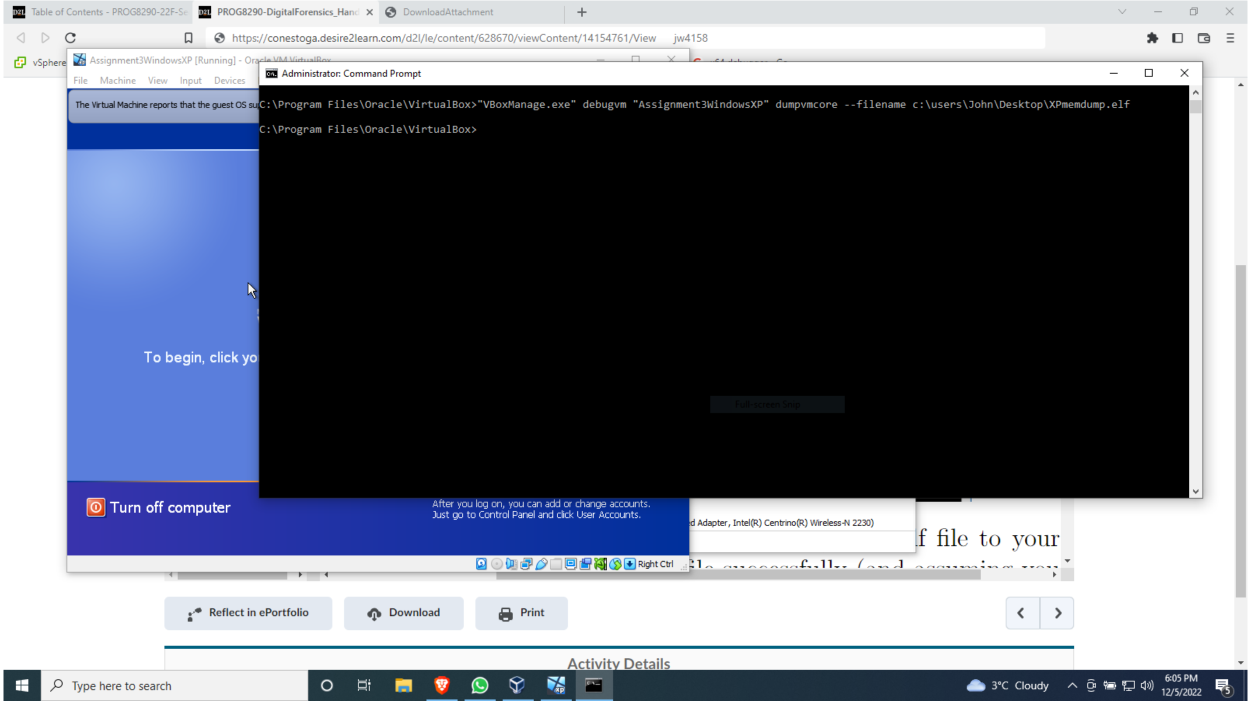
PROG8290 – Assignment 5 – John White (6714158)

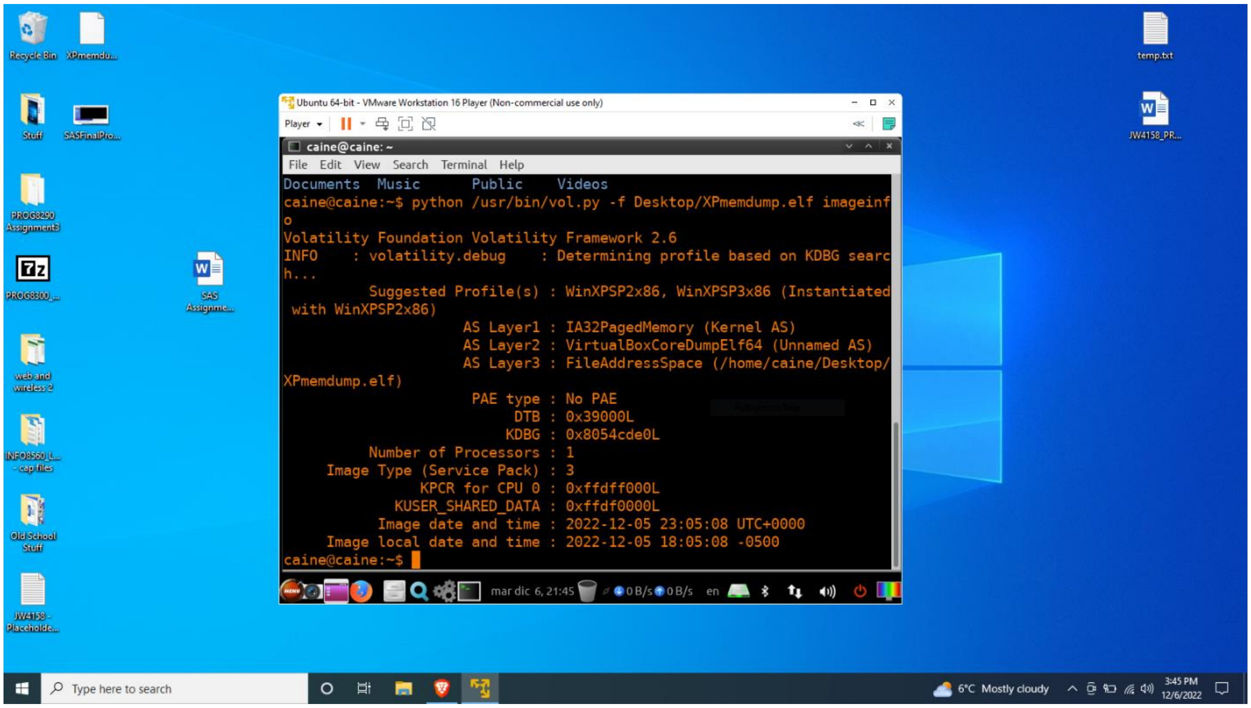
During this assignment, I had many problems with the installation of Caine. I ended up doing all of my work from the Live CD. I was originally using VMWare for the memory analysis because VirtualBox would not let my transfer my files via USB, and I was using VirtualBox for the image analysis because it's easier to attach multiple drives in VirtualBox.

Part 1 – Memory Collection


Administrator: Command Prompt
Assignment3WindowsXP [Running] - Oracle VM VirtualBox
File Machine View Input Devices
To begin, click yo
Turn off computer
After you log on, you can add or change accounts.
Just go to Control Panel and click User Accounts.
Reflect in ePortfolio
Download
Print
Activity Details
Type here to search
3°C Cloudy
6:05 PM
12/5/2022

```
C:\Program Files\Oracle\VirtualBox>"VBoxManage.exe" debugvm "Assignment3WindowsXP" dumpvmcore --filename c:\users\John\Desktop\XPmemdump.elf

C:\Program Files\Oracle\VirtualBox>
```

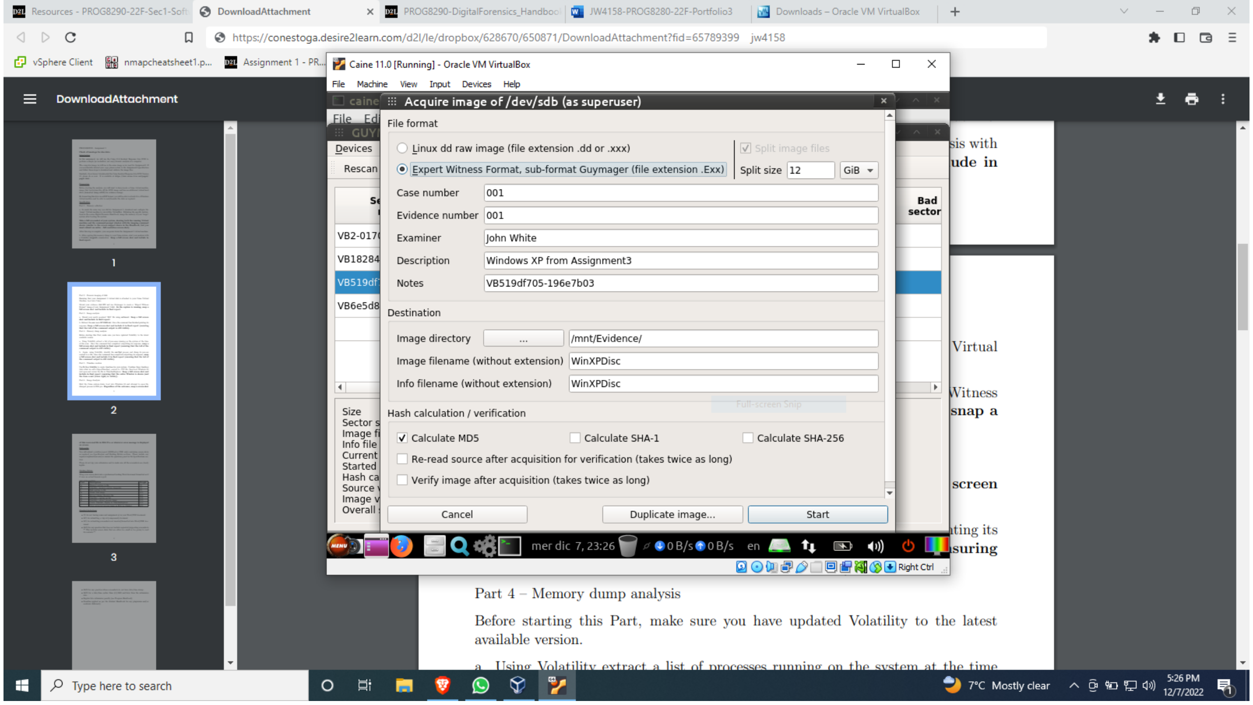
Figure 1.1 – Capturing the memory dump of the XP VM into a .elf file.



```
caine@caine: ~
Documents  Music      Public    Videos
caine@caine:~$ python /usr/bin/vol.py -f Desktop/XPmemdump.elf imageinf
o
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG searc
h...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated
 with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : VirtualBoxCoreDumpElf64 (Unnamed AS)
                     AS Layer3 : FileAddressSpace (/home/caine/Desktop/
XPmemdump.elf)
                      PAE type : No PAE
                           DTB : 0x39000L
                          KDBG : 0x8054cde0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2022-12-05 23:05:08 UTC+0000
     Image local date and time : 2022-12-05 18:05:08 -0500
caine@caine:~$
```

Figure 1.2 – Using Volatility to display the ImageInfo of the .elf file.

Part 2 – Forensic imaging of disc



Acquire image of /dev/sdb (as superuser)

File format
- ○ Linux dd raw image (file extension .dd or .xxx)
- ● Expert Witness Format, sub-format Guymager (file extension .Exx)
- ☑ Split image files — Split size 12 GiB

Case number	001
Evidence number	001
Examiner	John White
Description	Windows XP from Assignment3
Notes	VB519df705-196e7b03

Destination

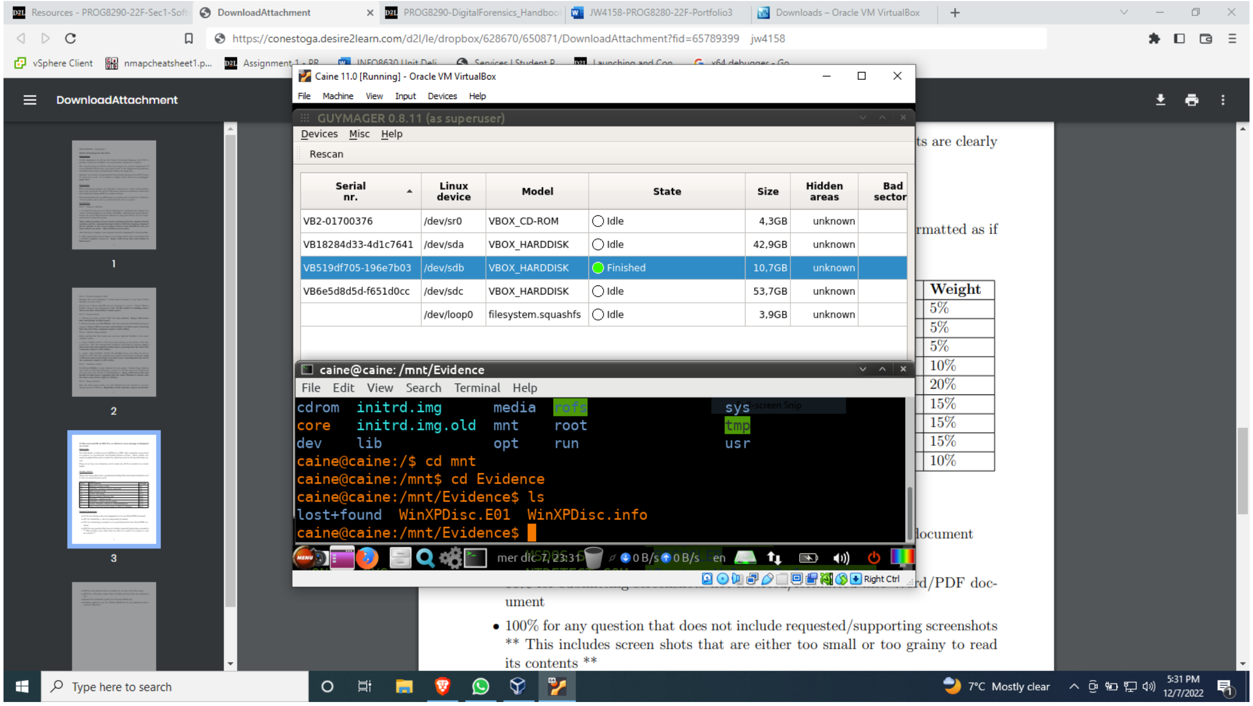
Image directory	/mnt/Evidence/
Image filename (without extension)	WinXPDisc
Info filename (without extension)	WinXPDisc

Hash calculation / verification
- ☑ Calculate MD5
- □ Calculate SHA-1
- □ Calculate SHA-256
- □ Re-read source after acquisition for verification (takes twice as long)
- □ Verify image after acquisition (takes twice as long)

Part 4 – Memory dump analysis

Before starting this Part, make sure you have updated Volatility to the latest available version.

Figure 2.1 – Guymager Expert Witness Format Settings.



GUYMAGER 0.8.11 (as superuser)

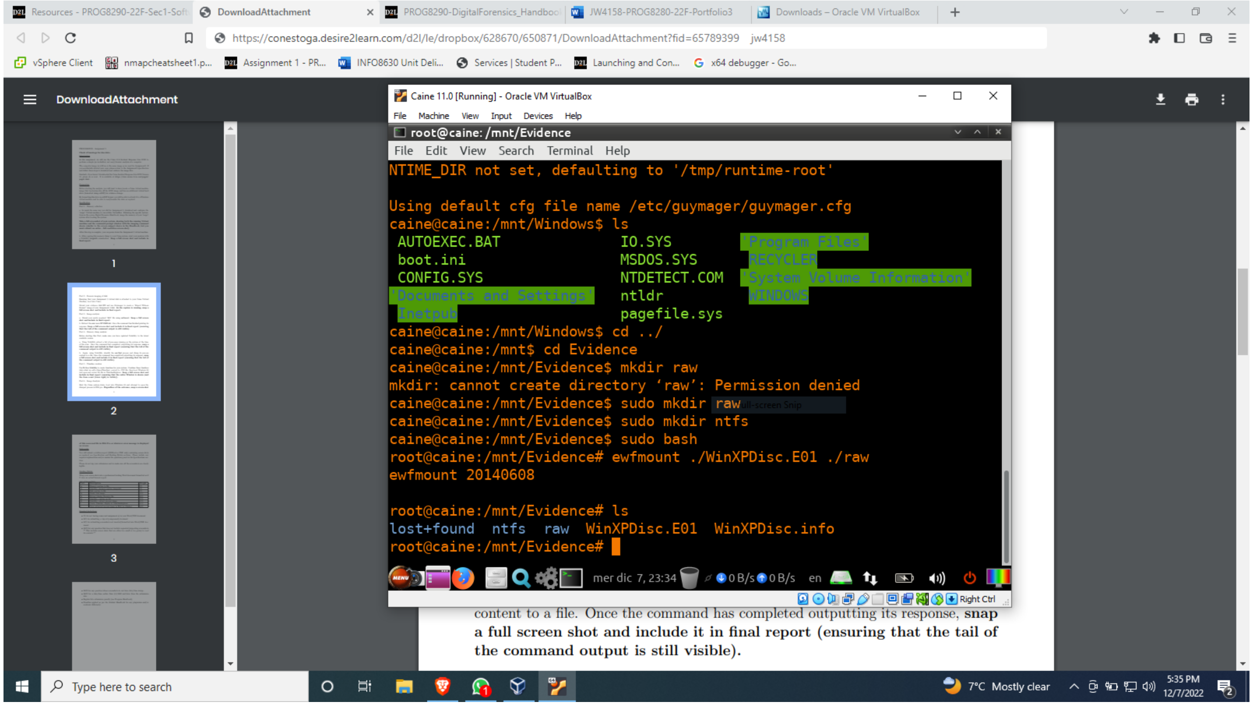
Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sector
VB2-01700376	/dev/sr0	VBOX_CD-ROM	○ Idle	4,3GB	unknown	
VB18284d33-4d1c7641	/dev/sda	VBOX_HARDDISK	○ Idle	42,9GB	unknown	
VB519df705-196e7b03	/dev/sdb	VBOX_HARDDISK	● Finished	10,7GB	unknown	
VB6e5d8d5d-f651d0cc	/dev/sdc	VBOX_HARDDISK	○ Idle	53,7GB	unknown	
	/dev/loop0	filesystem.squashfs	○ Idle	3,9GB	unknown	

```
cdrom  initrd.img      media  rofs          sys
core   initrd.img.old  mnt    root          tmp
dev    lib             opt    run           usr
caine@caine:/$ cd mnt
caine@caine:/mnt$ cd Evidence
caine@caine:/mnt/Evidence$ ls
lost+found  WinXPDisc.E01  WinXPDisc.info
caine@caine:/mnt/Evidence$
```

- 100% for any question that does not include requested/supporting screenshots ** This includes screen shots that are either too small or too grainy to read its contents **

Figure 2.2 - .E01 file successfully created with Guymager.

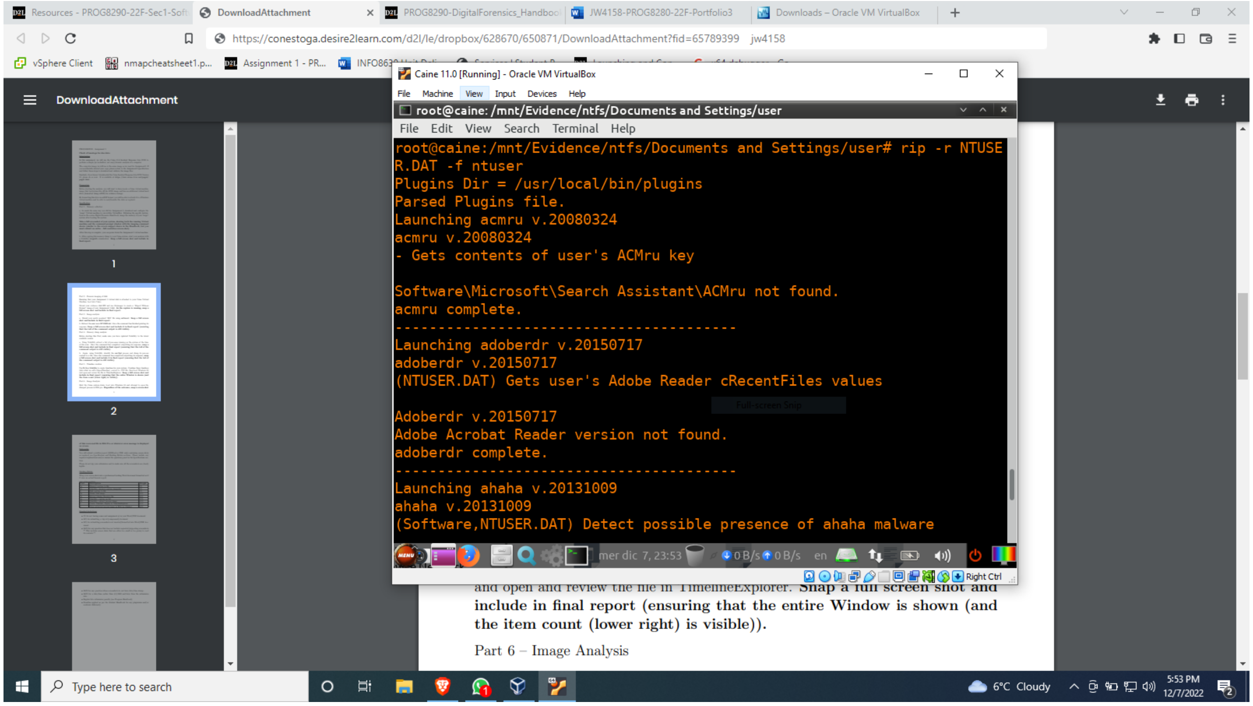
Part 3 – Image Analysis



```
NTIME_DIR not set, defaulting to '/tmp/runtime-root'

Using default cfg file name /etc/guymager/guymager.cfg
caine@caine:/mnt/Windows$ ls
 AUTOEXEC.BAT                IO.SYS         'Program Files'
 boot.ini                    MSDOS.SYS       RECYCLER
 CONFIG.SYS                  NTDETECT.COM   'System Volume Information'
'Documents and Settings'     ntldr           WINDOWS
 Inetpub                     pagefile.sys
caine@caine:/mnt/Windows$ cd ../
caine@caine:/mnt$ cd Evidence
caine@caine:/mnt/Evidence$ mkdir raw
mkdir: cannot create directory ‘raw’: Permission denied
caine@caine:/mnt/Evidence$ sudo mkdir raw
caine@caine:/mnt/Evidence$ sudo mkdir ntfs
caine@caine:/mnt/Evidence$ sudo bash
root@caine:/mnt/Evidence# ewfmount ./WinXPDisc.E01 ./raw
ewfmount 20140608

root@caine:/mnt/Evidence# ls
lost+found  ntfs  raw  WinXPDisc.E01  WinXPDisc.info
root@caine:/mnt/Evidence#
```

content to a file. Once the command has completed outputting its response, snap a full screen shot and include it in final report (ensuring that the tail of the command output is still visible).

Figure 3.1 – Using ewfmount to mount the .E01 file to /raw.



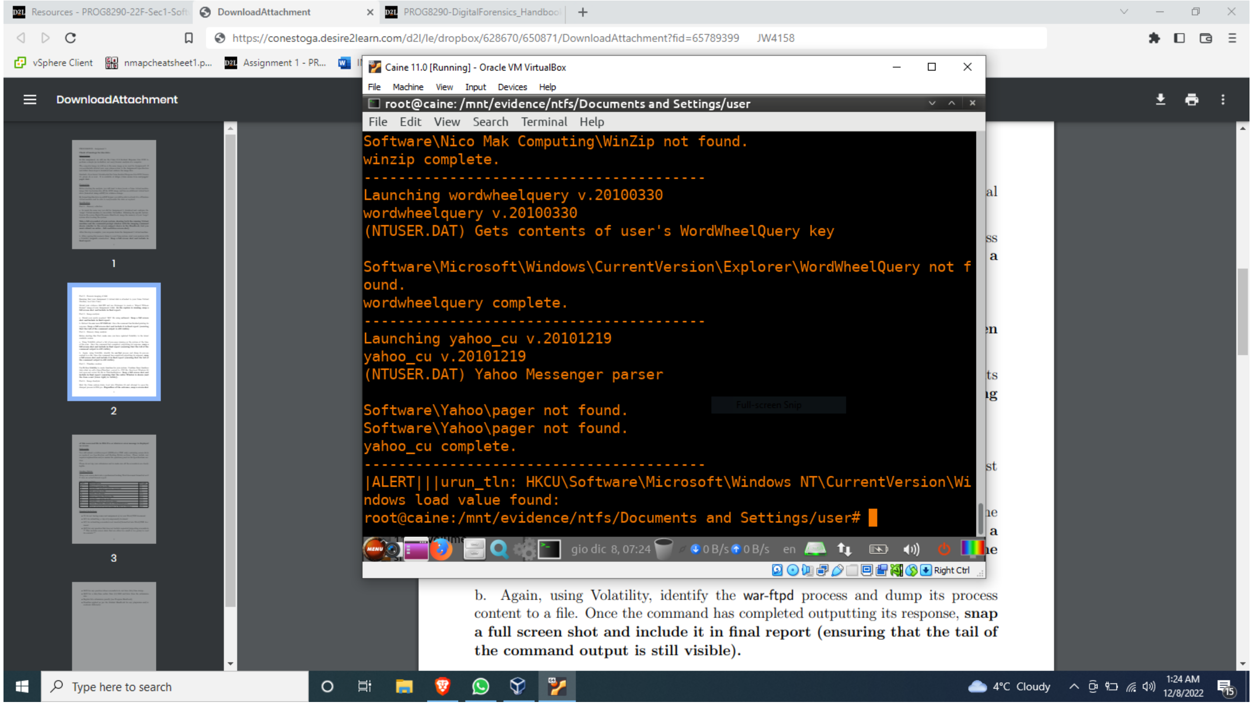
Caine 11.0 [Running] - Oracle VM VirtualBox
root@caine: /mnt/Evidence/ntfs/Documents and Settings/user
DownloadAttachment
https://conestoga.desire2learn.com/d2l/le/dropbox/628670/650871/DownloadAttachment?fid=65789399
Type here to search
6°C Cloudy
5:53 PM
12/7/2022

```
root@caine:/mnt/Evidence/ntfs/Documents and Settings/user# rip -r NTUSE
R.DAT -f ntuser
Plugins Dir = /usr/local/bin/plugins
Parsed Plugins file.
Launching acmru v.20080324
acmru v.20080324
- Gets contents of user's ACMru key

Software\Microsoft\Search Assistant\ACMru not found.
acmru complete.
----------------------------------------
Launching adoberdr v.20150717
adoberdr v.20150717
(NTUSER.DAT) Gets user's Adobe Reader cRecentFiles values

Adoberdr v.20150717
Adobe Acrobat Reader version not found.
adoberdr complete.
----------------------------------------
Launching ahaha v.20131009
ahaha v.20131009
(Software,NTUSER.DAT) Detect possible presence of ahaha malware
```

and open and review the file in TimelineExplorer. **Snap a full screen shot and include in final report (ensuring that the entire Window is shown (and the item count (lower right) is visible)).**

Part 6 – Image Analysis

Figure 3.2 – Using rip to acquire the user data from NTUSER.DAT.



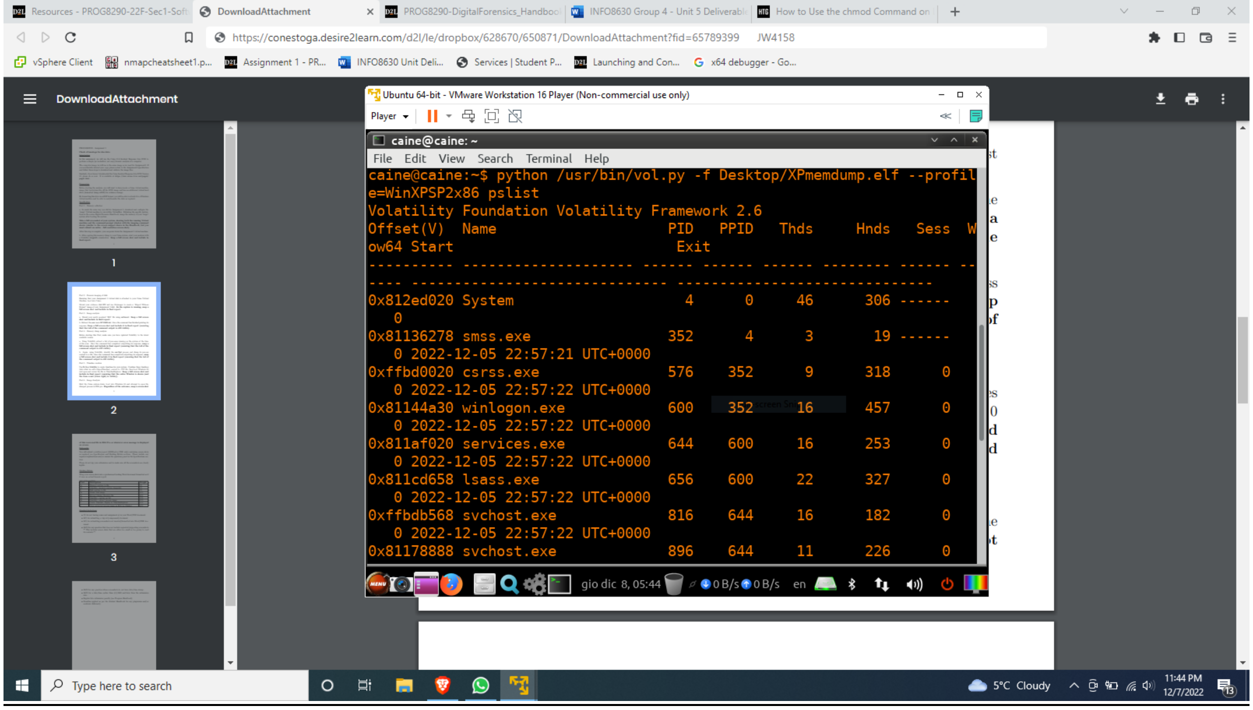
Caine 11.0 [Running] - Oracle VM VirtualBox
root@caine: /mnt/evidence/ntfs/Documents and Settings/user
DownloadAttachment
https://conestoga.desire2learn.com/d2l/le/dropbox/628670/650871/DownloadAttachment?fid=65789399
Type here to search
4°C Cloudy
1:24 AM
12/8/2022

```
Software\Nico Mak Computing\WinZip not found.
winzip complete.
----------------------------------------
Launching wordwheelquery v.20100330
wordwheelquery v.20100330
(NTUSER.DAT) Gets contents of user's WordWheelQuery key

Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery not f
ound.
wordwheelquery complete.
----------------------------------------
Launching yahoo_cu v.20101219
yahoo_cu v.20101219
(NTUSER.DAT) Yahoo Messenger parser

Software\Yahoo\pager not found.
Software\Yahoo\pager not found.
yahoo_cu complete.
----------------------------------------
|ALERT|||urun_tln: HKCU\Software\Microsoft\Windows NT\CurrentVersion\Wi
ndows load value found:
root@caine:/mnt/evidence/ntfs/Documents and Settings/user#
```

b. Again, using Volatility, identify the war-ftpd process and dump its process content to a file. Once the command has completed outputting its response, **snap a full screen shot and include it in final report (ensuring that the tail of the command output is still visible).**

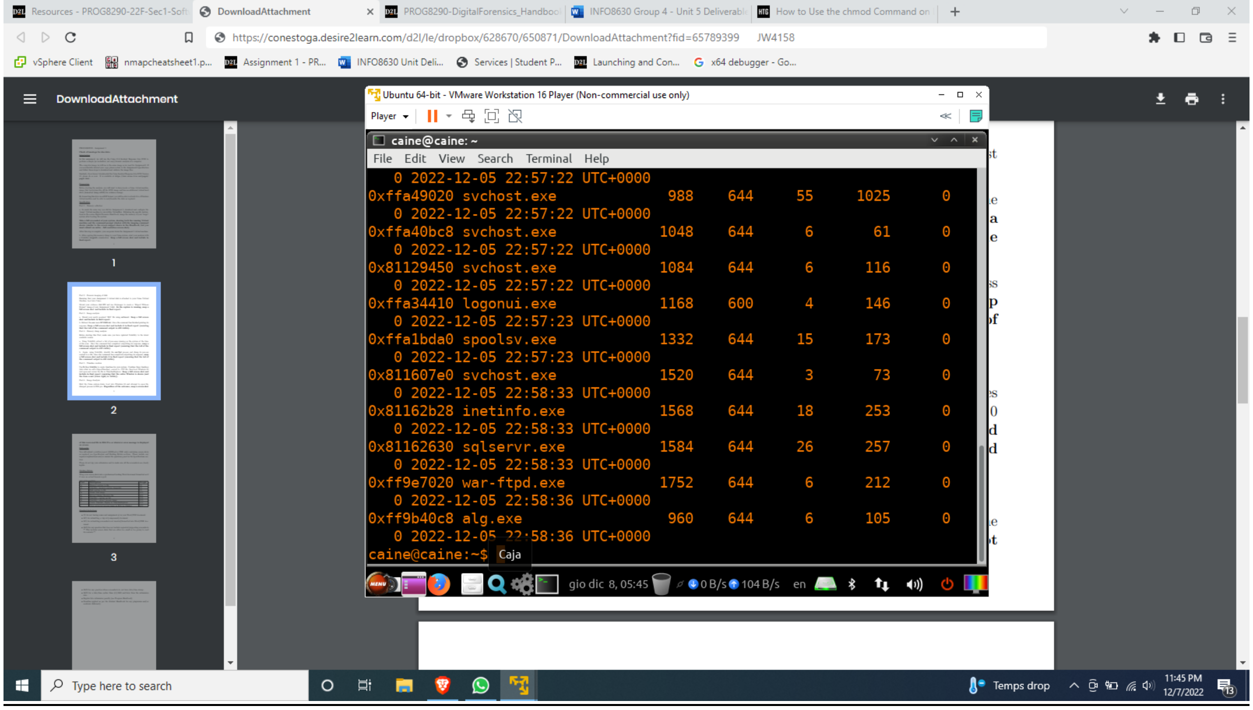
Figure 3.3 – Tail end of the rip command used on NTUSER.DAT.

Part 4 – Memory dump analysis


Ubuntu 64-bit - VMware Workstation 16 Player (Non-commercial use only)
caine@caine: ~
File Edit View Search Terminal Help
DownloadAttachment
https://conestoga.desire2learn.com/d2l/le/dropbox/628670/650871/DownloadAttachment?fid=65789399
gio dic 8, 05:44
Type here to search
5°C Cloudy
11:44 PM
12/7/2022

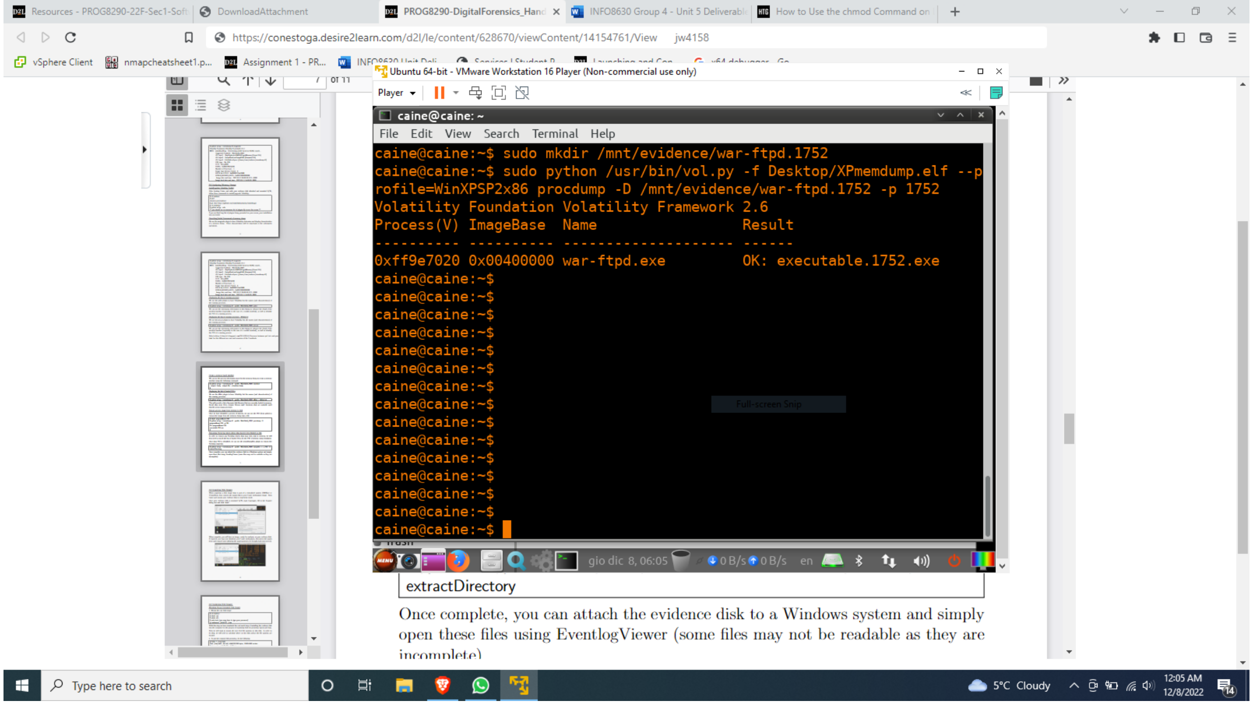
```
caine@caine:~$ python /usr/bin/vol.py -f Desktop/XPmemdump.elf --profil
e=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  W
ow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ --
---- ------------------------------ ------------------------------
0x812ed020 System                    4      0     46      306 ------
     0
0x81136278 smss.exe                352      4      3       19 ------
     0 2022-12-05 22:57:21 UTC+0000
0xffbd0020 csrss.exe               576    352      9      318      0
     0 2022-12-05 22:57:22 UTC+0000
0x81144a30 winlogon.exe            600    352     16      457      0
     0 2022-12-05 22:57:22 UTC+0000
0x811af020 services.exe            644    600     16      253      0
     0 2022-12-05 22:57:22 UTC+0000
0x811cd658 lsass.exe               656    600     22      327      0
     0 2022-12-05 22:57:22 UTC+0000
0xffbdb568 svchost.exe             816    644     16      182      0
     0 2022-12-05 22:57:22 UTC+0000
0x81178888 svchost.exe             896    644     11      226      0
```

Figure 4.1 – Beginning of the list of processes running when the XP VM was scanned.


Ubuntu 64-bit - VMware Workstation 16 Player (Non-commercial use only)
caine@caine: ~
File Edit View Search Terminal Help
DownloadAttachment
https://conestoga.desire2learn.com/d2l/le/dropbox/628670/650871/DownloadAttachment?fid=65789399
gio dic 8, 05:45
Type here to search
Temps drop
11:45 PM
12/7/2022

```
     0 2022-12-05 22:57:22 UTC+0000
0xffa49020 svchost.exe             988    644     55     1025      0
     0 2022-12-05 22:57:22 UTC+0000
0xffa40bc8 svchost.exe            1048    644      6       61      0
     0 2022-12-05 22:57:22 UTC+0000
0x81129450 svchost.exe            1084    644      6      116      0
     0 2022-12-05 22:57:22 UTC+0000
0xffa34410 logonui.exe            1168    600      4      146      0
     0 2022-12-05 22:57:23 UTC+0000
0xffa1bda0 spoolsv.exe            1332    644     15      173      0
     0 2022-12-05 22:57:23 UTC+0000
0x811607e0 svchost.exe            1520    644      3       73      0
     0 2022-12-05 22:58:33 UTC+0000
0x81162b28 inetinfo.exe           1568    644     18      253      0
     0 2022-12-05 22:58:33 UTC+0000
0x81162630 sqlservr.exe           1584    644     26      257      0
     0 2022-12-05 22:58:33 UTC+0000
0xff9e7020 war-ftpd.exe           1752    644      6      212      0
     0 2022-12-05 22:58:36 UTC+0000
0xff9b40c8 alg.exe                 960    644      6      105      0
     0 2022-12-05 22:58:36 UTC+0000
caine@caine:~$
```

Figure 4.2 – End of the list of processes running when the XP VM was scanned.


Ubuntu 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player
caine@caine: ~
File Edit View Search Terminal Help
https://conestoga.desire2learn.com/d2l/le/content/628670/viewContent/14154761/View
Type here to search
5°C Cloudy
12:05 AM
12/8/2022

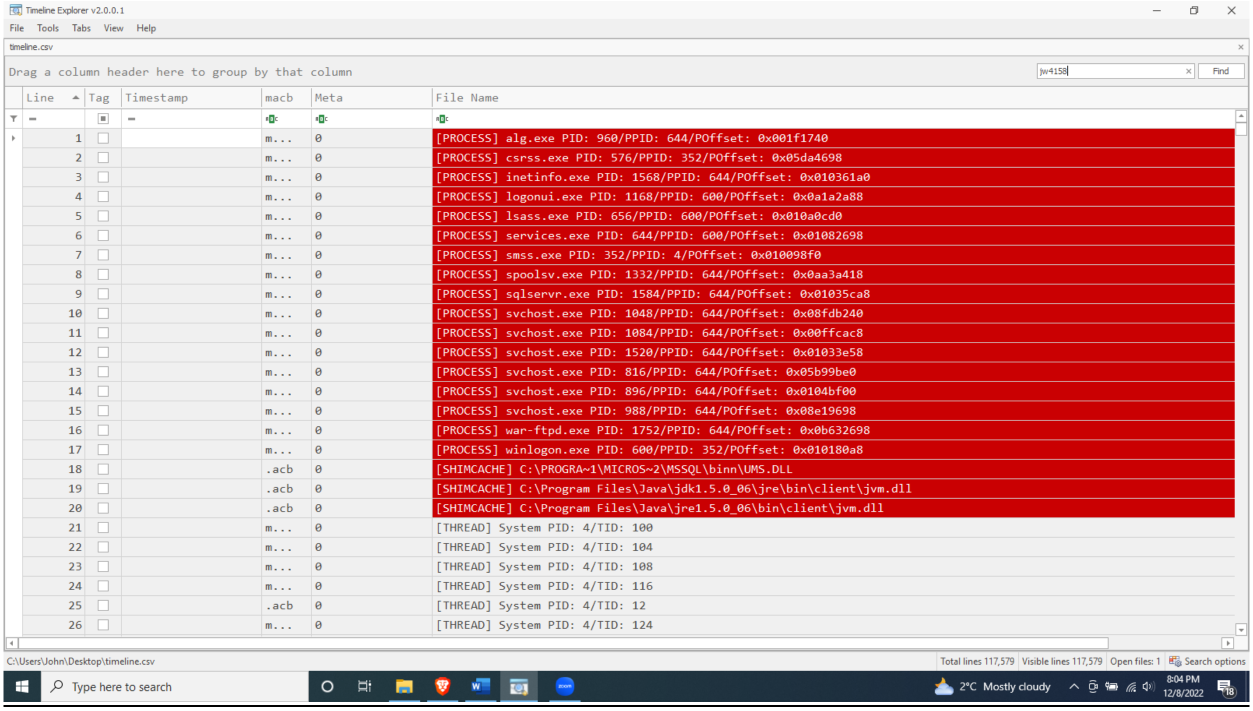
```
caine@caine:~$ sudo mkdir /mnt/evidence/war-ftpd.1752
caine@caine:~$ sudo python /usr/bin/vol.py -f Desktop/XPmemdump.elf --p
rofile=WinXPSP2x86 procdump -D /mnt/evidence/war-ftpd.1752 -p 1752
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0xff9e7020 0x00400000 war-ftpd.exe         OK: executable.1752.exe
caine@caine:~$
caine@caine:~$
caine@caine:~$
caine@caine:~$
caine@caine:~$
caine@caine:~$
caine@caine:~$
caine@caine:~$
caine@caine:~$
caine@caine:~$
caine@caine:~$
caine@caine:~$
caine@caine:~$
caine@caine:~$
caine@caine:~$
```

extractDirectory

Once complete, you can attach the evidence disk to a Windows system and simply open these files using EventlogViewer (some files may not be readable as they are incomplete)

Figure 4.3 – The war-ftpd process was exported to a .exe file.

Part 5 – Creating a timeline



Timeline Explorer v2.0.0.1

timeline.csv

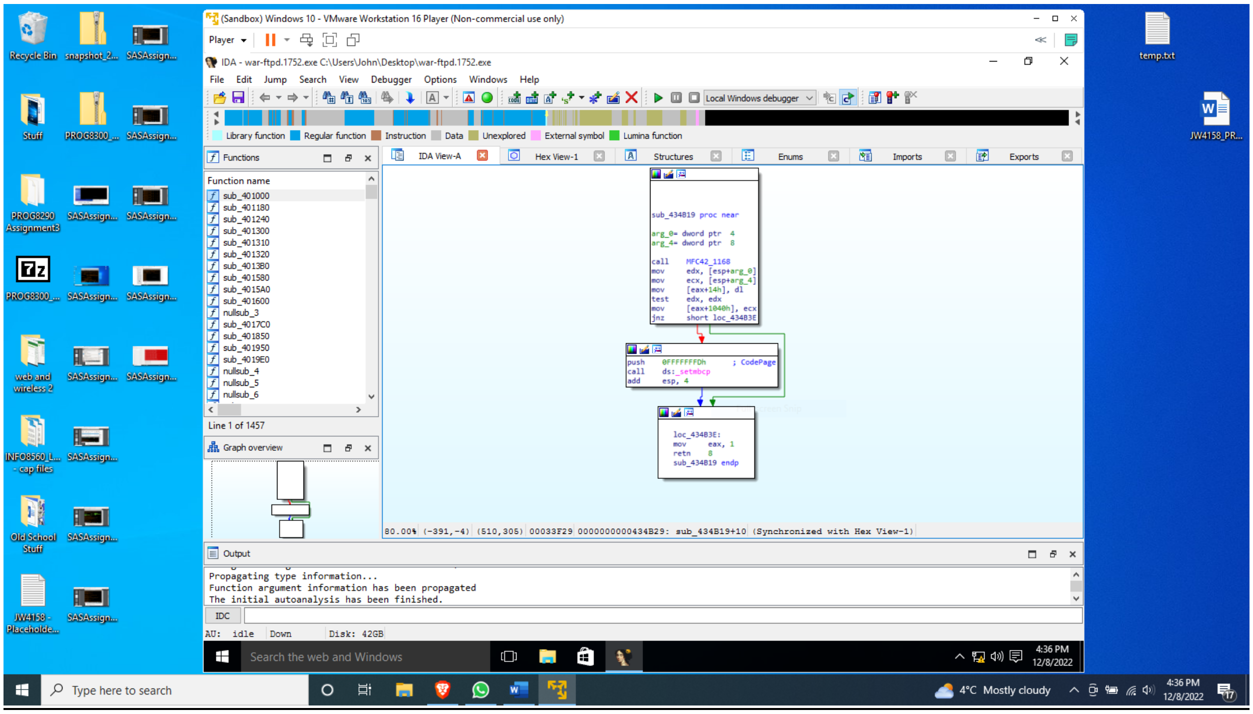
Drag a column header here to group by that column

Line	Tag	Timestamp	macb	Meta	File Name
1	□		m...	0	[PROCESS] alg.exe PID: 960/PPID: 644/POffset: 0x001f1740
2	□		m...	0	[PROCESS] csrss.exe PID: 576/PPID: 352/POffset: 0x05da4698
3	□		m...	0	[PROCESS] inetinfo.exe PID: 1568/PPID: 644/POffset: 0x010361a0
4	□		m...	0	[PROCESS] logonui.exe PID: 1168/PPID: 600/POffset: 0x0a1a2a88
5	□		m...	0	[PROCESS] lsass.exe PID: 656/PPID: 600/POffset: 0x010a0cd0
6	□		m...	0	[PROCESS] services.exe PID: 644/PPID: 600/POffset: 0x01082698
7	□		m...	0	[PROCESS] smss.exe PID: 352/PPID: 4/POffset: 0x010098f0
8	□		m...	0	[PROCESS] spoolsv.exe PID: 1332/PPID: 644/POffset: 0x0aa3a418
9	□		m...	0	[PROCESS] sqlservr.exe PID: 1584/PPID: 644/POffset: 0x01035ca8
10	□		m...	0	[PROCESS] svchost.exe PID: 1048/PPID: 644/POffset: 0x08fdb240
11	□		m...	0	[PROCESS] svchost.exe PID: 1084/PPID: 644/POffset: 0x00ffcac8
12	□		m...	0	[PROCESS] svchost.exe PID: 1520/PPID: 644/POffset: 0x01033e58
13	□		m...	0	[PROCESS] svchost.exe PID: 816/PPID: 644/POffset: 0x05b99be0
14	□		m...	0	[PROCESS] svchost.exe PID: 896/PPID: 644/POffset: 0x0104bf00
15	□		m...	0	[PROCESS] svchost.exe PID: 988/PPID: 644/POffset: 0x08e19698
16	□		m...	0	[PROCESS] war-ftpd.exe PID: 1752/PPID: 644/POffset: 0x0b632698
17	□		m...	0	[PROCESS] winlogon.exe PID: 600/PPID: 352/POffset: 0x010180a8
18	□		.acb	0	[SHIMCACHE] C:\PROGRA~1\MICROS~2\MSSQL\binn\UMS.DLL
19	□		.acb	0	[SHIMCACHE] C:\Program Files\Java\jdk1.5.0_06\jre\bin\client\jvm.dll
20	□		.acb	0	[SHIMCACHE] C:\Program Files\Java\jre1.5.0_06\bin\client\jvm.dll
21	□		m...	0	[THREAD] System PID: 4/TID: 100
22	□		m...	0	[THREAD] System PID: 4/TID: 104
23	□		m...	0	[THREAD] System PID: 4/TID: 108
24	□		m...	0	[THREAD] System PID: 4/TID: 116
25	□		.acb	0	[THREAD] System PID: 4/TID: 12
26	□		m...	0	[THREAD] System PID: 4/TID: 124

C:\Users\John\Desktop\timeline.csv — Total lines 117,579 | Visible lines 117,579 | Open files: 1 | Search options

Figure 5.1 – Combined timeline open in Timeline Explorer.

Part 6 – Image analysis



(Sandbox) Windows 10 - VMware Workstation 16 Player (Non-commercial use only)

IDA - war-ftpd.1752.exe C:\Users\John\Desktop\war-ftpd.1752.exe

```
Function name
sub_401000
sub_401180
sub_401240
sub_401300
sub_401310
sub_401320
sub_4013B0
sub_401580
sub_4015A0
sub_401600
nullsub_3
sub_4017C0
sub_401850
sub_401950
sub_4019E0
nullsub_4
nullsub_5
nullsub_6
```

Line 1 of 1457

```
sub_434B19 proc near

arg_0= dword ptr  4
arg_4= dword ptr  8

call    MFC42_1168
mov     edx, [esp+arg_0]
mov     ecx, [esp+arg_4]
mov     [eax+14h], dl
test    edx, edx
mov     [eax+1040h], ecx
jnz     short loc_434B3E

push    0FFFFFFFDh      ; CodePage
call    ds:_setmbcp
add     esp, 4

loc_434B3E:
mov     eax, 1
retn    8
sub_434B19 endp
```

```
80.00% (-391,-4) (510,305) 00033F29 0000000000434B29: sub_434B19+10 (Synchronized with Hex View-1)
```

Output

```
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
```

```
AU:  idle  Down  Disk: 42GB
```

Figure 6.1 – war-ftpd.1752.exe open in IDA.