Conducting Forensic Investigations on Windows Systems (4e)

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

Student:	Email:
Karan Atul Vora	kxv230021@utdallas.edu

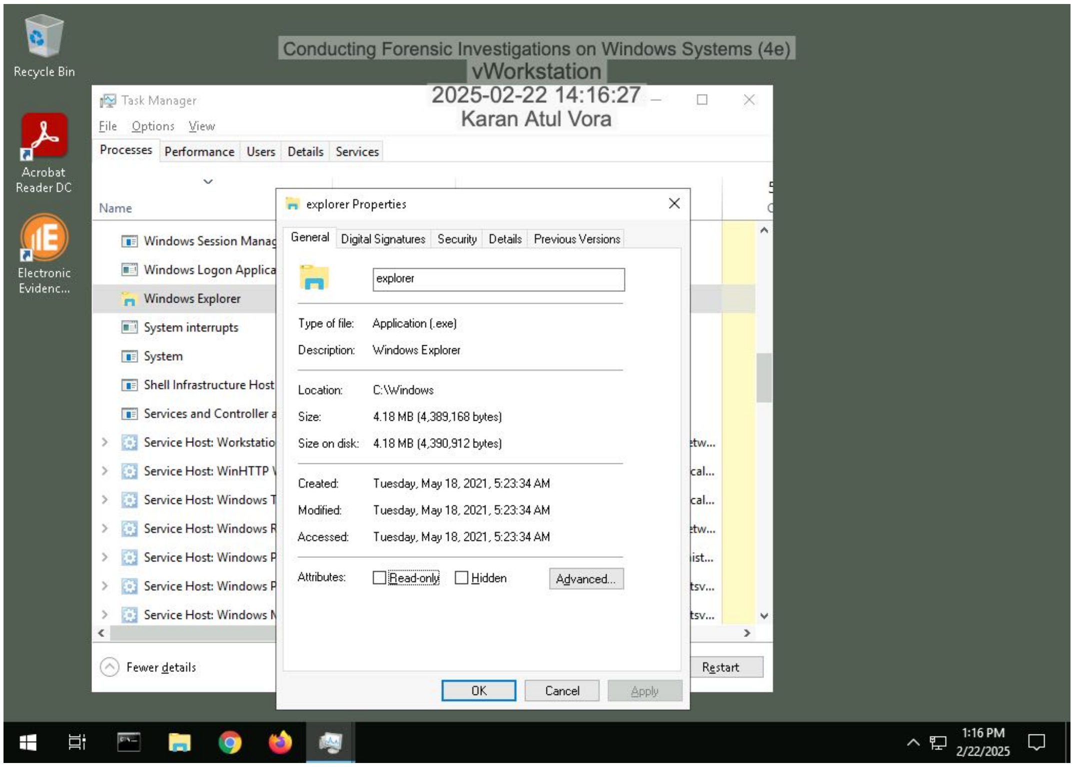
Time on Task:	Progress:
2 hours, 9 minutes	100%

Report Generated: Monday, February 24, 2025 at 4:29 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)
vWorkstation
2025-02-22 14:16:27
Karan Atul Vora

explorer Properties

explorer

Type of file: Application (.exe)
Description: Windows Explorer

Location: C:\Windows
Size: 4.18 MB (4,389,168 bytes)
Size on disk: 4.18 MB (4,390,912 bytes)

Created: Tuesday, May 18, 2021, 5:23:34 AM
Modified: Tuesday, May 18, 2021, 5:23:34 AM
Accessed: Tuesday, May 18, 2021, 5:23:34 AM

Attributes: □ Read-only □ Hidden

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

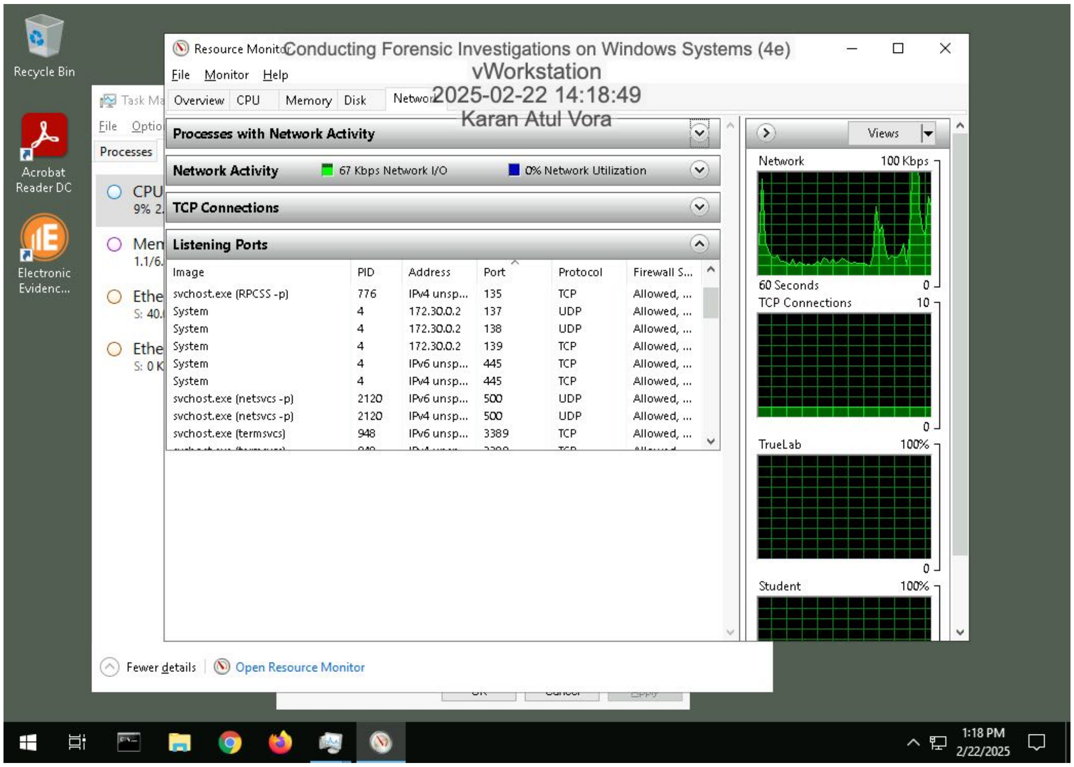
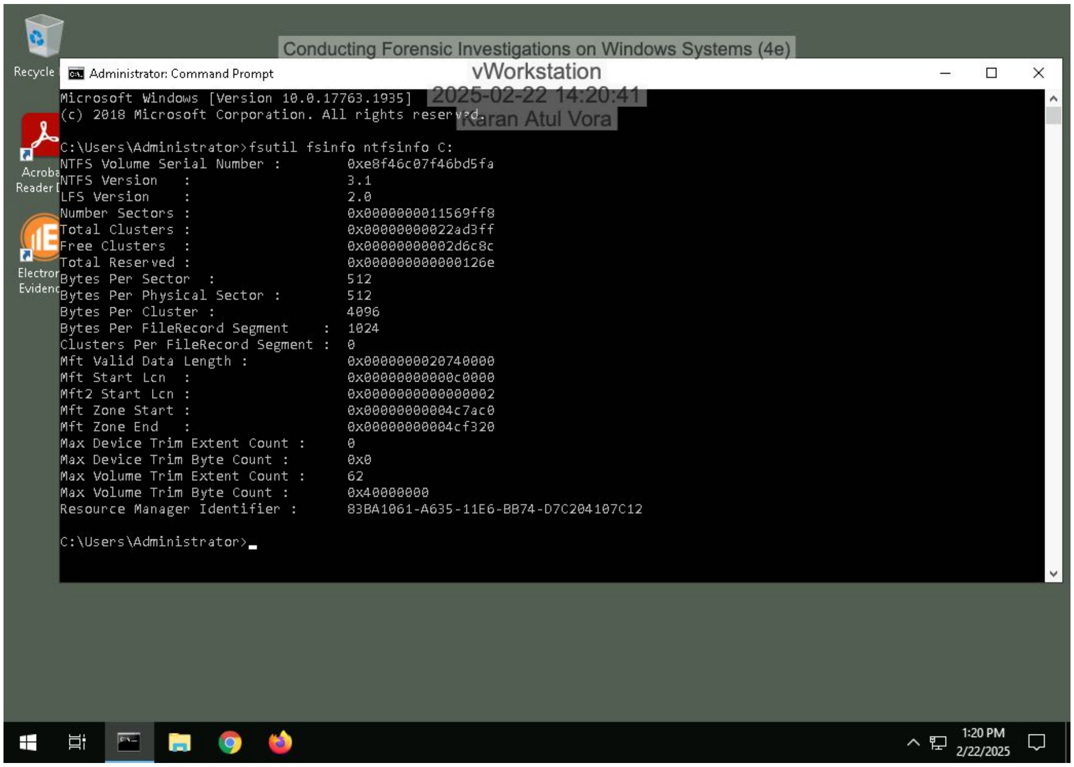


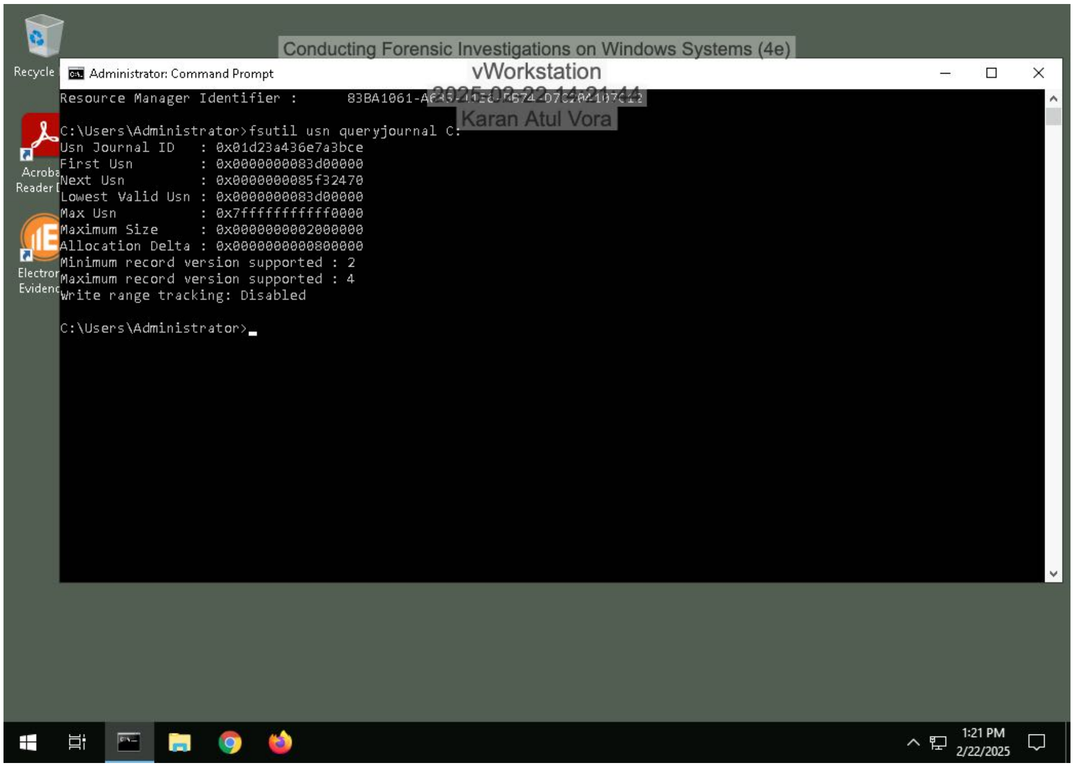
Image	PID	Address	Port	Protocol	Firewall S...
svchost.exe (RPCSS -p)	776	IPv4 unsp...	135	TCP	Allowed, ...
System	4	172.30.0.2	137	UDP	Allowed, ...
System	4	172.30.0.2	138	UDP	Allowed, ...
System	4	172.30.0.2	139	TCP	Allowed, ...
System	4	IPv6 unsp...	445	TCP	Allowed, ...
System	4	IPv4 unsp...	445	TCP	Allowed, ...
svchost.exe (netsvcs -p)	2120	IPv6 unsp...	500	UDP	Allowed, ...
svchost.exe (netsvcs -p)	2120	IPv4 unsp...	500	UDP	Allowed, ...
svchost.exe (termsvcs)	948	IPv6 unsp...	3389	TCP	Allowed, ...

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



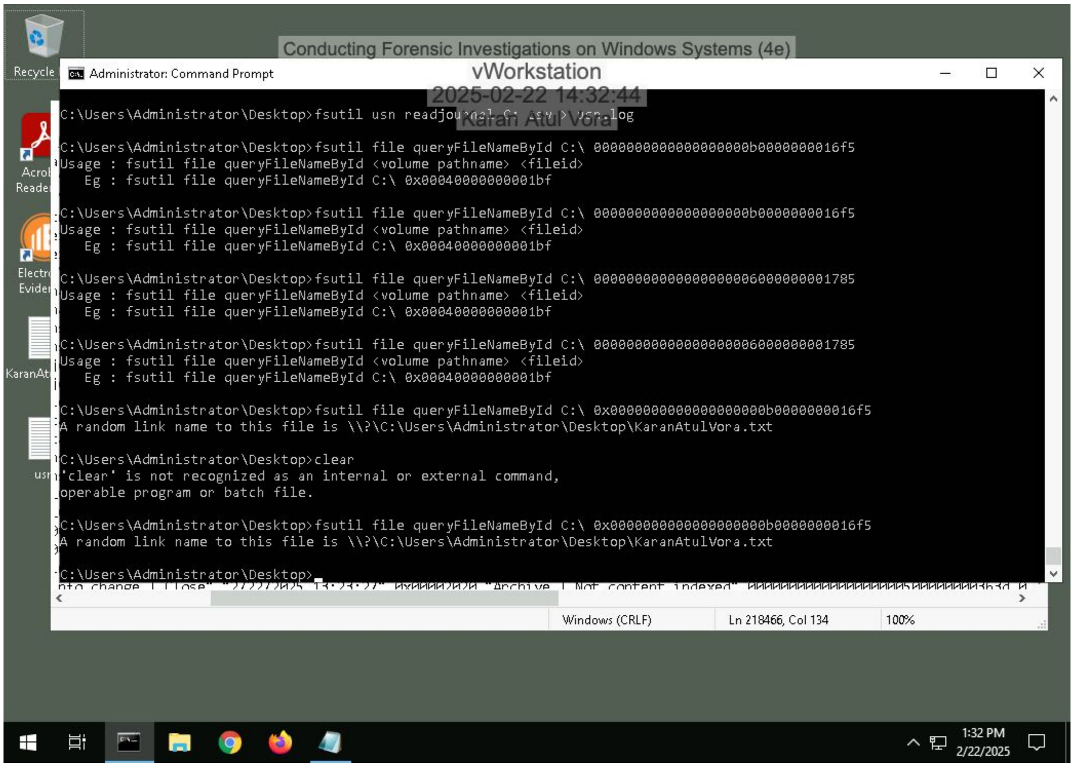
```
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>fsutil fsinfo ntfsinfo C:
NTFS Volume Serial Number :        0xe8f46c07f46bd5fa
NTFS Version   :                   3.1
LFS Version    :                   2.0
Number Sectors :                   0x0000000011569ff8
Total Clusters :                   0x00000000022ad3ff
Free Clusters  :                   0x00000000002d6c8c
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 :                   0x00000000004c7ac0
Mft Zone End   :                   0x00000000004cf320
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

C:\Users\Administrator>
```

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



```
Resource Manager Identifier :      83BA1061-A6[illegible]

C:\Users\Administrator>fsutil usn queryjournal C:
Usn Journal ID   : 0x01d23a436e7a3bce
First Usn        : 0x0000000083d00000
Next Usn         : 0x0000000085f32470
Lowest Valid Usn : 0x0000000083d00000
Max Usn          : 0x7fffffffffff0000
Maximum Size     : 0x0000000002000000
Allocation Delta : 0x0000000000800000
Minimum record version supported : 2
Maximum record version supported : 4
Write range tracking: Disabled

C:\Users\Administrator>
```

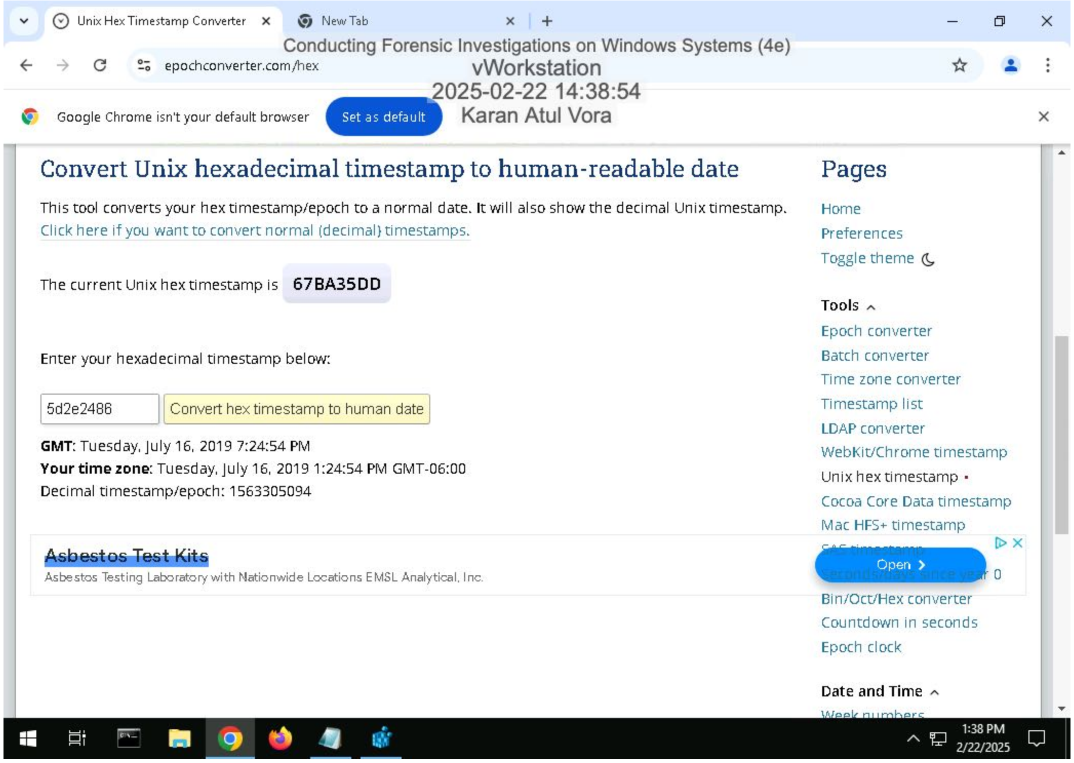
26. **Make a screen capture** showing the **file path for the *yourname*.txt file**.



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

C:\Users\Administrator\Desktop>fsutil file queryFileNameById C:\ 00000000000000000000b0000000016f5
Usage : fsutil file queryFileNameById <volume pathname> <fileid>
   Eg : fsutil file queryFileNameById C:\ 0x00040000000001bf

C:\Users\Administrator\Desktop>fsutil file queryFileNameById C:\ 00000000000000000000b0000000016f5
Usage : fsutil file queryFileNameById <volume pathname> <fileid>
   Eg : fsutil file queryFileNameById C:\ 0x00040000000001bf

C:\Users\Administrator\Desktop>fsutil file queryFileNameById C:\ 000000000000000000006000000001785
Usage : fsutil file queryFileNameById <volume pathname> <fileid>
   Eg : fsutil file queryFileNameById C:\ 0x00040000000001bf

C:\Users\Administrator\Desktop>fsutil file queryFileNameById C:\ 000000000000000000006000000001785
Usage : fsutil file queryFileNameById <volume pathname> <fileid>
   Eg : fsutil file queryFileNameById C:\ 0x00040000000001bf

C:\Users\Administrator\Desktop>fsutil file queryFileNameById C:\ 0x00000000000000000000b0000000016f5
A random link name to this file is \\?\C:\Users\Administrator\Desktop\KaranAtulVora.txt

C:\Users\Administrator\Desktop>clear
'clear' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator\Desktop>fsutil file queryFileNameById C:\ 0x00000000000000000000b0000000016f5
A random link name to this file is \\?\C:\Users\Administrator\Desktop\KaranAtulVora.txt

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

Part 2: Explore the Registry

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



Unix Hex Timestamp Converter
New Tab
epochconverter.com/hex
Google Chrome isn't your default browser
Set as default

Conducting Forensic Investigations on Windows Systems (4e)
vWorkstation
2025-02-22 14:38:54
Karan Atul Vora

Convert Unix hexadecimal timestamp to human-readable date

This tool converts your hex timestamp/epoch to a normal date. It will also show the decimal Unix timestamp.
Click here if you want to convert normal (decimal) timestamps.

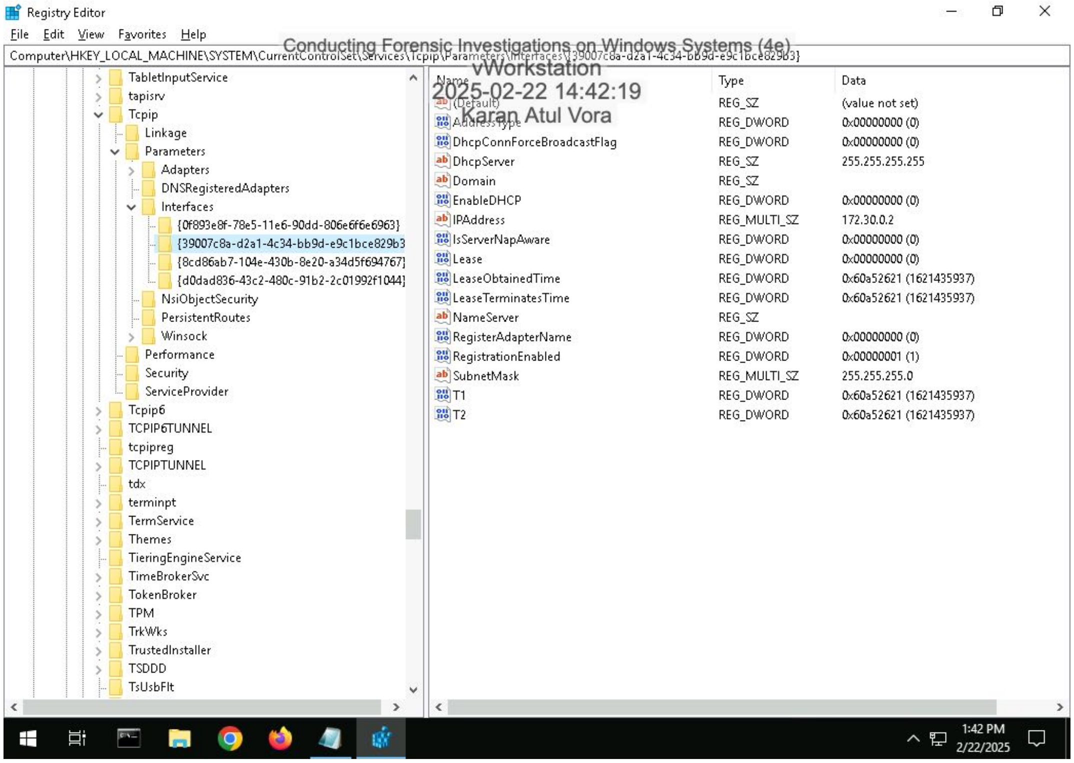
The current Unix hex timestamp is **67BA35DD**

Enter your hexadecimal timestamp below:

5d2e2486 Convert hex timestamp to human date

GMT: Tuesday, July 16, 2019 7:24:54 PM
Your time zone: Tuesday, July 16, 2019 1:24:54 PM GMT-06:00
Decimal timestamp/epoch: 1563305094

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

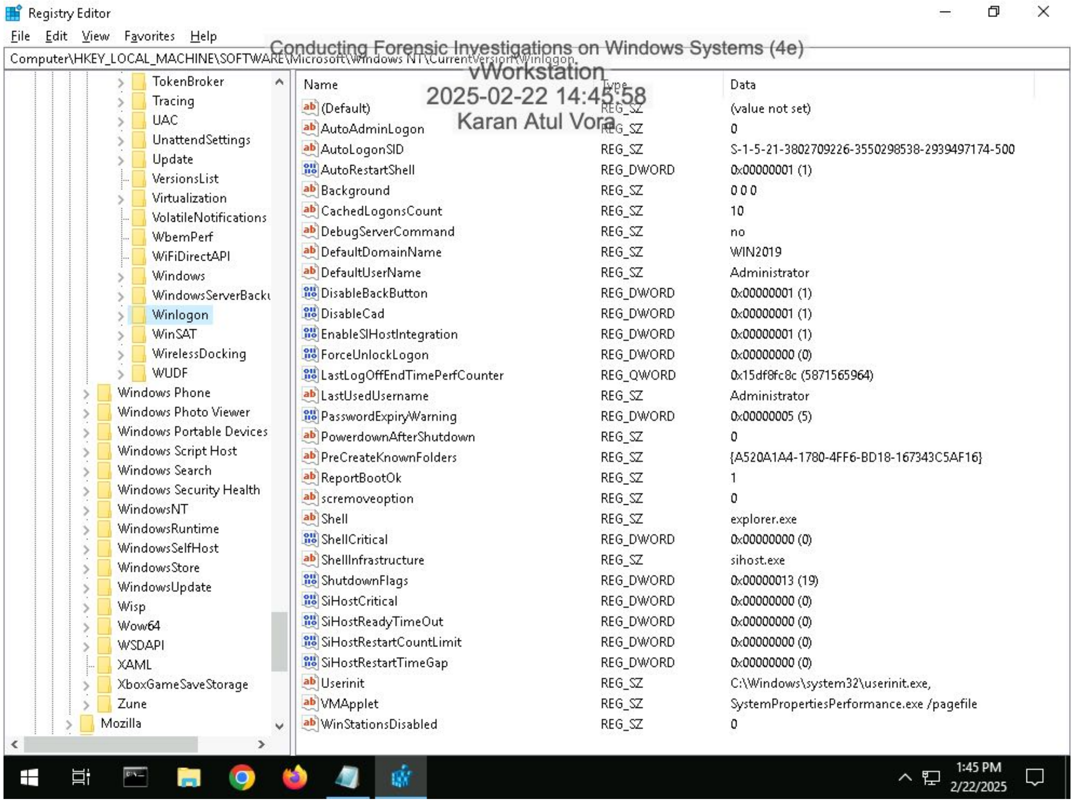


Conducting Forensic Investigations on Windows Systems (4e)
vWorkstation
2025-02-22 14:42:19
Karan Atul Vora

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{39007c8a-d2a1-4c34-bb9d-e9c1bce829b3}

Name	Type	Data
(Default)	REG_SZ	(value not set)
AddressType	REG_DWORD	0x00000000 (0)
DhcpConnForceBroadcastFlag	REG_DWORD	0x00000000 (0)
DhcpServer	REG_SZ	255.255.255.255
Domain	REG_SZ	
EnableDHCP	REG_DWORD	0x00000000 (0)
IPAddress	REG_MULTI_SZ	172.30.0.2
IsServerNapAware	REG_DWORD	0x00000000 (0)
Lease	REG_DWORD	0x00000000 (0)
LeaseObtainedTime	REG_DWORD	0x60a52621 (1621435937)
LeaseTerminatesTime	REG_DWORD	0x60a52621 (1621435937)
NameServer	REG_SZ	
RegisterAdapterName	REG_DWORD	0x00000000 (0)
RegistrationEnabled	REG_DWORD	0x00000001 (1)
SubnetMask	REG_MULTI_SZ	255.255.255.0
T1	REG_DWORD	0x60a52621 (1621435937)
T2	REG_DWORD	0x60a52621 (1621435937)

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

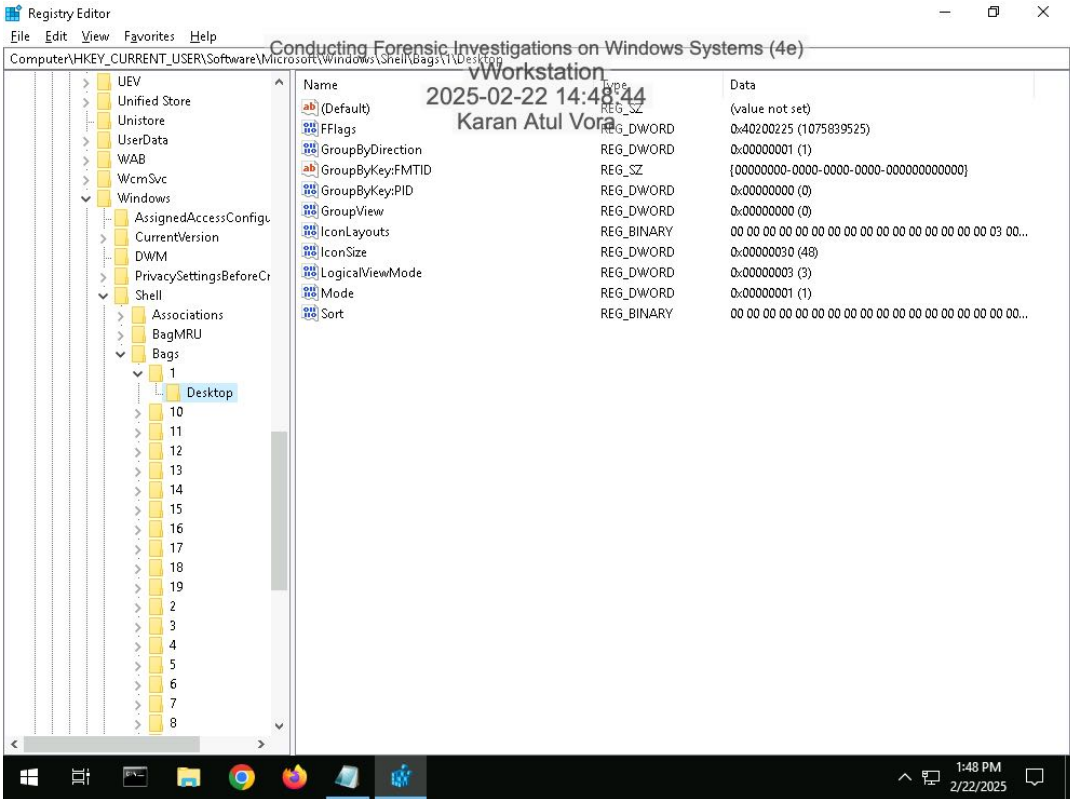


Conducting Forensic Investigations on Windows Systems (4e)
vWorkstation
2025-02-22 14:45:58
Karan Atul Vora

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Name	Type	Data
(Default)	REG_SZ	(value not set)
AutoAdminLogon	REG_SZ	0
AutoLogonSID	REG_SZ	S-1-5-21-3802709226-3550298538-2939497174-500
AutoRestartShell	REG_DWORD	0x00000001 (1)
Background	REG_SZ	0 0 0
CachedLogonsCount	REG_SZ	10
DebugServerCommand	REG_SZ	no
DefaultDomainName	REG_SZ	WIN2019
DefaultUserName	REG_SZ	Administrator
DisableBackButton	REG_DWORD	0x00000001 (1)
DisableCad	REG_DWORD	0x00000001 (1)
EnableSIHostIntegration	REG_DWORD	0x00000001 (1)
ForceUnlockLogon	REG_DWORD	0x00000000 (0)
LastLogOffEndTimePerfCounter	REG_QWORD	0x15df8fc8c (5871565964)
LastUsedUsername	REG_SZ	Administrator
PasswordExpiryWarning	REG_DWORD	0x00000005 (5)
PowerdownAfterShutdown	REG_SZ	0
PreCreateKnownFolders	REG_SZ	{A520A1A4-1780-4FF6-BD18-167343C5AF16}
ReportBootOk	REG_SZ	1
scremoveoption	REG_SZ	0
Shell	REG_SZ	explorer.exe
ShellCritical	REG_DWORD	0x00000000 (0)
ShellInfrastructure	REG_SZ	sihost.exe
ShutdownFlags	REG_DWORD	0x00000013 (19)
SiHostCritical	REG_DWORD	0x00000000 (0)
SiHostReadyTimeOut	REG_DWORD	0x00000000 (0)
SiHostRestartCountLimit	REG_DWORD	0x00000000 (0)
SiHostRestartTimeGap	REG_DWORD	0x00000000 (0)
Userinit	REG_SZ	C:\Windows\system32\userinit.exe,
VMApplet	REG_SZ	SystemPropertiesPerformance.exe /pagefile
WinStationsDisabled	REG_SZ	0

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

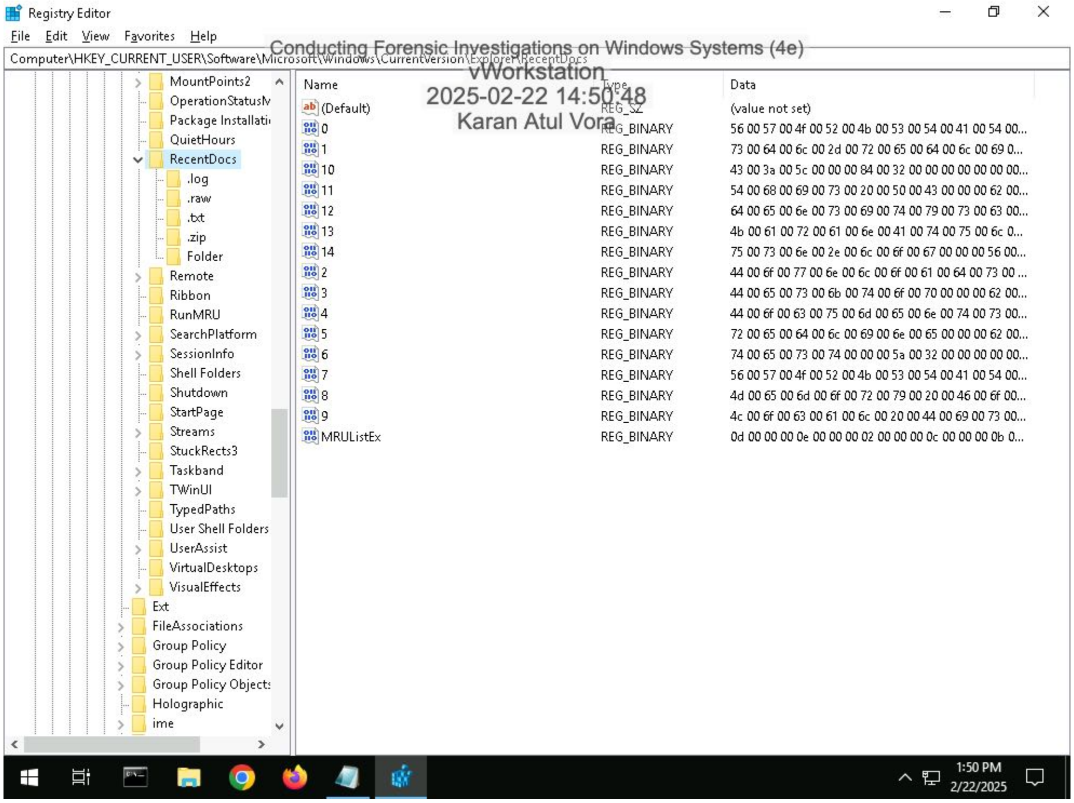


Conducting Forensic Investigations on Windows Systems (4e)
vWorkstation
2025-02-22 14:48:44
Karan Atul Vora

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\1\Desktop

Name	Type	Data
(Default)	REG_SZ	(value not set)
FFlags	REG_DWORD	0x40200225 (1075839525)
GroupByDirection	REG_DWORD	0x00000001 (1)
GroupByKey:FMTID	REG_SZ	{00000000-0000-0000-0000-000000000000}
GroupByKey:PID	REG_DWORD	0x00000000 (0)
GroupView	REG_DWORD	0x00000000 (0)
IconLayouts	REG_BINARY	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00...
IconSize	REG_DWORD	0x00000030 (48)
LogicalViewMode	REG_DWORD	0x00000003 (3)
Mode	REG_DWORD	0x00000001 (1)
Sort	REG_BINARY	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00...

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



Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

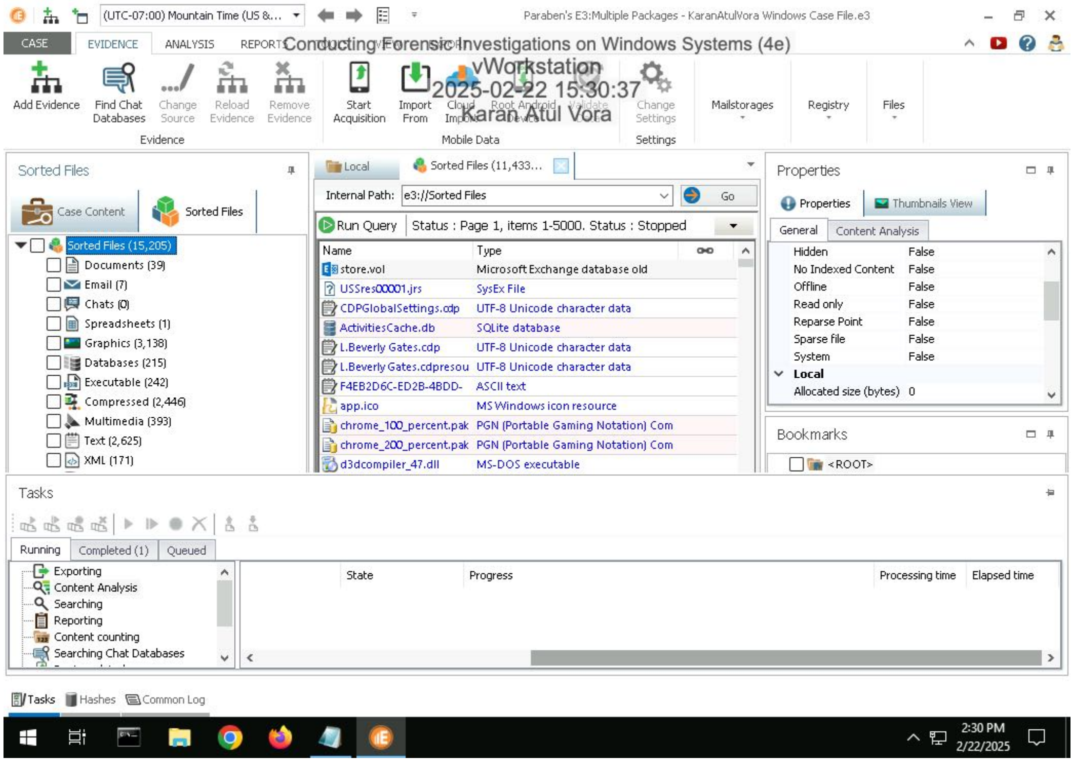
Conducting Forensic Investigations on Windows Systems (4e)
vWorkstation
2025-02-22 14:50:48
Karan Atul Vora

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 00 41 00 54 00...
1	REG_BINARY	73 00 64 00 6c 00 2d 00 72 00 65 00 64 00 6c 00 69 0...
10	REG_BINARY	43 00 3a 00 5c 00 00 00 84 00 32 00 00 00 00 00 00 00...
11	REG_BINARY	54 00 68 00 69 00 73 00 20 00 50 00 43 00 00 00 62 00...
12	REG_BINARY	64 00 65 00 6e 00 73 00 69 00 74 00 79 00 73 00 63 00...
13	REG_BINARY	4b 00 61 00 72 00 61 00 6e 00 41 00 74 00 75 00 6c 0...
14	REG_BINARY	75 00 73 00 6e 00 2e 00 6c 00 6f 00 67 00 00 00 56 00...
2	REG_BINARY	44 00 6f 00 77 00 6e 00 6c 00 6f 00 61 00 64 00 73 00 ...
3	REG_BINARY	44 00 65 00 73 00 6b 00 74 00 6f 00 70 00 00 00 62 00...
4	REG_BINARY	44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 73 00...
5	REG_BINARY	72 00 65 00 64 00 6c 00 69 00 6e 00 65 00 00 00 62 00...
6	REG_BINARY	74 00 65 00 73 00 74 00 00 00 5a 00 32 00 00 00 00 00...
7	REG_BINARY	56 00 57 00 4f 00 52 00 4b 00 53 00 54 00 41 00 54 00...
8	REG_BINARY	4d 00 65 00 6d 00 6f 00 72 00 79 00 20 00 46 00 6f 00...
9	REG_BINARY	4c 00 6f 00 63 00 61 00 6c 00 20 00 44 00 69 00 73 00...
MRUListEx	REG_BINARY	0d 00 00 00 0e 00 00 00 02 00 00 00 0c 00 00 00 0b 0...

Section 2: Applied Learning

Part 1: Create and Sort a New Case File

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



- □ Sorted Files (15,205)
  - □ Documents (39)
  - □ Email (7)
  - □ Chats (0)
  - □ Spreadsheets (1)
  - □ Graphics (3,138)
  - □ Databases (215)
  - □ Executable (242)
  - □ Compressed (2,446)
  - □ Multimedia (393)
  - □ Text (2,625)
  - □ XML (171)

Internal Path: e3://Sorted Files

Status : Page 1, items 1-5000. Status : Stopped

Name	Type
store.vol	Microsoft Exchange database old
USSres00001.jrs	SysEx File
CDPGlobalSettings.cdp	UTF-8 Unicode character data
ActivitiesCache.db	SQLite database
L.Beverly Gates.cdp	UTF-8 Unicode character data
L.Beverly Gates.cdpresou	UTF-8 Unicode character data
F4EB2D6C-ED2B-4BDD-	ASCII text
app.ico	MS Windows icon resource
chrome_100_percent.pak	PGN (Portable Gaming Notation) Com
chrome_200_percent.pak	PGN (Portable Gaming Notation) Com
d3dcompiler_47.dll	MS-DOS executable

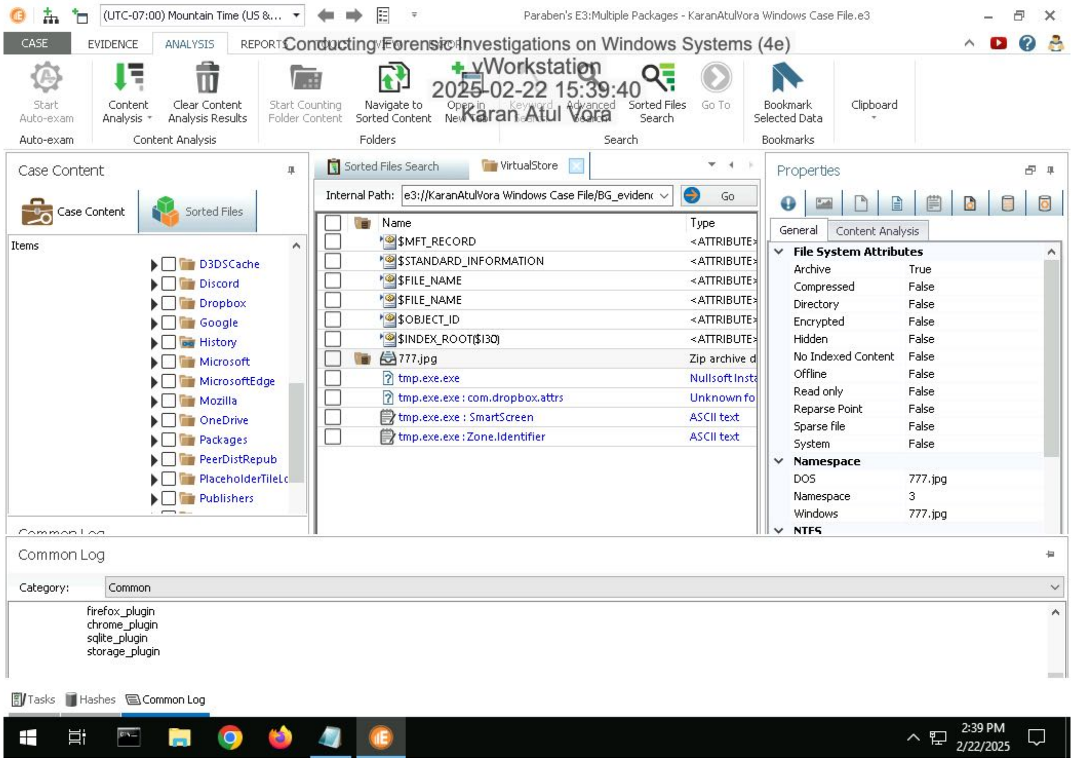
Hidden	False
No Indexed Content	False
Offline	False
Read only	False
Reparse Point	False
Sparse file	False
System	False
Local	
Allocated size (bytes)	0

- Exporting
- Content Analysis
- Searching
- Reporting
- Content counting
- Searching Chat Databases

	State	Progress	Processing time	Elapsed time

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.**



Internal Path: e3://KaranAtulVora Windows Case File/BG_evidenc

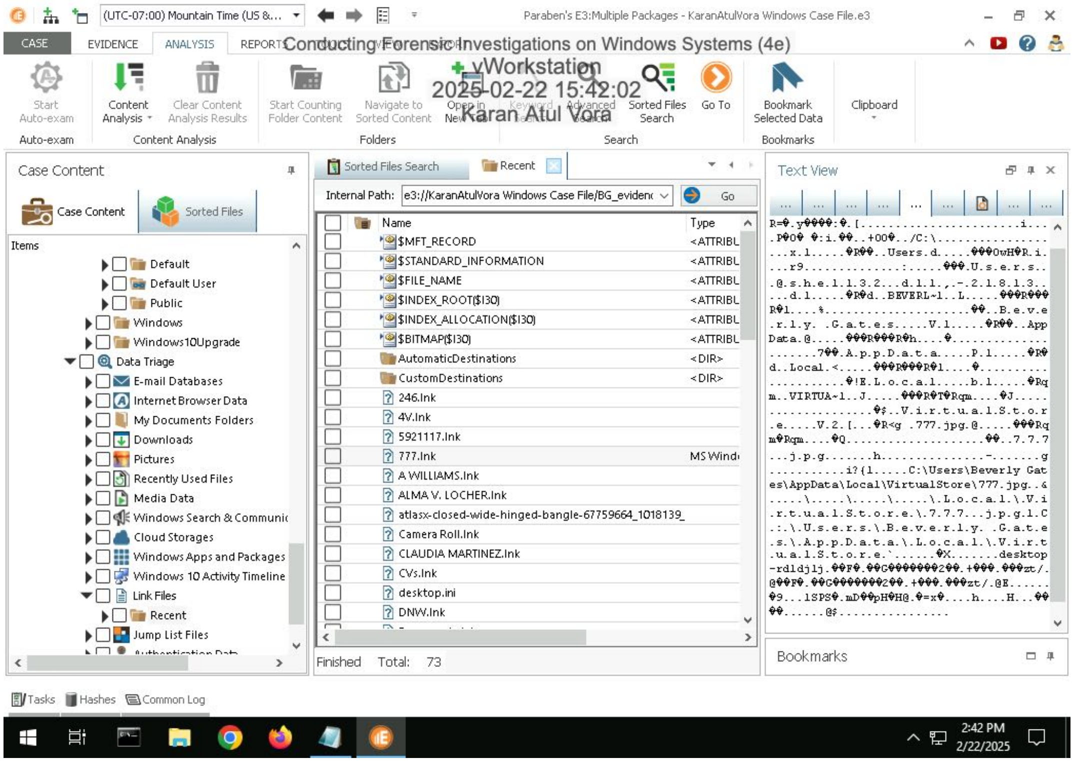
Name	Type
$MFT_RECORD	<ATTRIBUTE>
$STANDARD_INFORMATION	<ATTRIBUTE>
$FILE_NAME	<ATTRIBUTE>
$FILE_NAME	<ATTRIBUTE>
$OBJECT_ID	<ATTRIBUTE>
$INDEX_ROOT($I30)	<ATTRIBUTE>
777.jpg	Zip archive d
tmp.exe.exe	Nullsoft Insta
tmp.exe.exe : com.dropbox.attrs	Unknown fo
tmp.exe.exe : SmartScreen	ASCII text
tmp.exe.exe : Zone.Identifier	ASCII text

File System Attributes	
Archive	True
Compressed	False
Directory	False
Encrypted	False
Hidden	False
No Indexed Content	False
Offline	False
Read only	False
Reparse Point	False
Sparse file	False
System	False
Namespace	
DOS	777.jpg
Namespace	3
Windows	777.jpg
NTFS	

Category: Common

```
firefox_plugin
chrome_plugin
sqlite_plugin
storage_plugin
```

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



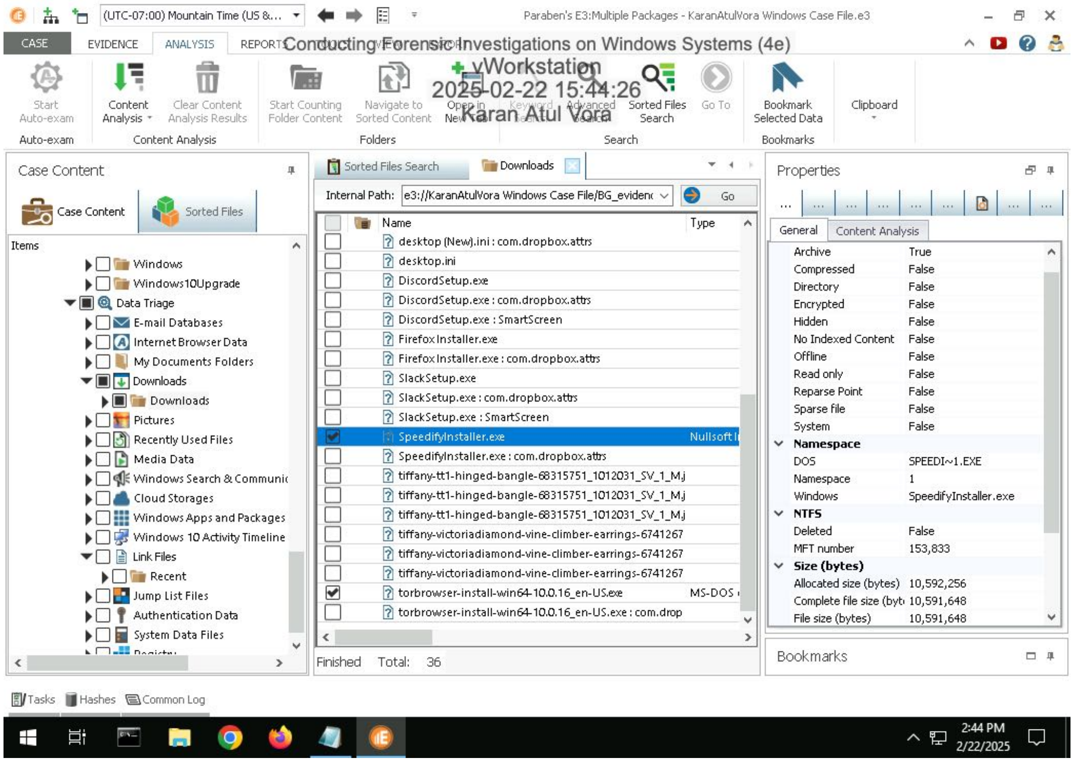
Internal Path: e3://KaranAtulVora Windows Case File/BG_evidenc

Name	Type
$MFT_RECORD	<ATTRIBL
$STANDARD_INFORMATION	<ATTRIBL
$FILE_NAME	<ATTRIBL
$INDEX_ROOT($I30)	<ATTRIBL
$INDEX_ALLOCATION($I30)	<ATTRIBL
$BITMAP($I30)	<ATTRIBL
AutomaticDestinations	<DIR>
CustomDestinations	<DIR>
246.lnk	
4V.lnk	
5921117.lnk	
777.lnk	MS Wind
A WILLIAMS.lnk	
ALMA V. LOCHER.lnk	
atlasx-closed-wide-hinged-bangle-67759664_1018139_	
Camera Roll.lnk	
CLAUDIA MARTINEZ.lnk	
CVs.lnk	
desktop.ini	
DNW.lnk	

Finished Total: 73

```
R=�.y����:�.[.......................i...
.P�O� �:i.��..+OO�../C:\................
...x.l.....�R��..Users.d.....���OwH�R.i.
...r9..............:.....���.U.s.e.r.s..
.@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3..
...d.l.....�R�d..BEVERL~1..L.....���R���
R�l....%.....................��..B.e.v.e
.r.l.y. .G.a.t.e.s.....V.1.....�R��..App
Data.@.....���R���R�h....�..............
.......7��.A.p.p.D.a.t.a.....P.l.....�R�
d..Local.<.....���R���R�l....�..........
...........�!E.L.o.c.a.l.....b.l.....�Rq
m..VIRTUA~1..J.....���R�T�Rqm....�J.....
...............�$..V.i.r.t.u.a.l.S.t.o.r
.e.....V.2.[...�R<g .777.jpg.@.....���Rq
m�Rqm....�Q....................��..7.7.7
...j.p.g.......h...................-.......g
...........i?{l.....C:\Users\Beverly Gat
es\AppData\Local\VirtualStore\777.jpg..&
.....\.....\.....\.....\.L.o.c.a.l.\.V.i
.r.t.u.a.l.S.t.o.r.e.\.7.7.7...j.p.g.l.C
.:.\.U.s.e.r.s.\.B.e.v.e.r.l.y. .G.a.t.e
.s.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.V.i.r.t
.u.a.l.S.t.o.r.e.`......�X.......desktop
-rdldjlj.��F�.��G�������Z��.+���.���zt/.
@��F�.��G�������Z��.+���.���zt/.@E.....
�9...1SPS�.mD��pH�H@.�=x�....h....H...��
��......@$................
```

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



Conducting Forensic Investigations on Windows Systems (4e)
vWorkstation
2025-02-22 15:44:26
Karan Atul Vora

Internal Path: e3://KaranAtulVora Windows Case File/BG_evidenc

	Name	Type
□	desktop (New).ini : com.dropbox.attrs	
□	desktop.ini	
□	DiscordSetup.exe	
□	DiscordSetup.exe : com.dropbox.attrs	
□	DiscordSetup.exe : SmartScreen	
□	Firefox Installer.exe	
□	Firefox Installer.exe : com.dropbox.attrs	
□	SlackSetup.exe	
□	SlackSetup.exe : com.dropbox.attrs	
□	SlackSetup.exe : SmartScreen	
☑	SpeedifyInstaller.exe	Nullsoft I
□	SpeedifyInstaller.exe : com.dropbox.attrs	
□	tiffany-tt1-hinged-bangle-68315751_1012031_SV_1_M.j	
□	tiffany-tt1-hinged-bangle-68315751_1012031_SV_1_M.j	
□	tiffany-tt1-hinged-bangle-68315751_1012031_SV_1_M.j	
□	tiffany-victoriadiamond-vine-climber-earrings-6741267	
□	tiffany-victoriadiamond-vine-climber-earrings-6741267	
□	tiffany-victoriadiamond-vine-climber-earrings-6741267	
☑	torbrowser-install-win64-10.0.16_en-US.exe	MS-DOS
□	torbrowser-install-win64-10.0.16_en-US.exe : com.drop	

Finished Total: 36

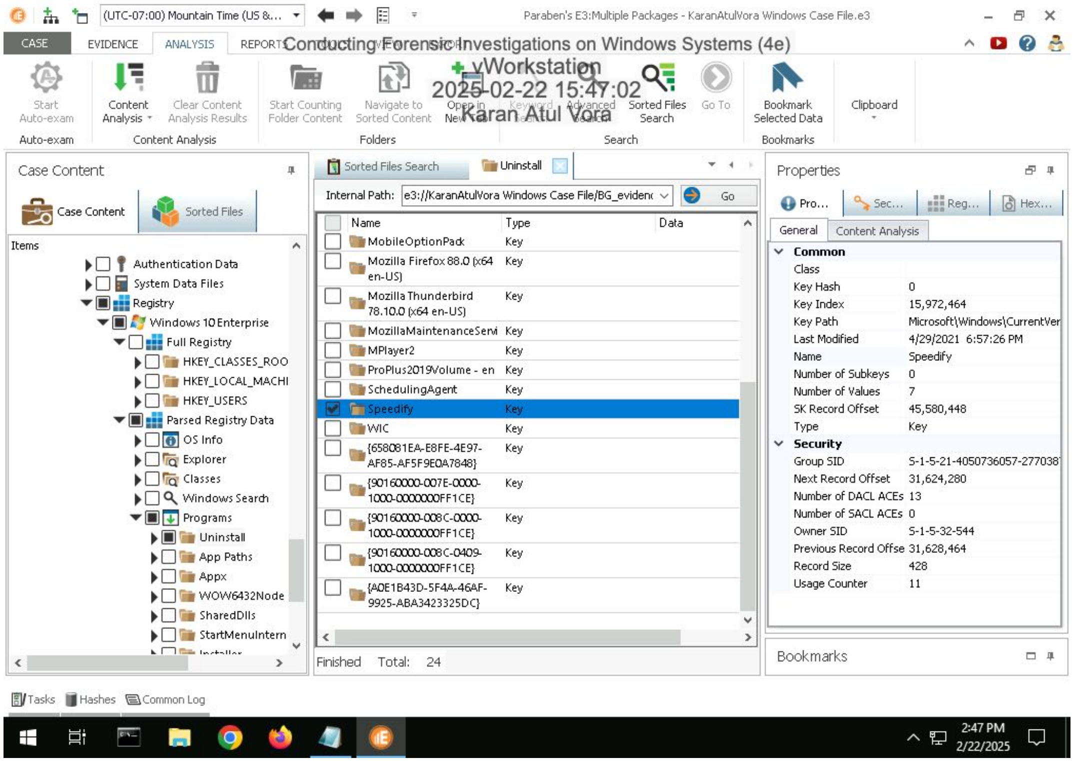
Properties

General | Content Analysis

Archive	True
Compressed	False
Directory	False
Encrypted	False
Hidden	False
No Indexed Content	False
Offline	False
Read only	False
Reparse Point	False
Sparse file	False
System	False
Namespace	
DOS	SPEEDI~1.EXE
Namespace	1
Windows	SpeedifyInstaller.exe
NTFS	
Deleted	False
MFT number	153,833
Size (bytes)	
Allocated size (bytes)	10,592,256
Complete file size (byt	10,591,648
File size (bytes)	10,591,648

Bookmarks

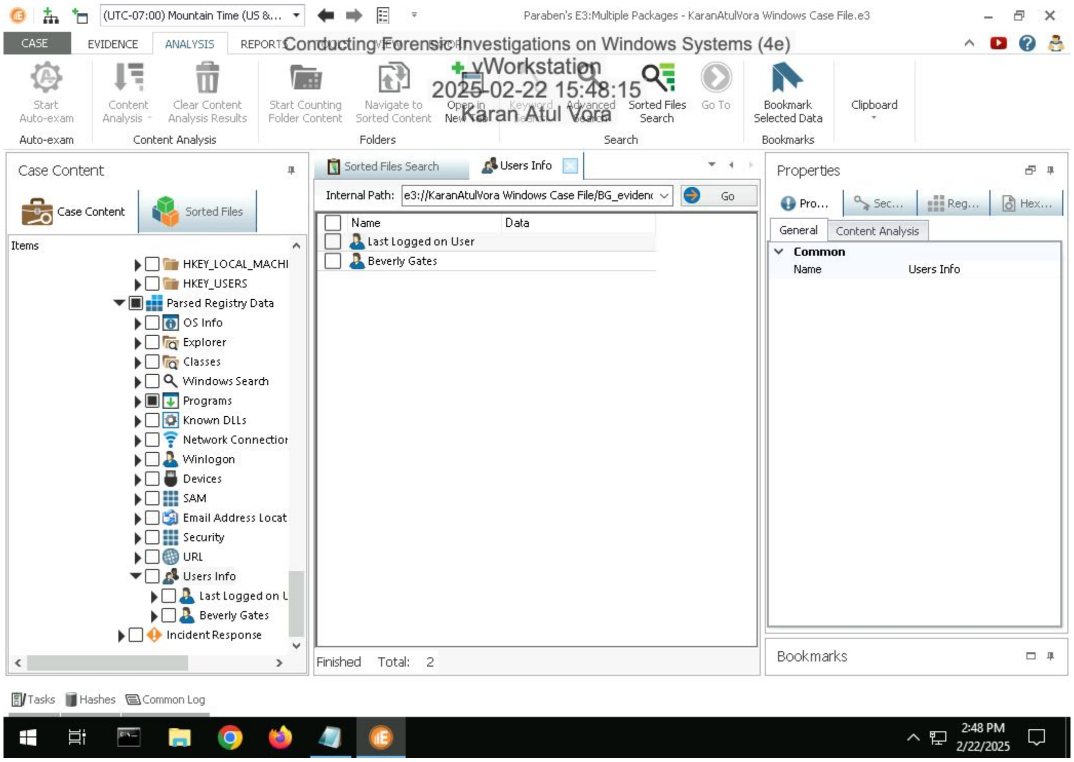
17. **Make a screen capture** showing the **VPN application (Speedify) in the Uninstall folder**.



Name	Type	Data
MobileOptionPack	Key	
Mozilla Firefox 88.0 (x64 en-US)	Key	
Mozilla Thunderbird 78.10.0 (x64 en-US)	Key	
MozillaMaintenanceServi	Key	
MPlayer2	Key	
ProPlus2019Volume - en	Key	
SchedulingAgent	Key	
☑ Speedify	Key	
WIC	Key	
{658081EA-E8FE-4E97-AF85-AF5F9E0A7848}	Key	
{90160000-007E-0000-1000-0000000FF1CE}	Key	
{90160000-008C-0000-1000-0000000FF1CE}	Key	
{90160000-008C-0409-1000-0000000FF1CE}	Key	
{A0E1B43D-5F4A-46AF-9925-ABA3423325DC}	Key	

Common	
Class	
Key Hash	0
Key Index	15,972,464
Key Path	Microsoft\Windows\CurrentVer
Last Modified	4/29/2021 6:57:26 PM
Name	Speedify
Number of Subkeys	0
Number of Values	7
SK Record Offset	45,580,448
Type	Key
Security	
Group SID	S-1-5-21-4050736057-277038
Next Record Offset	31,624,280
Number of DACL ACEs	13
Number of SACL ACEs	0
Owner SID	S-1-5-32-544
Previous Record Offse	31,628,464
Record Size	428
Usage Counter	11

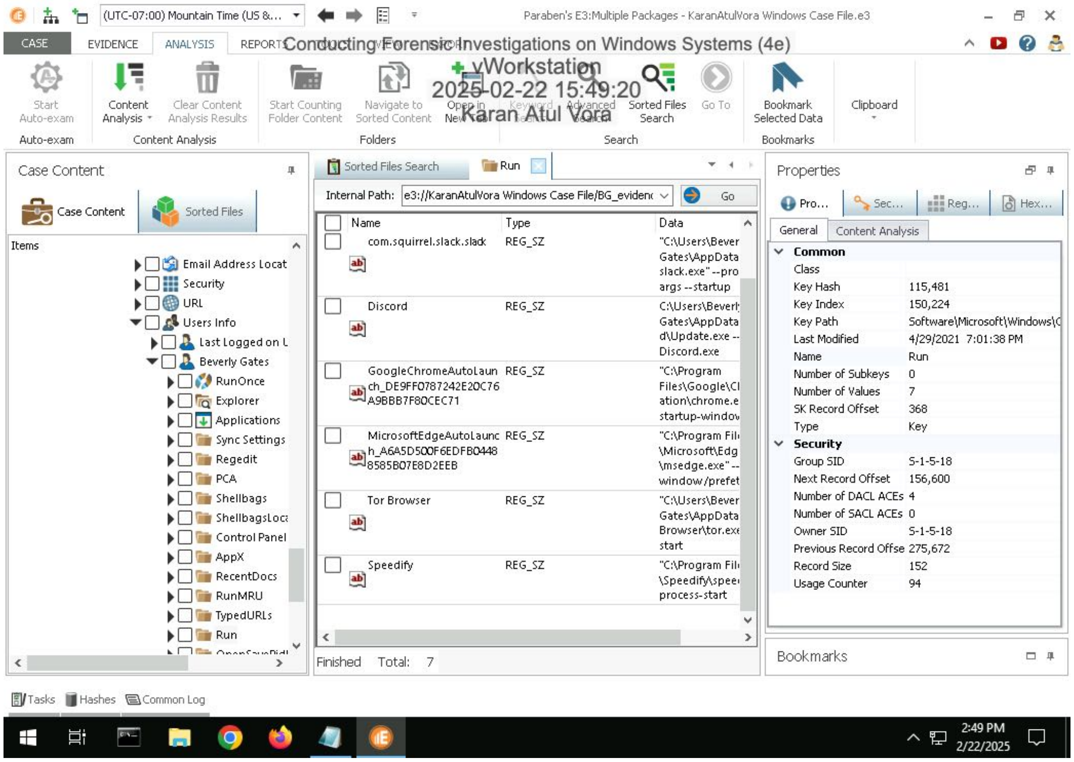
19. **Make a screen capture** showing the **users list**.



Name	Data
Last Logged on User	
Beverly Gates	

Common	
Name	Users Info

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



Conducting Forensic Investigations on Windows Systems (4e)
vWorkstation
2025-02-22 15:49:20
Karan Atul Vora

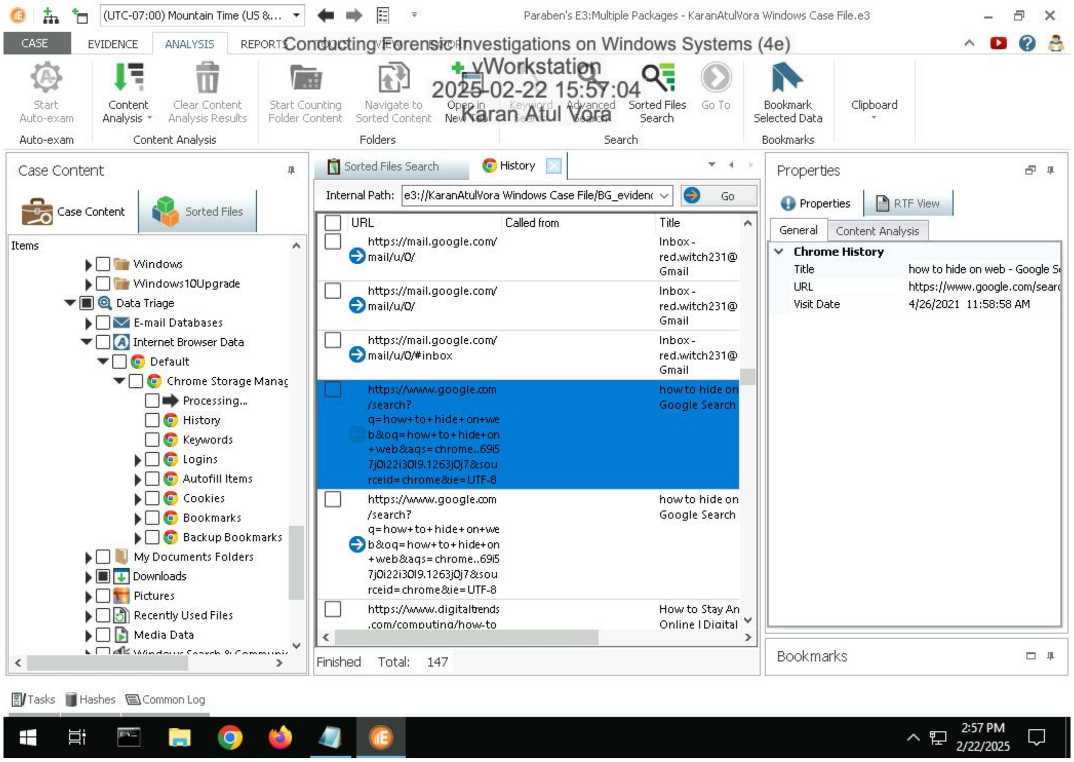
Internal Path: e3://KaranAtulVora Windows Case File/BG_evidenc

Name	Type	Data
com.squirrel.slack.slack	REG_SZ	"C:\Users\Bever Gates\AppData slack.exe" --pro args --startup
Discord	REG_SZ	C:\Users\Beverl Gates\AppData d\Update.exe -- Discord.exe
GoogleChromeAutoLaunch_DE9FF0787242E20C76A9BBB7F80CEC71	REG_SZ	"C:\Program Files\Google\Cl ation\chrome.e startup-window
MicrosoftEdgeAutoLaunch_A6A5D500F6EDFB04488585B07E8D2EEB	REG_SZ	"C:\Program Fil \Microsoft\Edg \msedge.exe" -- window/prefet
Tor Browser	REG_SZ	"C:\Users\Bever Gates\AppData Browser\tor.exe start
Speedify	REG_SZ	"C:\Program Fil \Speedify\spee process-start

Finished Total: 7

Common	
Class	
Key Hash	115,481
Key Index	150,224
Key Path	Software\Microsoft\Windows\C
Last Modified	4/29/2021 7:01:38 PM
Name	Run
Number of Subkeys	0
Number of Values	7
SK Record Offset	368
Type	Key
Security	
Group SID	S-1-5-18
Next Record Offset	156,600
Number of DACL ACEs	4
Number of SACL ACEs	0
Owner SID	S-1-5-18
Previous Record Offse	275,672
Record Size	152
Usage Counter	94

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)
vWorkstation
2025-02-22 15:57:04
Karan Atul Vora

Internal Path: e3://KaranAtulVora Windows Case File/BG_evidenc

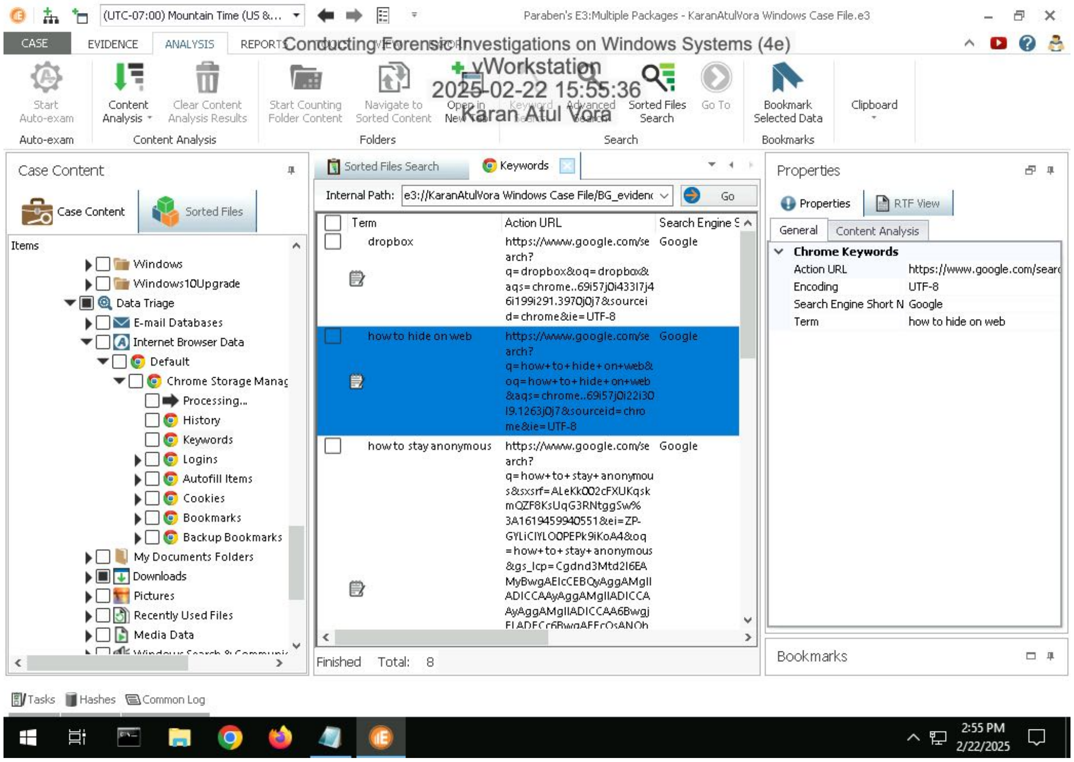
URL	Called from	Title
https://mail.google.com/mail/u/0/		Inbox - red.witch231@Gmail
https://mail.google.com/mail/u/0/		Inbox - red.witch231@Gmail
https://mail.google.com/mail/u/0/#inbox		Inbox - red.witch231@Gmail
https://www.google.com/search?q=how+to+hide+on+web&oq=how+to+hide+on+web&aqs=chrome..69i57j0i22i30l9.1263j0j7&sourceid=chrome&ie=UTF-8		how to hide on Google Search
https://www.google.com/search?q=how+to+hide+on+web&oq=how+to+hide+on+web&aqs=chrome..69i57j0i22i30l9.1263j0j7&sourceid=chrome&ie=UTF-8		how to hide on Google Search
https://www.digitaltrends.com/computing/how-to		How to Stay An Online	Digital

Finished Total: 147

Chrome History

Title	how to hide on web - Google S
URL	https://www.google.com/searc
Visit Date	4/26/2021 11:58:58 AM

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



Internal Path: e3://KaranAtulVora Windows Case File/BG_eviden

Term	Action URL	Search Engine S
dropbox	https://www.google.com/search?q=dropbox&oq=dropbox&aqs=chrome..69i57j0i433l7j46i199i291.3970j0j7&sourceid=chrome&ie=UTF-8	Google
how to hide on web	https://www.google.com/search?q=how+to+hide+on+web&oq=how+to+hide+on+web&aqs=chrome..69i57j0i22i30l9.1263j0j7&sourceid=chrome&ie=UTF-8	Google
how to stay anonymous	https://www.google.com/search?q=how+to+stay+anonymous&sxsrf=ALeKk002cFXUKqskmQZF8KsUqG3RNtggSw%3A1619459940551&ei=ZP-GYLiCIYLOOPEPk9iKoA4&oq=how+to+stay+anonymous&gs_lcp=Cgdnd3Mtd2l6EAMyBwgAEIcCEBQyAggAMgIIADICCAAyAggAMgIIADICCAAyAggAMgIIADICCAA6BwgjELADECc6BwgAEEcQsANQh	Google

Finished Total: 8

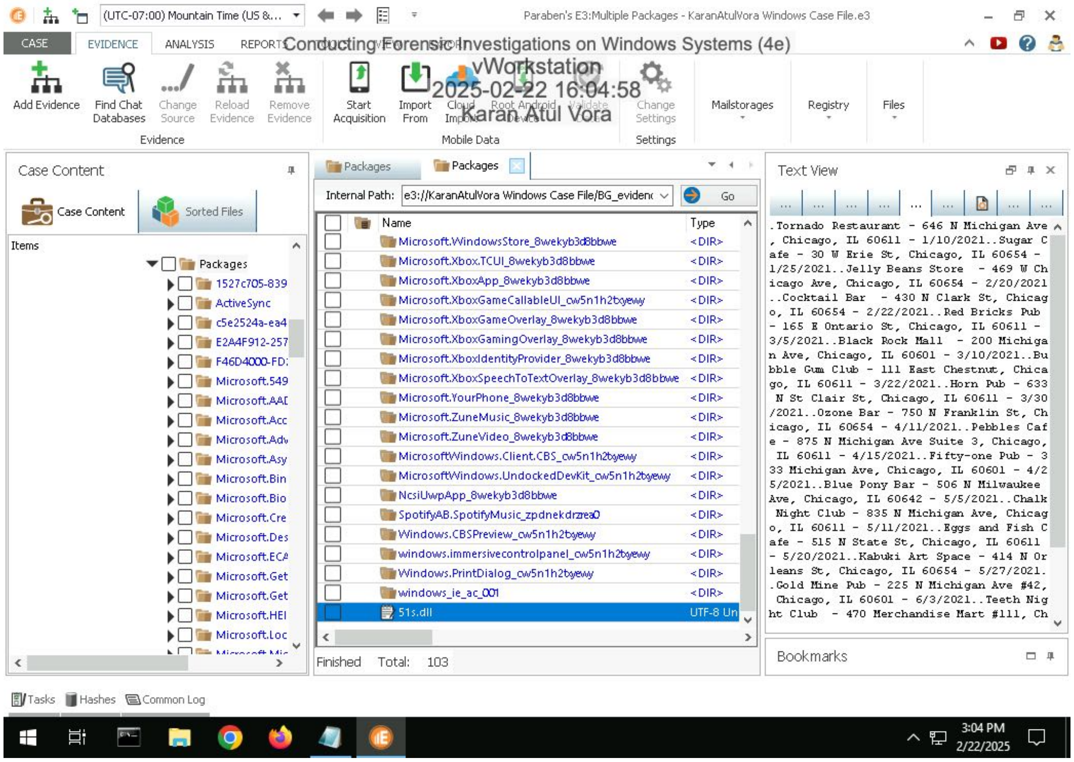
Chrome Keywords

Action URL	https://www.google.com/searc
Encoding	UTF-8
Search Engine Short N	Google
Term	how to hide on web

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**.

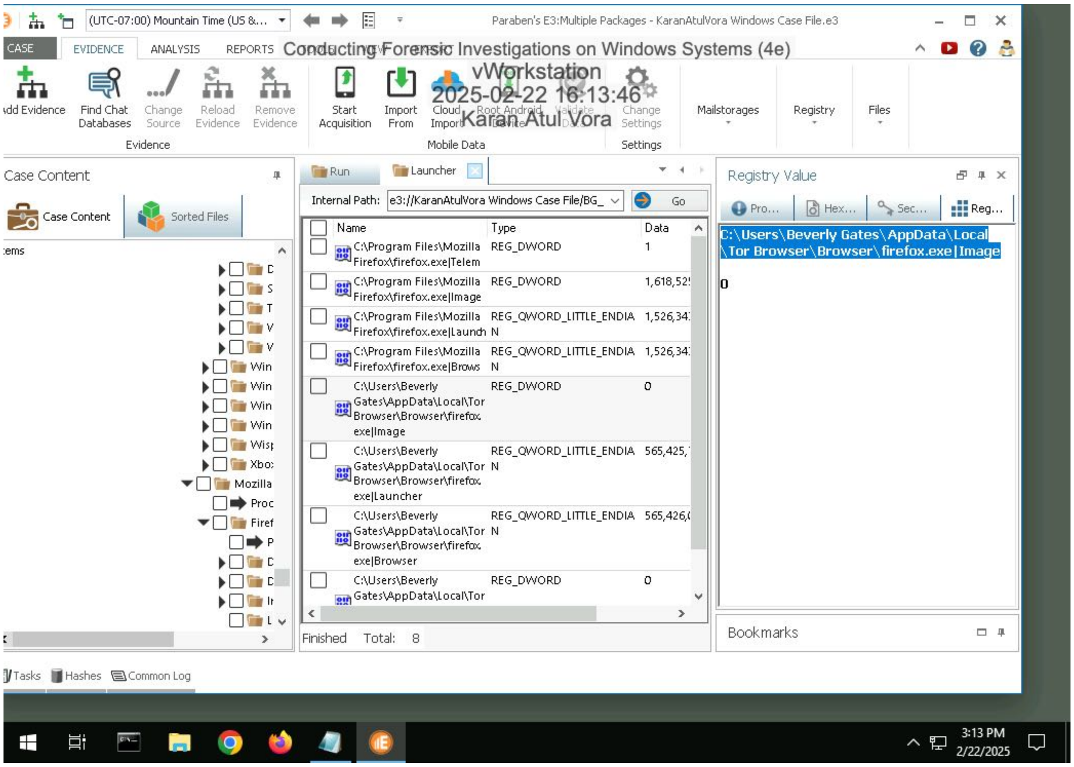


Name	Type
Microsoft.WindowsStore_8wekyb3d8bbwe	<DIR>
Microsoft.Xbox.TCUI_8wekyb3d8bbwe	<DIR>
Microsoft.XboxApp_8wekyb3d8bbwe	<DIR>
Microsoft.XboxGameCallableUI_cw5n1h2txyewy	<DIR>
Microsoft.XboxGameOverlay_8wekyb3d8bbwe	<DIR>
Microsoft.XboxGamingOverlay_8wekyb3d8bbwe	<DIR>
Microsoft.XboxIdentityProvider_8wekyb3d8bbwe	<DIR>
Microsoft.XboxSpeechToTextOverlay_8wekyb3d8bbwe	<DIR>
Microsoft.YourPhone_8wekyb3d8bbwe	<DIR>
Microsoft.ZuneMusic_8wekyb3d8bbwe	<DIR>
Microsoft.ZuneVideo_8wekyb3d8bbwe	<DIR>
MicrosoftWindows.Client.CBS_cw5n1h2txyewy	<DIR>
MicrosoftWindows.UndockedDevKit_cw5n1h2txyewy	<DIR>
NcsiUwpApp_8wekyb3d8bbwe	<DIR>
SpotifyAB.SpotifyMusic_zpdnekdrzrea0	<DIR>
Windows.CBSPreview_cw5n1h2txyewy	<DIR>
windows.immersivecontrolpanel_cw5n1h2txyewy	<DIR>
Windows.PrintDialog_cw5n1h2txyewy	<DIR>
windows_ie_ac_001	<DIR>
51s.dll	UTF-8 Un

```
.Tornado Restaurant - 646 N Michigan Ave
, Chicago, IL 60611 - 1/10/2021..Sugar C
afe - 30 W Erie St, Chicago, IL 60654 -
1/25/2021..Jelly Beans Store  - 469 W Ch
icago Ave, Chicago, IL 60654 - 2/20/2021
..Cocktail Bar  - 430 N Clark St, Chicag
o, IL 60654 - 2/22/2021..Red Bricks Pub
- 165 E Ontario St, Chicago, IL 60611 -
3/5/2021..Black Rock Mall  - 200 Michiga
n Ave, Chicago, IL 60601 - 3/10/2021..Bu
bble Gum Club - 111 East Chestnut, Chica
go, IL 60611 - 3/22/2021..Horn Pub - 633
 N St Clair St, Chicago, IL 60611 - 3/30
/2021..Ozone Bar - 750 N Franklin St, Ch
icago, IL 60654 - 4/11/2021..Pebbles Caf
e - 875 N Michigan Ave Suite 3, Chicago,
 IL 60611 - 4/15/2021..Fifty-one Pub - 3
33 Michigan Ave, Chicago, IL 60601 - 4/2
5/2021..Blue Pony Bar - 506 N Milwaukee
Ave, Chicago, IL 60642 - 5/5/2021..Chalk
 Night Club - 835 N Michigan Ave, Chicag
o, IL 60611 - 5/11/2021..Eggs and Fish C
afe - 515 N State St, Chicago, IL 60611
- 5/20/2021..Kabuki Art Space - 414 N Or
leans St, Chicago, IL 60654 - 5/27/2021.
.Gold Mine Pub - 225 N Michigan Ave #42,
 Chicago, IL 60601 - 6/3/2021..Teeth Nig
ht Club  - 470 Merchandise Mart #111, Ch
```

Part 2: Identify Suspicious Browser Activity

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



Internal Path: e3://KaranAtulVora Windows Case File/BG_

Name	Type	Data
C:\Program Files\Mozilla Firefox\firefox.exe|Telem	REG_DWORD	1
C:\Program Files\Mozilla Firefox\firefox.exe|Image	REG_DWORD	1,618,52
C:\Program Files\Mozilla Firefox\firefox.exe|Launch	REG_QWORD_LITTLE_ENDIAN	1,526,34
C:\Program Files\Mozilla Firefox\firefox.exe|Brows	REG_QWORD_LITTLE_ENDIAN	1,526,34
C:\Users\Beverly Gates\AppData\Local\Tor Browser\Browser\firefox.exe|Image	REG_DWORD	0
C:\Users\Beverly Gates\AppData\Local\Tor Browser\Browser\firefox.exe|Launcher	REG_QWORD_LITTLE_ENDIAN	565,425,
C:\Users\Beverly Gates\AppData\Local\Tor Browser\Browser\firefox.exe|Browser	REG_QWORD_LITTLE_ENDIAN	565,426,
C:\Users\Beverly Gates\AppData\Local\Tor	REG_DWORD	0

Finished Total: 8

C:\Users\Beverly Gates\AppData\Local\Tor Browser\Browser\firefox.exe|Image

0