
Disk forensics deals with the process of examining a computer hard disk drive.

While responding to incidents that involve examining a computer, the incident responders will seize the hard disk or create a disk image of the hard disk. This disk image is then provided to the analysts to locate and recover deleted files, and other artifacts of interest. These artifacts/files depend on the objective of the investigation. For example, in the case of internal financial fraud, the excel/word documents and emails will be important, whereas, in the case of a breach, the access logs and config changes to make access persistent will be important.

**What will you learn?**

- Creating a disk image from the provided evidence disk
- Mounting a disk image for analysis
- Carving files from provided disk images

**References:**

1. The Sleuth kit (https://www.sleuthkit.org/)
2. Foremost (http://foremost.sourceforge.net/)
3. Scalpel (https://github.com/sleuthkit/scalpel)
4. EWF Tools (https://dfir.science/2017/11/EWF-Tools-working-with-Expert-Witness-Files-in-Linux.html)

**Labs Covered:**

- Forensics Basics
  Analyze a provided disk image and discover the files present on it using The Sleuth Kit.

- File Carving (Foremost)
  Carve/extract a JPEG file present on a provided disk image using the Foremost tool.

- File Carving (Scalpel)
  Carve/extract a PDF file present on a provided disk image using the Scalpel tool.

- Bulk File Extraction
  Extract all files present on a provided disk image using the Bulk Extractor tool and locate relevant information.

- Image Acquisition (DD Tools)
  Create a disk image of the provided evidence hard disk using DD tools.

- Image Acquisition (EWF Tools)
  Create a disk image of the provided evidence hard disk using EWF tools.

- Mounting Image (Raw Mount)
  Mount a provided evidence hard disk image using native Linux tools.

- Mounting Image (EWF Mount)
  Mount a provided evidence hard disk image using EWF tools.

- Mounting Disk Image (Raw mount)
  Mount a provided evidence hard disk image using native Linux tools.

- Mounting Disk Image (Python)
  Mount a provided evidence hard disk image using Python.

Forensics Basics

Start

File Carving (Foremost)

Start

File Carving (Scalpel)

Start

Bulk File Extraction

Start

Image Acquisition (DD Tools)

Start

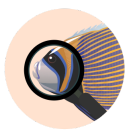

Image Acquisition (EWF Tools)

Start

Mounting Image (Raw Mount)

Start

Mounting Image (EWF Mount)

Start

Mounting Disk Image (Raw mount)

Start

Mounting Disk Image (Python)

Start