Assignment-1

USB Access Control Investigation Using Autopsy

1. Preparation: Set Up Autopsy and Case Creation

Install and Launch Autopsy

- Ensure Autopsy is installed (latest stable version preferred).
- Launch Autopsy from your operating system.

Create a New Case

- Select "Create New Case" in Autopsy.
- Enter the case name: **DataLeakage_Investigation**.
- Set the base directory where all findings and reports will be stored.
- Add Case Number/Examiner details for traceability and chain of custody.

Add Disk Image and Configure Analysis

- Choose "Add Data Source" > "Disk Image or VM File."
- Browse to and select the image: **cfreds_2015_data_leakage_rm#1.e01**.
- When prompted, ensure the timezone is set to **Eastern Time (UTC–05:00)**. This ensures file timestamp alignment with policy hours.
- If the option for "orphan file finding" appears (for FAT/exFAT), enable it to search for deleted files.

Start Ingest/Indexing

- Select analysis modules (file type identification, timeline, recent activity, hash lookup, etc.).
- Start the ingest process to have Autopsy index and extract artifacts for review.

2. Volume Metadata Verification

Locate the USB Image in Data Explorer

File Path	Created Timestamp	Policy Window	Violation
\Secret Project Data\proposal$$secret_project]_detailed_proposal.docx	2015-03-24 09:39:15	10:00–16:00	Yes (before)

- In Autopsy's "Data Explorer" view, find your image listed under "Images."(cfreds_2015_data_leakage-rm#1.e01)

View Image/Volume Details

- Look-out for these details
- Note the following metadata:
  - **File System:** exFAT
  - **Volume/Label name?**
  - **Size:** 4 GB (sometimes given in bytes)
  - **Model:** SanDisk Cruzer Fit or Model Number
  - **Serial Number:** 4C530012450531101593

3. File System Exploration, Content, and Timestamp Analysis

Navigating and Listing File Contents

- In the "Files" view, expand the USB volume to browse directory trees and files.
- Focus on sensitive directories like ***\Secret Project Data\design*** **and \Secret Project Data\proposal.**

Example: Documention of Relevant Files and Metadata

- For each confidential file (such as [secret_project]_proposal.docx, [secret_project]_detailed_proposal.docx, [secret_project]_design_concept.ppt, etc.), right-click and choose "Properties" or observe the relevant columns for timestamps.

Example Table: File Paths and Timestamps

- Correlate these with the allowed **access window** (10:00–16:00; per policy).

4. Policy Comparison and Violation Analysis

Review Access Policies

- **Device Authorization:** Only devices labeled **"Authorized USB"** in **exFAT** may be used (Policy 1).
- **Time Restriction:** Access to confidential files allowed only between **10:00 and 16:00** (Policy 2).

Question:

Did you find any violations like Time window violations and name the file?

Compare Evidence Against Policies

- **Device Compliance:** Check if any violations happen?

Question:

What access Control Violation did you notice:

a) Access outside authorized time/ Time window violation
b) Access by unauthorized users

NOTE: please answer all questions with short explanations justifying your answers.