Lab Assignment

Cybersecurity Professional Program

Digital Forensics &
Incident Response

Introduction to DFIR

DFIR-01-L2
Data Leak Investigation

Lab Objective

Understand how a hash comparison is performed on investigated files and how data can be extracted from images.

Lab Mission

Recover files from a suspicious USB drive image and prove they were used to steal sensitive data.

Lab Duration

20 – 30 min

Requirements

- Basic understanding of storage devices.
- Basic knowledge of file recovery and metadata.

Resources

- Environment & Tools
    - VirtualBox
        - Windows 10
            - PhotoRec
            - HashMyFiles
            - ExifTool

- Extra Lab Files
    - Evidence.zip
    - testdisk-7.2-WIP.win.zip
    - hashmyfiles-x64.zip
    - exiftool-11.81.zip

Textbook References

- Chapter 1: Introduction to DFIR
    - Section 4: DFIR Toolset
    - Section 5: DFIR Use Case

Lab Task

A data leak occurred in your organization. The CEO gave you a formatted flash drive that was found lying around and said it was suspected of having been used to leak sensitive documents. The CEO asks you to find the original leaked files and the owner of the drive.

Recover the data from the drive and find the drive's owner.

The "Evidence" folder contains the image that was leaked and a raw copy of the flash drive. Recover the leaked image, analyze the metadata of the image to see if it matches the leaked file, and get the owner's information.

1. Make sure Windows VM is running.
2. Drag all the provided files to the machine and extract all the compressed files.
3. Extract the data from the raw drive image file.
4. Compare the hash of the leaked file and the suspected files to verify they are the same.
5. Try to find any data that can lead to the owner of the drive.
6. Who is the owner of the drive?

Hints

Lab Task

- Extract the zip files by right-clicking them and selecting Extract All.
- Use qphotorec_win located in 'testdisk-7.2-WIP, for the data extraction.
- Set photorec's option to add a raw disk image and select the .dd file.
- Make sure the option 'Whole: extract files from whole partition' is selected before searching.
- Use hashMyFiles for the hash comparison.
- If the hashes are the same, the files are also the same, and the leakage is confirmed.
- Rename the ExifTool(-k) to exiftool, then move the file to the leaked evidence recup_dir.1 folder to extract data from the image.
- The command is **exiftool <image name.ext>** (ExifTool was introduced in DFIR-01).