CCSI 410 Forensic Lab Report

1) Investigator’s Name: \_Matt Ferry\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2) Date of Investigation:\_08/24/2013\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3) Lab Number and Title: \_7 File and Data Recovery\_\_\_\_\_

4) Summary of Findings:

*Answered the questions for the lab assignment, after examining the floppy image of the suspect it is clear that there is enough evidence to support the allegation that the suspect has been blackmailing people, and that the investigation should continue.*

5) Details of Investigation

**August 21, 2013**

 **12:35 pm Launching lab and beginning investigation of files**

**For this assignment we are looking for evidence of blackmail.**

**12:40 pm Detected “Other Known types” : 3 items detected that all link to deleted file letter.doc , which is attempting to blackmail Mrs. Thomas to pay $10,000 or else have her love letters revealed to her husband. The letter is signed “The Love Letter Bandit” This file also shows up in documents of FTK.**

 **Under detected documents, there is a file letter.txt claiming to have Mr. Travis cat, and demanding $2000 in return for the cat. Signed “The Cat Napper”**

 **Both detected files thus far tell the victim to meet them under a bridge at midnight.**

 **Most of the detected files show the deleted icon next to them indicating that the suspect tried to erase this information.**

6) Please type the answers to the questions found throughout the lab here.

**Question 1: You are given an .001 file for this investigation. What is the difference between a .001 file and the actual physical floppy disk? What must have happened prior to this step?**

**A .001 file is a bit copy image of the floppy disk. In order for this to have happened it must have been bit copied and then had its hash value compared to a hash value of the original floppy.**

**Question 2: On the Processes to Perform page, you were asked if you would like to perform a KFF Lookup. What is a KFF lookup and when is it important?**

A kff lookup is a known file filter lookup that searches md5 hash values of files against a database of known file hash values. This will allow the investigator to either eliminate files from importance, as the files are already known as legitimate program files, or locate files of interest due to matching hash values of already known illegal files.

**Question 3 - Is there any evidence on the suspect’s floppy disk? Would you see this evidence just looking at the floppy using Windows Explorer? Why or Why not? What other tools could you use to retrieve the evidence?**

Yes, there is evidence on the suspect’s disk. No, you would not see this evidence by just looking at the floppy using Windows Explorer. FTK has the files marked as deleted files, which means windows explorer would not recognize the files. Any utility that is capable of reading the bit copy image of .001 would be capable of accessing information on this floppy image, such as sleuth kit.