Forensic Analysis of Windows 11 Prefetch Artifact

Akash Budhrani
Computer Science and Engineering Department
Defense Institute of Advanced Technology
Pune, India
akashbudhrani12@gmail.com,

Upasna Singh
Computer Science and Engineering Department
Defense Institute of Advanced Technology
Pune, India
upasnasingh@diat.ac.in,

Bhupendra Singh
Computer Science and Engineering Department
Indian Institute of Information Technology
Pune, India
bhupendra@iiitp.ac.in

***Abstract*— The Operating System creates numerous objects to improve its efficiency and user experience and such objects are called artifacts. These artifacts record crucial data about the user activity. Such artifacts are the start point of any investigation as they can be an additional lead to a forensic triage. Prefetch file is one among various objects, presence of which confirms the execution of a particular application. Prefetch gives additional inside for the purpose of investigation. Thus, this paper brings out the forensic value of it, the tools required to decode the information it contains and also look in various caveats in interpreting this artifact to learn its strength and weaknesses to properly incorporate in support of opinion derived by the analyst. In this work, Prefetch is forensically examined to bring out its forensic value, knowledge it contains and all of that in whole or in parts can be used to help advance in investigation. Paper also brings out the difference in format of this artifact among various version of Windows OS.**

***Keywords*— Prefetch, Windows Operating System, Prefetch forensics, Artifacts, Examination tools.**

I. INTRODUCTION

WIN OS aims to improve the application start-up time and this is accomplished by loading data in to memory that an application needs to run. Thus, when an application is run for the first time the OS takes notice and creates a prefetch file for that specific program so that next time user runs that particular application then all its support files are loaded in the memory ahead of time and this then speeds up the process of starting the application thus improving user experience.

As Prefetch brings optimization function for the OS therefore it is automatically enabled by default on user level OS so analyst have this information that the artifact records.
From a forensic point of view the Prefetch artifact can give additional inside in any investigation as it provides evidence like executable name, run count, volume it was run from, associated time stamp of first and subsequent run time in the file that it uses. All of these as whole or in parts can be used to help advance the investigation.

Prefetch is existing in Windows system starting from Windows Xp and since then lot has changed from its format to the data it contains. This paper will bring out the changes that has taken place in various versions of Windows OS including the latest version i.e., Windows 11.

This paper has been outlined to give a deep knowledge on the artifact, refer figure 1. In section II, paper will cover details on Prefetch artefacts and the changes it has undergone since its origin. Section III will cover various experiments and test results based on user behaviour. Section IV will bring out the details of various tools that can be used to uncover the compressed information contained inside the artifact and last section will be the conclusion and future work

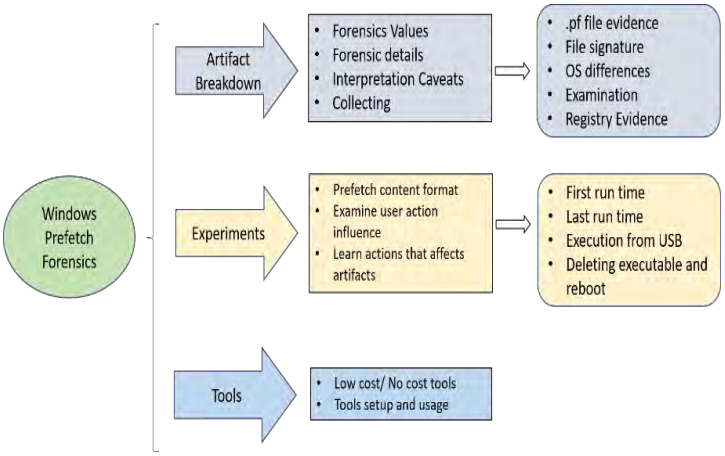

Fig. 1. Paper Outline

II. PREFETCH FILES: OVERVIEW AND BACKGROUND

Prefetch file is an OS artifact that improves application start-up time by loading the data application needs to run. This information is recorded by OS in prefetch folder maintained in the same volume where the OS resides in the system. As prefetch work is optimization thus it is automatically enabled in Windows system.

From a forensic point this artifact has a great value as it may help in adding evidences in the investigation or ay help to choose the start point of examination. Prefetch tracks the execution of program across a given system i.e., it accounts as central repository in witness of file execution on system and offer great value for file use and knowledge investigation when analyst is looking as what was run on a system.

Prefetch file includes information like file name, create time, modified time, file size, location of executable or process path, last run time and run counter. Thus, Prefetch information can be used to profile a system so looking at run count for instance and ordering it from the most frequently run to least frequently run, it can be determined the application that are frequently run on a system and it may provide information that is helpful in investigation

978-1-6654-9291-1/22/$31.00 ©2022 IEEE

Prefetch folder lives in same volume as that of OS. Thus, if an OS resided in C drive, then prefetch folder can be found at C:\Windows\Prefetch which list out all the prefetch files. Prefetch file have *.pf* extension[1]. To view Prefetch folder it requires specific tools and for this purpose **FTK Imager** and **WinPrefetchView** tools has been used for reading prefetch files as well as for conducting various experiments. Another tool which will be used in this paper is **Forensic Registry Editor** (FRED) which will help in finding out details about Prefetch activation on the system.

File Header: Prefetch was first found in Windows XP and since then it has undergone various changes, especially the signature value of prefetch files. Each prefetch file has 4-byte signature at offset 4 "SCCA" (or in hexadecimal notation 0x53 0x43 0x43 0x41)[2]. The signature is assumed to be preceded by a 4-byte format version indicator.

The header information comes very handy while carving for a windows prefetch file in a unallocated space and it is done using file header. Since Windows 10 and above the format has been change to MAM which is a compressed version and thus requires specified tools to uncompressed the information. Decompressed version will have same file header "SCCA" however delineation version will vary. Windows XP to Windows 8 the information is in plaintext.

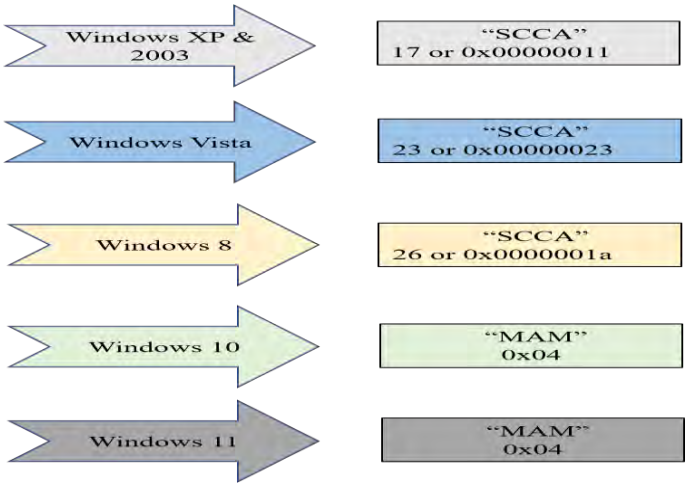

Fig. 2. Signature values in of various Windows OS

Prefetch Registry Key: Prefetch are enabled on Windows OS by default. However, there can be occasions though analyst expect to have prefetch evidence on user end point and they are not seen. Prefetch can be turned off and same can be checked through its Registry key. It is however difficult to disable prefetch but perpetrators of the crime are more forensic aware and thus this function cannot be neglected.

The key that gives out the information is system hive. System hive is extracted using FTK and Forensic Registry Editor (fred) tools. System hive is located in directory C:\Windows\System32\config\system [3][13].

FTK imager helps to export system file which gives the hive in a format that fred can easily decode. Thereafter a key called Prefetch Parameter will be examined to see if Prefetch is enabled or disabled. Prefetch can have different values which can be found under prefetch parameter in FRED tool[4].

Value 3 indicates that for both user application and boot application prefetch is enabled.
Value 2 indicates that only boot applications are prefetch enabled.
Value 1 indicates that only user applications are prefetch enabled.
Value 0 means prefetch is disabled (refer figure 3)

Forensic Value of Prefetch Object: Prefetch helps in tracking the execution of program across a given system and provides evidence in form of file name, create time of file, modified time, last run time, total run count, process path. Prefetch helps in creating a system profile as it provides a run count of each executable and this can help in identifying the most frequently run with those of a less frequently executed applications [5][14].
Prefetch can bring information that can help analyst to advance the investigation or may provide a start point of examination.

III. EXPERIMENTS AND RESULTS

Windows 11 v21H2 PC, will be treated as our suspected machine for investigation and thus all our experiments will be based on it including the one based on USB disk. The list of experiments and tools used is given in Table 1.

Table 1: List of Experiments and Tools

Scenario	Test Experiments	Tools
Local Machine	First Run Time	FTK, WinPrefetchView
Local Machine	Last Run Time	FTK, WinPrefetchView
Local Machine	Executing from USB	FTK, WinPrefetchView
USB Drive	Deleted Executable	FTK, WinPrefetchView

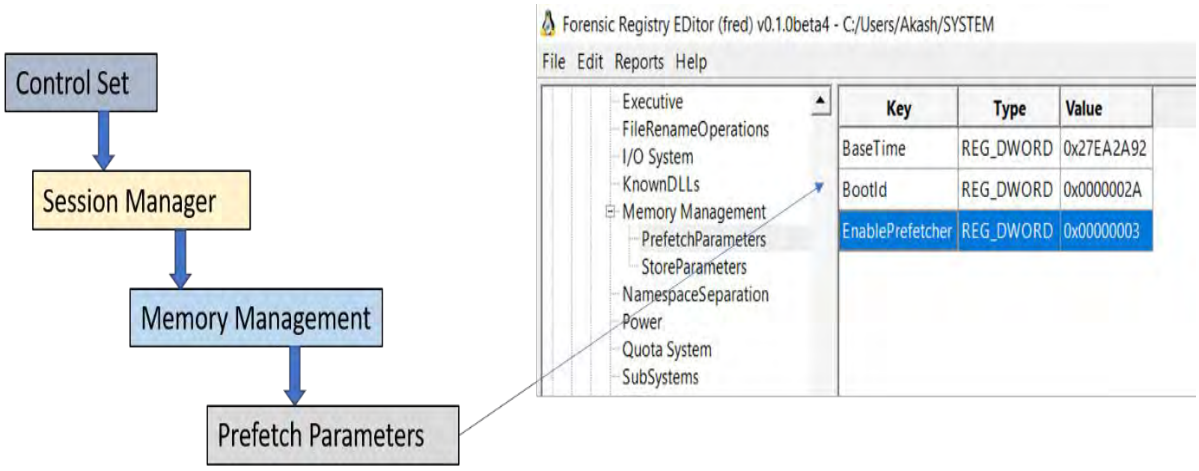

Fig. 3. Different values of Prefetch in FRED

A. First Run Time

In this phase of the experiment an application called "Wireless Network Watcher" which is a Nir Soft tool has been used for analysis. The application has been downloaded and saved on system Desktop from where it has been executed. While the execution begins the system date and time will be recorded for validating the analysis carried out in this experiment.

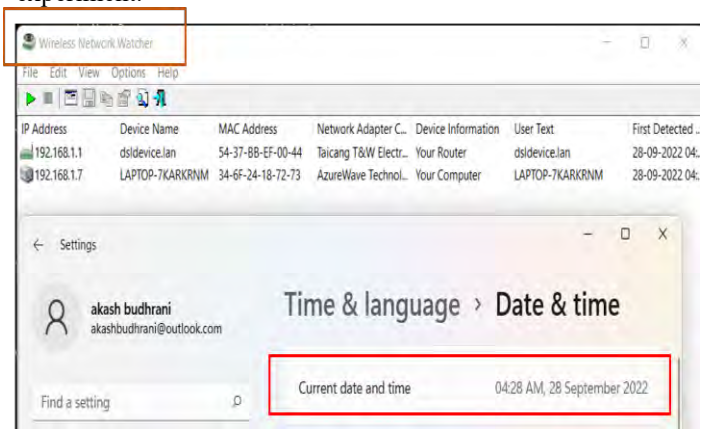

Fig. 4. Application running status with system date and time

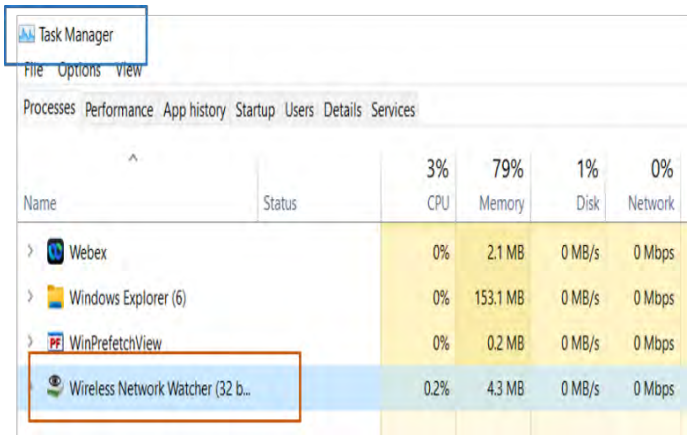

Fig. 5. Application running in Task Manager

The application "WNETWATCHER" was executed for the first time on the system. Same was confirmed through Task Manager. After running for few minutes the application was shut down and again same was conformed from Task Manager. Post this the WinPrefetchView tool was used to analyze the same.

Results- Particular application was selected in WinPrefetchView tool after terminating the application which gives out following information.

Create time – time when a file was first executed. The system time recorded matches the time recorded by the tool and thus it states that create time is the time of first execution of application

Modified time- time when a file was modified. Here the modified time is same as create time

File Size – gives out the size of the file executed.

Process Path - It brings out the location where the **executable was located in the system. The application was saved** on Desktop inside a folder called Winmonitor. Thus, process path is the directory of the application.

Run Counter – This mentions the number of times a particular application has been executed. The application has been executed only once and thus it shows the Run Counter value as 1.

Last Run Time – Gives the time when a particular application was executed for the last time. Here Last Run Time is same as create time which implies that the application has been executed only once.

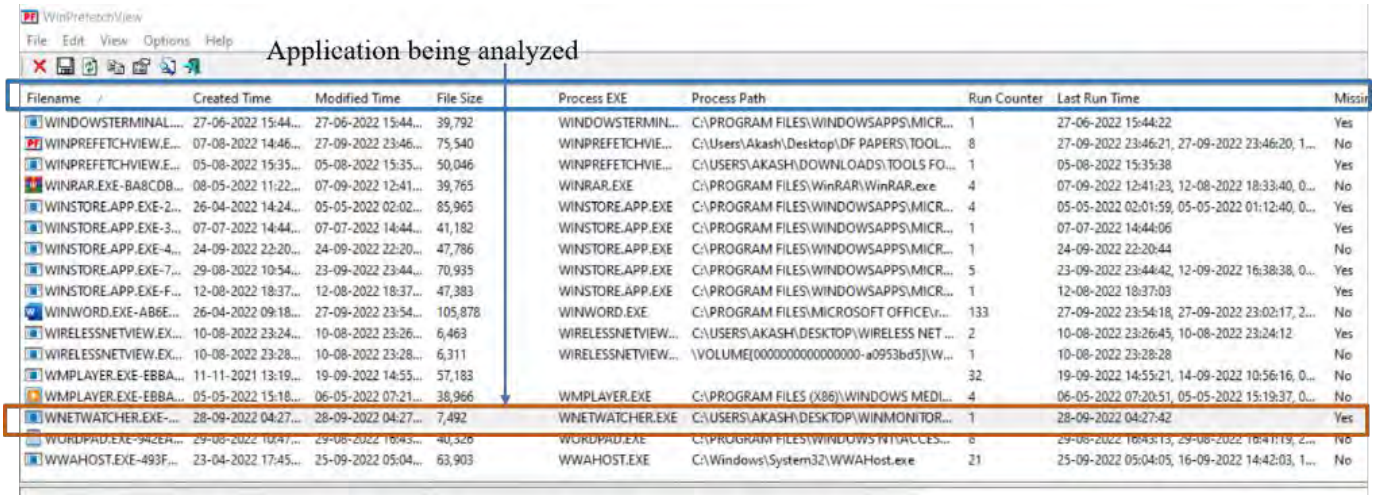

Fig. 6. WinPrefetchView decoding the artifact

B. *Last Run Time*

In this phase of the experiment same executable will be run again from the same location and Prefetch artefact will be analyzed for any changes.

Results – While the application was run for the second time the Create Time remains intact but the Modification Time updated to second run time. Process path and File size remains same but now the Run Counter updated to a value of 2 showing that "WNETWATCHER" has been executed twice.
This validate that we get our first and last run time in an accurate run count through this artifact.

In Prefetch Artifact with every application a trailing hash value is added [7]. Purpose of this hash value is to identify execution of similar executables but from different directory. Suppose in a system there lies an application called CCleaner which is located on Desktop in C drive as well as inside a system folder on the same drive. To differentiate the execution from both the path hash value comes in to play. In WinPrefetchView the executables may have similar names but will have different trailing hash if executed from different directory. This will be validated in next experiment. (Refer figure7)

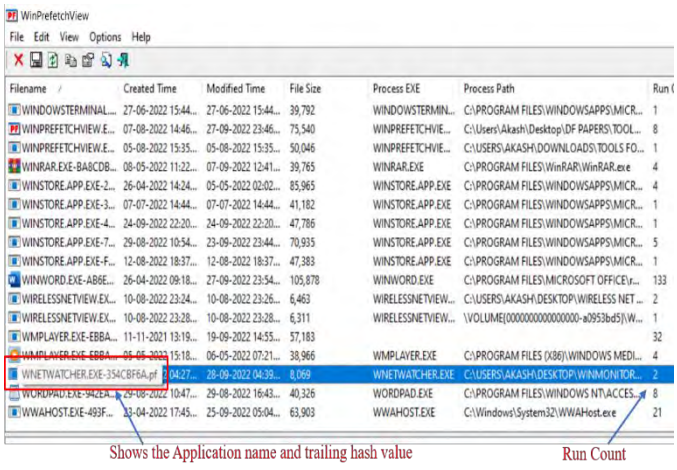

Fig. 7. Analysis of executable for Last Run Time

C. *Run from USB*

.

Here the same executable i.e., "WNETWATCHER" will be run from a USB device disk. Here we will test two main facts. Firstly, what happens with Windows Prefetch artifact when a file is executed from USB disk when it is a same executable .A new volume, a new directory but a same executable. The executable was run and system date and time was recorded. Task manager was used to confirm the program is running. Few moments later the program was killed

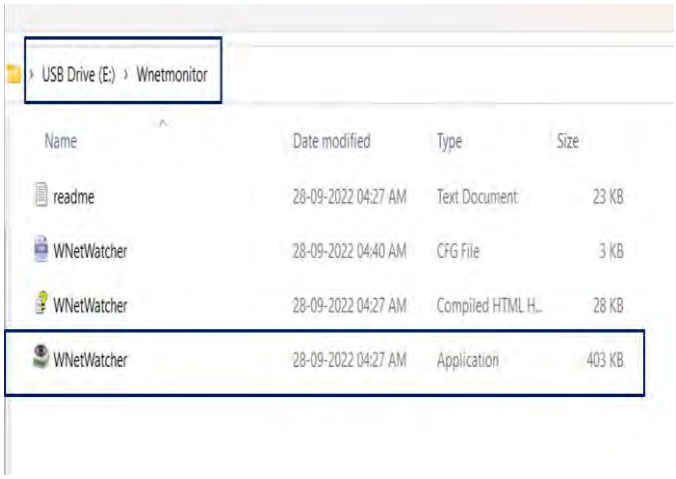

Fig. 8. Application executing from USB drive

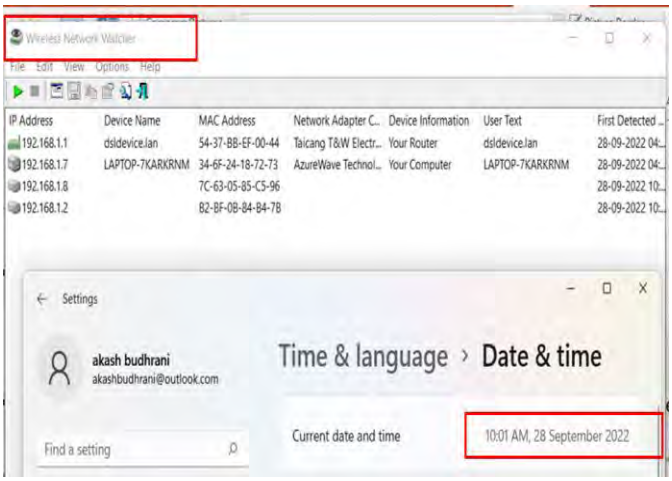

Fig. 9. WNetWatcher running from a USB disk. Date and Time recorded

Result - Win Prefetch View tool was run to find out the impact on prefetch artifact where it now shows two WNETWATCHER.exe programs. The top one was run from Desktop and bottom one was executed from USB disk. Both have two different Process path as well as trailing hashes. Same executables but different directories.

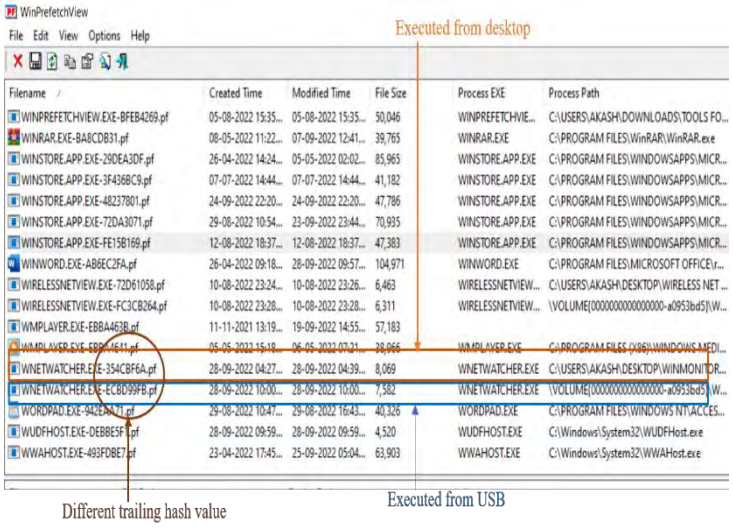

Fig. 10. View of same executables application in different directories

D. *Deleted Executables*

In this part of the experiment, we will find out the impact on Prefetch artifact when an executable is deleted. WNetWatcher has been running from desktop. This application entire folder will be deleted and recycle bin will be cleared. Also, to avoid any potential misleads the system will be rebooted and then Win Prefetch artifact will be analyzed to see any affects.

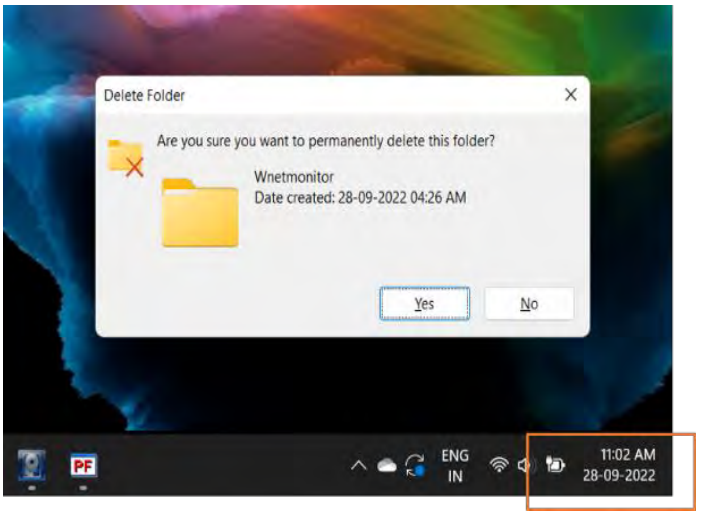

Fig. 11. Date and Time of deletion of executable

Result - After the system is freshly booted WinPrefetchView tool was examined to check if Prefetch artifact of deleted executable still exist or not. By looking at WinPrefetchView it can be observed that Prefetch artifact of the deleted executable still exist which means that Prefetch is a silent witness to the activity that executable did have on the system when it did exist. Therefore it's a important forensic evidence as it not only gives the executable on the system but post executables as well[8][16].

Tools: WinPrefetchView is alive and dead box analysis tool. It's a dragon drop executable which can be run from external media and can search for drive where OS is present and displays the required result. This tool has been built by DFIR community for computer forensic.

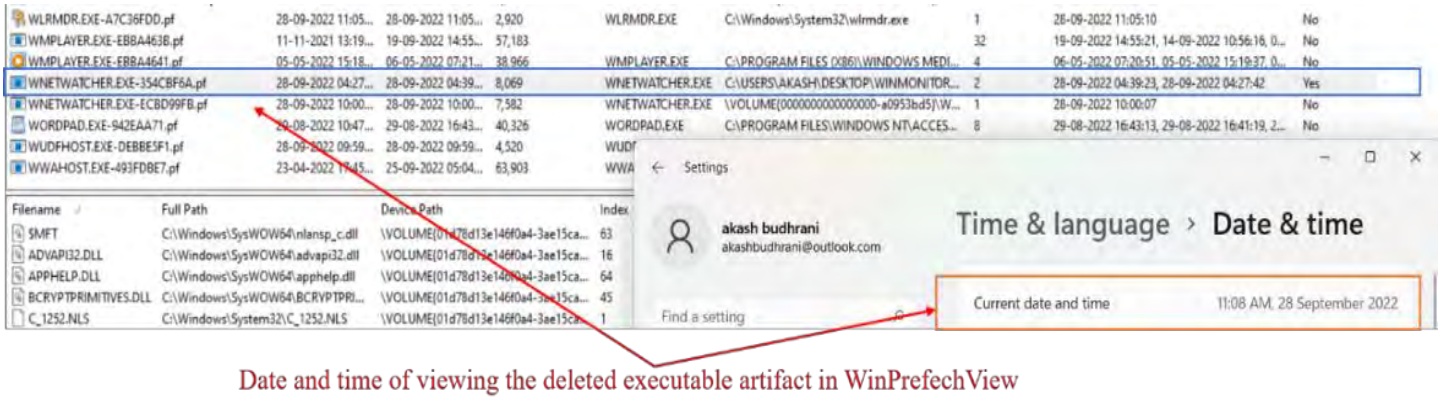

Fig. 12. Result of Prefetch artifact of deleted executable

IV. CONCLUSION AND RECOMMENDATIONS

This paper covers the Prefetch artifact, what it is and how it is valuable in Computer Forensic. User driven behavior affect changes to prefetch artifact and helps in interpretation of artifact in investigation or help advanced the investigation [10].
This paper includes analysis of various experiments conducted to brings out the relevance of prefetch artifact as it not only provides evidence of those present on the system but also about executables which have been deleted and no longer exist on the system.

Various other Windows objects can be used to validate the information provided by Prefetch object so as to confirm the user sequence of action performed on the suspected system. Most importantly prefetch can be used to profile a suspected system as Run Counter information can be used to determine the most frequently used application as well as lease frequently used application which may provide information that is helpful in investigation [12][13].

This paper brings out the forensic value of Prefetch artifact and various experiments conducted on methods to dug out the evidence however Validation of information from other artifacts can be looked into to confirm the accuracy of information decoded and also analyze the impact of Anti Forensic tool if executed on the artifacts with the aim to destroy the evidence.

V. REFERENCES

[1] Javed, Abdul Rehman, Waqas Ahmed, Mamoun Alazab, Zunera Jalil,Kashif Kifayat, and Thippa Reddy Gadekallu. "A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions." *IEEE Access* (2022).

[2] Neyaz, Ashar, Narasimha Shashidhar, Cihan Varol, and Amar Rasheed. "Digital Forensics Analysis of Windows 11 Shellbag with Comparative Tools." In *2022 10th International Symposium on Digital Forensics and Security (ISDFS)*, pp. 1-10. IEEE, 2022.

[3] Majed, Hussein, Hassan N. Noura, and Ali Chehab. "Overview of Digital Forensics and Anti-Forensics Techniques." In *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, pp. 1-5. IEEE, 2020.

[4] Đuranec, A., D. Topolčić, Kresimir Hausknecht, and Damir Delija. "Investigating file use and knowledge with Windows 10 artifacts." In *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 1213-1218. IEEE, 2019.

[5] Aziz, Normaziah A., Muhammad Saifulldin M. Yusof, Muhammad Helmi Bin Ab Malik, Ahmad Rasyad Hanizam, and Lukman Hakim Abd Rahman. "Acquiring and Analysing Digital Evidence-a Teaching and Learning Experience in Class." In *2018 Cyber Resilience Conference (CRC)*, pp. 1-4. IEEE, 2018.

[6] Majed, Hussein, Hassan N. Noura, and Ali Chehab. "Overview of Digital Forensics and Anti-Forensics Techniques." In *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, pp. 1-5. IEEE, 2020.

[7] Kim, Young-hoon, and Tae-kyoung Kwon. "On Artifact Analysis for User Behaviors in Collaboration Tools-Using differential forensics for distinct operating environments." *Journal of the Korea Institute of Information*

[8] Sachdeva, S., Raina, B. L., & Sharma, A. (2020). Analysis of digital forensic tools. *Journal of Computational and Theoretical Nanoscience*, *17*(6), 2459-2467.

[9] Singh, Bhupendra, and Upasna Singh. "A forensic insight into windows 10 jump lists." *Digital Investigation* 17 (2016): 1-13.

[10] Singh, Bhupendra, and Upasna Singh. "Leveraging the windows amcache. hve file in forensic investigations." *Journal of Digital Forensics, Security and Law* 11, no. 4 (2016): 7.

[11] Singh, B. and Singh, U., 2018. Program execution analysis in Windows: A study of data sources, their format and comparison of forensic capability. *Computers & Security*, *74*, pp.94-114.

[12] Singh, B., Singh, U., Sharma, P. and Nath, R., 2018, January. Recovery of forensic artifacts from deleted jump lists. In *IFIP International Conference on Digital Forensics* (pp. 51-65). Springer, Cham.

[13] Kondapally, Bhanu Prakash. "Forensically Important Artifacts in Windows Operating systems." (2015).

[14] Singh, Bhupendra, and Upasna Singh. "Program Execution Analysis using UserAssist Key in Modern Windows." In *SECRYPT*, pp. 420-429. 2017.

[15] Prasanthi, B. V. "Cyber forensic tools: a review." *International Journal of Engineering Trends and Technology (IJETT)* 41.5 (2016): 266-271.

[16] Kondapally, Bhanu Prakash. "Forensically Important Artifacts in Windows Operating systems." (2015).