

***Digital Forensics***

***Final Project***

***Submitted to: Dr. Safaa Hriez***

***Submitted by: Hamza AL-Risheq***

Table of Contents

[1. Digital Forensics 2](#_Toc166518349)

[1.1 Definition of Digital Forensics 2](#_Toc166518350)

[1.2 Types of Digital Forensics 2](#_Toc166518351)

[2. Rodney McKemmish Model 3](#_Toc166518352)

[2.1 Rodeny McKemmish Model Overview 3](#_Toc166518353)

[2.3 Importance of Rodney McKemmish Model 4](#_Toc166518354)

[3. Pros and Cons of Digital Forensic Investigations for System Security Enhancement 4](#_Toc166518355)

[4. Law Enforcement Investigation Guidelines Utilized in My Investigations 5](#_Toc166518356)

[5. Legal and Ethical Considerations in Conducting Investigations 6](#_Toc166518357)

[6. Safeguarding Legal Rights in the Investigation Process for the Victim 6](#_Toc166518358)

[7. Impact of Following and Not Following the Guidelines in Digital Forensic Evidence: A Legal Case Analysis 7](#_Toc166518359)

[8. Plan for Conducting the Analysis on BlackEAgle Case before Starting the Analysis 8](#_Toc166518360)

[9. Recommendations for Enhancing Forensic Analysis Capabilities in BlackEAgle’s Case 10](#_Toc166518361)

[10. Best Practices for Effective Digital Forensic Investigations 11](#_Toc166518362)

[11. Critical Evaluation and Improvement Strategies on the BlackEAgle Investigation Case 11](#_Toc166518363)

[12. Autopsy Vs FTK-imager 12](#_Toc166518364)

[Appendices 15](#_Toc166518365)

[Appendix 1 15](#_Toc166518366)

[Appendix 2 16](#_Toc166518367)

[Appendix 3 17](#_Toc166518368)

[References 18](#_Toc166518369)

# 1. Digital Forensics

## 1.1 Definition of Digital Forensics

Digital forensics is the systematic investigation, preservation, and analysis of digital information gathered from various electronic devices. It is a critical aspect of cybersecurity and forensic science. This profession uses recognized methods to identify and understand digital artifacts essential for investigating cybercrime, civil litigation, and criminal cases. Digital forensics professionals play a crucial role in law enforcement, corporate governance, and cybersecurity operations by ensuring evidence integrity and legal compliance. They aid in identifying offenders, recreating digital events, reducing cyber threats, promoting justice, and safeguarding digital integrity (McKemmish, 1999) (What is Digital Forensics, 2024).

## 1.2 Types of Digital Forensics

* Computer Forensics: involves the examination of data stored on computers, laptops, servers, and similar computing devices. It includes retrieving deleted files, analyzing internet browsing history, examining system logs, and recovering data from storage devices.
* Mobile Device Forensics: extracting and analyzing data from mobile devices such as smartphones, tablets, and GPS devices. It includes recovering text messages, call logs, photos, videos, and app data from devices running various operating systems like iOS, Android, and others.
* Network Forensics: Network forensics focuses on investigating security incidents and cyberattacks by analyzing network traffic and logs. It involves monitoring and capturing network packets to identify malicious activities, intrusions, and unauthorized access attempts.
* Database forensics: is the investigation of databases to collect and analyze data related to cybercrime or fraudulent activity. It includes detecting unauthorized access, data tampering, or data manipulation in database systems such as SQL databases, NoSQL databases, and cloud databases.
* Memory forensics is the analysis of a computer or device's volatile memory (RAM) to recover useful information such as running programs, open network connections, encryption keys, and malware artefacts. It helps in detecting live system activity and identifying complex cyber-attacks that may avoid standard disk-based forensics.
* Disc forensics, also known as storage media forensics, is a critical subset of digital forensics that examines, and analyses data stored on various storage devices. These devices include hard disc drives (HDDs), solid-state drives (SSDs), USB flash drives, memory cards, and other types of removable media. Drive forensics is critical for uncovering digital evidence in criminal investigations, cybersecurity events, and legal cases.
* Cloud Forensics: As cloud computing services become more widely used, cloud forensics focuses on investigating digital evidence stored in cloud environments such as SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS. It entails obtaining data from cloud storage, analyzing access logs, and tracking user activity across many cloud platforms (Naveen, 2024) (Tunggal, 2023).

# 2. Rodney McKemmish Model

## 2.1 Rodeny McKemmish Model Overview

The Rodney McKemmish model, also known as the Digital Forensics Analysis Model, is an Approach for digital forensics that guides the methodical examination and evaluation of digital data. This methodology, created by Rodney McKemmish, an Australian forensic computing expert, offers an organized approach to digital investigations, allowing forensic examiners to perform extensive and thorough investigations of digital evidence. It has four main stages Identification, Preservation, Analysis, and Presentation.

* Identification: This stage involves recognizing and understanding what digital evidence exists, where it is located, and how it is stored. It involves recognizing various kinds of electronic devices capable of storing data, such as computers, mobile phones, and smart cards. Furthermore, it requires determining the type of information stored and its format to use suitable methods for extraction.
* Preservation: Preservation is crucial to maintaining the integrity of digital evidence during the forensic process. It aims to minimize changes to the data and any alterations must be justified and documented. This step also involves preserving the original state of electronic devices, ensuring that any modifications made to facilitate data access are properly documented and explained.
* Analysis is the extraction, processing, and analysis of digital data. Extracted data frequently requires processing to make it understandable to investigators. For example, data from a hard disc drive image may require additional processing to be extracted into a human-readable format. Processing might take place independently or as part of the extraction process.
* Presentation: refers to presenting digital evidence in a court of law. It includes the style of presentation, the presenter's qualifications, and the reliability of the processes used to generate the evidence. Forensic computing characterizes itself by requiring evidence to be derived from legally recognized techniques, ensuring legality in court. Failure to follow legal criteria may result in evidence being declared inadmissible or unhealthy. Using third-party software that incorrectly shows data in a document, for example, could damage the reliability of both the evidence and the examiner who created it (McKemmish, 1999).

## 2.3 Importance of Rodney McKemmish Model

* Adapting to Technological Improvements: this model accepts that technology is always improving and changing, creating new challenges as well as possibilities for forensics computing. Understanding and dealing with the fast development in operating systems, storage media, and digital devices on technologies allows forensics investigators to stay current and build appropriate strategies for dealing with these improvement challenges.
* Balancing Technology with Legal Considerations: Forensic computer specialists serve two masters: technology and law. The model emphasizes the significance of establishing a balance between using technical improvements to conduct investigations and keeping up to legal requirements and regulations. This balance guarantees that digital evidence is collected, analyzed, and presented in a way that is legally admissible and trusted in court.
* Assisting investigators in developing a standardized and understandable strategy to manage digital devices while extracting evidence, therefore maintaining evidence integrity.
* Ensuring successful Law Enforcement: In an era when digital evidence is critical in criminal investigations and court cases, the Rodney McKemmish model highlights the role of forensic computing in ensuring successful law enforcement. By providing law enforcement agencies with the knowledge, skills, and resources they need to manage the details of digital investigations, the model helps to ensure the successful conviction of cybercriminals and protects digital integrity.

# 3. Pros and Cons of Digital Forensic Investigations for System Security Enhancement

Conducting digital forensic investigations to enhance system security offers several advantages and disadvantages:

* Pros:
  + Root Cause Analysis: Digital forensics enables organizations to do comprehensive root cause analyses of security issues. Identifying the underlying vulnerabilities and weaknesses in systems and networks allows organizations to implement new features, services, and efforts to prevent or to fix the vulnerability.
  + Adding a layer of protection to systems involves deterring potential attacks by making individuals aware that investigations will be conducted in the event of an attack. This awareness prompts potential attackers to think twice before carrying out their actions, as they fear being arrested. Otherwise, individuals may engage in attacks recklessly, without concern for consequences, knowing that they are unlikely to be caught.
  + Computer forensics requires continuous study and improvement since technology is constantly evolving. This means that in order to be competitive, professionals must constantly learn new skills. It's an interesting career in which you're always challenged to learn and progress.
  + Because of the investigation and the knowledge about the system that investigators have, they can provide vital information on the effectiveness of incident response policies and technologies. Organizations can use this information to improve their response plans, strengthen their skills, and shorten response times in the event of a security incident. (Mabry , 2024)
* Cons:
  + Digital forensic investigations can be time consuming, labor-intensive, and costly. They require specialized technologies, skilled employees, and dedicated resources to undertake extensive digital evidence.
  + Analyzing digital evidence and reconstructing security incidents can be complex and challenging. Investigators need to possess advanced technical skills and expertise in forensic methodologies to interpret digital artifacts accurately. Which sometime will require highly skilled people and as an organization they must spend a lot of time and money on learning their employees.
  + Becoming a skilled computer forensic analyst requires extensive training and certification. Entry-level positions typically require a bachelor's degree in computer science or a related subject. Furthermore, experts are expected to obtain certificates such as Certified Forensic Computer Examiner (CFCE) or Certified Computer Examiner (CCE) to improve their expertise and authority.

# 4. Law Enforcement Investigation Guidelines Utilized in My Investigations

* I obtained written authorization from the city policy to conduct the investigation, granting me access to critical data and information on the digital devices.
* I implemented techniques to safeguard the integrity of the devices and digital evidence, such as hashing values for all data to ensure their integrity. Additionally, I utilized tools like a write blocker to prevent accidental overwriting or alteration of the devices.
* I documented and reported all activities in detail.
* I stored all digital evidence and devices in a protected area inaccessible to unauthorized individuals, ensuring their integrity and confidentiality.
* I verified everything while gathering data and information, analysis, and reporting the results by using pictures, and screenshots.
* As an investigator, I did my best to minimize errors during my investigation process. So, I maintained accuracy and reliability by paying special attention to detail, adhering to standardized methods, and utilizing modern technologies. Double-checking procedures and reviews by others assist in detecting and correcting problems early on.

# 5. Legal and Ethical Considerations in Conducting Investigations

* Compliance with data privacy standards, such as the GDPR and CCPA, is essential for conducting ethical digital investigations. Protecting people's privacy requires a strict strategy for data gathering, usage, and storage throughout the investigative process. As an Investigator, I secure sensitive information, create public trust, and reduce the possibility of legal ramifications for privacy infractions by complying with strict data protection rules.
* I have used legal requirements that require obtaining necessary authority, such as a court order, before collecting digital evidence. This initial stage ensures compliance with protocols on jurisdiction and integrity of evidence for admissibility in legal proceedings.
* I maintained a Chain of Custody (COC) for all digital evidence collected during the investigation, demonstrating the integrity and admissibility of evidence in legal proceedings.
* As an investigator, I maintained integrity and fairness by refusing any form of prejudice based on color, ethnicity, gender, religion, or social status. These essential principles have been used as a guide for all aspects of my investigation’s parts, guaranteeing fair treatment for all parties involved.
* All sensitive information gathered throughout the investigation, including personal data, I kept confidential. This includes information from the victim as well as unrelated individuals who may appear in the evidence.

# 6. Safeguarding Legal Rights in the Investigation Process for the Victim

* I’ve made it a priority to always maintain ethical standards and respect Eagle’s Eye legal rights.
* Ethical conduct was essential throughout the investigation, ensuring Eagle's Eye's rights were protected. This includes acquiring correct authority, upholding privacy laws, following search and seizure standards, keeping confidentiality, and encouraging fairness and impartiality.
* Demonstrate fairness and justice in all investigative procedures, treat Eagle Eye with respect, and provide fair treatment in line with ethical and legal principles.
* I maintain open and continuing communication with Eagle's Eye, swiftly responding to any concerns or questions they had and providing updates on the investigation's progress, building transparency and ensuring their participation in the process.
* I provided Eagle's Eye with clear explanations of the investigation process, their rights, and any potential implications, fostering trust and accountability throughout the investigation.

# 7. Impact of Following and Not Following the Guidelines in Digital Forensic Evidence: A Legal Case Analysis

* Following Guidelines:
  + Following the guidelines for managing digital forensic evidence adds validity to the investigation and the evidence produced in court. This can strengthen the case's legitimacy and raise the chances of a successful judgment in the court.
  + Following the guidelines ensures that digital evidence is collected, analyzed, and presented in a way that protects its integrity. This helped me to protect the evidence and devices from corruption and tampering. Therefore, ensuring that the evidence remains admissible and reliable in court.
  + Help me, as an investigator, to protect myself from getting into trouble or being investigated for not reporting changes or using professional guidelines. These guidelines serve as protection for me as an investigator.
  + Following guidelines increases the likelihood that digital forensic evidence will be admitted in court. Courts demand that evidence meets specific requirements in order to be admitted.
  + Using clear rules and guidelines to gather and store data and evidence helps preserve the truth.
* Not Following Guidelines:
  + Failure of these guidelines increases the risk of evidence corruption or tampering, which can compromise the evidence's integrity and reliability. This can result in issues to the evidence's reliability and acceptability in court.
  + Ignoring guidelines may result in the mishandling or corruption of digital evidence, risking its integrity and reliability.
  + Legal Challenges: Evidence that is not collected or handled in line with guidelines can be challenged in court, potentially leading to its removal or rejection.
  + Failure to follow guidelines reflects poorly on the professionalism and skill of the investigators involved, harming my reputation in the legal and forensic communities.

# 8. Plan for Conducting the Analysis on BlackEAgle Case before Starting the Analysis

* Investigation Objectives:
  + Analyze the digital devices obtained from the crime scene device and USB drive to uncover any clues that might reveal the time and location of the next crime planned by the BlackEAgle organization.
  + Therefore, the type of information will be dates and locations for the next crime.
* Investigation Scope:
  + The investigation will focus on analyzing the data stored on the confiscated device and USB drive, including device drives, device RAM, file system, device OS, artifacts, device registries, and USB.
* The needed Resources:
  + A team of digital forensics experts with experience in data analysis and forensic tools will conduct the investigation. Due to the highly confidential nature of this case, the team will consist of a small, trusted group whose identities will remain undisclosed until the investigation is complete. The team members are referred to by their nicknames: OldGuard, WolfEyes, KingH, and PineappleFlavor.
  + Tools:
    - FTK imager.
    - Autopsy.
    - 010 Editor.
    - LECmd.
    - PECmd.
    - MFTBrowser.
    - Hashmyfiles.
* Methodology Selection:
  + To collect all evidence and securely store it in a designated, access-controlled room with access policy you can view the access policy in [**Appendix 1**](#_Appendix_1)**.**
  + Data Acquisition: Utilizing forensic imaging tools to create exact copies of the confiscated device and USB drive for analysis. Storing all images securely and implementing strict access policies and these images must be encrypted and secured with a strong password policy**.**
  + To do the Data Acquisition we must follow the following rules:
    - We must use write blocker either software or hardware write blocker.
    - We must do logical image for each evidence at least 3 images.
    - Two of these images must be RAW (dd).
    - Third one E01 with compression level 9, use encryption, and do segmentation 2500 per file.
    - To do the images we will use FTK imager.
    - We must apply hashing verification method:
      * Calculate cryptographic hash values (MD5, SHA-1, SHA-256, etc.) of the original device and compare them to the hash values of the forensic images.
      * We can use tools like hashmyfiles to compare the hashes.
  + After the acquisition here is a comprehensive Windows Evidence Analysis Framework that will be used in our case: A Step-by-Step Guide:
    - Starting with RAM analysis.
    - Then analyzing the operating system (OS) and its features.
    - Conducting file analysis to examine all stored files, documents, and communications for relevant information.
    - Timeline Reconstruction: Analyzing timestamps and event logs to reconstruct a timeline of activities related to the BlackEAgle organization.
    - Analyzing all artifacts and registries on the device such as:
      * $Log files.
      * .pf files.
      * .lnk files.
      * $Recycle Bin files.
      * Viewing all the registries.
      * Analysis the Internet Artifacts.
    - Data Correlation: Identifying patterns or connections between digital artifacts and potential criminal activities. To further understand our evidence analysis framework view [**Appendix 2**](#_Appendix_3).
  + Maintain detailed records documenting the handling and movement of forensic image files and investigation procedure, steps, and results. Log all access attempts, including timestamps, user identities, and actions taken, to establish an audit trail of custody.
* Timeline:
* Week 1:
  + - Day 1-2: Collecting and securing all evidence, including the confiscated device and USB drive.
    - Day 3-4: Conducting forensic imaging of the devices and storing the images securely.
    - Day 5-6: Commencing analysis of the RAM and the operating system (OS).
    - Day 7: Initial file analysis to identify potential leads.
* Week 2:
  + - Day 8-9: Continuing analysis of files and communications stored on the devices.
    - Day 10-11: Reconstructing a timeline of activities related to the BlackEAgle organization.
    - Day 12-13: Analyzing artifacts and registries on the device for further insights.
    - Day 14: Identifying patterns or connections between digital artifacts and potential criminal activities.
* Week 3:
  + - Day 15-16: Finalizing data correlation and conducting any additional analysis needed.
    - Day 17-18: Reviewing and verifying all findings for accuracy.
    - Day 19-20: Compiling a detailed report of all procedures and findings.
    - Day 21: Presenting the report to relevant authorities and stakeholders.
* Having obtained written permission from the city policy to conduct the investigation, you can view the permission in [**Appendix 3**](#_Appendix_4).
* Review the investigation plan with relevant stakeholders.

# 9. Recommendations for Enhancing Forensic Analysis Capabilities in BlackEAgle’s Case

* That they built the investigation plan was not the perfect way. I would change the sequence of the plan to be more effective and increase the speed of the investigation.
* Identify potential vulnerabilities and dangers in the forensic analysis workflow and create contingency risk assessment plans and practices to overcome them.
* Conduct a thorough evaluation of current forensic software and hardware solutions to discover gaps in functionality and capacity. To Find and use the best forensic technologies with advanced tools and acquisitions for data extraction, analysis, and visualization, aiming to boost investigative efficiency and accuracy.
* Create an environment of continual improvement for the forensic team, encouraging feedback and creativity. Regularly review and update investigative techniques to keep pace with new threats and technologies.
* Apply new digital forensics investigation models such as ACPO (Association of Chief Police Officers), NIST (National Institute of Standards and Technology) Model, and ISO/IEC 27037.
* Foster collaboration and technique-sharing among team members, ensuring they share knowledge and skills to improve overall team proficiency and achieve better results in less time.
* Verify the Accuracy of Automated Tools: Set a strict rule requiring manual verification of all tasks completed with automated tools. This additional step guarantees that the findings are accurate and reliable, preventing potential errors or oversights.

# 10. Best Practices for Effective Digital Forensic Investigations

The recommendations provided in the previous section can serve as best practices for conducting digital forensic investigations not only in my specific case at hand but also in general. The recommendations outlined for enhancing forensic analysis capabilities in BlackEagle’s case extend beyond the confines of this specific investigation, offering general best practices for digital forensic investigators. By systematically identifying possible weaknesses and risks in the analytical workflow and developing contingency risk assessment plans, forensic teams may be prepared for and handle challenges that might come up throughout any investigation. Furthermore, getting an in-depth review of current forensic software and hardware solutions enables teams to stay current with advanced technologies and adopt tools that are most suited to their investigative objectives, ensuring efficiency and accuracy in analyses across different environments.

Continuous development that comes from other experiences is also essential to all investigators and cases to the success of digital forensic investigations, by focusing on creating an environment that works with continual feedback and continuous examination of investigative methodologies. By adopting modern investigation models and promoting collaboration among team members, forensic teams can enhance their proficiency and adaptability to evolving threats and technologies. Furthermore, applying serious methods, such as manually reviewing findings provided by automated tools, improves the integrity and accuracy of forensic analysis results, securing these suggestions as critical foundations of best practices in digital forensic investigations.

# 11. Critical Evaluation and Improvement Strategies on the BlackEAgle Investigation Case

After completing the investigation, I gained significant insights and identified several areas for improvement. Initially, I approached the investigation in a highly complex manner, which proved to be inefficient. By not considering simpler methods, I expended more time and effort than necessary to uncover evidence. In future investigations, I will adopt a more straightforward approach at the outset, progressively delving into more intricate details as required. Despite these challenges, I believe that for my first digital investigation, I performed admirably, demonstrating professionalism and thoroughness. I successfully developed an effective plan and process for the investigation, which yielded valuable results. However, there is always room for enhancement.

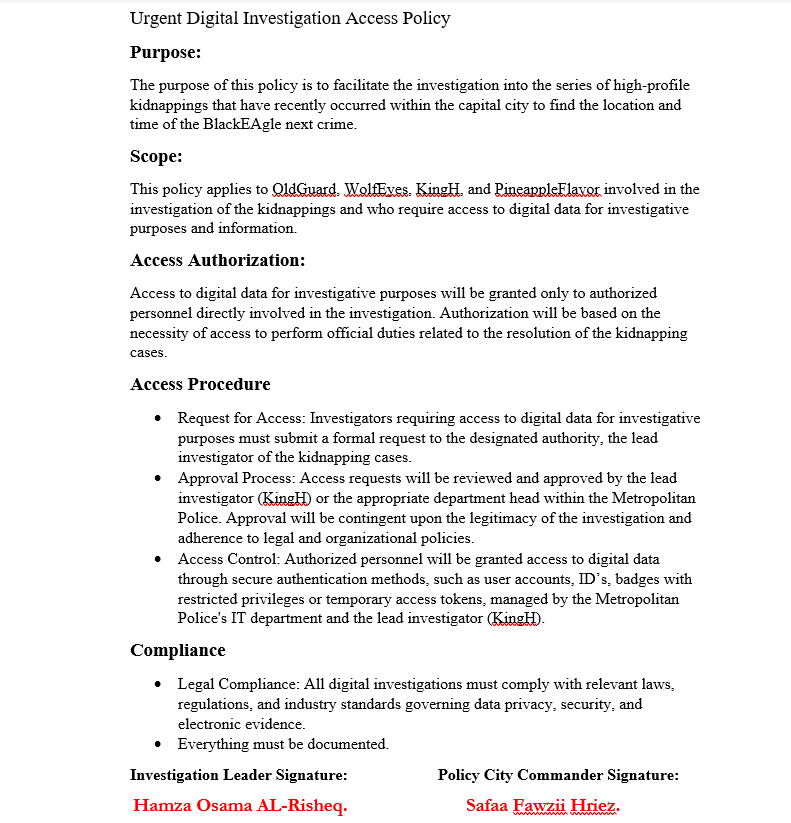
One area for improvement is the tools I employed. In future investigations, I intend to seek out or develop more advanced and sophisticated tools to enhance the efficiency and accuracy of my work. Additionally, I will consider utilizing more detailed and comprehensive models than those of Rodney McKemmish to guide my investigations. Overall, while my first digital forensic investigation was a remarkable and high-quality effort, I recognize the importance of continuous improvement. By refining my approach, upgrading my tools, and exploring more detailed models, I can further elevate the standards of my digital forensic investigations.

# 12. Autopsy Vs FTK-imager

|  |  |  |
| --- | --- | --- |
| *Features* | *Autopsy* | *FTK-imager* |
| Developer | Basis Technology | Exterro |
| Platform | Cross-platform (Windows, Linux, macOS) | Windows-only |
| License | Open source (GNU General Public License) | Unknown |
| Interface | Graphical User Interface (GUI) | Graphical User Interface (GUI) |
| Ease of Use | User-friendly, suitable for beginners | User-friendly, suitable for beginners |
| Image Acquisition | No | Supports disk imaging |
| Supported Image Formats | No | Supports various disk image formats (e.g., RAW, E01, AFF) |
| Data Carving | Yes | No |
| Keyword Search | Yes | Yes |
| Timeline Analysis | Yes | No |
| Artifact Analysis | Extensive support for analyzing various artifacts | Limited support compared to Autopsy |
| Plugin Support | Extensive plugin ecosystem | No plugin support |
| Community Support | Strong community support | Limited community support |
| Cost | Open-Source | Open-Source for basic version, paid for advanced features |
| Documentation | Comprehensive | Comprehensive |
| Updates | Regular updates and enhancements | Regular updates and enhancements |
| Usage | Widely used in both digital forensic investigations and as a teaching tool | Widely used in both digital forensic investigations and as a teaching tool |
| Acceptance in Courts | Accepted | Accepted |
| File Analysis | Yes | No |
| Memory Analysis | Yes | No |
| Mobile Forensics | Yes | No |
| Network Forensics | Yes | No |
| Write Blocking | Yes | Yes |
| Registry Analysis | Yes | No |
| Email Analysis | Autopsy can investigate emails for evidence. | FTK Imager doesn't handle emails. |
| Reporting | Autopsy can make detailed reports of findings. | FTK Imager doesn't help with reporting. |

# Appendices

## Appendix 1



## 

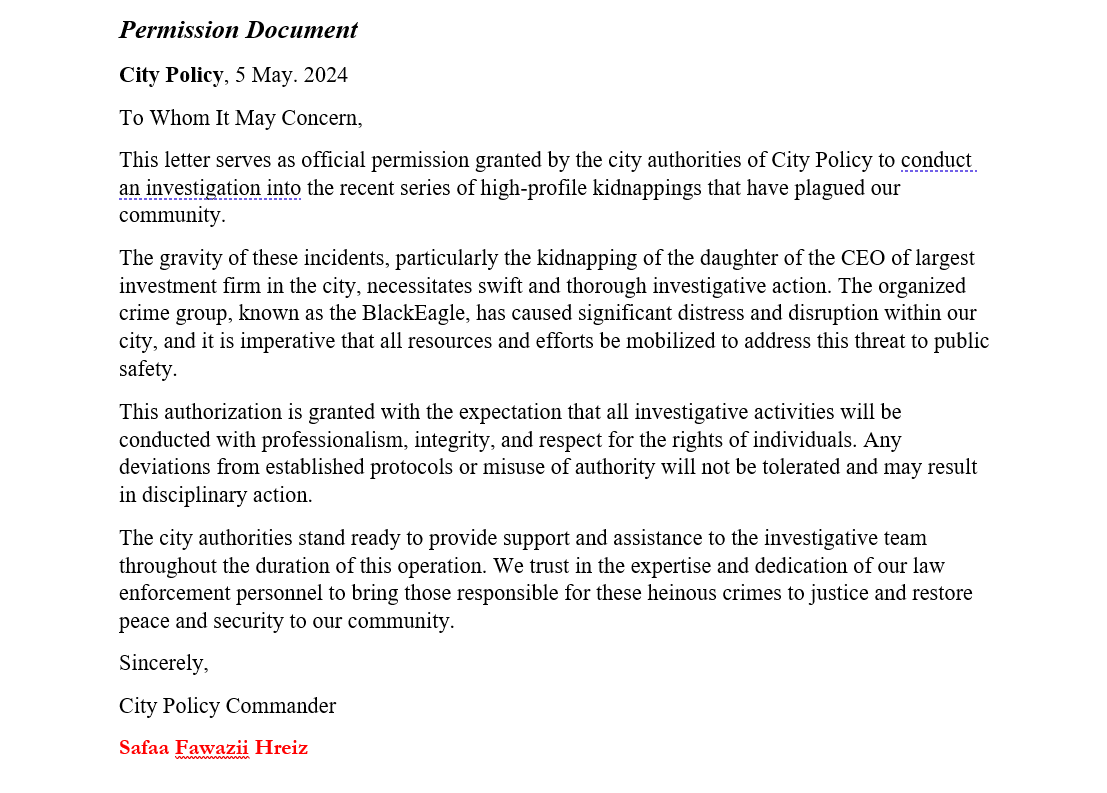
## Appendix 2

Comprehensive Windows Evidence Analysis Framework: A Step-by-Step Guide:

In order:

* ***Registry Analysis:***
  + Analysis SAM registries.
  + Analysis of SYSTEM registries.
  + Analysis Drives registries.
  + Analysis Security registries.
  + Analysis Machine registries.
* ***Files System Analysis***
  + Examine file metadata, including timestamps (creation, modification, access), file size, and attributes (hidden, system, read-only).
  + Look for remnants of deleted files and directories.
  + Analyzing MFT records and file system journal entries.
  + Focus on specific windows artifacts:
    - Prefetch Files.
    - Link Files (LNK).
    - Recycle Bin.
    - Logs.
    - Jump Lists.
    - Thumbnails.
    - Libraries.
    - Taskbar.
* ***Internet Artifact Analysis:***
  + Determine the used Browser in the machine.
  + Analysis the following parts:
    - Browser History.
    - Cookies.
    - Cache.
    - Download History.
    - Search History.
    - Bookmark and Favorites.
    - Browser Extensions.
* ***Timeline Analysis:***
  + Create a detailed timeline of events based on the analysis of RAM, file system, registry, and network data:
  + Document each event chronologically, including timestamps, event descriptions, and associated artifacts.
  + Sequence activities to understand the user activity.
  + Document every event sequentially with timestamps, descriptions, and related artefacts.
  + Identify key events such as malware execution, file creation/modification, network connections, and user activity.
* ***Start to link everything by building a roadmap that links everything together to find the time and location of the next crime for the BlackEAgle organization.***

## Appendix 3



# References

Mabry , K. (2024, April 24). *Computer Forensics: Unveiling the Hidden 5 Advantages*. Retrieved from sentreesystems: https://sentreesystems.com/computer-forensics/

McKemmish, R. (1999). What is Forensic. *Australian Institute of Criminology*, 1-6.

Naveen. (2024, April 15). *What is Digital Forensics - Types, Process, and Challenges*. Retrieved from intellipaat: https://intellipaat.com/blog/digital-forensics/

Tunggal, A. T. (2023, May 2). *What is Digital Forensics?* Retrieved from UpGuard: https://www.upguard.com/blog/digital-forensics

*What is Digital Forensics*. (2024, March 6). Retrieved from eccouncil: https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/what-is-digital-forensics/