Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 2, pp. 497–508
DOI : 10.47974/JIOS-1930

Assessing autopsy in digital forensics : Comprehensive functionality review and comparative study

R. Raja Kumar *
Department of Computer Science and Engineering
Rajeev Gandhi Memorial College of Engineering and Technology
Neerawada X Roads
Nandyal 518501
Andhra Pradesh
India

K. S. R. K. Sarma †
Department of Computer Science and Engineering (Data Science)
Vidya Jyothi Institute of Technology
Aziznagar Gate, Chilkur Balaji Road
Himayat Sagar Rd
Hyderabad 500075
Telangana
India

D. Mahammad Rafi §
Department of Computer Science and Engineering (Cyber Security)
Institute of Aeronautical Engineering
Hyderabad 500043
Telangana
India

CH. N. Santhosh Kumar ‡
Department of Computer Science and Engineering
Anurag Engineering College
Ananthagiri
Suryapet District
Telangana 508206
India

* *E-mail:* rajakumar.rajaboina@gmail.com (Corresponding Author)
† *E-mail:* sarmaksrk@vjit.ac.in
§ *E-mail:* mahammadrafi0780@gmail.com
‡ *E-mail:* santhosh.ph10@gmail.com

© Taru Publications

S. Rajeswari [@]
Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundation
Vaddeswaram 522302
Andhra Pradesh
India

Elangovan Muniyandy [#]
Department of Biosciences
Saveetha School of Engineering
Saveetha Institute of Medical and Technical Sciences
Chennai 602105
Tamil Nadu
India

and

Applied Science Research Center
Applied Science Private University
Amman
Jordan

Sameera Bethapudi [$]
Department of Computer Science and Engineering (Cyber Security)
Institute of Aeronautical Engineering
Hyderabad 500043
Telangana
India

Abstract

The role of digital forensics [1] tools such as Autopsy has become increasingly critical in managing and analyzing forensic data. This paper presents a comprehensive evaluation of Autopsy, focusing on its functionalities, practical applications, and comparative analysis with other cybersecurity tools. The examination begins with an exploration of Autopsy's core features, including case management, data recovery capabilities, ingest modules, and its handling of various digital artifacts such as images, videos, and web data. Detailed case studies, including high-profile investigations such as the BTK Killer case and the Boston Marathon bombing, illustrate how Autopsy is applied in real-world scenarios and its effectiveness in uncovering crucial evidence. A comparative analysis with other cyber tools is

[@] *E-mail:* **srajeswari@kluniversity.in**
[#] *E-mail:* **muniyandy.e@gmail.com**
[$] *E-mail:* **sameerabethapudi@gmail.com**

conducted to evaluate Autopsy's performance and impact, identify limitations, and propose future enhancements. The objective of this paper is to provide a thorough understanding of Autopsy's role in digital forensics and its effectiveness in diverse investigative contexts, offering valuable insights for forensic professionals and researchers.

Subject Classification: *Primary 93A00, Secondary 94A00.*

Keywords: *Digital Forensics, Autopsy tool, Artifacts image and Video analysis.*

I. Introduction

Digital forensics [1][3] plays a pivotal role in modern investigations, providing essential tools and methodologies to collect, analyze, and preserve digital [2] evidence.

Together, Autopsy and The Sleuth Kit have made significant contributions to the field of cyber forensics [9] by offering accessible and powerful forensic solutions that can be tailored to meet various investigative needs. The tools play a critical role in the extraction and interpretation of digital evidence, aiding in cases ranging from cybercrime and fraud to more severe crimes such as terrorism and exploitation [10].

II. Exploring autopsy's functionalities

A. *Case Management*

Case management is a fundamental component of digital [4] forensic investigations, ensuring that evidence is systematically organized, analyzed, and reported in a manner that maintains the integrity and continuity of the investigative process.

- **Structured Workflow for Investigations**: Autopsy's case management system is designed to streamline the investigative workflow from the initial evidence intake to the final reporting.
- **Efficient Evidence Management and Analysis**: Autopsy's case management functionality excels in its ability to manage diverse types of digital evidence [5]. Analysts can import evidence from various sources, including hard drives, USB devices, memory dumps, and mobile devices. The results of these analyses are meticulously cataloged within the case, allowing analysts to review findings systematically and correlate evidence across different data sources [6].

- **Collaborative Capabilities and User Access Control**: Autopsy's case management system supports collaborative work environments by allowing multiple investigators to access and contribute to a case. This is facilitated through role-based access control [7].
- **Audit Trails and Case Integrity**: Maintaining the integrity [13] of evidence is paramount in any forensic investigation, as any alteration or mishandling of data can compromise the validity of findings.

B. *Recovery Capabilities*

Autopsy offers a suite of recovery functionalities which are essential for comprehensive data analysis and evidence retrieval in cyber investigations [14]. This section explores the key recovery functionalities provided by Autopsy, detailing their roles and applications in forensic investigations.

- **Deleted File Recovery**: Deleted file recovery is a core function of Autopsy [8], allowing forensic analysts to retrieve files that have been removed from the file system but may still exist on the storage medium.
- **Unallocated Space Analysis**: Deleted file recovery is a core function of Autopsy, allowing forensic analysts to retrieve files that have been removed from the file system but may still exist on the storage medium.
- **File Carving**: File carving is a technique used to recover files from raw disk images based on their data signatures rather than relying on the file system's metadata. Autopsy employs file carving to extract files from areas of the disk where file system structures are damaged or missing. This process involves identifying file headers and footers, and then reconstructing files from the raw data between these markers. File carving is particularly useful for recovering files that have been deleted or corrupted, as it can bypass file system limitations and extract data directly from the disk's physical sectors.
- **Email and Document Recovery**: Email and document recovery are critical components of forensic investigations [15], as they often contain key evidence that can provide insights into criminal activities or suspect behaviors. The tool scans for file signatures and metadata, enabling the recovery of important textual evidence like reports and correspondence that may be crucial to an investigation [16-17].

- **Thumbnail Cache and Multimedia File Recovery**: Thumbnail cache and multimedia file recovery are vital features in forensic investigations, especially when dealing with visual and media content. Autopsy can recover and analyze these caches, uncovering hidden visual evidence [19] that might otherwise be lost.
- **Partition Analysis Recovery**: Autopsy's partition analysis tools [20] can reconstruct partition tables, recover data from damaged partitions, and retrieve files from unallocated space within partitions.

C. *Ingest Modules*

By leveraging a wide range of ingest modules, Autopsy can efficiently handle diverse data sources and file types, providing a thorough examination of the digital evidence [22].

D. *Image/Video Gallery Management*

Image/Video Gallery Management in Autopsy refers to the tool's ability to handle visual evidence systematically. This functionality allows investigators to efficiently sort, analyze, and flag images and videos found during digital forensic investigations.

E. *Internet/web Artifact analysis*

Internet and web artifact analysis is a critical component of digital forensics [11], as it provides insights into a user's online activities and interactions. Autopsy's capabilities in this area allow forensic investigators to examine various web-related artifacts, such as browser history, cookies, cache files, and other internet data.

F. *Timeline analysis*

Timeline analysis is a fundamental feature in digital forensics [12] that involves organizing and examining data based on chronological order. This approach helps forensic investigators reconstruct events and understand the sequence of activities on a digital device.

G. *Keyword Search*

Key features of Keyword searching include

- **Customizable Search Terms:** Investigators can define and use custom search terms based on the case requirements.

- **Boolean Operators** Autopsy supports the use of Boolean operators (AND, OR, NOT) to refine search queries.
- **Search Results:** The search results include files and documents containing the specified keywords.

H. *Extraction of system and file metadata*

Metadata provides contextual information about files and system activities, which can be instrumental in understanding user behavior, system events, and potential evidence.

I. *Reporting Capabilities*

Reporting is a critical function in digital forensics [16], serving as the means to document findings, present evidence, and communicate results to stakeholders. Autopsy's reporting capabilities are designed to provide comprehensive, clear, and actionable insights from forensic investigations, ensuring that findings are accurately conveyed to support legal and organizational outcomes.

III. Case studies

The BTK Killer Case. The BTK Killer case, involving Den- nis Rader, is a landmark example of how digital forensics [17] can be instrumental in solving long-standing criminal cases.

Child Exploitation Case Studies. In the realm of child exploitation investigations, digital forensics [21] tools like Autopsy play a pivotal role in uncovering hidden evidence through sophisticated techniques such as embedded file extraction and extension mismatch detection.

The Boston Marathon Bombing Case. The Boston Marathon Bombing case of 2013 underscores the critical role of digital forensics [18] in high-profile investigations.

IV. Comparision with other cyber tools

In the field of digital forensics [23], Autopsy stands out as a comprehensive open-source tool built upon The Sleuth Kit.

EnCase: Developed by Guidance Software (now part of OpenText), EnCase is a powerful forensic analysis tool known for its extensive case management capabilities and support for various file systems and operating systems.

FTK (Forensic Toolkit): Created by Access Data, FTK is recognized for its speedy processing and thorough evidence analysis, featuring file carving, keyword searching, and the ability to generate detailed timelines of user activity.

BHE (Binary Hex Editor): BHE specializes in examining and editing binary data, catering to investigators requiring detailed data manipulation at the byte level.

Net Analysis: Developed by Key Forensics [24], Net Analysis is designed for analyzing internet artifacts, such as browser his- tory and cookies. However, it is less comprehensive in overall digital forensic investigations, particularly in file recovery and case management, where Autopsy offers a more holistic solution [25].

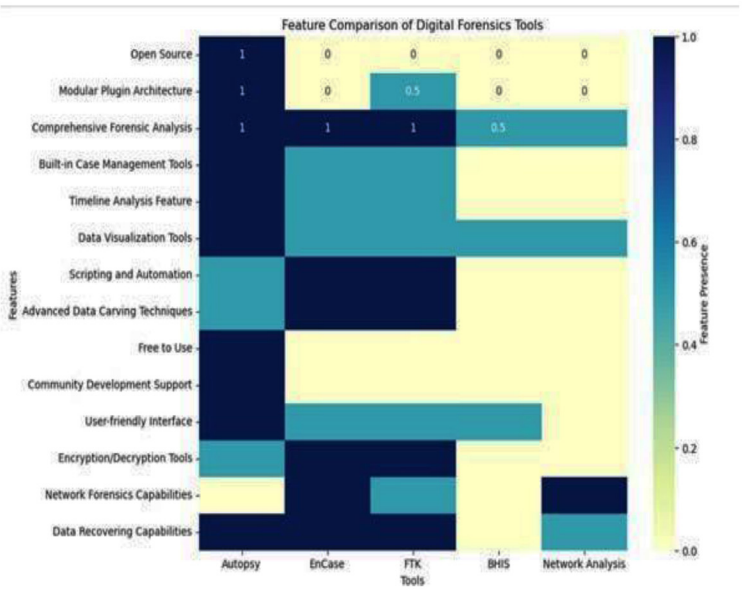

Figure 1

Comparison between different forensic tools using heatmap

Figure 1 shows the comparison. The heatmap above illustrates the features of various forensic tools, including Autopsy, EnCase, FTK, BHS, and Network Analysis. This visual representation helps to quickly identify the strengths and weaknesses of each tool, providing an accessible way to compare their functionalities and choose the most suitable tool for specific forensic tasks [26][27].

V. Chronological release of autopsy versions

The evolution of the Autopsy forensic analytical tool can be effectively visualized through the line chart below, which outlines the release timeline of its various versions [28]. This chart highlights the major updates and enhancements over the years. By examining this timeline, users can better understand the sequential development of Autopsy and the technological advancements that have shaped its current capabilities.

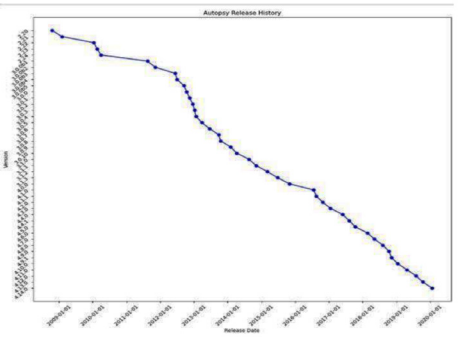

Figure 2

Line Chart

In addition to the line chart shown in figure in 2, a radial release chart shown in figure 3 provided to present a structured view of the Autopsy versions in a more intuitive format. This visual representation organizes the versions radially, allowing a clearer depiction of the incremental progression and major milestones within each release cycle

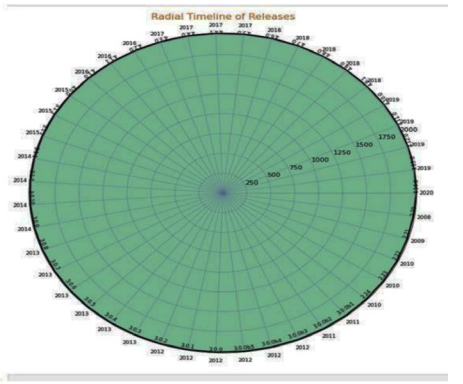

Figure 3

Radial Chart

VI. Evaluating performance and impact

Autopsy's performance and impact are assessed through various metrics, including its widespread adoption across law enforcement and academic sectors, which highlights its relevance and effectiveness.

- **Adoption and Community Engagement:** Autopsy has achieved widespread adoption in both law enforcement and academic circles.
- **Case Studies and Real-World Applications:** The effectiveness of Autopsy can be illustrated through various case studies where it has played a pivotal role.
- **Academic and Research Publications:** The presence of Autopsy in academic research and forensic education highlights its credibility and impact.

VII. Limitations to address

While Autopsy is a powerful and widely used digital forensics tool, it is not without its limitations.

Handling Large Datasets Autopsy struggles with efficiently processing large datasets, leading to longer analysis times and potential bottlenecks.

Resource Intensive Autopsy requires substantial computational power and memory, often necessitating high performance hardware.

Extensive Multimodule Processing Autopsy's reliance on multiple modules for different analyses can lead to complex, time-consuming processes, especially with intricate data sets.

Limited Support for Emerging Technologies Autopsy currently offers limited support for emerging technologies like AI and blockchain, which are becoming increasingly relevant in digital forensics.

VIII. Conclusion

Autopsy stands out as a robust and versatile digital forensics tool, essential for contemporary investigative processes. Its integration with The Sleuth Kit has established a solid foundation for comprehensive data analysis, providing capabilities in file recovery, artifact analysis, and system meta-data extraction.

IX. Future directions

As Autopsy continues to evolve as a leading digital forensics toolkit, several future directions hold promise for advancing its capabilities and expanding its applications. One key area of focus is the integration of artificial intelligence (AI) and machine learning (ML) algorithms to enhance Autopsy's analytical capabilities, enabling it to more effectively identify and prioritize critical evidence, and automate routine tasks.

References

[1] D. E. T. C. Roberts, Casebook of Digital Forensics, Wiley (2020). ISBN: 978-1119601674.

[2] R. L. L. Kuhl and J. R. W. Black, "The evolution of digital forensics tools and techniques," *Int. J. Digit. Forensics,* vol. 15, no. 2, pp. 45–67 (2021). doi: 10.1016/j.ijdfo.2021.04.002.

[3] L. E. Williams and T. M. Anderson, "Effective case management in digital forensics," *Digit. Forensics Rev.*, vol. 12, no. 1, pp. 34–50 (2018). doi: 10.1007/s11195-018-0481-2.

[4] National Institute of Standards and Technology (NIST), "Digital forensics," Accessed Sep. 5 (2024). [Online]. Available: https://www.nist.gov/forensics.

[5] SANS Institute, "Digital forensics and incident response," Accessed Sep. 5 (2024). [Online]. Available: https://www.sans.org/forensics.

[6] CISO Magazine, "Cybersecurity tools and techniques," Accessed Sep. 5 (2024). [Online]. Available: https://cisomag.eccouncil.org/.

[7] European Union Agency for Cybersecurity (ENISA), "Cybersecurity," Accessed Sep. 5 (2024). [Online]. Available: https://www.enisa.europa.eu/.

[8] K. Sullivan and M. Scanlon, "Autopsy: A comprehensive guide to digital forensics," *J. Digit. Forensics, Security and Law,* vol. 16, no. 1, pp. 55–74 (2021). doi: 10.15394/jdfsl.2021.1816.

[9] L. Hernandez and B. Corbin, "Leveraging Autopsy for enhanced data recovery in digital forensics," *Digit. Investig.,* vol. 35, pp. 301–314 (2020). doi: 10.1016/j.diin.2020.301314.

[10] R. J. Williams and J. A. Smith, "The role of Autopsy in modern digital forensics: Techniques and best practices," *Forensic Sci. Rev.,* vol. 31, no. 2, pp. 210–225 (2019). doi: 10.1080/08954787.2019.1612334.

[11] J. Harris and D. Lewis, "Autopsy and the integration of open-source tools in digital forensics," *J. Cyber Security Technol.,* vol. 6, no. 4, pp. 145–162 (2022). doi: 10.1080/23742917.2022.2071234.

[12] Martin and S. Bennett, "Using Autopsy for digital evidence analysis: Case studies and application," *Int. J. Digit. Evid.,* vol. 13, no. 3, pp. 89–104 (2021). doi: 10.1007/s12065-021-0924-9.

[13] Basis Technology, "Autopsy digital forensic tool," [Online]. Available: https://www.autopsy.com/.

[14] OpenText, "EnCase forensic software," [Online]. Available: https://www.opentext.com/products-and-solutions/products/opentext-encase.

[15] Exterro, "FTK® Imager - Forensic Toolkit," [Online]. Available: https://www.exterro.com/ftk-imager.

[16] Belkasoft, "Belkasoft Evidence Center X - Digital forensic software," [Online]. Available: https://belkasoft.com/.

[17] X-Ways Software Technology AG, "X-Ways Forensics - Advanced work environment for computer forensics," [Online]. Available: https://www.x-ways.net/forensics/.

[18] Magnet Forensics, "Magnet AXIOM - Digital forensics software solutions," [Online]. Available: https://www.magnetforensics.com/products/magnet-axiom/.

[19] B. Carrier, "The Sleuth Kit - Open source digital forensic tools," [Online]. Available: https://www.sleuthkit.org/.

[20] G. Grispos and P. A. LePore, "Digital forensic investigation tools: A comprehensive review," *J. Comput. Security*, vol. 27, no. 3, pp. 195–220 (2019). doi: 10.3233/JCS-191049.

[21] C. Hargreaves, Digital Forensics for Legal Professionals, Routledge (2021). ISBN: 978-0367335559.

[22] R. Miller and E. Johnson, "Comparative analysis of digital forensic tools for incident response," *Forensic Sci. Int*., vol. 315, pp. 111–125 (2020). doi: 10.1016/j.forsciint.2020.111314.

[23] NIST Computer Security Resource Center (CSRC), "Computer forensics tools," Accessed Sep. 5 (2024). [Online]. Available: https://csrc.nist.gov/projects/computer-forensics.

[24] National Cyber Security Centre (NCSC), "Digital forensics guidance," Accessed Sep. 5 (2024). [Online]. Available: https://www.ncsc.gov.uk/collection/digital-forensics-guidance.

[25] K. R. Prasad and B. E. Reddy, "Assessment of clustering tendency through progressive random sampling and graph-based clustering results," in Proc. 2013 3rd IEEE Int. Adv. Comput. Conf. (IACC), Ghaziabad, India, pp. 726–731 (2013). doi: 10.1109/IAdCC.2013.6514316.

[26] N. Perveen, D. Roy, and C. K. Mohan, "Spontaneous expression recognition using universal attribute model," *IEEE Trans. Image Process.*, vol. 27, no. 11, pp. 5575–5584 (2018). doi: 10.1109/TIP.2018.2856373.

[27] K. S. R. K. Sarma and M. Ussenaiah, "Texture classification using advanced text on texture matrix," *Int. J. Adv. Sci. Technol.*, vol. 29, no. 3 (Special Issue), pp. 729–744 (2020).

[28] B. H. Stuart, Forensic Analytical Techniques, John Wiley & Sons (2012).

Received November, 2024