DS Journal of Cyber Security
Volume 3 Issue 2, 1-15, Apr - Jun 2025
ISSN: 2584-0665 / https://doi.org/10.59232/CYS-V3I2P101

Original Article

Assessing the Performance of Forensic File Recovery Tools on Deleted Files from a USB Device

Grace Bunmi Akintola

Department of Cyber Security, Nigerian Defence Academy, Kaduna, Nigeria.

gbogundele@nda.edu.ng

Received: 04 February 2025; Revised: 03 March 2025; Accepted: 02 April 2025; Published: 30 April 2025

Abstract - Digital forensics plays a crucial role in investigating cyber incidents, with USB forensics being essential due to the widespread use of USB storage devices. This study evaluates the performance of Recuva, Puran File Recovery, and EaseUS Data Recovery tools in retrieving deleted files from USB devices, identifying 18 key features across these tools. Performance metrics such as Recovery Rate (RR), File Type Success Rate, File Size Recovery Rate, Speed Recovery Time, and File Hash Matching Rate were analyzed. Puran File Recovery achieved the highest recovery rate (88.89%), followed by EaseUS (77.78%) and Recuva (72.22%). Recuva and Puran had the highest file type success rate of 88.89%. However, Puran consumed the most memory, recovering 16 files totaling 296MB from an original 187MB (158.29%). Recuva, with a 66.31% file type success rate (124MB/187MB) for 13 files, demonstrated more efficient memory usage than Puran. EaseUS, recovering 14 files with a 27.86% success rate, consumed the least memory, making it the most space-efficient tool for forensic analysts. Puran was the fastest, recovering files in 5 minutes and 20 seconds, while EaseUS excelled in file hash matching with an accuracy rate of 84.62%. These findings contribute to digital forensics by providing insights into the effectiveness of file recovery tools for USB forensic investigations. The study concludes with recommendations for enhancing forensic techniques and guiding future research in deleted file recovery.

Keywords - Digital forensics, USB forensics, File recovery tools, Performance metrics, Deleted file recovery**.**

1. Introduction

Digital forensics is the branch of forensic science that focuses on identifying, collecting, analyzing, and preserving electronic data from digital devices to investigate cybercrimes, security incidents, and legal disputes. It ensures the integrity and admissibility of digital evidence for use in court or cybersecurity operations [1]. Digital forensics is crucial in cybersecurity and criminal investigations, enabling digital evidence identification, analysis, and preservation. Cybersecurity aids in detecting cyberattacks, mitigating threats, identifying attack vectors, and ensuring compliance with GDPR and HIPAA regulations. Criminal investigations help recover deleted data, trace cybercriminal activities and provide legally admissible evidence for prosecuting fraud, hacking, and identity theft. By ensuring the integrity of digital evidence, digital forensics plays a key role in strengthening security measures and supporting law enforcement in combating emerging cyber threats and digital crimes [1]. Digital forensics, a branch of forensic science, is categorized into several specialized areas, each focusing on different digital evidence collection and analysis aspects. This includes Computer forensics, which involves examining computer systems and storage media to gather, analyze, and preserve digital evidence. Mobile device forensics investigates

smartphones, tablets, and other mobile devices to extract and analyze data such as call logs, messages, and application activity. Network forensics is crucial in analyzing network traffic and systems to detect cyberattacks, monitor security incidents, and trace malicious activities. Forensic data analysis examines data from multiple sources, including computers, mobile devices, and networks, to identify patterns, anomalies, and digital evidence. Lastly, database forensics investigates databases to recover lost or tampered data, identify vulnerabilities, and analyze data breaches. Each branch contributes to digital investigations, assisting law enforcement and cybersecurity professionals in uncovering evidence, preventing cybercrimes, and strengthening data security [2].
USB forensics is identified under the computer forensics category. It is described as a specialized branch of digital forensics focused on analyzing USB storage devices to recover data, track usage, and detect malicious activities. It plays a critical role in identifying unauthorized data transfers, retrieving deleted or hidden files, and analyzing metadata to establish activity timelines. Additionally, USB forensic investigations help detect malware, exploit attempts, and use anti-forensic techniques to erase or obfuscate evidence. This field is essential in law enforcement, corporate security, and cybersecurity, aiding in detecting data breaches, insider threats, and cybercrimes. By examining USB activity logs and recovered data, forensic experts can gather crucial evidence for legal proceedings and enhance digital security measures [3].

USB devices are crucial in data transfer, storage, and portability, making them essential for personal and professional use. Their ease of use and high storage capacity enable quick file transfers, backups, and software installations. However, they also pose security risks and potential misuse, including unauthorized data exfiltration, malware infections, and BadUSB attacks, where malicious firmware can execute unauthorized commands. Lost or stolen USB drives containing sensitive data can lead to significant privacy breaches. Organizations implement USB access restrictions, encryption, endpoint security monitoring, and policy enforcement to mitigate these risks, ensuring secure usage and preventing cyber threats associated with USB misuse [4].

Recovering deleted files in forensic investigations is challenging due to modern storage technologies and anti-forensic techniques. File overwriting can make a recovery impossible, while SSD TRIM functionality automatically erases deleted data blocks, further complicating forensic retrieval. Encryption and secure deletion methods, such as data wiping tools and cryptographic erasure, also prevent access to deleted files. Additionally, file fragmentation scatters data across storage locations, making full recovery difficult. File system variations impact recovery effectiveness, and cloud storage and remote deletion further restrict forensic access [5].

Forensic experts rely on specialized recovery tools, metadata analysis, and advanced reconstruction techniques to overcome these challenges, but evolving technologies continue to demand new forensic strategies. However, several research related to the analysis of different file recovery tools conducted over the years only show the categories of different files recovered in various formats and comparing the effectiveness of adopted tools via several criteria but do not fully focus on applying relevant file performance metrics to verify the authenticity of the recovered files such as it is the file integrity (file hash matching), File Size Recovery Rate and so on which is highly required in assessing the effectiveness of file recovery tool used by the forensic analysts.
Therefore, this paper focuses on the analysis of deleted files which was created on a set-aside USB flash drive (one of the widely used USB device types) of 8GB size in which three different file recovery tools, namely Recuva, Puran file recovery and the EaseUs data recovery tools were employed to carry out the analysis as well as evaluating the effectiveness of the tools based on selected performance metrics.

This research paper is structured as follows:

- Section 1 introduces digital forensics, focusing on USB forensics, its significance, and associated challenges.
- Section 2 overviews USB storage devices, USB forensics, and related works on forensic analysis methods for deleted files.

- Section 3 outlines the research methodology, including the adopted approach, justification for the selected file recovery forensic tools, and the rationale behind choosing the storage device.
- Section 4 discusses the results, covering identified features of the selected forensic tools, an explanation of the original files created and deleted on the USB storage device, an analysis of recovered and unrecovered files, and the selected performance metrics.
- Finally, Section 5 concludes the study with key findings and future research recommendations.

2. Related Work

2.1. Overview of USB Storage Device

A Universal Serial Bus (USB) storage device, commonly known as a flash drive, thumb drive, or pen drive, is a compact, portable storage device that utilizes flash memory and connects to a computer via a USB interface. It provides a convenient solution for storing and transferring files. There are several types of USB storage devices, including USB Flash Drives, which are the most common type, known for their small size, portability, and ease of use. The second type is the USB External Hard Drives, which are larger than flash drives, offering significantly more storage capacity, making them ideal for backups and large data storage. The third type is the USB Memory Sticks, which is another term for USB flash drives, emphasizing their role as portable storage solutions [6]. USB devices use various file system structures to manage data efficiently, with the choice depending on factors like compatibility, performance, and storage needs. The file system types include FAT32, which is the most widely used due to its universal compatibility ((Windows, macOS, Linux, consoles)) but has a 4GB file size limit and is best for Small USB drives (≤32GB) then, the exFAT improves on FAT32 by supporting larger files and better flash storage performance, making it ideal for modern USB drives. NTFS, the default Windows file system, offers advanced features like encryption and journaling but is read-only on macOS without additional software. HFS+ and APFS are optimized for macOS, with APFS providing faster performance and encryption for SSDs and flash storage. Meanwhile, ext4 is commonly used in Linux-based systems but lacks native support on Windows and macOS [7].

Choosing the right file system depends on intended use and device compatibility. FAT32 remains the best for smaller USB drives that require cross-platform access, while exFAT is ideal for large file transfers across different operating systems. NTFS and APFS are better suited for external hard drives or Mac-specific storage, where advanced features like security and performance are needed. Linux users may prefer ext4 for their forensic and system-related USB storage needs. Understanding these file systems is crucial for efficient data management, forensic investigations, and cybersecurity applications [7]. USB devices are widely used for data transfer, storage, and connectivity, making them integral to personal and professional computing. However, their widespread adoption also makes them a potential vector for cyber threats and illicit activities. USB storage devices, such as flash drives and external hard drives, play a vital role in digital forensics, as they often contain critical evidence of cybercrimes like malware distribution and data theft. Investigators rely on these devices to collect, analyze, and reconstruct digital evidence, aiding in forensic investigations and cybersecurity efforts [8].

2.2. Overview of USB Forensics

USB forensics has become a critical component of an investigator's toolkit in the ever-evolving landscape of cybersecurity and digital crime. Given the widespread use of USB devices in personal and professional environments, understanding the intricacies of USB forensic analysis is essential for uncovering digital evidence and strengthening cybersecurity measures [9]. USB forensics involves examining and analysing USB devices to retrieve evidence related to data transfers, file activity, and deleted files. This process plays a crucial role in cybersecurity and law enforcement investigations, helping to trace unauthorized access, detect data breaches, and reconstruct digital activities. To investigate and mitigate such security risks, USB forensics focuses on collecting, examining, and preserving digital evidence from USB devices. This forensic discipline plays a crucial role in solving

various cybercrimes, including malware distribution, data theft, and unauthorized access, helping to strengthen cybersecurity defenses and support law enforcement investigations [9].

Recovering deleted files from USB devices is challenging due to factors like data overwriting, file system differences, and hardware limitations. When a file is deleted, the system marks its space as available rather than erasing it, but new data can overwrite it, making recovery impossible. File systems like FAT32 and NTFS handle deletions differently, with some allowing easier recovery than others. Additionally, TRIM-enabled USB SSDs erase data almost immediately, and encrypted files (e.g., BitLocker, VeraCrypt) are nearly impossible to recover without the decryption key. Secure deletion tools can further complicate recovery by overwriting data multiple times [10].

Other challenges include logical corruption, bad sectors, and wear-leveling in flash storage, which redistributes data writes unpredictably [10]. Advanced forensic tools like Autopsy or R-Studio may help, but they require expertise, and free recovery software often has limitations. Time is critical-continued use of the USB increases the risk of overwriting deleted files, reducing the chances of successful recovery [11]. USB forensics is essential for data recovery and security investigations but comes with legal and ethical challenges. Investigators must comply with laws such as the Federal Rules of Evidence (FRE), GDPR, and CCPA to ensure that recovered data is admissible in court and that privacy rights are not violated. Unauthorized data recovery can lead to legal penalties, making it crucial to obtain proper consent or warrants before conducting forensic examinations. Additionally, maintaining a clear chain of custody and using validated forensic tools helps prevent evidence tampering and ensure data integrity [12]. Ethically, forensic analysts must remain objective, accurately document recovered data, and handle sensitive information responsibly. They should follow data minimization principles, limiting their analysis to relevant data while avoiding unauthorized access or exploitation. Best practices include maintaining transparency, adhering to ethical standards, and preventing the misuse of forensic tools for malicious purposes. By balancing legal compliance with moral integrity, investigators can ensure credible and responsible USB forensic investigations [13].

2.3. Related Works on Forensic Analysis Methods of Deleted Files

A research paper proposed a method to systematically track deleted files by identifying and analyzing various sources that manage file-related metadata in macOS systems. Currently, no existing method can comprehensively track the spoliation of evidence, as contemporary investigations largely rely on the skills and knowledge of individual investigators. By leveraging metadata sources, this approach provides a structured and reliable framework for forensic investigations, enhancing the ability to detect and analyze file deletions systematically [14]. In another research project, various anti-forensic activities were conducted on USB devices within a Windows environment. One set of techniques focused on concealing data within a USB thumb drive, while the other aimed to erase USB usage traces from the computer system. Experiments were carried out using multiple digital forensic tools and techniques to determine the feasibility of detecting these anti-forensic activities. This research is valuable for forensic professionals, aiding in the examination and investigation of cybercrimes involving anti-forensic methods [15].

The research was done, which involved the evaluation of the effectiveness of various forensic approaches-signature-based detection, behavioral analysis, and Machine Learning (ML)-in identifying and analyzing BadUSB attacks. The experiments involved preconfigured USB peripherals executing malicious activities such as keystroke injection, data exfiltration, malware delivery, and network traffic manipulation. The findings indicate that behavioral analysis and ML-based methods achieve high detection accuracy with low false positive rates. Among these, machine learning proves to be the most efficient. While behavioral analysis excels in detecting abnormal device behavior, it requires a longer detection time than ML-based methods. This study contributes to the field of digital forensics by addressing key challenges in detecting BadUSB attacks and advocating for improvements in detection methodologies. It also explores the integration of these techniques into existing cybersecurity

frameworks. Future research should focus on optimizing detection strategies, expanding datasets for ML-based methods, and enhancing forensic techniques to adapt to emerging technologies such as the Internet of Things and cloud systems [16].

A paper that examines a key aspect of cyber forensics was reviewed, focusing on data recovery challenges, particularly in Android phone forensics. It highlights the significance of computer forensics, including forensic, and presents a structured methodology for effective data recovery. Recuva, a versatile data recovery tool, is introduced as part of the broader forensic process. The paper underscores the critical role of data recovery in criminal investigations, corporate inquiries, civil litigation, incident response, and regulatory compliance. Additionally, it acknowledges key challenges such as data overwriting and encryption. Overall, this study provides a concise overview of the importance and applications of data recovery in digital forensics [17]. This research aims to critically analyze the results of forensic tools applied to both HDDs and SSDs, focusing on the images generated from each storage medium. As SSDs represent a more modern storage technology, traditional forensic tools designed for HDDs have shown reduced efficiency when analyzing SSDs. This limitation arises from the unique data management process in flash memory, where data can only be written after an erase operation is performed on the storage block. Consequently, every write operation on an SSD is preceded by an erase cycle, impacting forensic investigations [18].

Computer forensic testing was conducted using Photorec to recover 2,781 erased files of various data formats from a 32 GB USB flash drive. Data recovery was conducted on an Intel-based computer with 2 GB RAM, a 1.8 GHz processor, and the Linux operating system Xubuntu 20.04. The testing followed a predefined set of scenarios, with observations recorded and analyzed. Photorec stored the recovered files in six *recup_dir* subdirectories. The results demonstrate that Photorec is a reliable tool for computer forensics, particularly for secure data recovery. It successfully restored 100% of the erased data and assigned root privileges to all recovered files, preventing unauthorized modifications or deletions without granted access [19].

Another study was conducted that evaluated various data recovery software tools, including Recuva, EnCase, WinHex, ILook Investigator, Digital Detective Blade, and Forensic Toolkit (FTK), to determine the most forensically sound option for data recovery. The findings provide insights into the effectiveness of these tools, ultimately identifying the best software for forensic data recovery. This research serves as a foundational reference for future studies, offering an overview of computer forensic data recovery software and its applications [20].

An experimental setup, including a forensic workstation, a write-blocker, and commercially purchased USB hard drives, was examined using digital forensic imaging tools such as DC3DD, DCFLDD, and Guymager. Various test cases were designed, distributing USB hard drives into different groups to assess their compliance with NIST functional and optional requirements while recovering and analyzing remnant data. The forensic tools were evaluated based on log analysis, hardware resource usage, and processing time. The findings indicate significant differences in performance among the tools. Guymager was the fastest and met all functional requirements in each test case, but it consumed more CPU and memory resources than DC3DD and DCFLDD. Analysis of the recovered data revealed that 88.23% of the USB hard drives contained sensitive personal or business information, including personal photos, bank transactions, and contracts. This suggests that many consumers in New Zealand are unaware of personal data security risks and the potential vulnerabilities associated with data leakage [21].

In another study that was carried out, a tool comparison approach was employed, which involved using Foremost and TestDisk for data recovery. However, these tools operate exclusively through the Command Line Interface (CLI) on the Linux operating system rather than a Graphical User Interface (GUI). The results indicate that all recovered files are fully restored [22].

3. Materials and Methods

3.1. Methodology Adopted

An experimental research methodology type was selected for this paper as it involves conducting systematic investigations under controlled conditions to analyze cause-and-effect relationships. The Experimental Research Methodology is appropriate when conducting systematic investigations to evaluate forensic techniques, tools, or frameworks for analyzing files from USB devices. This methodology allows controlled testing to determine effectiveness, accuracy, and reliability. As illustrated in Figure 1, the following step-by-step procedure uses the structural approach to acquire and obtain accurate results from the seized USB device for forensic analysis.

- Step 1 (Data collection): This is the first step in the structural approach, which involves the collection of the USB device data used as a case study for forensic analysis. A controlled environment was created to simulate real-world forensic scenarios by preparing USB devices with various file states. This ensures that forensic analysis is conducted on realistic data. Before conducting forensic analysis, different types of files (e.g., documents, images, videos, and audio) were placed on USB devices, as these files serve as the initial dataset for testing forensic recovery tools, and then the files were deleted and formatted manually from the USB device.
- Step 2 (Examination): After acquiring data from the USB device, the next crucial phase in forensic analysis is an examination, where the extracted files are analyzed to determine their authenticity, integrity, and potential forensic value. This process involves several key steps: Data Extraction (which involves retrieving existing, deleted files and metadata from the USB device using forensic tools). Forensic Tools Used for Extraction include the Recuva, Puran file recovery, and the EaseUS data recovery tools.
- Step 3 (Analysis): In the process of analysis, Once files are extracted using forensic tools, Hashmyfiles software is used to check if the data has been altered using hashing algorithms such as MD5 (Message Digest Algorithm 5) and SHA-256 (Secure Hash Algorithm 256-bit) by comparing the hash value of created files with the recovered deleted files. Also, selected performance metrics were used to evaluate the selected recovery file forensic tools.
- Step 4 (Reporting): This step involves the proper documentation of the forensic analysis conducted from the data collection phase to the analysis of the acquired and recovered files. This phase is the most important as it gives a clear understanding to the assigned law agency in charge of forensic investigation and presenting admissible reports in the court of law.

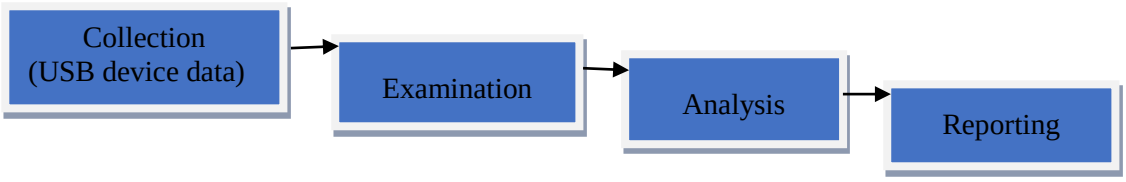

Fig. 1 The methodology process

3.2. Justification of the Selected File Recovery Forensic Tools

In obtaining accurate performance results, three file recovery forensic tools were selected for the analysis: the Recuva forensic tool, the Puran file recovery tool, and the EaseUS data recovery forensic tool.

3.2.1. The Recuva Forensic Tool

This file recovery forensic tool is selected due to its ability to recover deleted files from various storage devices, including hard drives, memory cards, and USB drives. This capability enables forensic investigators to identify and analyze deleted data that may serve as crucial evidence in digital investigations. Recuva supports a wide range of file types, such as documents, photos, videos, and emails, making it highly versatile for forensic applications. Its user-friendly interface, fast scanning capabilities, and file preview options enhance the efficiency of data recovery. Recuva operates in read-only mode to ensure evidence integrity, preventing accidental modifications during

recovery. Additionally, it supports multiple file systems, including FAT and NTFS, allowing for accurate file recovery even when metadata is damaged. A free version of Recuva offers basic data recovery features, making it accessible to a broader range of users [23].

3.2.2. The Puran File Recovery Tool

This forensic tool is selected due to its powerful features for forensic analysis, offering the ability to recover deleted or lost files from various storage devices. It can scan unallocated space, support multiple file systems, and perform deep scans to locate heavily overwritten data, making it highly valuable for digital investigations. The tool supports file systems such as FAT and NTFS, allowing forensic analysts to examine data across different storage media. Its "deep scan" feature conducts a thorough byte-by-byte search, increasing the likelihood of recovering deleted files even if they have been partially overwritten. Additionally, Puran File Recovery provides a file preview option, enabling investigators to assess the relevance of recovered data before saving it, which helps prioritize recovery efforts. To preserve digital evidence, the tool also allows for the creation of image files of the drive, ensuring that the original data remains intact for further forensic analysis. Its user-friendly interface enhances accessibility, making it a practical choice for forensic professionals [24].

3.2.3. The EaseUS Data Recovery Tool

This tool is a versatile solution for retrieving lost or deleted files, offering a user-friendly interface, broad compatibility with various storage devices, and support for multiple file types, including documents, photos, videos, audio files, and emails. With fast scanning speeds and a high success rate, it is a reliable choice for both novice and experienced users facing data loss scenarios such as accidental deletion, formatting, or partition loss. EaseUS supports data recovery from hard drives, external drives, USB devices, memory cards, and even lost partitions. Users can select between a quick scan for recently deleted files and a deep scan for comprehensive recovery in more complex situations. The tool also allows file previews before restoration, ensuring users retrieve the correct data. Known for its effectiveness even in challenging recovery cases where other tools may fail, EaseUS provides a free version for users to test its capabilities before committing to a paid subscription [25].

3.3. Justification of the Selected Storage Device

For the forensic analysis conducted in this paper, a USB flash drive (8GB memory size) was chosen due to its numerous benefits, including portability, compact size, ease of use, fast data transfer speeds, and broad compatibility with most devices. Its ability to store large amounts of data in a small, durable form makes it ideal for transferring files between computers and carrying important data on the go. Compared to other external storage devices, USB flash drives stand out for their extreme portability, lack of moving parts for enhanced durability, and the ability to quickly transfer small to medium-sized files without requiring an internet connection. They are compatible with most computers, laptops, and even some mobile devices with USB ports. Additionally, USB flash drives are relatively inexpensive, especially for smaller storage capacities, making them cost-effective. While external hard drives offer larger storage capacities, USB flash drives are often faster and more convenient for quick file transfers [26].

4. Results and Discussion

4.1. The Identified Features of the Selected File Recovery Forensic Tools

This section explains all the identified features across the three selected file recovery forensic tools: Recuva, Puran File Recovery, and EaseUS Data Recovery tools. This is expressed in Table 1, which shows the total number of sixteen (16) features. These are:

- Easy to Install and Compatible with Windows: This feature is found across all three selected file recovery forensic tools. It is compatible with the Windows operating system used for the analysis, making it easy to install and for forensic investigators to use.

- User-friendly Interface: All three selected file recovery forensic tools were identified with a simple user interface that enables forensic analysts to navigate and analyze the selected drive intended to be analyzed to obtain accurate results in recovering deleted files.
- Search Key Feature: This feature is identified across all three selected file recovery forensic tools as it makes it easier for forensic analysts to search for particular file types, such as documents, pictures, and so on, when performing the analysis.
- File Type: This feature explains the file type found in each selected file recovery forensic tool. File types discovered using the Recuva tool include pictures, music, documents, video, compressed files, and emails. The file types identified when using the Puran file recovery tool were picture, music, documents, video, compressed, and all files, while picture, music, documents, video, compressed, archives, emails, bookmarks, other files, and unsaved files were found in the EaseUS data recovery tool. This discovery helps forensic analysts understand the group of files that these tools can capture during analysis.
- Level of Scan to Perform: This feature shows the level of scan each of the selected file recovery forensic tools can perform when analyzing the seized storage device by the forensic investigator. It was discovered that the Recuva tool has a deep scan feature if enabled by the forensic analyst, to obtain and recover detailed information (deleted files) on the given storage device. The Puran file recovery tool has both deep (full) scan features. The Recuva tool also identified the deep scan feature, which helps check every file and folder on the seized USB drive.
- File Path: This feature means the path to a file from the root directory of a file system (USB drive) used for the analysis. This feature was identified in all the selected file recovery forensic tools.
- File Size: This feature shows the amount of storage space the deleted files take up on the seized USB storage device.
- Condition of the File: This feature shows the state of the deleted file to be recovered using the file recovery forensic tools. In the Recuva tool, the state of the deleted was categorized into three groups, namely: excellent state (file is in a very good state for recovery), poor (file can be recovered but not of high quality), very poor (file may not be fully recoverable), and unrecoverable (file cannot be recovered at all due to being corrupted). The states identified in the Puran file recovery tool were grouped into excellent, good, and poor. While there was no specificity in the file state, using EaseUS data recovery**.**
- File Preview: This feature is found across all the selected file recovery forensic tools. It helps the forensic investigator preview files using the chosen tool to correctly identify a particular file, such as images.
- Language Options: This feature is found across all the selected file recovery forensic tools, and it shows lists of several language options that forensic investigators can choose from based on the country to help in obtaining well-explained reports to be admissible in a court of law
- Shows the Drive Name and its Location to be Scanned: This feature shows the drive name (USB storage device) intended for analysis by forensic analysts. It is found across all the selected forensic tools.
- File System: This feature is described as a method used by an operating system to organize and manage files and directories on a USB storage device. This is identified across all the selected file recovery forensic tools as File Allocation Table (FAT32) file system type, which is a file system commonly used for smaller storage devices, such as USB flash drives.
- Total Space and Free Space**:** All the selected forensic tools show the total space on the seized USB storage device, which was 7.45GB and found across all the selected forensic tools.
- Recover Files to a Selected File Path: all the selected forensic tools have the navigation path (directory) to which each recovered file can be saved, which was created by the forensic analysts.
- Time Spent on the Analysis: This means the total amount of time spent by each of the selected forensic tools in analyzing the seized USB drive. The Recuva tool spent a total of 6 minutes 33 seconds analyzing the drive, the Puran file recovery tool spent 5 minutes 20 minutes analyzing the drive, and the EaseUs data recovery tool spent 9 minutes 29 minutes analyzing the seized drive.

- File Last Modified: This feature shows the time and date when the deleted file on the USB drive was modified to help forensic investigators obtain accurate reports. This feature was identified with the Recuva tool only.

Table 1. Identified features across the selected file recovery forensic tools

Identified Features	Recuva	Puran file recovery	EaseUS data recovery
Easy to install and compatible with Windows	Yes	Yes	Yes
User-friendly interface	Yes	Yes	Yes
Search key feature	Yes	Yes	Yes
File type	Pictures, music, documents, video, compressed, and emails	Pictures, music, documents, video, and compressed files	Picture, music, documents, video, compressed archives, emails, bookmarks, other files, and unsaved files
Level of scan to perform	Deep scan	Deep scan	Deep
File Path	Yes	Yes	Yes
File Size	Yes	Yes	Yes
Condition of the file	Yes (excellent, poor, very poor, unrecoverable)	Yes (Excellent, good, and poor)	Not specified
File Preview	Yes	Yes	Yes
Language options	Yes	Yes	Yes
File Metadata (header)	Yes	Yes	
Shows the drive name and its location to be scanned	Yes	Yes	Yes
File system	FAT32	FAT32	FAT32
Total Space and Free Space	Yes	Yes	Yes
Recover Files to a Selected File path	Yes	Yes	Yes
Time spent on the analysis	6min. 33secs	5min 20secs	9min 29secs
File Last Modified	Yes	No	No

4.2. The Original Files Created and Identified on the USB Storage Device

On the (captured) seized USB drive, which is a storage device used for conducting analysis, a total of eighteen (18) files were copied and identified. The identified file type was grouped into five categories: documents, audio files, video files, image (picture) files, and compressed files.

Under the document file type category on the USB storage device, there exist three (3) Microsoft Word document (.doc) files which is a word processing application that allows users to create, edit, format, and share

text-based documents, two (2) PDF (Portable Document Format (.pdf)) files which have a Universal Compatibility, one (1) Microsoft Excel documents(.xls), two (2) power points documents (.ppt) and one (1) text document(.txt). For the audio file type, only two files were identified on the seized device (.mp3), three (3) video files (.mp4), three (3) image files (.png, jpg), and one (1) compressed file (.rar), which is a zipped file.

Table 2. The identified files by each selected forensic tool

The identified deleted file type		Recuva	Puran file recovery	EaseUS data recovery
Documents	doc file	3	3	3
	Pdf file	2	2	2
	Pptx file	2	1	2
	Xls file	1	1	1
	Txt file	0	0	1
Audio file		1	2	2
Video file		1	3	1
Image file		2	3	3
Compressed file		1	1	1

4.3. Explanation of the Recovered and Unrecovered Files

Table 3 illustrates the proportion of recovered and unrecovered files using the three selected file recovery forensic tools from the seized USB drive. Generally, the total number of deleted files identified on the storage device was eighteen (18) files. The recovered files were divided into two categories: correctly recovered and incorrectly recovered. The correctly recovered files are the files that are successfully recovered using the selected file recovery forensic tools, showing the exact content of the deleted files, while the incorrectly recovered files are the files that are not fully recovered, thus, the recovered files do have the exact file content of the deleted file. The unrecovered files are the files that cannot be recovered at all due to being overwritten or corrupted.

The Recuva forensic tool is discovered to have a total number of thirteen correctly recovered files and five (5) unrecovered files. For the Puran file recovery forensic tool, a total number of sixteen files were correctly recovered while two (2) files were unrecovered, and finally, for the EaseUs data recovery tool, a total number of fourteen(14) files were correctly recovered, one file(1) was incorrectly recovered, and three(3) files were unrecovered.

Table 3. Recovered and unrecovered files

The Selected Forensic Tools	Recovered Files		Unrecovered Files
	Correctly	Incorrectly	
Recuva	13	0	5
Puran file recovery	16	0	2
EaseUS data recovery	14	1	3

4.4. The Selected Performance Metrics

The performance metrics used in evaluating the effectiveness of each of the chosen file recovery forensic tools include:

4.4.1. Recovery Rate (RR)

This performance metric calculates recovery effectiveness metrics. It is obtained by measuring the proportion of deleted files successfully recovered.

$$RR = \frac{\text{Number of successfully recovered files}}{\text{Total number of deleted files}} \times 100\%$$

4.4.2. File Type Success Rate

Measures how effectively a recovery method restores deleted files based on their type (e.g., images, videos, and documents). It helps identify which file types are more or less recoverable using a given method

$$\text{success rate} = \frac{\text{recovered files of type}}{deleted\ files\ of\ the\ same\ type} \times 100\%$$

4.4.3. File Size Recovery Rate

A metric measures how much of the total deleted file data (in terms of size) is successfully recovered. It provides insight into the effectiveness of a file recovery method, particularly when dealing with different file sizes.
Small files (<10MB), medium files 10- 100 MB vs. Large files (>100MB)

$$\text{FSRR} = \frac{\sum \text{Recovered File Sizes}}{\sum \text{delected File Sizes}} \times 100\%$$

4.4.4. Speed Recovery Time

This is the total time required to recover deleted files using a specific recovery method. It measures the efficiency of the recovery process in terms of the time taken to retrieve lost data. It measures the total time required to complete the recovery process.

$$\text{Time (s)} = \text{End time} - \text{Start time}$$

4.4.5. File Hash Matching (Data Integrity and Accuracy Metrics)

It is a technique used to verify the integrity and accuracy of recovered files by comparing their hash values before and after deletion/recovery. If the hash values match, it confirms that the recovered file is identical to the original file without corruption or modification. It compares hash values (e.g., MD5, SHA-256) of recovered files against their original versions to verify data integrity.

$$\text{Match rate} = \frac{\text{Files with matching hashes}}{Total\ recovered\ files} \times 100$$

Table 4 describes the obtained results using the selected file recovery performance metric in evaluating the effectiveness of each of the file recovery forensic tools.

The Recovery Rate (RR) is a performance metric for evaluating the selected file recovery forensic tools. The recovery performance rate of 72.22% was obtained when analyzing the deleted files on the Recuva tool, of which thirteen (13) files out of the total number of eighteen (18) files deleted on the seized USB drive were recovered. The recovery performance rate of 88.89% was obtained during the analysis of the identified deleted files in the Puran file recovery tool, hence showing that a total number of sixteen (16) files out of eighteen (18) files were recovered while the EaseUs data recovery tool, the recovery performance rate of 77.78% was obtained of which a total number of fourteen (14) out of eighteen (18) files were recovered from the USB drive.

File type success rate is another selected performance metric adopted in assessing the selected file recovery forensic tools. The file type success rate of 88.89% was obtained using the Recuva and the Puran file recovery tools, in which eight (8) out of a total number of nine (9) file types were recovered. In comparison, the file type success rate of 77.78% was obtained using the EaseUS data recovery tool, which indicates that seven (7) out of nine (9) file types were recovered.

In evaluating the file size recovery rate, a total number of 124 MB file size (summation of 13 recovered file sizes) out of a total number of 187 MB file size (summation of 18 deleted file sizes) was obtained, equivalent to 66.31%. In

assessing the effectiveness of Puran file recovery, a total number of 296MB file size (summation of 16 recovered file sizes) was calculated, and the total number of 187 MB file size was the summation of all 18 deleted file sizes.

This clearly shows that the recovered files generated larger file sizes than the original deleted file size. Lastly, in the EaseUS data recovery tool, the file size recovery rate of 27.86%, which is the summation of fourteen (14) recovered files out of eighteen (18) deleted files, was obtained, equivalent to the proportion of 52.1MB out of 187MB file size. This shows that the file size of the recovered files was small compared to the original deleted file size on the seized USB drive.

The next performance metric adopted was the speed of recovery time, which means the total amount of time taken by each of the selected file recovery tools to recover the deleted files on the seized USB drive. It took the Recuva tool 6min. 33 secs for the file recovery, and the Puran file recovery tool took 5min 20secs, while 9min 29secs was spent by the EaseUS data recovery tool in recovering the deleted files. This shows that the Puran file recovery tool is the fastest of the three forensic tools, followed by the Recuva tool, while the EaseUS data recovery tool is the slowest of the three selected tools.

Finally, the file hashing matching metric was used to assess the matching (data integrity) rate of the recovered files in comparison to the deleted files using the HashMyFiles software. This involves comparing recovered and deleted files hash value by viewing the MD5 and SHA-256 hash values.

A file hash matching rate of 84.62% was obtained using the Recuva tool, 56.25% file hash matching was obtained using the Puran file recovery tool, and a 73.33% file hash matching rate was obtained using the EaseUS data recovery tool. This shows that the Recuva tool is identified with the highest file hash matching rate of 84.62%, followed by the EaseUs data recovery tool with 73.33%, and the Puran file recovery tool shows the tool the lowest file hash matching rate of 56.25%.

Table 4. The results obtained using the selected Performance metrics

File Recovery Performance Metrics	Selected Forensic Tools		
	Recuva	**Puran File Recovery**	**EaseUS Data Recovery**
Recovery Rate (RR)	$\frac{13}{18}$×100 = 72.22%	$\frac{16}{18}$×100 = 88.89%	$\frac{14}{18}$×100 = 77.78%
File Type Success Rate	$\frac{8}{9}$x 100 = 88.89%	$\frac{8}{9}$x 100 = 88.89%	$\frac{7}{9}$x 100 = 77.78%
File Size Recovery Rate	$\frac{124(MB)}{187(MB)}$x 100 = 66.31%	$\frac{296(MB)}{187(MB)}$x 100 = 158.29%	$\frac{52.1(MB)}{187(MB)}$x 100 = 27.86%
Speed Recovery Time	6min. 33secs	5min 20secs	9min 29secs
File Hash Matching	$\frac{11}{13}$x 100 = 84.62%	$\frac{9}{16}$x 100 = 56.25%	$\frac{11}{15}$x 100 = 73.33%

Table 5 explains the comparative results obtained from the three selected data recovery forensic tools, namely Recuva, Puran file recovery, and EaseUs data recovery tools to an existing related work done by Putra et al. [27] which involves the use of Recuva and EaseUS Data Recovery Wizard tools for recovery data on the computer system and the overall performance result indicated that EaseUs data recovery wizard was identified as the best in retrieving lost or deleted information or formatted documents. The analysis done by Putra et al. only focuses on analyzing the chosen file recovery tools to determine the Causes of Data Loss, File Type (Email, encrypted, compressed, picture), and Supported File System (FAT, NTFS, RAW).

This current research paper focused on analyzing the selected file recovery tools based on performance metrics to determine their effectiveness and achieve better results. The results show that the Puran File Recovery achieved the highest recovery rate (88.89%), Both Recuva and Puran had the highest file type success rate of 88.89%, EaseUs,

recovering 14 files with a 27.86% success rate, consumed the least memory, making it the most space-efficient tool for forensic analysts, Puran was the fastest, recovering files in 5 minutes and 20 seconds while EaseUs excelled in file hash matching with an accuracy rate of 84.62%.

Table 5. Comparing the obtained results with the existing related works

Author(s)	Data Recovery Tools Used	Performance Results
[27]	Recuva and EaseUS Data Recovery Wizard	EaseUS Data Recovery Wizard was identified as the best **for** retrieving lost or deleted information or formatted documents.
This paper	Recuva, Puran file recovery, and EaseUS data recovery tool	Puran File Recovery achieved the highest recovery rate (88.89%). Both Recuva and Puran had the highest file type success rate of 88.89%, EaseUs, recovering 14 files with a 27.86% success rate, consumed the least memory, making it the most space-efficient tool for forensic analysts; Puran was the fastest, recovering files in 5 minutes and 20 seconds while EaseUs excelled in file hash matching with an accuracy rate of 84.62%

5. Conclusion and Future Recommendations

In conducting an in-depth forensic analysis on the seized (set-aside) USB flash drive of 8GB file size using three selected file recovery tools, namely the Recuva, the Puran file recovery, and the EaseUs data recovery tools based on their widely used and their functions, an experimental research methodology type was selected that involves conducting systematic investigations under controlled conditions to analysis starting from the data preparation on the USB, to the examination, analysis and full report of forensic investigation conducted.

Eighteen (18) files comprising documents, audio, video, and compressed files were identified on the flash drive, and sixteen (16) features were generally identified across the selected forensic tools. In the recovery of files using the selected file recovery tools, a total number of thirteen (13) out of eighteen (18) files were correctly recovered, five (5) files were unrecovered in the Recuva tool, sixteen (16) files were correctly recovered and two (2) files were unrecovered in the Puran file recovery tool, while fourteen (14) files were correct, one (1) file was incorrectly recovered and three (3) files were unrecoverable. To effectively evaluate the performance of the three selected file recovery tools, some performance metrics were employed, including Recovery Rate (RR), File Type Success Rate, File Size Recovery Rate, Speed Recovery Time, and file Hash matching rate. It was discovered that the Puran file recovery tool shows the highest recovery rate of 88.89%, followed by the EaseUs data recovery tool with a 77.78% recovery rate, while the Recuva tool has 72.22%, and this shows that the Puran file recovery tool works best in determining the recovery rate of the deleted file on the USB device.

In the calculation of the file type success rate, the Recuva and the Puran file recovery tools had the highest rate of 88.89%, while the EaseUs tool had 77.78%, and this shows that both the Recuva and the Puran can used effectively to determine the file type success rate of deleted files when conducting forensic analysis. In evaluating the file size recovery rate (296 MB/187 MB file size), 158.29% was obtained using the Puran file recovery, which was the total file size for the sixteen (16) files recovered. This shows that the tool consumes more file size (memory space) to recover deleted files. A file type success rate of (124 MB/187 MB) 66.31% was achieved using the Recuva tool in recovering thirteen (13) files. This shows that Recuva does not consume much memory in the recovery of files when compared with the Puran file recovery tool, while a 27.86% file type success rate was obtained using the EaseUS tool for a total number of fourteen (14) recovered files.

This shows that the EaseUS tool has the lowest file size for the recovery files compared with the Puran and Recuva tools, which makes it preferable for use by forensic analysts. In terms of speed recovery time, the Puran file recovery shows the shortest time of 5min 20secs in recovery files, followed by the Recuva tool, which took 6min. 33 secs and the EaseUs tool is the slowest, with 9 minutes and 29 seconds. Finally, in terms of the file hash matching rate, Recuva shows the best result of 84.62%, followed by the EaseUS data recovery tool with 73.33%, and the Puran file recovery tool shows 56.25%

For future work, it is recommended to expand the study by including a broader range of file recovery tools to gain deeper insights into their effectiveness across various file types and storage conditions. Additionally, examining the impact of anti-forensic techniques, such as secure deletion and data obfuscation, can provide a better understanding of their effects on file recoverability. Integrating machine learning techniques into forensic analysis could enhance the accuracy and efficiency of file recovery by identifying patterns in deleted data. Furthermore, evaluating recovery tools on encrypted USB devices and across different operating systems would improve forensic preparedness for complex scenarios.

Data Availability

All details about the forensic analysis results of each selected data recovery forensic tool are available on request.

Acknowledgments

I am deeply grateful to the Almighty God for His divine guidance, illuminating my path and inspiring my work. I also extend my sincere appreciation to the DS Journal of Cyber Security (DS-CYS) for their invaluable feedback and constructive suggestions, which have significantly enhanced the clarity and impact of my research.

References

[1] Lena Klasén, Niclas Fock, and Robert Forchheimer, “The Invisible Evidence: Digital Forensics as Key to Solving Crimes in the Digital Age,” *Forensic Science International,* vol. 362, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[2] Krishna Sanjay Vaddi et al., “Enhancements in the World of Digital Forensics,” *International Journal of Artificial Intelligence,* vol. 13, no. 1, pp. 680- 686, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] Daniel Septianto, Lukas, and Bagus Mahawan, “USB Flash Drives Forensic Analysis to Detect Crown Jewel Data Breach in Pt. XYZ (Coffee Shop Retail - Case Study)," *IEEE 9th International Conference on Information and Communication Technology*, Yogyakarta, Indonesia, pp. 286-290, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] Luge Yang, "A Research on USB Device Remote Sharing Methods in Virtual Desktop Environment," *IEEE 9th International Symposium on System Security, Safety, and Reliability*, Hangzhou, China, pp. 391-397, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] Ruwa F. Abu Hweidi et al., "SATA M.2 on Forensics: Trim Function Effect on Recovering Permanently Deleted Files," *International Conference on Smart Applications, Communications and Networking*, Istanbul, Turkiye, pp. 1-6, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] Julian Melo, Different Types Of USB Flash Drives, 2023. [Online]. Available: https://www.usbmemorydirect.com/blog/different-types-of-usb-flash-drives/?srsltid=AfmBOopQOm4qUprEWEMLs_kUzELm3503sYPmP9kmxN6mgVyu7HuJ7Ssg

[7] K. Nikhil, S.A. Hariprasad, and B. Aditya, "Comparative Study on Various File System Implementations on Different OS," *International Research Journal of Engineering and Technology (IRJET),* vol. 8, no. 11, pp. 1186 -1196, 2021. [Publisher Link]

[8] Hao Liu et al., “USB Powered Devices: A Survey of Side-Channel Threats and Countermeasures," *High-Confidence Computing*, vol. 1, no. 1, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Mohit Kumar Jha, USB Forensics: Ultimate Guide to Device, Drive & Data Analysis, Forensics, 2024. [Online]. Available: https://www.mailxaminer.com/blog/usb-forensics/

[10] Anguilano, 5 Factors to Consider When Attempting to Recover Deleted Data from Hard Drives, 2023. [Online]. Available: https://www.tcdi.com/5-factors-to-consider-when-attempting-to-recover-deleted-data-from-hard-drives/

[11] Kalpana Shinde et al., "Determining the Probability of Recovering Data from Damaged USB Flash Drive," *International Journal of Engineering and Advanced Technology*, vol. 8, no. 5S3, pp. 179-191, 2020. [CrossRef] [Publisher Link]

[12] Ngozi Tracy Aleke, and Mohamed Trigui, "Legal and Ethical Challenges in Digital Forensics Investigations," *Digital Forensics in the Age of AI*, pp. 147 -175, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[13] Rashmi Mandayam, "Ethical Considerations in Digital Forensics," *International Journal of Innovative Research in Engineering and Multidisciplinary Physical Sciences*, vol. 13, Issue 1, pp. 1-4, 2025. [CrossRef] [Publisher Link]

[14] Jihun Joun, Sangjin Lee, and Jungheum Park, "Discovering Spoliation of Evidence through Identifying Traces on Deleted Files in macOS," *Forensic Science International: Digital Investigation*, vol. 44, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] Deepak Raj Rao, Sonu Mandecha, and Kumarshankar Raychaudhuri, "An Empirical Study of Digital Forensic Tools and Techniques for Detection of Traces of Anti-Forensic Activities of Usb Devices in Windows," *Open Access International Journal of Science and Engineering*, vol. 5, no. 6, pp. 1-7, 2020. [Publisher Link]

[16] Bandr Siraj Fakiha, "Forensic Analysis of Bad Usb Attacks: A Methodology for Detecting and Mitigating Malicious Usb Device Activities," *Edelweiss Applied Science and Technology*, vol. 8, no. 5, pp. 1090-1100, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] Rashi Karnewar, and Arya Chahankar, "Data Recovery in Digital Forensics," *International Journal of Innovations in Engineering and Science*, vol. 9, no. 8, pp. 29-33, 2024. [Publisher Link]

[18] Varun Reddy Kondam, "Comparing SSD Forensics with HDD Forensics," *Culminating Projects in Information Assurance*, pp. 1-107, 2020. [Google Scholar] [Publisher Link]

[19] I Putu Agus Eka Pratama, " Computer Forensic using Photorec for Secure Data Recovery Between Storage Media: A Proof of Concept," *International Journal of Science, Technology and Management*, vol. 2, no. 4, pp. 1189-1196, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] Sai Niveditha Varayogula et al., "Computer Forensics Data Recovery Software: A Comparative Study," *International Journal of Innovative Research in Computer Science and Technology*, vol. 10, no. 2, pp. 513-518, 2022. [Google Scholar] [Publisher Link]

[21] Zawar Shah et al., "Forensic Investigation of Remnant Data on USB Storage Devices Sold in New Zealand," *Applied Sciences*, vol. 12, no, 12, pp. 1-29, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[22] Muhammad Fahmi Abdillah, and Yudi 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. [CrossRef] [Google Scholar] [Publisher Link]

[23] Kausalyani A/P Angamutu, Nor Azlina Abd Rahman, and Nik Nurul Ain Nik Suki, "A Customized Data Recovery Tool," *Journal of Physics: Conference Series*, vol. 1712, 2020. [CrossRef] [Publisher Link]

[24] William Bollson, Puran File Recovery Review in 2025: Is It Worth Trying?, 2025. [Online]. Available: https://4ddig.tenorshare.com/windows-recovery-solutions/puran-file-recovery-review.html

[25] Benedict Collins, Best Data Recovery Software of 2025, 2025. [Online]. Available: https://www.techradar.com/best/best-data-recovery-software

[26] Shengyu Li et al., "Watch Out Your Thumb Drive: Covert Data Theft from Portable Data Storage Via Backscatter," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 4, pp. 2434-2447, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[27] Ade Putra, Muhammad Donni Lesmana Siahaan, and Arpan Arpan, "Comparative Analysis of Data Recovery Using Easeus Data Recovery Wizard and Recuva Applications," *INFOKUM*, vol. 10, no. 3, pp. 161-165, 2022. [Google Scholar] [Publisher Link]