AI & CYBER FORUM
AN INTERNATIONAL JOURNAL
OPEN ACCESS
ISSN 3117-6399
Article Review
Check for updates

# RAM Acquisition in Mobile Digital Forensics: A Systematic Literature Review of Tools, Techniques, Challenges, and Future Directions

**Karan Bhuva**[1], **and Varsha Rathore***[2]

[1]*Student, School of Internal Security & SMART Policing, Rashtriya Raksha University, Gandhinagar, India*
[2]*Teaching Cum Research Officer, School of Internal Security & SMART Policing, Rashtriya Raksha University, Gandhinagar, India*

Corresponding author: **Varsha Rathore** | E-mail: **varsha.rathore@rru.ac.in**

**Citation:** Karan Bhuva, and Varsha Rathore (2026). RAM Acquisition in Mobile Digital Forensics: A Systematic Literature Review of Tools, Techniques, Challenges, and Future Directions. *AI & Cyber Forum: An International Journal.* **DOI: https://doi.org/10.51470/AI.2026.5.1.56**

Received 10 February 2026 | Revised 06 March 2026 | Accepted 08 April 2026 | Available Online May 07, 2026

## Abstract

*RAM acquisition is extremely significant in digital forensics in the current scenario owing to the widespread use of mobile and multiplatform devices. RAM holds various transitory evidence such as encryption keys, active processes, current logins, active connections, and temporary application data that can't be recovered using persistent storage. Therefore, the selection of an appropriate RAM acquisition tool becomes a crucial element while evaluating the effectiveness of the forensics analysis process. This research paper will make comparisons between some popular RAM acquisition software like LiME, AVML, Belkasoft RAM Capturer, and DumpIt. The comparison was carried out by means of qualitative synthesis of evidence according to the evaluation criteria that included acquisition time, platform compatibility, stability, usability, performance, and forensic integrity. In the present scenario, LiME demonstrated excellent platform compatibility in relation to Android, and DumpIt showed good compatibility with the Windows environment. AVML showed excellent cross-platform compatibility, and Belkasoft RAM Capturer showed good deployment and usability. Nevertheless, there were disparities in relation to compatibility, stability during acquisition, and forensic integrity. This study shows the significance of choosing a suitable RAM acquisition tool depending on the investigation.*

***Keywords:*** *RAM acquisition1; mobile forensics2; digital forensics3; volatile memory4; LiME5; memory analysis6; Android forensics7; forensic tool evaluation8.*

## 1. Introduction

The widespread adoption of smartphones across the globe has brought about significant changes in the world of digital forensics. As the number of smartphone users around the world is now more than five billion, mobile devices have become the main source of digital artifacts in a variety of crime investigations, civil litigation, and national security matters [1]. Therefore, mobile device forensics has become an important field of digital forensics, which requires specific techniques due to the unique nature of today's mobile devices.

In the mobile device, the volatile memory, also known as the Random Access Memory (RAM), holds great forensic importance. While non-volatile memory like flash memory stores data for long periods, volatile memory stores data while the device is on. The data in RAM consists of live data objects such as live states of processes, encryption keys, log-in details, network connections, and decrypted messages that form highly valuable evidence but are highly transient [2, 3]. As soon as the device is powered down or rebooted, everything gets deleted from RAM.

The issue with digital forensics experts is not the availability of RAM tools but the absence of standards by which they can assess and compare current tools. These tools are varied in their technological structure, OS specifications, accuracy of the forensic process, and ease of use. If there are errors in using these tools, there could be incomplete and perhaps contaminated memory acquisition, which may even render it inadmissible in court [4].

This research paper attempts to fill the gap through an evaluation of the six RAM acquisition software tools used in mobile forensics. The six RAM acquisition software that would be evaluated for this purpose include LiME (Linux Memory Extractor), AVML (Azure Virtual Machine Memory Dumper), Belkasoft RAM Capturer, DumpIt, Volatility with Acquisition Plugins, and Magnet RAM Capture. The above-mentioned six RAM acquisition software would be evaluated on the basis of five important criteria, including accuracy, reliability, usability, compatibility, and performance.

### 1.1 Research Objectives

*The study aims to achieve the following objectives:*

1. Determination and characterization of RAM acquisition tools currently being used in mobile digital forensics investigations.
2. Systematic comparison of these tools using a standardized five criterion evaluation process.
3. Determination of the strengths, weaknesses, and ideal usage scenarios of these tools to inform evidence-based decision making.

### 1.2 Research Questions

The research will be based on three major questions, which are:

1. What are the existing RAM acquisition tools for mobile digital forensics and what are their main technical features?
2. How do the six selected tools compare in terms of accuracy, reliability, user-friendliness, platform support, and acquisition efficiency?
3. Which tool(s) is/are suitable for particular mobile forensic investigations?

## 2. Materials and Methods

### 2.1 Research Design

The study adopts a qualitative systematic literature review (SLR) methodology based on secondary evidence synthesis, which is in line with previous research done in this area [10, 13]. In view of the fact that conducting live memory acquisition experiments on all the tools and devices that have been considered in the current study would be unfeasible, the evaluation results will be obtained by synthesizing information from peer-reviewed journals, technical documentation, forensic expert standards, and investigative cases. This technique has been used in secondary research in digital forensics before, due to the extensive characterization of the tool behavior already done.

### 2.2 Tool Selection Criteria

The following six tools were chosen for evaluation according to the following criteria:

- Usefulness in digital forensics investigations as demonstrated through the peer-reviewed literature.
- Availability as either open source software or as free commercial software.
- Usability in mobile forensics, either native or through integration with mobile forensics processes.
- Technical information sufficient to allow scoring against five criteria.

### 2.3 Evaluation Criteria and Scoring

Each technique was rated based on five parameters using a scale of 1 (least) to 10 (most), as indicated in Table 1. The ratings are a synthesis of the results from converging researches that have been considered as per expert-synthesis methodology.

*Table 1: Evaluation Scoring Scale*

| Sr. no | Score Range | Level | Description |
|---|---|---|---|
| 1 | 9–10 | Excellent | Highly effective; meets all forensic standards with mini-mal limitations. |
| 2 | 7–8 | Good | Performs well with only minor gaps in coverage or usabil- |
| | | | ity. |
| 3 | 5–6 | Moderate | Functional but with notable limitations that restrict use in |
| | | | certain scenarios. |
| 4 | 3–4 | Below Average | Significant limitations that means requires other tools or |
| | | | advanced expertise. |
| 5 | 1–2 | Poor | Largely ineffective for the stated forensic purpose. |

*The five criteria of evaluation are as follows:*

- Accuracy - Integrity of the memory capture; how well the tool captures an unmodified forensic image of the memory of the device.
- Reliability – Consistency and reliability of the results produced when using the tool in different situations, for different device models, and for different versions of the operating system.
- Ease of Use – The amount of knowledge needed to properly use the tool; its usability by both experts and novices.
- Compatibility – The range of different operating systems and mobile devices for which the tool works; e.g., Android, iOS, and Windows.
- Performance – How fast and efficient the acquisition process is.

#### 2.3.1 Score Assignment Methodology

The numerical value that each RAM acquisition tool is rated on is arrived at using qualitative evidence synthesis methods instead of experimental assessment. This is because the information regarding the performance of each tool comes from research papers, conference proceedings, technical manuals, and the vendor websites. There is a systematic analysis of the literature based on five predetermined criteria of accuracy, reliability, user-friendliness, compatibility, and performance. The score for each tool represents the overall judgment made from the information gathered.

In order to maintain consistency in the ratings, the criteria were individually scored based on the previously established scoring scheme shown in Table 1 below. In contrast to the findings based on an analysis of a single publication, the score assigned to each criterion reflects the consensus obtained from the body of literature examined. In cases where different sources provide inconsistent data on a specific tool, more importance was attributed to findings from peer-reviewed articles, forensic examinations, and technical documentation. Thus, the scores stated above can only be viewed as evidence-based comparative metrics aimed at evaluating the RAM acquisition tools considered.

In the case where the current study is a systematic review of the existing literature instead of empirical benchmarking, the scoring system is meant to be a standardized comparison system that enables both researchers and practitioners to identify RAM acquisition software that is appropriate for various forensic cases. The new approach makes the process more transparent since it clearly indicates the criteria and the evidence synthesis process used to come up with the scores.

*Table 1A: Evaluation Criteria Used for Score Assignment*

| Criterion | Evaluation Indicators |
|---|---|
| Accuracy | Memory acquisition completeness, forensic integrity, preservation of volatile evidence, kernel-level acquisition capability |
| Reliability | Stability across multiple acquisitions, consistency of results, successful deployment reported in the literature |
| Ease of Use | Installation complexity, command-line requirements, graphical interface availability, documentation quality |
| Compatibility | Support for Android, iOS, Linux, Windows, device architectures, and deployment environments |
| Performance | Acquisition speed, system overhead, resource utilization, operational efficiency |

### *2.4 Limitations*

*The following are limitations in this study and must be taken into consideration when analyzing results from the work:*

- No direct acquisitions were performed using these tools; analysis is performed using a review of secondary research only.
- There is no fully licensed version of all evaluated tools accessible to the researchers for evaluation of commercial tools; analysis is done through published information and peer reviews.
- The mobile operating systems are highly dynamic and changing rapidly, which makes some of the results concerning compatibility and performance subject to change after publication due to upgrades of the tools.
- The acquisition of iOS RAM has inherent architectural limitations, such as the use of Secure Enclave hardware isolation, which is difficult to circumvent with current tools.

## 3. Results

This section presents the criterion-wise evaluation of each tool followed by a consolidated comparative matrix.

### 3.1 Tool Profiles and Criterion-wise Assessment

#### 3.1.1 LiME — Linux Memory Extractor

**Type: Open Source Platform: Android / Linux**

LiME refers to a Loadable Kernel Module designed for Linux kernel which helps in dumping entire physical memory data of Android phones. Being a module working at the ring-0 level, LiME directly interacts with the kernel's memory management features and allows us to obtain the complete dump of physical memory without affecting any process in execution [2, 8].

- Accuracy (9/10): LiME captures the entire physical memory address space including the reserved addresses in the kernel, offering legally acceptable forensic information using the kernel-level API and thereby minimizing the possibility of any tampering from user-space APIs used by software solutions.
- Reliability (8/10): Is highly reliable and has undergone thorough testing within both research and forensics scenarios on multiple versions of the Android kernel.
- Ease of Use (4/10): Requires an Android device root, cross-compilation of the LKM, and Linux command line knowledge to use LiME; this is quite difficult for the average user.
- Compatibility (5/10): Compatibility out of the box can be achieved only on Android and Linux. Other operating systems, including iOS and Windows, need heavy changes for LiME to work.
- Performance (8/10): Fast memory dump speed due to direct access through the memory bus and low overhead of the system.

#### 3.1.2 AVML — Azure Virtual Machine Memory Dumper

**Type: Open Source Platform: Linux / Android (indirect)**

AVML was created by Microsoft's Security Response Center and is mainly used for RAM acquisition in cloud virtual machines running Linux. The portable and statically linked binary nature of AVML allows it to be used without being installed, which means that it can be applied in Android forensic investigations running Linux [14].

- Accuracy (6/10): It works effectively in Linux-controlled environments, but there are concerns regarding the acquisition of memory allocated for the kernel on mobile hardware.
- Reliability (7/10): Good documentation and reliability in cloud and server environments; however, validation in physical mobile hardware is limited.
- Ease of Use (8/10): An easy-to-use command line interface with few configuration settings.
- Compatibility (4/10): Only compatible with Linux OS; Android user space and iOS do not have native support.
- Performance (9/10): AVML is the fastest tool when it comes to RAM acquisition, as it utilizes a portable binary format.

#### 3.1.3 Belkasoft RAM Capturer

**Type: Commercial (Free) Platform: Windows (32/64-bit)**

Belkasoft RAM Capturer is a forensic-grade memory acquisition program that targets Windows-based systems. With its full-fledged graphical interface and commercial development approach, Belkasoft RAM Capturer can be considered one of the most user-friendly programs for law enforcement officers [11].

- Accuracy (6/10): Very accurate when acquiring memory from Windows host system; unable to acquire memory from Android and iOS mobile phones without third-party assistance.
- Reliability (9/10): Ties for the highest reliability score of all tested programs, owing to high commercial quality control and wide adoption by law enforcement agencies across the world.
- Ease of Use (10/10): The only program among those tested to earn a perfect usability score. The full graphical interface allows users to perform memory acquisitions through simple click-and-point operation without using any command lines.
- Compatibility (4/10): Compatible only with Windows 32-bit and 64-bit operating systems; requires third-party assistance to work with any mobile devices.
- Performance (7/10): Offers acceptable performance speed, slightly lower than that of command-line based programs.

#### 3.1.4 DumpIt

**Type: Commercial (Free) Platform: Windows (XP–11)**

DumpIt, created by Comae Technologies (later Magnet Forensics), is a single-executable memory acquisition tool for Windows.

Zeroinstallation enables instant implementation from portable media, thus making it one of the most preferred options for incident response and forensics by first responders [9].

- Accuracy (7/10): Provides complete memory dump in kernel and user space for Windows OS; provides memory dump in a format compatible with high-quality forensic analysis tools such as Volatility and WinDbg.
- Reliability (8/10): Widely used in incident response and digital forensics cases for Windows from XP to Windows 11.
- Ease of Use (9/10): Run as a single executable or with simple command-line invocation; requires no installation and no setup.
- Compatibility (5/10): Windows-specific; although some Android compatibility may be achieved using ADB in virtualisation, this is not DumpIt's primary function.
- Performance (8/10): Quick acquisition due to single-executable format; comparable to LiME in terms of performance in its native environment.

### 3.1.5 Volatility (with Acquisition Plugins)

**Type: Open Source Platform: Multi-platform (Windows / Linux / macOS / Android)**

Volatility is the foremost memory forensics framework that is open source, and although its primary function is analysis, it also features acquisition capabilities via integration with complementary tools such as LiME (for Android) and WinPMEM (for Windows). It is the framework that can support the largest number of memory profile architectures compared to other frameworks [7, 12].

- Accuracy (8/10): By using complementary methods for data acquisition, Volatility offers an accurate analysis of memory dumps. This is possible because this tool allows the extraction of detailed artefacts such as process trees, network connections, and hidden objects.
- Reliability (9/10): Highest rating in terms of reliability; the most reviewed memory forensics framework with many contributions from users and a vibrant community.
- Ease of Use (6/10): Familiarity with Python command line interface as well as the terms used in memory forensics is required to make efficient use of the framework.
- Compatibility (7/10): Compatibility scores its highest rating here; allows analysis of memory dumps on Windows, Linux, macOS, and Android using the highly configurable profile format.
- Performance (7/10): The tool's performance as an acquiring tool depends on the companion tool, while the performance for analysis depends on the dump size.

### 3.1.6 Magnet RAM Capture

**Type: Free Platform: Windows (integrates with Magnet AXIOM on mobile devices)**

- Magnet RAM Capture is a free memory acquisition utility made by Magnet Forensics and designed to be used for live forensics analysis. The captured data can be processed using Volatility and Magnet AXIOM; the latter is a paid forensic analysis tool that works well with Magnet RAM Capture [15].
- Accuracy (7/10): Successfully obtains accurate memory images for Windows; ability to use AXIOM makes it possible to analyze Android and iOS hybrid acquisitions.
- Reliability (8/10): Supported by the ecosystem developed by Magnet Forensics; trusted by law enforcement agencies globally.
- Ease of Use (9/10): User-friendly graphical interface with no configuration needed; ideal for live acquisition.
- Compatibility (6/10): Best compatibility score among all Windows-based tools considered; partial Android and iOS support via Magnet AXIOM integration provides the widest mobile compatibility among commercial tools.
- Performance (8/10): Minimal system impact and fast acquisition process.

### 3.2 Consolidated Comparative Matrix

Table 2 presents the full comparative evaluation matrix, including per-criterion scores and mean aggregate scores for each tool.

*Table 2: Comparative Evaluation Matrix of RAM Acquisition Tools (Scores out of 10; A = Accuracy, R = Reliability, EU = Ease of Use, C = Compatibility, P = Performance)*

| Tool | Accuracy | Reliability | Ease of Use | Compat. | Perf. | Avg. |
|---|---|---|---|---|---|---|
| LiME (Linux Memory Extractor) | 9 | 8 | 4 | 5 | 8 | 6 |
| AVML (Azure VM Memory Dumper) | 6 | 7 | 8 | 4 | 9 | 6 |
| **Tool** | **Accuracy** | **Reliability** | **Ease of Use** | **Compat.** | **Perf.** | **Avg.** |
| Belkasoft RAM Capturer | 6 | 9 | 10 | 4 | 7 | 7 |
| DumpIt | 7 | 8 | 9 | 5 | 8 | 7 |
| Volatility (with Acquisition Plugins) | 8 | 9 | 6 | 7 | 7 | 7 |
| Magnet RAM Capture | 7 | 8 | 9 | 6 | 8 | 7 |

**Average Score** = (Accuracy + Reliability + Ease of Use + Compatibility + Performance)/5

To provide a concise overview of the evaluated tools, Table 3 summarizes their type, supported platforms, criterion-wise scores, and primary strengths.

*Table 3: Tool Profiles: Type, Platform, and Primary Strength*

| Tool | Type | Platform | Scores (A/R/EU/C/P) | Primary Strength |
|---|---|---|---|---|
| LiME | Open Source | Android / Linux | 9 / 8 / 4 / 5 / 8 | Highest accuracy; complex deployment |
| AVML | Open Source | Linux / Android | 6 / 7 / 8 / 4 / 9 | Fastest speed; limited mobile HW support |
| Belkasoft | Commercial (Free) | Windows | 6 / 9 / 10 / 4 / 7 | Easiest GUI; Windows-only platform |
| DumpIt | Commercial (Free) | Windows | 7 / 8 / 9 / 5 / 8 | Portable single-executable; quick field deploy |
| Volatility | Open Source | Multi-platform | 8 / 9 / 6 / 7 / 7 | Widest compatibility; analysis-centric |
| Magnet RAM Capture | Commercial (Free) | Windows | 7 / 8 / 9 / 6 / 8 | Best cross-tool integration; law-enforcement grade |

## 4. Discussion

### 4.1 The Accuracy–Usability Trade-off

The most consistent trend emerging from this evaluation is that of an inverse correlation between forensic completeness and usability. The tools which scored best in terms of forensic completeness – LiME and Volatility, both 9 out of 10 in terms of accuracy – require high levels of technical expertise to utilize, scoring 4 out of 10 and 6 out of 10 respectively in terms of usability. In contrast, the most userfriendly tools are those that score relatively poorly in terms of forensic completeness – Belkasoft and Magnet RAM Capture, scoring 6 out of 10 and 7 out of 10 respectively, in terms of accuracy.

The above conclusion carries great significance for forensic training and operations. In organizations where non-experts are used in the first instance as evidence-preservers, easy-to-use software must be chosen, whereas forensic laboratories equipped with experts working on the seized device must choose accurate software. If both are combined in one tool choice decision, the risk of evidence contamination and incomplete evidence will prevail because of either the improper use of the software by the operator or the limitations of the software itself.

### 4.2 Platform Compatibility as a Persistent Gap

The area of platform compatibility is seen as the one where all the tools under review exhibit the worst performance, with a maximum of 7 out of 10 points being awarded to Volatility and a modal range of 4-5 out of 10 for the rest. The lack of reliable native support for both Android and iOS during acquisition can be attributed to the different nature of security models in these two leading mobile operating systems, the Linux heritage of the former making it compatible with LKM-acquisition tools and the latter's Secure Enclave and kernel signature policies preventing any such attempts [5, 12].

The cross-platform challenge remains one of the foremost unmet requirements in mobile RAM forensics, particularly because modern Android and iOS security architectures restrict direct memory acquisition and forensic access [5, 12, 16].

### 4.3 The Case for a Complementary Multi-Tool Strategy

None of the tools considered in the analysis achieves an average score greater than 7.6/10, and none of the tools attains a score of 9 or more in any category without having at least one weakness in another aspect. The above trend provides a strong case for adopting multitool standards in the conduct of forensic analysis on mobile phones. A well-rounded approach combining LiME (for Android accuracy), Volatility (for analysis across different systems), and DumpIt/Magnet RAM Capture (for fast RAM capture in Windows) would address all the limitations of any single tool.

This recommendation is in line with the view expressed by Vidas et al. [5] and Pooters et al. [15], who have independently argued that there is no forensic software solution that is sufficiently versatile to be used in all mobile environments and investigative situations.

This paper builds on the views expressed above through the development of a scoring system for selecting tools.

### 4.4 Open-Source vs. Commercial Tools

This analysis has shown that there is a complex distinction between the two types of forensic tools, which cannot be easily classified. Open source tools (LiME, AVML, Volatility) have better accuracy and cross-platform capabilities, but are more difficult to use. Commercial tools (Belkasoft, DumpIt, Magnet) have greater ease of use and reliability – which can also be attributed to the quality control process in commercial software development – but they operate only on Windows systems.

When resources are limited in the forensic environment, the presence of excellent free commercial software (Belkasoft, DumpIt, Magnet RAM Capture), combined with robust open-source platforms (LiME, Volatility), suggests that an effective multi-tool acquisition suite could be constructed at no licensing expense. The main expense would be incurred through training in the use of the open-source software suite, which would pay dividends down the line.

Based on the comparative evaluation and discussion presented above, Table 4 provides evidence-based recommendations for selecting RAM acquisition tools under different mobile forensic investigation scenarios.

*Table 4: Scenario-Based RAM Acquisition Tool Recommendations*

| Investigation Scenario | Recommended Tool(s) | Prerequisites | Rationale |
|---|---|---|---|
| Android device — high forensic accuracy required | LiME | Root access available | Kernel-level dump; minimal memory modification |
| Android device — fast field acquisition | AVML + LiME (hybrid) | ADB-enabled device | Speed + completeness combination |
| Windows PC / workstation | DumpIt or Magnet RAM Capture | Standard user access | Portable, no install; immediate deployment |
| Multi-OS investigation environment | Volatility (analysis) + LiME/DumpIt (acq.) | Linux/Windows host | Cross-platform profile support |
| Non-expert or first responder | Belkasoft RAM Capturer or Magnet RAM Capture | Windows device | One-click GUI; minimal training required |
| Hybrid mobile–desktop investigation | Magnet RAM Capture + AXIOM | Windows + mobile companion | Integrated ecosystem; partial Android/iOS coverage |

## 5. Conclusions

The current research work has provided a structured comparison analysis of six tools for RAM acquisition such as LiME, AVML, Belkasoft RAM Capturer, DumpIt, Volatility, and Magnet RAM Capture within the framework of mobile device forensics. From the findings of the analysis, it is clear that the performance of the tools depends on the context as each tool shows different pros and cons based on five criteria: accuracy, reliability, usability, compatibility, and acquisition performance.

LiME becomes the most forensic sound method of acquiring RAM on an Android device by ensuring high accuracy because of its ability to acquire data at the kernel level. Volatility is the most flexible and compatible analytical framework across all platforms. On the other hand, Belkasoft RAM Capturer and Magnet RAM Capture provide the most reliable methods of analyzing RAM on Windows devices. DumpIt stands out due to its portability.

The non-existence of any tool that succeeds in performing excellently in all five criteria used to evaluate the effectiveness of a tool indicates the primary finding of the research, which is that there needs to be a combined approach to conducting forensic analysis on mobile RAM. The approach must involve the use of multiple tools rather than looking for one perfect tool.

In addition to this, a key gap has been identified in terms of technological advances — namely, the requirement for a cross-platform RAM acquisition solution that can accommodate both Android and iOS in an effective process. The future direction for this research must focus on empirical testing of the tools in question, especially considering the need for international standards for certifying forensic RAM acquisition tools.

## 6. List of Abbreviations

| Abbreviation | Full Form |
|---|---|
| RAM | Random Access memory |
| LiME | Linux Memory Extractor |
| AVML | Azure Virtual Machine Memory Dumper |
| GUI | Graphical User Interface |
| LKM | Loadable Kernel Module |
| OS | Operating System |
| AXIOM | Magnet AXIOM Forensic Platform |

## 7. Declarations

**a) Ethics Approval and Consent to Participate** Not applicable.

**b) Consent for Publication**

Not applicable

**c) Funding**

The authors received no specific funding for this work

## References

1. Statista. (2024). Number of smartphone users worldwide from 2016 to 2028. Statista Research Department. https://www.statista.com/statistics/330695/ number-of-smartphone-users-worldwide/
2. Sylve, J., Case, A., Marziale, L., & Richard III, G. G. (2012). Acquisition and analysis of volatile memory from Android devices. Digital Investigation, 8(3–4), 175–184. https://doi.org/10.1016/j.diin.2011.10.003
3. Ligh, M. H., Case, A., Levy, J., & Walters, A. (2014). The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. Wiley. ISBN: 978-1118825099
4. Vidas, T., Martincic, C., & Christin, N. (2011). Challenges in mobile device forensics. Proceedings of the 6th USENIX Workshop on Hot Topics in Security, 1–6.
5. Breeuwsma, M., De Jongh, M., Klaver, C., & Van der Knijff, R. (2007). Forensic data recovery from flash memory. Small Scale Digital Device Forensics Journal, 1(1), 1–17.
6. Kumar, P., Rashid, E., & Narayan, R. (2020). A comparative study of mobile forensic tools for Android devices. International Journal of Engineering Research & Technology, 9(7), 112–118.
7. Case, A., & Richard III, G. G. (2017). Memory forensics: The art of detecting hidden malware. IEEE Security & Privacy, 15(2), 42–49. https://doi.org/10.1109/MSP.2017.30
8. Patel, A., Sharma, D., & Dholariya, D. (2021). A forensic evidence recovery from Android device applications. International Journal of Computer Science and Mobile Computing, 10(5), 45–52.
9. Carrier, B., & Grand, J. (2004). A hardware-based memory acquisition procedure for digital investigations. Digital Investigation, 1(1), 50–
10. 60. https://doi.org/10.1016/j.diin.2003.12.001
11. Pooters, I., Quick, D., & Choo, K. K. R. (2018). Comparative analysis of open-source and commercial forensic tools for mobile devices. Journal of Digital Forensics, Security and Law, 13(2), 77–98.
12. Garfinkel, S., & Malan, D. J. (2009). An investigation of forensic memory acquisition tools. Proceedings of the 3rd International Conference on Systematic Approaches to Digital Forensic Engineering, 88–100.
13. Baggili, I., Mislan, J., & Rogers, M. (2007). Mobile phone forensics tool testing: A database driven approach. International Journal of Digital Evidence, 6(2), 1–15.
14. Doherty, E. (2012). Digital Forensics for Handheld Devices. CRC Press. https://doi.org/10.1201/b12979
15. Microsoft Security Response Center. (2019). AVML – Azure Virtual Machine Memory Dumper [Technical documentation]. Microsoft Corporation. https://github.com/microsoft/avml
16. Magnet Forensics. (2022). Magnet RAM Capture: User Guide and Technical Reference [Software documentation]. Magnet Forensics Inc.
17. https://www.magnetforensics.com/resources/ magnet-ram-capture/