Cyber Security

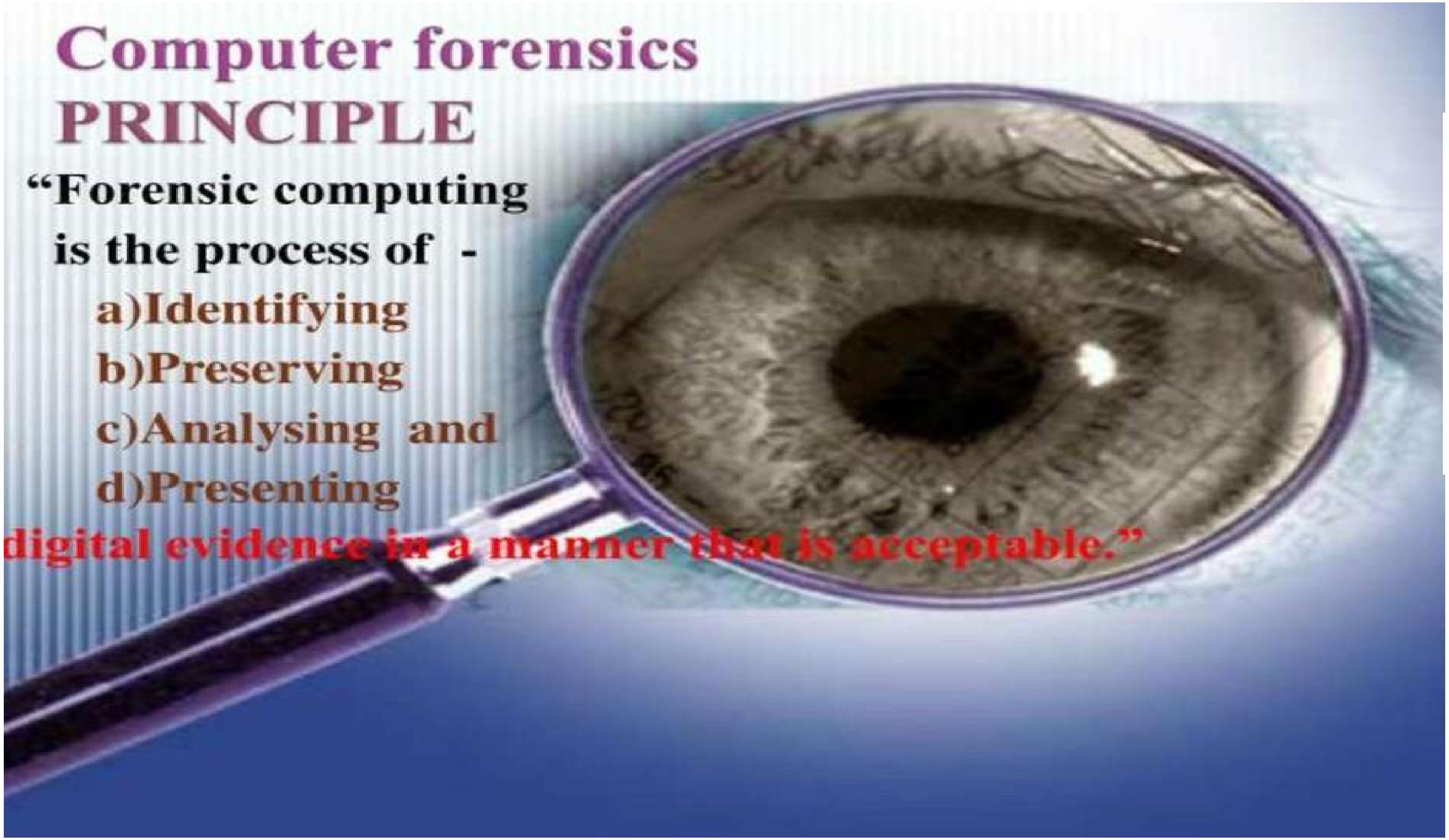
Unit :- 4

Understanding Computer Forensics

UNDERSTANDING COMPUTER FORENSICS: Introduction, Digital Forensics Science, The Need for Computer Forensics, Cyber forensics and Digital Evidence, Forensics Analysis of E-Mail, Digital Forensics Life Cycle, Chain of Custody Concept, Network Forensics, Approaching a Computer Forensics Investigation.
Forensics and Social Networking Sites: The Security/Privacy Threats, Challenges in Computer Forensics.

INTRODUCTION: CYBER FORENSICS

- Cyber forensics is a branch of forensic science which deals with the investigation, analysis techniques on computers.
- Cyber Forensic is also referred as Computer Forensic as it includes computer system indulged in Cyber Crime.
- Cyber Forensic aids in an investigation, collection and preservation of Evidences for legal purposes.



Computer forensics PRINCIPLE

"Forensic computing is the process of -

a)Identifying

b)Preserving

c)Analysing and

d)Presenting

digital evidence in a manner that is acceptable."

FUNCTION:

- Detect a computer incident, identify the intruders and prosecute the perpetrator in a court of law.

DIGITAL FORENSICS:

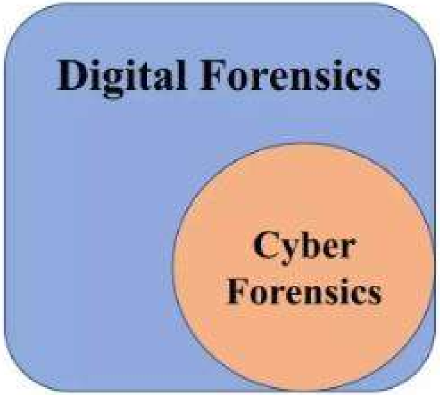
Digital Forensics is defined as the process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law. It is a science of finding evidence from digital media like a computer, mobile phone, server, or network. It provides the forensic team with the best techniques and tools to solve complicated digital-related cases.

Digital Forensics helps the forensic team to analyzes, inspect, identifies, and preserve the digital evidence residing on various types of electronic devices.

Digital forensic science is a branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to cybercrime.

<u>Difference between Cyber Forensics and Digital Forensics:</u>

Cyber Forensics	**Digital Forensics**
• It includes computer system for the commission of cyber crime.	• It includes not only computer but also other digital devices tlfor the commission of cyber crime.
• It involves network i.e., internet in various crimes.	• It can also work in the absence of internet.



Branches of Digital Forensics:

- **Media forensics:** It is the branch of digital forensics which includes identification, collection, analysis and presentation of audio, video and image evidences during the investigation process.
- **Cyber forensics:** It is the branch of digital forensics which includes identification, collection, analysis and presentation of digital evidences during the investigation of a cyber crime.
- **Mobile forensics:** It is the branch of digital forensics which includes identification, collection, analysis and presentation of digital evidences during the investigation of a crime committed through a mobile device like mobile phones, GPS device, tablet, laptop.
- **Software forensics:** It is the branch of digital forensics which includes identification, collection, analysis and presentation of digital evidences during the investigation of a crime related to softwares only.

THE NEED FOR COMPUTER FORENSICS

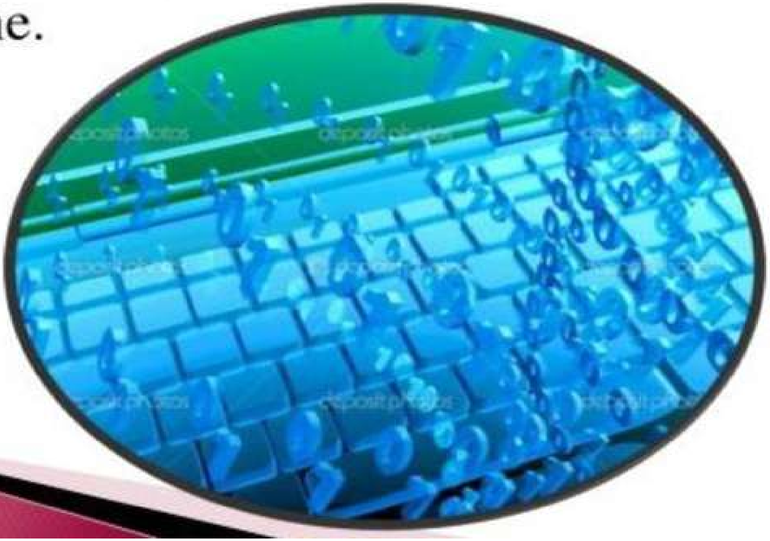
Computer forensics is also important because it can save your organization money. ... From a technical standpoint, the main goal of computer forensics is to identify, collect, preserve, and analyze data in a way that preserves the integrity of the evidence collected so it can be used effectively in a legal case.

Collection and Preservation of Digital Evidence:

- Determine the device is in On or OFF condition.
- Videograph and photograph the device.
- Note down the device model number and serial number.
- If any destructive device is suspected, remove the main plug immediately without shutting it down.
- Investigator must also look for CD, DVD, Flash drives, note pads, etc.
- Pack the collected devices in anti-static bag to prevent any kind of radiations.
- Place the devices in boxes or evidence bags and label them.
- Keep the devices safe and secure from magnets, extreme temperatures and other damages.
- Once all the evidences are collected and preserved, it can be sent to laboratory for further analysis.

NEEDS OF COMPUTER FORENSICS

- To produce evidence in the court that can lead to the punishment of the actual.
- To ensure the integrity of computer system.
- To focus on response to hi-tech offenses, started to intertwine.



CYBER FORENSICS AND DIGITAL EVIDENCE:

Digital evidence is information stored or transmitted in binary form that may be relied on in court. It can be found on a computer hard drive, a mobile phone, among other places. Digital evidence is commonly associated with electronic crime, or e-crime, such as child pornography or credit card fraud. However, digital evidence is now used to prosecute all types of crimes, not just e-crime. For example, suspects' e-mail or mobile phone files might contain critical evidence regarding their intent, their whereabouts at the time of a crime and their relationship with other suspects. In 2005, for example, a floppy disk led investigators to the BTK serial killer who had eluded police capture since 1974 and claimed the lives of at least 10 victims.

In an effort to fight e-crime and to collect relevant digital evidence for all crimes, law enforcement agencies are incorporating the collection and analysis of digital evidence, also known as computer forensics, into their infrastructure. Law enforcement agencies are challenged by the need to train officers to collect digital evidence and keep up with rapidly evolving technologies such as computer operating systems.

FORENSICS ANALYSIS OF EMAIL:

E-mail forensics refers to the study of source and content of e-mail as evidence to identify the actual sender and recipient of a message, data/time of transmission, detailed record of e-mail transaction, intent of the sender, etc. This study involves investigation of metadata, keyword searching, port scanning, etc. for authorship attribution and identification of e-mail scams.
Various approaches that are used for e-mail forensic are:

Header Analysis – Meta data in the e-mail message in the form of control information i.e. envelope and headers including headers in the message body contain information about the sender and/or the path along which the message has traversed. Some of these may be spoofed to conceal the identity of the sender. A detailed analysis of these headers and their correlation is performed in header analysis.

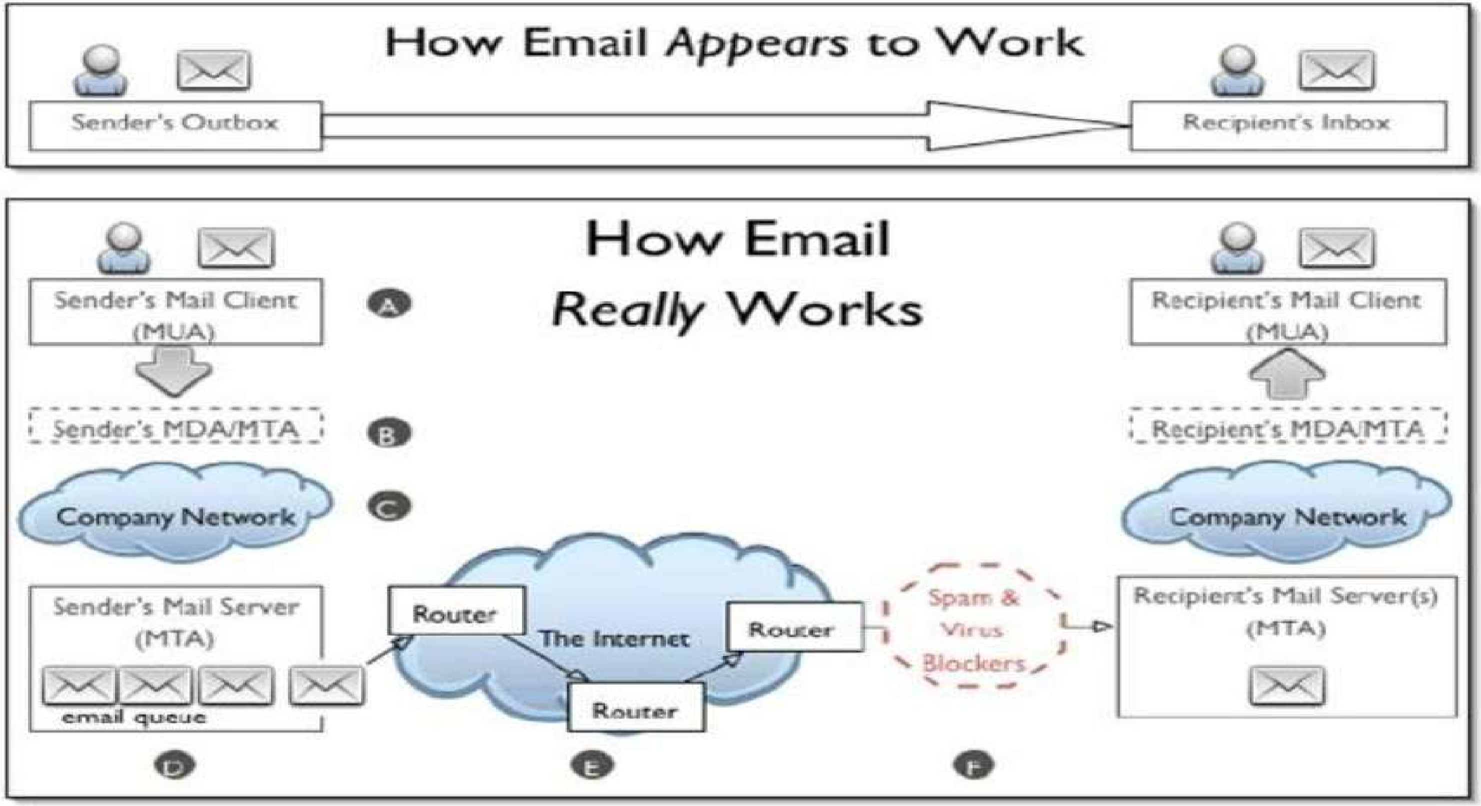
Bait Tactics – In bait tactic investigation an e-mail with http: "<imgsrc>" tag having image source at some computer monitored by the investigators is send to the sender of e-mail under investigation containing real (genuine) e-mail address. When the e-mail is opened, a log entry containing the IP address of the recipient (sender of the e-mail under investigation) is recorded on the http server hosting the image and thus sender is tracked. However, if the recipient (sender of the e-mail under investigation) is using a proxy server then IP address of the proxy server is recorded. The log on proxy server can be used to track the sender of the e-mail under investigation. If the proxy server's log is unavailable due to some reason, then investigators may send the tactic e-mail containing a) Embedded Java Applet that runs on receiver's computer or b) HTML page with Active X Object. Both aiming to extract IP address of the receiver's computer and e-mail it to the investigators.

Server Investigation – In this investigation, copies of delivered e-mails and server logs are investigated to identify source of an e-mail message. E-mails purged from the clients (senders or receivers) whose recovery is impossible may be requested from servers (Proxy or ISP) as most of them store a copy of all e-mails after their deliveries. Further, logs maintained by servers can be studied to trace the address of the computer responsible for making the e-mail transaction. However, servers store the copies of e-mail and server logs only for some limited periods and some may not co-operate with the investigators. Further, SMTP servers which store data like credit card number and other data pertaining to owner of a mailbox can be used to identify person behind an e-mail address.

Network Device Investigation – In this form of e-mail investigation, logs maintained by the network devices such as routers, firewalls and switches are used to investigate the source of an e-mail message. This form of investigation is complex and is used only when the logs of servers (Proxy or ISP) are unavailable due to some reason, e.g. when ISP or proxy does not maintain a log or lack of co-operation by ISP's or failure to maintain chain of evidence.

Software Embedded Identifiers – Some information about the creator of e-mail, attached files or documents may be included with the message by the e-mail software used by the sender for composing e-mail. This information may be included in the form of custom headers or in the form of MIME content as a Transport Neutral Encapsulation Format (TNEF). Investigating the e-mail for these details may reveal some vital information about the senders e-mail preferences and options that could help client side evidence gathering. The investigation can reveal PST file names, Windows logon username, MAC address, etc. of the client computer used to send e-mail message.

Sender Mailer Fingerprints – Identification of software handling e-mail at server can be revealed from the Received header field and identification of software handling e-mail at client can be ascertained by using different set of headers like "X-Mailer" or equivalent. These headers describe applications and their versions used at the clients to send e-mail. This information about the client computer of the sender can be used to help investigators devise an effective plan and thus prove to be very useful.



EMAIL FORENSICS TOOLS

Erasing or deleting an email doesn't necessarily mean that it is gone forever. Often emails can be forensically extracted even after deletion. Forensic tracing of e-mail is similar to traditional detective work. It is used for retrieving information from mailbox files.

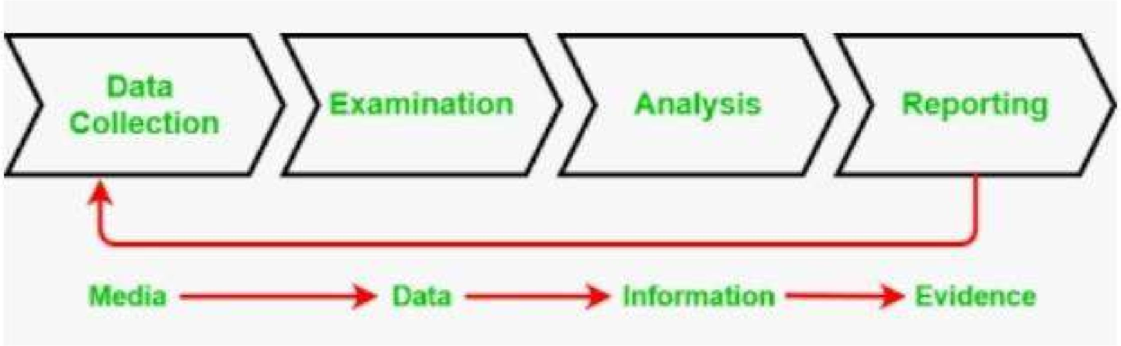
MiTec Mail Viewer – This is a viewer for Outlook Express, Windows Mail/Windows Live Mail, Mozilla Thunderbird message databases, and single EML files. It displays a list of contained messages with all needed properties, like an ordinary e-mail client. Messages can be viewed in detailed view, including attachments and an HTML preview. It has powerful searching and filtering capability and also allows extracting email addresses from all emails in opened folder to list by one click. Selected messages can be saved to eml files with or without their attachments. Attachments can be extracted from selected messages by one command.

OST and PST Viewer – Nucleus Technologies' OST and PST viewer tools help you view OST and PST files easily without connecting to an MS Exchange server. These tools allow the user to scan OST and PST files and they display the data saved in it including email messages, contacts, calendars, notes, etc., in a proper folder structure.

eMailTrackerPro – eMailTrackerPro analyses the headers of an e-mail to detect the IP address of the machine that sent the message so that the sender can be tracked down. It can trace multiple e-mails at the same time and easily keep track of them. The geographical location of an IP address is key information for determining the threat level or validity of an e-mail message.

EmailTracer – EmailTracer is an Indian effort in cyber forensics by the Resource Centre for Cyber Forensics (RCCF) which is a premier centre for cyber forensics in India. It develops cyber forensic tools based on the requirements of law enforcement agencies.

DIGITAL FORENSICS LIFECYCLE:



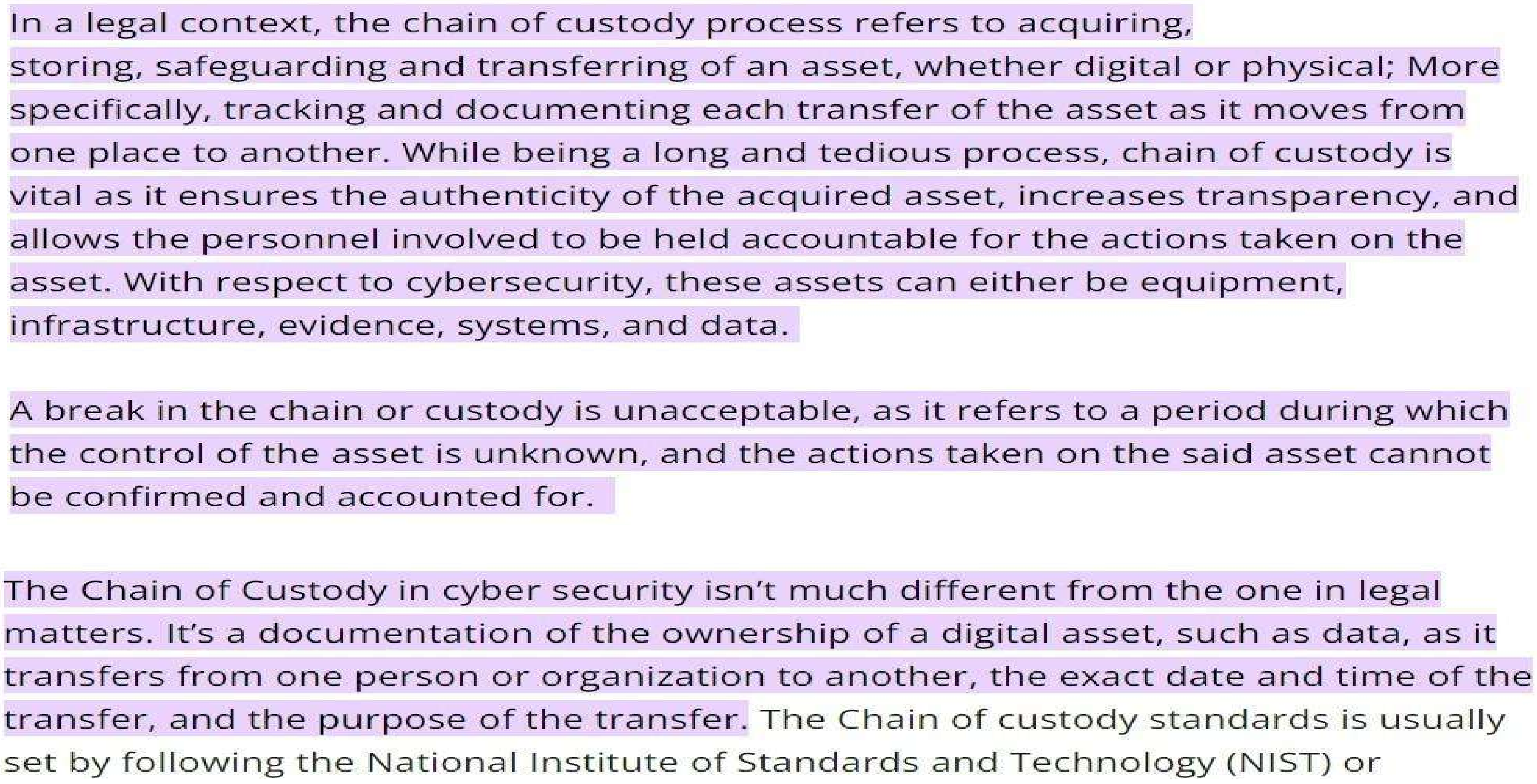
Collection: The first step in the forensic process is to identify potential sources of data and acquire data from them.

Examination: After data has been collected, the next phase is to examine the data, which involves assessing and extracting the relevant pieces of information from the collected data. This phase may also involve bypassing or mitigating OS or application features that obscure data and code, such as data compression, encryption, and access control mechanisms.

Analysis: Once the relevant information has been extracted, the analyst should study and analyze the data to draw conclusions from it. The foundation of forensics is using a methodical approach to reach appropriate conclusions based on the available data or determine that no conclusion can yet be drawn.

Reporting: The process of preparing and presenting the information resulting from the analysis phase.

Chain of Custody



In a legal context, the chain of custody process refers to acquiring, storing, safeguarding and transferring of an asset, whether digital or physical; More specifically, tracking and documenting each transfer of the asset as it moves from one place to another. While being a long and tedious process, chain of custody is vital as it ensures the authenticity of the acquired asset, increases transparency, and allows the personnel involved to be held accountable for the actions taken on the asset. With respect to cybersecurity, these assets can either be equipment, infrastructure, evidence, systems, and data.

A break in the chain or custody is unacceptable, as it refers to a period during which the control of the asset is unknown, and the actions taken on the said asset cannot be confirmed and accounted for.

The Chain of Custody in cyber security isn't much different from the one in legal matters. It's a documentation of the ownership of a digital asset, such as data, as it transfers from one person or organization to another, the exact date and time of the transfer, and the purpose of the transfer. The Chain of custody standards is usually set by following the National Institute of Standards and Technology (NIST) or

- Chain of custody is the accurate documentation of the movement and possession of a piece of evidence, from the time it is taken into custody until it is delivered to the court
  - Who collected it?
  - How and Where?
  - Who took possession of it?
  - How as it stored and protected?
  - Who took it out of storage and why?

Network Forensics

Network forensics is a subset of digital forensics that deals with the collection and analysis of network traffic with the goal of better understanding and avoiding cybercrime. The importance of network forensics has grown in recent years, according to a report from the European Union Agency for Cybersecurity (ENISA), with the emergence and popularity of network-based services such as e-mails, Directory services, World Wide Web, and others.

Using network forensics, the entire contents of e-mails, instant messages, web browsing operations, and file transfers can be recovered and rebuilt to reveal the original transaction. The payload inside the highest-layer packet may end up on disc, but the envelope that delivered it is only captured in network traffic. For the investigator, the network protocol data that surrounded each conversation is often highly valuable.

methods of Network Forensics?

“Stop, look, and listen” method: Administrators monitor each data packet that passes through the network, but only capture what is deemed suspicious and warrants further investigation. While this technique does not take up a lot of space, it does require a lot of processing power.

All network traffic is captured using the ”catch it as you can” technique. It ensures that no significant network events are overlooked. This is a time-consuming process that reduces storage efficiency as storage volume increases.

Conclusion

In a broad sense, forensics refers to anything that has to do with legal proceedings. Any organization that has been attacked should be able to recover quickly and effectively. In the case of Network Forensics, for example, if someone has sent an infected e-mail or if an attacker has broken into the webserver through a well-known vulnerability. Sony, Target, Home Depot, and a slew of other companies have been targeted and have suffered as a result. Companies are using intrusion detection systems, which help to perform a continuous wire recording in case an incident occurs, so there is a real need for forensics practitioners who can deal with network data.

Approaching a Computer Forensics Investigation

The phases in a computer forensics investigation are:

- Secure the subject system
- Take a copy of hard drive/disk
- Identify and recover all files
- Access/view/copy hidden, protected, and temp files
- Study special areas on the drive
- Investigate the settings and any data from programs on the system
- Consider the system from various perspectives
- Create detailed report containing an assessment of the data and information collected

Things to be avoided during forensics investigation:

- Changing date/timestamps of the files
- Overwriting unallocated space

Things that should not be avoided during forensics investigation:

- Engagement contract
- Non-Disclosure Agreement (NDA)

Elements addressed before drawing up a forensics investigation engagement contract:

- Authorization
- Confidentiality
- Payment
- Consent and acknowledgement
- Limitation of liability

General steps in solving a computer forensics case are:

- Prepare for the forensic examination
- Talk to key people about the case and what you are looking for
- Start assembling tools to collect the data and identify the target media
- Collect the data from the target media
- Use a write blocking tool while performing imaging of the disk
- Check emails records too while collecting evidence
- Examine the collected evidence on the image that is created
- Analyze the evidence
- Report your finding to your client

Forensics and Social Networking Sites

Social networking site is defined as web-based services

that allow individuals to:

- Create a public or semi-public profile
- Search or navigate through a list of users with whom they share a common connection
- View connections of other users

Although social networking sites have their uses, there are several associated security threats. The concerns regarding social networking sites are:

- Does the social networking site violate people's intellectual property rights
- Whether these sites infringe the privacy of their own users
- Whether these sites promote fraudulent and illegal activities

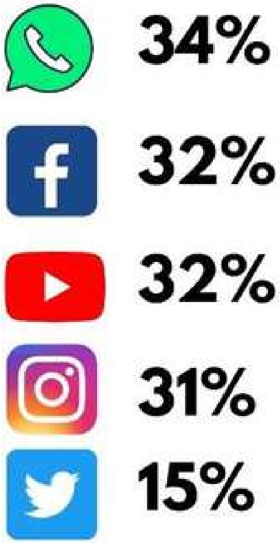
Content preservation can be challenging given the dynamic, short-lived and often multi-format nature of social media. There is generally no control over the content posted on social media networking sites. High level of forensic skill is required to analyze and quantify the preserved data to answer questions such as:

- Who posted the offending content?
- Is there a real live person to whom the offending content can be attributed even when evidence exists?
- Can we identify the time frame associated with the posting of the offending content?
- How much of the offending content exists across the entire social networking platform?
- Is there other content that supports interpretation of the relevant content?
- How accurate is the reported physical location?

The Security/Privacy Threats,

Security issues that are associated with social networking sites are:

- Corporate espionage
- Cross site scripting
- Virus and Worms
- Social networking site aggregators
- Phishing
- Network infiltration leading to data leakage
- ID theft
- Cyberbullying
- Content-Based Image Retrieval (CBIR)
- Spam
- Stalking

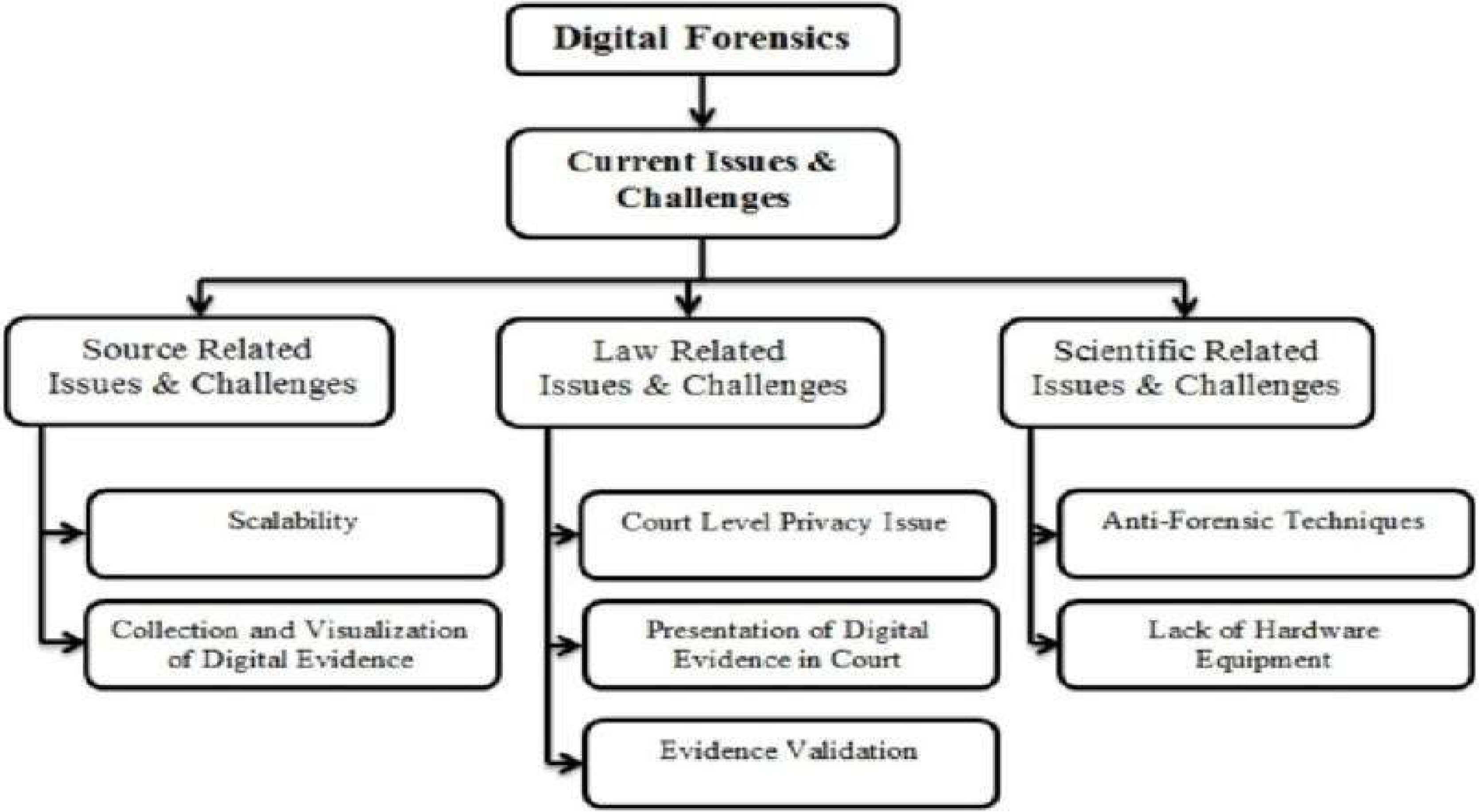


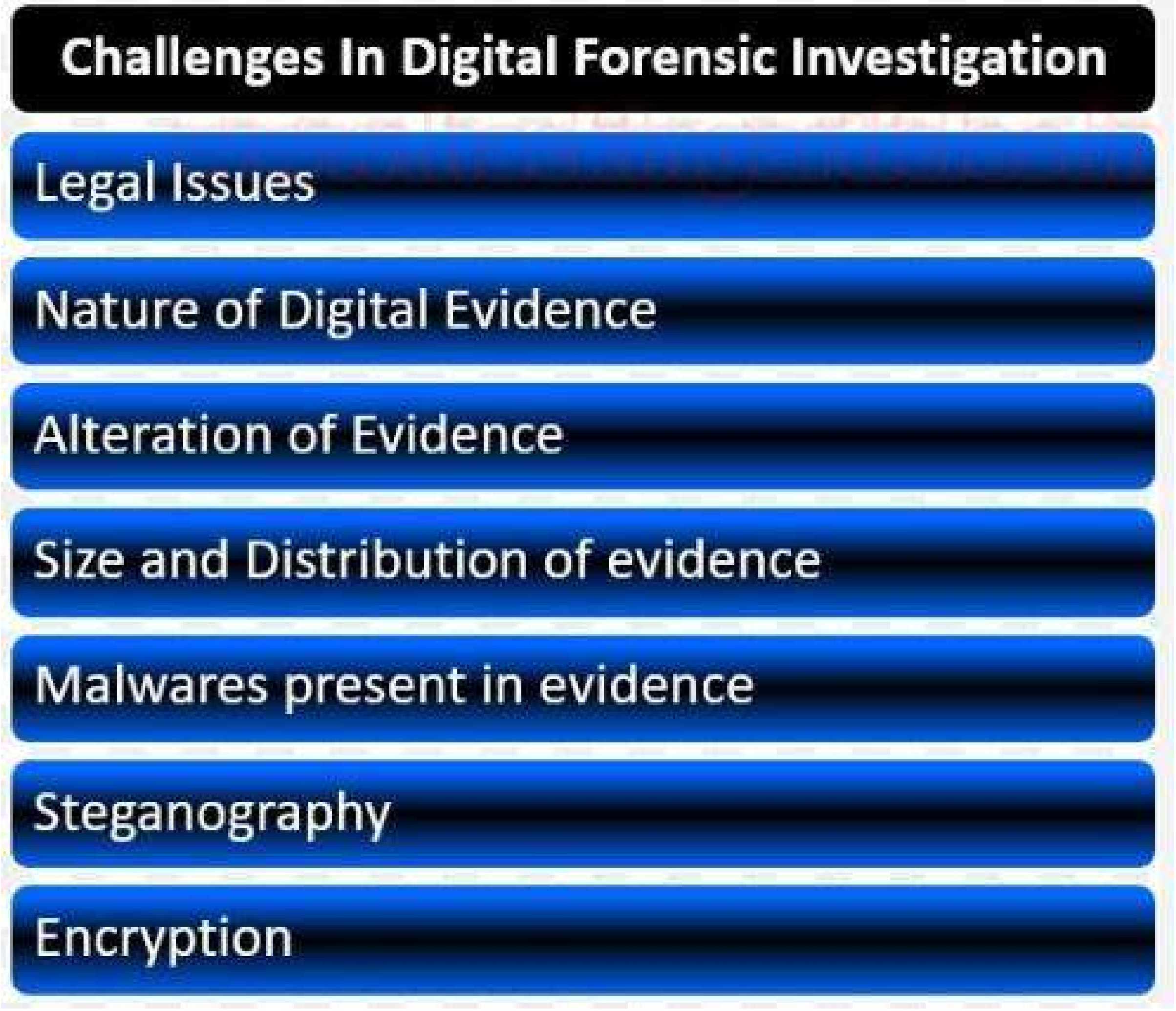
(Based on Lokniti Survey, 2019 in which they asked frequency at which they used Social Media Platforms)

Challenges in Computer Forensics

- The advancement of encryption. As encryption standards rise and the algorithms become more complex, it will be more difficult and more time-consuming for specialists to decrypt and then piece together encrypted files into meaningful information.

- Maintaining credible certifications and industry standards in the field.
  - The National Institute of Standards and Technology (NIST) creates the various standards for the technology industry in the US.
  - More standards need to be adopted for this field to make the gathered evidence and the compiled information used in court more credible in the eyes of the judge, jury and opposing attorneys.


Digital Forensics
Current Issues & Challenges
Source Related Issues & Challenges
Law Related Issues & Challenges
Scientific Related Issues & Challenges
Scalability
Collection and Visualization of Digital Evidence
Court Level Privacy Issue
Presentation of Digital Evidence in Court
Evidence Validation
Anti-Forensic Techniques
Lack of Hardware Equipment



Challenges In Digital Forensic Investigation

Legal Issues

Nature of Digital Evidence

Alteration of Evidence

Size and Distribution of evidence

Malwares present in evidence

Steganography

Encryption