VOL. 05 NO. 9,
FEBRUARY, 2025
E-ISSN 3026-958X
P-ISSN 3027-1169

African Scholar Publications & Research International
www.africanscholarpub.com

Journal of Science Innovation & Technology Research (JSITR)

An Overview of Digital Forensics Investigations and Threat Intelligence Tools

[1]Kareem, A.E.A, [2]Oduwole, O.A, [1]Akano, I.A & [3]Womiloju, A.A

[1]Department of Cybersecurity, University of Ilesa, Ilesa, Osun State, Nigeria. [2]Department of Computer Science, University of Ilesa, Ilesa, Osun State, Nigeria. [3]Department of Software Engineering, University of Ilesa, Ilesa, Osun State, Nigeria.

Corresponding Author: emiolafoye@gmail.com
DOI: https://doi.org/10.70382/ajsitr.v7i9.007

Abstract

This paper provides a comprehensive overview of digital forensics investigations and the tools utilized in threat intelligence. As cyber threats become increasingly sophisticated, the need for effective forensic methods to analyze and respond to these threats has grown significantly. We explore various digital forensics techniques, including data acquisition, analysis, and preservation, as well as the integration of these techniques into threat intelligence frameworks. Additionally, we examine a range of tools available for digital forensics, assessing their effectiveness in enhancing investigative processes and supporting decision-making during incidents. The findings underscore the importance of digital forensics in developing robust cybersecurity strategies and highlight areas for future research and improvement in the field.

Keywords: Digital forensics, Digital forensics tools, Threat intelligence, Cybersecurity investigations, Forensic analysis techniques

Introduction

In an era where digital interactions form the backbone of personal, corporate, and governmental operations, the rise of cybercrime poses significant challenges. Digital forensics, the science of collecting, preserving, and analyzing digital evidence, serves as a vital mechanism in combating these threats (Johnson et al., 2023). This paper aims to explore the intersection of digital forensics and threat intelligence, reviewing current investigations and tools that facilitate their integration. Digital forensics or digital forensic science is a branch of forensic science focused on the recovery and investigation of material found in digital devices and cybercrimes. Digital forensics was originally used as a synonym for computer forensics but has expanded to cover the investigation of all devices that store digital data (Aljawarneh & Alzahrani, 2023).

As society increases reliance on computer systems and cloud computing, digital forensics becomes a crucial aspect of law enforcement agencies and businesses. Digital forensics is concerned with the identification, preservation, examination and analysis of digital evidence, using scientifically accepted and validated processes, to be used in and outside of a court of law (Johnson et al., 2023). While its root stretch back to the personal computing revolution in the late 1970s, digital forensics begun to take shape in the 1990s and it wasn't until the early 21st century that countries like the United States begun rolling out nation-wide policies. Traditionally, digital forensics practitioners came from a general computer science background, were experienced sys admins who were comfortable with many of the tools used in digital forensics, or they learnt on the job in an apprentice model.

Purpose of Digital Forensics

Digital forensics is crucial for a variety of reasons:

i. It enables law enforcement to gather evidence for criminal investigations.
ii. It supports organizations in understanding the root causes of a security breach.
iii. It aids in compliance and regulatory investigations.

The most common use of digital forensics is to support or refute a hypothesis in a criminal or civil court. Digital forensics experts are also hired by the private sector as part of cybersecurity and information security teams to identify the cause

of data breaches, data leaks, cyber attacks and other cyber threats (Kebande, 2021). Digital forensic analysis may also be part of incident response to help recover or identify any sensitive data or personally identifiable information that was lost or stolen in a cybercrime (Younis, 2021).

Digital forensics is used in both criminal and private investigations (Greene & Stuckey, 2023). Traditionally, it is associated with criminal law where evidence is collected to support or negate a hypothesis before the court. Collected evidence may be used as part of intelligence gathering or to locate, identify or halt other crimes. As a result, data gathered may be held to a less strict standard than traditional forensics. In civil cases, digital forensics may help with electronic discovery. A common example is following unauthorized network intrusion. A forensics examiner will attempt to understand the nature and extent of the attack, as well as try to identify the attacker. As encryption becomes more widespread, forensic investigation becomes harder, due to the limited laws compelling individuals to disclose encryption keys (Greene & Stuckey, 2023).

Branches of Digital Forensics

Today, the technical aspect of an investigation is divided into five branches that encompass the seizure, forensic imaging and analysis of digital media. Digital forensics is no longer synonymous with computer forensics (Casey, 2023). It is increasingly concerned with data from other digital devices such as tablets, smartphones, flash drives and even cloud computing.

In general, we can break digital forensics into five branches:

1. Computer Forensics: Computer forensics or computer forensic science is a branch of digital forensics concerned with evidence found in computers and digital storage media. The goal of computer forensics is to examine digital data with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information (Khan & Qureshi, 2023).

   It is used in both computer crime and civil proceedings. The discipline has similar techniques and principles to data recovery, with additional guidelines and practices designed to create a legal audit trail with a clear chain of custody. Evidence from computer forensics investigations is subjected to the same guidelines and practices of other digital evidence.
2. Mobile Device Forensics:Mobile device forensics is a branch of digital forensics focused on the recovery of digital evidence from mobile devices

using forensically sound methods (Khan & Qureshi, 2023). While the phrase mobile device generally refers to mobile phones, it can relate to any device that has internal memory and communication ability including PDA devices, GPS devices and tablets. While the use of mobile phones in crime has been widely recognized for years, the forensic study of mobile phones is a new field, beginning in the late 1990s.

The growing need for mobile device forensics is driven by:

- Use of mobile phones to store and transmit personal and corporate information
- Use of mobile phones in online transactions

Mobile device forensics is particularly challenging due to:

- Evidential and technical challenges such as cell site analysis which makes it possible to determine roughly the cell site zone from which a call was made or received but not a specific location such as an address
- Changes in mobile phone form factors, operating systems, data storage, services, peripherals and even pin connectors and cables
- Storage capacity growth
- Their proprietary nature
- Hibernation behavior where processes are suspended when the device is off or idle

As a result of these challenges, many tools exist to extract evidence from mobile devices. But no one tool or method can acquire all evidence from all devices. This has forced forensic examiners, especially those who wish to be expert witnesses, to undergo extensive training to understand how each tool and method acquires evidence, how it maintains forensic soundness and how it meets legal requirements.

3. Network Forensics: Network forensics is a branch of digital forensics focused on monitoring and analyzing computer network traffic for information gathering, legal evidence or intrusion detection (Le-Khac et al., 2018). Unlike other branches of digital forensics, network data is volatile and dynamic. Once transmitted, it is gone so network forensics is often a proactive investigation. Network forensics has two general uses:
   i. Monitoring a network for anomalous traffic and identifying intrusions.
   ii. Law enforcement may analyze capture network traffic as part of criminal investigations.
4. Forensic Data Analysis: Forensic Data Analysis (FDA) is a branch of digital

forensics that examines structured data in regards to incidents of financial crime. The aim is to discover and analyze patterns of fraudulent activities. Structured data is data from application systems or their databases. This can be contrasted to unstructured data that is taken from communication, office applications and mobile devices. Unstructured data has no overarching structure and analysis therefore means applying keywords or mapping patterns. Analysis of unstructured data is usually done by computer forensics or mobile device forensics experts (Le-Khac et al., 2018), (Wang & Hu, 2023).

5. Database Forensics: Database forensics is a branch of digital forensics related to databases and their related metadata. Cached information may also exist in a server's RAM requiring live analysis techniques (Wang & Hu, 2023). A forensic examination of a database may relate to timestamps that apply to the update time of a row in a relational database that is being inspected and tested for validity to verify the actions of a database user. Alternatively, it may focus on identifying transactions within a database or application that indicate evidence of wrongdoing, such as fraud (Khan & Qureshi, 2023).

Threat Intelligence

Threat intelligence refers to the collection and analysis of information regarding current and potential threats to an organization's security posture. This intelligence is essential for identifying vulnerabilities, understanding attack vectors, and preparing for future threats.

Types of Threat Intelligence

- Strategic Intelligence: Provides high-level insights for decision-makers regarding broad trends in cyber threats.
- Tactical Intelligence: Involves specific, actionable information on imminent threats.
- Operational Intelligence: Focuses on understanding the tactics, techniques, and procedures (TTPs) used by adversaries.

Integration of Digital Forensics and Threat Intelligence

The integration of digital forensics and threat intelligence enhances an organization’s ability to respond to incidents proactively. Forensic investigations can provide

valuable context for understanding threats, improving the overall efficacy of threat intelligence gathered. Various case studies illustrate the successful integration of digital forensics into threat intelligence frameworks, showcasing the streamlined processes that lead to more efficient investigations and informed decision-making.

Digital Forensics Investigation Process

There are a number of process models for digital forensics, which define how forensic examiners should gather, process and analyze data. That said, digital forensics investigations commonly consist of four stages (Greene & Stuckey, 2023):

1. Data collection/Seizure: Prior to actual examination, digital media is seized. In this process, data is identified and collected for investigation.
2. Data Examination: In the second step the collected data is examined carefully.
3. Data Analysis: In this process, different tools and techniques are used and the collected evidence is analyzed to reach some conclusion.
4. Evidence Reporting: In this final step all the documentation and reports are compiled so that they can be submitted in court.

Digital Evidence Collection Process

1. Describe the scenario
    a. Data Breach
2. Define the scope
    a. Computer
    b. Mobile
    c. Cloud
    d. Network
    e. Other
3. Formulate a crime hypothesis – label the crime and identify the perpetrators
4. Define Investigation Objective & Select appropriate tool
    a. **Objective-1:** Evidence Collection & Preservation
        i. Activity: Acquire forensic image of the computer systems and logs.
        ii. Tool:
    b. **Objective-2:** Evidence/Data Examination
        i. Activity-1: Extract relevant data like user files,

logs, and browser history

ii. Tool-1: Autopsy, Scalpel and Foremost

iii. Activity-2: Recovering deleted files and uncovering hidden activity

iv. Tool-2:

v. Activity-3: Timeline Construction

vi. Tools-3: Employee log2timeline

c. **Objective-3:** Evidence/Data Analysis

i. Activity:
Identify malicious files
Identify evidence of data exfiltration Identify indications of compromise (IOC)
Identify the source of the attack (ip addresses, email addresses, etc.)

ii. Tool:

iii. Activity-2: Volatile Memory Analysis

iv. Activity-3: Analyse network traffic with Wireshark to identify suspicious connections, data exfiltration attempts, and potential accomplices

d. **Objective-4:** Evidence Reporting

i. Activity:
Summarise the incident
Summarise the evidence Provide conclusions

ii. Tool:

Digital Forensics Tools

In the 1980s, very few digital forensic tools existed forcing forensic investigators to perform live analysis, using existing sys-admin tools to extract evidence. This carried the risk of modifying data on the disk which led to claims of evidence tampering (Kebande, 2021). The need for software to address this problem was

first recognized in 1989 at the Federal Law Enforcement Training Center and resulted in the creation of IMDUMP and SafeBack. These tools create an exact copy of a piece of digital media to work on while leaving the original disk intact for verification. By the end of the 1990s, the demand for digital evidence meant more advanced tools such as EnCase and FTK were developed, allowing analysts to examine copies of media without live forensics. There is now a trend towards live memory forensics using tools such as WindowsSCOPE and tools for mobile devices. Today, there are single-purpose open-source tools like Wireshark, a packet sniffer, and HashKeeper, a tool to speed up examination of database files. As well as commercial platforms with multiple functions and reporting capabilities like Encase or CAINE, an entire Linux distribution designed for forensics programs (Kebande, 2021).

In general tools can be broken down into the following categories:

1. Disk Imaging and Analysis:
    a. Guymager: Efficient forensic image capture and analysis tool (Linux).
    b. FTK Imager
2. Hashing Tools
    a. Get-FileHash – Windows
    Get-FileHash "filename" -algorithm MD5
    b. sha1sum/sha256sum/md5sum – CSI Linux
3. File Recovery and Analysis:
    a. Photo Rec: Recovers lost files from a variety of media types.
    b. Foremost: Recovers files based on headers, footers, and internal data structures.
    c. Scalpel: High-performance file carving tool for targeted data extraction.
4. Data Analysis and Visualization:
    a. Autopsy: Open-Source, graphical interface for examining disk images and file systems.
    b. Sleuth Kit: Collection of command-line tools for file system analysis, data recovery and investigation.
    c. Log2timeline: Creates a timeline of events from various log files.
    d. bulk_extractor: Extracts information such as email addresses, credit-card numbers and histograms from disk images
5. Memory Analysis:

a. Volatility: Framework for volatile memory analysis.
b. Redline: Malware analysis tool with memory forensics capabilities.

6. Network Forensics:
    a. Wireshark: Network traffic analyser for capturing and inspecting packets.
    b. Network Miner: Tools for extracting files and network events from packet captures.
7. Malware Analysis:
    a. Cuckoo Sandbox: Automated malware analysis system.
    b. Viper: Binary analysis framework for malware identification and characterization.
8. Social media analysis
    a. Maltego Tools: Link analysis tool for visualizing relationships between entities.
    b. Twint Tools: Advanced Twitter scraping tool for collecting user data and tweets.
9. Password Cracking
    a. John the Ripper: Password cracking tool for various hash types.
    b. Hash cat: Advanced password recovery tool with high-performance cracking capabilities.
10. Encryption and Decryption:
    a. GnuPG: Open-Source implementation of the OpenPGP standard for encrypting and signing data.
    b. TrueCrypt: Tool for creating encrypted volumes for data protection.

Challenges of Digital Forensics Investigations

Digital forensics investigations and threat intelligence face overlapping and distinct challenges:

1. Data Volume and Complexity: The exponential growth of data, across various devices and cloud platforms, makes identifying relevant evidence time-consuming and resource-intensive. Data formats and encryption further complicate analysis.
2. Acquisition Challenges: Preserving evidence integrity during acquisition, especially from remote or volatile systems, is critical but technically demanding. Legal and jurisdictional issues can hinder access.

3. Expertise Gap: A shortage of skilled digital forensic examiners exists. The field demands constant learning due to rapidly evolving technologies and attacker techniques.
4. Legal and Ethical Considerations: Navigating legal requirements for evidence admissibility, privacy regulations, and ethical boundaries can be complex and time-consuming.
6. Anti-Forensics Techniques: Threat actors employ techniques to hide, destroy, or obscure their actions, making it difficult to reconstruct events and identify perpetrators.

Challenges of Threat Intelligence

1. Data Overload and Noise: The sheer volume of threat data, from multiple sources, presents a noise problem. Differentiating actionable intelligence from irrelevant information is critical.
2. Data Accuracy and Reliability: Intelligence sources can vary in accuracy and reliability. Validating and verifying information from various sources is essential to avoid false positives.
3. Timeliness: Threat intelligence becomes less valuable over time. Staying current with the evolving threat landscape, especially emerging threat, is crucial.
4. Integration and Automation: Seamless integration with security tools (SIEMs, firewalls, etc.) is essential for effective threat detection and response. Automated analysis and correlation of threat intelligence is critical.
5. Contextualization and Actionability: Raw threat data needs to be contextualized to provide meaningful insights for specific organizations. Converting intelligence into actionable steps for prevention, detection, and response is a key challenge.

The Legal Considerations of Digital Forensics and Nigeria Perspectives

The examination of digital media is covered by national and international legislation. For civil investigations, laws may restrict what can be examined. Restrictions against network monitoring or reading personal communications are common (Sadeghi & Wachsmann, 2023). Likewise, criminal investigations may be restricted by national laws that dictate how much information can be seized. As an example, seizure of evidence by law enforcement is governed by the PACE act in the United Kingdom. The 1990 computer misuse act legislates against

unauthorized access to computer material which makes it hard for civil investigators in the UK.

Digital evidence falls into the same legal guidelines as other evidence. In general, laws dealing with digital evidence are concerned with:

- Integrity: Ensuring the act of seizing and acquiring digital media does not modify the evidence (either the original or the copy).
- Authenticity: The ability to confirm the integrity of information. The chain of custody from crime scene through analysis and ultimately to the court, in the form of an audit trail, is an important part of establishing the authenticity of evidence.

Each of the branches of digital forensics has its own guidelines on how to conduct investigations and handle data.

The legal considerations of digital forensics in Nigeria encompass various aspects, including legislation, privacy rights, evidence collection, and the admissibility of digital evidence in court. These considerations are crucial due to the growing significance of digital evidence in criminal investigations and civil litigation. Here's an overview of key legal aspects pertinent to digital forensics in Nigeria (Johnson et al., 2023).

i. Legal Frameworks: Cybercrime (Prohibition, Prevention, etc.) Act, 2015: This legislation addresses various cybercrimes and includes provisions for the investigation and prosecution of offenses involving digital evidence. It provides the legal basis for digital forensics practices, ensuring that such evidence is admissible in court.
ii. Evidence Act, 2011: The Act stipulates how evidence should be collected and presented in Nigerian courts. It sets rules regarding the admissibility of electronic evidence, including the requirement of proper chain-of-custody practices to ensure authenticity.
iii. Chain of Custody: Maintaining a proper chain of custody is critical in digital forensics. It helps ensure that the evidence collected is preserved in its original state and remains unaltered. This process is vital for establishing the credibility of the evidence in legal proceedings.
iv. Privacy and Data Protection: The National Information Technology Development Agency (NITDA) Act 2007, along with the Data Protection Bill, outlines the responsibilities of data handlers concerning the protection of personal data. Forensic experts must navigate these laws carefully to

avoid infringing on individuals' privacy rights while conducting investigations.

v. Admissibility of Digital Evidence: Courts in Nigeria recognize electronic evidence, provided it meets certain standards of reliability and authenticity. Under the Evidence Act, electronic documents must be shown to be the original record and must be relevant to the matter being considered.

vi. Interagency Cooperation: Effective digital forensics often requires collaboration among various law enforcement agencies, both nationally and internationally. The need for a coordinated legal approach is particularly important given the transnational nature of many cybercrimes.

vii. Professional Standards and Ethics: Digital forensics practitioners in Nigeria need to adhere to ethical guidelines and professional standards. Best practices for evidence collection, analysis, and presentation must be followed to ensure that outcomes are accepted by courts and legal authorities.

viii. Training and Capacity Building: There is an ongoing need for training law enforcement, legal practitioners, and forensic experts in digital forensics. Enhanced skills and knowledge are necessary to keep up with rapidly evolving technology and cybercrime methods.

ix. Judicial Perception: Judges and legal practitioners must be educated about digital forensics to understand technical evidence properly. Good judicial understanding helps in making informed decisions regarding the admissibility and weight of digital evidence.

Jobs Availability in Digital Forensics

Jobs in digital forensics have titles like investigator, technician or analyst depending on specialization and seniority, with the majority of jobs in the public sector such as law enforcement, state or national agencies or crime labs (Johnson et al., 2023). That said, due to increasing cybersecurity risk, many organization are hiring their own digital forensic specialists to help prevent and identify the causes of cyber attacks. Increasing usage of third-party vendors means cybersecurity has never been more important. Digital forensics may also help with vendor risk management and third-party risk management. Third-party risk and fourth-party risk have never been higher. And it's a pretty lucrative career path (Bourgeois & Miller, 2023).

Conclusion

The paper has highlighted the critical role of digital forensics in enhancing threat intelligence and improving cybersecurity measures. As cyber threats continue to evolve in complexity and scale, the integration of advanced forensic tools and methodologies is essential for identifying, analyzing, and mitigating such threats effectively. By fostering collaboration between cybersecurity professionals and digital forensics experts, organizations can strengthen their defensive strategies and respond more swiftly to incidents. Continued research and development in this field will be paramount in addressing future challenges and ensuring a robust response to the ever-changing landscape of cyber threats.

REFERENCES

Aljawarneh, S., & Alzahrani, A. (2023). Digital Forensics and Its Role in Incident Investigation. Journal of Forensic Sciences, 68(4), 1578-1585.

Bourgeois, R. Y., & Miller, R. W. (2023). Advancements in Mobile Forensics: Addressing Emerging Technologies. International Journal of Digital Crime and Forensics, 15(2), 1-22.

Casey, E. (2023). Digital Forensics and Cybersecurity: Leveraging Interdisciplinary Approaches. Journal of Digital Forensics, Security and Law, 18(1), 1-16.

Greene, K. R., & Stuckey, J. (2023). Cybercrime Investigation and Digital Forensics: An Integrated Approach. Journal of Forensic Sciences, 68(4), 1230-1245.

Johnson, O. A, Kareem, A.E & Allen, A.A. (2023). Understanding the Fundamentals of Digital Forensic. International Journal of Science Research and Technology: Timbou-Africa Academic Publications. 13 (9). 201-206

Kebande, V. R. (2021). Digital forensic readiness intelligence repository. Journal of Cyber Security and Mobility, 10(1), 19-36.

Khan, N., & Qureshi, M. (2023). Foundations of Digital Forensics: An Overview of Key Concepts and Techniques. International Journal of Information Security, 22(3), 273-290.

Le-Khac, N. A., Mark, Y. L., & Choo, K. K. R. (2018). A proactive approach to forensic readiness: Forensic-by-design. Future Generation Computer Systems, 80, 103-115.

Nickson, R., & Victor, P. (2018). Challenges in modern digital forensics: Bridging the gap between theory and practice. Journal of Cybersecurity Research, 10(2), 67-84.

Sadeghi, A., & Wachsmann, C. (2023). Understanding Digital Forensics in the Context of Cyber Crime. International Journal of Cybersecurity Intelligence and Cybercrime, 3(2), 45-60.

Wang, X., & Hu, J. (2023). Digital Forensics in the Age of Cloud Computing. Journal of Computer Virology and Hacking Techniques, 19(2), 101-120.

Younis, M. (2021). Collaborative digital forensics and incident response framework. Cyber Security and Mobility Journal, 10(2), 125-138.