Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April-2025 | Page 988-993

A Review on Comparative Analysis of Commercial and Open-Source Digital Forensic Tools

Harika Diwaker
BSc forensic science
Department of Forensic Science
Kalinga University, New Raipur, Chhattisgarh, India

Abstract

This paper provides a systematic comparison of commercial and open-source digital forensic tools. It addresses the critical need for reliable tools in the context of increasing cybercrime by analyzing key parameters such as usability, cost, performance, scalability, and legal admissibility. Through a secondary research methodology utilizing recent (2020-2025) peer-reviewed literature, the study identifies the distinct advantages and limitations of both commercial tools (e.g., EnCase, FTK) and open-source alternatives (e.g., Autopsy, Sleuth Kit). Key findings highlight the professional support and legal validation of commercial tools versus the cost-effectiveness and customization of open-source options. The dissertation advocates for a complementary approach in tool selection based on specific investigative scenarios. While acknowledging its strengths in breadth of sources and current data, the review also notes limitations such as the absence of primary data and in-depth technical or legal analysis. Ultimately, the dissertation offers valuable insights for law enforcement, policymakers, and academics, concluding that a hybrid strategy leveraging both types of tools represents the most effective approach to digital forensic investigations.

1. Introduction

Digital forensics is a critical branch of forensic science focusing on the identification, acquisition, preservation, analysis, and presentation of digital evidence. With the proliferation of cybercrime, the need for reliable forensic tools has become paramount. This review analyzes Harika Diwaker's undergraduate dissertation submitted to Kalinga University, which presents a systematic comparison between commercial and open-source digital forensic tools. The dissertation explores key parameters like usability, cost, performance, scalability, and legal admissibility.

2. Objectives of the Dissertation

The dissertation sets out to:

- Compare commercial and open-source forensic tools based on empirical data and case-based analysis.
- Understand the advantages and limitations of both types in digital investigations.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April-2025 | Page 988-993

- Offer guidance for forensic analysts in selecting suitable tools for specific scenarios.

The work addresses a growing need for comprehensive benchmarking of forensic tools, particularly in the context of legal reliability and tool interoperability.

3. Literature Contributions and Theoretical Background

The dissertation is supported by a strong literature review from credible sources:

- **Kumar & Kumar (2024)** and **Kolla (2022)** provide side-by-side functional comparisons of tools such as FTK, EnCase, Autopsy, and Sleuth Kit, focusing on operational capabilities and legal credibility [Kumar & Kumar, 2024:
- As the complexity of the cybercrime increases, the selection of forensic tools has become a vital concern for the forensic investigators. Kolla (2022) discussed about widely used digital forensic tools, OS Forensic and Autopsy providing detail on their performance, usability, support/documentation and its real-world application. Kolla's study contributes to existing literature by addressing a crucial gap in comparative analysis of forensic tools. He finds that Autopsy, being open-source and built on The Sleuth Kit (TSK), offers more friendly interface which supports faster learning curves for beginners. In contrast OS Forensics is noticed to have more complex interface, due to its advanced features and options suggesting that more appropriate for experienced forensic analysts who require control over investigation parameters.
- Kumar & Kumar (2024) did vital comparative examination of open-source and commercial-source tools, focusing on their operational capabilities, cost effectiveness, usability, and legal reliability. They compared well-know commercial tools like EnCase, Falcon Neo, TX1, FTK (Forensic tool kit) against open-source alternatives like Autopsy, Sleuth Kit and CAINE (Computer Aided Investigative Environment). They tested functionality of the tools separately on digital media formatted with windows. The test was performed on each SSD media file after wiping the data from the media and repeated after formatting the media. The results of the experiments conducted show that both proprietary and open source computer forensics tools perform better in different scenarios and that the tools can be used to validate and complement each other.

- Ismail *et al.* (2024) study focuses on the capabilities, reliabilities, transparency, and legal admissibility of open-source digital tools providing a comprehensive overview of their role in digital forensic investigations. Their study aims to assess whether opensource tools can serve as viable alternatives to proprietary solutions in digital forensic investigations. They developed a conceptual framework to ensure the admissibility of the evidence so that it will be accepted in the court of law. This conceptual frame work was formed to outline the factors affecting the admissibility of digital evidence from opensource digital forensic tools, which include;1) The Availability and Capabilities of open-source digital forensic tools 2) the

Reliability and Integrity of the digital evidence obtained from opensource digital forensic tools 3) the Transparency of the open-source digital forensic tools and 4) the Lack of Reference and Standard of open-source digital forensic tools.

- Dweikat *et al*. (2021) their study highlights the necessity for advanced digital tools that are capable of addressing cyber offences such as data breaches, unauthorized access and financial frauds. The authors widely classified digital forensic tools into three primary domains: 1) Computer Forensics,2) Mobile Forensic and 3) Network Forensic. They also highlighted that tools like EnCase and FTK are robust in data acquisition and analysis, other like Pro Discover offer real-time capabilities that are essential for live investigation. Their study also emphasizes that no single tool is universally effective; instead, forensic investigators must choose digital forensic tools based on case-specific needs and technological environments. The importance of continuous research and use of updated digital forensic tools to maintain their relevance in increasingly complex cybercrime investigation is underlined in this paper.

4. Methodology

The dissertation adopts a **secondary research design**, employing literature from 2020 to 2025. The inclusion criteria focus on peer-reviewed, English-language articles addressing comparative. analysis of digital forensic tools. Boolean logic was used for database searches, and articles not aligned with forensic applications or lacking empirical data were excluded.

5. Key Findings

5.1 Commercial Tools

Commercial tools like EnCase, FTK, X-Ways, and Tableau TX1 are praised for:

- Professional technical support
- Legal validation
- Regular software updates
- High-speed forensic imaging and extensive reporting features

However, they often come at a high cost, limiting their accessibility for small-scale agencies.

5.2 Open-Source Tools

Tools such as Autopsy, Sleuth Kit, DFF, and FTK Imager offer:

- Cost-effectiveness
- Customization via open-source code

- Community-driven innovation

Yet, limitations include lack of official certification, technical complexity, and inconsistent legal acceptance.

5.3 Complementary Use

The dissertation wisely argues that both tool types can **complement each other**, depending on the scenario. For example, FTK may be used for imaging, while Autopsy can be used for timeline analysis.

6. Strengths of the Dissertation

- **Breadth of Sources:** A wide range of peer-reviewed articles provide a multi-dimensional view.
- **Clear Comparative Matrix:** Strengths, weaknesses, and legal admissibility are discussed comprehensively.
- **Current and Relevant Data:** Only recent (post-2020) studies are used, ensuring relevance.

7. Limitations Identified

- **Lack of Primary Data:** The study is entirely literature-based and lacks experimental or case-based validation.
- **Tool Depth:** While multiple tools are discussed, the level of technical depth on each remains introductory.
- **Legal Analysis:** Though court admissibility is mentioned, deeper engagement with real legal precedents is absent.

8. Practical Implications

This dissertation is highly valuable for:

- **Law enforcement agencies**, in tool procurement.
- **Policy makers**, for drafting guidelines on digital evidence admissibility.
- **Academicians and students**, as a foundation for more technical or empirical studies.

9. Recommendations for Future Research

- Conduct **experimental benchmarking** of tools under controlled conditions.
- Explore **AI integration** in forensic tools.

- Analyze **cross-border legal frameworks** on digital evidence to understand admissibility and compliance.

10. Conclusion

The dissertation by Harika Diwaker makes a solid academic contribution to forensic science by systematically comparing commercial and open-source digital forensic tools. It demonstrates that neither category is universally superior; instead, the selection must depend on the context, resources, and investigative needs. A hybrid approach—leveraging the strengths of both commercial and open-source tools—is presented as the most effective strategy for contemporary forensic investigations.

References

1. Kolla, V. R. K. (2022). A Comparative Analysis of OS Forensics Tools. International Journal of Research in IT and Management (IJRIM), 12(4).
2. Kumar, R., & Kumar, S. (2024). COMPARATIVE ANALYSIS OF COMMERCIAL AND OPEN-SOURCE DIGITAL FORENSIC TOOLS.
3. https://jcsdf.nfsu.ac.in/Uploads/EJournal/5/5/(20-30)%20COMPARATIVE%20ANALYSIS%20OF%20COMMERCIAL%20AND%20OPEN-SOURCE%20DIGITAL%20FORENSIC%20TOOLS.pdf
4. Ismail, I., & Ariffin, K. A. Z. (2024). Open Source Tools for Digital Forensic Investigation: Capability, Reliability, Transparency and Legal Requirements. KSII Transactions on Internet and Information Systems (TIIS), 18(9), 2692-2716. https://koreascience.kr/article/JAKO202430943227984.pdf
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. https://www.academia.edu/download/79747753/Digtal-Forensic-Tools-1.pdf
6. Bhattacharya, S. (2023). Comparative Study of Proprietary and Open-source Software used in Recovering Volatile Data (Doctoral dissertation, University of Technology).
7. https://www.researchgate.net/profile/Sagarnil-Bhattacharya/publication/375487419_Comparative_Study_of_Proprietary_and_Open-source_Software_used_in_Recovering_Volatile_Data_Under_the_Supervision_of/links/654bba9b3fa26f66f4e74ce2/Comparative-Study-of-Proprietary-and-Open-source-Software-used-in-Recovering-Volatile-Data-Under-the-Supervision-of.pdf
8. KOMITI, P. T. Comparative Analysis of Commercial And Open-Source Tools in The Examination And Analysis of Web Browser Data.
9. Bhatia, M. K., Gambhir, P., Sinha, S., & Singh, S. K. A Comparative Analysis of OS Forensics Tools. Int. J. Res. Appl. Sci. Eng. Technol, 10(11), 494-502. https://www.academia.edu/download/94381534/A_Comparative_Analysis_of_OS_Forensics_Tools.pdf
10. Sachdeva, S., Raina, B. L., & Sharma, A. (2020). Analysis of digital forensic tools. Journal of Computational and Theoretical Nanoscience, 17(6), 2459-2467.

https://www.researchgate.net/profile/Avinash-Sharma-26/publication/346809308_Analysis_of_Digital_Forensic_Tools/links/5fe315bf299bf1408837612b/Analysis-of-Digital-Forensic-Tools.pdf

11. Javed, A. R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K., & Gadekallu, T. R. (2022). A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions. IEEE Access, 10, 11065-11089. https://ieeexplore.ieee.org/iel7/6287639/6514899/09678340.pdf
12. Bhat, W. A., AlZahrani, A., & Wani, M. A. (2021). Can computer forensic tools be trusted in digital investigations?. Science & Justice, 61(2), 198-203. https://doi.org/10.1016/j.scijus.2020.10.002