

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:

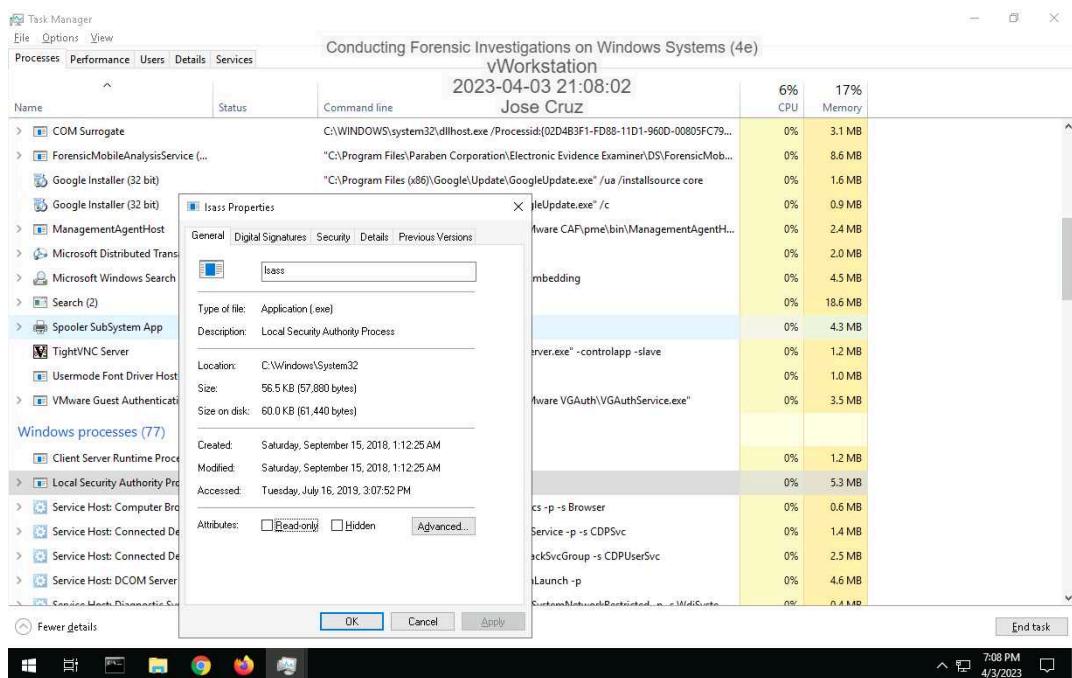
100%

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

Section 1: Hands-On Demonstration

Part 1: Gather Basic System Information

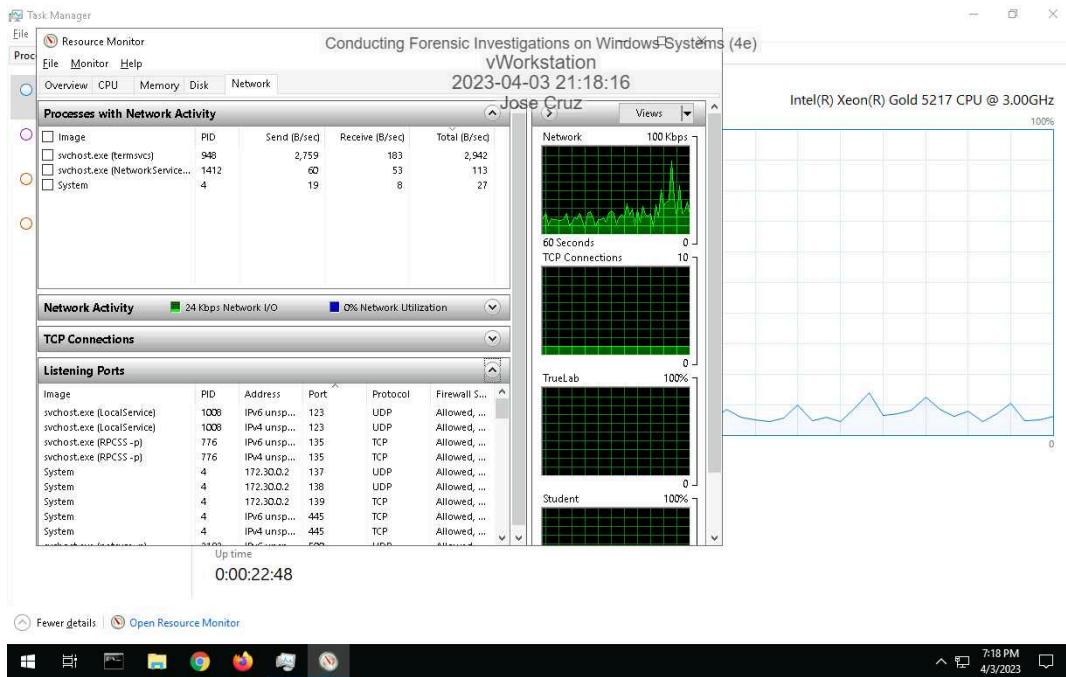
4. Make a screen capture showing the Properties window for the process you selected.



Conducting Forensic Investigations on Windows Systems (4e)

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

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



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

The screenshot shows an "Administrator: Command Prompt" window. The title bar indicates "Conducting Forensic Investigations on Windows Systems (4e)" and "vWorkstation". The date and time are "2023-04-03 21:55:52" and the user is "Jose Cruz". The command entered is "C:\Users\Administrator>fsutil ntfsinfo C:". The output displays various NTFS volume parameters:

```
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

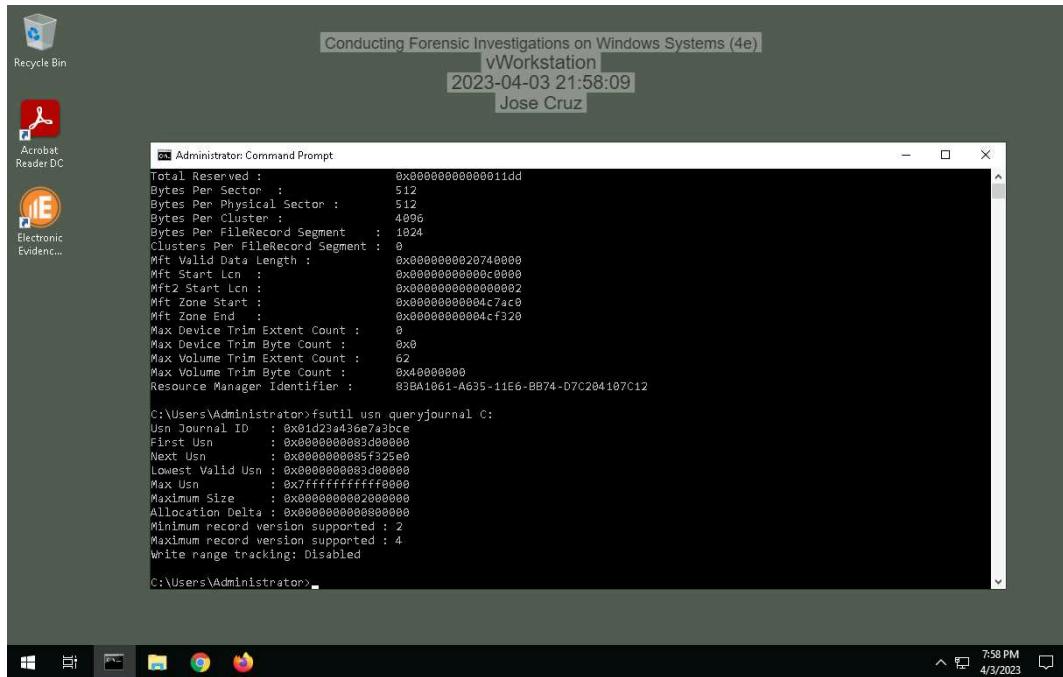
C:\Users\Administrator>fsutil ntfsinfo C:
NTFS Volume Serial Number : 0xe0f46c07f46bd5fa
NTFS Version : 3.1
LFS Version : 2.0
Number Sectors : 0x0000000001569ff8
Total Clusters : 0x00000000022ad3ff
Free Clusters : 0x00000000000zedf2b
Total Reserved : 0x00000000000011dd
Bytes Per Sector : 512
Bytes Per Physical Sector : 512
Bytes Per Cluster : 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 : 0x000000000004c7ac0
Mft Zone End : 0x000000000004cf320
Max Device Trim Extent Count : 0
Max Device Trim Byte Count : 0x0
Max Volume Trim Extent Count : 62
Max Volume Trim Byte Count : 0x40000000
Resource Manager Identifier : 83BA1061-A635-11E6-BB74-07C204107C12
```

The bottom status bar shows "7:55 PM 4/3/2023".

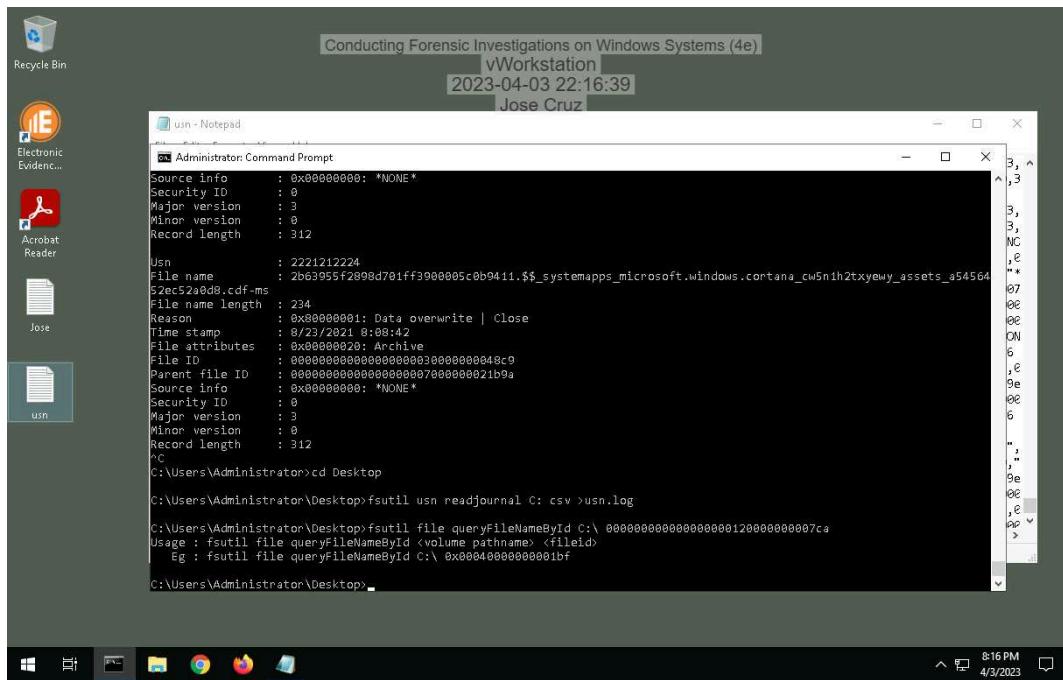
Conducting Forensic Investigations on Windows Systems (4e)

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

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



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

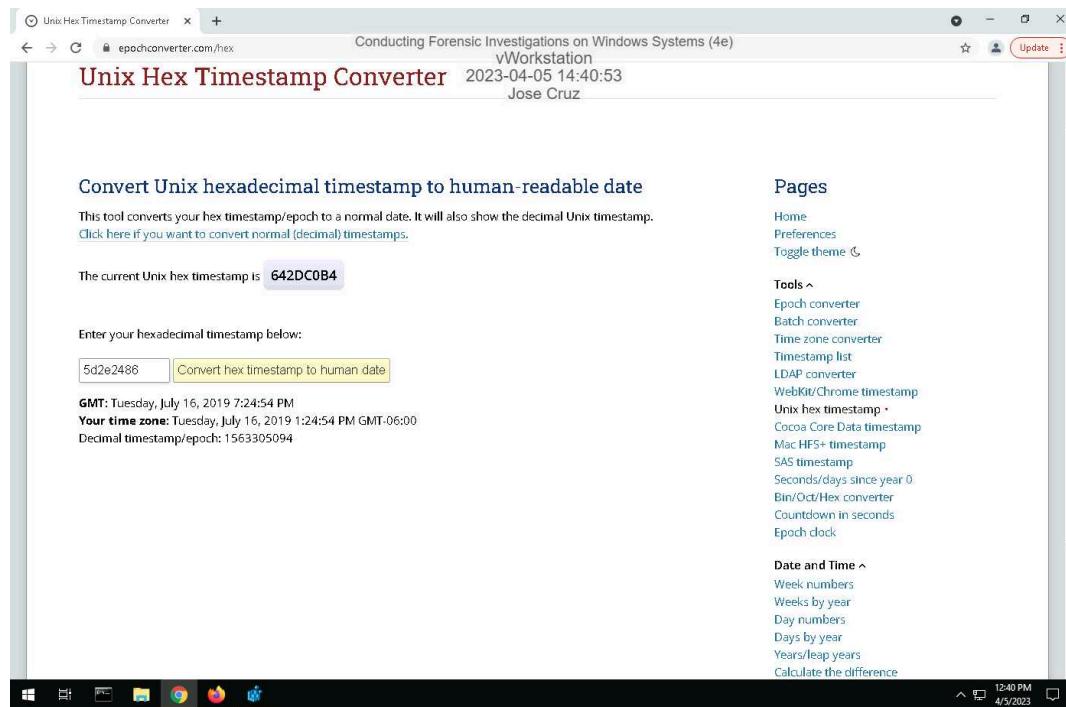


Part 2: Explore the Registry

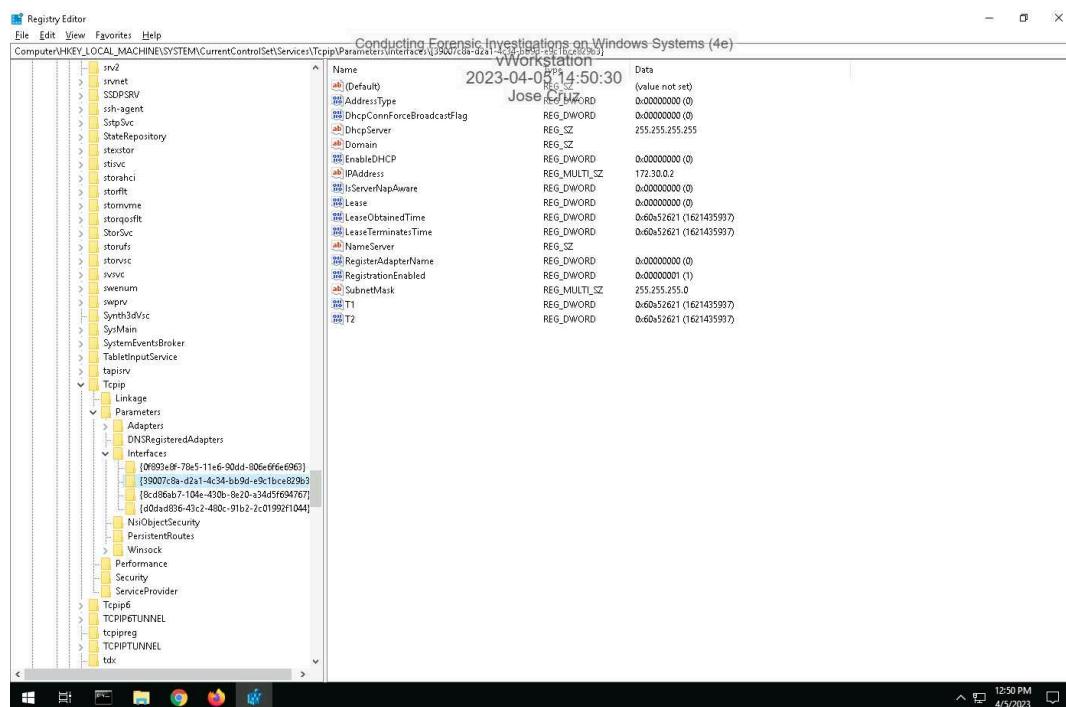
Conducting Forensic Investigations on Windows Systems (4e)

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.



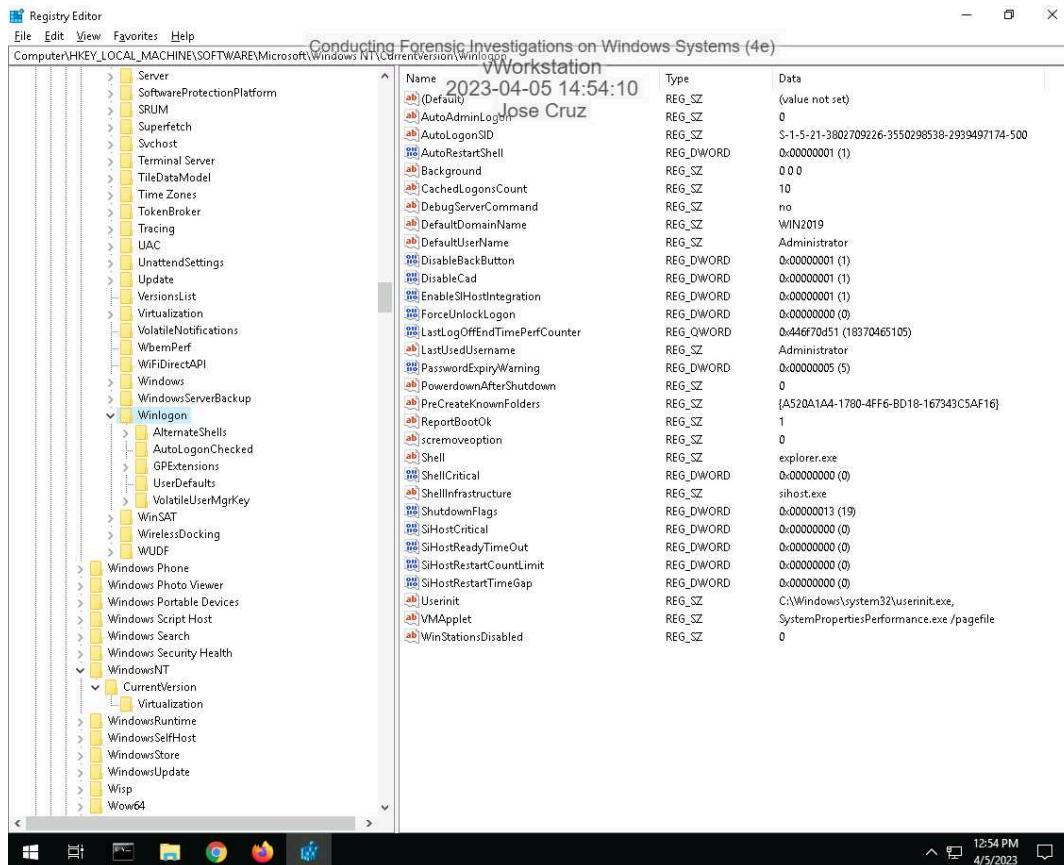
13. Make a screen capture showing the key values for the vWorkstation's default network interface.



Conducting Forensic Investigations on Windows Systems (4e)

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

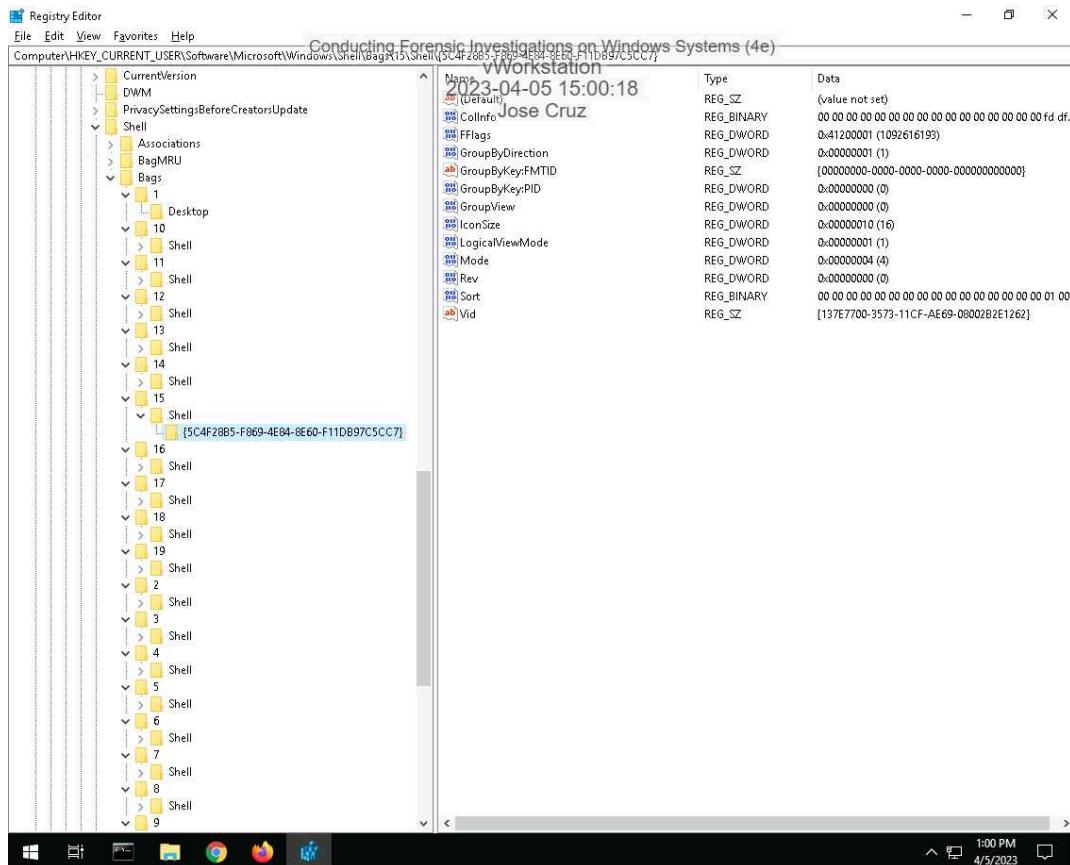
15. Make a screen capture showing the Winlogon key values.



Conducting Forensic Investigations on Windows Systems (4e)

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

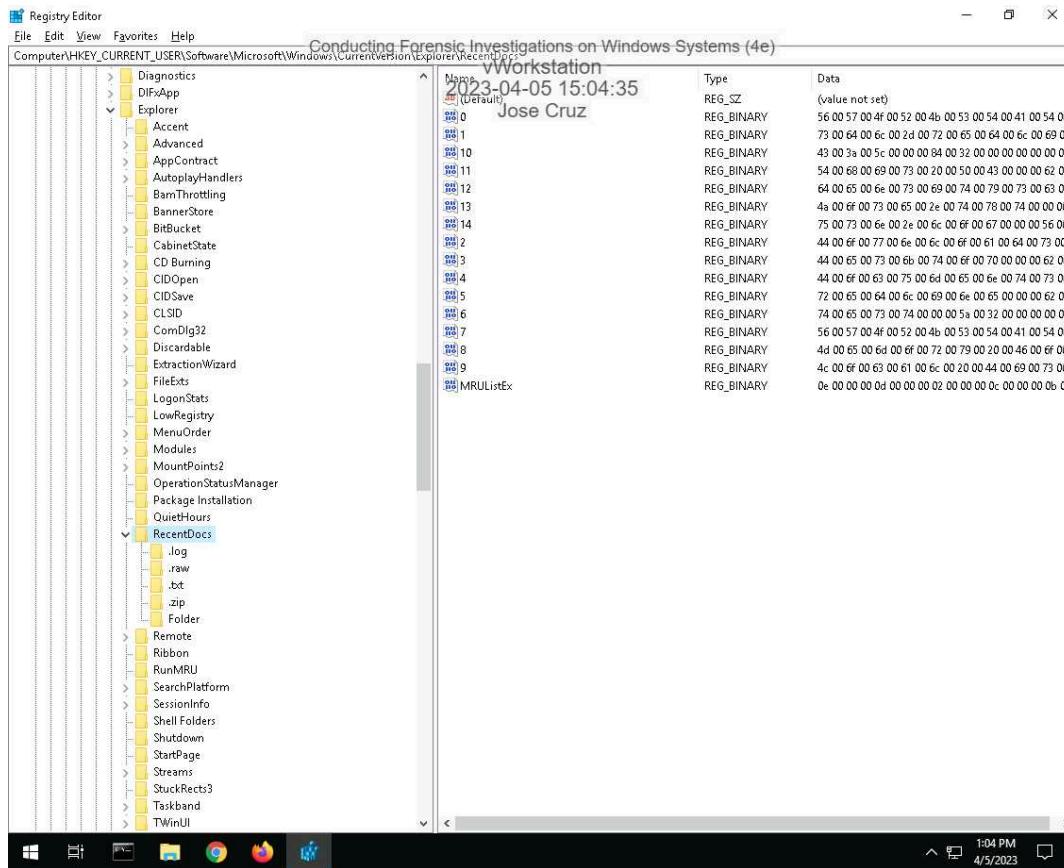
18. Make a screen capture showing the ShellBags key values.



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.



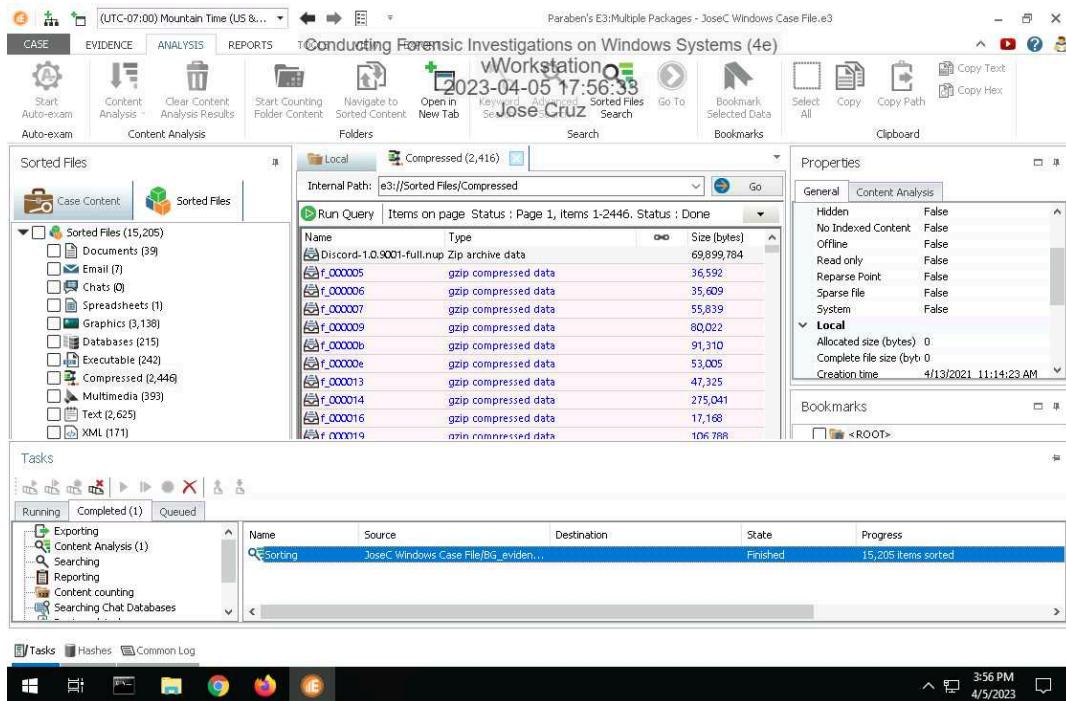
Conducting Forensic Investigations on Windows Systems (4e)

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

Section 2: Applied Learning

Part 1: Create and Sort a New Case File

14. Make a screen capture showing the Sorted Files.

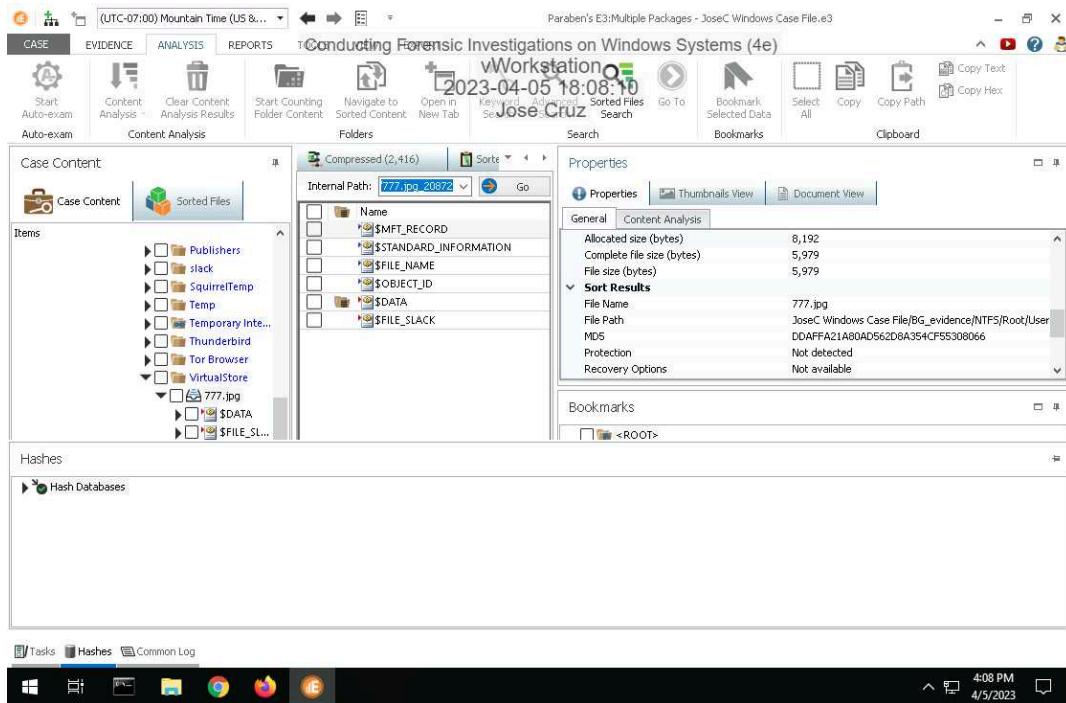


Part 2: Perform Forensic Analysis on a Windows Drive Image

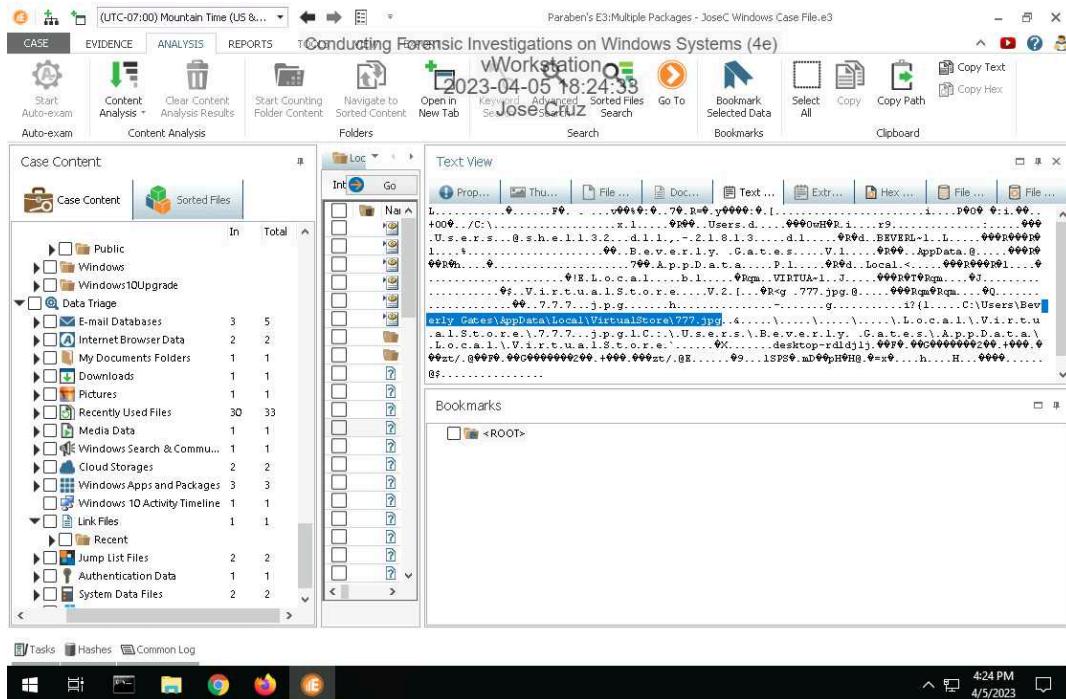
Conducting Forensic Investigations on Windows Systems (4e)

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.

The screenshot shows the EnCase Forensic interface. The main pane displays a list of files under the internal path `e3://JoseC Windows Case File/BG_evidence/NTFS/Data_Triage/Downloads/Downloads_1331`. The list includes various executables and setup files, many of which are from Dropbox. One file, `torbrowser-install-win64-10.0.16_en-US.exe`, is highlighted in blue and identified as an MS-DOS executable. The properties pane on the right shows details for this file, including its type as `MS-DOS executable`.

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

The screenshot shows the EnCase Forensic interface. The main pane displays a list of registry keys under the internal path `e3://JoseC Windows Case File/BG_evidence/NTFS/Data_Triage/Registry/SA_Ro`. One key, `UninstallString`, is highlighted in blue. The properties pane on the right shows details for this key, including its data as `C:\Program Files (\x0040)\Speedify\Uninstall.exe`. The left pane shows a list of installed applications, including Speedify, Mozilla Firefox, and others.

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.

The screenshot shows the EnCase Forensic interface. The top menu bar includes CASE, EVIDENCE, ANALYSIS, REPORTS, and a timestamp of (UTC-07:00) Mountain Time (US &...). The main window displays 'Case Content' with a tree view of items. Under 'Users Info', two users are listed: 'Last Logged on User' and 'Beverly Gates'. The right pane shows a table with columns 'Name' and 'Data', listing the same two users. A properties panel on the right shows 'Common' details for 'Nam Users Info'. The bottom status bar shows the date as 4/5/2023 and the time as 4:39 PM.

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

The screenshot shows the EnCase Forensic interface. The top menu bar includes CASE, EVIDENCE, ANALYSIS, REPORTS, and a timestamp of (UTC-07:00) Mountain Time (US &...). The main window displays 'Case Content' with a tree view of items. Under 'Run', several registry keys are listed: OneDrive, com.squirrel.slack.slack, Discord, GoogleChromeAutolaun, MicrosoftEdgeAutolaunc, and Tor Browser. The right pane shows a table with columns 'Name', 'Type', and 'Data', listing these registry keys. A properties panel on the right shows 'General' details for 'Nam Run' and 'Security' details for 'Grol S-1-5-18' and 'Nexl 156,600'. The bottom status bar shows the date as 4/5/2023 and the time as 4:41 PM.

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.

The screenshot shows the EnCase Forensic interface. The main pane displays a search result for the URL <https://www.digitaltrends.com/computing/how-to-be-anonymous/>. The properties pane on the right shows the title "How to Stay Anonymous" and the visit date "4/26/2021 11:59:21 AM". The status bar at the bottom indicates the time as 4:45 PM and the date as 4/5/2023.

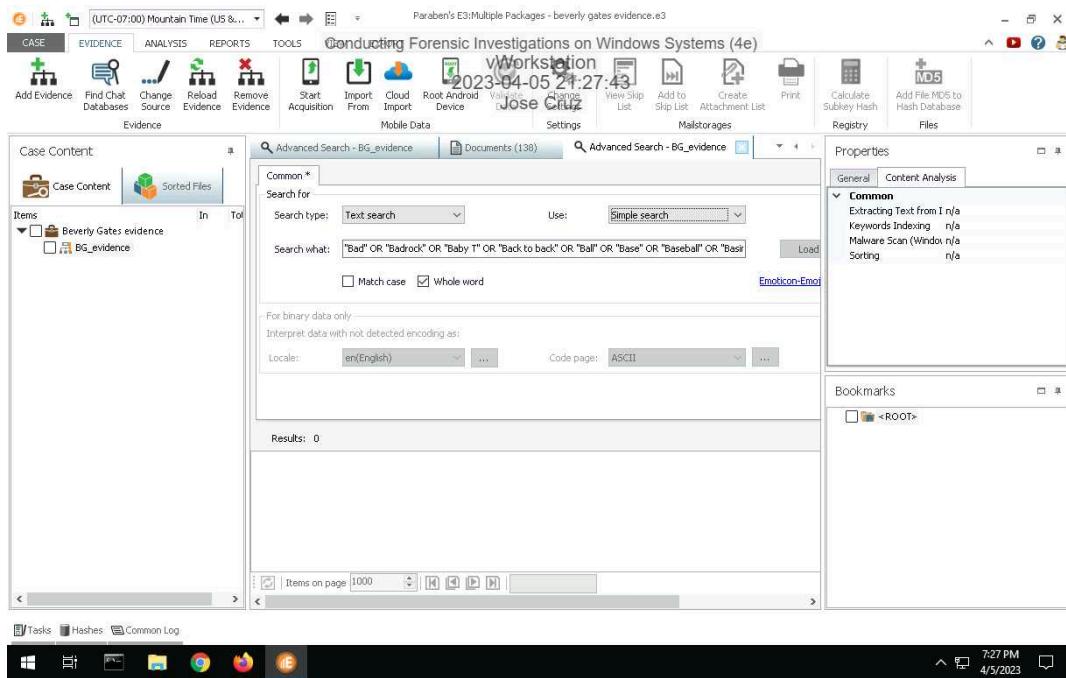
26. Make a screen capture showing at least one suspicious search found in the Keywords sub-node.

The screenshot shows the EnCase Forensic interface. The main pane displays a search result for the URL <https://www.google.com/search?q=online+anonymizers&oq=online+anonymizers&aqs=chrome..6957.1767JQ78Jsorlclchrome>. The properties pane on the right shows the title "online anonymizers - Google Search" and the visit date "4/27/2021 10:59:23 AM". The status bar at the bottom indicates the time as 4:48 PM and the date as 4/5/2023.

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.

