Computer Forensics

Week 1: Introduction to computer Forensics

Lemi Agrey Oliver

Email: codingissweet@gmail.com

Kumi University

Agenda

- Course General overview
- Course goals
- Grading
- Introduction to Computer Forensics
- Brief History of Computer Forensics
- Digital Forensics Process
- Types of Digital Evidence
- Legal Consideration in computer forensics
- Ethical Consideration
- Computer Crimes & Investigative process
- Etc

Course General overview

- This course explores the complex world of digital investigation. Explore the techniques and methodologies used to collect, preserve, and analyze digital evidence crucial for legal proceedings and incident response.
- From file systems to network forensics, learn to uncover hidden data, track digital footprints, and reconstruct digital incidents.
- Gain hands-on experience with industry-standard tools and practices, preparing the students to navigate complex cybercrime situations and contribute to solving real-world cases.
- Whether you are an IT professional, law enforcement officer, or aspiring cybersecurity expert, this course equips you with the essential skills to excel in the dynamic field of Computer Forensics

Course Goals

- Understand the principles, practices, and legal framework guiding digital evidence collection and analysis.
- Implement scene assessment, chain of custody, imaging, and live system acquisition techniques.
- Employ forensics tools to identify artifacts, reconstruct activity timelines, and interpret file systems.
- Compose accurate and well-organized forensic reports for legal proceedings.
- Understand critical ethical practices and relevant cybercrime laws in digital forensics.

Grading

- Course work and Assignment 30%
- Final Exams 70%

Introduction to Computer Forensics

- In this modern digital era, where most transactions are conducted using computers, the rate of cybercrimes has been increasing.
- The cybercriminals are indeed on the loose and to evade detection and possible prosecution, criminals are now employing high levels of technology to carry out these cybercrimes.
- Many companies and government entities globally have suffered considerable financial losses and disruptions to systems due to cybercriminals.
- A recent example is a cyberattack in the US state of Baltimore, where attackers stole a National Security tool and caused thousands of systems to freeze. The attack lasted three weeks, disrupting emails, real estate sales, water bills, health alerts, and several other services [1]

Introduction to computer Forensics++

- In Uganda, two giant telecom companies (MTN & Airtel Uganda) and a commercial bank were jointly hacked in 2019, resulting in a loss of 3.5 million US Dollars.
- The above examples clearly show that the cyberspace is unsafe, with criminals causing havoc. Therefore, there is a need for computer forensics. But what is computer forensics?
- Computer forensics is a branch of digital forensics that involves the investigation and analysis of electronic devices, systems, and networks to gather and preserve evidence for legal purposes.
- It focuses on the identification, extraction, documentation, and interpretation of digital evidence to uncover details of cybercrimes, security incidents, or other illicit activities.

Introduction to computer Forensics +++

- It can also be view as the application of investigative and analytical techniques to collect, preserve, analyze, and present digital evidence in legal proceedings
- According to [3]digital forensic is defined as “the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.”
- Computer Forensics uses specialized tools and techniques to recover data, like deleted files, internet history, and email communications from digital devices such as computers, smartphones, and storage media.[2]

Introduction to computer Forensics ++++

- In the digital forensics unlike governments, organizations/companies are mostly interested in protecting their digital assets rather than prosecuting the offenders
- This lecture and the remaining ones are geared towards empowering both law enforcement investigators and private investigators with the necessary skills that can enable them effectively carry out a successful forensic investigation.
- Unlike civil or administrative investigators, there is an acceptable threshold that must be met for the digital evidence to be admissible before legal proceedings/court of law

Introduction to computer Forensics +++++

- This threshold may vary from one legal jurisdictions to an other. It is therefore important to first get conversant with the law of evidence within one's jurisdiction before embarking forensic examination or investigation.
- Digital forensics can therefore be defined as the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.[3]
- Digital forensic is used to investigate data that is retrieved from a drive or storage media and network logs that helps to understand how the attackers gained access to the network.

Introduction to computer Forensics ++++++

- Digital or computer forensics is complete different from data recovery, in that, the goal of the data recovery is to restore data that might have been deleted in error
- Computer forensics basically deals with data that has been concealed or deleted intentional by the user with the purpose of evading justice.
- The content of electronic devices seized during search of or images created during forensic data acquisition remains unknown to the investigator until and analysis of the same is carried out. The further extractions and analysis of this data/devices require the use of forensically sound tools

Introduction to computer Forensics +++++++

- In some abnormal situations were storage disks are damaged or intentionally reformatted with the aim of concealing evidence, investigators may resort into the use of electron microscopes and other sophisticated tools
- In the end, the retrieved data may either be **inculpatory** evidence or **exculpatory** evidence. **Inculpatory** evidence is one that can help to pin the suspect down while exculpatory evidence is that one that is favor of the suspect

The investigations triad

- The forensic investigators are part and parcel of the ICT team of the organization and therefore they formed part of the investigation triad.
- This triad consist of the following functions

Introduction to computer Forensics ++++++++

- Vulnerability/threat assessment and risk management
- Network intrusion detection and incident response
- Digital investigations

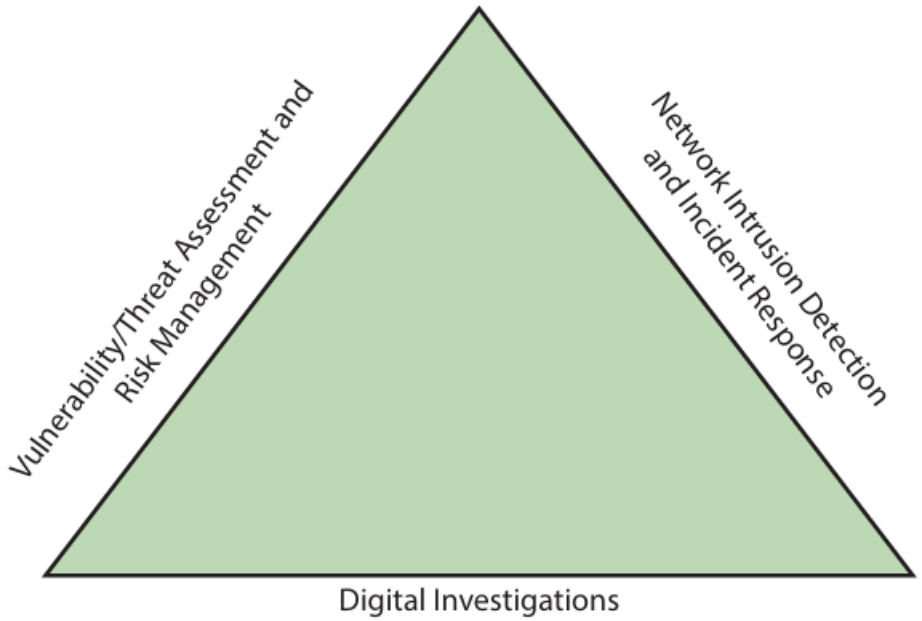

Figure: Forensic Investigation Triad [3]

Introduction to computer Forensics ++++++++++

- The people working under the vulnerability/threat assessment and risk management, test and verify the integrity of stand-alone workstations and network servers. The integrity checks involves the operating systems, applications and the physical security.
- There is also a need for the professionals in the vulnerability/threat assessment team to acquire skills in intrusion detection. Here you are supposed to detected intrusion attacks by the use of automated tools and also monitoring the logs of the firewall
- The digital investigations group manages investigations and conducts forensics analysis of systems suspected of containing evidence related to an incident or a crime.

Digital Forensics Process

- Identify the digital devices and systems relevant to the investigation, for example in a case involving child phonography, relevant devices could include the victim's smartphone and computer, as well as the suspect's devices.
- Preserve the integrity of digital evidence through proper handling and storage, this can be achieved through write-blocking devices to ensure that the original evidence is not altered or contaminated during the investigation.
- Collect relevant digital evidence using forensically sound methods, emphasis is placed on using a tools for forensic image tools of a hard drive using specialized software to ensure that the original data remains unchanged.
- Analyze the collected evidence to extract useful information

Digital Forensics Process+

- Using data recovery tools to extract deleted messages or files that may be relevant to the investigation.
- Interpret the findings to reconstruct events and determine the implications
- For example analyzing the timeline of events based on timestamps in digital communications to determine the sequence of child phonography incidents.
- Present the findings in a clear and understandable manner, often in court
- Creating a detailed report summarizing the findings of the investigation and presenting it as evidence in court.

Brief History of Computer Forensics

- Computer forensics, also known as digital forensics, has evolved alongside the development of computers and digital technology. 1970s, the field of computer forensics began to emerge as computers became more common in business and government. Initially, the focus was on recovering data from damaged or corrupted storage media.
- 1980s, As computer networks and the internet started to grow, the need for digital investigation capabilities became more apparent. Techniques for recovering data from networked computers and analyzing network traffic were developed.

Brief History of Computer Forensics+

- 1990s, the widespread use of personal computers and the internet led to an increase in cybercrime. Law enforcement agencies and private investigators began to develop specialized tools and techniques for investigating computer-related crimes.
- 2000s, the field of computer forensics continued to mature, with the development of more advanced tools and methodologies. The rise of mobile devices and cloud computing presented new challenges and opportunities for digital investigators.
- 2010s, The increasing use of encryption and other security measures made digital investigations more complex. Forensic investigators had to adapt their techniques to keep pace with technological advancements. As it stands now the field of computer forensic has reached its maturity with many tools available to the forensics investigators

Types of Digital Evidence

- You need to understand the two dimensions of the digital underworld and what they hold as potential evidence. The contents of both the visible and invisible dimensions can be recovered with forensics tools. General examples of each type are shown in this list[4]

Visible

- Documents, spreadsheets, image files, e-mail messages
- Files and folders
- Programs and applications
- Link files
- Log files

Types of Digital Evidence+

Invisible

- Deleted documents, spreadsheets, image files, e-mail messages
- Files and folders deliberately made invisible (hidden)
- File system artifacts
- Internet history
- Print jobs

Types of Digital Evidence++

- Random Access Memory (RAM)
- Protected storage areas (where credit card numbers entered on Web browsers are held)
- Storage areas outside the operating system's file system (areas that aren't readable by the operating system and that make good hiding places for files, even though computer forensics software can still find them)
- System log files

Legal Consideration in computer forensics

- Obtain proper legal authorization before conducting any computer forensic investigation. This may involve obtaining search warrants, subpoenas, or other legal documents depending on the jurisdiction.
- Adhere to privacy laws and regulations that protect the rights of individuals. Ensure that the collection and analysis of digital evidence comply with applicable data protection and privacy laws.
- Maintain a documented chain of custody for all digital evidence. This helps ensure the admissibility of evidence in court by demonstrating that it has been properly handled and preserved.
- Be aware of legal immunity issues. Computer forensic professionals should be cautious not to exceed the scope of their legal authority, as this could impact their immunity from legal action.

Legal Consideration in computer forensics+

- Follow forensic procedures and methodologies that are accepted in the legal system. Ensure that the evidence collected is admissible in court and can withstand legal scrutiny.
- Respect individuals' constitutional rights, including the rights against unreasonable searches and seizures. Ensure that searches and seizures are conducted in a manner consistent with legal standards.
- Understand the legal jurisdiction in which the investigation is taking place. Different jurisdictions may have varying laws and procedures related to computer forensics
- Be prepared to provide expert testimony in court. Computer forensic experts may be called upon to explain their methods, findings, and the reliability of the evidence collected.

Ethical Consideration

- Maintain the confidentiality of sensitive information obtained during the investigation. Unauthorized disclosure of information could lead to legal and ethical consequences.
- Conduct investigations with honesty and integrity. Do not manipulate or fabricate evidence, and accurately report findings without bias.
- Ensure that computer forensic professionals have the necessary skills and competence to conduct investigations. Continuous professional development is important to stay abreast of new technologies and methodologies.

Ethical Consideration+

- Be impartial and unbiased in the investigation process. Avoid any conflicts of interest that may compromise the integrity of the investigation.
- Obtain informed consent when applicable. In cases where individuals are involved, inform them about the nature of the investigation and seek their consent when required by law.
- Treat all individuals involved in the investigation with respect and dignity. Avoid unnecessary intrusion into personal matters and focus on the relevant evidence.
- Avoid conflicts of interest when working in dual roles, such as being both an investigator and a witness in legal proceedings

Applications+

The following are the fields/domains in which

- Criminal investigations for example cybercrimes, fraud, hacking.
- Corporate investigations for instant employee misconduct, intellectual property theft.
- Incident response and cybersecurity.

Computer Crimes

- Computer crimes, also known as cybercrimes, refer to criminal activities that involve the use of computers, networks, and digital technologies.
- These crimes can range from financial fraud and identity theft to hacking, malware distribution, and various forms of online harassment.
- As technology continues to advance, the range and complexity of computer crimes have also increased.

Examples of Computer Crime

- Unauthorized access to computer systems or networks to exploit vulnerabilities, steal information, or disrupt operations.
- The creation and distribution of malicious software, such as viruses, worms, trojans, ransomware, and spyware, designed to compromise or damage computer systems.
- Deceptive techniques as known as phishing which is phone done via email, to trick individuals into revealing sensitive information, such as passwords, credit card numbers, or personal details.
- Stealing personal information, such as social security numbers or bank account details, to impersonate someone else for financial gain or other malicious purposes.

Examples of Computer Crime++

- Various fraudulent activities conducted over the internet, including credit card fraud, online scams, and investment schemes.
- Overloading a computer system, network, or website with traffic to make it unavailable to users, disrupting normal operations.
- Covert activities conducted to gain unauthorized access to sensitive information for political, economic, or military purposes.
- Unauthorized access and extraction of sensitive or confidential information from databases or systems, often resulting in the exposure of personal or financial data.

Examples of Computer Crime+

- Harassment, threats, or intimidation using digital communication methods, such as social media, email, or messaging platforms.
- Unauthorized copying or distribution of copyrighted material, software piracy, and theft of trade secrets.
- Threatening to release sensitive information or launch a cyber attack unless a victim pays a ransom.
- Malicious activities conducted by individuals within an organization who exploit their privileged access for personal gain or to harm the organization.

Investigative Process

- The investigative process in the perspective of computer forensics and cybercrime typically follows a structured methodology to ensure the thorough and reliable collection, analysis, and presentation of digital evidence.

General overview of the investigative process

- The process begins with the identification and reporting of a potential incident. This could be initiated by an organization's internal monitoring systems, reports from users, or alerts from cybersecurity tools.

- Investigators conduct an initial assessment to determine the severity and nature of the incident. This involves gathering information about the affected systems, identifying potential evidence sources, and prioritizing the investigation

Investigative Process+

- To maintain the integrity of digital evidence, it's crucial to preserve the state of affected systems. This may involve isolating compromised systems, securing physical devices, and creating forensic images of storage media using forensically sound methods.
- Analyzing digital evidence involves examining the collected data to reconstruct events, identify patterns, and extract relevant information. This step helps investigators understand the nature of the incident, determine the extent of the compromise, and attribute actions to specific individuals or entities.
- Investigators create timelines of events by correlating information from different sources. This helps establish a chronological sequence of activities, which is crucial for understanding the flow of the incident.

Investigative Process+

- In cases involving cybercrime, attribution involves identifying the individuals or groups responsible for the incident. This can be a challenging task and may require collaboration with law enforcement agencies or cybersecurity organizations
- Investigators document their findings in a detailed and organized manner. This documentation is essential for creating a comprehensive report that can be used in legal proceedings. It includes information on the tools and techniques used, the analysis process, and the conclusions drawn.
- A final report is generated, summarizing the investigation's findings. This report is often presented to relevant stakeholders, including management, legal teams, and law enforcement. It may be used as evidence in court.

Investigative Process+

- Once the investigation is complete, recommendations for remediation and prevention of future incidents are provided. This may involve implementing security measures, updating policies, and improving incident response procedures

Common computer forensic tools includes

- **AccessData Forensic Toolkit (FTK)**, another popular forensic tool used for analyzing digital evidence, including files, emails, and other data.
- **Autopsy**, an open-source digital forensic platform that helps investigators analyze disk images and perform in-depth forensic analysis.
- **X-Ways Forensics**, a forensic tool that provides advanced analysis capabilities for digital evidence, including file recovery, metadata extraction, and timeline analysis.
- **Sleuth Kit**, another open-source tool that allows investigators to analyze disk images and perform file system analysis.

Common computer forensic tools includes

- **Cellebrite UFED**, A mobile forensic tool used to extract data from mobile devices such as smartphones and tablets.
- **Volatility**, A memory forensics tool used to extract information from volatile memory (RAM) to investigate security incidents and analyze malware.
- **EnCase**, A widely used forensic tool that allows investigators to collect and analyze electronic evidence from various devices and storage media.

Computer Forensics domains

- **Operating system forensics**, Operating System Forensics is the process of retrieving useful information from the Operating System (OS) of the computer or mobile device in question. The aim of collecting this information is to acquire empirical evidence against the perpetrator
- **Web forensics**, web forensics relates to any sort of crime committed over the Internet. With proper knowledge and expert skills, criminal activities like child pornography, hacking/cracking and identity theft may be traced back to its perpetrators.
- Criminals can only be successfully punished if a sufficient amount of conclusive evidence against them is found. In this case, Internet history, cache and server logs are of immense value. You might be surprised by the number of offenders who search the Internet for advice on how to conduct a crime.

Computer Forensics domains+

- **Email forensics**, email is the media or means of conveying messages/files or data to an other person over the internet. Email forensics is therefore the process of looking for evidence of crime or any wrong doing within the content of the messages being transmitted.
- The transmitted email, contains the source, content, actual sender and receiver information, date/time, protocols, and server information.
- **Network forensics**, this entails the monitoring and the analysis of network traffic with the intension of discovering an incident at the initial stages to avoid advanced effect on the organization's resources of infrastructure.

Computer Forensics domains++

- **Multimedia forensics**, the internet is a place that makes sharing multimedia content especially by the youngsters easy. This content may contain contrabands or leads to a crime agent or the source of the crime. For example an image might show some important details like when it was taken, the type of devices used and other metadata that might be important to the digital investigation

Principles of Computer Forensics

- Preservation of Evidence, Ensure the integrity of the original evidence by making exact copies (forensic images) before conducting any analysis.
- Use write-blocking tools and techniques to prevent any alterations to the original evidence during the investigation.
- Chain of Custody, Maintain a detailed and documented chain of custody for all evidence to establish its integrity and admissibility in court.
- Clearly document who had control of the evidence, when, and for what purpose.

Principles of Computer Forensics+

- Legal Compliance, adhere to all relevant laws and regulations while conducting computer forensic investigations.
- Obtain proper authorization and permissions before accessing or analyzing any electronic evidence.
- Volatility, recognize the volatile nature of digital evidence, which can be easily altered or lost. Act quickly to preserve and collect evidence to prevent loss or contamination.
- Order of Volatility prioritize the collection of volatile data first before moving on to less volatile data to ensure the preservation of critical evidence.

Principles of Computer Forensics++

- Document all steps and actions taken during the investigation process. This includes the tools used, procedures followed, and the results obtained.
- Create a comprehensive report that summarizes the findings and the methodology used..
- Analysis Without Alteration, analyze copies of the original evidence to avoid any accidental alteration of the primary data.
- Use specialized forensic tools and procedures that are designed to maintain the integrity of the evidence.

Principles of Computer Forensics+++

- Expertise, computer forensic investigations should be conducted by trained and qualified professionals with expertise in both computer systems and forensic techniques.
- Stay current with evolving technologies and techniques through continuous education and training
- Confidentiality, maintain the confidentiality of the investigation to protect sensitive information and the privacy of individuals involved.
- Share findings only with authorized personnel or entities as required by law.

Principles of Computer Forensics++++

❖Reporting, provide clear and concise reports detailing the findings of the investigation.

❖Present evidence in a format that is understandable to non-technical stakeholders, including law enforcement, legal professionals, and clients.

❖Testimony, be prepared to testify in court regarding the methods used, findings, and conclusions of the forensic investigation.

❖Present evidence in a manner that is admissible in court and withstands legal scrutiny

Principles of Computer Forensics+++++

❖Reporting, provide clear and concise reports detailing the findings of the investigation.

❖Present evidence in a format that is understandable to non-technical stakeholders, including law enforcement, legal professionals, and clients.

❖Testimony, be prepared to testify in court regarding the methods used, findings, and conclusions of the forensic investigation.

❖Present evidence in a manner that is admissible in court and withstands legal scrutiny

Evidence extraction and preservation

- Volatility Preservation, prioritize the preservation of volatile data, such as RAM or system memory, before shutting down or rebooting a system.
- Use tools that allow the capture and analysis of live system memory to collect volatile information.
- File System Analysis, use forensic tools to examine the file system and extract relevant files, directories, and metadata.
- Employ file carving techniques to recover deleted or fragmented files.

Evidence extraction and preservation

- Network Traffic Capture, capture and analyze network traffic to identify patterns, anomalies, or evidence of malicious activities.
- Employ network forensic tools to reconstruct communication patterns and extract relevant information.
- Mobile Device Extraction, Utilize specialized tools for extracting data from mobile devices, including smartphones and tablets.
- Consider both logical and physical extraction methods to retrieve various types of data.

Evidence Preservation

- Chain of Custody, establish and maintain a detailed chain of custody for all evidence.
- Document every person who handles the evidence, along with the date, time, and purpose of each interaction.
- Hashing and Digital Signatures, Create hash values for example MD5, SHA-256 for forensic images and individual files to ensure data integrity.
- Use digital signatures to verify the authenticity of forensic images and reports.

Evidence Preservation+

- Write Protection, implement write protection mechanisms to prevent any unintentional alteration or modification of the original evidence.
- Ensure that forensic tools used for analysis operate in a read-only mode when dealing with evidence.
- **Secure Storage,** store original evidence in a physically secure location to prevent unauthorized access or tampering.
- Use encrypted storage if sensitive data is involved, ensuring confidentiality.

Evidence Preservation++

- Documentation, document the condition of the evidence at the time of collection.
- Include detailed information about the extraction process, tools used, and any challenges faced during extraction
- Backup and Redundancy, create backup copies of extracted evidence to guard against accidental loss or corruption.
- Implement redundancy measures to ensure that evidence is not compromised if a storage medium fails.

Evidence Preservation+++

- Access Controls, restrict access to evidence to authorized personnel only.
- Implement access controls, encryption, and other security measures to protect stored evidence
- Regular Verification, periodically verify the integrity of stored evidence by rechecking hash values.
- Ensure that evidence remains in the same condition as when initially collected.
- Disposal Considerations, develop and follow protocols for the proper disposal of evidence once it is no longer needed.
- Comply with legal and organizational requirements for evidence retention and disposal.

Crime and incident scenes

❖ In the context of computer forensics and cybercrime, a "crime scene" or "incident scene" refers to the environment or context where a digital crime or security incident has occurred.

❖ Unlike traditional crime scenes, which involve physical spaces, digital crime scenes pertain to the electronic and virtual realm.

Digital Crime Scene Characteristics

❖Scope digital crime scenes can encompass a wide range of environments, including computer networks, servers, individual devices, and cloud-based systems.

Digital Crime Scene Characteristics+

- Data Sources, digital evidence can be found in various forms, including files, system logs, network traffic, emails, and databases. Each of these sources may contribute to the understanding of the incident.
- Volatility, digital environments are often dynamic, and evidence may be volatile. Real-time analysis may be necessary to capture transient data, such as network connections or system processes.
- Remote Nature, cybercrimes can be committed remotely, making it challenging to identify and physically secure a crime scene. The "crime scene" may span different geographic locations.

Digital Crime Scene Characteristics++

- Persistence, digital evidence can persist over time, even after the occurrence of the incident. Logs, timestamps, and artifacts may be preserved, aiding investigators in reconstructing events.

Challenges in Digital Crime Scene Management

- Rapid Evolution, technology evolves rapidly, and cyber threats continuously change. Investigators must stay updated on the latest tools, techniques, and threats to conduct effective investigations.
- Anti-Forensic Techniques, perpetrators may employ anti-forensic techniques to cover their tracks. Investigators must be aware of these techniques and employ countermeasures to overcome them.
- Encryption and Privacy Concerns, the widespread use of encryption technologies can hinder the ability to access and analyze data on digital devices. Encrypted data may be challenging to decipher without proper authentication credentials.

Challenges in Digital Crime Scene Management+

- Cloud Computing, the increasing use of cloud services makes it challenging for investigators to access and analyze data stored on remote servers. Legal and jurisdictional issues may also complicate the process of obtaining evidence from cloud service providers.
- Complexity, digital environments are complex, involving diverse technologies and interconnected systems. Investigating and managing digital crime scenes require expertise in various areas, including cybersecurity, network forensics, and data analysis.
- Global Nature, cybercrimes often transcend national borders. Coordination with international law enforcement agencies may be necessary for effective investigation and prosecution.

Challenges in Digital Crime Scene Management++

- Volatility of Digital Evidence, digital evidence is often volatile and can be easily altered or deleted. Investigators need to act quickly to preserve evidence and minimize the risk of data loss or tampering.
- Complexity of Digital Systems, the complexity and diversity of digital systems and devices present challenges in understanding and interpreting digital evidence. Investigators need a deep understanding of various operating systems, applications, and file systems.
- Global Jurisdiction and Legal Issues, computer crimes often transcend national borders, leading to jurisdictional challenges. Coordinating investigations across multiple jurisdictions and navigating different legal frameworks can be complex and time-consuming.

Challenges in Digital Crime Scene Management+++

❖Digital Rights and Privacy Laws, investigators must navigate legal frameworks that protect digital rights and privacy. Balancing the need for investigation with individual rights can be challenging, and improper handling of evidence can lead to legal consequences.

❖Skills Gap, the field of computer forensics requires highly specialized skills and knowledge. There is a shortage of skilled professionals, and keeping up with evolving technologies and forensic methodologies can be a significant challenge.

Challenges in Digital Crime Scene Management+++

- Costs and Resource Limitations, conducting thorough computer forensic investigations can be resource-intensive. Organizations may face budget constraints and limited access to the necessary tools and training.

Chain of custody

❖Refers to the chronological and documented record of the possession, handling, control, transfer, and analysis of physical or digital evidence during an investigation.

❖The purpose of maintaining a chain of custody is to ensure the integrity and admissibility of evidence in legal proceedings.

Components of the Chain of Custody

- Initial Collection, the chain of custody begins when the evidence is initially collected from the crime or incident scene. This involves properly identifying, documenting, and securing the evidence.
- Documentation, detailed documentation is crucial at each stage of the process. Information recorded may include the date and time of collection, the person collecting the evidence, a description of the evidence, and its condition at the time of collection.
- Sealing, evidence should be sealed in tamper-evident containers or packaging to prevent unauthorized access or tampering. Seals should be signed or initialed, and the seal number should be recorded

Components of the Chain of Custody++

- Transportation, during transportation, evidence must be securely and safely transferred from the collection site to the forensic laboratory or another secure location. Documentation should accompany the evidence to track its movement.
- Receiving, upon arrival at the forensic laboratory or another facility, the evidence is received by the forensic examiner or responsible personnel. This stage includes verifying the seal and comparing it to the recorded information.
- Analysis, during the analysis phase, the forensic examiner conducts examinations on the evidence. Any changes made or alterations should be documented, and the chain of custody record should be updated.

Components of the Chain of Custody+++

- Storage, when evidence is not actively being analyzed, it must be securely stored in a controlled environment. Access to the storage area should be restricted, and any retrieval or movement of the evidence should be documented.
- Court Presentation, if the evidence is presented in court, the chain of custody record is used to demonstrate that the evidence has been properly handled and preserved. The chain of custody document may be submitted as part of the testimony.

Summary

- In the lecture, we looked an overview of computer forensics and we defined computer forensics as a full branch of digital science for the investigation of digital devices and data carrying information in the court of law.
- We also delved into the steps involved in forensics which includes, digital investigation, identification, preservation, examination, analysis, and presentation of digital evidence.
- Further more we tackled some of the legal and ethical consideration with the field, so as to prepare the investigator with the realms of laws.
- The lecture also partly discussed the characteristics of a digital crime scene, challenges in the management of digital evidence

Summary+

- Chain of custody was explained as the path of the evidence from time of collection up to presentation in a court of law, under which it was very crucial for admissibility of digital evidence.
- The lecture is designed, in general terms, to make students acquainted with computer forensics so that they would at least have a modicum of elementary skills and knowledge necessary in this area at the moment when they start off further study or employability in this dynamic and fast-developing area.

Reference

1. A. R. Javed et al (2022) , *A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions*, IEEE paper 11066

2. *Computer forensics: Operating system forensics [updated 2019] | Infosec*. (n.d.). https://www.infosecinstitute.com/resources/digital-forensics/computer-forensics-operating-system-forensics/

3. Nelson, B., Phillips, A., & Steuarts (2018) *Guide to computer forensics and investigations*,, C. Cengage Learning. , page 6

4. Linda, V., Reynaldo, A., (2008), *Computer Forensics For Dummies*, Wiley Publishing, Inc, page 15