Digital Forensics Project #1

Technical Analysis

For this project, you will work **INDIVIDUALLY** and focus on the analysis of **FAT16** partition, and will require an understanding of how to recover data from each properly.

Background:

APT99 orchestrated a major heist targeting the Central Bank a few days ago, exploiting vulnerabilities in the bank's digital infrastructure. During the breach, large sums of money were siphoned off into anonymous accounts, causing a significant financial impact and raising concerns about the security of national financial institutions.

Investigators have recovered a laptop believed to belong to one of the key members of APT99. Forensic experts have extracted a disk image from this laptop, named **captured_image.dd**

As a member of the forensics team of the cybersecurity force, your task is to analyze the disk image to uncover the truth behind the hack of the APT99 as soon as possible. The group's failure to securely handle their data has left traces of their communications and plans within the disk image, despite their attempts to delete the files. The disk image may contain critical evidence about the breach that can help find the criminals.

Objectives

You will need to answer the following questions as you are working on your technical analysis:

Q1) Specify the number and type of partitions on the disk image.

Q2) Specify the number of files, file names, and file size of each file on the partition.

Q3) Specify the starting and ending byte offset location of each file on the partition.

Q4) For each FAT partition explain the contents of the File Allocation Table and Root Directory.

Q5) Manually recover all files from each disk image. **Note: You must show the step-by-step process for file recovery supported by annotated screenshots. Automated file recovery tools may not be used during this project!**

Q6) Provide a thorough analysis of the recovered files: Determine the contents of these files to understand the objective, the plan, and any other critical information about the hack.

Note: Root Directory Size (sectors): 32

Final Report

You need to provide a final report using the provided **template** along with the **FAT16 Data Recovery template**. The final report should provide answers to the questions from the grading rubric.

The format of the final report will include the following sections:

1) Executive summary

2) Detailed analysis of the partition allocation and an illustration of the partition map indicating the volume size, and the number of sectors per field in the partition map.

3) Detailed analysis of the data recovery process, including annotated screenshots.

4) Description of analysis techniques utilized.

5) Detailed analysis and description of the contents of each file, and how this information is relevant to find the hackers' objectives.

The purpose of this report is to show that an effective analysis of the disk image was properly conducted. A single-page report will not adequately answer all questions so be prepared to have an in-depth analysis and description of the methods you used to answer the questions. Your work must be supported by annotated screenshots showing how the information was extracted/gathered.

Grading Rubric

The grading rubric that will be used to grade each disk image will be based on the following criteria:

Activity	%	Points
Number and type of partitions specified?	5%	10
File status, filename, extension, attributes, and file sizes specified?	10%	20
Was the byte offset for each file specified?	15%	30
Was a File Allocation Table provided?	10%	20
Were all files recovered from partitions? You need to upload the recovered files along with your submission.	35%	70
Were hiding methods specified?	15%	30
Describe what tools or applications were used to hide data	5%	10
Describe the ultimate objective of users of the laptop	5%	10
	100%	200