The Forensic Significance of Indexing Applications on the Windows Operating System

I. Špoljarić, D. Delija, G. Sirovatka
Zagreb University of Applied Sciences, Zagreb, Croatia
ispoljaric@tvz.hr, ddelija@tvz.hr, gsirovatka@tvz.hr

***Abstract* - When forensic analysis of the Windows operating system and the search for the existence of suspected files, applications, or artifacts of the operating system, the process of restoring deleted data is very often hard drives (SSD) SATA or NVMe interfaces in personal computers and taking into account properties such as wear leveling and garbage collection solid state hard drives, it is significantly difficult to recover deleted data as well as proving the start and presence of suspected files on the computers of the attacker or victim. This article analyzes the Windows Windows Search feature with a linked Windows.edb file as well as the 3rd Party application for indexing operating system files to find records of suspect files, metadata, applications, and their activities relevant to forensic analysis.**

Keywords – digital forensic; Windows indexing system; database; file recovery tools; record recovery tools.

I. INTRODUCTION

Digital forensics is defined as „The process used to acquire, preserve, analyze, and report on evidence using scientific methods that are demonstrably reliable, accurate, and repeatable such that it may be used in judicial proceedings" [1]. In such context, forensic artifacts are items that get left behind based upon the activities of the end user of the device, and digital evidence is any digital artifacts that can prove or disapprove forensic hypothesis.

Digital forensic analyses of Windows artifacts are a complex and difficult task in an all-time changing environment, especially artifacts related to proprietary databases and indexing systems, with very scarce documentation which often lags versions behind the current state of the analyzed Windows tools.

This article highlights the significance of different indexing bases and mechanisms of Windows operating system in terms of retrieving and extracting artifacts. Additionally, it also presents a comparison of the databases containing specific artifacts. The key element for an efficient approach with such artifacts is cooperation among practitioners and sharing of acquired knowledge through available online forums and workgroups.

There is a common path to how this knowledge is incorporated into digital forensics legally acceptable practice. This path covers a distinguished set of steps

- Initial recognition of new features in the forensic process;
- Feature analyses based on the malware analyses – identification of artifacts and importance of these artifacts;
- Development of forensic tools and procedures for acquiring and analyses of these new artifacts
- Testing and proving of forensic tools and procedures;
- Peer review and in-community proofing;
- Legal acceptance and proofing in court during some legal cases (US-specific);
- Incorporation of artifacts into commercial tools and education curriculums [7].

New features appear in Windows as a part of the new version of the operating system or through patch or service pack updates [6]. Documentation that exists is, from the forensic viewpoint, scarce and imprecise, presenting only a user or system administrator view on that feature, lacking specific implementation data, like internal application structure, database organization, and structure meaning of different fields. In practice, all implementation data which is often defined as a company intellectual property not available outside of the development department. It often takes about 6 months up to a year to get new feature support into commercially available software, leaving a period of‘uncertainty “ while practitioners are on their own in accessing and interpreting the „new“forensic artifacts.

II. FORENSIC VALUES OF INDEXING SUBSYSTEM

On the current version of the Windows operating system, several indexing applications are operational. The main goal of all these applications is to efficiently store metadata about files on the computer to simplify the search and organization of the file content.

Forensic analysis of indexing applications like Windows Search feature and 3td Party applications like Everything and Locate32 can provide many advantages for digital forensic experts during digital investigations. Windows Search feature save indexed data in Windows.edb file, Everything application save indexed files and folders in the proprietary database on the local machine and Locate32 application save indexed data to the PostgreSQL database on a local hard drive Mentioned applications can help experts and investigators to quickly find specific files on a Windows system, possibly prove the persistence of specific files, and provides additional information like file metadata such as dates, sizes, or type. In this paper, we analyzed three applications, Windows

Search (Windows.edb file), Everything application, and Locate32 application.

III. FORENSIC ANALYSIS

A. *Windows.edb file*

In forensic investigations, the "Windows.edb" [1] is located in „C:\ProgramData\Microsoft\Search\Data\Applications\Windows\" and the file is often analyzed in combination with other data sources, such as Windows Event Logs and users activity logs from Windows Registry hive "NTUSER.dat", to provide a comprehensive understanding of a subject's activities on a computer. However, due to the complexity and size of the file, its analysis typically requires specialized software, like ESEDatabaseView [2] from Nirsoft (https://www.nirsoft.net/utils/ese_database_view.html) or WinSearchDBAnalyzer [3] (https://github.com/moaistory/WinSearchDBAnalyzer). The "Windows.edb" store valuable information about the activities and data stored on a Windows computer [8]. The file can be used to:

-Identify recently accessed files, emails, and other content;

-Track user activities, such as email communication and file transfers;

-Retrieve deleted or lost files and email messages that may have been overlooked during the normal deletion process.

The frequency of re-indexing data in the "Windows.edb" file depends on the specific configuration and settings of the Windows Search service in the Windows Operating System. By default, the Windows Search service continuously indexes and updates the "Windows.edb" database in real-time, adding new files and folders and updating information as they are created, modified, or deleted. Despite this, users are not satisfied with the capabilities of the Windows Search feature, and new, 3rd party applications like Everything and Locate32 have been created.

To open the "Windows.edb" file for forensic analysis, we used a combination of specialized forensic software and native Windows tools, followed by these steps:

1. Mount the image of the hard drive containing the "Windows.edb" file.
2. Use a forensic software tool, such as EnCase, Xways Forensics, or FTK to create a bit-by-bit image of the drive, which will preserve the original file system structure and contents of the file.

Use a Nirosft „ESE Database Viewer“, version 1.71, to view the contents of the "Windows.edb" file.

In some situations recovery of "Windows.edb" is required, for such purposes extracted database can be accessed and recovered in a forensically sound way by the Microsoft tool esenutl.exe as it is shown in Figure 1. This process should be well documented and screenshots were taken to prove that the procedure was followed correctly and no unwanted changes were done to the data in the database.

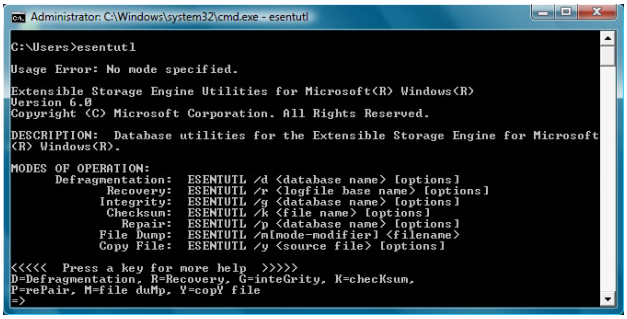

Figure 1: Recovery of the „Windows.edb“ through „esentutl.exe“ utility.

B. *Everything application*

The "Everything" application can be an important tool from a forensic perspective and it can provide valuable information about the user and system files and content stored on a computer. In addition, "Everything" stores a cache of its search results, which can be useful in reconstructing a timeline of activities and accessing information that may have been lost or deleted from the Windows file system. The Everything application stores its indexed data in a local database file named "everything.db". This file is typically stored in the same directory as the Everything executable file and is automatically created and updated when the application is run. The data stored in the "everything.db" file includes information about all the files and folders on a system, such as file names, paths, sizes, and dates. The database is designed to be fast and efficient, allowing the Everything application to quickly search for and display results based on a user's query.

The "Everything" database is a proprietary file format that is not designed to be opened or read directly. To access and search the "Everything" database, you need to use the "Everything" application.

In general, the data indexed by the Everything application will remain persistent as long as the underlying file system remains intact. The Everything application uses an NTFS-specific Master File Table (MFT) search algorithm, which is designed to be fast and efficient and to provide real-time results. However, if the file system is damaged or corrupted, or if files are deleted or otherwise changed, the indexed data in the Everything application may become outdated and may no longer accurately reflect the current state of the file system. In these cases, the Everything application will typically need to be re-indexed to update the indexed data and ensure that it remains accurate. The persistence of data in the Everything application depends on several factors, including the configuration of the application and the storage location of the indexed data. This means that the entries for deleted files and folders will remain in the database until the "Everything" application is re-indexed or until the database is manually cleared.

C. *Locate32 application*

Locate32 application version 3.1.11.7100, written by Janne Huttunen [3] is a free and open-source file indexing and searching application for Windows operating systems. It's designed to quickly locate files on a computer or network by indexing and storing the location of files and their metadata in a .dbs database file. Locate32 can be used to search for specific files or folders by name, date, size, or other metadata attributes. Locate32 support basic search functionality and advanced features, such as regular expression matching, support for networked file systems, and the ability to export search results to various file formats for further analysis.

Indexed data Locate32 save in a .dbs database on the local system (C:\Users\Username\Appdata\Roaming\Locate32\) where the application is installed. The default location for this database file is in the user's profile directory, in the folder named "locatedb". The database file is typically named "file.dbs" and contains the index of all the files and their metadata that have been indexed by Locate32. Some users may choose to store the database file on a network drive or other location to allow searching across multiple systems. Locate32 allows forensic analysts to export search results to various file formats, such as CSV or HTML, for further analysis or reporting.

D. *Indexing application comparison*

When comparing the "Windows.edb" file, Locate32, and Everything application in terms of forensic value, the following points can be considered:

•"Windows.edb" file: The "Windows.edb" file is a database file used by the Windows Search service to store information about indexed files and metadata. It can be valuable in forensic investigations as it contains information about files and their locations, which can be used to identify and analyze relevant data.

•Locate32: Locate32 is a search tool for Windows that creates and maintains a database of all files and folders on a system. This database can be searched quickly to locate specific files, making it useful in forensic investigations where time is a critical factor.

•Everything: Everything is a file search tool for Windows that uses a high-performance file search algorithm to quickly search and display files and folders. It can be useful in forensic investigations as it provides a fast and efficient way to search for specific files and folders on a system.

When running Everything, the application stores search data in the database "Everything.db", located in „C:\Users\<userprofile>\AppData\Local\Everything" and „Run History.csv" file located in the folder „C:\Users\ <userprofile>\AppData\Roaming\Everything\". In the "Everything.db" database we can find information about indexed files, while the "Run History.csv" file contains information about files searched using the Everything application, the number of times files were started or opened (Run Count), and the Last run time of applications, stored in Windows File Time format. If we compare the data about the launch of a single file from Run History.csv and the Windows Prefetch artifact, in our case we got additional information since Everything can store much older data, more precisely from the moment of Everything application installation, while the Windows Prefetch artifact store only 8 runs timestamp data.

TABLE I. INDEXING APPLICATIONS FEATURE COMPARISON

Indexing feature / Application name	**Windows.edb**	**Everything**	**Locate32**
Folders (System and users)	yes	yes	yes
Files (System and Users)	yes	yes	yes
Internet Links	yes	(partial – parsing from the browsers database)	(partial – parsing from the browsers database)
Network Drives	yes	yes	yes
File and Folders Timestamps	yes	(partial – only last write time)	(partial – only last write time)
LNK files	yes	yes	yes
Audio, Video and Pictures	yes	yes	yes
Hidden System Files (hiberfil.sys, $MFT, pagefile.sys, etc)	yes	yes	yes

In Table I, the relevance of the forensic artifacts stored in different indexing applications is presented. It is important to notice that databases present the state of the artifact or the content of the artifact in the moment of indexing even in the situation when a file or data was later removed from the system, like in the situation when a file was erased or email removed. Also, it is important to stress that indexing databases are also available through system restore points and backups if backups are done. System restore points are a much more reliable mechanism to access an earlier version of indexing databases on Windows systems. In this situation, the only additional step is to access the restore point through forensic software, which is well described the standard practice and extracts the previous version of index database files.

IV. FUTURE DEVELOPMENT

As the size of the disk grows up indexing applications become more and more important to accessing local and also remote data on networked or cloud environments. Also, these applications are performance issues In the situation where multiple indexing applications exist on the same system, with radically different infrastructures varying from property database systems like edb to open-source ones like PostgreSQL. It is reasonable to expect rationalization to simplify things and narrow down attack surfaces that different database systems provide.

It is uncertain in which way this effort will go, especially if the current development of AI services like chatGPT is taken into account, probably additional modifications to indexing systems will be developed with an integrated AI interface. This will again require a whole new forensic cycle probably much longer than the current one to get support for the whole new class of artifacts.

V. CONCLUSION

Forensic analysis of Windows.edb file, Everything application, and Locate32 application can provide valuable information and evidence in digital investigations. Windows.edb file is a database file that stores information about all the files and folders on a Windows operating system, which can help investigators track changes, recover deleted files, and gather evidence of illegal or unauthorized activity. The Everything application is a fast and efficient search tool that can quickly search for files and folders, even in large data sets, which records the total number and last run time of launching applications from the Everything application, and record persistence are not time-limited, only depends on the date of installation. While the Locate32 application is a search tool that can help investigators, after a mounting suspected hard drive, quickly find specific files based on various criteria such as date, size, or type and easily export findings to a human-readable file. Findings from these tools can help investigators to efficiently and effectively analyze and find files or file artifacts on the Windows Operating System, reconstruct timeline and user activities, and provide valuable information for investigation [5].

REFERENCES

[1] W. Oettinger: „Learn Computer Forensics“, Packt Publishing, 2020.

[2] NISoft: ESEDatabaseView v1.72 https://www.nirsoft.net/utils/ese_database_view.html (visited 05.01.2023.).

[3] Winsearchdbanalyzer https://github.com/moaistory/WinSearchDBAnalyzer (visited 05.01.2023.).

[4] Locate32 https://locate32.cogit.net/ (visited 05.01.2023.).

[5] O.Skulkin, S.Sourcier: “Windows Forensics Cookbook“, Packt Publishing, 2019

[6] Sans: „Digital Forensics and Incident Response“ https://www.sans.org/digital-forensics-incident-response/, / (visited 05.01.2023.)

[7] D.Delija,I.Špoljarić,G.Sirovatka: „Preparation and Planning of the Development of a Proficiency Test in the Field of Digital Forensics“, 2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO), ISSN: 2623-8764

[8] H.Chivers,C.Hargreaves: „Forensic data recovery from the Windows Search Database”, https://eprints.whiterose.ac.uk/75046/1/Forensic_Data_Recovery_From_The_Windows_Search_Database_preprint_DIIN328.pdf, (visited 05.01.2023.).