CIS484-78-4212

Project 1 Notes
You will need admin access to a Windows computer (physical or virtual) and a FAT32-formatted device for this project. All files and/or tools required for this project may be downloaded using the links posted on Blackboard or provided during lecture.

Forensic Image Conversion using FTK Imager
Download the Project 1 forensic image ("Project1-RawImageFile.zip") using the link under the Project 1 folder on Blackboard. Extract the raw forensic image from the downloaded .zip archive. Using FTK Imager, convert the downloaded raw image to E01 format. As a reminder, you can convert forensic images to different formats in FTK Imager using the same process forensic imaging by selecting "Image File" as the input source during the imaging process. Split the image into 10 MB chunks using a compression level of "1". Do not use AD Encryption. Check the option to "Verify images after they are created", "Pre-calculate Progress Statistics", and "Create directory listings of all files in the image after they are created". Once the image conversion process completes, answer the following questions:

1) How many E01 segments were created during the image conversion? 3 segments
2) What is the total file size in bytes of the raw forensic image? 10,053,000 bytes/2,147,483,648
3) According to the imaging log, how many sectors were located in the raw image? 4,194,304
4) What is calculated MD5 hash value of the raw image? d9361d55e6c5aa4e915767e17a455d62
5) What is the calculated SHA1 hash value for image verification (i.e., the SHA1 hash value of the E01 image)? b9f5fbc22627907a0f868d2a6950e3d40e9954c7
6) According to the directory listing, how many deleted files are present in the forensic image? 0
7) According to the directory listing, what is the file size in bytes of the largest .log file on the forensic image? 60041570 bytes
8) According to the directory listing, how many .JPG images are stored on the forensic image? 7

Working with Alternate Data Streams
On an NTFS formatted drive (such as your C:\ drive) and using Notepad, create a text file and name it "Project1" (do not insert any text into the file). Create an alternate (additional) data stream for the new file using the example on page 229 and name it "ads.txt". Insert your last name as the only text within the alternate data stream. Verify that the ADS has been created properly by typing "notepad project1.txt:ads.txt" at the command line (make sure you're in the same directory as the project1.txt file).

9) Check the size of the project1.txt file in Windows (right click on the file, select Properties). What is the size of the file displayed in the Windows Properties? 0
10) Open the NTFS drive you're working with as a physical device in WinHex and locate the MFT record that corresponds with the "Project 1.txt" file you created (right click

on the file > Navigation > Go to FILE Record). Based on examination at the hexadecimal level, how can you determine that this file has an alternate data stream? Two 0x80

Attempt to copy Project1.txt to a FAT32 formatted device.

11) When you tried to copy the file, what happened? The data in the alternate stream could not be copied, if I wanted to proceed, I would lose the data.
12) Why did this happen? FAT32 doesn't support ADS files.

Parsing MFT Records

Download the MFT Record from Blackboard under Projects > Project 1 and open the file using WinHex (File > Open). To interpret the timestamp values, use MFT Stampede. **Leave all timestamp values in UTC format.** Answer the following questions:

13) What is the type and allocation status of this item? The allocation status of this item is 01 (file allocated)
14) What is the MFT record number (decimal value) of this file/directory? 59117
15) What is the creation timestamp in the $STANDARD_INFORMATION attribute? Fri, 30 Oct 2020 19:23:02
16) What is the modified timestamp in the $STANDARD_INFORMATION attribute? Fri, 30 Oct 2020 19:23:03
17) What is the record update timestamp in the $STANDARD_INFORMATION attribute? Fri, 30 Oct 2020 19:23:03
18) What is the accessed timestamp in the $STANDARD_INFORMATION attribute? Fri, 30 Oct 2020 19:23:06
19) What is the name of this file/directory? WORKIN~1.ZIP and WorkingFiles.zip both appear
20) How many timestamps are included in this MFT Record? There are eight timestamps
21) What is the starting cluster of this file/directory? 38 00 00 00
22) Is the content of this file/directory resident or non-resident? Resident (00)
23) How many $DATA (0x80) attributes does this file/directory have? 2
24) What is the MFT record number for the parent of this file/directory? 5A0000001800
25) Is this file/directory fragmented? How do you know? No, this file is not fragmented because it is a resident and there are no data runs.