SUBJECT CODE : CS8074

Strictly as per Revised Syllabus of

ANNA UNIVERSITY

Choice Based Credit System (CBCS)

Semester - VIII (CSE / IT)
Professional Elective - IV

CYBER FORENSICS

Iresh A. Dhotre
M.E. (Information Technology)
Ex-Faculty, Sinhgad College of Engineering,
Pune.

® TECHNICAL ®
PUBLICATIONS
SINCE 1993
An Up-Thrust for Knowledge

Cyber Forensics

Subject Code : CS8074

Semester - VIII (CSE / IT) Professional Elective - IV

Published by :

TECHNICAL PUBLICATIONS
SINCE 1993
An Up-Thrust for Knowledge

Amit Residency, Office No.1, 412, Shaniwar Peth,
Pune - 411030, M.S. INDIA, Ph.: +91-020-24495496/97
Email : sales@technicalpublications.org Website : www.technicalpublications.org

Printer :
Yogiraj Printers & Binders
Sr.No. 10/1A,
Ghule Industrial Estate, Nanded Village Road,
Tal. - Haveli, Dist. - Pune - 411041.

ISBN 978-93-90450-40-4

9 789390 450404

AU 17

PREFACE

The importance of **Cyber Forensics** is well known in various engineering fields. Overwhelming response to my books on various subjects inspired me to write this book. The book is structured to cover the key aspects of the subject **Cyber Forensics.**

The book uses plain, lucid language to explain fundamentals of this subject. The book provides logical method of explaining various complicated concepts and stepwise methods to explain the important topics. Each chapter is well supported with necessary illustrations, practical examples and solved problems. All the chapters in the book are arranged in a proper sequence that permits each topic to build upon earlier studies. All care has been taken to make students comfortable in understanding the basic concepts of the subject.

Representative questions have been added at the end of each section to help the students in picking important points from that section.

The book not only covers the entire scope of the subject but explains the philosophy of the subject. This makes the understanding of this subject more clear and makes it more interesting. The book will be very useful not only to the students but also to the subject teachers. The students have to omit nothing and possibly have to cover nothing more.

I wish to express my profound thanks to all those who helped in making this book a reality. Much needed moral support and encouragement is provided on numerous occasions by my whole family. I wish to thank the **Publisher** and the entire team of **Technical Publications** who have taken immense pain to get this book in time with quality printing.

Any suggestion for the improvement of the book will be acknowledged and well appreciated.

Author
D.A.Dhotre

Dedicated to God

SYLLABUS

Cyber Forensics - CS8074

UNIT I INTRODUCTION TO COMPUTER FORENSICS

Introduction to Traditional Computer Crime, Traditional problems associated with Computer Crime. Introduction to Identity Theft & Identity Fraud. Types of CF techniques - Incident and incident response methodology - Forensic duplication and investigation. Preparation for IR : Creating response tool kit and IR team. - Forensics Technology and Systems - Understanding Computer Investigation - Data Acquisition. **(Chapter - 1)**

UNIT II EVIDENCE COLLECTION AND FORENSICS TOOLS

Processing Crime and Incident Scenes - Working with Windows and DOS Systems. **Current Computer Forensics Tools** : Software/ Hardware Tools. **(Chapter - 2)**

UNIT III ANALYSIS AND VALIDATION

Validating Forensics Data - Data Hiding Techniques - Performing Remote Acquisition - Network Forensics - Email Investigations - Cell Phone and Mobile Devices Forensics. **(Chapter - 3)**

UNIT IV ETHICAL HACKING

Introduction to Ethical Hacking - Footprinting and Reconnaissance - Scanning Networks - Enumeration - System Hacking - Malware Threats - Sniffing. **(Chapter - 4)**

UNIT V ETHICAL HACKING IN WEB

Social Engineering - Denial of Service - Session Hijacking - Hacking Web servers - Hacking Web Applications - SQL Injection - Hacking Wireless Networks - Hacking Mobile Platforms. **(Chapter - 5)**

TABLE OF CONTENTS

UNIT - I

Chapter 1 : Introduction to Computer Forensics 1 - 1 to 1 - 36

UNIT - II

UNIT - III

UNIT - IV

UNIT - V

Notes

UNIT - I

1 Introduction to Computer Forensics

Scope of the Syllabus

Introduction to Traditional Computer Crime, Traditional problems associated with Computer Crime. Introduction to Identity Theft & Identity Fraud. Types of CF techniques - Incident and incident response methodology - Forensic duplication and investigation. Preparation for IR: Creating response tool kit and IR team. - Forensics Technology and Systems -Understanding Computer Investigation – Data Acquisition.

1.1 Introduction to Traditional Computer Crime

- **Cyber crime** is any criminal activity involving computers and networks. The **cyber space** includes computer systems, computer networks and Internet. LAN and WAN is also part of cyber space. Cybercrime incorporates anything from downloading illegal music files to stealing millions of rupees from online bank accounts.
- **Cyber crime** is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Internet connected activities are as vulnerable to crime.
- Computer crime is any illegal activity that is perpetrated through the use of a computer.
- If a person without the permission of owner or any other person in charge of a computer, computer system or computer network, accesses or secures access to such computer, computer system or computer network, the said acts are torts and crimes under the Indian cyber law.
- There is no standard definition for “CYBER”. This word is used to describe the virtual world of computers e.g. an object in cyberspace refers to a block of data floating around a computer system or network.
- The word “cyberspace” is credited to William Gibson, who used it in his book, Neuromancer, written in 1984.
- **Cyber space :** The impression of space and community formed by computers, computer networks, and their users; the virtual “world” that Internet users inhabit when they are online.

- The term 'cyber' is derived from the word 'cybernetics' which means science of communication and control over machine and man. Cyberspace is the new horizon which is controlled by machine for information and communication between human beings across the world. Therefore, crimes committed in cyberspace are to be treated as cyber crimes. In wider sense, cyber crime is a crime on the Internet which includes hacking, terrorism, fraud, gambling, cyber stalking, cyber theft, cyber pornography, flowing of viruses etc.
- Over the past few years, the global cyber crime landscape has changed dramatically, with criminals employing more sophisticated technology and greater knowledge of cyber security. Until recently, malware, spam emails, hacking into corporate sites and other attacks of this nature were mostly the work of computer 'geniuses' showcasing their talent.

➤ Three Categories of Cybercrime

a. **Cyberpiracy :** Using cyber-technology in unauthorized ways to reproduce copies of proprietary software and proprietary information, or distribute proprietary information (in digital form) across a computer network.
   - **Example :** Distributing proprietary MP3 files on the Internet via peer-to peer (P2P) technology

b. **Cybertrespass :** Using cyber-technology to gain or to exceed unauthorized access to an individual's or an organization's computer system, or a password-protected Web site.
   - **Example :** Unleashing the ILOVEYOU computer virus

c. **Cybervandalism :** Using cyber-technology to unleash one or more programs that disrupt the transmission of electronic information across one or more computer networks, including the Internet, or destroy data resident in a computer or damage a computer system's resources, or both.
   - **Example :** Launching the denial-of-service attacks on commercial Web sites.

➤ Elements of Cyber Crime :

1. **Location/Place :** Where offender is in relation to crime.
2. **Victim :** Target of offense - government, corporation, organization, individual
3. **Offender :** Who the offender is in terms of demographics, motivation, level of sophistication.
4. **Action :** What is necessary to eliminate threat ?

- Cyber criminals are now moving beyond computers, and attacking mobile handheld devices, such as smart phones and tablet personal computers. In 2010, the number of malicious software programs specifically targeting mobile devices, rose 46 %, according to information technology security group McAfee.
- **Cybersquatting** is generally bad faith registration of another's trademark in a domain name. Cybersquatting refers to using an Internet domain name with the intent of profiting from someone else's name recognition. It generally is associated with the practice of buying up domain names that are similar to the names of existing businesses with the intent to sell these names back to the owners. Many organizations have to buy all related domain names to prevent cybersquatting.

- **Cyber crime example :** Child pornography, which includes the creation, distribution, or accessing of materials that sexually exploit underage children. Contraband to include transferring illegal items via the Internet.
- Online fraud and hacking attacks are just some examples of computer-related crimes that are committed on a large scale every day.

➥ 1.1.1 Types of Cybercrime

- There are many types of cyber crimes and the most common ones are explained below :
  1. **Hacking :** This is a type of crime wherein a person's computer is broken so that his personal or sensitive information can be accessed.
  2. **Theft :** This crime occurs when a person violates copyrights and downloads music, movies, games and software.
  3. **Cyber stalking :** This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails.
  4. **Identity theft :** This has become a major problem with people using the Internet for cash transactions and banking services. In this cyber crime, a criminal accesses data about a person's bank account, credit cards, debit card and other sensitive information to siphon money or to buy things online in the victim's name.
  5. **Malicious software :** These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.
  6. **Child soliciting and abuse :** This is also a type of cyber crime wherein criminals solicit minors via chat rooms for the purpose of child pornography.

➤ Example of cyber crime :

a. Online banking fraud

b. Fake antivirus

c. Stranded traveler' scams

d. Fake escrow' scams

e. Advanced fraud

f. Infringing pharmaceuticals

g. Copyright-infringing software

h. Copyright-infringing music and video

i. Online payment card fraud

j. In-person payment card fraud

k. Industrial cyber-espionage and extortion

l. Welfare fraud

- The trafficking, distribution, posting, and dissemination of obscene material including pornography, indecent exposure, and child pornography, constitutes one of the most important Cybercrimes known today. Stealing the significant information, data, account number, credit card number transmit the data from one place to another. Hacking and cracking are amongst the gravest Cybercrimes known till date.

➥ 1.1.2 Recognizing and Defining Computer Crime

- First computer crime really unknown. As no written or formal communications were enough at the time. Certainly had to be the theft or destruction of an abacus. First documented case is in early 19th Century in which the sabotage of a computer system developed by textile manufacturer, Joseph Jacquard. This machine, designed to introduce automated tasks, was attacked by individuals fearful of losing employment to computers.

- Prior to the 1980s, computer crime was considered a non-issue. However, three incidents shook American complacency to its core.

  a. Compromising of Milnet b. The Morris Worm c. Crash of AT and T.

- Robert Morris created a worm to impress his friends, but did not recognize the potentiality for destruction. It was attempted to warn victims and instructing them on how to remove the worm prior to massive destruction. But it is too late. It caused millions of dollars in damage and crippled 10 % of all computers connected to the Internet. First person convicted under the new computer fraud and abuse act.
- AT&T crashes due to their own failures but blame shifted to legion of doom.
- India owes a lot to the exponential growth of the Information Technology service industry over the last 15 years. In India we have substantially or fully adopted law as first codified act in the Information Technology Act (“IT Act), in the year 2000.

1.2 Clarification of Terms AU : Dec.-16.

- Crimes motivated by profit are different from those driven by passion, peer pressure or simple perversity of human nature. The profit-driven criminal can be assumed to behave in a way analogous to the profit-maximizing corporation.
- Computer crime has been traditionally defined as any criminal act committed via computer. Cybercrime has traditionally encompassed abuses and misuses of computer systems which result in direct and/or concomitant losses.
- Computer-related crime has been defined as any criminal act in which a computer is involved, usually peripherally devices.

1.2.1 Traditional Problems Associated with Computer Crime

- Individuals seeking a crime have always displayed a remarkable ability to adapt to changing technologies, environments, and lifestyles. Computer crime poses a daunting task for law enforcement agencies because they are highly technical crimes.
- Law enforcement agencies must have individuals trained in computer forensics in order to properly investigate computer crimes. Additionally, countries must update and create legislation, which prohibits computer crimes and outlines appropriate punishments for those crimes.
- Computer crimes will likely become more frequent with the advent of further technologies. It is important that civilians, law enforcement officials, and other members of the criminal justice system are knowledgeable about computer crimes in order to reduce the threat they pose.
- The earliest computer crimes were characterized as non-technological specific. Theft of computer components and software piracy were particular favorites. Hacking and technologically complicated computer crime came later.

University Question

1. Elaborate on the problems associated with computer crime. **AU : Dec.-16, Marks 16**

1.3 Introduction to Identity Theft and Identity Fraud

- Identity theft is the crime of using someone else's personal information, such as an account number, driver's license, health insurance card or Social Security number, to commit fraud.
- ID Theft is a form of fraud. Identity thieves may use a variety of low and high-tech methods to gain access to your personally identifying information.
- Once an identity has been stolen it can be used to withdraw money, open new bank accounts, apply for loans or credit cards, and purchase vehicles or property. In some cases, the thief may even use the stolen identity to engage in criminal activity.
- Identity theft occurs when someone wrongfully acquires and uses a consumer's personal identification, credit, or account information. Identity is a set of attributes of a person or company in a specific domain. An entity has multiple digital Identities.
- Fraud is an intentional effort to deceive another individual for personal gain
- Information is used in following purposes :
  1. To apply for a new driver's license
  2. To open new bank accounts
  3. To apply for credit cards
  4. To apply for loan
  5. To get a job
  6. To rent an apartment
  7. To make retail purchases
  8. Staying in the hotel
  9. For cyber crime
- Common ways Identity Theft occurs :
  1. Defrauding businesses or institutions.
  2. Stealing records from their employer
  3. Bribing an employee who has access to the records
  4. Conning information out of employees
  5. Hacking into the organization's computers
  6. Rummaging through your trash, the trash of businesses, or dumps in a practice known as "dumpster diving."
- Identity theft generally involves three stages: acquisition, use, and discovery.
- Evidence suggests that the longer it takes to discover the theft, the greater the loss incurred and the smaller the likelihood of successful prosecution. Older persons and those with less education are less likely to discover the identity theft quickly and to report it after discovery.
- There are a lot of ways that thieves can steal an identity. One way is to get possession of a person's debit card (ATM card) and their Personal Identification Number (PIN).

- Another way thieves steal information is by "phishing." Phishing involves sending an e-mail to a user falsely claiming to be a legitimate business or organization in an attempt to scam the user into disclosing private information. Usually, there is an HTML link within the e-mail that you are asked to click on. Once you click on the link you are taken to a fraudulent Web site and asked to provide personal information.
- Three main areas of vulnerability to identity theft :
  1. Practices and operating environments of document-issuing agencies that allow offenders to exploit opportunities to obtain identity documents.
  2. Practices and operating environments of document-authenticating agencies that allow offenders access to identity data, subsequently used for financial gain, avoiding arrest, or remaining anonymous.
  3. The structure and operations of the information systems involved with the operational procedures of agents in (1) and (2).
- **Identity theft** has become a major problem with people using the Internet for cash transactions and banking services. In this cyber crime, a criminal accesses data about a person's bank account, credit cards, debit card and other sensitive information to siphon money or to buy things online in the victim's name.
- Four approaches used by identity thieves
  1. Create a data breach
  2. Purchase personal data
  3. Use phishing to entice users to give up data
  4. Install spyware to capture keystrokes of victims

➤ How Thieves Steal Your Identity :

1. **Phishing :** Phishing scams are spam emails sent by cybercriminals that pretend to be from a legitimate person or organization with the intent of tricking you into revealing personal information.
2. **Spim :** Spim is spam sent via instant messaging (IM). The IMs could include spyware, keyloggers, viruses, and links to phishing sites.
3. **Spyware :** This is software that a hacker surreptitiously installs on your computer to collect personal information. It can also be used to direct you to fake websites, change your settings, or take control of your computer in other ways.
4. **Pharming :** In a pharming attempt, a hacker installs malicious code on your personal computer to direct you to fake websites without your knowledge.
5. **Keyloggers :** A keylogger is a form of spyware that records keystrokes as you type.
6. **Trojan horse :** A Trojan horse is a malicious program that appears to be harmless.

➤ How You Can Protect Yourself

1. Keep personal data private. When a person, website, or email asks for your personal information, ask yourself if it is standard practice for such information to be requested.

2. Use strong passwords.
3. Practice safe surfing on public hotspots : If you are using a public computer or accessing the Internet from a public hotspot or an unsecured wireless connection, do not log in to banking and credit card sites.
4. Secure your wireless network.
5. Review your financial statements promptly.

1.4 Types of Computer Forensics Techniques

- **Computer forensics** is the science of locating, extracting and analyzing types of data from difference devices, which specialists then interpret to serve as legal evidence.
- **Digital forensics** is the scientific acquisition, analysis and preservation of data contained in electronic media whose information can be used as evidence in a court of law.
- Computer Forensics is a four step process :
  1. **Acquisition :** Physically or remotely obtaining possession of the computer, all network mappings from the system, and external physical storage devices.
  2. **Identification :** This step involves identifying what data could be recovered and electronically retrieving it by running various computer forensic tools and software suite.
  3. **Evaluation :** Evaluating the information/data recovered to determine if and how it could be used again the suspect for employment termination or prosecution in court
  4. **Presentation :** This step involves the presentation of evidence discovered in a manner which is understood by lawyers, non-technically staff/management, and suitable as evidence as determined by United States and internal laws.

➤ Need for computer forensic techniques :

1. Legal cases : computer forensic techniques are frequently used to analyze computer systems belonging to defendants.
2. To recover data : In the event of software failure or hardware failure.
3. To analyze : computer system must be analyze after a break-in.
4. To gather evidence against an employee that an organization wish to terminate

- Forensics techniques for finding, preserving and preparing evidence.
- Finding evidence is a complex process as the forensic expert has to determine where the evidence resides. Evidence may be in files, evidence may be in disks, evidence may be on paper. Need to track all types of evidence.
- Preserving evidence includes ensuring that the evidence is not tampered with proof. It involves pre-incident planning and training in incident discovery procedures' If the machine is turned on, leave it on; do not run programs on that particular computer. Preparing evidence will include data recovery, documentation, etc.
- When files are deleted, usually they can be recovered. The files are marked as deleted, but they are still residing in the disk until they are overwritten. Files may also be hidden in different parts of the disk. The challenge is to piece the different part of the file together to recover the original file

1.5 Incident and Incident Response Methodology AU : Dec.-16, 17

- An **incident** is an unexpected event occurring when an attack, whether natural or human-made, affects information resources and/or assets, causing actual damage or disruption to a business's assets.
- Incident response is a set of procedures that commence when an incident is detected.
- Some common types of computer incidents include the following :
  1. Employee misuse of systems (for example, violations of Internet use policies)
  2. Malicious code (for example, viruses, worms, or Trojan horse programs)
  3. Intrusions or hacking
  4. Unauthorized electronic monitoring (sniffers, keyloggers, and so on)
  5. Web site defacement or vandalism
  6. Unauthorized access to confidential information
  7. Automated scanning tools and probes
  8. Insider sabotage (via espionage or disgruntled employees)
- When a threat becomes a valid attack, it is classified as an information security incident if :
  a. It is directed against information assets
  b. It has a realistic chance of success
  c. It threatens the confidentiality, integrity, or availability of information assets
- It is important to understand that IR is a reactive measure, not a preventative one. Incident response planning (IRP) focuses on immediate response.
- IT security incidents have three faces
  a. Data : An attempted or successful unauthorized access, use, disclosure, modification, or destruction of information
  b. Resources : It interference with IT operation
  c. People : violation of explicit or implied policy
- Impact is not all incidents are equal. Cyber security incidents are associated with malicious attacks or Advanced Persistent Threats
- Computer security incident as any unlawful, unauthorized, or unacceptable action that involves a computer system or a computer network. Such an action can include any of the following events :
  1. Theft of trade secrets
  2. Email spam or harassment
  3. Unauthorized or unlawful intrusions into computing systems
  4. Embezzlement
  5. Possession or dissemination of child pornography
  6. Denial-of-service attacks
  7. Extortion

8. Any unlawful action when the evidence of such action may be stored on computer media such as fraud, threats, and traditional crimes.

- Responding to computer security incidents can involve intense pressure, time, and resource constraints. Incident response helps personnel to minimize loss or theft of information and disruption of services caused by incidents.

➥ 1.5.1 Goals of Incident Response

- In incident response methodology, it emphasized the goals of corporate security professionals with legitimate business concerns, but it also take into the concerns of law enforcement officials.
  1. Confirms or dispels whether an incident occurred.
  2. Establishes controls for proper retrieval and handling of evidence.
  3. Minimizes disruption to business and network operations.
  4. Provides accurate reports and useful recommendation.
  5. Provides rapid detection and containment.
  6. Education senior management.
- Incident response is a multifaceted discipline. It demands a myriad of capabilities that usually require resources from several different operational units of an organization.
- Computer Security Incident Response Team (CSIRT), to respond to any computer security incident.
- A significant incident meets one or more of the following criteria :
  1. The incident has impacts the confidentiality, integrity, or availability of a critical system or sensitive data.
  2. There is a high probability of public disclosure of the incident and consequent embarrassment of the company.
- The impact of the incident results in company users losing access to a critical service (for example, email, network access, Internet access).
- An **Incident Response Plan (IRP)** is a detailed set of processes that anticipate, detect, and mitigate the effects of an unexpected event that might compromise information resources and assets.
- Then, the set of procedures, policies, and guidelines that commence at the detection of an incident is the **Incident Response (IR)**.
- A Computer Security Incident is an adverse event that negatively impacts the confidentiality, integrity and availability of information that is processed, stored and transmitted using a computer. Although they may not always be readily apparent, a computer incident has the following characteristics :
  a. The attacker or attack origin;
  b. The tool used;
  c. The vulnerability exploited;

d. The actions performed;

e. The intended target;

f. The unauthorized result

- After incident, the procedures for handling an incident are drafted, planners develop and document the procedures that must be performed immediately after the incident has ceased. Separate functional areas may develop different procedures.
- Once an actual incident has been confirmed and properly classified, the IR team moves from detection phase to reaction phase. In the incident response phase, a number of action steps taken by the IR team and others must occur quickly and may occur concurrently. These steps include notification of key personnel, the assignment of tasks, and documentation of the incident. As soon as incident is declared, the right people must be immediately notified in the right order.
- When incident violates civil or criminal law, it is organization's responsibility to notify proper authorities

➤ Incident Detection

- It is the responsibility of the IR team to determine if an incident is a valid incident or is just the product of “normal” system use.
- Incident candidates can be detected and tracked by end-users through several means; intrusion detection systems (IDS), host- and network-based virus detection software, and systems administrators.
- It is essential end-users, help desk staff, and all security personnel are properly trained in incident reporting, so in the event of an actual incident the IR team is properly notified and can effectively execute IRP procedures.
- Overloaded networks, computers, or servers, misbehaving computers systems or software packages may be hard to distinguish from an actual incident. Therefore, managers must insure IT professionals receive training to detect possible, probable, and definite indicators.

➥ 1.5.2 Components of Incident Response

1. Pre-incident preparation
2. Detection of incidents
3. Initial response
4. Formulate response strategy
5. Investigate the incident
6. Reporting
7. Resolution

- Pre-incident preparation : Take actions to prepare the organization and the CSIRT before an incident occurs.
- Detection of incidents : Identify a potential computer security incident.

- Initial response : Perform an initial investigation, recording the basic details surrounding the incident, assembling the incident response team, and notifying the individuals who need to know about the incident.
- Formulate response strategy : Based on the results of all the known facts, determine the best response and obtain management approval. Determine what civil, criminal, administrative, or other actions are appropriate to take, based on the conclusions drawn from the investigation.
- Investigate the incident : Perform a thorough collection of data. Review the data collected to determine what happened, when it happened, who did it, and how it can be prevented in the future.
- Reporting : Accurately report information about the investigation in a manner useful to decision makers.
- Resolution : Employ security measures and procedural changes, record lessons learned, and develop long-term fixes for any problems identified.

➡ 1.5.3 Forensic Duplication and Investigation

- Forensic analysis includes reviewing all the data collected. This includes reviewing log files, system configuration files, trust relationships, web browser history files, email mesages and their attachments, installed applications, and graphic files.
- You perform soft-ware analysis, review time/date stamps, perform keyword searches and take any other necessary investigative steps.
- Forensic analysis also includes performing more low-level tasks, such as looking through information that has been logically deleted from the sys-tem to determine if deleted files, slack space, or free space contain data fragments or en-tire files that may be useful to the investigation.
- Fig. 1.5.1 shows forensic analysis.
- Investigative process of digital forensics can be divided into several stages. Four major stages are : preservation, collection, examination and analysis.
- Computer forensics activities commonly include :
  a. the secure collection of computer data
  b. the identification of suspect data
  c. the examination of suspect data to determine details such as origin and content
  d. the presentation of computer-based information to courts of law
  e. the application of a country's laws to computer practice.
- Digital evidence can be useful in a wide range of criminal investigations including homicides, sex offenses, missing persons, child abuse, drug dealing, fraud, and theft of personal information. Digital information is all information in digital form and can be divided into the content itself.

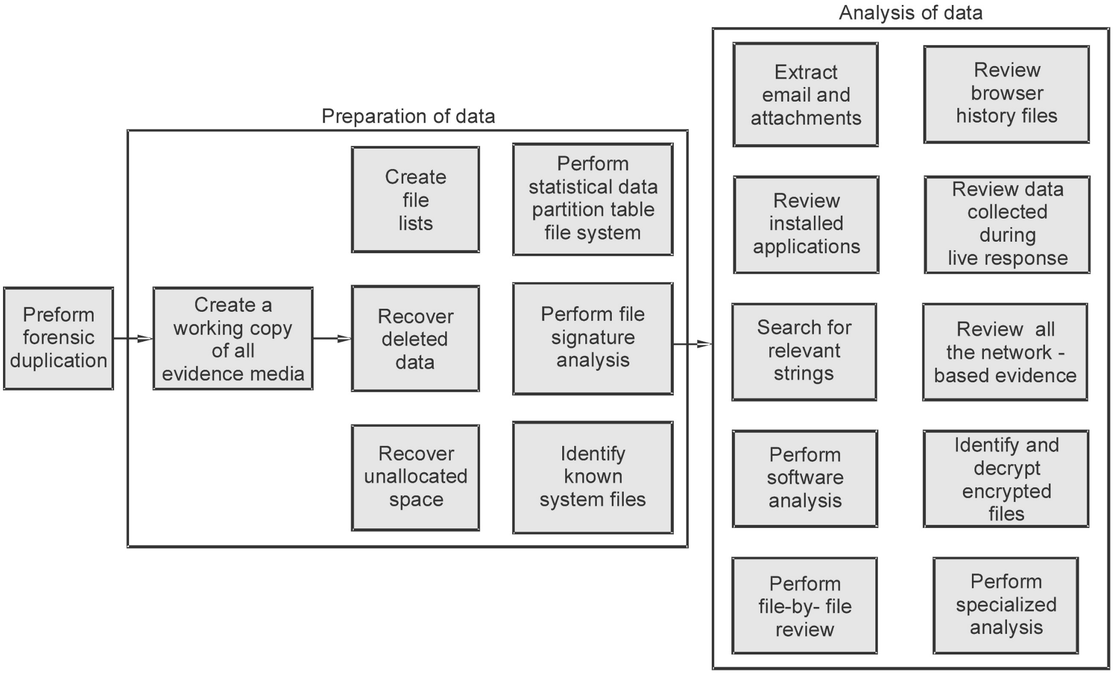

Preform forensic duplication
Preparation of data
Create a working copy of all evidence media
Create file lists
Perform statistical data partition table file system
Recover deleted data
Perform file signature analysis
Recover unallocated space
Identify known system files
Analysis of data
Extract email and attachments
Review browser history files
Review installed applications
Review data collected during live response
Search for relevant strings
Review all the network - based evidence
Perform software analysis
Identify and decrypt encrypted files
Perform file-by- file review
Perform specialized analysis

Fig. 1.5.1 : Forensics analysis

- Hard copy print outs of digital information are not digital evidence in the strict sense of this definition; it is considered a starting point for applying digital evidence gathering in the future.
- Forensics is the application of investigative and analytical techniques that conform to evidentiary standards used in or appropriate for a court of law or other legal context.
- There are three basic and essential principles in digital forensics :
  1. the evidence is acquired without altering it;
  2. demonstrably so;
  3. Analysis is conducted in an accountable and repeatable way.
- Digital forensic processes, hardware and software have been designed to ensure compliance with these requirements. The process of digital forensics is typically as follows :
  1. Preservation of the state of the device
  2. Survey and analysis of the data for evidence
  3. Event reconstruction
- Following are the principles must be followed when a person conducts the Computer Forensic Investigation.
  1. Data stored in a computer or storage media must not be altered or changed, as those data may be later presented in the court.
  2. A person must be competent enough in handling the original data held on a computer or storage media if it is necessary.

3. An audit trail or other documentation of all processes applied to computer-based electronic evidence should be created and preserved.
4. A person who is responsible for the investigation must have overall responsibility for accounting that the law.

- The scopes of the forensic investigations are as follows :
  1. To identify the malicious activities
  2. To identify the security lapse in their network.
  3. To find out the impact if the network system was compromised.
  4. To identify the legal procedures, if needed.
  5. To provide the remedial action in order to harden the system.

➥ 1.5.4 Stages of Investigative Process of Digital Forensics

1. Preservation : Preservation stage corresponds to freezing the crime scene. It involves operations such as preventing people from using computers during collection, stopping ongoing deletion processes, and choosing the safest way to collect information.
2. Collection : Collection stage consists in finding and collecting digital information that may be relevant to the investigation. Collection of digital information means collection of the equipment containing the information, or recording the information on some medium.
3. Examination : It is search of digital evidence. The output of examination is data objects found in the collected information which includes log and data files containing specific phrases, times-tamps etc.
4. Analysis : The aim of analysis is to draw conclusions based on evidence found.

➤ Computer Language :

- Software that may be used for gathering and analyzing digital information are as follows :
  1. Boot Software : Computer is booted by using boot software for imaging and / or analysis without making changes to the hard disk.
  2. Computer Forensic Software : This type of software is used for imaging and analyzing digital information.
  3. Forensic software write blockers are used to allow acquisition of digital information on a hard drive without changing and altering the contents.
  4. Hash Authentication Software is used to validate that a copy of digital information is identical to the original information
  5. Analysis Software helps for analyzing digital information.
  6. Bit stream imaging software is used to create an image of all areas of a data carrier. A bit stream image is an exact replica of each bit contained in the data carrier.

➤ Network Language :

- It is essential that computer investigators understand the language behind the technology.

1. TCP/IP (Transmission Control Protocol/Internet Protocol) : It is connection oriented protocol. TCP is a method of communication between programs which enables a bit-stream transfer of information.
2. IMAP (Internet Message Access Protocol) : Your can access mail using IMAP. IMAP does not copy e-mail to the user's personal machine because the user may have several. An IMAP client connects to a server by using TCP. IMAP supports the following modes for accessing e-mail messages : Offline, Online and Disconnected mode

➤ **Offline mode :** A client periodically connects to the server to download e-mail messages. After downloading, messages are deleted from the server. POP3 support this mode.

➤ **Online mode :** Client process e-mail messages on the server. The e-mail messages are stored on the server itself but are processed by an application on the client's end.

➤ **Disconnected mode :** In this mode, both offline and online modes are supported.

3. Post Office Protocol 3 (POP3) is used to transfer e-mail messages from a mail server to mail client software. POP3 begins when the user agent opens a TCP connection to the mail server on port 110. After TCP connection established, POP3 progresses three phases : Authorization, Transaction and Update. In authorization phase, user agent sends a user name and a password to authenticate the user downloading the mail. In transaction phase, the user agent retrieves messages. In this phase, user agent can also mark messages for deletion, remove deletion marks. In update phase, it occurs after the client has issued the quit command, ending the POP3 session. POP3 has two modes: Delete mode and the keep mode. In the delete mode, mail is deleted from the mailbox after each retrieval. In the keep mode, the mail remains in the mailbox after retrieval.
4. Routers are defined as special-purpose computers or software packages that handle the connection between two or more networks. Routers spend all their time looking at the destination addresses of the packets passing through them and deciding which route to send them on

- Internet crime is defined as any illegal activity involving one or more components of the Internet, such as websites, chat rooms and e-mail Internet crime involves the use of the Internet to communicate false or fraudulent representations to consumers.
- To track an e-mail message back to the sender you simply retrace the route that the e-mail travelled by reading through the e-mail's received headers. Killers, online sex offenders, cyber stalkers, computer intruders and fraudsters use the Internet as an instrument to commit their crimes.
- When the Internet plays a less active role in a crime, it is more useful to categorize it as “information as evidence.” For example, digital evidence on the Internet can simply indicate that a crime has occurred and provide investigative leads.
- To locate offenders and missing persons, Internet play very important role.
- Identity theft is one of the fastest growing crimes in the world. Identity theft occurs when enough information about an individual is obtained to open a credit card account in their name and charge items to that account. Examples of information needed are name, address, social security number and other personal information.

- Law enforcement officers use online anonymity when investigating questionable or illegal websites, to conduct online undercover operations and receive anonymous tips from informers about criminals or terrorists. In these situations, the law enforcement authorities and their contacts should have online anonymity for successful completion of investigation. If the suspects become aware of their being tracked, that could hamper the investigations.
- Military communications require maximum security. Today's Internet hackers are so smart that they are sometimes even able to crack or decipher encrypted communications.

University Questions

1. Briefly describe forensic investigation. **AU : Dec.-16, Marks 8**
2. Analyse briefly about the forensic duplication and investigation. **AU : Dec.-17, Marks 16**

1.6 Preparation for IR : Creating Response Tool Kit and IR Team

AU : May-17,18

- In a large business or organization the delegation of tasks is essential to maintaining effective operations. When looking at the makeup of an Incident Response Plan (IRP), a company's assumes responsibility for the creation of it.
- With the aid of other managers and systems administrators on the contingency planning (CP) team, the company should select members from each community of interest to form an independent IR team, which executes the IRP.
- The CP team creates three sets of incident-handling procedures :
  1. **During the incident :** The planners develop and document the procedures that must be performed during the incident.
  2. **After the incident :** Once the procedures for handling an incident are drafted, the planners develop and document the procedures that must be performed immediately after the incident has ceased.
  3. **Before the incident :** The planners draft a third set of procedures which are tasks that must be performed to prepare for the incident.
- Once an actual incident has been confirmed and properly classified, the IR team needs to be directed to move from the detection phase to the reaction phase.
- An IR is designed to first stop the incident (if still continuing), mitigate its effects, and provide information for the recovery from the incident.
- Three key steps include :
  1. Notification of key personnel
  2. Documentation of an Incident
  3. Incident containment strategies

➤ Incident Recovery :

- The recovery process includes the following steps :
  1. Identify and resolve vulnerabilities that allowed the incident to occur and spread.
  2. Address the safeguards that failed to stop or limit the incident - install, replace, or upgrade them.

3. Evaluate monitoring capabilities - improve detection and reporting methods, or install new monitoring capabilities
4. Restore systems backups

➥ 1.6.1 Incident Response Team

- The Incident response team is established to provide a quick, effective and orderly response to computer related incidents such as virus infections, hacker attempts and break-ins, improper disclosure of confidential information to others, system service interruptions, breach of personal information, and other events with serious information security implications.
- Team provides services and support, to a defined consistency, for preventing, handling and responding to computer security incidents.
- Every organization should have an incident response team. This team may consist of one person in an organization or several persons. In the event of suspected computer crime or violations of user policies, the team should be activated.
- The team should have written procedures for incident response, including what conditions warrant calling in local and/or federal law enforcement authorities. Violations of user policies may result in administrative actions whereas suspected computer crimes may require that law enforcement authorities be called in.
- Incident response team members are as follows :
- Each of the following members will have a primary role in incident response.
  1. Information Technology Director
  2. Information Technology Assistant Director
  3. Vice President Finance and Administration
  4. Qualified Member of Information Technology
  5. Network Engineer
  6. Security Analyst
- **Name and responsibility of the team member will change according to organization.**
- Following set of services provided by team :

Services	Alters
Reactive service	1. Alerts ad warning 2. Incident handling 3. Vulnerability handling
Proactive service	1. Announcements
Security quality management service	1. Security Consulting 2. Awareness building

➥ 1.6.2 Types of Incidents

- There are many types of computer incidents that may require IR team activation. Some examples include :

1. Breach of Personal Information
2. Denial of Service / Distributed Denial of Service
3. Excessive Port Scans
4. Firewall Breach
5. Virus Outbreak

- A security breach is defined as unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by organization.
- Forensic Software Tools are used for

  1. Data imaging
  2. Data recovery
  3. Data integrity
  4. Data extraction
  5. Forensic analysis
  6. Monitoring

1.6.3 Understanding Computer Investigation

- **Investigation :** is a process that develops and tests hypotheses to answer questions about events that occurred. In general, computer forensics investigates data that can be retrieved from a computer's hard disk or other storage media.
- Computer forensics is also different from data recovery, which involves recovering information from a computer that was deleted by mistake or lost during a power surge or server crash, for example. In data recovery, typically you know what you're looking for.
- Computer forensics is the task of recovering data that users have hidden or deleted, with the goal of ensuring that the recovered data is valid so that it can be used as evidence.
- The computer investigations group manages investigations and conducts forensic analysis of systems suspected of containing evidence related to an incident or a crime. For complex casework, the computer investigations group draws on resources from those involved in vulnerability assessment, risk management, and network intrusion detection and incident response. This group resolves or terminates all case investigations.
- **Digital Forensic Investigation :** A process that uses science and technology to examine digital objects and that develops and tests theories, which can be entered into a court of law, to answer questions about events that occurred.
- IT Forensic Techniques are used to capture and analyze electronic data and develop theories.

  Following steps are applied to the network to investigate the proof.

  1. Preparation and authorization
  2. Identification
  3. Documentation, collection and preservation
  4. Filtering and data reduction
  5. Class/Individual characteristics and evaluation of source
  6. Evidence recovery
  7. Investigative reconstruction
  8. Reporting result

➤ Digital Evidence on the Internet

- Internet crime is defined as any illegal activity involving one or more components of the Internet, such as websites, chat rooms and e-mail. Internet crime involves the use of the Internet to communicate false or fraudulent representations to consumers.
- To track an e-mail message back to the sender you simply retrace the route that the e-mail travelled by reading through the e-mail's received headers. Killers, online sex offenders, cyber stalkers, computer intruders and fraudsters use the Internet as an instrument to commit their crimes.
- When the Internet plays a less active role in a crime, it is more useful to categorize it as "information as evidence." For example, digital evidence on the Internet can simply indicate that a crime has occurred and provide investigative leads.
- To locate offenders and missing persons, Internet play very important role.
- Identity theft is one of the fastest growing crimes in the world. Identity theft occurs when enough information about an individual is obtained to open a credit card account in their name and charge items to that account. Examples of information needed are name, address, social security number and other personal information.
- An investigative analyst can find information that is hidden from traditional search engines. Most investigations start online. The investigator first gathers as much information as possible from Internet searches and databases because it's cheap, easy and can be done quickly.
- Like any piece of traditional evidence, Internet information too must be relevant, authentic and admissible. Most of the current case law surrounding Internet information gleaned from social media sites and other web pages is focused on the issue of authenticity.
- Digital evidence must follows the following rules of evidence :
  1. Admissible : it must conform to certain legal rules before it can be put before a court.
  2. Authentic : it must be possible to positively tie evidentiary material to the incident.
  3. Complete : it must tell the whole story.
  4. Reliable : there must be nothing about how the evidence was collected and subsequently handled that casts about its authenticity.

➥ 1.6.4 Digital Forensic Principles

1. When dealing with digital evidence, all of the general forensic and procedural principles must be applied.
2. Upon seizing digital evidence, actions taken should not change that evidence.
3. When it is necessary for a person to access original digital evidence, that person should be trained for the purpose that person should be trained for the purpose.
4. All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.

5. An Individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.
6. Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

➥ 1.6.5 Difference between Direct Evidence and Indirect Evidence

- Evidence comes in many forms, such as eyewitnesses, participants, prior statements by the defendant, documents, physical evidence, and scientific evidence, like fingerprints or DNA. No matter the form, there are two basic kinds of evidence that may be admitted in court - direct evidence and circumstantial evidence.
- Direct evidence does not require any reasoning or inference to arrive at the conclusion to be drawn from the evidence. Circumstantial evidence, also called indirect evidence, requires that an inference be made between the evidence and the conclusion to be drawn from it.
- A common example used to illustrate the difference between direct and circumstantial evidence is the determination of whether it rained. On the one hand, if a person testified that he or she looked outside a window and saw rain falling, that is direct evidence that it rained. If, on the other hand, a witness testified that he or she heard distant pitter patter, and later walked outside and saw that the ground was wet, smelled freshness in the air and felt that the air was moist, those sensations would be circumstantial evidence that it had rained.
- Circumstantial evidence is often discussed as if it carries less weight than direct evidence. Under the law - and in life - that is not necessarily true. The example above demonstrates that both direct and circumstantial evidence may be equally reliable. In both scenarios, there would be strong proof of rain. Any piece of evidence, whether direct or circumstantial, must be evaluated in terms of whether the source of the evidence is reliable.
- Major challenges to investigation are violent crimes. In such cases information is key in determining and then understanding the victim-offender relationships and to developing ongoing investigative strategy.
- More violent offenders and their victims are using computers and networks, therefore digital evidence are to be fully exploited.
- For any investigation the key is information about the circumstances. The information obtained has value only when it is properly recognized and collected.
- The information is usually stored in digital form such as cell phones, laptops and Tabs. In this case, the most informative and objective witnesses in violent crime investigations are computers and networks.
- Digital investigators use information from various digital evidences to :
  - Identify probable suspects,
  - Uncover previously unknown crimes,
  - Develop leads,
  - Cuild a more complete timeline

- o Reconstruction of events,
- o Check the accuracy of witness statements and offender statements.

➥ 1.6.6 Case Study of Computer Investigations

- Role of computer forensics professional is to collect evidence from a suspect's desktop and determine whether the suspect committed a crime or despoiled a company policy.
- If the evidence shows that crime or company policy violation happens then case is prepared against suspect. It contains collection of all evidence and investigator shows to the court or at a corporate inquiry.
- **Chain of custody :** Route the evidence takes from the time you find it until the case is closed or goes to court

➤ Taking a Systematic Approach

- Steps for problem solving
  1. Make an initial assessment about the type of case you are investigating
  2. Determine a preliminary design or approach to the case
  3. Prepare detailed checklist
  4. Find out resources which require for investigation
  5. Obtain and copy an evidence disk drive
  6. Find the possible risks
  7. Try to minimize the risks
  8. Test the design
  9. Digital evidence is analysis and if possible recovers.
  10. Investigate the information which recover
  11. Prepare the case report
  12. Evaluation the case

➤ Assessing the Case

- Following factors are consider for case details

  1. Situation 2. Nature of the case 3. Specifics of the case

  4. Evidence type 5. Operating system 6. Known disk format

  7. Evidence location

- **Guides for securing digital evidence at the scene.**
  1. Photograph all items before they are moved or disconnected.
  2. Disconnect the power supply and the modem connection. Secure the computer as evidence
     - i. If computer is “OFF”, do not turn “ON”.
     - ii. If computer is “ON”

- For Stand-alone computer
  1. Photograph screen, then disconnect all power sources; unplug from the wall AND the back of the computer.
  2. Place evidence tape over each drive slot.
  3. Photograph/diagram and label back of computer components with existing connections.
  4. If the screen is active, photograph the item that appears on the screen.
  5. Label all connectors/cable end to allow reassembly as needed.
  6. If transport is required, package components and transport/store components as fragile cargo.
  7. Keep away from magnets, radio transmitters and otherwise hostile environments.
  8. Do not do normal shut down procedures. Windows 95, 98x, NT, 2000, XP computers can be shut down by unplugging power plug from behind system.
- Networked or business computers
  1. Consult a computer specialist for further assistance
  2. If specialist is not available
- Seize all software and hardware manuals : These are often needed by the forensic technician for technical reference during the examination. Be sure to record their location in reference to the computer.
- Seize notes, scribbles, and notebooks : Notes may have references to software passwords and other computer accounts the suspect uses. Suspects who dial into other computers often use different passwords on the various systems they access. They have been known to keep notebooks listing the computer accounts they access and their login and passwords.

➡ 1.6.7 Method for Corporate High-Tech Investigations

- Develop formal procedures and informal checklists. To cover all issues important to high-tech investigations
- **Employee termination cases :** After investigation, employee is terminated because of abuse of corporate assets. Employee normally make mis-use of Internet and computer resources. It includes watching adult movies, sending personal email, chatting with friends, taking color printout, browsing Internet.
- **Internet abuse investigations :** To conduct an investigation for Internet abuse, following things are considered :
  1. Organization's Internet proxy server logs
  2. Suspect computer's IP address
  3. Suspect computer's disk drive
  4. Your preferred computer forensics analysis tool

- For Internet abuse investigations following steps are followed :
  a. Make use of standard forensic analysis techniques and tools.
  b. Use proper tools to pull out all Web page URL information
  c. Collect proxy server log from firewall administrator
  d. Compare the data recovered from forensic analysis to the proxy server log
  e. Continue analyzing the computer's disk drive data

➤ Attorney-Client Privilege Investigations

- The attorney-client privilege protects the functioning of the attorney and client relationship and, in essence, requires an attorney; a client; a relationship between the attorney and the client for the purpose of rendering and receiving legal advice; and a communication between the attorney and the client; and the intent that the communication be confidential.
- The attorney-client privilege allows a client to seek and receive legal advice from an attorney in confidence. The purpose is to promote adherence to the law, by encouraging a client to seek legal advice in the first instance and by fostering full and frank discussions in the course of the attorney-client relationship.
- First, internal investigations are necessary to ensure a company's compliance with laws and regulations.
- The attorney-client privilege, in turn, is critical to the integrity of internal investigations. Companies simply cannot conduct prompt, efficient and accurate investigations without this protection.
- Privilege creates a zone of confidentiality in which a company's in-house lawyers and outside counsel can fully assess the facts, reach accurate conclusions about potential wrongdoing, and make informed decisions about disclosures to regulators, law enforcement authorities and shareholders.
- Steps for conducting an **Attorney-Client Privilege** case
  a. Request a memorandum from the attorney directing you to start the investigation
  b. Request a list of keywords of interest to the investigation
  c. Initiate the investigation and analysis
  d. For disk drive examinations, make two bit-stream images using different tools
  e. Compare hash signatures on all files on the original and re-created disks
  f. Methodically examine every portion of the disk drive and extract all data
  g. Run keyword searches on allocated and unallocated disk space
  h. For Windows OSs, use specialty tools to analyze and extract data from the Registry
  i. For binary data files such as CAD drawings, locate the correct software product
  j. For unallocated data recovery, use a tool that removes or replaces nonprintable data
  k. Consolidate all recovered data from the evidence bit-stream image into folders and subfolders

➤ Attorney-Client Privilege : Requirements

- Protects communications that are :
  a. between the corporation/client and the attorney
  b. when the attorney is acting as an attorney
  c. for the purpose of seeking legal advice, and
  d. in confidence
- The Attorney-Client privilege does not protect communications when the privilege is waived. Privilege is the client's to assert and invoke. The form of communication is irrelevant. Merely stamping "privileged" or "confidential" on a document does not alone establish privilege.
- The attorney work-product doctrine protects from disclosure confidential work product prepared by or for attorneys in anticipation of litigation.

University Questions

1. Discuss in detail the systematic approach in computer investigations and conducting an investigation in computer organizations. **AU : May-17, Marks 16**
2. Discuss the investigation of employee termination case, Internet abuse investigation, Attorney Client Privilege investigation in corporate high tech investigation. **AU : May-17, Marks 16**
3. Outline the problems and challenges forensic examiners face when preparing and processing investigations, including the ideas and questions they must consider. **AU : May-18, Marks 16**

1.7 Data Acquisition

AU : Dec.-17, May-18

- Forensic data acquisition is a process that involves the identification of a digital source, such as a hard disk, a memory card or any other form of media and data storage, and the copying of the identified data to some accessible destination object, such as an image file, a clone or a bit-stream duplicate, performed in a complete and accurate manner.
- Hence, completeness and accuracy are the two most important features that any data acquisition tool must demonstrate, in order for the tool to be considered of a forensic standard of quality.
- During data acquisition an exact (typically bitwise) copy of storage media is created. A dead acquisition copies the data without the assistance of the suspect's (operating) system. A live acquisition copies the data using the suspect's (operating) system.
- Live Data Acquisition : Real-time forensic acquisition from computers, servers, database and email server applications that can't be taken offline or leave your site. When time is of the essence, systems are constantly running or you have a limited time-frame to capture evidence from a suspect computer our live data acquisition meets your deadlines and ensures electronic evidence maintains evidentiary status by validating MD5 hash values.

➤ 1. Write Blockers

- Allow acquisition of data from a storage device without changing the drive's contents. Here write commands are blocked. Only read commands are allowed to pass the write blocker.
- **Types of blockers :** Hardware Write Blocker and Software Write Blocker
- **Hardware Write Blockers :** The device sits in between investigator's PC and storage device. It supported storage interfaces are ATA, SCSI, USB or SATA. The controller cannot write values to the command register, which writes or erases data on the storage device.
- **Software Write Blockers (SWB) :** A software layer that sits in between the OS and the device driver for the storage device. It prevents all disc requests that use system calls to write data to the storage device. The SWB should not modify a read-only disk. The SWB is designed to prevent any operations on data storage media that are not write protected.
- Data acquisition methods are as follows :
  1. Disk-to-image file
  2. Disk-to-disk copy
  3. Logical disk-to-disk or disk-to-data file
  4. Sparse data copy

Data acquisition methods	Remarks
Disk-to-image file	• Most common method • Can make more than one copy • Copies are bit-for-bit replications of the original drive • ProDiscover, EnCase, FTK, SMART, Sleuth Kit, X-Ways, iLook
Bit-stream disk-to-disk	• When disk-to-image copy is not possible • Consider disk’s geometry configuration • EnCase, SafeBack, SnapCopy
Logical disk-to-disk or disk-to-data file	• When your time is limited • Logical acquisition captures only specific files of interest to the case
Sparse data copy	• Sparse acquisition also collects fragments of unallocated (deleted) data • For large disks • PST or OST mail files, RAID servers

- You can remotely connect to a suspect computer via a network connection and copy data from it

- Remote acquisition tools vary in configurations and capabilities
- Drawbacks
  a. LAN's data transfer speeds and routing table conflicts could cause problems
  b. Gaining the permissions needed to access more secure subnets
  c. Heavy traffic could cause delays and errors
  d. Remote access tool could be blocked by antivirus
- With ProDiscover Investigator you can :
  a. Preview a suspect's drive remotely while it's in use
  b. Perform a live acquisition
  c. Encrypt the connection
  d. Copy the suspect computer's RAM
  e. Use the optional stealth mode
- ProDiscover Incident Response additional functions
  a. Capture volatile system state information
  b. Analyze current running processes
  c. Locate unseen files and processes
  d. Remotely view and listen to IP ports
  e. Run hash comparisons
  f. Create a hash inventory of all files remotely
- PDServer remote agent
  a. ProDiscover utility for remote access
  b. Needs to be loaded on the suspect
- PDServer installation modes
  a. Trusted CD
  b. Preinstallation
  c. Pushing out and running remotely
- PDServer can run in a stealth mode and it can change process name to appear as OS function

➥ 1.7.1 Acquiring Data with a Linux Boot CD

- A bootable Linux CD is a complete Linux operating system that can boot from an optical disc, USB stick or Preboot eXecution Environment (PXE).
- It runs in the computer's memory and allows an operating system to run without installing or making changes to the computer's original configuration and files.
- There are many live image of known Linux distributions. Well-known live images are KNOPPIX and Ubuntu which can be used for various purposes.

- Live images can be adjusted to run special (start-up) scripts and contain special drivers and software. The process of adjusting the contents of a live image is called re-mastering.
- Linux can read hard drives that are mounted as read-only. Windows OSs and newer Linux automatically mount and access a drive
- Windows will write to the Recycle Bin, and sometimes to the NTFS Journal, just from booting up with a hard drive connected
- Linux kernel 2.6 and later write metadata to the drive, such as mount point configurations for an ext2 or ext3 drive. All these changes corrupt the evidence
- Forensic Linux Live CDs mount all drives read-only, which eliminates the need for a write-blocker.
- Forensic Linux Live CDs contain additional utilities.
- It is configured not to mount, or to mount as read-only, any connected storage media. Well-designed Linux Live CDs is used for computer forensics.
- Preparing a target drive for acquisition in Linux, the modern linux distributions can use Microsoft FAT and NTFS partitions.
- Use of **fdisk** command lists, creates, deletes, and verifies partitions in Linux. The **mkfs.msdos** command formats a FAT file system from Linux.
- Acquiring data with dd (“data dump”) command in Linux, can read and write from media device and data file. It creates raw format file that most computer forensics analysis tools can read.
- The dd command requires more advanced skills than average user and does not compress data. The dd command combined with the split command and segments output into separate volumes
- The dd command is intended as a data management tool and is not designed for forensics acquisitions.
- The “dcfldd” additional functions specify HEX patterns or text for clearing disk space. It log errors to an output file for analysis and review.
- It uses several hashing options. Referring to a status display indicating the progress of the acquisition in bytes.
- Split data acquisitions into segmented volumes with numeric extensions and verify acquired data with original disk or media data.
- Although live images run almost fully in the computer's memory, running an operating system from an optical disc is slower than running from a flash or hard disk drive.
- A live image provides the digital forensic investigator a working environment that doesn't change the computer's original configuration and files, especially when the live image doesn't mount the storage devices automatically.
- Thus, forensic images of storage devices can be made without disassembling the computer.
- An attack has taken place. You, the investigator have just arrived on the scene. It is expected that the attacker uses encrypted disk volumes.

- In any case, the machine contains memory-resident information that will be lost after a power cycle. Fig. 1.7.1 shows live analysis scenario.

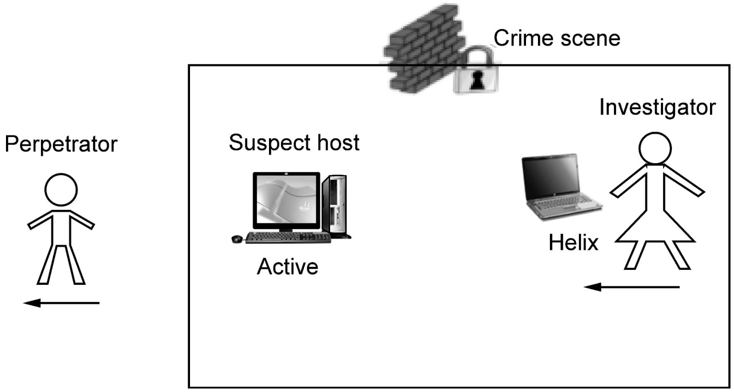


Fig. 1.7.1 : Live analysis scenario

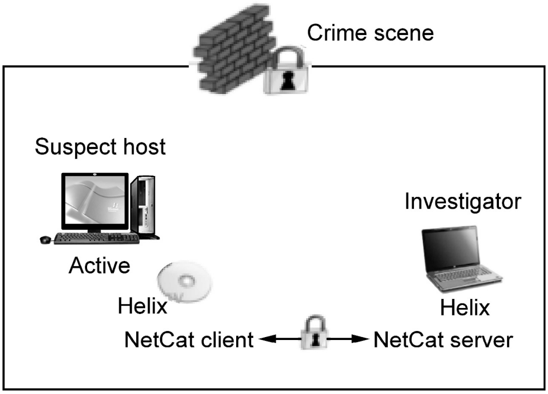


Fig. 1.7.2

- Set up the scene for data acquisition

  Suspect host (Linux) :

  1. Load Helix CD-ROM into drive.
  2. Ensure that your tools do NOT modify the disk.
  3. Use IP addresses instead of hostnames.
  4. Used trusted CD-ROM binaries only.
  5. Send acquired data over encrypted network.

University Questions

1. Demonstrate how to use remote network aquisition tools in cyber forensics. **AU : Dec.-17, Marks 16**
2. Explain the process of acquiring data with a Linux Boot CD. **AU : May-18, Marks 16**

1.8 University Questions Case Study

Q. 1 A patient with a heart ailment was transported to a hospital where an angiogram was performed. The patient later had a stint inserted into an artery, along with a second angiogram, but died shortly thereafter. A third angiogram was performed immediately after the patient's death. Images of the angiogram procedures were purportedly stored on computer hard drives. The day following the patient's death, hospital staff were able to locate images for the first and third angiograms but could not find any images of the second procedure. The hospital and doctor were sued for medical malpractice and wrongful death. The plaintiffs also claimed the defendants had deliberately deleted the images of the second angiogram that allegedly proved the wrongful death claim. A CFS team (CFST) was engaged by the doctor's insurance company to locate images of the second angiogram on the computer hard drive. Explain the possible actions that the CFST took to locate the images. **AU : May-19, Marks 15**

Ans. : This case study is related to Discovery of Electronic Evidence**.**

- No evidence could be found that the secondangiogram images had ever been stored on thecomputers, or that the images had beendeleted. Through inquiries of hospital staff, theCFST learned that the system was prone toproblems and periodically "crashed."
- TheCFST requested that the hospital perform a testcase on the system, and it was observed that thesystem malfunctioned; in the test case, no images were recorded.
- At the same time, the hospital replaced this system with a new system becauseof the periodic crashes that occurred.
- A CFSTexaminer testified at the court trial that systemcrashes may have caused the images to not bestored on the computer hard drives and that team had personally observed the system crashing.
- The plaintiff 's attorneys countered that themanufacturer examined the system the dayafter the patient's death and could not find anyproblems.
- The CFST's examiner counteredthat the system had been replaced by the hospital because of system malfunctions. Team furtherexplained that because the system was functioning normally on the day the manufacturerexamined the system, did not mean that it wasfunctioning on the day of the second angiogram procedure.
- The best outcome that theinsurance company expected was eliminationof any penalties for deliberate deletion of theimages. Court ruled that no monetary damages would have to be paid to the plaintiffs.

Q. 2 A parent was concerned that her son was accessing unwanted Web sites from his computer. Each time the computer was checked by a technician, no evidence was found. How would a CFS go about investigating this incident? **AU : Dec.-19, Marks 15**

Ans. :

- A computer forensics team was contracted to assist in an investigation for computer that suspected her son using PC. The team visited the site and, using correct forensic procedures, created an image of the hard drive of the suspect PC. The team was then able to recover a large amount of inappropriate material from the PC in a forensically sound manner, including files that had been deleted, renamed, and hidden in an attempt to disguise their true nature. **Also refer section 1.6.6.**

1.9 Questions with Answers

1.9.1 Two Marks Questions with Answers

Q. 1 What is software write blockers ?

Ans. : A software layer that sits in between the OS and the device driver for the storage device. It prevents all disc requests that use system calls to write data to the storage device.

Q. 2 List the data acquisition methods.

Ans. : Data acquisition methods are as follows :

a. Disk-to-image file

b. Disk-to-disk copy

c. Logical disk-to-disk or disk-to-data file

d. Sparse data copy

Q. 3 What do you mean forensic data acquisition ?

Ans. : Forensic data acquisition is a process that involves the identification of a digital source, such as a hard disk, a memory card or any other form of media and data storage, and the copying of the identified data to some accessible destination object, such as an image file, a clone or a bit-stream duplicate, performed in a complete and accurate manner.

Q. 4 What is difference between direct evidence and indirect evidence ?

Ans. : Direct evidence does not require any reasoning or inference to arrive at the conclusion to be drawn from the evidence. Circumstantial evidence, also called indirect evidence, requires that an inference be made between the evidence and the conclusion to be drawn from it.

Q. 5 List the rules of evidence for digital evidence.

Ans. : Digital evidence must follows the following rules of evidence :

a. Admissible : it must conform to certain legal rules before it can be put before a court.

b. Authentic : it must be possible to positively tie evidentiary material to the incident.

c. Complete : it must tell the whole story.

d. Reliable : there must be nothing about how the evidence was collected and subsequently handled that casts about its authenticity.

Q. 6 What is identity theft ?

Ans. : Identity theft is the crime of using someone else's personal information, such as an account number, driver's license, health insurance card or Social Security number, to commit fraud. ID Theft is a form of fraud. Identity thieves may use a variety of low and high-tech methods to gain access to your personally identifying information.

Q. 7 Define phishing.

Ans. : Phishing scams are spam emails sent by cybercriminals that pretend to be from a legitimate person or organization with the intent of tricking you into revealing personal information.

Q. 8 What is difference between computer forensics and digital forensics ?

Ans. : **Computer forensics** is the science of locating, extracting and analyzing types of data from difference devices, which specialists then interpret to serve as legal evidence.

Digital forensics is the scientific acquisition, analysis, and preservation of data contained in electronic media whose information can be used as evidence in a court of law.

Q. 9 What is incident response plan ?

Ans. : An Incident Response Plan (IRP) is a detailed set of processes that anticipate, detect, and mitigate the effects of an unexpected event that might compromise information resources and assets.

Q. 10 Define an incident.

Ans. : An **incident** is an unexpected event occurring when an attack, whether natural or human-made, affects information resources and/or assets, causing actual damage or disruption to a business's assets.

Q. 11 Define cyber forensics. **AU : CSE, Dec.-16**

Ans. : It is defined as the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation.

Q. 12 What is a forensic duplicate ? **AU : CSE, Dec-16**

Ans. : Forensic duplicate is a file that contains every bit of information from the source, in a raw bit stream format.

Q. 13 Brief on cyber crime. **AU : CSE, Dec.-16**

Ans. : When any crime is committed over the Internet it is referred to as a cyber crime. Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes).

Q. 14 Define 'Hacking'. **AU : May-17**

Ans. : Hacking refers to the practice of modifying or altering computer software and hardware to accomplish a goal that is considered to be outside of the creator's original objective.

Q. 15 Discuss RAID Data acquisition. **AU : May-17**

Ans. :

- Acquisitions of RAID drives can be challenging for computing forensics examiners because of how RAID systems are designed, configured, and sized. Size is the biggest problem.
- RAID was developed as a data-redundancy measure to minimize data loss caused by a disk failure. RAID implementation improves the I/O performance of storage systems by storing data across multiple hard disks.

Q. 16 List the tasks of a computer forensic examination protocol. **AU : Dec.-17**

Ans. : Tasks performed by computer forensics examination protocol are acquisition, validation and discrimination, extraction, reconstruction and reporting.

Q. 17 State the importance of phreaking. **AU : Dec.-17**

Ans. : When phone networks are hacked in order to make free calls or have calls charged to a different account. Phreakers use technology to gain unauthorized access to the telephone system.

Q. 18 Define identity fraud ? **AU : May-18**

Ans. : Identity fraud is the use by one person of another person's personal information, without authorization, to commit a crime or to deceive or defraud that other person or a third person. Most identity fraud is committed in the context of financial advantage, such as accessing a victim's credit card, bank or loan accounts.

Q. 19 What is e-mail abuse ? **AU : May-18**

Ans. : Email abuse is the unsolicited sending of spam, third party advertisements, derogatory language, slander, and threats via electronic mail.

Q. 20 List the benefits of computer forensics methodology. **AU : May-19**

Ans. :

1. Benefits is its ability to search and analyse a huge amount of data quickly and efficiently.
2. The ability to reduce or even eliminate sampling risk
3. The quick identification and extraction of certain risk criteria from the entire data population for further analysis

➡ 1.9.2 Multiple Choice Questions with Answers

Q. 1 The ability to recover and read deleted or damaged files from a criminal's computer is an example of a law enforcement specialty called ____________.

(a) simulation (b) computer forensics

(c) forecasting (d) data acquisition

Ans. : (b) computer forensics

Q. 2 Which of the following is comes under cybercrime ?

(a) Pornography (b) Online gambling

(c) Intellectual property crime (d) All of these

Ans. : (d) All of these

Q. 3 ____________ write blockers device sits in between investigators PC and storage device.

(a) Software (b) Hardware (c) Software and hardware (d) Code

Ans. : (b) Hardware

Q. 4 Many acquisition tools don't copy data in the ____________ of a disk drive.

(a) host protected area (b) memory protected area

(c) hardware protected area (d) write protected area

Ans. : (a) host protected area

Q. 5 When an attempt is to make a machine or network resource unavailable to its intended users, the attack is called ____________**.**

(a) denial-of-service attack (b) slow read attack

(c) spoofed attack (d) starvation attack

Ans. : (a) denial-of-service attack

Q. 6 The set of procedures, policies and guidelines that commence at the detection of an incident is the ____________**.**

(a) computer forensics (b) digital forensics

(c) incident response (d) investigation

Ans. : (c) Incident response

Q. 7 In investigative process of digital forensics, ____________ stage corresponds to freezing the crime scene.

(a) collection (b) preservation (c) examination (d) analysis

Ans. : (b) preservation

Q. 8 Which of the following is NOT data acquisition method ?

(a) Spare data copy (b) Disk to disk copy

(c) Acquisition (d) Bit stream disk to disk

Ans. : (c) Acquisition

Q. 9 The process of applying scientific methods to collect and analyse data and information that can be used as evidence is called as ___________.

(a) computer forensics (b) digital forensics

(c) data forensics (d) information forensics

Ans. : (a) Computer forensics

Q. 10 In __________ acquisition, the data acquisition method captures only specific files of interest to the case or specific types of files, such as Outlook PST files.

(a) live (b) sparse (c) logical (d) All of these

Ans. : (c) logical

Q. 11 In __________ acquisition, like logical acquisitions, this data acquisition method captures only specific files of interest to the case, but it also collects fragments of unallocated data.

(a) Live (b) sparse (c) logical (d) data and information

Ans. : (b) sparse

Q. 12 The most cost effective way to minimize the cost of fraud is:

(a) Prevention (b) Detection (c) Investigation (d) Prosecution

Ans. : (a) prevention

Q. 13 The aim of incident response is to identify an attack, contain the damage, and eradicate the root cause of the incident.

(a) identity theft (b) incident response

(c) cyber crime (d) all of these

Ans. : (b) incident response

Q. 14 Phishing is a form of __________.

(a) spamming (b) identity theft (c) impersonation (d) scanning

Ans. : (c) impersonation

Q. 15 What is the most significant legal issue in computer forensics ?

(a) Discovery evidence (b) Admissibility of evidence

(c) Seizing evidence (d) Preserving evidence

Ans. : (b) admissibility of evidence

Q. 16 Forensic software tools are used for __________.

(a) data imaging (b) data recovery

(c) data extraction (d) All of these

Ans. : (d) All of these

Q. 17 __________ means repeated acts of harassment or threatening behavior of the cyber-criminal towards the victim by using internet services.

(a) Pornography (b) Web hijacking (c) Hacking (d) Cyber stalking

Ans. : (d) Cyber stalking

Q. 18 Which of the following is a proper acquisition technique ?

(a) Disk to image (b) Disk to disk (c) Sparse acquisition (d) All of these

Ans. : (a) Disk to image

Q. 19 Which duplication method produces an exact replica of the original drive ?

(a) Bit-stream copy (b) Image copy (c) Mirror copy (d) Drive image

Ans. : (d) Drive image

Q. 20 A computer crime is __________.

(a) any activity in which the thief uses computer technology

(b) an illegal action in which the perpetrator uses special knowledge of computer technology

(c) an immoral action in which the thief uses special knowledge of computer technology without the other person knowing

(d) any threat to computer or data security

Ans. : (b) an illegal action in which the perpetrator uses special knowledge of computer technology

Q. 21 Theft can take many forms of hardware, software, data or computer time. White-collar computer crime involves the theft of __________**.**

(a) applications (b) spikes (c) data (d) property

Ans. : (c) data

Q. 22 People who gain unauthorized access to computers for the purpose of doing damage are called __________**.**

(a) employees (b) hackers (c) members of organized crime (d) crackers

Ans . : (d) crackers

Q. 23 Privacy is primarily a(n) __________ matter.

(a) ethical (b) legal (c) security (d) business

Ans. : (a) ethical

Q. 24 The issues that deal with the collection and use of data about individuals is

(a) access (b) property (c) accuracy (d) privacy

Ans. : (d) privacy

Q. 25 Why would a hacker use a proxy server ?

(a) To create a stronger connection with the target.

(b) To create a ghost server on the network.

(c) To obtain a remote access connection.

(d) To hide malicious activity on the network.

Ans. : (d) To hide malicious activity on the network

Q. 26 Which phase of hacking performs actual attack on a network or system?

(a) Reconnaissance (b) Maintaining access

(c) Scanning (d) Gaining access

Ans. : (d) Gaining access

Q. 27 What is the purpose of a Denial of Service attack ?

(a) Exploit a weakness in the TCP/IP stack

(b) To execute a Trojan on a system

(c) To overload a system so it is no longer operational

(d) To shutdown services by turning them off

Ans. : (c) To overload a system so it is no longer operational

Q. 28 Which of the following is considered as cyber crime ?

(a) Virus Attack (b) Worm Attack (c) Hacking (d) All of these

Ans. : (d) All of these

Q. 29 Phishing is a form of **__________.**

(a) Spamming (b) Identity theft (c) Impersonation (d) Scanning

Ans. : (c) Impersonation

Q. 30 Identity theft is the **__________.**

(a) impersonation by a thief of someone with a large bank account

(b) impersonation by a thief of someone with computer skills

(c) impersonation by a thief of someone with good credit

(d) impersonation by a thief of someone's identity for the purpose of economic gain

Ans. : (d) impersonation by a thief of someone's identity for the purpose of economic gain

❑❑❑

Notes

UNIT - II

2 Evidence Collection and Forensics Tools

Scope of the Syllabus

Processing Crime and Incident Scenes – Working with Windows and DOS Systems. Current Computer Forensics Tools: Software/ Hardware Tools.

2.1 Processing Crime and Incident Scenes

AU : Dec.-17

- Digital evidence can be any information stored or transmitted in digital form. Digital data is a tangible object. General tasks investigators perform when working with digital evidence :
  1. Identify digital information or artifacts that can be used as evidence
  2. Collect, preserve and document evidence
  3. Analyze, identify and organize evidence
  4. Rebuild evidence or repeat a situation to verify that the results can be reproduced reliably
- Collecting computers and processing a criminal or incident scene must be done systematically
- Crime scene refers to the location where a crime occurred or where evidence of a crime exists. For the purposes of this set of directives, crime scene will also refer to the scene of an incident that may not be criminal in nature, but where common crime scene methods are used to gather evidence.
- "Evidence" is any substance or material found or recovered in connection with a criminal investigation.
- "Evidence processing" refers to the specific actions taken at a crime scene or collision scene to identify, locate, document, preserve and collect evidence and/or known standards.
- "Software" refers to programs that have been or can be installed in a computer. "Storage media" refers to digital storage devices include, but may not be limited to, computer disks, flash cards, thumb drives and magnetic tape used to store computer data and/or images captured via a digital camera.

➤ Understanding Rules of Evidence

1. Consistent practices help verify your work and enhance your credibility.
2. Comply with your state's rules of evidence or with the federal rules of evidence.
3. Evidence admitted in a criminal case can be used in a civil suit and vice versa.
4. Keep current on the latest rulings and directives on collecting, processing, storing and admitting digital evidence.
5. Data you discover from a forensic examination falls under your state's rules of evidence.
6. Digital evidence is unlike other physical evidence because it can be changed more easily.
7. Most federal courts have interpreted computer records as hearsay evidence.

- Computer records are usually divided into :
  1. Computer-generated records
  2. Computer-stored records
- Computer and digitally stored records must be shown to be authentic and trustworthy. Computer-generated records are considered authentic if the program that created the output is functioning correctly. Collecting evidence according to the proper steps of evidence control helps ensure that the computer evidence is authentic.

➤ Authorization :

- Before gathering digital evidence relating to an investigation, computer security professionals should obtain instructions and written authorization from their attorneys.
- Usually the employer can search its employee's computers, e-mail and other data. For accessing personal and private data a search warrant is needed. In such case it may be permissible to seize the computer and secure it from alteration until the police arrive.
- A valid search warrant must describe particular property to be seized and probable cause for seizing it. Warrant should contain each item to be seized and the types of evidence that will be to prevent mistakes or misuse such as searching the wrong home or seizing items that are outside of the scope of the warrant.
- Digital investigators are authorized to collect and examine that is directly pertinent to the investigation.
- The following shall establish evidentiary-related guidelines and procedures used for collecting evidence in the field :
  1. The first officer to arrive at any incident scene shall be responsible for securing the area and preserving all observable evidence. Evidence technician work should not begin work until the entire area has been secured and declared safe.
  2. Evidence encountered at a scene shall be handled with care to preserve it for future processing. Discretion should be used when determining what evidence to process at the scene. Such decisions shall be based upon the seriousness of the offense, officer expertise and the processing materials available.

3. The progression of evidentiary-related tasks shall generally be as follows :
   a. Secure the scene;
   b. Photograph and/or videotape evidence;
   c. Develop potential evidence for latent prints;
   d. Sketch the scene;
   e. Label and collect evidence;
   f. Transport and appropriately store evidence;
   g. Analyze evidence.
4. Officers seizing evidence shall be responsible for notifying the property team of the need for laboratory examinations. Evidence technicians and/or other experts should be consulted when deemed appropriate.
5. Each item of evidence shall be inventoried using the department property documentation system. The system contains provisions for recording the following : Agency case number; offense; property invoice number; date seized; owner/suspect identifiers; current location; item descriptions; disposition recommendation; and chain of custody information. The property manager or designee should review property cards upon the submission of evidence. Improperly completed property cards may be returned to the officer completing the card. The officer's supervisor may also be notified.
6. As per the ACT, police officers are required to provide receipts to persons from whom they have seized items of evidence or contraband.

➤ Computer Equipment Seizure

- The following shall establish procedures for the seizure of computer equipment :
  1. Officers should exercise extreme caution when seizing and/or examining computer equipment so as not to cause severe damage or the loss of valuable data.
  2. Persons possessing specialized knowledge of computers and computer security should be consulted during the preparation and execution of search warrants when necessary.
  3. A person skilled in computer operation should be used to examine such equipment prior to startup.
  4. Whenever possible, a copy of the hard drive should be made before examination. The original should then be placed in secure storage and the copy used for examination purposes.
  5. When computer equipment is in operation at the time of seizure, the CPU should be disconnected from the power source. This procedure will ensure that all contents stored on the hard drive remain intact. However, data cached in memory will be lost when the computer is powered down.
  6. Strong consideration should be given to photographing and/or videotaping on-screen images before operating computer equipment is disconnected from the power source. This procedure will ensure that pertinent evidence will be captured when cached memory and/or embedded scripts are involved.

7. Non-operating computers, disks, drives and related peripherals should be considered fragile. Such equipment should be appropriately packaged, handled, and transported.
8. Special care must be taken to avoid exposing removable media to magnetic fields, static electricity and physical force.

- Forensic analysis function is sometimes broken into two parts :
  a. Examination
  b. Analysis
- Examination phase involves the use of forensic tools to recover deleted files and retrieve and characterize operating system artifacts and other relevant material. Analysis phase uses those materials to answer the questions that gave rise to the investigation. Analysis function is also responsible for reporting and presenting the investigation's findings.
- Public sector authorization may take the form of a search warrant; seizure of the relevant items containing the information
- Private sector authorization is specified by the organization's policy; many use affidavit; more common to authorize the collection of images of digital information.
- Private section includes private corporations and government agencies not involved with law enforcement. They must comply with state public disclosure and federal freedom of information act and make certain documents available as public records. Law enforcement is called if needed.
- Private organization wishing to search an employee's computer must generally meet the following conditions :
  1. Employee made aware of organizational policy that search may occur
  2. Search must be justified at its inception
  3. Search must be permissible in its scope
  4. Organization has clear ownership over container that material was discovered in
  5. Search must be authorized by the responsible manager or administrator
- Incident response policy must spell out the procedures for initiating investigative process. Particularly critical in private sector, as private organizations do not enjoy the broad immunity accorded to law enforcement investigations
- Digital evidence collection follows a four-step methodology :
  1. Identify sources of evidentiary material
  2. Authenticate the evidentiary material
  3. Collect the evidentiary material
  4. Maintain a documented chain of custody

➥ 2.1.1 Document Evidence

- **Documentary evidence** is any evidence that is, or can be, introduced at a trial in the form of documents, as distinguished from oral testimony. Documentary evidence is most widely understood to refer to writings on paper (such as an invoice, a contract or a will), but the term can also apply to any media by which information can be preserved, such as photographs; a medium that needs a mechanical device to be viewed, such as a tape recording or film; and a prined form of digital evidence, such as emails, spreadsheets, etc.
- Evidence contained in or on documents can be a form of real evidence. For example, a contract offered to prove the terms it contains is both documentary and real evidence. When a party offers a document into evidence, the party must authenticate it the same way as any other real evidence, either by a witness who can identify the document or by witnesses who can establish a chain of custody for the document.
- **Digital evidence** is useful in a wide range of criminal investigations such as homicides, sex offences, missing persons, cpersons, child abuse, fraud and theft.
- Digital evidence helps in tracing how a crime was committed, provide investigative leads, disapprove or support witness statements and identify likely suspects.
- Digital evidence is defined as information stored or transmitted in binary form that may be relied upon in court.
- For considering multiple sources of digital evidence, computer systems can be categorised in to three groups :
  1. Open Computer systems
  2. Communication systems
  3. Embedded computer systems.

➤ Ways to Challenge Documentary Evidence

- When people deal with documentary evidence, it is a good idea to consider these four potential pitfalls, which could be used to challenge a document's admissibility in court : Parol evidence, Authentication, Best evidence and Hearsay.
- The parol evidence rule prohibits the admission of certain evidence concerning the terms of a written agreement. It operates on the assumption that whatever is included in a signed agreement contains the final and complete agreement of the parties.
- Authentication is essentially showing the court that a piece of evidence is what it claims to be and documentary evidence can be authenticated similar to other real evidence.
- The best evidence rule can be used to deny the admissibility of copies or replications of certain documents. Under this rule, when the contents of a written document are offered in evidence, the court will not accept a copy or other proof of the document's content in place of the original document unless an adequate explanation is offered for the absence of the original.
- Hearsay : Documents can be considered hearsay if they contain statements made out of court (and not under oath) and where they are being used in court to prove the truth of those statements.

➥ 2.1.2 Documenting Evidence in the Lab

- After collecting digital evidence at the scene, send it to a forensics lab, which should be a controlled environment that ensures the security and integrity of digital evidence.
- In any investigative work, be sure to record investigator activities and findings as you work. To do so, investigator can maintain a journal to record the steps as taken as for processing evidence.
- Main goal is to be able to reproduce the same results when you or another investigator repeat the steps you took to collect evidence.
- If you get different results when you repeat the steps, the credibility of your evidence becomes questionable. At best, the evidence's value is compromised; at worst, the evidence will be dis-qualified. Because of the nature of electronic components, failures do occur.
- For example, you might not be able to repeat a data recovery because of a hardware failure, such as a disk drive head crash. Be sure to report all facts and events as they occur. Besides verifying your work, a journal serves as a reference that documents the methods you used to process digital evidence. You and others can use it for training and guidance on other investigations.

➥ 2.1.3 Processing and Handling Digital Evidence

- Must maintain the integrity of digital evidence in the lab, when collecting it in the field. The first task is to preserve the disk data. If you have a suspect computer that hasn't been copied with an imaging tool, you must create a copy.
- It is necessary to do the suspect drive read-only and document this step. If the disk has been copied with an imaging tool, you must preserve the image files. With most imaging tools, you can create smaller, compressed volume sets to make archiving your data easier.
- Steps to create image files :
  1. Copy all image files to a large drive.
  2. Start forensics tool to analyze the evidence.
  3. Run an MD5 or SHA-1 hashing algorithm on the image files to get a digital hash.
  4. When finish copying image files to a larger drive, secure the original media in an evidence locker. Don't work with the original media; it should be stored in a locker that has an evidence custody form. Be sure to fill out the form and date it.

➥ 2.1.4 Preparing to Acquire Digital Evidence

- The evidence you acquire at the scene depends on the nature of the case and the alleged crime or violation.
- Following questions are asked to supervisor or senior forensics examiner :
  a. Do you need to take the entire computer and all peripherals and media in the immediate area?
  b. How are you going to protect the computer and media while transporting them to your lab?
  c. Is the computer powered on when you arrive?
  d. Is the suspect you're investigating in the immediate area of the computer?

e. Is it possible the suspect damaged or destroyed the computer, peripherals, or media?

f. Will you have to separate the suspect from the computer?

- Digital forensics is the discipline that deals with all the process that includes collecting digital materials from the crime scene, examining, analyzing and reporting them according to certain standards and methods.
- Digital forensics consists of four main steps: preparation, collection, analysis and reporting.
- Collection is about accumulating digital evidence related with information technologies from the crime scene.
- Digital devices store the data in internal and external storage devices. The stored data has to be taken with certain methods. Shadow copying only the criminal part of the stored data or all of it from a device is named as image acquisition
- Direct analysis of digital evidences isn't considered appropriate because the data storage unit of the related device can break down and investigator can make a change on the evidence. For the forensics investigator, in order to assure the integrity of the evidence, a forensic copy must be taken.

University Question

1. Analyze how the following techniques are used :
   (i) Documents evidence in the lab
   (ii) Processing and handling Digital evidence **AU : Dec.-17, Marks 8**

2.2 Working with Windows and DOS Systems **AU : Dec.-16,17, May-17,18**

- Now days, majority of digital forensics tools operate over standard operating systems components, for example, standard file systems and caching mechanisms.
- In attempting to better understand the workings of a computer system at its core level, it is necessary to understand the difference between a file system and an operating system and the functionality of each.
- Examples of different file systems include the following : FAT12, FAT16, FAT32 and NTFS which are implemented on Windows OS.
- When trying to understand the mechanics of how computers actually manage data, it is necessary to delve into the physics of how a computer's OS uses the file system architecture.
- A file system defines the structure and the rules used to read, write and maintain information stored on a disk.

➤ File System

- File systems are abstraction that enables users to read, manipulate and organize data. Typically the data is stored in units known as files in a hierarchical tree where the nodes are known as directories.
- The file system enables a uniform view, independent of the underlying storage devices which can range between anything from floppy drives to hard drives and flash memory cards. Since file systems evolved from stand-alone computers the connection between the logical file system and the storage device was typically a one-to-one mapping.

- The DOS and Windows file systems use fixed-size clusters. Even if the actual data being stored requires less storage than the cluster size, an entire cluster is reserved for the file. This unused space is called the slack space.
- A **cluster**, *also known as an allocation unit*, consists of one or more sectors of storage space and represents the minimum amount of space that an operating system allocates when saving the contents of a file to a disk.
- File system must be mounted before it can be available to processes on the system. Procedure for mounting file system is as follows.
  1. Mount point is an empty directory at which the mounted file system will be attached.
  2. Name of the device and location within the file structure at which to attach the file system is required.
  3. Operating system verifies that the device contains a valid file system.
  4. Device driver is used by operating system for these verifications.
  5. Finally operating system mounts the file system at a specified mount point.

2.2.1 File Allocation Table

- A table that the operating system uses to locate files on a disk. Due to fragmentation, a file may be divided into many sections that are scattered around the disk. The FAT keeps track of all these pieces.
- The FAT system for older versions of Windows 95 is called FAT16 and the one for new versions of Windows 95 and Windows 98 is called FAT32.
- FAT file systems are commonly found on floppy disks, flash memory cards, digital cameras and many other portable devices because of their relative simplicity.
- File and folders are organized on FAT formatted volume which uses directory and file allocation table. The (C:\ or D:\) is the root folder at a per defined location on the volume. Folder contains a list of file and subdirectories. Fig. 2.2.1 shows the folder view of the file system.

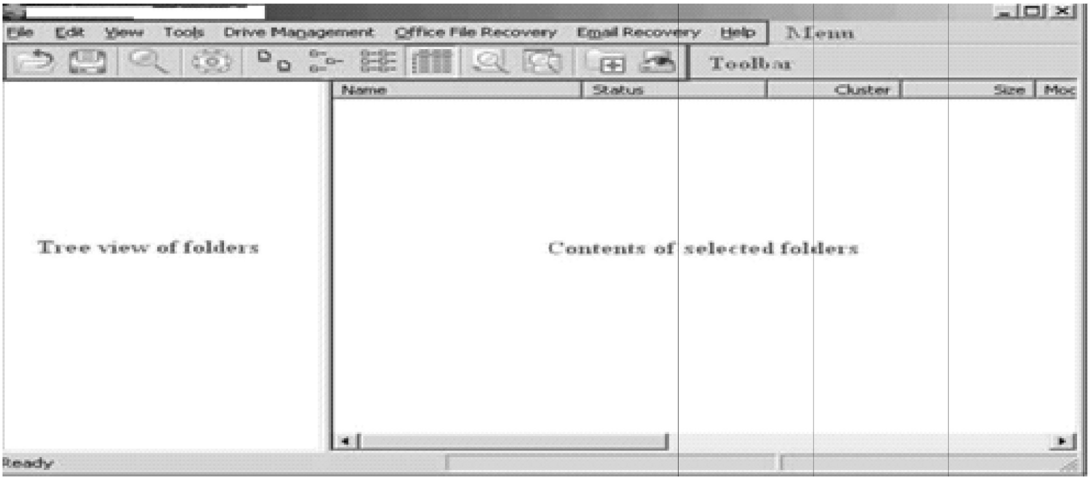
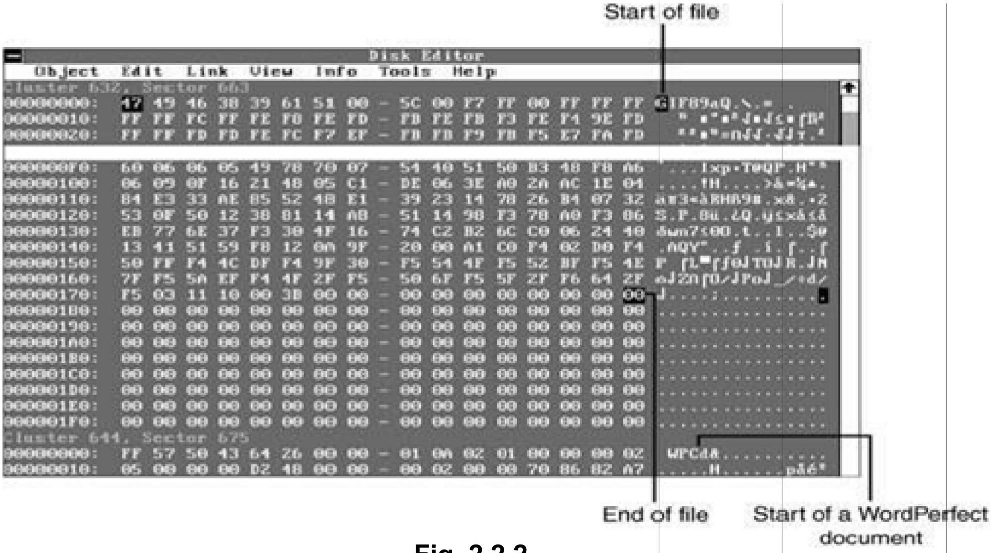


Fig. 2.2.1 : Folder view

- Folder view contains starting cluster, date, time associated with each file. FAT file system shows only last accessed date not time. At command line, "dir" command is used to gate the information about files and directory.
- The FAT shows only a list with one entry for each cluster in a volume. Each entry in the FAT indicates what the associated cluster is being used for the following Fig. 2.2.1 shows output from norton disk editor on file allocation table.

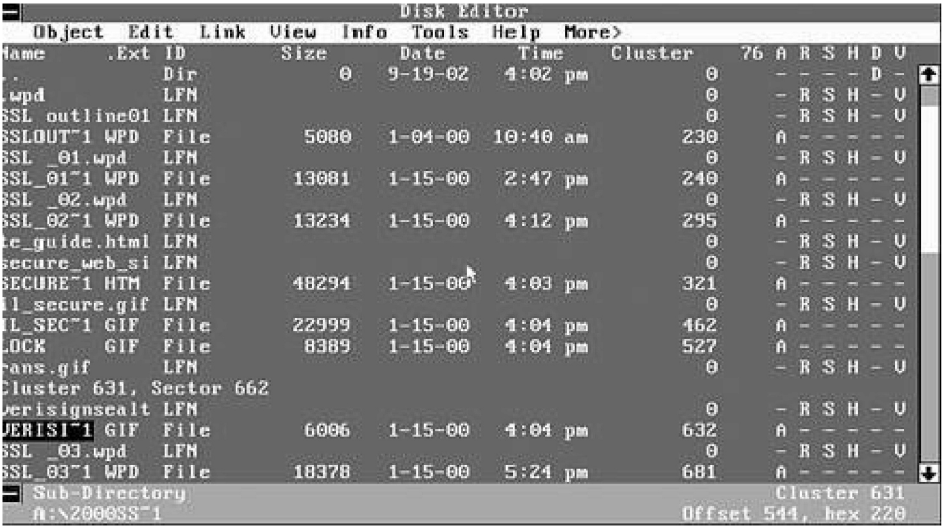

Disk Editor
Object Edit Link View Info Tools Help
Start of file
End of file
Start of a WordPerfect document

```
Cluster 632, Sector 663
00000000:  47 49 46 38 39 61 51 00 - 5C 00 F7 FF 00 FF FF FF  GIF89aQ.\.=  .
00000010:  FF FF FC FF FE F0 FE FD - FB FE FB F3 FE F4 9E FD
00000020:  FF FF FD FD FE FC F7 EF - FB FB F9 FB F5 E7 FA FD

000000F0:  60 06 06 05 49 78 70 07 - 54 40 51 50 B3 48 F8 A6  ...Ixp.T@QP.H
00000100:  06 09 0F 16 21 48 05 C1 - DE 06 3E A0 2A AC 1E 04  ....!H....>
00000110:  84 E3 33 AE 85 52 48 E1 - 39 23 14 78 26 84 07 32  .3..RH.9#.x&..2
00000120:  53 0F 50 12 38 81 14 A8 - 51 14 98 F3 78 A0 F3 86  S.P.8...Q...x...
00000130:  EB 77 6E 37 F3 30 4F 16 - 74 C2 B2 6C C0 06 24 40  .wn7.0O.t..l..$@
00000140:  13 41 51 59 F8 12 0A 9F - 20 00 A1 C0 F4 02 D0 F4  .AQY.... .......
00000150:  50 FF F4 4C DF F4 9F 30 - F5 54 4F F5 52 BF F5 4E  P..L...0.TO.R..N
00000160:  7F F5 5A EF F4 4F 2F F5 - 50 6F F5 5F 2F F6 64 2F  ..Z..O/.Po._/.d/
00000170:  F5 03 11 10 00 3B 00 00 - 00 00 00 00 00 00 00 00  .....;..........
00000180:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00  ................
00000190:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00  ................
000001A0:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00  ................
000001B0:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00  ................
000001C0:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00  ................
000001D0:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00  ................
000001E0:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00  ................
000001F0:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00  ................
Cluster 644, Sector 675
00000000:  FF 57 50 43 64 26 00 00 - 01 0A 02 01 00 00 00 02  .WPCd&..........
00000010:  05 00 00 00 D2 48 00 00 - 00 02 00 00 70 86 82 A7  .....H......p...
```

Fig. 2.2.2

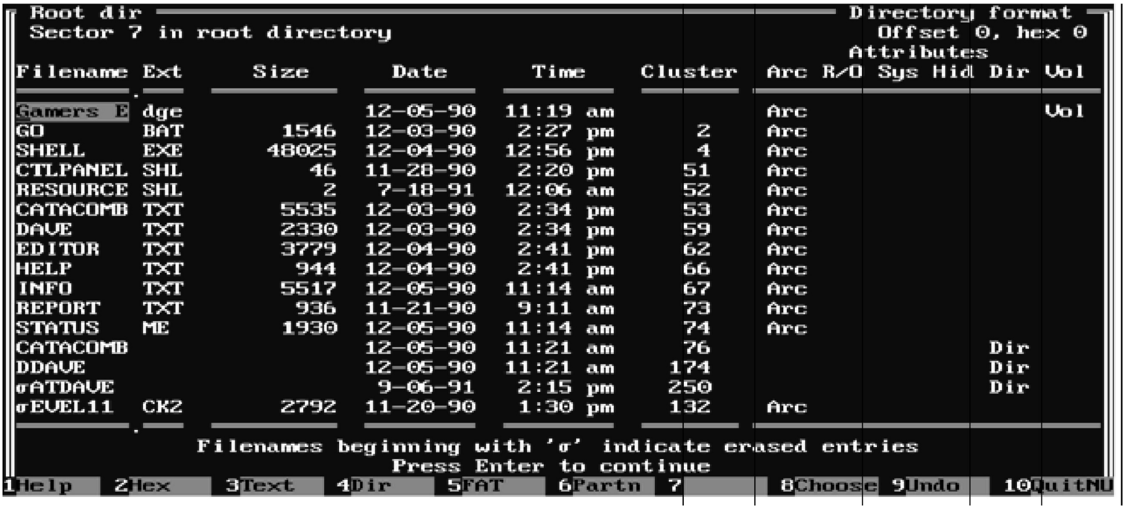
- Free allocation is marked by zero in the cluster. If it contains some value (i.e. Greater than zero) then that number is given to the next cluster for a given file or folder. EOF means end of file. Where file end, FAT marked it as EOF.
- Subdirectories are a special type of file. It contains information such as names, attributes, dates, times, sizes and the first cluster of each file on the system.



```
Name      .Ext ID       Size     Date      Time      Cluster   76 A R S H D V
..             Dir         0   9-19-02    4:02 pm          0      - - - - D -
.wpd           LFN                                         0      - R S H - V
SSL outline01  LFN                                         0      - R S H - V
SSLOUT~1  WPD  File     5080   1-04-00   10:40 am        230      A - - - - -
SSL _01.wpd    LFN                                         0      - R S H - V
SSL_01~1  WPD  File    13081   1-15-00    2:47 pm        240      A - - - - -
SSL _02.wpd    LFN                                         0      - R S H - V
SSL_02~1  WPD  File    13234   1-15-00    4:12 pm        295      A - - - - -
te_guide.html  LFN                                         0      - R S H - V
secure_web_si  LFN                                         0      - R S H - V
SECURE~1  HTM  File    48294   1-15-00    4:03 pm        321      A - - - - -
l1_secure.gif  LFN                                         0      - R S H - V
IL_SEC~1  GIF  File    22999   1-15-00    4:04 pm        462      A - - - - -
LOCK      GIF  File     8389   1-15-00    4:04 pm        527      A - - - - -
rans.gif       LFN                                         0      - R S H - V
Cluster 631, Sector 662
verisignsealt  LFN                                         0      - R S H - V
VERISI~1  GIF  File     6006   1-15-00    4:04 pm        632      A - - - - -
SSL _03.wpd    LFN                                         0      - R S H - V
SSL_03~1  WPD  File    18378   1-15-00    5:24 pm        681      A - - - - -
Sub-Directory                                                  Cluster 631
  A:\2000SS~1                                          Offset 544, hex 220
```

Fig. 2.2.3

- When a file is deleted, the file system will perform one of two tasks on the allocation table. The file's entry on the file allocation table marked as “free space” or the file's entry on the list is erased and then the space is marked as free.
- If a file needs to be placed on the storage unit, the operating system will put the file in the space marked as empty. After the new file is written to the “empty space”, the deleted file is now gone forever. When a deleted file is to be recovered, the user must not manipulate any files because if the “empty space” is used, then the file can never be retrieved.



```
Root dir                                                        Directory format
Sector 7 in root directory                                         Offset 0, hex 0
                                                                 Attributes
Filename Ext      Size      Date       Time     Cluster   Arc R/O Sys Hid Dir Vol

Gamers E dge              12-05-90   11:19 am             Arc                  Vol
GO       BAT      1546    12-03-90    2:27 pm        2    Arc
SHELL    EXE     48025    12-04-90   12:56 pm        4    Arc
CTLPANEL SHL        46    11-28-90    2:20 pm       51    Arc
RESOURCE SHL         2     7-18-91   12:06 am       52    Arc
CATACOMB TXT      5535    12-03-90    2:34 pm       53    Arc
DAVE     TXT      2330    12-03-90    2:34 pm       59    Arc
EDITOR   TXT      3779    12-04-90    2:41 pm       62    Arc
HELP     TXT       944    12-04-90    2:41 pm       66    Arc
INFO     TXT      5517    12-05-90   11:14 am       67    Arc
REPORT   TXT       936    11-21-90    9:11 am       73    Arc
STATUS   ME       1930    12-05-90   11:14 am       74    Arc
CATACOMB                  12-05-90   11:21 am       76                     Dir
DDAVE                     12-05-90   11:21 am      174                     Dir
σATDAVE                    9-06-91    2:15 pm      250                     Dir
σEVEL11  CK2      2792    11-20-90    1:30 pm      132    Arc

          Filenames beginning with 'σ' indicate erased entries
                        Press Enter to continue
1Help  2Hex   3Text  4Dir   5FAT   6Partn  7     8Choose 9Undo  10QuitNU
```

Fig. 2.2.4

- Floppy diskette uses FAT12 file system. Each entry contains 12 bits in the FAT. FAT16 uses 16 bit fields to identify a cluster. Hard disk uses FAT32 and 28 bits plus 4 bit reserved field used to identify the cluster.

➥ 2.2.2 Network File System

- Master file table is the heart of NTFS. The MFT is an array of file records. Each record is 1024 bytes. The first record in the MFT is for the MFT itself. The name of the MFT is $MFT. The first 16 records in the MFT are reserved for metadata files.
- An MFT can be too big if a volume used to have lots of files that were deleted. The files that were deleted cause internal holes in the MFT. These holes are significant regions that are unused by files. It is impossible to reclaim this space. This is at least true on a live NTFS volume.
- Fig. 2.2.5 shows NTFS Partition.

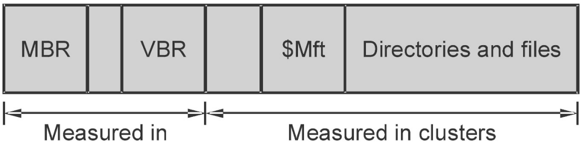


Fig. 2.2.5 : NTFS partition

- As files are added to an NTFS volume, more entries are added to the MFT and so the MFT increases in size. When files are deleted from an NTFS volume, their MFT entries are marked as free and may be reused, but the MFT does not shrink. Thus, space used by these entries is not reclaimed from the disk.
- Directories are treated in NTFS as index entries and store folder entries in a B-Tree to accelerate access and facilitate resorting when entries are deleted. NTFS uses an encoding scheme called unicode.
- The attribute places INDX records in a B+ tree, where the key is the file name. A B+ tree is a data structure where arbitrary records are organized by a sortable key value, such as a number or a string. For a forensic investigator, the effect of the B+ tree is that INDX records associated with a node are stored as a chunk in alphanumeric order.
- The size of a B+ node is 4096 bytes. When a file is added to a directory, a new record is added to the INDX attribute of the directory. Within the B+ tree, NTFS finds the appropriate node and inserts the new record, shifting records down, if necessary.
- Fig. 2.2.6 shows the file with a logical size that is larger than its valid data length, leaving un-initialized space.

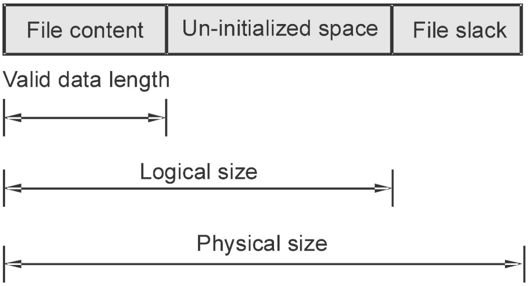


Fig. 2.2.6 : File with logical size

- Fig. 2.2.7 shows the behavior of the Microsoft NTFS driver as an INDX record is deleted. When the driver removes INDX record “F”, it shifts the records “G” and “H” to fill the space. As the contents of record “H” shift, a recoverable copy (inactive record “H' “) remains in the newly expanded slack space.

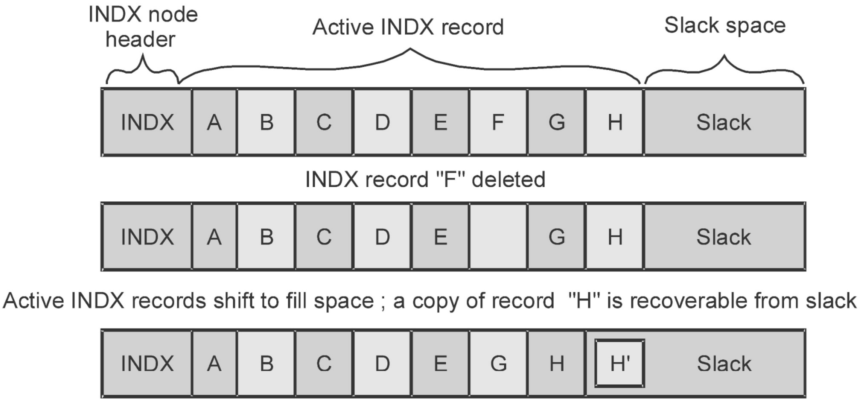


Fig. 2.2.7 : Behavior of NTFS driver

- NTFS captures the difference between logical file size and valid data length in two MFT fields.
- NTFS creates MFT entries whenever required. When a file is deleted, NTFS simply marks the associated MFT entry as deleted and available for a new file. It is possible to recover all of the information about a deleted file from the MFT entry, including the data for resident files and the location of data on disk for non-resident files.
- Recovery of deleted files in the NTFS is complicated. when a file is deleted, the next file that is created may overwrite the MFT entry for the deleted file.

➤ NTFS Data Streams

- NTFS data stream is a unique set of file attributes. NTFS supports multiple data streams per file : one main stream plus an optional set of alternate data streams.
- A data stream can be created in an existing file on an NTFS volume. NTFS supports multiple data streams, where the stream name identifies a new data attribute on the file. A handle can be opened to each data stream.
- A data stream is a unique set of file attributes. Streams have separate opportunistic locks, file locks, and sizes, but common permissions.
- A data stream does not appear when a file is opened in a text editor. The only way to see if a data stream is attached to a file is by examining the MFT entry for the file.
- In NTFS, a data stream becomes an additional file attribute. It allows the file to be associated with different applications. You can only tell whether a file has a data stream attached by examining that file's MFT entry.
- Alternate data stream : The stream in any data attribute on a file or directory other than the default, unnamed stream.

➤ NTFS Compressed Files

- NTFS is capable of compressing individual files, all files within a folder, all files/folders on the volume. Compression is executed within NTFS.
- Any Windows program can read/write compressed files without considering the extent of the compression. When a compressed file is opened, only a part of the file is decompressed while being read.
- Data already in memory is uncompressed. Modified and new data is compressed again, when written to the compressed file on disk.
- NTFS compression algorithms support cluster sizes of up to 4 kB.
- The best use of compression is for files which are repetitive, written seldom, usually accessed sequentially : log files are an ideal example.
- Compression works in blocks of 16 clusters. Data is compressed using a modified LZ77 algorithm, named LZNT1.
- Each block is compressed independently. If compressed block does not become less than the original 16 clusters, it is left uncompressed.

- Compressing a file adds serious complexity to the way the file is stored. The MFT is the only place that contains information about what parts are compressed and by how much. If MFT is corrupted there is little hope retrieving the data
- Each NTFS data stream contains information that indicates whether any part of the stream is compressed.
- NTFS provides real-time access to a compressed file, decompressing the file when it is opened and compressing it when it is closed.
- When writing a compressed file, the system reserves disk space for the uncompressed size. The system gets back unused space as each individual compression buffer is compressed.
- If the compressed information takes up less space than the source file, then the rest of the space is labeled as sparse space and no space on the volume is allocated to it. Because the compressed data often doesn't have a size exactly that of the cluster, the end of each of these blocks stays as unusable space of significant size.
- Most computer forensics tools can uncompress and analyze compressed Windows data.

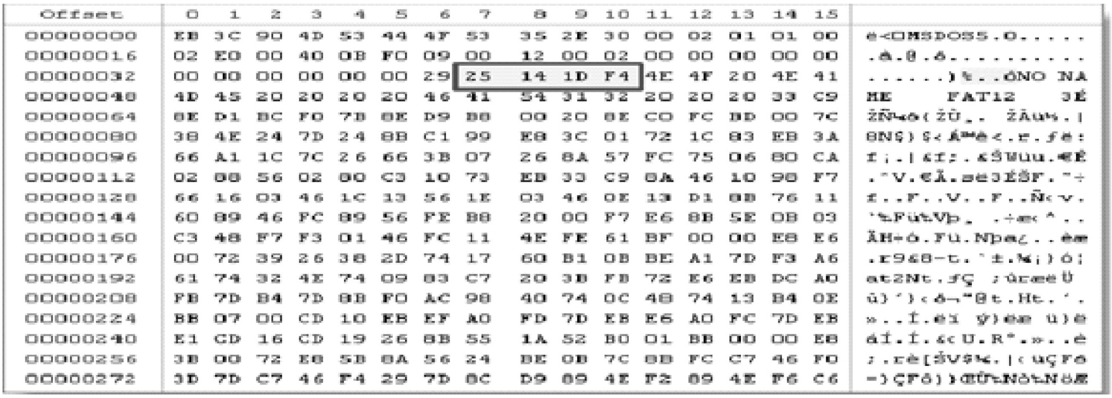
➤ NTFS Encrypting File System (EFS)

- NTFS files can be encrypted to protect the information from unauthorized users. It is valuable form of protection for local file access. Digital encryption keys from each user are implemented to encrypt and decrypt the file.
- As a first setp to encrypt file, NTFS creates a log file called "**Efs0.log**" in System Volume Information folder on the same drive, as encrypted file. Then EFS aquires access CryptoAPI context. EFS generate File Encryption Key (FEK).
- The next step is to get public/private key pair; if it does not exist at this stage, EFS generate a new pair. EFS uses 1024-bit RSA algorithm to encrypt FEK.
- EFS create Data Decryption Field (DDF) for the current user, where it places FEK and encrypts it with public key. If recovery agent is defined by system policy, EFS creates also Data Recovery Field (DRF) and places there FEK encrypted with public key of recover agent.
- A separate DRA is created for every recovery agent defined. Now a temporary file Efs0.tmp is created in the same folder as the file being encrypted.
- The contents of original file (plain text) is copied into temporary file, after that the original is overwritten with encrypted data.
- By default, EFS uses DESX algorithm with 128-bit key to encrypt file data, but Windows could be also configured to use stronger 3DES algorithm with 168-bit key. After encryption is done, temporary and log files are deleted.
- After file is encrypted, only users who has correspondent DDF or DRF can access the file. This mechanism is separate from common security meaning that beside rights to access file, the file must have its FEK encrypted with user's public key.

- Only user who can decrypt FEK with his own private key, can access the file. The consequence is, that user, who has access to the file, can encrypt it thus preventing the owner to access his own file.
- The decryption process is opposite to encryption : First, system checks if user has a private key used by EFS. If yes, it reads EFS attributes and walk through the DDF ring looking for DDF for current user.
- If DDF is found, user's private key is used to decrypt FEK extracted from DDF. Using decrypted FEK, EFS decrypts file data. It should be noticed that file never decrypted in whole but rather by sectors when upper level module requests particular sector.

➥ 2.2.3 Date and Time

- Changing the date or time on a computer is relatively easy; simply right click on the date in the Windows task bar and you can adjust the date on the computer. One defendant who was on notice that his computer would be examined on a given date sought to obscure evidence of his crime. He turned the computer clock back two months, deleted the incriminating files and returned the computer clock back to the correct time.
- It is necessary to understand the how date and time are stored and converted in the OS.
- Here is an example from a formatted FAT12 floppy diskette. With reference to Fig. 2.2.8 shows, at offset 39 (0x27), the hex values 25 14 1D F4 is the volume serial number. With FAT32 volumes, the volume serial number is stored in the boot sector at offset 67 (0x43). When formatted, this floppy diskette returned the volume serial 2514 - 1DF4. The disk was formatted on Sunday, 19th October 2003 at 22:33:27.01.



```
Offset     0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15
00000000  EB 3C 90 4D 53 44 4F 53  35 2E 30 00 02 01 01 00  ë<MSDOS5.0.....
00000016  02 E0 00 40 0B F0 09 00  12 00 02 00 00 00 00 00  .à.@.ð..........
00000032  00 00 00 00 00 00 29 25  14 1D F4 4E 4F 20 4E 41  ......)%..ôNO NA
00000048  4D 45 20 20 20 20 46 41  54 31 32 20 20 20 33 C9  ME    FAT12   3É
00000064  8E D1 BC F0 7B 8E D9 B8  00 20 8E C0 FC BD 00 7C  ŽÑ¼ð{ŽÙ¸. ŽÀü½.|
00000080  38 4E 24 7D 24 8B C1 99  E8 3C 01 72 1C 83 EB 3A  8N$}$‹Á™è<.r.ƒë:
00000096  66 A1 1C 7C 26 66 3B 07  26 8A 57 FC 75 06 80 CA  f¡.|&f;.&ŠWüu.€Ê
00000112  02 88 56 02 80 C3 10 73  EB 33 C9 8A 46 10 98 F7  .ˆV.€Ã.së3ÉŠF.˜÷
00000128  66 16 03 46 1C 13 56 1E  03 46 0E 13 D1 8B 76 11  f..F..V..F..Ñ‹v.
00000144  60 89 46 FC 89 56 FE B8  20 00 F7 E6 8B 5E 0B 03  `‰Fü‰Vþ¸ .÷æ‹^..
00000160  C3 48 F7 F3 01 46 FC 11  4E FE 61 BF 00 00 E8 E6  ÃH÷ó.Fü.Nþa¿..èæ
00000176  00 72 39 26 38 2D 74 17  60 B1 0B BE A1 7D F3 A6  .r9&8-t.`±.¾¡}ó¦
00000192  61 74 32 4E 74 09 83 C7  20 3B FB 72 E6 EB DC A0  at2Nt.ƒÇ ;ûræëÜ 
00000208  FB 7D B4 7D 8B F0 AC 98  40 74 0C 48 74 13 B4 0E  û}´}‹ð¬˜@t.Ht.´.
00000224  BB 07 00 CD 10 EB EF A0  FD 7D EB E6 A0 FC 7D EB  »..Í.ëï ý}ëæ ü}ë
00000240  E1 CD 16 CD 19 26 8B 55  1A 52 B0 01 BB 00 00 E8  áÍ.Í.&‹U.R°.»..è
00000256  3B 00 72 E8 5B 8A 56 24  BE 0B 7C 8B FC C7 46 F0  ;.rè[ŠV$¾.|‹üÇFð
00000272  3D 7D C7 46 F4 29 7D 8C  D9 89 4E F2 89 4E F6 C6  =}ÇFô)}Œ Ù‰Nò‰NöÆ
```

Fig. 2.2.8

- Calculation of volume serial number is as follows :

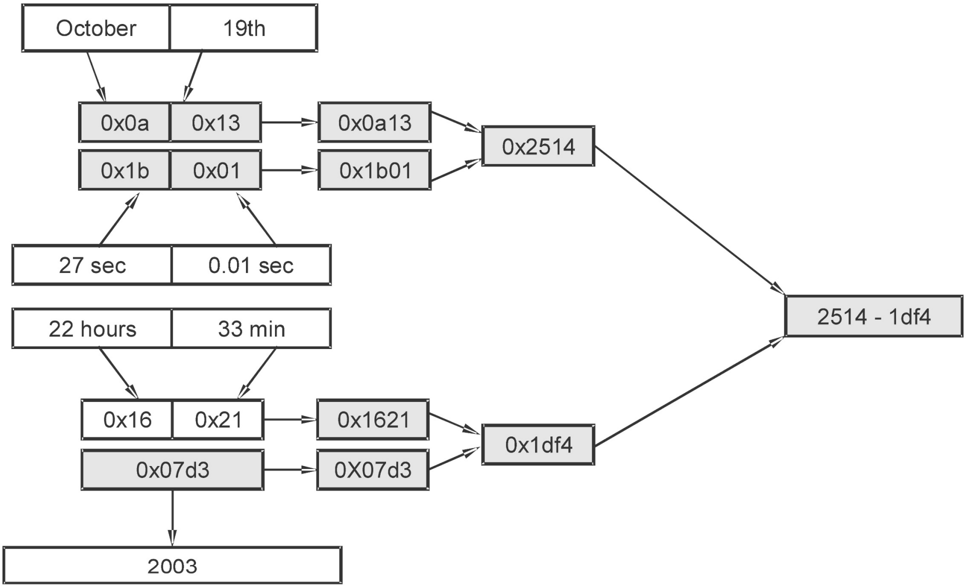


Fig. 2.2.9 Serial number calculation

➥ 2.2.4 Data Recovery

- Data recovery from FAT and NTFS is done in two ways :
  1. Recovering deleted data from unallocated space
  2. Recovering data from slack space.
- Unallocated space is searched for recovering deleted directory. Tools EnCase and X-Ways uses this method for data recovery. Undelete\File recovery software searches unallocated space and makes found files available.

➤ Windows-Based Recovery Tools

- Windows bases recovery tools are EnCase, FTK and X-Ways. These tools use a bit-stream copy of a disk to display a virtual reconstruction of the file system. It also displays deleted files, without actually modifying the FAT.

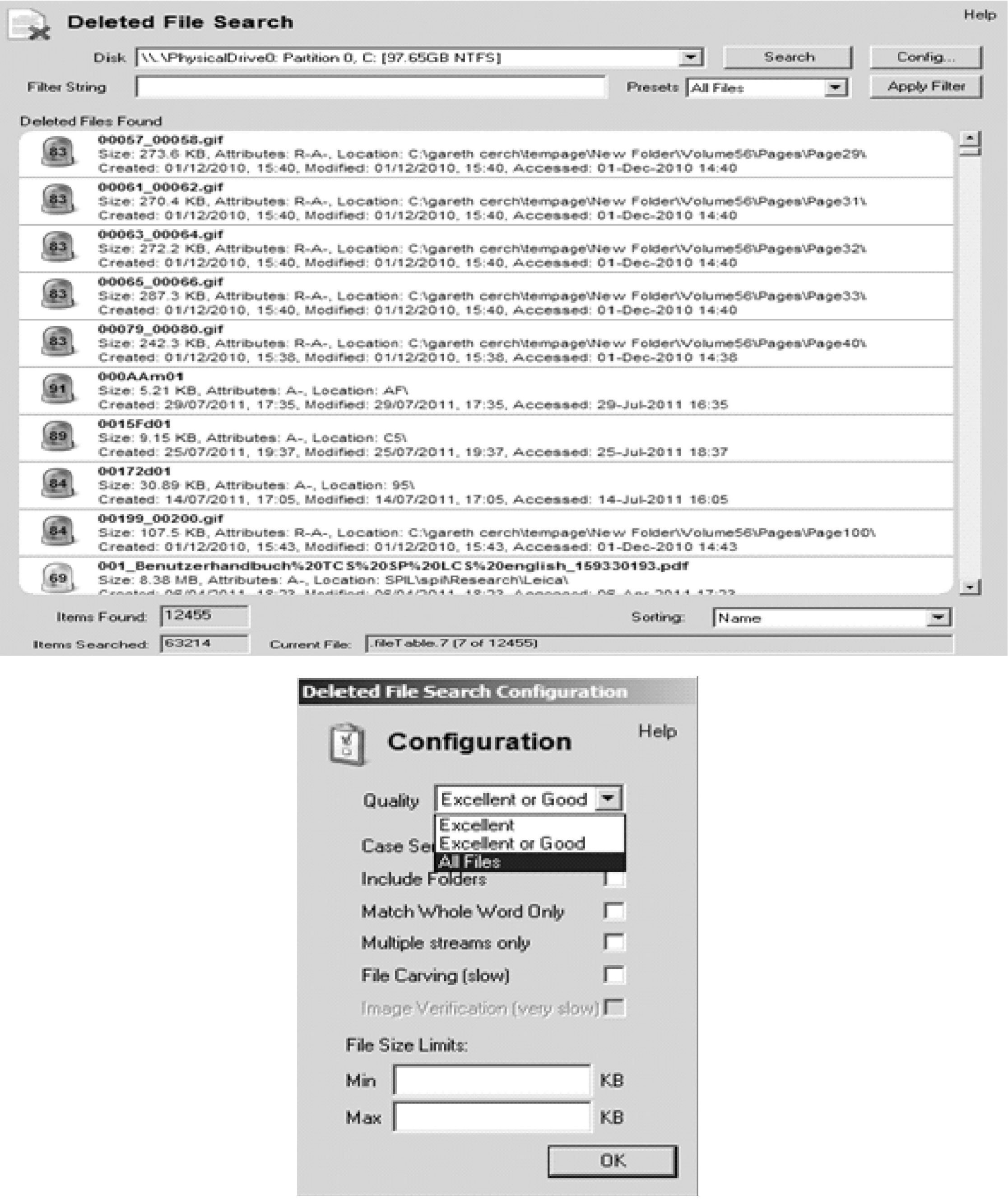
➤ Linux-Based Recovery Tools

- Sleuth kit and SMART 6 are used for Linux based recovery tool. These tools are used to recover deleted files from FAT and NTFS.

➤ File Carving with Windows

- File carving is a process used in computer forensics to extract data from a disk drive or other storage device without the assistance of the file system that originality created the file. carving looks for particular signatures or patterns that may give a clue that some interesting data can be stored in a particular spot on the disk

- It is a method that recovers files at unallocated space without any file information and is used to recover data and execute a digital forensic investigation.
- **Data carving technique :** A raw bits of disk analysed to identify recognisable patterns that may indicate a data file, e.g. header/footer, semantic information.



Deleted File Search

Disk: \\.\PhysicalDrive0: Partition 0, C: [97.65GB NTFS]

Filter String:

Presets: All Files

Deleted Files Found

83 **00057_00058.gif**
Size: 273.6 KB, Attributes: R-A-, Location: C:\gareth cerch\tempage\New Folder\Volume56\Pages\Page29\
Created: 01/12/2010, 15:40, Modified: 01/12/2010, 15:40, Accessed: 01-Dec-2010 14:40

83 **00061_00062.gif**
Size: 270.4 KB, Attributes: R-A-, Location: C:\gareth cerch\tempage\New Folder\Volume56\Pages\Page31\
Created: 01/12/2010, 15:40, Modified: 01/12/2010, 15:40, Accessed: 01-Dec-2010 14:40

83 **00063_00064.gif**
Size: 272.2 KB, Attributes: R-A-, Location: C:\gareth cerch\tempage\New Folder\Volume56\Pages\Page32\
Created: 01/12/2010, 15:40, Modified: 01/12/2010, 15:40, Accessed: 01-Dec-2010 14:40

83 **00065_00066.gif**
Size: 287.3 KB, Attributes: R-A-, Location: C:\gareth cerch\tempage\New Folder\Volume56\Pages\Page33\
Created: 01/12/2010, 15:40, Modified: 01/12/2010, 15:40, Accessed: 01-Dec-2010 14:40

83 **00079_00080.gif**
Size: 242.3 KB, Attributes: R-A-, Location: C:\gareth cerch\tempage\New Folder\Volume56\Pages\Page40\
Created: 01/12/2010, 15:38, Modified: 01/12/2010, 15:38, Accessed: 01-Dec-2010 14:38

91 **000AAm01**
Size: 5.21 KB, Attributes: A-, Location: AF\
Created: 29/07/2011, 17:35, Modified: 29/07/2011, 17:35, Accessed: 29-Jul-2011 16:35

89 **0015Fd01**
Size: 9.15 KB, Attributes: A-, Location: C5\
Created: 25/07/2011, 19:37, Modified: 25/07/2011, 19:37, Accessed: 25-Jul-2011 18:37

84 **00172d01**
Size: 30.89 KB, Attributes: A-, Location: 95\
Created: 14/07/2011, 17:05, Modified: 14/07/2011, 17:05, Accessed: 14-Jul-2011 16:05

84 **00199_00200.gif**
Size: 107.5 KB, Attributes: R-A-, Location: C:\gareth cerch\tempage\New Folder\Volume56\Pages\Page100\
Created: 01/12/2010, 15:43, Modified: 01/12/2010, 15:43, Accessed: 01-Dec-2010 14:43

69 **001_Benutzerhandbuch%20TCS%20SP%20LCS%20english_159330193.pdf**
Size: 8.38 MB, Attributes: A-, Location: SPIL\spil\Research\Leica\

Items Found: 12455

Sorting: Name

Items Searched: 63214

Current File: .fileTable.7 (7 of 12455)

Deleted File Search Configuration

Configuration

Quality: Excellent or Good

Case Se

Include Folders ☐

Match Whole Word Only ☐

Multiple streams only ☐

File Carving (slow) ☐

Image Verification (very slow) ☐

File Size Limits:

Min KB

Max KB

Fig. 2.2.10

- Carving software designed to take a linear approach to locating data files. An incomplete files, large files containing information from multiple sources, extracts embedded images from PowerPoint's are creates **Franken files**. Following Fig. 2.2.10 shows deleted file search.

➤ Limitations of Data Carving

- Not all data can be carved. Carving is based on characteristic signatures or patterns.
- For example, JPEG files typically have the "JFIF" signature in the beginning, followed by the file header.
- PDF files begin with "%PDF" and ZIP archives start with "PK". Some other files can be true binary.
- **Logical file size :** It is the actual size of the file.
- **Physical file size :** It is the size given to the file on the hard disk. The physical file size is always greater than or equal to the logical file size.
- **File slack** is the difference between the physical file size and logical file size. The file slack should always be less than 1 cluster.
- **For example :** A data file size is 5055 bytes and it is given 2 clusters space. 1 cluster = 4096 bytes. Two clusters mean 8192 bytes.

  File slack = 8192 – 5055

  = 3137 bytes

- New file is created by overwriting unallocated space. The file slack is essentially old fragments of unallocated file space. File slack can contain anything at all, from fragments of web pages, emails and even complete small pictures, to junk text.
- Important evidence often ends up in the **recycle bin**. This is especially true for Windows PCs. Literally, deleted files can often be successfully retrieved by analyzing the content of the recycle bin, a temporary storage they're placed before being erased. If deleted files do not show up in the recycle bin, there are still good chances to recover them by using one of the many commercial data recovery tools. The principle of deleted file recovery is based on the fact that Windows does not wipe the contents of the file when it's being deleted. Instead, a file system record storing the exact location of that file on the disk is being marked as "deleted". The disk space previously occupied by the file is then advertised as available - but not overwritten with zeroes or other data just yet.

➤ Dealing with Password Protection and Encryption

- In some cases, digital investigators to overcome password protection or encryption on a computer they are processing.
- Hard disk is fully encrypted and suspect who refuses to give up the key is totally useless to an investigator. If type of encryption algorithm is also known, a brute force attack on any good encryption key is infeasible.
- If the suspect has chosen one long and random password, then it is impossible to recover any data form that computer.

- For this type of situation, there are many specialized tools available that can bypass or recover passwords of various files. The most powerful and versatile password recovery programs currently available are PRTK and Distributed Network Attack (DNA) from Access Data.

➥ 2.2.5 Log File

- Windows operating systems store log files in the **"%systemroot%\system32\config\"** folder. System log files can contains the information about the user account. Each log contains a list of events that occurred, along with problems, failures and warnings.
- The Windows application, security, and system log files can be read with a Windows application called "Event Viewer," which is accessed through the Control Panel.
- Most log files are in plain text format. You can view them with any text editor such as Vi or Emacs. Some log files are readable by all users on the system; however, root privileges are required to read most log files.

➥ 2.2.6 Registry

- The registry is made up of keys. Each key is like the branch of a tree. Each key has one parent key and zero or more child keys. Each key can contain zero or more "Values", each of which contains a single piece of data.
- Windows operating systems use the registry to store system configuration information and usage details. Registry is a database that stores initialization files such as hardware/software configuration, network connections, user preferences, setup information.
- The registry contains following main keys :
  1. HKEY_CLASSES_ROOT : It contains information on file types, including which programs are used to open a particular file type.
  2. HKEY_CURRENT_USER : It contains user-specific settings that are built from information in the HKEY_USERS key during the logon process.
  3. HKEY_LOCAL_MACHINE : It contains computer specific information including installed hardware and software. This is the one users tend to spend the most time in.
  4. HKEY_USERS : It contains information about all of the users who log on to the computer. This includes settings for programs, desktop configurations and so on. This key contains one sub-key for each user.
  5. HKEY_CURRENT_CONFIG : It contains information about the computer's hardware configuration.
- In some registry file, keys value stored in hexadecimal format but it can be converted to ASCII and saved to a text file.
- The registry contains the configuration information for the hardware and software and may also contain information about recently used programs and files.15 proof that a suspect had installed a program or application may be found in the registry.

University Questions

1. While processing crime, how will you work with windows and DOS systems ? **AU : Dec.-16, Marks 8**
2. Explain in detail about how the understanding NTFA, FAT, FAT32 file system plays a Crucial role in cyber forensic. **AU : May-17, Marks 16**
3. Examine the MS - DOS startups tasks and about other disk operating system in detail. **AU : Dec.-17, Marks 16**
4. Explain the following : NTFS data streams, NTFS compressed files and NTFS encrypting file system. **AU : May-18, Marks 16**

2.3 Current Computer Forensics Tools : Software/ Hardware Tools

AU : Dec.-16

- The field of computer forensic investigation includes the capture and analysis of digital data to either prove a crime has or has not been committed. The range of crimes can include computer related crime as well as other crimes that have left evidence in digital formats.
- There are two basic types of data that are collected, persistent data and volatile data. Persistent data is that which is stored on a hard drive or another medium and is preserved when the computer is turned off. Volatile data is any data that is stored in memory or exist in transit and will be lost when the computer is turned off. Volatile data might be key evidence, so it is important that if the computer is on at the scene of the crime it remain on. There are a variety of tools used to collect data.
- Tools are used to analyze digital data and prove or disprove criminal activity. It is used in 2 of the 3 phases of computer forensics.
  1. Acquisition - Images systems and gathers evidence
  2. Analysis - Examines data and recovers deleted content
  3. Presentation - Tools not used

➤ Types of Computer Forensics Tools

1. Hardware forensic tools : Range from single-purpose components to complete computer systems and servers
2. Software forensic tools : There are two types of software forensic tools. Command-line applications and GUI applications are two types. It is commonly used to copy data from a suspect's disk drive to an image file.

➤ Computer Forensic Tools Capabilities

1. Recover deleted files
2. Find out what external devices have been attached and what users accessed them
3. Determine what programs ran
4. Recover web pages

5. Recover emails and users who read them
6. Recover chat logs
7. Determine file servers used
8. Discover document's hidden history
9. Recover phone records and SMS text messages from mobile devices

➤ Tasks Performed by Computer Forensics Tools

1. Acquisition
2. Validation and discrimination
3. Extraction
4. Reconstruction
5. Reporting

- Computer forensics procedures can be distilled into three major components :

  1) Make a digital copy of the original evidence. Investigator make a copy of the evidence and work with the copy to reduce the possibility of inadvertently changing the original evidence.
  2) Authenticate that the copy of the evidence. Investigators must verify the copy of the evidence is exactly the same as the original.
  3) Analyze the digital copy. The specific procedures performed in an investigation are determined by the specific circumstances under which the investigation is occurring.

- 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 :

  1. Disk and data capture tools
  2. File viewers
  3. File analysis tools
  4. Registry analysis tools
  5. Internet analysis tools
  6. Email analysis tools
  7. Mobile devices analysis tools
  8. Mac OS analysis tools
  9. Network forensics tools
  10. Database forensics tools

➥ 2.3.1 Tools

➤ 1. The Sleuth Kit (TSK)

- The Sleuth Kit (TSK) is a library and collection of Unix- and Windows-based tools and utilities to allow for the forensic analysis of computer systems. It allows examination of DOS, BSD, Mac, Sun, GPT partitions and disks.

- It also includes the autopsy forensic browser as a graphical analysis tool and supports integration with SQLite database. It can be run on live Windows systems for incident response.
- With this kit, the user can examine the computer file systems through a non-intrusive approach that is not dependent on the investigated machine operating system to process the file system, deleted and hidden from files DOS, BSD, Mac, Sun and Linux partitions.
- The results generated by Sleuth Kit tools are used by another tool. The autopsy forensic browser which presents such details as image integrity, keyword searches and other automatized operations about the investigated partition through a graphical interface.
- The Sleuth Kit was written in C and Perl and uses an aspect of the TCT code.

➤ 2. The Coroner's Toolkit (TCT)

- The TCT tools do not recognize NTFS, FAT or EXT3 partitions, making them of little use when performing forensic investigations in machines with Microsoft Windows and/or Linux operating systems with EXT3 file systems.
- Investigating Windows (FAT) partitions with TCT is only possible with a conversion to EXT2 format, demanding alterations on the i-nodes table of the investigated partition. This activity is not always possible with data analysis.

➤ 3. FTK TOOL

- FTK can analyze data from several sources, including image files from other vendors. FTK also produces a case log file, where you can maintain a detailed log of all activities during the examination such as keyword searches and data extractions.
- FTK provides two options for searching for keywords. One option is an indexed search, which catalogs all words on the evidence drive so that FTK can find them quickly. The other option is live search, which can locate items such as text hidden in unallocated space that might not turn up in an indexed search.

➤ 4. Maresware

- Maresware computer forensics software provides an essential set of tools for investigating computer records and securing private information. It is highly flexible to meet the needs of all types of investigators including : law enforcement, intelligence agency, private investigator, corporate security officers and human resources personnel.
- It is used within a forensic paradigm, the software enables discovery of evidence for use in criminal or civil legal proceedings. Internal investigators can develop documentation to support disciplinary actions, yet do so non-invasively, to preserve evidence that could end up in court.

➤ Functions of Maresware

a. Discovery of “hidden” files(such as NTFS Alternate Data Streams)

b. For incident response purposes

c. Evaluation of timelines

d. Key word searching

e. Files verification

f. Drive wiping for information privacy and security

g. File reformatting

h. Documenting all the examiner's steps and procedures

➤ 5. ProDiscover Basic

- ProDiscover basic from technology pathways is a forensics data analysis tool. It can be used to acquire and analyze data from several different file systems such as Microsoft FAT and NTFS, Linux Ext2 and Ext3 and other UNIX file system.

University Question

1. Explain in details the various computer forensic tools. **AU : Dec.-16, Marks 8**

2.4 Questions with Answers

2.4.1 Two Marks Questions with Answers

Q. 1 What is evidence and evidence processing ?

Ans. : Evidence” is any substance or material found or recovered in connection with a criminal investigation.

“Evidence processing” refers to the specific actions taken at a crime scene or collision scene to identify, locate, document, preserve and collect evidence and/or known standards.

Q. 2 List the step of digital evidence collection.

Ans. : Digital evidence collection follows a four-step methodology :

a. Identify sources of evidentiary material

b. Authenticate the evidentiary material

c. Collect the evidentiary material

d. Maintain a documented chain of custody

Q. 3 What is file allocation table ?

Ans. : A table that the operating system uses to locate files on a disk. Due to fragmentation, a file may be divided into many sections that are scattered around the disk. The FAT keeps track of all these pieces. The FAT system for older versions of Windows 95 is called FAT16 and the one for new versions of Windows 95 and Windows 98 is called FAT32.

Q. 4 What is purpose of The Sleuth Kit (TSK) ?

Ans. : The Sleuth Kit (TSK) is a library and collection of Unix- and Windows-based tools and utilities to allow for the forensic analysis of computer systems. It allows examination of DOS, BSD, Mac, Sun, GPT partitions and disks. It also includes the Autopsy Forensic Browser as a graphical analysis tool and supports integration with SQLite database. It can be run on live Windows systems for incident response.

Q. 5 What are the tasks performed by computer forensics tools ?

Ans. : Tasks performed by computer forensics tools :

1. Acquisition
2. Validation and discrimination
3. Extraction
4. Reconstruction
5. Reporting

Q. 6 Explain types of computer forensics tools

Ans. : Types of computer forensics tools :

1. Hardware forensic tools : Range from single-purpose components to complete computer systems and servers
2. Software forensic tools : There are two types of software forensic tools. Command-line applications and GUI applications are two types. It is commonly used to copy data from a suspect's disk drive to an image file.

Q. 7 Define file carving.

Ans. : File carving is a process used in computer forensics to extract data from a disk drive or other storage device without the assistance of the file system that originality created the file. Carving looks for particular signatures or patterns that may give a clue that some interesting data can be stored in a particular spot on the disk.

Q. 8 What does a forensic tool do ? **AU : CSE, Dec.-16**

Ans. : Tools are used to analyze digital data & prove or disprove criminal activity. It is used in 2 of the 3 Phases of computer forensics

Q. 9 Label any three types of field kit to be used in crime scene. **AU : May-17**

Ans. : Three types of field kit to be used in crime scene are camera, Pen with indelible ink, Evidence tags and Evidence receipts.

Q. 10 Classify and compare hardware and software Forensic tools. **AU : May-17**

Ans. : Hardware Forensics Tools : Simple to use. Used for single purpose components and for server.

Software Forensics Tools : These tools are grouped into command-line applications and GUI applications. Some software tools are Technology Pathways Pro-Discover, X-Ways Forensics, Guidance Software EnCase, and AccessData FTK.

Q. 11 Define Master Boot Record (MBR). **AU : Dec.-17**

Ans. : On Windows and DOS computer systems, the boot disk contains a file called the Master Boot Record (MBR), which stores information about partitions on a disk and their locations, size, and other important items.

Q. 12 What is Zoned Bit Recording (ZBR)? **AU : Dec.-17**

Ans. : The method most manufacturers use to deal with a platter's inner tracks being shorter than the outer tracks. Grouping tracks by zones ensures that all tracks hold the same amount of data.

Q. 13 When you delete a image/audio/video, do you really delete it? It it possible to revert the deleted data ? **AU : May-18**

Ans. : When you a delete a file, it isn't really erased , it continues existing on your hard drive, even after you empty it from the recycle bin. This allows you and other people to recover files you've deleted. When you delete a file, Windows removes the pointer and marks the sectors containing the file's data as available. A file recovery program can scan a hard drive for these deleted files and restore them. If the file has been partially overwritten, the file recovery program can only recover part of the data.

Q. 14 What is virtual machine? **AU : May-18**

Ans. : In a pure virtual machine architecture the operating system gives each process the illusion that it is the only process on the machine. The user writes an application as if only its code were running on the system.

Q. 15 Distinguish between validation and discrimination. **AU : Dec.-18**

Ans. : Validation means ensuring the integrity of data being copied. Discrimination of data involves sorting and searching through all investigation data.

Q. 16 Define Registry.

Ans. : A database that stores hardware and software configuration information, network connections, user references, and setup information.

Q. 17 What is the use of initial response field kit?

Ans. : The initial response field kit should be a lightweight and easy to transport. With this kit, you can arrive at a scene, acquire the data you need, and return to the lab as quickly as possible.

Q. 18 Write down the task performed by computer forensics tools.

Ans. : Tasks are Acquisition, Validation and discrimination, Extraction, Reconstruction and Reporting.

➥ 2.4.2 Multiple Choice Questions with Answers

Q. 1 Linux OS stores password file in __________ directory.

(a) /etc/shodow (b) /etc/bin (c) /usr (d) /bin

Ans. : (a) /etc/shodow

Q. 2 In terms of Information security, acronym CIA stands for :

(a) confidentiality, integrity, and availability (b) computers, information, and assets

(c) confidence in applications (d) controls, integrity, and availability

Ans. : (a) confidentiality, integrity, and availability

Q. 3 The statement, "Information systems should be configured to require strong passwords," is an example of a/an :

(a) Security requirement (b) Security policy

(c) Security objective (d) Security control

Ans. : (b) Security policy

Q. 4 An information system that processes sensitive information is configured to require a valid userid and strong password from any user. This process of accepting and validating this information is known as:

(a) Authentication (b) Strong authentication

(c) Two-factor authentication (d) Single sign-on

Ans. : (a) Authentication

Q. 5 Windows NT stores passwords in two formats : __________ and __________.

(a) LM hash and NT hash (b) ASCII and binary

(c) LANMAN and NT hash (d) LM hash and LANMAN

Ans. : (a) LM hash and NT hash

Q. 6 A valid definition of digital evidence is :

(a) data stored or transmitted using a computer

(b) information of probative value

(c) digital data of probative value

(d) any digital evidence on a computer

Ans. : (c) digital data of probative value

Q. 7 Private networks can be a richer source of evidence than the Internet because :

(a) They retain data for longer periods of time.

(b) Owners of private networks are more cooperative with law enforcement.

(c) Private networks contain a higher concentration of digital evidence.

(d) All of the above.

Ans. : (c) Private Networks contain a higher concentration of digital evidence

Q. 8 In terms of digital evidence, a hard drive is an example of :

(a) Open computer systems

(b) Communication systems

(c) Embedded computer systems

(d) None of the above

Ans. : (a) Open computer system

Q. 9 In terms of digital evidence, a mobile telephone is an example of :

(a) Open computer systems (b) Communication systems

(c) Embedded computer systems (d) None of the above

Ans. : (c) Embedded computer systems

Q. 10 In terms of digital evidence, a Smart Card is an example of :

(a) Open computer systems (b) Communication systems

(c) Embedded computer systems (d) None of the above

Ans. : (c) Embedded computer systems

Q. 11 In terms of digital evidence, the Internet is an example of :

(a) Open computer systems (b) Communication systems

(c) Embedded computer systems (d) None of the above

Ans. : (b) Communication system

Q. 12 Cyber Forensic Investigation Process consists of **__________.**

(a) Imaging - Copy - Analysis - Communication.

(b) Imaging - Cloning - Documenting - Communication.

(c) Identification - Preservation - Collection - Analysis - Communication.

(d) Searching - Extracting - Imaging - Cloning - Analysis.

Ans. : (c) Identification - Preservation - Collection - Analysis - Communication

Q. 13 What happens when first securing the area?

(a) Start looking for evidence (b) Make sure that the crime scene is safe

(c) Gather evidence (d) Make sure computer is on

Ans. : (b) Make sure that the crime scene is safe

Q. 14 Phone company records are an example of :

(a) Hardware as contraband or fruits of crime

(b) Information as contraband or fruits of crime

(c) Information as an instrumentality

(d) Information as evidence

Ans. : (d) Information as evidence

Q. 15 When assessing the reliability of digital evidence, the investigator is concerned with whether the computer that generated the evidence was functioning normally, and:

(a) Whether chain of custody was maintained

(b) Whether there are indications that the actual digital evidence was tampered with

(c) Whether the evidence was properly secured in transit

(d) Whether the evidence media was compatible with forensic machines

Ans. : (b) Whether there are indications that the actual digital evidence was tampered with

Q. 16 FAT means **__________.**

(a) file allocation time (b) file allocation task

(c) file allocation table (d) file allocation technology

Ans. : (c) file allocation table

Q. 17 In Microsoft file structures, sectors are grouped to form **__________**, which are storage allocation units of one or more sectors.

(a) Partition (b) cluster (c) cylinder (d) track

Ans. : (b) cluster

Q. 18 Even if the actual data being stored requires less storage than the cluster size, an entire cluster is reserved for the file. This unused space is called the __________.

(a) slack space (b) free space

(c) unmarked space (d) bad sector

Ans. : (a) slack space

Q. 19 Windows bases recovery tools are __________.

(a) EnCase (b) FTK (c) X-Ways (d) All of these

Ans. : (d) All of these

Q. 20 Sleuth Kit and SMART 6 are used for __________ based recovery tool.

(a) MS-DOS (b) Windows (c) Linux (d) Android

Ans. : (c) Linux

Q. 21 Tasks Performed by Computer Forensics Tools are __________.

(a) Acquisition (b) Validation and discrimination

(c) Extraction (d) All of these

Ans. : (d) All of these

Q. 22 Windows operating systems use the __________ to store system configuration information and usage details.

(a) SAM (b) Registry (c) FAT (d) NFS

Ans. : (b) registry

Q. 23 What is the goal of a Denial of Service attack?

(a) Capture files from a remote system

(b) Incapacitate a system or network

(c) Exploit a weakness in the TCP/IP stack

(d) Execute a Trojan using the hidden shares

Ans. : (b) Incapacitate a system or network

❑❑❑

Notes

UNIT - III

3 Analysis and Validation

Scope of the Syllabus

Validating Forensics Data - Data Hiding Techniques - Performing Remote Acquisition - Network Forensics - Email Investigations - Cell Phone and Mobile Devices Forensics.

3.1 Validating Forensics Data

AU : May-17

- Validation involves performing laboratory tests to verify that a particular instrument, software program, or measurement technique is working properly. Confidence in forensic DNA results is gained through validation studies, which provide objective evidence that a DNA testing method is robust, reliable and reproducible.
- Validation experiments define procedural limitations, identify critical components of the procedure that require quality control and monitoring, and establish standard operating procedures and interpretation guidelines for laboratories to follow while processing samples.
- Validation is useful for achieving a number of desired outcomes. It minimizes reinvention of methods in different laboratories. Methods that have been validated are more readily accepted, more easily standardized, and can be compared internationally between different laboratories. Validation also helps to identify potential limitations specific to a method or laboratory.

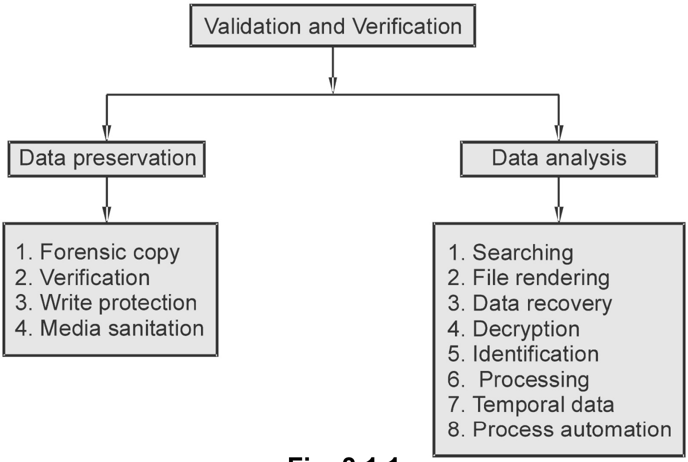


Fig. 3.1.1

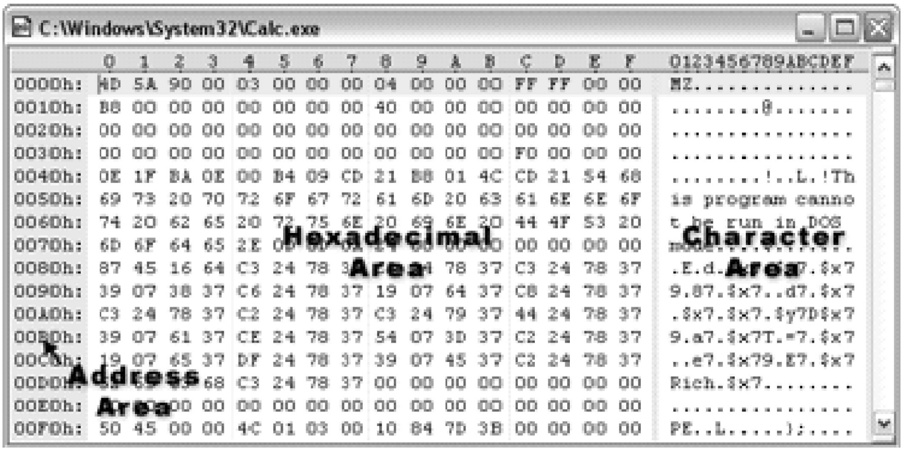
- Validation is the confirmation by examination and the provision of objective evidence that a tool, technique or procedure functions correctly and as intended.
- Verification is the confirmation of a validation with a laboratories tools, techniques and procedures.
- Validation should be distinguished from other method-assessment processes such as verification or evaluation. Verification is the process by which collaborating lines of evidence are collected in order to determine if a method is working as expected within a specific laboratory's own conditions (operators, equipment, environment).
- During verification, results from a few samples are compared with results obtained from other evidence. In the forensic field, this evidence is usually validation data, typically in the form of publications or reports that detail the performance characteristics of the standard method. The outcomes of the verification process are closely linked to the quality and reliability of the validation process. However, validation is a more intensive and rigorous process than verification.
- System validation is associated with data generation and requires the unique identification of systems, identification of system restarts, identification of changed system configuration and attributes, and validation that messages were in fact generated by the designated system.
- Application validation is similar to system validation except applied to specific applications running on a system. As with system validation, it must be verified that the application is expected to be sending the events and that the application itself matches known characteristics.
- Application restarts, the user starting the application, and application parameter settings can all be of critical importance in determining the validity of the events generated by the application.
- User validation attempts to provide validation of the users of a system.
- Algorithm implementation : Given that an algorithm itself has been validated, the implementation must be similarly validated. Errors often occur in the transcription from a theoretical algorithm to an implemented algorithm. For example, SSH uses a well-established protocol for initiation of a connection and for maintaining the security of that connection. This protocol is well validated. However, there have been well-known bugs in the implementation of the SSH protocol that have allowed it to be compromised.
- Data collection : After data is generated, a repository must collect the data. This will require ensuring that the data is not modified on the way to the repository and providing validation of temporal relationships. These needs for forensics would be insufficient in terms of security, which would also require that the data could not be read and examined in transit.
- Investigative digital forensics can be divided into several stages according to the Digital Forensic Research Workshop and its examination of digital forensic models. The different stages are :
  1. Identification : Recognizing an incident from indicators and determining its type. This is not within the field of forensics, but significant because it impacts other steps and determines if a forensic examination is needed.

2. Preparation : Preparing a plan of action by selecting tools, techniques, monitoring authorizations and management support. This also includes warrants if the evidence lies with a third party.
3. Preservation : The preservation stage tries to freeze the crime scene. It consists of stopping or preventing any activities that can damage the digital information being collected like using electromagnetic devices, stopping ongoing file deletion processes and stopping any scheduled jobs which might interfere with the evidence.
4. Collection : Collecting digital information relevant to the investigation. The evidence is duplicated in some other medium. It may involve removal of personal computers and hard disks from the crime scene, copying log files from computer devices and taking system snapshots of the devices involved.
5. Examination : Examination stage consists of in-depth systematic search of evidence relating to the suspected crime. This stage focuses on identifying and locating potential evidence, within unconventional locations, and constructing detailed documentation for analysis. The outputs of examination are data objects found in collected evidence. They may include log file time stamps matching the security camera timestamp. It is a mapping process of all the evidence collected.
6. Analysis : The aim of analysis is to draw conclusions based on the evidence found. Different types of evidence are linked during this process.
7. Presentation : Summarises and provides explanations of conclusions based on the analysis report. The technical data is translated into layman's terms using abstracted terminology. All abstracted terminology should reference the specific details.
8. Returning evidence : Ensuring physical and digital property is returned to its proper owner after the investigation. It's not a forensic step but a clean way of concluding the investigation.

- Follow these basic steps for all digital forensics investigations :
  1. For target drives, use recently wiped media that have been reformatted and inspected for viruses
  2. Inventory the hardware on the suspect's computer, and note condition of seized computer
  3. For static acquisitions, remove original drive and check the date and time values in system's CMOS
  4. Record how you acquired data from the suspect drive
  5. Process drive's contents methodically and logically
  6. List all folders and files on the image or drive
  7. Examine contents of all data files in all folders
  8. Recover file contents for all password-protected files
  9. Identify function of every executable file that doesn't match hash values

➥ 3.1.1 Validating with Hexadecimal Editors

- Advanced hexadecimal editors support many features, which is not available in computer forensics tools.
- A hex editor is a software used to view and edit binary files. A binary file is a file that contains data in machine-readable form.
- Hex editors allow editing the raw data contents of a file, instead of other programs which attempt to interpret the data for you. Since a hex editor is used to edit binary files, they are sometimes called a binary editor or a binary file editor.
- If you edit a file with a hex editor, you are said to hex edit the file, and the process of using a hex editor is called hex editing.
- A typical hex editor has three areas : An address area on the left, a hexadecimal area in the center and a character area on the right.



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00   MZ..............
0010h: B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0020h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0030h: 00 00 00 00 00 00 00 00 00 00 00 00 F0 00 00 00   ................
0040h: 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68   ........!..L.!Th
0050h: 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F   is program canno
0060h: 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20   t be run in DOS
0070h: 6D 6F 64 65 2E [illegible]          00 00 00 00   [illegible]
0080h: 87 45 16 64 C3 24 78 [illegible] 78 37 C3 24 78 37   .E.d.[illegible]7.$x7
0090h: 39 07 38 37 C6 24 78 37 19 07 64 37 C8 24 78 37   9.87.$x7..d7.$x7
00A0h: C3 24 78 37 C2 24 78 37 C3 24 79 37 44 24 78 37   .$x7.$x7.$y7D$x7
00B0h: 39 07 61 37 CE 24 78 37 54 07 3D 37 C2 24 78 37   9.a7.$x7T.=7.$x7
00C0h: 19 07 65 37 DF 24 78 37 39 07 45 37 C2 24 78 37   ..e7.$x79.E7.$x7
00D0h: [illegible] 68 C3 24 78 37 00 00 00 00 00 00 00 00   Rich.$x7........
00E0h: [illegible] 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00F0h: 50 45 00 00 4C 01 03 00 10 84 7D 3B 00 00 00 00   PE..L.....};....
```

- Data can be edited in a hex editor just like a normal text editor. A hex editor has a cursor that can be moved by clicking with the mouse or using the cursor keys.
- Position the cursor over the byte you want to edit and type the value you want to change to using the keyboard. The cursor can be switched between the hexadecimal area and the character area by pressing the 'Tab' key.
- When the cursor is in the hexadecimal area, you have to enter byte values in hexadecimal notation, but when the cursor is in the character area, you can enter regular characters just like a text editor.
- The most advanced feature of hex editors is now the ability to place a template over a file that allow you to understand what the bytes of a binary file actually mean.
- Hex workshop generates the hash value of selected data in a file or sector.

University Question

1. Discuss the procedure to validate the hexadecimal editors.	**AU : May-17, Marks 8**

3.2 Data Hiding Techniques

AU : May-17, Dec.-17

- Data hiding : Changing or manipulating a file to conceal information.
- Techniques :

  1. Hiding entire partitions
  2. Changing file extensions
  3. Setting file attributes to hidden
  4. Bit-shifting
  5. Using encryption
  6. Setting up password protection.

- Files are hiding by using operating system. One method is change the file extension. Advanced digital forensics tools check file headers and compare the file extension to verify that it's correct or not. If there's a discrepancy, the tool flags the file as a possible altered file. One more hiding technique is selecting the hidden attribute in a file's properties dialog box.
- **Marking bad clusters :** A data-hiding technique used in FAT file systems is placing sensitive or incriminating data in free or slack space on disk partition clusters. It involves using old utilities such as Norton Disk Edit. It can mark good clusters as bad clusters in the FAT table so the OS considers them unusable.
- Only way they can be accessed from the OS is by changing them to good clusters with a disk editor. Disk Edit runs only in MS-DOS and can access only FAT-formatted disk media
- **Bit-shifting :** Some users use a low-level encryption program that changes the order of binary data. It makes altered data unreadable. To secure a file, users run an assembler program to scramble bits. Run another program to restore the scrambled bits to their original order. Bit shifting changes data from readable code to data that looks like binary executable code.

3.2.1 Steganography

- **Steganography** is the art and science of communicating in a way which hides the existence of the communication. The goal of steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present
- Steganography can be used in a large amount of data formats in the digital world of today. The most popular data formats are .bmp, .doc, .gif, .jpeg, .mp3, .txt and .wav. Steganographic technologies are a very important part of the future of internet security and privacy on open systems such as internet.
- Steganography is the science of hiding information. The purpose of steganography is covert communication-to hide the existence of a message from a third party.
- Information hiding generally relates to both water-marking and steganography. A watermarking system's primary goal is to achieve a high level of robustness. It should be impossible to remove a watermark with-out degrading the data object's quality.
- Steganography is used for high security and capacity, which often entails that the hidden information is breakable.

- Fig. 3.2.1 shows a common taxonomy of steganographic techniques

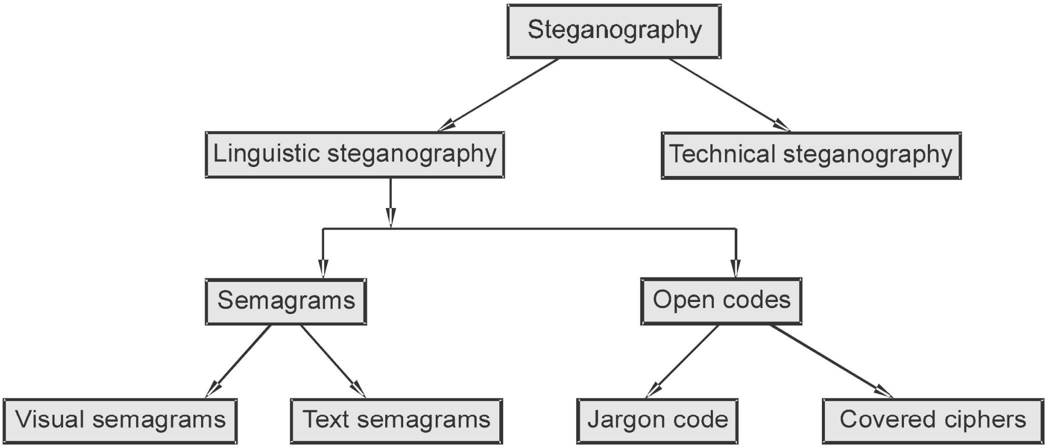


Fig. 3.2.1 : Taxonomy of steganographic techniques

- Technical steganography : it uses scientific methods to hide a message.
- Linguistic steganography : It hides the message in the carrier in some non-obvious ways and is further categorized as semagrams or open codes.
- Semagrams : It uses symbol or signs for information hiding.
- A visual semagram uses normal physical objects to convey a message.
- A text semagram hides a message by modifying the appearance of the carrier text.
- Open codes hide a message in a legitimate carrier message in ways that are not obvious to an unsuspecting observer.
- Jargon code uses language that is understood by a group of people but is meaningless to others.
- The goal of steganography is to avoid the detection or even raising the suspicion that a secret message is being passed on. Steganalysis is the art of detecting these covert messages. It involves the detection of embedded messages. The types of steganalysis attacks are similar to those of cryptanalysis attacks.

➤ Steganography tools

1. **MP3Stego :** Hide files within mp3 files. MP3Stego will hide information in MP3 files during the compression process. The data is first compressed, encrypted and then hidden in the MP3 bit stream.
2. **TextHide :** Simple text steganography
3. **wbStego :** This tool used for bitmaps, text files, HTML files and PDF files Steganography.
4. **Hide4PGP** is a freeware program distributed as source code in ANSI C and precompiled executables for DOS and the Win32 console

3.2.2 Difference between Stenography and Cryptography

Steganography	Cryptography
Output of information hiding is the stego-media.	Output in cryptography is a cipher text
It hides information	It does not hides information
Additional carrier is needed	Additional carrier is not needed
Steganography does not alter secret of message but hides inside the cover image	In cryptography, the structure of message is scrambled to make it meaningless
In steganography the secret message embeds in a harmless looking cover such as a digital image file, then the image file is transmitted.	Cryptography is the science of using mathematics to encrypt and decrypt data

University Questions

1. Briefly explain any one steganography algorithm to hide data in a image. **AU : May-17, Marks 8**
2. Explain data hiding techniques. **AU : Dec.-17, Marks 8**

3.3 Performing Remote Acquisition

- Remote forensic tools give digital investigators an alternative to the most common and readily accessible methods of volatile data and RAM acquisition. These remote forensic solutions can be used to access live systems, and include the ability to acquire and sometimes analyze memory.
- These tools include enterprise solutions from core forensic application vendors such as access data, guidance software, and technology pathways, which all have agent-style installation options that may be rolled out to most of the systems in a large network and accessed during an incident, rather than run for the first time when a digital investigator accesses the system.
- The OnlineDFS tool can acquire data from remote systems without installing an agent. Another tool that can be used to acquire volatile data and hard drive contents remotely from windows systems is F-Response. This tool does not acquire the data from the remote system, but rather provides access to memory and hard drives on a remote computer via an iSCSI connection, which digital investigators can then acquire using their tool of choice.
- Following are the three different way of determining the best acquisition method of data acquisition :
  1. Bit-stream disk-to-image file
  2. Bit-stream disk-to-disk
  3. Sparse data copy of a file or folder

- **Bit-stream copy :** Is a bit-by-bit copy of the original storage medium and is an exact duplicate of the original disc. It is different from a simple backup copy because backups can only copy files stored in a folder or are of a known file type.
- **Bit-stream image :** Is the file that contains the bit-stream copy of all the data on a disk or disk partition.

3.4 Network Forensics

AU : Dec.-16

- Network forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection. Unlike other areas of digital forensics, network investigations deal with volatile and dynamic information.
- Now a day, most of the peoples depends upon e-mail, e-commerce, m-commerce which required network support. Various networking technology is used to support this type of operation. Digital investigators at-least known the basics of computer network, working and functions of networking devices. It helps to digital investigators to solve the problem and think in all directions.
- Digital investigators understand the technology then it will enable to recognize, collect, preserve, examine, and analyze evidence related to crimes involving networks. Day by day, crime is increases by using networking technology, so digital investigators must be familiar with the networking technology.
- Investigators need the ability to identify different packet types according to various Internet Protocols. These include :

  a. Email (POP3, SMTP and IMAP)

  b. Web Mail (Yahoo Mail, Gmail, Hotmail)

  c. Instant Messaging (Windows Live Messenger, Yahoo, ICQ)

  d. FTP e. Telnet

  f. HTTP g. VOIP

- Network forensics is the process of capturing information that moves over a network and trying to make sense of it in some kind of forensics capacity. Network forensics is the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents.
- A network forensics appliance is a device that automates this process. Wireless forensics is the process of capturing information that moves over a wireless network and trying to make sense of it in some kind of forensics capacity.

➤ Network attack :

➤ 1. Denial of service

- Denial of service attacks cause the service or program to cease functioning or prevent others from making use of the service or program. These may be performed at the network layer by sending carefully crafted and malicious datagrams that cause network connections to fail.

- They may also be performed at the application layer, where carefully crafted application commands are given to a program that cause it to become extremely busy or stop functioning.
- Preventing suspicious network traffic from reaching hosts and preventing suspicious program commands and requests are the best ways of minimizing the risk of a denial of service attack.
- It is useful to know the details of the attack method, so you should educate yourself about each new attack as it gets publicized.

➤ 2. Spoofing

- This type of attack causes a host or application to mimic the actions of another. Typically the attacker pretends to be an innocent host by following IP addresses in network packets.
- For example, a well-documented exploit of the BSD rlogin service can use this method to mimic a TCP connection from another host by guessing TCP sequence numbers.
- To protect against this type of attack, verify the authenticity of datagrams and commands. Prevent datagram routing with invalid source addresses. Introduce unpredictablility into connection control mechanisms, such as TCP sequence numbers and the allocation of dynamic port addresses.

➤ 3. Eavesdropping

- This is the simplest type of attack.
- A host is configured to “listen” to and capture data not belonging to it. Carefully written eavesdropping programs can take usernames and passwords from user login network connections.
- Broadcast networks like ethernet are especially vulnerable to this type of attack.
- To protect against this type of threat, avoid use of broadcast network technologies and enforce the use of data encryption.
- IP firewalling is very useful in preventing or reducing unauthorized access, network layer denial of service, and IP spoofing attacks. It not very useful in avoiding exploitation of weaknesses in network services or programs and eavesdropping.

➤ Network Security Mechanisms

- Network security starts from authenticating any user, most likely a username and a password. Once authenticated, a stateful firewall enforces access policies such as what services are allowed to be accessed by the network users
- Though effective to prevent unauthorized access, this component fails to check potentially harmful contents such as computer worms being transmitted over the network.
- An Intrusion Prevention System (IPS) helps detect and prevent such malware. IPS also monitors for suspicious network traffic for contents, volume and anomalies to protect the network from attacks such as denial of service.
- Communication between two hosts using the network could be encrypted to maintain privacy.

- Individual events occurring on the network could be tracked for audit purposes and for a later high level analysis.
- Honeypots, essentially decoy network-accessible resources, could be deployed in a network as surveillance and early-warning tools.
- Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques.
- Such analysis could be used to further tighten security of the actual network being protected by the honeypot.
- Some tools : Firewall, Antivirus software and Internet Security Software. For authentication, use strong passwords and change it on a bi-weekly/monthly basis. When using a wireless connection, use a robust password. Network analyzer to monitor and analyze the network.

➤ **Network forensics systems can be one of two kinds :**

1. "Catch-it-as-you-can" systems, in which all packets passing through a certain traffic point are captured and written to storage with analysis being done subsequently in batch mode. This approach requires large amounts of storage, usually involving a RAID system.
2. "Stop, look and listen" systems, in which each packet is analyzed in a rudimentary way in memory and only certain information saved for future analysis. This approach requires less storage but may require a faster processor to keep up with incoming traffic.

- Network forensics is the process of collecting and analyzing raw network data and then tracking network traffic to determine how an attack took place.
- When intruders break into a network they leave a trail. Need to spot variations in network traffic; detect anomalies.
- Network forensics can usually help to determine whether network has been attacked or there is a user error.
- Examiners must establish standards procedures to carry out forensics.

➤ **Network forensics tools :**

➤ **1. NetworkMiner**

- NetworkMiner is a Network Forensic Analysis Tool (NFAT) for windows.
- NetworkMiner can be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network.
- The purpose of NetworkMiner is to collect data (such as forensic evidence) about hosts on the network rather than to collect data regarding the traffic on the network.
- The main view is host centric (information grouped per host) rather than packet centric (information showed as a list of packets/frames).

➤ Open source tools

1. Wireshark
2. Kismet
3. Snort
4. OSSEC
5. NetworkMiner is an open source Network Forensics Tool available at SourceForge.
6. Xplico is an Internet/IP Traffic Decoder (NFAT). Protocols supported: HTTP, SIP, FTP, IMAP, POP, SMTP, TCP, UDP, IPv4, IPv6

➥ 3.4.1 Open Source Tools : Wireshark

- Wireshark is the most widely used graphical application for network monitoring and analysis. It is open-source and runs on most popular computing platforms, including UNIX, Linux, and Windows. It is available for download from **http://www.wireshark.org.**
- Wireshark is initiated by Gerald Combs under the name Ethereal. First version was released in 1998. The name Wireshark was adopted in June 2006. Wireshark is a free and open source packet analyzer. Wireshark is software that "understands" the structure of different networking protocols.
- Wireshark is a network packet/protocol analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible. Wireshark is perhaps one of the best open source packet analyzers available today for **UNIX and Windows**.
- Wireshark does not support intrusion detection system. Wireshark is a GUI Network Protocol Analyzer. Wireshark software has been developed towork on Microsoft Windows, Linux, Solaris, and Mac OS X.

➤ Use of wireshark :

1. Network administrators use it to troubleshoot network problems
2. Network security engineers use it to examine security problems
3. Developers use it to debug protocol implementations
4. People use it to learn network protocol internals
5. Displays the network traffic in human-readable format.

- Use filters to capture only packets of interest to you. Wireshark uses two types of filters:

  1. ‡ Capture filters
  2. ‡ Display filters

- Capture filters : Filtered while capturing. Like TCPDump. Wireshark contains a powerful capture filter engine that helps remove unwanted packets from a packet trace and only retrieves the packets of our interest.
- ‡ Display filters let you compare the fields within a protocol against a specific value, compare fields against fields, and check the existence of specified fields or protocols. More detailed filtering. Allows to compare values in packets but not real time.

- Fig. 3.4.1 shows wireshark startup screen.

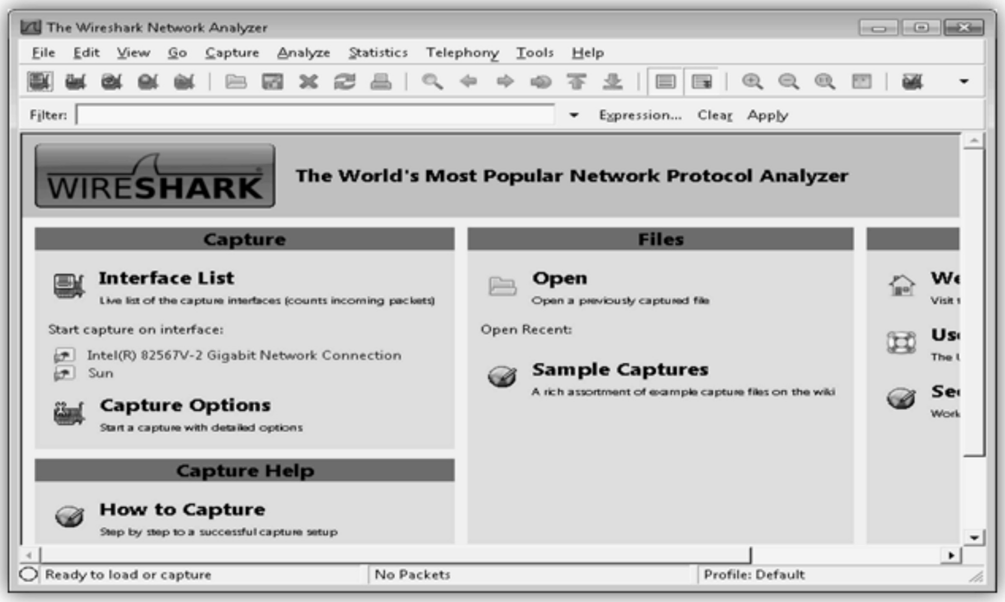
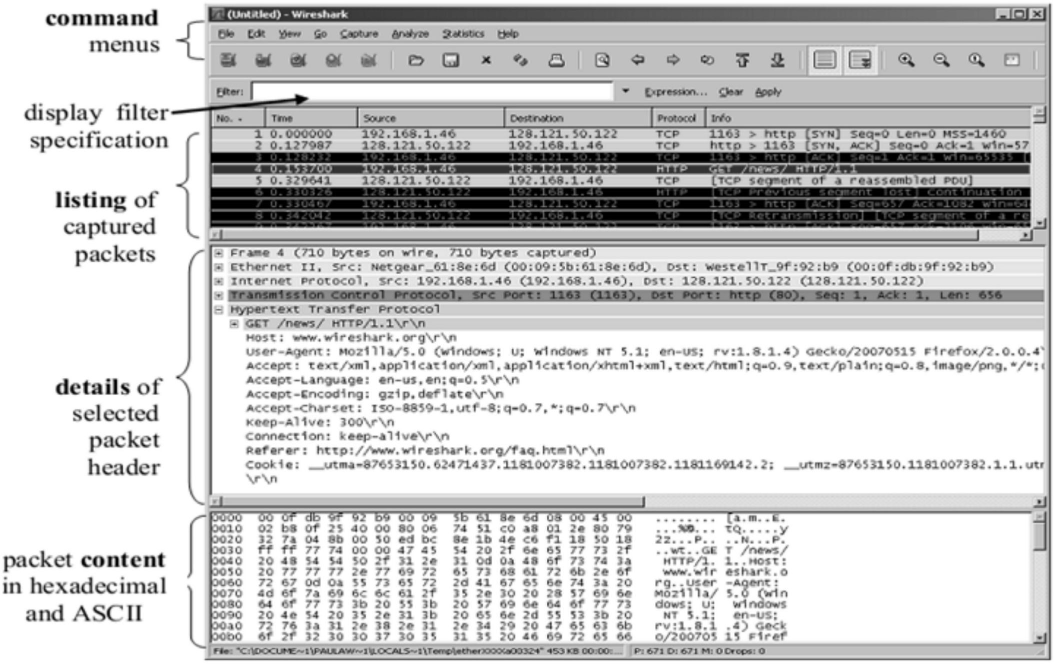

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start capture on interface:
Intel(R) 82567V-2 Gigabit Network Connection
Sun
Capture Options
Start a capture with detailed options
Capture Help
How to Capture
Step by step to a successful capture setup
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki
We
Visit t
Us
The U
Se
Work
Ready to load or capture
No Packets
Profile: Default

Fig. 3.4.1

- Fig. 3.4.2 shows Wireshark graphical user interface.


command menus
display filter specification
listing of captured packets
details of selected packet header
packet content in hexadecimal and ASCII
(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply

```
No. -  Time        Source           Destination      Protocol  Info
     1 0.000000    192.168.1.46     128.121.50.122   TCP       1163 > http [SYN] Seq=0 Len=0 MSS=1460
     2 0.127987    128.121.50.122   192.168.1.46     TCP       http > 1163 [SYN, ACK] Seq=0 Ack=1 Win=57
     3 0.128232    192.168.1.46     128.121.50.122   TCP       1163 > http [ACK] Seq=1 Ack=1 Win=65535 [
     4 0.153700    192.168.1.46     128.121.50.122   HTTP      GET /news/ HTTP/1.1
     5 0.329641    128.121.50.122   192.168.1.46     TCP       [TCP segment of a reassembled PDU]
     6 0.330326    128.121.50.122   192.168.1.46     HTTP      [TCP Previous segment lost] Continuation
     7 0.330467    192.168.1.46     128.121.50.122   TCP       1163 > http [ACK] Seq=657 Ack=1082 Win=64
     8 0.342042    128.121.50.122   192.168.1.46     TCP       [TCP Retransmission] [TCP segment of a re
```

```
⊞ Frame 4 (710 bytes on wire, 710 bytes captured)
⊞ Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: WestellT_9f:92:b9 (00:0f:db:9f:92:b9)
⊞ Internet Protocol, Src: 192.168.1.46 (192.168.1.46), Dst: 128.121.50.122 (128.121.50.122)
⊞ Transmission Control Protocol, Src Port: 1163 (1163), Dst Port: http (80), Seq: 1, Ack: 1, Len: 656
⊟ Hypertext Transfer Protocol
  ⊞ GET /news/ HTTP/1.1\r\n
    Host: www.wireshark.org\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.4) Gecko/20070515 Firefox/2.0.0.4
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Referer: http://www.wireshark.org/faq.html\r\n
    Cookie: __utma=87653150.62471437.1181007382.1181007382.1181169142.2; __utmz=87653150.1181007382.1.1.utr
    \r\n
```

```
0000  00 0f db 9f 92 b9 00 09  5b 61 8e 6d 08 00 45 00   ........ [a.m..E.
0010  02 b8 0f 25 40 00 80 06  74 51 c0 a8 01 2e 80 79   ...%@... tQ.....y
0020  32 7a 04 8b 00 50 ed bc  8e 1b 4e c6 f1 18 50 18   2z...P.. ..N...P.
0030  ff ff 77 74 00 00 47 45  54 20 2f 6e 65 77 73 2f   ..wt..GE T /news/
0040  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1..Host:
0050  20 77 77 77 2e 77 69 72  65 73 68 61 72 6b 2e 6f    www.wir eshark.o
0060  72 67 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   rg..User -Agent: 
0070  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 57 69 6e   Mozilla/ 5.0 (Win
0080  64 6f 77 73 3b 20 55 3b  20 57 69 6e 64 6f 77 73   dows; U;  Windows
0090  20 4e 54 20 35 2e 31 3b  20 65 6e 2d 55 53 3b 20    NT 5.1;  en-US; 
00a0  72 76 3a 31 2e 38 2e 31  2e 34 29 20 47 65 63 6b   rv:1.8.1 .4) Geck
00b0  6f 2f 32 30 30 37 30 35  31 35 20 46 69 72 65 66   o/200705 15 Firef
```

File: "C:\DOCUME~1\PAULAW~1\LOCALS~1\Temp\etherXXXXa00324" 453 KB 00:00:... P: 671 D: 671 M: 0 Drops: 0

Fig. 3.4.2

➤ Example :

1. Capture only UDP packets with destination port 53 (DNS requests) : “udp dstport 53”
2. Capture only UDP packets with source port 53 (DNS replies) : “udp srcport 53”
3. Capture only UDP packets with source or destination port 53 (DNS requests and replies) : udpport 53

➤ Comparison operators

- ‡ Fields can also be compared against values. The comparison operators can be expressed either through English like abbreviations or through C-like symbols.

Symbol	Meaning
==	Equal (eq)
!=	Not equal (ne)
>	Greater than (gt)
<	Less than (lt)
>=	Greater than or equal to (ge)
<=	Less than or equal to (le)
( )	Grouping

➤ Logical expressions

- Tests can be combined using logical expressions. These too are expressible in C-like syntax or with English like abbreviations :

Symbol	Meaning
&&	Logical AND
||	Logical OR
!	Logical NOT

➥ 3.4.2 Snort

- Snort is an open source Network Intrusion Detection System (NIDS) which is available free of cost. NIDS is the type of Intrusion Detection System (IDS) that is used for scanning data flowing on the network. Snort is a tool for small, lightly utilized networks. Fig. 3.4.3 shows location of snort.
- Intrusion detection is a set of techniques and methods that are used to detect suspicious activity both at the network and host level. Intrusion Detection System is software, hardware or combination of both used to detect intruder activity.
- A lightweight intrusion detection system can easily be deployed on most any node of a network, with minimal disruption to operations. Snort is a libpcap based packet sniffer and logger that can be used as a lightweight network intrusion detection system.

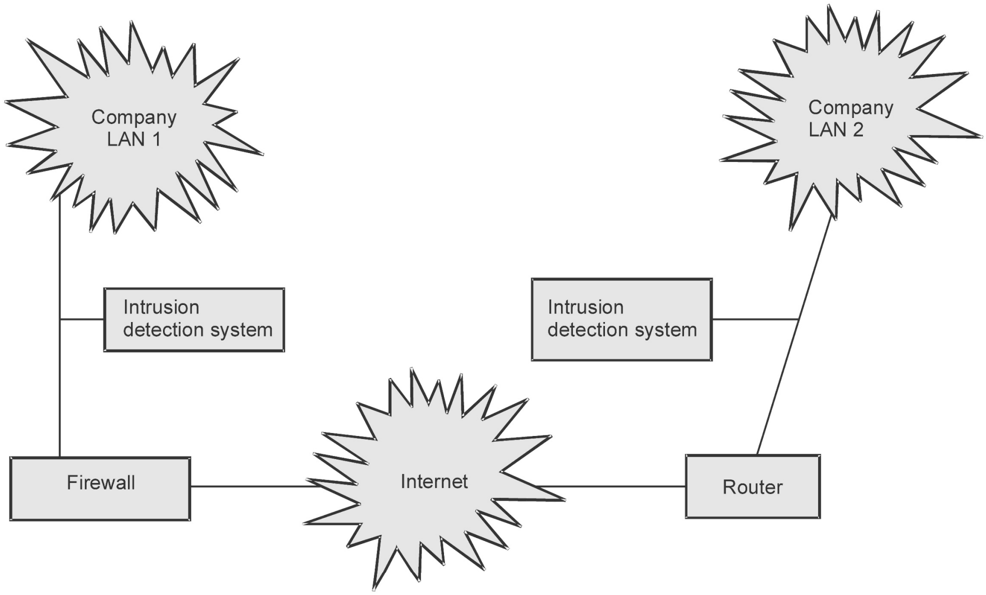


Fig. 3.4.3 : Location of the snort

- Snort uses rules stored in text files. Text editor can use for modifying the rules. Rules are grouped in categories. Separate file is maintained for each group. The "snort.conf " is the main configuration file and all group files are included in this file. At startup time, snort reads these rules and builds data structure.

➤ Components of snort

- A snort IDS contains the following components :

  1. Packet decoder 2. Preprocessors 3. Detection engine
  4. Logging and alerting system 5. Output modules

- **Packet decoder :** It takes packets from different types of network interfaces like Ethernet, SLIP,PPP and prepare for processing. Packets are passed into the packet decoder. Translates specific protocol elements into an internal data structure.
- **Preprocessor :** Preprocessors are components that can be used with snort to arrange or modify data packets before the detection engine does some operation to find out if the packet is being used by an intruder. They are also used to prepare data for detection engine; detect anomalies in packet headers; packet defragmentation; decode HTTP URI and reassemble TCP streams.
- **Detection engine :** The most important part, applies rules to packets. The detection engine performs simple tests on a single aspect of each packet to detect intrusions.
- Fig. 3.4.4 shows snort components.
- **Logging and alerting system :** It generates alert and log messages depending upon what the detection engine finds inside a packet. Logs are kept in simple text files and tcpdump-style files. Log files are stored under /var/log/snort folder by default.

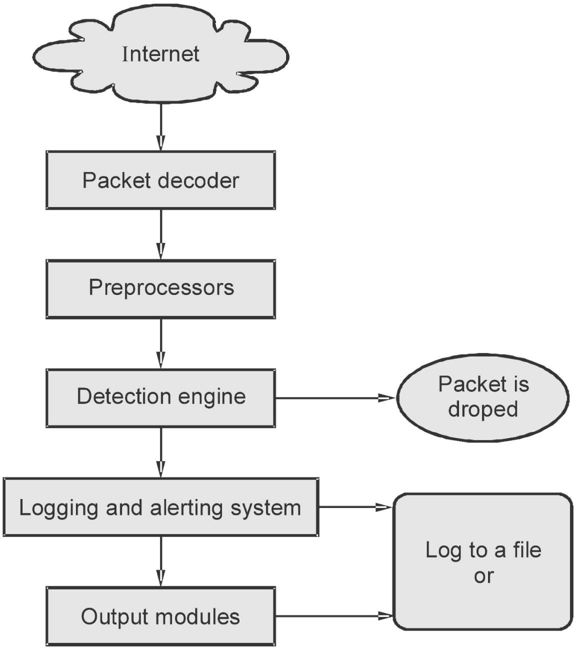


Fig. 3.4.4 : Snort components

- **Output modules :** It process alerts and logs and generate final output. Depending on the configuration, output modules can take following actions :
  a. Simply logging to /var/log/snort/alerts file
  b. Sending SNMP traps c. Sending messages to syslog facility
  d. Logging to a database like MySQL or Oracle.
  e. Generating XML output
  f. Modifying configuration on routers and firewalls

University Question

1. Discuss about network forensics. **AU : Dec.-16, Marks 16**

3.5 Email Investigations **AU : May-17, 18, Dec.-17**

- Email is used in criminal acts, but also in inappropriate actions, such as threats and frauds (phishing). While in principle email is hard to connect to an individual, in practice, email can be traced and connected to the perpetrator.
- Over a period of year's e-mail protocols have been secured through several security extensions and producers, however, cybercriminals continue to misuse it for illegitimate purposes by sending spam, phishing e-mails, distributing child pornography, and hate e-mails besides propagating viruses, worms, hoaxes and trojan horses.
- E-mail forensic analysis is used to study the source and content of e-mail message as evidence, identifying the actual sender, recipient and date and time it was sent, etc. to collect credible evidence to bring criminals to justice.

- For networks, a port means an endpoint to a logical connection. The port number identifies what type (application/service offered) of port it is. The commonly used default port numbers used in e-mail are shown below :

Protocol	Port number
SMTP	25
HTTP	80
POP3	110
IMAP	143
HTTPS	443
SMTPS	465
MSA	587
IMAPS	993
POP3S SPOP	995
MSA	587

- Identities used in e-mail are globally unique and are: mailbox, domain name, message-ID and ENVID. Mailboxes are conceptual entities identified by e-mail address and receive mail.
- E-mail forensics refers to the study of source and content of e-mail as evidence to identify the actual sender and recipient of a message, data/time of transmission, detailed record of e-mail transaction, intent of the sender, etc
- A forensic investigation of e-mail can examine both email header and body. An investigation should have the following :
  1. Examining sender's e-mail address
  2. Examining message initiation protocol (HTTP, SMTP)
  3. Examining message ID
  4. Examining sender's IP address

➤ Email headers

- When investigating email, we usually start with the piece of email itself and analyze the headers of the email. Since each SMTP server that handles a message adds lines on top of the header.
- Meta data in the e-mail message in the form of control information i.e. envelope and headers including headers in the message body contain information about the sender and/or the path along which the message has traversed.
- Inconsistencies between the data that subsequent SMTP servers supposedly created can prove that the email in question is faked. Another investigation is that of the header contents itself.
- If a message does not have these, then it is faked. If possible, one can obtain another email following supposedly the same path as the email under investigation and see whether these ideosyncratic lines have changed. While it is possible that the administrator of an SMTP node changed the behavior or even the routing, these changes tend to be far and in between.

- In email server investigation, copies of delivered e-mails and server logs are investigated to identify source of an e-mail message. E-mails purged from the clients (senders or receivers) whose recovery is impossible may be requested from servers (Proxy or ISP) as most of them store a copy of all e-mails after their deliveries
- Some other aspects that controls forensics step include the following properties :
  1. **Storage format of email :** Server side storage format may include maildir, mbox format. Server-side stores email in SQL Server databases. Reading different types of formats can be done for forensics analysis by using notepad editor and applying regular expression-based searches. At the client-side, an email is stored as mbox format. Client side may also store emails as .PST (MSOutlook), and NSF (Lotus Notes) files.
  2. **Availability of backup copy of email :** When checking from the serve side, all copies are transferred to the client. This requires seizing the client computer. For webmail, copies are always saved at the server side.
  3. **Protocol used to transport email :** Email can be initiated and transported based on SMTP or HTTP depending on the email server applications.

➤ **E-Mail forensic tools :**

1. **eMailTrackerPro** analyses the headers of an e-mail to detect the IP address of the machine that sent the message so that the sender can be tracked down. It can trace multiple e-mails at the same time and easily keep track of them.
2. **EmailTracer** is an Indian effort in cyber forensics by the Resource Centre for Cyber Forensics (RCCF) which is a premier centre for cyber forensics in India. It develops cyber forensic tools based on the requirements of law enforcement agencies.
3. **Adcomplain** is a tool for reporting inappropriate commercial e-mail and usenet postings, as well as chain letters and “make money fast” postings.

➥ 3.5.1 Checking UNIX E-mail Server Logs

- Log file provides useful information for investigation. After sending the mail, it creates number of files on the server to track and maintain the email service.
- The “/etc/sendmail.cf” is the file for configuration information for send mail. The “/etc/syslog.conf” file specifies how and which events send mail logs.
- Communication between SMTP and POP3 is maintained in /var/log/maillog file. It also record IP address and time stamp.
- Email evidence is in the email itself (header). ? Email evidence is left behind as the email travels from sender to recipient.
- Reviewing e-mail headers can offer clues to true origins of the mail and the program used to send it.
- Received is the most essential field of the email header : It creates a list of all the email servers through which the message traveled in order to reach the receiver.
- The best way to read are from bottom to top.
  1. The bottom “Received” shows the IP address of the sender's mail server.
  2. The top “Received” shows the IP address of receiver mail server.

3. The middle "Received" shows the IP address of the mail server through which email passes from sender to receiver.

- The syslog.conf file simply specifies where to save different types of e-mail log files. The first log file it configures is /var/log/maillog, which usually contains a record of simple mail transfer protocol communication between servers.
- UNIX systems are set to store log files in the /var/log directory.

➥ 3.5.2 Microsoft E-mail Server Log

- Microsoft e-mail server software is exchange server. It uses database and based on the Microsoft Extensible Storage Engine.
- Microsoft Extensible Storage Engine (ESE) uses different files in various combinations for providing E-mail service. For investigation two database files are helpful. They are ".edb " and ".stm " files.
- Checkpoint and temporary files also helpful for investigation. The .edb file contains many tables that hold metadata for all e-mail messages and other items in the exchange store.
- The .stm file stores native Internet content. Because Internet content is written in native format, there is no need to convert messages and other items to exchange format.
- An .edb file is responsible for messages formatted with Messaging Application Programming Interface (MAPI), a Microsoft system that enables different e-mail applications to work together.
- The .edb and .stm files function as a pair, and the database signature is stored as a header in both files. The internal schema for the .stm pages is stored in the .edb file.

➥ 3.5.3 E-mail Forensic Tools : MailXaminer

- MailXaminer is a tool-kit having multiple functionalities out of which powerful search mechanism is the best feature without any limitation. With this email search software, users can scan, view, search, investigate, analyze, smart review and generate a report of emails in a very less amount of time.

  1) Input file in disk required : This indicates the presence of email file at the local disk. MailXaminer requires input file to be present in the disk.
  2) Search option : This feature indicates how to perform search of interesting words in the content of an email. MailXaminer can perform plain text-based search.
  3) Information provided : This feature indicates the information extracted and shown as part of forensic analysis. The MailXaminer tool shows the message, date and time details of an email.
  4) Recovery capability : A forensic tools should have the capability to recover corrupted email or deleted email to be useful for investigation. The MailXaminer can recover corrupted email. It also has the capability to import corrupted contacts, calendar.
  5) Email format supported : This feature indicates the file type supported by a tool. The MailXaminer supports Gmail, yahoo, Hotmail, IMAP, Mozilla Thunderbird, Lotus Notes, Outlook, Exchange, Mac Outlook email format.

6) Visualization format supported : A forensic tool should allow investigator different types of display of the extracted information to enable more intelligence gathering. MailXaminer supports different view options.
7) OS Supported : Ideally, a forensic tool should support different types of operating systems to make it useful for email applications running on different platforms. The MailXaminer can run on Windows
8) Export format : A forensic tools should have friendly format for saving the examination results for compatible analysis with other forensic tools.
9) Extended device support : This feature indicates if a tool can act on plug-ins devices such as added hard disk or USB memory stick, etc.

University Questions

1. Examine and list the procedure to analyze the UNIX and Microsoft e-mail server logs. **AU : May-17, Marks 16**
2. Explain the process of investing e-mail crimes and violation. **AU : May-18, Marks 16**
3. Describe in detail about specialized E - mail forensic tools. **AU : Dec.-17, Marks 8**
4. Elaborate about mobile device forensics. **AU : Dec.-17, Marks 8**
5. List out the steps involved in eximining in Microsoft e-mail server logs. **AU : Dec.-17, Marks 8**

3.6 Cell Phone and Mobile Devices Forensics **AU : Dec.-16, May-18**

- Mobile devices are an evolving form of computing, used widely for personal and organizational purposes. These compact devices are useful in managing information, such as contact details and appointments, corresponding electronically, and conveying electronic documents.
- Over time, they accumulate a sizeable amount of information about the owner. When involved in crimes or other incidents, proper tools and techniques are needed to recover evidence from such devices and their associated media.
- Mobile device forensics is the science of recovering digital evidence from a mobile device under forensically sound conditions using accepted methods. Mobile device forensics is an evolving specialty in the field of digital forensics.
- Different mobile devices have different technical and physical characteristics (e.g., size, weight, processor speed, memory capacity). Mobile devices may also use different types of expansion capabilities to provide additional functionality. Furthermore, mobile device capabilities sometimes include those of other devices such as handheld Global Positioning Systems (GPS), cameras (still and video) or personal computers.
- People store a lot of information on cell phones. But people do not think about securing their cell phones. Data stored on mobile phones are as follows :

1. lncoming, outgoing and missed calls
2. SMS
3. E-mail
4. lnstant-messaging logs

5. Web pages
6. Pictures
7. Personal calendars
8. Address books
9. Music files
10. Voice recordings.

- Mobile phone consists of hardware components. It includes microprocessor, ROM, RAM, a digital signal processor, a radio module , a microphone and speaker, hardware interfaces, and display.
- Most basic phones have a proprietary OS and smart phone have Android and other OS.
- Phones store system data in Electronically Erasable Programmable Read-Only Memory (EEPROM). It enables service providers to reprogram phones without having to physically access memory chips. OS is stored in ROM
- The personal nature of the information on these devices can provide digital investigators with valuable insights into the model operator of suspects and activities of victims. Windows mobile uses a variation of the FAT file system called the Transaction safe FAT (TFAT) file system, which has sorne recovery features in the event of a sudden device shutdown.
- The forensic acquisition tools that are available to most forensic analysts do not have direct access to flash memory on Windows Mobile devices and are limited to acquiring data through a hardware abstraction layer.
- Mobile devices contain non- volatile and volatile memory. Volatile memory (i.e., RAM) is used for dynamic storage and its contents are lost when power is drained from the mobile device. Non- volatile memory is persistent as its contents are not affected by loss of power or overwriting data upon reboot. For example, Solid- State Drives (SSD) that stores persistent data on solid- state flash memory.
- Mobile devices typically contain one or two different types of non- volatile flash memory. These types are NAND and NOR. NOR flash has faster read times, slower write times than NAND and is nearly immune to corruption and bad blocks while allowing random access to any memory location. NAND flash offers higher memory storage capacities, is less stable and only allows sequential access.
- NAND flash memory contains : PIM data, graphics, audio, video, and other user files. This type of memory generally provides the examiner with the most useful information in most cases. NAND flash memory may leave multiple copies of transaction- based files (e.g., databases and logs) due to wear leveling algorithms and garbage collection routines.
- Since NAND flash memory cells can be re-used for only a limited amount of time before they become unreliable, wear leveling algorithms are used to increase the life span of Flash memory storage, by arranging data so that erasures and re-writes are distributed evenly across the SSD.

➤ SIM card

- Identity modules are synonymous with mobile devices that interoperate with GSM cellular networks. Under the GSM framework, a mobile device is referred to as a mobile station and is partitioned into two distinct components: the Universal Integrated Circuit Card (UICC) and the Mobile Equipment (ME).

- A UICC, commonly referred to as an identity module (e.g., Subscriber Identity Module [SIM], Universal Subscriber Identity Module [USIM], CDMA Subscriber Identity Module [CSIM]), is a removable component that contains essential information about the subscriber.
- The ME and the radio handset portion cannot fully function without a UICC. The UICC's main purpose entails authenticating the user of the mobile device to the network providing access to subscribed services. The UICC also offers storage for personal information, such as phonebook entries, text messages, Last Numbers Dialed (LND) and service- related information.
- Fig. 3.6.1 shows SIM card.

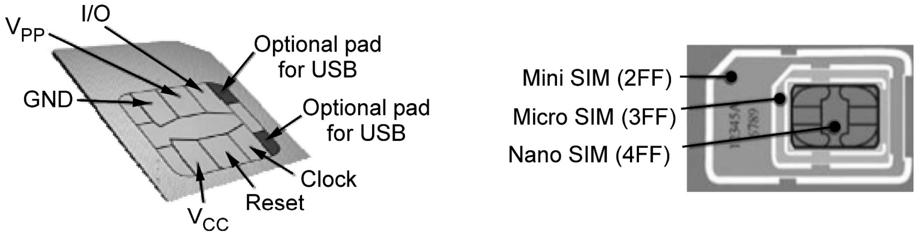


Fig. 3.6.1 : SIM

- SlM stores following types of information :
  1. SIM stores the International Mobile Subscriber Identity (IMSI), which is a unique identifier for each subscriber in the system.
  2. Subscribers can maintain a list of the numbers they call or they are called from more frequently.
  3. Information about SMS traffic.
  4. Information about subscriber's location : The SIM stores the last area where the subscriber has been registered by the system.
  5. Information about calls : The last numbers dialed are stored in a file in the SIM filesystem.
  6. Information about the provider : It is possible to extract the provider name and the mobile network commonly used for communications, along with mobile networks that are forbidden to the subscriber.
  7. Information about the system : Every SIM card has a unique ID stored in it

3.6.1 Mobile Virtual Network Operator (MVNO)

- An MVNO does not own spectrum, it leases it from a network operator with whom it has a relationship. An MVNO supplies the SIM card and has full control over its subscribers and handles its own billing.
- An MVNO buys network capacity, usually as close to the base level as possible and invests in a service infrastructure of its own.

- The MVNO thereby establishes a more independent position and is able to compete directly with other mobile network operators in the market by offering advanced services.
- MVNOs typically offer prepaid wireless plans on a subscription basis. Sales and customer service may be handled directly by the MVNO or by yet another entity called a Mobile Virtual Network Enabler (MVNE). MVNEs specialize in marketing and administering mobile services.
- An MVNO usually offers not only voice services but also value-added services or sometimes referred as mobile value-added services, which are a combination of voice, data, graphics and video information. Examples include mobile music, mobile TV, games, ring tones, multimedia messaging, mobile commerce and location-based services.
- There are different kinds of MVNOs :
  1. Classic service provider : Resellers merely resell subscription to end users. In most cases, resellers are completely dependent on MNOs for every aspect of service provision, billing and customer care. MVNOs that operate as resellers are likely to require an ASP license.
  2. ESP (Enhanced Service Provider) : Procures their own SIM cards and controls a few network elements. So, enhanced service providers are those who do not own or provide network facilities but have the ability to secure its own numbering range, operate its own HLR and offer its own SIM cards with its own mobile network code. They are dependent on MNOs for network facilities, as well access to radio network.
  3. Full MVNO : Owns everything (including HLR) except the radio network equipments. A full MVNO is one that owns or provides network facilities and network services such as towers, mobile switching centers, home location registers ("HLR") and cellular mobile services.

➤ 1. Types of evidence on mobile devices

- Two types of evidence can be retrieved from mobile :
  1. Electronic evidence
  2. Retained data evidence.
- Electronic evidence includes the user's call history, contacts/phone book, calendar information, and information stored on the SIM card.
- Retained data evidence is telecom records involving the detail of calls made and received and the geographical location of the mobile phone when a call took place.
- The address book, call history and text messages are the three main components for digital evidence.
  1. **Address book :** It contains contact information. Digital investigator will reach to suspect to a victim using information from address book. It can provide a cross-reference between real names and nicknames.
  2. **Call history :** It maintains the last call sent, last call receiver with time and date. It also gives the time taken to speak with other person.

3. **Text messages :** Texts are one of the most common forms of electronic evidence. Texts offer concrete and direct information in contrast to the call history and address book that only offer indirect and inferential information. These contain the actual words written by the owner or intended for the owner.

➥ 3.6.2 Evidence Extraction Process

- Mobile phone evidence extraction process is as follows :

1. **Intake :** The evidence intake phase generally entails request forms and intake paperwork to document chain of custody, ownership information and the type of incident the phone was involved in.
2. **Identification :** For every examination, the examiner should identify the legal authority to examine the phone, goals of the examination, make, model and identifying information for the cellular phone.
3. **Preparation :** The preparation phase involves specific research the regarding the particular phone to be examined, the appropriate tools to be used during the examination and preparation of the examination machine to ensure that all of the necessary equipment, cables, software and drivers are in place for the examination.
4. **Isolation :** Isolation of the phone prevents the addition of new data to the phone through incoming calls and text messages as well as the potential destruction of data through a kill signal or accidental overwriting of existing data as new calls and text messages come in.
5. **Processing :** SIM cards should be processed separately from the cellular phone they are installed in to preserve the integrity of the data contained on the SIM card.
6. **Verification :** The examiner could extract the file system of the cell phone initially, perform the examination and then extract the file system of the phone a second time.
7. **Documentation/reporting :** Documentation should include information such as :

   a. The date and time the examination was started.

   b. The physical condition of the phone.

   c. Pictures of the phone and individual components.

   d. Status of the phone when received.

   e. Make, model, and identifying information.
8. **Presentation :** The investigator may also want to provide reference information regarding the source of date and time information, EXIF data extracted from images or other data formats, in order that recipients of the data are better able to understand the information.

➥ 3.6.3 Challenges in Mobile Device Forensics

1. **Data volatility :** It may be necessary to keep a seized device powered up until the analysis is complete in order to prevent loss of important data that may be changed or overwritten when the power shuts off or the device is rebooted.

2. **Data Preservation :** For a mobile phone investigation, it is important to prevent the device from receiving any further data or voice communication. As text messages are stored in a “First In, First Out” order, any new incoming text messages could delete older stored text messages. Likewise, incoming calls could erase call history logs, and some devices can be wiped of all data remotely if not protected from incoming communications.
3. **Operating Systems and Communication Protocols :** Another challenge impeding the development of forensics tools is the various operating systems used on mobile phones. Mobile phones have evolved into full-fledged computing platforms requiring vendors to use sophisticated operating systems so that various software applications can be run on them.
4. **Security Mechanisms :** There are several security mechanisms used on mobile phones to protect data. The handset lock is normally activated upon power-up, which presents a problem for examiners who must attempt to investigate a phone that was found or seized in a powered off state.
5. **Unique Data Formats :** Textual information such as telephone numbers, address books, email messages, and text messages are stored using proprietary file formats. Makers of forensic software tools will need to be aware of these formats so they can write software that will convert these files to information easily understood by humans. An exception to these proprietary file formats is for image and video files which are typically stored in common JPG and MPEG formats.

➥ 3.6.4 Understanding Acquisition Procedures for Cell Phones and Mobile Devices

- Mobile device forensic acquisition can be performed using multiple methods. The main concerns with mobile devices are loss of power and synchronization with PCs.
- Acquisition should occur at a forensics laboratory once the seized equipment has arrived and been checked in. The forensic examination begins with the identification of the device.
- The type of device, its operating system, and other characteristics determine the route to take in creating a forensic copy of the contents of the device
- All mobile devices have volatile memory. Making sure they don't lose power before you can retrieve RAM data is critical.
- Mobile device attached to a PC via a cable or cradle/docking station should be disconnected from the PC immediately
- Depending on the warrant or subpoena, the time of seizure might be relevant.
- Messages might be received on the mobile device after seizure. Isolate the device from incoming signals with one of the following options :
  1. Place the device in a paint can
  2. Use the Paraben Wireless StrongHold Bag
  3. Use eight layers of antistatic bags to block the signal
- The drawback to using these isolating options is that the mobile device is put into roaming mode, which accelerates battery drainage.

- Check these areas in the forensics lab : Internal memory, SIM card, removable or external memory cards and system server.
- Checking system servers requires a search warrant or subpoena. The SIM card file system is a hierarchical structure .
  1. Information that can be retrieved:
  2. Service-related data, such as identifiers for the SIM card and the subscriber
  3. Call data, such as numbers dialed
  4. Message information
  5. Location information
- If power has been lost, PINs or other access codes might be required to view files
- To acquire data from a phone, a connection must be established to the device from the forensic workstation. Before performing an acquisition, the version of the tool being used should be documented, along with any applicable patches or errata from the manufacturer applied to the tool.
- Caution should be taken to avoid altering the state of a mobile phone when handling it, for example, by pressing keys that could potentially corrupt or erase evidence.
- Once the connection has been established, the forensic software suite can proceed to acquire data from the device.
- Acquiring a device's contents logically, the prevailing technique used by present day forensic tools, requires the device to be switched on.
- The goal during acquisition is to affect memory contents as little as possible and then only with the knowledge of what is occurring internally, relying more on adherence to the second and third evidentiary principles that respectively emphasize high competence of the specialist and the capture of a detailed audit trail of the actions taken.
- The date and time maintained on the mobile phone is an important piece of information. The date and time may be obtained from the network or manually set by the user.
- Suspects may manually set the day or time to a completely different value from the actual one to leave misleading values in the call and message records found on the phone.
- If the phone was on when seized, the date and time maintained and differences from a reference clock should have already been recorded, as mentioned earlier. Nevertheless, confirmation at acquisition may prove useful.
- If the phone was off when seized, the date and time maintained and differences from a reference clock should be recorded immediately when first turned on in the laboratory.
- Note that actions taken during acquisition, such as removal of the battery to view the device label, may affect the time value maintained.
- Unlike desktop machines or network servers, only a few phones have a hard disk and rely instead completely on semiconductor memory.
- Specialized software exists for performing a logical acquisition of PIM data and, for certain phones, producing a physical image. However, the contents of a phone are typically dynamic and continually changing.

- Two back-to-back acquisitions of a device using the same tool may produce different results overall, though the majority of information, such as PIM data, remains unchanged.
- Increasingly, mobile phones come with a built-in slot for some family of memory cards.
- Forensic tools that acquire the contents of a resident memory card normally perform a logical acquisition.
- To recover deleted data that might reside on the memory card, a direct acquisition can be performed on it after the contents of the mobile phone have been successfully acquired.
- With either type of acquisition, the forensic tool may or may not have the capability to decode recovered phone data stored on the card, requiring additional manual steps to be taken.
- After an acquisition is finished, the forensic specialist should always confirm that the contents of a device were captured correctly.
- **On occasion**, a tool may fail its task without any error notification and require the specialist to reattempt acquisition with the same tool or another tool.
- Similarly, some tools do not work as well with certain devices as others do, and may fail with an error notification. Thus, where possible, it is advisable to have multiple tools available and be prepared to switch to another if difficulties occur with the initial tool.

University Questions

1. Appraise the acquisition procedures for cell phones and mobile devices. **AU : May-18, Marks 16**
2. Describe cell phone device forensics. **AU : Dec.-16, Marks 16**

3.7 Questions with answers

3.7.1 Two Marks Questions with Answers

Q. 1 What is validation and verification ?

Ans. : Validation is the confirmation by examination and the provision of objective evidence that a tool, technique or procedure functions correctly and as intended. Verification is the confirmation of a validation with a laboratories tools, techniques and procedures.

Q. 2 What is system validation ?

Ans. : System validation is associated with data generation and requires the unique identification of systems, identification of system restarts, identification of changed system configuration and attributes, and validation that messages were in fact generated by the designated system.

Q. 3 List the validation techniques.

Ans. : Validation techniques are hiding entire partitions, changing file extensions, setting file attributes to hidden, bit-shifting, encryption and setting up password protection.

Q. 4 What is mobile device forensic ?

Ans. : Mobile device forensics is the science of recovering digital evidence from a mobile device under forensically sound conditions using accepted methods. Mobile device forensics is an evolving specialty in the field of digital forensics

Q. 5 Define snort.

Ans. : Snort is an open source Network Intrusion Detection System (NIDS) which is available free of cost. NIDS is the type of Intrusion Detection System (IDS) that is used for scanning data flowing on the network. Snort is a tool for small, lightly utilized networks.

Q. 6 Define network forensics.

Ans. : Network forensics is the process of capturing information that moves over a network and trying to make sense of it in some kind of forensics capacity. Network forensics is the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents

Q. 7 What is steganography ? **AU : May-18**

Ans. : Steganography is the art and science of communicating in a way which hides the existence of the communication. The goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present.

Q. 8 What is bit stream copy ?

Ans. : Bit-stream copy is a bit-by-bit copy of the original storage medium and is an exact duplicate of the original disc. It is different from a simple backup copy because backups can only copy files stored in a folder or are of a known file type.

Q. 9 What is bit stream image ?

Ans. : Bit-stream image is the file that contains the bit-stream copy of all the data on a disk or disk partition

Q. 10 Explain difference between steganography and cryptography.

Ans. :

Steganography	Cryptography
Output of information hiding is the stego-media.	Output in cryptography is a cipher text
It hides information	It does not hides information
Additional carrier is needed	Additional carrier is not needed
Steganography does not alter secret of message but hides inside the cover image	In cryptography, the structure of message is scrambled to make it meaningless

Q. 11 What is a MVNO ? **AU : CSE, Dec.-16**

Ans. : A Mobile Virtual Network Operator (MVNO) is a company that provides mobile phone services but does not have its own licensed frequency allocation of radio spectrum, nor does it necessarily have all of the infrastructure required to provide mobile telephone service.

Q. 12 What is the purpose of PUK ? **AU : CSE, Dec.-16**

Ans. : Personal Unblocking Key (PUK) code (8 digits) is required to change a blocked PIN code. The PUKs are fixed and cannot be changed. Since the PUK is fixed, the network operator usually keeps track of the PUKs for all of its users.

Q. 13 Name any three standard procedures used in network forensics. **AU : May-17**

Ans. : Three standard procedure are :

a. Always use a standard installation image for systems on a network.

b. Attempt to retrieve all volatile data, such as RAM and running processes, by doing a live acquisition before turning the system off.

c. Compare files on the forensic image to the original installation image.

Q. 14 Decide the roles of client and servers in e-mail investigations. **AU : May-17**

Ans. : Role of client is find and copy any potential evidence. Client also runs programs as Microsoft outlook and Novell evolution. E-mail servers run program such as exchange, groupwise or sendmail. Server keep log of sendmail.

Q. 15 Describe bit shifting with an example. **AU : Dec.-17**

Ans. : Bit-shifting changes data from readable code to data that looks like binary executable code. Technique for hiding data is shifting bit patterns to alter the byte values of data.

Q. 16 Mention the e-mail storage format available in novell evolution. **AU : Dec.-17**

Ans. : Mbox is used for storing e-mail messages in a flat plaintext file. Multipurpose Internet Mail Extensions (MIME)A specification for formatting non-ASCII messages, such as graphics, audio and video, for transmission over the Internet.

Q. 17 Give examples for email forensics tools. **AU : May-18**

Ans. : Examples of email forensics tools are eMailTrackerPro, EmailTracer, Aid4Mail Forensic, Adcomplain and AbusePipe.

Q. 18 Define Order of Volatility (OOV). **AU : Dec.- 18**

Ans. : The order of volatility is the sequence or order in which the digital evidence is collected. The order is maintained from highly volatile to less volatile data. An example order of volatility for a typical system are registers, cache, routing table, memory, temporary file systems, disk, physical configuration, network topology and archival media.

Q. 19 Show various Steganalysis attack methods. **AU : Dec.- 18**

Ans. : Steganalysis attack methods are as follows :

- **Steganography-only attack :** Only the steganography medium is available for analysis.
- **Known-carrier attack :** The original cover and steganography media are both available for analysis.
- **Known-message attack :** The hidden message is known.
- **Chosen-steganography attack :** The steganography medium and tool are both known.
- **Known-steganography attack :** The carrier and steganography medium, as well as the steganography tool or algorithm, are known.

Q. 20 How to perform the remote acquisition process? **AU : May-19**

Ans. : Remote data acquisition is collecting information about a system or a process. It uses three methods: bit-stream disk to image file, bit stream disk to disk and sparse data copy of a file.

Q. 21 Write any one the network forensics scenario. **AU : May-19**

Ans. : "Catch-it-as-you-can" system in which all packets passing through a certain traffic point are captured and written to storage with analysis being done subsequently in batch mode. This approach requires large amounts of storage usually involving a RAID system.

Q. 22 Name any three mobile device forensics tools. **AU : Dec.-19**

Ans. : Mobile device forensics tools are Bitpim, Autopsy, Oxygen Forensic, Mobiledit Lite etc.

Q. 23 Write the validation process of forensics data. **AU : Dec.-19**

Ans. : Validation in the analytical context refers to the process of establishing, through documented experimentation, that a scientific method or technique is fit for its intended purpose.

➡ 3.7.2 Multiple Choice Questions with Answers

Q. 1 ________ is the practice of concealing a file, message, image, or video within another file, message, image, or video.

(a) Imaging (b) Encryption

(c) Steganography (d) Data hiding

Ans. : (c) Steganography

Q. 2 PEM stands for ________.

(a) Public Encryption Mail (b) Privacy Enhanced Mail

(c) Privacy Enhanced Message (d) Public Encryption Message

Ans. : (b) Privacy Enhanced Mail

Q. 3 SNORT is an open source network ________ system which is available free of cost.

(a) intrusion prevention (b) intrusion avoidance

(c) intrusion detection (d) all of these

Ans. : (c) intrusion detection

Q. 4 The process of tracking unauthorized activity using techniques such as inspecting user actions, security logs, or audit data is called as ________

(a) intrusion prevention (b) intrusion detection

(c) host detection (d) host prevention

Ans. : (b) intrusion detection

Q. 5 SMTP uses port number ________.

(a) 143 (b) 110 (c) 80 (d) 25

Ans. : (d) 25

Q. 6 An Internet protocol designed for accessing e-mail on a mail server is ________.

(a) POP (b) ICMP (c) IMAP (d) TCP

Ans. : (c) IMAP

Q. 7 Which of the following is the data hiding techniques ?

(a) Bit-shifting (b) Using encryption

(c) Changing file extensions (d) All of these

Ans. : (d) All of these

Q. 8 A set of duplicate data that is stored in a temporary location to allow rapid access for computers to function more efficiently, is known as ________.

(a) boot record (b) metadata (c) swap (d) cache

Ans. : (d) cache

Q. 9 Which service runs on port 80 ?

(a) HTTP (b) HTTPS (c) FTP (d) SMTP

Ans. : (a) HTTP

Q. 10 Which service runs on port 443 ?

(a) HTTP (b) HTTPS (c) UDP (d) TCP

Ans. : (b) HTTPS

Q. 11 A basic unit of communication over a digital network is called ?

(a) Payload (b) Packets (c) BIOS (d) frame

Ans. : (b) packets

Q. 12 The Netstat command indicates that POP3 is in use on remote server. Which port is the remote server?

(a) port 25 (b) port 110 (c) port 80 (d) port 143

Ans. : (b) port 110

Q. 13 The directory can be viewed as a ________ that translate file names into their directory entries.

(a) symbol table (b) records (c) volumes (d) none of these

Ans. : (a) symbol table

Q. 14 A relative path name defines a path from the ________.

(a) root (b) current directory (c) parent directory (d) all of these

Ans. : (b) current directory

Q. 15 Path's name are ________.

(a) absolute path (b) relative path (c) both (a) and (b) (d) none of these

Ans. : (c) both (a) and (b)

Q. 16 When the user of a network workstation initiates EFS, the recovery key is sent to the local domain **________** server's administrator account.

(a) workstation (b) server's (c) third party (d) all of these

Ans. : (b) server's

Q. 17 Mobile security is also known as **________.**

(a) OS security (b) wireless security

(c) cloud security (d) database security

Ans. : (b) wireless security

Q. 18 Hackers cannot do which of the following after compromising your phone ?

(a) Shoulder surfing (b) Accessing your voice mail

(c) Steal your information (d) Use your app credentials

Ans. : (a) Shoulder surfing

❑❑❑

Notes

UNIT - IV

4 Ethical Hacking

Scope of the Syllabus

Introduction to Ethical Hacking - Footprinting and Reconnaissance - Scanning Networks - Enumeration - System Hacking - Malware Threats - Sniffing.

4.1 Introduction to Ethical Hacking

4.1.1 Hackers

- Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access. Example of Hacking : Using password cracking algorithm to gain access to a system
- Hacking refers to the practice of modifying or altering computer software and hardware to accomplish a goal that is considered to be outside of the creator's original objective.
- Penetration testing can be defined as a legal and authorized attempt to locate and successfully exploit computer systems for the purpose of making those systems more secure. Authorization is the process of obtaining approval before con-ducting any tests or attacks.
- Hacking is an art of exploring various security breaches. Each hacker has Motives, Methods and Skills. Computer Hacker is a typically knowledgeable person. He/she knows several different languages, familiar with UNIX and NT, Networking protocols.
- In other words can be referred to as the unauthorized access to any computer systems or network. This method can occur if computer hardware and software has any weaknesses which can be infiltrated if such hardware or software has a lack in patching, security control, configuration or poor password choice.
- A hacker will look for internal and external system holes or bugs to break into the system, fun and challenging.
- Cracker and hacker are two different terms. Cracker is making an attempt to break into the system by guessing or cracking user’s passwords. Crackers can easily be identified because their actions are malicious.

- An ethical hacker possesses the skills, mindset, and tools of a hacker but is also trustworthy. Ethical hackers perform the hacks as security tests for their systems. Ethical hacking is also known as penetration testing or white-hat hacking. It involves the same tools, tricks, and techniques that hackers use, but with one major difference : Ethical hacking is legal.

➥ 4.1.2 Types of Hackers

1. Crackers : - A cracker is one who breaks security on a system. Crackers are hardcore hackers characterized more as professional security breakers and thieves.
2. Hacktivists :- Hacktivists are conscious hackers with a cause.
3. Cyber terrorists : Based on motives, cyber terrorists can be divided into two categories : The terrorists and information warfare planners.

➤ How hackers hack the system?

a. The hacker will initially determine all available information about the target network. The hacker will select a target which has the least amount of protection, which will allow him to get the data he wants.

b. The target will be compared against well known attacks. If source code is available for the target's systems, the hacker will examine the code for new ways in.

c. The hacker may attempt to gain access to the password database. The hacker will attempt brute force access to the system. The hacker may attempt to gain physical access to the system.

- Steps performed by hackers

  1) Reconnaissance 2) Scanning

  3) Gaining Access 4) Maintaining Access 5) Clearing Tracks

- Reconnaissance is the act of gaining information about our target. Such as open ports, operating system, what services those ports are running, and any vulnerable applications they have installed. All of this information will be absolutely vital to choosing an attack.
- Port scanning refers to the surveillance of computer ports, most often by hackers for malicious purposes. Hackers conduct port-scanning techniques in order to locate holes within specific computer ports.
- Network scanning is a procedure for identifying active hosts on a network, either for the purpose of attacking them or for network security assessment.
- In the enumeration phase, the attacker gathers information such as network user and group names, routing tables, and Simple Network Management Protocol (SNMP) data.

➥ 4.1.3 Advantages and Disadvantages of Hacking

➤ Advantages of Hacking :

1. It is used to recover the lost of information, especially when user lost password.
2. It is used to perform penetration testing to increase the security of the computer and network.
3. It is used to test how good security is on your network.

➤ Disadvantages of Hacking :

1. It can harm the privacy of someone.
2. Hacking is illegal.
3. Criminal can use hacking to their advantage.
4. Hampering system operations.

➡ 4.1.4 Ethical Hacking

- Ethical hacking is an authorized practice of bypassing system security to identify potential data breaches and threats in a network.
- Ethical hacking is identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses.
- Ethical hacking is also known as penetration testing or white-hat hacking involves the same tools, tricks, and techniques that hackers use.
- Ethical hacking is performed withthe target’s permission. The intent of ethical hacking is to discover vulnerabilities from a hacker’s viewpoint so systems can be better secured.

➤ Ethical Hacking Terminology :

- **Threat** is a set of circumstances that has the potential to cause loss or harm.
- An exploit is a piece of software that takes advantage of a bug, glitch, or vulnerability, leading to unauthorized access, privilege escalation, or denial of service on a computer system.

➤ Classification of exploits :

- A remote exploit works over a network and exploits security vulnerabilities without any prior access to the vulnerable system.
- A local exploit requires prior access to the vulnerable system to increase privileges.
- An exploit is a defined way to breach the security of an IT system through a vulnerability.
- **Vulnerability** is a weakness in the security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user identity before allowing data access. Bugs in the system that enable users to violate the site security policy are called **Vulnerability.**
- Vulnerability : A design flaw, defect, or mis-configuration which can be exploited by an attacker.
- A vulnerability scanner scans a specified set of ports on a remote host and tries to test the service offered at each port for its known vulnerabilities.

➡ 4.1.5 Phases of Hacking

- Fig. 4.1.1 shows phases of hacking.

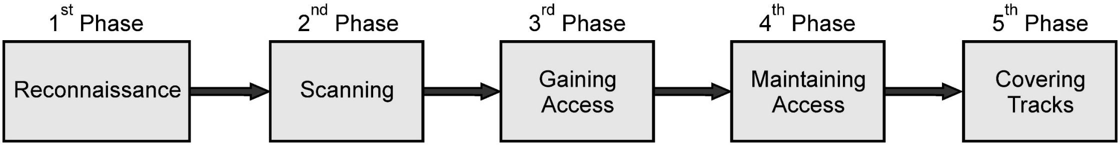


Fig. 4.1.1 : Phases of hacking

➤ 1. First Phase : Passive and Active Reconnaissance

- Passive reconnaissance : It is a penetration testing technique where attackers extract information related to the target without interacting with the target. That means no request has been sent to the target. Generally, the public resource is used to gather information.
- Active reconnaissance : It is a penetration testing technique where an attacker gets information related to the target by interacting with the target. Here, different vulnerability scanner such as Nessus, Nmap, etc. may be used to extract information.

➤ 2. Second Phase : Scanning

- Scanning involves taking the information discovered during reconnaissance and using it toexamine the network. Tools that a hacker may employ during the scanning phase can includedialers, port scanners, network mappers, sweepers, and vulnerability scanners.
- Hackers areseeking any information that can help them perpetrate attack such as computer names, IPaddresses, and user accounts.

➤ 3. Third Phase : Gaining Access

- In this phase, actual hacking takes place. Vulnerabilities discovered during the reconnaissance and scanning phase are now exploited to gain access. The method of connection the hacker uses for an exploit can be a LAN, local access to a PC, the Internet, or offline.
- Examples include stack-based buffer overflows, denial of service, and session hijacking.

➤ 4. Fourth Phase : Maintaining Access

- Once a hacker has gained access, they want to keep that access for future exploitation and attacks. Sometimes, hackers harden the system from other hackers or security personnel by securing their exclusive access with backdoors, rootkits, and Trojans.
- Once the hacker owns the system, they can use it as a base to launch additional attacks. In some case, the owned system is sometimes referred to as a zombie system.

➤ 5. Fifth Phase : Covering Tracks

- Once hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal action.
- Hackers try to remove all traces of the attack, such as log files or intrusion detection system (IDS) alarms. Examples of activities during this phase of the attack include steganography, the use of tunneling protocols, and altering log files.

➥ 4.1.6 Hacktivism

- Hacktivism refers to hacking for a cause. Hacktivism's main goal is to bring issues to light and cause social change. It can also be considered activism because it achieves these goals in a relatively peaceful manner.
- Hacktivism relies on many properties of the internet, allowing people to use different methods than they would offline. Because of the scalability of the internet, even small groups of people are able to make statements through hacktivism.
- Hacktivism also relies on the internet being relatively difficult to censor and mostly anonymous.

➥ 4.1.7 Types of Hacker Classes

- Hackers are of different types and are named based on their intent of the hacking system. Broadly, there are two main hackers : White-Hat hacker and Black-Hat hacker.
- One more type is gray hackers.

  1. **White Hat :** A white hat hacker is a computer network security professional and has non-malicious intent whenever he breaks into security systems. A White Hat hacker has deep knowledge in Computer Networking, Network Protocols and System Administration. White Hat hacker has also good knowledge in hacking tools and know how to program hacking tools.

- A white hat hacker has the skills to break into networks but he uses his skills to protect organizations. A White Hat hacker can conduct vulnerability assessments and penetration tests are also known as an Ethical Hacker.
- Often white hat hackers are employed by companies and organizations to check the vulnerabilities of their network and make sure that no hole is available in their network for an intruder.

  2. **Black Hat :** A black hat hacker, also known as a cracker, is a computer professional with deep knowledge in computer networking, network protocols and system administration. Black hat hacker has also good knowledge in many hacking tools and know how to program hacking tools.

- A black hat hacker uses his skills for unethical reasons. A black hat hacker always has malicious intention for intruding a network.
- Example : To steal research data from a company, to steal money from credit cards, hack email accounts etc.

  3. **Grey Hat :** A grey hat hacker is someone who is between white hat hacker and black hat hacker. Grey hat normally do the hacking without the permissions from the administrators of the network he is hacking. But he will expose the network vulnerabilities to the network admins and offer a fix for the vulnerability for money.

➥ 4.1.8 Benefits of Ethical Hacking

- The primary benefit of ethical hacking is to prevent data from being stolen and misused by malicious attackers, as well as :
  1. Implementing a secure network that prevents security breaches.
  2. Defending national security by protecting data from terrorists
  3. Gaining the trust of customers and investors by ensuring the security of their products and data.
  4. Discovering vulnerabilities from an attacker's so that weak points can be fixed.
  5. Helping protect networks with real-world assessments.

➥ 4.1.9 The Importance of Ethical Hacking

- Ethical hacking offers an objective analysis of an organization's information security posture for organizations of any level of security expertise. The ethical hacking organization has no knowledge of the company's systems other than what they can gather.
- Hackers must scan for weaknesses, test entry points, priorities targets, and develop a strategy that best leverages their resources. The objectiveness of this kind of security assessment has a direct impact on the value of the whole evaluation.
- Ethical hackers, or white hat hackers, offer a new approach to safety. In order to test your security measures, they perform 'pen tests' on your organisation.
- In other words, they 'hack' your systems for you and provide you with insight and valuable information regarding your organization's security posture.
- As a result, you catch the opportunity to see your organization from the perspective of a hacker without facing actual threats like sensitive data theft.

➥ 4.1.10 Goals Attackers Try to Achieve

- Security consists of four basic elements : Confidentiality, Authenticity, Integrity and Availability
- Confidentiality, integrity, and availability, often known as CIA, are the building blocks of information security. Any attack on an information system will compromise one, two, or all three of these components.
  1. **Confidentiality** refers to limiting information access and disclosure to authorized users and preventing access by or disclosure to unauthorized ones. Sensitive information should be kept secret from individuals who are not authorized to see the information.
  2. **Integrity** ensures that information is not changed or altered intransit. Under certain attack models, an adversary may not have to power to impersonate an authenticated party or understand a confidential communication, but may have the ability to change the information being transmitted.
  3. **Availability** refers, to the availability of information resources. An information system that is not available when you need it is at least as bad as none at all. Availability means that people who are authorized to use information are not prevented from doing so. It may be much worse, depending on how reliant the organization has become on a functioning computer and communications infrastructure.

➥ 4.1.11 Vulnerability Research

- Vulnerability research is the process of discovering vulnerabilities and design weaknesses that could lead to an attack on a system.
- To exploit a 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.
- Security bug (security defect) is a narrower concept : there are vulnerabilities that are not related to software: hardware, site, personnel vulnerabilities are examples of vulnerabilities that are not software security bugs.
- Hackers often rely on is the exploit techniques pioneered and shared by security researchers and people in the computer underground.

➥ 4.1.12 Types of Ethical Hacks

- Ethical hackers can use many different methods to breach an organization's security during a simulated attack or penetration test. The most common methods follow :
  1. Remote Dial-Up Network : The kind of ethical hacking identify and tries to save from the attack which is causing among the modern pool of client to find the open system, organizations make use of the method named war dialing for representative dialing. An open system is the best example of this kind of attacks.
  2. Remote Network : This procedure is mainly used to identify the attacks that cause among internet Mainly, the ethical hacker, try to recognize default as well as proxy information in a network. Some of them involve proxy or firewalls.
  3. Local Network : The local network hacking is a process which is utilized to access all the illegal information by making use of someone with the physical access gaining through a local network. For this process, the hacker needs to be ready to access the local network directly.
  4. Stolen Equipment : With the use of stolen equipment hack it is extremely easy to recognize the information about the thefts such as a laptop. The data secured by the owner of a laptop can be easily identified. The information includes password, username and other security settings in equipment can be encoded by stealing a laptop.
  5. Physical Entry : The physical entry hacking is utilized in the businesses to control attacks being attained through some physical premises.
  6. Social Network : The social engineering attack is a procedure being used to check the reliability of the business. This can be fulfilled by making use of face to face communication or telecommunication by gather data which can be utilized further in attacks. This kind of hack is used to know about security method being used by an organization.
  7. Application Network : The logic flaws being present in application results in an illegal access of network and even in application and data being offered in applications.
  8. Wireless Network Testing : In this procedure of hacking, the wireless network decreases the liability of network to an attacker by utilizing the radio access to given wireless space.

9. Network Testing : This kind of hacking recognizes all unsafe data being present in external as well as internal network. It not only works in the particular network but also in a device that includes a virtual private network.
10. War dialing : This kind of hack recognized all the default information which is being checked in a modem and is much dangerous for organizations.

4.2 Footprinting and Reconnaissance

4.2.1 Footprinting

- Footprinting refers to the process of collecting as much as information as possible about the target system to find ways to penetrate into the system. An ethical hacker has to spend the majority of his time in profiling an organization, gathering information about the host, network and people related to the organization.
- Information such as IP address, Whois records, DNS information, an operating system used, employee email id, Phone numbers etc is collected.
- The process of accumulating data regarding a specific network environment, usually for the purpose of finding ways to intrude into the environment.
- The EC-Council divides footprinting and scanning into seven basic steps. These include

1. Information gathering
2. Determining the network range
3. Identifying active machines
4. Finding open ports and access points
5. OS fingerprinting
6. Fingerprinting services
7. Mapping the network

1. **Information Gathering :** Good information gathering can make the difference between a successful pen test and one that has failed to provide maximum benefit to the client. An amazing amount of information is available about most organizations in business today. This information can be found on the organization's website, trade papers, Usenet, financial databases, or even from disgruntled employees. Some potential sources are discussed, but first, let's review documentation.
2. **Determining the Network Range :** Now that the pen test team has been able to locate name, phone numbers, addresses, some server names, and IP addresses, it's important to find out what range of IP addresses are available for scanning and further enumeration. If you take the IP address of a web server discovered earlier and enter it into the Who is lookup at www.arin.net, the network's range can be determined.
3. **Identify Active Machines :** Attackers will want to know if machines are alive before they attempt to attack. One of the most basic methods of identifying active machines is to perform a ping sweep.
4. **Finding Open Ports and Access Points :** With knowledge of the network range and a list of active devices, the next step is to identify open ports and access points. Identifying open ports will go a long way toward potential attack vectors. There is also the possibility of using war dialing programs to find ways around an organization's firewall. If the organization is located close by, the attacker might war drive the area to look for open access points.

5. **OS Fingerprinting :** At this point in the information gathering process, the hacker has made some real headway. IP addresses, active systems, and open ports have been identified. There are two ways in which the hacker can attempt to identify the targeted devices. The hacker's first choice is passive fingerprinting. The hacker's second choice is to perform active fingerprinting, which basically sends malformed packets to the target in hope of eliciting a response that will identify it. Although active fingerprinting is more accurate, it is not as stealthy as passive fingerprinting
6. **Fingerprinting Services :** Knowing what services are running on specific ports allows the hacker to formulate and launch application specific attacks.
7. **Mapping the Network :** Mapping the network provides the hacker with a blueprint of the organization. There are manual and automated ways to compile this information.

4.2.2 Whois

- Whois is a query/response protocol tool. It is widely used for querying an official database in order to determine the owner of a domain name, an IP address, or an autonomous system number on the Internet.
- Whois normally runs on TCP port 43. Whois is the primary tool used to query Domain Name Services.
- Linux system provides built in facility of whois. Windows does not have a built-in Whois client. Windows users will have to use a third-party tool or website to obtain Whois information.

```
$ whois vtubooks.com
Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

Domain Name: VTUBOOKS.COM
Registrar: DOMAIN.COM, LLC
Sponsoring Registrar IANA ID: 886
Whois Server: whois.domain.com
Referral URL: http://www.domain.com
Name Server: NS5.INDIALINKS.COM
Name Server: NS6.INDIALINKS.COM
Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Updated Date: 23-oct-2013
Creation Date: 18-nov-2000
Expiration Date: 18-nov-2015
```

```
>>> Last update of whois database: Sun, 26 Jul 2015 17:11:41 GMT <<<
$ whois google.com
Domain Name: google.com
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2015-06-12T10:38:52-0700
Creation Date: 1997-09-15T00:00:00-0700
Registrar Registration Expiration Date: 2020-09-13T21:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Registry Registrant ID:
Registrant Name: Dns Admin
Registrant Organization: Google Inc.
Registrant Street: Please contact contact-admin@google.com, 1600 Amphitheatre Parkway
Registrant City: Mountain View
Registrant State/Province: CA
Registrant Postal Code: 94043
Registrant Country: US
Registrant Phone: +1.6502530000
Registrant Phone Ext:
Registrant Fax: +1.6506188571
Registrant Fax Ext:
Registrant Email: dns-admin@google.com
Registry Admin ID:
Admin Name: DNS Admin
Admin Organization: Google Inc.
Admin Street: 1600 Amphitheatre Parkway
Admin City: Mountain View
Admin State/Province: CA
Admin Postal Code: 94043
Admin Country: US
Admin Phone: +1.6506234000
>>> Last update of WHOIS database: 2015-07-26T09:56:49-0700
```

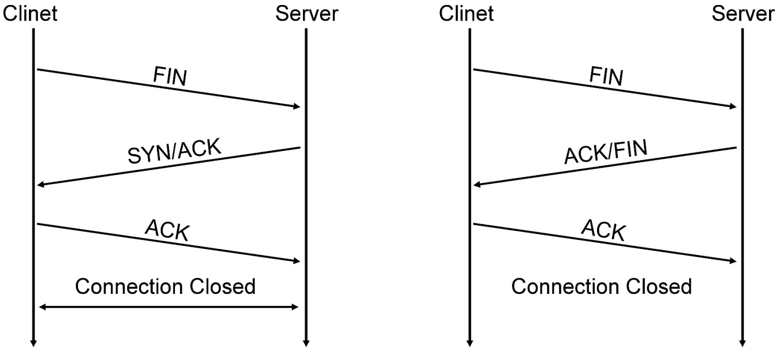
4.2.3 Network Reconnaissance

- Reconnaissance attack is a kind of information gathering on network system and services. This enables the attacker to discover vulnerabilities or weaknesses on the network.
- One of the old reconnaissance methods was simply to sequentially ping every IP address on a network, starting with the local subnet and then expand outward. If an IP address responded to a ping then the attacker knew there was a active device at that IP address and would add it to a locally list of potential attack targets. This ping method would require the attacker to guess what subnets existed on the network.
- Reconnaissance attack can be active or passive. Tools that could be used for active reconnaissance are :
  1. Application Mapper (AMAP) : AMAP uses the results from Nmap to mine for more information.
  2. Nessus : It is vulnerability Scanner
  3. Scanrand : Tt is fast network scanner
  4. Paratrace : TCP Traceroute that utilizes selected TTL messages
- Intruders are increasingly making use of compromised hosts to launch reconnaissance against target networks.

4.2.3.1 Nmap

- Nmap was developed by Fyodor Yarochkin. This tool is available for Windows and Linux as a GUI and command-line program. It is most widely-used port scanner tool. It can performs many types of scans and OS identification, and also allows user to control the speed of the scan.
- Network Mapped (Nmap) is a network scanning and host detection tool that is very useful during several steps of penetration testing. It is an open-source port or security scanner. Primary function of Nmap is to discovery and mapping of hosts on a network.
- Almost every Linux install its packaged, Windows you will need to download Nmap and the Win-Pcap files.
- Nmap can perform ping sweeps. Port scanning tools depends upon communication between two machines and TCP, UDP services. State of the connection is represented by flags in TCP connection. TCP uses six flags. For connecting to a TCP port, client sends a packet with the SYN flag. When SYN flag is set, it indicates clients wish to communicate with the port services.
- Nmap tool is capable to detect types of victims' operation systems just using TCP fingerprinting. TCP fingerprinting uses advanced fingerprinting analyses of the TCP stack implementation. A TCP packet is crafted by switching on or off certain flags and sent to the remote machine.
- The remote operating system, based on its TCP stack implementation sends a response, with some specific flags turned on or off.Depending on TCP responses collected for each crafted packet we can make an intelligent guess of the operating system from its database of TCP stack signatures.

- Standard TCP communications are controlled by flags in the TCP packet header. Following are the list of TCP connection flags :
  a. Urgent (URG) : The Urgent pointer is valid if it set to 1.
  b. Acknowledgement (ACK) : ACK bit is set to 1 to indicate that the acknowledgment number is valid.
  c. Push (PSH) : The receiver should pass this data to the application as soon as possible.
  d. Reset (RST) : This flag is used to reset the connection. It is also used to reject an invalid segment.
  e. Synchronize(SYN) : Synchronize sequence number to initiate a connection. The connection request has SYN = 1 and ACK = 0 to indicate that the piggyback acknowledgement field is not in use.
  f. Finish (FIN) : The FIN bit is used to release a connection. It specifies that the sender is finished sending data.
- The port number along with the source and destination IP addresses in the IP header, uniquely identify each connection. The combination of an IP address and a port number is sometimes called a socket. When a new connection is being established, the SYN flag is turned on. The sequence number of the first byte of data sent by this host will be the ISN plus one because; the SYN flag consumes a sequence number.
- The three-way handshake involves the exchange of three messages between the client and the server. Three messages are client SYN, service SYN-ACK and client ACK etc. Fig. 4.2.1 shows three-way handshake for TCP.



(a) connect **(b) Disconnect**

Fig. 4.2.1 : Three way handshake TCP connection

- The client initiates a connection to the server via a packet with only the **SYN** flag set. The server replies with a packet with both the **SYN** and the **ACK** flag set. For the final step, the client responds back the server with a single **ACK** packet. If these three steps are completed without complication, then a TCP connection has been established between the client and server.
- Client sends a single **SYN** packet to the server on the appropriate port. If the port is open then the server responds with a **SYN/ACK** packet.If the server responds with an **RST** packet, then the remote port is in state closed. The client sends **RST** packet to close the initiation before a connection can ever be established. This scan also known as “half-open” scan.

➤ Command Line Syntax

```
$ nmap [ <Scan Type> …] [ <Options> ] { <target specification> }
```

- Target specification can be hostnames, IP address etc.
- The output of Nmap is a list of scanned targets, with additional information on each depending on the options used. Port table is the main information of Nmap. Table list the port number and protocol, service name and state. The state is either open, filtered, closed, or unfiltered.
  1. Open state means that an application on the target machine is listening for connections/packets on that port.
  2. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed.
  3. Closed means ports have no application listening on them, though they could open up at any time.
  4. Ports are classified as unfiltered. When they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or closed.
- Open port : A service process is listening at the port. The OS receives packets arriving at this port and passes the messages to the service process. If the OS receives a SYN at an open port, this is the first packet of the three way handshake.
- Closed : No process is listening at the port. If the OS receives a SYN at a closed port, an RST is sent.
- Filtered : A packet filter is listening at the port DOS

➤ Nmap Options :

Sr. No.	Options	Remarks
1.	-sS	TCP SYN scan
2.	-sF -sX -sN	Stealth FIN, Xmas Tree, or Null scan modes
3.	-sP	Ping scanning
4.	-sW	Window scan
5.	-sA	ACK scan
6.	-sL	List scan
7.	-P0	Do not try to ping hosts at all before scanning them
8.	-sT	TCP Connect
9.	-U	UDP Scanning: Sends a UDP packet to target ports to determine if a UDP service is listening
10.	-b	Bounces a TCP scan off of an FTP server, hiding originator of the scan.
11.	-sR	RPC Scanning: Scans RPC services using all discovered open TCP/UDP ports on the target to send RPC NULL commands.

➤ Nmap timing options :

Sr. No.	Options	Remarks
1.	paranoid	Send one packet every 5 minutes
2.	Sneaky	Send one packet every 15 seconds
3.	Polite	Send one packet every 0.4 seconds
4.	Normal	Send packets ASAP without missing target ports
5.	Aggressive	wait no more than 1.25 seconds for any response
6.	Insane	wait no more than 0.3 seconds for any response

- Nmap can be used for following compliance testing :
  1. Testing for open ports on the interfaces of a firewall.
  2. Performing scans across workstation IP address ranges to determine if any unauthorized networking applications are installed.
  3. Determining if the correct version of web service is installed in De-Militarized Zone
  4. Locating systems with open file sharing ports.
  5. Locating unauthorized FTP servers, printers or operating systems.

➤ Nmap with help :

```
C:\nmap>nmap -h
Nmap 3.93 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
* -sS TCP SYN stealth port scan (default if privileged (root))
-sT TCP connect() port scan (default for unprivileged users)
* -sU UDP port scan
-sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
-sV Version scan probes open ports determining service and app names/versions
-sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
-p <range> ports to scan. Example range: '1-1024,1080,6666,31337'
-F Only scans ports listed in nmap-services
-v Verbose. Its use is recommended. Use twice for greater effect.
-P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
-6 scans via IPv6 rather than IPv4
-T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
-n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
-oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
```

```
-iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
--interactive Go into interactive mode (then press h for help)
--win_help Windows-specific features
```

- Nmap is considered a required tool for all ethical hackers.

4.2.3.2 THC-Amap

- Amap is a tool for determining what application is listening on a given port. THC means The Hackers Choice.
- Most of port scanners assume that if a particular port is open, then default application for that port must be present. Amap probes these ports to find out what is really running on that port.
- You can download from **http://thc.segfault.net/thc-amap/**
- THC-Amap runs in following modes :

Sr. No.	Modes	Remarks
1.	-A	It identifies the service associated with the port.
2.	-B	This mode does not perform identification
3.	-P	It conducts a port scan.

4.3 Scanning Networks

- Scanning is another essential step, which is necessary, and it refers to the package of techniques and procedures used to identify hosts, ports, and various services within a network. Scanning is the process of locating systems that are alive and responding on the network.
- Types of scanning are port scanning, network scanning and Vulnerability scanning.

4.3.1 Vulnerability Scanning

- **Vulnerability** is a weakness in the security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user identity before allowing data access. Bugs in the system that enable users to violate the site security policy are called **Vulnerability.**
- Vulnerability : A design flaw, defect, or mis-configuration which can be exploited by an attacker.
- A vulnerability scanner scans a specified set of ports on a remote host and tries to test the service offered at each port for its known vulnerabilities.
- **Threat** is a set of circumstances that has the potential to cause loss or harm.
- Hardware is more visible than software, largely because it is composed of physical objects**.** Software is vulnerable to modification that either cause it to fail or cause it to perform an unintended task. Data is especially vulnerable to modification.

- A vulnerability scanner is software application that assesses security vulnerabilities in networks or host systems and produces a set of scan results. However, because both administrators and attackers can use the same tool for fixing or exploiting a system, administrators need to conduct a scan and fix problems before an attacker can do the same scan and exploit any vulnerability found.
- Vulnerability remediation is the process of fixing vulnerabilities. There are different types of vulnerability scanners that operate at different levels of invasiveness. Some simple scanners just check the Windows Registry and software version information to determine whether the latest patches and updates have been applied.
- Scanners use predefined tests to identify vulnerabilities. Scanner may produce false positive if written test is poor. There is no vulnerability attack but scanner reports it as vulnerable.
- Vulnerability scanner is made up of four main modules: Scan Engine, Scan Database, Report Module and a User Interface.
- Vulnerability scanners can be divided broadly into two groups: *network-based and host-based scanners*
- A **network-based scanner** is usually installed on a single machine that scans a number of other hosts on the network. It helps detect critical vulnerabilities such as mis-configured firewalls, vulnerable web servers, risks associated with vendor-supplied software, and risks associated with network and systems administration.
- A **host-based scanner** is installed in the host to be scanned, and has direct access to low-level data, such as specific services and configuration details of the host's operating system.A database scanner is an example of a host-based vulnerability scanner.

➤ Working of Vulnerability Scanning

- Steps for scanning :
  1. Checking if the remote host is alive
  2. Detect firewall if any
  3. TCP / UDP port scanning
  4. Detection of operating system
  5. TCP / UDP service discovery
  6. Vulnerability assessment based on the services detected

➤ Limitations of Vulnerability Scanners

1. Generate overwhelming amount of data
2. No indication of how vulnerabilities can be combined
3. Vulnerability scanners can only report vulnerabilities according to the plug-ins installed in the scan database.

- The key difference between vulnerability assessment and penetration testing is the lack of exploitation in vulnerability assessment and the actual exploitation in penetration testing.

➥ 4.3.2 Port Scanning

- Some of the services are naturally secure. Services do not always run on default ports. Port scanning is the process of identifying open and available TCP/IP ports on a system
- The main goal of port scanning is to find out which ports are open, which are closed, and which are filtered. When we say a port is filtered, what we mean is that the packets passing through that port are subject to the filtering rules of a firewall.
- In TCP/IP and UDP networks, a port is an endpoint to a logical connection and the way a client program specifies a specific server program on a computer in a network. Some ports have numbers that are pre-assigned to them by the IANA, and these are called the "well-known ports".
- A port number is a 16-bit unsigned integer that ranges from 0 to 65535
- A specific network port is identified by its number commonly referred to as port number, the IP address in which the port is associated with and the type of transport protocol used for the communication.

➤ **Standard port numbers are listed below :**

1. Ports number 0 to port number 1023 are known as **Well Known Ports**
2. Port number 1024 to port number 49151 are named as **Registered Ports**
3. Port number49152 to Port number 65535 **are Dynamic and/or Private Ports**

Port Number	Protocol Name	Port Number	Protocol Name
21	FTP	110	POP3 port
22	SSH server listing port	123	NTP
23	Telnet port	135	RPC
25	SMTP mail port	143	IMAP4 port
53	DNS port	161	SNMP port
67	DHCP	179	BGP Port
80	HTTP	443	SSL Port

- Port scanning may involve all of the 65,535 ports or only the ports that are well-known to provide services vulnerable to different security-related exploits.
- **Open port :** A service process is listening at the port. The operating system receives packets arriving at this port and gives the messages to the service process. If the operating system receives a SYN at an open port, this is the first packet of the three way handshake.
- **Closed port :** No process is listening at the port. If the OS receives a SYN at a closed port, an RST is sent.
- **Filtered port :** A packet filter is listening at the port.
- Port scanner tool can be used to identify available services running on a server, it uses raw IP packets to find out what ports are open on a server or what operating system is running or to check if a server has firewall enabled etc.

- Port scanner is an essential security tool for finding open ports corresponding to the TCP or UDP services running on a target device. This scanner allows you to run four different types of scanning patterns while looking for TCP or UDP open ports.
- **Port scanning technique** consists of sending a message to a port and listening for an answer. The received response indicates the port status and can be helpful in determining a host's operating system and other information relevant to launching a future attack.
- The vertical scan is a port scan that targets several destination ports on a single host. A horizontal scan is a port scan that targetsthe same port on several hosts.

➥ 4.3.3 Network Scanning

- Network scanning refers to the process of obtaining additional information and performing a more detailed reconnaissance based on the collected information in the footprinting phase.
- In this phase, a number of different procedures are used with the objective to identify hosts, ports, and services in the target network. The whole purpose is to identify vulnerabilities in communication channels and then create an attack plan.

4.4 Enumeration

- Enumeration is the process of extracting user names, machine names, network resources, shares, and services from a system. Enumeration techniques are conducted in an intranet environment. During enumeration, information is systematically collected and individual systems are identified.
- Example :
  1. Discovering NetBIOS name enumeration with NBTscan.
  2. Establishing null sessions and connections. Null sessions tools like Dumpsec, Winfo and Sid2User or more, may used to perform this attack
- Enumeration can be used to gain information on :
  a. Network shares
  b. SNMP data, if they are not secured properly
  c. IP tables
  d. Usernames of different systems
  e. Passwords policies lists
- Enumerations depend on the services that the systems offer. They can be DNS enumeration, NTP enumeration, SNMP enumeration, Linux/Windows enumeration and server message block (SMB) enumeration.

➤ 1. Netbios Null Sessions

- The null session is often referred to as the Holy Grail of Windows hacking. Null sessions take advantage of flaws in the Common Internet File System/Server Messaging Block (CIFS/SMB).

- User can establish a null session with a Windows (NT/200/XP) host by logging on with a null user name and password. Using these null connections, you can gather the following information from the host :

  a) List of users and groups

  b) List of machines

  c) List of shares

  d) Users and host SIDs (Security Identifiers)

- **Techniques for Enumeration**

  a. Extracting user names using email ID's

  b. Extract information using the default password

  c. Brute force active directory

  d. Extract user names using SNMP

  e. Extract user groups from Windows

  f. Extract information using DNS zone transfer

  g. SNMP enumeration

- **Server Message Block Enumeration :** It is mainly used for providing shared access to files, printers and miscellaneous communications between nodes on a network. It also provides an authenticated inter-process communication mechanism.

- **DNS Enumeration :** DNS enumeration retrieves information regarding all the DNS servers and their corresponding records related to an organization. DNS enumeration will yield usernames, computer names, and IP addresses of potential target systems.

- **SNMP Enumeration :** SNMP is an application layer protocol which uses UDP protocol to maintain and manage routers, hubs, switches and other network devices. It is based on a client-server architecture where SNMP client or agent is located on every network device and communicates with the SNMP managing station via requests and responses. Both SNMP request and responses are configurable variables accessible by the agent software. SNMP contains two passwords for authenticating the agents before configuring the variables and for accessing the SNMP agent from the management station.

- Default SNMP password allow attackers to view or modify the SMMP configuration settings. Attackers can enumerate SNMP on remote network devices for the following :

  a. Information about network resources such as routers, shares, devices, etc.

  b. ARP and routing tables

  c. Device specific information

  d. Traffic statistics etc.

- **NetBIOS Enumeration and Null Session :** Net BIOS null Sessions occurs when you connect any remote system without user-name and password. It is usually found in systems with Common Internet File System (CIFS) or SMB depending on operating system. Once attacker is in with null session he/she can explore information about groups, shares, permissions, policies and even password hashes.

- Null session attack uses vulnerability in SMB protocol for creating connection because it uses SMB uses trust for any kind of relationship between devices available in network.

- Now to check whether the system is vulnerable to null session or not, type following commands :

```
 C:\>net use \\IP_Address\IPC$
For example
C:\>net use\\192.168.56.1\IPC$
Next type
C:\>net use \\IP_Address\IPC “”/u:“”
where “”/u:“” denotes you want to connect without user-name and password. Now
explore further information.
C:\>net view \\IP_Address
```

- The Steps Involved in Performing Enumeration :
- The following steps are an example of those a hacker might perform in preparation for hacking a target system :
  1. Extract usernames using enumeration.
  2. Gather information about the host using null sessions.
  3. Perform Windows enumeration using the Superscan tool.
  4. Acquire the user accounts using the tool GetAcct.
  5. Perform SNMP port scanning

4.5 System Hacking

4.5.1 Password Cracking

- When your log in to a computer and enter password, the computer checks that password belongs to you and then grants access. The password is the secret that is known only to the user and server. But it would be quite dangerous to store the passwords in the file in the computer.
- If an internal attacker obtains access to that file, all passwords stored on that computer could get compromised.
- Password cracking is one of the oldest hacking arts. Every system must store passwords somewhere in order to authenticate users. However, in order to protect these passwords from being stolen, they are encrypted. Password cracking is the art of decrypting the passwords in order to recover them.
- A password cracking program if used ethically can be used by the system administrator to detect weak passwords amongst the system so they can be changed. A password cracking program is most likely used to check the security of your own system.
- Crack is a type of password cracking utility that runs through combinations of passwords until it finds one that it matches. It also scans the content of a password file looking for weak login passwords.
- Passwords are not stored in clear text format. As a rule, passwords are stored as hashes. Hashes are one-way encryption that is unique for a given input. In the Windows operating system, passwords on the local system are stored in the SAM file, while Linux stores them in the /etc/shadow file.

- Reasons behind password cracking :
  1. To gain unauthorized access to a computer/server.
  2. Some time we forget the password so to recover a password
  3. To check the security of your system
  4. To do the crime with other name.
- Manual password cracking is easy. Attacker uses following method for password cracking.
  1. Select administrator account or guest account
  2. Make a list of possible password. Here date of birth, pet name, company name, any particular event happens to that person are consider.
  3. Prepared the password list with higher priority to lower priority
  4. Try one by one password until you found the proper password.
- Password is stored in database with encrypted format. Manual cracking of password is time consuming process. Encrypted password is used to ensure confidentiality.
- UNIX Operating system stores the hashed value of passwords in the password file instead of the actual passwords. Then when a user inputs their password, the system can simply take the hash of the input and compare it to the stored hash value. On most Unix-based file systems the password file is located at **/etc/passwd.**
- The password file for Windows, known as the Security Accounts Manager (SAM) file, is located in **C:\windows\system32\config\sam**.
- Online services typically store passwords for their system in a non-standardized way, and these systems are not always designed by engineers with backgrounds in privacy or security.
- The default Android program requires the user to create a password which connects at least four dots in any order.

➥ 4.5.1.1 Password Cracker Tools

- **Dictionary Attack** is the simplest and fastest password cracking attack. It just runs through a dictionary of words trying each one of them to see if they work.
- **Rainbow Table :** Most modern systems now store passwords in a hash i.e. encrypted password. To crack this encrypted password is to take dictionary file and hash each word and compare it to the hashed password.
- **Brute Force :** Brute force password cracking attempts all possibilities of all the letters, number, special characters that might be combined for a password and attempts them. It is the most time consuming approach to password cracking.
- **Hybrid :** A hybrid password attack is one that uses a combination of dictionary words with special characters, numbers, etc. Often these hybrid attacks use a combination of dictionary words with numbers appending and prepending them, and replacing letters with numbers and special characters.

1. **JOHN THE RIPPER :** John the Ripper is a fast password cracker, currently available for many flavors of UNIX, Win32 and OpenVMS. Its primary purpose is to detect weak UNIX passwords. It can use specialized wordlists or password rules based on character type and placement.
2. **L0phtCrack :** Window password is cracked using l0phtCrack. L0phtCrack obtains password hashes from the operating system, and then begins hashing possible password values. The password is discovered when there is a match between a target hash and a computed hash. L0phtCrack must first obtain password hashes from the target system, and then uses various cracking methods to retrieve the passwords.
3. **Aircrack-ng :** Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the all-new PTW attack, thus making the attack much faster compared to other WEP cracking tools.
4. **THC-Hydra :**When you need to brute force crack a remote authentication service, Hydra is often the tool of choice. It can perform rapid dictionary attacks against more than 21 protocols, including Telnet, FTP, HTTP, SMB etc.
5. **Cain and Abel :** Written strictly for Windows, it can crack numerous hash types, including NTLM, MD5, wireless, Oracle, MySQL, SQL Server etc. It can crack passwords using a dictionary attack, rainbow attack, and brute force. It selects the password length and character set when attempting a brute force attack.
6. **Brutus :** It is an online password cracking tool that many consider the fastest online password cracker. It is free and available on both Linux and Windows, and it supports password cracking in HTTP.

➥ 4.5.1.2 Password Cracking Attacks

- Password attacks, such as password guessing or password cracking, are time-consuming attacks. Tools that make use of pre-computed hashes reduce the time needed to obtain passwords greatly.
- Classification of password cracking attacks are as follows :

  1. Online attacks   2. Offline attacks

➤ Online Password Attacks

- It is also known as password guessing. It is the process of attempting to find passwords by trying to login. Online attacks are of two types: *passive and active online attack.*
- In passive online attacks an attacker do not contact with authorizing party for stealing password. A passive attack is not detectable to the end user.Types of passive online attacks include wire sniffing, Man in the middle attack and reply attack.
- A*ctive online attack* can be directly termed as password guessing. An attacker tries number of passwords one by one against victim to crack user password.
- Online password attacks are relatively slow.

➤ Offline Password Attacks

- An offline password attack, also known as password cracking. The main advantage of offline cracking is the speed.
- Offline attacks require physical access to the system. It copy the password file from the system onto storage disk.
- In this attack, the attacker will start cracking the password by creating a hash of a password or a challenge-response sequence and comparing it to the hash or response that he captured. If a match is found, the attempt to crack the hash is considered successful.
- It is not possible to prevent offline attacks by restricting the security policies. Offline attacks are in general much faster than online attacks.
- Offline attacks include, dictionary attacks, hybrid attacks, brute force attack, pre-computed hash attacks, syllable attacks, rule based attacks and rainbow attacks.

➥ 4.5.1.3 LAN Manager Hash

- Windows does not store your actual password with your account; when you select a new password, Windows computes a hash of the password and stores that with your account in the local SAM or Active Directory depending on the type of account. In fact, by default Windows computes 2 hashes: one is called an NT or Unicode hash and the other is called the LANMAN (LANMANAGER) hash.
- The LAN manager hash is an encryption mechanism implemented by Microsoft prior to its release of Windows 2000 uses NT Lan Manager (NTLM). The LANMAN hash was advertised as a one-way hash that would allow end users to enter their credentials at a workstation, which would, in turn, encrypt said credentials via the LANMAN hash.
- The LANMAN password can't exceed 14 characters and if it exceeds 7 characters, LANMAN actually builds 2 independent hashes of the first 7 characters and then the 2nd 7 characters. LANMAN also converts lower case letters to upper case before hashing.
- For example, the hash for the password "QBMzftvX" is broken into two parts (QBMZFTV and X). You will also see that all of the cleartext characters of these LM hashes are upper-cased.

C88062822433f468	**bcbb464a6f1414b9**
Characters 1 to 7 Cleartext : QBMZFTV	Characters 7 to 14 Cleartext : X

➥ 4.5.1.4 Cracking Windows 2000 Passwords

- The Security Account Manager (SAM) file in Windows contains the usernames and hashed passwords. It is located in the *Windows\system32\config* directory. The file is locked when the operating system is running so a hacker can't attempt to copy the file while the machine is booted to Windows.

- In addition it's also located in the registry file HKEY_LOCAL_MACHINE\SAM which cannot be accessed during run time. Finally backup copies can be often found in Windows\Repair.
- The SAM file is further encrypted with the SysKey (Windows 2000 and above) which is stored in *%SystemRoot%\system32\config\system* file.
- During the boot-time of Windows the hashes from the SAM file gets decrypted using the SysKey and the hashes are loaded to the registry is then used for authentication purpose. Both system and SAM files are unavailable to standard programs during Windows' runtime.

4.6 Password Cracking and Brute-Force Tools

- A Brute-Force attack is method of breaking a cipher by trying every possible key. Feasibility of brute force attack depends on the key length of the cipher, and on the amount of computational power available to the attacker.
- Brute-force attacks are often used for attacking authentication and discovering hidden content/pages within a web application. These attacks are usually sent via GET and POST requests to the server.
- In Brute-Force we specify a charset and a password length range.
- Hackers launch brute-force attacks using widely available tools that utilize wordlists and smart ruleset to intelligently and automatically guess user passwords. This type attacks are easy to detect, but they are not so easy to prevent.
- A Brute force attack is an automated process of trial and error used to guess a person's user name, password, credit-card number of cryptographic key. Insufficient authentication occurs when a web site permits an attacker to access sensitive content or functionality without having to properly authenticate. Weak password recovery validation is when a website permits an attacker to illegally obtain, change or recover another user's password.
- Password is a front line protection against the unauthorized access to the system. A password authenticates the identifier (ID) and provides security to the system. Therefore almost all systems are password protected.
- Linearization attack is used to crack any password in seconds

4.6.1 John the Ripper

- John the Ripper is a fast password cracker, currently available for many flavors of UNIX, Windows and OpenVMS. Its primary purpose is to detect weak UNIX passwords. It can use specialized wordlists or password rules based on character type and placement.
- John the Ripper is a command line tool. A dictionary attack uses a word database, and tries it repeatedly. John the Ripper has this capability.
- John will accept three different password file formats. It crack any password encrypted in one of the formats listed by the "-test" option.

- John the Ripper supports the following cracking modes :
  1. wordlist with or without rules;
  2. "single crack", makes use of the login information;
  3. incremental, tries all character combinations;
  4. External, allows you to define your own cracking mode.
- John the Ripper comes pre-installed with a small dictionary of some typical passwords located in “/usr/share/john/password.lst” file.
- John automatically selects the correct encryption algorithm for the hashes and begins cracking. All the cracked passwords are saved in the John.pot file, which is a text file. This tool uses for brute force is called "Incremental".In incremental mode john does not use a word list, but just tries all possible passwords.
- While cracking, you can press the Enter key for status, or Ctrl+C to abort the session, saving point information to a file. By the way, if you press Ctrl+C twice John will abort immediately without saving.

➤ Cracking Modes

1. **Wordlist mode :** User must specify a wordlist and some password files.
2. **Single crack mode :** It will try using thelogin information as passwords. This mode is much fasterthan the wordlist mode, which allows using a lot of rules in a reasonable time.
3. **Incremental mode :** This is the most powerful cracking mode, it can try all possible character combinations as passwords.
4. **External mode :** You can define an external cracking mode for use with John**.** This is done with ~/john.ini's sections called [List.External:<mode>], where <mode> is any identifier that you assign to the mode. The section should contain some functions that John will use to generate the words it tries. These functions are coded in a subset of the C language, and are compiled by John at startup.

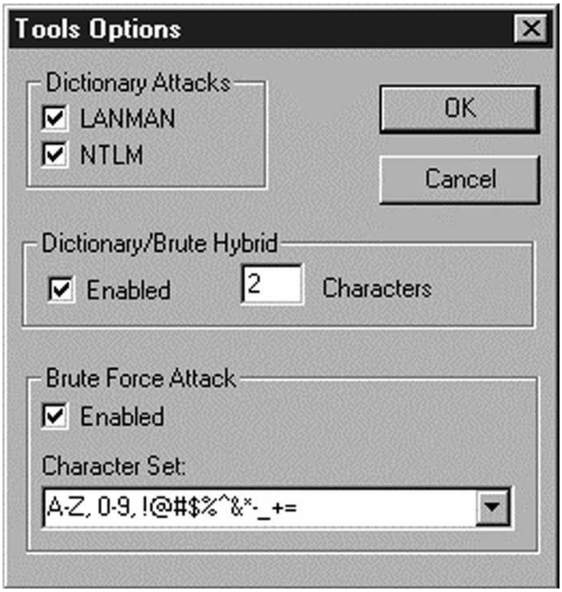
➤ John Ripper Command Line Options :

Sr. No.	Command	Remark
1.	Wordfile	Set to your wordlist file name.
2.	Timeout	Set to the value in minutes
3.	Beep	Set to something starting with 'Y' or 'N' to specify whether to beep when a password is found or not

➡ 4.6.2 L0PHTCRACK

- This tool used to crack Windows NT/2000 passwords. Easy to use GUI interface. It runs on MS Windows 9x, NT, and 2000 systems.
- Windows stores passwords in the Security Accounts Manager (SAM). It is binary file that is difficult to read without special tools.

- Not only will L0phtCrack guess passwords, it will extract LANMan hashes from any SAM file, the local system, or a remote system, and it will even sniff hashes as they cross a network. The SAM file is stored in the *\WINNT\system32\config\ directory.*
- L0phtCrack will extract passwords from the local or remote computers with the Dump Passwords From Registry option.
- Attacker must get a copy of the encrypted/hashed password representations stored in the SAM database of target machine. L0phtCrack includes "pwdump" tool for dumping Windows NT password representation from a local or remote machine across the network. Requires administrator privileges on target machine.
- Fig. 4.6.1 shows configuration options for L0phtCrack.



Dictionary Attacks
☑ LANMAN
☑ NTLM

Dictionary/Brute Hybrid
☑ Enabled 2 Characters

Brute Force Attack
☑ Enabled
Character Set: A-Z, 0-9, !@#$%^&*-_+=

Fig. 4.6.1

➥ 4.6.3 Pwdump

- Pwdump is able to extract NTLM and LanMan hashes from a Windows target, regardless of whether Syskey is enabled. It is also capable of displaying password histories if they are available. It outputs the data in L0phtcrack-compatible form, and can write to an output file.
- This tool is written by Jeremy Allison in the year 1997.
- It only affects Windows XP/2000 computers, and it is used in order to dump users and password hash tables in local or remote Windows XP/2000 computers. These hash tables allow brute force password cracking in order to try to guess the original values of the user names and passwords associated, and dictionary attacks.
- Login as system admin to windows machine and then run following command at command prompt :

```
C:\> pwdump7 >c:\hash.txt
```

pwdump7 will dump the SAM to the screen and the > character redirects the output to a file called hash.txt

- **Syntax:**

  pwdump [-h][-o][-u][-p] machineName

  where

-h	Prints the usage message and exits
-o	Specifies a file to which to write the output
-u	Specifies the user name used to connect to the target
-p	Specifies the password used to connect to the target
-s	Specifies the share to be used on the target, rather than searching for one

4.7 Keyloggers and Spyware

- A keylogger is a type of surveillance software that has the capability to record every keystroke you make to a log file. A keylogger recorder can record instant messages, e-mail, and any information you type at any time using your keyboard. The log file created by the keylogger can then be sent to a specified receiver.
- A keylogger is a program that runs in the background or hardware, recording all the keystrokes. Once keystrokes are logged, they are hidden in the machine for later retrieval, or shipped raw to the attacker.
- Security using keyloggers will monitor email, internet, chats or anything that requires a keystroke. This will help capture all information in image and/or text form. Keyloggers are a type of malicious malware that track the users' keystrokes and captures the characters that are pressed in and writes the information to a file.
- There are two types of keylogger: hardware keylogger and software keylogger

4.7.1 Hardware Keyloggers

- Hardware Keyloggers are small electronic devices used for capturing the data in between a keyboard device and I/O port**.** These devices have built in memory where they store the keystrokes. They must be retrieved by the person who installed it in order to obtain the information.
- Hardwar keyloggers is not detected by anti-viral software or scanners.
- Hardwar keyloggers are of three types :
  1. Inline devices that are attached to the keyboard cable
  2. Devices which can be installed inside standard keyboards
  3. Replacement keyboards that contain the key logger already built-in
- **List of hardware keyloggers :**
  1. **Hardware KeyLogger Stand-alone Edition :** A tiny hardware device that can be attached in between a keyboard and a computer.
  2. **Hardware KeyLogger Keyboard Edition :** Looks and behaves exactly like a normal keyboard, but it keeps a record of all keystrokes typed on it.

3. **KeyGhost Hardware Keylogger :** A tiny hardware device that can be attached in between a keyboard and a computer.
4. **KeyKatcher Keystroke Logger :** A tiny hardware device that can be attached in between a keyboard and a computer.

➤ **Advantages :**

1. Antivirus techniques cannot catch these
2. Work on all computing platforms

➤ **Disadvantage :**

1. It can be spotted by a suspicious user

➥ 4.7.2 Software Keyloggers

- Software keyloggers track systems, collect keystroke data within the target operating system, store them on disk or in remote locations, and send them to the attacker who installed the Keyloggers.
- They are implemented as traditional applications or kernel-based. In almost all malicious instances of this type of keylogger, users participated in some way in the software's installation.
- Anti-malware, personal firewall, and host-based intrusion prevention (HIPS) solutions detect and remove application keyloggers.
- Software keylogger detection methods include :
  1. Scan local drives for log.txt or other log file names associated with known keyloggers;
  2. Implement solutions that detect unauthorized file transfers via FTP or other protocols;
  3. Scan content sent via email or other authorized means looking for sensitive information;
  4. Detect encrypted files transmitted to questionable destinations.
- Software keyloggers can be detected using software tools. For this reason, users of keyloggers often prefer hardware solutions.

➤ **Advantages :**

1. Are hard to detect
2. Can be deployed remotely via a software-vulnerability attack
3. Are fairly easy to write

➤ **Disadvantages :**

1. A good Antivirus scheme could sniff these out.
2. Far fewer cons with the software, so these are much more common than hardware-type keyloggers.

➤ **Examples of Windows Keyloggers**

1. **Badtrans :** A keylogger worm that exploited vulnerabilities in Outlook Express and Internet Explorer. It collected keystrokes and sent them to various e-mail address.
2. **Magic Lantern/Carnivore :** FBI's own software to wiretap/log e-mails passing through ISPs

4.7.3 Spywares

- Software that is installed on a computer without the user’s knowledge which monitors user activity and transmits it to another computer. Many spyware programs are set to monitor what web sites you visit and how long you visit them for, generally for advertising / marketing purposes.
- Spyware originated in the 1990's with programs that secretly observed and logged user web surfing habits. It can do more than steal your personal information but also rob user PC of its speeds, stability and Internet access efficiency.
- **Adware :** It is software that gathers information about your Web-surfing habits in order to target you with pop-up advertisements for products and services that might be of interest to you. Adware is generally not malicious or illegal. Adware can be Spyware when it tracks browser activity and reports such activity back to some unknown recipient.
- Spyware differs from viruses and worms in that it does not usually self-replicate. Like many recent viruses, spyware is designed to exploit infected computers for commercial gain. Spyware may have to same effect as viruses.

Prevention of Spyware

1. Do not install freesoftware available on Internet.
2. Do not click on email attachments or links if you don’t know the sender or even if you know the sender, but the content is unexpected.
3. Do not install unknown software
4. Do not click on links or buttons on pop-up windows.
5. Do not install non-work-related software onto your work computers
6. Save your data and backup often

4.8 Buffer Overflow

- The main cause for the problem of buffer overflow vulnerabilities is the fact that in many languages, such as C, bounds are not checked when arrays are accessed.
- Buffer is a contiguous block of computer memory that holds multiple instances of the same type. Overflow means to fill more than full. Buffer Overflow happens when a program attempts to write data outside of the memory allocated for that data.
- In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information.
- The stack is a section of memory used for temporary storage of information. In a stack-based buffer overflow attack, the attacker adds more data than expected to the stack, overwriting data. For example, "Let's say that a program is executing and reaches the stage where it expects to use a postal coder or zip code, which it gets from a Web-based form that customers filled out."

- The longest postal code is fewer than twelve characters, but on the web form, the attacker typed in the letter "A" 256 times, followed by some other commands. The data overflows the buffer allotted for the zip code and the attacker's commands fall into the stack. After a function is called, the address of the instruction following the function call is pushed onto the stack to be saved so that the function knows where to return control when it is finished.
- Fig. 4.8.1 shows buffer overflow attack.

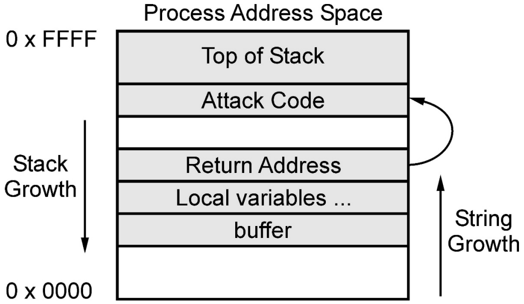


Fig. 4.8.1 : Buffer overflows attack

- A buffer overflow allows the attacker to change the return address of a function to a point in memory where they have already inserted executable code. Then control can be transferred to the malicious attack code contained with the buffer, called the payload.
- The payload is normally a command to allow remote access or some other command that would get the attacker closer to having control of the system.
- C language example :

```
#define BUFSIZE 128
int main(int argc, char **argv)
{
char buf[BUFSIZE];
strcpy(buf, argv[1]);
}
```

- The buffer size is fixed, but there is no guarantee the string in argv[1] will not exceed this size and cause an overflow.

4.8.1 Stack Based Buffer Overflows

- A stack is contiguous block of memory which is used by functions, two instructions are used to put or remove data from stack, “PUSH” puts data on stack, & “POP” removes data from stack. The stack works on Last in First out “LIFO” basis.
- Stack based buffer overflows affects any function that copies input to memory without doing bounds checking. For example: Strcpy(),memcpy(),gets()etc…
- A buffer overflow occurs when a function copies data into a buffer without doing bounds checking. So if the source data size is larger than the destination buffer size this data will overflow the buffer towards higher memory address and probably overwrite previous data on stack.

4.8.2 Heap-based Buffer Overflows

- A heap overflow is a form of buffer overflow; it happens when a chunk of memory is allocated to the heap and data is written to this memory without any bound checking being done on the data. This is can lead to overwriting some critical data structures in the heap such as the heap headers, or any heap-based data such as dynamic object pointers, which in turn can lead to overwriting the virtual function table.
- Function longjump( ) in C allows the programmer to explicitly jump back to functions, not going through the chain of return addresses. Function setjmp() uses environment data to store the point where longjmp() should return. If we can overwrite it to point to the attack code, longjmp() jumps to that.

4.8.3 Tools Used to Protect Buffer Overflow

1. **Libsafe :** It provides a combination of static and dynamic intrusion prevention. Statically it patches library functions in C language. A range check is made before the actual function call. Libsafe uses the old base pointer pushed onto the stack after the return address. No local variable should be allowed to expand further down the stack than the beginning of the old base pointer. The boundary is imposed by overloading the functions with wrapping functions. Fig. 4.8.2 shows memory layout for Libsafe.

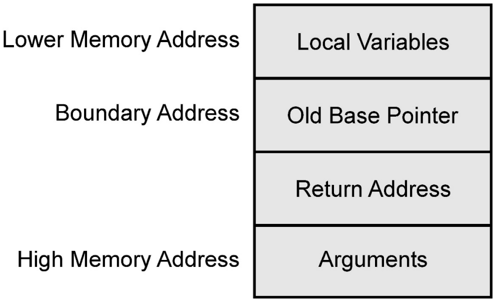


Fig. 4.8.2 : Memory layout for Libsafe

2. **StackGuard :** StackGuard is a systematic compiler tool that prevents a broad class of buffer overflow security attacks from succeeding. If we place a dummy value in between the return address and the stack data above, and then check whether this value has been over-written or not before we allow the return address to be used, we could detect this kind of attack and possibly pre-vent it. The inventors have chosen to call this dummy value the **canary.**

- StackGuard is a small set of patches to gcc. StackGuard is available both as a patch to gcc 2.7.2.2.

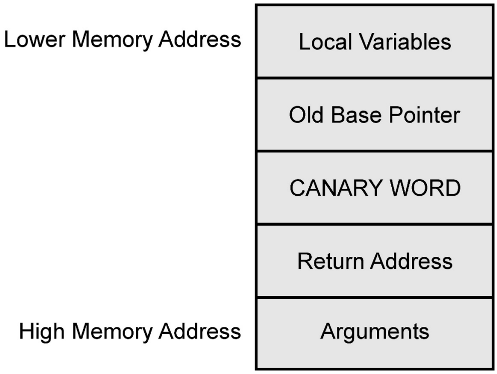


Fig. 4.8.3 : StackGuard stack frame

4.9 Steganography

- Steganography is the science of hiding information. The purpose of steganography is covert communication-to hide the existence of a message from a third party.
- Information hiding generally relates to both water-marking and steganography. A watermarking system's primary goal is to achieve a high level of robustness. It should be impossible to remove a watermark with-out degrading the data object's quality.
- Steganography is used for high security and capacity, which often entails that the hidden information is breakable. Fig. 4.9.1 shows a common taxonomy of steganographic techniques

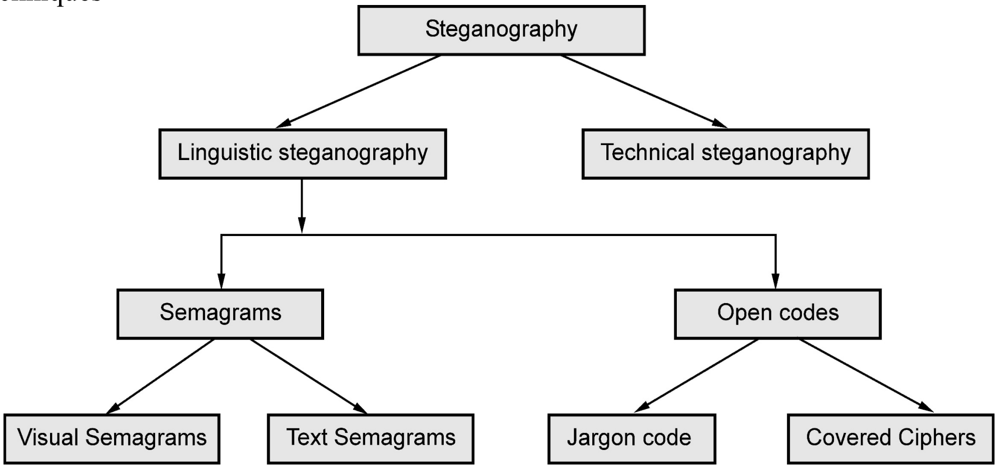


Fig. 4.9.1 : Taxonomy of steganographic techniques

- Technical Steganography: It uses scientific methods to hide a message.
- Linguistic Steganography: It hides the message in the carrier in some non-obvious ways and is further categorized as semagrams or open codes.
- Semagrams : It uses symbol or signs for information hiding.
- A visual semagram uses normal physical objects to convey a message.

- A text semagram hides a message by modifying the appearance of the carrier text.
- Open codes hide a message in a legitimate carrier message in ways that are not obvious to an unsuspecting observer.
- Jargon code uses language that is understood by a group of people but is meaningless to others.
- The goal of steganography is to avoid the detection or even raising the suspicion that a secret message is being passed on. Steganalysis is the art of detecting these covert messages. It involves the detection of embedded messages. The types of steganalysis attacks are similar to those of cryptanalysis attacks.

➤ Steganography Tools

1. **MP3Stego :** Hide files within mp3 files. MP3Stego will hide information in MP3 files during the compression process. The data is first compressed, encrypted and then hidden in the MP3 bit stream.
2. **TextHide :** Simple text Steganography
3. **wbStego :** This tool used for bitmaps, text files, HTML files and PDF files Steganography.
4. **Hide4PGP** is a freeware program distributed as source code in ANSI C and precompiled executables for DOS and the Win32 console

4.9.1 Difference between Steganography and Cryptography

Steganography	Cryptography
Output of information hiding is the stego-media.	Output in cryptography is a cipher text
It hides information	It does not hides information
Additional carrier is needed	Additional carrier is not needed
Steganography does not alter secret of message but hides inside the cover image	In cryptography, the structure of message is scrambled to make it meaningless
In steganography the secret message embeds in a harmless looking cover such as a digital image file, then the image file is transmitted.	Cryptography is the science of using mathematics to encrypt and decrypt data

4.10 Malware Threats

- “Malware” is short for malicious software and used as a single term to refer to virus, spy ware, worm etc. Malware is designed to cause damage to a stand-alone computer or a networked PC.
- Malware is any software intentionally designed to cause damage to a computer, server or computer network.

- Malware does the damage after it is implanted or introduced in some way into a target's computer and can take the form of executable code, scripts, active content, and other software.
- A common step to protect your computers and mobile devices from malware is to install anti-virus software from trusted vendors. Anti-virus, sometimes called anti-malware, is security software designed to detect and stop malicious software

➥ 4.10.1 Trojan Horse

- The city of Troy was protected by a high wall built around the city. Greeks attacked to one of the Troy's cities. After an unsuccessful attack, Greeks made a great plan to win.
- There plan was to build a horse, a beautiful and huge wooden horse, and leave it outside the gate. Then, the entire Greek army would pretend to leave, as if they had finally admitted defeat. But the horse would be hollow. Thirty men would be hiding inside. Horse is left it in front of the Troy's gate.
- The troy's civilians thought that it was a gift and brought that horse which is called Trojan into the city. That night, while the Trojan people were sleeping, the men hiding inside the wooden horse climbed out and opened the gates. Greek militaries destroyed the whole city.
- The applications works like this story and it is one of the most popular applications which is used for attacking computers. Trojan horse is not a virus and it do not do replicate.
- Trojan horse is malicious code hidden in an apparently useful host program. When the host program is executed, trojan does something harmful or unwanted.
- Trojan horses are programs that enter a system or network under the guise of another program. A Trojan horse may be included as an attachment or as part of an installation program. The Trojan horse could create a backdoor or replace a valid program during installation.

➤ How can your computer be infected by Torjan Horse?

1. **Websites :** You can be infected by visiting a bogus website. Internet Explorer is most often targeted by makers of Trojans. Even using a secure web browser, such as Mozilla's Firefox, if Java is enabled, your computer has the potential of receiving a Trojan horse.
2. **Instant message :** Many get infected through files sent through various messengers.
3. **E-mail :** Attachments on e-mail messages may contain Trojans.

➤ Objectives of Trojan horse Programs

1. It creates a backdoor and allows remote access to control your computer
2. Keystrokes are recorded to steal password and bank account information.
3. Destroy or delete data.
4. Uploading or downloading files
5. Your activity is monitored by camera and send to remote location.

➤ How to avoid getting infected with Trojan horse?

a. Install latest security patches for the operating system

b. NEVER download any type of software which you are not guarantee about that web site.

c. Install a secure firewall

d. Even if the file comes from a friend, you still must be sure what the file is before opening it

e. NEVER use features in your programs that automatically get or preview files

f. Never blindly type commands that others tell you to type.

g. Do regular backup of your system

➥ 4.10.1.1 Types of Trojan Horses

1. Remote Access Trojans
2. Data Sending Trojans
3. Destructive Trojans
4. Proxy Trojans
5. FTP Trojans
6. Security software disabler Trojans
7. Denial-of-service attack Trojans

➤ Example of a simple Trojan horse

1. Simple example of a Trojan horse would be a program named "waterfalls.scr" where its author claims it is a free waterfall screensaver. When run, it instead unloads hidden programs, commands, scripts, or any number of commands with or without the user's knowledge or consent.
2. AIDS also known as Aids Info Disk or PC Cyborg Trojan, is a trojan horse that replaces the AUTOEXEC.BAT file, which would then be used by AIDS to count the number times the computer has booted. Once this boot count reaches 90, AIDS hides directories and encrypts the names of all files on drive.
3. Dmsys is a dangerous Trojan that specializes in infecting various instant messengers and stealing user confidential information.

➥ 4.10.2 Backdoors

- A backdoor is any hidden method for obtaining remote access to a computer. A Backdoor is a remote administration utility that allows a user access and control a computer, usually remotely over a network or the Internet.
- Backdoor is also called trapdoor. It is an undocumented entry point to a module. A backdoor's goal is to remove the evidence of initial entry from the system's log files

- Backdoors can be installed for accessing a variety of services; of particular interest for network security are ones that provide interactive access. It frequently run over protocols such as Telnet and Rlogin or SSH.
- Backdoor is difficult to detect. A common method for masking their presence is to run a server for a standard service such as Telnet, but on an undistinguished port rather than the well-known port associated with the service.
- Network administrators often use backdoors to control their clients and supervise their actions in a business network.
- Backdoors are usually based on a client-server network communication, where the server is the attacked machine and the client is the attacker. It is a kind of standard. This is called direct connection, when the client directly connects to the server.
- Remote Administration Trojans (RATs) are a class of backdoors used to enable remote control over a compromised machine.
- RATs are used by the attacker with malicious intent to surveillance the infected victim by recording audio, video, keystrokes, in addition RATs enable attacker to run services from the victim's computer, it is also capable of exfiltrating files, and more.

4.11 Virus

- The term computer virus was originally used by Dr. Fred Cohen in his PhD thesis, in 1986. The term malware will be used to describe all forms of malicious software. The term virus writer will be used to describe the person who is responsible for creating all types of malicious software.
- A computer virus is a small program that can copy itself to infect computers. Self-replicating programs that spread by infecting other programs or data files. A Virus is a malicious program that spreads using a propagation technique that generally requires user intervention, and always possesses a malicious intent.
- A virus infects another executable and uses this carrier program to spread itself. The virus code is injected into the previously benign program and is spread when the program is run.
- A computer virus requires some sort of user action to abet their propagation. A virus program infects other programs by modifying them.
- A major **component of virus** is an *infection code, payload and trigger*.
  1. Infection code : This is the part that locates an infectable object.
  2. Payload : Any operation that any other program can do but is usually something meant to be possibly destructive.
  3. Trigger : Whatever sets it off, time-of-day, program execution by user.
- Viruses usually have two phases :
  1. **Infection phase :** Virus reproduce as widely as possible without being detected
  2. **Attack phase :** Virus an attempt to carry out whatever damage they were designed to inflict

- A virus is dependent upon a host file or boot sector, and the transfer of files between machines to spread. A virus can be either **transient or resident.**
  1. **Transient virus :** Runs when its attached program executes and terminates when its attached program ends
  2. **Resident virus :** Locates itself in memory so that it can remain active even after its attached program ends
- Virus cannot be completely invisible but can be very hard to detect, especially if it has self modifying code. The code it executes can be identified and a program can scan for entire code. Usually it is at the start of a program or maybe a test and jump to code at the bottom of the file.
- If the virus writer wants to keep the program size the same to prevent detection then it has to replace some of the program code or compress the program and prepaid the virus to the program. But a good scanner with a checksum can detect the changes in the code.
- Virus program can be small so it hides very easily in a large program. It might hide in a compiler, a data base manager or a file manager.Macro virus so named because it's a macro in Microsoft Word, Excel and others. The number one spot is an attachment to email or some public download file.
- Virus code is both prepended and appended to the host file. Virus code could be split into several segment and interspersed throughout the infected file using JUMP statement at the end of each virus segment.
- Fig. 4.11.1 shows virus infected host file.Host file is not damage and easy to clean the file. It is called prepended.

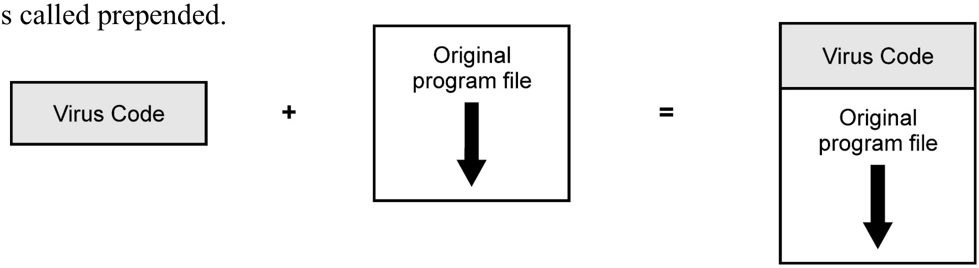


Fig. 4.11.1(a) : Prepended virus infected host file

- Virus does not damage host file but it is difficult to remove the virus from file.

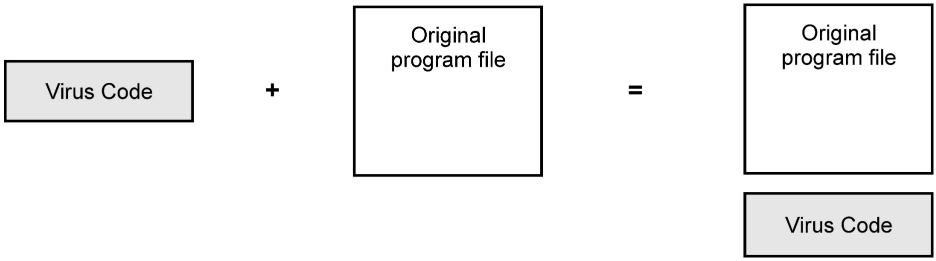
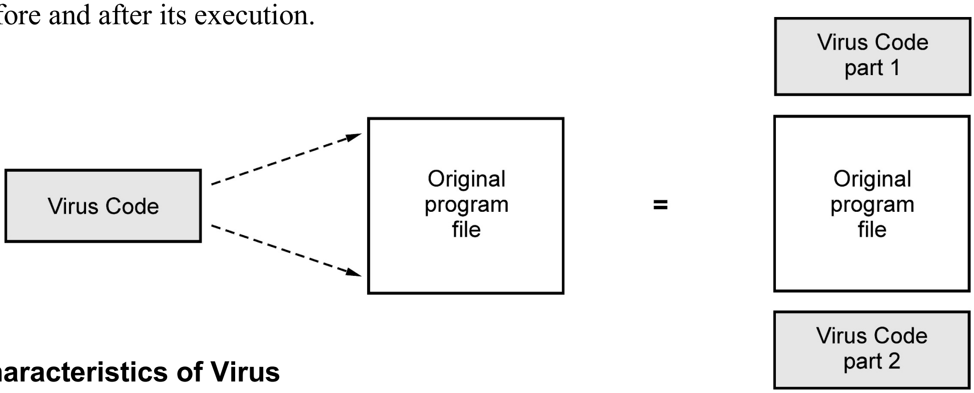


Fig. 4.11.1(b) : Appended virus infected host file

- **Viruses that surround a program :** Virus code runs the original program but has control before and after its execution.



➤ Characteristics of Virus

1. Propagates when the host program is executed
2. All the virus code need not be located at the start of the infected file.
3. Virus makes a set of system call.

➤ Preventing Virus Infection

- Ways to prevent Virus infections
  1. Test all new software on an isolated computer.
  2. Use only commercial software acquired from reliable, well established vendors.
  3. Do not put a floppy disk in the machine unless it has been scanned first.
  4. Do not open attachments to email unless they have been scanned. Including turn off the auto open of attachments in mail readers.
  5. Scan any downloaded files before they are run.
  6. At least once a week update the virus signature data files.
- Make a bootable disk/CD with a virus scan program on it and write protected.
- Make and retain backup copies of executable system files in the event the virus detection program can't remove the virus.

➡ 4.11.1 Phases of Viruses

- During its lifecycle, virus goes through following phases :

1. Dormant phase	2. Propagation phase
3. Triggering phase	4. Execution phase

- **Dormant phase :** The virus is idle. It is activated by some event.
- **Propagation phase :** During this phase, the virus is replicating itself, infecting new files on new systems. Virus will typically not propagate to another infected program.
- **Triggering phase :** The virus is activated to perform the function for which it was intended. It is caused by a variety of system events.

- **Execution phase :** In this phase, the virus performs the malicious action that it was designed to perform, called payload. This action could include something seemingly innocent, like displaying a silly picture on a computer's screen, or something quite malicious, such as deleting all essential files on the hard drive.

➥ 4.11.2 Types of Virus

1. **Boot Sector Virus :** It infects a master boot record or partition boot record and spreads when a system is booted from the disk containing the virus. Virus gains control very early in the boot process before most detection tools are active. Operating systems usually make files in the boot area invisible to the user, therefore, virus code is not readily noticed.
2. **File Infector :** This type of virus infects files that the operating system or shell consider to be executable. File viruses infect executable files.Most really successful file infectors are classified as Worms.
3. **Macro Virus :** Infects files with macro code that is interpreted by an application.
4. **Appended Viruses :** Virus code attaches itself to a program and is activated whenever the program is run.
5. **Integrated Viruses :** This type of virus replace some of the target program or the entire target and give the effect that the target program worked.
6. **Document Virus :** This virus is implemented within a formatted document. For example database, written document, picture, spreadsheet and slide presentation. Document is structured files which contains data and commands. Commands are part of programming language. Virus uses features of programming language to perform malicious actions.
7. **Macro Viruses :** A macro is an executable program embedded in a word processing document (MS Word) or spreadsheet (Excel). When infected document is opened, virus copies itself into global macro file and makes itself auto-executing. Melissa was really successful macro virus.
8. **Metamorphic Virus :** A metamorphic virus mutates with every infection. Virus rewrites itself completelyateach iteration, increasing the difficulty of detection. Some even have the ability to dynamically disassemble themselves, change their code, and reassemble themselves into an executable form. It may change their behavior as well as their appearance in every incarnation.
9. **Memory Resident Viruses :** Memory resident viruses remain in memory after the initialization of virus code. They take control of the system and allocate a block of memory for their own code. They remain in memory while other programs run and infect them.
10. **E-mail Viruses :** If the recipient opens the email attachment, the Word Macro is activated. Thee-mail virus sends itself to everyone on the mailing list in the user's e-mail package. The virus does local damage. The first rapidly spreading e-mail viruses, such as Melissa, made use of a Microsoft Word Macro embedded in an attachment.
11. **Polymorphic Virus :** A virus can change its appearance is called a polymorphic virus.
12. **Stealth Virus :** Virus explicitly designed to hide itself from detection by antivirus software. Thus, the entire virus, not just a payload is hidden.
13. **Multipartite Viruses :** Viruses that use more than one infection mechanism like file and boot viruses.

➥ 4.11.3 Virus Countermeasures

- Prevention is best solution for virus. A countermeasure is an action, process, device, or system that can prevent, or mitigate the effects of, threats to a computer, server or network.
- **Antivirus software** mainly prevents and removes computer viruses, including worms and trojan horses. Such programs may also detect and remove adware, spyware, and other forms of malware.
  1. Prevention : Do not allow a virus to get into the system
  2. Detection : Once infection has occurred, determine that it has occurred and locate the virus;
  3. Identification : Once a virus is detected, identify it;
  4. Removal : Once the specific virus has been identified, remove all traces of the virus and restores the infected programs to their original states.

➤ Generations of antivirus software

- Four generations of antivirus software are

➤ 1. First generation : - simple scanners

- This type of scanners typically looked for certain patterns or sequences of bytes called string signatures.
- Virus may contain wildcards. Such signature-specific scanners are limited to the detection of known viruses.
- Program size and length is maintained by scanner. It program length is compared before and after.
- Once a virus is detected, it can be analyzed precisely and a unique sequence of bytes extracted from the virus code.

➤ 2. Second generation :- heuristic scanners

- The scanner uses heuristic rules to search for probable virus infection.
- Smart scanning refers to a defense optimizing method for the newer generation of viruses, which try to conceal their code within a sequence of worthless instructions such as no operation NOP instructions.
- The heuristics analysis is a useful method for detection of new unknown malwares. It is especially helpful for detection of macro viruses too.

➤ 3. Third generation :- activity traps

- Third-generation programs are memory-resident programs that identify a virus by its actions rather than its structure in an infected program.
- Memory-resident programs that identify a virus by its actions in run time rather than by its signature or its structure.
- It is necessary to identify the small set of indicative actions

4. Fourth generation : - full featured protection

- Fourth-generation products are packages consisting of a variety of antivirus techniques used in conjunction. These include scanning and activity trap components.
- Packages consisting of a variety of antivirus techniques used together: Scanning; Activity trap and Control capability.

4.12 Worm

- A worm is a sophisticated piece of replicating code that uses its own program coding to spread, with minimal user intervention. A worm usually exists as a standalone program that executes itself automatically on a remote machine, without any user interaction. Worms are network viruses, primarily replicating on networks.
- Worm infects the environment rather than specific objects. Unlike a virus, does not require a host to propagate.
- The Morris worm or Internet worm was one of the first computer worms distributed via the Internet. Morris worm uses topological techniques. Topological worm searches for local information to find new victims by trying to discover the local communication topology.
- Passive worm does not seek out victim machines. Instead, it either waits for potential victims to contact the worm or rely on user behavior to discover new targets

4.12.1 Worm Classification

Worms can be classified according to the following categories :

1. **Stealth worms** do not spread in a very rapid fashion but instead they spread in a slow. This worm is very hard to detect.
2. **Polymorph worms** can change themselves during propagation in order to make signature-based detection more complicated.
3. **File worms** are a modified form of viruses, but unlike viruses they do not connect their presence with any executable file. When they multiply, they simply copy their code to some other disk or directory hoping that these new copies will someday be executed by the user.
4. **Multi-vector worms** use different propagation methods in order to make more hosts vulnerable for attack and effectively propagate behind firewalls.
5. **Email worms** email themselves to other email addresses and make the user execute email attachments with malicious code or use bugs in the email programs to get attachments executed automatically.

4.12.2 Difference between Worm and Virus

Worm	Virus
A worm has ability to self-propagate, and may or may not have malicious intent computer worm is a program that self-propagates across a network exploiting security or policy flaws.	A virus is a malicious program that spreads using a propagation technique that generally requires user intervention, and always possess a malicious intent

Worm	Virus
Worms do not need hosts.	Virus needs hosts
Worm can spread quicker than virus	Virus can spread slower than worm
Example : Self modified virus, stealth virus	Example : Multi-vector worm, Email worm

4.13 University Question Case Study

Q. 1 A public institution was the victim of a hacker. The subject got into the network and placed several large media files on several computers and changed the desktop configurations. Management decided against calling law enforcement initially (because of media attention) and instructed the IT department to get a CFS to privately investigate. How did the CFS go about conducting the investigation? **AU : Dec.- 19, 15 Marks**

Ans. :

- This case study is related to Information and Tactics of Terrorists and Rogues.
- CFS team performed forensic analysis of the hard drives. Try to find or trace IP address and any other information using by the hackers.
- Here it is necessary to perform detail analysis of forensic analysis of the hard drives and investigation.
- Using a combination of forensic analysis of the hard drives and investigation (tracing IP addresses, etc.), a CFS was able to identify the hacker, which would enable law enforcement to obtain a search warrant if the client elected to press charges.
- Disk forensics is the science of extracting forensic information from digital storage media like Hard disk, USB devices, Firewire devices, CD, DVD, Flash drives, Floppy disks etc.. The process of Disk Forensics are :
  1. Identify digital evidence
  2. Seize & Acquire the evidence
  3. Authenticate the evidence
  4. Preserve the evidence
  5. Analyze the evidence
  6. Report the findings
  7. Documenting
- The Windows Registry plays a crucial role in the operation of a PC.The registry keeps track of user and system configuration and preferences, which is no simple task. From a forensic standpoint, it can provide an abundance of potential evidence.
- Many of the artifacts we look for are kept in the registry. Some of the potential evidence could include search terms, programs that were run or installed, web addresses, files that have been recently opened, and so on.

4.14 Questions with Answers

4.14.1 Two Marks Questions with Answers

Q. 1 What is ethical hacking?

Ans. : Ethical hacking is an authorized practice of bypassing system security to identify potential data breaches and threats in a network.Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses

Q. 2 Define malicious program.

Ans. : A program that is intentionally included or inserted in a system for harmful purpose is malicious program.

Q. 3 What is a virus ?

Ans. : A virus is a piece of program code that can infect other programs by modifying them.

Q. 4 What is a worm ?

Ans. : A worm is a program designed to copy itself and send copies from a computer to other computer across the network.

Q. 5 What is trojan horse ?

Ans. : A trojan horse is a computer program that appears to be useful but that actually does damage

Q. 6 Enlist 4-types of viruses.

Ans. :

1. Parasitic virus
2. Memory resident virus
3. Boot sector virus
4. Stealth virus.

Q. 7 What are the steps in virus removal process ?

Ans. :

1. Detection of virus
2. Identification of virus
3. Removal of traces of virus

Q. 8 Differentiate macro Virus and boot Virus.

Ans. : A macro virus is platform independent virtually all of the macro viruses infect MS Word documents. Macro viruses take advantage of a feature found in Word and other office applications such as Microsoft Excel, namely the macro. Boot sector virus infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus

Q. 9 Define keyloggers.

Ans. : A keylogger is a type of surveillance software that has the capability to record every keystroke you make to a log file. A keylogger recorder can record instant messages, e-mail, and any information you type at any time using your keyboard.

Q. 10 What is steganography?

Ans. : Steganography is the science of hiding information. The purpose of steganography is covert communication-to hide the existence of a message from a third party.

Q. 11 What is footprinting ?

Ans. : Footprinting is process of collecting as muchinformation as possible about a target system/network for identifying different ways of intrudingan organization's network.

Q. 12 What is reconnaissance ?

Ans. : Reconnaissance is the act of gaining information about our target. Such as open ports, operating system, what services those ports are running, and any vulnerable applications they have installed. All of this information will be absolutely vital to choosing an attack.

Q. 13 What is network scanning ?

Ans. : Network scanning is a procedure for identifying active hosts on a network, either for the purpose of attacking them or for network security assessment. In the enumeration phase, the attacker gathers information such as network user and group names, routing tables, and Simple Network Management Protocol (SNMP) data.

Q. 14 Define port scanning.

Ans. : Port scanning refers to the surveillance of computer ports, most often by hackers for malicious purposes. Hackers conduct port-scanning techniques in order to locate holes within specific computer ports. For an intruder, these weaknesses represent opportunities to gain access for an attack. There are 65,535 ports in each IP address, and hackers may scan each and every one to find any that are not secure.

4.14.2 Multiple Choice Questions with Answers

Q. 1 Linux OS stores password file in _________ directory.

(a) /etc/shodow (b) /etc/bin (c) /usr (d) /bin

Ans. : (a) /etc/shodow

Q. 2 In windows SAM stands for _________.

(a) security add manager (b) separate account manager

(c) security accounts manager (d) all of above

Ans. : (c) Security account manager

Q. 3 Nitko tool is written in _________ Language.

(a) Java (b) Python (c) C (d) Perl

Ans. : (d) Perl

Q. 4 Vulnerability tool W3af stand for

(a) Web application attack and audit framework

(b) Web three attack forum

(c) Web app framework

(d) Web three attach file

Ans. : (a) Web application attack and audit framework

Q. 5 Following which tool provides encrypted connection to client or server.

(a) CURL (b) Stunnel (c) OpenSSL (d) Nitko

Ans. : (b) Stunnel

Q. 6 Damn vulnerable web app needs _________ server and _________ server.

(a) Proxy, Apache (b) Apache, email

(c) Apache, MySQL (d) MySQL, Proxy

Ans. : (c) Apache, MySQL

Q. 7 Which of the following in NOT cracking mode of John Ripper ?

(a) Wordlist mode (b) Single crack mode

(c) Incremental mode (d) Internal mode

Ans. : (d) internel mode

Q. 8 The tool _________ is divide in two main parts:core and plugins

(a) CURL (b) Openssl (c) W3af (d) Nikto

Ans. : (c) W3af

Q. 9 Windows NT stores passwords in two formats : _________ and _________.

(a) LM hash and NT hash (b) ASCII and binary

(c) LANMAN and NT hash (d) LM hash and LANMAN

Ans. : (a) LM hash and NT hash

Q. 10 PEM stands for _________.

(a) Public Encryption Mail (b) Privacy Enhanced Mail

(c) Privacy Enhanced Message (d) Public Encryption Message

Ans. : (b) Privacy Enhanced Mail

Q. 11 Which one of the following is not an attack, but a search for vulnerabilities to attack?

(a) Denial of service (b) Port scanning

(c) Memory access violation (d) Dumpster diving

Ans. : (b) port scanning

Q. 12 In RADIUS any user passwords are sent _________.

(a) encrypted format (b) hashed format

(c) in text format. (d) none of all

Ans. : (a) Encrypted format

Q. 13 Which of the following is not considered good practice for password security?

(a) Changing the password on a regular basis

(b) Using a combination of upper- and lower-case characters, a number, and a special character in the password

(c) Not writing the password down

(d) Using less than eight characters long

Ans. : (d) Using less than eight characters long

Q. 14 Buffer overflow, SQL injection, and stack smashing are examples of:

(a) Vulnerabilities (b) Exploits

(c) Input attacks (d) Injection attacks

Ans. : (c) Input attacks

Q. 15 The software or hardware component that records each keystroke a user enters into a word processing document is called a _________.

(a) sniffer (b) keylogger (c) trojan program (d) buffer overflow

Ans. : (b) Keylogger

Q. 16 What type of network attack relies on multiple servers participating in an attack on one host system?

(a) Trojan attack (b) Buffer overflow

(c) Denial of service attack (d) Distributed Denial of service attack

Ans. : (d) Distributed Denial of service attack

Q. 17 Rootkits can be difficult to detect because :

(a) They are encrypted

(b) They are polymorphic

(c) They reside in ROM instead of the hard drive

(d) They use techniques to hide themselves

Ans. : (d) They use techniques to hide themselves

Q. 18 A program that fills a computer system with self-replicating information thus clogging the system is called a _________.

(a) virus (b) worm (c) denial-of-service attack (d) damage

Ans. : (b) worm

Q. 19 _________ is a computer virus encoded as a macro in programs that support a macro language.

(a) virus (b) macro virus (c) worm (d) trojans

Ans. : (b) micro virus

Q. 20 The pattern that can be used to identify a virus is known as _________.

(a) stealth (b) virus signature (c) armoured (d) multipartite

Ans. : (b) virus signature

Q. 21 A program that migrates through networks and operating systems and attaches itself to different programs and databases is a __________.

(a) virus (b) worm (c) denial-of-service attack (d) damage

Ans. : (a) virus

Q. 22 Which statement best describes a worm?

(a) A virus that is designed to destroy your hard drive

(b) A virus that is designed to frighten people about a nonexistent virus

(c) A virus that doesn't attach itself to programs and databases

(d) A virus that is designed to shut down a server

Ans. : (c) A virus that doesn't attach itself to programs and databases

Q. 23 An attempt to slow down or stop a computer system or network by flooding the system with requests for information is called a

(a) virus (b) worm (c) denial-of-service attack (d) Trojan horse

Ans. : (c) denial-of-service attack

Q. 24 _________ is a computer virus encoded as a macro in programs that support a macro language.

(a) virus (b) macro virus (c) worm (d) trojans

Ans. : (b) micro virus

Q. 25 _________ is a computer program that replicates and propagates itself without having to attach itself to a host.

(a) virus (b) worm (c) trojan (d) spyware

Ans. : (b) worm

Q. 26 Nimda and code red are _________.

(a) Viruses (b) Spyware (c) Worms (d) Adware

Ans. : (c) worms

Q. 27 What is the main purpose of malware?

(a to learn passwords (b) to do harm to a computer system

(c) to discover open ports (d) to identify an operating system

Ans. : (b) to do harm to a computer system

Q. 28 The software or hardware component that records each keystroke a user enters into a word processing document is called a ________

(a) sniffer (b) keylogger (c) trojan program (d) buffer overflow

Ans. : (b) keylogger

Q. 29 What type of network attack relies on multiple servers participating in an attack on one host system?

(a) Trojan attack (b) Buffer overflow

(c) Denial of service attack (d) Distributed Denial of service attack

Ans. : (d) Distributed Denial of service attack

Q. 30 What are the types of scanning ?

(a) Port, network, and services (b) Network, vulnerability, and port

(c) Passive, active, and interactive (d) Server, client, and network

Ans. : (b) Network, vulnerability and port

❑❑❑

UNIT - V

5 Ethical Hacking in Web

Scope of the Syllabus

Social Engineering - Denial of Service - Session Hijacking - Hacking Web servers - Hacking Web Applications - SQL Injection - Hacking Wireless Networks - Hacking Mobile Platforms.

5.1 Social Engineering

- Social engineering is the art of manipulating people so they give up confidential information.
- Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password.
- Social engineering is important to understand because hackers can use it to attack the human element of a system and circumvent technical security measures.
- It is a way for criminals to gain access to information systems. The purpose of social engineering is usually to secretly install spyware, other malicious software or to trick persons into handing over passwords and/or other sensitive financial or personal information.
- Social engineers use various tricks to convince their victims to give out sensitive information. In a very simple social engineering attack, an attacker would call his victim, pretend to be a bank official, and then ask the victim for his credit card number and PIN.
- The victim would give away the details, believing the call was really from an authorized bank official. All the information that is gathered through various footprinting techniques is very useful in building successful social engineering attacks.
- Phases of social engineering :
  1. **Research and information gathering :** The attacker does comprehensive research on the target organization through various information sources. Social networking sites, job boards, and people search engines give out a lot of valuable information.

2. **Choosing the victim/target :** Based on the information collected, the attacker then analyzes and chooses the most vulnerable person who could reveal sensitive information to engage with.
3. **Establish trust relationship :** Once the victim has been chosen, the attacker communicates with the victim through various ways, like instant messaging, email,or a direct call. The attacker claims to be someone the victim can relate to and trust.
4. **Exploit the relationship :** The attacker now tries to exploit the established trust relationship. By engaging the victim in deceptive talk, the attacker tries to extract as much as information as possible.

- Social engineering can be broken into two common types :
  1. Human-based social engineering refers to person-to-person interaction to retrieve the desired information. An example is calling the help desk and trying to find out a password.
  2. Computer-based social engineering refers to having computer software that attempts to retrieve the desired information. An example is sending a user an e-mail and asking them to reenter a password in a web page to confirm it. This social-engineering attack is also known as phishing.

➤ Common social engineering attacks :

- Social engineering is a tactic used by cyber criminals that uses lies and manipulation to trick people into revealing their personal information.
- Social engineering attacks frequently involve very convincing fake stories to lure victims into their trap. Common social engineering attacks include :
  1. Sending victims an email that claims there's a problem with their account and has a link to a fake website. Entering their account information into the site sends it straight to the cyber criminal (phishing).
  2. Trying to convince victims to open email attachments that contain malware by claiming it is something they might enjoy (like a game) or need (like anti-malware software).
  3. Pretending to be a network or account administrator and asking for the victim's password to perform maintenance.
  4. Claiming that the victim has won a prize but must give their credit card information in order to receive it.
  5. Asking for a victim's password for an Internet service and then using the same password to access other accounts and services since many people re-use the same password.
  6. Promising the victim, they will receive millions of dollars, if they will help out the sender by giving them money or their bank account information.

5.2 Denial of Service

- The goal of a denial of service attack is to deny legitimate users access to a particular resource. An incident is considered an attack if a malicious user intentionally disrupts service to a computer or network resource.

- The SYN attack is denial of service attack. It is related to TCP connection setup. In a SYN attack, a remote attacker floods user machine with SYN packets, causing it to spend all its cycles setting up bogus TCP connections.
- Telnet protocol establish virtual connection with server is called session. Session is established with three way TCP handshake protocol. Each TCP packet has flag bits, two of which are denoted SYN and ACK. To establish a TCP connection, the originators send a packet with the SYN bit on.
- If the recipient is ready to establish a connection, it replies with a packet with both the SYN and ACK bits on. The first party then sends a packet with the ACK bits on. Sometime, packets get lost or damaged in transmission. Destination maintains a queue called SYN_RECV connection.
- If ACK or SYN-ACK packet is lost, the destination host will time out the incomplete connection and discard it from its waiting queue. The attacker can deny service to the target by sending many SYN requests and never responding ACK with ACKs, thereby filling the victim SYN_RECV queue and never processes it. This queue is small which contain up to 20 entries. Therefore the target system keeps on waiting. The result may be a hard disk crash or reboot.
- If a few SYN packets are sent by the attacker every 10 seconds, the victim will never clear the queue and stops to respond.
- Another DoS attack is to send a stream of packets to a router. Packets contains all bits turn on. The router spends so much time processing these options that it fails to process BGP updates.
- The denial of service attack does not result in information theft or any kind of information loss. DoS attacks affect the destination rather than a data packet or router.
- DoS attack affects a specific network service, such as e-mail or domain name system. One way of initiating this attack is by causing buffer overflow. Inserting an executable code inside memory can potentially by causing buffer overflow. Fig. 5.2.1 shows denial of service attack.

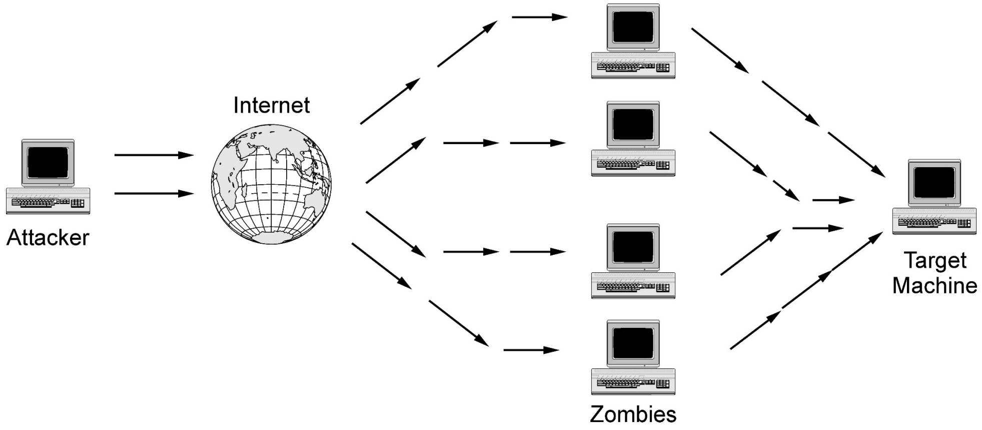


Fig. 5.2.1 : DoS Attack

- DoS attacks are easy to generate but difficult to detect.
- Protecting against DoS attack is as follows :
  1. Make a list of all resource consumed by every user.
  2. Detect when the resources consumed by a given user exceed those allowed by some system policy.
  3. After detecting attack, reclaim the consumed resources using as few additional resources as possible or removal of an offending user.
- **Classification of DoS Attacks**
  1. **Logic attacks :** This attack takes place in network software such as TCP/IP protocol stack or web server.
  2. **Protocol attacks :** Protocol is a set of rules. This attack takes place to specific feature or implementation bug.
  3. **Bandwidth attacks :** Attacker open many web pages and keep on refreshing for consuming more bandwidth. After some time web site becomes out of service.

➥ 5.2.1 Types of DoS Attacks

1. **Ping of death :** Ping of death attack sends large oversized ICMP packets. Maximum legal size of IP packets is 65535 bytes. Because of limitations in the physical layer, packets may have to be fragmented and then reassembled at the destination. So this packet is fragmented for transport. The receiver then starts to reassemble the fragments as the ping fragments arrive. The total packet length becomes too large. It may possible that system may crash.
2. **Smurf :** It is a variation of ping attack. Attacker selects a network of unwitting victims. The attacker spoofs the source address in the ping packet so that it appears to come from the victim. Then the attacker sends this request to the network in broadcast mode by setting the last byte of the address to all 1s.
3. **Teardrop attack :** This attack misuse a feature designed to improve network communication. Attacker sends a series of datagram that cannot fit together properly. One datagram might say it is position 0 for length 60 bytes, another position 30 for 90 bytes so on. These fragment pieces overlap so they can not be reassembled properly.
4. **Malicious misrouting of packets :** A attacker may attacks a router and change its routing table, resulting in misrouting of data packets, causing a denial of service.
5. Attacker send large number of UDP packets to non listing ports on the victim. This cause victim to respond with an ICMP Host Unreachable message for each packet that it receives.

➤ DoS Shortfalls

1. This type of attacks are unable to attack large bandwidth websites.

2. New distributed server architecture makes it harder for one denial of service to take down an entire site.
3. New software protections deactivate existing DoS attacks quickly
4. Service Providers know how to prevent these attacks from affecting their networks.

➥ 5.2.2 Distributed Denial of Service (DDoS) Attack

- In DDoS attack, a large number of hosts are used to flood unwanted traffic to a single target. The target cannot then be accessible to other users in the network, as it is processing the flood of traffic.
- Highly visible site like CNN, eBay and Yahoo were brought down by a DDoS attack in Feb 2000.
- In DDoS attack, the attacker scans the Internet to find multiple vulnerable hosts called handlers and comprises them. Each handler, in turn, recruits many agents to launch the attack.
- IP spoofing is a common technique used in almost all forms of attack.
- Botnets consist of a large number of "zombie" machines controlled by a single user which can be used to carry out all sorts of attacks. Network and protocol implementation loopholes can also be used for launching such attacks.
- Attackers can use different kinds of scanning techniquesin order to find vulnerable machines.
  1. **Hit-list scanning :** Long before attackers start scanning, they collect a list of a large number of potentially vulnerable machines.
  2. **Random scanning :** The machine that is infected by the malicious code probes IP addresses randomly from the IP address space and checks their vulnerability.

➤ How do you know if an attack is happening?

- The following symptoms could indicate a DoS or DDoS attack:
  a) Inability to access any website.
  b) Suddenly increase in the amount of spam you receive in your account
  c) Slowdown the network/Internet speed
  d) Particular website is unavailable
- DDoS attack consumes system resources thereby reducing the speed of computer. The resources attack can be classified as
  1. Internal resource attack
  2. Attacking data transmission resources

- Fig. 5.2.2 shows distributed denial of service attack.

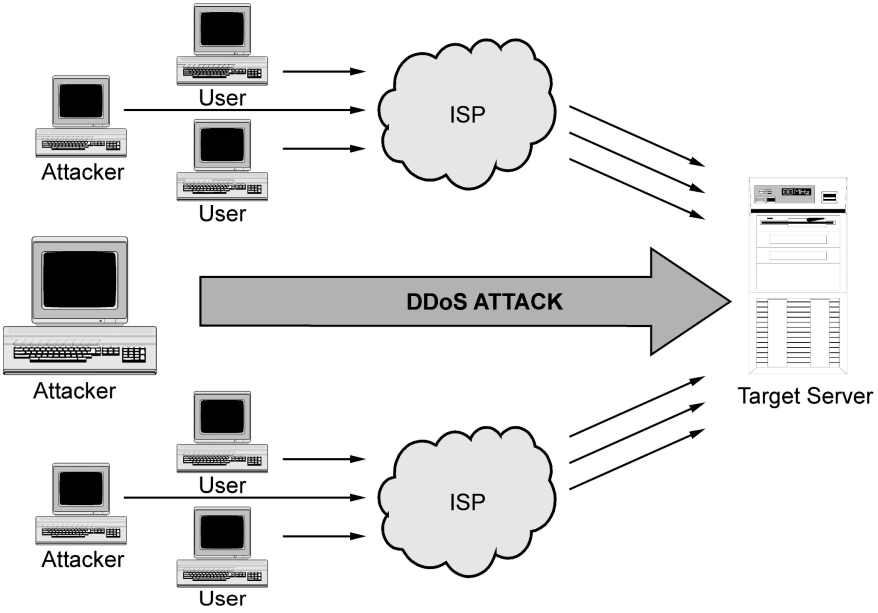


Fig. 5.2.2 : DDoS Attack

➥ 5.2.3 Widely Used DDoS Programs/Tools

1. **Trinoo :** This is the first DDoS Tool widely available. A trinoo network consists of a master host and many broadcast hosts. When an attacker wishes to launch a denial-of-service attack, he/ she issues commands to the master host using a TCP connection. The master then communicates with all of the broadcast hosts via UDP, telling them to send a flood of UDP packets to random ports on the specified target host. The flood of UDP packets coming from the broadcast hosts causes denial of service to the target host. An attacker must have prior access to a host in order to install a trinoo master or broadcast, either by breaking in or by some other means.
2. **TFN (Tribe Flood Network) :** TFN is a distributed denial of service tool that allows an attacker to use several hosts at once to flood a target. It has four different kinds of floods: ICMP Echo flood, UDP Flood, SYN Flood, and Smurf attack. The TFN client and server use ICMP echo reply packets to communicate with each other. The attacker uses the TFN client to control the remote servers and initiate the denial of service attack.
3. **Stacheldraht** is also based on the TFN and trinoo client/server model where a master program communicates with potentially many thousands of agent programs. The perpetrator connects to the master program to initiate the attack. Stacheldraht adds the new features: encrypted communication between the attacker and the master program, as well as automated updates of the agent programs using RCP.

- In a DoS attack, one computer and one internet connection is used to flood a server with packets, with the aim of overloading the targeted server’s bandwidth and resources.

- DDoS attack, uses many devices and multiple Internet connections, often distributed globally into what is referred to as a botnet. A DDoS attack is much harder to deflect, simply because there is no single attacker to defend from, as the targeted resource will be flooded with requests from many hundreds and thousands of multiple sources.

5.3 Session Hacking

- Session hijacking refers to the exploitation of a valid computer session where an attacker takes over a session between two computers. The attacker steals a valid session ID, which is used to get into the system and sniff the data.
- To perform session hijacking, an attacker needs to know the victim's session ID (session key). This can be obtained by stealing the session cookie or persuading the user to click a malicious link containing a prepared session ID.
- In both cases, after the user is authenticated on the server, the attacker can take over (hijack) the session by using the same session ID for their own browser session. The server is then fooled into treating the attacker's connection as the original user's valid session.
- Session Hijacking can be done at two levels: Network Level and Application Level. Network level hijacking involves TCP and UDP sessions, whereas Application level session hijack occurs with HTTP sessions.
- Session hijacking involves the following three steps to perform an attack:
  1. Tracking the session: The hacker identifies an open session and predicts the sequence number of the next packet.
  2. Desynchronizing the connection: The hacker sends the valid user's system a TCP reset (RST) or finish (FIN) packet to cause them to close their session.
  3. Injecting the attacker's packet: The hacker sends the server a TCP packet with the predicted sequence number, and the server accepts it as the valid user's next packet.

5.3.1 Types of Session hijacking

1. Active : In an active attack, the culprit takes over your session and stops your device from communicating with the web server, kicking you off. Posing as you, the criminal can perform actions only you would be able to. Depending on what website the session is taking place on, the hacker can then make online purchases, change passwords, or recover accounts as if they were you.
2. Passive : In a passive attack, you don't get kicked out of the session. Instead, the criminal quietly observes the data traffic between your device and the server, collecting your sensitive information. This way they can find out your passwords, credit card details, and other information without raising suspicions.

5.4 Hacking Web Server

- Web server is defined as an application that responds to web page requests submitted by various users over the Internet using the HTTP. The web server basically constitutes the interface between users and web based applications and databases.

- The applications/databases that users connect to through these Web servers are called websites. Any vulnerability occurring in the front end applications, database or OS can translate to Web Server vulnerabilities.

➤ Types of Web Server Vulnerabilities :

1. Web server software misconfiguration
2. Lack of proper security policies and procedures
3. Application bugs, or flaws in programming code
4. Vulnerable default installation of operating system and web server software

➤ Attacks against Web Servers :

- A website defacement is an attack on a website that changes the visual appearance of the site.
- A message is often left on the webpage. Most times the defacement is harmless, however, it can sometimes be used as a distraction to cover up more sinister actions such as uploading malware.
- Defacing a website means the hacker exploits a vulnerability in the operating system or web server software and then alters the website files to show that the site has been hacked. Often the hacker displays their hackername on the website's home page.
- A web site defacement consist of following key elements :
  1) A system with a vulnerability is identified and exploited, allowing unauthorized access by a malicious third party
  2) Existing web pages are modified or replaced with new text or graphics
  3) Something that an attacker might hope to accomplish as a result of a web site defacement
- Common website attacks that enable a hacker to deface a website include the following :
  1. Using man-in-the-middle attack, capture administrator credentials
  2. Compromising an FTP or e-mail server
  3. Misconfiguring web shares
  4. Using SQL injection attacks
  5. Using Telnet or Secure Shell intrusion
  6. Carrying out URL poisoning, which redirects the user to a different URL

➤ Patch Management Techniques

- Patch management is the process that helps acquire, test and install multiple patches (code changes) on existing applications and software tools on a computer, enabling systems to stay updated on existing patches and determining which patches are the appropriate ones. Managing patches thus becomes easy and simple.

- Generally, software patches can be categorized into three different categories: feature updates, bug fixes, and security updates.
  1. Feature patches: they improve software functionality and provide additional capabilities.
  2. Bug fix patches: they address certain errors found in software, helping it run smoothly and prevent crashes.
  3. Security patches: through security patch management they correct known software vulnerabilities and cover holes in your systems, thus preventing malicious actors from exploiting the flaws and compromising your organization.
- **Countermeasures for Web server-based attacks are :**
  a) Keep web software patched and updated.
  b) Disable client-side scripting.
  c) Block unsigned applets.
  d) Disable cookies.
  e) Use a proxy server with content filtering.
  f) Don't install scripting languages on Web servers.
  g) Inspect all scripts before deploying them.
  h) Audit and log activity.
  i) Deny access from known malicious domains.
  j) Disable harmful or exploited URL constructions such as directory traversals (..), backslashes, or multiple CGI processes in a single URL.
  k) Restrict non-Web file types from being referenced in a URL.
  l) Disable unused script extension mappings.

5.5 Hacking Web Applications

- Web applications are programs that reside on a web server to give the user functionality. Database queries, webmail, discussion groups, and blogs are all examples of web applications.
- Web application uses a client/server architecture, with a web browser as the client and the web server acting as the application server.
- Prominent examples of web application vulnerabilities are the following :
  1. Code injection vulnerabilities : Code injection vulnerabilities or injection flaws are prevalent and extremely popular types of flaws which may quite profoundly undermine a web application's security. The key point here is a connection between the application interface and a back-end database. Provided that a RDBMSand SQL are used to access the Database.. For example, this could happen, if parts of a random user's input were integrated into an SQL query without further securing this input against classified malicious ones.

2. Cross-Site Scripting (XSS) : Cross-Site Scripting is another vulnerability of paramount importance, also stemming from the lack of web application development provisions to validate input. The application is not the ultimate target but, rather the means to it.

- Fig. 5.5.1 shows the stages of a web application attack.

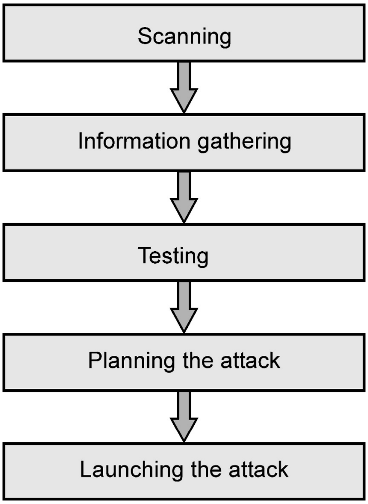


Fig. 5.5.1 : Stages of a web application attack

➤ Web Application Threats

- The following are the most common threats :
  1. SQL Injection - SQL injection is a type of web application security vulnerability in which an attacker is able to submit a database SQL command, which is executed by a web application, exposing the back-end database.
  2. Command injection : The hacker inserts programming commands into a web form.
  3. Cookie poisoning and snooping : The hacker corrupts or steals cookies
  4. Cross-site scripting : A parameter entered into a web form is processed by the web application.

5.6 SQL Injection

- SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution. SQL injection attacks are also known as SQL insertion attacks. SQL Injection is one of the most common application layer attack techniques used today.
- SQL injection refers to a class of code-injection attacks in which data provided by the user is included in an SQL query in such a way that part of the user's input is treated as SQL code. An attacker can submit SQL commands directly to the database.
- SQL injection attacks can lead to privilege bypass and/or escalation, disclosure of confidential information and corruption of database information, among other effects.

- SQL Injection Example: An example SQL injection attack starts with code utilizing an SQL statement, such as:

```
$db_statement = "SELECT COUNT(1) FROM `users` WHERE `username` =
'$username' AND `password` ='$password'";
```

- In an SQL injection attack against code such as this, the attacker supplies input, such as the following, to the application:

```
$username = "badUser";
$password = "' OR '1'='1";
```

- Using this example, the SQL statement executed becomes the following:

```
SELECT COUNT (1) FROM `users` WHERE `username`='badUser' AND `password`=''
OR '1'='1';
```

- In the above example, this results in returning a count of all rows in the "users" table, regardless of the user name or password supplied, since the conditional '1'='1' always returns as true. If the query shown in this example is used for authentication purposes, the example SQL injection attack has just bypassed the authentication process for the application in question.
- This form of SQL injection occurs when user input is not filtered for escape characters and is then passed into an SQL statement. These results in the potential manipulation of the statements performed on the database by the end user of the application.
- In web application, the values received from a Web form, cookie, input parameter, etc., are not typically validated before passing them to SQL queries to a database server. Then dynamically built SQL statements. An attacker can control the input that is sent to an SQL query and manipulate that input.
- Attacker may be able to execute the code on the back-end database. Fig. 5.6.1 shows three tier application with SQL commands.

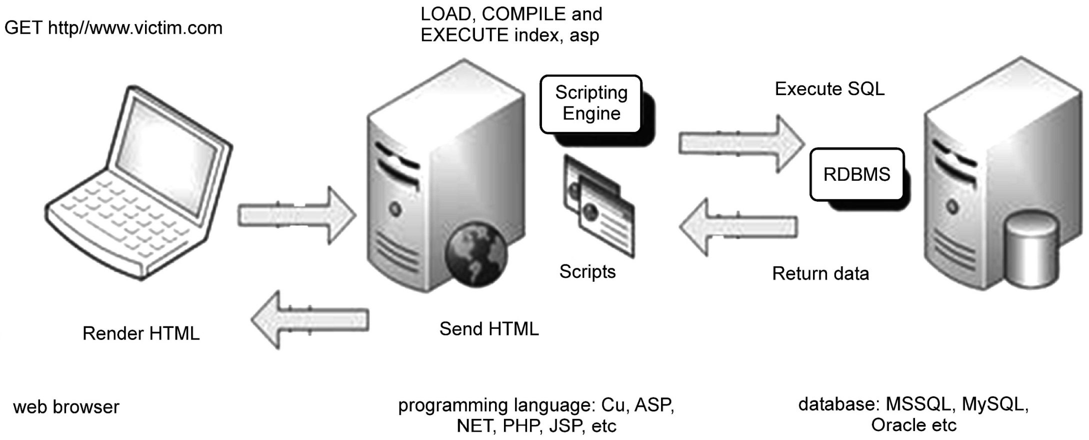

GET http//www.victim.com
LOAD, COMPILE and EXECUTE index, asp
Scripting Engine
Execute SQL
RDBMS
Scripts
Return data
Render HTML
Send HTML
web browser
programming language: Cu, ASP, NET, PHP, JSP, etc
database: MSSQL, MySQL, Oracle etc

Fig. 5.6.1 Three tier application

- Using SQL injections, attackers can add new data to the database; modify data currently in the database and sometime gain access to other user's system capabilities by obtaining their password.

➤ Prevention from SQL Injection Attack

1. Check syntax of input for validity
2. Specify the length limits for input string
3. Scan query string for undesirable word combinations that indicate SQL statements
4. Limit database permissions

➤ Blind SQL Injection

- Blind SQL Injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker. Time Delays are a type of blind SQL injection that cause the SQL engine to execute a long running query or a time delay statement depending on the logic injected.
- Blind SQL Injection is used when there is No Output and No Error from the web application. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.
- Blind SQL injection is identical to normal SQL Injection except that when an attacker attempts to exploit an application rather than getting a useful error message they get a generic page specified by the developer instead.
- Web applications commonly use SQL queries with client-supplied input in the WHERE clause to retrieve data from a database. By adding additional conditions to the SQL statement and evaluating the web application’s output, you can determine whether or not the application is vulnerable to SQL injection.
- To secure an application against SQL injection, developersmust never allow client-supplied data to modify the syntax of SQL statements. All SQL statements required by the application should be in stored procedures and kept on the database server.

➤ SQL server penetration Tools

1. **Sqlpoke** is a NT based tool that locates MSSQL servers and tries to connect with the default account. Scans IP addresses looking for SQL Servers with the default sa password.
2. **NGSSQLCrack :** This is a Password auditing tool. It identifies user accounts with weak passwords that could be vulnerable to brute force attacks.
3. **SQLScan :** Scans IP addresses looking for SQL Servers, with IP list to scan, optional dictionary file and optional installation of backdoor on vulnerable hosts.

5.7 Hacking Wireless Networks

- Following is the key factors contributing to higher security risk of wireless networks.

1. **Communication Channel :** Wireless networking typically involves broadcast communications, which is far more susceptible to eavesdropping and jamming than wired networks. Wireless networks are also more vulnerable to active attacks that exploit vulnerabilities in communications protocols.

2. **Mobility :** Wireless devices are far more portable and mobile, thus resulting in a number of risks.
3. **Accessibility :** Some wireless devices, such as sensors and robots, may be left unattended in remote and/or hostile locations, thus greatly increasing their vulnerability to physical attacks.

➥ 5.7.1 Type of Wireless Attack

- The main categories of attack on wireless computer networks are as follows :
  1. Interruption of service : Resource becomes unavailable because it is destroyed.
  2. Modification : Attacker gain access of the resources and modify the database values, alters the program etc.
  3. Fabrication : The attacker send fake message to the neighboring nodes without receiving any related message.
  4. Jamming : Jamming is a special class of DoS attacks which are initiated by malicious node after determining the frequency of communication. In this type of attack, the jammer transmits signals along with security threats. Jamming attacks also prevents the reception of legitimate packets.
  5. Attacks against encryption : Wired equivalent privacy encryption method is used 802.11b wireless LAN but there is some weakness in this algorithm. Sophisticated attacker can break the WEP method.
  6. Brute force attacks against passwords of access points. A 'brute force' login attack is a type of attack against a access point to gain access by guessing the username and password, over and over again.
  7. Mis-configuration : Because of heavy load on the network admin, most of the access points are not configure properly. These access points remain at high risk of being accessed by unauthorized parties or hackers.
  8. Interception : As the communication takes place on wireless medium can easily be intercepted with receiver tuned to the proper frequency. The main aim of such attacks is to obtain the confidential information that should be kept secret during the communication. The information may include private key, public key, location or passwords of the nodes.

➥ 5.7.2 Wireless EquivalentPrivacy Protocol (WEP)

- Wired Equivalent Privacy (WEP)is a security protocol, specified in the IEEE Wireless Fidelity (Wi-FI) standard, 802.11b, that is designed to provide a wireless local area network (WLAN). WEP is designed to provide the same level of security as that of a wired LAN.
- The WEP algorithm was designed to be used to protect wireless communication from unauthorized eavesdropping and restricting access to a wireless network.
- A wired local area network (LAN) is generally protected by physical security mechanism that are effective for a controlled physical environment, because a wireless network broadcasts messages using radio, it is particularly susceptible to eavesdropping.

- WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, WEP is not as secure as believed. WEP is used at the two lowest layers of the OSI model - the data link and physical layers; it therefore does not offers end-to-end security.
- WEP is part of the IEEE 802.11 standard. It uses the stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity. Fig. 5.7.1 shows basic WEP Encryption where RC4 Keystream XORed with Plaintext.

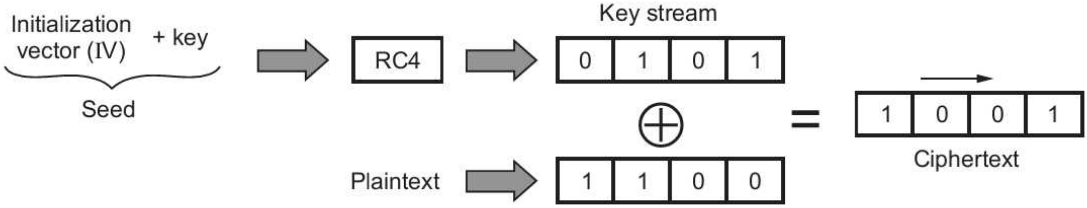


Fig. 5.7.1 : Basic WEP Encryption where RC4 Keystream XORed with Plaintext

- Standard 64-bit WEP uses a 40 bit key, which is concatenated to a 24-bit initialization vector (IV) to form the RC4 traffic key. But restrictions on cryptographic technology limit the key size. Once the restrictions were lifted, all of the major manufacturers eventually implemented an extended 128-bit WEP protocol using a 104-bit key size.
- Key size is not the only major security limitation in WEP. Cracking a longer key requires interception of more packets, but there are active attacks that stimulate the necessary traffic. There are other weakness in WEP, including the possibility of IV collisions and altered packets, that are not helped at all by a longer key.
- Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packet.
- WEP security involves two parts: **Authentication and Encryption**.
- When device initially join the LAN, then authentication starts. It prevents the device or station to join the network unless they know the WEP key. Fig. 5.7.2 shows WEP authentication.

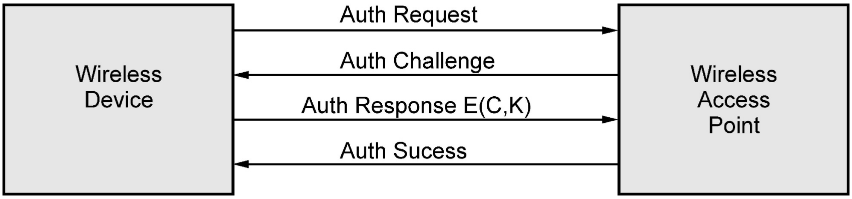


Fig. 5.7.2 : WEP authentication

- Wireless device sends authentication request to the wireless access point, then wireless access point sends 128 bit random challenge in a clear text to the requesting client. The wireless device uses the shared secret key to sign the challenge and sends it to the wireless access point.
- Wireless access point decrypts the signed message using the shared secret key and verifies the challenge that it has sent before. If the challenge matches, then authentication succeeds otherwise not.
- In WEP, same key is used for authentication and encryption. So it is difficult to tell whether the subsequent message come from the trusted device or from an impostor. There is possibility of man in the middle attack.

➤ Strengthening WEP

- Following are the solution to overcome the weakness of WEP :
  1. Initialization Vector size should be increases.
  2. The hashed value of IV can be pre-pended or appended to the cipher-text instead of the clear-text.
  3. For the data integrity verification, use different method instead of CRC checksum.
  4. Change secret key regularly.
  5. Better key management using security handshake protocols.
  6. New authentication mechanisms using the Extensible Authentication Protocol(EAP).

➥ 5.7.3 Wireless Sniffers and Locating SSIDs

- Sniffing is eavesdropping on the network. A packet sniffer is a program that intercepts and decodes network traffic broadcast through a medium.
- Sniffing is the act by a machine S of making copies of a network packet sent by machine A intended to be received by machine B. Such sniffing, strictly speaking, is not a TCP/IP problem, but it is enabled by the choice of broadcast media, Ethernet and 802.11, as the physical and data link layers.
- Sniffing has long been a reconnaissance technique used in wired networks. Attackers sniff the frames necessary to enable the exploits described in later sections.
- Sniffing is the underlying technique used in tools that monitor the health of a network. Sniffing can also help find the easy kill as in scanning for open access points that allow anyone to connect, or capturing the passwords used in a connection session that does not even use WEP, or in telnet, rlogin and ftp connections.
- It is easier to sniff wireless networks than wired ones. It is easy to sniff the wireless traffic of a building by setting shop in a car parked in a lot as far away as a mile, or while driving around the block.
- In a wired network, the attacker must find a way to install a sniffer on one or more of the hosts in the targeted subnet. Depending on the equipment used in a LAN, a sniffer needs to be run either on the victim machine whose traffic is of interest or on some other host in the same subnet as the victim.

- An attacker at large on the Internet has other techniques that make it possible to install a sniffer remotely on the victim machine.
- Scanning is the act of sniffing by tuning to various radio channels of the devices. A passive network scanner instructs the wireless card to listen to each channel for a few messages. This does not reveal the presence of the scanner.
- The Service Set Identifier (SSID) is the name of the WLAN and can be located in a beacon. Wireless computers need to configure the SSID before connecting to a wireless network.
- If two wireless networksare physically close, the SSIDs are used to identify and differentiate the respective networks.
- The attacker can discover the SSID of a network usually by passive scanning because the SSID occurs in the following frame types: Beacon, Probe Requests, Probe Responses, Association Requests, and Reassociation Requests.
- The SSID is usually sent in the clear in a beacon packet. Most APs allow the WLAN administrator to hide the SSID.
- If the Beacons are not turned off, and the SSID in them is not set to null, an attacker obtains the SSID included in the Beacon frame by passive scanning.
- If Beacon transmission is disabled, the attacker has two choices. The attacker can keep sniffing waiting for a voluntary Associate Request to appear from a legitimate station that already has a correct SSID and sniff the SSID as described above. The attacker can also chose to actively probe by injecting frames that he constructs, and then sniffs the response. When the above methods fail, SSID discovery is done by active scanning.

➤ Collecting the MAC Addresses :

- The attacker gathers legitimate MAC addresses for use later in constructing spoofed frames. The source and destination MAC addresses are always in the clear in all the frames.
- There are two reasons why an attacker would collect MAC addresses of stations and APs participating in a wireless network.
  1. The attacker wishes to use these values in spoofed frames so that his station or AP is not identified.
  2. The targeted AP may be controlling access by filtering out frames with MAC addresses that were not registered.

➥ 5.7.4 Wireless Hacking Techniques

- Wireless hacking attacks can be categorized as follows:
  1. Cracking encryption and authentication mechanisms : It includes cracking WEP, WPA etc. Hackers can use them to connect to the WLAN using stolen credentials or can capture other users' data and decrypt/encrypt it.
  2. Eavesdropping or sniffing : This involves capturing passwords or other confidential information from an unencrypted WLAN or hotspot.
  3. Denial of Service : DoS can be performed at the physical layer.

4. AP masquerading or spoofing : Rogue APs pretend to be legitimate APs by using the same configuration SSID settings or network name.
5. MAC spoofing : The hacker pretends to be a legitimate WLAN client and bypasses MAC filters by spoofing another user's MAC address.

5.8 Hacking Mobile Platform

- When a mobile phone transmits audio, it applies an oscillating electric current to the mobile phone antenna. The mobile phone antenna then emits corresponding electromagnetic waves, which are also known as radio waves.
- To receive calls, the mobile phone antenna intercepts an electromagnetic wave of a particular frequency. Its terminal then receives a minuscule amount of voltage, which is amplified and converted to sound by other components.
- Mobile phone antennas transmit signals to radio towers and receive signals back simultaneously.
- Modern mobile phones use cellular networks. Cellular networks are also radio networks. In a cellular network, the towers are distributed over portions of land called cells. These cells are usually hexagonal in shape, but they can also be square or circular. Each cell of land contains at least one radio tower.
- Each cell is also assigned a number of frequencies which correspond to radio base stations. Other cells can use the same frequencies as long as they are not adjacent.
- A cell-phone carrier typically gets 832 radio frequencies to use in a city.
- Each cell phone uses two frequencies per call, a duplex channel. So there are typically 395 voice channels per carrier. (The other 42 frequencies are used for control channels).
- Therefore, each cell has about 56 voice channels available. In other words, in any cell, 56 people can be talking on their cell phone at one time.
- Cell-phone handset is composed of two components: **Radio frequency (RF) and Baseband**
- RF is the mode of communication for wireless technologies of all kinds, including cordless phones, radar, ham radio, GPS, and radio and television broadcasts.
- RF waves are electromagnetic waves which propagate at the speed of light, or 186,000 miles per second (300,000 km/s). The frequencies of RF waves, however, are slower than those of visible light, making RF waves invisible to the human eye.
- Baseband: In signal processing, baseband describes signals and systems whose range of frequencies is measured from zero to a maximum bandwidth or highest signal frequency. In telecommunications, it is the frequency range occupied by a message signal prior to modulation. It can be considered as a synonym to low-pass.
- Mobile phone contains SMD components, Microprocessor, Flash memory etc. In addition to the Circuit board, Mobile phone also has Antenna, LCD , Keyboard, Microphone, Speaker and Battery.

➤ International mobile equipment identity (IMEI) :

- IMEI is a unique number given to every single mobile phone, typically found behind the battery. IMEI numbers of cellular phones connected to a GSM network are stored in a database containing all valid mobile phone equipment. When a phone is reported stolen or is not type approved, the number is marked invalid.

➤ Equipment Identity Register (EIR) :

- The EIR keeps a black list of stolen phones that should be barred from access. Stolen phones can be re-flashed with a new IMEI and thus avoid the EIR check.
- EIR can also block phones that are malfunctioning and disturb the network.
- The EIR feature is used to reduce the number of GSM mobile handset thefts by providing a mechanism to assist network operators in preventing stolen or disallowed handsets from accessing the network.
- This control is done by comparing the International Mobile Equipment Identity (IMEI) that is provided during handset registration to a set of three lists provided by the network operator :

  a) Black list - Mobile Stations (MS) on the BlackList will be denied access to the network

  b) White list - MSs on the White List will be allowed access to the network

  c) Gray list - MSs on the Gray List will be allowed on the network, but may be tracked

➥ 5.8.1 Mishing

- Mishing is the combination of the words mobile phone and phishing. It is just like phishingbut instead of using a computer, the scammer targets mobile devices. This is especially true for users thatbuy goods and services on their mobile device or useit for banking.
- The typical mishing scam involves the scammer calling or text messaging, posing as an employee from your bank claiming to need your personal details for authorization.
- Scammers are very good at coming up with different reasons why they need your information. It could be to authorize a payment or a purchase you have made on your mobile phone.
- For example, the image on the right shows the sort of text message that could be used to trick you into opening a link that looks genuine, but is afraudulent site.
- To stay safe, keep in mind your bank or business is never going to call you and ask you for your account information with them and never select a link in the text message.

➤ Mobile hacking

- Hacking means indexing the weakness in the computer system or network or cracking the system to gain access. Hacking is not all about cracking the password and stealing, anything. if you use anything without the owner permission is known ashacking.

- Mobile phone hacking can also mean : intercepting mobile telephone calls to listen to the call in progress taking covert control of the mobile phone to receive copies of text messages and other activity, and to remotely listen to activity around the phone.
- This is done by installing software on the phone to provide the functionality that is remotely accessed. The phone user is not aware of the operation of the software. Information is sent using the phone data capability and is not readily identifiable from the phone bill

➥ 5.8.2 Designing Mobile Security Policy

- The mobile device policy should take into account the risks of working with mobile devices in unprotected environments.
- The mobile device policy should consider :

1. registration of mobile devices;
2. requirements for physical protection;
3. restriction of software installation;
4. requirements for mobile device software versions and for applying patches;
5. restriction of connection to information services;
6. access controls;
7. cryptographic techniques;
8. malware protection;
9. remote disabling, erasure or lockout;
10. backups;
11. usage of web services and web apps.

➥ 5.8.3 Security Challenges Posed by Mobile Device

- Physical threats : Gaining physical access to a device would allow an attacker to perform malicious actions such as flashing it with a malicious system image that is connected to a computer to install malicious software or conduct data extraction.
- Network-based threats : Mobile devices use common wireless network interfaces such as Wi-Fi and Bluetooth for connectivity.
- System-based threats : Manufacturers can sometimes introduce vulnerabilities into their devices unintentionally.
- Application-based threats : Similar to system vulnerabilities, third-party applications on mobile devices may also be out-of-date. Some application developers do not release software updates in a timely manner or may have dropped support for older OS versions.

5.9 Questions with Answers

5.9.1 Two Marks Questions with Answers

Q. 1 What Is the difference between session hijacking and session spoofing?

Ans. : Session hijacking is performed against a user who is currently logged in and authenticated, so from the victim's point of view the attack will often cause the targeted application to behave unpredictably or crash. With session spoofing, attackers use stolen or counterfeit session tokens to initiate a new session and impersonate the original user, who might not be aware of the attack.

Q. 2 What is shoulder surfing?

Ans. : Shoulder surfing is one of the simplest wayof gathering sensitive data and it occurs mostly inpublic places. It is a technique of gatheringinformation such as usernames and passwords bywatching over a person's shoulder while he/she logsinto the system, thereby helping an attacker to gainaccess to the system.

Q. 3 Define vishing.

Ans. : Vishing is criminal practice of using socialengineering over the telephone system. Criminalsuse the phone to solicit your personal information.This telephone version of phishing is sometimescalled vishing.

Q. 4 What is mishing ?

Ans. : Mishing is the combination of the wordsmobile phone and phishing. It is just like phishingbut instead of using a computer, the scammer targetsmobile devices. This is especially true for users thatbuy goods and services on their mobile device or useit for banking.

Q. 5 What is international mobile equipmentidentity ?

Ans. : IMEI is a unique number given to everysingle mobile phone, typically found behind thebattery. IMEI numbers of cellular phones connectedto a GSM network are stored in a database containingall valid mobile phone equipment.

Q. 6 What is SQL injection ?

Ans. : SQL injection is a code injection technique,used to attack data-driven applications, in whichmalicious SQL statements are inserted into an entryfield for execution.

Q. 7 What is blind SQL injection ?

Ans. : Blind SQL injection is used when a webapplication is vulnerable to an SQL injection but theresults of the injection are not visible to the attacker.Time delays are a type of blind SQL injection thatcause the SQL engine to execute a long runningquery or a time delay statement depending on thelogic injected.

Q. 8 Define session hacking.

Ans. : Session hijacking refers to the exploitation of a valid computer session where an attacker takes over a session between two computers. The attacker steals a valid session ID, which is used to get into the system and sniff the data.

Q. 9 What is social engineering?

Ans. : Social engineering is the art of manipulating people so they give up confidential information.

Q. 10 What is art of manipulation?

Ans. : Hackers who are able to blend in and appear to be a part of the organization are the most successful at social-engineering attacks. This ability to blend in is commonly referred to as the *art of manipulation.*

Q. 11 Explain human based social engineering attack.

Ans. : Human-based social engineering refers to person-to-person interaction to retrieve the desired information. An example is calling the help desk and trying to find out a password.

Q. 12 What is denial of service ?

Ans. : A denial of service is an attempt to prevent a genuine user of service from using it.

Q. 13 What is replay attack ?

Ans. : A replay attack is one which an attacker obtains a copy of an authenticated packet and the later transmits it to the intended destination.

Q. 14 Define Botnets. **AU : Dec.-16, CSE/IT**

Ans. : A botnet is collection of compromised computers often referred to as "zombies" infected with malware that allows as attacker to control them. Botnet owners or "herders" are able to control the machines in their botnet by means of a covert channel such as Internet Relay Chat, issuing commands to perform malicious activities such as distributed denial-of-service attacks, the sending of spam mail and information theft.

Q. 15 What is an intruder ?

Ans. : Accessing a network unauthorizedly is called intrusion.

Q. 16 What is intrusion detection system ?

Ans. : An Intrusion Detection System (IDS) is a system for detection unauthorized access to the system.

Q. 17 Define order of volatility (OOV). **AU : Dec.- 18**

Ans. : The order of volatility is the sequence or order in which the digital evidence is collected. The order is maintained from highly volatile to less volatile data. An example order of volatility for a typical system are registers, cache, routing table, memory, temporary file systems, disk, physical configuration, network topology and archival media.

Q. 18 Show various Steganalysis attack methods. **AU : Dec.- 18**

Ans. : Steganalysis attack methods are as follows :

a. Steganography-only attack: Only the steganography medium is available for analysis.

b. Known-carrier attack: The original cover and steganography media are both available for analysis.

c. Known-message attack: The hidden message is known.

d. Chosen-steganography attack: The steganography medium and tool are both known.

e. Known-steganography attack: The carrier and steganography medium, as well as the steganography tool or algorithm, are known.

➡ 5.9.2 Multiple Choice Questions with Answers

Q. 1 Mishing is a combination of mobile phone and __________.

(a) virus (b) phishing (c) spamming (d) vishing

Ans. : (b) pishing

Q. 2 __________ surfing is a technique of gathering passwords by watching over a person's shoulder while they log in to the system.

(a) Hand (b) head (c) shoulder (d) None

Ans. : (c) shoulder

Q. 3 What is it called when a hacker pretends to be a valid user on the system?

(a) Impersonation (b) Third-person authorization

(c) Help desk (d) Valid user

Ans. : (a) Impersonation

Q. 4 Which of the following is a type of social engineering?

(a) User identification (b) Shoulder surfing

(c) System monitoring (d) Face-to-face communication

Ans. : (b) Shoulder surfing

Q. 5 Wired Equivalent Privacy is a shared-secret key encryption system used to encrypt packets transmitted between a station and an __________.

(a) base state (b) mobile (c) access point (d) router

Ans. : (c) Access point

Q. 6 SQL injection is an attack in which __________ code is inserted into strings that are later passed to an instance of SQL Server.

(a) non malicious (b) clean (c) redundant (d) malicious

Ans. : (d) Malicious

Q. 7 WEP stands for __________.

(a) Wireless Equivalent Privacy (b) Wired Equivalent Protocol

(c) Wired Element Privacy (d) Wired Equivalent Privacy

Ans. : (d) Wired Equivalent Privacy

Q. 8 URL is the __________ and is commonly used in the address bar of a web browser to access a particular website.

(a) Uniform Resource Location (b) Uniform Rest Locator

(c) Uniform Resource Locator (d) Uniform Router Location

Ans. : (c) Uniform Resource Locator

Q. 9 Session hijacking is made possible by tools that perform __________ number prediction.

(a) sequence (b) serial (c) random (d) all of these

Ans. : (a) sequence

Q. 10 What is a sequence number?

(a) A number that indicates where a packet falls in the data stream

(b) A way of sending information from the sending to the receiving station

(c) A number that the hacker randomly chooses in order to hijack a session

(d) A number used in reconstructing UDP session

Ans. : (b) A way of sending information from the sending to the receiving station

Q. 11 The term "computer contaminant" refers to:

(a) Excessive dust found inside the computer case

(b) Viruses, worms, and other malware

(c) Spam e-mails

(d) Nigerian scam e-mails

Ans. : (b) Viruses, worms, and other malware

Q. 12 What is the art of exploiting the human elements to gain access to un-authorized resources?

(a) Ethical Hacking (b) Social Engineering

(c) Caller ID Spoofing (d) Reverse Engineering

Ans. : (b) Social Engineering

Q. 13 Which attack is used to crash Web Server?

(a) SQL Injection (b) ARP poisoning

(c) DOS attack (d) Cross Site Scripts

Ans. : (a) SQL Injection

Q. 14 Buffer overflow, SQL injection, and stack smashing are examples of:

(a) Vulnerabilities (b) Exploits

(c) Input attacks (d) Injection attacks

Ans. : (c) Input attacks

Q. 15 The purpose for putting a "canary" value in the stack is:

(a) To detect a dictionary attack (b) To detect a stack smashing attack

(c) To detect parameter tampering (d) To detect script injection

Ans. : (b) To detect a stack smashing attack

Q. 16 The following are characteristics of a computer virus EXCEPT:

(a) Polymorphic (b) Downloadable

(c) Self-propagating (d) Embedded in spam

Ans. : (c) Self-propagating

Q. 17 Rootkits can be difficult to detect because:

(a) They are encrypted

(b) They are polymorphic

(c) They reside in ROM instead of the hard drive

(d) They use techniques to hide themselves

Ans. : (d) They use techniques to hide themselves

Q. 18 An attack on a DNS server to implant forged "A" records is characteristic of a:

(a) Pharming attack (b) Phishing attack

(c) Whaling attack (d) Spim attack

Ans. : (a) Pharming attack

Q. 19 An organization wants to prevent SQL and script injection attacks on its Internet web application. The organization should implement a/an:

(a) Intrusion detection system (b) Firewall

(c) Application firewall (d) SSL certificate

Ans. : (c) Application firewall

Q. 20 When an attempt is to make a machine or network resource unavailable to its intended users, the attack is called __________.

(a) denial-of-service attack (b) slow read attack

(c) spoofed attack (d) starvation attack

Ans. : (a) denial-of-service attack

Q. 21 The pattern that can be used to identify a virus is known as __________.

(a) stealth (b) virus signature (c) armoured (d) multipartite

Ans. : (b) virus signature

Q. 22 A program that migrates through networks and operating systems and attaches itself to different programs and databases is a __________.

(a) virus (b) worm (c) denial-of-service attack (d) damage

Ans. : (a) virus

Q. 23 A program that fills a computer system with self-replicating information thus clogging the system is called a __________.

(a) virus (b) worm (c) denial-of-service attack (d) damage

Ans. : (b) worm

Q. 24 Which statement best describes a worm?

(a) A virus that is designed to destroy your hard drive

(b) A virus that is designed to frighten people about a nonexistent virus

(c) A virus that doesn't attach itself to programs and databases

(d) A virus that is designed to shut down a server

Ans. : (c) A virus that doesn't attach itself to programs and databases

Q. 25 An attempt to slow down or stop a computer system or network by flooding the system with requests for information is called a __________.

(a) virus (b) worm (c) denial-of-service attack (d) trojan horse

Ans. : (c) denial-of-service attack

Q. 26 __________ is a computer virus encoded as a macro in programs that support a macro language.

(a) Virus (b) Macro virus (c) Worm (d) Trojans

Ans. : (b) micro virus

Q. 27 __________ is a computer program that replicates and propagates itself without having to attach itself to a host.

(a) Virus (b) Worm (c) Trojan (d) Spyware

Ans. : (b) worm

Q. 28 Nimda and code red are __________.

(a) Viruses (b) Spyware (c) Worms (d) Adware

Ans. : (c) worms

Q. 29 What is the main purpose of malware?

(a) To learn passwords (b) To do harm to a computer system

(c) To discover open ports (d) To identify an operating system

Ans. : (b) To do harm to a computer system

Q. 30 The software or hardware component that records each keystroke a user enters into a word processing document is called a __________.

(a) sniffer (b) keylogger

(c) trojan program (d) buffer overflow

Ans. : (b) Keylogger

Q. 31 What type of network attack relies on multiple servers participating in an attack on one host system?

(a) Trojan attack (b) Buffer overflow

(c) Denial of service attack (c) Distributed Denial of service attack

Ans. : (d) Distributed Denial of service attack

❑❑❑

Notes

SOLVED MODEL QUESTION PAPER

(As Per New Syllabus)

Cyber Forensics

Semester – VIII (CSE/IT) Professional Elective-IV

Time : Three Hours] **[Maximum Marks : 100**

Answer All Questions

PART - A (10 × 2 = 20 Marks)

Q.1 *Define cyber forensics.* **(Refer Two Marks Q.11 of Chapter - 1)**

Q.2 *What do you mean forensic data acquisition ?*
(Refer Two Marks Q.3 of Chapter - 1)

Q.3 *What are the tasks performed by computer forensics tools ?*
(Refer Two Marks Q.5 of Chapter - 2)

Q.4 *What is the use of initial response field kit ?*
(Refer Two Marks Q.17 of Chapter - 2)

Q.5 *What is the purpose of PUK ?* **(Refer Two Marks Q.12 of Chapter - 3)**

Q.6 *How to perform the remote acquisition process ?*
(Refer Two Marks Q.20 of Chapter - 3)

Q.7 *What is trojan horse ?* **(Refer Two Marks Q.5 of Chapter - 4)**

Q.8 *Define port scanning.* **(Refer Two Marks Q.14 of Chapter - 4)**

Q.9 *Define order of volatility (OOV).* **(Refer Two Marks Q.17 of Chapter - 5)**

Q.10 *What is shoulder surfing ?* **(Refer Two Marks Q.2 of Chapter - 5)**

PART - B (5 × 13 = 65 Marks)

Q.11 a) *i) Briefly describe forensic investigation.* **(Refer section 1.5)** **[7]**

ii) What is cyber crime ? Explain types of cyber crime. **(Refer section 1.1)** **[6]**

OR

b) *Explain the process of acquiring data with a linux boot CD.* **(Refer section 1.7)** **[13]**

Q.12 a) *i) While processing crime, how will you work with windows and DOS systems ?* **(Refer section 2.2)** **[7]**

ii) Explain in details the various computer forensic tools. **(Refer section 2.3)** **[6]**

OR

b) *Analyze how the following techniques are used :* **[13]**

i) Documents evidence in the lab ii) Processing and handling digital evidence

iii) Preparing to acquire digital evidance. **(Refer section 2.1)**

Q.13 a) *Explain the process of investing e-mail crimes and violation.* **(Refer section 3.5)** **[13]**

OR

b) *Describe cell phone device forensics.* **(Refer section 3.6)** **[13]**

Q.14 a) *What is hacking ? How hackers hack the system ? Explain various phase of hacking.* **(Refer section 4.1)** **[13]**

OR

b) *What is enumeration ? Explain various techniques for enumeration.* **(Refer section 4.4)** **[13]**

Q.15 a) *i) What is SQL injection ? Explain blind SQL injection.* **(Refer section 5.6)** **[6]**

ii) What is WEP ? Explain its working. **(Refer section 5.7)** **[7]**

OR

b) *What is mishing ? What is IMEI and EIR ? Explain security challenges posed by mobile device.* **(Refer section 5.8)** **[13]**

PART - C (1 × 15 = 15 Marks)

Q.16 a) *A public institution was the victim of a hacker. The subject got into the network and placed several large media files on several computers and changed the desktop configurations. Management decided against calling law enforcement initially (because of media attention) and instructed the IT department to get a CFS to privately investigate. How did the CFS go about conducting the investigation ?* **(Refer section 4.13)** **[15]**

OR

b) *A patient with a heart ailment was transported to a hospital where an angiogram was performed. The patient later had a stint inserted into an artery, along with a second angiogram, but died shortly thereafter. A third angiogram was performed immediately after the patient's death. Images of the angiogram procedures were purportedly stored on computer hard drives. The day following the patient's death, hospital staff were able to locate images for the first and third angiograms but could not find any images of the second procedure. The hospital and doctor were sued for medical malpractice and wrongful death. The plaintiffs also claimed the defendants had deliberately deleted the images of the second angiogram that allegedly proved the wrongful death claim. A CFS team (CFST) was engaged by the doctor's insurance company to locate images of the second angiogram on the computer hard drive. Explain the possible actions that the CFST took to locate the images.* **(Refer section 1.8)** **[15]**

❑❑❑

Notes