Chapter 5: Understanding Computer Forensics

Understanding Computer Forensics: Introduction, Historical Background of Cyberforensics, Digital Forensics Science, Need for Computer Forensics, Cyber Forensics and Digital Evidence, Digital Forensic Life cycle, Chain of Custody Concepts, network forensics.

Learning Objective

- Fundamental concepts in Cyberforensics
- Understand the meaning of the term "Cyberforensics and the need for Cyberforensics
- Learn what "digital evidence" means along with the base term forensics science
- Get an overview of cardinal rules of computer forensics.
- Learn how Cyberforensics is used in cybercrime investigations
- Understand the legal requirements for Cyberforensics and compliance aspects of Cyberforensics
- Get an overview of the role of forensics experts.
- Understand the "data privacy issues" involved in Cyberforensics
- Forensic Auditing, Cyberforensics tools available, Challenges faced in Cyberforensics

5.1 Introduction,

- Cyber forensics plays role in investigation of cybercrime.
- Evidence in the case of Cyber offenses is extremely important from legal perspective.
- There are legal aspects involved in the investigation as well as handling of the digital forensics evidence.
- Technically trained and experienced experts are involved in the forensics activities.
- Use of hand-held devices are incensing now a days. [PDA (Personal Digital Assistance), mobile Phones, iPods]
- Use of data mining in cyber forensics, forensics auditing and anti-forensics.

5.2 Historical Background of Cyberforensics,

- The Florida Computer Crimes Act was the first computer crime law to address computer fraud and intrusion. It was enacted in Florida in 1978.
- The application of computer for investigating computer-based crime has led to development of a new field called computer forensics. Sometimes, computer forensics is also referred to as "digital forensics.

"Forensics evidence" is important in the investigation of Cyber-crimes.

- Computer Forensics needs DIGITAL EVIDENCE, in cases involving data acquisition, preservation, recovery, analysis and reporting, intellectual property theft, computer misuses corporate policy violation, mobile device (PDA, cell phone) data acquisition and analysis, malicious software/application, system intrusion and compromise, encrypted, deleted and hidden files recovery pornography, confidential information leakage etc.,
- The focus of Computer Forensics is to find out digital evidence.
- DE is required to establish whether or a fraud or crime has been conducted.

Computer forensics

- Computer forensics is primarily concerned with the systematic identification, acquisition preservation and analysis of digital evidence, typically after an unauthorized access to computer or unauthorized use of computer has taken place:

- while the main focus of "computer security is to computer systems as well as maintaining "confidentiality, integrity and availability of computer systems.

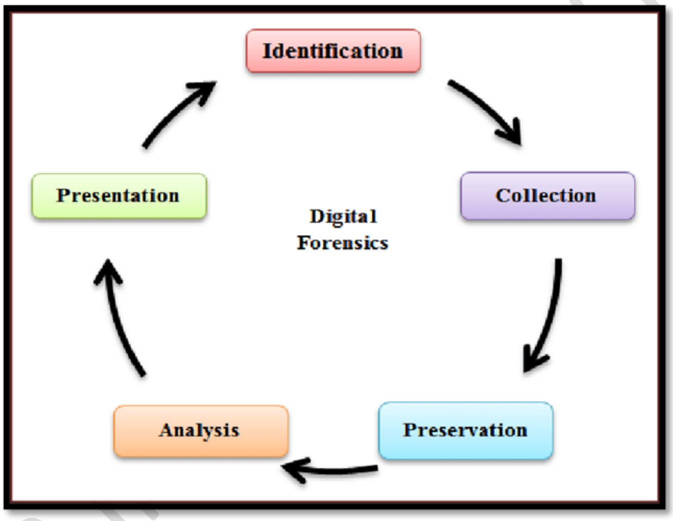
Two Categories of Computer Crime

- 1). Criminal Activity that involves using a Computer to commit a crime
- 2). Criminal activity that has a computer as a target.
- Typical types of data requested for a digital forensics examination by the law enforcement agencies include.
- 1) Investigation into electronic mail (E-Mail) usage, website history, cell phone usage, cellular and Voice over Internet Protocol (VolP) phone usage, file activity history, file creation or deletion, chat history, account login/logout records and more.

Q1: Discuss the Historical Background of Cyberforensics

Historical Background of Cyberforensics.

- Forensics means a "characteristic of evidence that satisfies its suitability for admission as fact and it persuade based upon proof.
- "Forensics science" is the application of science to law and it is ultimately defined by use in court.



5.3 Digital Forensics Science,

Digital forensics is the application of analyses techniques to the reliable and unbiased collection, analysis interpretation and presentation of digital evidence. There is a number of slightly varying definitions/The term computer forensics, however, is generally considered to be related to the use of analytical and investigative techniques to identify, collect, examine and preserve evidence/information which is magnetically stored or encoded

The objective of "Cyberforensics" is to provide digital evidence of a specific or general activity. Following are two more definitions worth considering:

1. **Computer forensics:** It is the lawful and ethical seizure, acquisition, analysis, reporting and safeguarding of data and metadata derived from digital devices which may contain information that is notable and perhaps of evidentiary value to the trier of fact in managerial, administrative, civil and criminals' investigations. In other words, it is the collection of techniques and tools used to find evidence in a computer.

2. **Digital forensics:** It is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation

and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

It is difficult to provide a precise definition of "digital evidence" because the evidence is recovered from devices that are not traditionally considered to be computers. (Some researchers prefer to expand the definition by including the "collection" and "examination" of all forms of digital data, including the data found in cell phones, PDAs, iPods and other electronic devices. In general, the role of digital forensics is to:

.

1. Uncover and document evidence and leads.
2. Corroborate evidence discovered in other ways (E-Discovery)
3. Assist in showing a pattern of events (data mining has an application here).
4. Connect attack and victim computers (Locard's Exchange Principle)
5. Reveal an end-to-end path of events leading to a compromise attempt, successful or not.
6. Extract data that may be hidden, deleted or otherwise not directly available.

.

The typical scenarios involved are:

1. Employee Internet abuse
2. Data leak/ data breach - unauthorized disclosure of corporate information and data (accidental and intentional);
3. Industrial espionage (corporate "spying" activities);
4. damage assessment (following an incident);
5. criminal fraud and deception cases;
6. criminals Cases (many criminals simply store information on computers, intentionally or unwittingly) and countess others;
7. copyright violation

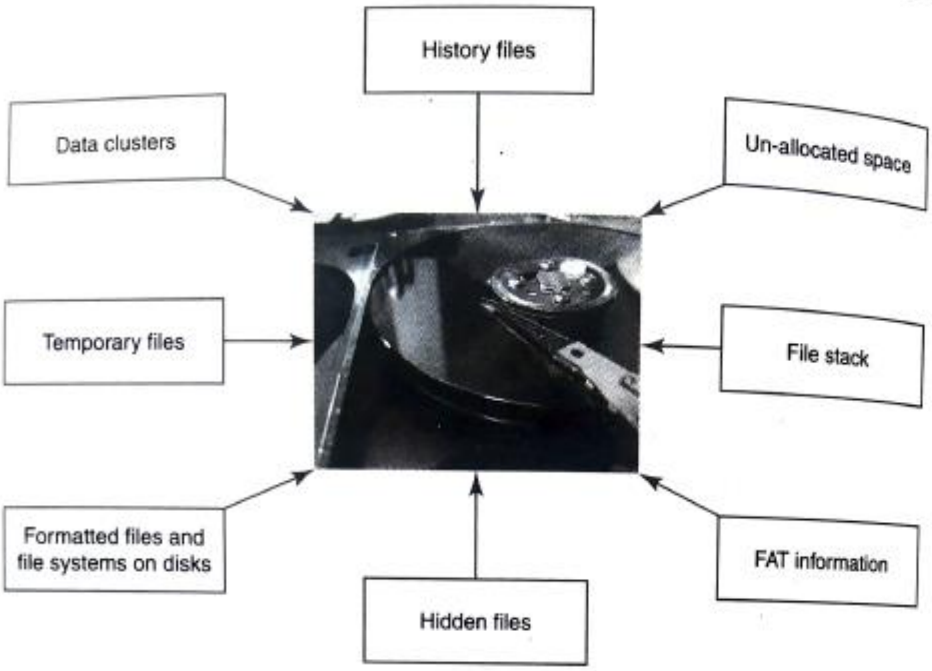


Figure 5.1 shows the kind of data you "see" using forensics tools.

Using digital forensics techniques, one can:

1. Corroborate and clarify evidence otherwise discovered.
2. Generate investigative leads for follow-up and verification in óther ways.
3. Provide help to verify an intrusion hypothesis.
4. Eliminate incorrect assumptions.

Box 5.1: COFEE Time:

- **Computer Online Forensics Evidence Extractor (COFEE)** is a USB thumb drive-gadget onto which Microsoft have loaded 150+ commands that can, among other things, decrypt passwords, display internet activity and uncover all a data stored on the computer.
- The tool was developed by Anthony Fung, a former Hong Kong police office and now an employee who works for Microsoft.
- Microsoft collected the problem faced by law enforcement agencies around the world to develop solution to the problem.
- Law enforcement professional need to capture critical evidence on a computer at the scene of an investigation before the evidence is powered down and removed for forensic analysis.
- COFEE helps the Law Enforcement Agencies even when there are no on-the scene computer forensic capabilities.
- It enables them to collect live volatile evidence more easily.
- On-the-scene, agents can run more than 150 commands on a live computer system. COFEE tool also provides reports in simple format that are easy for later interpretation. These reports can be used by experts and can also be used as supportive evidence for subsequent investigation and prosecution.
- The COFEE fool and its underlying framework can be tailored to effectively meet the needs of a particular investigation, that is, it can be fully customized. On the lighter side, one wonders if there will also be Total Evidence Analyzer (TEA) soon.

Q2: Is there a difference between computer security and computer forensics? Explain

BOX 5.2: Difference between Forensics Policy and Security Policy

Forensics Policy	**Security Policy**
forensics policy is a statement that clearly states which assets are forensically important. those It also specifies data needed for investigation into breach of those assets.	It is a statement that clearly specifies the allowed and disallowed elements with regard to security.
Forensics policy partitions space of all possible breaches or criminal activity into sets events that to are forensically noteworthy and those that are not.	It partitions the system states into "secure" and "unauthorized security" policy that helps implement mechanisms enforce system security policy.
It allows for mechanisms or design decision to enforce policy. Here is another way to understand the difference between security policy and forensics policy - violation of security policy	

leads to insecure information systems/application with vulnerabilities arising due to consequences of break-in or insider is misuse	
On the other hand, **violation of forensics policy means** lack of evidence which results in the loss of ability of an organization to prove guilty the people who are involved in cybercrime incidence.	
Example of forensics policy: 1.Goal is to capture data from network intrusions for possible prosecution. 2. Forensics policy states that all events identified as intrusions will have their associated data captured and preserved 3. Enforcement mechanisms: routine preservation of IDS, firewall, router and web server logs for some configurable length of time	

Q3: List various Computer Forensics services available, explain any two of them.

Box 5.3:
Digital forensics investigations and E-discovery

Digital evidence plays an important role in threat management life cycle, from incident response to high-stakes corporate litigation. Evidences involve computer hard drives, portable storage, floppy diskettes, portable music players and PDA's, etc.....

Key evidences often reside on more than a user hard drive or file server, requiring the capture and analysis of evidence from enterprise productivity servers, network logs or proprietary databases.

Many threats arise from illegal internet activities that extend beyond the firewall and require new investigative and forensics approaches. Forensics professionals need supporting solution for the acquisition, management and analysis of digital evidence.

Such computer forensics services include the following:

1. Data culling and targeting
2. Discovery/subpoena process
3. Production of evidence
4. Expert affidavit support
5. Criminal/Civil testimony
6. Cell phone forensics
7. PDA (Personal Digital Assistants) forensics

Specific client requests for forensics evidence extracting solution support include:

1. Index of files on hard drive
2. Index of recovered files
3. MS Office / user generate document extraction
4. Unique e-mail address extraction
5. Internet activity/ history
6. Keywords search
7. Chain of custody

8. Deleted file/ folder recovery
9. Instant messaging history recovery
10. Password recovery

- Such types of computer evidences are important because quite often the evidence becomes the deciding factor in a criminal, civil or employee dismissal action.
- Investigations involving **trade secrets, commercial disputes and misdemeanor and felony crimes** can be won or lost solely with the introduction of recovered E-mail and other documentation. If someone makes an attempt to delete, erase or otherwise hide critical evidence, you need the competent data recovery capabilities of forensics discoveries.

- Computer users typically “Delete” incriminating or sensitive computer files(For e.g., using tools such as “Deep Freeze”, a software tool that is actually meant to protect your computer) but the information may still exist in slack space on the computer’s hard drive that is hidden.
- This computer data may linger (remain) for months or even years**.** However , it can be recovered and documented using computer forensics methods and techniques.
- Unfortunately, there are many examples of computer usage in violation of computer policy**.** Sexual harassment, theft of trade secrets, abuse of the internet and unauthorized outside employment on company time are just few examples of violation that warrant a forensics examination of a computer.
- Even in investigations where hard drives are reformatted in an attempt to hide evidence, forensics discoveries can still potentially recover critical information.
- Forensics discoveries can also aid in recovering passwords for critical files that have been maliciously set or changed.
- There are further challenges; for example, many times, computer

are reissued when employees leave.

- Computer that is used continuously may destroy the incriminating evidence that can be used against a former disgruntled employee
- Also, constant use of the computer may raise questions as to who created the incriminating evidence and when
- To prevent these problems and to preserve potentially valuable information, it is recommended that a strict chain of custody should be followed and the subject computer should be shut down, that is, the computer on which digital evidence is believed to be residing
- The following links (accessed on 28 March 2010) provide information about various tools including Deep Freeze
- http://software.informer.com/getfree-deep-format-recover/ (Deep Format Recover Tools):
- http://www.astahost.com/info.php/Deep-Freeze-Partition_12571.html (Deep Freeze-related Blog):
- http://www.hochstadt.com/protecting-your-computer-using-deep freeze (an article here explains how you can protect your computer using "Deep Freeze"):
- http://technodata.blogspot.com/2006/11/how-to-format-hard-disk-by-disk.html (this article explains how to format the hard disk);
- 5. http://www.softlist.net/search/deep-freeze-2000-xp/ (Deep Freeze 200 XP Free Downloads):
- http://www.pctechguide.com/forums/ubbthreads.php/topics/4391/Hard%20Disk%20re-format(technical blog):

Q4: Discuss the need for concept of Computer Forensics

5.4 Need for Computer Forensics,

- The convergence of information and communication technology (ICT) advances and the pervasive use of computer worldwide together have brought many advantages to mankind.
- At the same time, this tremendously high technical capacity of modern computer/computing devices provides avenues for misuse as well as opportunities for committing crime.
- This leads to new risks for computer users and also increased opportunities for social harm.
- The users, businesses and organizations worldwide have to live with a constant threat from hackers who use a variety of techniques and tools to break into the computer to steal information, change data and cause havoc.
- The widespread use of computer forensics is the result of two factors: 1.The increasing dependence of law enforcement on digital evidence. 2. Ubiquity of computers that followed from the microcomputer revolution.
- The media on which clues related to cybercrime reside may vary from case to case.
- There are many challenges for the forensics investigator because storage devices are getting miniaturized due to advances in electronic technology; for example, external storage devices such as mini hard disks (pen drives) are available in amazing shapes.
- Looking for digital forensics evidence (DFE) is like looking for a needle in the haystack.
- Here is a way to illustrate why there is always the need for forensics software on suspect media - the capacity of a typical regular hard disk is 500 GB (gigabytes).
- In an A4 size page, there are approximately 4,160 bytes (52 lines x 80 Characters = 4160 bytes assuming 1 byte per character). This is equivalent to 4 KB (kilobytes). An A4 size of paper sheet has thickness of 0.004 inches.
- Data of 4 MB (megabyte; 1,000 times of 4 KB) when printed on A4 size of paper would be 4 inches thick.
- Data of 4 GB if printed on A4 sheet would be 4,000 inches, that is, 1,000 times of be virtually impossible to "retrieve" relevant forensics data from this heap!! There comes the help from forensics MB.
- This would turn out to be 4 inches thick. The printout of 500 GB would be 500,000 inches!
- It would be virtually impossible to "retrieve" relevant forensics data from this heap!!

There comes the help from forensics software-it helps sieve relevant data from the irrelevant mass (vital few from trivial many as the proverb goes).

Fungibility:

- ***"Fungibility"*** means the extent to which the components of an operation or product can be inter- changed with similar components without decreasing the value of the operation or product.
- For a person to be considered as "identifiable person," he/she must always have the physical custody of a piece of evidence.
- Practically speaking, this means that a police officer or detective will take charge of a piece of evidence, document its collection and hand it over to an evidence clerk for storage in a secure place.

- All such transactions as well as every succeeding transaction between evidence collection and its appearance in court need to be completely documented chronologically to withstand legal challenges to the authenticity of the evidence.
- Documentation must include conditions under which the evidence is collected, the identity of all those who handled the evidence, duration of evidence custody, security conditions while handling or storing the evidence and the manner in which evidence is transferred to subsequent custodians each time such a transfer occurs (along with the signatures of persons involved at each step).
- Chain of custody is also used in most evidence situations to maintain the integrity of the evidence by providing documentation of the control, transfer and analysis of evidence.
- Chain of custody is particularly important in situations where sampling can identify the existence of contamination and can be used to identify the responsible party.

Box 5.4: Chain of Custody Example

CASE STUDY
Officer Amar collects the knife and places it into a container, then gives it to forensic technician Balan. Forensics technician Balan takes the knife to the laboratory and collects fingerprints and other evidence from the knife. He then gives the knife and all evidence gathered from the knife to evidence clerk Charu. Charu then stores the evidence until it needed, documenting everyone who has accessed the original evidence (the knife and original copies of the lifted fingerprints).

The chain of custody requires that from the moment the evidence is collected, every transfer of Evidence from one person to another person should be documented as it helps to prove that nobody else could have accessed that evidence. It is advisable to keep the number of evidence transfers as low as possible. In the courtroom, if the defendant challenges the chain of custody of the evidence, it can be proven that the knife in the evidence room is the same as found at the crime scene. However, if due to some discrepancies it cannot be proven who had the knife at a particular point in time. Then the chain of custody is broken and the defendant can ask to have the resulting evidence declares inadmissible.

Q5: Discuss the Cyber Forensics and Digital Evidence
Q6: Explain the rules of evidence

5.5 Cyber Forensics and Digital Evidence,

Cyberforensics can be divided into two main domains

1. Computer forensic
2. Network forensic

As compared the physical evidence digital visions is different in nature because of it has some unique characteristics.

- digital evidence is much easier to change or manipulate
- prefers digital copies can be made without harming original.

At the same time the integrity of digital evidence can be proven.
There are many forms of Cybercrimes sexual harassment cases-memos, letters, emails, obscene chats or embezzlement cases-spreadsheets, memos, letters, emails, online banking, information; corporate espionage by of memos, letters, emails and chats; and fraud through memos, letters, spreadsheet and email.

In case of computer crime or cybercrime computer forensic helps
computer forensic experts know the technique to retrieve the data from files listed in standard directory search hidden files deleted files deleted Email and password login IDS encrypted files hidden partitions etc., Typically the evidence is to decide on computer system used user created files use a protected files computer created files and on computer networks computer system have the following
1. Logical file system that consists of

- **File system:** It includes files, volumes, directories and folders, file allocation tables (FAT) as in the folder version of Windows Operating System, clusters, partitions, sectors.

- **Random access memory.**
- **Physical storage media:** It has magnetic force microscopy that can be used to recover data from overwritten area.
  - Slack space: It is a space allocated to the file but is not actually used due to internal fragmentation and
  - unallocated space.

2. User created files: It consists of address books, audio/video files, calendars, database files, spread- 2. sheets, E-Mails, Internet bookmarks, documents and text files.
3. Computer created files: It consists of backups, cookies, configuration files, history files, log files, Swap files, system files, temporary files, etc.
4. Computer networks: It consists of the Application Layer, the Transportation Layer, the Network Layer, the Data Link Layer. Readers who are not savvy with these terms

Box 5.5: The Father of Forensics Science the Sherlock Holmes of France:

Dr. Edmard Locard→ 1877-1966, Pioneer in Forensic Science and was popularly known as Sherlock Holmes of France.
He Formulated the basic principle of forensics science; " Every contact leaves a trace".
→ known as Locard's exchange principle.

Wherever he steps, wherever he touches, whatever he leaves, even without consciousness. Will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibres from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it. can diminish its value. In *other words, whenever two human beings come into contact. something from one is exchanged to the other, that is, dust, skin cells, hair etc.*

Link to know more: https://science.howstuffworks.com/locards-exchange-principle.htm/printable (11 September 20o9)

5.5.1. The Rules of Evidence

According to the "Indian Evidence Act 1872," "Evidence" means and includes:

1. All statements which the court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry, are called oral evidence.
2. All documents that are produced for the inspection of the court are called documentary evidence.

Legal community believes that "electronic evidence" is a new breed of evidence. They also, at times, have an apprehension that the law of evidence as per Indian Evidence Act of 1872 may not hold good for electronic evidence. Some lawyers express doubts and apprehensions about the process of leading electronic evidence in the courts. However, this is not true; the traditional principles of leading evidence, along with certain newly added provisions in the Indian Evidence Act 1972 through the Information Technology Act (ITA) 2000, constitute the body of law applicable to electronic evidence. The challenges, however, need to be understood from the "rules of evidence" perspective.

Paper evidence, the process is clear and intuitively obvious. Digital evidence by its very nature Invisible to the eye. Therefore, the evidence must be developed using tools other than the is human eye.

There are number of contexts involved in actually identifying a piece of digital evidence:

1. Physical context: It must be definable in its physical form, that is, it should reside on a specific piece of media.

2. Logical context: It must be identifiable as to its logical position, that is, where does it reside relative to the file system.
3. Legal context: We must place the evidence in the correct context to read its meaning, this may require looking at the evidence as machine language, for example, American Standard Code for Information Interchange (ASCII).

The path taken by digital evidence can be conceptually depicted as shown in Fig. 5.3.

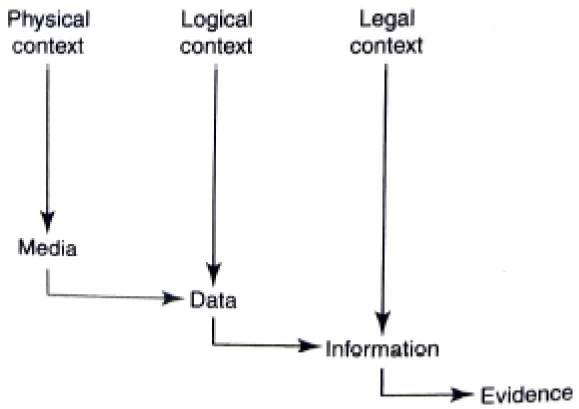


Fig. 5.3: Path of the digital evidence.

What are the guidelines for the (digital) evidence Collection Phase.

1. Adhere to your site's security policy and engage the appropriate incident handling and law enforcement personnel.
2. Capture a picture of the system as accurately as possible.
3. Keep detailed notes with date and times, if possible, generate an automatic transcript. Notes and printout should be signed and dated.
4. Not the difference between the system clock and coordinated universal time for each time stand provided indicate whether UTC or local time is used.
5. be prepared to testify perhaps your leader outlining all actions you to convert times detail notes will be vital.
6. minimise changes to the data as you are collecting it this is not limited to content changes avoid updating files or directly access time.
7. Remove external avenues for change.
8. when confronted with the choice between collection and analysis used to do collection first and analysis later.
9. Needless to say, your procedures should be implementable. As with any aspect of an incident response policy, procedures should be tested to ensure feasibility, particularly, in a crisis. If possible, procedures should be automated for reasons of speed and accuracy. Being methodical always helps.
10. For each device, a systematic approach should be adopted to follow the guidelines laid down in your collection procedure. Speed will often be critical; therefore, where there are a number of devices requiring examination, it may be appropriate to spread the work among your team to collect the evidence in parallel. However, on a single given system collection should be done step by step.
11. Proceed from the volatile to the less volatile; order of volatility is as follows:
    - Registers, cache (most volatile, i.e., contents lost as soon as the power is turned OFF); routing table, Address Resolution Protocol (ARP) cache, process table, kernel statistics, memory;
    - Temporary file systems;
    - disk;
    - remote logging and monitoring data that is relevant to the system in question;
    - physical configuration and network topology;
    - archival media (least volatile, i.e., holds data even after power is turned OFF).
12. we should make a bit-level copy of the system's media. If we wish to do forensics analysis we should make a bit-level copy of pour evidence copy for that purpose, as our analysis will almost certainly alter file access times. try to avoid doing forensics on the evidence copy.

Note: ***Address Resolution Protocol (ARP)*** is a very important part of IP networking.

ARP is used to connect O er (Network) to OSI Laver 2 (Datalink), For most of us this means that ARP is used to link to our IP addressing to our Ethernet addressing (MAC Addressing). For you to communicate with any device on you network, you must have the Ethernet MAC address for that device. If that device is not on your land you go to your default gateway.

In this case your rooter will be destination MAC address that your PC will communicate with they are two types of ARP entries Static and dynamic.

Most of the time you will use dynamic ARP and trees what does means that the ARP entry (the Ethernet Mac to the IP address link) is kept on a device for some period of time as long as it is being used.

The opposite of a dynamic ARP entry is static ARP entry. With the static ARP entry, you are manually entering the link between the Ethernet MAC address and IP address because of Management headache that lack of insignificant negative to using dynamic entries are used most of the time.

7.Expalin the Forensic Analysis of E-Mail
8. Briefly explain RFC2822

Forensics Analysis of E-Mail

Criminal use fake mail for various cybercrime offences. there are tools available but help create fake mail. forensic analysis of email is an important aspect of Cyber forensic analysis.
It help established the authenticity of an email when suspected.
As we know email are the common means of communication word White and the often the subject of forensic analysis.

Email system is the hardware and software that controls the flow of email.
The two most important components of an email system are the email server and email gateway.

Email server are computer set forward collect store and deliver an email to their clients and email gateways are the connections between the email server.

Mail server software is a network software that controls the flow of email and the mail clients of their helps each user read compose send and delete messages and email consists of two parts the header and the body.

Message he does are the important part of investigating email messages.

Theatre of an email is very important from forensic point of you a full header view of an email provides the inter part of emails journey from its Origins to its destination. the header view include sleep originating IP address and other useful information.

Header information very sweet email service provider Email application and system configuration.

Box 5.6: Electronic messages and an Indian Evidence Act

Section 88 of Indian Evidence Act is about presumption as an telegraphic messages it states the following
Presumption as to telegraphic messages the court may presume that a message forwarded from a telegraph office to the person to whom such message for ports to be address corresponds with the message delivered for transmission at the office from which the

message for post to be sent but the court shell not make up presumption as to the person but whom that message was delivered for transmission.

As per section 66a of c and Indian act any electronic mail electronic message for the purpose of causing convenience about the origin of such messages shall be punishable with imprisonment for a term which may extend to 2 to 3 years and with fine.

Typically, the sender's E-Mail address can be found after the "From" section of the header. However, that is not the only place it can be found. It can also be found under other sections depending on the E-Mail client uses. These sections include the following.

1. X-originating E-Mail;
2. X-sender;
3. return-path.

RFC2822

RFC2822 is the Internet Message Format. According to the Internet specification RFC2822, there are several formats of valid E-Mail addresses, like joshi@host.net, john@[10.0.3.19], "Joshi Ganesh'@host.net or "Joshi Ganesh"@[10.0.3.19]. Many E-Mail address validators on the Web fail to recognize some of those valid E-Mail addresses. Some examples of invalid E-Mail addresses are as follows:

1. joshi@box@host.net: Two at signs (@) are not allowed;
2. joshi@host.net: Leading dor () is not allowed;
3. joshi@-host.net: Leading dash (-) is not allowed in on domain name;
4. joshi@host.web: Web is not a valid top-level domain;
5. joshi@[10.0.3.1999]: Invalid IP address.

The RFC2822 standard applies only to the Internet Message Format and some of the semantics of messages contents. It contains no specification of the information in the envelope.
RFC2822 states that each E-Mail must have a globally unique identifier. It is included into the header of an E-Mail.

9.With neat diagram explain process model for understanding a seizure and handling of forensics evidence legal framework.

10.Discuss the following phases of Forensics life cycles
i) Preparation and Identification
ii) Collection and Recording

11. Discuss the following phases of Forensics life cycle
i) Storing and Transporting
ii) Examination/Investigation

12.Discuss the precautions to be taken when collecting electronic evidence.

5.6 Digital Forensic Life cycle,

As per FBI's (Federal Bureau of Investigation) view, digital evidence is present in nearly every crime scene. That is why law enforcement must know how to recognize, seize, transport and store original digital evidence to preserve it for forensics examination. Figure 5.5 shows the process model for understanding a seizure and handling of forensics evidence legal framework.

The cardinal rules to remember are that evidence

- 1. is admissible;
- 2. is authentic;
- 3. is complete;
- 4. is reliable;
- 5. is understandable and believable.

5.6.1. The Digital Forensic Process.

Digital forensic process needs to be understood in the legal context starting from preparation of the evidence to testifying.

Digital forensic evidences consist of exhibits each consisting of a sequence of BITS presented by witnesses in legal matter to help Jurors established the facts of the case and support or refute legal theories of the case.

the exhibit should be introduced and presented and our challenge by properly qualified people using a properly applied methodology that address is the legal theories and issue

Expert witness is very important and is associated with Digital forensic evidence.

as per the court procedure the exhibits are introduced as evidences by either side.

testimony is presented to established the process to identify collect preserve transport store analyse interpret at tribute and or reconstruct the information contained in the exhibit and to establish to the standard of proof required by the matter at hand that the evidence reflects the sequence of events that is asserted to have produced it.

The assumption is that adequate facts can be established for the introduction of an evidence exhibit.

people involved in the chain of custody need to justify a number of aspects relating to the evidence- the testimonial typically include the process of used for creating handling and introducing the evidence the method used for collecting the exhibit as well as the manner in which the exhibit is brought to court.

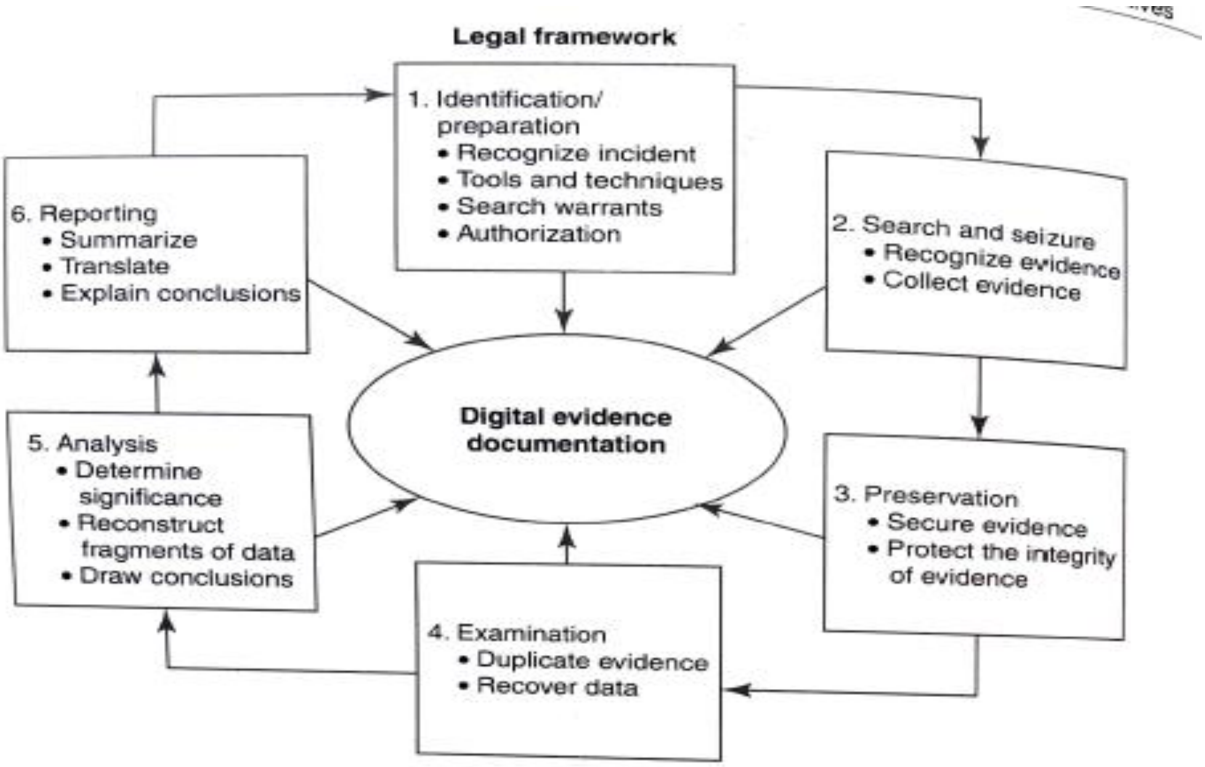


Fig. 5.5: Process model for understanding a seizure and handling of forensics evidence legal framework.

Box 5.8: **Forensics Experts What do they Do?**
The role of forensics experts has become a very special one in digital forensics and there are many reasons for it. Handling of digital evidence requires special expertise that come from training and experience.

A forensics expert team brings the following additional benefits:

1.Technology expertise:
This is perhaps the biggest advantage of partnership with a computer forensics expert. As an example of the technological complexity, consider the proliferation of operating systems in the last decade: mainframe operating systems, Windows 95/98, UNIX, Linux, Windows NT, Windows Server, Macintosh, Windows 2000, Windows XP and Novell Netware. Specific forensics tools must be used with each of these file systems, along with training and experience to interpret search results. Although some evidence may be found easily, other evidence may have been deleted, altered, hidden or encrypted. Forensics experts routinely deal with such complexities and nuances.
2. Forensics methodology: A comprehensive forensics methodology, repeatable and defensible, has become a key attribute in choosing a forensics expert firm. Proper use of a repeatable process prevents making the same mistake twice, ensures proper chain of custody, leverages successful techniques from prior cases, supports clear and concise testimony, and generally guarantees efficient forensics case management.
3. Experience and efficiency: The tools and methods of computer forensics examination are still in their infancy. Experts know how to quickly navigate through the variety of esoteric tools and procedures. Experts also have the experience to cull thousands of files based on patterns and keywords. Therefore, working with experts will efficiently produce relevant results for counsel.

5.6.2. The Phases in Computer Forensics/Digital Forensics

The Forensics life cycle involves the following phases namely.
1. Preparation and identification;
2. collection and recording;
3. storing and transporting;
4. examination/investigation;
5. analysis, interpretation and attribution;
6. reporting;
7. testifying.

To mention very briefly, the process involves the following activities:
1. Prepare: Case briefings (see Box 5.9), engagement terms, interrogatories, spoliation Prevention disclosure and discovery planning, discovery requests. ·
2. Record: Drive imaging, indexing, profiling, search plans, cost estimates, risk analysis.
3. Investigate: Triage images, data recovery, keyword searches, hidden data review, communicate
iterate. '
4. Report: Oral vs. written, relevant document production, search statistic reports, chain of custody reporting, case log reporting.
5. Testify: Testimony preparation, presentation preparation, testimony.

Let us take a brief look at each of the activities mentioned. Table 5.5 shows phase-wise outcome from the phases mentioned above.

Box 5.9: Case Briefings
In case briefings, consider the following:
seen all re~

1. Ensure that you know both your client 's and the adverse party's position. and have seen all relevant paperwork.
2. Try not to project a bias in the case description; the intent should be to consider the case objectively, and provide you with the good news and the bad news (bad news early can be good news)
3. Be upfront in discussing any limitations or restrictions on the forensics investigation including budgetary constraints, time deadlines, cooperation levels to be expected from the adverse party required travel, onsite or after-hours forensics imaging requirements, etc.

Preparing for the evidence and identifying the evidence
In order to be processed and applied evidence must be first identified as evidence. it can happen that there is an enormous amount of potential evidence of available for a legal matter and it is possible that the vast majority of the potential evidence may never get identified.
consider that every sequence of events within a single computer might cause interaction with files the file system in which day recite other processes and the program they are executive and
the files they produce and manage and block files and file of various sorts.

Network environment these extents to all network devices potentially all over the world. evidence of an activity that cause Digital forensic evidences to come into being might be continuous contained in a time stamp associated with the different program in a different computer on the other side of the word that was offset from its usual pattern of behaviour by a few many microseconds.

If the evidence cannot be identified as relevant evidence it may be never be collected or process that all and may not even continue to exit in digital form by the time it is discovered to have relevance

Collecting and Recording Digital Evidence.

- Digital evidence can be collected from many sources.
- The sources are computers, cell phones, digital cameras hard drives, CD-ROM, USB memory devices and so on.
- Non-obvious sources include settings of digital thermometers, black boxes inside automobiles, RFID tags and webpages (which must be preserved as they are subject to change).
- Special care must be taken when handling computer evidence: most digital
- information is easily changed, and once changed it is usually impossible to detect that a change has taken place unless other measures have been taken.
- For this reason, it is common practice to calculate a cryptographic hash of an evidence file and to record that hash elsewhere, usually in an investigator's notebook, so that one can establish at a later point in time that the evidence has not been modified as the hash was calculated.
- Figures 5 .6 and 5.7 show the media that typically holds digital evidence.

Collecting volatile data requires special technical skills
If the machine is still active any intelligence that can be gained by examining the applications currently open is recorded.

if the machine is suspected of being used for illegal communication such as terrorist traffic not all of this information may be stored on the hard drive.
If information told solely in Random Access Memory and not recovered before powering down it may be lost.
This results in the need to collect volatile data from the computer at the onset of the response.

Memory falls under the family of solid-state non-time memory it is used in some drive USB sticks cell phone game console secure digital card and multimedia cards.

This technology differs from the normal hard disc by not containing any moving parts in every device that interact with our daily life.
The benefit of Embedded memory continues to increase life expectancy. figure 5.8 shows the various types of embedded memories inside a computer ROM, PROM, EPROM, EEPROM.

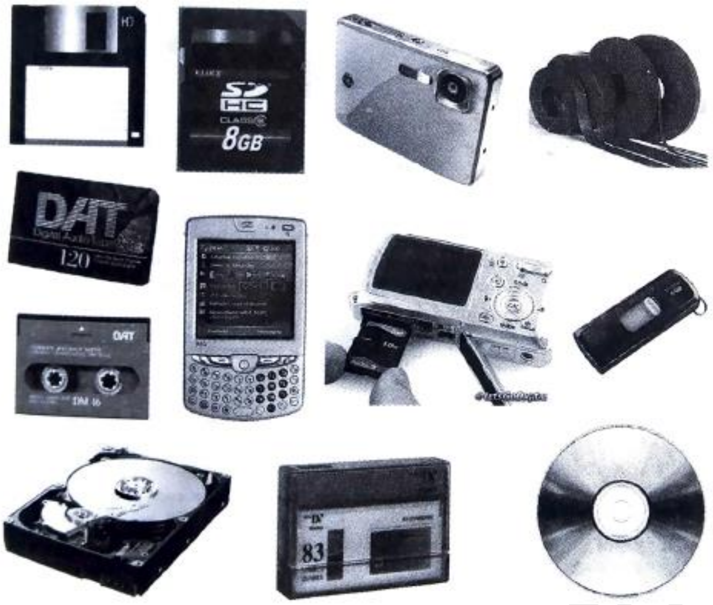


Fig. 5.6: Media that can hold digital evidences_.

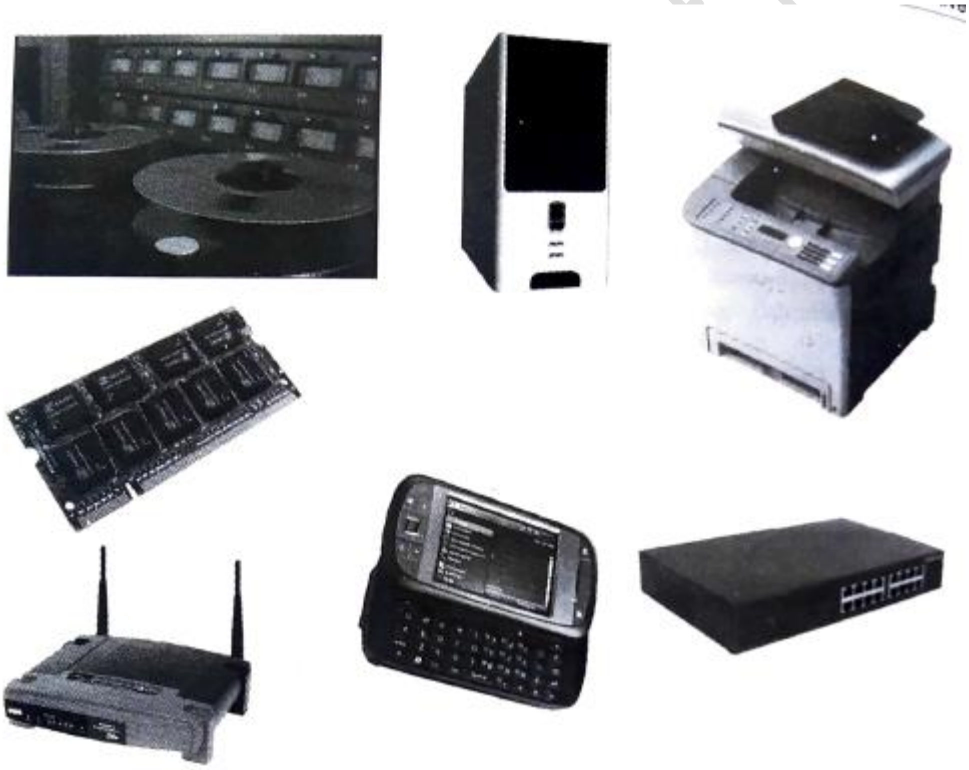


Fig. 5.7. Some more media that can hold digital evidences

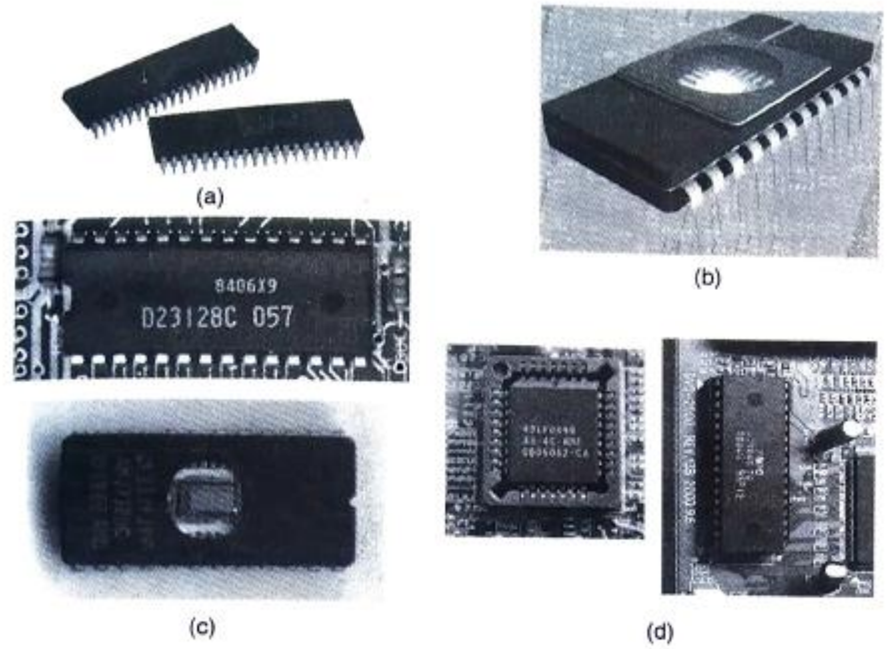


Fig. 5.8. Embedded memories inside computer.

Storing and Transporting digital Evidence

The following are specific practices char have been adopted in the handling of digital evidence.

1. Image computer media using a write-blocking tool to ensure that no data is added to suspect device;

2. Establish and maintain the chain of custody (refer co Section 5.7);

3. Document everything that has been done;

4. Only use cools and methods that have been tested and evaluated to validate their accuracy and reliability.

Storage must be adequately secure to assure proper "chain of custody

Many things can go wrong in storage, including decay over time; environment changes resulting in the presence of a necessary condition for preservation;

Examining/Investigating digital Evidence

Investigation in which the owner of the digital vision has not given consent to have his or her media examined as in some criminal cases some care must be taken to ensure that the forensic specialist has the legal authority to C copy and examine the data sometimes authority stems from search warrant.

It is understanding the difference between live and dead analysis after that we explain about the imaging of the media.

Traditionally computer for insect investigations for performed on a data at rest.

For a exam well the content of hard drives the scan we brought thought of as a analysis investigators were told to shut down computer system when they are impounded for fear that digital time bomb might cause data to be at rest.

Process of creating an exact duplicate of the original evidence media is often called imaging computer forensics software packages make this possible by converting an entire hard drive into a single searchable file is file is called an image.

Analysis, Interpretation and Attribution

Analysis, interpretation and attribution of evidence are the most difficult aspects encountered by most forensics' analysts.
In the digital forensics arena, there are usually only a finite number of possible events sequences that could have produced evidence; however, the actual number of possible sequences may be almost unfathomably large.
In essence, almost any execution of an instruction by the computing environment containing or generating the evidence may have an impact on the evidence. Basic ally, all digital evidence must be analysed to determine the type of information that is stored upon it.
For this purpose, specialty tools are used that can display information in a format useful to investigators. Such forensics tools include but are not limited to the following list.

1. Access Data's FTK
2. guidance Software's EnCase;
3. Dr. Golden Richard III's file carving tool Scalpel; "file carving" is the process of recovering files from an investigative target, potentially without knowledge of the file system structure;
4. Brian Carrier's Sleuth Kitl5l: The Sleuth Kit (TSK) is a library and collection of Unix- and Windows based tools and utilities to allow for the forensics analysis of computer systems.

Box 5.10: The file carving techniques are
File carving is a process of recovering the files from an investigative target, potential without knowledge of the file system structure. the process is based on information about the format of the file types of interest, as well as on assumption about how files are typically laid out on block devices.

if the file system metadata is used at all, it is typically used only for establishing cluster sizes and avoiding carving of undeleted file.

covering is an important technique for Digital forensic investigation and for simple data recovery.

Why using a database of headers and footers for specific file types file covers can retri files from a raw disc image regardless of the type of a file system on the disc image.

File carving ignore the file system and car of the images directly from the data blocks. in cases of fragmented files, the carbon returns in perfect photo but this image might be sufficient to identify the subject. (As in fig. 5.9)

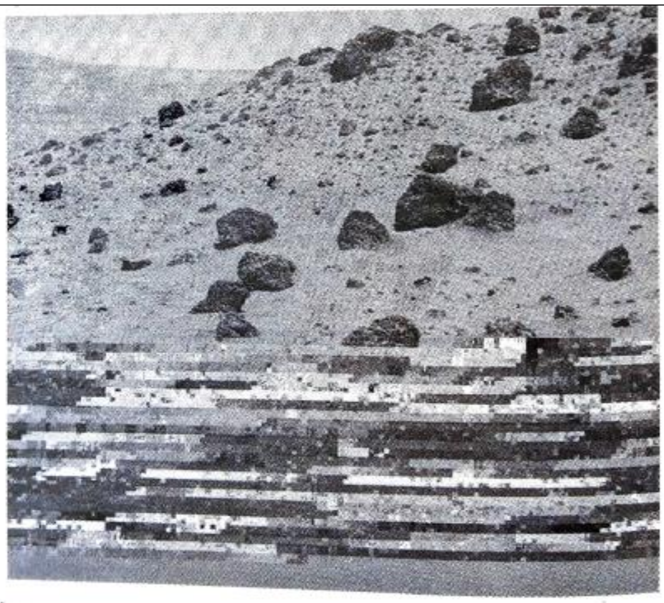


Fig 5.9: An image constructed fragmented file

Digital analysis is very important in Digital forensic because a digital investigation may encounter many forms of digital data and therefore there is a several types of digital analysis.
The different analysis types are based on interpretation obstruction layers which are generally part of the data design.

For example, consider the date on a hard disc which has been designed with several interpretation layers lowest layer me contain partitions or other containers that are used for volume management.
Inside each partition is data that has been organised into a file system or database.
Data in the file system is interpreted to create file that contain data in an application specific format and requirement

What are the common digital analysis types:

1. **Media analysis:** It is analysis of the data from a storage device. This analysis does not consider any partitions or other operating system (OS)-specific data structures. If the storage device uses a fixed size unit, such as a sector, then it can be used in this analysis.
2. **Media management analysis:** It is analysis of the management system use d to organize media. This typically involves partitions and may include volume management or redundant array of independent (or inexpensive) disks (RAID, see Box 5.11) systems chat merge data from multiple storage devices into a single virtual storage device.
3. **File system analysis:** It is the analysis of the file system data inside a partition or disk. This typically involves processing the data to extract the contents of a fil e or to recover the contents of a deleted files.
4. **Application analysis:** It is the analysis of the data inside a file. Files are created by users and applications. The format of the contents is application-specific.

5. **Network analysis:** It is the analysis of data on a communications network. Network packers can be examined using the OSI Model to interpret the raw data into an application-level scream.
   Analysis types are
   OS analysis: An OS is an application; it is the first one that is run when a computer starts. This analysis examines another configuration file and output data of the OS to determine what events may be occurred.

   Executable analysis:
   executables are digital object that can cause events to occur and their frequently examine during intrusion investigation because the investigator needs to determine what events the executable could cause
6. **Image analysis:**
   image is a single searchable file.
   Digital images are the target of many digital investigations because some are Contraband.
   this type of analysis Looks for information about where the picture was taken and who are what is in the picture image analysis also includes examining images for evidence of steganography
7. **Video analysis**
   digital radio is used in security cameras and then personal videos cameras and webcams investigation of online predators can sometimes involve digital video from webcams this type of analysis examine the video for identification of objects in the video and the location where it was shot

Box: 5.11 The RAID Levels

RAID data acquisitions are performed as a part of Computer forensic.
RAID stands for redundant array of independent discs.
It is category of disc drive that employees' multiple drives in combination for fault tolerance and performance.
The use of raid describe is frequent on servers, the uses not generally necessary for personal computer.
storage technology had become too expensive to place a large number of high-capacity hard drive in the servers.
the response to the situation came through the concept of raid subsequently rate become very popular.
Note that data stripping me spreading out block for each file access multiple disc drives.
It was a system developed as a solution to link together a large number of low-cost hard drive with a view to form a single large capacity storage device that provided superior performance storage capacity and reliability as compared to the older storage solutions. since then, RAID become widely used and is deployed as an enterprise storage method in server market.
Attractiveness of RAID comes from the fat that the array of disc distributed the data across multiple discs. however, the computer user and operating system to the serve such. The different RAID levels are

level 0: this is nothing but a strip would Disc a rate without fault tolerance. it provides data stripping but no redundancy. this results in an improved performance however it does not deliver fault tolerance all data in the array is lost if one drive fails.

level 1: This is mirroring and duplex into provide disc mirroring. level 1 provides double the rate of read transaction for single discs, but provide the same bright transaction rate as single disc.

level 2: this is error correcting coding however it is not a typical implementation. this level is rarely used it stripes data at the bit level rather than at the block level.

This is bit interleaved parity level 3 provides byte level stripping with a dedicated parity disc. It is really used probably because it cannot service simultaneous multiple requests.

level 4: this is dedicated parity drive. its use is common for implementation of RAID. Level 4 offers block level stripping with the parity disc if a data disc fails. The parity data is used to create a replacement disc. there is a disadvantage to level 4 in that the parity dis can create write bottlenecks.
Level 5 this is the block interleaved distributed parity. the idea year is to provide data stripping at the bite level and also strike error correction information. level 5 results in excellent performance and good fault tolerance. it most popular among RAID implementation methods.

level 6 this is independent data disc with the double parity. this level provides block level striping with parity data distributed across all disks.

level 0+1: this is nothing but a mirror of stripes. it is not one of the original RAID levels. With this level used, to RAID 0 stripes are created and one RAID 1 mirror is created over them. The use of the level is typically seen for both replicating and sharing data among these.

Level 10 this is a stripe of mirrors however it is not considered to be an original red level. with this level multiple RAID 1 Mirrors are created, and RAID 0 stripe is created over these.
Level 7: this is a Trademark of STC (storage Computer Corporation) it at cashing to level 3 or 4.
RAID S: This is also known as parity rate it is an MNC corporation's priority stripped parity rate system used in its Symmetrix storage system.

Reporting:

Once the analysis is complete, a report is generated. The report may be in a written form or an oral testimony or it may be a combination of the two. Finally, evidence, analysis, interpretation and attribution

The following are the broad-level elements of the report:
1. Identity of the reporting agency;
2. case identifier or submission number;
3. case investigator;
4. identity of the submitter;
5. date of receipt;
6. date of report;
7. descriptive list of items submitted for examination, including serial number, make and model;
8. identity and signature of the examiner;

9. brief description of steps taken during examination, such as string searches, graphics image searches
and recovering erased files;
10. results/ conclusions.

Testifying
This face in wall of presentation and cross examination of expert witness.

Depending on the country and legal Framework in which a cyber cream cases register that is standards me apply with regard the issue of expert witnesses.

Digital forensic evidence is normally introduced by expert witness set in the case where non expert can bring the clarity to non-scientific issues by taking what they observed or did.

For example, and non-expert who works at a company may introduce the data here she extracted from a company data base and discuss how the database works and how it normally use from a non-technical standpoint.

To the extent that the witness is the custodian of a system or a content he or she can justify to matters related to that custodial Rose as well.

Only expert witness can address issues based on scientific, technical or other specialized knowledge.
A witness qualified as an expert by knowledge, skill, experience or education.
a). If a Testimony is based on sufficient facts or data.
b). Testimony is the product of reliable principles and methods
c). the witness as applied the principles and methods reliable

Table 5.5. Digital Forensic- Phase wise outputs.

Evidence preparation and identification	• Monitoring authorisation and management support, and obtained authorisation to do the investigation. • ensuring that operations and Infrastructures are able to support an investigation. • providing a mechanism for the incident to be detected and conformer. • providing a mechanism for the incident to be detected and conformer • creating an awareness so that the investigation is needed (I didn't if I the need for an investigation) • planning for getting the information needed from both inside and outside the investigation organization. • identifying the strategy policy and previous investigation • informing the subject of an investigation or other consent party that the investigation is taking place	plan authorisation warrant notification confirmation

collection and recording preserving and transportation	• Determine water particular piece of digital evidence is and identifying possible source of data • determine where the evidence is physically located the variable • Translating the media into data • ensuring integrity and authenticity of the digital evidence for example write protection hashes etc • packaging transporting and storing the digital evidence • preventing people from using the digital device or allowing other electromagnetic device to be used within an affected radius • recording the physical scene • duplicating the digital evidence using standardised and accepted procedure • ensuring the validity and integrity of evidence for later use	crime type potential evidence source media device event
examination investigation and analysis interpretation and attribution	• Determine Hing how the data is produced, when and why whom. • determine and validating the techniques to find and interpret significant data. • extracting hidden data, discovering the hidden data and matching the pattern. • recognising fbs pieces of digital evidence and assessing the skills level of suspect. • transform the data into more manageable size and form for analysis. • confirming or refuting allegations of suspicious activity. • identifying and locating potential evidence, possibly Within unconventional locations. • constructing detailed documentation for analysis and drawing conclusions based on evidence found. • determining significant based on evidence found. • testing and rejecting theories based on digital evidence. • organising the analysis results from the collected physical and digital evidence. • eliminating duplication of analysis • build a timeline • constructing a hypothesis of what occurred and comparing the extracted data with the target. • documenting the finding and all steps taken.	log files, file events log data information

presentation and reporting	• Preparing and presenting the information resulting from analysis phase. • determine the issues relevance of the information, its reliability and who can testify to it. • interpreting the statistical from analysis phase. • clarifying the evidence and documenting the finding. • summarizing and providing explanation of conclusions. • presenting the physical and digital evidence to a court or corporate management. • attempting to confirm each piece of evidence and each event in the chain either along with each other are independent of one evidence and or other events. • providing the validity of the hypothesis and defend it against criticism and challenge. • Communicating Relevant findings to a variety of audience management technical personally law enforcement.	evidence, report
disseminating the case	• Physical and digital property is return to proper owner. • determining how and what criminal evidence must be removed. • reviewing the investigation to identify areas of improvement. • discriminating the information from the investigation. • closing out the investigation and preserving knowledge gained	evidence explanation new policies and investigation procedures evidence the post investigation closed

5.7.3. Precautions to be taken when collecting Electronic Evidence.

Collection of evidence must happen with due care. special measures should be taken while conducting a forensic investigation if it is desired for the results to be used in a court of law one of the most important major is to ensure that the evidence has been accurately collected and that there is a clear chain of custody right from the scene of crime to the investigator and ultimately to the court.

in order to comply with the need to maintain the integrity of digital dividend certain rules must be compiled with.

the general principles are

Principle 1:

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

Principle 2:

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

Principle 3:

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

Principle 4:

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

13. Explain the chain Custody Concepts in Cyber Forensics

5.7 Chain of Custody Concepts,

A chain of custody is the process of validating how many kinds of evidences have been gathered, tracked and protected on the way to a court of law

It is essential to get in the habit of protecting all evidences equally so that they will hold up in court. Forensic nvestigation professionals know that if you do not have a chain of custody, the evidence is worthless. They learn to deal with everything as if it would go to litigation.

Purpose of the chain of custody is that the proponent of a piece of evidence must demonstrate that it is what it purports to be.

In other words, there is a reliable information to suggest that the party offering the evidence can demonstrate the piece of evidence is actually, in fact, what the party claims it to be and can further demonstrate its origin and the handling of the evidence because it was acquired.
The Chain of Custody is a chronological written record of those individuals who have had custody of the evidence from, its initial acquisition until its final disposition.

A chain of custody begins when an item of relevant evidence is collected, and the chain is maintained until the evidence is disposed off (Figs. 5.10 and 5.11). The chain of custody assumes continuous accountability. This accountability is important because, if not properly maintained, an item (of evidence) may be inadmissible

5.8 Network forensics.

- Open networks can be source of many network-based cyberattack
- Wireless Forensics
- Wireless Forensics is a discipline included within the computer forensics science, and specifically, within the network forensics field.
- The goal of wireless forensics is to provide the methodology and) tools required to collect network traffic that can be presented as valid digital evidence a court of law.

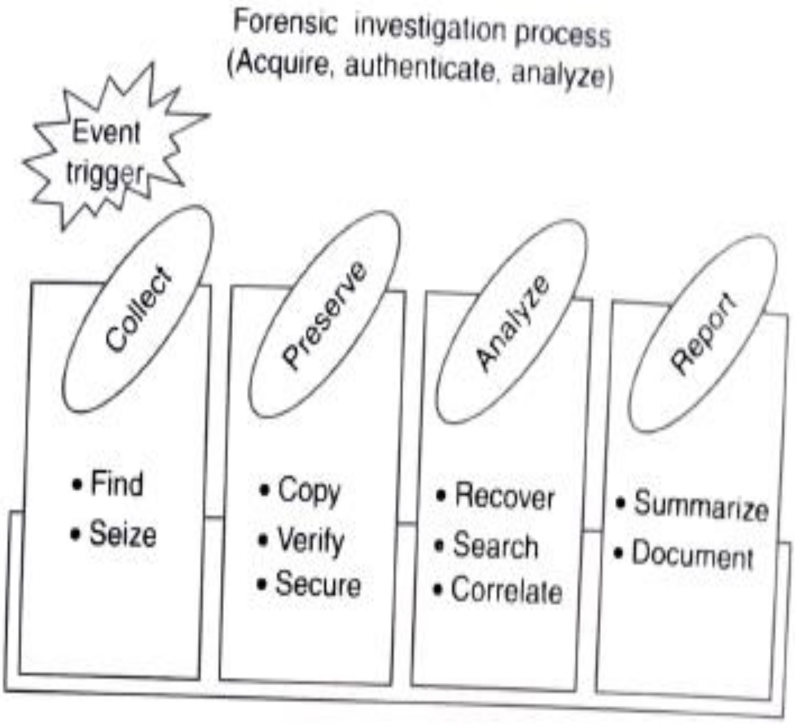


Fig. 5.10: Maintaining chain of custody

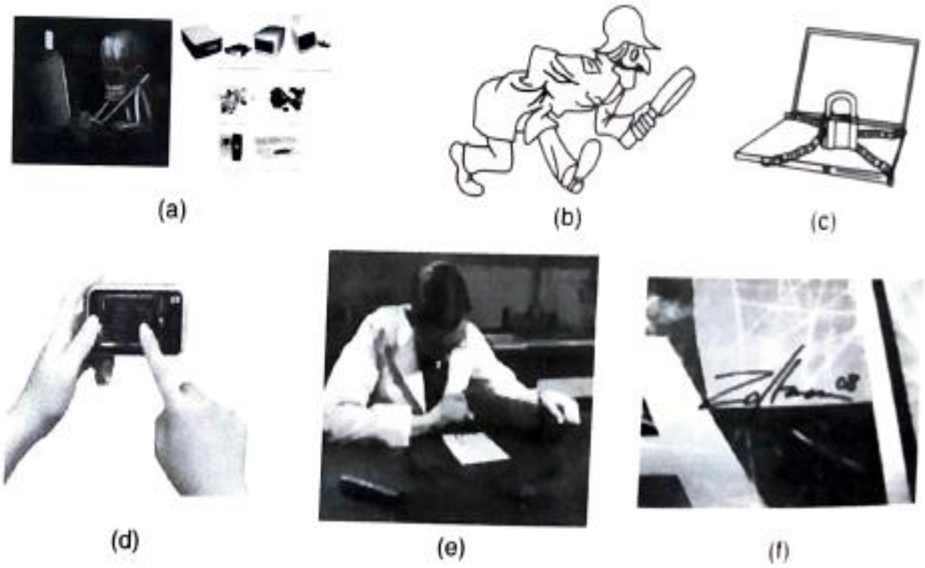


Fig. 5.11: Maintaining chain of custody 2. (a) Source of evidence - where did it come (b). Who found it? (c) Where was it stored/locked up? (d) Who touched it/tampered With it? (e) What did they do to it? What did they do with it? (f) Human signature always required

********************************** END*************************************