

Conducting Forensic Investigations on Windows Systems (4e)

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

Student:

Jose Cruz

Email:

jose.cruz2@udc.edu

Time on Task:

10 hours, 6 minutes

Progress:

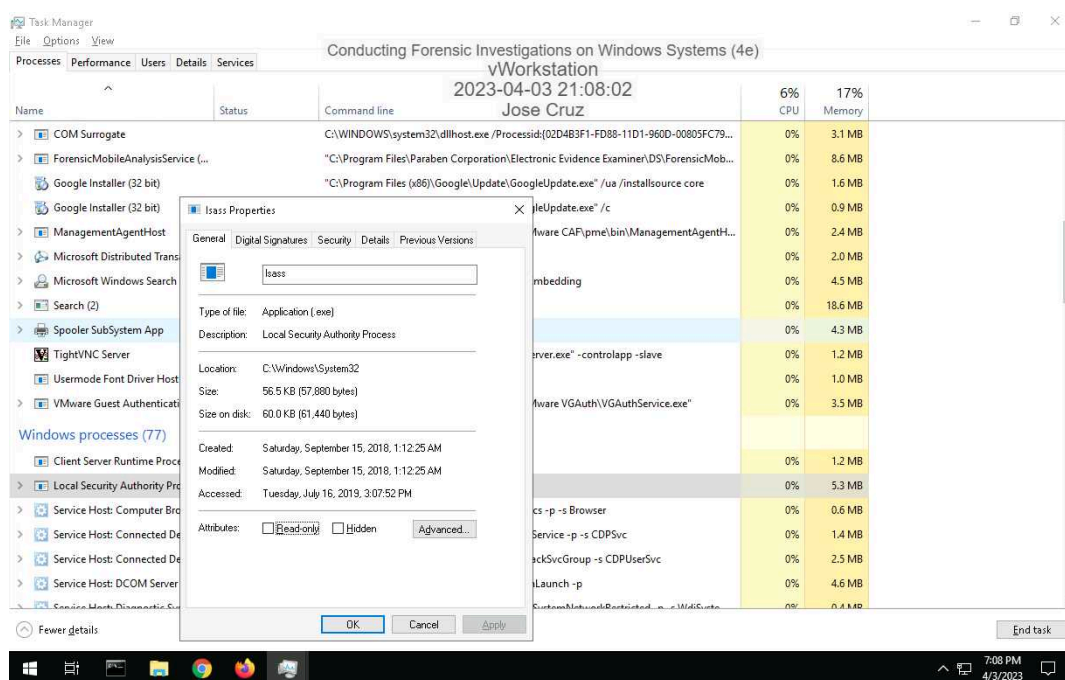
100%

Report Generated: Wednesday, April 5, 2023 at 9:52 PM

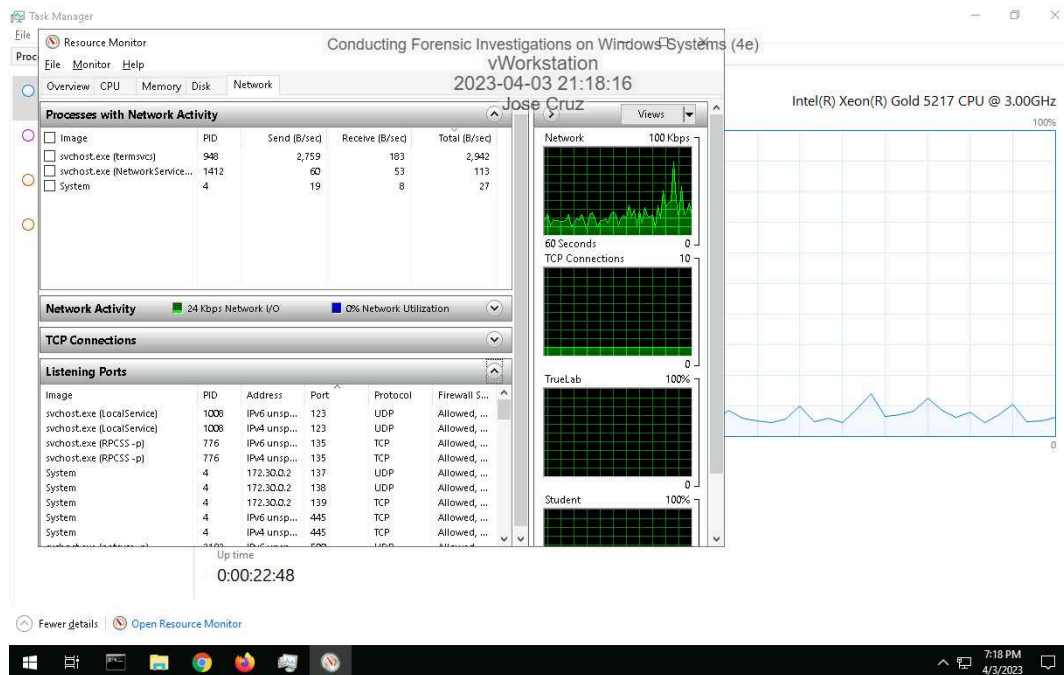
Section 1: Hands-On Demonstration

Part 1: Gather Basic System Information

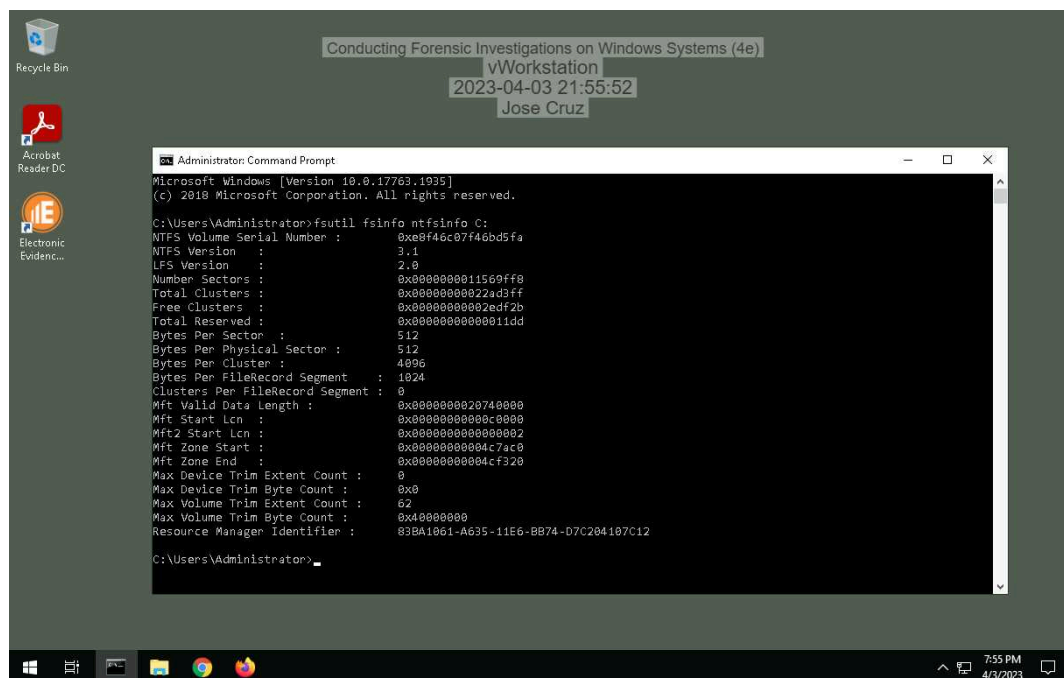
4. Make a screen capture showing the **Properties** window for the process you selected.



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

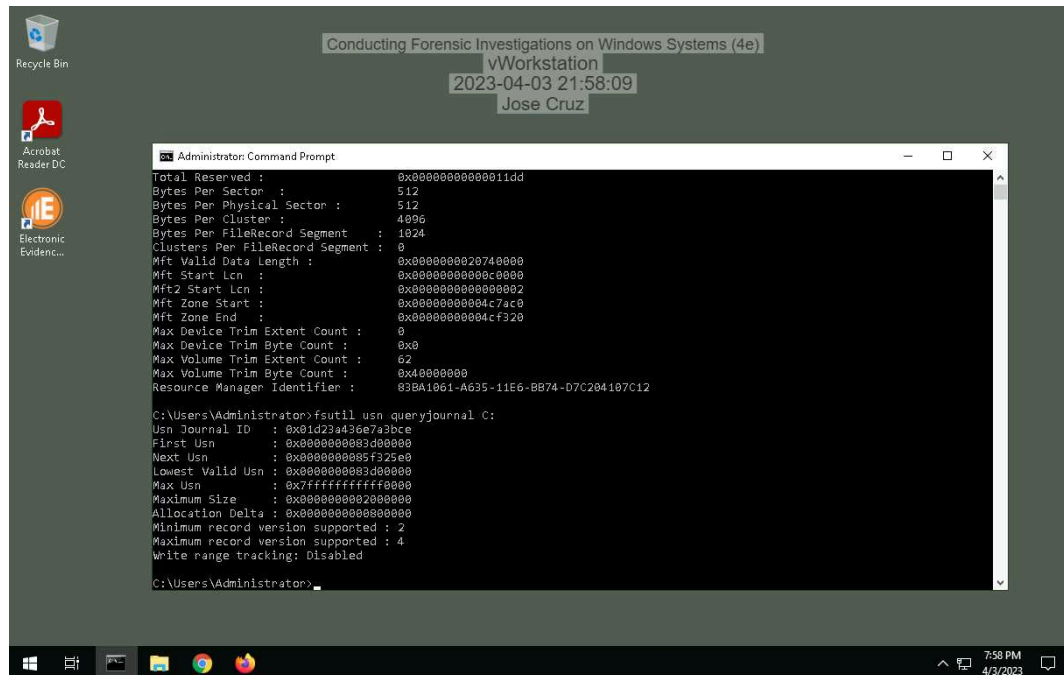


14. Make a screen capture showing the information about the C: drive.

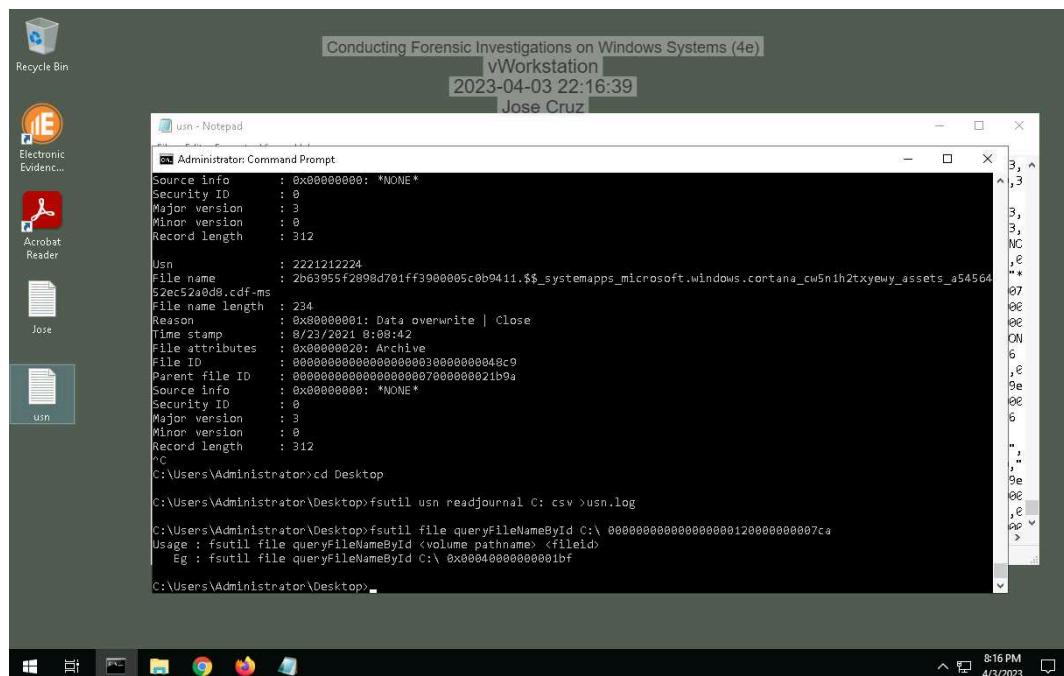


Digital Forensics, Investigation, and Response, Fourth Edition - Lab 05

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

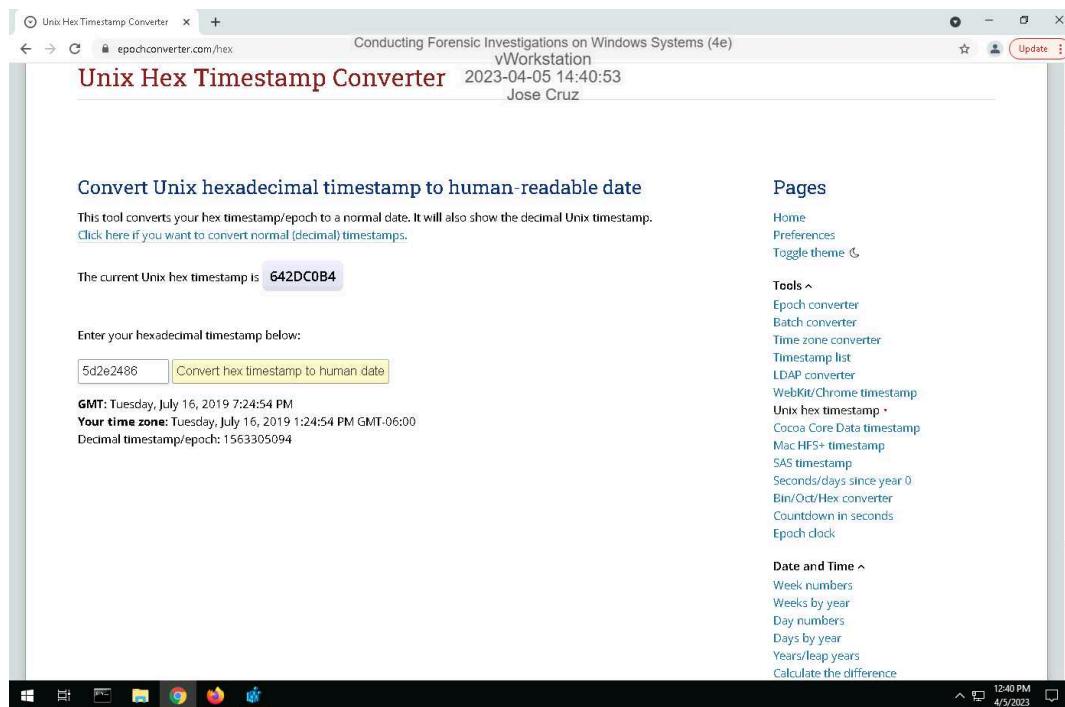


26. **Make a screen capture** showing the file path for the *yourname.txt* file.

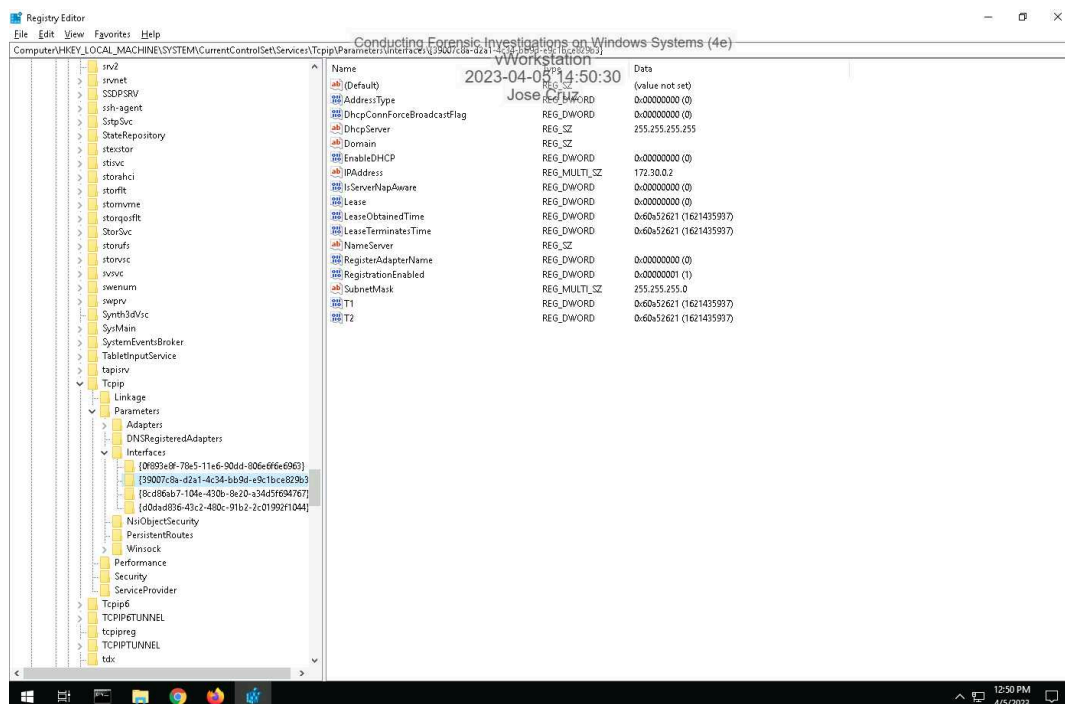


Part 2: Explore the Registry

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



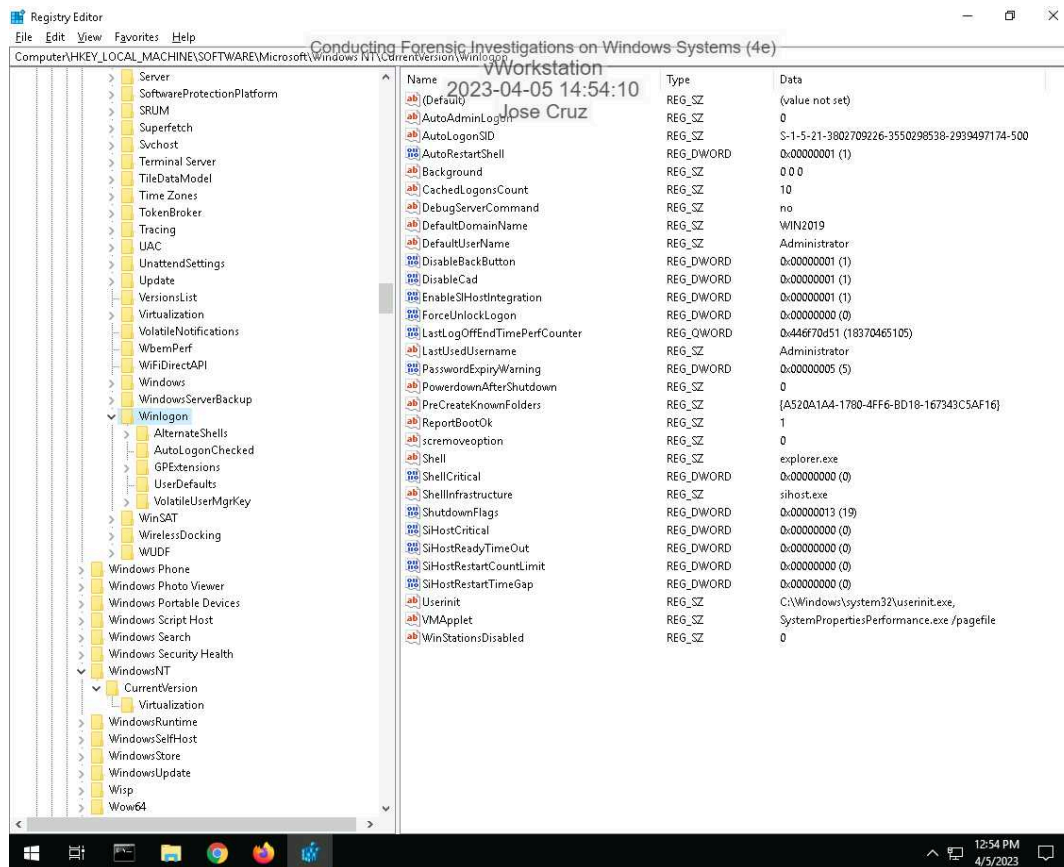
13. Make a screen capture showing the key values for the vWorkstation's default network interface.



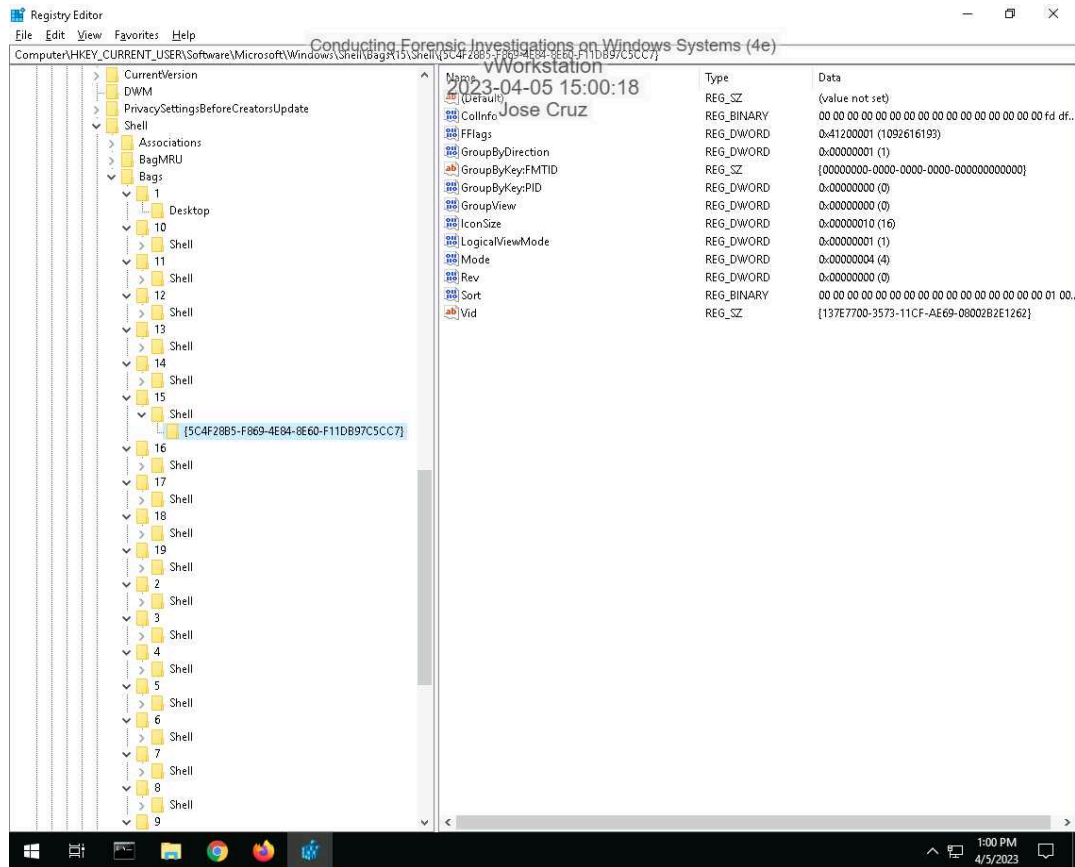
Conducting Forensic Investigations on Windows Systems (4e)

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

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



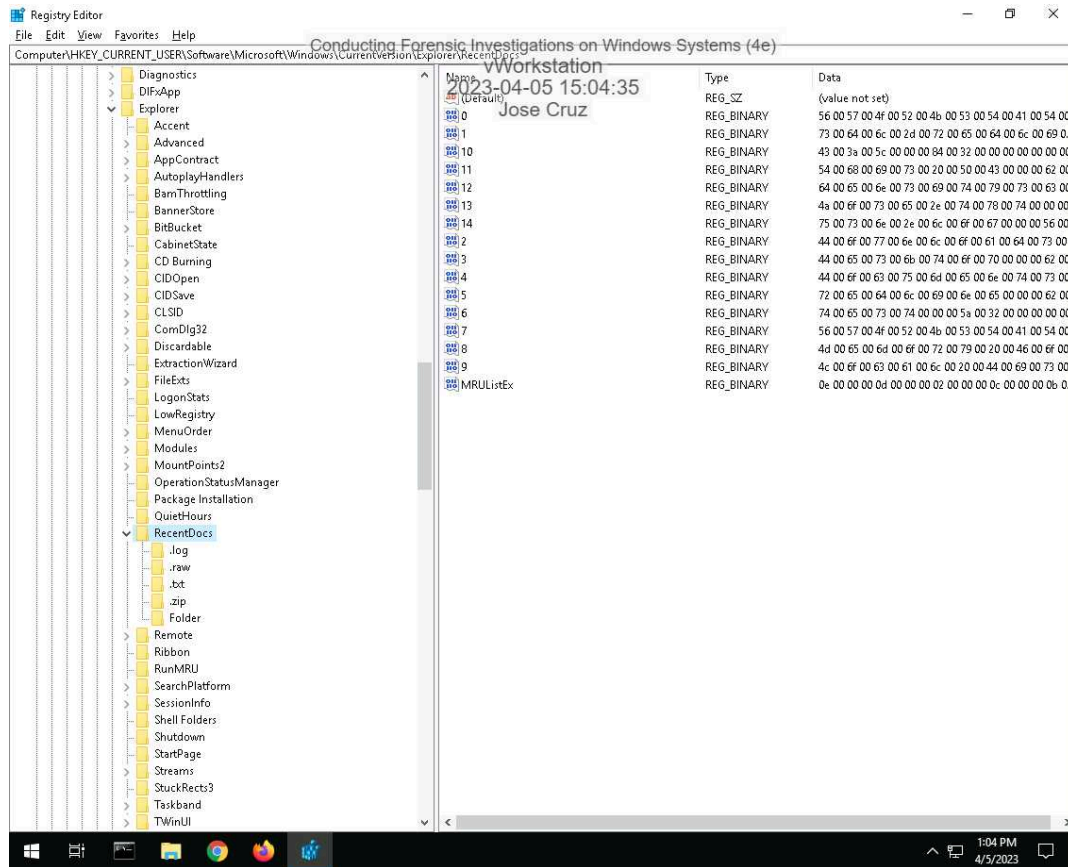
18. Make a screen capture showing the **ShellBags** key values.



Conducting Forensic Investigations on Windows Systems (4e)

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

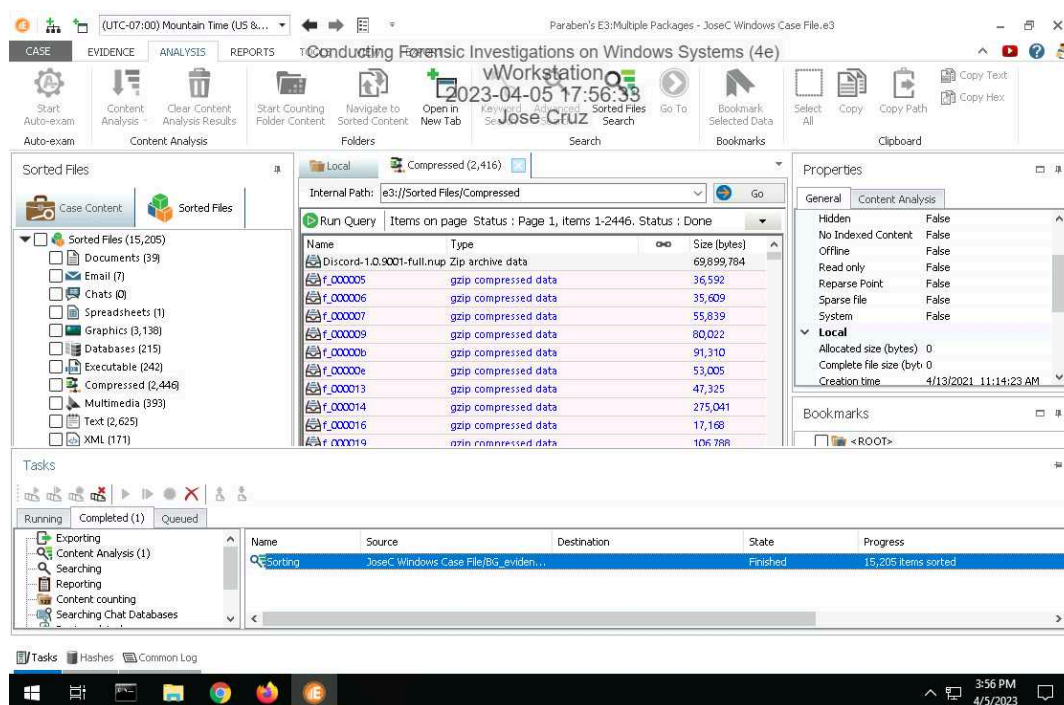
20. Make a screen capture showing the RecentDocs key values.



Section 2: Applied Learning

Part 1: Create and Sort a New Case File

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

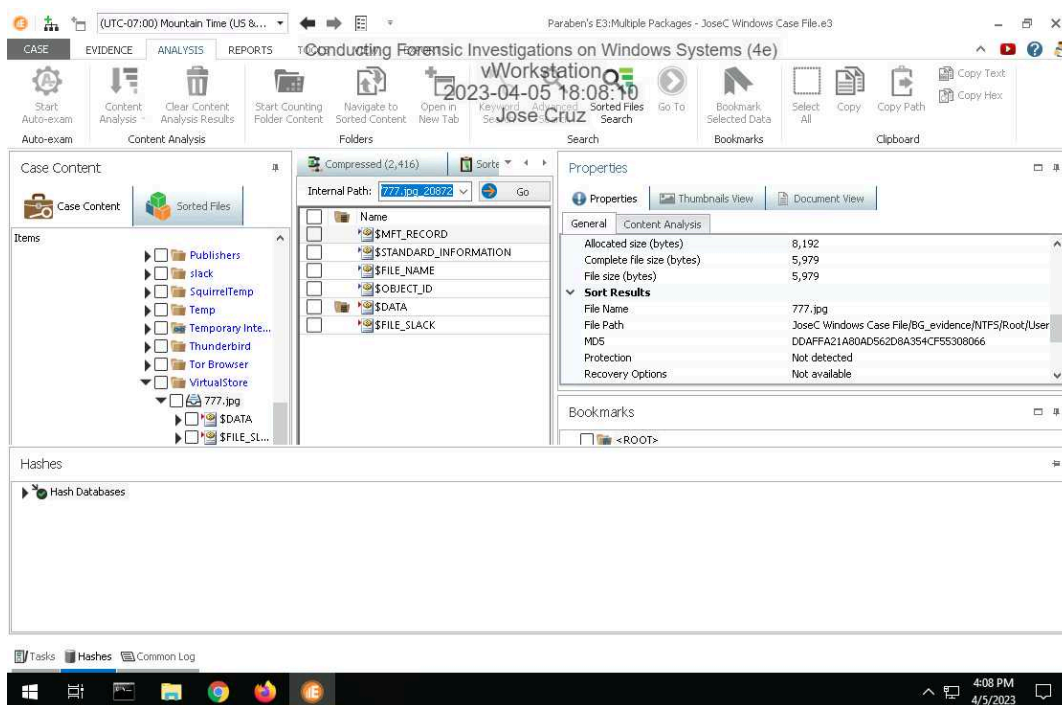


Part 2: Perform Forensic Analysis on a Windows Drive Image

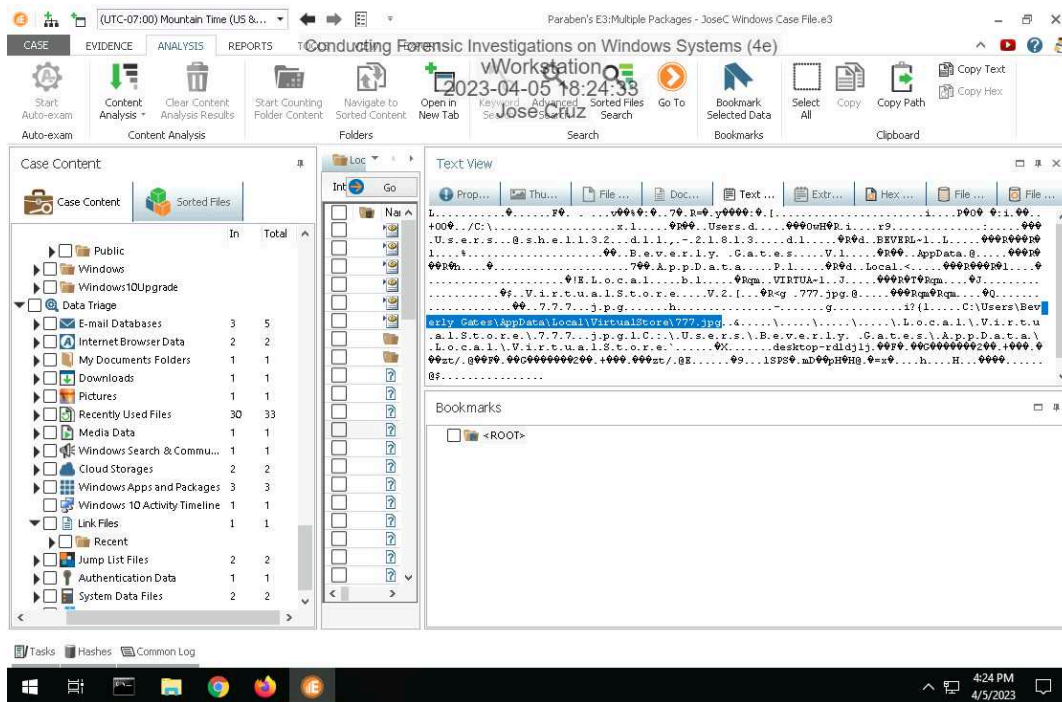
Conducting Forensic Investigations on Windows Systems (4e)

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

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



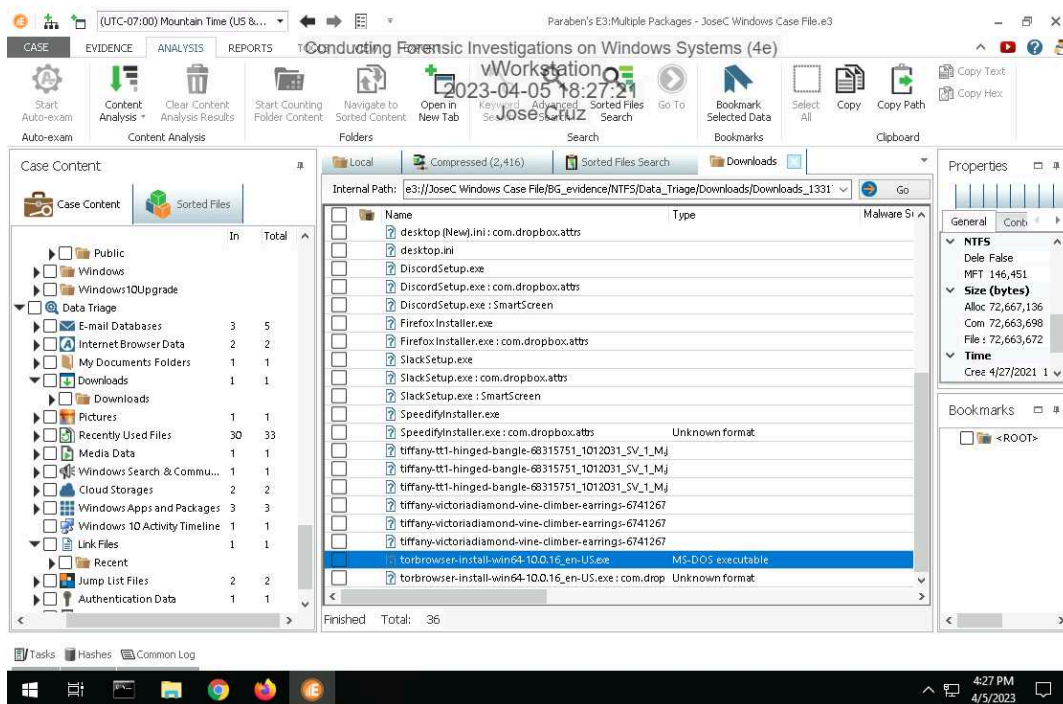
10. Make a screen capture showing the 777.lnk file contents including the path to the file in the system.



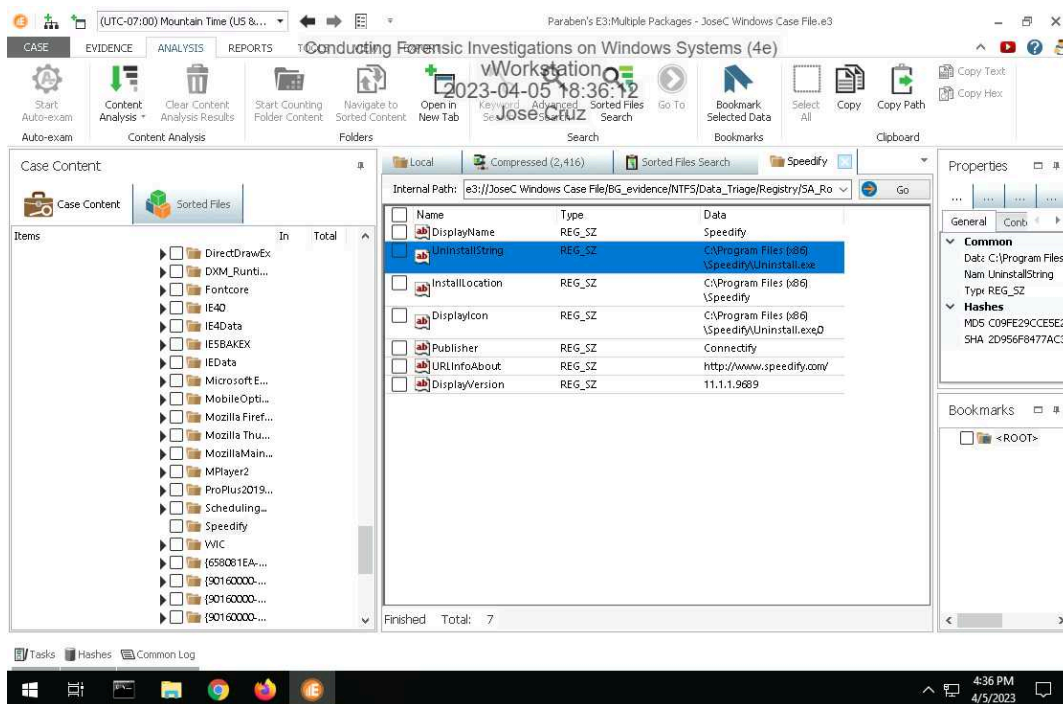
Conducting Forensic Investigations on Windows Systems (4e)

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

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



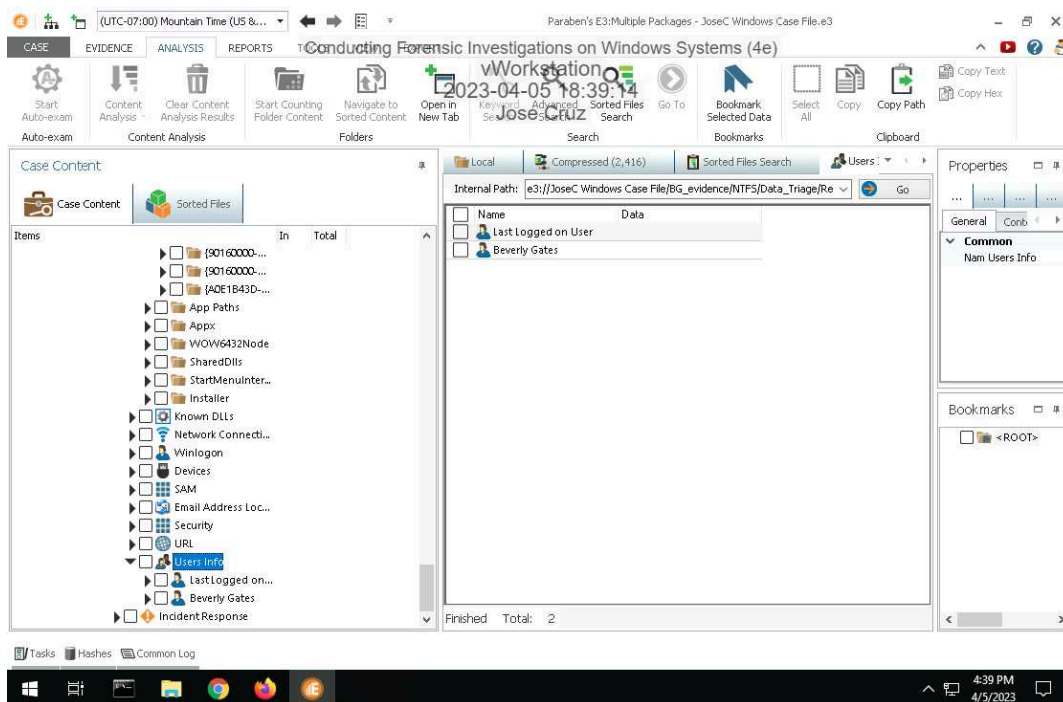
17. Make a screen capture showing the VPN application (Speedify) in the Uninstall folder.



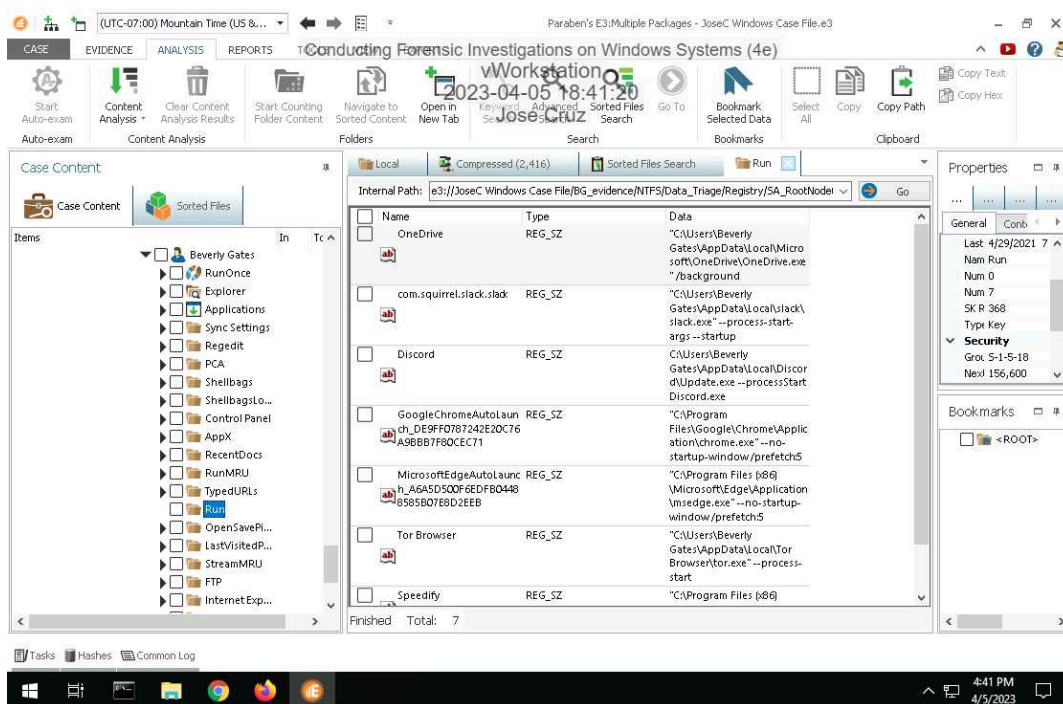
Conducting Forensic Investigations on Windows Systems (4e)

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

19. Make a screen capture showing the users list.



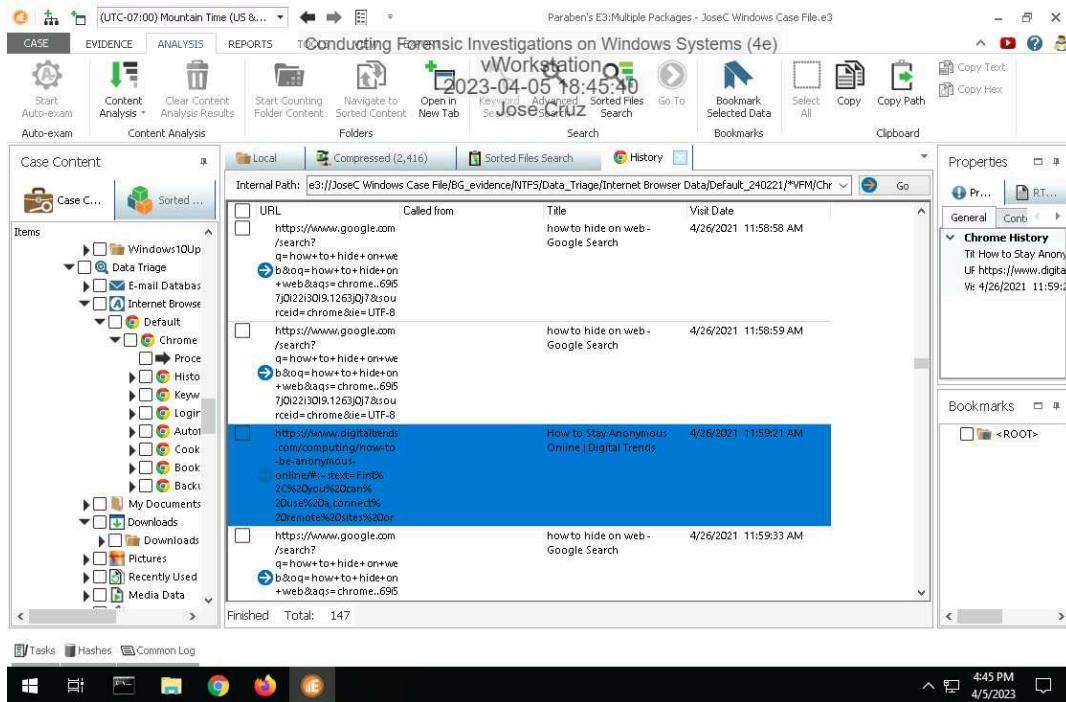
21. Make a screen capture showing the contents of the Beverly Gates / Run folder.



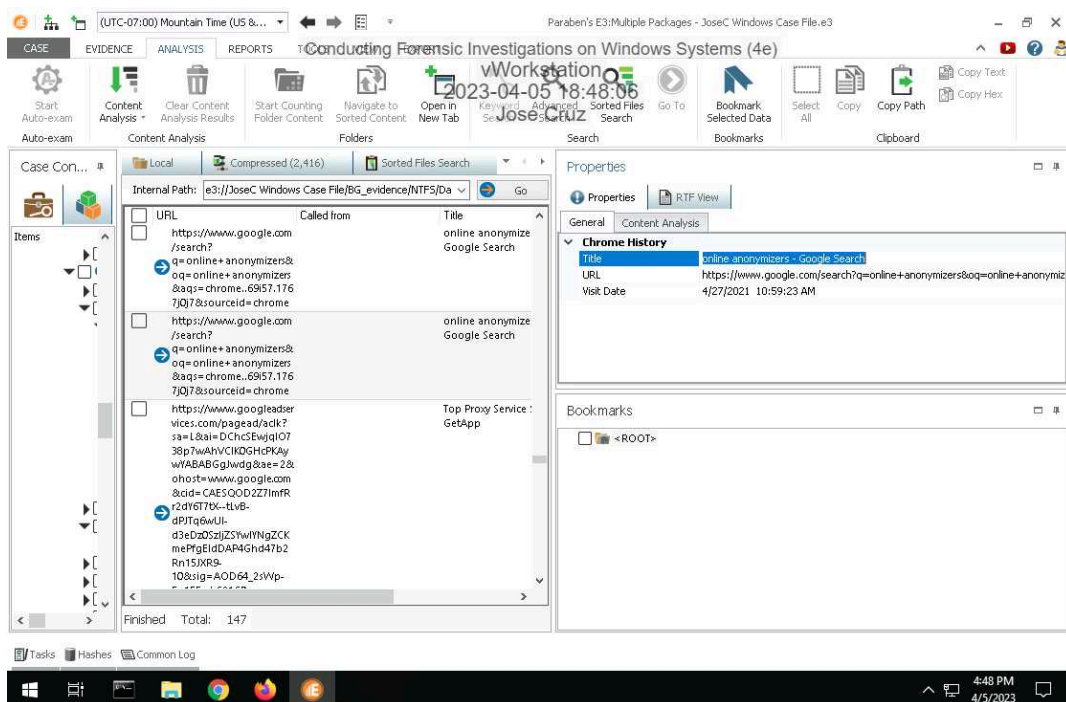
Conducting Forensic Investigations on Windows Systems (4e)

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.



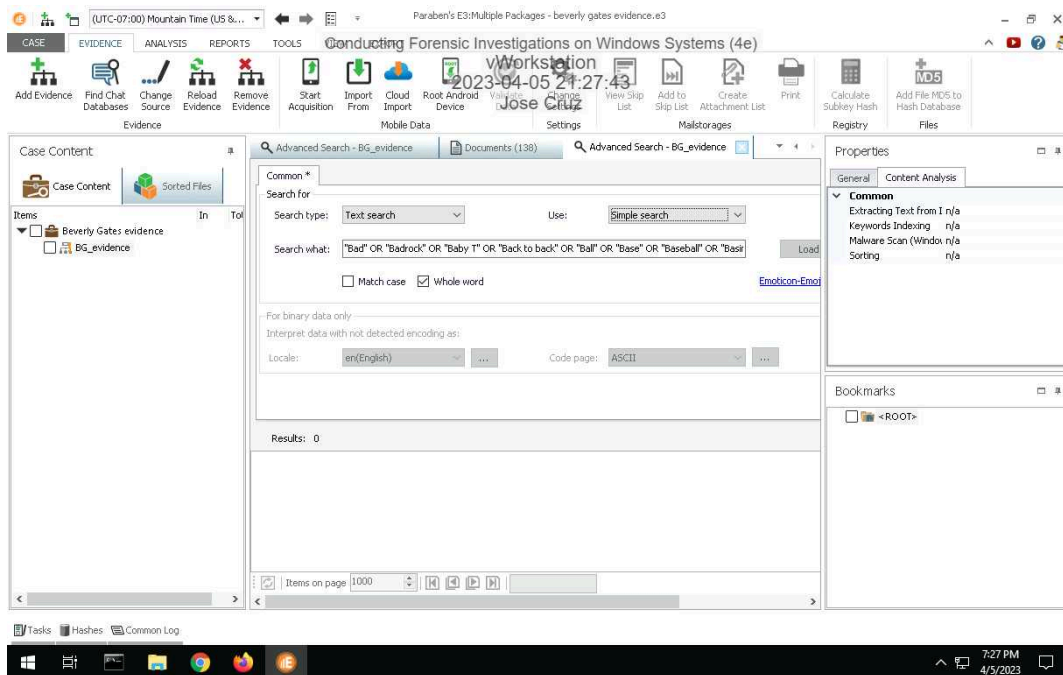
26. Make a screen capture showing at least one suspicious search found in the Keywords sub-node.



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

Paraben's E3 Multiple Packages Case File v3.03

Workstation
2023-04-05 21:43:21
Jose Cruz

Case Co...
Internal Path: e3://Josec Windows Case File/BG_evidence/NTFS/Data_Triage/Registry/SA_RootNode0/ParsedRegistryD...

Registry Value
C:\Users\Beverly Gates\AppData\Local\Tor Browser\Browser\firefox.exe
53 41 43 50 01 00 00 00 00 00 00 00 00 07 00 00 00 28 00 00 00 FA 17 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 0A 00 00 00 50 BB 64 ED 00 AC D5 01 00 00 00 00 00 00 00

Tasks
Running Completed (2) Queued
Exporting
Content Analysis
Searching
Reporting
Content counting
Searching Chat Databases

Tasks Hashes Common Log

7:43 PM
4/5/2023