three hours, and the wrong time was stored. Note that just because we trust the number for the content address does not mean that we trust the actual content at that address. For example, the address value in a deleted file may be accurate, but the data unit could have been reallocated and the content at that address is for a new file. Nonessential data may be correct most of the time, but you should try to find additional data sources to support them when they are used in an incident hypothesis (i.e., the correlation in the PICL guidelines).

6.5 Overview of Toolkits

There are many tools that can help an investigator analyze a digital system. Most tools focus on the preservation and searching phases of the investigation

EnCase by Guidance Software

There are no official numbers on the topic, but it is generally accepted that *EnCase* (http://www.encase.com) is the most widely used computer investigation software. EnCase is Windows-based and can acquire and analyze data using the local or network-based versions of the tool. EnCase can analyze many file system formats, including FAT, NTFS, HFS+, UFS, Ext2/3, Reiser, JFS, CD-ROMs, and DVDs. EnCase also supports Microsoft Windows dynamic disks and AIX LVM.

EnCase allows you to list the files and directories, recover deleted files, conduct keyword searches, view all graphic images, make timelines of file activity, and use hash databases to identify known files. It also has its own scripting language, called EnScript, which allows you to automate many tasks. Add-on modules support the decryption of NTFS encrypted files and allow you to mount the suspect data as though it were a local disk.

Forensic Toolkit by AccessData

The *Forensic Toolkit* (FTK) is Windows-based and can acquire and analyze disk, file system, and application data (http://www.accessdata.com). FTK supports FAT, NTFS, and Ext2/3 file systems, but is best known for its searching abilities and application-level analysis support. FTK creates a sorted index of the words in a file system so that individual searches are much faster. FTK also has many viewers for different file formats and supports many email formats. FTK allows you to view the files and directories in the file system, recover deleted files, conduct keyword searches, view all graphic images, search on various file characteristics, and use hash databases to identify known files. AccessData also has tools for decrypting files and recovering passwords.

ProDiscover by Technology Pathways

ProDiscover (http://www.techpathways.com) is a Windows-based acquisition and analysis tool that comes in both local and network-based versions. ProDiscover can analyze FAT, NTFS, Ext2/3, and UFS file systems and Windows dynamic disks. When searching, it provides the basic options to list the files and directories, recover deleted files, search for keywords, and use hash databases to identify known files. ProDiscover is available with a license that includes the source code so that an investigator or lab can verify the tool's actions.

SMART by ASR Data

SMART (http://www.asrdata.com) is a Linux-based acquisition and analysis tool. Andy Rosen, who was the original developer for Expert Witness (which is now called EnCase), developed SMART. SMART takes advantage of the large number of file systems that Linux supports and can analyze FAT, NTFS, Ext2/3, UFS, HFS+, JFS, Reiser, CD-ROMs, and more. To search for evidence, it allows you to list and filter the files and directories in the image, recover deleted files, conduct keyword searches, view all graphic images, and use hash databases to identify known files.

The Sleuth Kit / Autopsy

The Sleuth Kit (TSK) is a collection of Unix-based command line analysis tools, and Autopsy is a graphical interface for TSK (http://www.sleuthkit.org). The file system tools in TSK are based on *The Coroner's Toolkit* (TCT) (http://www.porcupine.org), which was written by Dan Farmer and Wietse Venema. TSK and Autopsy can analyze FAT, NTFS, Ext2/3, and UFS file systems and can list files and directories, recover deleted files, make timelines of file activity, perform keyword searches, and use hash databases. We will be using TSK throughout this book, and Appendix A, "The Sleuth Kit and Autopsy," provides a description of how it can be used.

6.6 Collecting Evidence

The investigator should collect the following types of evidence:

• *General evidence*: This includes the date and time the investigator visited the incident site and with whom the investigator spoke.

• *Physical and demonstrative evidence*: This includes pictures taken at the incident site. The investigator can demonstrate the evidence using maps, X-rays, diagrams, and floor plans.

• ***Testimonial evidence***: This is oral evidence, presented by a competent eyewitness to the incident, that is relevant and material to the case. It includes testimony from all the persons interviewed by the investigator in order of the date and time of the interview.

Collecting Physical and Demonstrative Evidence

The following information should be collected for physical and demonstrative evidence:

• The manner in which the scene of the incident was secured

• A list of each type of physical evidence that was collected and secured

• The manner in which the physical evidence was collected and logged

• The manner in which the physical evidence was preserved after collection to maintain the chain of custody

• A list of any pictures that were taken

• A list of any demonstrative evidence available to the investigation

Collecting Testimonial Evidence

The following information should be collected for testimonial evidence:

• The manner in which the investigator determined whom to interview

• A list of the persons interviewed in chronological order, including the name, title, date, and time of each interview

• A list of persons who are identified as the targets of the case

• The manner in which the investigator afforded the target or the witnesses any right to representation

Dos and Don'ts of Forensic Computer Investigations

• Ask questions

• Document thoroughly

• Operate in good faith

- Do not get in over your head
- Make the decision to investigate
- Treat everything as confidential
- File everything appropriately

6.7 Case Report Writing and Documentation

All conclusions and findings of computer media analysis should go into an investigative analysis report, which is then directly sent to a case officer.

This report should have the following documents:

- Forms
- Analysis notes
- Items that come as a result of analysis, i.e., printouts and CDs
- Copies of search warrants
- Evidence listing
- Media analysis worksheet
- Keyword lists
- Support requests

Creating a Report to Attach to the Media Analysis Worksheet

An investigator should maintain notes and provide more information on the following to create a report that can be attached to the media analysis worksheet:

- Date and time when any computer taken as evidence
- Current date and time
- Lapses in analysis
- Finding evidence
- Special techniques required that are beyond the normal processes
- Significant problems or broken items
- Outside sources that provide assistance during the investigation

Best Practices for Investigators

Before submitting the final report, an investigator should read it over to see if there are any places where he or she needs to make changes. The report should contain only relevant material. It should also be coherent, not repetitive, and consistently structured. The investigator should also let an outsider read the report. The reportneeds to be understandable to someone who is completely unfamiliar with the case.

Writing a Report Using FTK

To prepare a new case using FTK, perform the following steps:

1. Write-protect the evidence floppy disk.

2. Create a work folder and another folder under this folder.

3. Run FTK.

4. Click **OK**.

5. Select **Start a new case** and click **OK** in the **FTK Startup** dialog box (Figure 6-5).

6. Fill out the appropriate information in the **New Case** dialog box and click **Continue**.

7. Use the **Browse** button to access the case path.

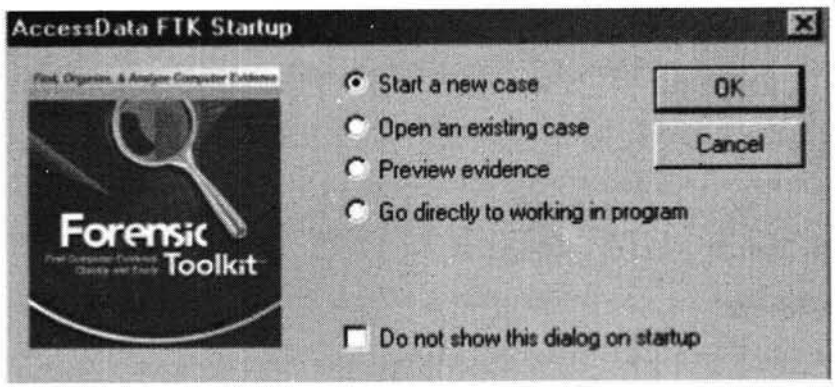


Figure 6-5 Select **Start a new case** in the **FTK Startup** dialog box.

8. Give a brief description of the investigation (Figure 6-6) and click **Next**.

9. Check all the boxes in the **Case Log Options** window (Figure 6-7).

10. Click **Next** in the **Evidence Processing Options** window (Figure 6-8).

11. Click **Next** in the **Refine Case and Refine Index** window.

12. In the **Add Evidence to Case** window (Figure 6-9), click the **Add Evidence** button.

13. The **Add Evidence to Case** dialog box appears. Click the **Local Drive** option and then click **Continue**.

14. Select the **A: drive** option and the **Logical option** button in the **Select Local Drive** dialog box, and click **OK**.

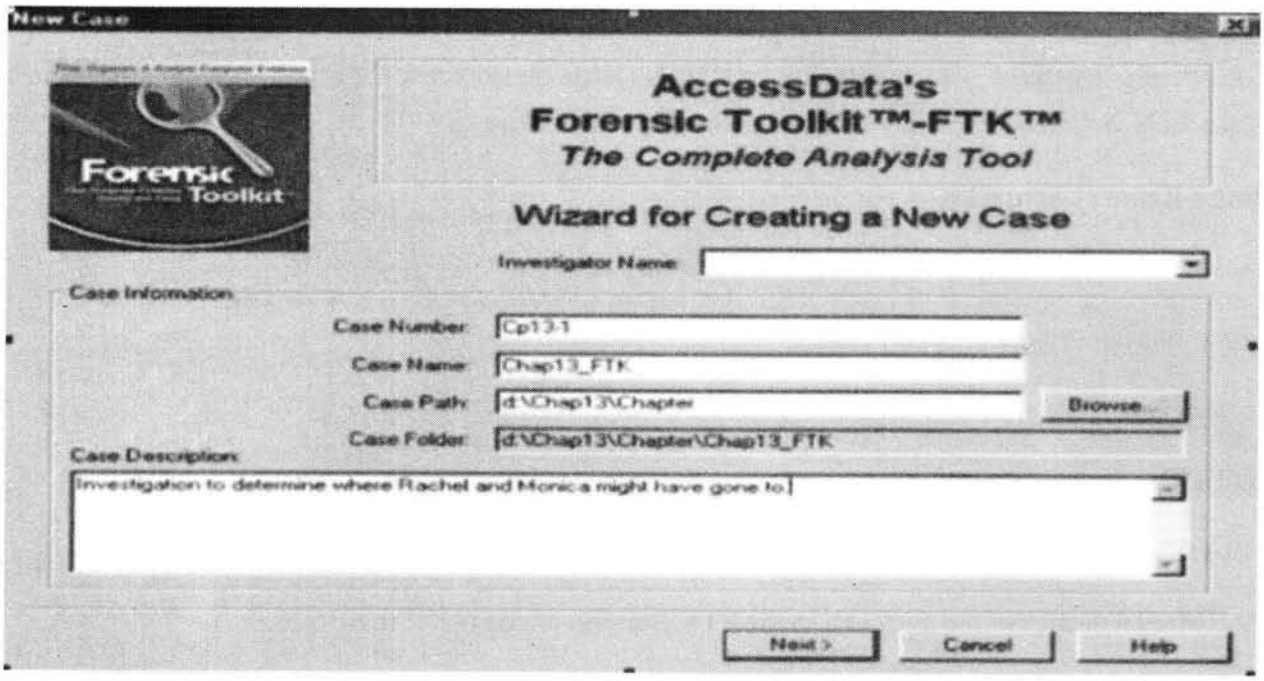


Figure 6-6 The case description should be brief but informative.

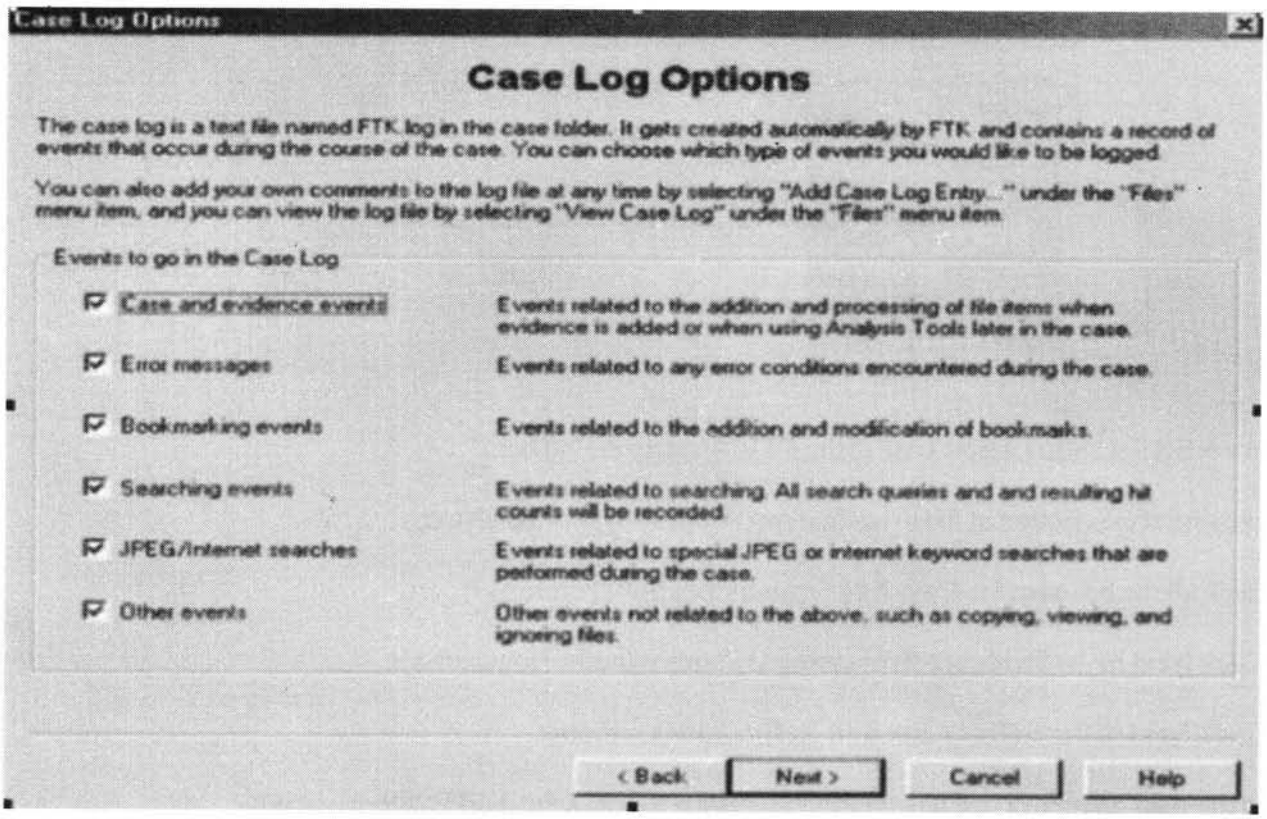


Figure 6-7 The **Case Log Options** window lets a user choose what to include in the case log.

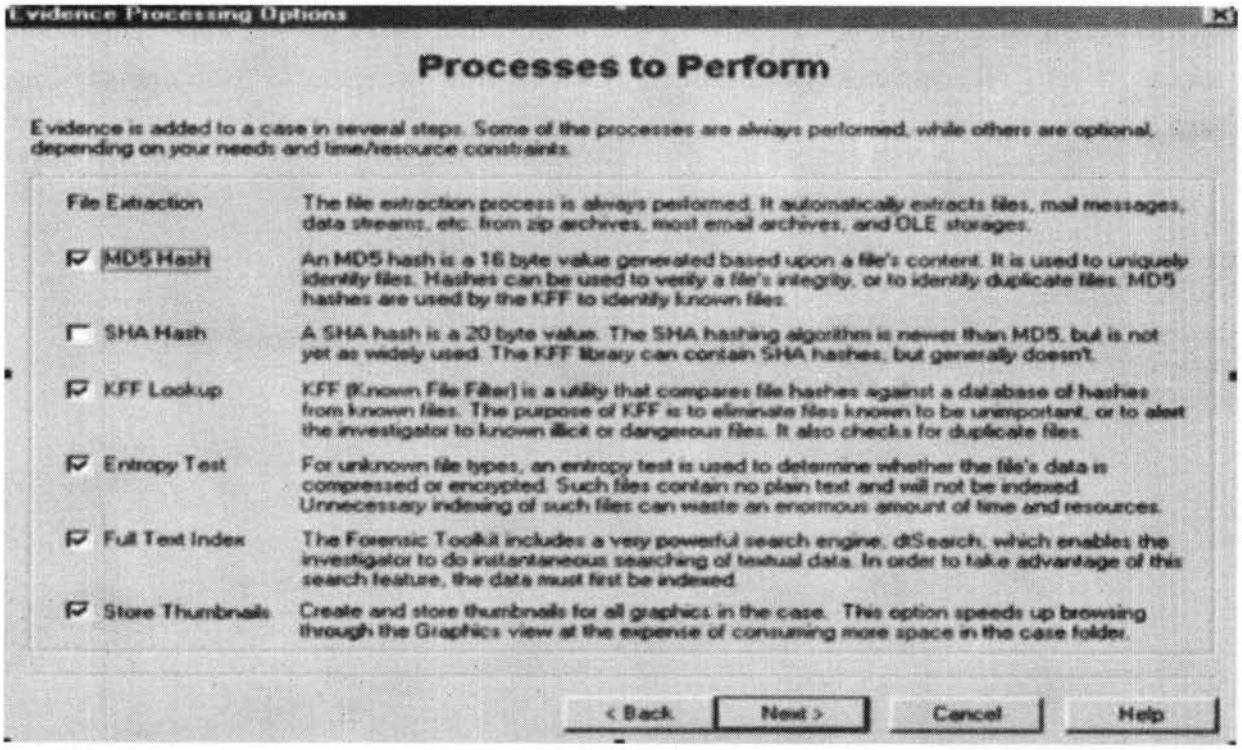


Figure 6-8 The **Evidence Processing Options** window tells FTK which processes to perform on the evidence files.

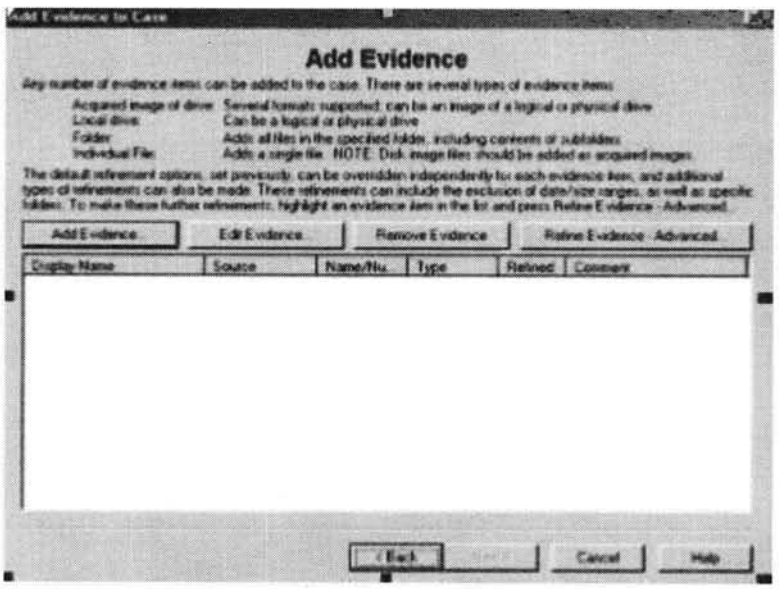


Figure 6-9 Click the **Add Evidence** button to add evidence.

15. Enter comments in the **Evidence Information** window (Figure 6-10) and then click **OK**.

16. Click **Next** in the **Add Evidence** window.

17. Check the information in the **Case Summary** window (Figure 6-11). If it is correct, click **Finish**.

Otherwise, click **Back** to fix any errors.

FTK starts analyzing the data on the investigation floppy disk when the FTK **Processing Files** window (Figure 6-12) appears. When FTK completes the analysis, the main FTK window (Figure 6-13) appears showing all data found from the analysis process.

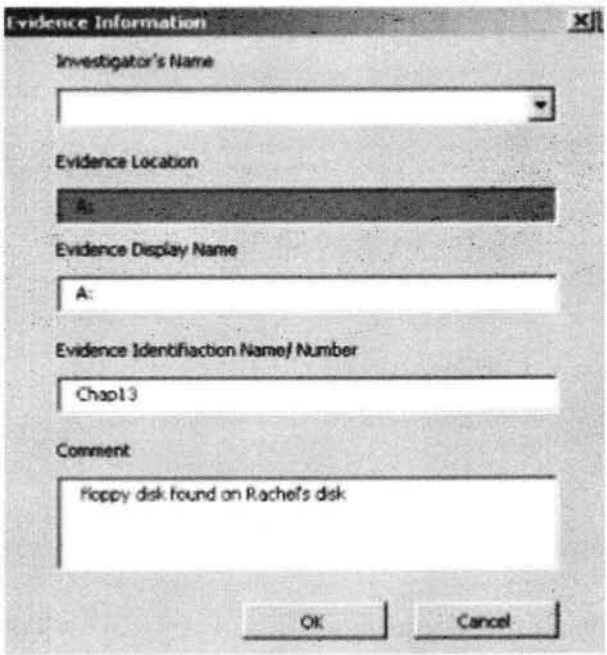


Figure 6-10 Enter a comment that describes the evidence.

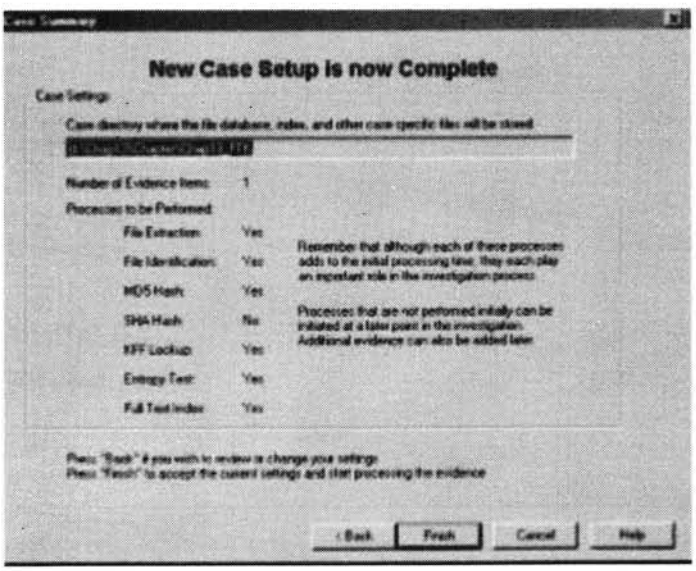


Figure 6-11 Check to make sure that all the information in this window is correct before moving on.

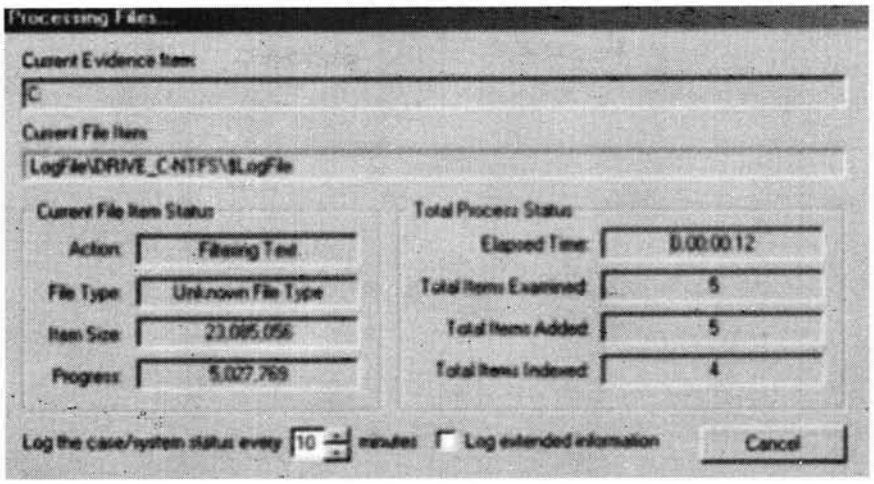


Figure 6-12 This screen shows FTK's progress in processing the evidence files.

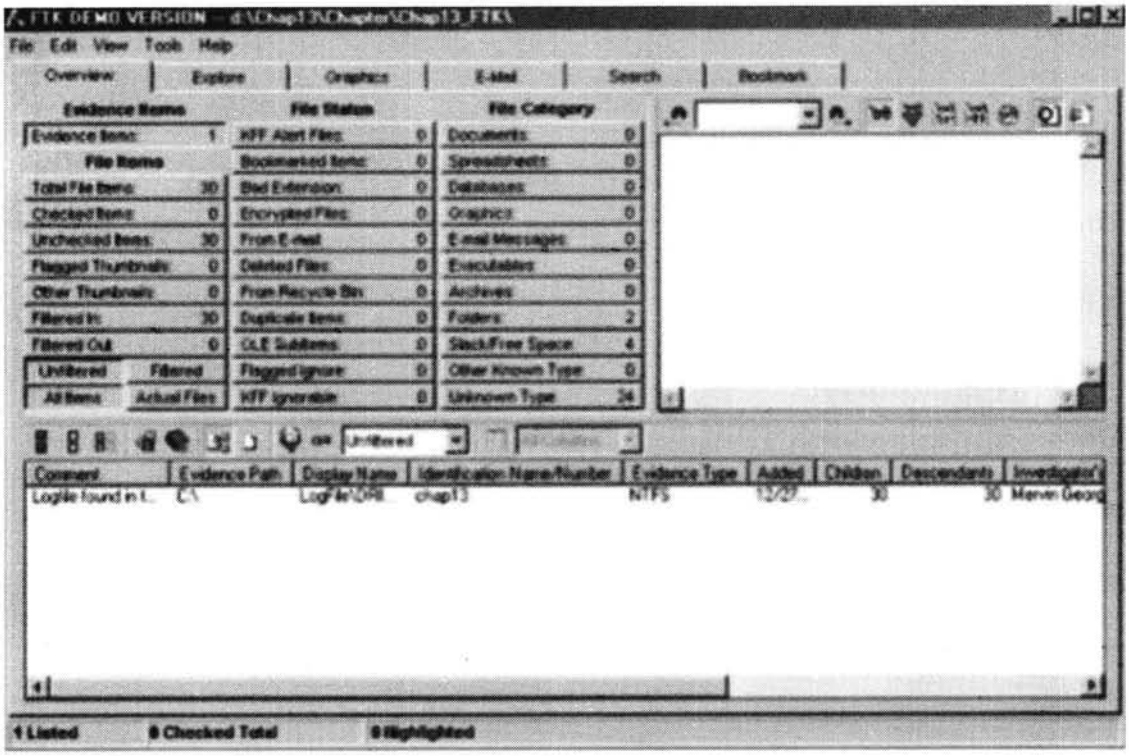


Figure 6-13 The main FTK window shows all of the processed evidence files.

Analyzing with FTK

Perform the following steps to collect pictures with FTK:

1. Click the **Graphics** tab and check the **List all descendants** box.

2. Click any picture in the upper pane and check the box next to its filename.

Locating Encrypted Files with FTK

To locate encrypted files with FTK, click the **Overview** tab, click the **Encrypted Files** button, and click any file in the lower pane.

Viewing Encrypted Files

After locating the encrypted files, perform the following steps to view them:

1. Check the box next to the clicked file.

2. Right-click the file and click **Export File** on the shortcut menu.

3. Uncheck all boxes located at the bottom of the **Export Files** dialog box and click **OK**.

4. Click **OK** in the **Export Files** window message.

Searching with FTK

Perform the following steps to execute an indexed search:

1. Click the **Search** tab.

2. Type the first search term in the **Search Term** field and click **Add**.

3. Then type another search term and click **Add**.

4. Click **View Cumulative Results**.

Perform the following steps to execute a live search:

1. Click the **Live Search** tab in the **Search** pane .

2. Type a keyword and click **Add**. Click **Search**, and then click **OK** in the **Retrieve Search Hits** dialog box.

3. Click **View Results** in the **Live Search Progress** dialog box.

4. To minimize the data, click the **View files in filtered text format** icon .

Creating a Bookmark for Investigation Findings

Perform the following steps to create a bookmark for investigation findings:

1. Right-click any checked file and then click **Create Bookmark** on the shortcut menu.

2. Type **ch13_search_results** in the **Bookmark name** text box. Click **All checked items**, and then check **Include in report** and **Export files** in the **Create New Bookmark** dialog box.

3. To describe the bookmark, type a comment and then click **OK**.

Reviewing Case Findings in FTK

To review case findings in FTK, click the **Overview** tab and then click the **Checked Items** button.

Viewing Selected Items

To view selected items, perform the following steps:

1. Click the first file in the lower pane.

2. The contents of the bookmark can be read by scrolling down the upper-right pane.

3. Type the keyword value in the search text box to locate a specific keyword that is displayed in the upperright pane.

4. To view graphic files, click the **Internet Explorer** icon located above the upper-right pane.

5. To view binary files, click the **HEX** icon.

Running the FTK Report Wizard

1. Go to **File** in the main FTK window and then click **Report Wizard**.

2. Enter the appropriate information in the **Case Information** window. Click **Next**.

. Click **Next** on both the **Bookmarks – A** and **Bookmarks – B** dialog boxes.

4. In the **Graphic Thumbnails** dialog box , check **Export full-size graphics and link them to the thumbnails** and then click **Next**.

5. In the **List by File Path** dialog box , check the **Include a list by file path section in the report** box. Also check the **Include in the report** and **Export to the report** boxes and then click **Next**.

6. In the **Case Audit Files** dialog box, click **Add Files** and navigate to the chap13chapter folder.

7. In the **Open** dialog box, press and hold down the **Ctrl** key to select all the evidence files and then click **Open**.

8. Click **Next** in the **Case Audit Files** dialog box.

Click **Finish** in the **Report Location** dialog box.

10. Click **Yes** to view the report generated. The report opens in Windows Explorer. Double-click Index.html in the chap13chap13_FTKReport folder to view the report in Internet Explorer.

CHAPTER 7

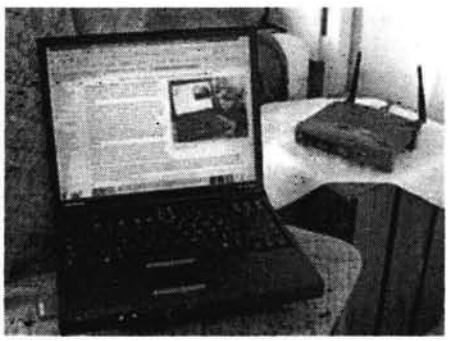
WIRLESS TECHNOLOGIES AND SECURITY

7.1 PERSONAL AREA NETWORK (PAN)

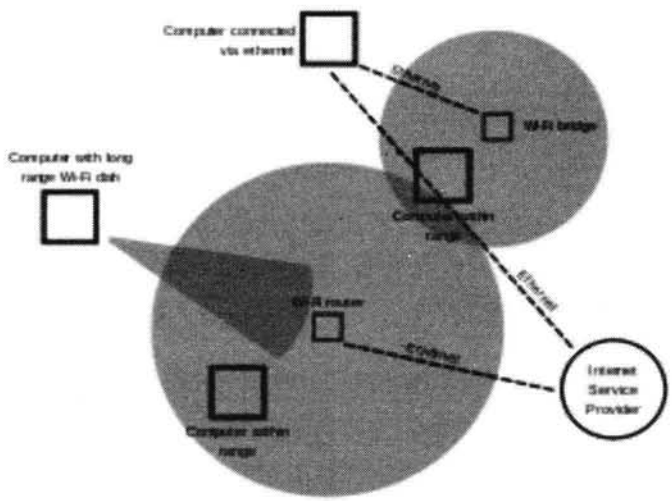
A personal area network (PAN) is the interconnection of information technology devices within the range of an individual person, typically within a range of 10 meters. For example, a person traveling with a laptop, a personal digital assistant (PDA), and a portable printer could interconnect them without having to plug anything in, using some form of wireless technology. Typically, this kind of personal area network could also be interconnected without wires to the Internet or other networks.

Wireless personal area network (WPAN) which is virtually a synonym since almost any personal area network would need to function wirelessly. Conceptually, the difference between a PAN and a wireless LAN is that the former tends to be centered around one person while the latter is a local area network (LAN) that is connected without wires and serving multiple users.

"WLAN" redirects here. For other uses, see WLAN (disambiguation).



This notebook computer is connected to a wireless access point using a PC card wireless card.

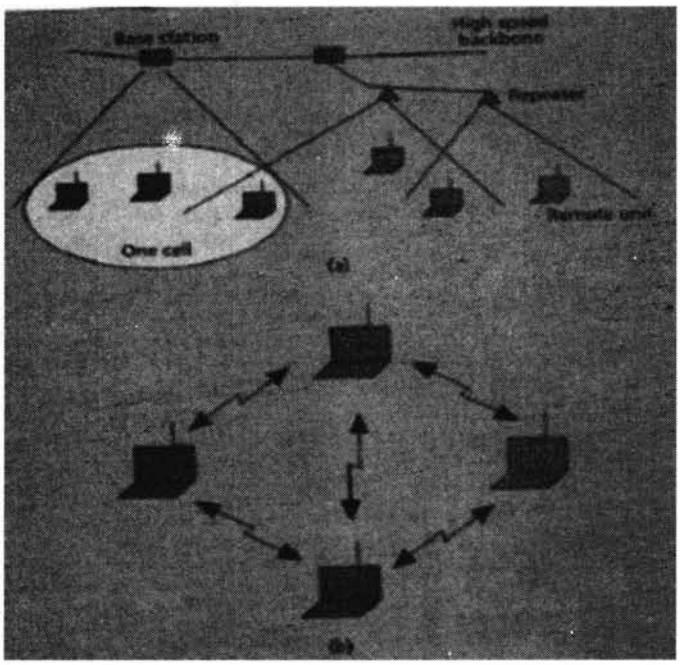


An example of a Wi-Fi network

A **wireless local area network (WLAN)** is a wireless computer network that links two or more devices using a wireless distribution method (often spread-spectrum or OFDM radio) within a limited area such as a home, school, computer laboratory, or office building. This gives users the ability to move around within a local coverage area and yet still be connected to the network. A WLAN can also provide a connection to the wider Internet.

Wireless local area networks (WLANs) are the same as the traditional LAN but they have a wireless interface. With the introduction of small portable devices such as PDAs (personal digital assistants), the WLAN technology is becoming very popular. WLANs provide high speed data communication in small areas such as a building or an office. It allows users to move around in a confined area while they are still connected to the network. Examples of wireless LAN that are available today are NCR's wave LAN and Motorola's ALTAIR.

The Project 802.11 committee distinguished between two types of wireless LAN : "ad-hoc" and "infrastructure"networks.



7.2 TYPES OF WIRELESS NETWORKS

WLANS: Wireless Local Area Networks

WLANS allow users in a local area, such as a university campus or library, to form a network or gain access to the internet. A temporary network can be formed by a small number of users without the need of an access point; given that they do not need access to network resources.

WPANS: Wireless Personal Area Networks

The two current technologies for wireless personal area networks are Infra Red (IR) and Bluetooth (IEEE 802.15). These will allow the connectivity of personal devices within an area of about 30 feet. However, IR requires a direct line of site and the range is less.

WMANS: Wireless Metropolitan Area Networks

This technology allows the connection of multiple networks in a metropolitan area such as different buildings in a city, which can be an alternative or backup to laying copper or fiber cabling.

WWANS: Wireless Wide Area Networks

These types of networks can be maintained over large areas, such as cities or countries, via multiple satellite systems or antenna sites looked after by an ISP. These types of systems are referred to as 2G (2nd Generation) systems.

7.3 COMPARISON OF WIRELESS NETWORK TYPES

Type	Coverage	Performance	Standards	Applications
Wireless PAN	Within reach of a person	Moderate	Wireless PAN Within reach of a person Moderate Bluetooth, IEEE 802.15, and IrDa Cable replacement for peripherals	Cable replacement for peripherals
Wireless LAN	Within a building or campus	High	IEEE 802.11, Wi-Fi, and HiperLAN	Mobile extension of wired networks
Wireless MAN	Within a city	High	Proprietary, IEEE 802.16, and WIMAX	Fixed wireless between homes and businesses and the Internet
Wireless WAN	Worldwide	Low	CDPD and Cellular 2G, 2.5G, and 3G	Mobile access to the Internet from outdoor areas

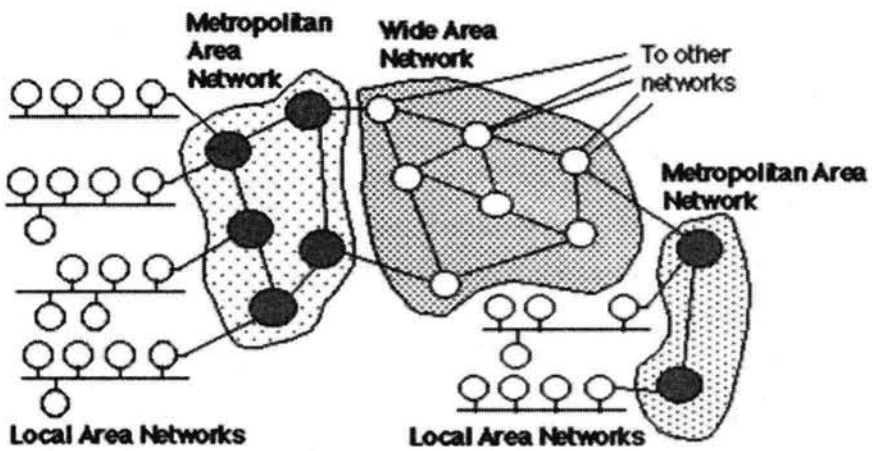
7.4 METROPOLITAN AREA NETWORK (MAN)

A metropolitan area network (MAN) is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN). The term is applied to the interconnection of networks in a city into a single larger network (which may then also offer efficient connection to a wide area network). It is also used to mean the interconnection of several local area networks by bridging them with backbone lines. The latter usage is also sometimes referred to as a campus network.

A Metropolitan Area Network (MAN) is one of a number of types of networks (see also LAN and WAN). A MAN is a relatively new class of network, it serves a role similar to an ISP, but for corporate users with large LANs. There are three important features which discriminate MANs from LANs or WANs:

1. The network size falls intermediate between LANs and WANs. A MAN typically covers an area of between 5 and 50 km diameter. Many MANs cover an area the size of a city, although in some cases MANs may be as small as a group of buildings or as large as the North of Scotland.
2. A MAN (like a WAN) is not generally owned by a single organisation. The MAN, its communications links and equipment are generally owned by either a consortium of users or by a single network provider who sells the service to the users. This level of service provided to each user must therefore be negotiated with the MAN operator, and some performance guarantees are normally specified.
3. A MAN often acts as a high speed network to allow sharing of regional resources (similar to a large LAN). It is also frequently used to provide a shared connection to other networks using a link to a WAN.

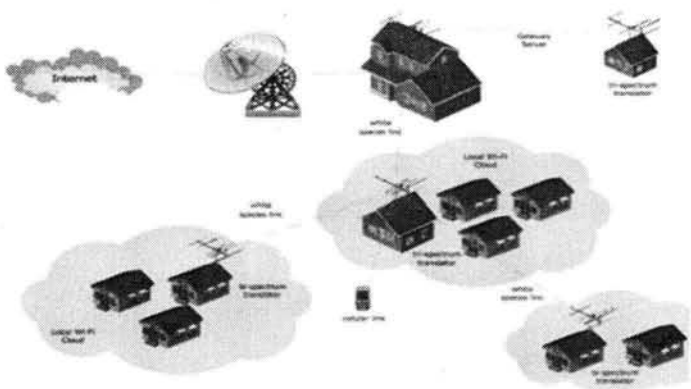
A typical use of MANs to provide shared access to a wide area network is shown in the figure below:



Use of MANs to provide regional networks which share the cost of access to a WAN

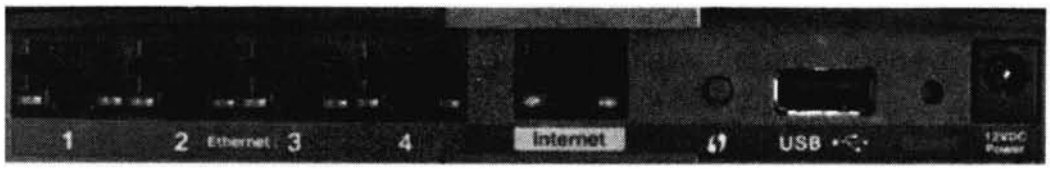
7.5 WAN (wide area network)

A wide area network (WAN) is a geographically distributed private telecommunications network that interconnects multiple local area networks (LANs). In an enterprise, a WAN may consist of connections to a company's headquarters, branch offices, colocation facilities, cloud services and other facilities. Typically, a router or other multifunction device is used to connect a LAN to a WAN. Enterprise WANs allow users to share access to applications, services and other centrally located resources. This eliminates the need to install the same application server, firewall or other resource in multiple locations.



7.6 WAN on home router

On home routers, the port that your home network uses to connect to the Internet is labeled as **WAN**, **Network**, or **Internet**. The picture below is an example of the Internet port on the back of a home router, next to four standard Ethernet ports.



What is the largest WAN in the world?

The Internet is a collection of networks and is considered the largest WAN in the world.

7.7 WIRELESS THREATS

Wireless threats come in all shapes and sizes, from someone attaching to your WAP (Wireless access point) without authorization, to grabbing packets out of the air and decoding them via a packet sniffer. Many wireless users have no idea what kinds of danger they face merely by attaching a WAP to their wired network, the most common threats faced by adding a wireless component to your network.

The airborne nature of WLAN transmission opens your network to intruders and attacks that can come from any direction. WLAN traffic travels over radio waves that the walls of a building cannot completely constrain. Although employees might enjoy working on their laptops from a grassy spot outside the building, intruders and would-be hackers can potentially access the network from the parking lot or across the street using the Pringles can antenna.

- **Bluetooth Attacks**

  Bluetooth technology is growing and being adopted at an amazing rate, surpassing one billion Bluetooth devices shipped in 2006! With increased prevalence in adoption and use comes increased scrutiny from attackers, who have uncovered significant security vulnerabilities in Bluetooth technology. Attacks including unauthorized access, information disclosure, remote eavesdropping, device manipulation and full host compromise are all possible against Bluetooth technology in use today. Due to the ad-hoc and decentralized nature of Bluetooth technology, administrators are often unaware of the amount of Bluetooth technology in use, and their exposure to Bluetooth attacks. While many organizations disregard Bluetooth threats, thinking the technology is limited to short-range communication, the reality is that tests have shown it is possible for an attacker to communicate to a short-range Bluetooth device from over a mile away!

- **PEAP and TTLS Configuration Weaknesses**

Many organizations have turned to stronger authentication protocols such as PEAP and TTLS to authenticate wireless users and protect access to the wireless network. When deploying PEAP and TTLS networks, the configuration of client systems is a critical component of the overall security of the wireless network. Often, PEAP and TTLS networks are poorly configured on client systems, exposing them to network impersonation attacks.

In a network impersonation attack, the adversary adopts the enterprise SSID, and provides enough of a realistic network environment to simulate the legitimate network while attempting to steal network credentials, or to attack client systems directly.

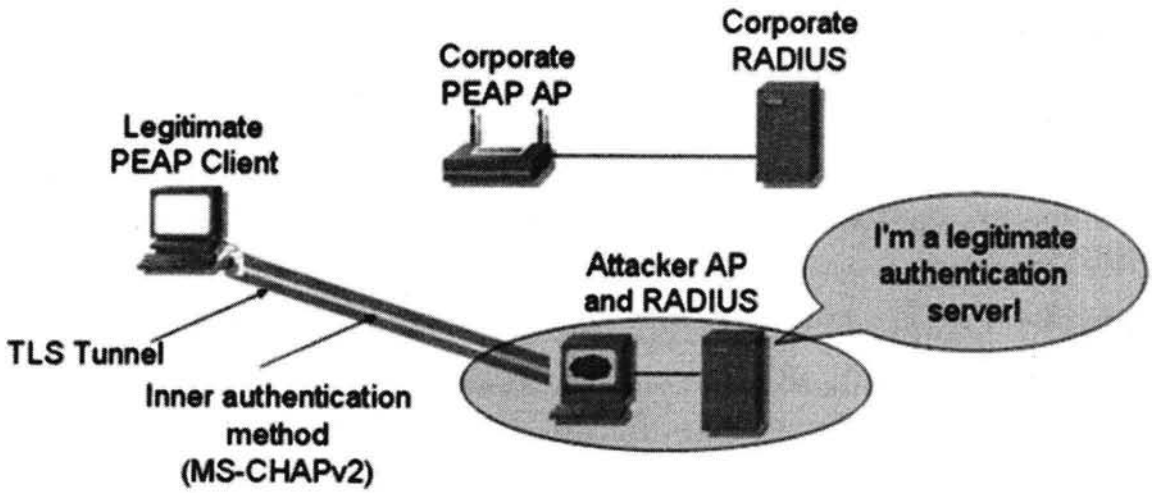


Figure : Attacker impersonates a legitimate AP and RADIUS Server

- **Mobile Device Weaknesses**

Mobile devices such as PDAs, smart-phones, communicators such as the Nokia 800 and even point-of-sale devices, all require wireless connectivity to be effective. Often, these embedded device platforms are well behind what is generally considered to be modern security options for wireless networks, with operating systems that do not receive regular patch updates for application flaws. In many cases, organizations cannot upgrade the operating system or applications on mobile devices until the patches are certified by application vendors, leaving the device vulnerable to attacks for an extended period of time.

Wireless Driver Attacks

The next generation of attacks against wireless networks aren't targeting the wireless network itself; rather, these attacks are targeting client vulnerabilities directly. Exploitable vulnerabilities in wireless drivers have been discovered in all major wireless card manufacturers, with working exploits readily available through tools such as the Metasploit Framework.

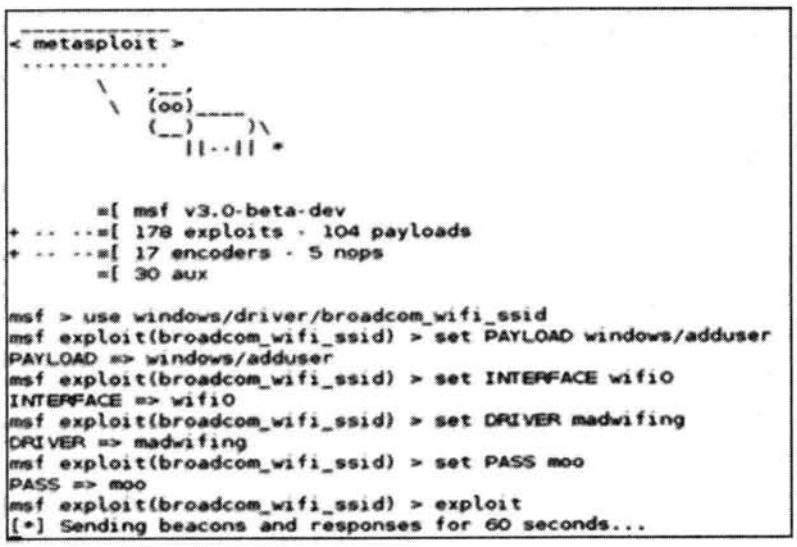


Figure 2: Sample Metasploit attack targeting a flaw in Broadcom wireless drivers

Targeting wireless vulnerabilities, an attacker can exploit vulnerable systems even if the user isn't connected to a wireless network! It's trivial for an attacker to exploit vulnerable systems on an airplane, for example, even when there is no wireless network available. Further, since these attacks exploit deficiencies at layer 2, traditional firewall, HIPS and NAC systems provide little to no defense against these attacks.

The wireless security market has matured significantly in the past several years, but still many organizations remain vulnerable to attacks, either through legacy protocols with well-published deficiencies, or through new threats that are not adequately addressed. In the SANS Institute Assessing and Securing Wireless Networks course.

VULNERABILITIES AND SECURITY

Vulnerability refers to the inability (of a system or a unit) to withstand the effects of a hostile environment. A **window of vulnerability** (WoV) is a time frame within which defensive measures are diminished, compromised or lacking.

In relation to hazards and disasters, vulnerability is a concept that links the relationship that people have with their environment to social forces and institutions and the cultural values that sustain and contest them. "The concept of vulnerability expresses the multi-dimensionality of disasters by focusing attention on the totality of relationships in a given social situation which constitute a condition that, in combination with environmental forces, produces a disaster".It's also the extent to which changes could harm a system, or to which the community can be affected by the impact of a hazard or exposed to the possibility of being attacked or harmed, either physically or emotionally: "we were in a vulnerable position".

7.8 TYPES OF VULNERABILITY

Social vulnerability

In its sense, social vulnerability is one dimension of vulnerability to multiple stressors (agent responsible for stress) and shocks, including abuse, social exclusion and natural hazards. Social vulnerability refers to the inability of people, organizations, and societies to withstand adverse impacts from multiple stressors to which they are exposed. These impacts are due in part to characteristics inherent in social interactions, institutions, and systems of cultural values.

Cognitive vulnerability

A cognitive vulnerability, in cognitive psychology, is an erroneous belief, cognitive bias, or pattern of thought that is believed to predispose the individual to psychological problems.It is in place before the symptoms of psychological disorders start to appear, such as high neuroticism,and after the individual encounters a stressful experience, the cognitive vulnerability shapes a maladaptive response that may lead to a psychological disorder.Inpsychopathology, cognitive vulnerability is constructed from schema models, hopelessness models, and attachment theory. Attentional bias is one mechanism leading to faulty cognitive bias that leads to cognitive vulnerability. Allocating a danger level to a threat depends on the urgency or intensity of the threshold. Anxiety is not associated with selective orientation.

Military

In military terminology, vulnerability is a subset of survivability, the others being susceptibility and recoverability. Vulnerability is defined in various ways depending on the nation and service arm concerned, but in general it refers to the near-instantaneous effects of a weapon attack. In aviation it is defined as the inability of an aircraft to withstand the damage caused by the man-made hostile environment. In some definitions, recoverability (damage control, firefighting, restoration of capability) is included in vulnerability. Some military services develop their own concept of vulnerability.

Invulnerability

Invulnerability is a common feature found in video games. It makes the player impervious to pain, damage or loss of health. It can be found in the form of "power-ups" or cheats; when activated via cheats, it is often referred to as "god mode". Generally, it does not protect the player from certain instant-death hazards, most notably "bottomless" pits from which, even if the player were to survive the fall, they would be unable to escape. As a rule, invulnerability granted by power-ups is temporary, and wears off after a set amount of time, while invulnerability cheats, once activated, remain in effect until deactivated, or the end of the level is reached. Depending on the game in question, invulnerability to damage may or may not protect the player from non-damage effects, such as being immobilized or sent flying.

7.9 SECURITY

Security is the degree of resistance to, or protection from, harm. It applies to any vulnerable and/or valuable asset, such as a person, dwelling, community, item, nation, or organization. As noted by the Institute for Security and Open Methodologies (ISECOM) in the OSSTMM 3, security provides "a form of protection where a separation is created between the assets and the threat." These separations are generically called "controls," and sometimes include changes to the asset or the threat.

Security, in information technology (IT), is the defense of digital information and IT assets against internal and external, malicious and accidental threats. This defense includes detection, prevention and response to threats through the use of security policies, software tools and IT services.

Security is critical for enterprises and organizations of all sizes and in all industries. Weak security can result in compromised systems or data, either by a malicious threat actor or an unintentional internal threat. Not meeting security standards that are regulated by a separate organization or law, such as PCI DSS 3.0 or HIPAA compliance, can also result in financial penalties.

Physical security

Physical security is the protection of personnel, hardware, software, networks and data from physical actions, intrusions and other events that could damage an organization. This includes natural disasters, fire, theft and terrorism, among others. Physical security for enterprises often includes employee access control to the office buildings as well as specific locations, such as data centers. An example of a common physical security threat is an attacker gaining entry to an organization and using a USB storage drive to either copy and remove sensitive data or physically deliver malware directly to systems. Threats to physical security may require less technical savvy on the part of the attacker, but physical security is just as important as information security.

Information security

Information security, also called infosec, encompasses a broad set of strategies for managing the process, tools and policies that aim to prevent, detect and respond to threats to both digital and non digital information assets. Infosec includes several specialized categories, including:

- **Application security** - the protection of applications from threats that seek to manipulate application and access, steal, modify or delete data. These protections use software, hardware and policies, and are sometimes called countermeasures. Common countermeasures include application firewalls, encryption programs, patch management and biometric authentication systems.

Cloud security - the set of policies and technologies designed to protect data and infrastructure involved in a cloud computing environment. The top concerns that cloud security looks to address are identity and access management, and data privacy.

Endpoint security - the part of network security that requires network devices nodes to meet certain security standards before they can connect to a secure network. Nodes devices include PCs, laptops, smartphones and tablets. Endpoint security also extends to equipment like point-of-sale (POS) terminals, bar code readers and IoT devices.

Internet security -the protection of software applications, web browsers and virtual private networks (VPNs) that use the internet. Using techniques such as encryption and internet security aim to defend the transfer of data from attacks like malware and phishing as well as denial-of-service (DoS) attacks.

Mobile security - the protection of portable devices, such as smartphones, tablets and laptops. Mobile security, also known as wireless security, secures the devices and the networks they connect to in order to prevent theft, data leakage and malware attacks.

Network security - the protection of a network infrastructure and the devices connected to it through technologies, policies and practices. Network security defends against threats such as unauthorized access, and malicious use and modifications.

7.10 SECURITY CONCEPTS AND PRINCIPLES

Security in IT is a broad concept that blankets many different ideas and principles. Some of the most important security concepts and principles are:

Defense in depth - a strategy that uses multiple countermeasures to protect information and is based on the military principle that it's more difficult for an enemy to beat a multilayered defense system than it is to beat a single layer.

Least privilege - a principle that limits user and program access to the lowest possible level of access rights in order to strengthen security.

Vulnerability management - an approach to security that requires checking for vulnerabilities, identifying them, verifying them, mitigating them and patching the vulnerabilities.

Risk management - the process of identifying, assessing and controlling risks to an organization's IT environment.

Patch management - an area of systems management that involves acquiring, testing and installing patches and updates for flawed code in applications, operating systems and firmware.

Application lifecycle management-the concept of protecting all stages of the development of an application to reduce its exposure to bugs, design flaws and configuration errors, such as not changing default passwords that could be exploited by attackers.

While there are many other concepts and principles that make up security, these are some of the most important. The combination of all of these principles will not guarantee security for an organization, but it puts the organization in a better position to defend itself from infosec threats.

7.11 WARDRIVING

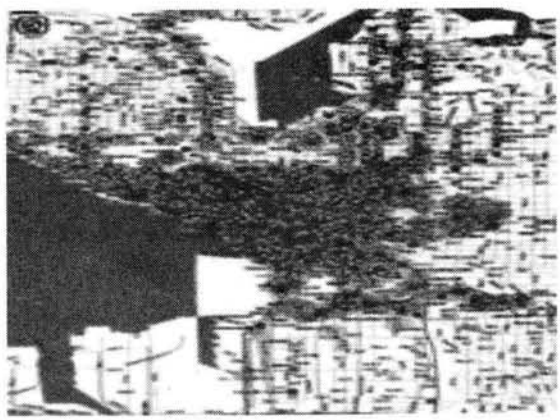
War driving is the act of searching for Wi-Fiwireless networks by a person in a moving vehicle, using a laptop or smartphone. Software for war driving is freely available on the Internet.

War biking or **war cycling** is similar to war driving, but is done from a moving bicycle or motorcycle. This practice is sometimes facilitated by mounting a Wi-Fi enabled device on the vehicle. **War walking**, or war jogging, is similar to war driving, but is done on foot rather than from a moving vehicle. War railing, or war training, is similar to war driving, but is done on a train or tram. War droning is accomplished with a drone.

7.12 WAR DRIVING (ACCESS POINT MAPPING)

The term war driving is derived from the "war-dialing" exploits of the teenage hacker character in the 1983 movie Wargames who has his computer randomly dial hundreds of numbers and eventually winds up tapping into a nuclear command and control system.

War driving, also called access point mapping, is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. To do war driving, you need a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a wireless LAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources.



7.13 WARCHALKING (WAR CHALKING)

War chalking is the drawing of symbols in public places to advertise an open Wi-Finetwork. Inspired by hobo symbols, the war chalking marks were conceived by a group of friends in June 2002 and publicized by Matt Jones who designed the set of icons and produced a downloadable document containing them. Within days of Jones publishing a blog entry about war chalking, articles appeared in dozens of publications and stories appeared on several major television news programs around the world.

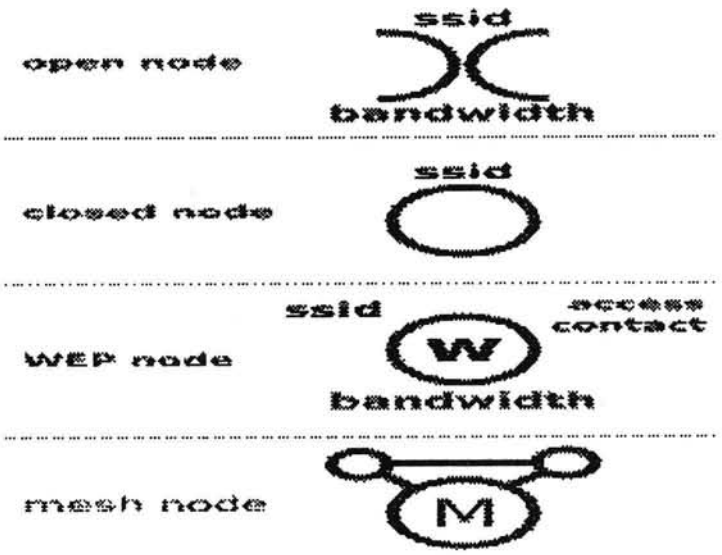
The word is formed by analogy to *war driving*, the practice of driving around an area in a car to detect open Wi-Fi nodes. That term in turn is based on *war dialing*, the practice of dialing many phone numbers hoping to find a modem.

Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object, such as a wall, the pavement, or a lamp post. Those offering Wi-Fi service might also draw such a symbol to advertise the availability of their Wi-Fi location, whether commercial or personal.

War chalking is the drawing of symbols in public places to advertise an open Wi-Finetwork. Inspired by hobo symbols, the war chalking marks were conceived by a group of friends in June 2002 and publicized by Matt Jones who designed the set of icons and produced a downloadable document containing them.[1][2] Within days of Jones publishing a blog entry about war chalking, articles appeared in dozens of publications and stories appeared on several major television news programs around the world.

The word is formed by analogy to *war driving*, the practice of driving around an area in a car to detect open Wi-Fi nodes. That term in turn is based on *war dialing*, the practice of dialing many phone numbers hoping to find a modem.[3]

Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object, such as a wall, the pavement, or a lamp post. Those offering Wi-Fi service might also draw such a symbol to advertise the availability of their Wi-Fi location, whether commercial or personal.



7.14 WARFLYING

War flying or **war storming** is an activity consisting of using an airplane and a Wi-Fi-equipped computer, such as a laptop or a PDA, to detect Wi-Fiwireless networks. War storming shares similarities to War driving and War walking in all aspects except for the method of transport.

It originated in Western Australia with the WaFreeNet (WAFN) group taking up a Grumman Tiger four-seater near Perth City in 2002, as documented on the weblog of Jason Jordan

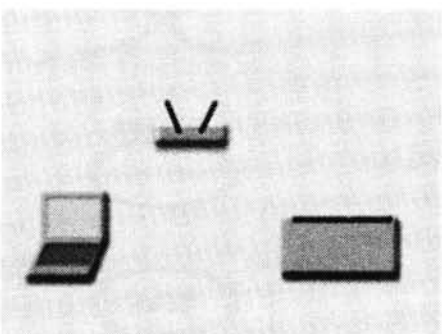
Most war flying is harmless, as most of the people will just scan for the networks, either as an experiment, or just for the pure amusement, or to map out the wireless networks in the area.Due to the nature of flying, it is much more difficult to attempt to access open networks while war flying.

Brian Grimm, a spokesman for the Mountain View, Calif.-based Wireless Ethernet Compatibility Alliance, said these early war-flying reports once again illustrate the need for wireless LAN users to encrypt their signals. But, he noted, "war-flying is self-limiting," since a hacker needs to remain stationary in order to intercept network traffic.

7.15 COMMON WIFI SECURITY RECOMMENDATION

Wi-Fi or **WiFi** (/ˆwajˆfajˆ/) is a technology for wireless local area networking with devices based on the IEEE 802.11 standards. *Wi-Fi* is a trademark of the Wi-Fi Alliance, which restricts the use of the term *Wi-Fi Certified* to products that successfully complete interoperability certification testing.

Devices that can use Wi-Fi technology include personal computers, video-game consoles, smartphones, digital cameras, tablet computers, smart TVs, digital audio players and modern printers. Wi-Fi compatible devices can connect to the Internet via a WLAN and a wireless access point. Such an access point (or hotspot) has a range of about 20 meters (66 feet) indoors and a greater range outdoors. Hotspot coverage can be as small as a single room with walls that block radio waves, or as large as many square kilometres achieved by using multiple overlapping access points.



Depiction of a device sending information wirelessly to another device, both connected to the local network, in order to print a document

Wi-Fi most commonly uses the 2.4 gigahertz (12 cm) UHF and 5 gigahertz (6 cm) SHFISM radio bands. Having no physical connections.

A common measure to deter unauthorized users involves hiding the access point's name by disabling the SSID broadcast. While effective against the casual user, it is ineffective as a security method because the SSID is broadcast in the clear in response to a client SSID query. Another method is to only allow computers with known MAC addresses to join the network,but determined eavesdroppers may be able to join the network by spoofing an authorized address.

Wired Equivalent Privacy (WEP) encryption was designed to protect against casual snooping but it is no longer considered secure. Tools such as AirSnort or Aircrack-ng can quickly recover WEP encryption keys. Because of WEP's weakness the Wi-Fi Alliance approved Wi-Fi Protected Access(WPA) which uses TKIP. WPA was specifically designed to work with older equipment usually through a firmware upgrade. Though more secure than WEP, WPA has known vulnerabilities.

The more secure WPA2 using Advanced Encryption Standard was introduced in 2004 and is supported by most new Wi-Fi devices. WPA2 is fully compatible with WPA.

A flaw in a feature added to Wi-Fi in 2007, called Wi-Fi Protected Setup (WPS), allows WPA and WPA2 security to be bypassed and effectively broken in many situations. The only remedy as of late 2011 is to turn off Wi-Fi Protected Setup,which is not always possible.

Virtual Private Networks are often used to secure Wi-Fi

Wi-Fi Protected Access encryption (WPA2) is considered secure, provided a strong passphrase is used. A proposed modification to WPA2 is WPA-OTP or WPA3, which stores an on-chip optically generated onetime pad on all connected devices which is periodically updated via strong encryption then hashed with the data to be sent or received. This would be unbreakable using any (even quantum) computer system as the hashed data is essentially random and no pattern can be detected if it is implemented properly. Main disadvantage is that it would need multi-GB storage chips so would be expensive for the consumers.

7.16 PDA SECURITY

Personal digital assistants (PDAs) are now commonplace in every type of business. They extend the central computing power of an organization to the roaming worker within the office environment and in the wider world. The delivery of multiple connectivity methods such as wireless or return-to-base technologies has enabled a much expanded roaming computing ability.

PDAs have their origins in simple digital organizers for telephone numbers. The first true PDA, the Newton from Apple, appeared in 1993 [CNI06]. Its main features were fax and email communications, built-in personal information management applications (e.g., contacts, calendar, notes), character recognition of pen-based input entered on a touch screen, and data synchronization with a desktop computer. These same characteristics can be seen in present-day PDA devices. PDAs are in many ways like handheld personal computers; however, they have important differences. For example, PDAs are designed for mobility, hence compact in size and battery powered. They store user data in solid-state memory instead of a hard disk, and they hibernate to conserve battery power and avoid a time-consuming reboot when needed again. Because data retained in volatile memory is subject to loss and even data in non-volatile memory can be cleared if the device is reset, PDAs are also designed to synchronize data with a desktop computer and automatically reconcile and replicate data between the two devices. Most types of PDAs have comparable features and capabilities. They house a microprocessor, Read Only Memory (ROM), Random Access Memory (RAM), a variety of hardware keys and interfaces, and

a touch-sensitive display screen. The Operating System (OS) of the device is held in ROM. Several varieties of ROM are used, including Flash ROM, which can be erased and reprogrammed electronically with OS updates or an entirely different OS. Flash ROM may also be used to store critical user data and applications. RAM, which normally contains user data, is kept active by batteries whose failure or exhaustion causes all information to be lost. The latest PDAs come equipped with system-level microprocessors that reduce the number of supporting chips required and include considerable memory capacity. Built-in Compact Flash (CF) and combination Secure Digital (SD)/MultiMedia Card (MMC) slots support memory cards and peripherals, such as a digital camera or wireless communications card. Wireless communication capabilities such as Infrared Data Association (IrDA), Bluetooth, and Wi-Fi may also be built in. Different devices have different technical and physical characteristics (e.g., size, weight, processor speed, memory capacity). Devices may also use different types of expansion capabilities (e.g., I/O and memory card slots, device expansion sleeves, and external hardware interfaces) to provide additional functionality. PDA capabilities sometimes appear in other devices such as cell phones and GPS receivers. PDAs with cellular communications capabilities are generally considered to be smart phones. The two most prominent families of PDA devices revolve around the operating systems used: Microsoft Windows Mobile (formerly Pocket PC) and Palm OS. Some Linux-based PDAs are also manufactured. Regardless of the PDA family, all devices support a set of basic PIM applications, which include contact, calendar, email, and task management. In addition, most PDAs provide the ability to communicate wirelessly, review electronic documents, and access Web sites. The ability to install third-party applications or to develop them using an available Software Development Kit (SDK) or Integrated Development Environment (IDE) is also a common feature. PIM data residing on a PDA can be synchronized with a desktop computer or server using synchronization protocols such as Microsoft's ActiveSync protocol and Palm's HotSync protocol. Synchronization protocols can also be used to exchange other kinds of data (e.g., text files, images, and other media formats). A cable to link the PDA to a desktop computer is often supplied with the device to facilitate synchronization; it may also be possible to use a wireless interface for synchronization.

7.18 CELL PHONE SECURITY

Mobile security is the protection of smartphones, tablets, laptops and other portable computing **devices**, and the networks they connect to, from threats and vulnerabilities associated with wireless computing. **Mobile security** is also known as wireless **security**.

Ways to stay secure

1. Lock your phone with a password or fingerprint detection. ...
2. If it's not already the default on your phone, consider encrypting your data. ...
3. Set up remote wipe. ...
4. Back up phone data. ...
5. Avoid third-party apps. ...
6. Avoid jailbreaking your iPhone or rooting your Android. ...

Update operating systems often.

Simple steps can protect your phone and information:

1. Smartphones need to be updated when security fixes are developed. ...
2. Security software is a must for smartphone users. ...
3. Minimize losses and avoid intrusions with a secure PIN. ...
4. Think before you click, download, forward, or open. ...
5. Understand the terms of use. ...
6. Surf safely.
7. A **secure telephone** is a **telephone** that provides voice security in the form of end-to-end encryption for the **telephone** call, and in some cases also the mutual authentication of the call parties, protecting them against a man-in-the-middle attack.

7.19 WIRLESS DOS ATTACKS

Wireless network is a data communication network that uses radio frequency band for transmission by obviating wires for connection, transmission and reception. Wireless LAN is a computer network that connects computing nodes over the wireless medium.

Wired networks for data communication were considered to be faster than wireless networks. However technological advancements in wireless networks have disapproved the claims made by the proponents of wired networks. Wireless data networks use radio waves for data communication between devices. By the very nature, the medium for wireless communication is intangible. Wireless networking has changed the fabric of data communication by unbinding users from the shackles of wires and chords. The promise of anytime and anywhere connectivity can only be fulfilled by wireless networks. Wireless data networks are the need of the hour for every emerging business. It's equally essential for an established business to incorporate wireless networks in their IT infrastructure to gain a technological edge over its peers. The reason is that, wireless data networks add a great deal of mobility, flexibility and expandability in the business. Besides, there is considerable cost saving when compared to traditional wired networks. However, organizations should be well prepared to face the problems that come with wireless networks. DoS attacks are a commonplace in data networks. Guarding against DoS attacks should be a critical component of a security system in the current modern day era. Threats like virus, worm, and malware are old school when compared to Denial of Service (DoS) attacks because Denial of Service attacks in wireless data networks have a potential to undermine the advantages that come with wireless networks. It's because of the shared medium of transmission that WLANs are very much vulnerable to DoS attacks. While traditional DoS attack involve overwhelming a host with service requests, in wireless networks limited bandwidth and routing functionality associated with nodes open up new avenues for launching DoS

attacks. The aftermath of DoS attacks range from crippling the network performance to completely bringing it down. So for an organization that has critical operations like point of sales, security cameras over wireless network, surveillance systems etc., any hiccups in the network can cause severe impact on their business. It only makes sense for organizations that have wireless networks deployed, that they be prepared for DoS attacks. For traditional wired networks DoS have been extensively studied but there has been a lack of research study to prevent such attacks on wireless data networks. DoS attacks are perpetrated at various levels of the network defined in the OSI seven-layer network model. This paper covers the attacks carried out at the first two layers wiz Physical layer and MAC layer - a sub layer of Data Link layer. At the physical layer, DoS attack is perpetrated by signal jamming also known as intentional interference. There is another form of unintentional interference that is induced by signals from other devices. The two main protocol 2 attacks that are carried out at the MAC layer are masquerading attacks and resource exhaustion attacks. This paper also discusses the solution methods available for mitigating the DoS attacks discussed here. II. Jamming(intentional interference) and unintentional interference at the Physical layer Wireless data communication happens over a shared medium where information is broadcasted as data frames via radio waves. Although shared medium is the biggest advantage of wireless networks, it's the same-shared medium that makes wireless networks more vulnerable to DoS attacks. WLANs use 2.4 GHz spectrum, which is free and non-regulated. These frequency bands are unlicensed and can be used by any radio devices for data communication; all of which have the same right to use a band.

WLAN DoS Attacks

1. Physical Layer Attacks
2. MAC Layer Attacks

CHAPTER 8

8.1 GPS JAMMING

Information about GPS Jamming. Jamming devices are radio frequency transmitters that intentionally block, jam, or interfere with lawful communications, such as cell phone calls, text messages, PS systems, and Wi-Fi networks. Jammers are illegal to market, sell, or use in the United States. Cell towers divide a city into small areas, or cells. As a cell-phone user drives down the street, the signal is handed from tower to tower. A jamming device transmits on the same radio frequencies as the cell phone, disrupting the communication between the phone and the cell-phone base station in the tower. A mobile phone jammer is an instrument used to prevent cellular phones from receiving signals from base stations. When used, the jammer effectively disables cellular phones. Jamming devices are radio frequency transmitters that intentionally block, jam, or interfere with lawful communications, such as cell phone calls, text messages, GPS systems, and Wi-Fi networks. "We need consumers to be our eyes and ears. Jammers do not just weed out noisy or annoying conversations and disable unwanted GPS tracking, they can prevent 911 and other emergency phone calls from getting through in a time of need." A jammer for a specific service like GPS can simply be a low power transmitter on the frequency range used by the GPS satellites. Even if it transmits enough signal to overwhelm your GPS receiver for a few feet, anyone standing near you could carry one in a pocket.

GPS Jamming Threat

The GPS Jamming Threat Scheduled RFI is probably the largest cause of GPS outages today. The military testing of GPS jamming causes these outages. The events are localized (usually in the Southwestern US), scheduled (during periods of light air traffic), and approved/coordinated by the Federal Aviation Administration. The FAA announces all upcoming events in Notices to Airmen. Because of the ever-greater Airway-Dependency on GPS, the FAA is increasingly reluctant to grant permission for these tests. Accidental RFI has certainly interfered with GPS countless times, both domestically and internationally. Most events are probably not reported. The user who is denied service may not even know to whom it should be reported. These disruptive events include unintentional interference due to harmonics from broadcast television, and improperly designed wireless data communication systems. Deliberate interference, called jamming, is the looming threat. Many of the billion GPS users have become extremely dependent on GPS accuracy, 24 hour availability, and outstanding integrity. This dependency makes GPS a very appealing target for sabotage or malicious mischief. This white paper is a plea that the National Decision Makers address this situation.

8.2 IDENTIFY THREATS IN CLIENT TRADE IN MOBILE PHONES

The Joint Operation Planning and Execution System function that provides: timely warning of potential **threats** to US interests; intelligence collection requirements; the effects of environmental, physical, and health hazards, and cultural factors on friendly and enemy operations; and determines the enemy military. The **Threat** and Hazard **Identification** and Risk Assessment (THIRA) is a 4 step common risk assessment process that helps the whole

community—including individuals, businesses, faith-based organizations, nonprofit groups, schools and academia and all levels of government—understand its risks and estimate capability. **Threat assessment** is a structured group process used to evaluate the risk posed by a student or another person, typically as a response to an actual or perceived**threat** or concerning behavior. **Threat assessment** as a process was developed by the Secret Service as a response to incidents of school violence.

THREAT IDENTIFICATION

The first step in the assessment process is to help you to identify threats that are a priority concern in your area and that may pose a risk to your assets (see Figure 1-1). The threat identification and rating process involves the following tasks: M' Identifying the threats M' Collecting information M' Determining the design basis threat M' Determining the threat rating TASKS: 1.1 Identifying the threats 1.2 Collecting information 1.3 Determining the design basis threat 1.4 Determining the threat rating Step 1: Threat Identification and Rating Step 4: Risk Assessment Step 2: Asset Value Assessment Step 3: Vulnerability Assessment Figure 1-1 Steps and tasks Identifying the Threats (Task 1.1) For this document, threat is defined as any indication, circumstance, or event with the potential to cause loss of, or damage to an asset. Within the military services, the intelligence community, and law enforcement, the term "threat" is typically used to describe the design criteria for terrorism or manmade disasters. The Federal Emergency Management Agency (FEMA) and other civil agencies use the term "hazard" in several different contexts. "Natural hazard" typically refers to a natural event such as a flood, wind, or seismic disaster.

8.3 Threats classification

Threats can be classified according to their type and origin:

- Types of threats:
  - Physical damage: fire, water, pollution
  - Natural events: climatic, seismic, volcanic
  - Loss of essential services: electrical power, air conditioning, telecommunication
  - Compromise of information: eavesdropping, theft of media, retrieval of discarded materials
  - Technical failures: equipment, software, capacity saturation,
  - Compromise of functions: error in use, abuse of rights, denial of actions

8.4 CLIENT TRADE IN MOBILE PHONES

After online trading; the latest and the most far reaching trade channel is predicted to be the ubiquitous mobile handset. A new breed of clients has arisen, equipped to trade at the convenience of their time and place – using their mobile handset. No more waiting to get to a trading terminal or a PC to trade. Mobile Trading is essentially an extension of internet based trading –but with small form factor device i.e: the mobile phone Similar to a Client logging on to the broker's trade portal on his internet enabled PC. Broker will have full control of the risk parameters since orders submitted by client on his mobile will be sent via the Broker's servers to the exchange.

Client Trading

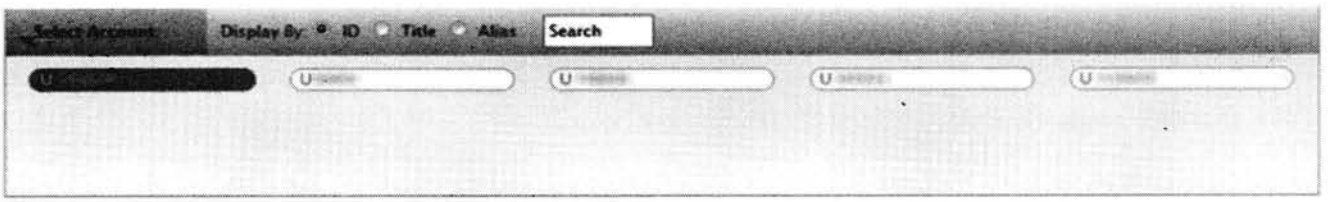
The Client Trading page lets you enable or disable trading for a specific client account. Changes made on this page do not take effect until the next business day.

Who can access the Client Trading page?

To enable or disable client trading

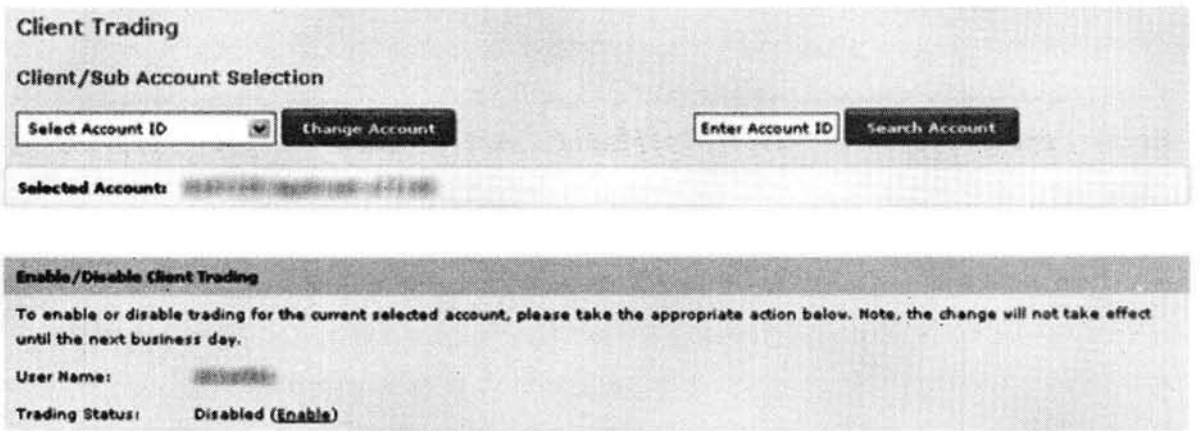
1. Click **Manage Clients > Trading > Configuration**.

Use the Account Selector to search for a client account by Account ID, Account Title or Account Alias, then click the desired account.



The Account Selector is closed once you select an account. To change the selected account, click the tab to open the Account Selector, and then click a different account.

The Client Trading page opens.



The current trading status (Enabled or Disabled) of the selected client account appears.

3. To enable trading for the client account, click the *Enable* link. To disable trading for the client account, click the *Disable* link.

8.5 VOICE, SMS AND IDENTIFICATION OF DATA INTERCEPTION

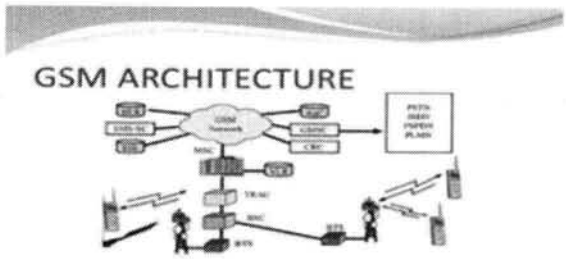
Interactive voice response (**IVR**) is a technology that allows a computer to interact with humans through the use of voice and DTMF tones input via keypad. In telecommunications, IVR allows customers to interact with a company's host system via a telephone keypad or by speech recognition, after which services can be inquired about through the IVR dialogue. IVR systems can respond with prerecorded or dynamically generated audio to further direct users on how to proceed. IVR systems deployed in the network are sized to handle large call volumes and also used for outbound calling, as IVR systems are more intelligent than many predictive dialer systems.

IVR systems can be used for mobile purchases, banking payments and services, retail orders, utilities, travel information and weather conditions. A common misconception refers to an automated attendant as an IVR. The terms are distinct and mean different things to traditional telecommunications professionals—the purpose of an IVR is to take input, process it, and return a result, whereas the job of an automated attendant is to route calls. The term **voice response unit** (**VRU**) is sometimes used as well.

intercepting data communicated between a sender and a receiver, and conditionally altering that data, the apparatus comprising: an interception unit, capable of intercepting said data, setting information for storing predetermined device settings, access functionality, associated with said interception unit operable to access information within said intercepted data, and a search and replace unit, associated with both said interception unit and said access functionality, for conditionally altering the intercepted data in response to said accessed information and said device settings. The device is useful for dynamically updating web pages and the like and said updating may be made conditional on communication control information such as the identity of an intended recipient as well as data content. Multiple-access schemes are introduced and analyzed for the integration of voice and data traffic in packet radio networks using code-division multiple-access (CDMA). The multiple-access capability of the CDMA channel is used to accommodate several voice calls simultaneously, while the data users follow the ALOHA protocol with retransmission control and contend for the remaining (if any) multiple-access capability of that channel. An **interception** means that some unauthorized party has gained access to an asset. The outside party can be a person, a program, or a computing system. Examples of this type of failure are illicit copying of program or data files, or wiretapping to obtain data in a network. **Lawful interception** (**LI**) refers to the facilities in telecommunications and telephone networks that allow law enforcement agencies with court order or other legal authorization to selectively wiretap individual subscribers. Most countries require licensed telecommunications operators to provide their networks with Legal Interception gateways and nodes for the interception of communications. The interfaces of these gateways have been standardized by telecommunication standardization organizations.

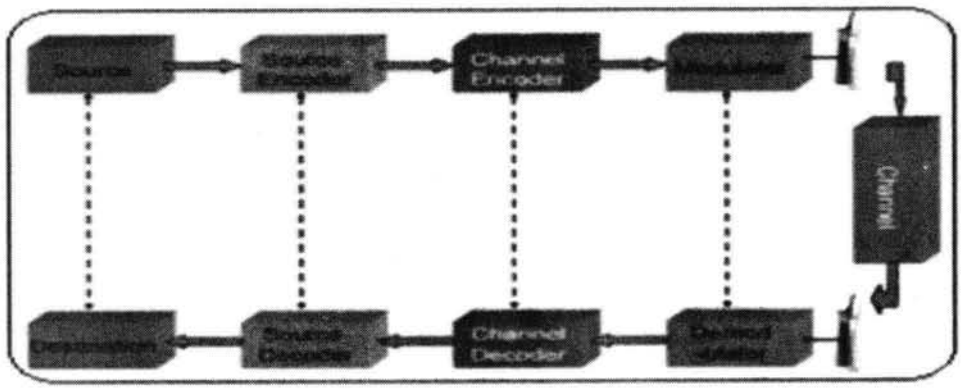
8.6 GSM Global System for Mobile communications, a mobile phone system based on multiple radio cells (cellular mobile phone network).

In the GPRS system, the frames are transmitted as cipher text from the MS to the SGSN. This is done because the GPRS system uses multiple timeslots in parallel in order to achieve a greater transmission rate. One GPRS phone can be allocated multiple timeslots by the network, thus increasing the transmission rate of that MS. The frames can be sent in 'parallel' timeslots to the same BTS or to two different BTSs if the MS is handed over from one BTS to another. To a BTS the use of one timeslot is seen as a separate call. Thus, the BTS is unable to put the frames from different timeslots together. This means that there has to be a network component that is able to receive the frames from one MS, defragment them and send them onwards to the actual destination. GSM Interception The BTSs are also unable to decrypt the frames, because consecutive frames on one channel have not got consecutive frame numbers. To simplify the implementation, the frames are decrypted at the SGSN where all of the frames end up and it is thus easy to keep track of frame numbers. The solution is based on the ease of implementation and has not been implemented in order to increase system security. As a side effect, the GPRS system effectively prevents eavesdropping on the backbone between the BTS and SGSN, because the frames are still encrypted at this point. In GPRS, the triples from the HLR are transmitted to the SGSN and not to the MSC. Thus, security of GPRS depends largely on the placement and security of the SGSNs. GPRS architecture The GPRS system uses a new A5 implementation as well, which is not known publicly. This and the fact that the frames are not decrypted at the BTS, but at the SGSN, rules out a couple of attacks. First, it is very hard to attack the A5 implementation when it is not known. Secondly, the Kc is not transmitted to the BTSs and the transmission channel between the BTS and the SGSN is encrypted making it thus useless to monitor the backbone between the BTS and the SGSN. This does not mean that the GPRS security model would somehow be more secure than the GSM-only security model. It means that identical attacks do not work with GPRS that work with a GSM-only network. As soon as the A5 implementation used in GPRS leaks out, the GPRS security model is vulnerable to new attacks. And the implementation will leak out eventually or the design is successfully reverse-engineered. As was states above, the security of a crypto system should be based solely on the key. However the majority of the attacks against the GSM-only system are applicable against GPRS as well. E.g. the SIM-cloning attack. Additionally, the GPRS model introduces another security threat through the use of SGSNs, which know the triples from the HLR. This means that the security of the GPRS network depends largely on the positions of the SGSNs in the network architecture and the security of the SGSNs. If the SGSNs are vulnerable to an attack, than the triples are vulnerable as well.



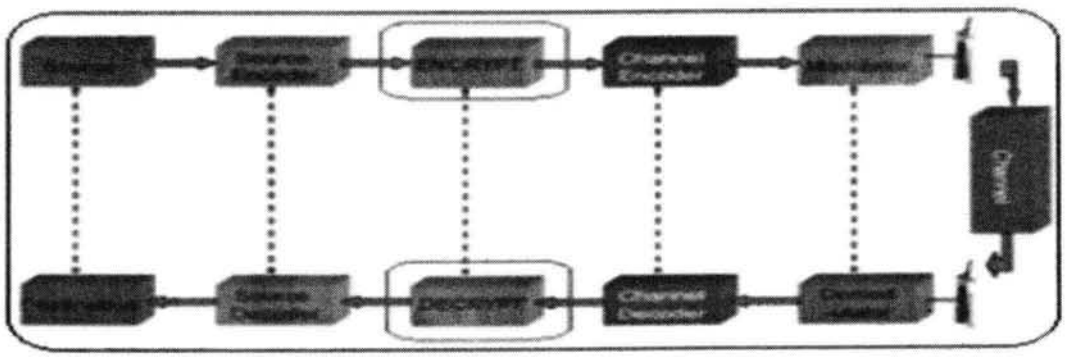
8.7 COMMUNICATIONS IN GSM NETWORKS

Each SIM card in its GSM mobile terminal (MT) contains a different 128 bit secret key Ki (random challenge), known only to it and to the base station (BS) of the GSM network. When a GSM phone call is being processed, the BS sends via the network a generated 128 bit random number to the SIM of the MT. The SIM uses a hash function called A3 to generate a 32-bitrandom challenge (SRES), and send it back to the base station.



Typical wireless communication system

The BS compares the received SRES value with the computed one by using its own copy of the RAND challenge and the private key Ki [21]. If they are matched, the BS believes that the SIM is authentic and the call is allowed to proceed. The call exchanged between the MT and the network is encrypted using an encrypted algorithm called A5 to produce a 64 session key Ks. Thus, for each new call the required A5 session key Ks is generated using a hash function called A8 which take the same 128 bit key Ki and 128-bit key to produce the 64 bit session key Ks. However, the authentication module only works between the BS and the mobile terminal and cannot provide end-to-end secure communication in the GSM network.



END-TO-END Security Model

The block diagram consists of four main subsystems: a source encoder/decoder subsystem, channel Decoding/ encoding subsystem, and modulation/demodulation subsystem. In case of wireless connection, the A5 security subsystem can function as an encryption/decryption module. Obviously, the system does not support end-to-end security, since the communicated data are protected only by the BS which involves two separate security channels. At the transmitter side, the source encoder converts the analog or digital information source to a sequence of binary digits by an A/D converter, including sampling at 8 KHz sampling rate. It usually generates 14-16 bits/sample. Before the sampling the direct component is removed by the FIR filter, and the transmitter pre-emphasis uses high-frequency boosting to enhance the high-frequency content of the signal. The data is then sampled and broken into frames, and the coder operates on 160 sample frames that span 20ms. The linear predictive coders (LPC) filter takes a digitized signal and generates a set of predictive coefficients as well as a set of error coefficients (residual signal). Finally, long-term predication (LTP) is used to eliminate the redundancy in digitized signal. At the receiver side, the process is reversed to obtain and decode the original data. In the GSM system, the encryption-decryption subsystem takes place before modulation subsystem, which is easy to implement in the mobile terminal. However, it is highly desirable to have end-to-end secure protocol over the communication channel. In order to achieve end-to-end secure communication, data must be encrypted before it enters the GSM network. An encryption module that enables end-to-end secure communication over the GSM channel is proposed. The proposed scheme does not require any modification in the BS neither the GSM standard. It only requires a small modification on the mobile terminals. A real-time prototype is implemented demonstrating the end-to-end secure data communication over the GSM network. security algorithm is inserted between the source encoder and the channel encoder of the MT, so that the coming signal from the source encoder subsystem would firstly arrive to the newly-added data Encryption/Decryption module and finishes the encryption. After that, it is sent to the channel module. Hence, this encryption method must penetrate the RPE-LTP vocoder and have ideal encryption intensity. Simultaneously this encrypted signal can be recovered to get the original understandable data at the receiver. This proposed encryption method is a kind of signal source encryption technology, so it could achieve the end-to-end secured communication.

8.8 SECURITY ANALYSIS

This section discusses the results of the proposed method. It also presents the obtained driving strategies and the test cases that show how the system is secured, In order to implement such strategies, one must go through several steps which were discussed in details in the preceding sections. It is among all base stations and mobile terminals of the same traffic type. A key is used to secure communications between mobile terminals as well as decipher broadcast frames from the terminals. The following notation is used throughout the remainder of this section: BS and MT refer to Base Station and Mobile Terminal.

- K is a private key, whereas EC is an elliptic curve and G the generator number.
- M is a message (stream of bits) and C is the cipher.
- R( ) is a family of pseudo-random numbers.
- AC (C, K) is an authentication code to the encrypted data which uses the same Key.

It is assumed that the communication between the Base Station Transceivers (BST) and Base Station Controllers (BSC) is highly secured. Messages between base station and mobile terminals are encrypted by ECC algorithm.

ADVANTAGE

The advantage of using ECC is that it provides an equal security as RSA but with less overhead in the processing of messages. Thus, to secretly communicate with each other, mobile terminals must have keys which are known only by the communicating terminals. A random public point G is chosen on the elliptic curve EC to produce a compressed public key.

In addition, BS chooses a random number RBS (its symmetric key), then the BS computes it session key SRBS = RBS * G . Mobile terminals also compute shared session key that each one share with the BS. The shared session key is computed by:

K= KMT * SRBS = KMT * RBS * G

This private key is used to secure communication between the base station and the mobile terminals. The cipher C is used to denote the encrypted message M with the shared session key K. After this message is encrypted, the authentication process takes place. In order to verify data authenticity and integrity of the message M, it uses a key to authenticate messages, for example; MD5 [28]. The messages sent by mobile terminals to the BS are with the following structure:

MC = SRBS + C + AC (C, KF)

It is assumed that the BS has a powerful computing power and more energy than regular mobile terminals. Thus, after establishing the first channel of communication between the BS and mobile terminals, the BS authenticates the shared session key until the end of the session. Therefore, after authenticating keys, messages are coded as shown.

MC = C + AC (C, KF)

In this manner, the BS also distributes and authenticates session keys to the communicated mobile terminals.

8.9 INTRODUCTION PRATICAL SETUP AND TOOLS

ISD provides assistance to install and set-up desktop and laptop computer hardware and software. ISD can also assist with moving current desktop systems or removing systems that are no longer in use. Centralized installation can reduce costs for installing new desktop systems or moving computers to new locations, allowing you to direct resources to core services. ISD analysts work with you and your staff to develop hardware and software configurations to support your infrastructure and ensure your data and computer assets are properly protected. Centralized set-up helps standardize your hardware and software platforms to facilitate staff cross-training and minimize ramp-up time for new employees.

IMPLEMENTATION Hardware AND SOFTWARE Mobile Phone Tricks

Mobile phone handsets and networks offer a wealth of applications and functionalities that the average user never gets to use. Nonetheless, they are affecting the security of the phone, either positively or negatively. In this chapter, we will examine a few of them, namely Netmonitor, GSM/UMTS network codes, mobile phone codes, and the AT command set. There is also a brief software section since, as stated earlier, the software applications and their security fit better in the context of a computer literature work.

Implementation (trick replay)

- Qt Quick 3D (QML)
- Accelerometer data used:
- Realtime graphs
- 3D model translation
- Pressure pad determines skateboarder's presence
- Gyro data not used
- Qt C++ to QML binding

Network Monitoring

Network monitoring is the information collection function of network management. Network monitoring applications are created to collect data for network management applications. The purpose of network monitoring is the collecting of useful information from various parts of the network so that the network can be managed and controlled using the collected information. Most of the network devices are located in remote locations. These devices do not usually have directly connected terminals so that network management application cannot monitor their statuses easily. Thus, network monitoring techniques are developed to allow network management applications to check the states of their network devices. As more and more network devices are used to build bigger networks, network monitoring techiques are expanded to monitoring networks as a whole.

As more people communicate using networks, networks have become bigger and more complex. The proliferation of the internet has increased the pace of network expansions. At this age of big and complex networks, network monitoring applications need to use effective ways of checking the status of their networks so that network management applications can fully control their network and provide economical, and high-quality networking services to the users. It is very important to know what the goals to achieve in network monitoring are. By knowing the goals of network monitoring, network monitoring application can choose among network monitoring techniques that will best help them monitor their networks.

There are generally three basic goals for network monitoring

- Performance monitoring
- Fault monitoring
- Account monitoring

These goals are three of the five functional areas of network management proposed by OSI, Open Systems Interconnect. The other two functional areas are not related to network monitoring. They are configuration management and security management.

Monitoring Internet

Internet is a network of many networks. Each individual network is owned and operated by different organizations. Monitoring the internet is different from monitoring a single network because in a single network, all components are usually under the control of a single network management, but in the case of internet, each individual network has different base layer platform and is managed by different network management.

Monitoring difficulties

The internet is getting more and more difficult to monitor because more and more users are added to it everyday, and there is a lack of measurements of the quality for the internet as a whole. There is no standardized metric being used in measuring the internet. But usually host response time, time delay, and loss rate are being measured by individual network. The users of the internet has to measure aspects of the internet which tell them the performance of their network applications.

8.10 GSM NETWORK SERVICE CODES

The GSM standard allows most of the functions to be controlled by entering codes into the keypad of a mobile phone: you can set diverts and the like, accept or reject calls, or even change your PIN code by typing at the keypad.

Unfortunately, not all the codes listed here are enabled by every network. If a code isn't supported, it simply won't work: you won't break anything by trying to use it! Why bother?

Many (though not all) handsets offer menus to do most of these things, but they vary from handset model to model, and are sometimes hidden by networks who don't want to confuse their users.

If you can use the codes directly, you can also store them in memory, so that you can easily recall and reuse them. For example, you might want to divert all calls to your office phone on a regular basis: from memory, it's just two or three keypresses to set up or cancel such a diversion. Types of call

You know about voice calls, but there are also fax calls, data calls, ALS (line two) calls and SMS messages. Calls of different types can all have different settings associated, using the relevant "bearer code" as shown in the examples below. The snags

Some networks don't support all services, so some GSM codes will fail. Others sometimes seem to use their own interpretation of the GSM codes.

If you are having trouble setting call diversion, try ##002#[SEND] and/or ##004#[SEND] to clear all existing diverts first. You probably have to cancel a 'no reply' diversion before you can set another with a different timeout.

- Call Divert
- Divert Voice Calls
- Divert Data Calls
- Divert Fax Calls
- Divert Line 2 Calls
- Call Barring
- SMS
- Calling Line Identity
- Dial number from memory
- Change PIN codes

GSM Code Scheme and Passwords :Most of the codes given below follow this pattern. With enough use, you will learn to know what each means:

- *** activate**
- **** register and activate**
- ***# check status**
- **# unregister**
- **## unregister and deactivate**

Some service providers will also let you change your passwords as follows:

Change Call Barring PIN code: ****03*oldPIN*newPIN*newPIN#**

Change SIM PIN code: ****04*oldPIN*newPIN*newPIN#**

If you have never set a PIN before, try the usual default of '0000', '1111', or the last 4 digits of your phone number. If none of these work then contact your service provider.

GSM network servicecodes

Attention!only 11, 13 and 25 are functioning today. Maybe later you will be able to use all these codes to monitor every single of the commands above by entering the service code just before the last # on the command line. If you wish to divert all data calls to another PhoneNumber, you'll enter the command '*21*PhoneNumber*12#

Phone related

Service code	Code description
10	All types of phone services
11	Speech sevice
12	Data sevice
13	Fax
14	Datex-J
15	Teletex
16	SMS
18	All data services except SMS
19	All phone services except SMS

Carrier related

Service code	Code description
20	All services
21	All asynchronous services
22	All synchronous services
23	3.1kHz services
24	Synchronous Point-to-Point connections
25	Asynchronous Point-to-Point connections
26	Data packet sending
27	Sevices with PAD share
29	Digital connection with 12 kbps

8.11 MOBILE PHONE CODES

All mobile numbers in India starts with **9**, **8**, **7** or **6**, this includes pager services, but the use of pagers is on the decline. Each telecom circle is allowed to have multiple private operators, earlier it was 2 private + BSNL/ MTNL, subsequently it changed to 3 private + BSNL/MTNL in GSM, now each telecom circle has more than 10 operators including BSNL/MTNL.

All mobile phone numbers are 10 digits long. The way to split the numbers is defined in the National Numbering Plan 2003 as XXXX-NNNNNN where *XXXX* indicates the network operator and telecom circle, and *NNNNNN* is the subscriber numbers.

Codes working with most of cell phones

Code	Function
press 1 for longer than aone second	Dial mailbox number (mailbox number must bve specified in the settings)
press # for longer than one seconds	Activate/deactivate silent profile
*#06#	Display the IMEI (International Mobile Equipment Identity)

Codes	Information
##232339#*#* OR *#*#526#*#* OR *#*#528#*#*	W-LAN test (Use "Menu" button to start various tests).
##232338#*#*	Shows Wi-Fi MAC address.
##1472365#*#*	GPS test.
##1575#*#*	Another GPS test.
##232331#*#*	Bluetooth test.
##232337#*#	Shows Bluetooth device address.
##0842#*#*	Device test (Vibration test and Back Light test).
##0588#*#*	Proximity sensor test.
##0*#*#*	LCD test.
##2664#*#*	Touch screen test.
##2663#*#*	Touch screen version.
##0283#*#*	Packet Loopback.
##0673#*#* OR *#*#0289#*#*	Melody test.
##3264#*#*	RAM version.
##1111#*#*	FTA SW Version.
##2222#*#*	FTA HW Version.
##44336#*#*	PDA, Phone, CSC, Build Time, Change list number.
##4986*2650468#*#*	PDA, Phone, H/W, RFCallDate.
##1234#*#*	PDA and Phone.

CATLOG TRICKS AND AT COMMAND SECURITY

• The catalog application in most cell phones matches only the 6-8 last digits of a number in order to show the relative entry name.

- If +30694577875=ΣΗΦΗΣ, then 4577875 shows also ΣΗΦΗΣ but of course can't be called
- If I dial 2651007164477875, I will read ΣΗΦΗΣ on screen but 265100716 will be called!
- 55# shows entry 55 etc.

CATLOG

- AT+CPBS (Select the phonebook type) "DC" – Dialed calls "EN" - Emergency numbers, writeprotected stored on SIM "FD" - Fixdialing numbers "MC" - Missed calls "ME" - Phonebook "MT" - "ME" + SIM phonebook "ON" - Own number "RC" - Received calls "TA" - TA phonebook
- AT+CPBR (Read phonebook)
- AT+CPBR=? (Reads out the number of supported entries from the phonebook)
- AT+CPBR=2 (Reads the entry number 2 of the phonebook)
- AT+CPBF (Search by name in phonebook)
- AT+CPBF="Max" (Searches for an entry with name "Max" and displays it)
- AT+CPBR=11 (phonebook) +CPBR: 11,"2220",129,"infoArea".

8.12 SMS SECURITY ISSUES

Definition: A globally accepted wireless service that enables the transmission of alphanumeric messages between mobile subscribers and external systems such as electronic mail, paging and voice mail systems (International Engineering Consortium, 2002)

Guaranteed delivery: if a wireless recipient is switched off, out of range or if there is a network outage, the SMS message will be stored in the network and delivered when the recipient announces its presence, or when the outage is rectified. No guarantees existed with previous such services eg. Alphanumeric paging. This is the basis of the store-and-forward concept.

Send or receive during voice or data calls: SMS messaging makes use of a separate channel, normally used for transfer of control messaging to transfer its packets. Being out-of-band, this means voice and data calls will not be interrupted by SMS transfer. Furthermore, the low-bandwidth requirements of transmitting short alphanumeric strings allows messaging worldwide with very low latency. This of course depends upon network operator agreements.

SMS Network **Architecture** and Internal Protocols. ... In this figure you can see which protocols are used and which GSM network entities take place in the communication process. As you can see, the mobile phone (Mobile station) transmits the **SMS** message to the GSM base station (BTS) through a wireless link.

SMS Architecture Store and Forward Cleartext with many different formats among manufacturers (SMPP, EMI/UCP, TAP êëð).

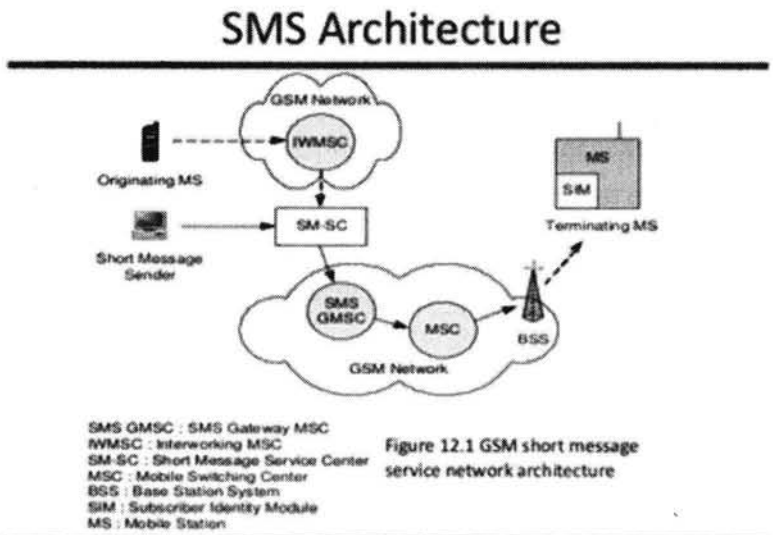


Figure 12.1 GSM short message service network architecture

8.13 History of SMS

Analogue: the world-wide standard in the late 1980s and early 1990s had no capability for text messaging GSM: European networks began development of a digital standard (GSM) in 1991. Phase 2 of the standard, release in 1993, defined data bearing services over GSM – SMS was a part of this standard. Vodacom (South Africa) became the first company in the world to implement fax and data services on its network, later that year.

CDMA/TDMA: The American networks decided to take an alternative route, using first TDMA and later, the superior CDMA which integrated text messaging into its standard. TDMA later gained this capability through Motorola's iDEN development.

Interoperability: When the buildout of personal communication service (PCN) networks was complete in 1998, SMS was fully deployed. All that remained was the agreement between network operators to allow this.

Applications of SMS

Originally SMS was used for:

- notification purposes: particularly voice mail (eg. Optus)

- 2-way messaging: intended to supersede alphanumeric paging, the capability was introduced simply to allow general-purpose messaging between wireless entities.

Newer implementations for SMS include:

- E-mail: a number of services now exist that allow you to check a POP3 mail account on your handset, or employ translation of e-mail into SMS form for receipt on a handset
- Fax: allows of transfer through handset to a notebook, or translation into actual SMS messages for viewing on the handset.

- Interactive banking: services such as the Vodafone/Commonwealth Bank mobileBank service allow account balances, funds transfers and other transactions to be completed via SMS messaging on a user's handset.
- Information services: for a fee, a number of service providers will now send regular updates on share prices, news headlines, the weather and even goings on at the Big Brother house straight to your handset via SMS.

Web integration:

- a number of forms exist, including the ability to receive web content through SMS, the sending/receiving of actual WAP datagrams through SMS, as well as emerging cross-platform approaches such Internet instant messaging services being combined with SMS sending capabilities – allowing 'SMS chat'.

Using SMS

FlashMX presentation of SMS operation on a mobile handset. The 'user's view' of SMS.

8.14 SMS SECURITY

THE BASICS OF SMS SECURITY

The technical specifications for SMS are laid down in ETSI TS 03.485 . Certain options in the technical specification, such as the Security Parameter Index (SPI), the Ciphering Key Identifier (KIc), and the Integrity Value (RC/CC/DS), provide specifications for available security parameters. A Redundancy Check (RC), Cryptographic Checksum (CC) or Digital Signature (DS) might also be used for integrity verification of the data. However, these confidentiality and integrity mechanisms are only specified as optional security measures that can be made available, but they are not mandatory requirements for SMS system implementation6 . The availability of SMS services may also be interrupted by the SMSC. Without proper implementation of these SMS security options, everyday SMS messages transmitted on a network are only protected by the communication network itself such as a GSM network. In practical use, SMS messages are not encrypted by default during transmission. A cyclic redundancy check is provided for SMS information passing across the signalling channel to ensure short messages do not get corrupted. Forward error protection is also incorporated using conventional encoding. Cryptographic protection on confidentiality and integrity is not available for SMS messages.

Digital cellular telecommunications system (Phase 2+); Technical realization of the Short Message Service (SMS) Point-to-Point (PP) 3GPP TS 03.40 version 7.5.0 ,1998 ETSI TS 100 901 V7.5.0 (2001-12).

SMS Attacks

- Denial of Service in the network or the phone with consecutive messages (from another phone or the net) –Phone Buffers –SMSC Buffers
- Long names, invalid characters –Especially crafted Vcards –Especially crafted SMSs (i.e. Broken UDH) –Obexftp through Bluetooth
- History: Nokia 5100 all dot SMS crash
- SMS spoofing

SMS flash

• Flash message appears immediately on the screen usually close to the Network Name

• User does not have to "open" the message to read it. It is already "opened"

• Can deceit the user to trust that it comes from the provider. Can be used for various Social Engineering attacks.

SMS ping

• Every simple user (not the mighty provider!) can stealthily discover whether another user has her cell phone switched on or off!

• He can reveal her behavior using patterning techniques (i.e. time of awakening or sleeping)

SMS Spoofing

Bulk SMS through marketing companies Bulksms, Prosms, Websms, Sendsms You can arbitrarily chose originator name or number 11 latin characters or 16-digit number Interconnection fee.

8.15 MOBILE TECHNOLOGY AND CRIME

Mobile technology is exactly what the name implies – technology that is portable. Mobile IT devices include:

• Laptop computers.

• Palmtop computers or personal digital assistants.

• Mobile phones and 'smart phones' – high-end phones with more advanced capabilities.

• Global positioning system (GPS) devices.

• Wireless debit/credit card payment terminals. Mobile devices can be enabled to use a variety of communications technologies such as;

• Wireless fidelity (WiFi) – a type of wireless local area network technology.

• Bluetooth – connects mobile devices wirelessly.

• 'Third Generation' (3G), global system for mobile communications (GSM) and general packet rádio service (GPRS0 data services – data networking services for mobile phones.

• Dial-up-service – data networking services using modems and telephone lines.

• Virtual private networks – secure access to a private network. It is therefore possible to network the mobile device to a home office or the internet while travelling. Benefits Benefits

• Mobile computing can improve the service you offer your customers. For example, you could use your laptop computers to give a presentation. Or you could remotely to your diary to arrange a follow-up appointment.

• More powerful solutions can link you directly into the office network while working off site, for instance to access your company's database or accounting systems.

• This leads to great flexibility in working – for example, enabling home working, or working while travelling. Increasingly, networking 'hot spots' are being provided in public areas that allow connection back to the office network or the internet. Drawbacks Drawbacks

• Mobile IT devices can expose valuable data to unauthorized people if proper precautions are not taken to ensure that the devices, and the data they can access, are kept safe.

In today's world with the advent of SMART PHONES there is virtually no difference between COMPUTER and MOBILE phones, so whatever Cyber Crime we were aware of related to Computers are also applicable to Mobile Crime.

–A definition. A definition. A definition. Defining cybercrimes, as "acts that are punishable by the Information technology Act" would be unsuitable as the Indian Penal Code also covers many cybercrimes, such as email spoofing and cyber defamation, sending threatening emails etc. a simple yet sturdy definition of cybercrime would be "unlawful acts wherein computer is either a tool or a target or both.

Criminals can operate anonymously over the computer networks, hackers invade privacy, hackers destroy "Property" in the form of computer files or Records. • Hackers Injure Other Computer Users by Destroying Information System. • Computer Pirates Steal Intellectual Property.

8.16 CRIME RALATED TO THE MOBILE TECHNOLOGY

• As the new millennium dawned, the computer has gained popularity in every aspect of our lives. This includes the use of computers by persons involved in the commission of crimes. Today, computers play a major role in almost every crime that is committed. Every crime that is committed is not necessarily a computer crime, but it does mean that law enforcement must become much more computer literate just to be able to keep up with criminal element. According to Donn Parker, "For the first time in human history, computers and automated processes make it possible to possess, not just commit, a crime. Today, criminals can pass a complete crime in software from one to another, each improving or adapting it to his or her own needs."

• The first recorded cybercrime took place in the year 1820. The era of modern computers, however, began with the analytical engine of Charles Babbage. Cybercrime is an evil having its origin in the growing dependence on computers in modern life. In a day and age when everything from microwave ovens and refrigerators to nuclear power plants is being run on computers, cybercrime has assumed rather threatening implications.

• The majority of what are termed "cybercrimes" is really violations of longstanding criminal law, perpetrated through the use of computers or information networks. The problems of crime using computers will rarely require the creation of new substantive criminal law; rather, they suggest need for better and more effective means of international co-operation to enforce existing laws.

• On the other hand, there are new and serious problems posed by attacks against computer and information systems, such as malicious hacking, dissemination of viruses, and denial-of-service attacks. Such attacks should be effectively prohibited, wherever they may originate. At the same time, it is to be remembered that often the most effective way to counter such as attacks is to quickly deploy technical countermeasures; therefore, to the extent that well-meaning but overbroad criminal regulations diminish the technical edge of legitimate information security research and engineering, they could have the unintended consequences of actually undermining information security. Classification of Cyber Crimes Classification of Cyber Crimes the Information Technology Act deals with the following cybercrimes along with others

• Tampering with computer source documents

• Hacking

• Publishing of information, which is obscene in electronic form

• Child Pornography • Accessing protected system

• Breach of confidentiality and privacy

TYPES OF CYBER/MOBILE CRIME

Cybercrime other than those mentioned under the IT Act

• Cyber Stalking

• Cyber squatting

• Data Diddling

• Cyber Defamation

• Trojan Attack

• Forgery

• Financial crimes

• Internet time theft

• Virus/worm attack

• E-mail spoofing

• E-mail bombing

• Salami attack

• Web jacking

CYBER/MOBILE CRIMINALS

• Any person who commits an illegal act with a guilty intention or commits a crime is called an offender or a criminal.

In this context, any person who commits a Cyber Crime is known as a Cyber Criminal. The Cyber Criminals may be children and adolescents aged between 6 to 18 years. They may be organized hackers, may be professional hackers or crackers, discontented employees, cheaters or even psychic person. A. Kids & Teenagers (age group 9 – 16 etc)

• This is really difficult to believe but it is true. Most amateur hackers and cyber crime criminals are teenagers. To them, who have just begun to understand what appears to be a lot about computers, it is a matter of pride to have

hacked into a computer system or a website. There is also that little issue of appearing really among friends. These young rebels may also commit cybercrimes without really knowing that they are doing anything wrong.

• According to the BBC, teen hackers have gone from simply trying to make a name for themselves to actually working their way into a life of crime from the computer angle. According to Kevin Hogan, one of the biggest changes of 2004 was the waning influence of the boy hackers play around with malicious code, 2004 saw a significant rise in criminal use of malicious programs. The financial incentives were driving criminal use of technology.

• Another reason for the increase in number of teenage offenders in cybercrimes are that many of the offenders who are mainly young college students are unaware of its seriousness. Recently the Chennai city police have arrested an engineering college student from Tamil Nadu for sending unsolicited message to a chartered accountant. The boy is now released on bail. So counseling session for college students has to be launched to educate them on the gravity and consequences emanating from such crimes.

8.17 CRIMINAL LAW –GENERAL PRINCIPLES

• According to law, certain persons are excluded from criminal liability for their actions, if at the relevant time; they had not reached an age of criminal responsibility. After reaching the initial age, there may be levels of responsibility dictated by age and the type of offense allegedly committed.

• Governments enact laws to label certain types of activity as wrongful or illegal. Behavior of a more antisocial nature can be stigmatized in a more positive way to show society's disapproval through the use of the word criminal. In this context, laws tend to use the phrase, "age of criminal responsibility" in two different ways:

1. As a definition of the process for dealing with alleged offenders, the range of ages specifies the exemption of a child from the adult system of prosecution and punishment. Most states develop special juvenile justice systems in parallel to the adult criminal justice system. Children are diverted into this system when they have committed what would have been an offense in an adult.

2. As the physical capacity of the child to commit a crime. Hence, children are deemed incapable of committing some sexual or other acts requiring abilities of a more mature quality.

• The age of majority is the threshold of adulthood as it is conceptualized in the law. It is the chronological moment when children legally assume majority control over their actions and decisions, thereby terminating the legal control and legal responsibilities of their parents over and for them. Bu in the cyber world it is not possible to follow these traditional principles of criminal law to fix liability. Statistics reveal that in cybercrime world, most of the offenders are those who are under the age of majority. Therefore, some other mechanism has to be evolved to deal with cyber criminals.

• Ethics and morality in different circumstances connotes varied and complex meaning. Each and everything which is opposed to public policy, against public welfare and which may disturb public tranquility may be immoral and unethical.

• In the past terms such as imperialism, colonialism, apartheid, which were burning issues have given way to cybercrime, hacking, 'cyber-ethics' etc. Today in the present there is a need to evolve a 'cyber-jurisprudence' based on which 'cyber-ethics' can be evaluated and criticized. Further there is a dire need for evolving a code of Ethics on the Cyber-Space and discipline.

• The Information Technology Act 2000 was passed when the country was facing problem of growing cybercrimes. Since the Internet is the medium for huge information and a large base of communications around the world, it is necessary to take certain precautions while operating it. Therefore, in order to prevent cybercrime it is important to educate everyone and practice safe computing.

8.18 EVIDENCE AND FORENSIC PROCEDURE

The **Forensic Procedure** Act 2000 ['the Act'] allows **forensic procedures** to be carried out on certain people such as suspects or people charged with a serious offence, to assist police in solving crime. A **forensic procedure** can either be non-intimate or intimate. The Crimes (Forensic Procedures) Act 2002 (NSW) gives wide powers to Police and other enforcement officers to take photographs, body samples (including DNA samples, dental impressions and casts from convicted criminals and people suspected of committing a criminal offence.

A forensic procedure does not include any intrusion into a person's cavities (except the mouth) or the taking of a sample for the sole purpose of establishing the identity of the person from whom the sample is taken.

TYPES OF FORENSIC PROCEDURES

There are three types of forensic procedures:

- An intimate forensic procedure
- A non-intimate forensic procedure
- A buccal swab (saliva taken from a person's mouth)

A non-intimate forensic procedure means any of the following:

- An external examination of a person's body other than the private parts, that requires touching of the body or removal of clothing
- The carrying out of a self-administered buccal swab
- The taking of a sample of hair, other than pubic hair
- The taking of a sample of nails or of matter from under the nails
- The taking of a sample of any matter from the external part of the body
- The taking of handprint, fingerprint, footprint or toe print

- The taking of a photograph of a person's body, other than the private parts
- The taking of an impression or cast of a wound from a part of the person's body
- The taking of the measurements of a body or any part of the body, other than private parts.

An intimate forensic procedure means any of the following:

- An external examination of a person's private parts
- The carrying out go a buccal swab
- The taking of a sample of blood
- The taking of a sample of pubic hair
- The taking of a sample of any external matter from a person's private parts
- The taking of a dental impression
- The taking of a photograph of a person's private parts
- The taking from an impression or cast of a wound from the person's private parts.

The police must usually destroy forensic samples after 12 months if:

- They have not charged you with an offence at that time
- A court has found you not guilty of the offence.

EVIDENCE

Evidence is anything that can be used to prove something like the *evidence* presented in a trial, or the trail of bread crumbs that is *evidence* of the path Hansel took through the woods.

The word *evidence* is derived from the Latin *evident-*, meaning "obvious." The word *evidence* shows up frequently in legal documents and dramas, because evidence is necessary proof in linking someone to a crime or crime scene.

There are four general types of evidence:

- Real evidence (tangible things, such as a weapon)
- Demonstrative (a model of what likely happened at a given time and place)
- Documentary (a letter, blog post, or other document)
- Testimonial (witness testimony)

- **Evidence** refers to information or objects that may be admitted into court for judges and juries to consider when hearing a case. **Evidence** can come from varied sources — from genetic material or trace chemicals to dental history or fingerprints.
- **Trace evidence** is created when objects contact. Material is often transferred by heat or induced by contact friction. The importance of **trace evidence** in criminal investigations was shown by Dr. Edmond Lockard in the early 20th Century.
- The Role of **Forensics** in Solving Crimes. One of the most **important** aspects of criminal justice is **forensic** science, or the practice of scientifically examining physical **evidence** collected from the scene of a crime or a person of interest in a crime.
- Lifting – This process is similar to lifting fingerprints. Investigators use the sticky side of special tape to **collect evidence**. Combing – This technique is used to comb the hair of an individual to **collect** any debris or other foreign objects, such as hair or dandruff deposited by a killer, or rapist.
- **Physical Evidence** Law and Legal Definition. **Physical evidence** usually involves objects found at the scene of a crime. ... An examination of documents found at the scene or related to the crime is often an integral part of **forensic** analysis.

8.19 SIM Technology and Functionality

SIMs are found in GSM, iDEN, and Blackberry handsets and are also used by satellite phone networks such as Iridium, Thuraya, and Inmarsat. Under the GSM framework, a cell phone is termed a Mobile Station, consisting of a SIM card and a handset (Mobile Equipment–ME). One very important and functional feature of a SIM card is that it can be moved from one GSM compatible phone to another, thereby transferring all of the subscriber's information.

The first SIM cards were about the size of a credit card. As cell phones began to shrink in size, the mini-SIM (about one-third the size of a credit card) was developed. Today an even smaller version, the micro-SIM, is available. Each of these three iterations varies in physical size and the functionality supported. Normally, a SIM card provides functionality for both the identification and authentication of the subscriber's phone to its network; contains storage for phone numbers, SMS, and other information; and allows for the creation of applications on the card itself. The basic functions are illustrated in Figure 1.

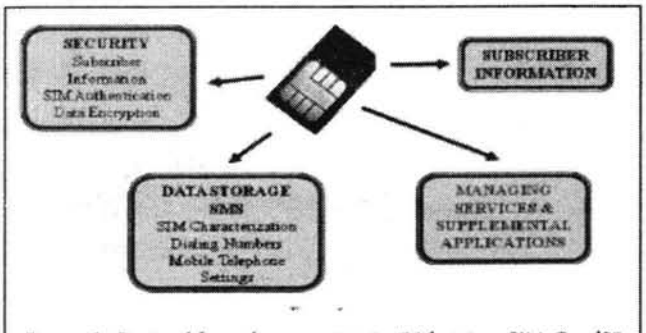


Figure 1: Derived from the narrative in "What is a SIM Card?" which can be found at: www.mpf.org.in/pdf/technology/SIM_Card_Committee_Report.pdf.

FILES PRESENT IN SIM CARD

A smart card, also known as an Integrated Circuit Card (ICC), is a micro-controller based access module. It is a physical/logical entity and can be either a Subscriber Identity Module (SIM) or a Universal Integrated Circuit Card (UICC). Originally, the ICC defined for 2G networks was the SIM. In 3G networks, the SIM may also be a logical entity (application) on a 3G UICC thereby making it functionally the same as a 2G SIM. The Universal Subscriber Identity Module (USIM) is a logical application running on a UICC smart card, which normally only accepts 3G Universal Mobile Telecommunications Service (UMTS) commands. A USIM can have multiple phone numbers assigned to it, thus allowing one phone to have multiple numbers. If the USIM and SIM applications reside on the same UICC, they cannot be active at the same time.

SIM Structure

SIMs contain both a processor (CPU) and an operating system which is either native (proprietary, vendor specific) or Java Card (a subset of the Java programming language). SIMs also have Electrically Erasable Programmable Read Only Memory (EEPROM), Random Access Memory (RAM) for controlling program execution, and persistent Read Only Memory (ROM) which stores user authentication, data encryption algorithms, the operating system, and other applications. Communication between the SIM card and the handset is via a serial interface.

A SIM card also contains a hierarchical file system which resides in EEPROM. The file structure consists of a Master File (MF), which is the root of the file system, Dedicated Files (DFs), and Elementary Files (EFs). Dedicated Files are subordinate directories under the MF, their contents and functions being defined by the GSM11.11 standards. Three are usually present: DF (DCS1800), DF (GSM), and DF (Telecom). Also present under the MF is EF (ICCID). Subordinate to each of the DFs are supporting EFs which contain the actual data. The EFs under DF (DCS1800) and DF (GSM) contain network related information and the EFs under DF (Telecom) contain the service related information. A typical SIM card file system is shown in Figure 2.

While all the files have headers, only the EFs contain data. The first byte of the header identifies the file type. Headers contain the security and meta-information related to the structure and attributes of the file, such as length of record. The body of the EFs contains information related to the application(s). Files can be either administrative or application specific and access to stored data is controlled by the operating system.

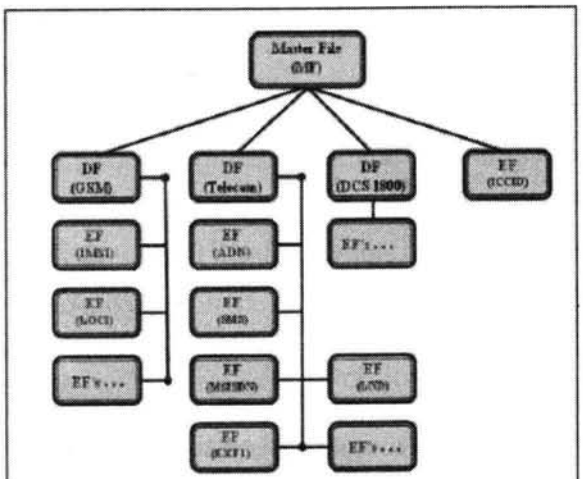


Figure 2: Modified from a diagram in the presentation "SIM Card Security" by Sheng He which included the citation: http://en.wikipedia.org/wiki/User:Sheng.He.

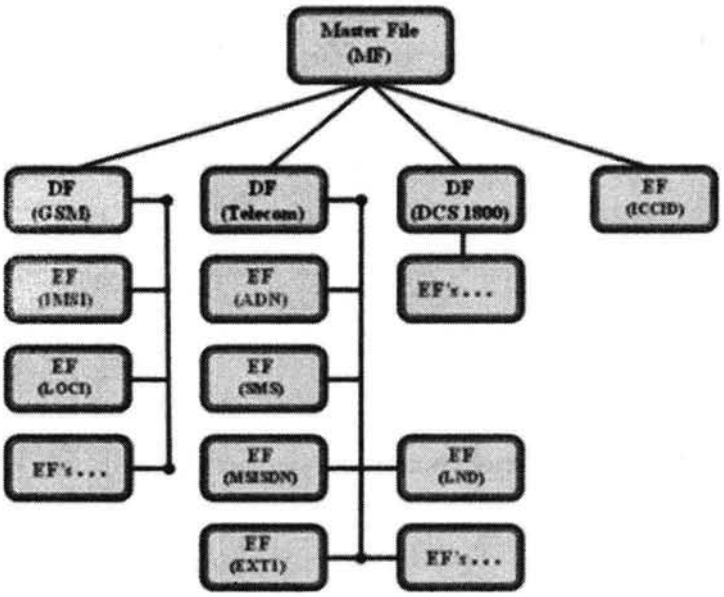
SIM CARD SECURITY

SIM SECURITY

SIM cards have built in security features that are designed to make them tamper resistant, thereby ensuring data security. A SIM card's MF, DFs, and EFs all contain security attributes. One security attribute, the access conditions, are constraints upon the execution of commands. They filter every execution attempt, thus ensuring that only those with the proper authorization can access the requested functionality controlled by the DFs or EFs. Access conditions can be thought of as somewhat analogous to the user rights associated with the file/directory attributes found in computer operating systems. There are different levels of access conditions associated with DF and EF files:

- Always (ALW): file access is allowed without restrictions and the command is executable upon the file.
- Card Holder Verification 1 (CHV1): file access is allowed with the valid verification of the users PIN1 (or PIN1 verification is disabled) and the command is executable upon the file.
- Card Holder Verification 2 (CHV2): file access is allowed with a valid verification of the user's PIN2 (or PIN2 verification is disabled) and the command is executable upon the file.
- Administrative (ADM): the administrative authority (i.e. the card issuer who provides the SIM card to subscribers), is responsible for the allocation of these levels.
- Never (NEV): file access is prohibited and the command is never executable upon the file.

Typical SIM Card File System



8.20 DEVICE DATA EXTERNAL MEMORY DUMP

Definition of: **memory dump**. **memory dump**. A display or printout of all or selected contents of RAM. After a program abends (crashes), a **memory dump** is taken in order to analyze the status of the program. The programmer looks into the**memory** buffers to see which data items were being worked on at the time of failure.

MEMORY DUMP

A memory dump is the process of taking all information content in RAM and writing it to a storage drive.

Developers commonly use memory dumps to gather diagnostic information at the time of a crash to help them troubleshoot issues and learn more about the event. Information yielded by the memory dump can help developers fix errors in operating systems and other programs of all kinds.

Some computer errors are unrecoverable because they require a reboot to regain functionality, but the information stored in RAM at the time of a crash contains the code that produced the error. Memory dumps save data that might other wise be lost to RAM's volatilenature or overwriting.

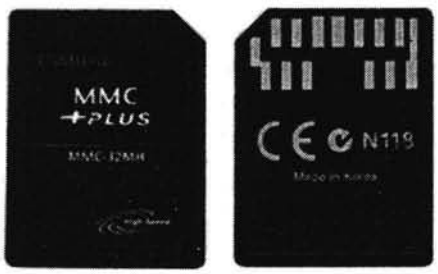
Memory dumps are seen in blue screen of death error in Microsoft operating systems. The errors display some basic suggestions, information and a faulting module while the percentage of the memory written to storage counts up. Following reboot, the memory dump can be sent to Microsoft for analysis to help the company fix the issue in updates and learn about usage.

As these dumps can include anything in the computer's active RAM, some users have privacy concerns. Furthermore, since the dumps are stored on the drive, they can also present security risks. If savvy hackers get their hands on a memory dump, they can potentially find cleartext passwords or decryption keys that normally would not be easily accessible. Some Microsoft and other operating systems allow for memory dumps that contain less information, and some make it possible to turn off memory dumps.

External memory devices are SIM cards, SD cards (commonly found within GPS devices as well as mobile phones), MMC cards, CF cards, and the Memory Stick.

EVIDENCES IN MEMORY CARD OPERATORS SYSTEMS

The **MultiMediaCard** (**MMC**) is a memory card standard used for solid-state storage. Unveiled in 1997 by SanDisk and Siemens AG, it is based on a surface contact low pin-count serial interface using a single memory stack substrate assembly, and is therefore much smaller than earlier systems based on high pin-count parallel interfaces using traditional surface mount assembly such as CompactFlash. Both products were initially introduced using SanDisk NOR-based Flash technology. MMC is about the size of a postage stamp: 24 mm × 32 mm × 1.4 mm. MMC originally used a 1-bit serial interface, but newer versions of the specification allow transfers of 4 or 8 bits at a time. MMC can be used in many devices that can use Secure Digital (SD) cards.



MEMROY CARD

An electronic flash memory storage disk commonly used in consumer electronic devices such as digital cameras, MP3 players, mobile phones, and other small portable devices.

Types of memory cards include:

- PCMCIA,
- CompactFlash,
- SD Card,
- MiniSD,
- xD-Picture Card and others. Memory cards are usually read by connecting the device containing the card to your computer, or by using a USB card reader.

A flash **memory card** (sometimes called a storage **card**) is a small storage device that **uses** nonvolatile semiconductor **memory** to store data on portable or remote computing devices. Such data includes text, pictures, audio and video.

A memory card reader is a device for accessing the data on a memory card **such** as a CompactFlash (CF), Secure Digital (SD) or Multimedia Card (MMC). Most card readers also offer write capability, and together with the card, this can function as a pen drive.

USE A MEMORY CARD FOR YOUR PHONE

1. From a Home screen, navigate: Apps > My Files. ...
2. Select an option (e.g., Images, Audio, etc.).
3. Tap the Menu icon (located in the upper-right).
4. Tap Select then select (check) the desired file(s).
5. Tap the Menu icon.
6. Tap Move.
7. Tap SD card.
8. Navigate to the preferred folder then select MOVE HERE (located in the upper-right).

Insert a micro SD Card

1. Gently pull the back cover off your device, using the slot on the side.
2. Lift the cover up and away from the device.
3. Remove your device's battery.
4. Carefully slide the card into the microSD card slot.

8.21 ANDROID FORENSICS

Android is an open source mobile device platform based on the Linux 2.6 kernel and managed by the Open Handset Alliance—a group of major mobile device, hardware, and software vendors. The open source nature of the project has not only established a new direction for the industry (forcing behemoths like Nokia/Symbian to open source their platform) but enables a developer or code savvy forensic analyst to understand the device at the most fundamental level. As the core platform is quickly maturing and is provided free of charge, carriers and hardware vendors alike can focus their efforts in customizations intended to retain their customers.

Android mobile device Applications for Android are developed in Java and run in a separate Dalvik virtual machine (DVM) with a unique user id and process which is a key mechanism used to enforce data security. Applications can only access the data within their DVM unless another application and the phone owner specifically allows the data to be shared. As a result of this secure architecture, forensic examiners do not have a built-in mechanism we can use on the phone to extract core user data. Instead, new techniques must be developed which require some interaction with the device.

Forensics Strategies for Android Devices

There are four primary ways to approach forensics on an Android device. They are:

- SD Card analysis
- Logical acquisition
- Physical acquisition
- Chip-off

Before exploring these techniques, a brief discussion on the challenges of mobile phone forensics is warranted. A fundamental goal in digital forensics is to prevent any modification of the target device by the examiner. However, mobile phones lack traditional hard drives which can be shutdown, connected to a write blocker, and imaged in a forensically sound way. The end result is that Android forensic techniques, short of chip-off, do alter the device. Examiners must use their discretion when examining a mobile device and if the device is modified, they must explain how it was modified and, as important, why that choice was made.

SD Card Analysis

Nearly every Android device comes with an external SD Card for storing data. Upon receiving and securing an Android device (as you would any other mobile device), an examiner should remove the SD Card and process it in the standard way. The card is formatted with a FAT32 file system.

Logical Analysis

The logical acquisition of an Android device is the technique we recommended first. This technique involves copying a small (~25k) Android Forensics application to the device, running the application, and then removing it from the device. An application, written by viaForensics and distributed for free to law enforcement and government agencies charged with digital forensic responsibilities, currently acquires the following information:

1. Browser history
2. Call Logs
3. Contact Methods

4. External Image Media (meta data)
5. External Image Thumbnail Media (meta data)
6. External Media, Audio, and Misc. (meta data)
7. External Videos (meta data)
8. MMS
9. MMS Parts (includes full images sent via MMS)
10. Organizations
11. People
12. SMS
13. List of all applications installed and version
14. Contacts Extensions
15. Contacts Groups
16. Contacts Phones
17. Contacts Settings

And new data sources are being developed weekly. The data is written to an SD Card the examiner placed into the device. The files are currently written as CSV, however we will likely change this to an XML format. Also, there are some challenges when interpreting this data and we are currently developing viaExtract, a reporting application for the data. The application will be released in the next few months and sold at significant discount to active law enforcement.

Physical Analysis

In some cases, a more significant analysis is required. To this end, we have developed a technique to physically acquire a "dd" image from support Android devices (currently any Android 1.5 devices and Motorola Droid 2.0 and 2.01). This technique requires root privileges on the device and can yield a significant amount of information. This technique will provide a forensic image of the various user data partitions. These partitions use the open source file system YAFFS2 (Yet another Flash File System 2) and is one of the significant challenges with the Android platform.

YAFFS2 was built specifically for the growing NAND memory devices and has a number of important features which address the stringent needs of this medium. It is a log-structured file system, provides built in wear-leveling and error correction, is fast, and has a small footprint in RAM. However, since its usage was limited prior to

Android, no commercial forensic product supports the file system.For the brave, you can download the YAFFS2 source code, grab a forensic image of a partition, open it up in your favorite hex editor and start digging. However, we are making progress in the development of some tools. The tools allow an examiner to forensically acquire the NAND data (you cannot use dd for this...we've developed a special nanddump program for this purpose), mount the image in Linux (using nandsim) and extract the data. Traditional techniques such as file carving and strings also work. However, the real potential is in the development of a program which will provide a "point-in-time" version of any file on the YAFFS2 file system; this is a very fortunate (for the forensic examiner) byproduct of YAFFS2 being a log-structured file system.

Chip-off

For those with full lab facilities, there is always the option of using chip-off techniques on the NAND memory.

8.22 PROCEDURES FOR HANDLING AN ANDROID DEVICES

The concept of Android forensics consists of techniques to extract the most possible data from the device without losing, or altering the content of the device. Modification of the data or data preservation is the biggest problem when dealing with Android devices.

The technique that is most recommended is live acquisition due to the volatile nature of the device's memory. Live acquisition is recommended because the volatile memory can hold various data which could be of value for the investigation.

The examples of data that could be found in the volatile, RAM memory are:

- Passwords
- Encryption keys
- Usernames
- Application data
- Data from system processes and services

There is a technique developed by security engineer Thomas Cannon which helps acquiring significant application data. The technique is using the Android's ability to dump the application memory to a file by sending the application a special signal - SIGUSR1 (Hoog, 2011). Tendencies are that there will be more solutions to help analysis of the Android memory in the future.

Procedures for handling an Android device

Procedures for handling the Android device are the same as the procedures for handling the personal computer or lap top. The procedures still have five steps that are very important to hold on to while handling the device. The five steps are:

- Identifying
- Preserving
- Acquiring
- Analyzing
- Reporting

As in the computer forensic investigation, the chain of custody must be followed as well. Regardless of whether the investigation is in the corporate environment or is a part of the criminal investigation, it is necessary to follow the rules for evidence handling. Any case in any time can end up in court. The best practice is that investigation should always be conducted as the case will be in the court of law. The important considerations while conducting the Android device investigation are:

• Chain of custody

• Detailed notes and final reports

Validation of results by different tools or examiners

• Fact or opinion based testimony (Hoog, 2011).

Andrew Hoog thinks the four principles of electronic based computer evidence are of the essence. The four principles are:

1. No action taken by law enforcement agencies or their agents should change data held on a computer or storage media, which may subsequently be relied upon in court.

2. In circumstances where a person finds it necessary to access original data held on a computer or on the storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

3. An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result. 4. The person in charge of the investigation (the case officer) has overall responsibility for ensuring that law and these principles are adhered to. (Hoog, 2011)

Handling the Android device is different than handling personal Computer in the investigation. The nature of the handheld device that loses some important data if powered off makes the distinction from personal computer handling. It is also very important to secure device from locking down, accessing network or losing power.

Techniques for securing the device vary from pass code procedures, through powering, to network isolation. On most Android devices, pass code locking could be circumvented by:

1. Increasing the timeout to prevent or postpone the screen locking.

2. Enabling the USB debugging and "stay awake".

8.23 IMAGING ANDROID USB MASS STORAGE DEVICE

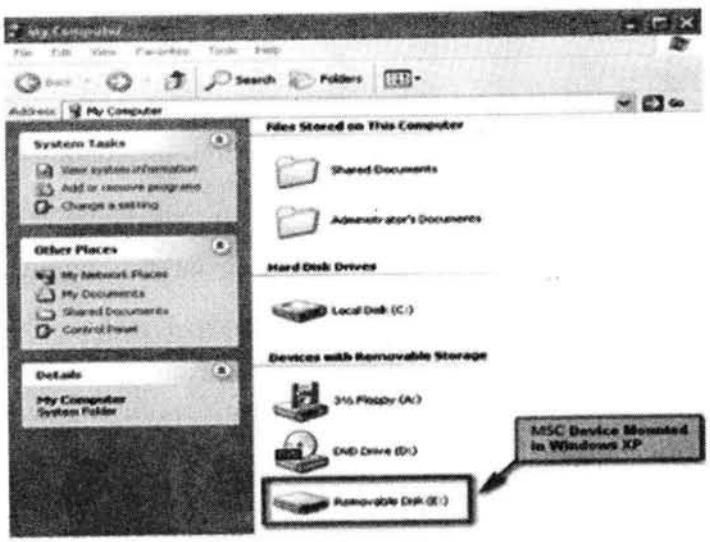
USB Mass Storage Class

Most of the forensic research and information for inserted USB devices has focused on MSC devices. Classic examples of these devices include: external drives, thumb/flash drives, and MP3 players. Within Windows, MSC devices are supported in Windows 2000 and onward.

MSC is a transfer protocol that allows mounting of a device's storage area as removable media, and provides direct access to sectors of data for reading and writing. Mounting of these devices occurs at the physical level, where if one were to open a mounted partition with a hex editor, all areas of the filesystem are available for view.

For MSC devices with embedded operating systems such as cameras, smart phones, tablets and MP3 players, the storage area or partition must first be unmounted from within the device's OS before it can be enumerated or mounted in Windows.

An MSC device mounted in Windows XP appears in Windows Explorer under "Devices with Removable Storage", and is assigned the next available drive letter.



MSC Device in Windows XP

With Android phones, before the release of Ice Cream Sandwich (Android 4.0), phones were more likely to use MSC as their transport protocol. With Ice Cream Sandwich and later, MTP (Media Transport Protocol) has become the standard transfer protocol used.

CHAPTER – 9

9.1 INTRODUCTION TO CYBER SECURITY

A Definition of Cyber Security

Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security.

The Importance of Cyber Security

Cyber security is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and cyber security describes the discipline dedicated to protecting that information and the systems used to process or store it. As the volume and sophistication of cyber attacks grow, companies and organizations, especially those that are tasked with safeguarding information relating to national security, health, or financial records, need to take steps to protect their sensitive business and personnel information. As early as March 2013, the nation's top intelligence officials cautioned that cyber attacks and digital spying are the top threat to national security, eclipsing even terrorism.

Challenges of Cyber Security

For an effective cyber security, an organization needs to coordinate its efforts throughout its entire information system. Elements of cyber encompass all of the following:

- **Network security**
- **Application security**
- **Endpoint security**
- **Data security**
- **Identity management**
- **Database and infrastructure security**
- **Cloud security**
- **Mobile security**
- **Disaster recovery/business continuity planning**
- **End-user education**

The most difficult challenge in cyber security is the ever-evolving nature of security risks themselves. Traditionally, organizations and the government have focused most of their cyber security resources on perimeter security to protect only their most crucial system components and defend against known treats. Today, this approach is insufficient, as the threats advance and change more quickly than organizations can keep up with. As a result, advisory organizations promote more proactive and adaptive approaches to cyber security. Similarly, the National Institute of Standards and Technology (NIST) issued guidelines in its risk assessment framework that recommend a shift toward continuous monitoring and real-time assessments, a data-focused approach to security as opposed to the traditional perimeter-based model.

Managing Cyber Security

The National Cyber Security Alliance, through SafeOnline.org, recommends a top-down approach to cyber security in which corporate management leads the charge in prioritizing cyber security management across all business practices. NCSA advises that companies must be prepared to "respond to the inevitable cyber incident, restore normal operations, and ensure that company assets and the company's reputation are protected." NCSA's guidelines for conducting cyber risk assessments focus on three key areas: identifying your organization's "crown jewels," or your most valuable information requiring protection; identifying the threats and risks facing that information; and outlining the damage your organization would incur should that data be lost or wrongfully exposed. Cyber risk assessments should also consider any regulations that impact the way your company collects, stores, and secures data, such as PCI-DSS, HIPAA, SOX, FISMA, and others. Following a cyber risk assessment, develop and implement a plan to mitigate cyber risk, protect the "crown jewels" outlined in your assessment, and effectively detect and respond to security incidents. This plan should encompass both the processes and technologies required to build a mature cyber security program. An ever-evolving field, cyber security best practices must evolve to accommodate the increasingly sophisticated attacks carried out by attackers. Combining sound cyber security measures with an educated and security-minded employee base provides the best defense against cyber criminals attempting to gain access to your company's sensitive data. While it may seem like a daunting task, start small and focus on your most sensitive data, scaling your efforts as your cyber program matures.

9.2 THE SECURITY PROBLEM IN COMPUTING

The meaning of computer security

The meaning of the term computer security has evolved in recent years. Before the problem of data security became widely publicized in the media, most people's idea of computer security focused on the physical machine. Traditionally, computer facilities have been physically protected for three reasons:

- To prevent theft of or damage to the hardware
- To prevent theft of or damage to the information
- To prevent disruption of service

Computer security is security applied to computing devices such as computers and smartphones, as well as computer networks such as private and public networks, including the whole Internet. The field covers all the processes and mechanisms by which digital equipment, information and services are protected from unintended or unauthorized access, change or destruction, and are of growing importance in line with the increasing reliance on computer systems of most societies worldwide. It includes physical security to prevent theft of equipment, and information security to protect the data on that equipment. It is sometimes referred to as "cyber security" or "IT security", though these terms generally do not refer to physical security (locks and such).

Some important terms used in computer security are:

Vulnerability

Vulnerability is a weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw. To exploit vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerability is also known as the attack surface.

Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities.This practice generally refers to software vulnerabilities in computing systems.

Backdoors

A backdoor in a computer system, is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice), or could be a modification to an existing program or hardware device. It may also fake information about disk and memory usage.

Denial-of-service attack

Unlike other exploits, denials of service attacks are not used to gain unauthorized access or control of a system. They are instead designed to render it unusable. Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once. These types of attack are, in practice, very hard to prevent, because the behaviour of whole networks needs to be analyzed, not only the behaviour of small pieces of code. Distributed denial of service (DDoS) attacks are common, where a large number of compromised hosts (commonly referred to as "zombie computers", used as part of a botnet with, for example; a worm, trojan horse, or backdoor exploit to control them) are used to flood a target system with network requests, thus attempting to render it unusable through resource exhaustion.

Direct-access attacks

An unauthorized user gaining physical access to a computer (or part thereof) can perform many functions, install different types of devices to compromise security, including operating system modifications, software worms,

key loggers, and covert listening devices. The attacker can also easily download large quantities of data onto backup media, for instance CD-R/DVD-R, tape; or portable devices such as key drives, digital cameras or digital audio players. Another common technique is to boot an operating system contained on a CD-ROM or other bootable media and read the data from the hard drive(s) this way. The only way to defeat this is to encrypt the storage media and store the key separate from the system. Direct-access attacks are the only type of threat to Standalone computers (never connect to internet), in most cases.

Eavesdropping

Eavesdropping is the act of surreptitiously listening to a private conversation, typically between hosts on a network. For instance, programs such as Carnivore and NarusInsight have been used by the FBI and NSA to eavesdrop on the systems of internet service providers.

Spoofing

Spoofing of user identity describes a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

Tampering

Tampering describes an intentional modification of products in a way that would make them harmful to the consumer.

Repudiation

Repudiation describes a situation where the authenticity of a signature is being challenged.

Information disclosure

Information Disclosure (Privacy breach or Data leak) describes a situation where information, thought as secure, is released in an untrusted environment.

Elevation of privilege

Elevation of Privilege describes a situation where a person or a program want to gain elevated privileges or access to resources that are normally restricted to him/it.

Exploits

An exploit is a piece of software, a chunk of data, or sequence of commands that takes advantage of a software "bug" or "glitch" in order to cause unintended or unanticipated behaviour to occur on computer software, hardware, or something electronic (usually computerized). This frequently includes such things as gaining control of a computer system or allowing privilege escalation or a denial of service attack. The term "exploit" generally refers to small programs designed to take advantage of a software flaw that has been discovered, either remote or local. The code from the exploit program is frequently reused in Trojan horses and computer viruses.

Indirect attacks

An indirect attack is an attack launched by a third-party computer. By using someone else's computer to launch an attack, it becomes far more difficult to track down the actual attacker. There have also been cases where attackers took advantage of public anonymizing systems, such as the tor onion router system.

Computer crime: Computer crime refers to any crime that involves a computer and a network.

Top 10 Cyber Crime Prevention Tips

1. **Use Strong Passwords** Use different user ID / password combinations for different accounts and avoid writing them down. Make the passwords more complicated by combining letters, numbers, special characters (minimum 10 characters in total) and change them on a regular basis.

2. **Secure your computer**

o **Activate your firewall** Firewalls are the first line of cyber defence; they block connections to unknown or bogus sites and will keep out some types of viruses and hackers.

o **Use anti-virus/malware software** Prevent viruses from infecting your computer by installing and regularly updating anti-virus software.

o **Block spyware attacks** Prevent spyware from infiltrating your computer by installing and updating anti-spyware software.

3. **Be Social-Media Savvy** Make sure your social networking profiles (e.g. Facebook, Twitter, Youtube, MSN, etc.) are set to private. Check your security settings. Be careful what information you post online. Once it is on the Internet, it is there forever!

4. **Secure your Mobile Devices** Be aware that your mobile device is vulnerable to viruses and hackers. Download applications from trusted sources.

5. **Install the latest operating system updates** Keep your applications and operating system (e.g. Windows, Mac, Linux) current with the latest system updates. Turn on automatic updates to prevent potential attacks on older software.

6. **Protect your Data** Use encryption for your most sensitive files such as tax returns or financial records, make regular back-ups of all your important data, and store it in another location.

7. **Secure your wireless network** Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Public Wi-Fi, a.k.a. "Hot Spots", are also vulnerable. Avoid conducting financial or corporate transactions on these networks.

8. **Protect your e-identity** Be cautious when giving out personal information such as your name, address, phone number or financial information on the Internet. Make sure that websites are secure (e.g. when making online purchases) or that you've enabled privacy settings (e.g. when accessing/using social networking sites).

9. **Avoid being scammed** Always think before you click on a link or file of unknown origin. Don't feel pressured by any emails. Check the source of the message. When in doubt, verify the source. Never reply to emails that ask you to verify your information or confirm your user ID or password.

10. **Call the right person for help** Don't panic! If you are a victim, if you encounter illegal Internet content (e.g. child exploitation) or if you suspect a computer crime, identity theft or a commercial scam, report this to your local police. If you need help with maintenance or software installation on your computer, consult with your service provider or a certified computer technician.

Principle security

There are five principles of security. They are as follows:

1. *Confidentiality:*

The principle of confidentiality specifies that only the sender and the intended recipient should be able to access the content of the message.

2. *Integrity:*

The confidential information sent by A to B which is accessed by C without the permission or knowledge of A and B.

3. *Authentication:*

Authentication mechanism helps in establishing proof of identification.

Non-repudiation:

4. *Access control:*

Access control specifies and control who can access what.

5. *Availability:*

It means that assets are accessible to authorized parties at appropriate times.

Attacks

We want our security system to make sure that no data are disclosed to unauthorized parties.

- Data should not be modified in illegitimate ways
- Legitimate user can access the data

Types of attacks

Attacks are grouped into two types:

- P*assive attacks:* does not involve any modification to the contents of an original message
- *Active attacks:* the contents of the original message are modified in some ways.

9.3 SECURITY PLANNING:

Contents of security planning:

A security plan identifies and organizes the security activities for a computing system. The plan is both a description of the current situation and a plan for improvement. Every security plan must address seven issues.

1. P*olicy*, indicating the goals of a computer security effort and the willingness of the people involved to work to achieve those goals

2. *Current state*, describing the status of security at the time of the plan

3. Requirements, recommending ways to meet the security goals

4. R*ecommended controls*, mapping controls to the vulnerabilities identified in the policy and requirements

5. *Accountability*, describing who is responsible for each security activity

6. *Timetable*, identifying when different security functions are to be done

7. *Continuing attention*, specifying a structure for periodically updating the security plan

Policy:

The policy statement should specify the following:

The organization's *goals* on security. For example, should the system protect data from leakage to outsiders, protect against loss of data due to physical disaster, protect the data's integrity, or protect against loss of business when computing resources fail?

What is the higher priority: serving customers or securing data?

Where the *responsibility* for security lies. For example, should the responsibility rest with a small computer security group, with each employee, or with relevant managers?

The organization's *commitment* to security. For example, who provides security support for staff, and where does security fit into the organization's structure?

Current Security Status:

To be able to plan for security, an organization must understand the vulnerabilities to which it may be exposed. The organization can determine the vulnerabilities by performing a risk analysis: a careful investigation of the system, its environment, and the things that might go wrong. The risk analysis forms the basis for describing the current status of security. The status can be expressed as a listing of organizational assets, the security threats to the assets, and the controls in place to protect the assets.

The status portion of the plan also defines the limits of responsibility for security. It describes not only which assets are to be protected but also who is responsible for protecting them. The plan may note that some groups may be excluded from responsibility; for example, joint ventures with other organizations may designate one organization to provide security for all member organizations. The plan also defines the boundaries of responsibility, especially when networks are involved. For instance, the plan should clarify who provides the security for a network router or for a leased line to a remote site.

Even though the security plan should be thorough, there will necessarily be vulnerabilities that are not considered. These vulnerabilities are not always the result of ignorance rather, they can arise from the addition of new equipment or data as the system evolves.

They can also result from new situations, such as when a system is used in ways not anticipated by its designers. The security plan should detail the process to be followed when someone identifies a new vulnerability. In particular, instructions should explain how to integrate controls for that vulnerability into the existing security procedures.

Requirements:

The heart of the security plan is its set of security requirements: functional or performance demands placed on a system to ensure a desired level of security. The requirements are usually derived from organizational needs. Sometimes these needs include the need to conform to specific security requirements imposed from outside, such as by a government agency or a commercial standard.

Recommended Controls:

The security requirements lay out the system's needs in terms of what should be protected. The security plan must also recommend what controls should be incorporated into the system to meet those requirements. Throughout this book you have seen many examples of controls, so we need not review them here. As we see later in this chapter, we can use risk analysis to create a map from vulnerabilities to controls. The mapping tells us how the system will meet the security requirements. That is, the recommended controls address implementation issues: how the system will be designed and developed to meet stated security requirements.

Responsibility for Implementation:

A section of the security plan should identify which people are responsible for implementing the security requirements. This documentation assists those who must coordinate their individual responsibilities with those of

other developers. At the same time, the plan makes explicit who is accountable should some requirement not be met or some vulnerability not be addressed. That is, the plan notes who is responsible for implementing controls when a new vulnerability is discovered or a new kind of asset is introduced.

People building, using, and maintaining the system play many roles. Each role can take some responsibility for one or more aspects of security. Consider, for example, the groups listed here.

Personal computer users may be responsible for the security of their own machines. Alternatively, the security plan may designate one person or group to be coordinator of personal computer security.

Project leaders may be responsible for the security of data and computations.

***Timetable*:**

A comprehensive security plan cannot be executed instantly. The security plan includes a timetable that shows how and when the elements of the plan will be performed. These dates also give milestones so that management can track the progress of implementation.

Continuing Attention:

Good intentions are not enough when it comes to security. We must not only take care in defining requirements and controls, but we must also find ways for evaluating a system's security to be sure that the system is as secure as we intend it to be. Thus, the security plan must call for reviewing the security situation periodically. As users, data, and equipment change, new exposures may develop. In addition, the current means of control may become obsolete or ineffective (such as when faster processor times enable attackers to break an encryption algorithm). The inventory of objects and the list of controls should periodically be scrutinized and updated, and risk analysis performed anew.

Security Planning Team Members:

The membership of a computer security planning team must somehow relate to the different aspects of computer security described in this book. Security in operating systems and networks requires the cooperation of the systems administration staff. Program security measures can be understood and recommended by applications programmers. Physical security controls are implemented by those responsible for general physical security, both against human attacks and natural disasters. Finally, because controls affect system users, the plan should incorporate users' views, especially with regard to usability and the general desirability of controls.

Thus, no matter how it is organized, a security planning team should represent each of the following groups.

- Computer hardware group
- System administrators
- Systems programmers

- Applications programmers
- Data entry personnel
- Physical security personnel
- Representative users

In some cases, a group can be adequately represented by someone who is consulted at appropriate times, rather than a committee member from each possible constituency being enlisted.

Assuring Commitment To a security plan:

After the plan is written, it must be accepted and its recommendations carried out. Acceptance by the organization is key; a plan that has no organizational commitment is simply a plan that collects dust on the shelf. Commitment to the plan means that security functions will be implemented and security activities carried out. Three groups of people must contribute to making the plan a success.

The planning team must be sensitive to the needs of each group affected by the plan. Those affected by the security recommendations must understand what the plan means for the way they will use the system and perform their business activities. In particular, they must see how what they do can affect other users and other systems.

Management must be committed to using and enforcing the security aspects of the system.

Management commitment is obtained through understanding. But this understanding is not just a function of what makes sense technologically; it also involves knowing the cause and the potential effects of lack of security. Managers must also weigh tradeoffs in terms of convenience and cost. The plan must present a picture of how cost effective the controls are, especially when compared to potential losses if security is breached without the controls. Thus, proper presentation of the plan is essential, in terms that relate to management as well as technical concerns.

Management is often reticent to allocate funds for controls until the value of those controls is explained. As we note in the next section, the results of a risk analysis can help communicate the financial tradeoffs and benefits of implementing controls. By describing vulnerabilities in financial terms and in the context of ordinary business activities (such as leaking data to a competitor or an outsider), security planners can help managers understand the need for controls.

The plans we have just discussed are part of normal business. They address how a business handles computer security needs. Similar plans might address how to increase sales or improve product quality, so these planning activities should be a natural part of management.

Next we turn to two particular kinds of business plans that address specific security problems: coping with and controlling activity during security incidents.

Business Continuity Plan:

A business continuity plan documents how a business will continue to function during a computer security incident. An ordinary security plan covers computer security during normal times and deals with protecting against a wide range of vulnerabilities from the usual sources.

A business continuity plan deals with situations having two characteristics:

- ***Catastrophic situations***, in which all or a major part of a computing capability is suddenly unavailable
- ***Long duration***, in which the outage is expected to last for so long that business will suffer

There are many situations in which a business continuity plan would be helpful. Here are some examples that typify what you might find in reading your daily newspaper:

- A fire destroys a company's entire network.
- A seemingly permanent failure of a critical software component renders the computing system unusable.
- A business must deal with the abrupt failure of its supplier of electricity, telecommunications, network access, or other critical service.
- A flood prevents the essential network support staff from getting to the operations center.

The key to coping with such disasters is advance planning and preparation, identifying activities that will keep a business viable when the computing technology is disabled. The steps in business continuity planning are these:

- Assess the business impact of a crisis.
- Develop a strategy to control impact.
- Develop and implement a plan for the strategy

Incident response plan:

Incident response Plan should be

- define what constitutes an *incident*
- identify who is responsible for *taking charge* of the situation
- describe the plan of *action*

9.4 CYBER SECURITY LAWS

Indian Cybersecurity Law

India's Information Technology Act of 2000 (IT Act) addresses the protection of electronic data and computer-related offenses (e.g., hacking and tampering with computer source documents)

• Under 2008 amendments, IT Act does not criminalize hacking, but prohibits computer- related fraud and tampering with computer source documents. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules – "Privacy Rules" Together, IT Act and Privacy Rules impose cyber requirements on companies.

• "Reasonable Security Practices" interpreted as operation of documented, comprehensive information security program, policies, and procedures

• Parties can specify "reasonable security practices" in contract.

United States Cybersecurity Law

Cybersecurity legal parameters arise from multiple layers and sources.

• Federal law

- Computer Fraud and Abuse Act prohibits unauthorized computer access, interference, obtaining data
- Electronic Communications Privacy Act governs interception, access to data

• State law — fills gaps in federal law, but can set de facto national standards

• Example: Massachusetts data breach requirement triggered by a (1) substantial risk of identity theft or fraud (2) OR acquisition or use for an unauthorized purpose

❖ Companies handling sensitive personal data must have Written Information Security Policy; encryption of personal data transmitted externally; and specific minimum "administrative, technical, and physical" security controls.

U.S. Cybersecurity Law Critical Infrastructure and Information Sharing

- Enhancing cybersecurity for "critical infrastructure" has been a key focus of the Obama administration.
- February 2013: Executive Order 13636
  - Identifies 16 critical infrastructure areas
  - Regulators directed to review existing authorities and act to improve cybersecurity among regulated entities

• February 2014: NIST releases Cybersecurity Framework and CI Cyber Community ("C³")

Cybersecurity Act of 2015:

- Information-Sharing through DHS Portal. Establishes a voluntary framework for confidential, two-way sharing of cyber threat information between private sector and U.S. government, via a Department of Homeland Security portal; offers protection from liability for sharing

U.S. Cybersecurity Law Protecting Personal Information

Companies have generally applicable legal obligations to protect personal information.

• Data Security: Massachusetts data security law requires specific affirmative acts

• Data Breach Notification: State laws generally require alerts to state regulators and impacted individuals if breach involving personal data.

Companies may not make "deceptive" data security claims or engage in "unfair" data security practices. Policed by Federal Trade Commission and state regulators.

In certain sectors, specific laws impose additional layer of security duties for certain categories of sensitive personal data.

• Financial Services: Gramm-Leach-Bliley Act (Nonpublic Personal Information, "NPI")

• Healthcare: HIPAA (Protected Health Information, "PHI" and "ePHI")

• Telecommunications Carriers: Communications Act (Customer Proprietary Network Information, "CPNI")

United Kingdom Cybersecurity Law

Computer Misuse Act of 1990 (Amended in 2006)

• Prohibits hacking, unauthorised access to computer systems, and purposefully spreading malware. Enforcement

• UK ICO can issue an Enforcement Notice for breach of the data protection principles in the UK Data Protection Act of 1998. (This will change GDPR in 2018.)

• Staysure.com.uk (2015): Fine of £175,000 on holiday insurance company for inadequate security systems and policy, causing breach of credit card data of 90,000+ customers

• Worldview Limited (2014): Fine of £7,500 for vulnerability in company's website, enabling hackers to access payment card data of 3,500+ customers.

9.5 COPY RIGHT, INTERNET INFRINGEMENT, FAIR USE

A **copyright** is a form of legal protection automatically provided to the authors or creators of original works. Copyright protection is vast and very inclusive. It applies to items such as original literary, dramatic, musical, choreographic, photographic, architectural, and artistic works.

It's important to note, though, that ideas can't be copyrighted. Copyright protection only applies to tangible forms of expression. For example, let's say that I have an idea for a song. I've been working on the lyrics in my head. These lyrics aren't copyrighted. Then, late one night I jot down a few verses of the song on a notepad. These verses are automatically copyrighted because they're an original and creative work that's now been expressed in a tangible form. I don't have to actually publish this work in order to have copyright protection. Also, note that the copyright belongs to me, since I'm the author or creator. But, let's say that I write songs as a part of my job, and I'm writing this song in the capacity of my employment. In this case, my employer will automatically own the copyright.

Copyright protection automatically attaches once an original work is expressed in tangible form. This is known as an **unregistered copyright** and is represented by the circle c designation. An unregistered copyright allows an author the exclusive right to reproduce, sell and perform his or her copyrighted work. This means that an author or creator could sue for an **injunction** to prohibit, or cease, the unauthorized use of the material. Mike Tyson's tattoo artist asked for, but was denied, an injunction. He wanted to stop the movie from b being shown since it featured his copyrighted work without his permission.

Copyright Infringement

In order to bring a lawsuit for copyright infringement, the author or creator must first register his or her copyright with the U.S. Copyright Office. This requires filing an application and paying a fee. A **registered copyright** is designated with a circle r symbol. Generally, it allows the author or creator the exclusive right to control the use of the material for his or her entire lifetime. A registered copyright won't expire for another 70 years after the author's death. The author can designate the owner of the copyright through his or her will, just like any other property right.

Like an unregistered copyright, these rights include:

- The right to reproduce, copy, or distribute the original work;
- The right to create new works based on the original work;
- The right to perform the work; and
- The right to publicly display the work.

The registered, copyrighted material becomes an official government record. Once a copyright is registered, the author is protected under the **Federal Copyright Act**. This is the main set of laws that govern copyright

infringement. Copyright infringement is a federal tort. A registered copyright holder can bring a lawsuit for copyright infringement and ask for an injunction, money damages and attorney's fees should any of the author's copyright privileges be violated. This is considered to be an added level of protection over that afforded for an unregistered copyright, as these are additional remedies provided to an author holding a registered copyright. For these reasons, registration is recommended.

Exceptions to Infringement

It's important to note that not all unauthorized uses of copyrighted material will amount to copyright infringement. A party can use copyrighted material without the author's authorization if the material is used for fair use.

Fair use is any copying of copyrighted material done for a limited and transformative purpose, such as to comment up

Fair Use

Fair use is a copyright principle based on the belief that the public is entitled to freely use portions of copyrighted materials for purposes of commentary and criticism. For example, if you wish to criticize a novelist, you should have the freedom to quote a portion of the novelist's work without asking permission. Absent this freedom, copyright owners could stifle any negative comments about their work.

Unfortunately, if the copyright owner disagrees with your fair use interpretation, the dispute may have to be resolved by a lawsuit or arbitration. If it's not a fair use, then you are infringing upon the rights of the copyright owner and may be liable for damages.

The only guidance for fair use is provided by a set of factors outlined in copyright law. These factors are weighed in each case to determine whether a use qualifies as a fair use. For example, one important factor is whether your use will deprive the copyright owner of income. Unfortunately, weighing the fair use factors is often quite subjective. For this reason, the fair use road map can be tricky to navigate.

CHAPTER 10

10.1 NETWORK SECURITY

Types and Sources Of Network Threats

Now, we've covered enough background information on networking that we can actually get into the security aspects of all of this. First of all, we'll get into the types of threats there are against networked computers, and then some things that can be done to protect yourself against various threats.

Denial-of-Service

DoS (Denial-of-Service) attacks are probably the nastiest, and most difficult to address. These are the nastiest, because they're very easy to launch, difficult (sometimes impossible) to track, and it isn't easy to refuse the requests of the attacker, without also refusing legitimate requests for service.

The premise of a DoS attack is simple: send more requests to the machine than it can handle. There are toolkits available in the underground community that make this a simple matter of running a program and telling it which host to blast with requests. The attacker's program simply makes a connection on some service port, perhaps forging the packet's header information that says where the packet came from, and then dropping the connection. If the host is able to answer 20 requests per second, and the attacker is sending 50 per second, obviously the host will be unable to service all of the attacker's requests, much less any legitimate requests (hits on the web site running there, for example).

Such attacks were fairly common in late 1996 and early 1997, but are now becoming less popular.

Some things that can be done to reduce the risk of being stung by a denial of service attack include

- Not running your visible-to-the-world servers at a level too close to capacity
- Using packet filtering to prevent obviously forged packets from entering into your network address space.

Obviously forged packets would include those that claim to come from your own hosts, addresses reserved for private networks as defined in RFC 1918 [4], and the *loopback* network (127.0.0.0).

- Keeping up-to-date on security-related patches for your hosts' operating systems.

Unauthorized Access

"Unauthorized access" is a very high-level term that can refer to a number of different sorts of attacks. The goal of these attacks is to access some resource that your machine should not provide the attacker. For example, a host might be a web server, and should provide anyone with requested web pages. However, that host should not provide command shell access without being sure that the person making such a request is someone who should get it, such as a local administrator.

Executing Commands Illicitly

It's obviously undesirable for an unknown and untrusted person to be able to execute commands on your server machines. There are two main classifications of the severity of this problem: normal user access, and administrator access. A normal user can do a number of things on a system (such as read files, mail them to other people, etc.) that an attacker should not be able to do. This might, then, be all the access that an attacker needs. On the other hand, an attacker might wish to make configuration changes to a host (perhaps changing its IP address, putting a start-up script in place to cause the machine to shut down every time it's started, or something similar). In this case, the attacker will need to gain administrator privileges on the host.

Confidentiality Breaches

We need to examine the threat model: what is it that you're trying to protect yourself against? There is certain information that could be quite damaging if it fell into the hands of a competitor, an enemy, or the public. In these cases, it's possible that compromise of a normal user's account on the machine can be enough to cause damage (perhaps in the form of PR, or obtaining information that can be used against the company, etc.)

While many of the perpetrators of these sorts of break-ins are merely thrill-seekers interested in nothing more than to see a shell prompt for your computer on their screen, there are those who are more malicious, as we'll consider next. (Additionally, keep in mind that it's possible that someone who is normally interested in nothing more than the thrill could be persuaded to do more: perhaps an unscrupulous competitor is willing to hire such a person to hurt you.)

Destructive Behavior

Among the destructive sorts of break-ins and attacks, there are two major categories.

Data Diddling.

The data diddler is likely the worst sort, since the fact of a break-in might not be immediately obvious. Perhaps he's toying with the numbers in your spreadsheets, or changing the dates in your projections and plans. Maybe he's changing the account numbers for the auto-deposit of certain paychecks. In any case, rare is the case when you'll come in to work one day, and simply know that something is wrong. An accounting procedure might turn up a discrepancy in the books three or four months after the fact. Trying to track the problem down will certainly be difficult, and once *that* problem is discovered, how can any of your numbers from that time period be trusted? How far back do you have to go before you think that your data is safe?

Data Destruction.

Some of those perpetrate attacks are simply twisted jerks who like to delete things. In these cases, the impact on your computing capability — and consequently your business — can be nothing less than if a fire or other disaster caused your computing equipment to be completely destroyed.

10.2 FIREWALLS

As we've seen in our discussion of the Internet and similar networks, connecting an organization to the Internet provides a two-way flow of traffic. This is clearly undesirable in many organizations, as proprietary information is often displayed freely within a corporate *intranet* (that is, a TCP/IP network, modeled after the Internet that only works within the organization).

In order to provide some level of separation between an organization's intranet and the Internet, *firewalls* have been employed. A firewall is simply a group of components that collectively form a barrier between two networks.

(1) Intelligent devices generally known as "Firewalls" shall be used to isolate organisation's data network with the external network. Firewall device should also be used to limit network connectivity for unauthorized use.

(2) Networks that operate at varying security levels shall be isolated from each other by appropriate firewalls. The internal network of the organization shall be physically and logically isolated from the Internet and any other external connection by a firewall.

(3) All firewalls shall be subjected to thorough test for vulnerability prior to being put to use and at least half-yearly thereafter.

(4) All web servers for access by Internet users shall be isolated from other data and host servers.

The following components encompass the firewalls:

Bastion host.

A general-purpose computer used to control access between the internal (private) network (intranet) and the Internet (or any other untrusted network). Typically, these are hosts running a flavor of the Unix operating system that has been customized in order to reduce its functionality to only what is necessary in order to support its functions. Many of the general-purpose features have been turned off, and in many cases, completely removed, in order to improve the security of the machine.

Router.

A special purpose computer for connecting networks together. Routers also handle certain functions, such as *routing* , or managing the traffic on the networks they connect.

Access Control List (ACL).

Many routers now have the ability to selectively perform their duties, based on a number of facts about a packet that comes to it. This includes things like origination address, destination address, destination service port, and so on. These can be employed to limit the sorts of packets that are allowed to come in and go out of a given network.

Demilitarized Zone (DMZ).

The DMZ is a critical part of a firewall: it is a network that is neither part of the untrusted network, nor part of the trusted network. But, this is a network that connects the untrusted to the trusted. The importance of a DMZ is tremendous: someone who breaks into your network from the Internet should have to get through several layers in order to successfully do so. Those layers are provided by various components within the DMZ.

Proxy.

This is the process of having one host act in behalf of another. A host that has the ability to fetch documents from the Internet might be configured as a *proxy server* , and host on the intranet might be configured to be *proxy clients* . In this situation, when a host on the intranet wishes to fetch the <http://www.interhack.net/> web page, for example, the browser will make a connection to the proxy server, and request the given URL. The proxy server will fetch the document, and return the result to the client. In this way, all hosts on the intranet are able to access resources on the Internet without having the ability to direct talk to the Internet.

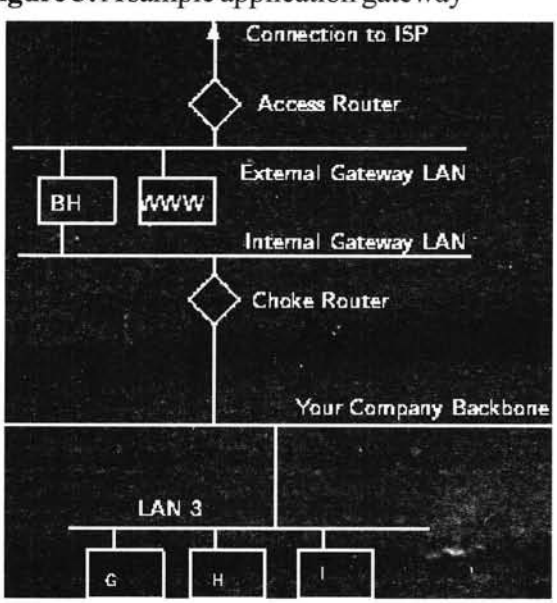
Types of Firewalls

There are three basic types of firewalls, and we'll consider each of them.

Application Gateways

The first firewalls were application gateways, and are sometimes known as proxy gateways. These are made up of bastion hosts that run special software to act as a proxy server. This software runs at the *Application Layer* of our old friend the ISO/OSI Reference Model, hence the name. Clients behind the firewall must be *proxitized* (that is, must know how to use the proxy, and be configured to do so) in order to use Internet services. Traditionally, these have been the most secure, because they don't allow anything to pass by default, but need to have the programs written and turned on in order to begin passing traffic.

Figure 5: A sample application gateway



These are also typically the slowest, because more processes need to be started in order to have a request serviced. Figure 5 shows a application gateway.

Packet Filtering

Packet filtering is a technique whereby routers have *ACLs* (Access Control Lists) turned on. By default, a router will pass all traffic sent it, and will do so without any sort of restrictions. Employing ACLs is a method for enforcing your security policy with regard to what sorts of access you allow the outside world to have to your internal network, and vice versa.

There is less overhead in packet filtering than with an application gateway, because the feature of access control is performed at a lower ISO/OSI layer (typically, the transport or session layer). Due to the lower overhead and the fact that packet filtering is done with routers, which are specialized computers optimized for tasks related to networking, a packet filtering gateway is often much faster than its application layer cousins. Figure 6 shows a packet filtering gateway.

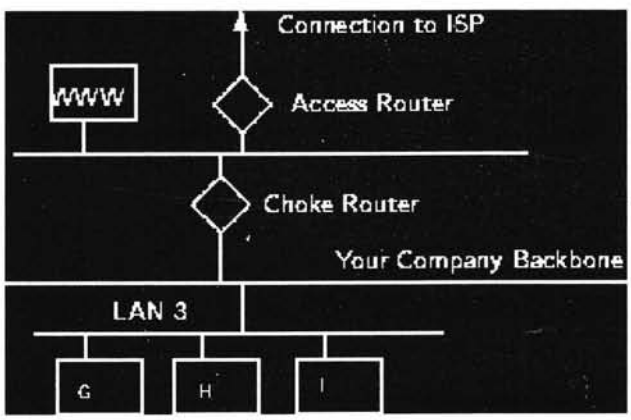
Because we're working at a lower level, supporting new applications either comes automatically, or is a simple matter of allowing a specific packet type to pass through the gateway. (Not that the *possibility* of something automatically makes it a good idea; opening things up this way might very well compromise your level of security below what your policy allows.)

There are problems with this method, though. Remember, TCP/IP has absolutely no means of guaranteeing that the source address is really what it claims to be. As a result, we have to use layers of packet filters in order to localize the traffic. We can't get all the way down to the actual host, but with two layers of packet filters, we can differentiate between a packet that came from the Internet and one that came from our internal network. We can identify which network the packet came from with certainty, but we can't get more specific than that.

Hybrid Systems

In an attempt to marry the security of the application layer gateways with the flexibility and speed of packet filtering, some vendors have created systems that use the principles of both.

Figure 6: A sample packet filtering gateway



In some of these systems, new connections must be authenticated and approved at the application layer. Once this has been done, the remainder of the connection is passed down to the session layer, where packet filters watch the connection to ensure that only packets that are part of an ongoing (already authenticated and approved) conversation are being passed.

Other possibilities include using both packet filtering and application layer proxies. The benefits here include providing a measure of protection against your machines that provide services to the Internet (such as a public web server), as well as provide the security of an application layer gateway to the internal network. Additionally, using this method, an attacker, in order to get to services on the internal network, will have to break through the access router, the bastion host, and the choke router.

So, what's best for me?

Lots of options are available, and it makes sense to spend some time with an expert, either in-house, or an experienced consultant who can take the time to understand your organization's security policy, and can design and build a firewall architecture that best implements that policy. Other issues like services required, convenience, and scalability might factor in to the final design.

Some Words of Caution

The business of building firewalls is in the process of becoming a commodity market. Along with commodity markets come lots of folks who are looking for a way to make a buck without necessarily knowing what they're doing. Additionally, vendors compete with each other to try and claim the greatest security, the easiest to administer, and the least visible to end users. In order to try to quantify the potential security of firewalls, some organizations have taken to firewall certifications. The certification of a firewall means nothing more than the fact that it *can* be configured in such a way that it can pass a series of tests. Similarly, claims about meeting or exceeding U.S. Department of Defense "Orange Book" standards, C-2, B-1, and such all simply mean that an organization was able to configure a machine to pass a series of tests. This doesn't mean that it was loaded with the vendor's software at the time, or that the machine was even usable. In fact, one vendor has been claiming their operating system is "C-2 Certified" didn't make mention of the fact that their operating system only passed the C-2 tests without being connected to any sort of network devices.

Such gauges as market share, certification, and the like are no guarantees of security or quality. Taking a little bit of time to talk to some knowledgeable folks can go a long way in providing you a comfortable level of security between your private network and the big, bad Internet.

Additionally, it's important to note that many consultants these days have become much less the advocate of their clients, and more of an extension of the vendor. Ask any consultants you talk to about their vendor affiliations, certifications, and whatnot. Ask what difference it makes to them whether you choose one product over another, and vice versa. And then ask yourself if a consultant who is certified in technology XYZ is going to provide you with competing technology ABC, even if ABC best fits your needs.

Single Points of Failure

Many "firewalls" are sold as a single component: a bastion host, or some other black box that you plug your networks into and get a warm-fuzzy, feeling safe and secure. *The term "firewall" refers to a number of components that collectively provide the security of the system.* Any time there is only one component paying attention to what's going on between the internal and external networks, an attacker has only one thing to break (or fool!) in order to gain complete access to your internal networks.

Secure Network Devices

It's important to remember that the firewall is only one entry point to your network. Modems, if you allow them to answer incoming calls, can provide an easy means for an attacker to sneak *around* (rather than *through*) your front door (or, firewall). Just as castles weren't built with moats only in the front, your network needs to be protected at all of its entry points.

Secure Modems; Dial-Back Systems

If modem access is to be provided, this should be guarded carefully. The *terminal server* , or network device that provides dial-up access to your network needs to be actively administered, and its logs need to be examined for strange behavior. Its passwords need to be strong — not ones that can be guessed. Accounts that aren't actively used should be disabled. In short, it's the easiest way to get into your network from remote: guard it carefully.

There are some remote access systems that have the feature of a two-part procedure to establish a connection. The first part is the remote user dialing into the system, and providing the correct userid and password. The system will then drop the connection, and call the authenticated user back at a known telephone number. Once the remote user's system answers that call, the connection is established, and the user is on the network. This works well for folks working at home, but can be problematic for users wishing to dial in from hotel rooms and such when on business trips.

Other possibilities include one-time password schemes, where the user enters his userid, and is presented with a "challenge," a string of between six and eight numbers. He types this challenge into a small device that he carries with him that looks like a calculator. He then presses enter, and a "response" is displayed on the LCD screen. The user types the response, and if all is correct, he login will proceed. These are useful devices for solving the problem of good passwords, without requiring dial-back access. However, these have their own problems, as they require the user to carry them, and they must be tracked, much like building and office keys.

No doubt many other schemes exist. Take a look at your options, and find out how what the vendors have to offer will help you *enforce your security policy effectively.*

Crypto-Capable Routers

A feature that is being built into some routers is the ability to use session encryption between specified routers. Because traffic traveling across the Internet can be seen by people in the middle who have the resources (and time) to snoop around, these are advantageous for providing connectivity between two sites, such that there can be secure routes.

See the Snake Oil FAQ [6] for a description of cryptography, ideas for evaluating cryptographic products, and how to determine which will most likely meet your needs.

10.3 Virtual Private Networks

Given the ubiquity of the Internet, and the considerable expense in private leased lines, many organizations have been building *VPNs* (Virtual Private Networks). Traditionally, for an organization to provide connectivity between a main office and a satellite one, an expensive data line had to be leased in order to provide direct connectivity between the two offices. Now, a solution that is often more economical is to provide both offices connectivity to the Internet. Then, using the Internet as the medium, the two offices can communicate.

The danger in doing this, of course, is that there is no privacy on this channel, and it's difficult to provide the other office access to "internal" resources without providing those resources to everyone on the Internet.

VPNs provide the ability for two offices to communicate with each other in such a way that it looks like they're directly connected over a private leased line. The session between them, although going over the Internet, is private (because the link is encrypted), and the link is convenient, because each can see each others' internal resources without showing them off to the entire world.

A number of firewall vendors are including the ability to build VPNs in their offerings, either directly with their base product, or as an add-on. If you have need to connect several offices together, this might very well be the best way to do it.

10.4 INTRUSION DETECTION SYSTEM:

An intrusion detection system (IDS) is a device, typically another separate computer, that monitors activity to identify malicious or suspicious events. An IDS is a sensor, like a smoke detector, that raises an alarm if specific things occur. A model of an IDS is shown in below figure. The components in the figure are the four basic elements of an intrusion detection system, based on the Common Intrusion Detection Framework of [STA96]. An IDS receives raw inputs from sensors. It saves those inputs, analyzes them, and takes some controlling action.

Types of IDSs

The two general types of intrusion detection systems are signature based and heuristic. Signature-based intrusion detection systems perform simple pattern-matching and report situations that match a pattern corresponding to a known attack type. Heuristic intrusion detection systems, also known as anomaly based, build a model of acceptable

behavior and flag exceptions to that model; for the future, the administrator can mark a flagged behavior as acceptable so that the heuristic IDS will now treat that previously unclassified behavior as acceptable.

Intrusion detection devices can be network based or host based. A network-based IDS is a stand-alone device attached to the network to monitor traffic throughout that network; a host-based IDS runs on a single workstation or client or host, to protect that one host.

Signature-Based Intrusion Detection:

A simple signature for a known attack type might describe a series of TCP SYN packets sent to many different ports in succession and at times close to one another, as would be the case for a port scan. An intrusion detection system would probably find nothing unusual in the first SYN, say, to port 80, and then another (from the same source address) to port 25. But as more and more ports receive SYN packets, especially ports that are not open, this pattern reflects a possible port scan. Similarly, some implementations of the protocol stack fail if they receive an ICMP packet with a data length of 65535 bytes, so such a packet would be a pattern for which to watch.

Heuristic Intrusion Detection:

Because signatures are limited to specific, known attack patterns, another form of intrusion detection becomes useful. Instead of looking for matches, heuristic intrusion detection looks for behavior that is out of the ordinary. The original work in this area focused on the individual, trying to find characteristics of that person that might be helpful in understanding normal and abnormal behavior. For example, one user might always start the day by reading e-mail, write many documents using a word processor, and occasionally back up files. These actions would be normal. This user does not seem to use many administrator utilities. If that person tried to access sensitive system management utilities, this new behavior might be a clue that someone else was acting under the user's identity.

Inference engines work in two ways. Some, called state-based intrusion detection systems, see the system going through changes of overall state or configuration. They try to detect when the system has veered into unsafe modes. Others try to map current activity onto a model of unacceptable activity and raise an alarm when the activity resembles the model.

These are called model-based intrusion detection systems. This approach has been extended to networks in [MUK94]. Later work sought to build a dynamic model of behavior, to accommodate variation and evolution in a person's actions over time. The technique compares real activity with a known representation of normality.

Alternatively, intrusion detection can work from a model of known bad activity. For example, except for a few utilities (login, change password, create user), any other attempt to access a password file is suspect. This form of intrusion detection is known as misuse intrusion detection. In this work, the real activity is compared against a known suspicious area.

Stealth Mode:

An IDS is a network device (or, in the case of a host-based IDS, a program running on a network device). Any network device is potentially vulnerable to network attacks. How useful would an IDS be if it itself were deluged with a denial-of-service attack? If an attacker succeeded in logging in to a system within the protected network, wouldn't trying to disable the IDS be the next step?

To counter those problems, most IDSs run in stealth mode, whereby an IDS has two network interfaces: one for the network (or network segment) being monitored and the other to generate alerts and perhaps other administrative needs. The IDS uses the monitored interface as input only; it *never* sends packets out through that interface. Often, the interface is configured so that the device has no published address through the monitored interface; that is, a router cannot route anything to that address directly, because the router does not know such a device exists. It is the perfect passive wiretap. If the IDS needs to generate an alert, it uses only the alarm interface on a completely separate control network.

Goals for Intrusion Detection Systems:

1. Responding to alarms:

Whatever the type, an intrusion detection system raises an alarm when it finds a match. The alarm can range from something modest, such as writing a note in an audit log, to something significant, such as paging the system security administrator. Particular implementations allow the user to determine what action the system should take on what events.

In general, responses fall into three major categories (any or all of which can be used in a single response):

Monitor, collect data, perhaps increase amount of data collected

Protect, act to reduce exposure

Call a human

2. False Results:

Intrusion detection systems are not perfect, and mistakes are their biggest problem. Although an IDS might detect an intruder correctly most of the time, it may stumble in two different ways: by raising an alarm for something that is not really an attack (called a false positive, or type I error in the statistical community) or not raising an alarm for a real attack (a false negative, or type II error). Too many false positives means the administrator will be less confident of the IDS's warnings, perhaps leading to a real alarm's being ignored. But false negatives mean that real attacks are passing the IDS without action. We say that the degree of false positives and false negatives represents the sensitivity of the system. Most IDS implementations allow the administrator to tune the system's sensitivity, to strike an acceptable balance between false positives and negatives.

IDS strength and limitations:

On the upside, IDSs detect an ever-growing number of serious problems. And as we learn more about problems, we can add their signatures to the IDS model. Thus, over time, IDSs continue to improve. At the same time, they are becoming cheaper and easier to administer. On the downside, avoiding an IDS is a first priority for successful attackers. An IDS that is not well defended is useless. Fortunately, stealth mode IDSs are difficult even to find on an internal network, let alone to compromise. IDSs look for known weaknesses, whether through patterns of known attacks or models of normal behavior. Similar IDSs may have identical vulnerabilities, and their selection criteria may miss similar attacks. Knowing how to evade a particular model of IDS is an important piece of intelligence passed within the attacker community. Of course, once manufacturers become aware of a shortcoming in their products, they try to fix it. Fortunately, commercial IDSs are pretty good at identifying attacks. Another IDS limitation is its sensitivity, which is difficult to measure and adjust. IDSs will never be perfect, so finding the proper balance is critical.

In general, IDSs are excellent additions to a network's security. Firewalls block traffic to particular ports or addresses; they also constrain certain protocols to limit their impact. But by definition, firewalls have to allow some traffic to enter a protected area.

10.5 Access Control and Authorization

Access control mechanisms are a necessary and crucial design element to any application's security. In general, a web application should protect front-end and back-end data and system resources by implementing access control restrictions on what users can do, which resources they have access to, and what functions they are allowed to perform on the data. Ideally, an access control scheme should protect against the unauthorized viewing, modification, or copying of data. Additionally, access control mechanisms can also help limit malicious code execution, or unauthorized actions through an attacker exploiting infrastructure dependencies (DNS server, ACE server, etc.).

Authorization and Access Control are terms often mistakenly interchanged. Authorization is the act of checking to see if a user has the proper permission to access a particular file or perform a particular action, assuming that user has successfully authenticated himself. Authorization is very much credential focused and dependent on specific rules and access control lists preset by the web application administrator(s) or data owners. Typical authorization checks involve querying for membership in a particular user group, possession of a particular clearance, or looking for that user on a resource's approved access control list, akin to a bouncer at an exclusive nightclub. Any access control mechanism is clearly dependent on effective and forge-resistant authentication controls used for authorization.

Access Control refers to the much more general way of controlling access to web resources, including restrictions based on things like the time of day, the IP address of the HTTP client browser, the domain of the HTTP client browser, the type of encryption the HTTP client can support, number of times the user has authenticated that day,

the possession of any number of types of hardware/software tokens, or any other derived variables that can be extracted or calculated easily.

Before choosing the access control mechanisms specific to your web application, several preparatory steps can help expedite and clarify the design process;

1. Try to quantify the relative value of information to be protected in terms of Confidentiality, Sensitivity, Classification, Privacy, and Integrity related to the organization as well as the individual users. Consider the worst case financial loss that unauthorized disclosure, modification, or denial of service of the information could cause. Designing elaborate and inconvenient access controls around unclassified or non-sensitive data can be counterproductive to the ultimate goal or purpose of the web application.

2. Determine the relative interaction that data owners and creators will have within the web application. Some applications may restrict any and all creation or ownership of data to anyone but the administrative or built-in system users. Are specific roles required to further codify the interactions between different types of users and administrators?

3. Specify the process for granting and revoking user access control rights on the system, whether it be a manual process, automatic upon registration or account creation, or through an administrative front-end tool.

4. Clearly delineate the types of role driven functions the application will support. Try to determine which specific user functions should be built into the web application (logging in, viewing their information, modifying their information, sending a help request, etc.) as well as administrative functions (changing passwords, viewing any users data, performing maintenance on the application, viewing transaction logs, etc.).

5. Try to align your access control mechanisms as closely as possible to your organization's security policy. Many things from the policy can map very well over to the implementation side of access control (acceptable time of day of certain data access, types of users allowed to see certain data or perform certain tasks, etc.). These types of mappings usually work the best with Role Based Access Control.

There are a plethora of accepted access control models in the information security realm. Many of these contain aspects that translate very well into the web application space, while others do not. A successful access control protection mechanism will likely combine aspects of each of the following models and should be applied not only to user management, but code and application integration of certain functions.

Types of access Control

- Discretionary Access Control
- Mandatory Access Control
- Role Based Access Control

Discretionary Access Control

Discretionary Access Control (DAC) is a means of restricting access to information based on the identity of users and/or membership in certain groups. Access decisions are typically based on the authorizations granted to a user based on the credentials he presented at the time of authentication (user name, password, hardware/software token, etc.). In most typical DAC models, the owner of information or any resource is able to change its permissions at his discretion (thus the name). DAC has the drawback of the administrators not being able to centrally manage these permissions on files/information stored on the web server. A DAC access control model often exhibits one or more of the following attributes.

- Data Owners can transfer ownership of information to other users
- Data Owners can determine the type of access given to other users (read, write, copy, etc.)
- Repetitive authorization failures to access the same resource or object generates an alarm and/or restricts the user's access
- Special add-on or plug-in software required to apply to an HTTP client to prevent indiscriminant copying by users ("cutting and pasting" of information)
- Users who do not have access to information should not be able to determine its characteristics (file size, file name, directory path, etc.)
- Access to information is determined based on authorizations to access control lists based on user identifier and group membership.

Mandatory Access Control

Mandatory Access Control (MAC) ensures that the enforcement of organizational security policy does not rely on voluntary web application user compliance. MAC secures information by assigning sensitivity labels on information and comparing this to the level of sensitivity a user is operating at. In general, MAC access control mechanisms are more secure than DAC yet have trade offs in performance and convenience to users. MAC mechanisms assign a security level to all information, assign a security clearance to each user, and ensure that all users only have access to that data for which they have a clearance. MAC is usually appropriate for extremely secure systems including multilevel secure military applications or mission critical data applications. A MAC access control model often exhibits one or more of the following attributes.

- Only administrators, not data owners, make changes to a resource's security label.
- All data is assigned security level that reflects its relative sensitivity, confidentiality, and protection value.
- All users can read from a lower classification than the one they are granted (A "secret" user can read an unclassified document).

- All users can write to a higher classification (A "secret" user can post information to a Top Secret resource).
- All users are given read/write access to objects only of the same classification (a "secret" user can only read/write to a secret document).
- Access is authorized or restricted to objects based on the time of day depending on the labeling on the resource and the user's credentials (driven by policy).
- Access is authorized or restricted to objects based on the security characteristics of the HTTP client (e.g. SSL bit length, version information, originating IP address or domain, etc.)

Role Based Access Control

In Role-Based Access Control (RBAC), access decisions are based on an individual's roles and responsibilities within the organization or user base. The process of defining roles is usually based on analyzing the fundamental goals and structure of an organization and is usually linked to the security policy. For instance, in a medical organization, the different roles of users may include those such as doctor, nurse, attendant, nurse, patients, etc. Obviously, these members require different levels of access in order to perform their functions, but also the types of web transactions and their allowed context vary greatly depending on the security policy and any relevant regulations (HIPAA, Gramm-Leach-Bliley, etc.).

An RBAC access control framework should provide web application security administrators with the ability to determine who can perform what actions, when, from where, in what order, and in some cases under what relational circumstances. http://csrc.nist.gov/rbac/ provides some great resources for RBAC implementation. The following aspects exhibit RBAC attributes to an access control model.

- Roles are assigned based on organizational structure with emphasis on the organizational security policy
- Roles are assigned by the administrator based on relative relationships within the organization or user base. For instance, a manager would have certain authorized transactions over his employees. An administrator would have certain authorized transactions over his specific realm of duties (backup, account creation, etc.)
- Each role is designated a profile that includes all authorized commands, transactions, and allowable information access.
- Roles are granted permissions based on the principle of least privilege.
- Roles are determined with a separation of duties in mind so that a developer Role should not overlap a QA tester Role.
- Roles are activated statically and dynamically as appropriate to certain relational triggers (help desk queue, security alert, initiation of a new project, etc.)
- Roles can be only be transferred or delegated using strict sign-offs and procedures.
- Roles are managed centrally by a security administrator or project leader.

Watching what that traffic actually does inside the protected area is an IDS's job, which it does quite well.
Bottom of Form

10.6 Kerberos Overview

Kerberos is a secret-key network authentication protocol, developed at the Massachusetts Institute of Technology (MIT), that uses the Data Encryption Standard (DES) cryptographic algorithm for encryption and authentication. Kerberos was designed to authenticate requests for network resources. Kerberos, like other secret-key systems, is based on the concept of a trusted third party that performs secure verification of users and services.

In the Kerberos protocol, this trusted third party is called the Key Distribution Center (KDC). It performs the same function as a certification authority (CA), which is discussed in Chapter 9, "Building Advanced IPSec VPNs Using Cisco Routers and Certificate Authorities." The following lists some of the distinguishing characteristics of Kerberos:

- Secret-key authentication protocol
- Authenticates users and network services that they use
- Uses 40- or 56-bit DES for encryption and authentication (weak by today's standards)
- Relies on a trusted third party (KDC) for key distribution
- Embodies "single login" concept
- Expensive to administer—labor intensive

Cisco IOS Release 12.0 includes Kerberos 5 support, which allows organizations that are already deploying Kerberos 5 to use an existing KDC (similar to a CA in IP Security [IPSec]) with their routers and NAS. The following network services are Kerberized in Cisco IOS software:

- **Telnet**—Logs a client (from router to another host) into a server (from another host to router) to permit interactive Telnet sessions
- **rlogin**—Logs a user in to a remote UNIX host for an interactive session similar to Telnet
- **rsh**—Logs a user in to a remote UNIX host and allows execution of one UNIX command
- **rcp**—Logs a user in to a remote UNIX host and allows copying of files from the host

NOTE

You can use the **connect** EXEC command with the **/telnet** or **/rlogin** keyword to log in to a host that supports Telnet or rlogin, respectively. You can use the **/encrypt kerberos**keyword to establish an encrypted Telnet session from a router to a remote Kerberos host. Alternatively, you can use the **telnet** EXEC command with the **/encrypt kerberos**keyword to establish an encrypted Telnet session.

You can use the **rlogin** and **rsh** EXEC commands to initiate rlogin and rsh sessions.

You can use the **copy rcp** EXEC command or configuration command to enable obtaining configuration or image files from an RCP server.

What is Kerberos?

Kerberos is a trusted third-party authentication service based on the model presented by Needham and Schroeder. It is trusted in the sense that each of its clients believes Kerberos' judgement as to the identity of each of its other clients to be accurate. Timestamps (large numbers representing the current date and time) have been added to the original model to aid in the detection of replay. Replay occurs when a message is stolen off the network and resent later. For a more complete description of replay, and other issues of authentication, see Voydock and Kent.

What Does Kerberos Do?

Kerberos keeps a database of its clients and their private keys. The private key is a large number known only to Kerberos and the client it belongs to. In the case that the client is a user, it is an encrypted password. Network services requiring authentication register with Kerberos, as do clients wishing to use those services. The private keys are negotiated at registration.

Because Kerberos knows these private keys, it can create messages which convince one client that another is really who it claims to be. Kerberos also generates temporary private keys, called session keys, which are given to two clients and no one else. A session key can be used to encrypt messages between two parties.

Kerberos provides three distinct levels of protection. The application programmer determines which is appropriate, according to the requirements of the application. For example, some applications require only that authenticity be established at the initiation of a network connection, and can assume that further messages from a given network address originate from the authenticated party. Our authenticated network file system uses this level of security.

Other applications require authentication of each message, but do not care whether the content of the message is disclosed or not. For these, Kerberos provides safe messages. Yet a higher level of security is provided by private messages, where each message is not only authenticated, but also encrypted. Private messages are used, for example, by the Kerberos server itself for sending passwords over the network.

Kerberos Software Components

The Athena implementation comprises several modules:

- Kerberos applications library
- encryption library
- database library

- database administration programs
- administration server
- authentication server
- db propagation software
- user programs
- applications

The Kerberos applications library provides an interface for application clients and application servers. It contains, among others, routines for creating or reading authentication requests, and the routines for creating safe or private messages.

Encryption in Kerberos is based on DES, the Data Encryption Standard. The encryption library implements those routines. Several methods of encryption are provided, with tradeoffs between speed and security. An extension to the DES Cypher Block Chaining (CBC) mode, called the Propagating CBC mode, is also provided. In CBC, an error is propagated only through the current block of the cipher, whereas in PCBC, the error is propagated throughout the message. This renders the entire message useless if an error occurs, rather than just a portion of it. The encryption library is an independent module, and may be replaced with other DES implementations or a different encryption library.

Another replaceable module is the database management system. The current Athena implementation of the database library uses ndbm, although Ingres was originally used. Other database management libraries could be used as well.

The Kerberos database needs are straightforward; a record is held for each principal, containing the name, private key, and expiration date of the principal, along with some administrative information. (The expiration date is the date after which an entry is no longer valid. It is usually set to a few years into the future at registration.)

Other user information, such as real name, phone number, and so forth, is kept by another server, the Hesiod nameserver. This way, sensitive information, namely passwords, can be handled by Kerberos, using fairly high security measures; while the non-sensitive information kept by Hesiod is dealt with differently; it can, for example, be sent unencrypted over the network.

The Kerberos servers use the database library, as do the tools for administering the database.

The administration server (or KDBM server) provides a read-write network interface to the database. The client side of the program may be run on any machine on the network. The server side, however, must run on the machine housing the Kerberos database in order to make changes to the database.

The authentication server (or Kerberos server), on the other hand, performs read-only operations on the Kerberos database, namely, the authentication of principals, and generation of session keys. Since this server does not modify the Kerberos database, it may run on a machine housing a read-only copy of the master Kerberos database.

Database propagation software manages replication of the Kerberos database. It is possible to have copies of the database on several different machines, with a copy of the authentication server running on each machine. Each of these slave machines receives an update of the Kerberos database from the master machine at given intervals.

Finally, there are end-user programs for logging in to Kerberos, changing a Kerberos password, and displaying or destroying Kerberos tickets (tickets are explained later on).

Kerberos Names

Part of authenticating an entity is naming it. The process of authentication is the verification that the client is the one named in a request. What does a name consist of? In Kerberos, both users and servers are named. As far as the authentication server is concerned, they are equivalent. A name consists of a primary name, an instance, and a realm, expressed as name.instance@realm.

The primary name is the name of the user or the service. The instance is used to distinguish among variations on the primary name. For users, an instance may entail special privileges, such as the "root" or "admin" instances. For services in the Athena environment, the instance is usually the name of the machine on which the server runs. For example, the rlogin service has different instances on different hosts: rlogin.priam is the rlogin server on the host named priam. A Kerberos ticket is only good for a single named server. As such, a separate ticket is required to gain access to different instances of the same service. The realm is the name of an administrative entity that maintains authentication data. For example, different institutions may each have their own Kerberos machine, housing a different database. They have different Kerberos realms. (Realms are discussed further in Interaction with Other Kerberi.)

How Kerberos Works?

This section describes the Kerberos authentication protocols. As mentioned above, the Kerberos authentication model is based on the Needham and Schroeder key distribution protocol. When a user requests a service, her/his identity must be established. To do this, a ticket is presented to the server, along with proof that the ticket was originally issued to the user, not stolen. There are three phases to authentication through Kerberos. In the first phase, the user obtains credentials to be used to request access to other services. In the second phase, the user requests authentication for a specific service. In the final phase, the user presents those credentials to the end server.

Kerberos Credentials

There are two types of credentials used in the Kerberos authentication model: tickets and authenticators. Both are based on private key encryption, but they are encrypted using different keys. A ticket is used to securely pass the identity of the person to whom the ticket was issued between the authentication server and the end server. A ticket also passes information that can be used to make sure that the person using the ticket is the same person to which it was issued. The authenticator contains the additional information which, when compared against that in the ticket proves that the client presenting the ticket is the same one to which the ticket was issued.

A ticket is good for a single server and a single client. It contains the name of the server, the name of the client, the Internet address of the client, a timestamp, a lifetime, and a random session key. This information is encrypted using the key of the server for which the ticket will be used. Once the ticket has been issued, it may be used multiple times by the named client to gain access to the named server, until the ticket expires. Note that because the ticket is encrypted in the key of the server, it is safe to allow the user to pass the ticket on to the server without having to worry about the user modifying the ticket.

Unlike the ticket, the authenticator can only be used once. A new one must be generated each time a client wants to use a service. This does not present a problem because the client is able to build the authenticator itself. An authenticator contains the name of the client, the workstation's IP address, and the current workstation time. The authenticator is encrypted in the session key that is part of the ticket.

Get the Initial Kerberos Ticket

When the user walks up to a workstation, only one piece of information can prove her/his identity: the user's password. The initial exchange with the authentication server is designed to minimize the chance that the password will be compromised, while at the same time not allowing a user to properly authenticate her/himself without knowledge of that password. The process of logging in appears to the user to be the same as logging in to a timesharing system. Behind the scenes, though, it is quite different.

The user is prompted for her/his username. Once it has been entered, a request is sent to the authentication server containing the user's name and the name of a special service known as the ticket-granting service.

The authentication server checks that it knows about the client. If so, it generates a random session key which will later be used between the client and the ticket-granting server. It then creates a ticket for the ticket-granting server which contains the client's name, the name of the ticket-granting server, the current time, a lifetime for the ticket, the client's IP address, and the random session key just created. This is all encrypted in a key known only to the ticket-granting server and the authentication server.

The authentication server then sends the ticket, along with a copy of the random session key and some additional information, back to the client. This response is encrypted in the client's private key, known only to Kerberos and the client, which is derived from the user's password.

Once the response has been received by the client, the user is asked for her/his password. The password is converted to a DES key and used to decrypt the response from the authentication server. The ticket and the session key, along with some of the other information, are stored for future use, and the user's password and DES key are erased from memory.

Once the exchange has been completed, the workstation possesses information that it can use to prove the identity of its user for the lifetime of the ticket-granting ticket. As long as the software on the workstation had not been previously tampered with, no information exists that will allow someone else to impersonate the user beyond the life of the ticket.

Request a Kerberos Service

For the moment, let us pretend that the user already has a ticket for the desired server. In order to gain access to the server, the application builds an authenticator containing the client's name and IP address, and the current time. The authenticator is then encrypted in the session key that was received with the ticket for the server. The client then sends the authenticator along with the ticket to the server in a manner defined by the individual application.

Once the authenticator and ticket have been received by the server, the server decrypts the ticket, uses the session key included in the ticket to decrypt the authenticator, compares the information in the ticket with that in the authenticator, the IP address from which the request was received, and the present time. If everything matches, it allows the request to proceed.

It is assumed that clocks are synchronized to within several minutes. If the time in the request is too far in the future or the past, the server treats the request as an attempt to replay a previous request. The server is also allowed to keep track of all past requests with timestamps that are still valid. In order to further foil replay attacks, a request received with the same ticket and timestamp as one already received can be discarded.

Finally, if the client specifies that it wants the server to prove its identity too, the server adds one to the timestamp the client sent in the authenticator, encrypts the result in the session key, and sends the result back to the client.

At the end of this exchange, the server is certain that, according to Kerberos, the client is who it says it is. If mutual authentication occurs, the client is also convinced that the server is authentic. Moreover, the client and server share a key which no one else knows, and can safely assume that a reasonably recent message encrypted in that key originated with the other party.

Get Kerberos Server Tickets

Recall that a ticket is only good for a single server. As such, it is necessary to obtain a separate ticket for each service the client wants to use. Tickets for individual servers can be obtained from the ticket-granting service. Since the ticket-granting service is itself a service, it makes use of the service access protocol described in the previous section.

When a program requires a ticket that has not already been requested, it sends a request to the ticket-granting server. The request contains the name of the server for which a ticket is requested, along with the ticket-granting ticket and an authenticator built as described in the previous section.

The ticket-granting server then checks the authenticator and ticket-granting ticket as described above. If valid, the ticket-granting server generates a new random session key to be used between the client and the new server. It then builds a ticket for the new server containing the client's name, the server name, the current time, the client's IP address and the new session key it just generated. The lifetime of the new ticket is the minimum of the remaining life for the ticket-granting ticket and the default for the service.

The ticket-granting server then sends the ticket, along with the session key and other information, back to the client. This time, however, the reply is encrypted in the session key that was part of the ticket-granting ticket. This way, there is no need for the user to enter her/his password again.

10.7 CASE STUDY ON WINDOWS AND LINUX OPERATING SYSTEMS

History

The first Windows system was released in 1985. Originally, it was just a graphical user interface on top of MS-DOS – a state of affairs that lasted until the release of Windows 95, when MS-DOS products were integrated into Windows. Windows 95 was a huge departure from the previous systems and was the first major step in Window's transition from GUI to operating system.

Linux has the unlikely origin of being the hobby project of Finnish university student Linus Torvalds. He was unsatisfied with an existing Unix-like academic operating system – with limited licensing – named Minix, and decided he could do better (and make it free, open-source software). The resulting system was eventually named after Torvalds. The Linux kernel was first released independently in 1991, designed to be used with GNU software. GNU developers eventually integrated their software into Linux to create an OS. Linux is available in many forms to suit many needs, from consumer-oriented systems for home use to distributions for use in specific industries.

Benefits

The Windows series of operating systems have the obvious benefit of market ubiquity. For most people, Windows will be extremely familiar and therefore easy to use; Windows is the "standard" operating system bundled with new PCs. This means that the vast majority of software, hardware, support and training available is designed with Windows compatibility primarily in mind. The overwhelming market dominance of the Windows operating system has shaped the way consumers relate to and think about OS's and GUI's – "taskbar" "start menu" and "desktop" all entered the common lexicon following the immense popularity of Windows 95.

Linux has the immediate benefit of being free to obtain, and available for use without restrictions. It is open source with a large, supportive community building a seemingly infinite range of free applications for use on Linux

machines. Many (many!) distributions of Linux are available, giving users the ability to choose one that suits their personal needs (then further customize it). Similar to OS X, Linux is less vulnerable to attack than a Windows PC, and Linux distributions are typically updated frequently – incredibly frequently compared to other operating systems – further enhancing their stability and security. Linux operating systems are perhaps the most widely ported – there are distributions used in a wide range of devices from smartphones to TiVo.

Differences

Windows is designed to run on PCs, whether bought new or built cheaply, so hardware costs are essentially determined by the consumer. However, the cost of buying the latest version of Windows can be prohibitive (Windows XP is still the most widely used version), and the restrictive licensing inevitably forces each user to purchase a copy as they cannot be shared. Coupled with the similarly inevitable cost of purchasing the also-ubiquitous Microsoft Office suite and it is easy to see how users may prefer to simply wait until they need to buy a new PC bundled with Microsoft software.

Linux may be the cheapest, most easily available and customizable of the three, but the continued dominance of Windows (not to mention the fact it comes pre-installed on most machines) often deters home users from changing to this unfamiliar platform. Additionally, while Linux may have a large number of community-sourced applications available, it does not offer as many professional quality one as the other systems. Minority use means some third party software (such as popular PC games) is yet to have a Linux release.

Popularity

Windows continues to be the most popular OS worldwide, with Microsoft estimated to be holding on to roughly 90% of desktop users. Windows still represents the extent of many home users' experience with operating systems.

Linux may have the smallest share of home users, however commercial use is huge. Servers, mainframes and supercomputers commonly use Linux, as do the film industry, governments both nationally and locally, and many portable device manufacturers. As personal computers move away from the desktop and increasingly become portable, adoption of other operating systems will surely follow.

Model Question Paper

INFORMATION SECURITY AND DIGITAL FORENSICS

Part A – (2 X 12 = 24 Marks)

Answer Any TWO Questions

1. Explain how Forensic Toolkit is used during the investigation process with an example.

There are many tools that can help an investigator analyze a digital system. Most tools focuson the preservation and searching phases of the investigation

EnCase by Guidance Software

There are no official numbers on the topic, but it is generally accepted that *EnCase* (http://www.encase.com) is the most widely used computer investigation software. EnCase is Windows-based and can acquire and analyze data using the local or network-based versions of the tool. EnCase can analyze many file system formats, including FAT, NTFS, HFS+, UFS, Ext2/3, Reiser, JFS, CD-ROMs, and DVDs. EnCase also supports Microsoft Windows dynamic disks and AIX LVM.

EnCase allows you to list the files and directories, recover deleted files, conduct keyword searches, view all graphic images, make timelines of file activity, and use hash databases to identify known files. It also has its own scripting language, called EnScript, which allows you to automate many tasks. Add-on modules support the decryption of NTFS encrypted files and allow you to mount the suspect data as though it were a local disk.

Forensic Toolkit by AccessData

The *Forensic Toolkit* (FTK) is Windows-based and can acquire and analyze disk, file system, and application data (http://www.accessdata.com). FTK supports FAT, NTFS, and Ext2/3 file systems, but is best known for its searching abilities and application-level analysis support. FTK creates a sorted index of the words in a file system so that individual searches are much faster. FTK also has many viewers for different file formats and supports many email formats. FTK allows you to view the files and directories in the file system, recover deleted files, conduct keyword searches, view all graphic images, search on various file characteristics, and use hash databases to identify known files. AccessData also has tools for decrypting files and recovering passwords.

ProDiscover by Technology Pathways

ProDiscover (http://www.techpathways.com) is a Windows-based acquisition and analysis tool that comes in both local and network-based versions. ProDiscover can analyze FAT, NTFS, Ext2/3, and UFS file systems and Windows dynamic disks. When searching, it provides the basic options to list the files and directories, recover deleted files, search for keywords, and use hash databases to identify known files. ProDiscover is available with a license that includes the source code so that an investigator or lab can verify the tool's actions.

SMART by ASR Data

SMART (http://www.asrdata.com) is a Linux-based acquisition and analysis tool. Andy Rosen, who was the original developer for Expert Witness (which is now called EnCase), developed SMART. SMART takes advantage of the large number of file systems that Linux supports and can analyze FAT, NTFS, Ext2/3, UFS, HFS+, JFS, Reiser, CD-ROMs, and more. To search for evidence, it allows you to list and filter the files and directories in the image, recover deleted files, conduct keyword searches, view all graphic images, and use hash databases to identify known files.

The Sleuth Kit / Autopsy

The Sleuth Kit (TSK) is a collection of Unix-based command line analysis tools, and Autopsy is a graphical interface for TSK (http://www.sleuthkit.org). The file system tools in TSK are based on *The Coroner's Toolkit* (TCT) (http://www.porcupine.org), which was written by Dan Farmer and Wietse Venema. TSK and Autopsy can analyze FAT, NTFS, Ext2/3, and UFS file systems and can list files and directories, recover deleted files, make timelines of file activity, perform keyword searches, and use hash databases. We will be using TSK throughout this book, and Appendix A, "The Sleuth Kit and Autopsy," provides a description of how it can be used.

Collecting Evidence

The investigator should collect the following types of evidence:

- *General evidence*: This includes the date and time the investigator visited the incident site and with whom the investigator spoke.
- *Physical and demonstrative evidence*: This includes pictures taken at the incident site. The investigator can demonstrate the evidence using maps, X-rays, diagrams, and floor plans.
- ***Testimonial evidence***: This is oral evidence, presented by a competent eyewitness to the incident, that is relevant and material to the case. It includes testimony from all the persons interviewed by the investigator in order of the date and time of the interview.

Collecting Physical and Demonstrative Evidence

The following information should be collected for physical and demonstrative evidence:

- The manner in which the scene of the incident was secured
- A list of each type of physical evidence that was collected and secured
- The manner in which the physical evidence was collected and logged
- The manner in which the physical evidence was preserved after collection to maintain the chain of custody
- A list of any pictures that were taken
- A list of any demonstrative evidence available to the investigation

Collecting Testimonial Evidence

The following information should be collected for testimonial evidence:

- The manner in which the investigator determined whom to interview
- A list of the persons interviewed in chronological order, including the name, title, date, and time of each interview
- A list of persons who are identified as the targets of the case
- The manner in which the investigator afforded the target or the witnesses any right to representation

6.7 Case Report Writing and Documentation

All conclusions and findings of computer media analysis should go into an investigative analysis report, which is then directly sent to a case officer.

This report should have the following documents:

- Forms
- Analysis notes
- Items that come as a result of analysis, i.e., printouts and CDs
- Copies of search warrants
- Evidence listing
- Media analysis worksheet
- Keyword lists
- Support requests

Creating a Report to Attach to the Media Analysis Worksheet

An investigator should maintain notes and provide more information on the following to create a report that can be attached to the media analysis worksheet:

- Date and time when any computer taken as evidence
- Current date and time
- Lapses in analysis
- Finding evidence

• Special techniques required that are beyond the normal processes

• Significant problems or broken items

• Outside sources that provide assistance during the investigation

Best Practices for Investigators

Before submitting the final report, an investigator should read it over to see if there are any places where he or she needs to make changes. The report should contain only relevant material. It should also be coherent, not repetitive, and consistently structured. The investigator should also let an outsider read the report. The reportneeds to be understandable to someone who is completely unfamiliar with the case.

Writing a Report Using FTK

To prepare a new case using FTK, perform the following steps:

1. Write-protect the evidence floppy disk.

2. Create a work folder and another folder under this folder.

3. Run FTK.

4. Click **OK**.

5. Select **Start a new case** and click **OK** in the **FTK Startup** dialog box (Figure 6-5).

6. Fill out the appropriate information in the **New Case** dialog box and click **Continue**.

7. Use the **Browse** button to access the case path.

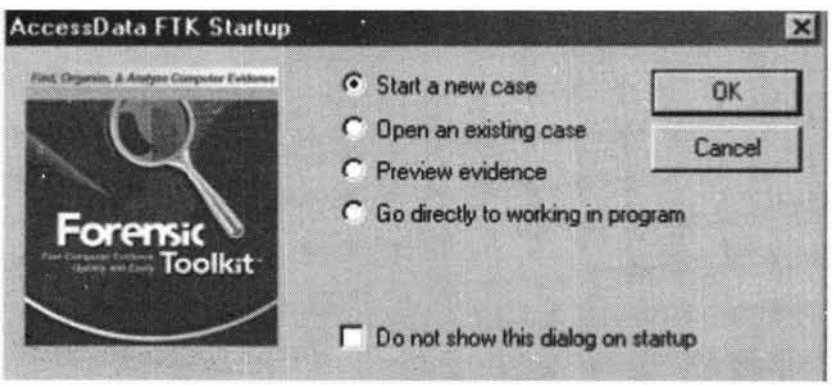


Figure 6-5 Select **Start a new case** in the **FTK Startup** dialog box.

8. Give a brief description of the investigation (Figure 6-6) and click **Next**.

9. Check all the boxes in the **Case Log Options** window (Figure 6-7).

10. Click **Next** in the **Evidence Processing Options** window (Figure 6-8).

11. Click **Next** in the **Refine Case and Refine Index** window.

12. In the **Add Evidence to Case** window (Figure 6-9), click the **Add Evidence** button.

13. The **Add Evidence to Case** dialog box appears. Click the **Local Drive** option and then click **Continue**.

14. Select the **A: drive** option and the **Logical option** button in the **Select Local Drive** dialog box, and click **OK**.

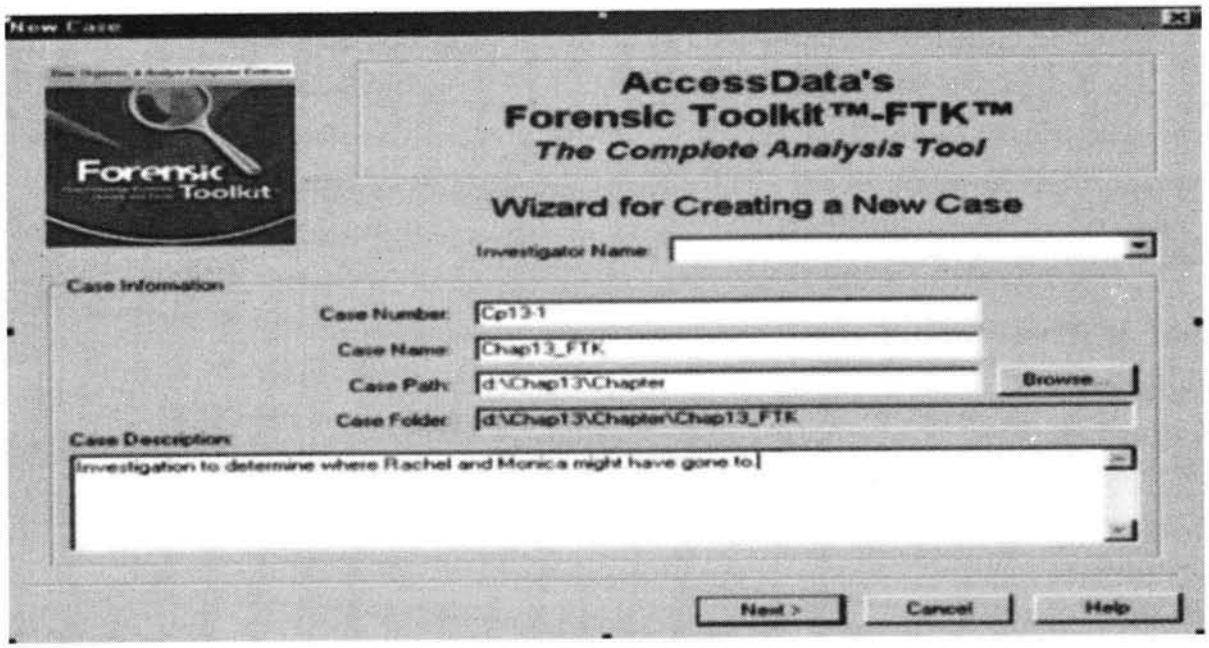


Figure 6-6 The case description should be brief but informative.

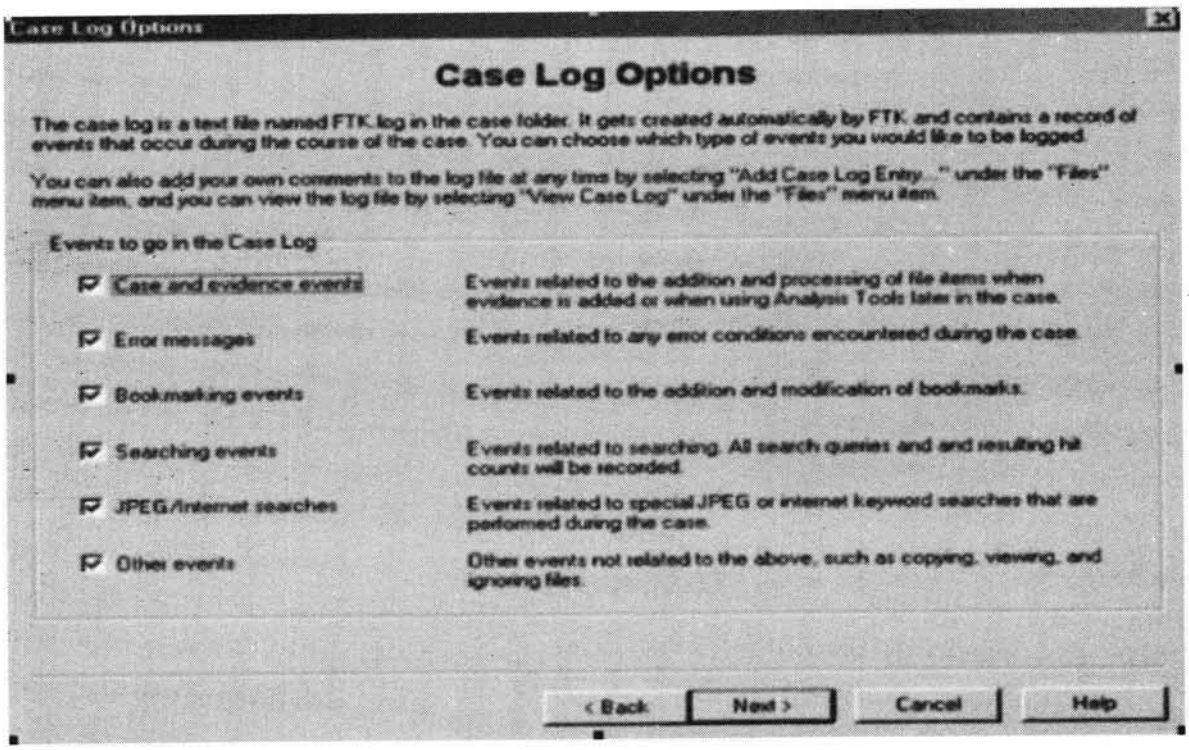


Figure 6-7 The **Case Log Options** window lets a user choose what to include in the case log.

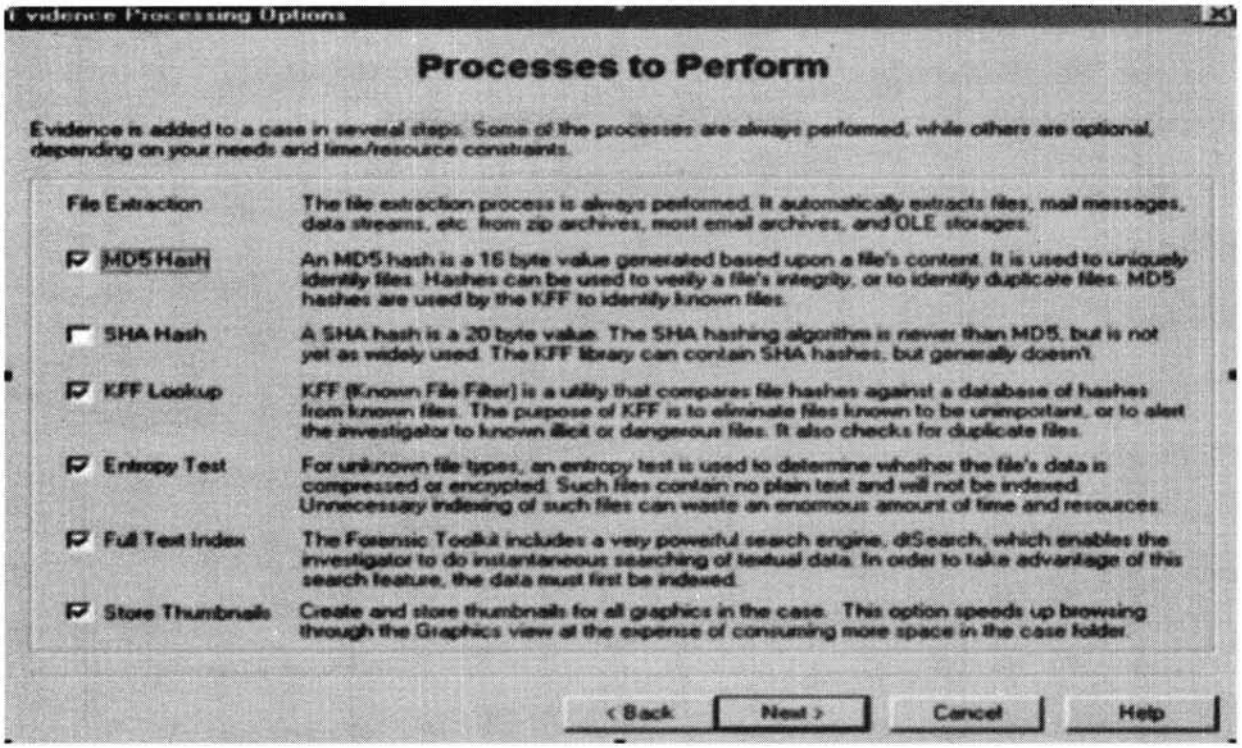


Figure 6-8 The **Evidence Processing Options** window tells FTK which processes to perform on the evidence files.

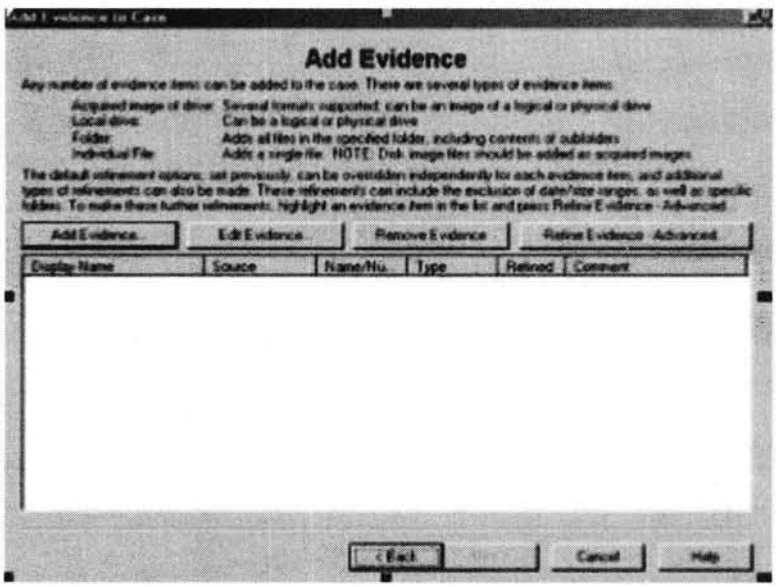


Figure 6-9 Click the **Add Evidence** button to add evidence.

15. Enter comments in the **Evidence Information** window (Figure 6-10) and then click **OK**.

16. Click **Next** in the **Add Evidence** window.

17. Check the information in the **Case Summary** window (Figure 6-11). If it is correct, click **Finish**.

Otherwise, click **Back** to fix any errors.

FTK starts analyzing the data on the investigation floppy disk when the FTK **Processing Files** window (Figure 6-12) appears. When FTK completes the analysis, the main FTK window (Figure 6-13) appears showing all data found from the analysis process.

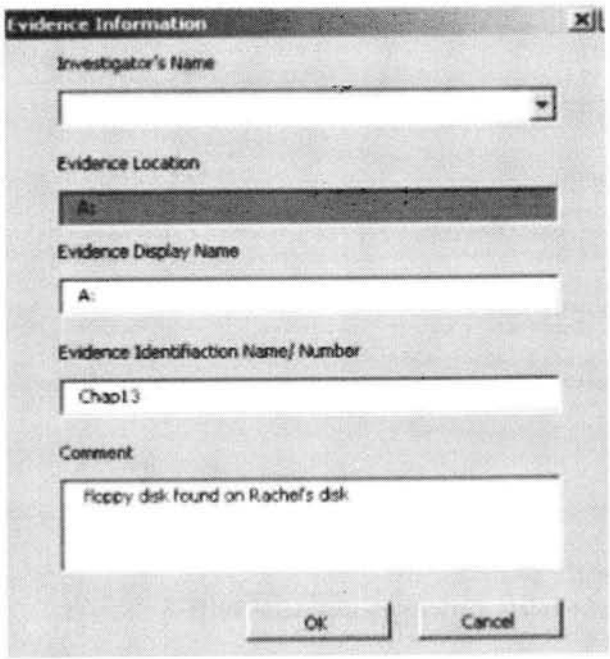


Figure 6-10 Enter a comment that describes the evidence.

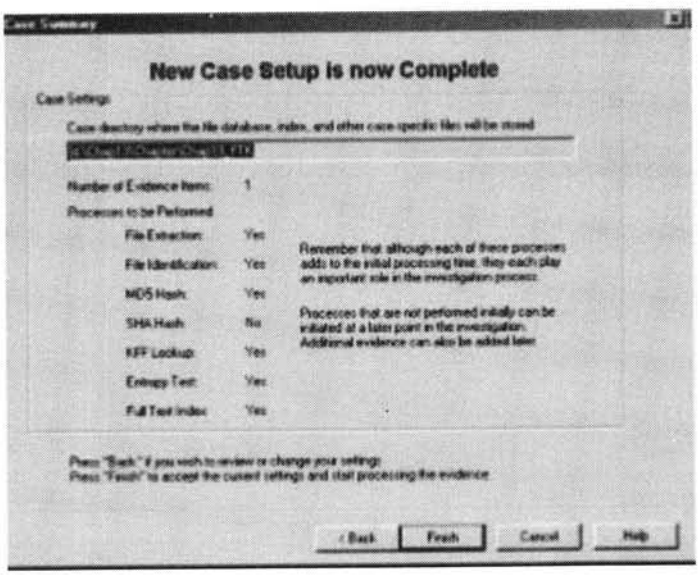


Figure 6-11 Check to make sure that all the information in this window is correct before moving on.

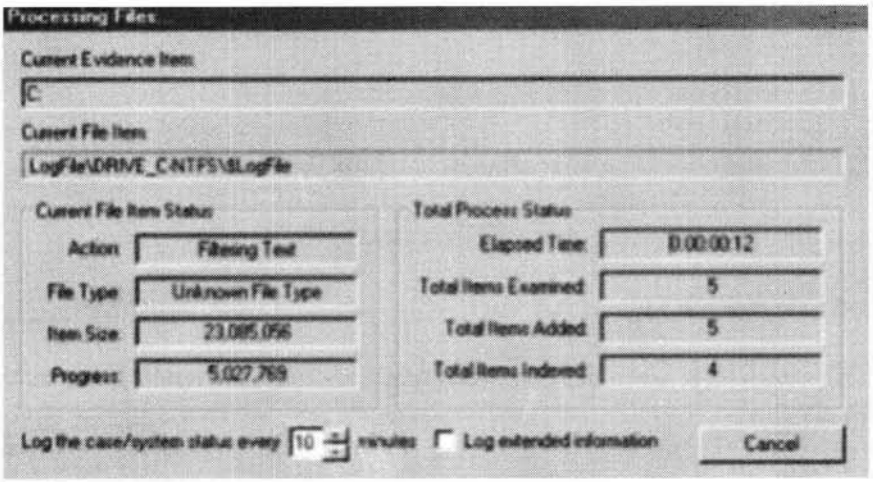


Figure 6-12 This screen shows FTK's progress in processing the evidence files.

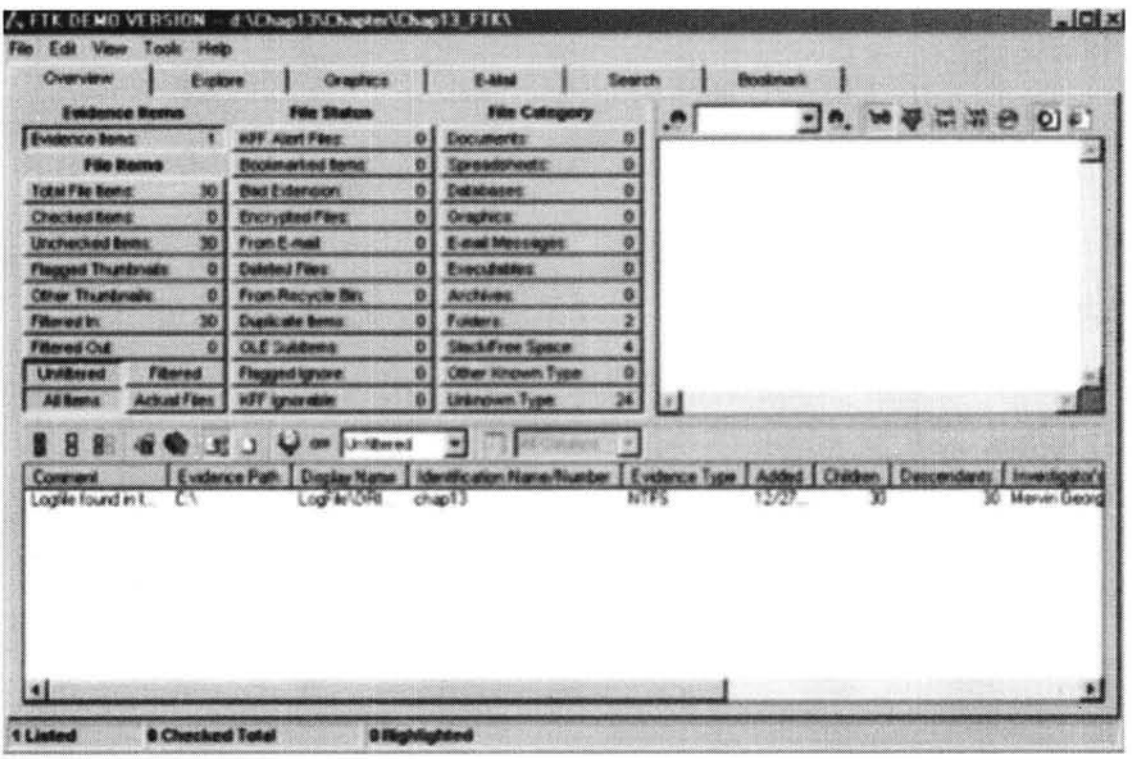


Figure 6-13 The main FTK window shows all of the processed evidence files.

Analyzing with FTK

Perform the following steps to collect pictures with FTK:

1. Click the **Graphics** tab and check the **List all descendants** box.

2. Click any picture in the upper pane and check the box next to its filename.

Locating Encrypted Files with FTK

To locate encrypted files with FTK, click the **Overview** tab, click the **Encrypted Files** button, and click any file in the lower pane.

Viewing Encrypted Files

After locating the encrypted files, perform the following steps to view them:

1. Check the box next to the clicked file.

2. Right-click the file and click **Export File** on the shortcut menu.

3. Uncheck all boxes located at the bottom of the **Export Files** dialog box and click **OK**.

4. Click **OK** in the **Export Files** window message.

Searching with FTK

Perform the following steps to execute an indexed search:

1. Click the **Search** tab.

2. Type the first search term in the **Search Term** field and click **Add**.

3. Then type another search term and click **Add**.

4. Click **View Cumulative Results**.

Perform the following steps to execute a live search:

1. Click the **Live Search** tab in the **Search** pane .

2. Type a keyword and click **Add**. Click **Search**, and then click **OK** in the **Retrieve Search Hits** dialog box.

3. Click **View Results** in the **Live Search Progress** dialog box.

4. To minimize the data, click the **View files in filtered text format** icon .

Creating a Bookmark for Investigation Findings

Perform the following steps to create a bookmark for investigation findings:

1. Right-click any checked file and then click **Create Bookmark** on the shortcut menu.

2. Type **ch13_search_results** in the **Bookmark name** text box. Click **All checked items**, and then check **Include in report** and **Export files** in the **Create New Bookmark** dialog box.

3. To describe the bookmark, type a comment and then click **OK**.

Reviewing Case Findings in FTK

To review case findings in FTK, click the **Overview** tab and then click the **Checked Items** button.

Viewing Selected Items

To view selected items, perform the following steps:

1. Click the first file in the lower pane.

2. The contents of the bookmark can be read by scrolling down the upper-right pane.

3. Type the keyword value in the search text box to locate a specific keyword that is displayed in the upperright pane.

4. To view graphic files, click the **Internet Explorer** icon located above the upper-right pane.

5. To view binary files, click the **HEX** icon.

Running the FTK Report Wizard

1. Go to **File** in the main FTK window and then click **Report Wizard**.

2. Enter the appropriate information in the **Case Information** window. Click **Next**.

. Click **Next** on both the **Bookmarks – A** and **Bookmarks – B** dialog boxes.

4. In the **Graphic Thumbnails** dialog box , check **Export full-size graphics and link them to the thumbnails** and then click **Next**.

5. In the **List by File Path** dialog box , check the **Include a list by file path section in the report** box. Also check the **Include in the report** and **Export to the report** boxes and then click **Next**.

6. In the **Case Audit Files** dialog box, click **Add Files** and navigate to the chap13chapter folder.

7. In the **Open** dialog box, press and hold down the **Ctrl** key to select all the evidence files and then

click **Open**.

8. Click **Next** in the **Case Audit Files** dialog box.

Click **Finish** in the **Report Location** dialog box.

10. Click **Yes** to view the report generated. The report opens in Windows Explorer. Double-click Index.html in the chap13chap13_FTKReport folder to view the report in Internet Explorer.

2. Discuss about the offence and penalties against all the mentioned sections of Information Technology Act, 2000?

The following table shows the offence and penalties against all the mentioned sections of the I.T. Act "

Section	Offence	Punishment	Bailability and Congizability
65	Tampering with Computer Source Code	Imprisonment up to 3 years or fine up to Rs 2 lakhs	Offence is Bailable, Cognizable and triable by Court of JMFC
66	Computer Related Offences	Imprisonment up to 3 years or fine up to Rs 5 lakhs	Offence is Bailable, Cognizable and
66-A	Sending offensive messages through Communication service, etc...	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable and triable by Court of JMFC
66-B	Dishonestly receiving stolen computer resource or communication device	Imprisonment up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-C	Identity Theft	Imprisonment of either description up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-D	Cheating by Personation by using computer resource	Imprisonment of either description up to 3 years and /or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-E	Violation of Privacy	Imprisonment up to 3 years and /or fine up to Rs. 2 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-F	Cyber Terrorism	Imprisonment extend to imprisonment for Life	Offence is Non-Bailable, Cognizable and triable by Court of Sessions

Section	Offence	Punishment	Bailability and Congizability
67	Publishing or transmitting obscene material in electronic form	On first Conviction, imprisonment up to 3 years and/or fine up to Rs. 5 lakh On Subsequent Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh	Offence is Non-Bailable, Cognizable and triable by Court of JMFC
67-A	Publishing or transmitting of material containing sexually explicit act, etc... in electronic form	On first Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non-Bailable, Cognizable and triable by Court of JMFC
67-B	Publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form	On first Conviction imprisonment of either description up to 5 years and/ or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment of either description up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non Bailable, Cognizable and triable by Court of JMFC
67-C	Intermediary intentionally or knowingly contravening the directions about Preservation and retention of information	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.
68	Failure to comply with the directions given by Controller	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
69	Failure to assist the agency referred to in sub section (3) in regard interception or monitoring or decryption of any information through any computer resource	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.
69-A	Failure of the intermediary to comply with the direction issued for blocking for public access of any information through any computer resource	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.

Section	Offence	Punishment	Bailability and Congizability
69-B	Intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) in regard monitor and collect traffic data or information through any computer resource for cybersecurity	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.
70	Any person who secures access or attempts to secure access to the protected system in contravention of provision of Sec. 70	Imprisonment of either description up to 10 years and fine	Offence is Non-Bailable, Cognizable.
70-B	Indian Computer Emergency Response Team to serve as national agency for incident response. Any service provider, intermediaries, data centres, etc., who fails to prove the information called for or comply with the direction issued by the ICERT.	Imprisonment up to 1 year and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable
71	Misrepresentation to the Controller to the Certifying Authority	Imprisonment up to 2 years and/ or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
72	Breach of Confidentiality and privacy	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
72-A	Disclosure of information in breach of lawful contract	Imprisonment up to 3 years and/or fine up to Rs. 5 lakh.	Offence is Cognizable, Bailable
73	Publishing electronic Signature Certificate false in certain particulars	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
74	Publication for fraudulent purpose	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.

1. Elaborate on various Access Control models.

Access Control and Authorization

Access control mechanisms are a necessary and crucial design element to any application's security. In general, a web application should protect front-end and back-end data and system resources by implementing access control restrictions on what users can do, which resources they have access to, and what functions they are allowed to perform on the data. Ideally, an access control scheme should protect against the unauthorized viewing, modification, or copying of data. Additionally, access control mechanisms can also help limit malicious code execution, or unauthorized actions through an attacker exploiting infrastructure dependencies (DNS server, ACE server, etc.).

Authorization and Access Control are terms often mistakenly interchanged. Authorization is the act of checking to see if a user has the proper permission to access a particular file or perform a particular action, assuming that user has successfully authenticated himself. Authorization is very much credential focused and dependent on specific rules and access control lists preset by the web application administrator(s) or data owners. Typical authorization checks involve querying for membership in a particular user group, possession of a particular clearance, or looking for that user on a resource's approved access control list, akin to a bouncer at an exclusive nightclub. Any access control mechanism is clearly dependent on effective and forge-resistant authentication controls used for authorization.

Access Control refers to the much more general way of controlling access to web resources, including restrictions based on things like the time of day, the IP address of the HTTP client browser, the domain of the HTTP client browser, the type of encryption the HTTP client can support, number of times the user has authenticated that day, the possession of any number of types of hardware/software tokens, or any other derived variables that can be extracted or calculated easily.

Before choosing the access control mechanisms specific to your web application, several preparatory steps can help expedite and clarify the design process;

1. Try to quantify the relative value of information to be protected in terms of Confidentiality, Sensitivity, Classification, Privacy, and Integrity related to the organization as well as the individual users. Consider the worst case financial loss that unauthorized disclosure, modification, or denial of service of the information could cause. Designing elaborate and inconvenient access controls around unclassified or non-sensitive data can be counterproductive to the ultimate goal or purpose of the web application.
2. Determine the relative interaction that data owners and creators will have within the web application. Some applications may restrict any and all creation or ownership of data to anyone but the administrative or built-in system users. Are specific roles required to further codify the interactions between different types of users and administrators?

3. Specify the process for granting and revoking user access control rights on the system, whether it be a manual process, automatic upon registration or account creation, or through an administrative front-end tool.

4. Clearly delineate the types of role driven functions the application will support. Try to determine which specific user functions should be built into the web application (logging in, viewing their information, modifying their information, sending a help request, etc.) as well as administrative functions (changing passwords, viewing any users data, performing maintenance on the application, viewing transaction logs, etc.).

5. Try to align your access control mechanisms as closely as possible to your organization's security policy. Many things from the policy can map very well over to the implementation side of access control (acceptable time of day of certain data access, types of users allowed to see certain data or perform certain tasks, etc.). These types of mappings usually work the best with Role Based Access Control.

There are a plethora of accepted access control models in the information security realm. Many of these contain aspects that translate very well into the web application space, while others do not. A successful access control protection mechanism will likely combine aspects of each of the following models and should be applied not only to user management, but code and application integration of certain functions.

Types of access Control

- Discretionary Access Control
- Mandatory Access Control
- Role Based Access Control

Discretionary Access Control

Discretionary Access Control (DAC) is a means of restricting access to information based on the identity of users and/or membership in certain groups. Access decisions are typically based on the authorizations granted to a user based on the credentials he presented at the time of authentication (user name, password, hardware/software token, etc.). In most typical DAC models, the owner of information or any resource is able to change its permissions at his discretion (thus the name). DAC has the drawback of the administrators not being able to centrally manage these permissions on files/information stored on the web server. A DAC access control model often exhibits one or more of the following attributes.

- Data Owners can transfer ownership of information to other users
- Data Owners can determine the type of access given to other users (read, write, copy, etc.)
- Repetitive authorization failures to access the same resource or object generates an alarm and/or restricts the user's access
- Special add-on or plug-in software required to apply to an HTTP client to prevent indiscriminant copying by users ("cutting and pasting" of information)

- Users who do not have access to information should not be able to determine its characteristics (file size, file name, directory path, etc.)
- Access to information is determined based on authorizations to access control lists based on user identifier and group membership.

Mandatory Access Control

Mandatory Access Control (MAC) ensures that the enforcement of organizational security policy does not rely on voluntary web application user compliance. MAC secures information by assigning sensitivity labels on information and comparing this to the level of sensitivity a user is operating at. In general, MAC access control mechanisms are more secure than DAC yet have trade offs in performance and convenience to users. MAC mechanisms assign a security level to all information, assign a security clearance to each user, and ensure that all users only have access to that data for which they have a clearance. MAC is usually appropriate for extremely secure systems including multilevel secure military applications or mission critical data applications. A MAC access control model often exhibits one or more of the following attributes.

- Only administrators, not data owners, make changes to a resource's security label.
- All data is assigned security level that reflects its relative sensitivity, confidentiality, and protection value.
- All users can read from a lower classification than the one they are granted (A "secret" user can read an unclassified document).
- All users can write to a higher classification (A "secret" user can post information to a Top Secret resource).
- All users are given read/write access to objects only of the same classification (a "secret" user can only read/write to a secret document).
- Access is authorized or restricted to objects based on the time of day depending on the labeling on the resource and the user's credentials (driven by policy).
- Access is authorized or restricted to objects based on the security characteristics of the HTTP client (e.g. SSL bit length, version information, originating IP address or domain, etc.)

Role Based Access Control

In Role-Based Access Control (RBAC), access decisions are based on an individual's roles and responsibilities within the organization or user base. The process of defining roles is usually based on analyzing the fundamental goals and structure of an organization and is usually linked to the security policy. For instance, in a medical organization, the different roles of users may include those such as doctor, nurse, attendant, nurse, patients, etc. Obviously, these members require different levels of access in order to perform their functions, but also the types of web transactions and their allowed context vary greatly depending on the security policy and any relevant regulations (HIPAA, Gramm-Leach-Bliley, etc.).

An RBAC access control framework should provide web application security administrators with the ability to determine who can perform what actions, when, from where, in what order, and in some cases under what relational circumstances. http://csrc.nist.gov/rbac/ provides some great resources for RBAC implementation. The following aspects exhibit RBAC attributes to an access control model.

- Roles are assigned based on organizational structure with emphasis on the organizational security policy
- Roles are assigned by the administrator based on relative relationships within the organization or user base. For instance, a manager would have certain authorized transactions over his employees. An administrator would have certain authorized transactions over his specific realm of duties (backup, account creation, etc.)
- Each role is designated a profile that includes all authorized commands, transactions, and allowable information access.
- Roles are granted permissions based on the principle of least privilege.
- Roles are determined with a separation of duties in mind so that a developer Role should not overlap a QA tester Role.
- Roles are activated statically and dynamically as appropriate to certain relational triggers (help desk queue, security alert, initiation of a new project, etc.)
- Roles can be only be transferred or delegated using strict sign-offs and procedures.
- Roles are managed centrally by a security administrator or project leader.

Part B - (2 X 7 = 14 Marks)

Answer Any TWO Questions

4. Discuss on Data Recovery Techniques.

DATA RECOVERY TECHNIQUES

- Use of software to recover data
- Use of machines to recover data

Software Data Extraction

- Data extraction is the process of moving data off of the imaged drive to another destination location.
- Data extraction software scans sectors of the hard drive and restructures the file system either in memory or another hard drive. The software can be used to copy the recoverable data to a destination location

Software Recovery

- Data loss can occur because the hard drive may have problems accessing the data it contains at a software or logical level.
- By making a complete sector copy (an exact copy including all deleted information) of the hard drive, using a program such as Norton GHOST, most data recovery programs search for deleted MFT (Master File Table) entries to undelete files.
- If the MFT is corrupt or defective, this method will not work. Some data recovery programs will ignore the MFT and search all of the unallocated clusters to try to find and recover files.

Data recovery techniques

- **Scanning Probe Microscopy (SPM)**
- **Magnetic Force Microscopy (MFM)**
- **Scanning Tunneling Microscopy (STM)**

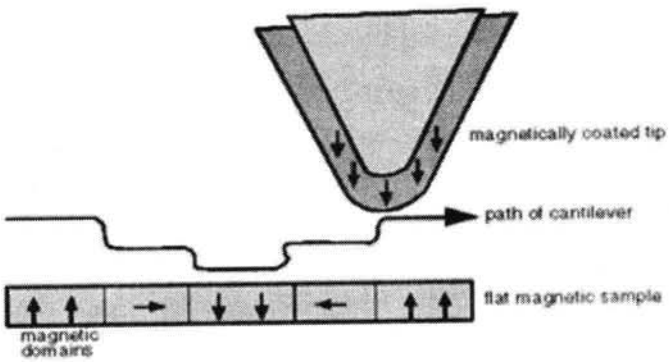
Scanning Probe Microscopy (SPM)

- A technique that is used to image and measure surfaces at the atomic level.
- Scans an atomically sharp probe over a surface which produces a 3D topographic image of the surface at the atomic scale.

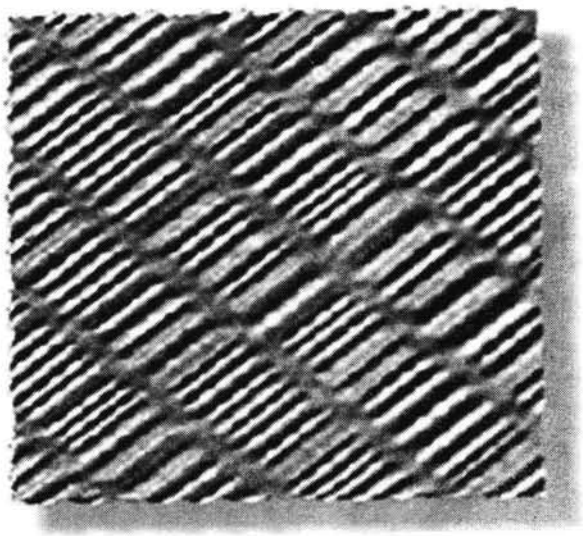
Magnetic Force Microscopy (MFM)

- MFM (Magnetic Force Microscopy) is a new technique which images the spatial variation of magnetic forces on a sample surface.
- MFM is derived from scanning probe microscopy (SPM) and uses a sharp magnetic tip attached to a flexible cantilever for analysis.
- An image of the field at the surface is formed by moving the tip across the surface and measuring the force.
- Detectable old data will be present beside new data on the track which is usually ignored.
- Together with software, MFM can see past various kinds of data loss/removal.
- Each track contains an image of everything ever written to it, but each layer gets progressively smaller the earlier it was written.

MFM looks at the minute sampling region to detect remnant magnetization at track edges.



MFM image showing the bits of a hard disk



Scanning Tunneling Microscopy (STM)

- STM (Scanning Tunneling Microscopy) is a more recent variation of MFM which uses a probe tip typically made by plating nickel onto a pre-patterned surface.
- The probe is scanned across the surface that is to be analyzed. STM measures a weak electrical current flowing between the tip and the sample. The image is then generated in the same way as MFM.

5. What is meant by Android Forensics? List the Procedure for handling Android Forensics.

Android is an open source mobile device platform based on the Linux 2.6 kernel and managed by the Open Handset Alliance—a group of major mobile device, hardware, and software vendors. The open source nature of the project has not only established a new direction for the industry (forcing behemoths like Nokia/Symbian to open source their platform) but enables a developer or code savvy forensic analyst to understand the device at the most fundamental level. As the core platform is quickly maturing and is provided free of charge, carriers and hardware vendors alike can focus their efforts in customizations intended to retain their customers.

Android mobile device Applications for Android are developed in Java and run in a separate Dalvik virtual machine (DVM) with a unique user id and process which is a key mechanism used to enforce data security. Applications can only access the data within their DVM unless another application and the phone owner specifically allows the data to be shared. As a result of this secure architecture, forensic examiners do not have a built-in mechanism we can use on the phone to extract core user data. Instead, new techniques must be developed which require some interaction with the device.

Forensics Strategies for Android Devices

There are four primary ways to approach forensics on an Android device. They are:

- SD Card analysis
- Logical acquisition
- Physical acquisition
- Chip-off

Before exploring these techniques, a brief discussion on the challenges of mobile phone forensics is warranted. A fundamental goal in digital forensics is to prevent any modification of the target device by the examiner. However, mobile phones lack traditional hard drives which can be shutdown, connected to a write blocker, and imaged in a forensically sound way. The end result is that Android forensic techniques, short of chip-off, do alter the device. Examiners must use their discretion when examining a mobile device and if the device is modified, they must explain how it was modified and, as important, why that choice was made.

SD Card Analysis

Nearly every Android device comes with an external SD Card for storing data. Upon receiving and securing an Android device (as you would any other mobile device), an examiner should remove the SD Card and process it in the standard way. The card is formatted with a FAT32 file system.

Logical Analysis

The logical acquisition of an Android device is the technique we recommended first. This technique involves copying a small (~25k) Android Forensics application to the device, running the application, and then removing it from the device. An application, written by viaForensics and distributed for free to law enforcement and government agencies charged with digital forensic responsibilities, currently acquires the following information:

1. Browser history
2. Call Logs
3. Contact Methods
4. External Image Media (meta data)
5. External Image Thumbnail Media (meta data)
6. External Media, Audio, and Misc. (meta data)
7. External Videos (meta data)
8. MMS
9. MMS Parts (includes full images sent via MMS)
10. Organizations
11. People
12. SMS
13. List of all applications installed and version
14. Contacts Extensions
15. Contacts Groups
16. Contacts Phones
17. Contacts Settings

And new data sources are being developed weekly. The data is written to an SD Card the examiner placed into the device. The files are currently written as CSV, however we will likely change this to an XML format. Also, there are some challenges when interpreting this data and we are currently developing viaExtract, a reporting application for the data. The application will be released in the next few months and sold at significant discount to active law enforcement.

Physical Analysis

In some cases, a more significant analysis is required. To this end, we have developed a technique to physically acquire a "dd" image from support Android devices (currently any Android 1.5 devices and Motorola Droid 2.0 and 2.01). This technique requires root privileges on the device and can yield a significant amount of information. This technique will provide a forensic image of the various user data partitions. These partitions use the open source file system YAFFS2 (Yet another Flash File System 2) and is one of the significant challenges with the Android platform.

YAFFS2 was built specifically for the growing NAND memory devices and has a number of important features which address the stringent needs of this medium. It is a log-structured file system, provides built in wear-leveling and error correction, is fast, and has a small footprint in RAM. However, since its usage was limited prior to Android, no commercial forensic product supports the file system.For the brave, you can download the YAFFS2 source code, grab a forensic image of a partition, open it up in your favorite hex editor and start digging. However, we are making progress in the development of some tools. The tools allow an examiner to forensically acquire the NAND data (you cannot use dd for this...we've developed a special nanddump program for this purpose), mount the image in Linux (using nandsim) and extract the data. Traditional techniques such as file carving and strings also work. However, the real potential is in the development of a program which will provide a "point-in-time" version of any file on the YAFFS2 file system; this is a very fortunate (for the forensic examiner) byproduct of YAFFS2 being a log-structured file system.

Chip-off

For those with full lab facilities, there is always the option of using chip-off techniques on the NAND memory.

PROCEDURES FOR HANDLING AN ANDROID DEVICES

The concept of Android forensics consists of techniques to extract the most possible data from the device without losing, or altering the content of the device. Modification of the data or data preservation is the biggest problem when dealing with Android devices.

The technique that is most recommended is live acquisition due to the volatile nature of the device's memory. Live acquisition is recommended because the volatile memory can hold various data which could be of value for the investigation.

The examples of data that could be found in the volatile, RAM memory are:

- Passwords
- Encryption keys
- Usernames
- Application data
- Data from system processes and services

There is a technique developed by security engineer Thomas Cannon which helps acquiring significant application data. The technique is using the Android's ability to dump the application memory to a file by sending the application a special signal - SIGUSR1 (Hoog, 2011). Tendencies are that there will be more solutions to help analysis of the Android memory in the future.

Procedures for handling an Android device

Procedures for handling the Android device are the same as the procedures for handling the personal computer or lap top. The procedures still have five steps that are very important to hold on to while handling the device. The five steps are:

- Identifying
- Preserving
- Acquiring
- Analyzing
- Reporting

As in the computer forensic investigation, the chain of custody must be followed as well. Regardless of whether the investigation is in the corporate environment or is a part of the criminal investigation, it is necessary to follow the rules for evidence handling. Any case in any time can end up in court. The best practice is that investigation should always be conducted as the case will be in the court of law. The important considerations while conducting the Android device investigation are:

• Chain of custody

• Detailed notes and final reports

Validation of results by different tools or examiners

• Fact or opinion based testimony (Hoog, 2011).

Andrew Hoog thinks the four principles of electronic based computer evidence are of the essence. The four principles are:

1. No action taken by law enforcement agencies or their agents should change data held on a computer or storage media, which may subsequently be relied upon in court.

2. In circumstances where a person finds it necessary to access original data held on a computer or on the storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

3. An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result. 4. The person in charge of the investigation (the case officer) has overall responsibility for ensuring that law and these principles are adhered to. (Hoog, 2011)

Handling the Android device is different than handling personal Computer in the investigation. The nature of the handheld device that loses some important data if powered off makes the distinction from personal computer handling. It is also very important to secure device from locking down, accessing network or losing power.

Techniques for securing the device vary from pass code procedures, through powering, to network isolation. On most Android devices, pass code locking could be circumvented by:

1. Increasing the timeout to prevent or postpone the screen locking.

2. Enabling the USB debugging and "stay awake".

1. Explain the steps and techniques involved in Money Laundering.

Steps in Money Laundering

Money laundering is accomplished in many ways, though most include three common steps, including

1. Obtaining the money or introducing it into the financial system in some way
2. Transferring or concealing the source of the money through complex or multiple transactions
3. Returning the money back into the financial world so that it appears legitimate.

Of these steps, placement of the money into financial institutions is the most difficult. This is because the Bank Secrecy Act of 1970 requires financial institutions to report deposits over $10,000 in a single day. To circumvent this step then, launderers funnel cash through a legitimate high-cash business, such as a check cashing service, bar, nightclub, or convenience store.

Money Laundering Techniques

There are many forms of money laundering though some are more common and profitable than others. Some of the more popular money laundering techniques include:

- **Bulk cash smuggling** involves literally smuggling cash into another country for deposit into offshore banks or other type of financial institutions that honor client secrecy.
- **Structuring**, also referred to as "smurfing," is a method in which cash is broken down into smaller amount, which are then used to purchase money orders or other instruments to avoid detection or suspicion.
- **Trade-based laundering** is similar to embezzlement in that invoices are altered to show a higher or lower amount in order to disguise the movement of money.
- **Cash-intensive business** occurs when a business that legitimately deals with large amounts of cash uses its accounts to deposit money obtained from both everyday business proceeds and money obtained through illegal means. Businesses able to claim all of these proceeds as legitimate income include those that provide services rather than goods, such as strip clubs, car washes, parking buildings or lots, and other businesses with low variable costs.

- **Shell companies** and trusts are used to disguise the true owner or agent of a large amount of money.
- **Bank capture** refers to the use of a bank owned by money launderers or criminals, who then move funds through the bank without fear of investigation.
- **Real estate laundering** occurs when someone purchases real estate with money obtained illegally, then sells the property. This makes it seem as if the profits are legitimate.
- **Casino laundering** involves an individual going into a casino with illegally obtained money. The individual purchases chips with the cash, plays for a while, then cashes out the chips, and claims the money as gambling winnings.

Part C - (5 X 4 = 20 Marks)

7.Answer Any FIVE Questions

a) Explain the Classes of Cybercrime.

Two classes of cyber crimes:

A. Computer Assisted Cyber Crimes: computer is instrumental in committing the crime.

Selling nonexistent, defective, substandard or counterfeit goods, theft of credit card, bank fraud, fake stock shares, intellectual property offences including unauthorized sharing of the copy righted content of movies, music, digitized books

- Selling obscene and prohibited sexual representations.

B. Computer Oriented Cyber Crimes: Computer is the target of the crime

- Malicious Software: viruses, Trojans (which corrupt server)
- Cyber terrorism:
- Child pornography
- Violent and extreme pornography
- Internet inspired homicides and suicides

❖ *Worm: Self-replicating programmes, spread autonomously without a carrier.*

❖ *Trojan: installed during downloading some programme as a back ground activity causing irreparable damage*

❖ *Spyware: parasitic software-invades privacy-divulging details- through tracking cookies.*

Even though our basic understanding about cyber crime is that computer is necessary as one of the components of the offence, it is also interpreted that a crime committed by using any digital device is covered under the ambit of cyber crime. For example: Casio digital diary, Mobiles, Calculators, Pen drives, CDs.

At the onset, let us satisfactorily define "cybercrime" and differentiate it from "conventional Crime". Computer crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

b) What is social engineering?

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

SOCIAL ENGINEERING ATTACK TECHNIQUES

Social engineering attacks come in many different forms and can be performed anywhere where human interaction is involved. The following are the five most common forms of digital social engineering assaults.

Baiting

As its name implies, baiting attacks use a false promise to pique a victim's greed or curiosity. They lure users into a trap that steals their personal information or inflicts their systems with malware.

The most reviled form of baiting uses physical media to disperse malware. For example, attackers leave the bait—typically malware-infected flash drives—in conspicuous areas where potential victims are certain to see them (e.g., bathrooms, elevators, the parking lot of a targeted company). The bait has an authentic look to it, such as a label presenting it as the company's payroll list.

Victims pick up the bait out of curiosity and insert it into a work or home computer, resulting in automatic malware installation on the system.

Baiting scams don't necessarily have to be carried out in the physical world. Online forms of baiting consist of enticing ads that lead to malicious sites or that encourage users to download a malware-infected application.

Scareware

Scareware involves victims being bombarded with false alarms and fictitious threats. Users are deceived to think their system is infected with malware, prompting them to install software that has no real benefit (other than for the perpetrator) or is malware itself. Scareware is also referred to as deception software, rogue scanner software and fraudware.

A common scareware example is the legitimate-looking popup banners appearing in your browser while surfing the web, displaying such text such as, "Your computer may be infected with harmful spyware programs." It either offers to install the tool (often malware-infected) for you, or will direct you to a malicious site where your computer becomes infected.

Scareware is also distributed via spam email that doles out bogus warnings, or makes offers for users to buy worthless/harmful services.

Pretexting

Here an attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by a perpetrator pretending to need sensitive information from a victim so as to perform a critical task.

The attacker usually starts by establishing trust with their victim by impersonating co-workers, police, bank and tax officials, or other persons who have right-to-know authority. The pretexter asks questions that are ostensibly required to confirm the victim's identity, through which they gather important personal data.

All sorts of pertinent information and records is gathered using this scam, such as social security numbers, personal addresses and phone numbers, phone records, staff vacation dates, bank records and even security information related to a physical plant.

Phishing

As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.

An example is an email sent to users of an online service that alerts them of a policy violation requiring immediate action on their part, such as a required password change. It includes a link to an illegitimate website—nearly identical in appearance to its legitimate version—prompting the unsuspecting user to enter their current credentials and new password. Upon form submittal the information is sent to the attacker.

Given that identical, or near-identical, messages are sent to all users in phishing campaigns, detecting and blocking them are much easier for mail servers having access to threat sharing platforms.

Spear phishing

This is a more targeted version of the phishing scam whereby an attacker chooses specific individuals or enterprises. They then tailor their messages based on characteristics, job positions, and contacts belonging to their victims to make their attack less conspicuous. Spear phishing requires much more effort on behalf of the perpetrator and may take weeks and months to pull off. They're much harder to detect and have better success rates if done skillfully.

A spear phishing scenario might involve an attacker who, in impersonating an organization's IT consultant, sends an email to one or more employees. It's worded and signed exactly as the consultant normally does, thereby deceiving recipients into thinking it's an authentic message. The message prompts recipients to change their password and provides them with a link that redirects them to a malicious page where the attacker now captures their credentials.

c) What Causes Data Loss?

Cause	Example	Percentage
Hardware & System Problems	Disk drive crashes, electrical outages or power surges, manufacturer defects.	45%
Human Errors	Accidental deletions, overwriting files, causing trauma to desktop or laptop.	33%
Software Corruption or Application Error	Application displays an error message when a document is opened. Installing or removing a program corrupts another.	12%
Computer Viruses	i.e.: MyDoom.A MyDoom.B W32.Welchia.Worm W32.Blaster.Worm W32.Spybot.Worm Downloader.Trojan W32.Swen.A@mm	6%
Natural Disasters	Fires, floods, lightning, earthquakes.	4%

d) Brief on Time-Frame Analysis

In situations where an individual is suspected of using a certain computer, time-frame analysis can contribute to associating the events that occurred on the computer with that individual.

Time-frame analysis can be performed using two methods:

1. The first involves reviewing the time stamps and date stamps that are found in the file system metadata (for example, when the files were last modified, last accessed, created, or changed status). These clues might provide useful details to further the investigation. An example of this analysis would be using the last modified date and time to establish when the contents of a file were last changed.

2. The second method involves reviewing the application logs that are found (the logs may include the error logs, installation logs, connection logs, and security logs). For example, examination of a security log may indicate when a user name/password combination was used to log in to a system.

e) Explain various types of Wireless Network.

TYPES OF WIRELESS NETWORKS

WLANS: Wireless Local Area Networks

WLANS allow users in a local area, such as a university campus or library, to form a network or gain access to the internet. A temporary network can be formed by a small number of users without the need of an access point; given that they do not need access to network resources.

WPANS: Wireless Personal Area Networks

The two current technologies for wireless personal area networks are Infra Red (IR) and Bluetooth (IEEE 802.15). These will allow the connectivity of personal devices within an area of about 30 feet. However, IR requires a direct line of site and the range is less.

WMANS: Wireless Metropolitan Area Networks

This technology allows the connection of multiple networks in a metropolitan area such as different buildings in a city, which can be an alternative or backup to laying copper or fiber cabling.

WWANS: Wireless Wide Area Networks

These types of networks can be maintained over large areas, such as cities or countries, via multiple satellite systems or antenna sites looked after by an ISP. These types of systems are referred to as 2G (2nd Generation) systems.

f) Discuss on SMS security

SMS SECURITY

The technical specifications for SMS are laid down in ETSI TS 03.485 . Certain options in the technical specification, such as the Security Parameter Index (SPI), the Ciphering Key Identifier (KIc), and the Integrity Value (RC/CC/ DS), provide specifications for available security parameters. A Redundancy Check (RC), Cryptographic Checksum (CC) or Digital Signature (DS) might also be used for integrity verification of the data. However, these confidentiality and integrity mechanisms are only specified as optional security measures that can be made available, but they are not mandatory requirements for SMS system implementation6 . The availability of SMS services may also be interrupted by the SMSC. Without proper implementation of these SMS security options, everyday SMS messages transmitted on a network are only protected by the communication network itself such as a GSM network. In practical use, SMS messages are not encrypted by default during transmission. A cyclic redundancy check is provided for SMS information passing across the signalling channel to ensure short messages do not get corrupted. Forward error protection is also incorporated using conventional encoding. Cryptographic protection on confidentiality and integrity is not available for SMS messages.

Digital cellular telecommunications system (Phase 2+); Technical realization of the Short Message Service (SMS) Point-to-Point (PP) 3GPP TS 03.40 version 7.5.0 ,1998 ETSI TS 100 901 V7.5.0 (2001-12).

SMS Attacks

- Denial of Service in the network or the phone with consecutive messages (from another phone or the net) –Phone Buffers –SMSC Buffers
- Long names, invalid characters –Especially crafted Vcards –Especially crafted SMSs (i.e. Broken UDH) –Obexftp through Bluetooth
- History: Nokia 5100 all dot SMS crash
- SMS spoofing

SMS flash

• Flash message appears immediately on the screen usually close to the Network Name

• User does not have to "open" the message to read it. It is already "opened"

• Can deceit the user to trust that it comes from the provider. Can be used for various Social Engineering attacks.

SMS ping

• Every simple user (not the mighty provider!) can stealthily discover whether another user has her cell phone switched on or off!

• He can reveal her behavior using patterning techniques (i.e. time of awakening or sleeping)

SMS Spoofing

Bulk SMS through marketing companies Bulksms, Prosms, Websms, Sendsms You can arbitrarily chose originator name or number 11 latin characters or 16-digit number Interconnection fee.

g) Explain Public Key Cryptography.

PUBLIC-KEY CRYPTOGRAPHY,

Public-key cryptography, or asymmetric cryptography, is an encryption scheme that uses two mathematically related, but not identical, keys - a public key and a private key. Unlike symmetric key algorithms that rely on one key to both encrypt and decrypt, each key performs a unique function. The public key is used to encrypt and the private key is used to decrypt.

It is computationally infeasible to compute the private key based on the public key. Because of this, public keys can be freely shared, allowing users an easy and convenient method for encrypting content and verifying digital signatures, and private keys can be kept secret, ensuring only the owners of the private keys can decrypt content and create digital signatures.

Since public keys need to be shared but are too big to be easily remembered, they are stored on digital certificates for secure transport and sharing. Since private keys are not shared, they are simply stored in the software or operating system you use, or on hardware (e.g., USB token, hardware security module) containing drivers that allow it to be used with your software or operating system.

Digital certificates are issued by entities known as Certificate Authorities (CAs).

The main business applications for public-key cryptography are:

- **Digital signatures** - content is digitally signed with an individual's private key and is verified by the individual's public key
- **Encryption** - content is encrypted using an individual's public key and can only be decrypted with the individual's private key

Part D - (6 X 2 = 12 Marks)

8. Answer Any SIX Questions

a) Define Cybercrime.

Defining cybercrimes, as "acts that are punishable by the Information Technology Act" would be unsuitable as the Indian Penal Code also covers many cybercrimes, such as email spoofing and cyber defamation, sending threatening emails etc. A simple yet sturdy definition of cybercrime would be "unlawful acts wherein the computer is either a tool or a target or both".

b) What is E-Mail spoofing?

Email spoofing

A spoofed email is one that appears to originate from one source but actually has been sent from another source.

Email spoofing can also cause monetary damage. In an American case, a teenager made millions of dollars by spreading false information about certain companies whose shares he had short sold. This misinformation was spread by sending spoofed emails, purportedly from news agencies like Reuters, to share brokers and investors who were informed that the companies were doing very badly. Even after the truth came out the values of the shares did not go back to the earlier levels and thousands of investors lost a lot of money.

c) **What is meant by audit trails and logs?**

A system can maintain several different audit trails concurrently. There are typically two kinds of audit records,

(1) an event-oriented log and

(2) a record of every keystroke, often called keystroke monitoring. Event-based logs usually contain records describing system events, application events, or user events.

An audit trail should include sufficient information to establish what events occurred and who (or what) caused them. In general, an event record should specify when the event occurred, the user ID associated with the event, the program or command used to initiate the event, and the result. Date and time can help determine if the user was a masquerader or the actual person specified.

d) **What is Data Recovery?**

Data recovery is the process of retrieving or restoring digital information that is no longer accessible for some reason. A good example would be any file that has been mistakenly deleted, lost, or corrupted. The data recovery process varies based on the circumstances under which it was lost.

Data Recovery

- The majority of data loss situations are recoverable.
- Computer storage systems may fail, but the data stored on them is not always completely lost.
- There are occasions when damage to data is permanent and complete data recovery is not possible.
- However, some data is usually always recoverable.
- Data recovery professionals can recover data from crashed hard drives, operating systems, storage devices,
- servers, desktops, and laptops using various proprietary data recovery tools and techniques.

e) Define War driving.

WARDRIVING

War driving is the act of searching for Wi-Fiwireless networks by a person in a moving vehicle, using a laptop or smartphone. Software for war driving is freely available on the Internet.

War biking or **war cycling** is similar to war driving, but is done from a moving bicycle or motorcycle. This practice is sometimes facilitated by mounting a Wi-Fi enabled device on the vehicle. **War walking**, or war jogging, is similar to war driving, but is done on foot rather than from a moving vehicle. War railing, or war training, is similar to war driving, but is done on a train or tram. War droning is accomplished with a drone.

f) Define Cyber Security.

Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security.

g) What is meant by Copy right?

A **copyright** is a form of legal protection automatically provided to the authors or creators of original works. Copyright protection is vast and very inclusive. It applies to items such as original literary, dramatic, musical, choreographic, photographic, architectural, and artistic works.

h) What is Digital signature?

Authentication of electronic records

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record. Explanation- For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible-

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.