Digital Forensics Hands-on #4

This project consists of two parts.

Case Background

Following an ongoing cybercrime investigation, digital forensics investigators seized a laptop believed to have been used in planning a high-value theft against a private financial organization.

At first glance, the recovered directories appeared to contain ordinary images and documents. However, initial triage suggests that these files have been deliberately manipulated using advanced steganography and concealment techniques to hide operational details about an upcoming heist.

You have been assigned to analyze the confiscated data as part of the **Auburn Incident Response Team**. Your objective is to uncover any hidden information and piece together the plan behind this operation.

Files: You can download the files for this assignment **here**. You should use the **Template**we have used in previous projects to complete your report.

Evidence Overview

The recovered drive contains **two primary directories**:

1. **/Recovered_Images** — contains a collection of suspicious image files and a map layout grid.
2. **/Recovered_Documents** — contains few files that's believed to be somehow related to the heist.

You are tasked with performing a **forensic deep-dive** into both directories to uncover and interpret any concealed evidence.

Investigation Objectives

Inspect the image files for signs of tampering or hidden content. The directory contains several photographs (e.g., beach.jpg, lena.bmp, mountain.jpg, nyc.jpg) along with a grid image (grid.png).

- Examine metadata and identify anomalies. Look for comments, encoded messages, or other irregular entries.
- Apply **steganalysis techniques** (e.g., **steghide**, **stegseek**, **wordlists** or other utilities) to extract hidden artifacts. Some of these files may contain fragments of a larger composite image.
- You may need to interpret **hex, binary, or octal** representations to recover the original ASCII text.
- Use **file**, **xxd** to analyze the structure of the file and identify hidden sections or appended data (e.g., ZIP headers such as pk\x03\x04).
- Carve and extract any concealed archives discovered within the document.
- If an archive is password-protected, test the passwords you have previously recovered from the image analysis.

Reporting Requirements

You need to produce a **professional forensic report** documenting your complete investigation. Use the provided report template. Your report should include:

- **Methodology** — A clear, step-by-step explanation of your analysis process, tools, and reasoning.
- **Evidence and Findings** — Annotated screenshots or command outputs (exiftool, stegseek, binwalk, xxd, etc.) demonstrating how each artifact was discovered, *with explanations*.
- **Answers to Key Questions:**
  - Which files contained which Map Fragment?
  - What are the decoded messages contained within the images?
  - Which **city** is the target of the operation?
  - What is the **specific location and time** of the planned event?

  - What is the **getaway vehicle model, color, and license plate** associated with the operation?
  - Who are the **individuals involved**, and what are their **roles or profit shares**?
  - What is the **target item** of the heist?
  - What **password(s)** were used and what files were they used for?
- **Conclusion** — A concise summary of how your forensic analysis connects the hidden data to the suspected criminal plan.
- A **Table in Your Executive Summary** with key questions and answers***:**

Question	**Answer** (No Explanation Needed in Executive Summary Table)
Which **city** is the target of the operation?	Ex. "Scranton"
...	....
...	...
....	....
....	....

* The table should be in this exact format, 2 columns & 1 row for each question, followed by your definitive answer. Any other format or not including the table will result in a minimum deduction of 20 points.

Prerequisites

- Install stegseek : **sudo apt install -y stegseek**
- Install wordlists : **sudo apt install –y wordlists**
- Download '**passphrases.txt**' from the given files
- Copy it to the directory with .txt files that the wordlist tool uses.

sudo cp passphrases.txt /usr/share/wordlists/

- Usage: **stegseek -wl /usr/share/wordlists/passphrases.txt <stego-image>**
- Install LibreOffice (if on Kali): **sudo apt install libreoffice**

Recommended Tools

- stegseek, steghide, exiftool, wordlists, file, xxd, strings, and other standard Linux tools and libraries for data carving and encoding conversion.
- You can use online tools for encoding conversions
- https://gchq.github.io/CyberChef/

Scenario Reminder and Disclaimer

All files and names in this exercise are **fictional** and designed solely for educational purposes. This practical exercise is intended to strengthen your understanding of **steganography, file structure analysis, metadata forensics, and data recovery** in a realistic investigative workflow.

The stories, names, characters, and scenarios portrayed in this assignment are fictional. No identification with actual persons, groups, places, or products is intended or should be inferred.