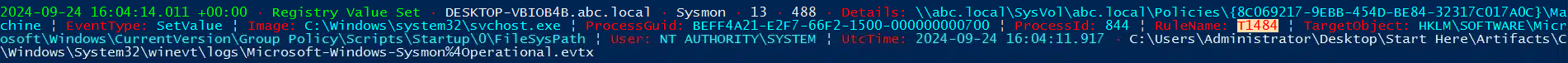
<https://cyberdefenders.org/blueteam-ctf-challenges/meteorhit/>

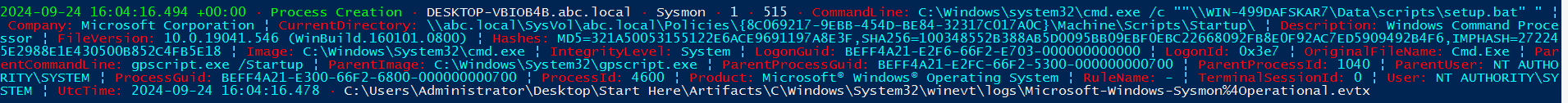
1. The attack began with using a Group Policy Object (GPO) to exec nmbvnm vnm vnm vnm vnm vnm vnm vnm vnm vute a malicious batch file. What is the name of the malicious GPO responsible for initiating the attack by running a script?

I used **hayabusa** tool to investigate windows events. I specifically was looking for anything related to sysvol (for group policy configs related to startup scripts)

I got a sysmon event 13 that matched T1484 (domain or tenant policy modification)

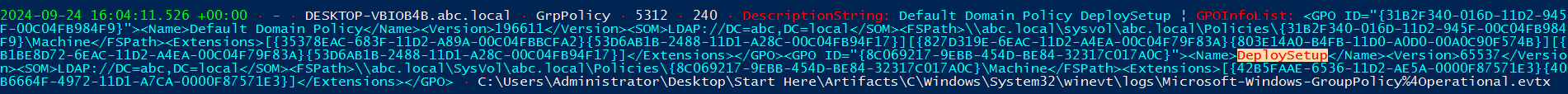


Followed directly by Sysmon event 1 for the execution of the script



Apparently the malicious GPO guid is 8C069217-9EBB-454D-BE84-32317C017A0C

We need then to look for the event id 5312(**Event id 5312 shows when a GPO is applied** ) indicates that applicable GPOs were discovered for either a user or a computer. And indeed we found it 3 seconds earlier



Reference

<https://github.com/Psmths/windows-forensic-artifacts/blob/main/group-policy/evtx-5312-list-of-gpo.md>

<https://www.elastic.co/guide/en/security/8.17/prebuilt-rule-8-4-2-startup-logon-script-added-to-group-policy-object.html>

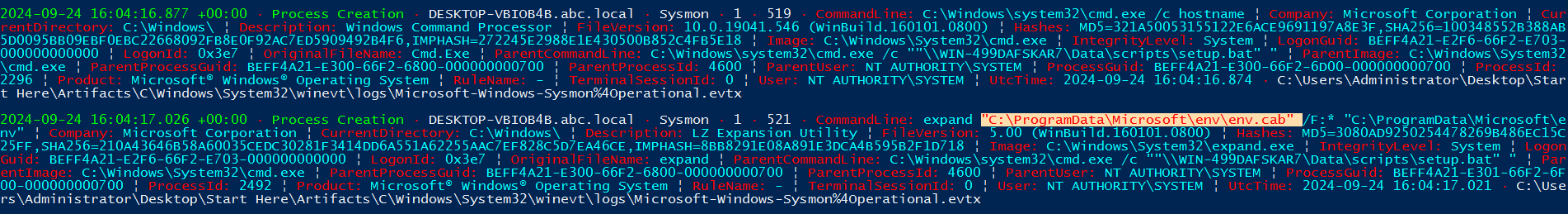
<https://www.elastic.co/guide/en/security/current/prebuilt-rule-8-2-1-startup-logon-script-added-to-group-policy-object.html>

processeid 4600

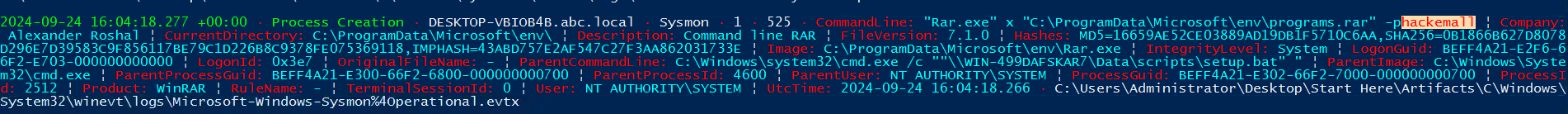
machine name DESKTOP-VBIOB4B

1. During the investigation, a specific file containing critical components necessary for the later stages of the attack was found on the system. This file, expanded using a built-in tool, played a crucial role in staging the malware. What is the name of the file, and where was it located on the system? Please provide the full file path.

By tracking the process cmd.exe (process id 4600)

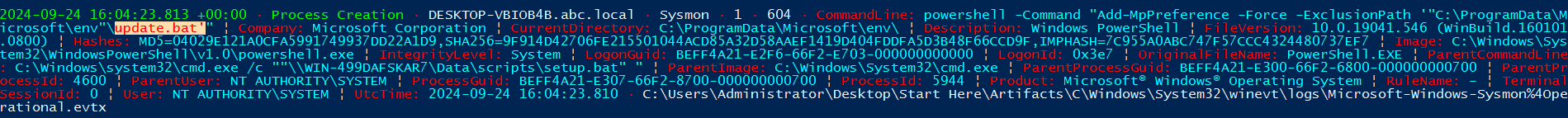


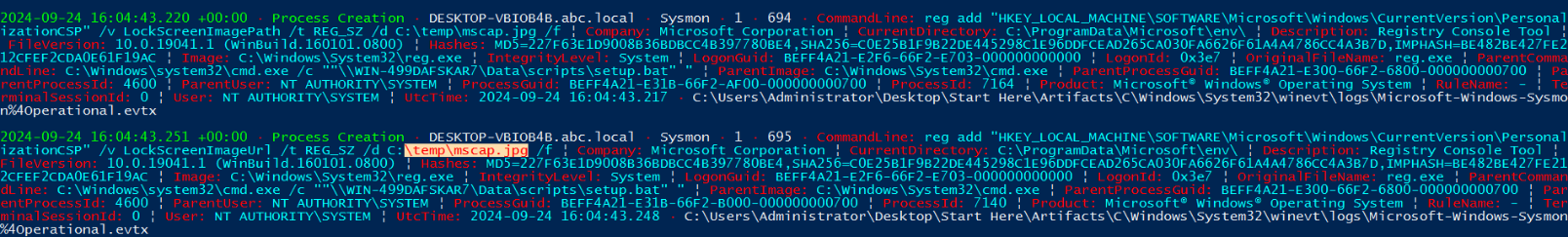
1. The attacker employed password-protected archives to conceal malicious files, making it important to uncover the password used for extraction. Identifying this password is key to accessing the contents and analyzing the attack further. What is the password used to extract the malicious files?



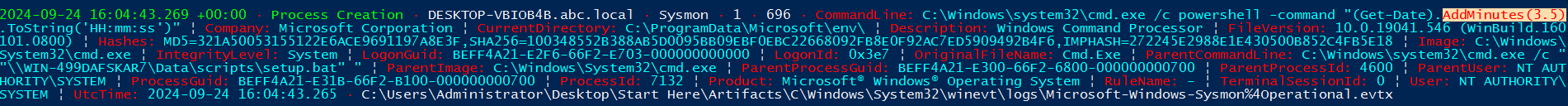
Password is hackemall

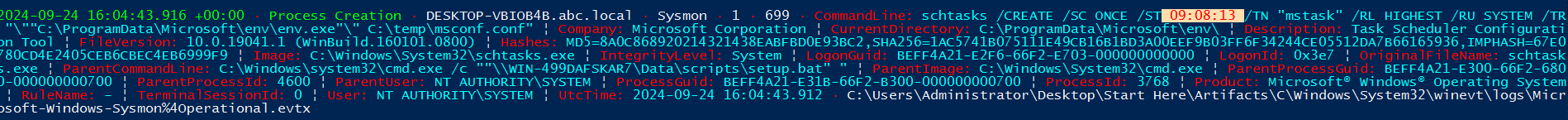
1. Several commands were executed to add exclusions to Windows Defender, preventing it from scanning specific files. This behavior is commonly used by attackers to ensure that malicious files are not detected by the system's built-in antivirus. Tracking these exclusion commands is crucial for identifying which files have been protected from antivirus scans. What is the name of the first file added to the Windows Defender exclusion list?

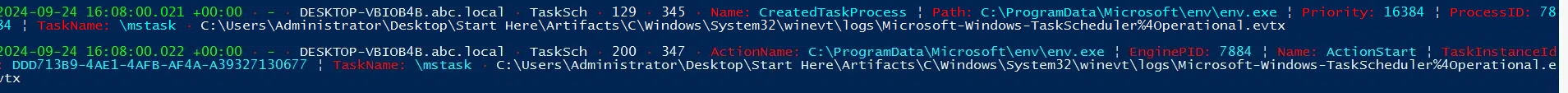




1. A scheduled task has been configured to execute a file after a set delay. Understanding this delay is important for investigating the timing of potential malicious activity. How many seconds after the task creation time is it scheduled to run?





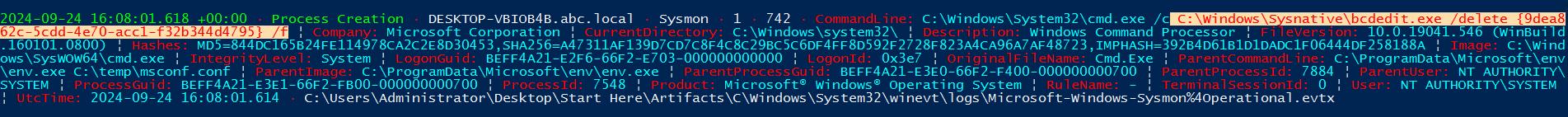
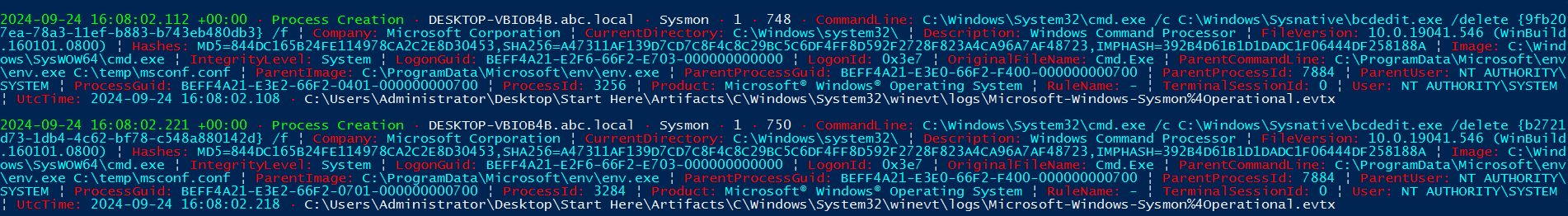


env.exe >> sha256 (2AA6E42CB33EC3C132FFCE425A92DFDB5E29D8AC112631AEC068C8A78314D49B)

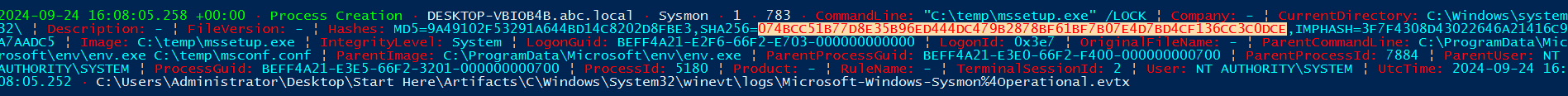
this is Meteor (ransomware)

process id 7884

1. The malware executed a command to delete the Windows Boot Manager, a critical component responsible for loading the operating system during startup. This action can render the system unbootable, leading to serious operational disruptions and making recovery more difficult. What command did the malware use to delete the Windows Boot Manager?

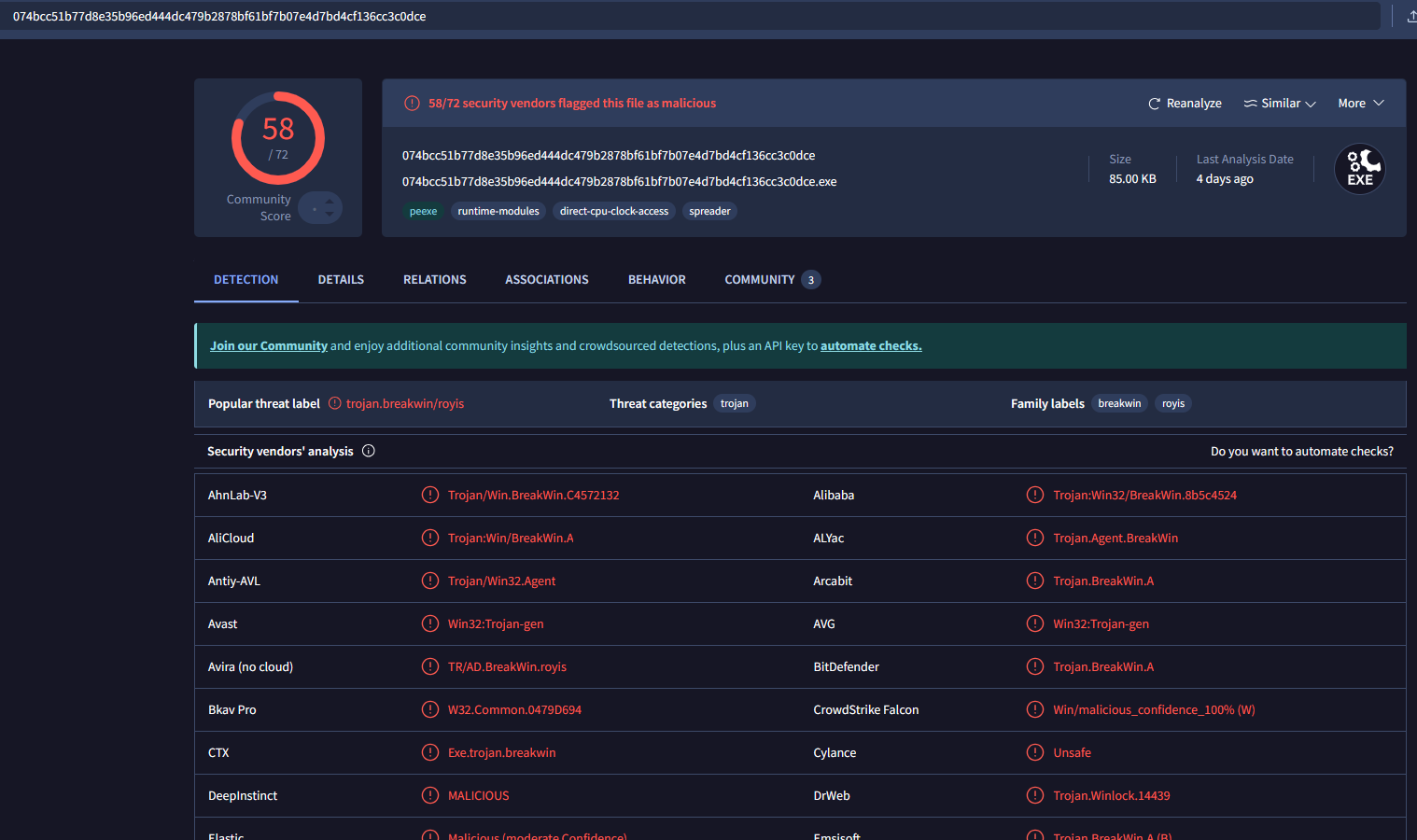
 

1. A malicious program was used to lock the screen, preventing users from accessing the system. Investigating this malware is important to identify its behavior and mitigate its impact. What is the name of this malware? (not the filename)

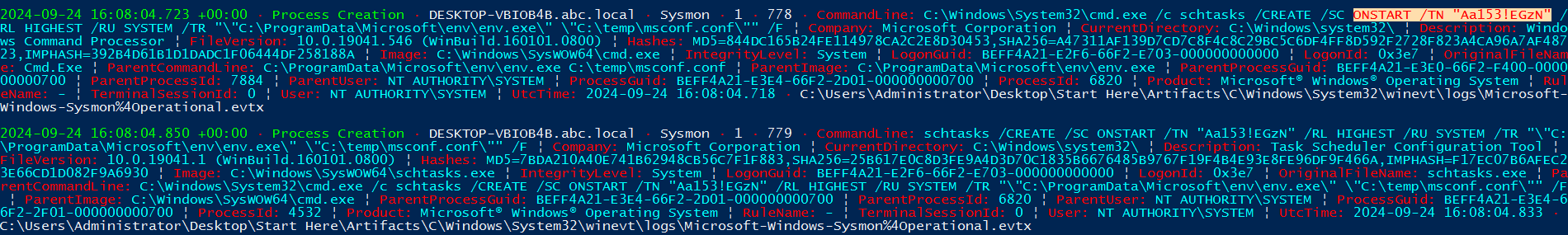


Filehash 074BCC51B77D8E35B96ED444DC479B2878BF61BF7B07E4D7BD4CF136CC3C0DCE

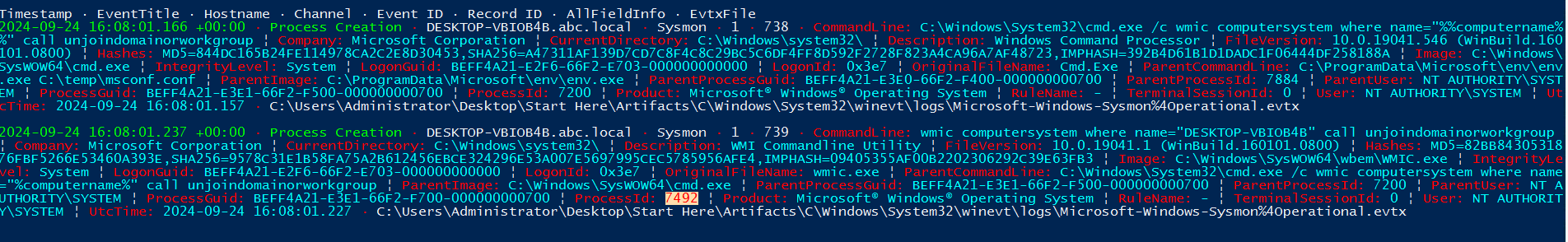
Malware is breakwin



1. The malware created a scheduled task to ensure persistence and maintain control over the compromised system. This task is configured to run with elevated privileges every time the system starts, ensuring the malware continues to execute. What is the name of the scheduled task created by the malware to maintain persistence?



1. After the malware execution, the wmic utility was used to unjoin the computer system from a domain or workgroup. Tracking this operation is essential for identifying system reconfigurations or unauthorized changes. What is the Process ID (PID) of the utility responsible for performing this action?



1. The disk shows a pattern where malware overwrites data (potentially with zero-bytes) and then deletes it, a behavior commonly linked to Wiper malware activity. The USN (Update Sequence Number) is vital for tracking filesystem changes on an NTFS volume, enabling investigators to trace when files are created, modified, or deleted, even if they are no longer present. This is critical for building a timeline of file activity and detecting potential tampering. What is the USN associated with the deletion of the file msuser.reg?

**Explanation first:**

The **Update Sequence Number (USN) in NTFS** volumes is a feature that maintains a record of changes made to the volume. This feature is known as the USN Journal or Change Journal. It provides a persistent log of all changes made to files on the volume, such as additions, deletions, and modifications. Each record in the journal is assigned a unique USN, which helps in tracking changes efficiently  
12.To investigate the USN in NTFS volumes, you can use the following tools:

1. fsutil: This is a command-line utility that allows you to manage the USN change journal. You can create, delete, query, and enumerate the USN journal using various fsutil usn commands. For example:
   * fsutil usn queryjournal <volumepath>: Queries the USN journal for a specific volume.
   * fsutil usn enumdata <fileref> <lowUSN> <highUSN> <volumepath>: Enumerates and lists the change journal entries between two specified boundaries1.
2. PowerShell: You can use PowerShell scripts to query and analyze the USN journal. For example, you can use the Get-Content cmdlet to read the USN journal file and filter the records based on specific criteria.
3. Third-Party Tools: There are various third-party forensic tools available that can help you analyze the USN journal. These tools often provide a graphical interface and additional features for easier analysis.

By using these tools, you can effectively investigate the USN in NTFS volumes and track changes made to files on the volume.

The Master File Table (MFT) is a critical component of the NTFS (New Technology File System) used by Windows operating systems. It contains a detailed record of every file and directory on an NTFS volume. Each entry in the MFT includes information about the file, such as its size, time and date stamps, permissions, and data content. Here are some key points about the MFT:

* Structure: The MFT is essentially a database where each file and directory on the NTFS volume has at least one entry. This includes the MFT itself.
* Information Storage: All information about a file, including its metadata and data content, is stored either directly in the MFT entries or in space outside the MFT that is described by these entries.
* Growth and Fragmentation: As files are added to the NTFS volume, more entries are added to the MFT, causing it to grow. When files are deleted, their MFT entries are marked as free and can be reused, but the size of the MFT does not decrease. The NTFS file system reserves space for the MFT to keep it as contiguous as possible as it grows1.

To investigate the MFT, you can use various tools:

1. Mft2Csv: This tool can read the MFT from various sources, including live system acquisition, and convert it to a CSV format for analysis2.
2. NTFS File System Tools: Built-in tools like fsutil and third-party forensic tools can help you analyze the MFT and extract useful information.

Extracting and Analyzing the MFT:

1. Mft2Csv: This tool can read the MFT from various sources, including live system acquisition, and convert it to a CSV format for analysis. It supports reading the MFT directly from a live system, raw disk images, and shadow copies
2. MFTECmd: Developed by Eric Zimmerman, this tool parses the MFT from NTFS file systems and provides detailed information about the files and directories
3. analyzeMFT: This Python tool is designed to fully parse the MFT file from an NTFS filesystem and present the results in multiple formats, such as CSV or bodyfile

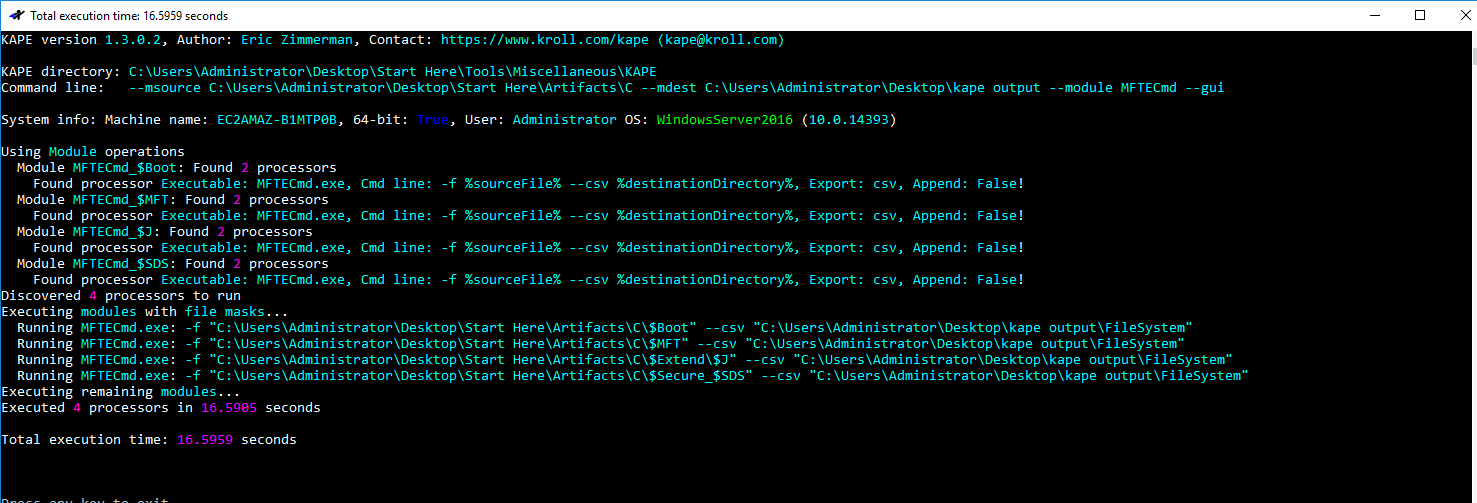
Example Usage:

* Mft2Csv:
* Mft2Csv.exe -f C:\$MFT -o output.csv
* This command reads the MFT from the specified file and outputs the data to a CSV file.
* MFTECmd:
* MFTECmd.exe -f C:\$MFT -o output.csv
* This command parses the MFT and outputs the data to a CSV file.
* analyzeMFT:
* python analyzeMFT.py -f C:\$MFT -o output.csv
* This command reads the MFT from the specified file and outputs the data to a CSV file.

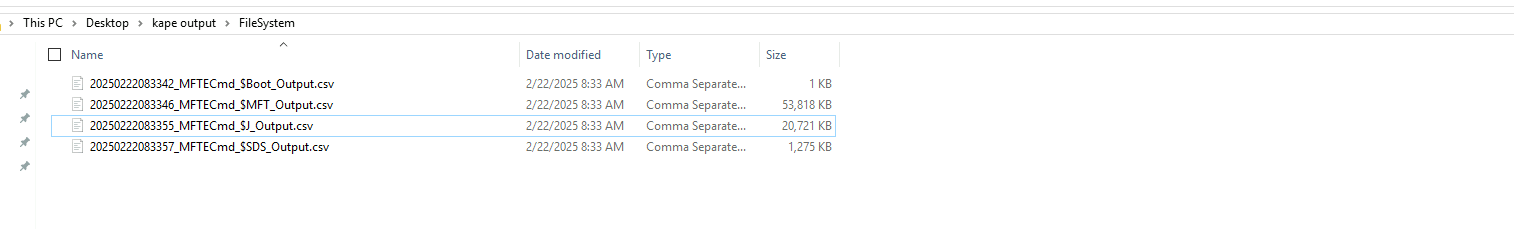
These tools allow you to extract and analyze the MFT for forensic purposes, providing detailed information about the files and directories on an NTFS volume.

**Solution**:

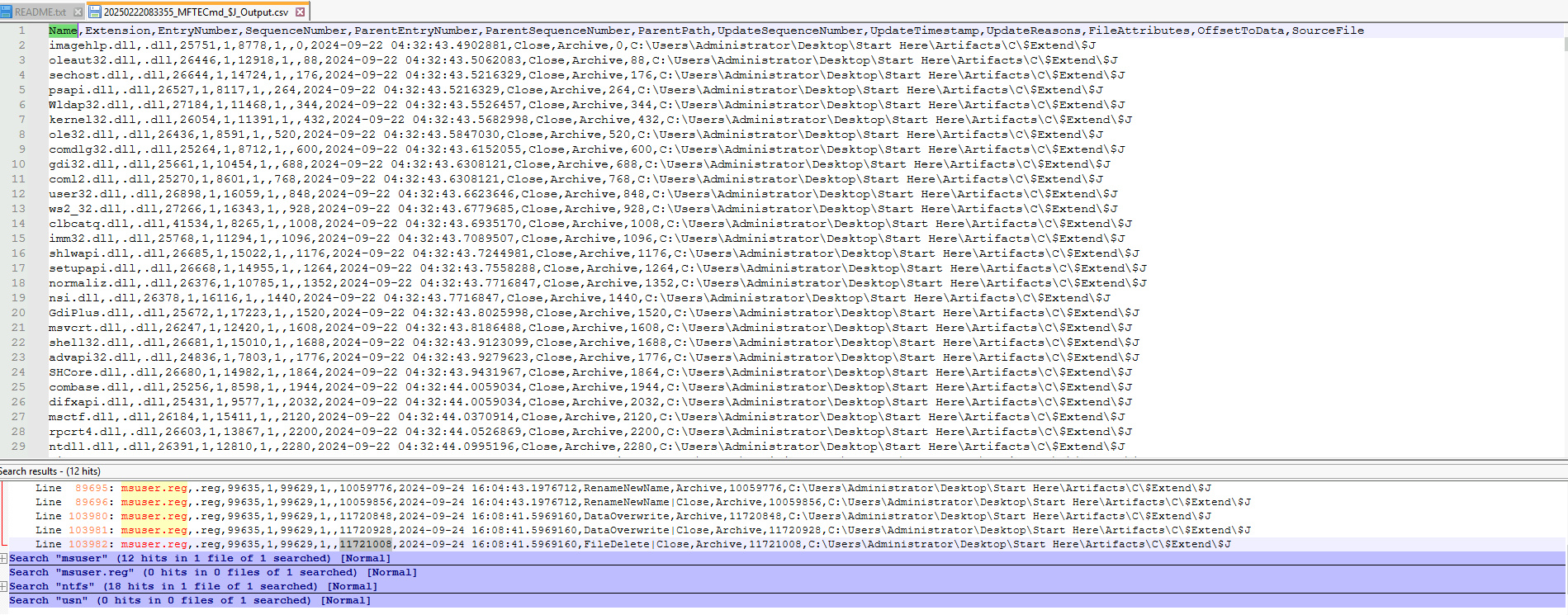
we need to analyze the Master file table MFT file , for that we can use the MFTECMD. This tool is available as a module in KAPE.



After parsing the MFT there we have 4 output files



We should look for the $J\_Output which is the output for parsed USN Journal.



We look for the file needed msuser.reg and FileDelete Operation , note the update sequence number for the operation.