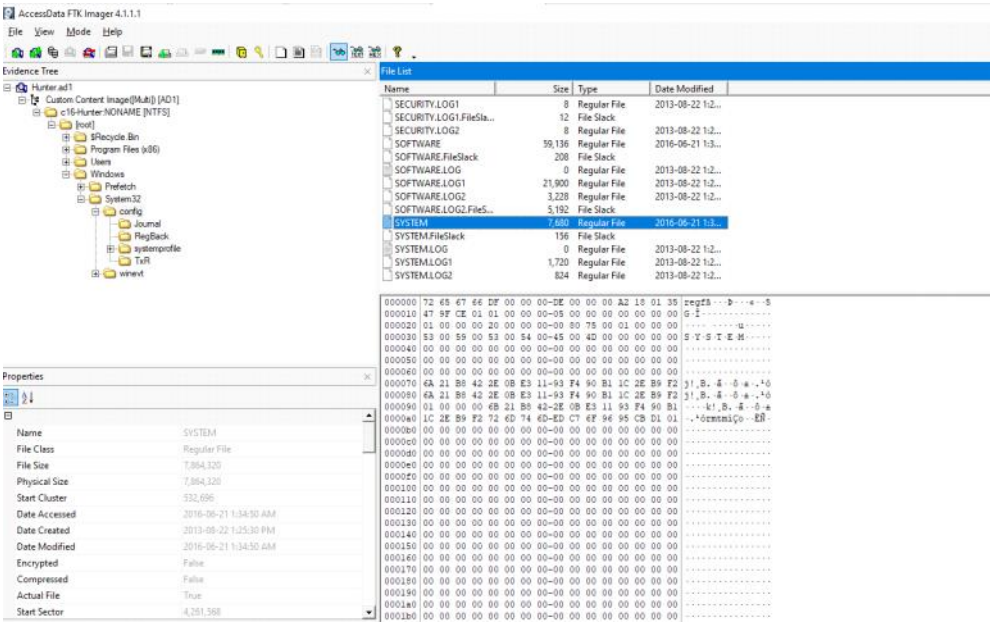
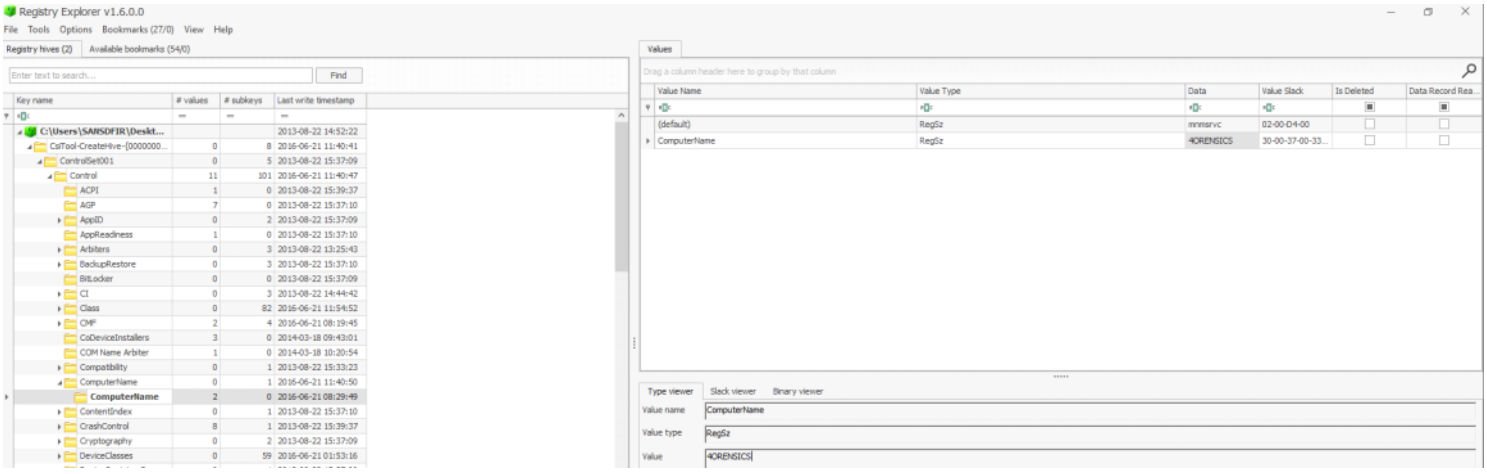
Hunter

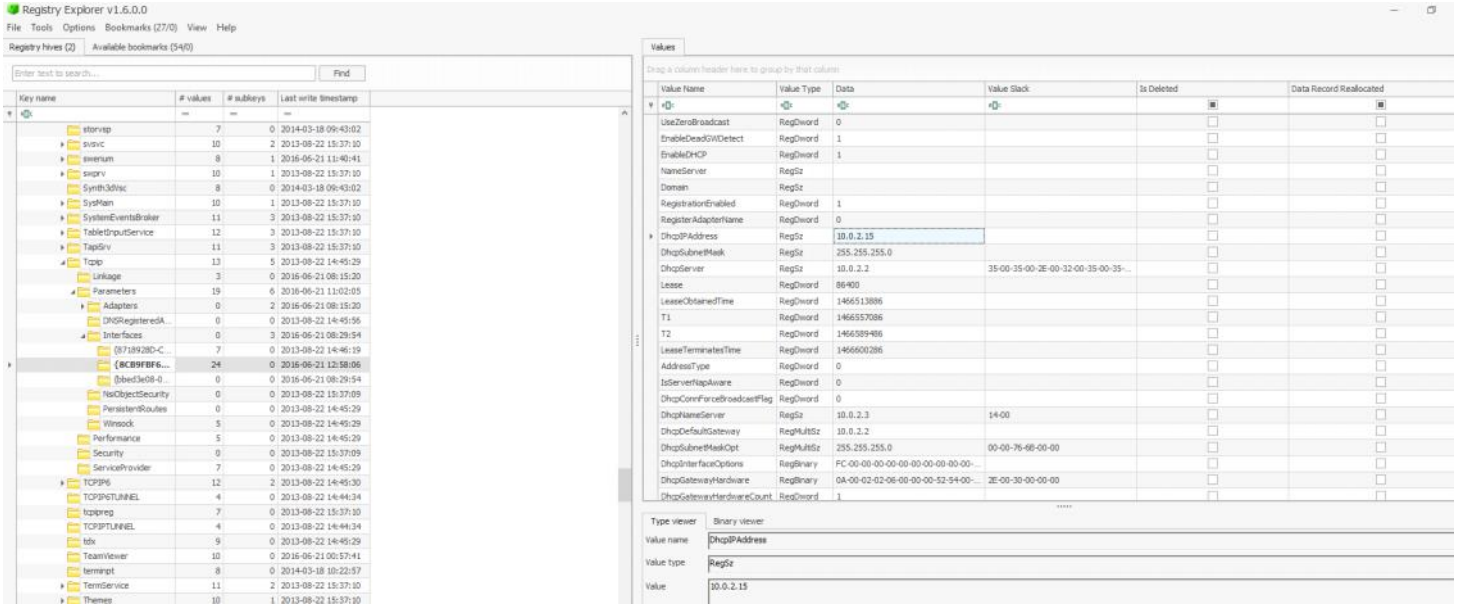
Friday, 17 June, 2022 10:13 PM

#1 What is the computer name of the suspect machine?
4ORENSICS

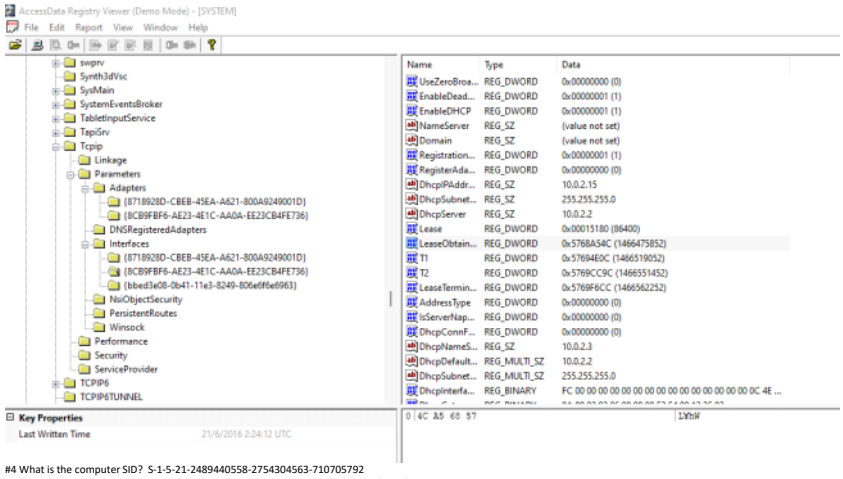




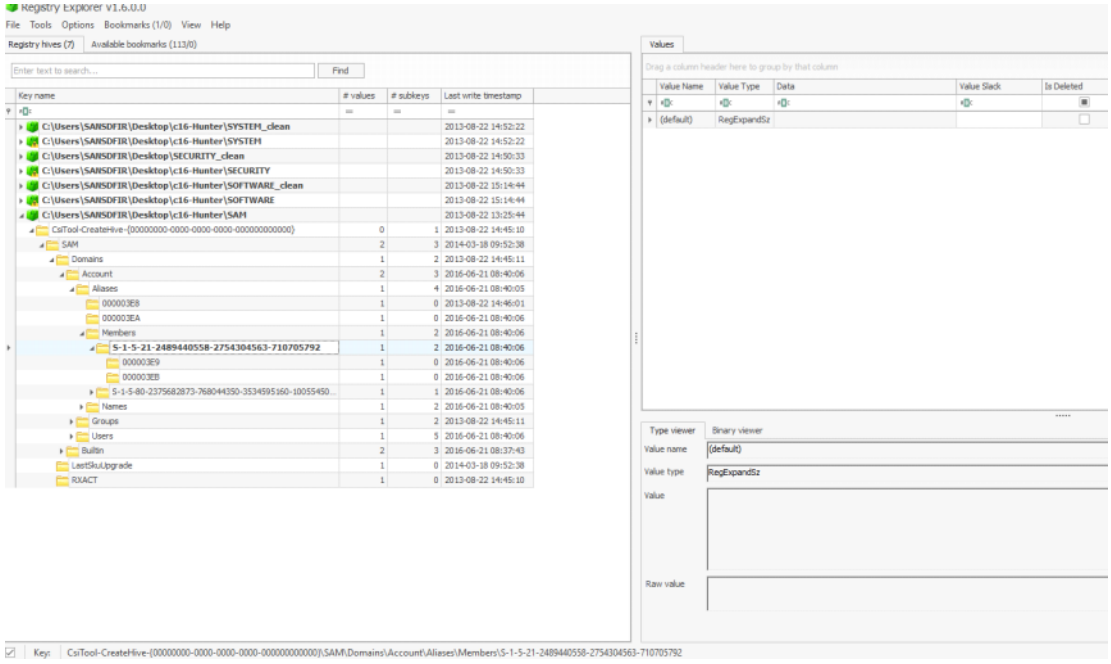
#2 What is the computer IP?
10.0.2.15



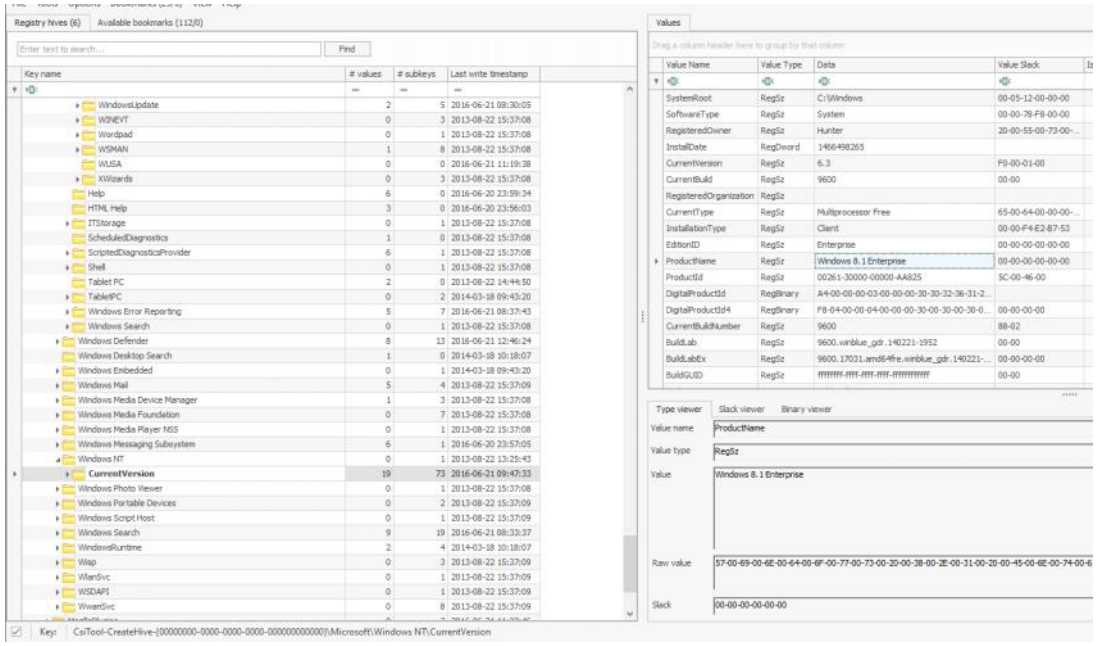
#3 What was the DHCP LeaseObtainedTime?
21/06/2016 02:24:12 UTC



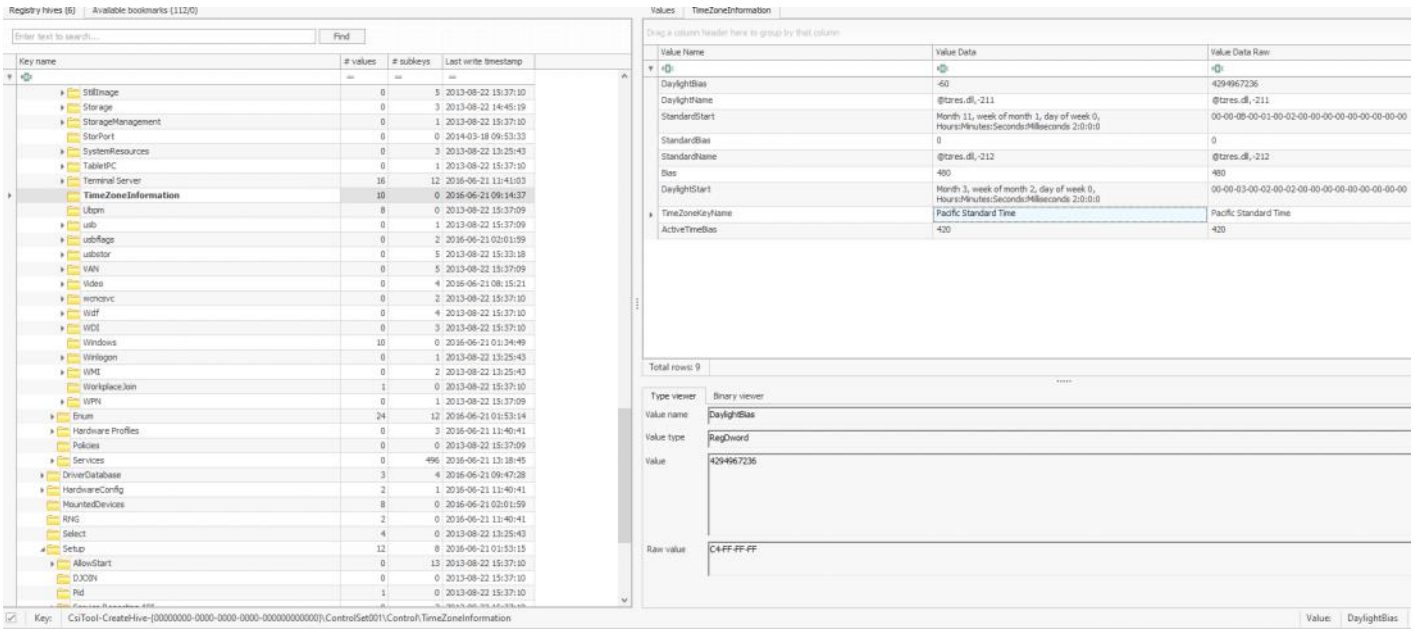
#4 What is the computer SID? S-1-5-21-2489440558-2754304563-710705792
A computer's SID is stored in the Registry's SECURITY hive under HKLM\SECURITY\SAM\Domains
\Account.
S-1-5-21-2489440558-2754304563-710705792



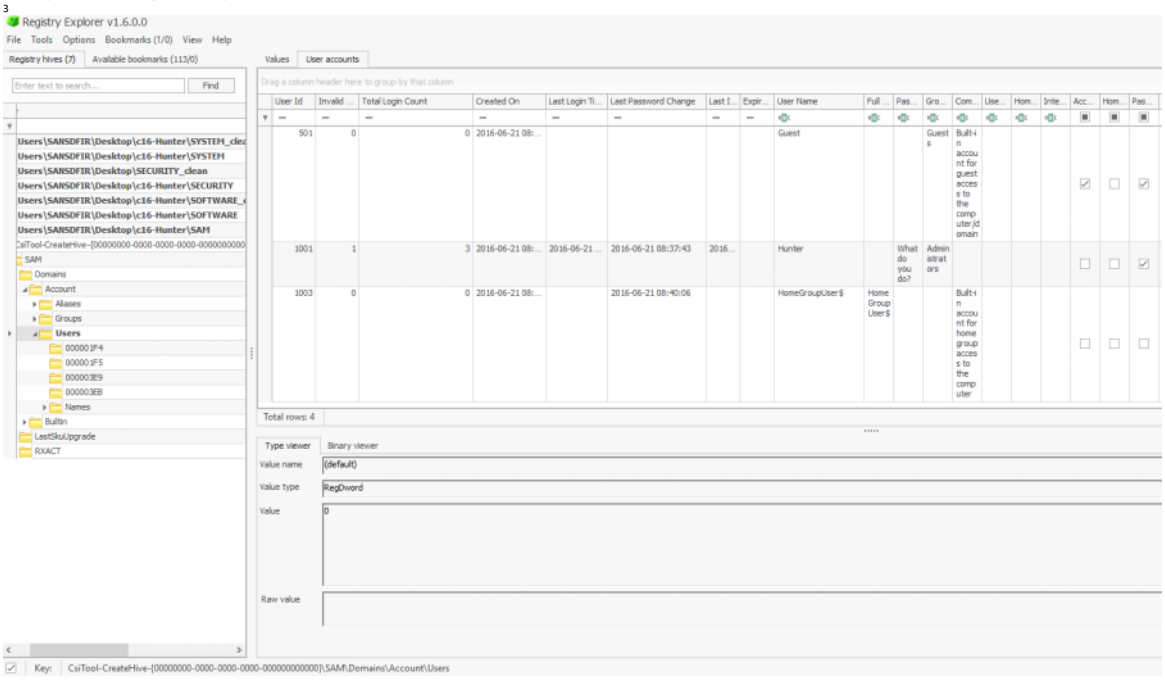
What is the Operating System(OS) version?
8.1



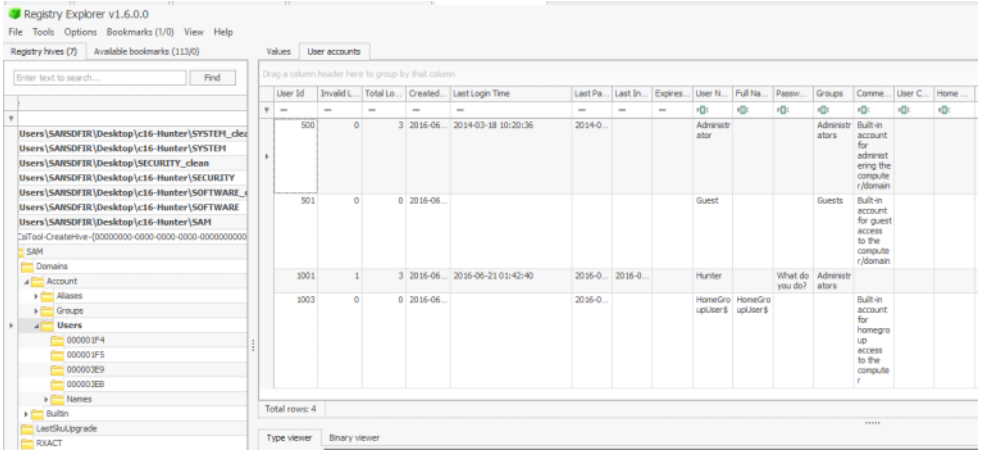
What was the computer timezone?
UTC-07:00



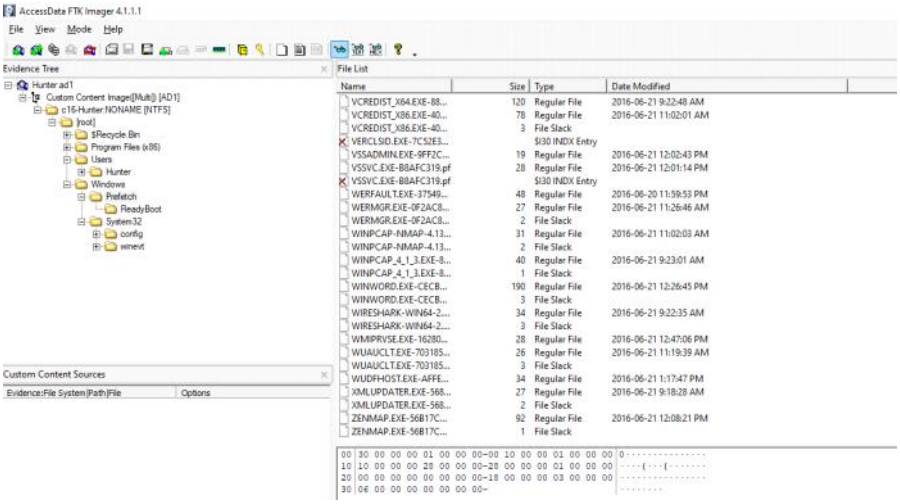
How many times did this user log on to the computer?
3

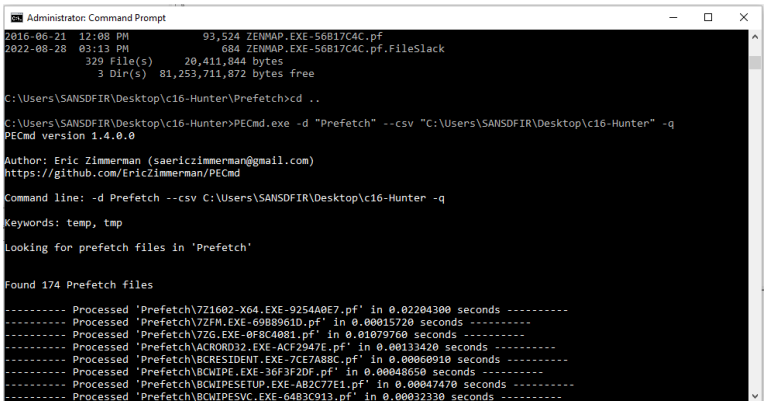


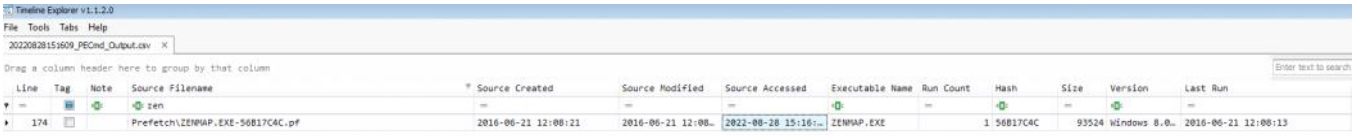
When was the last login time for the discovered account? Format: one-space between date and time
2016-06-21 01:42:40



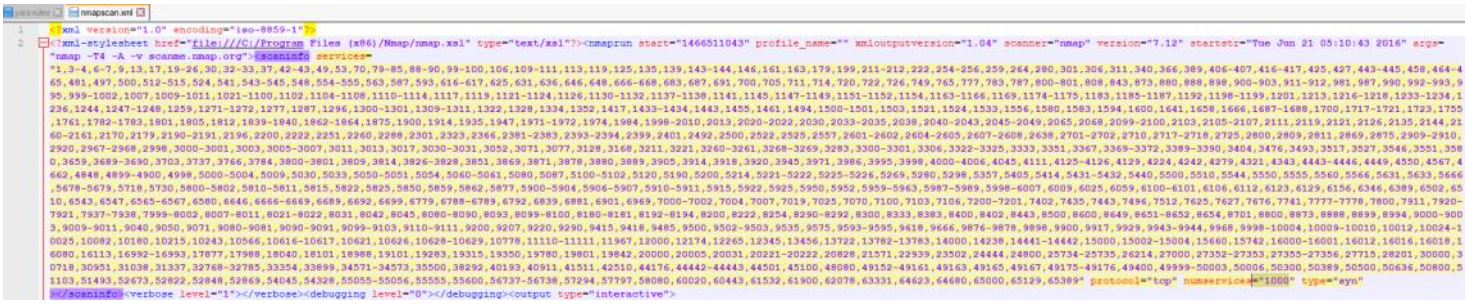
#9 There was a "Network Scanner" running on this computer, what was it? And when was the last time the suspect used it? Format: program.exe,YYYY-MM-DD HH:MM:SS UTC







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



```
1   1.00 ms 10.0.2.2

2   1.00 ms 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

Read data files from: C:\Program Files (x86)\Nmap

OS and Service detection performed. Please 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 (64.387KB)
```

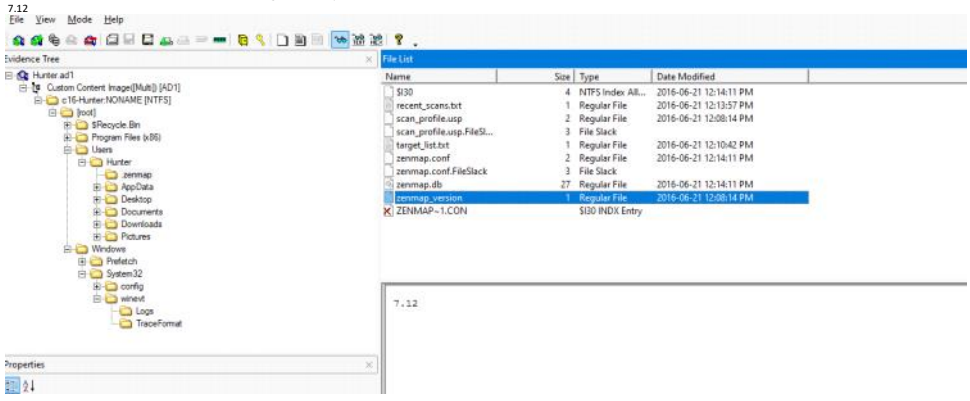

```
</output><host comment=""><status state="up"></status><address addrtype="ipv4" vendor="" addr="45.33.32.156"></address><hostnames><hostname type="user" name="scanme.nmap.org"></hostname><hostname type="PTR" name=
"scanme.nmap.org"></hostname></hostnames><ports><extraports count="994" state="closed"></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><portused state="open"
portid="22" proto="tcp"></portused><portused state="closed" portid="1" proto="tcp"></portused><portused state="closed" portid="37741" proto="udp"></portused><osmatch line="84526" name="QEMU user mode network gateway" accuracy=
"96"><osclass type="general purpose" osfamily="QEMU" vendor="QEMU" osgen="" accuracy="96"></osclass></osmatch><osmatch line="27173" name="GNU Hurd 0.3" accuracy="87"><osclass type="general purpose" osfamily="Hurd" vendor="GNU"
osgen="" accuracy="87"></osclass></osmatch><osmatch line="2383" name="Allied Telesyn AT-9006SX/SC switch" accuracy="87"><osclass type="switch" osfamily="embedded" vendor="Allied Telesyn" osgen="" accuracy="87"
></osclass></osmatch><osmatch line="8655" name="Bay Networks BayStack 450 switch (software version 3.1.0.22)" accuracy="87"><osclass type="switch" osfamily="embedded" vendor="Bay Networks" osgen="" accuracy="87"
></osclass></osmatch><osmatch line="8673" name="Bay Networks BayStack 450 switch (software version 4.2.0.16)" accuracy="87"><osclass type="switch" osfamily="embedded" vendor="Bay Networks" osgen="" accuracy="87"
></osclass></osmatch><osmatch line="11315" name="Cabletron ELS100-24TXM Switch or Icom IC-7800 radio transceiver" accuracy="87"><osclass type="specialized" osfamily="embedded" vendor="Icom" osgen="" accuracy="87"
></osclass></osmatch><osmatch line="13078" name="Cisco Catalyst 1900 switch or RAD IPMUX-1 TDM-over-IP multiplexer" accuracy="87"><osclass type="switch" osfamily="embedded" vendor="RAD Data Communications" osgen="" accuracy="87"
></osclass></osmatch><osmatch line="82858" name="Oracle Virtualbox" accuracy="87"><osclass type="bridge" osfamily="Virtualbox" vendor="Oracle" osgen="" accuracy="87"></osclass></osmatch><osmatch line="40192" name="TiVo series 1
(Sony SVR-2000 or Philips HDR112) (Linux 2.1.24-TiVo-2.5, PowerPC)" accuracy="86"><osclass type="media device" osfamily="embedded" vendor="Sony" osgen="" accuracy="86"></osclass></osmatch><osmatch line="37456" name="Konica
Minolta 7035 printer" accuracy="86"><osclass type="printer" osfamily="embedded" vendor="Konica Minolta" osgen="" accuracy="86"></osclass></osmatch></os><uptime lastboot="" seconds=""></uptime><tcpsequence index="" values=""
difficulty=""></tcpsequence><ipidsequence values="" class=""></ipidsequence><tcptssequence values="" class=""></tcptssequence><trace port="80" proto="tcp"><hop rtt="1.00" host="" ipaddr="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>
```


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

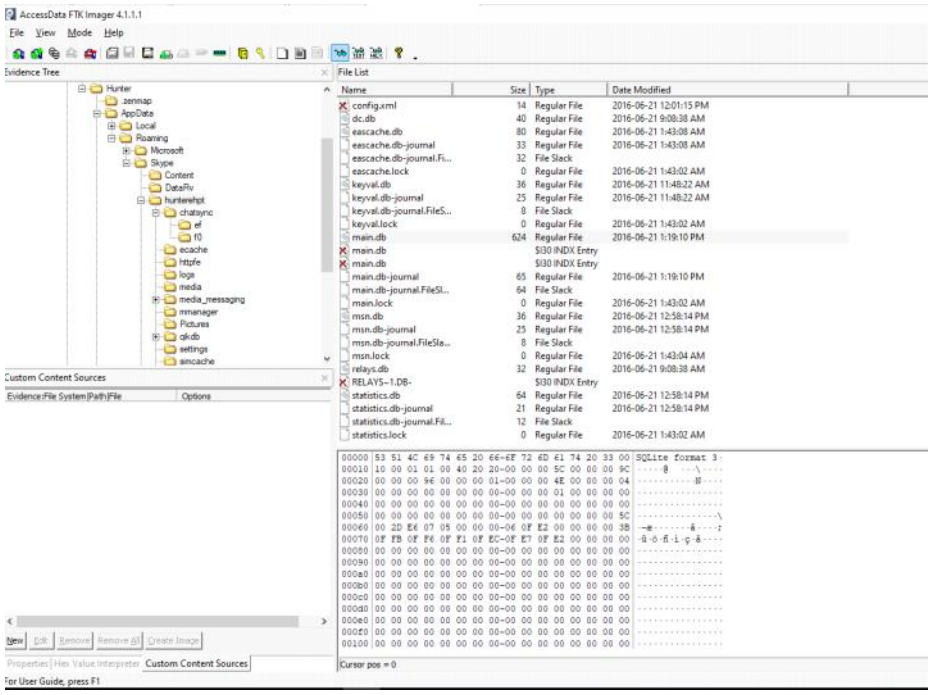
```
PORT      STATE    SERVICE       VERSION

22/tcp    open     ssh           OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)

|_  256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)

25/tcp    filtered smtp

26/tcp    filtered rsftp

80/tcp    open     http          Apache httpd 2.4.7 ((Ubuntu))

|_http-favicon: Unknown favicon MD5: 156515DA3C0F7DC6B2493BD5CE43F795

| http-methods:

|_  Supported Methods: POST OPTIONS GET HEAD

|_http-server-header: Apache/2.4.7 (Ubuntu)

|_http-title: Go ahead and ScanMe!

9929/tcp  open     nping-echo    Nping echo

31337/tcp open     ssl/ncat-chat Ncat chat (users: nobody)
```

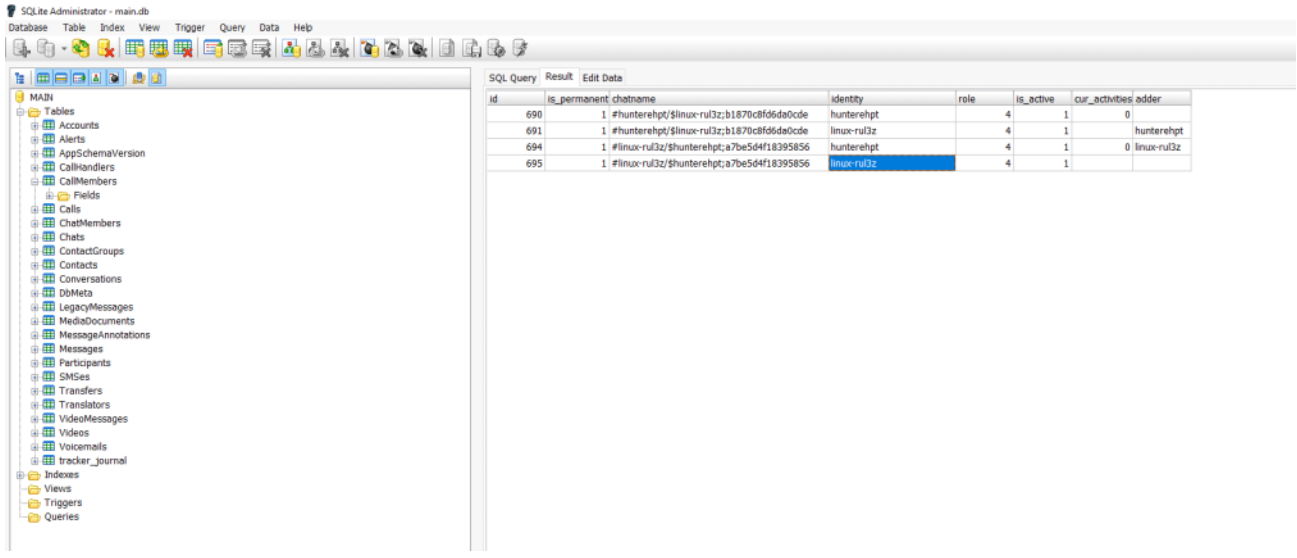
#13 What was the version of the network scanner running on this computer?

7.12

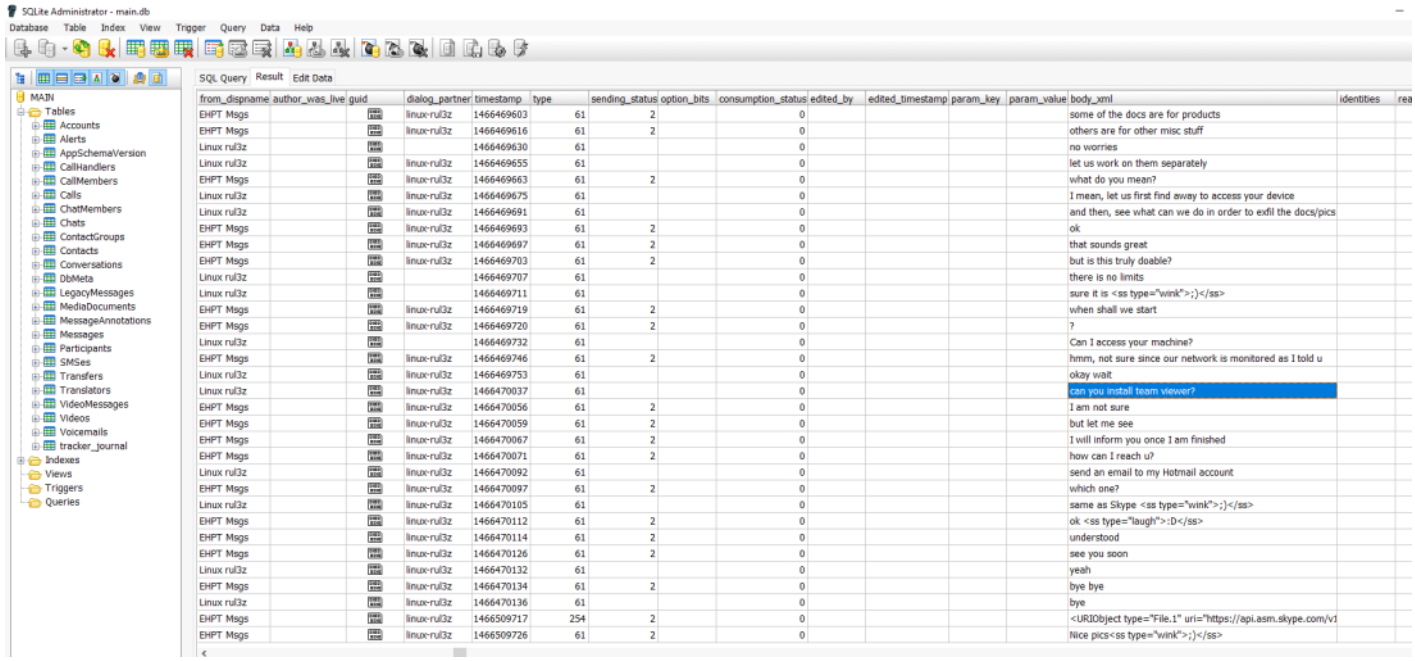


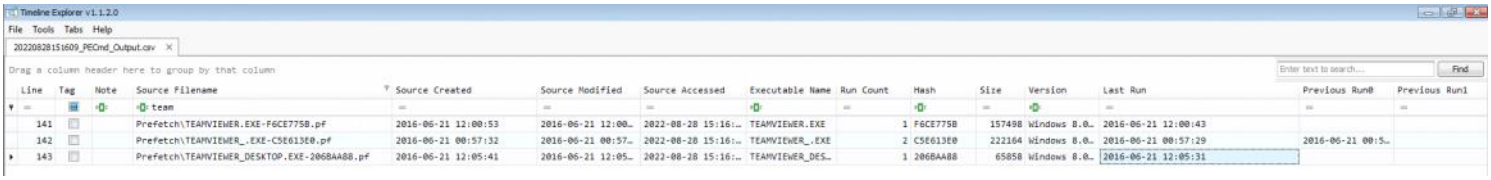
14. The employee engaged in a Skype conversation with someone. What is the skype username of the other party?



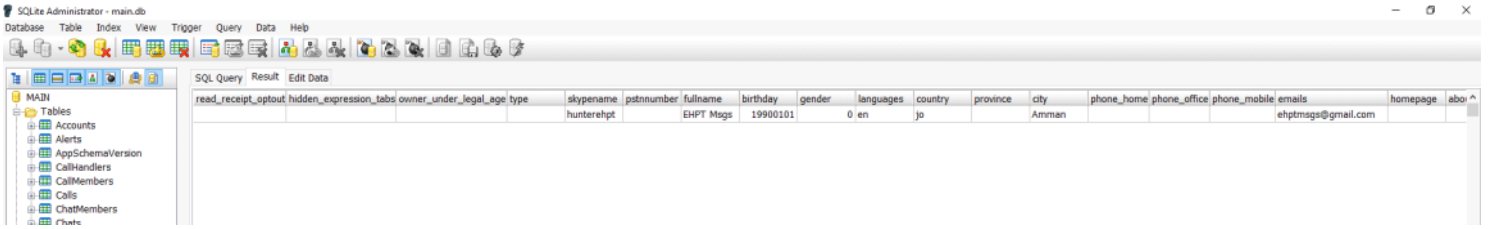


15. What is the name of the application both parties agreed to use to exfiltrate data and provide remote access for the external attacker in their Skype conversation?

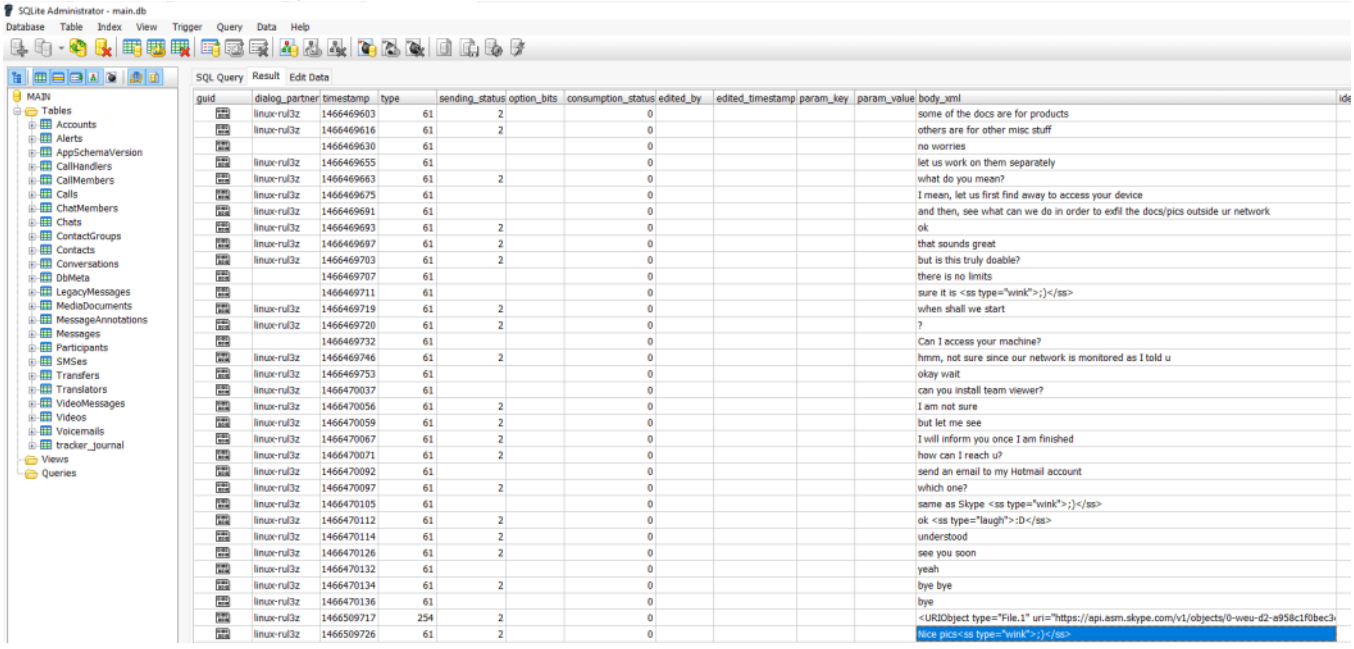


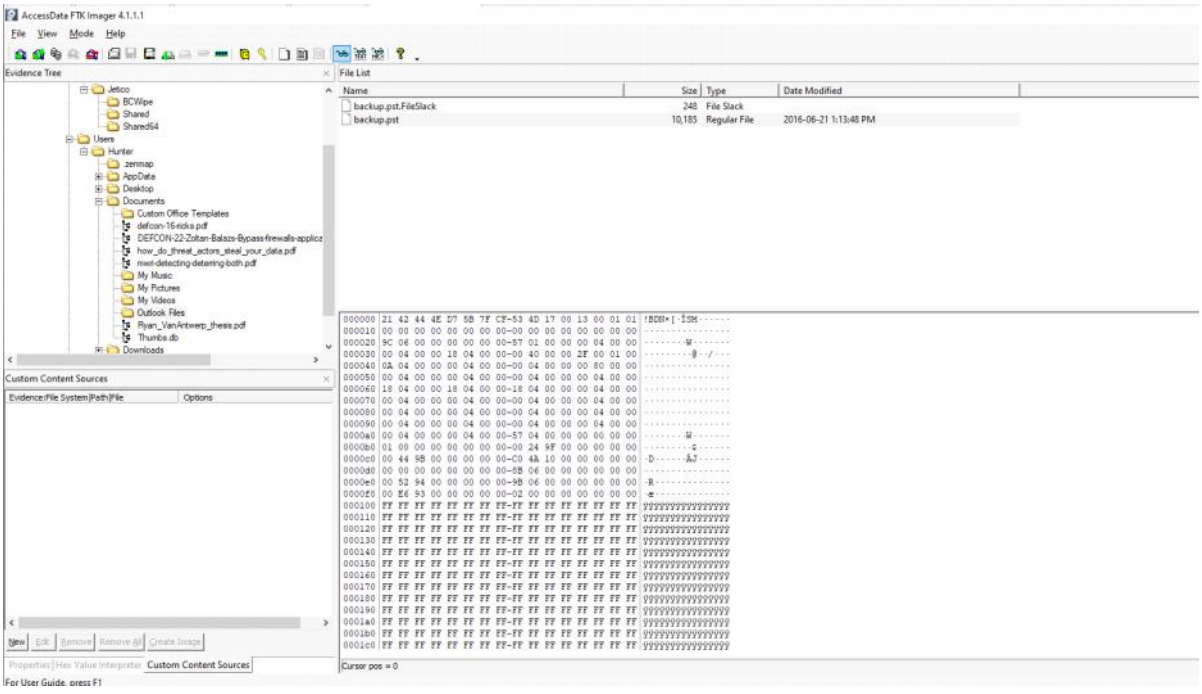


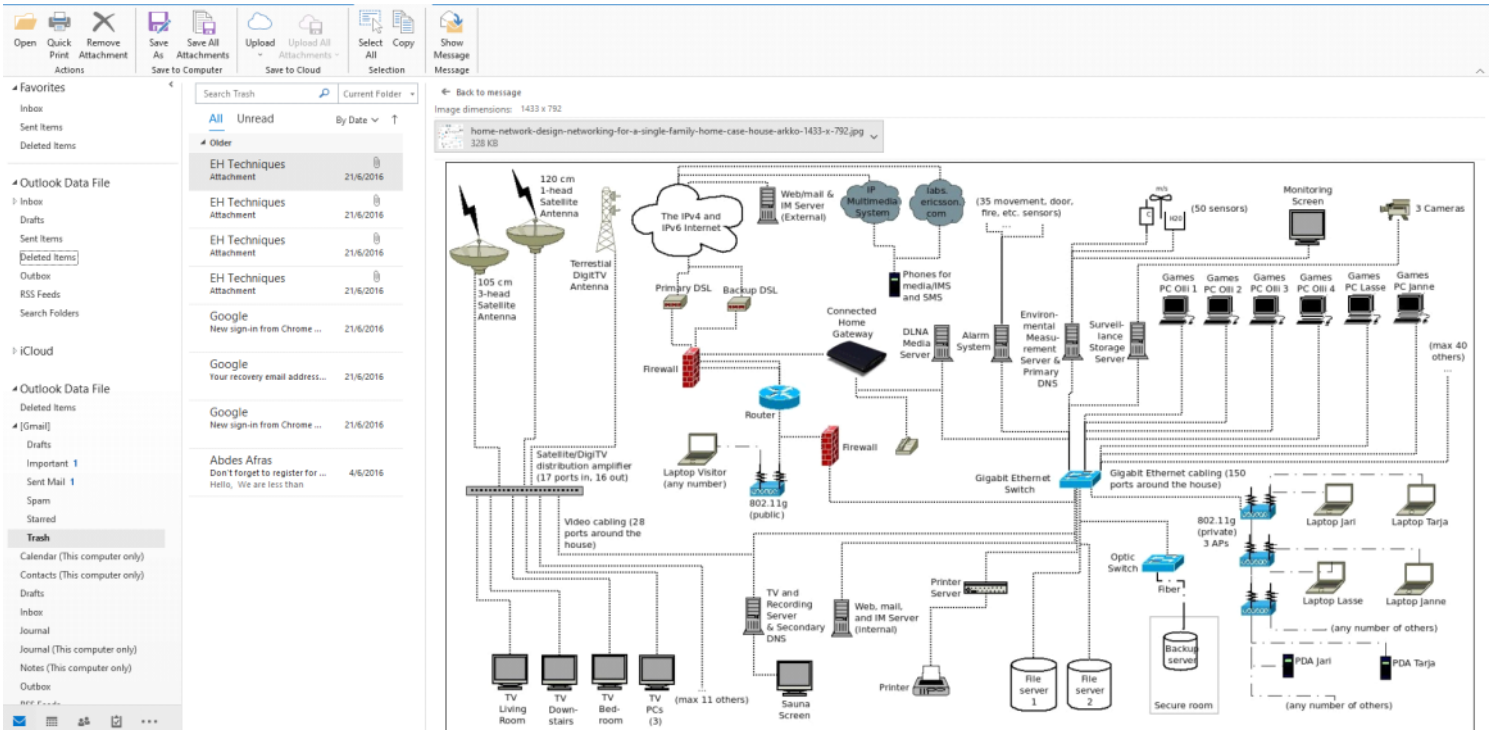
16. What is the Gmail email address of the suspect employee?



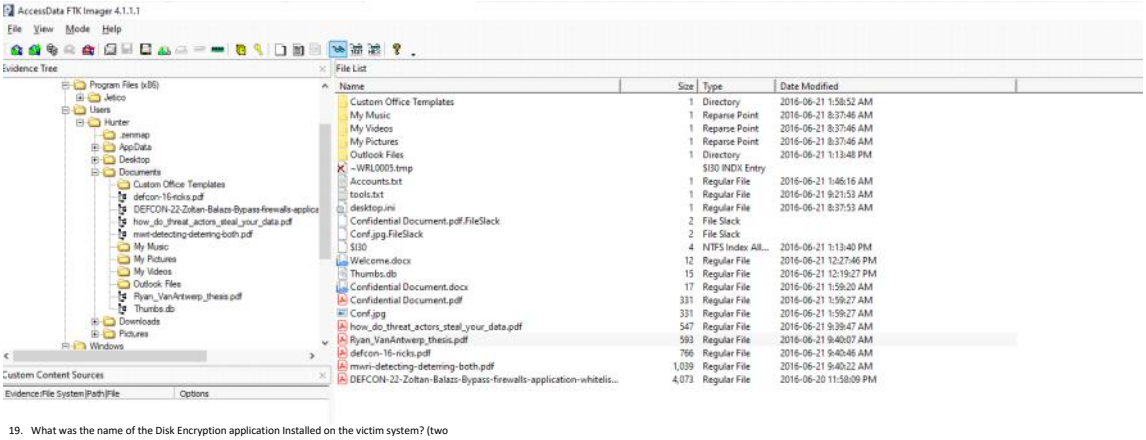
17. It looks like the suspect user deleted an important diagram after his conversation with the external attacker. What is the file name of the deleted diagram?



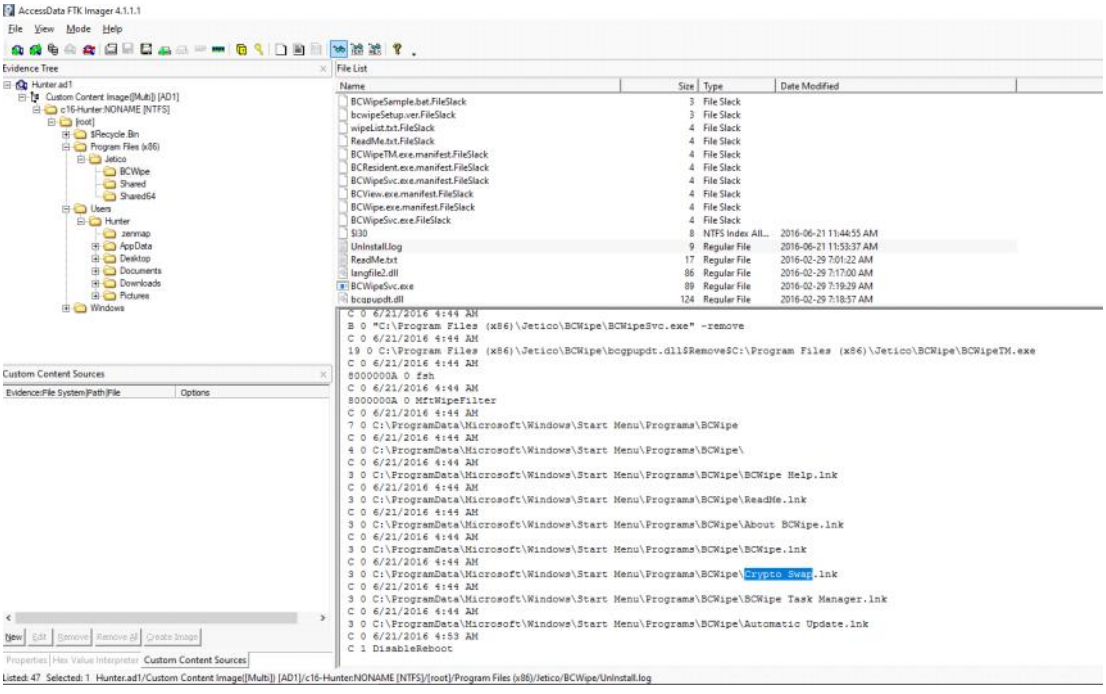




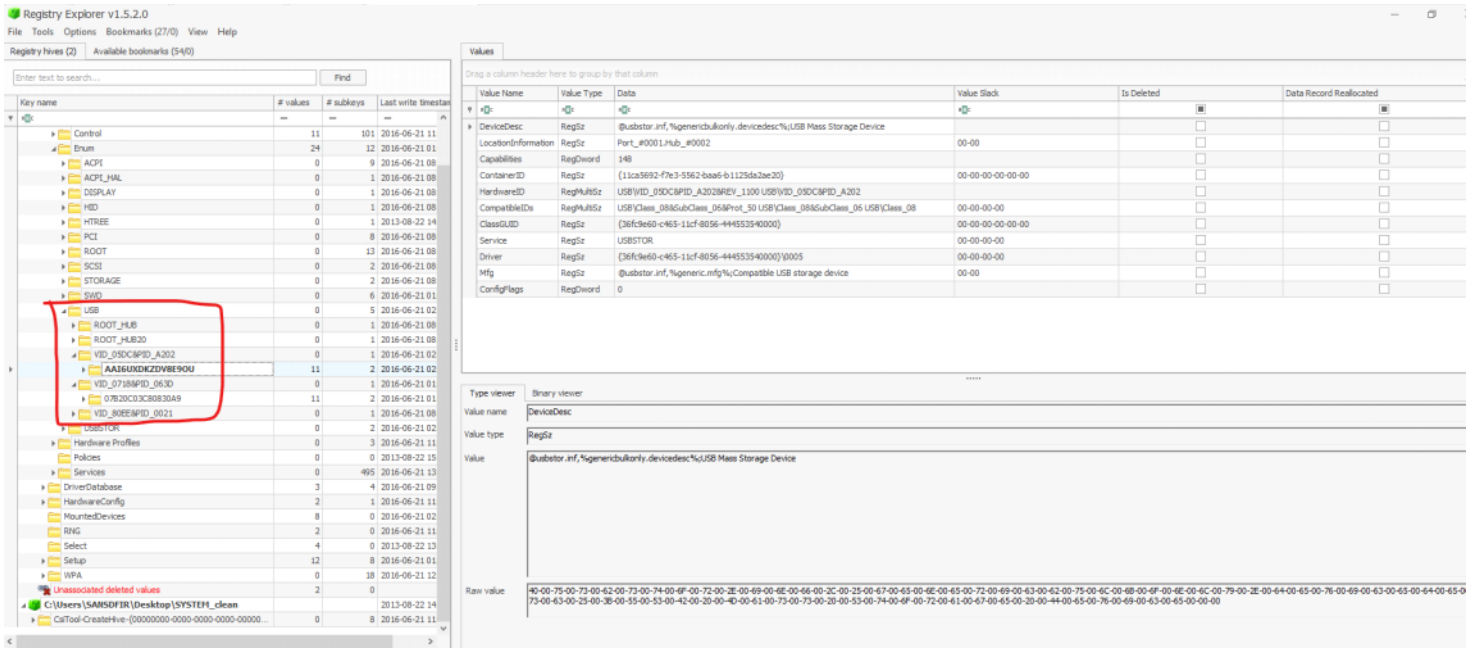
18. The user Documents' directory contained a PDF file discussing data exfiltration techniques. What is the name of the file?



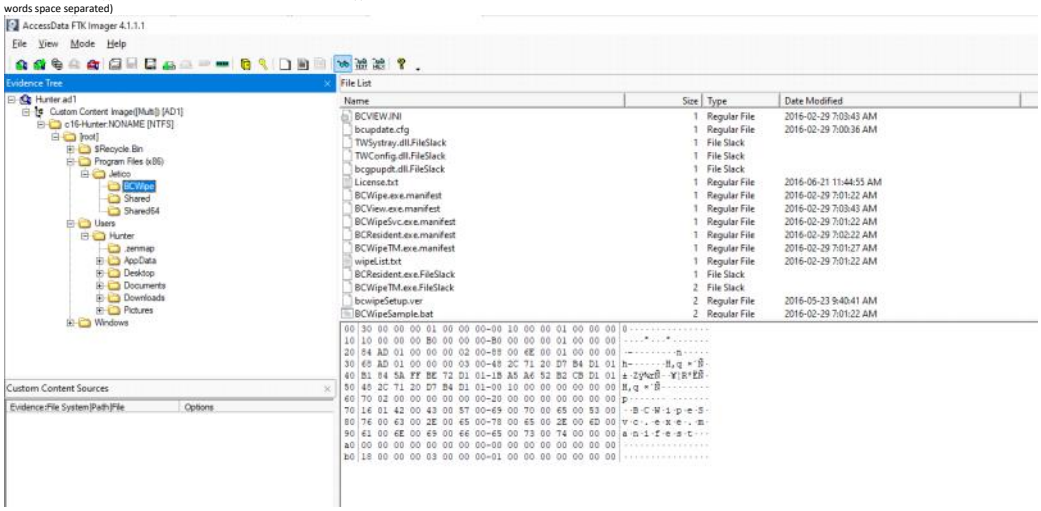
19. What was the name of the Disk Encryption application Installed on the victim system? (two words space separated)

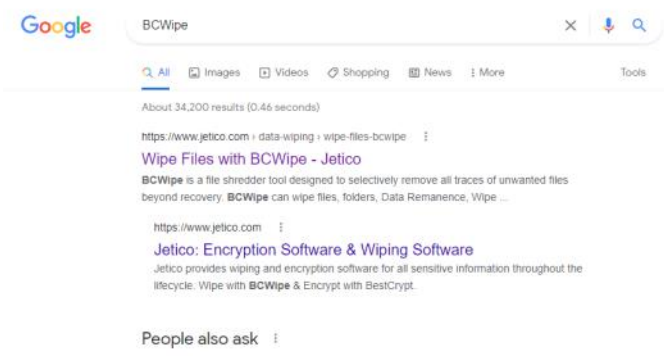


20. What are the serial numbers of the two identified USB storage?

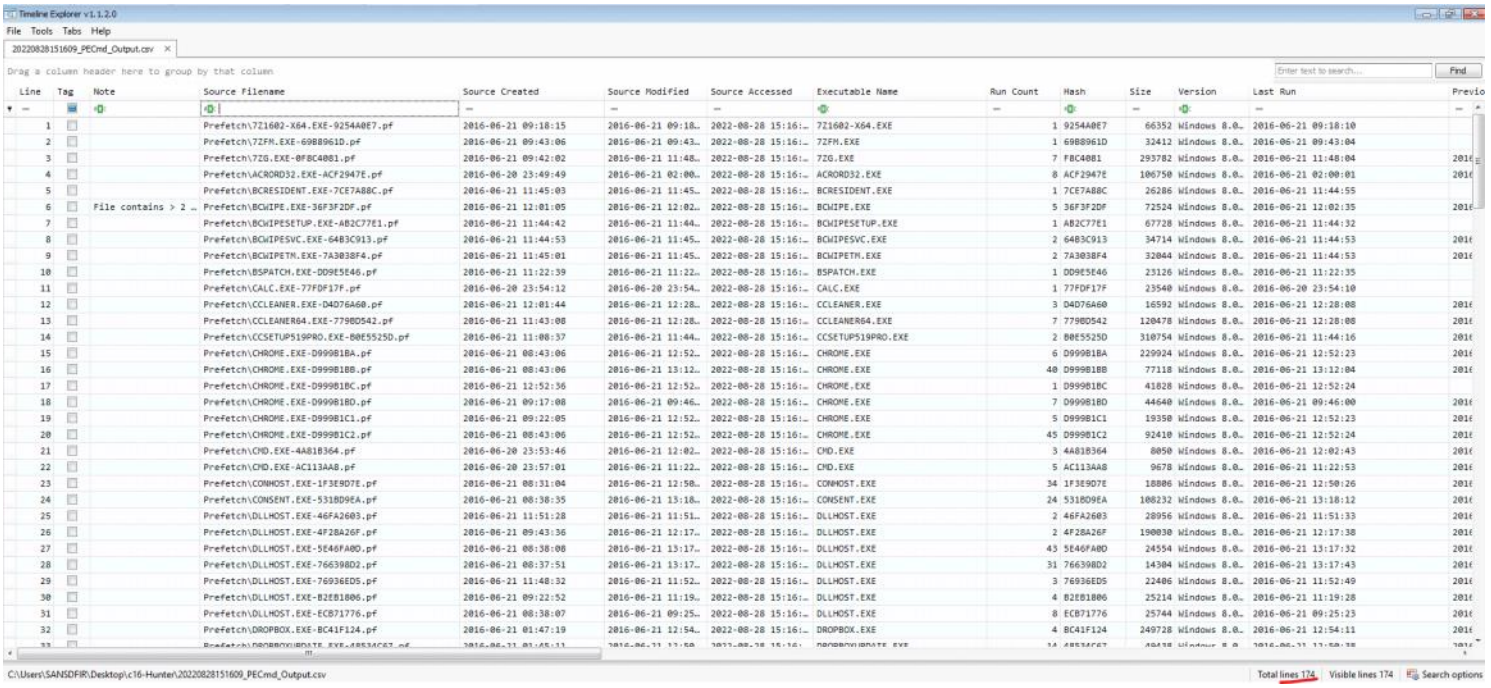


21. One of the installed applications is a file shredder. What is the name of the application? (two words space separated)

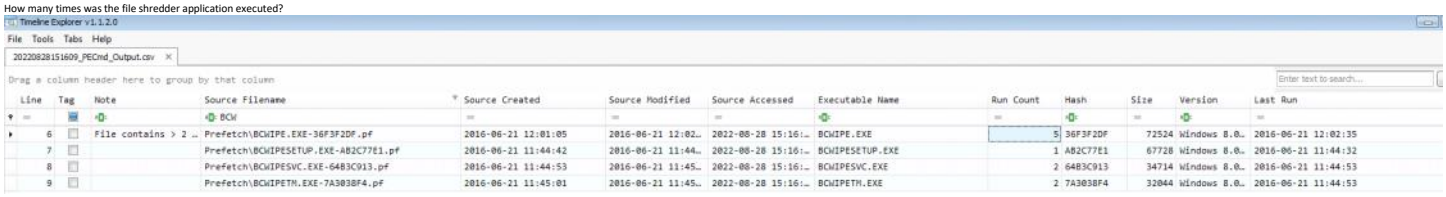




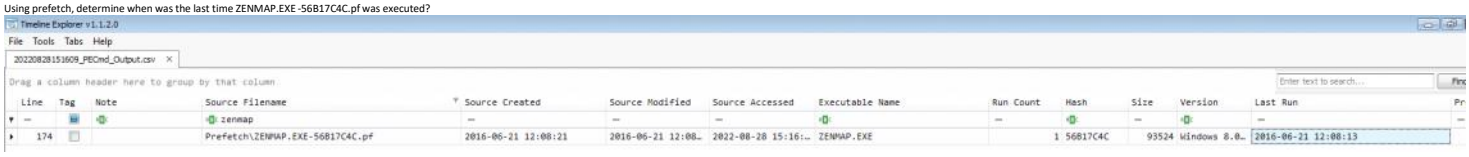
22. How many prefetch files were discovered on the system?



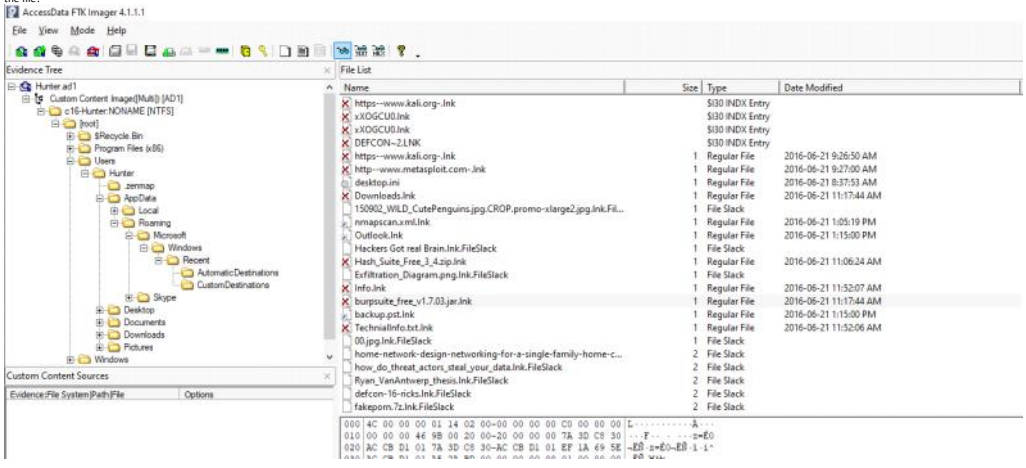
23. How many times was the file shredder application executed?



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

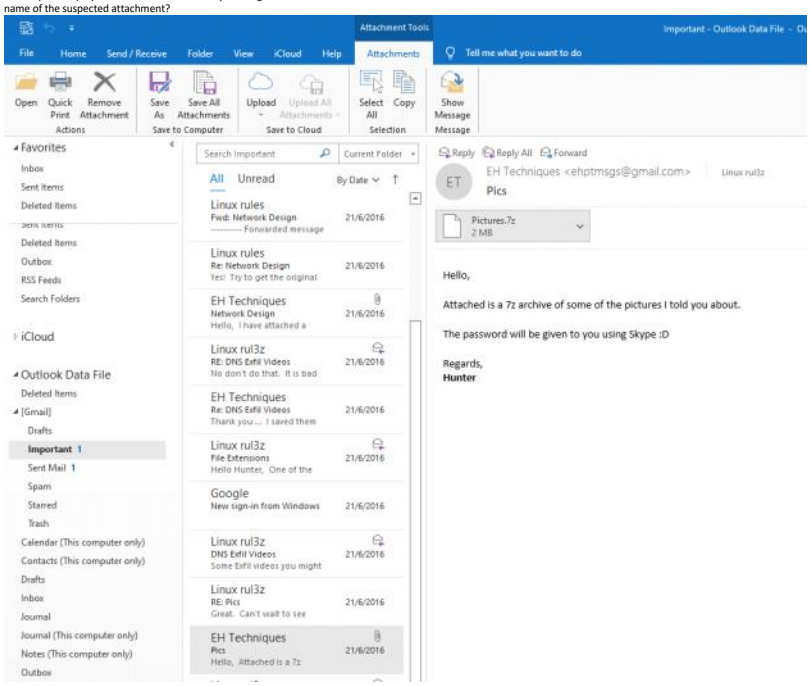


25. A JAR file for an offensive traffic manipulation tool was executed. What is the absolute path of the file?

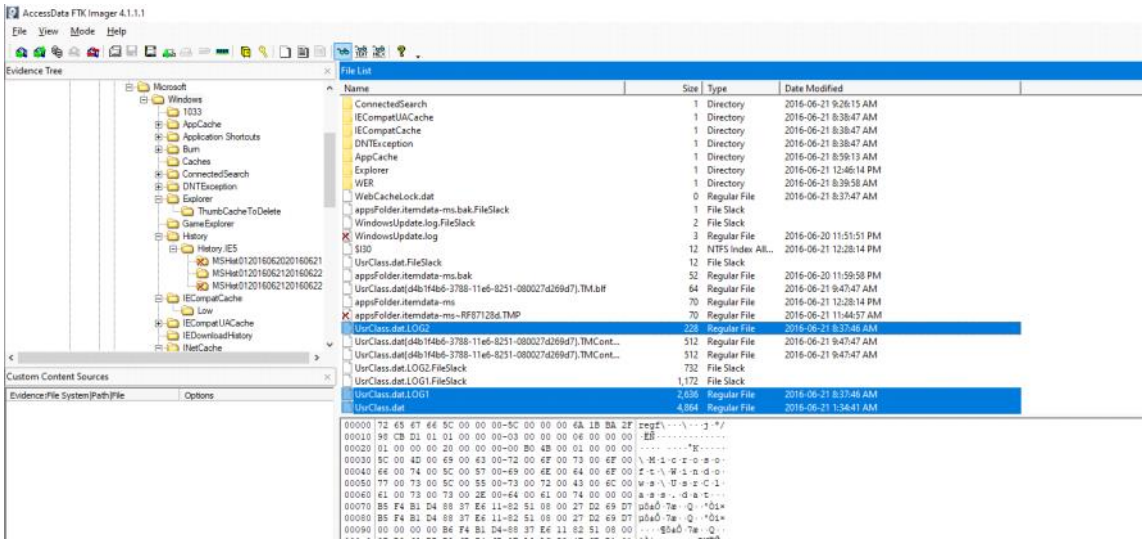


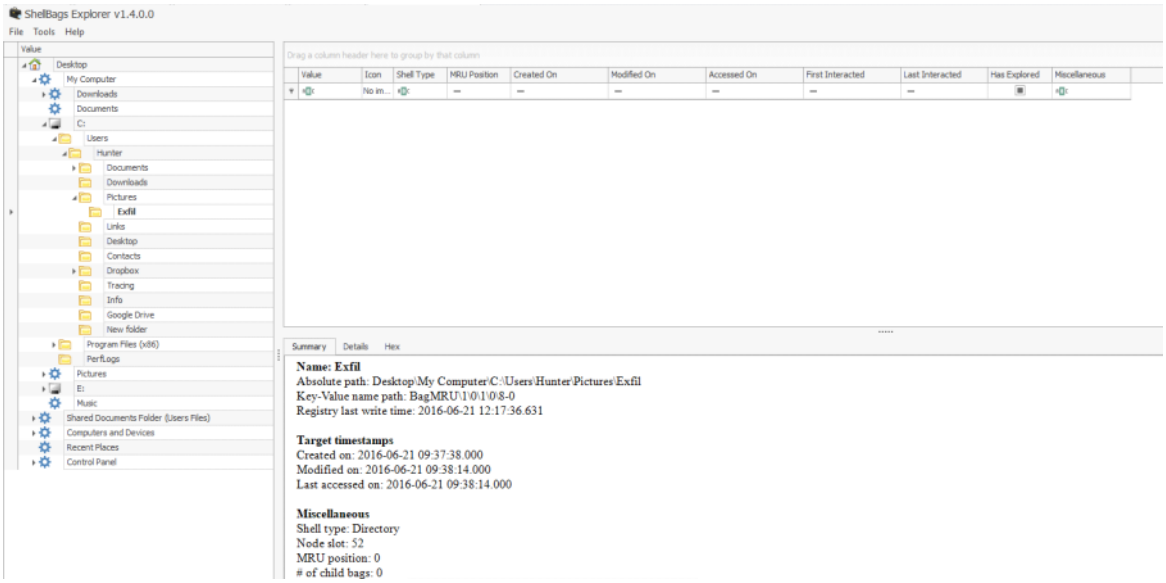
```
C:\Users\SANSDFIR\Desktop\c16-Hunter>clear
'clear' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\SANSDFIR\Desktop\c16-Hunter>LECmd -f burpsuite_free_v1.7.03.jar.lnk
LECmd version 1.4.0.0

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

Command line: -f burpsuite_free_v1.7.03.jar.lnk

Processing 'burpsuite_free_v1.7.03.jar.lnk'

Source file: C:\Users\SANSDFIR\Desktop\c16-Hunter\burpsuite_free_v1.7.03.jar.lnk
  Source created:  2016-06-21 11:17:44
  Source modified: 2016-06-21 11:17:44
  Source accessed: 2022-08-30 15:59:53

--- Header ---
  Target created:  2016-06-21 11:00:58
  Target modified: 2016-06-21 11:02:14
  Target accessed: 2016-06-21 11:00:58

  File size: 12,397,221
  Flags: HasTargetIdList, HasLinkInfo, HasRelativePath, HasWorkingDir, IsUnicode, DisableKnownFolderTracking
  File attributes: FileAttributeArchive
  Icon index: 0
  Show window: SwNormal (Activates and displays the window. The window is restored to its original size and position if the window is minimized or maximized.)

Relative Path: ..\..\..\..\..\Downloads\burpsuite_free_v1.7.03.jar
Working Directory: C:\Users\Hunter\Downloads

--- Link information ---
Flags: VolumeIdAndLocalBasePath, CommonNetworkRelativeLinkAndPathSuffix

>>Volume information
  Drive type: Fixed storage media (Hard drive)
  Serial number: 669B1B2A
  Label: (No label)

  Network share information
    Share name: \\4ORENSICS\Users
    Provider type: WnncNetLanman
    Share flags: ValidNetType
  -File ex burpsuite_free_v1.7.03.jar
```

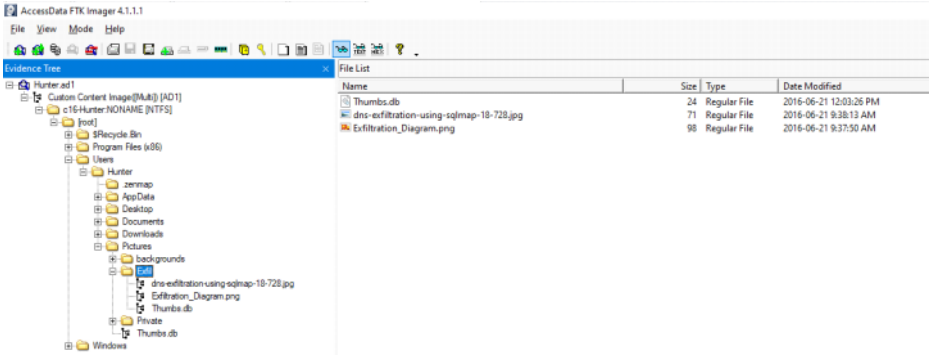
26. The suspect employee tried to exfiltrate data by sending it as an email attachment. What is the name of the suspected attachment?



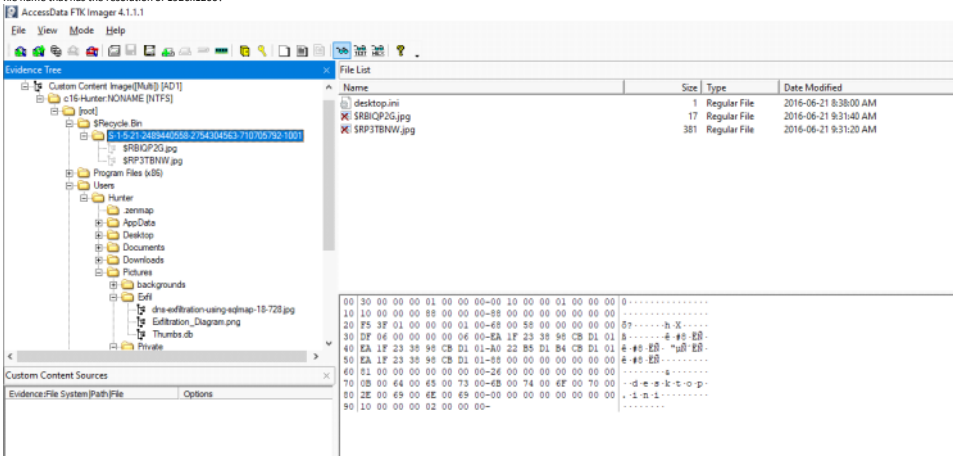
27. Shellbags shows that the employee created a folder to include all the data he will exfiltrate. What is the full path of that folder?

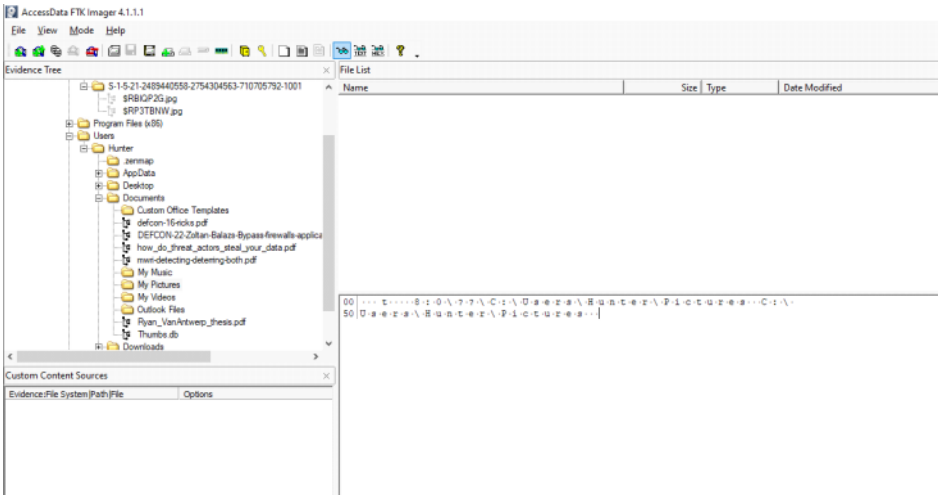


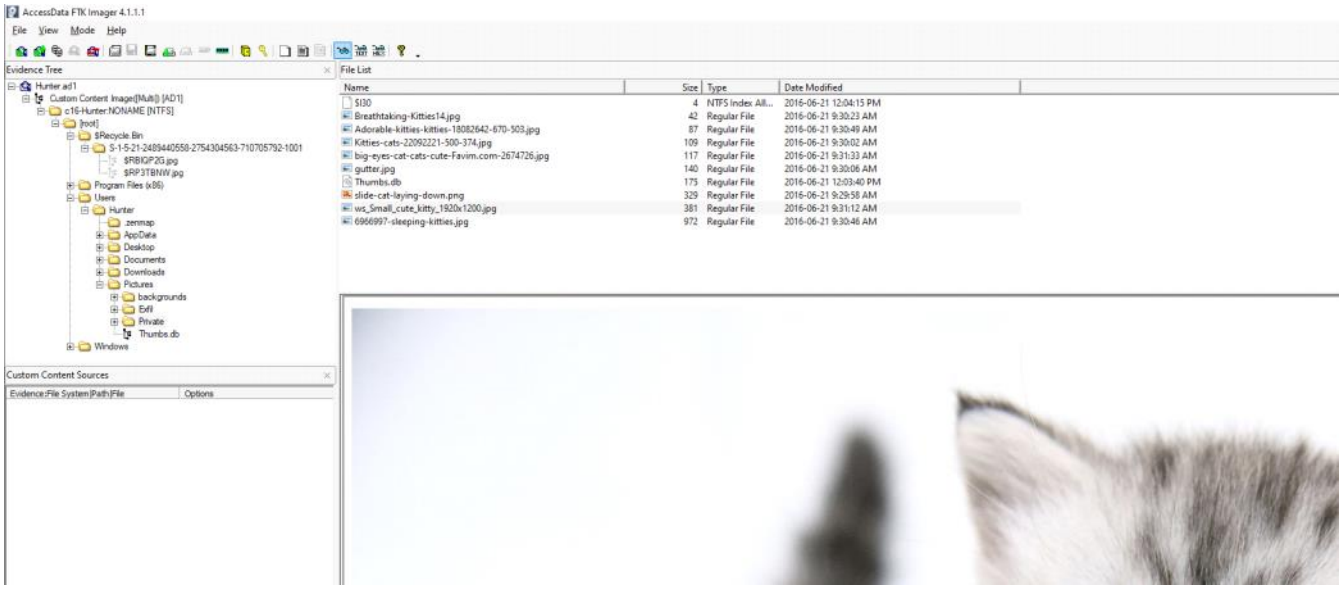


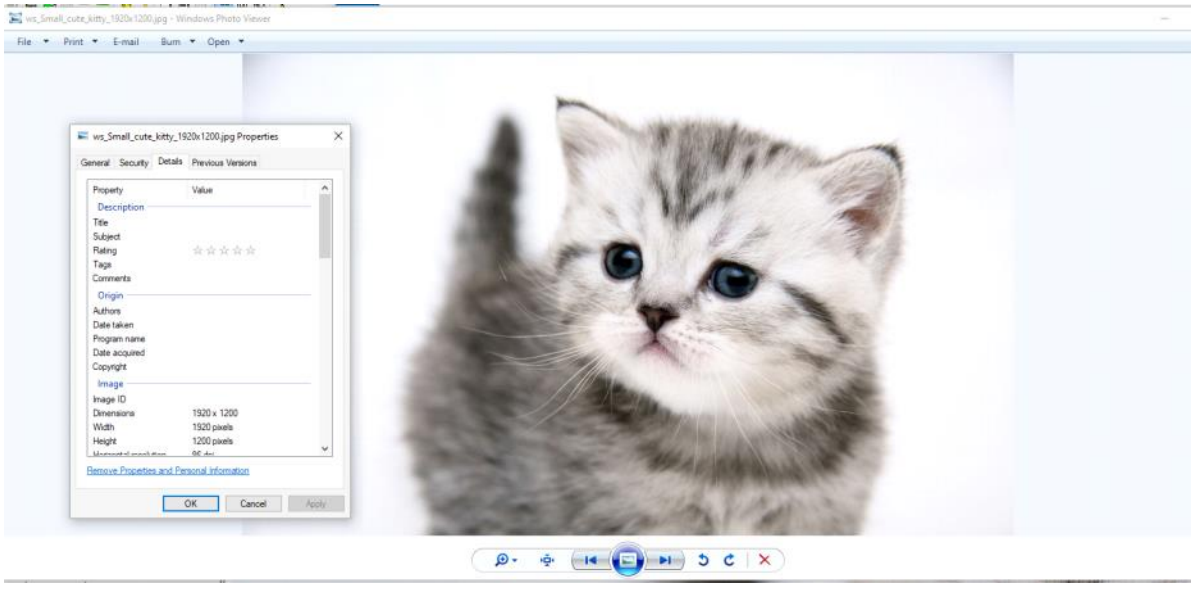


28. The user deleted two JPG files from the system and moved them to $Recycle -Bin. What is the file name that has the resolution of 1920x1200?

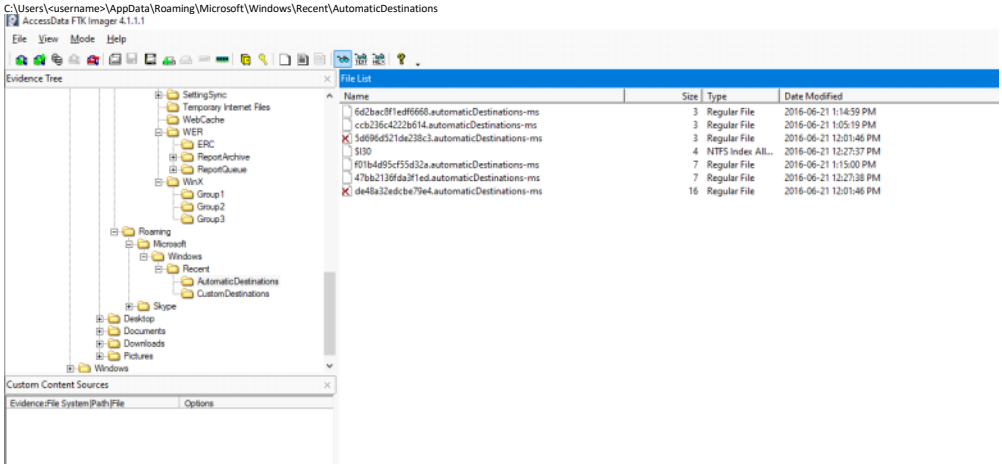




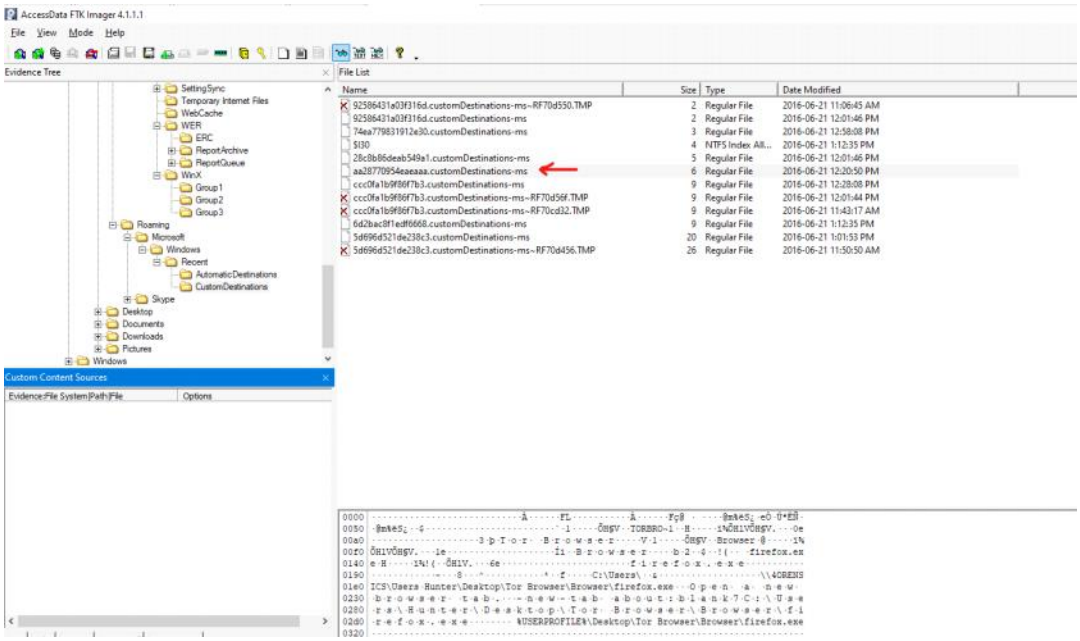


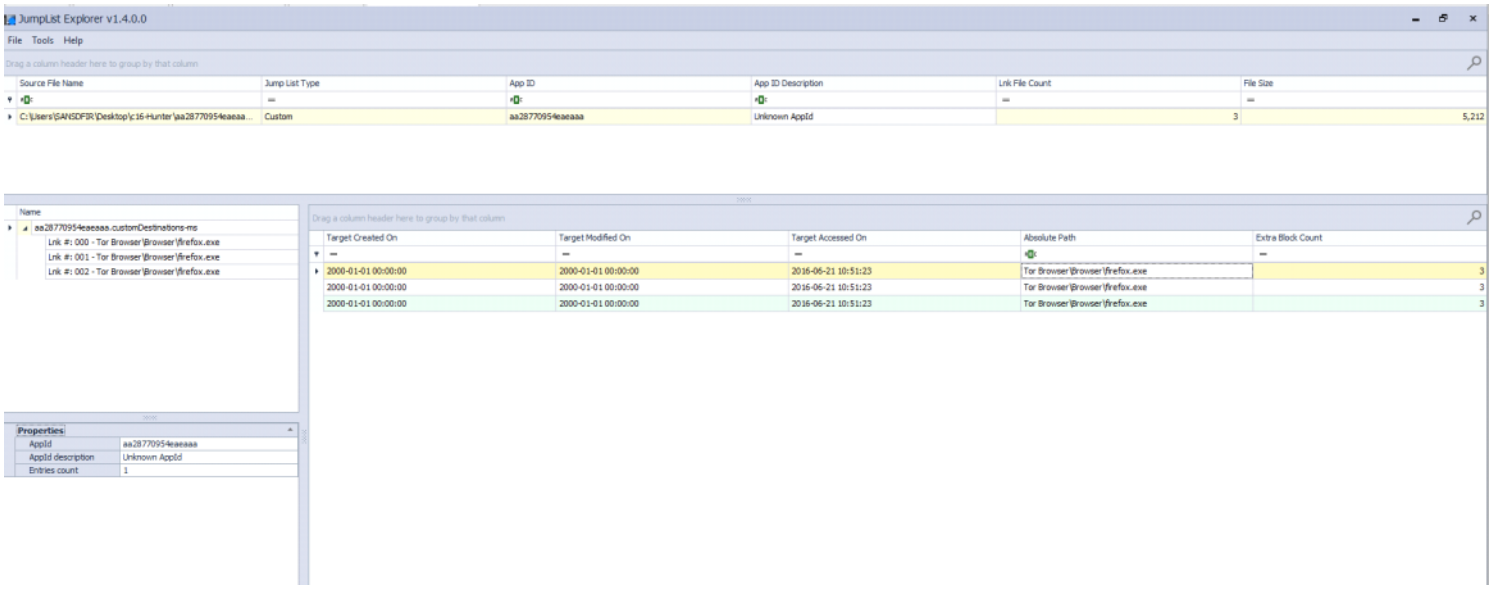


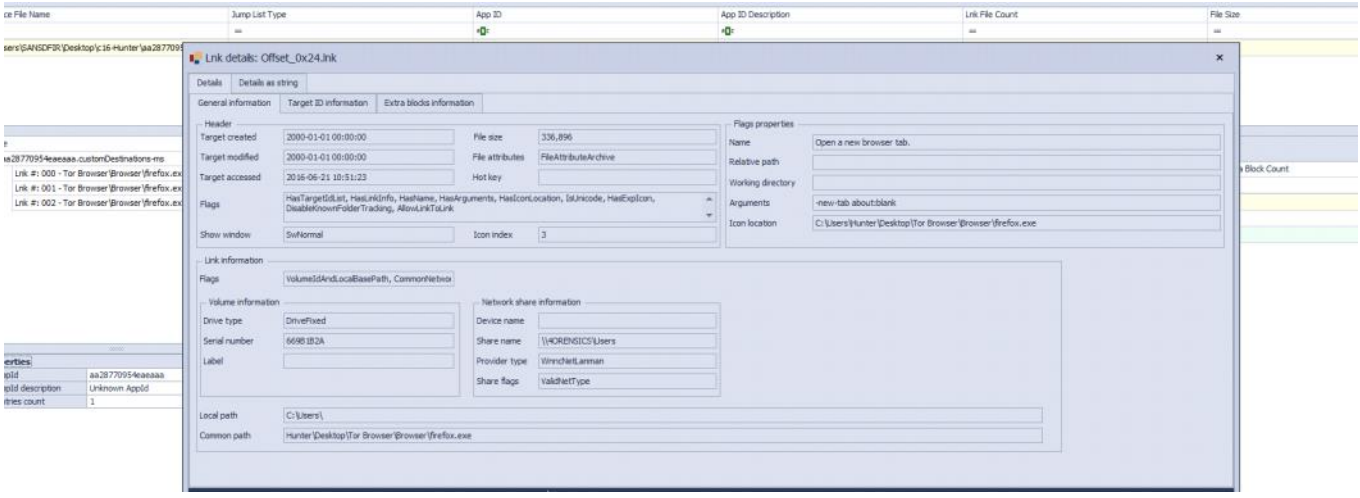
29. Provide the name of the directory where information about jump lists items (created automatically by the system) is stored?
C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations



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







References:

[https://forensafe.com/blogs/challenges/hunter.html]

https://www.turkhackteam.org/konular/hunter-cyberdefenders-lab-part-2.2016658/

https://medium.com/@OmarMohamed20/cyber-defenders-hunter-windows-disk-image-forensics-7219f92eefde