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 $/img\_c16 - Hunter/ProgramData/Microsoft/IlsCache/imcrcache.xml$ where there is the answers

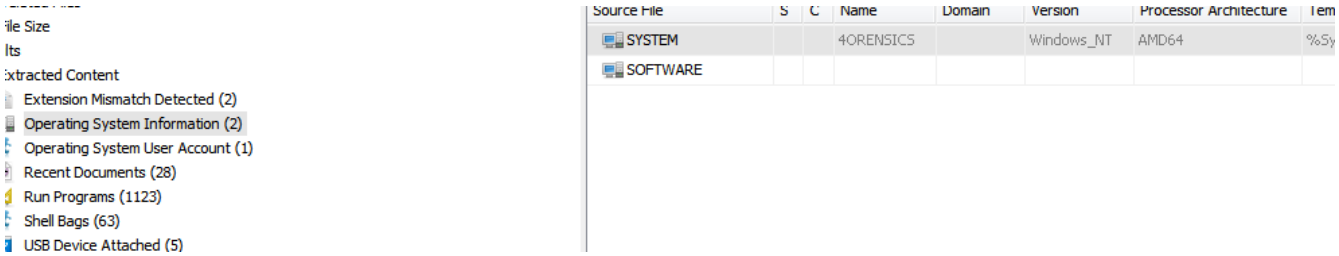


Figure 1.1

2 What is the computer IP?

Using Autopsy and exploring windows registry i found in $/img\_c16 - Hunter/Windows/System32/config/SYSTEM$ and then $ControlSet001/Services/Tcpip/Parameters/Interfaces$

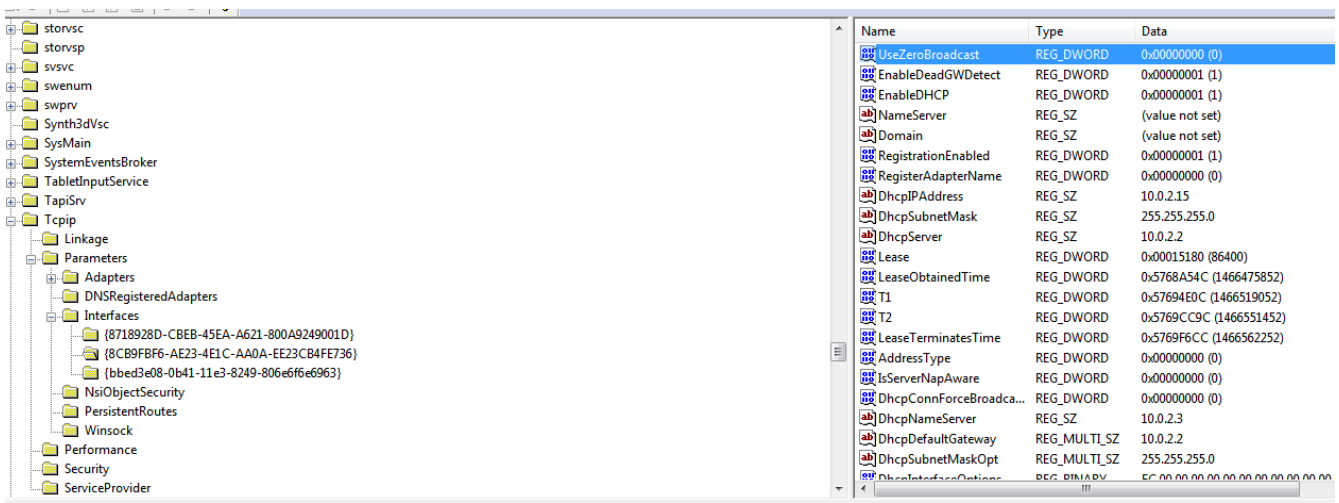


Figure 2.1

3 What was the DHCP LeaseObtainedTime?

Always in $/img\_c16 - Hunter/Windows/System32/config/SYSTEM$ and then $ControlSet001/Services/Tcpip/Parameters/Interfaces$

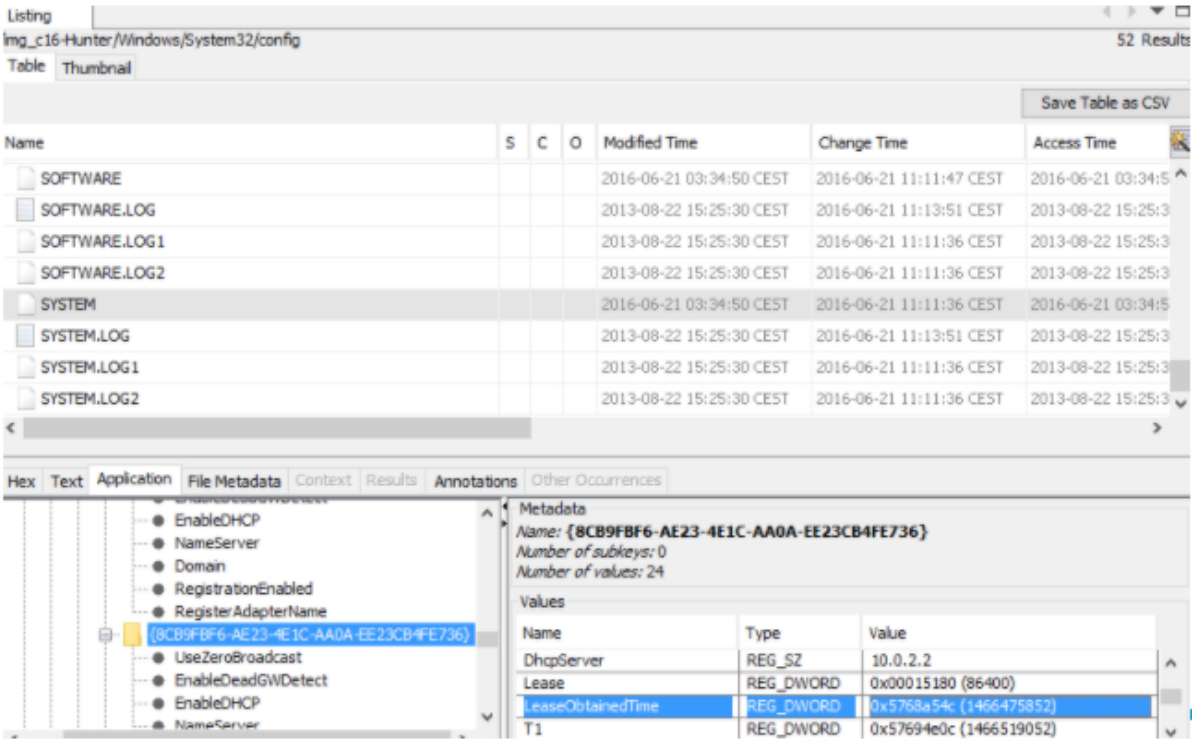


Figure 3.1

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?

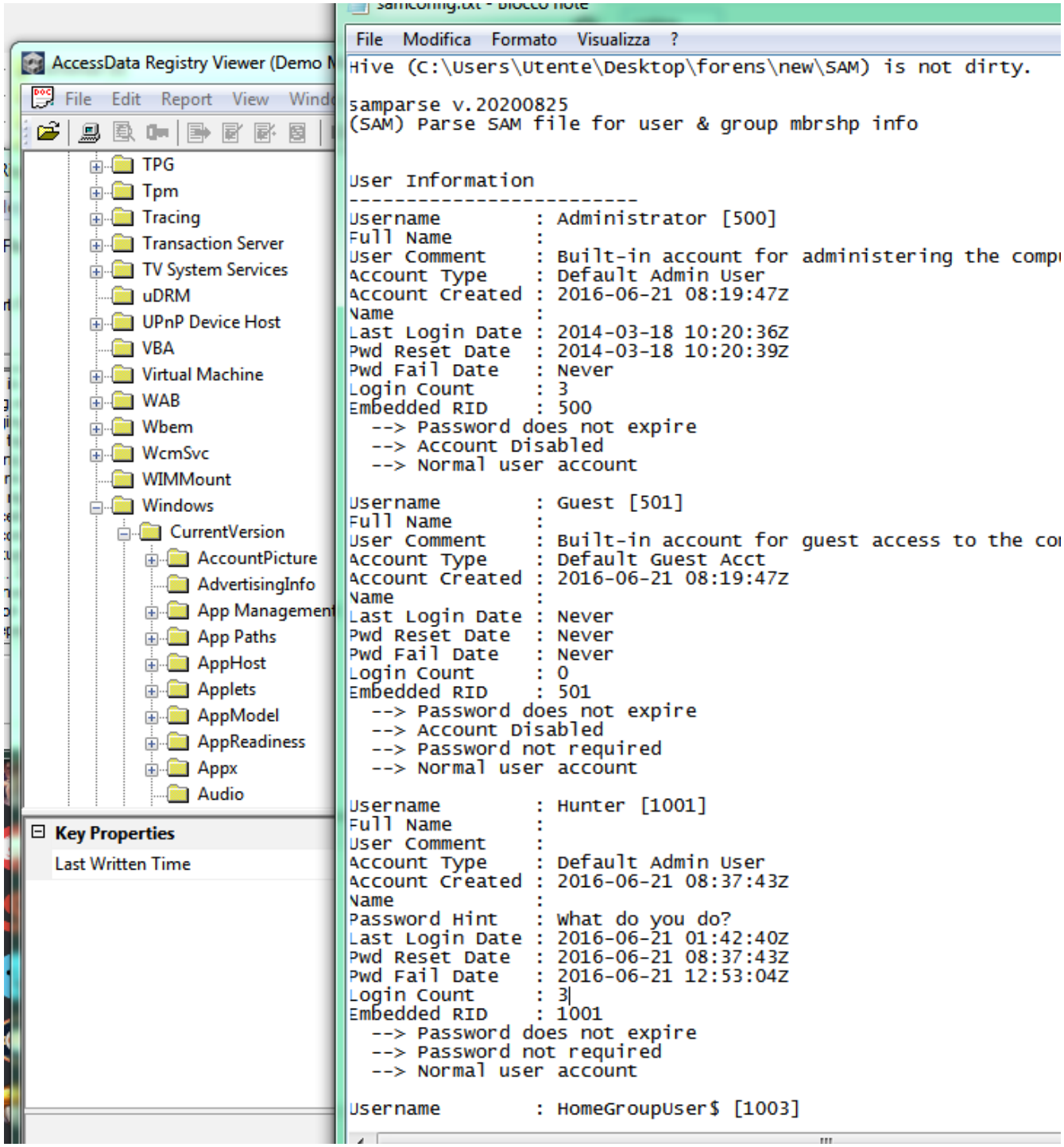


Figure 4.1

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

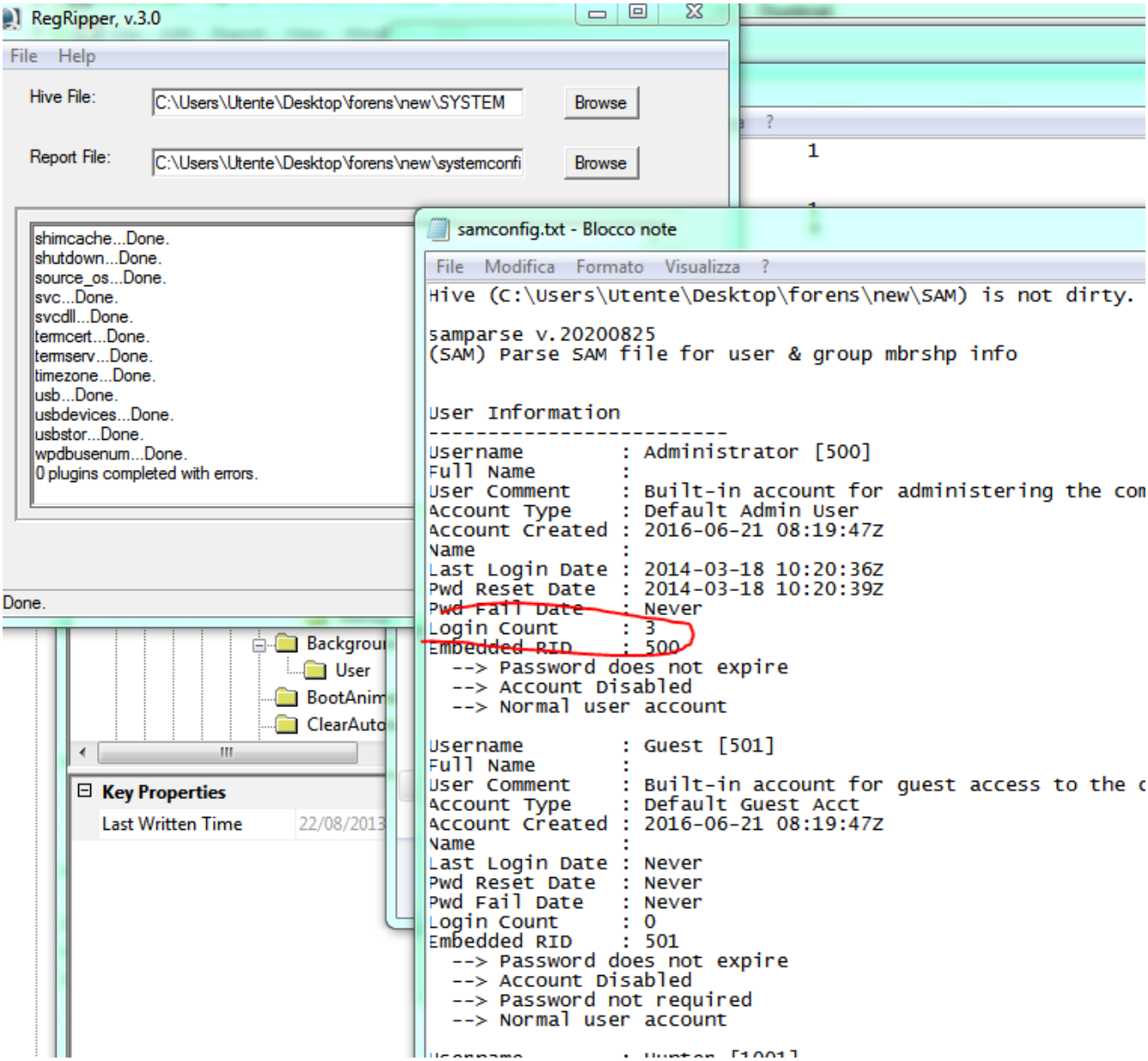

RegRipper, v.3.0
File Help
Hive File: C:\Users\Utente\Desktop\forens\new\SYSTEM
Browse
Report File: C:\Users\Utente\Desktop\forens\new\systemconfi
Browse
shimcache...Done.
shutdown...Done.
source_os...Done.
svc...Done.
svcdll...Done.
termcert...Done.
termserv...Done.
timezone...Done.
usb...Done.
usbdevices...Done.
usbstor...Done.
wpdbusenum...Done.
0 plugins completed with errors.
Done.
samconfig.txt - Blocco note
File Modifica Formato Visualizza ?
Hive (C:\Users\Utente\Desktop\forens\new\SAM) is not dirty.
samparse v.20200825
(SAM) Parse SAM file for user & group mbrshp info
User Information
Username : Administrator [500]
Full Name :
User Comment : Built-in account for administering the com
Account Type : Default Admin User
Account Created : 2016-06-21 08:19:47Z
Name :
Last Login Date : 2014-03-18 10:20:36Z
Pwd Reset Date : 2014-03-18 10:20:39Z
Pwd Fail Date : Never
Login Count : 3
Embedded RID : 500
--> Password does not expire
--> Account Disabled
--> Normal user account
Username : Guest [501]
Full Name :
User Comment : Built-in account for guest access to the c
Account Type : Default Guest Acct
Account Created : 2016-06-21 08:19:47Z
Name :
Last Login Date : Never
Pwd Reset Date : Never
Pwd Fail Date : Never
Login Count : 0
Embedded RID : 501
--> Password does not expire
--> Account Disabled
--> Password not required
--> Normal user account
User
BootAnim
ClearAuto
Key Properties
Last Written Time 22/08/2013

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

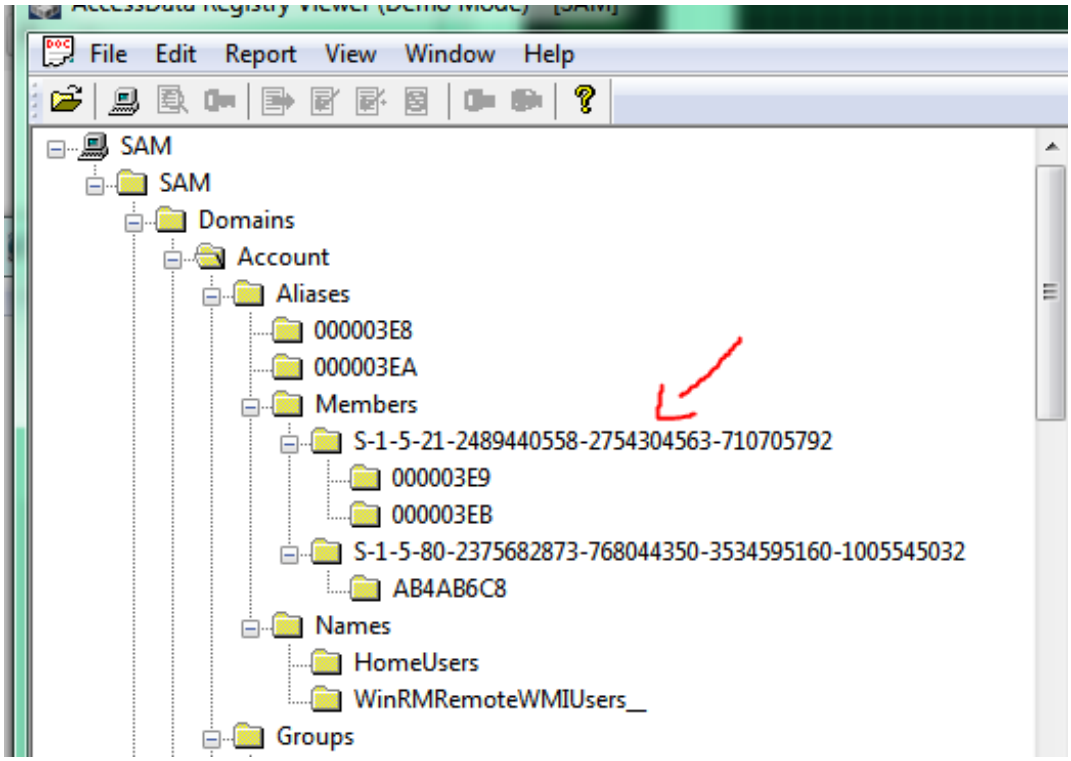


Figure 5.1

6 What is the Operating System(OS) version?

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

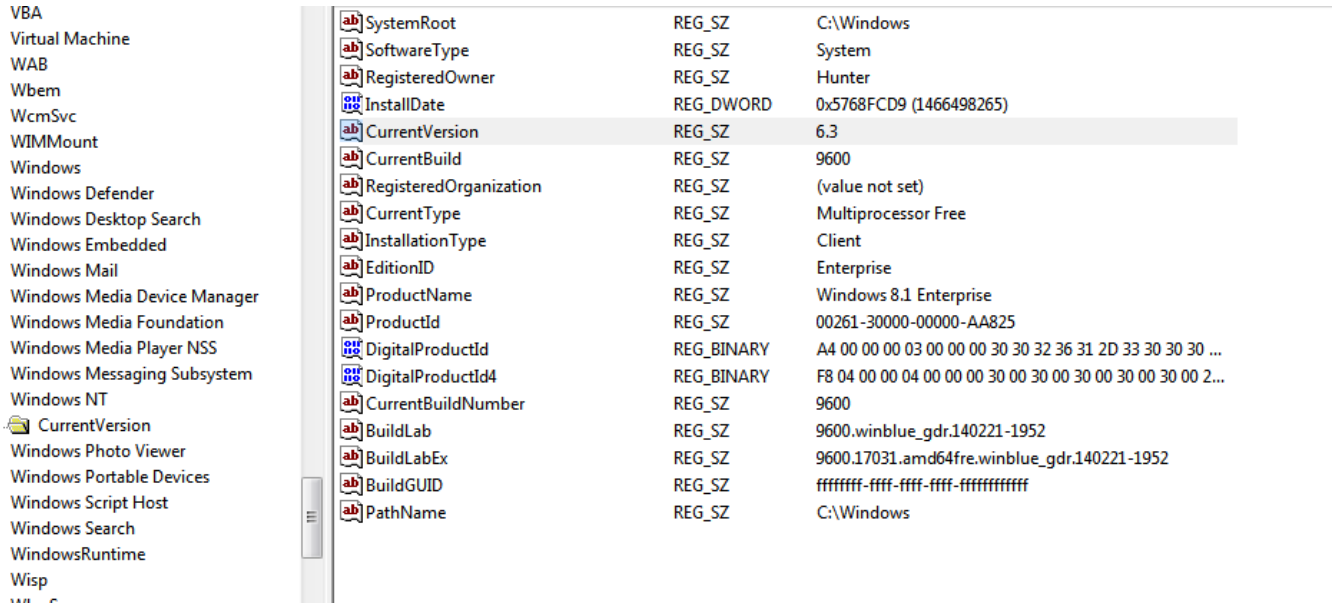


Figure 6.1

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

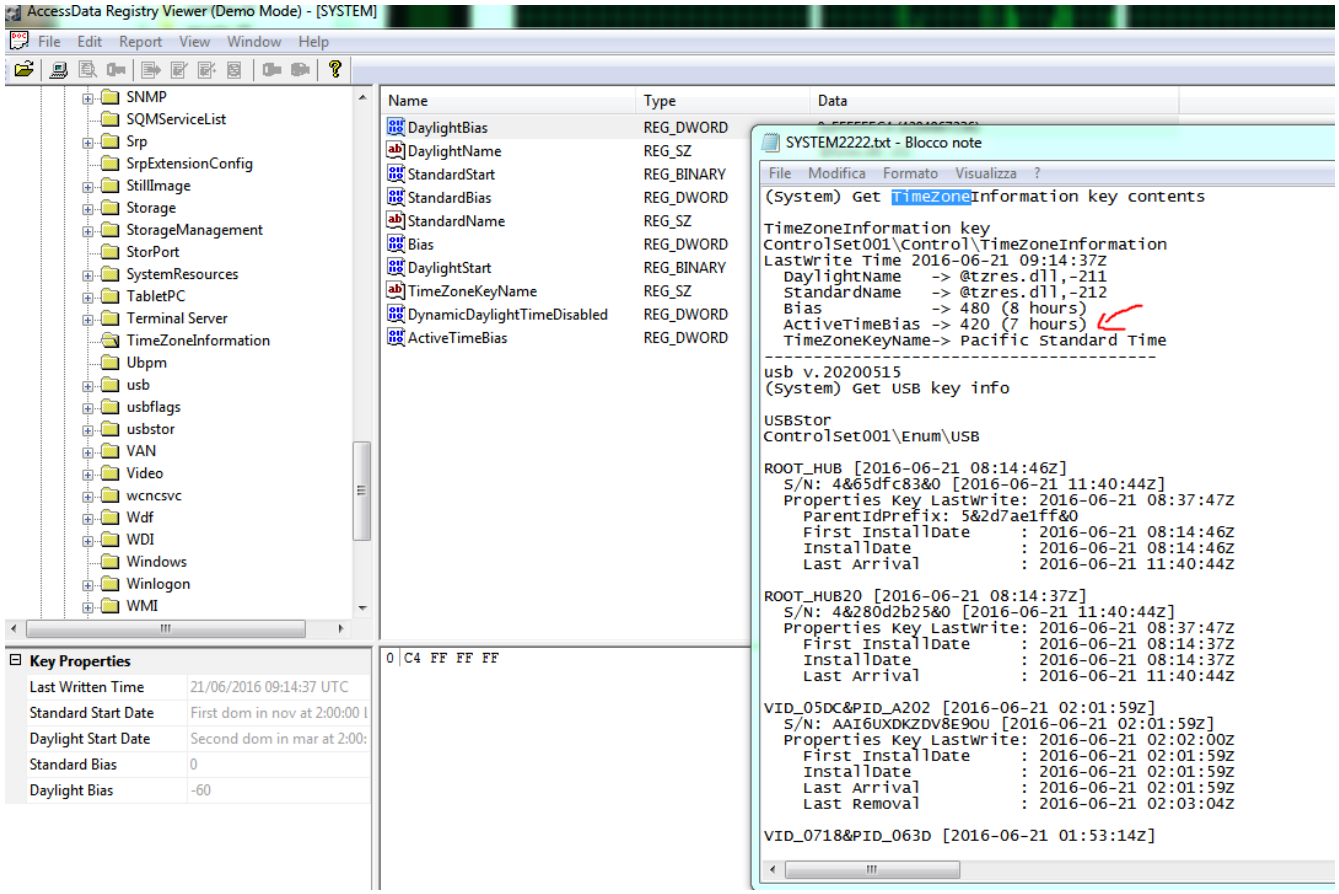


Figure 7.1

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.

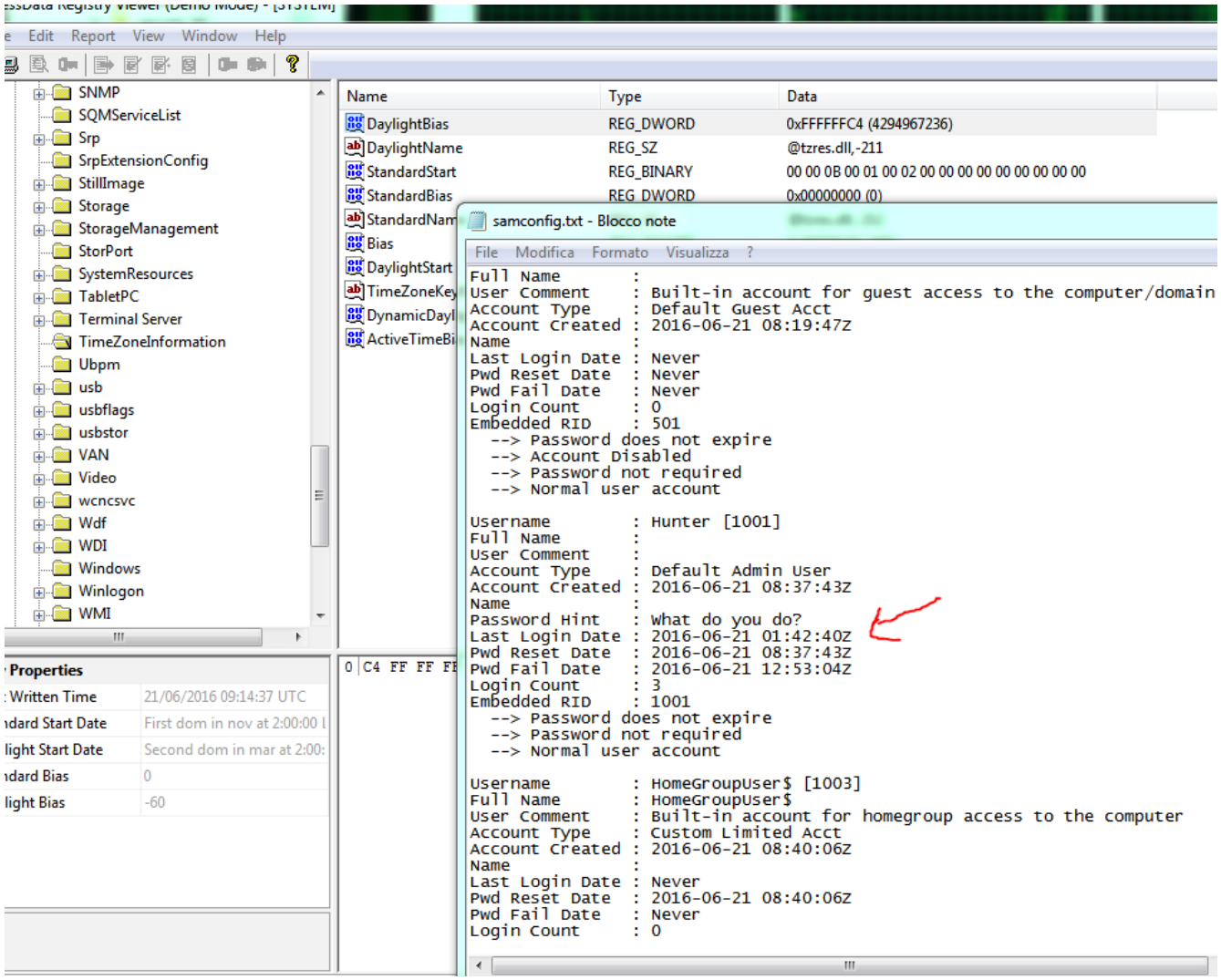


Figure 8.1

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-36F3F2D			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-77			CCLEANER64.EXE		2016-06-21 14:01:44 CEST			Prefetch File
CCLEANER64.EXE-77			CCLEANER64.EXE		2016-06-21 14:01:44 CEST			Prefetch File
BCWIPE.EXE-36F3F2D			BCWIPE.EXE		2016-06-21 14:02:35 CEST			Prefetch File
CONSENT.EXE-531BD			CONSENT.EXE		2016-06-21 14:02:38 CEST			Prefetch File
BCWIPE.EXE-36F3F2D			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_DESKT			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-854F6B4			MSHTA.EXE		2016-06-21 14:14:38 CEST			Prefetch File

Cest is 2h less than UTC

Figure 9.1

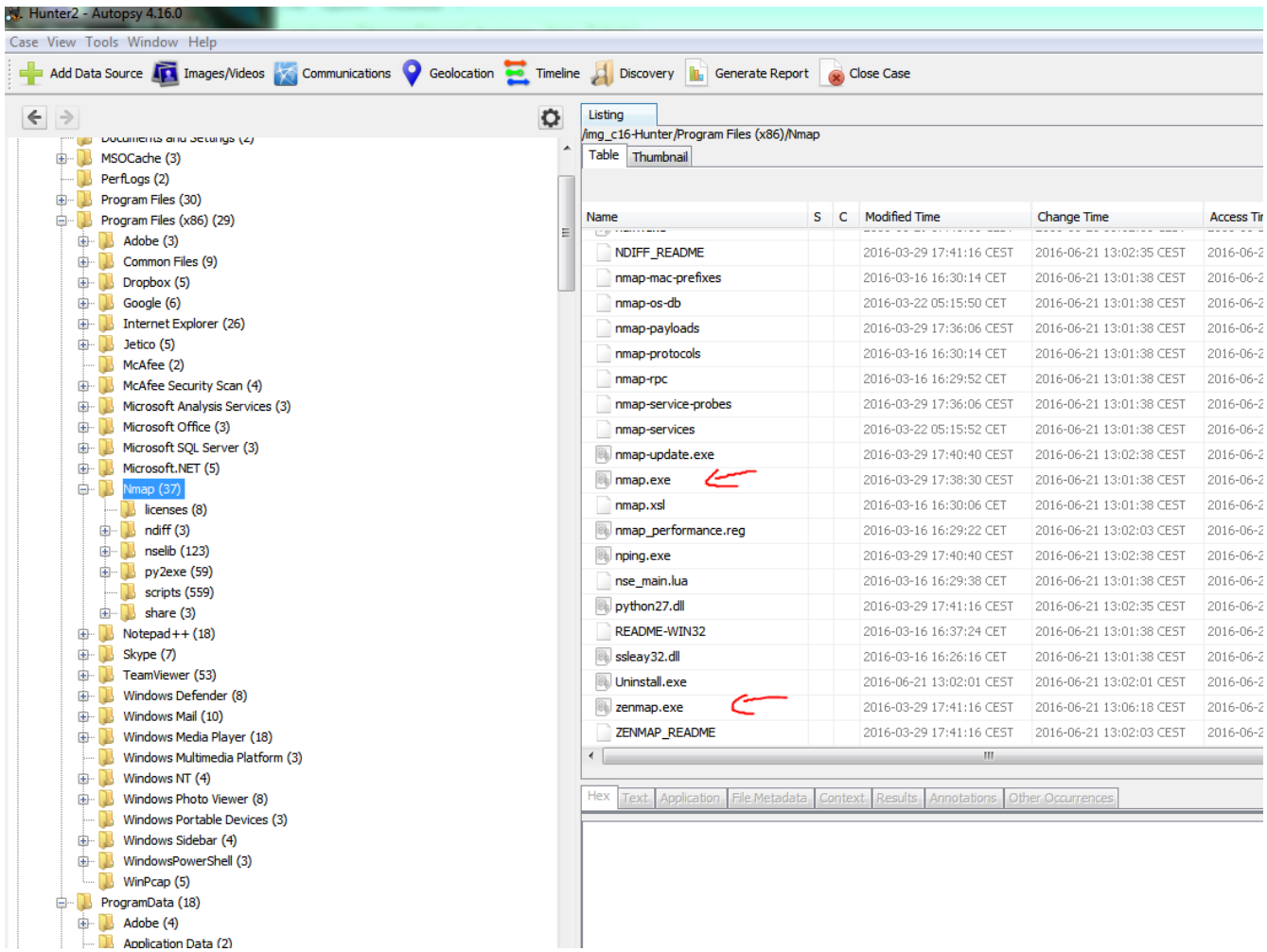


Figure 9.2

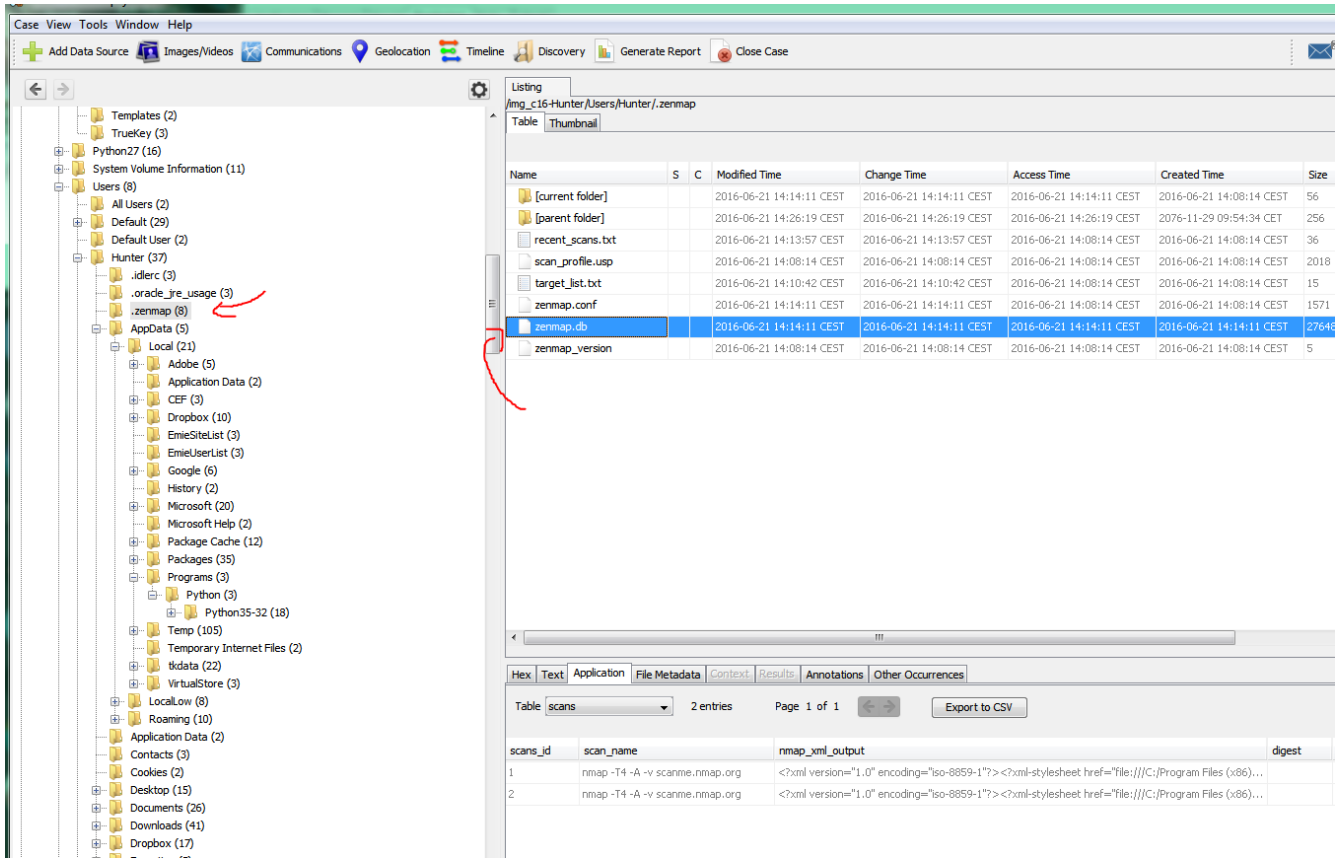

Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Listing
/img_c16-Hunter/Users/Hunter/.zenmap
Table
Thumbnail
Name
S
C
Modified Time
Change Time
Access Time
Created Time
Size
[current folder]
[parent folder]
recent_scans.txt
scan_profile.usp
target_list.txt
zenmap.conf
zenmap.db
zenmap_version
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
nmap -T4 -A -v scanme.nmap.org
Templates (2)
TrueKey (3)
Python27 (16)
System Volume Information (11)
Users (8)
All Users (2)
Default (29)
Default User (2)
Hunter (37)
.idlerc (3)
.oracle_jre_usage (3)
.zenmap (8)
AppData (5)
Local (21)
Adobe (5)
Application Data (2)
CEF (3)
Dropbox (10)
EmieSiteList (3)
EmieUserList (3)
Google (6)
History (2)
Microsoft (20)
Microsoft Help (2)
Package Cache (12)
Packages (35)
Programs (3)
Python (3)
Python35-32 (18)
Temp (105)
Temporary Internet Files (2)
tkdata (22)
VirtualStore (3)
LocalLow (8)
Roaming (10)
Application Data (2)
Contacts (3)
Cookies (2)
Desktop (15)
Documents (26)
Downloads (41)
Dropbox (17)

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

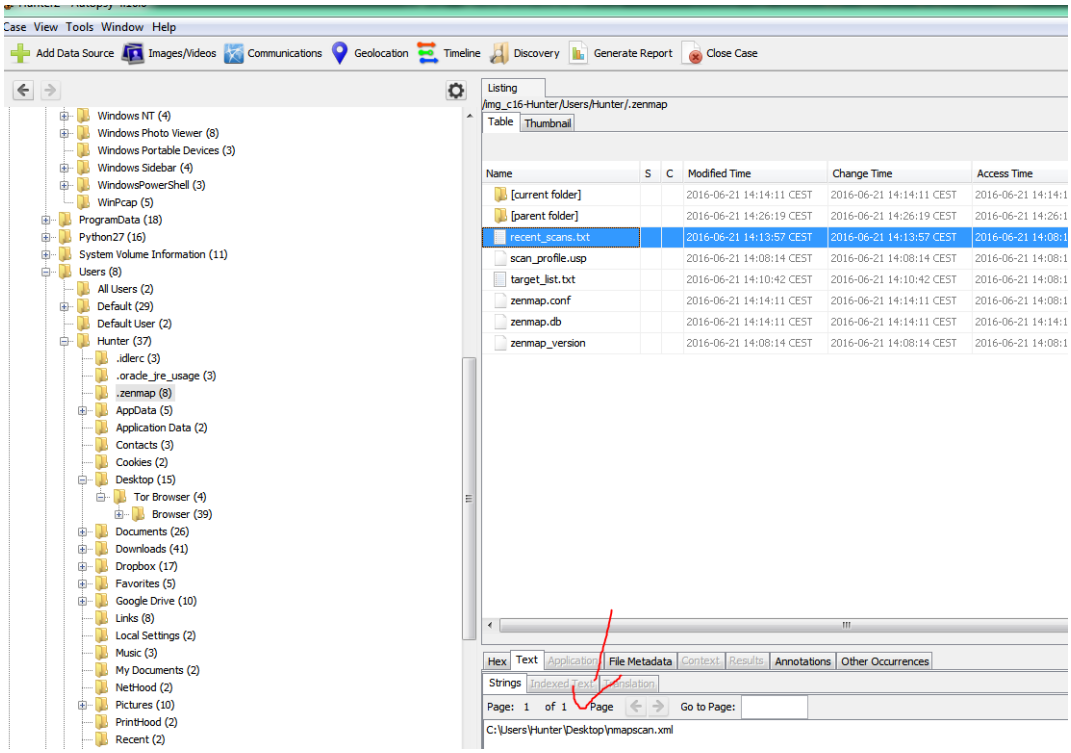


Figure 10.1

11 How many ports were scanned?

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

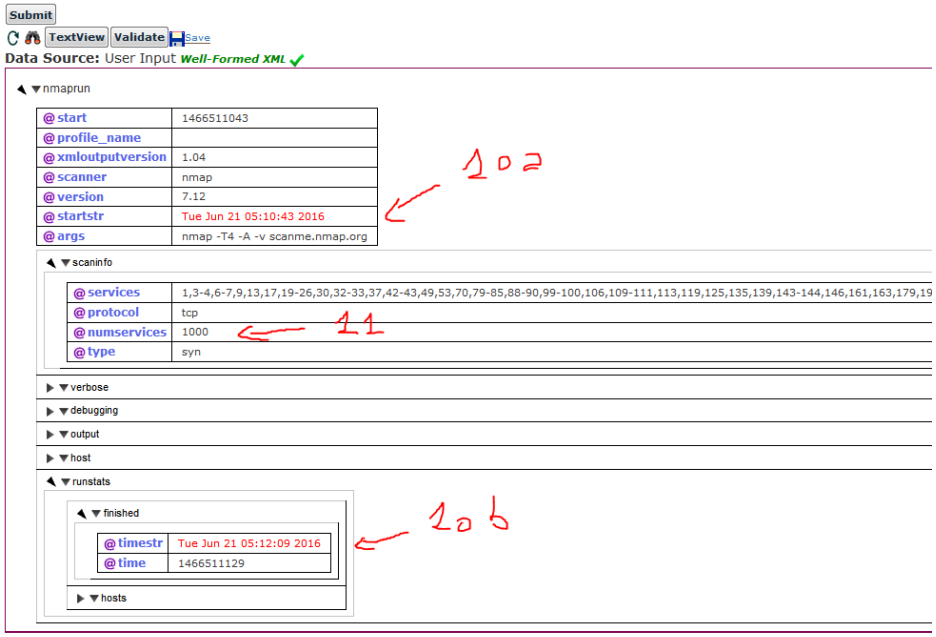


Figure 11.1

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=0%Q=)T2(R=Y%DF=N%T=100%W=0%S=Z%A=S%F=AR%O=%RD=0%
%O=%RD=0%Q=)T4(R=Y%DF=N%T=100%W=0%S=A%A=Z%F=R%O=%RD=0 OS:%Q=)T5(R=Y%DF=N%T=100%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=N%T=100%W=0
%O=%RD=0%Q=)U1 OS:(R=Y%DF=N%T=34%IPL=164%UN=0%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.

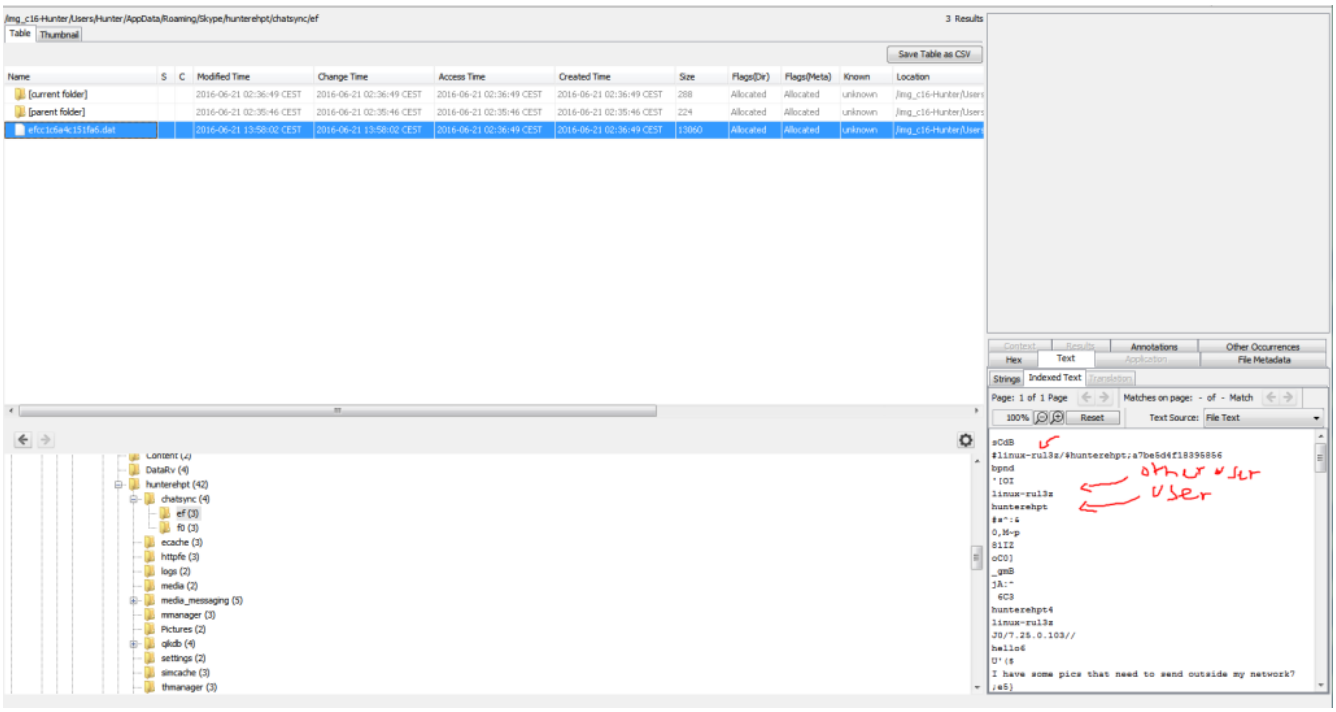


Figure 13.1

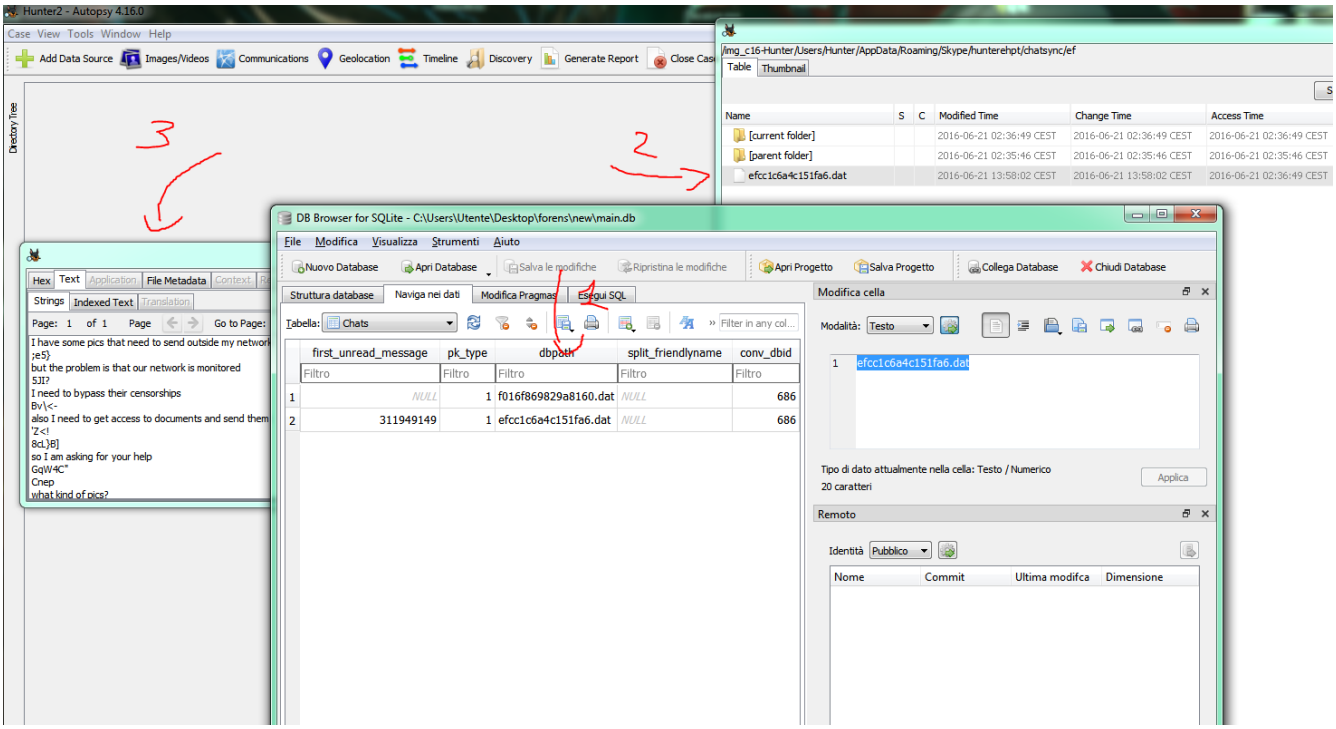


Figure 13.2

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.

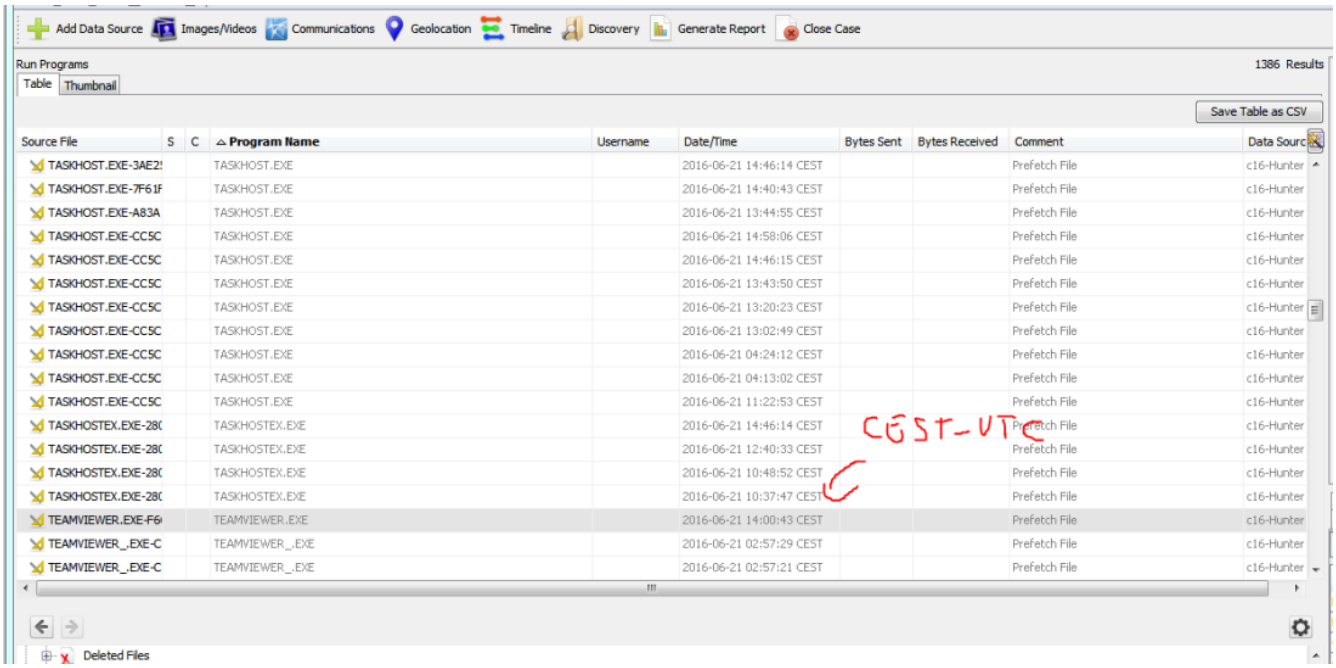


Figure 14.1

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

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

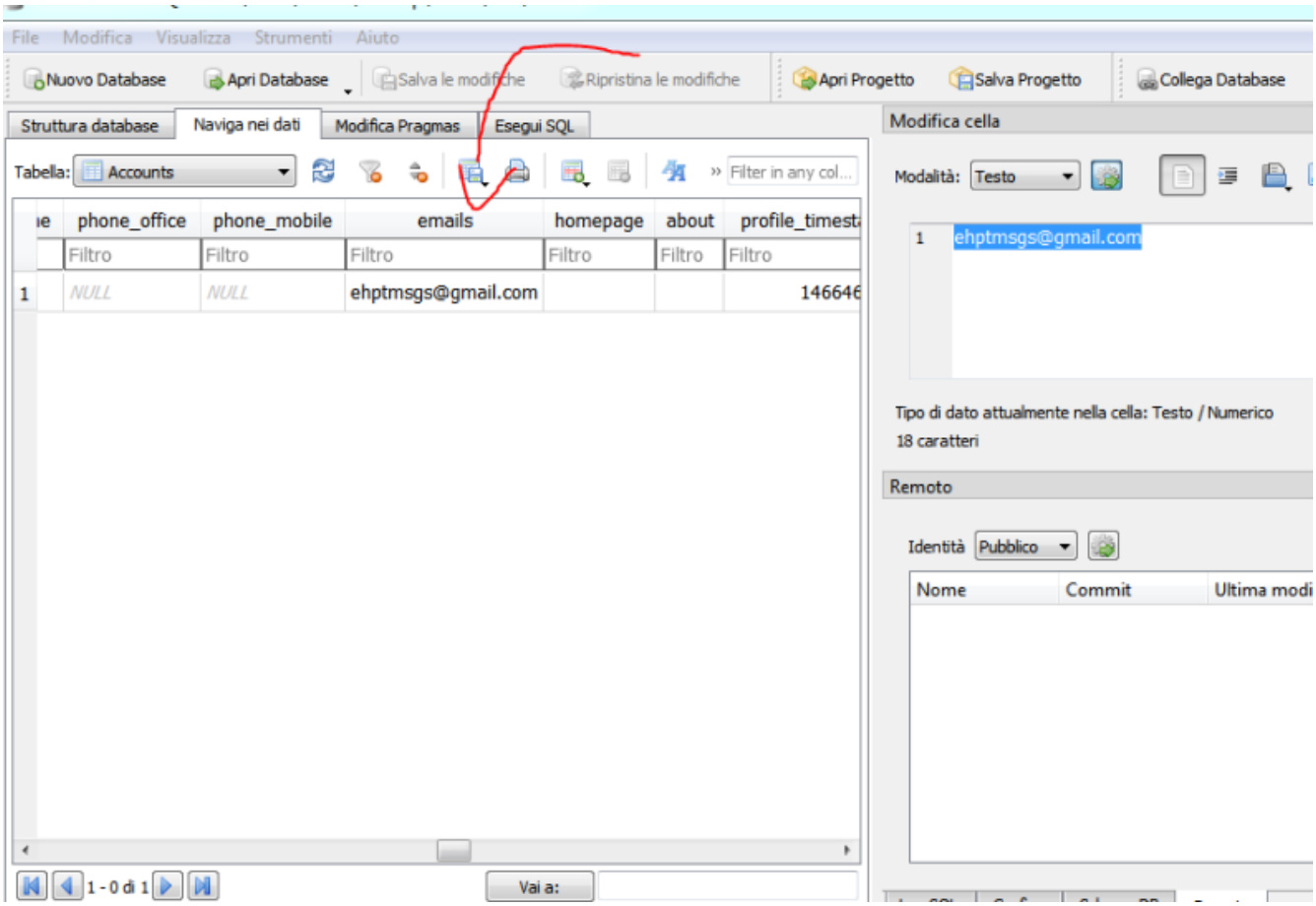


Figure 15.1

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

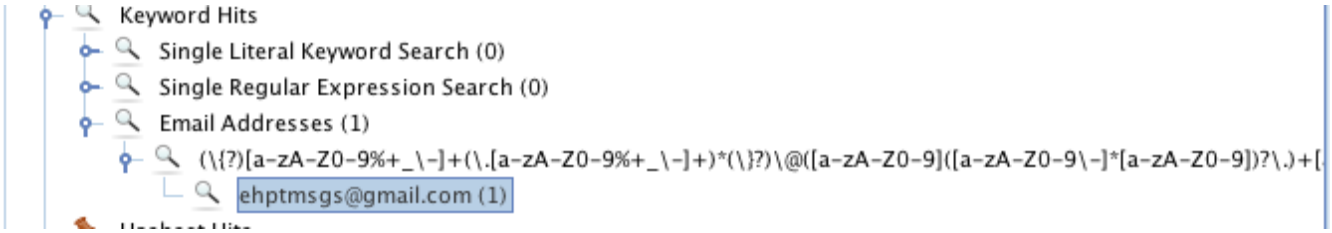


Figure 15.2

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

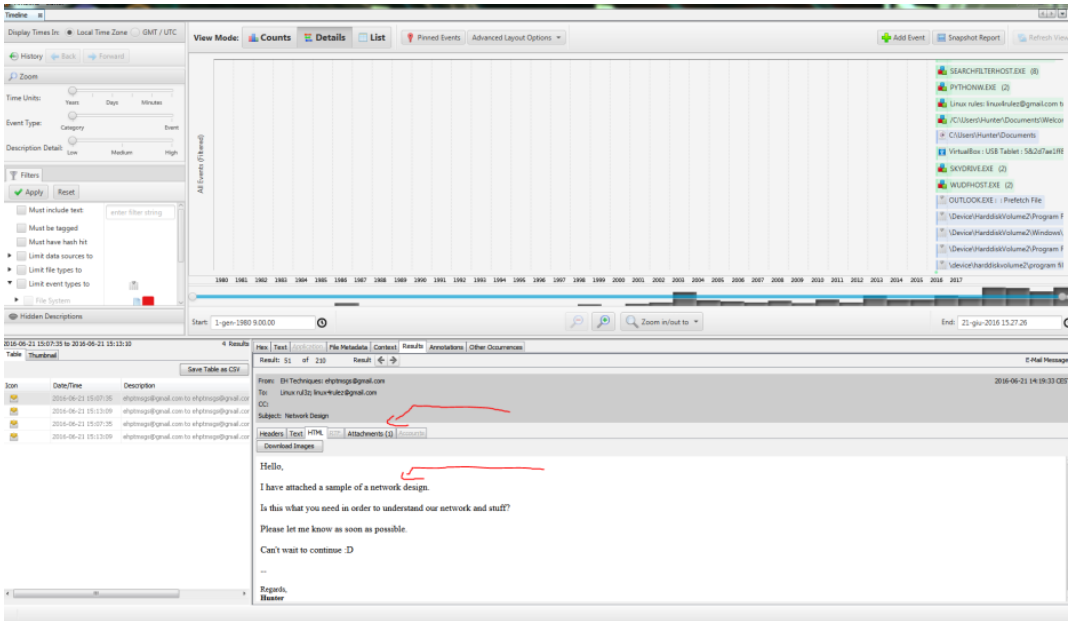


Figure 16.1

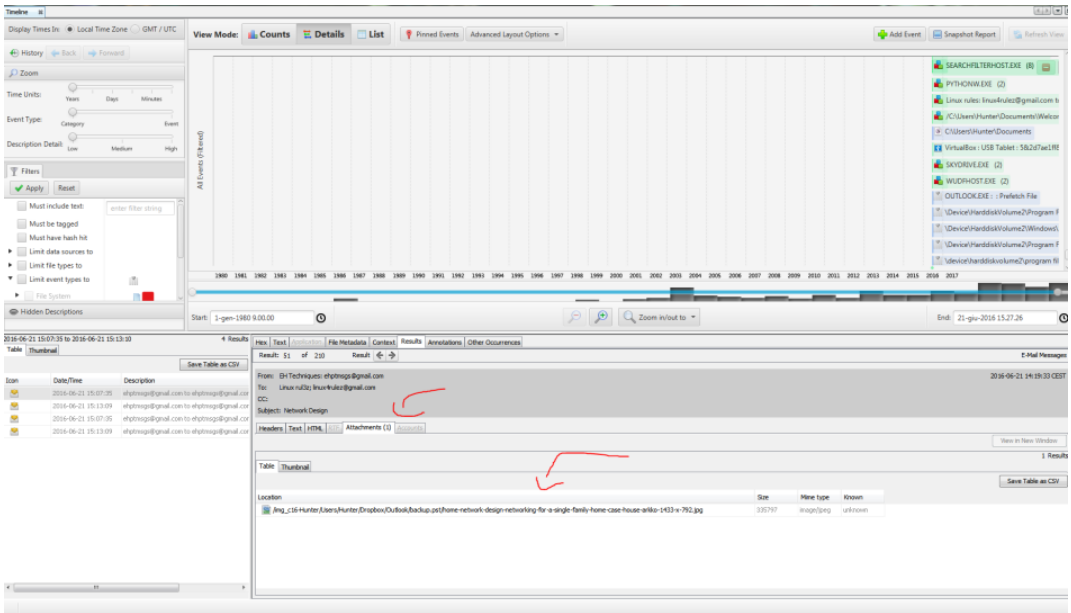


Figure 16.2

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.

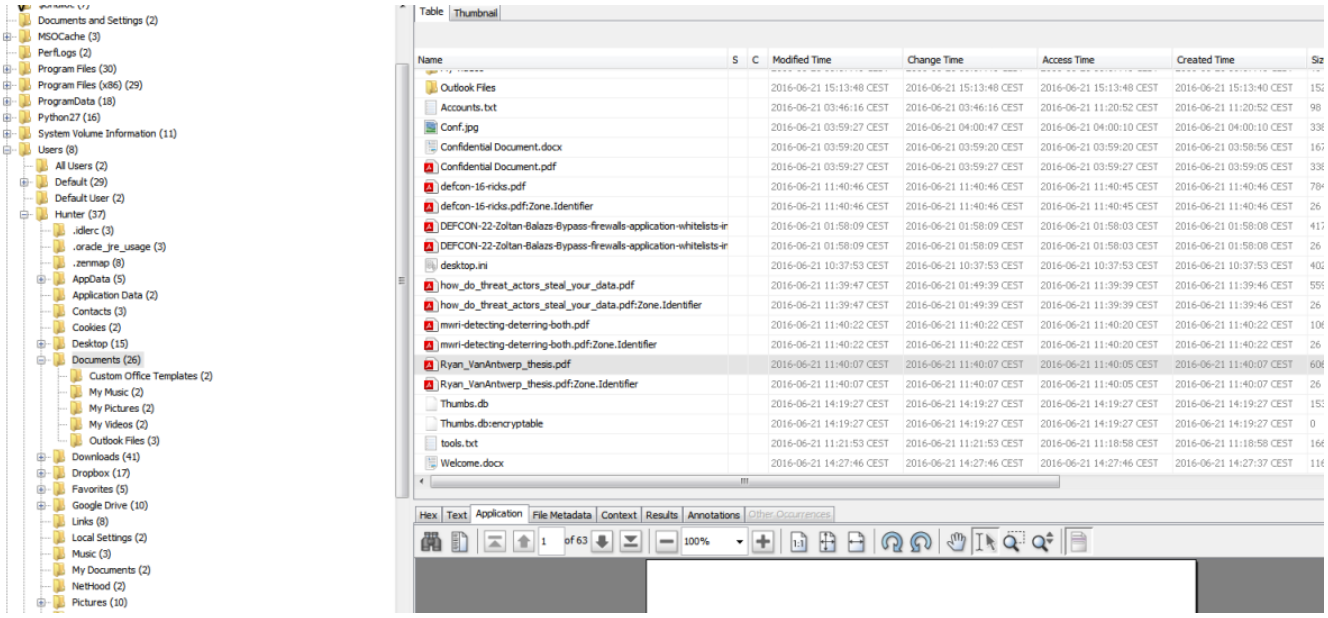


Figure 17.1

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

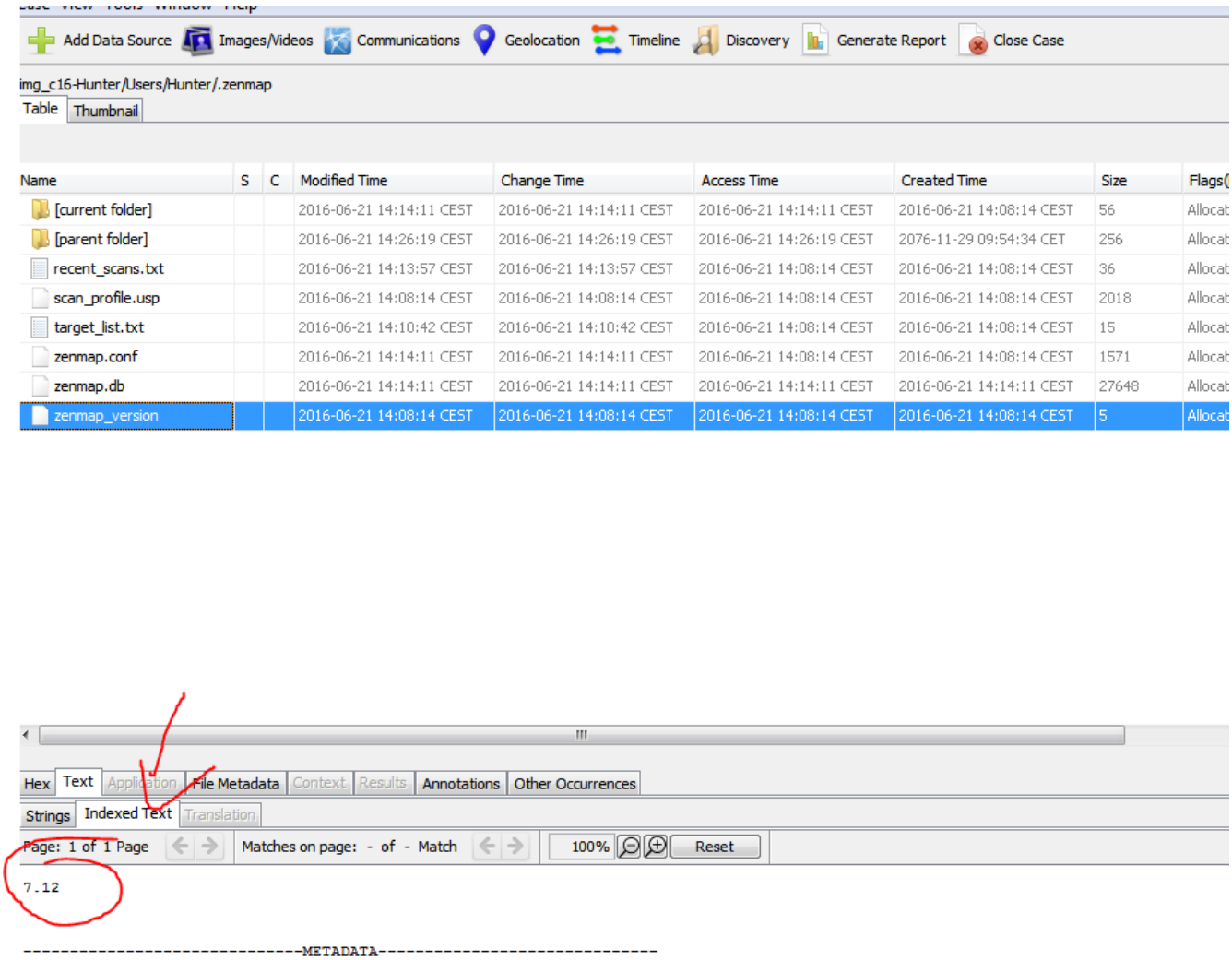


Figure 18.1

19 What was the name of the crypto payment application possibly used by the suspect employee to transfer funds for the external attacker?

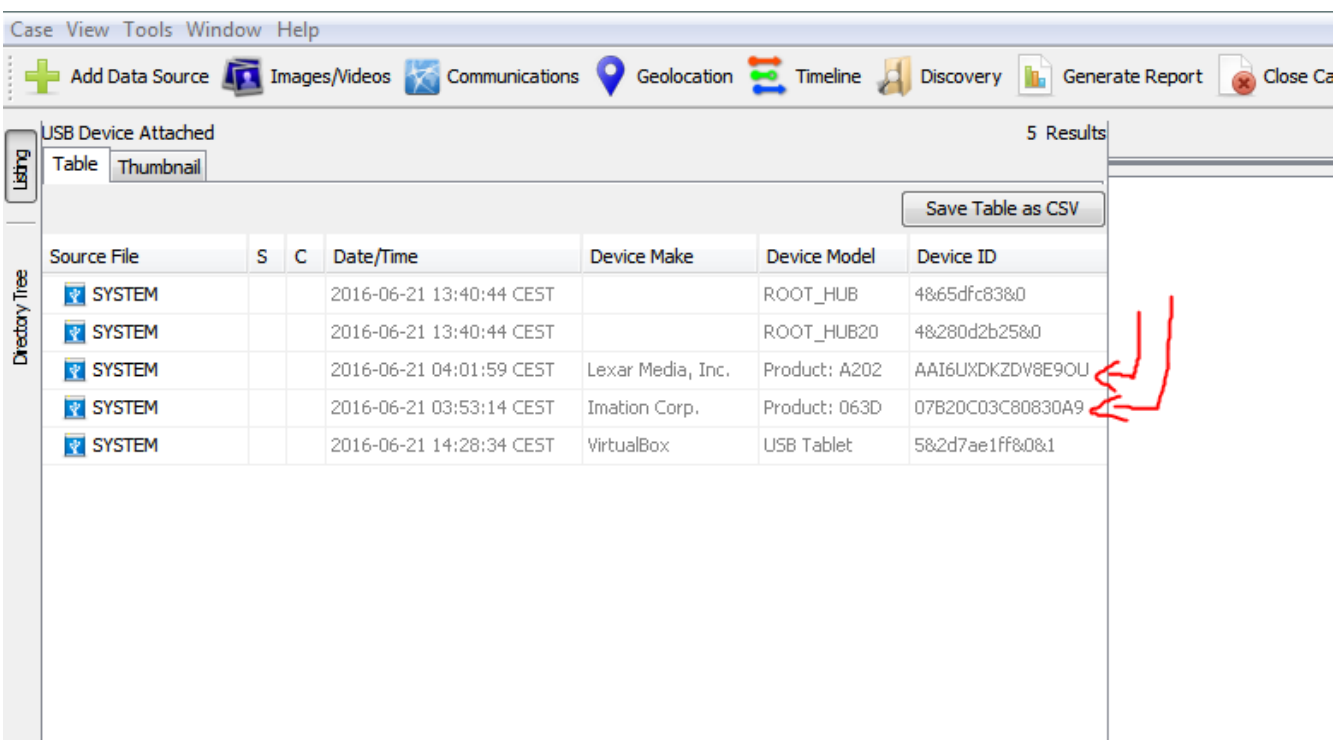
Looking for the answer in the programs manually

Name	Keyword Preview	Location
Crypto Swap.lnk-slack	«crypto« swap.lnk-slack	/img_c16-Hunter/ProgramData/Microsoft/Windows/Start Menu/Programs/BCWipe/Crypto Swap.lnk-slack
FTKImager_UserGuide.pdf	● Hash algorithm SHA-512● «Crypto« ...	/img_c16-Hunter/Users/Hunter/Downloads/FTK-Imager.zip/FTK-Imager/help/enu/FTKImager_UserGuide.pdf
setupapi.dll	File '%ws' %hs signed NT5 «Crypto«.DrpG...	/img_c16-Hunter/Windows/SysWOW64/setupapi.dll
nld_adshattrdefs.dll	imports «crypto« functions, contains «cryp...	/img_c16-Hunter/Users/Hunter/Downloads/FTK-Imager/langs/nld_adshattrdefs.dll
setupapi.dll	specified for non NT5 «Crypto« file '%ws'....	/img_c16-Hunter/Windows/WinSxS/amd64_microsoft-windows-setupapi_31bf3856ad364e35_6.3.9600.17031_none_...
AgRobust.db	MENU\PROGRAMS\BCWIPE\«CRYPTO« SW...	/img_c16-Hunter/Windows/Prefetch/AgRobust.db
crypt32.dll	Microsoft Base Smart Card «Crypto« Provi...	/img_c16-Hunter/Windows/System32/crypt32.dll
ptb_adshattrdefs.dll	imports «crypto« functions, contains «cryp...	/img_c16-Hunter/Users/Hunter/Downloads/FTK-Imager/langs/ptb_adshattrdefs.dll
cryptuiwizard.dll	type="win32"<description>«Crypto« User ...	/img_c16-Hunter/Windows/System32/cryptuiwizard.dll
deu_adshattrdefs.dll	imports «crypto« functions, contains «cryp...	/img_c16-Hunter/Users/Hunter/Downloads/FTK-Imager.zip/FTK-Imager/langs/deu_adshattrdefs.dll
mssign32.dll	type="win32"<description>«Crypto« MSSi...	/img_c16-Hunter/Windows/WinSxS/x86_microsoft-windows-mssign32-dll_31bf3856ad364e35_6.3.9600.16384_none...
cryptui.dll	type="win32"<description>«Crypto« User ...	/img_c16-Hunter/Windows/System32/cryptui.dll
esp_adshattrdefs.dll	imports «crypto« functions, contains «cryp...	/img_c16-Hunter/Users/Hunter/Downloads/FTK-Imager.zip/FTK-Imager/langs/esp_adshattrdefs.dll
sve_adshattrdefs.dll	imports «crypto« functions, contains «cryp...	/img_c16-Hunter/Users/Hunter/Downloads/FTK-Imager/langs/sve_adshattrdefs.dll
setup_wm.exe	failed. Could not load «Crypto« Lib. Last r...	/img_c16-Hunter/Program Files (x86)/Windows Media Player/setup_wm.exe

Figure 19.1

20 What are the serial numbers of the two identified USB storage?

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

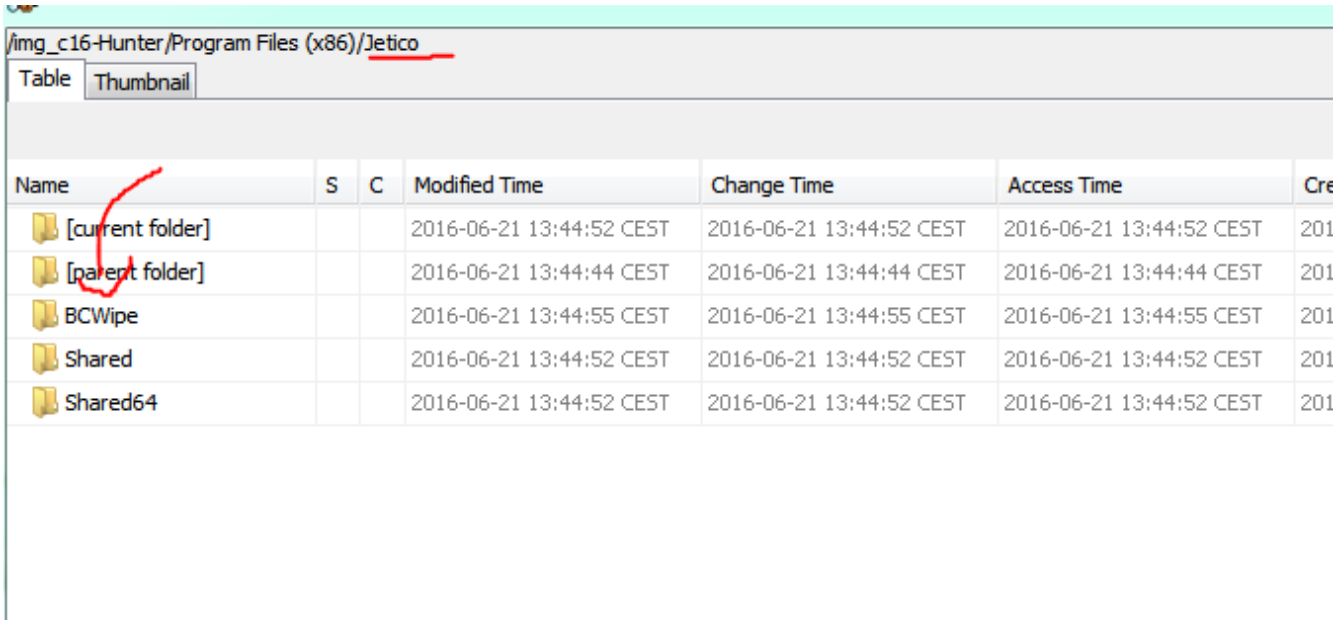


Source File	S	C	Date/Time	Device Make	Device Model	Device ID
SYSTEM			2016-06-21 13:40:44 CEST		ROOT_HUB	4&65dfc83&0
SYSTEM			2016-06-21 13:40:44 CEST		ROOT_HUB20	4&280d2b25&0
SYSTEM			2016-06-21 04:01:59 CEST	Lexar Media, Inc.	Product: A202	AAI6UXDKZDV8E9OU
SYSTEM			2016-06-21 03:53:14 CEST	Imation Corp.	Product: 063D	07B20C03C80830A9
SYSTEM			2016-06-21 14:28:34 CEST	VirtualBox	USB Tablet	5&2d7ae1ff&0&1

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

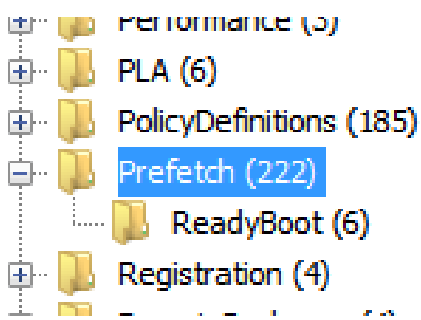


Figure 22.1

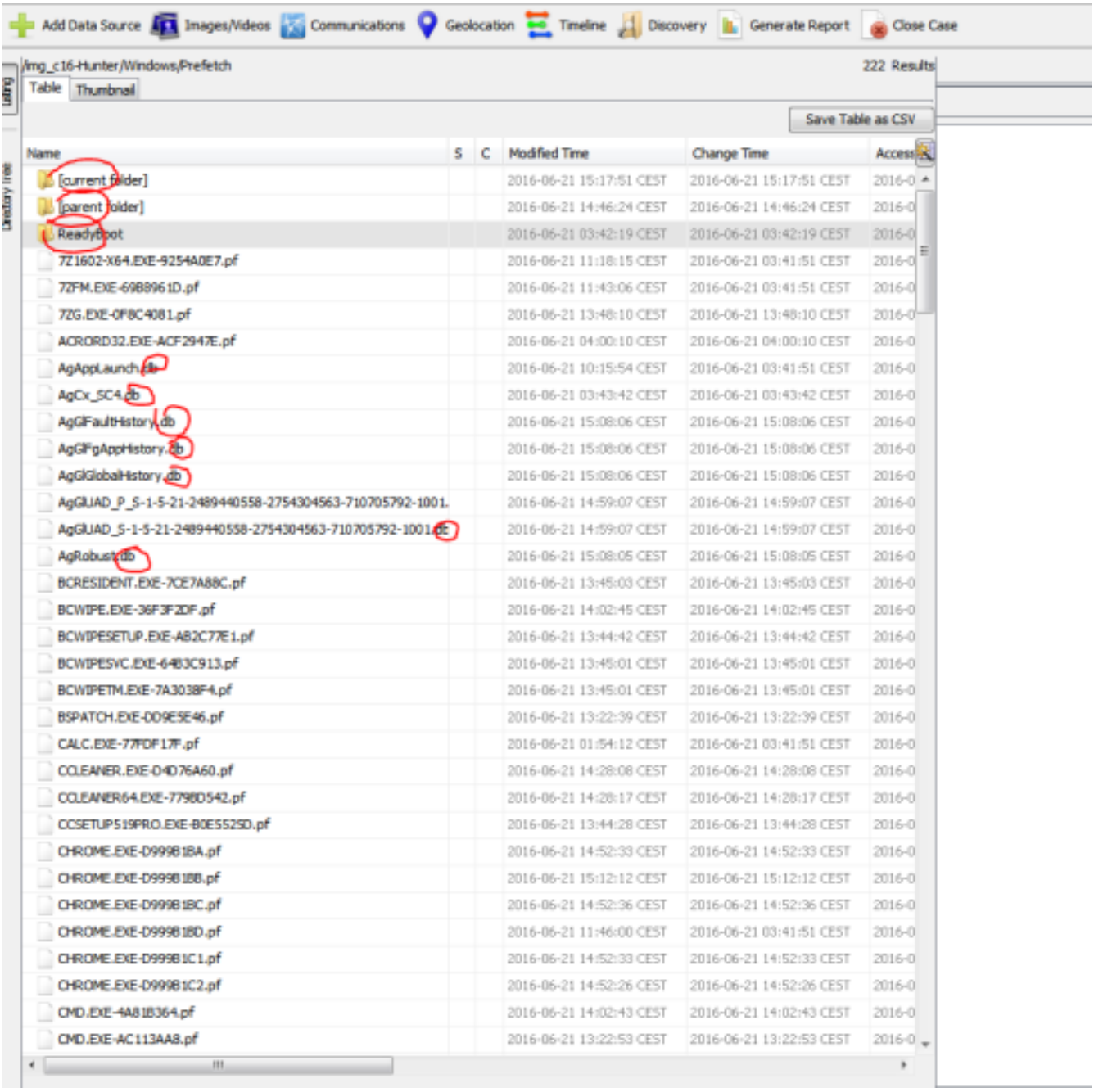

Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
/img_c16-Hunter/Windows/Prefetch
222 Results
Table
Thumbnail
Save Table as CSV
Name
S
C
Modified Time
Change Time
[current folder]
[parent folder]
ReadyBoot
7Z1602-X64.EXE-9254A0E7.pf
7ZFM.EXE-69B8961D.pf
7ZG.EXE-0F8C4081.pf
ACRORD32.EXE-ACF2947E.pf
AgAppLaunch.db
AgCx_SC4.db
AgGlFaultHistory.db
AgGlFgAppHistory.db
AgGlGlobalHistory.db
AgGlUAD_P_S-1-5-21-2489440558-2754304563-710705792-1001.
AgGlUAD_S-1-5-21-2489440558-2754304563-710705792-1001.db
AgRobust.db
BCRESIDENT.EXE-7CE7A88C.pf
BCWIPE.EXE-36F3F2DF.pf
BCWIPESETUP.EXE-AB2C77E1.pf
BCWIPESVC.EXE-64B3C913.pf
BCWIPETM.EXE-7A3038F4.pf
BSPATCH.EXE-DD9E5E46.pf
CALC.EXE-77FDF17F.pf
CCLEANER.EXE-04D76A60.pf
CCLEANER64.EXE-7798D542.pf
CCSETUP519PRO.EXE-B0E552SD.pf
CHROME.EXE-D999B1BA.pf
CHROME.EXE-D999B1BB.pf
CHROME.EXE-D999B1BC.pf
CHROME.EXE-D999B1BD.pf
CHROME.EXE-D999B1C1.pf
CHROME.EXE-D999B1C2.pf
CMD.EXE-4A81B364.pf
CMD.EXE-AC113AA8.pf

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

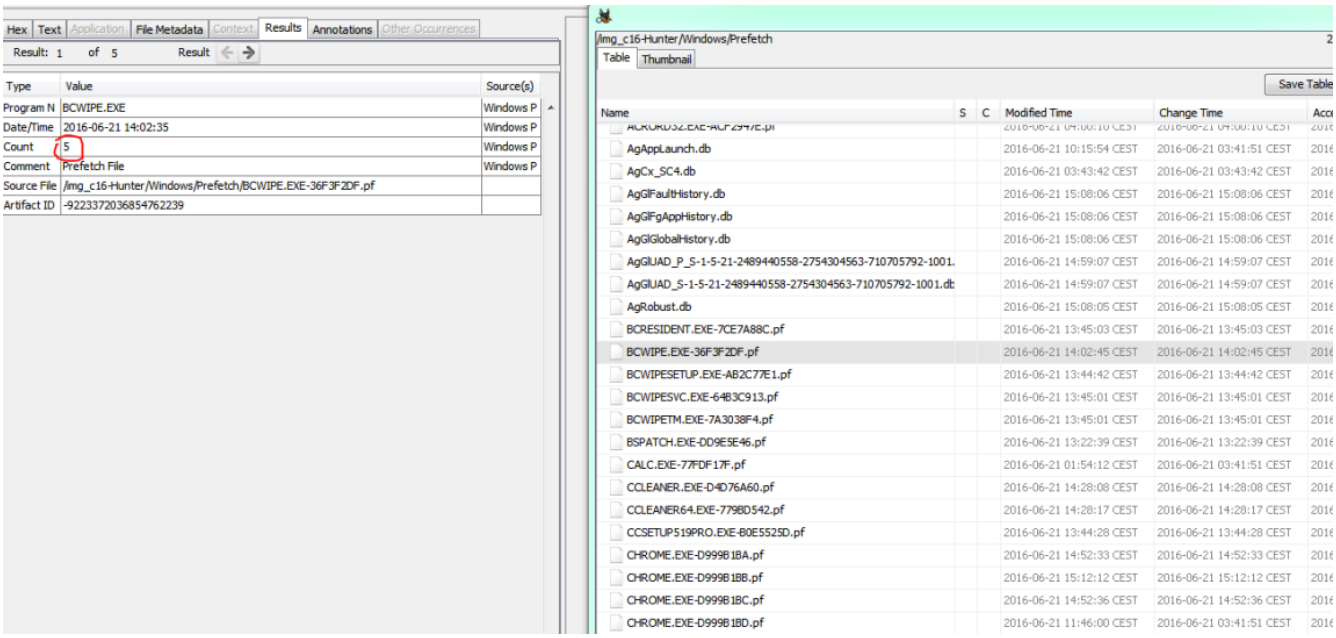


Figure 23.1

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.

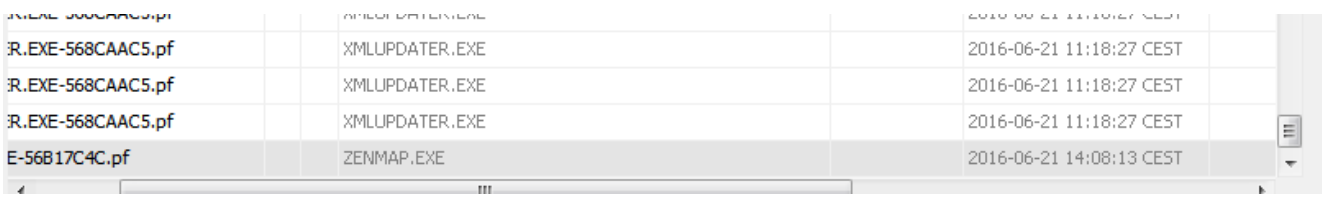


Figure 24.1

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.

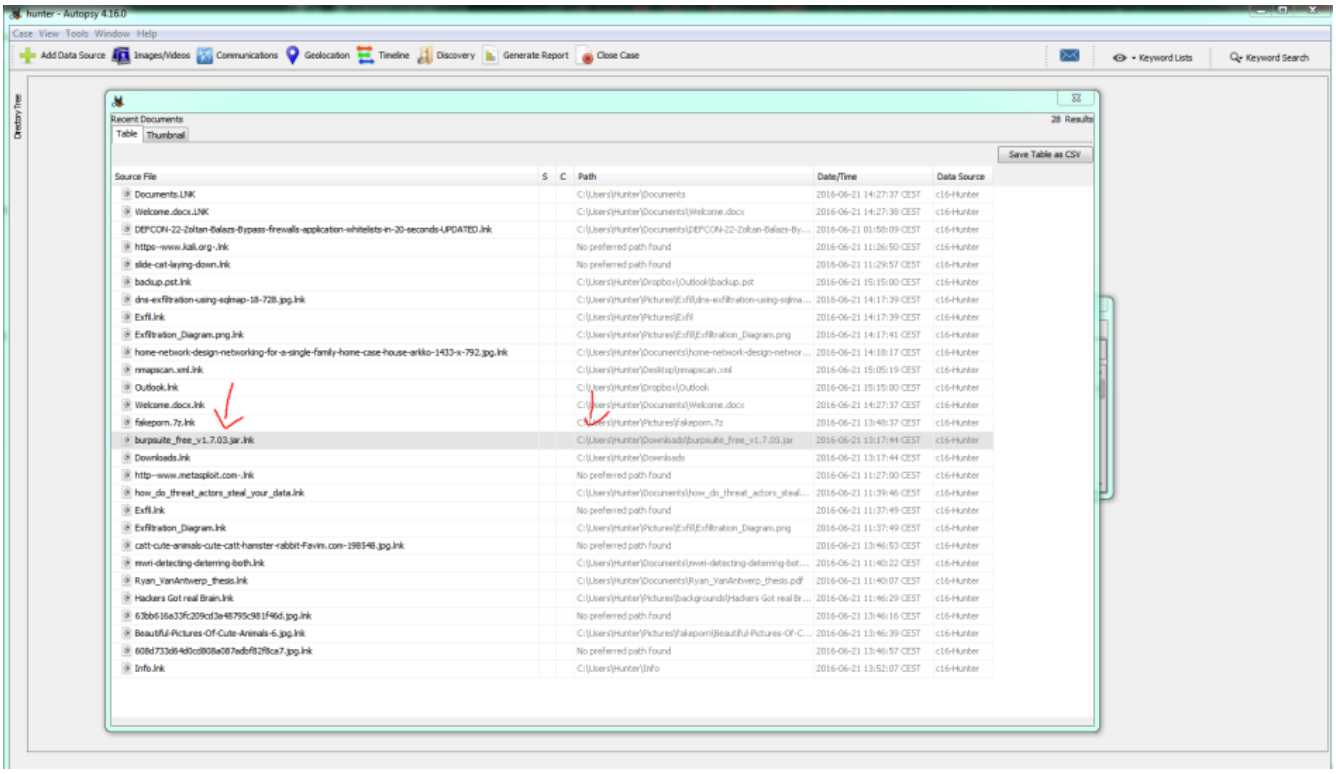


Figure 25.1

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.

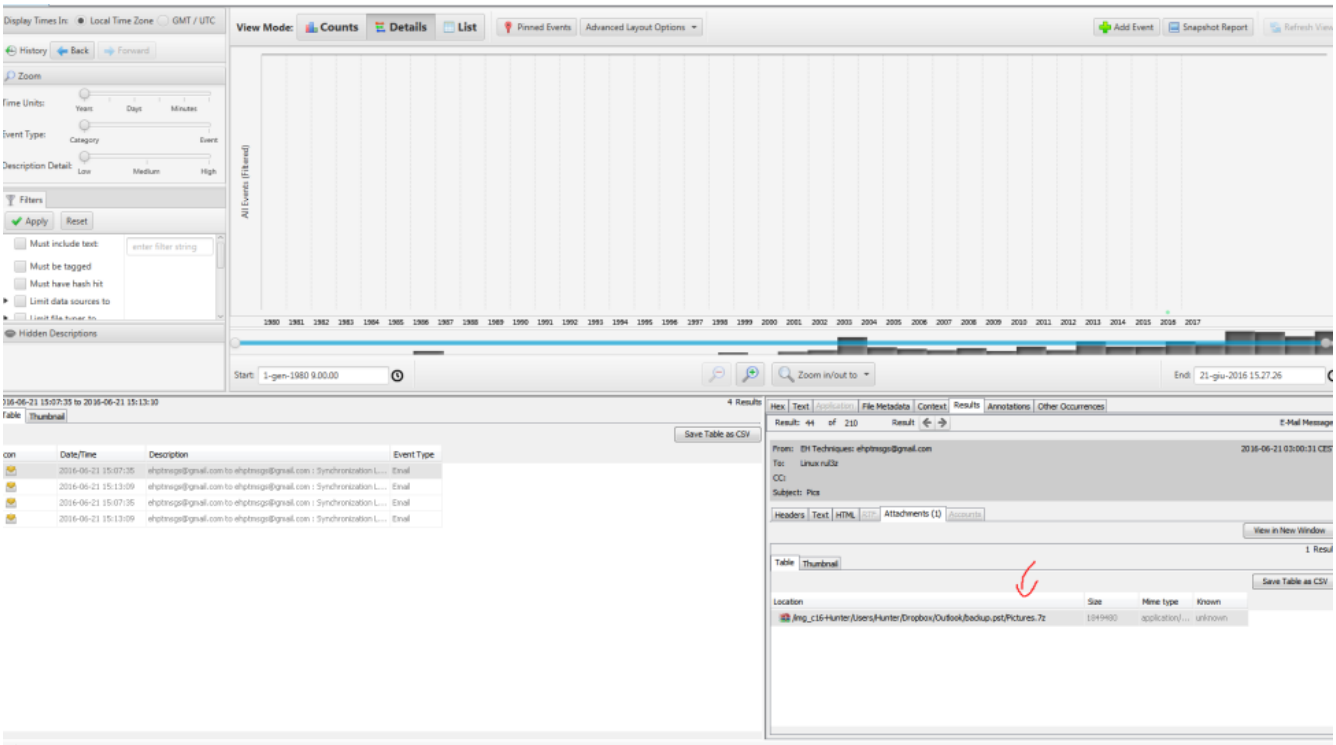


Figure 26.1

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.

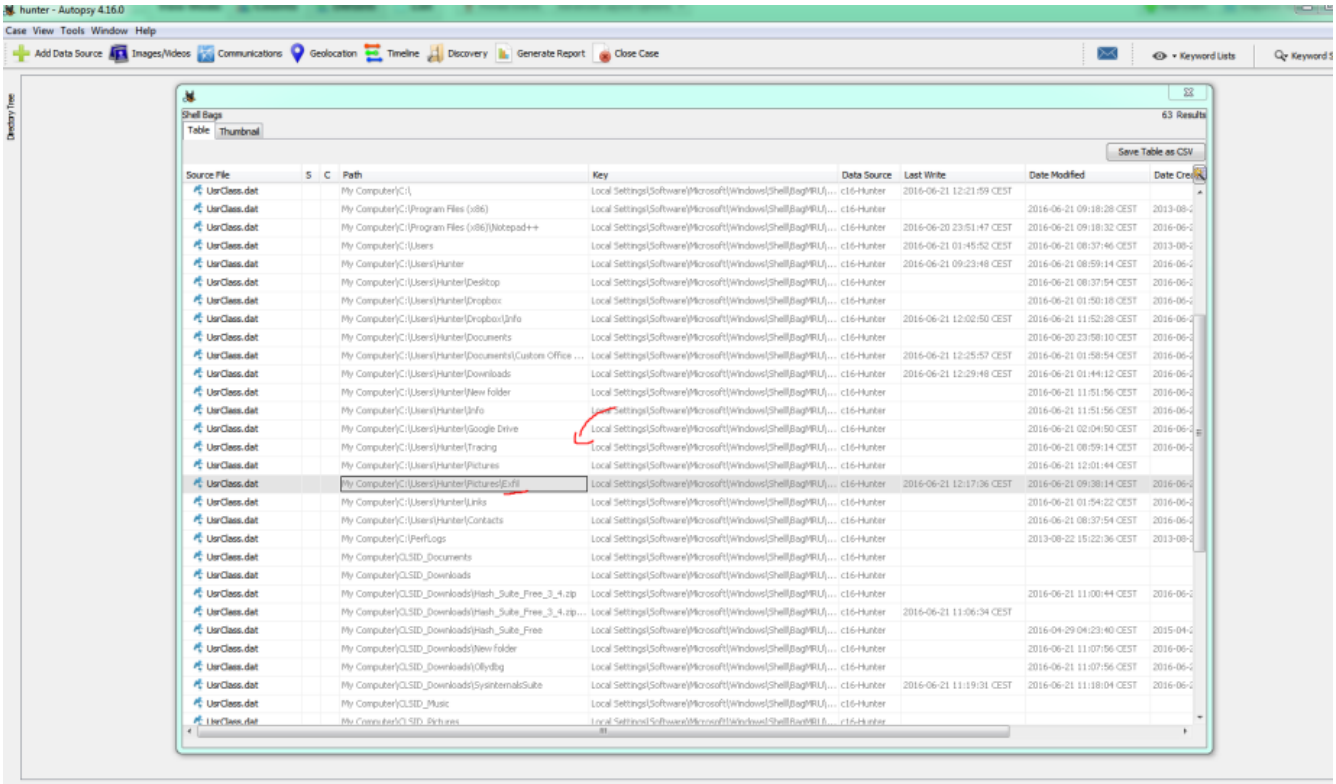


Figure 27.1

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

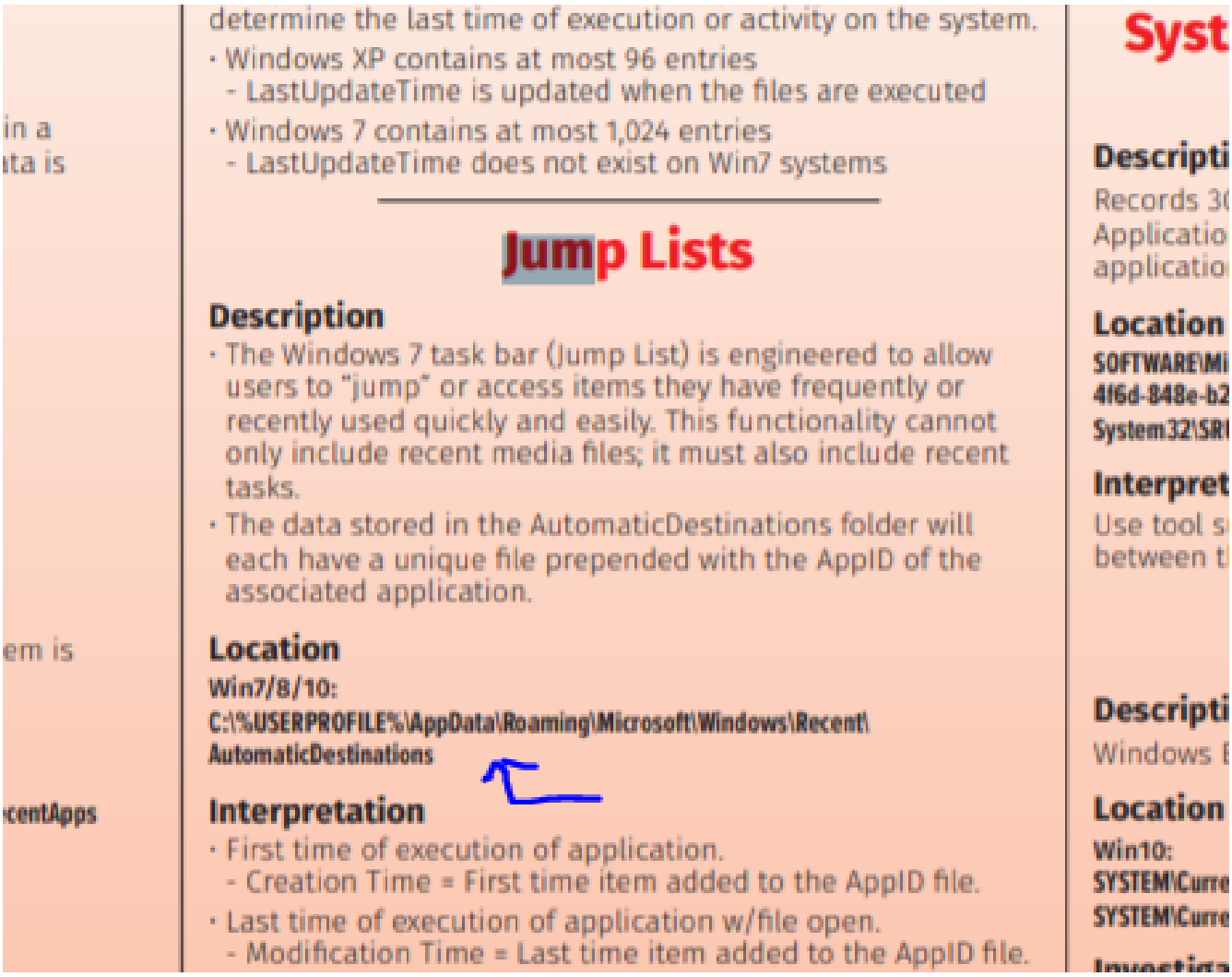
Table | Thumbnail

S	C	Path	URL	Date Accessed	Don
		C:\Users\Hunter\Downloads\SkypeSetup.exe	https://get.skype.com/go/getskype-windows	2016-06-21 10:54:19 CEST	get.
		C:\Users\Hunter\Downloads\SkypeSetup.exe	https://get.skype.com/go/getskype	2016-06-21 10:54:19 CEST	get.
		C:\Users\Hunter\Downloads\SkypeSetup.exe	https://download.skype.com/1f4a80c895182a5238c9be18...	2016-06-21 10:54:19 CEST	dow
		C:\Users\Hunter\Downloads\Wireshark-win64-2.0.4.exe	https://1.na.dl.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://admdownload.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/Kittie...	2016-06-21 11:30:00 CEST	imag
		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	imag
		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/bhutastan/Cats...	2016-06-21 11:31:39 CEST	i212
		C:\Users\Hunter\Pictures\backgrounds\F3AIS3K.jpg	http://wallpapercave.com/wp/F3AIS3K.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	imag
		C:\Users\Hunter\Pictures\backgrounds\The-Walking-Dead-Wallpap...	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://ihdwallpapers.com/download/andrew_lincoln_the_w...	2016-06-21 11:36:09 CEST	ihdw
			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.



determine the last time of execution or activity on the system.

- Windows XP contains at most 96 entries
  - LastUpdateTime is updated when the files are executed
- Windows 7 contains at most 1,024 entries
  - LastUpdateTime does not exist on Win7 systems

Jump Lists

Description

- 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.

Location

Win7/8/10:
C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

Interpretation

- First time of execution of application.
  - Creation Time = First time item added to the AppID file.
- Last time of execution of application w/file open.
  - Modification Time = Last time item added to the AppID file.

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 : $C : Browser.exe$

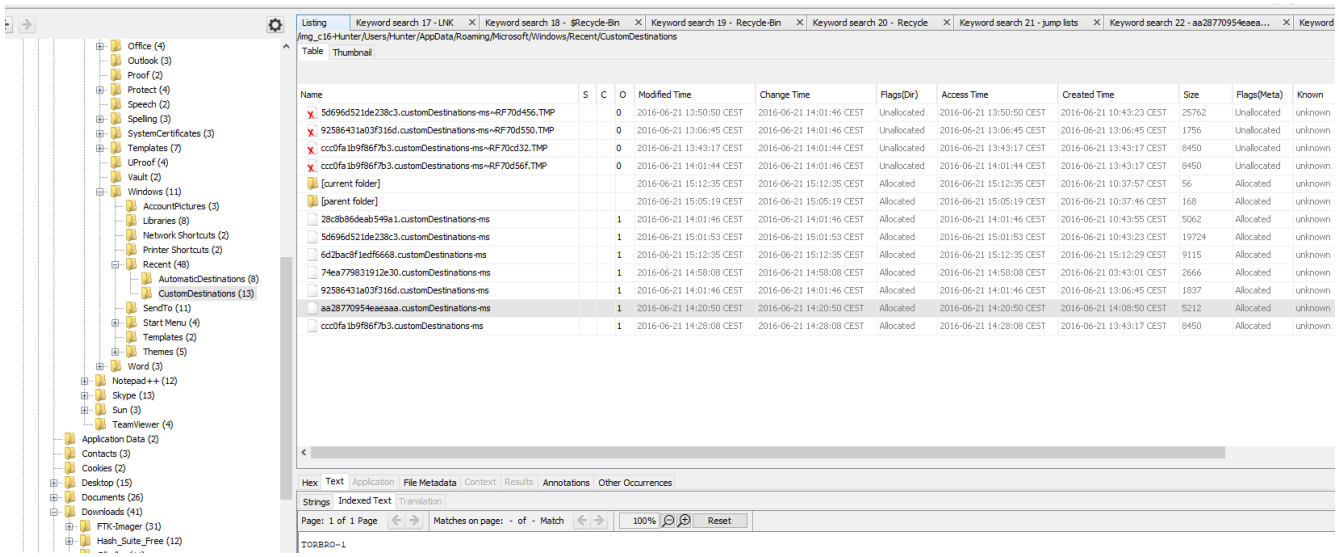


Figure 30.1

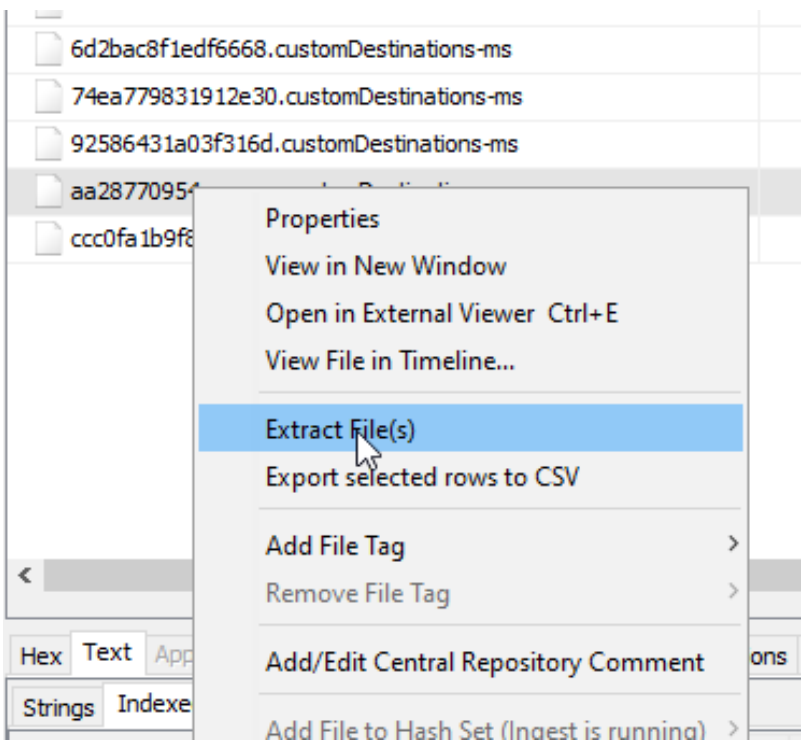


Figure 30.2

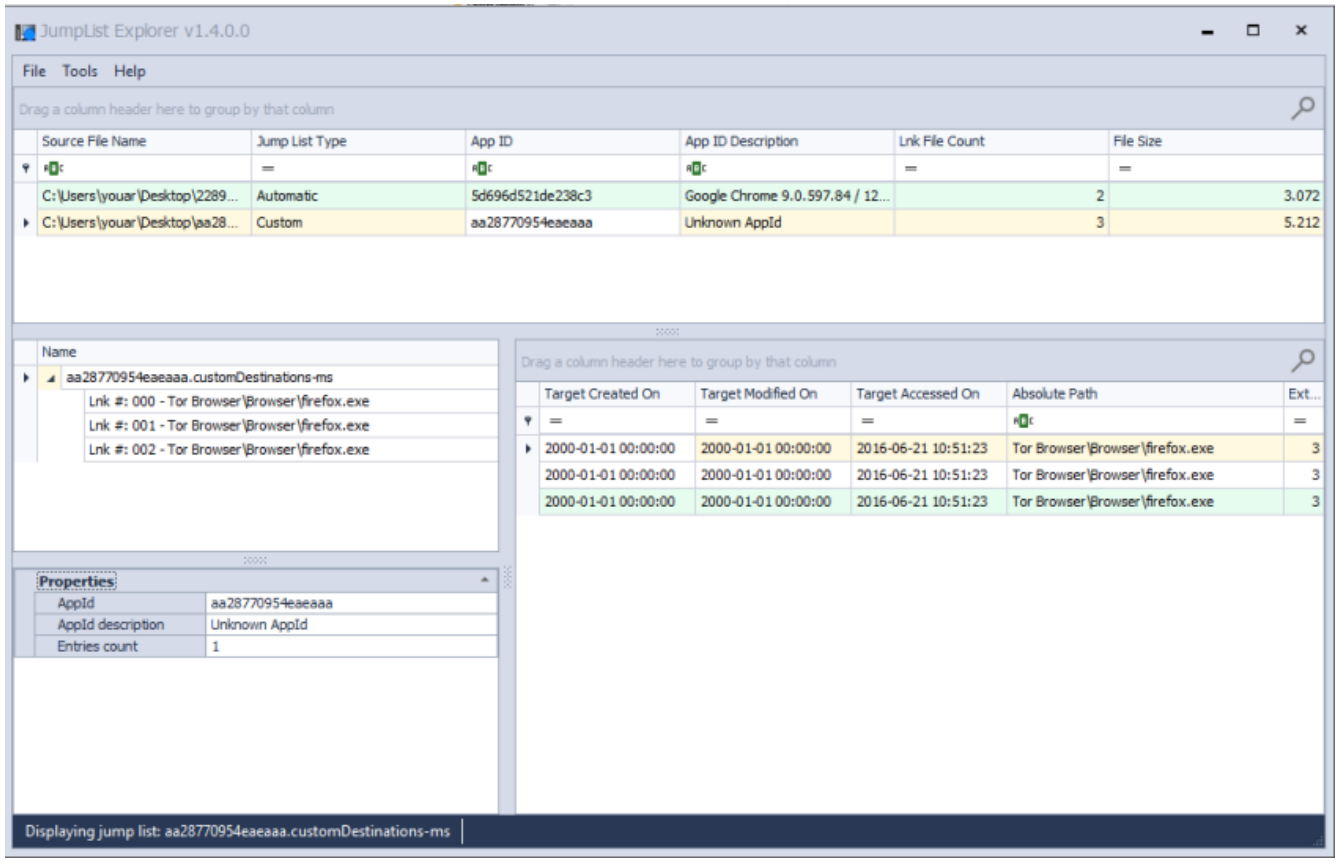

JumpList Explorer v1.4.0.0
File Tools Help
Drag a column header here to group by that column
Source File Name | Jump List Type | App ID | App ID Description | Lnk File Count | File Size
C:\Users\youar\Desktop\2289... | Automatic | 5d696d521de238c3 | Google Chrome 9.0.597.84 / 12... | 2 | 3.072
C:\Users\youar\Desktop\aa28... | Custom | aa28770954eaeaaa | Unknown AppId | 3 | 5.212
Name
aa28770954eaeaaa.customDestinations-ms
Lnk #: 000 - Tor Browser\Browser\firefox.exe
Lnk #: 001 - Tor Browser\Browser\firefox.exe
Lnk #: 002 - Tor Browser\Browser\firefox.exe
Drag a column header here to group by that column
Target Created On | Target Modified On | Target Accessed On | Absolute Path | Ext...
2000-01-01 00:00:00 | 2000-01-01 00:00:00 | 2016-06-21 10:51:23 | Tor Browser\Browser\firefox.exe | 3
2000-01-01 00:00:00 | 2000-01-01 00:00:00 | 2016-06-21 10:51:23 | Tor Browser\Browser\firefox.exe | 3
2000-01-01 00:00:00 | 2000-01-01 00:00:00 | 2016-06-21 10:51:23 | Tor Browser\Browser\firefox.exe | 3
Properties
AppId | aa28770954eaeaaa
AppId description | Unknown AppId
Entries count | 1
Displaying jump list: aa28770954eaeaaa.customDestinations-ms

Figure 30.3