THE AMERICAN UNIVERSITY IN CAIRO

100 YEARS | SCHOOL OF SCIENCES AND ENGINEERING

Digital Forensics

CSCE 4930

Digital Forensics Investigation Report

Submitted by:

Mohammed Riad 900192833

Submitted to:

Dr. Mohamed Sedky

Summer 2023

Table of Contents

1. Introduction

Forensics, in the realm of law enforcement and criminal justice, refers to the application of scientific techniques and technology to investigate and establish facts relevant to legal cases. This field plays a crucial role in gathering evidence and uncovering the truth behind various criminal activities. One of the significant branches within forensics is digital forensics, which deals with investigating cybercrimes and extracting valuable information from digital devices.

Digital forensics is a complex and specialized process that involves the meticulous retrieval and examination of digital data. This could range from analyzing computer hard drives, mobile phones, and other electronic devices to uncovering deleted files, identifying network intrusions, and tracing online activities. Given the prevalence of technology in our daily lives, digital forensics has become increasingly important in solving a wide range of criminal cases, including cyber fraud, hacking, online harassment, and intellectual property theft.

One of the key aspects that make digital forensics a formidable tool in the courtroom is the reliability and strength of the evidence it produces. Digital evidence, when properly collected and preserved, can be highly persuasive in legal proceedings. However, ensuring the integrity of digital evidence is a meticulous process that requires strict adherence to established protocols.

Moreover, all procedures and methodologies used in digital forensics should follow a scientific and accepted approach. This means employing validated tools and techniques to extract and analyze data, ensuring that the results are both accurate and reproducible.

2. Business Case

2.1 Report on Cyber Crimes

The digital transformation has ushered in significant advancements, revolutionizing our lives and businesses with its efficiency and connectivity. However, this rapid digital expansion has also given rise to a concerning surge in cyber crimes. The global cost of cybercrime is projected to reach $6 trillion annually, while data breaches have exposed over 155 million individuals' personal information in the United States alone. Ransomware attacks have increased by a staggering 715% in 2020, and phishing websites reached an all-time high of 2.1 million in Q1 2021. The digital transformation has expanded the attack surface, offering cybercriminals more opportunities to exploit vulnerabilities in systems and networks. To combat this growing threat, it is crucial for businesses and individuals to prioritize cybersecurity measures, including education and awareness, regular updates and patches, multi-factor authentication, data encryption, and well-defined incident response plans. By taking these proactive steps and collaborating to share information, we can collectively work towards a safer digital world.

2.2 Potential Customers

A digital forensics investigation lab caters to a diverse array of potential customers who seek assistance in the ever-expanding realm of cybersecurity threats. In the wake of recent cyber crimes and the growing threat landscape, the demand for digital forensics services has escalated across various sectors. Businesses and corporations, regardless of size or industry, recognize the criticality of safeguarding their sensitive information and proprietary data from cyber attacks, making them primary customers for digital forensics investigation labs. Government agencies, faced with increasingly sophisticated cyber threats from both nation-state actors and cybercriminals, require specialized expertise to conduct thorough investigations into cyber incidents and identify the perpetrators, thus turning to these labs for support.

In parallel, law enforcement entities are confronted with complex cybercrime cases that necessitate specialized digital forensics skills to collect digital evidence, analyze data, and build strong cases against cybercriminals. Financial institutions, including banks and credit card companies, deal with threats such as financial fraud and phishing attacks, making digital forensics services indispensable for uncovering evidence and mitigating risks. Moreover, the healthcare sector, which holds vast amounts of sensitive patient data, has become a lucrative target for cybercriminals, leading healthcare organizations to enlist digital forensics experts to investigate data breaches and other cyber incidents, ensuring patient privacy and data protection.

Lastly, individuals may also require digital forensics services to investigate cybercrimes, identity theft, or personal cyber incidents, seeking resolution and protection from future harm. As cyber threats continue to evolve in complexity and scale, the role of digital forensics investigation labs becomes increasingly indispensable in safeguarding digital assets, reconstructing cyber incidents, and providing invaluable insights to strengthen cybersecurity practices. Collaborating with IT security teams, incident response units, and law enforcement agencies, these labs contribute to a comprehensive and effective response to cyber incidents, thus fortifying the digital landscape for their wide range of customers.

2.3 Major Cybercrimes

In recent years, cyber breaches have become a growing concern, with numerous high-profile incidents impacting organizations and individuals alike. These breaches not only compromise sensitive data but also lead to significant financial repercussions. In this context, we will explore five of the most destructive cyber breaches based on their estimated cost, shedding light on the financial toll and highlighting the importance of robust cybersecurity measures.

Equifax Data Breach (2017): The breach impacted approximately 147 million people, resulting in a settlement of over $700 million to compensate affected individuals and cover regulatory fines.

Yahoo Data Breach (2013-2014): Two breaches affected over 3 billion user accounts, leading to hundreds of millions of dollars in settlements and regulatory fines.

Marriott International Data Breach (2014-2018): The breach exposed the personal information of around 500 million customers, resulting in a settlement of $117 million with various regulators.

Capital One Data Breach (2019): The breach compromised the personal information of over 100 million individuals, leading to an $80 million settlement to resolve regulatory claims.

Target Data Breach (2013): The breach exposed payment card data and personal information of about 41 million customers, resulting in significant legal settlements totaling hundreds of millions of dollars.

2.4 Business Plan

2.4.1 Executive Summary

As the digital landscape continues to evolve, the need for specialized cybersecurity services has never been more critical. We are dedicated to establishing a cutting-edge digital forensics investigation lab to meet the growing demand for cyber incident analysis, data recovery, and evidence preservation. Our lab aims to provide comprehensive and reliable digital forensics services to businesses, government agencies, law enforcement, and individuals. With a team of highly skilled and certified experts, state-of-the-art technology, and a commitment to excellence, we strive to be a trusted partner in tackling cyber threats and preserving the integrity of digital evidence.

2.4.2 Our Services:

Digital Forensics Investigations: We conduct in-depth investigations into cyber incidents, such as data breaches, ransomware attacks, intellectual property theft, and cyber espionage, to identify the source and extent of the breach.

Data Recovery and Analysis: Our lab employs advanced tools and techniques to recover and analyze digital evidence from various storage devices, ensuring data integrity and accuracy.

Incident Response: We provide rapid incident response services to help clients contain and mitigate the impact of cyber attacks, minimizing downtime and financial losses.

Litigation Support: Our expert testimony and digital evidence analysis support legal proceedings related to cybercrime, data breaches, and other digital incidents.

Cybersecurity Consulting: We offer comprehensive cybersecurity consulting services to help clients strengthen their defenses, identify vulnerabilities, and implement effective risk management strategies.

2.4.3 Marketing and Sales

To establish a strong presence in the market, we will begin by conducting comprehensive market research to identify potential customers and their specific digital forensics needs. Leveraging this understanding, we will build a robust brand identity and create a professional website to showcase our expertise and services. Strategic networking and partnerships with law firms, cybersecurity companies, and industry associations will help expand our reach and collaborate on complex cases.

Our commitment to customer satisfaction will drive us to deliver high-quality services and exceed client expectations, leading to positive referrals and repeat business. Hosting webinars and workshops on digital forensics trends and best practices will position us as industry thought leaders, attracting potential customers and further enhancing our credibility in the market.

3. Computer Forensic Workstation

3.1 Roles/Responsibilities

Digital Forensics Analysts: Responsible for conducting forensic examinations, analyzing digital evidence, and generating comprehensive reports.
System Administrators: Manage and maintain the computer forensic workstation's hardware and software, ensuring its optimal performance and security.
Lab Manager: Oversees the overall operation of the computer forensic workstation, coordinates tasks, and ensures adherence to standard procedures.
Quality Assurance (QA) Analysts: Verify and validate the accuracy and completeness of forensic analyses and reports.
Security Officers: Implement and enforce lab security measures to protect sensitive data and prevent unauthorized access.
Training Specialists: Provide ongoing training to analysts on the latest forensic tools, techniques, and best practices.

3.2 Hardware

The selection of appropriate hardware for a computer forensic workstation is of utmost importance as it directly impacts the efficiency, speed, and accuracy of the forensic analysis process.

3.2.1 Workstation

- Processing Power:
  Digital forensics involves computationally intensive tasks like data carving, decryption, and advanced analysis. Therefore, workstations must be equipped with high-performance processors. Modern multi-core processors, such as Intel Core i9 or AMD Ryzen 9 series,

provide the required processing power to handle complex forensic examinations efficiently.

- Memory (RAM):
  Sufficient RAM is critical to store and process large amounts of data during forensic analysis. Workstations should have ample RAM capacity, typically a minimum of 32GB, to handle memory-intensive tasks like memory analysis, virtualization, and running multiple forensic tools simultaneously.

- Storage Capacity:
  Workstations should be equipped with large storage capacity to hold forensic images, case files, and other data securely. High-speed, reliable Solid-State Drives (SSDs) are preferred for faster data access and improved performance during evidence processing.

- Graphics Processing Unit (GPU):
  A powerful GPU is beneficial for tasks that involve GPU-accelerated analysis, such as password cracking, cryptographic operations, and image processing. While not mandatory for all investigations, a dedicated GPU can significantly speed up certain tasks, especially when using specialized forensic software that supports GPU acceleration.

- Biometric Authentication and Security:
  To ensure strict access control, workstations should ideally incorporate biometric authentication methods, like fingerprint readers, in addition to traditional password protection. Strong security measures are necessary to prevent unauthorized access to sensitive case data and protect the integrity of evidence.

3.2.2 Workbench

The workbench is used to prepare hardware devices for investigative analysis, such as cloning hard drives. It should be equipped with rubber mats to prevent static electricity interference and ensure safe dismantling of devices like Apple iMacs.

3.2.3 Mobile Device Examination Hardware

SIM Card Readers :For examining SIM cards from cellular telephones operating on GSM networks.

Cellebrite UFED Touch2: A widely used mobile device forensic tool capable of extracting data from a wide range of smartphones and mobile devices. It allows investigators to access, analyze, and interpret data, including call logs, messages, media files, and app data.

GrayKey: A specialized device designed to unlock iPhones and extract data, including passcode-protected information. It is typically available only to law enforcement agencies for legal investigative purposes.

ZRT3 (Zero Recovery Time 3): A hardware tool for manual burner phone examinations, aiding in data extraction from various mobile devices.

RIFF Box 2: This hardware tool is used for JTAG (Joint Test Action Group) analysis of burner phones or Windows-based devices that require physical access for data extraction.

MFC Dongle: Used for specific iPhone models, the MFC Dongle can bypass passcode locks and assist in data extraction from Apple devices.

ORT Box: Another JTAG analysis tool that facilitates physical access to burner phones for forensic examination.

Ramsay Box STE6000 (Faraday Box): A Faraday cage used to isolate and shield mobile devices from external signals, preventing remote communication and data alteration during examination.

Paraben Stronghold Bags (Faraday Bags): Faraday bags are used to store and transport mobile devices securely while preventing any external signals from interfering with the data.

3.2.4 Faraday Room

A Faraday room allows for analyzing mobile devices without network connections, preventing remote wiping and preserving evidence integrity.

3.2.5 Redundancy and Backup

Redundancy and data backup are critical aspects of a forensic workstation's hardware design. Employing redundant components, such as power supplies and RAID configurations for storage, ensures data integrity and continuity of operations.

3.2.6 Write-Blockers

Hardware write-blockers are essential tools in a forensic workstation. These devices ensure that the original evidence remains unaltered during acquisition, preventing accidental data modification. Write-blockers are available for various storage interfaces like SATA, USB, FireWire, and PCIe, accommodating different types of media.

3.2.7 Cloning devices

Cloning devices are essential hardware tools used in digital forensics labs to create forensic copies (also known as clones or images) of storage media, such as hard drives, solid-state drives (SSDs), USB drives, memory cards, and other storage devices. These devices play a critical role in the evidence acquisition process, ensuring the preservation of the original data while allowing investigators to work on forensic copies for analysis.

3.2.8 Evidence Locker

An evidence locker is a secure cabinet with individual compartments, each lockable with tamper-resistant padlocks, for storing physical evidence securely.

3.2.9 Toolkit

Screwdrivers, flashlights and other tools for removing hard drives from various devices and enclosures.

3.2.10 Digital Cameras

Used to photograph the location of seized devices and document the investigation.

3.3 Software

The software requirements of a computer forensic workstation are critical for efficiently analyzing and interpreting digital evidence. These software programs enable digital forensics experts to process, examine, and extract valuable information from various digital sources while maintaining the integrity of the evidence. Below are some essential software programs commonly used in computer forensic workstations:

1. Forensic Imaging Software:

AccessData FTK Imager: A powerful and widely used tool for creating forensic images of storage media, including hard drives, SSDs, and USB drives. FTK Imager allows for the acquisition of data in various formats, such as DD, E01, and RAW.

2. Forensic Analysis and Examination Software:

EnCase Forensic: One of the leading digital forensic software suites used for evidence examination and analysis. EnCase Forensic supports a wide range of file systems and provides advanced search, carving, and reporting capabilities.
X-Ways Forensics: A versatile and efficient forensic tool known for its speed and ability to handle large datasets. X-Ways Forensics offers comprehensive analysis features and supports a variety of evidence formats.

3. **Volatility**: An essential open-source memory forensics tool used to analyze and extract information from the volatile memory of a computer. Volatility aids in the investigation of malware, network attacks, and system manipulation.

4. **Autopsy**: An open-source digital forensics platform that provides a user-friendly interface for data analysis, keyword searching, and reporting. Autopsy is widely used for both simple and complex forensic examinations.

5. Registry Viewer/Editor:

RegRipper: An open-source tool used to extract valuable information from Windows registry files. RegRipper enables investigators to gather insights into user activity, system configuration, and installed applications.

6. Hashing and Verification Tools:

md5sum, sha256sum: Command-line tools for generating hash values (MD5 and SHA-256) to verify the integrity of files and forensic images.
HashCalc: A user-friendly hashing tool for generating various hash values.

7. Password Cracking and Decryption Tools:

John the Ripper: A popular open-source password cracking tool used to test the strength of passwords and perform dictionary attacks.

Hashcat: A powerful password cracking tool that supports a wide range of algorithms and can utilize the GPU for faster processing.

8. Virtualization Software:

VMware Workstation: Virtualization software used to create and manage isolated virtual machines for safe malware analysis and other virtual forensic environments.

9. Network Analysis Tools:

Wireshark: A widely used network protocol analyzer for capturing and analyzing network traffic during digital investigations.
10. Mobile Forensics Tools:

Magnet AXIOM: A comprehensive mobile forensics software that supports a wide range of devices and enables investigators to analyze app data, recover deleted content, and examine cloud-based accounts.

Oxygen Forensic Detective: A powerful mobile forensic software with advanced capabilities, including data carving, cloud extraction, and social media analysis.

XRY: A mobile forensic tool used to extract data from a wide variety of mobile devices, including feature phones, smartphones, and GPS devices. XRY supports both physical and logical extractions.

11. Reporting and Documentation Tools:

Microsoft Word/Excel: Standard office tools for creating detailed forensic examination reports and organizing case-related data.

3.4 Accreditation and License

Accreditation and licenses are crucial aspects of establishing a reputable and trustworthy digital forensics laboratory. Compliance with industry standards and regulations ensures that the lab operates with the highest levels of professionalism, ethical practices, and data integrity. The specific accreditation needed for a digital forensics lab may vary depending on the country or region, but some common requirements include:

ISO/IEC 17025 Accreditation: an international standard that outlines the general requirements for the competence of testing and calibration laboratories. Achieving this accreditation demonstrates that the lab meets rigorous technical and management requirements, ensuring the accuracy and reliability of forensic examinations.

The American Society of Crime Laboratory Directors Lab Accreditation Board (ASCLD/LAB) : is responsible for certifying various crime labs, including computer forensics labs, for federal, state, and local agencies, as well as some international crime labs. Acting as an impartial entity, ASCLD/LAB is committed to upholding specific standards for forensics labs, encompassing both the conduct and practices of lab employees and their managers. In essence, individuals working in a forensics lab must always adhere to legal regulations and consistently follow proper scientific protocols. Additionally, ASCLD/LAB emphasizes the importance of a code of ethics that governs the behavior of both lab staff and management.

Criminal Justice Agency Licensing: Digital forensics labs require specific licenses or certifications from criminal justice or law enforcement agencies. These licenses often indicate that the lab meets the necessary legal and regulatory standards to handle evidence for law enforcement purposes.

3.5 Lab Security

Lab security is of paramount importance in a digital forensic environment to safeguard sensitive data, maintain the integrity of evidence, and protect against unauthorized access or data breaches.

Physical Security:

Access Control: Implement strict access controls to limit entry to authorized personnel only. Use biometric authentication, access cards, or keys to ensure only approved individuals can enter the lab.
Visitor Management: Have a sign-in and sign-out procedure for visitors, and ensure they are accompanied by authorized staff during their visit.
Secure Evidence Storage: Keep physical storage media and devices in locked evidence lockers with limited access to designated evidence custodians.

Network Security:

Isolated Network: Create a separate and isolated network for the digital forensic lab to prevent unauthorized access from the organization's primary network.
Firewalls and Intrusion Detection: Set up firewalls to monitor incoming and outgoing network traffic, and employ intrusion detection systems to identify suspicious activities.

Regular Security Updates: Keep all network equipment and software up to date with the latest security patches and firmware updates to address vulnerabilities.

Data Encryption:

Data at Rest and in Transit: Encrypt all sensitive data at rest on storage devices and during transmission between systems to protect against unauthorized access or interception.

User Authentication and Authorization:

Strong Password Policies: Enforce the use of strong, unique passwords and regularly prompt users to change them.
Principle of Least Privilege: Assign appropriate access levels to staff members based on their roles and responsibilities to minimize the risk of unauthorized access.

Incident Response and Logging:

Incident Response Plan: Develop a comprehensive incident response plan to handle security breaches, data breaches, or other security incidents effectively.
Logging and Monitoring: Implement robust logging mechanisms to record and monitor all activities within the lab. Regularly review logs for potential security issues.

Data Backup and Recovery:

Regular Backups: Perform regular backups of critical data to ensure data integrity and availability in case of data loss or hardware failure.
Offsite Backup: Store backup data offsite to safeguard against physical disasters or incidents that could affect the lab premises.

Secure Disposal:

Proper Media Sanitization: Establish protocols for securely wiping or physically destroying storage media and devices that are no longer in use or contain sensitive data.

Employee Training and Awareness:

Security Awareness Training: Train all lab personnel on security best practices, procedures, and potential risks to promote a security-conscious culture.

Phishing Awareness: Educate staff about the risks of phishing attacks and other social engineering techniques that could compromise lab security.

Regular Security Audits and Assessments:

Conduct periodic security audits and assessments to identify potential vulnerabilities and areas for improvement.
Penetration Testing: Consider engaging third-party security experts to conduct penetration tests to identify weaknesses in the lab's security measures.

3.6 Facility Management

Climate Control: Maintain proper temperature and humidity levels to protect hardware and storage media.
Power Backup: Install uninterruptible power supply (UPS) to prevent data loss during power outages.
Redundancy: Implement redundant systems to minimize downtime in case of hardware failure.

3.7 Standard Operating Procedures (SOPs)

SOPs are detailed step-by-step guidelines that outline the standard processes and protocols to be followed in a digital forensic lab. These procedures are essential for maintaining consistency, ensuring accuracy, and promoting best practices in all aspects of digital investigations.

1. Purpose

The purpose of this SOP is to provide guidelines and procedures for the proper handling, analysis, and preservation of digital and computer-based evidence within the digital forensic lab. This SOP ensures the integrity of digital evidence and adherence to legal and ethical standards during investigations.

2. Principles of Digital / Computer-Based Evidence

Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
Principle 2: In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
Principle 3: An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
Principle 4: The officer in charge of the investigation (the OIC) has overall responsibility for ensuring that the law and these principles are adhered to.

3. Evidence at Crime Scenes

Preserve the crime scene to prevent contamination or tampering with potential digital evidence.
Document all digital devices and media found at the scene and note their location, condition, and potential relevance to the investigation.

4. Seizure of Digital Devices

Use proper anti-static precautions when handling digital devices to prevent accidental damage.
Use validated write-blockers to prevent any write operations on seized storage media.
Document all necessary details during the seizure, including device information, time, and location.

5. Mobile Phones

Mobile phones should be immediately placed in Faraday bags upon seizure to prevent remote data wiping or alteration.
Follow established procedures for data acquisition from mobile phones using approved forensic tools.

6. Other Storage Media

Use validated and approved imaging tools to create forensic images of storage media, such as hard drives, USB drives, and memory cards.
Perform a verification process to ensure the integrity of the acquired images.

7. Handling and Transportation

Use anti-static bags and proper packaging to protect digital devices during transportation.
Maintain the chain of custody documentation throughout the handling and transportation process.

8. Internet and Social Media Related Crimes

Preserve relevant webpages, social media content, or online communications as evidence using appropriate tools and techniques.
Document the methods used for acquiring and preserving digital evidence from online sources.

9. Investigation

Conduct a comprehensive analysis of the acquired digital evidence using validated forensic tools and methodologies.
Document all analysis procedures, findings, and interpretations with timestamps for accuracy.

10. Indecent Images of Children on Digital Media

Handle cases involving indecent images of children with utmost sensitivity and following legal protocols.
Report any discovery of illegal content to the appropriate authorities promptly.

11. Management of Digital Images

Properly store and archive digital images acquired during investigations for future reference or legal proceedings.
Implement security measures to protect archived images from unauthorized access or data breaches.

3.8 Current Standards

In the lab setup, adherence to current standards is crucial to ensure the competence, quality, and reliability of the digital forensic processes. Let's elaborate on how the lab complies with the following standards:

1. **ISO 17025** (General requirements for the competence of testing and calibration laboratories):

The lab has implemented ISO 17025 to demonstrate its competence in conducting accurate and reliable digital forensic analyses.
All personnel involved in digital forensic investigations receive appropriate training and qualifications to meet the standard's requirements.
Calibration and maintenance of forensic tools and equipment are performed regularly to ensure accuracy and reliability in testing.
The lab maintains proper documentation, including standard operating procedures, test methods, and records, as required by ISO 17025.
External audits are conducted periodically to assess compliance with the standard and identify areas for improvement.

2. **ISO 9001** (Quality management systems standards):

The lab has established a quality management system (QMS) based on ISO 9001 principles to ensure consistent and effective digital forensic processes.
Continuous improvement practices are integrated into the QMS to identify and address areas for enhancement in the investigation procedures.
Customer satisfaction is monitored and evaluated to meet the needs and expectations of clients and stakeholders.
The lab regularly conducts internal audits to assess the QMS's performance and make necessary adjustments for optimization.
3. **ACPO** (Association of Chief Police Officers) - Good Practice Guide for Computer-Based Electronic Evidence:

The lab adheres to the ACPO Good Practice Guide to ensure the highest standards in the handling and analysis of computer-based electronic evidence.
Guidelines from the ACPO guide are integrated into the lab's standard operating procedures to maintain consistency and best practices.
The lab follows the ACPO's recommended protocols for evidence handling, data acquisition, analysis, and reporting in digital forensic investigations.

4. **NIST 800-86** (Guide to Integrating Forensic Techniques into Incident Response):

The lab utilizes NIST 800-86 to incorporate forensic techniques into incident response procedures effectively.
The guide assists in identifying and containing security incidents while preserving digital evidence for further analysis.
Incident response teams are trained to follow NIST guidelines to ensure the integrity and admissibility of evidence collected during response activities.

4. Conclusion

The report provides a comprehensive overview of the digital forensics field, emphasizing its significance in the context of recent cybercrimes. It outlines the business case for the digital forensics lab, identifying potential customers and presenting a strategic business plan. The report also details the essential components of a computer forensic workstation, including requirements, guidelines, and a comprehensive action plan for setting up the lab. By addressing these key aspects, the report establishes a strong foundation for the successful establishment and operation of the digital forensics lab.

5. References

- *Capital one breach latest example of cybersecurity realities*. (2021, April 23). GovTech. https://www.govtech.com/security/capital-one-breach-latest-example-of-cybersecurity-realities.html

- Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. https://doi.org/10.6028/nist.sp.800-86

- Priede, J. (2012). Implementation of quality management system ISO 9001 in the world and its strategic necessity. *Procedia - Social and Behavioral Sciences*, 58, 1466-1475. https://doi.org/10.1016/j.sbspro.2012.09.1133

- M Reith; C Carr; G Gunsch (2002). "An examination of digital forensic models". International Journal of Digital Evidence. CiteSeerX 10.1.1.13.9683.

- Nelson, B., Phillips, A., & Steuart, C. (2014). *Guide to computer forensics and investigations*. Cengage Learning

- Hayes, D. R. (2020). *Practical Guide to Digital Forensics Investigations*. Pearson It Certification.

- (2022, August 11). ASCLD. https://www.ascld.org/

- Monteiro Bastos da Silva, J., Chaker, J., Martail, A., Costa Moreira, J., David, A., & Le Bot, B. (2021). Improving Exposure Assessment Using Non-Targeted and Suspect Screening: The ISO/IEC 17025: 2017 Quality Standard as a Guideline. *Journal of xenobiotics*, *11*(1), 1–15. https://doi.org/10.3390/jox11010001

- Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *digital investigation*, *7*, S64-S73.
- Lin, I. L., Yen, Y. S., & Chang, A. (2011, June). A study on digital forensics standard operation procedure for wireless cybercrime. In *2011 Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing* (pp. 543-548). IEEE.