International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 12– No. 47, April 2025 – www.ijais.org

Digital Forensic Tools for Cybercrime Investigation: A Comparative Analysis

P.S. Vinayagam, PhD
Assistant Professor
Department of Computer Science
Pondicherry University Community College
Puducherry

ABSTRACT
The rise of cybercrime incidents has brought the digital forensic tools into limelight. Used as a form of response, these tools are used to dissect and understand what happened and how it happened. This is also used as a measure to counter occurrence of such activities again in the future. Over the past few decades, the digital forensic tools have become highly sophisticated catering to the various needs of the investigation team. Earlier these tools were used only as a means of recovering deleted files from hard disk drives. As of now, the storage medias have taken various forms and the evidence pertaining to cybercrimes is not limited only to the hard disk drive of the systems. Though there is no all-in-one tool that can handle all the processes of forensic investigation, the selection of the right tool for the purpose at hand makes the investigation process easier and legally valid. This paper attempts to study the most popular digital forensic tools in use to find out their scope and limitations.

General Terms
Cybersecurity, Security, Tools, Cybercrime

Keywords
Digital Forensic Tools, Cybercrime Investigation

1. INTRODUCTION
Digital Forensics is defined as "The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations" [1]. The alarming rise in the cybercrime incidents have shifted the focus to use of digital forensic tools as a form of response and also as a lesson learner for avoidance of such incidents in the future.

The process of investigation starts right after an incident is reported or a crime is detected. An investigator starts collecting evidence from the objects identified to be included in the crime [2]. The process of digital forensics can be broken down into 6 steps as shown in Figure 1.

Identification is the process of identifying sources of evidence, such as computer devices, network logs, or cloud data. Preservation ensures that the evidence is preserved in its original state. This is done to prevent tampering or loss of data.

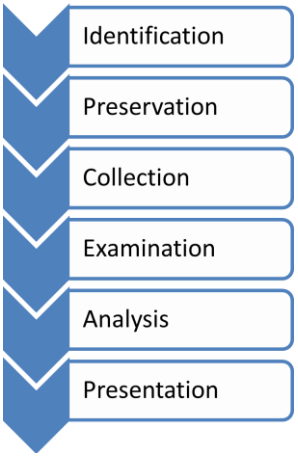

Fig 1: Digital Forensics Process

This step usually entails creating forensic copies of the data. After preservation, data is collected from the identified devices and systems. It needs to be ensured that the integrity of the data is maintained. In the next step, a detailed examination of the collected data is performed to identify and recover files, metadata and deleted data, if any.

Next, Forensic experts analyze collected data to identify evidence, reconstruct events and develop conclusions. All through the entire process, it is very essential to maintain detailed records of procedures, tools and actions taken to ensure transparency and legal admissibility. In the next step, a comprehensive report summarizing the findings, analysis and conclusions is generated. If needed, forensic experts may be required to testify in court, explaining their findings and the methodology used during the investigation [3] [4].

The digital forensics can be classified into the following specialized areas [5] [6]:

a) Operating System Forensics
b) Disk and File System Forensics
c) Live Memory Forensics
d) Web Forensics
e) Email Forensics
f) Network Forensics
g) Multimedia Forensics
h) Mobile Forensics
i) Database Forensics

Operating System Forensics is used to examine configuration files and output data of the Operating System to determine sequence of events. It allows users to identify suspicious files

and activity with hash matching, drive signature comparisons, emails, memory and binary data [5].

Disk and File System Forensics involves processing data to extract the contents of a file or recovering the contents of a deleted file. It includes listing the files, recovering deleted content and viewing sector contents [5].

Live Memory Forensics is used to recover information from live memory, such as running processes, passwords, encryption keys and malware traces. It helps to reveal hidden processes, malware trying to hide information and toolkits. Web Forensics is used to retrieve data from web storage record sessions, searches, history to trace a crime. Email forensics is a process of collecting evidence from emails. It involves email header analysis, email content recovery, attachments and logs of email server activity. Network forensic analysis involves traffic analysis, packet capturing, intrusion detection and examining logs from routers, firewalls and other network devices [5].

Multimedia Forensics focuses on image, audio and video forensics to identify tampering or manipulation, extraction of metadata from multimedia files. Digital image analysis is used to validate the history of an image by exploring, analyzing and retrieving information about the image. It also focuses on identifying the imaging device that captured the image and detecting traces of forgeries. Image analysis also includes examining images for evidence of stenography. Digital video is used to analyze videos from personal cameras, CCTV cameras and webcams. It examines the video for the identity of objects and the location where it was shot [5].

Mobile Forensics is used to secure data from the internal memory of a cell phone and related media as a form of evidence. Data include text messages, call logs, GPS data and app data. Database Forensics handle query logs, transaction logs, backup files and database schema analysis to find unauthorized changes or activities [6].

The field of Digital Forensic Investigation has come a long way from being a tool just only for recovery of data from hard disk drive to touching all the facets of the digital world. The role of digital forensic tools for investigation cannot be overstated. In this paper, we conduct a study about the most popular digital forensic tools in use to find out their scope and limitations.

The rest of this paper is organized as follows. Section 2 provides a review of the literature. The most popular Digital Forensic Tools are discussed in Section 3. The conclusion summarizes findings and suggests future research directions.

2. LITERATURE REVIEW

Authors in [7] have discussed various digital forensic tools, focusing specifically on software forensic tools used to detect forged digital images. Five software forensic tools, namely, FotoForensics, JPEGsnoop, Ghiro, Forensically and Izitru have been evaluated based on various features. The authors have observed that the selected tools provide no information regarding the basic concepts that have been used in the tools for detection of the forged images.

In [8], the authors provide a comparative analysis of Network Forensic Tools and Network Forensic Processes. Four tools, namely, Xplico, OmniPeek, NetDetector and NetIntercept, are evaluated with focus on capabilities to detect, collect and analyze network incidents. The authors conclude that Xplico performs better than others.

Authors in [9] compared two forensic suites and three stand alone non-forensic commercial applications. The authors opine that the individual functions available in the forensic suites are also available as commercial products, usually at a lower cost or free of cost.Since many of the forensic suites are closed source, only black box evaluation is possible. They found out that the commercial data recovery tools provide performance comparable to the forensic software suites.

The research work presented in [10] explore in depth the digital forensic issues focusing on the domain specific issues and possible helpful areas. The article also focuses on the role of the cognitive and human factors in a digital forensic investigation with an aim to strengthen the investigation process. The authors have compared four digital forensic tools. The authors emphasize the necessity of standardization and improved practices across the field.

In [11], the authors evaluate and contrast free forensic tools, Autopsy, FTK Imager, ProDiscover Basic, Wireshark etc., focusing on network examination, data analysis and password cracking. The criteria for evaluation includes platform support, file system support, imaging capabilities, data-driven features, reporting capabilities, hash type support, attack types, resource utilization and pattern matching capabilities. The study shows that the Autopsy, FTK Imager and ProDiscover Basic display unique strengths and limitations for data analysis. The authors conclude that John the Ripper and Hashcat perform better for password cracking due to robust hash type support. Wireshark is recommended for network analysis.

In the research work [12], the authors classify the literature pertaining to “cloud forensics” into three dimensions – survey-based, technology-based and forensics-procedural based. The authors have attempted to analyse the related work and generate a mind map to identify the research gaps. The digital forensic tools that can be used for evidence acquisition, examination and cloud forensics test purposes are summarized.The article recommends continuous research and development to address the evolving complexities of digital forensics.

The portable and small size of the smartphones, tablets and personal digital assistants prove to be a double-edged sword. On one end they are preferred by the users because of their portability and compactness but on the other end they are more prone to theft and easy to compromise. In [13], the authors focus on mobile forensics, which is a sub-domain of digital forensics. Mobile forensics focus on extracting and processing evidence from mobile devices to identify and trace the attacking entities. The authors review the literature pertaining to mobile forensics to identify the gaps and to address the challenges and issues in the field.

Over the years the attacks against the mobile phones and attacks with the aid of mobile phones have proliferated, as the devices have become sophisticated and rich in functionality. The data available from mobile phones in admissible as evidence in the court of law. Hence it becomes imperative to be able to acquire the data and present it in an admissible form. The authors in [14] focus on four forensic tools to extract data, specifically deleted data, from Android mobile phones. The authors conclude that AccessData FTK Imager

ad Encase show better performance than MOBILedit Forensic and Oxygen Forensic Suite in the case of acquiring deleted data. The study highlights the fact that there is no one single tool that works across all mobile device platforms and operating systems. They conclude that mobile forensics is still developing and more robust tools are necessary for broader applicability.

3. DIGITAL FORENSIC TOOLS

The list of digital forensic tools available in the market is long and dynamic. But some of the digital forensic tools have stood the test of time and have created a place for themselves due to their unique capabilities and performance characteristics. The focus of our study is on four digital forensic tools, namely, EnCase, FTK Imager, Volatility and Cellebrite UFED.

3.1 Encase

EnCase Forensic is widely trusted by law enforcement and corporate investigators for its robust features and reliability in digital investigations. EnCase Forensic is a digital forensics tool developed by OpenText (earlier Guidance Software). It assists investigators in acquiring, analyzing and reporting on digital evidence. It is widely used in law enforcement, government and corporate investigations. It can handle variety of forensic needs like data imaging, recovery, in-depth analysis and legal reporting. It operates on Windows and also supports cross-platform compatibility.

Encase can be used to create forensic disk images to preserve data integrity to ensure that the original remains unmodified. Encase can recover deleted files from unallocated space. It supports various file systems such as NTFS, FAT, Ext3/4, HFS+ and ZFS. Encase can also be used for data extraction from Android and iOS devices to analyze SMS, call logs and app data.

This tool has the capability to integrate with cloud platforms like Google Drive and Dropbox to acquire cloud-based evidence, supporting investigations in modern, cloud-centric environments. It offers powerful keyword searching and data filtering capabilities, allowing investigators to find relevant evidence quickly across large datasets.

It extracts detailed metadata from files, including creation dates, modification times, authorship, crucial for combining timelines and actions.The tool can parse email files from various clients (e.g., Outlook, Thunderbird), offering insight into communication patterns and key pieces of evidence. EnCase creates detailed timelines of system activity, providing a visual representation of events that can help identify the sequence of actions in an investigation.

EnCase provides tools to handle encrypted files, using password recovery techniques or bypassing encryption when necessary. The software generates comprehensive forensic reports with detailed findings, including graphs, charts and a summary of collected evidence, tailored for legal proceedings. It allows investigators to maintain a strict chain of custody, recording every action taken with the evidence, ensuring its integrity in court. EnCase uses hashing algorithms like MD5, SHA-1 and SHA-256 to verify the integrity of evidence and ensure that the data has not been tampered with.

EnCase integrates with other forensic tools and platforms, allowing investigators to extend its functionality for more specialized tasks. The software provides robust audit logs, automatically tracking every step of the forensic investigation to ensure proper chain of custody management. EnCase is designed to scale, from single-device investigations to handling large, multi-terabyte datasets in complex investigations. Encase supports EnScript for custom scripting and automation of forensic tasks. [15] [16] [17]. A sample user interface of Encase is shown in Figure 2.

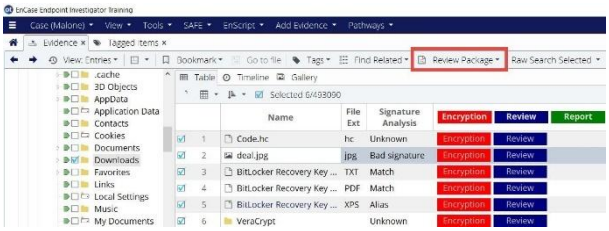

Fig 2: Encase User Interface [18]

3.2 FTK Imager

FTK Imager is a free digital forensics tool developed by AccessData (now maintained by Exterro) that enables investigators to acquire, preview and analyze forensic images from a wide range of digital devices. It is widely regarded as an essential tool in digital forensic investigations due to its ability to create forensically sound images while preserving data integrity.

FTK Imager supports multiple file systems and image formats, making it versatile for handling sensitive data acquisition and analysis tasks. Its user-friendly interface and robust features, such as file recovery, hash verification and memory capture, make it a trusted choice for law enforcement, corporate investigators and incident response teams. It operates on Windows platforms. It can create forensic disk images of hard drives, external storage devices, memory cards and network drives without compromising the integrity of the original data.

A wide range of image file formats including E01, AFF, RAW and Ex01 are supported. This tool uses write-blocking to prevent any changes to the source device. There is provision to preview the contents of storage devices. Different file systems such as FAT, NTFS, exFAT, HFS+, Ext3/Ext4 and ISO9660 are supported. Hash algorithms such as MD5, SHA-1 and SHA-256 are supported.

Both full disk imaging and logical imaging facilities are available. Facility to acquire memory dumps is provided for analyzing running processes, network connections and malwares. Individual files can also be extracted from disk images. To reduce the storage space requirements, compression options are available. Others features include basic searching with images, support for virtual drives and report generation [19] [20].Figure 3 depicts a sample user interface of the FTK Imager.

3.3 Volatility

Volatility is an open-source memory forensics framework used for analyzing volatile memory (RAM) dumps and performing memory analysis to detect and investigate various types of cyber incidents. It is primarily used in digital forensics and incident response to understand what happened on a system by analyzing its memory state at a particular point in time.

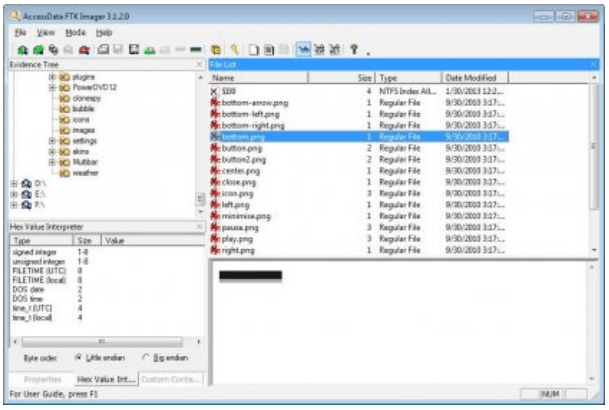

Fig 3: FTK Imager User Interface [21]

Volatility is one of the most powerful tools for memory forensics, supporting a wide range of operating systems and file formats. Volatility supports memory analysis for Windows, Linux, Mac OS X and Android systems, making it versatile for different environments.

The primary function of Volatility is to parse memory dumps (e.g., raw RAM images) to extract useful forensic data such as running processes, open network connections and loaded kernel modules. Volatility can analyze memory dumps in different formats, including raw memory dumps, Hibernation files (Windows hiberfil.sys) and Crash Dumps (Windows memory.dmp). Volatility provides the ability to list running processes, identify hidden or injected processes and extract detailed information about each process.

It allows analysts to inspect kernel modules and drivers loaded into memory, helping in the detection of rootkits or other types of kernel-level malware. Volatility can reveal open network connections, including IP addresses, ports and protocols in use, providing critical information for identifying malicious network activity. On Windows systems, Volatility can extract information from memory regarding registry keys, providing insights into system configuration and user activities.

The tool can recover deleted files or remnants of files that were present in memory at the time the image was taken, which is crucial in cases involving evidence deletion. Volatility can extract password hashes (e.g., Windows LM/NTLM) from the memory dump, useful in post-compromise investigations to check for credential theft.

Volatility is effective in detecting malware by identifying suspicious processes, memory injections, hidden threads and injected DLLs that often go unnoticed during traditional file-based forensics. The framework can help generate timelines of system activity, such as process start times, file creation and network activity, aiding in understanding the attack sequence.

It can analyze various memory artifacts, such as clipboard contents, passwords and encryption keys that are often stored in volatile memory. Volatility is widely used in malware investigations to analyze memory-based threats, including fileless malware that resides solely in memory and does not write to disk.

Volatility is non-intrusive, ensuring that it does not alter the memory image during analysis, maintaining the integrity of forensic evidence. Volatility is a command-line tool, offering flexibility and automation for forensic analysts, especially in large-scale investigations. As an open-source project,Volatility is continuously updated by its active community,allowing it to evolve and stay relevant to the latest memory forensics needs [21] [23] [24]. A sample user interface of Volatility is portrayed in Figure 4.

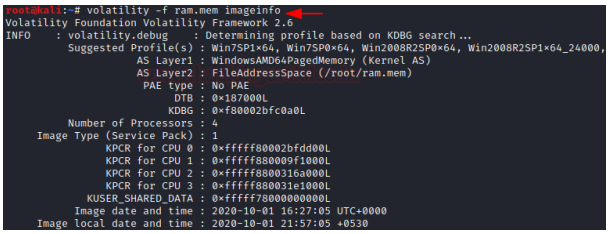

Fig 4: Volatility User Interface [25]

3.4 Cellebrite UFED

Cellebrite UFED (Universal Forensic Extraction Device) is a leading mobileforensicstoolusedbylawenforcement,intelligence agencies and forensic investigators to extract, analyze and report data from mobile devices. It is particularly known for its advanced capabilities in acquiring data from smartphones, tablets, GPS devices and other mobile electronics. UFED enables logical, file system and physical data extraction from mobile devices, even when the device is locked or encrypted.

It works with multiple mobile operating systems, including iOS, Android, Windows Phone and Blackberry. Cellebrite UFED offers advanced decryption capabilities, allowing forensic investigators to bypass device security, such as PINs, patterns and passwords, or extract data from encrypted devices when possible. It supports various extraction methods such as XRY, JTAG and chip-off for devices with non-standard configurations or that are damaged.

Cellebrite UFED can extract data from cloud accounts (Google, Apple iCloud, etc.), including call logs, contacts, photos and messages, providing a comprehensive view of a subject's activities. UFED can extract data from SIM cards and SD cards in mobile devices, allowing for a deeper level of analysis on communications and data stored outside the internal storage. UFED allows investigators to perform rooting (Android) or jailbreaking (iOS) when necessary to access restricted parts of the mobile device for advanced extraction. It supports extraction and analysis of app data from third-party applications like WhatsApp, Facebook, Instagram and Skype, often used in investigations for understanding social interactions and communications. The user interface of Cellebrite UFED is shown in Figure 5.

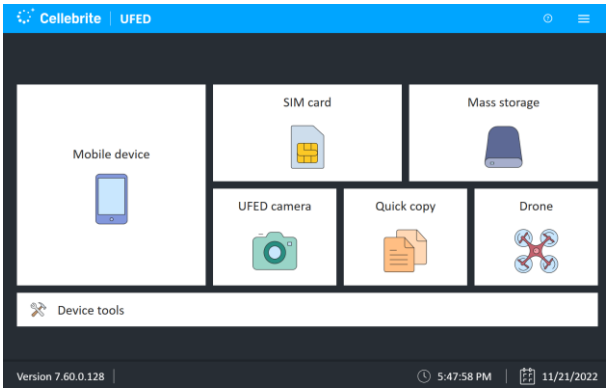

Fig 5: Cellebrite UFED User Interface [26]

UFED extracts call logs, SMS/MMS messages and instant messaging data, which are essential for understanding mobile communications. It can extract GPS and geolocation data from mobile devices, providing information on the user's locations, routes and places visited. UFED allows for the simultaneous extraction from multiple devices, improving efficiency during large-scale investigations.

Cellebrite ensures the integrity of extracted data using hashing and offers customizable reporting options that produce forensic reports for legal use, including screenshots, logs and evidence summary. UFED guarantees the secure handling of extracted data, using encryption and secure protocols to prevent data tampering during extraction and transport [27] [28] [29].

A detailed comparative analysis of EnCase, FTK Imager, Volatility and Cellebrite UFED is presented in Table 1.

4. CONCLUSION

Digital forensics tools have made significant advancements, starting from only hard disk analysis to reaching the point where everything from Operating System, Memory, Web, Email, Network, Multimedia Mobile and Databases are covered. It is observed that there is no single all-in-one tool that can handle all the steps pertaining to Cybercrime investigation and handle collection and analysis of data from all sources related to the incident or crime. Each artifact requires a specialized tool catering to its specific needs with reference to the crime under investigation.

Table 1. Comparative Analysis of Digital Forensic Tools

Feature	EnCase Forensic	FTK Imager	Volatility	Cellebrite UFED
Tool Type	Digital Forensics Suite	Forensic Imaging Tool	Memory Forensics Framework	Mobile Forensics Tool
Primary Use	Acquisition, analysis, reporting of digital evidence	Acquisition and analysis of forensic images	Memory dump analysis and incident response	Mobile device data extraction and analysis
Platforms Supported	Windows (cross-platform support)	Windows	Windows, Linux, Mac OS X, Android	Mobile devices (iOS, Android, Windows Phone, etc.)
Data Acquisition	Full disk imaging, cloud data, mobile device support	Forensic disk imaging and memory dumps	Analyzing volatile memory (RAM) dumps	Logical, file system, physical extraction from mobile
Data Recovery	Deleted file recovery, cross-platform support	Supports file recovery, hash verification and memory capture	Recover deleted files from memory	Data extraction from SIM cards, SD cards, cloud accounts
File Systems Supported	NTFS, FAT, Ext3/4, HFS+, ZFS	NTFS, FAT, Ext3/4, HFS+, exFAT, ISO9660	Not file system dependent (works with memory)	Extracts app data and other data types from mobile platforms
Cloud Integration	Google Drive, Dropbox	No direct cloud support	No direct cloud support	iCloud, Google Drive, other cloud services
Password/Encryption Handling	Can bypass or recover passwords, handle encryption	Supports hash verification, write-blocking	Extract password hashes from memory	Can bypass or recover device security (PIN, pattern)
Advanced Features	Detailed timelines, metadata extraction, legal reporting	Compression, logical and full disk imaging	Malware detection, kernel analysis, hidden process identification	Rooting (Android), Jailbreaking (iOS), App data extraction
Mobile Forensics Support	Android, iOS (via external modules)	No mobile support	No mobile support	Extensive mobile device support
Hashing Algorithms Supported	MD5, SHA-1, SHA-256	MD5, SHA-1, SHA-256	Not applicable for hashing but can recover hashes from RAM	Hashing for data integrity, includes extraction from devices
Forensic Reports	Customizable legal reports with graphs and charts	Flexible reporting, simple UI	No reporting; focused on analysis	Customizable forensic reports for legal use
Timeline Creation	Visual representation of system activity	No timeline feature	Generates activity timelines based on memory analysis	Limited timeline; focuses on mobile device activity
Integration with Other Tools	Integrates with other forensic tools and platforms	Integrates with other forensic software	Open-source; can be extended with community scripts	Integrates with other Cellebrite products
Use Case	Suitable for large-scale investigations	Ideal for smaller investigations, imaging, and previewing data	Best for incident response and memory-based investigations	Best for mobile device-focused investigations
Cost	Expensive (enterprise level)	Free (basic version)	Free (open-source)	Expensive (enterprise level)

There are several challenges in the field. One of the primary concerns is the encryption of data, which has made it increasingly difficult for investigators to access critical evidence. Another challenge is the interoperability of digital forensic tools. Furthermore, the volume of data generated by modern devices presents a significant hurdle. Integrating Artificial Intelligence and Machine Learning into digital forensic tools could help automate the analysis of large datasets, improving the efficiency and accuracy of the forensic process.

5. REFERENCES

[1] "A Road Map for Digital Forensic Research," First Digital Forensic Research Workshop (DFRWS), 2001. [Online]. Available: https://dfrws.org/wp-content/uploads/2019/06/2001_USA_a_road_map_for_digital_forensic_research.pdf.

[2] C. Altheide and H. Carvey, Digital Forensics with Open Source Tools, Syngress, 2011.

[3] Y. Yusoff, R. Ismail and Z. Hassan, "Common phases of computer forensics investigation models," International Journal of Computer Science & Information Technology (IJCSIT), vol. 3, no. 3, pp. 17–31, Jun. 2011, doi: 10.5121/ijcsit.2011.3302.

[4] EC-Council, "What is Digital Forensics in Cybersecurity Explained: 9 Powerful Facts You Need to Know Now!," EC-Council Cybersecurity Exchange, [Online]. Available: https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/what-is-digital-forensics/.

[5] A. R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat and T. R. Gadekallu, "A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges and future directions," IEEE Access, vol. 10, pp. 11065–11089, 2022, doi: 10.1109/ACCESS.2022.3142508.

[6] S. Singh and S. Kumar, "Qualitative assessment of digital forensic tools," Asian Journal of Electrical Sciences, vol. 9, no. 1, pp. 25–32, 2020.

[7] A. Parveen, Z. H. Khan and S. N. Ahmad, "Classification and evaluation of digital forensic tools," TELKOMNIKA Telecommunication, Computing, Electronics and Control, vol. 18, no. 6, pp. 3096–3106, Dec. 2020, doi: 10.12928/TELKOMNIKA.v18i6.15295.

[8] F. M. Ghabban, I. M. Alfadli, O. Ameerbakhsh, A. N. AbuAli, A. Al-Dhaqm and M. A. Al-Khasawneh, "Comparative Analysis of Network Forensic Tools and Network Forensics Processes," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Cameron Highlands, Malaysia, 2021, pp. 78-83, doi: 10.1109/ICSCEE50312.2021.9498226.

[9] J. Buchanan-Wollaston, T. Storer and W. B. Glisson, "A comparison of forensic toolkits and mass market data recovery applications," Ninth Annual IFIP WG 11.9 International Conference on Digital Forensics, 28- 30th January 2013. [Online] Available: https://core.ac.uk/download/9649321.pdf.

[10] H. Dubey, S. Bhatt and L. Negi, "Digital forensics techniques and trends: A review," The International Arab Journal of Information Technology, vol. 20, no. 4, Jul. 2023.

[11] A. Valluvar, S. Shetty, S. Pandian and S. Chaure, "Forensic tools in comparison: An assessment of performance across different parameters," International Journal of Innovative Science and Research Technology, Vol.8, No.9, pp.485-491, Sept. 2023.

[12] S. Almulla, Y. Iraqi and A. Jones, "A state-of-the-art review of cloud forensics," J. Digital Forensics, Security and Law, vol. 9, no. 4, Art. 2, 2014. DOI: https://doi.org/10.15394/jdfsl.2014.1190.

[13] K. Barmpatsalou, T. Cruz, E. Monteiro and P. Simoes, "Current and future trends in mobile device forensics: A survey," ACM Computing Surveys (CSUR), vol. 51, no. 3, pp. 1–31, May 2019, doi: 10.1145/3177847.

[14] O. Osho and S. O. Ohida, "Comparative Evaluation of Mobile Forensic Tools", International Journal of Information Technology and Computer Science (IJITCS), Vol.8, No.1, pp.74-83, 2016. DOI:10.5815/ijitcs.2016.01.09.

[15] OpenText, "EnCase Forensic," [Online]. Available: http://encase-docs.opentext.com/documentation/encase/forensic/8.07/Content/Resources/External%20Files/EnCase%20Forensic%20v8.07%20User%20Guide.pdf.

[16] M. Britz (2013). Computer Forensics and Cyber Crime: An Introduction, Third Edition, Pearson Education India.

[17] C. Altheide and H. Carvey, (2011). Digital Forensics with Open Source Tools, 1st Edition, Syngress.

[18] OpenText, "The EnCase Evidence Viewer," OpenText Blogs, Feb. 28, 2023. [Online]. Available: https://blogs.opentext.com/the-encase-evidence-viewer/.

[19] Exterro (2021). FTK Imager User Guide, [Online]. Available: https://www.exterro.com/uploads/documents/FTK_7.4.2_UG.pdf.

[20] L. Daniel and L. Daniel (2011). Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom. First Edition, Syngress.

[21] Software Informer, "AccessData FTK Imager 3.1," Software Informer, Mar. 26, 2025. [Online]. Available: https://accessdata-ftk-imager.software.informer.com/3.1/.

[22] Volatility Foundation, "Volatility Framework," [Online]. Available: https://volatilityfoundation.org/the-volatility-framework/.

[23] M. Ligh, A. Case, J. Levy, and A. Walters (2014). The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux and Mac Memory. Wiley.

[24] H. K. Mann and G. S. Chhabra, "Volatile Memory Forensics: A Legal Perspective," International Journal of Computer Applications, vol. 155, no. 3, pp. 11-15, Dec. 2016.

[25] J. Kothari, "Memory Forensics: Using Volatility Framework," Hacking Articles, Oct. 29, 2020. [Online]. Available: https://www.hackingarticles.in/memory-forensics-using-volatility-framework/.

[26] Cellebrite, "Cellebrite UFED | Access and Collect Mobile Device Data," Cellebrite, [Online]. Available: https://cellebrite.com/en/ufed/.

[27] Cellebrite, "UFED: Universal Forensic Extraction Device," [Online]. Available: https://www.cellebrite.com/.

[28] R. Ayers, S. Brothers, and W. Jansen(2014). "Guidelines on Mobile Device Forensics," NIST Special Publication 800-101 Revision 1. National Institute of Standards and Technology.

[29] E. Casey, (2011). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (3rd ed.). Academic Press.