Computer Forensics

Week 3: Processing Crime and Incident Scenes

Lecturer: Lemi Agrey Oliver

codingissweet@gmail.com

Content

- Introduction
- Tasks investigators perform when working with digital evidence
- Understanding digital evidence
- Computer-Generated vs. Computer-Stored Records
- How to Identify file metadata using OSForensic
- Collecting Evidence in Private-Sector Incident Scenes
- Understanding Concepts and Terms Used in Warrants
- Preparing for a Search
- Evidence Retention and Media Storage Needs
- etc

Introduction

- Processing digital crime and incident scenes involves collecting, preserving, and analyzing digital evidence to reconstruct events, identify perpetrators, and support legal proceedings
- The purpose of digital evidence collected is to investigate the process of cybercrime occurred. Therefore, the process how to find the digital evidences and the perpetrators is called a criminal investigation procedure[2]
- Digital evidence is any incriminating information stored or transmitted in digital form.
- There is a debate of as to whether digital evidence should be considered as physical evidence or not. To that end, most legal jurisdiction especially courts in United States of America consider digital evidence as physical evidence
- To ensure the integrity of digital evidence, groups such as Scientific Working Group on Digital Evidence (SWGDE) set some guides for the recovery, preservation and examination of digital evidence[1]

Processing Incident or Crime Scenes

- Processing a computer forensic incident or crime scene involves several key steps to ensure that digital evidence is properly identified, collected, preserved, and analyzed.
- Before processing the scene, assess the situation to determine the scope of the incident or crime. Develop a plan for how to approach the scene, including what equipment and resources will be needed.
- Secure the scene to prevent unauthorized access or tampering. This may involve restricting access to the area and documenting the condition of the scene before any evidence is collected.
- Identify potential sources of digital evidence, such as computers, mobile devices, external storage devices, and network devices.

Processing Incident or Crime Scenes+

- Document the location and condition of each device and any other relevant physical evidence.
- Use proper forensic techniques to collect digital evidence, such as creating forensic images of storage devices to preserve their contents without altering them.
- Follow chain of custody procedures to maintain the integrity of the evidence.
- Once evidence is collected, it should be properly preserved to prevent alteration or damage. Use anti-static bags and other appropriate packaging materials.
- Transport the evidence to a secure location for analysis.

Processing Incident or Crime Scenes++

- Conduct a detailed analysis of the digital evidence to extract relevant information. This may involve recovering deleted files, analyzing file metadata, and identifying patterns of use or behavior.
- Document the findings of the analysis in a detailed report. Include information about the evidence collected, the analysis methods used, and any conclusions or findings.
- If the case goes to court, present the digital evidence in a clear and understandable manner. Be prepared to testify about the methods used to collect and analyze the evidence.

Tasks investigators perform when working with digital evidence

- **Identification**, identifying potential sources of digital evidence, such as computers, smartphones, servers, and cloud services.
- **Collection**, collecting relevant digital evidence using forensically sound methods to ensure its integrity and admissibility in court.
- **Preservation**, preserving the integrity of digital evidence by making a forensic copy and ensuring that the original data remains unchanged.
- **Analysis**, analyzing digital evidence to extract relevant information, such as deleted files, internet history, and communication logs.

Tasks investigators perform when working with digital evidence

- **Documentation**, documenting the chain of custody and all actions taken during the investigation to maintain the integrity of the evidence.
- **Interpretation**, interpreting the digital evidence in the context of the investigation to draw conclusions and support findings.
- **Presentation**, presenting digital evidence in a clear and understandable manner in court or other legal proceedings.
- **Reporting**, creating detailed reports of the investigation, including findings, methodology, and conclusions reached based on the digital evidence.

Understanding digital evidence

- Consistency, consistent practice helps verify your work and enhance credibility. This simply mean that one should apply the same security and controls for either civil or criminal digital evidence
- Compile with the evidence laws of your country or state
- Be mindful that evidences accepted in civil matter may also be accepted in a criminal case
- Keep updated on the latest rulings and instructions on collection, preservation, analysis and admitting of digital evidence

Understanding digital evidence+

- Any data discover during forensic investigations falls under your countries laws of evidence
- Digital evidence can change so easily unlike other types of evidence and therefore the only safeguard is always to compare the original copy with the duplicate
- Hearsay is also a concern when dealing with digital evidence. Hearsay can be anything that is said during the time of the testimony by a person other than the witness. This is an indirect evidence
- In some countries, a distinction exists between these categories.

Understanding digital evidence++

- Real evidence have verifiable content e.g., email sent and opened.
- Hearsay evidence are unverifiable content e.g., email content that has not been open.
- Business records often fall under real evidence category.
- An other way of categorizing business records is by grouping them into computer generated records and computer stored records
- **Computer-generated records** are data the system maintains, such as system log files and proxy server logs.[1]
- **Computer-stored records**, are electronic data that a person creates and saves on a computer or digital device, such as a spreadsheet or word processing document .[1]

Circumstance under which original evidence might not be possible to avail

- Inquires that involves collecting information about the network servers
- Removing the server from the network may paralyze the operations of the business and may therefore not be a desirable options as it may harm the business or its owners who maybe innocent bystanders
- When the original evidences are destroyed by a natural calamity or arson, the duplicate data may also be use in court

Computer-Generated vs. Computer-Stored Records

- Computer-generated records can be considered true only if it is confirmed that the program which produced the output is functioning normally.
- Computer-stored records can only be admissible in court if the person offering the records can prove that a person created the records and that the records have not been tampered with.
- Computer records must be collected according to the guidelines for digital records.
- Confirming the authenticity of digital evidence is important to avoid challenges from opponents who may try to raise questions on whether the records are altered or damaged.
- This doubt can be settled by proving that the records were indeed created by someone based on the metadata.

Computer-Generated vs. Computer-Stored Records+

- Attorneys can use circumstantial evidence, which requires finding other clues associated with the suspect's computer or location in case of records recovered from slack or unallocated space because they do not identify the authorship
- Computer-generated records can be considered true only if it is confirmed that the program which produced the output is functioning normally.
- Computer-stored records can only be admissible in court if the person offering the records can prove that a person created the records and that the records have not been tampered with.
- Computer records must be collected according to the guidelines for digital records.

Computer-Generated vs. Computer-Stored Records++

- Confirming the authenticity of digital evidence is important to avoid challenges from opponents who may try to raise questions on whether the records are altered or damaged.
- This doubt can be settled by proving that the records were indeed created by someone based on the metadata.
- Attorneys can use circumstantial evidence, which requires finding other clues associated with the suspect's computer or location in case of records recovered from slack or unallocated space because they do not identify the authorship

How to Identify file metadata using OSForensic

❖OSForensics is a digital forensic tool that can be used to identify file metadata, such as file creation date, modification date, access date, file size, and other attributes.

❖The following are the steps to follow

❖Launch the OSForensics application on your computer.

❖Click on the "Add Evidence" button to add the disk or image file containing the files for which you want to identify metadata.

How to Identify file metadata using OSForensic+

❖Use the search functionality in OSForensics to locate the files for which you want to identify metadata. You can search by file name, file type, or other criteria.

❖Once you have located the files, you can view their metadata by right-clicking on the file and selecting "View File Details." This will display a window showing the file's metadata, including creation date, modification date, access date, file size, and other attributes.

❖If you need to export the file metadata for further analysis or reporting, you can do so by selecting the files and clicking on the "Export" button. This will allow you to save the metadata in a CSV or XML format.

Collecting Evidence in Private-Sector Incident Scenes

- Private-sector organizations, including small to medium businesses, large corporations, and NGOs, must comply with state public disclosure and federal FOIA laws regarding public records.
- ISPs and communication companies must preserve customer privacy, especially regarding email, but federal regulations like the Homeland Security Act and the PATRIOT Act of 2001 redefine how they operate and maintain their records.
- Private-sector investigators are mainly concerned with protecting company assets, such as intellectual property, and enforcing company policy, not seeking out and prosecuting employees.

Collecting Evidence in Private-Sector Incident Scenes+

- Companies must establish clear policies regarding the inspection of digital assets, allowing for internal investigations within legal boundaries while safeguarding sensitive data and complying with public record laws.
- In cases of discovering criminal activities during internal investigations, companies must follow legal procedures, including reporting crimes to law enforcement, protecting confidential data, and ensuring compliance with search warrant requirements to avoid potential civil liability.
- **Commingled data**, Investigators in private-sector environments may encounter complex scenarios involving criminal acts intertwined with company data, requiring careful handling to report crimes, protect sensitive information, and collaborate with legal counsel to navigate legal and ethical challenges effectively.

Collecting Evidence in Private-Sector Incident Scenes++

- Private-sector investigators must be well informed about the privacy and evidence laws in their respective countries and should refer to the organization's attorney on how to respond to a police demand for evidence.
- In private investigation, there must be a reasonable suspicion that a law or policy is being violated to caused an investigation.
- Employers can conduct underground investigation and access company computer systems and digital devices without a warrant if there is a policy statement about misuse of digital assets.
- Private companies are at liberty to conduct an investigation as long as there is a policy statement or a warning banner informing employees of the organizations right to freely initiate any inquiry necessary to protect the company or organization

Understanding Concepts and Terms Used in Warrants

- Before being permitted to carry out any search, investigators are usually expected to obtain a warrant. In law enforcement crime scene processing, understanding warrant terminology is essential to govern the seizure of evidence, especially in digital investigations where vast amounts of data may contain unrelated information alongside the evidence being sought.
- Judges often issue limiting phrases in warrants to allow for the separation of innocent information from evidence, emphasizing the importance of listing specific items that can be seized to ensure compliance with legal requirements.
- **The plain view doctrine** permits law enforcement officers to seize objects without a warrant if they are in plain sight and meet specific criteria, such as being lawfully present, not using enhanced senses, and having probable cause to believe the item is evidence of a crime or contraband.

Understanding Concepts and Terms Used in Warrants

- The Horton test, established in Horton v. California, outlines criteria for the plain view doctrine, requiring lawful presence, lawful access to the object, and the immediate apparent incriminating character of the object for seizure without a warrant.
- While the plain view doctrine has been expanded to include sub doctrines like plain feel, plain smell, and plain hearing, its applicability in digital forensics is being debated, with varying interpretations across different circuit courts regarding its use in computer searches and the requirement for additional warrants when new incriminating evidence is discovered during a search.

Key concepts and terms related to search warrants

- **Search Warrant,** a legal document issued by a judge or magistrate that authorizes law enforcement officers to conduct a search of a specific location for specific items or evidence of a crime.
- **Probable Cause,** the standard of proof required to obtain a search warrant, meaning that there is a reasonable basis to believe that a crime has been committed and that evidence of the crime can be found at the location to be searched.
- **Affidavit,** a written statement of facts sworn to or affirmed by an oath before a person authorized to administer oaths, such as a notary public or a judge. In the context of a search warrant, the affidavit is a document submitted by law enforcement to the judge or magistrate to establish probable cause for the search.

Key concepts and terms related to search warrants+

❖**Particularity,** the requirement that a search warrant must describe with particularity the place to be searched and the items or evidence to be seized. This prevents general searches and ensures that the search is limited to specific areas and items related to the alleged crime.

❖**Exigent Circumstances,** emergency situations that require immediate action, such as when there is a risk of evidence being destroyed, removed, or hidden if law enforcement officers do not act quickly. In such cases, law enforcement may conduct a search without a warrant.

Key concepts and terms related to search warrants++

❖**Execution of Warrant,** the process of carrying out a search warrant, which typically involves law enforcement officers entering the specified location, conducting the search, and seizing any relevant evidence.

❖**Knock and Announce Rule,** a rule that requires law enforcement officers executing a search warrant to announce their presence and purpose before entering a premises, unless doing so would be dangerous or futile.

Key concepts and terms related to search warrants++

- **Return of Warrant,** after a search warrant is executed, the officer executing the warrant must prepare a written inventory of any items seized and provide a copy of the inventory to the person from whom the items were seized, if present.
- **Suppression of Evidence,** if evidence is obtained in violation of the legal requirements, it may be subject to suppression, meaning that it cannot be used in court against the defendant.
- **Franks Hearing,** a hearing held to determine whether false or misleading information was knowingly or recklessly included in the affidavit supporting a search warrant. If such information is found, the warrant may be invalidated.

Preparing for a Search

- **Identifying the Nature of the Case,** private-sector investigations may involve various scenarios such as employee misconduct, while law enforcement cases can range from fraud rings to homicides, influencing the investigative approach and required resources.
- **Identifying the Type of OS or Digital Device,** understanding the operating systems and devices involved in an investigation is crucial for determining the tools and resources needed, especially in cases where the crime scene is uncontrolled and the types of devices used are unknown.

Preparing for a Search+

- **Determining Whether You Can Seize Computers and Digital Devices,** the decision to seize computers and digital devices from a crime scene depends on the type of case and location of evidence, with law enforcement requiring warrants for removal, considerations for offsite files, and challenges posed by cloud storage.
- **Getting a Detailed Description of the Location,** gathering detailed information about the crime scene location is essential for efficient evidence collection, addressing environmental hazards, and ensuring safety, especially in hazardous situations like drug labs or terrorist attacks requiring specialized recovery procedures.

Preparing for a Search++

- **Determining Who Is in Charge,** establishing clear leadership roles and lines of authority is critical for coordinating investigations, with private-sector investigations typically requiring one designated responder while law enforcement cases may necessitate a designated scene leader for large-scale operations.
- **Using Additional Technical Expertise**, Identifying the need for specialized technical expertise to process complex crime scenes involving advanced systems like RAID servers or specialized databases, emphasizing the importance of recruiting skilled personnel and providing necessary training for effective evidence processing.
- **Determining the Tools You Need,** Proper preparation involves creating field kits tailored to initial and extensive response needs, ensuring that investigators are equipped with essential tools and resources to effectively process crime scenes and gather evidence efficiently.

Components of a search warrant

- A search warrant is a legal document that authorizes law enforcement officers to conduct a search of a specific location for specific items or evidence of a crime. The components of a search warrant typically include the following:
- **Caption, t**he caption of the warrant includes the name of the court issuing the warrant, the jurisdiction, and the title of the document (e.g., "Search Warrant").
- **Identification of Issuing Court,** the warrant should clearly identify the court or magistrate that issued the warrant.

Components of a search warrant+

- **Case Information,** the warrant may include information about the case, such as the case number and the names of the parties involved.
- **Affidavit or Sworn Statement,** the warrant is usually supported by an affidavit or sworn statement that provides the facts and circumstances establishing probable cause for the search. This affidavit is typically signed by a law enforcement officer and may include information from witnesses, informants, or other sources.
- **Description of Premises,** the warrant must describe with particularity the place to be searched. This description should be specific enough to identify the location clearly, such as the address or a detailed description of the property.

Components of a search warrant++

❖**Description of Items to be Seized,** the warrant must describe with particularity the items or evidence to be seized during the search. This description should be specific enough to identify the items clearly, such as by their nature, type, or location.

❖**Statement of Probable Cause, t**he warrant must include a statement of probable cause, explaining why there is reason to believe that the items or evidence sought are located at the specified location.

❖**Authorization for Search,** the warrant should include an authorization for law enforcement officers to search the specified location for the specified items or evidence.

Components of a search warrant+++

- **Execution Clause,** the warrant should include a statement authorizing law enforcement officers to execute the warrant at any time of the day or night, unless otherwise specified by the court.
- **Date and Time,** the warrant should include the date and time it was issued, as well as any limitations on the time frame for executing the warrant.
- **Signature of Issuing Authority,** the warrant should be signed by the judge or magistrate issuing the warrant, indicating their approval of the search.
- **Seal,** the warrant may include the court's seal or stamp to authenticate the document.

Securing a digital evidence scene

❖ Securing a digital evidence scene is crucial to preserve the integrity of the evidence and ensure that it can be used effectively in a forensic investigation.

The following are some of the steps that can be taken to secure digital evidence

❖ **Document the Scene,** before touching anything, document the scene thoroughly. Take photographs and videos to capture the layout of the area and the placement of devices and cables. Make notes of any observations that may be relevant to the investigation.

The following are some of the steps that can be taken to secure digital evidence+

- **Secure the Physical Space,** limit access to the area where the digital evidence is located. Use physical barriers or locks to prevent unauthorized entry. Ensure that only authorized personnel, such as forensic analysts and law enforcement officers, have access to the scene.
- **Shut Down Devices,** if possible, shut down any devices that are part of the digital evidence. This helps prevent data from being altered or lost due to automatic updates or processes running on the device.
- **Use Write-Blocking Devices,** when connecting storage devices (such as hard drives or USB drives) to a forensic workstation for analysis, use write-blocking devices to prevent any data from being written to the storage device. This ensures that the original evidence remains unchanged.

The following are some of the steps that can be taken to secure digital evidence++

- **Label and Document Evidence,** label all evidence items with unique identifiers and document their chain of custody. Record who collected the evidence, when and where it was collected, and any other relevant information.
- **Maintain a Log,** keep a detailed log of all activities and personnel involved in securing and processing the digital evidence scene. This log should include the date and time of each activity, the identity of the personnel involved, and a description of the activity performed.
- **Secure Network Connections,** if the digital evidence scene includes networked devices, secure the network connections to prevent unauthorized access or tampering. Use encryption and strong passwords to protect the network.

Evidence Retention and Media Storage Needs

- Computer forensic evidence retention and storage media needs are critical aspects of any digital investigation. Proper retention and storage ensure that evidence is preserved securely and can be used effectively in legal proceedings. Here are some key considerations:
- Determine the required retention period for digital evidence based on legal and regulatory requirements. This period may vary depending on the nature of the investigation and jurisdiction.
- Use reliable and secure storage media for preserving digital evidence. Examples include hard drives, solid-state drives, write-once-read-many (WORM) media, and digital evidence bags.

Evidence Retention and Media Storage Needs+

- Maintain a detailed chain of custody for all digital evidence, documenting who accessed it, when, and for what purpose. This ensures the integrity and admissibility of the evidence in court.
- Implement backup and redundancy measures to protect digital evidence from loss or corruption. Regularly back up evidence to secure locations and verify the integrity of backups.
- Restrict access to digital evidence to authorized personnel only. Implement access controls, encryption, and secure storage practices to protect against unauthorized access.

Evidence Retention and Media Storage Needs++

- Ensure the integrity of digital evidence by using cryptographic hash functions to create digital signatures of evidence files. Compare these signatures regularly to detect any changes.
- Maintain detailed documentation of all storage and retention practices, including the location of evidence, storage media used, and access logs.
- When digital evidence is no longer required to be retained, ensure secure and irreversible disposal using methods such as degaussing, shredding, or secure erasure.

Evidence Retention and Media Storage Needs+++

- Ensure that all retention and storage practices comply with relevant legal and regulatory requirements, such as data protection laws and chain of custody standards.
- Provide training to personnel involved in handling digital evidence on proper retention, storage, and disposal practices to minimize risks and ensure compliance.

The following are some of the steps that can be taken to secure digital evidence+++

- **Maintain Physical Security,** ensure that the physical security of the evidence scene is maintained at all times. This includes protecting evidence from environmental hazards such as water, heat, or physical damage.
- **Limit Communication,** limit communication about the evidence scene to only those personnel directly involved in the investigation. Avoid discussing details of the scene in public or over unsecured communication channels.

Evidence Activity Log

Evidence Activity Log				
This form is for tracking access by examiners of evidence items. Use one form for each piece of evidence.				
Case Number:				
Evidence Number:				
Evidence Description:				
Examiner's Name	Date Logged Out	Time	Date Logged in	Time

Figure 1: Activity log form[1]

An example of a private forensic investigation

- Kumi University faculty secretary has been altering students' results in the academic records system. The university hires a computer forensic investigator to conduct an investigation.

- **Investigation Steps**

- The investigator meets with the Kumi University's management team and the secretary to gather information about the suspected theft, including the timeline of events and any relevant background information.

An example of a private forensic investigation +

- The investigator collects digital evidence, such as the employee's work computer, external storage devices, and any other devices that may have been used to transfer data.
- The investigator creates forensic images of the devices using write-blocking technology to ensure the integrity of the original evidence.
- The investigator analyzes the forensic images to search for evidence of data theft, including deleted files, email communications, and file transfer logs.
- The investigator reconstructs a timeline of events to determine when the data theft occurred and how it was carried out.

An example of a private forensic investigation ++

- The investigator prepares a detailed report outlining the findings of the investigation, including the evidence collected, the methods used, and any conclusions drawn.
- The investigator ensures that the investigation complies with all relevant legal requirements, such as obtaining consent for the search and seizure of digital evidence.
- If the case goes to court, the investigator may provide expert testimony to explain the findings of the investigation and their significance.

Summary

- The lecture covered key concepts and practices in computer forensics, focusing on the investigation of digital evidence in criminal cases.
- It highlighted the importance of proper evidence collection, preservation, and analysis to ensure the integrity and admissibility of digital evidence in court.
- The lecture also discussed the use of tools like OSForensic to identify file metadata and the challenges of collecting evidence in private-sector incident scenes.
- Additionally, it touched on the legal aspects of obtaining warrants, preparing for a search, and retaining and storing evidence. Overall, the lecture provided a comprehensive overview of Processing Crime and Incident Scenes and its critical role in modern criminal investigations.

Reference

1. Nelson, B., Phillips, A., & Steuart, C. (2019). *Guide to computer forensics and investigations* Course Technology Cengage Learning. Page 145
2. Sun, J. R., Shih, M. L., & Hwang, M. S. (2015). A Survey of Digital Evidences Forensic and Cybercrime Investigation Procedure. *Int. J. Netw. Secur.*, *17*(5), 497-509. page 1
3. Oettinger, W. (2020). *Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence*. Packt Publishing Ltd.