

# Navigating cyber investigations: strategies and tools for forensic data acquisition

Srinivas Kanakala<sup>1</sup>, Vempaty Prashanthi<sup>2</sup>, K. V. Sharada<sup>3</sup>

<sup>1</sup>Department of Computer Science and Engineering, VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India

<sup>2</sup>Department of Information Technology, Chaitanya Bharathi Institute of Technology, Hyderabad, India

<sup>3</sup>Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad, India

## Article Info

### Article history:

Received Aug 23, 2024

Revised Mar 24, 2025

Accepted May 23, 2025

### Keywords:

Civil litigations

Computer forensics

Cybercrimes

Data acquisition

Data automation

Digital evidence

Forensic investigation

## ABSTRACT

The rapid proliferation of cybercrimes has underscored the critical importance of robust data acquisition methodologies in the field of digital forensics. This research publication explores various aspects of forensic data acquisition, focusing on techniques, tools, and best practices employed by forensic investigators to collect and preserve digital evidence effectively. Beginning with an overview of the escalating cyber threat landscape and the consequential need for forensic investigations, the publication delves into the fundamental concepts of data acquisition, emphasizing the significance of ensuring data integrity and admissibility in legal proceedings. It examines the process of acquiring both volatile and non-volatile data from diverse sources, including hard drives, RAM, and other digital storage media. Furthermore, it evaluates a range of forensic imaging and validation methods, encompassing tools such as Belkasoft live RAM capturer, AccessData FTK Imager, and ProDiscover, alongside validation techniques using PowerShell utility and commercial forensic software. Through comprehensive analysis and discussion, this study serves as a valuable resource for forensic practitioners, researchers, and legal professionals seeking to enhance their understanding of forensic data acquisition methodologies in the ever-evolving landscape of cybercrime investigation.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



## Corresponding Author:

Srinivas Kanakala

Department of Computer Science and Engineering, VNR Vignana Jyothi Institute of Engineering and Technology

Hyderabad, Telangana, India

Email: [srinivaskanakala@gmail.com](mailto:srinivaskanakala@gmail.com)

## 1. INTRODUCTION

The rise in cybercrimes and civil lawsuits involving major corporations has underscored the importance of computer forensics. Organizations are increasingly finding it necessary to either engage a computer forensics agency or employ experts in the field to address issues related to the use of computers and digital technology. The substantial economic damages incurred from cybercrimes have further fueled the demand for expertise in computer forensics, which is crucial for identifying, tracking, and prosecuting cybercriminals. As a subset of digital forensics, computer forensics focuses on crimes conducted via computing devices like networks, computers, and digital storage devices. It involves a systematic approach to discovering, collecting, preserving, analyzing, documenting, and presenting digital evidence in such a way that it is upheld in legal and administrative proceedings in court. Essentially, computer forensics is concerned with uncovering legally sound evidence pertinent to digital crimes to pinpoint and legally confront those responsible. Here are the distinct stages of the computer forensics investigation process:

- Pre-investigation phase: This initial phase includes all preparatory actions before the actual investigation begins. It covers setting up a forensics lab, preparing a forensics workstation, assembling an investigative toolkit, forming a team, and securing necessary approvals. Planning, defining the investigation's objectives, and safeguarding the perimeter and devices involved are also critical at this stage.
- Investigation phase: This is the core phase where the actual forensic activities take place, including the collection, safeguarding, and analysis of evidence to pinpoint the crime's origin and perpetrator. This phase requires the application of technical expertise to discover and meticulously handle, document, and conserve the evidence and findings. Skilled professionals ensure the precision and integrity of the investigative process.
- Post-investigation phase: This final phase involves compiling and documenting all activities and results from the investigation. The goal is to produce a report that is comprehensible to its intended readers and provides robust and admissible evidence. The report must adhere to the specific reporting standards of each jurisdiction and be legally robust to withstand scrutiny in a court of law.

Data acquisition serves as the initial active phase in the forensic investigation process. This process involves more than just transferring files from one device to another. Forensic data acquisition aims to capture every single piece of information from the memory and storage of the affected system to create a forensic replica of this data. Importantly, this replica must be made in a way that preserves the data's integrity, ensuring it remains verifiable and admissible in court proceedings. This section explores the essential principles of data acquisition and outlines the steps involved in the data acquisition methodology. To commence a forensic examination of a potential evidence source, investigators must first replicate the data found on any digital storage mediums at the crime scene, such as a hard disk. This replication can be conducted either directly at the crime scene or after transporting the device to a secure location for further analysis. Forensic data acquisition is the process of systematically imaging or collecting information from various media using standardized methods to preserve its forensic value. It involves extracting electronically stored information (ESI) from potential suspect computers or storage media to analyze a crime or incident. As technology advances, data acquisition methods have become more accurate, simple, and flexible. Nonetheless, it is crucial for investigators to use an acquisition methodology that is forensically sound, meaning it should be both verifiable and repeatable. This is important to ensure the admissibility of the data or evidence in a court of law. A critical aspect of forensic data acquisition is timing. Data stored on certain mediums like hard drives can remain unchanged and can be collected even after the system has been powered down. However, data stored on volatile sources such as RAM is dynamic and must be collected immediately because it is lost when the power is turned off or if the system is rebooted. This study explores various forensic tools and validation techniques to identify effective methodologies for acquiring and preserving digital evidence. By analyzing these approaches, the research aims to enhance forensic investigations amidst evolving cyber threats.

## 2. LITERATURE SURVEY

The field of forensic data acquisition has garnered considerable attention from researchers and practitioners alike, leading to a wealth of existing literature exploring various aspects of digital evidence collection and preservation. Several notable papers have contributed significantly to our understanding of forensic data acquisition methodologies, tools, and best practices. One seminal work in this domain is the paper by Kohn *et al.* [1], proposed a standardized digital forensic process model to aid investigators in following a uniform approach in digital forensic investigations. A comprehensive study by Casey and Rose [2] delves into the intricacies of forensic imaging and acquisition, examining different approaches for capturing data from storage devices while maintaining data integrity. The paper discusses various imaging tools and methodologies, in forensic investigations. Gengenbach *et al.* [3], presents preliminary results from ongoing research conducted as part of the BitCurator project, a two-year grant funded initiative to build, test, and analyze systems and software for incorporating digital forensics methods into collecting institutions' workflows. The paper by Huebner *et al.* [4] explores the use of volatile memory forensics for acquiring and analyzing volatile data from live systems, offering insights into the evolving landscape of digital evidence collection. Brain and Smith [5] provides an overview of recent advancements in forensic imaging techniques, focusing on emerging technologies and methodologies for capturing and preserving digital evidence. Abiodun *et al.* [6] paper explores the unique challenges associated with forensic data acquisition in cloud environments and presents innovative solutions to address these challenges. Kim and Lee [7] paper examines the unique challenges and solutions in mobile forensic data acquisition, focusing on the complexities of extracting digital evidence from smartphones and other mobile devices. Pang *et al.* [8] presents an overview of next-generation forensic imaging techniques, highlighting recent trends and future directions in the field. The authors discuss advancements in hardware-based imaging solutions, such as solid-

state drive (SSD) forensics and firmware-level acquisition methods. Fakhouri *et al.* and Javed *et al.* [9], [10] explores the use of open-source and commercial forensic tools, challenges cyber forensic frameworks and standards, and best practices in cyber forensic investigations. Prasanthi [11], Sindhu and Meshram [12] describes importance of computer forensics and its origin, forensic framework and different types of existing computer forensic tools and its usage. Tageldin and Venter [13] shows that machine learning algorithms can be used for predictions of different aspects and in forensics also. Barik *et al.*, Kamble and Jain, and Lovanshi and Bansal [14]–[16] shows systematic approach using artificial intelligence to enable the system security team to facilitate the process of conducting a security audit taking into account the sensitivity of their systems. Machine learning algorithms can also be used for prediction of diseases [17]–[19]. Awad *et al.*, Eden *et al.*, and Kurkowski and Sheno [20]–[22] presents a survey into the literature on digital forensics applied to SCADA systems. Dubey *et al.* [23], [24] discuss the tools in forensics. Dubey *et al.*, S. Vömel and J. Stüttgen, and Shree [24]–[26] study the complexity and readiness of community-accepted devices in a smart application towards assistance in criminal investigations and also memory forensics acquisition techniques are discussed. The proposed system introduces an integrated toolset that combines functionalities from existing tools like Belkasoft Live RAM Capturer and AccessData FTK Imager, ensuring seamless data capture across various operating systems and devices. Real-time validation mechanisms are implemented to maintain data integrity throughout the acquisition process, minimizing errors and discrepancies.

### 3. METHODOLOGY

This section discusses the various steps that investigators need to undertake to effectively collect data that holds evidentiary value. When conducting forensic data acquisition, it is essential to carefully select approaches and methodologies that preserve the integrity and accuracy of the original evidence. The data acquisition process must adhere to departmental or organizational policies and comply with relevant standards, regulations, and laws. Additionally, investigators should ensure that the data acquisition is performed in a forensically sound manner. This includes authenticating the integrity of the acquired data image using hash algorithms, which help verify that the data has not been altered from its original state. Figure 1 represents block diagram of data acquisition methodology.

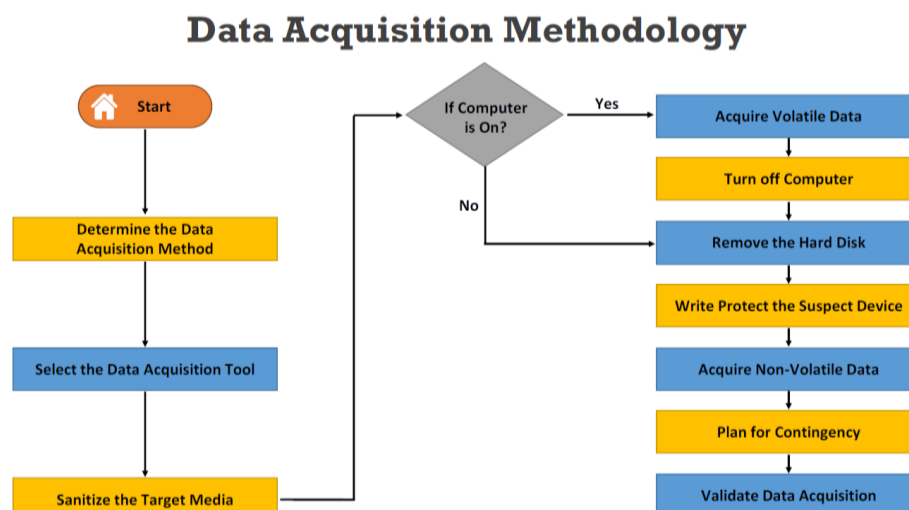


Figure 1. Block diagram of data acquisition methodology

Step 1: determine the best data acquisition method: In forensic investigations, selecting the appropriate data acquisition method is crucial for ensuring data integrity and legal admissibility. For large suspect drives, disk-to-image copying is preferred, but if storage is limited, data size can be reduced using compression tools like Microsoft DriveSpace, DoubleSpace, PKZip, WinZip, or WinRAR to eliminate slack space. Integrity verification through hash values such as MD5, SHA-2, or SHA-3 before and after compression ensures lossless data retention. Since acquisition time depends on drive size (e.g., a 1 TB drive may take over 11 hours), investigators should prioritize relevant data to optimize time and resources. In cases where the original drive must remain untouched, such as in civil litigation, logical acquisition may be an

option. When possible, creating a reliable copy using trusted forensic tools is essential, as investigations often allow only one opportunity to capture data accurately. A thorough evaluation of these factors ensures an efficient and legally compliant forensic process.

Step 2: select the data acquisition tool: Selecting the right forensic data acquisition tool is crucial, as it must meet strict standards to ensure accuracy and reliability. The tool should not modify the original data, log I/O errors with details, and alert users if the destination size is insufficient. It must withstand scientific scrutiny, capture all visible and hidden data sectors, and create a complete bit-stream copy unless access errors occur. In such cases, a qualified bit-stream copy should be made. The tool should only copy data if the destination is equal to or larger than the source and must provide precise documentation for consistent results.

Step 3: Sanitize the target media: Before data acquisition, proper data sanitization is essential to prevent unauthorized access to existing information on the target media. Simple deletion or formatting is insufficient, as data remains physically intact. To ensure complete erasure, data should be overwritten with sequential zeroes or ones. After data collection and analysis, secure disposal of media is crucial to prevent retrieval. Investigators follow standards like the Russian GOST P50739-95 (6 passes: zeros first, then random bytes) or the German VSITR (7 passes: alternating 0x00, 0xFF, and 0xAA) for thorough data destruction.

Step 4: Acquire volatile data; acquiring volatile data, such as the contents of RAM, requires special attention from investigators due to its dynamic nature. Working on a live system can potentially alter RAM contents or running processes, leading to unintended consequences such as changes in file access dates, execution of malware, or system reboots that render the system inaccessible. Therefore, it's crucial to approach the examination of a live system and volatile data acquisition with caution. While most volatile data can be retrieved by examining the live system directly, an equivalent amount of data can also be obtained by analyzing an image acquired from the system's memory. The following sections outline the methods for acquiring volatile data from Windows, Linux, and Mac systems, ensuring a thorough and careful approach to the acquisition process.

Step 5: Enable write protection on the evidence media: Write protection involves implementing measures to prevent storage media from being written to or modified. This can be achieved through hardware devices or software programs installed on the accessing computer. Enabling write protection ensures that data can only be read, preventing any writing or modification. In the context of forensic data acquisition, it's essential to enable write protection on the evidence media. This refers to the storage within the original device from which data is being copied onto a separate storage device. By write protecting the evidence media, forensic investigators safeguard it from any unauthorized modifications. Maintaining the integrity of the evidence throughout acquisition, analysis, and management is crucial for forensic investigations. It's imperative that investigators have confidence in the legitimacy of the evidence they obtain, as it must be admissible in court. To prevent any alteration of disk contents, investigators can implement various defense mechanisms, such as: Setting a hardware jumper to configure the disk as read-only. Using an operating system and software that are incapable of writing to the disk unless explicitly instructed to do so. Employing a hard disk write block tool, which provides protection against any attempts to write to the disk.

Step 6: Acquire non-volatile data non-volatile data, typically stored on hard disks, can be acquired through both live and dead acquisition processes. For live acquisition, investigators may utilize remote acquisition tools like Netcat or bootable CDs/USBs with tools like CAINE to access the hard disk. The dead acquisition process involves the following steps: Remove the hard drive from the suspect device. Connect the hard drive to a forensic workstation for acquisition. Implement write-blocking on the hard disk to ensure it provides only read-only access, preventing any modification or tampering of its contents. Utilize a forensic acquisition tool suitable for collecting the required data.

Step 7: Plan for contingency in digital forensics investigations, planning for contingency is essential to address potential failures or unforeseen events during the acquisition process. This involves having a backup plan in place in case hardware or software malfunctions occur. Contingency planning is crucial in all cyber investigations as it enables investigators to prepare for unexpected circumstances. It involves developing strategies to mitigate risks and ensure the completion of the investigation process even if certain tools or systems fail. For hard disk data acquisition, investigators should create at least two images of the digital evidence collected. This redundancy helps to preserve the integrity of the evidence. In the event that one copy of the digital evidence becomes corrupted or compromised, investigators can rely on the backup copy to continue their analysis and ensure the integrity of the investigation. Figure 2 shows Hard disk data acquisition.

When you have access to multiple imaging tools like pro-discover forensics or AccessData FTK Imager, it is advisable to create the first image with one tool and the second image with another tool. This approach helps to validate the integrity of the imaging process by cross-verifying the results obtained from different tools. However, if you only have access to one imaging tool, it is still crucial to create multiple images of the drive using the same tool. This redundancy ensures that you have backup copies of the digital

evidence, which can be invaluable in case of corruption or other issues with one of the images. By employing multiple imaging tools for creating multiple images with the same tool, you enhance the reliability and integrity of the forensic imaging process, thereby strengthening the validity of the evidence collected for analysis. When conducting data acquisition, it's worth considering the use of hardware acquisition tools like UFED Ultimate or IM SOLO-4 G3 IT RUGGEDIZED. These tools offer advantages such as accessing the drive at the BIOS level, which allows for copying data from the host protected area (HPA). Accessing the drive at the BIOS level provides a deeper level of access compared to software-based methods, enabling the acquisition of data that may be hidden or protected within the HPA. By utilizing hardware acquisition tools, shown in Figure 3 investigators can ensure comprehensive data collection, enhancing the thoroughness and accuracy of the forensic process.



Figure 2. Data Acquisition with imaging tools



Figure 3. Data Acquisition with hardware tool

#### 4. RESULTS AND DISCUSSION

To extract volatile memory data from a Windows machine, forensic investigators can utilize tools like Belkasoft Live RAM Capturer. This tool enables the reliable extraction of the entire contents of the computer's volatile memory, even when protected by active anti-debugging or anti-dumping systems. Belkasoft Live RAM Capturer saves the extracted data in .mem format, facilitating further analysis. Belkasoft Live RAM Capturer is an open-source forensic tool, ensuring transparency and flexibility in the acquisition process. The tool captures the entire contents of volatile memory, providing a comprehensive snapshot of the system's state at the time of acquisition. Belkasoft Live RAM Capturer is compatible with all versions and editions of Windows, including XP, Vista, Windows 7, 8, and 10, as well as 2003 and 2008 Server editions. It can bypass active anti-debugging or anti-dumping systems, ensuring successful acquisition even in protected environments. Separate 32-bit and 64-bit builds are available, minimizing the tool's footprint and ensuring compatibility with different system architectures. Memory dumps captured with Belkasoft Live RAM Capturer can be further analyzed using tools like Belkasoft Evidence Center software, facilitating in-depth examination and interpretation of the acquired data. By leveraging Belkasoft Live RAM Capturer, forensic investigators can effectively acquire volatile memory data from Windows machines, enhancing their ability to gather crucial evidence for forensic analysis. Figure 4 represents capturing RAM of a machine. While performing live acquisition, an investigator must be aware of the fact that working on a live system may alter the contents of RAM or processes running on the system. Any involuntary action performed on the system may potentially make the system inaccessible.

AccessData FTK Imager is a powerful tool used by forensic professionals to preview, acquire, and image computer data while maintaining the integrity of the original evidence. Its comprehensive features make it an essential component of digital forensics investigations. Figure 5 show selecting destination directory to store image file and Figure 6 shows that image is created successfully. Validate data Acquisition – Windows validation methods. In Windows environments, there are several methods for validating data acquisition to ensure the integrity of evidence: Windows includes PowerShell, which offers the Get-FileHash cmdlet. This cmdlet computes the hash value of an evidence file using a specified hash algorithm. Investigators can use this hash value throughout the investigation to validate the integrity of the evidence. Many commercial computer forensics programs come with built-in validation features. These features allow investigators to validate evidence files directly within the forensic software. By comparing hash values or other metadata, investigators can confirm the integrity of the acquired data. ProDiscover generates .eve files containing metadata, including hash values, for segmented files or acquisition files. When loading an image into ProDiscover, the tool compares the hash value of the image to the hash value of the original media. If the hashes do not match, ProDiscover notifies the user that the image may be corrupt, indicating that the evidence may not be reliable. By leveraging these validation methods, forensic investigators can ensure the integrity and reliability of the acquired evidence, strengthening the validity of their findings during legal proceedings. In Figure 7 we can see that hash value is computed.

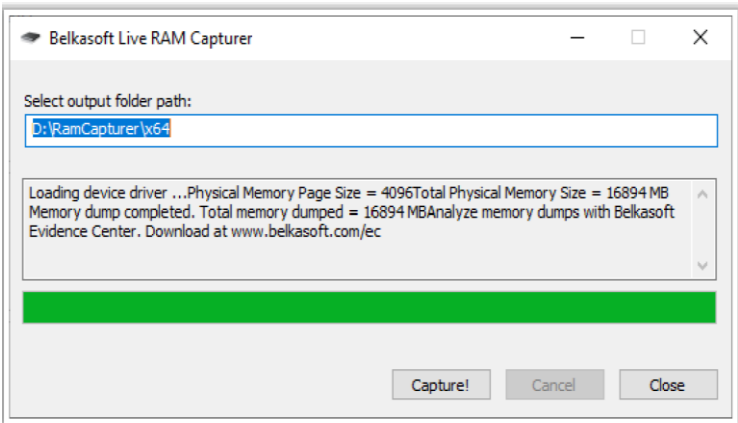


Figure 4. Capturing RAM of a machine

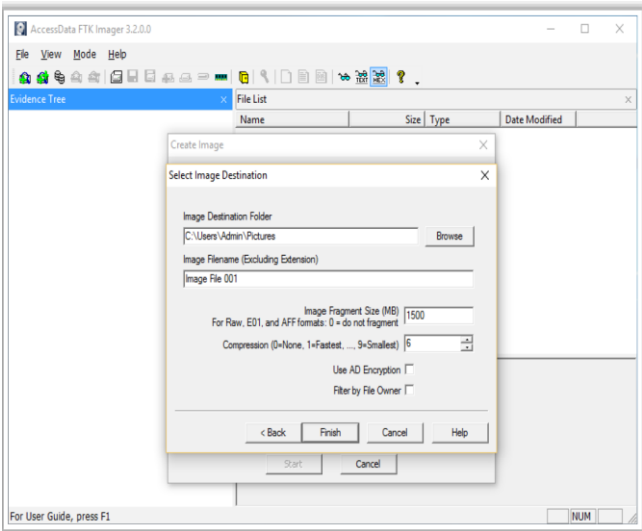


Figure 5. Selecting destination directory

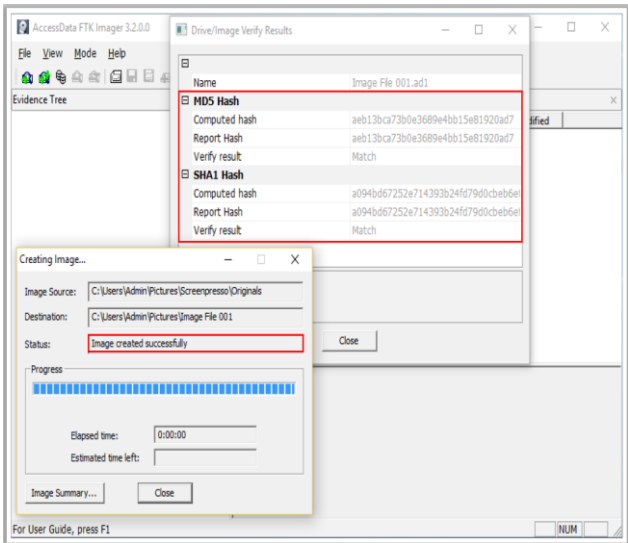


Figure 6. Image created successfully

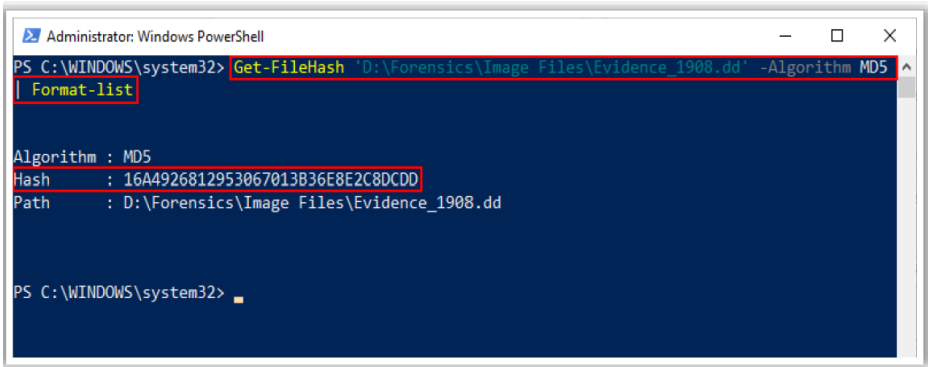


Figure 7. Computing hash value

5. CONCLUSION

The culmination of our discussion on forensic data acquisition reflects a nuanced understanding of this pivotal aspect within digital investigations. Commencing with the acknowledgment of the burgeoning landscape of cybercrimes and the ensuing imperative for robust forensic practices, our dialogue traversed through the intricacies of data acquisition methodologies and validation techniques. Our exploration elucidated the pivotal roles of various tools such as Belkasoft Live RAM Capturer and AccessData FTK Imager in capturing volatile memory data from Windows machines. These tools, each tailored to specific forensic requirements, underscored the sophistication and diversity present within the forensic toolkit. Furthermore, our discourse shed light on the significance of validation methods, encompassing PowerShell utilities and commercial forensic software, in ensuring the integrity and reliability of acquired data. The comparative analysis among different tools and methods underscored their unique features, capabilities, and compatibility with Windows systems. While Belkasoft Live RAM Capturer emerged as a specialized solution for volatile memory acquisition, AccessData FTK Imager offered a comprehensive suite of functionalities including imaging and validation. Simultaneously, validation methods stood as essential safeguards, ensuring the veracity of acquired data and its admissibility in legal proceedings. In essence, our discussion underscores the critical importance of employing apt tools and methodologies in forensic data acquisition, thereby facilitating the effective gathering of digital evidence while upholding legal and procedural standards. Armed with the insights gleaned from our discourse, forensic practitioners are empowered to conduct thorough and reliable digital investigations amidst the evolving landscape of cyber threats. Looking ahead, several avenues for future work present themselves in the realm of forensic data acquisition. Continued refinement and development of forensic acquisition tools can enhance their capabilities and adaptability to evolving technologies and forensic challenges. Future tools may focus on improving efficiency, scalability, and compatibility across diverse operating systems and devices.

FUNDING INFORMATION

There is no funding involved for this research work.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Srinivas Kanakala	✓	✓	✓	✓	✓	✓			✓	✓			✓	
Vempaty Prashanthi			✓			✓		✓	✓	✓	✓	✓		
K. V. Sharada				✓		✓					✓			

C : Conceptualization	I : Investigation	Vi : Visualization
M : Methodology	R : Resources	Su : Supervision
So : Software	D : Data Curation	P : Project administration
Va : Validation	O : Writing - Original Draft	Fu : Funding acquisition
Fo : Formal analysis	E : Writing - Review & Editing	



**CONFLICT OF INTEREST STATEMENT**

Authors state no conflict of interest.

**DATA AVAILABILITY**




Derived data supporting the findings of this study are available from the corresponding author Srinivas Kanakala on request.

**REFERENCES**




- [1] M. D. Kohn, M. M. Eloff, and J. H. P. Eloff, "Integrated digital forensic process model," *Computers & Security*, vol. 38, pp. 103–115, Oct. 2013, doi: 10.1016/j.cose.2013.05.001.
- [2] E. Casey and C. W. Rose, "Forensic analysis," in *Handbook of digital forensics and investigation*, Academic Press, 2010, pp. 21–62.
- [3] M. Gengenbach, A. Chassanoff, and P. Olsen, "Integrating digital forensics into born-digital workflows: The BitCurator project," *Proceedings of the ASIST Annual Meeting*, vol. 49, no. 1, pp. 1–4, 2012, doi: 10.1002/meet.14504901343.
- [4] E. Huebner, D. Bem, F. Henskens, and M. Wallis, "Persistent systems techniques in forensic acquisition of memory," *Digital Investigation*, vol. 4, no. 3–4, pp. 129–137, 2007, doi: 10.1016/j.diin.2008.02.001.
- [5] B. E. Dalrymple and E. J. Smith, *Forensic digital image processing*. Boca Raton, FL : CRC Press, [2018]: CRC Press, 2018.
- [6] O. I. Abiodun, M. Alawida, A. E. Omolara, and A. Alabdulatif, "Data provenance for cloud forensic investigations, security, challenges, solutions and future perspectives: A survey," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 10217–10245, Nov. 2022, doi: 10.1016/j.jksuci.2022.10.018.
- [7] D. Kim and S. Lee, "Study of identifying and managing the potential evidence for effective Android forensics," *Forensic Science International: Digital Investigation*, vol. 33, 2020, doi: 10.1016/j.fsidi.2019.200897.
- [8] J. B. Pang *et al.*, "A 124-plex microhaplotype panel based on next-generation sequencing developed for forensic applications," *Scientific Reports*, vol. 10, no. 1, 2020, doi: 10.1038/s41598-020-58980-x.
- [9] H. N. Fakhouri, M. A. Alsharaiah, A. K. Al Hwaitat, M. Alkalailieh, and F. F. Dweikat, "Overview of challenges faced by digital forensic," *2nd International Conference on Cyber Resilience, ICCR 2024*, 2024, doi: 10.1109/ICCR61006.2024.10532850.
- [10] 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.
- [11] B. V. Prasanthi, "Cyber forensic tools: a review," *International Journal of Engineering Trends and Technology*, vol. 41, no. 5, pp. 266–271, 2016, doi: 10.14445/22315381/ijett-v41p249.
- [12] K. K. Sindhu and B. B. Meshram, "Digital forensic investigation tools and procedures," *International Journal of Computer Network and Information Security*, vol. 4, no. 4, pp. 39–48, 2012, doi: 10.5815/ijcnis.2012.04.05.
- [13] L. Tageldin and H. Venter, "Machine-learning forensics: state of the art in the use of machine-learning techniques for digital forensic investigations within smart environments," *Applied Sciences (Switzerland)*, vol. 13, no. 18, 2023, doi: 10.3390/app131810169.
- [14] K. Barik, A. Abirami, K. Konar, and S. Das, "Research perspective on digital forensic tools and investigation process," *Lecture Notes on Data Engineering and Communications Technologies*, vol. 109, pp. 71–95, 2022, doi: 10.1007/978-3-030-93453-8\_4.
- [15] D. R. Kamble and N. Jain, "Digital forensic tools: A comparative approach," *International Journal of Advance Research In Science And Engineering IJARSE*, vol. 8354, no. 4, pp. 157–168, 2015.
- [16] M. Lovanshi and P. Bansal, "Comparative study of digital forensic tools," in *Data, Engineering and Applications*, Singapore: Springer Singapore, 2019, pp. 195–204.
- [17] K. V. Sharada, V. Prashanthi, and S. Kanakala, "Detection and classification of intracranial brain hemorrhage," *Lecture Notes in Networks and Systems*, vol. 244, pp. 455–464, 2022, doi: 10.1007/978-981-16-2919-8\_41.
- [18] H. Dasi and S. Kanakala, "Student dropout prediction using machine learning techniques," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 10, no. 4, pp. 408–414, 2022.
- [19] S. Ruiz-Villafranca, J. M. C. Gómez, and J. Roldán-Gómez, "A forensic tool for the identification, acquisition and analysis of sources of evidence in IoT investigations," *Internet of Things (Netherlands)*, vol. 27, p. 101308, Oct. 2024, doi: 10.1016/j.iot.2024.101308.
- [20] R. A. Awad, S. Beztchi, J. M. Smith, B. Lyles, and S. Prowell, "Tools, techniques, and methodologies: A survey of digital forensics for SCADA systems," *ACM International Conference Proceeding Series*, pp. 1–8, 2018.
- [21] P. Eden *et al.*, "A cyber forensic taxonomy for SCADA systems in critical infrastructure," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9578, pp. 27–39, 2016, doi: 10.1007/978-3-319-33331-1\_3.
- [22] E. Kurkowski and S. Sheno, *Advances in digital forensics XX*, vol. 724. Cham: Springer Nature Switzerland, 2024.
- [23] H. Dubey and S. Bhatt, "Comparative analysis of Autopsy and WinHex tools on data acquisition method," *International Journal of Information Privacy, Security and Integrity*, vol. 5, no. 3, pp. 200–210, 2023, doi: 10.1504/IJIPSI.2023.131545.
- [24] H. Dubey, S. Bhatt, and L. Negi, "Digital forensics techniques and trends: a review," *International Arab Journal of Information Technology*, vol. 20, no. 4, pp. 644–654, 2023, doi: 10.34028/iajit/20/4/11.
- [25] S. Vömel and J. Stüttgen, "An evaluation platform for forensic memory acquisition software," *Digital Investigation*, vol. 10, pp. S30–S40, Aug. 2013, doi: 10.1016/j.diin.2013.06.004.
- [26] R. Shree, A. Kant Shukla, R. Prakash Pandey, V. Shukla, and D. Bajpai, "Memory forensic: Acquisition and analysis mechanism for operating systems," *Materials Today: Proceedings*, vol. 51, pp. 254–260, 2022, doi: 10.1016/j.matpr.2021.05.270.






**BIOGRAPHIES OF AUTHORS**

**Srinivas Kanakala**    is working as senior assistant professor, Department of CSE, VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad. He completed Ph.D. from Osmania University, Hyderabad in the year 2018 and has 19 years of academic and research experience. Prior to PhD, he had earned M.Tech in CSE from JNTUH in the year 2008 and B.Tech in computer science and information technology from JNTUH in the year 2004. His research interests include developing algorithms and models for building systems and applications in areas of data mining, machine learning, deep learning and big-data analytics. He has around 40 publications, in various international journals and conferences. He can be contacted at email: [srinivaskanakala@gmail.com](mailto:srinivaskanakala@gmail.com).



**Vempaty Prashanthi**    is working as associate professor, Department of IT, CBIT, Hyderabad. She completed Ph.D. from JNTU, Hyderabad in the year 2020 and has 18 years of academic and research experience. Her Ph.D. work was on Network Coding Aware Routing Techniques in Mobile Ad hoc Networks. Prior to PhD, she had earned M. Tech in CSE from JNTUH in the year 2010 and B. Tech in Computer Science and Information Technology from JNTUH in the year 2005. Dr. V. Prashanthi's research interests include cyber security, forensics, developing algorithms and models for building systems and applications in areas of data mining, machine learning and big-data analytics. She has around 30 publications, in various journals and conferences. She can be contacted at email: [prashuvempaty@gmail.com](mailto:prashuvempaty@gmail.com).



**K. V. Sharada**    is working as an assistant professor in KL University Hyderabad, and have more than thirteen years' experience in teaching and Industrial. She has completed her B.Tech in Computer Science and Engineering from JNTU Hyderabad, M.Tech in Computer Science and Engineering from JNTU Hyderabad with distinction. She is pursuing Ph.D in Computer Science and Engineering at KLEF deemed University Hyderabad. She has started research in data science domain. Her research works in presented in more than 2+ international/national conferences. She is also member of ACM. Her area of interest is data science, NLP and deep learning. She can be contacted at email: [kvadlasharada@gmail.com](mailto:kvadlasharada@gmail.com).