CIS/ECE 387 Fall 2022 Lab4

Due: **10/12/2022**
Total points: 20

ACTIVITY: FAT File System Analysis with Sleuthkit

DOWNLOAD THE DISK IMAGE FILE

You can download the disk image file, fatDisk.dd, on canvas under the Files->Labs->Lab4 folder. This is a disk image with a FAT file system.

GOAL

In this exercise, we'll practice using the Sleuthkit tools at data layer, meta data layer, file system layer and file name layer. You may watch this youtube video for instructions (https://www.youtube.com/watch?v=R-IE2j04Chc).

The steps provided here are only guidelines. Please feel free to try a variety of Sleuthkit tools with different options to fully understand this powerful toolkit.

You may check the following website for detailed documents: https://www.sleuthkit.org/sleuthkit/

INSTRUCTIONS

Use the Sleuthkit commandline tools to analyze the image file, fatDisk.dd.

1. Open the SANS Investigative Forensic Toolkit (SIFT) Workstation.

2. Find the offset of the starting sector for the FAT partition.
   Command: mmls fatDisk.dd

3. Carve out the **MBR** (the first sector of the disk) and **VBR** (boot sector, the first sector of the FAT partition) records with dd command and check it with xxd command.

   Example: dd if=fatDisk.dd of=MBR.dd count=1

   Example: xxd MBR.dd

4. Find the image's file system information (use the offset you got from mmls in step 2). Report the details of the file system, including reserved area, fat 0, fat 1, data area, root directory, cluster area, sector size, and cluster size.
   Command: fsstat –o offset fatDisk.dd

5. Use fls to list all deleted files and directories.

   Command: fls -o offset -f fat -rd fatDisk.dd

6. Use istat to view the details of metadata information of **each deleted file**.

   Example: istat -o offset -f fat fatDisk.dd 7

7. Use icat to dump out data of **each deleted file**.

   Example: icat -o 32 -f fat fatDisk.dd 7 > demoDocx.docx

8. Dump out just one datablock of “demoDocx.docx” file

   Choose a datablock number from your istat result, for example, 2048.
   Example: blkcat -o offset -f fat fatDisk.dd 2048 | xxd

Report

1. Report the details of the file system, including reserved area, fat 0, fat 1, data area, root directory, cluster area, sector size, and cluster size.
2. Include the activity log (the detailed steps you take or the exact commands you run) with some screenshots and/or outputs.
3. Include a brief reflection on what you learned (one or two paragraphs).

Please submit your lab report to Canvas under the “lab4” assignment folder.