ITIS 4250 / 5250

Gregory Ododa

Lab #4

10/10/2017

**Overview:**

It is believed that a criminal has acquired schematics for technology he plans to sell off to a competing company's representative. The purpose of this forensic examination is to provide conclusive proof for management and company attorneys that someone is stealing technology using a CD left behind.

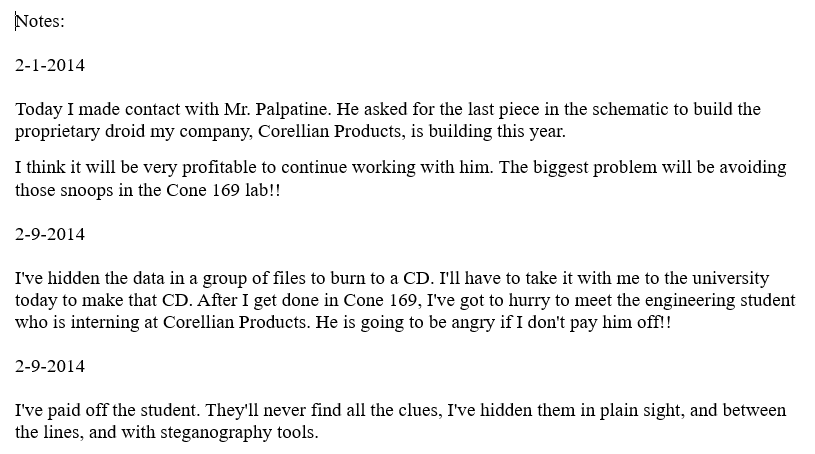
**Forensic Acquisition & Exam Preparation**

The first step I took was to make a copy of the CD and saved it to a folder on my desktop so that I can fully examine it without fear of damaging the evidence.

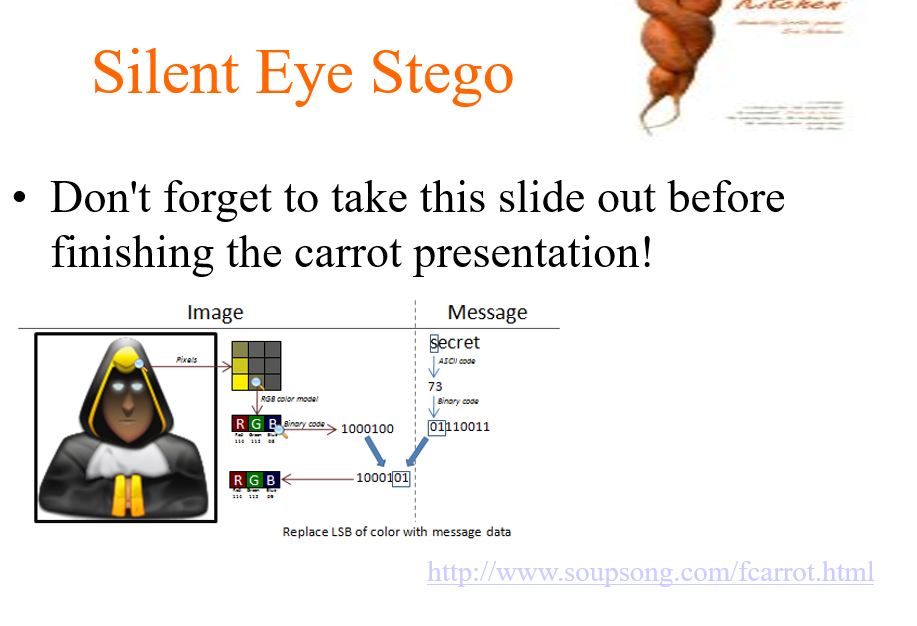
I then used FTK Imager to open and examine the copy of the file. I also discovered the use of a steganography tool called Silent Eye which I used to further uncover information from the image.

**Findings and Report (Forensic Analysis)**

Luckily the image did not contain a large number of files, it consisted of a few images, an HTML (Hypertext Markup Language) Webpage, a PowerPoint presentation and a word document. The first file that I opened was the word document, which contained a journal that included a fairly detailed description of the suspects criminal activity. The most valuable information for my examination was in the February 9th 2014 entry in which he said that he used steganography tools to hide the information in plain sight, which is what the purpose of steganography tools is. This told me that to find the stolen information, I needed to closely examine the disk for the smallest clues that could provide the password and tool settings used to hide the information. Below is the word document:



Next, I examined the PowerPoint presentation. Below is a slide that was meant to be deleted:



This unveiled which tool (Silent Eye) was used to hide the stolen information. I then downloaded the program in preparation to decrypt one of the image files on the image. The image files were all JPEG except for one that was JPG so that gave me a clue that the JPG file was the one with the hidden file, that, and the fact that it had the largest file size. JPG and JPEG stand both for an image format proposed and supported by the Joint Photographic Experts Group with the only difference being that JPG is a newer version. I later found that Silent Eye only accepts JPG so that is also why I had reason to believe that it is the file containing the stolen file.

Next I opened the RootFoods.html file. There was nothing out of the ordinary on the page, however when I looked at the source code revieled the password for decoding the image with Silent Eye: 

The final line gives a hint that the password is in the comments, sure enough the password ‘droids’ was in quotes:



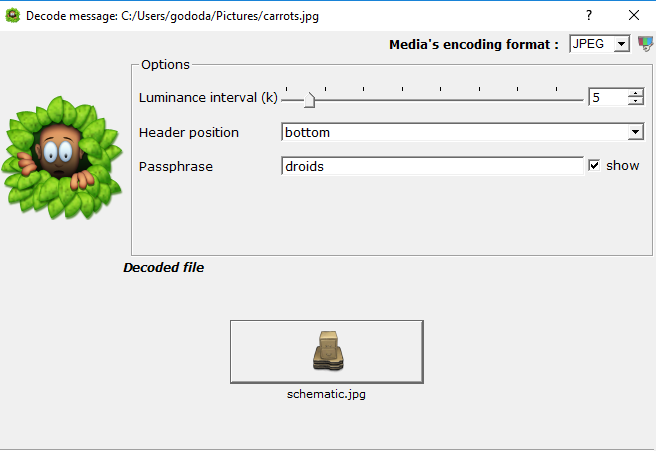
At this point I had the password as well as an idea of which file was hiding the stolen information. However, without the proper settings for Silent Eye, this information is useless.

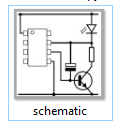
The settings were hidden inside the UNTITLE6 file. I found the settings by opening the file in notepad and found a hidden line stating the tool used and the settings for the decryption:





After applying all known information the hidden schemaric.jpg file was uncovered:





Below are the hashes for the schematic and carrots file (The file containing the schematic):

**Conclusion:**

The files on the image included a journal documenting the suspects illegal activities, a PowerPoint slide that was meant to be deleted that stated the tool used to hide the stolen information, clues in the webpage source code that lead to the password used in Silent Eye, and the settings used to hide the stolen file in Silent Eye was located in the UNTITLE6 file. Using all these clues I uncovered the stolen schematic file hidden within the carrots.jpg file using the steganography tool Silent Eye.