

# Conducting Forensic Investigations on Windows Systems (4e)

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

Student:

Matias Kun

Email:

rkh4zx@virginia.edu

Time on Task:

11 hours, 40 minutes

Progress:

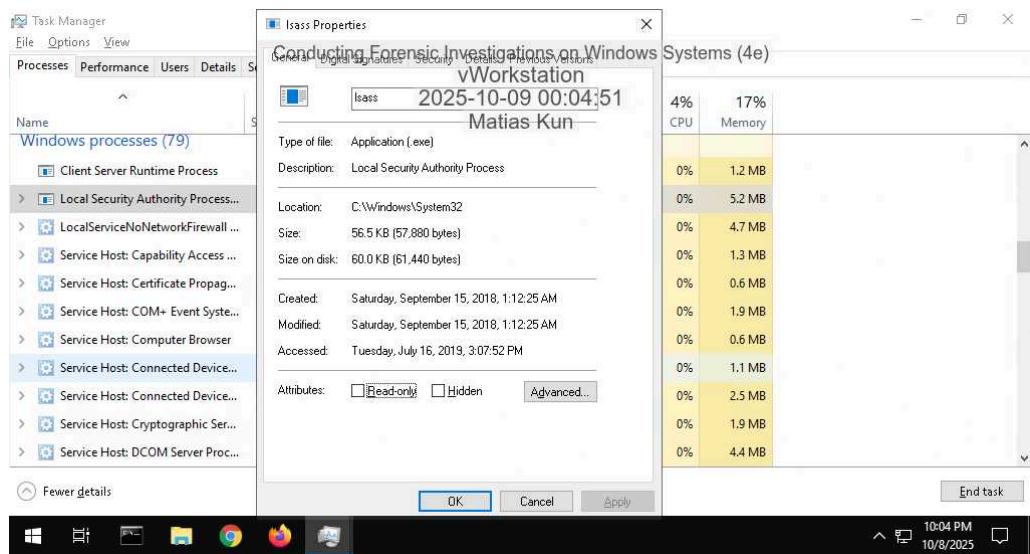
100%

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

## Section 1: Hands-On Demonstration

### Part 1: Gather Basic System Information

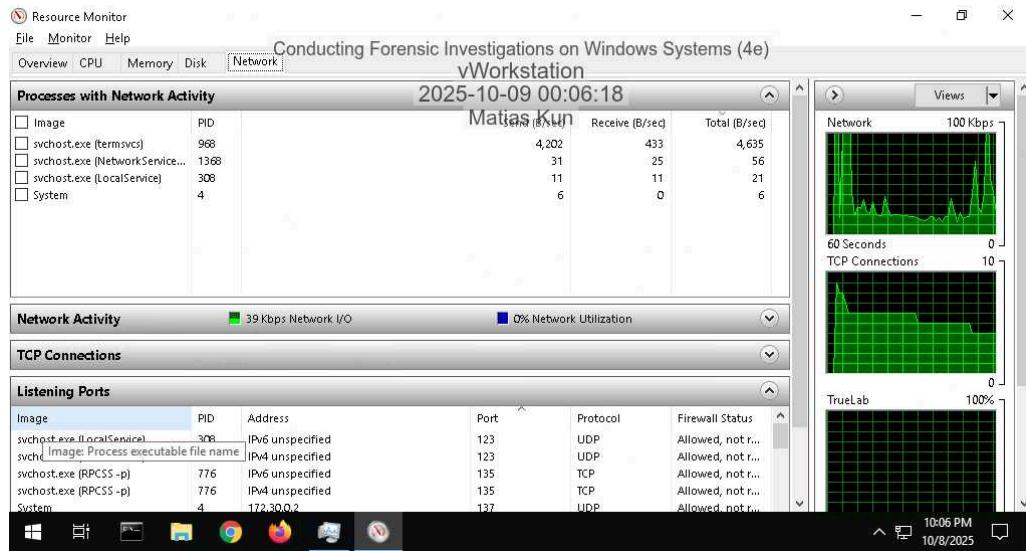
4. Make a screen capture showing the Properties window for the process you selected.



# 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 with the title "Conducting Forensic Investigations on Windows Systems (4e) vWorkstation". The command entered is "fsutil fsinfo ntfsinfo c:". The output provides detailed information about the NTFS volume on drive C:

```
C:\Users\Administrator>fsutil fsinfo ntfsinfo c:
2025-10-09 00:06:57
NTFS Volume Serial Number : 0xe0f46c07f46bd5fa
NTFS Version : 3.1
LFS Version : 2.0
Number Sectors : 0x0000000011569ff8
Total Clusters : 0x00000000022ad3ff
Free Clusters : 0x00000000002edf57
Total Reserved : 0x00000000000126e
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 : 0x0000000028740000
Mft Start Lcn : 0x000000000000c8000
Mft2 Start Lcn : 0x0000000000000002
Mft Zone Start : 0x0000000000047ac0
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-D7C204107C12
```

The bottom right corner of the window shows the date and time: 10:06 PM 10/8/2025.

# 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.**

```
Administrator: Command Prompt
Total Reserved : 0x000000000000126e
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 : 0x00000000000c0000
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 : B3BA1e61-A635-11E6-BB74-D7C204107C12

C:\Users\Administrator>fsutil usn queryjournal C:
User Journal ID : 0x01d34436e7a3bce
First Usn : 0x00000000083d0000
Next Usn : 0x00000000085708998
Lowest Valid Usn : 0x00000000083d0000
Max Usn : 0x7fffffffffffff0000
Maximum Size : 0x0000000002000000
Allocation Delta : 0x0000000000000000
Minimum record version supported : 2
Maximum record version supported : 4
Write range tracking: Disabled

C:\Users\Administrator>
```

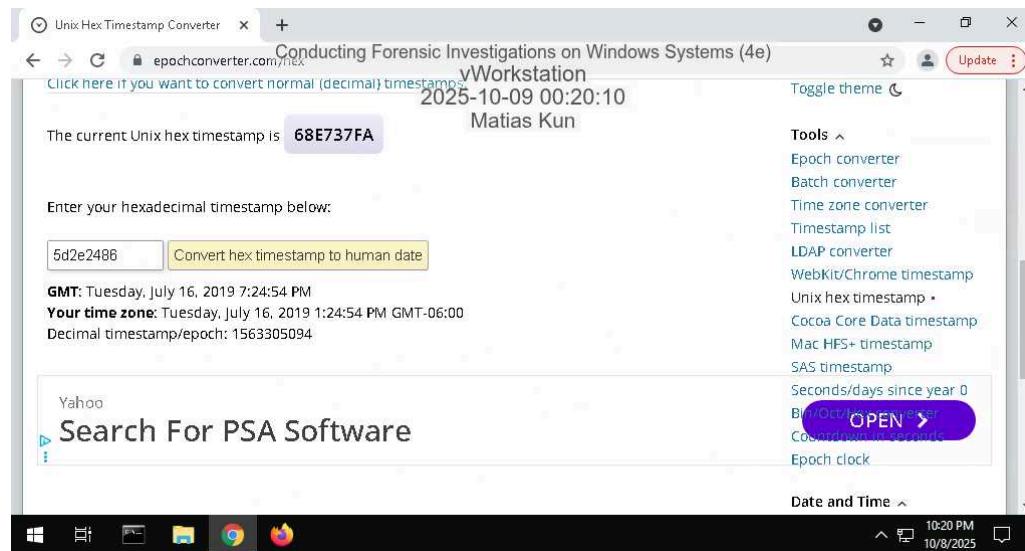
26. Make a screen capture showing the file path for the `yourname.txt` file.

## Part 2: Explore the Registry

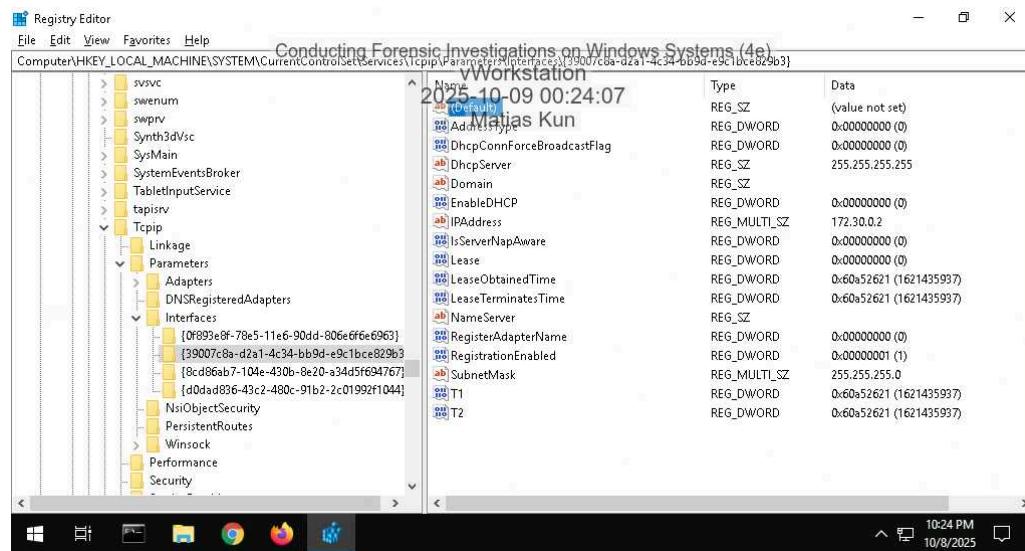
# Conducting Forensic Investigations on Windows Systems (4e)

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.



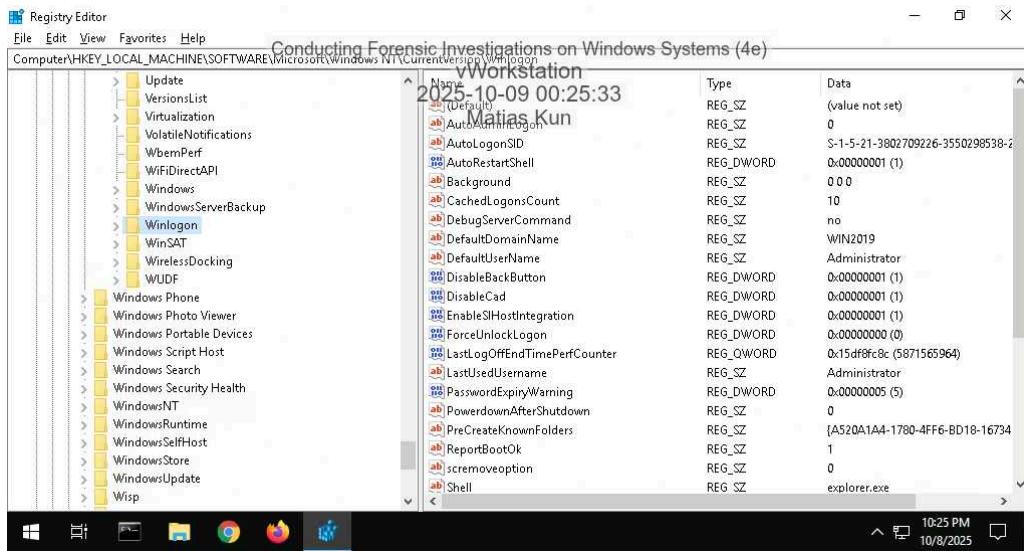
13. Make a screen capture showing the key values for the vWorkstation's default network interface.



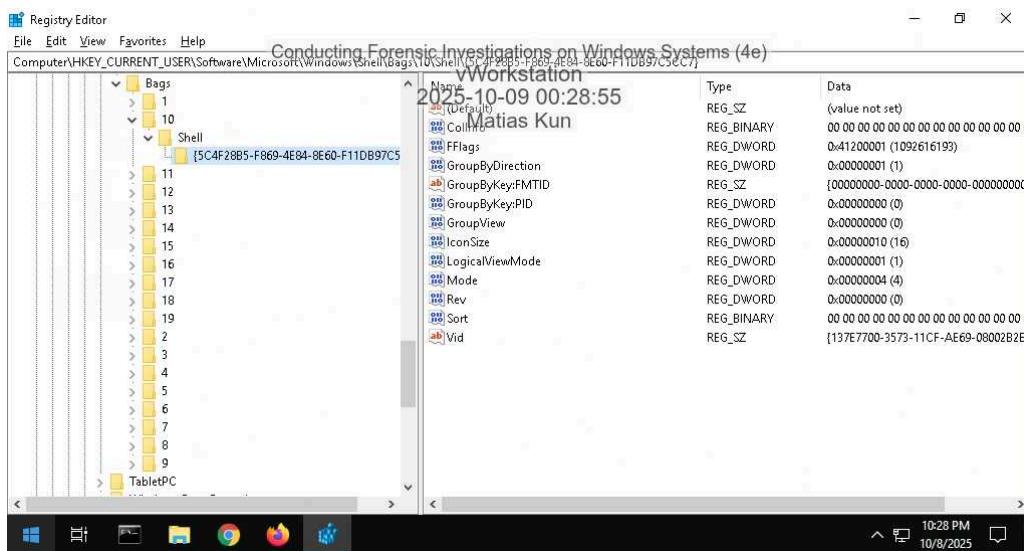
# Conducting Forensic Investigations on Windows Systems (4e)

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

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



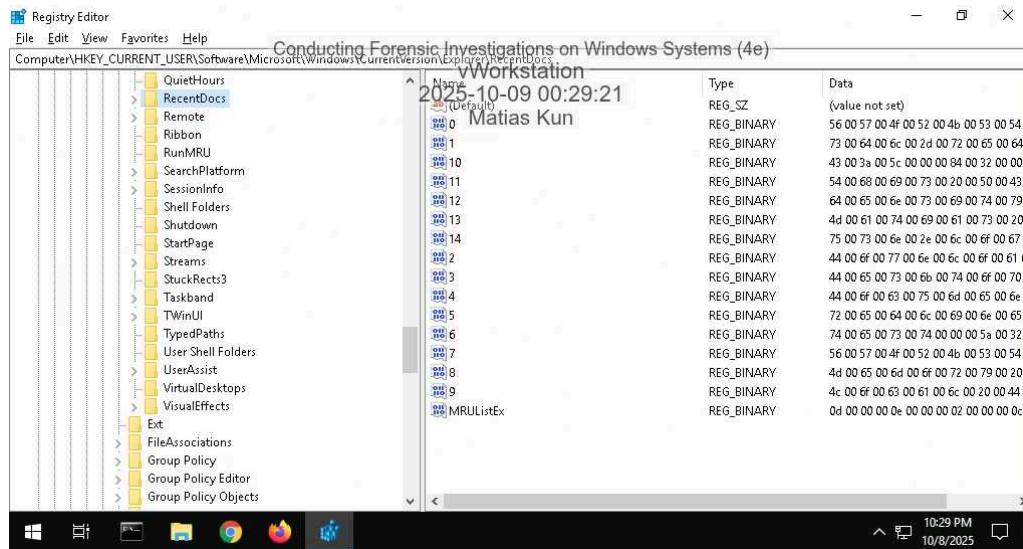
## 18. Make a screen capture showing the ShellBags key values.



# 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.



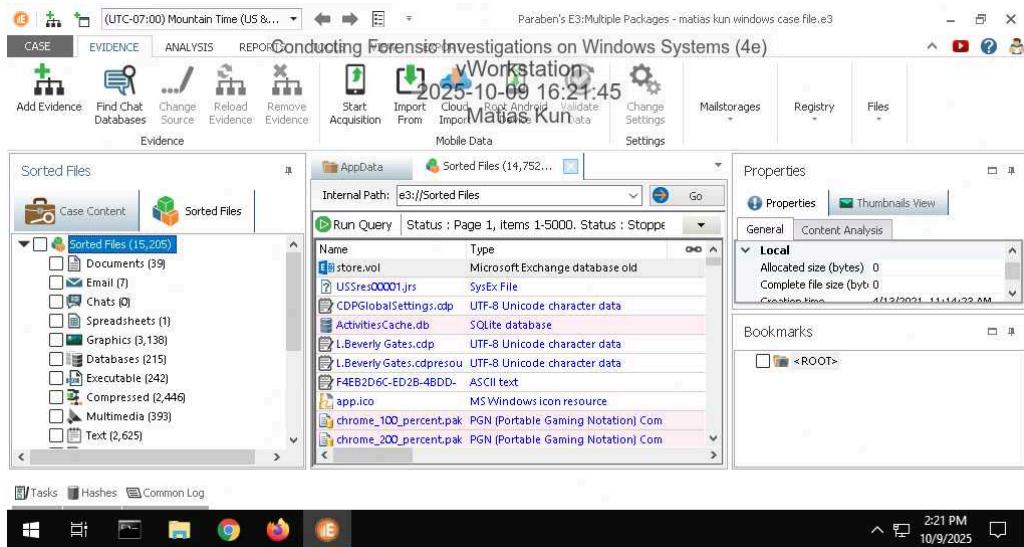
# Conducting Forensic Investigations on Windows Systems (4e)

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

## Section 2: Applied Learning

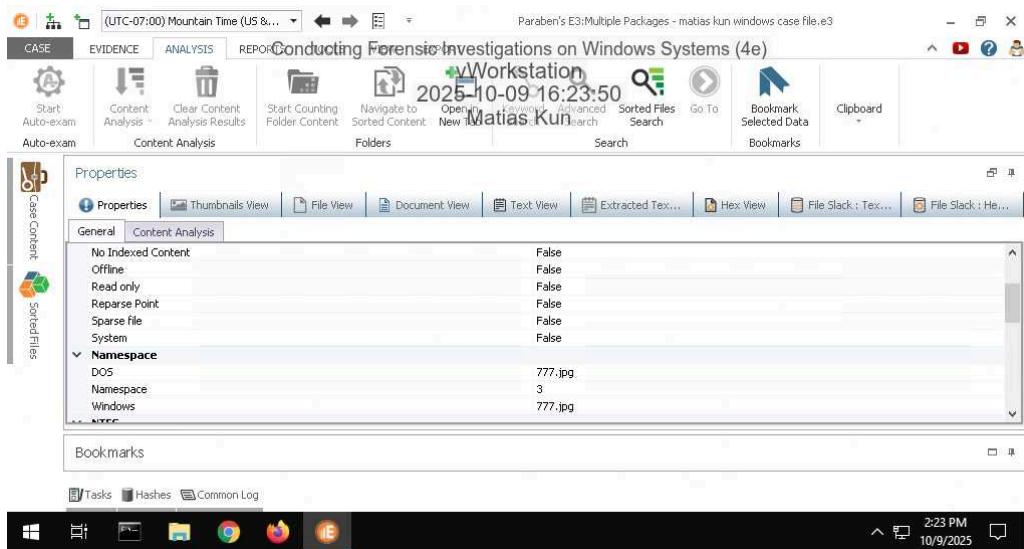
### Part 1: Create and Sort a New Case File

14. Make a screen capture showing the Sorted Files.



### Part 2: Perform Forensic Analysis on a Windows Drive Image

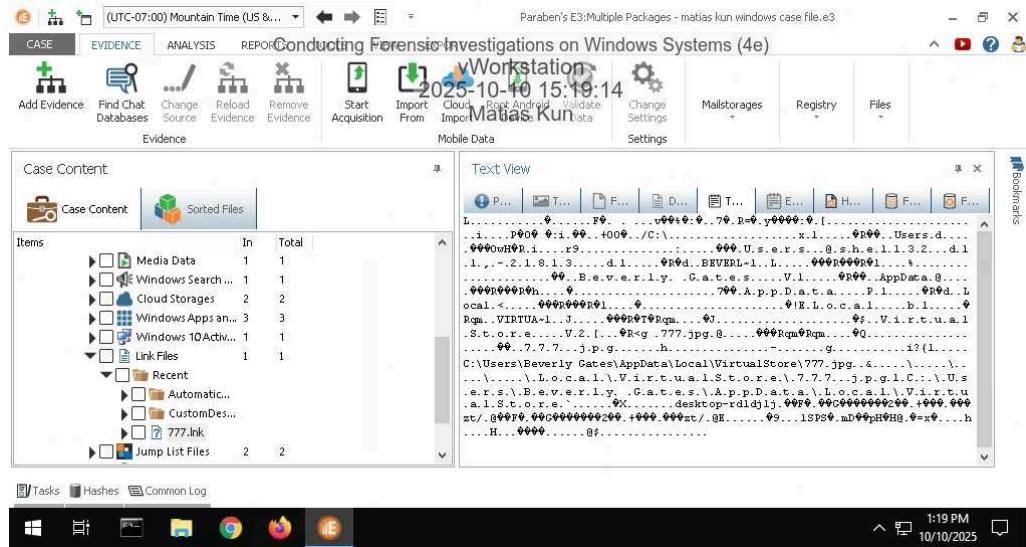
6. Make a screen capture showing the contents of the 777.jpg file in the Document View.



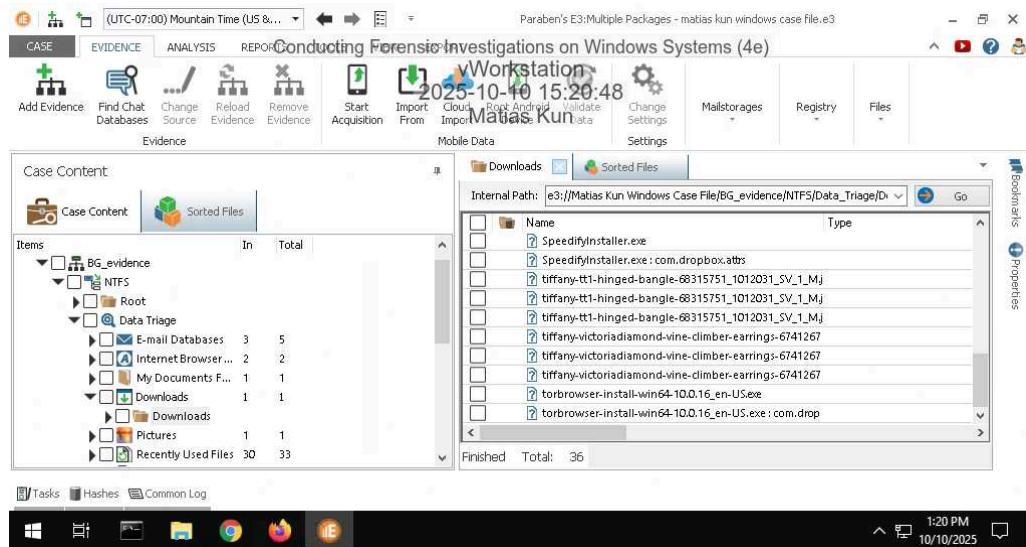
# Conducting Forensic Investigations on Windows Systems (4e)

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.

The screenshot shows the Paraben's E3 forensic tool interface. The main window title is "Conducting Forensic Investigations on Windows Systems (4e)". The top menu bar includes "CASE", "EVIDENCE", "ANALYSIS", "REPORT", "Mobile Data", "Mailstorages", "Registry", and "Files". The timeline at the top right shows "2025-10-10 15:23:05" and the case name "Matias Kun". The left sidebar has "Case Content" and "Sorted Files" tabs. The "Sorted Files" tab is selected, showing a table of registry keys under the internal path "e3://Matias Kun Windows Case File/BG\_evidence/NTFS/Data\_Triage/R". The table has columns "Name", "Type", and "Data". The data includes:

Name	Type	Data
DisplayName	REG_SZ	Speedify
UninstallString	REG_SZ	C:\Program Files (x86)\Speedify\Uninstall.exe
InstallLocation	REG_SZ	C:\Program Files (x86)\Speedify
DisplayIcon	REG_SZ	C:\Program Files (x86)\Speedify\Uninstall.exe0
Publisher	REG_SZ	Connectify
URLInfoAbout	REG_SZ	http://www.speedify.com/
DisplayVersion	REG_SZ	11.1.969

The bottom status bar shows "1:23 PM 10/10/2025".

## 19. Make a screen capture showing the users list.

The screenshot shows the Paraben's E3 forensic tool interface. The main window title is "Conducting Forensic Investigations on Windows Systems (4e)". The top menu bar includes "CASE", "EVIDENCE", "ANALYSIS", "REPORT", "Mobile Data", "Mailstorages", "Registry", and "Files". The timeline at the top right shows "2025-10-10 15:28:36" and the case name "Matias Kun". The left sidebar has "Case Content" and "Sorted Files" tabs. The "Sorted Files" tab is selected, showing a table of user information under the internal path "e3://Matias Kun Windows Case File/BG\_evidence/NTFS/Data\_Triage/R". The table has columns "Name" and "Data". The data includes:

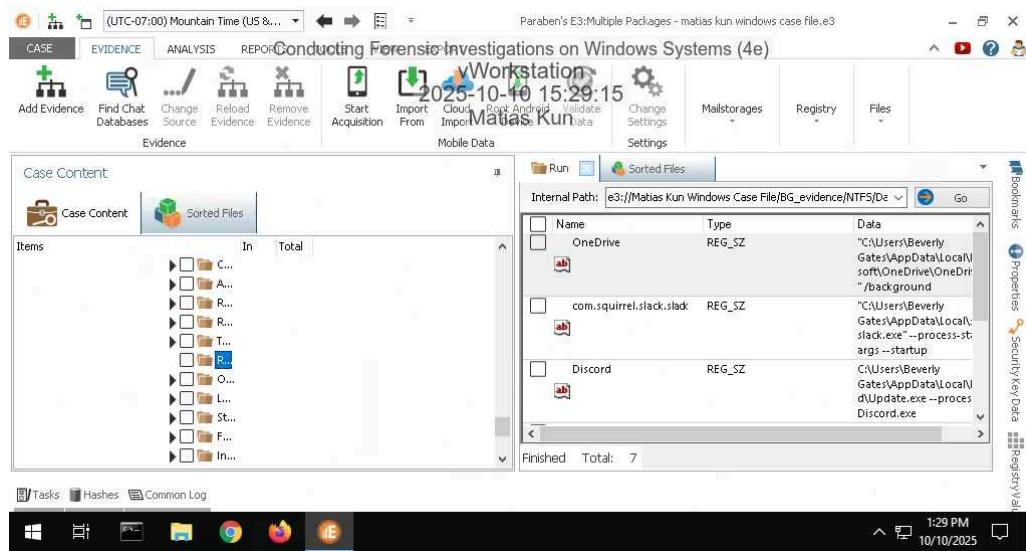
Name	Data
Last Logged on User	
Beverly Gates	

The bottom status bar shows "1:28 PM 10/10/2025".

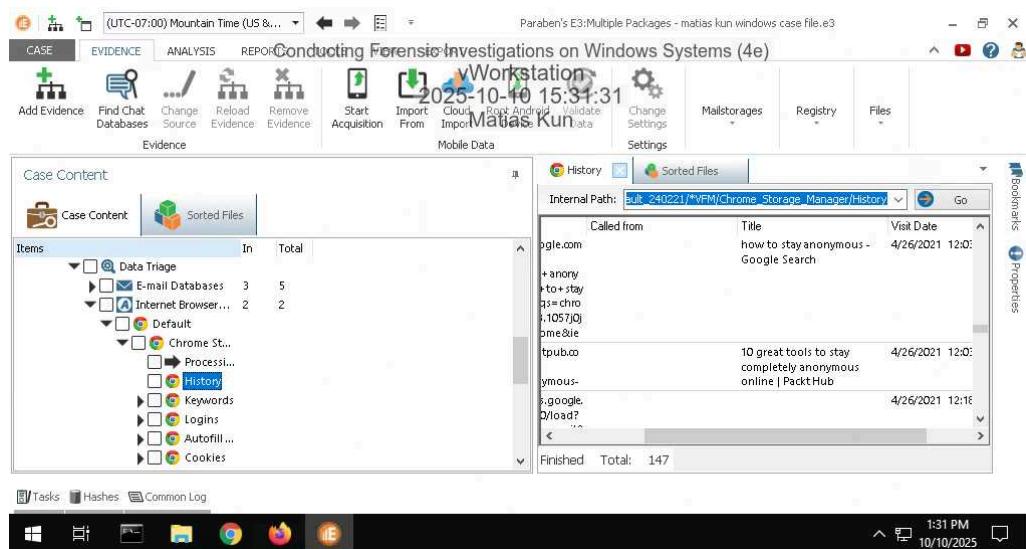
# Conducting Forensic Investigations on Windows Systems (4e)

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

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



## 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.

The screenshot shows the Paraben's E3 forensic tool interface. The main window title is "Paraben's E3:Multiple Packages - matias.kun.windows.casefile.e3". The top menu bar includes CASE, EVIDENCE, ANALYSIS, and REPO. The EVIDENCE tab is selected. The timeline shows "2025-10-10 15:31:52". The left sidebar has sections for Add Evidence, Find Chat Databases, Change Source, Reload Evidence, Start Acquisition, Import From, Change Settings, Mailstorages, Registry, and Files. The "Evidence" section is expanded, showing "Case Content" and "Sorted Files". Under "Case Content", there are nodes for Data Triage, E-mail Databases (3 In, 5 Total), Internet Browser... (2 In, 2 Total), and Default. The Default node is expanded, showing sub-nodes for Chrome St..., Process..., History, Keywords (which is highlighted in blue), Logins, Autofill..., and Cookies. The "Sorted Files" tab is selected in the evidence sidebar. On the right, a "Keywords" pane is open with the internal path "e3:///Matias.Kun.Windows.CaseFile/BG\_evidence/NTFS". It lists two search results:

Term	Action URL	Search Engine Short
how to hide on web	https://www.google.com/search?q=how+to+hide+on+web&oq=how+to+hide+on+web&aqs=chrome..6957j0j2230j9.1263j0j7&sourceid=chromium&ie=UTF-8	Google search?
how to stay anonymous	https://www.google.com/search?q=how+to+stay+anonymous&oq=how+to+stay+anonymous&aqs=chrome..6957j0j2230j9.1263j0j7&sourceid=chromium&ie=UTF-8	Google search?

At the bottom, the status bar shows "Finished Total: 8" and the system clock "1:31 PM 10/10/2025".

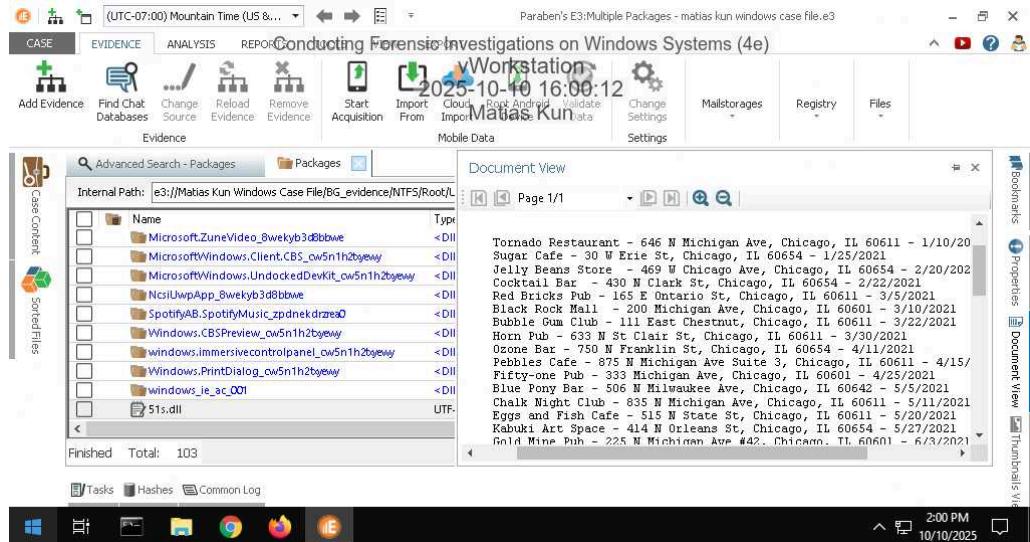
# Conducting Forensic Investigations on Windows Systems (4e)

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

## 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.

