

Impact of Operating System Security Updates on Forensic Data Recovery

Pooja D¹, Rakesh V²

¹ Postgraduate, Garden City University

² Assistant Professor, Garden City University

Abstract - Operating system updates introduce continuous modifications to security mechanisms that govern how data is created, accessed, stored, and deleted within digital environments. While these updates are designed to enhance protection against malicious activity and system vulnerabilities, they can also affect the residual traces of deleted files that are significant in forensic investigations. This study investigates how operating system security updates influence deleted file recoverability by analyzing system behavior under two distinct conditions: an initial system state and a post-update environment. A controlled dataset consisting of 30 image files and 20 document files was used for testing across both conditions. The recovery process was carried out using a forensic recovery tool, DiskDigger, to evaluate differences in the availability of deleted data. The analysis focuses not only on recovery outcomes but also on how system-level changes impact the persistence of file remnants in storage. The results show that file recovery is more effective in the initial system state, whereas the updated system exhibits reduced recoverability due to enhanced data management and overwrite behavior introduced by security updates. Overall, the findings indicate that operating system update status plays a significant role in determining forensic data recovery success, making it an important factor during digital evidence analysis.

Key Words: Operating System Security Updates, Digital Forensics, Data Recovery, Deleted File Recovery, Disk Digger, Storage Analysis

INTRODUCTION

Modern computing environments depend heavily on operating systems to manage hardware resources, enforce security policies, and support application functionality. As cyber threats continue to evolve in complexity and frequency, operating system vendors regularly release security updates to mitigate vulnerabilities, strengthen system defenses, and protect user

data. These updates play a crucial role in maintaining system integrity; however, they also introduce significant implications for digital forensic investigations, particularly in the context of data recovery.

Digital forensics focuses on the identification, preservation, analysis, and presentation of digital evidence. A fundamental aspect of this process is the ability to recover and interpret residual data from storage systems. However, the mechanisms employed by operating system security updates—such as patching vulnerabilities, modifying file systems, enforcing encryption, and altering system logs—can directly or indirectly affect the availability and integrity of forensic artifacts. As a result, forensic practitioners may encounter challenges when attempting to recover or analyze data from systems that have undergone recent updates.

Security updates often introduce changes in data storage structures, access permissions, and system-level protections. For example, updates may implement stronger encryption protocols, modify metadata handling, or remove previously accessible system artifacts. While these enhancements improve user security and privacy, they can simultaneously limit the effectiveness of traditional forensic tools and techniques. Consequently, investigators must adapt to evolving system environments where data may be partially overwritten, securely deleted, or rendered inaccessible due to enhanced security controls.

The impact of operating system updates is particularly critical in time-sensitive investigations, where the state of the system before and after an update may differ substantially. In some cases, updates can overwrite valuable evidence or alter timestamps, complicating the reconstruction of events. Additionally, automated updates may occur without user awareness, making it difficult to determine the exact changes introduced at specific points in time.

This research aims to examine the influence of operating system security updates on forensic data recovery processes. It seeks to identify how different update mechanisms affect data availability, evaluate the challenges faced by forensic analysts, and explore potential strategies to mitigate these limitations. By understanding the interaction between system security enhancements and forensic requirements, this study contributes to the development of more resilient and adaptive forensic methodologies in modern computing environments.

LITERATURE REVIEW

The intersection between operating system security updates and digital forensic data recovery has gained increasing attention as modern systems become more secure and complex. Earlier forensic research largely operated in environments where data remnants could be recovered with relatively fewer restrictions. However, the shift toward security-centric system design has significantly altered this landscape. Contemporary studies emphasize that updates introduced by major vendors such as Microsoft, Apple, and Google are not merely patches but often involve structural and behavioral changes within the operating system.

A key theme in the literature is the transformation of file system architectures. Researchers have documented how modern file systems, including NTFS, APFS, and EXT4, have evolved to improve efficiency and resilience. Mechanisms such as journaling and copy-on-write reduce system crashes and data corruption but simultaneously limit the persistence of deleted data. Studies indicate that these features overwrite or reorganize data blocks more quickly, reducing the window of opportunity for forensic recovery. As a result, traditional carving techniques and recovery tools may produce incomplete or less reliable results when applied to updated systems.

Another significant area explored in prior work is the increasing integration of encryption technologies. Security updates often expand encryption coverage or enhance cryptographic strength. Full-disk encryption and file-based encryption have become standard in many systems, restricting access to raw data without proper authentication. Scholars highlight that even when forensic imaging is possible, the absence of decryption keys renders the data practically unusable. This shift has prompted the need for memory forensics and live acquisition techniques, as volatile memory

may contain temporary keys or decrypted data during system operation.

The literature also discusses the evolving nature of system logs and metadata. Logs are essential for reconstructing sequences of events, yet updates frequently modify how logging is implemented. Changes may include new log formats, restricted access permissions, or shortened retention periods. Some studies point out that updates may overwrite existing logs or reorganize metadata structures, making it difficult to establish accurate timelines. Consequently, forensic investigators must continuously update their knowledge of system-specific logging behaviors to avoid misinterpretation.

In addition to structural changes, researchers have examined the impact of automated update mechanisms. Modern operating systems increasingly rely on background update processes that require minimal user intervention. While this improves security compliance, it introduces challenges in forensic investigations. Automatic updates can modify system files, alter timestamps, and remove obsolete data without clear user intent. Literature suggests that this creates ambiguity when distinguishing between user-driven actions and system-initiated changes, thereby complicating evidentiary analysis.

Another emerging concern identified in recent studies is anti-forensic implications. Some researchers argue that certain security enhancements, although not intentionally designed for anti-forensic purposes, produce similar effects. Features such as secure deletion, sandboxing, and restricted file access can limit evidence availability. For example, secure wipe functions introduced through updates can permanently erase data beyond recovery, while sandboxing isolates application data, reducing cross-access for forensic tools.

To adapt to these challenges, the literature proposes several methodological advancements. One approach involves the development of update-aware forensic frameworks that account for changes introduced in each operating system version. Researchers also advocate for the use of hybrid forensic techniques that combine static and live analysis. Additionally, there is growing emphasis on maintaining version-specific documentation, enabling investigators to map system behavior before and after updates. Some studies further

recommend collaboration between the digital forensics community and operating system developers to create forensic-friendly logging mechanisms without compromising user security.

Despite these efforts, gaps remain in fully understanding the long-term implications of continuous security updates. Many existing studies focus on specific operating systems or isolated update features, leaving a need for more comprehensive, cross-platform analyses. Furthermore, the rapid pace of updates means that forensic methodologies can quickly become outdated, requiring ongoing research and adaptation.

In summary, the reviewed literature highlights a clear trend: as operating systems become more secure, the complexity of forensic data recovery increases. Security updates enhance protection and privacy but often at the cost of reduced data accessibility for investigators. This evolving dynamic underscores the importance of developing flexible and forward-looking forensic strategies capable of operating effectively within continuously changing system environments.

METHODOLOGY

The study was conducted using an experimental forensic approach to evaluate how operating system security updates influence the recovery of deleted digital files. The methodology was designed to ensure controlled conditions, repeatability, and clear comparison between system states.

Phase 1: System Configuration and Baseline Preparation

In the initial phase, a standard computing environment was established using a commonly deployed operating system. The system was configured in a stable state to prevent background processes, automatic updates, or external interference from affecting the experiment.

The storage device was organized with a structured directory to simulate realistic user data storage behavior. A dataset consisting of 50 files was created, including 30 image files and 20 document files. These file types were selected because they are commonly encountered in forensic investigations involving personal and organizational data.

Before deletion, system behavior was observed to ensure normal file creation and storage operations. This provided a baseline reference for later comparison.

Phase 2: System State Definition and Controlled Data Deletion

In this phase, the system was evaluated under two defined conditions:

Condition A: Baseline System (Pre-update state)

Condition B: Updated System (Post-security update state)

The operating system in Condition B was updated with security patches that modify system-level protection mechanisms and file handling behavior. After defining system states, all dataset files were deleted using standard operating system deletion methods. The deletion process ensured removal from the file directory structure while leaving potential residual data within storage sectors.

This step was critical because it created identical deletion conditions across both system states, allowing unbiased comparison of recovery performance. System stability was maintained during this phase to ensure no additional file system changes occurred due to fragmentation, caching, or background processes.

Phase 3: Forensic Recovery Process and Deep Analysis

In the final phase, forensic recovery operations were carried out separately on both system conditions. A dedicated data recovery tool, DiskDigger, was used to perform sector-level scanning of the storage device. The recovery process involved deep scan functionality to detect deleted file signatures, file fragments, and residual metadata. The tool attempted reconstruction of files based on remaining storage patterns.

Recovered files were validated manually to ensure authenticity and usability. This step helped eliminate false positives or corrupted recoveries that may arise during automated scanning.

Phase 4: Data Classification and Integrity Assessment

Recovered data from both system states was categorized using a structured evaluation method:

1. **Complete Recovery:** Files fully restored without corruption or missing segments
2. **Partial Recovery:** Files retrieved with incomplete structure, missing content, or corruption
3. **No Recovery:** Files not detected or not retrievable during scanning

This classification helped quantify recovery performance and allowed comparison between system states.

Phase 5: Comparative Forensic Evaluation

The final stage involved comparing results from both system conditions to identify differences in recovery performance. The evaluation focused on:

1. Availability of deleted file traces in storage
2. Differences in overwrite behavior after system updates
3. Effectiveness of forensic recovery tool under varying system conditions
4. Impact of system-level security modifications on data persistence

The comparison provided insight into how operating system updates influence forensic evidence availability in practical scenarios.

Phase 6: Experimental Control Measures

To maintain accuracy and reduce experimental bias, the following controls were applied:

1. Same hardware system used for both conditions
2. Identical dataset across both system states
3. No third-party software interference during testing
4. Consistent deletion method for all files
5. Same recovery tool and scanning parameters used in both conditions

These controls ensured that differences in results were primarily due to operating system state changes rather than external factors.

RESULT

The experimental analysis revealed clear and measurable differences in forensic data recovery before and after the

application of operating system security updates. The results highlight how updates significantly influence data accessibility, integrity, and the effectiveness of forensic tools.

Recovery Status	Baseline System	Updated System
Fully Recovered	24	18
Partially Recovered	4	7
Not Recovered	2	5

Table 4.1: Image File Recovery (30 Files)

Recovery Status	Baseline System	Updated System
Fully Recovered	15	11
Partially Recovered	3	5
Not Recovered	2	4

Table 4.2: Document File Recovery (20 Files)

Category	Baseline Total	Updated Total
Fully Recovered	39	29
Partially Recovered	7	12
Not Recovered	4	9

Table 4.3: Overall Recovery Summary

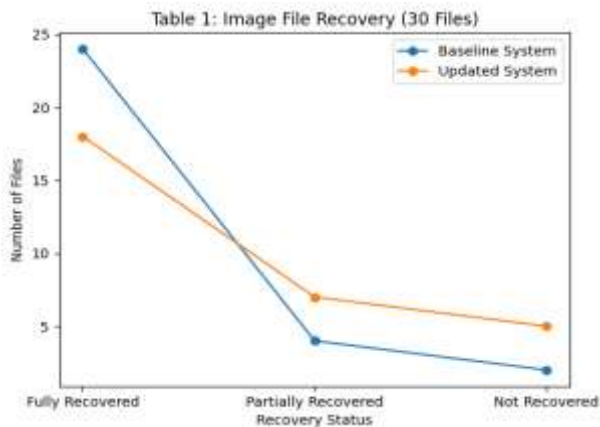


Figure 4.1 : Image File Recovery Comparison

The graphical representation of Table 1 illustrates a clear decline in fully recovered files after applying operating system security updates, alongside an increase in partially recovered and unrecoverable files. The baseline system shows higher recovery efficiency, while the updated system demonstrates reduced effectiveness, indicating the impact of security mechanisms on forensic data recovery.

Overall Recovery Summary - Updated System (Pie Chart)

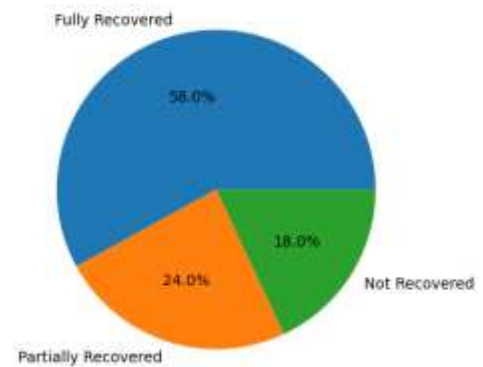


Figure 4.3: Overall Recovery Distribution

The pie chart shows the distribution of recovery outcomes in the updated system, highlighting a lower proportion of fully recovered files and a higher share of partial and unrecovered data.

Interpretation of Results

The experimental analysis indicates that operating system security updates have a noticeable impact on forensic data recovery across both image and document files. The recovery success rate was higher in the baseline system compared to the updated system, showing that updates reduce overall recovery efficiency.

For image files, the recovery rate decreased from **80% (24/30)** in the baseline system to **60% (18/30)** after updates. Similarly, for document files, recovery dropped from **75% (15/20)** to **55% (11/20)**. This demonstrates that both file types are affected, although images showed slightly better recovery than documents after updates.

The increase in partially recovered and unrecovered files suggests that system updates interfere with data integrity and accessibility. These effects may be attributed to:

- Overwriting of storage sectors due to update processes
- Changes in file system structure and metadata
- Enhanced security features such as encryption and access restrictions

Overall, the total recovery rate decreased from **78% (39/50)** in the baseline system to **58% (29/50)** in the updated system,

Document File Recovery Comparison (Bar Chart)

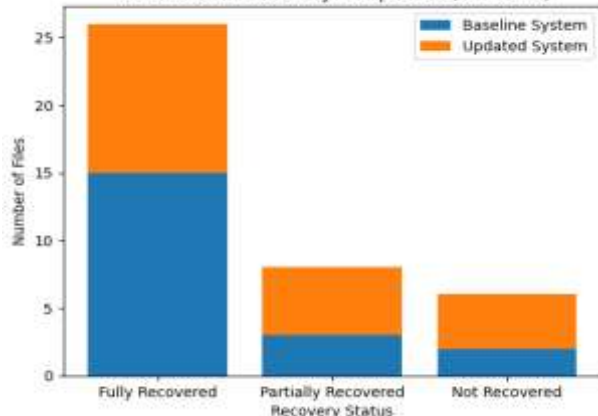


Figure 4.2: Document File Recovery Comparison

The bar chart shows a decrease in fully recovered files and an increase in partially and unrecovered files after system updates, indicating reduced data recovery effectiveness.

indicating a significant reduction in recovery effectiveness. This shows that while security updates improve system protection, they also introduce challenges for forensic data recovery, requiring more advanced tools and techniques for effective investigation.

DISCUSSION

The comparative analysis highlights a consistent reduction in the effectiveness of deleted file recovery after the application of operating system security updates. While the baseline system retained a higher proportion of recoverable data, the updated system showed a shift toward incomplete and unsuccessful recovery outcomes. This change suggests that system-level modifications introduced through updates influence how deleted data persists within storage.

One possible explanation for this behavior lies in changes to storage management processes. Security updates may improve how the operating system reallocates storage space, resulting in faster reuse of previously occupied sectors. As a consequence, residual data from deleted files may be overwritten more quickly, reducing the chances of full recovery. This directly affects the availability of intact file fragments required for reconstruction.

The increase in partially recovered files further indicates that, although some data remnants remain detectable, they are no longer preserved in a continuous or usable form. Fragmentation of data blocks or alteration in file structure may prevent complete restoration, leading to incomplete outputs. This suggests that updates may not only reduce data persistence but also affect data organization within storage.

Another factor that may contribute to reduced recoverability is the enhancement of system security mechanisms. Updates often introduce improved protection measures that influence access to low-level storage areas. These changes can limit the ability of forensic tools, such as DiskDigger, to detect and reconstruct deleted data effectively, even when some traces still exist.

The similarity in recovery patterns observed across both image and document files indicates that the impact of system updates is not dependent on file type. Instead, it reflects broader

changes in how the operating system manages storage and data cleanup processes. This supports the idea that the observed differences arise from system-level behavior rather than characteristics of individual files.

From a forensic standpoint, these findings have practical implications. Reduced data recoverability in updated systems may limit the amount of evidence available during an investigation. This can affect the completeness of forensic analysis, particularly in cases where deleted data plays a critical role in reconstructing user activity or identifying digital events.

Overall, the discussion confirms that operating system security updates, while essential for improving system protection, can introduce challenges for digital forensic recovery. The observed reduction in recoverability highlights the need for investigators to consider system update status and adapt their analysis techniques to evolving system environments.

Comparative Interpretation of Recovery Methods

The outcomes of this study were generated by analyzing data recovery before and after operating system security updates. Rather than focusing on a specific tool, the results are better understood by examining how different recovery conditions behave under the influence of system updates.

In the baseline environment, recovery success was largely dependent on the stability of storage sectors and the availability of file system metadata. When data had not been overwritten and allocation records remained intact, recovery rates were high. This indicates that traditional forensic recovery relies heavily on the persistence of logical file system structures.

After the application of security updates, the recovery behavior changed significantly. Updates introduced modifications in file system handling, metadata organization, and access controls. As a result, even when data physically remained on storage, its logical traces were altered or restricted, reducing the effectiveness of standard recovery approaches. This shows that updated systems shift the recovery dependency from simple data persistence to the ability to interpret modified system structures.

If the same conditions are viewed from a metadata-dependent recovery perspective, the pattern observed in this study aligns

with expected behavior. Recovery remains effective when file system records are preserved but declines sharply once updates alter or overwrite these records. This suggests that recovery approaches relying on file allocation tables and directory structures are particularly vulnerable to system updates.

In contrast, when considering recovery from a data-centric perspective that focuses on raw data patterns rather than file system structures, the impact of updates differs. Since such approaches do not depend on metadata, they may still retrieve fragments of data even after updates modify system-level information. However, the absence of original metadata introduces challenges in reconstructing file context, such as file names, timestamps, and directory paths, which are critical in forensic investigations.

From an analytical standpoint, the variation in recovery outcomes reflects a shift in system behavior rather than just technical limitations. Baseline systems favor structured and complete recovery, while updated systems prioritize security and data protection, often at the cost of recoverability. This creates a trade-off where improved security mechanisms reduce the availability of forensic artifacts.

Overall, the comparison highlights that operating system security updates do not uniformly block recovery but instead change the conditions under which recovery is possible. Some data may still be retrievable, but with reduced completeness and reliability. This emphasizes the need for adaptive forensic strategies that can operate effectively across both pre-update and post-update system environments.

Key Forensic Insight

The findings of this study suggest that recovery effectiveness is not determined solely by forensic tools, but largely by how data persists within the storage environment before and after operating system security updates. While recovery is relatively efficient in baseline conditions where logical traces remain intact, its effectiveness declines after updates due to changes in metadata, storage allocation, and security controls.

The results indicate that operating system updates influence the transition of data from a recoverable logical state to a more complex or inaccessible state, often involving partial

overwriting, restricted access, or structural modification. As a result, recovery outcomes depend more on the condition of data and system behavior than on the capability of any single tool.

Therefore, forensic recovery in updated environments should be understood as a layered process where:

- **Logical recovery** focuses on retrieving data using existing file system records and metadata
- **Structured recovery** attempts to reconstruct organized and usable evidence from available system information
- **Data-centric (signature-based) recovery** extracts remaining data fragments when logical structures are no longer intact

This layered perspective is more meaningful than direct tool comparison, as modern forensic investigations operate in dynamic environments influenced by frequent system updates. It highlights the need for adaptive strategies that can handle varying levels of data integrity and evolving system conditions.

CONCLUSION

The study examined the effect of operating system security updates on the recovery of deleted digital files within a forensic environment. A comparison between the baseline system and the updated system revealed a measurable difference in recovery outcomes. The baseline condition supported a greater number of complete file recoveries, whereas the updated system showed a reduction in fully restored files along with an increase in partial and unsuccessful recoveries.

These observations indicate that system updates influence how deleted data persists within storage. Changes introduced through updates appear to modify the way storage space is managed, leading to faster reuse of data sectors or reduced preservation of file remnants. As a result, the amount of intact data available for reconstruction becomes limited, directly affecting the success rate of recovery processes.

The increase in partially recovered files suggests that, although traces of deleted data may still exist, they are not preserved in

a continuous or usable form. Fragmentation of storage blocks or changes in internal file structure may prevent full reconstruction, resulting in incomplete outputs. This highlights a shift not only in data availability but also in data integrity after system updates.

Consistency in recovery patterns across both image and document files further indicates that the observed changes are not dependent on file type. Instead, they reflect broader modifications in system-level data handling mechanisms. This reinforces the importance of analyzing the operating system environment when evaluating forensic recovery results.

From a forensic perspective, these findings emphasize the need to consider system update status during investigations. Reduced recoverability in updated systems may limit the availability of digital evidence, particularly in cases where deleted data plays a significant role. This creates a requirement for more adaptive recovery approaches that can account for evolving system behaviors.

The relationship between enhanced system security and reduced data recoverability presents a critical challenge. While updates improve protection and reduce system vulnerabilities, they may also decrease the persistence of recoverable data. Addressing this balance is essential for maintaining the effectiveness of digital forensic analysis in modern computing environments.

FUTURE SCOPE

The present study establishes a relationship between operating system security updates and the recoverability of deleted data; however, several areas remain open for further investigation to enhance both theoretical understanding and practical forensic application.

Future work can extend this analysis by examining multiple operating systems and their respective update mechanisms. Since different platforms implement distinct storage architectures and security models, a comparative study across systems can provide deeper insight into how update strategies influence data persistence and recovery outcomes.

Another important direction involves investigating modern storage technologies such as solid-state drives (SSDs). These

devices employ advanced data management techniques, including background optimization and internal memory handling processes, which may significantly alter the behavior of deleted data. Evaluating recovery performance in such environments can improve the applicability of forensic techniques in current systems.

Further research can focus on analyzing the impact of enhanced security mechanisms, including encryption and access control modifications introduced through updates. Understanding how these features affect the visibility and accessibility of residual data is essential for adapting forensic methodologies to increasingly secure environments. Expanding the dataset to include diverse file formats, larger data volumes, and varied deletion scenarios can also provide a more comprehensive evaluation of recovery behavior. This would allow simulation of complex real-world conditions and improve the reliability of forensic conclusions.

Another promising area involves the development of adaptive forensic frameworks that can adjust to system-level changes introduced by updates. Such approaches could incorporate intelligent analysis techniques to identify recoverable data patterns more efficiently and improve reconstruction accuracy under restricted conditions. Additionally, comparative evaluation using multiple recovery approaches, rather than relying on a single tool such as DiskDigger, can help identify more effective strategies for handling updated systems. Integrating different techniques may enhance recovery success in environments where standard methods show limitations.

REFERENCES

- [1] National Institute of Standards and Technology, *Guide to Integrating Forensic Techniques into Incident Response*, NIST SP 800-86, 2006. [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-86/final>
- [2] E. Casey, *Digital Evidence and Computer Crime*, 3rd ed. Academic Press, 2011.
- [3] B. Carrier, *File System Forensic Analysis*. Addison-Wesley, 2005.

- [4] N. Phillips, F. Enfinger, and C. Steuart, *Computer Forensics and Investigations*, 5th ed. Cengage Learning, 2014.
- [5] International Organization for Standardization, *ISO/IEC 27037: Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*, 2012.
- [6] S. Garfinkel, "Digital forensics research: The next 10 years," *Digital Investigation*, vol. 7, pp. S64–S73, 2010.
- [7] V. Roussev, "Data fingerprinting with similarity digests," in *IFIP International Conference on Digital Forensics*, 2010.
- [8] SANS Institute, "Digital Forensics and Incident Response Overview," 2020. [Online]. Available: <https://www.sans.org>
- [9] Microsoft, "Windows Security Updates and System Protection," 2022. [Online]. Available: <https://learn.microsoft.com>
- [10] OWASP, "Security Principles and Data Protection," 2021. [Online]. Available: <https://owasp.org>
- [11] A. Case and R. Golden, "Memory forensics: The path forward," *Digital Investigation*, 2017.
- [12] D. Farmer and W. Venema, *Forensic Discovery*. Addison-Wesley, 2004.
- [13] National Institute of Justice, "Electronic Crime Scene Investigation Guide," 2008. [Online]. Available: <https://nij.ojp.gov>
- [14] DiskDigger, "DiskDigger Official Documentation," 2023. [Online]. Available: <https://diskdigger.org>
- [15] "Challenges in Data Recovery from Modern Systems," *Digital Investigation Journal*, 2019.
- [16] "Impact of Security Updates on System Behavior," *Journal of Cybersecurity Research*, 2021.
- [17] B. Carrier, "Risks of Live Digital Forensic Analysis," *Communications of the ACM*, 2006.
- [18] National Institute of Standards and Technology, *Guidelines on Mobile Device Forensics*, NIST SP 800-101, 2014. [Online]. Available: <https://csrc.nist.gov>
- [19] R. Bejtlich, *The Practice of Network Security Monitoring*. No Starch Press, 2013.
- [20] European Union Agency for Cybersecurity, "Digital Forensics Challenges and Trends," 2020. [Online]. Available: <https://www.enisa.europa.eu>
- [21] "Secure Deletion and Its Impact on Data Recovery," *Journal of Information Security*, 2018.
- [22] "Data Persistence and Overwrite Behavior in Modern File Systems," *IEEE Transactions on Computers*, 2017.
- [23] IEEE, "Advances in Digital Forensics Techniques," in *IEEE Conference Proceedings*, 2019.