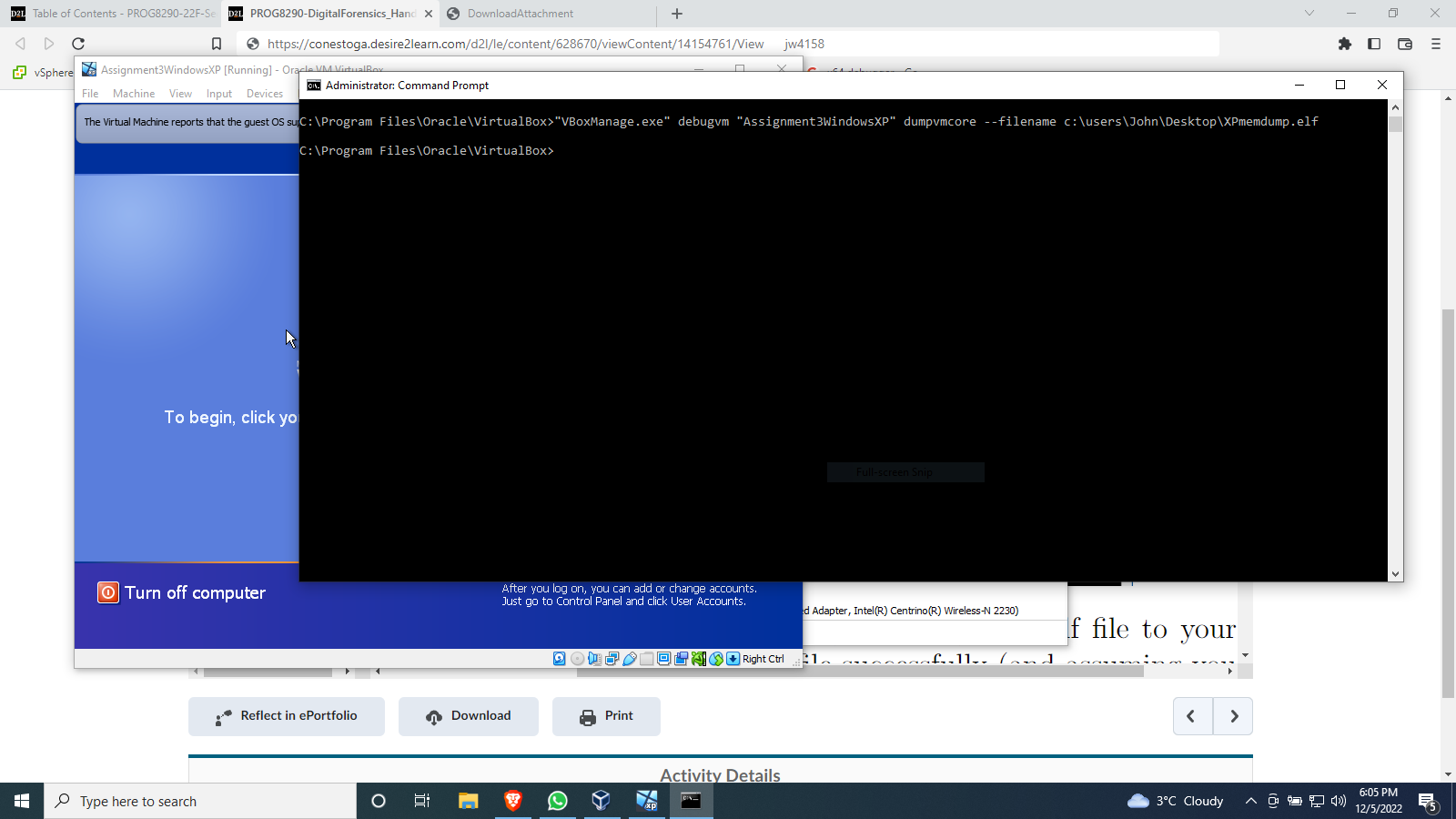
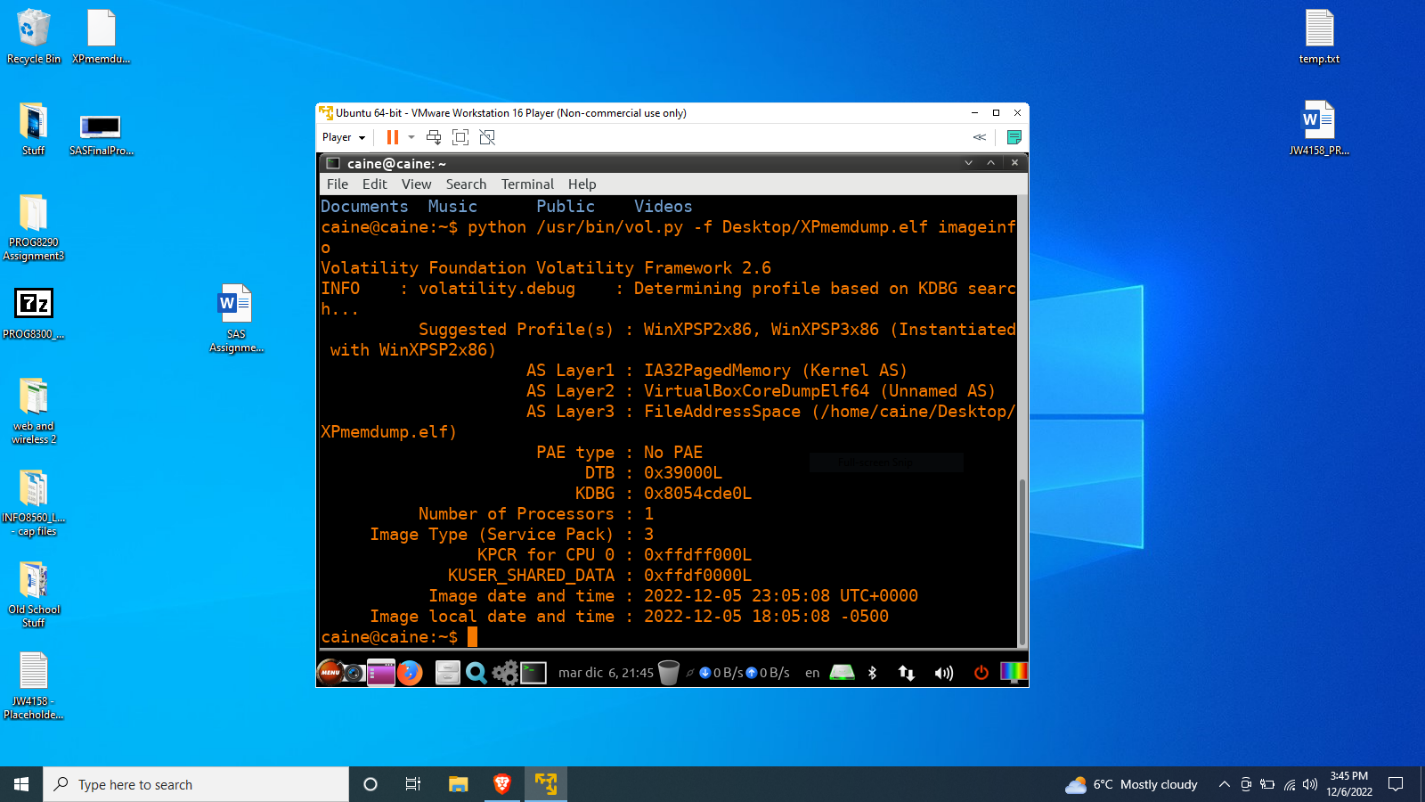
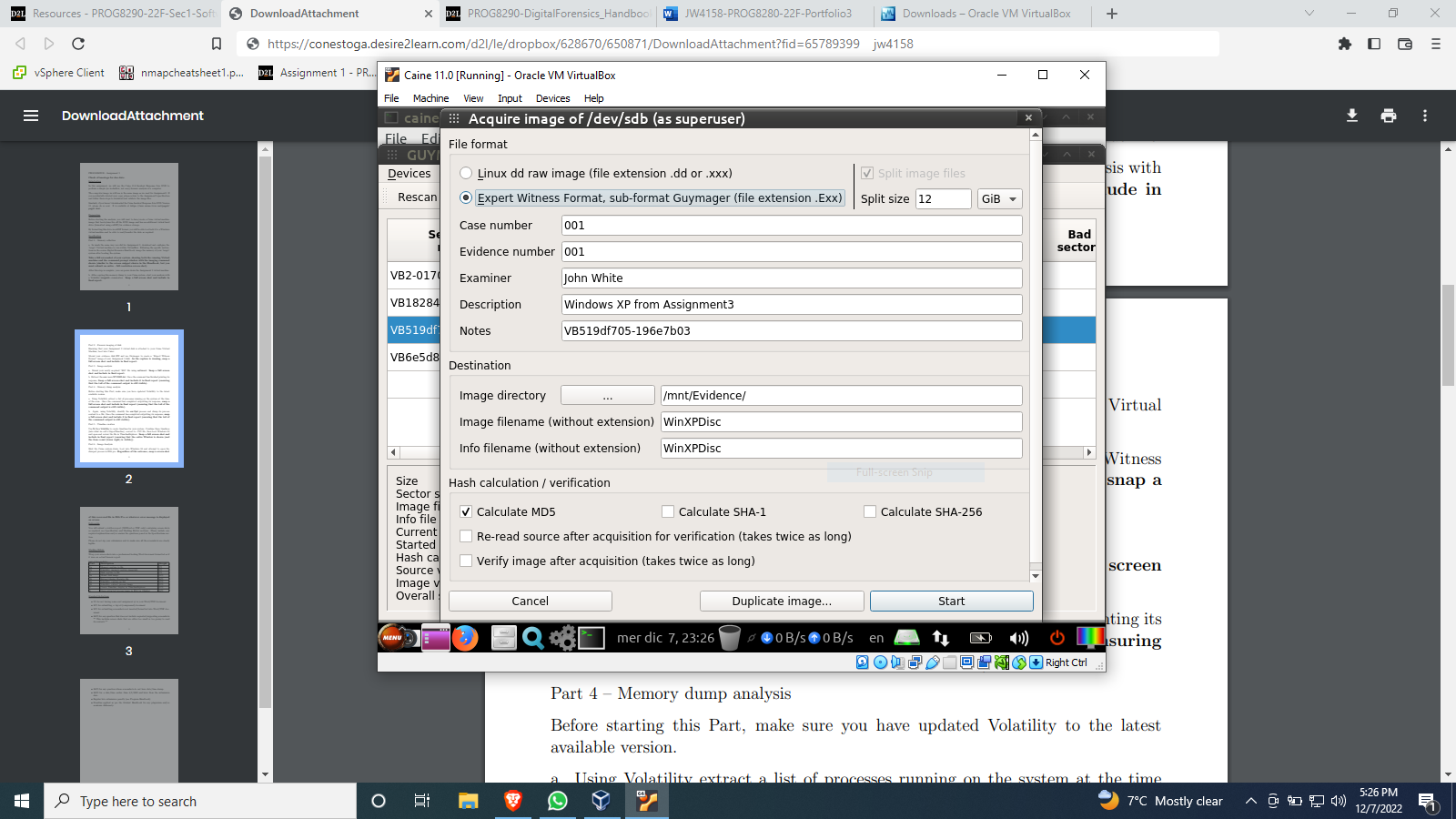
PROG8290 – Assignment 5 – John White (6714158)

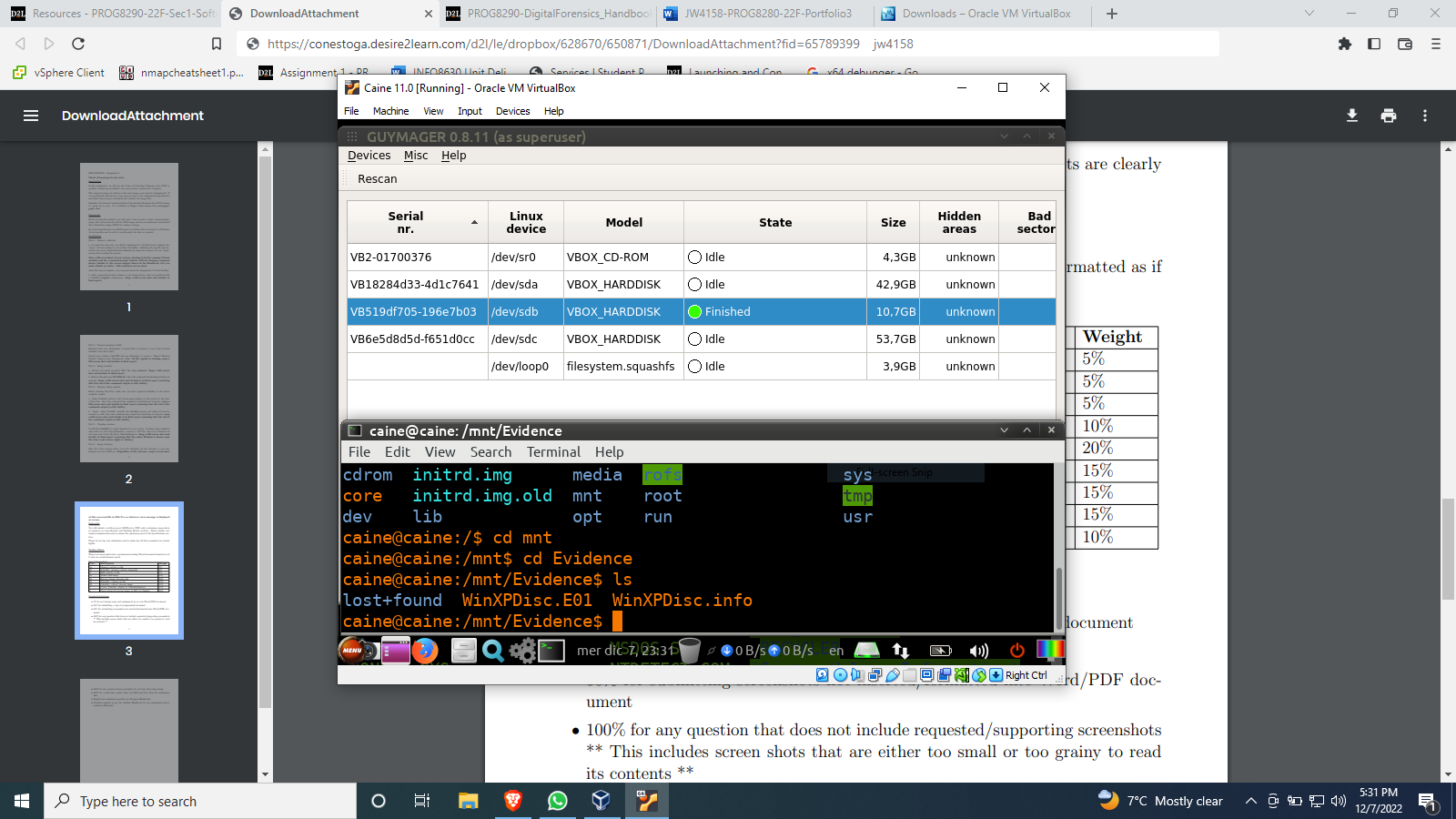
During this assignment, I had many problems with the installation of Caine. I ended up doing all of my work from the Live CD. I was originally using VMWare for the memory analysis because VirtualBox would not let my transfer my files via USB, and I was using VirtualBox for the image analysis because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

Part 1 – Memory Collection

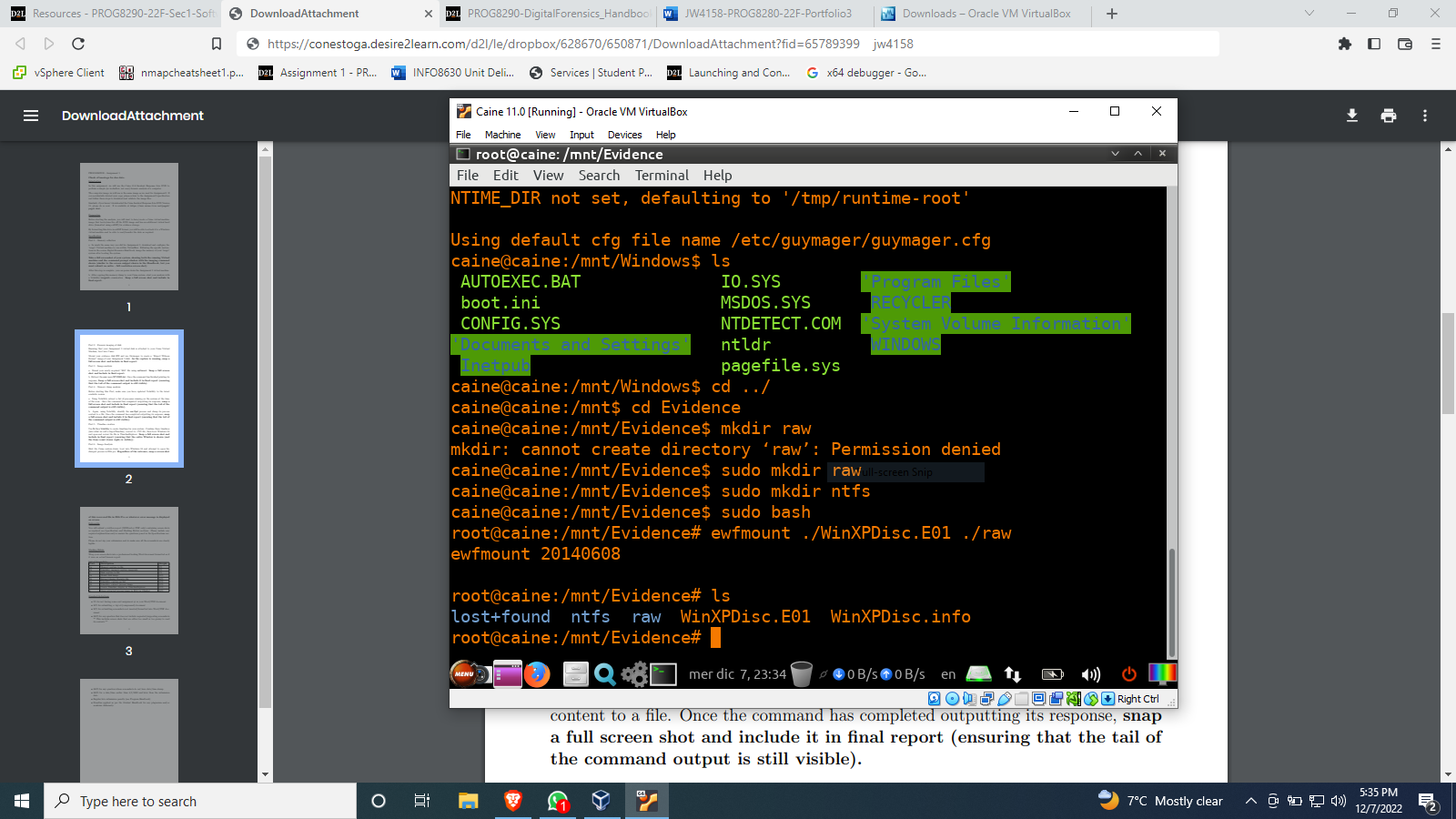
**Figure 1.1** – Capturing the memory dump of the XP VM into a .elf file.**Figure 1.2** – Using Volatility to display the ImageInfo of the .elf file.

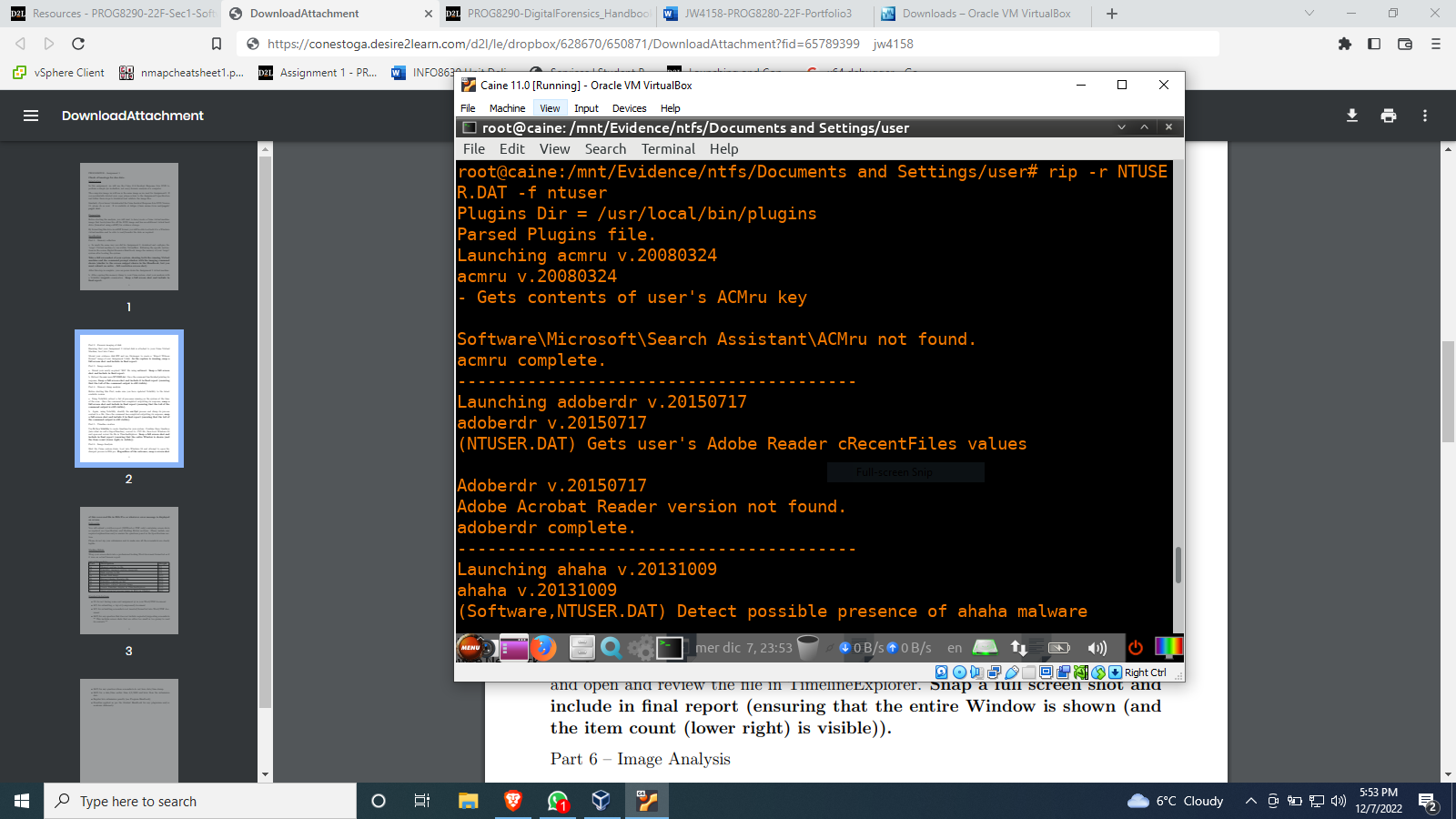
Part 2 – Forensic imaging of disc

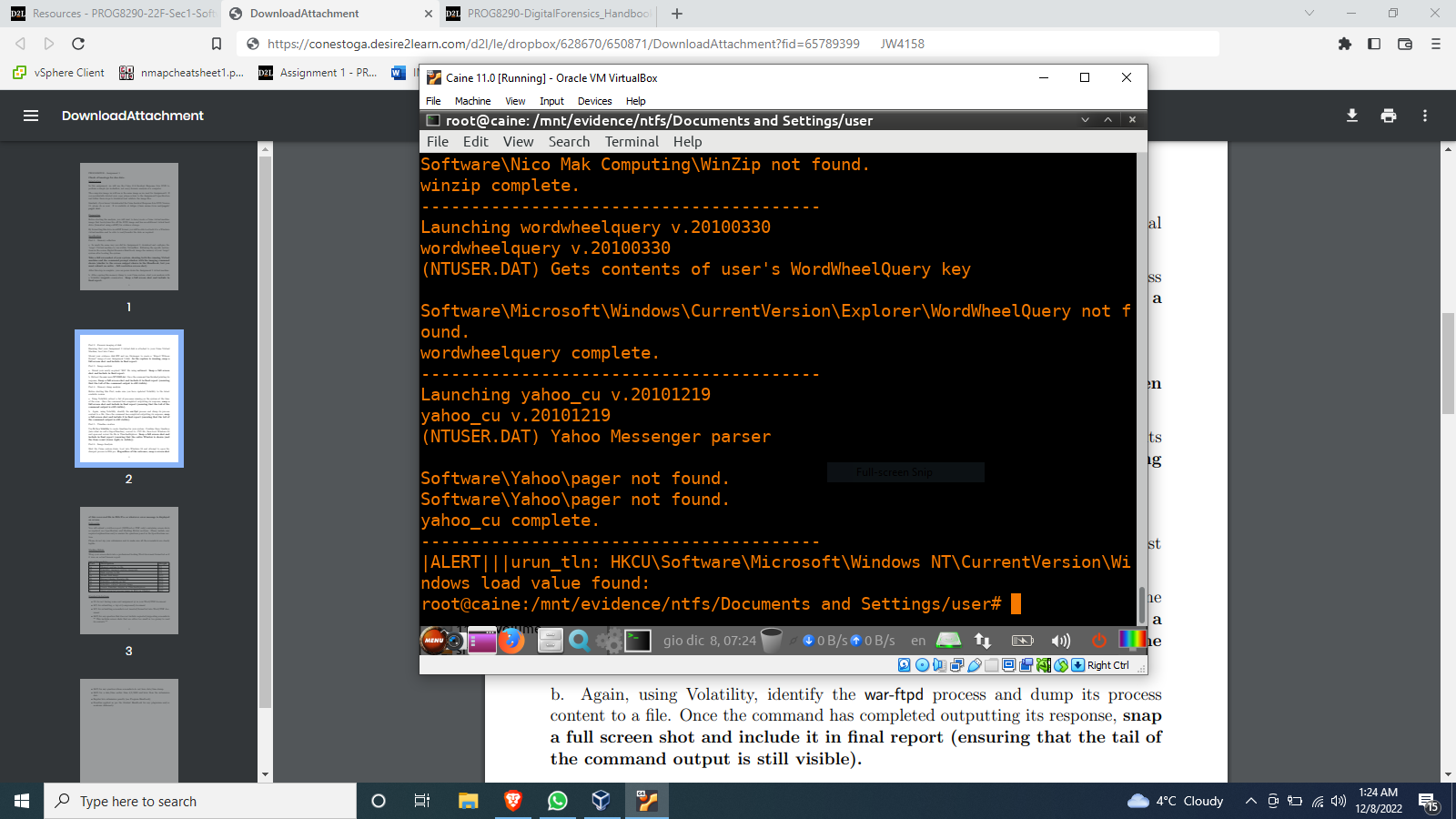
**Figure 2.1** – Guymager Expert Witness Format Settings.

**Figure 2.2** - .E01 file successfully created with Guymager.

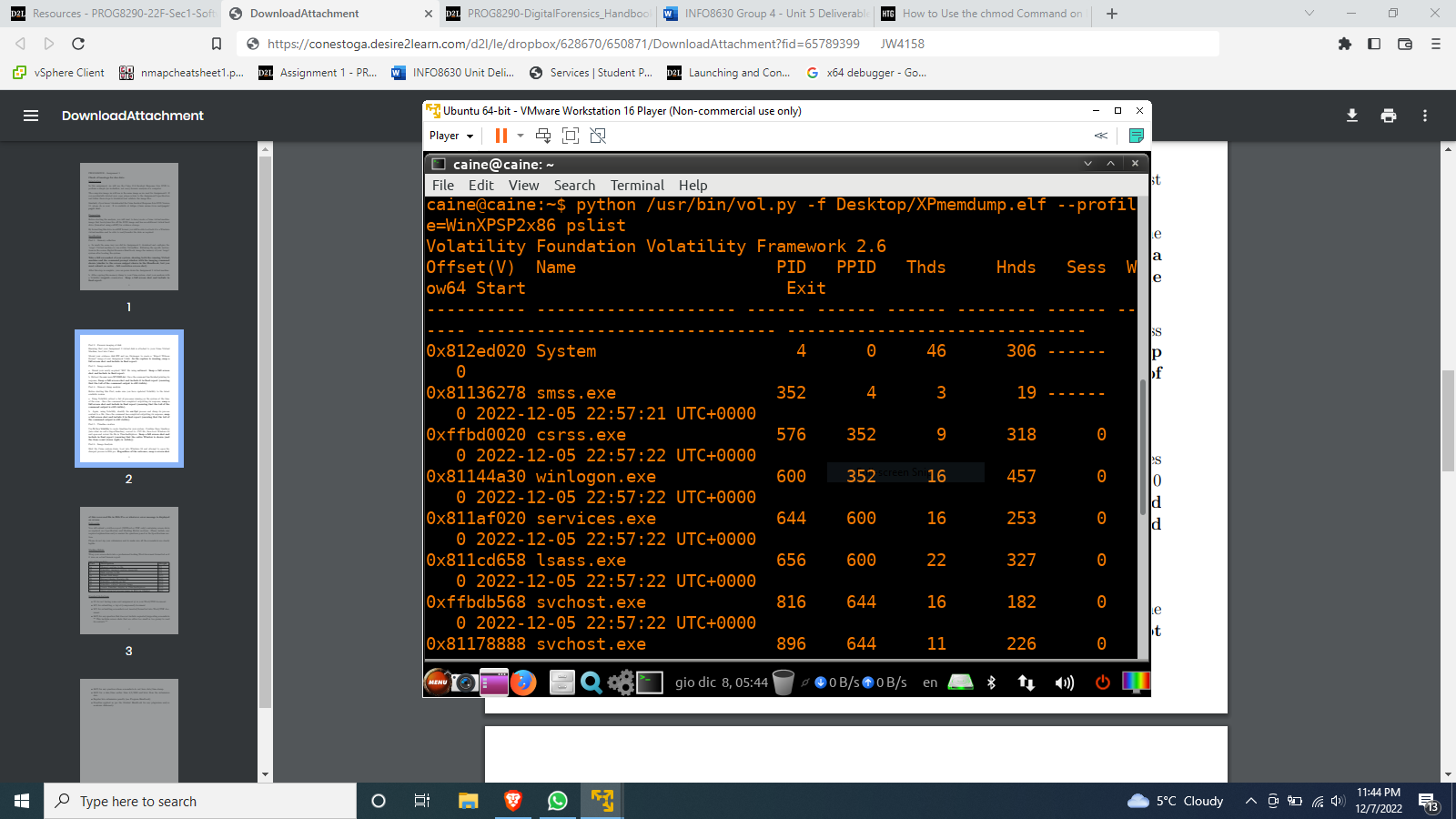
Part 3 – Image Analysis

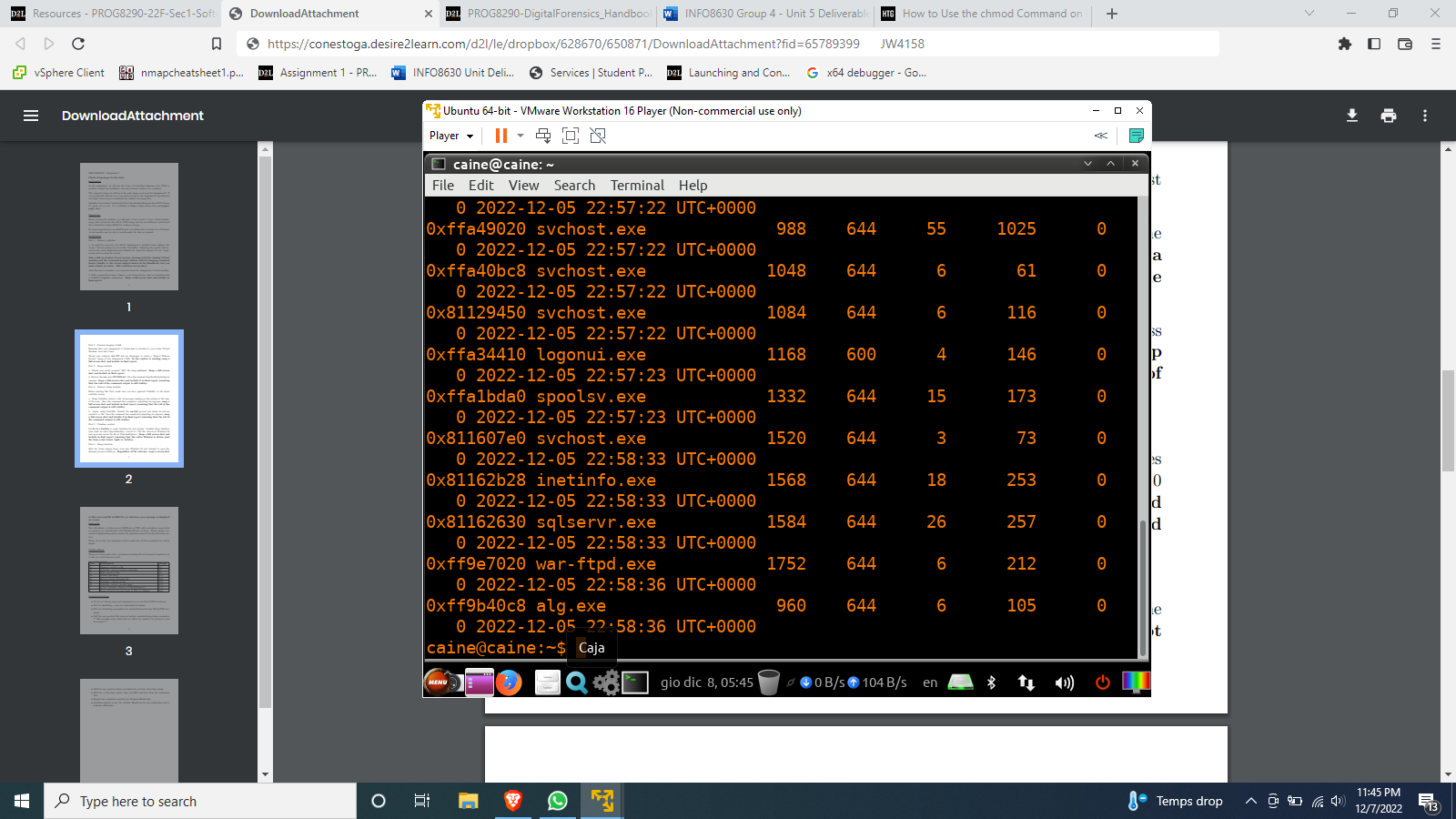
**Figure 3.1** – Using ewfmount to mount the .E01 file to /raw.

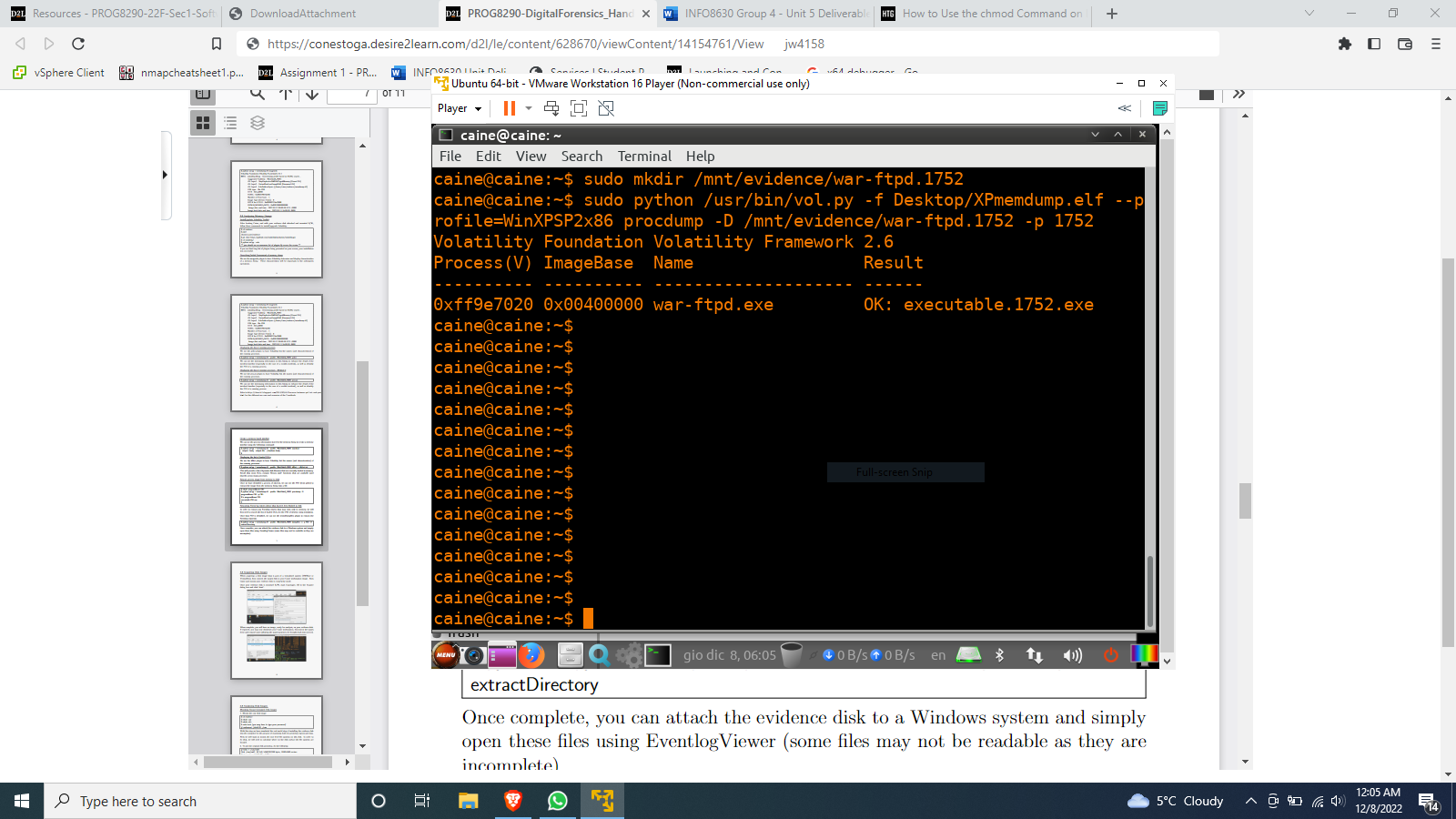
**Figure 3.2** – Using rip to acquire the user data from NTUSER.DAT.

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

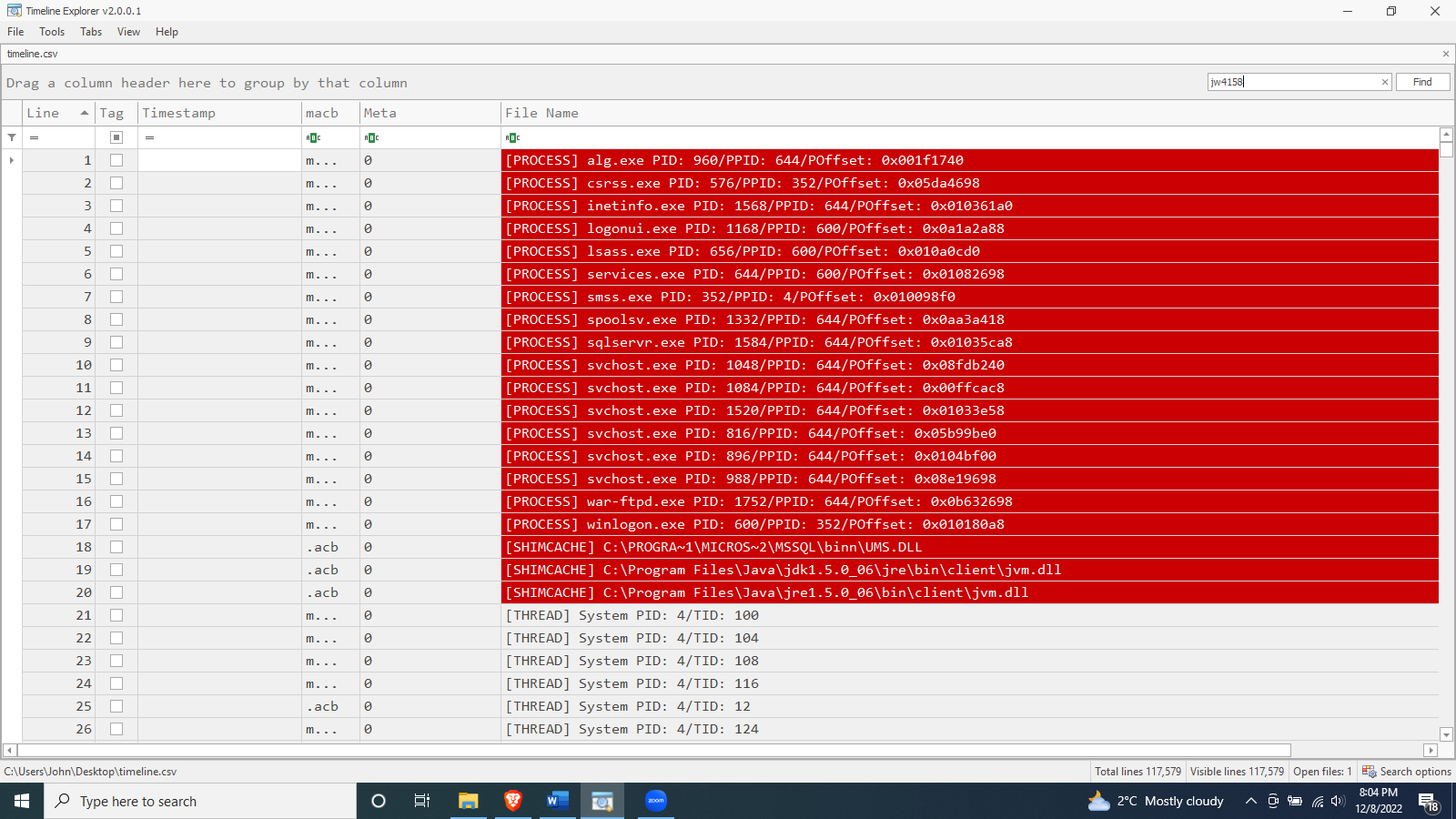
Part 4 – Memory dump analysis

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

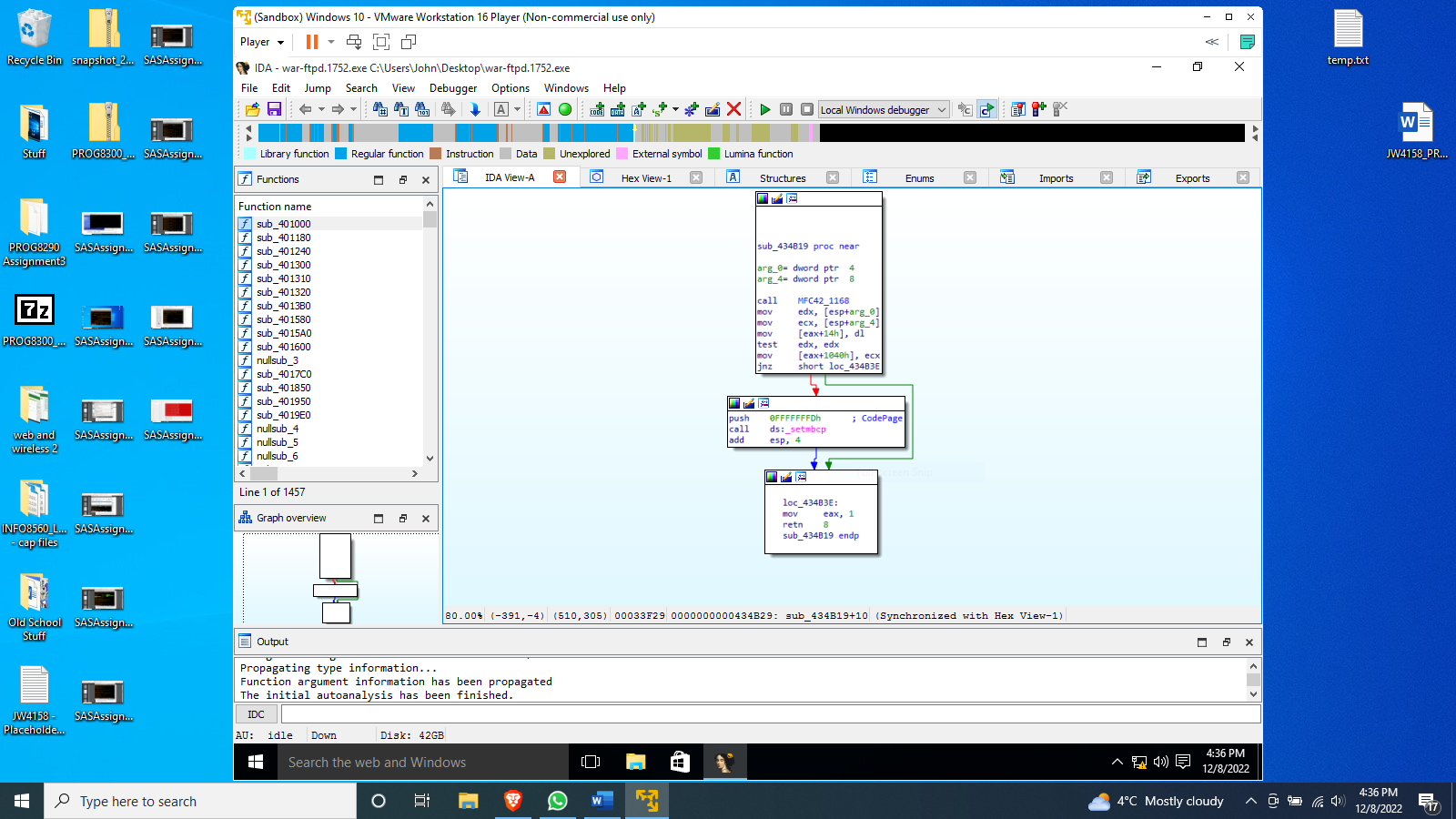
**Figure 4.2** – End of the list of processes running when the XP VM was scanned.

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

Part 5 – Creating a timeline

**Figure 5.1** – Combined timeline open in Timeline Explorer.

Part 6 – Image analysis

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