GRADAMIC

B.Tech–2nd Year Session 2023–24 Odd/Even Semester

Dr. A. P. J. Abdul Kalam Technical University
Lucknow, Uttar Pradesh

# CYBER SECURITY

## (BCC301 / BCC401/ BCC301H / BCC401H)

app.gradamic.com

UNIT – 4th

# UNIT-IV

# DIGITAL FORENSIC SCIENCE

Digital forensic science is the art of recovering and analysing the contents found on digital devices such as desktops, notebooks/net books, tablets, smart phones, etc., was little-known a few years ago.

However, with the growing incidence of cybercrime, and the increased adoption of digital devices, this branch of forensics has gained significant importance in the recent past.

## COMPUTER FORENSIC

Computer Forensics is a scientific method of investigation and analysis in order to gather evidence from digital devices or computer networks and components which is suitable for presentation in a court of law or legal body.

It involves performing a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it.

## TYPES

- ✓ **Memory Forensics:** Deals with collecting data from system memory (system registers, cache, RAM) in raw form and then analysing it for further investigation.
- ✓ **Disk Forensics:** It deals with extracting raw data from the primary or secondary storage of the device by searching active, modified, or deleted files.
- ✓ **Network Forensics:** It is a sub-branch of Computer Forensics that involves monitoring and analysing the computer network traffic.
- ✓ **Database Forensics:** It deals with the study and examination of databases and their related metadata.
- ✓ **Malware Forensics:** It deals with the identification of suspicious code and studying viruses, worms, etc.
- ✓ **Email Forensics:** It deals with emails and their recovery and analysis, including deleted emails, calendars, and contacts.
- ✓ **Mobile Phone Forensics:** It mainly deals with the examination and analysis of phones and smartphones and helps to retrieve contacts, call logs, incoming, and outgoing SMS, etc

## Advantages of Computer Forensics

- To produce evidence in the court, which can lead to the punishment of the culprit.
- It helps the companies gather important information on their computer systems or networks potentially being compromised.
- Efficiently tracks down cyber criminals from anywhere in the world.
- Helps to protect the organization's money and valuable time.
- Allows to extract, process, and interpret the factual evidence, so it proves the cybercriminal actions in the court

## Disadvantages of Computer Forensics

- Before the digital evidence is accepted into court it must be proved that it is not tampered with. ¬
- Producing and keeping electronic records safe is expensive.
- Legal practitioners must have extensive computer knowledge.
- Need to produce authentic and convincing evidence.
- If the tool used for digital forensics is not according to specified standards, then in a court of law, the evidence can be disapproved by justice.
- A lack of technical knowledge by the investigating officer might not offer the desired result.

## APPLICATIONS

Intellectual Property theft, Employment disputes, Fraud investigations, Misuse of the Internet and email in the workplace, Forgeries related matters, Bankruptcy investigations

## PROCEDURE COMPUTER FORENSIC

- ✓ **Identification:** Identifying what evidence is present, where it is stored, and how it is stored (in which format). Electronic devices can be personal computers, Mobile phones, PDAs, etc.
- ✓ **Preservation:** Data is isolated, secured, and preserved. It includes prohibiting unauthorized personnel from using the digital device so that digital evidence, mistakenly or purposely, is not tampered with and making a copy of the original evidence.
- ✓ **Analysis:** Forensic lab personnel reconstruct fragments of data and draw conclusions based on evidence.
- ✓ **Documentation:** A record of all the visible data is created. It helps in recreating and reviewing the crime scene. All the findings from the investigations are documented
- ✓ **Presentation:** All the documented findings are produced in a court of law for further investigations.

## Some Tools used for Investigation:

### Tools for Laptop or PC

- **COFFEE** – A suite of tools for Windows developed by Microsoft.
- **The Coroner's Toolkit** – A suite of programs for Unix analysis.
- **The Sleuth Kit** – A library of tools for both Unix and Windows.

### Tools for Memory

- **Volatility**
- **Windows SCOPE**

### Tools for Mobile Device

- **Microsystem Tion XRY/XAC**

## NEED OF COMPUTER FORENSIC

1. **Digital Evidence:** In the modern world, a significant amount of criminal activity involves digital devices. Computer forensics is crucial for collecting, analysing, and preserving digital evidence in criminal investigations.
2. **Cybercrime Investigations:** With the rise of cybercrime, computer forensics plays a vital role in investigating and preventing various online criminal activities, including hacking, identity theft, a in financial fraud.
3. **Legal Admissibility:** Computer forensic techniques ensure that evidence gathered from digital devices is collected in a legally admissible manner. This is essential for maintaining the integrity of evidence.
4. **Data Recovery:** Computer forensics allows for the recovery of lost, deleted, or corrupted data. This is Particularly important in cases where critical information may have been intentionally or unintentionally tampered with.
5. **Employee Misconduct:** Organizations use computer forensics to investigate cases of employee misconduct, including unauthorized access to confidential information, intellectual property theft, or violations of company policies.
6. **Intellectual Property Theft:** Businesses often use computer forensics to investigate cases of intellectual property theft, including the unauthorized access, copying, or distribution of proprietary information.
7. **Malware Analysis:** Computer forensics experts analyse malware to understand its behaviour, origin, and impact. This knowledge is critical for developing effective cybersecurity measures.
8. **Training and Prevention:** Computer forensics professionals provide training to law enforcement, IT professionals, and organizations to enhance awareness of cyber threats and best practices for preventing and responding to incidents. ¬
9. **Civil Litigation Support:** In civil litigation, computer forensics can be used to uncover electronic evidence related to disputes. This may include email communications, document trails, or other digital artifacts that are relevant to legal proceedings. ¬
10. **Network Security:** Computer forensics is essential for assessing the security of computer systems and networks.

## COMPLIANCE AND REGULATIONS

Many industries are subject to specific regulations regarding the handling and protection of digital information. Computer forensics helps organizations comply with these regulations and standards.

**Incident Response:** Computer forensics is a key component of incident response in the case of a security breach. It helps identify the source of the breach, the extent of the damage, and provides ¬insights for preventing future incidents.

## Techniques used in Computer Forensic

- Cross-drive analysis
- Steganography
- Deleted files recovery:
- Live analysis
- Stochastic forensics

## CYBER FORENSIC

- ✓ Cyber forensics is a process of extracting data as proof for a crime (that involves electronic devices)
- ✓ The main aim of cyber forensics is to maintain the thread of evidence and documentation to find out who did the crime digitally

### Cyber forensics can do the following:

- It can recover deleted files, chat logs, emails, etc
- It can also get deleted SMS, Phone calls. ¬It can get recorded audio of phone conversations.
- It can determine which user used which system and for how much time.
- It can identify which user ran which program.

### Why is cyber forensics important?

- Cyber forensics helps in collecting important digital evidence to trace the criminal
- Electronic equipment stores massive amounts of data that a normal person fails to see.
- It is also helpful for innocent people to prove their innocence via the evidence collected online.
- It is not only used to solve digital crimes but also used to solve real-world crimes like theft cases, murder, etc.
- Businesses are equally benefitted from cyber forensics in tracking system breaches and finding the attackers.

### The Process Involved in Cyber Forensics

- Obtaining a digital copy of the system that is being or is required to be inspected.
- Authenticating and verifying the reproduction.
- Recovering deleted files (using Autopsy Tool).
- Using keywords to find the information you need.
- Establishing a technical report.

### Techniques that cyber forensic investigators use

**Reverse steganography:** Steganography is a method of hiding important data inside the digital file, image, etc. So, cyber forensic experts do reverse steganography to analyse the data and find a relation with the case.

**Deleted file recovery:** This includes searching for memory to find fragments of a partially deleted file in order to recover it for evidence purposes.

**Cross-drive analysis:** In this process, the information found on multiple computer drives is correlated and cross-references to analyse and preserve information that is relevant to the investigation

**Live analysis:** In this technique, the computer of criminals is analysed from within the OS in running mode. It aims at the volatile data of RAM to get some valuable information.

**Stochastic forensics:** It is a method to forensically re-establish the digital activities that have insufficient digital artifacts

## ADVANTAGES

- They efficiently track down the culprit anywhere in the world. They help people or organizations to protect their money and time.
- The relevant data can be made trending and be used in making the public aware of it.
- Cyber forensics ensures the integrity of the computer.
- Through cyber forensics, many people, companies, etc get to know about such crimes, thus taking proper measures to avoid them.

## How did Cyber Forensics Experts work?

**Identification:** The first step of cyber forensics experts is to identify what evidence is present, where it is stored, and in which format it is stored.

**Preservation:** After identifying the data, the next step is to safely preserve the data and not allow other people to use that device so that no one can tamper data.

**Analysis:** After getting the data, the next step is to analyse the data or system. Here the expert recovers the deleted files and verifies the recovered data and finds the evidence that the criminal tried to erase by deleting secret files. This process might take several iterations to reach the final conclusion

**Documentation:** Now after analysing data a record Is created This record contains all the recovered and available (not deleted). data which helps in recreating the crime scene and reviewing it.

**Presentation:** This is the final step in which the analysed data is presented in front of the court to solve cases.

## SKILL NEEDED FOR CYBER EXPERT

- the expert must be aware of criminal laws, a criminal investigation, etc. and must have strong knowledge of basic cyber security.
- the experts must be updated with the latest technology.
- The expert should be very attentive while examining a large amount of data to identify proof/evidence.
- Cyber forensic experts must be able to analyse the data, derive conclusions from it and make proper interpretations.
- The communication skill of the expert must be good so that while presenting evidence in front of the court, everyone understands each detail with clarity.

## DIGITAL EVIDENCE

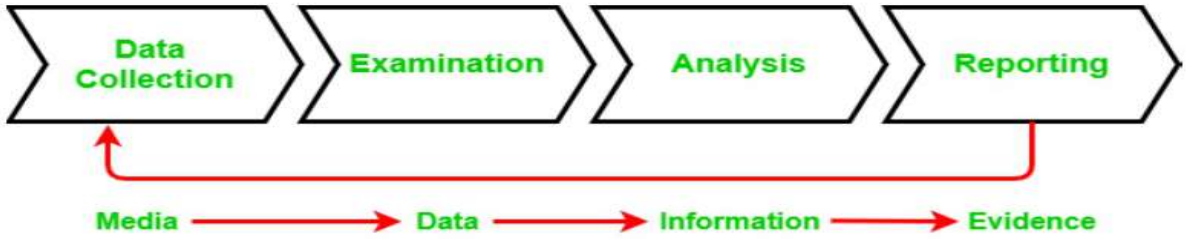
Digital evidence is any information or data of value to an investigation that is stored on, received by, or transmitted by an electronic device.

Text messages, emails, pictures and videos, and internet searches are some of the most common types of digital evidence.

### Challenges Faced During Digital Evidence Collection:

- Collecting data from volatile storage.
- Recovering lost data.
- Ensuring the integrity of collected data.
- Evidence should be handled with utmost care as data is stored in electronic media and it can get damaged easily

### Process involved in Digital Evidence Collection




- **Data collection:** In this process data is identified and collected for investigation.
- **Examination:** In the second step the collected data is examined carefully.
- **Analysis:** In this process, different tools and techniques are used and the collected evidence is analysed to reach some conclusion.
- **Reporting:** In this final step all the documentation, reports are compiled so that they can be submitted in court.

### FORENSIC ANALYSIS OF E-MAIL

Email forensics is the analysis of the content source of the email message, by identifying the sender and the receiver, the date and time of the email, and analysing all the activities involved.

### Email Header Forensics Analysis

- A full header view of an email provides the entire path email's journey from its source to destination.
- The header also includes IP and other useful information.
- The body of email contains actual message. Headers can be easily spoofed by spammers
- Header protocol analysis is important for investigating evidence. After getting the source IP address we find the ISP's details.
- By contacting ISP, we can get further information like: Name, Address, Contact number, Internet facility, Type of IP address, Any other relevant information.

- It is important during investigations that logs of all servers in the chain need to be examined as soon as possible. If the server mentioned in the bottom received section does not match the server of the email sender, it is a fake email.
- The Message-ID will help to find a particular email log entry in an email server. RFC2822 defines the Internet message format.

**Email header forensics can help investigators trace the origin of fraudulent or malicious emails. Some important components of email headers include:**

- **Reply-to:** The address the email will go to if you reply
- Return-path: The web address that can be traced back to the sender
- **Received:** Shows all the servers the email went through to reach the recipient, as well as any associated IP addresses
- **Message ID:** An identifier that can help find a particular email log entry within an email server's log file
- **DKIM signature:** A digital signature attached to the email's header that verifies the legitimacy of the email source

**According to RFC2822**

- Each email must have a globally unique identifier
- Defines the syntax of Message-ID

**Message-ID can appear in three header fields:**

- Message-ID header
- In-reply-to header
- References header

**Email Server Investigation**

- Email servers are investigated to locate the source of an email.
- For example, if an email is deleted from a client application, senders, or receivers, then related ISP or Proxy servers are scanned as they usually save copies of emails after delivery.
- Servers also maintain logs that can be analysed to identify the computer's address from which the email originated.

**Investigation of Network Devices**

In some cases, logs of servers are not available. This can happen for many reasons, such as when servers are not configured to maintain logs or when an ISPs refuses to share the log files.

In such an event, investigators can refer to the logs maintained by network devices such as switches, firewalls, and routers to trace the source of an email message.

### Sender Mailer Fingerprints

X-headers are email headers that are added to messages along with standard headers, like Subject and To. These are often added for spam filter information, authentication results, etc., and can be used to identify the software handling the email at. the client such as Outlook or Opera Mail. In addition, the x-originating-IP header can be used to find the original sender, i.e., the IP address of the sender's computer.

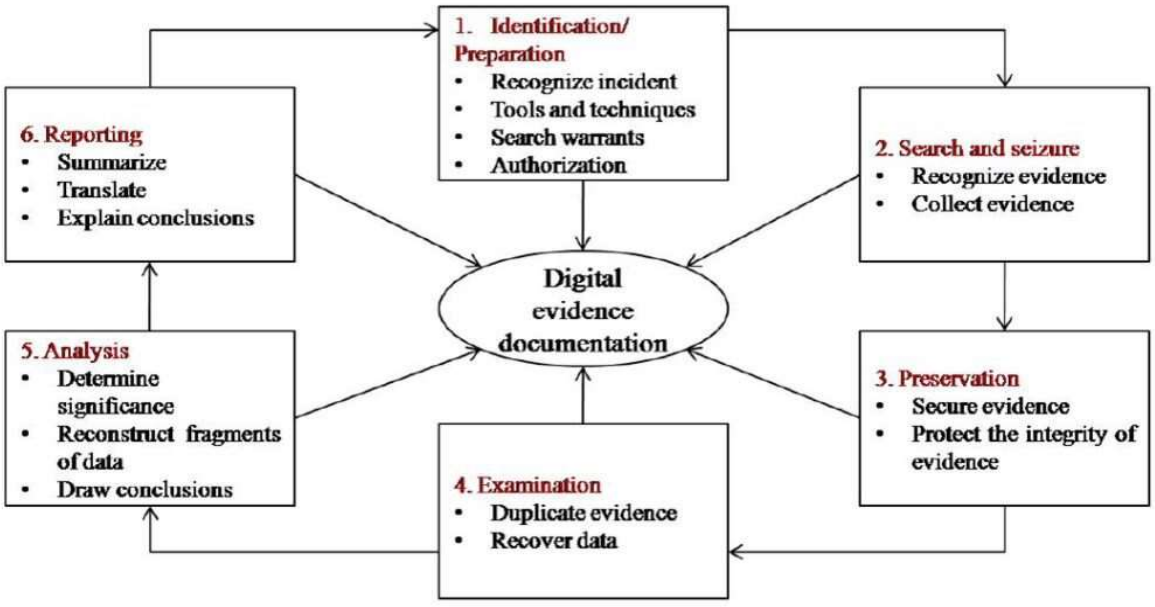
### Message-IDs

Message-ID is a unique identifier that helps forensic examination of emails across the globe. It comprises a long string of characters that end with the Fully Qualified Domain Name (FQDN). Message IDs are generated by client programs that send emails, such as Mail User Agents (MUA) or Mail Transfer Agents (MTA).

*There are two parts of a Message-ID. One part is before @, and another part is after @. The first part of the message-ID contains information, such as the message's timestamp. This information is the data regarding the time when the message was sent. The second part of the Message-ID contains information related to FQDN*.

### Forensic life cycle phases are:

1. Preparation and identification
2. Collection and recording.
3. Storing and transporting
4. Examination/investigation
5. Analysis, interpretation, and attribution
6. Reporting
7. Testifying




**DIGITAL FORENSIC LIFECYCYLE**

### 1. Preparing for the Evidence and Identifying the Evidence

- In order to be processed and analysed, evidence must first be identified. It might be possible that the evidence may be overlooked and not identified at all. A sequence of events in a computer might include interactions between: Different files, Files and file systems, Processes and files, Log files
- In case of a network, the interactions can be between devices in the organization or across the globe (Internet). If the evidence is never identified as relevant, it may never be collected and processed.

### 2. Collecting and Recording Digital Evidence

- Digital evidence can be collected from many sources. The obvious sources can be:
- Mobile phone, Digital cameras, Hard drives, CDs, USB memory devices
- Non-obvious sources can be: Digital thermometer settings, Black boxes inside automobiles
- Proper care should be taken while handling digital evidence as it can be changed easily. Once changed, the evidence cannot be analysed further. A cryptographic hash can be calculated for the evidence file and later checked if there were any changes made to the file or not

### 3. Storing and Transporting Digital Evidence

*Some guidelines for handling of digital evidence:*

- Image computer-media using a write-blocking tool to ensure that no data is added to the suspect device. Document everything that has been done.Only use tools and methods that have been tested and evaluated to validate their accuracy and reliability.
- Care should be taken that evidence does not go anywhere without properly being traced. Sometimes evidence must be transported from place to place either physically or through a network.

### 4. Examining/Investigating Digital Evidence

- Forensics specialist should ensure that he/she has proper legal authority to seize, copy and examine the data. As a general rule, one should not examine digital information unless one has the legal authority to do so. Forensic investigation performed on data at rest (hard disk) is called dead analysis.

### 5. Analysis, Interpretation and Attribution

- The digital evidence must be analysed to determine the type of information stored on it. Examples of forensics tools: Forensics Tool Kit (FTK), EnCase, Scalpel (file carving tool).

### 6. Reporting

- After the analysis is done, a report is generated. The report may be in oral form or in written form or both.

- The report contains all the details about the evidence in analysis, interpretation, and attribution steps.
- Some of the general elements in the report are:
- Identity of the report agency, Case identifier or submission number, Case investigator, Identity of the submitter, Date of receipt, Date of report, Descriptive list of items submitted for examination, Identity and signature of the examiner, Brief description of steps taken during examination, Results/conclusions.

### 7. Testifying

This phase involves presentation and cross-examination of expert witnesses. An expert witness can testify in the form of:

- Testimony is based on sufficient facts or data
- Testimony is the product of reliable principles and methods
- Witness has applied principles and methods reliably to the facts of the case.

## CHAIN OF CUSTODY

Chain of Custody refers to the chronological documentation or paper trail showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence.

It's crucial in legal contexts, particularly in criminal cases, to ensure that evidence presented in court is reliable and has not been tampered with.

A proper chain of custody establishes the integrity of the evidence by documenting who had possession of it at any given time, from its collection at the crime scene to its presentation in court.

This documentation typically includes dates, times, locations, and the identities of individuals handling the evidence.

Any break or gap in the chain of custody can raise doubts about the authenticity or admissibility of the evidence.

### Importance of Chain of Custody

- **Evidence Integrity:** Ensures that evidence remains intact and unaltered from the time of collection to its presentation in court.
- **Legal Admissibility:** Establishes a clear and documented trail of custody, strengthening the reliability and admissibility of the evidence in court.
- **Preservation of Rights:** Protects the rights of the accused by ensuring that evidence is handled and stored properly, minimizing the risk of tampering or contamination
- If any of the evidence is brought to the court, and has undergone a broken chain of custody, the evidence cannot be presented in the court of law. The chain of custody must always be maintained by identified persons, who have the authority by law to possess the evidence such as police officers, forensic experts, evidence technicians, officers of the court, etc.

### Chain of custody must be maintained

- Criminal investigation, Civil litigation, Dope testing of athletes, Clinical trials, Violence and abuse cases
- Fields of history, art collection, Postal services
- Research if animals are ethically raised or not
- Testing of food products
- Seizure of prohibited substance, Seizure of money, gold ornaments or other valuables by income tax, customs or revenue departments

### Role of police in maintaining a chain of custody

- Collecting the evidence from the crime scene.
- Keeping the evidence collected safe in sealed bags with unique identification numbers.
- Examining the evidence collected.
- Be responsible if the evidence is transferred to another specialist for examination or analysis.
- Handle all the transfers of the evidence taking place.
- Maintaining the record of every procedure which the evidence is handled through.
- Presenting the evidence with all authenticated records before the court.

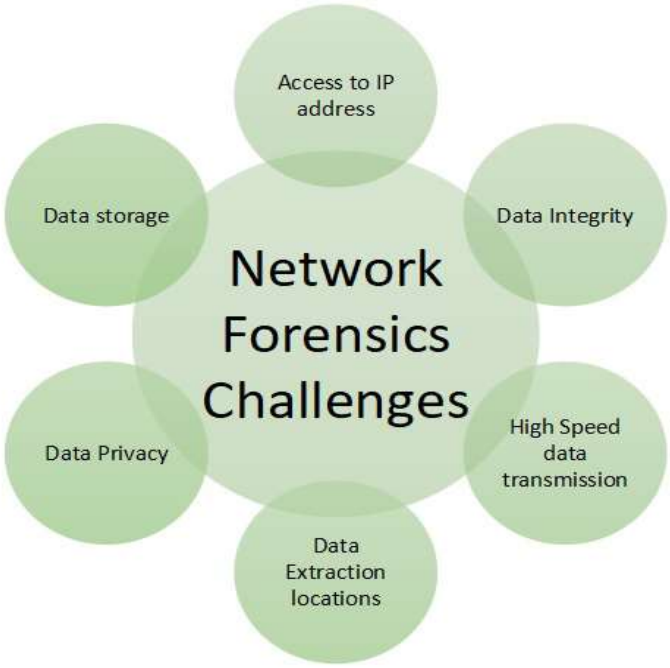
## NETWORK FORENSIC

**Network forensics** is a subcategory of digital forensics that essentially deals with the examination of the network and its traffic going across a network that is suspected to be involved in malicious activities, and its investigation.

For example a network that is spreading malware for stealing credentials or for the purpose analysing the cyberattack

### Processes Involved in Network Forensics:

- **Identification:** In this process, investigators identify and evaluate the incident based on the network pointers.
- **Safeguarding:** In this process, the investigators preserve and secure the data so that the tempering can be prevented.
- **Accumulation:** In this step, a detailed report of the crime scene is documented and all the collected digital shreds of evidence are duplicated.
- **Observation:** In this process, all the visible data is tracked along with the metadata.
- **Investigation:** In this process, a final conclusion is drawn from the collected shreds of evidence.
- **Documentation:** In this process, all the shreds of evidence, reports, conclusions are documented and presented in court.




**Advantages-**

- Network forensics helps in identifying security threats and vulnerabilities.
- It analyses and monitors network performance demands.
- Network forensics helps in reducing downtime.
- Network resources can be used in a better way by reporting and better planning.
- It helps in a detailed network search for any trace of evidence left on the network.

**Disadvantage-** The only disadvantage of network forensics is that it is difficult to implement.

**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
- Analyse the evidence Report your finding to your client

### Forensic & Social networking site

**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

**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 analyse 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?

**Security issues that are associated with social networking sites are:**

- Corporate espionage
- Cross site scripting
- Virus and Worms
- Phishing
- Network infiltration leading to data leakage
- ID theft
- Cyberbullying
- Spam
- Stalking.

**Challenges in Computer Forensic**

**Evolving Technology-**

- **Rapid Technological Advancements:** The pace of technological change can outstrip the development of forensic tools and techniques, making it challenging to keep up. Encryption and Security Measures:
- **Encrypted Data:** The widespread use of encryption can make it difficult to access and analyse data during forensic investigations.
- **Security Mechanisms:** Increasingly sophisticated security measures can impede the extraction of evidence from devices.

**Data Volume and Complexity-**

- **Big Data Challenges:** The sheer volume of digital data generated makes it challenging to sift through and analyse relevant information efficiently
- **Complex Data Structures:** The complexity of data structures and file formats can complicate the extraction and interpretation of evidence.

**Anti-Forensic Techniques-**

- **Anti-Forensic Tools:** Perpetrators may employ anti-forensic tools and techniques to erase or alter digital evidence, making it harder for investigators to reconstruct events.
- **Data Obfuscation:** Deliberate attempts to hide or obfuscate digital trails can pose challenges in uncovering the truth.

**Legal and Ethical Issues-**

- **Privacy Concerns:** Striking a balance between forensic investigations and individual privacy rights poses a significant challenge.

- **Legal Compliance:** Adhering to legal procedures, obtaining proper warrants, and ensuring the admissibility of evidence can be complex.

### Volatility of Digital Evidence-

- **Data Volatility:** Digital evidence can be volatile and easily altered, requiring swift and careful handling to preserve its integrity.
- **Live Systems:** Analysing live systems without causing disruption or altering data is a challenge.

### International Jurisdiction-

- **Cross-Border Investigations:** The global nature of cybercrime requires collaboration across international borders, introducing challenges related to jurisdiction and legal frameworks. Skill Shortages and Training:
- **Specialized Expertise:** Computer forensics demands highly specialized skills, and there may be shortages of qualified professionals.
- **Continuous Training:** Rapid changes in technology necessitate ongoing training for forensic investigators to stay current Budgetary Constraints.
- **Resource Limitations:** Adequate resources, both in terms of technology and personnel, are crucial, and budget constraints can hinder effective forensic investigations

### Digital Forensic Tool Validation-

- **Tool Reliability:** Ensuring the reliability and accuracy of forensic tools is challenging and requires continuous validation and testing.
- **Open-Source Tools:** While open-source tools are valuable, their security and reliability need to be carefully assessed. Data Privacy and Consent:
- **Consent Challenges:** Obtaining consent for digital investigations can be complex, especially in corporate environments or when dealing with sensitive personal data

### Cloud Computing Challenges-

- **Data Residency:** Data stored in the cloud may reside in different jurisdictions, adding complexity to the legal aspects of investigations.
- **Access to Cloud Data:** Obtaining access to cloud-based evidence can be challenging due to service provider policies and security measures.

### Forensic Readiness

**Proactive Planning:**

- Organizations may lack proactive forensic readiness plans, hindering their ability to respond effectively to incidents.
- Addressing these challenges requires a combination of technical innovation, legal frameworks, collaboration, and ongoing professional development within the field of computer forensics