Emerging Issues in Computer Science

Week 9: Digital Forensics and Ethical Hacking

Lecturer: Ikwap Flavia Agatha

Lecture learning out come:

- At the end of this lecturer, you will be able to
- Understand computer forensics
- Understand the use of computer forensics in law enforcement
- Understand various forensics services
- Understand the types of computer forensics
- Understand the Computer forensics investigation process
- Understand the computer forensics tools
- Understand the evidence collection and data seizure
- Understand the types of digital evidence
- Understand Ethical Hacking
- Understand the application and limitations of digital forensics

What Is Computer Forensics?

- Computer forensics is the process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence.
- In other words, computer forensics is the collection, preservation, analysis, and presentation of computer-related evidence.

USE OF COMPUTER FORENSICS IN LAW ENFORCEMENT

- Computer forensics assists in Law Enforcement. This can include:
- Recovering deleted files such as documents, graphics, and photos.

Use Of Computer Forensics In Law Enforcement

- Searching unallocated space on the hard drive, places where an abundance of data often resides.
- Tracing artifacts, those tidbits of data left behind by the operating system.
- Processing hidden files — files that are not visible or accessible to the user. Often, this process requires reconstructing and analyzing the date codes for each file and determining when each file was created, last modified, last accessed and when deleted.
- Running a string-search for e-mail, when no e-mail client is obvious.

Digital forensic crime scene

- Safeguarding Crime Scenes: By The Help of Digital Forensics | by Abhishek sanjeev | Medium

Steps Taken By Computer Forensics Specialists

- The computer forensics specialist should take several careful steps to identify and attempt to retrieve possible evidence that may exist on a subject's computer system.
- Protect the subject computer system during the forensic examination from any possible alteration, damage, data corruption, or virus introduction.
- Discover all files on the subject system. This includes existing normal files, deleted yet remaining files, hidden files, password-protected files, and encrypted files
- Recover all of discovered deleted files.
- Reveal the contents of hidden files as well as temporary or swap files used by both the application programs and the operating system.
- Access the contents of protected or encrypted files.

Steps Taken By Computer Forensics Specialists

- Analyze all possibly relevant data found in special areas of a disk. This includes but is not limited to what is called unallocated space on a disk, as well as slack space in a file
- Print out an overall analysis of the subject computer system, as well as a listing of all possibly relevant files and discovered file data.
- Provide an opinion of the system layout; the file structures discovered; any discovered data and authorship information; any attempts to hide, delete, protect, and encrypt information; and anything else that has been discovered and appears to be relevant to the overall computer system examination.
- Provide expert consultation and/or testimony, as required.

Forensic Services Available

- Lost password and file recovery
- Location and retrieval of deleted and hidden files
- File and email decryption
- Email supervision and authentication
- Threatening email traced to source
- Identification of Internet activity
- Computer usage policy and supervision

Forensic Services Available

- Remote PC and network monitoring
- Tracking and location of stolen electronic files
- Honeypot sting operations
- Location and identity of unauthorized software users
- Theft recovery software for laptops and PCs
- Investigative and security software creation
- Protection from hackers and viruses.

Types of Computer Forensics

- File System Forensics: Focuses on examining data stored on physical media like hard drives or flash drives. Investigators analyze file systems (e.g., FAT, NTFS, EXT) to find hidden, misplaced, or suspicious files. Custom or unusual file systems may indicate illicit activities.
- Memory Forensics: Involves analyzing volatile memory (RAM, cache, processor registers) during a live system session. Since this data vanishes once the system is powered off, timely extraction is crucial.
- Operating System Forensics: Involves examining OS-specific data like logs and registries. Investigators must understand various systems (Windows, Linux, etc.) and how they store information differently to interpret logs accurately.

Types of Computer Forensics

- Multimedia Forensics: Targets non-text data such as images, audio, and video. It's useful for identifying pirated content, illegal imagery, or media recordings of crimes.
- Network Forensics: Focuses on monitoring and analyzing network traffic and communications. Investigators trace IPs, monitor data transfers, and study online behavior, including activity across social media or virtual networks.
- Database Forensics: Deals with investigating databases to uncover data misuse, unauthorized access, or deletion. Database structures can also reveal patterns of criminal activity.
- Malware Forensics: Involves detecting and reverse-engineering malicious software. Tools like goat files help track how malware behaves and affects other files.

Types of Computer Forensics

- Mobile Device Forensics: Covers smartphones, GPS devices, PDAs, and more. These devices run on diverse operating systems and store various data types (texts, photos, location history). Each model may require a unique approach to extract data.
- Email Forensics: Analyzes email content and metadata (e.g., headers, IPs) to detect phishing, forgery, or malware spread. Email headers are especially valuable for verifying authenticity.
- Firewall Forensics: Examines firewall logs to trace attempted or successful breaches. Logs provide details like access attempts, IP addresses, requested data, and more.
- Financial Forensics: Targets fraud and financial crimes. Investigators look for tampered transactions, altered metadata, or falsified records. Techniques include digital auditing, data mining, and reconciliation of records.

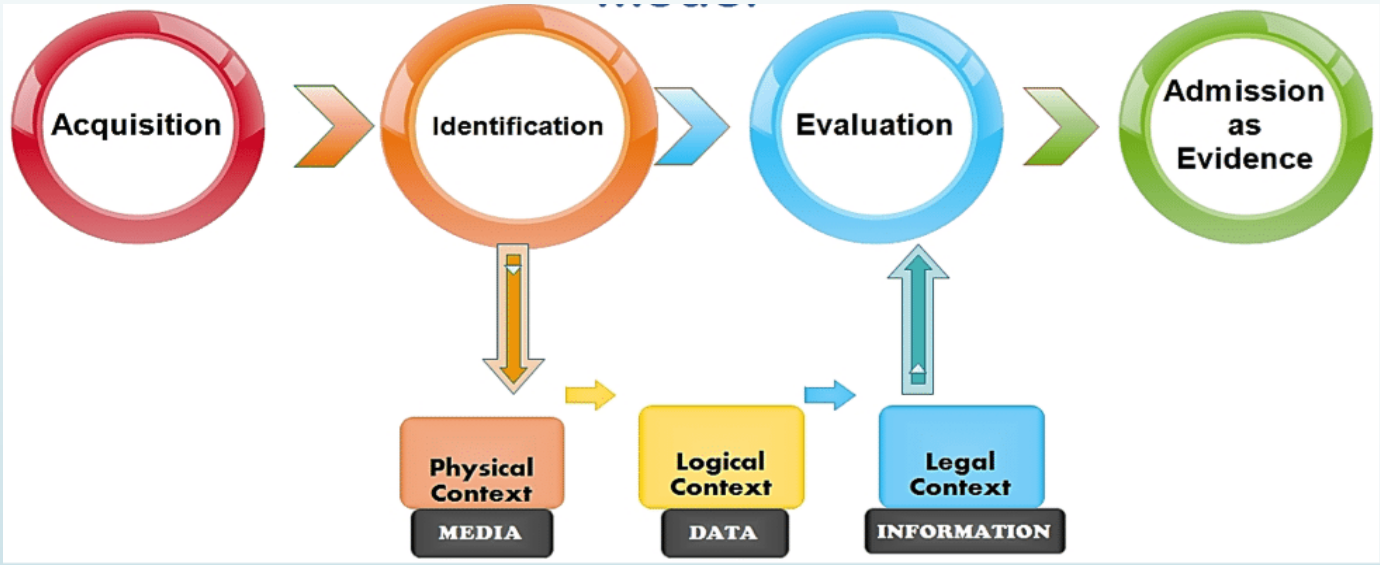
Computer Forensics Investigation Process

- The Acquisition phase involves collecting evidence in a lawful and standardized manner, typically with proper authorization from relevant authorities.
- Identification phase, where digital components are recognized from the collected data and translated into a format that is understandable to humans.
- Evaluation phase, these identified components are assessed to determine their relevance to the case and whether they qualify as valid evidence.
- Admission phase, the processed evidence is formally presented in a court of law.

Computer Forensics Investigation Process

- The Computer Forensics Investigation Process involves a systematic series of steps designed to gather, safeguard, examine, and present digital evidence in a way that complies with legal standards. Over the years, various models have been introduced to help investigators carry out this process efficiently and accurately. Below is an overview of the general process.

Computer Forensics Investigation Process



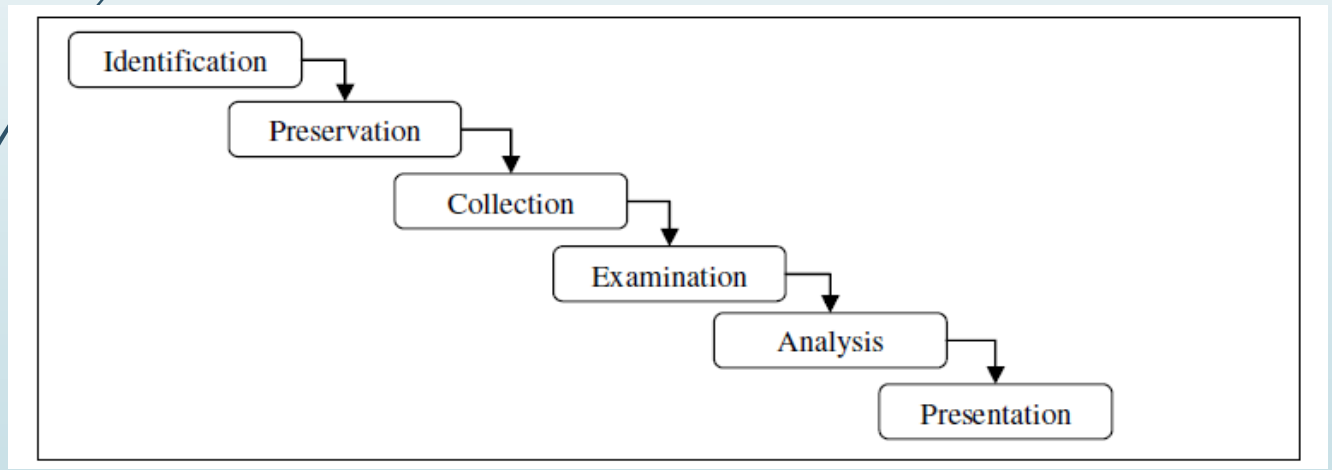
x.com/cfkassociates/status/1275410352658878464?lang=bg

DFRWS Investigative Model (2001)

- In 2001, the first Digital Forensics Research Workshop (DFRWS) introduced a general-purpose framework for conducting digital forensic investigations, which consists of six distinct phases.
- Identification phase, where activities such as profile detection, system monitoring, and audit analysis are carried out to recognize potential evidence.
- Preservation phase, which focuses on maintaining case integrity through proper case management and securing the chain of custody, ensuring the evidence remains unaltered.
- Collection phase, during which relevant data is gathered using approved procedures and various recovery techniques. This is followed by two key phases:

DFRWS Investigative Model (2001)

- Examination and Analysis. These stages involve processes such as evidence tracking, validation, recovering hidden or encrypted data, conducting data mining, and building timelines.
- Presentation, which involves preparing documentation and delivering expert testimony to clearly convey the findings in a legal context.



(Yusoff, 2011)

Computer Forensics Tools

- Computer forensics tools are critical for efficiently investigating and analyzing digital evidence. These tools allow forensic experts to collect, preserve, and analyze data from a variety of devices. Below are some of the main categories of computer forensics tools:

1. Disk Imaging Tools:

- These tools create exact copies of storage devices to maintain the integrity of evidence.
- FTK Imager: Acquires disk images and verifies data.
- EnCase: Used for imaging and data recovery.
- dd: Command-line tool for creating disk images.

Computer Forensics Tools

2. Data Recovery Tools:

- Designed to recover deleted or corrupted files.
- Recuva: Recovers files from drives and memory cards.
- R-Studio: Retrieves lost data from various file systems.
- ProDiscover: Investigates and recovers deleted or hidden data.

3. File Analysis Tools:

- Analyze file systems and detect suspicious data.
- X1 Social Discovery: Extracts data from social media and emails.
- Autopsy: Helps with evidence collection and case management.
- Sleuth Kit: Analyzes file systems and recovers deleted files.

Computer Forensics Tools

4. Memory Forensics Tools:

- Focus on analyzing volatile memory (RAM) to understand system activity.
- Volatility: Analyzes RAM dumps to extract running processes and network activity.
- Redline: Detects malware and abnormal behaviors in memory dumps.

5. Mobile Forensics Tools:

- Used for extracting and analyzing data from mobile devices.
- Cellebrite UFED: Extracts data from mobile devices, including encrypted data.
- Oxygen Forensics Detective: Extracts and decrypts mobile data.
- XRY: Extracts and analyzes data from mobile devices.

Computer Forensics Tools

6. Network Forensics Tools:

- Monitor and analyze network traffic to identify cybercrimes.
- Wireshark: Captures and analyzes network packets.
- Tcpdump: Command-line tool for capturing network packets.
- Network Miner: Extracts evidence from network traffic.

7. Email and Web Forensics Tools:

- Analyze email data and web activity for investigations.
- MailXaminer: Analyzes email content and headers, recovers deleted emails.
- Web Historian: Investigates web browsing history and extracts relevant evidence.

Computer Forensics Tools

8. Antivirus and Malware Analysis Tools:

- Identify, analyze, and remove malware from systems.
- VirusTotal: Analyzes files and URLs using multiple antivirus engines.
- IDA Pro: Reverse engineers malware to understand its behavior.
- Sandboxie: Isolates and analyzes suspicious files in a controlled environment.

9. Forensic Analysis Suites:

- Comprehensive tools for full forensic investigations, from data collection to reporting.
- FTK (Forensic Toolkit): Offers data analysis, keyword searching, and imaging.
- EnCase Forensic: A complete solution for data collection and analysis.
- X1 Search: Efficiently searches large data sets for evidence.

Computer Forensics Tools

10. Hashing Tools:

- Generate unique hash values to verify the integrity of digital evidence.
- HashMyFiles: Verifies file integrity using hash values.
- Md5sum: Generates MD5 hash values for integrity verification.

11. Firewall and Log Analysis Tools:

- Examine firewall logs and system logs for unauthorized access or malicious activity.
- LogParser: Parses logs from multiple sources and generates reports.
- Splunk: Analyzes machine-generated data for network forensics.

Evidence Collection And Data Seziure
Why Collect Evidence?

- Digital evidence refers to any data in electronic form that can be used in legal proceedings. It is typically gathered from digital devices like computers, phones, servers, or cloud services during investigations.
- Examples include:
- Messages (texts], social media chats)
- Digital documents
- Browsing history

- Images and videos
- Metadata (like timestamps and locations)
- System logs
- Deleted or recovered files
- It can be found on:
- Hard drives, mobile phones, USBs
- Servers, cloud storage, and social media platforms

Types of Evidence

- Real Evidence: Real evidence is any evidence that speaks for itself without relying on anything else. In electronic terms, this can be a log produced by an audit function— provided that the log can be shown to be free from contamination.
- Testimonial Evidence: Testimonial evidence is any evidence supplied by a witness. As long as the witness can be considered reliable, testimonial evidence can be almost as powerful as real evidence.
- Hearsay: Hearsay is any evidence presented by a person who was not a direct witness. Hearsay is generally inadmissible in court and should be avoided

The Rules of Evidence

- Admissible: Admissible is the most basic rule. The evidence must be able to be used in court.
- Authentic: You must be able to show that the evidence relates to the incident in a relevant way
- Complete: It’s not enough to collect evidence that just shows one perspective of the incident.
- Reliable: Your evidence collection and analysis procedures must not cast doubt on the evidence’s authenticity and veracity.
- Believable: The evidence you present should be clearly understandable and believable to a jury.

The Process of collecting Digital Evidence

1. Identification

- ❑ Recognize potential sources of digital evidence (e.g., computers, USBs, emails).
- ❑ Determine which devices or data may be relevant to the investigation.

Example

- ❖ Shut down the computer. Depending on the computer operating system, this usually involves pulling the plug or shutting down a network computer using relevant commands required by the network involved.
- ❖ Document the hardware configuration of the system. Be-fore dismantling the computer, it is important that pictures are taken of the computer.
- ❖ Labeling each wire is also important, so that it can easily be reconnected when the system configuration is restored to its original condition at a secure location.

The Process of collecting Digital Evidence

2. **Preservation**

- Secure the scene and prevent tampering or data loss.
- Create a forensic image (exact copy) of the storage device.
- Ensure integrity using hashing (like MD5 or SHA-1).

Examples

- Transport the computer system to a secure location. A seized computer left unattended can easily be compromised. Don’t leave the computer unattended unless it is locked up in a secure location.
- Make bit stream backups of hard disks and floppy disks. All evidence processing should be done on a restored copy of the bit stream backup rather than on the original computer.
- Mathematically authenticate data on all storage devices. You want to be able to prove that you did not alter any of the evidence after the computer came into your possession.

The Process of collecting Digital Evidence

3. Collection

- Systematically gather digital evidence using approved tools.
- Document the system date and time. If the system clock is one hour slow because of daylight-savings time, then file timestamps will also reflect the wrong time.
- Make a list of key search words. it is all but impossible for a computer specialist to manually view and evaluate every file on a computer hard disk drive

The Process of collecting Digital Evidence

4. Examination

- Analyze the data using forensic tools to uncover relevant information.
- Recover deleted files, examine logs, search for keywords, etc.
- Evaluate the Windows swap file. The Windows swap file is a potentially valuable source of evidence and leads. When the computer is turned off, the swap file is erased.
- Evaluate file slack. It is a source of significant security leakage and consists of raw memory dumps that occur during the work session as files are closed
- Evaluate unallocated space (erased files). Unallocated space should be evaluated for relevant keywords to supplement the keywords identified in the previous steps.

The Process of collecting Digital Evidence

5. Analysis

- Interpret the examined data to build a timeline or link evidence to events.
- Identify how and when specific actions were taken on the device.

6. Documentation

- Keep detailed records of all steps taken during the investigation.
- Maintain a clear chain of custody.
- Retain copies of software used. As part of your documentation process, it is recommended that a copy of the software used be included with the output of the forensic tool involved.

The Process of collecting Digital Evidence

7. Presentation

- ❑ Prepare reports that explain findings in a clear, legal-friendly format.
- ❑ Testify in court if necessary, explaining how the evidence was handled and what it shows.

Types of Digital Evidence Acquisition

1. Live Acquisition: This involves retrieving data from a system that is actively running.

To capture temporary (volatile) data that would be lost once the system is shut down.

Data Captured:

- ❑ Memory (RAM)

Types of Digital Evidence Acquisition

- Current processes
- Active network connections
- Logged-in users

Common Applications:

- Investigating ongoing intrusions
- Analyzing malware behavior
- Responding to security incidents

Types of Digital Evidence Acquisition

2. Static (Dead) Acquisition: Collecting information from a device that has been powered down.

Data Captured:

- ❑ Stored files and directories
- ❑ System logs
- ❑ Traces of deleted files

Common Applications:

- ❑ Preserving evidence over time
- ❑ Legal case preparation
- ❑ Internal security audits

Types of Digital Evidence Acquisition

3. Disk Imaging (Bit-for-Bit Copy): Making an exact replica of the entire storage device, down to each bit.

Imaging Types**:**

- **Physical Image**: Complete duplication of the entire storage space, including unused areas.
- **Logical Image**: Duplication of only the visible files and directory structure.

Common Applications:

- Recovering lost or deleted data
- Full-scale forensic examinations
- Ensuring data authenticity for legal use

Cloud Evidence Acquisition

- Extracting digital evidence from cloud-based services and platforms.
  Data Captured:
- Files stored in cloud drives
- Logs of user activities
- Metadata from cloud accounts
  Common Applications:
- Analyzing cloud service misuse
- Investigating internal data leaks
- Corporate security assessments

Remote Acquisition

- Gathering data from systems over a network without being physically present.

Common Applications:

- Investigations in global or distributed networks
- Responding to incidents in off-site offices
- Forensic analysis of remote servers or cloud-based systems

Ethical Hacking
What is Ethical Hacking?

- Ethical hacking refers to the practice of probing computer systems and networks for vulnerabilities, but without any harmful intent. These professionals, often known as ethical hackers, use the same techniques as malicious hackers but do so to improve security rather than exploit it. They assess systems, identify weaknesses, and report their findings along with solutions to fix them.

Types of Hackers

- In the digital world, hackers differ based on their motives, skills, and intentions. Understanding these categories is essential to cyber security:
- **White Hat Hackers**: These are ethical hackers focused on protecting systems and preventing cyber-attacks. They often hold certifications and may perform penetration testing to uncover and fix security issues. Some were formerly involved in malicious hacking but have since shifted to ethical roles.
- **Black Hat Hackers**: These hackers act with malicious intent, aiming to steal data, damage systems, or gain unauthorized access. They are skilled in writing their own code and exploiting system vulnerabilities for personal or criminal gain.

Types of Hackers

- **Grey Hat Hackers**: Operating in a moral gray area, these individuals may switch between ethical and malicious behavior depending on personal interest or compensation. They can pose serious risks due to their unpredictability.
- **Green Hat Hackers**: These are beginners or novices in the hacking world. They typically lack formal knowledge and rely on pre-written scripts while learning the basics through trial, error, and curiosity.
- **Red Hat Hackers**: Known for their aggressive approach, red hats target malicious hackers using offensive tactics. They may go as far as disabling or damaging the equipment of black hat hackers in retaliation.

Types of Hackers

- **Script Kiddies**: These are unskilled individuals who use pre-made tools and scripts without fully understanding how they work. They often launch basic attacks, such as DoS or DDoS, and may rely on software like Metasploit.
- **Blue Hat Hackers**: Similar to script kiddies, blue hats may seek revenge through hacking but show little interest in improving their skills. In some contexts, the term also refers to external security testers brought in to identify vulnerabilities in a system.

The Code Of Conduct Of An Ethical Hacker: -

- Identifying and determining the confidentiality and privacy of the data of any organization before hacking and should not violate any rule and regulations.
- Before and after the hacking maintaining the transparency with the client or owner of the organization.
- The intensions of an ethical hacker must be very clear, that not to harm the client or organization.
- Working within the limits set by the client or the organization, do not go beyond them.
- After the hacking do not disclose the private or confidential findings during the hacking with others.

Hacker Classifications

- Understanding the different types of hackers involves examining their intentions, resources, and objectives. Below is a breakdown of some of the most recognized categories:
- **State/Nation-Sponsored Hackers**: These individuals work for government agencies and often have access to advanced tools and virtually unlimited resources. Their missions can include gathering intelligence, disrupting rival nations, or influencing political outcomes, such as interfering in foreign elections.
- **Hacktivists**: These hackers act out of political or social motivation. They target governments, organizations, or institutions to draw attention to a cause. Their attacks often include website defacements or denial-of-service actions to gain media coverage for their message.

Hacker Classifications

- **Whistle-Blowers**: Often insiders, these individuals leak confidential company data either out of revenge or for personal gain. They may have legitimate access to systems but use their privileges to damage the organization's operations or reputation, potentially causing significant financial losses.
- **Cyber-Spies**: Employed by intelligence agencies or rival companies, cyber-spies gather sensitive data through digital surveillance. Their activities include espionage, sabotage, or data theft aimed at gaining a strategic advantage or launching future cyber-attacks.
- **Cyber-Heists**: These hackers focus on financial gain, typically by stealing money from banks or users through hacking or phishing. Such operations are often quick and large-scale, targeting multiple accounts or systems at once.

Hacker Classifications

- **Botnet Controllers**: These hackers take over poorly secured devices—like computers, smartphones, or tablets—by exploiting software vulnerabilities.
- They use these hijacked devices as part of a botnet to launch larger attacks, such as Distributed Denial of Service (DDoS) attacks.
- **Cybercriminals**: This group includes anyone committing crimes online. Their actions span a wide range, from fraud and identity theft to hacking into systems for data or monetary gain. Some may even operate in organized groups.

Hacker Classifications

- **Cyber-Terrorists**: These attackers aim to cause major disruption or fear, often targeting critical infrastructure or public services.
- They may use defacement, DDoS attacks, or other forms of digital disruption to create economic or psychological impact.
- **Suicide Hackers**: These individuals carry out cyber-attacks without concern for the consequences. They may be highly skilled or not, but what sets them apart is their willingness to face severe legal penalties to fulfill a mission or cause.

Tests on real life scenarios

- There are several methods to test and challenge a computer security system, each designed to simulate real-world scenarios an organization might face.
- **Local Network Test**: This simulates an internal user, such as an employee, trying to bypass internal defenses like intranet firewalls, web servers, and email systems.
- **Stolen Laptop Test**: Here, a laptop belonging to a key staff member is taken (with permission from the company) and given to ethical hackers. Since many users store passwords and sensitive data locally, the laptop is tested for access into corporate systems using the owner's privileges.

Tests on real life scenarios

- **Social Engineering Test**: This evaluates how likely staff are to unintentionally share sensitive information. For example, attackers might impersonate IT support to extract data. Since this method targets human behavior, it's among the hardest to defend against, requiring strong awareness and training.
- **Physical Entry Test**: Ethical hackers attempt to physically breach the organization’s premises. They might use found documents or props to avoid suspicion. The test assesses physical security measures like guards, access controls, and employee vigilance.

Each of these attacks can be performed from different levels of access:

- **Total Outsider**: Someone with no inside knowledge, relying only on public information. Strong systems should prevent any access at this level.
- **Semi-Insider**: Has some access, such as a customer using limited software or tools. These users should only be able to access what they're authorized to.
- **Valid Insider**: A legitimate user with access to certain systems. The test checks if they can extend their privileges beyond what's allowed. A secure system enforces strict access controls even for insiders.

Application of Digital Forensics

1. Criminal Case Analysis: Law enforcement relies on digital forensics to extract and examine electronic evidence in cases involving crimes like fraud, cyber harassment, kidnapping, murder, and drug operations.
2. Responding to Cybersecurity Incidents: After a cyberattack—such as ransomware or data theft—digital forensics is used to understand the breach, assess damage, and prevent further compromise.
3. Corporate and Internal Investigations: Organizations use forensic tools to investigate internal security risks, such as employee misconduct, data leaks, or policy breaches.

Application of Digital Forensics

4. Civil Disputes and Legal Proceedings: Digital forensics is increasingly used in legal cases, including divorce, custody battles, or workplace lawsuits.
Examples:

- Retrieving financial transactions or communication records.
- Using metadata to verify dates, times, or locations.
- Supporting or refuting legal claims through electronic records.

5. Investigating Intellectual Property Violations: Businesses use digital forensics to uncover and prove cases of intellectual property misuse or unauthorized data sharing.
Examples:

- Investigating the unauthorized use of proprietary software or code.
- Tracing distribution of confidential content through external sources.
- Reviewing access logs to detect internal data theft.

Application of Digital Forensics

6. Compliance and Audit Support: Forensic practices assist in ensuring organizations comply with data privacy regulations and maintain secure data management.

7. National Security & Intelligence Gathering: Defense and intelligence agencies use forensics to combat cyber_terrorism, foreign interference, and online espionage.

Examples:

- Tracing digital activity linked to terrorist networks.
- Analyzing threats from other nations.
- Extracting intelligence from seized electronic devices.

Application of Digital Forensics

8. Accident and Disaster Forensics: Digital forensics helps reconstruct events by examining system logs or electronic devices from incidents like crashes or technical failures.

9. Data Retrieval and Restoration: Digital forensics helps recover lost, deleted, or encrypted data during criminal investigations or business recovery operations.

10. Training and Cyber Awareness: Educational institutions and professional development programs incorporate digital forensics to train future cybersecurity specialists.

Challenges in Digital Forensics

1. Fast-Paced Technological Change: Constantly emerging devices, platforms, and software make it difficult for forensic tools to stay up to date. Analysts may struggle to access or interpret data from new or encrypted systems.

2. Massive and Diverse Data: The volume and variety of digital information—from emails and chats to cloud and app data—can be overwhelming. Sorting and pinpointing relevant evidence takes more time and effort.

3. Strong Encryption: While encryption protects privacy, it also blocks forensic access—even with legal permission. Important data may remain locked and unavailable for investigation.

Challenges in Digital Forensics

4. Anti-Forensics Tactics: Offenders use techniques like wiping, hiding, or masking data to avoid detection. These practices make evidence recovery more difficult and can mislead investigators.

5. Legal Barriers and Jurisdictional Limits: Data privacy laws vary across countries, creating complications in cross-border cases. Legal red tape can slow down or prevent access to crucial evidence.

6. Cloud-Based Storage: Digital evidence is often stored remotely on cloud platforms beyond the investigator's control. Gaining access requires service provider cooperation and proper legal procedures.

Challenges in Digital Forensics

7. Device Variety and BYOD Culture: The use of personal and Internet-connected devices adds complexity. Tools may not support all device types, making consistent data acquisition harder.

8. Preserving Chain of Custody: Evidence must be carefully handled from start to finish to ensure its authenticity. Any mishandling can invalidate the evidence in legal proceedings.

9. Shortage of Skilled Professionals: Digital forensics demands expertise and advanced tools, which may be costly or hard to find. This could limit timely and thorough investigations.

10. Loss of Volatile Data: Temporary data like RAM content is lost once a device shuts down or restarts. Delays in capturing live data may lead to permanent loss of vital information.

References

A., J.-P. (2021). A SURVEY ON ETHICAL HACKING: ISSUES AND CHALLENGES. 1-49.
Gupta, A. (2017). Ethical Hacking and Hacking Attacks. *International Journal Of Engineering And Computer Science*, 1-9.

Sahare, B. (2014). Study Of Ethical Hacking. *Jean-Paul A.*, 1-5.

Yusoff, Y. (2011). COMMON PHASES OF COMPUTER FORENSICS INVESTIGATION MODELS. *Bhawana Sahare1*, 1-16.

Next Class

Human- Computer Interaction (HCI) and Augmented Reality (AR)/ Virtual Reality (VR)