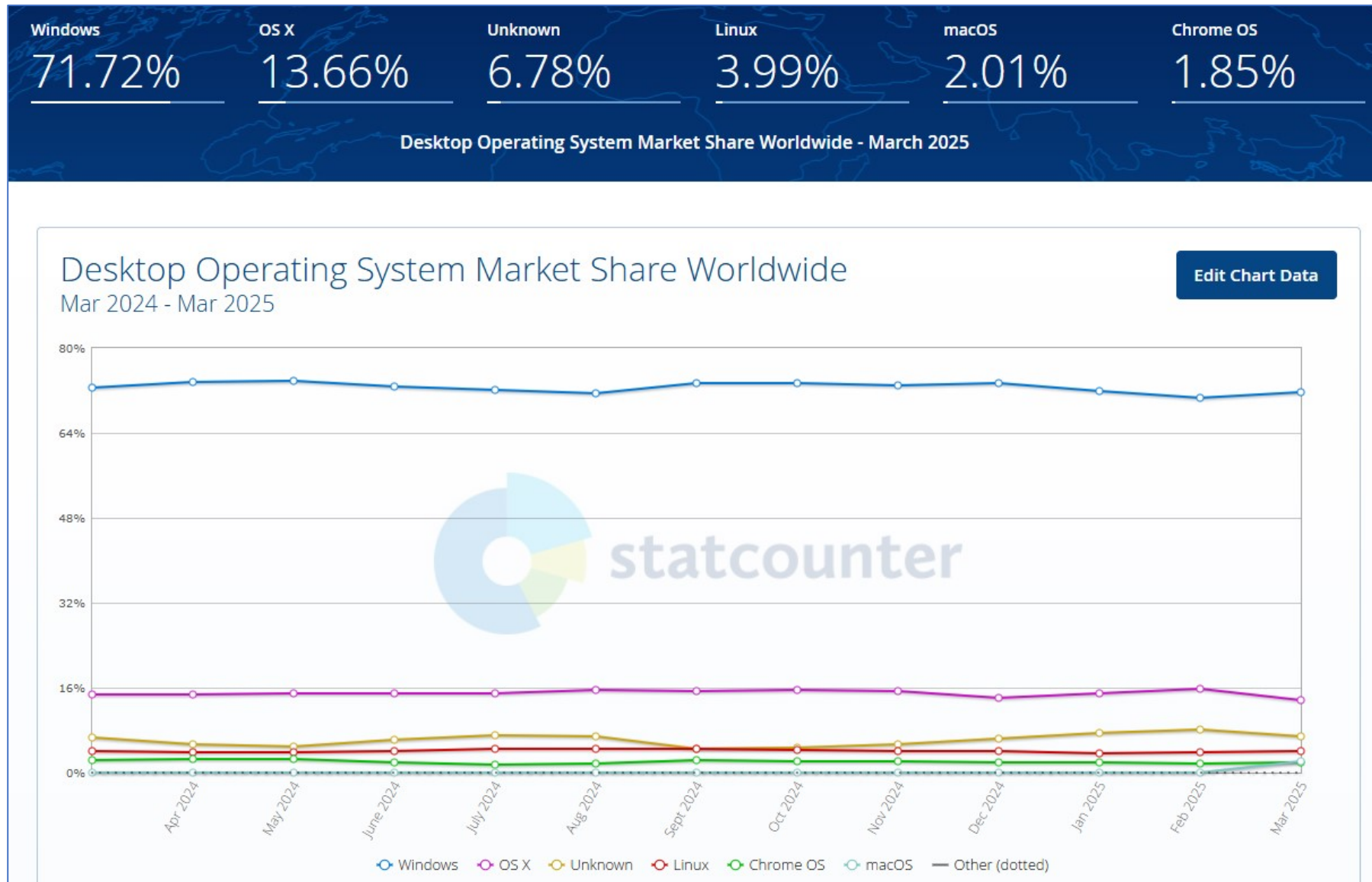


Windows Forensics

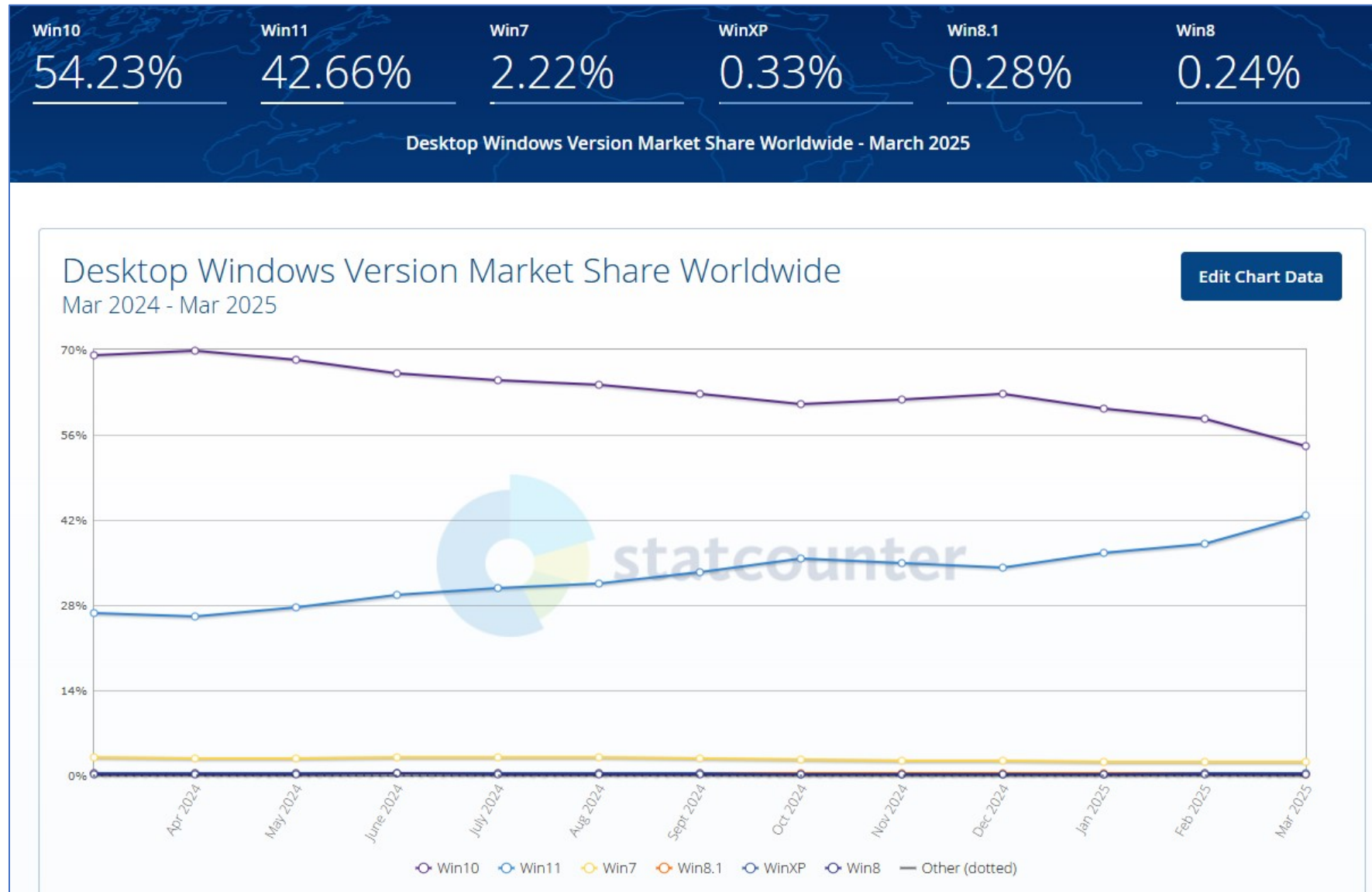
Digital Forensics

University of Genoa 2025

Why Windows Forensics?



Why Windows Forensics?



Requirements

- **Exterro FTK Imager 4.7.3.81**
<https://www.exterro.com/digital-forensics-software/ftk-imager>
- **Arsenal Image Mounter**
<https://arsenalrecon.com/downloads/>
- **Eric Zimmerman's tools**
<https://ericzimmerman.github.io/>
- **Hindsight**
<https://github.com/obsidianforensics/hindsight>

OWL Traffick case

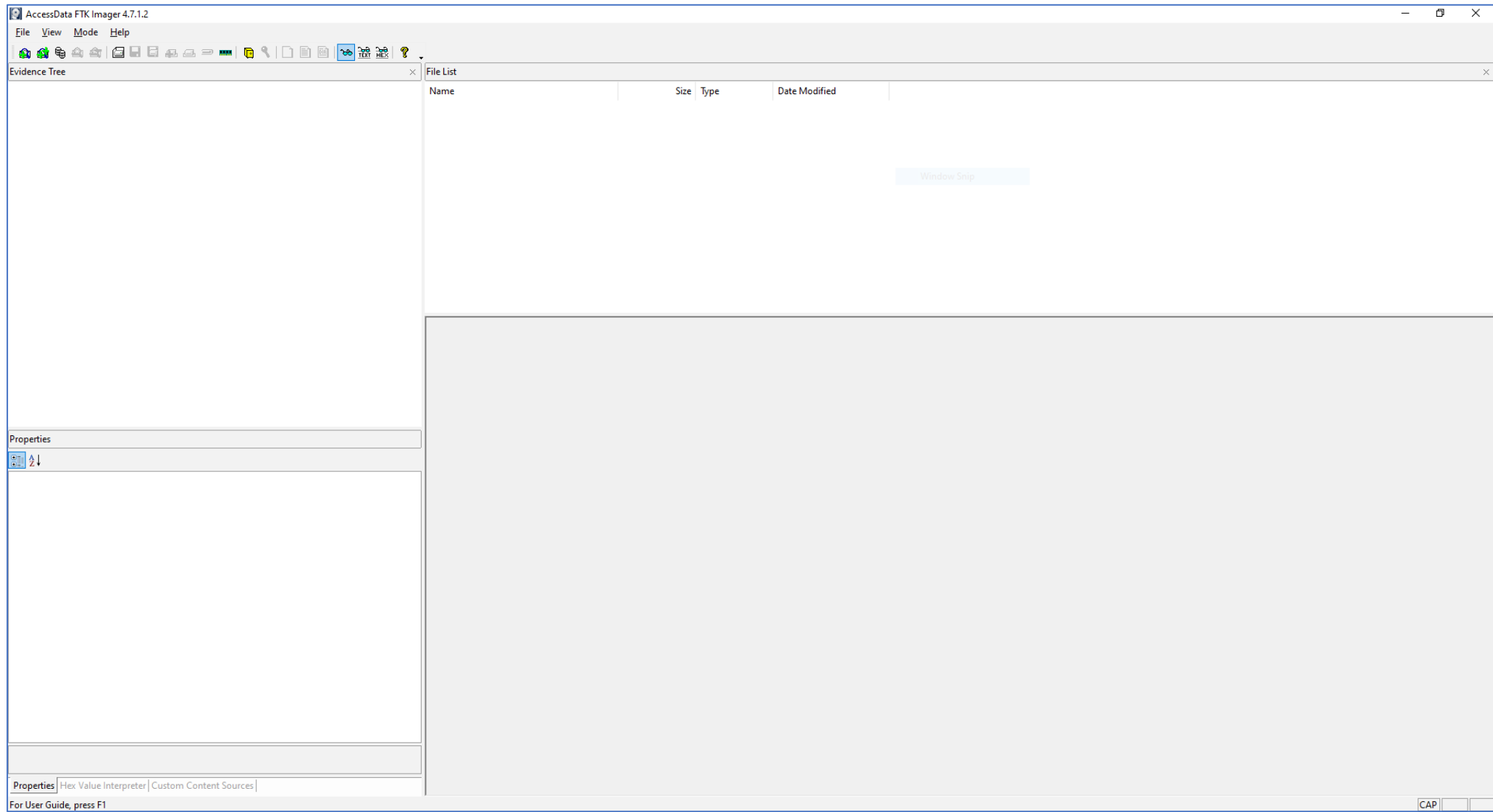
Scenario

In a jurisdiction where Owls are illegal to trade and buy, two users are discussing the illegal trade of owls. The computer and mobile device taken into evidence are of a user who is attempting to purchase owls illegally. The user has contacted another user who can provide an owl in exchange for cash. An owl is decided upon, and an exchange is scheduled. After the exchange, a communication message is sent confirming the owl purchase has been completed.

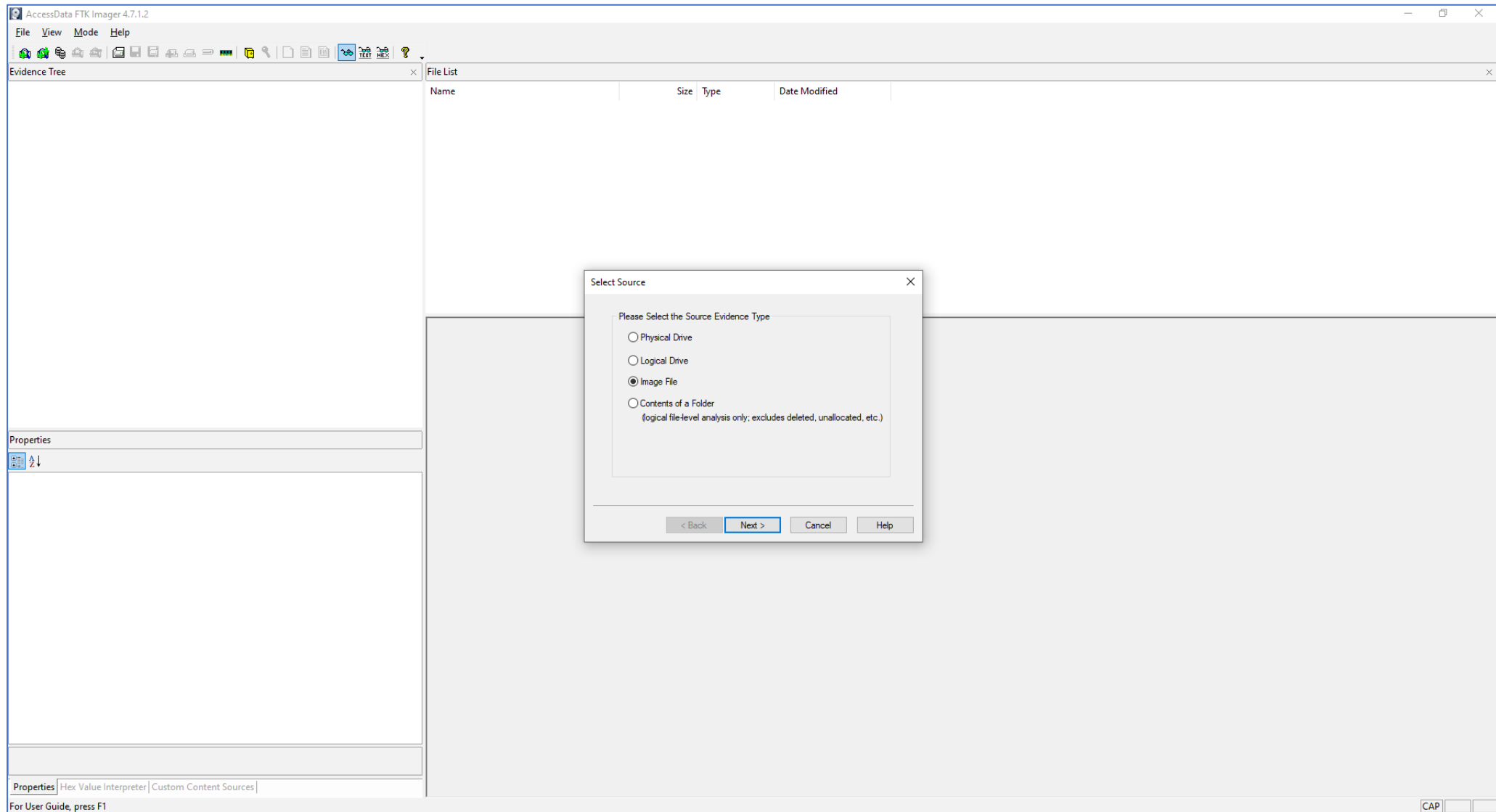
HD1.zip	67,374,178,318	2020-11-22 11:52:58Z
Nexus5-Full.zip	1,922,857,615	2020-11-22 11:54:12Z



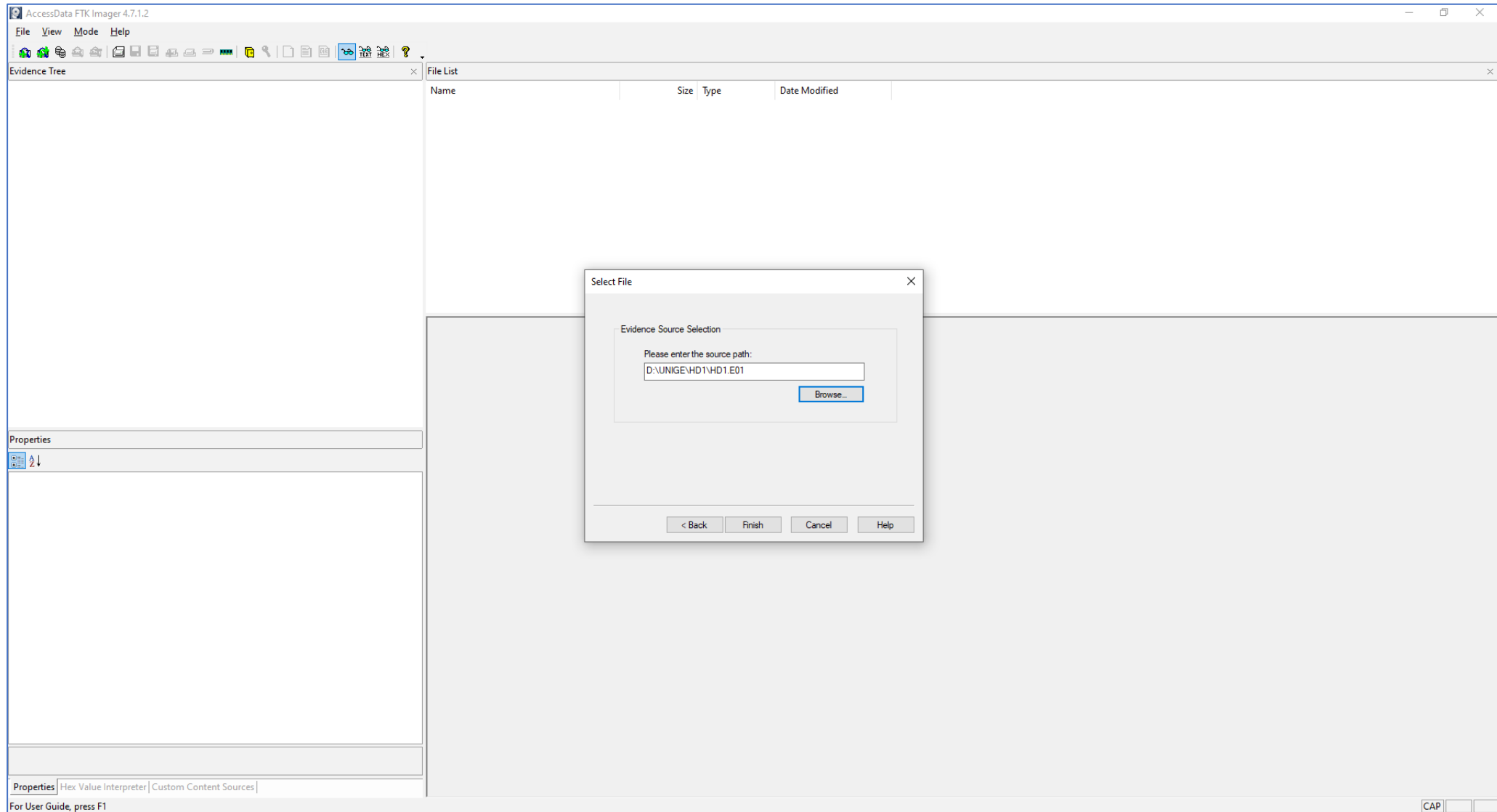
AccessData FTK Imager



AccessData FTK Imager



AccessData FTK Imager



AccessData FTK Imager

The screenshot displays the AccessData FTK Imager 4.7.1.2 interface. The main window is divided into three primary sections: the Evidence Tree on the left, the File List in the center, and the Properties panel at the bottom left.

Evidence Tree: Shows the hierarchical structure of the image. The selected path is HD1.E01 > Basic data partition (3) [459432MB] > Windows [NTFS] > [root] > \$UpCase.

File List: A table listing files and directories found in the selected location. The table has columns for Name, Size, Type, and Date Modified.

Name	Size	Type	Date Modified
\$Extend		1 Directory	27/01/2017 00:06:48
\$GetCurrent		1 Directory	26/01/2017 23:57:23
\$RECYCLE.BIN		1 Directory	27/01/2017 00:35:45
\$WINDOWS--BT		1 Directory	27/01/2017 01:50:51
Documents and Settings		1 Reparse Point	04/11/2015 01:37:52
hp		1 Directory	27/01/2017 00:53:35
inetpub		1 Directory	27/01/2017 05:09:55
Intel		1 Directory	27/01/2017 00:58:03
PerfLogs		1 Directory	16/07/2016 11:47:47
Program Files		1 Directory	27/01/2017 02:45:59
Program Files (x86)		1 Directory	27/01/2017 02:46:02
ProgramData		1 Directory	27/01/2017 16:57:23
Recovery		1 Directory	27/01/2017 02:43:18
SWSETUP		1 Directory	26/01/2017 23:44:38
System Volume Information		1 Directory	06/02/2017 19:19:25
SYSTEM.SAV		1 Directory	26/01/2017 23:44:38
Temp		1 Directory	27/01/2017 01:20:43
Users		1 Directory	27/01/2017 02:46:07
Windows		1 Directory	27/01/2017 02:56:28
Windows.old		1 Directory	27/01/2017 05:27:29
Windows10Upgrade		1 Directory	26/01/2017 23:58:49
\$AttrDef	3	Regular File	27/01/2017 00:06:48
\$BadClus	0	Regular File	27/01/2017 00:06:48
\$Bitmap	14,358	Regular File	27/01/2017 00:06:48
\$Boot	8	Regular File	27/01/2017 00:06:48
\$I30	8	NTFS Index All...	30/01/2017 18:47:50
\$LogFile	65,536	Regular File	27/01/2017 00:06:48
\$MFT	343,040	Regular File	27/01/2017 00:06:48
\$MFTMirr	4	Regular File	27/01/2017 00:06:48
\$Secure	1	Regular File	27/01/2017 00:06:48
\$TXF_DATA	1	NTFS Logged ...	30/01/2017 18:47:50
\$UpCase	128	Regular File	27/01/2017 00:06:48
\$Volume	0	Regular File	27/01/2017 00:06:48
BNB15WWAVAT602.ini		\$I30 INDX Entry	
hiberfil.sys	8,266,340	Regular File	07/02/2017 14:01:38
OS	0	Regular File	27/01/2017 00:21:12
pagefile.sys	1,310,720	Regular File	07/02/2017 14:01:40
swapfile.sys	262,144	Regular File	07/02/2017 14:01:40

Properties Panel: Displays details for the selected file, \$UpCase.

Property	Value
Name	\$UpCase
File Class	Regular File
File Size	131,072
Physical Size	131,072
Start Cluster	3
Date Accessed	27/01/2017 00:06:48
Date Created	27/01/2017 00:06:48
Date Modified	27/01/2017 00:06:48

The bottom status bar indicates: Listed: 38 Selected: 1 HD1.E01/Basic data partition (3) [459432MB]/Windows [NTFS]/[root]/\$UpCase

Windows OS – Folder structure

- **Root folder**

- Hiberfil.sys
- Pagefile.sys

- **“Program Files” and “Program Files (x86)” folders**

- Installed applications
- Sometimes applications data

- **“Users” folder**

- One folder for each user
- User Registry
- User data
- User configuration
- Apps configuration

- **“Windows” folder**

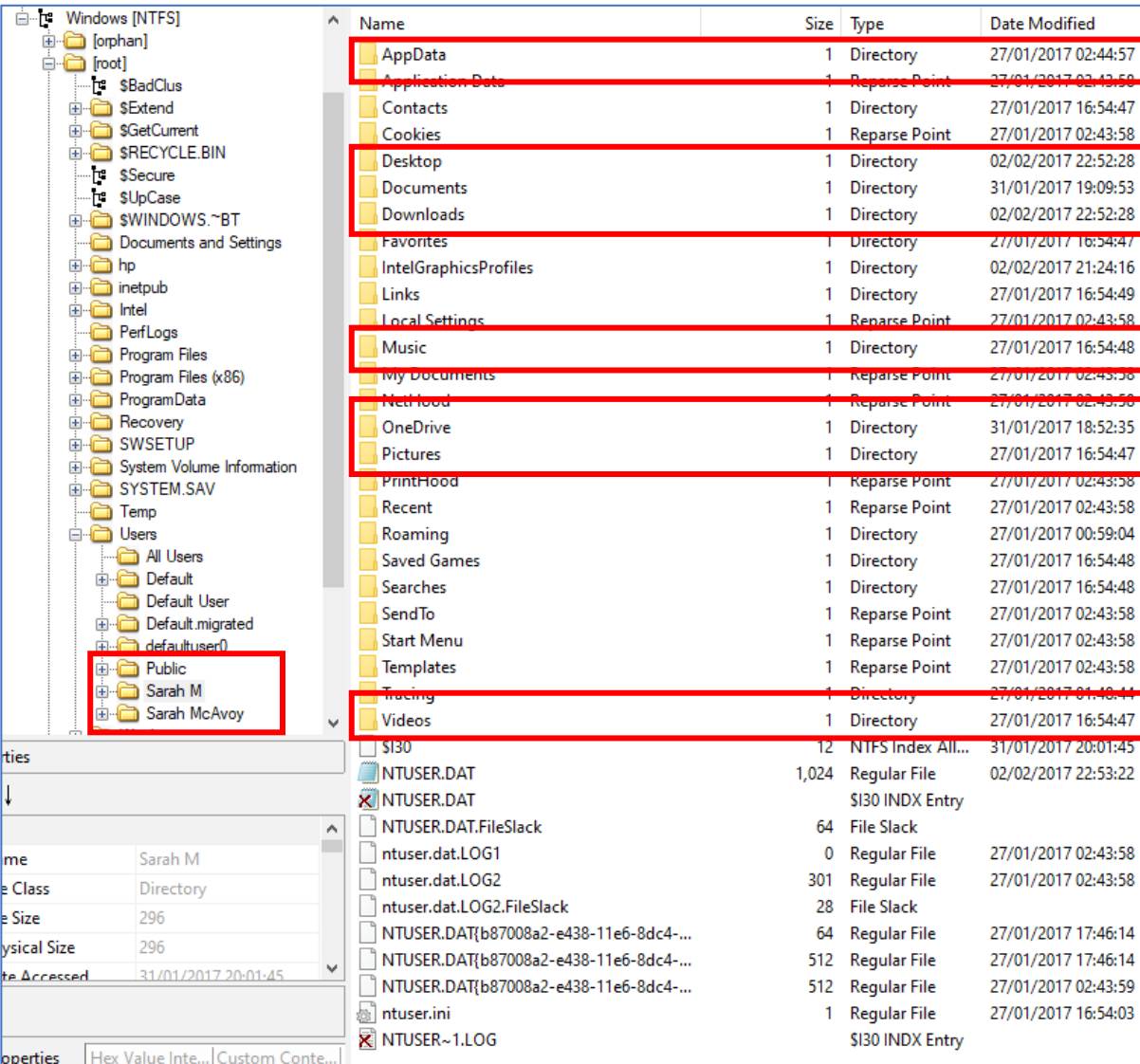
- Operating system exe/dll
- Windows System Registry
- Windows Events
- ...

Name	Size	Type	Date modified
\$Extend	1	Directory	27/01/2017 00:06:48
\$GetCurrent	1	Directory	26/01/2017 23:57:23
\$RECYCLE.BIN	1	Directory	27/01/2017 00:35:45
\$WINDOWS.~BT	1	Directory	27/01/2017 01:50:51
Documents and Settings	1	Reparse Point	04/11/2015 01:37:52
hp	1	Directory	27/01/2017 00:53:35
inetpub	1	Directory	27/01/2017 05:09:55
Intel	1	Directory	27/01/2017 00:58:03
PerfLogs	1	Directory	16/07/2016 11:47:47
Program Files	1	Directory	27/01/2017 02:45:59
Program Files (x86)	1	Directory	27/01/2017 02:46:02
ProgramData	1	Directory	27/01/2017 16:57:23
Recovery	1	Directory	27/01/2017 02:43:18
SWSETUP	1	Directory	26/01/2017 23:44:38
System Volume Information	1	Directory	06/02/2017 19:19:25
SYSTEM.SAV	1	Directory	26/01/2017 23:44:38
Temp	1	Directory	27/01/2017 01:20:43
Users	1	Directory	27/01/2017 02:46:07
Windows	1	Directory	27/01/2017 02:56:28
Windows.old	1	Directory	27/01/2017 05:27:29
Windows10Upgrade	1	Directory	26/01/2017 23:58:49
\$AttrDef	3	Regular File	27/01/2017 00:06:48
\$BadClus	0	Regular File	27/01/2017 00:06:48
\$Bitmap	14,358	Regular File	27/01/2017 00:06:48
\$Boot	8	Regular File	27/01/2017 00:06:48
\$I30	8	NTFS Index All...	30/01/2017 18:47:50
\$LogFile	65,536	Regular File	27/01/2017 00:06:48
\$MFT	343,040	Regular File	27/01/2017 00:06:48
\$MFTMirr	4	Regular File	27/01/2017 00:06:48
\$Secure	1	Regular File	27/01/2017 00:06:48
\$TXF_DATA	1	NTFS Logged ...	30/01/2017 18:47:50
\$UpCase	128	Regular File	27/01/2017 00:06:48
\$Volume	0	Regular File	27/01/2017 00:06:48
\$BNT15M0WAVAT602.ini		\$I30 INDX Entry	
hiberfil.sys	8,266,340	Regular File	07/02/2017 14:01:38
OS	0	Regular File	27/01/2017 00:21:12
pagefile.sys	1,310,720	Regular File	07/02/2017 14:01:40
swapfile.sys	262,144	Regular File	07/02/2017 14:01:40

Name	\$UpCase
File Class	Regular File
File Size	131,072
Physical Size	131,072
Start Cluster	3

Windows OS – User Folder structure

- **AppData**
 - Apps configuration
 - Apps data
 - User data
 - A LOT!
- **Contacts**
- **Desktop**
- **Downloads**
- **Music**
- **OneDrive**
- **Pictures**
- **Videos**



Name	Size	Type	Date Modified
AppData	1	Directory	27/01/2017 02:44:57
Application Data	1	Reparse Point	27/01/2017 02:43:58
Contacts	1	Directory	27/01/2017 16:54:47
Cookies	1	Reparse Point	27/01/2017 02:43:58
Desktop	1	Directory	02/02/2017 22:52:28
Documents	1	Directory	31/01/2017 19:09:53
Downloads	1	Directory	02/02/2017 22:52:28
Favorites	1	Directory	27/01/2017 16:54:47
IntelGraphicsProfiles	1	Directory	02/02/2017 21:24:16
Links	1	Directory	27/01/2017 16:54:49
Local Settings	1	Reparse Point	27/01/2017 02:43:58
Music	1	Directory	27/01/2017 16:54:48
My Documents	1	Reparse Point	27/01/2017 02:43:58
NetHood	1	Reparse Point	27/01/2017 02:43:58
OneDrive	1	Directory	31/01/2017 18:52:35
Pictures	1	Directory	27/01/2017 16:54:47
PrintHood	1	Reparse Point	27/01/2017 02:43:58
Recent	1	Reparse Point	27/01/2017 02:43:58
Roaming	1	Directory	27/01/2017 00:59:04
Saved Games	1	Directory	27/01/2017 16:54:48
Searches	1	Directory	27/01/2017 16:54:48
SendTo	1	Reparse Point	27/01/2017 02:43:58
Start Menu	1	Reparse Point	27/01/2017 02:43:58
Templates	1	Reparse Point	27/01/2017 02:43:58
Tracing	1	Directory	27/01/2017 01:48:11
Videos	1	Directory	27/01/2017 16:54:47
\$I30	12	NTFS Index All...	31/01/2017 20:01:45
NTUSER.DAT	1,024	Regular File	02/02/2017 22:53:22
NTUSER.DAT		\$I30 INDX Entry	
NTUSER.DAT.FileSlack	64	File Slack	
ntuser.dat.LOG1	0	Regular File	27/01/2017 02:43:58
ntuser.dat.LOG2	301	Regular File	27/01/2017 02:43:58
ntuser.dat.LOG2.FileSlack	28	File Slack	
NTUSER.DAT{b87008a2-e438-11e6-8dc4-...}	64	Regular File	27/01/2017 17:46:14
NTUSER.DAT{b87008a2-e438-11e6-8dc4-...}	512	Regular File	27/01/2017 17:46:14
NTUSER.DAT{b87008a2-e438-11e6-8dc4-...}	512	Regular File	27/01/2017 02:43:59
ntuser.ini	1	Regular File	27/01/2017 16:54:03
NTUSER~1.LOG		\$I30 INDX Entry	

DEMO and EXERCISE 1

Opening and browsing an image with FTK Imager

Exercise 1

1. Examine the content of the “**Desktop**”, “**Documents**” and “**Downloads**” folder of the **Sarah M** user. Which files are potentially relevant for our case?
2. Examine the content of the “**Downloads**” folder of the **Sarah M** user. Which setup files can you find? Which is potentially relevant for our case?

Exercise 1.1

AccessData FTK Imager 4.7.1.2

File View Mode Help

Evidence Tree

- Sarah M
 - AppData
 - Application Data
 - Contacts
 - Cookies
 - Desktop
 - pets
 - Snowy Owl 2.jpg
 - Snowy Owl 3.jpg
 - Snowy Owl 4.jpg
 - Snowy Owl.jpg
 - what is this_files
 - WOLF Awsome_files
 - Documents
 - Downloads
 - Favorites
 - IntelGraphicsProfiles
 - Links
 - Local Settings
 - Music
 - My Documents
 - NetHood
 - OneDrive
 - Pictures
 - PrintHood
 - Recent
 - Roaming
 - Saved Games

File List

Name	Size	Type	Date Modified
\$I30	4	NTFS Index All...	27/01/2017 17:35:45
Snowy Owl 2.jpg	10	Regular File	27/01/2017 17:33:22
Snowy Owl 3.jpg	74	Regular File	27/01/2017 17:33:24
Snowy Owl 4.jpg	3,415	Regular File	27/01/2017 17:33:24
Snowy Owl.jpg	5,810	Regular File	27/01/2017 17:19:18

00	30	00	00	00	01	00	00	00-00	10	00	00	01	00	00	00	0
10	10	00	00	00	28	00	00	00-28	00	00	00	01	00	00	00	 (... (.....
20	00	00	00	00	00	00	00	00-18	00	00	00	03	00	00	00	
30	00	00	00	00	00	00	00	00-								

Exercise 1.1

AccessData FTK Imager 4.7.1.2

File View Mode Help

Evidence Tree

- Documents
 - hp.applications.package.appdata
 - hp.system.package.metadata
 - My Music
 - My Pictures
 - My Videos
 - New Pet Care
 - Owl_Emergency_Care.pdf
 - Owl_Keeping.pdf
 - Sightings2005 (1).xls
 - Snowy_Owl.pdf
 - Owl_Keeping.pdf
- Downloads
- Favorites
- IntelGraphicsProfiles
- Links
- Local Settings
- Music
- My Documents
- NetHood
- OneDrive
- Pictures
- PrintHood
- Recent
- Roaming
- Saved Games

File List

Name	Size	Type	Date Modified
\$I30	4	NTFS Index All...	02/02/2017 22:00:34
My New Pet.jpg	57	Regular File	02/02/2017 21:37:30
Owl_Emergency_Care.pdf	140	Regular File	31/01/2017 19:09:01
Owl_Keeping.pdf	214	Regular File	31/01/2017 19:09:11
Sightings2005 (1).xls	110	Regular File	31/01/2017 19:22:02
Snowy Owl Care.pdf	580	Regular File	02/02/2017 21:38:12
Snowy_Owl.pdf	580	Regular File	31/01/2017 19:15:04

00	30	00	00	00	01	00	00	00-00	10	00	00	01	00	00	00	0
10	10	00	00	00	28	00	00	00-28	00	00	00	01	00	00	00	(- - - (- - - - -
20	00	00	00	00	00	00	00	00-18	00	00	00	03	00	00	00
30	00	00	00	00	00	00	00	00-							

Exercise 1.2

AccessData FTK Imager 4.7.1.2

File View Mode Help

Evidence Tree

- Documents
 - Downloads
 - Background.jpg
 - Bibliography - Snowy Owl 14 April 2014 - GLOW posting.xls
 - ChromeSetup.exe
 - Cool picture of a tiger maybe wallhanging.jpg
 - Owl_Emergency_Care.pdf
 - Owl_Keeping.pdf
 - pidgin-2.11.0 (1).exe
 - pidgin-2.11.0.exe
 - Sightings2005.xls
 - SkypeSetupFull.exe
 - yahoo-messenger-0.8.288-win32.exe
- Favorites
- IntelGraphicsProfiles
- Links
- Local Settings
- Music
- My Documents
- NetHood
- OneDrive
- Pictures
- PrintHood
- Recent
- Roaming
- Saved Games
- Searches
- SendTo

File List

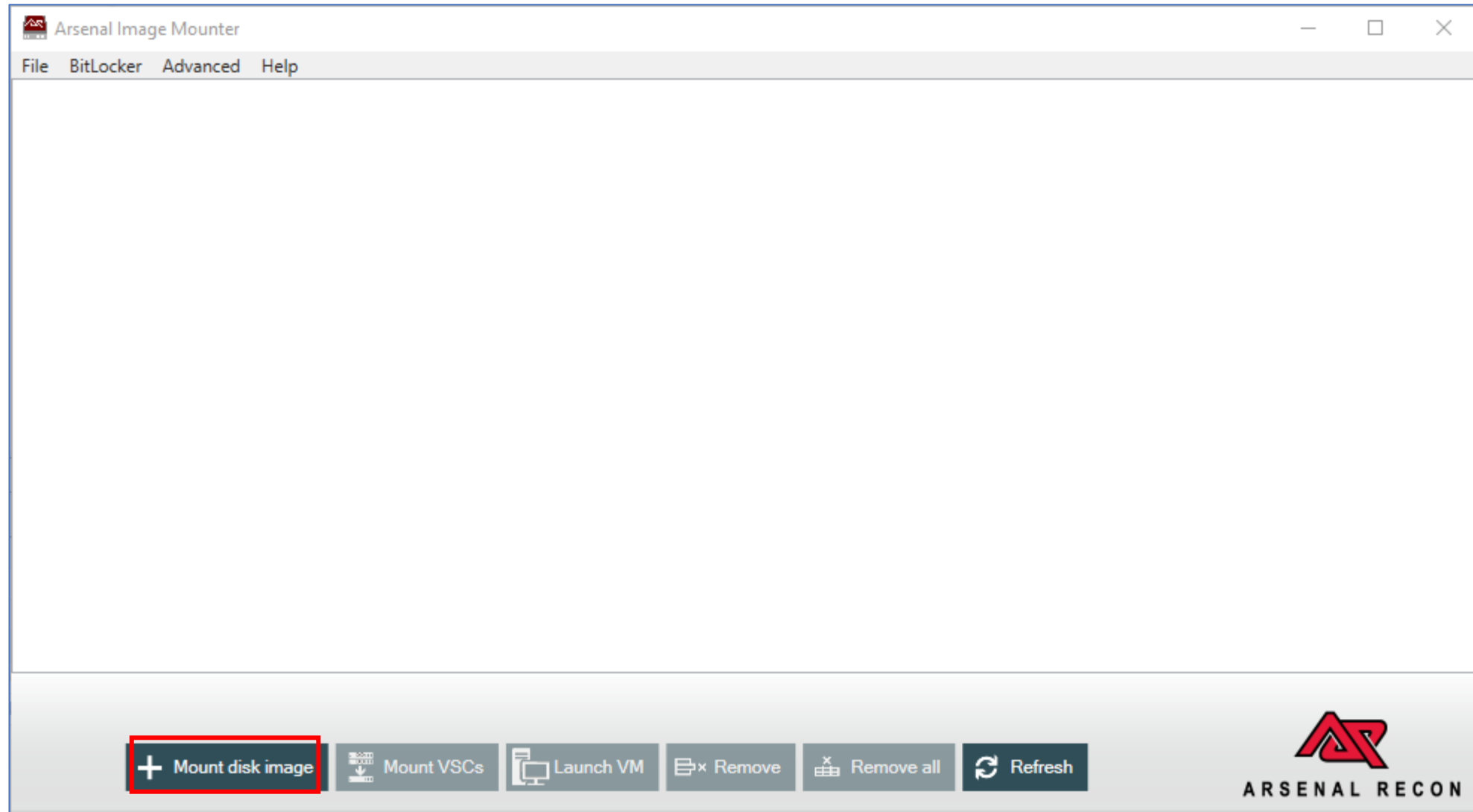
Name	Size	Type	Date Modified
\$I30	12	NTFS Index All...	02/02/2017 22:52:28
1745.tmp		\$I30 INDEX Entry	
Background.jpg	10	Regular File	28/01/2017 22:36:41
Bibliography - Snowy Owl 14 April 2014	288	Regular File	21/01/2017 10:12:44
ChromeSetup.exe	1,041	Regular File	27/01/2017 00:54:29
Cool picture of a tiger maybe wallhanging...	18	Regular File	28/01/2017 22:34:42
desktop.ini	1	Regular File	27/01/2017 16:54:48
Owl_Emergency_Care.pdf	140	Regular File	31/01/2017 19:09:01
Owl_Keeping.pdf	214	Regular File	31/01/2017 19:09:11
pidgin-2.11.0 (1).exe	9,040	Regular File	01/02/2017 17:05:55
pidgin-2.11.0.exe	9,040	Regular File	01/02/2017 16:59:37
Sightings2005.xls	110	Regular File	31/01/2017 19:21:15
SkypeSetupFull.exe	42,890	Regular File	27/01/2017 01:48:03
yahoo-messenger-0.8.288-win32.exe	45,867	Regular File	02/02/2017 22:25:11

Properties

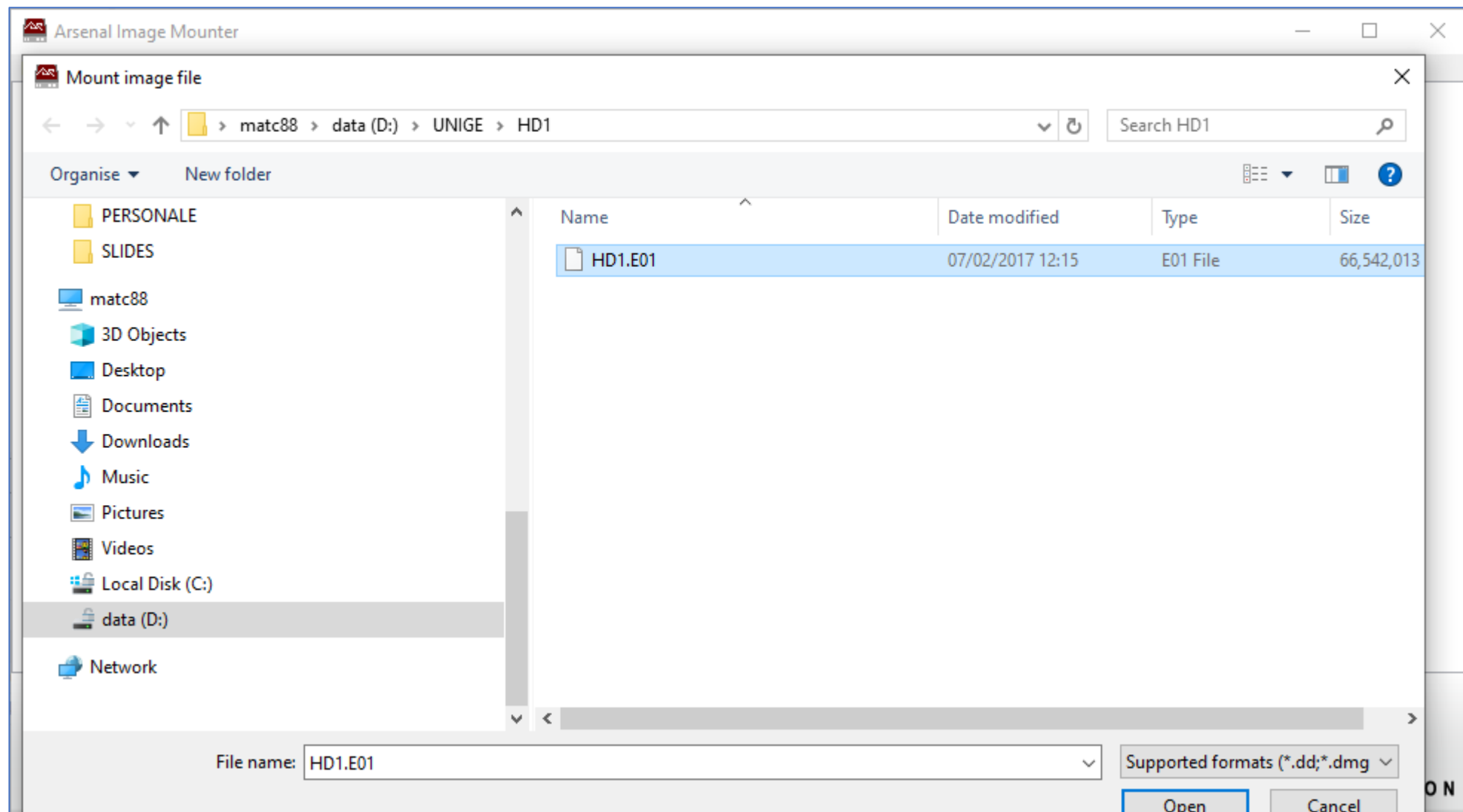
Name Downloads
File Class Directory

00 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00 0
10 10 00 00 00 E0 00 00 00-E0 00 00 00 01 00 00 00
20 14 47 04 00 00 00 05 00-B8 00 9C 00 01 00 00 00
30 B0 08 00 00 00 00 04 00-AB 99 00 B8 B6 79 D2 01
40 A1 82 3A B8 B6 79 D2 01-A1 82 3A B8 B6 79 D2 01
50 25 94 B2 AA B6 79 D2 01-00 50 00 00 00 00 00 00
60 6D 47 00 00 00 00 00 00-20 00 00 00 00 00 00
70 2D 01 43 00 6F 00 6F 00-6C 00 20 00 70 00 69 00
80 63 00 74 00 75 00 72 00-65 00 20 00 6F 00 66 00
90 20 00 61 00 20 00 74 00-69 00 67 00 65 00 72 00
a0 20 00 6D 00 61 00 79 00-62 00 65 00 20 00 77 00
b0 61 00 6C 00 6C 00 68 00-61 00 6E 00 67 00 69 00
c0 6E 00 67 00 2E 00 6A 00-70 00 67 00 00 00 00 00
d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
e0 18 00 00 00 03 00 00 00-01 00 00 00 00 00 00

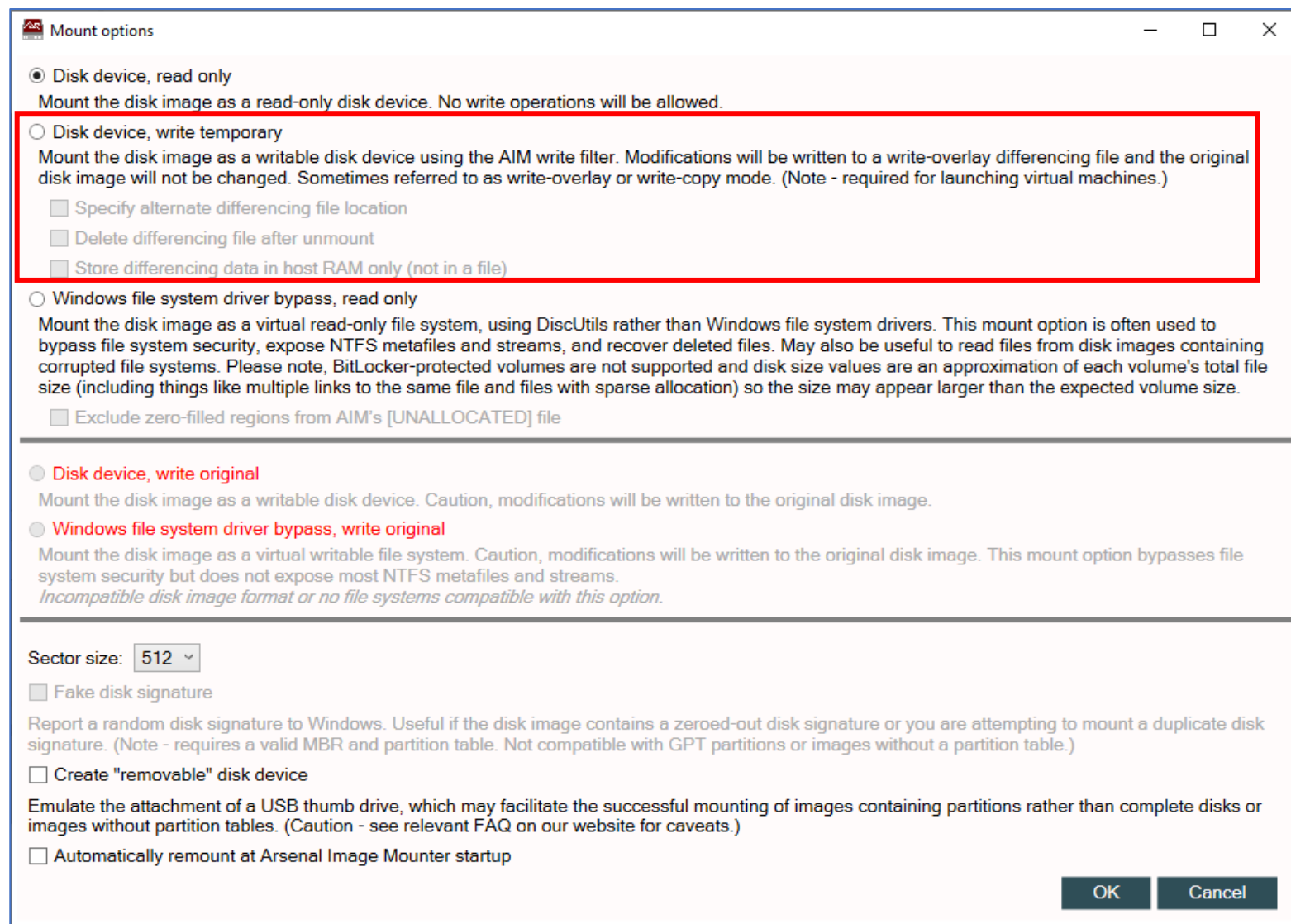
Arsenal Image Mounter



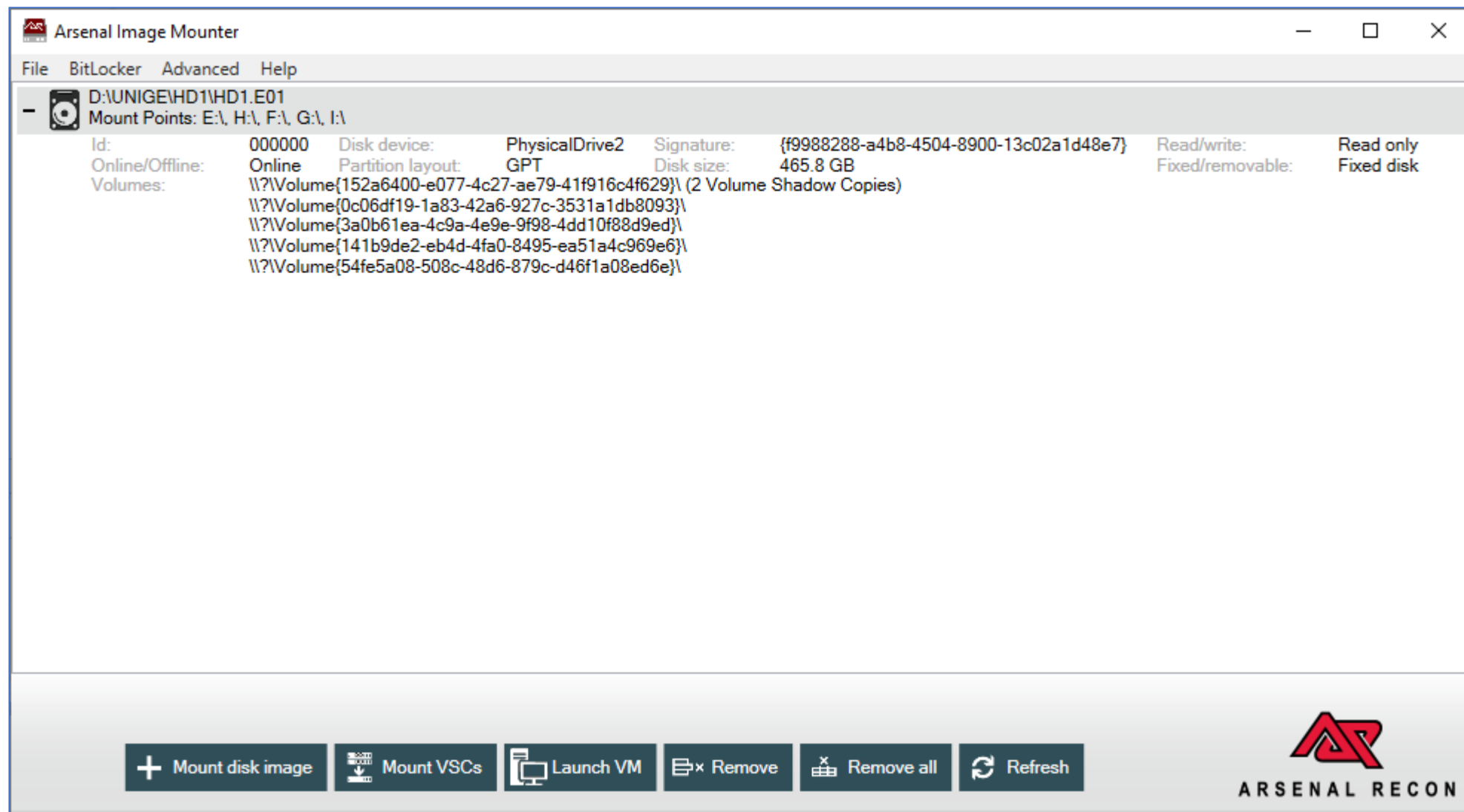
Arsenal Image Mounter



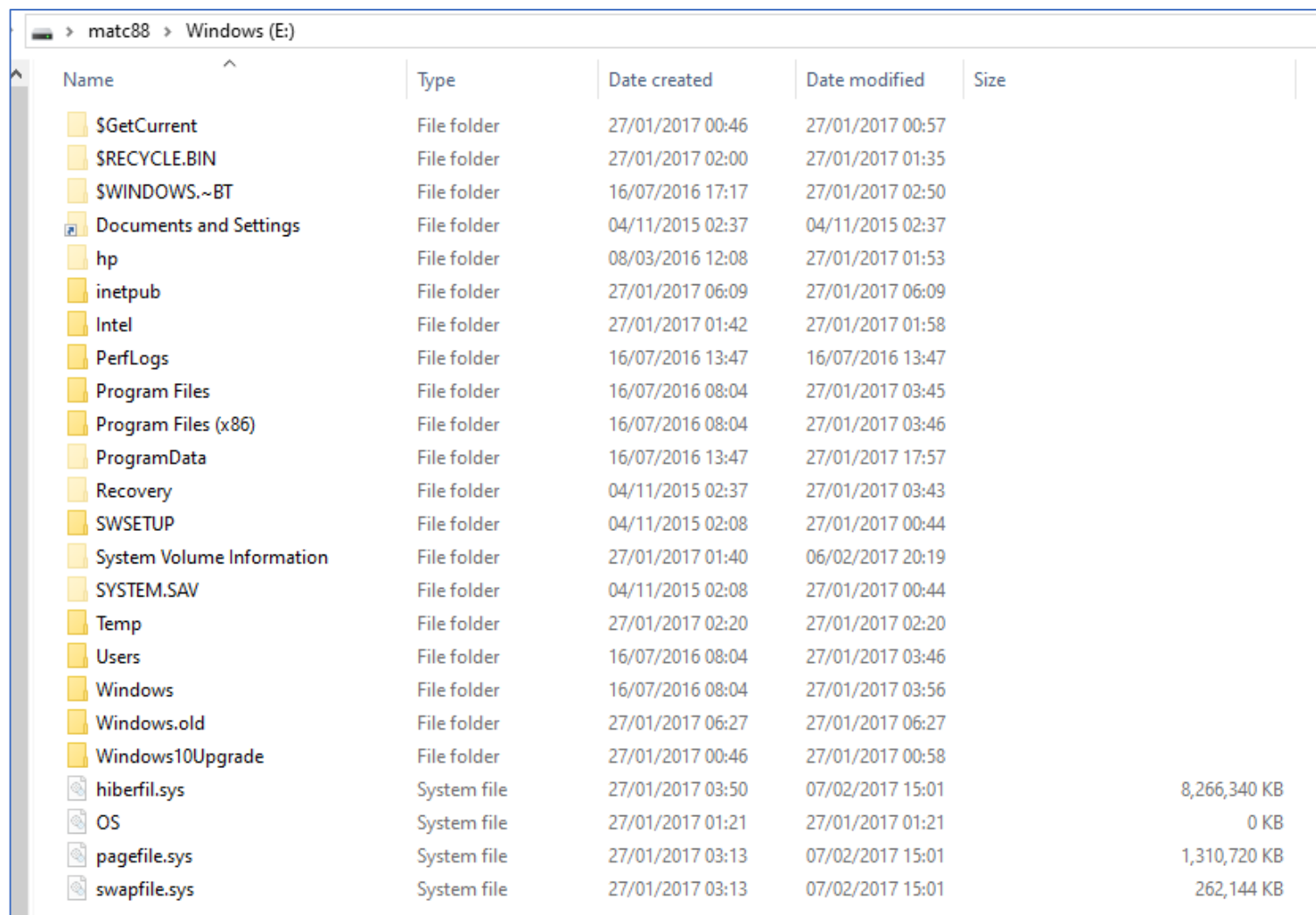
Arsenal Image Mounter



Arsenal Image Mounter

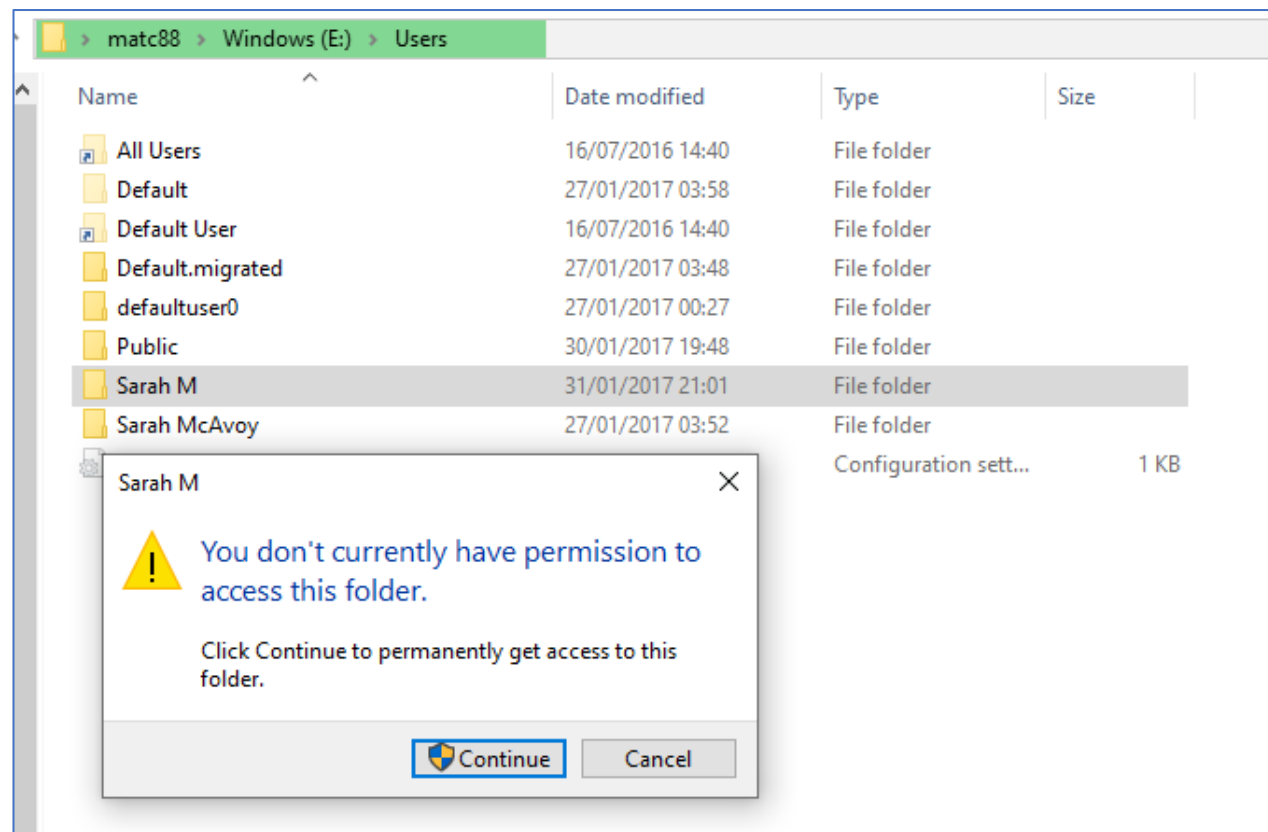


Arsenal Image Mounter

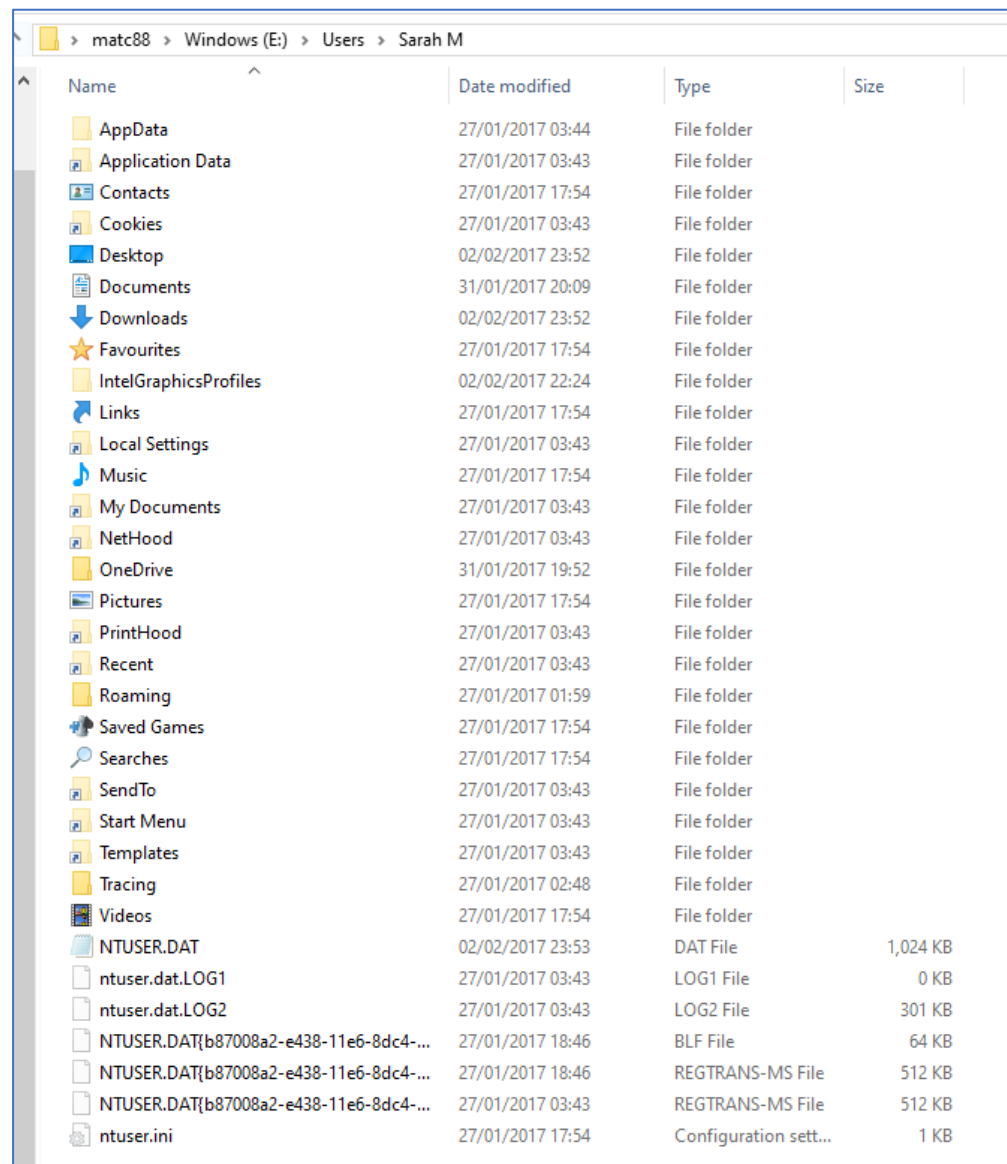


Name	Type	Date created	Date modified	Size
\$GetCurrent	File folder	27/01/2017 00:46	27/01/2017 00:57	
\$RECYCLE.BIN	File folder	27/01/2017 02:00	27/01/2017 01:35	
\$WINDOWS.~BT	File folder	16/07/2016 17:17	27/01/2017 02:50	
Documents and Settings	File folder	04/11/2015 02:37	04/11/2015 02:37	
hp	File folder	08/03/2016 12:08	27/01/2017 01:53	
inetpub	File folder	27/01/2017 06:09	27/01/2017 06:09	
Intel	File folder	27/01/2017 01:42	27/01/2017 01:58	
PerfLogs	File folder	16/07/2016 13:47	16/07/2016 13:47	
Program Files	File folder	16/07/2016 08:04	27/01/2017 03:45	
Program Files (x86)	File folder	16/07/2016 08:04	27/01/2017 03:46	
ProgramData	File folder	16/07/2016 13:47	27/01/2017 17:57	
Recovery	File folder	04/11/2015 02:37	27/01/2017 03:43	
SWSETUP	File folder	04/11/2015 02:08	27/01/2017 00:44	
System Volume Information	File folder	27/01/2017 01:40	06/02/2017 20:19	
SYSTEM.SAV	File folder	04/11/2015 02:08	27/01/2017 00:44	
Temp	File folder	27/01/2017 02:20	27/01/2017 02:20	
Users	File folder	16/07/2016 08:04	27/01/2017 03:46	
Windows	File folder	16/07/2016 08:04	27/01/2017 03:56	
Windows.old	File folder	27/01/2017 06:27	27/01/2017 06:27	
Windows10Upgrade	File folder	27/01/2017 00:46	27/01/2017 00:58	
hiberfil.sys	System file	27/01/2017 03:50	07/02/2017 15:01	8,266,340 KB
OS	System file	27/01/2017 01:21	27/01/2017 01:21	0 KB
pagefile.sys	System file	27/01/2017 03:13	07/02/2017 15:01	1,310,720 KB
swapfile.sys	System file	27/01/2017 03:13	07/02/2017 15:01	262,144 KB

Arsenal Image Mounter



Arsenal Image Mounter



Name	Date modified	Type	Size
AppData	27/01/2017 03:44	File folder	
Application Data	27/01/2017 03:43	File folder	
Contacts	27/01/2017 17:54	File folder	
Cookies	27/01/2017 03:43	File folder	
Desktop	02/02/2017 23:52	File folder	
Documents	31/01/2017 20:09	File folder	
Downloads	02/02/2017 23:52	File folder	
Favourites	27/01/2017 17:54	File folder	
IntelGraphicsProfiles	02/02/2017 22:24	File folder	
Links	27/01/2017 17:54	File folder	
Local Settings	27/01/2017 03:43	File folder	
Music	27/01/2017 17:54	File folder	
My Documents	27/01/2017 03:43	File folder	
NetHood	27/01/2017 03:43	File folder	
OneDrive	31/01/2017 19:52	File folder	
Pictures	27/01/2017 17:54	File folder	
PrintHood	27/01/2017 03:43	File folder	
Recent	27/01/2017 03:43	File folder	
Roaming	27/01/2017 01:59	File folder	
Saved Games	27/01/2017 17:54	File folder	
Searches	27/01/2017 17:54	File folder	
SendTo	27/01/2017 03:43	File folder	
Start Menu	27/01/2017 03:43	File folder	
Templates	27/01/2017 03:43	File folder	
Tracing	27/01/2017 02:48	File folder	
Videos	27/01/2017 17:54	File folder	
NTUSER.DAT	02/02/2017 23:53	DAT File	1,024 KB
ntuser.dat.LOG1	27/01/2017 03:43	LOG1 File	0 KB
ntuser.dat.LOG2	27/01/2017 03:43	LOG2 File	301 KB
NTUSER.DAT{b87008a2-e438-11e6-8dc4-...}	27/01/2017 18:46	BLF File	64 KB
NTUSER.DAT{b87008a2-e438-11e6-8dc4-...}	27/01/2017 18:46	REGTRANS-MS File	512 KB
NTUSER.DAT{b87008a2-e438-11e6-8dc4-...}	27/01/2017 03:43	REGTRANS-MS File	512 KB
ntuser.ini	27/01/2017 17:54	Configuration sett...	1 KB

DEMO and EXERCISE 2

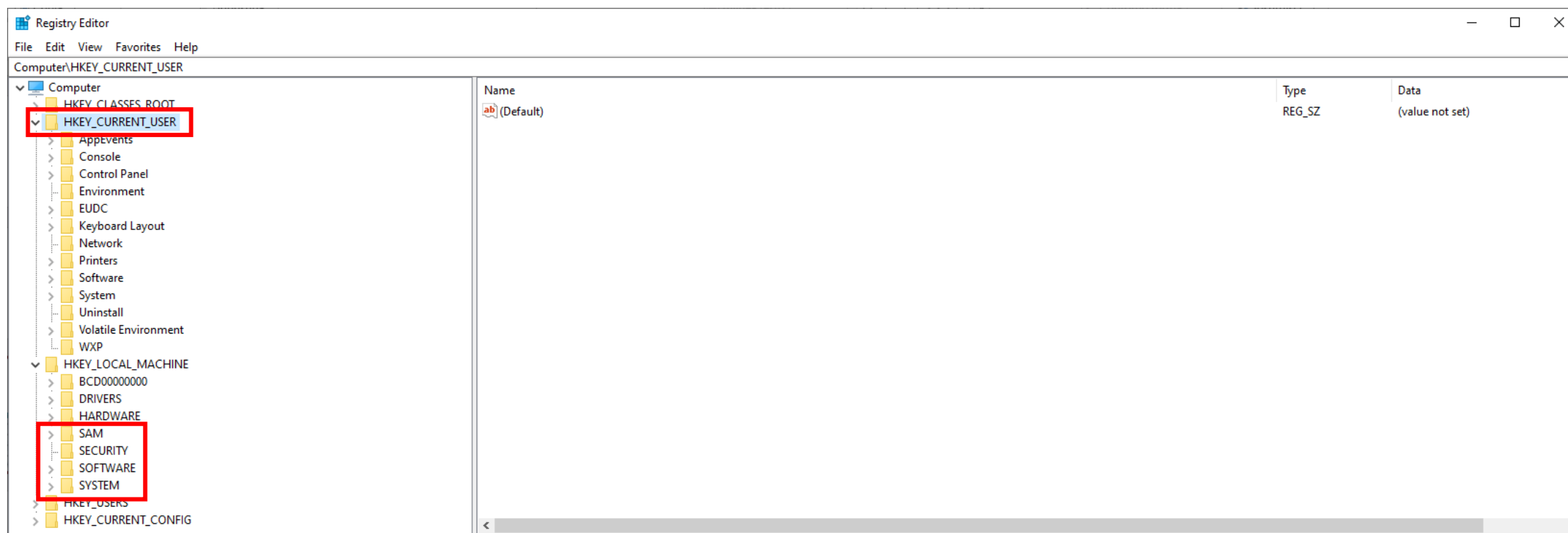
Mounting an image with Arsenal Image Mounter

Windows OS relevant files

- **Registry**
 - System based
 - User based
- **LNK (Shortcut) files**
- **JumpLists**
- **ShellBags**
- **USB Device Analysis**
- **Prefetch**
- **Windows Events**
- **Recycle Bin**
- **Thumbnails**
- **System Resource Usage Monitor (SRUM)**

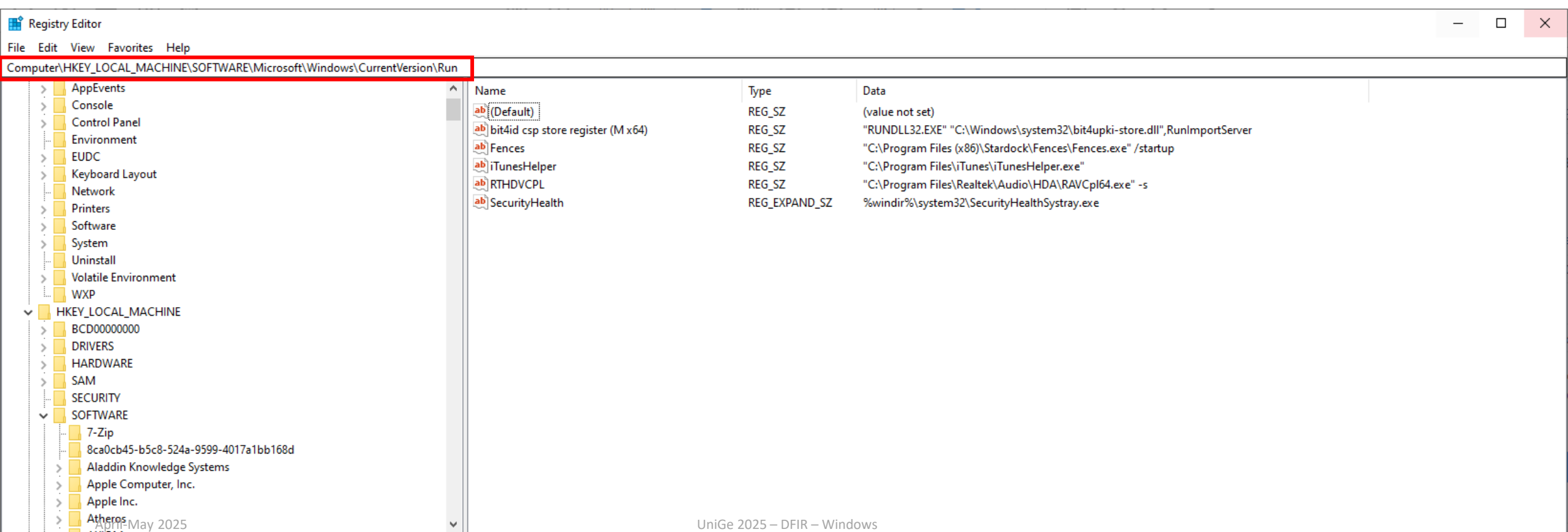
Windows Registry

- Stored in files known as **hives**
- A hive contains **keys** and **values**
- Live interaction via **RegEdit**



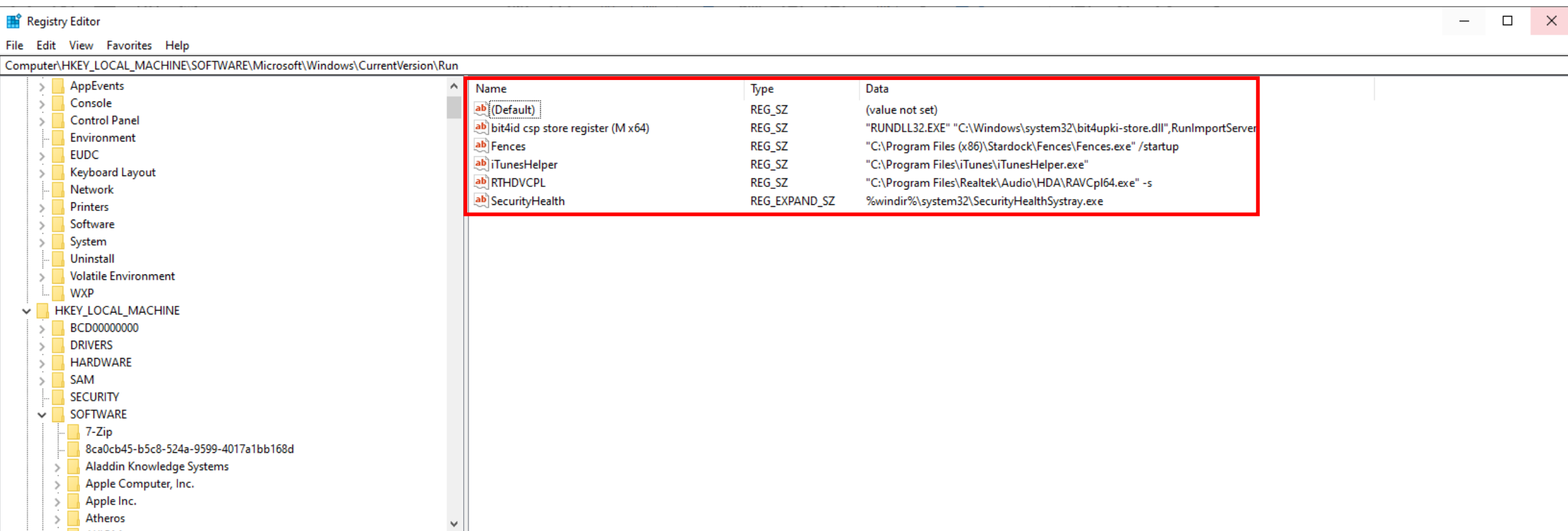
Windows Registry

- HKLM (**Hive**)
SOFTWARE (**Key**)
\Microsoft\Windows\CurrentVersion\Run (**Subkeys**)
- Every **key** in each **hive** has a **Last Write Time stored in UTC**



Windows Registry

- Values can be: **Strings, Binary data, Integers, Lists**



Windows Registry – System Hives

- Stored in

%WINDIR%\System32\Config

Live Registry	Hive file
HKLM\SAM	%WINDIR%\System32\config\SAM
HKLM\SECURITY	%WINDIR%\System32\config\SECURITY
HKLM\SOFTWARE	%WINDIR%\System32\config\SOFTWARE
HKLM\SYSTEM	%WINDIR%\System32\config\SYSTEM

The screenshot displays a file explorer window with two panes: 'Evidence Tree' and 'File List'. The 'Evidence Tree' pane on the left shows a directory structure with various files and folders, including 'comres.dll', 'comsnap.dll', 'comsvcs.dll', 'comuid.dll', 'config', 'configmanager2.dll', 'Configuration', 'Configurationclient.dll', 'ConfigureExpandedStorage.x', 'conhost.exe', 'ConhostV1.dll', 'ConhostV2.dll', 'connect.dll', 'ConnectedAccountState.dll', 'consent.exe', 'ConsentUX.dll', 'console.dll', 'ConsoleLogon.dll', 'ContactActivation.dll', 'ContactApis.dll', 'ContactHarvesterDS.dll', 'container.dll', 'container_xml.dll', 'ContentDeliveryManager.Util', 'control.exe', 'convert.exe', and 'coreaudioioolicvmanagerext.c'. The 'File List' pane on the right shows a table of files and folders with columns for Name, Size, Type, and Date Modified. The files listed include 'TxR', 'systemprofile', 'RegBack', 'Journal', 'bbimigrate', 'VSMIDK', 'userdiff.LOG2', 'userdiff.LOG1', 'userdiff', 'SYSTEM.LOG2.FileSlack', 'SYSTEM.LOG2', 'SYSTEM.LOG1.FileSlack', 'SYSTEM.LOG1', 'SYSTEM.FileSlack', 'SYSTEM', 'SOFTWARE.LOG2.FileSlack', 'SOFTWARE.LOG2', 'SOFTWARE.LOG1', 'SOFTWARE.FileSlack', 'SOFTWARE', 'SECURITY.LOG2.FileSlack', 'SECURITY.LOG2', 'SECURITY.LOG1.FileSlack', 'SECURITY.LOG1', 'SECURITY.FileSlack', 'SECURITY', 'SAM.LOG2.FileSlack', 'SAM.LOG2', 'SAM.LOG1', 'SAM.FileSlack', and 'SAM'. The 'config' directory is highlighted in the 'Evidence Tree' pane, and the 'File List' pane shows the contents of the 'config' directory.

Windows Registry – User(s) Hives

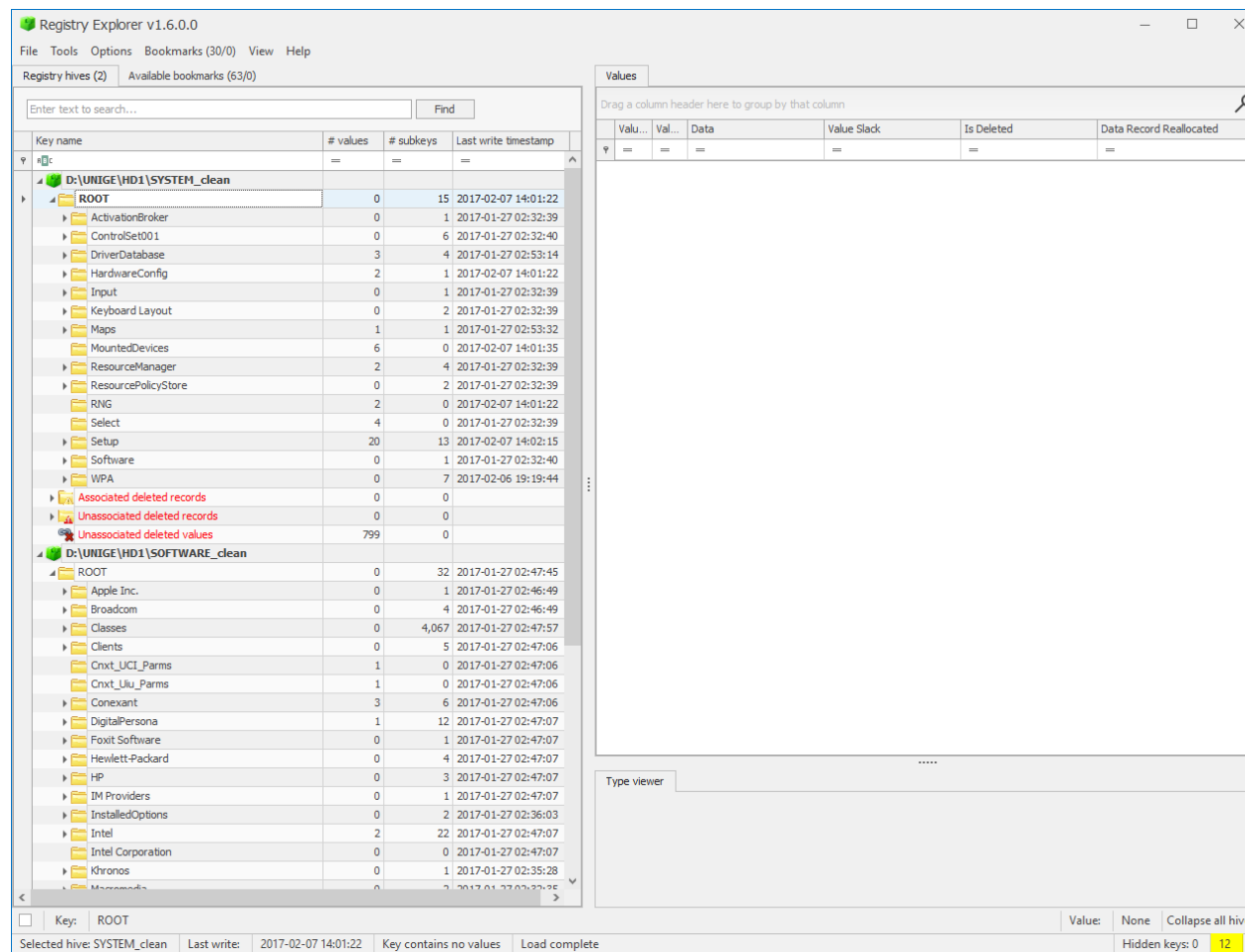
- Stored in
%USERS%

Live Registry	Hive file
HKCU\	%USERS%\<username>\NTUSER.DAT
HKCU\Software\Classes	%USERS%\<username>\AppData\Local\Microsoft\Windows\USRCLASS.DAT

The screenshot displays the Windows Explorer interface for a user profile. The 'Evidence Tree' pane on the left shows the hierarchy from 'defaultuser0' to 'Sarah M' and then to 'AppData'. The 'File List' pane on the right shows a detailed list of files and folders in the 'AppData' directory, including 'Videos', 'Tracing', 'Templates', 'Start Menu', 'SendTo', 'Searches', 'Saved Games', 'Roaming', 'Recent', 'PrintHood', 'Pictures', 'OneDrive', 'NetHood', 'My Documents', 'Music', 'Local Settings', 'Links', 'Favorites', 'Downloads', 'Documents', 'Desktop', 'Cookies', 'Contacts', 'Application Data', 'AppData', 'NTUSER~1.LOG', 'ntuser.ini', 'NTUSER.DAT', 'NTUSER.DAT.LOG2', 'NTUSER.DAT.LOG1', 'NTUSER.DAT.FileSlack', 'NTUSER.DAT', and '\$I30'. The 'Properties' pane at the bottom shows details for the selected file 'Sarah M', including its name, file class, size, date accessed, date created, date modified, encryption status, compression status, and alternate data stream.

Opening a Windows Registry File

- **Registry Explorer** by Eric Zimmerman



Registry Explorer – Browsing a Registry File

Registry Explorer v1.5.2.0

File Tools Options Bookmarks (21/0) View Help

Registry hives (2) Available bookmarks (41/0)

Enter text to search... Find

Key name

Windows

- CurrentVersion
 - Action Center
 - Applets
 - Controls Folder
 - Device Metadata
 - Explorer
 - Advanced
 - ApplicationDestinations
 - AutoplayHandlers
 - BitBucket
 - CabinetState
 - CD Burning
 - CIDSave
 - CLSID
 - ComDlg32
 - ControlPanel
 - Discardable
 - FileExts
 - LowRegistry
 - Map Network Drive MRU
 - MenuOrder
 - Modules
 - MountPoints2
 - NewShortcutHandlers
 - RecentDocs**
 - RunMRU
 - SearchPlatform
 - Shell Folders
 - StartPage
 - StartPage2
 - Streams

Values Recent documents

Value Name Value Type Data Value Slack Is Deleted Data Record Reallocated

MRUListEx	RegBinary	08-00-00-00-0E-00-00-00-0D-00-00-00-0B-00-00-00-09-00-00-00-0C-00-00-00-0...	01-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
0	RegBinary	5B-00-73-00-65-00-63-00-72-00-65-00-74-00-5F-00-70-00-72-00-6F-00-6A-00-65...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
2	RegBinary	5B-00-73-00-65-00-63-00-72-00-65-00-74-00-5F-00-70-00-72-00-6F-00-6A-00-65...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
1	RegBinary	73-00-65-00-63-00-72-00-65-00-74-00-00-00-5C-00-32-00-00-00-00-00-00-00...		<input type="checkbox"/>	<input type="checkbox"/>
3	RegBinary	28-00-73-00-65-00-63-00-72-00-65-00-74-00-5F-00-70-00-72-00-6F-00-6A-00-65...		<input type="checkbox"/>	<input type="checkbox"/>
4	RegBinary	70-00-72-00-69-00-63-00-69-00-6E-00-67-00-20-00-64-00-65-00-63-00-69-00-73...	00-00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
5	RegBinary	5B-00-73-00-65-00-63-00-72-00-65-00-74-00-5F-00-70-00-72-00-6F-00-6A-00-65...		<input type="checkbox"/>	<input type="checkbox"/>
6	RegBinary	66-00-69-00-6E-00-61-00-6C-00-00-00-58-00-32-00-00-00-00-00-00-00-00-00...	00-00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
7	RegBinary	77-00-69-00-6E-00-74-00-65-00-72-00-5F-00-77-00-68-00-65-00-74-00-68-00-65...		<input type="checkbox"/>	<input type="checkbox"/>
10	RegBinary	42-00-44-00-2D-00-52-00-45-00-20-00-44-00-72-00-69-00-76-00-65-00-20-00-28...	00-00-E8-F3-0D-00	<input type="checkbox"/>	<input type="checkbox"/>
12	RegBinary	50-00-65-00-6E-00-67-00-75-00-69-00-6E-00-73-00-2E-00-6A-00-70-00-67-00-00...	46-00	<input type="checkbox"/>	<input type="checkbox"/>
9	RegBinary	4B-00-6F-00-61-00-6C-00-61-00-2E-00-6A-00-70-00-67-00-00-00-64-00-32-00-0...	48-00	<input type="checkbox"/>	<input type="checkbox"/>
11	RegBinary	54-00-75-00-6C-00-69-00-70-00-73-00-2E-00-6A-00-70-00-67-00-00-00-68-00-3...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
13	RegBinary	42-00-44-00-2D-00-52-00-45-00-20-00-44-00-72-00-69-00-76-00-65-00-20-00-28...		<input type="checkbox"/>	<input type="checkbox"/>
14	RegBinary	52-00-65-00-73-00-69-00-67-00-6E-00-61-00-74-00-69-00-6F-00-6E-00-5F-00-4C...	74-00-72-00-53-00	<input type="checkbox"/>	<input type="checkbox"/>
8	RegBinary	52-00-65-00-73-00-69-00-67-00-6E-00-61-00-74-00-69-00-6F-00-6E-00-5F-00-4C...	67-00	<input type="checkbox"/>	<input type="checkbox"/>

Type viewer

	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22	
00000000	5B 00 73 00 65 00 63 00 72 00 65 00 74 00 5F 00 70 00 72 00 6F 00 6A 00 65 00 63 00 74 00 5D 00 5F 00 70	[.s.e.c.r.e.t._.p.r.o.j.e.c.t._.p
00000023	00 72 00 6F 00 70 00 6F 00 73 00 61 00 6C 00 2E 00 64 00 6F 00 63 00 78 00 00 00 94 00 32 00 00 00 00 00	.r.o.p.o.s.a.l...d.o.c.x....2....
00000046	00 00 00 00 00 00 5B 73 65 63 72 65 74 5F 70 72 6F 6A 65 63 74 5D 5F 70 72 6F 70 6F 73 61 6C 2E 6C 6E 68[secret_project]_proposal.lnk
00000069	00 68 00 08 00 04 00 EF BE 00	.h.....i¼.....*
0000008C	00 00 00 00 00 00 00 00 5B 00 73 00 65 00 63 00 72 00 65 00 74 00 5F 00 70 00 72 00 6F 00 6A 00 65 00 63[.s.e.c.r.e.t._.p.r.o.j.e.c
000000AF	00 74 00 5D 00 5F 00 70 00 72 00 6F 00 70 00 6F 00 73 00 61 00 6C 00 2E 00 6C 00 6E 00 68 00 00 00 2C 00	.t)._..p.r.o.p.o.s.a.l...l.n.k....
000000D2	00 00	..

Current offset: 0 (0x0) Bytes selected: 0 (0x0)

Key: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Selected hive: NTUSER.DAT Last write: 2015-03-25 15:29:08 16 of 16 values shown (100,00%) Load complete

Data interpreter ?

Value: 0 Collapse all hives

Hidden keys: 0 1

Registry Explorer – Browsing a Registry File

Registry Explorer v1.5.2.0

File Tools Options Bookmarks (21/0) View Help

Registry hives (2) Available bookmarks (41/0)

Enter text to search... Find

Key name	# values	# subkeys
ComDlg32	0	4
CurrentVersion	0	24
CurrentVersion	0	10
FileExts	0	134
FirstFolder	2	0
FTP	1	0
General	3	0
Internet Settings	21	12
Main	40	2
Map Network Drive MRU	2	0
MountPoints2	0	6
PrinterPorts	2	0
RecentDocs	16	8
Run	0	0
RunMRU	3	0
Shell Folders	30	0
TypedURLs	3	0
User Assist	0	2
WordWheelQuery	2	0

Bookmark information

Hive: D:\UNIGE_2020\Data_Leakage_Extracted\NTUSER.DAT

Category: User files and folders

Name: RecentDocs

Key path: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Short description: Recently opened files by extension

Long description: See MRU key for order of opening

Values Recent documents

Extension	Value Name	Target Name	Lnk Name	MrU Position	Opened On	Extension Last Opened
RecentDocs	8	Resignation_Letter_(Iaman_Informant).docx	Resignation_Letter_(Iaman_Informant).docx.lnk	0	2015-03-25 15:29:08	2015-03-25 15:29:08
RecentDocs	14	Resignation_Letter_(Iaman_Informant).xps	Resignation_Letter_(Iaman_Informant).xps.lnk	1		2015-03-25 15:28:33
RecentDocs	13	BD-RE Drive (D:) IAMAN CD	CD Drive (2).lnk	2		2015-03-24 21:01:14
RecentDocs	11	Tulips.jpg	Tulips.jpg.lnk	3		2015-03-24 21:01:14
RecentDocs	9	Koala.jpg	Koala.jpg.lnk	4		
RecentDocs	12	Penguins.jpg	Penguins.jpg.lnk	5		
RecentDocs	10	BD-RE Drive (D:)	CD Drive.lnk	6		
RecentDocs	7	winter_weather_advisory.zip	winter_weather_advisory.zip.lnk	7		2015-03-24 20:44:18
RecentDocs	6	final	final.lnk	8		
RecentDocs	5	[secret_project]_final_meeting.pptx	[secret_project]_final_meeting.pptx.lnk	9		2015-03-23 20:27:33
RecentDocs	4	pricing decision	pricing decision.lnk	10		
RecentDocs	3	(secret_project)_pricing_decision.xlsx	(secret_project)_pricing_decision.xlsx.lnk	11		2015-03-23 20:26:53
RecentDocs	1	secret	secret.lnk	12		
RecentDocs	2	[secret_project]_design_concept	[secret_project]_design_concept.lnk	13		2015-03-23 18:28:31

Total rows: 30

Export

Type viewer Slack viewer

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22

00000000 08 00 00 00 0E 00 00 00 0D 00 00 00 0B 00 00 00 09 00 00 00 0C 00 00 00 0A 00 00 00 07 00 00 00 06 00 00

00000023 00 05 00 00 00 04 00 00 00 03 00 00 00 01 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Current offset: 0 (0x0) Bytes selected: 0 (0x0)

Data interpreter ?

Key: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Value: MRUListEx Collapse all hives

Selected hive: NTUSER.DAT Last write: 25/03/2015 15:29:08 +00:00 16 of 16 values shown (100,00%)

Hidden keys: 0 1

Registry Explorer – Searching

Find

Options Help

Standard

Search for RESIGNATION

History

Search in

☒ Key name ☒ Value name ☒ Value data ☐ Value slack

Search type

☒ Simple ☐ Regular expression

☐ Literal Search

Last write timestamp

Earliest (UTC) Latest (UTC)

☒ Before ☐ Between ☐ After

Search

Minimum value size

Minimum size (bytes) 512

Search

Base64 in values

Minimum length 50

Search

NOTE: Unassociated deleted records are not searched in this version

Results (Double click a row in the Results grid to select the search hit in the main window)

Drag a column header here to group by that column

	Hive Name	Hit Location	Hit text	Last Write Time	Key Path	Value Data	Value N...	Deleted
▼	Hive Name	Hit Location	Hit text	=	Key Path	Value Data	Value N...	Deleted
▶	NTUSER.DAT	Value data	Resignation	2015-03-24 18:48:40	Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidMRU\docx	B8-00-32-00-00-00-0...	0	<input type="checkbox"/>
	NTUSER.DAT	Value data	Resignation	2015-03-24 18:48:40	Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidMRU\docx	B8-00-32-00-00-00-0...	0	<input type="checkbox"/>
	NTUSER.DAT	Value data	RESIGNATI...	2015-03-24 18:59:30	Software\Microsoft\Office\15.0\Word\Reading Locations\Document 1	C:\Users\informant\...	File Path	<input type="checkbox"/>
	NTUSER.DAT	Value data	RESIGNATI...	2015-03-25 15:24:49	Software\Microsoft\Office\15.0\Word\File MRU	[F00000000][T01D06...	Item 1	<input type="checkbox"/>
	NTUSER.DAT	Value data	Resignation	2015-03-25 15:28:33	Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidMRU*	B8-00-32-00-00-00-0...	1	<input type="checkbox"/>
	NTUSER.DAT	Value data	Resignation	2015-03-25 15:28:33	Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidMRU*	B8-00-32-00-00-00-0...	1	<input type="checkbox"/>
	NTUSER.DAT	Value data	Resignation	2015-03-25 15:28:33	Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidMRU*	B6-00-32-00-00-00-0...	4	<input type="checkbox"/>
	NTUSER.DAT	Value data	Resignation	2015-03-25 15:28:33	Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidMRU*	B6-00-32-00-00-00-0...	4	<input type="checkbox"/>
	NTUSER.DAT	Value data	Resignation	2015-03-25 15:28:33	Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidMRU\xps	B6-00-32-00-00-00-0...	0	<input type="checkbox"/>
	NTUSER.DAT	Value data	Resignation	2015-03-25 15:28:33	Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidMRU\xps	B6-00-32-00-00-00-0...	0	<input type="checkbox"/>
	NTUSER.DAT	Value data	Resignation	2015-03-25 15:28:33	Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\,xps	52-00-65-00-73-00-6...	0	<input type="checkbox"/>
	NTUSER.DAT	Value data	Resignation	2015-03-25 15:28:33	Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\,xps	52-00-65-00-73-00-6...	0	<input type="checkbox"/>
	NTUSER.DAT	Value data	Resignation	2015-03-25 15:29:08	Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	52-00-65-00-73-00-6...	14	<input type="checkbox"/>
	NTUSER.DAT	Value data	Resignation	2015-03-25 15:29:08	Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	52-00-65-00-73-00-6...	14	<input type="checkbox"/>
	NTUSER.DAT	Value data	Resignation	2015-03-25 15:29:08	Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	52-00-65-00-73-00-6...	8	<input type="checkbox"/>
	NTUSER.DAT	Value data	Resignation	2015-03-25 15:29:08	Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	52-00-65-00-73-00-6...	8	<input type="checkbox"/>
	NTUSER.DAT	Value data	Resignation	2015-03-25 15:29:08	Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\,docx	52-00-65-00-73-00-6...	1	<input type="checkbox"/>
	NTUSER.DAT	Value data	Resignation	2015-03-25 15:29:08	Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\,docx	52-00-65-00-73-00-6...	1	<input type="checkbox"/>
	NTUSER.DAT	Value data	Resignation	2015-03-25 15:30:54	Software\Microsoft\Windows\Shell\Bags\1\Desktop	00-00-00-00-00-00-0...	ItemPos...	<input type="checkbox"/>

Hive path: D:\UNIGE_2020\Data_Leakage_Extracted\NTUSER.DAT Search hits: 19 Search completed in 2.43770 seconds across 2 hives

Cancel search Always on top Export results

DEMO

Opening a Registry File with Registry Explorer

SAM

- It contains information about **local users**
- **Username**
- **User RID (Relative Identifier)**
- **Account Creation timestamp**
- **Last login**
- **Last failed login**
- **Last password change**
- **Password “hint”**
- **Group Information**

Selected hive: SAM

UniGe 2025 – DFIR – Windows

Exercise 3

1. Which users did at least one successful login? (LogonCount > 0)
2. When was the user **Sarah McAvoy** created?
3. What is the RID of the **Sarah M** user?
4. Is the **Sarah McAvoy** user an administrator?

Exercise 3

The screenshot displays the Registry Explorer v1.6.0.0 interface. The left pane shows the tree view of the SAM registry hive, expanded to show the path E:\Windows\System32\config\SAM. The right pane shows the 'User accounts' tab, which contains a table listing user accounts.

Registry Explorer Tree View:

- #c
- D:\UNIGE\HD1\SYSTEM_clean
- D:\UNIGE\HD1\SOFTWARE_clean
- E:\Windows\System32\config\SAM
 - ROOT
 - SAM
 - Domains
 - Account
 - Aliases
 - Groups
 - Users
 - Builtin
 - LastSkuUpgrade
 - RXACT

User Accounts Table:

Val...	Invalid Login...	Total Logi...	Created On	Last Login Time	Last Password Change	User Name	Full Name	Password ...	Groups	Comment
[x]	500	0	5	2017-01-27 02:14:33	2017-01-27 02:06:52	Administrator			Administrators	Built-in account for administering the computer/domain
[x]	501	0	0	2017-01-27 02:14:33		Guest			Guests	Built-in account for guest access to the computer/domain
[x]	503	0	0	2017-01-27 02:14:33		DefaultAccount			System Managed Accounts Group	A user account managed by the system.
[x]	1001	0	8	2017-01-26 23:41:56	2017-01-27 01:48:12	Sarah McAvoy	Admin	.	Administrators	
[x]	1002	0	12	2017-01-27 00:33:10	2017-02-02 21:24:14	Sarah M	Sarah M 87		Users	

Bottom Panel:

Type viewer: Binary viewer
Value name: (default)
Value type: RegDword
Value: 0
Raw value: [Empty field]

Status bar: Selected hive: SAM | Last write: 2017-01-27 00:33:10 | 1 of 1 values shown (100.00%) | Load complete | Value: (default) | Collapse all hives | Hidden keys: 0 | 12