© JAN 2026 | IRE Journals | Volume 9 Issue 7 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I7-1713887

A Comparative Study of Mobile Forensics Tools - Open Source vs Commercial Tools

AKSHAY PHALKE, SANIKA CHANDODE, KIRAN K JOSHI, MAYURI PAWAR
Department of CE and IT
Veermata Jijabai Technological Institute (VJTI), Mumbai, India

Abstract*— With the proliferation of mobile devices, forensic investigation of these devices has become imperative in today's digital landscape. This paper presents a comparative analysis of Android mobile forensics tools, aiming to address the challenges posed by the diversity of Android devices and operating system versions. Leveraging both open source and commercial tools, logical and physical acquisition methods were employed to retrieve data from Android devices. Android Debug Bridge (ADB) Tool , Magnet Acquire and Belkasoft Acquisition tools were used for acquisition. The study utilizes Commercial tools - Magnet Axiom, E3:Universal, MOBILedit forensics and Belkasoft Evidence Centre while Open Source Tools used are SIFT Work- station and the Sleuth Kit with Autopsy. The findings provide insights into the strengths and limitations of each tool category through a comparison matrix, offering guidance for selecting the most suitable toolset for forensic investigations. Additionally, this study aims to assess the extent to which open source tools match or surpass their commercial counterparts, raising pertinent questions regarding their viability as substitutes.Can free open-source tools do the same job as expensive proprietary ones? Is such a transition feasible for the forensic industry? These inquiries underscore the paper's broader implications for the evolution of forensic practices.

***Index Terms*—Mobile Forensics, Digital investigation, Forensic Tools, Open Source, Data Acquisition**

I. INTRODUCTION

Nowadays, there is a great spread of mobile smart devices because they have become necessary for carrying out most of our daily life activities. Mobile smart devices are becoming an integral part of our lives [1]. The rapid growth of Android mobile devices, made the mobile devices outstanding targets of malware attacks and many crimes have been committed using Android devices. Android devices thus become a vital source of evidence for forensic investigators [9] [11].

As mobile technology advances, security vulnerabilities escalate, with risks like Bluetooth and Mobile AdHoc attacks [2]. Categorized into Application and Frequency Based, attacks showcase remote control capabilities for data retrieval and eavesdropping [12]. Meanwhile, the neglect of security measures amidst rapid evolution leads to a surge in cyber threats [13]. The collective findings stress the necessity of security measures against rising threats in Android Devices. There is a need to emphasize on internet security's significance and providing prevention methods for developers against OWASP's top 10 web attacks [15].

Forensics entails systematically examining digital evidence according to legal standards, encompassing phases such as preparation, access to the crime scene, evidence collection, preservation, analysis, documentation, and presentation [3] [4]. Additionally, Android OS forensics, highlighted in a recent study, plays a crucial role in combating cybercrimes [14].

In mobile forensics, extracting and analyzing data from An- droid devices is vital for investigations [17]. Smartphones store extensive data, necessitating specialized tools for extraction [18]. The Android OS's popularity attracts cybercriminals, underscoring the need for thorough forensic analysis [17]. Tools like those using Android Recovery Mode address data integrity challenges [19]. More Research on Android architecture enhances forensic techniques, bolstering investigative capabilities [16].

Open source and commercial tools frequently vary in several aspects, including their quality, user-friendliness, availability, security features, customization options, and flexibility for software development. This study conducts a comparative analysis between various commercial mobile device forensic tools and open source alternatives. The objective is to determine whether open source mobile forensic tools possess the capability to effectively substitute commercial mobile forensics tools.
This paper is structured into 7 different sections, each

serving a distinct purpose. The initial section provides an overview of digital trends, outlines the paper's objectives, and emphasizes the importance of mobile forensics in light of increasing cyber threats from mobile devices. Following this, the subsequent section engages in an in-depth exploration of the domain through a comprehensive literature review, offering crucial background knowledge. Section 3 provides a compiled list encompassing both open-source and proprietary mobile device forensic tools utilized throughout this study. This comprehensive overview offers insights into the diverse range of tools employed. The following section outlines the essential phases of forensic investigation, accompanied by the key criteria formulated to evaluate the efficiency and suitability of the tool categories. Furthermore, Section 5 of the paper provides a detailed description of the study environment, which includes a variety of workstations and mobile devices utilized in the research. Additionally, a dedicated section addressing the challenges encountered during the examination process has been included, providing a thorough exploration of the obstacles faced throughout the study.

The principal achievement of this paper encompasses the development of a comparison matrix and the valuable insights extracted through its analysis.

II. LITERATURE REVIEW

Numerous research papers in the field of digital forensics have highlighted the significance and effectiveness of both proprietary and open source mobile device forensic tools in crime investigation

Sindhu, K.K. and Meshram, B.B. presented the paper "Digital Forensic Investigation Tools and Procedures" [4], which addresses the growing importance of data security in the IT industry, highlighting the role of digital forensics in investigating cyber attacks and the use of both commercial and open source tools to preserve and analyze digital evidence for legal proceedings.

In their one of the publications of authors S. C. Sathe and N.
M. Dongre [5] thoroughly examine the intricacies of mobile forensics. They discuss various challenges encountered and delve into the exploration of logical and physical acquisition methods. This exploration aids in determining the most suitable approach for extracting digital evidence from mobile devices.

In a recent study, researchers Masanam. Sai Prasanna Lakshmi and Pasupuleti Rajesh propose a forensic methodology that utilizes the Android Debug Bridge (ADB) tool for comprehensive analysis of Android devices. Their approach involves examining both temporary and permanent data, net- work activities, and application records, aiming to address the limitations of existing open-source forensic tools. They also consider various comparison criteria such as cost, MD5 Hashing mechanism, user-friendliness, and platform support [6].

The comparison criteria encompass cost, MD5 Hashing mechanism, user-friendliness, and platform support, among others. A study by Ritika Lohiya, Priya John, and Pooja Shah outlined the process steps of mobile forensic tools, covering acquisition, analysis, and preservation in "Survey on Mobile Forensics" [7].

One of the study titled investigated by Dhirendra Yadav, Manuj Mishra, and Sourabh Prakash investigates the swift evolution of mobile communication technology within India and the growing significance of mobile forensics within law enforcement circles. It delves into the hurdles encountered during investigations and the complexities surrounding the acceptance of mobile data as evidence in Indian judicial proceedings [8].

III. TOOLS INSIGHTS

Analyzing open-source and commercial tools entails a comprehensive approach. Initially, essential evaluation metrics like cost, functionality, security, and user-friendliness are established. Subsequently, pertinent data is gathered. Lastly, the tools are meticulously evaluated against these criteria, discerning the merits and drawbacks of each avenue (open- source versus commercial) to facilitate informed decision- making.

A. The Sleuth Kit (including Autopsy)

The Sleuth Kit, an open-source framework, concentrates on volume and file system analysis. It offers a foundation for application-layer modules to function independently of file access and intermittent

© JAN 2026 | IRE Journals | Volume 9 Issue 7 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I7-1713887

data duplication. Additionally, it can be utilized via a graphical user interface (GUI) with Autopsy.

B. Sans Investigative Forensic Toolkit (SIFT)

SANS Investigative Forensics Toolkit (SIFT) is a versatile forensic OS with a range of essential tools for digital forensics. Updated to version 3.0, it's integrated with Ubuntu and adapt- able to Windows via VMWare. Featuring GUI with MantaRay and command-line capabilities, SIFT is free and includes open- source forensic utilities.

C. MOBILEdit! Forensic

Mobiledit Forensic extracts data from phones and cloud storage, even deleted content. It offers physical and logical acquisition, application data analysis, and comprehensive re- porting. With wide device support, it bypasses security on locked phones and employs concurrent processing for faster investigations.

D. E3: Universal

Paraben E3 Universal is a versatile forensic software known for its wide compatibility with various devices and file systems. It provides comprehensive data extraction and analysis capabilities, including deleted data recovery.

E. Magnet AXIOM

Magnet AXIOM enables digital forensics experts to acquire data from diverse sources like mobile devices and cloud storage. With a user-friendly interface and cloud-based processing, Magnet AXIOM streamlines investigations. Paid plans offer advanced functionalities for enhanced forensic procedures.

F. Belkasoft X Forensic

Belkasoft X Forensic handles digital forensics across de- vices, offering data acquisition, deleted file analysis, and reporting. It serves law enforcement and corporations with features like mobile data recovery and email analysis. Flexible pricing caters to individual investigators and large organizations.

IV. THE INVESTIGATIVE PROCEEDINGS

A. Gathering Evidence

Attackers aiming to exploit vulnerabilities like as identified by OWASP's Top 10 Mobile Risks, might target emulators to gain access to sensitive data. In such cases, forensic investigators would need to analyze the emulator environment to identify traces of the attack and retrieve the stolen data. Techniques for evidence collection would differ depending on whether the attacker compromised a physical device or the emulator software itself. Physical devices require special tools to create a secure copy, while extracting data from compromised emulator software might involve advanced techniques to ensure the evidence isn't tampered.

Fig. 1. Investigative Processes

B. Identification Phase

The identification phase aims to empower investigators by matching forensic tools to their specific needs, considering both attack methods and available evidence sources. This evaluation considers both open-source and commercially available options. To guide selection, information on popularity and availability is gathered for each tool, including Open Source tools (Autopsy, Sans sift) and Commercial tools (Magnet, MOBILedit, Paraben E3, Belkasoft). Furthermore, key metrics are defined to assess functionalities critical for mobile foren- sics, such as keyword searching, report generation, deleted file recovery, and capabilities relevant to identifying attacks like related to M2: Inadequate Supply Chain Security or M3: Insecure Authentication/Authorization (as per OWASP's Top 10 Mobile Risks). By considering these factors, investigators can make informed decisions about which tools will best serve their forensic needs, particularly when dealing with mobile devices potentially compromised through these attack vectors.

© JAN 2026 | IRE Journals | Volume 9 Issue 7 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I7-1713887

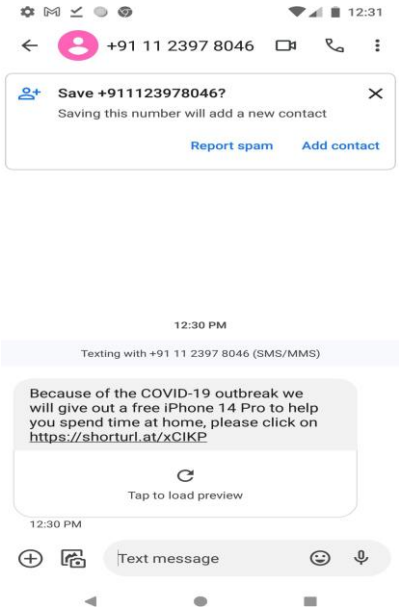

Fig. 2. Attacker Exploits M3: Insecure Authentication/Authorization*

*For educational purposes only.

C. *Preparation Phase*

The preparation phase focuses on ensuring compatibility between evidence and chosen forensic tools. This involves identifying the tool's supported input formats and potentially pre-processing the evidence (e.g., converting files) to match those formats. If the tool lacks format flexibility, a direct connection to the mobile device might be necessary for compatibility checks. In essence, this phase optimizes the evidence for successful analysis by the selected forensic tool.

D. *Acquisition Phase*

The acquisition phase prioritizes isolating the evidence to prevent data alteration. This involves disconnecting the device from networks (Wi-Fi, infrared, Bluetooth) and potentially enabling airplane mode to ensure no new data enters the device [9]. However, for logical and physical extractions on Android devices, rooting the phone is necessary. Rooting grants deeper access, allowing logical extraction of specific files (adb pull) or physical extraction of a complete disk image (.dd format). It's crucial to weigh the benefits of rooting against potential data volatility concerns.

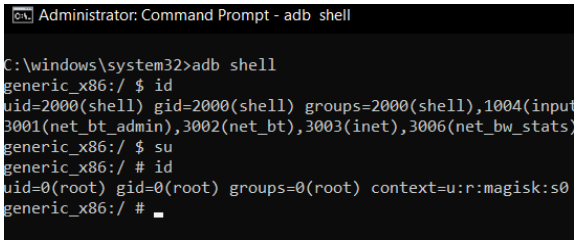

Fig. 3. Rooting the Device

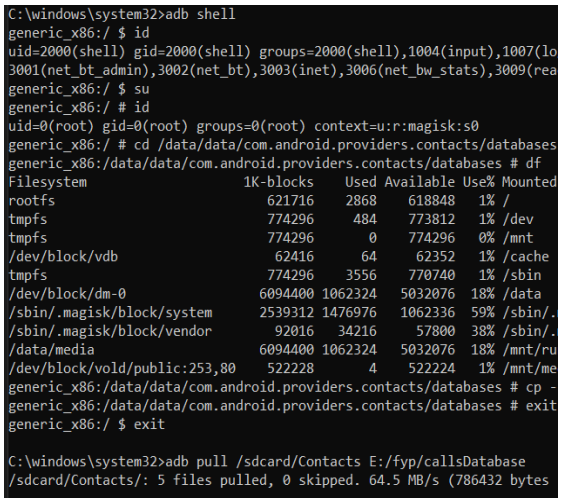

Fig. 4. Acquisition Of Data

E. *Preservation Phase*

The preservation phase safeguards the integrity of the ac- quired evidence. This is paramount to ensure no alterations, damage, or loss occurs during storage or analysis. This might involve creating write-protected copies, maintaining a documented chain of custody, and employing secure storage solutions. By prioritizing preservation, the digital evidence retains its admissibility in court.

F. *Analysis Phase*

The analysis phase leverages the prepared evidence. Data is fed into the chosen forensic tools according to their specific format requirements. Each tool then analyzes the data based on its functionalities. This analysis allows for evaluation against the pre-defined metrics, such as filtering and sorting capa- bilities, deleted data recovery effectiveness, report generation features, geolocation analysis, etc, if the tool offers it. Through this analysis, investigators can assess the tools' performance and determine which ones yielded the most valuable results based on the case requirements.

G. *Integrity Validation Phase*

Following the Analysis phase, an Integrity Validation Phase is crucial. This step verifies that the data analyzed by the forensic tools hasn't been altered

© JAN 2026 | IRE Journals | Volume 9 Issue 7 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I7-1713887

during the process. This is achieved by comparing a hash value, a unique digital fingerprint, of the original acquired evidence with a hash generated from the data analyzed by the tools.

H. Result and Documentation Phase

The Results and Documentation phase focuses on consolidating the findings, with a particular emphasis on attack identification capabilities. Here, the tools are evaluated based on the pre-defined metrics, creating a comparison table that highlights each tool's strengths and weaknesses, especially regarding functionalities relevant to attacks as identified by OWASP's Top 10 Mobile Risks). Additionally, screenshots, video recordings demonstrating tool usage in the context of attack identification, and documented evidence showcasing successful application of the metrics (e.g., analysis of artifacts indicating a compromised app store download) are compiled. This comprehensive documentation serves as a clear and verifiable record of the forensic tool analysis, aiding in informed decision-making about future tool selection, particularly when dealing with mobile devices potentially compromised through these attack vectors.

V. STUDY ENVIRONMENT

A. Coverage and Operation System Version of Device

Device used is the Oppo A33f smartphone running on Android version 5.1.1 with ColorOS version 2.1

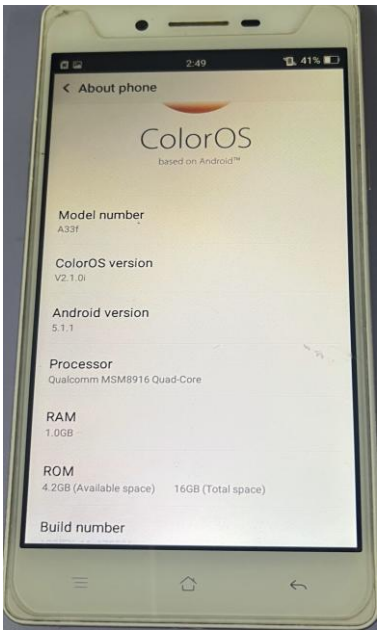

Fig. 5. OPPO A33F

B. Supported Platforms for Tools

Tools	Supported Platforms
Autopsy	Windows, Linux, MacOS
Sansift	Windows, Linux, MacOS, VM
Magnet	Windows, Linux, Cloud
Belkasoft	Windows, Linux, MacOS, VM, Cloud
MOBILedit	Windows, Linux, MacOS, Cloud
Paraben E3	Windows, Linux, MacOS

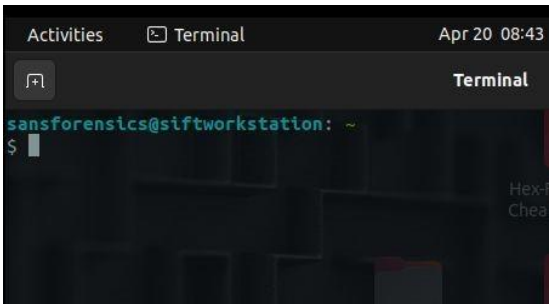

Fig. 6. SIFT Linux Workstation

C. Limitations and Considerations

- Hardware Considerations: Ensure your laptop has at least 20GB of free space for evidence and tool files, along with a high-speed processor for efficient analysis, especially with large datasets.
- Data Size and Processing Time: Expect varying acquisition and analysis times based on data size. Large files may require a minimum of 1 hour for processing. For very large datasets, physical extraction (full disk copy) might be necessary, which can significantly extend the acquisition time compared to logical extraction.
- Data Compression: Compressing acquired data can be a strategy to manage storage limitations, but consider potential compatibility issues with forensic tools.
- Rooting Considerations: Rooting an Android device can grant advanced access for data acquisition, but the ease of rooting varies. Older Android versions are generally easier to root compared to newer ones

D. Mobile Device Connection Methods

- Wired Connections: Most forensic tools (Autopsy, Belkasoft Evidence Center, Magnet Forensics, Paraben E3) require a physical connection using a micro USB cable to establish a secure link with the mobile device for data acquisition.
- Wireless Connections: Some tools, like

© JAN 2026 | IRE Journals | Volume 9 Issue 7 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I7-1713887

MOBILedit Forensic, offer the flexibility of connecting via Bluetooth or Wi-Fi for data acquisition, although wired connections are generally considered more reliable for forensic purposes.

VI. ISSUES CONFRONTED

- Emulator Image Challenges: Emulator RAMdisk images weren't visible in the command prompt. This hurdle was overcome by modifying the ANDROIDHOME environment variable to point to the Android SDK directory.
- Unpredictable File Size: Acquired files may not have a predefined size, potentially leading to storage exhaustion during acquisition. Careful monitoring and space management are crucial.
- Wired Connection Stability: Stable wired connections are essential. Interruptions during data acquisition via micro USB cable necessitate restarts, impacting efficiency.
- Open-Source Tool Limitations: Limited virtual disk space in virtual workstations used by open-source tools (e.g., Sans SIFT) can interrupt analysis of large datasets, ex- tending processing time significantly.
- Commercial Tool Support Delays: Delayed trial access from some commercial tool vendors hampered evaluation efforts
- Limited User Guidance: Certain tools lacked comprehensive user manuals or tutorials, hindering intuitive use.
- Trial Version Feature Limitations: Restricted functionalities in trial versions (e.g., case management in Mobile Edit) limited the scope of evaluation.

VII. COMPARISON MATRIX

TABLE I COMPARISON MATRIX

Metric	Open Source tools		Commercial tools			
	TSK with Autopsy	SIFT	MOBILedit Forensics	E3 Universal	Magnet Axiom	Belkasoft X
Ease of Use	Moderate	Difficult	Easy	Easy	Easy	Easy
Database Analysis	Limited	No	Yes	Yes	Yes	Yes
Can tool detect Attack?	Yes	Yes	Yes	Yes	Yes	Yes
Open Source	Yes	Yes	No	No	No	No
Acquisition of Disk Images	Yes	Yes	Yes	Yes	Yes	Yes
Cloud storage Analysis?	No	No	Yes	Yes	Yes	Yes
Hashing Mecha-nisms	MD5 , SHA-1	MD5	MD5, SHA-1, SHA-256	MD5, SHA-1, SHA-256	MD5, SHA-1, SHA-256	MD5, SHA-1, SHA-256
Customised Report	No	No	Yes	Yes	Yes	Yes
License required?	No	No	Yes	Yes	Yes	Yes
Multi- user capabili-ties	Yes	Yes	Yes	No	No	Yes
GUI Available	Yes	Yes	Yes	Yes	Yes	Yes
External Plugins	Supported	Not Supported	Supported	Not Supported	Supported	Supported
Physical Extraction	No	Yes	Yes	Yes	Yes	Yes

	Open Source tools	Commercial tools

© JAN 2026 | IRE Journals | Volume 9 Issue 7 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I7-1713887

Metric	TSK with Autopsy	SIFT	MOBILedit Forensics	E3 Universal	Magnet Axiom	Belkasoft X
Keyword Searching	Yes	Yes	Yes	Yes	Yes	Yes
Timeline Analysis	Yes	Yes	Yes	Yes	Yes	Yes
CLI Available	Yes	Yes	No	No	No	No
Communication Analysis	Yes	Yes	Yes	Yes	Yes	Yes
Images/Video Analysis	Yes	Yes	Yes	Yes	Yes	Yes
Types of Reports	Various (HTML Excel Text Summary Portable-Case Unique-Words)	Various	HTML report, PDF report, MS Excel report	Various (HTML, CSV, PDF (Investiga - tive and Mobile Evidence Report))	Various (CSV, EXCEL, HTML, KML, LOAD FILE, PORTABLE CASE, XML)	Various
Browser History Analysis	Yes	Yes	Yes	Yes	Yes	Yes
Is evidence acceptable in judiciary?	Yes	Yes	Yes	Yes	Yes	Yes
Is internet required?	No	No	No	No	Depends	No
Report Generation	Yes	Yes	Yes	Yes	Yes	Yes
Community Support	Yes	No	Yes	Yes	No	No
Supported File Types	Various (.mp4 .mp3 .zip .rar .dd .db .sqlite .html .doc .exe .cmd)	.dd, .raw, E01	Various (.xml, .mo-bileedit, .ab, .zip, .001, .aa, .bin, .dd, .img, .raw, .xml)	.e3, .p2c, .nmx	Various (E01, .aff4, .ufd, .AD1, .raw, .dd, .img, .ima, .vfd, .flp, bif, .docx, .pptx, .rar)	E01, DD, AFF, ZIP, TAR, .mp4 .mp3, .html, .db, .exe, .doc, .cmd, .raw
Geo-location Analysis	Yes	No	Yes	Yes	Yes	Yes
File Encryption Detection	Yes	Yes	Yes	Yes	Yes	Yes
Supported Platforms	Windows, Linux, MacOS	Windows, Linux, MacOS, VM	Windows, MacOS	Windows, Linux, MacOS	Windows, Linux	Windows, Linux, MacOS, VM, Cloud
Price	Free	Free	$5K	$6,295	$6K[a]	$2K[a]
Data Visualization	No	No	Yes	Yes	Yes	Yes
Recovery of Email Files	Yes	Yes	Yes	Yes	Yes	Yes
Scanning Speed[b]	Moderate	Less	Fast	Fast	Moderate	Fast
Customer Support	Communit y- driven	Yes	Yes	Yes	Yes	Yes
File Sorting and Filtering Options	Yes	Yes	Yes	Yes	Yes	Yes

Case Management Capabilities	Yes	Yes	Yes	Yes	Yes	Yes
SQLite Viewer	No	Yes	Yes	Yes	Yes	Yes
Recovery of Deleted Files	Yes	Partially Yes[c]	Yes	Yes	Yes	Yes
File Carving Capability	Yes	Yes	Yes	Yes	Yes	Yes
Advanced Image/Video Modules	Yes	No	Yes	Yes	Yes	No
Can case file be shared?	Yes	Yes	Yes	Yes	Yes	Yes
Used by Authoritative Agencies?	Yes	Yes	Yes	Yes	No	Yes
Sorting Capability	No	Yes	Yes	Yes	Yes	Yes
Trace Window[d]	Yes	No	Yes	No	No	Yes
Case Merging Capabilities	No	No	No	No	Yes	No
Can a tool root device?	No	No	Yes	Yes	No	No

[a]Pricing hinges on subscription duration, user volume, and the spectrum of features.

[b]Moderate = 1GB/1Hr, Fast=2-20GB/1HR

[c]It detects deleted files, but recovery depends on the examiner's expertise.

[d]It provides real-time updates on data processing activity.

VIII. FUTURE SCOPE

With the increasing use of smartphones and the evolving nature of forensic techniques, there is a growing demand for additional research in forensic evaluation. In future works, the authors propose a more thorough examination of forensic methods and tools to provide comprehensive reference on this matter. As cybercrime keeps rising, we might encounter even more advanced and intelligent bots in the future. The metrics that focus on these threats and concern them may thus be developed to see if the tools can handle these risks .Suggestions for refining evaluation parameters and exploring additional variations of forensic tools can be explored in subsequent research efforts.

Authors also tend to explore alternative types of tools, analyzing their respective strengths and weaknesses. Addition- ally, efforts will be made to develop new forensic guidelines tailored to specific tools and their application in addressing particular issues.

IX. ACKNOWLEDGMENT

This study was conducted as the authors' final year en- gineering project at Veermata Jijabai Technological Institute. The authors express their gratitude to their Project Mentor, Prof. K. K. Joshi, for his invaluable advice, encouragement, and guidance throughout the project.

In addition, we extend our heartfelt gratitude to the Belka- soft Forensics Team, Paraben Corporation, Magnet Foren- sics, and MOBILedit Team for graciously providing us with access to complimentary trials of their respective cutting-edge commercial mobile device forensic tools: Belkasoft X, E3:Universal, Magnet Axiom, and MOBILedit Forensic PRO Cloud DEMO, spanning durations of 30 days, 7 days, 14 days, and 30 days, respectively.

REFERENCES

[1] Alatawi, H., Alenazi, K., Alshehri, S., Alshamakhi, S., Mustafa, M., Aljaedi, A. (2020). Mobile Forensics: A Review. 2020 International Conference on Computing and Information Technology (ICCIT-1441). doi:10.1109/iccit-144147971.2020.9213739

[2] P. Ruggiero, J. Foote, Carnegie Mellon University, and US-CERT, "Cyber threats to mobile phones," 2011. [Online].

[3] Sridhar N, Bhaskari D L, and Avadhani P. Plethora of Cyber Forensics. International Journal of Advanced Computer Science and Applications, 2011, 2(11),110 – 114.

[4] Sindhu K K, and Meshram B B. Digital Forensic

Investigation Tools and Procedures. International Journal of Computer Network and Information Security, 2012, 4, 39-48, doi: 10.5815/ijcnis.2012.04.05.

[5] S. C. Sathe and N. M. Dongre, ”Data acquisition techniques in mobile forensics,” 2018 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 2018, pp. 280-286, doi: 10.1109/ICISC.2018.8399079.

[6] M. S. P. Lakshmi and P. Rajesh, ”A Forensic Approach to perform Android Device Analysis,” in Proceedings of the 7th Volume, 6S Issue of Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP), March 2019, pp. 5-11.

[7] R. Lohiya, P. John and P. Shah, “Survey on Mobile Forensics,” Interna- tional Journal ofComputer Applications, vol. 118, p. 0975 – 8887,2015.

[8] D. Yadav, M. Mishra and S. Prakash, ”Mobile Forensics Challenges and Admissibility of Electronic Evidences in India,” 2013 5th International Conference and Computational Intelligence and Communication Net- works, Mathura, India, 2013, pp. 237-242, doi: 10.1109/CICN.2013.57.

[9] A. Al-Dhaqm, S. A. Razak, R. A. Ikuesan, V. R. Kebande and K. Siddique, ”A Review of Mobile Forensic Investigation Process Models,” in IEEE Access, vol. 8, pp. 173359-173375, 2020.

[10] Al-Sabaawi, A., Foo, E. (2019). ”A Comparison Study of Android Mobile Forensics for Retrieving Files System.” , 13, 148-166.

[11] M. Hassan and L. Pantaleon, ”An investigation into the impact of rooting android device on user data integrity,” 2017 Seventh International Conference on Emerging Security Technologies (EST), Canterbury, UK, 2017.

[12] S. Sudin, A. Tretiakov, R. H. R. M. Ali and M. E. Rusli, ”Attacks on mobile networks: An overview of new security challenge,” 2008 International Conference on Electronic Design, Penang, Malaysia, 2008, pp. 1-6, doi: 10.1109/ICED.2008.4786772.

[13] N. Varol, A. F. Aydogan and A. Varol, ”Cyber attacks targeting Android cellphones,” 2017 5th International Symposium on Digital Forensic and Security (ISDFS), Tirgu Mures, Romania, 2017, pp. 1-5, doi: 10.1109/ISDFS.2017.7916511.

[14] Raju, S., Koundinya, A. K. and Bharathi, R. (2020). Gathering Evi- dence from Android OS for Mobile Forensics. International Journal of Computer Science and Network (IJCSN), 9(4), 1-10. (ISSN: 2277-5420)

[15] Patole, P., Totade, A., Patil, P. and Nagpure, R. (2022). OWASP Top 10 Web Attacks (2017) with Prevention Methods. International Research Journal of Engineering and Technology (IRJET), 9(4), 686. (e-ISSN: 2395-0056)

[16] F. Dian and J. Hudec, ”Efficient Sensitive Data Gathering with Forensic Analysis of Android Operating System,” 2019 17th International Con- ference on Emerging eLearning Technologies and Applications(ICETA)

[17] V. V. Rao and A. S. N. Chakravarthy, ”Forensic analysis of android mobile devices,” 2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE), Jaipur, India, 2016, pp. 1-6, doi: 10.1109/ICRAIE.2016.7939540.

[18] P. Dibb and M. Hammoudeh, ”Forensic Data Recovery from Android OS Devices: An Open Source Toolkit,” 2013 European Intelligence and Security Informatics Conference, Uppsala, Sweden, 2013, pp. 226-226, doi: 10.1109/EISIC.2013.58.

[19] Son, N., Lee, Y., Kim, D., James, J. I., Lee, S. and Lee, K. (2013). A study of user data integrity during acquisition of Android devices. Digital Investigation, 10(Supplement), S3-S11. https://doi.org/10.1016/j.diin.2013.06.001.