

1 What is the computer name of the suspect machine?

Using Autopsy and after load image, I use keyword search and search “machine name” and it show me a file */img_c16 – Hunter/ProgramData/Microsoft/ILSCache/imcr-cache.xml* where there is the answers

File Size
Its
Extracted Content
Extension Mismatch Detected (2)
Operating System Information (2)
Operating System User Account (1)
Recent Documents (28)
Run Programs (1123)
Shell Bags (63)
USB Device Attached (5)

Source File	S	C	Name	Domain	Version	Processor Architecture	Item
SYSTEM			4ORENSICS		Windows_NT	AMD64	%Sy
SOFTWARE							

Figure 1.1

2 What is the computer IP?

Using Autopsy and exploring windows registry i found in */img_c16–Hunter/Windows/System32/config/SYSTEM* and then *ControlSet001/Services/Tcpip/Parameters/Interfaces*

storvsc
storvsp
svsvsc
swenum
swprv
Synth3dVsc
SysMain
SystemEventsBroker
TabletInputService
TapiSrv
Tcpip
Linkage
Parameters
Adapters
DNSRegisteredAdapters
Interfaces
{8718928D-CBEB-45EA-A621-800A9249001D}
{8CB9FBF6-AE23-4E1C-AA0A-EE23CB4FE736}
{bbcd3e08-0b41-11e3-8249-806e6f6e6963}
NsiObjectSecurity
PersistentRoutes
Winsock
Performance
Security
ServiceProvider

Name	Type	Data
UseZeroBroadcast	REG_DWORD	0x00000000 (0)
EnableDeadGWDetect	REG_DWORD	0x00000001 (1)
EnableDHCP	REG_DWORD	0x00000001 (1)
NameServer	REG_SZ	(value not set)
Domain	REG_SZ	(value not set)
RegistrationEnabled	REG_DWORD	0x00000001 (1)
RegisterAdapterName	REG_DWORD	0x00000000 (0)
DhcpIPAddress	REG_SZ	10.0.2.15
DhcpSubnetMask	REG_SZ	255.255.255.0
DhcpServer	REG_SZ	10.0.2.2
Lease	REG_DWORD	0x00015180 (86400)
LeaseObtainedTime	REG_DWORD	0x5768A54C (1466475852)
T1	REG_DWORD	0x57694E0C (1466519052)
T2	REG_DWORD	0x5769CC9C (1466551452)
LeaseTerminatesTime	REG_DWORD	0x5769F6CC (1466562252)
AddressType	REG_DWORD	0x00000000 (0)
IsServerNapAware	REG_DWORD	0x00000000 (0)
DhcpConnForceBroadca...	REG_DWORD	0x00000000 (0)
DhcpNameServer	REG_SZ	10.0.2.3
DhcpDefaultGateway	REG_MULTI_SZ	10.0.2.2
DhcpSubnetMaskOpt	REG_MULTI_SZ	255.255.255.0
DhcpInterfaceOptions	REG_BINARY	FC 00 00 00 00 00 00 00 00 00 00

Figure 2.1

3 What was the DHCP LeaseObtainedTime?

Always in `/img_c16 - Hunter/Windows/System32/config/SYSTEM` and then `ControlSet001/Services/Tcpip/Parameters/Interfaces`

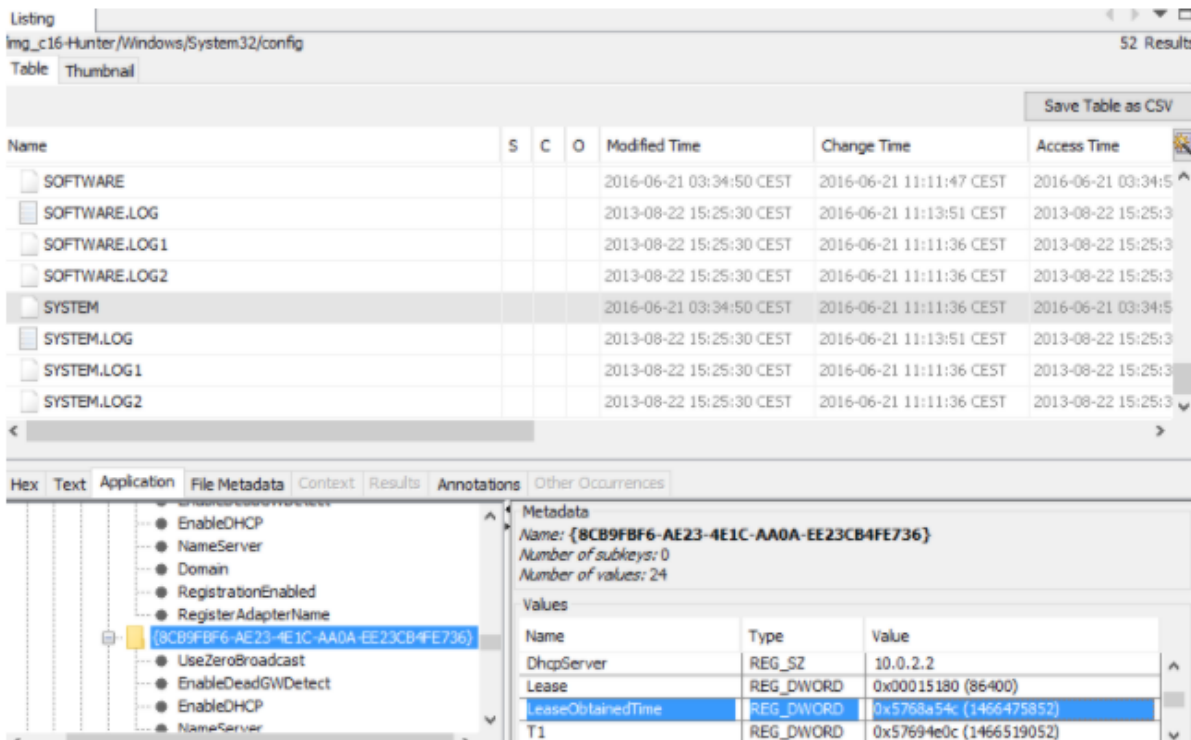


Figure 3.1

and when obtained REG_DWORD 0x5768a54c. We converted it using EpochConverter (before we convert from DWORD to DEC= 1466475852)



Figure 3.2

4 How many times did this user log on to the computer?

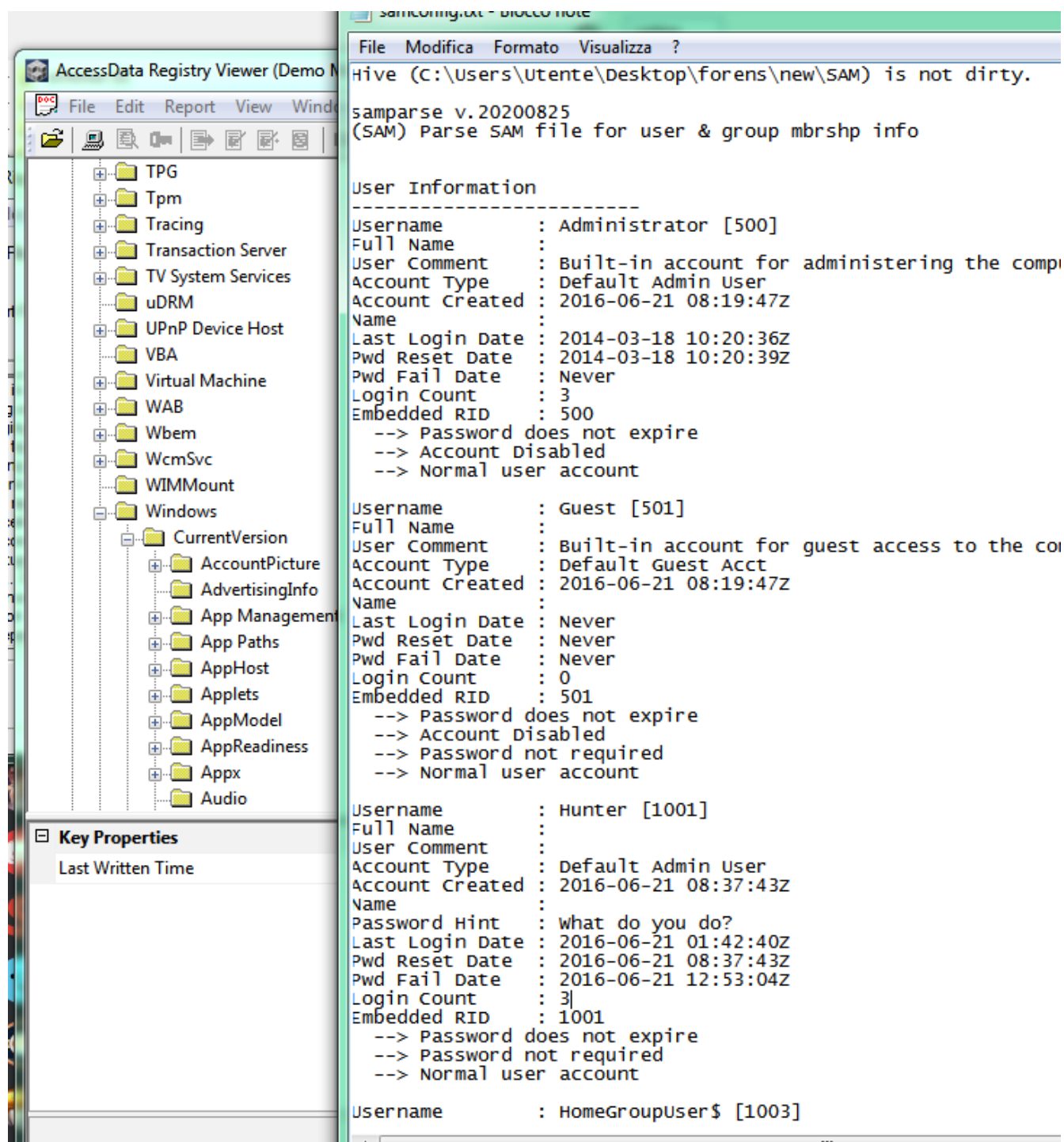


Figure 4.1

SAM registry store information about the users and how many times they have logged in. Extracting SAM and making more readable with RegRipper did the trick.

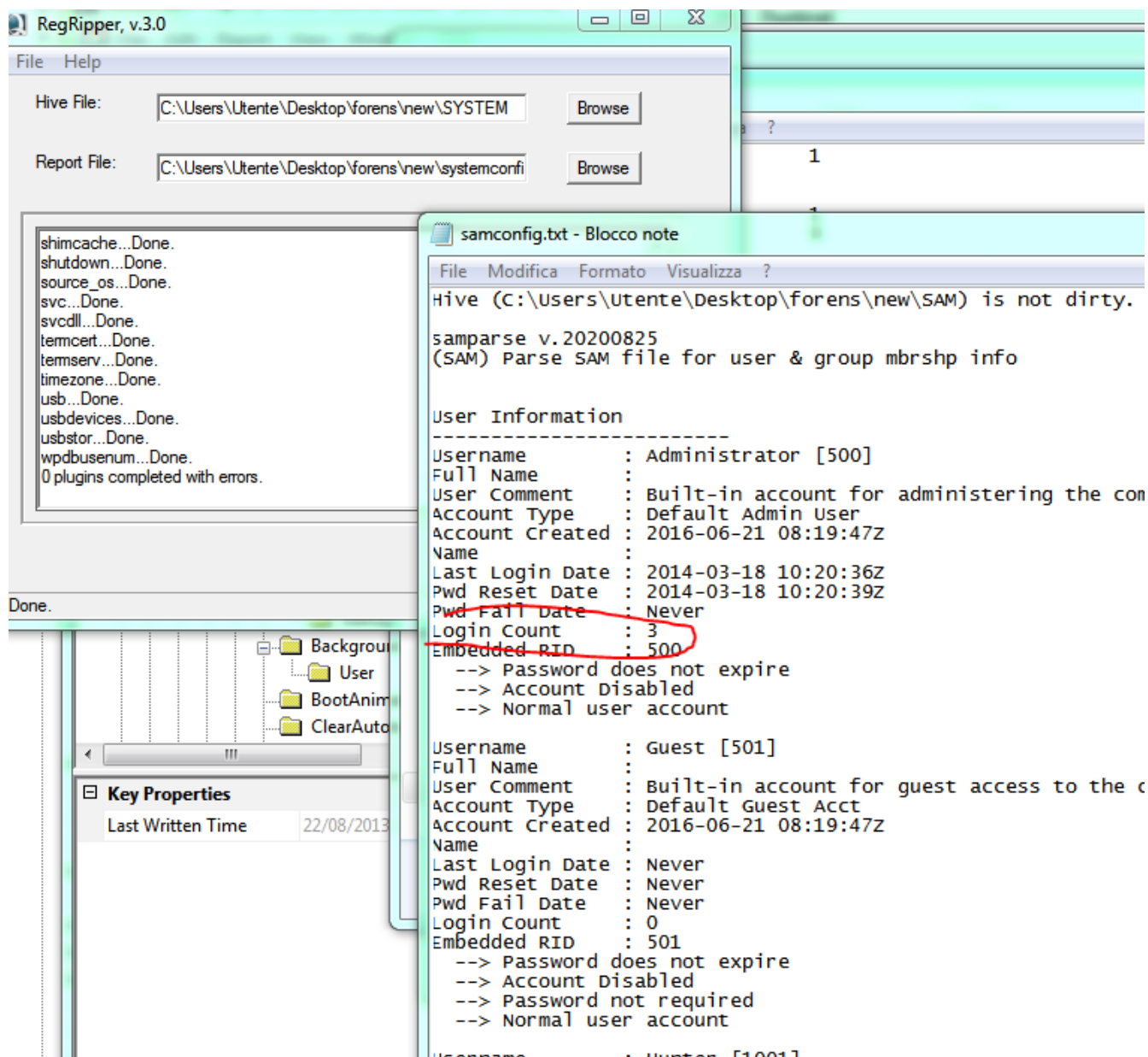


Figure 4.2

5 What is the computer SID?

This information can be found in SAM under account, using registry viewer or it can be parsed with RegRipper for a better human readable content

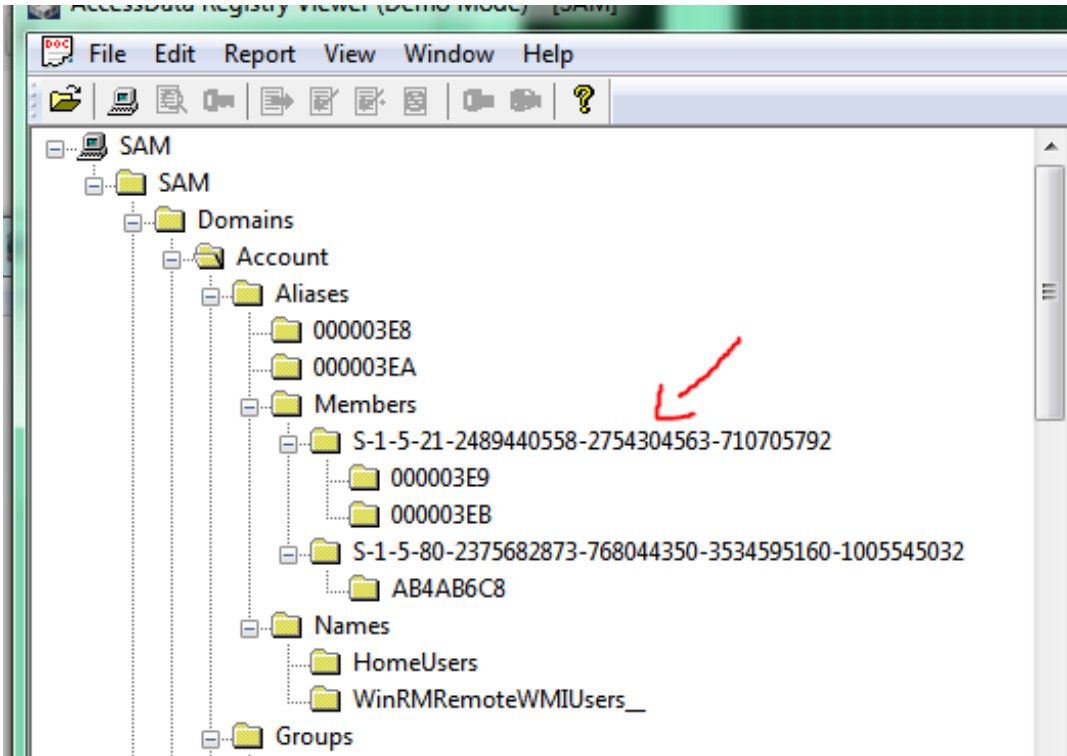


Figure 5.1

6 What is the Operating System(OS) version?

It's always in the registry, in SOFTWARE, under *WindowsNT/CurrentVersion*.

VBA	SystemRoot	REG_SZ	C:\Windows
Virtual Machine	SoftwareType	REG_SZ	System
WAB	RegisteredOwner	REG_SZ	Hunter
Wbem	InstallDate	REG_DWORD	0x5768FCD9 (1466498265)
WcmSvc	CurrentVersion	REG_SZ	6.3
WIMMount	CurrentBuild	REG_SZ	9600
Windows	RegisteredOrganization	REG_SZ	(value not set)
Windows Defender	CurrentType	REG_SZ	Multiprocessor Free
Windows Desktop Search	InstallationType	REG_SZ	Client
Windows Embedded	EditionID	REG_SZ	Enterprise
Windows Mail	ProductName	REG_SZ	Windows 8.1 Enterprise
Windows Media Device Manager	ProductId	REG_SZ	00261-30000-00000-AA825
Windows Media Foundation	DigitalProductId	REG_BINARY	A4 00 00 00 03 00 00 00 30 32 36 31 2D 33 30 30 30 ...
Windows Media Player NSS	DigitalProductId4	REG_BINARY	F8 04 00 00 04 00 00 00 30 00 30 00 30 00 30 00 2...
Windows Messaging Subsystem	CurrentBuildNumber	REG_SZ	9600
Windows NT	BuildLab	REG_SZ	9600.winblue_gdr.140221-1952
CurrentVersion	BuildLabEx	REG_SZ	9600.17031.amd64fre.winblue_gdr.140221-1952
Windows Photo Viewer	BuildGUID	REG_SZ	ffffffff-ffff-ffff-ffff-ffffffffffff
Windows Portable Devices	PathName	REG_SZ	C:\Windows
Windows Script Host			
Windows Search			
WindowsRuntime			
Wisp			

Figure 6.1

7 What was the computer timezone?

Time zone bias is stored as a number of minutes to be added to the local time to set it back to UTC. ... If the number is positive, it is simply added. Not so, if the number is negative. Answer to 7 is UTC-07:00

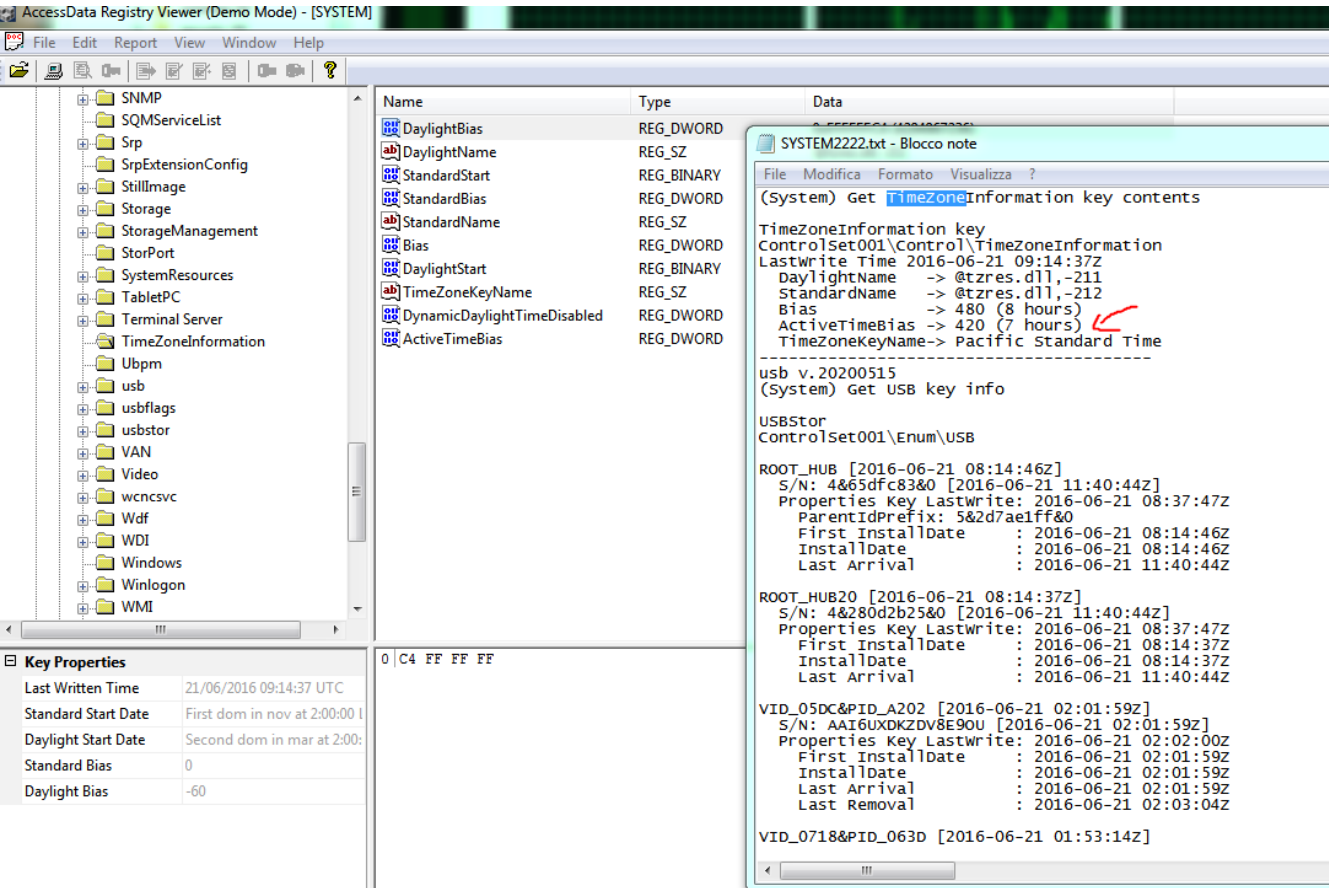


Figure 7.1

8 When was the last login time for the discovered account?

This information is stored in SAM. Using the same "ripped" file from the before is fine.

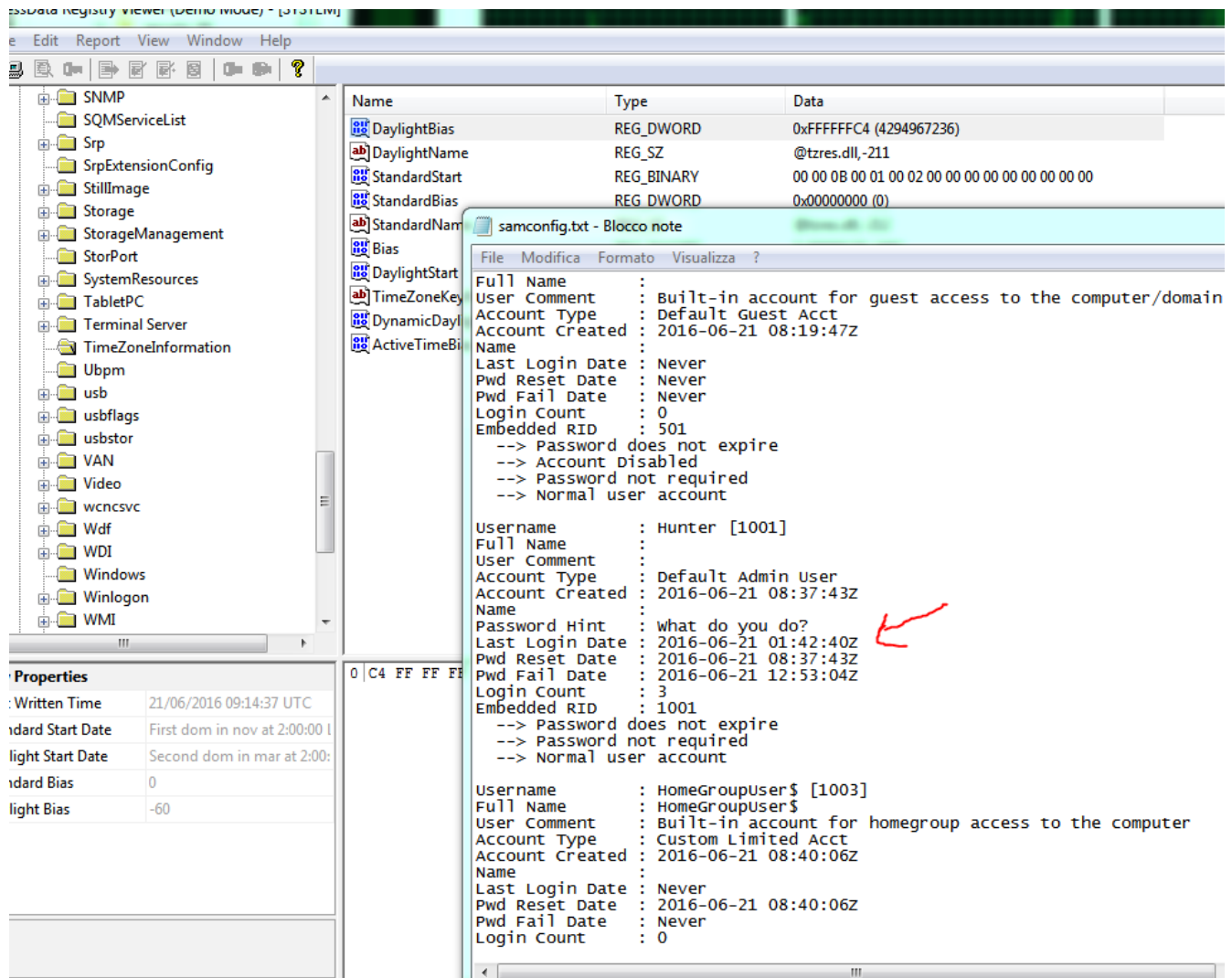


Figure 8.1

9 There was a "Network Scanner" running on this computer, what was it? And when was the last time the suspect used it?

From the installed programs, it's in plain view both nmap and the .zenmap data folder for the hunter account. The execution time is specified in the run programs functionality of autopsy.

Source File	S	C	Program Name	Username	Date/Time	Bytes Sent	Bytes Received	Comment
BCWIPE.EXE-36F3F2C			BCWIPE.EXE		2016-06-21 14:01:35 CEST			Prefetch File
CCLEANER.EXE-D4D7			CCLEANER.EXE		2016-06-21 14:01:44 CEST			Prefetch File
CCLEANER.EXE-D4D7			CCLEANER.EXE		2016-06-21 14:01:44 CEST			Prefetch File
CCLEANER64.EXE-775			CCLEANER64.EXE		2016-06-21 14:01:44 CEST			Prefetch File
CCLEANER64.EXE-775			CCLEANER64.EXE		2016-06-21 14:01:44 CEST			Prefetch File
BCWIPE.EXE-36F3F2C			BCWIPE.EXE		2016-06-21 14:02:35 CEST			Prefetch File
CONSENT.EXE-5318D			CONSENT.EXE		2016-06-21 14:02:38 CEST			Prefetch File
BCWIPE.EXE-36F3F2C			BCWIPE.EXE		2016-06-21 14:02:39 CEST			Prefetch File
CMD.EXE-4A81B364.p			CMD.EXE		2016-06-21 14:02:43 CEST			Prefetch File
VSSADMIN.EXE-9FF2C			VSSADMIN.EXE		2016-06-21 14:02:43 CEST			Prefetch File
TEAMVIEWER_DESKTOP			TEAMVIEWER_DESKTOP.EXE		2016-06-21 14:05:31 CEST			Prefetch File
ZENMAP.EXE-56B17C			ZENMAP.EXE		2016-06-21 14:08:13 CEST			Prefetch File
CONHOST.EXE-1F3E9			CONHOST.EXE		2016-06-21 14:10:42 CEST			Prefetch File
NMAP.EXE-50E1AF31			NMAP.EXE		2016-06-21 14:10:42 CEST			Prefetch File
NMAP.EXE-50E1AF31			NMAP.EXE		2016-06-21 14:10:51 CEST			Prefetch File
MPCMDRUN.EXE-F401			MPCMDRUN.EXE		2016-06-21 14:11:08 CEST			Prefetch File
MPCMDRUN.EXE-F401			MPCMDRUN.EXE		2016-06-21 14:11:08 CEST			Prefetch File
THUMBNAILEXTRACTI			THUMBNAILEXTRACTIONHOST.EXE		2016-06-21 14:14:03 CEST			Prefetch File
MSHTA.EXE-854F684			MSHTA.EXE		2016-06-21 14:14:38 CEST			Prefetch File

CEST
is 2h less
than UTC

Figure 9.1

Hunter2 - Autopsy 4.16.0

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing
/img_c16+Hunter/Program Files (x86)/Nmap

Name	S	C	Modified Time	Change Time	Access Time
NDIFF_README			2016-03-29 17:41:16 CEST	2016-06-21 13:02:35 CEST	2016-06-2
nmap-mac-prefixes			2016-03-16 16:30:14 CET	2016-06-21 13:01:38 CEST	2016-06-2
nmap-os-db			2016-03-22 05:15:50 CET	2016-06-21 13:01:38 CEST	2016-06-2
nmap-payloads			2016-03-29 17:36:06 CEST	2016-06-21 13:01:38 CEST	2016-06-2
nmap-protocols			2016-03-16 16:30:14 CET	2016-06-21 13:01:38 CEST	2016-06-2
nmap-rpc			2016-03-16 16:29:52 CET	2016-06-21 13:01:38 CEST	2016-06-2
nmap-service-probes			2016-03-29 17:36:06 CEST	2016-06-21 13:01:38 CEST	2016-06-2
nmap-services			2016-03-22 05:15:52 CET	2016-06-21 13:01:38 CEST	2016-06-2
nmap-update.exe			2016-03-29 17:40:40 CEST	2016-06-21 13:02:38 CEST	2016-06-2
nmap.exe			2016-03-29 17:38:30 CEST	2016-06-21 13:01:38 CEST	2016-06-2
nmap.xsl			2016-03-16 16:30:06 CET	2016-06-21 13:01:38 CEST	2016-06-2
nmap_performance.reg			2016-03-16 16:29:22 CET	2016-06-21 13:02:03 CEST	2016-06-2
nping.exe			2016-03-29 17:40:40 CEST	2016-06-21 13:02:38 CEST	2016-06-2
nse_main.lua			2016-03-16 16:29:38 CET	2016-06-21 13:01:38 CEST	2016-06-2
python27.dll			2016-03-29 17:41:16 CEST	2016-06-21 13:02:35 CEST	2016-06-2
README-WIN32			2016-03-16 16:37:24 CET	2016-06-21 13:01:38 CEST	2016-06-2
ssleay32.dll			2016-03-16 16:26:16 CET	2016-06-21 13:01:38 CEST	2016-06-2
Uninstall.exe			2016-06-21 13:02:01 CEST	2016-06-21 13:02:01 CEST	2016-06-2
zenmap.exe			2016-03-29 17:41:16 CEST	2016-06-21 13:06:18 CEST	2016-06-2
ZENMAP_README			2016-03-29 17:41:16 CEST	2016-06-21 13:02:03 CEST	2016-06-2

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Figure 9.2

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing
/img_c16-Hunter/Users/Hunter/.zenmap

Table Thumbnail

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]			2016-06-21 14:14:11 CEST	2016-06-21 14:14:11 CEST	2016-06-21 14:14:11 CEST	2016-06-21 14:08:14 CEST	56
[parent folder]			2016-06-21 14:26:19 CEST	2016-06-21 14:26:19 CEST	2016-06-21 14:26:19 CEST	2016-11-29 09:54:34 CET	256
recent_scans.txt			2016-06-21 14:13:57 CEST	2016-06-21 14:13:57 CEST	2016-06-21 14:08:14 CEST	2016-06-21 14:08:14 CEST	36
scan_profile.usp			2016-06-21 14:08:14 CEST	2016-06-21 14:08:14 CEST	2016-06-21 14:08:14 CEST	2016-06-21 14:08:14 CEST	2018
target_list.txt			2016-06-21 14:10:42 CEST	2016-06-21 14:10:42 CEST	2016-06-21 14:08:14 CEST	2016-06-21 14:08:14 CEST	15
zenmap.conf			2016-06-21 14:14:11 CEST	2016-06-21 14:14:11 CEST	2016-06-21 14:08:14 CEST	2016-06-21 14:08:14 CEST	1571
zenmap.db			2016-06-21 14:14:11 CEST	2016-06-21 14:14:11 CEST	2016-06-21 14:14:11 CEST	2016-06-21 14:14:11 CEST	27648
zenmap_version			2016-06-21 14:08:14 CEST	2016-06-21 14:08:14 CEST	2016-06-21 14:08:14 CEST	2016-06-21 14:08:14 CEST	5

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Table scans 2 entries Page 1 of 1 Export to CSV

scans_id	scan_name	nmap_xml_output	digest
1	nmap -T4 -A -v scanme.nmap.org	<?xml version="1.0" encoding="iso-8859-1"?><?xmlstylesheet href="file:///C:/Program Files (x86)..."	
2	nmap -T4 -A -v scanme.nmap.org	<?xml version="1.0" encoding="iso-8859-1"?><?xmlstylesheet href="file:///C:/Program Files (x86)..."	

Figure 9.3

10 When did the port scan start and end?

In the application data of zenmap there is the scan_results a path to the xml

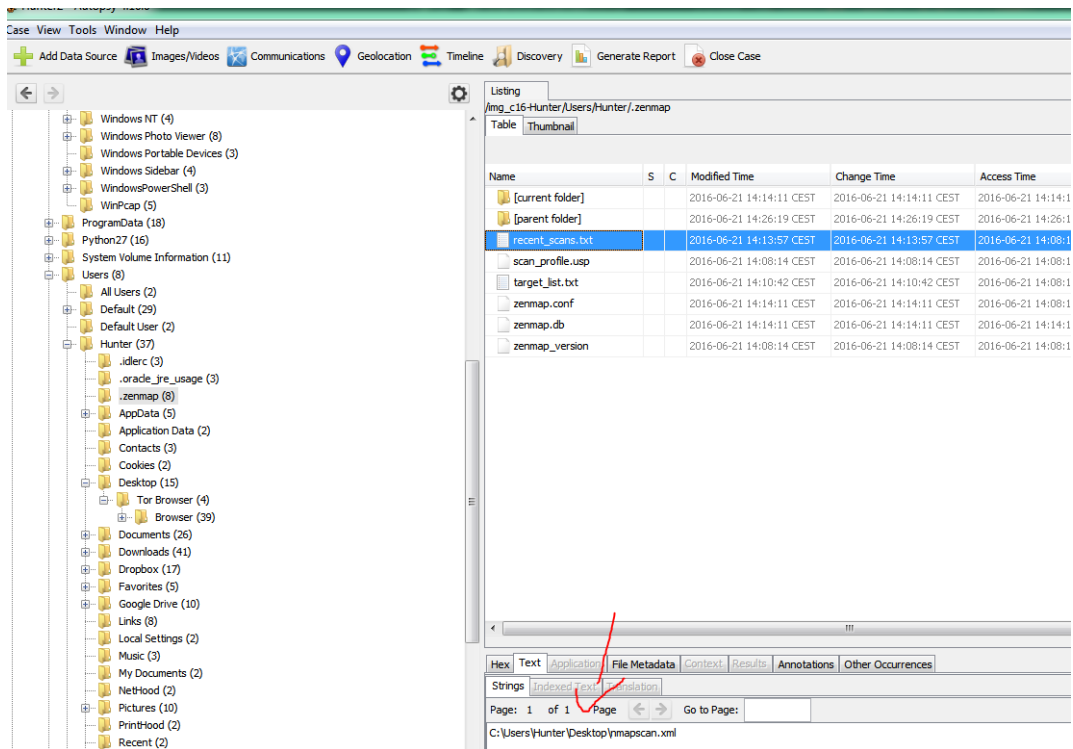


Figure 10.1

11 How many ports were scanned?

Take the xml in the desktop and beautify it using an online tool

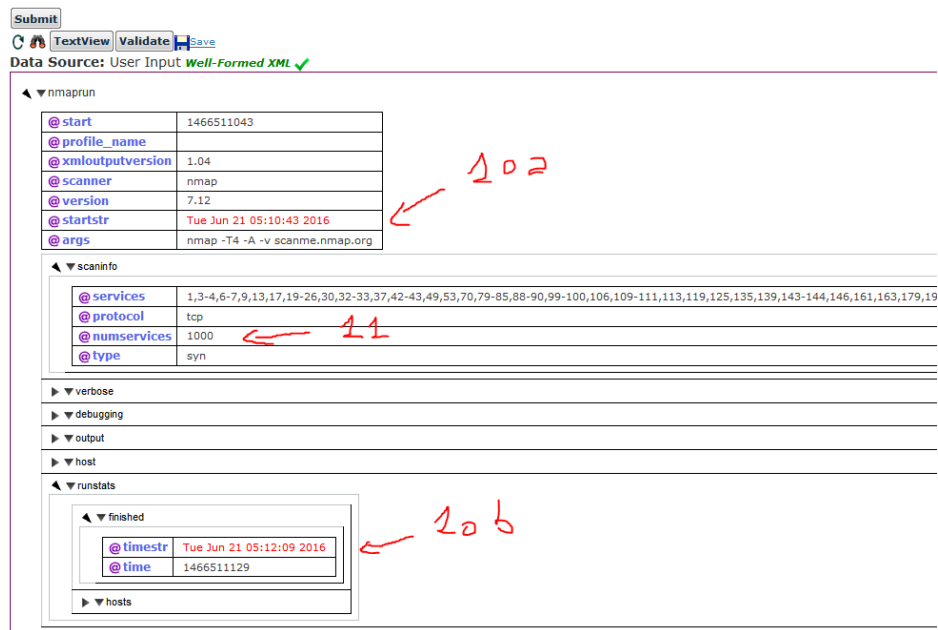


Figure 11.1

12 What ports were found "open"?

In the xml too

```
OS:=Y%DF=N%T=41%W=FFFF%O=M5B4%CC=N%Q=)ECN(R=N)T1(R=Y%DF=N%T=41%S=O%A=S+%F=A OS:S%RD=O%Q=)T2(R=Y%DF=N%T=100%W=O%S=Z%A=S%F=AR%O=%RD=O%
%O=%RD=O%Q=)T4(R=Y%DF=N%T=100%W=O%S=A%A=Z%F=R%O=%RD=O OS:%Q=)T5(R=Y%DF=N%T=100%W=O%S=Z%A=S+%F=AR%O=%RD=O%Q=)T6(R=Y%DF=N%T=100%W=O
%O=%RD=O%Q=)U1 OS:(R=Y%DF=N%T=34%IPL=164%UN=O%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=N) Network Distance: 2 hops Service Info: OS: Linux; CPE: cpe:/o:linux
scanme.nmap.org (45.33.32.156) NSE: Script Post-scanning. Initiating NSE at 05:12 Completed NSE at 05:12, 0.00s elapsed Initiating NSE at 05:12 Completed NSE at 05:12, 0.00s elapsed
report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 87.13 seconds +++++ Raw packets sent: 1331 (66.198KB) | Rcvd: 1445 (64.387k
[<host comment="">
  <status state="up"></status>
  <address addrtype="ipv4" vendor="" addr="45.33.32.156"></address>
  <hostnames>
    <hostname type="user" name="scanme.nmap.org"></hostname>
    <hostname type="PTR" name="scanme.nmap.org"></hostname>
  </hostnames>
  <ports>
    <extraports count="994" state="closed"></extraports>
    <port protocol="tcp" portid="22">
      <state reason="syn-ack" state="open" reason_ttl="64"></state>
      <service product="OpenSSH" name="ssh" extrainfo="Ubuntu Linux; protocol 2.0" version="6.6.1p1 Ubuntu 2ubuntu2.7" conf="10" method="probed"></service>
    </port>
    <port protocol="tcp" portid="25">
      <state reason="no-response" state="filtered" reason_ttl="0"></state>
      <service method="table" conf="3" name="smtp"></service>
    </port>
    <port protocol="tcp" portid="26">
      <state reason="no-response" state="filtered" reason_ttl="0"></state>
      <service method="table" conf="3" name="rsftp"></service>
    </port>
    <port protocol="tcp" portid="80">
      <state reason="syn-ack" state="open" reason_ttl="64"></state>
      <service product="Apache httpd" name="http" extrainfo="(Ubuntu)" version="2.4.7" conf="10" method="probed"></service>
    </port>
    <port protocol="tcp" portid="9929">
      <state reason="syn-ack" state="open" reason_ttl="64"></state>
      <service product="Nping echo" method="probed" conf="10" name="nping-echo"></service>
    </port>
    <port protocol="tcp" portid="31337">
      <state reason="syn-ack" state="open" reason_ttl="64"></state>
      <service product="Ncat chat" extrainfo="users: nobody" method="probed" conf="10" name="ncat-chat"></service>
    </port>
  </ports>
  <os>
```

Figure 12.1

13 The employee engaged in a Skype conversation with someone. What is the skype username of the other party?

Opening the main db (with db browser) of skype there was a chat table and in that table there were the two name of the chat files. In these chats there were the information requested.

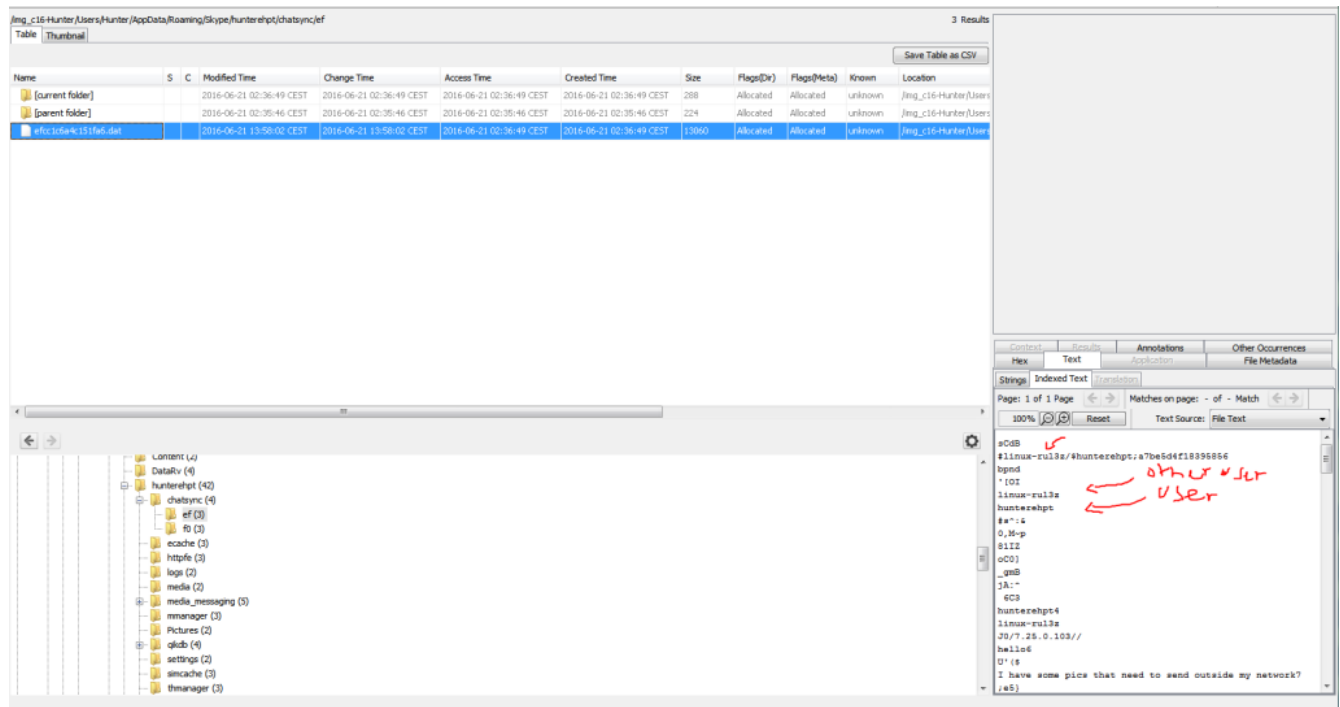


Figure 13.1

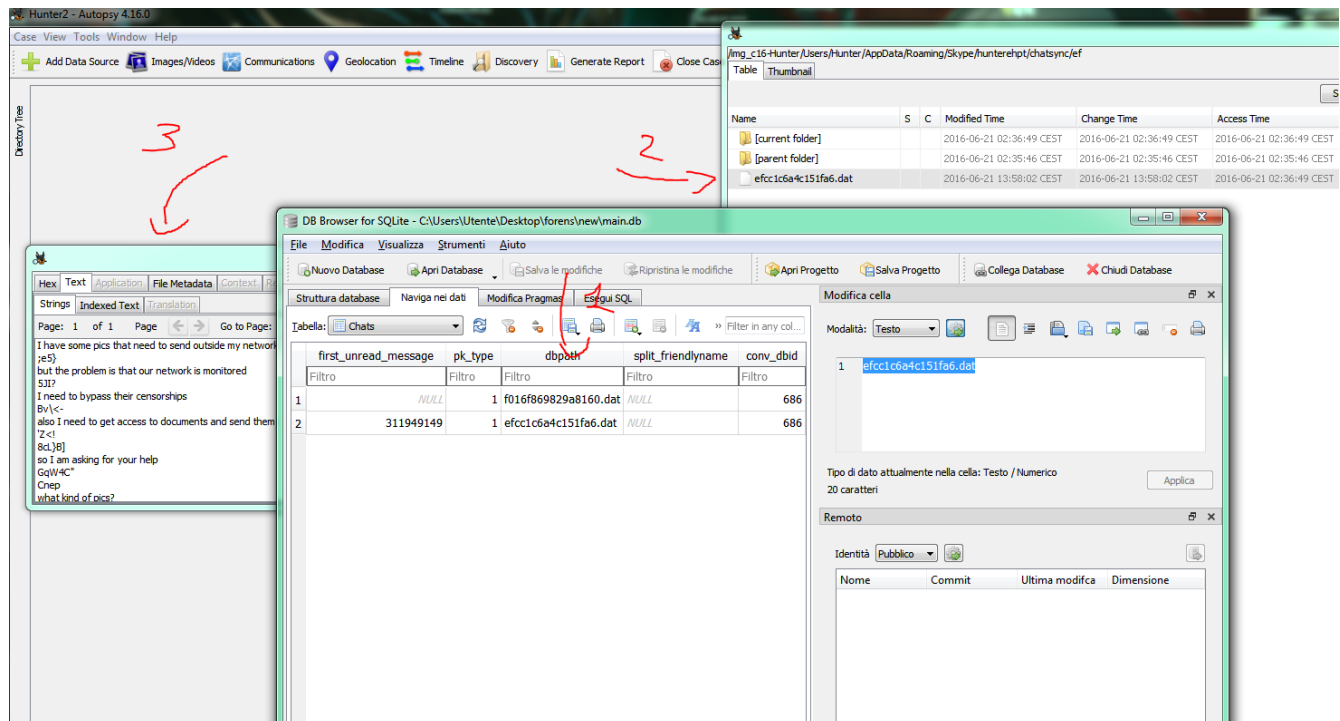


Figure 13.2

14 What is the name of the application both parties agreed to use to exfiltrate data and provide remote access for the external attacker in their Skype conversation? And when did the suspect run it?

The name could be found in the skype chat meanwhile the data in the run programs tab. Noting it's in CEST time and the answer is in UTC.

Source File	S	C	Program Name	Username	Date/Time	Bytes Sent	Bytes Received	Comment	Data Source
TASKHOST.EXE-3AE21			TASKHOST.EXE		2016-06-21 14:46:14 CEST			Prefetch File	c16-Hunter
TASKHOST.EXE-7F61F			TASKHOST.EXE		2016-06-21 14:40:43 CEST			Prefetch File	c16-Hunter
TASKHOST.EXE-A83A			TASKHOST.EXE		2016-06-21 13:44:55 CEST			Prefetch File	c16-Hunter
TASKHOST.EXE-CC5C			TASKHOST.EXE		2016-06-21 14:58:06 CEST			Prefetch File	c16-Hunter
TASKHOST.EXE-CC5C			TASKHOST.EXE		2016-06-21 14:46:15 CEST			Prefetch File	c16-Hunter
TASKHOST.EXE-CC5C			TASKHOST.EXE		2016-06-21 13:43:50 CEST			Prefetch File	c16-Hunter
TASKHOST.EXE-CC5C			TASKHOST.EXE		2016-06-21 13:20:23 CEST			Prefetch File	c16-Hunter
TASKHOST.EXE-CC5C			TASKHOST.EXE		2016-06-21 13:02:49 CEST			Prefetch File	c16-Hunter
TASKHOST.EXE-CC5C			TASKHOST.EXE		2016-06-21 04:24:12 CEST			Prefetch File	c16-Hunter
TASKHOST.EXE-CC5C			TASKHOST.EXE		2016-06-21 04:13:02 CEST			Prefetch File	c16-Hunter
TASKHOST.EXE-CC5C			TASKHOST.EXE		2016-06-21 11:22:53 CEST			Prefetch File	c16-Hunter
TASKHOSTEX.EXE-28K			TASKHOSTEX.EXE		2016-06-21 14:46:14 CEST			Prefetch File	c16-Hunter
TASKHOSTEX.EXE-28K			TASKHOSTEX.EXE		2016-06-21 12:40:33 CEST			Prefetch File	c16-Hunter
TASKHOSTEX.EXE-28K			TASKHOSTEX.EXE		2016-06-21 10:48:52 CEST			Prefetch File	c16-Hunter
TASKHOSTEX.EXE-28K			TASKHOSTEX.EXE		2016-06-21 10:37:47 CEST			Prefetch File	c16-Hunter
TEAMVIEWER.EXE-F6			TEAMVIEWER.EXE		2016-06-21 14:00:43 CEST			Prefetch File	c16-Hunter
TEAMVIEWER_.EXE-C			TEAMVIEWER_.EXE		2016-06-21 02:57:29 CEST			Prefetch File	c16-Hunter
TEAMVIEWER_.EXE-C			TEAMVIEWER_.EXE		2016-06-21 02:57:21 CEST			Prefetch File	c16-Hunter

Figure 14.1

15 What is the Gmail email address of the suspect employee?

One approach it's using the database and looking for the email associated

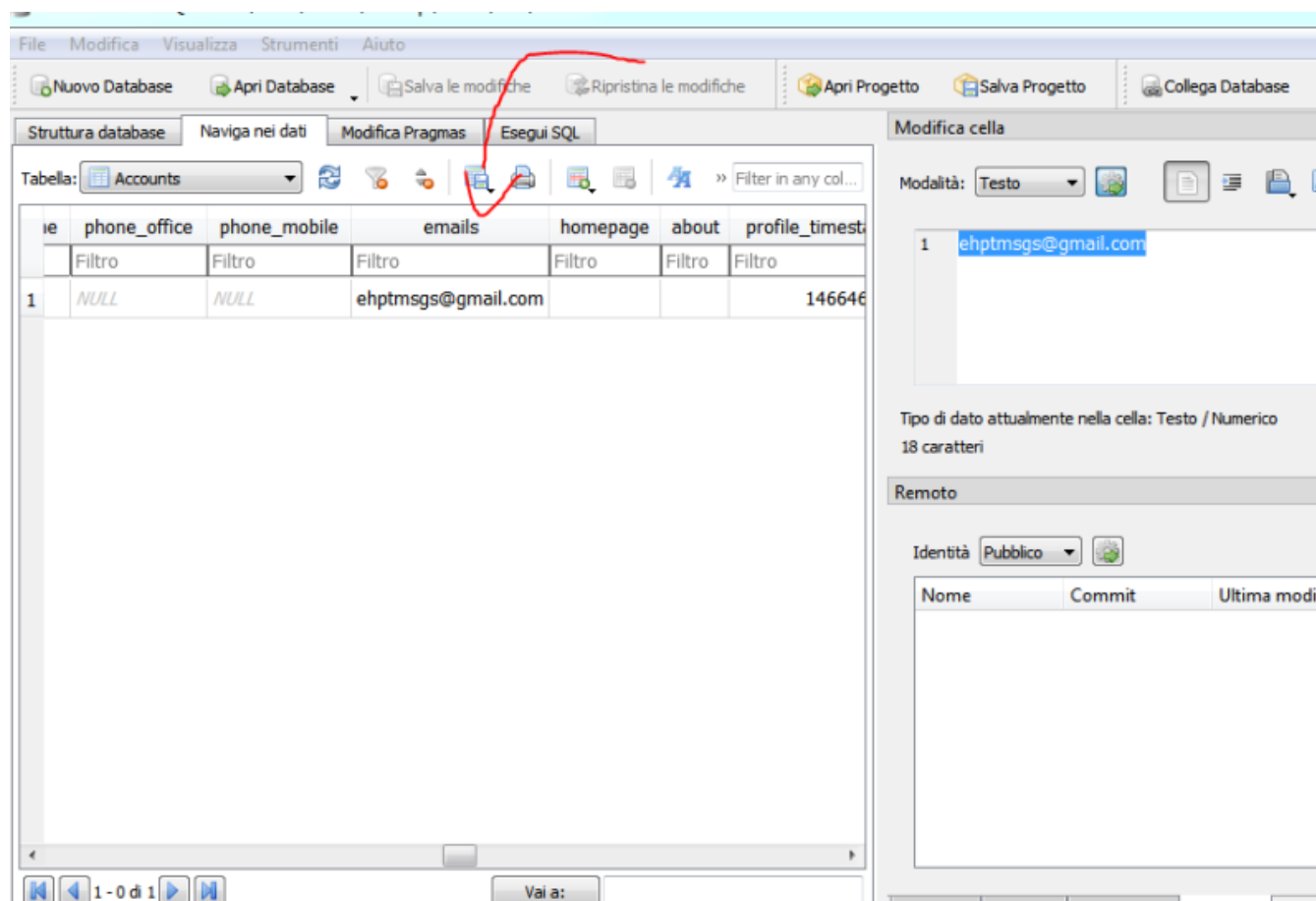


Figure 15.1

Alternatively, the emails can be found in the results section under Email addresses

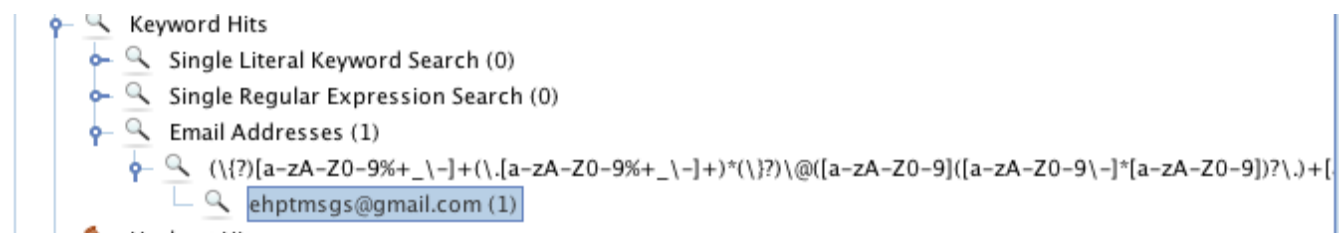


Figure 15.2

16 It looks like the suspect user deleted an important diagram after his conversation with the external attacker. What is the file name of the deleted diagram?

In the mail exchange it was visible all the flow of conversation and in one mail they were talking about this diagram, the user sent it to the outsider and then in the next reply it was wondering about deleting it to remain undetected

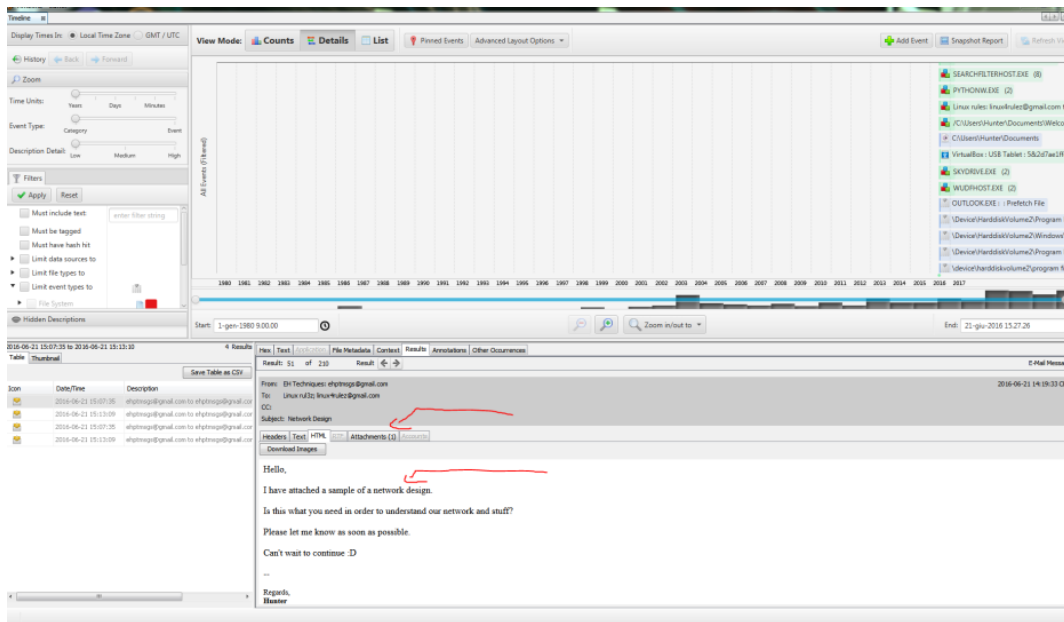


Figure 16.1

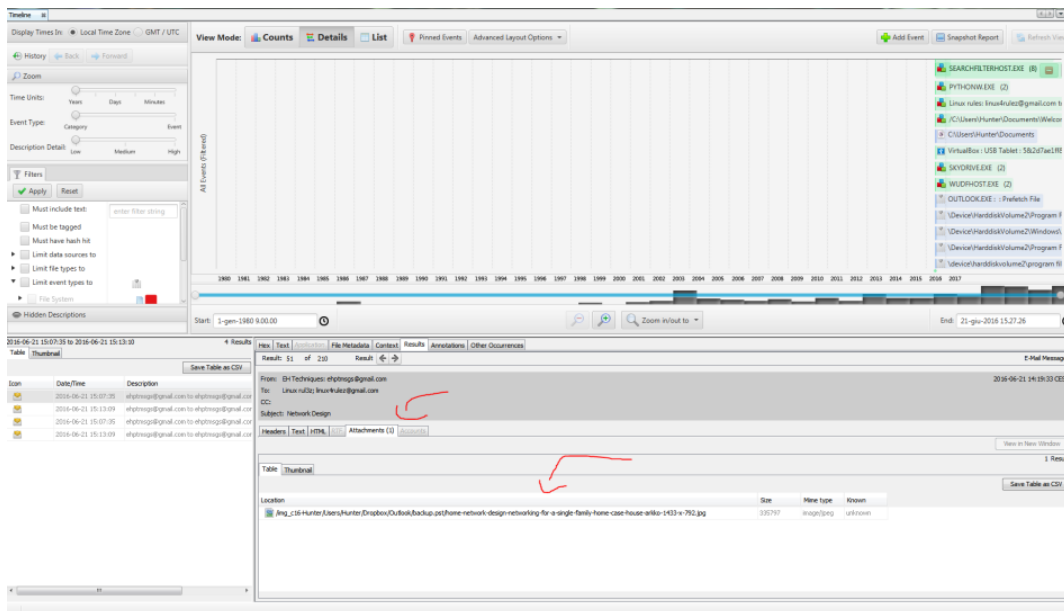


Figure 16.2

17 The user Documents' directory contained a PDF file discussing data exfiltration techniques. What is the name of the file?

This was just about retrieving the file.

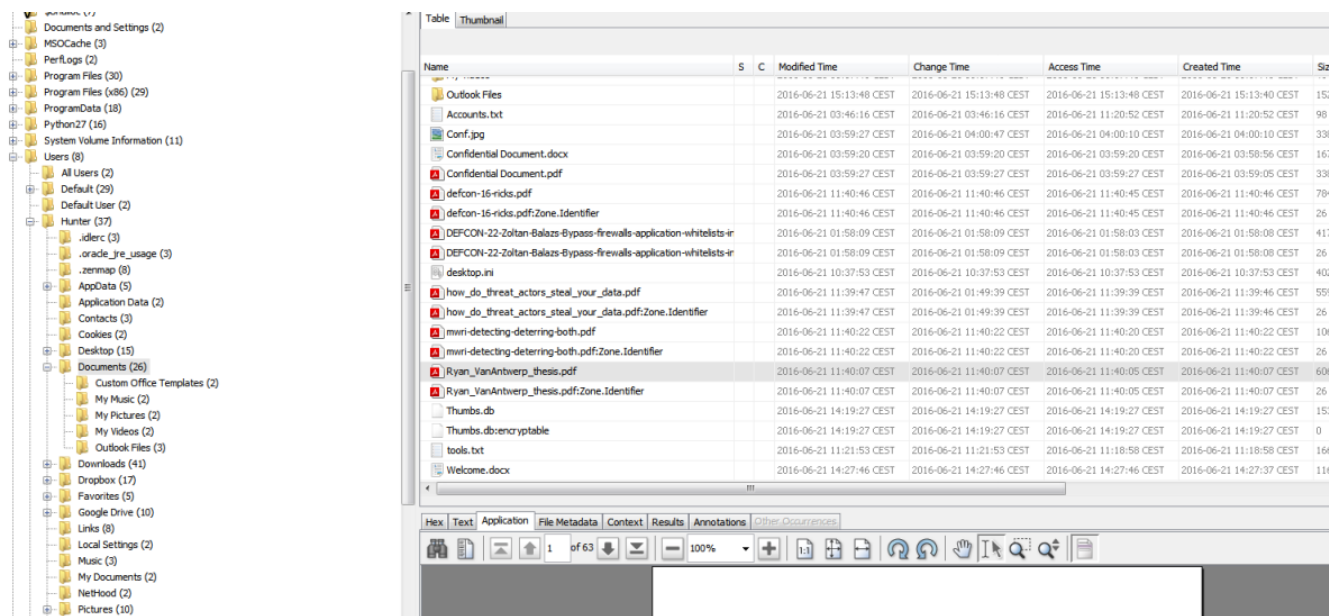
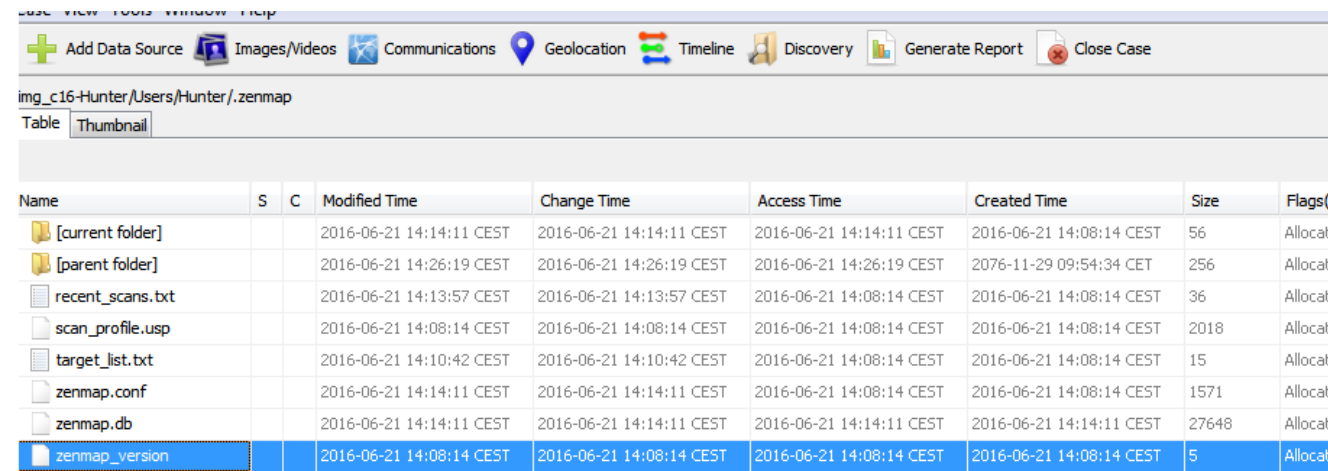


Figure 17.1

18 The suspect user downloaded a Nmap installer. What version did he download?

This information is stored in the .zenmap application data and in the zenmap_version file



Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags
[current folder]			2016-06-21 14:14:11 CEST	2016-06-21 14:14:11 CEST	2016-06-21 14:14:11 CEST	2016-06-21 14:08:14 CEST	56	Allocat
[parent folder]			2016-06-21 14:26:19 CEST	2016-06-21 14:26:19 CEST	2016-06-21 14:26:19 CEST	2016-06-21 14:08:14 CEST	256	Allocat
recent_scans.txt			2016-06-21 14:13:57 CEST	2016-06-21 14:13:57 CEST	2016-06-21 14:08:14 CEST	2016-06-21 14:08:14 CEST	36	Allocat
scan_profile.usp			2016-06-21 14:08:14 CEST	2016-06-21 14:08:14 CEST	2016-06-21 14:08:14 CEST	2016-06-21 14:08:14 CEST	2018	Allocat
target_list.txt			2016-06-21 14:10:42 CEST	2016-06-21 14:10:42 CEST	2016-06-21 14:08:14 CEST	2016-06-21 14:08:14 CEST	15	Allocat
zenmap.conf			2016-06-21 14:14:11 CEST	2016-06-21 14:14:11 CEST	2016-06-21 14:08:14 CEST	2016-06-21 14:08:14 CEST	1571	Allocat
zenmap.db			2016-06-21 14:14:11 CEST	2016-06-21 14:14:11 CEST	2016-06-21 14:14:11 CEST	2016-06-21 14:14:11 CEST	27648	Allocat
zenmap_version			2016-06-21 14:08:14 CEST	2016-06-21 14:08:14 CEST	2016-06-21 14:08:14 CEST	2016-06-21 14:08:14 CEST	5	Allocat

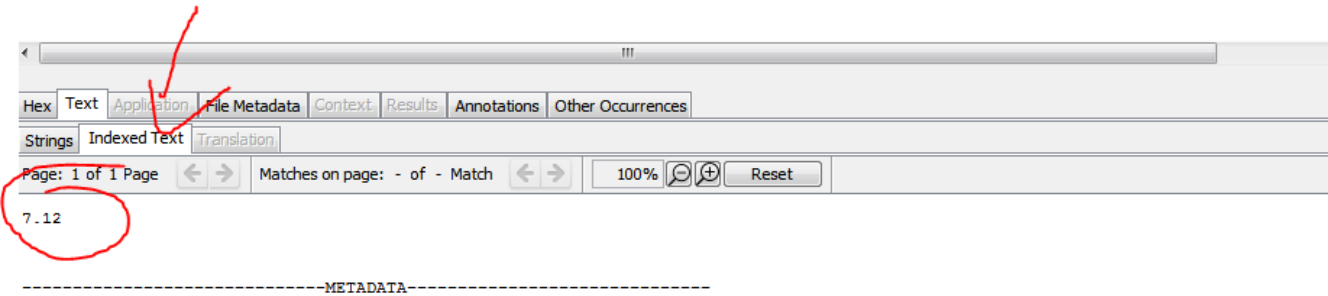


Figure 18.1

Looking for the answer in the programs manually

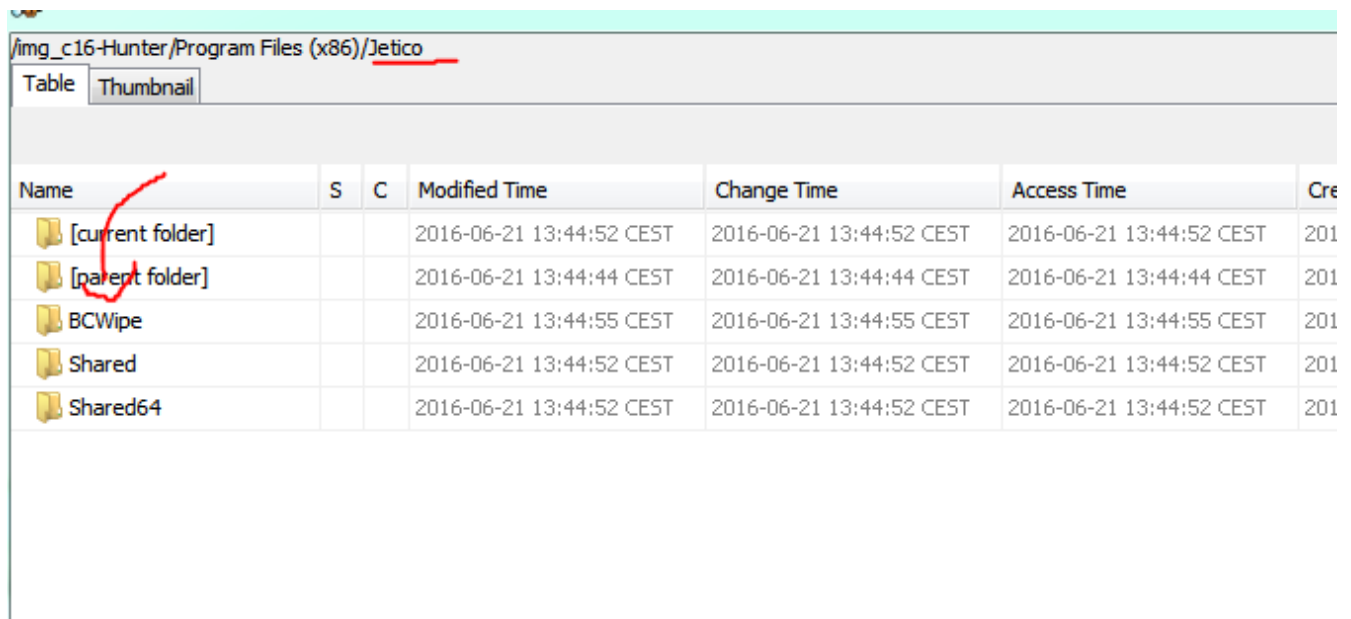
Figure 19.1

This information it's in the usb device tab of autopsy.

Figure 20.1

21 One of the installed applications is a file shredder. What is the name of the application?

Looking for the answer in the programs manually



Name	S	C	Modified Time	Change Time	Access Time	Cre
[current folder]			2016-06-21 13:44:52 CEST	2016-06-21 13:44:52 CEST	2016-06-21 13:44:52 CEST	201
[parent folder]			2016-06-21 13:44:44 CEST	2016-06-21 13:44:44 CEST	2016-06-21 13:44:44 CEST	201
BCWipe			2016-06-21 13:44:55 CEST	2016-06-21 13:44:55 CEST	2016-06-21 13:44:55 CEST	201
Shared			2016-06-21 13:44:52 CEST	2016-06-21 13:44:52 CEST	2016-06-21 13:44:52 CEST	201
Shared64			2016-06-21 13:44:52 CEST	2016-06-21 13:44:52 CEST	2016-06-21 13:44:52 CEST	201

Figure 21.1

22 How many prefetch files were discovered on the system?

In the prefetch folder there are 222 file, but they are not all .pf because there are two folders (current folder, parent folder and a third one named ReadyBoot) and some .ini and .db files. Doing the math will have the answer revealed.

$$222 - 48 = 174$$

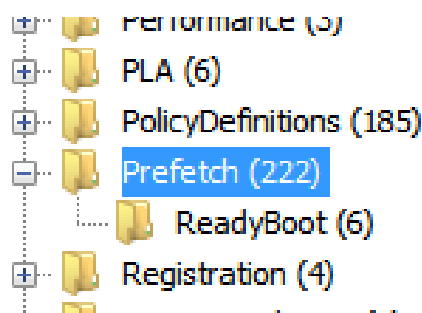


Figure 22.1

<div> Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case </div>					
/img_c16-Hunter/Windows/Prefetch					222 Results
<div> <div>Table</div> <div>Thumbnail</div> <div>Save Table as CSV</div> </div>					
Name	S	C	Modified Time	Change Time	Access
[current folder]			2016-06-21 15:17:51 CEST	2016-06-21 15:17:51 CEST	2016-0
[parent folder]			2016-06-21 14:46:24 CEST	2016-06-21 14:46:24 CEST	2016-0
Readyboot			2016-06-21 03:42:19 CEST	2016-06-21 03:42:19 CEST	2016-0
7Z1602-X64.EXE-9254A0E7.pf			2016-06-21 11:18:15 CEST	2016-06-21 03:41:51 CEST	2016-0
7ZPM.EXE-69B8961D.pf			2016-06-21 11:43:06 CEST	2016-06-21 03:41:51 CEST	2016-0
7ZG.EXE-0F8C4081.pf			2016-06-21 13:48:10 CEST	2016-06-21 13:48:10 CEST	2016-0
ACRORD32.EXE-ACF2947E.pf			2016-06-21 04:00:10 CEST	2016-06-21 04:00:10 CEST	2016-0
AgAppLaunch.db			2016-06-21 10:15:54 CEST	2016-06-21 03:41:51 CEST	2016-0
AgCx_SC4.db			2016-06-21 03:43:42 CEST	2016-06-21 03:43:42 CEST	2016-0
AgGIFaultHistory.db			2016-06-21 15:08:06 CEST	2016-06-21 15:08:06 CEST	2016-0
AgGIFgAppHistory.db			2016-06-21 15:08:06 CEST	2016-06-21 15:08:06 CEST	2016-0
AgGIGlobalHistory.db			2016-06-21 15:08:06 CEST	2016-06-21 15:08:06 CEST	2016-0
AgGLUAD_P_S-1-5-21-2489440558-2754304563-710705792-1001.			2016-06-21 14:59:07 CEST	2016-06-21 14:59:07 CEST	2016-0
AgGLUAD_S-1-5-21-2489440558-2754304563-710705792-1001.de			2016-06-21 14:59:07 CEST	2016-06-21 14:59:07 CEST	2016-0
AgRobust.db			2016-06-21 15:08:05 CEST	2016-06-21 15:08:05 CEST	2016-0
BCRESIDENT.EXE-7CE7A88C.pf			2016-06-21 13:45:03 CEST	2016-06-21 13:45:03 CEST	2016-0
BCWIPE.EXE-36F3F2DF.pf			2016-06-21 14:02:45 CEST	2016-06-21 14:02:45 CEST	2016-0
BCWIPESETUP.EXE-AB2C77E1.pf			2016-06-21 13:44:42 CEST	2016-06-21 13:44:42 CEST	2016-0
BCWIPESVC.EXE-64B3C913.pf			2016-06-21 13:45:01 CEST	2016-06-21 13:45:01 CEST	2016-0
BCWIPETM.EXE-7A3038F4.pf			2016-06-21 13:45:01 CEST	2016-06-21 13:45:01 CEST	2016-0
BSPATCH.EXE-0D9E5E46.pf			2016-06-21 13:22:39 CEST	2016-06-21 13:22:39 CEST	2016-0
CALC.EXE-77FDF17F.pf			2016-06-21 01:54:12 CEST	2016-06-21 03:41:51 CEST	2016-0
COLEANER.EXE-D4D76A60.pf			2016-06-21 14:28:08 CEST	2016-06-21 14:28:08 CEST	2016-0
COLEANER64.EXE-7798D542.pf			2016-06-21 14:28:17 CEST	2016-06-21 14:28:17 CEST	2016-0
CCSETUP519PRO.EXE-80E552SD.pf			2016-06-21 13:44:28 CEST	2016-06-21 13:44:28 CEST	2016-0
CHROME.EXE-D999B1BA.pf			2016-06-21 14:52:33 CEST	2016-06-21 14:52:33 CEST	2016-0
CHROME.EXE-D999B1BB.pf			2016-06-21 15:12:12 CEST	2016-06-21 15:12:12 CEST	2016-0
CHROME.EXE-D999B1BC.pf			2016-06-21 14:52:36 CEST	2016-06-21 14:52:36 CEST	2016-0
CHROME.EXE-D999B1BD.pf			2016-06-21 11:46:00 CEST	2016-06-21 03:41:51 CEST	2016-0
CHROME.EXE-D999B1C1.pf			2016-06-21 14:52:33 CEST	2016-06-21 14:52:33 CEST	2016-0
CHROME.EXE-D999B1C2.pf			2016-06-21 14:52:26 CEST	2016-06-21 14:52:26 CEST	2016-0
CMD.EXE-4A81B364.pf			2016-06-21 14:02:43 CEST	2016-06-21 14:02:43 CEST	2016-0
CMD.EXE-AC113AA8.pf			2016-06-21 13:22:53 CEST	2016-06-21 13:22:53 CEST	2016-0

Figure 22.2

23 How many times was the file shredder application executed?

The file shredder found was executed 5 times like shown in the count of the prefetch file about that program

The screenshot shows a forensic tool interface with two main panes. The left pane displays file metadata for a prefetch file, and the right pane displays a list of prefetch files.

Left Pane: File Metadata

Type	Value	Source(s)
Program N	BCWIPE.EXE	Windows P
Date/Time	2016-06-21 14:02:35	Windows P
Count	5	Windows P
Comment	Prefetch File	Windows P
Source File	/img_c16-Hunter/Windows/Prefetch/BCWIPE.EXE-36F3F2DF.pf	
Artifact ID	-9223372036854762239	

Right Pane: Prefetch Files

Name	S	C	Modified Time	Change Time	Accu
ALUKUKU32.CAC-PLF-277C.pf			2016-06-21 09:00:10 CEST	2016-06-21 09:00:10 CEST	2016
AgAppLaunch.db			2016-06-21 10:15:54 CEST	2016-06-21 03:41:51 CEST	2016
AgCx_SC4.db			2016-06-21 03:43:42 CEST	2016-06-21 03:43:42 CEST	2016
AgGFAuthHistory.db			2016-06-21 15:08:06 CEST	2016-06-21 15:08:06 CEST	2016
AgGFgAppHistory.db			2016-06-21 15:08:06 CEST	2016-06-21 15:08:06 CEST	2016
AgGGlobalHistory.db			2016-06-21 15:08:06 CEST	2016-06-21 15:08:06 CEST	2016
AgGLUAD_P_S-1-5-21-2489440558-2754304563-710705792-1001			2016-06-21 14:59:07 CEST	2016-06-21 14:59:07 CEST	2016
AgGLUAD_S-1-5-21-2489440558-2754304563-710705792-1001.db			2016-06-21 14:59:07 CEST	2016-06-21 14:59:07 CEST	2016
AgRobust.db			2016-06-21 15:08:05 CEST	2016-06-21 15:08:05 CEST	2016
BCRESIDENT.EXE-7CE7A88C.pf			2016-06-21 13:45:03 CEST	2016-06-21 13:45:03 CEST	2016
BCWIPE.EXE-36F3F2DF.pf			2016-06-21 14:02:45 CEST	2016-06-21 14:02:45 CEST	2016
BCWIPESETUP.EXE-AB2C77E1.pf			2016-06-21 13:44:42 CEST	2016-06-21 13:44:42 CEST	2016
BCWIPESVC.EXE-64B3C913.pf			2016-06-21 13:45:01 CEST	2016-06-21 13:45:01 CEST	2016
BCWIPETM.EXE-7A3038F4.pf			2016-06-21 13:45:01 CEST	2016-06-21 13:45:01 CEST	2016
BSPATCH.EXE-DD9E5E46.pf			2016-06-21 13:22:39 CEST	2016-06-21 13:22:39 CEST	2016
CALC.EXE-77FDF17F.pf			2016-06-21 01:54:12 CEST	2016-06-21 03:41:51 CEST	2016
CLEANER.EXE-D4D76A60.pf			2016-06-21 14:28:08 CEST	2016-06-21 14:28:08 CEST	2016
CLEANER64.EXE-779BD542.pf			2016-06-21 14:28:17 CEST	2016-06-21 14:28:17 CEST	2016
CCSETUP519PRO.EXE-B0E5525D.pf			2016-06-21 13:44:28 CEST	2016-06-21 13:44:28 CEST	2016
CHROME.EXE-D999B1BA.pf			2016-06-21 14:52:33 CEST	2016-06-21 14:52:33 CEST	2016
CHROME.EXE-D999B1BB.pf			2016-06-21 15:12:12 CEST	2016-06-21 15:12:12 CEST	2016
CHROME.EXE-D999B1BC.pf			2016-06-21 14:52:36 CEST	2016-06-21 14:52:36 CEST	2016
CHROME.EXE-D999B1BD.pf			2016-06-21 11:46:00 CEST	2016-06-21 03:41:51 CEST	2016

Figure 23.1

24 Using prefetch, determine when was the last time ZENMAP.EXE-56B17C4C.pf was executed?

It's in the run programs tab in plain view.

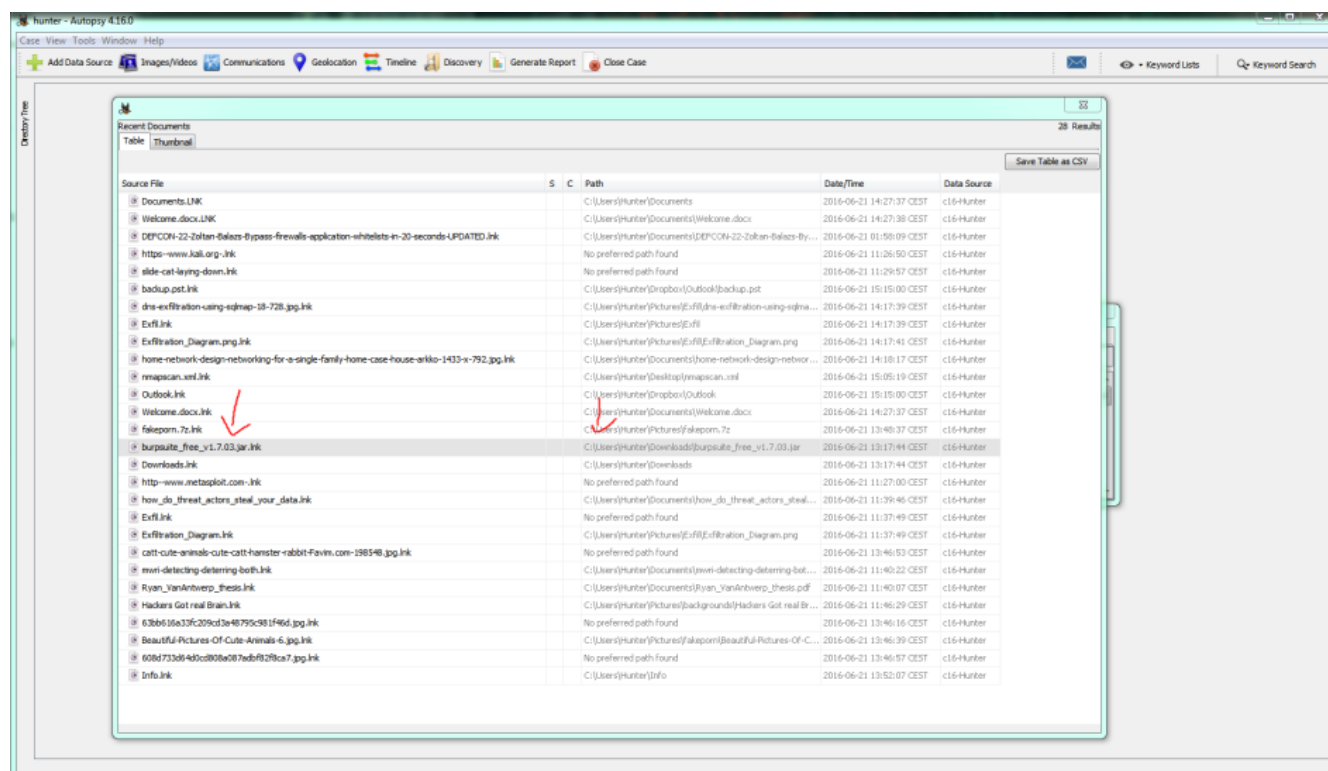
The screenshot shows a forensic tool interface with a table of run programs.

Name	S	C	Modified Time	Change Time	Accu
ZENMAP.EXE-56B17C4C.pf			2016-06-21 14:08:13 CEST	2016-06-21 14:08:13 CEST	2016
XMLUPDATER.EXE-568CAAC5.pf			2016-06-21 11:18:27 CEST	2016-06-21 11:18:27 CEST	2016
XMLUPDATER.EXE-568CAAC5.pf			2016-06-21 11:18:27 CEST	2016-06-21 11:18:27 CEST	2016
XMLUPDATER.EXE-568CAAC5.pf			2016-06-21 11:18:27 CEST	2016-06-21 11:18:27 CEST	2016

Figure 24.1

25 LNK file analysis shows that a JAR file for an offensive traffic manipulation tool was executed. What is the absolute path of the file?

In the recent document there is that .lnk too with its path.



Recent Documents

Source File	S	C	Path	Date/Time	Data Source
Documents.LNK			C:\Users\Hunter\Documents	2016-06-21 14:27:37 CEST	c16-Hunter
Welcome.docx.LNK			C:\Users\Hunter\Documents>Welcome.docx	2016-06-21 14:27:38 CEST	c16-Hunter
DPFCON-22-Zafan-Selazs-0ypass-freewall-application-whitelets-in-30-seconds-UPDATED.lnk			C:\Users\Hunter\Documents\DPFCON-22-Zafan-Selazs-By...	2016-06-21 01:58:09 CEST	c16-Hunter
https-www.jail.org.lnk			No preferred path found	2016-06-21 11:26:50 CEST	c16-Hunter
slide-cat-lying-down.lnk			No preferred path found	2016-06-21 11:29:57 CEST	c16-Hunter
backup.pst.lnk			C:\Users\Hunter\Dropbox\Outlook\backup.pst	2016-06-21 15:15:00 CEST	c16-Hunter
dns-exfiltration-using-sdmap-18-728.jpg.lnk			C:\Users\Hunter\Pictures\sdmap\dns-exfiltration-using-sdmap...	2016-06-21 14:17:39 CEST	c16-Hunter
Exfil.lnk			C:\Users\Hunter\Pictures\Exfil	2016-06-21 14:17:39 CEST	c16-Hunter
Exfiltration_Diagram.png.lnk			C:\Users\Hunter\Pictures\Exfil\Exfiltration_Diagram.png	2016-06-21 14:17:41 CEST	c16-Hunter
home-network-design-networking-for-a-single-family-home-case-house-arkko-1433-a-792.jpg.lnk			C:\Users\Hunter\Documents\home-network-design-network...	2016-06-21 14:18:17 CEST	c16-Hunter
mapscan.xml.lnk			C:\Users\Hunter\Desktop\mapscan.xml	2016-06-21 15:05:19 CEST	c16-Hunter
Outlook.lnk			C:\Users\Hunter\Dropbox\Outlook	2016-06-21 15:15:00 CEST	c16-Hunter
Welcome.docx.lnk			C:\Users\Hunter\Documents>Welcome.docx	2016-06-21 14:27:37 CEST	c16-Hunter
falepom.7z.lnk			C:\Users\Hunter\Pictures\falepom.7z	2016-06-21 13:46:37 CEST	c16-Hunter
burpsuite_free_v1.7.03.jar.lnk			C:\Users\Hunter\Downloads\burpsuite_free_v1.7.03.jar	2016-06-21 13:17:44 CEST	c16-Hunter
Downloads.lnk			C:\Users\Hunter\Downloads	2016-06-21 13:17:44 CEST	c16-Hunter
http-www.netasploit.com.lnk			No preferred path found	2016-06-21 11:27:00 CEST	c16-Hunter
how_to_threat_actors_steal_your_data.lnk			C:\Users\Hunter\Documents\how_to_threat_actors_steal...	2016-06-21 11:39:46 CEST	c16-Hunter
Exfil.lnk			No preferred path found	2016-06-21 11:37:49 CEST	c16-Hunter
Exfiltration_Diagram.png.lnk			C:\Users\Hunter\Pictures\Exfil\Exfiltration_Diagram.png	2016-06-21 11:37:49 CEST	c16-Hunter
catt-cute-animals-cute-catt-hamster-rabbit-Favim.com-198548.jpg.lnk			No preferred path found	2016-06-21 13:46:53 CEST	c16-Hunter
msni-detecting-determining-bot.lnk			C:\Users\Hunter\Documents\msni-detecting-determining-bot...	2016-06-21 11:40:22 CEST	c16-Hunter
Ryan_YanAnbversp_thesis.lnk			C:\Users\Hunter\Documents\Ryan_YanAnbversp_thesis.pdf	2016-06-21 11:40:07 CEST	c16-Hunter
Hackers Got real Brain.lnk			C:\Users\Hunter\Pictures\backgrounds\Hackers Got real Br...	2016-06-21 11:46:29 CEST	c16-Hunter
63b616a33c209cd3a48795c981f46d.jpg.lnk			No preferred path found	2016-06-21 13:46:16 CEST	c16-Hunter
Beautiful Pictures Of Cute Animals-6.jpg.lnk			C:\Users\Hunter\Pictures\falepom\Beautiful Pictures Of C...	2016-06-21 13:46:39 CEST	c16-Hunter
608d73d614d0c808a087adb8f28fca7.jpg.lnk			No preferred path found	2016-06-21 13:46:57 CEST	c16-Hunter
Info.lnk			C:\Users\Hunter\Info	2016-06-21 13:52:07 CEST	c16-Hunter

Figure 25.1

26 The suspect employee tried to exfiltrate data by sending it as an email attachment. What is the name of the suspected attachment?

This information can be found in the email exchange, under the attachment tab.

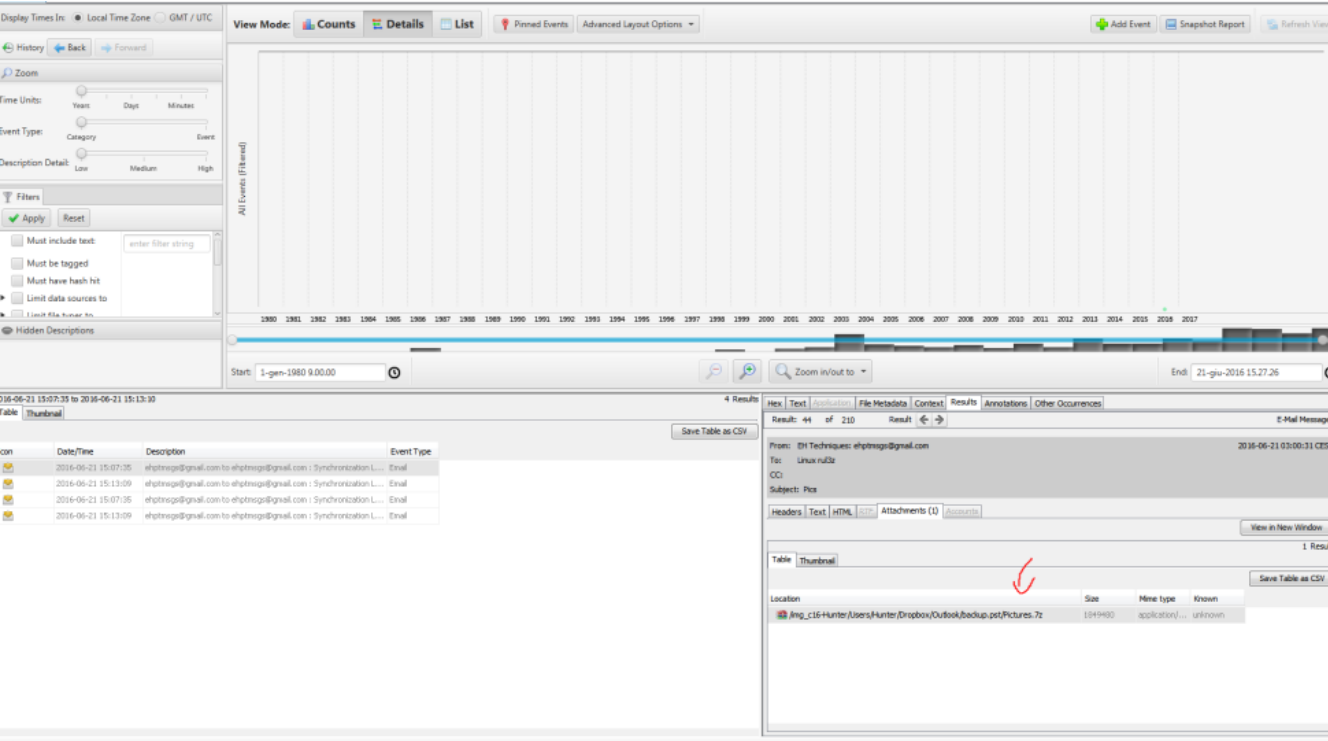


Figure 26.1

27 Shellbags shows that the employee created a Folder to include all the data he will exfiltrate. What is the full path of that folder?

We've used the shellbags tab looking for a suspicious folder, like it was mentioned in the request.

hunter - Autopsy 4.16.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

63 Results

Save Table as CSV

Source File	S	C	Path	Key	Data Source	Last Write	Date Modified	Date Created
UirClass.dat			My Computer\C\	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter	2016-06-21 12:21:59 CEST		
UirClass.dat			My Computer\C:\Program Files (x86)	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter		2016-06-21 09:18:28 CEST	2013-08-2
UirClass.dat			My Computer\C:\Program Files (x86)\Notepad++	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter	2016-06-20 23:51:47 CEST	2016-06-21 09:18:32 CEST	2016-06-2
UirClass.dat			My Computer\C:\Users	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter	2016-06-21 01:45:52 CEST	2016-06-21 08:37:46 CEST	2013-08-2
UirClass.dat			My Computer\C:\Users\Hunter	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter	2016-06-21 09:23:48 CEST	2016-06-21 08:59:14 CEST	2016-06-2
UirClass.dat			My Computer\C:\Users\Hunter\Desktop	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter		2016-06-21 08:37:54 CEST	2016-06-2
UirClass.dat			My Computer\C:\Users\Hunter\Dropbox	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter		2016-06-21 01:50:18 CEST	2016-06-2
UirClass.dat			My Computer\C:\Users\Hunter\Dropbox\Info	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter	2016-06-21 12:02:50 CEST	2016-06-21 11:52:28 CEST	2016-06-2
UirClass.dat			My Computer\C:\Users\Hunter\Documents	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter		2016-06-20 23:58:10 CEST	2016-06-2
UirClass.dat			My Computer\C:\Users\Hunter\Documents\Custom Office ...	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter	2016-06-21 12:25:57 CEST	2016-06-21 01:58:54 CEST	2016-06-2
UirClass.dat			My Computer\C:\Users\Hunter\Downloads	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter	2016-06-21 12:29:48 CEST	2016-06-21 01:44:12 CEST	2016-06-2
UirClass.dat			My Computer\C:\Users\Hunter\New folder	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter		2016-06-21 11:51:56 CEST	2016-06-2
UirClass.dat			My Computer\C:\Users\Hunter\Info	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter		2016-06-21 11:51:56 CEST	2016-06-2
UirClass.dat			My Computer\C:\Users\Hunter\Google Drive	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter		2016-06-21 02:04:50 CEST	2016-06-2
UirClass.dat			My Computer\C:\Users\Hunter\Tracking	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter		2016-06-21 08:59:14 CEST	2016-06-2
UirClass.dat			My Computer\C:\Users\Hunter\Pictures	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter		2016-06-21 12:01:44 CEST	
UirClass.dat			My Computer\C:\Users\Hunter\Pictures\Info	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter	2016-06-21 12:17:36 CEST	2016-06-21 09:38:14 CEST	2016-06-2
UirClass.dat			My Computer\C:\Users\Hunter\Links	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter		2016-06-21 01:54:22 CEST	2016-06-2
UirClass.dat			My Computer\C:\Users\Hunter\Contacts	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter		2016-06-21 08:37:54 CEST	2016-06-2
UirClass.dat			My Computer\C:\PerfLogs	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter			2013-08-22 15:22:36 CEST
UirClass.dat			My Computer\CLSID_Documents	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter			
UirClass.dat			My Computer\CLSID_Downloads	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter			
UirClass.dat			My Computer\CLSID_Downloads\Hash_Suite_Free_3_4.zip	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter		2016-06-21 11:00:44 CEST	2016-06-2
UirClass.dat			My Computer\CLSID_Downloads\Hash_Suite_Free_3_4.zip...	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter	2016-06-21 11:06:34 CEST		
UirClass.dat			My Computer\CLSID_Downloads\Hash_Suite_Free	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter		2016-04-29 04:23:40 CEST	2015-04-2
UirClass.dat			My Computer\CLSID_Downloads\New folder	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter		2016-06-21 11:07:56 CEST	2016-06-2
UirClass.dat			My Computer\CLSID_Downloads\Olydig	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter		2016-06-21 11:07:56 CEST	2016-06-2
UirClass.dat			My Computer\CLSID_Downloads\Systemerms\Suite	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter	2016-06-21 11:19:31 CEST	2016-06-21 11:18:04 CEST	2016-06-2
UirClass.dat			My Computer\CLSID_Music	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter			
UirClass.dat			My Computer\CLSID_Exchange	Local Settings\Software\Microsoft\Windows\Shell\Bag\WU...	c16-Hunter			

Figure 27.1

28 The user deleted two JPG files from the system and moved them to \$Recycle-Bin. What is the file name that has the resolution of 1920x1200?

After it's been deleted it'll lose its name, so it'll be required to looking for that file before it was deleted or when it was downloaded. Since it was given the resolution too and that information was in the filename directly it was easy to spot.

Web Downloads						
Table Thumbnail						
	S	C	Path	URL	Date Accessed	Don
			C:\Users\Hunter\Downloads\SkyeSetup.exe	https://get.skype.com/go/getskype-windows	2016-06-21 10:54:19 CEST	get.
			C:\Users\Hunter\Downloads\SkyeSetup.exe	https://get.skype.com/go/getskype	2016-06-21 10:54:19 CEST	get.
			C:\Users\Hunter\Downloads\SkyeSetup.exe	https://download.skype.com/f14a80c895182a5238c9be18...	2016-06-21 10:54:19 CEST	dow
			C:\Users\Hunter\Downloads\Wireshark-win64-2.0.4.exe	https://1.na.di.wireshark.org/win64/Wireshark-win64-2.0...	2016-06-21 11:15:24 CEST	1.na
			C:\Users\Hunter\Downloads\7z1602-x64.exe	http://www.7-zip.org/a/7z1602-x64.exe	2016-06-21 11:16:35 CEST	www
			C:\Users\Hunter\Downloads\npp.6.9.2.Installer.exe	https://notepad-plus-plus.org/repository/6.x/6.9.2/npp.6...	2016-06-21 11:16:49 CEST	note
			C:\Users\Hunter\Downloads\readerdc_en_ka_install.exe	https://adownload.adobe.com/bin/live/readerdc_en_ka...	2016-06-21 11:17:53 CEST	adm
			C:\Users\Hunter\Pictures\slide-cat-laying-down.png	http://www.kindredkitties.org/sites/default/files/styles/slid...	2016-06-21 11:29:51 CEST	www
			C:\Users\Hunter\Pictures\Kitties-cats-22092221-500-374.jpg	http://images4.fanpop.com/image/photos/22000000/Kittle...	2016-06-21 11:30:00 CEST	ima
			C:\Users\Hunter\Pictures\gutter.jpg	http://www.gutterkitties.co.nz/sites/default/files/images/g...	2016-06-21 11:30:05 CEST	www
			C:\Users\Hunter\Pictures\Breathtaking-Kitties14.jpg	http://www.orangedonkey.net/wp-content/uploads/2011/...	2016-06-21 11:30:23 CEST	www
			C:\Users\Hunter\Pictures\6966997-sleeping-kitties.jpg	http://7.themes.com/data_images/out/57/6966997-sleepin...	2016-06-21 11:30:45 CEST	7-th
			C:\Users\Hunter\Pictures\Adorable-kitties-kitties-18082642-670-50...	http://images4.fanpop.com/image/photos/18000000/Ador...	2016-06-21 11:30:49 CEST	ima
			C:\Users\Hunter\Downloads\ws_small_cute_kitty_1920x1200.jpg	http://img.wallpaperstock.net/81/small-cute-kitty-wallpape...	2016-06-21 11:31:09 CEST	img.
			C:\Users\Hunter\Downloads\ws_small_cute_kitty_1920x1200.jpg	http://wallpaperstock.net/small-cute-kitty-wallpapers_242...	2016-06-21 11:31:09 CEST	wall
			C:\Users\Hunter\Downloads\ws_small_cute_kitty_1920x1200 (1).jpg	http://img.wallpaperstock.net/81/small-cute-kitty-wallpape...	2016-06-21 11:31:18 CEST	img.
			C:\Users\Hunter\Downloads\ws_small_cute_kitty_1920x1200 (1).jpg	http://wallpaperstock.net/small-cute-kitty-wallpapers_242...	2016-06-21 11:31:18 CEST	wall
			C:\Users\Hunter\Pictures\big-eyes-cat-cats-cute-Favim.com-2674...	http://s6.favim.com/orig/150423/big-eyes-cat-cats-cute-F...	2016-06-21 11:31:32 CEST	s6.f
			C:\Users\Hunter\Pictures\GoodKitty2-1.jpg	http://i212.photobucket.com/albums/cc70/bhustastan/Cats...	2016-06-21 11:31:39 CEST	i212
			C:\Users\Hunter\Pictures\backgrounds\F3A153K.jpg	http://wallpapercave.com/wp/F3A153K.jpg	2016-06-21 11:35:12 CEST	wall
			C:\Users\Hunter\Pictures\backgrounds\565053.jpg	https://images7.alphacoders.com/565/565053.jpg	2016-06-21 11:35:26 CEST	ima
			C:\Users\Hunter\Pictures\backgrounds\The-Walking-Dead-Walpap...	http://hdwallpaperbackgrounds.net/wp-content/uploads/2...	2016-06-21 11:35:46 CEST	hdw
				http://hdwallpaperbackgrounds.net/wp-content/uploads/2...	2016-06-21 11:35:53 CEST	hdw
			C:\Users\Hunter\Downloads\andrew_lincoln_the_walking_dead-25...	http://hdwallpapers.com/download/andrew_lincoln_the_w...	2016-06-21 11:36:09 CEST	hdw
				http://hdwallpaperbackgrounds.net/wp-content/uploads/2...	2016-06-21 11:36:42 CEST	hdw
			C:\Users\Hunter\Pictures\Exfil\Exfiltration_Diagram.png	http://www.filetransferconsulting.com/wp-content/uploads...	2016-06-21 11:37:32 CEST	www

Figure 28.1

29 Provide the name of the directory where information about jump lists items (created automatically by the system) is stored?

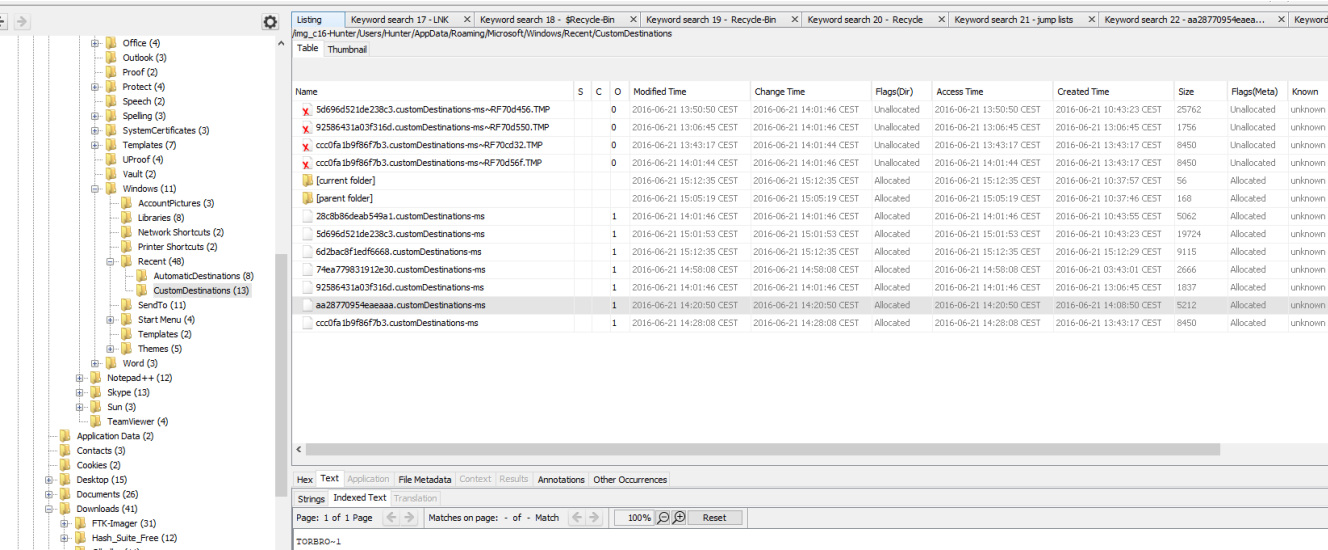
Using the cheatsheet provided, under the jump list section, it's written the default folder of the jump list items.

in a ita is	<p>determine the last time of execution or activity on the system.</p> <ul style="list-style-type: none">• Windows XP contains at most 96 entries<ul style="list-style-type: none">- LastUpdateTime is updated when the files are executed• Windows 7 contains at most 1,024 entries<ul style="list-style-type: none">- LastUpdateTime does not exist on Win7 systems	Syst
	<h3 data-bbox="686 558 959 617">Jump Lists</h3> <p>Description</p> <ul style="list-style-type: none">• The Windows 7 task bar (Jump List) is engineered to allow users to "jump" or access items they have frequently or recently used quickly and easily. This functionality cannot only include recent media files; it must also include recent tasks.• The data stored in the AutomaticDestinations folder will each have a unique file prepended with the AppID of the associated application.	<p>Description</p> <p>Records 30 Application application</p> <p>Location</p> <p>SOFTWARE\MI 4f6d-848e-b2 System32\SR</p> <p>Interpret</p> <p>Use tool s between t</p>
em is	<p>Location</p> <p>Win7/8/10: C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations</p>	<p>Description</p> <p>Windows 6</p>
centApps	<p>Interpretation</p> <ul style="list-style-type: none">• First time of execution of application.<ul style="list-style-type: none">- Creation Time = First time item added to the AppID file.• Last time of execution of application w/file open.<ul style="list-style-type: none">- Modification Time = Last time item added to the AppID file.	<p>Location</p> <p>Win10: SYSTEM\Curre SYSTEM\Curre Investiga</p>

Figure 29.1

30 Using JUMP LIST analysis, provide the full path of the application with the AppID of "aa28770954eaeaaa" used to bypass network security monitoring controls.

Under that folder, which jump files are stored, there is that file, extract it and using JumpList explorer will give us the answer : *C : Browser.exe*



Name	S	C	O	Modified Time	Change Time	Flags(Dir)	Access Time	Created Time	Size	Flags(Meta)	Known
5d696d521de238c3.customDestinations-ms~RF70d456.TMP			0	2016-06-21 13:50:50 CEST	2016-06-21 14:01:46 CEST	Unallocated	2016-06-21 13:50:50 CEST	2016-06-21 10:43:23 CEST	25762	Unallocated	unknown
92586431a03f316d.customDestinations-ms~RF70d550.TMP			0	2016-06-21 13:06:45 CEST	2016-06-21 14:01:46 CEST	Unallocated	2016-06-21 13:06:45 CEST	2016-06-21 13:06:45 CEST	1756	Unallocated	unknown
ccc0fa1b9f67b3.customDestinations-ms~RF70d32.TMP			0	2016-06-21 13:43:17 CEST	2016-06-21 14:01:44 CEST	Unallocated	2016-06-21 13:43:17 CEST	2016-06-21 13:43:17 CEST	8450	Unallocated	unknown
ccc0fa1b9f67b3.customDestinations-ms~RF70d56f.TMP			0	2016-06-21 14:01:44 CEST	2016-06-21 14:01:46 CEST	Unallocated	2016-06-21 14:01:44 CEST	2016-06-21 13:43:17 CEST	8450	Unallocated	unknown
[current folder]				2016-06-21 15:12:35 CEST	2016-06-21 15:12:35 CEST	Allocated	2016-06-21 15:12:35 CEST	2016-06-21 10:37:57 CEST	56	Allocated	unknown
[parent folder]				2016-06-21 15:05:19 CEST	2016-06-21 15:05:19 CEST	Allocated	2016-06-21 15:05:19 CEST	2016-06-21 10:37:46 CEST	168	Allocated	unknown
28c8b8deab549a1.customDestinations-ms			1	2016-06-21 14:01:46 CEST	2016-06-21 14:01:46 CEST	Allocated	2016-06-21 14:01:46 CEST	2016-06-21 10:43:55 CEST	5062	Allocated	unknown
5d696d521de238c3.customDestinations-ms			1	2016-06-21 15:01:53 CEST	2016-06-21 15:01:53 CEST	Allocated	2016-06-21 15:01:53 CEST	2016-06-21 10:43:23 CEST	19724	Allocated	unknown
6d2bac8f1edf6668.customDestinations-ms			1	2016-06-21 15:12:35 CEST	2016-06-21 15:12:35 CEST	Allocated	2016-06-21 15:12:35 CEST	2016-06-21 15:12:29 CEST	9115	Allocated	unknown
74ea779831912e30.customDestinations-ms			1	2016-06-21 14:58:08 CEST	2016-06-21 14:58:08 CEST	Allocated	2016-06-21 14:58:08 CEST	2016-06-21 03:43:01 CEST	2666	Allocated	unknown
92586431a03f316d.customDestinations-ms			1	2016-06-21 14:01:46 CEST	2016-06-21 14:01:46 CEST	Allocated	2016-06-21 14:01:46 CEST	2016-06-21 13:06:45 CEST	1837	Allocated	unknown
aa28770954eaeaaa.customDestinations-ms			1	2016-06-21 14:20:50 CEST	2016-06-21 14:20:50 CEST	Allocated	2016-06-21 14:20:50 CEST	2016-06-21 14:08:50 CEST	5212	Allocated	unknown
ccc0fa1b9f67b3.customDestinations-ms			1	2016-06-21 14:28:08 CEST	2016-06-21 14:28:08 CEST	Allocated	2016-06-21 14:28:08 CEST	2016-06-21 13:43:17 CEST	8450	Allocated	unknown

Figure 30.1

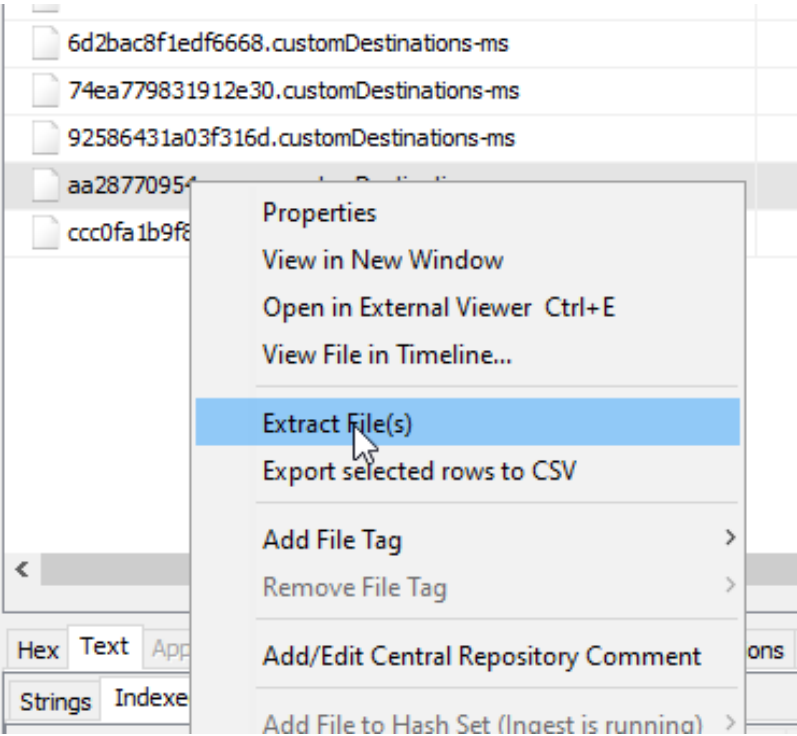


Figure 30.2

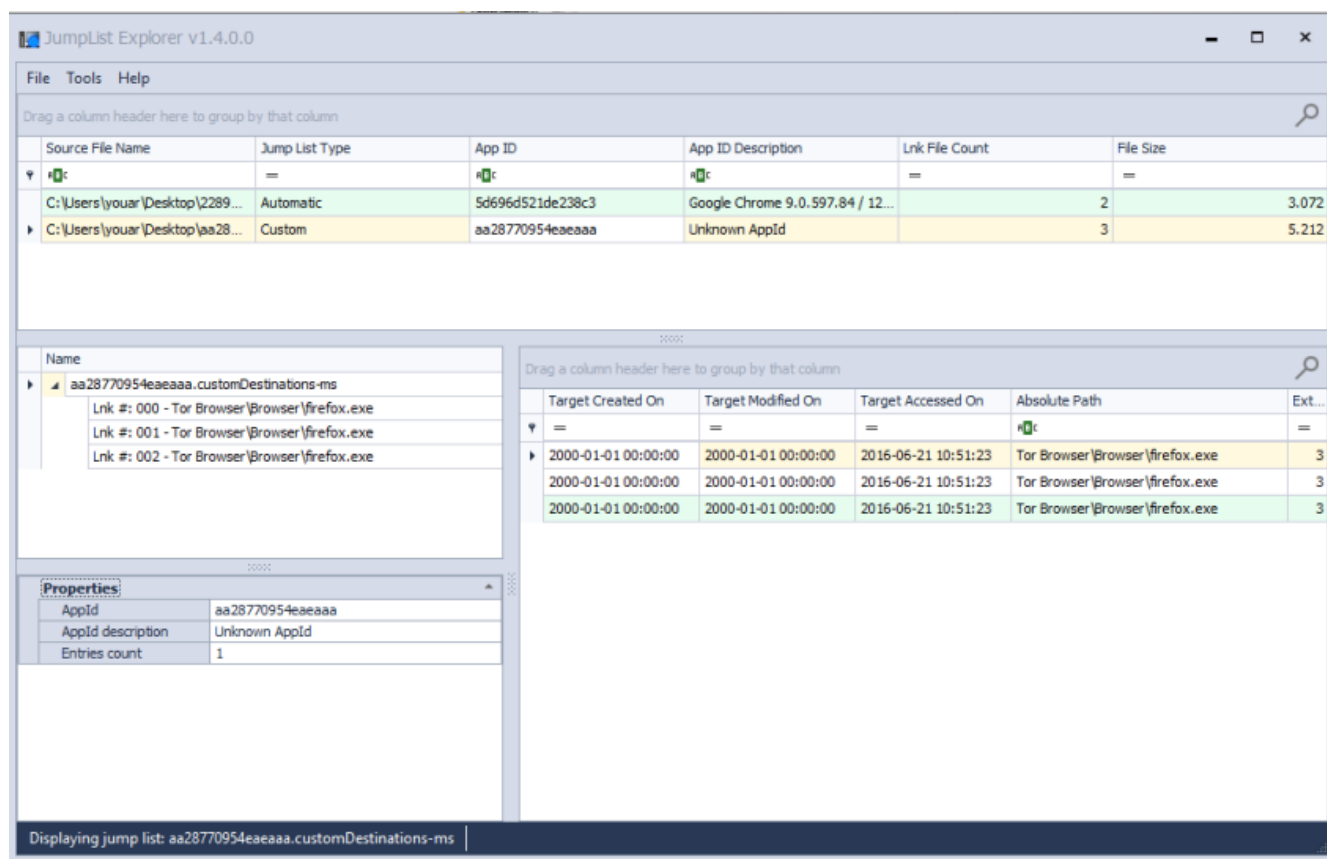


Figure 30.3