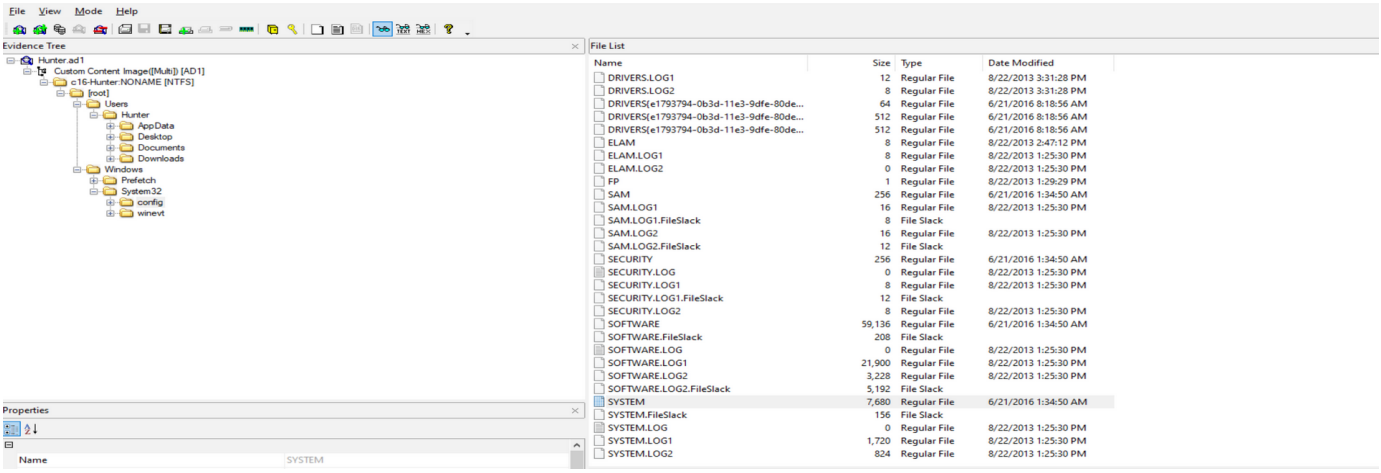
# CTF Hunter

### 1-What is the computer name of the suspect machine?

1-من خلال المسار نحمل ملف System

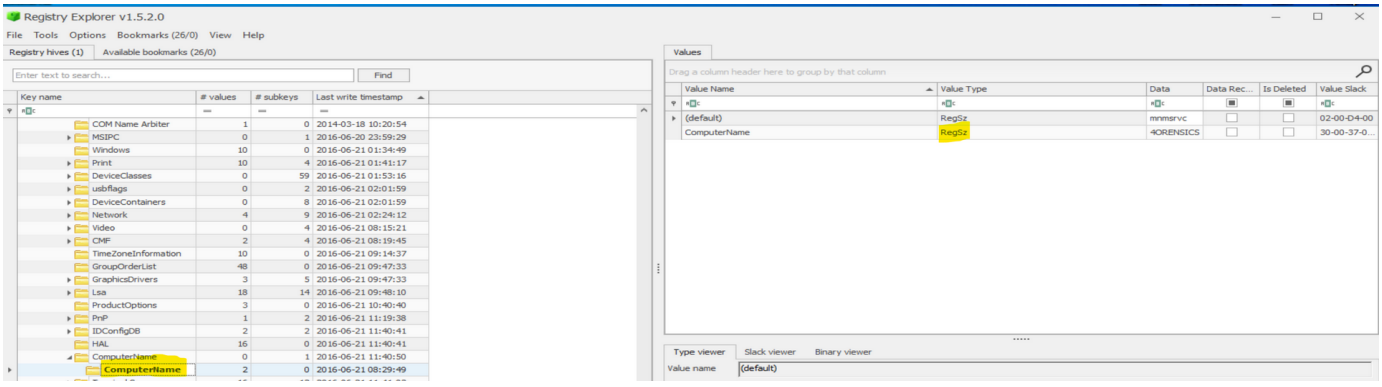
```
`%Windir%\System32\Config`
```




بعد كذا نفتح Registry Explorer

ونبحث عن اسم الكمبيوتر من خلال هذا المسار !

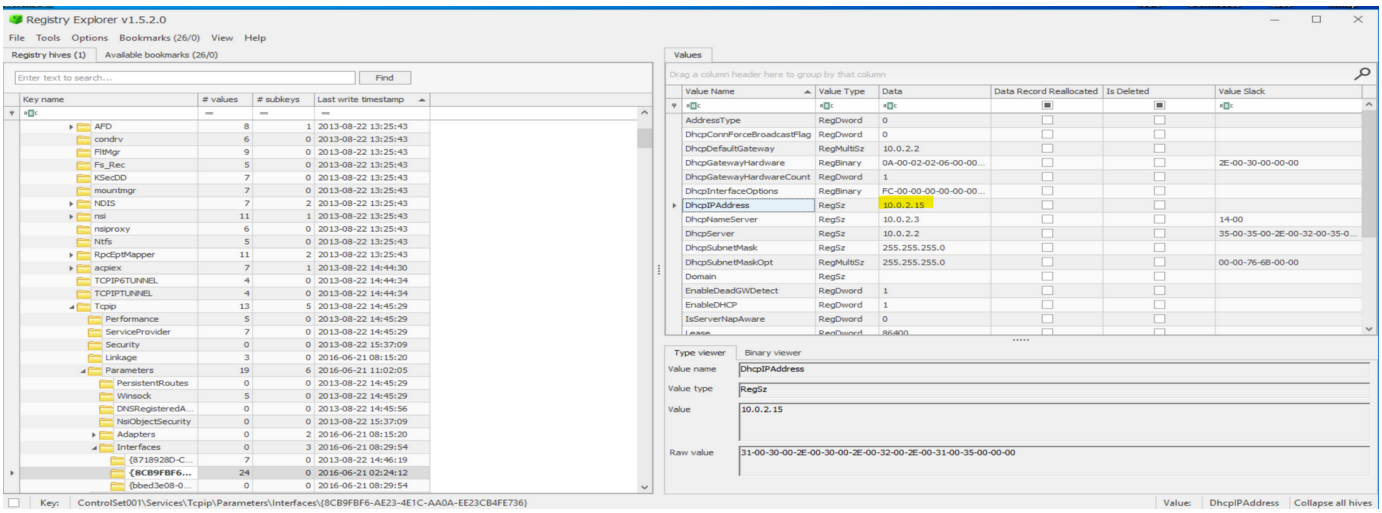
```
\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName
```




### 2-What is the computer IP?

ملف الـSystem ومن ثم Registry Explorer خلال هذا المسار

```
\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\
```

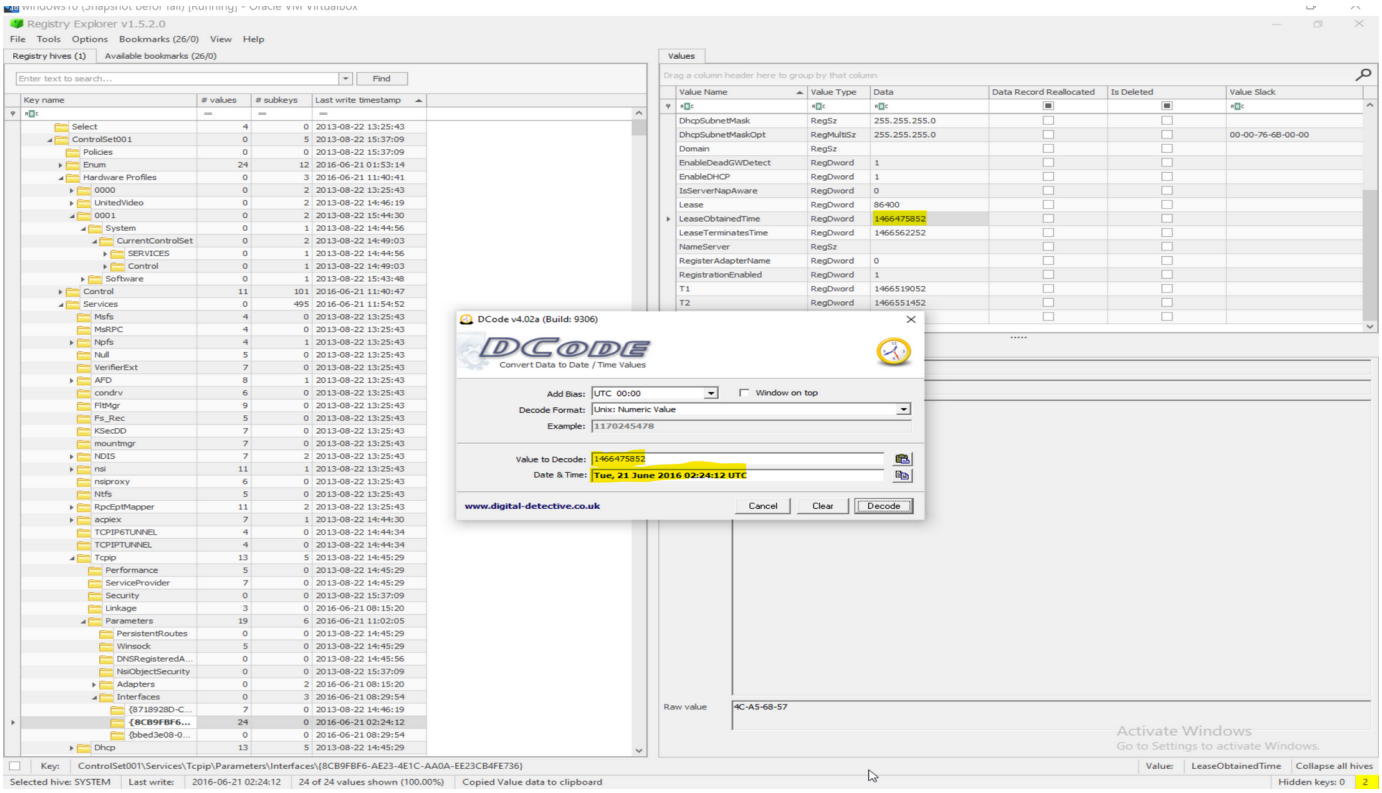



## 3-What was the DHCP LeaseObtainedTime?

ملف الـSystem ومن ثم Registry Explorer خلال هذا المسار

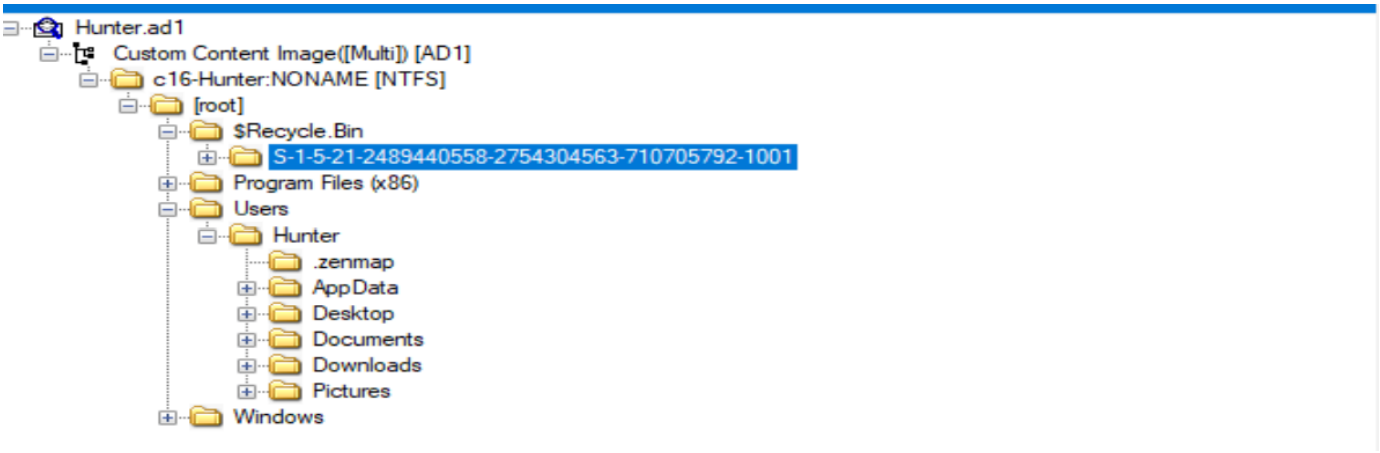
```
\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\
```

وما ننسى نحول التاريخ باستخدام Dcoder

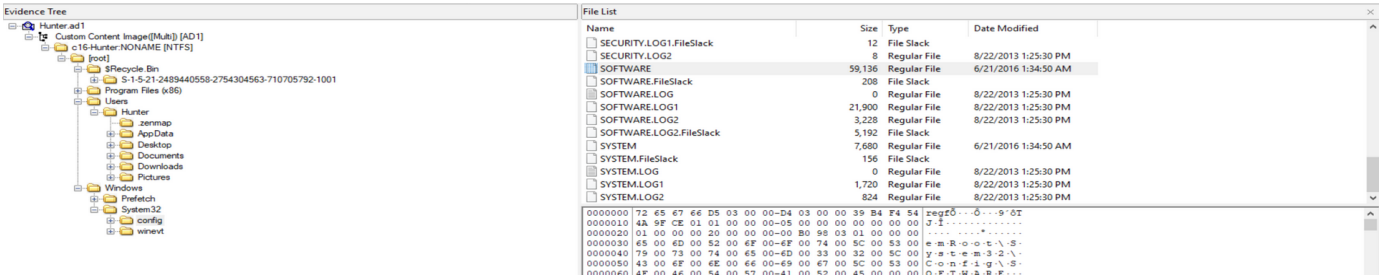



## 4-What is the computer SID?

**من FTK**

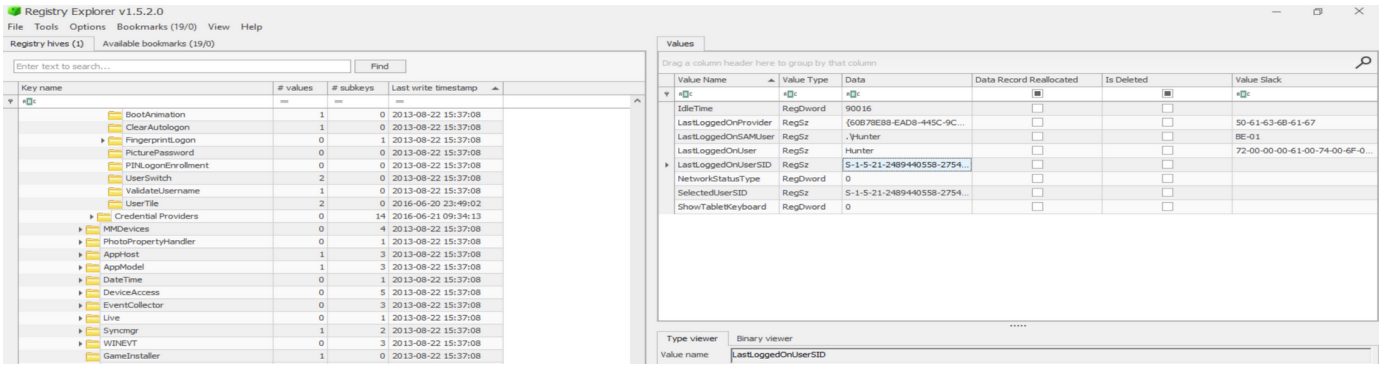



أو من تحميل ملف Software

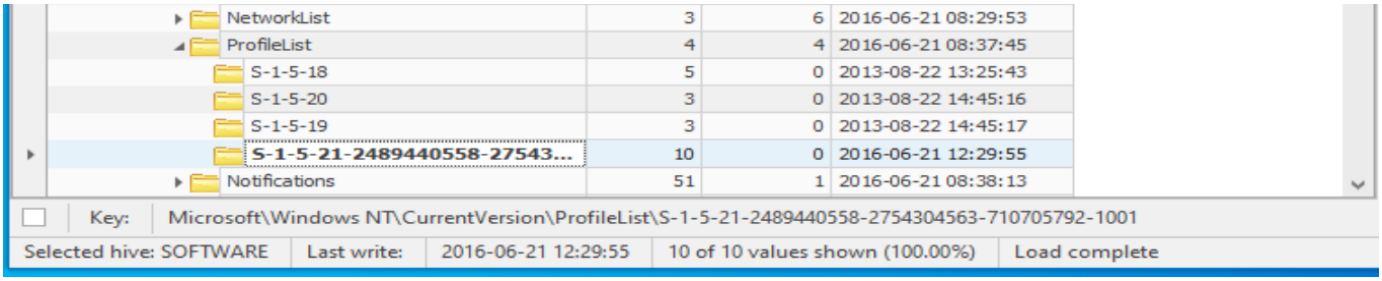


ومن ثم Registry Explorer خلال هذا المسار

\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\LastLoggedOnUser



أو من




---

**5-What is the Operating System(OS) version?**

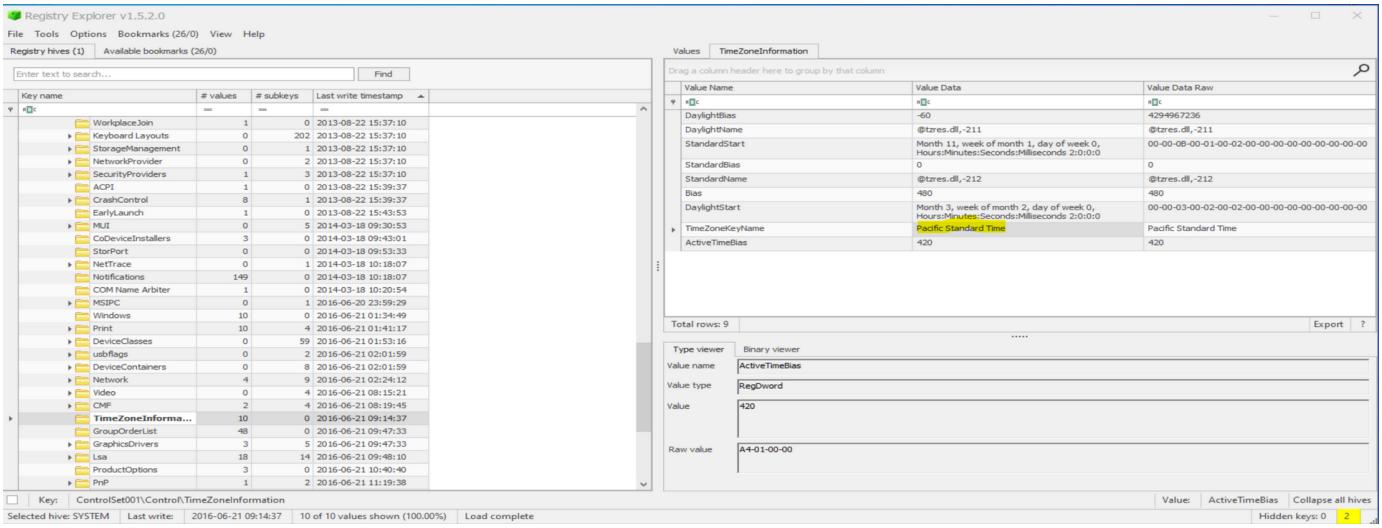
من ملف Software ومن ثم Registry Explorer خلال هذا المسار

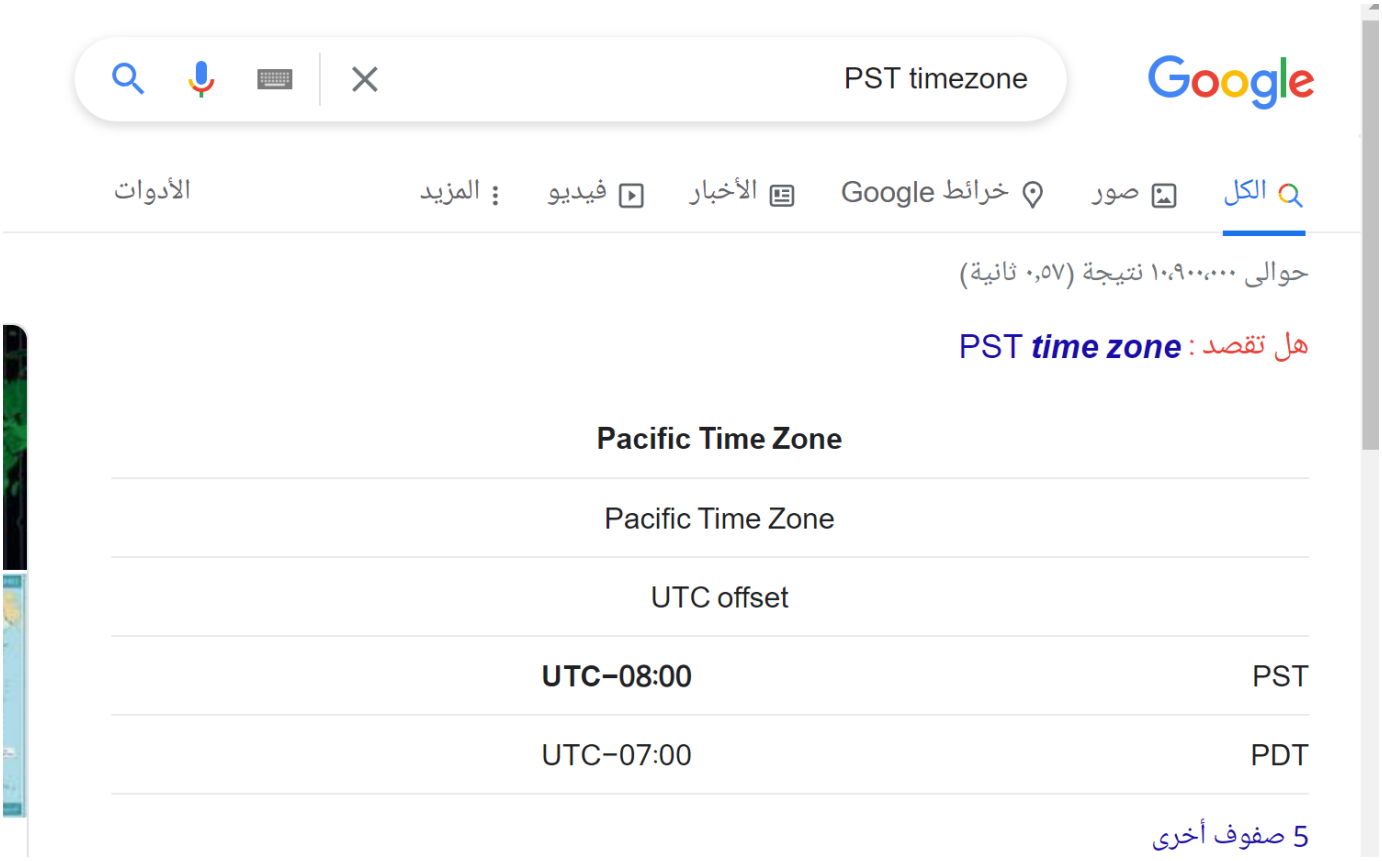
\SOFTWARE\Microsoft\Windows NT\CurrentVersion

**6-What was the computer timezone?**

من ملف الـSystem ومن ثم Registry Explorer خلال هذا المسار

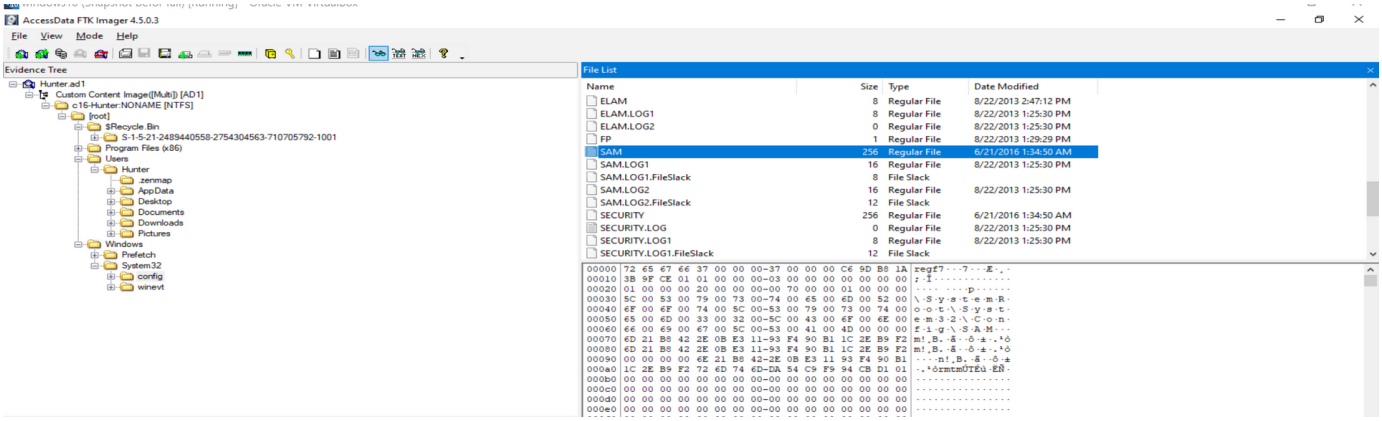
\System\CurrentControlSet\Control\TimeZoneInformation



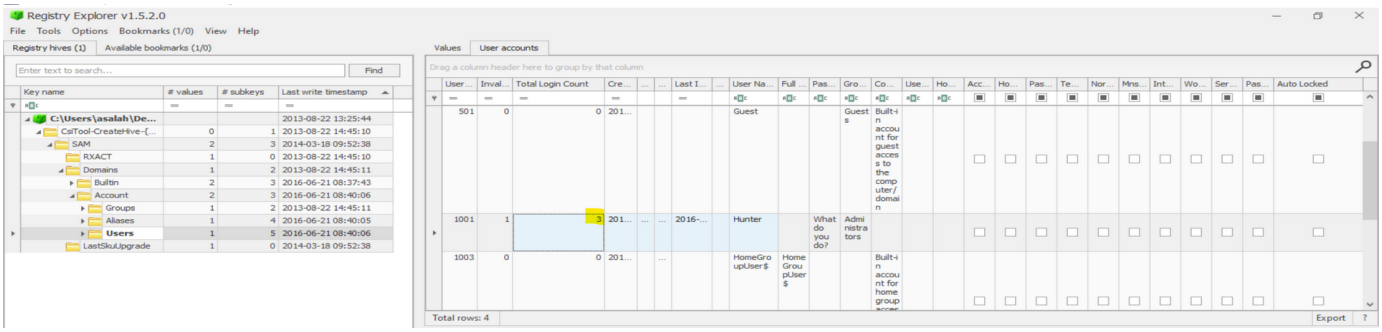

**7-How many times did this user log on to the computer?**

من خلال تحميل ملف SAM

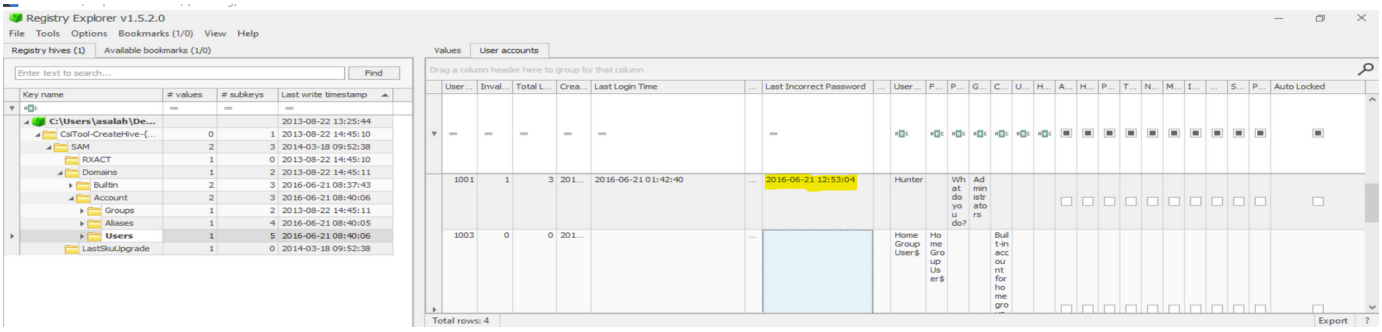



ومن ثم Registry Explorer خلال هذا المسار

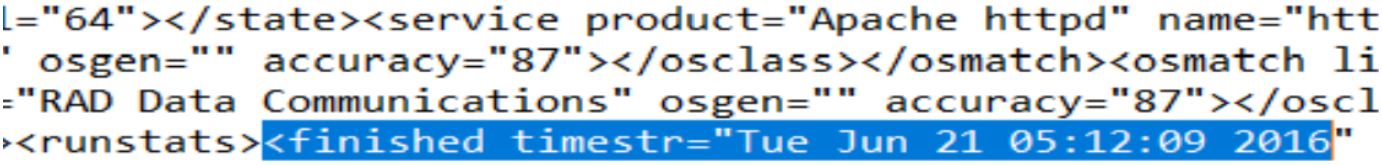
\SAM\Domains\Account



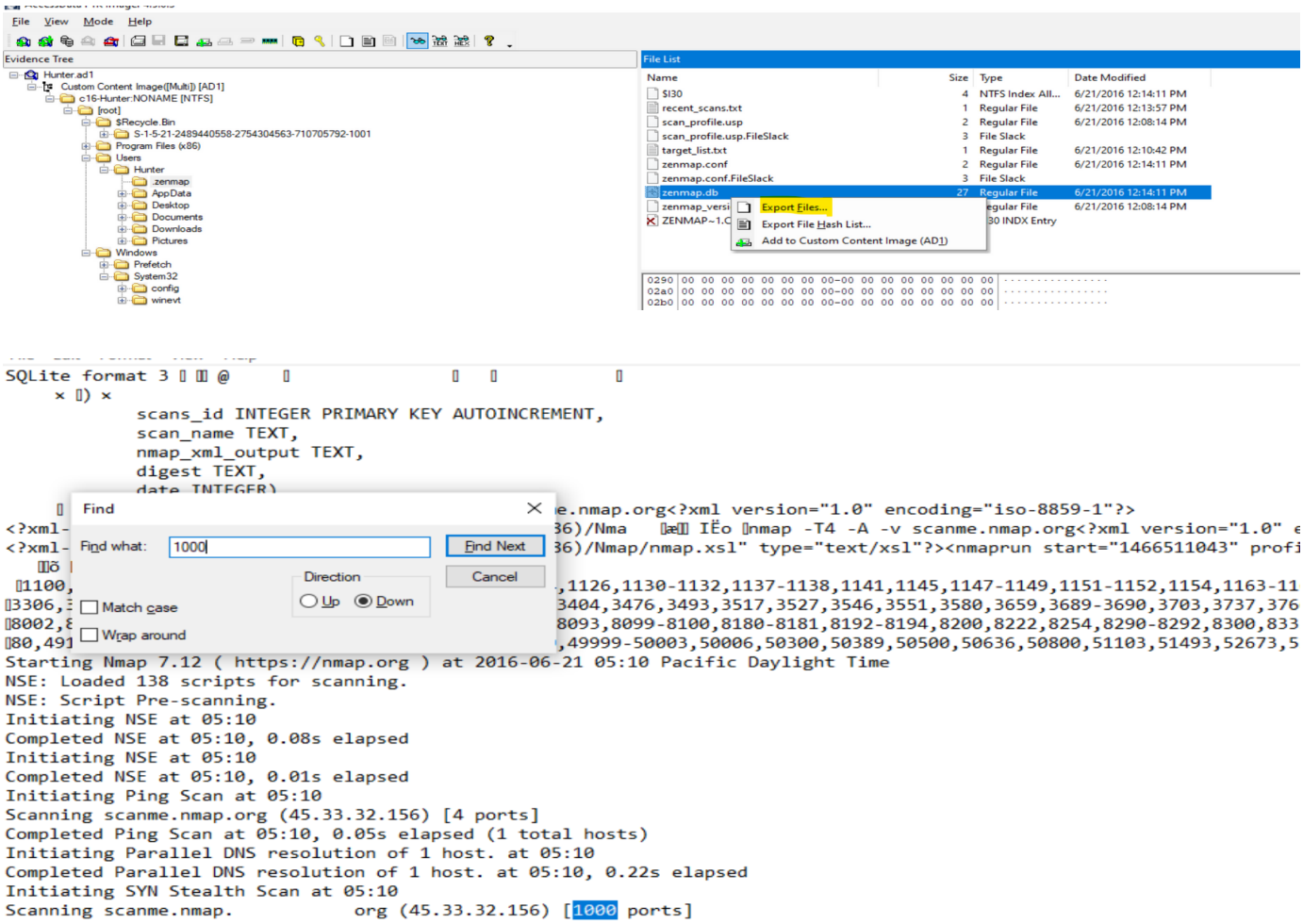

**8-When was the last login time for the discovered account? Format: one-space between date and time?**



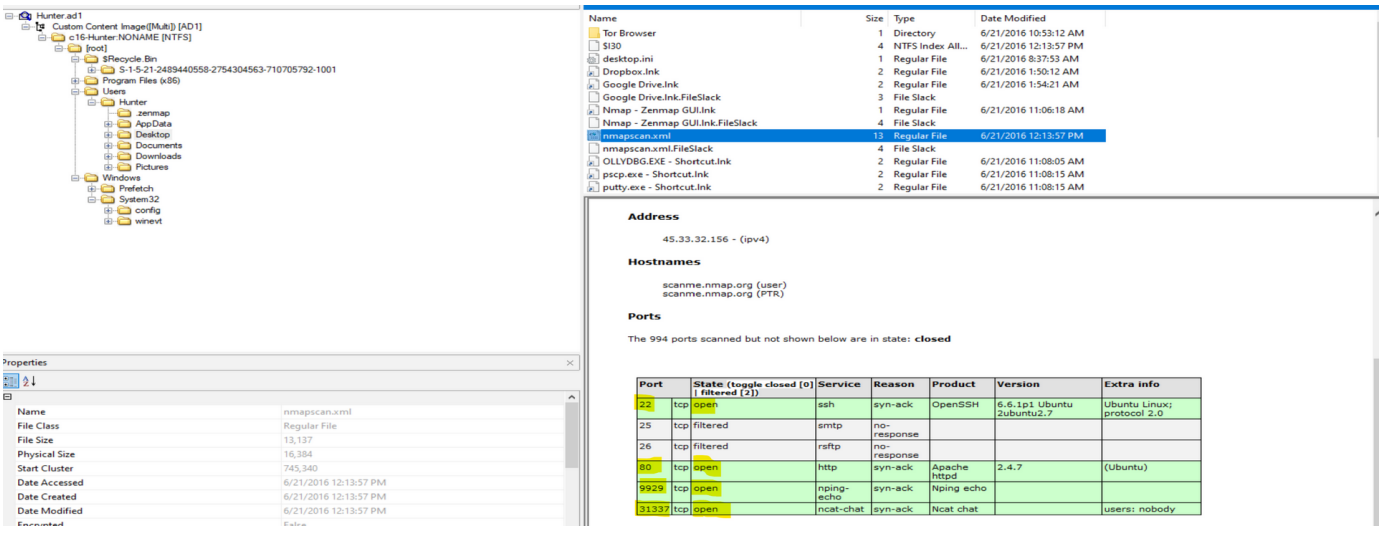

**9-There was a “Network Scanner” running on this computer, what was it? And when was the last time the suspect used it? Format: program.exe,YYYY-MM-DD HH:MM:SS UTC?**



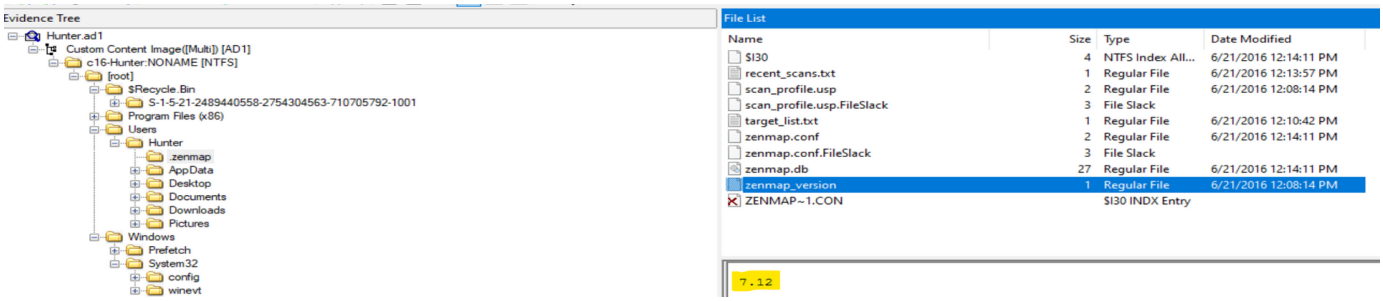
## 11-How many ports were scanned?



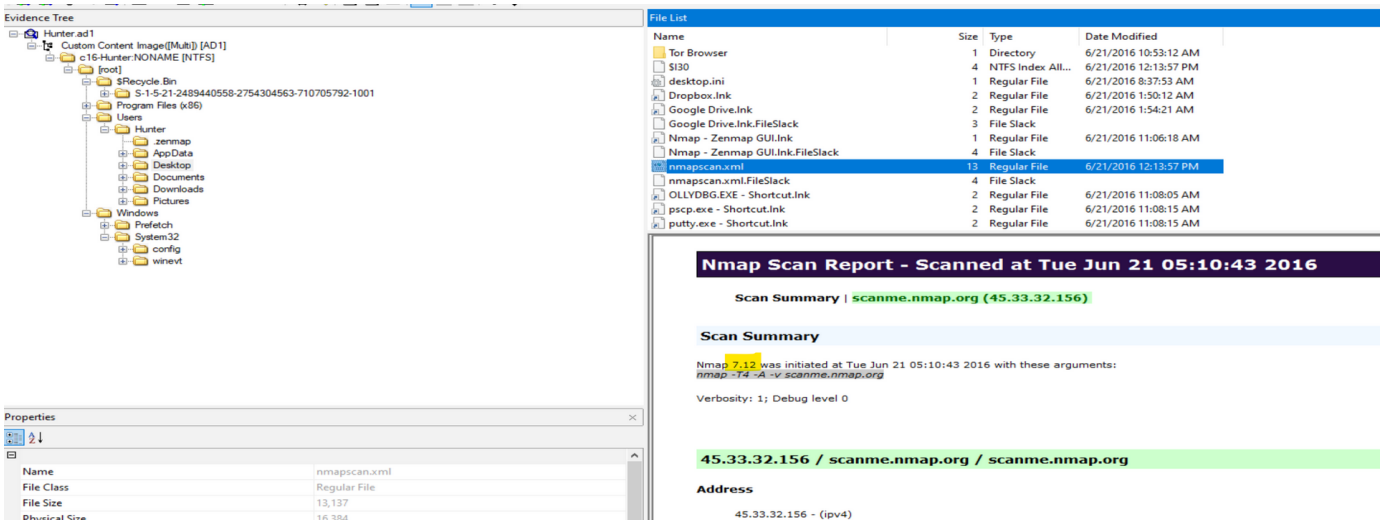

## 12-What ports were found "open"?(comma-separated, ascending)?



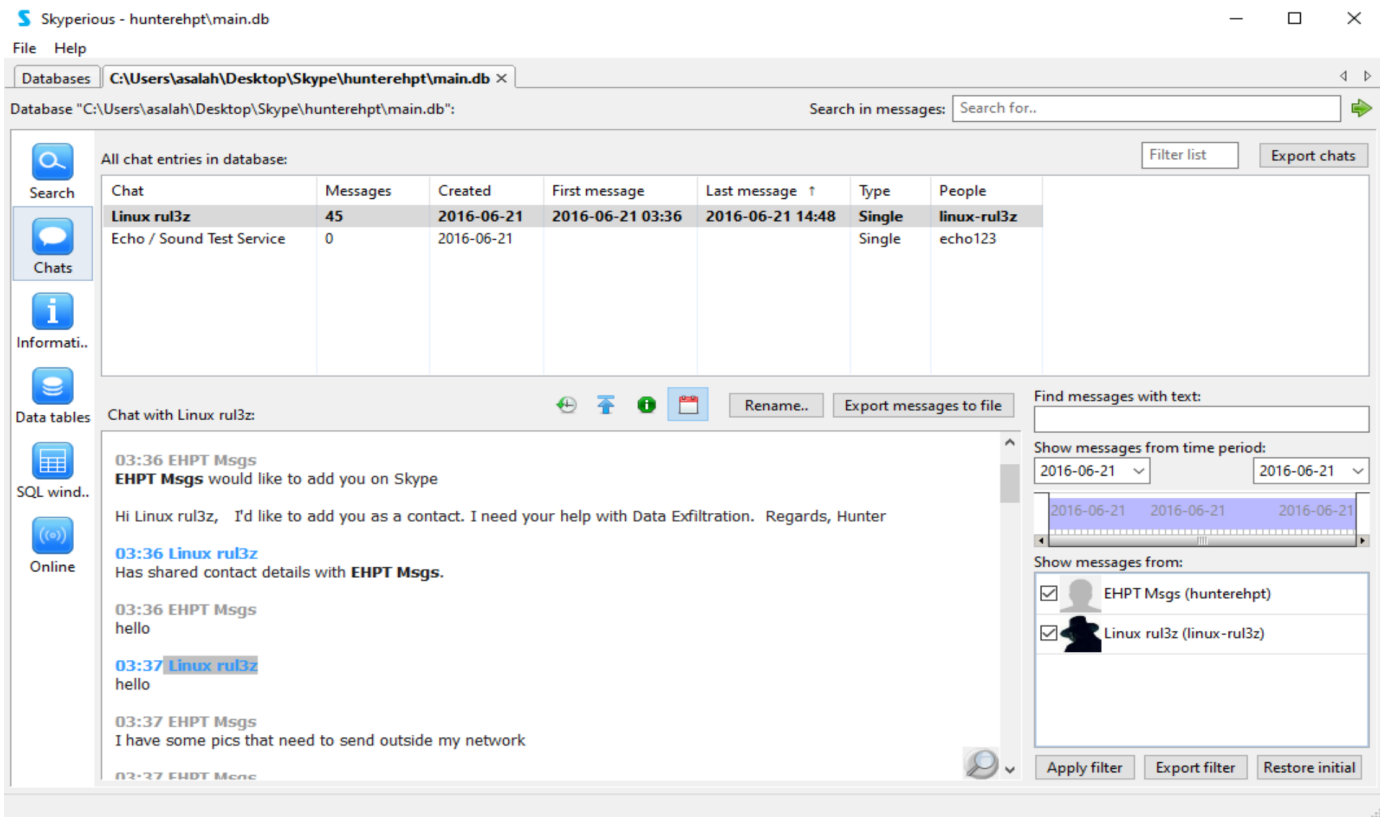

## 13-What was the version of the network scanner running on this computer?




أو من خلال :




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



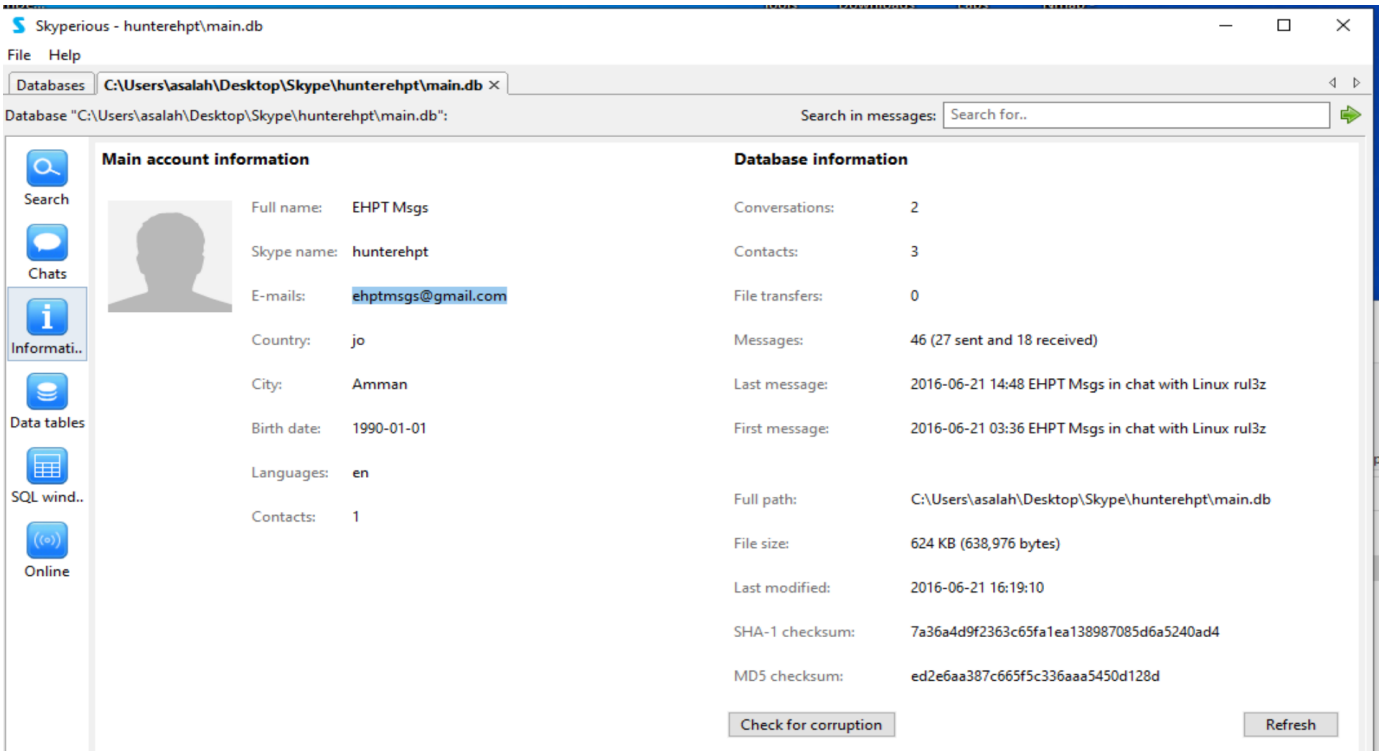
**15-What is the name of the application both parties agreed to use to exfiltrate data and provide remote access for the external attacker in their Skype conversation?**

03:47 Linux rul3z
can you install team viewer?

03:47 EHPT Msgs
I am not sure

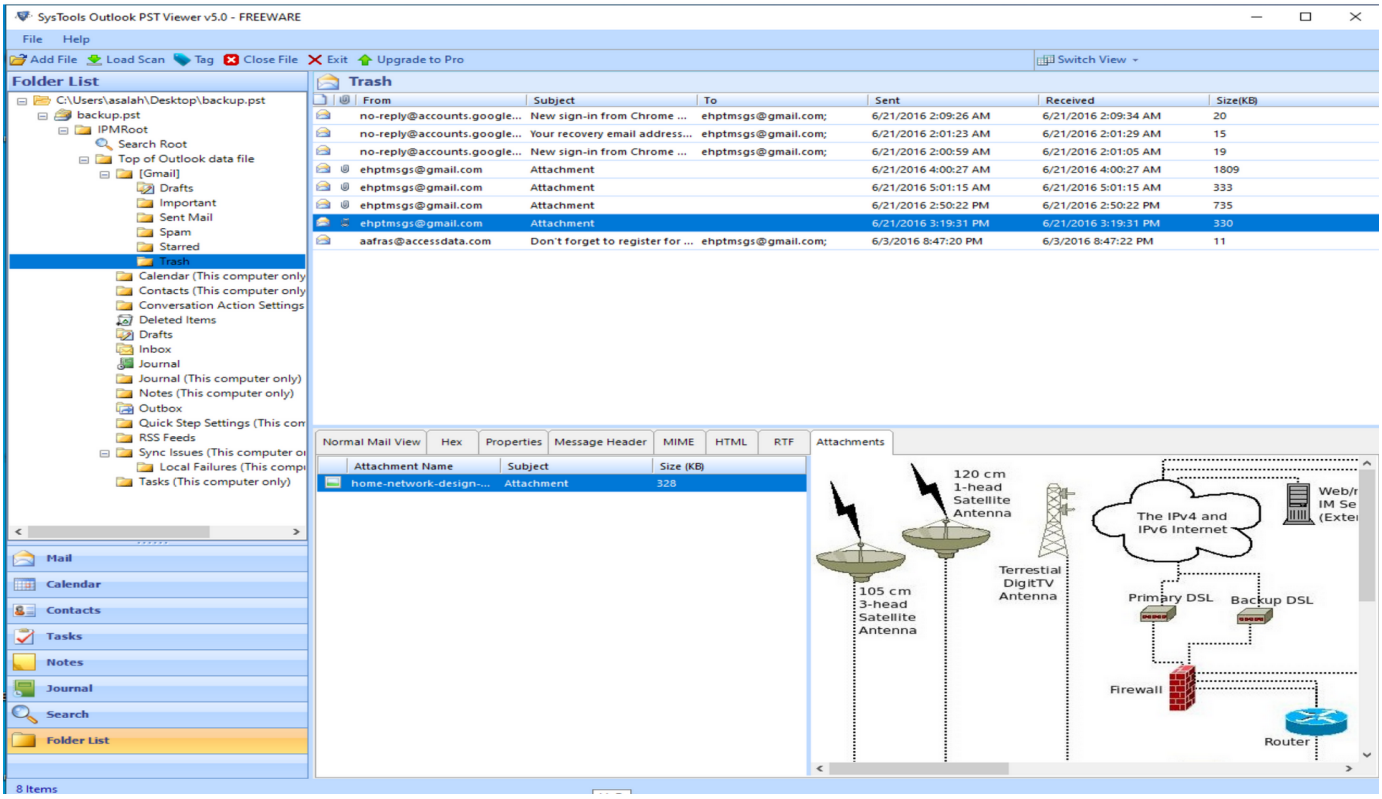
---

**16-What is the Gmail email address of the suspect employee?**

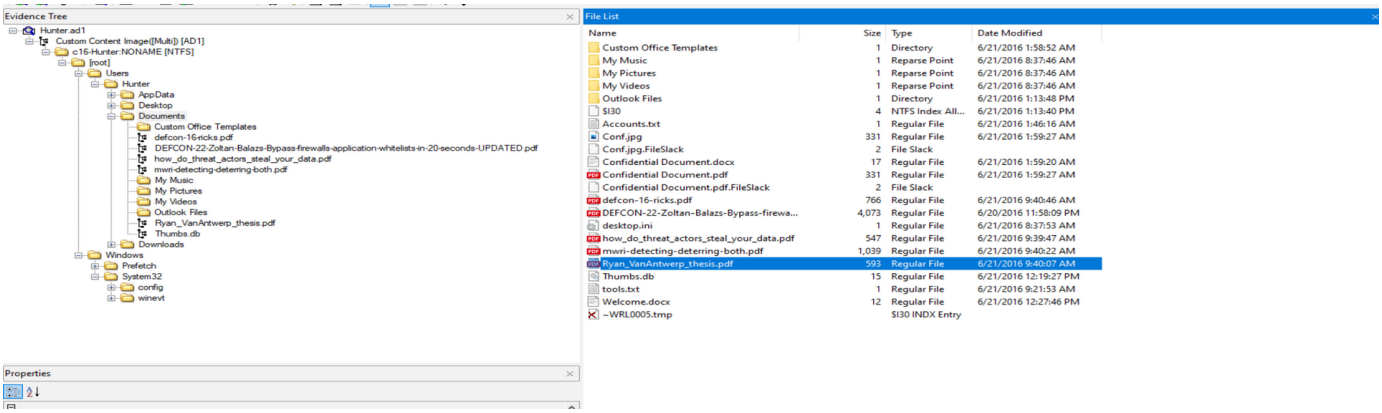



---

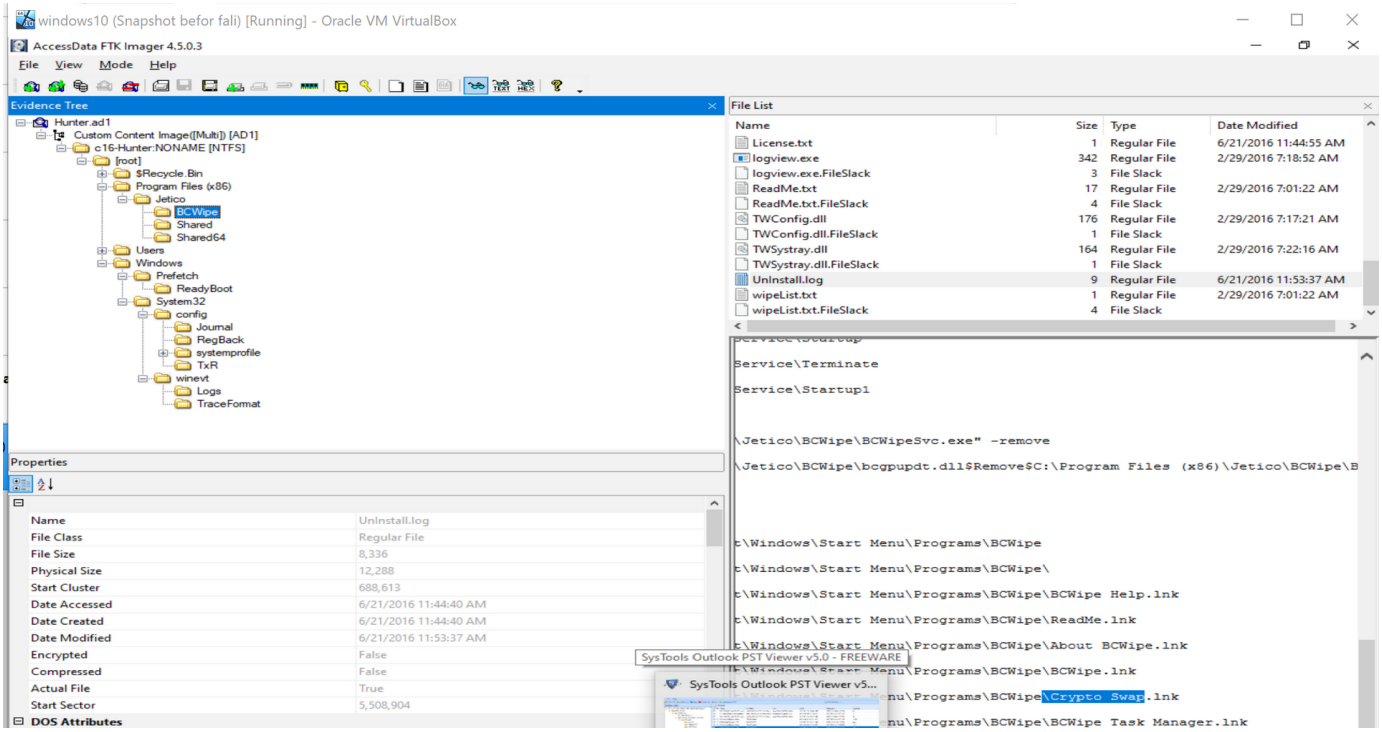
**17-It looks like the suspect user deleted an important diagram after his conversation with the external attacker. What is the file name of the deleted diagram?**




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




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

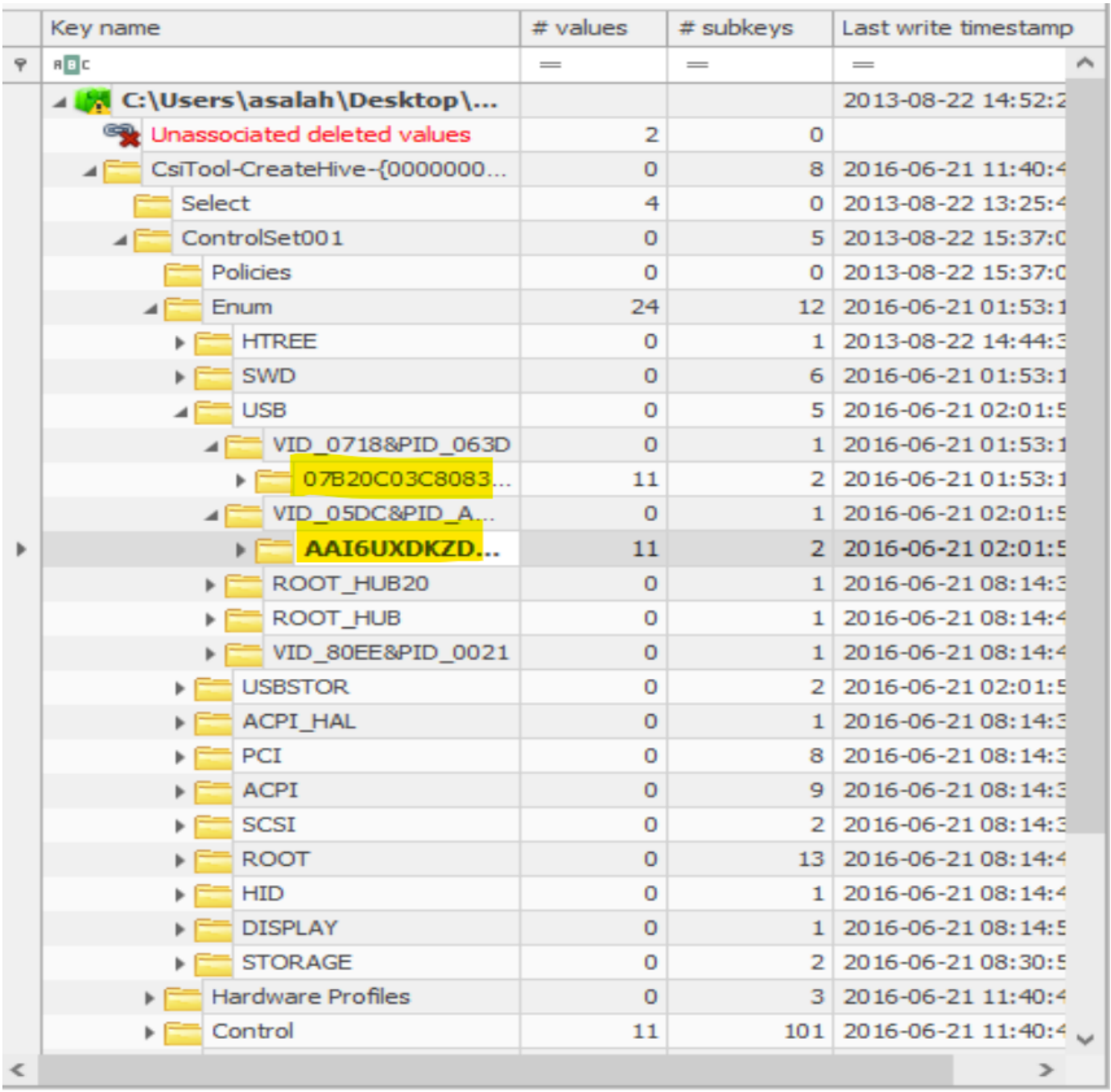



---

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

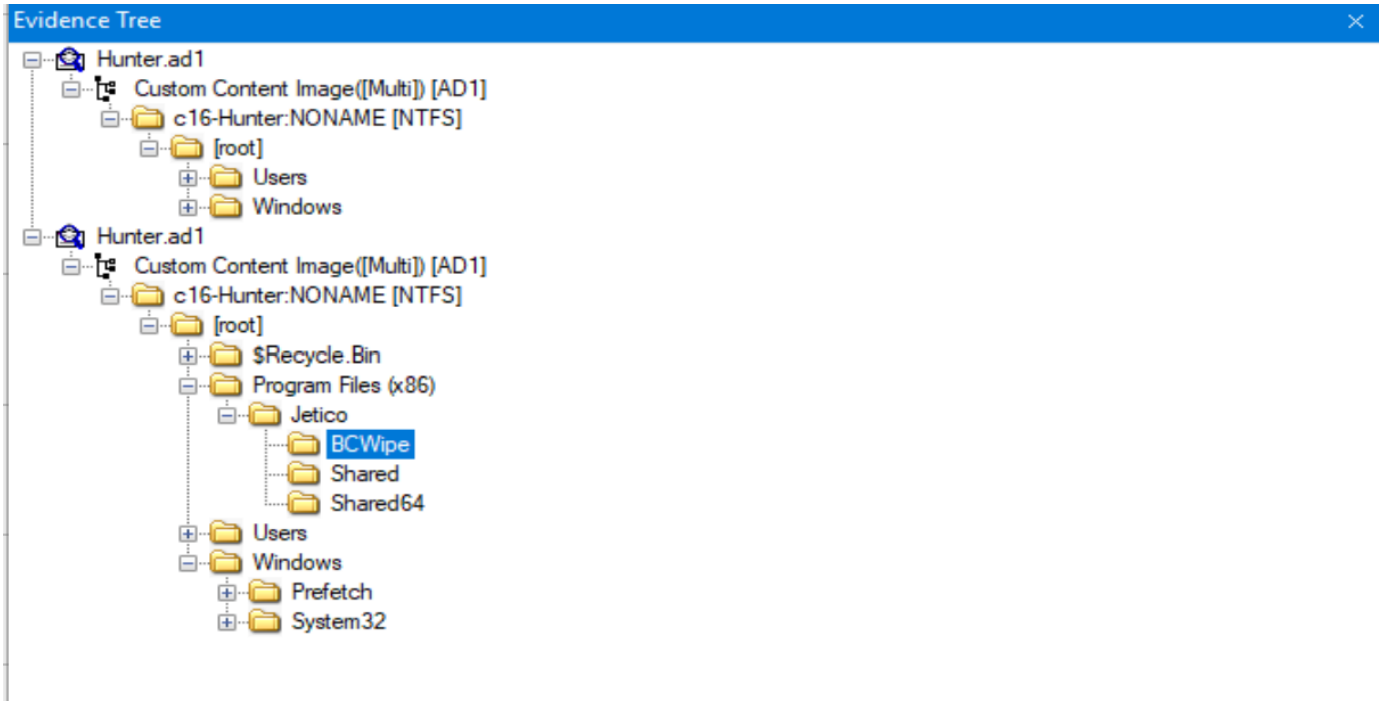
من ملف الـSystem ومن ثم Registry Explorer خلال هذا المسار

```
\SYSTEM\CurrentControlSet\Enum\USB\
```

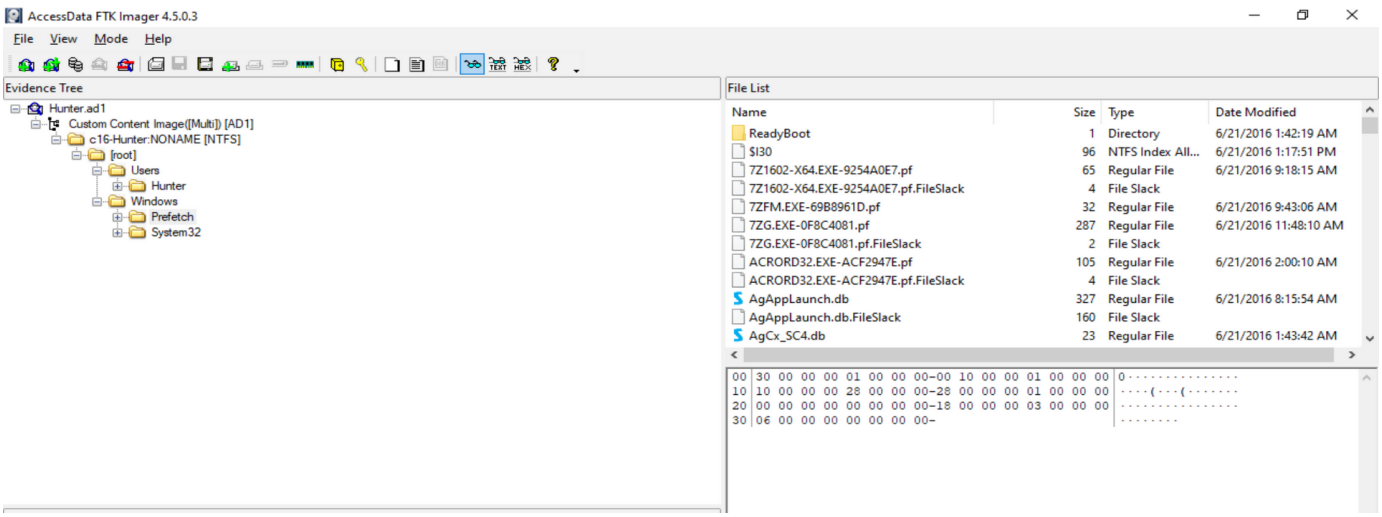


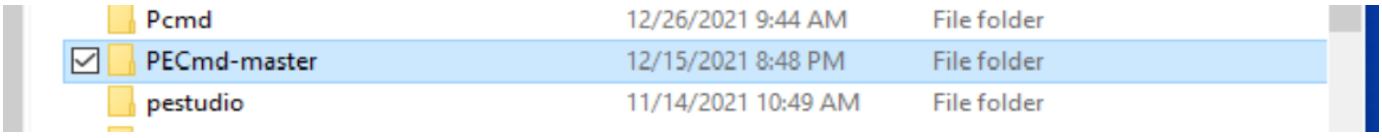
| Key name | # values | # subkeys | Last write timestamp |
|---|---|---|---|
| C:\Users\asalah\Desktop\... | | | 2013-08-22 14:52:2 |
| Unassociated deleted values | 2 | 0 | |
| CsiTool-CreateHive-{0000000... | 0 | 8 | 2016-06-21 11:40:4 |
| Select | 4 | 0 | 2013-08-22 13:25:4 |
| ControlSet001 | 0 | 5 | 2013-08-22 15:37:0 |
| Policies | 0 | 0 | 2013-08-22 15:37:0 |
| Enum | 24 | 12 | 2016-06-21 01:53:1 |
| HTREE | 0 | 1 | 2013-08-22 14:44:3 |
| SWD | 0 | 6 | 2016-06-21 01:53:1 |
| USB | 0 | 5 | 2016-06-21 02:01:5 |
| VID_0718&PID_063D | 0 | 1 | 2016-06-21 01:53:1 |
| 07B20C03C8083... | 11 | 2 | 2016-06-21 01:53:1 |
| VID_05DC&PID_A... | 0 | 1 | 2016-06-21 02:01:5 |
| AAI6UXDKZD... | 11 | 2 | 2016-06-21 02:01:5 |
| ROOT_HUB20 | 0 | 1 | 2016-06-21 08:14:3 |
| ROOT_HUB | 0 | 1 | 2016-06-21 08:14:4 |
| VID_80EE&PID_0021 | 0 | 1 | 2016-06-21 08:14:4 |
| USBSTOR | 0 | 2 | 2016-06-21 02:01:5 |
| ACPI_HAL | 0 | 1 | 2016-06-21 08:14:3 |
| PCI | 0 | 8 | 2016-06-21 08:14:3 |
| ACPI | 0 | 9 | 2016-06-21 08:14:3 |
| SCSI | 0 | 2 | 2016-06-21 08:14:3 |
| ROOT | 0 | 13 | 2016-06-21 08:14:4 |
| HID | 0 | 1 | 2016-06-21 08:14:4 |
| DISPLAY | 0 | 1 | 2016-06-21 08:14:5 |
| STORAGE | 0 | 2 | 2016-06-21 08:30:5 |
| Hardware Profiles | 0 | 3 | 2016-06-21 11:40:4 |
| Control | 11 | 101 | 2016-06-21 11:40:4 |

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




## 22-How many prefetch files were discovered on the system?

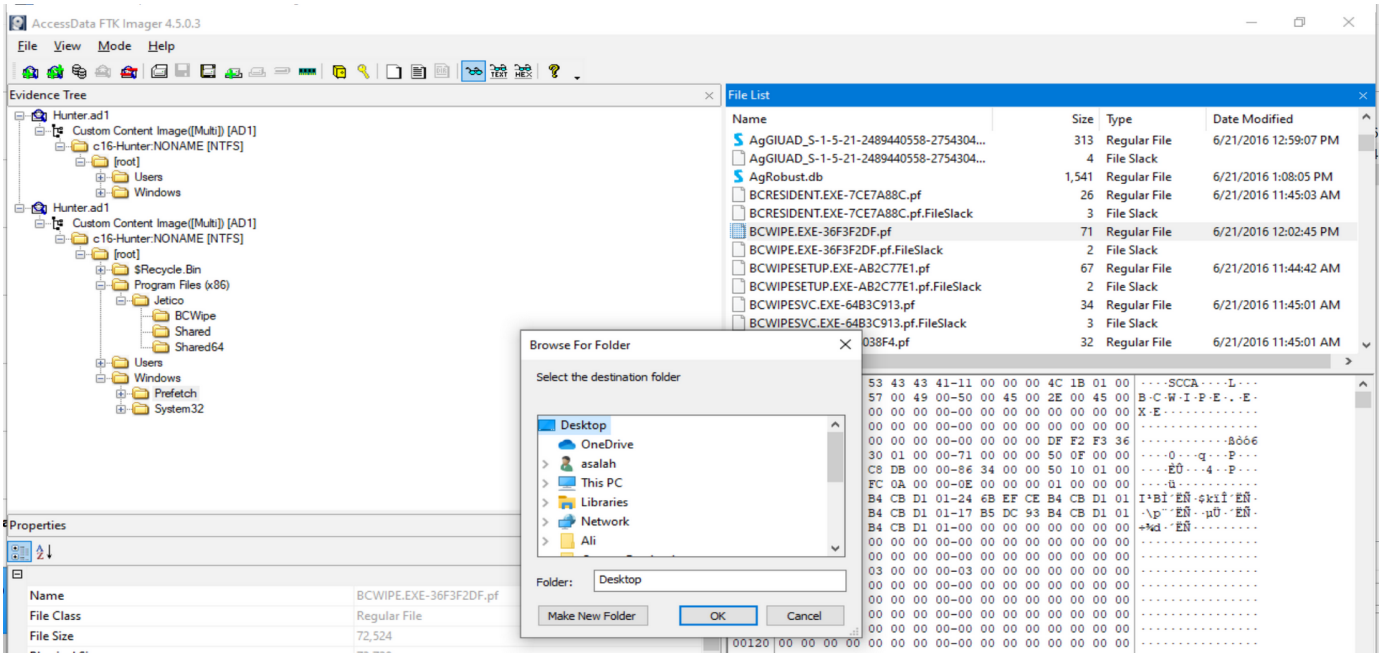



```
C:\Users\asalah\Desktop\Tools\Pcmd>PECmd.exe -d C:\Users\asalah\Desktop\Prefetch
```

```
---------- Processed 'C:\Users\asalah\Desktop\Prefetch\ZENMAP.EXE-56B17C4C.pf' in 0.04484180 seconds ----------
Processed 174 out of 174 files in 7.2692 seconds
```

## 23-How many times was the file shredder application executed?



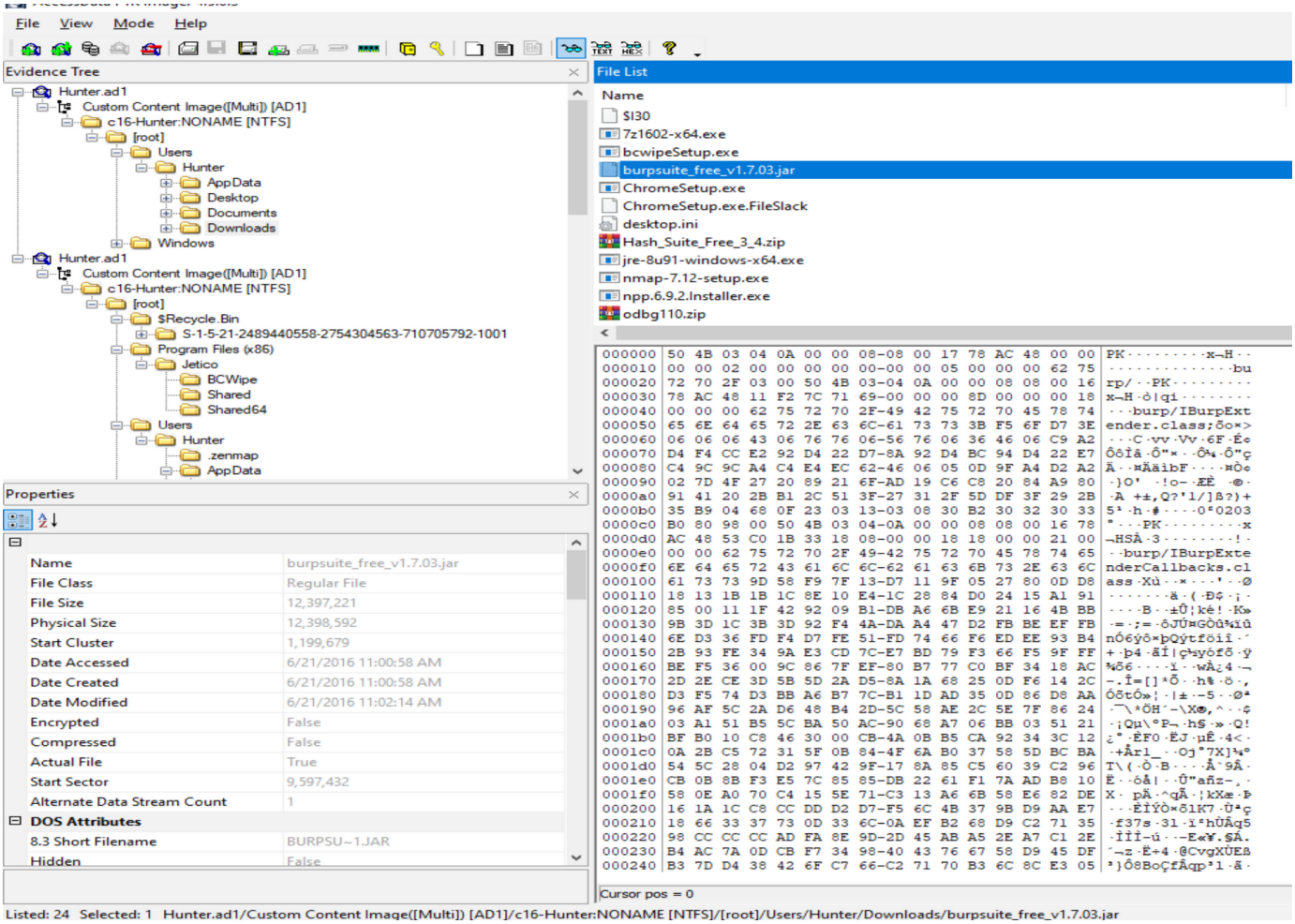

```
C:\Users\asalah\Desktop\Tools\Pcmd>PECmd.exe -f "C:\Users\asalah\Desktop\BCWIPE.EXE-36F3F2DF.pf"
PECmd version 1.4.0.0
```

```
Executable name: BCWIPE.EXE
Hash: 36F3F2DF
File size (bytes): 72,524
Version: Windows 8.0, Windows 8.1, or Windows Server 2012(R2)

Run count: 5
Last run: 2016-06-21 12:02:35
Other run times: 2016-06-21 12:02:39, 2016-06-21 12:01:35, 2016-06-21 12:01:00, 2016-06-21 12:00:56

Volume information:

#0: Name: \DEVICE\HARDDISKVOLUME2 Serial: 669B1B2A Created: 2016-06-21 09:09:24 Directories: 14 File references: 84
#1: Name: \DEVICE\HARDDISKVOLUMESHADOWCOPY1 Serial: 669B1B2A Created: 2016-06-21 09:09:24 Directories: 0 File references
: 0
#2: Name: \DEVICE\HARDDISKVOLUMESHADOWCOPY2 Serial: 669B1B2A Created: 2016-06-21 09:09:24 Directories: 0 File references
: 0
```

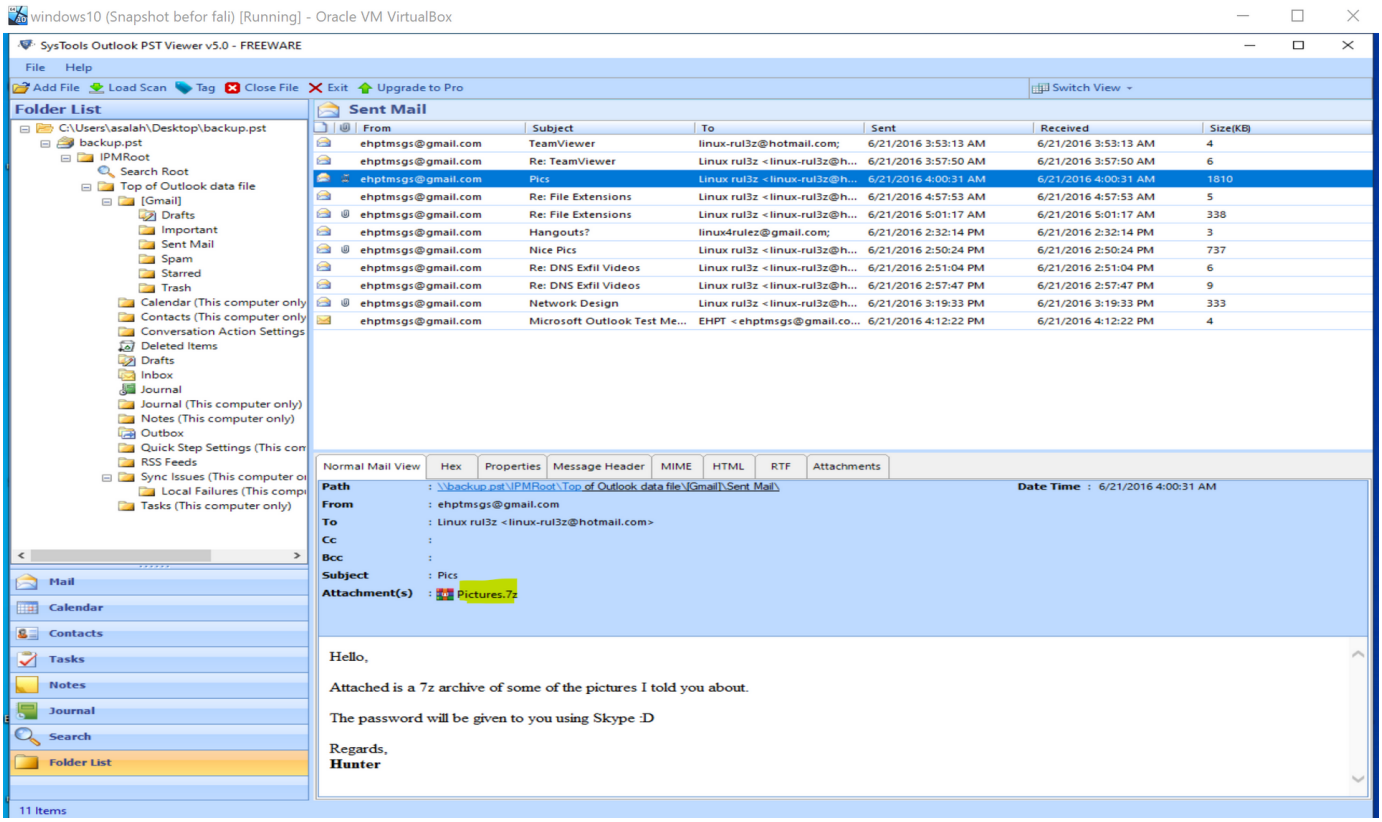
## 24-Using prefetch, determine when was the last time ZENMAP.EXE-56B17C4C.pf was executed?

```
C:\Users\asalah\Desktop\Tools\Pcmd>PECmd.exe -f "C:\Users\asalah\Desktop\ZENMAP.EXE-56B17C4C.pf"
PECmd version 1.4.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd

Command line: -f C:\Users\asalah\Desktop\ZENMAP.EXE-56B17C4C.pf

Warning: Administrator privileges not found!

Keywords: temp, tmp

Processing 'C:\Users\asalah\Desktop\ZENMAP.EXE-56B17C4C.pf'

Created on: 2016-06-21 12:08:21
Modified on: 2016-06-21 12:08:21
Last accessed on: 2021-12-27 09:02:09

Executable name: ZENMAP.EXE
Hash: 56B17C4C
File size (bytes): 93,524
Version: Windows 8.0, Windows 8.1, or Windows Server 2012(R2)

Run count: 1
Last run: 2016-06-21 12:08:13
```

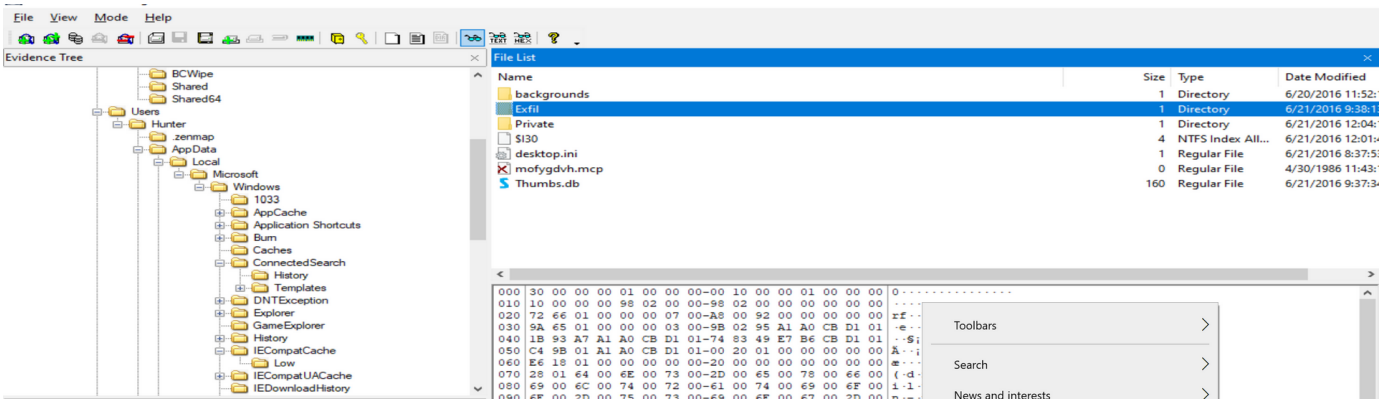
## 25-A JAR file for an offensive traffic manipulation tool was executed. What is the absolute path of the file?



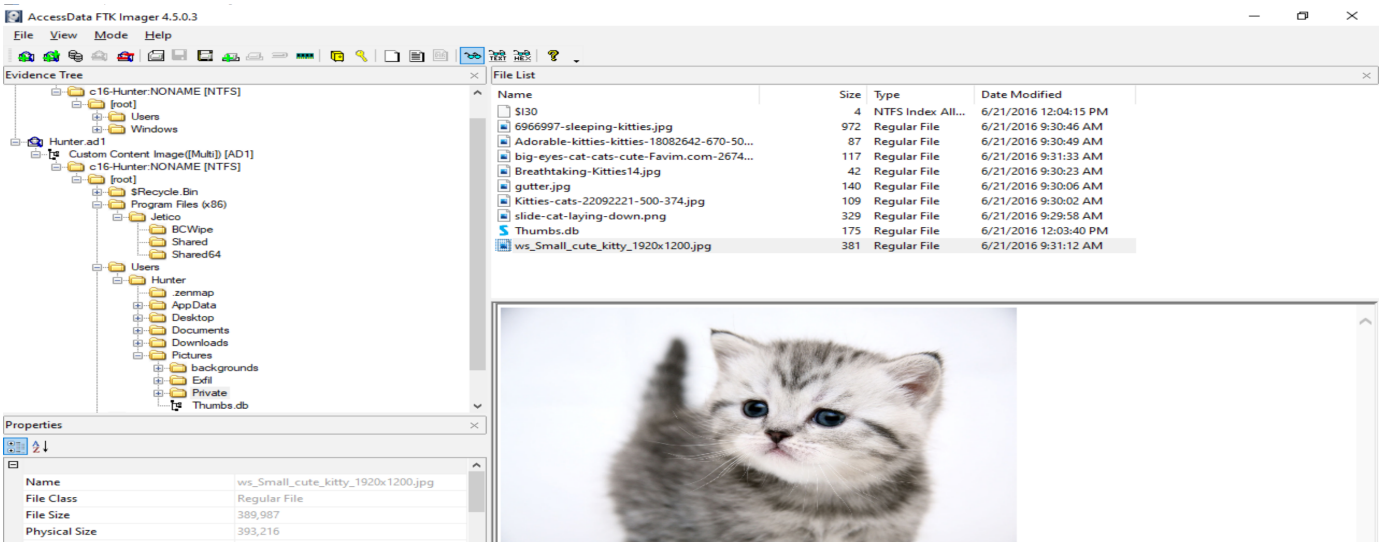

**26-The suspect employee tried to exfiltrate data by sending it as an email attachment. What is the name of the suspected attachment?**



**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?**

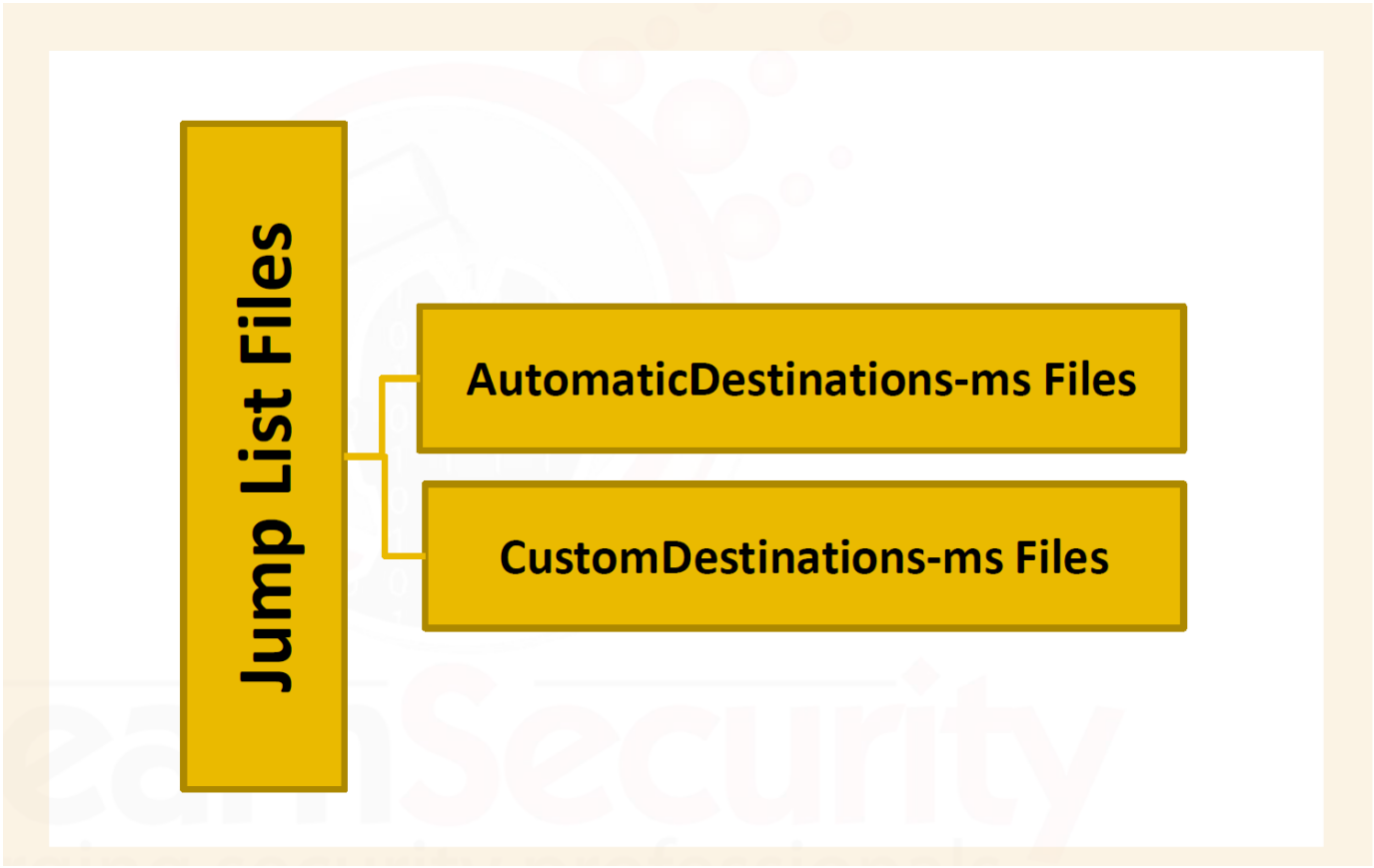



**28-The user deleted two JPG files from the system and moved them to $Recycle-Bin. What is the file name that has the resolution of 1920x1200?**



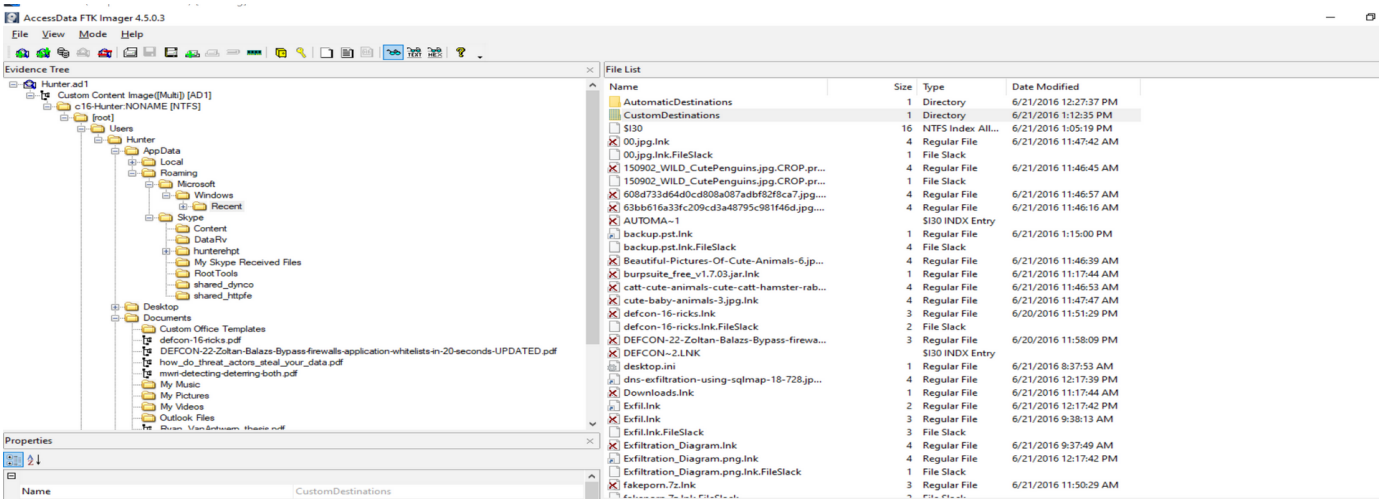

**29-Provide the name of the directory where information about jump lists items (created automatically by the system) is stored?**

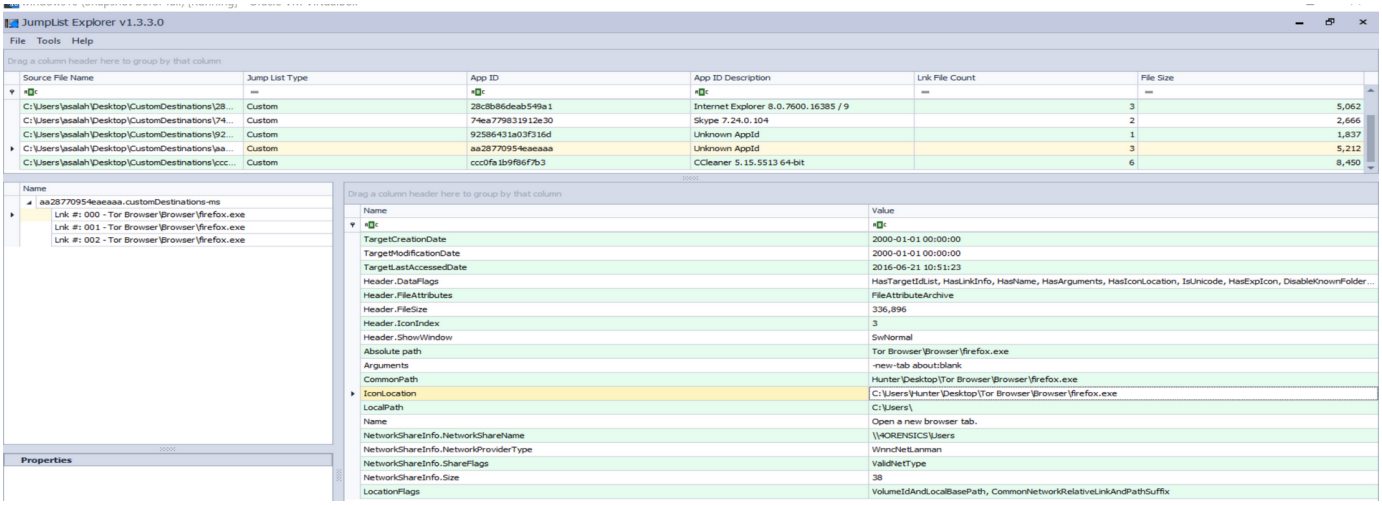
AutomaticDestinations-ms




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

\AppData\Roaming\Microsoft\Windows\






---

AsalahMohammed..

---