T.Y.Bsc. Computer Science : Cyber Forensics : Unit 1: Chapter 1 : Introduction to Computer Forensics And Standard Procedure

Computer Forensics :

- It is collection, preservation, analysis and presentation of computer related evidence
- Determines past actions that have taken place on a computer system using computer forensics techniques.
- Process of methodically examining computer media(hard disks, diskettes, tapes, etc.) for evidence.

Importance of Cyber Forensics :

- Use of Data Hiding techniques like encryption and steganography by smarter criminals cause traditional evidence method difficulty in finding evidence.
- People consider Cyber Forensics to be detective work but it is more than that since its also worried with :
  - ✓ Sensitive data handling responsibly and confidentiality.
  - ✓ Taking precautions to not nullify findings by corrupting data.
  - ✓ Taking precautions to make certain the integrity of the information.
  - ✓ Staying with the regulations and guidelines of evidence.

Computer Forensic Process Steps :

- There are four steps for forensic investigation :
  1. Collection : In this phase data is identified, labeled and recorded and gathering the data and Physical evidence related to the incident being invested is done.
  2. Examination : Required information is identified and extracted from the collected data using forensic tools and techniques.
  3. Analysis : Results of the examination phase are analysed. Useful answers to the questions are generated which are presented in the previous phases.
     Most cases are solved in this phase.
  4. Reporting : Results of the analysis are done this phase. Contains the information related to the case such as actions that have been accomplished, actions left to be performed, moves left to be performed and advocated enhancement processes and tools

Crimes For Investigation :

- ☐ Identity theft

- ☐ Fraud and embezzlement
- ☐ the software piracy and hacking
- ☐ the blackmail and extortion
- ☐ child pornography and exploitation
- ☐ Prostitution, infidelity domestic violence
- ☐ Terrorism and national security
- ☐ Theft of intellectual property and trade secret

Evidence Collected at the time of investigation :

Investigation of Identity theft :

- ❑ Credit card numbers
- ☐ Credit card readers writers and scanner
- ☐ Identification template such as driving license birth certificate
- ☐ Images of the electronic signatures information of online trading

Incident Verification and System Identification :

Incident :

Computer security incident is any unlawful, unauthorized or unsuitable activity that includes a computer system or a computer network. Such activity involves the following activities :

1. Theft of the trade secrets.
2. Email spam or harassment.
3. Embezzlement.
4. Unauthorized or unlawful intrusions into computing systems.
5. Denial-of-service (DoS) attacks.
6. Extortion.

7. Any unlawful action when the evidence of such action may be stored on computer media
   for example fraud, threats, and traditional crimes
8. Possession or dissemination of child pornography.

Goals of Incident Response :

1. To prevent a disconnected, no cohesive response.
2. Confirms or dispels whether an incident happened.
3. Promotes gathering of accurate information.
4. Establishes controls for proper retrieval and handling of evidence
5. Protects privacy rights established by law and policy
6. Minimizes damage to business and network operations.
7. Allows for criminal or civil action against culprits.
8. Provides accurate reports and useful recommendations.
9. Provides quick detection and containment.
10. Minimizes exposure and compromise of proprietary data.
11. Protects your organization's reputation and assets.
12. Educates senior management.
13. Promotes quick detection and/or prevention of such incidents in the future

Persons Involved in the Incident Response Process : There are two people involved here Organisation and CSIRT(Computer Security Incident Response Team). Organisation involves Technical Specialist, HR Personnel , Legal Counsel , Security Professional, Corporate Security Official , End Users and Help Desk Workers

Incident Process Methodology :

Incident Process Methodology consists of the following steps :

1. **Pre-incident :** In this phase there is need to prepare the Organization as well as the Computer Security Incident Response Team(CSIRT) to handle as well as prevent the attacks or criminal activities that can occur.

a) **Preparing the organization:** Includes company-wide strategies like :

I. Applying host-based security measures.
II. Applying network-based security measures.
III. Training end users
IV. Hire an Intrusion Detection System (IDS)
V. Creating strong access control
VI. Performing timely vulnerability examination
VII. Ensuring backups are done on a regular basis.

b) **Preparing the CSIRT :** Consists of :

I. The hardware required to investigate computer security incidents.
II. The software required to investigate computer safety incidents.
III. The documentation like forms and reports required to investigate computer safety incidents.
IV. The ideal guidelines and operating tactics to implement your response techniques.
V. The training required to perform the incident response to staff or employees

2. Detection of Incident : Whenever any unauthorized or illegal thing happens that involves organization or computer network or data processing unit, the computer security incident are identified. Initially, the incident may be reported by an end user, detected by a system administrator, recognized by intrusion detection system or discovered by means of other methods. End users may additionally document an incident through certainly three ways :
(a) Their immediately supervisor,
(b) The company help desk
(c) An incident hotline controlled by the Information Security entity

In order to record the incident an initial checklist is to be prepared. This should include :

1. Current time and date of the incident
2. Who reported the incident ?
3. Nature of the incident
4. When the incident happened?

5. What Hardware/software involved ?

6. Points of contact for involved personnel.

3. Initial Response : The data collected during this phase consist of reviewing network-based and other evidence. This phase does the following tasks :

1. Interviewing system administrators.

2. Interviewing business unit personnel.

3. Reviewing intrusion detection reports and network-based logs to identify data that would support that an incident has happened.

4. The network topology reviewing and access control lists to determine if any ways of attack can be ruled out.

The team should also verify whether the Incident has actually occurred, which systems are directly or indirectly affected, which users are involved or the potential business impact.

4.Formulate Response Strategy : The goal of the response strategy formulation is to determine appropriate response strategy, given the circumstances of the incident. Here the political, technical, legal, and business factors that surround the incident are taken into consideration. The final result depends on the objectives of the group or individual with responsibility for selecting the strategy.

☐ Considering the Totality of the Circumstances :

- Circumstances of the computer security incident affect the response strategies.

- Some factors need while deciding the resources required for investigating an incident.

- So the strategy must have to take into account whether to make a forensic duplication of pertinent systems, whether to make a criminal referral, whether to accompany civil litigation, and added aspects of your response strategy

- Estimated dollar loss

- Network downtime and its impact to operations

- User downtime and its impact to operations

- Whether or not your organization is legally compelled to take certain actions

- Public announcement of the incident and its effect on the organization's reputation/business
- Theft of intellectual property and its potential economic impact.
- Taking action : Organizations have to take action to discipline an employee. The organizational respond to a malicious act done by an outsider.

☐ Legal action :

- There are two legal choices, one is to file a civil complaint or another is to notify law enforcement.
- Law enforcement involvement will results in reducing the autonomy that the organization has in dealing with an incident and cautious deliberation ought to arise earlier than you have interaction the precise government.
- The following standards have to be considered while identifying whether or not to include law enforcement in the incident response
- Does the damage/cost of the incident merit a criminal referral ?
- Is it likely that civil or criminal action will accomplish the outcome desired by your organization ?
- Has the reason of the incident been reasonably established?
- Does your organization have proper documentation and an organized report that will be conducive to an effective investigation?
- Can tangible investigative leads be given to law enforcement officials for them to act on?

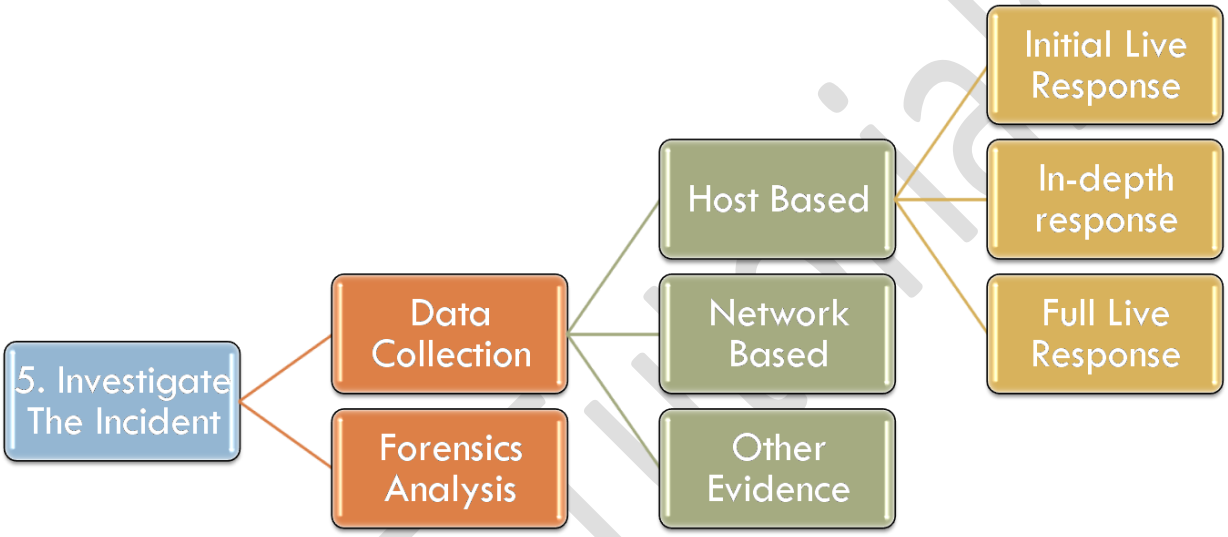
❑ **Admin :** Following are some administrative actions to discipline internal employees :

- Letter of scolding
- Immediate dismissal.
- Mandatory leave of absence for a specific length of time.
- Reassignment of job duties.
- Temporary reduction in pay to account for losses/damage
- Public/private apology for actions conducted
- Withdrawal of certain privileges, such as network or web access

5. Investigate Incident : The investigation phase involves determining who, what, when, where, how, and why surrounding an incident. One can also conduct the investigation by, reviewing host-based evidence, network-based evidence and evidence gathered traditionally. Computer security investigation can be divided into two phases :

(a) Data collection

(b) Forensic analysis



a) Data Collection : Data collection is the gathering of facts and clues that are considered during forensic analysis. The data you gather forms the basis of your conclusions. The data you get amid the information accumulation stage can be partitioned into three key ranges: host-based data, system based data and other.

i) Host-based Information : Host-based evidence contains logs, records, documents, and any other information that you get on a system and not gathered from network-based nodes. Host-based data collection is done in two ways : live data collection and forensic duplication. In few cases, the evidence that is required to understand an incident is temporary or lost when the victim/relevant system is powered down. Such type of volatile data can give critical information when attempt to understand the nature of an incident. This is also known as live response. There are three types of live response:

(i) Initial live response : Initial live response collect only the volatile data from a target or victim system

(ii) In-depth response : In this response the CSIRT gather enough additional

information from the target/victim system to decide a valid response strategy. Even the Non volatile information is collected like log files to help understand the nature of the incident.

(iii) Full live response : It is a full investigation on a live system. For forensic duplication all data for the investigation is collected from the live system which requires the system to be powered off.

ii) Network Based Evidence : Contains information gathered from the following sources Intrusion Detection System logs, Consensual tracking logs, Non-consensual wiretaps, Pen-register/trap and traces, Router logs, Firewall logs and Authentication servers. Network surveillance permits an organization to accomplish a number of tasks such as Confirm or dispel suspicions surrounding an alleged computer, Gather additional evidence and information, Verify the scope of a compromise, Identify any other parties involved, Form a timeline of events happening on the network and Ensure compliance with a desired activity

iii) Other Evidence : It is the other information obtained from the people. Other evidences follow the traditional investigative techniques to collect the evidence. Other evidence you get when you collect personnel files, interview employees, interview witnesses, interview character witnesses, and document the information gathered.

(b) Forensic analysis: Forensic analysis reviews all the collected data. Review includes log files review, system configuration files, trust relationships, web browser history files, email messages and their attachments, installed applications, and graphic files. When you perform software analysis, review time/date stamps, perform keyword searches, and take any other necessary investigative steps. Also examines the information which has been logically deleted from the system to determine if deleted files, slack space, or free space contain data fragments or entire files that may be useful to the investigation

6. Reporting : The big challenge reporting is to create reports that precisely describe the details of an incident which should be understandable to decision makers, that can bear the wall of legal scrutiny, and that are produced in a timely manner. The guidelines for reporting are as follows :

(i)Document immediately : Document all investigative steps and conclusions which are necessary to document as early as possible It results in time saving and ensure that can be communicated more clearly to others at any time.

(ii) Write concisely and clearly : Write down everything in such a way that it is easy to understand to everyone. Try to avoid the shorthand or shortcuts.

(ii) Use a standard format : Build up a format for your reports and stick to it. Make forms,

outlines, and layouts that sort out the response process and cultivate the recording of all relevant information. This
makes report writing versatile, spares time, and advances exactness.
(iv) Use editors : Recruit technical editors to read the forensic reports. This helps to develop reports that are conceivable to nontechnical personnel who affect your incident response and resolution.

7. Resolution : The objective of the resolution stage is to execute host-based, network-based and procedural counter measures to keep an incident from creating additional harms and to give back your organization to a protected, solid operational status. The following activities are involved here :

- Identify your organization's top needs.
- Determine the way of the incident in enough detail to understand how the security occurred and what host-based and network-based remedies are required to address it.
- Determine if there are basic or systemic reasons for the incident that need to be addressed
- Restore any affected or compromised systems.
- Apply corrections required to address any host-based vulnerabilities.
- Apply network-based countermeasures, for example access control lists, firewalls, or IDS
- Assign responsibility for correcting any systemic issues
- Track progress on all corrections that are required
- Validate that all remedial steps or countermeasures are viable.
- Update your security policy and methods as needed to improve your response process.

Data Encryption And Compression :

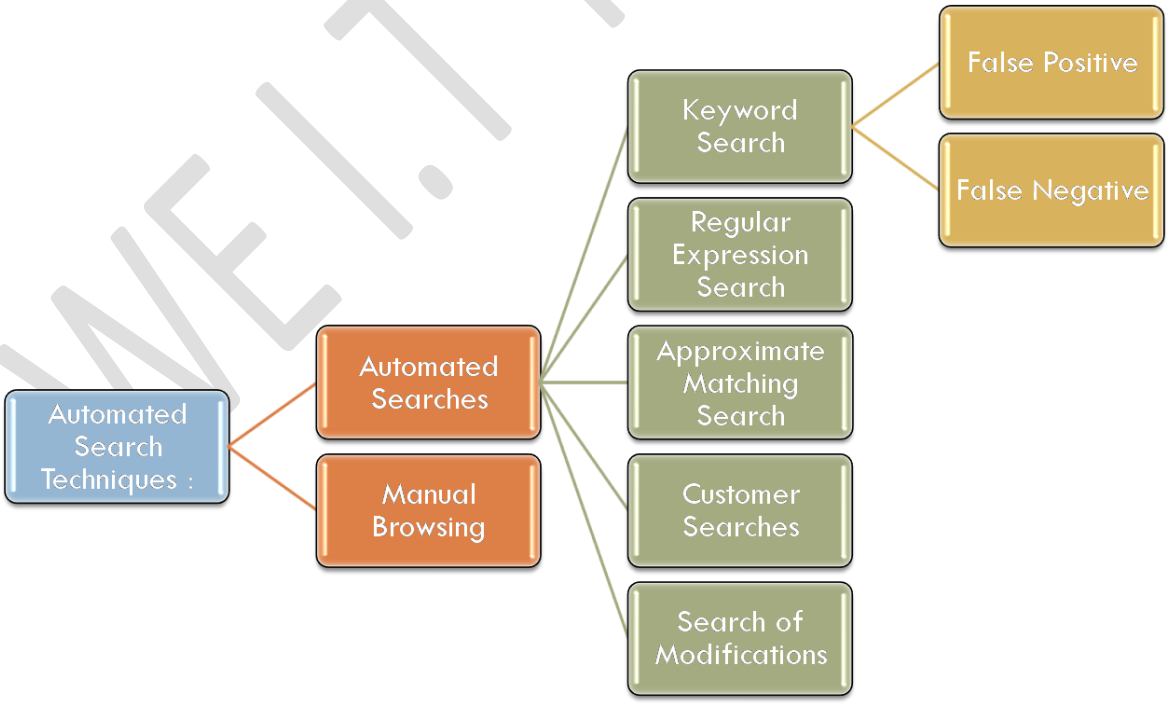
- ☐ **Encryption :** Scrambling data, so that it cannot be readable to the interceptor. Many publically available programs permit the user to create virtual encrypted disks which are opened by selected key. It is not possible to read the encrypted data without the key. When you encrypt a file, only contents of the file get encrypted but the name of the file, size and the timestamps are unencrypted. It is possible to build the parts of the content of the file from other locations, such as swap file, temporary files, and deleted, unencrypted copies. In computer forensics many encryption program with extra

function makes the investigation difficult. Few functions include use of a key file, plausible deniability, and full-volume encryption.

- **Steganography :** It is nothing but hiding a message into a larger file, typically in a photographic image or sound file. Steganography has the capability of disrupting the forensic process when used correctly.In computer forensics to preserve the data evidence MD5 is used for data integrity and cryptcat is used to encrypt the data which is transferred via net.

- **Data Compression:** Many computer users use the compression tools like WinZip, Alzip and WinRAR. These are the widely used compression tools and support many compressed formats. These tools are mainly used for archiving purposes. DEFLATE algorithm is the main compression algorithm for WinZip and Alzip. WinRAR uses uses a modified version of this DEFLATE algorithm. For example,. zip, .gz and .alz are extensions of the given compression algorithms which
use the DEFLATE data compression algorithm. The dual algorithm for decompression is known as INFLATE. Since the DEFLATE and INFLATE algorithms are common among compression utilities these are used for damaged compressed file recovery methodology.

Automated Search Techniques :



- There are two levels of search automation techniques, they are :

1. Automated Search Technique
2. Manual Browsing

1. Automated Search Technique : Keyword search : Keyword search is an automatic search of digital information that consists of specific keywords. It is easy and widely used technique and it speedup manual browsing. The output of keyword search is the list of found data objects. There are two problems with keyword search:

I. False positive
II. False negative

i)False Positive : Keyword searches do not precisely gives the required type of data objects, due to this, output of keyword search can have false positives, it mean the objects that do not belong to the specific type even though they contain specified keywords. Forensic analyst has to browse the keyword search data objects manually to remove false positives.

ii) False negative : False negative means there are objects of given type but they are missed by search. If the search utility cannot correctly interpret the data objects then it results in false negative. This may happen due to encryption, compression, or lack of ability of the search utility to interpret new data. It sets

(1) to select words and phrases highly precise to the objects of the required type like particular names, address, bank account number, etc and

(2) to give every possible variation of these words.

2.Manual Browsing : In manual browsing the forensic analyst browses gathered information and selects objects of preferred type.The single tool used in manual browsing is a watcher of some type. It takes a data object, for example, file, decodes it and gives the result in a human-comprehensible form.Manual browsing is time consuming and slow as there is large amount of data is gathered in maximum investigations.

(iii) Approximate matching search :

- Approximate matching search is an expansion of regular expression search.
- It uses matching algorithm.
- These algorithms allow character mismatches while searching for keyword.
- Here user has to specify the degree of mismatches allowed.

- This search detects the misspelled words, but it gives mismatches and raises the number of false positives.
- The agrep is used for approximate search.

(iv) Custom searches :

- The regular expressions have limited expressiveness.
- The programs are written for the more complex searches, for example, the FILTER_1 tool from new Technologies Inc.
- This tool uses heuristic procedure to find full names of persons in the gathered information.
- FILTER 1 tool also suffers from false positives and false negatives

(v) Search of modifications : Search of modification is used for data objects that have been modified since specified instant in the past. The modification of the data objects that are not frequently, such as operating system utilities, these utilities are detected by comparing their current hash with their expected hash. Before the search a library of expected hashes is built. Some tools for building libraries of expected hashes are given in the "file hashes". Modification of a file can likewise be construed from adjustment of its timestamp. Albeit conceivable in many cases, this adjustment is circumstantial. Investigator assumes that a file is constantly modified concurrently with its timestamp, and since the timestamp is adjusted, he induces that the file was changed as well. This is a type of event reconstruction.

Forensics Software : Following are the softwares used for Cyber Forensics :

1. SANS SIFT
2. Crowdstrike CrowdResponse
3. Volatility
4. The Sleuth Kit(+Autopsy)
5. FTK Imager
6. ExifTool
7. Free Hex Editor Neo
8. Bulk Extractor
9. Deft
10. Xplico
11. LastActivityView
12. Dsi USB Write Blocker
13. FireEye RedLine
14. PlainSight
15. HxD
16. HELIX3 Free

17. Paladin Forensic Suite

18. USB Historian

1. SANS SIFT : The SANS Investigative Forensic Toolkit (SIFT) is an Ubuntu based Live CD which includes all the tools you add to conduct an in -depth forensic or incident response investigation.It supports analysis of Expert Witness Format (E O1), Advanced Forensic Format(AFF), and RAW (dd) evidence formats, SIFT includes tools such as log2timeline for generating a timeline from system logs, Scalpel for data file carving, Rifiuti for examining the recycle bin, and lots more.

2. CrowdStrike CrowdResponse : CrowdResponse is a lightweight console application that can be used as part of an incident response scenario to gather contextual information such as a process scheduled tasks, or Shim Cache. Using embedded YARA signatures you can also scan your host for malware report if there are any indicators of compromise

3. Volatility : Volatility is a memory forensics framework for incident response and malware analysis that allows you to extract digital artefacts from volatile memory (RA dumps
   - Using Volatility you can extract information about running processes, open network sockets and network connections, DLLs loaded for each process, cached registry hives, process IDs, and more

4. The Sleuth Kit (+Autopsy) : The Sleuth Kit is an open source digital forensics toolkit that can be used to perform in-depth analysis of various file systems. Autopsy is essentially a GUI that sits on top of The Sleuth Kit. It comes with features like Timeline Analysis, Hash Filtering, File System analysis and Keyword Searching out of the box, with the ability to add other modules for extended functionality

5. FTK lmager : FTK Imager is a data preview and imaging tool that allows you to examine files and folders on local hard drives, network drives, CDs/DVDs, and review the forensic images or memory dumps

Recovery of Erased and Damaged Data :

- Deleting the file doesn't means the data is gone permanently, operating system simply remove the pointer of that file but data is still present there and the new data can be written in this place
- On the magnetic media data is recorded in the form of zeros and ones when this data is overwritten, the disk detects only the new data leaving only remnants of the old data. Reading the remnant is time consuming and the old data would not be read correctly.
- There are different reasons of data recovery behind different users :

i. End users : The end users wanted to recover the files which they have deleted accidentally and the files that have been compromised due to Hardware failure and Malicious activity

ii. Companies/organizations : Companies wanted to recover the data from the ex-employees computer or to recover the lost files due to Hardware failure and Compromised or lost due to network problem.

iii. Government Agencies :Government Agencies wanted to recover the data from the ex-employees computer or to recover the lost files due to Hardware failure or network problem.

iv. Law Enforcement Agencies : Law Enforcement Agencies needs to recover evidence from a suspect's computer, recover data from hard drive, find out the motive of the crime, to find out the any co-conspirator and to support forensic analysis of computers.

Techniques used to recover erased or damaged data:

- ☐ Carry out a forensic analysis of the computer.
- ☐ Search for single file type.
- ☐ Attack encryption methods.
- ☐ Use the existing image to restore the disk
- ☐ Inspect data in Random Access Memory (RAM)
- ☐ Inspect disk at the cluster level or sector level
- ☐ Analyze data using hex editor
- ☐ Create hash of whole disk and export it in another tool for use.

Types of Damages : There are two types of damages : Physical damage & Logical Damage

1. **Physical damage :** Physical damages means scratches on CDs, breaking of tapes and mechanical problem in hard disk.
2. **Logical damage :** Logical damage is mainly caused by power interruption that does not let the file to be completely written to the storage device. It results in an inconsistent state of file, total data loss, system crash, Strange behavior and Partial storage of data.Tools used for data recovery are WinHex, Forensic Tool Kit (FTK) and Encase

Recovering Deleted Files on Windows Systems :

When a file or directory is deleted from a FAT file system, the first letter of its filename is set to the sigma character (Ó), or, in hex, OxE5. This means that these files will remain intact until new data has overwritten the physical area where these deleted files are located on the hard drive. Special tools can find these "intact" deleted files and recover them for review. After a file has been marked for deletion, each hard drive I/O could overwrite the data you want to recover. To recover the file on windows system we use following tools:

1. Windows based tools : Encase, FTK
2. Linux tools : Fatback, TASK, and Foremost

Windows-Based Tools to Recover Files on FAT File Systems : Encase & FTK

EnCase and FTK are the tools of the windows system for recovering files on FAT filesystems. Both EnCase and FTK have this capability built-in, and they automatically recover any files they can.

Linux Tools to Recover Files on FAT File Systems : Three Linux utilities that can recover data : **Fatback, TASK, and Foremost.**

FatBack to Recover Deleted Files :

- Fatback is used to recover the deleted files from the Fat System.
- Fatback also performs file recovery on FAT12, FAT16, and FAT32 file systems from a Linux forensics platform.
- Following are the features of Fatback
  (a) It supports the Long filename.
  (b) There is recursive undeletion of directories.

(c) Lost cluster chain recovery
(d) It can work within single partitions or entire disks.

- Fatback is flexible because it works on image files as well as devices Fatback installation is easily on Linux and FreeBSD systems

Using TASK to Recover Deleted Files :

- Task is a tool used to recover the deleted files. It is open-source forensic toolkit.
- It is used to analyze Microsoft and Unix file systems. TASK can recover files from different file systems, including FAT, FATI2, FAT16, FAT32, FreeBSD, EXT2, EXT3, OpenBSD and UFS.
- TASK can work on binary images which do not have embedded checksum values.
- TASK cannot work on EnCase evidence files and SafeBack files. TASK works with only a single partition so image each partition on a drive separately in order to use this tool.

Using foremost to Recover lost files :

- Foremost is a Linux program used to recover or files based on the file headers and footers.
- Foremost is a portable, exceptional tool for data recovery. Foremost can work on forensic image files such as those generated by dd, SafeBack, and Encase, or act directly on device
- Foremost consults a configuration file at runtime. This configuration file specifies the headers and footers that Foremost is looking for, so you can choose which ones you want to look for simply by editing the foremost.conf file.
- The Foremost can find GIF files, JPG files, common Microsoft Office documents, email repositories, HTML pages, PDF files, ZIP files, Windows Registry files, WordPerfect files, and even America Online (AOL) mail files.

Recovering Deleted Files on Unix Systems:

- Recovering previously deleted files on Unix systems can be quite a challenge. Since most of the files you attempt to recover on Unix systems are flat text files.
- For recovering previously deleted files in Unix system you can use debugfs on files stored on the ext2 (second extended file system) file system

- Debugfs is a very powerful tool in the hands of the computer forensic examiner It is an interactive file debugger used to examine and to change the state of the ext2 file systems
- The debugfs provides the best means for recovering files on media using the ex2 file system.

File Slack Space :

Cluster :

- Operating systems arrange all data stored an a hard drive into segments called allocation units (also called clusters).
- For e.g., an operating system that uses 32k cluster reads and writes data from a hard drive 32k at a time. It cannot read less than 32K of data from a hard drive, and it cannot write less than 32k at a time on hard drive. However, very few files have the exact amount of data to occupy an entire cluster or set of clusters. When an operating system that writes 32K clusters is being asked to save 20k of data the remaining 12k of unused space is called file slack.

Unallocated space : Unallocated space is the area of the hard drive which is not currently allocated to a file. Sections of deleted files are frequently scattered crosswise over unallocated space on a hard drive. Free space is the segment of the hard drive media that is mot inside of my currently active partition.MS-DOS tools have been written that examine the information on a hard drive and create files that contain all the information inside of the unallocated space, free space, and slack space on a drive. To write the contents of slack space and free space to a file the NTI's tools are used.

Disk Imaging/File duplication and Preservation :

- Disk Imaging makes a large compressed file of your drive. You can restore this data to drive. Image file is large in size and maximum people store it to external drives or file shares. The disk imaging software's creates the exact copy of the hard disk. The forensic image consists of Deleted files, system files, slack space and executables.A disk imaging/duplication is a file that contains every bit of information from the source, in a raw bit stream format. A 5GB hard drive would result in a 5GB forensic duplicate.
- No extra data is stored within the file, except in the case where errors occurred in a read operation from the original. When this occurs, a placeholder is put where the bad data would have been. A forensic duplicate may be compressed after the duplication process.

The tools that create a forensic image are Unix dd command, dfcldd (U.S. Department of Defense (DoD) Computer Forensics Lab version of the dd command) and Open-source Open Data Duplicator (ODD) e.g. FTK imager

- **1. Qualified Forensic Duplicate :** A qualified forensic duplicate is a file that contains every bit of information from the source, but may be stored in an altered or changed form. Two examples of paperwork are in-band hashes and Empty Quarter compression.A few equipments will examine in some of sectors from the supply, generate a hash from that group of sectors, and write the world organization, accompanied via the hash value to the output document. This approach works very well if something is going wrong in the course of the duplication or recovery of the reproduction. If a quarter groups fail to fit the hash cost generated for it, the recovery can continue, and the analyst is conscious that records from that area organization may be invalid. If a similar state of affairs came about with a forensic duplicate file, the place of the mistake may be unknown, probable invalidating the entire reproduction. Empty Quarter compression is a not unusual technique for minimizing the dimensions of the output document. If the tool comes throughout 500 sectors, all filled with zeros, it will make a unique entry inside the output file that the healing application will recognize. Three tools that create qualified forensic duplicate output files are :

1. SafeBack
2. EnCase
3. FTK imager

2.Restored Image : A restored image is what you get when you restore a forensic duplicate or a qualified forensic duplicate to another storage medium. The restoration process is more complicated than it sounds. For example, one method involves a blind sector-to-sector copy of the duplicate file to the destination hard drive. If the destination hard drive is the same as the original hard drive, everything will work fine. The information in the partition table will match the geometry of the hard drive.

3.Mirror Image : A mirror image is created from hardware that does a bit-by-bit copy from one hard drive to another. Hardware solutions are very fast, pushing the theoretical maximum data rate of the IDE or SCSI interfaces. Investigators do not make a mirror image very often, because it introduces an extra step in the forensic process, requiring the examiner to create a working copy in a forensically sound manner. If your organisation has the ability to keep the original drive, seized from the computer system being investigated, you can easily make working copies. If the original must be returned (or never taken offsite), the analyst will still be required to

create a working copy of the mirror image for analysis. The small amount of time saved onsite is overshadowed by the overhead of making a second working copy. We will not cover the process of creating a mirror image of evidence here. Most hardware duplicators are relatively simple to set up and operate. Two such duplicators are Log cube's Forensic SF-5000 and Intelligent Computer Solutions' Image MASSter Solo-2 Professional Plus. You do need to ensure that the hardware duplicator actually creates a true mirror image

Forensic Duplication/Disk Imaging Tool Requirement :A legal duplication tool must be perfect in the following areas:

1. The tool must be able to image all of information on the storage medium.
2. The tool must make a forensic duplicate or mirror image of the original storage medium
3. The tool must handle read errors in a vigorous and elegant way. In the event that a process fails after repeated endeavors, the error is noted and the imaging process proceeds. A placeholder might be placed in the output file with the same dimensions as the portion of the input with errors. The contents of this placeholder must be archived in the tool's documentation
4. The tool must not make any changes to the source medium.
5. The tool must be able to be involved to scientific and peer review. Results must be repeatable and certain by a third party, if essential.
6. Action and error logs are crucially important also. The more data logged by the tool amid operation, the less demanding your occupation will be the point at which you record the procedure

Creating a Forensic Duplicate of Hard Drive :

To create the forensic duplicate of hard drive the following tools are used.

1. dd and dcfldd
2. ODD (Open Data Duplicator)

Creating forensic duplicate using dd and dcfldd :

- The dd tool is the part of the GNU software suite, afterwards dd was improved by the programmers and re-released as dcfldd. The dd tool is very reliable to create the true forensic duplicate. The dd tool performs a complete bit-by-bit copy of the original.

- While using the dd tool simply transposing a single character may destroy evidence, so one must have to be familiar with the dd tool before using it as well as with the Unix environment address storage devices

- The steps require for duplicating hard drive using dd are :

1. Create a boot media

2. Perform the duplication with dd. In some situations the duplication is stored in the series of the files which are sized to fit on a specific media type or file system type, we call this as segmented image. So do the following things to perform the duplication
   o Write the script to perform hard drive duplication
   o Write down the source device name.
   o Write down the output file name and set the output file size.
   o Use the dd command

- It is also possible to create the duplicate without splitting the output file in Linux. To create such type of duplicate calculate MD5 sum of the entire drive in one pass over the source hard drive

- **2 Creating forensic duplicate with Open Data Duplicator (ODD) :**The Open Data Duplicator (ODD) is an open-source tool which follows the client server model. This client server model allows the investigator to perform forensic duplications on a number of computer systems simultaneously over a local LAN. The ODD package is having three portions:

1. Bootable CD-ROMs : These are similar to the Trinux Linux distribution.

2. Server-side application : The server will perform most of the processing of the duplicate image, including the calculation of hashes, string scarches, and the storage of the true forensic duplication.

3. Client-side application : This portion may be run locally if you are duplicating drives on a forensic workstation

Creating Qualified Forensic Duplication of a Hard Drive :

- -It is must to know as an investigator that never boot from the evidence drive. Many items on the evidence media can be altered, starting from the moment the BIOS executes the boot block on the hard drive.

- In the initial boot process, file access timestamps, partition information, the Registry configuration files, and important log files may be changed in a matter of seconds. The qualifier "forensic" implies that the copy is a true copy that is the bit stream from the original and the duplicate are the same

- In order to certify this, one can compare and duplicate bit-by-bit or one can speed up the process by using signatures, also known as hash. A signature is a small piece of data, typically between 4 and 22 bytes long calculated from the contents of a sector, a track, a file, or a whole hard drive.32-bit cyclic redundancy codes SHA1 use an algorithm so complicated that it is computationally impossible to generate a sector, block, track, or file that has the same signature as a given sector, block, track or file.

- A good duplication tool will have some way of proving that the duplicate is true,typically by calculating the signature.

  1. Creating Boot Disk

  - A clean operating environment is required for imaging a system. For doing the imaging DOS applications like SafeBack or EnCase is used it means that you must create an MS DOS boot disk.

  - There should be four files in the root directory of the floppy. These files contain the code to get the computer running a minimal operating system and these four file are IO.SYS, MSDOS SYS, and COMMAND COM. DRVSPACE BIN .The computer first process the IO.SYS file and then the code in IOsys contents of MSDOS.SYS and begins to initialize device drivers, tests and hardware, and loads the command interpreter, COMMAND .COMDuring the process of loading device drivers, if a disk or partition connected to the machine uses compression software then IO.SYS loads the DRVSPACE.BIN drive file.When the driver loads it mount the compressed volume and present the operating system with an uncompressed view of the file system. When it mounts the compressed volume, it changes the time/date stamps on the compressed file; it means that the .evidence will be altered. These files are not required to you. When you boot from your clean boot disk, you want to make sure that the loading of the DRVSPACE BIN driver file fails. Simply removing the file is a good start, but IO SYS is smart enough to check the root directories of all active partitions for the file. The most effective way to prevent the loading of DRVSPAC.BIN İSto load IOSYS into a hex editor and alter the strings manually. Perform the string search operation in word space. Notice that the period in the filename is not represented in the executable file. Continue to search the file for the SPACE string There are four instances in 10 SYS that will need to be changed. When you are finished, save the file and exit the hex editor. On the safer side remove the DRVSPACE.BIN file from the floppy as well After you've created the clean boot floppy,

copy over any DOS mode drivers that you will need to access the hard drives on the computer system under investigation. The best source for DOS drivers is the web site for each hardware manufacturer, rather than on the driver CD that ships with the product

2. Use Encase tool : Encase is a totally high-priced, but very surprising windows based Forensics suite that consists of the making of certified forensics duplicates. Being home windows based totally makes Encase easy to apply, however it additionally introduces a few issues, approximately the OS spotting suspect drives and inside the procedure changing their contents. That does not imply of direction that Encase should ever generate person information. Encase strength lies in their seamless integration of all forensics investigation obligations. Encase generates a certified forensics duplicate.

3. Use Safe back tool :Safe back is small software program software that is positioned on a DOS boot disk(normally a floppy, however this could be changing as floppy drives die out) . It offers options on the kind of duplicate, a real forensics duplicate or a reflect. We will need to have a clean DOS

Introduction :

- Network Forensics is the process of collecting and analyzing raw network data and tracking network traffic systematically to find out how an attack was carried out or how an event occurred on a network.
- Network forensics helps you to find out that the attacks on the network are done intentionally or unintentionally.
- Whenever an intruder attacks a system generally they leave some trace behind. So it is necessary to monitor changes in network traffic.
- DoS attacks are also considered to be one of network attacks, These overloads network resources to make the network unavailable to genuine users, but the attacker never gains access to any computer on the network.
- The network forensics examiners have to set standard procedures to acquire data after an attack or intrusion incident.
- Normally, the network administrators desire to find compromised machines, get them offline, and restore them as fast as possible to reduce downtime.
- It is necessary to take time to follow the standard procedure to make sure that all the compromised systems are tracked and find out attack methods in an attempt to prevent them from happening again.

Securing a network :

- Hardening contains a series of tasks, like applying the latest patches using a layered network defense strategy, which sets up layers of protection to hide the valuable data at the deepest part of the network. It make sure that if the attacker goes deeper then the access become more difficult and the more safeguard are in place.
- The National Security Agency (NSA) developed a similar approach, called the Defense in Depth (DiD) strategy.
- DiD has the following three modes of protection:
  I. People
  2. Technology
  3. Operations
- If any of the mode out of 3 fails the other mode is used to prevent the attack.
- Posting people as a mode of protection implies organizations must hire very much qualified individuals and treat them well so they have no motivation to look for revenge

- Train the employees adequately in security procedures and the organizations security policy.
- This mode includes Physical as well as personnel security measures.
- The technology mode consists of, selection strong network architecture and using tested tools, for example, firewalls and Intrusion Detection Systems (IDSs).
- Regular penetration testing combined with risk assessment will help you to enhance network security, too.
- Having set up that permit speedy and exhaustive examination where a security break happens is likewise part of the technology mode of protection.
- At last, the operations mode tends to everyday activities. Updating antivirus software security patches, and OSs falls into this class, as does evaluation and monitoring methods and disaster recovery plans.

Reviewing Network Logs :

- The incoming and the outgoing traffic of network is recorded by the Network logs. Network servers, firewalls, routers, and other devices record the activities and events that go through them.
- Running the Tcp dump program is the common method to examine the network traffic. It generates the Hundreds or thousands of lines of records.
- The First line is the header and the remaining lines follow the format time. protocol, interface, size, source and destination addresses.
- The second line given below, shows that the data was transmitted on for e.g., Wednesday, December 15, 2010 at 1506:33. The packet sent was TCP packet through the Ethernet0 interface of 1296 bytes.
- When you view the network log, the port information gives you hint for investigation such as you can observe that a specific IP address is coming very frequently on a unusual port.
- The ports above 1024 raise a flag. If you wanted to generate a list of translation the top 10 Web sites users in your network are visiting, use the Ethereal tool. This tool will give you the list of 10 websites along with the information like, the number of bytes transferred followed by the IP address.
- Network logs also show you the patterns, like an employee is sending information frequently from a particular IP address. If you investigate it, you will come to know that the employee was doing the online shopping during company timing.
- After the investigation, keep the preserved evidenced in your mind, your investigation may edge other companies that have been compromised. You should not reveal the findings about the other companies.
- The solution to this is, contact the companies and enlist their aid in tracking down network intruders or you can report the incident to federal authorities.

Network Forensic Tools :

There are different types of tools available for network administrator or forensic. By using these tools one can perform remote shutdowns, monitor device use and more.

Windows Operating System Network Tools : Sysinternals is a collection of freeware tools for examining windows products. These tools are created by Mark Russinovich and Bryce Cogswell and acquired by Microsoft.These tools are very helpful for monitoring the network traffic thoroughly and efficiently. You can monitor your network and shutdown machines or processes that could be harmful.

Tools	**Description**
Regmon	Shows all registry data in real time
Process explorer	Shows what files. Registry keys, and dynamic link libraries(DLLs) are loaded at a specific time
Handle	Shows what files are open and which processes are using these files
Filemon	Shows file system activity
PsExec	Runs processes remotely
PsGetSid	Displays the security identifier(SID) of a computer or user
PsKill	Kills processes by name or process ID
PsList	Lists detailed information about processes
PsLoggedOn	Displays who's logged on locally
PsPasswd	Allows you to change account passwords
PsService	Enables you to view and control services.
PsShutdown	Shuts down and optionally restarts a computer
PsSuspend	Allows you to suspend processes

Unix/Linux operating System Network Tools : Knoppix Security Tools Distribution is a bootable Linux CD intended for computer and network forensics. Before using this tool one has to adjust the BIOS of the system you are using and make sure that it is booting from your CD. Offers tools of various categories like authentication, firewalls, password tools, wireless tools, encryption, IDS's, honeynets, forensics, packet sniffers, vulnerability, assessment, etc.

Tools	**Description**
Dcfldd	The US DOD computer forensics lab version of the dd command
Memfetch	Forces a memory dump
Photorec	Retrieves files from a digital camers
Snort	A popular IDS that performs capture and

	analysis in real time
Oinkmaster	Helps manager snort rules so that you can specify what items to ignore and regular traffic and what items should raise alarms
John	Latest version of John the Ripper, a password checker
Chntpw	Enables you to reset passwords on a Windows computer, including the administrator password.
tcpdump and ethereal	Packet Sniffer

Using PACKET SNIFFERS :

PACKET SNIFFERS" are device and/or software placed network to monitor traffic.
Network administrators use sniffers for increasing security and tracking bottlenecks.
Attackers use sniffers to obtain information illegally. On TCP/IP networks, sniffers examine packets. Thus termed as "Packet sniffers".
In OSI model, Packet sniffers work at Layer 2 or Layer 3. Some sniffers perform packet captures. Sniffers are used for analysis. Some of the sniffers are used for both the purpose.

As in windows, they have many sniffing tools capable of capturing and analyzing packets. But can't feed data (they collect directly into other tools).
Most of tools can read anything captured in Pcap (Packet capture) format (LibPcap is for LINUX/UNIX and WinPcap is for Windows).
As forensics experts, you must choose tools that best suit your purpose.
For Example: If your network is being hit by SYN flood attacks. You need to find packet with SYN flag set.
To find these packets, TCP dump Tethereal and SNORT can be programmed to examine TCP headers to SYN flag (Flag areas contains several flags and SYN flag is one of them).

Tools	**Description**
Tcpslice	Tool for extracting information from large Libpcap files; you specify the time frame you want to examine. Also capable of combining files.
Tcpreplay	A suite of tools which can be used to replay network traffic recorded in lipcap format, this information used to test network devices such as routers, switches, etc.
Ngrep	Used to examine email headers or IRC logs. It collects and hashes data for verification
Ethereal	Tools used for viewing Network traffic graphically. Used in real time environment to open saved and trace files from packet capture. Also

	used to rebuild sessions
Netdude	GUI tool, which are designed as an easy-to-use interface for inspecting and analyzing large TCPdump files
Argus	Session data probe, collector and analysis tool

Examining Honeynet Project :

- The first step is making people and organizations aware that threats exists and they might be targets.
- The second is to provide information on how to protect against these threats, including how attackers operate, how they communicate, and what tactics they use.
- Finally for people who want to do their own research, the Honey net Project offers tools and methods.

- The recent major threats to a network are Distributed denial-of-service (DDoS) and zero day attacks.
- DDoS attacks : Here, the attacker uses hundreds or even thousands of machines These machines are known as zombies because they have unwittingly become part of the attack. When the first DDoS attacks began, the main concerns were the high monetary impact and the amount of time it took to track down these attacks

- Zero Day Attacks : Attackers look for holes in networks and OSs and try to exploit these weaknesses before patches are available.

- The honeynet project set up as a resource to help network administrators' deal with DDoS and other attacks. It involves installing honeypots and Honeywalls at various locations in the world.

- Honeypot :A Honeypot is a computer set up to look like any other machine on your network; its purpose is to lure attackers to your network, but the computer contains no information of real value. In this way, you can take the Honeypot offline and not affect the running your network\

- Honeywalls : Honeywalls are computers set up to monitor what's happening to honeypots on your network and record what attackers are doing.

- **Objective of Honeywall and Honeypot :** The principle behind honey pots is that they aren't used on the network: they are simply set out to act as bait.The original machine is loaded with the standard software used on that part of network, a forensic image of it is created, and then the machine is deployed on the network. If the machine is compromised, its taken offline and another image of it is made. The software then

compares the two images to determine what method of attack was used and what files were altered or added. Both images are stored in the database.

- **Performing Live Acquisitions :**
  Live acquisitions are mainly useful when you are dealing with active network attacks or intrusions or you have doubt that employees are accessing network areas that they should not have to access.
- Live acquisitions is formed before the system go offline and it has become necessity as attack may left footprint or evidence only in processes or RAM for instance, there are some malware which get disappeared when the system is restarted.
  The information in RAM gets lost when the suspects system is turned off.
- The following is the general procedure given for live acquisition, the steps are:
  1.)Create/download a bootable forensic CD, before using it test on the suspected drive. If the suspected system is on your network and you can access it remotely, add the suitable forensic tools to your computer. Otherwise insert the bootable forensics CD in the suspected system.
  2)Ensure that you are keeping the log of all of your actions. Documenting the actions and reasons for these actions is important.
  3)A network drive is perfect as a place to send the data you gather. In the event that you don't have one accessible, interface a USB thumb drive to the suspect system for gathering information. Ensure that you have noted this step in your log,
  4). Now copy the physical memory (RAM),
  5). The next step is depends on the incident you are investigating. For example, you want to shut down the system and make the static acquisition later, you want to see whether a rootkit is present by using a tool such as RootKit Revealer; You may also want to access the firmware to check it is changed or not.
  6)Be confident that you will get the forensically sound digital hash value of all files you have recovered in the live acquisition to ensure that they are not modified later.

Performing a Live Acquisition in Windows : To perform the live acquisitions many tools are available for capturing RAM, for example, network sniffers, password crackers, and freeware forensics tools. You can also use the GUI tools, but it needs many resources. Few GUI tools may get the false readings from windows Os. As compare to GUI tool, Command-line tools give you more control.

Tools available to capture RAM for performing a live acquisition in windows :

Win32dd	Tools runs on command line for performing memory dump on windows
BackTrack 3	Combines the tool from White Hat Hackers CD and the Auditor CD. This tool is popular with penetration testers.

Mantech Memory DD	Acquires up to 4 GB RAM in standard format
Win.exe from guidance software	Standalone RAM acquisition tool

Order of Volatility : The investigators faces the problem of the Order Of Volatility (00V), it means how long a part of information lasts on a system.

Data such as RAM and running processes might exist for only milliseconds; other data, such as files stored on the hard drive, might last for years.

While collecting the evidences related to network based on the volatility a proper order of collecting the evidence have to follow, this is known as order of volatility.The OOV is given as follows

1. Registers, Cache
2 Routing Table, ARP Cache, Process Table, Kernel Suatisties
3. Memory
4. Established Network Connections
5. Running Processes
6. Temporary File Systems
7. Media in use: Disk
8 Remote Logging and Monitoring Data
9 Backup media: tapes, disks not in use
10. Archival Media
11. WOM: CD ROMs, DVD's

After this you can separately collect the analogue material like physical configuration and network topology. paper, figure prints and DNA

Developing Standard Procedures for Network Forensics : Network forensics is a long and, tiresome process. A standard procedure is used in work forensics is as follows :

1. Every time use the standard installation image for systems on a network. This image is not a bit-stream image but an image containing all the standard applications used. For all the applications and OS files you should have the MD5 and SHA-1 hash values.
2. In case, intrusion incident occurs, ensure the vulnerability has been fixed to avoid other attacks from taking advantage of the opening
3. Try to recover all the volatile data by performing the live acquisition before the system turns off, for example, RAM and running processes.
4. Acquire and make the forensic image of the compromised drive.
5. Perform the comparison between files on forensic image and the original installation image. Also compare the common files hash values, such as Win.exe and standard DLLS and find out whether they have altered

T.Y.Bsc. Computer Science : Cyber Forensics : Unit 1: Chapter 3 : Cell Phone and Mobile Forensics :

Introduction :

In cell phone people save lots and lots of data, so if in case you lose your mobile phone, the data stored in the cell phone also get lost and it may be used for wrong purposes. Maximum transactions are also done via cell phones.

Problems in Mobile Phone Forensics :

1. For storing the message no single standard id exist although many of the phones use same storage scheme.
2. As technology is changing new phones are coming in the market about every 5 to 6 months and they are merely compatible with the previous model of the phone. In near future the cables and accessories may become obsolete in a short time.
3. As cell phones are often combined with PDAs, which can make forensics investigations more complex

Mobile Phone Basics :

-In 1970, Motorola introduced cell phones, and it is developed rapidly.

- There were 3 generations of the mobile phones till 2008, and they are: analog, digital Personal Communications Service (PCS), and third-generation (3G).

-3G gives the increased bandwidth, as compare to analog and PCS. It gives 384kbps for pedestrian use, 2 Mbps in fixed locations, such as office buildings and 128 Kbps in a moving vehicle.

Digital networks for mobile phones :

1. Code Division Multiple Access(CDMA) : CDMA is developed by Qualcomm. To define the channels CDMA uses complete radio frequency spectrum. Sprint and Verizon uses the CDMA networks Many of the CDMA networks match to IS-95, which is created by the TIA(Telecommunications Industry Association). These systems are known as cdmaOne, and when they go to 3G services, they will become cdma2000.
2. Global System for Mobile Communication (GSM) : GSM is used by AT&T and T-mobile. It is a standard in Asia and Europe. It uses Time Division Multiple Access (TDMA) technique, thus many phones get turns sharing a channel, a lot like token ring networks

3. Time Division Multiple Access (TDMA) : The TDMA network divides a radio frequency into timeslots. GSM also uses the techniques. TDMA refers to the IS-136 standard, which introduced sleep mode to enhance battery life. TDMA can work in the cell phone with frequency 800 MHz to 1000 MHz) or PCs (1900 MHz) frequency, as a result it is compatible with a number of cell phone networks

4. Integrated Digital Enhanced Network (iDEN) : It is a Motorola protocol which combines various services including data transmissions into one network

5. Digital Advanced Mobile Phone Service (D-AMPS) : D-AMPS is a digital version of original analog standard for cell phone.

6. Enhanced Data GSM Environment (EDGE) : EDGE digital network is used to deliver data and it is a faster version of GSM. It is specially designed for 3G. The 3G standard is developed by the International Telecommunication Union(ITU). It is compatible with CDMA, TDMA, and GSM

7. Orthogonal Frequency Division Multiplexing (OFDM): OFDM technology for 4G network utilizes energy more efficiently than 3G networks. It is more immune to inference.

4G Network : Has the following technologies :

1. Orthogonal Frequency Division Multiplexing (OFDM) : Orthogonal Frequency Division Multiplexing (OFDMD) this techniques uses radio waves broadcast over dissimilar frequencies it uses power more resourcefully, and is more resistant to interference.

2. Mobile WiMAX : This technology supports transmission speed of 12 Mbps. It is chosen by Sprints for its 4G network. This technology uses the OFDMA and IEEE 802.16e standard

3. Ultra Mobile Broadband (UTMS): CDMA network provider use this technology to switch to 4G and to support the transmission speed of 100 Mbps.This technology also known CDMA2000 EV-DO.

4. Multiple Input Multiple Output (MIMO) : Aigro developed this technology and Qualcomm acquired it.It is expected to support 312 Mbps transmission speeds.

5. Long Term Evolution(LTE) : LTE technology supports the transmission speed of 45 Mbps to 144 Mbps and is designed for UMTS and GSM technology, is expected to support 45 Mbps to 144 Mbps transmission speeds. The main components used for communication with these cells are BTS, BSC and MSC

i. Base Transceiver Station(BTS) : BTS is made up of radio transceiver equipment.It describes cells and communicates with mobile phones
ii. Base Station Controller(BSC) : BSC is a combination of hardware and software.BSC manages BTSs and allots channels by connecting to the mobile switching center
iii. Mobile Switching Center(MSC) : MSC connects calls by routing digital packets for the network and relies on a database to support subscribers. This central database has location data, account data, and other key information needed during an investigation. To access information from a carrier's central database warrant is needed.

Inside Mobile Devices :

- The hardware of the Mobile devices consists of is ROM, RAM, a microprocessor, a digital signal processor, a microphone and speaker, a radio module, hardware interfaces(for example, cameras, keypads, and GPS devices), and an LCD display, removable memory cards (in some mobile), Bluetooth and Wi-Fi, Operating system (such as, Linux, Windows Mobile, Android, RIM OS, Palm OS, Symbian OS, Mac OS X).
- Usually, data is stored in the phone electronically erasable programmable read-only memory (EEPROM)
- It allows the service providers to reprogram phones without accessing memory chips physically. Many users take advantage of this facility and reprogram their phone to add new features or switch to different service providers.

SIM Cards :

- Subscriber identity module (SIM) cards are used in GSM devices and consists of microprocessor and 16 KB to 4 MB EEPROM or more than that.
- SIM cards are like to standard memory cards, but the connectors are associated differently
- The mobile station is divided into two parts : The SIM card and the Mobile Equipment(ME), which is the remainder of the phone.
- The SIM card is needed for the mobile equipment to work and serves these following additional purposes :
  o To identify the subscriber to the network.
  o To store personal information

o To store address books and messages.
o To store service-related information.

- You will get SIM cards in two sizes. The most standard size is 0.75 mm thicks.
- SIM card is portable; simply by switching a SIM card between compatible phones, you can move your information to another phone.
- If you are travelling to neighboring countries then you have two SIM cards one for your country and other is for foreign country, you can easily switch to new SIM card.

Inside PDAs :

- Personal Digital Assistants (PDAs) are separate devices from mobile phones.
- The majority users carry them in place of a laptop to keep track of appointments, deadlines, address books, and so forth.
- Most of the PDAs have integrated phones. PDAs consists of RAM, microprocessor, flash ROM, and a variety of hardware components.
- You can retrieve the users calendar address book, Web access, and other items from PDA's
- PDA's uses many peripheral memory cards :

1. Compact Flash (CF) : These cards are used for extra storage and work
2. MultiMedia Card (MMC): These cards are designed for mobile phones, but you can use with PDAs to give another storage area.
3. Secure Digital (SD) : These cards are like MMCs, only extra security features are added to protect data

Acquisition Procedure for Cell Phone and Mobile Device :

- As you know mobile devices are disconnected immediately from the PC.
- It helps to prevent automatic synchronization that might occur on a fixed schedule and overwrite data on the device.
- Additionally, collect the PC and any peripheral devices that determine whether the hard drive consists of any information that's not on the mobile device are connected to the PC via cable cradle station should be

- Based on the warrant, the time of seizure may be relevant It may be possible that messages may be received after seizure that may or may not be admissible in court.
- If you are turning of the device to protect the battery power or attacks then note down the date and time when you have taken this step.
  In the forensic lab when you come back then you have to assess what can be retrieved. You have to check following 4 areas for critical information:

i. The SIM card
ii. The internal memory
iii. Any removable card or external memory cards
iv. The system server

- For checking the system server warrant is required, so to check the voicemail you need to warrant. Help from service provider is also needed to discover the time of a call, to access backups of address books, and other
- On mobile device, there is both, volatile and non-volatile memory available for storage.
- Volatile memory needs power to preserve its contents, but non-volatile memory does no SIM card's file structure is hierarchical structure. This file structure starts with the root of the system (MF)
- In the next level there are Directory Files (DF) and under DF there are files which contain elementary data (EF).
- From SIM card you can recover moderately a little of data.
- The recovered information falls into four categories:
  i. Service-related data, for example identifiers for the SIM card and subscriber
  ii. Call data, like dialed numbers
  iii. Message information
  iv. Location information
- If power is lost, you require PINs or other access codes to view files. normally the original PIN assigned to the SIM card, so while collecting evidence at the scene, seek users' manuals and additional documentation that can help you access the SIM card.
- In many SIM cards you have 3 attempts of entering an access code before the device is locked, else you need to call the service provider or you have to wait for a certain amount of time before trying again.

Mobile Forensics :

- In mobile forensics the biggest challenge is constantly changing models of cell phones and what works with the current cell phone model will not work with upcoming model.

- Like computer forensics we cannot recover deleted files in mobile forensics.

- In mobile forensics usually you are performing two tasks :
  (a) By synchronizing PC with the device
  (b) Reading the SIM card.

Steps in Mobile Forensics :

Step 1: Identifying the mobile device. Many users do not change their device, but some users don't alter their devices, but some file off serial numbers, modify the display to show deceptive data, and so on.There are many online sources available to identify the phone. For example, www.phonescoop.com, www.cellphoneshop.com, and www.mobileforensicscentral.com

Step 2: Ensure that mobile device software is installed on your forensic machine.

Step 3 : Attach the phone to its power supply and connect the correct cables. Use rig cables to connect to devices as cables for the model you're investigating may or may not be available.Lastly, after connecting the device, start the forensics program and start downloading the available information.

SIM Card Readers : With mobile devices, next step is to access SIM card using the hardware/ software device called a SIM card reader. To use this device, you should be in a forensics lab equipped with antistatic devices. In addition, biological agents, such as fingerprints, might be present on the inside of the case, so you should consult the lead investigator when you're ready to proceed to this step. The general procedure is as follows:

1. Take out the back panel of the device.
2. Take out the battery.
3. Under the battery, take out the SIM card from its holder
4. Now into the card reader insert the SIM card

Problems with SIM card Reader :

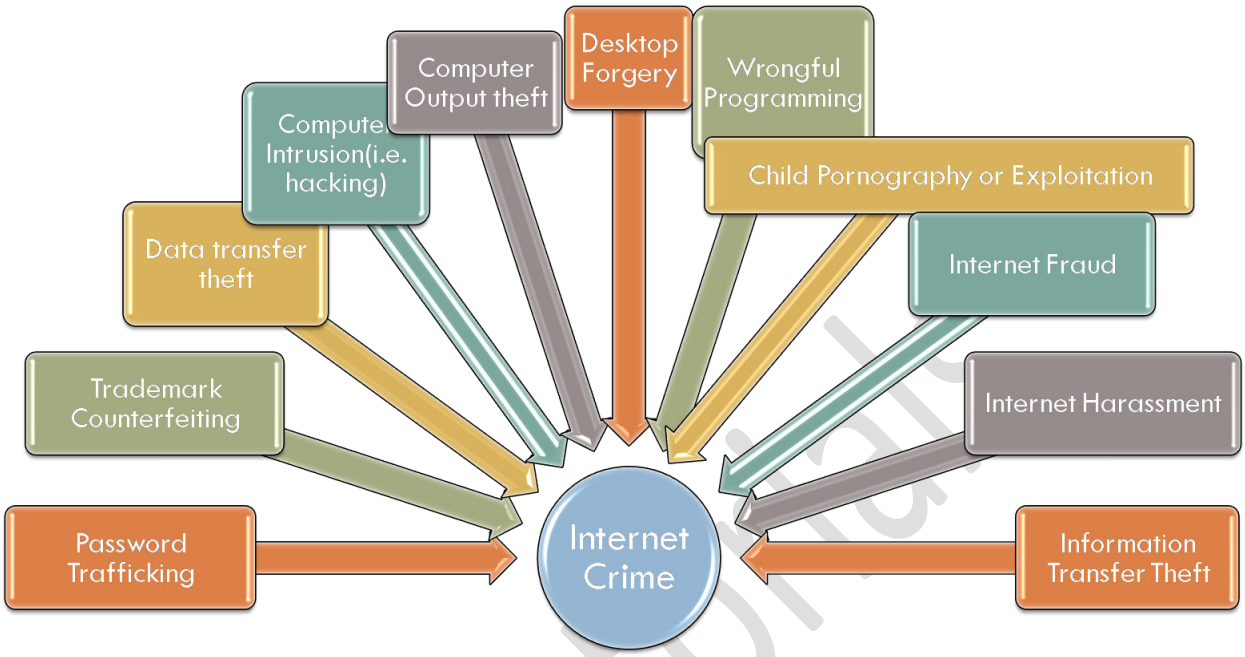
To understand the data collection procedure or cell phones and mobile devices. There are many different types of SIM card readers available in market. Some SIM card readers are forensically sound and some are not; note down this feature of the device in your device investigation log. Second problem is related to the text and SMS messages. It is very difficult to document the unread message. In such situation use a tool that takes pictures of each screen that can be important in this situation. These screen captures can provide extra documentation.

Chapter : Internet Forensics

- In internet forensics the focus is on the internet rather than an individual machine and it is quite challenging to identify criminal activity and people around the globe.
- Internet Spawn : Internet Spawn crimes are crimes that are internet oriented.
- Spam : An activity where unwanted mails are the burdens on may servers each day. Main aim is to get you credentials like credit card number.
- Phishing : Phishing involves fraud activities like fake websites.
- These fake websites look like those of banks or credit card companies.
- A phishing email is sent away like well-known legitimate business like HDFC bank or Amazon.
- This message tells you to click the URL and then direct you to fake website which looks like the original web site.
- This asks the user to enter the account number, personal data online.
- Computer Virus(Worms) : Initially it was regarded as malicious activities wherein people wanted to show their programming skills and wanted to get in the face of computer users around the world.
- Infects computers
- Affects antivirus software and stop such tools from being installed on an already infected software.

Internet Crime :

- Internet Crime : Illegal activity that involves a computer system, where the system as a whole is used as a device for committing crime.
- Types :



1. Password Trafficking :Misusage and illegal selling of individual's password.
2. Trademark counterfeiting : Stealing other individuals' thoughts and whatever else that could be copyrighted and offering them or abusing them for individual addition.
3. Data Transfer theft : It includes Public and private representatives who uses organization's chance and cash, surf the PC or play diversions without appropriate approval. This sort of conduct in numerous occasions is not acknowledged by directors, but rather there is little approach to manage it
4. Computer Intrusion : Stated as "it is an illegal access by any person using a computer and any
communications tool to break computer security or avoid it to enter into a system
5. Computer Output theft : Thieves take data that originate from individual or organization PCs for the sole purpose of discovering mystery or individual data. They do this by taking PC's printouts, mailing records, client records, and so forth
6. Desktop Forgery
With PC innovation and desktop distributed projects, hoodlums duplicate

authority letterhead, records, and travel permits, conception endorsements, and money receipts for individual increase.

7. Wrongful Programming : Wrongful programming violations happen when somebody changes a PC and guides it to control data on the system or somebody's close to home data. This is a more entangled wrongdoing than most others

8. Child Pornography or Exploitation
   Illegally setting a small child obscenity on the web so as to make a benefit, or a gander at small child erotic entertainment for joy

9. Internet Fraud
   Any type of fraud blueprint that uses internet for example chat rooms, emails, or web sites to present fraudulent proposals to prospective victims to organize fraudulent transactions or to send the proceeds to fraud to financial institutions.

10. Internet Harassment :
    Stalking or badgering any individual through the utilization of the web.

11. Information Transfer Theft : Tapping so as to steal of individual data into a telephone line outside one's home and running a line straightforwardly into one's own PC. This should frequently be possible without one notwithstanding knowing it through split lines.

World Wide Web Threats, Hacking and Illegal Access :

Attack Types : These are the attack types :

1. Pre-intrusion/attack activities
2. Password-Cracking Techniques
3. Technical exploits
4. Malicious code attacks

1. **Pre-intrusion/ Attack Activities :** Focuses on information gathering. The attack procedure is broken down into following steps :

I. Pre-attack
II. Initial Access
III. Full System Access
IV. Planting back doors for future access
V. Covering Tracks

To identify potential targets and their flaws :

1. Perform port Scanning
2. IP Proofing to hide identity
3. Inserting Trojans
4. Inserting attacking devices on the target system
5. Placing sniffers in place to capture transmission goto and from the target system

Port Scanning : Port is a point where date enters or leaves the computer. When port scanning is performed attacker gets the information about the standard ports and services are running and responding on target system, operating systems are installed on the target system and applications and versions of an application are present. Scanning is used for :

1. Target Enumeration : Locate the host system which is open to attack

2.Service Identification : It is also used to identify vulnerable ports and services on the target system.

3.Target Identification : Used to identify target system

Types of Port Scan :

1.TCP Connect : Makes use of TCP open system call. TCP open system call is provided by the operating kernel to connect to particular ports on the target host.

2.TCP SYN/Half-Open : TCP SYNN scanning is responsible for sending the SYN packet to the target host. The target host responds with SYN+ACK. In case when

the target host is alive but is not listening to a specific port then RST packet will be received.

3. FIN : Fin packet us send to the target machine to close the connection. In case when the target host is alive but is not listening to a specific port then RST packet will be received.

Address Spoofing : Hacker uses spoofed addresses to contact other computers and fool them into thinking a message from originated from a different machine. These address spoofing are IP Spoofing, DNS Spoofing and ARP Spoofing

IP Spoofing :

IP spoofing means changing the header of message; this indicates that message is not come from the true source. The attacker computer impersonates another machine and makes the recipient to accept messages which come from the attacker machine. Trusted ports are spoofed and it permits the hacker to get a message from the firewall or router. Proper configuration of firewall is necessary to protect from the IP spoofing. The IP spoofing is used in combination with one of the other types of attacks. Remote Procedure Call (RPC) services, the X Window system, the UNIX service(rlogin, rsh, and so on) and any service that uses IP address authentication are all susceptible to IP spoofing

Finding the address of the trusted host is the goal of the attacker. Normally the communication between the sender and the receiver is intercepted by the attacker The attackers frequently perform a DoS attack against the trusted host to prevent trusted host from communicating on the network

Then next step is to change the packet headers to make it look as though the attacker's message are coming from the trusted host and the packets are sent to a service or port that uses address authentication.

ARP Spoofing : At the time of deriving frames from packets, the Ethernet header knows only the destination IP not the MAC address. The header needs to determine the MAC address, given the IP of the machine. This is where ARP comes in. The Address Resolution Protocol (AR) maintains the ARP cache ARP table maps unique network IP of the machine to unique MAC addresses.

This cache is necessary because the MAC address is used at the physical level to locate the destination computer to which a message should be delivered. Involves changing the MAC to IP address entries, causing traffic to be redirected from legitimate system to unauthorized system of the attacker's choice.For a

particular IP address if there is no entry in the ARP cache then ARP sends a broadcast message to all the computers on the subnet and request that the machine with the IP address in question respond with its MAC address. This mapping then gets added to
the ARP cache. ARP spoofing, also known as ARP poisoning

DNS Spoofing : DNS spoofing attack is based on the concept of domain name server. A DNS is a table that converts the domain names like XYZ.com into network addresses like 211.217.74.130; this process is known as resolving the domain. DNS spoofing refers to two methods of causing a DNS server to direct users incorrectly.

1. Poisoning of the DNS cache results caching the false entries and servers' direct users to the wrong Web sites or e-mail being sent to the wrong mail servers
2. Predicting the DNS server's send request by using the recursive mechanism of DNS and respond to it with fake information.

Placement of Trojans:

Trojans are also known as Trojan horse. This software is programs that appear as legitimate and does something else in addition to or instead of their ostensible purposes. In the pre-attack phase, a hacker can plan a Trojan program on the victim's machine, this program installs keystroke-logging programs to gather information for the main attack or later the attacker will use that information to get into victims machine.

Placement of Tracking Devices and Software:

Another way to attack is place a physical tracking device on a system if an attacker has onsite access to the victim system. The device is very small and can be installed in less than a minute.
We just have to unplug the keyboard from the PC and then plug the logger into the PCs keyboard port. This device is not noticeable to most users inside the logger there are microchip and a non- volatile memory chip. Depending on the memory size it can record the pages of keystroke

Placement of Packet Capture and Protocol Analyzer Software : Network monitors are also known as protocol analyzers. These protocol analyzers allow the administrators to capture and analyze the network traffic for troubleshooting purposes or to monitor network activity. To capture the packets secretly the

hackers use this tool and then hacker read the information from the packets. The network sniffers are also used to listen the activity on the wire.

Understanding Password Cracking : There are many ways to crack password :

1. **Brute Force :** Here attacker tries all the possible combinations to crack the password until the attacker gets success. Also known as dictionary attack.
2. **Recover and exploit password stored on the system:** Some people store password in the system itself since they might have many passwords. The cracker just have to acquire those files here. Similarly some people might store this password in some encrypted format and the cracker acquires this encrypted file and decrypts it using some software.
3. **Make use of password decryption software :**
   i) One byte patching : Decrypts password by simply changing one byte in the program.
   ii) Known plain-text method : Used with algorithms. Used to attack password protected files like.zip,.rar, and .arj files
4. **Social Engineering :** Requires Social abilities and individual communication to make somebody to uncover security related data and maybe even to accomplish something that allows an attack.

Understanding Technical Exploits :

There are many technical exploits which the hacker uses to get access of network.

1. Protocol Exploits : DNS DOS Attacks, SYN/LAND Attacks, The Ping of Death, Ping flood, fraggle and smurf attacks, UDP bomb and UDP anork Teardrop Attacks and Exploits of SNMP
2. Other Protocol Exploits :Application Exploits, Unix Exploits, Rootkit Attacks NFS exploits
3. Other UNIX Exploits : Includes Router Exploits, Bug Exploits, Mail Bombs,
4. Browser Exploits
5. WebServer Exploits
6. Operating System Exploits : Includes The WinNuke Out-Of-Band Attack and Windows Registry Attack

Obscence and Incident Transmission:

Obscenity is defines as "anything which appears to the prurient interest or if its effect is tend to degrade and corrupt persons."

Punishment for Transmitting or Publishing of Data or Information Containing Sexually Expressive Act in Electronic Form and is punishable under Section 67 of The Information Technology Act, 2008

Punishment for Transmitting or Publishing of Data or Information Depicting Children in Sexually Expressive Act in Electronic Form and is punishable under Section 67 of The Information Technology Act(Ammendment), 2008[12]

Domain Name Ownership :

Domain Name :

- It is a string of characters.
- Used as an internet identifier to simplify internet location of an entity's website.
- For example, google.com, ebay.com, amazon.com, etc.
- Some concepts related to domain name :
- Registrar : Company that sells the domain name which is available to the clients to its relationship with one or more name registries.
- Registry : Entity who gives unique domain names within particular country code or top level domain
- Registrant : Real domain owner. Although he/she/it may not be the person using the domain name.
- WHOIS Record : Record that gives detailed information for particular domain which usually includes a registrant and an administrative contract.

DOMAIN NAME OWNERSHIP :

- Domain name ownership is obtained by accessing the WHOIS record for the domain name.
- There are few registrars who use the automated tools that create domain names including one or more terms and related WHOIS records
- The administrative contact has the authority to alter the domain name, as well as changing registrant information and accepting change of registrars.

OBTAINING A WHOIS RECORD :

- There are two types of domain extensions, centralized and decentralized. The centralized domains have extensions such as us, info, and.biz and the decentralized domain names have the extensions like .com and .Net.
- To get the WHOIS records for decentralized extensions, visit the registry to first identify the registrar associated with the domain name, after that visit the registrar to get the WHOIS record. To get the centralized extensions visit the registry

STEPS FOR DOMAIN NAME INVESTIGATIONS

1. Determine ownership of the domain name.
2. Retain copies of the WHOIS record and content
3. Check whether the entity is associated with additional domain names.
4. View prior versions of the domain name content.
5. Check meta tags and keywords
6. Perform a brand/trademark search.
7. Check for prior UDRP and court decisions.

Event Reconstruction: To find out who is responsible for an attack the investigator can reconstruct events in the past. There are many techniques for

reconstructing the events. They are categorized as per primary object of analysis. The basis of which are :

1. **Log File Analysis :**
   A log file is a purposefully generated record of past events in a computer system organised as sequence of entries. An entry usually consists of a timestamp, an identifier of tge process that generated the entry, and some description of the reason for generating an entry. It is common to have multiple log files on a single computer system. Different log files are usually created by the operating system for different types of events In addition many applications maintain their own log files. Log file entries are generated by the system process when something important happens. The knowledge of circumstances, in which processes generate log file entries. permits forensic scientist to infer from presence or absence of log file entries that certain event happened. It is assumed that the log file enteries were generated by the TCP wrapper, which functioned according to the expectations of the forensic scientist; that the entries have not been tampered with; and that the timestamps on the entries react real time of the moments when the entries were generated.
2. **File System Analysis :** In Unix file systems, the information about a file is stored in a combination of i-node and directory entries pointing to that i-node
   In Windows NT File System(NTFS) information about a file of the Master File Table.
   When a disk or a disk partition is first formatted, all such file set to initial "unallocated" value.
   When a file entry is allocated for a file, it becomes active. Its fields are filled with proper information about the file
   In most file systems, however, the file entry is not restored to the unallocated value when the file is deleted. As a result, presence of a file entry whose value is different from the initial "unallocated" value, indicates that that file entry once represented a file, which was subsequently deleted.
   File attribute analysis

In most file systems a file has at least one timestamp. In NTFS, for example, every active (i.e. non-deleted) file has three timestamps, which are collectively known as MAC-times

Time of last Modification (M)

o Time of last Access (A)

o Time of Creation (C)

Reconstructing past internet activities : To rebuild the past internet there are two methods

1. Use DNS cache to find deleted browsing history
2. To recover lost browsing history files
3. To recover deleted history by using Google history

1.Use DNS Cache to find deleted browsing history :

- DNS is Domain Name System, it is faster method to restore searches or history.
- The problem in this is, if the computer is restarted, it will not be able to help you find browsing history. DNS cache will work only when about everything is connected to the internet.
- So do not shut down the computer if you want to restore deleted browsing history for an app or video game Perform the following steps to restore the browsing history
- Press Windows +R type cmd and click OK. Or you can also type cmd in Windows search bar
- Open Command Prompt, type ipcongif/displaydns and click Enter
  Then all your recently visited websites will be displayed. You can view all your recent browsing history and find those important websites back

2. **To recover lost browsing history files :** Use data recovery software to recover lost browsing history files you are not aware where the browsing history is saved then follow next path to check that the history file is deleted or not
3. **Recover deleted history by using Google history :** The Google history is not deleted if you delete the history from browser, it stores all browsing history, including all pages visited and all devices attached to your Google Account. This means, you can also recover that history from your Android phone. The following are steps:
   Go to Google History and sign in with the Google account
   It will display the date and time, calendar that you use. Go to the date at which you would like to see the browsing history.
4.

Chapter 5:Email Forensics

Email Forensics :

- Email client message is made up of two parts that are header and the body.
- Header contains information about email origin, like the address from where it comes, how it reached the destination and who sent it.
- Body contains message and attachments if any.
- Many organizations have their own email server.
- User sends the mail to the ISP server and the ISP server sends the message to the client.
- When we investigate email crime, the internal emails are easy to trace.
- They use Universal Naming Convention(UNC) coupled with central authentication and controls ; making it easier to compose or delete the message.
- Email client performs task listing all the messages in mailbox by displaying header as well as time and date of the messages.
- It also tells the sender the size of the message.
- The client can view, compose or delete the message.
- Email server is having the list of accounts.
- Whenever a person send an email it first is send to the mail server with sender and receiver's name and message.
- Server formats this information and appends it to the bottom of the recipient's text file.
- To interact with the server following email protocols are required :

1. Post Office Protocol(POP) : Stores only incoming messages. Investigation is done at work station.

2. Internet Message Access Protocol(IMAP) : Stores all the messages. Copies of incoming and outgoing message are stored on the server or workstation or both.
3. Microsoft Mail API(MAPI) : Works same as IMAP.
4. Simple Mail Transfer Protocol(SMTP) : Responsible for sending and receiving email. Uses port 25. Easy to spoof SMTP and send the fake mail.

Email Analysis : Email crime investigation or analysis contains the following steps:

1. Examine the email message
2. Copy the email message
3. Print the email message
4. View the mail headers
5. Examine the email headers
6. Examine attachment if it is there in email
7. Trace the Email

1. Examine The E-mail : Whenever email crime has happened then it is necessary to collect the evidence which is required to prove the crime in the court of law. Evidence may be gathered from the victim. Steps for the same are as follows :

I. First take the image of machines hard drive.
II. Obtain the victim machine password to open the encrypted file.
III. Take the printed copy of the crime mail (including header)
IV. Examine the IP address of the sender's server

2. Copy the email message into the USB key.

3. Take the printout of the email message by using the print option available in the mail program.

4. View the mail header :

I. To check the mail header

II. Open your mail

III. Right click on your mail.

IV. After right click menus will display. Click on view full header.

V. The file header will get opened.

5. **Examine The Email Header :** The email header contains the message header and the subject body. The email header contains the information of the email origin. You can see in the given message that the IP address of the senders machine is sent. It also give the return path, and the receiver mail id.

6. **Examine the attachments :** If the mail contains any attachment then copy that attachment and also take the print of the attachment

7. **Trace the Email :** The IP address of the origination computer machine tells the owner of the email address which has been used in the possible crime that is being investigated. It may be possible that this information may be fake. So its important to validate the evidence which you uncover. There are many sites which tell owner associated with the domain name . The examples of the site which tells the owner of the mail associated with the sites are:
   1. www.arin.net :
   The ARIN (American Registry for Internet Numbers) is used to find the domain name from the IP addresses. It also gives the contact personal listed against the domain name.
   2. www.freeality.com :This website provides many different searching options like names, phone number and mail address. This websites permit the users to reverse email searches. This may help to reveal the subjects original identity.

E-mail Headers and Spoofing : Email spoofing is the forgery of an email header.The message which you receive is actually originated from someone else than the actual user.

1. Email Spoof with PHP function mail0 : The mail() function allows you to send mail. Bool mail(string $to, string $subject, string $message [, string $additional headers[, string $additional parameters]])
2. Email Spoof with telnet : Open command prompt and type telnet 25.

Email Recovery Tools : The list of the email recovery tools is as follows:

- FINALeMAIL
- Email Examiner
- Network E-mail Examiner
- R-mail

Laws Against e-mail Crime :

The CAN-SPAM Act :

- The CAN-SPAM Act, a law that sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have you stop from emailing them, and spells out tough penalties for violations
- It covers every single business message, which the law characterizes as "any electronic mail message the basic role of which is the business ad or advancement of a business item or administration," including email that advances content on business sites.
- Each separate email infringing upon the CAN-SPAM Act is liable to penalties of up to $16,000
- CAN-SPAM's Main Requirements:

1. Try not to utilize false or deceiving header data. Your "From," "To," "ReplyTo," and directing data - including the beginning space name and email address - must be exact and distinguish the individual or business who initiated the message.

2. Try not to utilize tricky titles. The headline should precisely reflect the content of the message.

3. Recognize the message as a promotion. The law gives you a great deal of space in how to do this, however you should reveal unmistakably and prominently that your message is an ad.

4. Tell recipients where you are located. Your message must incorporate your substantial physical postal address.

5. Advise recipients how to quit accepting future email from you. Your message must incorporate a reasonable and prominent clarification of how the recipients can quit getting email from you later on. Specialty the notice in a way that is simple for a customary individual to perceive, read, and get it. Innovative utilization of sort size, shading and area can enhance lucidity. Give an arrival email address or another simple internet based approach to enable individuals to impart their decision to you. You may make a menu to enable a recipients to quit specific sorts of messages, however you should incorporate the choice to prevent every single business message from you. Ensure your spam doesn't shut these quit requests however you should incorporate the choice to prevent every single message from you.

6. Respect quit asks for immediately : Any quit component you offer must have the capacity to process quit demands for no less than 30 days after you send your message. You should respect a recipient's quit demand inside 10 business days. You can't charge an expense require the recipient to give you any specifically recognizing data past an email address or make the recipient make any stride other than sending an answer email or visiting a solitary page on an Internet site as a condition for respecting a quit demand. When individuals have revealed to you they would prefer not to get more messages from you can't move or exchange their email addresses, even as a mailing list.The main special case is that you may exchange the addresses to an organization you have procured to enable you to conform to the CAN-SPAM Act.

7. Monitor what others are doing on your behalf : The law clarifies that regardless of whether you employ another organization to deal with your

email advertising, you can't contract away your lawful duty to conform to the law. Both the organization whose item is advanced in the message and the organization that really sends the message might be considered lawfully dependable

Section 66A : Sending offensive messages through communication service, causing irritation etc through an electronic communication or sending an email to mislead or deceive the recipient about the origin of such messages (commonly known as IP or email spoofing) are all covered here. Punishment for these acts is imprisonment up to three years or fine.

Chapter 5 : Messenger Forensics : Yahoo Messenger

Yahoo Messenger : Yahoo Messenger is one of the popular instant messaging clients from Yahoo. By using the yahoo messenger you can send messages, photos, videos, files. You can do video chat as well as internet phone calls. Yahoo messenger has some default preferences such as alerts, sounds and signing into Yahoo Messenger. In yahoo messenger by default chat messages are archived and saved but these messages are cleared out once the user signs out of Yahoo Messenger. If you do not log out then it is possible to view these archived messages.

Data Analysis In Yahoo Messenger : Investigation of the evidence start from the registry structure for Windows Vista and Windows 7 using the built in registry editor for Windows. The registry is examined with respect to the Yahoo Messenger files. Windows registry structure is same as Yahoo Messenger registry structure. While investigating the investigator tries to find out the following things on the computer :

1. Yahoo user ID of the person who is using the account version of the Yahoo Messenger installed on the computer.
2. All the revisions made to the YM version,
3. if the save password option is turned on and also if the Auto sign in has been enabled.
4. There is one extra feature in Windows Vista that is P2P count P2P count is the number of allowed P2P users who can send huge data among each other.

User\Software\Yahoo\Pager\profiles\profile_name\chat : Location shows the last selected chat room category, but not essentially the correct chat room entered. Using this information investigator can understand chat room category that the predators potentially use.

User\Software\Yahoo\Pager\profiles\profile_name\chat\favourite_rooms: Location provides the list of saved favorite rooms for the user. This information is important to understand the different chat rooms that the predator uses.

User\Software\Yahoo\Pager\profiles\profile_name\FT : Location provides the last saved location of a received file as well the last sent location of a transferred file, that is, the location from where the last sent file was uploaded. This information is useful when validating whether a user has been sharing or receiving files.

User\Software\Yahoo\Pager\profiles\profile_name\FriendIcons: Location provides the icon that the user has set for himself, that is displayed to the user's friends. The name of the file used will be visible in the path as well as where it is located on the hard drive.

Photo Sharing: Creation of the "S" Folder : In the Yahoo Messenger whenever a photo sharing session is initiated from a Vista machine, a photo sharing folder starting with the letter "S" is created in the Program Data folder. In addition random assigned numbers and alphanumeric characters are appended to the end of the naming structure. The following is the path for the created "S" folder :

C:\ProgramData\Yahoo!\Messenger\PhotoSharing\Sc8b0

The "S" folder is created when the user initiates the photo sharing session. Once the session is initiated, immediately the other yahoo user accepts the photo sharing invite, the S folder is created in the Photo Sharing folder on the initiator's side. The "S" folder is empty until a picture is shared. As soon as an image is shared or sent, a thumbs file `_t.jpg' is created followed by the image file ~m.jpg'. The name of this file is displayed as randomly assigned series of alphanumeric characters. If there are multiple chat sessions and photo sharing sessions open on users machine then at the same time with different users, a different " folder is created for each chat session.

File Transfer in Yahoo Messenger : Two ways of sharing a photo :

1. Yahoo Photo Sharing
2. File Transfer Option

File Transfer Option : For the photo sharing the "S" folder' creation is applicable but it is not applicable to file transfer. If the user wants to save the photos through Photo Sharing the default folder where these pictures will be saved is in the Picture folder. The 'picture" folder is a shortcut located under Libraries. The

full path is "C:\Users\UserName\Pictures". The user can save the photos to any location they wish on the computer. The file transfer is used to transfer all types of media such as, photos, music, documents, etc.

Chapter 6 : Social Media Investigation

Social Media is a rich wellspring of data for pretty much any examination. In the event that your objectives incorporate get-together data about somebody's developments. Partners, or character ,social media investigations are incredible fit.

Popular Social Media Sites :

- Facebook
- Linkedin
- Twitter
- Youtube
- Instagram
- Linkedin
- Tumblr
- Reddit

Gathering Evidence for Court :

For court cases social media is a great source. Evidences are collected to prove someone's character, prove or disprove defense, or collect other various supporting evidence Investigator collects the more information from statuses, photos tweets from social media. The metadata attached with the post is used to determine where someone was at a given time it also provides information about someone s claims, or even establish their reliability as a witness. Social media evidences should be collected methodologically with proper metadata and other validating information intact. If the evidence is not collected properly then it won't be considered in the court.

Types of Evidence Typically Collected For Court Cases :

- Relevant statements or comments.
- Metadata from posts establishing time and location of posting
- Posts relating to past illegal activity
- Photos
- Content establishing character (for example, attiudes to police, past sentiments, racist or Sexist content etc)
- List of social media profiles and screen names associated with target individual.

Employment Checks :

- The social media is also used in employment where the employer can assess your character, work experience, and education.
- Social media investigations helps to find the past illegal behavior, provide evidence to support or discredit claims about education and employment and assess whether they are probable to conduct themselves in a manner befitting your organization. Before conducting social media investigation on an employee, you should know that these types of background checks are subject to the fair Credit Reporting Act.
- It means applicants consent is needed.

Types of Evidence Typically Collected:

- Posts and photos relating to illegal activity or **drug use**
- Posts relating to objectionable content (e.g. **racist or sexist** content)
- Relevant statements and comments.
- List of social media profiles and screen names associated with target individual

Person Location :

Social media posts contains location data .it will be helpful you to find your long lost friend then social media is useful. Social media investigations merge social connections and biographical information to find people.

Tools Used For Social Media Investigation:

Screencast-O-Matic :

Screencast –O –Matic tool is used to record the screen. This too; record the social media screen as evidence. It records the posts, comments, photos and video posted on the social media.

Browser Forensics :

Web browsers overview :

- Nowadays there are many web browsers available in market like internet Explorer, Google Chrome, and Mozilla etc.These all web browsers are slightly different in web services.
- To display the same website Faster on future occasions , web browsers maintain the Downloaded web site data, so that it remains available on the computer even if the user closes the browser or shuts down the machine.
- The downloaded web files are known as caches, cached history or temporary files.
- Based on the operating system and browser applications are in different locations.

Internet Explorer :

The most famous web browser is Internet Explorer (IE) as it is a component of the Windows operating system. IE is frequently used as a default web browser

In windows 10 IE is replaced with Microsoft EDGE (ME) .IE and ME both work in private mode, without storing information about web resources visited by the user.

Google Chrome :

Google Chrome is browser by provided by Google It has incorporation with Google Services. It allows the Synchronization of user passwords between devices. One can use the extensions and plug-in.Google Chrome performs fast operations and collects user data but it Consumes large amounts of memory. The important feature of google chrome is that it works in Incognito mode, which prevents the browser from permanently storing any history information , cookies , site data or from inputs. There are many web browsers created by the third party developers based on Chrome Engine like Chromodo, Amigo Sputnik, Uran Epic Browser, SafeZone,Comodo Dragon Flock,Rockmelt Sleipnir SR Ware Iron, Titan Browser, Torch Browser, 360 Extreme Explorer. Avast Chromium, CoolNovo ,Coc Coc ,Vivaldi, Yandex. Browser, Opera , Orbitum Breach

Nihrome Perk QIP Surf, Baidu Spark, etc. All of these browsers function like Google Chrome and create web browser artifacts like Google Chrome and also support most of Google Chrome's extensions and plugins.

Opera : The Opera web browser is also a famous web browser .it was the first web browser to introduce features that other web browsers adopted like pop-up blocking, Speed Dial, Private browsing and tabbed browsing re-opening recently closed pages. Opera have a free Virtual Private Network (VPN) service which permits users to surf the web incognito.

Firefox : Firefox is also one of the popular web browsers. It is more secure as compare to other Browsers. It has advanced Incognito mode, disabling tracking of users locations and advertisements. Firefox has its own extensions

Difficulties of web browsers forensic analysis : Following difficulties are faced by the forensic examiner while analyzing the web browsers:

- Many web browsers are available with lots of data.
- Different data to protect the data Encryption is used.
- If the user is using the Incognito mode (private mode) then computer do not contain the browser artifacts.

Web Browser forensic artifacts : Each web browser has its own artifacts in operating system. The artifacts are depend on the version of the web browser usually one can get the following artifacts:

- History
- Cache
- Cookies
- Typed URLs
- Sessions
- Most Visited sites
- Screenshots

- Financial info
- From values(Searches, Autofill)
- Downloaded files(Downloads)
- Favorites

Cookie Storage and Analysis:

- Cookies are the text files .These files are used to feedback from the user to the server.
- When performing some actions with a web resource like viewing web links, downloading files, etc, these actions are registered in a cookie that secretly sent by the server to the user's computer.
- By using this web resource, the server can find out what actions the user has taken on previous visits to this web resource.
- The cookies are stored in cookies folder but the location of cookies folder is based on the web browser and the operating system.

Analyzing Cache And Temporary Internet Files :

- **Cache Files :** The cache folder contains the browser history and it automatically creates the profile folder at start. This folder is the storage place for the browsing history

- **Windows Temporary Internet Files :** Are immediate downloads from the internet, more often than not containing realistic pictures in Windows bitmp(bmp),jpeg,gif,or art format. There will likewise be html and htm files for Website home page components,and so forth.Approaching Yahoo and Hotmail messages may likewise exist as in the Temporary Internet Files folder.Downloaded movies ,mpege.avi files,and Adobe PDF files will not be found in Temporary Internet Files.

- **Temporary Files :** Windows Temp Files (C:\Windows\Temp)are temporary files made by Windows as different programs are running and diverse processes are occurring. They are regularly exact copy of files put away somewhere else on the PC. At different occasions they are exact duplicates of files which are waiting to be handled by the PC

How is the data stored ?

- Internet Explorer and Windows Explorer store most of the data in index.dat files.
- INDEX.DAT files are used by Internet Explorer to store information about visited about visited pages, cookies and the time they are used.
- To this end , Internet Explorer indexes files that are located in folders that are browser caches
- And maps these files to the network resource from which these files were downloaded.
- In addition, INDEX.DAT files contain such information as the decryption of HTTP-header packets, in which the was
- Transferred, the date of creation and last access to the file, the number of calls to it and much more.

Web Browsing Activity Reconstruction

To reconstruct the web browsing activity, you have to reconstruct it from cached file in users computer .Examine Cached files created by web browsers.The following are the steps to reconstruct the web browsing activity:

- First cheek the cookies folder, here we are considering browser firefox and operating system
- Is windows XP, so you get the cache file at the location given below:
- *Check the cache file at the given location*
- *Check the favorites at the given location*
- *For session recover check the following location*
- *Check the downloaded file given at the following location*
- *Check the URL's visited in the location given below*
- *Check the from value*

- *Check the typed URL's*
- *Check the session restore artfacts*

Google Chrome, safari, Firefox, Opera store most of the data in SQLite databases. Manual analysis of these databases and carving will allow you to extract the maximum amount of data. When analyzing SQLite data bases, remember Some deleted records can found in Freelist—unused tables that can contain deleted data.

Where can I find the Web Browsers artifacts?

- Physical dumps of mobile devices.
- File systems of mobile devices
- Backups of mobile devices.
- Data, which can be extracted from Clouds.
- Hard drives
- Images of hard drives.
- Memory dumps.
- Hibernation and page files
- Location metadata from posts.
- Location metadata from images.
- Relevant statements and claims.
- Photo analysis.
- Leads from interviews and social connections

Chapter 1 : Evidence Analysis:

- The evidence is any information of supporting value, that means which proves or helps to prove something relevant to the case
- The digital evidence consists of the data on a computer , images audio and video.
- It is a data and information of value to an investigation that is stored on an electronic machine, received or transmitted by an electronic machine.
- You can acquire the evidence when data or electronic machines are seized and secured for the examination. Examples of evidence are a fingerprint, DNA, files or system, etc.
- The problems in acquiring digital evidence are :

1. Digital Evidences can be easily modified, damaged or destroyed.
2. Digital Evidences are time sensitive

The places from where you can the digital evidence are:

I . Computers.

Ii. External hard drives

iii. Floppy disks

iv. Pen Drive

v. CDs and DVDs

vi. Thumb drives

vii. cell phones and mobile devices

viii. Voice over IP phones

ix . Answering machines

x. iPods

xi. PDAs

xii. Electronic game devices

xiii. Digital video recorders (Tivos)

xiv. Digital cameras

xv. PSAs

xvi. GPSs

xvii. Servers

xviii . Routers

xxi. Fax machines

xx. Wireless access points.

xxiii. Photo –copiers that buffer files xxiv. Scanners that buffer files.

Evidence Characteristics : There are characteristics of evidence. They are as follow :

1) Admissible
2) Authentic
3) Complete
4) Reliable
5) Acceptable

1) **Admissible :** Evidence ought to be acceptable , if the proof you reveal wont stand up in court you have squandered your time and conceivably allowed a guilty party to go unpunished
2) **Authentic :** Evidence ought to be Authentic ,Authentication is directly related to the incident being investigated. The investigation may reveal evidence that is interesting but not relevant.
3) **Complete :** Evidence ought to be Complete The specialist ought to approach the case with no assumptions about some body's blame or blamelessness. Criminological routines ought to take out option Suspects and clarifications until an unmistakable conclusion is come to
4) **Reliable :** Evidence ought to be Reliable. There ought to be no doubt about the reality of the specialist decisions Reliability originates from standardized and verified forensic tools and techniques . Qualification of a specialist as an expert witness for a case will set up believability and reliability.
5) **Acceptable :** Evidence ought to be acceptable. The investigator must create results that are clear and straight forward even among the most nontechnical individuals from a jury. Have different agents have used the same forensic techniques and reached similar conclusions .

Authorization to Collect the Evidence:

- Digital evidence can be fragile and exceedingly delicate . Cyber security experts understand the estimation of this data and regard the way that it very well be effectively compromised if not appropriately handled and ensured.
- Therefore it is basic to set up and pursue strict guidelines and procedures for exercises identified with computer forensic investigations. Such procedures can incorporate detailed instructions about when computer forensics are authorized to recuperate potential digital evidence how to appropriately prepare systems for evidence recovery where to store any recovered evidence and how to record exercise to help guarantee the authenticity of the information.
- In Criminal cases Law enforcement agencies train the persons as technicians to make sure the preservation of the evidence.
- They follow strict procedures for forensic cyber security divisions have to set forth rules of governance for all other digital activity inside an organization
- Actions for collecting the evidence are defined by the law enforcement such as where to look for said evidence and how to handle it once it has been retrieved. Before the investigation it is important to understand the warrant and authorization In criminal matters there are laws related to search warrants.
- In the civil matters the company officer has the right to collect the evidence The company officers are not trained one. In civil proceeding it is assumed that a company is able to investigate their own equipment without a warrant Providing the privacy and human rights of employees are observed.
- Any individual who is using a computer system can collect the data from the system for example a wife can collect data from the husband computer or vice versa.

Acquisition of Evidence :

- Once exhibits have been seized an accurate sector level duplicate (or forensic duplicate) of the media is created usually via a write blocking device a process referred to as Imaging or Acquisition. Obtaining Volatile Data Prior to Forensic Duplication .
- Data which is in a state of change is called volatile data. The data in the computer system will get lost as the power loss., Volatile data is present in the active physical memory. We will find the volatile data in physical memory, registers, virtual memory in the file system and in the peripheral device memory.
- To ensure all relevant data are collected, you should prepare an order of volatility while gathering evidence, the Order of Volatility (OoV) should be from the most volatile to the least.
- If you are certain that you may be doing a forensic duplication of the target device, you have to focus on obtaining the volatile system data before powering down the system. The risky information consists of presently open sockets, strolling approaches, the contents of system RAM, and the location of unlinked documents.
- The unlinked files are documents marked for deletion while processes that get entry to it to terminate.

Collecting the Data :

1. Date and time of system .
2. Currently logged on the users list.
3. Entire file systems time and date stamp.
4. Currently running processes list.
5. Currently open sockets list
6. The applications listening on open sockets.

7. A list of the systems that have current or had recent connections to the system.

The Following steps are taken to collect the live data:

1. **Execute a trusted shell :** When you are responding to a targeted system on which UNIX operating system is running. you will come across one of two scenarios :
   1. The system runs in console mode.
   2. The system runs X Windows, a GU1 like to the Windows desktop.

   Exit the X windows prior to you begin your response; it helps to avoid common X Windows-based vulnerabilities that permit the attacker to log keystrokes.If you are responding to a Linux system, you possibly able to switch to another vital
   by pressing ALT-F2
   To avoid generating traffic Log on locally at the victim console with root-level privileges. Now mount the trusted toolkit and respond with trusted tools
   The following is the command syntax to mount a floppy drive when responding to a Linux system

   mount/dev/fd0/mnt/floppy

   -This command mounts your trusted toolkit on the mount point/mnt/floppy. To access the trusted file change the directory to /mnt/floppy
   The first step in all response is to be certain you are executing a trusted command shell.

   The Unix shells can be trojaned by attackers to log all the commands executed or to perform immoral and evil operations invisible to the investigator
   Therefore, you will want to execute your own trusted shell. Once you have execute your trusted shell, set your PATH environment variable equal to dot ().

This will decrease the chances of someone accidentally executing untrusted commands that are in the target system's PATH.

2. **Record the system time and date :**

   The local date and time settings are important for later correlation of time/date stamps, and they also show when you were on the system.

   To capture this information, use the date command
   .
   [root@conan/root]#date
   Tue Dec 17 16:12:43 UTC 2003

3. **Determine who is logged on to the system :**
   The (what) command determines who is logged on. It displays the logged on userIDs, and from which system they have logged on. It also shows what they are currently executing on the system with the date and system time

4. **Record modification creation and access times of all files :**

   ~ You may need to retrieve all of the time/date stamps at the file device. As with home windows structures, Unix structures have 3 time/date stamps to collect for every file and listing: get right of entry to time (atime), amendment or modification
   (mtime), and the inode alternate time (ctimc). An inode is a data structure in Unix which is used to represent file system objects
   You can use a depended on Is command with the proper command-line arguments to obtain those times for every file. The subsequent strains show the way to obtain the time/date stamps and show the output on a trusted floppy disk :

   Is -alRu/> /floppy/atime
   Is-alRc/>/floppy/ctime
   ls-alR/>/floppy/mtime

5. **Determine open ports :-** The netstat command is used to determine the open ports. By using netstat - a command is used to view all open ports.

The -n option tells netstat to not resolve hostnames, which reduces the impact on the system and speeds the execution of the command.

6. **List applications associated with open ports :** With the netstat command -p option is used which maps the name of the application and its Process ID (PID) to the open ports.

7. **Determine the running processes :** Taking a snapshot of all the running processes during the initial response is critical. This can be done by using the standard ps(process status) command.
   - The output varies a bit among the different UNIX flavors
   1. Use ps -caf on Solaris systems
   2. Use ps-aux on FreeBSD and Linux systems.

8. **List current and recent connection :** The netsat command provides information about another aspect of live response: current and recent connections. The command usage is identical for determining which ports are open.

9. **Record the steps taken :** Finally, record all of the commands you have issued to the system. There are several possibilities here: use script, history, or even if you performed your live response from the editor. Since you issued all commands from a trusted shell, using the history command will record all of the commands you have executed. However a better choice is the script command, which will record your keystrokes and the output. If you choose to use the script command, you'll need to run this command before you perform the live response

10. **Record cryptographic checksums :** Finally, record the cryptographic checksums of all recorded data. Simply run the md5sum program against all files in the data directory,

11. **Scripting the initial response :** Writing a simple shell script to automate the collection of live data.

Reports on the Findings :

Report Goals : Report should always meet the standards established by the organization and hence it is necessary that it has some goals.

1. Details of the incident should be accurately described
2. A report must be understandable to the decision-makers
3. A report should withstand barrage of legal examination
4. A report should be clear and not open to misunderstandings
5. A report should be easily referenced
6. A report should contain all data needed to explain your conclusions.
7. A report should offer valid conclusions, opinions or recommendations when required.
8. A report should be created in a timely manner

Report Writing Guidelines :

1. **Document investigation steps immediately and clearly :** Write everything down in an understandable format for you as well as for others. Do not use shorthand or shortcuts. Unclear notations, incomplete scribbling, or unclear documentation leads to redundant efforts, forced translation of notes , confirmation of notes and a failure to comprehend notes by yourself and or others. As you discover evidence writing it down clearly and concisely saves time and promotes accuracy. Also the details of the investigation can be communicated more clearly to others as and when required. This is known as "write it tight" philosophy.
2. **Know the goal of your analysis :** Important to know the goals of your examination before you being analysis. Your report should unearth evidence that confirms or dispels the elements which are required to prove the crime.
3. **Organize your report :** Organize your report to start at a high level and increase the complexity of your report. The high level executive would then have to read only the first page so as to get idea of your conclusions. Include a table of content for longer reports.

4. **Follow a Template :** Follow a standardized report template. This template makes your report writing scalable, establishes a repeatable standard and saves time.

5. **Use Consistent Identifiers :** You have to create a unique identifier or reference tag for each person, place, and thing(noun) referred to in your report

6. **Use Attachments and Appendices :** Any information, files and file fragments that you cite in your report that are over a page long should be included as appendices or attachments.

7. **Have co-workers read your reports :** Employ other co-workers to read your report. This helps develop reports that are comprehensible to non-technical personnel who have an impact on your incident response strategy and resolution.

8. **Use MD5 Hashes :** Create and record MD5 hashes of your evidence, whether it is an entire hard drive or specific files.

9. **Include Metadata :** Record and include metadata for every file or file fragment cited in your report. This metadata includes time/date stamps, full path of file, the file size, and the file's MD5 sum.

A template for Forensic Reports:

1. **Executive Summary :** This section gives the background data of the conditions that realized the requirement for an investigation. The senior management reads translation summary, they need not go to the detailed report.

2. **Objectives :** Used to outline all the tasks that our investigation planned to complete. The prepared plan list should be discussed and approved by the legal counsel, decision-makers, the client before any forensic analysis.

3. **Computer Evidence Analyzed :** All collected evidence and their interpretations are introduced. Here we get detailed information about the assignment of evidence tag numbers, media serial numbers and description of the evidence.

4. **Relevant Findings :** Findings of probative value.
5. **Supporting Details :** Outline all the tasks undertook to meet the objectives.
6. **Investigate Leads :** Actions that could be carried out to discover additional information related to the investigation.
7. **Additional Subsections such as Attacker Methodology, User Application :**

   Additional Subsections are depended on the need and want of the client.

   Attacker methodology gives additional briefing to help the reader understand the general or exact attacks performed. Useful in computer intrusion cases.

   User Application : Relevant applications that are installed on the media analyzed.

8. **Internet Activity And Recommendation :**

   Internet activity gives details about the web surfing history of the user or media analyzed. Recommendation section gives the recommendation to posture the client to be more trained for the next computer security incident.

Testimony :

- **Preparing For Testimony :** Whenever your case goes to the court the forensic player plays two roles: technical/scientific witness and expert witness. As a technical/scientific evidence the forensic examiner gives only the information which is found in an investigation.
- **Documenting And Preparing Evidence :** It is necessary to document each and every step. Also it is necessary to gather and preserve evidences too.
- **Reviewing Your role as a Consulting Expert or Expert Witness :** Based on your lawyer's requirement you may only give your opinion and technical expertise of him instead of testifying in court; this is known as consulting expert.

- **Preparing Technical Definitions :** Prepare the technical definitions of the concepts before you testify in court. These definitions can be used when your lawyer or the opposing lawyer questions.

Chapter : Introduction To Legal Aspects Of Digital Forensics

Introduction to Legal Aspects of Digital Forensics :

Laws are divided into three bodies :

1. Criminal
2. Civil
3. Administrative/Regulatory law

1. Criminal Law :

- These laws are made to protect society and individuals from harmful behavior. Intended to punish offenders as discouragement both to the wrongdoers and to others and by placing the offender in the jail.
- Criminal protests can be filed by individuals, Law authorization offices, people who watch offence and those Who are hurt.
- Crime characterized in the state penal code is prosecuted by state and a federal crime is prosecuted by the federal government.
- Complaint : Person or entity filing the charge
- Defendant : Person(or company) against whom the charges are filed.
- Penalties : Violating a criminal law can include monetary payment or loss of liberty. These can range from light to severe. For example, A warning citation(usually in case of traffic law or low level of crimes) or a citation that imposes fine, Compensation or settlement(money going to victim), Community service or administration (required "volunteer work for some Organization or governmental body, Probation (supervision by the government for a specified period of time in lieu of imprisonment, which can include court-order restrictions on behaviour such as no use of computers or required attendance at counselling sessions), Confinement in prison (usually for a limited time, such as a couple of days to a year or for a more extended time and can extend a few months to life) or for the death penalty (for the people who convicted murder)
- Criminal offenses are usually categorized in keeping with the seriousness of the crime and the severity of the penalty.
- These classifications can consist of the following :

1. Violations : The least critical offenses, for this penalty is only fine
2. Misdemeanours : It is serious than violations with a penalty and jail term
3. Felonies : It is a serious offense, which bring a penalty of imprisonments(in some jurisdictions death penalty for severe case

2. Civil Law : The goal of civil law is to settle disagreements between persons or entities. In civil law the style of the case usually consist of two private parties Some terms related to civil law are :

- Torts : Civil wrongs
- Plaintiff: The party who initiates the lawsuit
- Respondent/Defendant : The person against who is the suit is brought.

The losing party in a civil suit does not generally go to jail or prison unless also convicted of a criminal offense such as contempt of court. Instead, he or she is subject to one of two types of court orders :

1. An order requiring that the respondent should pay the money for damage. The damages can include compensatory damages for the actual and expected losses suffered by the plaintiff both tangible and intangible and punitive damages beyond the actual losses made to punish the party who committed the wrong.

2.An injunction requiring that the respondent do some specified action or not do some specified action. For example, there can be an order to the party for to stop sending mail to the plaintiff. An injunction is a legally binding order, and ignoring it can result in criminal charges

3. Administrative/Regulatory Laws :

- Administrative law is the third body of law this body of law is often overlooked discussions of criminal and civil law. Also known as regulatory law.
- This body of law consists of rules and regulations that are approved by a governmental agency under authority given to it by the legislative body and that applies to a particular occupational field or governs a particular area of life
- Examples are Environmental Protection Agency regulations as well as rules that govern the practice of medicine, law, engineering, and the like
- Administrative laws are neither criminal nor civil yet have the power of law inside of their regions of purview. For instance, an administrative

activity can be specialist or lawyer who disregards the state administrative organization's rules.

- In the event that discovered liable, the blamed individual may be rebuffed, fined, or have his then again her permit disavowed. (On the off chance that the recent happens, and the individual keeps on honing, criminal accusations of honing without a permit could be brought)
- Administrative activities are generally led by set out by law that are like those of a court yet the committees or different bodies that hear the cases are not officers of the court. Thus the procedures are called quasi-judicial.

Levels of Law : The scope of law falls into one of the following level/category :

1. Local laws
2. State laws
3. Federal laws
4. International laws

- The processes of approving these laws are very similar, the differences are the legislative body that approves them, the executive officer who signs them, and the geographic jurisdiction within which they can be enforced.
- Local laws are approved by a city or town council or by a county commission, signed into law by the mayor or a county judge.
- Some cities and counties give the executive officer the power to veto laws; in others, the signing is a mere formality
- Local laws are also known as ordinances. Cities and counties can approve ordinances to make certain acts criminal offenses, but generally only at the lowest levels
- For example, in Texas a criminal offense under city law is a Class C misdemeanor the lowest level of criminal offense. Local laws can be enforced only within the boundaries of the city or county that approves them.

- The People who violates the ordinances are tried in municipal or county courts.
- These courts often are not courts of record that are; no court reporter records the proceedings. A guilty verdict in these lower courts can be appealed to a higher court of record.
- Cities and counties could pass laws regarding computer and network usage, but this generally done at the local level.

2. State Laws :

- The laws enforced by police including municipal police and county sheriffs/judges offices are state laws, passed by a state legislature and signed into law by the state governor
- Many states have a bicameral legislature patterned after the U.S. Congress, so the laws must be passed by both houses.
- In some states, the governor has veto power. States can pass criminal laws at all offense grades (misdemeanors and felonics), with penalties ranging from fines to the death penalty (in states that allow it).

3. Federal Laws : The U.S. Constitution grants all federal legislative powers to Congress, which comprises of two branches
   (a) The Senate
   (b) House of Representatives

Process of Federal law formation:

- Federal laws are introduced as bills in either the House or the Senate and are debated and amended in committee, where public hearings may be held to obtain citizen input, before being brought to the full body for a vote.
- After passage by one branch the bill must go to the other. If changes are made there, it comes back to the originating body for approval and it goes back and forth until agreement is reached.
- Alternately, a gathering advisory from both the House and Senate may be selected to determine the distinctions.

- Once a law has been gone by both bodies, it goes to the President, who can sign it, veto it, or let it go into law without mark. A presidential veto can be overridden by vote of 66% dominant part of both the House and Senate. Federal criminal laws are upheld by the FBI and other requirement organizations that have practical experience specifically regions of law, for example, the Drug Enforcement Administration (DEA): the Bureau of Alcohol, Tobacco and firearms and the Criminal Investigation Division of the Internal Revenue Service.
- The FBI examines government cybercrime offenses, and the Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the Department of Justice gives lawful skill to elected prosecutors
- The national government doesn't have general police powers inside of the states. That is the FBI can't capture individuals for infringement or violation of state laws.

4 International Laws : Laws can likewise begin through settlements, which are agreement gone into between nations

Levels of Culpability : Intent, Knowledge, Recklessness, Negligence

Culpable means Responsibility. Culpable mental states are as follows :

1. Intent
2. Knowledge
3. Recklessness
4. Negligence

1. Intent : It is planned yearning of the person to obtain the outcome of the act.

2. Knowledge : The person knows that the act will result the outcome
3. Recklessness : The person is aware about a huge threat if he or she engages in the act; it will bring about the outcome

4. Negligence : The individual should have realized that there was a generous danger that he or she engaged in the act

Level and Burden of Proof Criminal Versus Civil Case :

In criminal law the level of proof required to prove that a person is guilty and civil law the side at which the burden of proof lies is required in order to prove the case.

Criminal Case/Law	Civil Case/Law
Burden is on the prosecution to prove its case	Burden is on the respondent who is accused of a civil wrong to prove that he or she is not reliable
Level of proof required is very high	Level of proof required is very low as compared to criminal case
Guilt must be proven beyond a reasonable doubt	The party that proves by preponderance of the evidence wins the case.
All jurors must agree on the verdict.	Majority of jurors must be convinced.

Vicarious Liability :

- Lawful responsibility that one person has over other person's unlawful activity
- Usually created by some sort of over sight relationship.
- This oversight relationship means the person has control or other person and can be held civically liable for wrong s committed by that person.

Information Technology Act, 2000 :

Table shows the punishment of the IT Act.

Section	Punishment
Section 43	Any act of destroying, altering or stealing computer system/network or deleting information with act of damaging data or information without authorization of owner is liable to payment as compensation for the damage
Section 43A	Section of IT Act states any corporate body dealing with sensitive information and negligent with implementing reasonable security

	practices causing loss or wrongful gain to any other person will also be liable as convict for compensation to the affected party.
Section 66	Section states hacking of computer system by individual with dishonesty or fraudulently with 3 yrs. imprisonment with fine of Rs.5,00,000 or both.
Section 66A	This Section states any offensive information with demean character or information known as false but sent for purpose.
Section 66 B,C,D	This Section is for fraudulently or dishonesty using or transmitting information or Identity theft is punishable with 3 yr imprisonment or 1,00,000 fine or both.
Section 66E	This Section is for Violation of privacy by transmitting image of private area is punishable with 3 yr imprisonment or 2,00,000 fine or both
Section 66F	This Section is on Cyber Terrorism affecting unity, integrity security, sovereignty of India through digital medium is liable for life imprisonment.
Section 67	This section states publishing obscene information or pornography transmitting obscene information in public is liable for imprisonment up to 5 years or penalty of Rs. 10,00,000 or both.

Giving Evidence in Court :

The digital investigators are asked to testify(produce) their findings in the form of affidavit or expert report. The process of giving evidence in a court is as follows :

1. Testifying in a Cyber Crime Case
2. The Trial Process
3. Testifying as an evidentiary Witness
4. Testifying as an Expert Witness

5. Qualifying as an expert
6. Employing Experts
7. Giving Direct Testimony
8. Cross Examination Tactics
9. Using Notes And Visual Aids

1. Testifying in a Cyber Crime Case :

- The whole examination and working of the case record is pointed toward one final product getting a conviction of the cyber criminal in a court of law.
- Regardless of how great the evidence you acquire log documents demonstrating unapproved access to the system, hard disks seized from the presumes PC containing obvious signs of the criminal movement, organize records following the interloper back through Internet servers to his or her PC none of this evidence can remain solitary.
- Under most criminal justice systems, physical and intangible evidence must be bolstered by testimony. Somebody must testify with respect to when, where, and how the evidence was acquired and confirm that it is a similar when it is introduced in court as it was the point at which it was gathered
- At the point when evidence is technical in nature and troublesome for laypersons to understand, specialists might be required to testify to explain the nature of the evidence and what it intends to the jury and judge. Police specialists and IT Workforce may both be required to take the witness stand in a cyber crime case

2. Trial Process :

- The trial process really starts when a suspect is arrested or a warrant is issued for a presumes arrest.
- After the arrest, the respondent is taken under the steady gaze of a justice(a judge or, now and again, the mayor of a city or town) inside a predetermined time period more often than not inside 48 hours and charged.
- This allegation is a casual process whereby the justice tells the litigant what charges have been documented against him or her, Mirandizes the respondent, and sets or denies bail.

- A primary hearing normally happens inside a couple of days. In this hearing, the prosecution must present enough evidence to persuade the judge that the litigant/defendant ought to go to trial.
- In a few cases, the litigant goes before a grand jury rather than a judge. This is a mystery continuing in which the grand jury chooses whether to hand down a prosecution.
- Next, a formal allegation might be held, at which the respondent can enter a request for the charges against him or her.
- Prior to the real trial, there is generally a pretrial gathering or hearing at which motions can be documented (for instance, requesting for a change of venue). At last, the case goes to trial

3. **Testifying as an Evidentiary Witness :** An evidentiary witness has direct knowledge of the case, such as, a network administrator might be called to testify, to tell what he/she observed during an attack on the network or an investigator may be testified as to the evidence that he/ she observed on a computer that was seized pursuant to a search warrant. An evidentiary witness can only testify as to details (what he / she saw or hear) but cannot provide opinions or draw conclusions.

4. **Testifying as an Expert Witness :** There is no direct involvement of an expert in the case but has expertise or special technical knowledge that qualifies him/her to provide professional opinions on technical issues Some time the expert witness prepares the report, he/she outlines their opinion and give reasons for every opinion. In a few countries, expert witnesses are registered as experts in a particular field.

5. **Qualifying as an Expert :** If you are an expert witness; it is required for the people to know about the following details of yours :

   - What degrees do you have?
   - What positions have you held in the field?
   - What courses have you taught in this field?
   - What books or papers have you written pertaining to the field?
   - What is your past experience as an expert witness in this field?

6. Employing Experts : Individuals contract themselves as expert witnesses. These individuals have gained practical experience in wide range of technical or logical fields, including computer forensics. These witnesses are paid as a set of expenses basis and these expenses can include travel and lodging.

7. Giving Direct Testimony : While giving testimony one should take care of the following :

- Be on time or slightly early for the court
- Do not appear nervous
- Remain calm and do not get angry
- Do not volunteer extra information only answer the questions
- Dress professionally
- Consider the question before you answer.
- Speak clearly and confidently

8. Explain cross examination tactics : Be set up for and prepared to avoid from such cross-examination strategies as:

- Rapid-fire questions with no time to answer between questions
- Leading questions "Isn't it true that what… ?
- Prolonged silence designed to cause discomfort in hopes you'll say more keep in mind, when subjected to these tactics is this: Do not take the lawyers strategies or tactics personally; he/she is just doing a job. As a witness you do your job: maintain your cool and state the information.0

9. Notes And Visual : Cops utilize notes as a memory help amid court testimony constantly. A few members of the jury may be inspired by the way that you're perusing from notes, since they may confide in the written word more than somebody who depends on memory lone aids. Then again, others may believe you're being instructed or incited on the off chance that you refer to notes; they trust that if what you're stating is reality, you would recollect it without notes. A very important thought in choosing whether to utilize notes is the way that if a witness does so, the notes will be gone into evidence and taken into the custody of the court for the span of the trial. On the off chance that you do utilize notes, in this way, it's imperative to make sure that the journal or paper on which they're composed doesn't have different notes that refer to issues not related with the case, on the grounds that the opposing lawyer can question you concerning anything in the notes