Conducting Forensic Investigations on Windows Systems (4e)

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

Student:	Email:
Loksharan Saravanan	loksharan.soc@gmail.com

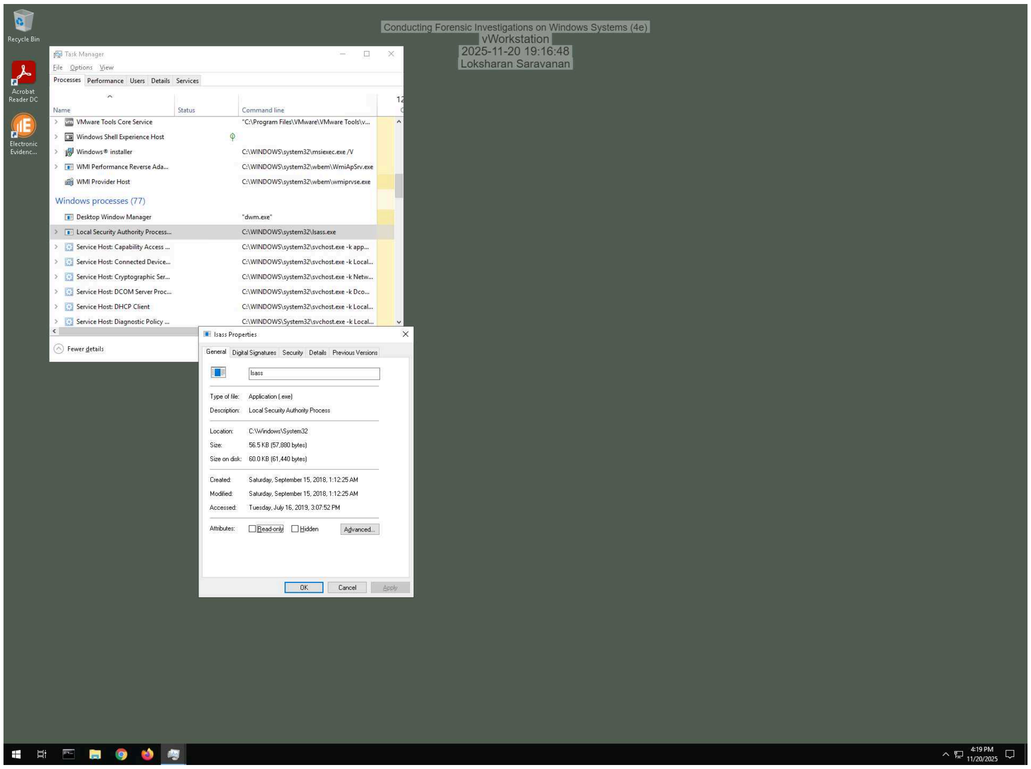
Time on Task:	Progress:
2 hours, 8 minutes	100%

Report Generated: Friday, November 21, 2025 at 2:04 AM

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
2025-11-20 19:16:48
Loksharan Saravanan

Task Manager

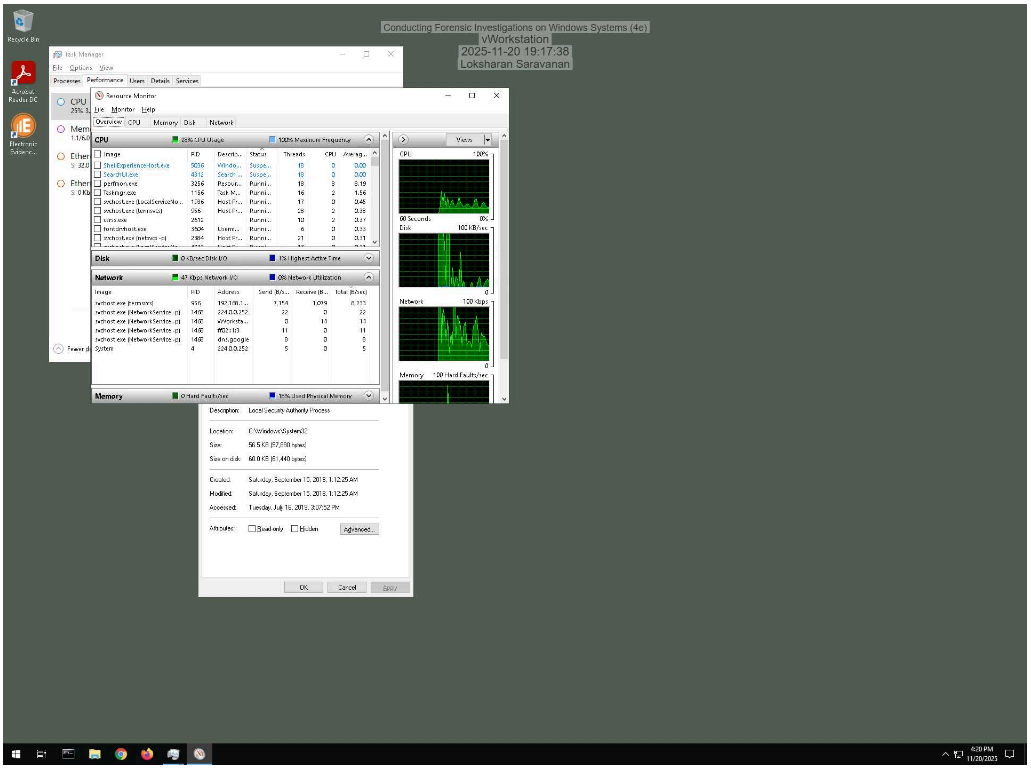
Name	Status	Command line
VMware Tools Core Service		"C:\Program Files\VMware\VMware Tools\v...
Windows Shell Experience Host		
Windows® installer		C:\WINDOWS\system32\msiexec.exe /V
WMI Performance Reverse Ada...		C:\WINDOWS\system32\wbem\WmiApSrv.exe
WMI Provider Host		C:\WINDOWS\system32\wbem\wmiprvse.exe
Windows processes (77)		
Desktop Window Manager		"dwm.exe"
Local Security Authority Process...		C:\WINDOWS\system32\lsass.exe
Service Host: Capability Access ...		C:\WINDOWS\system32\svchost.exe -k app...
Service Host: Connected Device...		C:\WINDOWS\system32\svchost.exe -k Local...
Service Host: Cryptographic Ser...		C:\WINDOWS\system32\svchost.exe -k Netw...
Service Host: DCOM Server Proc...		C:\WINDOWS\system32\svchost.exe -k Dco...
Service Host: DHCP Client		C:\WINDOWS\system32\svchost.exe -k Local...
Service Host: Diagnostic Policy ...		C:\WINDOWS\System32\svchost.exe -k Local...

lsass Properties

lsass

Type of file: Application (.exe)
Description: Local Security Authority Process
Location: C:\Windows\System32
Size: 56.5 KB (57,880 bytes)
Size on disk: 60.0 KB (61,440 bytes)
Created: Saturday, September 15, 2018, 1:12:25 AM
Modified: Saturday, September 15, 2018, 1:12:25 AM
Accessed: Tuesday, July 16, 2019, 3:07:52 PM
Attributes: ☐ Read-only ☐ Hidden

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



CPU 28% CPU Usage 100% Maximum Frequency

Image	PID	Descrip...	Status	Threads	CPU	Averag...
ShellExperienceHost.exe	5036	Windo...	Suspe...	18	0	0.00
SearchUI.exe	4312	Search ...	Suspe...	18	0	0.00
perfmon.exe	3256	Resour...	Runni...	18	8	8.19
Taskmgr.exe	1156	Task M...	Runni...	16	2	1.56
svchost.exe (LocalServiceNo...	1936	Host Pr...	Runni...	17	0	0.45
svchost.exe (termsvcs)	956	Host Pr...	Runni...	28	2	0.38
csrss.exe	2612		Runni...	10	2	0.37
fontdrvhost.exe	3604	Userm...	Runni...	6	0	0.33
svchost.exe (netsvcs -p)	2384	Host Pr...	Runni...	21	0	0.31

Disk 0 KB/sec Disk I/O 1% Highest Active Time

Network 47 Kbps Network I/O 0% Network Utilization

Image	PID	Address	Send (B/s...	Receive (B...	Total (B/sec)
svchost.exe (termsvcs)	956	192.168.1...	7,154	1,079	8,233
svchost.exe (NetworkService -p)	1468	224.0.0.252	22	0	22
svchost.exe (NetworkService -p)	1468	vWorksta...	0	14	14
svchost.exe (NetworkService -p)	1468	ff02::1:3	11	0	11
svchost.exe (NetworkService -p)	1468	dns.google	8	0	8
System	4	224.0.0.252	5	0	5

Memory 0 Hard Faults/sec 18% Used Physical Memory

Description: Local Security Authority Process

Location: C:\Windows\System32

Size: 56.5 KB (57,880 bytes)

Size on disk: 60.0 KB (61,440 bytes)

Created: Saturday, September 15, 2018, 1:12:25 AM

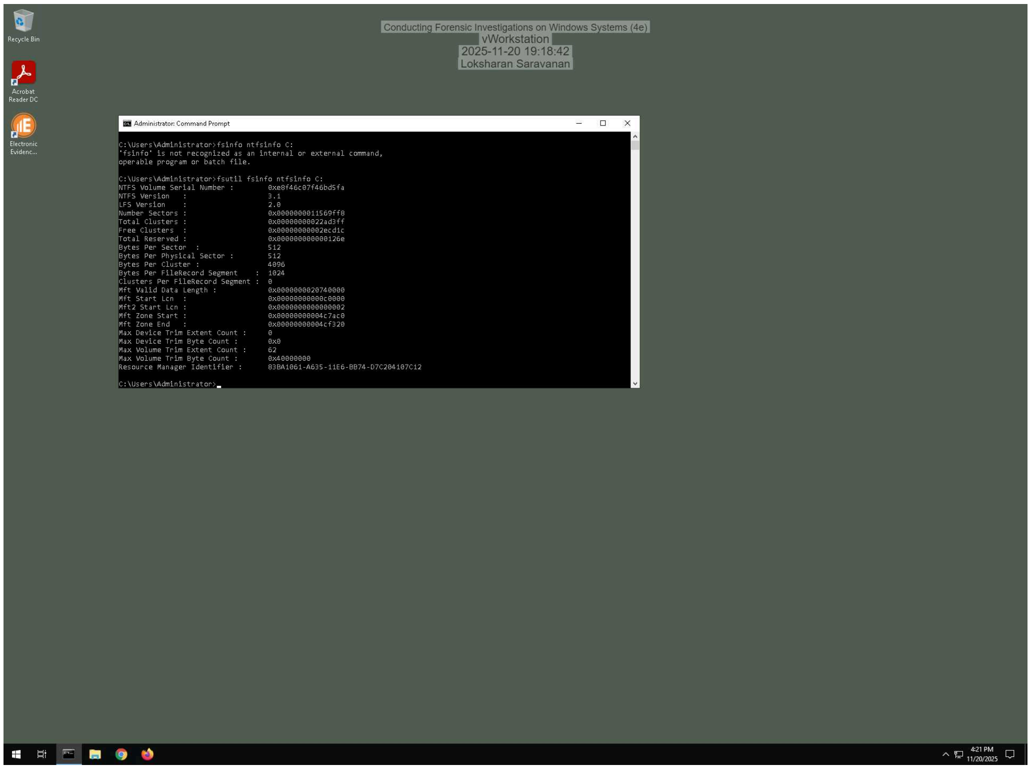
Modified: Saturday, September 15, 2018, 1:12:25 AM

Accessed: Tuesday, July 16, 2019, 3:07:52 PM

Attributes: □ Read-only □ Hidden Advanced...

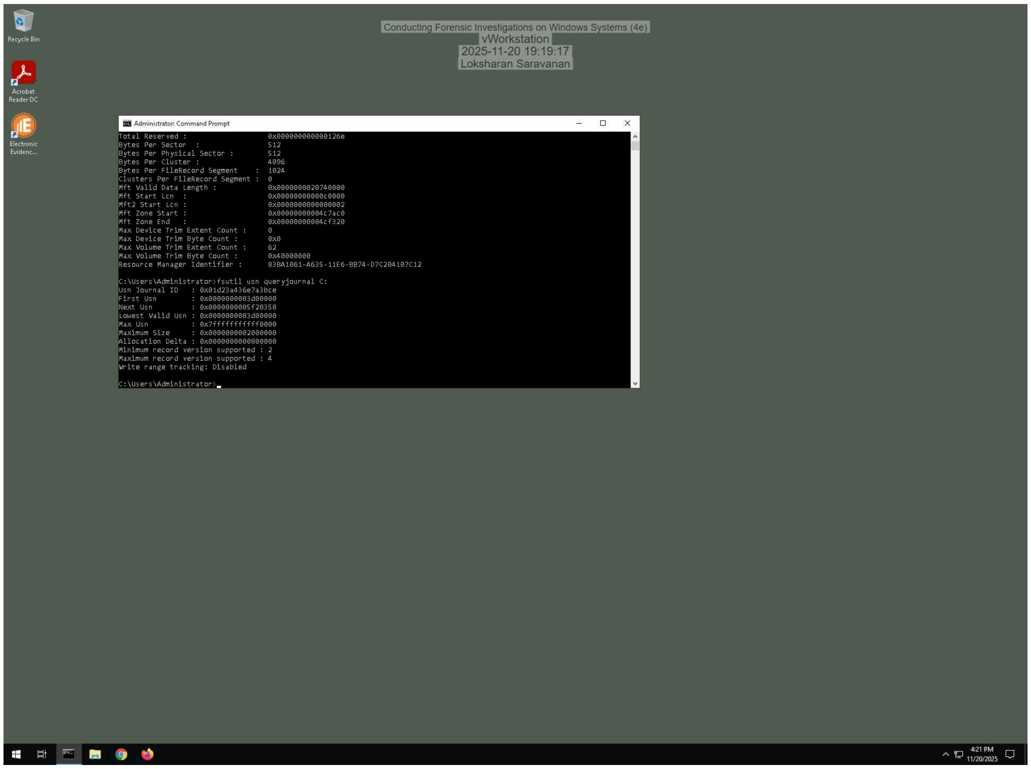
OK Cancel Apply

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



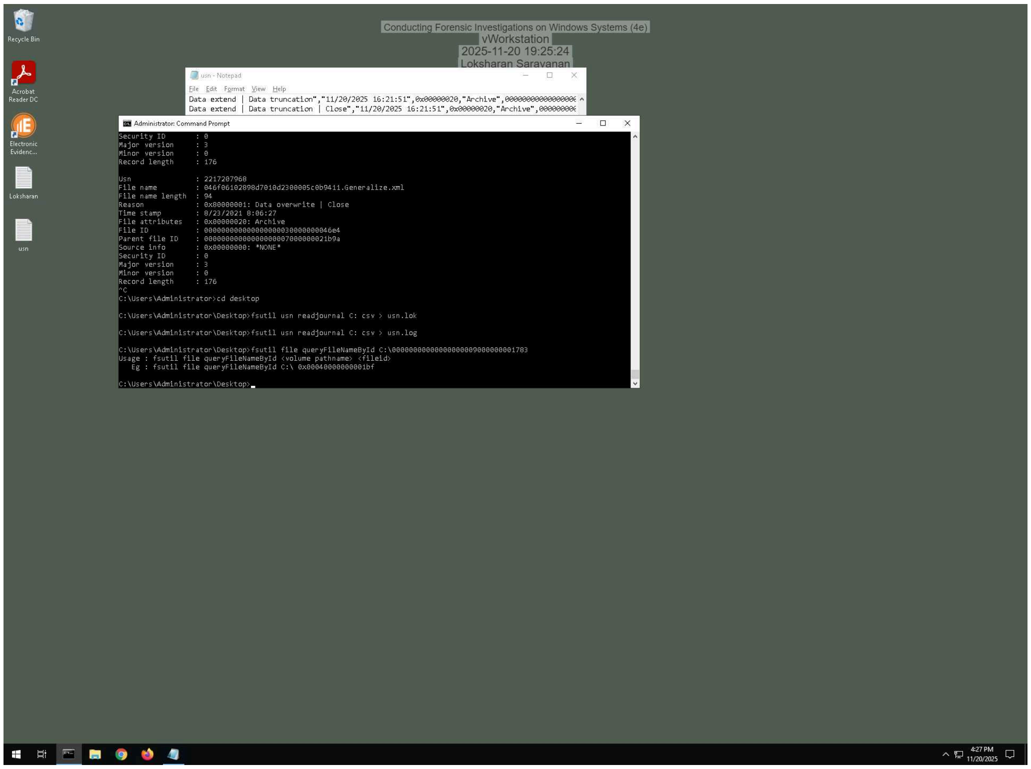
```
C:\Users\Administrator>fsinfo ntfsinfo C:
'fsinfo' is not recognized as an internal or external command,
operable program or batch file.

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  :                   0x00000000002ecd1c
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**.



```
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>fsutil usn queryjournal C:
Usn Journal ID   : 0x01d23a436e7a3bce
First Usn        : 0x0000000083d00000
Next Usn         : 0x0000000085f28358
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**.

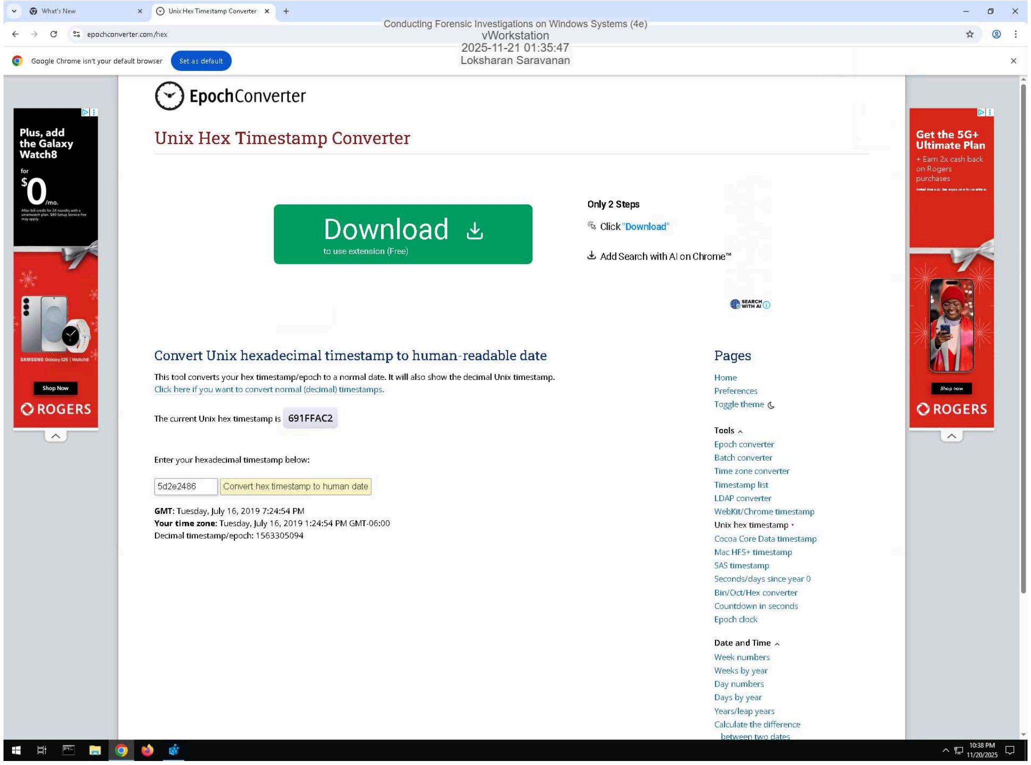


```
Data extend | Data truncation","11/20/2025 16:21:51",0x00000020,"Archive",0000000000000000
Data extend | Data truncation | Close","11/20/2025 16:21:51",0x00000020,"Archive",00000000
```

```
Security ID      : 0
Major version    : 3
Minor version    : 0
Record length    : 176

Usn              : 2217207968
File name        : 046f06102898d7010d2300005c0b9411.Generalize.xml
File name length : 94
Reason           : 0x80000001: Data overwrite | Close
Time stamp       : 8/23/2021 8:06:27
File attributes  : 0x00000020: Archive
File ID          : 000000000000000000030000000046e4
Parent file ID   : 00000000000000000007000000021b9a
Source info      : 0x00000000: *NONE*
Security ID      : 0
Major version    : 3
Minor version    : 0
Record length    : 176
^C
C:\Users\Administrator>cd desktop

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

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

C:\Users\Administrator\Desktop>fsutil file queryFileNameById C:\00000000000000000009000000001783
Usage : fsutil file queryFileNameById <volume pathname> <fileid>
   Eg : fsutil file queryFileNameById C:\ 0x00040000000001bf

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**.



Conducting Forensic Investigations on Windows Systems (4e)
vWorkstation
2025-11-21 01:35:47
Loksharan Saravanan

Unix Hex Timestamp Converter

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.

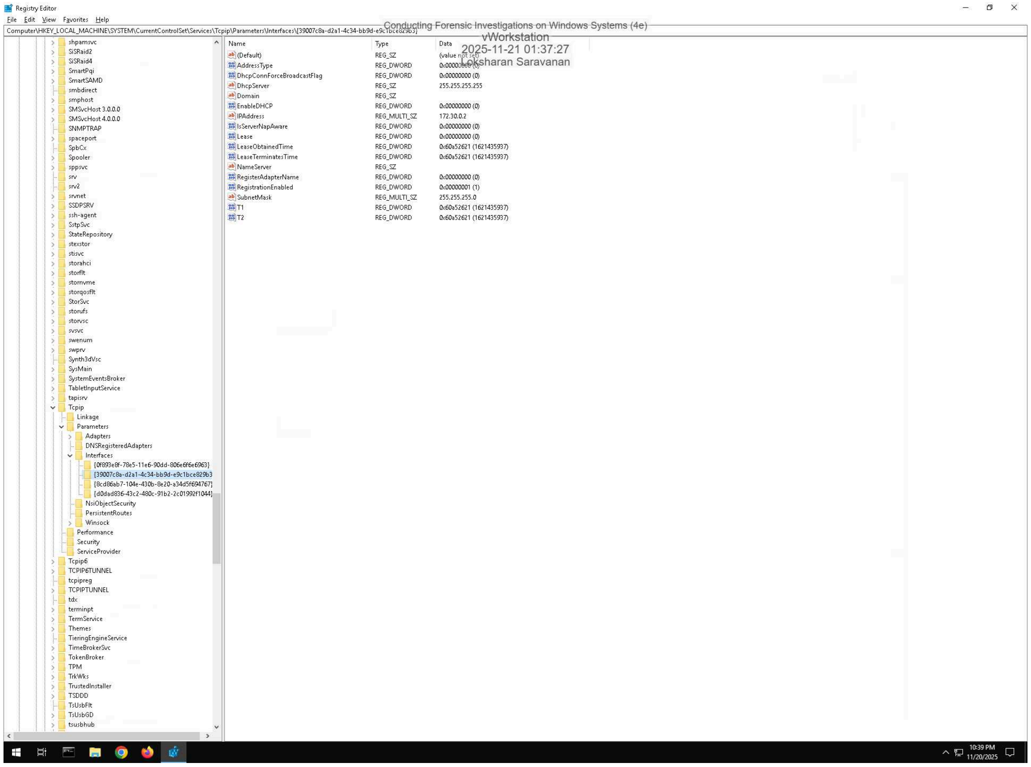
The current Unix hex timestamp is 691FFAC2

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**.

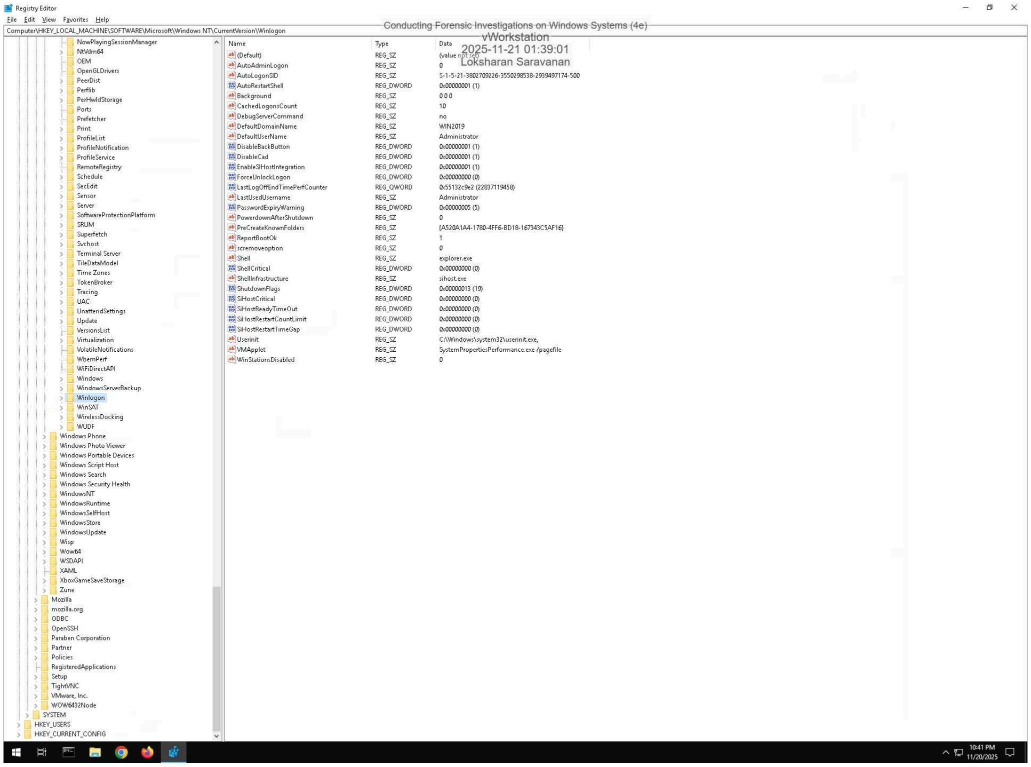


Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{39007c8a-d2a1-4c34-bb9d-e9c1bce829b3}

Conducting Forensic Investigations on Windows Systems (4e)
vWorkstation
2025-11-21 01:37:27
Loksharan Saravanan

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**.

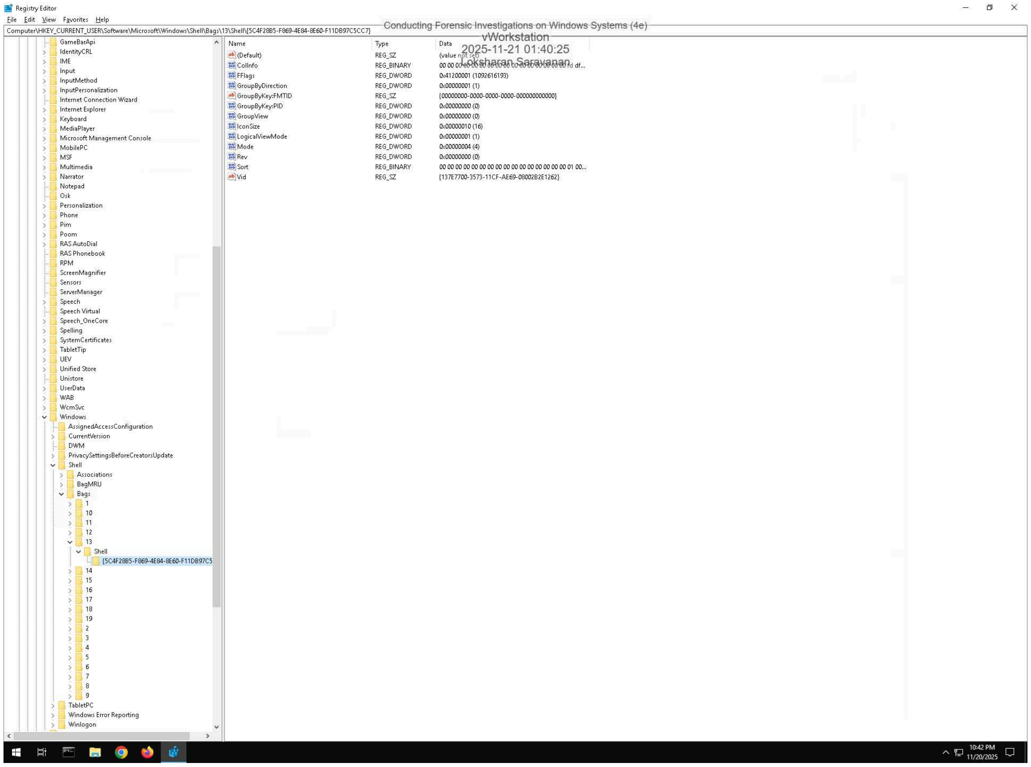


Conducting Forensic Investigations on Windows Systems (4e)
vWorkstation
2025-11-21 01:39:01
Loksharan Saravanan

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	0x55132c9e2 (22837119458)
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**.

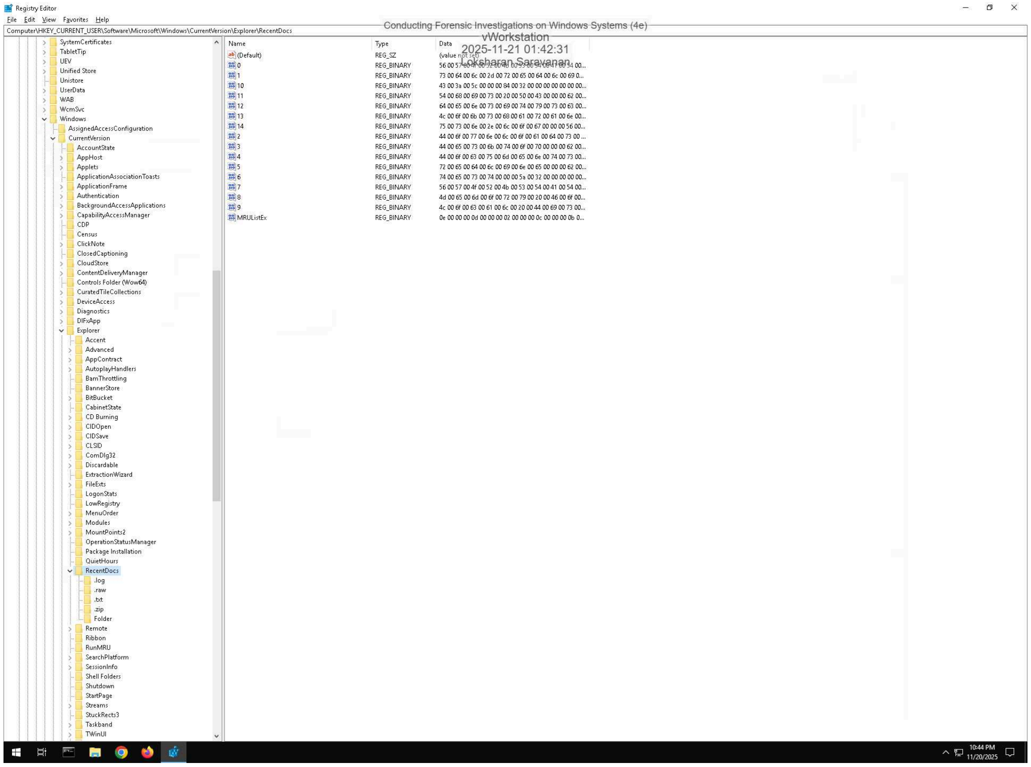


Conducting Forensic Investigations on Windows Systems (4e)
vWorkstation
2025-11-21 01:40:25
Loksharan Saravanan

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags\13\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}

Name	Type	Data
(Default)	REG_SZ	(value not set)
ColInfo	REG_BINARY	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd df...
FFlags	REG_DWORD	0x41200001 (1092616193)
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)
IconSize	REG_DWORD	0x00000010 (16)
LogicalViewMode	REG_DWORD	0x00000001 (1)
Mode	REG_DWORD	0x00000004 (4)
Rev	REG_DWORD	0x00000000 (0)
Sort	REG_BINARY	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00...
Vid	REG_SZ	{137E7700-3573-11CF-AE69-08002B2E1262}

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



Conducting Forensic Investigations on Windows Systems (4e)
vWorkstation
2025-11-21 01:42:31
Loksharan Saravanan

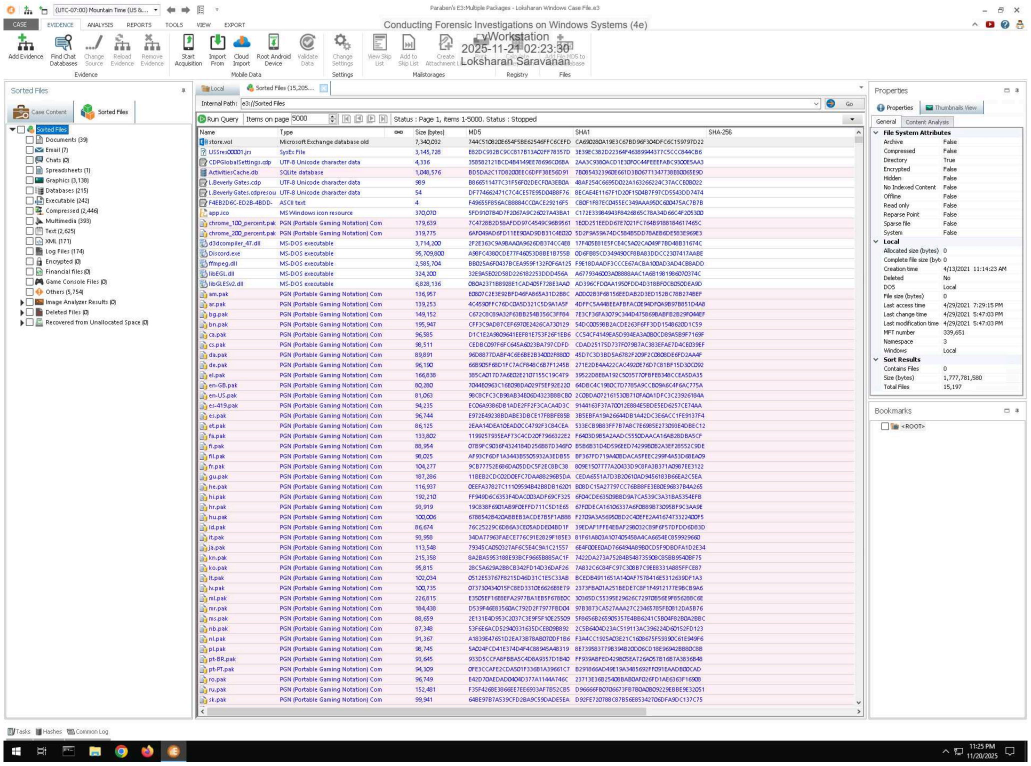
Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

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	4c 00 6f 00 6b 00 73 00 68 00 61 00 72 00 61 00 6e 00...
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	0e 00 00 00 0d 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**.



Conducting Forensic Investigations on Windows Systems (4e)
vWorkstation
2025-11-21 02:23:30
Loksharan Saravanan

Sorted Files

Case Content | Sorted Files

- Sorted Files
  - □ 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)
  - □ Log Files (174)
  - □ Encrypted (0)
  - □ Financial files (0)
  - □ Game Console Files (0)
  - □ Others (5,754)
  - □ Image Analyzer Results (0)
  - □ Deleted Files (0)
  - □ Recovered from Unallocated Space (0)

Local | Sorted Files (15,205...

Internal Path: e3://Sorted Files

Run Query | Items on page 5000 | Status : Page 1, items 1-5000. Status : Stopped

Name	Type	Size (bytes)	MD5	SHA1	SHA-256
store.vol	Microsoft Exchange database old	7,340,032	744C510820E654F5BE62546FFC6CEFD	CA690280A19E3C67BD96F304DFC6C159797D22	
USSres00001.jrs	SysEx File	3,145,728	E82DC932BC9CC817B13A02FF78357D	3E39EC382D22364F46389944377C5CCC844CB6	
CDPGlobalSettings.cdp	UTF-8 Unicode character data	4,336	358582121BCD4B4149EE78696C06BA	2AA3C9380ACD1E30F0C44FEEEFABC9300E5AA3	
ActivitiesCache.db	SQLite database	1,048,576	BD5DA2C17D8200EEC6DFF38E56D91	7B0854323960E661D3B06771347738E80065E9D	
L.Beverly Gates.cdp	UTF-8 Unicode character data	989	B866511477C31F56F02DECF0A3EB0A	48AF254C6695D022A163266224C37ACCE0B022	
L.Beverly Gates.cdpresou	UTF-8 Unicode character data	54	DF774662471C7C4CE57E95D04B8F76	8ECAE4E1167F1D20F1504B7F97CD5543DD7474	
F4EB2D6C-ED2B-4BDD-	ASCII text	4	F49655F856ACB8884CC0ACE29216F5	CB0F1F87EC0455EC349AAA950C600475AC7B7B	
app.ico	MS Windows icon resource	370,070	5FD9107B4D7F2067A9C26027A43BA1	C172E33984943F8426865C78A34D66C4F205300	
chrome_100_percent.pak	PGN (Portable Gaming Notation) Com	179,639	7C4728B2D58AFDD97C4549C96B9561	1E0D251EEDD67E7021FC764B9188184617465C	
chrome_200_percent.pak	PGN (Portable Gaming Notation) Com	319,775	6AF049AD6FD11EE90AD9DB31C4E020	5D2F9A59A74DC584B5DD78AEB6DE583E969E3	
d3dcompiler_47.dll	MS-DOS executable	3,714,200	2F2E363C9A9BAA0A9626DB374CC4E8	17F405E81E5FCE4C5A02CA049F7BD48B31674C	
Discord.exe	MS-DOS executable	95,709,800	A98FC4380CDE77F46053D8BE1B755B	0D6FB85CD349490CF8BA83DDCC2307417AABE	
ffmpeg.dll	MS-DOS executable	2,585,704	BB025A6F0437BCEA959F132F0F6A125	F9E18DAADF3CCCE67ACBA100AD3AD4CB8ADD	
libEGL.dll	MS-DOS executable	324,200	32E9A5E02D58D226182253DDD456A	A6779346003A08888AAC1A6B1981986070374C	
libGLESv2.dll	MS-DOS executable	6,828,136	0B0A2371B8928E1CAD405F728E3AA0	AD396CFD0AA1950FDD4D318BF0CB050DEA9D	
am.pak	PGN (Portable Gaming Notation) Com	136,957	E0807C2E3E92BFD46FA865A31D2B8C	A0D02B3F68156EEDAB2D3ED152BC78B274BEF	
ar.pak	PGN (Portable Gaming Notation) Com	139,253	4C4590FFC76DC0A5D321C5D9A1A5F	4DFFC5A448EEAFBFAC0E94DF0A9B97B851D4A8	
bg.pak	PGN (Portable Gaming Notation) Com	149,152	C672C8C89A32F63BB254B356C3FF84	7E3CF36FA3079C344D475869BABFB2B29F044EF	
bn.pak	PGN (Portable Gaming Notation) Com	195,947	CFF3C9AD87CEF6970E2426CA730129	54DC00598B2ACDE263F6FF3DD1548620D1C59	
ca.pak	PGN (Portable Gaming Notation) Com	96,585	D1C1E2A9809641EEF81E753F26F1EB6	CC54CF4149EA5D934EA3A0B0CD89A5B9F7169F	
cs.pak	PGN (Portable Gaming Notation) Com	98,511	CEDBC097F6FC645A6023BA797CDFD	CDAD25175D737F079B7AC383EFAE7D4CE039EF	
da.pak	PGN (Portable Gaming Notation) Com	89,891	96D8877DABF4C6E6BE2B34002F8800	45D7C3D3BD5A6782F209F2C0808DE6FD2AA4F	
de.pak	PGN (Portable Gaming Notation) Com	96,190	66B905F68D1FC7ACF848C6B7F1245B	271E2DE4A422CAC4920E76D7C81BF15D30C092	
el.pak	PGN (Portable Gaming Notation) Com	166,838	385CA017D7A6E02E2107155C19C479	39522D8E8A192C5035770FBFE8348CCEA5DA35	
en-GB.pak	PGN (Portable Gaming Notation) Com	80,280	7044E0963C16E098DA02975EF92E220	64DBC4C1980C7D7785A9CCB09A6C4F6AC775A	
en-US.pak	PGN (Portable Gaming Notation) Com	81,063	98C8CFC3CB98AB34E06D4323B8BCB0	2C0BDA072161530B710FA0A1DFC3C23926184A	
es-419.pak	PGN (Portable Gaming Notation) Com	94,235	EC06A9386DB1ADE2FF2F3CACA4D3C	9144163F37A70012E884E5BDE5ED6257CE74AA	
es.pak	PGN (Portable Gaming Notation) Com	96,744	E972E49238BDABE3DBCE17F8BFE85B	3B5EBFA19A26644DB1A42DC3E6ACC1FE9137F4	
et.pak	PGN (Portable Gaming Notation) Com	86,125	2EAA14DEA10EAD0CC4792F3C84CEA	533ECB9B83FF7B7A8C7E6985E273093E4DBEC12	
fa.pak	PGN (Portable Gaming Notation) Com	133,802	1199257935EAF73C4CD20F7966322E2	F6403D9B5A2AADC5550DAACA16AB28DBA5CF	
fi.pak	PGN (Portable Gaming Notation) Com	88,954	07B9FC9036F4324184D256B87D346F0	B5B6B31D4D596EED74299B0B2A3EF28552C9DE	
fil.pak	PGN (Portable Gaming Notation) Com	98,025	AF93CF6DF1A3443B5505932A3EDB55	BF367FD719A40BDACA5FEEC299F4A53D68EA09	
fr.pak	PGN (Portable Gaming Notation) Com	104,277	9CB77752E686DA05DDC5F2EC8BC38	809E1507777A20433D9C8FA3B371A0987EE3122	
gu.pak	PGN (Portable Gaming Notation) Com	187,286	11BEB2CDC02D0EFC7DAA88296B5DA	CEDA6551A7D3B20610AD9456183B66EA2C5EA	
he.pak	PGN (Portable Gaming Notation) Com	116,937	0EEFA37827C11109594B42B8DB16201	B08DC15A27797CC76BB8FE3E80E96837B4A265	
hi.pak	PGN (Portable Gaming Notation) Com	192,210	FF949D6C6353F4DAC003ADF69CF325	6F04CDE63509BBD9A7CA539C3A31BA5354EFB	
hr.pak	PGN (Portable Gaming Notation) Com	93,919	19C838F6901AB9F0EFFD711C5D1E65	67F0DECA16106337A6F0B89B73095BF9C3AA9E	
hu.pak	PGN (Portable Gaming Notation) Com	100,006	6788542B420ABBEB3ACDE7B5F1AB88	F2709A3A56950BD2C40EFE2A4167473322400F5	
id.pak	PGN (Portable Gaming Notation) Com	86,674	76C25229C6D86A3CE05ADDE04BD1F	39EDAF1FFE4EBAF298032C89F6F57DFDD6D83D	
it.pak	PGN (Portable Gaming Notation) Com	93,958	34DA77963FAECE776C91E2829F185E3	81F61A803A107405458A4CA6654EC859929660	
ja.pak	PGN (Portable Gaming Notation) Com	113,548	79345CA050327AF6C5E4C9A1C21557	6E4F00EE0AD766494A89B0CD5F9DBDFA1D2E34	
kn.pak	PGN (Portable Gaming Notation) Com	215,358	8A2BA5953188E93BCF9665B885AC1F	7422DA273A75284B548735908C85BB9540BF75	
ko.pak	PGN (Portable Gaming Notation) Com	95,815	28C5A629A2B8CB342FD14D36DAF26	7A832C6C84FC97C308B7C9EE8331A885FFCE87	
lt.pak	PGN (Portable Gaming Notation) Com	102,034	0512E53767F8215D46D31C1E5C33AB	BCEDB4911651A140AF7578416E5312639DF1A3	
lv.pak	PGN (Portable Gaming Notation) Com	100,735	073730434015FC8ED3310E6626E8E79	2373FBA01A251BEDE7C8F1F4912177E9BCB9A6	
ml.pak	PGN (Portable Gaming Notation) Com	226,815	E3505EF16E8EFA2977BA1EB5F678E0C	30365DC55395E29626C72970B56E9F856288C6E	
mr.pak	PGN (Portable Gaming Notation) Com	184,438	D539F46E83560AC792D2F7977FBD04	97B3873CA527AAA27C23465785FE0812DA5B76	
ms.pak	PGN (Portable Gaming Notation) Com	88,659	2E131E4D953C2037C3E9F5F10E25509	5F8656B265905357E4BB6241C5B04F82B0A2BBC	
nb.pak	PGN (Portable Gaming Notation) Com	87,348	53F6E6ACD52940331635DCE809B892	2C5B6404D23AC519113AC396224D60152FD123	
nl.pak	PGN (Portable Gaming Notation) Com	91,367	A1839E47651D2EA73B78AB070DF1B6	F3A4CC1925A03E21C1608675F59390C61E949F6	
pl.pak	PGN (Portable Gaming Notation) Com	98,745	5A024FCD41E374D4F4C88945A48319	8E739583779B394B20D06CD18E96942BB80C8B	
pt-BR.pak	PGN (Portable Gaming Notation) Com	93,645	933D5CCFA8FBBA5C4D8A9357D1B40	FF939ABFED429B05EA726A057B16B7A3836B48	
pt-PT.pak	PGN (Portable Gaming Notation) Com	94,309	0FE3CCAFE2CDA501F336B1A39661C7	B291866AD49E19A3485692FF091EAADB00CAD	
ro.pak	PGN (Portable Gaming Notation) Com	96,749	E42D70AEDAD0404D377A1144A746C	23713E36B25408BAB0AF026FD1AE6363F16908	
ru.pak	PGN (Portable Gaming Notation) Com	152,481	F35F4268E3866EE7EE6933AF7B52CB5	D96666FB0706673FB7B0A0B09229EBBE9E32051	
sk.pak	PGN (Portable Gaming Notation) Com	99,941	64BE97B7A539CFD2BA9C59DADE5EA	D92FE720788C87B56E85342706DFA9DC137C75	

Properties

Properties | Thumbnails View

General | Content Analysis

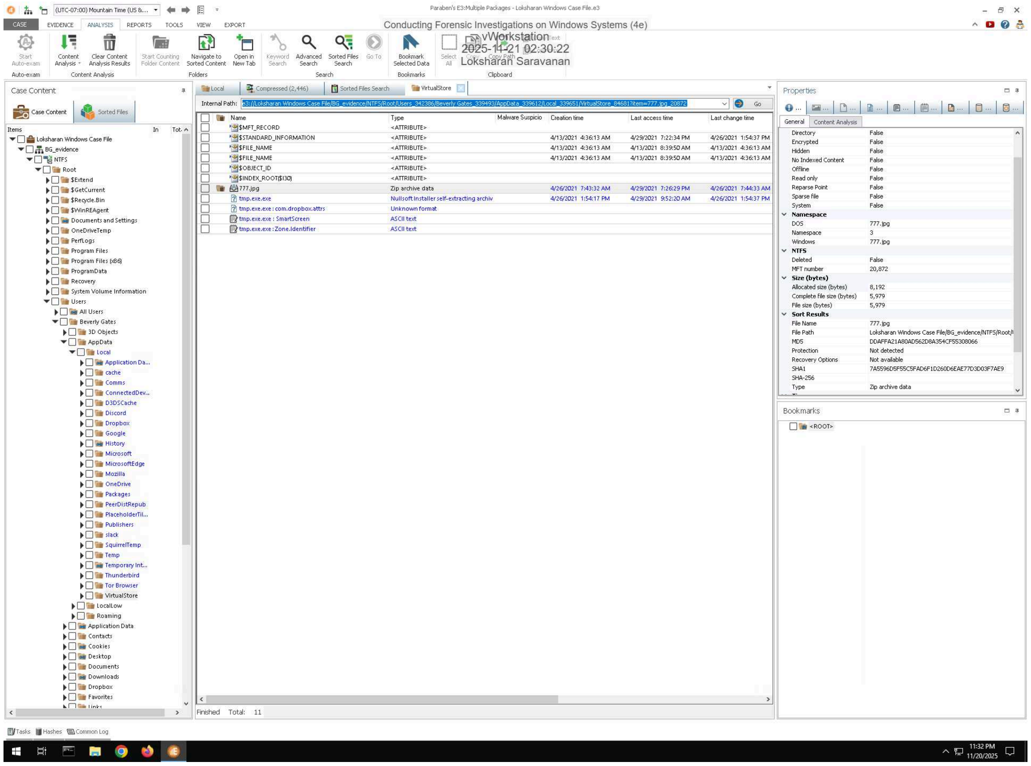
File System Attributes	
Archive	False
Compressed	False
Directory	True
Encrypted	False
Hidden	False
No Indexed Content	False
Offline	False
Read only	False
Reparse Point	False
Sparse file	False
System	False
Local	
Allocated size (bytes)	0
Complete file size (byt	0
Creation time	4/13/2021 11:14:23 AM
Deleted	No
DOS	Local
File size (bytes)	0
Last access time	4/29/2021 7:29:15 PM
Last change time	4/29/2021 5:47:03 PM
Last modification time	4/29/2021 5:47:03 PM
MFT number	339,651
Namespace	3
Windows	Local
Sort Results	
Contains Files	0
Size (bytes)	1,777,781,580
Total Files	15,197

Bookmarks

□ <ROOT>

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)
vWorkstation
2025-11-21 02:30:22
Loksharan Saravanan

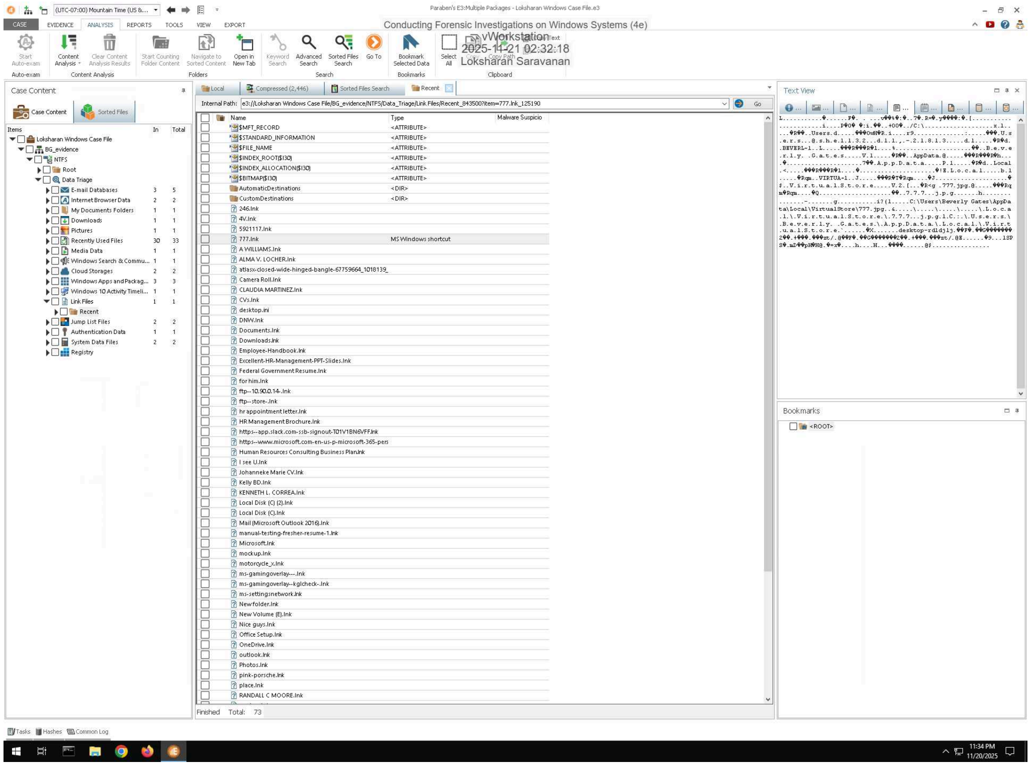
Internal Path: e3://Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/VirtualStore_84681?item=777.jpg_20872

Name	Type	Malware Suspicio	Creation time	Last access time	Last change time
$MFT_RECORD	<ATTRIBUTE>				
$STANDARD_INFORMATION	<ATTRIBUTE>		4/13/2021 4:36:13 AM	4/29/2021 7:22:34 PM	4/26/2021 1:54:37 PM
$FILE_NAME	<ATTRIBUTE>		4/13/2021 4:36:13 AM	4/13/2021 8:39:50 AM	4/13/2021 4:36:13 AM
$FILE_NAME	<ATTRIBUTE>		4/13/2021 4:36:13 AM	4/13/2021 8:39:50 AM	4/13/2021 4:36:13 AM
$OBJECT_ID	<ATTRIBUTE>				
$INDEX_ROOT($I30)	<ATTRIBUTE>				
777.jpg	Zip archive data		4/26/2021 7:43:32 AM	4/29/2021 7:26:29 PM	4/26/2021 7:44:33 AM
tmp.exe.exe	Nullsoft Installer self-extracting archiv		4/26/2021 1:54:17 PM	4/29/2021 9:52:20 AM	4/26/2021 1:54:37 PM
tmp.exe.exe : com.dropbox.attrs	Unknown format				
tmp.exe.exe : SmartScreen	ASCII text				
tmp.exe.exe : Zone.Identifier	ASCII text				

Finished Total: 11

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	
Deleted	False
MFT number	20,872
Size (bytes)	
Allocated size (bytes)	8,192
Complete file size (bytes)	5,979
File size (bytes)	5,979
Sort Results	
File Name	777.jpg
File Path	Loksharan Windows Case File/BG_evidence/NTFS/Root/
MD5	DDAFFA21A80AD562D8A354CF55308066
Protection	Not detected
Recovery Options	Not available
SHA1	7A5596D5F55C5FAD6F1D260D6EAE77D3D03F7AE9
SHA-256	
Type	Zip archive data

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)
vWorkstation
2025-11-21 02:32:18
Loksharan Saravanan

Items	In	Total
Loksharan Windows Case File		
BG_evidence		
NTFS		
Root		
Data Triage		
E-mail Databases	3	5
Internet Browser Data	2	2
My Documents Folders	1	1
Downloads	1	1
Pictures	1	1
Recently Used Files	30	33
Media Data	1	1
Windows Search & Commu...	1	1
Cloud Storages	2	2
Windows Apps and Packag...	3	3
Windows 10 Activity Timeli...	1	1
Link Files	1	1
Recent		
Jump List Files	2	2
Authentication Data	1	1
System Data Files	2	2
Registry		

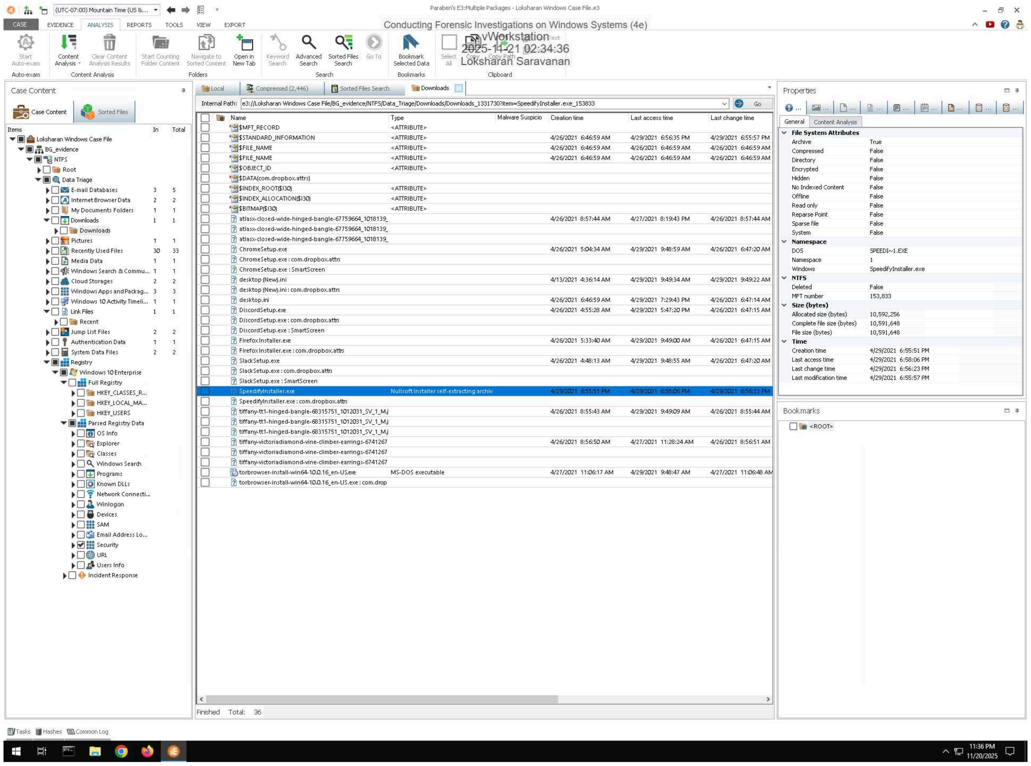
Internal Path: e3://Loksharan Windows Case File/BG_evidence/NTFS/Data_Triage/Link Files/Recent_843500?item=777.lnk_125190

Name	Type	Malware Suspicio
$MFT_RECORD	<ATTRIBUTE>	
$STANDARD_INFORMATION	<ATTRIBUTE>	
$FILE_NAME	<ATTRIBUTE>	
$INDEX_ROOT($I30)	<ATTRIBUTE>	
$INDEX_ALLOCATION($I30)	<ATTRIBUTE>	
$BITMAP($I30)	<ATTRIBUTE>	
AutomaticDestinations	<DIR>	
CustomDestinations	<DIR>	
246.lnk		
4V.lnk		
5921117.lnk		
777.lnk	MS Windows shortcut	
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		
Documents.lnk		
Downloads.lnk		
Employee-Handbook.lnk		
Excellent-HR-Management-PPT-Slides.lnk		
Federal Government Resume.lnk		
for him.lnk		
ftp--10.90.0.14-.lnk		
ftp--store-.lnk		
hr appointment letter.lnk		
HR Management Brochure.lnk		
https--app.slack.com-ssb-signout-T01V1BN6VFF.lnk		
https--www.microsoft.com-en-us-p-microsoft-365-pers		
Human Resources Consulting Business Plan.lnk		
I see U.lnk		
Johanneke Marie CV.lnk		
Kelly BD.lnk		
KENNETH L. CORREA.lnk		
Local Disk (C) (2).lnk		
Local Disk (C).lnk		
Mail (Microsoft Outlook 2016).lnk		
manual-testing-fresher-resume-1.lnk		
Microsoft.lnk		
mockup.lnk		
motorcycle_x.lnk		
ms-gamingoverlay---.lnk		
ms-gamingoverlay--kglcheck-.lnk		
ms-settingsnetwork.lnk		
New folder.lnk		
New Volume (E).lnk		
Nice guys.lnk		
Office Setup.lnk		
OneDrive.lnk		
outlook.lnk		
Photos.lnk		
pink-porsche.lnk		
place.lnk		
RANDALL C MOORE.lnk		

Finished Total: 73

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

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



Conducting Forensic Investigations on Windows Systems (4e)
vWorkstation
2025-11-21 02:34:36
Loksharan Saravanan

Items	In	Total
Loksharan Windows Case File		
BG_evidence		
NTFS		
Root		
Data Triage		
E-mail Databases	3	5
Internet Browser Data	2	2
My Documents Folders	1	1
Downloads	1	1
Downloads		
Pictures	1	1
Recently Used Files	30	33
Media Data	1	1
Windows Search & Commu...	1	1
Cloud Storages	2	2
Windows Apps and Packag...	3	3
Windows 10 Activity Timeli...	1	1
Link Files	1	1
Recent		
Jump List Files	2	2
Authentication Data	1	1
System Data Files	2	2
Registry		
Windows 10 Enterprise		
Full Registry		
HKEY_CLASSES_R...		
HKEY_LOCAL_MA...		
HKEY_USERS		
Parsed Registry Data		
OS Info		
Explorer		
Classes		
Windows Search		
Programs		
Known DLLs		
Network Connecti...		
Winlogon		
Devices		
SAM		
Email Address Lo...		
☑ Security		
URL		
Users Info		
Incident Response		

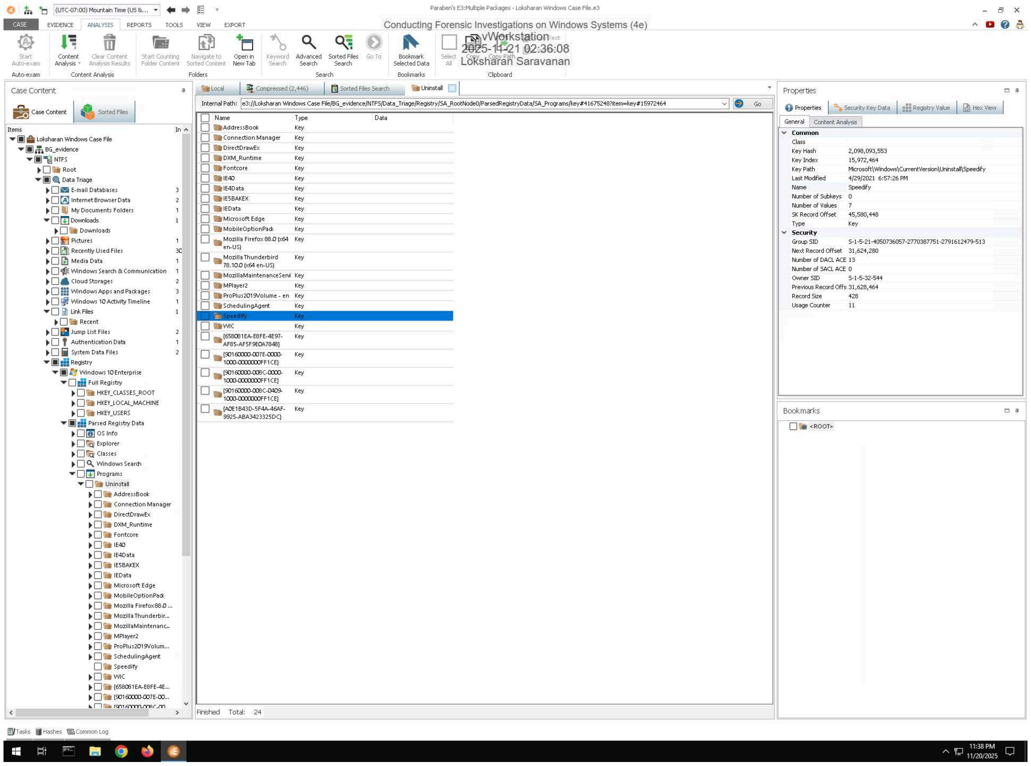
Internal Path: e3://Loksharan Windows Case File/BG_evidence/NTFS/Data_Triage/Downloads/Downloads_1331730?item=SpeedifyInstaller.exe_153833

Name	Type	Malware Suspicio	Creation time	Last access time	Last change time
$MFT_RECORD	<ATTRIBUTE>				
$STANDARD_INFORMATION	<ATTRIBUTE>		4/26/2021 6:46:59 AM	4/29/2021 6:56:35 PM	4/29/2021 6:55:57 PM
$FILE_NAME	<ATTRIBUTE>		4/26/2021 6:46:59 AM	4/26/2021 6:46:59 AM	4/26/2021 6:46:59 AM
$FILE_NAME	<ATTRIBUTE>		4/26/2021 6:46:59 AM	4/26/2021 6:46:59 AM	4/26/2021 6:46:59 AM
$OBJECT_ID	<ATTRIBUTE>				
$DATA(com.dropbox.attrs)					
$INDEX_ROOT($I30)	<ATTRIBUTE>				
$INDEX_ALLOCATION($I30)	<ATTRIBUTE>				
$BITMAP($I30)	<ATTRIBUTE>				
atlasx-closed-wide-hinged-bangle-67759664_1018139_			4/26/2021 8:57:44 AM	4/27/2021 8:19:43 PM	4/26/2021 8:57:44 AM
atlasx-closed-wide-hinged-bangle-67759664_1018139_					
atlasx-closed-wide-hinged-bangle-67759664_1018139_					
ChromeSetup.exe			4/26/2021 5:04:34 AM	4/29/2021 9:48:59 AM	4/26/2021 6:47:20 AM
ChromeSetup.exe : com.dropbox.attrs					
ChromeSetup.exe : SmartScreen					
desktop (New).ini			4/13/2021 4:36:14 AM	4/29/2021 9:49:34 AM	4/29/2021 9:49:22 AM
desktop (New).ini : com.dropbox.attrs					
desktop.ini			4/26/2021 6:46:59 AM	4/29/2021 7:29:43 PM	4/26/2021 6:47:14 AM
DiscordSetup.exe			4/26/2021 4:55:28 AM	4/29/2021 5:47:20 PM	4/26/2021 6:47:15 AM
DiscordSetup.exe : com.dropbox.attrs					
DiscordSetup.exe : SmartScreen					
Firefox Installer.exe			4/26/2021 5:33:40 AM	4/29/2021 9:49:00 AM	4/26/2021 6:47:15 AM
Firefox Installer.exe : com.dropbox.attrs					
SlackSetup.exe			4/26/2021 4:48:13 AM	4/29/2021 9:48:55 AM	4/26/2021 6:47:20 AM
SlackSetup.exe : com.dropbox.attrs					
SlackSetup.exe : SmartScreen					
SpeedifyInstaller.exe	Nullsoft Installer self-extracting archiv		4/29/2021 6:55:51 PM	4/29/2021 6:58:06 PM	4/29/2021 6:56:23 PM
SpeedifyInstaller.exe : com.dropbox.attrs					
tiffany-tt1-hinged-bangle-68315751_1012031_SV_1_M.j			4/26/2021 8:55:43 AM	4/29/2021 9:49:09 AM	4/26/2021 8:55:44 AM
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			4/26/2021 8:56:50 AM	4/27/2021 11:28:24 AM	4/26/2021 8:56:51 AM
tiffany-victoriadiamond-vine-climber-earrings-6741267					
tiffany-victoriadiamond-vine-climber-earrings-6741267					
torbrowser-install-win64-10.0.16_en-US.exe	MS-DOS executable		4/27/2021 11:06:17 AM	4/29/2021 9:48:47 AM	4/27/2021 11:06:48 AM
torbrowser-install-win64-10.0.16_en-US.exe : com.drop					

Finished Total: 36

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	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 (bytes)	10,591,648
File size (bytes)	10,591,648
Time	
Creation time	4/29/2021 6:55:51 PM
Last access time	4/29/2021 6:58:06 PM
Last change time	4/29/2021 6:56:23 PM
Last modification time	4/29/2021 6:55:57 PM

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



Paraben's E3:Multiple Packages - Loksharan Windows Case File.e3

Conducting Forensic Investigations on Windows Systems (4e)
vWorkstation
2025-11-21 02:36:08
Loksharan Saravanan

Internal Path: e3://Loksharan Windows Case File/BG_evidence/NTFS/Data_Triage/Registry/SA_RootNode0/ParsedRegistryData/SA_Programs/key#41675248?item=key#15972464

Name	Type	Data
AddressBook	Key	
Connection Manager	Key	
DirectDrawEx	Key	
DXM_Runtime	Key	
Fontcore	Key	
IE40	Key	
IE4Data	Key	
IE5BAKEX	Key	
IEData	Key	
Microsoft Edge	Key	
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	

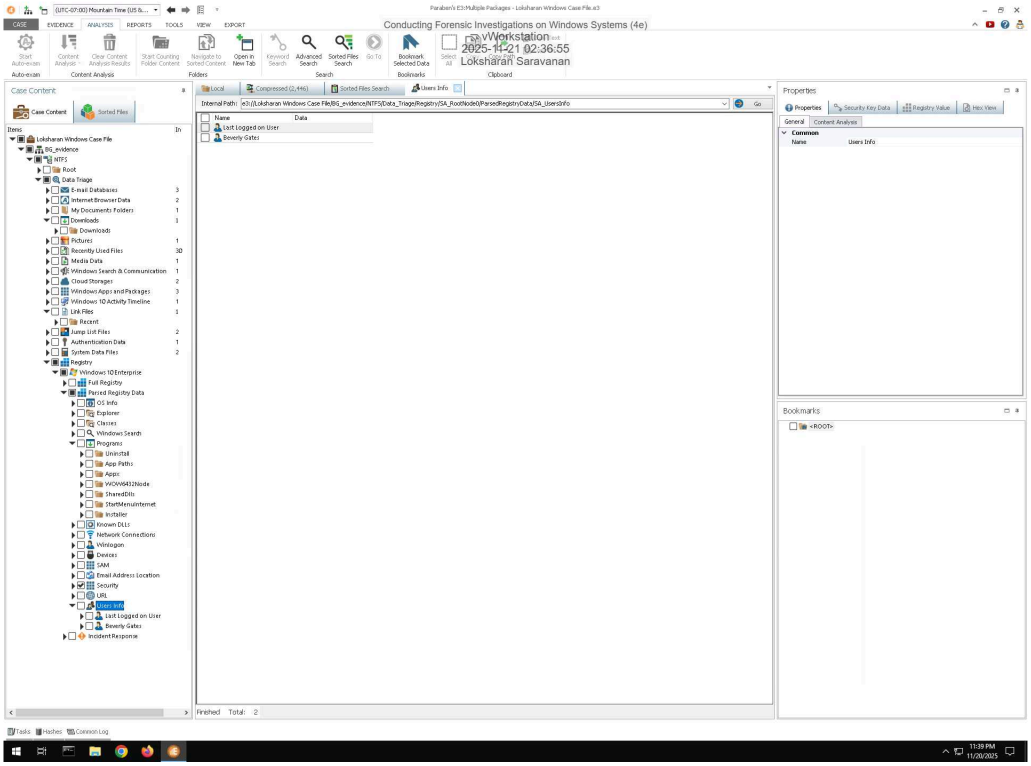
Finished Total: 24

Properties

Common	
Class	
Key Hash	2,098,093,553
Key Index	15,972,464
Key Path	Microsoft\Windows\CurrentVersion\Uninstall\Speedify
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-1-5-21-4050736057-2770387751-2791612479-513
Next Record Offset	31,624,280
Number of DACL ACE	13
Number of SACL ACE	0
Owner SID	S-1-5-32-544
Previous Record Offs	31,628,464
Record Size	428
Usage Counter	11

11:38 PM
11/20/2025

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



Paraben's E3:Multiple Packages - Loksharan Windows Case File.e3

Conducting Forensic Investigations on Windows Systems (4e)
vWorkstation
2025-11-21 02:36:55
Loksharan Saravanan

Internal Path: e3://Loksharan Windows Case File/BG_evidence/NTFS/Data_Triage/Registry/SA_RootNode0/ParsedRegistryData/SA_UsersInfo

Name	Data
Last Logged on User	
Beverly Gates	

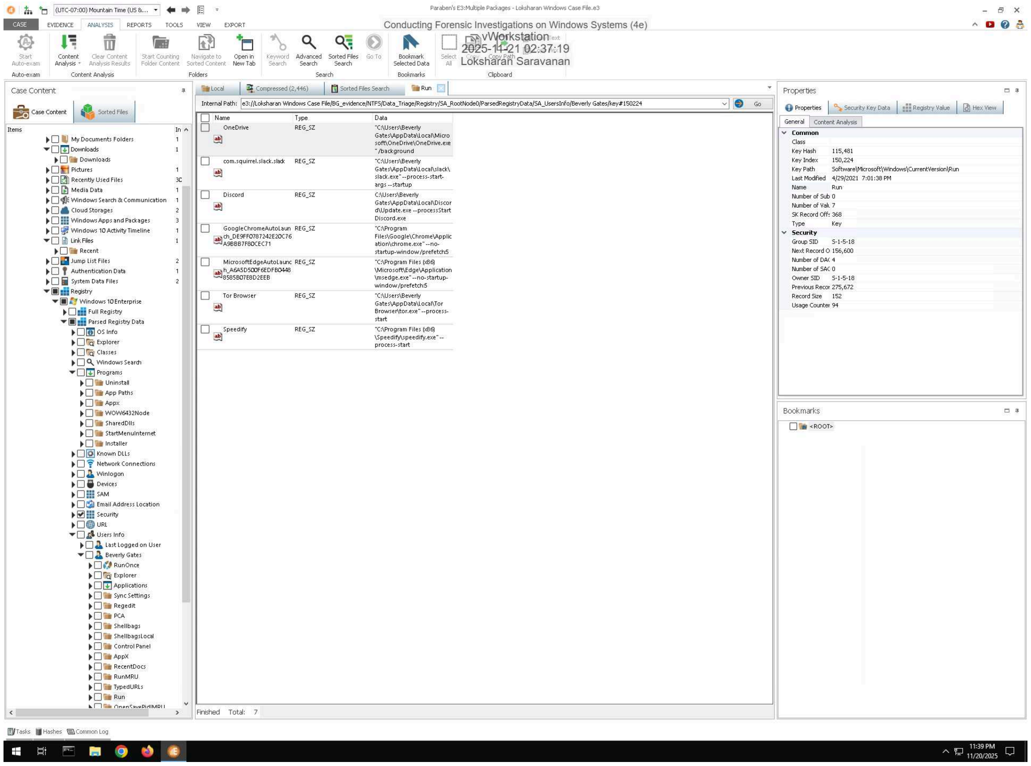
Finished Total: 2

Properties

Common	
Name	Users Info

11:39 PM
11/20/2025

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



Paraben's E3:Multiple Packages - Loksharan Windows Case File.e3
Conducting Forensic Investigations on Windows Systems (4e)
vWorkstation
2025-11-21 02:37:19
Loksharan Saravanan
Local
Compressed (2,446)
Sorted Files Search
Run

Internal Path: e3://Loksharan Windows Case File/BG_evidence/NTFS/Data_Triage/Registry/SA_RootNode0/ParsedRegistryData/SA_UsersInfo/Beverly Gates/key#150224

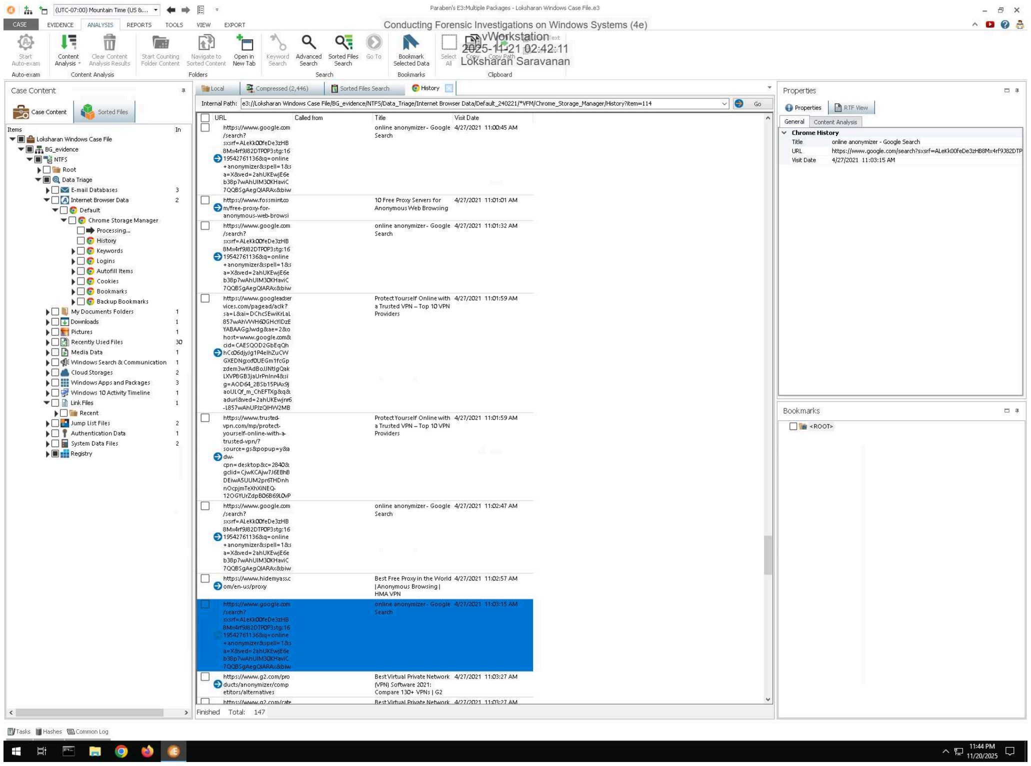
Name	Type	Data
OneDrive	REG_SZ	"C:\Users\Beverly Gates\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
com.squirrel.slack.slack	REG_SZ	"C:\Users\Beverly Gates\AppData\Local\slack\slack.exe" --process-start-args --startup
Discord	REG_SZ	C:\Users\Beverly Gates\AppData\Local\Discord\Update.exe --processStart Discord.exe
GoogleChromeAutoLaunch_DE9FF0787242E20C76A9BBB7F80CEC71	REG_SZ	"C:\Program Files\Google\Chrome\Application\chrome.exe" --no-startup-window /prefetch:5
MicrosoftEdgeAutoLaunch_A6A5D500F6EDFB04488585B07E8D2EEB	REG_SZ	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window /prefetch:5
Tor Browser	REG_SZ	"C:\Users\Beverly Gates\AppData\Local\Tor Browser\tor.exe" --process-start
Speedify	REG_SZ	"C:\Program Files (x86)\Speedify\speedify.exe" --process-start

Finished Total: 7

Properties

Common	
Class	
Key Hash	115,481
Key Index	150,224
Key Path	Software\Microsoft\Windows\CurrentVersion\Run
Last Modified	4/29/2021 7:01:38 PM
Name	Run
Number of Sub	0
Number of Valu	7
SK Record Offs	368
Type	Key
Security	
Group SID	S-1-5-18
Next Record O	156,600
Number of DAC	4
Number of SAC	0
Owner SID	S-1-5-18
Previous Recor	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**.



Internal Path: e3://Loksharan Windows Case File/BG_evidence/NTFS/Data_Triage/Internet Browser Data/Default_240221/*VFM/Chrome_Storage_Manager/History?item=114

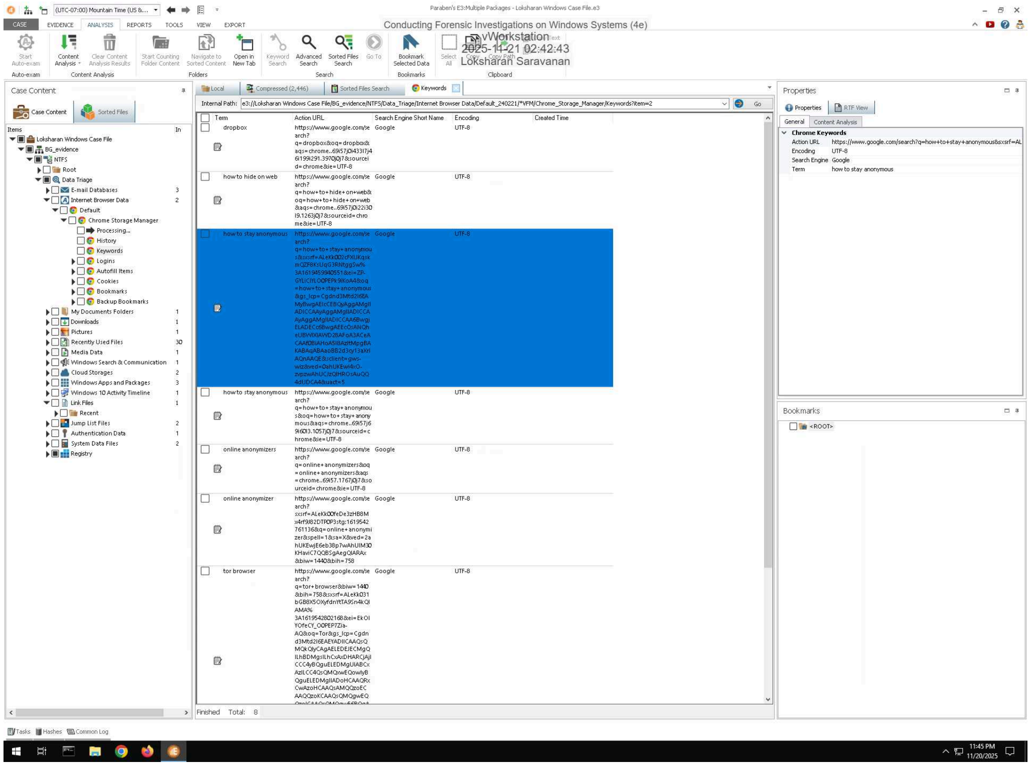
URL	Called from	Title	Visit Date
https://www.google.com/search?sxsrf=ALeKk00feDe3zHB8Mx4rf9J82DTP0P3stg:1619542761136&q=online+anonymizer&spell=1&sa=X&ved=2ahUKEwjE6eb38p7wAhUIM30KHaviC7QQBSgAegQIARAx&biw		online anonymizer - Google Search	4/27/2021 11:00:45 AM
https://www.fossmint.com/free-proxy-for-anonymous-web-browsi		10 Free Proxy Servers for Anonymous Web Browsing	4/27/2021 11:01:01 AM
https://www.google.com/search?sxsrf=ALeKk00feDe3zHB8Mx4rf9J82DTP0P3stg:1619542761136&q=online+anonymizer&spell=1&sa=X&ved=2ahUKEwjE6eb38p7wAhUIM30KHaviC7QQBSgAegQIARAx&biw		online anonymizer - Google Search	4/27/2021 11:01:32 AM
https://www.googleadservices.com/pagead/aclk?sa=L&ai=DChcSEwiKrLaL857wAhVVH60GHcYIDzEYABAAGgJwdg&ae=2&ohost=www.google.com&cid=CAESQOD2GbEqQhhCo06djyJg1P4elhZuCVVGXEDNgxxf0UEGm1fcGpzdem3wYAdBoJJNtIgQakLXVP8GB3jaUrPnInr4&sig=AOD64_2BSb15PiAx9jaoULQf_m_ChEFTXg&q&adurl&ved=2ahUKEwjnr6-L857wAhUPJzQIHW2MB		Protect Yourself Online with a Trusted VPN – Top 10 VPN Providers	4/27/2021 11:01:59 AM
https://www.trusted-vpn.com/mp/protect-yourself-online-with-a-trusted-vpn/?source=gs&popup=y&adw-cpn=desktop&c=2840&gclid=CjwKCAjw7J6EBhBDEiwA5UUM2pr6THDnhnOcpjmTeXhXiNEQ-12OGYUrZdpB06B69L0vP		Protect Yourself Online with a Trusted VPN – Top 10 VPN Providers	4/27/2021 11:01:59 AM
https://www.google.com/search?sxsrf=ALeKk00feDe3zHB8Mx4rf9J82DTP0P3stg:1619542761136&q=online+anonymizer&spell=1&sa=X&ved=2ahUKEwjE6eb38p7wAhUIM30KHaviC7QQBSgAegQIARAx&biw		online anonymizer - Google Search	4/27/2021 11:02:47 AM
https://www.hidemyass.com/en-us/proxy		Best Free Proxy in the World | Anonymous Browsing | HMA VPN	4/27/2021 11:02:57 AM
https://www.google.com/search?sxsrf=ALeKk00feDe3zHB8Mx4rf9J82DTP0P3stg:1619542761136&q=online+anonymizer&spell=1&sa=X&ved=2ahUKEwjE6eb38p7wAhUIM30KHaviC7QQBSgAegQIARAx&biw		online anonymizer - Google Search	4/27/2021 11:03:15 AM
https://www.g2.com/products/anonymizer/competitors/alternatives		Best Virtual Private Network (VPN) Software 2021: Compare 130+ VPNs | G2	4/27/2021 11:03:27 AM
https://www.g2.com/cate		Best Virtual Private Network	4/27/2021 11:03:27 AM

Finished Total: 147

Chrome History

Title	online anonymizer - Google Search
URL	https://www.google.com/search?sxsrf=ALeKk00feDe3zHB8Mx4rf9J82DTP
Visit Date	4/27/2021 11:03:15 AM

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



Paraben's E3:Multiple Packages - Loksharan Windows Case File.e3
Conducting Forensic Investigations on Windows Systems (4e)
vWorkstation
2025-11-21 02:42:43
Loksharan Saravanan
Local
Compressed (2,446)
Sorted Files Search
Keywords

Internal Path: e3://Loksharan Windows Case File/BG_evidence/NTFS/Data_Triage/Internet Browser Data/Default_240221/*VFM/Chrome_Storage_Manager/Keywords?item=2

Term	Action URL	Search Engine Short Name	Encoding	Created Time
dropbox	https://www.google.com/search?q=dropbox&oq=dropbox&aqs=chrome..69i57j0i433l7j46i199i291.3970j0j7&sourceid=chrome&ie=UTF-8	Google	UTF-8	
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	UTF-8	
how to stay anonymous	https://www.google.com/search?q=how+to+stay+anonymous&sxsrf=ALeKk002cFXUKq3kmQZF8KsUqG3RNtggSw%3A1619459940551&ei=ZP-GYLiCIYLO0PEPk9iKoA4&oq=how+to+stay+anonymous&gs_lcp=Cgdnd3Mtd2l6EAMyBwgAEIcCEBQyAggAMgIIADICCAAyAggAMgIIADICCAAyAggAMgIIADICCAA6BwgjELADECc6BwgAEEcQsANQheUBWIXIAWD28AFoA3ACeACAAf0BiAHoA5IBAzItMpgBAKABAqABAaoBB2d3cy13aXrIAQnAAQE&sclient=gws-wiz&ved=0ahUKEwi4xO-zvpzwAhUCJzQIHROsAuQQ4dUDCA4&uact=5	Google	UTF-8	
how to stay anonymous	https://www.google.com/search?q=how+to+stay+anonymous&oq=how+to+stay+anonymous&aqs=chrome..69i57j69i60l3.1057j0j7&sourceid=chrome&ie=UTF-8	Google	UTF-8	
online anonymizers	https://www.google.com/search?q=online+anonymizers&oq=online+anonymizers&aqs=chrome..69i57.1767j0j7&sourceid=chrome&ie=UTF-8	Google	UTF-8	
online anonymizer	https://www.google.com/search?sxsrf=ALeKk00feDe3zHB8Mx4rf9J82DTP0P3stg:1619542761136&q=online+anonymizer&spell=1&sa=X&ved=2ahUKEwjE6eb38p7wAhUIM30KHaviC7QQBSgAegQIARAx&biw=1440&bih=758	Google	UTF-8	
tor browser	https://www.google.com/search?q=tor+browser&biw=1440&bih=758&sxsrf=ALeKk031bGB8X5OXyfdnYtTA9Sn4kQIAMA%3A1619542802168&ei=EkOIYOfeCY_O0PEP7Zia-AQ&oq=Tor&gs_lcp=Cgdnd3Mtd2l6EAEYADIICAAQsQMQkQIyCAgAELEDEJECMgQILhBDMgsILhCxAxDHARCjAjIICC4yBQguELEDMgUIABCxAzILCC4QsQMQxwEQowIyBQguELEDMgIIADoHCAAQRxCwAzoHCAAQsAMQQzoECAAQQzoKCAAQsQMQgwEQ	Google	UTF-8	

Finished Total: 8

Properties

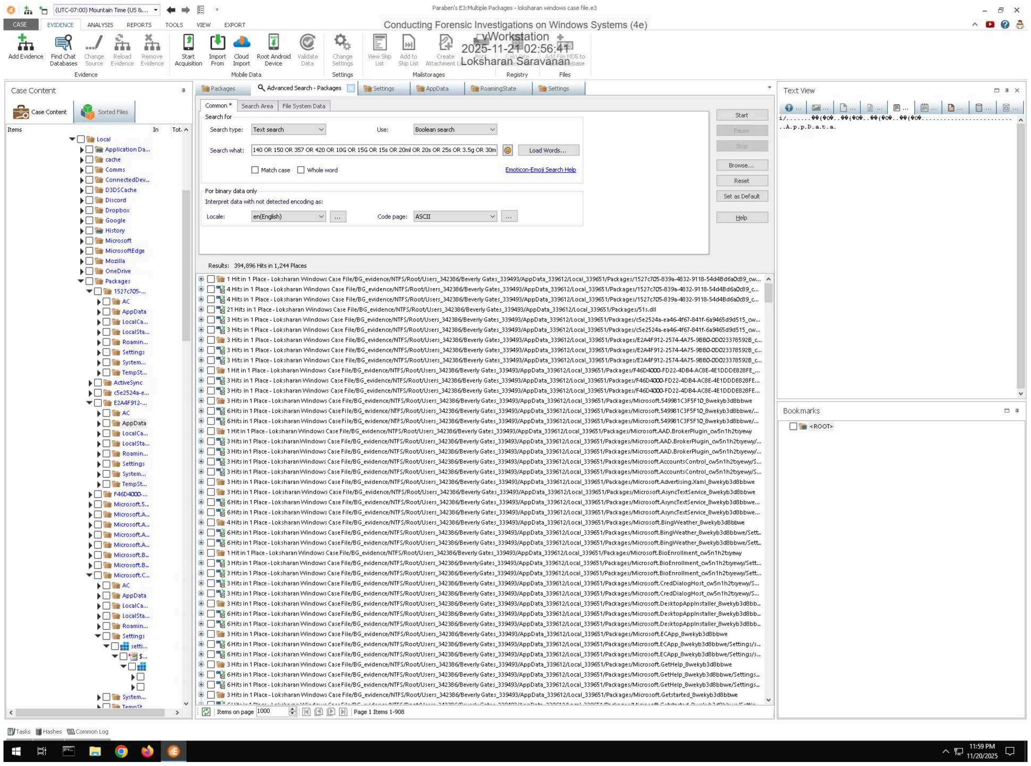
Chrome Keywords

Action URL	https://www.google.com/search?q=how+to+stay+anonymous&sxsrf=AL
Encoding	UTF-8
Search Engine	Google
Term	how to stay anonymous

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**.



Paraben's E3:Multiple Packages - loksharan windows case file.e3

Conducting Forensic Investigations on Windows Systems (4e)
vWorkstation
2025-11-21 02:56:41
Loksharan Saravanan

Search for

Search type: Text search   Use: Boolean search

Search what: 140 OR 150 OR 357 OR 420 OR 10G OR 15G OR 15s OR 20ml OR 20s OR 25s OR 3.5g OR 30m

□ Match case   □ Whole word

For binary data only

Interpret data with not detected encoding as:

Locale: en(English)   Code page: ASCII

Results: 394,896 Hits in 1,244 Places

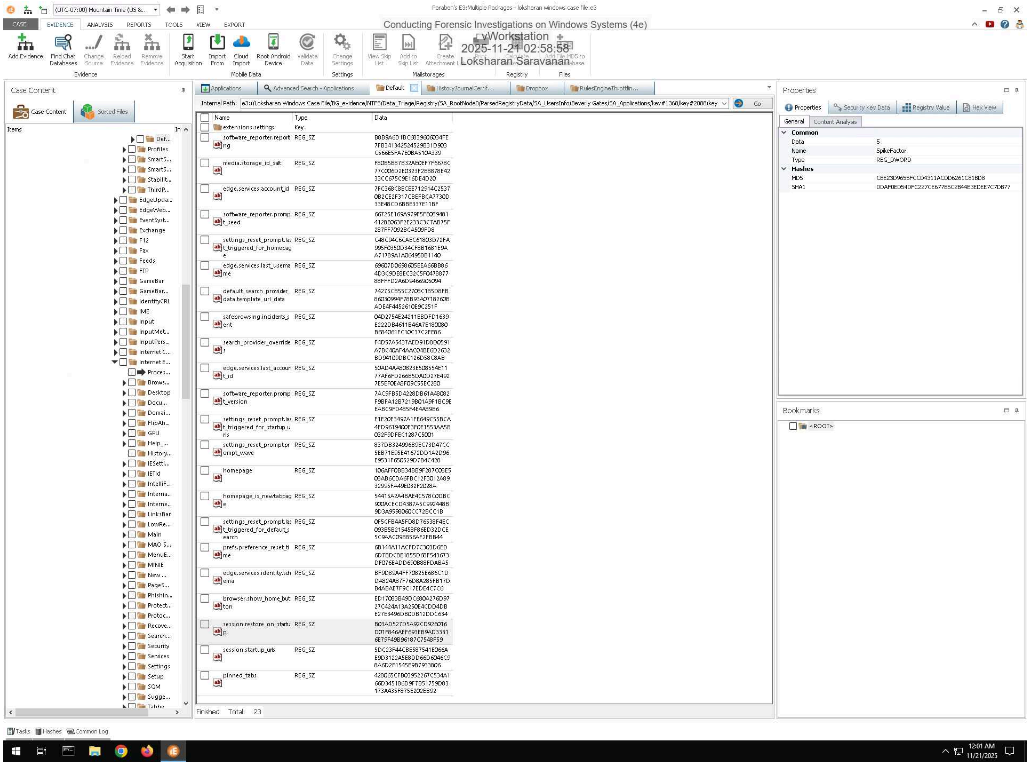
```
1 Hit in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/1527c705-839a-4832-9118-54d4Bd6a0c89_cw...
4 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/1527c705-839a-4832-9118-54d4Bd6a0c89_c...
4 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/1527c705-839a-4832-9118-54d4Bd6a0c89_c...
21 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/51s.dll
3 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/c5e2524a-ea46-4f67-841f-6a9465d9d515_cw...
3 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/c5e2524a-ea46-4f67-841f-6a9465d9d515_cw...
3 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/E2A4F912-2574-4A75-9BB0-0D023378592B_c...
3 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/E2A4F912-2574-4A75-9BB0-0D023378592B_c...
3 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/E2A4F912-2574-4A75-9BB0-0D023378592B_c...
1 Hit in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/F46D4000-FD22-4DB4-AC8E-4E1DDDE828FE_...
3 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/F46D4000-FD22-4DB4-AC8E-4E1DDDE828FE...
3 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/F46D4000-FD22-4DB4-AC8E-4E1DDDE828FE...
3 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.549981C3F5F10_8wekyb3d8bbwe
6 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.549981C3F5F10_8wekyb3d8bbwe/...
6 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.549981C3F5F10_8wekyb3d8bbwe/...
1 Hit in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy
3 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy/...
3 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy/...
3 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.AccountsControl_cw5n1h2txyewy/S...
3 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.AccountsControl_cw5n1h2txyewy/S...
3 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.Advertising.Xaml_8wekyb3d8bbwe
3 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.AsyncTextService_8wekyb3d8bbwe
6 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.AsyncTextService_8wekyb3d8bbwe...
6 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.AsyncTextService_8wekyb3d8bbwe...
4 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.BingWeather_8wekyb3d8bbwe
6 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.BingWeather_8wekyb3d8bbwe/Sett...
6 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.BingWeather_8wekyb3d8bbwe/Sett...
1 Hit in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.BioEnrollment_cw5n1h2txyewy
3 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.BioEnrollment_cw5n1h2txyewy/Sett...
3 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.BioEnrollment_cw5n1h2txyewy/Sett...
3 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.CredDialogHost_cw5n1h2txyewy/S...
3 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.CredDialogHost_cw5n1h2txyewy/S...
3 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.DesktopAppInstaller_8wekyb3d8bb...
6 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.DesktopAppInstaller_8wekyb3d8bb...
6 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.DesktopAppInstaller_8wekyb3d8bb...
3 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.ECApp_8wekyb3d8bbwe
6 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.ECApp_8wekyb3d8bbwe/Settings/s...
6 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.ECApp_8wekyb3d8bbwe/Settings/s...
3 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.GetHelp_8wekyb3d8bbwe
6 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.GetHelp_8wekyb3d8bbwe/Settings...
6 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.GetHelp_8wekyb3d8bbwe/Settings...
3 Hits in 1 Place - Loksharan Windows Case File/BG_evidence/NTFS/Root/Users_342386/Beverly Gates_339493/AppData_339612/Local_339651/Packages/Microsoft.Getstarted_8wekyb3d8bbwe
```

Items on page 1000   Page 1 Items 1-908

```
i/.......��{��..��{��..��{��..��{��.........................
..A.p.p.D.a.t.a.
```

Part 2: Identify Suspicious Browser Activity

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



Conducting Forensic Investigations on Windows Systems (4e)
vWorkstation
2025-11-21 02:58:58
Loksharan Saravanan

Internal Path: e3://Loksharan Windows Case File/BG_evidence/NTFS/Data_Triage/Registry/SA_RootNode0/ParsedRegistryData/SA_UsersInfo/Beverly Gates/SA_Applications/key#1368/key#2088/key-

Name	Type	Data
extensions.settings	Key	
software_reporter.reporting	REG_SZ	B8B9A6D1BC6839606034FE7FB341342524529B31D903C566E5FA7E0BA510A339
media.storage_id_salt	REG_SZ	F80B5B87B32AE0EF7F6678C77C006D2E0323F2B8878E4233CC675C9E16DE4D20
edge.services.account_id	REG_SZ	7FC368C8ECEE712914C25370B2CE2F317CBEFBCA7730D33E48CD6BBE337E11BF
software_reporter.prompt_seed	REG_SZ	66725E169A979F5FE0894814128E063F2E233C3C7AB75F287FF7092BCA509FD8
settings_reset_prompt.last_triggered_for_homepage	REG_SZ	C48C94C6CAEC61803D72FA995F0350D34CF8B1681E9AA71789A1A064958B1140
edge.services.last_username	REG_SZ	69607D0698605EEA66BB864D3C9DE8EC32C5F047887788FFFD2A6D9466905094
default_search_provider_data.template_url_data	REG_SZ	74275CB55C2708C185D8FB86030994F78B93A0718260BADE4F4452610E9C251F
safebrowsing.incidents_sent	REG_SZ	04D2754E24211EBDFD1639E222DB4611B46A7E180080B684061FC10C37C2FE86
search_provider_overrides	REG_SZ	F4D57A5437AED91D8D0591A7BC40AF4AAC04BE6D2632BD94109DBC126D58C8AB
edge.services.last_account_id	REG_SZ	50AD4AA80823E508554E1177AF6FD266B5DA0D27E4927E5EF0EA8F09C55EC280
software_reporter.prompt_version	REG_SZ	7AC9FB5D4228DB61A48082F9BFA12B7219B01A9F1BC9EEABC9FD485F4E4A89B6
settings_reset_prompt.last_triggered_for_startup_urls	REG_SZ	E1E20E3497A1FE649C55BCA4FD9619400E3F0E1553AA5B032F9DFEC1287C5001
settings_reset_promptprompt_wave	REG_SZ	837DB324996B9EC73D47CC5EB71E95E41672DD1A2D96E9531F650529D7B4C428
homepage	REG_SZ	106AFF0BB34BB9F287C08E508AB6CDA6FBC12F3012A8932995FA49E032F2028A
homepage_is_newtabpage	REG_SZ	54415A2A4BAE4C578C0DBC900ACECD4387A5C992448B9D3A959806 0CC72BCC1B
settings_reset_prompt.last_triggered_for_default_search	REG_SZ	0F5CFB4A5FD8D76538F4EC093B5B215458F86ED32DCE5C9AAC09B856AF2FBB44
prefs.preference_reset_time	REG_SZ	6B144A11ACFD7C303D6ED6D7BDC8E1855D68F543673DF076EADD690B88FDABA5
edge.services.identity.schema	REG_SZ	BF9D89A4FF70825E686C1DDA824A87F76D8A285FB17DB4ABAE7F9C17EDE4C7C6
browser.show_home_button	REG_SZ	ED17083B49DC680A276D9727C424A13A250E4CDD4DBE27E3496DB0DB12DDC634
session.restore_on_startup	REG_SZ	B03AD527D5A92CD926016D01F846AEF693EB9AD33316E79F49B96187C7548F59
session.startup_urls	REG_SZ	5DC23F44CBE587541E066AE9D3122A5E8DD66D6046C98A6D2F1545E9B7933806
pinned_tabs	REG_SZ	428065CFB03952267C534A166D345186D9F7B51759D83173A435F875E202EB92

Finished Total: 23

Properties
Properties | Security Key Data | Registry Value | Hex View
General | Content Analysis

Common	
Data	5
Name	SpikeFactor
Type	REG_DWORD
Hashes	
MD5	CBE23D9655FCCD4311ACDD6261C81BD8
SHA1	DDAF0ED54DFC227CE677B5C2B44E3EDEE7C7DB77

Bookmarks
□ <ROOT>