BlackEAgle Investigation

Digital Forensics

Maram Isam Assaf

Dr.Safaa hriez

1. **Discuss what is meant by digital forensics.**

Digital forensics has evolved as a specialized field within computer forensics, focusing on investigating crimes involving digital evidence. It involves the methods for locating, obtaining, and safeguarding digital data found on various digital devices, with the main objective being to solve computer-related crimes by carefully examining digital traces [1].

This branch of forensic science is valuable for both criminal and civil investigations, but it is predominantly used in the realm of cybercrimes. For instance, law enforcement agencies may analyze data from a suspect's devices in a murder case, while cybersecurity experts may use digital forensics to identify those responsible for a malware attack. The fundamental principle of digital forensics is to treat digital evidence with the same rigor and procedural integrity as physical evidence, following strict forensic procedures to preserve the chain of custody and prevent evidence tampering [2].

While digital forensics and computer forensics are often used interchangeably, there is a subtle distinction. Digital forensics involves collecting and analyzing evidence from any digital device, including computers, mobile phones, tablets, and any device with a CPU. In contrast, computer forensics specifically focuses on computing devices. The broader scope of digital forensics underscores its versatility and crucial role in modern forensic investigations, whether related to cyber threats or other criminal activities involving digital data [2].

1. **Did you use the Rodney McKemmish model? If yes, explain it.**

**(slides), (Mckemmish and Graycar, 1999)**

Yes, the Rodney McKemmish model was utilized in the investigation of the USB and computer belonging to the suspect. This model, which comprises four phases: Identification, Preservation, Analysis, and Presentation provided a structured and methodical approach to handling the digital evidence.

**Identification**

In the initial phase, Identification, we identified potential sources of digital evidence. This involved recognizing that the suspect's computer and USB drive could contain crucial data related to the kidnapping cases orchestrated by the BlackEagle group. Also, we identified where and how the data is being stored. This could be done by capturing images of these devices immediately after taking the evidence from the suspects.

**Preservation**

The second phase, Preservation, was critical to maintaining the integrity of the evidence. We created forensic images of the suspect's computer and USB drive to prevent any alteration of the original data. Utilizing write-blocking tools, we ensured that the data remained unmodified during the imaging process. This step is essential in maintaining a reliable chain of custody, which is necessary for the evidence to be admissible in court.

**Analysis**

During the Analysis phase, we conducted a thorough examination of the forensic images. This involved using specialized forensic software to search for hidden files, recover deleted data, and analyze file system metadata. We looked for any evidence that could indicate the timing and location of the next crime, such as emails, documents, or logs that could provide clues about the criminal organization's plans. Additionally, we analyzed communication records, financial transactions, and any encrypted files that could contain valuable information

**Presentation**

Finally, in the Presentation phase, we compiled our findings into a coherent and detailed report. The report should be structured to be easily understandable by law enforcement officials and legal personnel. We prepared to present these findings in a clear and concise manner, ensuring that all evidence was documented in compliance with legal standards

1. **What is the importance of following the model presented in the previous question?**

**Preserving Evidence**

It is crucial to adhere to the McKemmish model to maintain the integrity of digital evidence. During the Preservation phase, forensic images of the suspect's digital devices are created to ensure that the original data remains unaltered. This step is necessary for maintaining a trustworthy chain of custody, proving that the evidence has not been altered from the moment it was taken to when it is presented in court.

**Repeatability and Reproducibility**

The structured approach of the McKemmish model is crucial for ensuring that forensic procedures can be replicated by other experts. The phases of Identification, Preservation, Analysis, and Presentation provide a clear and consistent framework. This consistency is essential for validating findings and enabling other forensic investigators to replicate the results under similar conditions.

**Minimizing Errors**

Following the McKemmish model helps forensic investigators reduce errors throughout the investigation. Each step in the model includes specific protocols and tools to avoid mistakes.

**Efficiency**

The McKemmish model boosts the efficiency of digital forensic investigations by providing a clear and systematic approach. It helps investigators methodically identify, preserve, analyze, and present evidence, which is crucial for delivering quick and accurate results, especially in urgent cases.

**Legal Admissibility**

Following the McKemmish model ensures that digital evidence is legally admissible. Its structured phases meet legal standards and protocols, and maintaining proper documentation and chain of custody during Preservation and Presentation proves the evidence is genuine and correctly handled.

1. **Evaluate the advantages and disadvantages of conducting a digital forensic investigation to improve system security.**

**Advantages:**

1. Ensuring System Integrity:

Digital forensics plays a crucial role in safeguarding the integrity of computer systems by identifying unauthorized access, data alterations, or deletions. This helps in maintaining the reliability and trustworthiness of digital assets within an organization.

1. Capturing Critical Information:

Organizations can leverage digital forensics to capture vital information and evidence in the event of a security breach or cyberattack. This includes gathering data on the methods and motives of attackers, which can inform proactive security measures to prevent future incidents.

1. Legal Admissibility of Evidence:

Digital forensic investigations follow strict protocols to ensure the admissibility of evidence in legal proceedings. Properly conducted investigations provide reliable digital evidence that can support legal actions, such as prosecuting offenders or defending against litigation.

1. Identification of Security Weaknesses:

Through forensic analysis, organizations can identify vulnerabilities and weaknesses in their security infrastructure. This proactive approach allows for the implementation of targeted security improvements to mitigate future risks and enhance overall system resilience.

**Disadvantages:**

1. Time-Consuming process:

The meticulous collection, preservation, and analysis of digital data can extend investigations for weeks or months, potentially impacting incident response times and the organization's ability to promptly resume normal operations.

1. Costing process:

Digital forensic investigations can be expensive due to the need for specialized tools, software, and expertise. The investment in equipment and trained personnel can be prohibitive for smaller organizations or law enforcement agencies with limited budgets. This financial barrier may limit access to comprehensive forensic capabilities.

1. Complexity of Analysis:

Digital forensic investigations often involve complex technical processes and require specialized knowledge. Analyzing large volumes of data and interpreting findings correctly can be challenging, especially in cases involving sophisticated cyber threats or advanced data manipulation techniques.

1. Privacy and Compliance Concerns:

Handling and analyzing digital evidence raises privacy concerns, particularly regarding sensitive personal or corporate information. Organizations must navigate legal and regulatory frameworks (such as GDPR or HIPAA) to ensure compliance with data protection laws while conducting investigations. Mishandling or improper disclosure of data can lead to legal repercussions and reputational damage.

1. **What are the law enforcement guidelines that you used when conducting the investigation?**

In the investigation of the BlackEagle group's involvement in the kidnapping cases, several law enforcement guidelines were followed to ensure the legality, integrity, and effectiveness of the digital forensic process:

* Adherence to Search and Seizure Laws:

Securing Warrants: A warrant was obtained to search the suspect's digital devices, including the computer and USB drive. This warrant ensured that the search was legally authorized. The warrant specified the scope of the search, detailing the places to be searched and the items to be seized, thus ensuring that the investigation stayed within legal boundaries.

* Data Privacy Regulations:

Compliance with Data Protection Laws: Throughout the investigation, we collected data in compliance with relevant data privacy laws, such as the GDPR. This included handling any personal data from the suspect's devices responsibly, with measures in place to protect its confidentiality and integrity. The data collection process was designed to avoid unnecessary data acquisition and focused only on information relevant to the investigation.

* Chain of Custody Documentation:

Maintaining Detailed Records: A comprehensive chain of custody (CoC) was maintained throughout the investigation. This included documenting every step of the evidence-handling process, from the initial seizure of the digital devices to their analysis and presentation in court. Each entry in the CoC records included the time and date of each transfer, as well as the names of the individuals involved. This careful documentation ensured that the integrity of the evidence was preserved, making it admissible in court.

1. **Discuss legal and ethical requirements that you have considered when conducting the investigation.**

The legal requirements that I have considered when conducting the BlackEAgle investigation were:

1. **Adherence to Search and Seizure Laws:**

Search and seizure are crucial for criminal investigations, giving law enforcement the authority to search individuals, their properties, or belongings, and seize relevant evidence. This process is governed by strict legal standards to protect individuals' rights and maintain the integrity of the justice system. (Justia Law, n.d.)

Warrants play a crucial role in legitimizing searches and seizures. A warrant must clearly describe the place to be searched and the items to be seized, limiting the scope of the search to what is considered necessary and relevant to the investigation. (National Constitution Center, 2019).

In the current investigation, a warrant has been secured to search a criminal's device and USB. This warrant ensures the search is carried out legally, with judicial authorization granted after a judge reviewed the probable cause provided by law enforcement.

1. **Data Privacy Regulations:**

The exponential increase in data generation and the proliferation of digital technologies have prompted governments around the world to adopt and expand laws and regulations aimed at protecting personal privacy. This shift has been driven by rising public concern regarding the misuse of personal information. As a result, data privacy has emerged as a critical policy area. For instance, the European Union's General Data Protection Regulation (GDPR) is a comprehensive legal framework that sets stringent standards for data protection and privacy, impacting how organizations worldwide handle personal data. (digitalprivacy.ieee.org, n.d.).

In the current investigation, it is crucial to ensure data collection from devices, such as a criminal's device or a USB drive, which means that the data must be collected in a way that does not alter or tamper with it, ensuring its reliability in legal contexts. Proper handling, usage, and storage of such data are essential to maintain its integrity and admissibility in court proceedings.

1. **Chain of Custody Documentation:**

Chain of custody (CoC) documentation is a crucial process in the handling of evidence, whether physical or electronic. It serves as a chronological record that traces the seizure, custody, control, transfer, analysis, and disposition of evidence.

The primary importance of maintaining a robust chain of custody lies in its role in the judicial system. Evidence is often central to the prosecution or defense in legal cases. (LHH, 2023).

In my investigation, I ensured that a comprehensive chain of custody was maintained. This included detailed records of every stage in the handling of evidence, from collection to analysis and presentation. Each entry in the CoC documentation noted the time and date of the collection, as well as the name of the investigator involved.

The Ethical Requirements that I considered when conducting the BlackEAgle investigation were:

1. **Minimizing Data Acquisition:**

Data minimization is a crucial principle within the domain of data privacy and protection. It emphasizes the collection and retention of only the minimal amount of personal information necessary for a specific purpose and ensures that this information is kept for the shortest duration possible. This approach is not only a best practice but also a legal requirement in many jurisdictions, aimed at reducing the risk of data breaches and enhancing privacy. (www.piiano.com, n.d.).

1. **Confidentiality:**

In digital forensics, the ethical guidelines mandate that all information discovered during an investigation must be kept confidential. This confidentiality is maintained unless disclosure is required by law, an authorized client, or an organization. This approach is critical to prevent unauthorized access and misuse of sensitive data, ensuring that the privacy of individuals is safeguarded throughout the investigative process. (Lucifer, 2023).

During my investigation, I ensured that all information regarding the suspect, the suspect's device, USB drives, and the victim was kept confidential. Access to this information was restricted to authorized individuals only, thus maintaining the integrity and confidentiality of the investigation. This careful handling of sensitive information aligns with the ethical standards in digital forensics, reinforcing the commitment to confidentiality.

1. **Objectivity and Integrity:**

The field of digital forensics is underpinned by fundamental principles of objectivity and integrity. These principles ensure that investigations are conducted fairly, findings are credible, and justice is served. In this discussion, we will explore the importance of objectivity and integrity in digital forensic investigations, emphasizing the necessity for investigators to maintain an unbiased stance, act with honesty, and uphold ethical standards throughout their work. (Lucifer, 2023)

1. **Eagle’s Eye is an individual in the city and has legal rights. In reference to these rights, assess how ethical you were when conducting the investigation.**

When assessing the ethics of the investigation into Eagle’s Eye, it’s crucial to consider their legal rights. Firstly, when conducting the investigation, I respected the privacy of both the suspect and the victim this was done by following the GDPR laws. These were as follows: 1. Only relevant data was collected from Eagle’s Eye’s devices, ensuring minimal intrusion into their personal information. Data acquisition was limited to what was necessary for the investigation. 2. Efforts were taken to avoid collecting irrelevant data, focusing primarily on information relevant to the kidnapping instances.

Secondly, when conducting the investigation, I made sure to protect the confidentiality of all data related to the investigation, this was done by: 1. Ensuring that all sensitive data regarding Eagle’s Eye, including information found on their computer and USB drives, was kept confidential. 2. Accessing any data related to the Eagle’s Eye investigation was restricted to authorized personnel only, ensuring that the privacy of Eagle’s Eye was not compromised.

Thirdly, when conducting the investigation, I made sure to protect the objectivity and integrity of the investigation, 1. The investigation was conducted fairly, with an unbiased attitude toward Eagle's Eye. All conclusions were based on objective research analysis and forensic evidence. 2. The Rodney McKemmish methodology guaranteed that each part of the investigation was conducted with integrity and following recognized forensic protocols.

Lastly, when conducting the investigation, I made sure to follow the legal standards of conducting an investigation. 1. The investigation followed search and seizure laws, which include obtaining a proper warrant to clearly specify the scope of the search, thereby respecting Eagle’s Eye’s rights and making sure that the investigation stays within the legal boundaries. 2. Proper chain of custody documentation was maintained to safeguard the integrity of the evidence, ensuring its reliable use in legal proceedings.

1. **Evaluate the impact of both following and not following guidelines in a legal case, regarding digital forensic evidence.**

* **The Impact of Following Guidelines: (Francis, 2022)**

1. Ensuring Evidence Integrity: Adhering to guidelines safeguards the integrity of digital evidence. Using correct methods for acquisition, preservation, and analysis helps maintain the chain of custody and prevents tampering.
2. Admissibility in Court: Evidence collected under established procedures is more likely to be accepted by the courts. Proper handling makes evidence more convincing and reliable.
3. Efficiency: following guidelines enhances the efficiency of investigations by minimizing errors and saving time.
4. Ethical and Legal Compliance: Following guidelines ensure that investigations are conducted ethically and in compliance with legal requirements.

* **The Consequences of Not Following Guidelines: (Francis, 2022)**

1. Evidence Contamination: Improper handling can result in contaminated or altered evidence, making it inadmissible.
2. Loss of Credibility: Investigators fear losing their credibility in court by not following established guidelines.
3. Inefficiency: Not following guidelines can cause inefficiencies, delays, and mistakes.
4. **What was your forensic examination plan for conducting the analysis before starting the analysis?**

(www.infosecinstitute.com, n.d.), (Mckemmish and Graycar, 1999)

After arresting the suspect, the investigator found that he had a computer and a USB drive so an examination plan for these devices should be considered.

This forensic examination plan aims to detail a systematic method for analyzing the suspect's computer and USB drive. This approach adheres to best practices and legal standards to ensure the digital evidence remains unaltered and admissible in the investigation of the Black Eagle group's kidnapping cases.

Firstly, the examination focuses on discovering, analyzing, protecting, and presenting digital evidence retrieved from the suspect’s computer and USB drive, including logs, history, emails, messages, photos, and documents found in the suspect's devices.

To do this examination the investigator should download digital forensic tools such as FTK imager to create an image for the computer and the USB drive, and Autopsy to analyze data.

**The Plan:**

I will start by examining the USB for any evidence regarding the next drive also to check if any data is missing. Since the PC's operating system is Windows, I will then search through each PC file, focusing on Windows artifacts. I'll begin with internet artifacts, such as browsing history, cache, and cookies, to find anything related to the next crime, such as potential locations they plan to target.

Next, I will search the jump lists for each application on the PC. Deleted files from the system might still have corresponding jump list entries, which can provide valuable information about the time and place of the next crime.

I will also investigate link files, as deleting a file from the device does not remove its link file, potentially leading us to the evidence we need. Additionally, I will examine prefetch files, which can offer crucial information such as creation and modification dates. This data can help determine if the suspect used a specific file or application during their criminal activities.

Following Rodney McKemmish's model starting with the **identification phase,** acknowledges that the suspect’s computer and USB drive may contain important data. Then multiple images should be taken immediately for the devices to prevent data loss and to ensure the integrity of these devices. Then the **preservation phase**, in this phase, we should maintain the integrity of the devices, this can be done by taking images of the devices, validating the integrity of these images by calculating the hash value, and storing the original devices in a secure place where only authorized personnel are allowed. Moving to the **analysis phase**, where the investigator should examine these images of the devices searching for hidden files, and deleted data, and extract relevant emails, documents, and logs. Lastly, the **presentation phase**, where the investigator should present all his findings clearly and understandably by writing a report, presenting the findings using charts, make sure that the reports are structured and understandable by the legal personnel.

Finally, to adhere to legal and ethical standards, ensure all actions comply with search and seizure laws, data privacy regulations, and chain of custody documentation. Maintain confidentiality, minimize data collection, and ensure objectivity and integrity. Implement backup procedures for all forensic images and documentation, and prepare for potential issues such as data corruption, equipment failure, or legal challenges.

1. **Based on your journey in the analysis, what improvement recommendations do you suggest?**

I started with the USB drive since it had urgent evidence that needed to be addressed. I looked over the USB in detail before moving to the PC to carry out more research. I blended manual and automatic searches throughout, which produced important findings—particularly when looking for hidden data in files. Furthermore, I included thorough verification procedures that turned out to be crucial for guaranteeing data integrity, especially for the VBR on the USB, which had not been envisaged at first.

A few things that were part of the original analysis plan were not employed. At first, I had planned to devote a lot of attention to several Windows artifacts, including jump lists, internet artifacts, link files, and prefetch files. But a lot of these produced no meaningful information, so I had to refocus. For instance, I performed thorough manual searches and used specialist tools like FTK Imager to extract and analyze particular file types and artifacts rather than using prefetch files.

The Recommendations:

1. Regular Training and Certification

Continuous training and certification in the latest digital forensic tools and methods are essential, which will keep investigators updated on new techniques and best practices.

2. Learning New Forensic Tools

While FTK Imager is effective and used, learning new tools like Encase, X-Ways Forensics, Magnet AXIOM, and Autopsy can enhance analysis by offering more features and insights.

4. Enhanced Data Integrity Checks

Implement multiple data integrity checks throughout the analysis. Beyond initial hash calculations, periodic checks and blockchain logging can ensure data remains unaltered and provide an immutable audit trail.

5. Regular Updates to Legal Knowledge

Keep all team members informed about the latest legal standards and requirements for digital evidence, including recent case laws, data privacy regulations, and changes in search and seizure laws.

6. Backup and Redundancy Plans

Develop comprehensive backup and redundancy plans for all forensic images and documentation, including regular backups, off-site storage, and verification processes to prevent data loss from corruption or equipment failure.

1. **Are your recommendations help in this investigation only or can be used as best practices for conducting digital forensic investigation in general? Discuss your thoughts.**

The suggestions are helpful for the ongoing inquiry as well as for digital forensics best practices. Investigators stay current and capable of adjusting to new dangers by regular training in new techniques and instruments. Acquiring knowledge of extra forensic software such as EnCase and Magnet AXIOM improves the efficacy and quality of analysis.

Strict data integrity procedures, such as blockchain logging and hash computations, guarantee that the evidence is reliable and unaltered in court. By keeping up with the most recent legal standards, investigators can ensure that evidence is acceptable by complying with laws and regulations.

Comprehensive backup and redundancy plans prevent data loss from corruption or equipment failure. Regular backups and off-site storage ensure critical evidence is preserved and available.

These procedures improve forensic investigations' efficacy, dependability, and legal compliance while offering a methodical approach to the many problems and constantly changing cybersecurity threats.

1. **Critically evaluate your investigation, suggesting improvements to the current digital forensic investigation guidelines, processes, and procedures. (tools, how did they help, Rodney model, challenges, what tool I did not use)**

First of all, following the Rodney McKemmish approach worked incredibly well. The integrity and effectiveness of the investigation were improved by the systematic treatment of digital evidence, from identification to presentation. I made sure that every stage—identification, preservation, analysis, and presentation—was carried out precisely by closely adhering to this plan. This methodology not only preserved the authenticity of digital evidence but also expedited its acceptance for use in court.

These resources improved my analysis in several ways. 010 Editor made it possible to deeply examine and alter a variety of file formats, which is essential for comprehending file structures and data integrity. To retain data in its original state for in-depth analysis, FTK Imager made it easier to create forensic images. MD5 and SHA1 hashes were made available by HashMyFiles for file integrity checks. Reconstructing user behaviors is made easier by BrowsingHistoryView, which aggregates browser history. The use of JumpListExplorer to parse program usage data was essential for reconstructing the timeline. RBCmd revealed deletion details by extracting metadata from items in the recycle bin. As visual proof, Thumbcache Viewer retrieved thumbnail images. In order to determine shortcut targets and recreate user activities and accessed files, LECmd evaluated link data. By providing specific functions for data extraction, verification, and chronology reconstruction all essential for comprehending digital events and effectively assisting investigations these technologies improved my forensic analysis collectively.

Tools like libraries, registry file analysis tools, and prefetch files were not used by me. I could have gotten the investigation done faster if I had employed these tools.

I didn't face any significant obstacles, but the investigation took a lot of time. It's possible that the investigation's duration may have been lowered by learning more investigation tools like Encase or Magnet AXIOM.

Improved instruction and certification in cutting-edge forensic techniques and tools, like Magnet AXIOM and Encase, guarantee that investigators will always be able to handle changing cyber threats. FTK Imager and Autopsy can be integrated with these cutting-edge technologies to improve analysis skills and gain deeper insights into complex data environments. The trustworthiness of conclusions in court processes is maintained through regular hash validations and strengthened data integrity checks via blockchain logging. Reducing procedural risks in investigations is ensured by staying up to date on revised legal requirements. Putting thorough backup plans in place for forensic photos and paperwork reduces the chance of data loss and protects important evidence. By optimizing efficacy, compliance, and evidence reliability, these guidelines together ensure that forensic teams can effectively support just and fair legal decisions.

1. **Compare Autopsy and FTK-imager as tools that can be used in digital forensic investigation.** (Anon, 2023)

|  |  |  |
| --- | --- | --- |
|  | FTK-imager | Autopsy |
| Features and Capabilities | - Disk imaging and cloning.  - Verify disk integrity.  - File system analysis.  - Export forensic images.  - Simple and fast imaging tool.  - Support Widows only. | - Disk image analysis.  - Keyword search.  - Contextual and hash analysis.  - Supports multiple file formats.  - Simple user interface.  - Multi-platform support (Windows, macOS, Linux). |
| Cost | Free | Free, and open source. |
| Integration with other forensic tools | Limited integration | Good integration |
| File System Support | Both support NTFS, FAT, exFAT, Ext2/3/4, HFS+, ReFS | Both support NTFS, FAT, exFAT, Ext2/3/4, HFS+, ReFS, but Autopsy also supports APFS. |
| When to use | - When disk imaging is required.  - For basic forensic tasks.  - Ideal for organizations with limited budgets.  - When minimal investment in forensic tools is needed. | - For digital forensic evidence in legal actions.  - When a comprehensive analysis of disk images is needed.  - Suitable for organizations of all sizes.  - When user-friendly, easy-to-use forensic tools are preferred. |
| Advantages | - Cost-effective  - Easy to use  - Reliable for basic imaging tasks | - Free and open-source  - User-friendly  - Comprehensive analysis capabilities  - Supports multiple operating systems |

**References:**

[1] RecFaces. (n.d.). Digital forensics. Retrieved from <https://recfaces.com/articles/digital-forensics#1>

[2] IBM. (n.d.). Digital forensics. Retrieved from

<https://www.ibm.com/topics/digital-forensics>

[3] Rody Model

[4] Simply Forensic. (n.d.). Digital forensics: Pros and cons. Retrieved from <https://simplyforensic.com/digital-forensics-pros-and-cons>

[5] Justia Law. (n.d.). Search & Seizure Supreme Court Cases. [online] Available at: <https://supreme.justia.com/cases-by-topic/search-seizure/>.

[6] National Constitution Center (2019). The 4th Amendment of the U.S. Constitution. [online] National Constitution Center – The 4th Amendment of the U.S. Constitution. Available at: <https://constitutioncenter.org/interactive-constitution/amendment/amendment-iv>

[7] digitalprivacy.ieee.org. (n.d.). Global Adoption of Data Privacy Laws and Regulations - IEEE Digital Privacy. [online] Available at: <https://digitalprivacy.ieee.org/publications/topics/global-adoption-of-data-privacy-laws-and-regulations>.

[8] LHH (2023). How to Document Your Chain of Custody and Why It’s Important | LHH. [online] www.lhh.com. Available at: <https://www.lhh.com/us/en/insights/how-to-document-your-chain-of-custody-and-why-its-important/>.

[9] www.piiano.com. (n.d.). What is Data Minimization? Main Principles & Techniques. [online] Available at: <https://www.piiano.com/blog/data-minimization>.

[10] Lucifer (2023). Role of Ethics in Digital Forensics: A Digital Code of Conduct. [online] Forensics Insider. Available at: <https://www.forensicsinsider.com/digital-forensics/ethics-in-digital-forensics/>.

[11] Anon, (2023). Forensic Analysis Tools: Comparing FTK and Autopsy - Cyber Insight. [online] Available at: <https://cyberinsight.co/what-is-the-difference-between-ftk-and-autopsy/FTK-Imager>

[12] Francis, A. (2022). The Impact of Digital Forensics on Legal Proceedings. [online] Lawyer Monthly | Legal News Magazine. Available at: <https://www.lawyer-monthly.com/2022/05/the-impact-of-digital-forensics-on-legal-proceedings/>.

[13] www.infosecinstitute.com. (n.d.). Computer Forensics: Forensic Analysis and Examination Planning | Infosec. [online] Available at: <https://www.infosecinstitute.com/resources/digital-forensics/computer-forensics-forensic-analysis-examination-planning/>.

[14] Mckemmish, R. and Graycar, A. (1999). What is Forensic Computing? [online] Available at: <https://www.aic.gov.au/sites/default/files/2020-05/tandi118.pdf>.

‌