**SUB: Cyber Security**

**Unit 5 : Cyber Forensics**

Prof: Morade D.S.

## 5.1 Introduction to Cyber Forensics

Cyber Forensics is like detective work, but for computers and digital devices. When a **cybercrime** happens—like hacking, online fraud, or data theft—experts look for **digital evidence** to solve the crime.

- **Why is it important?** Because the evidence found on computers, phones, or the internet can be used in **court**.
- Only **trained professionals** with technical knowledge can handle this evidence properly.

**Example:**
Imagine someone hacks into a bank account online. Cyber forensic experts can track the hacker by checking logs, emails, and digital footprints to find out who did it.

---

## 5.2 Historical Background of Cyber Forensics

Cyber Forensics (also called **Computer Forensics** or **Digital Forensics**) started because people began committing crimes using computers and digital devices.

- As long as people **store data digitally**, experts can investigate and find evidence.
- It is a **new but fast-growing field** because cybercrime is increasing.

**Main goal:** To find **digital evidence** that proves if a crime or fraud happened.

**Example:**
If a company suspects an employee of stealing confidential files, cyber forensic experts can check computers and servers to see which files were accessed or copied, and by whom.

---

## Difference Between Computer Security and Computer Forensics

- **Computer Security:** Focuses on **preventing cybercrimes** and protecting computers from hackers.
- **Computer Forensics:** Focuses on **investigating cybercrimes** after they happen and finding evidence.

**Example:**

- Computer security: Installing antivirus to stop a hacker.
- Computer forensics: If a hacker breaks in anyway, investigators find out **how** it happened and **who** did it.

---

## 5.3 **Digital Forensics Science**

Digital forensics is like detective work for computers and digital devices. It's about **finding, analyzing, and protecting digital evidence** in a legal and scientific way.

- **Digital Forensic:** Using careful scientific methods to find digital proof from devices like computers, phones, or USB drives.
- **Computer Forensic:** Following the law to collect and examine data safely from digital devices.

**Example:**
If someone hacks a company's computer, forensic experts can check the computer to find **who did it, when, and how**, without changing any evidence.

---

## Key Points about Digital Evidence

- Evidence can be on **computers, phones, tablets, or any electronic device**.
- Experts use tools and techniques to **collect, examine, and preserve** this evidence.
- Even deleted or hidden files can sometimes be recovered.

**Example:**
If a student deletes a file with cheating answers from a school computer, forensic tools may still recover it.

---

## Role of Digital Forensics

1. **Uncover and document evidence** – Like taking notes of what you find on a computer.
2. **Support other evidence** – Match digital evidence with other clues.
3. **Show patterns of events** – For example, tracing a hacker's steps over time.
4. **Connect attacker and victim computers** – See which computer sent a virus.
5. **Track full sequence of events** – Understand how a security breach happened.
6. **Recover hidden or deleted data** – Bring back files that are hidden or erased.

**Example:**
In an online fraud case, forensic experts can show **exactly how the hacker stole money**, from start to finish, even if the hacker tried to hide the evidence.

---

Digital forensics deals with investigating **all kinds of digital crimes and misuse**. Some common situations are:

- **Abuse of internet by employees** – e.g., using office computers for personal work or illegal activities.
- **Unauthorized disclosure of corporate information** – e.g., leaking company secrets.
- **Corporate spying** – stealing confidential data from competitors.
- **Damage assessment after an incident** – e.g., checking how much damage a hacker caused.
- **Criminal fraud or misleading cases** – e.g., online scams or fake transactions.
- **Other criminal cases** – like cyberstalking or identity theft.
- **Copyright violations** – e.g., illegal copying or sharing of software, movies, or music.

**Example:**
If an employee sends company secrets to a competitor, digital forensics can find **emails, hidden files, or history logs** to prove it.

---

### *Digital Forensics Tools and Data*

Forensic tools can examine many types of digital data:

- **Data Cluster** – small blocks of data on a hard drive.
- **Temporary Files** – files created by programs for short-term use.
- **Formatted Files and File Systems** – old or erased files.
- **Hidden Files** – files that are invisible in normal view.
- **History Files** – e.g., web browser history.
- **Unallocated Space** – free space on a drive that may contain deleted files.
- **File Stack** – collection of related files.
- **File Allocation Table Information** – how files are stored on the hard drive.

**Uses of Digital Forensics:**

1. Verify other evidence.
2. Generate new leads for investigation.
3. Help confirm or eliminate assumptions about a crime.

**Example:**
In an online fraud case, digital forensics can trace deleted emails and recover hidden transactions to show what really happened.

---

## 5.4 The Need for Computer Forensics

- Computers and ICT are everywhere, giving us many benefits.
- But modern technology can also be **misused for crimes**, like hacking, stealing data, or spreading viruses.
- This creates a **threat for individuals, businesses, and organizations**.

**Example:**
A hacker can break into a company system to steal customer data. Computer forensics is needed to **investigate, find the hacker, and prevent future attacks**.

---

Cyber Forensics is about investigating crimes involving computers and digital devices. Two main reasons it is important:

1. Law enforcement increasingly relies on **digital evidence**.
2. Computers are everywhere, from big systems to tiny microdevices.

**Challenges for forensic investigators:**

- Storage devices are getting **smaller and more advanced**: external hard drives, SSDs, pen drives, and even tiny memory chips. This makes finding evidence harder.
- Forensic tools/software help to **extract relevant data** from these devices, even when capacities are huge (GB, TB, PB, EB).
- Digital evidence includes anything that can **prove the truth of a crime** in court.
- Handling evidence carefully is crucial to **avoid tampering**.

**Chain of Custody:**

- A record of who **collected, transferred, and analyzed evidence**.
- Ensures that evidence is **authentic and related to the alleged crime**.
- Evidence must be stored **safely** and documented **chronologically** for legal purposes.

**Example:**
If a hacker steals customer data from a company, investigators must show **how they collected the hard drives, who handled them, and what was found**, so the evidence is accepted in court.

---

## 5.5 Cyber Forensics and Digital Evidence

Cyber Forensics has **two main areas**:

1. **Computer Forensic:** Investigating crimes on computers and storage devices.
2. **Network Forensic:** Investigating crimes over networks like the internet or company LAN.

**Why network forensic matters:**

- Many crimes happen online (hacking, phishing, data leaks).
- Network forensic studies **network traffic** to find who did what and protect users from exploitation.

**Difference between physical and digital evidence:**

- Physical evidence: tangible items (like fingerprints, documents).
- Digital evidence: data stored electronically (emails, files, logs).
- Each has its own rules and handling requirements in court.

**Example:**

- Physical: A broken laptop found at a crime scene.
- Digital: The files and browsing history on that laptop used to prove a cybercrime.

---

## 5.5 Cyber Forensics

Digital evidence is **fragile and easy to change**, but **copies can be made** without harming the original. Cyber forensic experts handle and maintain this evidence carefully.

**Digital evidence can include:**

- Emails, chats, letters, memos, files, spreadsheets
- Hidden or deleted files, passwords, login IDs, encrypted files
- Data stored in standard directories, hidden partitions, or temporary files

**Sources of Digital Evidence:**

1. **Logical File Systems:** File system, RAM, and storage media
2. **User-Created Files:** Documents, audio/video, email, bookmarks, calendars, databases
3. **System-Created Files:** Backups, cookies, configuration files, log files, swap files, temporary files
4. **Computer Networks:** Four layers – application, transport, network, data link

**Example:**
If someone hacks a company computer, forensic experts can recover deleted emails or encrypted files to see what was stolen.

---

## 5.5.1 The Rule of Evidence

- Indian Evidence Act (1872): Evidence can be **oral** (spoken) or **documentary** (written).
- Indian IT Act: **Electronic evidence** is now recognized as a legal type of evidence.

**Contexts of Digital Evidence:**

1. **Physical:** Exists on a physical medium (hard drive, USB)
2. **Logical:** Its location or structure in the system
3. **Legal:** Must be interpreted correctly to have meaning in court

**Guidelines for Collecting Digital Evidence:**

1. Follow security policies and involve law enforcement if needed
2. Take accurate pictures or documentation of the system
3. Record all information with **date and time**
4. Note differences between system clock and real-world time
5. Be ready to testify and explain all actions step by step
6. **Minimize changes to the data** while collecting it.
7. **Remove external ways** that could accidentally change the data.
8. **Collect first, analyze later** – never analyze live data before making a copy.
9. **Use implementable procedures** – the steps must be practical and reproducible.
10. **Follow a systematic approach** for every piece of evidence.
11. **Collect volatile data first**, then less volatile data:
    1. **Volatile:** Registers, cache, process table, memory (RAM)
    2. **Less volatile:** Disk storage, network topology, archives
12. **Make a bit-level copy** of storage media to preserve original evidence.

**Path of Digital Evidence:**

- **Physical Context:** Media → Data → Information → Evidence
- **Logical Context:** Data → Information → Evidence
- **Legal Context:** Information → Evidence

**Example:**
If a hacker deletes files from a computer, the forensic expert first makes a **bit-level copy** of the hard drive before analyzing it. This prevents the original data from being changed.

---

## 5.6 Forensic Analysis of Email

Emails are often used in cybercrimes, sometimes **faked or forged**. Cyber forensic analysis can determine if an email is authentic.

**Key points to know for email analysis:**

1. **Email Components:** Subject, sender, receiver, body, attachments
2. **Email Header Structure:** Contains metadata like timestamps, sender IP, routing info

**Email System Components:**

- **Email Server:** Computers that **send, receive, store, and forward emails**
- **Email Gateway:** Acts as the **connection between servers** and controls the flow of emails

**Example:**
If someone sends a fake threatening email, forensic analysis of the **email header** can reveal the original sender's IP address, server route, and whether it was forged.

---

### Cyber Forensics – Email Analysis

Emails are important pieces of **digital evidence** in cybercrime investigations. Each email has **two main parts**:

1. **Header** – Contains technical information about the email's journey from sender to receiver.
2. **Body** – Contains the actual message content.

---

### Why the Header is Important

- The **header shows the entire path** the email took to reach the recipient.
- It includes details like:
    - **Sender's IP address**
    - **Email servers it passed through**
    - **Authentication results** (like SPF, DKIM)
- Investigators use the header to **verify the sender, detect forgery, or trace the origin of the email**.

**Example:**
If someone sends a threatening or fake email, forensic experts can use the header to trace the sender's IP address and see which servers were involved. This can help identify the culprit.

- Following is the **E-mail header example**:

Received: from 10.197.39.76 by atlall08.free.mail.bfi.yahoo.com with HTTPS; Wed, 4 Aug 2021 10:20:52 +0000
Return-Path: <bounces+1298689-ed92 nimbalkar=yahoo.com@em6154.manadesigner.com>
X-Originating-IP: [167.89.52.239]
Received-SPF: pass (domain of em6154.manadesigner.com designates 167.89.52.239 as permitted sender)
Authentication-Results: atlall08.free.mail.bfi.yahoo.com; dkim=pass header.i=@manadesigner.com header.s=s1
X-Apparently-To: nimbalkar@yahoo.com; Wed, 4 Aug 2021 10:20:52 +0000
X-YMailISG: DTFRRWAWLD5B.90JJT79WMLgjRLEOkkYeXcAEX47zS6hEX3n.
Received: from 167.89.52.239 (EHLO o1678952x239.outbound-mail.sendgrid.net) by 10.197.39.76 with SMTPs (version=TLS1_2 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256); Wed, 04 Aug 2021 10:20:52 +0000
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=manadesigner.com; m-content-Type: from:subject:content-transfer-encoding:mime-version:reply-to:to;
Received: by filterdrecv-7d5fff68cf-m64np with SMTP id filterdrecv- 7d5fff68cf-m64np-1-610A6A02-70
Received: from [127.0.0.1] (unknown)
Content-Type: text/html; charset=us-ascii
From: Brainovision <it@brainovision.in>
Subject: MoU proposal...
Message-ID: <c2c84e89-4622-c547-96bd-c63120eeb869@brainovision.in>
Content-Transfer-Encoding: quoted-printable
Date: Wed, 04 Aug 2021 10:20:50 +0000 (UTC)
MIME-Version: 1.0
Reply-To: it@brainovision.in
To: nimbalkar@yahoo.com
X-Entity-ID: Y3EjUeVTYEeTaew5rnSLxFA==
Content-Length: 8487
<Body>
[You can get above email header details from yahoo, open your Email click on triple dots, select "View raw message"; for Gmail click on triple dots and click on "Show original"]

The **main purpose of an email header** is to provide information about:

- **Sender and recipient**
- **Email route (path)**
- **Preventing spam and phishing**

All the lines **from the start of the email to the `<body>` tag** make up the header.

---

## Six Main Points in an Email Header

### *1) "Received:" Lines*

- Show the **IP addresses of the servers** the email passed through.
- Cannot be easily forged, so they are very reliable.
- **Received By:** Shows details of the **last SMTP server** that handled the email, including:
  - Server's IP address
  - SMTP-ID of the server
  - Date and time the email was received
- **Received From:** Shows the **sender's IP address, host name, and timestamp**.
- **Example:** You can trace where an email originated by reading these lines.

---

### *2) MIME-Version*

- Stands for **Multipurpose Internet Mail Extensions**.
- Supports **attachments** like audio, video, or multiple-part messages.
- **Example:** An email with a PDF attachment uses MIME to carry the file.

---

### *3) Message-ID*

- A **globally unique identifier** for every email.
- No two emails have the same Message-ID.
- **Example:** This helps forensic experts identify a specific email among thousands.

---

### *4) DKIM Signatures*

- Stands for **Domain Key Identified Mail**.
- Confirms that the **email really came from the claimed domain**.
- Helps prevent **spam and phishing**.
- **Key DKIM fields:**
  - `v` → Version (always 1)
  - `a` → Encryption algorithm (usually RSA-SHA256)
  - `c` → Canonicalization method

- **s (Selector):** Record name used with the domain
- **h (Signed headers):** List of headers used in the signing algorithm
- **bh:** Hash of the email body
- **b:** Hash of the headers listed in `h` (the **DKIM signature**)
- **d (Domain):** Domain used with the selector record

All these tags are **required** for DKIM verification. Missing tags may cause errors.

#### *Other Important Header Fields*

- **Return Path:** Email address where undelivered messages are returned.
- **Received-SPF:**
  - SPF (Sender Policy Framework) verifies the sender's domain.
  - Helps ensure the email is not forged.
- **Authentication-Results:**
  - Shows which authentication checks were performed by mail servers.
  - Includes results of SPF, DKIM, and other techniques.
- **CC / BCC:**
  - **CC:** Carbon copy – recipients can see who else got the email
  - **BCC:** Blind carbon copy – recipients cannot see other BCC addresses

**Example:**
If an email claims to be from a bank, SPF and DKIM tags help forensic experts confirm that it **actually came from the bank's server**.

---

## Role of Internet Service Provider (ISP)

- Once the sender's **IP address** is found, investigators can contact the ISP.
- ISPs provide details like:
  - Subscriber's name, address, and contact info
  - Location and type of IP address
  - Connection details at a specific date and time

**Example:**
Tracing a hacker's IP through the ISP can reveal the **location and account used** to send fraudulent emails.

---

## 5.6.1 RFC 2822 – Email Standard

- RFC 2822 defines the **standard format for emails** on the internet.
- Valid email addresses can include unusual formats like:
  - `Patil@host.net`

    - `Akash@10.0.0.3_19]`
    - `_Kadam@host.net`
- Many online email validators **fail to recognize some valid formats**, so forensic experts rely on RFC 2822 standards.

- **RFC 2822** defines the **internet message format** and some rules about email content, but it **does not cover envelope information** (like routing details).
- Each email must have a **globally unique Message-ID**.
- The **Message-ID** can appear in three header fields:
    1. **Message-ID** header
    2. **In-Reply-To** header
    3. **Reference** header
- Only **legitimate emails** can usually be traced for authentication. Spam or fake emails may not be fully traceable.
- **Note:** Email headers cannot always be trusted; they can sometimes be forged.

**Example:**
Even if an email looks like it comes from a bank, the Message-ID and other header fields must be checked to verify its authenticity.

---

## 5.7 Digital Forensics Life Cycle

According to the **FBI**:

- Digital evidence is present in **almost every crime scene**.
- Law enforcement must know how to:
    - **Identify** digital evidence
    - **Seize** and **transport** it
    - **Store** it safely
    - **Preserve** it for forensic examination

**Rules for Evidence:** Must be **admissible, authentic, complete, reliable, understandable, and believable**.

---

## 5.7.1 The Digital Forensics Process

1. **Exhibit:** Digital evidence is presented in court to help the jury understand the facts.
2. **Testimony:** Experts explain **how the evidence was collected, preserved, and analyzed**.
3. **Admissibility:** Parties must prove that the evidence is **related, authentic, and not hearsay**.
4. **Chain of Custody:** Everyone handling evidence must testify about how it was **controlled and transferred**.

5. **Tools and Methodology:** Forensic experts use **scientific tools and methods** to extract and analyze evidence reliably.

**Example:**
In a hacking case, forensic experts can show:

- How a hard drive was copied (bit-level copy)
- How deleted files were recovered
- How evidence was preserved without alteration
- All steps documented in the chain of custody

---

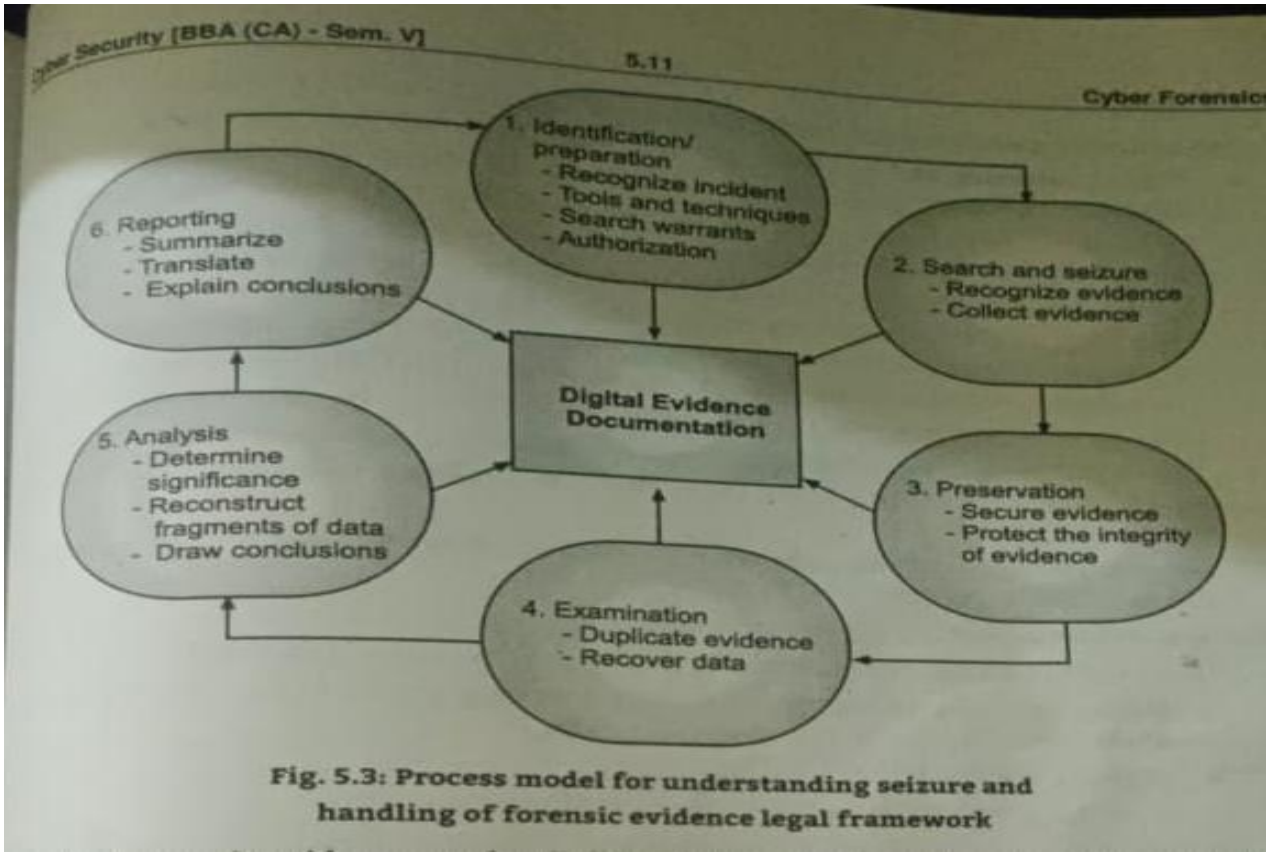


**Fig. 5.3: Process model for understanding seizure and handling of forensic evidence legal framework**

## Digital Forensic Evidence Challenges

- Digital evidence can be **challenged** by proving issues with:
  - **Intent or accident**
  - **Content, context, meaning**
  - **Timing, location, relationships**
  - **Corroboration**
- This can produce **false positives** (wrongly accused) or **false negatives** (missed evidence).
- **Trained forensic examiners** follow strict protocols to ensure:

- **Authenticity**
- **Chain of custody**

## 5.7.2 Phases in Computer/Digital Forensics

The **forensic life cycle** consists of several key phases:

---

### *1. Preparation and Identification of Digital Evidence*

- Evidence must be **identified first**; otherwise, it may never be collected.
- Identify evidence by looking at **sequences of events on a device**—files, file systems, logs, etc.
- **Example:** A deleted email or hidden file may be relevant evidence.

---

### *2. Collection and Recording of Digital Evidence*

- Sources: computers, USB drives, cell phones, cameras, hard drives, memory sticks, black boxes in cars, RFID tags, digital thermometers, web pages, etc.
- **Volatile data** (like RAM) must be collected carefully because it disappears when power is off.
- **Non-volatile memory**: USB sticks, SD cards, cell phones, SSDs
- **Computer memory types:** ROM, PROM, EPROM, EEPROM
- **Important:** Use **cryptographic hash functions** to detect any change in evidence.

**Example:**
When collecting a USB drive from a suspect, create a **bit-level copy** and use a hash to confirm the copy matches the original.

---

### *3. Storing and Transporting Digital Evidence*

- **Best practices:**
    1. Use **write-blocking tools** to prevent changes to the original media.
    2. Maintain **chain of custody**.
    3. Document every step carefully.
    4. Use **validated tools and methods**.
- Store media properly to avoid **damage from humidity or temperature**.
- For transportation, make **exact bit-level duplicates (clones)** to prevent spoliation.
- Ensure a witness can **testify about the handling and transport**.

**Example:**
A hard drive collected from a crime scene is cloned, documented, and stored in a secure evidence locker to prevent tampering.

---

### *4. Examining or Investigating Digital Evidence*

- Only **authorized forensic experts** can examine evidence.
- Two types of analysis:
    1. **Dead analysis** – analyzing data on a copied device
    2. **Live analysis** – analyzing data on a running system

**Example:**
If a suspect's computer is running, live analysis may help recover active network connections or running malware.

**Dead Analysis:**

- Performed on a **copied image** of the media (like a hard disk).
- The original media remains **untouched**.
- Hashing algorithms like **SHA-1** and **MD5** are used to **verify integrity**.

**Live Analysis:**

- Performed on a **running system**.
- Important when attackers exploit **data in RAM**.
- Evidence must be collected **before powering off** the machine.

---

## 5. Analysis, Interpretation, and Attribution

Digital evidence can come in many formats. Types of forensic analysis include:

1. **Media Analysis** – Reviewing storage devices
2. **Media Management Analysis** – Managing and categorizing evidence
3. **File System Analysis** – Checking folder structures and deleted files
4. **Application Analysis** – Investigating apps like email clients or browsers
5. **Network Analysis** – Tracing network activity and logs
6. **Image Analysis** – Analyzing photos or graphics
7. **Video Analysis** – Examining videos for evidence

**Forensic Tools:**

- Commercial: **AccessData FTK, Brain Carrier's Sleuth Kit**

- Open Source: Tools to scan **RAM, registry, and recently accessed web-based emails**

**Example:**
Reviewing the Windows Registry can show **recently accessed files, emails, or browser activity**.

---

## 6. Reporting

- After analysis, a **report is generated**: written, oral, or both.
- Reports summarize:
    - Evidence collected
    - Analysis and interpretation
    - Conclusions and attribution

**Key Elements of a Forensic Report:**

- Reporting agency and case identifier
- Investigator and submitter details
- Date of receipt and report
- Detailed list of items examined (serial numbers, make, model)
- Examiner's identity and signature
- Steps taken during analysis (e.g., file recovery, image searches)
- Final conclusion

**Audience:**

- Law enforcement, technical experts, legal experts, corporate management, or court.

---

## 7. Testifying

- **Testifying** means presenting digital forensic evidence in court.
- Only **qualified expert witnesses** can give opinions on technical or scientific matters.
- Requirements for expert testimony:
    - Based on **sufficient facts or data**
    - Uses **reliable principles and methods**
    - Applies those methods reliably to the case

**Example:**
An expert can explain how a deleted email was recovered and prove it is genuine.

---

### 5.7.3 Precautions When Collecting Electronic Evidence

- Ensure **chain of custody** is maintained.
- Do **not alter original data** during collection.
- If original data must be accessed, the investigator must:
  - Be competent
  - Explain relevance of evidence
- Integrity of digital evidence is critical for **court admissibility**.

**Example:**
A USB drive from a crime scene should be copied with a **write-blocker**, documented, and stored securely without altering the original.

- An **audit trail** must be maintained to record all processes applied to electronic evidence.
- The **investigation in charge** is responsible for ensuring that **laws and forensic principles** are strictly followed.

---

## 5.8 Challenges in Computer Forensics

Digital forensics is **not an easy task** due to:

1. **Huge Volume of Data**
   - Computers may have hundreds of GBs of storage.
   - Billions of emails, documents, and web pages exist online.
   - Finding **relevant evidence** is like looking for a **needle in a haystack**.
2. **Data Collection**
   - Investigators must collect **specific, case-related information** from vast amounts of data.
   - Existing tools can **alter data attributes**, so accuracy is a concern.
3. **Text Mining and Data Mining**
   - Techniques like **text mining** help sift through massive datasets efficiently.
4. **Network Forensics Challenges**
   - Networks operate across **time zones and jurisdictions**, requiring **trusted timestamps**.
   - Real-time and offline data collection is complex and may involve **permissions, privileges, and avoiding server damage**.

---

### 5.8.1 Technical Challenges: Raw Data Complexity & Quantity

1. **Complexity Problem**
   - Digital evidence is often acquired in its **raw format**.
   - Non-technical people may struggle to understand the data.

2. **Quantity Problem**
    - The sheer **volume of data** makes analysis difficult.
    - **Data reduction** is used to:
        - Group related data into a **larger event**
        - Remove **known or irrelevant data**

---

## 5.16 Cyber Forensics – Data Abstraction and File Systems

- Goal: Present **digital data accurately** at the right layer of abstraction.
- **ASCII layer:** Converts numeric values into readable characters (letters, numbers, symbols).
- **FAT File System Layers (7 layers of abstraction):**

  Layer 0 : Raw file system image

  Layer 1 : File system image + Boot Sector + FAT Entry Size

  Layer 2 : FAT Area + Data Area

  Layer 3 : Starting Cluster + FAT Entries

  Layer 4 : Clusters + Raw Cluster Content + Content Type

  Layer 5 : Formatted Cluster Content

  Layer 6 : List of Clusters

**Example:**
A forensic tool can use these layers to **reconstruct deleted files** or view raw disk content.

---

## 5.8.2 Legal Challenges & Data Privacy Issues

- **Digital evidence** is easily **copied, altered, or deleted**, sometimes leaving no trace.
- Challenges include:
    - Locating relevant evidence in huge data volumes
    - Ensuring **legal admissibility** in court
    - Dealing with **constitutional, statutory, and procedural limitations**
- Forensic investigators must:
    - Use **special tools and techniques** to capture evidence accurately
    - Determine if a **search warrant** is required before seizing computers or hardware

**Example:**
Copying a hard drive without following proper legal procedures may render the evidence **inadmissible in court**.

---