INDEX

ABSTRACT

In the evolving landscape of cybercrime and digital evidence, the need for reliable, tamper-proof, and automated forensic tools has become more critical than ever. Traditional digital forensic methods often rely on tools that must be installed on the suspect's machine or depend heavily on manual operation, introducing the risk of evidence contamination and data modification. These approaches are not only time-consuming but also jeopardize the integrity and admissibility of digital evidence in legal proceedings.

To address these limitations, we introduce **XtracTorq**, an innovative digital forensic evidence extractor designed to revolutionize how evidence is collected and preserved. Unlike conventional tools, XtracTorq is deployed through a **WORM (Write Once Read Many) USB drive**, ensuring that once written, the contents of the tool cannot be altered. This guarantees zero tampering, absolute integrity, and legal soundness of the tool's operations—qualities essential in digital forensics. The WORM USB mechanism also prevents malware or malicious tampering of the tool after deployment, making it highly reliable for field operations.

XtracTorq operates with a plug-and-play architecture that automates the entire process of data extraction, eliminating the need for human intervention during the most critical stages of evidence collection. It is capable of extracting system logs, registry data, browser artifacts, USB histories, recent file activity, and more—without leaving a digital footprint on the host system. The tool also utilizes cryptographic hashing (SHA-256) to verify the integrity of each extracted file and encrypts all collected data before securely storing it back onto the USB device.

Another distinguishing factor of XtracTorq is its modular design. The tool is equipped with multiple extraction modules that can be customized or expanded based on specific investigation requirements. It also generates a comprehensive, court-admissible forensic report, providing investigators with an easy-to-interpret summary of all findings, complete with timestamps and hash validations.

Designed with input from law enforcement and cybersecurity professionals, XtracTorq provides a robust, field-ready solution for digital investigations. Whether in the context of cybercrime analysis, insider threat detection, incident response, or digital fraud investigation, XtracTorq offers a modern, automated, and trustworthy approach to digital evidence acquisition.

With its emphasis on automation, security, **WORM-based integrity**, and legal compliance, XtracTorq represents a significant leap forward in the field of digital forensics—transforming tedious, error-prone forensic procedures into streamlined, foolproof processes that investigators can trust.

INTRODUCTION

The exponential growth of digital technologies has transformed the way we communicate, work, transact, and even commit crimes. With the surge of internet-connected devices, remote systems, and digital transactions, cybercrime has evolved into a global threat affecting individuals, corporations, and governments alike. From ransomware attacks and insider threats to intellectual property theft and data breaches, the digital domain has become a battlefield where evidence is virtual, and time is of the essence.

In this fast-paced environment, digital forensics plays a critical role. It provides investigators with the ability to trace criminal activity, recover deleted or hidden data, and build a timeline of actions taken on digital devices. Whether it's uncovering the source of a breach, analyzing employee misconduct, or gathering evidence for prosecution, digital forensic tools are the backbone of cyber investigations.

However, despite their importance, traditional forensic tools come with a multitude of limitations. Most require prior installation on the target system—an act that inherently violates the cardinal principle of digital forensics: "Do not alter the original evidence." Others operate in live environments that are vulnerable to anti-forensic techniques, malware, or even simple misconfigurations that can corrupt the investigation. Furthermore, these tools often demand deep technical knowledge, making them inaccessible for first responders, HR professionals, or smaller investigative teams lacking specialized skills.

XtracTorq was born out of this very gap. It is not just another forensic tool—it is a paradigm shift in how digital evidence is extracted and secured. Built with a forensics-first approach, XtracTorq operates independently from the target system by booting from a WORM (Write Once Read Many) USB device. This hardware-backed constraint ensures that once the tool is written to the USB, it cannot be modified or infected—making it immune to tampering, backdoors, or post-deployment corruption.

Unlike traditional live forensic environments that operate from mutable USBs or system installs, XtracTorq offers a trusted, immutable launchpad. The use of WORM USBs not only preserves the authenticity of the forensic toolkit but also guarantees that all data extracted is stored in a write-once format—securing the chain of custody and meeting legal evidentiary standards.

Beyond its trusted deployment model, XtracTorq excels in its **automation, portability, and coverage**. It does not require user configuration or execution of multiple commands. **Once plugged into a system and booted, it silently begins extracting digital footprints: from system logs, registry keys, and browser activities, to connected USB histories and document metadata. The findings are hashed with cryptographic integrity checks, encrypted using AES-256, and compiled into structured reports for court admissibility.**

Moreover, XtracTorq is designed with future extensibility in mind. It supports modular plugins, allowing new forensic modules to be developed and frozen into future WORM builds, ensuring the tool evolves with the threats it aims to investigate.

As digital crime continues to grow in volume and sophistication, the tools used to combat it must be equally resilient, trustworthy, and efficient. XtracTorq represents the next generation of digital forensic automation—a tool designed not just to function, but to inspire confidence, maintain legal standards, and empower even non-technical personnel to act swiftly and securely when time and truth are critical.

PROBLEM STATEMENT

In the high-stakes world of cybercrime investigations, time, accuracy, and evidence integrity are the pillars upon which justice is built. Yet, ironically, many of the digital forensic tools currently in use pose a risk to the very evidence they are meant to protect. The core problem? Most forensic tools alter the system they're analyzing.

When investigators use traditional software-based tools, they often must install or execute programs directly on the suspect machine. This action—however necessary—immediately changes the state of the system, potentially overwriting or modifying crucial evidence like temporary files, timestamps, logs, or registry entries. In a courtroom, even a single byte of change can lead to the dismissal of evidence on grounds of contamination.

Further complicating matters is the lack of automation in existing forensic solutions. Analysts are often required to manually identify relevant files, sift through logs, and selectively extract artifacts—a tedious process prone to human error, oversight, and inconsistency. This not only slows down investigations but makes them heavily dependent on the skill of the operator.

Additionally, most commercial forensic suites come with steep learning curves and prohibitively expensive licensing models. Open-source alternatives, while powerful, frequently lack integration, automation, or security against tampering. In an environment where investigators must often work under pressure—with minimal time and maximum risk—these shortcomings are unacceptable.

There is also the looming threat of anti-forensic techniques. Malware, rootkits, and system-level protections can detect and disrupt forensic tools during operation. If the forensic tool is not isolated and secure, it may be sabotaged before completing its task. This is particularly dangerous when the tool is executed from a traditional USB, which is vulnerable to being modified before or during an investigation.

To sum up, the primary pain points faced by digital forensic investigators today include:

- Risk of evidence modification due to tool installation or execution on live systems.
- Manual, error-prone evidence extraction processes that require expert involvement.
- Lack of tool integrity and trust, especially in field environments.
- High costs and complexity associated with traditional solutions.
- Vulnerability to tampering and anti-forensic techniques.

These challenges create an urgent need for a secure, portable, automated, and tamper-proof forensic extraction tool that can be deployed quickly, used by both experts and non-experts, and preserve the sanctity of digital evidence. This is the precise problem space that XtracTorq addresses—with its revolutionary use of WORM USB deployment, automation-first design, and cryptographic integrity checks.

RESEARCH OBJECTIVE

The goal of digital forensics is not just to collect data—but to collect truth, in a way that is unquestionable, unaltered, and admissible in court. Yet, the existing ecosystem of tools and methodologies often falls short of this gold standard. With increasing pressure on investigators to act swiftly, accurately, and discreetly, there is an urgent need for a next-gen solution that redefines the foundation of digital evidence acquisition.

The primary objective of this research is to conceptualize, design, and develop XtracTorq—a futuristic digital forensic extraction tool that operates with zero trust on the host system and delivers maximum trust in its output.

Unlike traditional tools that rely on reactive workflows, the vision for XtracTorq is proactive, automated, and resilient, built to withstand the dynamic challenges of live investigations, system volatility, and anti-forensic threats.

Specifically, this project aims to:

1. Establish a non-intrusive forensic environment by utilizing WORM (Write Once Read Many) USB drives that prevent any post-deployment modifications, thereby ensuring the tool's credibility and security from tampering or malware infections.
2. Automate the end-to-end extraction process of critical forensic artifacts—such as system logs, browser caches, registry hives, user activity trails, USB histories, and metadata—without user input or manual configuration.
3. Enforce data integrity through the implementation of SHA-256 cryptographic hashing, allowing for real-time verification of every extracted file and creating a trusted audit trail.
4. Secure all acquired data using AES-256 encryption before writing it back to a separate, secure section of the WORM device, maintaining the chain of custody and confidentiality throughout the process.
5. Design a modular and extensible architecture that allows for the integration of future plugins—such as volatile memory capture, AI-assisted anomaly detection, keyword search engines, or dark web indicators—making XtracTorq a platform rather than just a tool.
6. Deliver cross-platform operability, with the ability to function seamlessly across modern Windows and Linux systems, ensuring broader applicability in diverse digital environments.
7. Generate comprehensive, legally admissible forensic reports in human-readable and machine-verifiable formats (PDF, HTML, JSON), complete with timestamps, hash logs, and extraction summaries.
8. Minimize the technical threshold so that first responders, corporate analysts, or even HR/security personnel can operate XtracTorq effectively without needing expert-level forensic knowledge.

Ultimately, the objective is not just to build another forensic tool—but to set a new benchmark for secure, autonomous, and tamper-proof digital evidence collection using hardware-level trust, intelligent software automation, and robust cryptographic integrity.

LITERATURE SURVEY

Digital forensics, as a multidisciplinary domain, has evolved significantly since its early adoption in law enforcement and cybersecurity investigations. Rooted in computer science, legal standards, and investigative practices, the field has been shaped by both academic research and policy-driven frameworks. The literature reflects a growing consensus on the need for automation, data integrity, tamper-resistance, and legal admissibility in forensic methodologies. However, despite these theoretical advances, the translation into field-ready, hardware-backed solutions remains limited.

Early foundational works in digital forensic science, such as those by Carrier and Spafford (2004), emphasized the importance of preserving the original state of digital evidence during collection and analysis. Their work formalized the Digital Evidence Collection Process, introducing models for chain of custody, data validation, and procedural integrity. They argued that any contamination or modification of evidence during acquisition could invalidate it in court, highlighting the need for non-invasive, reliable tools.

A parallel line of research has explored the role of automation and scripting in forensic workflows. Several studies have proposed frameworks for automating evidence extraction, metadata parsing, and report generation. These studies argue that manual processes introduce not only delays but also inconsistencies that may compromise investigations. However, most of these efforts have remained at the software layer, without exploring how automation can be fused with hardware-level trust mechanisms.

Cryptographic methods have also gained prominence in forensic literature. The use of hashing algorithms such as SHA-256 and MD5 for data integrity verification has been widely adopted as a standard practice. Research indicates that every stage of evidence collection and transfer must be accompanied by hash verification logs to ensure tamper-proof custody. However, very few studies explore how these cryptographic guarantees can be combined with immutable storage hardware, such as WORM (Write Once Read Many) devices, to elevate the trust boundary from software to physical media.

Another critical area highlighted in recent academic discourse is the risk posed by anti-forensic techniques—deliberate attempts by malicious actors to interfere with forensic tools, overwrite logs, or manipulate system states to obstruct investigations. Papers published in journals like Digital Investigation and IEEE have underscored the importance of trusted execution environments and hardware-based isolation to ensure the reliability of forensic operations in compromised systems.

The concept of "forensic soundness"—a term frequently revisited in modern literature—stresses that tools must not only gather evidence but do so in a way that ensures reproducibility, verifiability, and legal defensibility. This has led to increasing advocacy for forensic frameworks that can operate independently of the target system, without assuming trust in its operating environment.

Lastly, while the industry is gradually moving toward cloud-based forensics and AI-assisted analysis, researchers continue to caution against over-reliance on centralized infrastructure. Local, hardware-backed, and portable forensic tools remain essential, especially in environments where network access is restricted, cloud use is prohibited, or privacy concerns are paramount.

COMPARISION WITH EXISTING IMPLEMENTATION

The landscape of digital forensic tools is rich with well-established solutions such as Autopsy, FTK Imager, and the Volatility Framework. These tools have played a significant role in advancing forensic investigation methodologies. However, when critically examined through the lens of modern investigative demands—particularly automation, system non-intrusiveness, and tamper-proof evidence handling—each of these implementations reveals crucial limitations that XtracTorq directly addresses.

Autopsy, for instance, is a GUI-based forensic analysis tool built on top of The Sleuth Kit. It is widely used for parsing disk images, conducting keyword searches, timeline reconstruction, and file system analysis. While Autopsy offers a rich set of features, it is primarily designed for post-acquisition analysis. It requires the user to first obtain an image of the target drive using other tools, often necessitating installation and manual configuration. This makes it less effective in live acquisition scenarios and unsuitable in field conditions where time and technical constraints are a concern.

FTK Imager, developed by AccessData, is another notable tool used for imaging and previewing data from storage media. It supports disk cloning, file recovery, and integrity checks through hash values. However, FTK Imager is not fully automated and requires active user interaction at every step. It must also be executed from the host system, which introduces the possibility of altering timestamps, logs, or volatile memory—compromising evidence integrity.

The Volatility Framework, on the other hand, is a command-line tool specialized for memory forensics. It enables investigators to analyze RAM dumps for active processes, hidden malware, loaded DLLs, and more. While powerful in memory analysis, it is not intended for full-system evidence acquisition. Additionally, it requires technical expertise to use effectively and lacks an intuitive interface, making it impractical for first responders or non-expert personnel.

What sets **XtracTorq** apart from these tools is its zero-footprint architecture, hardware-backed integrity, and end-to-end automation. XtracTorq runs entirely from a WORM (Write Once Read Many) USB drive, eliminating the need for any installation or execution on the suspect system. This approach preserves the state of the system under investigation and prevents any unintended modifications, malware interference, or tampering.

Moreover, unlike traditional tools that rely on operator judgment and manual input, XtracTorq is designed to automatically scan, extract, hash, encrypt, and report on forensic artifacts without user intervention. It collects logs, registry data, browser histories, USB device trails, and more—encrypts them using AES-256, and stores them back onto a secure partition of the WORM USB. This level of automation ensures consistency, saves time, and significantly reduces human error.

Additionally, XtracTorq includes built-in SHA-256 hash verification for all extracted data, ensuring the forensic chain of custody is preserved. It also supports modular plugin extensions, making it future-ready and customizable for specific investigative needs—something that is often rigid or limited in other tools.

In essence, while tools like Autopsy, FTK Imager, and Volatility serve important forensic functions, they each rely on environments that assume trust in the host system or the operator. XtracTorq breaks from this assumption by anchoring its trust model in hardware-level immutability, full automation, and cryptographic rigor, making it a uniquely powerful solution for modern digital forensic investigations.

IMPLEMENTATION / METHODOLOGY

The development of XtracTorq is grounded in a multi-layered architectural approach that integrates hardware-backed security, automated evidence acquisition, cryptographic assurance, and modular extensibility. The tool is designed to function as a plug-and-play forensic suite, capable of operating independently of the host system, with no reliance on pre-installed software or user interaction.

At the heart of XtracTorq is its deployment mechanism via a WORM (Write Once Read Many) USB device. This hardware choice is fundamental to the tool's methodology, ensuring that the software environment is immutable after creation. The WORM USB prevents any modification, infection, or tampering of the tool, even if the target system is compromised. This creates a trusted, verifiable launchpad from which forensic operations are conducted.

4.1 System Architecture Overview

XtracTorq is structured into five key layers:

1. Boot Environment Layer

Upon insertion into a target system, the WORM USB boots into a lightweight, isolated Linux-based environment. This live OS is read-only and includes all necessary drivers and scripts required for data acquisition. It ensures that the host operating system is never loaded or interacted with, thus preserving the volatile state of the machine and minimizing the digital footprint.

2. Automation & Execution Layer

Once booted, XtracTorq automatically initiates its evidence extraction sequence without requiring user input. All modules are triggered through shell scripts or Python automation wrappers. This layer scans the target system for predefined forensic artifacts, using file system traversal, registry parsing, and log collection mechanisms. The goal is to minimize human intervention and eliminate potential errors during critical phases of evidence gathering.

3. Forensic Data Collection Modules

The core functionality is delivered through dedicated extraction modules:

System Log Collector: Parses event logs, boot records, crash dumps, and OS alerts.

Registry Analyzer: Extracts installed software details, user activity logs, and configuration hives.

Browser Artifact Scanner: Captures cookies, browsing history, saved credentials, and cache files.

USB Forensics Module: Retrieves metadata about connected devices, including timestamps, serial numbers, and usage frequency.

User Activity Tracker: Scans recent files, open document records, session logs, and clipboard contents. Each module operates in an isolated sandbox and writes data into a protected staging directory within the secure partition of the USB.

4. Data Integrity & Security Layer

Every file and artifact extracted by XtracTorq is passed through a SHA-256 hashing algorithm, and the hash values are logged for validation. These logs ensure that the extracted data remains unchanged from the moment of acquisition to the time of presentation in a forensic report. Following hashing, the data is encrypted using AES-256 encryption standards and securely written into the WORM device's encrypted storage partition. The tool is also equipped to generate signed hash chains for audit trails and evidence chain-of-custody verification.

5. Report Generation Layer

After the extraction and encryption processes, XtracTorq compiles a detailed forensic report. This report includes metadata of all extracted files, timestamped activity logs, hash value mappings, and a list of modules triggered during the operation. Reports are generated in multiple formats (PDF, HTML, and optionally JSON) to ensure compatibility with both legal and technical review processes.

4.2 Workflow Summary

The tool's operation follows a streamlined, seven-step methodology:

1. Insert WORM USB into target machine.

2. Boot system from USB into the pre-installed live forensic OS.

3. Auto-trigger forensic modules, each executing silently in the background.

4. Extract and stage artifacts to a secure area within USB.

5. Hash and encrypt data, logging each operation for verification.

6. Generate reports with all findings and integrity checks.

7. Power down safely—leaving zero footprint on the target system.

4.3 Modularity and Extensibility

XtracTorq's architecture is designed for modular growth. Each forensic operation is implemented as a discrete module, allowing new capabilities to be added without reengineering the core system. Future modules may include:

- RAM snapshot acquisition
- AI-powered anomaly detection
- Keyword-based content filtering
- Image forensics and steganalysis
- Network session reconstruction

Because of the WORM medium, any new modules must be finalized and frozen into a new USB build, reinforcing the integrity of each deployment cycle.

RESULTS & DISCUSSION

The development of XtracTorq culminated in a series of structured tests to validate its performance, reliability, forensic integrity, and real-world applicability. The evaluation was conducted across diverse Windows-based environments to simulate field scenarios and ensure that the tool behaves consistently across modern systems.

5.1 Test Environment and Setup

Target Operating Systems: Windows 10 (Pro & Home editions), Windows 11

Hardware Platforms:

System A: Intel Core i5, 8 GB RAM, 256 GB SSD
System B: AMD Ryzen 5, 16 GB RAM, 1 TB HDD

Deployment Medium: 64 GB WORM (Write Once Read Many) USB drive
Data Conditions: Each system was preloaded with synthetic user data including browsing history, registry changes, connected USB logs, and recent document activities

Evaluation Metrics:

- Extraction success rate
- Execution time
- Footprint on target system
- Accuracy of hashing
- Report completeness and readability

5.2 Key Results

1. **Zero Footprint Operation**

On both Windows 10 and Windows 11 systems, XtracTorq successfully operated without leaving any trace or altering the system state. After booting through the WORM USB into the forensic live OS, the tool bypassed the host OS entirely. Post-operation scans using SHA-256 baseline comparison confirmed zero modification to the target system's file structure or registry values—affirming XtracTorq's forensic non-intrusiveness.

2. **Successful Artifact Extraction**

The tool consistently extracted the following data with a 100% success rate:

- System logs (event viewer data, boot logs)
- Registry hives (NTUSER.DAT, SOFTWARE, SYSTEM)
- Browser artifacts (Chrome, Edge—history, cookies, bookmarks)
- Connected USB metadata
- Recent document history and user shellbag analysis

- All data was organized in a structured folder hierarchy and encrypted immediately post-extraction.

3. Hash Verification and Integrity

Each artifact was hashed using SHA-256 at the time of acquisition. These hash values were logged and embedded within the final forensic report. Independent rehashing of files using external tools confirmed 100% consistency, proving that the data was neither modified during extraction nor compromised in storage.

4. Execution Time Efficiency

System A (SSD): Full scan and report in 3 minutes 52 seconds
System B (HDD): Full scan and report in 6 minutes 14 seconds

This makes XtracTorq significantly faster than traditional manual workflows that may take 20–40 minutes, depending on the investigator's expertise and number of tools used.

5.2 Report Quality and Clarity

The generated forensic reports were clear, timestamped, and legally structured. Each section (System Info, User Activity, Browser Logs, USB Events, Hash Map) was indexed and referenced, making the report suitable for direct submission to investigative or legal entities.

5.3 Discussion

The results affirm that XtracTorq is not just a proof of concept but a viable, field-ready solution for forensic professionals. Its ability to perform live evidence extraction without compromising the integrity or admissibility of data marks a significant advancement over many existing solutions. The use of WORM USB for deployment ensured trust at the hardware level, and the automation pipeline eliminated the risk of human error.

Moreover, the tool's consistent performance across both Windows 10 and 11 highlights its relevance for current enterprise and consumer environments. Investigators can now rely on a forensic suite that works reliably across multiple system builds without additional configuration.

CONCLUSION & FUTURE SCOPE

Digital investigations demand tools that are not only technically powerful but also legally defensible, user-friendly, and resilient to the unpredictable environments in which they operate. XtracTorq was developed to answer this demand with a forward-thinking design centered on security, automation, integrity, and trust.

The tool's architecture—built around WORM (Write Once Read Many) USB deployment—ensures that it operates in an immutable, tamper-proof environment, establishing trust before any interaction with the target system occurs. Its zero-footprint approach prevents contamination of evidence, a common concern with traditional system-resident tools. By booting into a live forensic OS and automating the full cycle of evidence extraction, hashing, encryption, and reporting, XtracTorq minimizes human error while maximizing efficiency and consistency.

Test results on Windows 10 and 11 confirmed the tool's reliability, speed, and forensic soundness. It successfully acquired a wide range of digital artifacts without altering the host system, and its reports—complete with hash validation—provide investigators with ready-to-use, court-admissible documentation.

While XtracTorq already offers significant advancements over existing implementations, its architecture is deliberately designed to support further evolution. The modular plugin system allows developers and forensic teams to add new capabilities tailored to emerging threats, investigative needs, or platform compatibility.

Future Scope

To continue evolving and increasing its utility in broader forensic contexts, the following future enhancements are planned:

1. **RAM Dumping & Volatile Memory Analysis**

Adding modules for capturing and analyzing live RAM snapshots to detect in-memory malware, process trees, and running services.

2. **AI-Driven Anomaly Detection**

Integrating lightweight machine learning models to flag suspicious behavior patterns, rare system events, or abnormal user activity.

3. **Cross-Platform Compatibility**

Expanding support for macOS and Linux-based systems to make XtracTorq a universal solution for multi-environment digital investigations.

4. **Cloud Forensics Module**

Introducing secure modules to extract browser-synced cloud data (Google Drive, OneDrive history, etc.) for digital footprint analysis.

5. **Blockchain-Based Integrity Logs**

Leveraging blockchain to record hash chains and event logs for enhanced tamper-evidence and decentralized audit trails.

6. **Real-Time Investigator Dashboard**

A GUI-based live monitoring interface where forensic operators can view progress, access real-time logs, and flag findings as they emerge.

7. **Multi-User Role Access**

Enabling administrative and observer roles to allow collaborative investigations with restricted permissions and report visibility levels.

In conclusion, XtracTorq is not just a forensic tool—it is a platform: one that can scale with evolving technology, adapt to investigative complexities, and uphold the strictest standards of digital evidence integrity. It empowers professionals with a faster, more reliable, and more secure way to uncover the truth in the digital domain.

REFERENCES

1. **XtracTorq Portfolio Website Page**
https://raj-two.vercel.app/project5.html
2. **XtracTorq Project Insight Webpage**
https://raj-two.vercel.app/XtracTorq.pdf
3. **XtracTorq GitHub Repository**
https://github.com/Raj010505/XtracTorq
4. Carrier, B., & Spafford, E. H. (2004). Getting Physical with the Digital Investigation Process. International Journal of Digital Evidence, 2(2), 1–20.
5. Garfinkel, S. L. (2010). Digital Forensics Research: The Next 10 Years. Digital Investigation, 7, S64–S73.
6. National Institute of Standards and Technology (NIST). Computer Forensics Tool Testing (CFTT) Program. Available at: https://cftt.nist.gov/
7. Ayers, D., Brothers, S., & Jansen, W. (2007). Guidelines on Cell Phone Forensics. NIST Special Publication 800-101.
8. Cohen, M. I., Bilby, D., & Caronni, G. (2011). Distributed Forensics and Incident Response in the Enterprise. Digital Investigation, 8, S101–S110.
9. Rogers, M. K., & Seigfried, K. (2004). The Future of Computer Forensics: A Needs Analysis Survey. Computers & Security, 23(1), 12–16.
10. Volatility Foundation. The Volatility Framework. Available at: https://www.volatilityfoundation.org/
11. The Sleuth Kit & Autopsy Documentation. Available at: https://www.sleuthkit.org/
12. NIST Special Publication 800-88 Rev.1. Guidelines for Media Sanitization.
13. Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current Challenges and Future Research Areas for Digital Forensic Investigation. The Computer Journal, 59(11), 1611–1631.