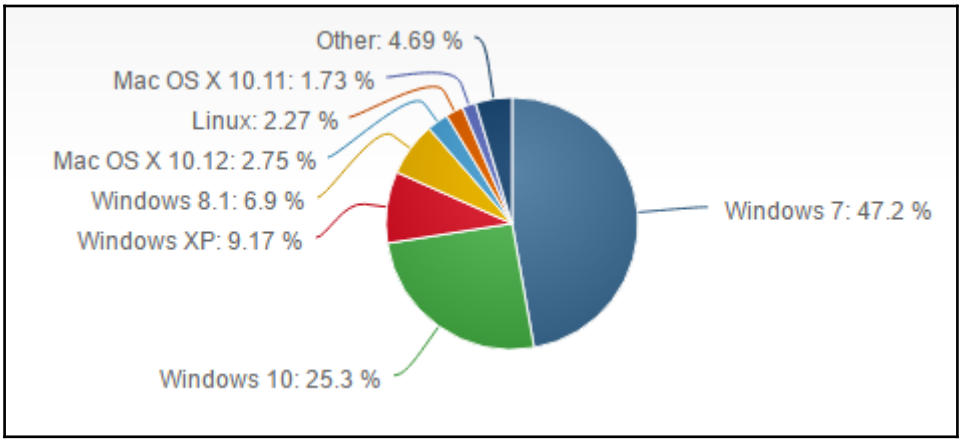
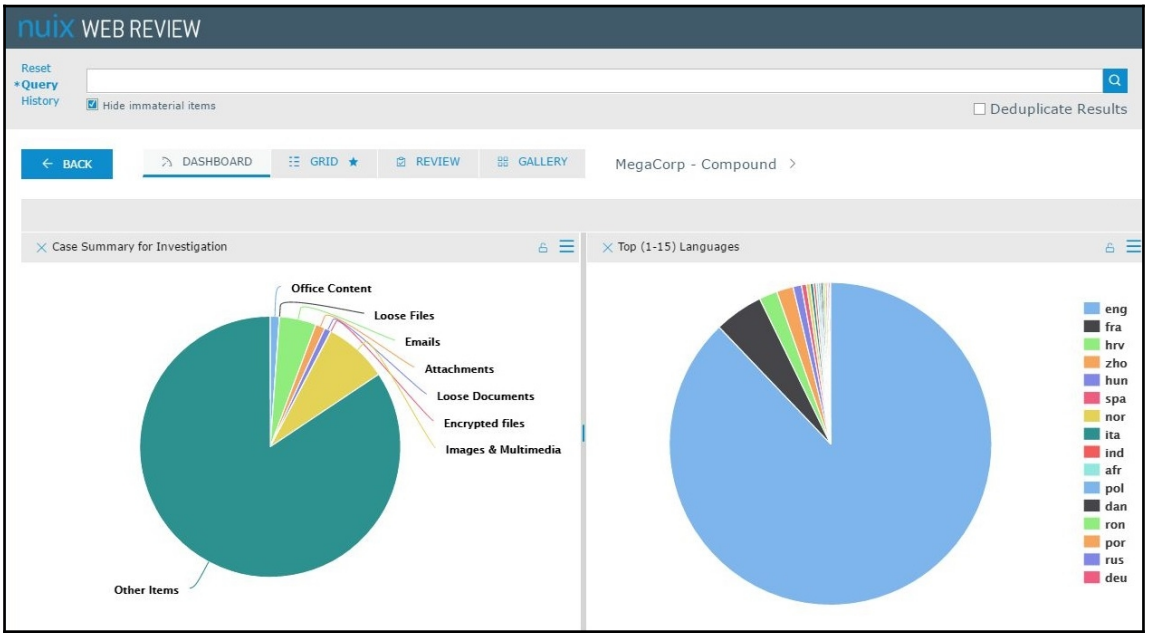
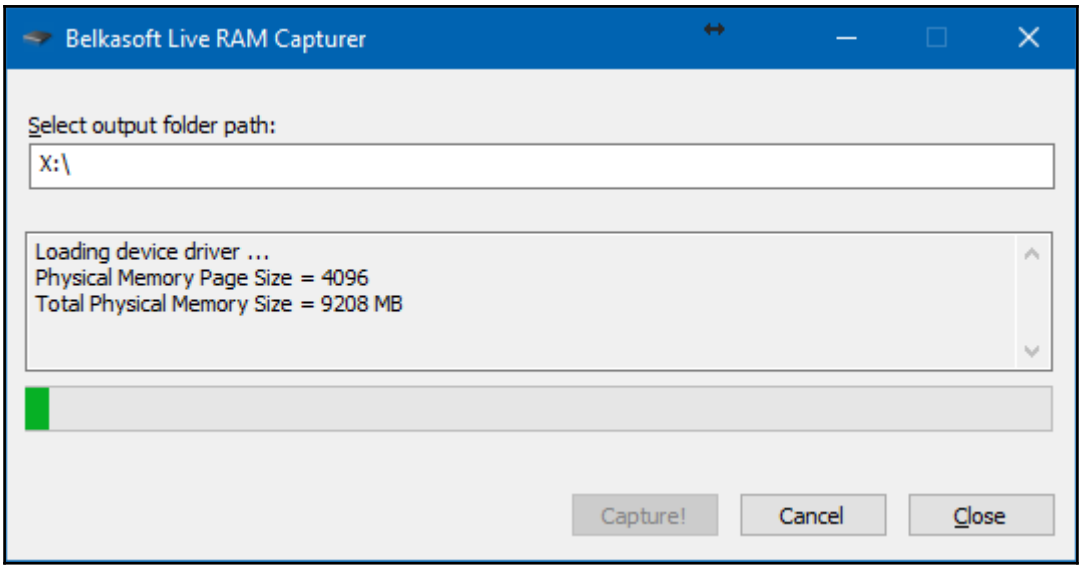
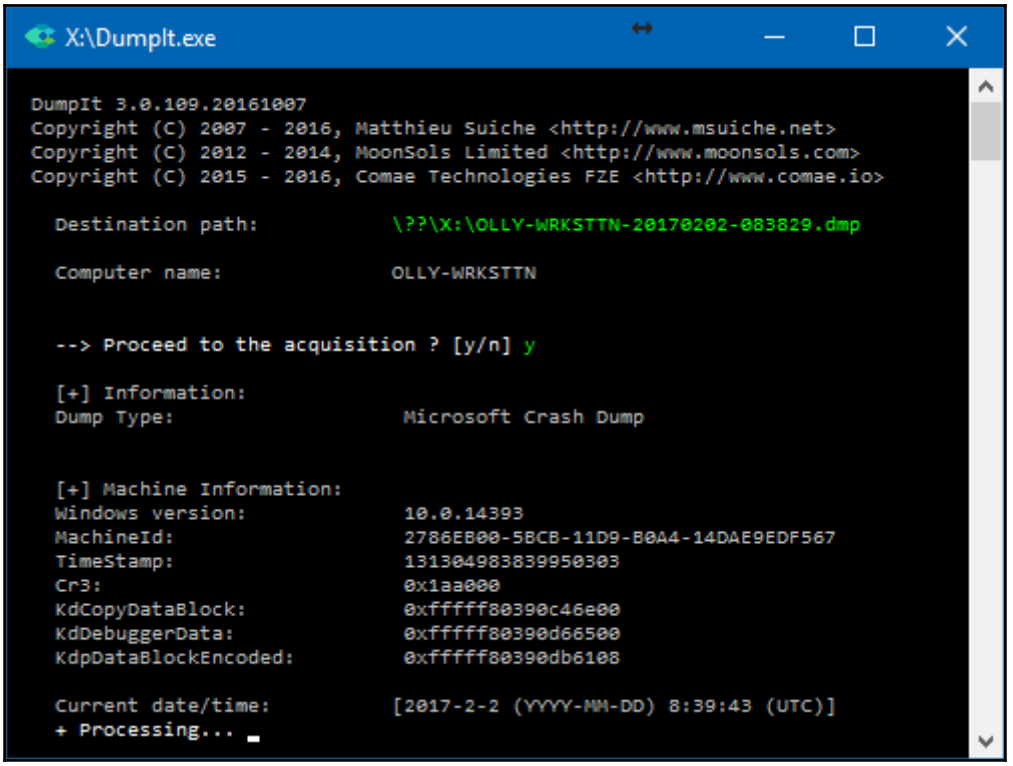
Chapter 1 : Digital Forensics And Evidence Acquisition

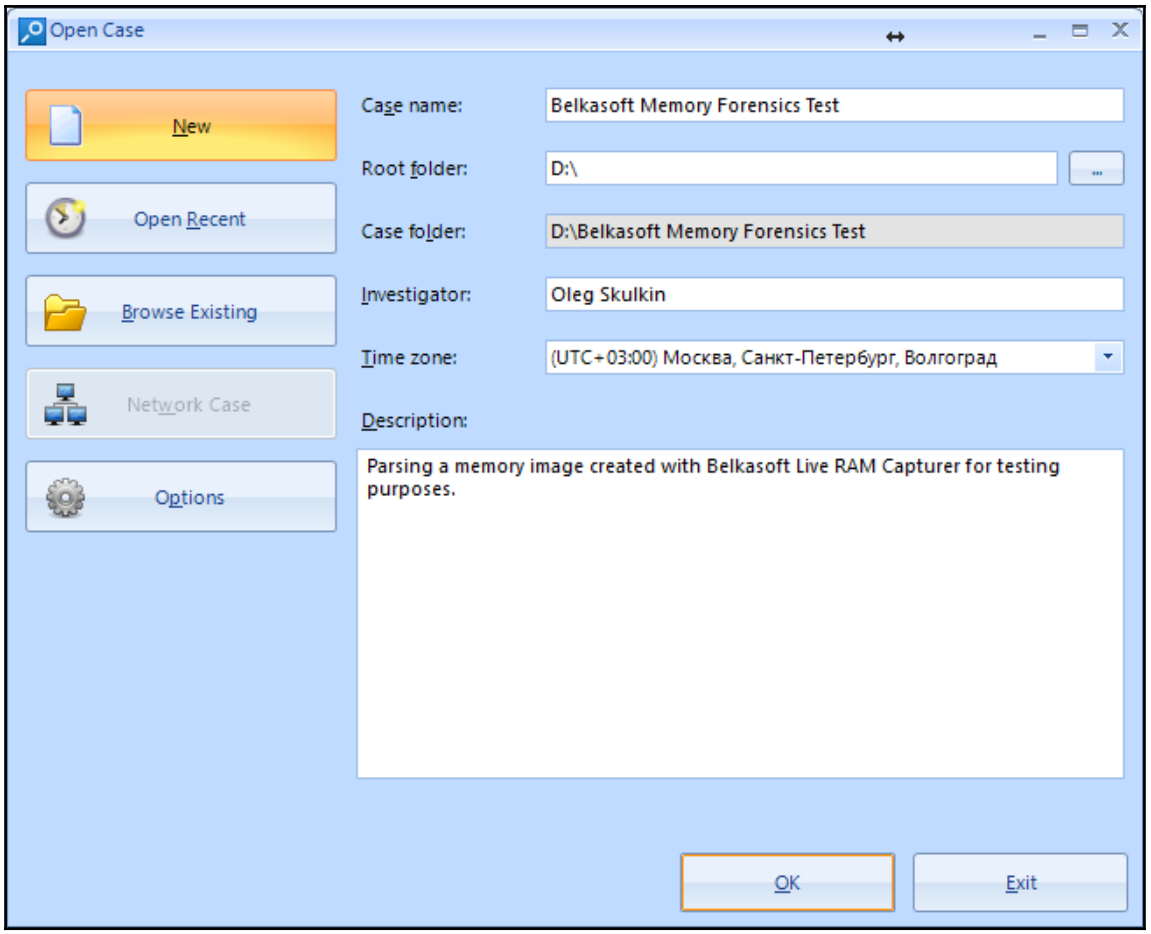


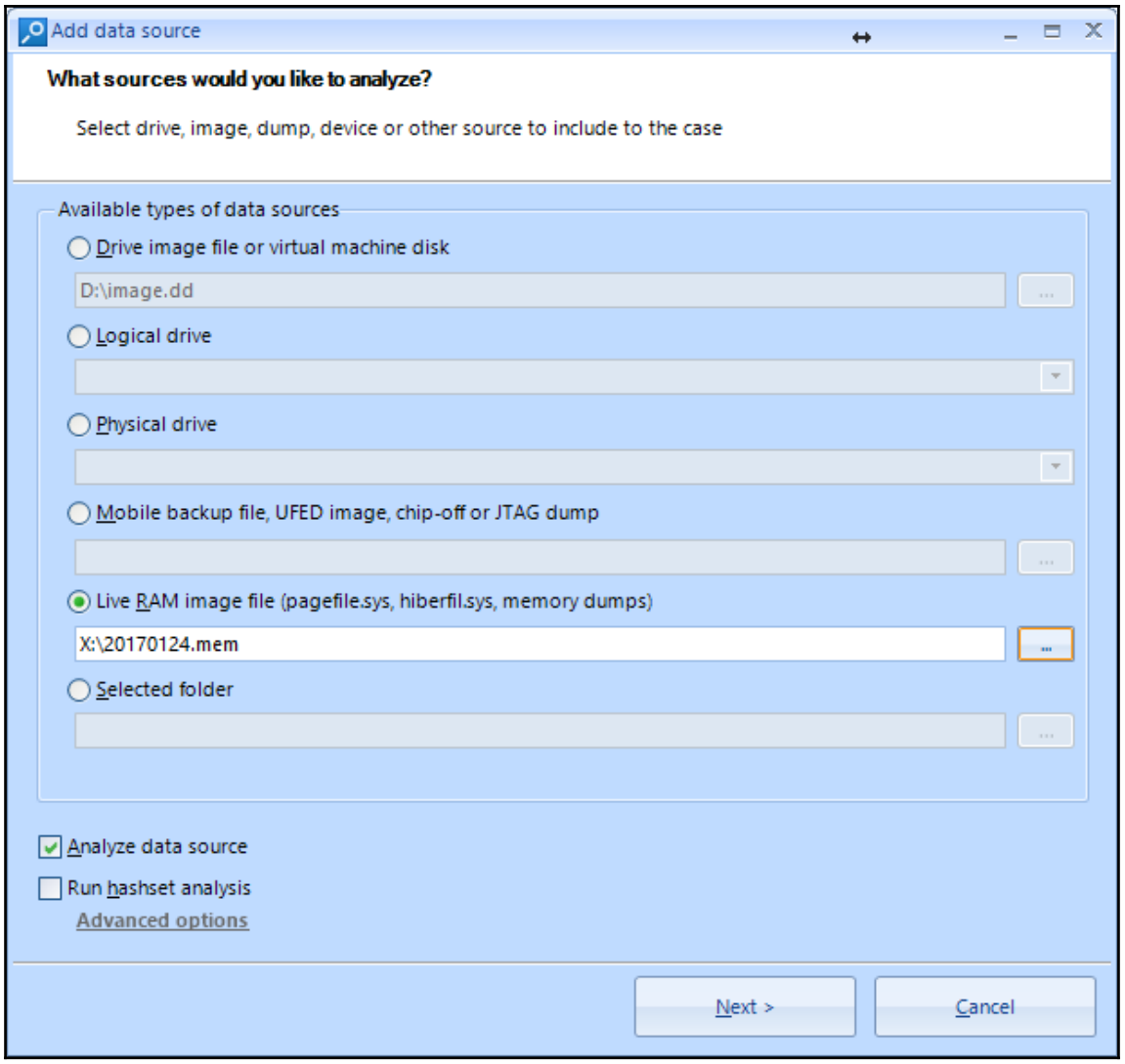


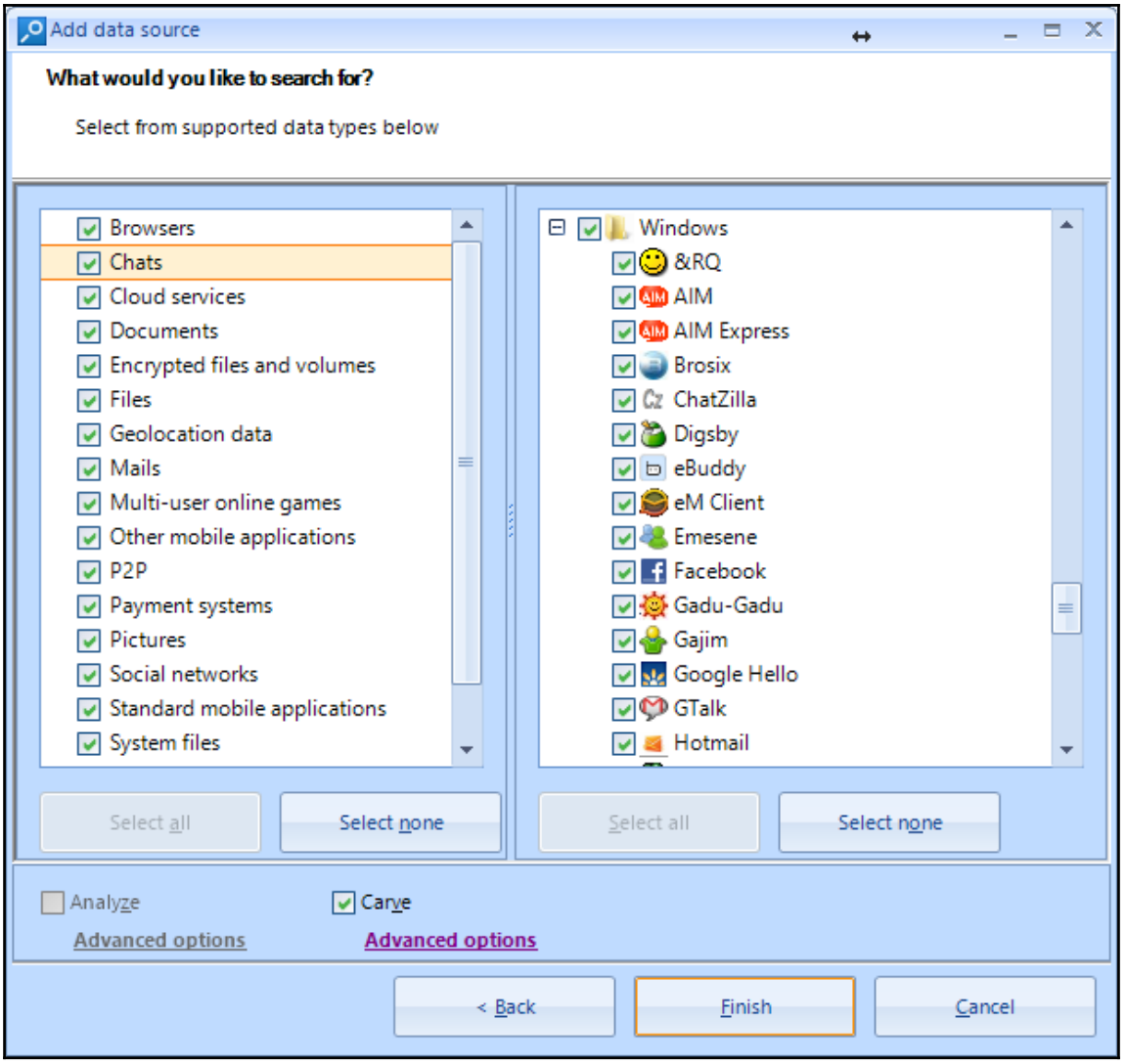
Chapter 2 : Windows Memory Acquisition and Analysis

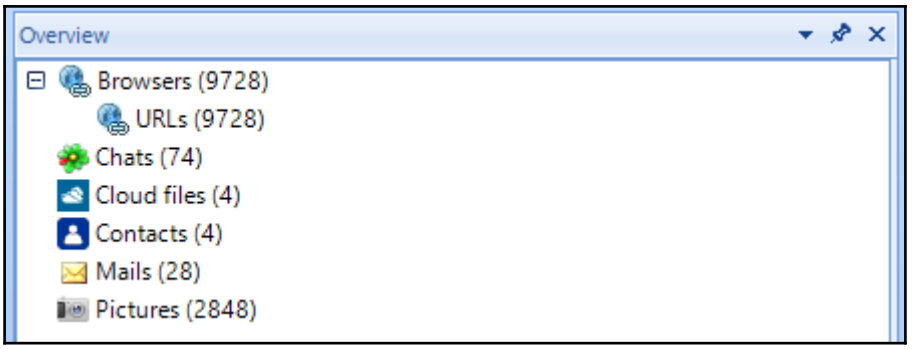

Belkasoft Live RAM Capturer
Select output folder path:
X:\
Loading device driver ...
Physical Memory Page Size = 4096
Total Physical Memory Size = 9208 MB
Capture!
Cancel
Close

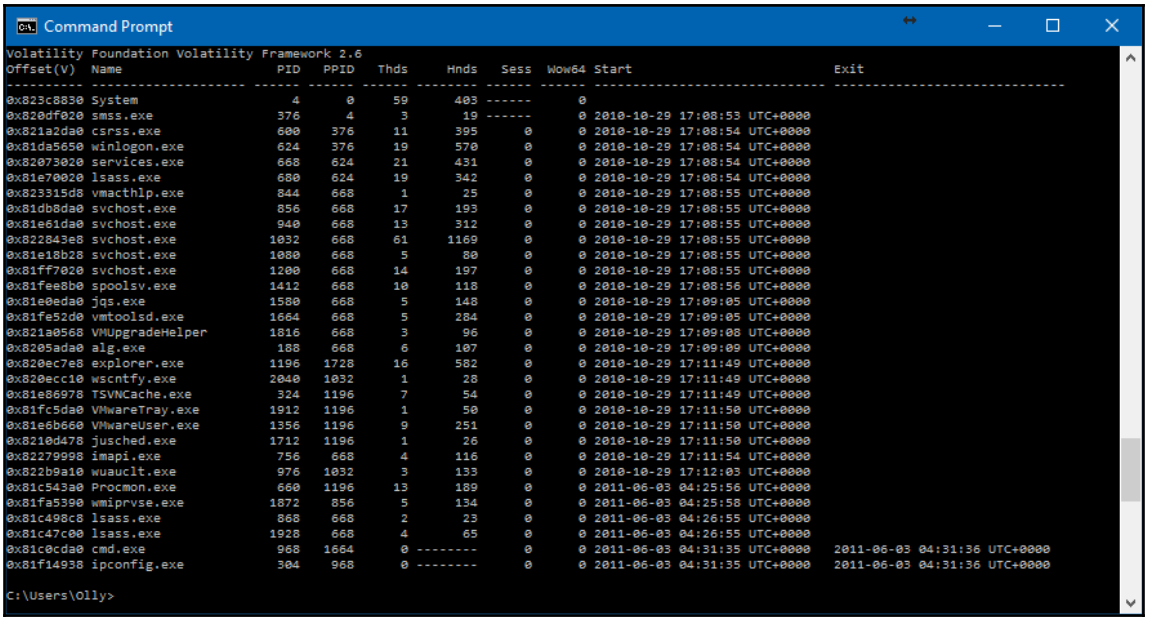

X:\DumpIt.exe
DumpIt 3.0.109.20161007
Copyright (C) 2007 - 2016, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2012 - 2014, MoonSols Limited <http://www.moonsols.com>
Copyright (C) 2015 - 2016, Comae Technologies FZE <http://www.comae.io>
Destination path: \??\X:\OLLY-WRKSTTN-20170202-083829.dmp
Computer name: OLLY-WRKSTTN
--> Proceed to the acquisition ? [y/n] y
[+] Information:
Dump Type: Microsoft Crash Dump
[+] Machine Information:
Windows version: 10.0.14393
MachineId: 2786EB00-5BCB-11D9-B0A4-14DAE9EDF567
TimeStamp: 131304983839950303
Cr3: 0x1aa000
KdCopyDataBlock: 0xfffff80390c46e00
KdDebuggerData: 0xfffff80390d66500
KdpDataBlockEncoded: 0xfffff80390db6108
Current date/time: [2017-2-2 (YYYY-MM-DD) 8:39:43 (UTC)]
+ Processing...

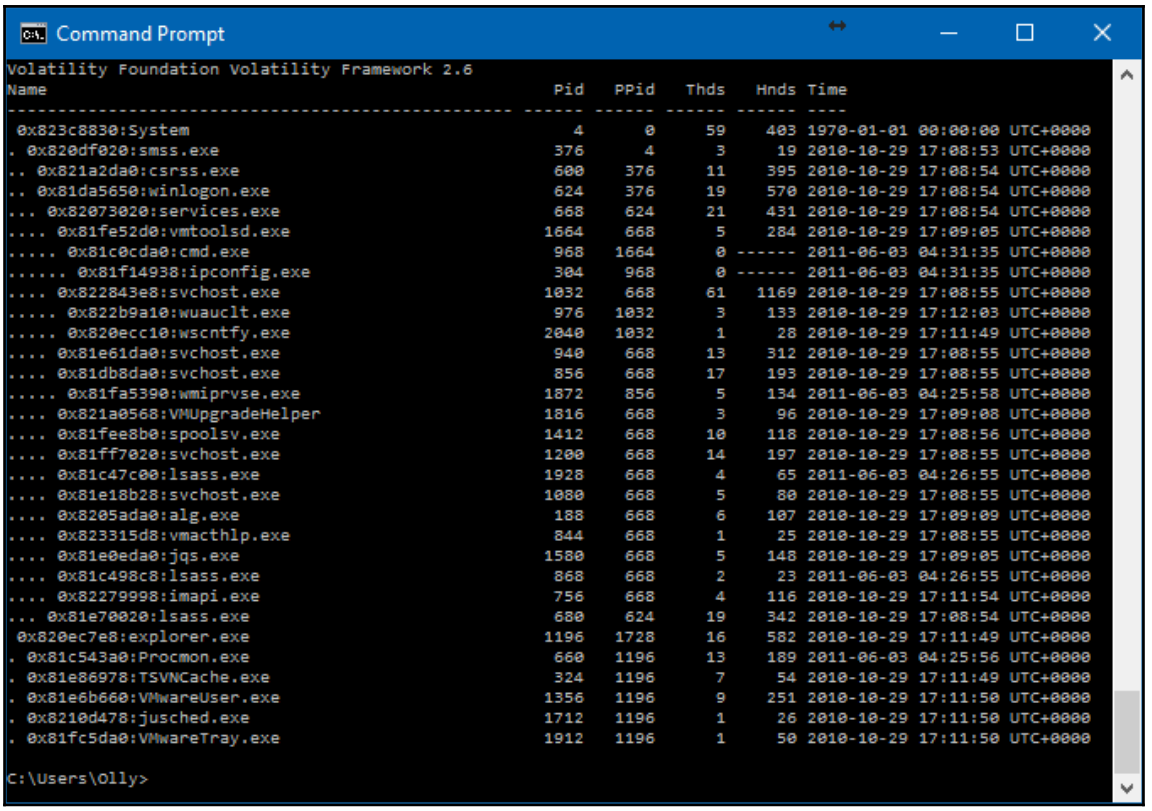

Open Case
New
Open Recent
Browse Existing
Network Case
Options
Case name:
Belkasoft Memory Forensics Test
Root folder:
D:\
...
Case folder:
D:\Belkasoft Memory Forensics Test
Investigator:
Oleg Skulkin
Time zone:
(UTC+03:00) Москва, Санкт-Петербург, Волгоград
Description:
Parsing a memory image created with Belkasoft Live RAM Capturer for testing purposes.
OK
Exit


Add data source
What sources would you like to analyze?
Select drive, image, dump, device or other source to include to the case
Available types of data sources
Drive image file or virtual machine disk
D:\image.dd
Logical drive
Physical drive
Mobile backup file, UFED image, chip-off or JTAG dump
Live RAM image file (pagefile.sys, hiberfil.sys, memory dumps)
X:\20170124.mem
Selected folder
Analyze data source
Run hashset analysis
Advanced options
Next >
Cancel

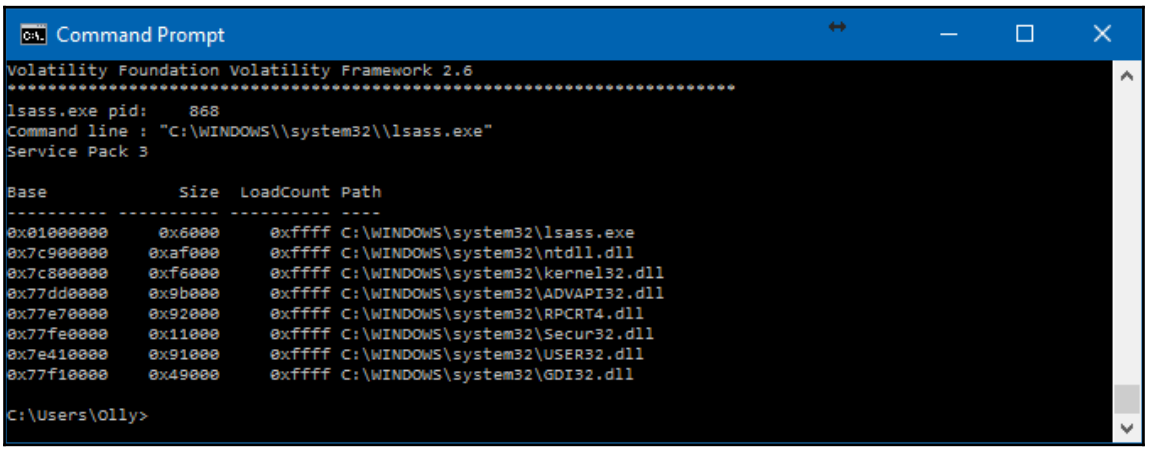

Add data source
What would you like to search for?
Select from supported data types below
Browsers
Chats
Cloud services
Documents
Encrypted files and volumes
Files
Geolocation data
Mails
Multi-user online games
Other mobile applications
P2P
Payment systems
Pictures
Social networks
Standard mobile applications
System files
Select all
Select none
Windows
&RQ
AIM
AIM Express
Brosix
ChatZilla
Digsby
eBuddy
eM Client
Emesene
Facebook
Gadu-Gadu
Gajim
Google Hello
GTalk
Hotmail
Select all
Select none
Analyze
Advanced options
Carve
Advanced options
< Back
Finish
Cancel


Overview
Browsers (9728)
URLs (9728)
Chats (74)
Cloud files (4)
Contacts (4)
Mails (28)
Pictures (2848)

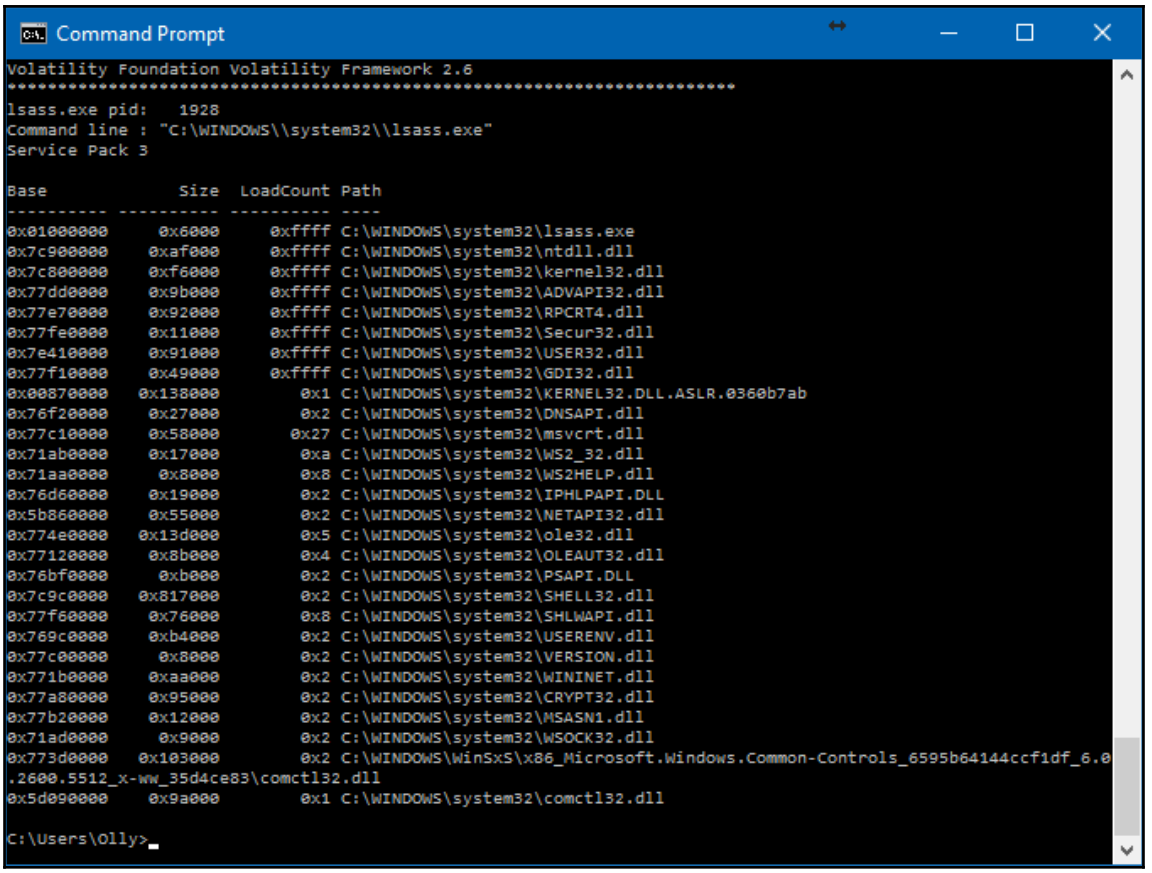

Command Prompt
Volatility Foundation Volatility Framework 2.6
Offset(V) Name PID PPID Thds Hnds Sess Wow64 Start Exit
0x823c8830 System 4 0 59 403 ------ 0
0x820df020 smss.exe 376 4 3 19 ------ 0 2010-10-29 17:08:53 UTC+0000
0x821a2da0 csrss.exe 600 376 11 395 0 0 2010-10-29 17:08:54 UTC+0000
0x81da5650 winlogon.exe 624 376 19 570 0 0 2010-10-29 17:08:54 UTC+0000
0x82073020 services.exe 668 624 21 431 0 0 2010-10-29 17:08:54 UTC+0000
0x81e70020 lsass.exe 680 624 19 342 0 0 2010-10-29 17:08:54 UTC+0000
0x823315d8 vmacthlp.exe 844 668 1 25 0 0 2010-10-29 17:08:55 UTC+0000
0x81db8da0 svchost.exe 856 668 17 193 0 0 2010-10-29 17:08:55 UTC+0000
0x81e61da0 svchost.exe 940 668 13 312 0 0 2010-10-29 17:08:55 UTC+0000
0x822843e8 svchost.exe 1032 668 61 1169 0 0 2010-10-29 17:08:55 UTC+0000
0x81e18b28 svchost.exe 1080 668 5 80 0 0 2010-10-29 17:08:55 UTC+0000
0x81ff7020 svchost.exe 1200 668 14 197 0 0 2010-10-29 17:08:55 UTC+0000
0x81fee8b0 spoolsv.exe 1412 668 10 118 0 0 2010-10-29 17:08:56 UTC+0000
0x81e0eda0 jqs.exe 1580 668 5 148 0 0 2010-10-29 17:09:05 UTC+0000
0x81fe52d0 vmtoolsd.exe 1664 668 5 284 0 0 2010-10-29 17:09:05 UTC+0000
0x821a0568 VMUpgradeHelper 1816 668 3 96 0 0 2010-10-29 17:09:08 UTC+0000
0x8205ada0 alg.exe 188 668 6 107 0 0 2010-10-29 17:09:09 UTC+0000
0x820ec7e8 explorer.exe 1196 1728 16 582 0 0 2010-10-29 17:11:49 UTC+0000
0x820ecc10 wscntfy.exe 2040 1032 1 28 0 0 2010-10-29 17:11:49 UTC+0000
0x81e86978 TSVNCache.exe 324 1196 7 54 0 0 2010-10-29 17:11:49 UTC+0000
0x81fc5da0 VMwareTray.exe 1912 1196 1 50 0 0 2010-10-29 17:11:50 UTC+0000
0x81e6b660 VMwareUser.exe 1356 1196 9 251 0 0 2010-10-29 17:11:50 UTC+0000
0x8210d478 jusched.exe 1712 1196 1 26 0 0 2010-10-29 17:11:50 UTC+0000
0x82279998 imapi.exe 756 668 4 116 0 0 2010-10-29 17:11:54 UTC+0000
0x822b9a10 wuauclt.exe 976 1032 3 133 0 0 2010-10-29 17:12:03 UTC+0000
0x81c543a0 Procmon.exe 660 1196 13 189 0 0 2011-06-03 04:25:56 UTC+0000
0x81fa5390 wmiprvse.exe 1872 856 5 134 0 0 2011-06-03 04:25:58 UTC+0000
0x81c498c8 lsass.exe 868 668 2 23 0 0 2011-06-03 04:26:55 UTC+0000
0x81c47c00 lsass.exe 1928 668 4 65 0 0 2011-06-03 04:26:55 UTC+0000
0x81c0cda0 cmd.exe 968 1664 0 -------- 0 0 2011-06-03 04:31:35 UTC+0000 2011-06-03 04:31:36 UTC+0000
0x81f14938 ipconfig.exe 304 968 0 -------- 0 0 2011-06-03 04:31:35 UTC+0000 2011-06-03 04:31:36 UTC+0000
C:\Users\Olly>

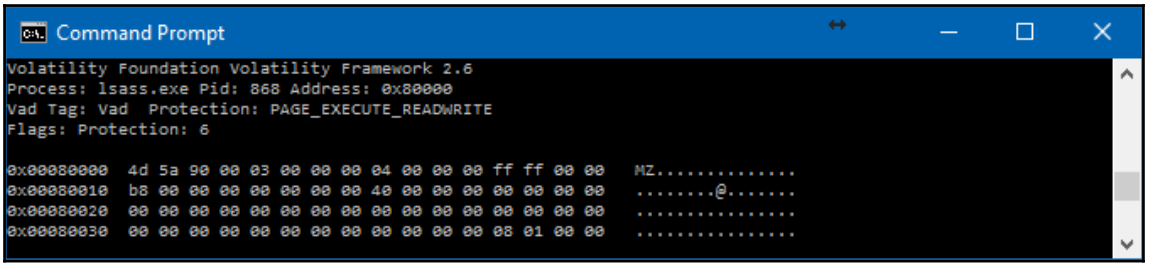


```
Command Prompt
Volatility Foundation Volatility Framework 2.6
Name                                                 Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x823c8830:System                                     4      0     59    403 1970-01-01 00:00:00 UTC+0000
. 0x820df020:smss.exe                                376      4      3     19 2010-10-29 17:08:53 UTC+0000
.. 0x821a2da0:csrss.exe                              600    376     11    395 2010-10-29 17:08:54 UTC+0000
.. 0x81da5650:winlogon.exe                           624    376     19    570 2010-10-29 17:08:54 UTC+0000
... 0x82073020:services.exe                          668    624     21    431 2010-10-29 17:08:54 UTC+0000
.... 0x81fe52d0:vmtoolsd.exe                        1664    668      5    284 2010-10-29 17:09:05 UTC+0000
..... 0x81c0cda0:cmd.exe                             968   1664      0 ------ 2011-06-03 04:31:35 UTC+0000
...... 0x81f14938:ipconfig.exe                       304    968      0 ------ 2011-06-03 04:31:35 UTC+0000
.... 0x822843e8:svchost.exe                         1032    668     61   1169 2010-10-29 17:08:55 UTC+0000
..... 0x822b9a10:wuauclt.exe                         976   1032      3    133 2010-10-29 17:12:03 UTC+0000
..... 0x820ecc10:wscntfy.exe                        2040   1032      1     28 2010-10-29 17:11:49 UTC+0000
.... 0x81e61da0:svchost.exe                          940    668     13    312 2010-10-29 17:08:55 UTC+0000
.... 0x81db8da0:svchost.exe                          856    668     17    193 2010-10-29 17:08:55 UTC+0000
..... 0x81fa5390:wmiprvse.exe                       1872    856      5    134 2011-06-03 04:25:58 UTC+0000
.... 0x821a0568:VMUpgradeHelper                     1816    668      3     96 2010-10-29 17:09:08 UTC+0000
.... 0x81fee8b0:spoolsv.exe                         1412    668     10    118 2010-10-29 17:08:56 UTC+0000
.... 0x81ff7020:svchost.exe                         1200    668     14    197 2010-10-29 17:08:55 UTC+0000
.... 0x81c47c00:lsass.exe                           1928    668      4     65 2011-06-03 04:26:55 UTC+0000
.... 0x81e18b28:svchost.exe                         1080    668      5     80 2010-10-29 17:08:55 UTC+0000
.... 0x8205ada0:alg.exe                              188    668      6    107 2010-10-29 17:09:09 UTC+0000
.... 0x823315d8:vmacthlp.exe                         844    668      1     25 2010-10-29 17:08:55 UTC+0000
.... 0x81e0eda0:jqs.exe                             1580    668      5    148 2010-10-29 17:09:05 UTC+0000
.... 0x81c498c8:lsass.exe                            868    668      2     23 2011-06-03 04:26:55 UTC+0000
.... 0x82279998:imapi.exe                            756    668      4    116 2010-10-29 17:11:54 UTC+0000
... 0x81e70020:lsass.exe                             680    624     19    342 2010-10-29 17:08:54 UTC+0000
 0x820ec7e8:explorer.exe                            1196   1728     16    582 2010-10-29 17:11:49 UTC+0000
. 0x81c543a0:Procmon.exe                             660   1196     13    189 2011-06-03 04:25:56 UTC+0000
. 0x81e86978:TSVNCache.exe                           324   1196      7     54 2010-10-29 17:11:49 UTC+0000
. 0x81e6b660:VMwareUser.exe                         1356   1196      9    251 2010-10-29 17:11:50 UTC+0000
. 0x8210d478:jusched.exe                            1712   1196      1     26 2010-10-29 17:11:50 UTC+0000
. 0x81fc5da0:VMwareTray.exe                         1912   1196      1     50 2010-10-29 17:11:50 UTC+0000

C:\Users\Olly>
```

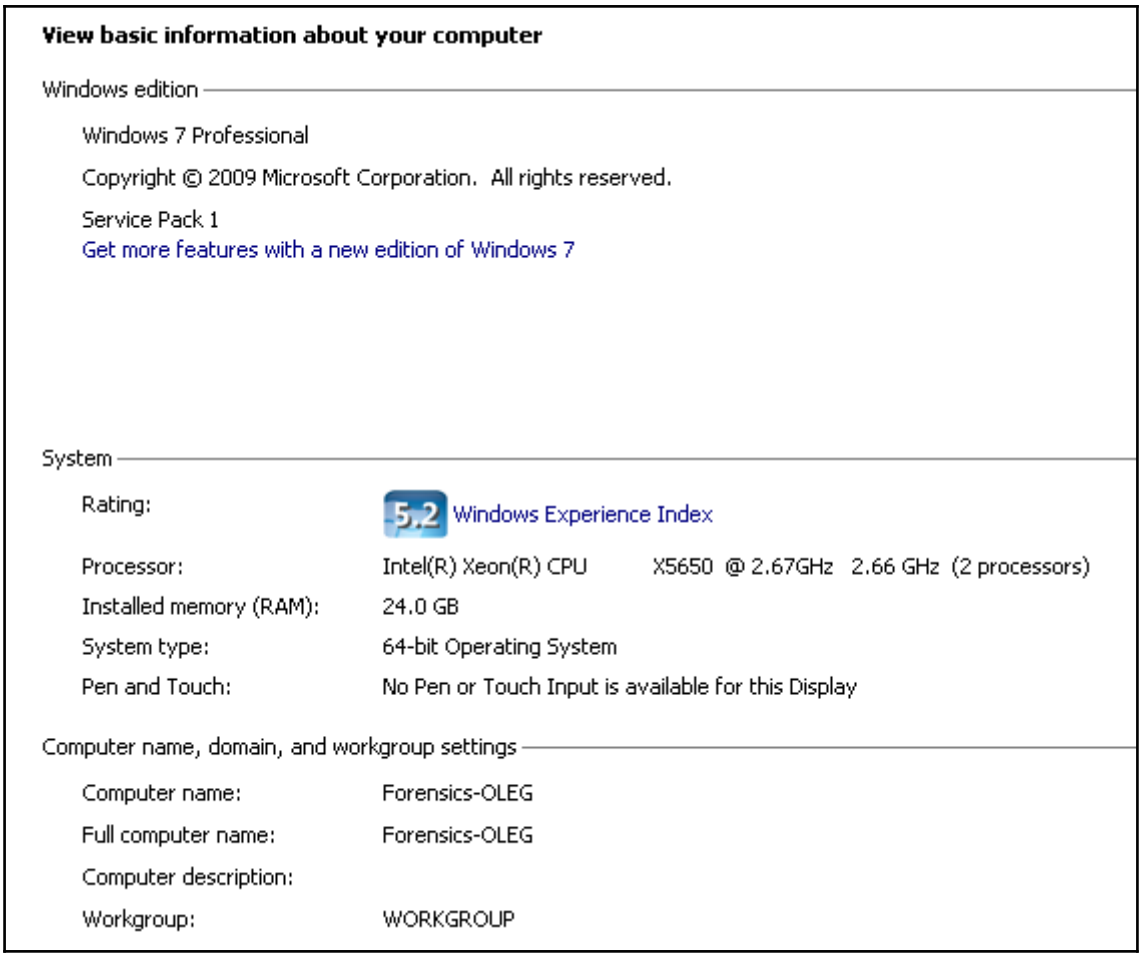


```
Command Prompt
Volatility Foundation Volatility Framework 2.6
**************************************************************************
lsass.exe pid:    868
Command line : "C:\WINDOWS\\system32\\lsass.exe"
Service Pack 3

Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x01000000     0x6000     0xffff C:\WINDOWS\system32\lsass.exe
0x7c900000    0xaf000     0xffff C:\WINDOWS\system32\ntdll.dll
0x7c800000    0xf6000     0xffff C:\WINDOWS\system32\kernel32.dll
0x77dd0000    0x9b000     0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000    0x92000     0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000    0x11000     0xffff C:\WINDOWS\system32\Secur32.dll
0x7e410000    0x91000     0xffff C:\WINDOWS\system32\USER32.dll
0x77f10000    0x49000     0xffff C:\WINDOWS\system32\GDI32.dll

C:\Users\Olly>
```

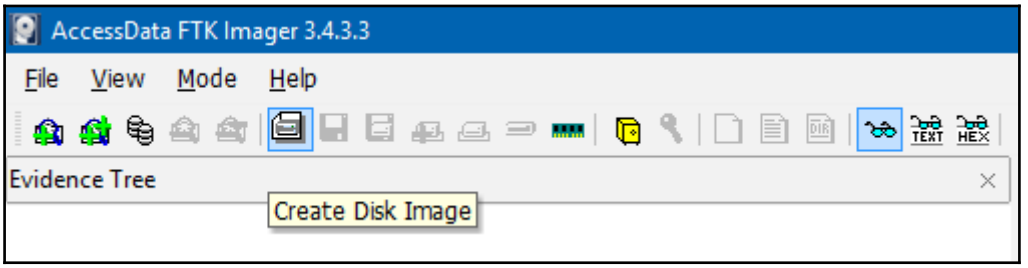

Command Prompt
Volatility Foundation Volatility Framework 2.6
****
lsass.exe pid: 1928
Command line : "C:\WINDOWS\\system32\\lsass.exe"
Service Pack 3
Base Size LoadCount Path
0x01000000 0x6000 0xffff C:\WINDOWS\system32\lsass.exe
0x7c900000 0xaf000 0xffff C:\WINDOWS\system32\ntdll.dll
0x7c800000 0xf6000 0xffff C:\WINDOWS\system32\kernel32.dll
0x77dd0000 0x9b000 0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000 0x92000 0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000 0x11000 0xffff C:\WINDOWS\system32\Secur32.dll
0x7e410000 0x91000 0xffff C:\WINDOWS\system32\USER32.dll
0x77f10000 0x49000 0xffff C:\WINDOWS\system32\GDI32.dll
0x00870000 0x138000 0x1 C:\WINDOWS\system32\KERNEL32.DLL.ASLR.0360b7ab
0x76f20000 0x27000 0x2 C:\WINDOWS\system32\DNSAPI.dll
0x77c10000 0x58000 0x27 C:\WINDOWS\system32\msvcrt.dll
0x71ab0000 0x17000 0xa C:\WINDOWS\system32\WS2_32.dll
0x71aa0000 0x8000 0x8 C:\WINDOWS\system32\WS2HELP.dll
0x76d60000 0x19000 0x2 C:\WINDOWS\system32\IPHLPAPI.DLL
0x5b860000 0x55000 0x2 C:\WINDOWS\system32\NETAPI32.dll
0x774e0000 0x13d000 0x5 C:\WINDOWS\system32\ole32.dll
0x77120000 0x8b000 0x4 C:\WINDOWS\system32\OLEAUT32.dll
0x76bf0000 0xb000 0x2 C:\WINDOWS\system32\PSAPI.DLL
0x7c9c0000 0x817000 0x2 C:\WINDOWS\system32\SHELL32.dll
0x77f60000 0x76000 0x8 C:\WINDOWS\system32\SHLWAPI.dll
0x769c0000 0xb4000 0x2 C:\WINDOWS\system32\USERENV.dll
0x77c00000 0x8000 0x2 C:\WINDOWS\system32\VERSION.dll
0x771b0000 0xaa000 0x2 C:\WINDOWS\system32\WININET.dll
0x77a80000 0x95000 0x2 C:\WINDOWS\system32\CRYPT32.dll
0x77b20000 0x12000 0x2 C:\WINDOWS\system32\MSASN1.dll
0x71ad0000 0x9000 0x2 C:\WINDOWS\system32\WSOCK32.dll
0x773d0000 0x103000 0x2 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
0x5d090000 0x9a000 0x1 C:\WINDOWS\system32\comctl32.dll
C:\Users\Olly>

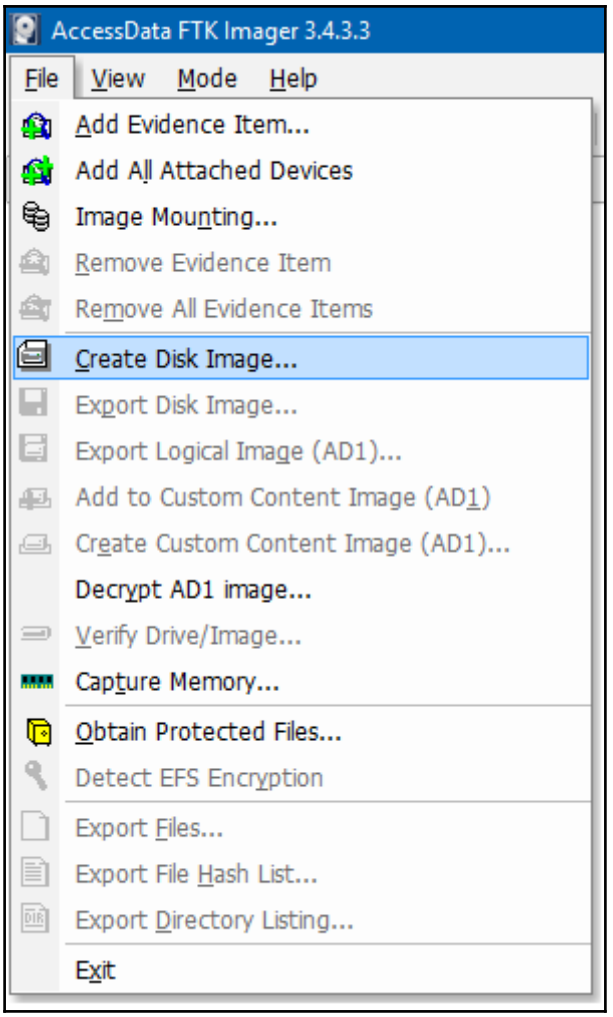

Command Prompt
Volatility Foundation Volatility Framework 2.6
Process: lsass.exe Pid: 868 Address: 0x80000
Vad Tag: Vad Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6
0x00080000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..............
0x00080010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ....@.......
0x00080020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x00080030 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 ....

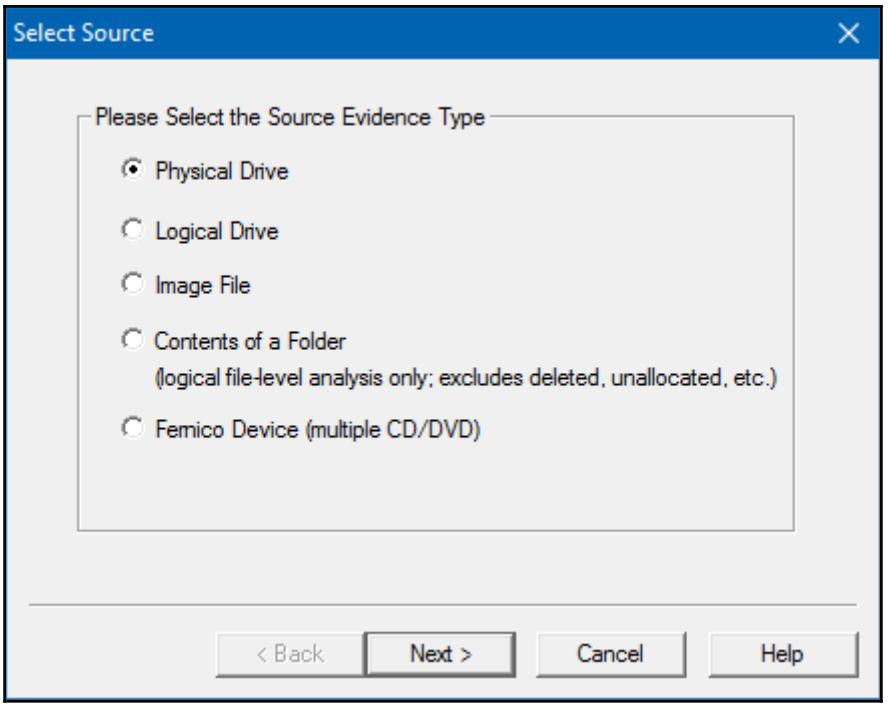

About Windows
Windows 10
Microsoft Windows
Version 1607 (OS Build 14393.693)
© 2016 Microsoft Corporation. All rights reserved.
The Windows 10 Home operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.
This product is licensed under the Microsoft Software Licence Terms to:
Razer
OK

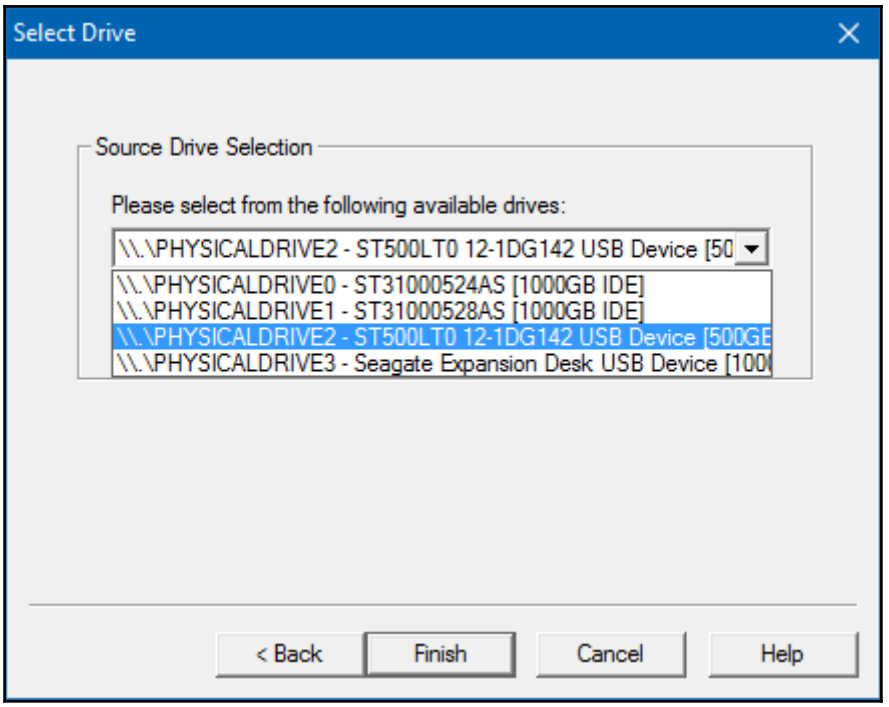

View basic information about your computer
Windows edition
Windows 7 Professional
Copyright © 2009 Microsoft Corporation. All rights reserved.
Service Pack 1
Get more features with a new edition of Windows 7
System
Rating:
5.2
Windows Experience Index
Processor:
Intel(R) Xeon(R) CPU X5650 @ 2.67GHz 2.66 GHz (2 processors)
Installed memory (RAM):
24.0 GB
System type:
64-bit Operating System
Pen and Touch:
No Pen or Touch Input is available for this Display
Computer name, domain, and workgroup settings
Computer name:
Forensics-OLEG
Full computer name:
Forensics-OLEG
Computer description:
Workgroup:
WORKGROUP

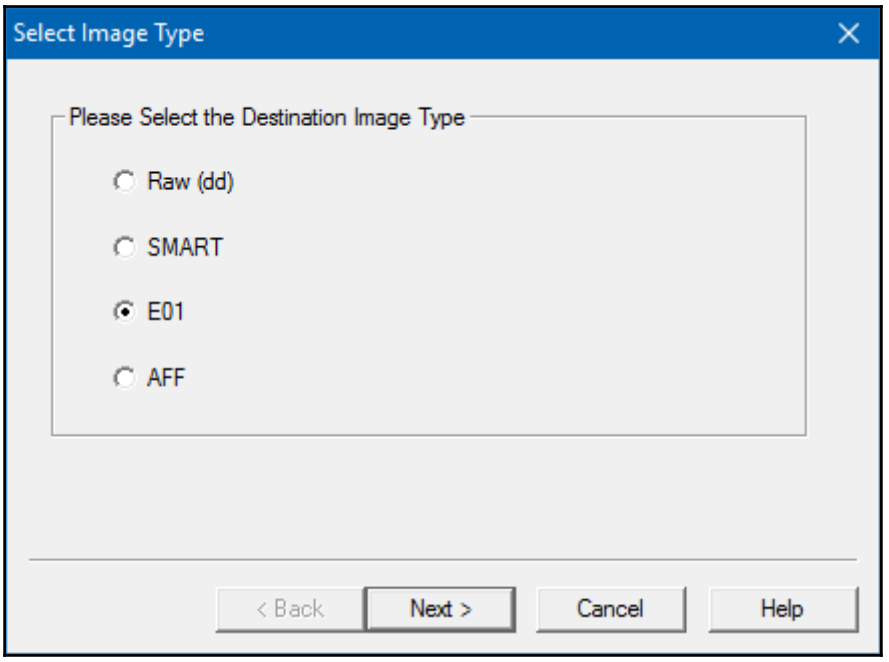
Chapter 3 : Windows Drive Acquisition

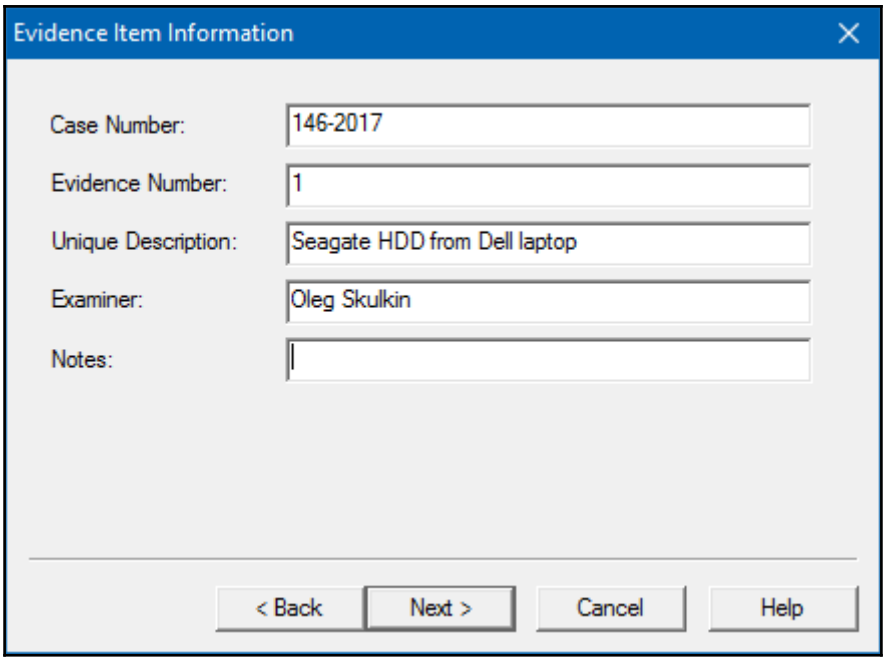


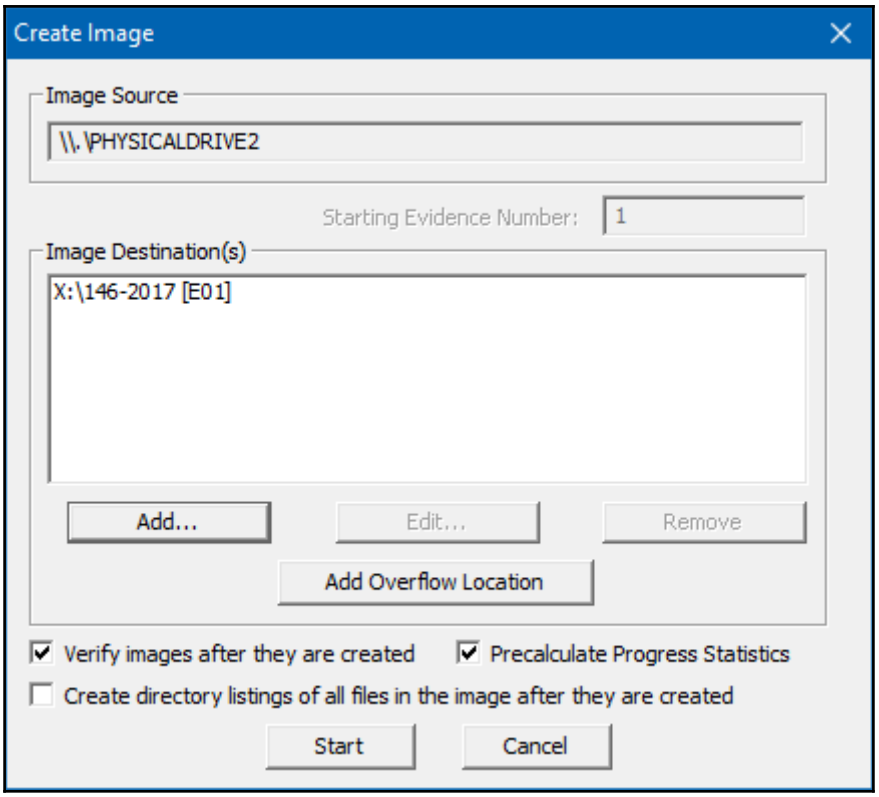

AccessData FTK Imager 3.4.3.3
File
View
Mode
Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...
Add to Custom Content Image (AD1)
Create Custom Content Image (AD1)...
Decrypt AD1 image...
Verify Drive/Image...
Capture Memory...
Obtain Protected Files...
Detect EFS Encryption
Export Files...
Export File Hash List...
Export Directory Listing...
Exit

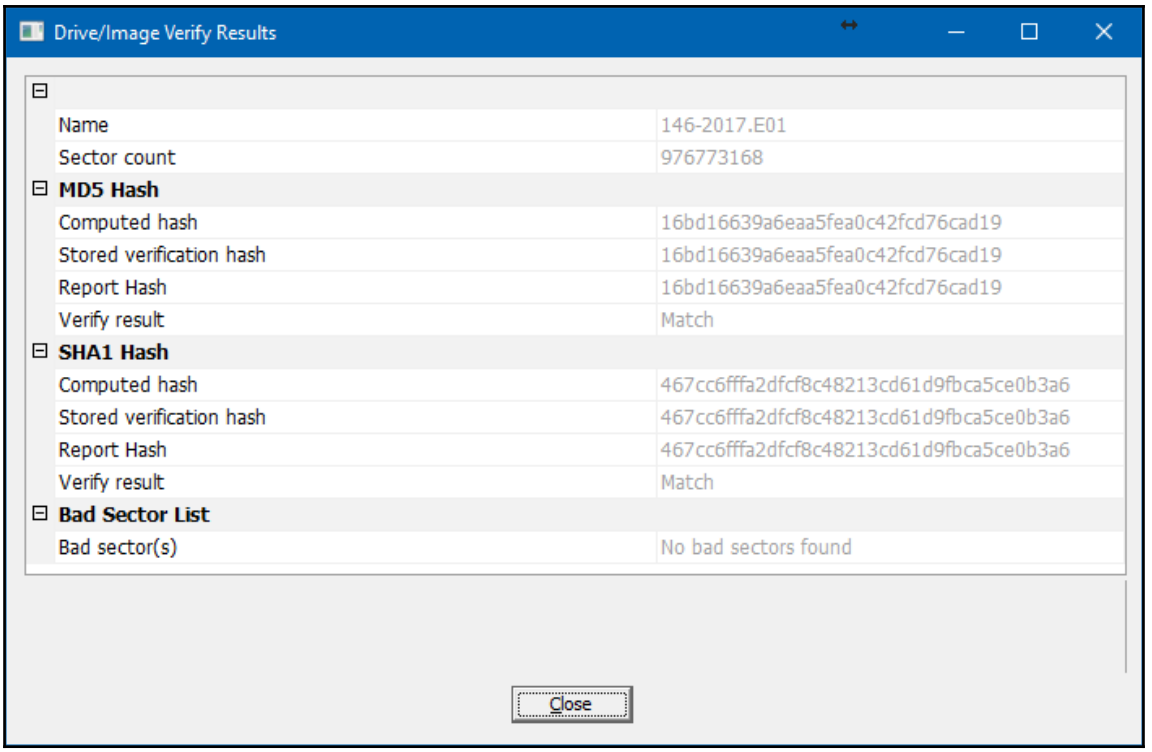

Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
Fernico Device (multiple CD/DVD)
< Back
Next >
Cancel
Help

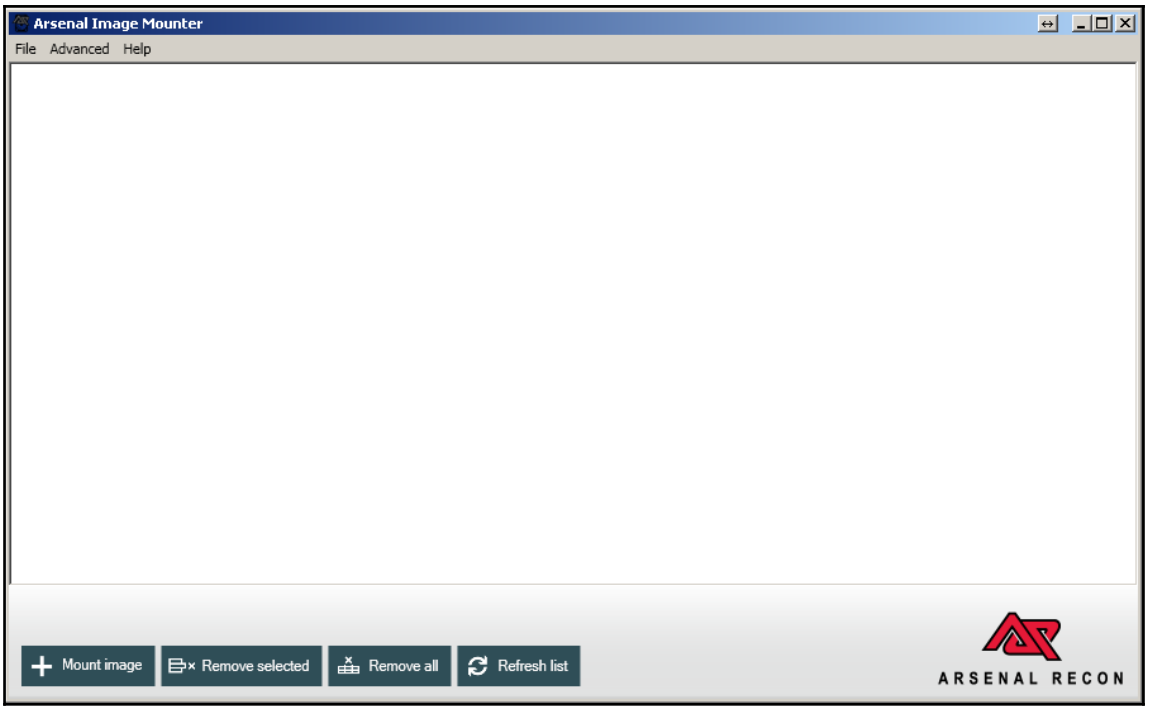

Select Drive
Source Drive Selection
Please select from the following available drives:
\\.\PHYSICALDRIVE2 - ST500LT0 12-1DG142 USB Device [50
\\.\PHYSICALDRIVE0 - ST31000524AS [1000GB IDE]
\\.\PHYSICALDRIVE1 - ST31000528AS [1000GB IDE]
\\.\PHYSICALDRIVE2 - ST500LT0 12-1DG142 USB Device [500GE
\\.\PHYSICALDRIVE3 - Seagate Expansion Desk USB Device [100
< Back
Finish
Cancel
Help

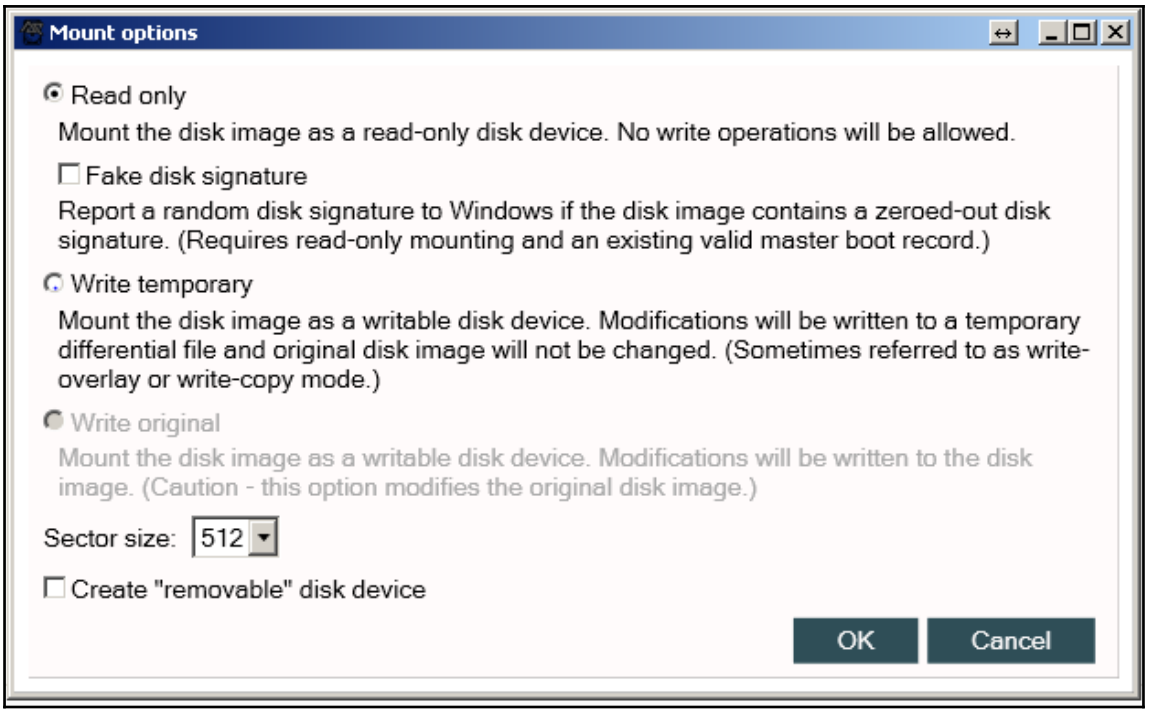

Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
AFF
< Back
Next >
Cancel
Help


Evidence Item Information
Case Number:
146-2017
Evidence Number:
1
Unique Description:
Seagate HDD from Dell laptop
Examiner:
Oleg Skulkin
Notes:
< Back
Next >
Cancel
Help

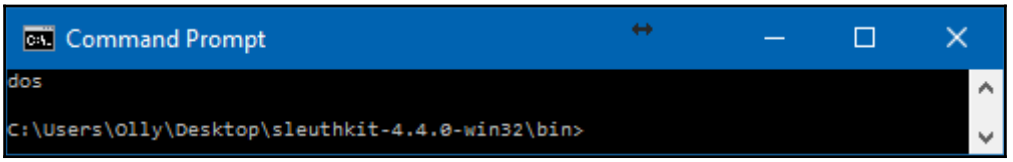

Create Image
Image Source
\\.\PHYSICALDRIVE2
Starting Evidence Number:
1
Image Destination(s)
X:\146-2017 [E01]
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start
Cancel

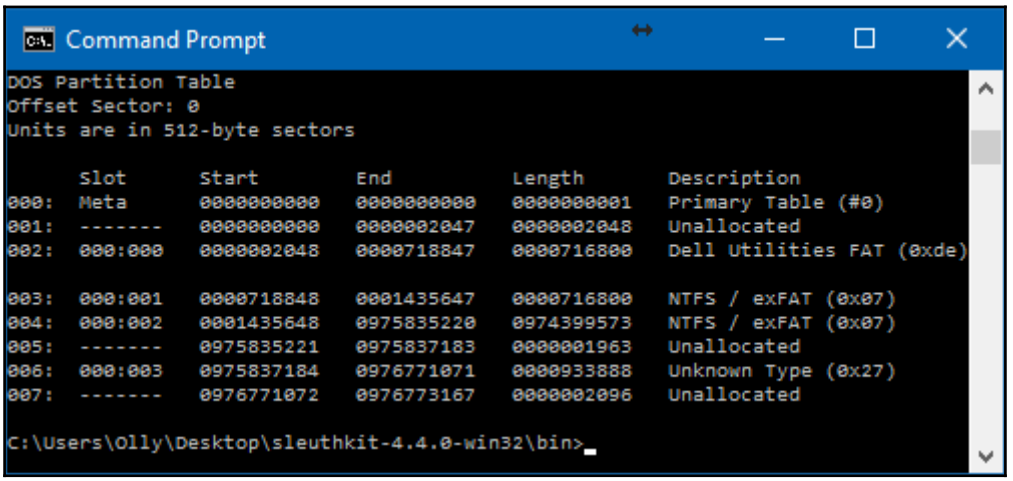

Drive/Image Verify Results
Name
146-2017.E01
Sector count
976773168
MD5 Hash
Computed hash
16bd16639a6eaa5fea0c42fcd76cad19
Stored verification hash
16bd16639a6eaa5fea0c42fcd76cad19
Report Hash
16bd16639a6eaa5fea0c42fcd76cad19
Verify result
Match
SHA1 Hash
Computed hash
467cc6fffa2dfcf8c48213cd61d9fbca5ce0b3a6
Stored verification hash
467cc6fffa2dfcf8c48213cd61d9fbca5ce0b3a6
Report Hash
467cc6fffa2dfcf8c48213cd61d9fbca5ce0b3a6
Verify result
Match
Bad Sector List
Bad sector(s)
No bad sectors found
Close

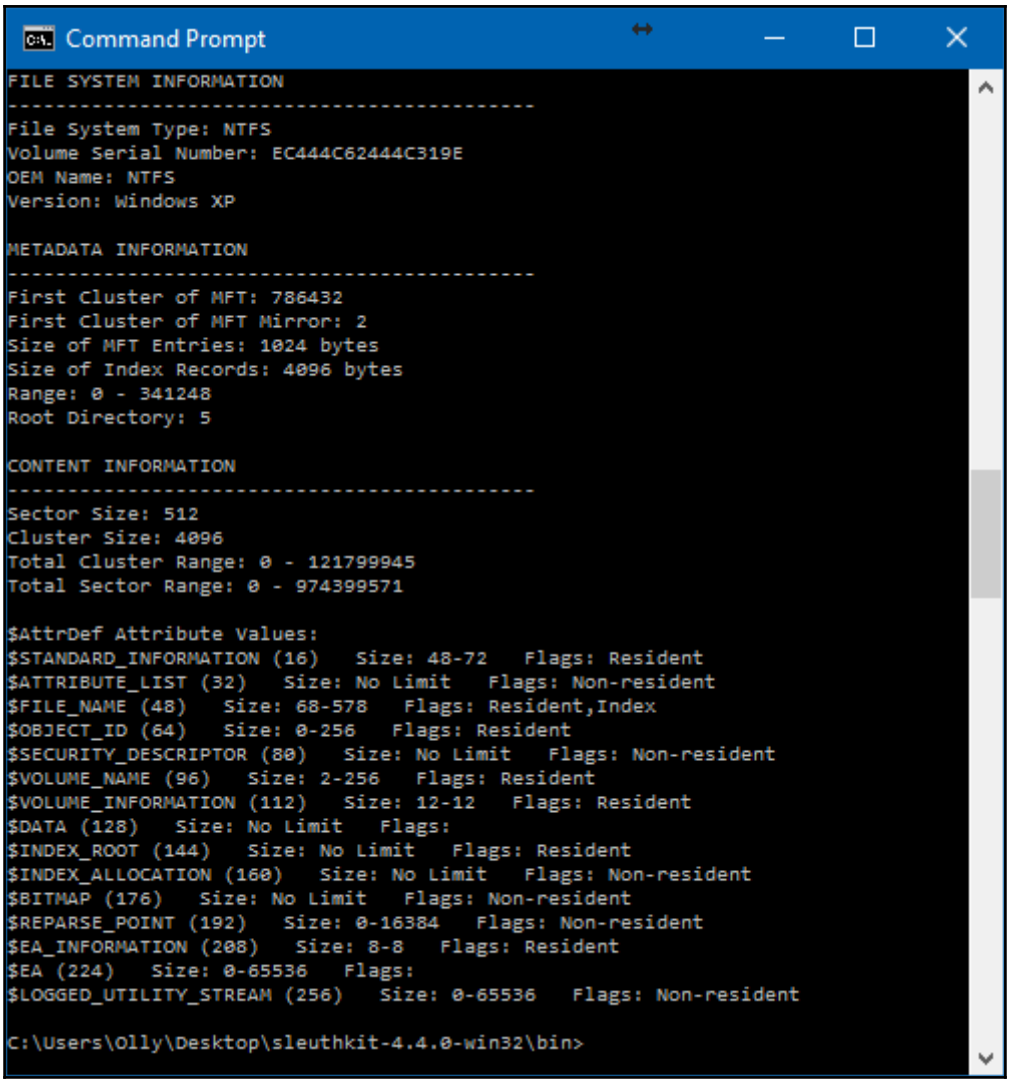

Arsenal Image Mounter
File
Advanced
Help
Mount image
Remove selected
Remove all
Refresh list
ARSENAL RECON

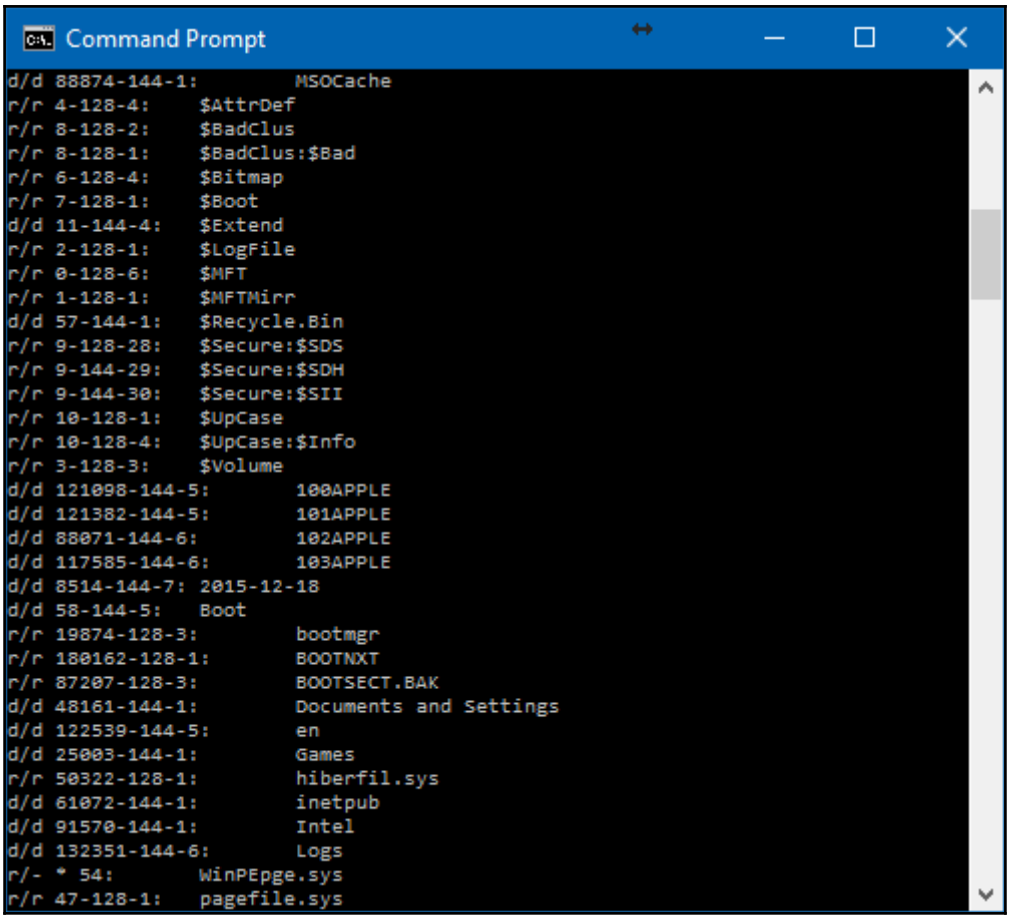

Mount options
Read only
Mount the disk image as a read-only disk device. No write operations will be allowed.
Fake disk signature
Report a random disk signature to Windows if the disk image contains a zeroed-out disk signature. (Requires read-only mounting and an existing valid master boot record.)
Write temporary
Mount the disk image as a writable disk device. Modifications will be written to a temporary differential file and original disk image will not be changed. (Sometimes referred to as write-overlay or write-copy mode.)
Write original
Mount the disk image as a writable disk device. Modifications will be written to the disk image. (Caution - this option modifies the original disk image.)
Sector size:
512
Create "removable" disk device
OK
Cancel

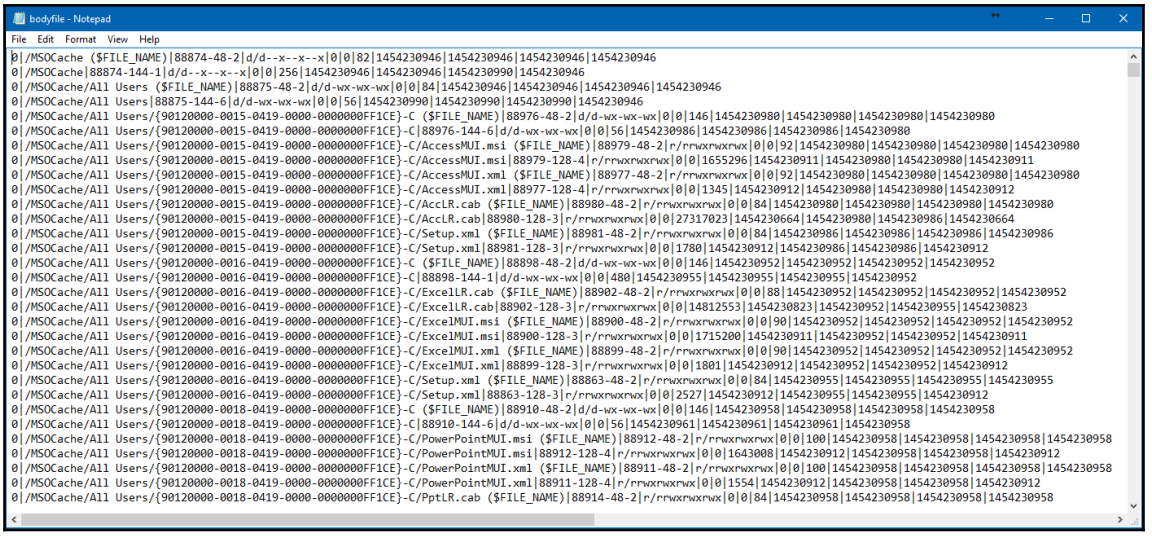
Chapter 4 : Windows File Systems Analysis






Command Prompt
FILE SYSTEM INFORMATION
File System Type: NTFS
Volume Serial Number: EC444C62444C319E
OEM Name: NTFS
Version: Windows XP
METADATA INFORMATION
First Cluster of MFT: 786432
First Cluster of MFT Mirror: 2
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 341248
Root Directory: 5
CONTENT INFORMATION
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 121799945
Total Sector Range: 0 - 974399571
$AttrDef Attribute Values:
$STANDARD_INFORMATION (16) Size: 48-72 Flags: Resident
$ATTRIBUTE_LIST (32) Size: No Limit Flags: Non-resident
$FILE_NAME (48) Size: 68-578 Flags: Resident,Index
$OBJECT_ID (64) Size: 0-256 Flags: Resident
$SECURITY_DESCRIPTOR (80) Size: No Limit Flags: Non-resident
$VOLUME_NAME (96) Size: 2-256 Flags: Resident
$VOLUME_INFORMATION (112) Size: 12-12 Flags: Resident
$DATA (128) Size: No Limit Flags:
$INDEX_ROOT (144) Size: No Limit Flags: Resident
$INDEX_ALLOCATION (160) Size: No Limit Flags: Non-resident
$BITMAP (176) Size: No Limit Flags: Non-resident
$REPARSE_POINT (192) Size: 0-16384 Flags: Non-resident
$EA_INFORMATION (208) Size: 8-8 Flags: Resident
$EA (224) Size: 0-65536 Flags:
$LOGGED_UTILITY_STREAM (256) Size: 0-65536 Flags: Non-resident
C:\Users\Olly\Desktop\sleuthkit-4.4.0-win32\bin>


Command Prompt
d/d 88874-144-1: MSOCache
r/r 4-128-4: $AttrDef
r/r 8-128-2: $BadClus
r/r 8-128-1: $BadClus:$Bad
r/r 6-128-4: $Bitmap
r/r 7-128-1: $Boot
d/d 11-144-4: $Extend
r/r 2-128-1: $LogFile
r/r 0-128-6: $MFT
r/r 1-128-1: $MFTMirr
d/d 57-144-1: $Recycle.Bin
r/r 9-128-28: $Secure:$SDS
r/r 9-144-29: $Secure:$SDH
r/r 9-144-30: $Secure:$SII
r/r 10-128-1: $UpCase
r/r 10-128-4: $UpCase:$Info
r/r 3-128-3: $Volume
d/d 121098-144-5: 100APPLE
d/d 121382-144-5: 101APPLE
d/d 88071-144-6: 102APPLE
d/d 117585-144-6: 103APPLE
d/d 8514-144-7: 2015-12-18
d/d 58-144-5: Boot
r/r 19874-128-3: bootmgr
r/r 180162-128-1: BOOTNXT
r/r 87207-128-3: BOOTSECT.BAK
d/d 48161-144-1: Documents and Settings
d/d 122539-144-5: en
d/d 25003-144-1: Games
r/r 50322-128-1: hiberfil.sys
d/d 61072-144-1: inetpub
d/d 91570-144-1: Intel
d/d 132351-144-6: Logs
r/- * 54: WinPEpge.sys
r/r 47-128-1: pagefile.sys



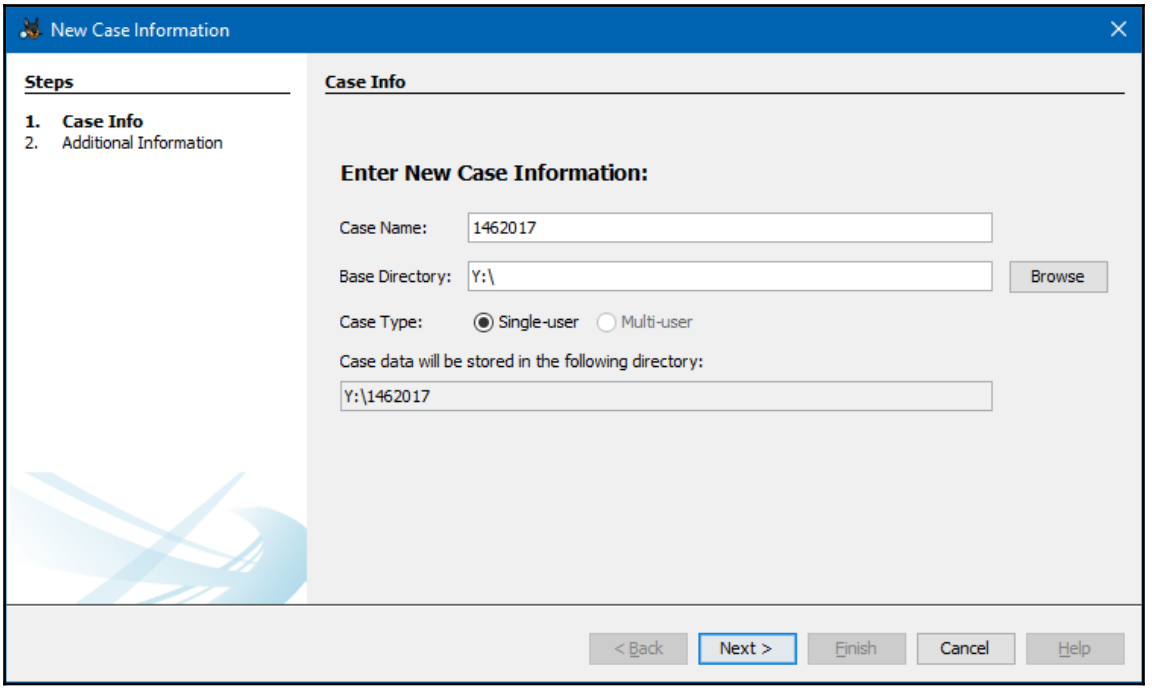
bodyfile - Notepad

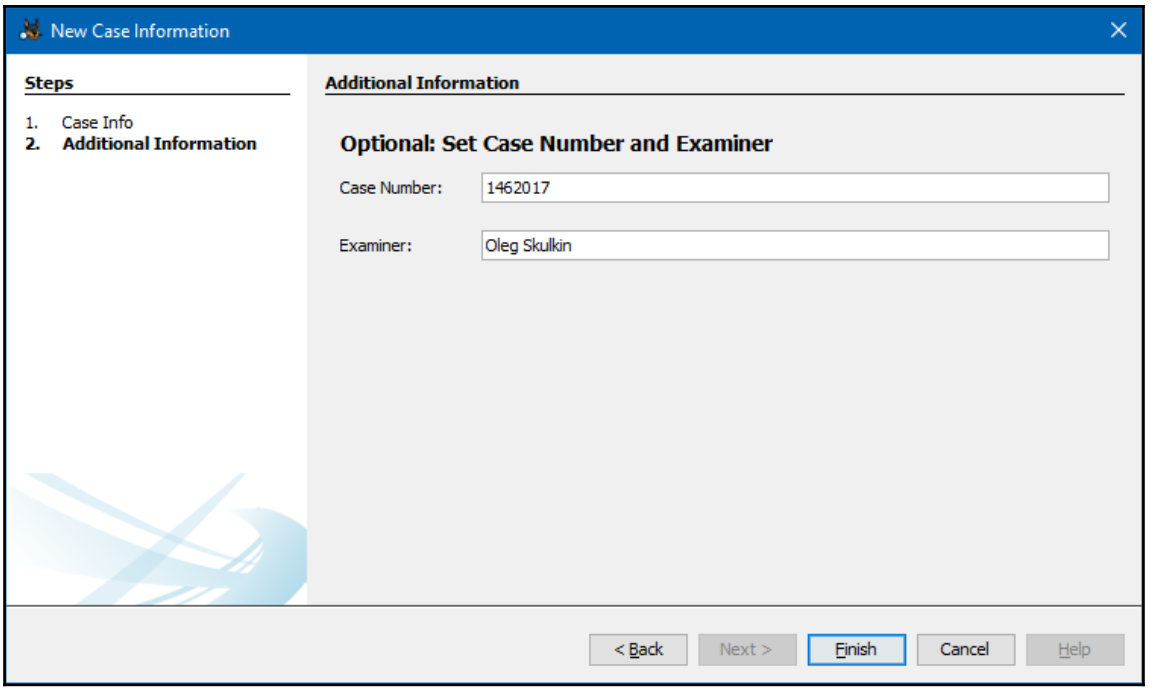
File Edit Format View Help

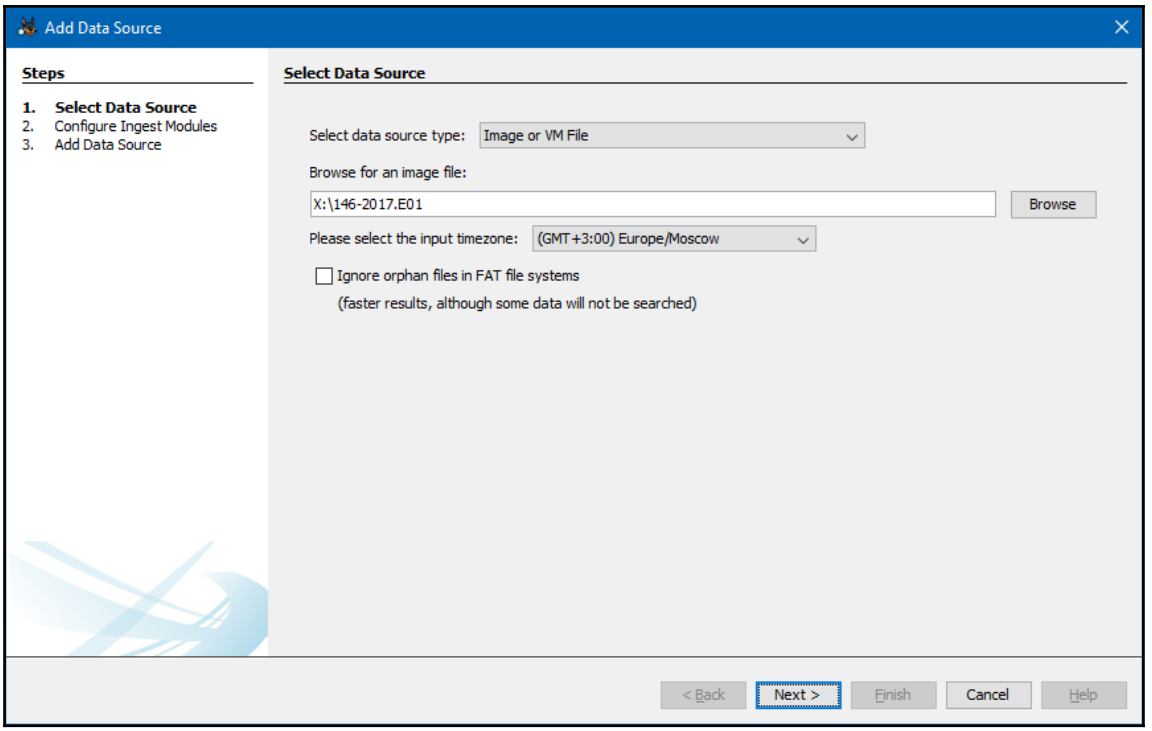
```
0|/MSOCache ($FILE_NAME)|88874-48-2|d/d--x--x--x|0|0|82|1454230946|1454230946|1454230946|1454230946
0|/MSOCache|88874-144-1|d/d--x--x--x|0|0|256|1454230946|1454230946|1454230990|1454230946
0|/MSOCache/All Users ($FILE_NAME)|88875-48-2|d/d-wx-wx-wx|0|0|84|1454230946|1454230946|1454230946|1454230946
0|/MSOCache/All Users|88875-144-6|d/d-wx-wx-wx|0|0|56|1454230990|1454230990|1454230990|1454230946
0|/MSOCache/All Users/{90120000-0015-0419-0000-0000000FF1CE}-C ($FILE_NAME)|88976-48-2|d/d-wx-wx-wx|0|0|146|1454230980|1454230980|1454230980|1454230980
0|/MSOCache/All Users/{90120000-0015-0419-0000-0000000FF1CE}-C|88976-144-6|d/d-wx-wx-wx|0|0|56|1454230986|1454230986|1454230986|1454230980
0|/MSOCache/All Users/{90120000-0015-0419-0000-0000000FF1CE}-C/AccessMUI.msi ($FILE_NAME)|88979-48-2|r/rrwxrwxrwx|0|0|92|1454230980|1454230980|1454230980|1454230980
0|/MSOCache/All Users/{90120000-0015-0419-0000-0000000FF1CE}-C/AccessMUI.msi|88979-128-4|r/rrwxrwxrwx|0|0|1655296|1454230911|1454230980|1454230980|1454230911
0|/MSOCache/All Users/{90120000-0015-0419-0000-0000000FF1CE}-C/AccessMUI.xml ($FILE_NAME)|88977-48-2|r/rrwxrwxrwx|0|0|92|1454230980|1454230980|1454230980|1454230980
0|/MSOCache/All Users/{90120000-0015-0419-0000-0000000FF1CE}-C/AccessMUI.xml|88977-128-4|r/rrwxrwxrwx|0|0|1345|1454230912|1454230980|1454230980|1454230912
0|/MSOCache/All Users/{90120000-0015-0419-0000-0000000FF1CE}-C/AccLR.cab ($FILE_NAME)|88980-48-2|r/rrwxrwxrwx|0|0|84|1454230980|1454230980|1454230980|1454230980
0|/MSOCache/All Users/{90120000-0015-0419-0000-0000000FF1CE}-C/AccLR.cab|88980-128-3|r/rrwxrwxrwx|0|0|27317023|1454230664|1454230980|1454230986|1454230664
0|/MSOCache/All Users/{90120000-0015-0419-0000-0000000FF1CE}-C/Setup.xml ($FILE_NAME)|88981-48-2|r/rrwxrwxrwx|0|0|84|1454230986|1454230986|1454230986|1454230986
0|/MSOCache/All Users/{90120000-0015-0419-0000-0000000FF1CE}-C/Setup.xml|88981-128-3|r/rrwxrwxrwx|0|0|1780|1454230912|1454230986|1454230986|1454230912
0|/MSOCache/All Users/{90120000-0016-0419-0000-0000000FF1CE}-C ($FILE_NAME)|88898-48-2|d/d-wx-wx-wx|0|0|146|1454230952|1454230952|1454230952|1454230952
0|/MSOCache/All Users/{90120000-0016-0419-0000-0000000FF1CE}-C|88898-144-1|d/d-wx-wx-wx|0|0|480|1454230955|1454230955|1454230955|1454230952
0|/MSOCache/All Users/{90120000-0016-0419-0000-0000000FF1CE}-C/ExcelLR.cab ($FILE_NAME)|88902-48-2|r/rrwxrwxrwx|0|0|88|1454230952|1454230952|1454230952|1454230952
0|/MSOCache/All Users/{90120000-0016-0419-0000-0000000FF1CE}-C/ExcelLR.cab|88902-128-3|r/rrwxrwxrwx|0|0|14812553|1454230823|1454230952|1454230955|1454230823
0|/MSOCache/All Users/{90120000-0016-0419-0000-0000000FF1CE}-C/ExcelMUI.msi ($FILE_NAME)|88900-48-2|r/rrwxrwxrwx|0|0|90|1454230952|1454230952|1454230952|1454230952
0|/MSOCache/All Users/{90120000-0016-0419-0000-0000000FF1CE}-C/ExcelMUI.msi|88900-128-3|r/rrwxrwxrwx|0|0|1715200|1454230911|1454230952|1454230952|1454230911
0|/MSOCache/All Users/{90120000-0016-0419-0000-0000000FF1CE}-C/ExcelMUI.xml ($FILE_NAME)|88899-48-2|r/rrwxrwxrwx|0|0|90|1454230952|1454230952|1454230952|1454230952
0|/MSOCache/All Users/{90120000-0016-0419-0000-0000000FF1CE}-C/ExcelMUI.xml|88899-128-3|r/rrwxrwxrwx|0|0|1801|1454230912|1454230952|1454230952|1454230912
0|/MSOCache/All Users/{90120000-0016-0419-0000-0000000FF1CE}-C/Setup.xml ($FILE_NAME)|88863-48-2|r/rrwxrwxrwx|0|0|84|1454230955|1454230955|1454230955|1454230955
0|/MSOCache/All Users/{90120000-0016-0419-0000-0000000FF1CE}-C/Setup.xml|88863-128-3|r/rrwxrwxrwx|0|0|2527|1454230912|1454230955|1454230955|1454230912
0|/MSOCache/All Users/{90120000-0018-0419-0000-0000000FF1CE}-C ($FILE_NAME)|88910-48-2|d/d-wx-wx-wx|0|0|146|1454230958|1454230958|1454230958|1454230958
0|/MSOCache/All Users/{90120000-0018-0419-0000-0000000FF1CE}-C|88910-144-6|d/d-wx-wx-wx|0|0|56|1454230961|1454230961|1454230961|1454230958
0|/MSOCache/All Users/{90120000-0018-0419-0000-0000000FF1CE}-C/PowerPointMUI.msi ($FILE_NAME)|88912-48-2|r/rrwxrwxrwx|0|0|100|1454230958|1454230958|1454230958|1454230958
0|/MSOCache/All Users/{90120000-0018-0419-0000-0000000FF1CE}-C/PowerPointMUI.msi|88912-128-4|r/rrwxrwxrwx|0|0|1643008|1454230912|1454230958|1454230958|1454230912
0|/MSOCache/All Users/{90120000-0018-0419-0000-0000000FF1CE}-C/PowerPointMUI.xml ($FILE_NAME)|88911-48-2|r/rrwxrwxrwx|0|0|100|1454230958|1454230958|1454230958|1454230958
0|/MSOCache/All Users/{90120000-0018-0419-0000-0000000FF1CE}-C/PowerPointMUI.xml|88911-128-4|r/rrwxrwxrwx|0|0|1554|1454230912|1454230958|1454230958|1454230912
0|/MSOCache/All Users/{90120000-0018-0419-0000-0000000FF1CE}-C/PptLR.cab ($FILE_NAME)|88914-48-2|r/rrwxrwxrwx|0|0|84|1454230958|1454230958|1454230958|1454230958
```

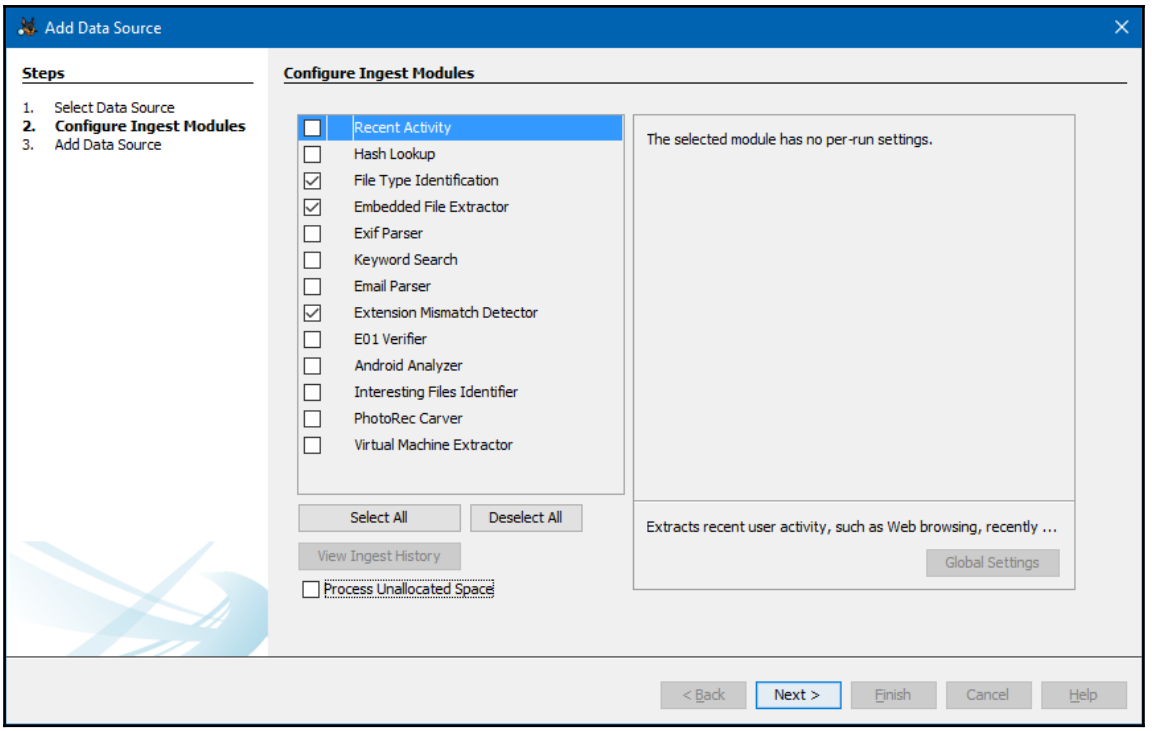
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Date	Size	Type	Mode	UID	GID	Meta	File Name								
2	Sun Aug 13 2006 16:51:02	78	m..b	r/rrwxrwxrwx	0	0	94436-128-1	/Program Files/Microsoft Office/Office12/Mso Example Setup File A.txt								
3	Fri Aug 18 2006 15:20:02	84	m..b	r/rrwxrwxrwx	0	0	94125-128-1	/Program Files/Microsoft Office/Office12/1049/Mso Example Intl Setup File A.txt								
4	Fri Aug 18 2006 15:20:02	84	m..b	r/rrwxrwxrwx	0	0	94126-128-1	/Program Files/Microsoft Office/Office12/1049/Mso Example Intl Setup File B.txt								
5	Thu Oct 26 2006 13:41:56	92424	m..b	r/rrwxrwxrwx	0	0	94511-128-3	/Program Files/Common Files/microsoft shared/OFFICE11/1033/msxml5r.dll								
6	Thu Oct 26 2006 19:28:04	88	...b	r/rrwxrwxrwx	0	0	94573-48-2	/Program Files/Microsoft Office/Office12/MSOHEVI.DLL ($FILE_NAME)								
7	Thu Oct 26 2006 19:28:06	90	...b	r/rrwxrwxrwx	0	0	94577-48-2	/Program Files/Common Files/microsoft shared/OFFICE12/msoshext.dll ($FILE_NAME)								
8	Thu Oct 26 2006 20:25:20	483632	m..b	r/rrwxrwxrwx	0	0	94437-128-3	/Program Files/Microsoft Office/Office12/VISSHE.DLL								
9	Thu Oct 26 2006 20:34:16	63248	m..b	r/rrwxrwxrwx	0	0	94432-128-3	/Program Files/Common Files/microsoft shared/OFFICE12/MSOXEV.DLL								
10	Thu Oct 26 2006 20:34:18	80656	m..b	r/rrwxrwxrwx	0	0	94433-128-3	/Program Files/Common Files/microsoft shared/OFFICE12/MSOXMLED.EXE								
11	Thu Oct 26 2006 20:34:20	90	...b	r/rrwxrwxrwx	0	0	94580-48-2	/Program Files/Common Files/microsoft shared/OFFICE12/MSOXMLMF.DLL ($FILE_NAME)								
12	Thu May 15 2008 11:24:40	206606	m...	r/rrwxrwxrwx	0	0	141978-128-1	/en/Setup/TestPageLogo.bmp								
13	Thu May 15 2008 11:24:40	26	m...	r/rrwxrwxrwx	0	0	141978-128-4	/en/Setup/TestPageLogo.bmp:Zone.Identifier								
14	Thu May 15 2008 11:24:40	63888	m...	r/rrwxrwxrwx	0	0	141979-128-1	/en/Setup/WizardBitmap.bmp								
15	Thu May 15 2008 11:24:40	26	m...	r/rrwxrwxrwx	0	0	141979-128-4	/en/Setup/WizardBitmap.bmp:Zone.Identifier								
16	Thu May 15 2008 11:24:40	2784	m...	r/rrwxrwxrwx	0	0	141980-128-1	/en/Setup/WizardLogo.bmp								
17	Thu May 15 2008 11:24:40	26	m...	r/rrwxrwxrwx	0	0	141980-128-4	/en/Setup/WizardLogo.bmp:Zone.Identifier								
18	Thu May 15 2008 11:24:40	9056	m...	r/rrwxrwxrwx	0	0	141981-128-1	/en/Setup/WizardLogoForVista.bmp								
19	Thu May 15 2008 11:24:40	26	m...	r/rrwxrwxrwx	0	0	141981-128-4	/en/Setup/WizardLogoForVista.bmp:Zone.Identifier								
20	Thu May 15 2008 11:24:40	4080	m...	r/rrwxrwxrwx	0	0	141982-128-1	/en/Setup/WizardLogoForVistaAlpha.bmp								
21	Thu May 15 2008 11:24:40	26	m...	r/rrwxrwxrwx	0	0	141982-128-4	/en/Setup/WizardLogoForVistaAlpha.bmp:Zone.Identifier								
22	Thu May 15 2008 11:24:42	62464	m...	r/rrwxrwxrwx	0	0	142000-128-1	/en/Utility/KmCopy64.exe								
23	Thu May 15 2008 11:24:42	26	m...	r/rrwxrwxrwx	0	0	142000-128-3	/en/Utility/KmCopy64.exe:Zone.Identifier								
24	Thu May 15 2008 11:24:42	45056	m...	r/rrwxrwxrwx	0	0	142001-128-1	/en/Utility/KmInstCm.exe								
25	Thu May 15 2008 11:24:42	26	m...	r/rrwxrwxrwx	0	0	142001-128-3	/en/Utility/KmInstCm.exe:Zone.Identifier								

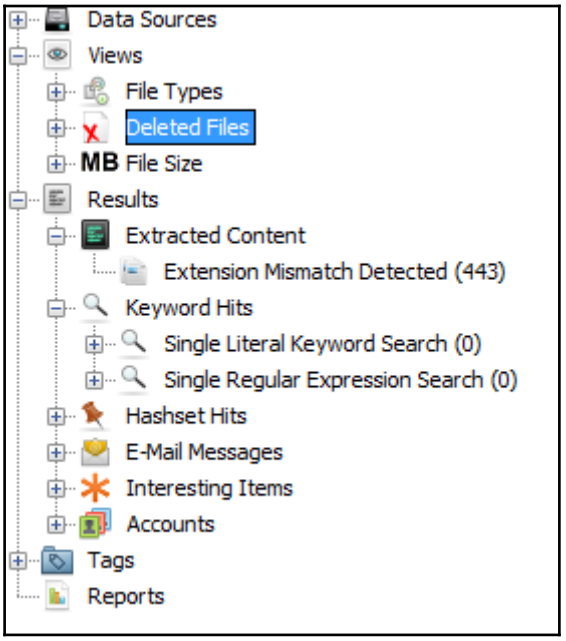

Welcome
Create New Case
Open Recent Case
Open Existing Case
Close
Autopsy®
OPEN | EXTENSIBLE | FAST

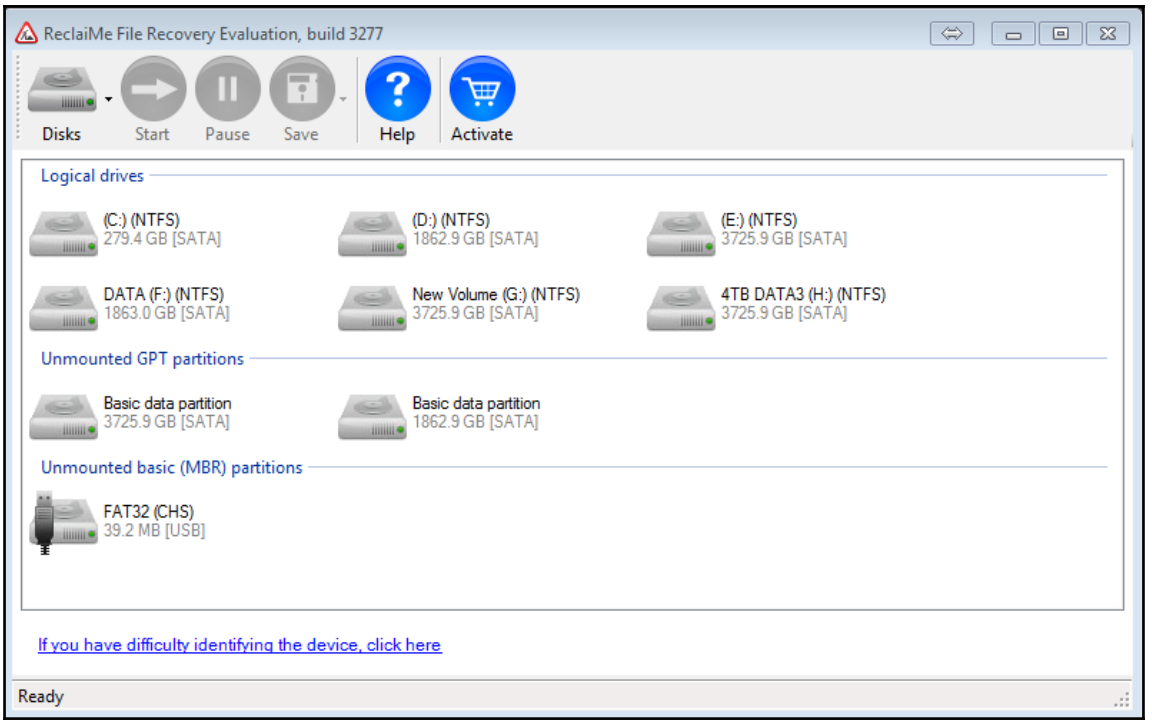

New Case Information
Steps
1. Case Info
2. Additional Information
Case Info
Enter New Case Information:
Case Name: 1462017
Base Directory: Y:\
Browse
Case Type: Single-user Multi-user
Case data will be stored in the following directory:
Y:\1462017
< Back
Next >
Finish
Cancel
Help

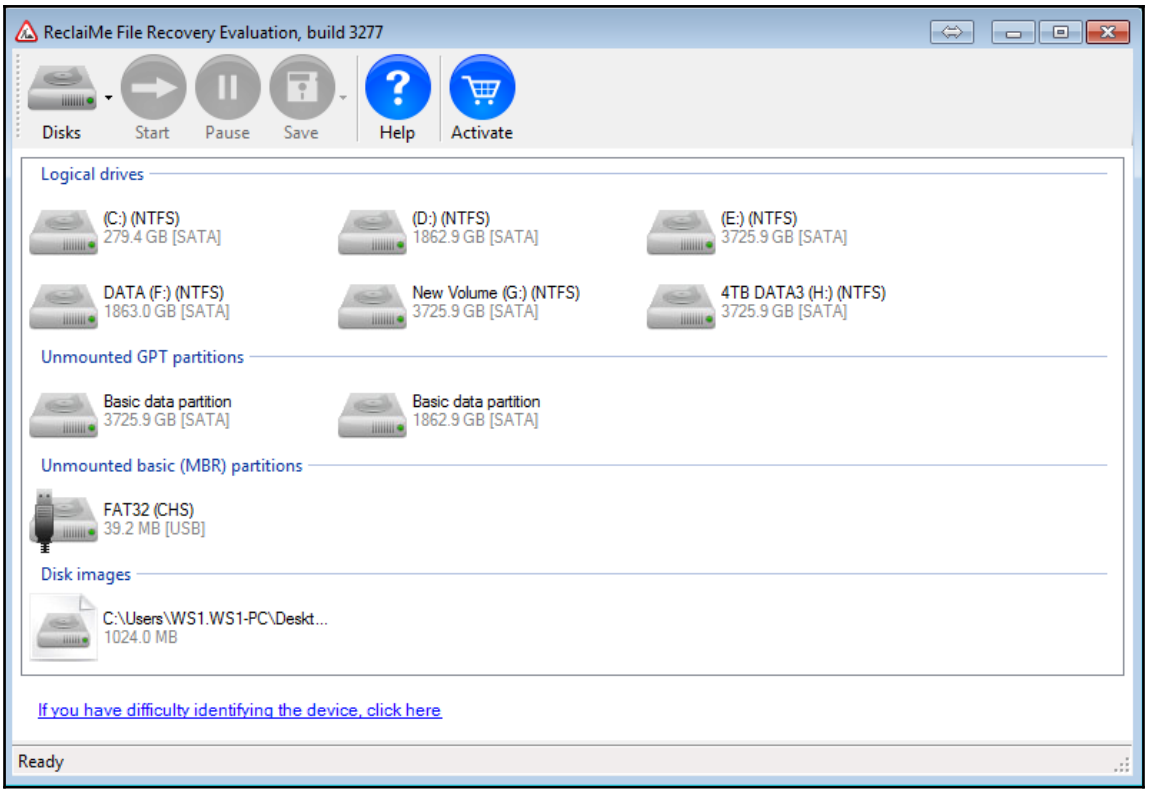

New Case Information
Steps
1. Case Info
2. Additional Information
Additional Information
Optional: Set Case Number and Examiner
Case Number:
1462017
Examiner:
Oleg Skulkin
< Back
Next >
Finish
Cancel
Help

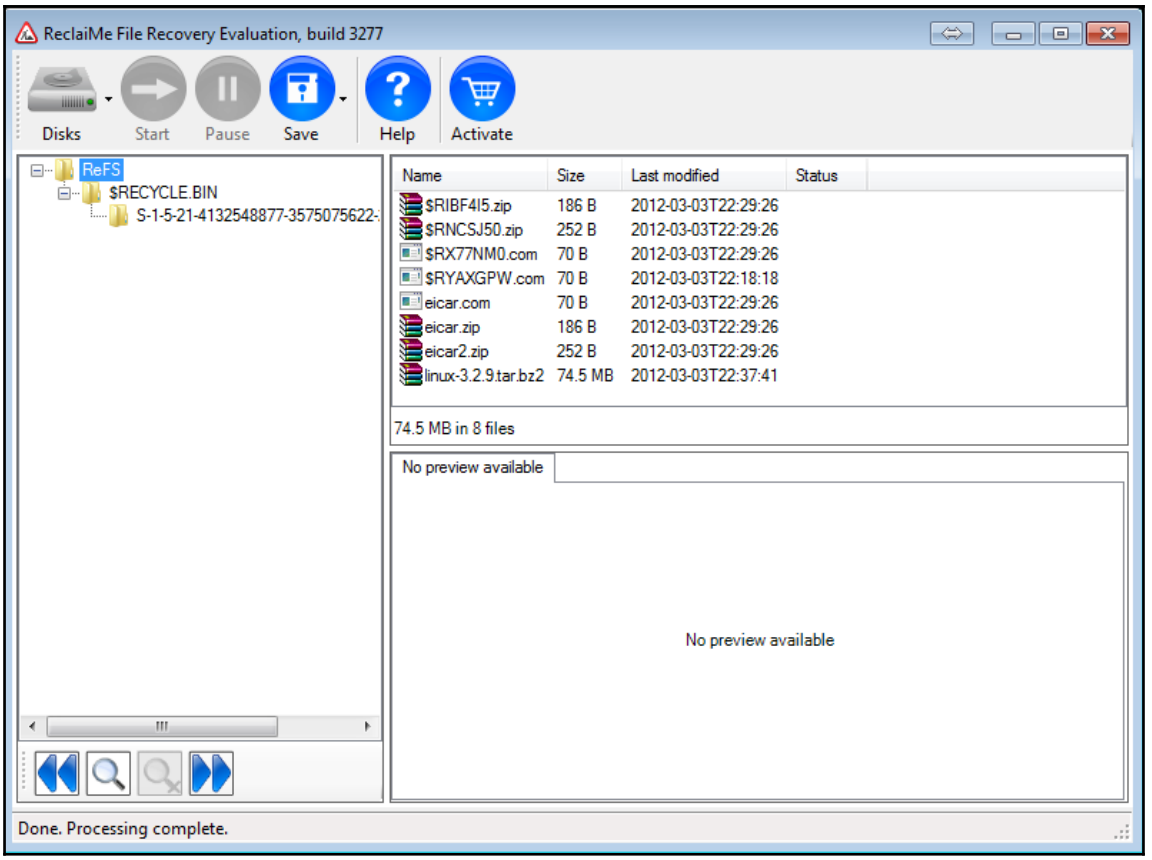

Add Data Source
Steps
1. Select Data Source
2. Configure Ingest Modules
3. Add Data Source
Select Data Source
Select data source type:
Image or VM File
Browse for an image file:
X:\146-2017.E01
Browse
Please select the input timezone:
(GMT+3:00) Europe/Moscow
Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)
< Back
Next >
Finish
Cancel
Help

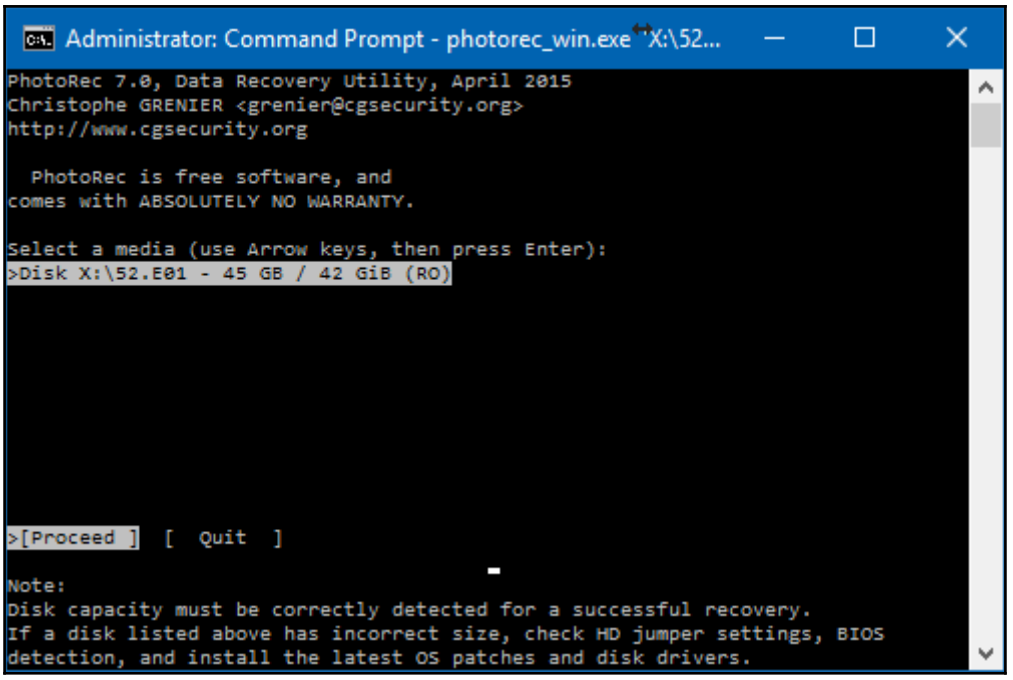

Add Data Source
Steps
1. Select Data Source
2. Configure Ingest Modules
3. Add Data Source
Configure Ingest Modules
Recent Activity
Hash Lookup
File Type Identification
Embedded File Extractor
Exif Parser
Keyword Search
Email Parser
Extension Mismatch Detector
E01 Verifier
Android Analyzer
Interesting Files Identifier
PhotoRec Carver
Virtual Machine Extractor
The selected module has no per-run settings.
Select All
Deselect All
View Ingest History
Process Unallocated Space
Extracts recent user activity, such as Web browsing, recently ...
Global Settings
< Back
Next >
Finish
Cancel
Help

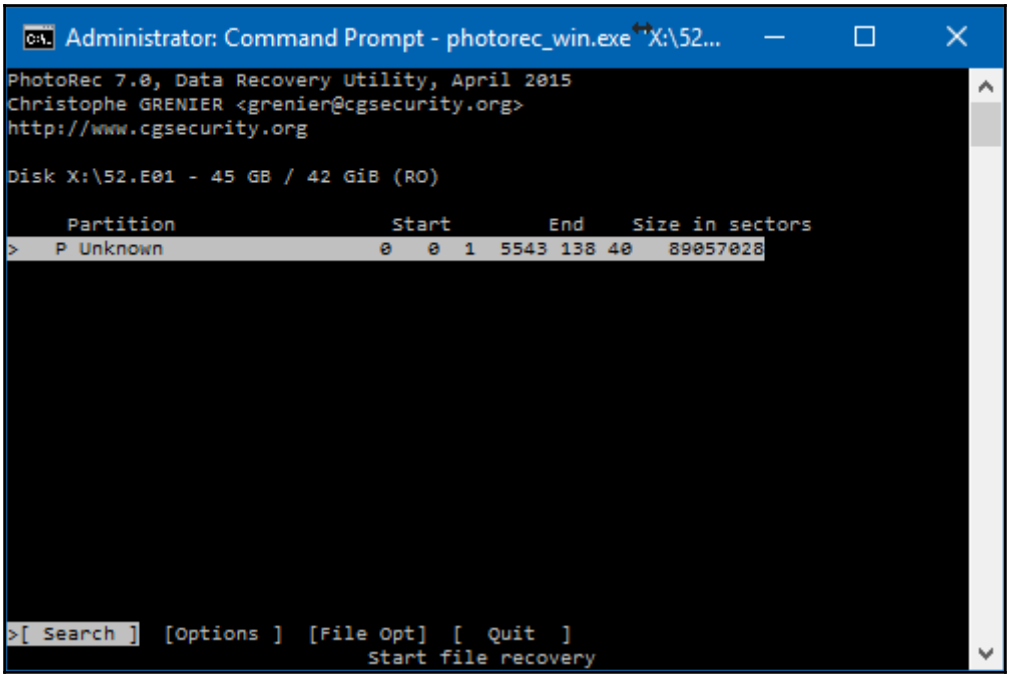

Data Sources
Views
File Types
Deleted Files
MB File Size
Results
Extracted Content
Extension Mismatch Detected (443)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Reports

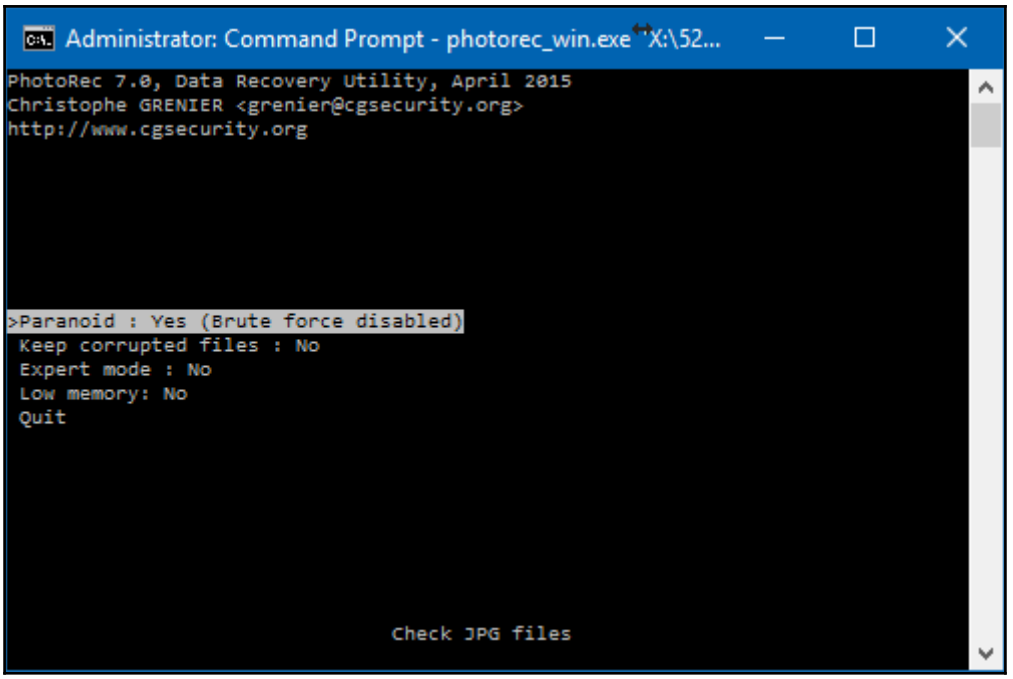

ReclaiMe File Recovery Evaluation, build 3277
Disks
Start
Pause
Save
Help
Activate
Logical drives
(C:) (NTFS)
279.4 GB [SATA]
(D:) (NTFS)
1862.9 GB [SATA]
(E:) (NTFS)
3725.9 GB [SATA]
DATA (F:) (NTFS)
1863.0 GB [SATA]
New Volume (G:) (NTFS)
3725.9 GB [SATA]
4TB DATA3 (H:) (NTFS)
3725.9 GB [SATA]
Unmounted GPT partitions
Basic data partition
3725.9 GB [SATA]
Basic data partition
1862.9 GB [SATA]
Unmounted basic (MBR) partitions
FAT32 (CHS)
39.2 MB [USB]
If you have difficulty identifying the device, click here
Ready

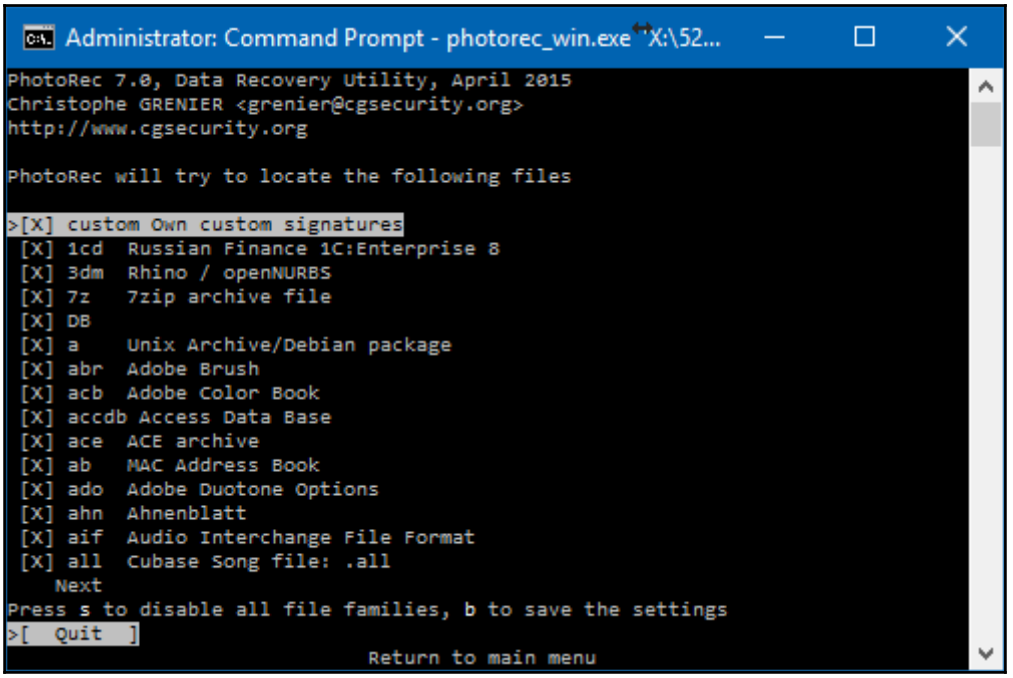

ReclaiMe File Recovery Evaluation, build 3277
Disks
Start
Pause
Save
Help
Activate
Logical drives
(C:) (NTFS)
279.4 GB [SATA]
(D:) (NTFS)
1862.9 GB [SATA]
(E:) (NTFS)
3725.9 GB [SATA]
DATA (F:) (NTFS)
1863.0 GB [SATA]
New Volume (G:) (NTFS)
3725.9 GB [SATA]
4TB DATA3 (H:) (NTFS)
3725.9 GB [SATA]
Unmounted GPT partitions
Basic data partition
3725.9 GB [SATA]
Basic data partition
1862.9 GB [SATA]
Unmounted basic (MBR) partitions
FAT32 (CHS)
39.2 MB [USB]
Disk images
C:\Users\WS1.WS1-PC\Deskt...
1024.0 MB
If you have difficulty identifying the device, click here
Ready

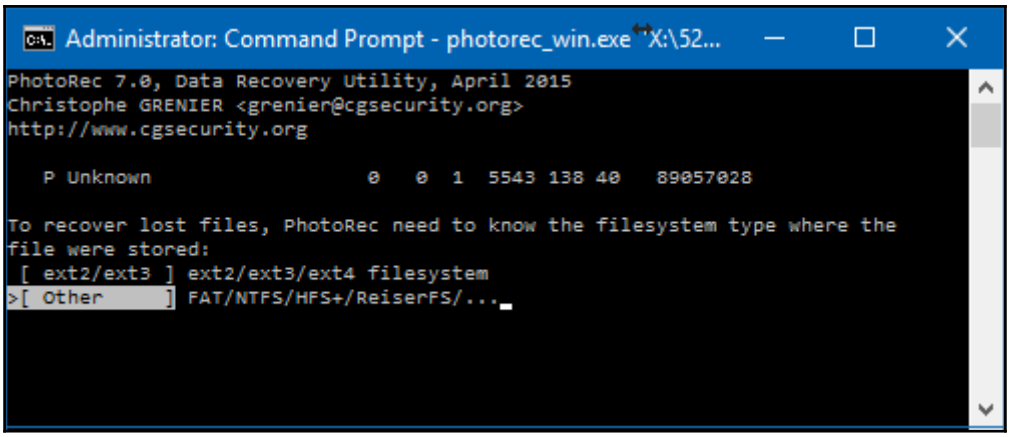

ReclaiMe File Recovery Evaluation, build 3277
Disks
Start
Pause
Save
Help
Activate
ReFS
$RECYCLE.BIN
S-1-5-21-4132548877-3575075622-
Name
Size
Last modified
Status
$RIBF4I5.zip 186 B 2012-03-03T22:29:26
$RNCSJ50.zip 252 B 2012-03-03T22:29:26
$RX77NM0.com 70 B 2012-03-03T22:29:26
$RYAXGPW.com 70 B 2012-03-03T22:18:18
eicar.com 70 B 2012-03-03T22:29:26
eicar.zip 186 B 2012-03-03T22:29:26
eicar2.zip 252 B 2012-03-03T22:29:26
linux-3.2.9.tar.bz2 74.5 MB 2012-03-03T22:37:41
74.5 MB in 8 files
No preview available
No preview available
Done. Processing complete.

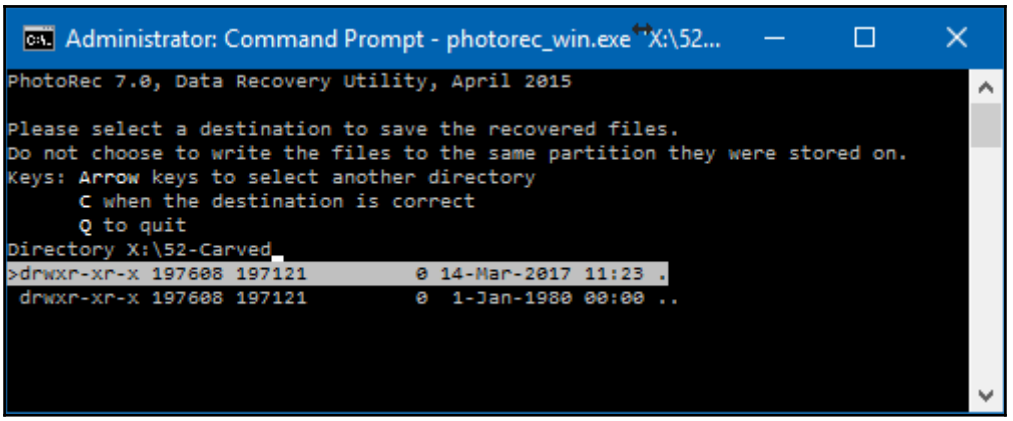

Administrator: Command Prompt - photorec_win.exe X:\52...
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
PhotoRec is free software, and
comes with ABSOLUTELY NO WARRANTY.
Select a media (use Arrow keys, then press Enter):
>Disk X:\52.E01 - 45 GB / 42 GiB (RO)
>[Proceed] [Quit]
Note:
Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has incorrect size, check HD jumper settings, BIOS
detection, and install the latest OS patches and disk drivers.


Administrator: Command Prompt - photorec_win.exe X:\52...
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
Disk X:\52.E01 - 45 GB / 42 GiB (RO)
Partition Start End Size in sectors
> P Unknown 0 0 1 5543 138 40 89057028
>[Search] [Options] [File Opt] [Quit]
Start file recovery

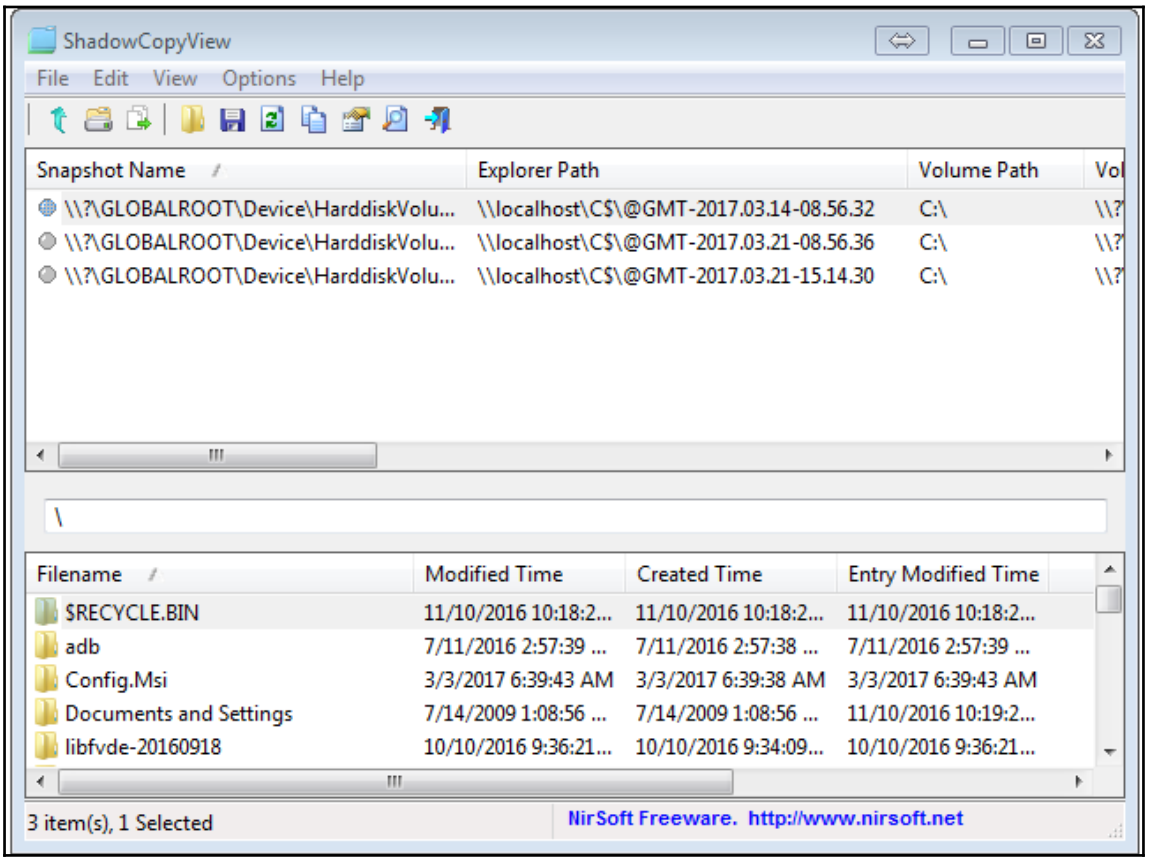

Administrator: Command Prompt - photorec_win.exe X:\52...
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
>Paranoid : Yes (Brute force disabled)
Keep corrupted files : No
Expert mode : No
Low memory: No
Quit
Check JPG files

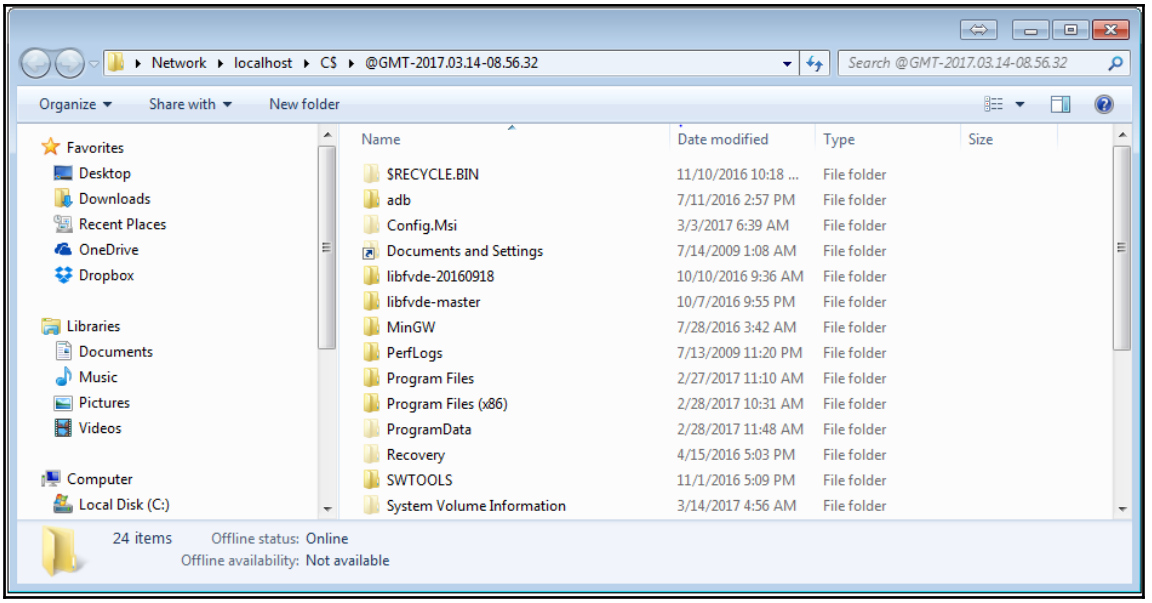

Administrator: Command Prompt - photorec_win.exe X:\52...
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
PhotoRec will try to locate the following files
>[X] custom Own custom signatures
[X] 1cd Russian Finance 1C:Enterprise 8
[X] 3dm Rhino / openNURBS
[X] 7z 7zip archive file
[X] DB
[X] a Unix Archive/Debian package
[X] abr Adobe Brush
[X] acb Adobe Color Book
[X] accdb Access Data Base
[X] ace ACE archive
[X] ab MAC Address Book
[X] ado Adobe Duotone Options
[X] ahn Ahnenblatt
[X] aif Audio Interchange File Format
[X] all Cubase Song file: .all
Next
Press s to disable all file families, b to save the settings
>[Quit]
Return to main menu

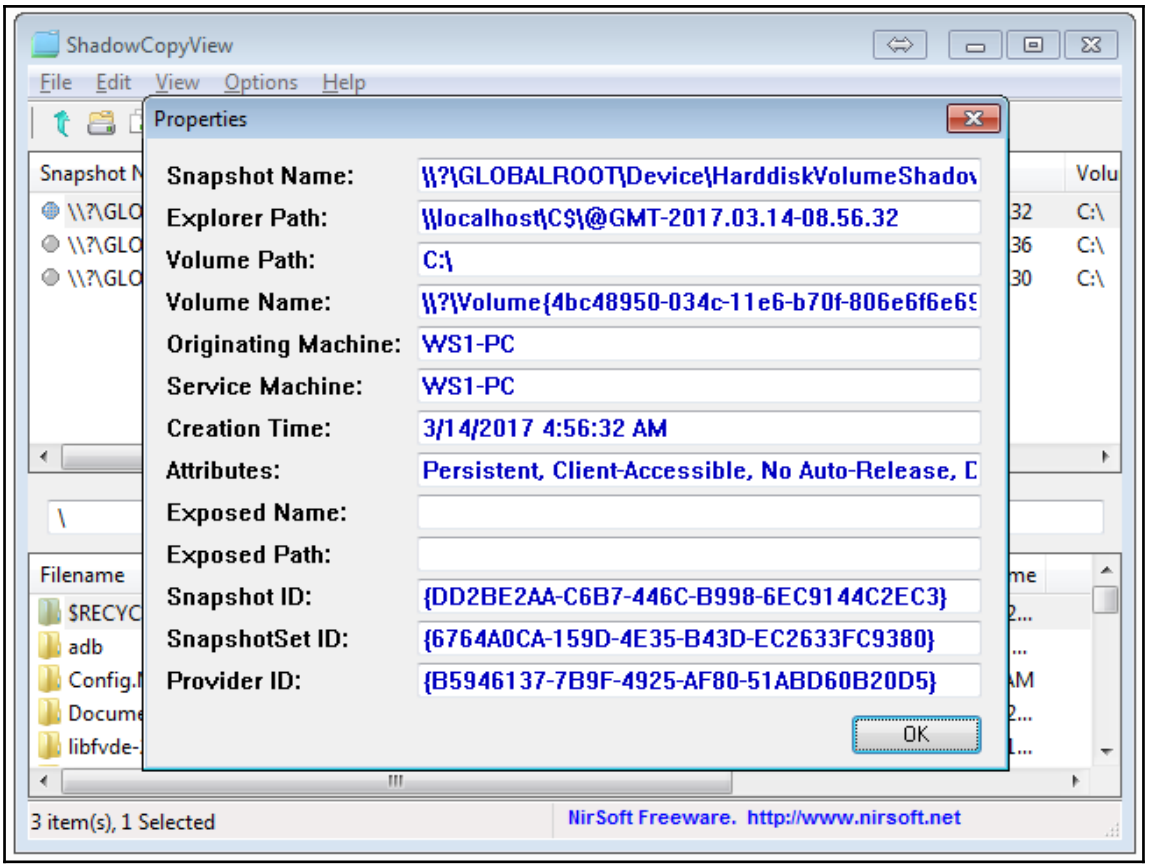

Administrator: Command Prompt - photorec_win.exe X:\52...
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
P Unknown 0 0 1 5543 138 40 89057028
To recover lost files, PhotoRec need to know the filesystem type where the file were stored:
[ext2/ext3] ext2/ext3/ext4 filesystem
>[Other] FAT/NTFS/HFS+/ReiserFS/...

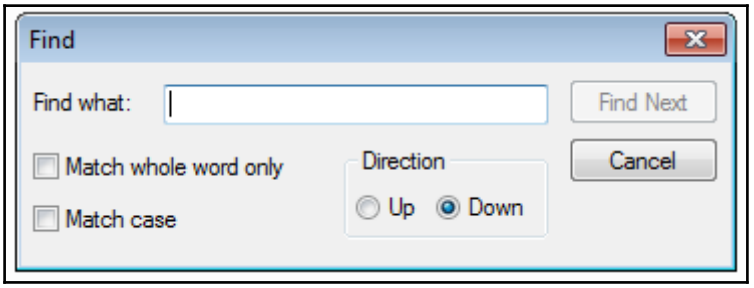

Administrator: Command Prompt - photorec_win.exe X:\52...
PhotoRec 7.0, Data Recovery Utility, April 2015
Please select a destination to save the recovered files.
Do not choose to write the files to the same partition they were stored on.
Keys: Arrow keys to select another directory
C when the destination is correct
Q to quit
Directory X:\52-Carved
>drwxr-xr-x 197608 197121 0 14-Mar-2017 11:23 .
drwxr-xr-x 197608 197121 0 1-Jan-1980 00:00 ..

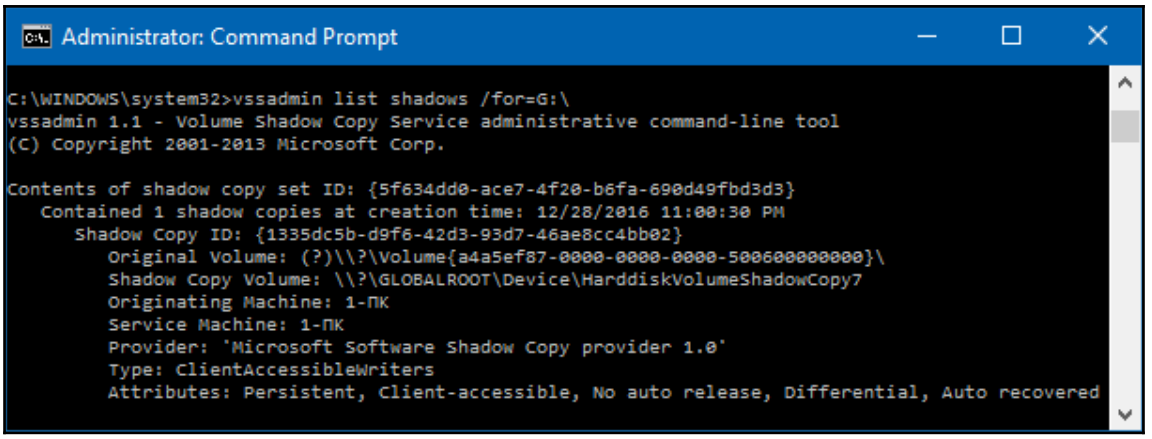
Chapter 5 : Windows Shadow Copies Analysis

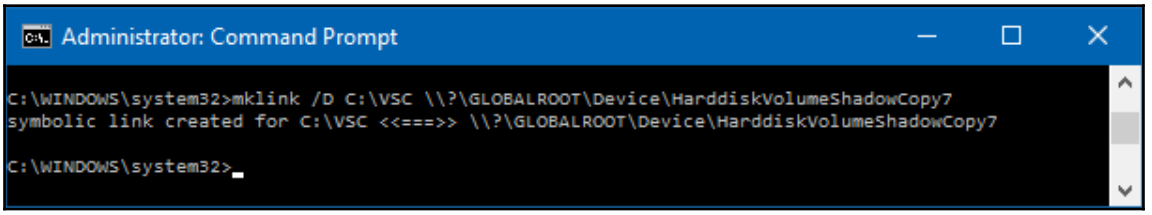


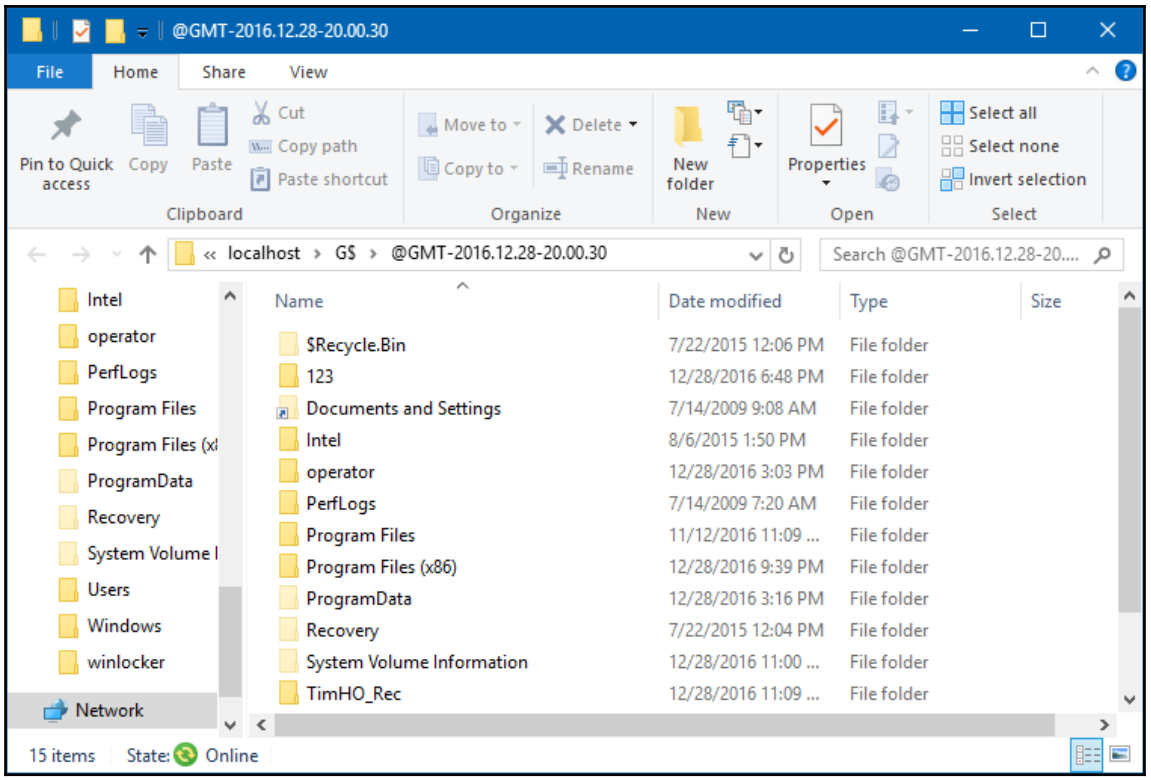

Network ▸ localhost ▸ C$ ▸ @GMT-2017.03.14-08.56.32
Search @GMT-2017.03.14-08.56.32
Organize
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
OneDrive
Dropbox
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Name
Date modified
Type
Size
$RECYCLE.BIN 11/10/2016 10:18 ... File folder
adb 7/11/2016 2:57 PM File folder
Config.Msi 3/3/2017 6:39 AM File folder
Documents and Settings 7/14/2009 1:08 AM File folder
libfvde-20160918 10/10/2016 9:36 AM File folder
libfvde-master 10/7/2016 9:55 PM File folder
MinGW 7/28/2016 3:42 AM File folder
PerfLogs 7/13/2009 11:20 PM File folder
Program Files 2/27/2017 11:10 AM File folder
Program Files (x86) 2/28/2017 10:31 AM File folder
ProgramData 2/28/2017 11:48 AM File folder
Recovery 4/15/2016 5:03 PM File folder
SWTOOLS 11/1/2016 5:09 PM File folder
System Volume Information 3/14/2017 4:56 AM File folder
24 items
Offline status: Online
Offline availability: Not available

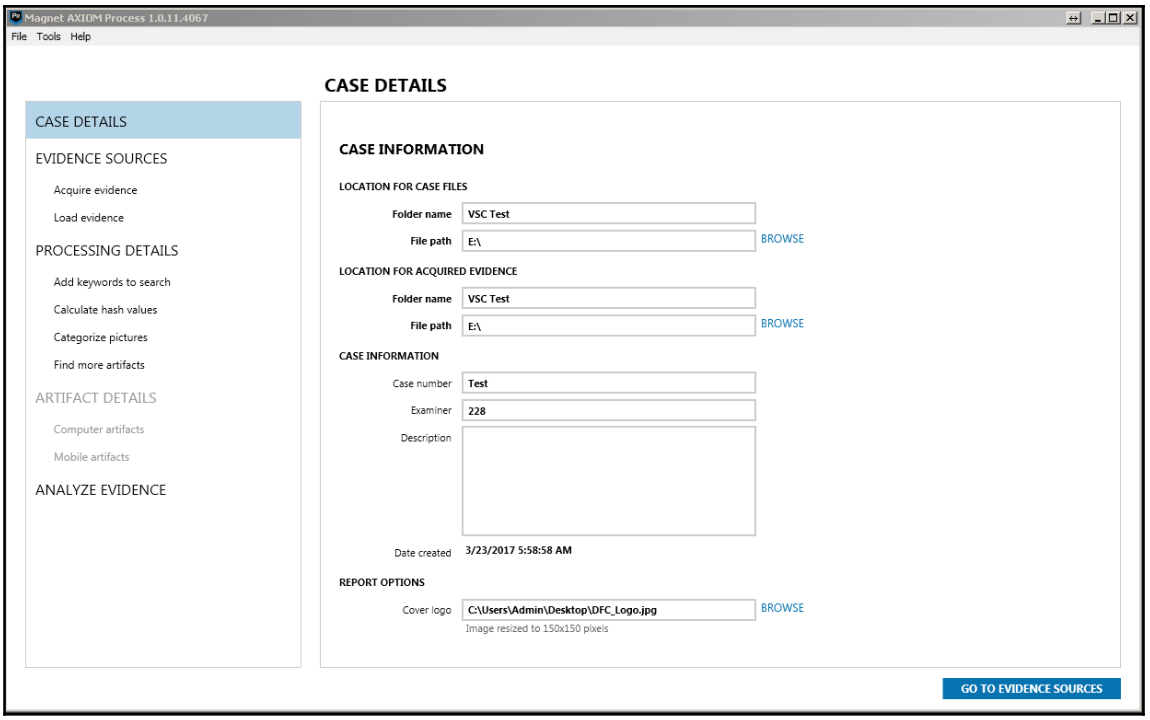

ShadowCopyView
File Edit View Options Help
Properties
Snapshot Name: \\?\GLOBALROOT\Device\HarddiskVolumeShadow
Explorer Path: \\localhost\C$\@GMT-2017.03.14-08.56.32
Volume Path: C:\
Volume Name: \\?\Volume{4bc48950-034c-11e6-b70f-806e6f6e69
Originating Machine: WS1-PC
Service Machine: WS1-PC
Creation Time: 3/14/2017 4:56:32 AM
Attributes: Persistent, Client-Accessible, No Auto-Release, C
Exposed Name:
Exposed Path:
Snapshot ID: {DD2BE2AA-C6B7-446C-B998-6EC9144C2EC3}
SnapshotSet ID: {6764A0CA-159D-4E35-B43D-EC2633FC9380}
Provider ID: {B5946137-7B9F-4925-AF80-51ABD60B20D5}
OK
Snapshot N
Volu
Filename
3 item(s), 1 Selected
NirSoft Freeware. http://www.nirsoft.net

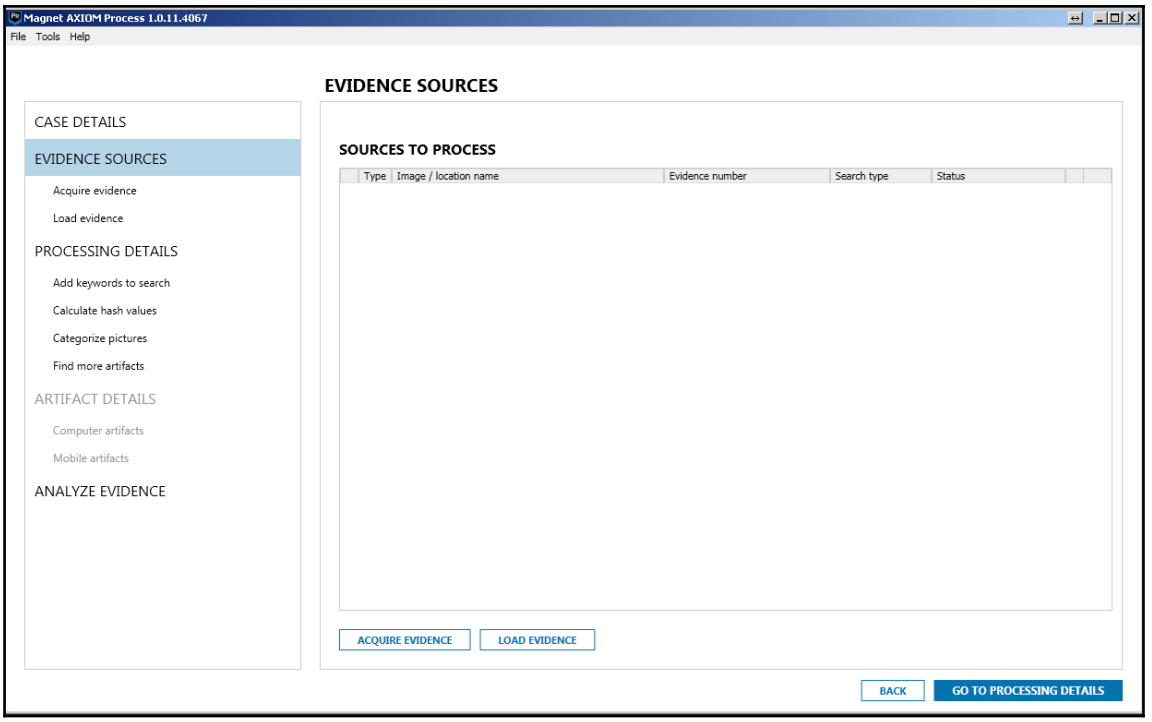

Find
Find what:
Find Next
Cancel
Match whole word only
Match case
Direction
Up
Down

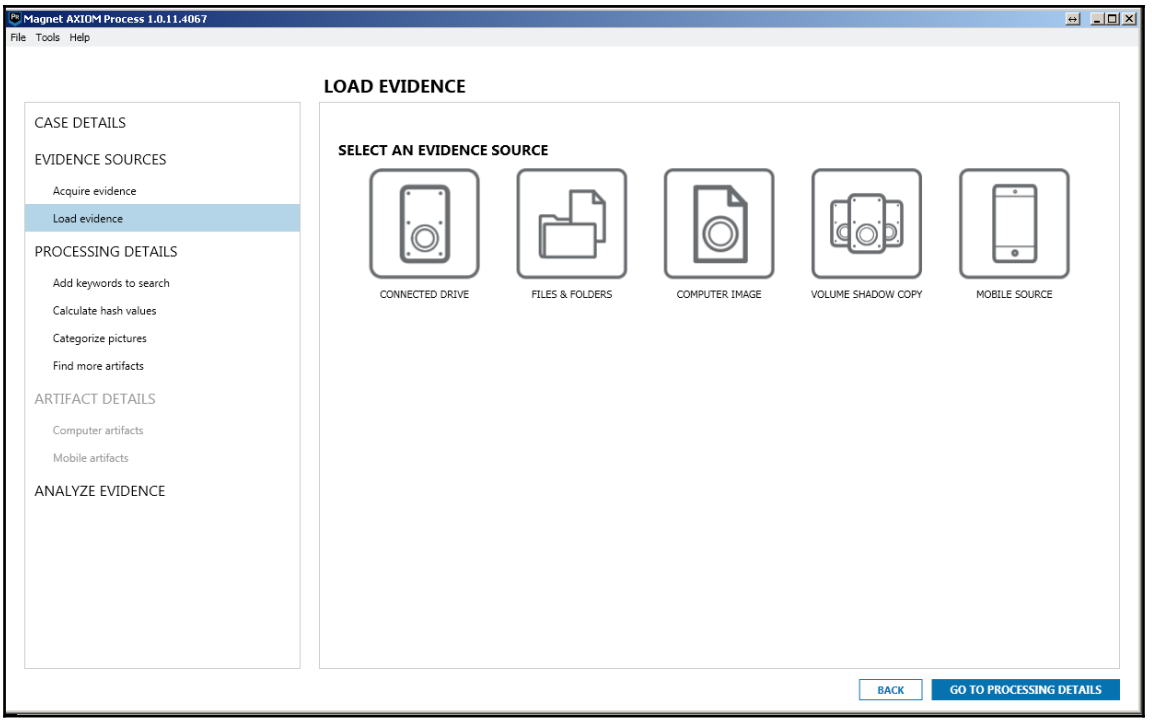

Administrator: Command Prompt
C:\WINDOWS\system32>vssadmin list shadows /for=G:\
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.
Contents of shadow copy set ID: {5f634dd0-ace7-4f20-b6fa-690d49fbd3d3}
Contained 1 shadow copies at creation time: 12/28/2016 11:00:30 PM
Shadow Copy ID: {1335dc5b-d9f6-42d3-93d7-46ae8cc4bb02}
Original Volume: (?)\\?\Volume{a4a5ef87-0000-0000-0000-500600000000}\
Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7
Originating Machine: 1-ПК
Service Machine: 1-ПК
Provider: 'Microsoft Software Shadow Copy provider 1.0'
Type: ClientAccessibleWriters
Attributes: Persistent, Client-accessible, No auto release, Differential, Auto recovered

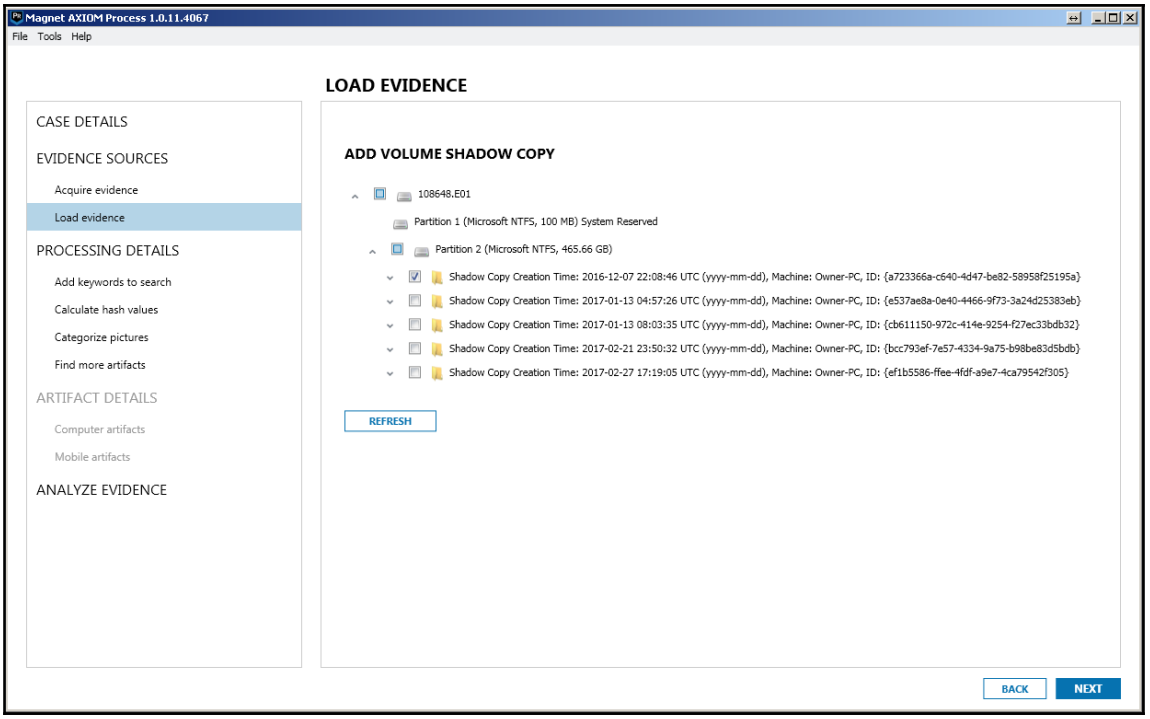

Administrator: Command Prompt
C:\WINDOWS\system32>mklink /D C:\VSC \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7
symbolic link created for C:\VSC <<===>> \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7
C:\WINDOWS\system32>

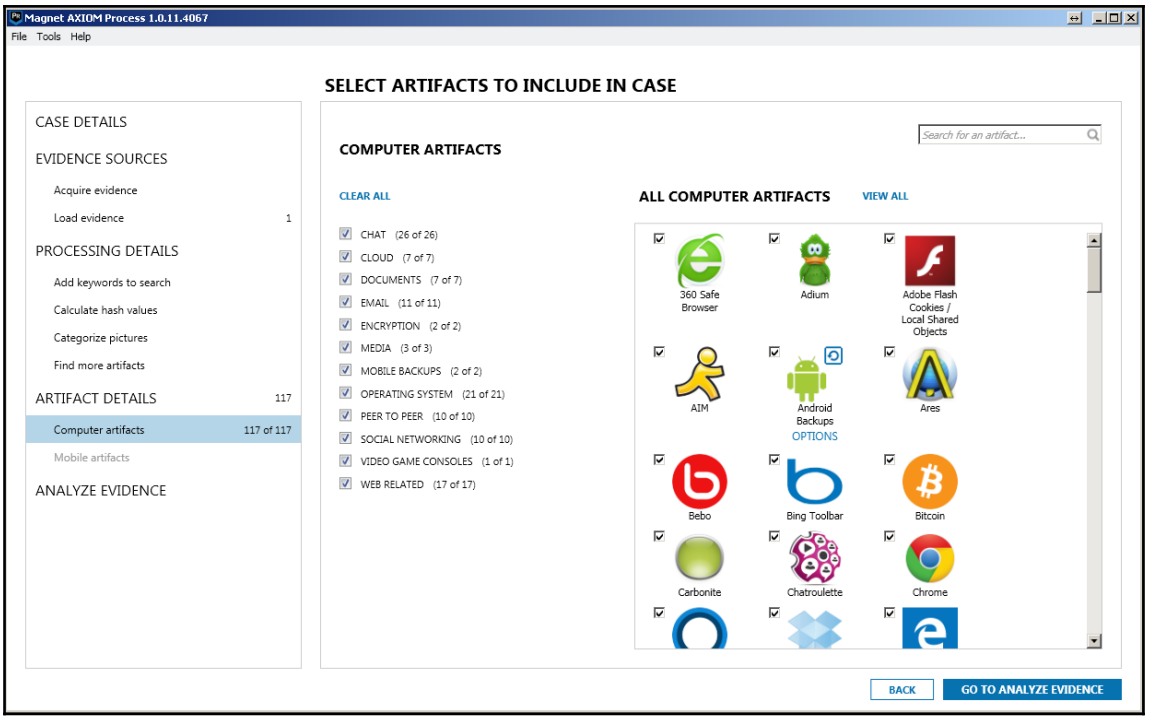

@GMT-2016.12.28-20.00.30
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Delete
Copy to
Rename
Organize
New folder
New
Properties
Open
Select all
Select none
Invert selection
Select
« localhost › G$ › @GMT-2016.12.28-20.00.30
Search @GMT-2016.12.28-20....
Intel
operator
PerfLogs
Program Files
Program Files (x
ProgramData
Recovery
System Volume I
Users
Windows
winlocker
Network
Name
Date modified
Type
Size
$Recycle.Bin 7/22/2015 12:06 PM File folder
123 12/28/2016 6:48 PM File folder
Documents and Settings 7/14/2009 9:08 AM File folder
Intel 8/6/2015 1:50 PM File folder
operator 12/28/2016 3:03 PM File folder
PerfLogs 7/14/2009 7:20 AM File folder
Program Files 11/12/2016 11:09 ... File folder
Program Files (x86) 12/28/2016 9:39 PM File folder
ProgramData 12/28/2016 3:16 PM File folder
Recovery 7/22/2015 12:04 PM File folder
System Volume Information 12/28/2016 11:00 ... File folder
TimHO_Rec 12/28/2016 11:09 ... File folder
15 items
State: Online


Magnet AXIOM Process 1.0.11.4067
File Tools Help
CASE DETAILS
CASE DETAILS
EVIDENCE SOURCES
Acquire evidence
Load evidence
PROCESSING DETAILS
Add keywords to search
Calculate hash values
Categorize pictures
Find more artifacts
ARTIFACT DETAILS
Computer artifacts
Mobile artifacts
ANALYZE EVIDENCE
CASE INFORMATION
LOCATION FOR CASE FILES
Folder name VSC Test
File path E:\ BROWSE
LOCATION FOR ACQUIRED EVIDENCE
Folder name VSC Test
File path E:\ BROWSE
CASE INFORMATION
Case number Test
Examiner 228
Description
Date created 3/23/2017 5:58:58 AM
REPORT OPTIONS
Cover logo C:\Users\Admin\Desktop\DFC_Logo.jpg BROWSE
Image resized to 150x150 pixels
GO TO EVIDENCE SOURCES

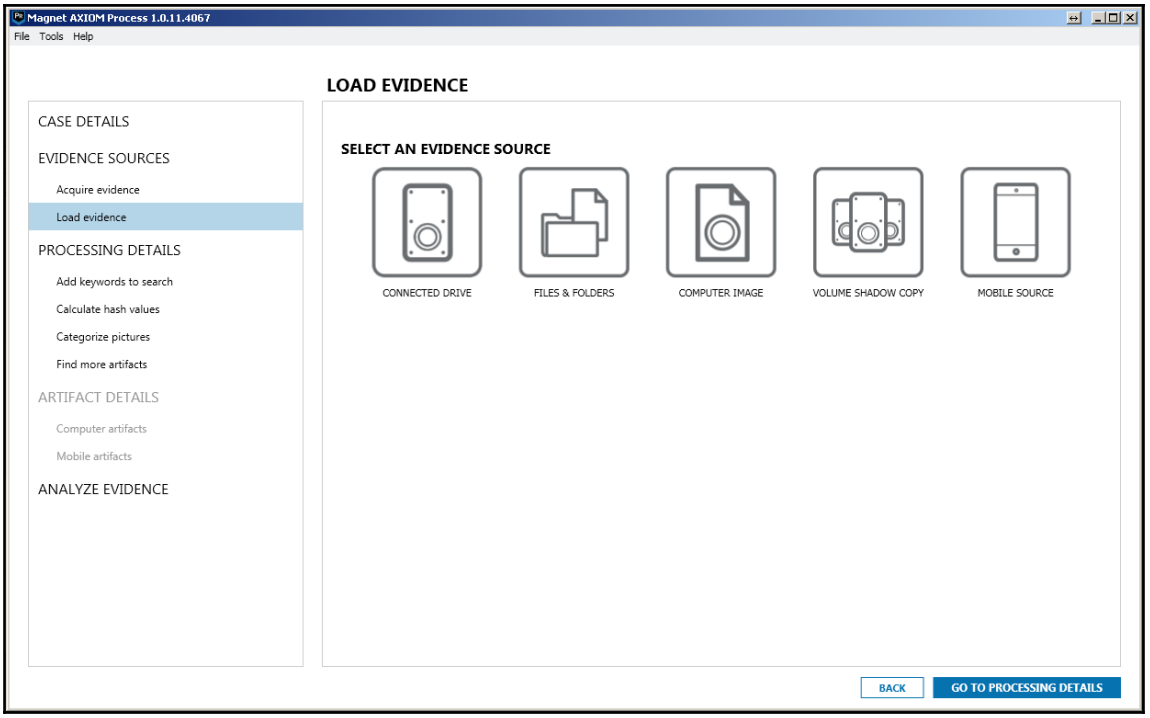

Magnet AXIOM Process 1.0.11.4067
File Tools Help
EVIDENCE SOURCES
CASE DETAILS
EVIDENCE SOURCES
Acquire evidence
Load evidence
PROCESSING DETAILS
Add keywords to search
Calculate hash values
Categorize pictures
Find more artifacts
ARTIFACT DETAILS
Computer artifacts
Mobile artifacts
ANALYZE EVIDENCE
SOURCES TO PROCESS
Type
Image / location name
Evidence number
Search type
Status
ACQUIRE EVIDENCE
LOAD EVIDENCE
BACK
GO TO PROCESSING DETAILS

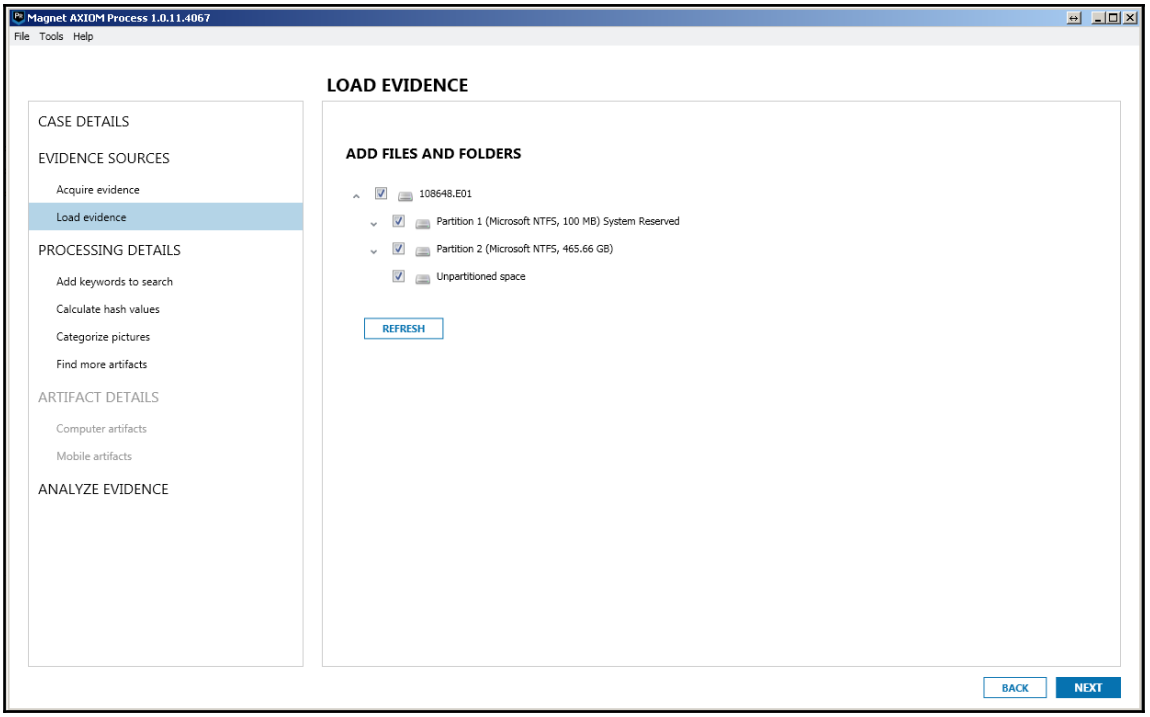

Magnet AXIOM Process 1.0.11.4067
File Tools Help
LOAD EVIDENCE
CASE DETAILS
EVIDENCE SOURCES
Acquire evidence
Load evidence
PROCESSING DETAILS
Add keywords to search
Calculate hash values
Categorize pictures
Find more artifacts
ARTIFACT DETAILS
Computer artifacts
Mobile artifacts
ANALYZE EVIDENCE
SELECT AN EVIDENCE SOURCE
CONNECTED DRIVE
FILES & FOLDERS
COMPUTER IMAGE
VOLUME SHADOW COPY
MOBILE SOURCE
BACK
GO TO PROCESSING DETAILS

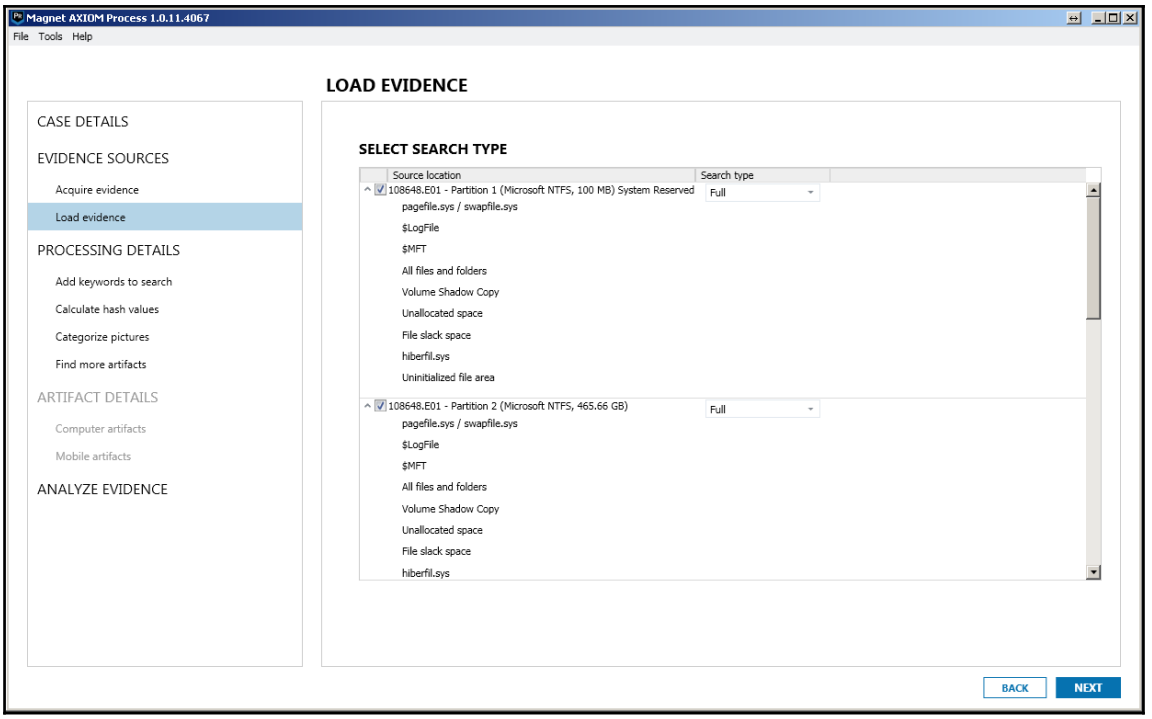

Magnet AXIOM Process 1.0.11.4067
File Tools Help
LOAD EVIDENCE
CASE DETAILS
EVIDENCE SOURCES
Acquire evidence
Load evidence
PROCESSING DETAILS
Add keywords to search
Calculate hash values
Categorize pictures
Find more artifacts
ARTIFACT DETAILS
Computer artifacts
Mobile artifacts
ANALYZE EVIDENCE
ADD VOLUME SHADOW COPY
108648.E01
Partition 1 (Microsoft NTFS, 100 MB) System Reserved
Partition 2 (Microsoft NTFS, 465.66 GB)
Shadow Copy Creation Time: 2016-12-07 22:08:46 UTC (yyyy-mm-dd), Machine: Owner-PC, ID: {a723366a-c640-4d47-be82-58958f25195a}
Shadow Copy Creation Time: 2017-01-13 04:57:26 UTC (yyyy-mm-dd), Machine: Owner-PC, ID: {e537ae8a-0e40-4466-9f73-3a24d25383eb}
Shadow Copy Creation Time: 2017-01-13 08:03:35 UTC (yyyy-mm-dd), Machine: Owner-PC, ID: {cb611150-972c-414e-9254-f27ec33bdb32}
Shadow Copy Creation Time: 2017-02-21 23:50:32 UTC (yyyy-mm-dd), Machine: Owner-PC, ID: {bcc793ef-7e57-4334-9a75-b98be83d5bdb}
Shadow Copy Creation Time: 2017-02-27 17:19:05 UTC (yyyy-mm-dd), Machine: Owner-PC, ID: {ef1b5586-ffee-4fdf-a9e7-4ca79542f305}
REFRESH
BACK
NEXT

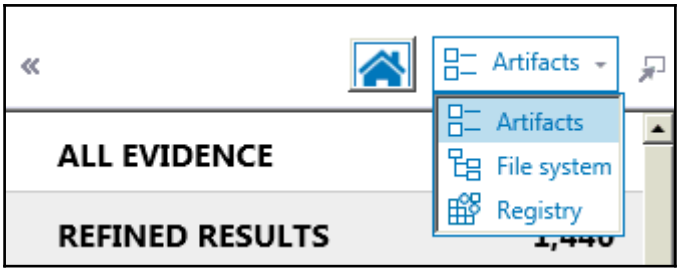


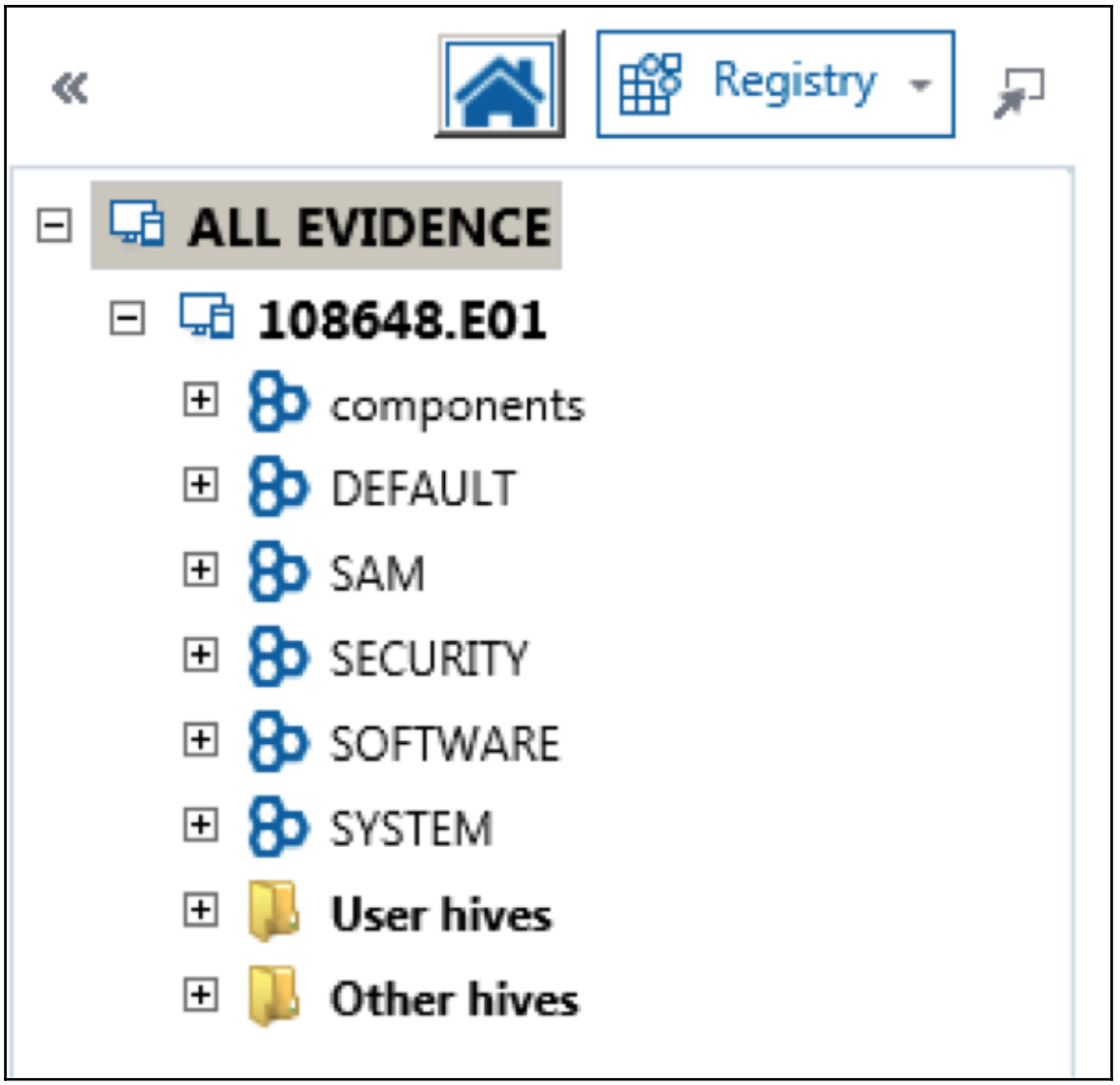
Chapter 6 : Windows Registry Analysis

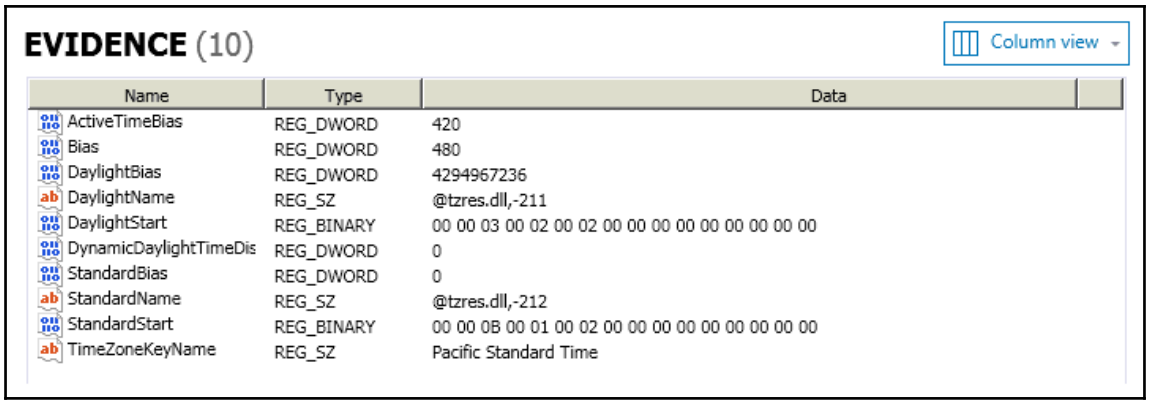

Magnet AXIOM Process 1.0.11.4067
File Tools Help
LOAD EVIDENCE
CASE DETAILS
EVIDENCE SOURCES
Acquire evidence
Load evidence
PROCESSING DETAILS
Add keywords to search
Calculate hash values
Categorize pictures
Find more artifacts
ARTIFACT DETAILS
Computer artifacts
Mobile artifacts
ANALYZE EVIDENCE
SELECT AN EVIDENCE SOURCE
CONNECTED DRIVE
FILES & FOLDERS
COMPUTER IMAGE
VOLUME SHADOW COPY
MOBILE SOURCE
BACK
GO TO PROCESSING DETAILS


Magnet AXIOM Process 1.0.11.4067
File Tools Help
LOAD EVIDENCE
CASE DETAILS
EVIDENCE SOURCES
Acquire evidence
Load evidence
PROCESSING DETAILS
Add keywords to search
Calculate hash values
Categorize pictures
Find more artifacts
ARTIFACT DETAILS
Computer artifacts
Mobile artifacts
ANALYZE EVIDENCE
ADD FILES AND FOLDERS
108648.E01
Partition 1 (Microsoft NTFS, 100 MB) System Reserved
Partition 2 (Microsoft NTFS, 465.66 GB)
Unpartitioned space
REFRESH
BACK
NEXT


Magnet AXIOM Process 1.0.11.4067
File Tools Help
LOAD EVIDENCE
CASE DETAILS
EVIDENCE SOURCES
Acquire evidence
Load evidence
PROCESSING DETAILS
Add keywords to search
Calculate hash values
Categorize pictures
Find more artifacts
ARTIFACT DETAILS
Computer artifacts
Mobile artifacts
ANALYZE EVIDENCE
SELECT SEARCH TYPE
Source location
Search type
108648.E01 - Partition 1 (Microsoft NTFS, 100 MB) System Reserved
Full
pagefile.sys / swapfile.sys
$LogFile
$MFT
All files and folders
Volume Shadow Copy
Unallocated space
File slack space
hiberfil.sys
Uninitialized file area
108648.E01 - Partition 2 (Microsoft NTFS, 465.66 GB)
Full
pagefile.sys / swapfile.sys
$LogFile
$MFT
All files and folders
Volume Shadow Copy
Unallocated space
File slack space
hiberfil.sys
BACK
NEXT


Artifacts
Artifacts
File system
Registry
ALL EVIDENCE
REFINED RESULTS

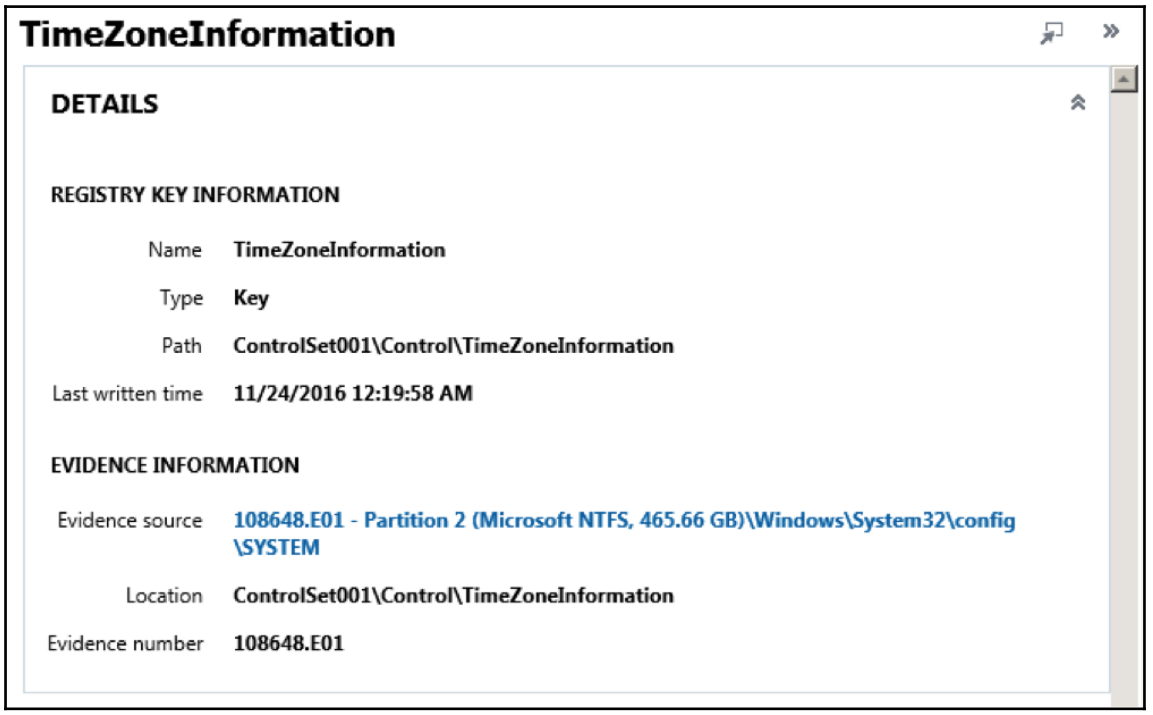

Registry
ALL EVIDENCE
108648.E01
components
DEFAULT
SAM
SECURITY
SOFTWARE
SYSTEM
User hives
Other hives



EVIDENCE (10)

Column view

Name	Type	Data
ActiveTimeBias	REG_DWORD	420
Bias	REG_DWORD	480
DaylightBias	REG_DWORD	4294967236
DaylightName	REG_SZ	@tzres.dll,-211
DaylightStart	REG_BINARY	00 00 03 00 02 00 02 00 00 00 00 00 00 00 00 00
DynamicDaylightTimeDis	REG_DWORD	0
StandardBias	REG_DWORD	0
StandardName	REG_SZ	@tzres.dll,-212
StandardStart	REG_BINARY	00 00 0B 00 01 00 02 00 00 00 00 00 00 00 00 00
TimeZoneKeyName	REG_SZ	Pacific Standard Time



TimeZoneInformation

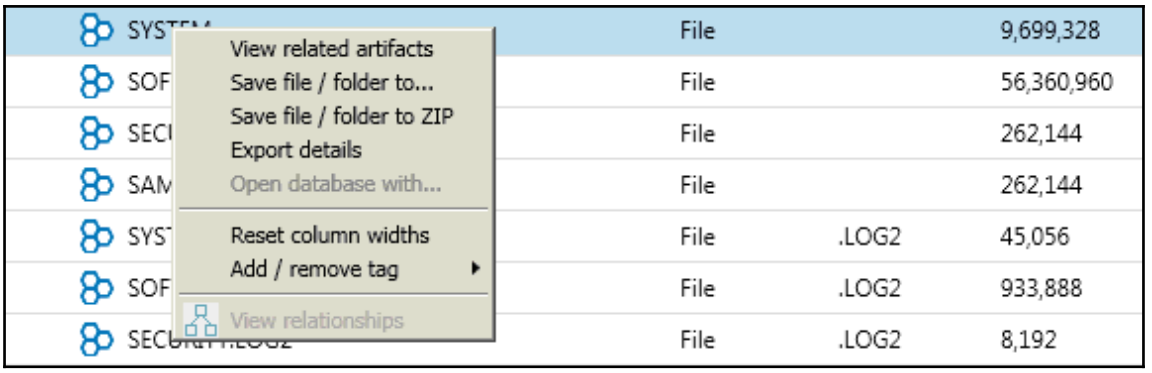
DETAILS

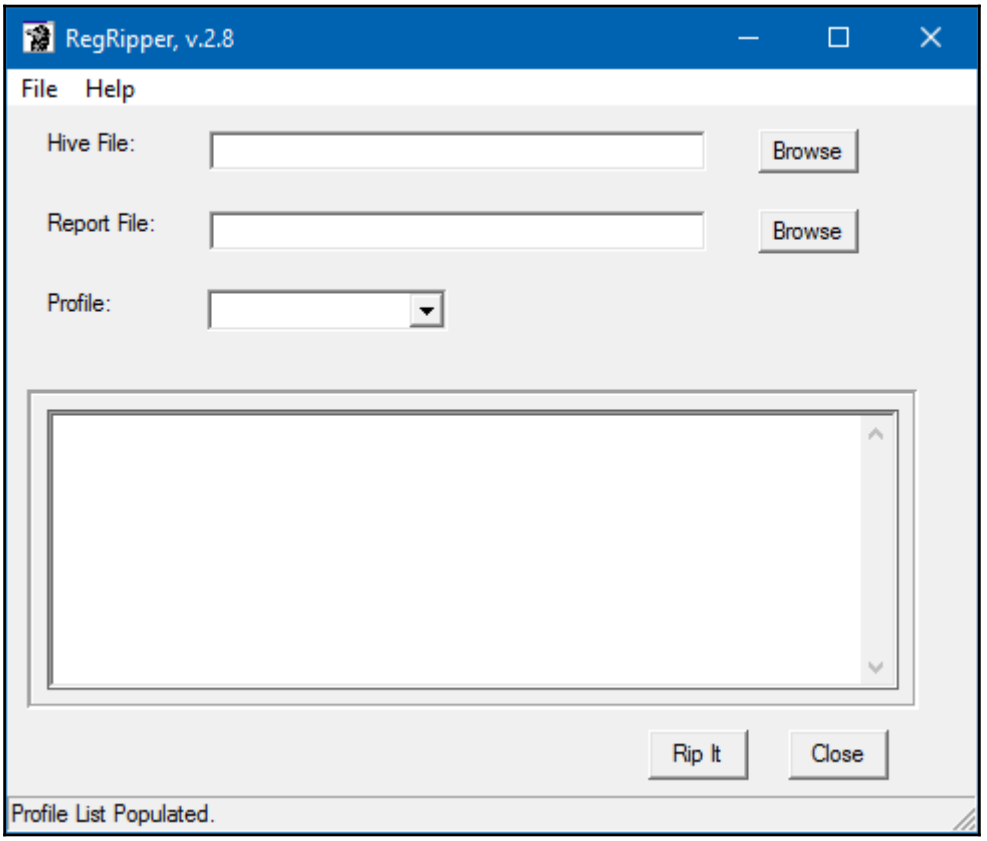
REGISTRY KEY INFORMATION

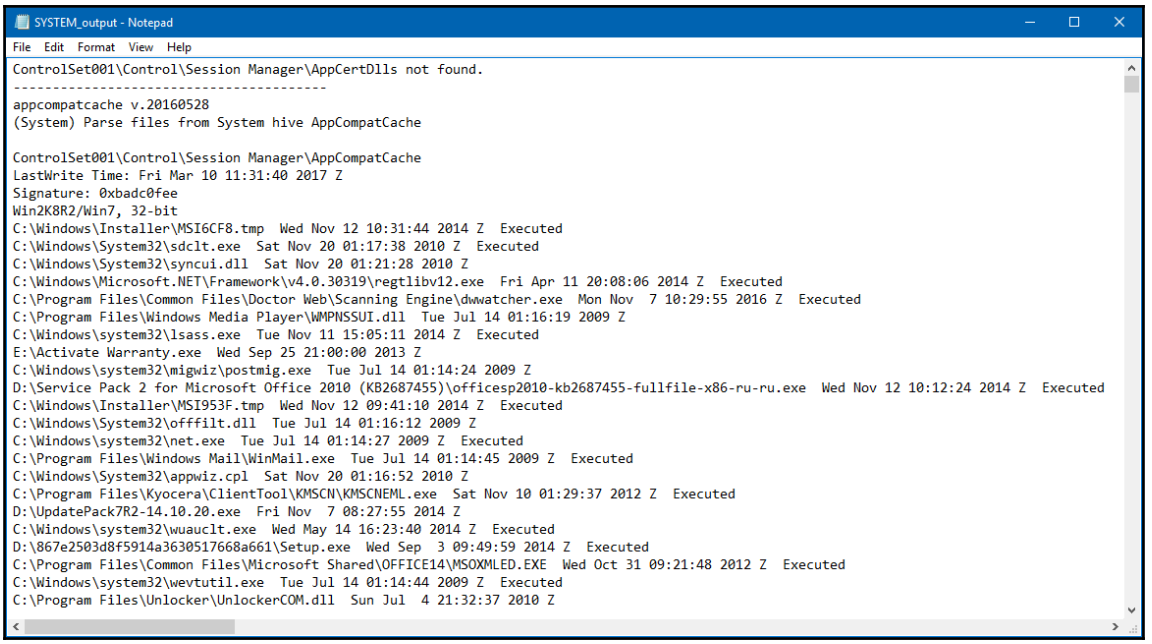
Name	**TimeZoneInformation**
Type	**Key**
Path	**ControlSet001\Control\TimeZoneInformation**
Last written time	**11/24/2016 12:19:58 AM**

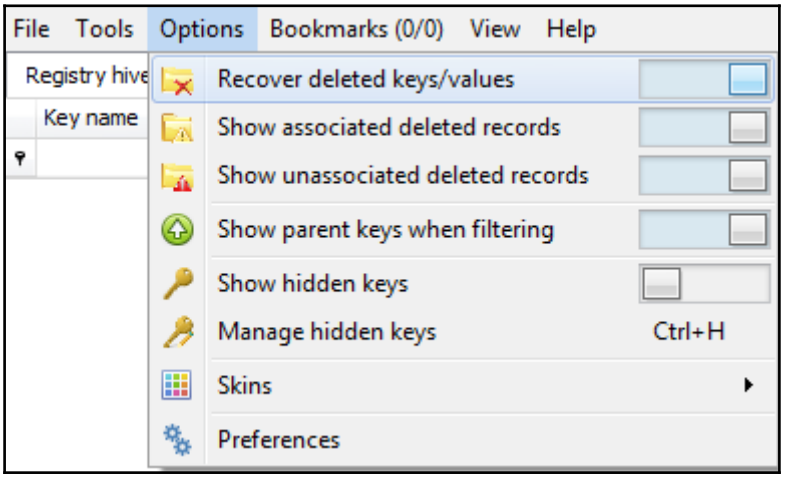
EVIDENCE INFORMATION

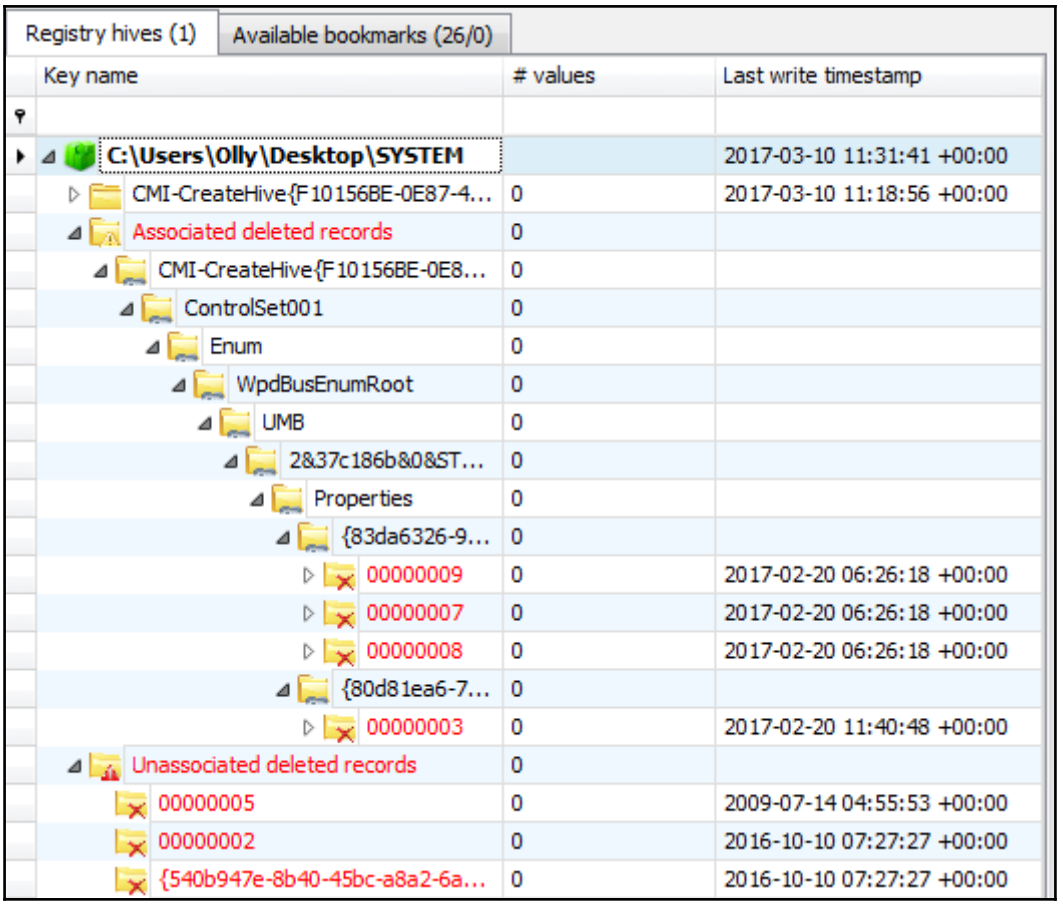
Evidence source	**108648.E01 - Partition 2 (Microsoft NTFS, 465.66 GB)\Windows\System32\config\SYSTEM**
Location	**ControlSet001\Control\TimeZoneInformation**
Evidence number	**108648.E01**


View related artifacts
Save file / folder to...
Save file / folder to ZIP
Export details
Open database with...
Reset column widths
Add / remove tag
View relationships
File
9,699,328
File
56,360,960
File
262,144
File
262,144
File
.LOG2
45,056
File
.LOG2
933,888
File
.LOG2
8,192

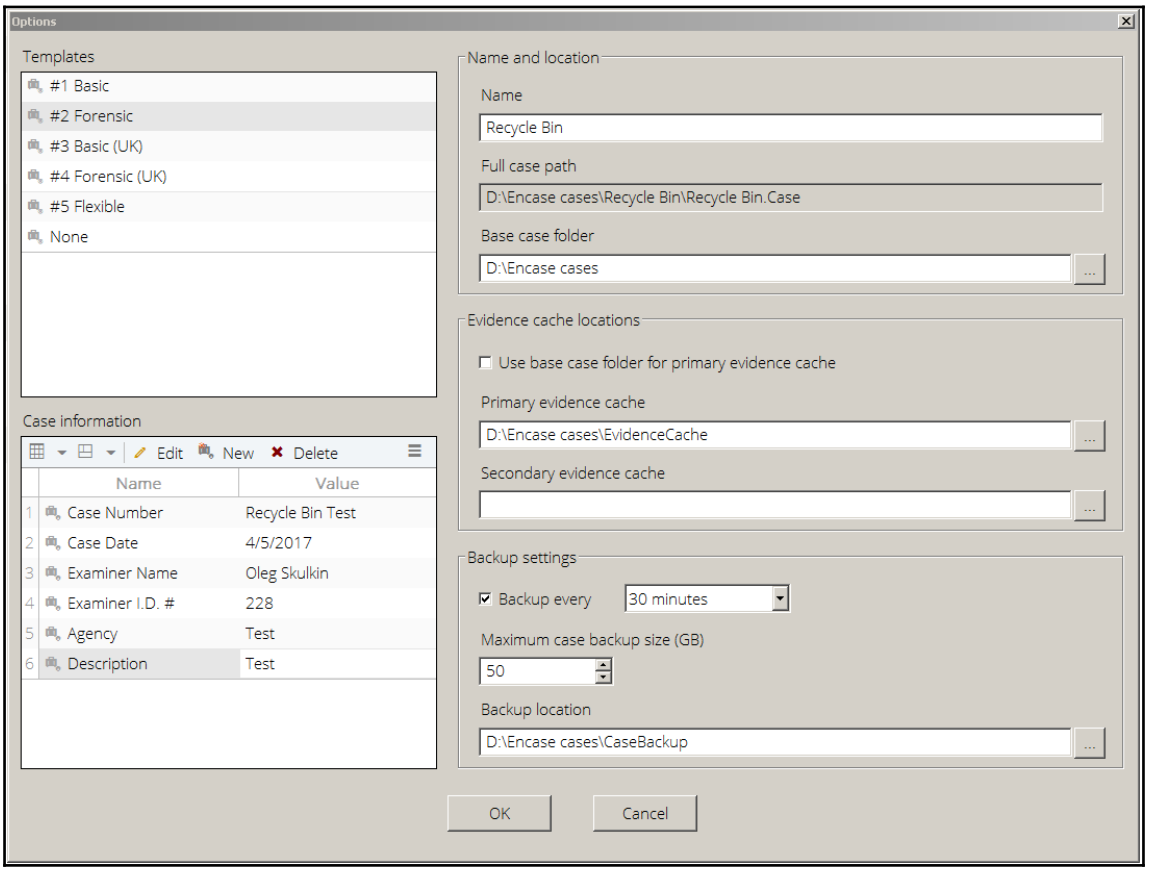

RegRipper, v.2.8
File
Help
Hive File:
Browse
Report File:
Browse
Profile:
Rip It
Close
Profile List Populated.

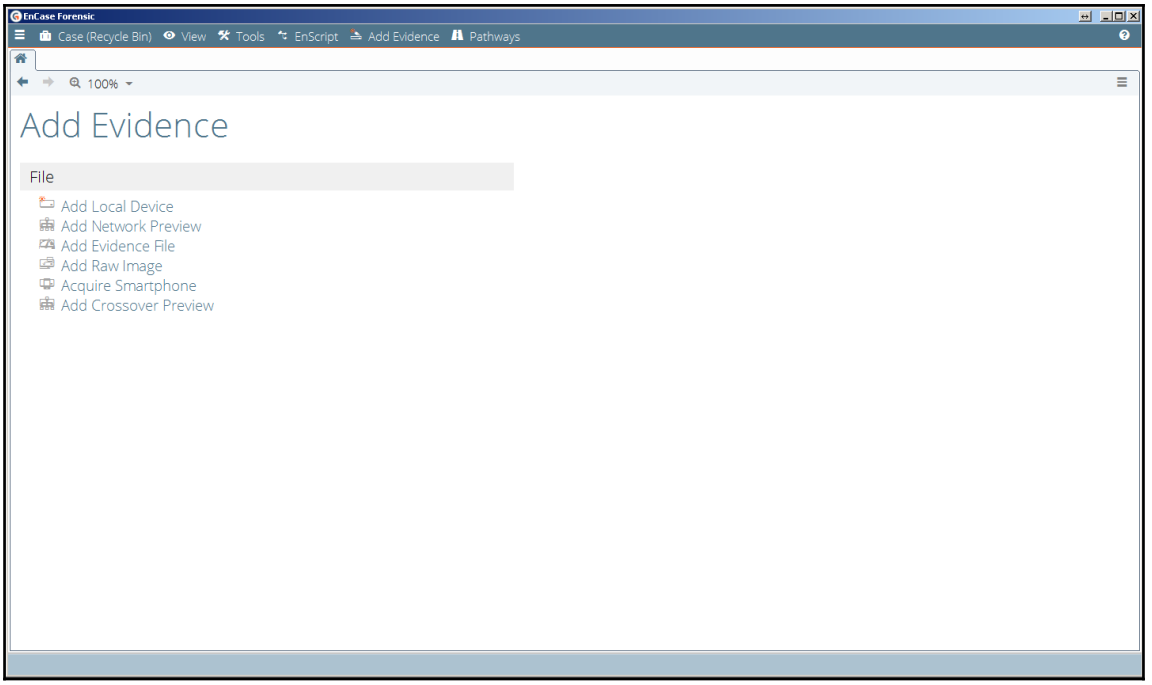

SYSTEM_output - Notepad
File Edit Format View Help
ControlSet001\Control\Session Manager\AppCertDlls not found.
---
appcompatcache v.20160528
(System) Parse files from System hive AppCompatCache
ControlSet001\Control\Session Manager\AppCompatCache
LastWrite Time: Fri Mar 10 11:31:40 2017 Z
Signature: 0xbadc0fee
Win2K8R2/Win7, 32-bit
C:\Windows\Installer\MSI6CF8.tmp Wed Nov 12 10:31:44 2014 Z Executed
C:\Windows\System32\sdclt.exe Sat Nov 20 01:17:38 2010 Z Executed
C:\Windows\System32\syncui.dll Sat Nov 20 01:21:28 2010 Z
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regtlibv12.exe Fri Apr 11 20:08:06 2014 Z Executed
C:\Program Files\Common Files\Doctor Web\Scanning Engine\dwwatcher.exe Mon Nov 7 10:29:55 2016 Z Executed
C:\Program Files\Windows Media Player\WMPNSSUI.dll Tue Jul 14 01:16:19 2009 Z
C:\Windows\system32\lsass.exe Tue Nov 11 15:05:11 2014 Z Executed
E:\Activate Warranty.exe Wed Sep 25 21:00:00 2013 Z
C:\Windows\system32\migwiz\postmig.exe Tue Jul 14 01:14:24 2009 Z
D:\Service Pack 2 for Microsoft Office 2010 (KB2687455)\officesp2010-kb2687455-fullfile-x86-ru-ru.exe Wed Nov 12 10:12:24 2014 Z Executed
C:\Windows\Installer\MSI953F.tmp Wed Nov 12 09:41:10 2014 Z Executed
C:\Windows\System32\offfilt.dll Tue Jul 14 01:16:12 2009 Z
C:\Windows\system32\net.exe Tue Jul 14 01:14:27 2009 Z Executed
C:\Program Files\Windows Mail\WinMail.exe Tue Jul 14 01:14:45 2009 Z Executed
C:\Windows\System32\appwiz.cpl Sat Nov 20 01:16:52 2010 Z
C:\Program Files\Kyocera\ClientTool\KMSCN\KMSCNEML.exe Sat Nov 10 01:29:37 2012 Z Executed
D:\UpdatePack7R2-14.10.20.exe Fri Nov 7 08:27:55 2014 Z
C:\Windows\system32\wuauclt.exe Wed May 14 16:23:40 2014 Z Executed
D:\867e2503d8f5914a3630517668a661\Setup.exe Wed Sep 3 09:49:59 2014 Z Executed
C:\Program Files\Common Files\Microsoft Shared\OFFICE14\MSOXMLED.EXE Wed Oct 31 09:21:48 2012 Z Executed
C:\Windows\system32\wevtutil.exe Tue Jul 14 01:14:44 2009 Z Executed
C:\Program Files\Unlocker\UnlockerCOM.dll Sun Jul 4 21:32:37 2010 Z

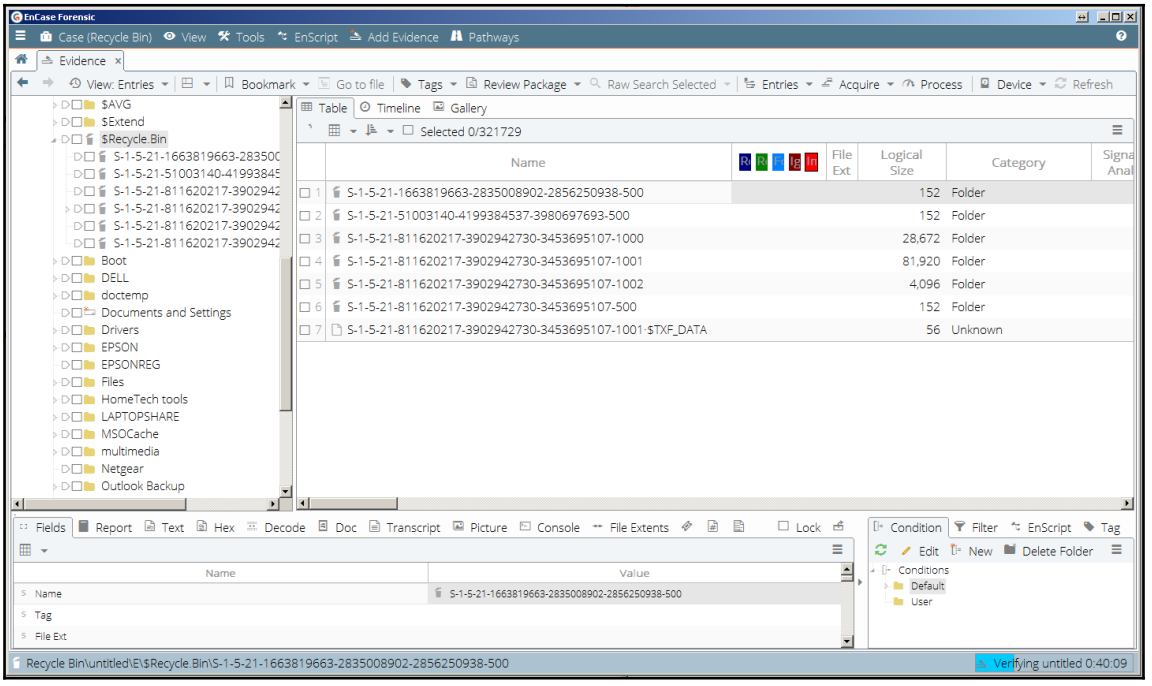

File Tools Options Bookmarks (0/0) View Help
Registry hive
Key name
Recover deleted keys/values
Show associated deleted records
Show unassociated deleted records
Show parent keys when filtering
Show hidden keys
Manage hidden keys Ctrl+H
Skins
Preferences

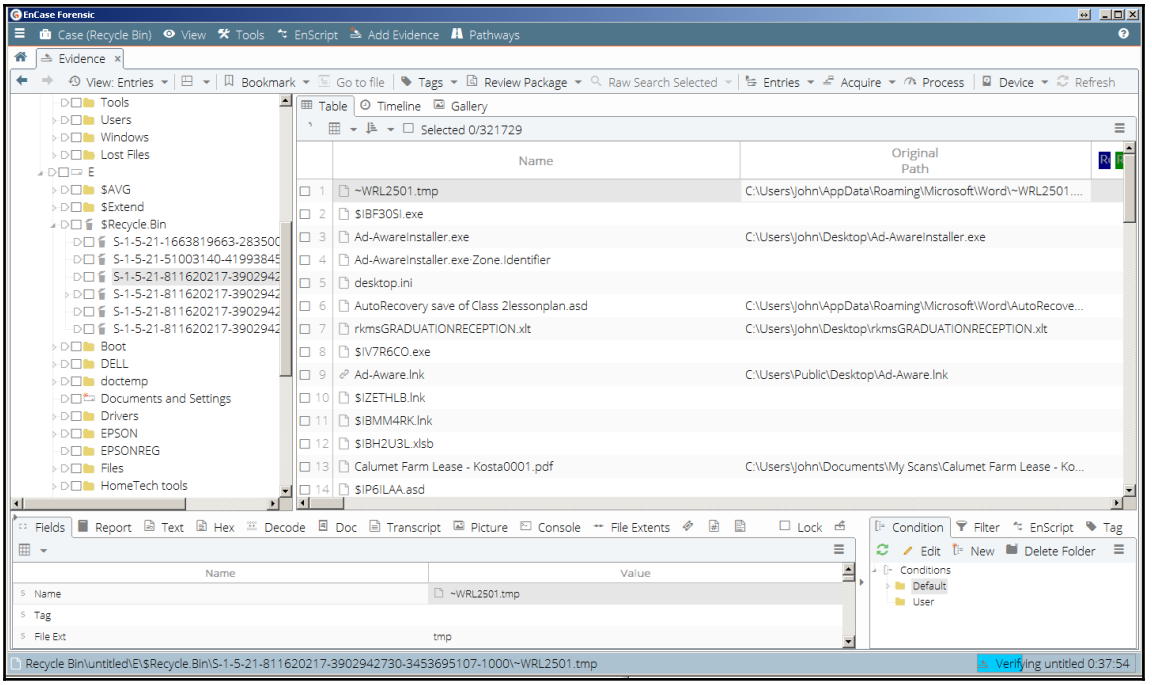

Registry hives (1)
Available bookmarks (26/0)
Key name
values
Last write timestamp
C:\Users\Olly\Desktop\SYSTEM
2017-03-10 11:31:41 +00:00
CMI-CreateHive{F10156BE-0E87-4...
0
2017-03-10 11:18:56 +00:00
Associated deleted records
0
CMI-CreateHive{F10156BE-0E8...
0
ControlSet001
0
Enum
0
WpdBusEnumRoot
0
UMB
0
2&37c186b&0&ST...
0
Properties
0
{83da6326-9...
0
00000009
0
2017-02-20 06:26:18 +00:00
00000007
0
2017-02-20 06:26:18 +00:00
00000008
0
2017-02-20 06:26:18 +00:00
{80d81ea6-7...
0
00000003
0
2017-02-20 11:40:48 +00:00
Unassociated deleted records
0
00000005
0
2009-07-14 04:55:53 +00:00
00000002
0
2016-10-10 07:27:27 +00:00
{540b947e-8b40-45bc-a8a2-6a...
0
2016-10-10 07:27:27 +00:00

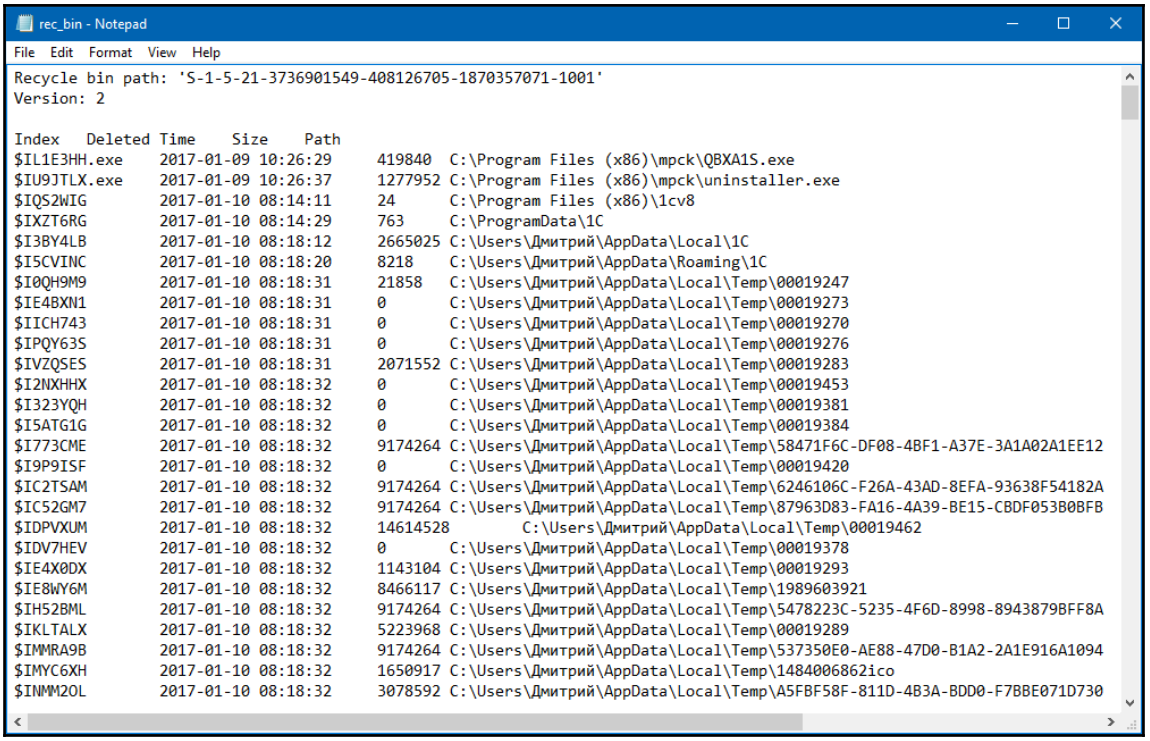
Chapter 7 : Main Windows System Artifacts

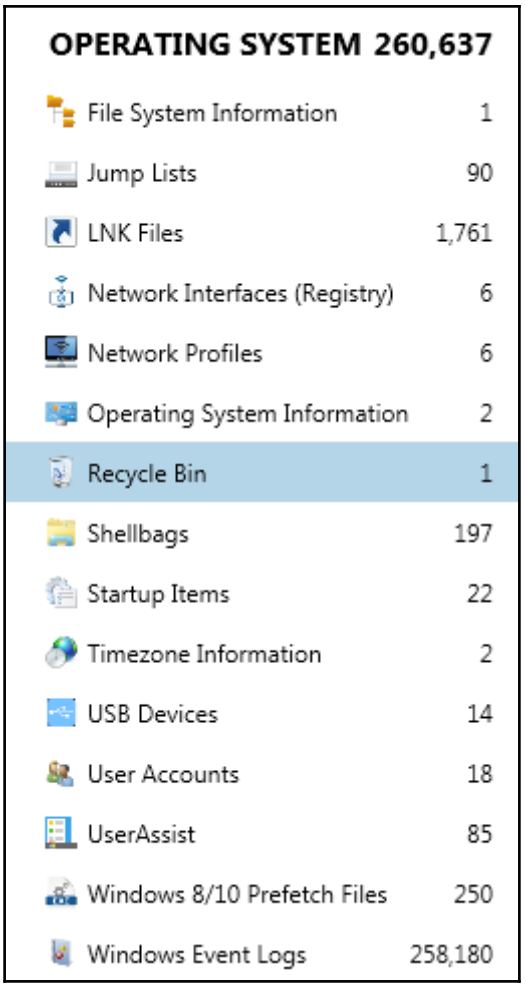



EnCase Forensic
Case (Recycle Bin)
View
Tools
EnScript
Add Evidence
Pathways
100%
Add Evidence
File
Add Local Device
Add Network Preview
Add Evidence File
Add Raw Image
Acquire Smartphone
Add Crossover Preview

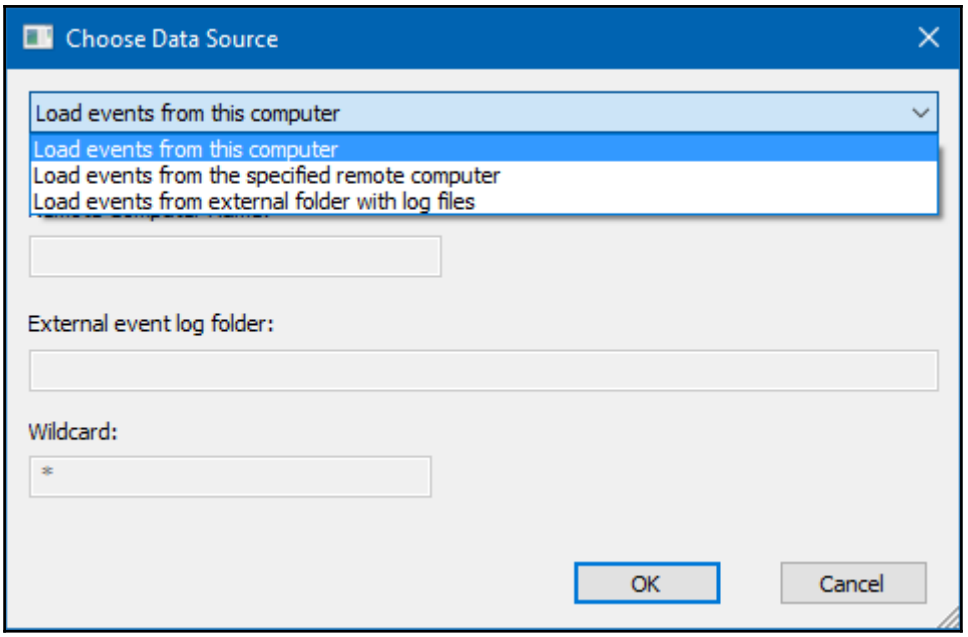

EnCase Forensic
Case (Recycle Bin)
View
Tools
EnScript
Add Evidence
Pathways
Evidence
View: Entries
Bookmark
Go to file
Tags
Review Package
Raw Search Selected
Entries
Acquire
Process
Device
Refresh
$AVG
$Extend
$Recycle.Bin
Boot
DELL
doctemp
Documents and Settings
Drivers
EPSON
EPSONREG
Files
HomeTech tools
LAPTOPSHARE
MSOCache
multimedia
Netgear
Outlook Backup
Table
Timeline
Gallery
Selected 0/321729
Name
File Ext
Logical Size
Category
1 S-1-5-21-1663819663-2835008902-2856250938-500 152 Folder
2 S-1-5-21-51003140-4199384537-3980697693-500 152 Folder
3 S-1-5-21-811620217-3902942730-3453695107-1000 28,672 Folder
4 S-1-5-21-811620217-3902942730-3453695107-1001 81,920 Folder
5 S-1-5-21-811620217-3902942730-3453695107-1002 4,096 Folder
6 S-1-5-21-811620217-3902942730-3453695107-500 152 Folder
7 S-1-5-21-811620217-3902942730-3453695107-1001:$TXF_DATA 56 Unknown
Fields
Report
Text
Hex
Decode
Doc
Transcript
Picture
Console
File Extents
Lock
Condition
Filter
EnScript
Tag
Edit
New
Delete Folder
Conditions
Default
User
Name
Value
Name
S-1-5-21-1663819663-2835008902-2856250938-500
Tag
File Ext
Recycle Bin\untitled\E\$Recycle.Bin\S-1-5-21-1663819663-2835008902-2856250938-500
Verifying untitled 0:40:09

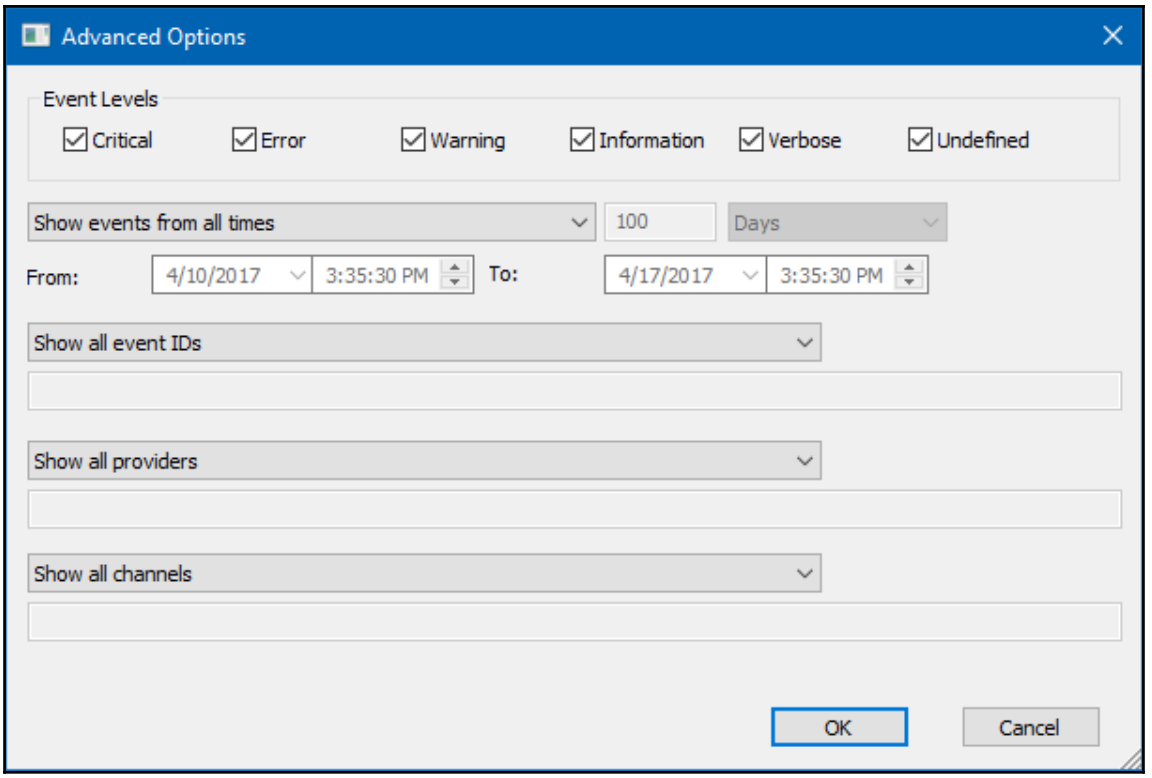

EnCase Forensic
Case (Recycle Bin)
View
Tools
EnScript
Add Evidence
Pathways
Evidence
View: Entries
Bookmark
Go to file
Tags
Review Package
Raw Search Selected
Entries
Acquire
Process
Device
Refresh
Tools
Users
Windows
Lost Files
E
$AVG
$Extend
$Recycle.Bin
S-1-5-21-1663819663-283500
S-1-5-21-51003140-41993845
S-1-5-21-811620217-3902942
S-1-5-21-811620217-3902942
S-1-5-21-811620217-3902942
S-1-5-21-811620217-3902942
Boot
DELL
doctemp
Documents and Settings
Drivers
EPSON
EPSONREG
Files
HomeTech tools
Table
Timeline
Gallery
Selected 0/321729
Name
Original Path
1 ~WRL2501.tmp C:\Users\John\AppData\Roaming\Microsoft\Word\~WRL2501....
2 $IBF30SI.exe
3 Ad-AwareInstaller.exe C:\Users\John\Desktop\Ad-AwareInstaller.exe
4 Ad-AwareInstaller.exe:Zone.Identifier
5 desktop.ini
6 AutoRecovery save of Class 2lessonplan.asd C:\Users\John\AppData\Roaming\Microsoft\Word\AutoRecove...
7 rkmsGRADUATIONRECEPTION.xlt C:\Users\John\Desktop\rkmsGRADUATIONRECEPTION.xlt
8 $IV7R6CO.exe
9 Ad-Aware.lnk C:\Users\Public\Desktop\Ad-Aware.lnk
10 $IZETHLB.lnk
11 $IBMM4RK.lnk
12 $IBH2U3L.xlsb
13 Calumet Farm Lease - Kosta0001.pdf C:\Users\John\Documents\My Scans\Calumet Farm Lease - Ko...
14 $IP6ILAA.asd
Fields
Report
Text
Hex
Decode
Doc
Transcript
Picture
Console
File Extents
Lock
Condition
Filter
EnScript
Tag
Edit
New
Delete Folder
Conditions
Default
User
Name
Value
Name ~WRL2501.tmp
Tag
File Ext tmp
Recycle Bin\untitled\E\$Recycle.Bin\S-1-5-21-811620217-3902942730-3453695107-1000\~WRL2501.tmp
Verifying untitled 0:37:54

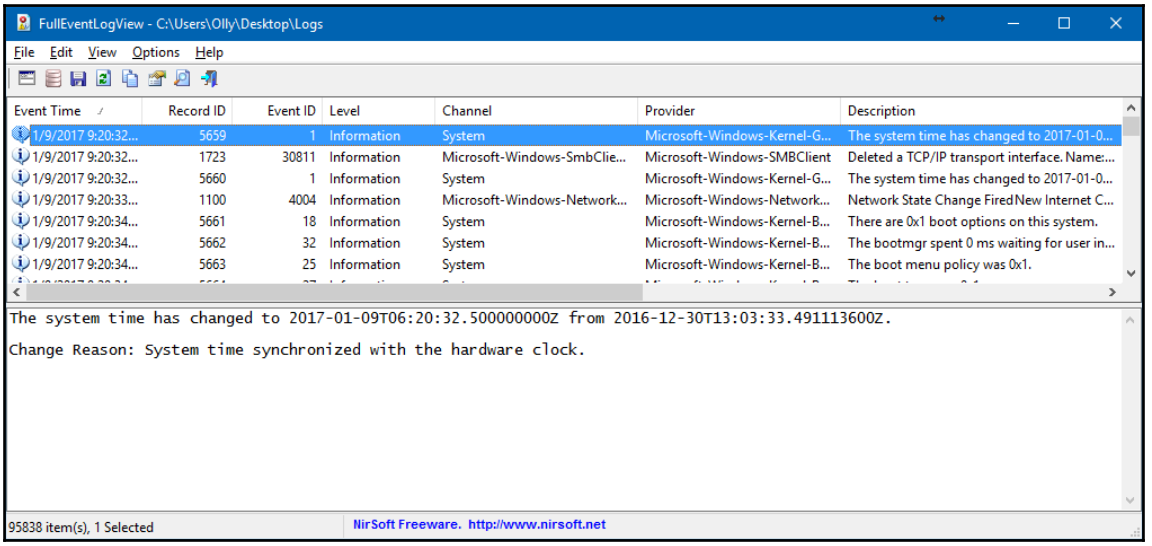

rec_bin - Notepad
File Edit Format View Help
Recycle bin path: 'S-1-5-21-3736901549-408126705-1870357071-1001'
Version: 2
Index Deleted Time Size Path
$IL1E3HH.exe 2017-01-09 10:26:29 419840 C:\Program Files (x86)\mpck\QBXA1S.exe
$IU9JTLX.exe 2017-01-09 10:26:37 1277952 C:\Program Files (x86)\mpck\uninstaller.exe
$IQS2WIG 2017-01-10 08:14:11 24 C:\Program Files (x86)\1cv8
$IXZT6RG 2017-01-10 08:14:29 763 C:\ProgramData\1C
$I3BY4LB 2017-01-10 08:18:12 2665025 C:\Users\Дмитрий\AppData\Local\1C
$I5CVINC 2017-01-10 08:18:20 8218 C:\Users\Дмитрий\AppData\Roaming\1C
$I0QH9M9 2017-01-10 08:18:31 21858 C:\Users\Дмитрий\AppData\Local\Temp\00019247
$IE4BXN1 2017-01-10 08:18:31 0 C:\Users\Дмитрий\AppData\Local\Temp\00019273
$IICH743 2017-01-10 08:18:31 0 C:\Users\Дмитрий\AppData\Local\Temp\00019270
$IPQY63S 2017-01-10 08:18:31 0 C:\Users\Дмитрий\AppData\Local\Temp\00019276
$IVZQSES 2017-01-10 08:18:31 2071552 C:\Users\Дмитрий\AppData\Local\Temp\00019283
$I2NXHHX 2017-01-10 08:18:32 0 C:\Users\Дмитрий\AppData\Local\Temp\00019453
$I323YQH 2017-01-10 08:18:32 0 C:\Users\Дмитрий\AppData\Local\Temp\00019381
$I5ATG1G 2017-01-10 08:18:32 0 C:\Users\Дмитрий\AppData\Local\Temp\00019384
$I773CME 2017-01-10 08:18:32 9174264 C:\Users\Дмитрий\AppData\Local\Temp\58471F6C-DF08-4BF1-A37E-3A1A02A1EE12
$I9P9ISF 2017-01-10 08:18:32 0 C:\Users\Дмитрий\AppData\Local\Temp\00019420
$IC2TSAM 2017-01-10 08:18:32 9174264 C:\Users\Дмитрий\AppData\Local\Temp\6246106C-F26A-43AD-8EFA-93638F54182A
$IC52GM7 2017-01-10 08:18:32 9174264 C:\Users\Дмитрий\AppData\Local\Temp\87963D83-FA16-4A39-BE15-CBDF053B0BFB
$IDPVXUM 2017-01-10 08:18:32 14614528 C:\Users\Дмитрий\AppData\Local\Temp\00019462
$IDV7HEV 2017-01-10 08:18:32 0 C:\Users\Дмитрий\AppData\Local\Temp\00019378
$IE4X0DX 2017-01-10 08:18:32 1143104 C:\Users\Дмитрий\AppData\Local\Temp\00019293
$IE8WY6M 2017-01-10 08:18:32 8466117 C:\Users\Дмитрий\AppData\Local\Temp\1989603921
$IH52BML 2017-01-10 08:18:32 9174264 C:\Users\Дмитрий\AppData\Local\Temp\5478223C-5235-4F6D-8998-8943879BFF8A
$IKLTALX 2017-01-10 08:18:32 5223968 C:\Users\Дмитрий\AppData\Local\Temp\00019289
$IMMRA9B 2017-01-10 08:18:32 9174264 C:\Users\Дмитрий\AppData\Local\Temp\537350E0-AE88-47D0-B1A2-2A1E916A1094
$IMYC6XH 2017-01-10 08:18:32 1650917 C:\Users\Дмитрий\AppData\Local\Temp\1484006862ico
$INMM2OL 2017-01-10 08:18:32 3078592 C:\Users\Дмитрий\AppData\Local\Temp\A5FBF58F-811D-4B3A-BDD0-F7BBE071D730

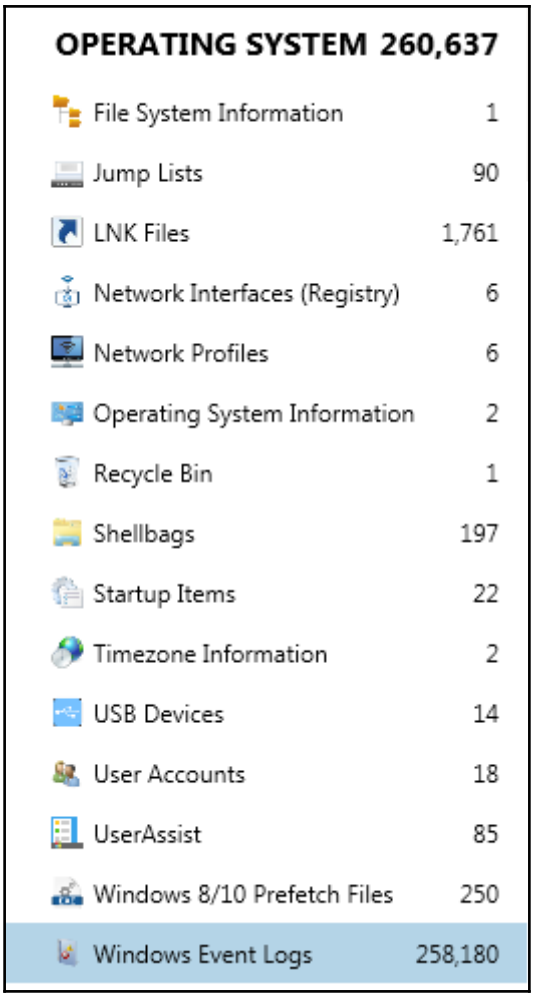


File Name	Deleted Date/Time	User Security Identifier	Original Path	Type	Current...	File Siz...
TeamViewer 9.lnk	3/29/2017 12:14:58 AM	S-1-5-21-2250098342-4205279653-4187590567-1000	C:\Users\Public\Desktop\TeamViewer 9.lnk	File	$RIVPSZD.lnk	1199

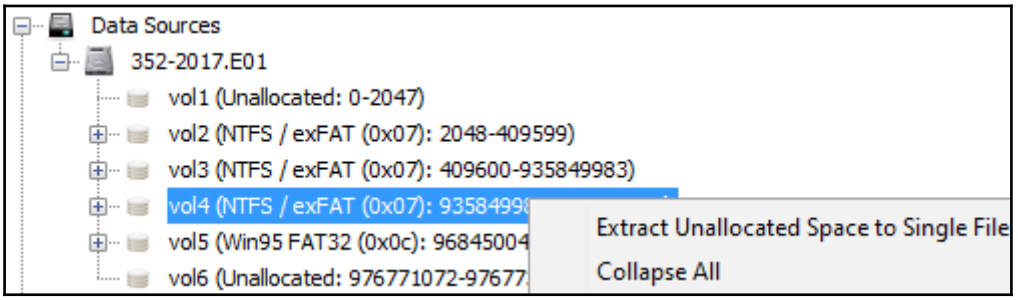

Choose Data Source
Load events from this computer
Load events from this computer
Load events from the specified remote computer
Load events from external folder with log files
External event log folder:
Wildcard:
*
OK
Cancel

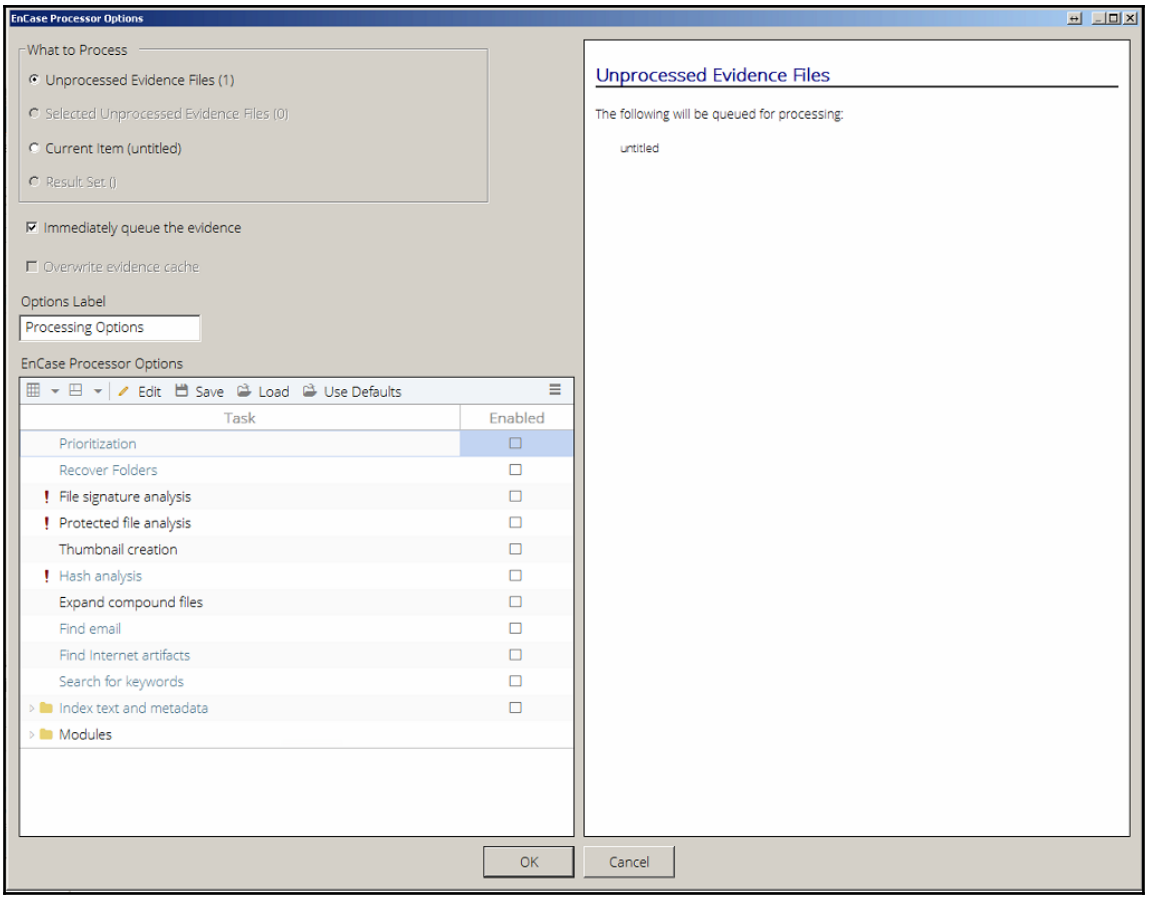

Advanced Options
Event Levels
Critical
Error
Warning
Information
Verbose
Undefined
Show events from all times
100
Days
From:
4/10/2017
3:35:30 PM
To:
4/17/2017
3:35:30 PM
Show all event IDs
Show all providers
Show all channels
OK
Cancel


FullEventLogView - C:\Users\Olly\Desktop\Logs
File Edit View Options Help
Event Time | Record ID | Event ID | Level | Channel | Provider | Description
1/9/2017 9:20:32... 5659 1 Information System Microsoft-Windows-Kernel-G... The system time has changed to 2017-01-0...
1/9/2017 9:20:32... 1723 30811 Information Microsoft-Windows-SmbClie... Microsoft-Windows-SMBClient Deleted a TCP/IP transport interface. Name:...
1/9/2017 9:20:32... 5660 1 Information System Microsoft-Windows-Kernel-G... The system time has changed to 2017-01-0...
1/9/2017 9:20:33... 1100 4004 Information Microsoft-Windows-Network... Microsoft-Windows-Network... Network State Change FiredNew Internet C...
1/9/2017 9:20:34... 5661 18 Information System Microsoft-Windows-Kernel-B... There are 0x1 boot options on this system.
1/9/2017 9:20:34... 5662 32 Information System Microsoft-Windows-Kernel-B... The bootmgr spent 0 ms waiting for user in...
1/9/2017 9:20:34... 5663 25 Information System Microsoft-Windows-Kernel-B... The boot menu policy was 0x1.
The system time has changed to 2017-01-09T06:20:32.500000000Z from 2016-12-30T13:03:33.491113600Z.
Change Reason: System time synchronized with the hardware clock.
95838 item(s), 1 Selected
NirSoft Freeware. http://www.nirsoft.net

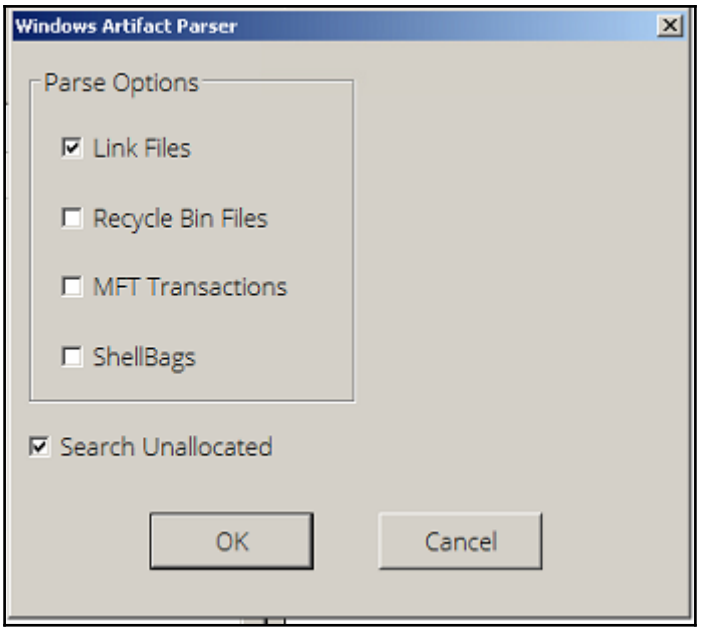

OPERATING SYSTEM 260,637
File System Information 1
Jump Lists 90
LNK Files 1,761
Network Interfaces (Registry) 6
Network Profiles 6
Operating System Information 2
Recycle Bin 1
Shellbags 197
Startup Items 22
Timezone Information 2
USB Devices 14
User Accounts 18
UserAssist 85
Windows 8/10 Prefetch Files 250
Windows Event Logs 258,180

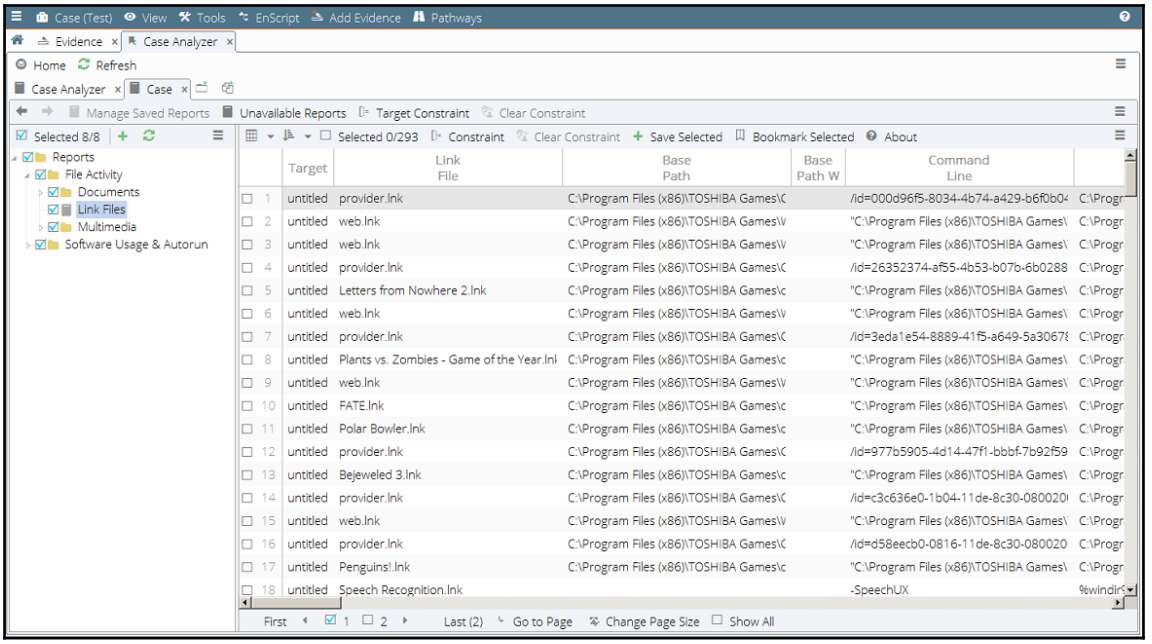
Event ID	Security User ID	Created Date/T...	Event Description Summary	Level	Keywords	Provider Name
23	LocalSystem	7/14/2009 4:56:45 AM	Remote Desktop Services: Session logoff succeeded.	Information	0x1000000000000000	Microsoft-Windows-TerminalServices-Lo
101	LocalSystem	7/14/2009 4:56:45 AM	Windows Defender state updated.	Information	0x4000000000000000	Microsoft-Windows-Windows Defender
1002	LocalService	7/14/2009 4:56:45 AM	The Windows Resource Exhaustion Detector stopped.	Information	0x4000000010000000	Microsoft-Windows-Resource-Exhaustio
5320	LocalSystem	10/19/2010 3:15:20 AM	Checking for Group Policy client extensions that are...	Information	0x4000000000000000	Microsoft-Windows-GroupPolicy
5320	LocalSystem	10/19/2010 3:15:20 AM	Checking for Group Policy client extensions that are...	Information	0x4000000000000000	Microsoft-Windows-GroupPolicy
5320	LocalSystem	10/19/2010 3:15:20 AM	Checking for Group Policy client extensions that are...	Information	0x4000000000000000	Microsoft-Windows-GroupPolicy
5321	LocalSystem	10/19/2010 3:15:20 AM	A previous instance of the Group Policy Client Servic...	Information	0x4000000000000000	Microsoft-Windows-GroupPolicy
4001	LocalService	10/19/2010 3:15:25 AM		Information	0x4000200000000000	Microsoft-Windows-NetworkProfile
10000	LocalService	10/19/2010 3:15:25 AM		Information	0x4000200000000000	Microsoft-Windows-NetworkProfile
4002	LocalService	10/19/2010 3:15:26 AM		Information	0x4001200000000000	Microsoft-Windows-NetworkProfile
10000	LocalService	10/19/2010 3:15:26 AM		Information	0x4000200000000000	Microsoft-Windows-NetworkProfile
10001	LocalService	10/19/2010 3:15:40 AM		Information	0x4000200000000000	Microsoft-Windows-NetworkProfile
4001	LocalService	10/19/2010 3:15:45 AM		Information	0x4000200000000000	Microsoft-Windows-NetworkProfile
10000	LocalService	10/19/2010 3:15:45 AM		Information	0x4000200000000000	Microsoft-Windows-NetworkProfile
4002	LocalService	10/19/2010 3:15:46 AM		Information	0x4001200000000000	Microsoft-Windows-NetworkProfile
10000	LocalService	10/19/2010 3:15:46 AM		Information	0x4000200000000000	Microsoft-Windows-NetworkProfile
1006	LocalService	10/19/2010 3:15:57 AM	Router Advertisement settings have been changed...	Information	0x8000000000000000	Microsoft-Windows-DHCPv6-Client
1017	LocalSystem	10/19/2010 3:16:03 AM	A device will not be used for a ReadyBoost cache be...	Information	0x8000000000004000	Microsoft-Windows-ReadyBoost
1015	LocalSystem	10/19/2010 3:16:13 AM	Summary of ReadyBoot Performance.	Information	0x8000000000002000	Microsoft-Windows-ReadyBoost
1016	LocalSystem	10/19/2010 3:16:14 AM	Boot plan calculation completed.	Information	0x8000000000002000	Microsoft-Windows-ReadyBoost
306	LocalSystem	10/19/2010 3:17:25 AM	The BITS service loaded the job list from disk.		0x4000000000000000	Microsoft-Windows-Bits-Client

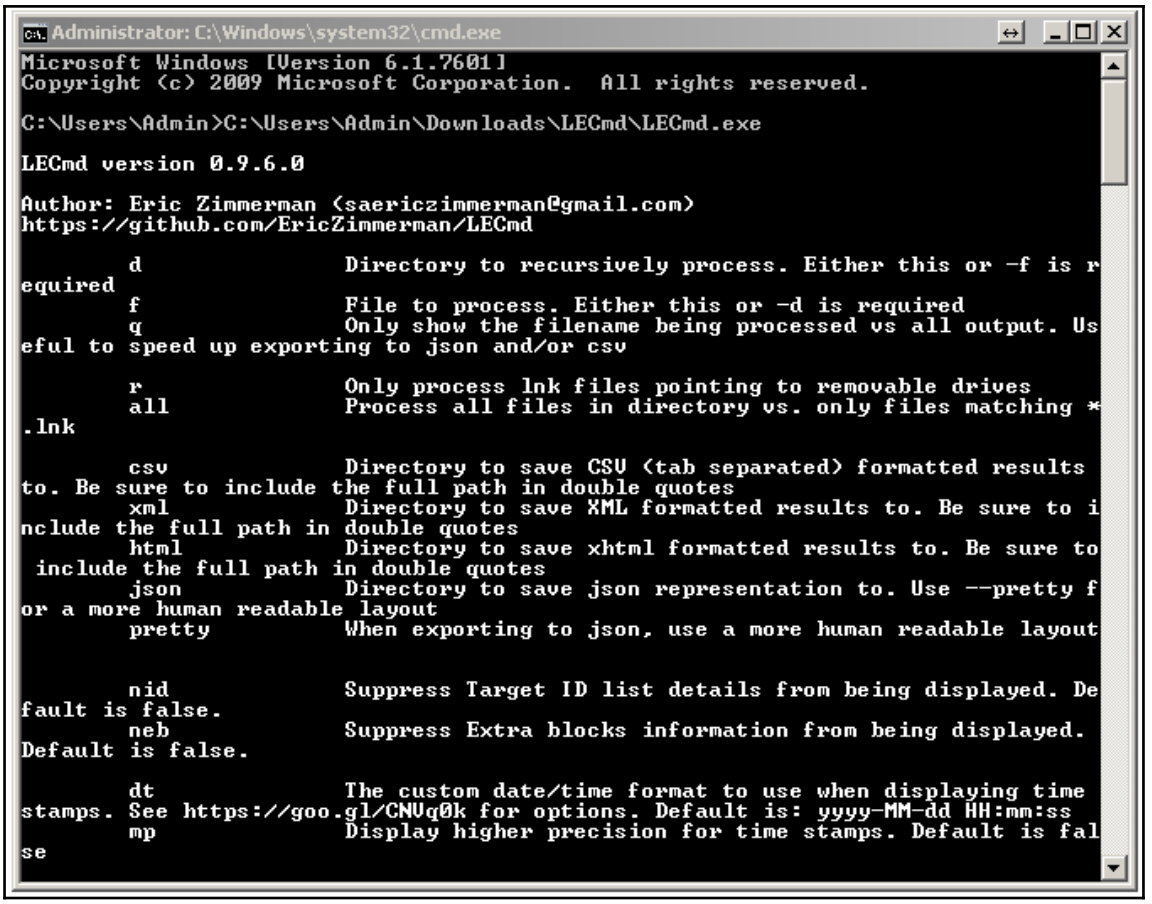



EnCase Processor Options
What to Process
Unprocessed Evidence Files (1)
Selected Unprocessed Evidence Files (0)
Current Item (untitled)
Result Set ()
Immediately queue the evidence
Overwrite evidence cache
Options Label
Processing Options
EnCase Processor Options
Edit
Save
Load
Use Defaults
Task
Enabled
Prioritization
Recover Folders
File signature analysis
Protected file analysis
Thumbnail creation
Hash analysis
Expand compound files
Find email
Find Internet artifacts
Search for keywords
Index text and metadata
Modules
Unprocessed Evidence Files
The following will be queued for processing:
untitled
OK
Cancel

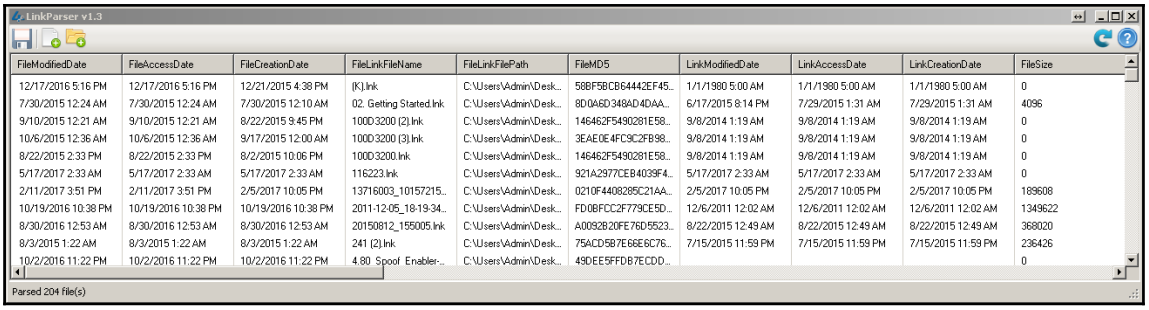

Modules
System Info Parser
File Carver
Windows Event Log Parser
Windows Artifact Parser
Unix Login
Linux Syslog Parser
OS X Artifact Parser

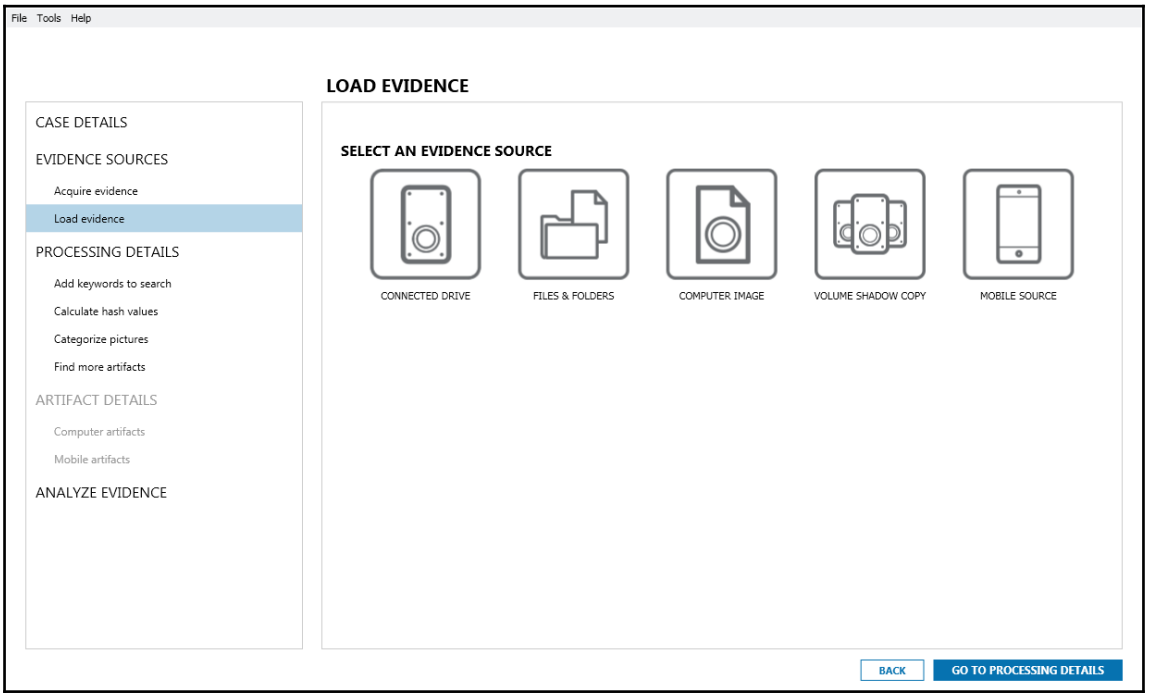

Windows Artifact Parser
Parse Options
Link Files
Recycle Bin Files
MFT Transactions
ShellBags
Search Unallocated
OK
Cancel

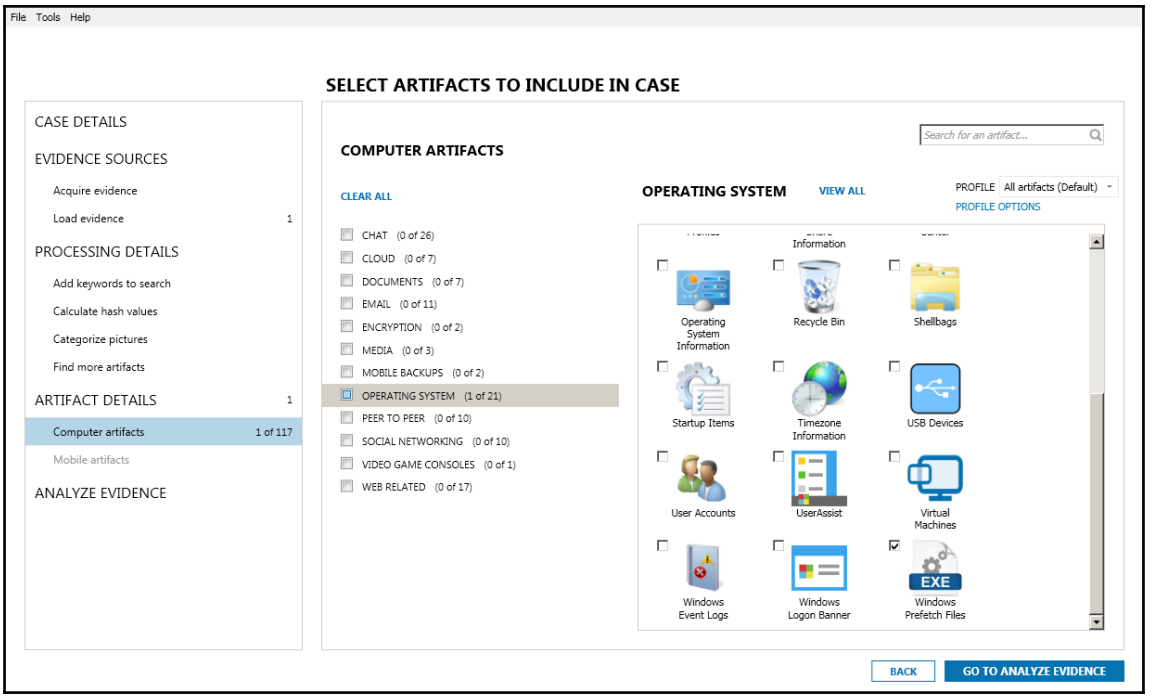

Case (Test)
View
Tools
EnScript
Add Evidence
Pathways
Evidence
Case Analyzer
Home
Refresh
Case
Manage Saved Reports
Unavailable Reports
Target Constraint
Clear Constraint
Selected 8/8
Reports
File Activity
Documents
Link Files
Multimedia
Software Usage & Autorun
Selected 0/293
Constraint
Save Selected
Bookmark Selected
About
Target
Link File
Base Path
Base Path W
Command Line
1 untitled provider.lnk C:\Program Files (x86)\TOSHIBA Games\C /id=000d96f5-8034-4b74-a429-b6f0b0
2 untitled web.lnk C:\Program Files (x86)\TOSHIBA Games\W "C:\Program Files (x86)\TOSHIBA Games\
3 untitled web.lnk C:\Program Files (x86)\TOSHIBA Games\W "C:\Program Files (x86)\TOSHIBA Games\
4 untitled provider.lnk C:\Program Files (x86)\TOSHIBA Games\C /id=26352374-af55-4b53-b07b-6b0288
5 untitled Letters from Nowhere 2.lnk C:\Program Files (x86)\TOSHIBA Games\c "C:\Program Files (x86)\TOSHIBA Games\
6 untitled web.lnk C:\Program Files (x86)\TOSHIBA Games\W "C:\Program Files (x86)\TOSHIBA Games\
7 untitled provider.lnk C:\Program Files (x86)\TOSHIBA Games\C /id=3eda1e54-8889-41f5-a649-5a3067
8 untitled Plants vs. Zombies - Game of the Year.lnl C:\Program Files (x86)\TOSHIBA Games\c "C:\Program Files (x86)\TOSHIBA Games\
9 untitled web.lnk C:\Program Files (x86)\TOSHIBA Games\W "C:\Program Files (x86)\TOSHIBA Games\
10 untitled FATE.lnk C:\Program Files (x86)\TOSHIBA Games\c "C:\Program Files (x86)\TOSHIBA Games\
11 untitled Polar Bowler.lnk C:\Program Files (x86)\TOSHIBA Games\c "C:\Program Files (x86)\TOSHIBA Games\
12 untitled provider.lnk C:\Program Files (x86)\TOSHIBA Games\C /id=977b5905-4d14-47f1-bbbf-7b92f59
13 untitled Bejeweled 3.lnk C:\Program Files (x86)\TOSHIBA Games\c "C:\Program Files (x86)\TOSHIBA Games\
14 untitled provider.lnk C:\Program Files (x86)\TOSHIBA Games\C /id=c3c636e0-1b04-11de-8c30-080020
15 untitled web.lnk C:\Program Files (x86)\TOSHIBA Games\W "C:\Program Files (x86)\TOSHIBA Games\
16 untitled provider.lnk C:\Program Files (x86)\TOSHIBA Games\C /id=d58eecb0-0816-11de-8c30-080020
17 untitled Penguins!.lnk C:\Program Files (x86)\TOSHIBA Games\c "C:\Program Files (x86)\TOSHIBA Games\
18 untitled Speech Recognition.lnk -SpeechUX
First
Last (2)
Go to Page
Change Page Size
Show All

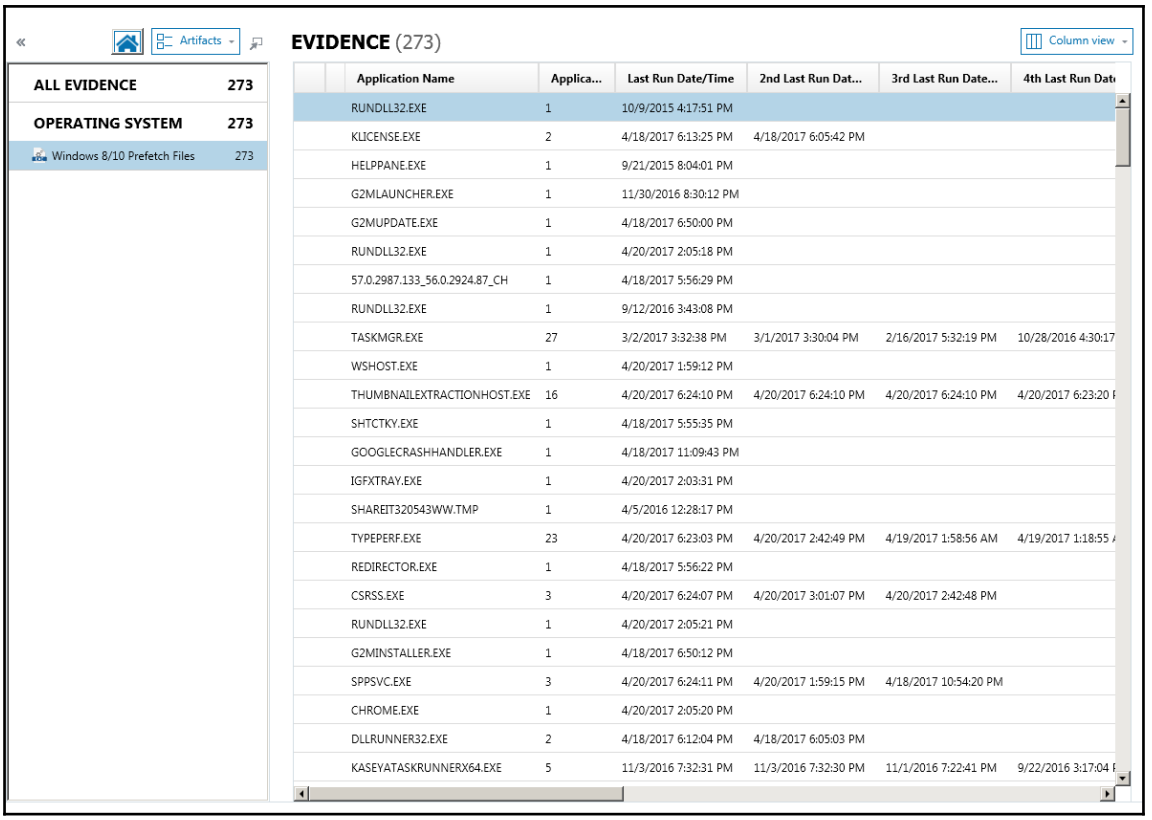

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Admin>C:\Users\Admin\Downloads\LECmd\LECmd.exe
LECmd version 0.9.6.0
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/LECmd
d Directory to recursively process. Either this or -f is required
f File to process. Either this or -d is required
q Only show the filename being processed vs all output. Useful to speed up exporting to json and/or csv
r Only process lnk files pointing to removable drives
all Process all files in directory vs. only files matching *.lnk
csv Directory to save CSV (tab separated) formatted results to. Be sure to include the full path in double quotes
xml Directory to save XML formatted results to. Be sure to include the full path in double quotes
html Directory to save xhtml formatted results to. Be sure to include the full path in double quotes
json Directory to save json representation to. Use --pretty for a more human readable layout
pretty When exporting to json, use a more human readable layout
nid Suppress Target ID list details from being displayed. Default is false.
neb Suppress Extra blocks information from being displayed. Default is false.
dt The custom date/time format to use when displaying time stamps. See https://goo.gl/CNVq0k for options. Default is: yyyy-MM-dd HH:mm:ss
mp Display higher precision for time stamps. Default is false


N:\Users\NP\AppData\Roaming\Microsoft\Office\Recent\LacyMilletCL.LNK
Source Created: 2016-07-28 13:43:04
Source Modified: 2016-08-04 17:58:23
Source Accessed: 2016-08-04 17:58:23
Target Created: 2016-07-28 13:43:03
Target Modified: 2016-08-04 17:58:22
Target Accessed: 2016-08-04 17:58:22
File Size: 25088 (bytes)
Relative Path: ..\..\..\..\..\Desktop\LacyMilletCL.doc
Working Directory:
File Attributes: FileAttributeArchive
Header Flags: HasTargetIdList, HasLinkInfo, HasRelativePath, IsUnicode
Drive Type: Fixed storage media (Hard drive)
8E19DC20 OS
Local Path: C:\Users\
Common Path: NP\Desktop\LacyMilletCL.doc
Arguments:
TargetID Absolute Path: My Computer\C:\Users\NP\Desktop\LacyMilletCL.doc
Target $MFT Entry Number: 0x173C6
Target $MFT Sequence Number: 0x2B
MachineID: np-pc
Machine MAC Address: 5c:e0:c5:6d:aa:b9
MAC Vendor: (Unknown vendor) (vendor not included in source .lnk file, auto-resolved by LECmd for end-user upon parsing)
Tracker Created On: 2016-07-14 08:23:35
Extra Blocks Present: KnownFolderDataBlock, PropertyStoreDataBlock, TrackerDataBaseBlock

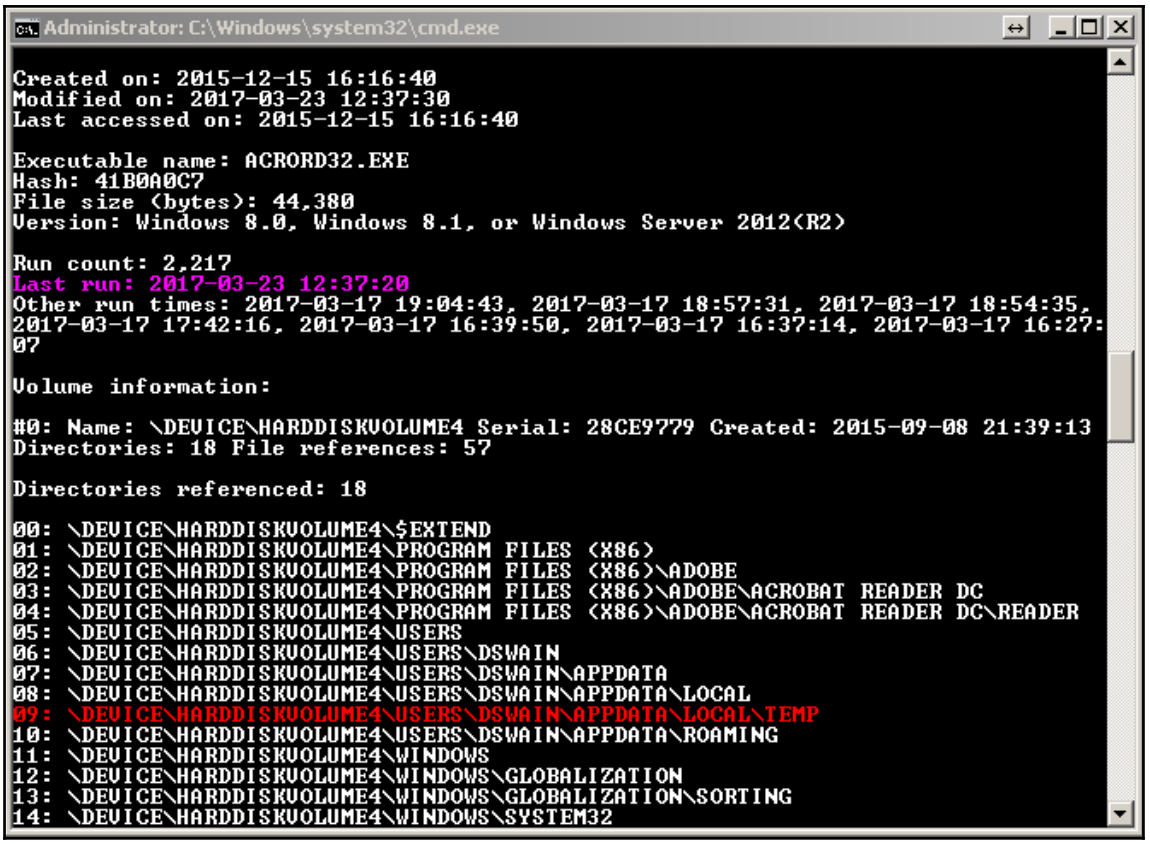

LinkParser v1.3
FileModifiedDate
FileAccessDate
FileCreationDate
FileLinkFileName
FileLinkFilePath
FileMD5
LinkModifiedDate
LinkAccessDate
LinkCreationDate
FileSize
12/17/2016 5:16 PM 12/17/2016 5:16 PM 12/21/2015 4:38 PM (K).lnk C:\Users\Admin\Desk... 58BF5BCB64442EF45... 1/1/1980 5:00 AM 1/1/1980 5:00 AM 1/1/1980 5:00 AM 0
7/30/2015 12:24 AM 7/30/2015 12:24 AM 7/30/2015 12:10 AM 02. Getting Started.lnk C:\Users\Admin\Desk... 8D0A6D348AD4DAA... 6/17/2015 8:14 PM 7/29/2015 1:31 AM 7/29/2015 1:31 AM 4096
9/10/2015 12:21 AM 9/10/2015 12:21 AM 8/22/2015 9:45 PM 100D3200 (2).lnk C:\Users\Admin\Desk... 146462F5490281E58... 9/8/2014 1:19 AM 9/8/2014 1:19 AM 9/8/2014 1:19 AM 0
10/6/2015 12:36 AM 10/6/2015 12:36 AM 9/17/2015 12:00 AM 100D3200 (3).lnk C:\Users\Admin\Desk... 3EAE0E4FC9C2FB98... 9/8/2014 1:19 AM 9/8/2014 1:19 AM 9/8/2014 1:19 AM 0
8/22/2015 2:33 PM 8/22/2015 2:33 PM 8/2/2015 10:06 PM 100D3200.lnk C:\Users\Admin\Desk... 146462F5490281E58... 9/8/2014 1:19 AM 9/8/2014 1:19 AM 9/8/2014 1:19 AM 0
5/17/2017 2:33 AM 5/17/2017 2:33 AM 5/17/2017 2:33 AM 116223.lnk C:\Users\Admin\Desk... 921A2977CEB4039F4... 5/17/2017 2:33 AM 5/17/2017 2:33 AM 5/17/2017 2:33 AM 0
2/11/2017 3:51 PM 2/11/2017 3:51 PM 2/5/2017 10:05 PM 13716003_10157215... C:\Users\Admin\Desk... 0210F4408285C21AA... 2/5/2017 10:05 PM 2/5/2017 10:05 PM 2/5/2017 10:05 PM 189608
10/19/2016 10:38 PM 10/19/2016 10:38 PM 10/19/2016 10:38 PM 2011-12-05_18-19-34... C:\Users\Admin\Desk... FD0BFCC2F779CE5D... 12/6/2011 12:02 AM 12/6/2011 12:02 AM 12/6/2011 12:02 AM 1349622
8/30/2016 12:53 AM 8/30/2016 12:53 AM 8/30/2016 12:53 AM 20150812_155005.lnk C:\Users\Admin\Desk... A0092B20FE76D5523... 8/22/2015 12:49 AM 8/22/2015 12:49 AM 8/22/2015 12:49 AM 368020
8/3/2015 1:22 AM 8/3/2015 1:22 AM 8/3/2015 1:22 AM 241 (2).lnk C:\Users\Admin\Desk... 75ACD5B7E66E6C76... 7/15/2015 11:59 PM 7/15/2015 11:59 PM 7/15/2015 11:59 PM 236426
10/2/2016 11:22 PM 10/2/2016 11:22 PM 10/2/2016 11:22 PM 4.80 Spoof Enabler-... C:\Users\Admin\Desk... 49DEE5FFDB7ECDD... 0
Parsed 204 file(s)


File Tools Help
LOAD EVIDENCE
CASE DETAILS
EVIDENCE SOURCES
Acquire evidence
Load evidence
PROCESSING DETAILS
Add keywords to search
Calculate hash values
Categorize pictures
Find more artifacts
ARTIFACT DETAILS
Computer artifacts
Mobile artifacts
ANALYZE EVIDENCE
SELECT AN EVIDENCE SOURCE
CONNECTED DRIVE
FILES & FOLDERS
COMPUTER IMAGE
VOLUME SHADOW COPY
MOBILE SOURCE
BACK
GO TO PROCESSING DETAILS


File Tools Help
SELECT ARTIFACTS TO INCLUDE IN CASE
CASE DETAILS
EVIDENCE SOURCES
Acquire evidence
Load evidence 1
PROCESSING DETAILS
Add keywords to search
Calculate hash values
Categorize pictures
Find more artifacts
ARTIFACT DETAILS 1
Computer artifacts 1 of 117
Mobile artifacts
ANALYZE EVIDENCE
COMPUTER ARTIFACTS
Search for an artifact...
CLEAR ALL
CHAT (0 of 26)
CLOUD (0 of 7)
DOCUMENTS (0 of 7)
EMAIL (0 of 11)
ENCRYPTION (0 of 2)
MEDIA (0 of 3)
MOBILE BACKUPS (0 of 2)
OPERATING SYSTEM (1 of 21)
PEER TO PEER (0 of 10)
SOCIAL NETWORKING (0 of 10)
VIDEO GAME CONSOLES (0 of 1)
WEB RELATED (0 of 17)
OPERATING SYSTEM
VIEW ALL
PROFILE All artifacts (Default)
PROFILE OPTIONS
Operating System Information
Recycle Bin
Shellbags
Startup Items
Timezone Information
USB Devices
User Accounts
UserAssist
Virtual Machines
Windows Event Logs
Windows Logon Banner
Windows Prefetch Files
EXE
BACK
GO TO ANALYZE EVIDENCE

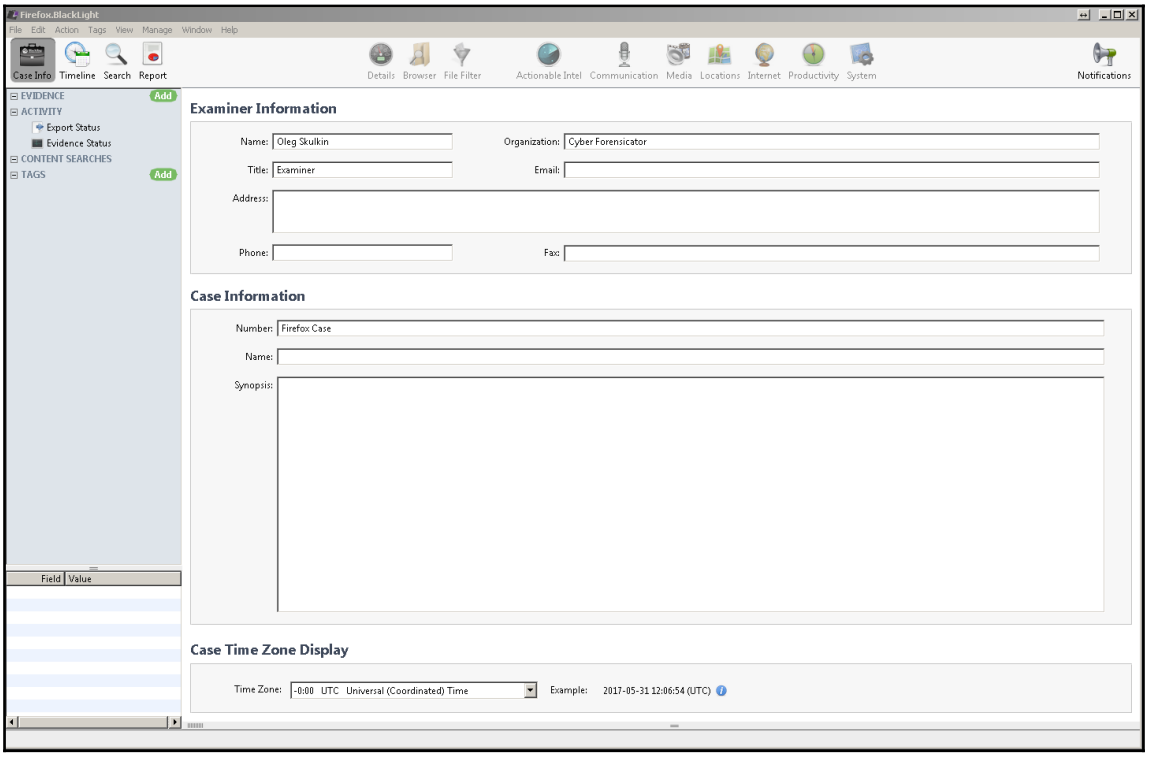


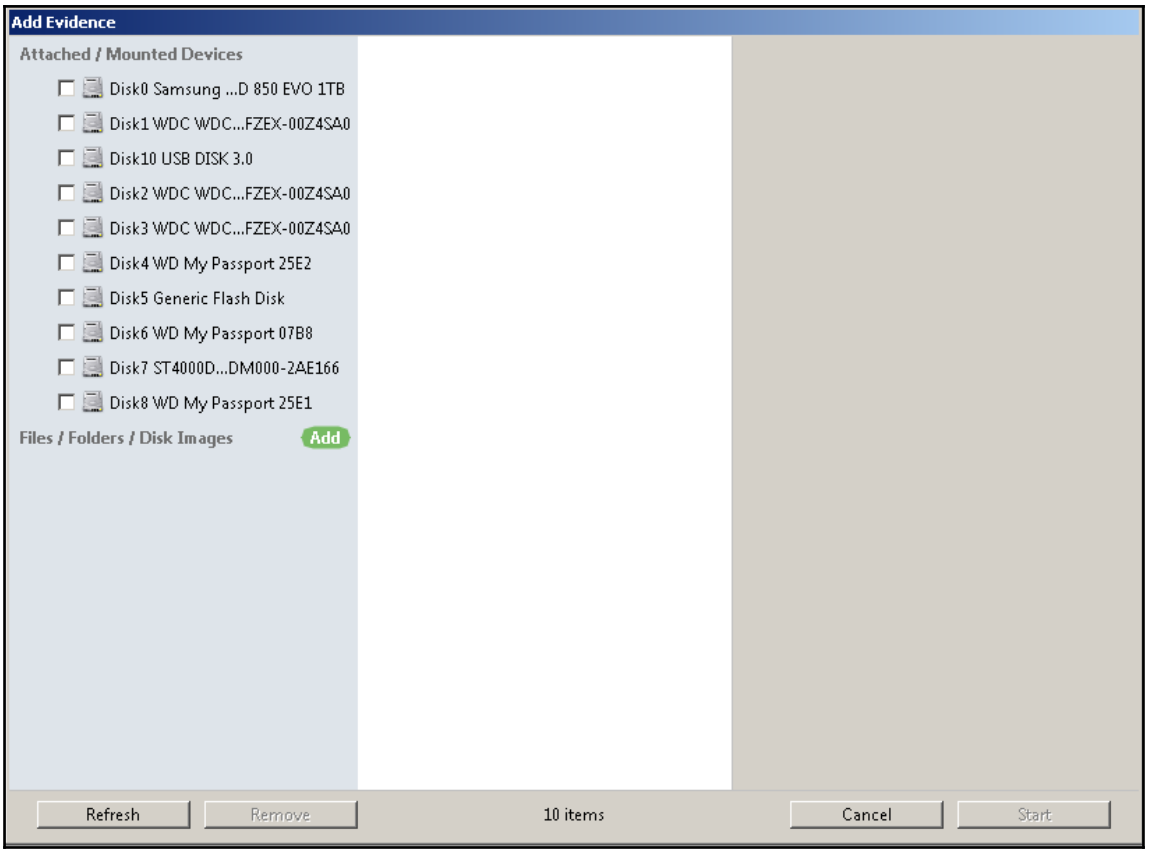
Application Name	Applica...	Last Run Date/Time	2nd Last Run Dat...	3rd Last Run Date...	4th Last Run Dat
RUNDLL32.EXE	1	10/9/2015 4:17:51 PM			
KLICENSE.EXE	2	4/18/2017 6:13:25 PM	4/18/2017 6:05:42 PM		
HELPPANE.EXE	1	9/21/2015 8:04:01 PM			
G2MLAUNCHER.EXE	1	11/30/2016 8:30:12 PM			
G2MUPDATE.EXE	1	4/18/2017 6:50:00 PM			
RUNDLL32.EXE	1	4/20/2017 2:05:18 PM			
57.0.2987.133_56.0.2924.87_CH	1	4/18/2017 5:56:29 PM			
RUNDLL32.EXE	1	9/12/2016 3:43:08 PM			
TASKMGR.EXE	27	3/2/2017 3:32:38 PM	3/1/2017 3:30:04 PM	2/16/2017 5:32:19 PM	10/28/2016 4:30:17
WSHOST.EXE	1	4/20/2017 1:59:12 PM			
THUMBNAILEXTRACTIONHOST.EXE	16	4/20/2017 6:24:10 PM	4/20/2017 6:24:10 PM	4/20/2017 6:24:10 PM	4/20/2017 6:23:20 P
SHTCTKY.EXE	1	4/18/2017 5:55:35 PM			
GOOGLECRASHHANDLER.EXE	1	4/18/2017 11:09:43 PM			
IGFXTRAY.EXE	1	4/20/2017 2:03:31 PM			
SHAREIT320543WW.TMP	1	4/5/2016 12:28:17 PM			
TYPEPERF.EXE	23	4/20/2017 6:23:03 PM	4/20/2017 2:42:49 PM	4/19/2017 1:58:56 AM	4/19/2017 1:18:55 A
REDIRECTOR.EXE	1	4/18/2017 5:56:22 PM			
CSRSS.EXE	3	4/20/2017 6:24:07 PM	4/20/2017 3:01:07 PM	4/20/2017 2:42:48 PM	
RUNDLL32.EXE	1	4/20/2017 2:05:21 PM			
G2MINSTALLER.EXE	1	4/18/2017 6:50:12 PM			
SPPSVC.EXE	3	4/20/2017 6:24:11 PM	4/20/2017 1:59:15 PM	4/18/2017 10:54:20 PM	
CHROME.EXE	1	4/20/2017 2:05:20 PM			
DLLRUNNER32.EXE	2	4/18/2017 6:12:04 PM	4/18/2017 6:05:03 PM		
KASEYATASKRUNNERX64.EXE	5	11/3/2016 7:32:31 PM	11/3/2016 7:32:30 PM	11/1/2016 7:22:41 PM	9/22/2016 3:17:04 P

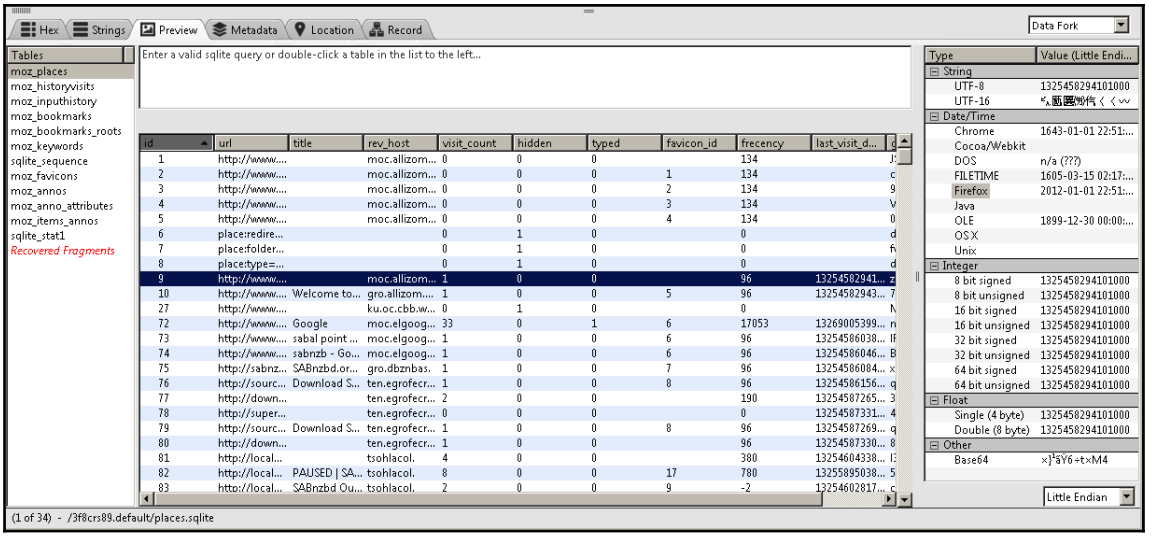


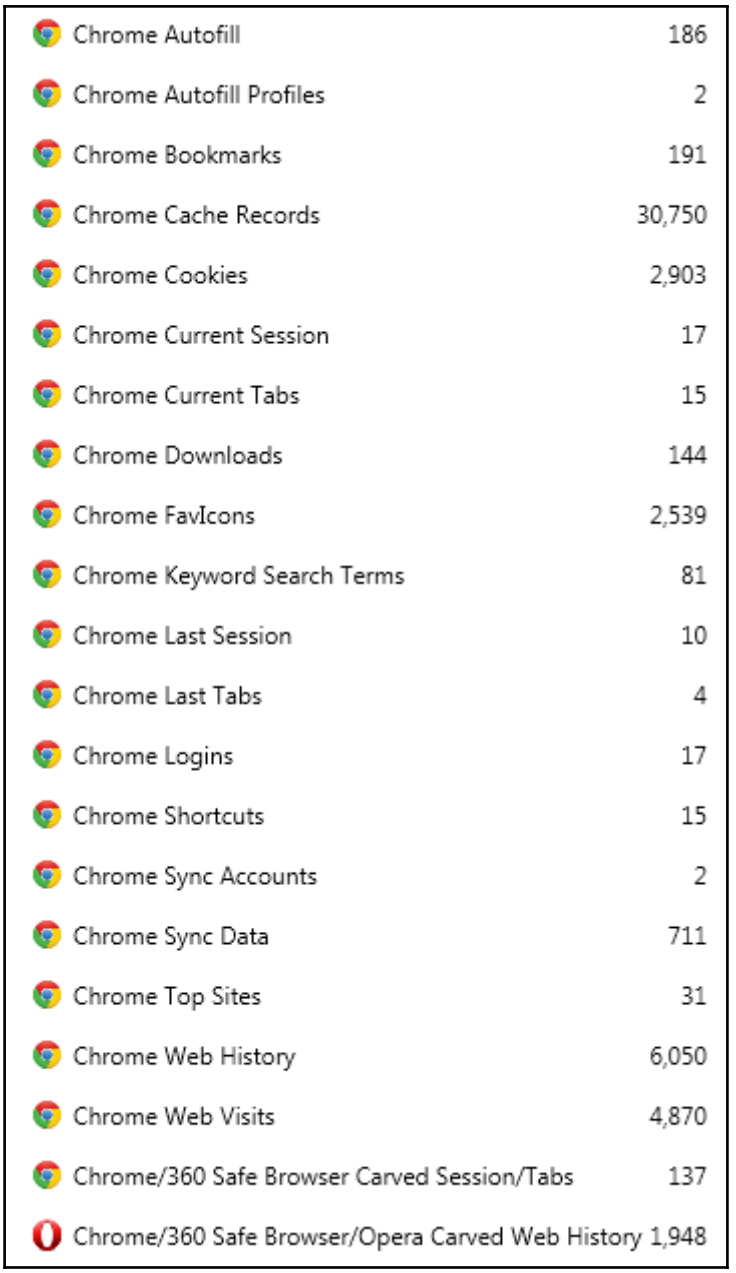

```
2013-03-23 02:06:43.592936 | WMIPRVSE.EXE-1628051c | run_count: 2
2013-03-23 02:07:34.168224 | CONHOST.EXE-1f3e9d7e | run_count: 7
2013-03-23 02:06:46.744143 | VSSVC.EXE-b8afc319 | run_count: 1
2013-03-23 02:07:34.277426 | TASKHOST.EXE-7238f31d | run_count: 5
2013-03-23 02:06:43.405735 | WMIADAP.EXE-f8dfdfa2 | run_count: 1
2013-03-23 02:06:52.796951 | DRVINST.EXE-4cb4314a | run_count: 14
2013-03-23 02:06:45.854940 | NOTEPAD.EXE-d8414f97 | run_count: 1
2013-03-23 02:07:34.152624 | SC.EXE-945d79ae | run_count: 1
2013-03-23 01:57:31.976156 | SVCHOST.EXE-9efc97f2 | run_count: 1
2013-03-23 02:07:34.152624 | SC.EXE-945d79ae | run_count: 1
2013-03-23 02:06:46.931341 | SVCHOST.EXE-7cfedea3 | run_count: 1
2013-03-23 02:07:08.334579 | WUAUCLT.EXE-70318591 | run_count: 2
2013-03-23 02:07:08.240978 | WUSETUPV.EXE-c61614f3 | run_count: 1
```

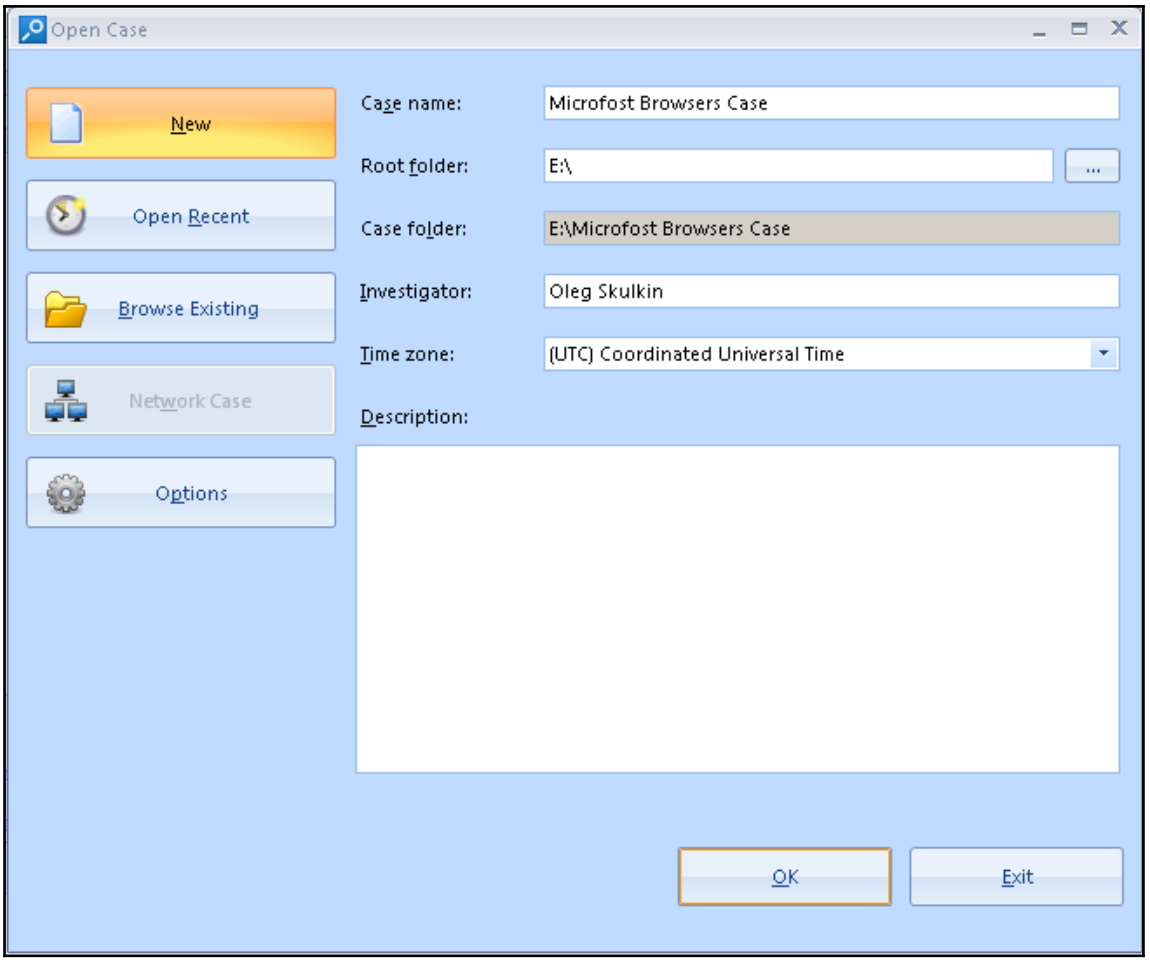
Chapter 8 : Web Browser Forensics

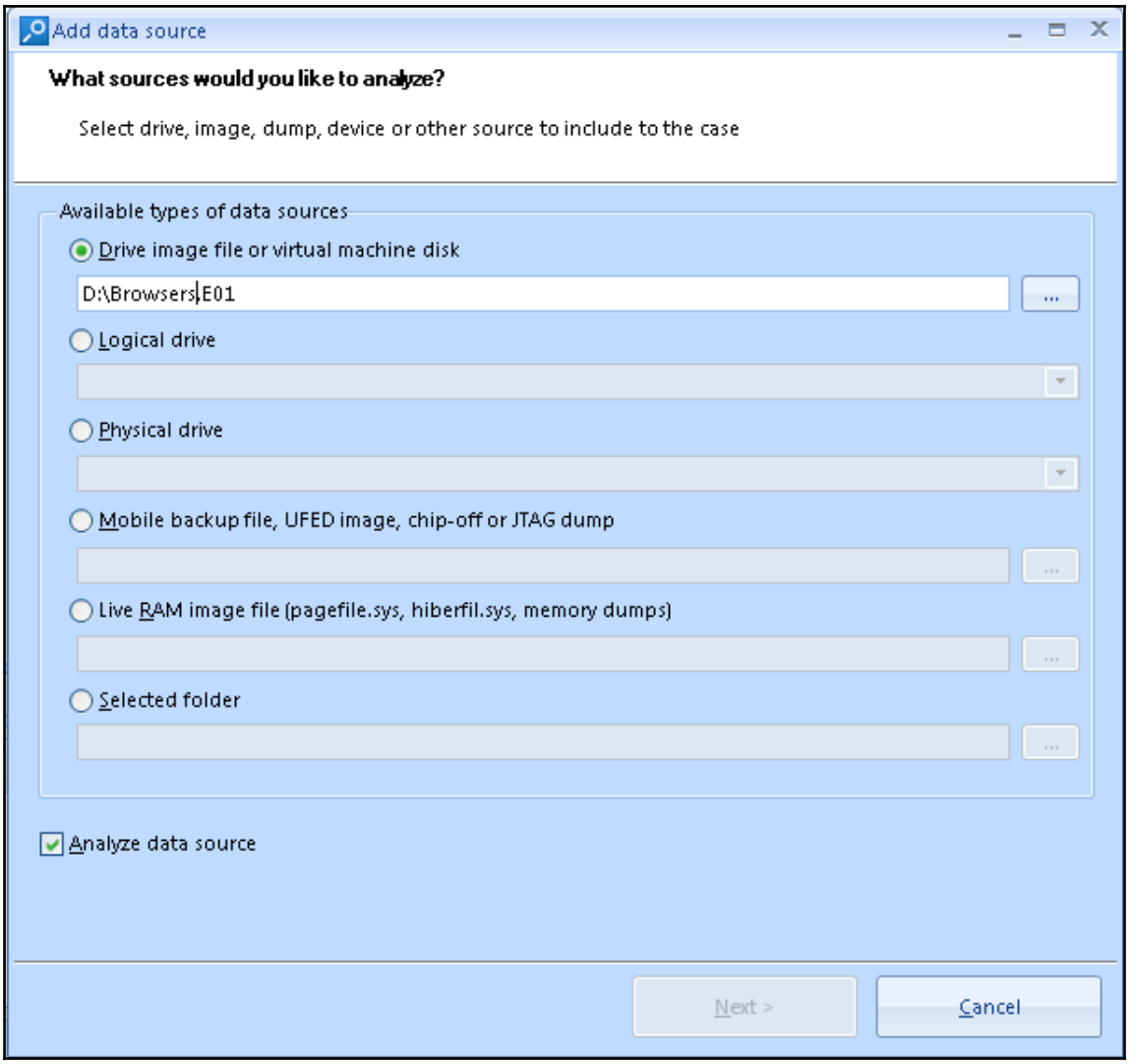


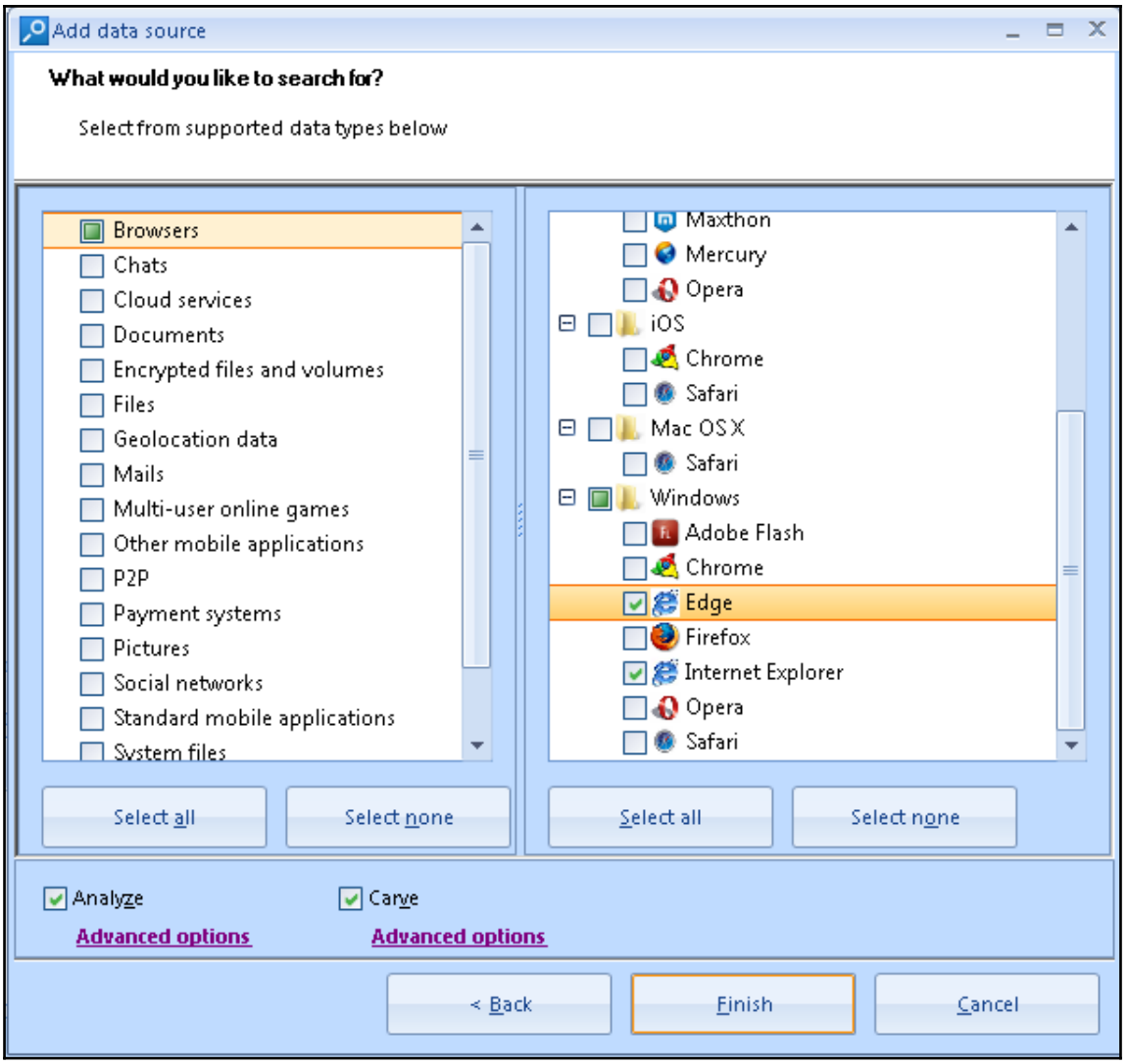

Add Evidence
Attached / Mounted Devices
Disk0 Samsung ...D 850 EVO 1TB
Disk1 WDC WDC...FZEX-00Z4SA0
Disk10 USB DISK 3.0
Disk2 WDC WDC...FZEX-00Z4SA0
Disk3 WDC WDC...FZEX-00Z4SA0
Disk4 WD My Passport 25E2
Disk5 Generic Flash Disk
Disk6 WD My Passport 07B8
Disk7 ST4000D...DM000-2AE166
Disk8 WD My Passport 25E1
Files / Folders / Disk Images
Add
Refresh
Remove
10 items
Cancel
Start

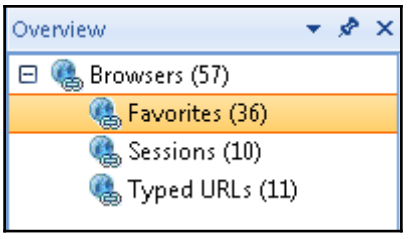

Hex
Strings
Preview
Metadata
Location
Record
Data Fork
Tables
moz_places
moz_historyvisits
moz_inputhistory
moz_bookmarks
moz_bookmarks_roots
moz_keywords
sqlite_sequence
moz_favicons
moz_annos
moz_anno_attributes
moz_items_annos
sqlite_stat1
Recovered Fragments
Enter a valid sqlite query or double-click a table in the list to the left...
id
url
title
rev_host
visit_count
hidden
typed
favicon_id
frecency
last_visit_d...
Type
Value (Little Endi...
String
UTF-8
UTF-16
Date/Time
Chrome
Cocoa/Webkit
DOS
FILETIME
Firefox
Java
OLE
OS X
Unix
Integer
8 bit signed
8 bit unsigned
16 bit signed
16 bit unsigned
32 bit signed
32 bit unsigned
64 bit signed
64 bit unsigned
Float
Single (4 byte)
Double (8 byte)
Other
Base64
Little Endian
(1 of 34) - /3f8crs89.default/places.sqlite

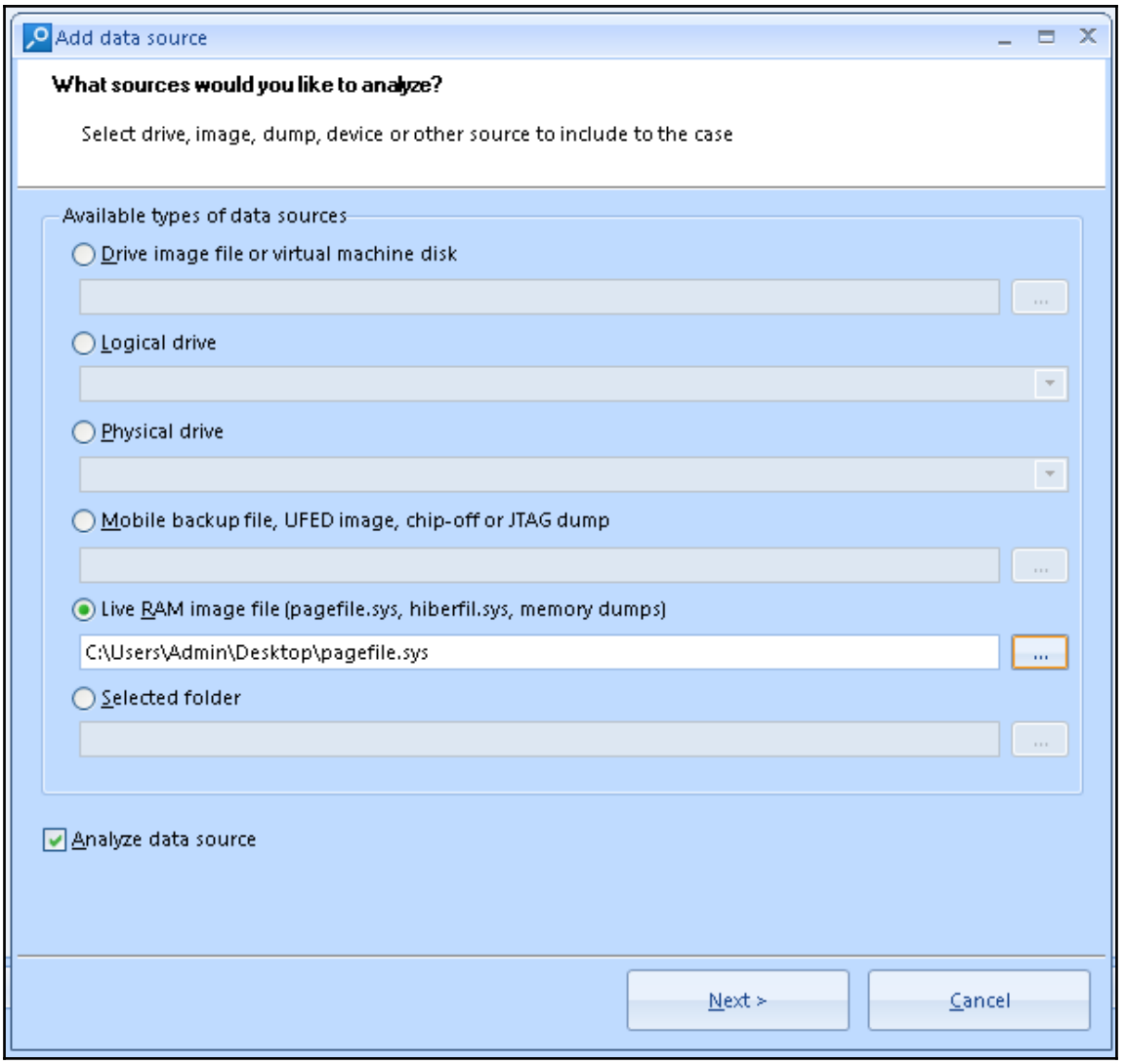

Chrome Autofill 186
Chrome Autofill Profiles 2
Chrome Bookmarks 191
Chrome Cache Records 30,750
Chrome Cookies 2,903
Chrome Current Session 17
Chrome Current Tabs 15
Chrome Downloads 144
Chrome FavIcons 2,539
Chrome Keyword Search Terms 81
Chrome Last Session 10
Chrome Last Tabs 4
Chrome Logins 17
Chrome Shortcuts 15
Chrome Sync Accounts 2
Chrome Sync Data 711
Chrome Top Sites 31
Chrome Web History 6,050
Chrome Web Visits 4,870
Chrome/360 Safe Browser Carved Session/Tabs 137
Chrome/360 Safe Browser/Opera Carved Web History 1,948

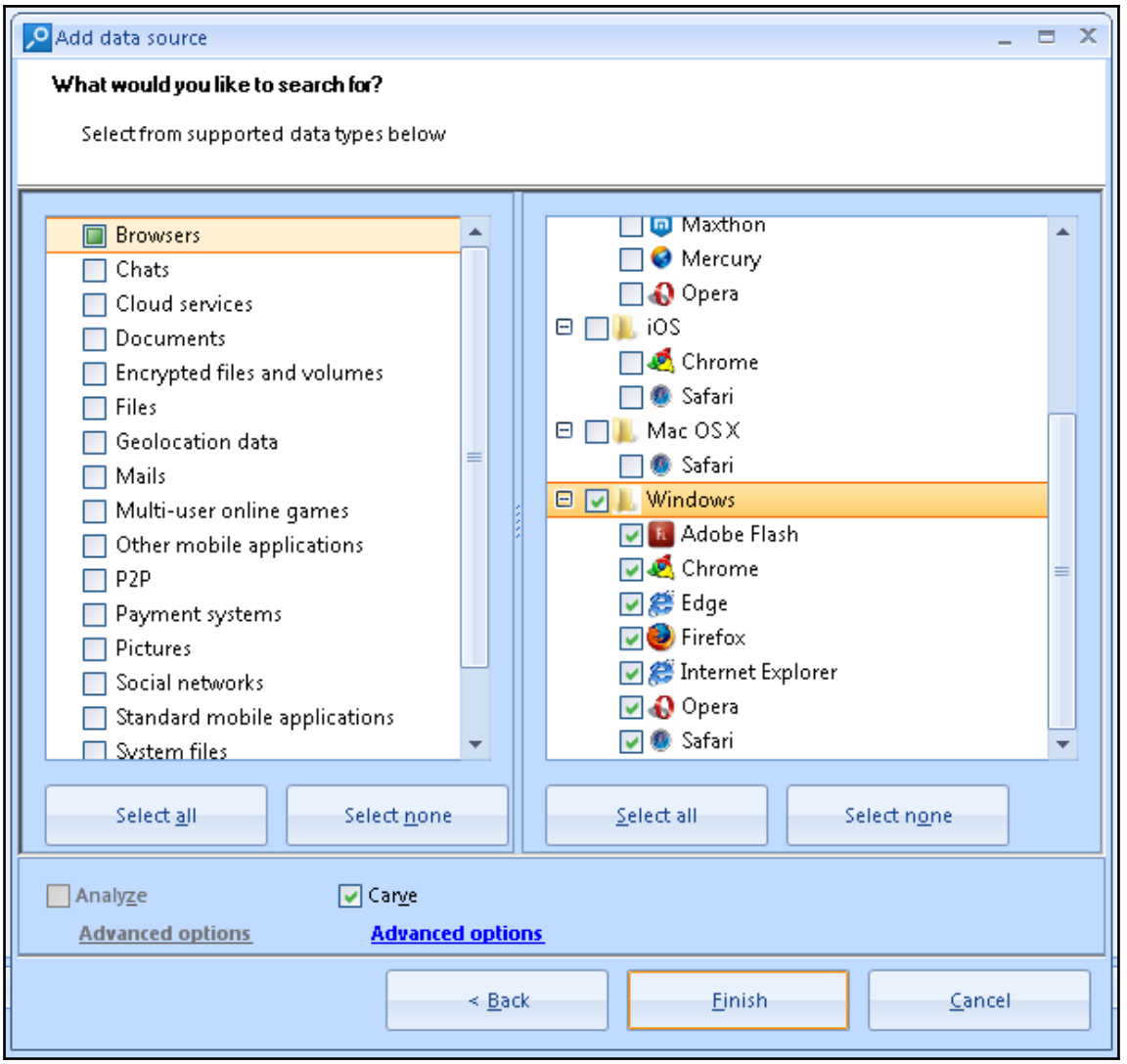

Open Case
New
Open Recent
Browse Existing
Network Case
Options
Case name:
Microfost Browsers Case
Root folder:
E:\
...
Case folder:
E:\Microfost Browsers Case
Investigator:
Oleg Skulkin
Time zone:
(UTC) Coordinated Universal Time
Description:
OK
Exit

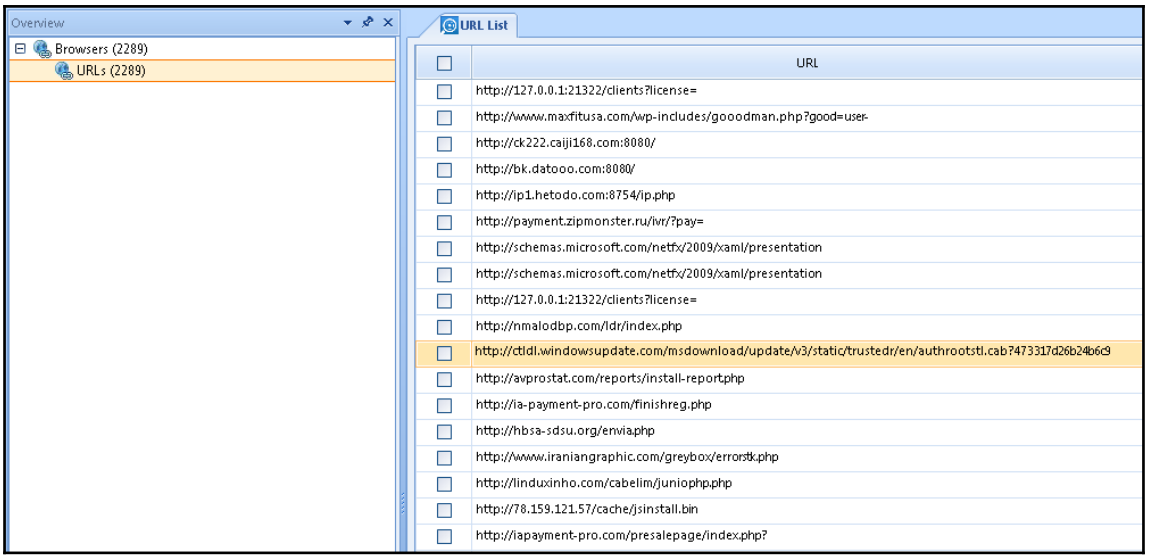

Add data source
What sources would you like to analyze?
Select drive, image, dump, device or other source to include to the case
Available types of data sources
Drive image file or virtual machine disk
D:\Browsers\E01
...
Logical drive
Physical drive
Mobile backup file, UFED image, chip-off or JTAG dump
Live RAM image file (pagefile.sys, hiberfil.sys, memory dumps)
Selected folder
Analyze data source
Next >
Cancel


Add data source
What would you like to search for?
Select from supported data types below
Browsers
Chats
Cloud services
Documents
Encrypted files and volumes
Files
Geolocation data
Mails
Multi-user online games
Other mobile applications
P2P
Payment systems
Pictures
Social networks
Standard mobile applications
System files
Maxthon
Mercury
Opera
iOS
Chrome
Safari
Mac OS X
Safari
Windows
Adobe Flash
Chrome
Edge
Firefox
Internet Explorer
Opera
Safari
Select all
Select none
Select all
Select none
Analyze
Advanced options
Carve
Advanced options
< Back
Finish
Cancel

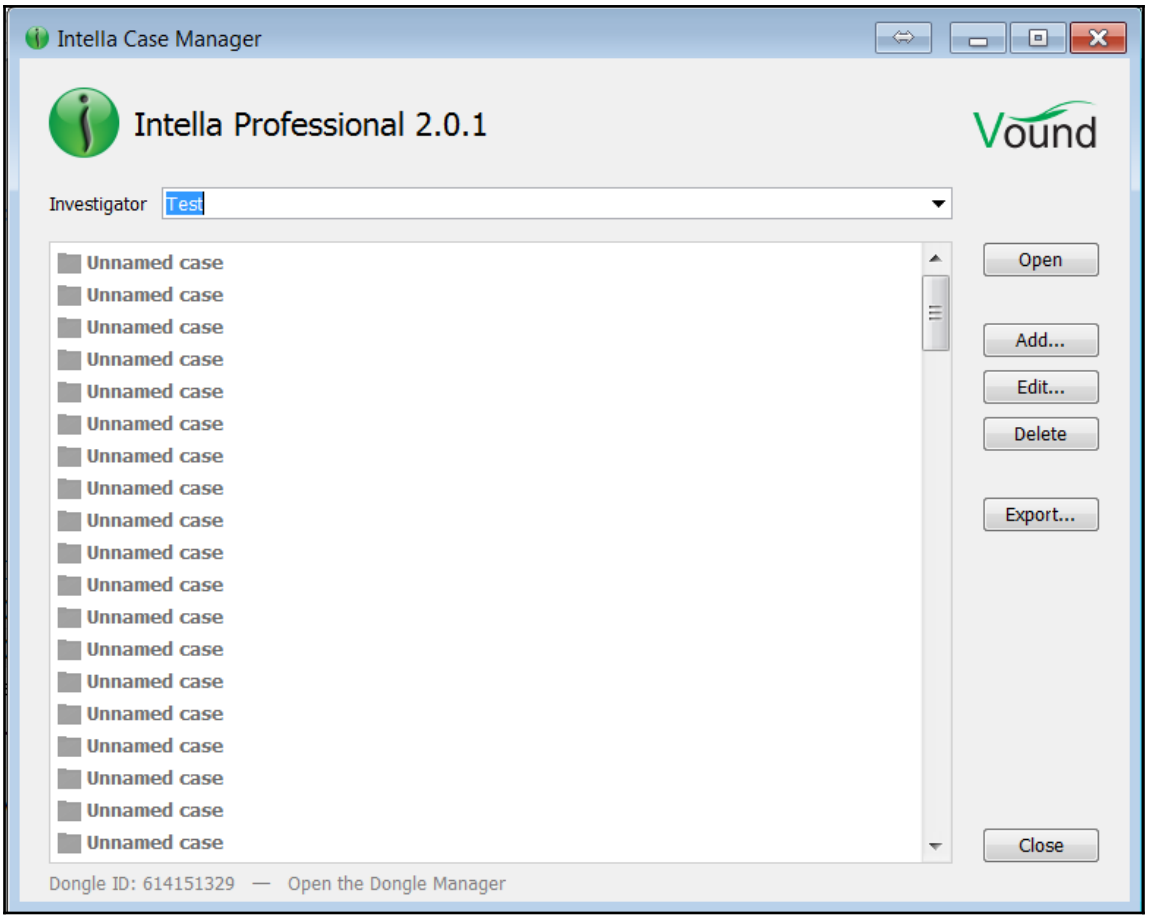

Overview
Browsers (57)
Favorites (36)
Sessions (10)
Typed URLs (11)

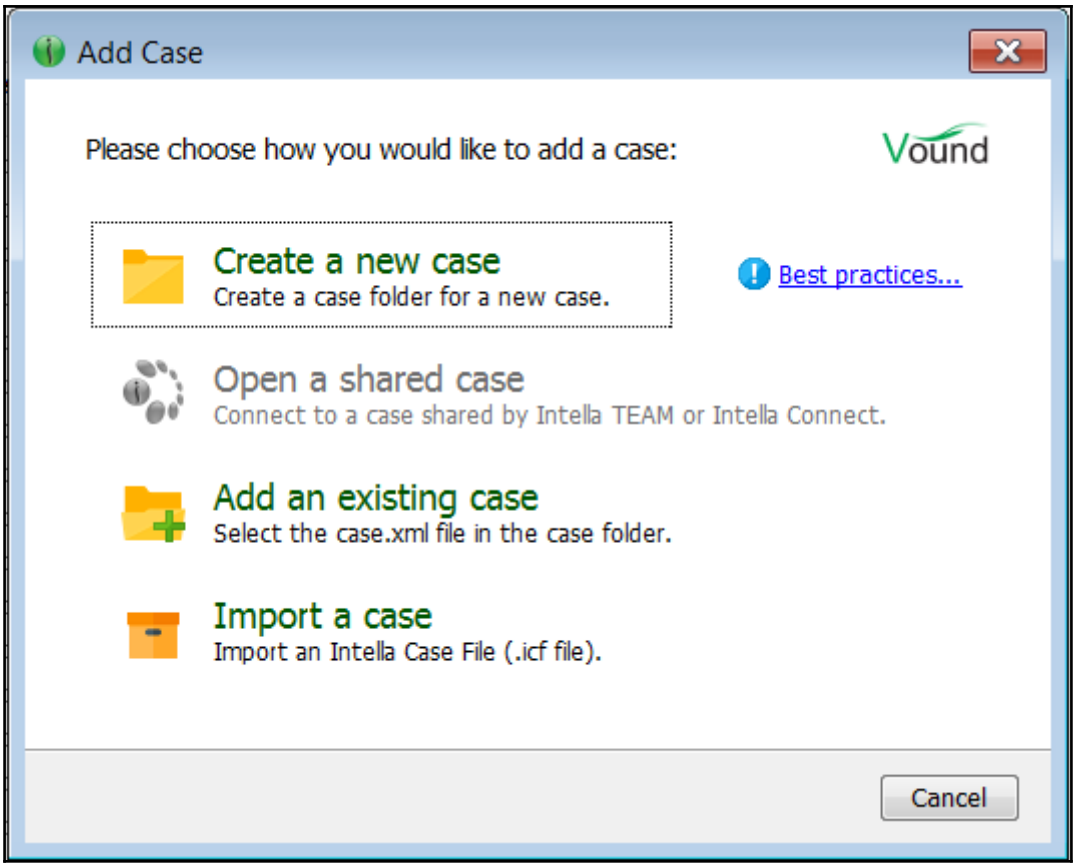

Add data source
What sources would you like to analyze?
Select drive, image, dump, device or other source to include to the case
Available types of data sources
Drive image file or virtual machine disk
Logical drive
Physical drive
Mobile backup file, UFED image, chip-off or JTAG dump
Live RAM image file (pagefile.sys, hiberfil.sys, memory dumps)
C:\Users\Admin\Desktop\pagefile.sys
Selected folder
Analyze data source
Next >
Cancel

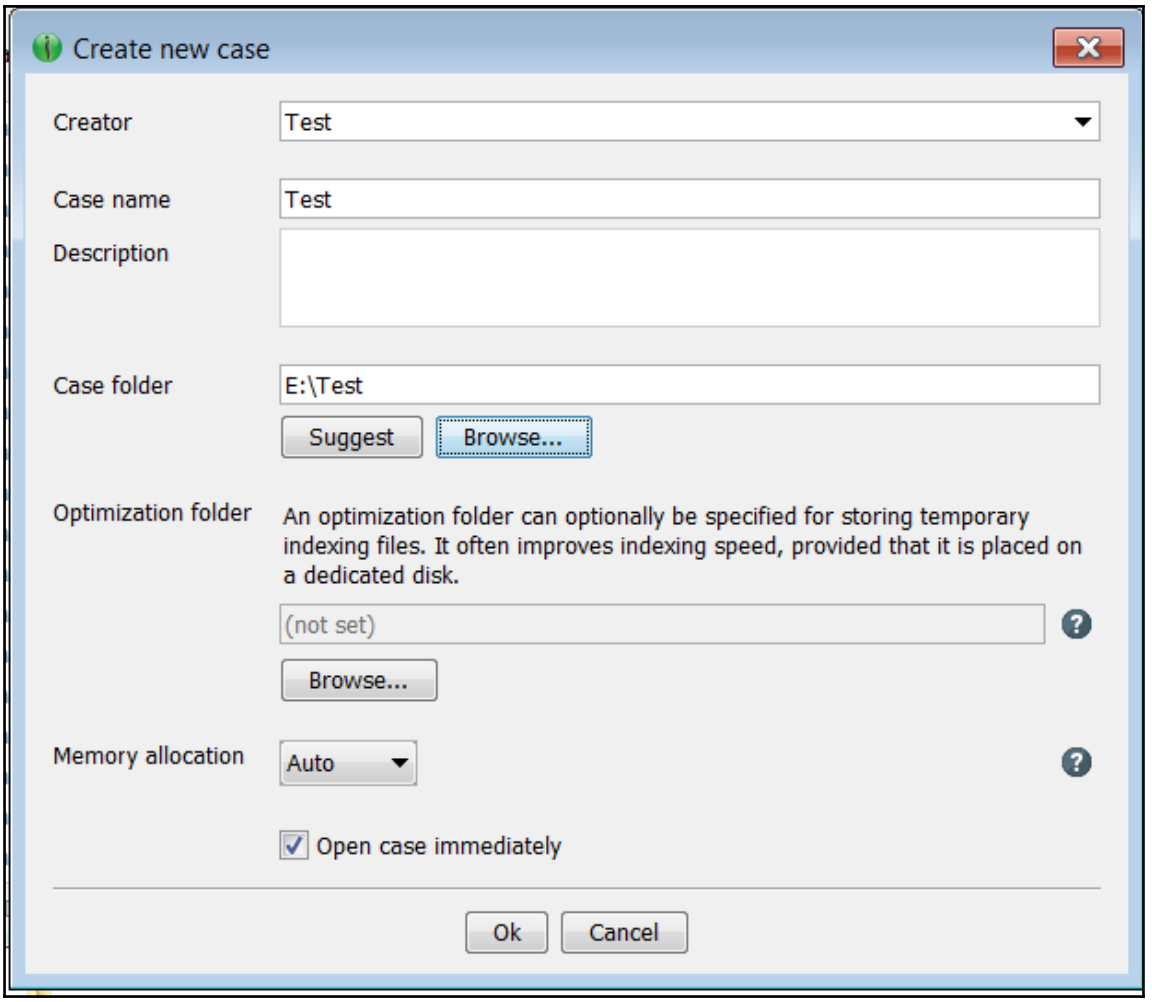

Add data source
What would you like to search for?
Select from supported data types below
Browsers
Chats
Cloud services
Documents
Encrypted files and volumes
Files
Geolocation data
Mails
Multi-user online games
Other mobile applications
P2P
Payment systems
Pictures
Social networks
Standard mobile applications
System files
Maxthon
Mercury
Opera
iOS
Chrome
Safari
Mac OS X
Safari
Windows
Adobe Flash
Chrome
Edge
Firefox
Internet Explorer
Opera
Safari
Select all
Select none
Select all
Select none
Analyze
Advanced options
Carve
Advanced options
< Back
Finish
Cancel

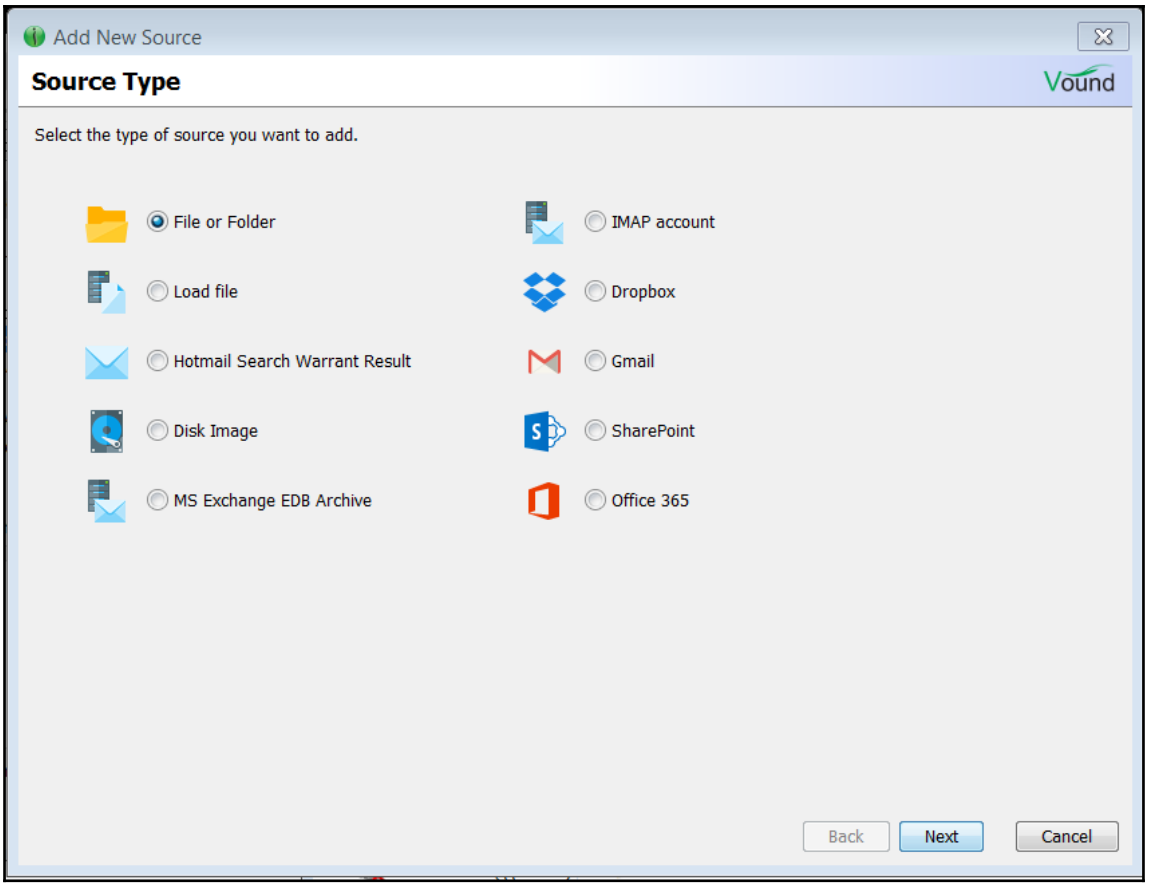


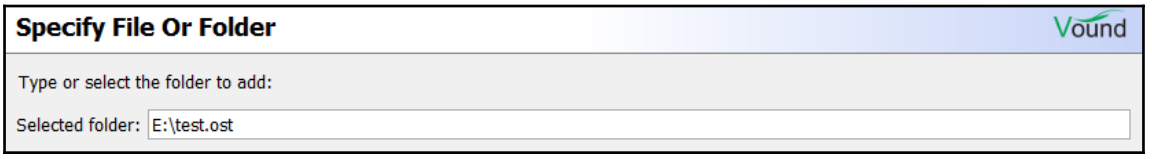
Chapter 9 : Email and Instant Messaging Forensics

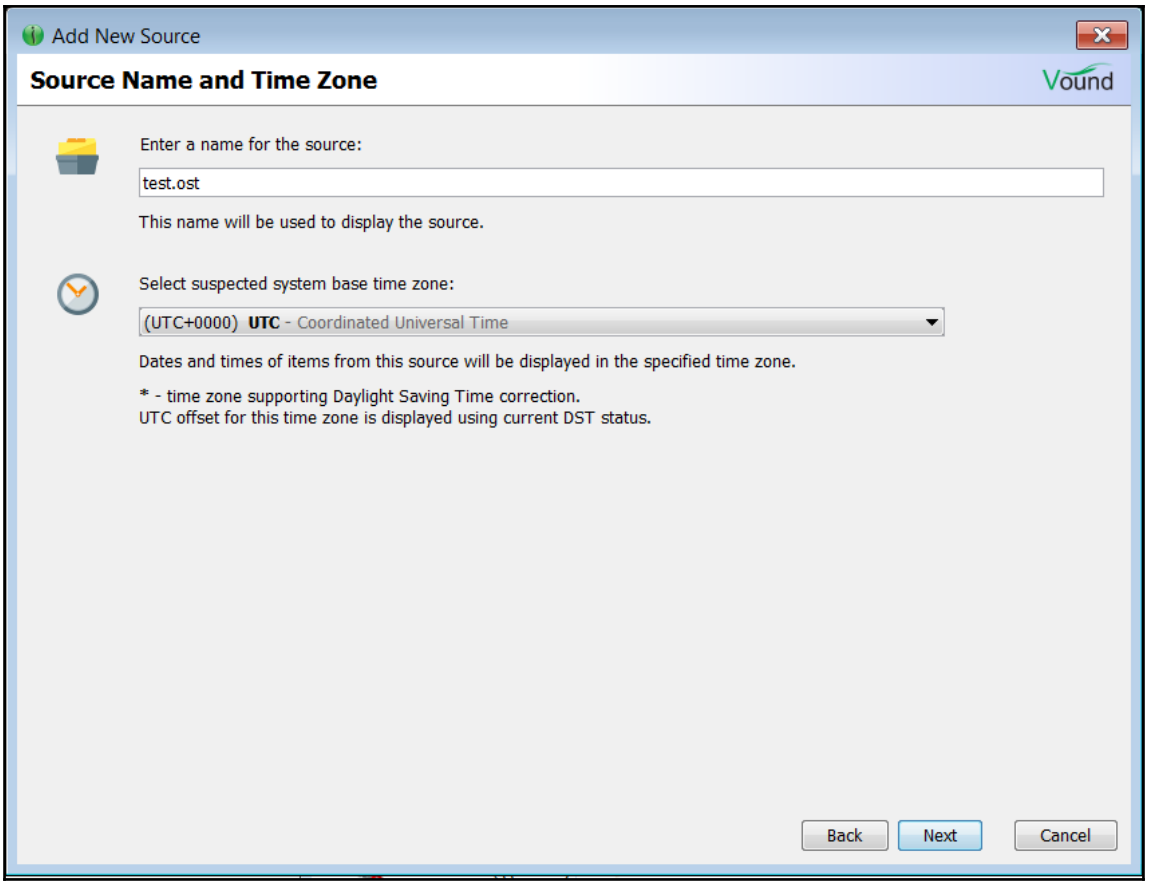

Intella Case Manager
Intella Professional 2.0.1
Vound
Investigator
Test
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Open
Add...
Edit...
Delete
Export...
Close
Dongle ID: 614151329 — Open the Dongle Manager

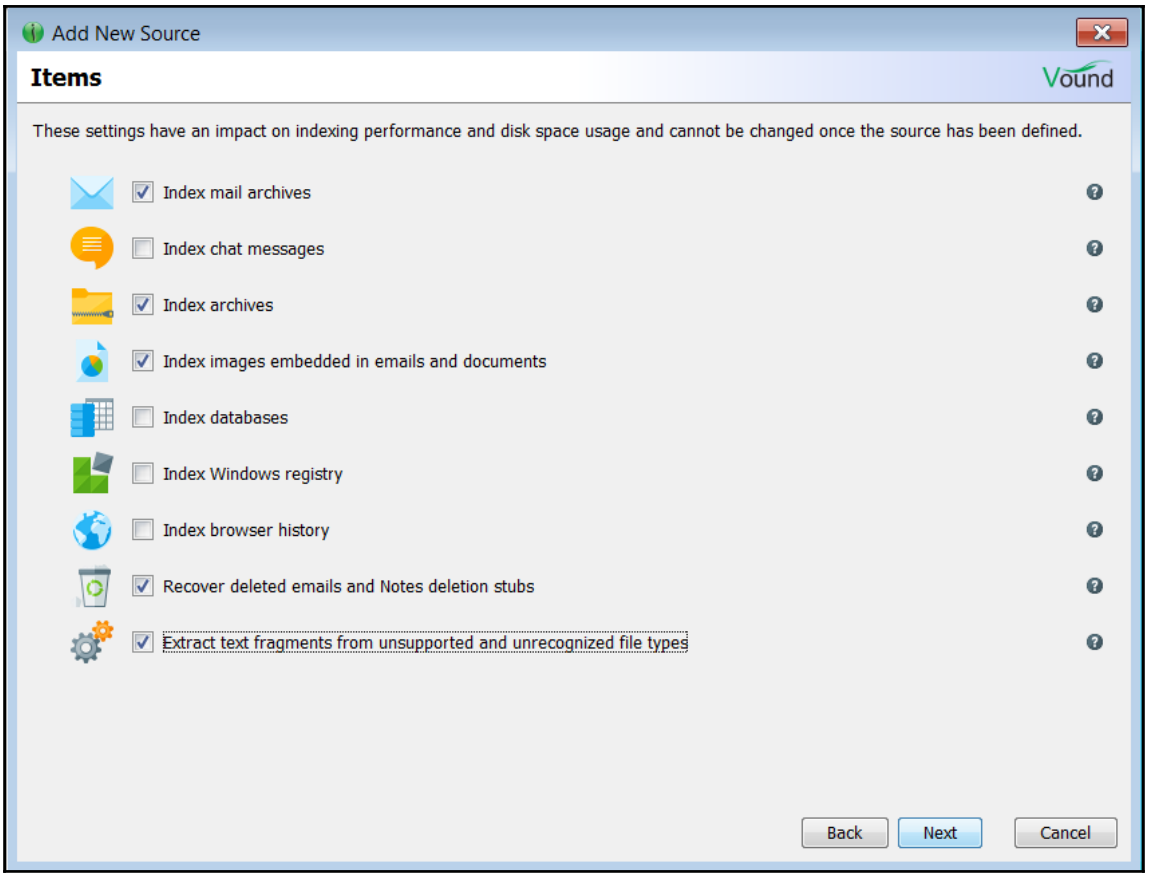

Add Case
Please choose how you would like to add a case:
Vound
Create a new case
Create a case folder for a new case.
Best practices...
Open a shared case
Connect to a case shared by Intella TEAM or Intella Connect.
Add an existing case
Select the case.xml file in the case folder.
Import a case
Import an Intella Case File (.icf file).
Cancel

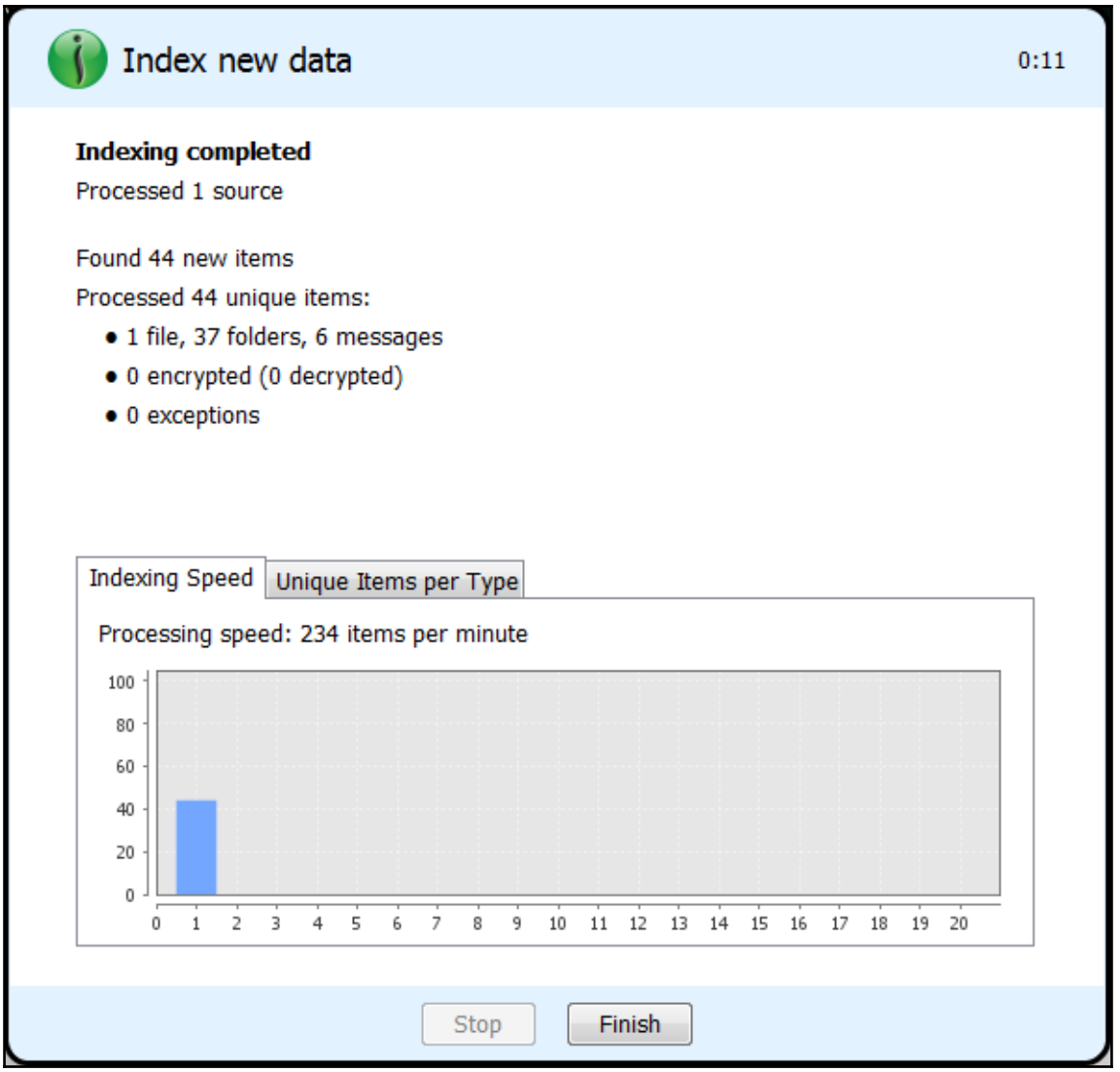

Create new case
Creator
Test
Case name
Test
Description
Case folder
E:\Test
Suggest
Browse...
Optimization folder
An optimization folder can optionally be specified for storing temporary indexing files. It often improves indexing speed, provided that it is placed on a dedicated disk.
(not set)
Browse...
Memory allocation
Auto
Open case immediately
Ok
Cancel

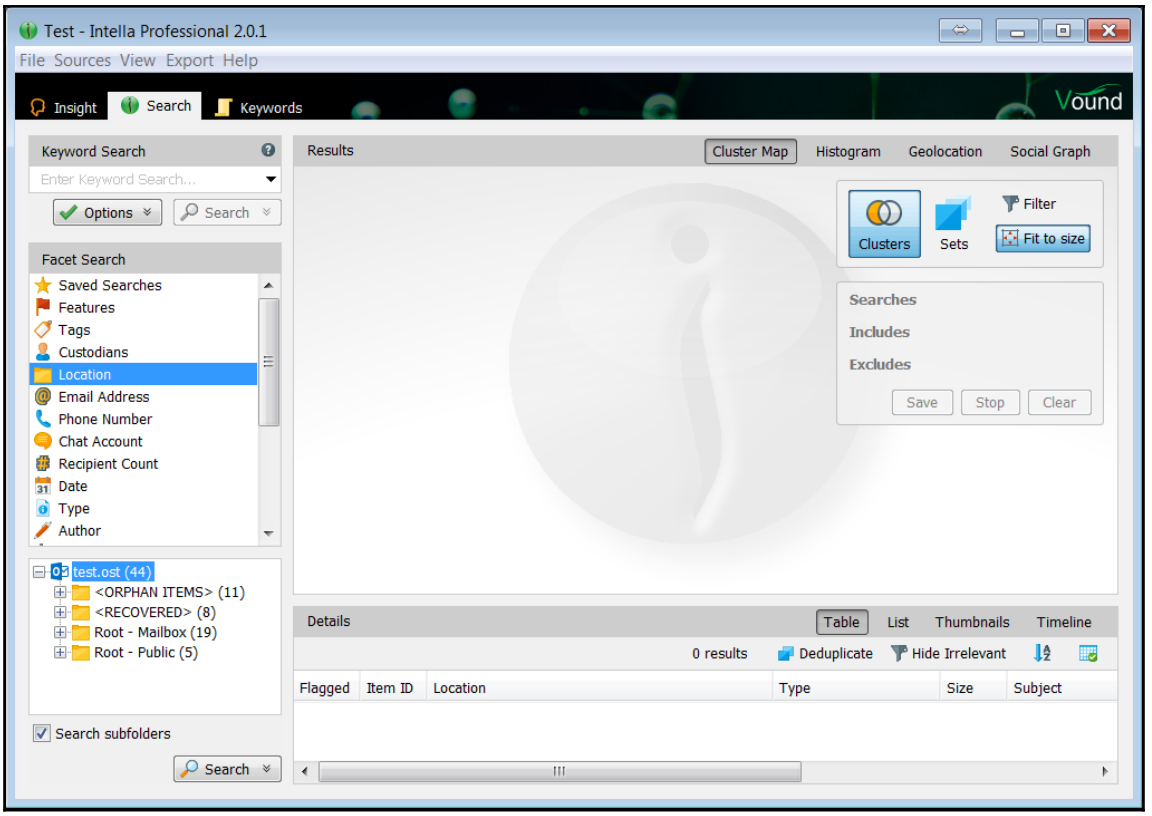

Add New Source
Source Type
Vound
Select the type of source you want to add.
File or Folder
IMAP account
Load file
Dropbox
Hotmail Search Warrant Result
Gmail
Disk Image
SharePoint
MS Exchange EDB Archive
Office 365
Back
Next
Cancel

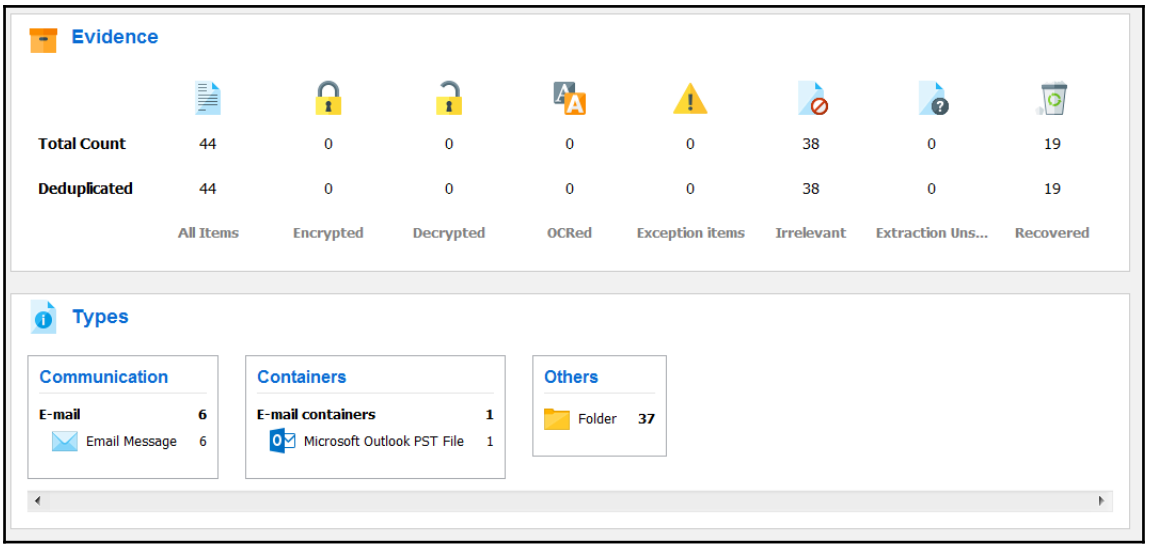

Specify File Or Folder
Vound
Type or select the folder to add:
Selected folder:
E:\test.ost

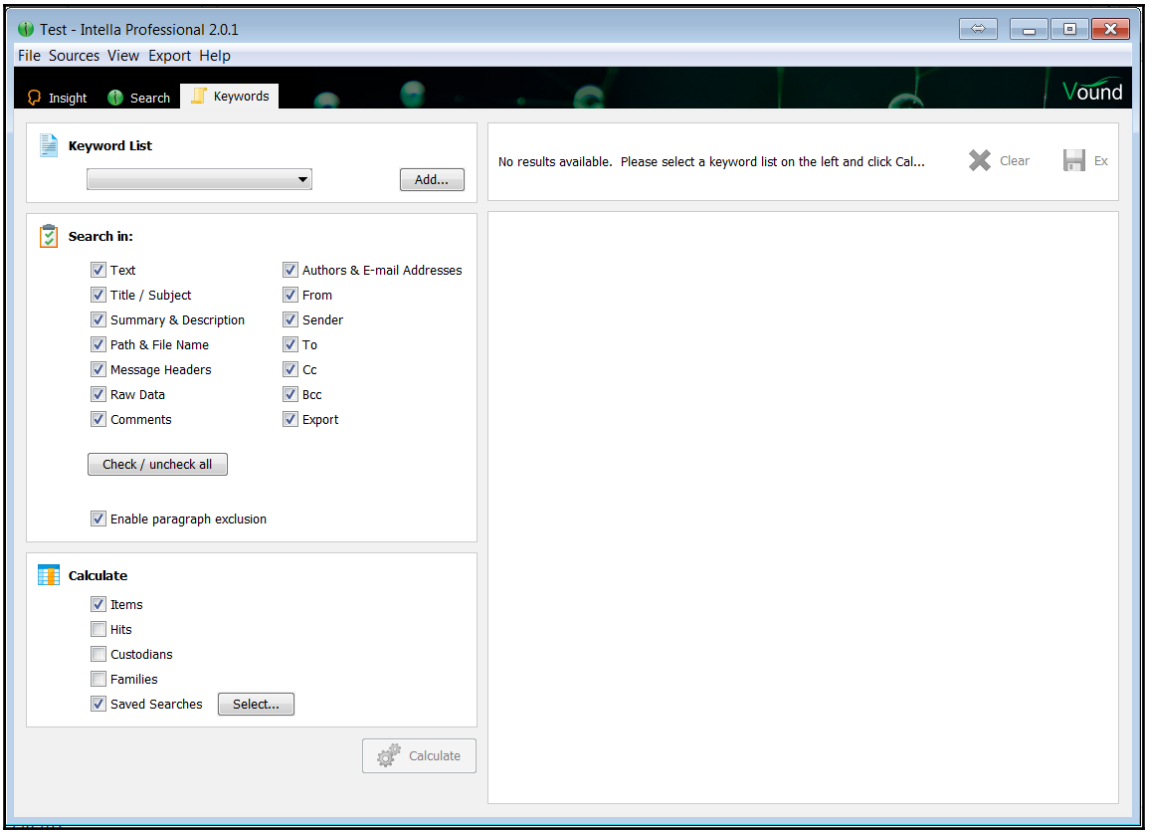

Add New Source
Source Name and Time Zone
Vound
Enter a name for the source:
test.ost
This name will be used to display the source.
Select suspected system base time zone:
(UTC+0000) UTC - Coordinated Universal Time
Dates and times of items from this source will be displayed in the specified time zone.
* - time zone supporting Daylight Saving Time correction.
UTC offset for this time zone is displayed using current DST status.
Back
Next
Cancel

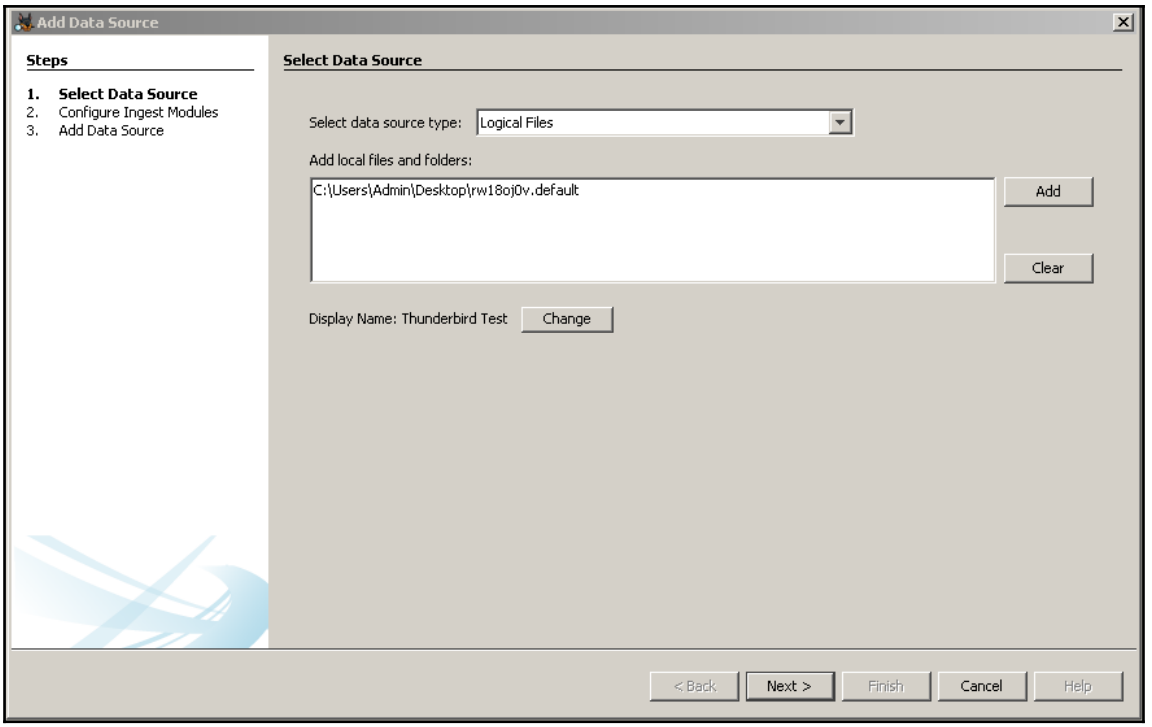

Add New Source
Items
Vound
These settings have an impact on indexing performance and disk space usage and cannot be changed once the source has been defined.
Index mail archives
Index chat messages
Index archives
Index images embedded in emails and documents
Index databases
Index Windows registry
Index browser history
Recover deleted emails and Notes deletion stubs
Extract text fragments from unsupported and unrecognized file types
Back
Next
Cancel

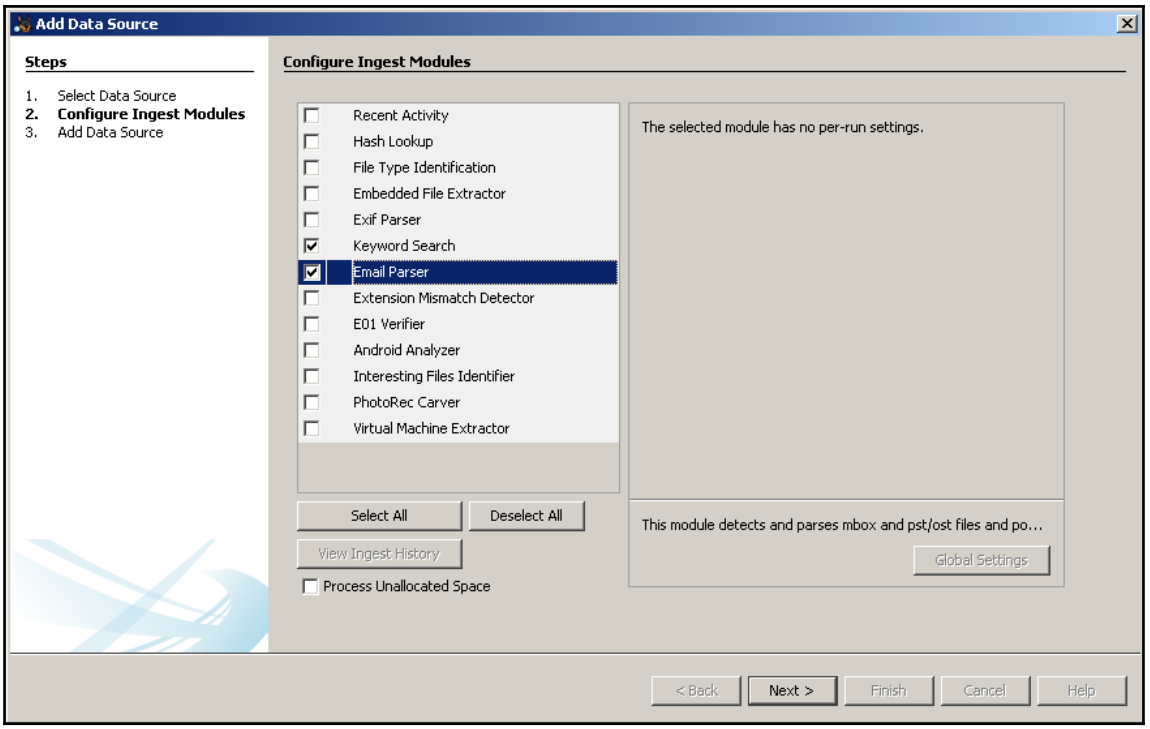

Index new data
0:11
Indexing completed
Processed 1 source
Found 44 new items
Processed 44 unique items:
• 1 file, 37 folders, 6 messages
• 0 encrypted (0 decrypted)
• 0 exceptions
Indexing Speed
Unique Items per Type
Processing speed: 234 items per minute
100
80
60
40
20
0
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
Stop
Finish

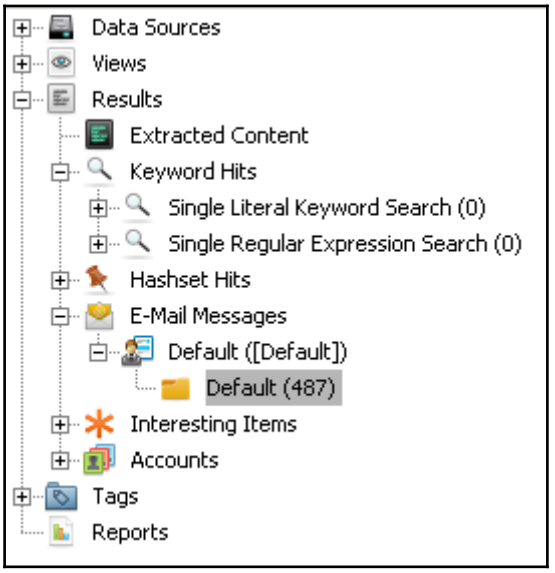

Test - Intella Professional 2.0.1
File Sources View Export Help
Insight
Search
Keywords
Vound
Keyword Search
Enter Keyword Search...
Options
Search
Facet Search
Saved Searches
Features
Tags
Custodians
Location
Email Address
Phone Number
Chat Account
Recipient Count
Date
Type
Author
test.ost (44)
<ORPHAN ITEMS> (11)
<RECOVERED> (8)
Root - Mailbox (19)
Root - Public (5)
Search subfolders
Search
Results
Cluster Map
Histogram
Geolocation
Social Graph
Clusters
Sets
Filter
Fit to size
Searches
Includes
Excludes
Save
Stop
Clear
Details
Table
List
Thumbnails
Timeline
0 results
Deduplicate
Hide Irrelevant
Flagged
Item ID
Location
Type
Size
Subject

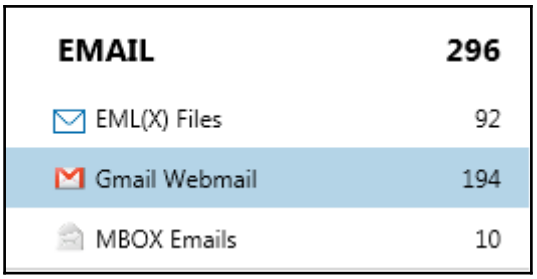

Evidence
Total Count 44 0 0 0 0 38 0 19
Deduplicated 44 0 0 0 0 38 0 19
All Items
Encrypted
Decrypted
OCRed
Exception items
Irrelevant
Extraction Uns...
Recovered
Types
Communication
E-mail 6
Email Message 6
Containers
E-mail containers 1
Microsoft Outlook PST File 1
Others
Folder 37

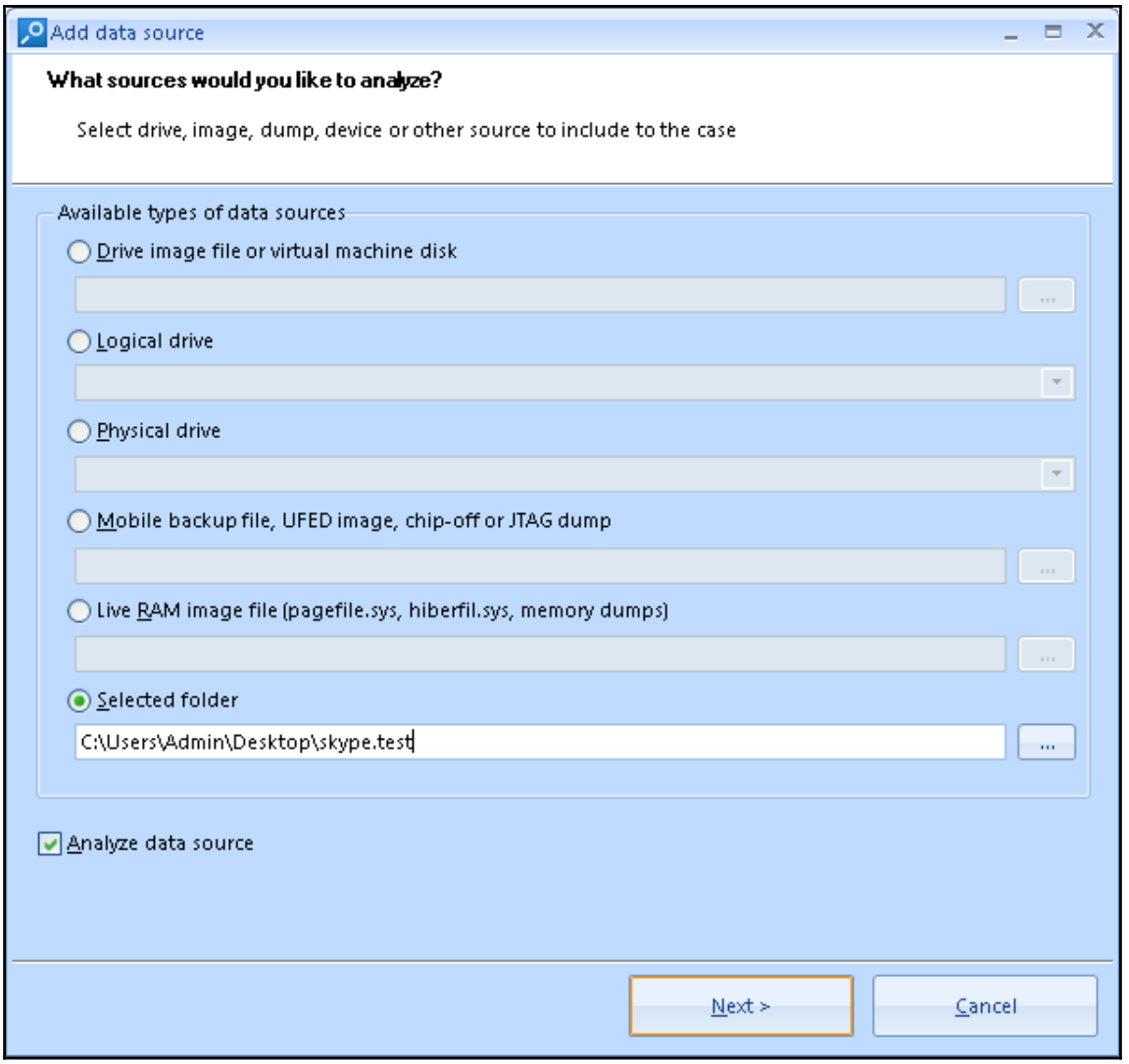

Test - Intella Professional 2.0.1
File Sources View Export Help
Insight
Search
Keywords
Vound
Keyword List
Add...
No results available. Please select a keyword list on the left and click Cal...
Clear
Ex
Search in:
Text
Title / Subject
Summary & Description
Path & File Name
Message Headers
Raw Data
Comments
Authors & E-mail Addresses
From
Sender
To
Cc
Bcc
Export
Check / uncheck all
Enable paragraph exclusion
Calculate
Items
Hits
Custodians
Families
Saved Searches
Select...
Calculate

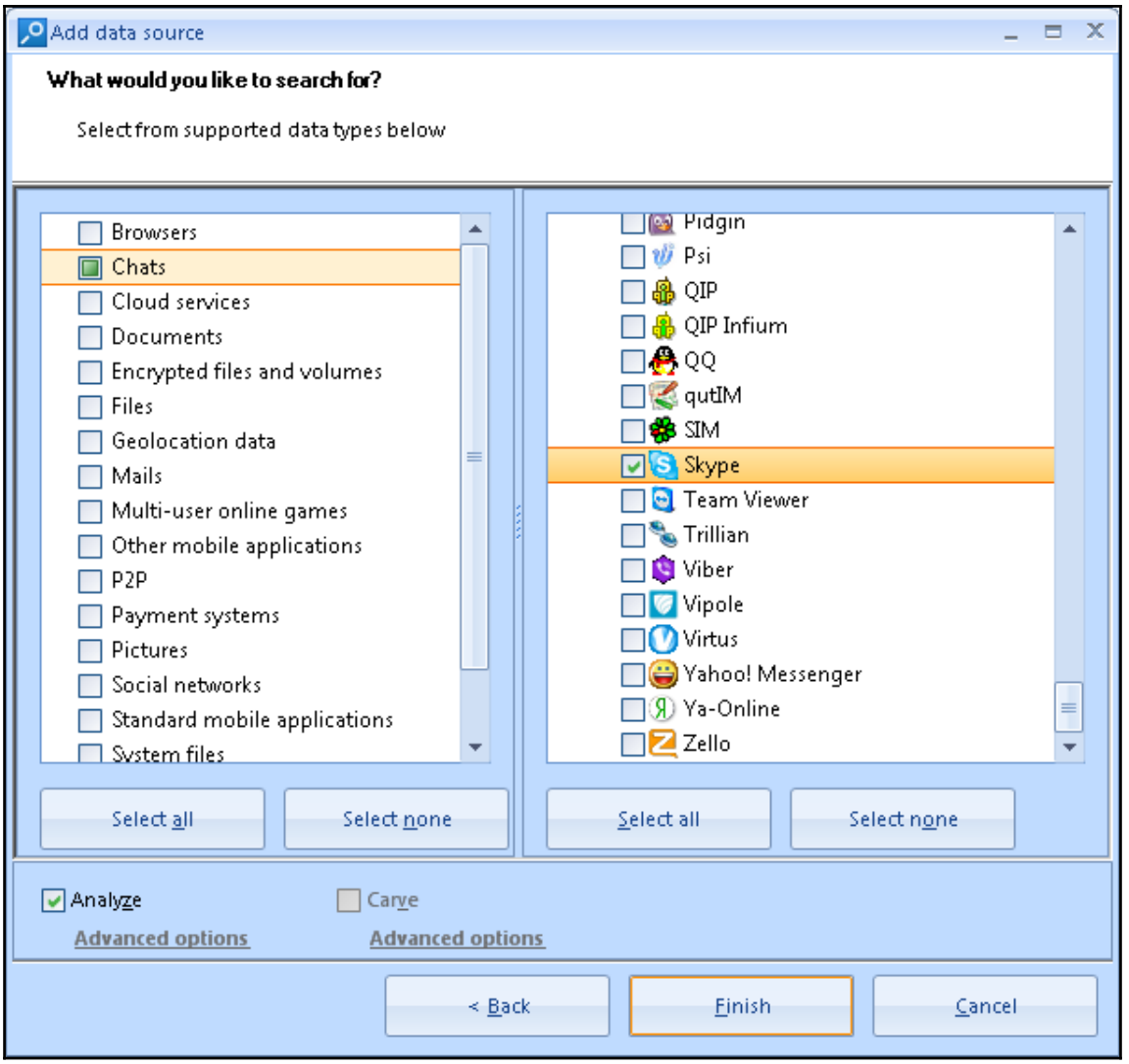

Add Data Source
Steps
1. Select Data Source
2. Configure Ingest Modules
3. Add Data Source
Select Data Source
Select data source type:
Logical Files
Add local files and folders:
C:\Users\Admin\Desktop\rw18oj0v.default
Add
Clear
Display Name: Thunderbird Test
Change
< Back
Next >
Finish
Cancel
Help

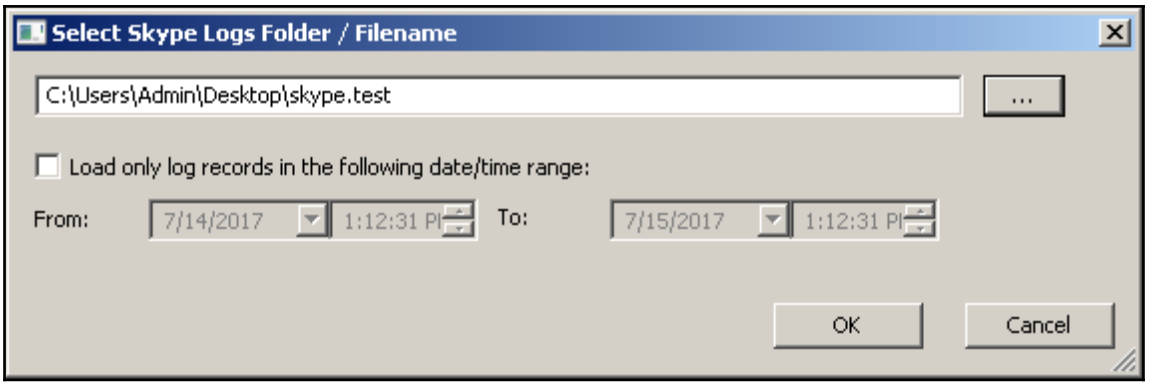

Add Data Source
Steps
1. Select Data Source
2. Configure Ingest Modules
3. Add Data Source
Configure Ingest Modules
Recent Activity
Hash Lookup
File Type Identification
Embedded File Extractor
Exif Parser
Keyword Search
Email Parser
Extension Mismatch Detector
E01 Verifier
Android Analyzer
Interesting Files Identifier
PhotoRec Carver
Virtual Machine Extractor
The selected module has no per-run settings.
Select All
Deselect All
View Ingest History
Process Unallocated Space
This module detects and parses mbox and pst/ost files and po...
Global Settings
< Back
Next >
Finish
Cancel
Help

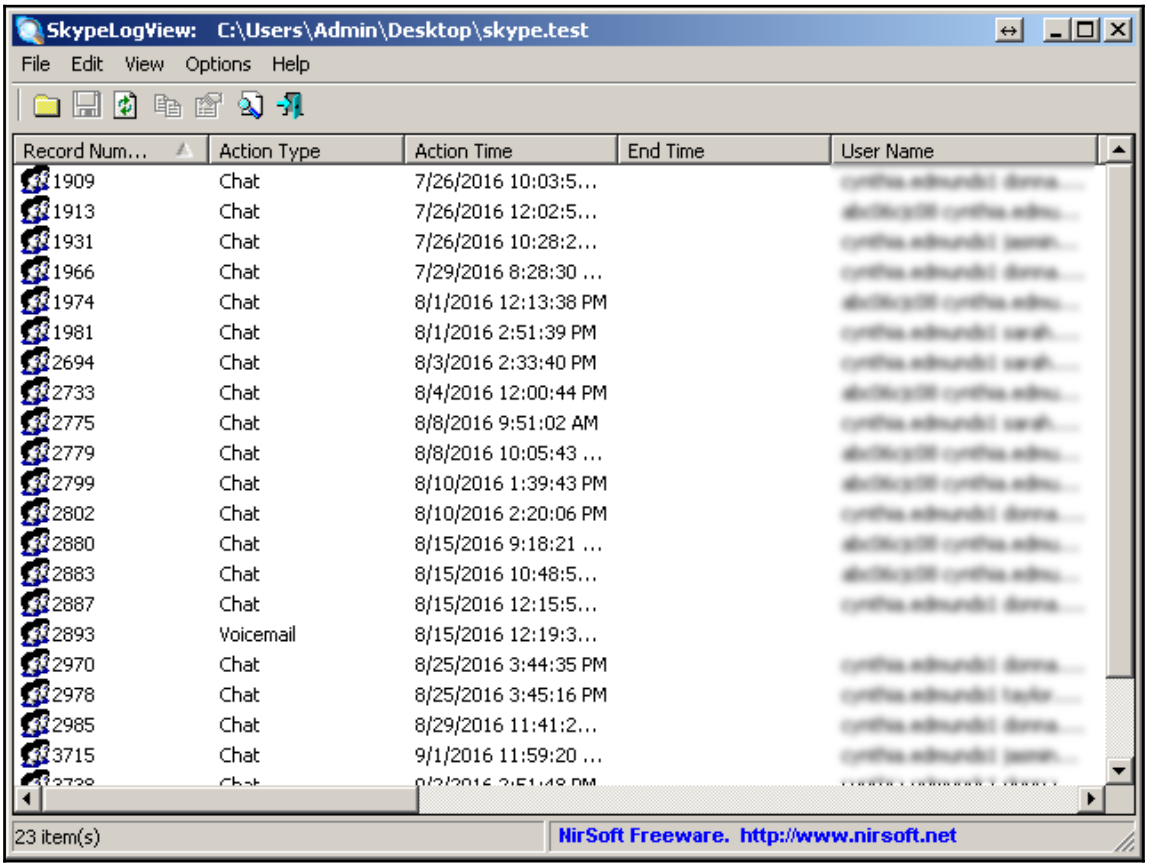

Data Sources
Views
Results
Extracted Content
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Hashset Hits
E-Mail Messages
Default ([Default])
Default (487)
Interesting Items
Accounts
Tags
Reports


EMAIL
296
EML(X) Files
92
Gmail Webmail
194
MBOX Emails
10

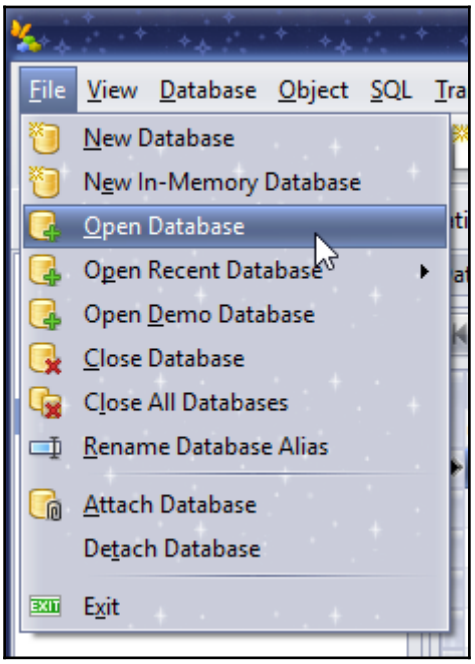

Add data source
What sources would you like to analyze?
Select drive, image, dump, device or other source to include to the case
Available types of data sources
Drive image file or virtual machine disk
Logical drive
Physical drive
Mobile backup file, UFED image, chip-off or JTAG dump
Live RAM image file (pagefile.sys, hiberfil.sys, memory dumps)
Selected folder
C:\Users\Admin\Desktop\skype.test
Analyze data source
Next >
Cancel

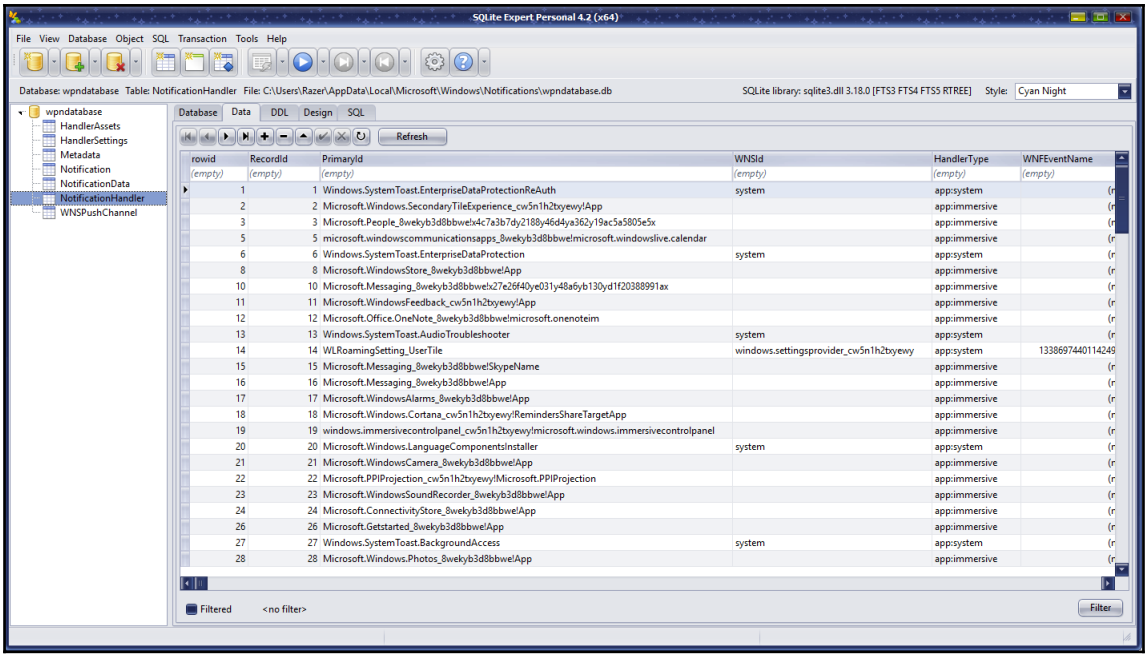

Add data source
What would you like to search for?
Select from supported data types below
Browsers
Chats
Cloud services
Documents
Encrypted files and volumes
Files
Geolocation data
Mails
Multi-user online games
Other mobile applications
P2P
Payment systems
Pictures
Social networks
Standard mobile applications
System files
Pidgin
Psi
QIP
QIP Infium
QQ
qutIM
SIM
Skype
Team Viewer
Trillian
Viber
Vipole
Virtus
Yahoo! Messenger
Ya-Online
Zello
Select all
Select none
Select all
Select none
Analyze
Advanced options
Carve
Advanced options
< Back
Finish
Cancel

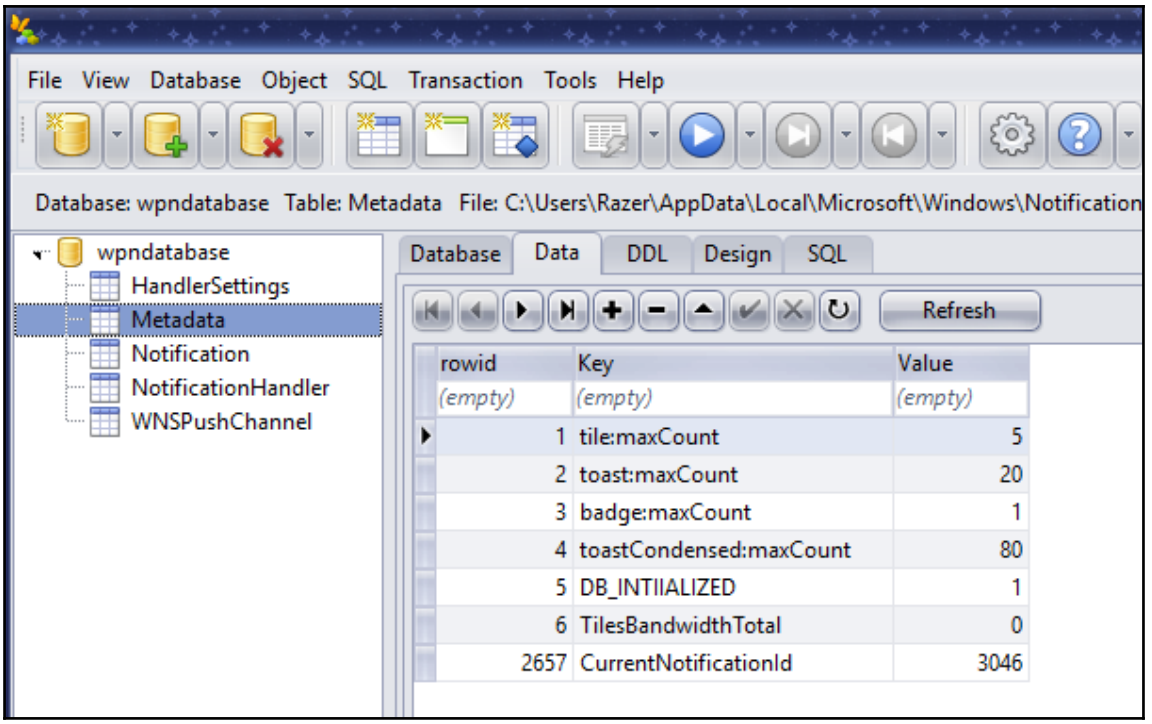

Select Skype Logs Folder / Filename
C:\Users\Admin\Desktop\skype.test
...
Load only log records in the following date/time range:
From:
7/14/2017
1:12:31 PM
To:
7/15/2017
1:12:31 PM
OK
Cancel

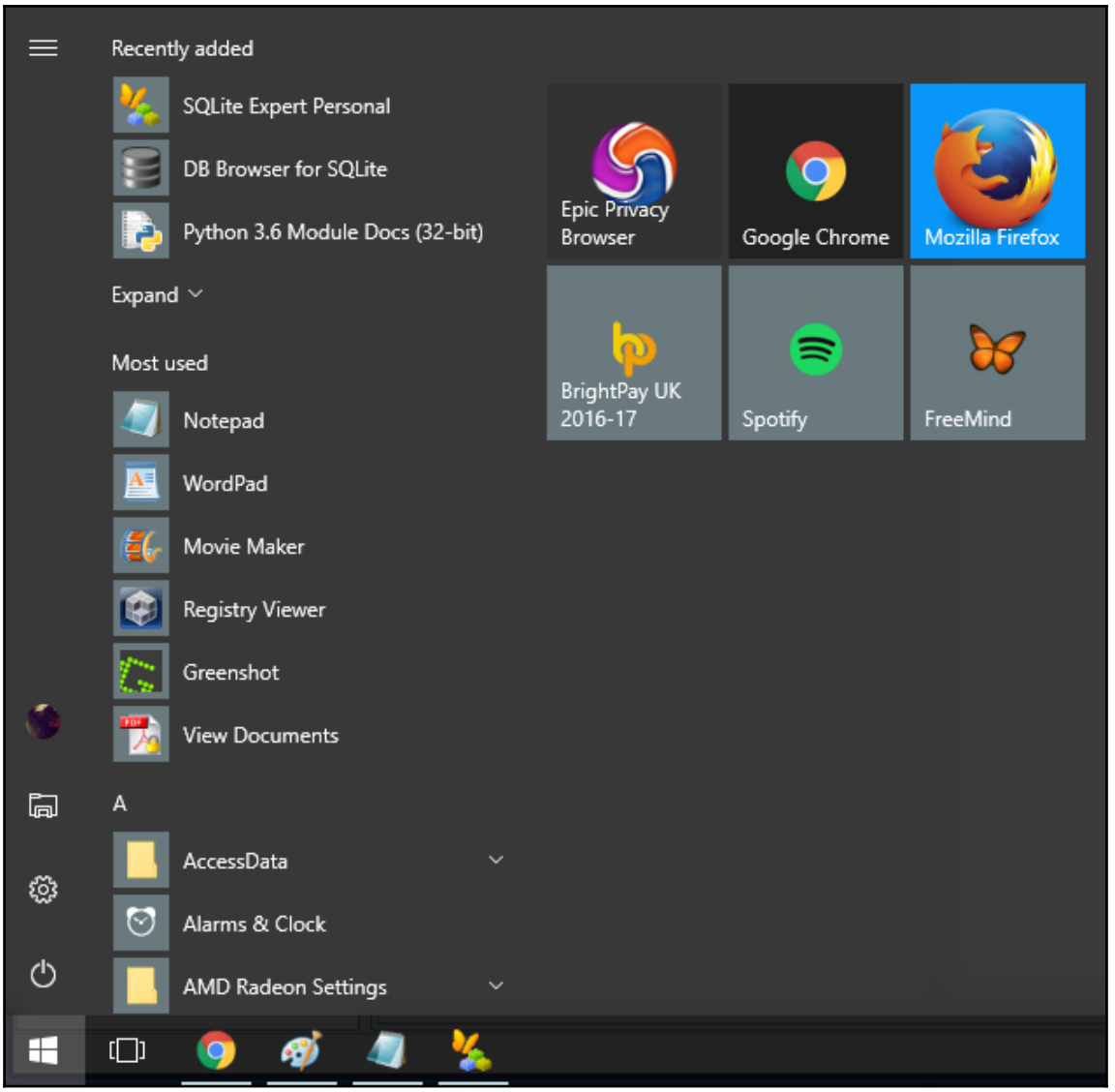

SkypeLogView: C:\Users\Admin\Desktop\skype.test
File Edit View Options Help
Record Num... Action Type Action Time End Time User Name
1909 Chat 7/26/2016 10:03:5...
1913 Chat 7/26/2016 12:02:5...
1931 Chat 7/26/2016 10:28:2...
1966 Chat 7/29/2016 8:28:30 ...
1974 Chat 8/1/2016 12:13:38 PM
1981 Chat 8/1/2016 2:51:39 PM
2694 Chat 8/3/2016 2:33:40 PM
2733 Chat 8/4/2016 12:00:44 PM
2775 Chat 8/8/2016 9:51:02 AM
2779 Chat 8/8/2016 10:05:43 ...
2799 Chat 8/10/2016 1:39:43 PM
2802 Chat 8/10/2016 2:20:06 PM
2880 Chat 8/15/2016 9:18:21 ...
2883 Chat 8/15/2016 10:48:5...
2887 Chat 8/15/2016 12:15:5...
2893 Voicemail 8/15/2016 12:19:3...
2970 Chat 8/25/2016 3:44:35 PM
2978 Chat 8/25/2016 3:45:16 PM
2985 Chat 8/29/2016 11:41:2...
3715 Chat 9/1/2016 11:59:20 ...
23 item(s)
NirSoft Freeware. http://www.nirsoft.net

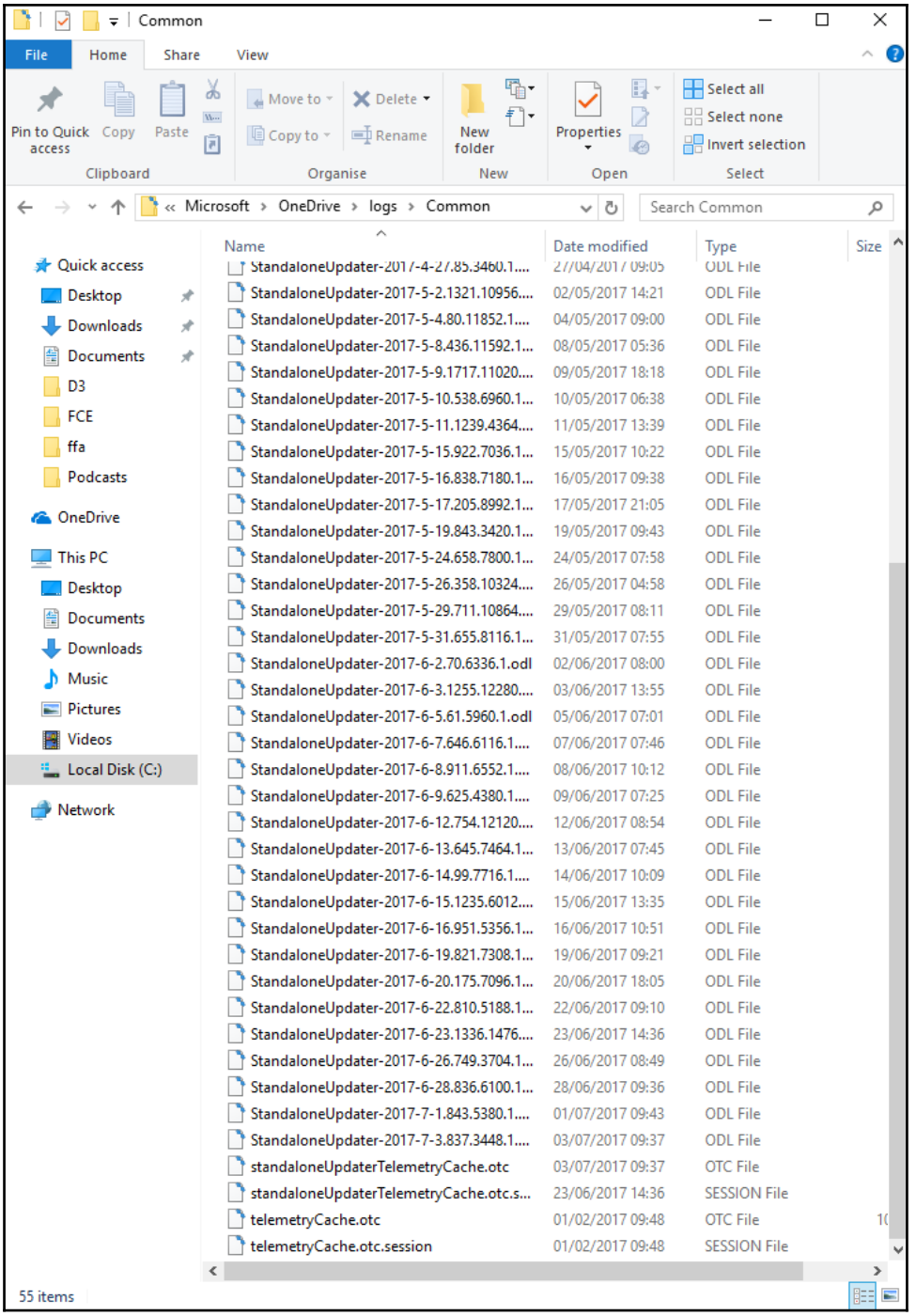
Chapter 10 : Windows 10 Forensics

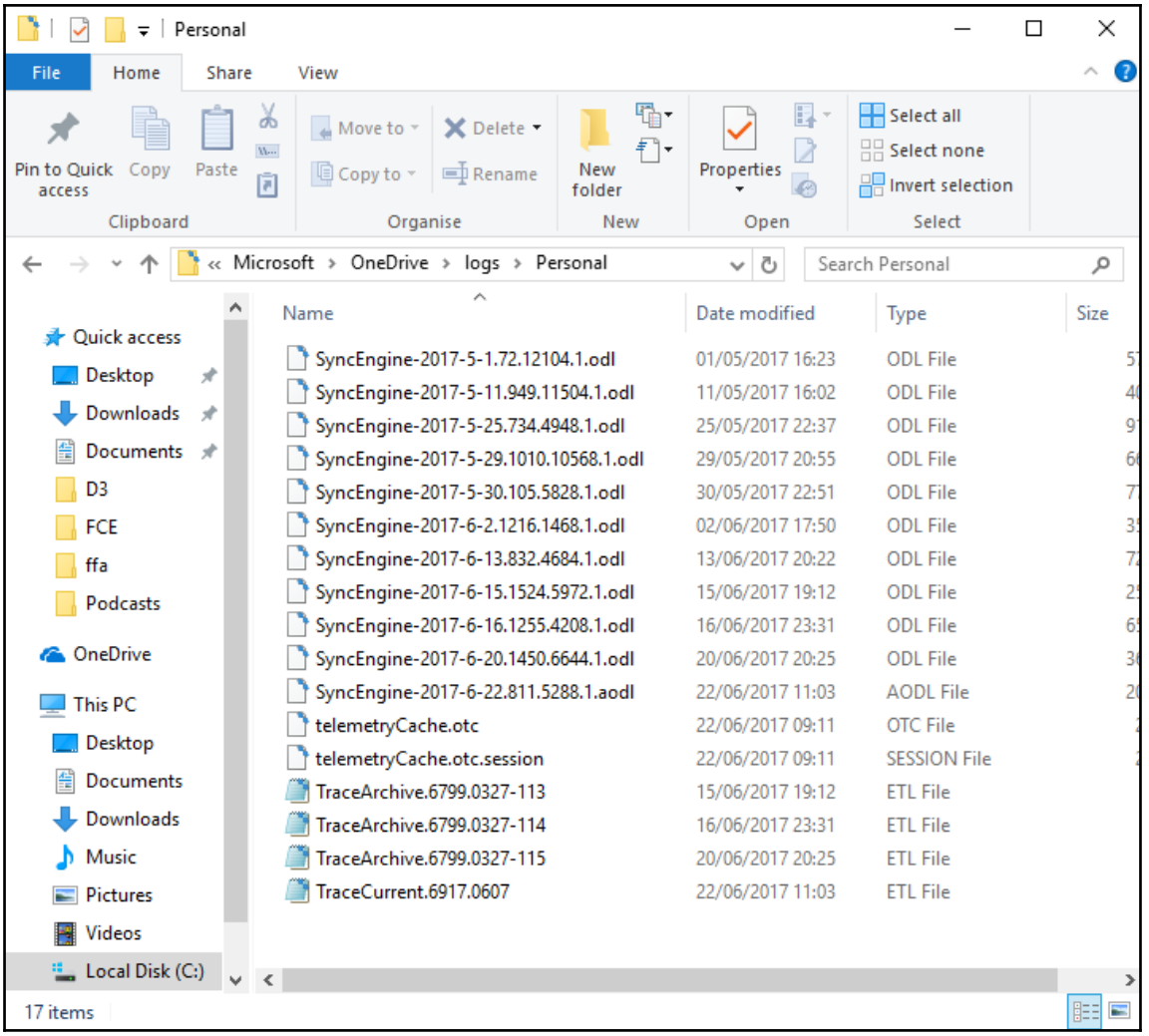


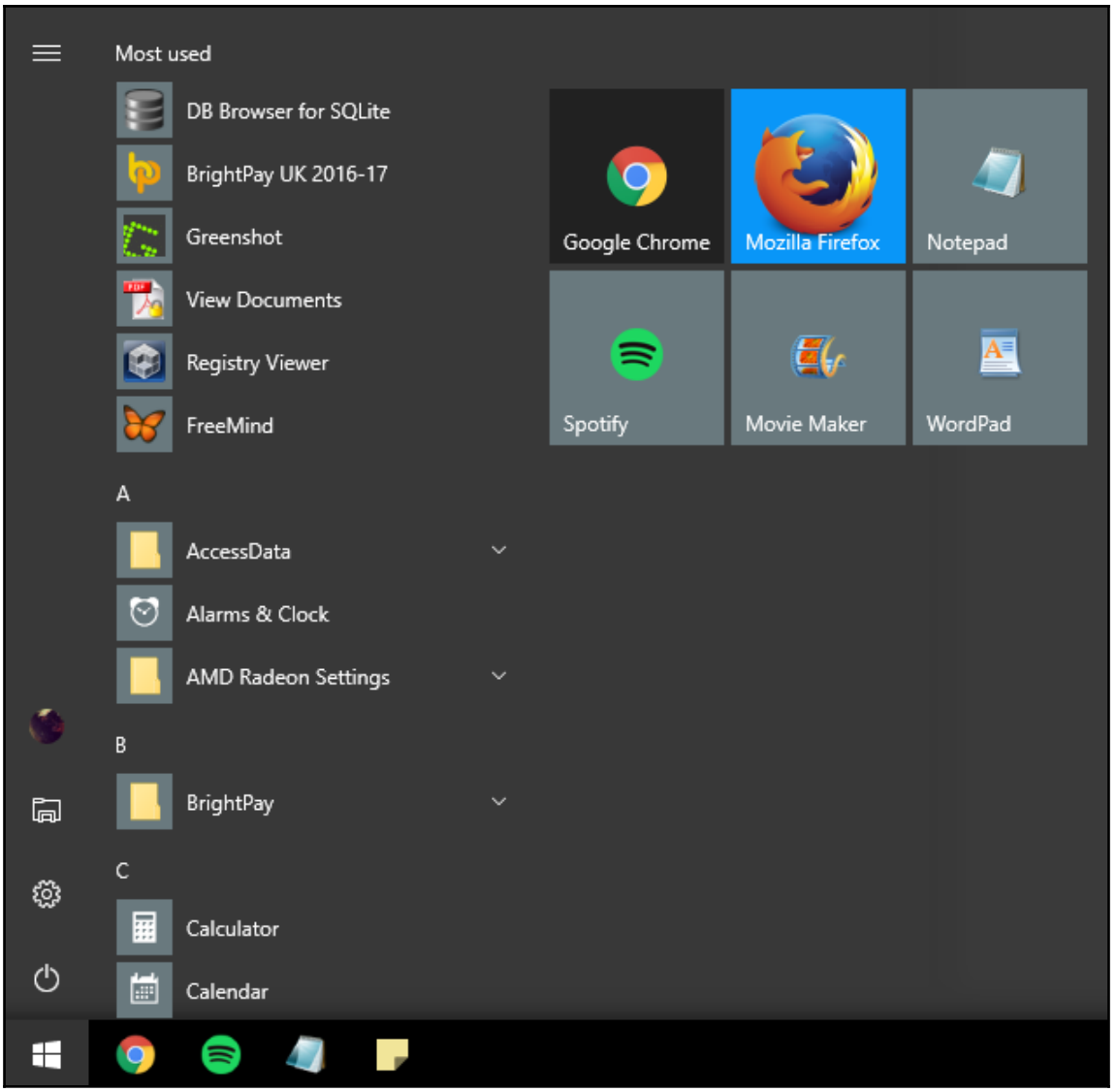

SQLite Expert Personal 4.2 (x64)
File View Database Object SQL Transaction Tools Help
Database: wpndatabase Table: NotificationHandler File: C:\Users\Razer\AppData\Local\Microsoft\Windows\Notifications\wpndatabase.db
SQLite library: sqlite3.dll 3.18.0 [FTS3 FTS4 FTS5 RTREE] Style: Cyan Night
wpndatabase
HandlerAssets
HandlerSettings
Metadata
Notification
NotificationData
NotificationHandler
WNSPushChannel
Database Data DDL Design SQL
Refresh
rowid RecordId PrimaryId WNSId HandlerType WNFEventName
1 1 Windows.SystemToast.EnterpriseDataProtectionReAuth system app:system
2 2 Microsoft.Windows.SecondaryTileExperience_cw5n1h2txyewy!App app:immersive
3 3 Microsoft.People_8wekyb3d8bbwe!x4c7a3b7dy2188y46d4ya362y19ac5a5805e5x app:immersive
5 5 microsoft.windowscommunicationsapps_8wekyb3d8bbwe!microsoft.windowslive.calendar app:immersive
6 6 Windows.SystemToast.EnterpriseDataProtection system app:system
8 8 Microsoft.WindowsStore_8wekyb3d8bbwe!App app:immersive
10 10 Microsoft.Messaging_8wekyb3d8bbwe!x27e26f40ye031y48a6yb130yd1f20388991ax app:immersive
11 11 Microsoft.WindowsFeedback_cw5n1h2txyewy!App app:immersive
12 12 Microsoft.Office.OneNote_8wekyb3d8bbwe!microsoft.onenoteim app:immersive
13 13 Windows.SystemToast.AudioTroubleshooter system app:system
14 14 WLRoamingSetting_UserTile windows.settingsprovider_cw5n1h2txyewy app:system 1338697440114249
15 15 Microsoft.Messaging_8wekyb3d8bbwe!SkypeName app:immersive
16 16 Microsoft.Messaging_8wekyb3d8bbwe!App app:immersive
17 17 Microsoft.WindowsAlarms_8wekyb3d8bbwe!App app:immersive
18 18 Microsoft.Windows.Cortana_cw5n1h2txyewy!RemindersShareTargetApp app:immersive
19 19 windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel app:immersive
20 20 Microsoft.Windows.LanguageComponentsInstaller system app:system
21 21 Microsoft.WindowsCamera_8wekyb3d8bbwe!App app:immersive
22 22 Microsoft.PPIProjection_cw5n1h2txyewy!Microsoft.PPIProjection app:immersive
23 23 Microsoft.WindowsSoundRecorder_8wekyb3d8bbwe!App app:immersive
24 24 Microsoft.ConnectivityStore_8wekyb3d8bbwe!App app:immersive
26 26 Microsoft.Getstarted_8wekyb3d8bbwe!App app:immersive
27 27 Windows.SystemToast.BackgroundAccess system app:system
28 28 Microsoft.Windows.Photos_8wekyb3d8bbwe!App app:immersive
Filtered
<no filter>
Filter

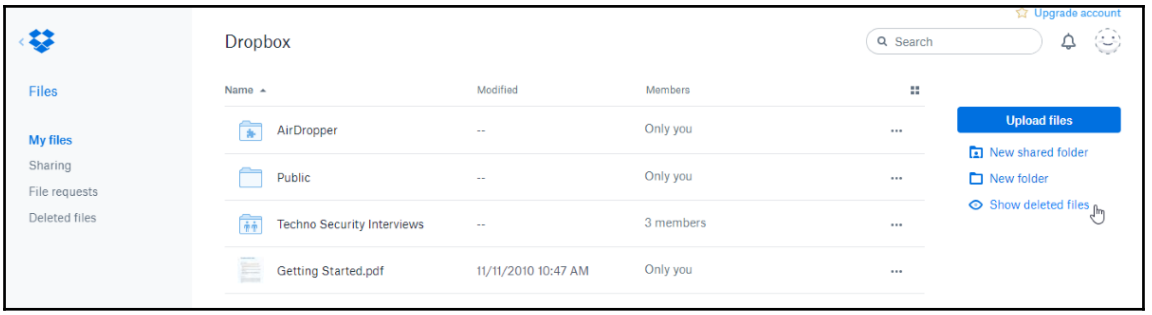

File View Database Object SQL Transaction Tools Help
Database: wpndatabase Table: Metadata File: C:\Users\Razer\AppData\Local\Microsoft\Windows\Notification
wpndatabase
HandlerSettings
Metadata
Notification
NotificationHandler
WNSPushChannel
Database Data DDL Design SQL
Refresh
rowid Key Value
(empty) (empty) (empty)
1 tile:maxCount 5
2 toast:maxCount 20
3 badge:maxCount 1
4 toastCondensed:maxCount 80
5 DB_INTIIALIZED 1
6 TilesBandwidthTotal 0
2657 CurrentNotificationId 3046

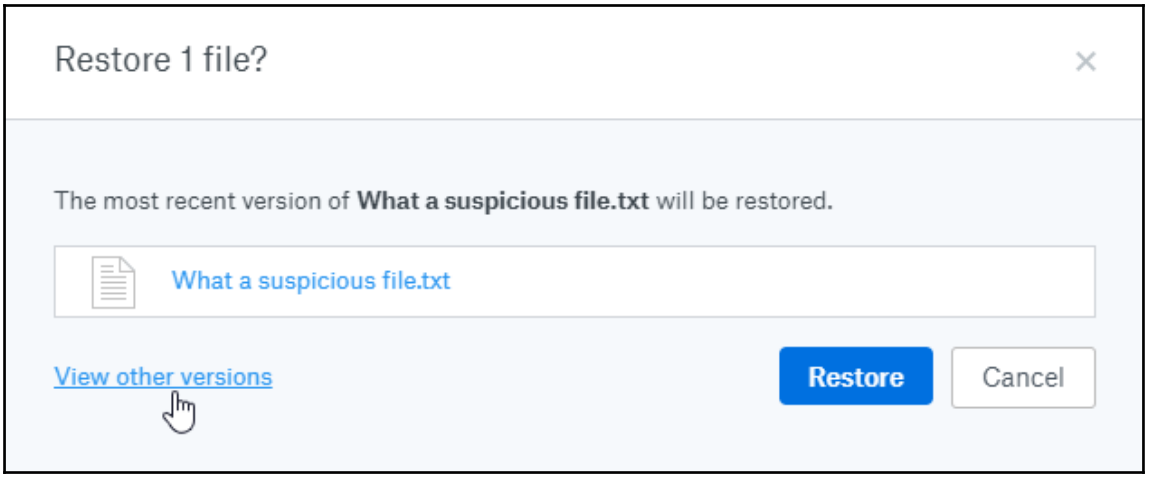

Recently added
SQLite Expert Personal
DB Browser for SQLite
Python 3.6 Module Docs (32-bit)
Expand
Most used
Notepad
WordPad
Movie Maker
Registry Viewer
Greenshot
View Documents
A
AccessData
Alarms & Clock
AMD Radeon Settings
Epic Privacy Browser
Google Chrome
Mozilla Firefox
BrightPay UK 2016-17
Spotify
FreeMind

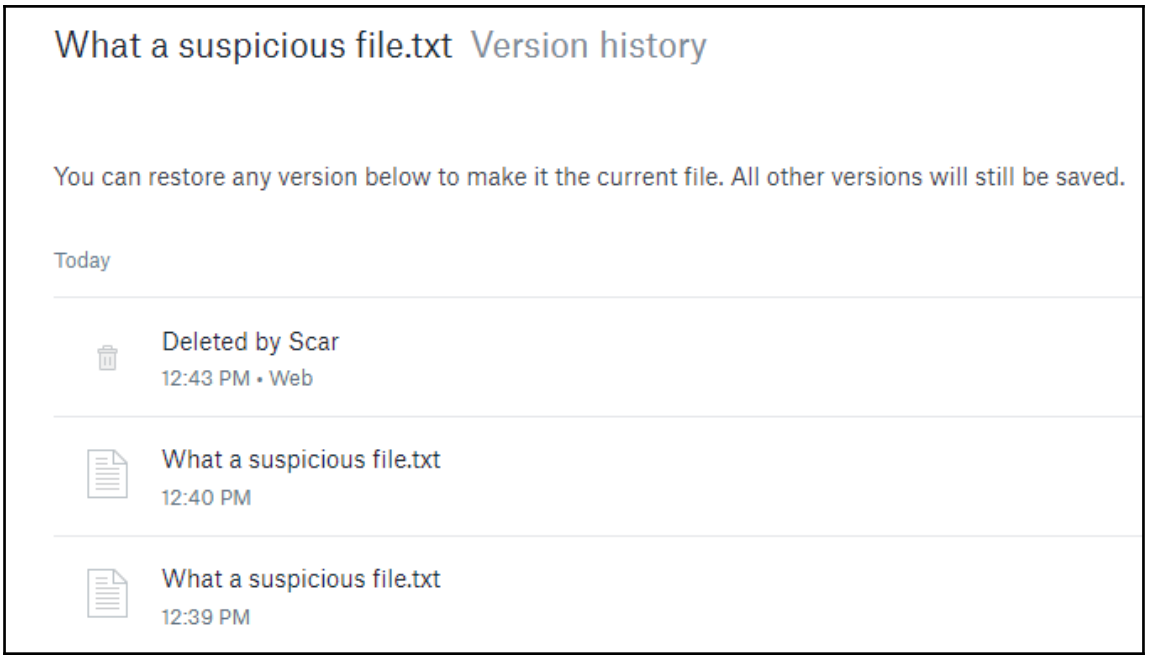

Common
File
Home
Share
View
Pin to Quick access
Copy
Paste
Clipboard
Move to
Copy to
Delete
Rename
Organise
New folder
New
Properties
Open
Select all
Select none
Invert selection
Select
« Microsoft › OneDrive › logs › Common
Search Common
Quick access
Desktop
Downloads
Documents
D3
FCE
ffa
Podcasts
OneDrive
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
Name
Date modified
Type
Size
StandaloneUpdater-2017-5-2.1321.10956.... 02/05/2017 14:21 ODL File
StandaloneUpdater-2017-5-4.80.11852.1.... 04/05/2017 09:00 ODL File
StandaloneUpdater-2017-5-8.436.11592.1... 08/05/2017 05:36 ODL File
StandaloneUpdater-2017-5-9.1717.11020.... 09/05/2017 18:18 ODL File
StandaloneUpdater-2017-5-10.538.6960.1... 10/05/2017 06:38 ODL File
StandaloneUpdater-2017-5-11.1239.4364.... 11/05/2017 13:39 ODL File
StandaloneUpdater-2017-5-15.922.7036.1... 15/05/2017 10:22 ODL File
StandaloneUpdater-2017-5-16.838.7180.1... 16/05/2017 09:38 ODL File
StandaloneUpdater-2017-5-17.205.8992.1... 17/05/2017 21:05 ODL File
StandaloneUpdater-2017-5-19.843.3420.1... 19/05/2017 09:43 ODL File
StandaloneUpdater-2017-5-24.658.7800.1... 24/05/2017 07:58 ODL File
StandaloneUpdater-2017-5-26.358.10324.... 26/05/2017 04:58 ODL File
StandaloneUpdater-2017-5-29.711.10864.... 29/05/2017 08:11 ODL File
StandaloneUpdater-2017-5-31.655.8116.1... 31/05/2017 07:55 ODL File
StandaloneUpdater-2017-6-2.70.6336.1.odl 02/06/2017 08:00 ODL File
StandaloneUpdater-2017-6-3.1255.12280.... 03/06/2017 13:55 ODL File
StandaloneUpdater-2017-6-5.61.5960.1.odl 05/06/2017 07:01 ODL File
StandaloneUpdater-2017-6-7.646.6116.1.... 07/06/2017 07:46 ODL File
StandaloneUpdater-2017-6-8.911.6552.1.... 08/06/2017 10:12 ODL File
StandaloneUpdater-2017-6-9.625.4380.1.... 09/06/2017 07:25 ODL File
StandaloneUpdater-2017-6-12.754.12120.... 12/06/2017 08:54 ODL File
StandaloneUpdater-2017-6-13.645.7464.1... 13/06/2017 07:45 ODL File
StandaloneUpdater-2017-6-14.99.7716.1.... 14/06/2017 10:09 ODL File
StandaloneUpdater-2017-6-15.1235.6012.... 15/06/2017 13:35 ODL File
StandaloneUpdater-2017-6-16.951.5356.1... 16/06/2017 10:51 ODL File
StandaloneUpdater-2017-6-19.821.7308.1... 19/06/2017 09:21 ODL File
StandaloneUpdater-2017-6-20.175.7096.1... 20/06/2017 18:05 ODL File
StandaloneUpdater-2017-6-22.810.5188.1... 22/06/2017 09:10 ODL File
StandaloneUpdater-2017-6-23.1336.1476.... 23/06/2017 14:36 ODL File
StandaloneUpdater-2017-6-26.749.3704.1... 26/06/2017 08:49 ODL File
StandaloneUpdater-2017-6-28.836.6100.1... 28/06/2017 09:36 ODL File
StandaloneUpdater-2017-7-1.843.5380.1.... 01/07/2017 09:43 ODL File
StandaloneUpdater-2017-7-3.837.3448.1.... 03/07/2017 09:37 ODL File
standaloneUpdaterTelemetryCache.otc 03/07/2017 09:37 OTC File
standaloneUpdaterTelemetryCache.otc.s... 23/06/2017 14:36 SESSION File
telemetryCache.otc 01/02/2017 09:48 OTC File
telemetryCache.otc.session 01/02/2017 09:48 SESSION File
55 items

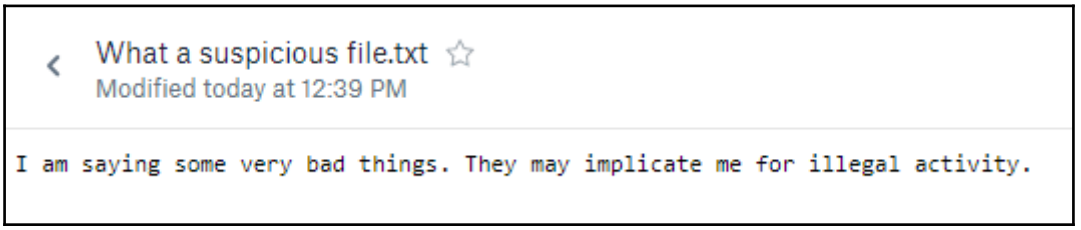

Personal
File
Home
Share
View
Pin to Quick access
Copy
Paste
Move to
Copy to
Delete
Rename
New folder
Properties
Select all
Select none
Invert selection
Clipboard
Organise
New
Open
Select
« Microsoft › OneDrive › logs › Personal
Search Personal
Quick access
Desktop
Downloads
Documents
D3
FCE
ffa
Podcasts
OneDrive
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Name
Date modified
Type
Size
SyncEngine-2017-5-1.72.12104.1.odl 01/05/2017 16:23 ODL File
SyncEngine-2017-5-11.949.11504.1.odl 11/05/2017 16:02 ODL File
SyncEngine-2017-5-25.734.4948.1.odl 25/05/2017 22:37 ODL File
SyncEngine-2017-5-29.1010.10568.1.odl 29/05/2017 20:55 ODL File
SyncEngine-2017-5-30.105.5828.1.odl 30/05/2017 22:51 ODL File
SyncEngine-2017-6-2.1216.1468.1.odl 02/06/2017 17:50 ODL File
SyncEngine-2017-6-13.832.4684.1.odl 13/06/2017 20:22 ODL File
SyncEngine-2017-6-15.1524.5972.1.odl 15/06/2017 19:12 ODL File
SyncEngine-2017-6-16.1255.4208.1.odl 16/06/2017 23:31 ODL File
SyncEngine-2017-6-20.1450.6644.1.odl 20/06/2017 20:25 ODL File
SyncEngine-2017-6-22.811.5288.1.aodl 22/06/2017 11:03 AODL File
telemetryCache.otc 22/06/2017 09:11 OTC File
telemetryCache.otc.session 22/06/2017 09:11 SESSION File
TraceArchive.6799.0327-113 15/06/2017 19:12 ETL File
TraceArchive.6799.0327-114 16/06/2017 23:31 ETL File
TraceArchive.6799.0327-115 20/06/2017 20:25 ETL File
TraceCurrent.6917.0607 22/06/2017 11:03 ETL File
17 items

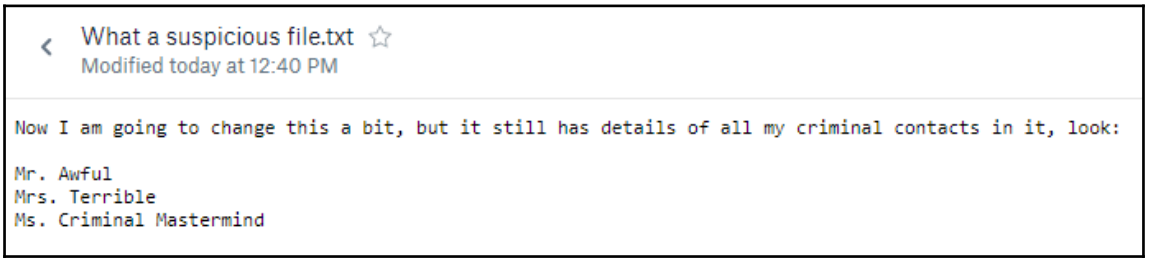

Most used
DB Browser for SQLite
BrightPay UK 2016-17
Greenshot
View Documents
Registry Viewer
FreeMind
A
AccessData
Alarms & Clock
AMD Radeon Settings
B
BrightPay
C
Calculator
Calendar
Google Chrome
Mozilla Firefox
Notepad
Spotify
Movie Maker
WordPad

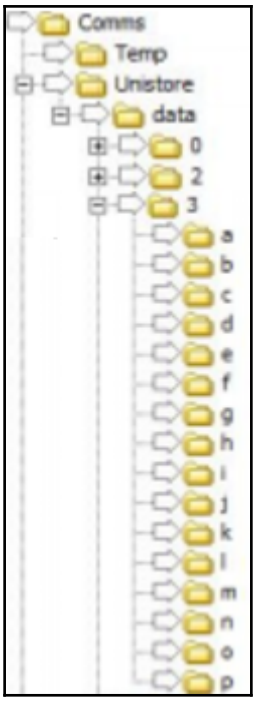

Upgrade account
Dropbox
Search
Files
My files
Sharing
File requests
Deleted files
Name
Modified
Members
AirDropper
--
Only you
Public
--
Only you
Techno Security Interviews
--
3 members
Getting Started.pdf
11/11/2010 10:47 AM
Only you
Upload files
New shared folder
New folder
Show deleted files


Restore 1 file?
The most recent version of **What a suspicious file.txt** will be restored.
What a suspicious file.txt
View other versions
Restore
Cancel


What a suspicious file.txt Version history
You can restore any version below to make it the current file. All other versions will still be saved.
Today
Deleted by Scar
12:43 PM • Web
What a suspicious file.txt
12:40 PM
What a suspicious file.txt
12:39 PM

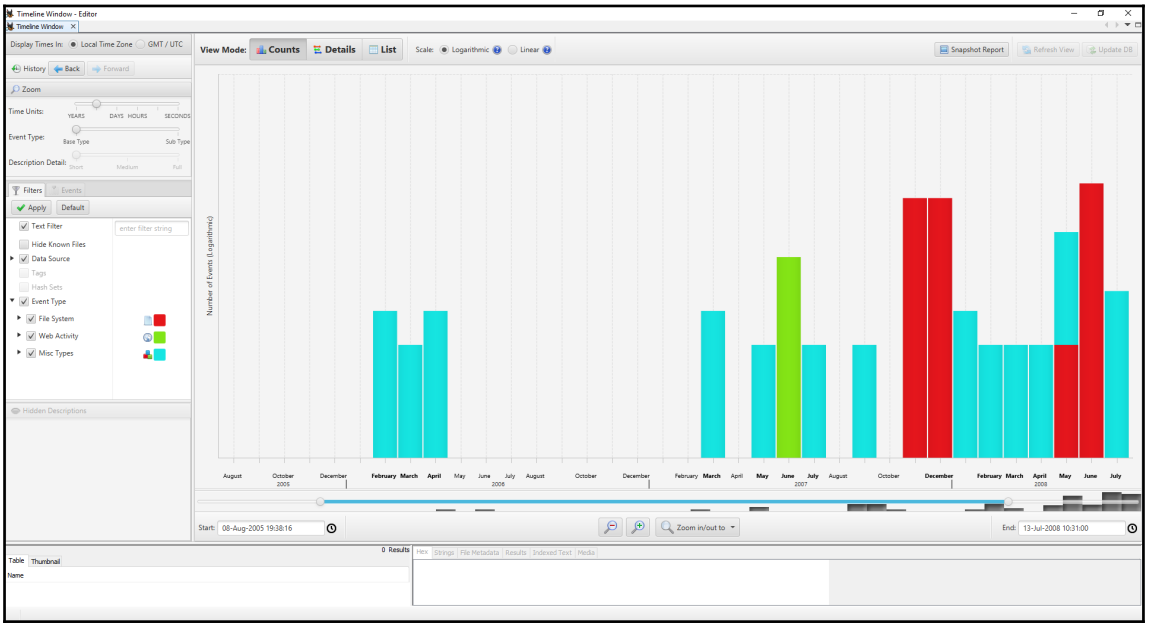

What a suspicious file.txt
Modified today at 12:39 PM
I am saying some very bad things. They may implicate me for illegal activity.

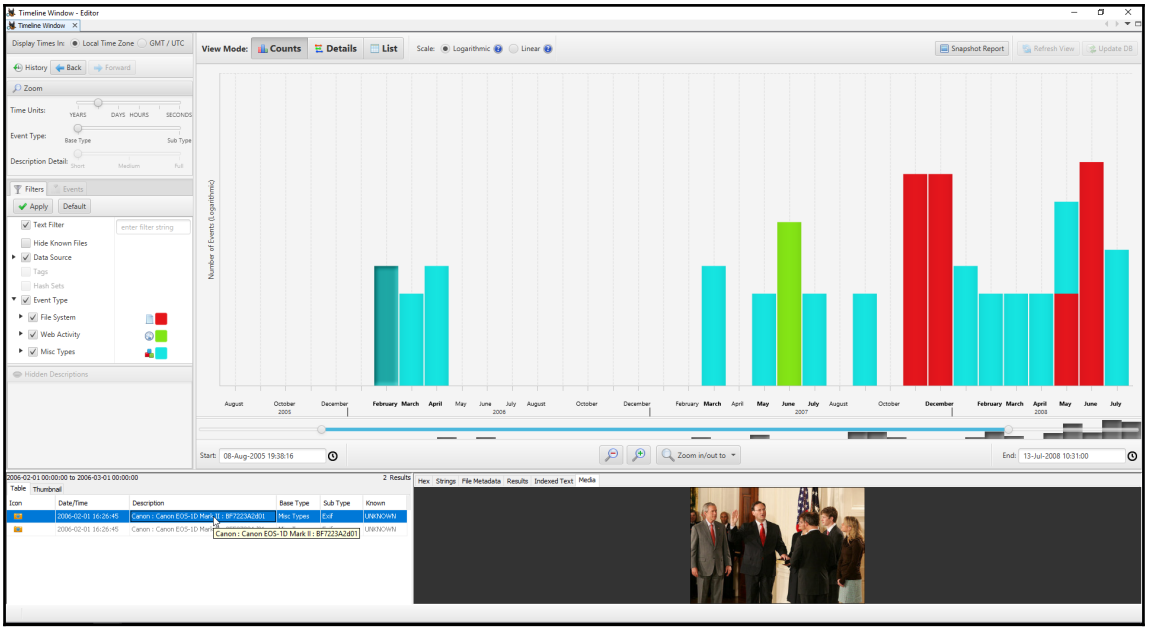

What a suspicious file.txt
Modified today at 12:40 PM
Now I am going to change this a bit, but it still has details of all my criminal contacts in it, look:
Mr. Awful
Mrs. Terrible
Ms. Criminal Mastermind

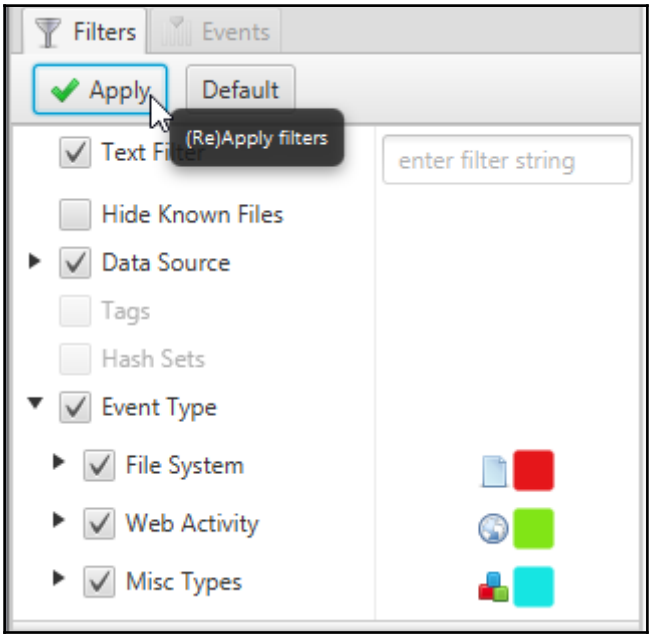


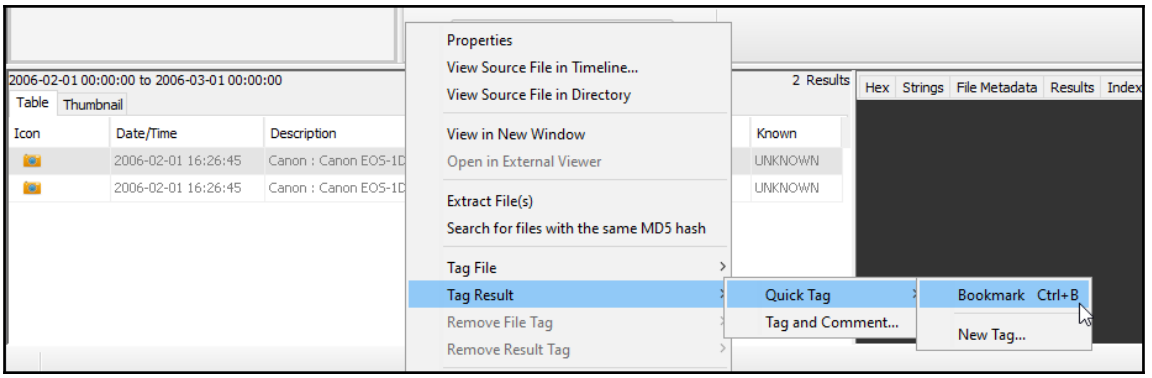

```
<a:lastMessage>
<a:hasAudio> false
<a:hasPhoto> true
<a:isRead> false
<a:lastUpdateTime> 0001-02-03T01:02:03
<a:messageFolder> SentItems
<a:messageId> 10
<a:messageText> Let's do some illegal things on this computer.
```

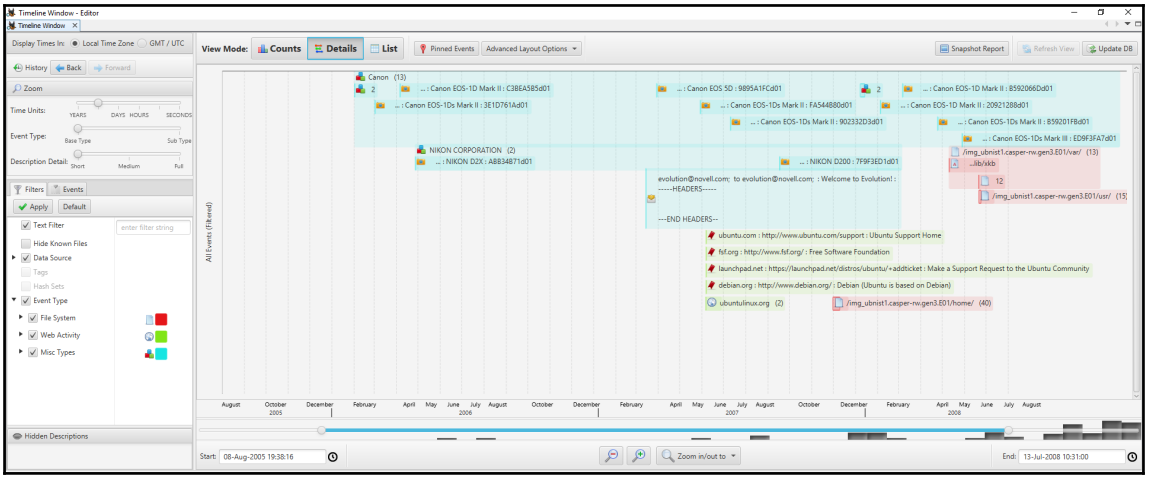
Chapter 11: Data Visualisation

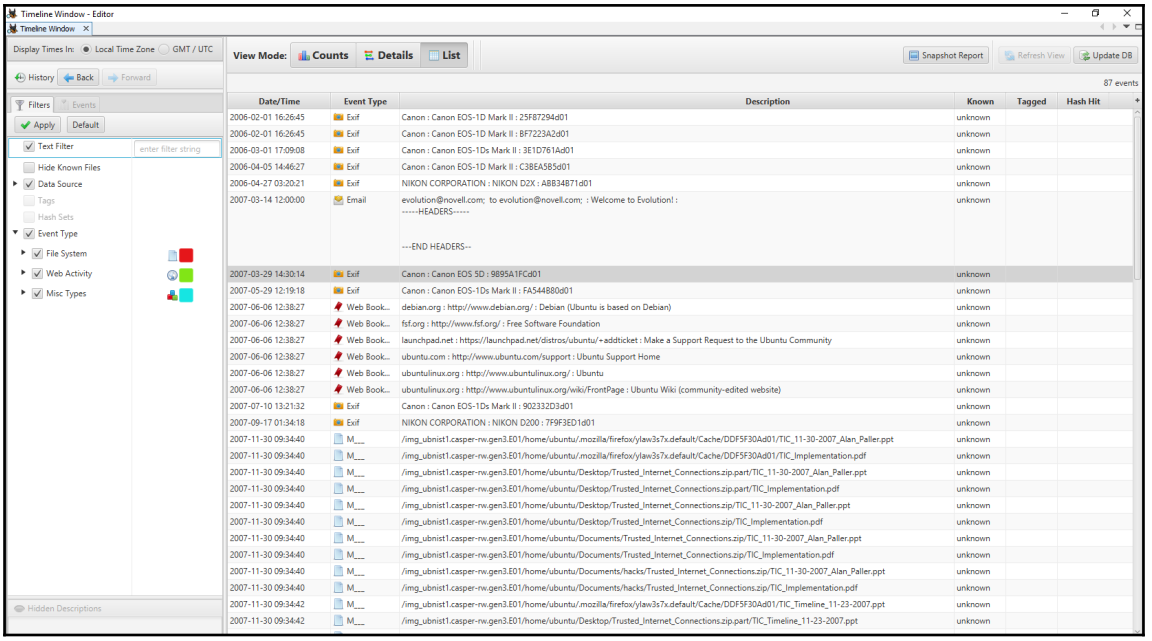


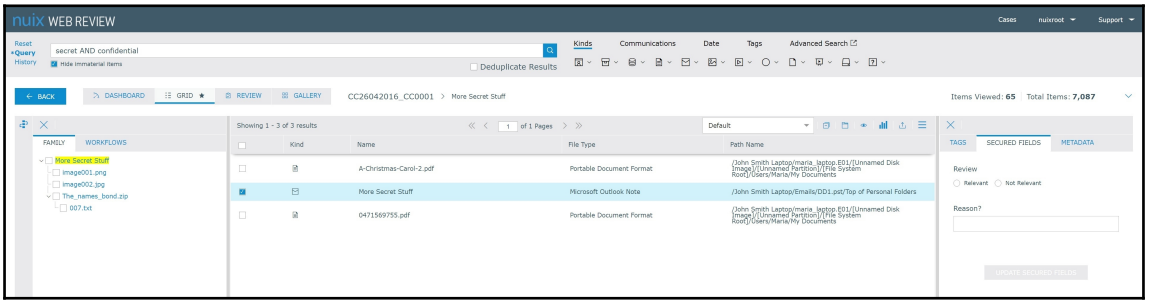

Timeline Window - Editor
Timeline Window
Display Times In: Local Time Zone GMT / UTC
History Back Forward
Zoom
Time Units: YEARS DAYS HOURS SECONDS
Event Type: Base Type Sub Type
Description Detail: Short Medium Full
Filters Events
Apply Default
Text Filter
enter filter string
Hide Known Files
Data Source
Tags
Hash Sets
Event Type
File System
Web Activity
Misc Types
Hidden Descriptions
View Mode: Counts Details List
Scale: Logarithmic Linear
Snapshot Report Refresh View Update DB
Number of Events (Logarithmic)
August October December February March April May June July August October December February March April May June July August October December February March April May June July
2005 2006 2007 2008
Start: 08-Aug-2005 19:38:16
Zoom in/out to
End: 13-Jul-2008 10:31:00
2006-02-01 00:00:00 to 2006-03-01 00:00:00
2 Results
Table Thumbnail
Icon Date/Time Description Base Type Sub Type Known
2006-02-01 16:26:45 Canon : Canon EOS-1D Mark II : BF7223A2d01 Misc Types Exif UNKNOWN
2006-02-01 16:26:45 Canon : Canon EOS-1D Mark II : BF7223A2d01 UNKNOWN
Hex Strings File Metadata Results Indexed Text Media


Filters
Events
Apply
Default
(Re)Apply filters
Text Filter
enter filter string
Hide Known Files
Data Source
Tags
Hash Sets
Event Type
File System
Web Activity
Misc Types


Properties
View Source File in Timeline...
View Source File in Directory
View in New Window
Open in External Viewer
Extract File(s)
Search for files with the same MD5 hash
Tag File
Tag Result
Remove File Tag
Remove Result Tag
Quick Tag
Tag and Comment...
Bookmark Ctrl+B
New Tag...
2006-02-01 00:00:00 to 2006-03-01 00:00:00
Table
Thumbnail
Icon
Date/Time
Description
2006-02-01 16:26:45
Canon : Canon EOS-1D
2006-02-01 16:26:45
Canon : Canon EOS-1D
2 Results
Known
UNKNOWN
UNKNOWN
Hex
Strings
File Metadata
Results
Index

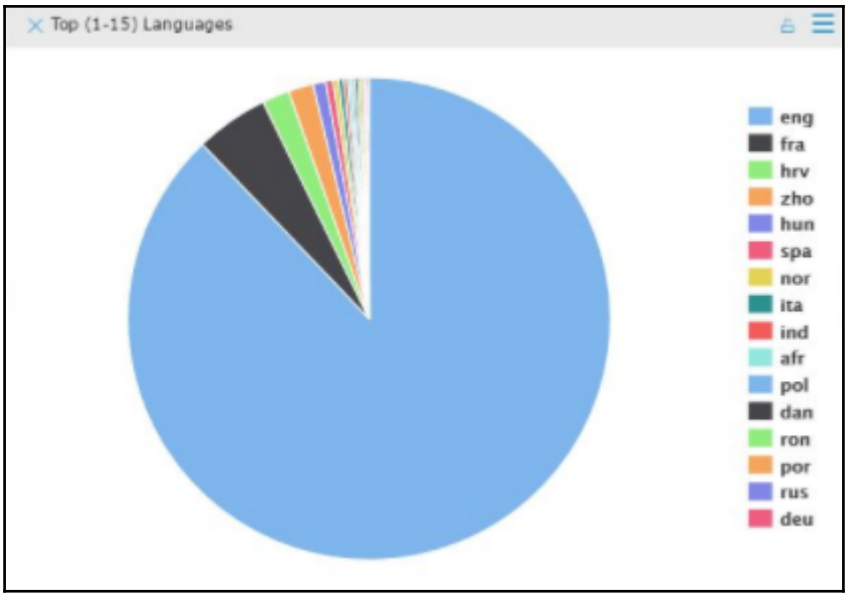

Timeline Window - Editor
Timeline Window
View Mode:
Counts
Details
List
Pinned Events
Advanced Layout Options
Snapshot Report
Refresh View
Update DB
Display Times In:
Local Time Zone
GMT / UTC
History
Back
Forward
Zoom
Time Units:
Event Type:
Description Detail:
Filters
Events
Apply
Default
Text Filter
Hide Known Files
Data Source
Tags
Hash Sets
Event Type
File System
Web Activity
Misc Types
Hidden Descriptions
All Events (Filtered)
Canon (13)
NIKON CORPORATION (2)
ubuntu.com : http://www.ubuntu.com/support : Ubuntu Support Home
fsf.org : http://www.fsf.org/ : Free Software Foundation
launchpad.net : https://launchpad.net/distros/ubuntu/+addticket : Make a Support Request to the Ubuntu Community
debian.org : http://www.debian.org/ : Debian (Ubuntu is based on Debian)
ubuntulinux.org (2)
August
October
December
February
April
May
June
July
August
2005
2006
2007
2008
Start:
08-Aug-2005 19:38:16
Zoom in/out to
End:
13-Jul-2008 10:31:00


Timeline Window - Editor
Timeline Window
Display Times In: Local Time Zone GMT / UTC
History Back Forward
Filters Events
Apply Default
Text Filter enter filter string
Hide Known Files
Data Source
Tags
Hash Sets
Event Type
File System
Web Activity
Misc Types
Hidden Descriptions
View Mode: Counts Details List
Snapshot Report Refresh View Update DB
87 events
Date/Time Event Type Description Known Tagged Hash Hit
2006-02-01 16:26:45 Exif Canon : Canon EOS-1D Mark II : 25F87294d01 unknown
2006-02-01 16:26:45 Exif Canon : Canon EOS-1D Mark II : BF7223A2d01 unknown
2006-03-01 17:09:08 Exif Canon : Canon EOS-1Ds Mark II : 3E1D761Ad01 unknown
2006-04-05 14:46:27 Exif Canon : Canon EOS-1D Mark II : C38EA585d01 unknown
2006-04-27 03:20:21 Exif NIKON CORPORATION : NIKON D2X : ABB34B71d01 unknown
2007-03-14 12:00:00 Email evolution@novell.com; to evolution@novell.com; : Welcome to Evolution! : unknown
-----HEADERS-----
---END HEADERS--
2007-03-29 14:30:14 Exif Canon : Canon EOS 5D : 9895A1FCd01 unknown
2007-05-29 12:19:18 Exif Canon : Canon EOS-1Ds Mark II : FA544880d01 unknown
2007-06-06 12:38:27 Web Book... debian.org : http://www.debian.org/ : Debian (Ubuntu is based on Debian) unknown
2007-06-06 12:38:27 Web Book... fsf.org : http://www.fsf.org/ : Free Software Foundation unknown
2007-06-06 12:38:27 Web Book... launchpad.net : https://launchpad.net/distros/ubuntu/+addticket : Make a Support Request to the Ubuntu Community unknown
2007-06-06 12:38:27 Web Book... ubuntu.com : http://www.ubuntu.com/support : Ubuntu Support Home unknown
2007-06-06 12:38:27 Web Book... ubuntulinux.org : http://www.ubuntulinux.org/ : Ubuntu unknown
2007-06-06 12:38:27 Web Book... ubuntulinux.org : http://www.ubuntulinux.org/wiki/FrontPage : Ubuntu Wiki (community-edited website) unknown
2007-07-10 13:21:32 Exif Canon : Canon EOS-1Ds Mark II : 902332D3d01 unknown
2007-09-17 01:34:18 Exif NIKON CORPORATION : NIKON D200 : 7F9F3ED1d01 unknown
2007-11-30 09:34:40 M... /img_ubnist1.casper-rw.gen3.E01/home/ubuntu/.mozilla/firefox/ylaw3s7x.default/Cache/DDF5F30Ad01/TIC_11-30-2007_Alan_Paller.ppt unknown
2007-11-30 09:34:40 M... /img_ubnist1.casper-rw.gen3.E01/home/ubuntu/.mozilla/firefox/ylaw3s7x.default/Cache/DDF5F30Ad01/TIC_Implementation.pdf unknown
2007-11-30 09:34:40 M... /img_ubnist1.casper-rw.gen3.E01/home/ubuntu/Desktop/Trusted_Internet_Connections.zip.part/TIC_11-30-2007_Alan_Paller.ppt unknown
2007-11-30 09:34:40 M... /img_ubnist1.casper-rw.gen3.E01/home/ubuntu/Desktop/Trusted_Internet_Connections.zip.part/TIC_Implementation.pdf unknown
2007-11-30 09:34:40 M... /img_ubnist1.casper-rw.gen3.E01/home/ubuntu/Desktop/Trusted_Internet_Connections.zip/TIC_11-30-2007_Alan_Paller.ppt unknown
2007-11-30 09:34:40 M... /img_ubnist1.casper-rw.gen3.E01/home/ubuntu/Desktop/Trusted_Internet_Connections.zip/TIC_Implementation.pdf unknown
2007-11-30 09:34:40 M... /img_ubnist1.casper-rw.gen3.E01/home/ubuntu/Documents/Trusted_Internet_Connections.zip/TIC_11-30-2007_Alan_Paller.ppt unknown
2007-11-30 09:34:40 M... /img_ubnist1.casper-rw.gen3.E01/home/ubuntu/Documents/Trusted_Internet_Connections.zip/TIC_Implementation.pdf unknown
2007-11-30 09:34:40 M... /img_ubnist1.casper-rw.gen3.E01/home/ubuntu/Documents/hacks/Trusted_Internet_Connections.zip/TIC_11-30-2007_Alan_Paller.ppt unknown
2007-11-30 09:34:40 M... /img_ubnist1.casper-rw.gen3.E01/home/ubuntu/Documents/hacks/Trusted_Internet_Connections.zip/TIC_Implementation.pdf unknown
2007-11-30 09:34:42 M... /img_ubnist1.casper-rw.gen3.E01/home/ubuntu/.mozilla/firefox/ylaw3s7x.default/Cache/DDF5F30Ad01/TIC_Timeline_11-23-2007.ppt unknown
2007-11-30 09:34:42 M... /img_ubnist1.casper-rw.gen3.E01/home/ubuntu/Desktop/Trusted_Internet_Connections.zip.part/TIC_Timeline_11-23-2007.ppt unknown

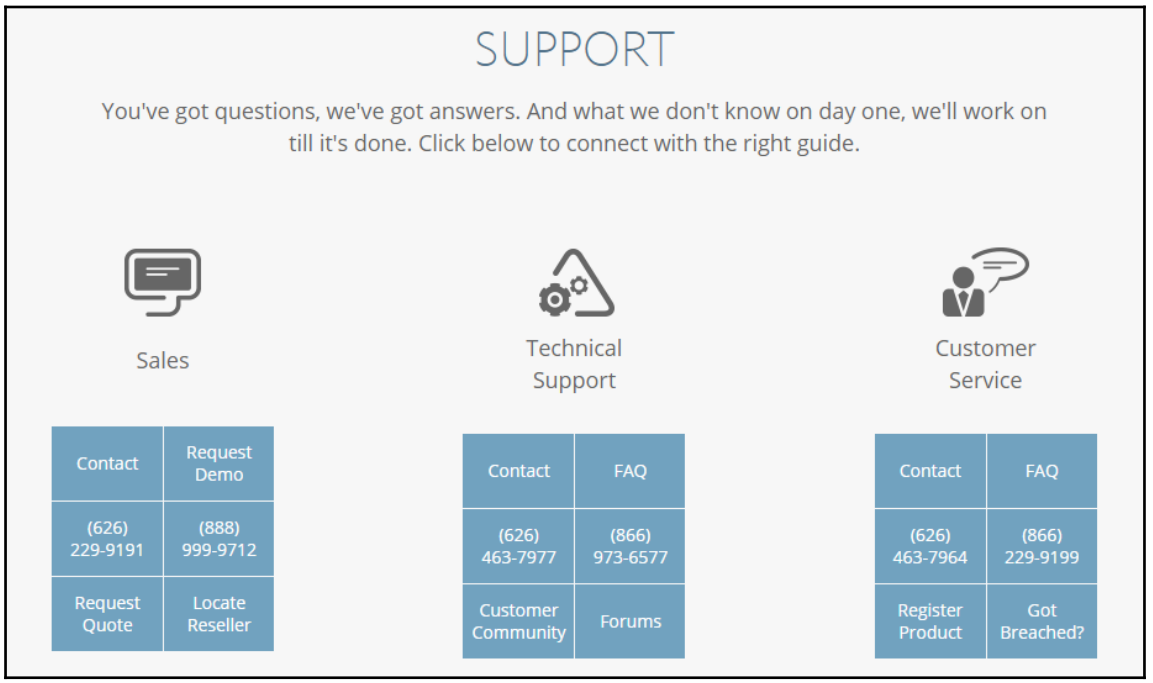

nuix WEB REVIEW
Cases nuixroot Support
Reset Query History
secret AND confidential
Hide immaterial items
Kinds Communications Date Tags Advanced Search
Deduplicate Results
BACK DASHBOARD GRID REVIEW GALLERY
CC26042016_CC0001 > More Secret Stuff
Items Viewed: 65 Total Items: 7,087
FAMILY WORKFLOWS
More Secret Stuff
image001.png
image002.jpg
The_names_bond.zip
007.txt
Showing 1 - 3 of 3 results
1 of 1 Pages
Default
Kind Name File Type Path Name
A-Christmas-Carol-2.pdf Portable Document Format /John Smith Laptop/maria_laptop.E01/[Unnamed Disk Image]/[Unnamed Partition]/[File System Root]/Users/Maria/My Documents
More Secret Stuff Microsoft Outlook Note /John Smith Laptop/Emails/DD1.pst/Top of Personal Folders
0471569755.pdf Portable Document Format /John Smith Laptop/maria_laptop.E01/[Unnamed Disk Image]/[Unnamed Partition]/[File System Root]/Users/Maria/My Documents
TAGS SECURED FIELDS METADATA
Review
Relevant Not Relevant
Reason?
UPDATE SECURED FIELDS

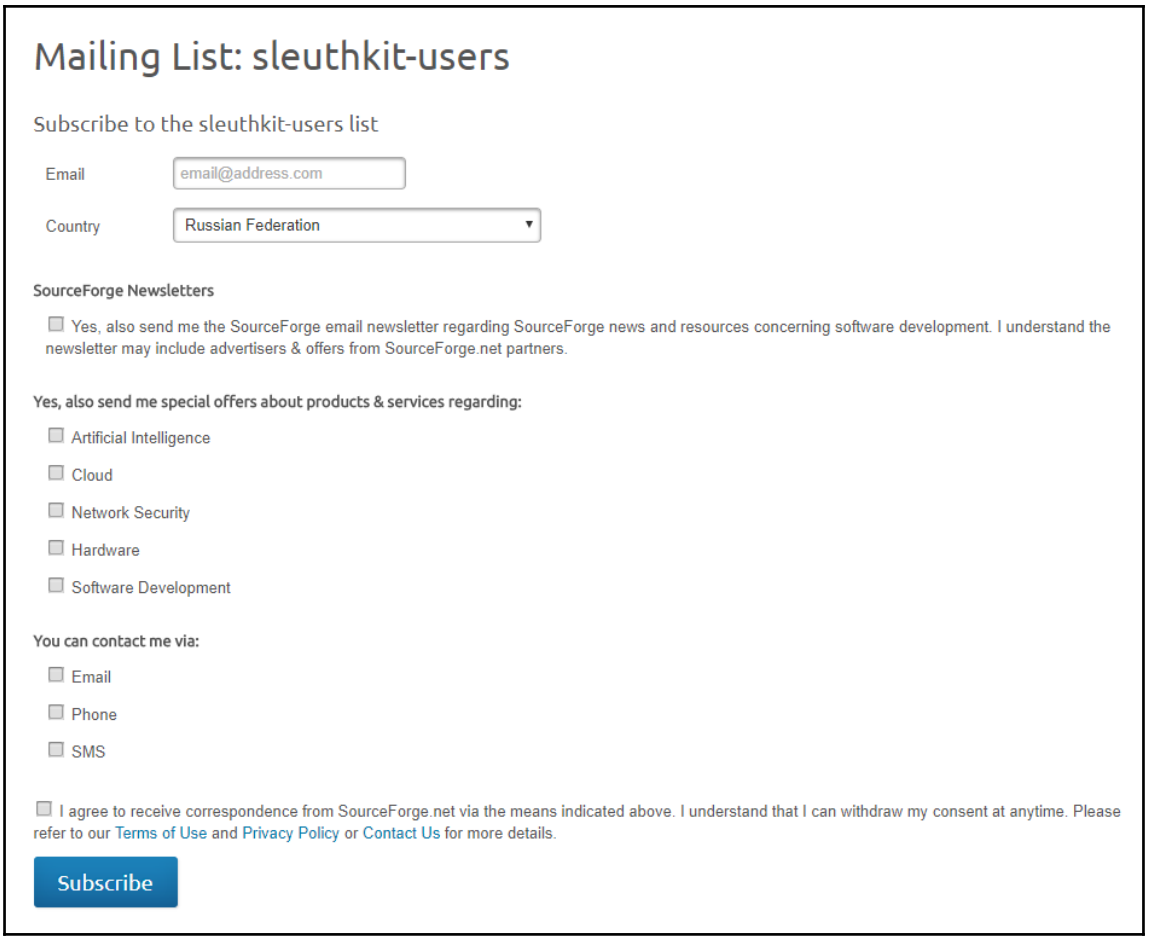

TAGS
SECURED FIELDS
METADATA
Search Default


Location
Map
Satellite
North Sea
Edinburgh
Glasgow
United Kingdom
Isle of Man
Dublin
Manchester
Liverpool
London
Amsterdam
Netherlands
Hamburg
Copenhagen
Denmark
Poland
Warsaw
Brussels
Cologne
Germany
Belgium
Frankfurt
Luxembourg
Paris
Prague
Czechia
Munich
Vienna
Slovakia
Austria
Hungary
Switzerland
France
Milan
Slovenia
Zagreb
Google
Map data ©2017 GeoBasis-DE/BKG (©2009), Google, Inst. Geogr. Nacional, Mapa GISrael, ORION-ME
Terms of Use
Report a map error


Top (1-15) Languages
eng
fra
hrv
zho
hun
spa
nor
ita
ind
afr
pol
dan
ron
por
rus
deu

Chapter 12 : Troubleshooting in Windows Forensic Analysis





Mailing List: sleuthkit-users

Subscribe to the sleuthkit-users list

Email email@address.com

Country Russian Federation

SourceForge Newsletters

Yes, also send me the SourceForge email newsletter regarding SourceForge news and resources concerning software development. I understand the newsletter may include advertisers & offers from SourceForge.net partners.

Yes, also send me special offers about products & services regarding:

Artificial Intelligence

Cloud

Network Security

Hardware

Software Development

You can contact me via:

Email

Phone

SMS

I agree to receive correspondence from SourceForge.net via the means indicated above. I understand that I can withdraw my consent at anytime. Please refer to our Terms of Use and Privacy Policy or Contact Us for more details.

Subscribe

	Search...	Source	Location
	0`	119491-1.E01 - Partition 3 (Microsoft NTFS, 453.99...	File Offset 2809764368
	0`	119491-1.E01 - Partition 3 (Microsoft NTFS, 453.99...	File Offset 670642416
	0a	119491-1.E01 - Partition 3 (Microsoft NTFS, 453.99...	File Offset 670642448
	0`	119491-1.E01 - Partition 3 (Microsoft NTFS, 453.99...	File Offset 366085328
	0a	119491-1.E01 - Partition 3 (Microsoft NTFS, 453.99...	File Offset 2809764416
	0a	119491-1.E01 - Partition 3 (Microsoft NTFS, 453.99...	File Offset 366085728