Digital Forensics Introduction:

The definition of digital forensics has evolved from basic computer evidence analysis to a broader application of computer science and investigative procedures for legal purposes.

digital forensics as the application of science and procedures for analyzing digital evidence for legal purposes, ensuring proper chain of custody, mathematical validation (hash functions), repeatability, and expert reporting.

Digital Forensics and Other Related Disciplines

Digital forensics is about examining and analyzing data from digital devices, like computers or phones, to use as evidence in legal cases.

Key Tasks in Digital Forensics:

- **Collecting Data**: Securely retrieving information from computers or storage devices.
- **Examining Data**: Analyzing the content to find details like origin and purpose.
- **Presenting Data**: Sharing findings in court as evidence.
- **Applying Laws**: Ensuring digital investigations follow legal rules.

Types of Evidence

1. Inculpatory Evidence (Incriminating)

- This type of evidence supports the case against the suspect.
- **Example**: The recovered logs show that the hacker used stolen employee credentials to log in.

2. Exculpatory Evidence (Clearing)

- This type of evidence proves the suspect is innocent.
- **Example**: Suppose an employee is accused of sharing customer data. The forensics team finds that their credentials were stolen and used by someone else, clearing the employee's name.

Digital Forensics vs. Data Recovery

- **Digital forensics**: Focuses on finding *intentionally hidden* or *deleted* evidence to support legal cases.
    - **Example**: The hacker hid malicious software (malware) in the system. Investigators uncover this software and confirm it was used to steal data.
- **Data recovery**: Focuses on retrieving accidentally lost data (e.g., files lost during a power outage).
    - **Example**: A worker accidentally deletes an important presentation, and data recovery experts retrieve it.

Network Forensics

Focus: This part involves analyzing the network to track how the hacker got in and what they did.

- **Example**:
  - Investigators review the firewall logs and notice a large number of failed login attempts followed by a successful one at 2:00 AM.
  - They trace the login back to an IP address from a foreign country.
  - Further analysis shows the hacker copied customer data and attempted to upload it to an external server.

Challenges in Investigating Digital Devices

1. **Uncertainty in Data**:
   - Investigators often have no idea what data they'll find. They must carefully search for clues, as digital evidence is not always obvious.
   - **Example**: A confiscated smartphone might contain encrypted files or hidden folders. Investigators need specialized tools to reveal and analyze this data.
2. **Recovering Damaged Data**:
   - When devices are damaged or intentionally reformatted, advanced tools or techniques (e.g., electron microscopes) are needed to recover data. However, these methods are expensive and only used in rare cases.

Let me simplify and explain these points with more detail and examples:

Challenges in Investigating Digital Devices

1. **Uncertainty in Data**:
   - Investigators often have no idea what data they'll find. They must carefully search for clues, as digital evidence is not always obvious.
   - **Example**: A confiscated smartphone might contain encrypted files or hidden folders. Investigators need specialized tools to reveal and analyze this data.
2. **Recovering Damaged Data**:
   - When devices are damaged or intentionally reformatted, advanced tools or techniques (e.g., electron microscopes) are needed to recover data. However, these methods are expensive and only used in rare cases.
   - **Example**: If a suspect smashes their hard drive to destroy evidence, forensic experts might use high-tech equipment to extract traces of data from the broken parts.

The Investigations Triad

Digital forensics is part of a broader process called the **Investigations Triad**, which includes three key functions:

1. **Vulnerability/Threat Assessment and Risk Management**:
   - Focuses on identifying and fixing weaknesses in systems and networks.
   - Includes **penetration testing** (ethical hacking) to simulate attacks and improve security.

- **Example**: A company hires a penetration tester to try hacking their network. The tester finds that employees are using weak passwords, so the company implements a stricter password policy.

2. **Network Intrusion (entry point) Detection and Incident Response**:
   - Detects unauthorized access or hacker attacks and responds to minimize damage.
   - Collects evidence for legal action against attackers.
   - **Example**: If hackers breach a university's network, this team finds out how they got in, blocks their access, and gathers logs to trace their activities.
3. **Digital Investigations**:
   - Handles cases involving digital evidence, such as identifying and recovering hidden, deleted, or tampered data.
   - **Example**: After an internal employee sends confidential data to a competitor, this team retrieves the email and proves their misconduct.

- **Forensics investigators often work as part of a team, known as the investigations triad**

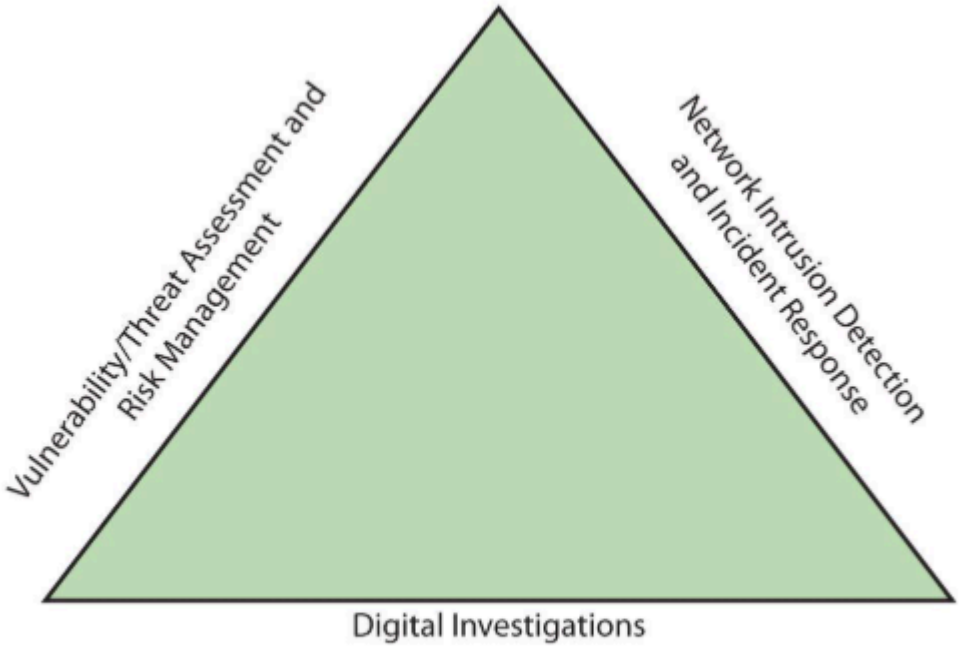

Figure 1-1 The investigations triad

A Brief History of Digital Forensics

1. Early Digital Crimes:

Fifty years ago, computers were rare and used only by professionals in specific fields like finance and engineering. As technology developed, people realized they could manipulate these systems for personal gain.

Example: The *One-Half Cent Crime*

Banks calculate interest for accounts down to fractions of a cent (e.g., 0.005 dollars). Since customers can't get fractions of a cent, banks round up or down, assuming everyone will benefit over time. However, some clever programmers wrote a program to collect all these fractions and deposit them

into their own secret accounts.

- Small Banks: Only a few hundred dollars per month would be stolen.
- Large Banks: This added up to hundreds of thousands of dollars because of millions of accounts.

Imagine stealing pennies from millions of people—it seems small, but it adds up to a fortune.

---

2. Early Challenges for Law Enforcement:

Back in the 1970s, most police officers didn't know much about computers. If a computer was involved in a crime, they didn't know:

- What questions to ask (e.g., "Where is the data stored?").
- How to preserve evidence (e.g., making sure digital data wasn't overwritten).

To address this, the Federal Law Enforcement Training Center (FLETC) started training officers in handling digital evidence.

3. Rise of Personal Computers (1980s):

By the 1980s, mainframe computers were replaced by personal computers (PCs) that anyone could use. Popular models included the Apple IIe, Commodore 64, and Macintosh. This era introduced new challenges:

- Each PC had different operating systems (OS) (e.g., MS-DOS, IBM-DOS, Apple's OS).
- Digital crimes became easier because people now had access to computers at home.

Forensic Tools of the Time:

Simple tools emerged to recover files and detect tampering.

- Xtree Gold: Identified file types and retrieved lost/deleted files.
- Norton DiskEdit: Helped recover deleted files on PCs.

---

4. Advances in Computer Storage (1987):

As computers improved, storage capacity grew. For example:

- The Mac SE introduced a 60 MB external hard disk, a huge improvement over floppy disks and audiotapes used by older models like the Commodore 64.

However, as hard disks grew in size, investigators faced a problem:

- Early forensic tools (designed for small hard drives) couldn't handle large storage devices.

5. Rise of Specialized Digital Forensics Tools (1990s):

The 1990s marked a turning point in digital forensics. Specialized tools and training programs became available to handle the growing complexity of computer crimes.

- Training:
    - The International Association of Computer Investigative Specialists (IACIS) began teaching investigators to use forensic software.
    - The IRS developed programs to search for digital evidence during raids.
- Software:
    - *Expert Witness* for Macintosh was one of the first commercial forensic tools to recover deleted files.

    - Later, tools like EnCase and AccessData Forensic Toolkit (FTK) became industry standards.

6. Continuous Evolution of Forensic Tools:

As technology advanced, new challenges emerged:

- Large hard disks (500 GB+): Older tools couldn't handle these sizes, so new tools had to be developed.
- Encrypted data: Modern criminals use encryption to hide their activities, requiring sophisticated tools to crack.

Forensic software is now produced by both government agencies and private companies. For example:

- ILook: Used by the IRS to analyze special disk files (limited to law enforcement).
- FTK: A commercial tool for civilians and law enforcement to examine digital evidence.

Case Law and Its Importance

- Definition: Case law refers to the decisions made by courts in previous legal cases, which guide legal practices in future cases.
- In common law systems (like the United States), case law helps clarify legal ambiguities and fills in gaps where statutes (written laws) might be outdated or don't cover new technology.
- Example: If the law doesn't have specific guidelines for the use of smartphones in investigations, courts may use past decisions to determine whether it's acceptable to search a smartphone found on a suspect.
- These decisions might shape the procedures law enforcement follows in future cases.

Why Case Law is Critical for Digital Forensics Investigators:

- Privacy Issues: As technology advances, privacy concerns arise. For example, should law enforcement be allowed to search someone's smartphone just because they were arrested?
- This is often debated in courts.
- If a person's smartphone is seized during an arrest, a digital forensics examiner needs to understand the legal boundaries of what can be searched.
- They should know if it's permissible to inspect the phone's data without violating the individual's privacy rights.

Developing Digital Forensics Resources

- Definition: To be an effective digital forensics investigator, you must be knowledgeable about different operating systems and computing platforms (e.g., Windows, Linux, macOS).
- It's also crucial to build a network with other professionals in the field for support and knowledge-sharing.
- Example: An investigator specializing in Windows may not know the commands needed to analyze data on a vintage operating system like CoCo DOS.
- In such cases, they would contact experts or user groups familiar with those systems for help.

How to Build Resources:

- Joining User Groups: Being part of a community, like the *Computer Technology Investigators Network* (CTIN) or *High Technology Crime Investigation Association*, allows investigators to share knowledge and stay up-to-date on new developments.
- Example Case: In the 1996 Pierce County case, an investigator was able to contact a user group to gain access to a rarely-used operating system (CoCo DOS) on a suspect's computer.
- With their help, the investigator was able to retrieve crucial evidence, such as a diary detailing years of illegal activities.

Preparing for Digital Investigations

- Categories of Investigations:
  - Public-Sector Investigations:
    - These involve government agencies (like the police) investigating crimes, including cybercrimes.
    - They must follow legal guidelines (e.g., the Fourth Amendment in the U.S. Constitution, which protects citizens against unreasonable search and seizure).
  - Private-Sector Investigations:
    - These typically focus on civil cases (like corporate espionage or policy violations) but may evolve into criminal cases.
    - These investigations still need to follow legal procedures, and the evidence can sometimes transition from civil to criminal use.
- Example: A public-sector investigation could involve a police department looking into cybercrimes, such as hacking or fraud. Meanwhile, a private-sector investigation could focus on a company discovering an employee's data theft, which might later become a criminal case.

Understanding Law Enforcement Agency Investigations

- Computer Crimes: In criminal investigations, computers are often tools used to commit other crimes, such as fraud or cyberstalking. Many states have specific laws now to handle digital crimes, such as the *Computer Fraud and Abuse Act* (CFAA) in the U.S., which makes unauthorized access to computers illegal.

Expanding Laws for Digital Crimes:

- State-Specific Laws: States have added language to existing laws, making it illegal to steal digital data. For example, Alabama's law includes language that criminalizes stealing data from a computer, akin to stealing physical property like a car or a purse.

The Role of Technology in Serious Crimes

- Example Case of Sexual Exploitation: The use of digital devices in crimes like child exploitation is becoming more common. For instance, perpetrators might store illicit content on computers, smartphones, or cloud services. Investigators can trace these digital footprints to build a case.
- Other Digital Crimes: Similarly, crimes like drug trafficking, car theft, and missing persons investigations often involve digital evidence. Criminals might store transaction records or other illegal activities on their computers and smartphones.

Legal Processes in Computer Investigations

The process for investigating potential criminal violations depends on

local customs,

legislative standards,

and **rules of evidence**.

Criminal cases typically follow three key stages:

- **Complaint:** Someone files a complaint, often involving evidence or witnessing an illegal act.
- **Investigation:** Specialists investigate the complaint, collect evidence, and collaborate with prosecutors to build a case.
- **Prosecution:** If sufficient evidence exists, the case proceeds to trial, where evidence is presented for a judge or jury to decide.

Criminal Investigation Process

- **Filing a Complaint:**
  - A witness or victim reports an illegal act to the police, alleging that a crime has been committed.
  - Police officers interview the complainant and file a crime report.
- **Investigative Decisions:**
  - Law enforcement processes the report and decides whether to start an investigation or log the information into a **police blotter**.
  - **Police blotters** (now electronic databases) record past crimes and help identify patterns, especially in repeated criminal behavior, such as high-technology crimes.
- **Involvement of Specialists:**
  - Not all police officers are computer experts. Some may only retrieve basic data, while others are trained in advanced forensics.
  - **ISO Standard 27037** categorizes specialists as:
    1. **Digital Evidence First Responder (DEFR):** Trained to secure and preserve digital evidence on-site.
    2. **Digital Evidence Specialist (DES):** Skilled in analyzing data and calling in additional experts when required.
- **Investigator's Role:**
  - Assess the scope of the case, including the device's OS, hardware, and connected peripherals.
  - Ensure necessary resources and tools are available for collecting and analyzing evidence.
  - Delegate tasks to specialists if needed.
  - After gathering evidence, hand it over to the prosecutor, presenting findings in a report.

Affidavits and Search Warrants

- **Search Warrants:**
  - A search warrant allows investigators to seize evidence legally. It is typically issued when there is sufficient cause.
  - The investigator, often with the help of a prosecutor, prepares an **affidavit** (a sworn statement supported by evidence).
  - The affidavit is submitted to a judge for approval, and once signed, the search warrant is executed.
- **Executing the Warrant:**
  - DEFRs collect evidence as specified in the warrant.
  - The evidence is then processed, analyzed, and presented during a court hearing or trial.
  - The judge or jury delivers a verdict, after which the judge renders a judgment.

Private-Sector Investigations

- **Nature of Private-Sector Investigations:**
  - In private companies, investigations often address **policy violations** and **litigation disputes** (e.g., wrongful termination).
  - Businesses aim to minimize operational disruptions and financial losses caused by investigations.
- **Types of Cases:**
  - Email harassment.
  - Gender and age discrimination.
  - White-collar crimes (e.g., embezzlement, data falsification, sabotage).
  - Industrial espionage (selling confidential company information to competitors).
- **Focus on Policies:**
  - Private organizations rely heavily on well-documented and enforceable policies to

guide internal investigations.
    - The most critical policy is the **acceptable use policy**, which outlines rules for using company computers and networks.
- **Key Points about Policies:**
    - Policies define who can initiate investigations, who can seize and access evidence, and how evidence should be handled.
    - Clear policies help businesses avoid litigation by showing they follow fair and due process.
    - Regular updates to policies are necessary to ensure compliance with changing laws.

Reducing Risk Through Policies and Training

- Organizations should:
    - Create policies that employees can easily understand and follow.
    - Require employees to sign an **acceptable use agreement** to acknowledge their responsibilities.
    - Schedule regular training to educate employees on policy updates and proper usage of company systems.
- **Line of authority** - states who has the legal right to initiate an investigation, who can take possession of evidence, and who can have access to evidence
- **Benefits of Policies:**
    - Facilitate smoother investigations.
    - Demonstrate fairness and due process.
    - Protect organizations from lawsuits by employees.

- Business can avoid litigation by displaying a **warning banner** on computer screens
    - Informs end users that the organization reserves the right to inspect computer systems and network traffic at will

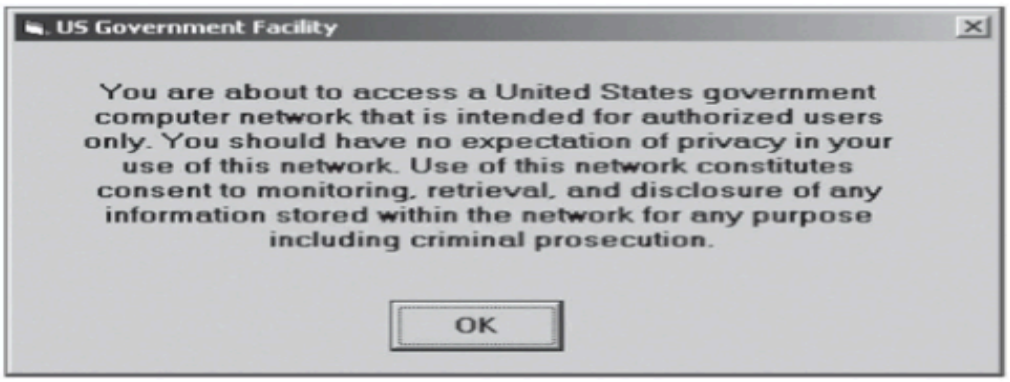

Figure 1-7 A sample warning banner

Establishing Authority in Investigations

- A company should clearly define who has the authority to request investigations.
  This avoids unnecessary or improper investigations caused by personal conflicts between departments.
- Without clear rules, some employees might misuse the system, like falsely accusing others to stop competing projects or funding requests.
- **How to do it?**
  Limit the number of people or groups who can authorize investigations, like:
  - Corporate Security
  - Ethics Office
  - Internal Auditing
  - Legal Department
- **Example:**
  If an employee is suspected of misusing company data, only the corporate security team or legal department can authorize an investigation, ensuring the process is fair and professional.

Investigating in Private vs. Public Sector

- **Private Sector:**
  Investigations focus on violations of company policies (e.g., email misuse, internet abuse).
- **Public Sector:**
  Investigations focus on crimes (e.g., hacking, fraud).
- **Similarities:**
  Both types involve collecting and preserving evidence that may be used in court.

Common Issues in Private Investigations

- **Misuse of Digital Assets:**
  Employees using company resources for personal gain.
  Example: Using company software to create a product and sell it for personal profit.
- **Email Abuse:**
  Employees sending inappropriate or threatening messages.
  Example: A worker sends offensive emails that create a hostile work environment.
- **Internet Abuse:**
  Employees spending too much time browsing or viewing inappropriate content.
  Example: An employee spends hours on social media or views illegal content like contraband images.

Handling Evidence and Legal Considerations

- **Preserve Evidence:**
  Always handle evidence with care, as civil investigations can turn into criminal cases.
- **Follow the Law:**
  If evidence points to a crime (e.g., theft of data), notify law enforcement. Once police take over, private investigators must follow strict rules for search and seizure.
- **Example:**
  If a company finds illegal images on an employee's computer, they must inform the police and stop their investigation, as this is now a criminal matter.

Distinguishing Personal vs Company Property

- With BYOD (Bring Your Own Device), personal devices (phones, tablets) often connect to company networks, leading to a mix of personal and work-related data.
- **Key Questions:**
  - If an employee connects their personal tablet to the company network, does the company own the data on the tablet?
  - If the company gave an employee a tablet as a gift, can the company still control it?

- **Policies to Address BYOD Issues:**
  Some companies state that **any personal device connected to the network is treated as company property.**
- **Example:**
  If an employee uses their phone to download sensitive company files, the company might investigate the device as part of its property.

Role of Digital Investigators

- **Goal:**
  Digital investigators help management by providing accurate evidence to address issues like policy violations or criminal acts.
- **Steps:**
  - Collect evidence.
  - Maintain a proper chain of custody to ensure evidence is admissible in court.
- **Example:**
  A digital investigator finds that an employee has been leaking confidential company data through email. The evidence is securely handed over to management or law enforcement.

Importance of Consistency and Professionalism

- Investigators must **follow the same rules** for all cases, whether civil or criminal.
- **Consistency** ensures evidence is admissible in court and reduces liability risks for the company.
- **Example:**
  If an employee sues for wrongful termination, the company can show the investigation followed fair policies.

Professional Conduct in Digital Forensics

Your professional conduct as a digital investigator directly affects your credibility and reputation.

To uphold high standards, you must focus on three critical areas: objectivity, confidentiality, and professional growth.

Objectivity

- **Definition**: Objectivity means forming conclusions strictly based on evidence, education, training, and experience.
- **Application**: Avoid biases or prejudices during investigations. For example:
  - If working for an attorney, do not let their legal agenda influence your findings.
  - Base your opinions solely on the data uncovered during your investigation, not assumptions or external pressure.
- **Key Principle**: Do not jump to conclusions. Exhaust all reasonable leads before finalizing your findings.

Why It's Important:

- A lack of objectivity could lead to invalid conclusions, damaging the investigation's credibility and potentially harming legal proceedings

Confidentiality

- **Definition**: Maintaining confidentiality involves discussing case details only with those who have a legitimate need to know.
- **Application**:
  - Share case information exclusively with authorized individuals, such as:
    - Investigators on the team.

        - The line of authority (e.g., supervisors or attorneys).
    - If consulting other professionals, share only general facts without revealing specific details.
    - Adhere to the **attorney-work-product rule** in legal investigations, which mandates discussing case details only with the attorney and authorized team members unless explicitly approved.
- **Example**:
    - In a private-sector case, leaking an employee's name or details of their termination could breach confidentiality agreements and expose the company to legal consequences.

Why It's Important:

- Breaching confidentiality can jeopardize investigations, compromise legal proceedings, and expose employers or investigators to lawsuits.

Continuous Learning and Professional Growth

Digital forensics is a rapidly evolving field. To remain effective, investigators must stay current with the latest tools, techniques, and legal requirements.

- **Training**:
    - Regularly attend workshops, conferences, and vendor courses to expand technical knowledge.
    - Learn advanced techniques for analyzing emerging technologies, including cloud systems, IoT devices, and encrypted systems.
- **Education**:
    - Obtain undergraduate or graduate degrees in relevant fields (e.g., computing, digital forensics, business law).
    - Pursue certifications (e.g., Certified Forensic Computer Examiner or EnCase Certified Examiner) to demonstrate specialized expertise.
- **Professional Organizations**:
    - Join organizations like the International Association of Computer Investigative Specialists (IACIS) or the High Technology Crime Investigation Association (HTCIA) for networking, resources, and training.
- **Example**: A company might fund employee education to ensure their investigators stay updated on advancements in hardware, software, and investigative methodologies.

Why It's Important:

- Keeping up with changes ensures you're capable of handling modern digital evidence and using the latest forensic tools effectively.

Integrity

- **Definition**: Integrity involves conducting investigations with honesty and upholding high ethical standards.
- **Application**:
    - Maintain professional behavior in all areas of life.
    - Avoid any conduct that could damage your credibility, such as tampering with evidence or exaggerating qualifications.

Why It's Important:

- A loss of integrity can lead to being discredited in court, invalidating your testimony and harming your reputation as an investigator.

Preparing for a Digital Forensics Investigation

Preparing for a digital investigation involves a structured approach to ensure accuracy, thoroughness, and compliance with legal standards.

1. Objectives

- **Primary Goal**: To determine whether evidence supports allegations of a crime or policy violation.
- **Secondary Goal**: To prepare a case for court or private-sector inquiry.

2. Case Preparation Steps

To prepare a digital investigation:

1. **Follow a Methodical Approach**:
    - Evaluate the evidence thoroughly.
    - Document the chain of custody to ensure evidence integrity.
    - **Chain Of Custody:** Route the evidence takes from the time you find it until the case is closed or goes to court
2. **Preserve Evidence**:
    - Store digital evidence on separate, secure devices to prevent alteration.
    - Conduct live acquisition if necessary to capture volatile data (e.g., RAM contents).

Case Scenarios

1. Computer Crime Example

Case Overview:

- **Scene**: Police raid a suspected drug dealer's home.
- **Evidence**:
    - Devices collected include a desktop computer, USB drives, a tablet, and a cell phone.
    - Investigators document the evidence with tags and photographs, including images of open windows on the desktop.

Investigation Process:

1. **Initial Documentation**:
    - Capture the scene by photographing open windows (e.g., File Explorer).
    - Perform a live acquisition to capture volatile data (e.g., RAM contents).
2. **Evidence Assessment**:
    - Analyze the hard drive and storage media for intact files, hidden files, and deleted data.
    - Use forensic tools such as Autopsy to identify emails, text messages, and other relevant data.
3. **Challenges**:
    - Prevent contamination of evidence (e.g., altering last access dates) through careful handling.
    - Address potential obstacles like encrypted files or damaged devices.
4. **Outcome**:
    - Identify evidence (e.g., drug contacts, photos) that supports the case.

Importance:

- Following proper procedures ensures evidence is admissible in court and maintains the investigation's integrity.

2. Company Policy Violation Example

Case Overview:

- **Incident**: A manager receives complaints about a sales representative's poor performance and unexplained absences.
- **Evidence**:
  - The IT department confiscates the employee's hard drive and storage media for analysis.

Investigation Process:

1. **Evidence Collection**:
   - Secure all devices in the employee's workspace.
   - Document the chain of custody.
2. **Analysis**:
   - Search for evidence of misconduct (e.g., excessive personal emails, unauthorized downloads).
   - Examine files for clues about the employee's behavior or whereabouts.
3. **Outcome**:
   - Identify whether the employee violated company policies (e.g., time theft, misuse of resources).

Importance:

- Protecting company assets and addressing policy violations promptly can prevent further damage.

Taking a Systematic Approach to Case Preparation

1. Initial Assessment

- **Determine the case type:** Understand the context by consulting involved parties. Questions to ask:
  - Has evidence (computers, disks, peripherals, etc.) already been seized?
  - Does the case involve criminal activity or evidence of another crime?
- Decide if you need to visit a location for evidence retrieval.

2. Preliminary Design

- **Outline investigation steps:** Decide how to acquire evidence, considering legal and practical constraints (e.g., seizing a computer during work hours vs. off-hours).
- For criminal cases, evaluate information already collected by law enforcement.

3. Checklist Creation

- **Develop a detailed checklist** of investigation steps with time estimates to maintain focus and organization.

4. Resource Determination

- Identify required software, hardware, tools, and expertise based on the operating system and complexity of the case.

5. Evidence Drive Copying

- If multiple media are involved (e.g., USB drives, mobile devices), create a **forensic copy** of the original media for analysis.

6. Risk Assessment

- **Identify risks:** For example, suspects may use password-protected hard drives or mechanisms that overwrite data during unauthorized logins.
- **Mitigate risks:** Prepare alternative approaches (e.g., making multiple copies of original media for redundancy).

7. Design Testing

- Verify your approach by comparing **hash values** to ensure accurate copying of original media.

8. Evidence Analysis

- Use forensic tools to extract digital evidence like deleted files, email records, or web history.

9. Investigation Report

- Write a thorough **case report** detailing procedures and findings.

10. Case Review

- **Critique your approach:** After the case, identify areas for improvement and ensure professional growth.

Case Assessment Example: George Montgomery

In this company-policy violation case:

- **Situation:** Employee abuse of resources.
- **Nature of Case:** George is suspected of using his work computer to run a side business.
- **Specifics:**
  - George reportedly registered domains and set up websites for clients during work hours.
  - Co-workers complained about poor work performance.
  - Company policy permits the inspection of company-owned digital assets.
- **Evidence:** A small USB drive using NTFS format.
- **Objective:** Confirm or deny George's involvement in the alleged misuse of company resources.

Planning the Investigation: Case "Montgomery_72018"

The investigation requires the following steps:

1. **Acquire Evidence:** Retrieve the USB drive from the IT Department.
2. **Document Evidence:** Complete a custody form and establish a **chain of custody** to ensure evidence integrity.
3. **Secure Evidence:** Place the USB drive in a locked, approved container in a digital forensics lab.
4. **Prepare Tools:** Set up a forensic workstation and gather required software.
5. **Forensic Copy:** Create and validate a copy of the evidence drive using hash values.
6. **Analyze the Data:** Extract and review all relevant digital evidence (files, deleted data, web activity).

Preserving Evidence Integrity

- **Key Rule:** Evidence should not be tampered with or contaminated.
- IT confirmed the USB drive had been securely stored since its retrieval.
- **Chain of Custody:** Essential for documenting who has handled evidence and when. Breaks in custody may compromise evidence admissibility.

Evidence Custody Form

An **evidence custody form** is a document that tells us what has been done with the original evidence and its forensics copies.
Also called a chain-of-evidence form.

A "single evidence form" refers to a document used to record details of only one piece of evidence in a case, while a "multiple evidence form" allows for the documentation of multiple pieces of evidence on a single form, providing a more comprehensive overview of all evidence gathered in an investigation

A custody form documents key details:

- **Case number:** Unique identifier.
- **Organization:** Name of investigating body.
- **Investigator:** Lead investigator handling the case.
- **Nature of the case:** Brief description (e.g., “employee resource abuse”).
- **Location:** Where evidence was collected.
- **Description:** Detailed notes about the evidence (e.g., “8 GB USB drive”).
- **Vendor/Model:** Manufacturer and serial numbers for precise identification.
- **Recovered by:** Name of the individual who initially recovered the evidence.

Standardized forms help maintain quality, prevent confusion, and ensure consistency in investigations.

COIN - LD - VR

Securing Evidence in Digital Investigations

Digital evidence can include:

1. **Flash drives** (small, portable storage devices)
2. **External hard drives** (larger storage devices that you can plug into a computer)
3. **Computer components** (like **CPUs**, **monitors**, and **printers**)

To **secure** these items properly, you'll use materials like:

4. **Evidence bags** (like plastic bags) to store and carry the items.
5. **Evidence tape** (to seal the evidence bags).
6. **Tags and labels** (to mark the evidence with important information, like date and location)

Preventing Damage to Digital Evidence

Digital evidence is very sensitive, and if you don't handle it properly, you could lose important data or make it unusable. Here’s how you can protect it:

7. **Avoid static electricity**:
    - Static electricity can **damage** computer components like hard drives and CPUs. To avoid this, you can use:
        i. **Antistatic bags**: These bags prevent static from damaging the device.
        ii. **Antistatic pads**: Place the equipment on these special pads when you're working with them.
        iii. **Wrist straps**: Wear a wrist strap that helps discharge any built-up static from your body safely.
8. **Use padded containers**:
   When you’re transporting computer parts (like hard drives or CPUs), put them in **well-padded** containers. This will protect them from physical shocks or drops.
    -

Certainly! Let me break this down for you in a more beginner-friendly way.

Adjusting Procedures for Evidence Types

When you're collecting **digital evidence** (like hard drives, USB flash drives, or computer parts), you need to be careful about how you handle these items, because they can be easily damaged. Digital evidence can include:

- **Flash drives** (small, portable storage devices)
- **External hard drives** (larger storage devices that you can plug into a computer)
- **Computer components** (like **CPUs**, **monitors**, and **printers**)

To **secure** these items properly, you'll use materials like:

- **Evidence bags** (like plastic bags) to store and carry the items.
- **Evidence tape** (to seal the bags and make sure no one tampered with the evidence).
- **Tags and labels** (to mark the evidence with important information, like date and location).

These materials can often be bought from places like **police suppliers** or regular **office supply vendors**.

Preventing Damage to Digital Evidence

Digital evidence is very sensitive, and if you don't handle it properly, you could lose important data or make it unusable. Here's how you can protect it:

1. **Avoid static electricity**:
    - Static electricity can **damage** computer components like hard drives and CPUs. To avoid this, you can use:
        - **Antistatic bags**: These bags prevent static from damaging the device.
        - **Antistatic pads**: Place the equipment on these special pads when you're working with them.
        - **Wrist straps**: Wear a wrist strap that helps discharge any built-up static from your body safely.
2. **Use padded containers**:
   When you're transporting computer parts (like hard drives or CPUs), put them in **well-padded** containers. This will protect them from physical shocks or drops.

Improvising Secure Containers

Sometimes, you might not have **ready-made** containers to secure the evidence, especially if it's large (like a computer or monitor). Here's what you can do:

- **Build your own containers**: If you don't have an evidence-specific container, you can use materials you have to create one. For example, you can use thick boxes or padded materials to create your own protective case.
- **Sealing openings**:
  For larger devices (like a computer), there may be **openings** (like where drives are inserted or power supply slots). You should seal these openings with **evidence tape** to make sure no one has tampered with the inside.
    - **Mark the tape** with your initials or a code, so you can tell if the tape was disturbed later.

9. **Transport and Storage Precautions**:
    - Maintain proper **temperature and humidity** during transport to prevent damage to

magnetic media.
    - Avoid exposing digital media to extreme conditions (e.g., heated car seats or electromagnetic interference from car radios).

Procedures for Private-Sector High-Tech Investigations

Employee Termination Cases

In cases where an **employee** is suspected of **misusing company resources** (like looking at inappropriate content or sending bad emails), there are common problems that could be investigated, such as:

- **Viewing pornography**
- **Sending inappropriate emails**

Internet Abuse Investigations

If someone is using the internet for **abuse** at work, like visiting harmful websites, the investigation will require the following materials:

- **Internet proxy server logs**: These are records showing what websites were visited and when.
- **IP address of the suspect's computer**: This helps to identify the specific computer used for the actions.
- **The suspect's computer's disk drive**: The storage where the computer's data is kept (important for forensic analysis).
- **Digital forensic tools**: Special software used to examine and recover data from devices.

Investigation Steps:

1. **Examine the disk drive**: Use forensic techniques to analyze the computer's hard drive for any evidence of internet abuse.
2. **Extract URLs**: Get the web pages that the person visited and any related data.
3. **Review proxy server logs**: Look at the logs from the internet proxy server and compare them with what you found on the suspect's computer.
4. **Analyze the data**: Look for **supporting evidence** to prove the abuse, or evidence that could **disprove** the allegations.

E-mail Abuse Investigations

Email abuse refers to using company emails for things like **spam**, sending **offensive content**, **harassment**, or even **threats**. Investigating email abuse requires the following materials:

- **Electronic copies of the emails**: These include the emails themselves, along with **email headers** (this information shows where the email came from, when it was sent, and other technical details).
- **Server logs or access to server data**: The logs contain information about email activities on the server, like which email was sent and when.
- **Digital forensic tools**: The same tools that help investigate other digital evidence can be used to analyze email data.

Steps for Investigation:

1. **Forensic analysis of emails**: Use forensic methods to dig into the email data to check for signs of abuse.
2. **Examine email headers**: These provide critical information, such as the sender's real location and whether the email was tampered with.
3. **Compare findings with server logs**: Cross-check what you find in the email headers and

content with the server logs to prove or disprove the claims.
4. **Follow laws**: Always consider **jurisdiction** (which laws apply to the case based on location) and **privacy laws** (how much personal information you can access legally) during the investigation.

Attorney-Client Privilege (ACP) Investigations

1. **Confidentiality and Authority**:
    - All findings are confidential, and the attorney (lawer) directs the investigation.
    - Investigators are responsible for extracting and reporting all relevant data.
    - Many attorneys like to have printouts of the data you have recovered.
    - You need to persuade and educate many attorneys on how digital evidence can be viewed electronically

Steps for Conducting ACP Investigations

1. **Obtain Formal Authorization:**
    - Before starting any investigation, you need a formal memo from the attorney authorizing the investigation. This ensures that the investigation is legally permitted and that you are not violating any privileges.
2. **Create Bit-Stream Images:**
    - Use two forensic tools to create bit-stream images (exact copies) of the data. The reason for using two tools is redundancy—it's a safety measure in case one tool fails.
3. **Verify Data Integrity:**
    - Check the hash values of the original drive and the bit-stream image to make sure the data hasn't been altered or tampered with. Hashing is a technique that provides a unique identifier for data, and if the hash values match, it confirms the data's integrity.
4. **Conduct Keyword Searches:**
    - You'll search through both allocated (used) and unallocated (free) disk space for important keywords. The unallocated space is where deleted data might still reside until it's overwritten by new data.

5. **Analyze Specialized Files**:

    - Some files, like **CAD drawings**, may require **special software** to open and analyze. Investigators need tools that can handle these types of complex files.

Important Considerations

- **Jurisdiction and Privacy Laws**:
    - Adhere to local, state, and international privacy laws.
    - Consult legal counsel to ensure compliance during investigations, especially when dealing with sensitive data (e.g., server logs).
- **Data Recovery Techniques**:
    - Recover unallocated data using forensic tools.
    - Use Registry analysis tools for investigating Windows systems.
    - Employ tools like **AccessData Registry Viewer** to extract relevant information from the Registry.