A Review: Digital Forensics Management System

Prof. Mirza Moiz Baig
Shreya Urkude , Shreya Wagh , Suraj Sirse

HOD, Department of Information Technology Engineering , JD Engineering College, Fetri Nagpur, Maharashtra , India
U.G. Student , Department of Information Technology Engineering, JD Engineering College, Fetri Nagpur, Maharashtra , India

Abstract: Digital forensics is critical in cybercrime investigations, but technological advancements present challenges for law enforcement. Ensuring data integrity, security, and accuracy requires robust management systems. This case study introduces a **Digital Forensic Case Management System (DFCMS)** designed to streamline case tracking, forensic analysis, and operational efficiency. The framework includes evidence verification, chain of custody control, task delegation, and progress monitoring, providing investigators with a centralized platform. By minimizing human error and speeding up processes, DFCMS enhances accuracy and efficiency. The study explores its design, key features, security measures, and real-world evaluation, demonstrating its potential to improve accountability and effectiveness in digital investigations. DFCMS offers a secure, efficient, and legally compliant solution for modern forensic challenges.

Keywords: Digital Forensics, Forensic Management System, Cybercrime, Evidence Integrity, Digital Investigations, Chain of Custody

I.Introduction

The increasing dependence of society on digital technology has led to the emergence of digital forensics as a crucial element in modern crime investigations. There is increasing pressure on investigative agencies to carry out comprehensive, safe, and systematic digital analyses as global cyber dangers increase. [1] Large amounts of electronic data are regularly processed by police departments, corporate security teams, and private investigators in order to detect and record illegal activity. However, there are several issues in handling these complicated situations, such as the need for multi-agency coordination and difficulties preserving the evidence.

The swift development of digital devices and storage techniques has made forensic procedures even more challenging. These days, investigators deal with cloud-based evidence dispersed across jurisdictions, increasingly complex encryption techniques, and volatile material that might vanish with a simple reboot. Standardized procedures that can speed up investigations without sacrificing quality or legal admissibility are desperately needed in light of these technological challenges and the mounting backlog of cases in many digital forensics labs.

Simplifying Case Administration: Managing computerized cases using traditional methods can be laborious and prone to human error.[2] A DFCMS automates many aspects of case administration, including announcing, case documenting, and prove logging, which saves time and reduces the possibility of mistakes .Enhancing Legal Compliance: When handling and evaluating computerized evidence, agents must adhere to stringent legal requirements.[3] Standardized procedures and integrated compliance checks are features of a DFCMS that help examiners stay within acceptable bounds and ensure that the evidence may be used in court.[4] Promoting Cross-Agency Cooperation: Several law enforcement offices, legal experts, and authorized entities are frequently asked to contribute to and participate in cybercrime investigations. A DFCMS promotes effective partner collaboration by strengthening secure communication, controlled access to case records, and real-time information sharing. [5] Increasing Investigative Effectiveness Conventional instruments struggle to keep up with the growing amount of electronic information.

A DFCMS is designed to manage large datasets and difficult situations, including advanced search, sorting, and analysis features that help agents work more effectively. [6] Providing Explanatory Bits of Information: A DFCMS can reinforce sophisticated analytics that assist in identifying patterns and designs across situations, promoting important information that aid in attempts to define approaches and prevent wrongdoing in general.

[7] Ensuring Scalability and Flexibility: Cybercrimes follow technological advancements. A DFCMS can be designed to coordinate contemporary tools and developments, guaranteeing that sophisticated forensics professionals can stay abreast of the evolving landscape of cybercrime. The process of gathering, organizing, and evaluating computerized evidence is rearranged by a DFCMS, which provides a centralized, well-organized stage. A DFCMS is specifically tailored to the unique requirements of computerized forensics, combining features like computerized chain-of-custody following, role-based access restrictions, and prove administration capabilities. This is in contrast to standard case administration frameworks. These tools ensure that evidence is maintained up to date, that case material is easily available to authorized professors, and that investigation forms are both auditable and comply with legal standards.

II. Literature Review

We looked at a few previous articles to develop this approach. In order to develop advanced scientific case administration, the paper [1] analyzes workflow execution, methods, and the ways in which different assignment models impact case handling timelines and overall competency. Together with suggested arrangements to handle lengthy examinations in computerized forensics scenarios, it provides a structured method for significantly increased efficiency in legal examinations and case completion. [2] The focus of this discussion is on achieving "advanced legal availability" in businesses, especially when they adapt to Industry 5.0 values like viable and human-

It places a strong emphasis on developing strategies and frameworks that ensure legal and administrative compliance, especially in intricate, cutting-edge scenarios with a variety of cyber threats and administrative requirements.[3] In subsequent research, a crucial focus has been using block chain technology to obtain sophisticated evidence in court cases. In order to advance the chain of care, guarantee sound judgment, and enhance access control in widely distributed computerized measuring systems, papers on this topic suggest a two-level block chain system.[4] highlights the impact of increased digitization and a sophisticated cyber framework while putting up conceptual ideas to advance computerized scientific organization. These programs address the need for consistent, standardized practices that adapt to legal and scientific requirements, promoting commonsense practices that help businesses become "forensically prepared."

[5].This allowed the investigator to weigh multiple options and determine the best course of action. The researchers have also described novel methods for collecting additional footprints on complex surfaces to aid in the study process. Additionally, the methods and functions of the instruments used in the inquiry were explained.

The ADF review was released in [6].An explanation of the information collection procedure is given by the author. Furthermore, the core concept, characteristics, and structure of Digital Forensics were described. Limiting potential changes to DF evidence used in court was the aim of the proposed framework. The development and analysis of the process were the main focus of this paper's grounded theory. Based on specific standards including validity and reliability, a variety of forensic tools were investigated. Additionally, it was claimed that the other variance performances in the three tools described above are influenced by both measurable and immeasurable factors. Consequently, the authors also investigated DF tools.

To characterize the different forensic methods and their performance, researchers employed comparison analysis [12].For data recovery, the EnCase tool was specifically stated to be significantly better than the Autopsy, Recuva, and Operating System (OS) forensic tools. This tool was deemed the most suitable for data retrieval and analysis since it produced the best results.

III. Digital Forensic Phases

The DF process usually consists of three phases: acquisition, analysis, and presentation.

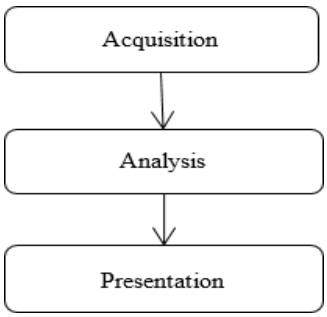

Figure2. Digital Forensics phases.

Acquisition

The crucial initial stage of forensic investigations is digital evidence acquisition, which is the methodical gathering of information from diverse electronic sources. To guarantee that evidence is admissible, investigators must adhere to stringent procedures, which frequently start with producing a forensic image, which is a bit-by-bit replica of the original storage media.[8] In order to avoid data tampering during imaging, this method uses specific tools such as write-blockers. Modern acquisition goes beyond conventional gadgets like USB sticks and hard disks to include cloud storage, Internet of Things devices, and car infotainment systems. New difficulties are brought about by the growing use of encrypted devices, necessitating sophisticated methods like cold boot attacks for memory acquisition or chip-off forensics (direct memory chip reading). At this stage, accurate documentation is essential, including thorough logs of hardware specs, system dates and hours, and hash values for validation.

Analysis

By carefully examining the raw data, the analysis phase turns it into intelligence that can be put to use. Digital activities are reconstructed by forensic experts using both automated tools and manual methods. This includes examining the information to confirm the legitimacy of the document, establishing event sequences using timeline analysis, and recovering lost content by file carving. [9] Advanced techniques like registry analysis and steganography detection expose system interactions and concealed data, respectively. The increasing amount of data calls for clever filtering systems that use machine learning algorithms to rank the most important evidence. Complex scenarios need analysts to correlate results across many devices, such as connecting computer login times to GPS data from smartphones. To discern between suspicious activity patterns and typical system behavior, technical evidence interpretation calls for both forensic knowledge and investigation intuition.

Presentation

It is the method by which the digital investigator will disseminate the findings of their research.[10] The case

analysis is brought before the court for additional procedures.
It includes the important stages the digital investigator takes and the procedures they take to complete the entire process. Additionally, the results of the inquiry were conducted, and the significance of the artifacts gathered is also provided [11]. Cyber fraud is one of the four stages of the DF process as outlined by the National Institute of Standards and Technology (NIST). The four stages of the Integrated Digital Forensics Process Model (IDFPM) of [12] include incident, preparation, DF investigation, and presentation.

IV. Digital Investigation Models

Digital forensic investigations follow a structured six-phase framework to ensure comprehensive evidence handling and maintain legal admissibility [17] This systematic approach guides investigators from initial evidence discovery through courtroom presentation.

1. **Evidence Identification**

The process begins with locating potential digital evidence sources. Investigators systematically survey crime scenes to identify all relevant devices, including computers, smartphones , IoT devices, and cloud storage accounts. Each item is carefully cataloged, documenting its physical characteristics, location found, and potential relevance to the case. Special attention is given to hidden data sources such as network logs, metadata, and temporary system files that might contain crucial evidence.

2. **Evidence Acquisition and Preservation**

This critical phase employs forensic imaging techniques to create exact bit-for-bit copies of storage media while maintaining evidentiary integrity. Investigators use write-blocking hardware to prevent data alteration and generate cryptographic hashes (like SHA-256) to verify image authenticity. The process addresses both volatile memory (requiring live acquisition techniques) and non-volatile storage. Proper chain-of-custody documentation begins at this stage, recording all handling of physical devices and digital images.

3. **Evidence Examination**

Forensic specialists conduct methodical examinations of acquired images using specialized tools. This involves file system analysis, recovery of deleted content through data carving, and extraction of metadata. Examiners reconstruct file systems, analyze partition tables, and identify anomalies in storage patterns. The examination identifies potentially relevant files while filtering out irrelevant system data, focusing on finding intentionally hidden or obfuscated information.

4. **Evidence Analysis**

Building upon examination findings, analysts interpret the significance of discovered artifacts. This phase correlates data across multiple sources, establishes timelines of digital events, and reconstructs user activities. Advanced techniques include registry analysis for Windows systems, plist examination for macOS , and application-specific artifact analysis. Analysts distinguish between normal system operations and suspicious patterns, often employing statistical methods and machine learning to process large datasets efficiently.

5. **Evidence Documentation**

Comprehensive documentation creates a permanent record of all investigative actions. This includes detailed reports of methodologies used, tools employed, and findings discovered. Documentation maintains the evidentiary chain by recording every access to and manipulation of evidence. Standardized formats ensure clarity for legal proceedings, while thorough notes support peer review and potential re-examination of evidence.

6. **Evidence Presentation**

The final phase translates technical findings into court-admissible formats. Investigators prepare clear, concise reports suitable for non-technical audiences and may provide expert testimony. Presentation materials often include visual aids explaining complex technical concepts, annotated timelines of events, and demonstrations of forensic processes. The presentation must withstand legal challenges by demonstrating strict adherence to forensic standards and proper evidence handling procedures throughout all phases. This structured approach ensures digital evidence maintains its integrity and admissibility while allowing investigators to methodically uncover and interpret increasingly complex digital artifacts in modern investigations.

V. Tools for Performing Digital Forensic Investigation

There are so many tools for performing DF investigations. Some are open-source, and some are licensed versions. According to the requirements, the investigator should use suitable and effective tools for that particular scenario. This section presents the four digital forensics tools with their characteristics.

Autopsy (Open-Source)
Autopsy is a powerful open-source digital forensics platform developed by Brian Carrier as part of the Sleuth Kit (TSK) project. Built on a modular architecture, it provides a user-friendly graphical interface (GUI) for forensic analysis. The tool is available in multiple versions,

including Autopsy(open-source) and Autopsy+ (commercial) with enhanced features.

En Case

En Case was created by Guidance Software in 1998. It is currently owned by Open-Text. Because of its characteristics, it is the most widely used forensic instrument in the world. En Case software is used by 89% of global merchandise companies and 91% of banks. In the United States, En Case software is used by 80% of universities and 98% of government agencies. The investigation, data collection and analysis, and report creation are the first steps of the investigation cycle. It is capable of gathering and analyzing data remotely. Password recovery is also made using it. Additionally, it performs memory acquisition and data acquisition. It maintains the integrity of the evidence and produces a large number of reports according to the findings. It performs Disk Imaging and data carving [15].

Pro Discover

It was created by the New York-based Anthony Reyes Company (ARC) Group. Pro Discover Basic, Pro Discover Forensic Edition, and Pro Discover Incident Response Edition (IRE) are the versions that are available. Pro Discover Basic is available as open source. In order to protect user data, it collects the activity snapshots that are required. When necessary, Pro Discover software can be used to gather device information, time zone, and web surfing activity. The Pro Discover forensic edition examines files without altering the metadata. It is quick and adaptable.It carries out memory and data acquisition. Malware finding hash sets are another option. It produces electronic reports that include crucial details about the evidence [20].

VI. Problem Statement

The rapid expansion of digital technologies has led to an unprecedented surge in cybercrime, creating complex challenges for forensic investigators. As digital evidence becomes more voluminous and varied, professionals grapple with maintaining evidentiary integrity while managing overwhelming data quantities across multiple platforms. The evolving nature of cyber threats demands increasingly sophisticated forensic methodologies to keep pace with technological advancements.

While contemporary Digital Forensics Management Systems (DFMS) have automated critical functions like evidence collection, examination, and documentation, significant limitations remain. These systems often fail to adequately address emerging technological paradigms including distributed cloud architectures, ubiquitous mobile computing, and AI-driven applications. Additionally, modern anti-forensic tactics, advanced encryption methods, and evolving legal standards present persistent obstacles, resulting in prolonged investigation timelines and heightened risk of procedural errors that may undermine evidentiary validity [8].

This landscape underscores the urgent requirement for next-generation DFMS solutions incorporating enhanced capabilities. Future systems must integrate scalable architectures for big data processing, specialized modules for cloud and mobile environments, and immutable verification mechanisms such as blockchain technology. Such advancements are crucial for optimizing investigative workflows, preserving evidentiary chain of custody, and ensuring digital evidence meets stringent legal admissibility standards in judicial proceedings.

VII. Future Scope

Since technology is advancing at a rapid rate and bringing with it both new opportunities and challenges ,digital forensics management systems (DFMS) have a bright future. As cybercrimes increase in complexity and variety, there will be an increasing demand for advanced and scalable forensic tools [12]. Through the automation of time-consuming procedures such as pattern recognition, anomaly detection, and data analysis, these technologies enable forensic investigators to accurately and efficiently sift through vast volumes of data. AI and ML can improve over time in addition to speeding reporting, spotting attack patterns, and continuously learning from new data. Another significant area of advancement is cloud and remote forensics. DFMS solutions will have to adapt to address the challenges posed by cloud-based digital evidence as cloud services gain traction. This includes developing secure APIs and technologies for the real-time gathering of evidence from distributed cloud networks and virtual computers [21].

Future DFMS will need to enable forensic tests on a wider variety of devices due to the growing prevalence of IoT and mobile devices. This means developing specialized tools to deal with encryption and device-specific problems while getting data from Internet of Things devices, smart phones, and tablets. The ability to properly assess mobile and IoT data is crucial because these devices frequently contain significant evidence in both criminal and civil investigations [22].

VIII. Conclusion

Several DFIM and tools, as well as DF methods and trends ,are covered in this study. A study framework is also provided. A comparison of the four DF tools is also included. Compared to the other tools described, the En Case digital forensic tool has been found to be more reliable. En Case has a fast data recovery rate. The essay also enumerates human factors that influence the process of digital inquiry. This article also presents the DFR parameters. Applying suitable models, tools, and processes to enhance the results of the digital inquiry process can be facilitated by the research findings [23]. This will be required to handle the problems posed by evolving technology and ever-evolving cyberthreats , as well as to maintain the legal requirements for digital evidence's

admissibility in court.

Future DFMS systems will integrate cutting-edge encryption techniques, block chain, cloud forensics, and artificial intelligence to give forensic investigators the tools they need to handle digital evidence more skillfully and maintain its integrity throughout the investigation process [24]. This will be necessary to address the issues brought on by developing technology and constantly changing cyber threats, as well as to uphold the legal standards for the admissibility of digital evidence in court. By combining cutting-edge encryption techniques, block chain, cloud forensics, and artificial intelligence, future DFMS systems will give forensic investigators the tools they need to handle digital evidence more skillfully and maintain its integrity throughout the investigation process [24].

IX. References

[1] Ademu I, Imafidon C., and Preston D.,"A New Approach of Digital Forensic Model for Digital Forensic Investigation ,"International Journal of Advanced Computer Science and Applications, vol. 2, no. 12, pp. 175-178, 2011.

[2] Agarwal A., Gupta M., Gupta S., and Gupta S., "Systematic Digital Forensic Investigation Model," International Journal of Computer Science and Security, vol. 5, no. 1, pp. 118-131, 2011.

[3] Agarwal R. and Kothari S., "Review of Digital Forensic Investigation Frameworks," Information Science and Applications, vol. 339, pp. 561-571, 2015.

[4] Ali M., Shiaeles S., Clarke N., and Kontogeorgis D., "A Proactive Malicious Software Identification Approach for Digital Forensic Examiners," Journal of Information Security and Applications, vol. 47, pp. 139-155, 2019.

[5] Al-Sharif Z., "Utilizing Program's Execution Data for Digital Forensics," in Proceedings of the 3rd International Conference on Digital Security and Forensics (DigitalSec), Kuala Lumpur, pp. 12-19, 2016.

[6] Aminnezhad A., Dehghantanha A., and Abdullah M., "A Survey on Privacy Issues in Digital Forensics," International Journal of Cyber- Security and Digital Forensics, vol. 1, no. 4, pp. 311-323, 2014.

[7] Anghel C., "Digital Forensics-A Literature Review," The Annals of "Dunarea de Jos" University of Galati. Fascicle, Electrotechnics, Electronics, Automatic Control, Informatics, vol. 42, no. 1, pp. 23-27, 2019.

[8] Arshad H., Jantan A., and Abiodun O., "Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence," Journal of Information Processing Systems, vol. 14, no. 2, pp. 346-376, 2018. DOI:10.3745/JIPS.03.0095

[9] Bariki H., Hashmi M., and Baggili I., "Defining a Standard for Reporting Digital Evidence Items in Computer Forensic Tools," Lecture Notes of the for Institute Informatics Engineering, Computer Sciences, Social- and Telecommunications vol. 53, pp. 78-95, 2010.

[10] Baryamureeba V. and Tushabe F., "The Enhanced Digital Investigation Process Digital Baltimore, Model," in proceedings of the Forensic pp. Research Conference, 1-10, 2004.

[11] Beebe N. and Clark J., "A Hierarchical, Objectives-based Framework for the Digital Investigations Process," Digit Investigation, vol. 2, no. 2, pp. 147-167, 2005.

[12] Bensefia H. and Ghoualmi N., "An Intelligent System for Decision Making in Firewall Forensics," in Proceedings of the Digital Information and Communication Technology and its Applications, Dijon, pp. 470-484, 2011.

[13] Carrier B. and Spafford E., "An Event-Based Digital Forensic Investigation Framework," in Proceedings of the DFRW Digital Forensic Research Conference, Baltimore, pp. 1-29, 2004.

[14] Castelo Gómez J., Carrillo Mondéjar J., Roldán Gómez J., and Martínez Martínez J., "A Context-Centered Methodology For IoT Forensic Investigations," International Journal of Information Security, vol. 20, pp. 647-673, 2021.

[15] Cusack B. and Liang J., "Comparing the Performance of three Digital Forensic Tools," Journal of Applied Computing and Information Technology, vol. 15, no. 1, pp. 1-9, 2011.

[16] Dalezios N., Shiaeles S., Kolokotronis N., and Ghita B., "Digital Forensics Cloud Log Unification: Implementing CADF in Apache CloudStack," Journal of Information Security and Applications, vol. 54, pp. 102555, 2020.

[17] Damshenas M., Dehghantanha A., and Mahmoud R., "A Survey on Digital Forensics Trends," International Journal of Cyber-Security and Digital Forensics, vol. 3, no. 4, pp. 209-235, 2014.

[18] Elyas M., Maynard S., Ahmad A., and Lonie A., "Towards a Systemic Framework for Digital Forensic Readiness," Journal of Computer Information and Systems, vol. 54, no. 3, pp. 97- 105, 2015.

[19] Galloway P., "Preservation of Digital Objects," Annual Review of Information Science and Technology, vol. 38, pp. 549-590, 2004.

[20] Garfinkel S., "Digital Forensics Research: The Next 10 Years," Digital Investigation, vol. 7, pp. S64-S73, 2010.

[21] Ghazinour K., Vakharia D., Kannaji K., and Satyakumar R., "A Study on Digital Forensic Tools," in Proceedings of the IEEE International Conference on Power, Control, Signals and Instrumentation Engineering, Chennai, pp. 3136- 3142, 2018.

[22] Grispos G., Storer T., and Glisson W., "A Comparison of Forensic Evidence Recovery Techniques for a Windows Mobile Smart Phone," Digital Investigation, vol. 8, no. 1, pp. 23-36, 2011.

[23] Guido M., Buttner J., and Grover J., “Rapid Differential Forensic Imaging of Mobile Devices,” Digital Investigation, Evaluation of Digital Forensics Tools on Data Recovery and Analysis, vol. 18, pp. S46-S54, 2016.
[24] Guo Y. and Slay J., “Data Recovery Function Testing for Digital Forensic Tools,” in Proceedings of the 6th International Conference on Advances in Digital Forensics, Hong Kong, pp. 297-311, 2010.