Research Journal of Computer and Information Technology Sciences _____ISSN 2320 – 6527
Vol. **14(1),** 18-22, June **(2026)** *Res. J. Computer and IT Sci.*

Review Paper

A comparative study of Contemporary Cyber Forensics Tools for Digital Investigation

Binita Thakkar*, Shweta Yande and Anuja Patil
Department of Computer Science, VIVA College of Arts, Commerce and Science, Virar (W), India
binitathakkar@vivacollege.org

Available online at: www.isca.in
Received 7th May 2026, revised 20th May 2026, accepted 19th June 2026

Abstract

The increasing reliance on digital systems has significantly elevated the importance of cyber forensics tools in modern investigations. This study focuses exclusively on the comparative analysis of contemporary cyber forensics tools used across various domains, including data recovery, disk imaging, steganography detection, email investigation, and comprehensive forensic analysis. Tools such as EaseUS Data Recovery Wizard, Recuva, FTK Imager, Access Data FTK, EnCase, and Autopsy are examined based on performance, usability, reliability, and investigative applicability. The study adopts a comparative framework to evaluate tool efficiency in handling digital evidence. The findings highlight that each tool serves a specialized purpose, and no single tool can address all forensic requirements effectively. The study emphasizes the importance of selecting appropriate tools based on investigation needs and suggests the integration of multiple tools for enhanced forensic outcomes.

Keywords: Cyber forensics, digital investigation, forensic tools, comparative analysis.

Introduction

The rapid advancement of digital technologies has altered how information is created, stored, and transmitted. Nevertheless, these modifications led to the emergence of cybercrime. This element necessitates the development of appropriate investigation techniques in order to tackle cybercrimes. Because they aid in the investigation, identification, collection, preservation, and analysis of digital evidence, specialised tools for cyber forensics are crucial.

As cybercrime grows increasingly complex, a number of solutions that address specific problems with digital investigation have emerged. They include disc imaging, email tracing, and data recovery tools. According to their functional features, cyber forensics tools vary widely. Every instrument has different capabilities that enable a certain outcome in an investigation. At the same time, since selecting a tool is difficult, it is necessary to evaluate its effectiveness.

Comparing modern cyber forensics tools across many categories is the aim of the current study. This will make it easier to recognise their strengths and weaknesses and comprehend their usefulness.

Literature Review

The authors focus on steganography and its application in digital forensics[1]. In the study, there is an explanation of methods used for hiding and discovering data. The paper addresses various difficulties experienced in the process by forensics specialists.

In the study, the author looks at the application of forensic tools during the investigation of cybercrimes[2]. This study reviews some of the forensic tools that are employed in the acquisition, analysis, and reporting of digital evidence. This study stresses the significance of the accuracy and reliability of such forensic tools.

The authors conducted their most recent research on the topic of forensic software for investigation purposes[3]. It brings forward the issue of the reliability of such software and its legal acceptability. The paper deals with advancements in the field of forensic software.

The authors examined recent advances in digital forensics and described new trends and techniques in digital forensics[4]. The research work brings up new advancements including the use of AI and automation. The research stresses the difficulties that have been faced in adapting to new technology.

Various forensic tools utilized during investigations into cyber crimes have been studied[5]. This paper analyses the effectiveness of those tools during evidence collecting and analyzing. Importance of selecting proper tool is stressed out here along with issues related to dealing with different kinds of data.

In a research, modern-day cyber forensic tools are analyzed alongside their working methods[6]. Challenges that are likely to emerge, such as the handling of large amounts of data and encryption, have been discussed.

Comparative evaluation of different digital forensic tools has been carried out. Performance, precision, and usability of particular tools have been analyzed there[7]. Strengths and weaknesses of each individual tool have been pointed out.

The authors in their study gives a summary of concepts and analysis tools for cyber forensics[8]. This article discusses methodologies applied in conducting digital investigation. It reviews the capability of the tools used by the investigator and challenges encountered during the process. This study also recommends better forensic practices.

The study provides a detailed explanation of the steganography techniques used to conceal messages within digital material[9]. This study categorises the methods based on how they are used in texts, sounds, and visuals, as well as their advantages and disadvantages. This study lays the groundwork for future forensic investigations by illuminating the challenges of identifying hidden data.

The study examines different approaches towards solving cases of cybercrimes[10]. Among other things, the article brings to light the significance of using forensic tools in detecting risks associated with crimes. At the same time, the researcher emphasizes the need to develop systematic processes for conducting investigations.

The study offers a detailed review of the existing modern forensic tools[11]. In this regard, it classifies tools depending on their functional aspects. The study brings out innovations in forensic technologies. At the same time, the author talks about some of the difficulties that arise during the standardization of these tools.

The study explores the application of digital forensics in the field of cybersecurity[12]. It focuses on the importance of using forensics tools in identifying as well as protecting the system from cyber threats. The research identifies that real-time analysis is vital in the process.

The study investigates the impact of forensic science during the identification and diagnosis of digital crimes[13]. Various tools and methods that have been employed in carrying out cyber forensic investigations have been discussed in the paper.

The work examines many tools used in cyber forensic investigations[14]. Their importance as evidence collecting mechanisms in the analysis phase becomes clear in this study. The limitations of the current tools are discussed here as well.

Network forensics tools and techniques applied for monitoring and analyzing network traffic have been evaluated[15]. Emphasis was laid on the necessity of real-time data analysis. Issues associated with handling large volumes of network data are pointed out. Monitoring tools are highly needed here as well.

The study reviews advanced tools in network forensics[16]. This research reviews the effectiveness of these tools in combating cyber threats. The research work identifies developments in network forensics including network surveillance.

The study elaborate on proactive approaches to cyber forensic investigation and the significance of preventive actions against cybercrimes[17]. The study looks at technology and tools that are helpful in spotting cyber threats. It is underlined how crucial it is to incorporate them into an effective procedure.

Forensics Tools

Forensic tools for cyber security refer to software packages utilized in locating, collecting, preserving, analyzing, and presenting evidence in an investigation. Forensic tools make it possible for evidence to be collected and presented legally in court without changing any of its components. They help investigators in restoring any deleted files, analyzing computer activities, and determining the actions of cyber criminals. In light of the increasing sophistication of cyber-attacks, manual investigations are not sufficient, hence the need for these kinds of tools. Generally, forensic tools improve the process of investigating digitally. The following are the types of forensics tools in Figure-1.

Data Recovery Tools: Data recovery refers to restoring data that has either been deleted or corrupted on storage devices. Data recovery is crucial in digital forensics where the goal is to recover the deleted or lost evidence.

EaseUS Data Recovery Wizard: EaseUS is a popular tool used in recovering deleted and formatted files with great efficiency. It can work in several file systems and has a good user interface. As stated in a study, tools like this one are necessary when recovering lost digital evidence[7]. This tool is capable of deep scans. Thus, it is good for both beginners and advanced users.

Recuva: Recuva is known for its lightweight design and rapid file recovery ability. It is ideal when undertaking small forensic investigations as stated in[5]. It has overwritten security options to protect confidential information during recovery. It is easy to use, but not ideal for complex situations.

PC Inspector File Recovery: This tool allows for file and partition recovery. It works effectively in FAT and NTFS systems and conducts deep scans. However, it lacks user-friendly interfaces. Its recovery accuracy is moderate as compared to other recovery tools.

Data Acquisition: Data acquisition is the term used for the process where collection of evidence from a system or storage media and creation of a forensic image of the evidence is done. Data acquisition guarantees that the original data is kept safe for future use while at the same time making the collected data accessible for further analysis on another copy.

FTK Imager: FTK imager is one of the popular tools used in forensics for making forensic disk images. Hashing is guaranteed by this software[7]. It is very reliable for acquiring data and comes in different formats. It is legally admissible.

R-Drive: This tool is used for making images and also for cloning purposes. It is a fast disk imaging software but does not offer forensic validation features.

Steganography Tools: Steganography involves the use of concealing confidential data in various forms of digital content including images, audio, and text documents. Forensic examination of steganographic techniques involves both detection and analysis of hidden data.

S-Tools: S-Tools is used in hiding and uncovering data embedded in images and audio files. S-Tools is important in the analysis of steganography[9]. This tool utilizes encryption technology in data embedding. It performs well in detecting hidden data. Nonetheless, it is not up to date when compared to other current tools.

Snow: The snow algorithm hides data in whitespace of text documents. Snow can be helpful in detecting concealed communication processes[9]. It is quite simple to use. Its main applications are confined to academic work only.

Quick-Stego: Quick Stego is an easy-to-use software that helps users hide text data in images. Quick Stego is common in conducting steganography tests[1]. It does not have powerful data detection capability.

Email Crime Tools: Email crimes include the use of the email system for criminal activity like phishing, fraud, or identity theft. This type of cybercrime needs forensic investigation that helps trace the origin, retrieve the emails, and uncover criminal intentions.

Email Tracker Pro: This software helps track the source of emails through IP tracing. It is helpful in tracking down cyber criminals[7]. It is able to provide precise geographic details. It proves helpful in conducting investigations of phishing cases. However, it relies on the accuracy of headers.

Recover My Email: This software enables the retrieval of lost emails. It supports various email formats. It can be very helpful in forensic email investigations. Its use ensures integrity while retrieving data.

Forensic Investigation Tools: Forensic investigation is a scientific approach to identifying, retrieving, examining, and presenting electronic evidence. This ensures that any findings made during the process are precise and admissible in court.

Access Data FTK: Access Data FTK is an all-around tool for performing forensic investigations and indexing data. The software has advanced search capabilities[7]. The software supports multiple forms of evidence. It is popular among law enforcement officers. It is efficient.

EnCase: EnCase is a renowned forensic tool used by investigators. The software has advanced evidence examination and presentation capabilities[7,10]. The software ensures admissibility of evidence. It is accepted in most courts. It is reliable.

ProDiscover Basic: ProDiscover is a tool used for disk investigation and forensics recovery. It comes with some basic forensic investigation features[5]. The software is ideal for beginners. It lacks advanced features. It is cheap.

Autopsy: Autopsy is an open-source forensic solution for investigation. It has powerful analysis capabilities and plugins support[8]. The software is highly scalable and flexible. It is cost effective.

Comparative Analysis

Table-1 compares forensic tools based on their performance, usefulness, accuracy, and key strength.

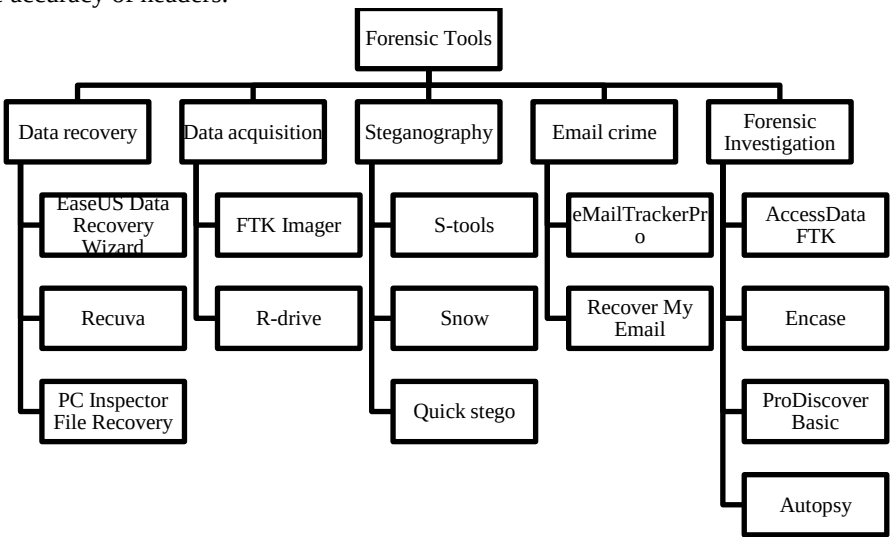

Figure-1: Types of Forensic Tools.

Table-1: Comparison of Tools.

Tool Category	Tool	Performance	Usability	Accuracy	Key Strength
Data Recovery	EaseUS	High	High	High	Deep recovery
	Recuva	Medium	High	Medium	Easy to use
	PC Inspector	Medium	Low	Medium	Partition recovery
Disk Imaging	FTK Imager	High	Medium	High	Forensic integrity
	R-Drive	High	Medium	Medium	Fast imaging
Steganography	S-Tools	Medium	Medium	High	Hidden data detection
	Snow	Low	Low	Medium	Text-based hiding
	Quick Stego	Low	High	Low	Simple usage
Email	EmailTrackerPro	High	Medium	Medium	Email tracing
	Recover My Email	High	Medium	High	Email recovery
Forensic Suite	FTK	High	Medium	High	Fast indexing
	EnCase	High	Medium	High	Industry standard
	ProDiscover	Medium	High	Medium	Beginner friendly
	Autopsy	High	High	High	Open-source flexibility

Conclusion

In this study, a number of contemporary cyber forensic programs in several domains, including data recovery, disc imaging, steganography, email investigation, and forensic suites, were compared. Each cyber forensic program is specifically designed to address particular investigative issues based on the analysis's findings. Commercial programs like EnCase and FTK were found to have more advanced features than their open-source rivals like Autopsy. Furthermore, the study discovered that no cyber forensic program can be employed on its own; as a result, an efficient combination of these systems is essential.

References

1. Alsaidi, N., Alshareef, M., Alsulami, A., Alsafri, M., & Aljahdali, A. (2020). Digital steganography in computer forensics. *International Journal of Computer Science and Information Security*, *18*(5), 54-61.

2. Berzinji, A. (2016). Forensic Tools For Investigating Cyber Crimes. *Asian Journal of Natural & Applied Sciences*, 5(3).

3. Bilous, V., Bodnenko, D., Lokaziuk, O., Skladannyi, P., & Abramov, V. (2025). Cyber Evidence Software as the Digital Forensics Tools in the Investigation of Cybercrime. *Cybersecurity Providing in Information and Telecommunication Systems*, (3991), 26-37.

4. Dubey, H., Bhatt, S., & Negi, L. (2023). Digital Forensics Techniques and Trends: A Review. *International Arab Journal of Information Technology*, 20(4).

5. Dweikat, M., Eleyan, D., & Eleyan, A. (2021). Digital forensic tools used in analyzing cybercrime. *Journal of University of Shanghai for Science and Technology*, 23(3), 367-379.

6. Fernando, V. (2021). Cyber forensics tools: A review on mechanism and emerging challenges. In *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)* (pp. 1-7). IEEE.

7. Hamad, N., & Eleyan, D. (2022). Digital forensics tools used in cybercrime investigation-comparative analysis. *Journal of Xi'an University of Architecture & Technology*, 4, 113-127.

8. Kaur, M., Kaur, N., & Khurana, S. (2016). A literature review on cyber forensic and its analysis tools. *International Journal of Advanced Research in Computer and Communication Engineering*, 5(1), 23-28.

9. Kaur, N., & Behal, S. (2014). A Survey on various types of Steganography and Analysis of Hiding Techniques. *International journal of engineering trends and technology*, 11(8), 388-392.

10. Kazaure, A. A., Jantan, A., & Yusoff, M. N. (2024). Digital forensic investigation on social media platforms: A survey on emerging machine learning approaches. *Journal of Information Science Theory and Practice*, 12(1), 39-59.

11. Salih, K. M. M., & Dabagh, N. B. I. (2023). Digital forensic tools: A literature review. *Journal of Education and Science*, 32(1), 109-124.

12. Paul Joseph, D., & Norman, J. (2018). An analysis of digital forensics in cyber security. In *First International Conference on Artificial Intelligence and Cognitive Computing: AICC 2018* (pp. 701-708). Singapore: Springer Singapore.

13. Prasanthi, B. V., Kanakam, P., & Hussain, S. M. (2017). Cyber forensic science to diagnose digital crimes-a study. *International Journal of Scientific Research in Network Security and communication*, 50(2), 107-113.

14. Prasanthi, B. V. (2016). Cyber forensic tools: a review. *International Journal of Engineering Trends and Technology*, 41(5), 266-271.

15. Qureshi, S., Tunio, S., Akhtar, F., Wajahat, A., Nazir, A., & Ullah, F. (2021). Network forensics: A comprehensive review of tools and techniques. *International Journal of Advanced Computer Science and Applications*, 12(5).

16. Shah, A. (2023). Evaluating network forensics applying advanced tools. *International Journal of Advanced Engineering, Management and Science*, 9(4), 01-09.

17. Vanlalsiama, B., & Jha, N. (2015). Cyber Forensic: Introducing A New Approach to Studying Cyber Forensic and Various Tools to Prevent Cybercrimes. *IITM Journal of Management and IT*, 6(1), 123-128.