

Lab 1: Acquisition of Digital Evidence

Overview

This laboratory session is designed to provide learners with practical experience in the acquisition of digital evidence. Participants will employ AccessData's FTK Imager to:

1. Create a forensic disk image in Expert Witness Compression Format (E01).
2. Capture volatile memory (RAM) from a live system.

Pre-Lab Preparation

Participants should:

- Review Chapters 3 and 4 of *Casey, E. (2011) Digital Evidence and Computer Crime* regarding acquisition theory.
- Ensure familiarity with Windows command-line basics.
- Have FTK Imager installed on the host workstation (Already installed in the UWTSD lab)
- Bring a USB drive (min. 16 GB) for image storage.

Workshop Activities

Creating a Forensics Image

1. Initial Setup:

- Connect the target device to the host via a hardware write-blocker.
- Launch FTK Imager with elevated privileges.

2. Image Configuration:

- Navigate to File > Create Disk Image.
- Select Physical Drive (or Logical Drive) and choose the target device.
- Select E01 as the image type.
- Define the destination directory and filename (e.g. Case1234_USB_E01).

- Enable Verify images after they are created and select SHA1 and SHA2 verification.
 - Enter examiner's details in the *Case Information* dialogue.
3. **Commence Acquisition:**
- Click Start, observe the acquisition progress bar.
 - Upon completion, record the MD5 and SHA1 hash values in the log template.

Capturing RAM

1. **Preparation:**
- Ensure minimal background processes to reduce contamination.
 - Confirm sufficient storage space on the destination drive.
2. **Memory Capture:**
- In FTK Imager, select File > Capture Memory.
 - Specify an output path (e.g. Case1234_RAM_YYYYMMDD.raw/E01/AFF).
 - Click Capture.
 - Wait for confirmation and note the file size and duration.
3. **Post-Acquisition Integrity Check**
- Use *Tools > Hash Hash Values* to generate an SHA1 checksum.
 - Append the hash to the acquisition log.