

Models of Forensic Investigation: End to End Digital Investigation Process (EEDIP)

Vaishnavi Limbhore¹, Pooja Gavhande², Mrs. P.S. Ghode³

Students, Information Technology¹⁻²

Guide, Information Technology³

Government Polytechnic, Awasari (Khurd)

Abstract: *Digital forensic investigation is a systematic process of identifying, collecting, preserving, and analyzing digital evidence. This paper presents the End-to-End Digital Investigation Process (EEDIP), which covers identification, preservation, collection, examination, analysis, documentation, reporting, and presentation. The proposed process helps maintain evidence integrity and provides a structured approach to digital investigations.*

Keywords: Digital Forensics, Digital Evidence, EEDIP, Cybercrime

I. INTRODUCTION

Digital forensics is the process of identifying, collecting, preserving, and analyzing digital evidence from computers, mobile devices, networks, and other digital systems. With the increasing use of technology, cybercrimes and digital security incidents are also increasing. Therefore, a systematic investigation process is required to handle digital evidence properly. Different digital forensic models provide different stages for conducting investigations. This paper focuses on the End-to-End Digital Investigation Process (EEDIP), which provides a structured approach from identification of evidence to final reporting and presentation.

II. DIGITAL FORENSICS:

Digital forensics is the systematic process of identifying, collecting, preserving, examining, and analyzing digital evidence from computers, mobile devices, storage media, networks, and other digital systems. It is mainly used to investigate cybercrime, unauthorized access, data theft, fraud, and security incidents. The main objective is to obtain reliable digital evidence while maintaining its integrity and authenticity.

III. DIGITAL FORENSIC INVESTIGATION MODELS:

Digital forensic investigation models provide a structured method for conducting forensic investigations. These models generally include stages such as identification, preservation, collection, examination, analysis, and reporting. Although different models may use different terminology or arrange activities differently, their common purpose is to handle digital evidence systematically and produce reliable investigative findings.

IV. EEDIP PROCESS

The End-to-End Digital Investigation Process (EEDIP) provides a complete approach to digital investigation from the beginning of an incident to the final presentation of findings. The process starts with identification of the incident and potential evidence sources, followed by preservation of evidence to prevent modification or loss. Relevant evidence is then collected or acquired and examined to identify useful information. The evidence is analyzed to establish relationships, timelines, and findings. Finally, the investigation is documented, reported, and presented to authorized persons or legal authorities when required.



V. PROPOSED EEDIP MODEL

The proposed EEDIP model connects the major forensic activities into one continuous investigation lifecycle. It follows the sequence of identification, preservation, collection or acquisition, examination, analysis, documentation, reporting, and presentation. The model emphasizes evidence integrity, systematic analysis, and complete documentation. If additional evidence is required during analysis, investigators may return to earlier stages, making the process iterative while maintaining proper records.

VI. ADVANTAGES AND APPLICATIONS:

EEDIP provides a clear and organized approach to digital investigations. It helps maintain evidence integrity, improves traceability, supports proper documentation, and creates a clear relationship between evidence and final conclusions. The process can be applied to computer forensics, mobile forensics, network forensics, cloud-related investigations, cybercrime investigation, incident response, online fraud, data theft, and unauthorized access investigations.

Challenges: Digital forensic investigations face several challenges, including large volumes of data, encrypted information, deleted or damaged files, anti-forensic techniques, rapidly changing technologies, volatile evidence, and cloud-based environments. Investigators also need appropriate technical skills, reliable forensic tools, proper procedures, and complete documentation to ensure that evidence is handled correctly.

TABLE I: DIGITAL FORENSIC INVESTIGATION MODELS

Stage	Description
Identification	Identifies the incident, affected systems, and potential sources of digital evidence.
Preservation	Protects digital evidence from modification, deletion, or damage.
collection	Collects or acquires relevant digital evidence using proper procedures.
Examination	Processes and searches the collected data to find Relevant information.
Analysis	Interprets evidence, correlates information, and identifies relationships between events.
Documentation	Records investigation activities, evidence details, methods, observations, and results.
Reporting	Presents the investigation methods, findings, limitations, and conclusions.
Presentation	Presents the final findings to authorized persons or legal authorities when required.

A. Figures and Tables

The figure shows two digital forensic models, IDIP and EDIP, and their main investigation stages. It highlights how each model organizes the investigation from readiness and deployment to review.

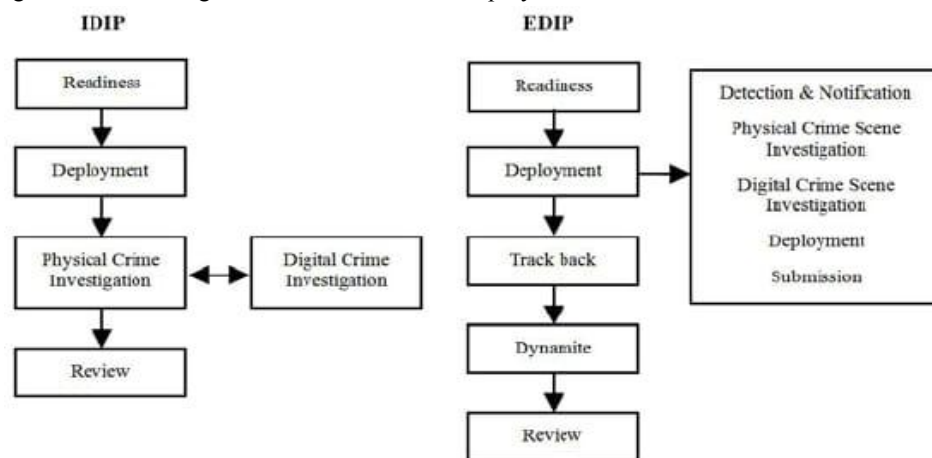


Fig. 1 End-to-End process of Digital Forensic Investigation



History of Digital Forensics: Digital forensics developed with the increasing use of computers and digital technologies. In the early stages, investigations mainly focused on recovering and examining information stored on computer systems and storage media. As the Internet, mobile devices, networks, and cloud technologies became widely used, digital investigations became more complex and required systematic methods for handling digital evidence. Researchers therefore developed different forensic investigation models to organize activities such as identification, preservation, collection, examination, analysis, and reporting. Models such as IDIP and EDIP helped provide structured approaches to digital investigations. Modern digital forensics now covers computers, smartphones, networks, cloud environments, applications, and other digital sources, with greater emphasis on evidence integrity, documentation, and reliable analysis.

Digital forensics emerged with the increasing use of computers and electronic storage systems. In the early period, investigations mainly involved recovering and examining information stored on computer systems and storage media. As computers became connected through the Internet, investigators faced new forms of digital evidence such as emails, network records, browser activity, and system logs. This increased the need for systematic forensic procedures and investigation models.

During the 1990s and 2000s, the growth of the Internet, mobile phones, and networked systems led to an increase in cyber-related incidents. Digital forensic researchers began proposing investigation models to organize the activities performed during an investigation. These models introduced structured stages such as readiness, deployment, identification, collection, examination, analysis, and review. The IDIP (Integrated Digital Investigation Process) and EDIP (Enhanced Digital Investigation Process) are examples of models that attempted to organize digital investigations into clearly defined stages.

As technology continued to develop, digital evidence expanded beyond traditional computers. Smartphones, social media, cloud computing, Internet of Things (IoT) devices, and online applications became important sources of evidence. Consequently, modern forensic investigations require techniques for handling different types of devices and large quantities of data. Standards and guidelines for the identification, collection, acquisition, and preservation of digital evidence have also become important for maintaining evidence integrity.

Today, digital forensics is an important part of cybercrime investigation, incident response, law enforcement, corporate security, and legal proceedings. Modern investigators use techniques such as deleted-data recovery, metadata analysis, timeline analysis, memory analysis, log analysis, and network analysis. The development of these technologies and investigation models has created the need for an integrated end-to-end approach. The EEDIP (End-to-End Digital Investigation Process) presented in this paper focuses on connecting the major stages of an investigation—from identification and preservation through collection, examination, analysis, documentation, reporting, and presentation—into a continuous and traceable process.

IV. CONCLUSION

Digital forensics is an important method for investigating cybercrime and digital security incidents. Different forensic models provide systematic steps for handling digital evidence. The EEDIP model provides an end-to-end process covering identification, preservation, collection, examination, analysis, documentation, reporting, and presentation. It helps maintain evidence integrity, improve investigation traceability, and organize forensic activities effectively. Thus, EEDIP provides a clear and structured approach for reliable digital forensic investigations.

V. ACKNOWLEDGMENT

I would like to express my sincere gratitude to my faculty members and Government Polytechnic Awasari for their valuable guidance and support in completing this research paper. I am also thankful to everyone who helped and encouraged me during this work.



REFERENCES

- [1] G. Palmer, "A Road Map for Digital Forensic Research," Digital Forensic Research Workshop (DFRWS) Technical Report, 2001.
- [2] M. Reith, C. Carr, and G. Gunsch, "An Examination of Digital Forensic Models," International Journal of Digital Evidence, 2002.
- [3] B. Carrier and E. H. Spafford, "Getting Physical with the Digital Investigation Process," CERIAS Technical Report TR 2003-29, Purdue University, 2003. CERIAS
- [4] N. L. Beebe and J. G. Clark, "A Hierarchical, Objectives-Based Framework for the Digital Investigations Process," Digital Investigation, 2005. ScienceDirect
- [5] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," NIST Special Publication 800-86, National Institute of Standards and Technology, 2006. NIST Computer Security Resource Center +1
- [6] B. Carrier, File System Forensic Analysis, Addison-Wesley, 2005.
- [7] ISO/IEC 27037:2012, Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. ISO
- [8] J. R. Lyle, B. Guttman, J. Butler, K. Sauerwein, C. Reed, and C. Lloyd, "Digital Investigation Techniques: A NIST Scientific Foundation Review," NISTIR 8354, National Institute of Standards and Technology, 2022. nist.gov

