Challenge: Hunter Lab

Platform: CyberDefenders

Category: Endpoint Forensics

Difficulty: Medium

Tools Used: FTK Imager, Registry Explorer, DCode, EvtxECmd, Timeline Explorer, PECmd, Sublime, DB Browser for SQLite, SysTools Outlook PST Viewer, ShellBags Explorer, JumpListExplorer

Summary: This challenge involved investigating an insider threat scenario, requiring the use of a series of tools. I found it relatively easy, because most questions direct you to look at a certain artifact, meaning you only need to figure out how to parse/view/analyse said artifact. That being said, this was a really enjoyable and insightful lab as it covers a bunch of Windows forensic artifacts, including extracting host information from registry, event logs, Prefetch, PST files, ShellBags, Jump Lists, and more.

Scenario: The SOC team got an alert regarding some illegal port scanning activity coming from an employee's system. The employee was not authorized to do any port scanning or any offensive hacking activity within the network. The employee claimed that he had no idea about that, and it is probably a malware acting on his behalf. The IR team managed to respond immediately and take a full forensic image of the user's system to perform some investigations.

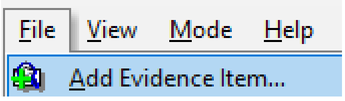
There is a theory that the user intentionally installed illegal applications to do port scanning and maybe other things. He was probably planning for something bigger, far beyond a port scanning!

It all began when the user asked for a salary raise that was rejected. After that, his behavior was abnormal and different. The suspect is believed to have weak technical skills, and there might be an outsider helping him!

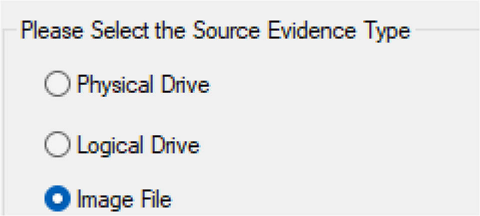
Your objective as a soc analyst is to analyze the image and to either confirm or deny this theory.

What is the computer name of the suspect machine?

Once you have extracted the lab zip file, you can find a single disk image, let's start by loading this into FTK Imager. To do so, navigate to File > Add Evidence Item:



Select Image File > Next:



Please Select the Source Evidence Type

○ Physical Drive

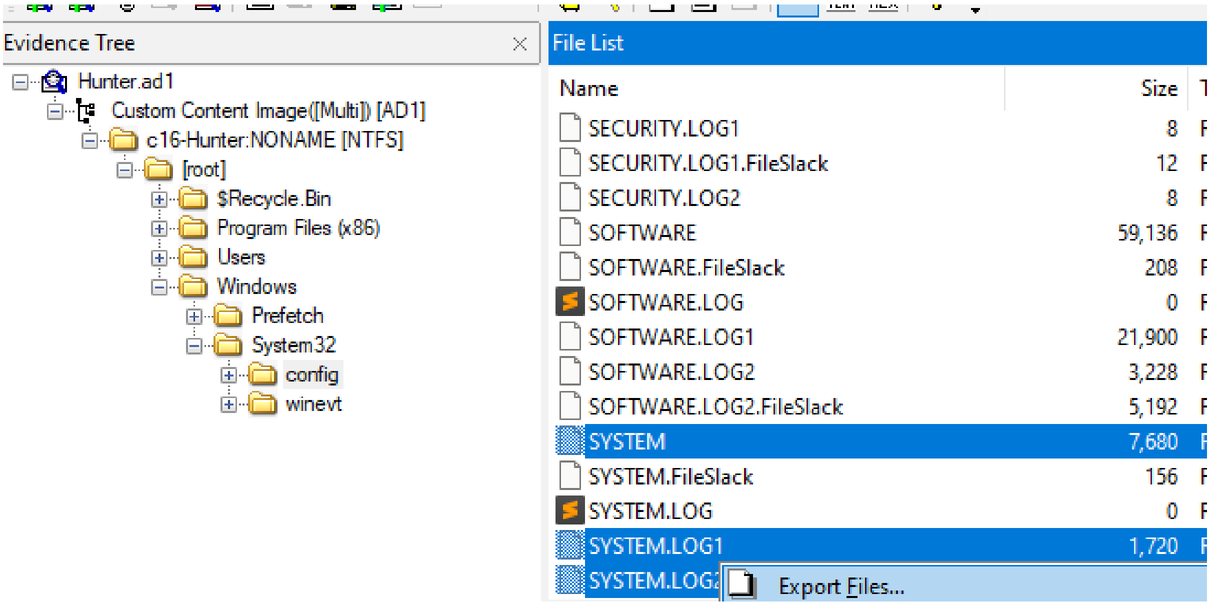
○ Logical Drive

● Image File

Browse to the .ad1 image extracted from the zip file, select it, and click Finish. To start, let's dump the SYSTEM registry hive, located at:

- `%SystemRoot%\System32\config\`

Here you will find a file called SYSTEM, SYSTEM.LOG1 and SYSTEM.LOG2. Export all these files by selecting them, then right-click > Export files:



Evidence Tree

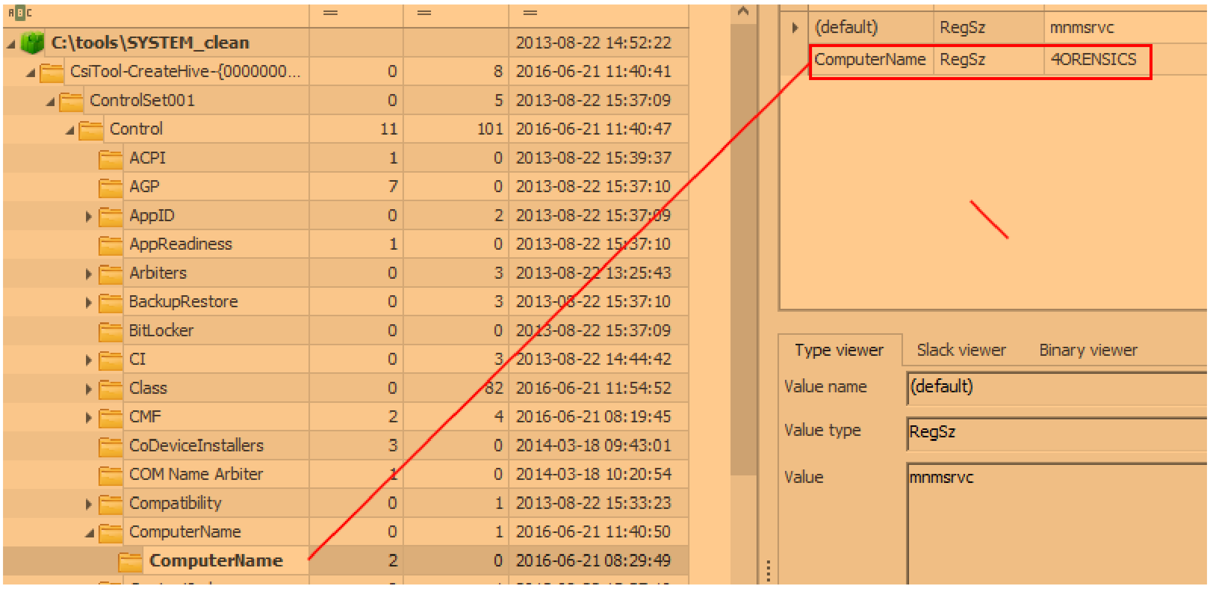
- Hunter.ad1
  - Custom Content Image([Multi]) [AD1]
    - c16-Hunter:NONAME [NTFS]
      - [root]
        - $Recycle.Bin
        - Program Files (x86)
        - Users
        - Windows
          - Prefetch
          - System32
            - config
            - winevt

File List

Name	Size	T
SECURITY.LOG1	8	F
SECURITY.LOG1.FileSlack	12	F
SECURITY.LOG2	8	F
SOFTWARE	59,136	F
SOFTWARE.FileSlack	208	F
SOFTWARE.LOG	0	F
SOFTWARE.LOG1	21,900	F
SOFTWARE.LOG2	3,228	F
SOFTWARE.LOG2.FileSlack	5,192	F
SYSTEM	7,680	F
SYSTEM.FileSlack	156	F
SYSTEM.LOG	0	F
SYSTEM.LOG1	1,720	F
SYSTEM.LOG2		

We can use a tool called Registry Explorer to load this hive. Once you have loaded the clean SYSTEM hive, navigate to:

- SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName



C:\tools\SYSTEM_clean			2013-08-22 14:52:22
CsiTool-CreateHive-{0000000...	0	8	2016-06-21 11:40:41
ControlSet001	0	5	2013-08-22 15:37:09
Control	11	101	2016-06-21 11:40:47
ACPI	1	0	2013-08-22 15:39:37
AGP	7	0	2013-08-22 15:37:10
AppID	0	2	2013-08-22 15:37:09
AppReadiness	1	0	2013-08-22 15:37:10
Arbiters	0	3	2013-08-22 13:25:43
BackupRestore	0	3	2013-08-22 15:37:10
BitLocker	0	0	2013-08-22 15:37:09
CI	0	3	2013-08-22 14:44:42
Class	0	82	2016-06-21 11:54:52
CMF	2	4	2016-06-21 08:19:45
CoDeviceInstallers	3	0	2014-03-18 09:43:01
COM Name Arbiter	1	0	2014-03-18 10:20:54
Compatibility	0	1	2013-08-22 15:33:23
ComputerName	0	1	2016-06-21 11:40:50
ComputerName	2	0	2016-06-21 08:29:49

(default)	RegSz	mnmsrvc
ComputerName	RegSz	4ORENSICS

Value name (default)

Value type RegSz

Value mnmsrvc

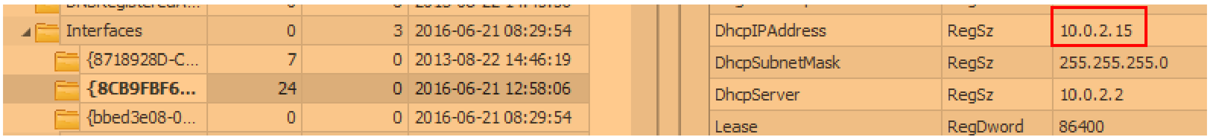
As you can see, the computer name is 4ORENSICS.

Answer: 4ORENSICS

What is the computer IP?

You can find the network interfaces and assigned IPs by navigating to the following registry key:

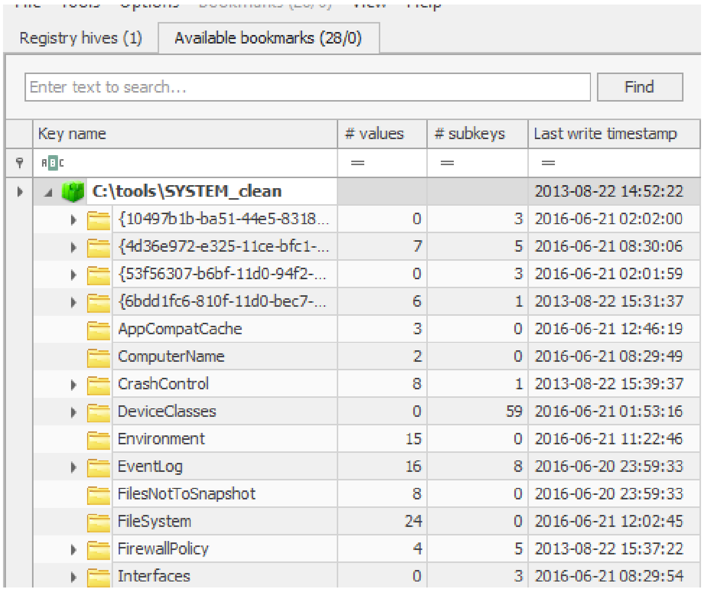
- `SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces`



Interfaces	0	3	2016-06-21 08:29:54
{8718928D-C...	7	0	2013-08-22 14:46:19
{8CB9FBF6...	24	0	2016-06-21 12:58:06
{bbed3e08-0...	0	0	2016-06-21 08:29:54

DhcpIPAddress	RegSz	10.0.2.15
DhcpSubnetMask	RegSz	255.255.255.0
DhcpServer	RegSz	10.0.2.2
Lease	RegDword	86400

Here we can find the DHCP leased IP address. Quick tip, within Registry Explorer is an Available Bookmarks tab. If you click this tab, you can see bookmarks which take you directly to key forensic artifacts within the respective loaded hive(s):



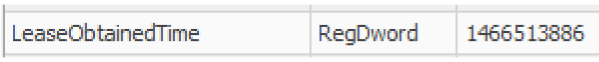
Key name	# values	# subkeys	Last write timestamp
C:\tools\SYSTEM_clean			2013-08-22 14:52:22
{10497b1b-ba51-44e5-8318...	0	3	2016-06-21 02:02:00
{4d36e972-e325-11ce-bfc1-...	7	5	2016-06-21 08:30:06
{53f56307-b6bf-11d0-94f2-...	0	3	2016-06-21 02:01:59
{6bdd1fc6-810f-11d0-bec7-...	6	1	2013-08-22 15:31:37
AppCompatCache	3	0	2016-06-21 12:46:19
ComputerName	2	0	2016-06-21 08:29:49
CrashControl	8	1	2013-08-22 15:39:37
DeviceClasses	0	59	2016-06-21 01:53:16
Environment	15	0	2016-06-21 11:22:46
EventLog	16	8	2016-06-20 23:59:33
FilesNotToSnapshot	8	0	2016-06-20 23:59:33
FileSystem	24	0	2016-06-21 12:02:45
FirewallPolicy	4	5	2013-08-22 15:37:22
Interfaces	0	3	2016-06-21 08:29:54

This is helpful to quickly navigate to key artifacts.

Answer: 10.0.2.15

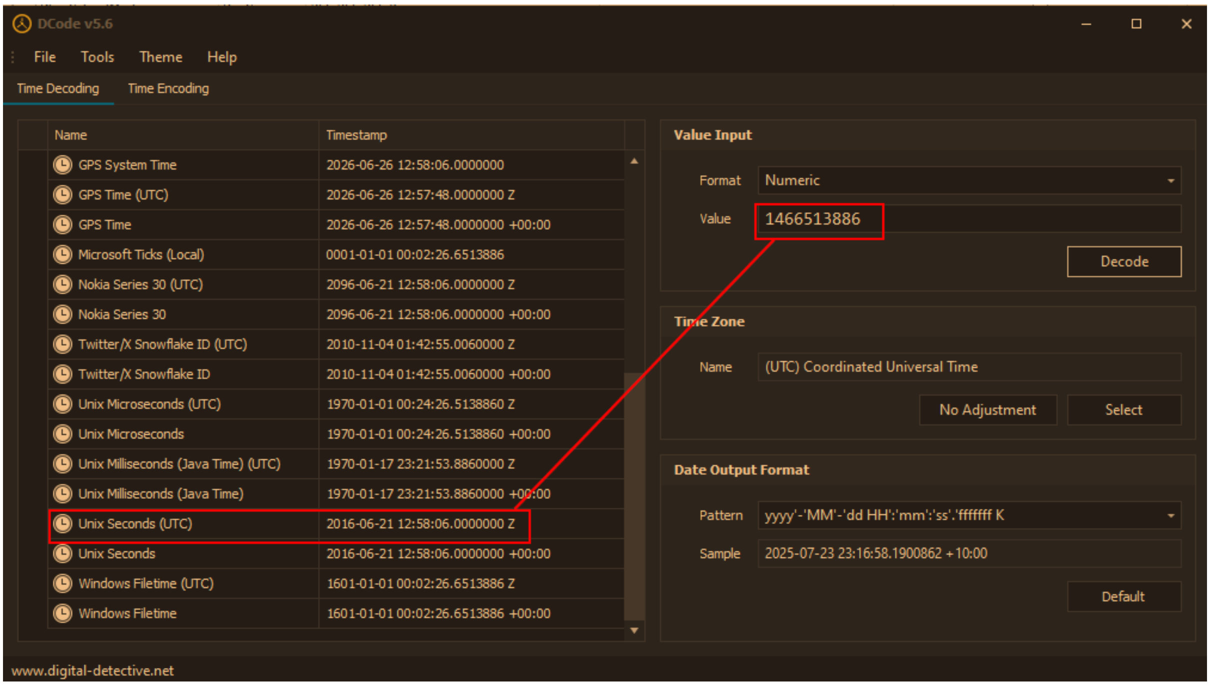
What was the DHCP LeaseObtainedTime?

Continuing with the previous question, scroll down and you will find the LeastObtainedTime value:



LeaseObtainedTime	RegDword	1466513886

You can probably tell that this is not a typical timestamp. If you enter it into a tool like Dcode, you can find the UTC timestamp:



Name	Timestamp
GPS System Time	2026-06-26 12:58:06.0000000
GPS Time (UTC)	2026-06-26 12:57:48.0000000 Z
GPS Time	2026-06-26 12:57:48.0000000 +00:00
Microsoft Ticks (Local)	0001-01-01 00:02:26.6513886
Nokia Series 30 (UTC)	2096-06-21 12:58:06.0000000 Z
Nokia Series 30	2096-06-21 12:58:06.0000000 +00:00
Twitter/X Snowflake ID (UTC)	2010-11-04 01:42:55.0060000 Z
Twitter/X Snowflake ID	2010-11-04 01:42:55.0060000 +00:00
Unix Microseconds (UTC)	1970-01-01 00:24:26.5138860 Z
Unix Microseconds	1970-01-01 00:24:26.5138860 +00:00
Unix Milliseconds (Java Time) (UTC)	1970-01-17 23:21:53.8860000 Z
Unix Milliseconds (Java Time)	1970-01-17 23:21:53.8860000 +00:00
Unix Seconds (UTC)	2016-06-21 12:58:06.0000000 Z
Unix Seconds	2016-06-21 12:58:06.0000000 +00:00
Windows Filetime (UTC)	1601-01-01 00:02:26.6513886 Z
Windows Filetime	1601-01-01 00:02:26.6513886 +00:00

Value Input

Format: Numeric

Value: 1466513886

Time Zone

Name: (UTC) Coordinated Universal Time

No Adjustment

Date Output Format

Pattern: yyyy'-'MM'-'dd HH':'mm':'ss'.'fffffff K

Sample: 2025-07-23 23:16:58.1900862 +10:00

Answer: 21/06/2016 02:24:12 UTC

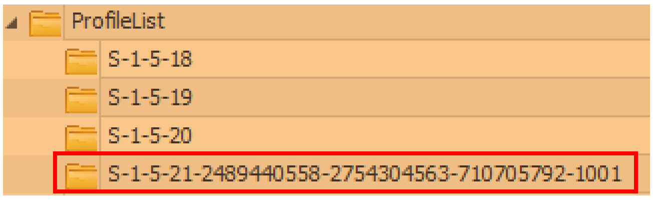
What is the computer SID?

To find the computer SID, we need to dump the SOFTWARE registry hive located at:

- `%SystemRoot%\System32\config`

You can find the computer SID at:

- `SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList`



ProfileList
- S-1-5-18
- S-1-5-19
- S-1-5-20
- S-1-5-21-2489440558-2754304563-710705792-1001

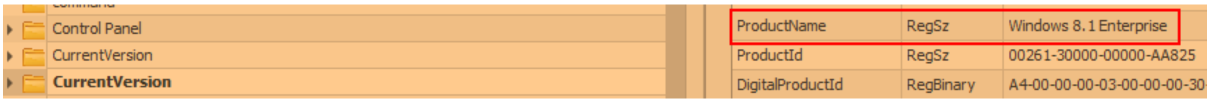
The last part of this key is the RID (Relative Identifier), which identifies a specific user or group within the computer. You can omit this from the answer in this lab.

Answer: S-1-5-21-2489440558-2754304563-710705792

What is the Operating System(OS) version?

You can find the OS version within the SOFTWARE hive, located at:

- `SOFTWARE\Microsoft\Windows NT\CurrentVersion`



- Control Panel
- CurrentVersion
- **CurrentVersion**

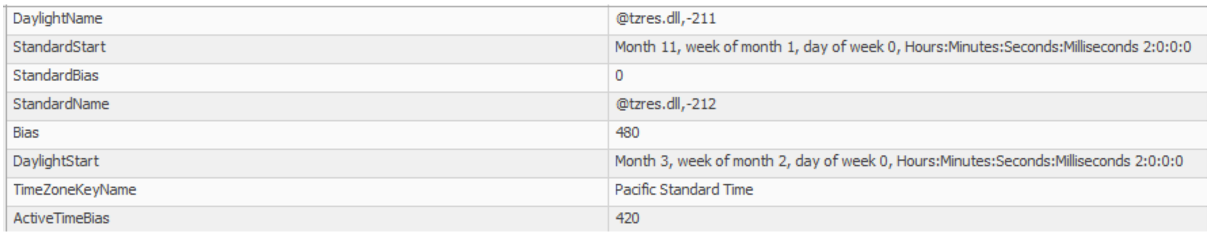
ProductName	RegSz	Windows 8.1 Enterprise
ProductId	RegSz	00261-30000-00000-AA825
DigitalProductId	RegBinary	A4-00-00-00-03-00-00-00-30

Answer: 8.1

What was the computer timezone?

Time zone information is found within the SYSTEM hive, located at:

- `SYSTEM\CurrentControlSet\Control\TimeZoneInformation`



DaylightName	@tzres.dll,-211
StandardStart	Month 11, week of month 1, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0
StandardBias	0
StandardName	@tzres.dll,-212
Bias	480
DaylightStart	Month 3, week of month 2, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0
TimeZoneKeyName	Pacific Standard Time
ActiveTimeBias	420

Given this information, the timzeone is UTC-07:00.

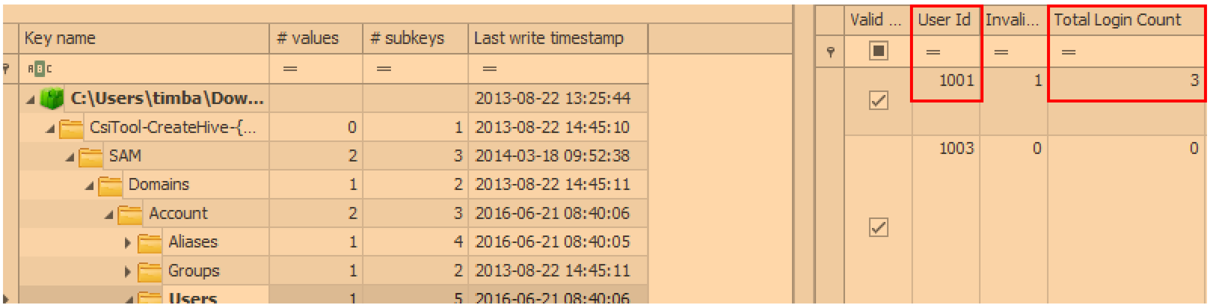
Answer: UTC-07:00

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

Within the SAM registry file is a key the records the Total Logon Count for each user. It is located at:

- `SAM\Domains\Account\Users`

We can use Registry Explorer to view this key and focus on the User ID 1001:



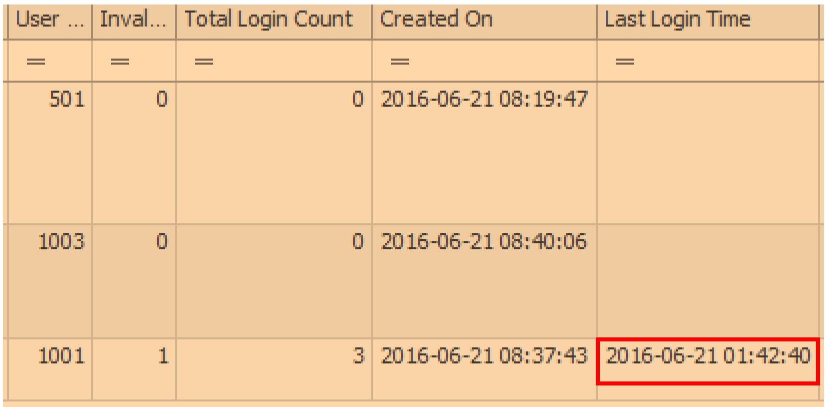
Key name	# values	# subkeys	Last write timestamp
C:\Users\timba\Dow...			2013-08-22 13:25:44
CsiTool-CreateHive-{...	0	1	2013-08-22 14:45:10
SAM	2	3	2014-03-18 09:52:38
Domains	1	2	2013-08-22 14:45:11
Account	2	3	2016-06-21 08:40:06
Aliases	1	4	2016-06-21 08:40:05
Groups	1	2	2013-08-22 14:45:11
Users	1	5	2016-06-21 08:40:06

Valid ...	User Id	Invali...	Total Login Count
☑	1001	1	3
☑	1003	0	0

Answer: 3

When was the last login time for the discovered account? Format: one-space between date and time

The last login time can also be found within the SAM registry hive, at the same location as the previous question:

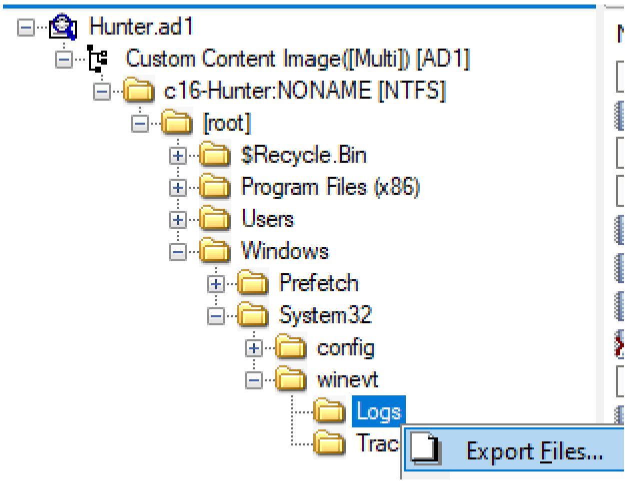


User ...	Inval...	Total Login Count	Created On	Last Login Time
=	=	=	=	=
501	0	0	2016-06-21 08:19:47	
1003	0	0	2016-06-21 08:40:06	
1001	1	3	2016-06-21 08:37:43	2016-06-21 01:42:40

You can also answer this question by dumping the security events logs, as these record all authentication related events. Event logs are found at:

- `%SystemRoot%\System32\winevt\Logs`

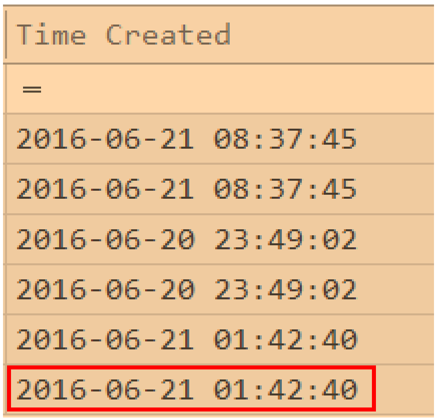
I am going to dump the entire directory, although you only need the Security.evtx logs for this question:



We can use a tool called EvtxECmd to parse the Security.evtx log, and view the output in Timeline Explorer:

- `.\EvtxECmd.exe -f ".\Security.evtx" --csv . --csvf security_out.csv`
  - -f specifies the event log to parse.
  - --csv tells EvtxECmd to output the results in csv format.
  - --csvf specifies the output filename.

Every successful authentication generates a log with event ID 4624; we can filter for this event ID and search for the SID to see the last login timestamp:



Time Created
=
2016-06-21 08:37:45
2016-06-21 08:37:45
2016-06-20 23:49:02
2016-06-20 23:49:02
2016-06-21 01:42:40
2016-06-21 01:42:40

Answer: 2016-06-21 01:42:40

There was a "Network Scanner" running on this computer, what was it? And when was the last time the suspect used it? Format: program.exe,YYYY-MM-DD HH:MM:SS UTC

Windows Prefetch files were introduced in Windows XP; they were designed to speed up the application startup process by preloading a snippet of code in commonly used programs. Prefetch files contain the:

- Name of the executable
- Count of how many times the executable was run
- Timestamp indicating the last 8 times the program was executed (Windows 8+), and more.

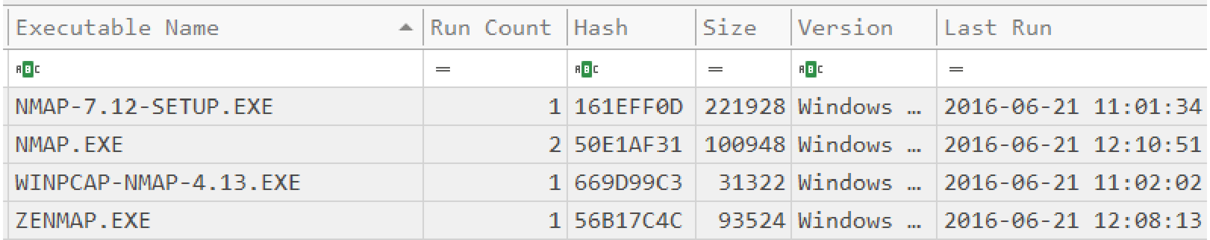
We can use this artifact to prove when the network scanner was executed. Prefetch files are located at:

- `%SystemRoot%\Prefetch`

Export the entire Prefetch directory using FTK Imager. We can then parse this entire directory using a tool called PECmd:

- `.\PECmd.exe -d ".\Prefetch\" --csv . --csvf prefetch_out.csv`
  - -d specifies the directory to recursively parse.
  - --csv tells PECmd to output the results in csv format.
  - --csvf specifies the output filename.

This outputs two CSV files, <filename>.csv and <filename>_Timeline.csv. I am going to focus on the <filename>.csv file to look for any network scanning tools:



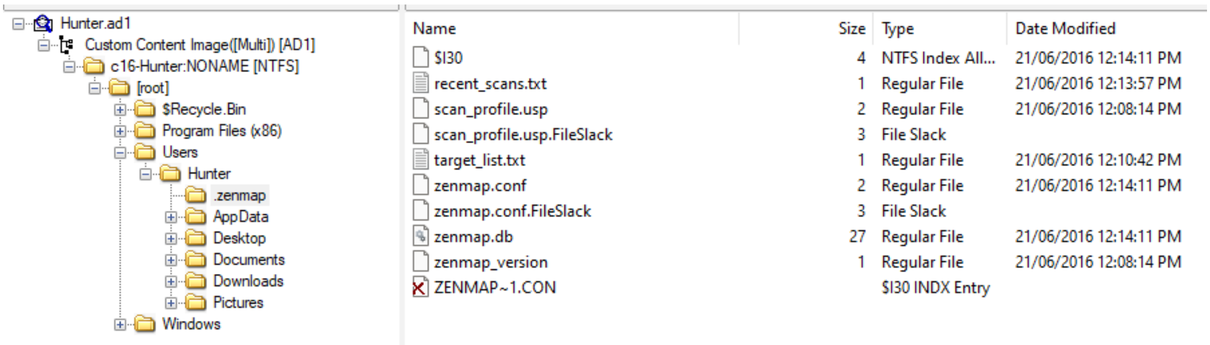
Executable Name	Run Count	Hash	Size	Version	Last Run
ABC	=	ABC	=	ABC	=
NMAP-7.12-SETUP.EXE	1	161EFF0D	221928	Windows ...	2016-06-21 11:01:34
NMAP.EXE	2	50E1AF31	100948	Windows ...	2016-06-21 12:10:51
WINPCAP-NMAP-4.13.EXE	1	669D99C3	31322	Windows ...	2016-06-21 11:02:02
ZENMAP.EXE	1	56B17C4C	93524	Windows ...	2016-06-21 12:08:13

As you can see, there are multiple entries for nmap, a popular network scanner. After some trial and error, it turns out that zenmap.exe is the correct answer. For context, Zenmap is the GUI version of namp.

Answer: ZENMAP.EXE,2016-06-21 12:08:13 UTC

When did the port scan end? (Example: Sat Jan 23 hh:mm:ss 2016)

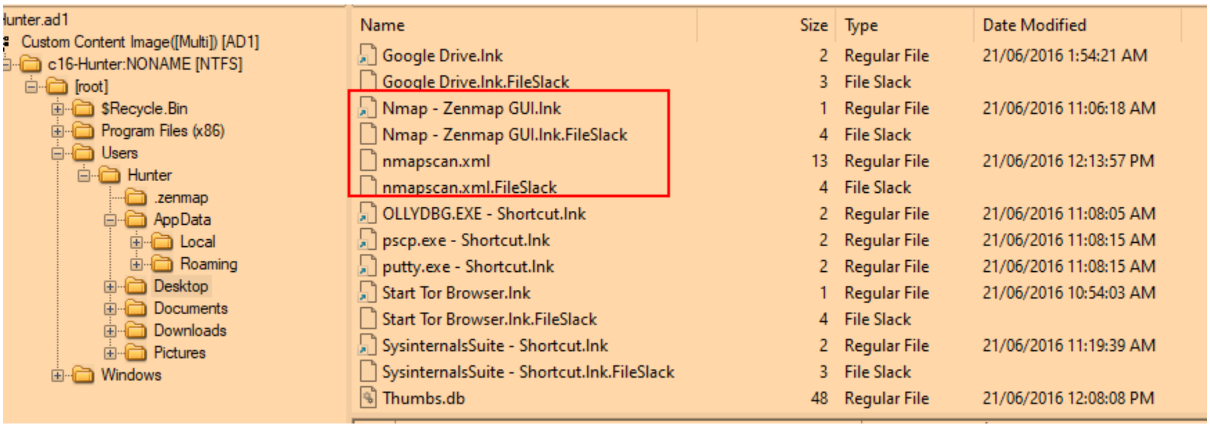
To determine when the port scan finished, we likely need to hunt for an artifact left over by Zenmap. In the home directory of 'Hunter' we can see a directory for zenmap that likely contains information about scans:



```
Hunter.ad1
  Custom Content Image([Multi]) [AD1]
    c16-Hunter:NONAME [NTFS]
      [root]
        $Recycle.Bin
        Program Files (x86)
        Users
          Hunter
            .zenmap
            AppData
            Desktop
            Documents
            Downloads
            Pictures
        Windows
```

Name	Size	Type	Date Modified
$I30	4	NTFS Index All...	21/06/2016 12:14:11 PM
recent_scans.txt	1	Regular File	21/06/2016 12:13:57 PM
scan_profile.usp	2	Regular File	21/06/2016 12:08:14 PM
scan_profile.usp.FileSlack	3	File Slack	
target_list.txt	1	Regular File	21/06/2016 12:10:42 PM
zenmap.conf	2	Regular File	21/06/2016 12:14:11 PM
zenmap.conf.FileSlack	3	File Slack	
zenmap.db	27	Regular File	21/06/2016 12:14:11 PM
zenmap_version	1	Regular File	21/06/2016 12:08:14 PM
ZENMAP~1.CON		$I30 INDX Entry	

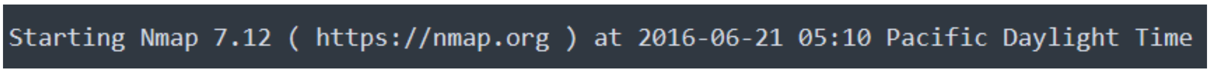
After looking through the files, there doesn't seem to be anything of use. I kept exploring until I found something interesting in the User's desktop folder:



```
Hunter.ad1
  Custom Content Image([Multi]) [AD1]
    c16-Hunter:NONAME [NTFS]
      [root]
        $Recycle.Bin
        Program Files (x86)
        Users
          Hunter
            .zenmap
            AppData
              Local
              Roaming
            Desktop
            Documents
            Downloads
            Pictures
        Windows
```

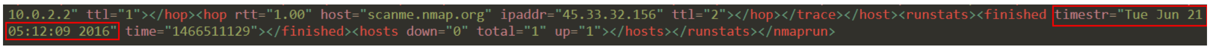
Name	Size	Type	Date Modified
Google Drive.lnk	2	Regular File	21/06/2016 1:54:21 AM
Google Drive.lnk.FileSlack	3	File Slack	
Nmap - Zenmap GUI.lnk	1	Regular File	21/06/2016 11:06:18 AM
Nmap - Zenmap GUI.lnk.FileSlack	4	File Slack	
nmapscan.xml	13	Regular File	21/06/2016 12:13:57 PM
nmapscan.xml.FileSlack	4	File Slack	
OLLYDBG.EXE - Shortcut.lnk	2	Regular File	21/06/2016 11:08:05 AM
pscp.exe - Shortcut.lnk	2	Regular File	21/06/2016 11:08:15 AM
putty.exe - Shortcut.lnk	2	Regular File	21/06/2016 11:08:15 AM
Start Tor Browser.lnk	1	Regular File	21/06/2016 10:54:03 AM
Start Tor Browser.lnk.FileSlack	4	File Slack	
SysinternalsSuite - Shortcut.lnk	2	Regular File	21/06/2016 11:19:39 AM
SysinternalsSuite - Shortcut.lnk.FileSlack	3	File Slack	
Thumbs.db	48	Regular File	21/06/2016 12:08:08 PM

Other than artifacts left from nmap, we can also see other interesting files for Tor and putty. After exporting the nmapscan.xml file and opening it up using Sublime, I found something interesting:



```
Starting Nmap 7.12 ( https://nmap.org ) at 2016-06-21 05:10 Pacific Daylight Time
```

This file appears to be the output of a nmap scan, the start time is found above, and the end time can be seen right at the bottom:

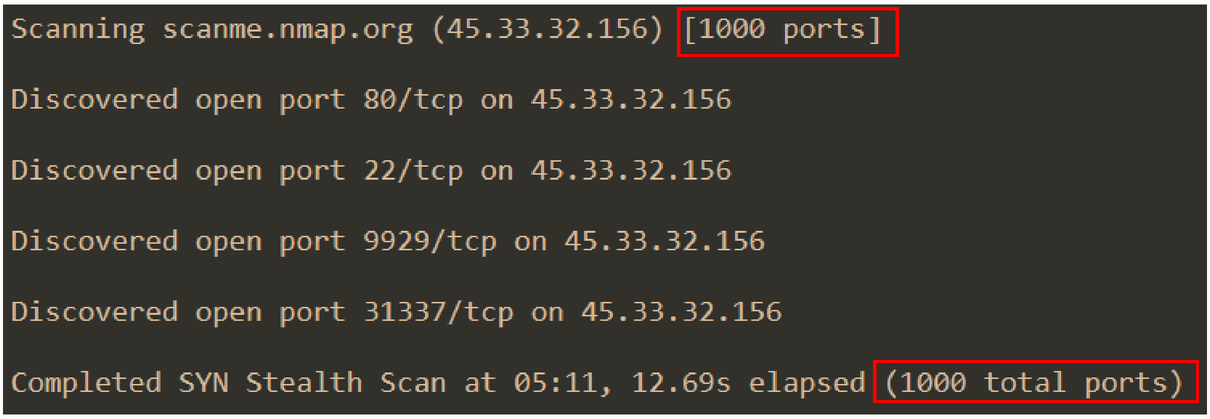


```
10.0.2.2" ttl="1"></hop><hop rtt="1.00" host="scanme.nmap.org" ipaddr="45.33.32.156" ttl="2"></hop></trace></host><runstats><finished timestr="Tue Jun 21
05:12:09 2016" time="1466511129"></finished><hosts down="0" total="1" up="1"></hosts></runstats></nmaprun>
```

Answer: Tue Jun 21 05:12:09 2016

How many ports were scanned?

The number of scanned ports can be found in the same .xml file as the previous question:

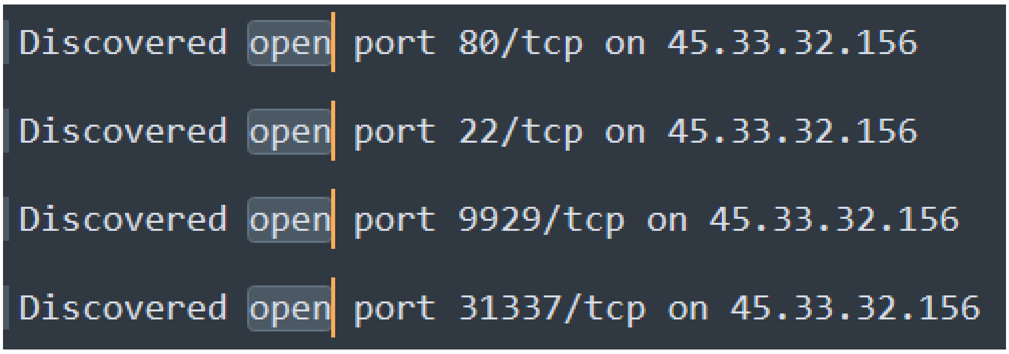


```
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Completed SYN Stealth Scan at 05:11, 12.69s elapsed (1000 total ports)
```

Answer: 1000

What ports were found "open"?(comma-separated, ascending)

Continuing with investigating the nmap .xml file, if you search for the keyword “open” you can find the following open ports:

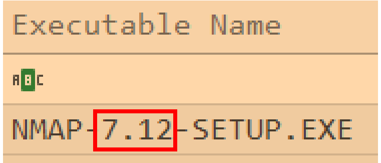


```
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
```

Answer: 22,80,9929,31337

What was the version of the network scanner running on this computer?

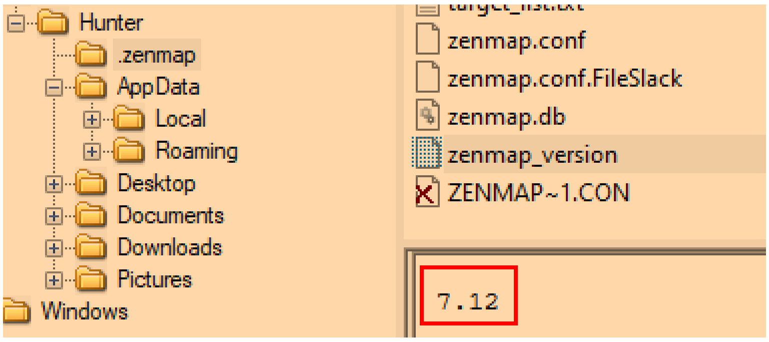
There are two approaches to answering this question, if you investigate the PECmd output (the parsed Prefetch artifacts), you can find the installer for namp:



Executable Name

NMAP-7.12-SETUP.EXE

Installers often include the program version in the filename, like seen above. A more concrete method of determining the version is to navigate to the zenmap folder found in the users home folder. Here we can find a folder called ‘zenmap_version’ that contains the version of zenmap being used:



```
Hunter
  .zenmap
  AppData
    Local
    Roaming
  Desktop
  Documents
  Downloads
  Pictures
Windows
```

```
zenmap.conf
zenmap.conf.FileSlack
zenmap.db
zenmap_version
ZENMAP~1.CON
```

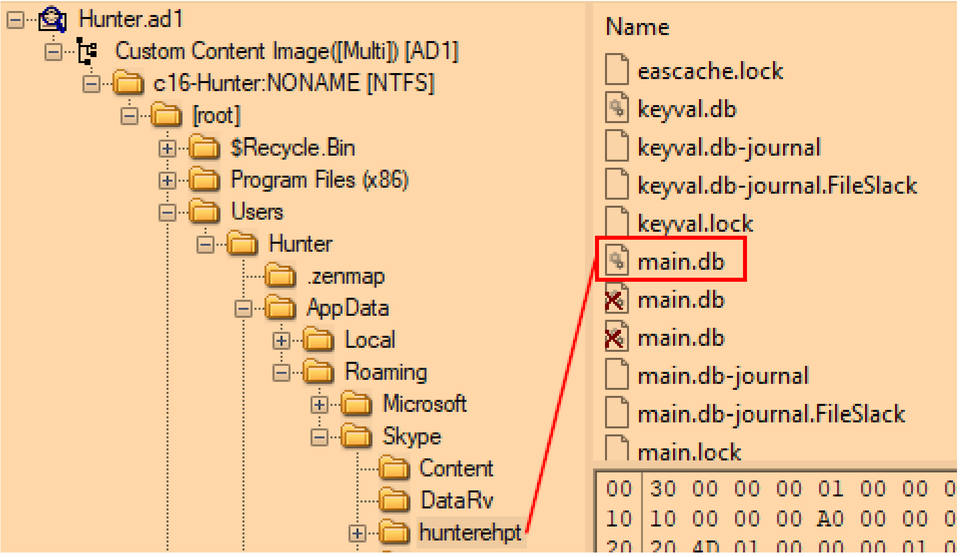
```
7.12
```

Answer: 7.12

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

Skype stores chat history, contacts. and other key information within a database file called main.db. This file is located at:

- `%SystemRoot%\Users\<username>\AppData\Roaming\Skype\<username>`

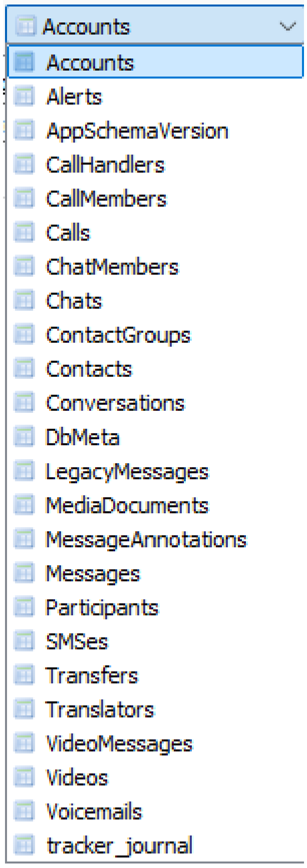


```
Hunter.ad1
  Custom Content Image([Multi]) [AD1]
    c16-Hunter:NONAME [NTFS]
      [root]
        $Recycle.Bin
        Program Files (x86)
        Users
          Hunter
            .zenmap
            AppData
              Local
              Roaming
                Microsoft
                Skype
                  Content
                  DataRv
                  hunterehpt
```

```
Name
eascache.lock
keyval.db
keyval.db-journal
keyval.db-journal.FileSlack
keyval.lock
main.db
main.db
main.db
main.db-journal
main.db-journal.FileSlack
main.lock
```

```
00  30  00  00  00  01  00  00  0
10  10  00  00  00  A0  00  00  0
20  20  4D  01  00  00  00  01  0
```

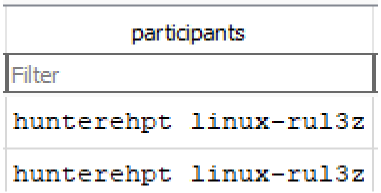
Once you have exported the main.db file, open it using DB Browser for SQLite. Here you will find multiple tables of interest:



Accounts

Accounts
Alerts
AppSchemaVersion
CallHandlers
CallMembers
Calls
ChatMembers
Chats
ContactGroups
Contacts
Conversations
DbMeta
LegacyMessages
MediaDocuments
MessageAnnotations
Messages
Participants
SMSes
Transfers
Translators
VideoMessages
Videos
Voicemails
tracker_journal

If you investigate the Chats table, we can see that Hunter (hunterehpt) has been messaging someone called linux-rul3z:

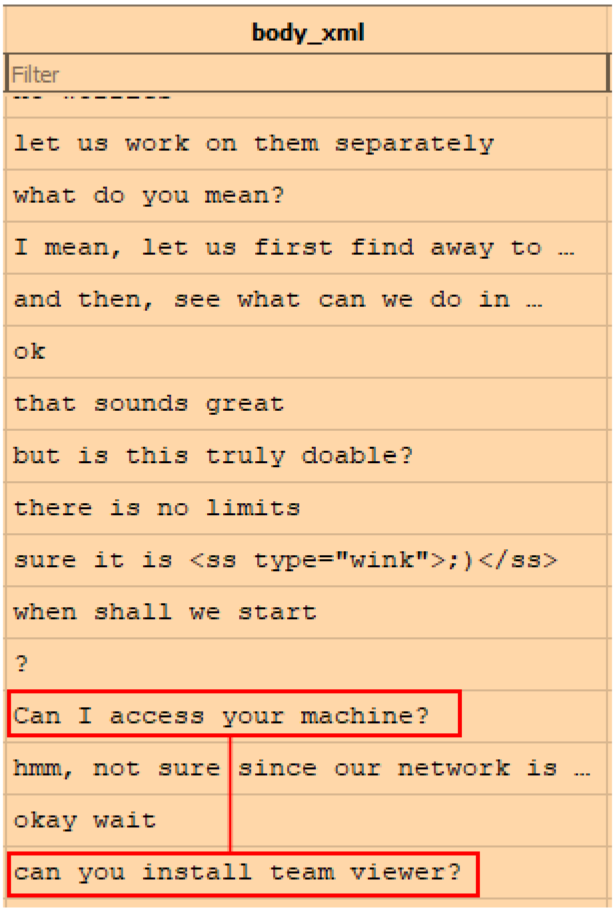


participants
Filter
hunterehpt linux-rul3z
hunterehpt linux-rul3z

Answer: linux-rul3z

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?

You can find the message history stored within the Messages table where the body_xml column stores the actual message body (the content we are interested in). After going through the messages, I came across the following conversation:



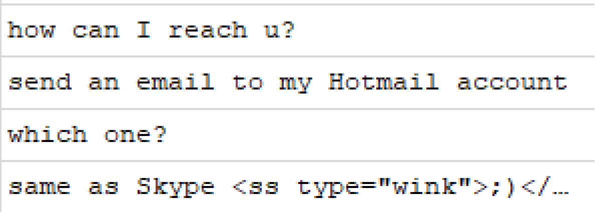
body_xml
Filter
let us work on them separately
what do you mean?
I mean, let us first find away to …
and then, see what can we do in …
ok
that sounds great
but is this truly doable?
there is no limits
sure it is <ss type="wink">;)</ss>
when shall we start
?
Can I access your machine?
hmm, not sure since our network is …
okay wait
can you install team viewer?

TeamViewer is a legitimate RMM (Remote Monitoring and Management) tool that is often used by threat actors for persistence and exfiltration.

Answer: teamviewer

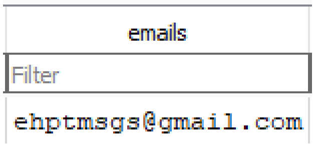
What is the Gmail email address of the suspect employee?

If you continue reading the Skype messages, you will see the following conversation:



how can I reach u?
send an email to my Hotmail account
which one?
same as Skype <ss type="wink">;)</…

This indicates that the employees email address is stored somewhere within the Skype database. There is a table called Accounts, within this table you can find a column called emails that contains the email of the suspect:



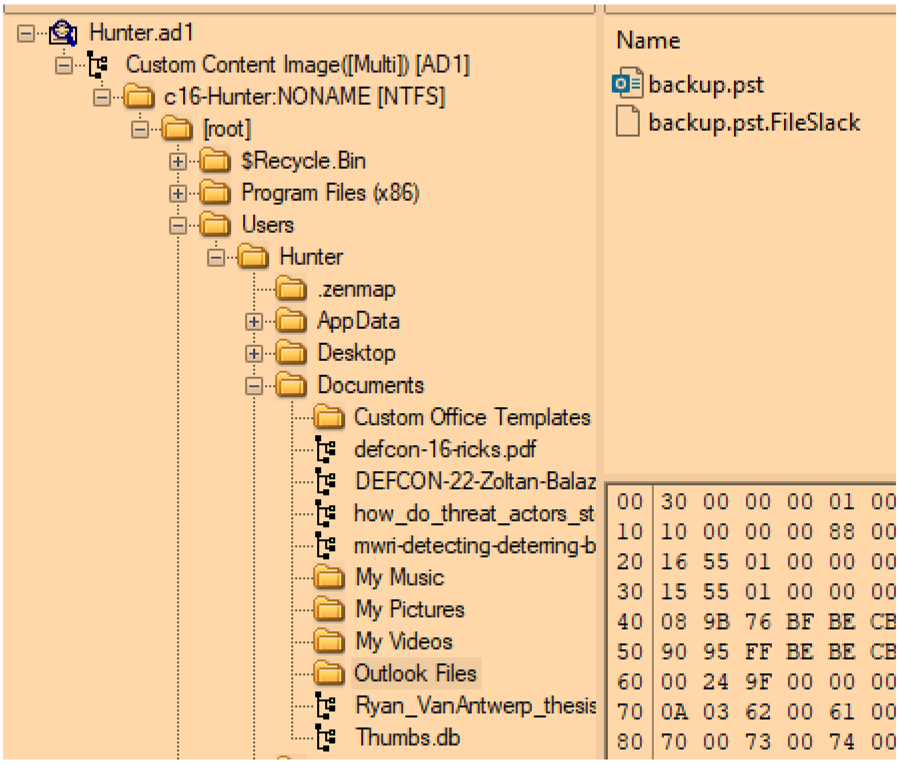
emails
Filter
ehptmsgs@gmail.com

Answer: ehptmsgs@gmail.com

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?

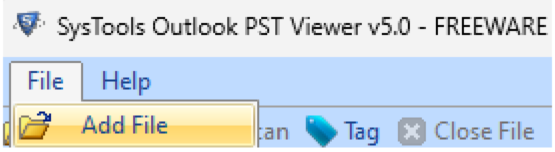
After using the hint, we need to find the user's Outlook PST file. An Outlook PST file is used by Microsoft Outlook to store copies of emails, calendar events, etc, on the user's computer. They are commonly used for archiving or backing up email data. These files are located at:

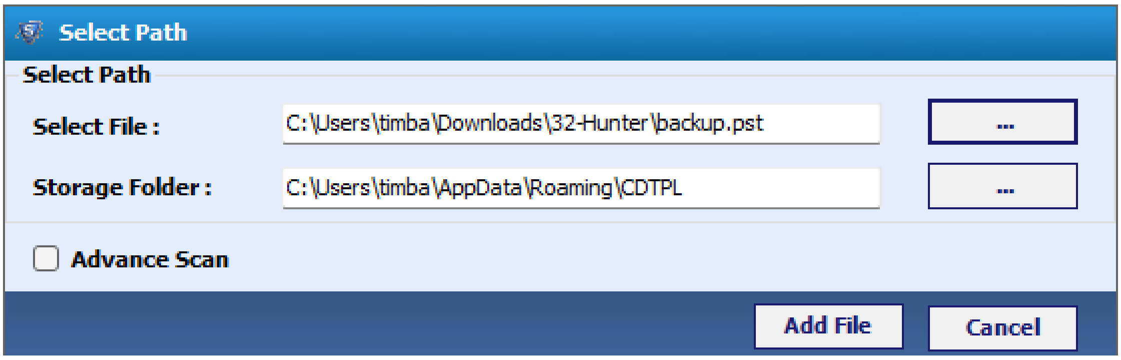
- `%SystemRoot%\Users\<username>\Documents\Outlook Files`



```
00 30 00 00 01 00
10 10 00 00 88 00
20 16 55 01 00 00 00
30 15 55 01 00 00 00
40 08 9B 76 BF BE CB
50 90 95 FF BE BE CB
60 00 24 9F 00 00 00
70 0A 03 62 00 61 00
80 70 00 73 00 74 00
```

After exporting the backup.pst file, we can open it using a tool called SysTools Outlook PST Viewer:





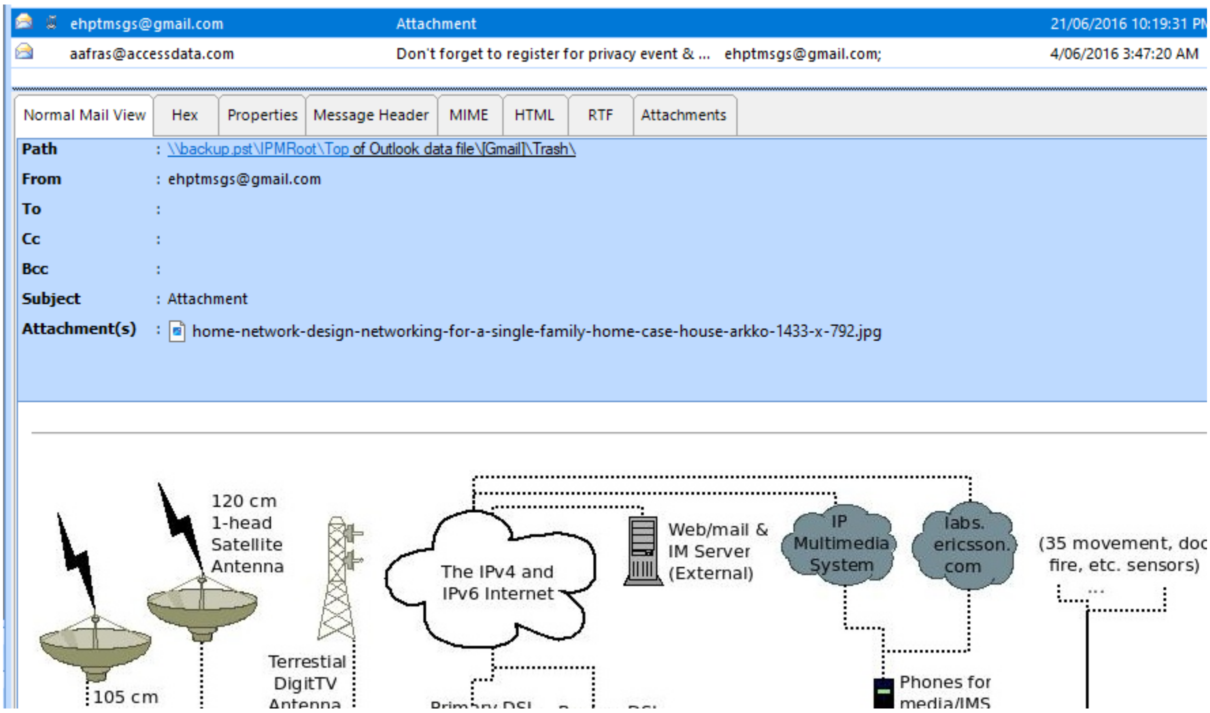
Select Path

Select File : C:\Users\timba\Downloads\32-Hunter\backup.pst

Storage Folder : C:\Users\timba\AppData\Roaming\CDTPL

□ Advance Scan

Within the user's trash folder, we can find an email that contains a network diagram:

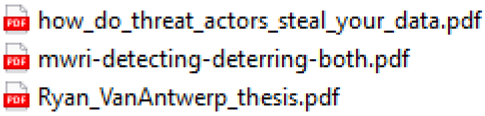

ehptmsgs@gmail.com	Attachment		21/06/2016 10:19:31 PM
aafras@accessdata.com	Don't forget to register for privacy event & ...	ehptmsgs@gmail.com;	4/06/2016 3:47:20 AM

Path : \\backup.pst\IPMRoot\Top of Outlook data file\[Gmail]\Trash\
From : ehptmsgs@gmail.com
To :
Cc :
Bcc :
Subject : Attachment
Attachment(s) : home-network-design-networking-for-a-single-family-home-case-house-arkko-1433-x-792.jpg

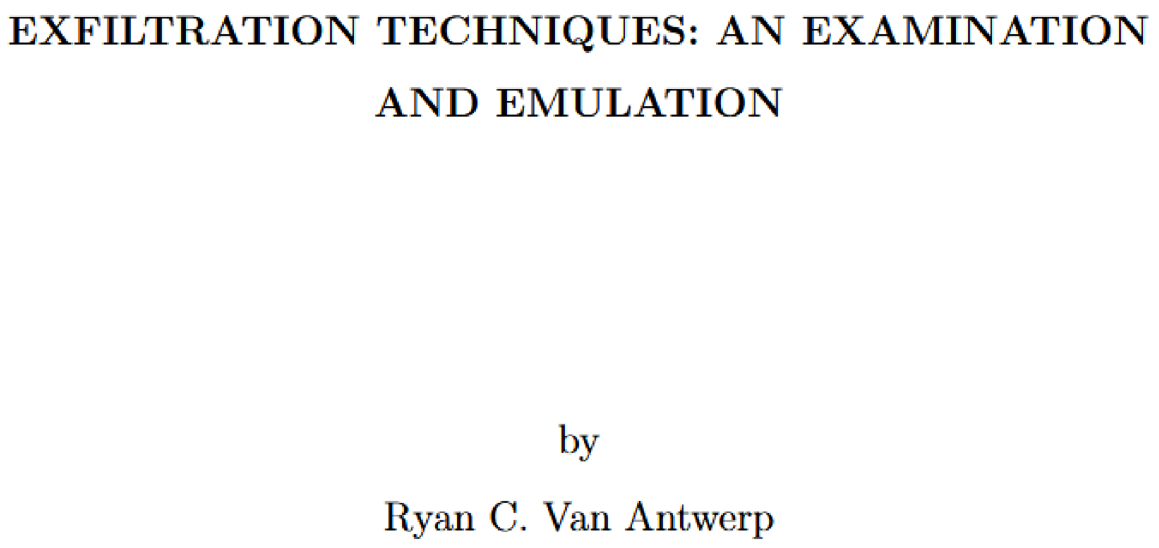
Answer: home-network-design-networking-for-a-single-family-home-case-house-arkko-1433-x-792.jpg

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

After navigating to the user's Documents folder, I found multiple pdf files of interest:


how_do_threat_actors_steal_your_data.pdf
mwri-detecting-deterring-both.pdf
Ryan_VanAntwerp_thesis.pdf

After exporting and viewing each file, I came across the following PDF named Ryan_VanAntwerp_thesis.pdf:



EXFILTRATION TECHNIQUES: AN EXAMINATION AND EMULATION

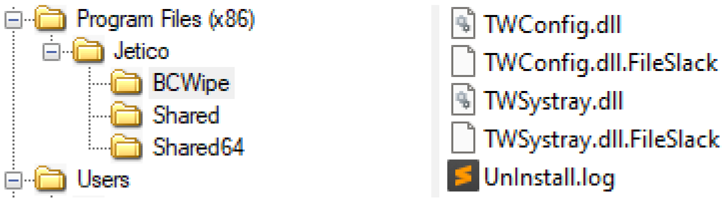
by

Ryan C. Van Antwerp

Answer: Ryan_VanAntwerp_thesis.pdf

What was the name of the Disk Encryption application Installed on the victim system? (two words space separated)

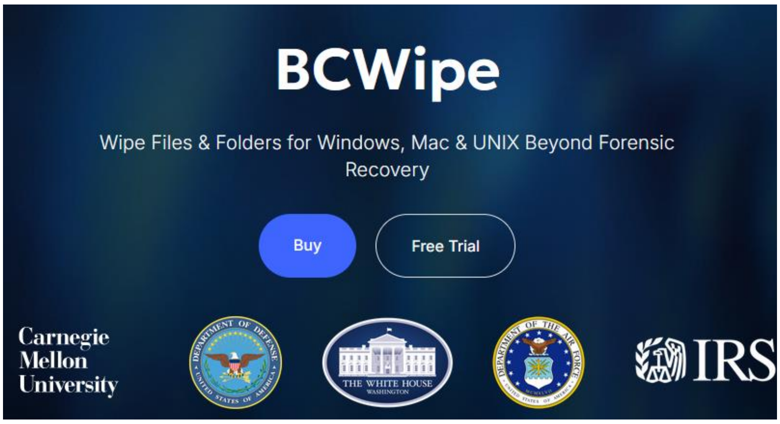
On Windows, the Program Files folder is a system folder that contains installed programs. If we examine the Program Files (x86) folder, we can see an interesting folder for BCWipe:



```
Program Files (x86)
  Jetico
    BCWipe
    Shared
    Shared64
Users
```

```
TWConfig.dll
TWConfig.dll.FileSlack
TWSystray.dll
TWSystray.dll.FileSlack
UnInstall.log
```

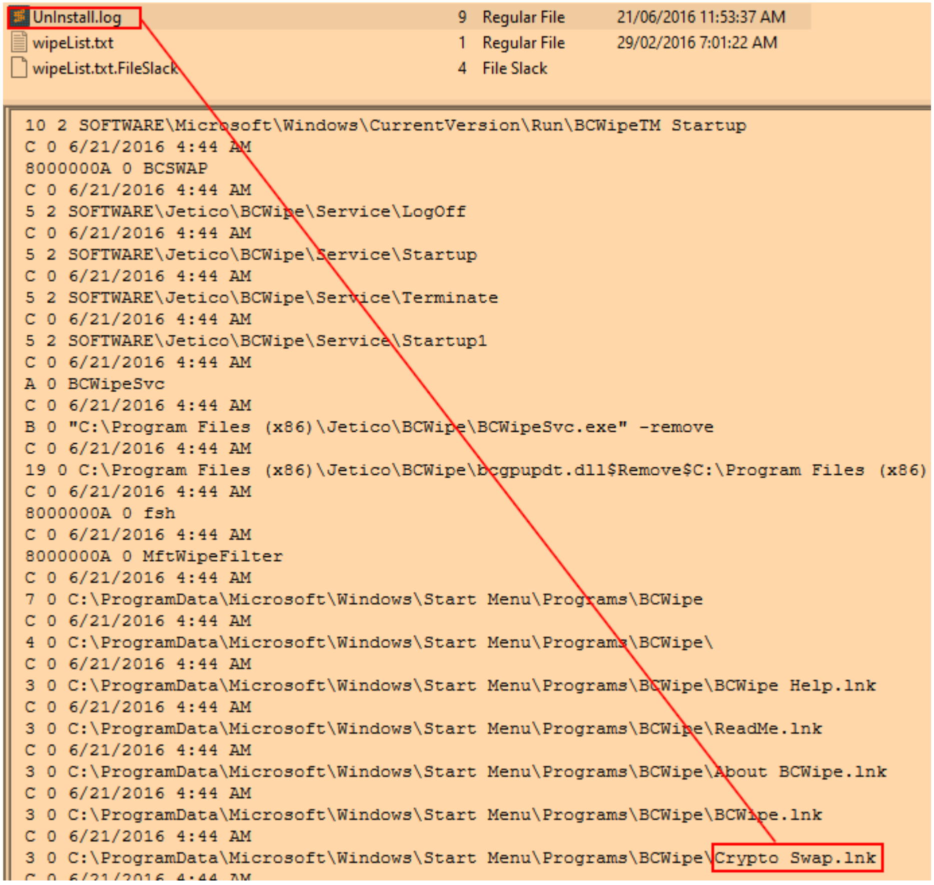
After a quick Google search, you can determine that BCWipe is a tool used to Wipe Files and Folders:



BCWipe

Wipe Files & Folders for Windows, Mac & UNIX Beyond Forensic Recovery

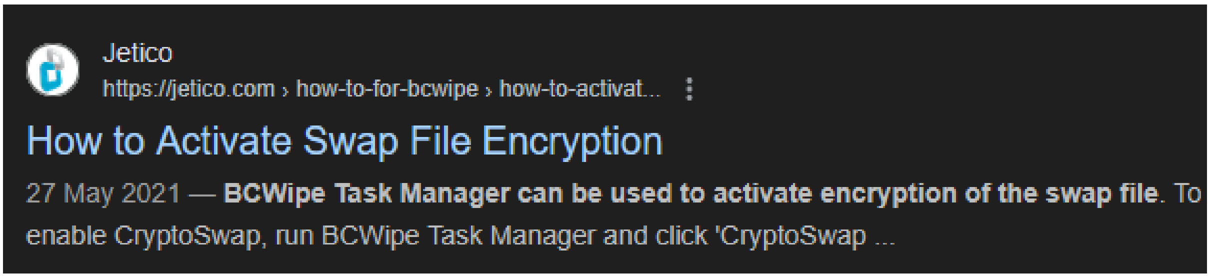
Within the BCWipe folder, you can find a file called UnInstall.log, which as the name suggests, logs uninstallation details.



```
UnInstall.log                9  Regular File  21/06/2016 11:53:37 AM
wipeList.txt                 1  Regular File  29/02/2016 7:01:22 AM
wipeList.txt.FileSlack       4  File Slack
```

```
10 2 SOFTWARE\Microsoft\Windows\CurrentVersion\Run\BCWipeTM Startup
C 0 6/21/2016 4:44 AM
8000000A 0 BCSWAP
C 0 6/21/2016 4:44 AM
5 2 SOFTWARE\Jetico\BCWipe\Service\LogOff
C 0 6/21/2016 4:44 AM
5 2 SOFTWARE\Jetico\BCWipe\Service\Startup
C 0 6/21/2016 4:44 AM
5 2 SOFTWARE\Jetico\BCWipe\Service\Terminate
C 0 6/21/2016 4:44 AM
5 2 SOFTWARE\Jetico\BCWipe\Service\Startup1
C 0 6/21/2016 4:44 AM
A 0 BCWipeSvc
C 0 6/21/2016 4:44 AM
B 0 "C:\Program Files (x86)\Jetico\BCWipe\BCWipeSvc.exe" -remove
C 0 6/21/2016 4:44 AM
19 0 C:\Program Files (x86)\Jetico\BCWipe\bcgpupdt.dll$Remove$C:\Program Files (x86)
C 0 6/21/2016 4:44 AM
8000000A 0 fsh
C 0 6/21/2016 4:44 AM
8000000A 0 MftWipeFilter
C 0 6/21/2016 4:44 AM
7 0 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\BCWipe
C 0 6/21/2016 4:44 AM
4 0 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\BCWipe\
C 0 6/21/2016 4:44 AM
3 0 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\BCWipe\BCWipe Help.lnk
C 0 6/21/2016 4:44 AM
3 0 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\BCWipe\ReadMe.lnk
C 0 6/21/2016 4:44 AM
3 0 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\BCWipe\About BCWipe.lnk
C 0 6/21/2016 4:44 AM
3 0 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\BCWipe\BCWipe.lnk
C 0 6/21/2016 4:44 AM
3 0 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\BCWipe\Crypto Swap.lnk
C 0 6/21/2016 4:44 AM
```

As you can see in the above image, there is a reference to Crypto Swap.lnk. If you search for Crypto Swap in BCWipe, you will come to the conclusion that it is used for file encryption:



Jetico
https://jetico.com › how-to-for-bcwipe › how-to-activat...

How to Activate Swap File Encryption

27 May 2021 — **BCWipe Task Manager can be used to activate encryption of the swap file**. To enable CryptoSwap, run BCWipe Task Manager and click 'CryptoSwap ...

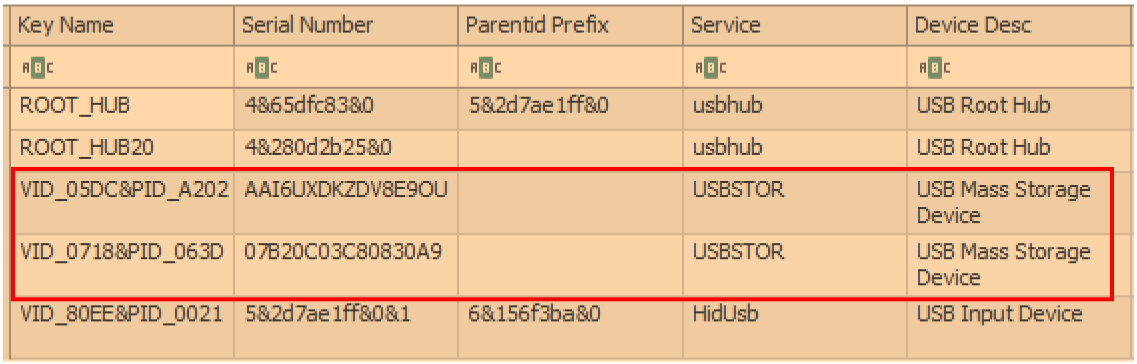
Answer: Crypto Swap

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

The USB registry key found in the SYSTEM hive stores information about connected USB devices. It is located at:

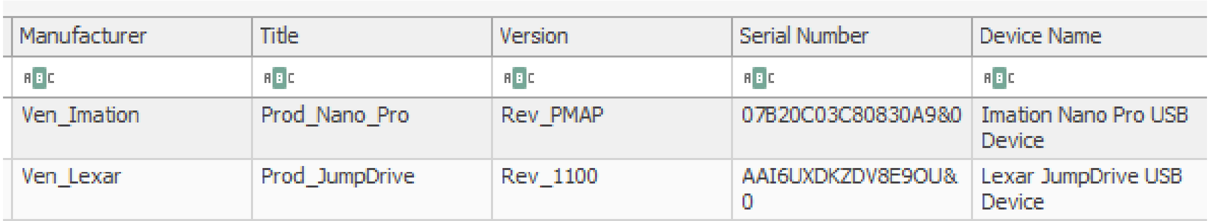
- `SYSTEM\CurrentControlSet\Enum\USB`

Here you can find the serial numbers for both USB storage devices, in the Serial Number column.



Key Name	Serial Number	Parentid Prefix	Service	Device Desc
ABC	ABC	ABC	ABC	ABC
ROOT_HUB	4&65dfc83&0	5&2d7ae1ff&0	usbhub	USB Root Hub
ROOT_HUB20	4&280d2b25&0		usbhub	USB Root Hub
VID_05DC&PID_A202	AAI6UXDKZDV8E9OU		USBSTOR	USB Mass Storage Device
VID_0718&PID_063D	07B20C03C80830A9		USBSTOR	USB Mass Storage Device
VID_80EE&PID_0021	5&2d7ae1ff&0&1	6&156f3ba&0	HidUsb	USB Input Device

You can also find the serial numbers of the two USB storage devices in the USBSTOR key, however, make sure to remove &0 at the end of each serial number. &0 is the instance number, this allows Windows to differentiate between multiple physical instances of the same device, i.e., if you have two identical USB drives with the same serial number, or one plugged into different ports at different times:



Manufacturer	Title	Version	Serial Number	Device Name
ABC	ABC	ABC	ABC	ABC
Ven_Imation	Prod_Nano_Pro	Rev_PMAP	07B20C03C80830A9&0	Imation Nano Pro USB Device
Ven_Lexar	Prod_JumpDrive	Rev_1100	AAI6UXDKZDV8E9OU&0	Lexar JumpDrive USB Device

Answer: 07B20C03C80830A9,AAI6UXDKZDV8E9OU

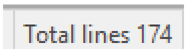
One of the installed applications is a file shredder. What is the name of the application? (two words space separated)

Recall in question 19 how we had to identify the disk encryption application, we also identified that BCWipe is a file shredding application created by Jetico.

Answer: Jetico BCWipe

How many prefetch files were discovered on the system?

Recall how in question 9 we parsed the Prefetch directory to find the network scanning tool used by the suspect. If you navigate back to the Prefetch output in timeline explorer, we can see that there are 174 total lines:



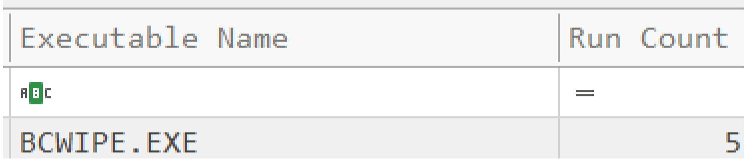
Total lines 174

This means that there was 174 Prefetch files.

Answer: 174

How many times was the file shredder application executed?

The Prefetch stores how many times an application was executed. If you filter for bcwipe in the Executable Name column, we can see that it was executed 5 times:

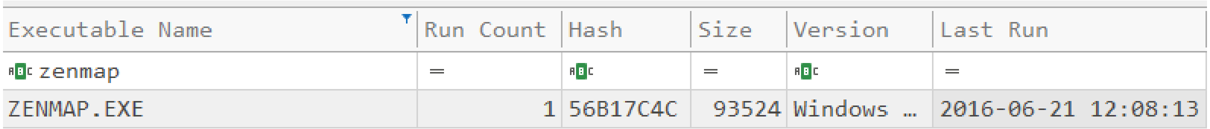


Executable Name	Run Count
ABC	=
BCWIPE.EXE	5

Answer: 5

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

Similarly to the previous question, if you filter for zenmap in the Prefetch output, we can find its Last Run timestamp:

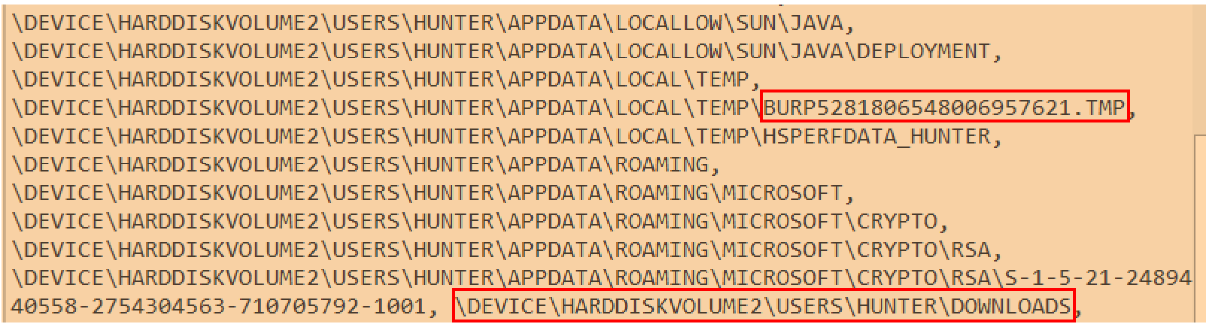


Executable Name	Run Count	Hash	Size	Version	Last Run
ABC zenmap	=	ABC	=	ABC	=
ZENMAP.EXE	1	56B17C4C	93524	Windows …	2016-06-21 12:08:13

Answer: 06/21/2016 12:08:13 PM

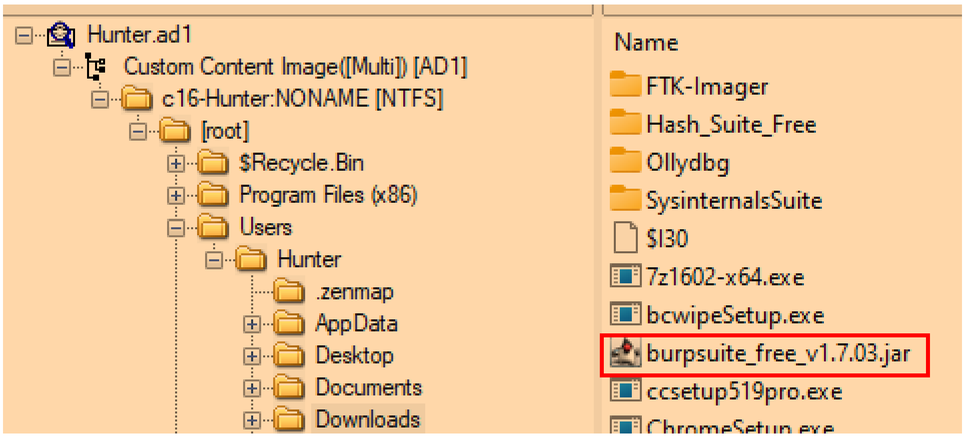
A JAR file for an offensive traffic manipulation tool was executed. What is the absolute path of the file?

A JAR (Java ARchive) file is a package file format used to aggregate Java class files and associated metadata and resources. If you search for java in the Prefetch, we can see what directories javaw.exe interacted with:



```
\DEVICE\HARDDISKVOLUME2\USERS\HUNTER\APPDATA\LOCALLOW\SUN\JAVA,
\DEVICE\HARDDISKVOLUME2\USERS\HUNTER\APPDATA\LOCALLOW\SUN\JAVA\DEPLOYMENT,
\DEVICE\HARDDISKVOLUME2\USERS\HUNTER\APPDATA\LOCAL\TEMP,
\DEVICE\HARDDISKVOLUME2\USERS\HUNTER\APPDATA\LOCAL\TEMP\BURP5281806548006957621.TMP,
\DEVICE\HARDDISKVOLUME2\USERS\HUNTER\APPDATA\LOCAL\TEMP\HSPERFDATA_HUNTER,
\DEVICE\HARDDISKVOLUME2\USERS\HUNTER\APPDATA\ROAMING,
\DEVICE\HARDDISKVOLUME2\USERS\HUNTER\APPDATA\ROAMING\MICROSOFT,
\DEVICE\HARDDISKVOLUME2\USERS\HUNTER\APPDATA\ROAMING\MICROSOFT\CRYPTO,
\DEVICE\HARDDISKVOLUME2\USERS\HUNTER\APPDATA\ROAMING\MICROSOFT\CRYPTO\RSA,
\DEVICE\HARDDISKVOLUME2\USERS\HUNTER\APPDATA\ROAMING\MICROSOFT\CRYPTO\RSA\S-1-5-21-24894
40558-2754304563-710705792-1001, \DEVICE\HARDDISKVOLUME2\USERS\HUNTER\DOWNLOADS,
```

We can see a refence to the Downloads directory, so let’s check it out:



```
Hunter.ad1
  Custom Content Image([Multi]) [AD1]
    c16-Hunter:NONAME [NTFS]
      [root]
        $Recycle.Bin
        Program Files (x86)
        Users
          Hunter
            .zenmap
            AppData
            Desktop
            Documents
            Downloads
```

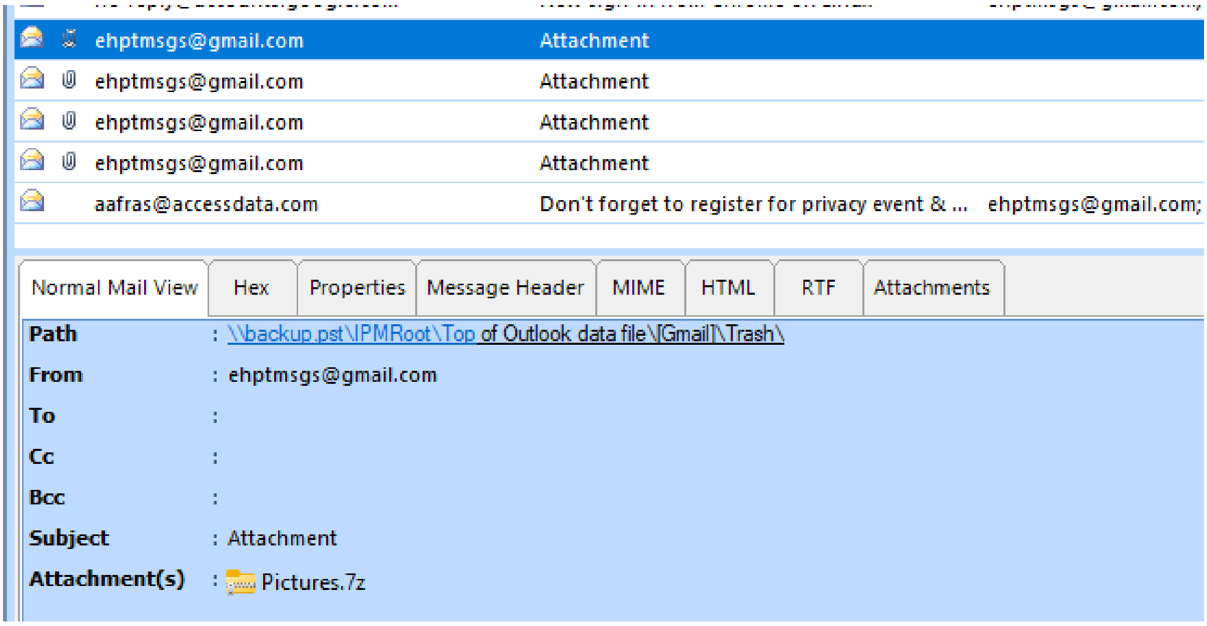
Name
FTK-Imager
Hash_Suite_Free
Ollydbg
SysinternalsSuite
$I30
7z1602-x64.exe
bcwipeSetup.exe
burpsuite_free_v1.7.03.jar
ccsetup519pro.exe
ChromeSetup.exe

As you can see, there is a .jar file for Burp Suite. Burp Suite is a proxy used for application security testing.

Answer: C:\Users\Hunter\Downloads\Burpsuite_free_v1.7.03.jar

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

Going back to SysTools Outlook PST Viewer, you can find an attachment called Pictures.7z in the trash folder:



ehptmsgs@gmail.com	Attachment	
ehptmsgs@gmail.com	Attachment	
ehptmsgs@gmail.com	Attachment	
ehptmsgs@gmail.com	Attachment	
aafras@accessdata.com	Don't forget to register for privacy event & ...	ehptmsgs@gmail.com;

Path : \\backup.pst\IPMRoot\Top of Outlook data file\[Gmail]\Trash\
From : ehptmsgs@gmail.com
To :
Cc :
Bcc :
Subject : Attachment
Attachment(s) : Pictures.7z

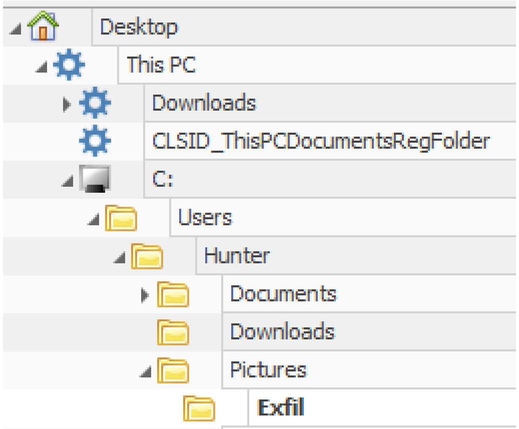
Answer: Pictures.7z

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

Shellbags are a set of registry keys that enables analysts to determine the browsing history of a suspect (through file explorer). If you dump the NTUSER.dat and UserClass.dat hives, we can use ShellBags Explorer to browse the folder structure:

- `%SystemRoot%/Users/<username>/AppData/Local/Microsoft/WindowsUsrClass.dat`

For some reason, the NTUSER.dat file is not found within the Hunter folder, so we can only work with the UsserClass.dat file. If you expand "This PC" and look at the folders Hunter has accessed, we can find an interesting folder within Pictures called Exfil:

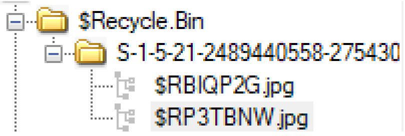


```
Desktop
  This PC
    Downloads
    CLSID_ThisPCDocumentsRegFolder
    C:
      Users
        Hunter
          Documents
          Downloads
          Pictures
            Exfil
```

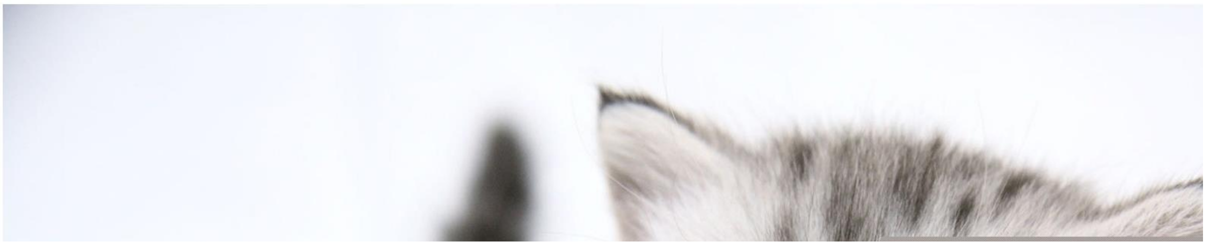
Answer: C:\Users\Hunter\Pictures\Exfil

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?

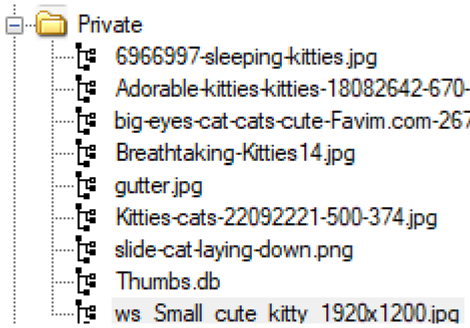
If you look at the $Recycle-Bin folder using FTK Imager, we can find the image in question:



```
$Recycle.Bin
  S-1-5-21-2489440558-275430
    $RBIQP2G.jpg
    $RP3TBNW.jpg
```



If you navigate to the Private folder within Hunter's Pictures folder, you can find the original image:



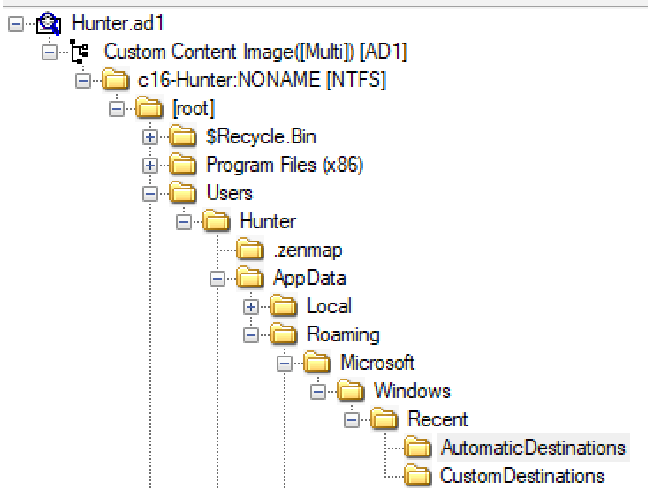
```
Private
    6966997-sleeping-kitties.jpg
    Adorable-kitties-kitties-18082642-670-503.jpg
    big-eyes-cat-cats-cute-Favim.com-2674726.jpg
    Breathtaking-Kitties14.jpg
    gutter.jpg
    Kitties-cats-22092221-500-374.jpg
    slide-cat-laying-down.png
    Thumbs.db
    ws_Small_cute_kitty_1920x1200.jpg
```

Answer: ws_small_cute_kitty_1920x1200.jpg

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

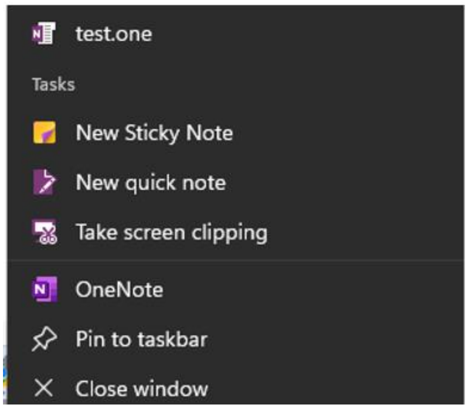
Jump lists are located at:

- `%SystemRoot%\Users\<username>\Roaming\Microsoft\Windows\Recent\AutomaticDestinations`



```
Hunter.ad1
    Custom Content Image([Multi]) [AD1]
        c16-Hunter:NONAME [NTFS]
            [root]
                $Recycle.Bin
                Program Files (x86)
                Users
                    Hunter
                        .zenmap
                        AppData
                            Local
                            Roaming
                                Microsoft
                                    Windows
                                        Recent
                                            AutomaticDestinations
                                            CustomDestinations
```

Jump lists provides users quick access to recently used files, tasks, or applications. For example, after right-clicking OneNote in the taskbar, I was presented with the following:

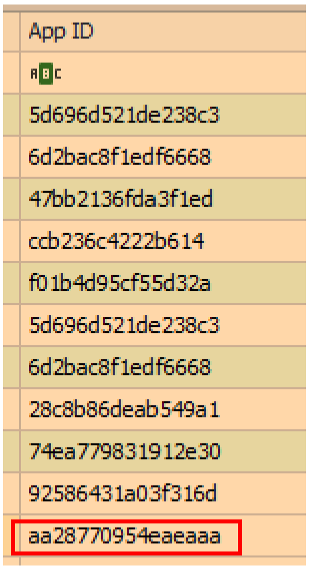


This shows the most recently accessed items for that program. Jump lists are valuable for forensic analysts because it offers insights into recently used files.

Answer: AutomaticDestinations

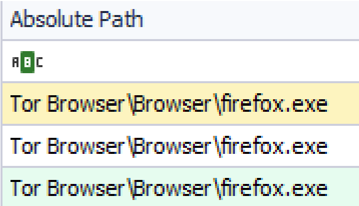
Using JUMP LIST analysis, provide the full path of the application with the AppID of "aa28770954eaeaaa" used to bypass network security monitoring controls.

First you need to dump the AutomaticDestinations and CustomDestinations folders. AutomaticDestinations files are created automatically when a user opens a file or application, while CustomDestinations are created when a user pins an item to the Taskbar or Start Menu. We can then use a tool called JumpListExplorer to parse the contents of both directories, and then look for the AppID in question:



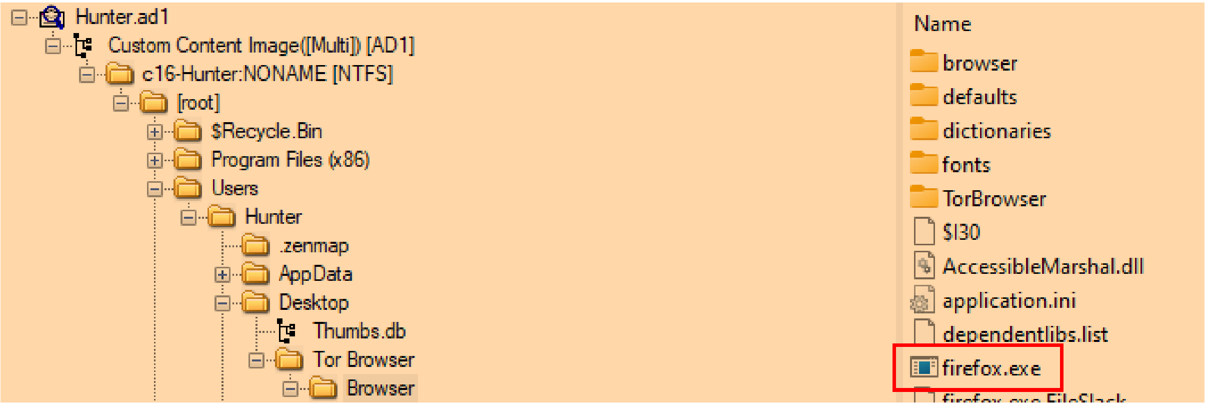
App ID
ABC
5d696d521de238c3
6d2bac8f1edf6668
47bb2136fda3f1ed
ccb236c4222b614
f01b4d95cf55d32a
5d696d521de238c3
6d2bac8f1edf6668
28c8b86deab549a1
74ea779831912e30
92586431a03f316d
aa28770954eaeaaa

If you click on this AppID, we can find the absolute path of this application:



Absolute Path
ABC
Tor Browser\Browser\firefox.exe
Tor Browser\Browser\firefox.exe
Tor Browser\Browser\firefox.exe

We can then use FTK Imager to find its full path:



```
Hunter.ad1
  Custom Content Image([Multi]) [AD1]
    c16-Hunter:NONAME [NTFS]
      [root]
        $Recycle.Bin
        Program Files (x86)
        Users
          Hunter
            .zenmap
            AppData
            Desktop
              Thumbs.db
              Tor Browser
                Browser
```

```
Name
browser
defaults
dictionaries
fonts
TorBrowser
$I30
AccessibleMarshal.dll
application.ini
dependentlibs.list
firefox.exe
firefox.exe.FileSlack
```

Answer: C:\Users\Hunter\Desktop\Tor Browser\Browser\firefox.exe