CSE 805 MID 2 (LAB exam)

Lab 04: Windows Registry Analysis (using Autopsy)

REGISTRY

What we need: Autopsy, Analyzing Image

Questions?

1. Find out the computer name?
2. Current version of windows?
3. User accounts?
4. Find out the time zone?
5. Find out the IP address?
6. Find out the mounted devices?

Note: The main system registry files most often viewed by examiners are:

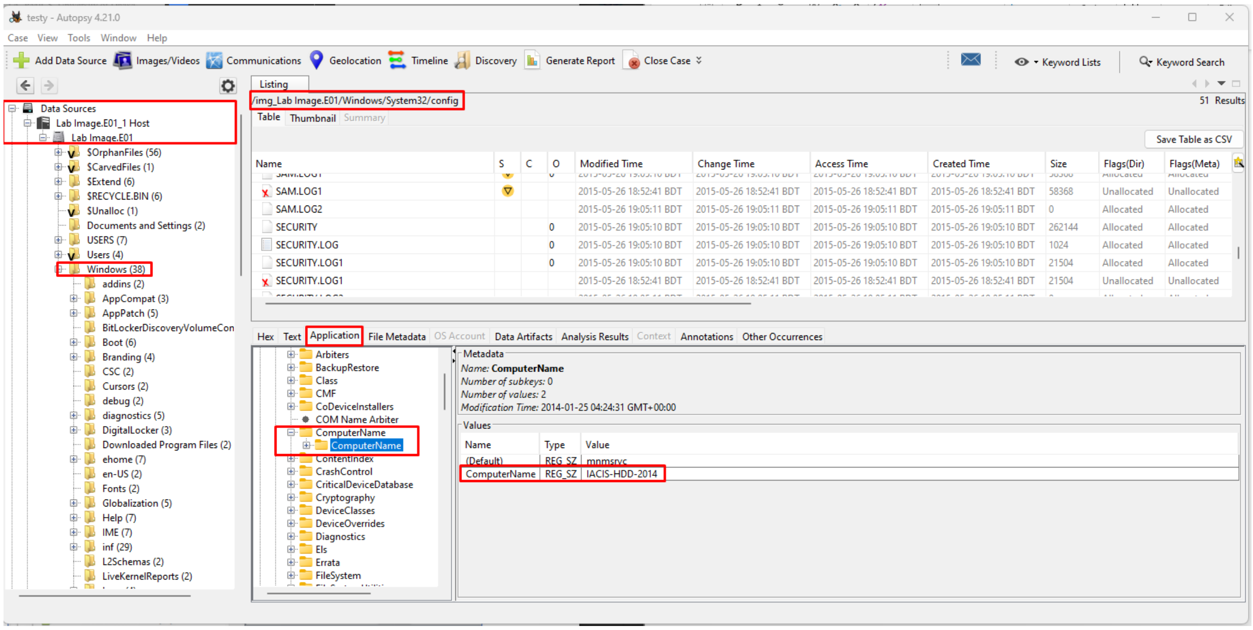
- **System**
- **Security**
- **Software**
- **SAM**

Ans to the Q: No: 1

/img_Lab Image.E01/WINDOWS/system32/config/

SYSTEM > ControlSet001 > Control > ComputerName

Computer Name:



/img_Lab Image.E01/Windows/System32/config

51 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
SAM.LOG1	▽			2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	58368	Unallocated	Unallocated
SAM.LOG2				2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	0	Allocated	Allocated
SECURITY			0	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	262144	Allocated	Allocated
SECURITY.LOG			0	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	1024	Allocated	Allocated
SECURITY.LOG1			0	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	21504	Allocated	Allocated
SECURITY.LOG1				2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	21504	Unallocated	Unallocated

Metadata

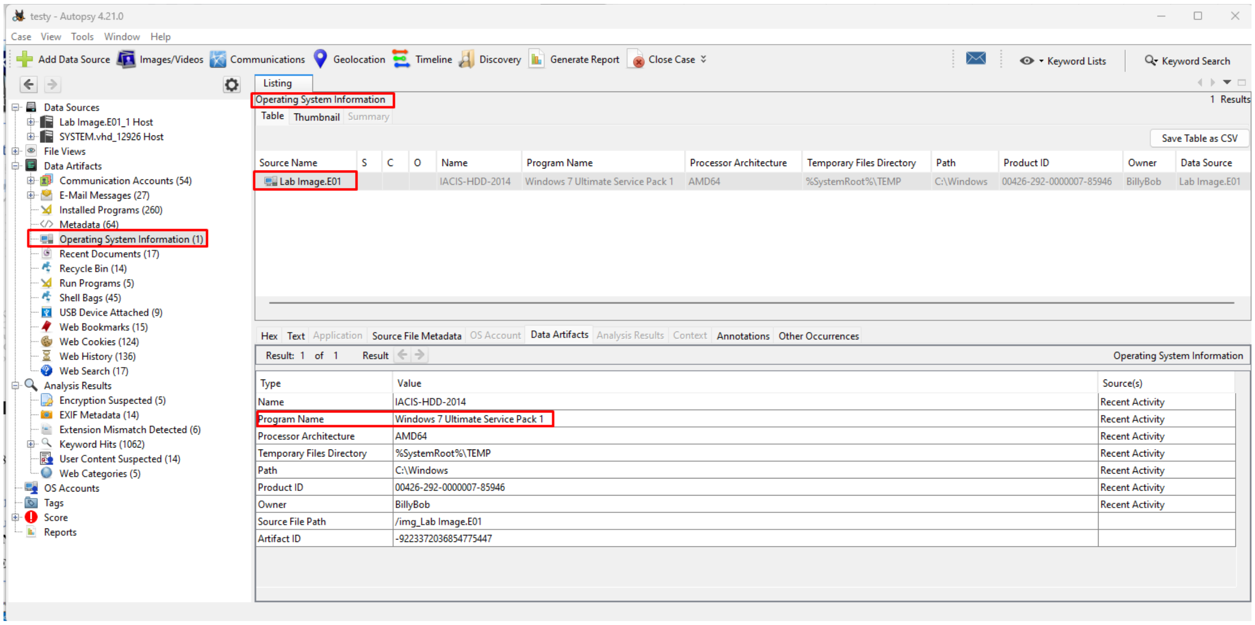
Name: **ComputerName**
Number of subkeys: 0
Number of values: 2
Modification Time: 2014-01-25 04:24:31 GMT+00:00

Values

Name	Type	Value
(Default)	REG_SZ	mnmsrvc
ComputerName	REG_SZ	IACIS-HDD-2014

Ans to the Q: No: 2

Current version of the windows:



Operating System Information

1 Results

Source Name	S	C	O	Name	Program Name	Processor Architecture	Temporary Files Directory	Path	Product ID	Owner	Data Source
Lab Image.E01				IACIS-HDD-2014	Windows 7 Ultimate Service Pack 1	AMD64	%SystemRoot%\TEMP	C:\Windows	00426-292-0000007-85946	BillyBob	Lab Image.E01

Result: 1 of 1 Result

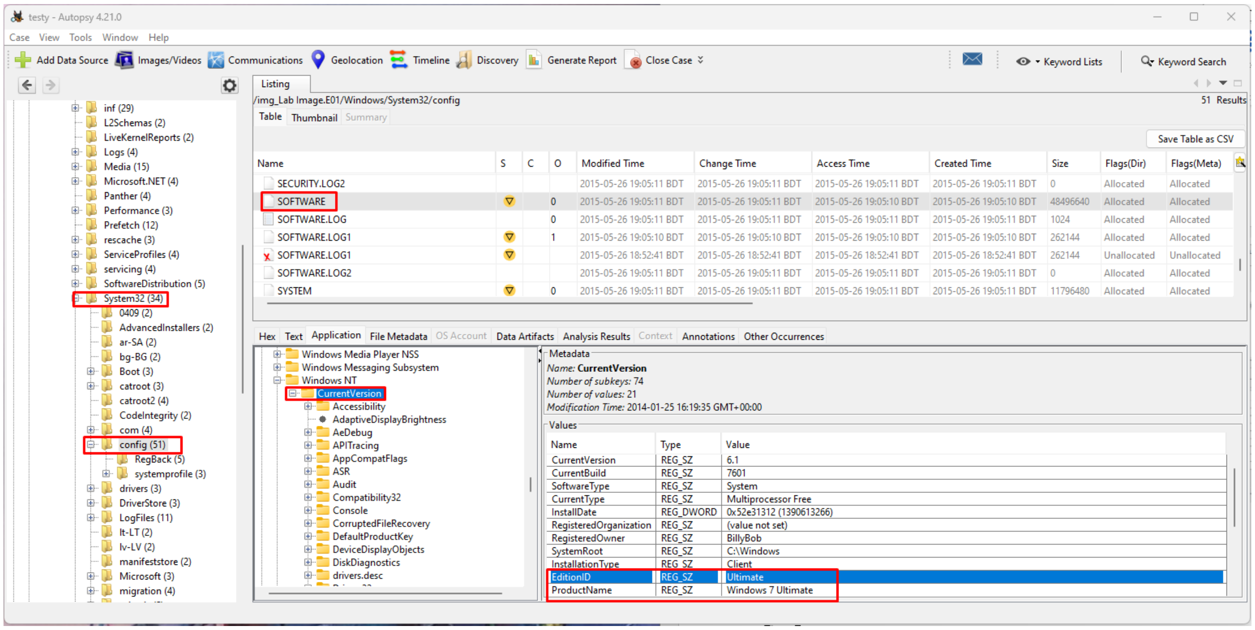
Operating System Information

Type	Value	Source(s)
Name	IACIS-HDD-2014	Recent Activity
Program Name	Windows 7 Ultimate Service Pack 1	Recent Activity
Processor Architecture	AMD64	Recent Activity
Temporary Files Directory	%SystemRoot%\TEMP	Recent Activity
Path	C:\Windows	Recent Activity
Product ID	00426-292-0000007-85946	Recent Activity
Owner	BillyBob	Recent Activity
Source File Path	/img_Lab Image.E01	
Artifact ID	-9223372036854775447	

Or,

/img_Lab Image.E01/WINDOWS/system32/config/

SOFTOWARE > Microsoft > Windows NT > CurrentVersion



/img_Lab Image.E01/Windows/System32/config

51 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
SECURITY.LOG2				2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	0	Allocated	Allocated
SOFTWARE	▽		0	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	48496640	Allocated	Allocated
SOFTWARE.LOG			0	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	1024	Allocated	Allocated
SOFTWARE.LOG1	▽		1	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	262144	Allocated	Allocated
SOFTWARE.LOG1	▽			2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	262144	Unallocated	Unallocated
SOFTWARE.LOG2				2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	0	Allocated	Allocated
SYSTEM	▽		0	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	11796480	Allocated	Allocated

Metadata

Name: **CurrentVersion**
Number of subkeys: 74
Number of values: 21
Modification Time: 2014-01-25 16:19:35 GMT+00:00

Values

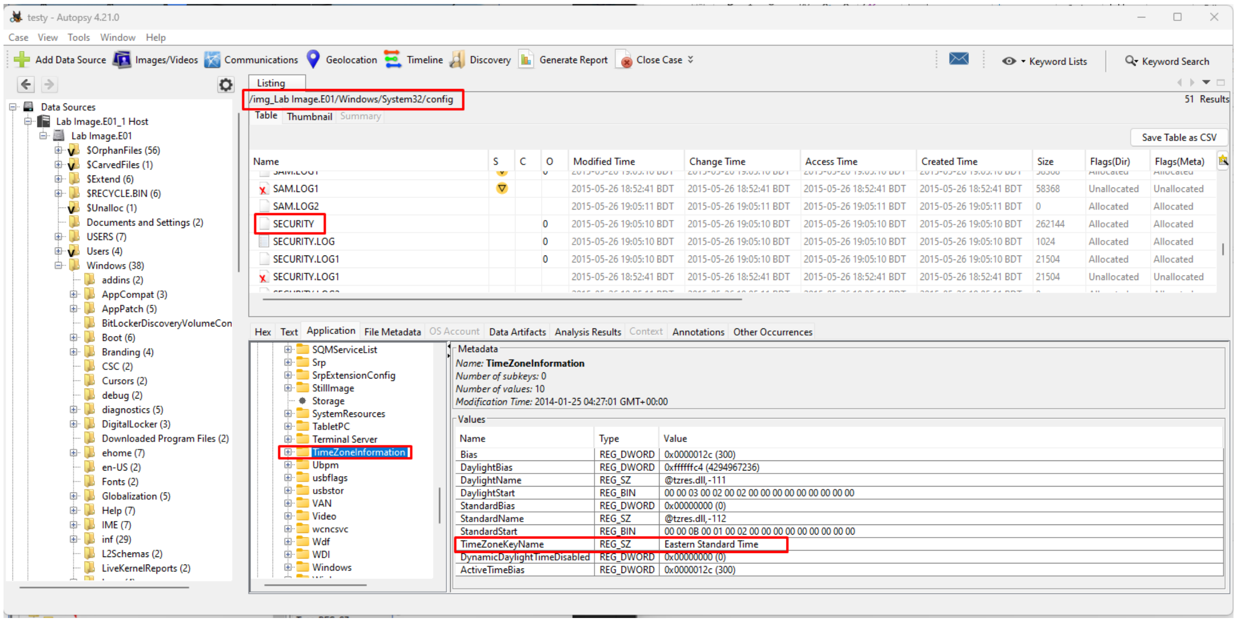
Name	Type	Value
CurrentVersion	REG_SZ	6.1
CurrentBuild	REG_SZ	7601
SoftwareType	REG_SZ	System
CurrentType	REG_SZ	Multiprocessor Free
InstallDate	REG_DWORD	0x52e31312 (1390613266)
RegisteredOrganization	REG_SZ	(value not set)
RegisteredOwner	REG_SZ	BillyBob
SystemRoot	REG_SZ	C:\Windows
InstallationType	REG_SZ	Client
EditionID	REG_SZ	Ultimate
ProductName	REG_SZ	Windows 7 Ultimate

Ans to the Q: No: 3

/img_Lab Image.E01/WINDOWS/system32/config/

SYSTEM > ControlSet001 > Control >TimeZoneInfromation

Time Zone:



/img_Lab Image.E01/Windows/System32/config

51 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
SAM.LOG1	▽			2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	58368	Unallocated	Unallocated
SAM.LOG2				2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	0	Allocated	Allocated
SECURITY			0	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	262144	Allocated	Allocated
SECURITY.LOG			0	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	1024	Allocated	Allocated
SECURITY.LOG1			0	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	21504	Allocated	Allocated
SECURITY.LOG1				2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	21504	Unallocated	Unallocated

Metadata

Name: **TimeZoneInformation**

Number of subkeys: 0

Number of values: 10

Modification Time: 2014-01-25 04:27:01 GMT+00:00

Values

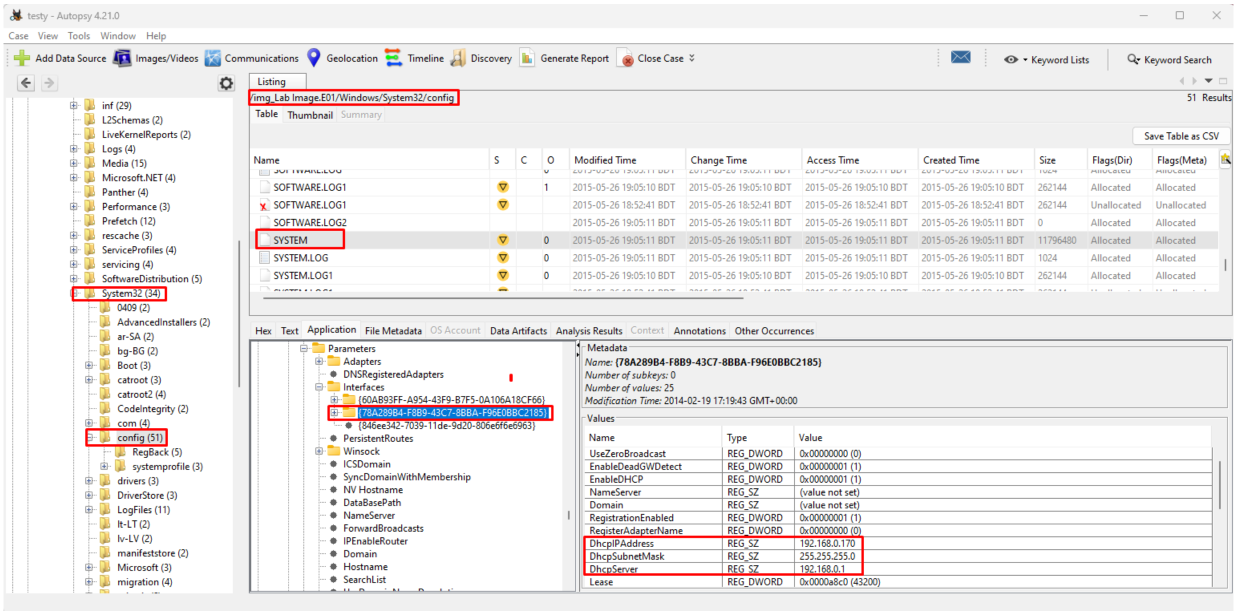
Name	Type	Value
Bias	REG_DWORD	0x0000012c (300)
DaylightBias	REG_DWORD	0xffffffc4 (4294967236)
DaylightName	REG_SZ	@tzres.dll,-111
DaylightStart	REG_BIN	00 00 03 00 02 00 02 00 00 00 00 00 00 00 00 00
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll,-112
StandardStart	REG_BIN	00 00 0B 00 01 00 02 00 00 00 00 00 00 00 00 00
TimeZoneKeyName	REG_SZ	Eastern Standard Time
DynamicDaylightTimeDisabled	REG_DWORD	0x00000000 (0)
ActiveTimeBias	REG_DWORD	0x0000012c (300)

Ans to the Q: No: 4

/img_Lab Image.E01/WINDOWS/system32/config/

SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{GUID}\

IP Address:



/img_Lab Image.E01/Windows/System32/config

51 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
SOFTWARE.LOG1	▽		1	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	262144	Allocated	Allocated
SOFTWARE.LOG1	▽			2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	262144	Unallocated	Unallocated
SOFTWARE.LOG2				2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	0	Allocated	Allocated
SYSTEM	▽		0	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	11796480	Allocated	Allocated
SYSTEM.LOG	▽		0	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	1024	Allocated	Allocated
SYSTEM.LOG1	▽		0	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	262144	Allocated	Allocated

Metadata

Name: **{78A289B4-F8B9-43C7-8BBA-F96E0BBC2185}**
Number of subkeys: 0
Number of values: 25
Modification Time: 2014-02-19 17:19:43 GMT+00:00

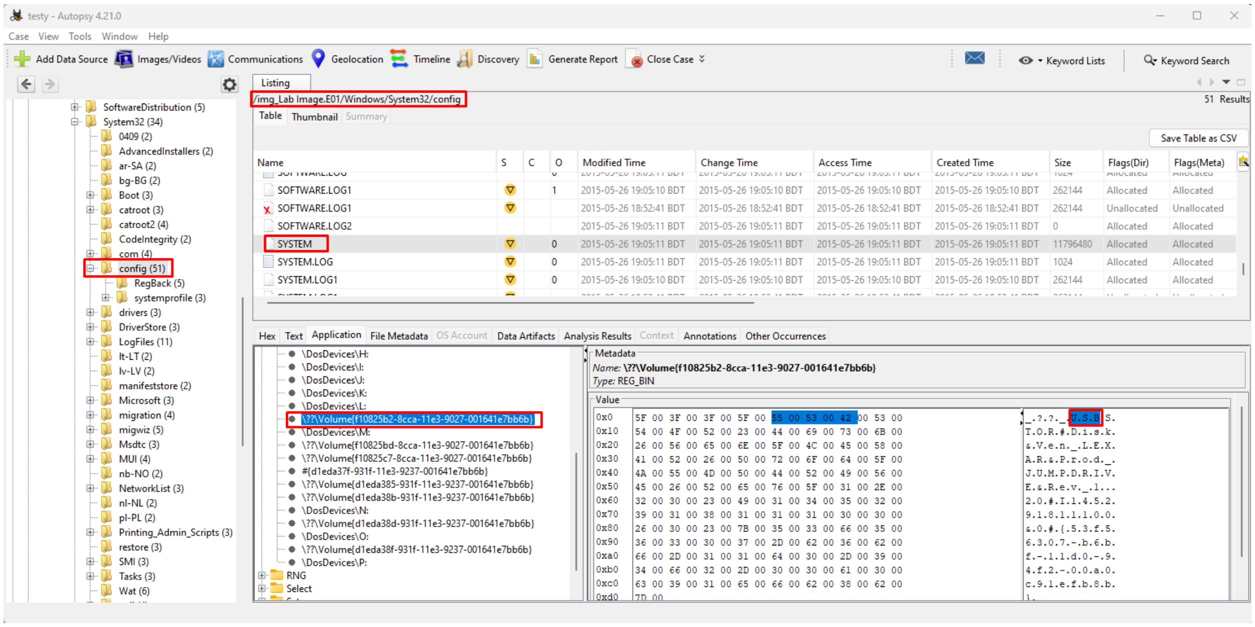
Values

Name	Type	Value
UseZeroBroadcast	REG_DWORD	0x00000000 (0)
EnableDeadGWDetect	REG_DWORD	0x00000001 (1)
EnableDHCP	REG_DWORD	0x00000001 (1)
NameServer	REG_SZ	(value not set)
Domain	REG_SZ	(value not set)
RegistrationEnabled	REG_DWORD	0x00000001 (1)
RegisterAdapterName	REG_DWORD	0x00000000 (0)
DhcpIPAddress	REG_SZ	192.168.0.170
DhcpSubnetMask	REG_SZ	255.255.255.0
DhcpServer	REG_SZ	192.168.0.1
Lease	REG_DWORD	0x0000a8c0 (43200)

Ans to the Q: No: 5

/img_Lab Image.E01/WINDOWS/system32/config/

SYSTEM\MountedDevices


testy - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Listing
Table Thumbnail Summary
Save Table as CSV
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
SoftwareDistribution (5)
System32 (34)
0409 (2)
AdvancedInstallers (2)
ar-SA (2)
bg-BG (2)
Boot (3)
catroot (3)
catroot2 (4)
CodeIntegrity (2)
com (4)
config (51)
RegBack (5)
systemprofile (3)
drivers (3)
DriverStore (3)
LogFiles (11)
lt-LT (2)
lv-LV (2)
manifeststore (2)
Microsoft (3)
migration (4)
migwiz (5)
Msdtc (3)
MUI (4)
nb-NO (2)
NetworkList (3)
nl-NL (2)
pl-PL (2)
Printing_Admin_Scripts (3)
restore (3)
SMI (3)
Tasks (3)
Wat (6)
\DosDevices\H:
\DosDevices\I:
\DosDevices\J:
\DosDevices\K:
\DosDevices\L:
\??\Volume{f10825b2-8cca-11e3-9027-001641e7bb6b}
\DosDevices\M:
\??\Volume{f10825bd-8cca-11e3-9027-001641e7bb6b}
\??\Volume{f10825c7-8cca-11e3-9027-001641e7bb6b}
#{d1eda37f-931f-11e3-9237-001641e7bb6b}
\??\Volume{d1eda385-931f-11e3-9237-001641e7bb6b}
\??\Volume{d1eda38b-931f-11e3-9237-001641e7bb6b}
\DosDevices\N:
\??\Volume{d1eda38d-931f-11e3-9237-001641e7bb6b}
\DosDevices\O:
\??\Volume{d1eda38f-931f-11e3-9237-001641e7bb6b}
\DosDevices\P:
RNG
Select

/img_Lab Image.E01/Windows/System32/config

51 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
SOFTWARE.LOG1	▽		1	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	262144	Allocated	Allocated
SOFTWARE.LOG1	▽			2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	262144	Unallocated	Unallocated
SOFTWARE.LOG2				2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	0	Allocated	Allocated
SYSTEM	▽		0	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	11796480	Allocated	Allocated
SYSTEM.LOG	▽		0	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	1024	Allocated	Allocated
SYSTEM.LOG1	▽		0	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	262144	Allocated	Allocated

Metadata

Name: **\??\Volume{f10825b2-8cca-11e3-9027-001641e7bb6b}**
Type: REG_BIN

Value

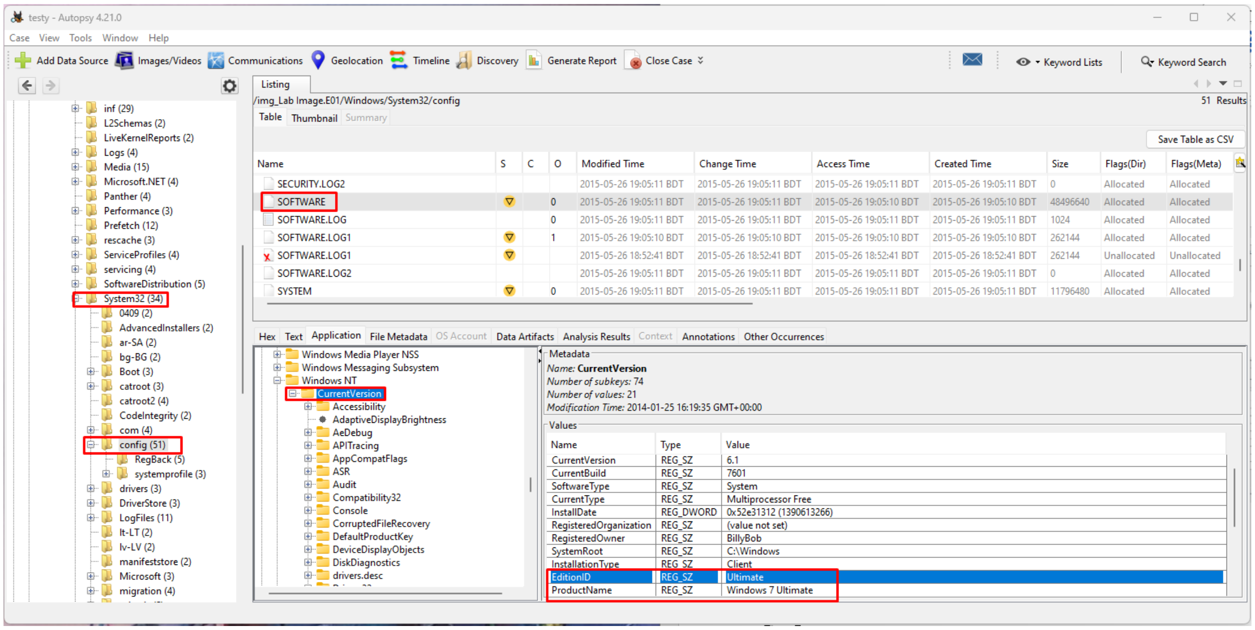
```
0x0   5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00   _.?.?._.U.S.B.S.
0x10  54 00 4F 00 52 00 23 00 44 00 69 00 73 00 6B 00   T.O.R.#.D.i.s.k.
0x20  26 00 56 00 65 00 6E 00 5F 00 4C 00 45 00 58 00   &.V.e.n._.L.E.X.
0x30  41 00 52 00 26 00 50 00 72 00 6F 00 64 00 5F 00   A.R.&.P.r.o.d._.
0x40  4A 00 55 00 4D 00 50 00 44 00 52 00 49 00 56 00   J.U.M.P.D.R.I.V.
0x50  45 00 26 00 52 00 65 00 76 00 5F 00 31 00 2E 00   E.&.R.e.v._.1...
0x60  32 00 30 00 23 00 49 00 31 00 34 00 35 00 32 00   2.0.#.I.1.4.5.2.
0x70  39 00 31 00 38 00 31 00 31 00 31 00 30 00 30 00   9.1.8.1.1.1.0.0.
0x80  26 00 30 00 23 00 7B 00 35 00 33 00 66 00 35 00   &.0.#.{.5.3.f.5.
0x90  36 00 33 00 30 00 37 00 2D 00 62 00 36 00 62 00   6.3.0.7.-.b.6.b.
0xa0  66 00 2D 00 31 00 31 00 64 00 30 00 2D 00 39 00   f.-.1.1.d.0.-.9.
0xb0  34 00 66 00 32 00 2D 00 30 00 30 00 61 00 30 00   4.f.2.-.0.0.a.0.
0xc0  63 00 39 00 31 00 65 00 66 00 62 00 38 00 62 00   c.9.1.e.f.b.8.b.
0xd0  7D 00                                              }.
```

More:

Operating System:

/img_Lab Image.E01/WINDOWS/system32/config/

SOFTWARE > Microsoft > Windows NT > Current Version



/img_Lab Image.E01/Windows/System32/config — 51 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
SECURITY.LOG2				2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	0	Allocated	Allocated
SOFTWARE	▽		0	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	48496640	Allocated	Allocated
SOFTWARE.LOG			0	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	1024	Allocated	Allocated
SOFTWARE.LOG1	▽		1	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	262144	Allocated	Allocated
SOFTWARE.LOG1	▽			2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	262144	Unallocated	Unallocated
SOFTWARE.LOG2				2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	0	Allocated	Allocated
SYSTEM	▽		0	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	11796480	Allocated	Allocated

Metadata

Name: **CurrentVersion**
Number of subkeys: 74
Number of values: 21
Modification Time: 2014-01-25 16:19:35 GMT+00:00

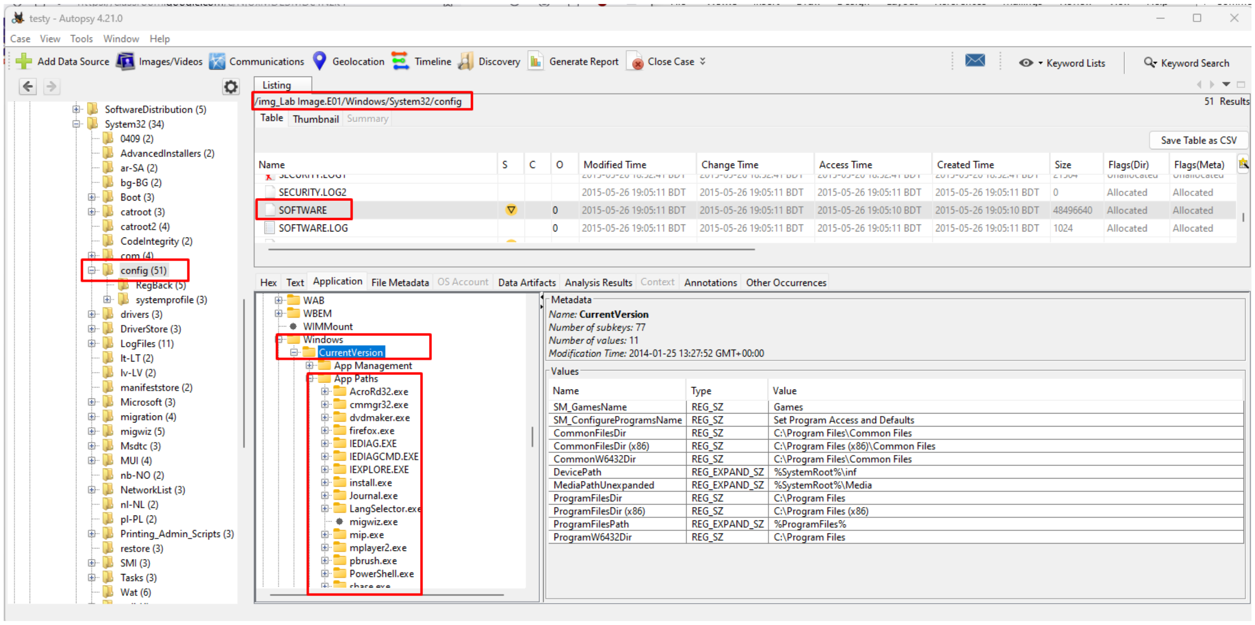
Values

Name	Type	Value
CurrentVersion	REG_SZ	6.1
CurrentBuild	REG_SZ	7601
SoftwareType	REG_SZ	System
CurrentType	REG_SZ	Multiprocessor Free
InstallDate	REG_DWORD	0x52e31312 (1390613266)
RegisteredOrganization	REG_SZ	(value not set)
RegisteredOwner	REG_SZ	BillyBob
SystemRoot	REG_SZ	C:\Windows
InstallationType	REG_SZ	Client
EditionID	REG_SZ	Ultimate
ProductName	REG_SZ	Windows 7 Ultimate

Installed Applications:

/img_Lab Image.E01/WINDOWS/system32/config/

SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths



/img_Lab Image.E01/Windows/System32/config — 51 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
SECURITY.LOG2				2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	0	Allocated	Allocated
SOFTWARE	▽		0	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	48496640	Allocated	Allocated
SOFTWARE.LOG			0	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	1024	Allocated	Allocated

Metadata

Name: **CurrentVersion**
Number of subkeys: 77
Number of values: 11
Modification Time: 2014-01-25 13:27:52 GMT+00:00

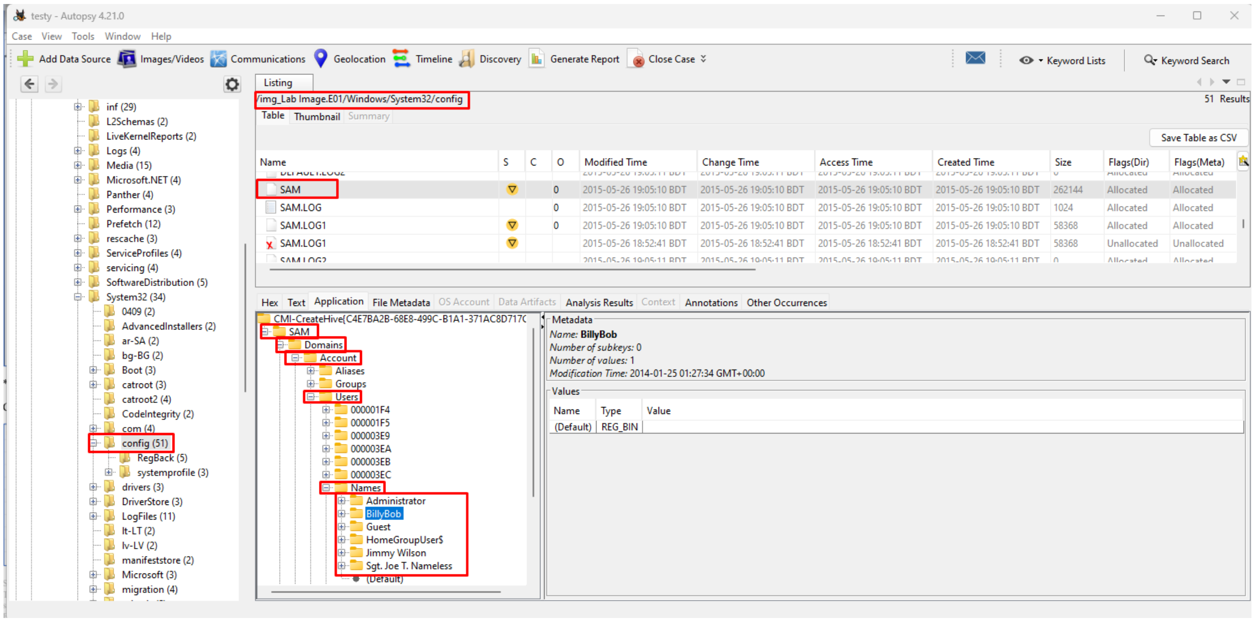
Values

Name	Type	Value
SM_GamesName	REG_SZ	Games
SM_ConfigureProgramsName	REG_SZ	Set Program Access and Defaults
CommonFilesDir	REG_SZ	C:\Program Files\Common Files
CommonFilesDir (x86)	REG_SZ	C:\Program Files (x86)\Common Files
CommonW6432Dir	REG_SZ	C:\Program Files\Common Files
DevicePath	REG_EXPAND_SZ	%SystemRoot%\inf
MediaPathUnexpanded	REG_EXPAND_SZ	%SystemRoot%\Media
ProgramFilesDir	REG_SZ	C:\Program Files
ProgramFilesDir (x86)	REG_SZ	C:\Program Files (x86)
ProgramFilesPath	REG_EXPAND_SZ	%ProgramFiles%
ProgramW6432Dir	REG_SZ	C:\Program Files

SAM (Security Accounts Manager):

/img_Lab Image.E01/WINDOWS/system32/config/

SAM/Domains/Account/Users/Names/



/img_Lab Image.E01/Windows/System32/config

51 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
SAM	▽		0	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	262144	Allocated	Allocated
SAM.LOG			0	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	1024	Allocated	Allocated
SAM.LOG1	▽		0	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	2015-05-26 19:05:10 BDT	58368	Allocated	Allocated
SAM.LOG1	▽			2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	2015-05-26 18:52:41 BDT	58368	Unallocated	Unallocated
SAM.LOG2				2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	2015-05-26 19:05:11 BDT	0	Allocated	Allocated

Metadata
Name: **BillyBob**
Number of subkeys: 0
Number of values: 1
Modification Time: 2014-01-25 01:27:34 GMT+00:00

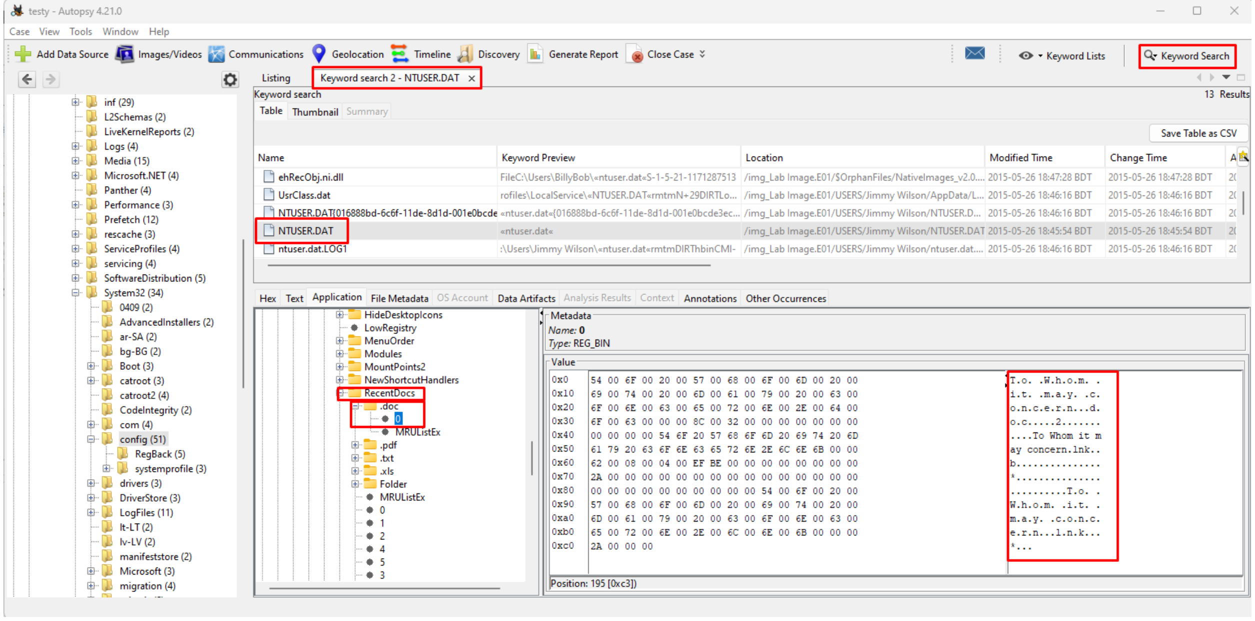
Values

Name	Type	Value
(Default)	REG_BIN	

<u>Recent documents:</u> Search keyword > NTUSER.DAT

/img_Lab Image.E01/WINDOWS/system32/config/

NTUSER.DAT/Software/Microsoft/Windows/CurrentVersion/Explorer/RecentDocs/



Keyword search

13 Results

Name	Keyword Preview	Location	Modified Time	Change Time
ehRecObj.ni.dll	FileC:\Users\BillyBob\«ntuser.dat«S-1-5-21-1171287513	/img_Lab Image.E01/$OrphanFiles/NativeImages_v2.0....	2015-05-26 18:47:28 BDT	2015-05-26 18:47:28 BDT
UsrClass.dat	rofiles\LocalService\«NTUSER.DAT«rmtmN+29DIRTLo...	/img_Lab Image.E01/USERS/Jimmy Wilson/AppData/L...	2015-05-26 18:46:16 BDT	2015-05-26 18:46:16 BDT
NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde	«ntuser.dat«{016888bd-6c6f-11de-8d1d-001e0bcde3ec...	/img_Lab Image.E01/USERS/Jimmy Wilson/NTUSER.D...	2015-05-26 18:46:16 BDT	2015-05-26 18:46:16 BDT
NTUSER.DAT	«ntuser.dat«	/img_Lab Image.E01/USERS/Jimmy Wilson/NTUSER.DAT	2015-05-26 18:45:54 BDT	2015-05-26 18:45:54 BDT
ntuser.dat.LOG1	:\Users\Jimmy Wilson\«ntuser.dat«rmtmDIRThbinCMI-	/img_Lab Image.E01/USERS/Jimmy Wilson/ntuser.dat....	2015-05-26 18:46:16 BDT	2015-05-26 18:46:16 BDT

Metadata
Name: **0**
Type: REG_BIN

Value

```
0x0   54 00 6F 00 20 00 57 00 68 00 6F 00 6D 00 20 00   T.o. .W.h.o.m. .
0x10  69 00 74 00 20 00 6D 00 61 00 79 00 20 00 63 00   i.t. .m.a.y. .c.
0x20  6F 00 6E 00 63 00 65 00 72 00 6E 00 2E 00 64 00   o.n.c.e.r.n...d.
0x30  6F 00 63 00 00 00 8C 00 32 00 00 00 00 00 00 00   o.c.....2.......
0x40  00 00 00 00 54 6F 20 57 68 6F 6D 20 69 74 20 6D   ....To Whom it m
0x50  61 79 20 63 6F 6E 63 65 72 6E 2E 6C 6E 6B 00 00   ay concern.lnk..
0x60  62 00 08 00 04 00 EF BE 00 00 00 00 00 00 00 00   b...............
0x70  2A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   *...............
0x80  00 00 00 00 00 00 00 00 00 00 54 00 6F 00 20 00   ..........T.o. .
0x90  57 00 68 00 6F 00 6D 00 20 00 69 00 74 00 20 00   W.h.o.m. .i.t. .
0xa0  6D 00 61 00 79 00 20 00 63 00 6F 00 6E 00 63 00   m.a.y. .c.o.n.c.
0xb0  65 00 72 00 6E 00 2E 00 6C 00 6E 00 6B 00 00 00   e.r.n...l.n.k...
0xc0  2A 00 00 00                                       *...
```

Position: 195 [0xc3])

Questions?

- **BillyBob user account creation date?**
- **BillyBob last login time?**
- **Did BillyBob try to reset the password of the other user?**

The location of the Event Logs:
WINDOWS\system32\winevt\Logs