

Student:	Email:
Matias Kun	rvh4zx@virginia.edu

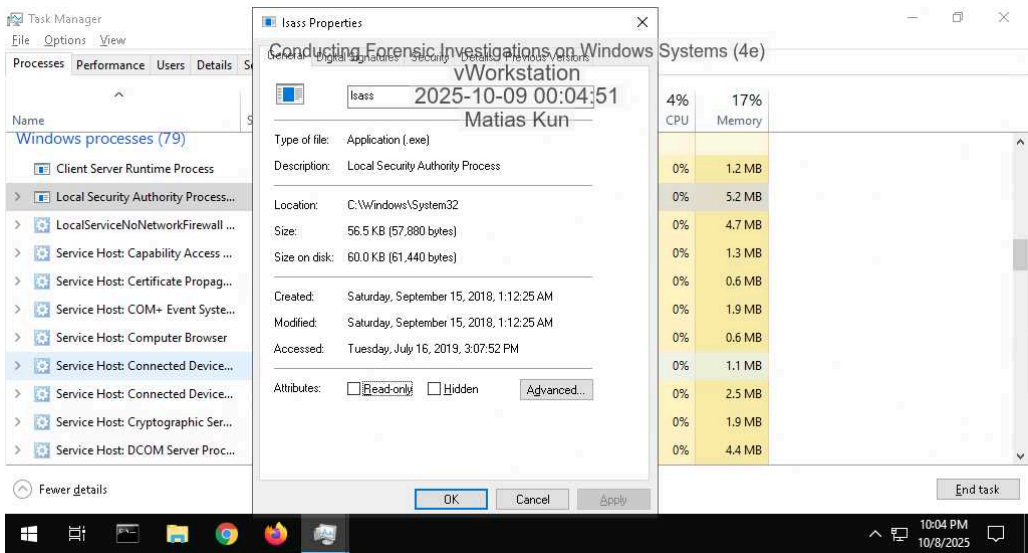
Time on Task:	Progress:
11 hours, 40 minutes	100%

Report Generated: Friday, October 17, 2025 at 5:24 PM

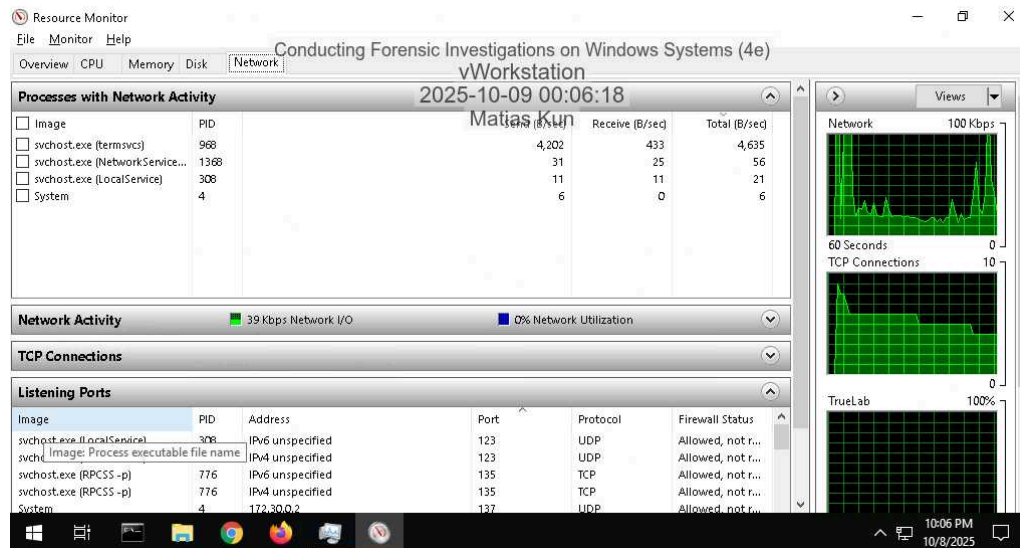
Section 1: Hands-On Demonstration

Part 1: Gather Basic System Information

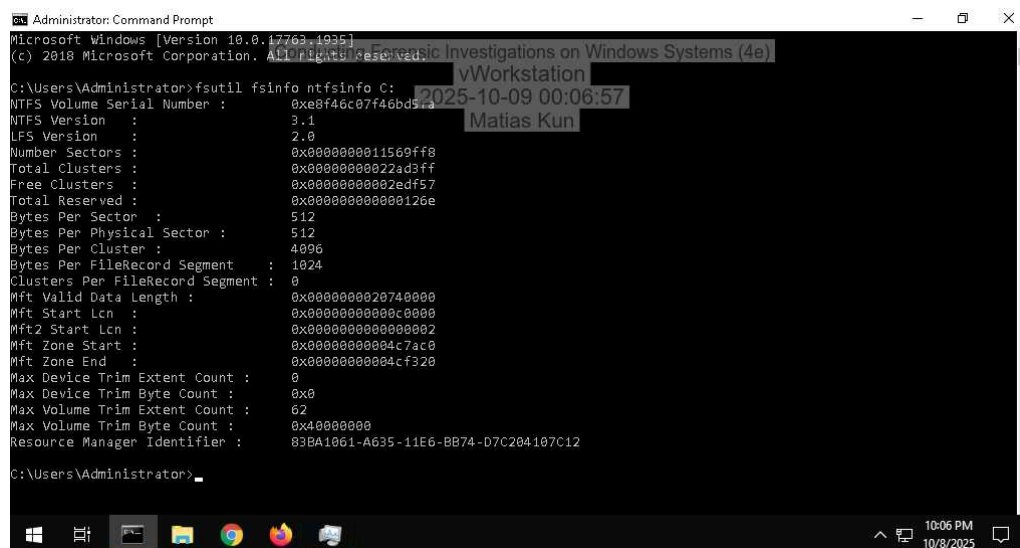
- 4. Make a screen capture showing the Properties window for the process you selected.



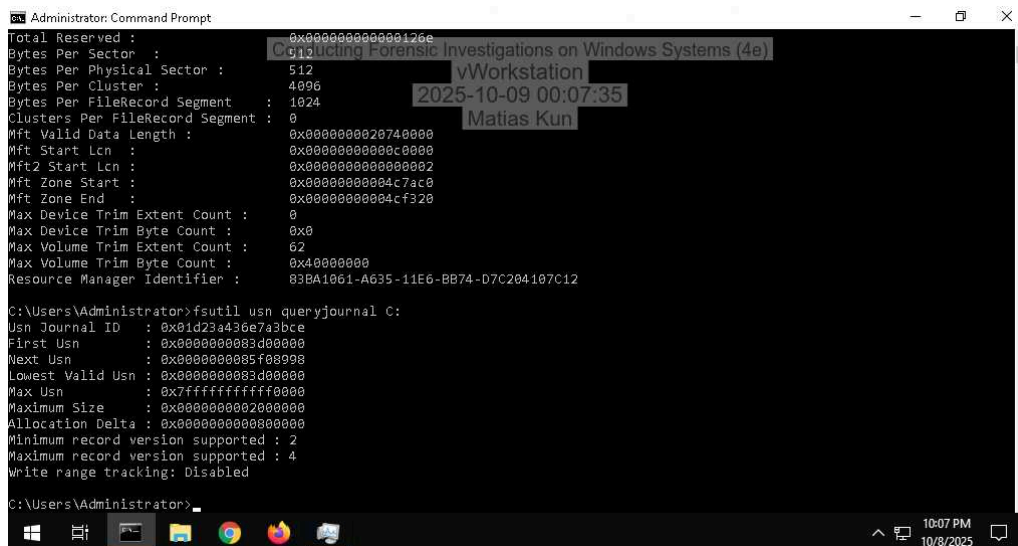
10. Make a screen capture showing the Listening Ports list.



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



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

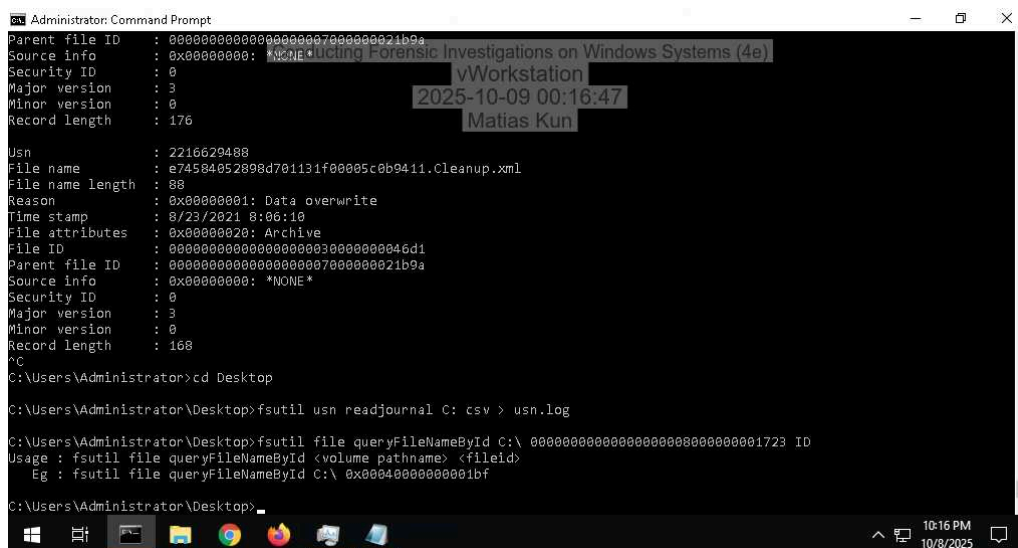


```
Administrator: Command Prompt
Total Reserved : 0x000000000000126e
Bytes Per Sector : 512
Bytes Per Physical Sector : 4096
Bytes Per FileRecord Segment : 1024
Clusters Per FileRecord Segment : 0
Mft Valid Data Length : 0x0000000020740000
Mft Start Lcn : 0x000000000000c0000
Mft2 Start Lcn : 0x0000000000000002
Mft Zone Start : 0x0000000000004c7ac0
Mft Zone End : 0x0000000000004cf320
Max Device Trim Extent Count : 0
Max Device Trim Byte Count : 0x0
Max Volume Trim Extent Count : 62
Max Volume Trim Byte Count : 0x4000000
Resource Manager Identifier : 83BA1061-A635-11E6-BB74-D7C204107C12

C:\Users\Administrator>fsutil usn queryjournal C:
Usn Journal ID : 0x01d23a436e7a3bce
First Usn : 0x0000000000000000
Next Usn : 0x0000000000005f089908
Lowest Valid Usn : 0x0000000000000000
Max Usn : 0x7fffffffffffffff0000
Maximum Size : 0x0000000020000000
Allocation Delta : 0x0000000000000000
Minimum record version supported : 2
Maximum record version supported : 4
Write range tracking: Disabled

C:\Users\Administrator>
```

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



```
Administrator: Command Prompt
Parent file ID : 00000000000000007000000021b9a
Source info : 0x00000000: *NONE*
Security ID : 0
Major version : 3
Minor version : 0
Record length : 176

Usn : 2216629488
File name : e74584052898d701131f00005c0b9411.Cleanup.xml
File name length : 88
Reason : 0x00000001: Data overwrite
Time stamp : 8/23/2021 8:06:10
File attributes : 0x00000020: Archive
File ID : 0000000000000000030000000046d1
Parent file ID : 00000000000000000700000021b9a
Source info : 0x00000000: *NONE*
Security ID : 0
Major version : 3
Minor version : 0
Record length : 168
^C

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

C:\Users\Administrator\Desktop>fsutil file queryFileNameById C:\ 00000000000000000000000000001723 ID
Usage : fsutil file queryFileNameById <volume pathname> <fileid>
Eg : fsutil file queryFileNameById C:\ 0x000400000000001bf

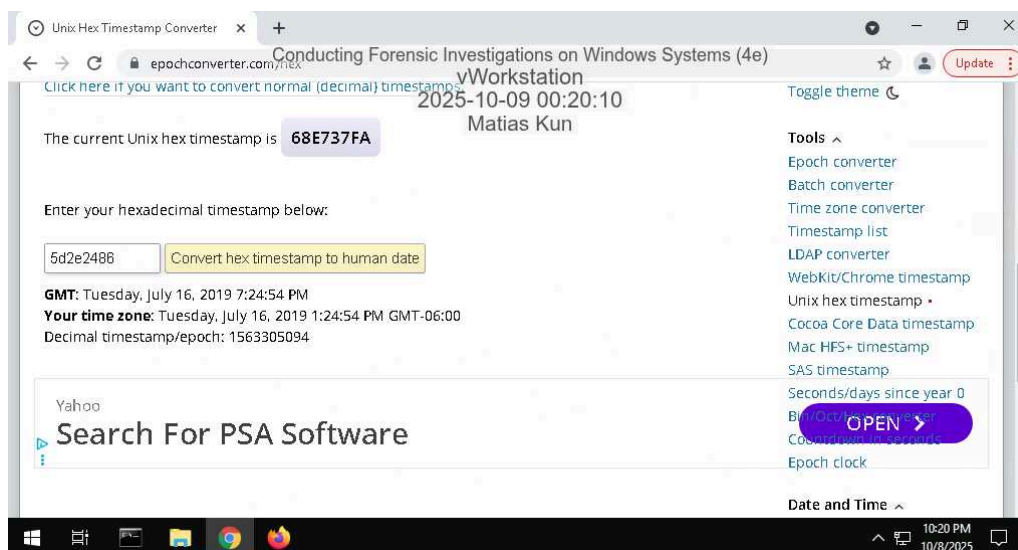
C:\Users\Administrator\Desktop>
```

Part 2: Explore the Registry

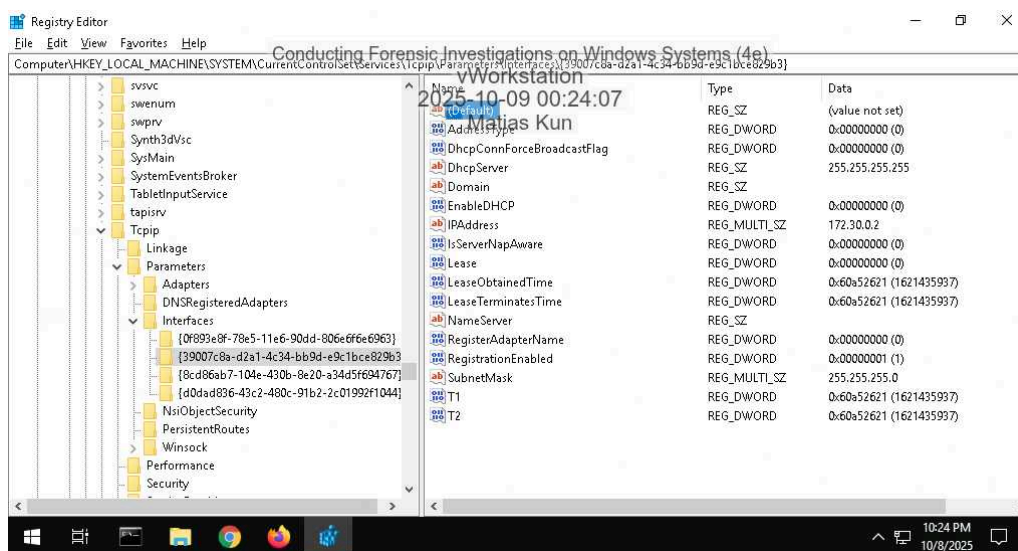
Conducting Forensic Investigations on Windows Systems (4e)

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

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



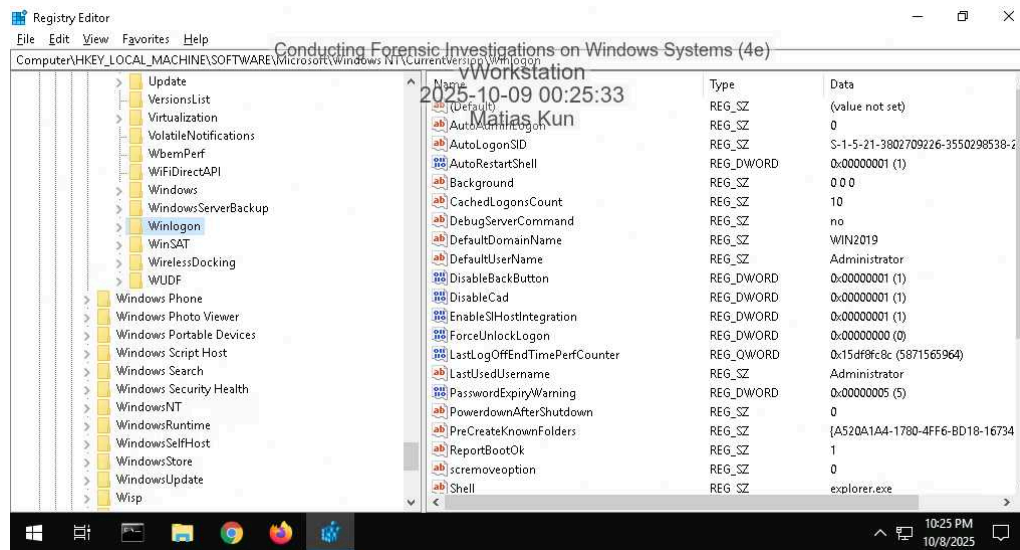
13. Make a screen capture showing the key values for the vWorkstation's default network interface.



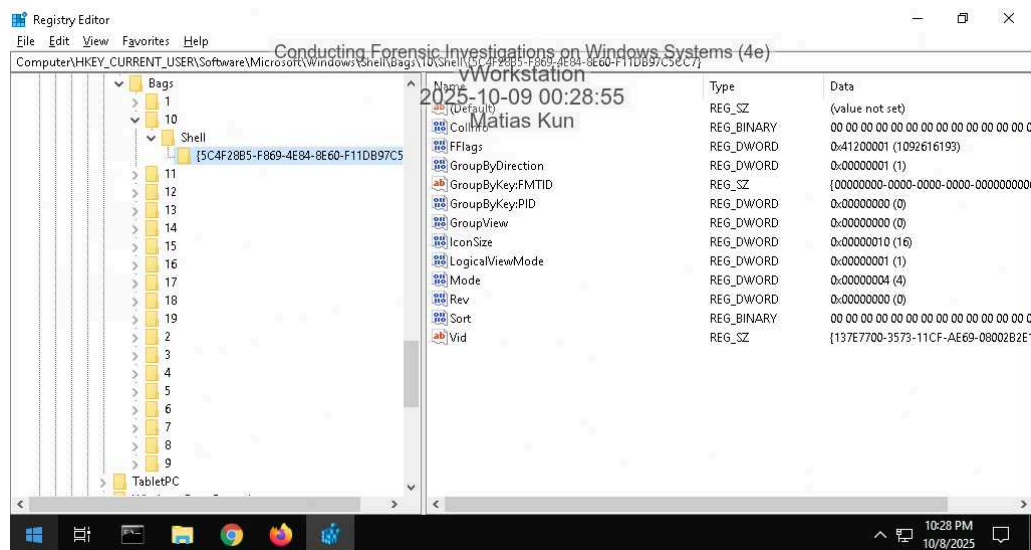
Conducting Forensic Investigations on Windows Systems (4e)

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.



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

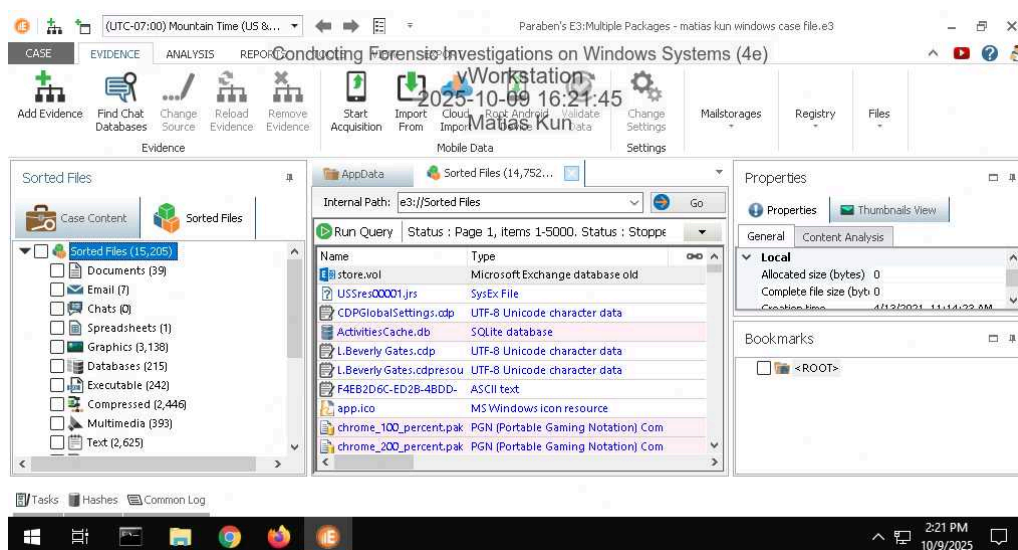
The screenshot shows the Windows Registry Editor interface. On the left, the tree view is expanded to show the path: Computer > HKEY_CURRENT_USER > Software > Microsoft > Windows > CurrentVersion > Explorer > RecentDocs. The right pane displays a list of registry values for RecentDocs, organized by Name, Type, and Data.

Name	Type	Data
(Default)	REG_SZ	(value not set)
0	REG_BINARY	56 00 57 00 4f 00 52 00 4b 00 53 00 54 ...
1	REG_BINARY	73 00 64 00 6c 00 2d 00 72 00 65 00 64 ...
10	REG_BINARY	43 00 3a 00 5c 00 00 00 84 00 32 00 00 ...
11	REG_BINARY	54 00 68 00 69 00 73 00 20 00 50 00 43 ...
12	REG_BINARY	64 00 65 00 6e 00 73 00 69 00 74 00 79 ...
13	REG_BINARY	4d 00 61 00 74 00 69 00 61 00 73 00 20 ...
14	REG_BINARY	75 00 73 00 6e 00 2e 00 6c 00 6f 00 67 ...
2	REG_BINARY	44 00 6f 00 77 00 6e 00 6c 00 6f 00 61 ...
3	REG_BINARY	44 00 65 00 73 00 6b 00 74 00 6f 00 70 ...
4	REG_BINARY	44 00 6f 00 63 00 75 00 6d 00 65 00 6e ...
5	REG_BINARY	72 00 65 00 64 00 6c 00 69 00 6e 00 65 ...
6	REG_BINARY	74 00 65 00 73 00 74 00 00 00 5a 00 32 ...
7	REG_BINARY	56 00 57 00 4f 00 52 00 4b 00 53 00 54 ...
8	REG_BINARY	4d 00 65 00 6d 00 6f 00 72 00 79 00 20 ...
9	REG_BINARY	4c 00 6f 00 63 00 61 00 6c 00 20 00 44 ...
MRUListEx	REG_BINARY	0d 00 00 00 0e 00 00 00 02 00 00 00 c...

Section 2: Applied Learning

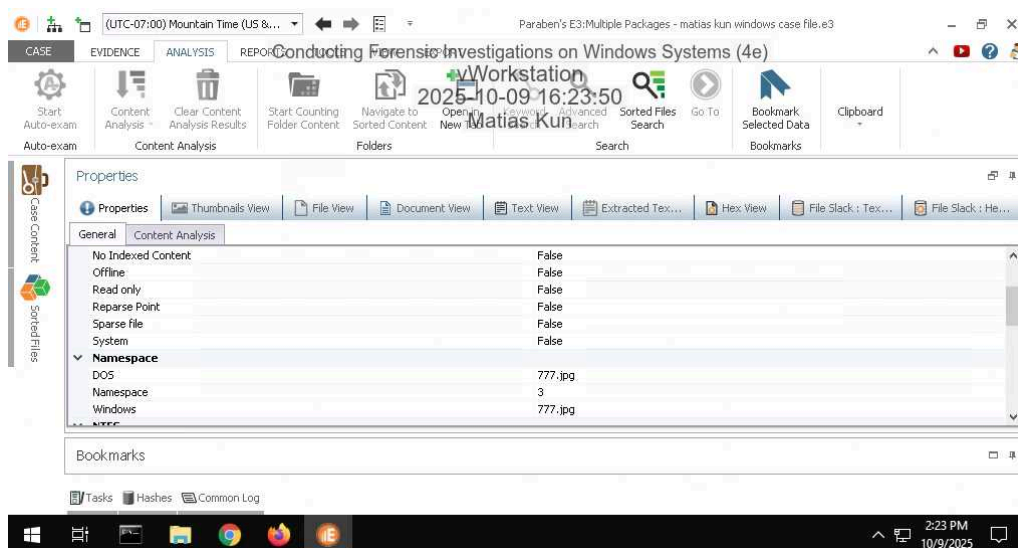
Part 1: Create and Sort a New Case File

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



Part 2: Perform Forensic Analysis on a Windows Drive Image

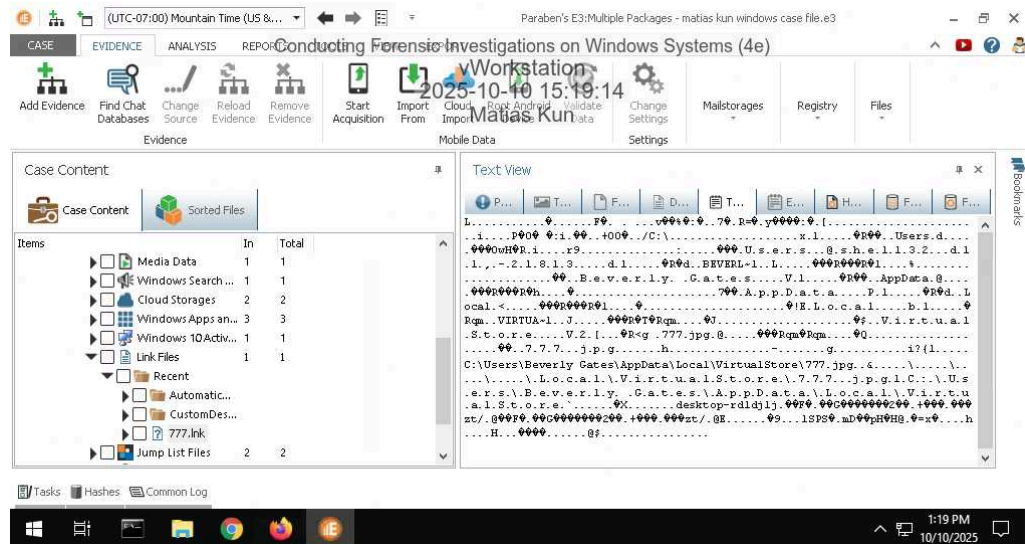
6. Make a screen capture showing the contents of the 777.jpg file in the Document View.



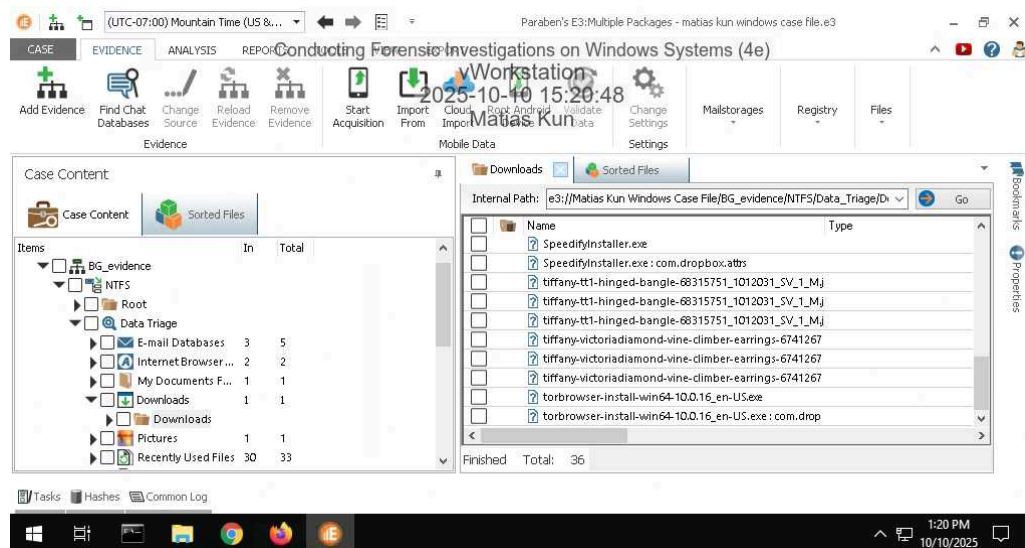
Conducting Forensic Investigations on Windows Systems (4e)

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

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



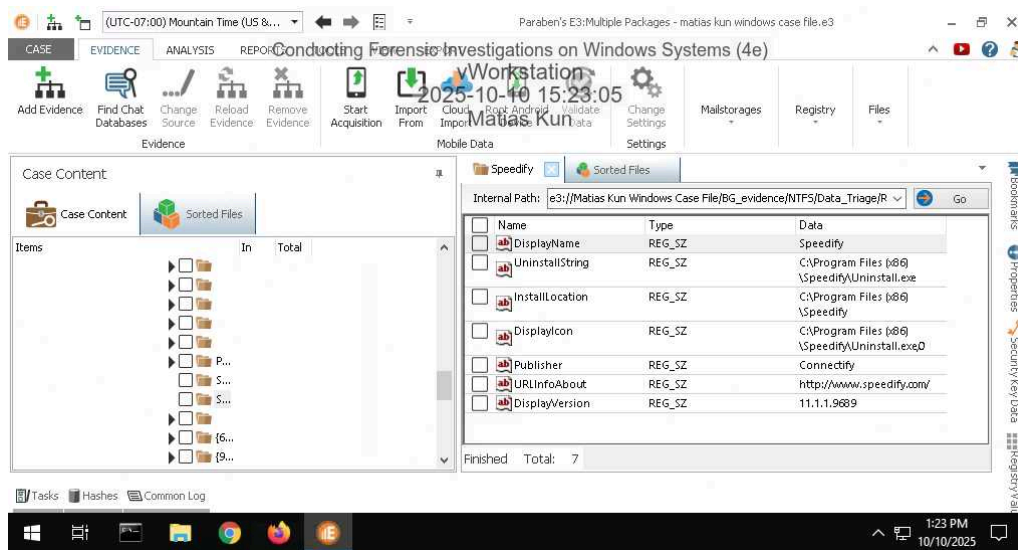
14. Make a screen capture showing the installation files for suspicious apps in the Downloads category.



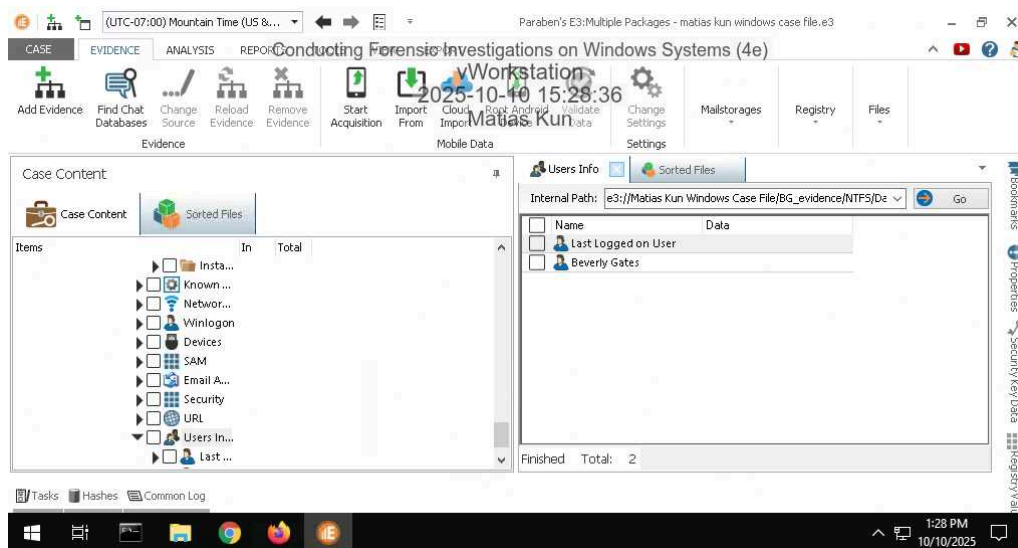
Conducting Forensic Investigations on Windows Systems (4e)

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

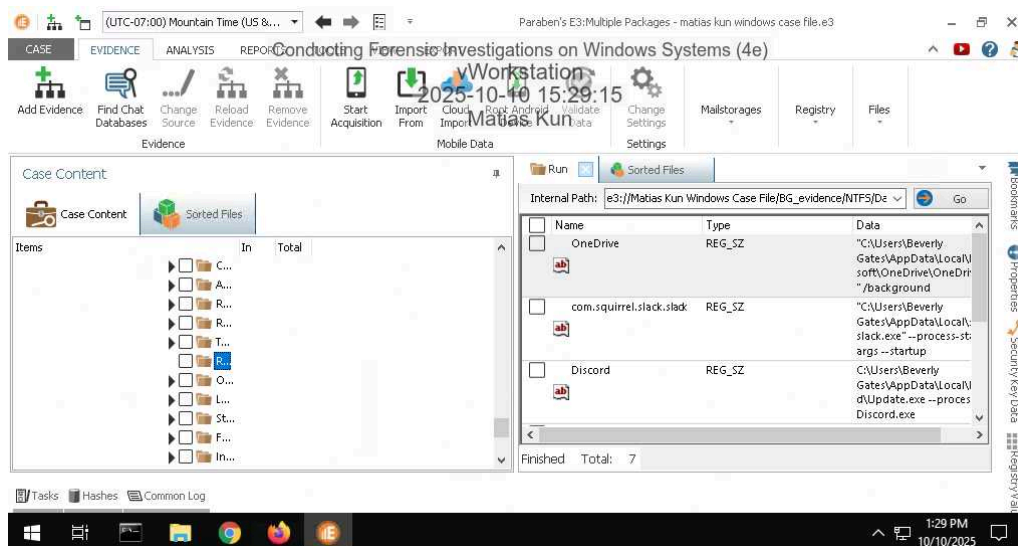
17. Make a screen capture showing the VPN application (Speedify) in the Uninstall folder.



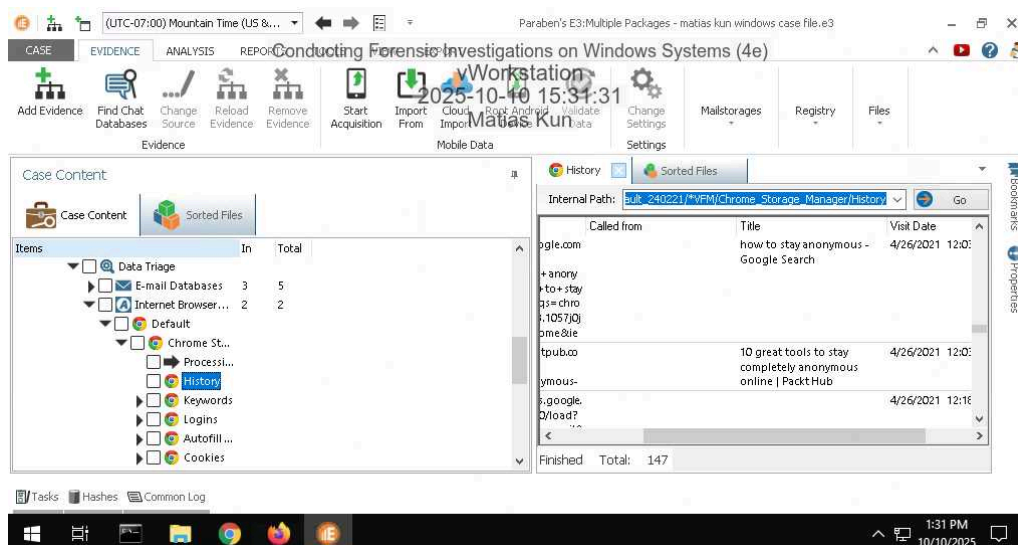
19. Make a screen capture showing the users list.



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



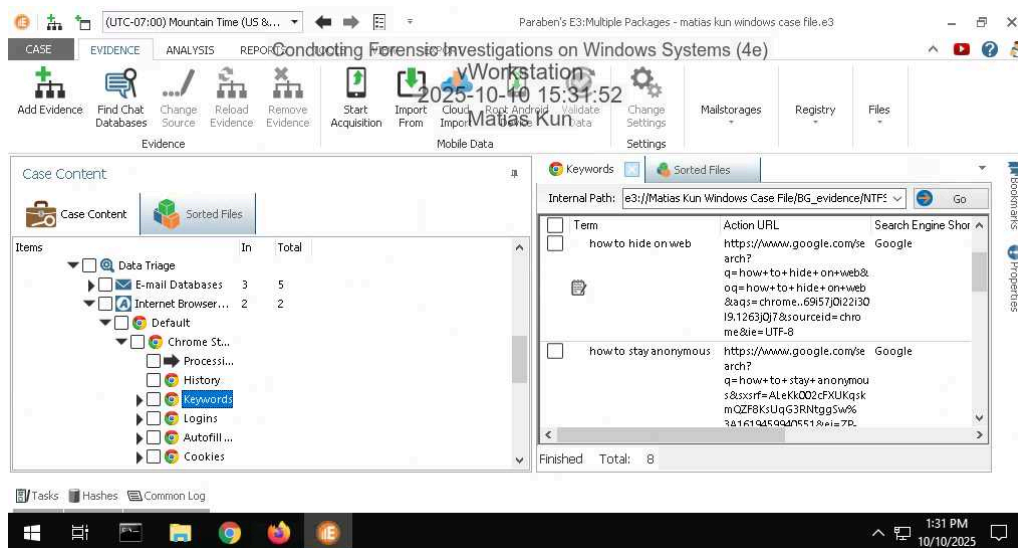
24. Make a screen capture showing at least one suspicious browsing record found in the History sub-node.



Conducting Forensic Investigations on Windows Systems (4e)

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

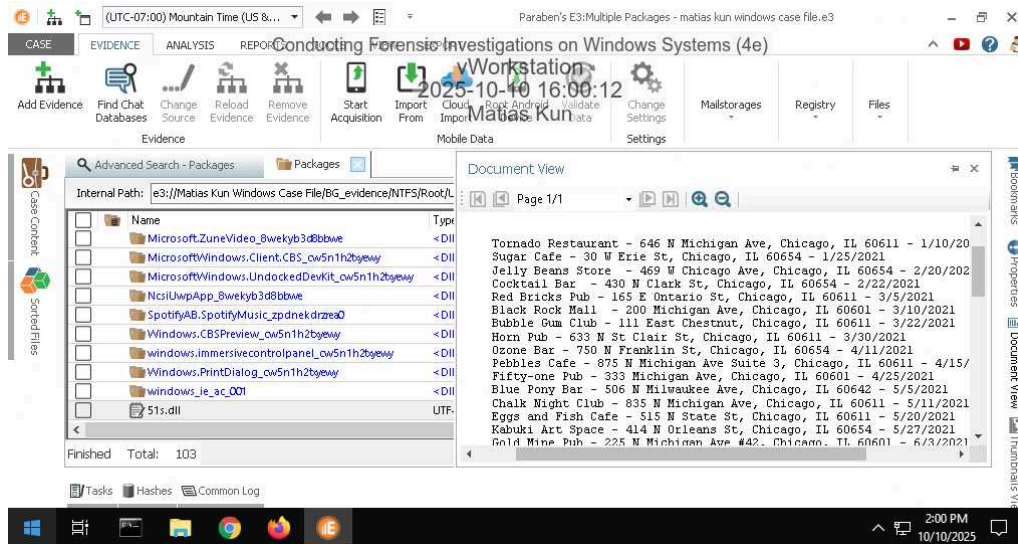
26. Make a screen capture showing at least one suspicious search found in the Keywords sub-node.



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

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

