

Conducting Forensic Investigations on Windows Systems (4e)

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

Student:

Alexis Cherpes

Email:

cherpea@ferris.edu

Time on Task:

4 hours, 30 minutes

Progress:

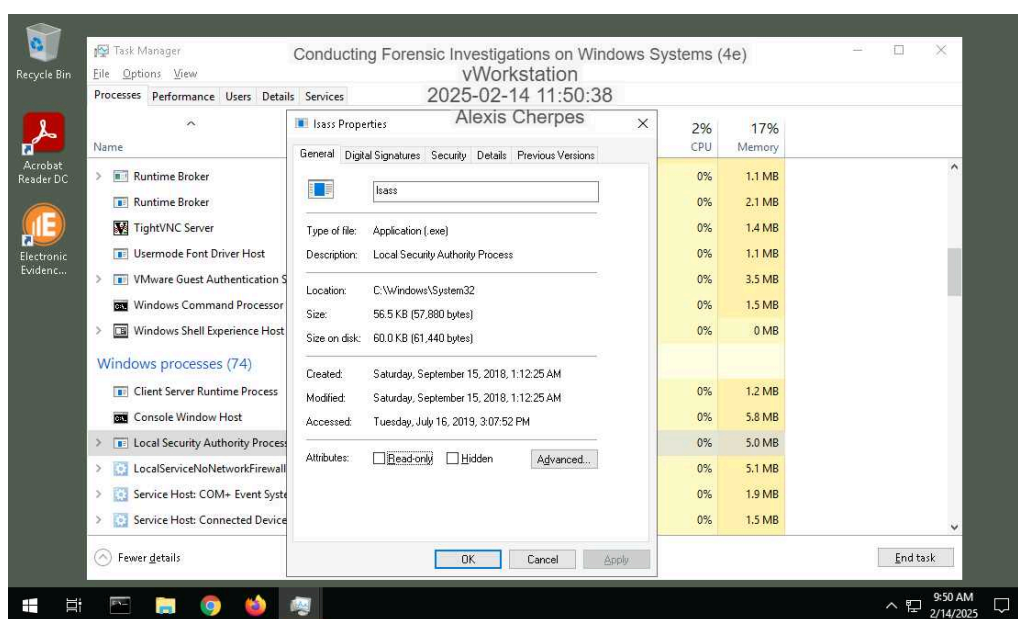
100%

Report Generated: Thursday, May 22, 2025 at 4:49 PM

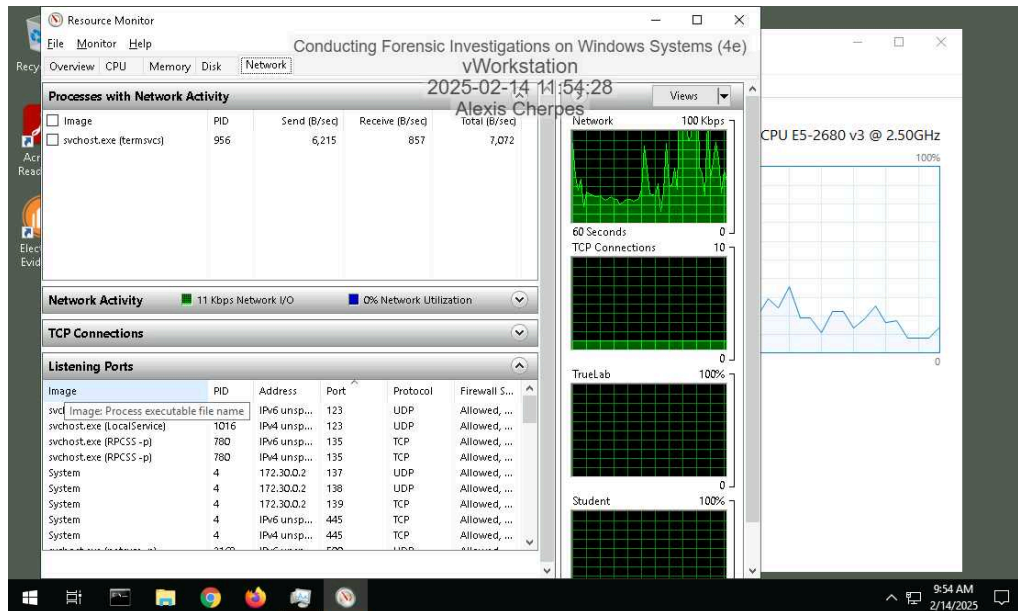
Section 1: Hands-On Demonstration

Part 1: Gather Basic System Information

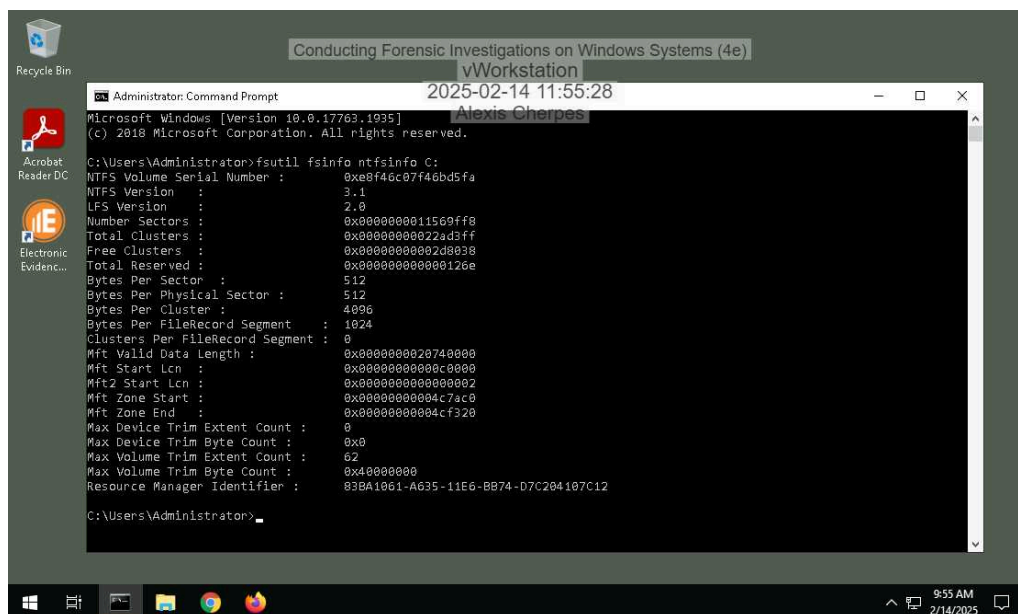
4. Make a screen capture showing the **Properties** window for the process you selected.



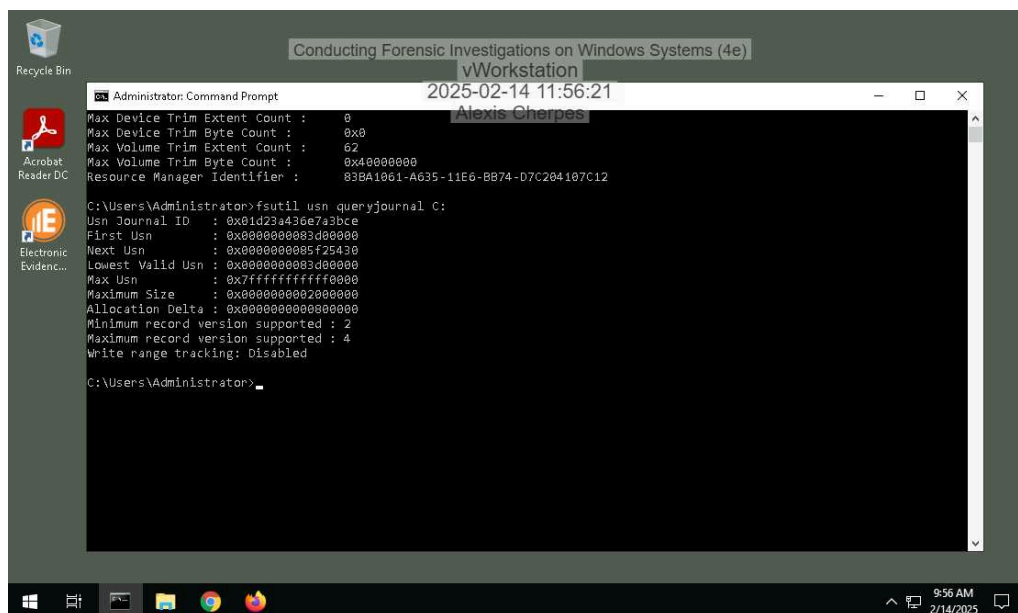
10. Make a screen capture showing the Listening Ports list.



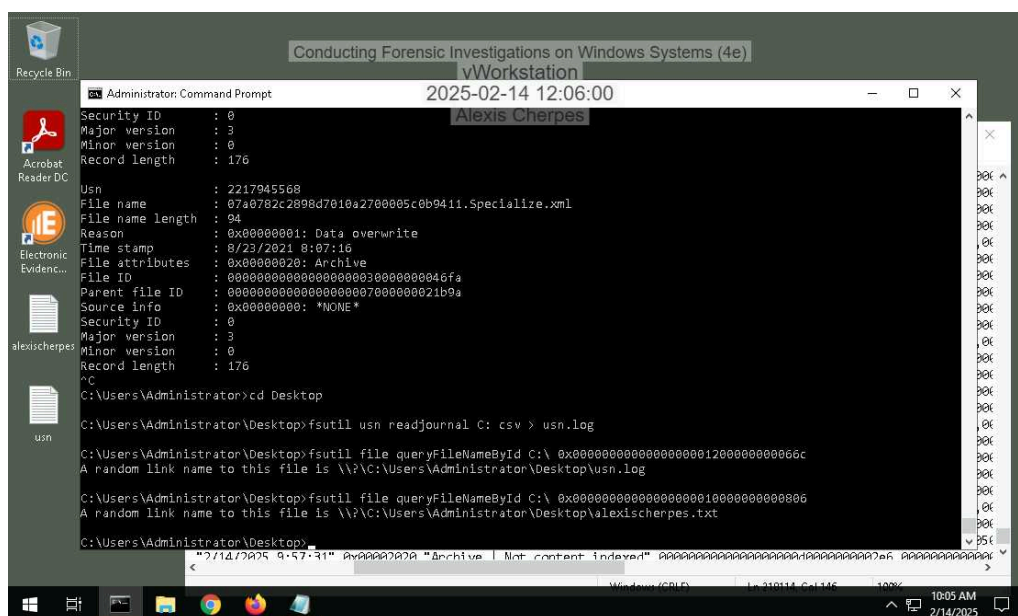
14. Make a screen capture showing the information about the C: drive.



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



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

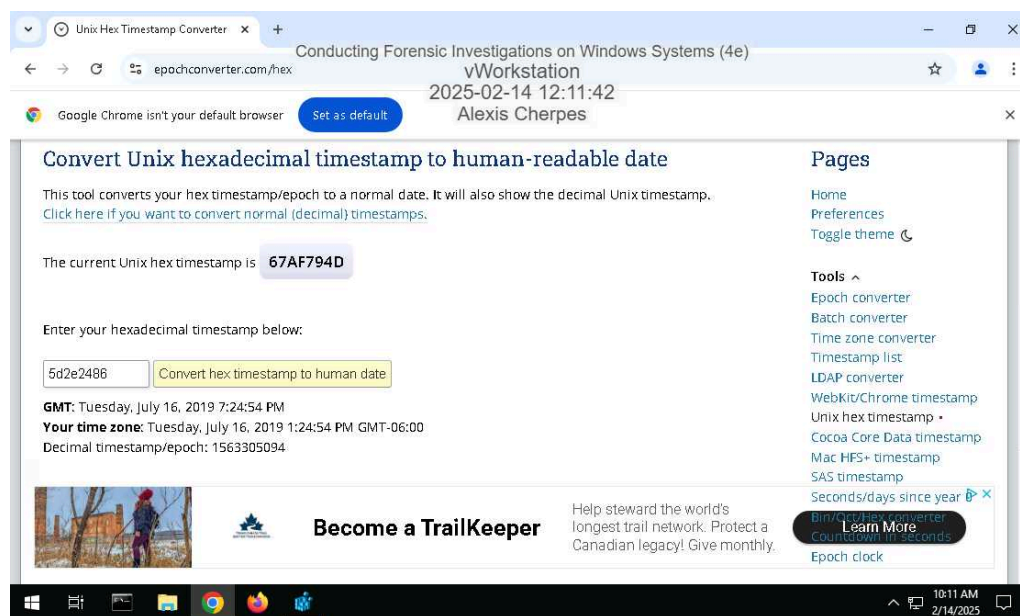


Part 2: Explore the Registry

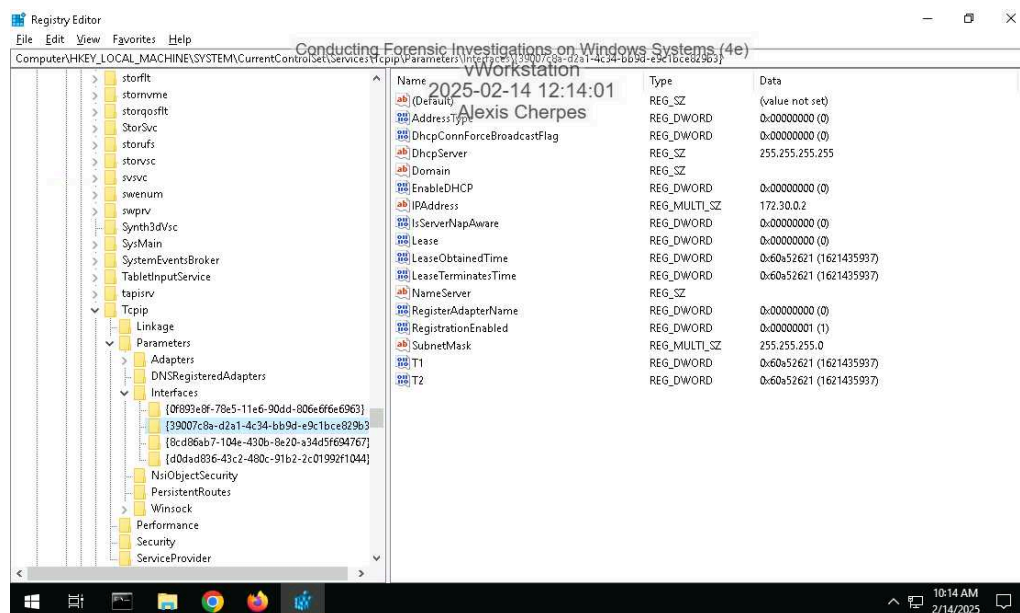
Conducting Forensic Investigations on Windows Systems (4e)

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

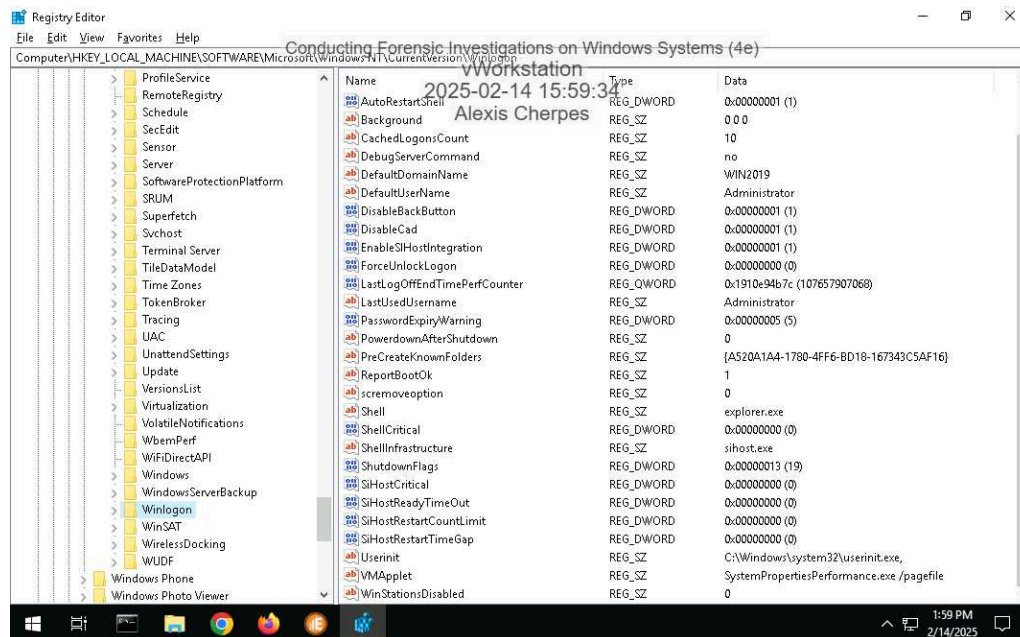
10. Make a screen capture showing the vWorkstation Windows installation timestamp in a human-friendly format.



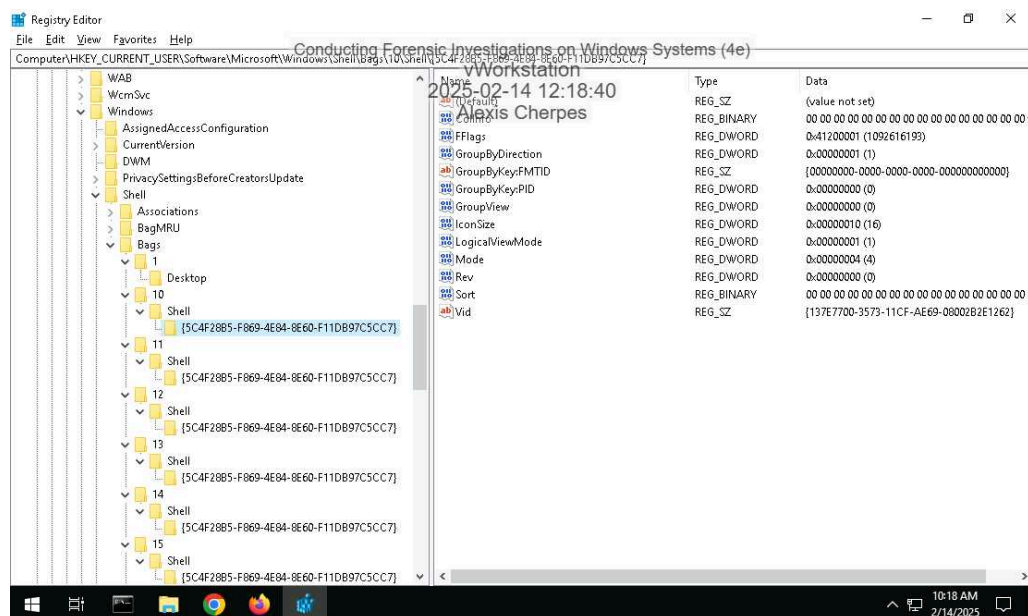
13. Make a screen capture showing the key values for the vWorkstation's default network interface.



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



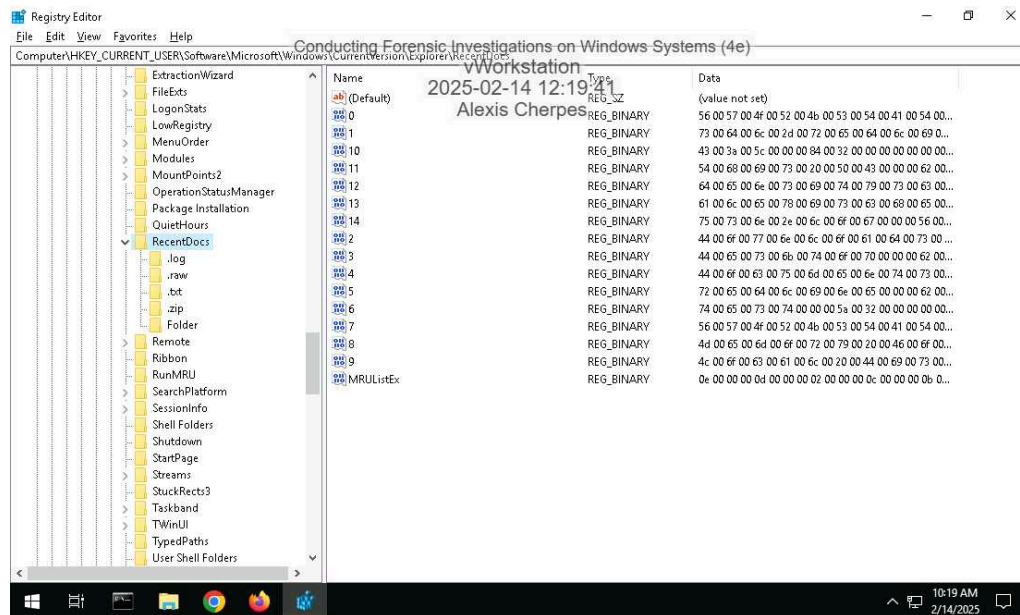
18. Make a screen capture showing the ShellBags key values.



Conducting Forensic Investigations on Windows Systems (4e)

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

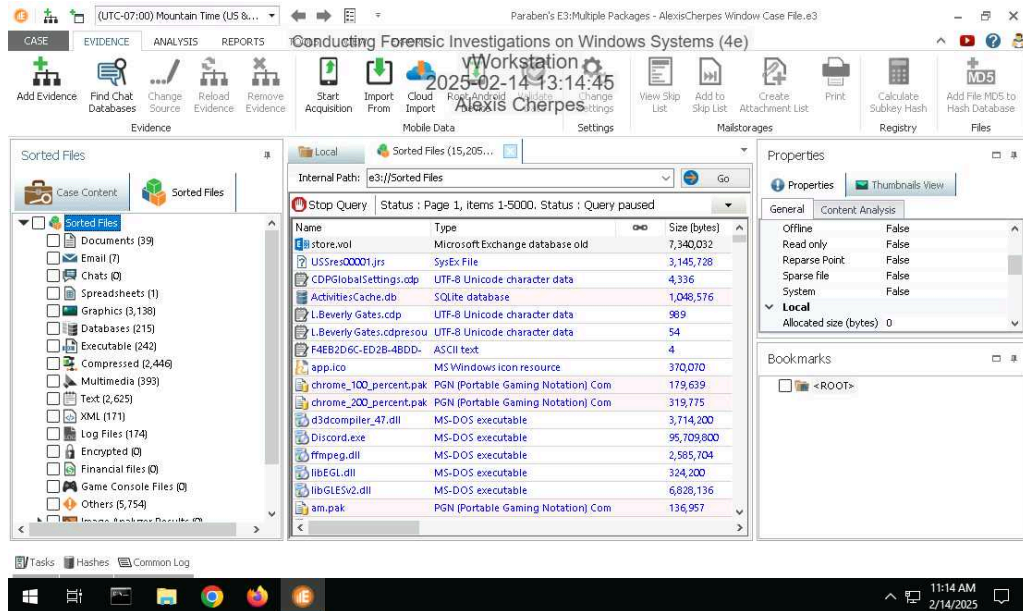
20. Make a screen capture showing the RecentDocs key values.



Section 2: Applied Learning

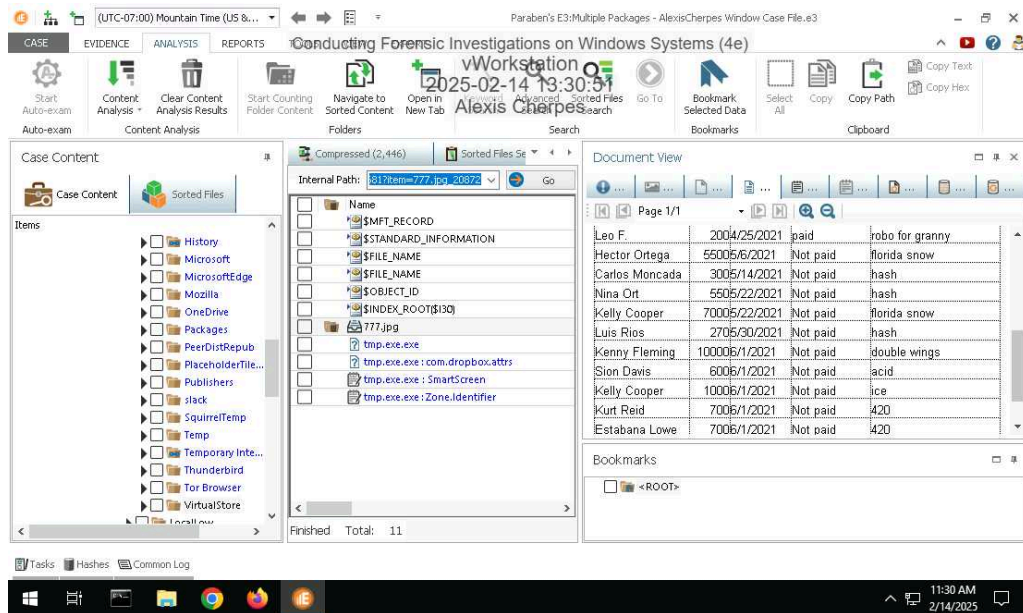
Part 1: Create and Sort a New Case File

14. Make a screen capture showing the Sorted Files.



Part 2: Perform Forensic Analysis on a Windows Drive Image

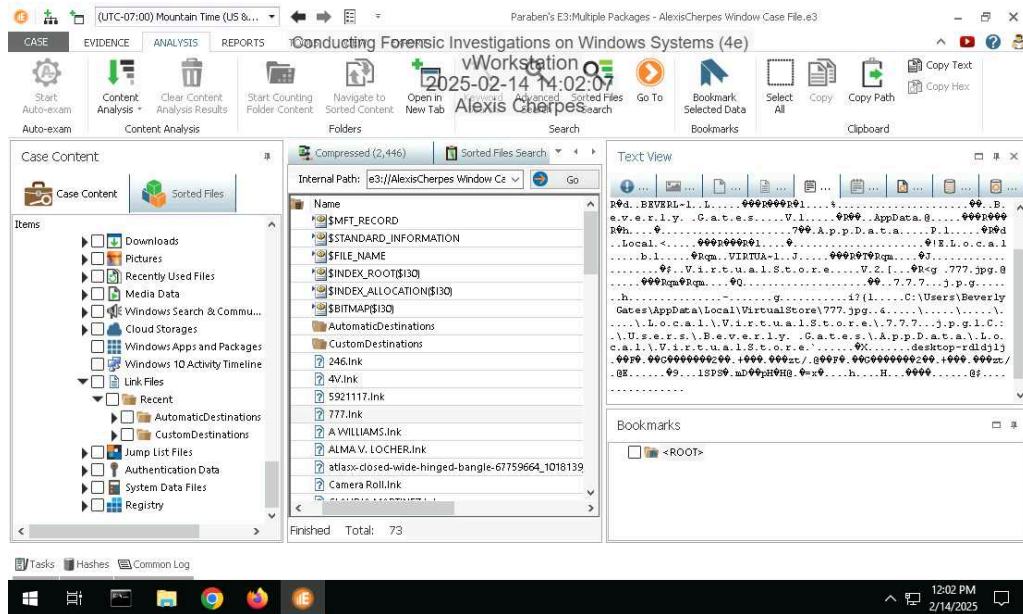
6. Make a screen capture showing the contents of the 777.jpg file in the Document View.



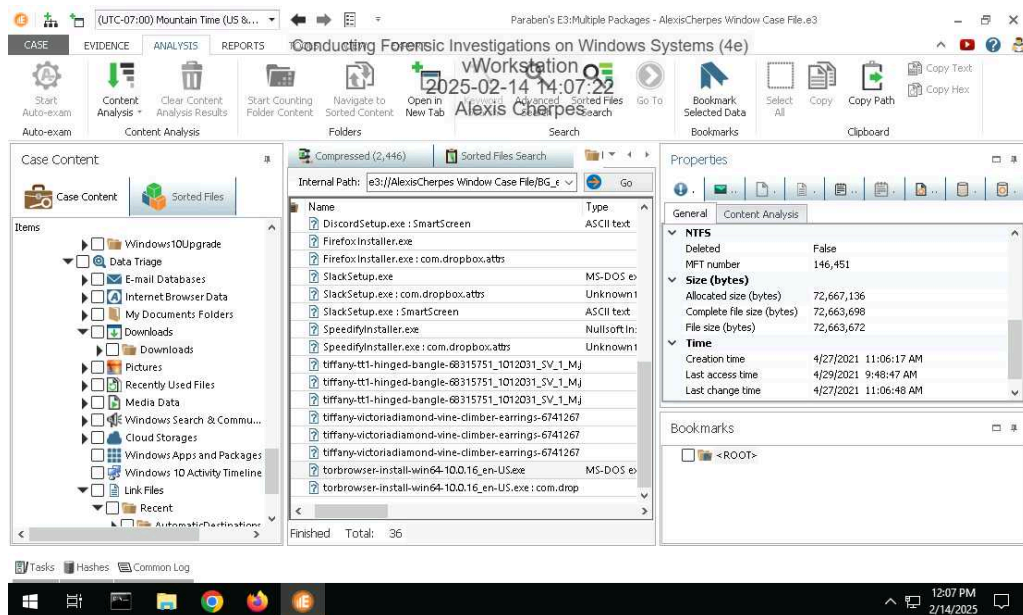
Conducting Forensic Investigations on Windows Systems (4e)

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.



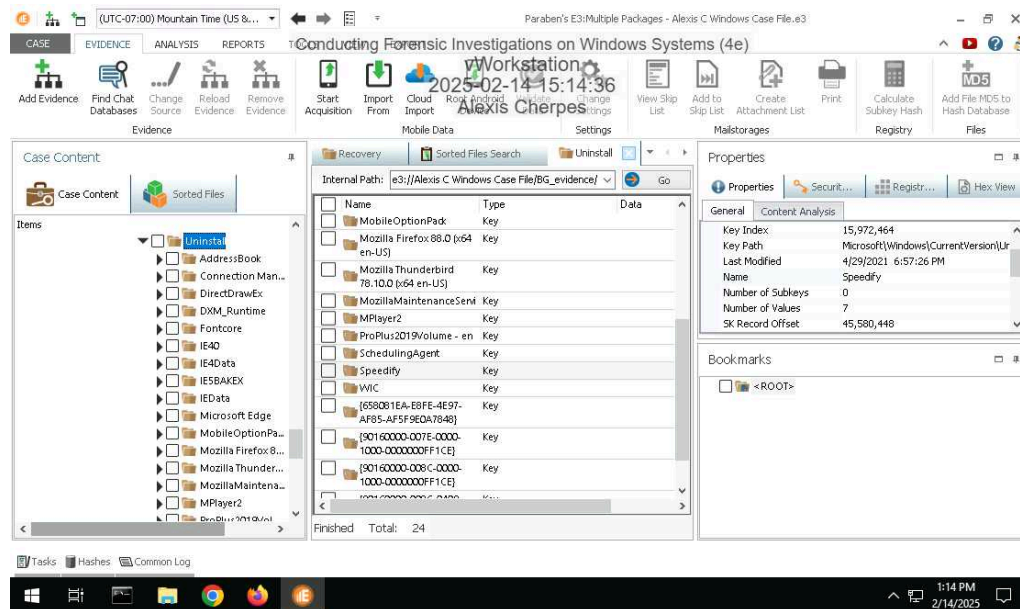
14. Make a screen capture showing the installation files for suspicious apps in the Downloads category.



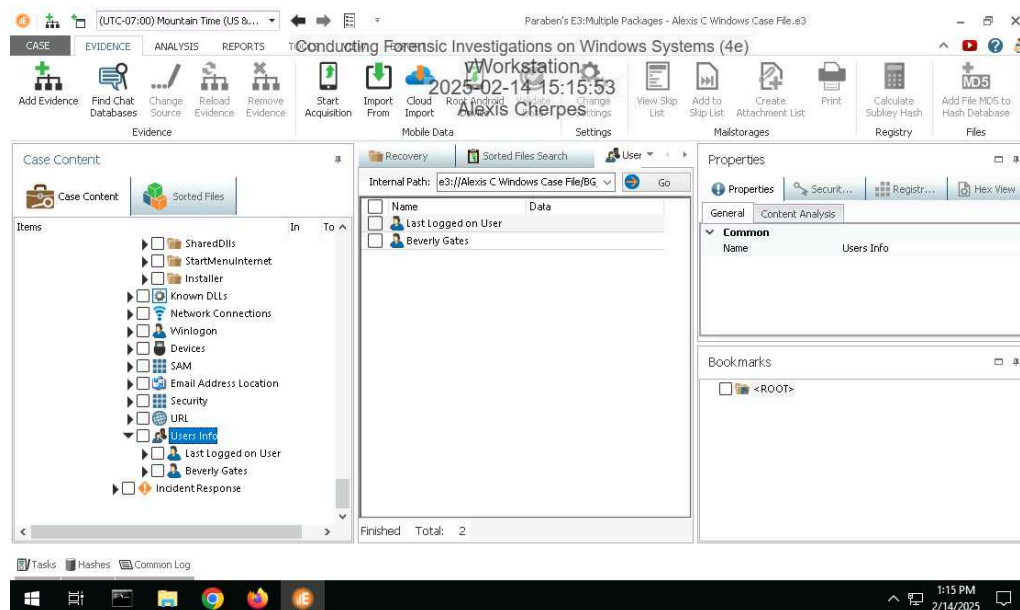
Conducting Forensic Investigations on Windows Systems (4e)

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

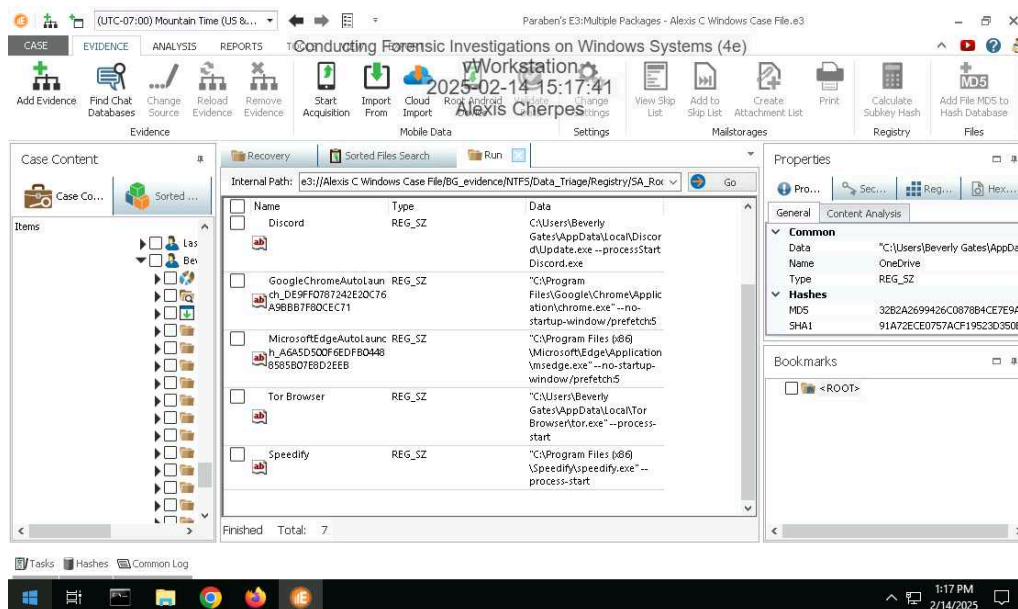
17. Make a screen capture showing the VPN application (Speedify) in the Uninstall folder.



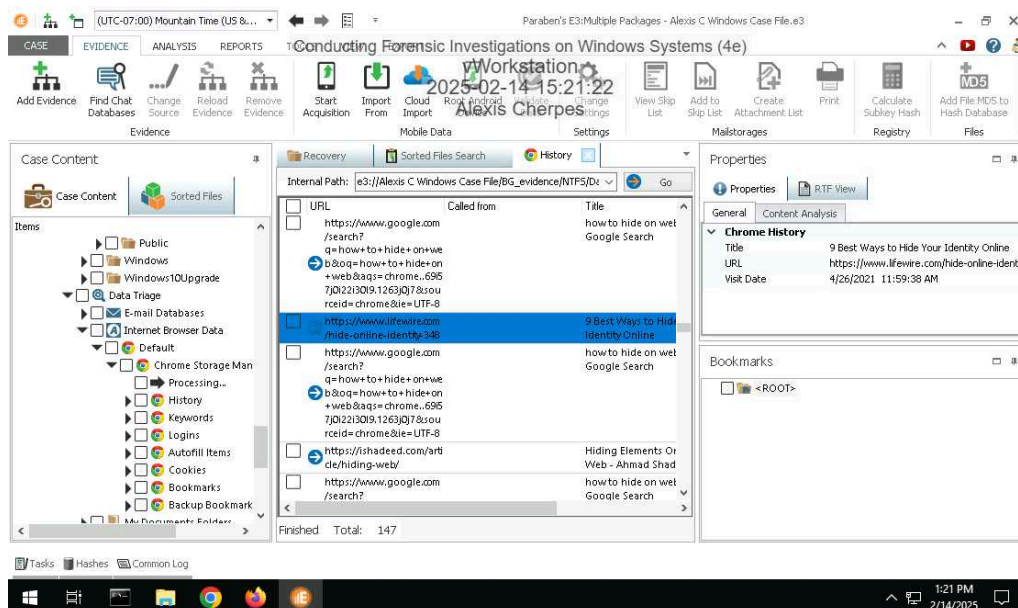
19. Make a screen capture showing the users list.



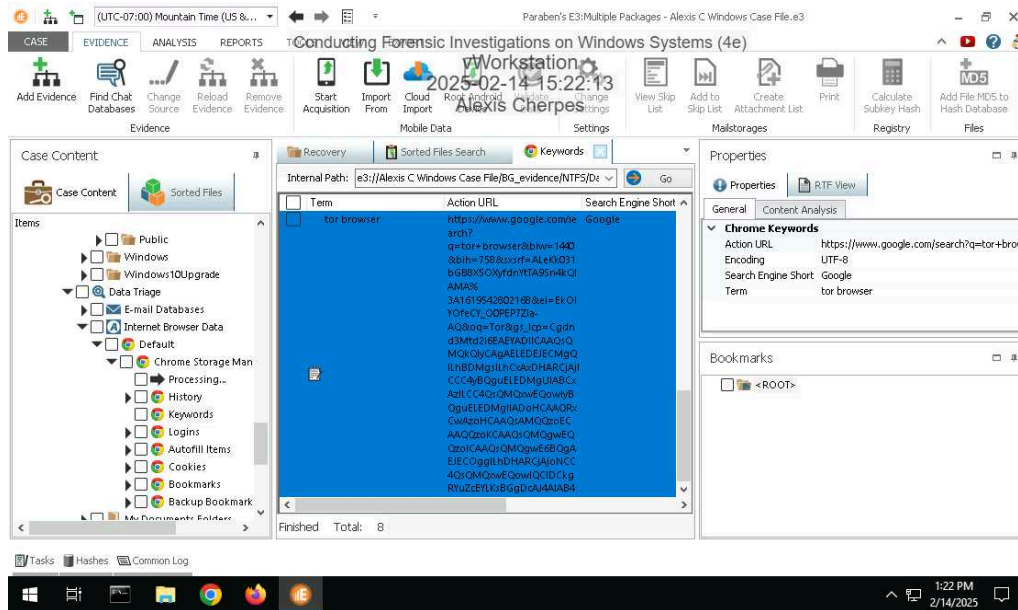
21. Make a screen capture showing the contents of the Beverly Gates / Run folder.



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



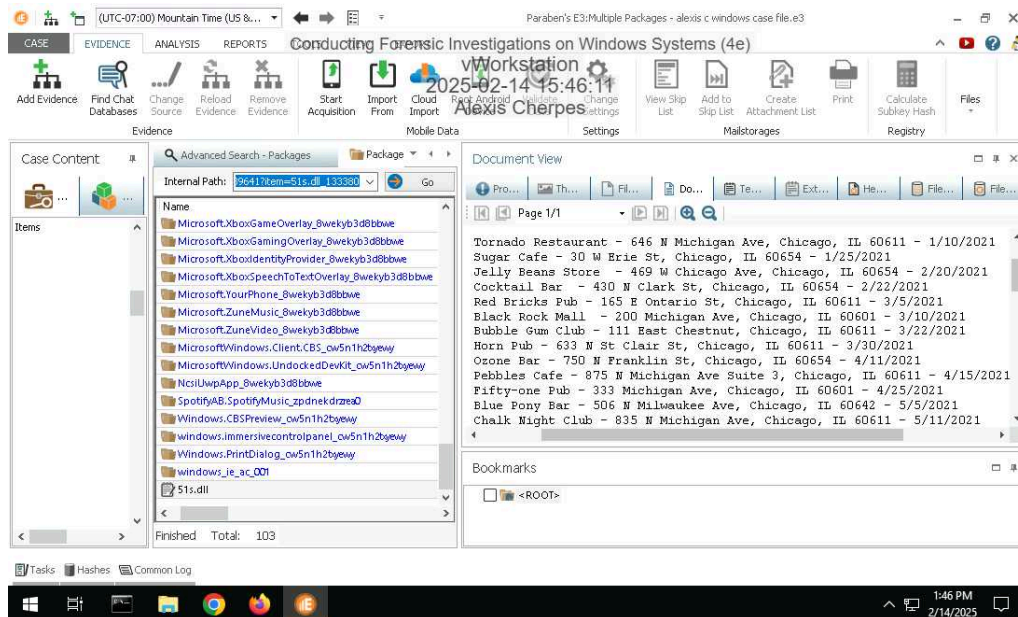
26. Make a screen capture showing at least one suspicious search found in the Keywords sub-node.



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

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

The screenshot displays the Paraben's E3 Multiple Packages interface for a forensic investigation on a Windows system. The main window shows a list of registry values under the path 'HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run'. The selected entry is 'C:\Users\Beverly\Gates\AppData\Local\Tor Browser\Browser\Firefox.exe'. The right sidebar shows the 'Properties' tab for the selected entry, displaying the 'Data' field as '53 41 43 50 01 00 00 00 00 00 00 07 00 00 00 28 00 00 00 FA 17 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 04 00 01 00 00 00 50 B6 64 ED DD AC D5 01 00 00 00 00 00 00 00'. The bottom status bar shows 'Finished Total: 31'.