CIS2376 PRACTICAL

Week 10

Questions

This week, you are to use Sleuthkit to examine and build a case based on the attached police report. Please be aware that this weeks work will require you to:

- understand and use the FAT file system
- perform some file carving
- validate the use and presence of stenography

Police Report

As a result of the information collected from the previous floppy disk case (see week 9), Jimmy Jungle was identified as the probable supplier of marijuana to Joe Jacobs. Jungle's address was also identified within the findings. Jacobs was again detained and offered the option to plead guilty to a single lesser charge in exchange for reliable information about his supplier of marijuana. Without knowing what police had already found on his disk, Jacobs agreed to plead guilty to the lesser charge and in turn provided police with the name and address of his marijuana supplier. The information Jacob's provided and the findings from week 9 matched exactly. Jacobs also noted that he missed a scheduled face-to-face meeting with Jungle because his arrest occurred on the same day. Since his arrest, Jacobs has had no contact with Jungle and fears Jungle may have become suspicious as a result of their missed meeting. Jacobs also noted that Jungle is fairly computer savvy and any *alterations* made on his disk were a result of Jungle walking him through the process step-by-step.

Once again the police need your help. Armed with the necessary search warrants, police raided suspect Jimmy Jungle's residence. Upon entering the residence, police found no indications that anyone currently occupied the house. There was no furniture, clothing beds, etc. However, there was a single floppy diskette lying on the floor in the only upstairs bedroom, a URL was written on the outside of the disk (a copy of the page at that link is in `~/Examples/dfrws.org.html`.

The police have imaged the floppy disk found on the floor and have provided you with a copy[1] along with its hash:

`4e6a80a46e1358c5589cd8bd9b48ed8c19b29ab3`.

They would like you to examine the floppy disk and provide them with as much information as possible. Afraid that Jungle is on the run and has been tipped off, police would like to obtain as much information about him as soon as possible.

[1] A copy is available in `~/Examples/scan26.dd`.