Journal of Applied Informatics and Computing (JAIC)
Vol.10, No.2, April 2026, pp. 1329~1337
e-ISSN: 2548-6861

Analysis of the Effectiveness of Data Sanitization Methods on Windows Against Data Recovery Using a Digital Forensic Approach

Rara Eka Septya [1]*, Agus Wijayanto [2]*, Muhammad Fahmi Abdillah [3]*, Djumhadi [4]*
* Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Mulia
raraseptya@students.universitasmulia.ac.id [1], aguswijayanto@universitasmulia.ac.id [2], muhammadfahmi@universitasmulia.ac.id [3]
djumhadi@universitasmulia.ac.id [4]

Article Info

Article history:

Received 2026-01-14
Revised 2026-02-23
Accepted 2026-04-08

Keyword:

Data Sanitization,
File Carving,
Windows 10,
ACPO,
Digital Forensics.

ABSTRACT

The growth of Windows 10 usage in Indonesia has made user data security an issue that needs to be considered. The Reset This PC feature provides three data sanitization options, namely Keep My Files, Just Remove My Files, and Fully Clean The Drive. However, the effectiveness of each method in permanently eliminating data has not been widely analyzed using a forensic approach. This study aims to evaluate the effectiveness of the three sanitization methods against the possibility of data recovery using file carving techniques. The research process was conducted using the ACPO forensic guidelines, which consist of Plan, Capture, Analyze, and Present. The disk images resulting from the reset process were analyzed using Autopsy, PhotoRec, and Foremost. Three main parameters used to determine effectiveness were volume, integrity, and functionality. The results show that the Fully Clean The Drive option is the only method that is truly effective, with an effectiveness rate of 0%. Meanwhile, Just Remove My Files still leaves digital artifacts with an average effectiveness of 77.8%, and Keep My Files is the least effective as a data sanitization technique. These findings confirm that Windows users cannot rely on the other two reset methods if the primary objective is to permanently delete data.

I. INTRODUCTION

The development of technology has made computers and laptops an essential part of daily activities across various sectors, including education, business, and government. Along with the increasing functions of these devices, ranging from simple document processing to internet browsing, personal data storage, and multimedia usage, data security and privacy issues have become critically important. [1].

In Indonesia, the Windows operating system dominates the desktop market. StatCounter records that as of September 2025, Windows accounts for more than 80% of desktop users, with Windows 10 being the most widely used version, representing more than 60% of total Windows users [2], [3]. This dominance makes data security on Windows 10 a relevant subject for research, particularly regarding the effectiveness of the built-in data sanitization mechanisms provided by the operating system.

Many users still assume that data will be completely lost simply by performing delete, emptying the recycle bin, or using a quick format [4]. In reality, however, deleted data does not necessarily disappear entirely from storage media. This condition has the potential to cause privacy breaches and misuse of personal data by unauthorized parties [5]. Data remnants can still be recovered with the assistance of forensic software such as Autopsy, PhotoRec, and Foremost, which are specifically designed to perform data recovery processes using file carving techniques [6], [7], [8].

Windows 10 provides a built-in feature called Reset This PC, which is designed to remove user data and restore the system to its factory default state. This feature has two main modes, namely Keep My Files and Remove Everything. Within the Remove Everything mode, there are two advanced options: Just Remove My Files and Fully Clean The Drive [9]. These three scenarios offer different levels of data deletion; however, to date, there has been limited research discussing

how effective each method is in preventing files from being recovered using file carving techniques.

From a technical perspective at the file system level, particularly on NTFS, these three reset options operate fundamentally differently. The Keep My Files method preserves the Master File Table (MFT) entries and data clusters of user profiles while only deleting the MFT records associated with system and application directories, ensuring user data remains fully intact. In contrast, the Just Remove My Files method performs a logical deletion akin to a quick format. It merely updates the MFT to mark the user's file entries as unallocated space but does not overwrite the actual data clusters residing on the physical storage sectors. Consequently, the physical file signatures (headers and footers) remain untouched, leaving the remnants highly vulnerable to reconstruction via file carving techniques [10]. Conversely, the Fully Clean The Drive method executes a comprehensive data sanitization process. Beyond deleting the MFT entries, it actively overwrites the physical data clusters across the storage media (e.g., via zero-filling). This process completely destroys the structural integrity of the file signatures at the sector level, rendering file carving attempts ineffective [10].

Previous studies provide an important foundation regarding data sanitization; however, most of them focus on Android devices or third-party data wiping applications. A study by Kuswara et al. found that factory reset on Android is fairly effective in deleting data, but the study was limited to a single device and used only one recovery tool [11]. Research by Blankesteijn et al. examined the effectiveness of factory reset on modern Android devices and found that although some log artifacts remained, user data was still secure due to encryption [12]. However, the focus of that study was on mobile devices rather than desktop operating systems such as Windows 10, which have different architectures and do not always use encryption by default. A study by Andika et al. compared various wiping applications such as AOMEI and Eraser and found significant differences in effectiveness, but the study did not examine Windows' built-in sanitization mechanisms [13]. Meanwhile, Abdillah and Prayudi evaluated the effectiveness of carving tools such as Foremost and TestDisk; however, the test files were limited to JPG, PNG, and MP4 formats and did not include operating system reset scenarios [14]. Research by Syahputra and Prayudi showed that different deletion methods resulted in varying levels of recovery success, but the research object was a flash drive, meaning the results cannot be generalized to desktop operating systems [15]. The limitations of previous studies lie in the absence of in-depth testing of the built-in data sanitization mechanisms of the most popular desktop operating system, namely the Reset This PC feature in Windows 10, particularly regarding comparisons of the effectiveness among its three built-in deletion options.

The Reset This PC feature can be considered a data protection mechanism intended to minimize the possibility of files being recovered by other parties. However, there is no guarantee that all deletion methods within this feature are truly effective in preventing data recovery processes. Therefore, research is needed to examine how effective the Reset This PC feature is in deleting data so that it cannot be recovered, whether there are differences in data recovery results among the three reset options, and what types of artifacts remain after the reset process is performed.

In this study, the level of effectiveness is measured using three main parameters: the number of files that can still be successfully recovered (volume), the correspondence of the hash values of recovered files with the original files (integrity), and the ability of the recovered files to be opened and function properly as intended (functionality) [16], [17]. The fewer files that can be recovered, the less valid the recovery results are, and the greater the number of files that cannot be opened, the more effective the method is as a data sanitization technique in preventing recovery by other parties.

This study employs a digital forensic approach by referring to the principles of ACPO (Association of Chief Police Officers), which ensure that each stage, from planning and acquisition to analysis and reporting, is conducted in a structured manner while maintaining data integrity. These principles include preserving data authenticity, documenting the entire process (audit trail), and being accountable for the results obtained[18].

In terms of practical application, this study is positioned within three primary usage scenarios. First, for individual users who intend to sell, donate, or dispose of their personal computers, understanding the effectiveness of each reset option is essential to prevent privacy breaches and unauthorized recovery of personal data. Second, for organizations or institutions that manage employee devices, selecting an appropriate data sanitization method is critical to ensure compliance with internal data protection policies and to minimize the risk of data leakage when assets are reassigned, recycled, or decommissioned. Third, within a legal and digital forensic context, the findings of this study provide empirical insight into the extent to which data remnants may still be recovered after a system reset. This is particularly relevant for investigators handling digital evidence, as knowledge of residual artifacts can support forensic analysis processes conducted in accordance with established guidelines such as ACPO [18].

By clarifying these usage scenarios, this research not only evaluates the technical effectiveness of Windows 10 reset mechanisms but also highlights their practical implications for personal data protection, organizational information security management, and digital forensic investigations.

II. METHOD

This study employs an experimental method to analyze the effectiveness of three data sanitization methods within the Reset This PC feature in Windows 10. The experimental approach was chosen because it allows the researcher to directly intervene in the test object, namely the Windows 10 operating system in a Virtual Machine (VM) environment,

and to evaluate the results in a measurable manner using digital forensic techniques. In addition, this study refers to the ACPO (Association of Chief Police Officers) framework, which ensures that the research process is conducted systematically, in a structured manner, and maintains the integrity of digital evidence throughout all stages. [18].

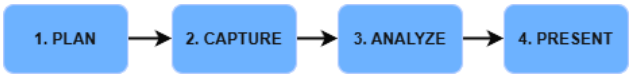

Figure 1. Research Flow

The research workflow shown in Figure 1 illustrates a series of stages arranged systematically to ensure that the problem-solving process is conducted scientifically. The outline of each stage is as follows:

A. Plan

The planning stage involves the strategic design of the forensic experiment to ensure controlled and reproducible conditions. Operationally, this included determining the three specific Windows 10 sanitization scenarios (Keep My Files, Just Remove My Files, and Fully Clean The Drive). It also involved configuring the isolated testing environment using VirtualBox, setting up the Windows 10 target VM and the CSI Linux forensic analysis VM, and deploying a standardized dataset of 100 files (consisting of .docx, .pdf, .txt, .jpg, .png, .mp3, .mp4, and .zip formats) into the target partitions. Crucially, a baseline was established by calculating the initial SHA-256 hash values of all test files and creating a verified VM snapshot before any reset execution began [18].

B. Capture

The capture stage focuses on the secure acquisition of digital evidence without altering the original data [18]. Operationally, after each reset scenario was executed within the Windows 10 VM, the virtual disk (.vmdk) was immediately exported into a forensic image format using the VBoxManage clonehd command.

To guarantee the integrity of the digital evidence, it is mandatory to implement a write-blocking mechanism and cryptographic hashing during the acquisition phase [19]. Because this research involves a virtualized environment, a logical write blocker is applied by mounting the exported .vmdk image in read-only mode within the CSI Linux forensic environment. This software-based write blocking prevents any accidental or intentional data modification by the host operating system or the forensic tools.

Furthermore, immediately following the export process, a SHA-256 hash value of the image is calculated and documented. This cryptographic hash acts as a unique digital fingerprint. Before any file carving analysis begins in the next stage, the hash is recalculated and compared against the initial value to mathematically verify that absolute bit-level integrity has been maintained and no spoliation occurred during the transfer process [20]. This rigorous process is conducted to strictly comply with the ACPO principle that digital evidence must not be altered.

C. Analyze

The analyze stage entails the extraction and examination of data remnants from the acquired evidence [18]. Operationally, the forensic images were imported into the CSI Linux environment and subjected to file carving techniques using three distinct open-source tools: Autopsy, PhotoRec, and Foremost. The effectiveness of the data sanitization scenarios was mathematically measured based on three operational parameters:

1. Volume (V)

This parameter measures the quantitative recovery rate. It is operationally defined as the percentage of test files successfully retrieved by the carving tool, regardless of their internal condition. The volume is calculated using the following formula [16], [17], [21]:

$$V\ (\%) = \frac{Number\ of\ successfully\ recovered\ files}{Total\ number\ of\ deleted\ files}\ X\ 100\%$$

where $Number\ of\ successfully\ recovered\ files$ is the total number of extracted files and $Total\ number\ of\ deleted\ files$ is the initial number of test files deployed before the reset process.

2. Integrity (I)

This parameter measures the bit-level authenticity of the recovered data. It is operationally defined as the percentage of recovered files that perfectly match the original files. This is verified by comparing the SHA-256 hash value of each recovered file with the pre-recorded baseline hash. The integrity is calculated as [16], [17], [21]:

$$I\ (\%) = \frac{Files\ with\ matching\ hashes}{Total\ recovered\ file}\ X\ 100\%$$

where $Files\ with\ matching\ hashes$ is the number of recovered files with hash values identical to their original counterparts.

3. Functionality (F)

This parameter assesses the practical usability of the recovered data. It is operationally defined as the percentage of recovered files that can be successfully opened, rendered, or executed by their default applications without displaying any corruption errors. The functionality is calculated as [16], [17], [21]

$$F\ (\%) = \frac{Number\ of\ Files\ That\ Can\ Still\ Be\ Opened}{Total\ recovered\ file}\ X\ 100\%$$

where $Number\ of\ Files\ That\ Can\ Still\ Be\ Opened$ is the number of accessible and readable files.

4. Final Average Effectiveness

To determine the overall effectiveness, the final average across the parameters is calculated.

$$Scenario\ Average\ (\%) = \frac{V_{avg} + I_{avg} + F_{avg}}{3}$$

The smaller the average effectiveness percentage value, the more effective the deletion method is in performing permanent data sanitization.

D. Present

The final stage involves the preparation of the analysis report, the presentation of data in graphical and descriptive forms, and the drawing of conclusions regarding the most effective Windows 10 reset method. All documentation and audit trails are preserved to ensure transparency [18].

III. RESULTS AND DISCUSSION

A. Plan

The Plan stage is the initial phase in the ACPO approach, which functions to design the entire experimental process in a systematic, measurable, and repeatable manner. This study employs the ACPO approach, which emphasizes strict control over the integrity of digital evidence. At this stage, three data sanitization scenarios are defined based on the Reset This PC feature in Windows 10, namely Keep My Files, Just Remove My Files, and Fully Clean The Drive. These three scenarios are selected to examine differences in the effectiveness of the reset methods against data recovery processes using file carving techniques.

TABLE 1
DETERMINATION OF RESEARCH SCENARIOS

Scenario	Description
Reset 1 (Keep My Files)	The system is reset while user files are retained.
Reset 2 (Just Remove My Files)	The system performs a quick deletion (quick format) without overwriting the storage sectors.
Reset 3 (Fully Clean The Drive)	The system deletes all user files and performs an overwrite process on the drive.

The research environment is created using VirtualBox so that each scenario can be tested from the same initial condition and does not alter the researcher's physical storage media. Two virtual machines are used in this study: a Windows 10 VM as the data sanitization test object and a CSI Linux VM as the forensic analysis environment.

TABLE 2
WINDOWS 10 TEST ENVIRONMENT SPECIFICATIONS (RESEARCH OBJECT)

Component	Description
VM Name	win 10
Operating System	Windows 10 Home 64-bit Version 22H2 (OS Build 19045.3803)
Storage Type	Virtual Machine Disk (.vmdk)
Disk Capacity	25.00 GB
RAM Allocation	4096 MB
File System	NTFS (New Technology File System)

TABLE 3
CSI LINUX TEST ENVIRONMENT SPECIFICATIONS (FORENSIC ANALYSIS)

Component	Description
VM Name	CSI Linux 2021.2
Operating System	CSI Linux 2021.2
Disk Capacity	58.00 GB
RAM Allocation	9216 MB

The test data consist of 100 files with various commonly used file extensions, including document formats (.docx, .pdf, .txt), images (.jpg, .png), audio (.mp3), video (.mp4), and archive files (.zip).

TABLE 4
TYPES OF TEST DATA

Extension	Quantity
.docx	15
.pdf	15
.txt	15
.jpg	15
.png	10
.mp3	10
.mp4	10
.zip	10

All data were calculated for their initial SHA-256 hash values, and the VM was saved as a snapshot to ensure that the testing process was reproducible in accordance with ACPO standards.

B. Capture

The next stage involves designing a forensic acquisition procedure to obtain disk images after the reset process is performed. Each reset scenario is executed from the Initial Snapshot condition, after which the disk is exported using the VBoxManage clonehd command to generate an image file in .vmdk format. Each image is then verified using a SHA-256 hash to ensure that no changes occur during the transfer process.

TABLE 5
IMAGE HASH DOCUMENTATION

Image Name	SHA-256
win10(reset1).vmdk	1D5B0C04F4C6C3553F35308E90D1AEAC39EECF04276B21B7E69CC358BC842C49
win10(reset2).vmdk	DEBFFF379745352926A9A7116F058E5194AC060012A1E1DF6CA3A4B531ED70ED
win10(reset3).vmdk	0ECCE8CF68FB07EC8CF8CFE026E8D80688AEE6B0EE1DF45546316B3EAB6379F0

In addition to hash values, the metadata of the image files were also recorded as part of the audit trail in accordance with ACPO guidelines, including file size, modification time, and access time.

TABLE 6
FORENSIC IMAGE METADATA

File Name	File Size	File Modification Date/Time	File Access Date/Time
win10(reset 1).vmdk	11 GB	2025:11:30 01:31:52-07:00	2025:11:30 02:03:43-07:00
win10(reset 2).vmdk	11 GB	2025:11:30 02:19:31-07:00	2025:11:30 02:35:59-07:00
win10(reset 3).vmdk	25 GB	2025:11:30 02:53:44-07:00	2025:11:30 03:16:33-07:00

C. Analyze

At this stage, the forensic image is imported into the CSI Linux environment. File carving analysis is performed using Autopsy, PhotoRec, and Foremost to recover data remnants. To ensure methodological reproducibility and the legal admissibility of the digital evidence, the exact versions and configurations of the open-source forensic tools must be explicitly documented [22]. The software configurations utilized in this study are as follows:

1. Autopsy (Version 2.24-3): Configured using the default ingest modules, specifically activating the "File Type Identification" and "Extension Mismatch Detector" modules to accurately parse file signatures across the NTFS file system.
2. PhotoRec (Version 7.1): Executed with the FileOpts parameter strictly configured to target only the specific extensions defined in the test dataset (.docx, .pdf, .txt, .jpg, .png, .mp3, .mp4, .zip) to optimize the carving process and reduce false positives.
3. Foremost (Version 1.5.7): Executed by modifying the default foremost.conf configuration file to uncomment and activate the exact hexadecimal headers and footers corresponding to the test dataset extensions.

The effectiveness of each scenario is measured based on three main parameters:

1. Volume (V)

The higher the volume value, the lower the effectiveness of data sanitization.

TABLE 7
NUMBER OF RECOVERED FILES

Tool/Scenario	Reset 1	Reset 2	Reset 3
Autopsy	100	43	0
Photorec	82	43	0
Foremost	61	35	0

As visualized in Figure 2, the test results show that in the Reset 1 (Keep My Files) scenario, Autopsy successfully recovered the highest number of files, totaling 100 files, followed by PhotoRec with 82 files and Foremost with 61 files. In the Reset 2 (Just Remove My Files) scenario, the number of recoverable files decreased significantly, with Autopsy and PhotoRec both able to recover 43 files, while Foremost only managed to recover 35 files. In the Reset 3 (Fully Clean The Drive) scenario, none of the tools were able to recover any files.

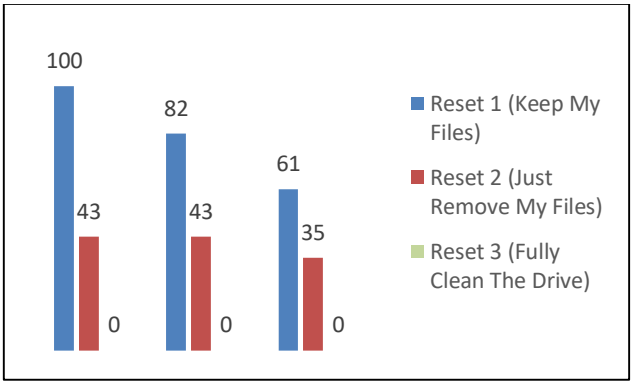

Figure 2. Comparison of the Number of Recovered Artifacts by Tool and Scenario

TABLE 8
AVERAGE VOLUME PER SCENARIO

Scenario	V_avg (%)
Reset 1 (Keep My Files)	81%
Reset 2 (Just Remove My Files)	40,3%
Reset 3 (Fully Clean The Drive)	0%

The Reset 1 (Keep My Files) scenario shows a very high file recovery rate of 81%. This result is consistent with Windows' built-in mechanism, which does not delete user files under this method but only removes applications and system settings, while the directory structure and the contents of user folders remain preserved. Although user files are not deleted by the system, recovery capabilities vary across the file carving tools used. PhotoRec is able to recover almost all file extensions; however, some limitations remain, such as three .mp4 files that could not be recovered and .txt files that were not fully readable, due to the signature-based recovery method that does not always detect all artifacts. Foremost only successfully recovers .zip and .pdf files completely, while other extensions such as .mp3 and .txt cannot be recovered because they are not included in the default foremost.conf configuration. In contrast to these two tools, Autopsy successfully recovers all files from all extensions by leveraging filesystem metadata analysis, allowing intact files to be properly identified. Overall, the results of this scenario confirm that user files are indeed not deleted by Windows, and any imperfections in recovery are more attributable to the limitations of the file carving tools rather than to data modification or deletion during the reset process.

In this scenario, recoverable artifacts include full metadata (e.g., filenames, paths from user directories, creation/modification timestamps, file sizes from NTFS MFT) and thumbnails for images (.jpg, .png) preserved in caches like Thumbcache.db or Thumbs.db if files were viewed pre-reset. No fragments are recovered as data clusters remain allocated. Meanwhile, Reset 2 results in a recovery

rate of 40.3% because it uses a quick deletion method that still leaves data artifacts, whereas Reset 3 demonstrates the most effective outcome, with no files recoverable (0%), in line with the overwrite mechanism designed to completely eliminate data traces. For Reset 2, artifacts recovered are primarily file fragments (headers/footers, partial content) from unallocated space, partial metadata from .lnk shortcuts or prefetch files (.pf) (e.g., filenames, paths, timestamps), and thumbnails in Thumbcache.db for previewed images/documents. In Reset 3, no artifacts like metadata, thumbnails, or fragments are detectable due to sector-level overwriting.

2. Integrity (I)

The higher the integrity value, the lower the effectiveness of data sanitization.

TABLE 9
NUMBER OF FILES WITH IDENTICAL HASH VALUES

Tool/Scenario	Reset 1	Reset 2	Reset 3
Autopsy	100	43	0
Photorec	82	43	0
Foremost	51	28	0

Based on the hash matching tests, in the Reset 1 (Keep My Files) scenario, Autopsy shows the best results with 100 files having hash values identical to the original files, followed by PhotoRec with 82 files and Foremost with 51 files. In the Reset 2 (Just Remove My Files) scenario, both Autopsy and PhotoRec each produce 43 files with identical hashes, while Foremost produces only 28 files with identical hash values. Meanwhile, in the Reset 3 (Fully Clean The Drive) scenario, none of the tools are able to recover any files with matching hash values.

TABLE 10
AVERAGE INTEGRITY PER SCENARIO

Scenario	I_avg (%)
Reset 1 (Keep My Files)	94,5%
Reset 2 (Just Remove My Files)	93,3%
Reset 3 (Fully Clean The Drive)	0%

The Reset 1 (Keep My Files) scenario shows a very high level of data integrity, amounting to 94.5%. This result is consistent with the Windows mechanism, which does not delete or modify user files, allowing the files to remain intact and the recovered hash values to ideally match the original hashes. Nevertheless, the testing reveals anomalies in the recovery results obtained using Foremost. Of the 61 files successfully recovered, 10 files have hash values that differ from the original files. This discrepancy is not caused by the Windows reset process but rather by Foremost's operational mechanism, which extracts files based on signature searching within disk sectors without utilizing filesystem metadata. As a result, the carving process may produce incomplete files or files with altered internal structures, even though the original files are actually still intact within the partition, leading to different hash values. Therefore, the hash mismatches in Foremost's results reflect the limitations of the file carving technique used rather than changes to the original files caused by the reset process. Meanwhile, Reset 2 shows an integrity value of 93.3% because although the files are deleted, the file headers and structures can still be fully recovered, resulting in many hash values identical to the initial data. In contrast, Reset 3 yields an integrity value of 0%, indicating that no files were successfully recovered or matched with the original hashes.

3. Functionality (F)

The higher the functionality value, the lower the effectiveness of data sanitization.

TABLE 11
NUMBER OF FILES THAT CAN STILL BE OPENED

Tool/Scenario	Reset 1	Reset 2	Reset 3
Autopsy	100	43	0
Photorec	82	43	0
Foremost	61	35	0

The evaluation of files that can still be opened shows that in the Reset 1 (Keep My Files) scenario, Autopsy maintains the best performance with 100 accessible files, followed by PhotoRec with 82 files and Foremost with 61 files. In the Reset 2 (Just Remove My Files) scenario, both Autopsy and PhotoRec successfully reopen 43 files, while Foremost only retains 35 files that remain valid. Meanwhile, in the Reset 3 (Fully Clean The Drive) scenario, none of the three tools are able to produce any files that can be opened.

TABLE 12
AVERAGE FUNCTIONALITY PER SCENARIO

Scenario	F_avg (%)
Reset 1 (Keep My Files)	100%
Reset 2 (Just Remove My Files)	100%
Reset 3 (Fully Clean The Drive)	0%

In the Reset 1 and Reset 2 scenarios, all recovered files can still be opened and function normally, indicating a good level of functionality. In contrast, in the Reset 3 scenario, no files are successfully recovered, resulting in a functionality value of 0%.

4. Final Average Effectiveness

This stage presents a recap of effectiveness values based on three main parameters: Volume, Integrity, and Functionality.

Based on the table of final average effectiveness for each scenario, the Reset 1 (Keep My Files) scenario has the highest average effectiveness value, amounting to 91.8%. This value indicates that the method almost does not delete user data, which is consistent with the Windows design that retains all files in user directories. Conceptually, all effectiveness parameters should reach 100%; however, the test results show lower values. This decrease is not caused by the Windows reset process but by the limitations of the extraction

techniques used by the file carving tools. PhotoRec and Foremost rely on signature-based methods, which are not always able to fully recover all files even when the files are still stored on the storage media.

TABLE 13
FINAL AVERAGE EFFECTIVENESS OF EACH SCENARIO

Scenario	V_avg	I_avg	F_avg	Final Average (%)
Reset 1 (Keep My Files)	81%	94,5%	100%	91,8%
Reset 2 (Just Remove My Files)	40,3%	93,3%	100%	77,8%
Reset 3 (Fully Clean The Drive)	0%	0%	0%	0%

In contrast, Autopsy is able to achieve a 100% recovery rate by leveraging filesystem metadata. Thus, the imperfections in the effectiveness values for the Keep My Files scenario are entirely influenced by differences in the capabilities and limitations of each tool, rather than by the Windows reset mechanism itself. The Reset 2 scenario produces an average value of 77.8%, indicating that this method deletes user files without applying a deep overwrite process. Although it is more effective than Reset 1 in removing data, this method still leaves a significant number of artifacts, allowing simple file carving techniques to recover some data. Meanwhile, the Reset 3 scenario achieves an average value of 0%, indicating the highest level of effectiveness in data removal.

Mathematically, this 0% effectiveness is calculated as the average of the three parameters: Effectiveness = $(V + I + F) / 3 = (0\% + 0\% + 0\%) / 3 = 0\%$, where no files were recovered across any metric. Conceptually, a 0% effectiveness rate signifies complete and unambiguous sanitization success, as the overwrite process destroys all data remnants, rendering recovery impossible and aligning with forensic definitions of effective erasure where lower (or zero) recovery percentages indicate superior data wiping [21].

This method is the only built-in Windows reset option capable of permanently deleting data through an overwrite mechanism, leaving no recoverable artifacts and therefore being suitable for use as a data sanitization technique.

D. Present

Reset 1 (Keep My Files) has the highest value at 91.8% because it does not delete user files. The imperfections in recovery are caused by the limitations of the carving tools, not by the reset process itself. Reset 2 deletes files with a value of 77.8% but still leaves many artifacts, making the data vulnerable to recovery. Reset 3 is the only method that is truly effective, with a value of 0%, because it performs an overwrite process that completely eliminates all files.

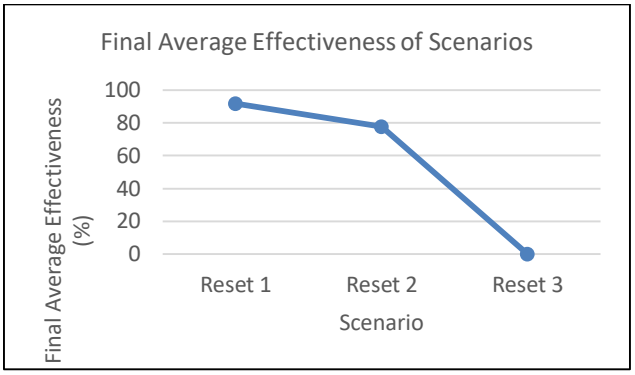

Figure 3. Final Average Effectiveness of Scenarios

The results of this study are highly consistent with previous research on data sanitization, albeit extending the context to native Windows 10 desktop environments. Similar to the findings of Kuswara et al. which demonstrated the effectiveness of Android factory resets, this study proves that native operating system reset features can achieve complete data wiping (0% recovery rate) provided that true sector overwriting is executed, as seen in the Fully Clean The Drive option [11]. Conversely, the high recovery rates observed in the Just Remove My Files scenario align with the conclusions of Andika et al. and Syahputra and Prayudi, who found that standard or logical deletion methods without deep overwriting leave significant digital artifacts vulnerable to carving tools [13], [15]. This comparison emphasizes that despite the platform difference, whether mobile devices, flash drives, or desktop operating systems, the fundamental principle of data remanence remains universal, only physical overwriting guarantees permanent sanitization.

Furthermore, it is critical to acknowledge how the underlying file system, specifically NTFS on Windows 10, dictates the recovery outcomes across these three scenarios. In the Keep My Files scenario (91.8% average effectiveness), file system variations are largely irrelevant because the OS deliberately bypasses user directories, leaving the data logically and physically untouched. However, the file system architecture becomes the primary determining factor in the Just Remove My Files scenario (77.8% average effectiveness). In NTFS, this logical deletion merely updates the Master File Table (MFT) to mark the space as unallocated while preserving metadata and contiguous cluster pointers. If this exact logical deletion were executed on a FAT32 partition (commonly utilized for external USB drives), the File Allocation Table's cluster chain would be immediately severed. This severance makes recovering fragmented files via file carving significantly harder and would naturally yield a much lower functional recovery rate compared to NTFS, even before any physical overwriting occurs [5], [21]. Finally, in the Fully Clean The Drive scenario (0% effectiveness), the logical file system structure becomes completely obsolete. The physical sector-level overwriting (zero-filling) ensures total data destruction regardless of whether the partition is formatted as NTFS, FAT32, or exFAT. This solidifies it as

the only universally secure sanitization method, capable of neutralizing data remnants across any file system architecture.

Finally, it is imperative to address the underlying hardware layer, specifically the distinction between Hard Disk Drives (HDD) and Solid State Drives (SSD), which significantly impacts forensic data recovery. Because this experimental study was conducted within a Virtual Machine environment utilizing virtual disks (.vmdk), the physical hardware layer was abstracted. By default, hypervisors do not pass hardware-level TRIM commands from the guest operating system to the host drive. Consequently, the virtual disk mimics the traditional behavior of an HDD, where logically deleted data remains physically intact in the unallocated space until overwritten. This abstraction allowed the study to purely isolate and evaluate the software-level deletion mechanisms of the Windows 10 Reset This PC feature. Had the Just Remove My Files scenario been tested on a bare-metal computer equipped with an SSD, the recovery rate of 77.8% would likely be drastically lower. Modern SSDs utilize the TRIM command and active background Garbage Collection, which autonomously and permanently erase data blocks marked as unallocated by the operating system to maintain write speeds. Once TRIM is executed, recovering data from those blocks using standard carving tools becomes nearly impossible, effectively acting as an automated anti-forensic mechanism [8], [21]. Therefore, while the Just Remove My Files method leaves significant recoverable artifacts on HDDs, the hardware-level data destruction inherent to SSDs introduces a crucial variable that investigators must consider in real-world digital forensics.

Beyond these technical and hardware architectures, the findings of this study bear significant practical implications for real-world data security, particularly concerning the disposal, donation, or resale of second-hand computing devices. Relying on standard logical deletion methods like Just Remove My Files leaves users highly vulnerable to data breaches, identity theft, and unauthorized exposure of personal information. Recent studies on electronic waste and second-hand markets confirm that poorly sanitized storage drives are frequently resold with highly sensitive, recoverable data still intact, posing severe global cybersecurity risks [23]. This critical vulnerability highlights the absolute necessity of aligning everyday data wiping practices with globally recognized cybersecurity frameworks. According to the National Institute of Standards and Technology (NIST) Special Publication 800-88 Guidelines for Media Sanitization, a proper sanitization process must either "Clear" (logical overwrite) or "Purge" (physical/cryptographic overwrite) the media to resist state-of-the-art laboratory recovery techniques [17]. The Keep My Files and Just Remove My Files options fundamentally fail to meet these NIST criteria, as they merely unlink file pointers. Therefore, it is strongly recommended that individual users and organizations strictly utilize the Fully Clean The Drive option as the absolute minimum baseline for data sanitization before transferring the ownership of any Windows 10 device, as it aligns with the NIST "Clear" standard. Furthermore, for devices equipped with SSDs that previously held highly confidential information, users are advised to supplement this built-in feature with manufacturer-provided "Secure Erase" tools to achieve the NIST "Purge" standard, ensuring irreversible data destruction across all flash memory blocks [23].

E. Limitations

Despite the conclusive results regarding the Windows 10 sanitization mechanisms, this study acknowledges certain experimental limitations. The testing was strictly confined to a single operating system iteration (Windows 10 Home 64-bit Version 22H2) operating within a virtualized storage environment (.vmdk). Consequently, the results may not perfectly mirror the sanitization efficacy of native hardware environments such as physical Solid State Drives (SSDs) employing active background TRIM commands, or newer operating systems like Windows 11, which may utilize updated data wiping algorithms.

IV. CONCLUSION

This study concludes that the effectiveness of the Reset This PC feature in Windows 10 is highly dependent on the reset option used. Of the three methods tested, Fully Clean The Drive is proven to be the only option that truly deletes data permanently. Under this method, all file carving processes using Autopsy, PhotoRec, and Foremost fail to recover a single file because all storage sectors have been overwritten.

In contrast, Just Remove My Files still leaves a significant amount of digital artifacts and allows file recovery with a high level of integrity, as Windows only performs logical deletion without overwriting. Keep My Files is the least effective method as a data sanitization technique, since all user files remain intact by design.

The differences in recovery results across the three scenarios indicate that the Reset This PC feature cannot be relied upon as a secure data deletion mechanism unless the Fully Clean The Drive option is used. These findings are important as a basis for selecting appropriate data sanitization methods, particularly when a device is to be sold, lent, or transferred to another owner.

To address the current experimental limitations, future research should not only consider testing on bare-metal physical storage types, but also expand the scope to evaluate the effectiveness of supplementary sanitization methods. Investigating the forensic resilience of Full Disk Encryption (FDE) like BitLocker applied prior to the reset process, evaluating third-party secure disk wiping tools, or testing hardware-level ATA Secure Erase commands would provide a more holistic understanding of absolute data sanitization strategies against advanced data recovery techniques.

REFERENCES

[1] A. Haris, A. Malik, A. N. Safitri, and A. S. Rahma, "Dasar-Dasar Komputer Yang Harus Dimiliki Oleh Masyarakat Dalam Menghadapi Perkembangan Teknologi," *Scientica: Jurnal Ilmiah Sains Dan Teknologi*, vol. 2, no. 1, pp. 1–9, 2024, doi: 10.572349/scientica.v2i1.673.

[2] Statcounter Global Stats, "Desktop Operating System Market Share Worldwide." Accessed: Oct. 09, 2025. [Online]. Available: https://gs.statcounter.com/os-market-share/desktop/indonesia

[3] Statcounter Global Stats, "Desktop Windows Version Market Share Indonesia." Accessed: Oct. 19, 2025. [Online]. Available: https://gs.statcounter.com/windows-version-market-share/desktop/indonesia

[4] J. Schneider *et al.*, "In Search of Lost Data: A Study of Flash Sanitization Practices," May 2025, [Online]. Available: http://arxiv.org/abs/2505.14067

[5] E. J. Lee, S. Y. Lee, H. Kwon, S. J. Lee, and G. B. Kim, "Identification of data wiping tools based on deletion patterns in ReFS $Logfile," *Forensic Science International: Digital Investigation*, vol. 46, p. 301607, Oct. 2023, doi: 10.1016/j.fsidi.2023.301607.

[6] A. Ardiansyah, D. S. Djoha, M. Z. Ardiansyah, and E. S. Eriana, "Penerapan Tools Autopsy Untuk Recovery File Pada Windows," *Jurnal Ilmu Komputer (JIK)*, vol. 7, no. 1, pp. 66–71, 2024.

[7] R. N. Dasmen, A. Triwulanda, R. Rasmila, D. Kurniawan, and J. Julia, "Implementation of Digital Forensics Photorec in Recovering Lost Files on External Storage," *PIKSEL : Penelitian Ilmu Komputer Sistem Embedded and Logic*, vol. 12, no. 1, pp. 173–178, Mar. 2024, doi: 10.33558/piksel.v12i1.9444.

[8] K. A. Dahlan, A. Yudhana, and H. Yuliansyah, "File carving Analyze of Foremost and Autopsy on external SSD mSATA using the Association of Chief Police Officer Method," *ILKOM Jurnal Ilmiah*, vol. 16, no. 3, pp. 283–295, Dec. 2024, doi: 10.33096/ilkom.v16i3.2360.283-295.

[9] M. Halsey, "Installing and Restoring Windows 11," in *Troubleshooting and Supporting Windows 11: Creating Robust, Reliable, Sustainable, and Secure Systems*, Springer, 2022, pp. 651–670.

[10] P. C. Sethi, "File Carving: Analyzing Data Retrieval in Digital Forensics," *International Journal of Computer and Information Technology*, vol. 13, no. 3, pp. 2279–0764, 2024, [Online]. Available: www.ijcit.com

[11] B. I. H. Kuswara, A. R. Pratama, and E. Ramadhani, "Studi Komparasi Metode Disk Overwrite dan Factory Reset sebagai Teknik Anti Forensik di Perangkat Android," *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, vol. 9, no. 2, pp. 1151–1161, Jun. 2022, doi: 10.35957/jatisi.v9i2.1955.

[12] M. B. Blankesteijn, A. Fukami, and Zeno. J. M. H. Geradts, "Assessing data remnants in modern smartphones after factory reset," *Forensic Science International: Digital Investigation*, vol. 46, p. 301587, Sep. 2023, doi: 10.1016/j.fsidi.2023.301587.

[13] R. A. Andika, N. D. W. Cahyani, and R. G. Utomo, "Testing Tools Data Wiping dalam Kegiatan Anti Forensik," *LOGIC: Jurnal Penelitian Informatika*, vol. 1, no. 1, p. 29, Sep. 2023, doi: 10.25124/logic.v1i1.6442.

[14] M. F. Abdillah and Y. Prayudi, "Data Recovery Comparative Analysis using Open-based Forensic Tools Source on Linux," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 9, pp. 633–639, 2022, doi: 10.14569/IJACSA.2022.0130975.

[15] R. R. Syahputra and Y. Prayudi, "Perbandingan Hasil Recovery File terhadap Penghapusan File menggunakan Perintah Sdelete dan Shift+Delete," *AJIE*, vol. 09, no. 02, pp. 117–131, May 2025, doi: 10.20885/ajie.vol9.iss2.art5.

[16] G. B. Akintola, "Assessing the Performance of Forensic File Recovery Tools on Deleted Files from a USB Device," *DS Journal of Cyber Security*, vol. 3, no. 2, Aug. 2025, doi: 10.59232/CYS-V3I2P101.

[17] J. Matondang, I. Maulana, and Carudin, "Analisis Perbandingan Perangkat Lunak Forensik Digital File Carving Menggunakan NIST," *INNOVATIVE: Journal Of Social Science Research*, vol. 3, no. 4, pp. 2154–2165, 2023, doi: https://doi.org/10.572349/scientica.v2i1.673.

[18] J. Williams, "ACPO Good Practice Guide for Digital Evidence," 2012.

[19] J. Sitima, "Understanding Digital Forensic Tools: Their Features, Applicability and Key Short Comings. A Compendium," *International Journal For Multidisciplinary Research*, vol. 6, no. 6, Nov. 2024, doi: 10.36948/ijfmr.2024.v06i06.30026.

[20] H. Syahida Alawi, I. Riadi, and S. Sunardi, "Improving Credibility of Digital Evidence Investigation in E-Commerce Fraud Cases using ISO/IEC 27037," *International Journal of Advances in Data and Information Systems*, vol. 6, no. 2, pp. 479–495, Aug. 2025, doi: 10.59395/ijadis.v6i2.1408.

[21] R. Naveen, A. Vijayarajan, K. P. Archana, and S. S. Nidhin, "Recovery of Deleted Files : Challenges and Techniques," *International Journal For Multidisciplinary Research*, vol. 7, no. 2, Apr. 2025, doi: 10.36948/ijfmr.2025.v07i02.41088.

[22] I. Ismail and K. Akram Zainol Ariffin, "The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance," *PLoS One*, vol. 20, no. 9, p. e0331683, Sep. 2025, doi: 10.1371/journal.pone.0331683.

[23] J. Schneider *et al.*, "Poor Sanitization Practices and Questionable Digital Evidence: A Comprehensive Study of Scope and Impact of Recycled NAND Flash Chips," *IEEE Trans. Dependable Secure Comput.*, vol. 22, no. 6, pp. 5970–5984, 2025, doi: 10.1109/TDSC.2025.3579237.

.