# MODULE 02 Computer Forensics Investigation Process LAB REPORT

Lara Alofi

2110886

Y

Computer Hacking Forensic Investigator (CHFI)

Lab Session Identifiers

1. <https://eccouncil.learnondemand.net/Lab/Launch/65580?AssignmentId=1454946&lang=>

Username on EC-Council System

1. 2110886@uj.edu.sa

A screenshot of a computer

Description automatically generated

Lab 1 - Recovering Deleted Data from a Windows Hard Drive

**Objective:**

The purpose of this lab was to explore how to recover files that were permanently deleted from a Windows system, using the **EaseUS Data Recovery Wizard** tool.

**Step-by-Step Breakdown:**

1. **Initial Setup:**
   * I logged into the **Windows 11 virtual machine** and copied two files: **Financial Statement Sample.pdf** and **Profit and Loss Statement Sample.xlsx** to the **Forensic Disk (F:)**.
   * To simulate permanent deletion, I used **Shift+Del**, ensuring the files wouldn’t be sent to the Recycle Bin.
2. **Preparing for Recovery:**
   * Before starting the recovery process, I created a folder called **Recovered Files** in the **Documents** directory, which would serve as the destination for any files I recover.
3. **Installing Data Recovery Tool:**
   * I located the **EaseUS Data Recovery Wizard** installer, launched it, and completed the installation. I ignored any updates or unnecessary pop-ups along the way to stay focused on the recovery task.
4. **Scanning the Hard Drive:**
   * After launching the tool, I selected the **Forensic Disk (F:)** and initiated a scan for lost data. The tool ran two types of scans: a **Quick Scan** followed by a more thorough **Advanced Scan**.
   * Once the scans were finished, I saw a list of **Lost Files** and **Existing Files**, clearly separated for easy navigation.
5. **Previewing Deleted Files:**
   * I opened the **Deleted** folder within the **Lost Files** section and found the file **Financial Statement Sample.pdf**. I previewed it using the built-in feature, which showed me a partial glimpse of the document.
6. **Recovering Files:**
   * Using the recovery option, I restored both **Financial Statement Sample.pdf** and **Profit and Loss Statement Sample.xlsx** to the **Recovered Files** folder I had set up earlier.
   * The software organized the recovered files neatly in a structure under **Recovered -> Forensic Disk (F:) -> Lost Files -> Deleted**.
7. **Confirming Recovery:**
   * After the recovery was completed, I manually navigated to the **Recovered Files** folder to ensure that the files had been successfully restored and were accessible.
8. **Finishing Up:**
   * With the recovery complete and verified, I closed the **EaseUS Data Recovery Wizard** and all other open windows to wrap up the lab.

Lab 2 – Performing Hash or HMAC Calculations

**Objective:**

The goal of this lab was to learn how to compute hash values for files and text, and use them to check the integrity of the data, as well as to search for malware traces using online databases like **VirusTotal**.

**Step-by-Step Breakdown:**

1. **Setting up the Environment:**
   * I logged into the **Windows Server 2022 virtual machine**, ensuring that the network settings allowed visibility to other devices.
2. **Locating Evidence Files:**
   * Navigated to **E:\CHFI-Tools\Evidence Files\Image Files** to access the files we needed to compute hash values for.
3. **Installing HashCalc:**
   * I installed **HashCalc** by following the standard installation steps. After finishing, I launched the tool directly.
4. **Computing the Hash for a File:**
   * From **HashCalc**, I selected **File** as the data format and chose an image file named **Kitty.jpg** from the **Image Files** folder.
   * After selecting the file, I deselected the **HMAC** option to calculate regular hash values.
   * I picked the desired algorithms (e.g., **MD5**, **SHA1**, **SHA512**) and clicked **Calculate**. The hash values for the image file were then displayed on the screen.
5. **Calculating HMAC for a File:**
   * I enabled the **HMAC** option to generate a Keyed-Hash Message Authentication Code.
   * Using **Text String** as the key format, I entered a key ("test") and selected several algorithms (e.g., **MD5**, **SHA1**, **SHA512**) for the calculation.
   * Clicking **Calculate** displayed the corresponding HMAC values for **Kitty.jpg**.
6. **Hashing a Text String:**
   * Switching the **Data Format** to **Text String**, I entered a custom string ("Hello David, how have you been?").
   * After selecting the necessary algorithms, I calculated the hash values for the text string, which appeared immediately.
7. **Hashing and Verifying a Malicious File:**
   * The next task was to hash a file named **Infected.pdf**, located in **E:\CHFI-Tools\Evidence Files**.
   * I selected **File** as the data format and located the **Infected.pdf** file. After choosing it, I clicked **Calculate** to generate the hash values.
   * Once the MD5 value was displayed, I copied it and opened **VirusTotal** in Firefox.
8. **Checking the MD5 Hash on VirusTotal:**
   * I pasted the MD5 hash of **Infected.pdf** into the **VirusTotal** search bar and pressed enter.
   * VirusTotal analyzed the hash and showed that the file was flagged as malicious by multiple anti-virus engines.
9. **Verifying Hash Results:**
   * The lab demonstrated how hashing and HMAC techniques can validate file integrity and identify potential malware by comparing the hashes against known databases.

Lab 3 – Comparing Hash Values to Verify File Integrity

**Objective:**

The purpose of this lab was to gain hands-on experience in calculating MD5 hash values for files and comparing them with pre-existing hashes to ensure data integrity. This process is critical for forensic investigations, helping verify whether files have been tampered with or modified.

**Setting up MD5 Calculator:**

* I logged into the Windows Server 2022 virtual machine and navigated to the MD5 Calculator setup location at:  
  E:\CHFI-Tools\CHFIv11 Module 02 Computer Forensics Investigation Process\Hash Value Calculator Tools\MD5 Calculator.
* I installed MD5 Calculator by following the wizard-driven setup process and ensured that the tool launched upon completion.

**Computing the MD5 Hash for a File:**

* In the MD5 Calculator window, I selected "Add Files" from the menu bar.
* I navigated to E:\CHFI-Tools\Evidence Files\Image Files and chose the file peacesign.jpg for hashing.
* After selecting the file, I clicked "Calculate" to generate the MD5 hash value for the image file.
* The computed hash value appeared under the "MD5 Value" section.

**Comparing Hash Values for File Integrity:**

* I opened the file Hashes.txt, located in E:\CHFI-Tools\Evidence Files\Image Files, which contained the pre-existing hash values for multiple files, including Friends2.jpg and Model.png.
* For **Friends2.jpg**:
  + I copied the hash value of Friends2.jpg from Hashes.txt.
  + Returning to MD5 Calculator, I added Friends2.jpg as a file for comparison and calculated its hash.
  + After generating the hash, I pasted the pre-existing hash value into the "Verify MD5 Value" field and clicked "Compare."
  + The two hashes matched, confirming that the file’s integrity was intact.
* For **Model.png**:
  + I repeated the process, selecting Model.png and copying its hash from Hashes.txt.
  + After calculating the current hash for Model.png and comparing it with the pre-existing value, I found that the hashes did not match.
  + This indicated a potential modification of the file, suggesting the need for further investigation.

**Verifying Results:**

* The MD5 Calculator successfully compared the hashes, and by matching or mismatching the values, I could determine if the integrity of each file was maintained.

Lab 4 – Viewing Files of Various Formats

**Objective:**

The objective of this lab was to practice using File Viewer to examine files of different formats, understand their properties, and identify any discrepancies or corruption that may require further investigation.

**Setting up File Viewer:**

* I logged into the Windows Server 2022 virtual machine and navigated to the File Viewer setup location at:  
  E:\CHFI-Tools\CHFIv11 Module 02 Computer Forensics Investigation Process\Computer Forensics Software\File Viewer.
* I double-clicked fileview.exe to initiate the installation and followed the wizard-driven steps.
* Upon completing the installation, I launched File Viewer by clicking the desktop icon.

**Opening a File for Viewing:**

* From the File Viewer main window, I selected File --> Open and navigated to E:\CHFI-Tools\Evidence Files\Image Files.
* I set the file type filter to "All files" and opened cartoon-article.jpg.
* The image file was displayed on the File Viewer screen without any issues.

**Viewing File Properties:**

* I clicked on File --> File Properties to view detailed properties of the image.
* The File Properties window showed various attributes such as the file size, creation date, and image dimensions.
* I noted the **Image Height** value as 105, confirming that the image had not been altered.

**Opening and Investigating an mp4 File:**

* Next, I repeated the process to open the file 520px-Biohazard\_symbol\_(blue).mp4 from the same directory.
* Upon opening, a pop-up stating "LTMM Error" appeared, indicating that File Viewer was unable to play the file. This suggested a possible corruption or format manipulation.
* The failure to open the mp4 file pointed to potential tampering, where the file extension may have been forcefully changed, making further investigation necessary.

**Identifying Suspicious Files:**

* The lab emphasized how File Viewer can help in identifying suspicious files and their original formats. Any files that fail to open or display unexpected behavior could be flagged for deeper analysis in future forensic investigations.

Lab 5 – Handling Evidence Data

**Objective:** The aim of this lab was to gain practical experience in utilizing the FTK Imager Forensic Platform to effectively handle and analyze forensic evidence data, ensuring proper evidence management and presentation.

**Setting Up FTK Imager:**

1. **Installation:**
   * I logged into the Windows Server 2022 virtual machine and navigated to the installation directory:

E:\CHFI-Tools\CHFIv11 Module 02 Computer Forensics Investigation Process\Evidence Handling Tools\FTK Imager

* + I double-clicked AccessData\_FTK\_Imager\_4.7.1.exe to start the installation process.
  + When prompted with an Open File - Security Warning, I clicked "Run."
  + I followed the wizard-driven steps, clicking "Next" until the installation was complete.
  + I ensured the "Launch AccessData FTK Imager" checkbox was checked and clicked "Finish" to exit the installation wizard.

**Adding Evidence Files:**

1. **Opening an Evidence File:**
   * I launched FTK Imager and clicked on "File," then selected "Add Evidence Item."
   * In the Select Source window, I chose the "Image File" radio button and clicked "Next."
   * I clicked "Browse," navigated to:

E:\CHFI-Tools\Evidence Files\Forensic Images

* + I selected Windows\_Evidence\_001.dd and clicked "Open." The path appeared in the source field, and I clicked "Finish."

1. **Exploring Evidence Contents:**
   * The contents of Windows\_Evidence\_001.dd were displayed in the left pane.
   * I expanded the directories: Evidence [NTFS] → [root].
   * I selected the "images" folder to view its contents.

**Analyzing Files:**

1. **Viewing Image Files:**
   * I clicked on an image file to examine its details and ensure it was accessible.
2. **Retrieving Deleted Files:**
   * I looked for files marked with an "X" icon, indicating deletion.
   * Upon selecting a deleted file, I clicked on the "Properties" tab to review its attributes.
   * To inspect hex values, I clicked the "HEX" option; for text values, I selected the "TEXT" option.

**Exporting Data:**

1. **Exporting Deleted Files:**
   * To save the deleted files for further analysis, I right-clicked on the selected file and chose "Export Files."
   * I selected a location (e.g., Desktop) in the "Browse For Folder" window and clicked "OK."
   * I confirmed the Export Results pop-up by clicking "OK."
   * I navigated to the Desktop to verify the exported file was saved correctly.

Lab 6 – Creating a Disk Image File of a Hard Disk Partition

**Objective:** The purpose of this lab was to understand the process of creating a disk image file of a hard disk partition using R-Drive Image, emphasizing the importance of generating duplicates of hard disks for forensic investigations.

**Setting Up R-Drive Image:**

1. **Access the Windows 11 Machine:**
   * I selected the Windows 11 virtual machine and pressed **Ctrl+Alt+Delete**.
   * I logged in with the Admin user profile by entering the password Pa$$w0rd.
2. **Network Configuration:**
   * When prompted about network discoverability, I clicked "Yes" to allow my PC to be visible to other devices on the network.
3. **Launching R-Drive Image:**
   * I navigated to the directory:

Z:\CHFIv11 Module 02 Computer Forensics Investigation Process\Computer Forensics Software\R-drive Image

* + I double-clicked RDriveImage7.exe to initiate the setup, selected "English" as the language, and clicked "OK."
  + I clicked "Run" if prompted by an Open File - Security Warning, and selected "Yes" for the User Account Control pop-up.

1. **Installation:**
   * I followed the installation wizard’s instructions until it was complete.
   * I ensured the "Launch R-Drive Image" option was checked and clicked "Finish" to open the application.

**Creating a Disk Image:**

1. **Initiating Image Creation:**
   * In the R-Drive Image GUI, I clicked on the "Create Image" option.
   * I selected the **C:** drive in the Partition Selection window to create an image of this partition, then clicked "Next."
2. **Choosing Image Destination:**
   * In the Image Destination panel, I expanded "This PC" and selected **New Volume (\SERVER22\CHFI-Tools) (Z:)** as the save location.
   * The filename was automatically generated by the application, and I selected **R-Drive Image files (\*.rdr)** from the file type dropdown, then clicked "Next."
3. **Starting the Imaging Process:**
   * In the Total operations list window, I clicked "Start" to commence the disk partition imaging process.
   * I monitored the progress bar, which indicated the percentage of completion. The imaging process took approximately 10 minutes.
4. **Completion of Imaging:**
   * Upon completion, a pop-up notified me that the image was created successfully. I clicked "OK" to acknowledge this.
   * I clicked on the three dots in the top right corner of the R-Drive Image tool and selected "Exit" to close the application.

**Verifying the Disk Image File:**

1. **Locating the Disk Image:**
   * I navigated to the **CHFI Tools (Z Drive)** to confirm the creation of the disk partition image file.
2. **File Size Confirmation:**
   * The size of the created image file depended on the amount of data stored on the C: drive.