Final Practical Exam

Allan Wheelock

University of Advancing Technology

Author Note

This paper was prepared for CFR 101 Computer Forensic Essentials, taught by Aaron Jones.

Final Practical Exam

 For the final in this class, I will be analyzing the same file that I analyzed in the FTK Imager lab. The difference between the two reports will be the amount of detail. This report will have far more detail in it than the previous report as this is a final. I did want to start with a fresh download of the file just to make sure nothing weird happened from the original download I had for the FTK Imager lab. I did begin this lab the same way I began the last one, by verifying the hash values were the same from the original file download and the hash that I got from FTK. To prove these were the same I included this screenshot that has the file path and the matching SHA-1 hash values.



 Now that I know the hash values are the same, I can open the file in 7Zip to dive deeper into what is being stored in this compressed file. Once in 7Zip, I pulled up the same text file that had all the information I used in the last report, “able2.log”. I figured this would be a good place to start as it seemed to contain most if not all the information I required for that lab. At the top of the report, we are given the first bit of information required for this report, which is who I believe to be the case detective, who is “Special Agent, Barry J. Grundy”. For a report like this I believe the examiner would be me, as I am examining the report done by the detective.

After some research, I was able to find a web page that had the specifications of the hard drive reported in the log file. It is a “7345AT Maxtor 7000 Series 345MB 3600RPM ATA/IDE 3.5-inch Internal Hard Drive” (memory4less.com). At first, I was quite surprised to see that the capacity of this drive was only 345 MB and though there was no way that it was this small. I found the number of bytes that the disk contained within the log file and did a conversion of that to megabytes. To my surprise the byte count was much smaller than I expected and nowhere near the limit of the hard drive. With a little more reading in the text file, I was able to discover where this hard drive came from as well. The source of the evidence is that the disk came from a machine with host name “able2” and the system was compromised and used to transfer illicit files.

 With the information above regarding I believe that the scope of this investigation was all the data contained within the subject computer. In the log file it is listed as “\*\*\*Practice Disk\*\*\* Hostname ‘able2’”. That information combined with the face that it’s at the top of the report followed by the reasoning the system was being investigated, I think this is all the warrant information.

 There are a few artifacts that I can access, however I cannot see the contents of the entire disk. At the highest level I can access the first two files, these being, “able2.dd” and “able2.log”. The log file is where I have gotten most of the information from, and the “.dd” artifact has quite a bit of additional information contained within it. Once in there I can see 4 partitions of the hard drive. Three of these partitions are Linux Filesystem partitions, leaving the fourth (2.img) as a Solaris x86 / Linux Swap drive. Of these four partitions, I was able to access the three Linux Filesystem partitions, but the swap drive appears to be corrupted, and I cannot open it.

 After doing some digging into each of these partitions, I found several artifacts that caught my eye from the name of them, however when I tried to view each one, I was unable to see much other than a bunch of symbols, leading me to believe that this information was encrypted somehow, and I won’t be able to view it decrypted without the key. I did find one file that explains what each of the files is, but I still can’t see within them due to the encryption. This file I found at path \able2.tar.gz\able2.dd\3.img\X11R6\man\whatis\.



 I continued to do some digging as I hadn’t found much that was interesting yet, but then I came across this file that contained some code for something. At the top of each script is a description of what that script does, and who wrote it. In this case all of them have the name “Arnold Robbins” attached to them.





 Finally, after lots of digging around these files I stumbled upon a folder called “man” that contained several subfolders with the same name and a series of numbers listing them in order. There was another “whatis” file here as well explaining what a bunch of different commands were and what function they would perform. After reading through many of these commands it appeared that the original claim in the log file that this hard drive had been used to transfer illicit files was true. Many of these commands had to do with filesystem and verifying credentials multiple times between both users involved. After reading into this “whatis” file further I opened the folder titled “man1” and discovered that almost in the exact same order as the “whatis” file, were all the same commands. That information leads me to believe that those commands were used to transfer files off the hard drive to another location titled “man1”.



 Based on this information that I discovered throughout my work on this hard drive I believe that the accusations of this hard drive being used to transfer illicit files is correct.

References

Us, A., Us, C., Policy, P., Policy, R., Info, W. and RMA, S., 2021. *7345AT Maxtor Hard Drive*. [online] Memory4Less.com. Available at: <https://www.memory4less.com/maxtor-hard-drive-7345at> [Accessed 12 August 2021].