COMP 597 - Computer Forensics
Assignment #4

Spring 2017

Due Date: Monday, April 24, 2017

Total Points: 100

This assignment represents a fictitious digital investigation scenario that still offers the challenges of a real situation. Please first read the scenario described below and start learning more about the digital image (*q.dd*) that is given to you. Your job here is to conduct a forensic analysis on the given image to answer the questions below. You are going to see two main types of questions:

- open ended ones that require you to postulate one or more hypothesis and try to prove/refute them through justified use of digital evidence
- short answer questions that are practice for concepts we went through in class

You can use TSK tools, strings (UNIX based tool), hexadecimal editor, and if there is a need file signatures. File signatures are the first two to eight bytes in a file that uniquely identifies its type. Make sure to justify your answers and include all the steps you took (the commands you used) to find the results.

Scenario:

You are having an onsite interview for a job vacancy with a digital forensics enforcement agency. Your interviewer enters the room and introduces herself indicating that she is a retired police officer who was in charge of narcotic investigations. She then tells you that today's interview will be a short one since your job is to investigate a real case she worked on around fifteen years ago. She hands you an image of a floppy disk and a paper that contains several questions for you to answer. She tells you that she is expecting a digital investigation report that answers these questions, and that if you did a good job with the report then the position is yours. The deadline for submitting your report (your findings) is Monday April 24th.

She then starts describing the incident that you are going to investigate:

Several schools contacted the police department complaining about the activities of a suspicious person that is talking to their students in the vicinity of their schools. They believe he is selling their students drugs. The police responded by talking to various students from different high schools but nobody saw anything. As a result, an undercover police officer was enrolled in one of the high schools to investigate this issue and to see if there is anybody selling drugs to high school students.

Several weeks passed and the undercover agent did not report anything. Finally on one Friday, a person in his twenties approached the undercover agent while hanging out with a group of four students in the school's parking lot. The person greets two of these students and ask them if they want anything for the weekend. The students give the suspect a list of paper with money enclosed in it and they tell the undercover agent that he is going to have fun tonight. The suspect reads the list and gives them the drugs then says he needs to go to his apartment to get the rest on the list. He tells the student that he will be back in 10 minutes. The undercover agent followed the suspect carefully to the apartment. As the agent attempted to enter the room, the suspect noticed that he was being followed and directly fires two shots from his gun through the closed door of the apartment. The agent opens the door late after the suspect had escaped the apartment through the window and there was no trace of him anymore. The police then search the suspect's place and find nothing except a floppy disk.

The interviewer then tells you this is the image of the floppy disk they found in the suspect's apartment and then asks you if you have any questions. You ask her what happened with the case. She responds that this is your job to find out. She then tells you that you need to strongly justify your findings (your answers to the questions) and that you need to clearly indicate the following:

- Exactly where you found the evidence on the disk
- The techniques and processes you used to discover your findings
- A detailed analysis of the steps taken by the suspect to hide the data (if there is any hidden information)

<u>Questions:</u>

1. What is the suspect's full name?
2. Do we have any information where the suspect stores his money?
3. What type of illegal drugs is being sold?
4. Who is the suspect's supplier? Give any relevant information about the supplier.
5. Is the suspect involved in selling drugs in other schools or just the school that the undercover agent was enrolled in? If there are more, then list all the details you find.
6. Are there any hidden files, hidden information or files that were modified to prevent you from accessing them? What was hidden and how did you uncover it?
7. If there is any word document in the image, then which Microsoft Word version was used?
8. What type of FAT system is this?
9. What is the maximum FAT entries that this file system supports?

10. Is there a backup for the boot sector?
11. Draw the file system layout.
12. Using the FAT structure, how many files are there?
13. Fill in the following table by going through the boot sector using a hex editor:

Description	***Value***
OEM Name in ASCII.	
Bytes per sector	
Sectors per cluster	
Size in sectors of the reserved area.	
Number of FATs	
# of Directory entries in root	
Number of sectors in file system	
16-bit size in sectors of each FAT	
Number of sectors before the start of partition.	
Number of sectors in file system	
Volume serial number (hexadecimal value)	
Volume label in ASCII	
File system type label in ASCII	

What to hand in

Submit your project electronically through Canvas. Please hand in the following:

- Your report. Make sure that you explain the steps you took, and the commands you wrote in order to answer each question.
- In addition to the contents of the reports, the grade will also be based on their readability and formatting/presentation.