COMP 5350 / 6350 – Project #2

Schedule:

Project #2 Assigned: 5 October 2022
Project #2 Due: 5 November 2022

Students Project Requirements:

Part I: Automated file recovery using file signature techniques

In Project #1 our focus was on understanding file system structures and recovering user generated files. In this project instead of using a step-by-step process based on file system boundaries, we will recover files by making use of file signatures. The objective of Project #2 is to develop a Python script that will take a disk image as an input, locate file signatures, properly recover user generated files without corruption, and generate a SHA-256 hash for each file recovered.

You will be provided with a disk image named Project2.dd which will contain several file types:

- ✓ MPG
- ✓ PDF
- ✓ BMP
- ✓ GIF
- ✓ JPG
- ✓ DOCX
- ✓ AVI
- ✓ PNG
- ✓ ZIP (Graduate Students Only)

The following resource will assist with determining file signatures for each file type:
https://www.garykessler.net/library/file_sigs.html

The following program is **an example** of what the kind of information that will be found after the program takes in a disk image. You may configure the output however you would like, but filename, start and end offset, and SHA-256 results must be provided.

Example Output:

./FileRecovery.py Project2.dd

The disk image contains 5 files

File1.mpg, Start Offset: 0x100000, End Offset: 0x200000
SHA-256: 9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0f00a08

File2.pdf, Start Offset: 0x100000, End Offset: 0x200000
SHA-256: 9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0f00a08

File3.gif, Start Offset: 0x100000, End Offset: 0x200000
SHA-256: 9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0f00a08

File4.mpg, Start Offset: 0x100000, End Offset: 0x200000
SHA-256: 9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0f00a08

File5.pdf, Start Offset: 0x100000, End Offset: 0x200000
SHA-256: 9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0f00a08

Recovered files are located in ~/RecoveredFiles

Part II: Conduct network and application scans of a network host to identify port number and protocol information

- ✓ Active

Using network forensics techniques, collect information about a network host and describe how each protocol works.

Final Report:

Each team will provide a final report that answers the questions from the grading rubric. The format of the final report will include the following sections:

1) Executive summary
2) Problem description
3) Description of analysis techniques utilized
4) Tables and screenshots
5) Conclusions and Recommendations

A single page report will not adequately answer all questions so be prepared to have an in-depth analysis and description of the methods you used to answer the questions. **In the final report ensure you document code utilized from any other sources and describe how the code works!**

Grading Rubric:

The grading rubric that will be used to grade each disk image will be based on the following criteria:

Part I: File forensics using file signature analysis

Activity	%	Pts
Are the correct starting and ending offsets specified for each file?	10%	20
Are the correct number of files recovered?	10%	20
Are the files correctly recovered and hash values provided?	15%	30
Is the file recovery process documented in the code?	25%	50

Part II: Network forensics

Activity	%	Pts
Did the team conduct network and service scans to identify port numbers, protocols, and versions running on the host?	20%	40

Part II: Final Report

Activity	%	Pts
Were findings effectively communicated in the final report?	20%	40
Total	100%	200

Project Grading:

Letter grades will be assigned based on a 10-point scale:

90 – 100 = A
80 - 89.9 = B
70 - 79.9 = C
60 - 69.9 = D
< 60 = F