

CS470

Computer Security

Laboratory Project

Forensic Evidence Analysis

Due Date:

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

Here is the scenario. Central Terrorism Unit (CTU) agents of the Department of Highest Security (DHS) raided a suspected terrorist hideout and captured a single piece of digital evidence: a floppy disk. Upon examination, the CTU IT personnel found that the floppy disk is almost empty. Jack Bummer, the current CTU head, had a very strong intuition that there was something in that disk. After hearing so many good things about the Computer Security and Forensic course at JSU, he decided to hand over the evidence to your CS470 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, Jack Bummer 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 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 almost 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 manage to reveal?
- 4) Task: Perform a steganalysis of the images. Do a research on steganalysis and write a concise report on that process. How and 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 the impending attack do they reveal?

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

- 1) To create a floppy disk image, use the Linux/cygwin 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 Excel/Powerpoint File

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

MS Word Document

Hex Header: 7B 5C72 74 66 31 5C 61

or

OD OD

MS Access File

Hex Header: 00 01 00 00 53 74 61 6E

Bitmap File (BMP)

Hex Header: 4D 42

Zip file

Hex Header: 50 4B 03 04 14