Performance and Application of Digital Forensic Tools: A Comparative Study

Savali Deshmukh and Pramod Kumar Jha

Abstract Currently, computers and the Internet are used to conduct the majority of business transactions, communications and the automated control of industrial equipment, among other things. Working online makes the process more efficient and convenient. The risk of cyber-attacks has also increased significantly as a result of devices being exposed to the Internet on a daily basis. The Internet's speed, ease of use and invisibility, lack of geographical boundaries cyber financial crimes, stalking and bullying are becoming more commonplace, according to the FBI. A digital forensic investigation carried out with the assistance of software tools yields evidence against cybercriminals that can be presented in court. This review work aimed to evaluate and compare the performance and applications of ten online digital forensic tools. The conclusions, limitations of these tools and how after moral improvement, they can be used to assist digital forensics professionals in discovering digital evidence are presented.

Keywords Digital forensic tools · Cybercrime · Open-source software · Performance · Application

1 Introduction

Modern digital forensics deliver reliable computer analysis and digital evidence collecting for a wide range of applications in law and industry. As a result, prototype implementations are commonly included in research projects. For example, look at the DJI Phantom III Drone [1]. The findings on the patented encrypted file format were reported in their research work in which a reference manager to automate the

S. Deshmukh (✉)
School of Computer Science and Engineering, Vellore Institute of Technology—AP University, Amravati, India
e-mail: sadip.19bce7348@vitsap.ac.in

P. Kumar Jha
Centre for Advanced Systems, DRDO Hyderabad, Hyderabad, India
e-mail: pkj@cas.drdo.in

B. Pati et al. (eds.), *Proceedings of the 6th International Conference on Advance Computing and Intelligent Engineering*, Lecture Notes in Networks and Systems 428,
https://doi.org/10.1007/978-981-19-2225-1_57

process was also included. Although digital storage media (such as a USB memory stick or a hard disc drive) may be physically and visually examined, the data stored on these devices can only be analysed using specialised equipment and software capable of deciphering and displaying it understandably. While microscopic technologies may allow for manual data analysis on specific device types at a sector level, it is not practical to investigate media in this manner in most cases. And, when it comes to accurately interpreting and presenting digital evidence, forensic investigators rely on the digital software tools they use for the investigation [2].

In private, digital forensic techniques are frequently used to find a piece of evidence that can be utilised in court, reverse engineering of computer systems, data recovery, maintenance and troubleshooting [3]. Online digital forensics can be used by any user who has a clear idea about their needs. Specific tools are created for this exact reason, helping one choose which software would best solve one's requirement. Additionally, the creation of digital forensic competitions encourages tool development, with the Digital Forensics Research Workshop (DFRWS) challenges being a notable example. The DFRWS conferences have been challenging scholars and practitioners since 2005 to push the state of the art in developing forensic tools [4].

1.1 Introduction to Cyber Crimes

When dealing with a cybercrime scene, it is critical to pay close attention to digital evidence as the crime scene evidence is presented in an electronic form, which significantly distinguishes cybercrime from traditional crime. Further, it facilitates the criminal to store, hide, spread and delete information, making arresting cybercrime suspects more difficult [5].

According to [6], cybercrime covers the following:

1. Intellectual property theft
2. Damaging of service networks of a company
3. Financial fraud
4. The intrusion of hackers system
5. Distribution of execution virus and worms

Cybercrime can be split into three comprises or "3Ts" [7]:

i. Tools to commit a crime
ii. Targets of the crime (Victim)
iii. Material that is tangential to the crime

To detect and find evidence against a cybercrime, digital forensic can be used. Wang and his team devised a strategy of leveraging forensic toolkits to aid the collecting of robust digital evidence in order to keep the compelling clues from computer-based systems. As a result, vital tracks left at a cybercrime scene can be used to convict the perpetrators. To raise awareness of cybercrime, researches created a Web forensic framework based on four different sorts of patterns that provide them with proof of harmful Bot activity on Web services [8].

1.2 Introduction to Tools

Tools are not only made for a specific purpose but also for general use [9]. However, Lexico defines a tool as a device or implementation that is used to perform a specific function [10]. They have also been described as a self-contained tool and provide a particular amount of automation, i.e. user intervention is minimal, reduced and abstracted. For example, a tool should not need the user to determine sector numbers or translate virtual to physical addresses manually to access the disc. Individuals or research groups frequently create and use forensic tools in any computer language of their choice. Also, if a tool is automated, it can be employed in other programmes. Various forensic tools support us in obtaining the disc images and automating much of the analysis process as well, such as:

I. File fragments, hidden and deleted files and directories can be identified and recovered from any location
II. The file structure, headers and other aspects determine directly the kind of data each file contains
III. All the contents of the graphic files can be displayed
IV. Advanced searches can be conducted
V. Can exhibit the directory structure of the drive acquired graphically
VI. And producing the reports

The Autopsy tool, an upgraded version from the sleuth kit forensic tools with some add-ons, is used in the fields of law enforcement, military, corporate examination, recovery, data backup, training and in some commercial areas with restriction included or with the limited privileges over the problems. Wireshark is a packet sniffer and analyser and records on the local network all the network traffic and saves it for later study. The Metasploit framework is a forensic tool that may be used by both cybercriminals and ethical hackers to investigate network and server vulnerabilities. Nessus is a remote complete security scanning programme that checks for security flaws on a computer and informs you whether such vulnerabilities may potentially be exploited by malicious hackers to grant access to other networked computers. Nmap is a free network mapper that uses IP packets to search a network for live hosts, port scans, ping sweeps, OS detection and version detection. AccessData created FTK Imager, a data viewing and imaging application. Volatility is a memory forensics framework that is free (under the GPL licence) and can be used for incident response and malware investigation. Computer-aided investigate environment (CAINE) is a Linux distribution that provides a detailed forensic investigation and reporting environment, with a graphical user interface that is designed to let users examine, investigate and gather actionable findings. MAGNET RAM Record is an effective imaging technique because it allows investigators to extract and examine artefacts that usually only exist in local physical memory. Network Miner is a network forensics programme that utilises packet sniffing or a PCAP file to identify OS, sessions, hostname and open ports without putting any traffic on the network.

1.3 Motivation and Contributions

No research has been done on the diversity, availability or quality of the tools that have been published. As a result, this review work came up with the following study question: What factors influence the applicability and use of tools? To get an answer to this question, the research papers from a variety of digital forensics magazines and conferences and tools' performance and applications have been studied. Tools were tested for availability, usability, deployment, GUI, error prevention and handling and API integration. Along with this, the current challenges in the area of forensic tool development have been discussed in the paper.

2 Methodology

In this review work, the research and review publications on digital forensic tools' performance, applications and limitations were reviewed and analysed. The purpose of this investigation is to locate software mainly designed for research purposes, as well as to investigate any preceding work or other features of these tools. Figure 1 shows how the current work was written using the process of a detailed review. Cumulated research articles were reviewed explicitly, focusing on tools usability and limitations. Tools were tested on their performance features such as availability, deployment, GUI, error prevention and handling and API integration. Along with this, research articles were found where the application of any of these tools in digital forensic or any other field was proven. The result of the comparative study was separated and documented into two tables. With the help of these two tables, the various features of each tool, their application and their limitations are concluded.

3 Observations

After segregating the tool-specific research articles, the software tool's performance was tested depending on various key features. It is essential for a tool to be deployed so as to create a collaborative environment. This would make it easy for everyone to see all of the outcomes in near real time. Hence, there's no need to integrate the results anymore, and a single, unified report may be generated at any moment [11]. Autopsy provides the best collaborative environment. GUI is by far the most popular

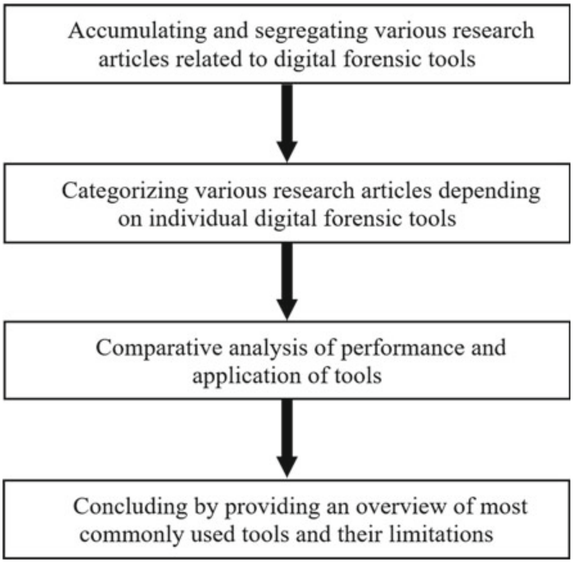
Accumulating and segregating various research articles related to digital forensic tools
Categorizing various research articles depending on individual digital forensic tools
Comparative analysis of performance and application of tools
Concluding by providing an overview of most commonly used tools and their limitations

Fig. 1 Steps involved in the review

means used to interact with software today [12]. As it enables increased productivity, while also reducing cognitive stress. It is critical to effectively prevent and handle errors in requirements analysis and design to improve software productivity and reliability [13]. Since many software are developed to support a wide range of applications. It is critical for software tools to rely on the implementation of mature application programming interfaces (APIs) to facilitate the growth of software for artificial intelligence of things (AIoT) [14] (Table 1).

This research work also highlights the various applications in which these forensic tools were used. Table 2 gives the observations made by authors while they were using these software tools for their requirements. The various fields in which these tools are incorporated prove that the digital forensics community has a strong application orientation, which means we solve problems in practice rather than a theory. After reviewing the works, we have tabulated the application, conclusion and limitations of tools observed by the authors.

3.1 Limitations Observed

To be admissible in court, digital forensics must follow a specific collection, analysis and reporting process. Despite the expanding use of electronic forensics to help out in criminal cases and the necessity for practical tools, NIST's forensic tool testing programme remains the only one available. Also, digital forensic tools have no international standard.

Table 1 Performance analysis of tools

Name of software	Deployment	GUI	Error prevention and handling	APIs
Autopsy	Single and multi-user	Easy to understand	Not considered	Integrated
Wireshark	Single user	Can be improved	Uses macros based on kazlib's exception code	Lack of integration
Metasploit	Metasploit pro deploys single and multi-user	Easy to understand	Not considered	Integrated with Metasploit pro with REST API command
Nessus	Single user	Can be improved	It can find vulnerabilities but cannot prevent attacks	It supports API, but Nessus pro does not
Nmap	Single user	Zenmap is the GUI version of Nmap	To implement an exception handler Nmap, new try API method is used	Nmap API enables integration
FTK imager	Single user	Easy to understand	Not considered	Integrated
Volatility tool	Single and multi-user	Absence of GUI	Can detect bugs, viruses and malware but cannot prevent attacks	Apihooks are used to detect API hooks in-process and kernel memory
CAINE	Single user	Easy to understand	Built-in tools which can handle errors	Lack of integration
MAGNET RAM capture	Single user	Easy to understand	Not considered	Lack of integration
NetworkMiner	Single user and Xplico allows multi-user	Easy to understand	Not considered	Integrated

The lack of support, documentation, updates and the software's safety are all risks associated with using free tools/software. Tools used in the research were either poorly documented or not documented at all. The study highlights the poor user interface and developers' disinterest. Despite publication, it has been discovered that most tools were only used in cited works (2014) [25]. When limited test data is provided, or only specific tool versions or single picture format is inputted, the NIST tool testing requirements are "narrowly specified" [26]. There is also a lack of testing methods to analyse the tool reliability that exist for established technologies as well.

Because no single digital forensics tool can do everything due to the ongoing evolution of the field, researchers frequently build solutions to fill in the gaps left

Table 2 Application analysis of tools

Authors	Name of software	Application	Conclusion	Limitations observed
Negrão and Domingues [15]	Autopsy	Autopsy's SpeechToText modules identify and transcribe voice material	The detection and transcription can speed up the process of finding relevant information in audio files in forensic images	Saved amr files without headers were not detected by autopsy and had to be converted to WAV
Umar et al. [16]	Wireshark	Using an android-based live email service, they compared Wireshark and NetworkMiner forensic tools	NetworkMiner forensic tools have succeeded in getting more digital evidence than Wireshark	Wireshark cannot capture the receiving port
Tantawy et al. [17]	Metasploit	Metasploit modules are used to semi-automate attack injections	The authors demonstrated the need for an integrated approach to safety and security system design	Asynchronous communication does not slow down control algorithm performance or support Metasploit capabilities
Bairwa et al. [18]	Nessus	Identification of the underlying vulnerabilities	Nessus is a commonly used tool and shows the best scanning capabilities in comparison with the other tools for the selected vulnerabilities	It lacks functionalities and so cannot be integrated with another tool that acts differently and produces different results
Wiberg [19]	Nmap	In an active scan, Nmap scans the target using information files and SCADAScan options	The prototype application can take advantage of Nmap's extensive active scanning capabilities	When performing port recognition or service detection on SCADA devices, it reveals a flaw

(continued)

by existing tools. It is difficult to quantify how research has affected the real world since most of the study is academic-focused. This also leads to a trade-off between academic and field interests. Authors point out how digital forensic is applicable in various areas, and as a result, collaboration and transparency are required, possibly through programmes that distribute research-based tools to industrial participants who would not otherwise contact with academia [27].

Table 2 (continued)

Authors	Name of software	Application	Conclusion	Limitations observed
Dykstra and Sherman [20]	FTK imager	FTK imager was tested to find its effectiveness in remotely acquiring forensic evidence through cloud computing	Remote access to a hard disc and memory image was successful	Since a lot of trust and risk is involved, the authors do not recommend using EnCase and FTK for remote forensics in the cloud
Ghafarian and Wood [21]	Volatility tool	Memory analysis for obtaining operating system level data	Volatility is a set of commands that parse the memory tree structure and report memory activity in processes and their interrelationships	Even though both volatility and process monitor expose data, establishing a link between the suspect and Skype actions is challenging
James and Gladyshev [22]	CAINE	Both programmes, along with Deepthought, were run from a CD on five test systems with known cryptographic hash values to see if they changed data	CAINE and Deepthought showed no effect on the test discs data	Time is taken per device for enhanced preview processing
Faiz and Prabowo 2019 [23]	MAGNET RAM capture	Comparison between five software for the acquisition of the best random-access memory	Most artefacts captured, registry key and DLL by the magnet RAM capturer	It took the longest processing time in seconds
Song et al. 2019 [24]	Network Miner	Comparing machine learning and rule-based approaches like NetworkMiner for OS identification	Machine learning along with OS attribute values correctly identified the operating systems	When it comes to OS identification, IP and timestamp are frequently left out

A tool is primarily built based on the developer's individual demands and preferred language. The tool is not thoroughly tested or documented due to lack of robustness and maintainability. Insecure coding compromises security, dependability, flexibility and scalability. No technologies exist to extract IoT traces from mobile devices.

Collecting and analysing IoT memory is also difficult. Bluetooth, Zigbee and Z-Wave forensics tools must be added.

4 Conclusions and Future Work

Due to the fact that the vast majority of transactions and communication in today's world takes place online, digital security has become increasingly important. The demand for forensic-based approaches and tools has also skyrocketed as a result of this. Accurate computer analysis and digital evidence collection are required for various legal and commercial applications, and digital forensics technologies are critical in this regard. This review work provides a comparison of a number of free source digital forensic tools, which anyone can use depending on their requirements. In this comparison, the tools are evaluated on a variety of criteria, allowing users to choose the tool that best meets their needs and, as a result, provided superior forensic visualisation. Various performance features along with applications of these ten tools are tabulated. The work also discusses the limitations for forensic tools like reliability, usability, maintainability and the need of integrating IoT. These observations can be utilised to develop software that meets the needs of digital forensics professionals. The advancement of these forensic techniques will significantly aid in the discovery of digital evidence.

It is proposed to extend this comparison study of digital forensic tools on various other factors and across other forensic tools, which will give a better insight into these tools. It can further work to provide a set of guidelines for designing digital forensics tools.

Author Contributions Savali Deshmukh: Performed the analysis, wrote the paper. Pramod Kumar Jha: Conceived and suggested the analysis of tools.

References

1. Clark, D. R., Meffert, C., Baggili, I., & Breitinger, F. (2017). DROP (DRone open-source parser) your drone: Forensic analysis of the DJI phantom III. In *DFRWS 2017 USA—Proceedings 17th Annual DFRWS USA*, 3–14, https://doi.org/10.1016/j.diin.2017.06.013
2. Guo, Y., Slay, J., & Beckett, J. (2009). Validation and verification of computer forensic software tools-searching function. *Digital Investigation, 6*, 12–22. https://doi.org/10.1016/j.diin.2009.06.015
3. Hibshi, H., Vidas, T., & Cranor, L. (2011). Usability of forensics tools: A user study. In *Sixth international conference on IT security incident management and IT forensics*, IMF, 81–91, https://doi.org/10.1109/IMF.2011.19
4. Wu, T., Breitinger, F., & O'Shaughnessy, S. (2020). Digital forensic tools: Recent advances and enhancing the status quo. *Forensic Science International: Digital Investigation, 34*, 300999. https://doi.org/10.1016/j.fsidi.2020.300999

5. Wang, S. J. (2007). Measures of retaining digital evidence to prosecute computer-based cybercrimes. *Computer Standards Interfaces, 29*(2), 216–223. https://doi.org/10.1016/j.csi.2006.03.008
6. Marcella, J. R. & Menendez, D. (2010). *Cyber Forensics*
7. Abdulhamid, M., Profile, S. E. E, & Waziri, V. O. (2013). Cyber crimes analysis based-on open-source digital forensics tools some of the authors of this publication are also working on these related projects: Nature inspired meta-heuristic algorithms for deep learning: Recent progress and novel perspective vie, July 2016
8. Rahman, R. U., & Tomar, D. S. (2020). A new web forensic framework for bot crime investigation. *Forensic Science International: Digital Investigation, 33*, 300943. https://doi.org/10.1016/j.fsidi.2020.300943
9. Sammons, J. (2015). Chapter 3—labs and tools. *Basics of digital forensics* (2nd ed., pp. 31–46). https://doi.org/10.1016/B978-0-12-801635-0/00003-6.
10. TOOL English definition and meaning _ Lexico.
11. Mohan, (2016). Digital forensic investigation using sleuth kit autopsy. In *National conference on information, communication cyber security at department of computer science and engineering Kalasalingam university*, 0–43, [Online]. https://www.researchgate.net/publication/302580146_Digital_forensic_investigation_using_sleuth_kit_autopsy.
12. Memon, M. (2003). Advances in GUI testing-4 challenges. *Advances in Computers, 58*, 159–161.
13. Liu, S. (2021). A three-step hybrid specification approach to error prevention. *Journal of Systems and Software, 178*, 110975. https://doi.org/10.1016/j.jss.2021.110975
14. Xu, Y., Wu, Y., Gao, H., Song, S., Yin, Y., & Xiao, X. (2021). Collaborative APIs recommendation for artificial intelligence of things with information fusion. *Future Generation Computer Systems, 125*, 471–479. https://doi.org/10.1016/j.future.2021.07.004
15. Negr, M. (2021). SpeechToText : An open-source software for automatic detection and transcription of voice recordings in digital forensics. *Forensic Science International: Digital Investigation 38*. https://doi.org/10.1016/j.fsidi.2021.301223
16. Umar, R., Riadi, I., & Muthohirin, B. F. (2019). Live forensics of tools on android devices for email forensics. *Telkomnika (Telecommunication Computing Electronics Control), 17*(4), 1803–1809. https://doi.org/10.12928/TELKOMNIKA.v17i4.11748
17. Tantawy, A., Abdelwahed, S., Erradi, A., & Shaban, K. (2020). Model-based risk assessment for cyber physical systems security. *Computers and Security, 96*. https://doi.org/10.1016/j.cose.2020.101864
18. Bairwa, S., Mewara, B., & Gajrani, J. (2014). Vulnerability scanners: A proactive approach to assess web application security. *International Journal of Computers and Application., 4*(1), 113–124. https://doi.org/10.5121/ijcsa.2014.4111
19. Wiberg, K. C., (2006). *Identifying supervisory control and data acquisition (SCADA) systems on a network via remote reconnaissance.* Security, *147*, [Online]. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.149.4823&amp;rep=rep1&amp;type=pdf.
20. Dykstra, J., & Sherman, A. T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Proceedings Digital Forensic Research Conference DFRWS 2012 USA*, *9*, 90–98. https://doi.org/10.1016/j.diin.2012.05.001
21. Ghafarian, A., & Wood, C. (2019). Forensics data recovery of skype communication from physical memory, 857. Springer International Publishing
22. James, J. I., & Gladyshev, P. (2012). A survey of digital forensic investigator decision processes and measurement of decisions based on enhanced preview. *Digital Investigation, 10*(2), 148–157. https://doi.org/10.1016/j.diin.2013.04.005
23. Faiz, M. N., & Prabowo, W. A. (2018). Comparison of acquisition software for digital forensics purposes. *Kinetik Game Technology Information System, Computer Network, Computer Electronics and Control, 4*(1), 37–44. https://doi.org/10.22219/kinetik.v4i1.687
24. Song, J., Cho, C. H., & Won, Y. (2019). Analysis of operating system identification via fingerprinting and machine learning. *Computers & Electrical Engineering, 78*, 1–10. https://doi.org/10.1016/j.compeleceng.2019.06.012

25. "Limitations—5 *Dangers of free software*."
26. Horsman, G. (2019). Tool testing and reliability issues in the field of digital forensics. *Digital Investigation, 28*, 163–175. https://doi.org/10.1016/j.diin.2019.01.009
27. Horsman, G. (2019). Raiders of the lost artefacts: Championing the need for digital forensics research. *Forensic Science International Reports, 1*, 100003. https://doi.org/10.1016/j.fsir.2019.100003