Digital Forensics Project #2

Technical Analysis

For this part of the project, you will work **INDIVIDUALLY** and focus on the analysis of **NTFS** partition and will require an understanding of how to recover data from each properly.

Background:

Your previous findings helped the police to catch one of the hackers "Ghost" at the old warehouse.

The captured hacker, under interrogation, revealed a critical detail: his partner, known by the alias "Shadow" was not only responsible for the planning phase but also for finalizing the digital heist and securing the stolen funds. Shadow has been operating in the shadows, covering their tracks meticulously. However, the captured hacker had one piece of valuable intel with him — a laptop belonging to Shadow.

This laptop holds a key to Shadow's whereabouts, but the information is hidden in the image and in "innocent-looking" files. You managed to create a disk image of the laptop, **ShadowLaptop.dd**, and now it's time to dig through it for clues.

The NTFS partition on SilentShadow.dd contains remnants of encoded messages, passphrases, and possibly a location of where the notorious hacker might be.

You can access the disk image using the following command:

wget https://auburn.box.com/shared/static/x9iwx0iu90ml8qz9sy4n1plbzl6pvcwn.zip

Objectives

You will need to answer the following questions as you are working on your technical analysis:

Q1) Specify the number and type of partitions on the disk image.

Q2) Specify the number of files, file names, and file size of each file on the partition.

Q3) Specify the starting and ending byte offset location of each file on the partition.

Q4) Provide a thorough analysis of the recovered files: Determine the contents of these files to understand the objective, the plan, and any other critical information about the hack.

Note: # System $MFT Records 27

Disk-Editor viewer is permitted, but automated file recovery tools are strictly prohibited during this project. For file recovery, you must use the "dd" command, as we have discussed in class.

Final Report

You will need to provide a final report using the provided **template** as well as the **Project #2 -- Excel template.xlsx**.

Make sure that you turn in all the recovered files along with your report.

Your report should include a:

- detailed analysis of the partition allocation and an illustration of the partition map indicating the volume size, and the number of sectors per field in the partition map.
- detailed analysis of the data recovery process including **annotated screenshots and clear explanations.**
- description of analysis techniques utilized.
- detailed analysis and description of the contents of each file, and how this information is relevant to find the hackers' objectives.
- table in the Executive Summary that clearly states the questions asked and your given answers.

Your report must contain all sections outlined in the template, with the exception of appendices if they are not applicable.

The purpose of this report is to show that an effective analysis of the disk image was properly conducted. 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. Your work must be supported by annotated screenshots showing how the information was extracted/gathered.