

Conducting Forensic Investigations on Windows Systems (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 05

Student:
muhammad zahid

Email:
zahid1mz@cmich.edu

Time on Task:
5 hours, 54 minutes

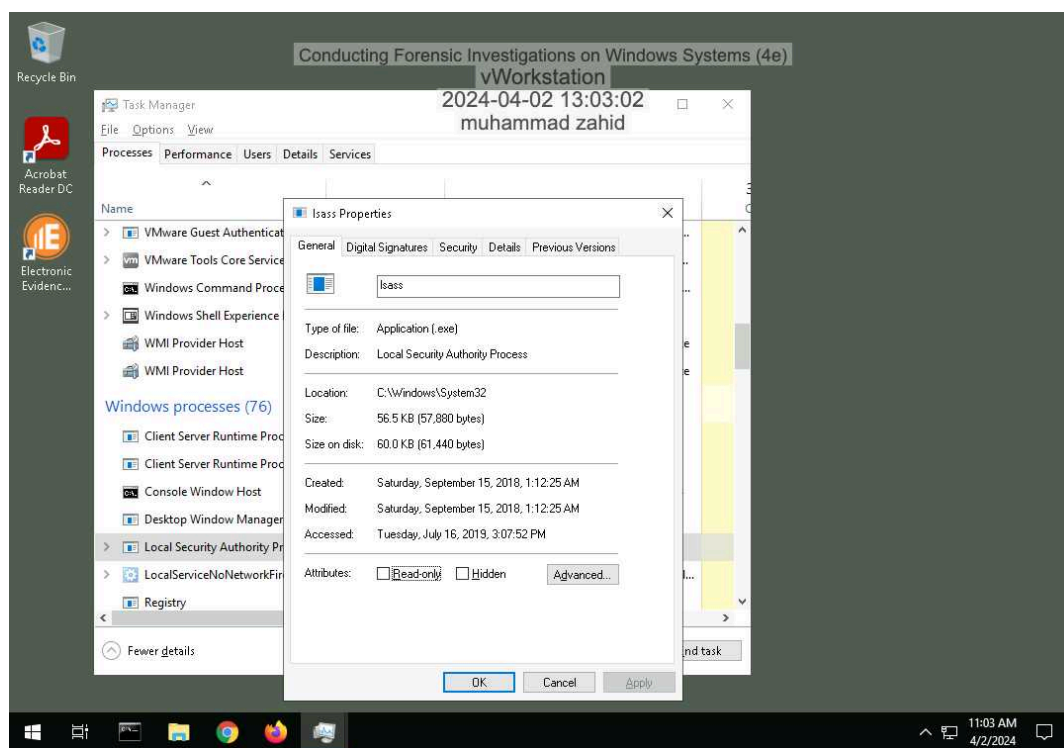
Progress:
100%

Report Generated: Tuesday, April 2, 2024 at 3:47 PM

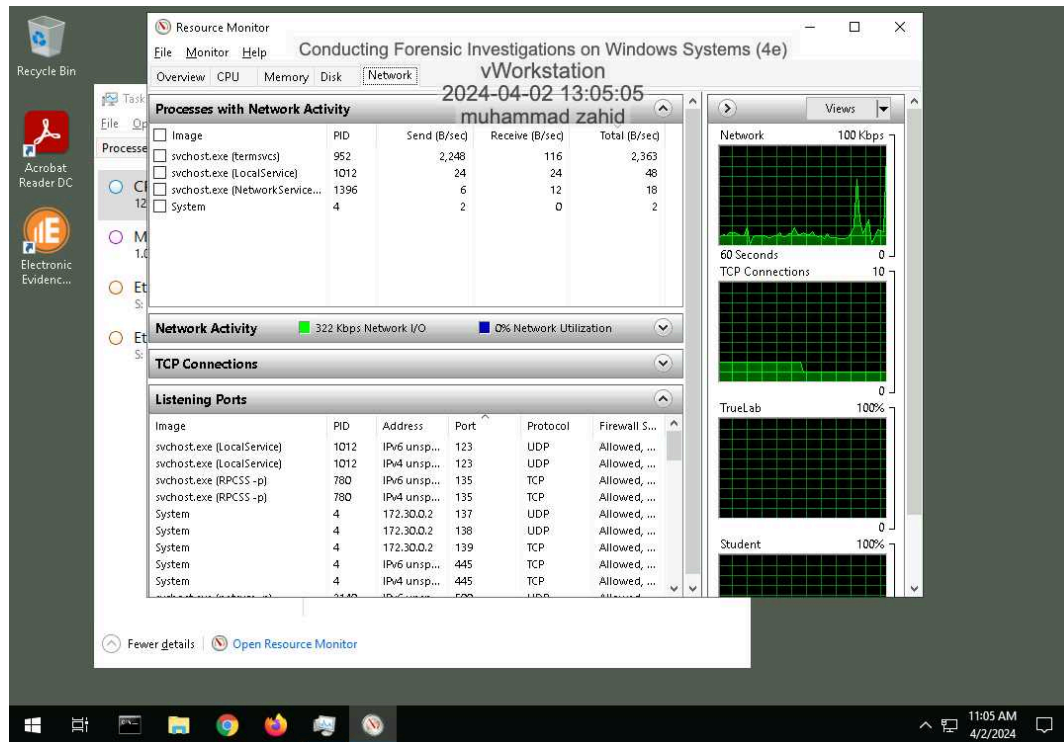
Section 1: Hands-On Demonstration

Part 1: Gather Basic System Information

4. Make a screen capture showing the **Properties** window for the process you selected.



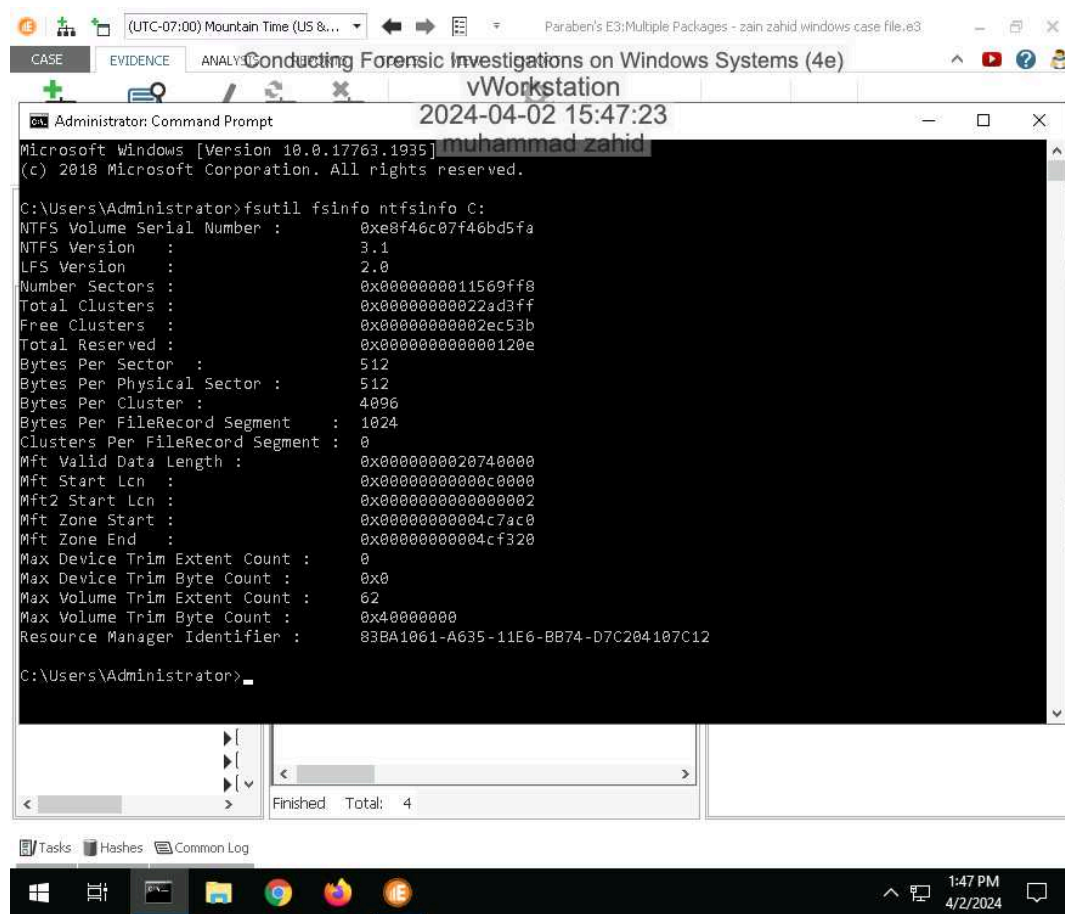
10. Make a screen capture showing the Listening Ports list.



14. Make a screen capture showing the information about the C: drive.

Conducting Forensic Investigations on Windows Systems (4e)

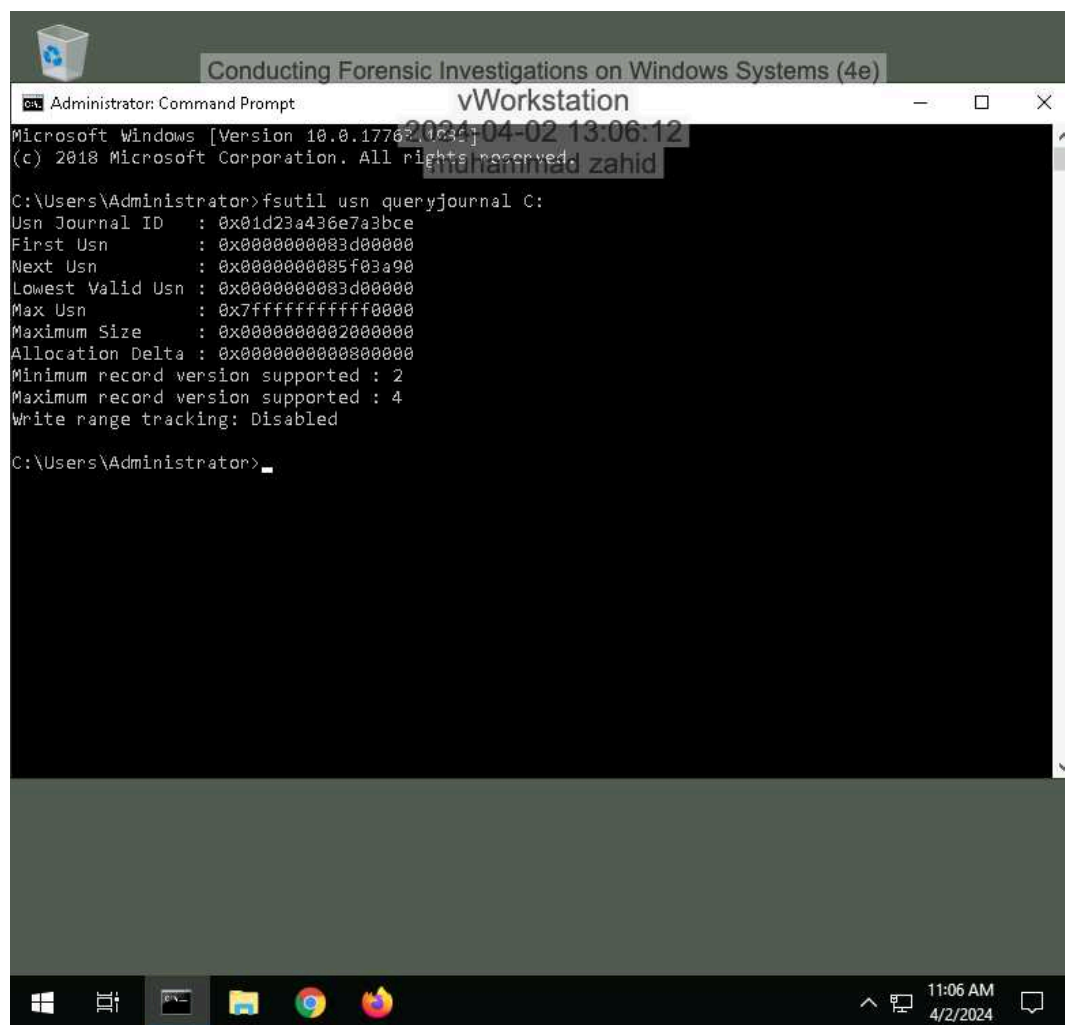
Digital Forensics, Investigation, and Response, Fourth Edition - Lab 05



16. Make a screen capture showing the information about the vWorkstation's usn journal.

Conducting Forensic Investigations on Windows Systems (4e)

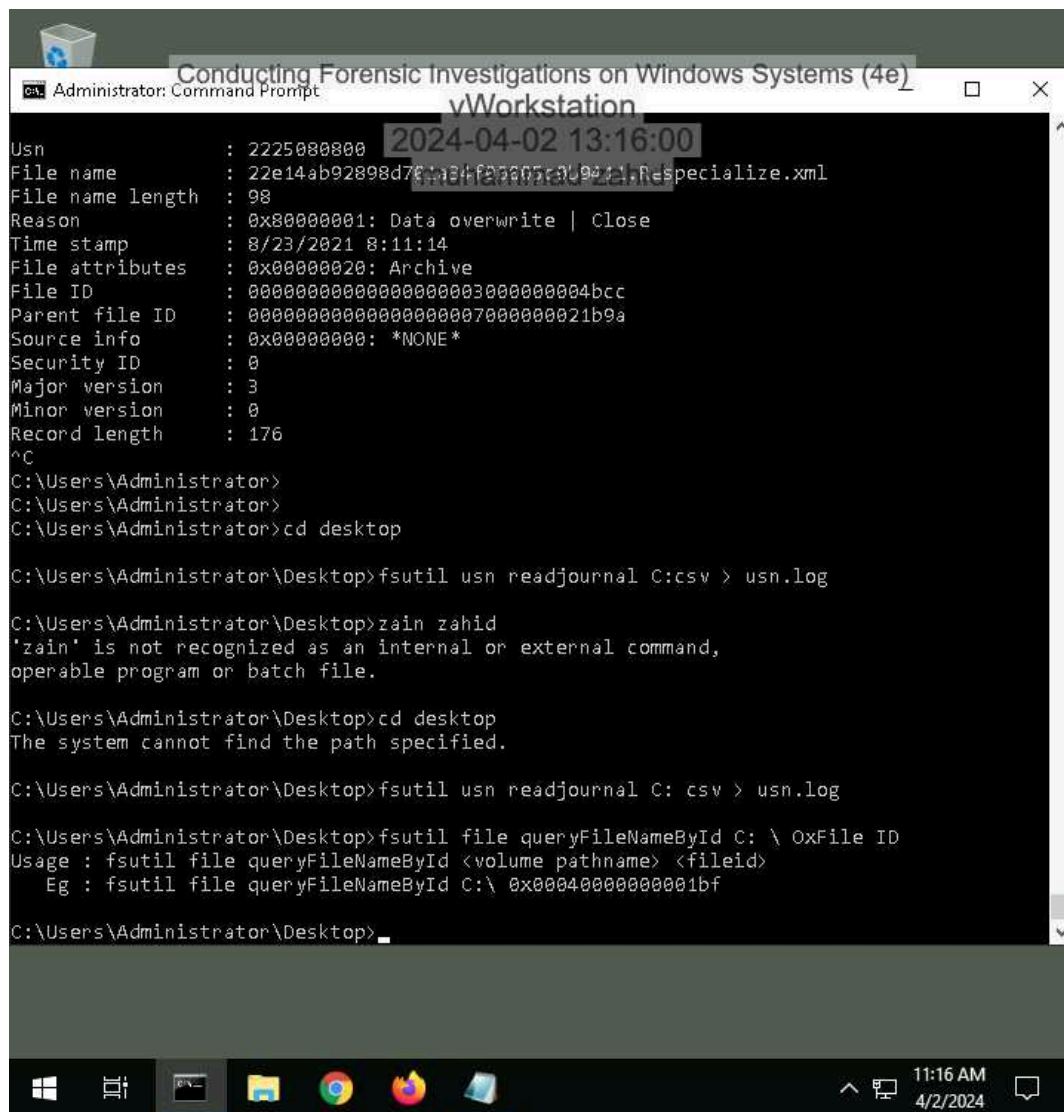
Digital Forensics, Investigation, and Response, Fourth Edition - Lab 05



26. Make a screen capture showing the file path for the *yourname.txt* file.

Conducting Forensic Investigations on Windows Systems (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 05



```
Administrator: Command Prompt
Conducting Forensic Investigations on Windows Systems (4e)
vWorkstation
2024-04-02 13:16:00
Usn      : 2225080800
File name : 22e14ab92898d761a3-f0000070009221-Respecialize.xml
File name length : 98
Reason    : 0x80000001: Data overwrite | Close
Time stamp : 8/23/2021 8:11:14
File attributes : 0x00000020: Archive
File ID    : 0000000000000000000000030000000004bcc
Parent file ID : 0000000000000000000000070000000021b9a
Source info : 0x00000000: *NONE*
Security ID : 0
Major version : 3
Minor version : 0
Record length : 176
^C
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>cd desktop

C:\Users\Administrator\Desktop>fsutil usn readjournal C:csv > usn.log

C:\Users\Administrator\Desktop>zain zahid
'zain' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator\Desktop>cd desktop
The system cannot find the path specified.

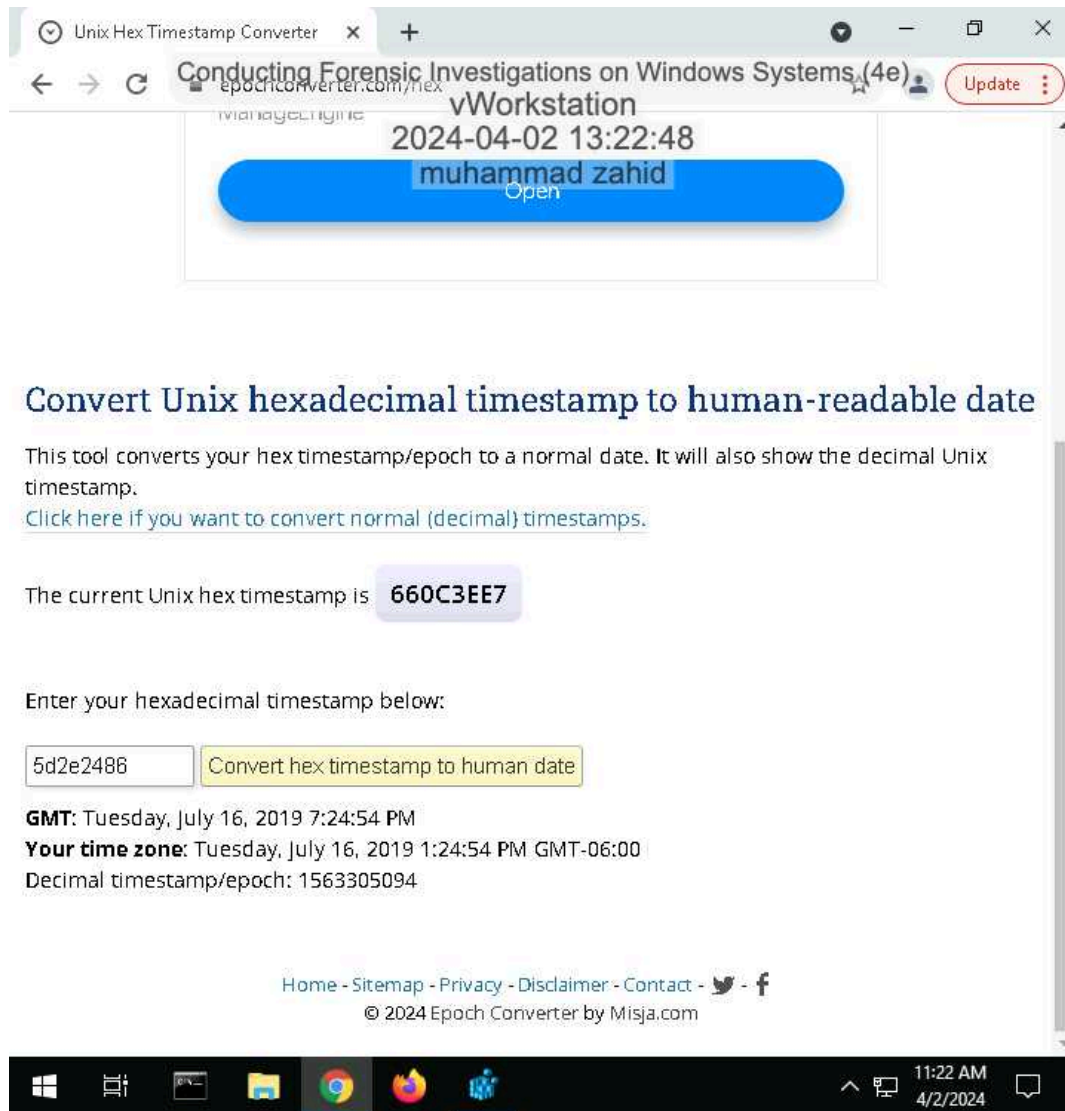
C:\Users\Administrator\Desktop>fsutil usn readjournal C: csv > usn.log

C:\Users\Administrator\Desktop>fsutil file queryFileNameById C: \ OxFile ID
Usage : fsutil file queryFileNameById <volume pathname> <fileid>
Eg : fsutil file queryFileNameById C:\ 0x000400000000001bf

C:\Users\Administrator\Desktop>
```

Part 2: Explore the Registry

10. **Make a screen capture** showing the **vWorkstation Windows installation timestamp** in a **human-friendly format**.



Convert Unix hexadecimal timestamp to human-readable date

This tool converts your hex timestamp/epoch to a normal date. It will also show the decimal Unix timestamp.

[Click here if you want to convert normal \(decimal\) timestamps.](#)

The current Unix hex timestamp is **660C3EE7**

Enter your hexadecimal timestamp below:

5d2e2486

Convert hex timestamp to human date

GMT: Tuesday, July 16, 2019 7:24:54 PM

Your time zone: Tuesday, July 16, 2019 1:24:54 PM GMT-06:00

Decimal timestamp/epoch: 1563305094

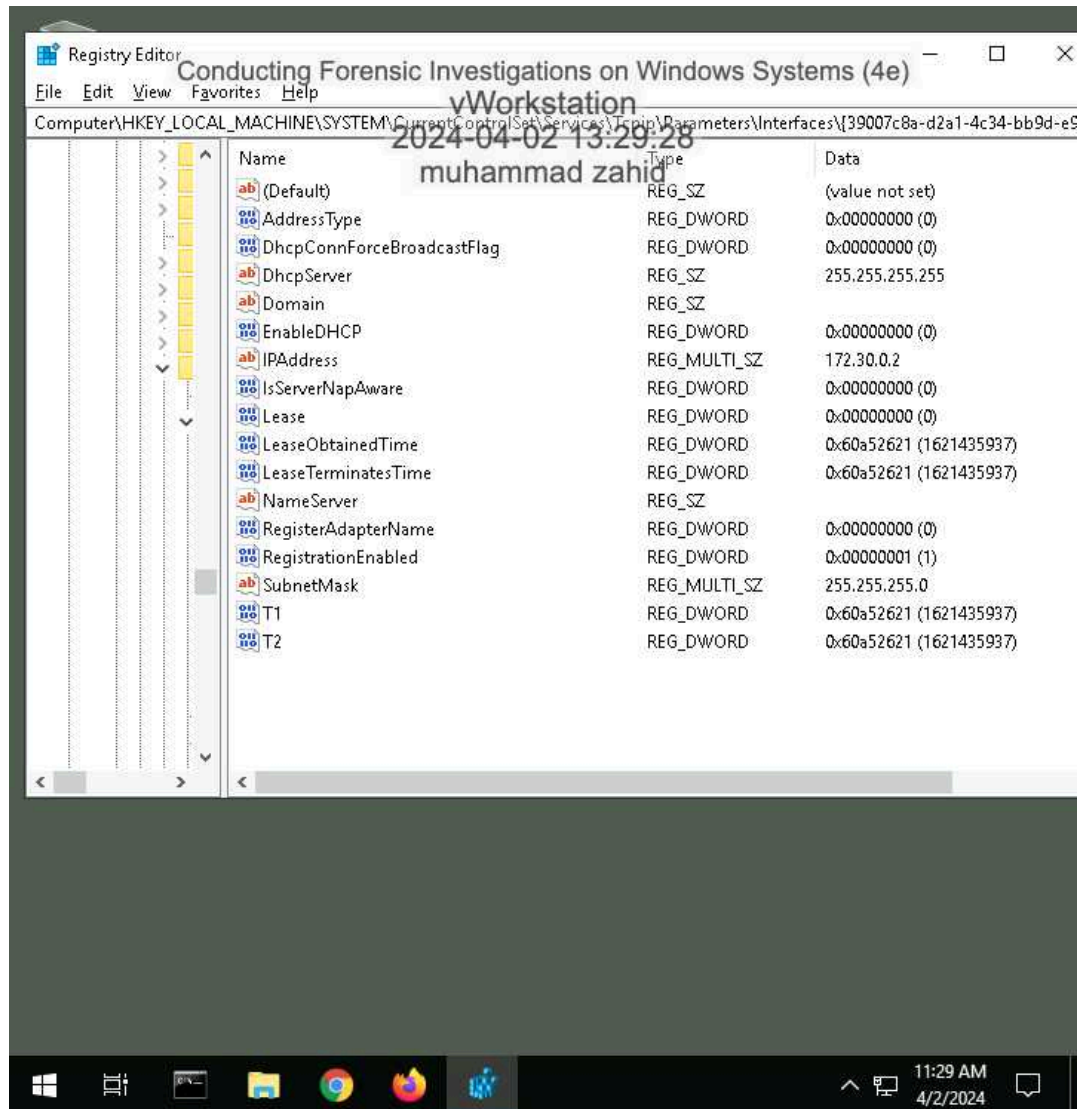
[Home](#) - [Sitemap](#) - [Privacy](#) - [Disclaimer](#) - [Contact](#) - [Twitter](#) - [Facebook](#)

© 2024 Epoch Converter by Misja.com

Conducting Forensic Investigations on Windows Systems (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 05

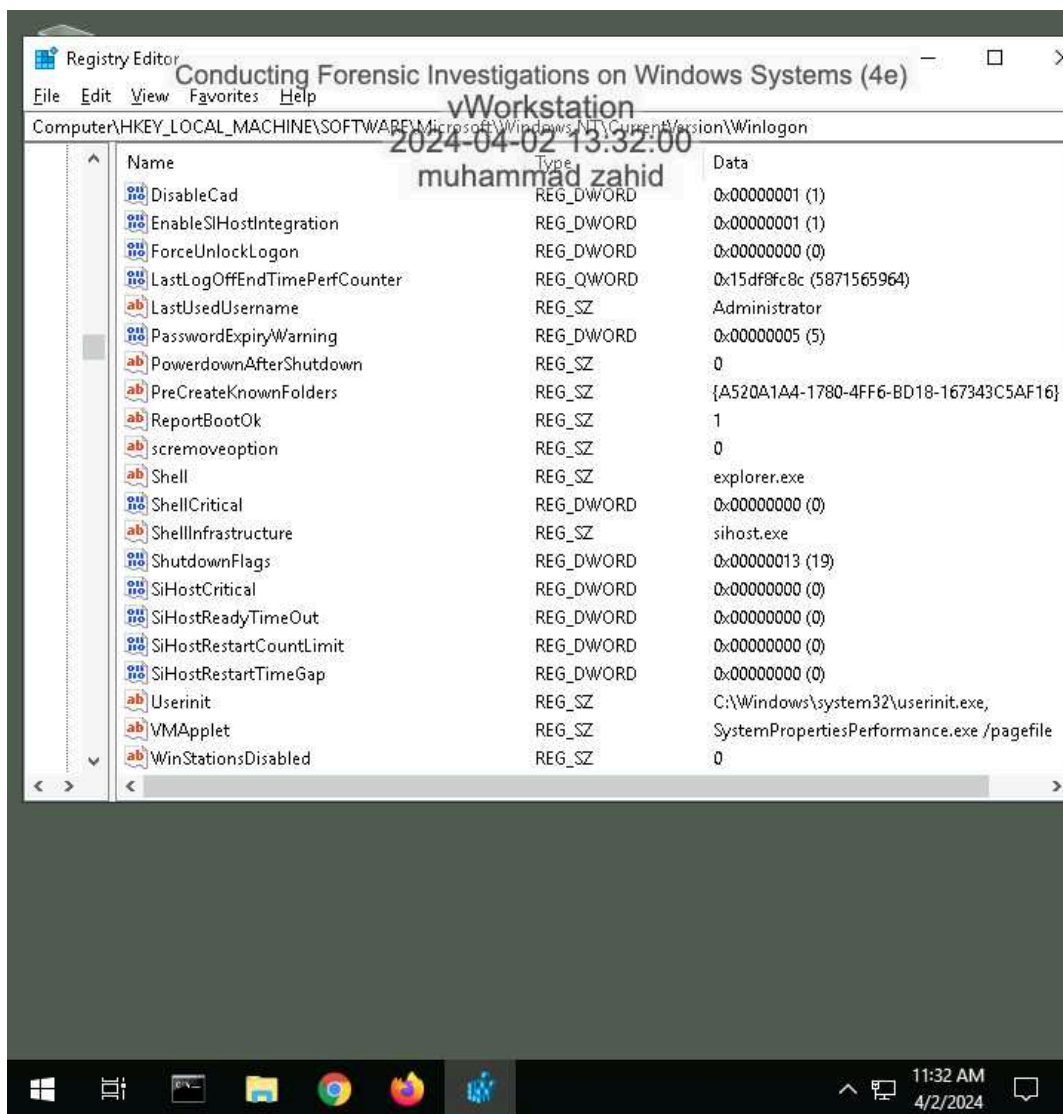
13. **Make a screen capture** showing the **key values for the vWorkstation's default network interface**.



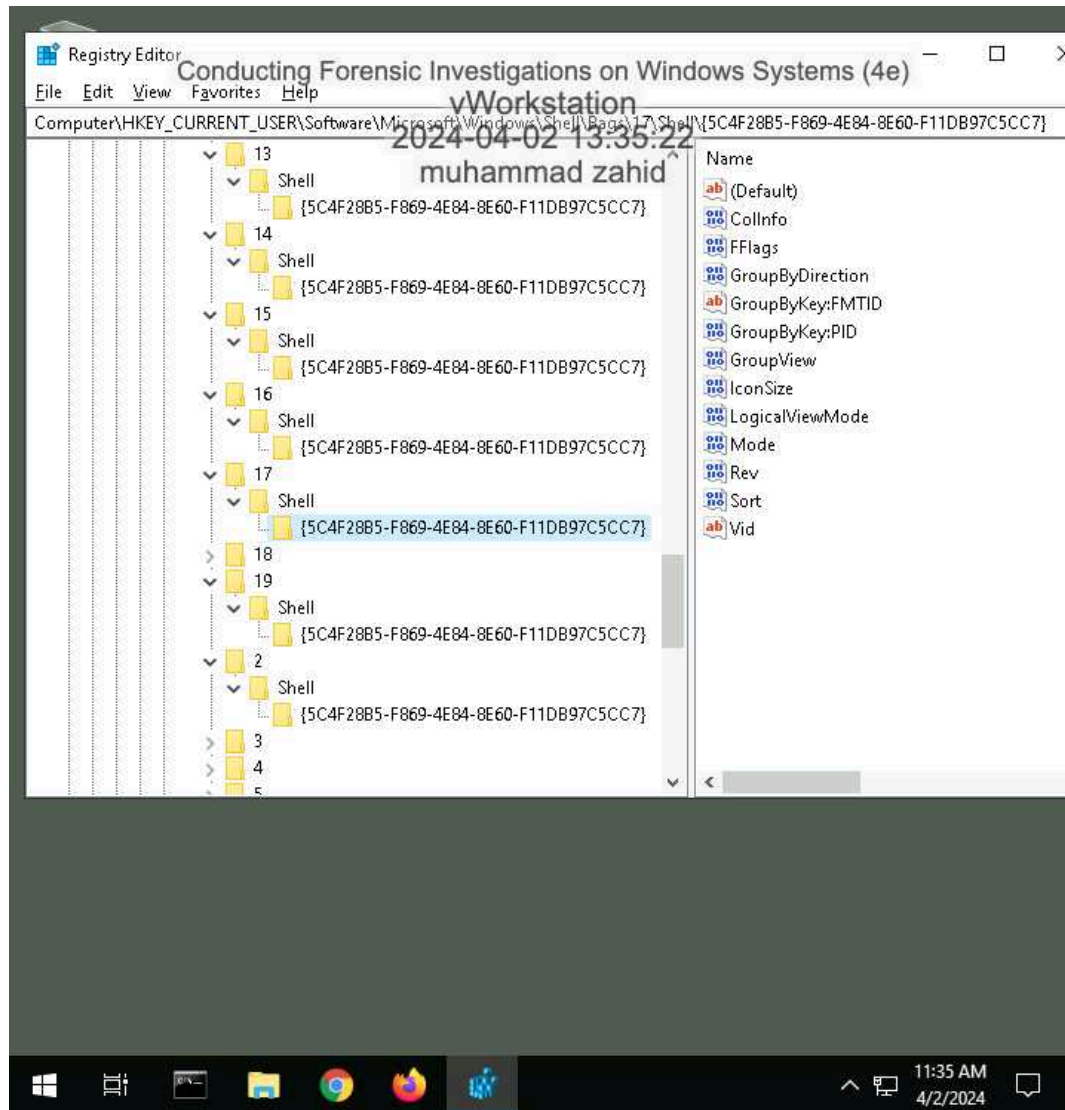
Conducting Forensic Investigations on Windows Systems (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 05

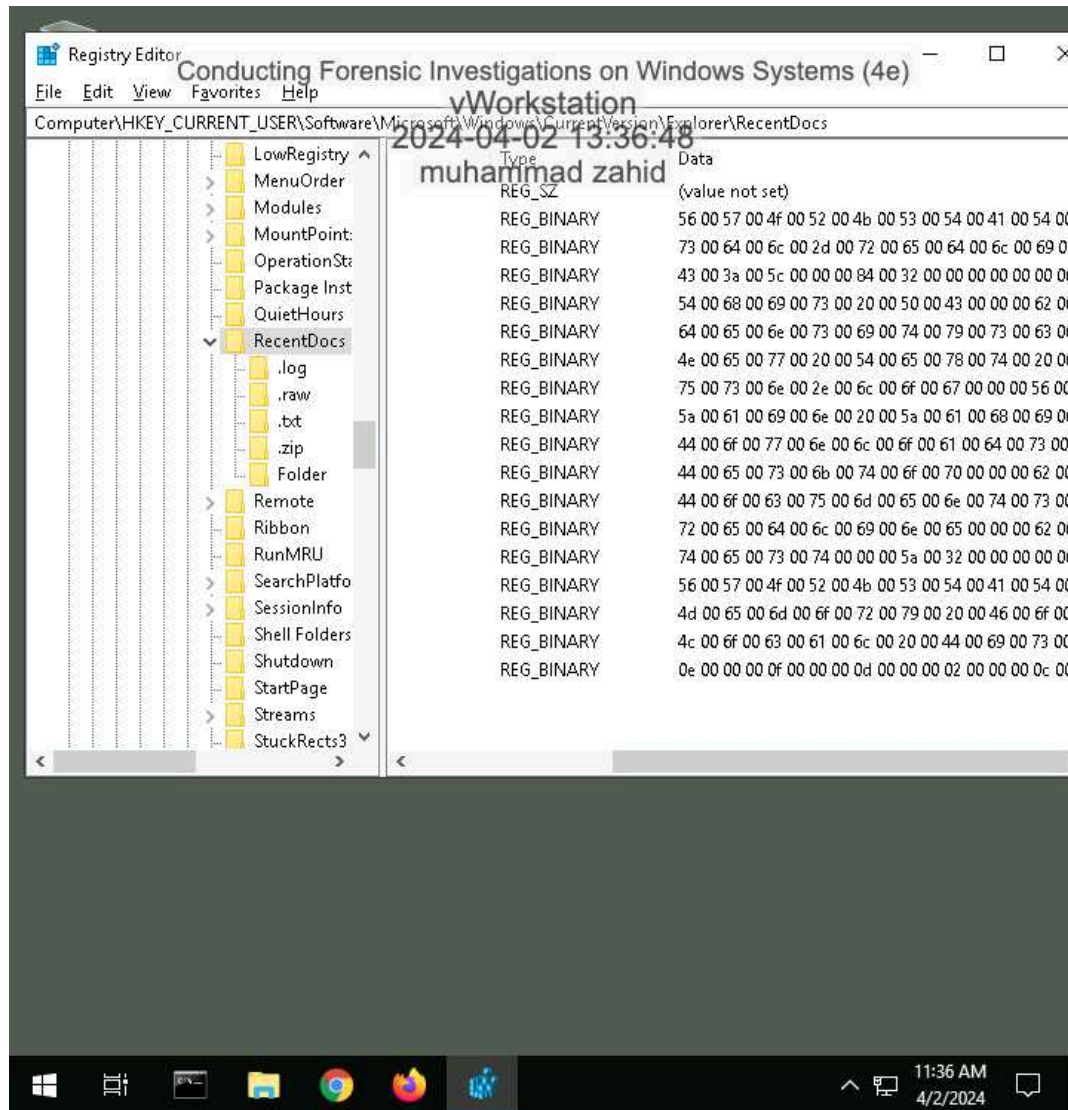
15. Make a screen capture showing the Winlogon key values.



18. Make a screen capture showing the **ShellBags** key values.



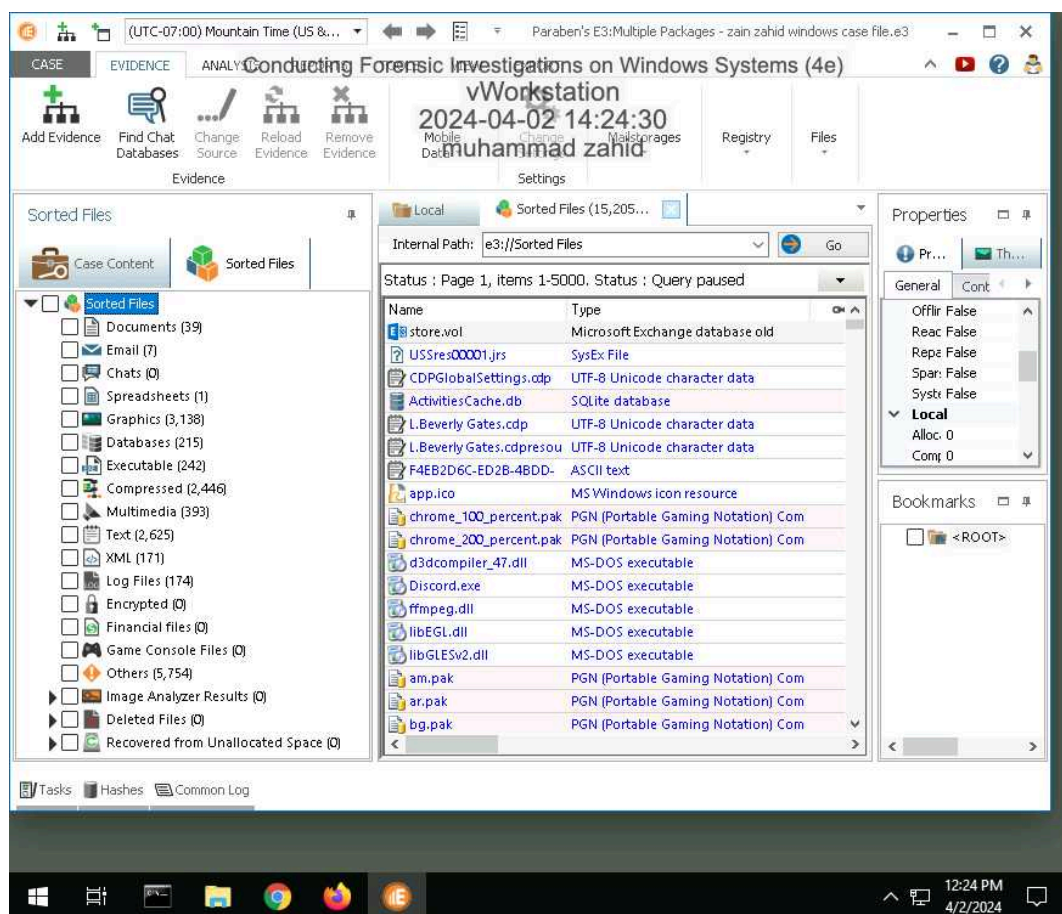
20. Make a screen capture showing the RecentDocs key values.



Section 2: Applied Learning

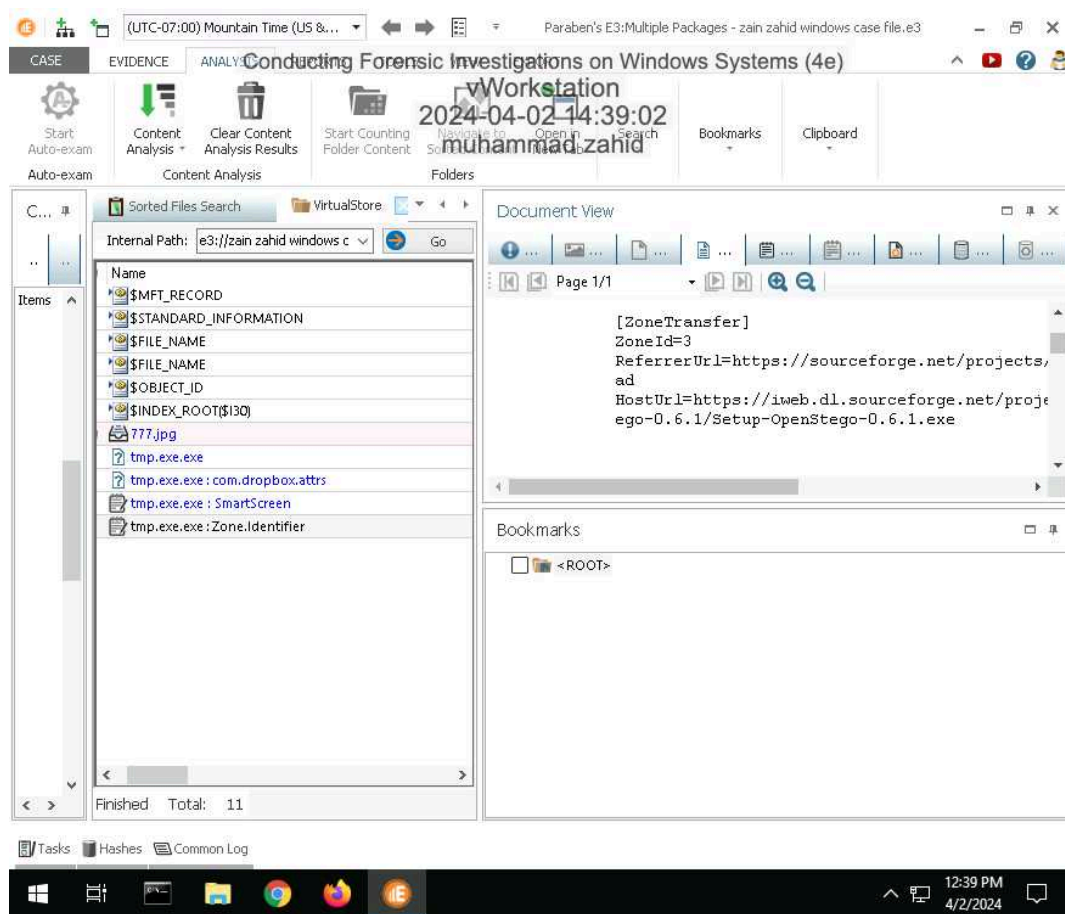
Part 1: Create and Sort a New Case File

14. Make a screen capture showing the **Sorted Files**.



Part 2: Perform Forensic Analysis on a Windows Drive Image

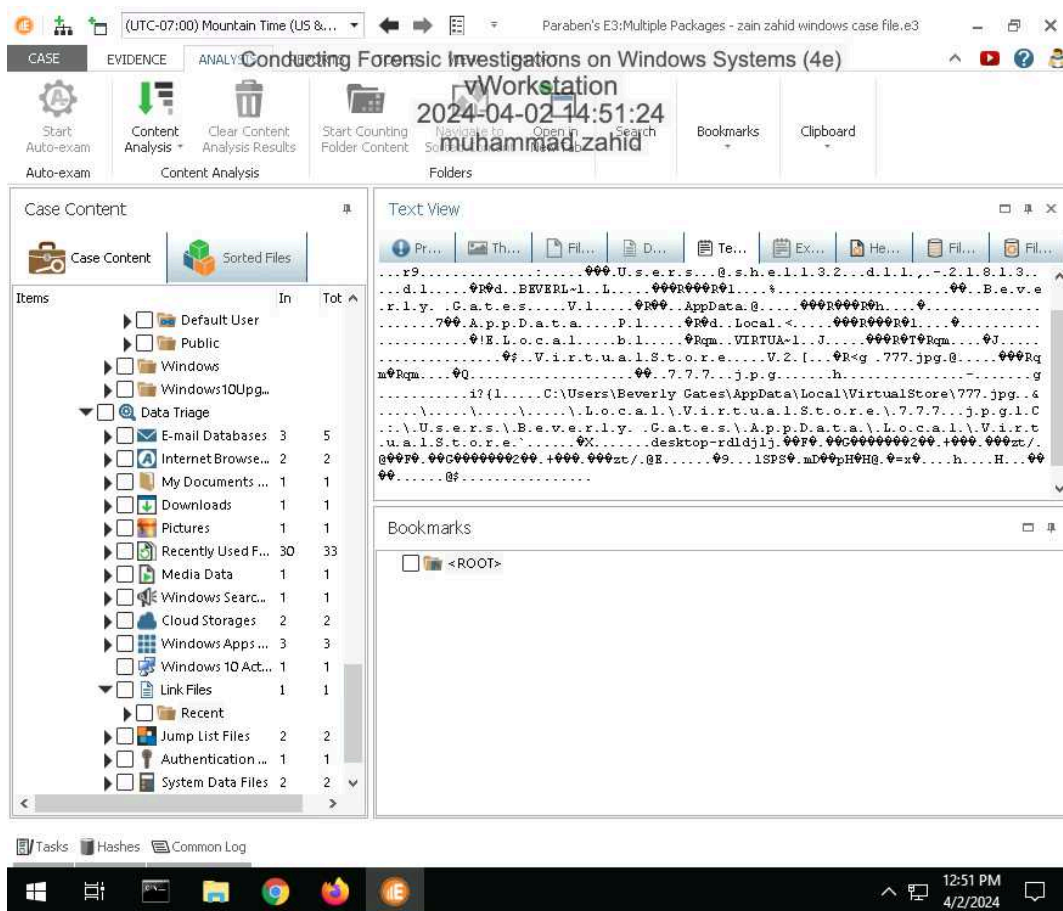
6. Make a screen capture showing the contents of the 777.jpg file in the Document View.



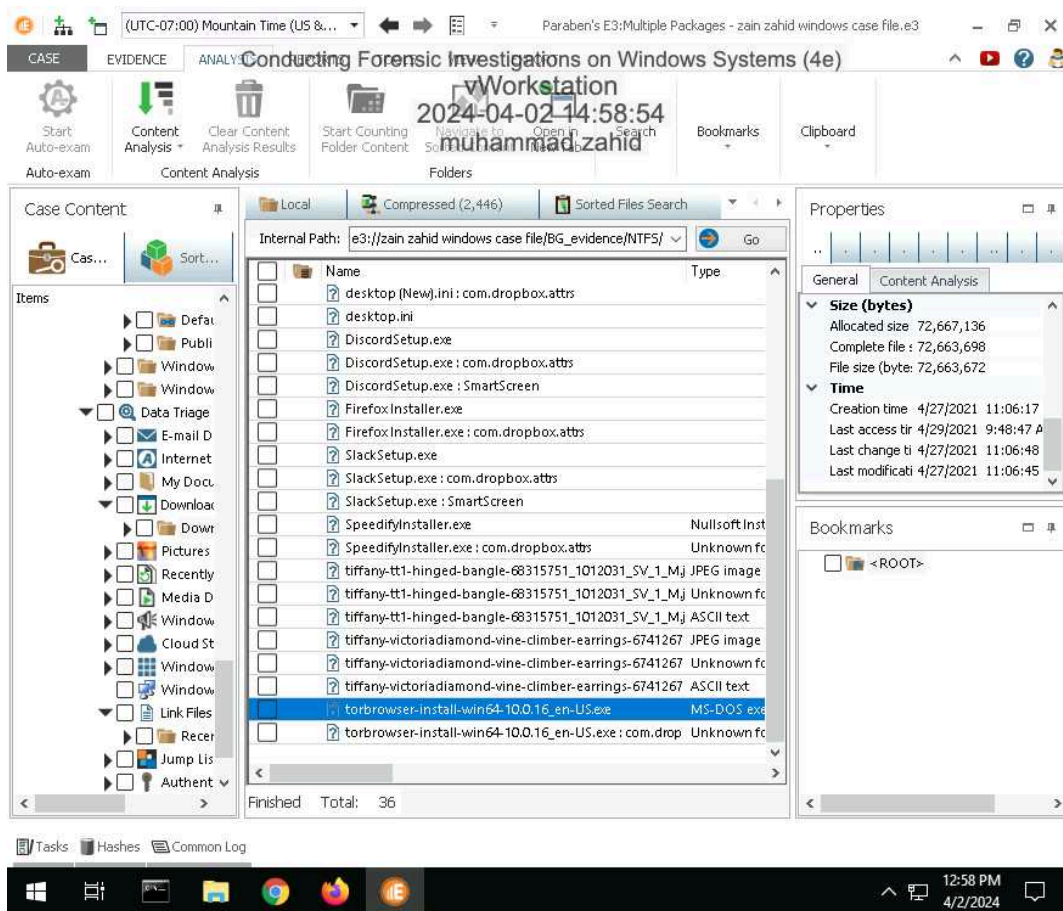
Conducting Forensic Investigations on Windows Systems (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 05

10. Make a screen capture showing the 777.lnk file contents including the path to the file in the system.



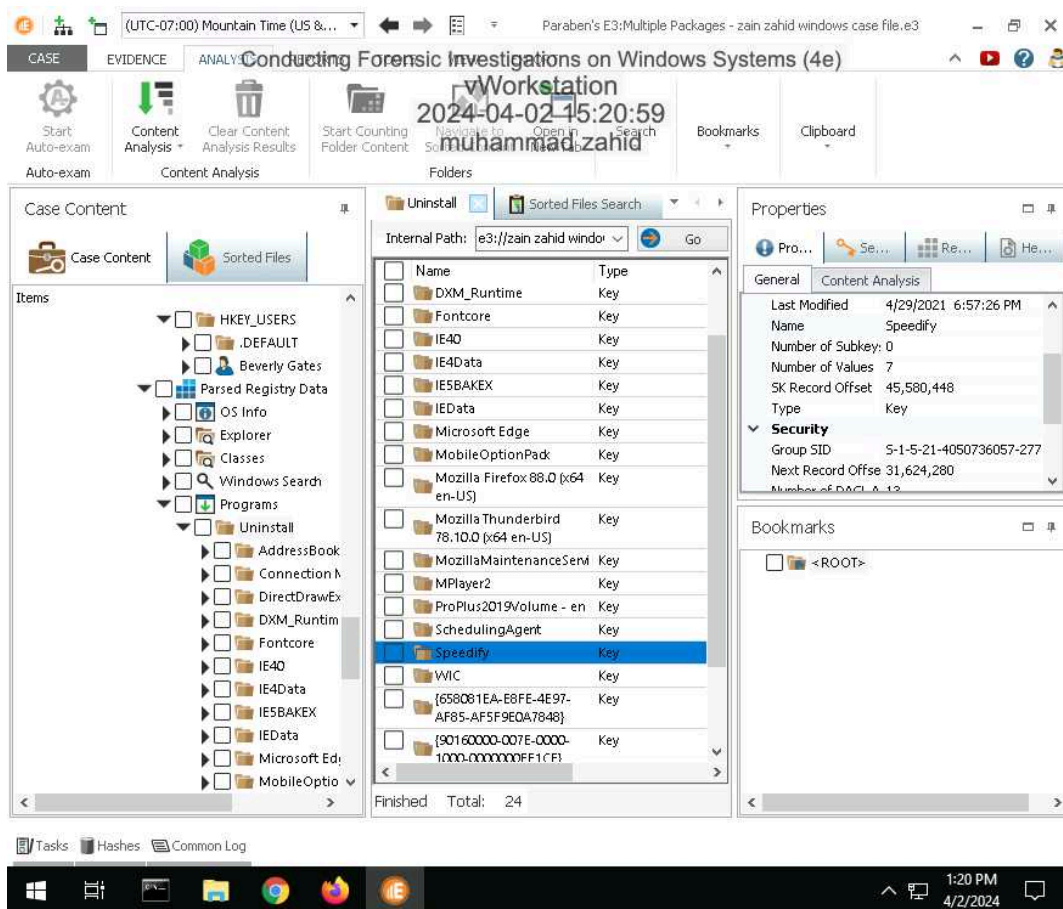
14. **Make a screen capture** showing the **installation files** for suspicious apps in the **Downloads** category.



Conducting Forensic Investigations on Windows Systems (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 05

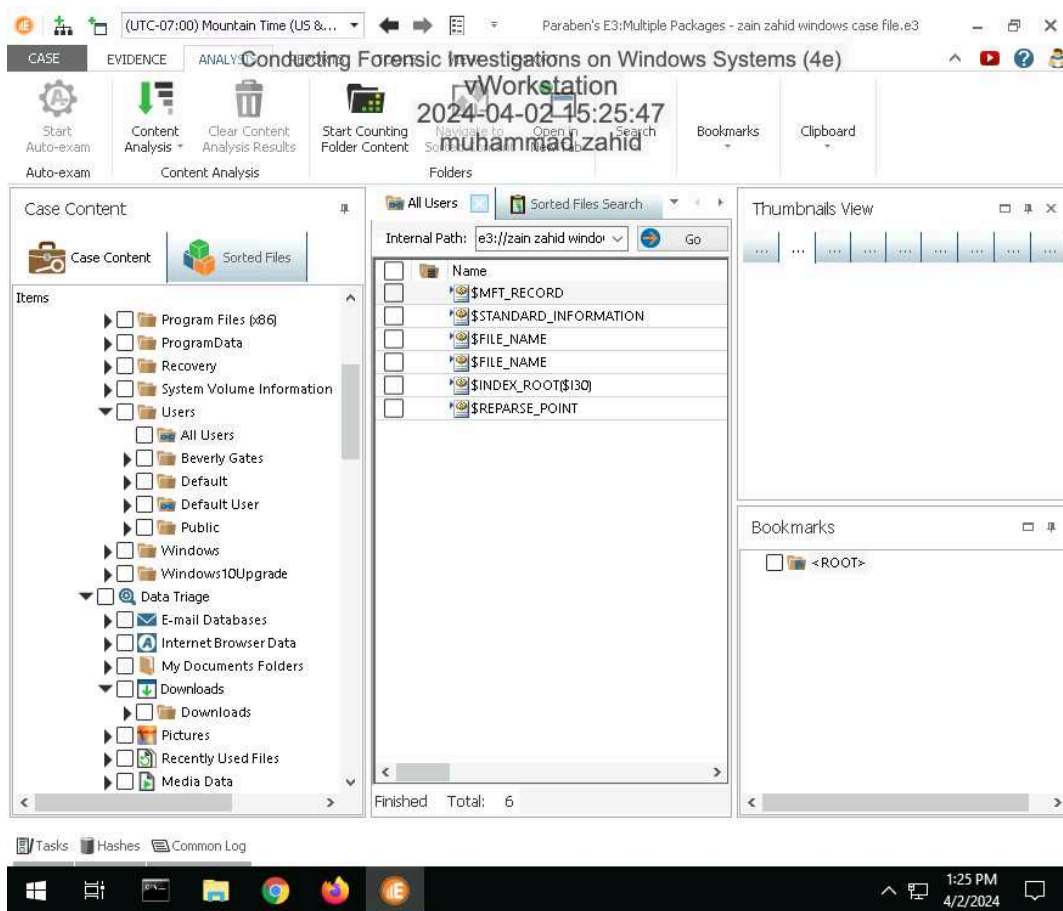
17. Make a screen capture showing the VPN application (Speedify) in the Uninstall folder.



Conducting Forensic Investigations on Windows Systems (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 05

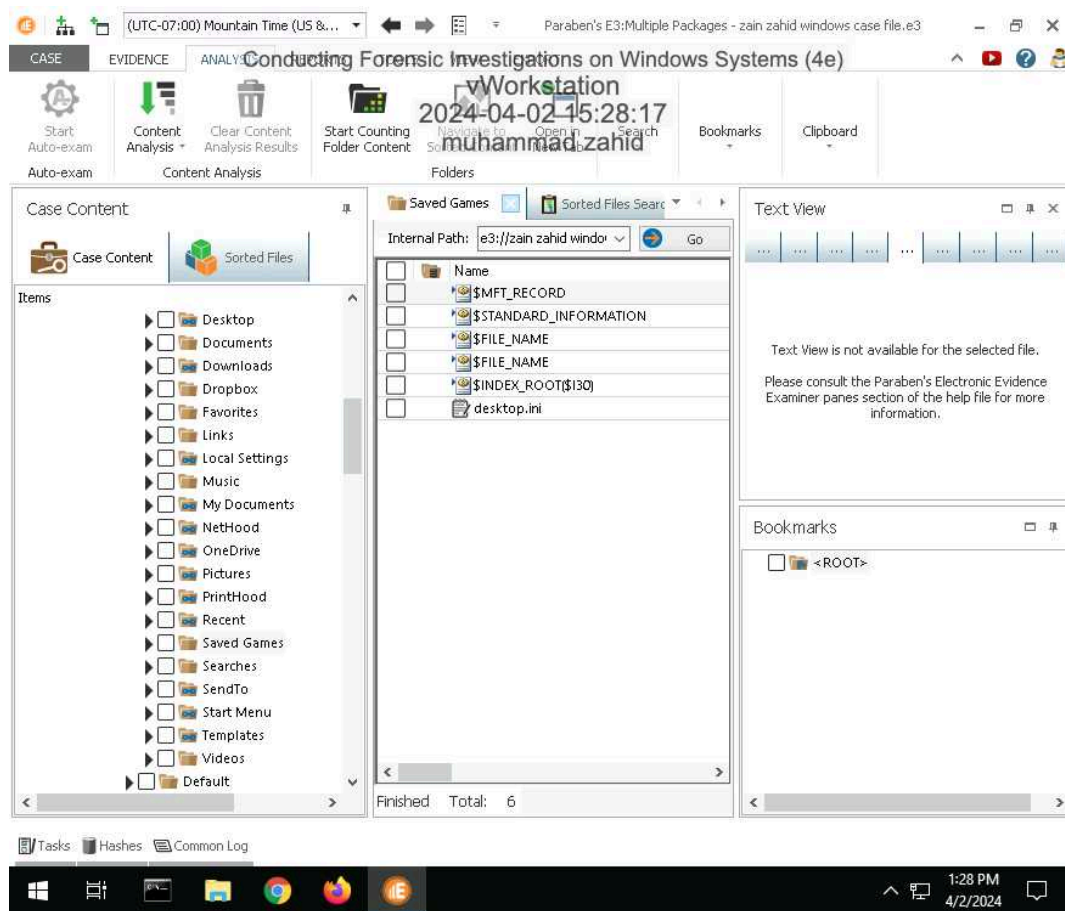
19. Make a screen capture showing the users list.



Conducting Forensic Investigations on Windows Systems (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 05

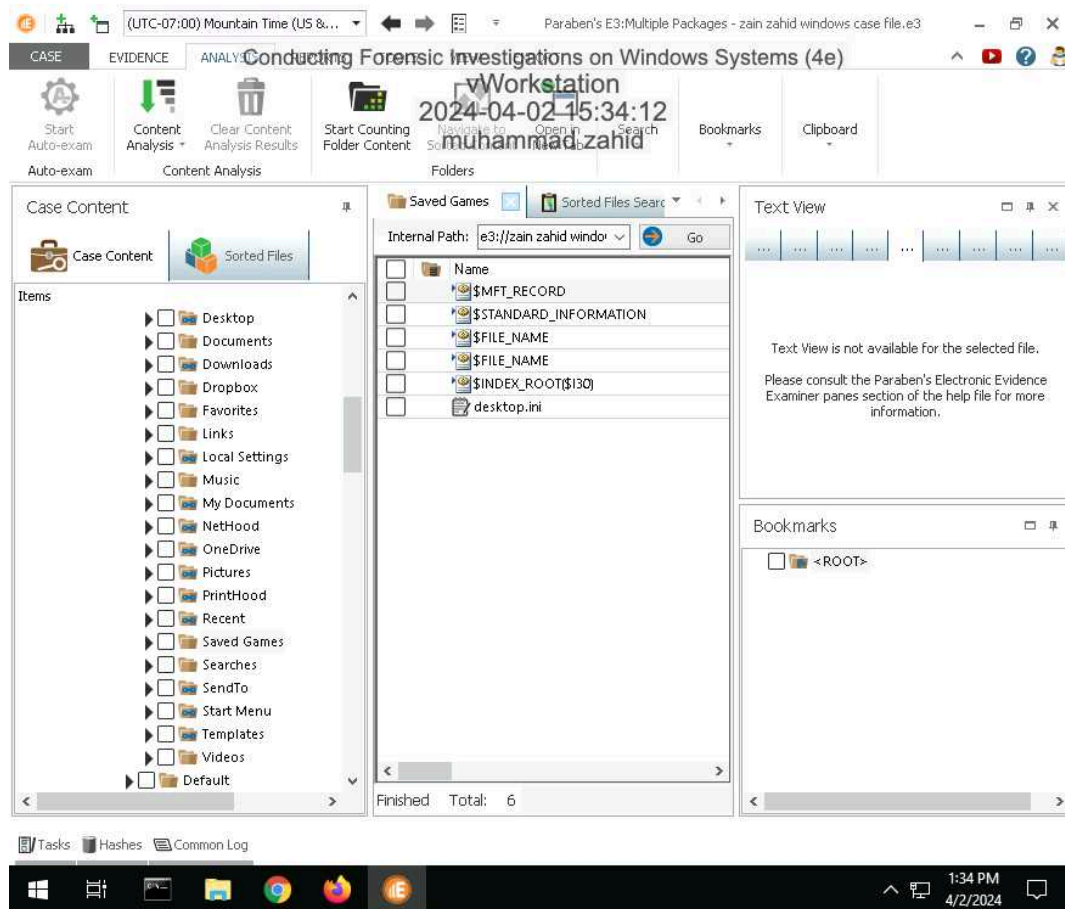
21. Make a screen capture showing the contents of the Beverly Gates / Run folder.



Conducting Forensic Investigations on Windows Systems (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 05

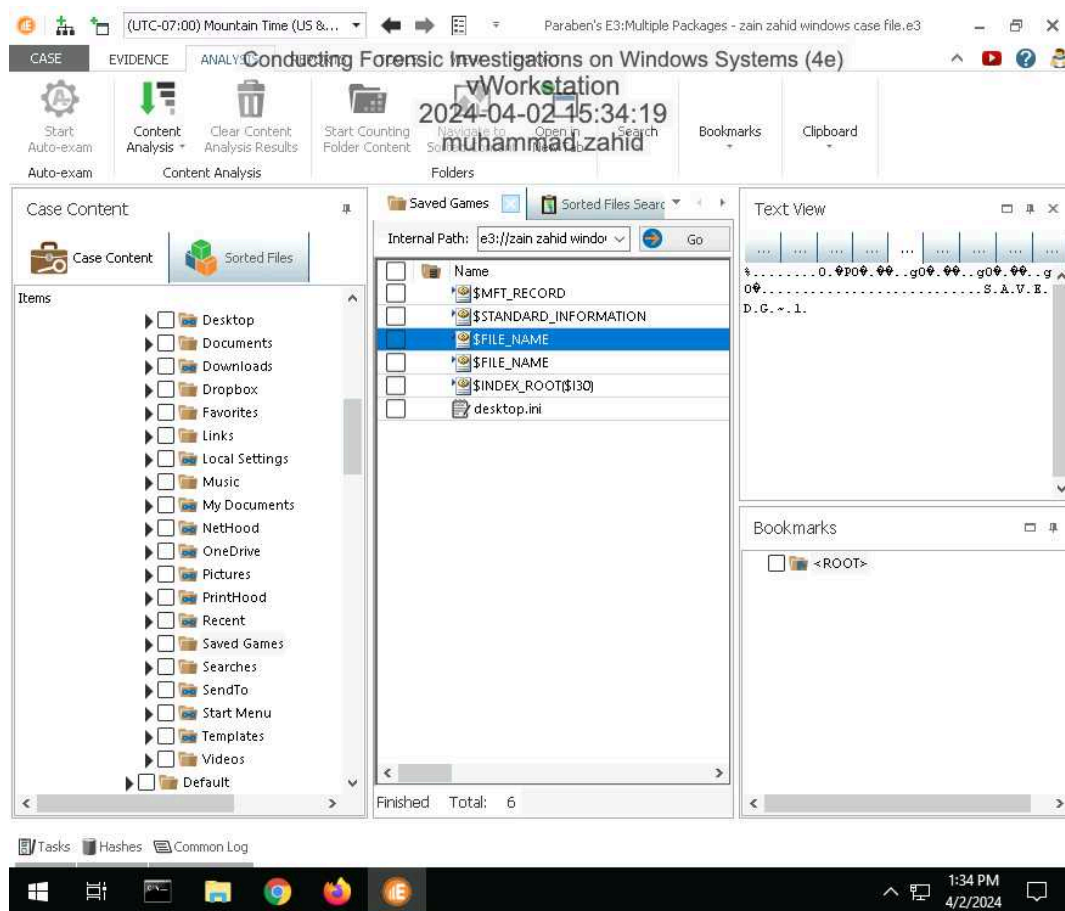
24. Make a screen capture showing at least one suspicious browsing record found in the History sub-node.



Conducting Forensic Investigations on Windows Systems (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 05

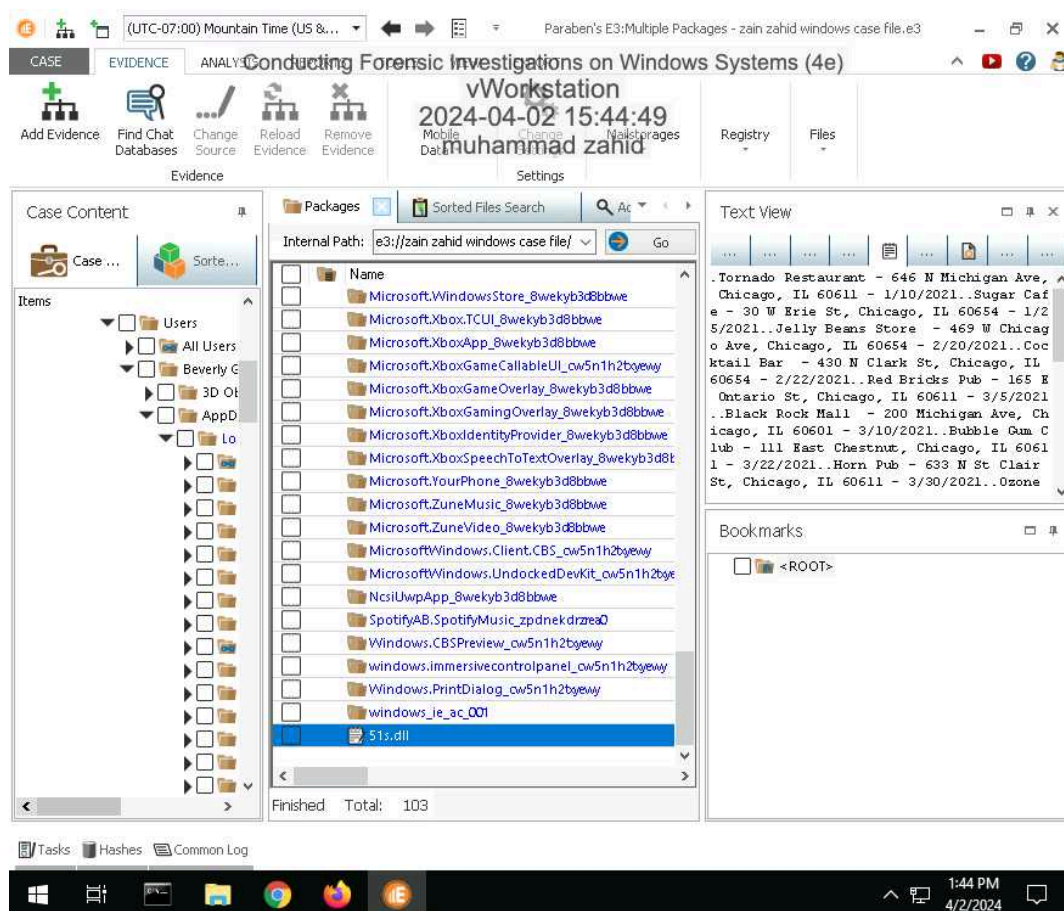
26. Make a screen capture showing at least one suspicious search found in the Keywords sub-node.



Section 3: Challenge and Analysis

Part 1: Use Advanced Search to Locate Additional Evidence

Make a screen capture showing the contents of the suspicious file in the Document View.



Part 2: Identify Suspicious Browser Activity

Conducting Forensic Investigations on Windows Systems (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 05

Make a screen capture showing at least one registry key with information associated with Tor and Firefox.

