International Journal of Innovative Research in Technology and Science
ISSN: 2321-1156 www.ijirts.org Volume 12 Issue 2, March 2024

Digital Forensics and Cyber Investigation

Muskan Maurya, Varun Jain
Department of Life Sciences, SAM Global University, Bhopal, India
muskxxn30@gmail.com

Selection and peer review of this article are under the responsibility of the scientific committee of the International Conference on Current Trends in Engineering, Science, and Management (ICCSTEM-2024) at SAM Global University, Bhopal.

Abstract- Digital forensics, a vital facet of forensic science, focuses on utilizing digital information from computers as evidence in investigations and legal proceedings. Initially government-centric, it has now permeated the commercial sector. This paper concisely overviews the digital forensics process and associated models. It highlights the growing importance of the "Digital Forensic Investigation Model," an active research area aiming to enhance field procedures. The paper concludes by addressing challenges and outlining the future scope of digital forensics. In computer forensics, a swiftly evolving discipline, the debate centres on effectiveness, static versus dynamic analysis, and the legal ramifications within the dynamic cyberspace domain. This paper navigates these issues, borrowing principles from the physical world to tackle unique challenges in the digital realm.

Keywords- Digital Forensics, Legal Proceedings, Digital Forensic Investigation Model, Forensic Procedures, Legal Implications.

1. INTRODUCTION

Digital Forensics (DF) has evolved significantly, becoming vital to modern investigations conducted by local, state, and Federal law enforcement agencies. Over the past decade, advancements in forensic research, tools, and processes have propelled DF into the mainstream. Computer forensics emerged in response to the rise in crimes involving computer systems, whether as targets, tools, or evidence repositories. Digital Forensics, defined as the systematic use of scientifically derived methods, serves the purpose of preserving, validating, identifying, analyzing, interpreting, documenting, and presenting digital evidence. Its primary goal is to reconstruct criminal events or anticipate unauthorized actions disruptive to planned operations. As technology advances, the role of Digital Forensics becomes increasingly crucial in ensuring justice and security in our digital world. Computer forensics traces back to around 1984, when the FBI and other law enforcement agencies started creating programs to investigate computer evidence. Organizations like the Computer Analysis and Response Team (CART), Scientific Working Group on Digital Evidence (SWGDE), Laboratory Accreditation Board (ASCLD-LAB), Technical Working Group on Digital Evidence (TWGDE), and the National Institute of Justice (NIJ) were established to discuss and develop the discipline of computer forensic science. These groups emphasized the need for standardized approaches in examinations. Digital Forensics (DF) is approximately forty years old and initially focused on data recovery. Over time, it has evolved into a crucial field, ensuring the integrity of digital evidence and contributing significantly

to solving cybercrimes. In 2001, Kruse & Heiser introduced a Digital Forensic Investigation Model that revolves around three critical phases: acquiring, authenticating, and analyzing evidence—commonly known as the three A's of digital forensics. This model primarily focuses on ensuring the integrity of evidence and was specifically designed for incident response.

The Digital Forensic Research Workshop (DFRW) model, originating from a 2001 workshop in Utica, USA, presented a significant advancement in digital forensics. Comprising seven phases—Identification, Preservation, Collection, Examination, Analysis, Presentation, and Decision—the DFRW model addressed stages often overlooked by previous models, particularly highlighting the importance of the presentation phase.

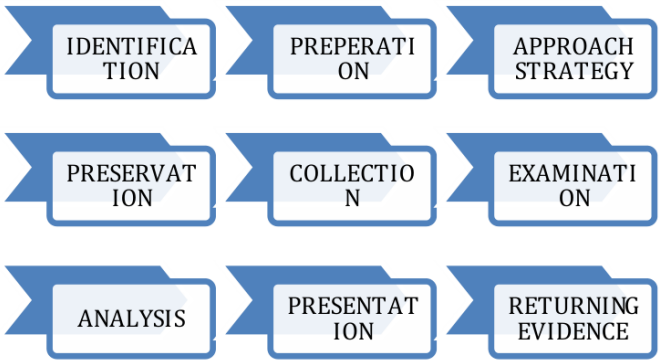

Figure 1. illustrates commonalities among the three models, with ADFM highlighting additional elements.

This model laid a crucial foundation for digital forensic investigations and set the stage for future research. 2002, Reith, Carr, and Gunsch enhanced the DFRW model, creating the Abstract Digital Forensic Model (ADFM). Notably, ADFM integrated all activities from both DFIM and DFRW, introducing three additional components: Preparation, Approach Strategy, and Return of Evidence. This comprehensive model emerged as the most inclusive, incorporating previously omitted elements. Figure 1 illustrates commonalities among the three models, with ADFM highlighting additional elements.

2. DIGITAL FORENSIC MODEL

1. Identification:- The initial phase involves recognizing an incident by identifying indicators and determining its type.
2. Preparation: This component encompasses preparing tools, techniques, search warrants, obtaining monitoring authorizations, and securing management support.
3. Approach Strategy:- Develop a strategic procedure to maximize the collection of untainted evidence while minimizing the impact on the victim.
4. Preservation: This phase involves isolating, securing, and preserving evidence's physical and digital states.
5. Collection:- Records the physical scene and duplicates digital evidence using standardized and accepted procedures.
6. Examination:- This component involves an in-depth systematic search of evidence related to the suspected crime.
7. Analysis:- Analysis includes determining the significance of findings, reconstructing data fragments, and drawing conclusions based on the evidence discovered.
8. Presentation:- Involves summarizing and explaining the conclusions derived from the analysis.
9. Returning Evidence:- The final phase ensures the proper return of physical and digital property to its rightful owner. The model aims to establish a standardized and comprehensive digital forensic process.

3. FUTURE SCOPE

1. More Detailed Research: Research should involve more people and gather detailed information about them. Instead of just finding problems, it should also solicit ideas on how to solve them.
2. Improving the Model: The new digital forensic model should be tested in different cases and refined based on feedback. This iterative process enhances its effectiveness over time and makes it more beneficial for investigations.
3. Keeping Up with Changes: The model must adapt as technology evolves. Regular updates should incorporate new challenges arising from technological advancements to ensure the model remains relevant and effective for investigating digital crimes.

4. CONCLUSIONS

In conclusion, this paper highlights an impending crisis in digital forensics spurred by ongoing trends. It advocates for enhanced efficiency in digital forensics research by introducing new abstractions for data representation and forensic processing. Digital forensics, once predominantly governmental, now extends into the commercial sector, underscoring its critical role in investigations. The "Digital Forensic Investigation Model" emerges as a focal point, representing an active research area poised to enhance field procedures. The paper offers a concise overview of the digital forensics process and associated models, illuminating its growing significance. The discussion encompasses effectiveness, static versus dynamic analysis, and legal implications in the dynamic cyberspace domain, recognizing the challenges within the rapidly evolving field of computer forensics. By navigating these issues and drawing on principles from the physical world, this paper contributes to addressing unique challenges and shaping the future trajectory of digital forensics.

REFERENCES

[1]. Ravneet Kaur and Amandeep Kaur, "Digital Forensics," International Journal of Computer Applications, vol. 50, no. 5, 2012.

[2]. Simson L. Garfinkel, "Digital Investigation," Digital Forensic Research Workshop, vol. 7, pp. S64 – S73, 2010.

[3]. Seema Yadav, Khaleel Ahmad, and J. Shekhar, "Analysis of Digital Forensic Tools and Investigation Process," International Conference on High-Performance Architecture and Grid Computing, vol. 169, pp. 435 – 441, 2011.

[4]. Soufiane Tahiri, "Digital Forensics Model," Digital Forensics, 2016.

[5]. Kaur, Ravneet, and Amandeep Kaur. "Digital Forensics." International Journal of Computer Applications, vol. 50, no. 5, 2012.

[6]. Garfinkel, Simson L. "Digital Investigation." Digital Forensic Research Workshop, vol. 7, 2010, pp. S64 – S73.

[7]. Yadav, Seema, Khaleel Ahmad, and J. Shekhar. "Analysis of Digital Forensic Tools and Investigation Process." International Conference on High-Performance Architecture and Grid Computing, vol. 169, 2011, pp. 435 – 441.

[8]. Tahiri, Soufiane. "Digital Forensics Model." Digital Forensics, 2016.