

MCAST

Computer Security Laboratory Project

Project #5: Digital Forensic Evidence Acquisition and Analysis

The objective of this project is to familiarize you with basic digital forensic acquisition and analysis. Your forensic investigation skills will be tested specifically on the following areas: evidence preservation and retrieval, data encryption/decryption, steganographic analysis, password recovery, file sector analysis and retrieval, and file type recognition.

Here is the scenario. Counter Terrorism Unit (CTU) agents of the EuroPol and G8 High Tech Crime Group raided a suspected terrorist hideout in Marsaxlokk and captured a single piece of digital evidence: a floppy disk. Upon examination, the CTU IT personnel found that the floppy disk is empty. Joquim Bajera, the current CTU head, had a very strong intuition that there is something in that disk. Upon hearing so many good things about the Computer Security and Forensic course at MCAST, he decided to hand over the evidence to your Computer Security course instructor and requested an immediate forensic analysis. Due to the fact that the CTU informer has indicated that some dirty bombs may have been planted around the country, this stage of the investigation is very critical and time is paramount. Thus, Joquim Bajera and your instructor have agreed to give you at most a week to complete the analysis and submit a final written and oral report.

You need to accomplish each of the following tasks and to briefly answer the question that is related to the task. You also need to document the command(s) that you used to accomplish each task.

- 1) Task: Create an image of the evidence floppy disk. Calculate its MD5 signature and save the signature in a text file. What is the importance of this step of the investigation?
- 2) Task: Gather all string information that you can find in the image. Why does the floppy disk appear to be empty? What files did you recover from the disk? How did you recover them?
- 3) Task: Break the encryption on one of the files that you managed to recover. What encryption technique was used? How did you break it? What password did you managed to reveal?
- 4) Task: Perform a steganalysis of the images. What made you infer which image is hiding some information? How did you extract the data? What information did the data reveal?
- 5) Task: Analyze the images. What information about impending attack do they reveal?
- 6) Task: Analyze the recovered files through the steganalysis procedure. Recover as many incriminating evidence as possible from those files.

Here are some notes that may prove helpful to your investigation.

- 1) To create a floppy disk image, use the utility program, dd.
- 2) For integrity checking, use the utility program, md5sum.
- 3) Some pertinent file information (header and trailer signatures):

JPEG/JPG Image file

Hex Header: FF D8 FF E0 XX XX 4A 46 49 46 00

String Header:JFIF(JPE, JPEG, or JPG).....

Hex Trailer: FF D9

String Trailer: (.)

.....

GIF87a Image File

Hex Header: 47 49 46 38 37 61

Hex Trailer: 00 3B

.....

MS Word Document

Hex Header: D0 CF 11 E0 A1 B1 1A E1

.....