APPLIED DIGITAL FORENSICS:
A SCENARIO-DRIVEN INVESTIGATION FRAMEWORK

Yosief Araya

WELLINGTON INSTITUTE OF TECHNOLOGY

27/08/2023

Table of Contents

Introduction: 2
Description Of Selected Methodology: 3
Applying The Chosen Methodology to The Case Study: 5
Digital forensic tools used during the examination phase: 6
What is a case summary and What Should It Contain? 8
Case Summary of The Given Case Study: 9
Conclusion: 11
References 11

Introduction:

Digital forensic is part of forensic discipline that absolutely covers crime that is related to computer technology (Dhwaniket Ramesh Kamble, & Nilakshi Jain, 02, February 2015). In today's digitally interconnected world, digital forensics has been determined as a modern method of preserving, collecting, examining, analyzing, reporting, and presentation of digital evidence extracted from both electronic and digital sources for the purpose of facilitating the reconstruction of incidents to be useful to solve a cybercrime or anticipate unauthorized activities that identified as undisciplined or illegal. Because of the widespread access to technology today, it is unavoidable that digital forensics has become an essential part of a criminal investigation. Digital evidence involves data from but is not limited to computers, cell phones, digital audio, digital video, emails, social media platforms, and printers. This report will provide a comprehensive digital forensic investigation methodology applied to solve a given case study that involves investigating a small business in relation to a card skimming crime that arose from a parcel intercepted by Customs, containing card skimming equipment, addressed to one of the staff members. The police plan to arrest the staff member after the package delivery. None of the staff have criminal records, some have travelled overseas, and one staff member is studying Information Technology

In this hypothetical case study, a forensic investigation technician is employed to examine a small business as part of a card-skimming equipment investigation. The business has six staff members in an open-plan office with four shared desktop machines, a router/modem for wireless and wired internet connection, and a dedicated office for the manager. The owner is hands-off the business, therefore owner's offsite computer is not within the scope.

This report will consist of five major sections that involve the discussion of the chosen methodology and clarity of phases in the methodology, a discussion of findings and tools for each phase, a discussion of what a case summary is and should contain, and case summary information relevant to the case study for the given case study, and overall review and conclusion of the case study.

Description Of Selected Methodology:

The "7 Phase Methodology" for digital forensics is the chosen method for this case's investigation. This methodology covers the following phases: Identification, Preservation, Collection, Examination, analysis, reporting, and Presentation, which aligns well with this given case and gives a structured approach to ensure the integrity of electronic evidence. This methodology will address the given case investigation by incrementing the process into phase and each phase has a clear and precise activity to assist in solving the given case investigation.

A. Identification: This phase describes the range of the investigation and defines the goals. The objective is to identify possible electronic evidence sources and establish the appropriate approach. The focus is to understand the business environment, network structure, and locations of all hardware and software devices connected to the crime scene.
B. Preservation: At this stage, the responsible team reaches to the crime location and freezes the whole spot completely (Umesh Kumar Singh, Neha Gaud, & Chanchala Joshi, November 2016). The preservation phase involves securing the digital evidence to protect it from any alteration or destruction to the original data. It ensures the separation of the crime scene premises by restricting physical and network access to any hardware and software electronic device that is a potential source of evidence.

C. Collection: This phase performs the collection of different electronic and digital evidence while maintaining the integrity of the data. It focuses on acquiring data from all hardware and software machines of the potential source of evidence such as:

Internet**:** From wired and wireless networks, emails, and social networking accounts, including data gathered from router/modem with collaboration from the internet service provider.

Standalone Devices: All data stored in any machines, like computers, servers, printers, scanners, modems, hard disks, SSD, USB, networks, and power cables.

Mobile Device: Focuses on collecting data from smartphones' internet activities such as internet browsing history, social media communications, content cookies, pictures, videos, and audio files, and mobile phone's internal storage.

D. Examination Phase: The examination phase of a digital report involves the findings and key events of a comprehensive investigation into a piece of digital evidence related to a specific incident. The main purpose of the phase is to uncover and analyze different digital devices to support in the investigation process and provide valuable evidence. The examination task involves the acquisition and analysis of digital evidence using specialized forensic tools and techniques. The phase outlines the methodologies applied for evidence acquisition such as recovering, examining, and scanning an email or any other communication tools correspondence, among staff members or any other external

stakeholders, analyzing user activity logs to find suspicious behavior, Examining files and other documents for potential involvement with the case, Analysing forensic imaging of storage, and capturing network traffic, while ensuring the preservation and integrity of the potential digital evidence throughout the investigation. This includes keyword searches, data carving to extract fragmented, stagnated, or deleted files, and forensic artifact analysis to identify potential evidence.

Finally, a timeline analysis will be conducted to establish the sequence of events examination for valuable information and reconstruct the evidence for the investigation case.

E. Reporting Phase: The report provides the critical and technical closure that investigators need when the case investigation ends, and the evidence is presented to the court. The digital forensic report consists of various sections that should capture the case summary, tools, techniques used, brief evidence summary, analysis, and recommendation required for a case. All the findings of the examination and analyzing phases will be presented in a comprehensive report that will detail the identified evidence, and the examination process, and the conclusions will be presented by a forensic accountant.

F. Presentation Phase: Based on the presentation report, a decision is made regarding the person to whom the incident can be attributed. The decision must be recorded in some database for future reference. All other relevant documentation that was compiled during the investigation and that might be relevant in reaching a decision is included in the final presentation report (Dhwaniket Ramesh Kamble, & Nilakshi Jain, 02, February 2015). This final stage involves presenting the findings in a clear and understandable manner. A comprehensive case summary that details the entire investigation process, findings, tools, techniques used in the process, and the result of the analysis will be prepared and presented for legal court prosecution.

Applying The Chosen Methodology to The Case Study:

A.Identification: In this case, the identification phase will be applied to:

- Understand the business's network architecture including the manager's office and staff shared desktops, network printer's fax, printing and copying activities, router/modem's wireless and wired connection, company-provided smartphones, and external storage devices.
- Identify, each employee's role, and their prospective access to digital resources.
- Identifying and understanding the skills and capacity that the IT student staff member has in relation to information security and anti-forensic tools and techniques.
- Excluding the owner's remote computer from the investigation scope.

B. Preservation: Therefore, in this stage, the preservation phase will be used to Secure the crime premises to prevent alteration and destruction of potential digital evidence and ensure its integrity. The manager's computer and staff members' shared desktop machines, the router/modem, and the network printer should be secured to avoid unauthorized access. Scan and monitor the flow of network traffic to identify any suspicious activities. Staff members will be asked to hand in company-provided smartphones, backup USB stick, and hard drives.

C. Collection: This phase involves collecting volatile and non-volatile data from the manager's office computer and shared desktop machines, collecting router/modem network logs, to track staff members' internal and external communication, and staff members' personal and company-provided smartphones, USB sticks, or external hard drives, will be collected for examination.

During The collection phase, hardware and software write blocker tools are used to ensure that the original data on the device is not being altered or distracted during the collection process.

Forensic imaging software such as EnCase FORENSIC and FTK Imager are used to create a bit-by-bit forensic image of the device that is being investigated. Data recovery software such as Recuva and EaseUS Data Recovery Wizard are used to recover deleted files and folders.

In maintaining integrity, hash values are used to ensure that the forensic image created during the collection phase has not been altered. Hash values are unique identifiers that are generated based on the contents of the file or device being investigated. If the hash value of the forensic image matches the hash value of the origin, it means the data or device has not been altered.

D. Examination Phase: During this stage, all collected data will be analyzed to find any relevant evidence. Communication patterns can be revealed from Network logs during the examination., Any remote access or data manipulation activities on the shared desktops must be investigated. Even though the postgraduate IT student staff member is not the recipient of the parcel, he might be relevant in case his knowledge and skills were used in the process of card skimming. Analyze email correspondence between staff members and external entities, examine user activity logs to trace any unusual behavior or unauthorized access, and search documents and files for evidence of involvement in card skimming activities. printer logs will also be analyzed to identify any suspicious print jobs. Backup USB drives and external hard drives of staff members and company-provided Smartphones for staff members will be examined as well.

digital forensic tools used during the examination phase:

Digital forensics tools play a critical role in providing reliable computer analysis and digital evidence collection to serve a variety of legal and industry purposes. These tools are typically used to conduct investigations of computer crimes by identifying evidence that can be used in a court of law (Dhwaniket Ramesh Kamble, & Nilakshi Jain, 02, February 2015).

- Autopsy, X-ways Forensics, and Sleuth Kit will help to do both dead analysis and live analysis of disk images, recover deleted files, search for specific keywords, and recover files from various file systems.
- Data carving tools such as Foremost and Scalpel will also be used to recover files that have been deleted or damaged.
- Timeline analysis tools such as Log2Timeline and Plaso are also used to create a timeline of events based on the collected data.
- EnCase will also be used to perform an in-depth analysis of various file systems, email formats, and mobile electronic evidence.
- Autopsy will attempt to crack the passwords for the protected files during the analysis phase with the help of tools like John the Ripper or Hashcat for password cracking.
- QXYGEN FORENSIC SUITE will be used to investigate company-provided smartphones. This tool will enable reading information from phones, including SIM card data, incoming and outgoing calls, pictures, videos, audio files, SMS messages, MMS messages, and other files from the phone memory or any other memory cards inserted into the smartphone.

  All these above tools will be helpful in identifying suspicious files, and uncovering hidden information, by conducting a comprehensive analysis.

E. Analysis Phase: After the examination phase, forensic accountants will begin connecting all the evidence dots to reconstruct events. This investigation will focus on creating a timeline of actions related to the intercepted parcel. Trying to connect the recipient's history (such as IT studying and overseas travelled staff members) with the scheme can provide insight into their motive or involvement with the crime.

F. Reporting Phase: During this report outlines the findings, investigation methodology, and conclusions will be provided by a forensic accountant. The report must address if the intercepted parcel points to a wider scheme, who might be involved, and if there are any signs of collaboration or innocent evidence related to a staff member has to be presented.

G. Presentation Phase: All findings are presented to all parties who are involved in this case (such as law enforcement and criminal justice). The presentation should be clear and well organized to indicate the connection between the intercepted parcel, evidence, potential motive, or any insights of the suspect's activity.

What is a case summary and What Should It Contain?

A case summary in a digital forensic investigation is a detailed and well-organized document that provides a summary of the entire investigation. It assists in understanding the picture of the whole investigation, key players, legal process, findings, and application of the investigation methodology. A well-prepared case summary in a digital forensic process should include:

Case Information: includes the name, date, and unique identifier of the investigated case.

Scope of investigation: Discuss the specific goal and objectives of the investigation. It indicates the scope of the investigation, and what the digital forensic accountant aimed to accomplish.

Methodology: Explain the digital forensic methodology used during the investigation process, and mention software and hardware tools utilized during data preservation, evidence collection, and data analyzing.

Key Events: Outlines the significant events, activities, and findings that were reached during an investigation.

Evidence: provides a list of digital and electronic evidence that was found during the examination process of the investigation, including computers, smartphones, network logs, external storage, and other relevant evidence**.**

Case Summary of The Given Case Study:

The case summary contains several key pieces of information relevant to the digital forensics' investigation:

1. **Business infrastructure:** The crime scene is a small business with an open-plan office containing four shared desktop machines.
- There is a dedicated office for the manager, which is likely to contain sensitive information.
2. **Owner's Involvement:** The owner of the business is hands-off and does not frequently visit the premises unless there's a significant issue.
- The owner's computer which is located offsite is not within the scope of the investigation.
3. **Network Infrastructure:** There is a router/modem providing both wireless and wired connectivity to the business premises.
- A modern business printer with network functionality (fax and copier) is present and considered part of the business's network.
4. **Staff and Access:** There are six staff members (part-time and full-time) sharing the desktop machines in the open-plan office.
- The manager has access to all the desktop machines.
- Staff members each have a backup device (USB stick or external USB hard drive) kept on-site or with them.
5. **Owner's Oversight:**
- The manager sends a monthly report to the owner, who can audit it off the business premises.
- Customers do not have access to the open plan office area or the manager's office.
- Customers are not relevant to the investigation.
6. **Intercepted Parcel:**
- Customs intercepted a parcel containing card skimming equipment addressed to one of the staff members at the business's address.
7. **Police Involvement:**
- The police are alerted to the intercepted parcel and have put the business under surveillance.
- The plan is to arrest the staff member after the parcel is delivered to the business.
8. **Suspect Profiles:**
- None of the staff members have prior criminal convictions.
- Some staff members have travelled overseas before January 2020.
- One staff member is studying a postgraduate qualification in Information Technology. However, he/she was not the recipient of the intercepted parcel.
9. **Mobile Devices:** The company-provided cell phones/smartphones for staff members.

10. **Owner's Status:** The owner is not under suspicion and seems unrelated to the intercepted parcel.

These pieces of information collectively set the stage for the digital forensics investigation by defining the scope, potential evidence sources, and the context within which the crime occurred. Digital forensic accountants can use this information to plan their approach, prioritize evidence collection, and prepare assumptions about the events leading up to the

intercepted parcel and the potential involvement of any internal or external individuals associated with the business.

Conclusion:

In this report, we have outlined a comprehensive methodology for conducting a digital forensic investigation in a small business setting. By selecting the "7 Phase Methodology," we have provided a structured approach to identifying, preserving, collecting, examining, analyzing, reporting, and presenting digital evidence. Applying this methodology to the provided case study allows us to discover potential evidence related to card skimming activities and present findings in a consistent and organized manner.

References

Asia ALJAHDALI, Nawal ALSAIDI, Maram ALSAFRI, Afnan ALSULAMI, Turkia ALMUTAIRI. (2021). Mobile device forensics. *Romanian Journal of Information Technology and Automatic Control*, 16. Retrieved from https://rria.ici.ro/wp-content/uploads/2021/09/art._Aljahdali_Alsaidi_Alsafri....pdf

Dhwaniket Ramesh Kamble, & Nilakshi Jain. (02, February 2015). DIGITAL FORENSIC TOOLS: A COMPARATIVE APPROACH. *International Journal of Advance Research In Science And Engineering*, 12. Retrieved from https://embeddedsw.net/doc/Openpuff_paper_Digital_forensic_tools_a_comparative_approach.pdf

Fernando Tiverio Molina Granja, & Glen D. Rodríguez Rafael. (2, 2017). Model for digital evidence preservation in criminal research institutions – PREDECI. *Int. J. Electronic Security and Digital Forensics*, 17. Retrieved from https://d1wqtxts1xzle7.cloudfront.net/88907679/IJESDF.2017.08398920220724-1-x32tma-libre.pdf?1658624765=&response-content-disposition=inline%3B+filename%3DModel_for_digital_evidence_preservation.pdf&Expires=1693131702&Signature=cQsuvEut-NDedBMaXkKozOdg8JY

Umesh Kumar Singh, Neha Gaud, & Chanchala Joshi. (November 2016). A Framework for Digital Forensic Investigation using Authentication Technique to maintain Evidence Integrity. *International Journal of Computer Applications ·*, 4. Retrieved from (PDF) A Framework for Digital Forensic Investigation using Authentication Technique to maintain Evidence Integrity (researchgate.net)