NTS405: Incident Response; Project 4.2 – Windows Investigation

Jackson Nestler

University of Advancing Technology

NTS405: Incident Response; Project 4.2 – Windows Investigation

Objective: Choose an investigative tool and document at least four unique aspects of the tool and analyze any results.

For this assignment, I chose to use FTK Imager Lite. FTK Imager is a premium tool developed by AccessData to perform forensic investigations of disks and basic memory analysis. The Lite version is handicapped in a few ways but will prove more than enough for basic forensics exercises and will be enough for this assignment. They haven't updated it in many years, but it functions incredibly well. AccessData posts the download link on their website.

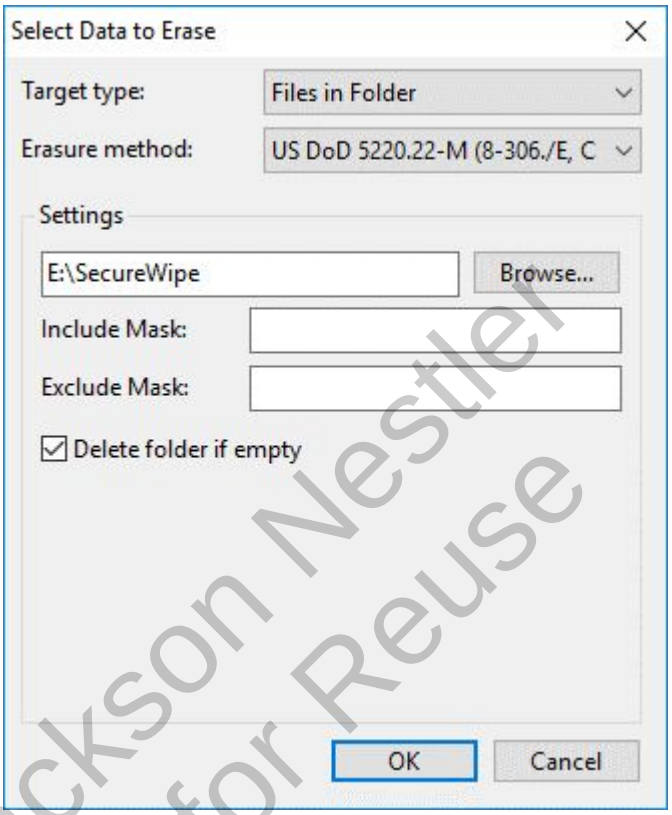
Setup

I got a 2GB SD card from a friend and wiped it following the DoD 5220.22-M wiping standard, a three-pass method that writes zeroes, ones, and then a random string of bits. Now I've formatted it NTFS and added a folder called "Pics" and inside is a photo of a dog called "dog.jpg." Additionally, inside the same "Pics" folder I made a folder called "Hidden" and changed its properties to be hidden and placed a picture of a second dog inside the Hidden folder. Back in the root directory I placed a text file called "simple_delete.txt" with the text "this file is just going to be deleted by right clicking and pressing delete." I created another text file called "shift_delete.txt" with the text "this file is going to be deleted with shift + delete." Finally I'll make a folder called "SecureWipe" which has a copy of the Manjaro Linux Wiki's homepage and a copy of the UAT logo (logo.png).

Secure Wiping

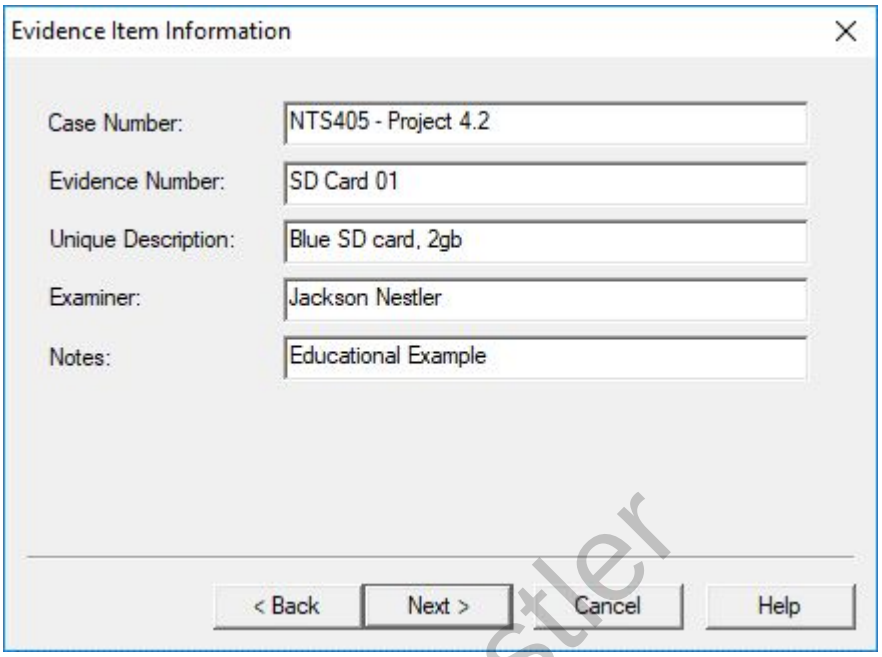
So to deal with the "SecureWipe" folder, I'll be running the Eraser tool, which has access to an array of erasure methods including the DOD secure wipes, Gutmann, and a few others like

Russian standards and RCMP standards. I launched the application, right clicked and created a new task. You can see my settings below. I ran this to completion and then launched FTK Imager.



Acquisition Using FTK Imager

Opening up FTK Imager and performing an acquisition is fairly straight-forward. File -> Create Disk Image -> Physical Drive -> Select the SD card. Now it'll ask about where to store the image and what file storage type to use: for my ease, I've decided to use "raw (DD)" to hold the image. Some data needed to be filled in:



Creating an image of the card took a few minutes. I stored the image to my Documents, inside a folder called "FTK" – in a real IR scenario we'd keep a backup of the image we just took on something like an external hard drive or a CD/DVD for future reference. Once the capture was complete, the contents of the image were loaded directly into my screen and I can take a look at the contents of the SD card.

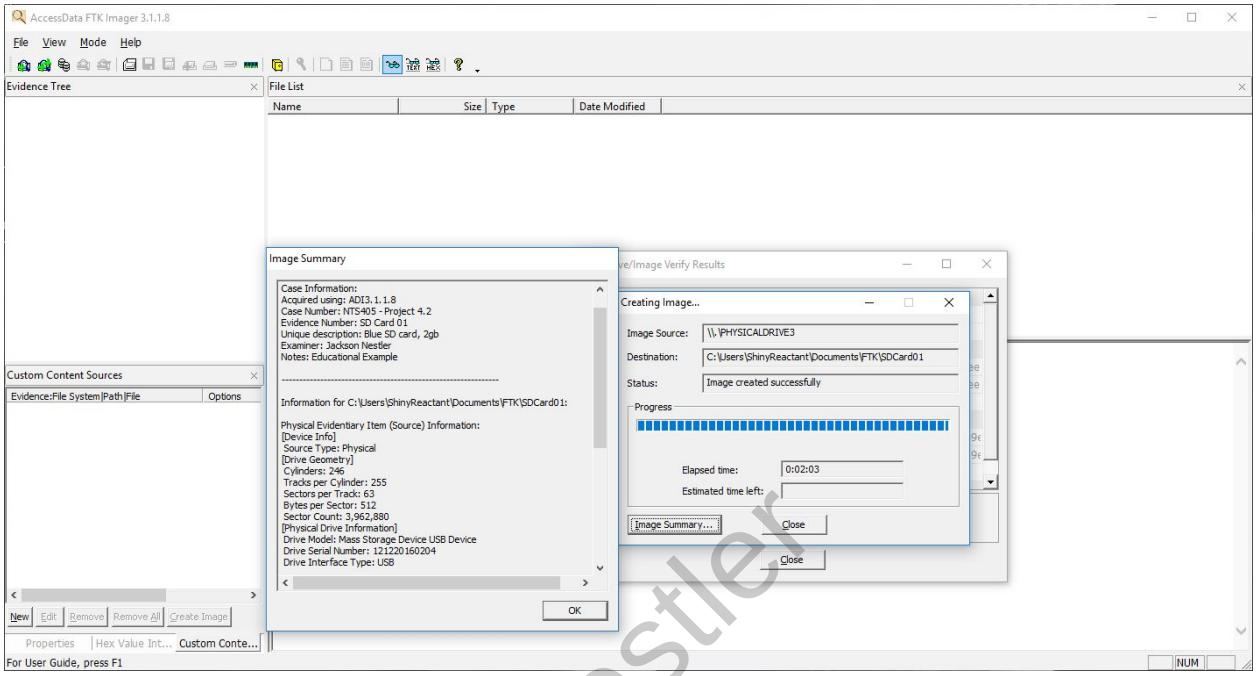
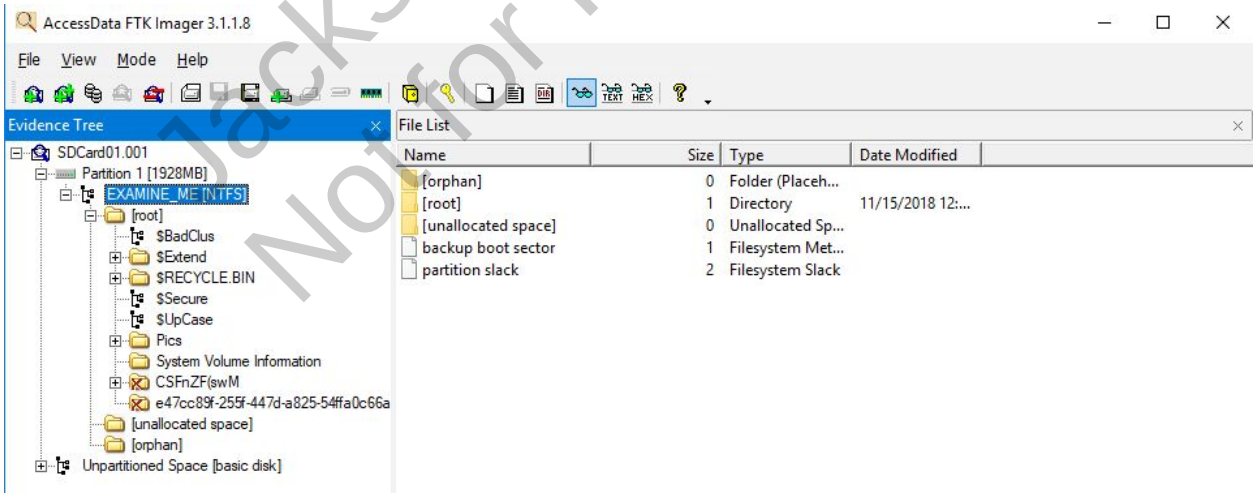


Image Inspection

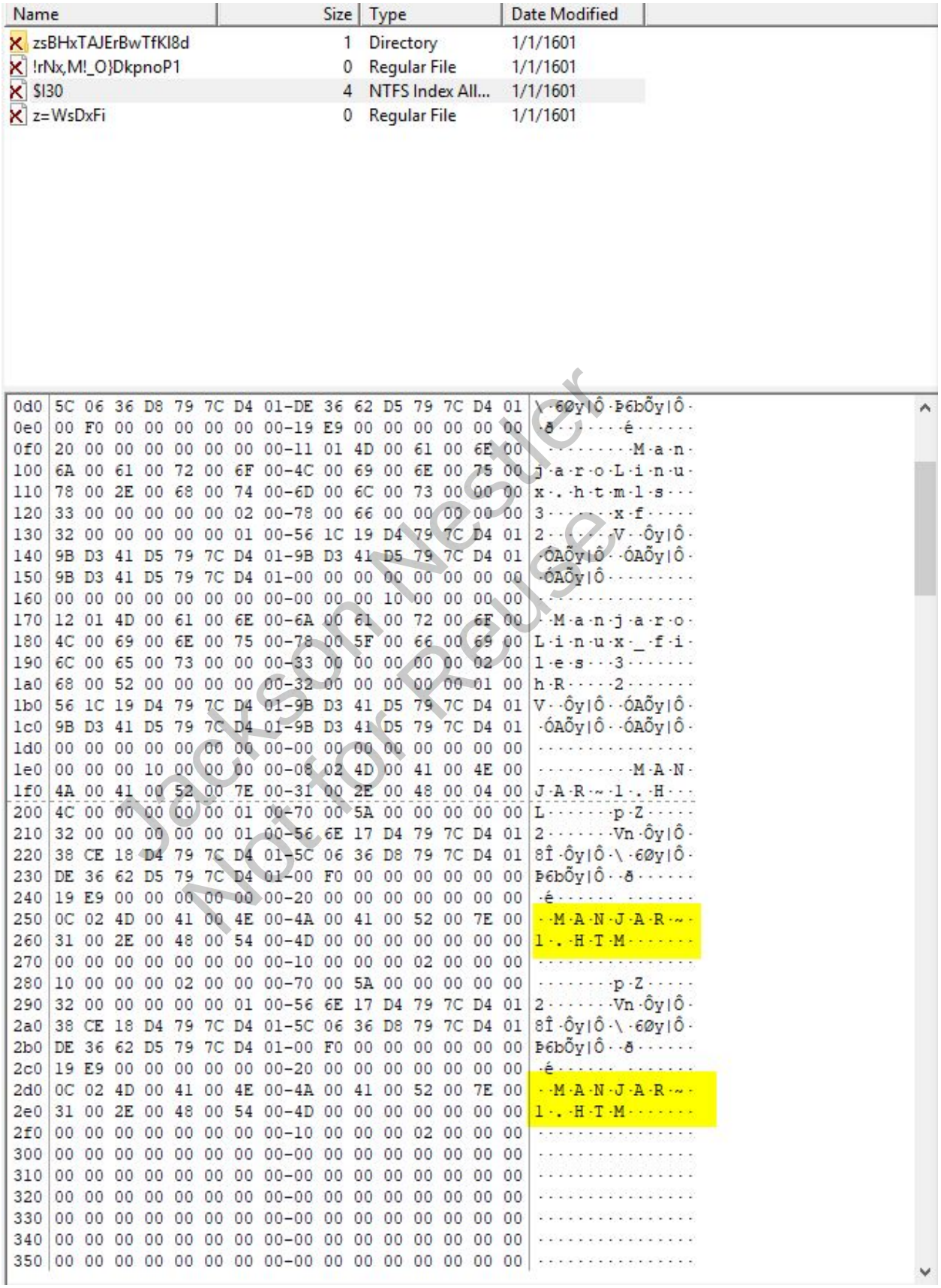
MD5 hash: 982bd8c776538d1365389f27d1aed3ee

SHA1 hash: 6923e6fe0a8237f33a28455318040739e6e32752



Expanding [root] gave us a ton of information: in short, the folder that needed to be securely wiped was in fact wiped securely; there are now two folders in its place that have

random names and completely unrecognizable filenames. However, the Manjaro HTML page has its name fragments still left.



Name	Size	Type	Date Modified
zsBHxTAJErBwTfKI8d	1	Directory	1/1/1601
!rNx,M!_O}DkpnoP1	0	Regular File	1/1/1601
$I30	4	NTFS Index All...	1/1/1601
z=WsDxFi	0	Regular File	1/1/1601

```
0d0 5C 06 36 D8 79 7C D4 01-DE 36 62 D5 79 7C D4 01 \·6Øy|Ô·Þ6bÕy|Ô·
0e0 00 F0 00 00 00 00 00 00-19 E9 00 00 00 00 00 00 ·ð·····é·····
0f0 20 00 00 00 00 00 00 00-11 01 4D 00 61 00 6E 00  ·····M·a·n·
100 6A 00 61 00 72 00 6F 00-4C 00 69 00 6E 00 75 00 j·a·r·o·L·i·n·u·
110 78 00 2E 00 68 00 74 00-6D 00 6C 00 73 00 00 00 x·.·h·t·m·l·s···
120 33 00 00 00 00 00 02 00-78 00 66 00 00 00 00 00 3·····x·f·····
130 32 00 00 00 00 00 01 00-56 1C 19 D4 79 7C D4 01 2·····V··Ôy|Ô·
140 9B D3 41 D5 79 7C D4 01-9B D3 41 D5 79 7C D4 01 ·ÓAÕy|Ô··ÓAÕy|Ô·
150 9B D3 41 D5 79 7C D4 01-00 00 00 00 00 00 00 00 ·ÓAÕy|Ô·····
160 00 00 00 00 00 00 00 00-00 00 00 10 00 00 00 00 ····------····
170 12 01 4D 00 61 00 6E 00-6A 00 61 00 72 00 6F 00 ··M·a·n·j·a·r·o·
180 4C 00 69 00 6E 00 75 00-78 00 5F 00 66 00 69 00 L·i·n·u·x·_·f·i·
190 6C 00 65 00 73 00 00 00-33 00 00 00 00 00 02 00 l·e·s···3·····
1a0 68 00 52 00 00 00 00 00-32 00 00 00 00 00 01 00 h·R·····2·····
1b0 56 1C 19 D4 79 7C D4 01-9B D3 41 D5 79 7C D4 01 V··Ôy|Ô··ÓAÕy|Ô·
1c0 9B D3 41 D5 79 7C D4 01-9B D3 41 D5 79 7C D4 01 ·ÓAÕy|Ô··ÓAÕy|Ô·
1d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ····------····
1e0 00 00 00 10 00 00 00 00-08 02 4D 00 41 00 4E 00 ····------M·A·N·
1f0 4A 00 41 00 52 00 7E 00-31 00 2E 00 48 00 04 00 J·A·R·~·1·.·H···
200 4C 00 00 00 00 00 01 00-70 00 5A 00 00 00 00 00 L·····p·Z·····
210 32 00 00 00 00 00 01 00-56 6E 17 D4 79 7C D4 01 2·····Vn·Ôy|Ô·
220 38 CE 18 D4 79 7C D4 01-5C 06 36 D8 79 7C D4 01 8Î·Ôy|Ô·\·6Øy|Ô·
230 DE 36 62 D5 79 7C D4 01-00 F0 00 00 00 00 00 00 Þ6bÕy|Ô··ð····
240 19 E9 00 00 00 00 00 00-20 00 00 00 00 00 00 00 ·é····· ·····
250 0C 02 4D 00 41 00 4E 00-4A 00 41 00 52 00 7E 00 ··M·A·N·J·A·R·~·
260 31 00 2E 00 48 00 54 00-4D 00 00 00 00 00 00 00 1·.·H·T·M·····
270 00 00 00 00 00 00 00 00-10 00 00 00 02 00 00 00 ····------····
280 10 00 00 00 02 00 00 00-70 00 5A 00 00 00 00 00 ····------p·Z·····
290 32 00 00 00 00 00 01 00-56 6E 17 D4 79 7C D4 01 2·····Vn·Ôy|Ô·
2a0 38 CE 18 D4 79 7C D4 01-5C 06 36 D8 79 7C D4 01 8Î·Ôy|Ô·\·6Øy|Ô·
2b0 DE 36 62 D5 79 7C D4 01-00 F0 00 00 00 00 00 00 Þ6bÕy|Ô··ð····
2c0 19 E9 00 00 00 00 00 00-20 00 00 00 00 00 00 00 ·é····· ·····
2d0 0C 02 4D 00 41 00 4E 00-4A 00 41 00 52 00 7E 00 ··M·A·N·J·A·R·~·
2e0 31 00 2E 00 48 00 54 00-4D 00 00 00 00 00 00 00 1·.·H·T·M·····
2f0 00 00 00 00 00 00 00 00-10 00 00 00 02 00 00 00 ····------····
300 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ····------····
310 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ····------····
320 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ····------····
330 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ····------····
340 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ····------····
350 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ····------····
```

Diving further into the folders, we can see that there are fragments in a lot of these folders: “Hardware.png” is leftover in the hex dump of “$l30”, an NTFS index file. Of note, it doesn’t seem like Eraser is secure when it comes to erasing files from a folder: I suspect a full drive wipe would have no recoverable data. Our “Pics” folder has the picture of a puppy, and the “Hidden” folder is in plain view containing the picture of our hidden pug. Interestingly, I cannot find the text files that were deleted (shift_delete.txt and simple_delete.txt) so they may be gone completely, or they’re not easily found: it could require file carving to eventually find that data.

Conclusion

FTK Imager is a solid application for doing forensics of hard disk images and memory: in this assignment, I tested a 2GB SD card and various erasure methods to see what was recoverable. In an IR situation, this could be used to find malware that hit the disk or recover files that a poorly-written ransomware didn’t fully encrypt. Alternatively it could find compromised corporate data that a disgruntled employee took, or verify that a sensitive document was or wasn’t on the drive of someone who shouldn’t have it. FTK Imager is absolutely worth adding to your toolbox.