ITIS 5250

Ruchira Pokhriyal

Lab 4

10/30/2018

**Overview**

In this lab, I will be uncovering certain hidden information from the provided image using FTK (Version 6.3.0.186). Additionally, I will be extracting hash value of the found schematic evidence.

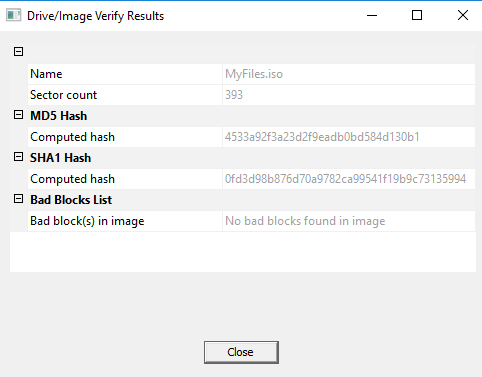
**Forensic Acquisition & Exam Preparation**

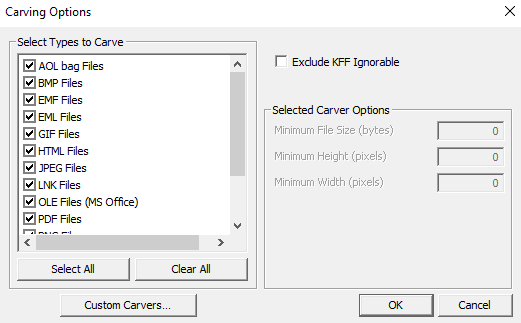
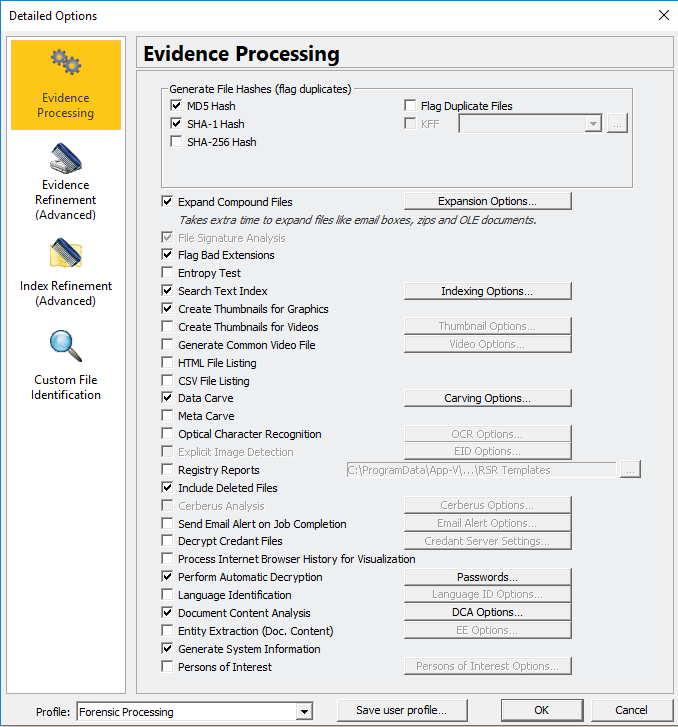
I loaded the provided forensic image **“Myfiles.iso”** into FTK Imager to verify the hash values used FTK for evidence processing.

**Hash Results:**

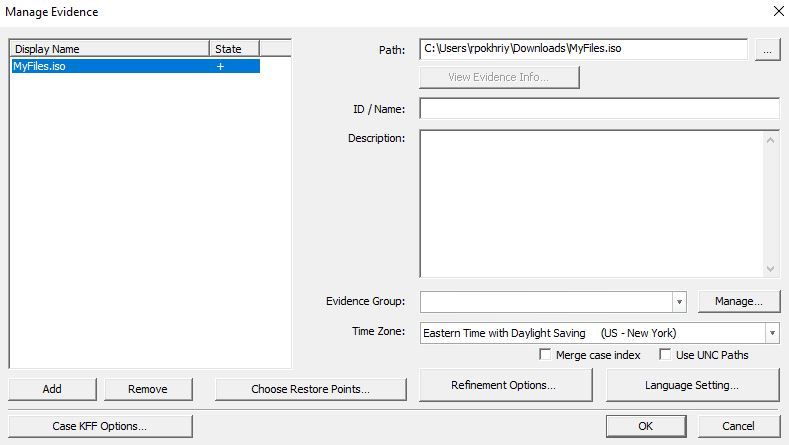
**MD5 Hash Value: 4533a92f3a23d2f9eadb0bd584d130b1**

**SHA1 Hash Value: 0fd3d98b876d70a9782ca99541f19b9c73135994**



**Evidence Processing using FTK:** **Carving Options:**

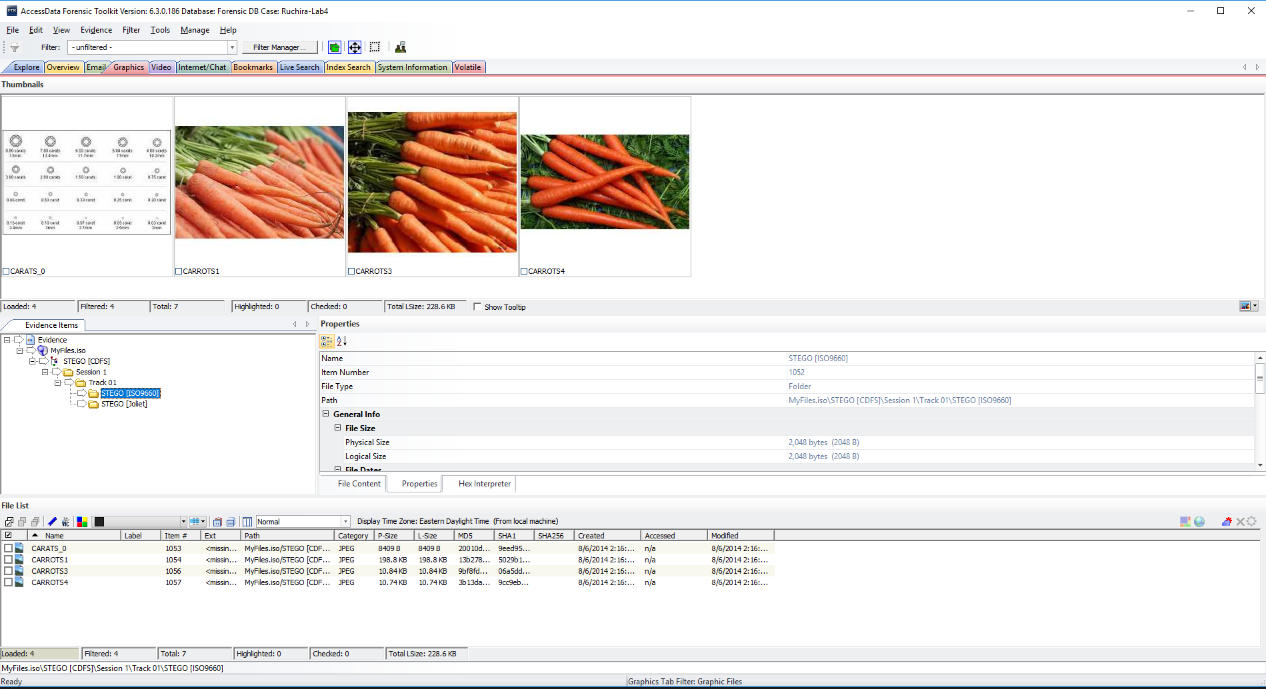
**Adding Image:**



**Findings & Report (Forensic Analysis)**

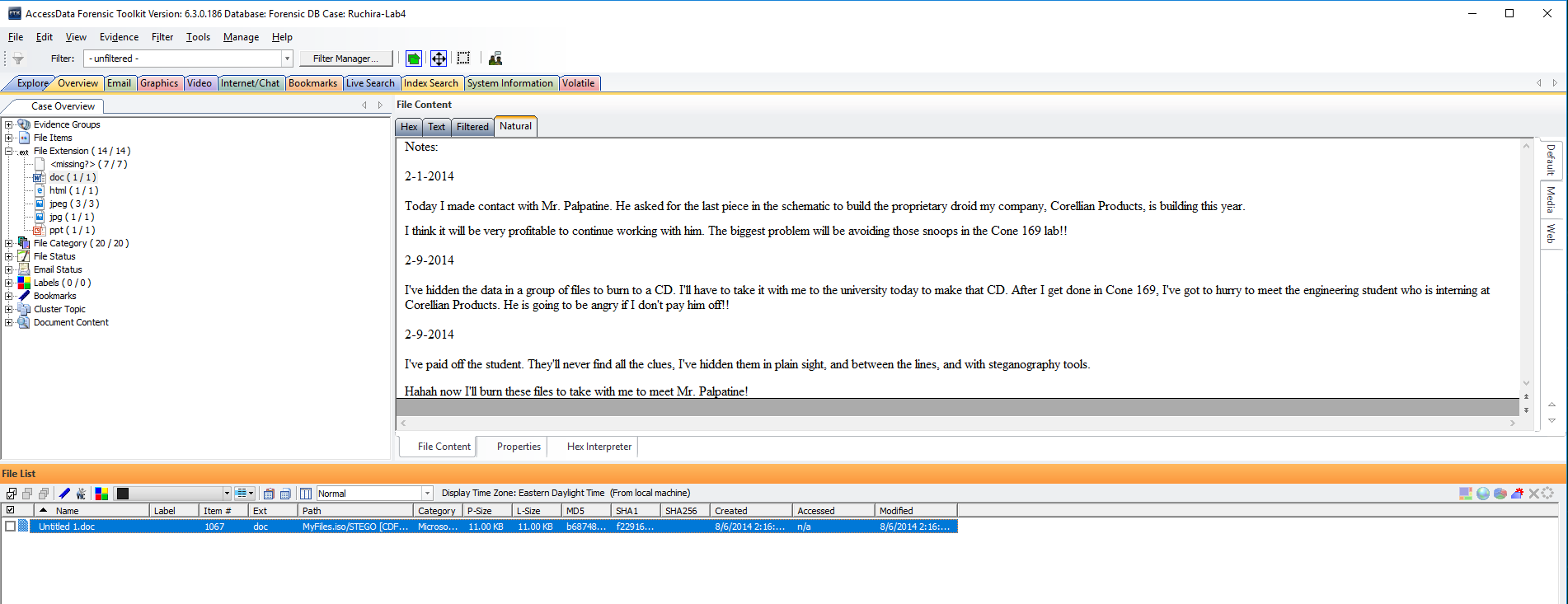
After loading the image into FTK, I began examining it to find any hidden information relating to the recovery of the schematic. In the Graphics tab, under **‘Evidence Items’**, I found four pictures: **CARATS\_0.jpeg, CARROTS1.jpeg, CARROTS3.jpeg, CARROTS4.jpeg**

**(Path: Myfiles.iso/STEGO [CDFS]/Session 1/ TRACK 01/STEGO [ISO9660])**



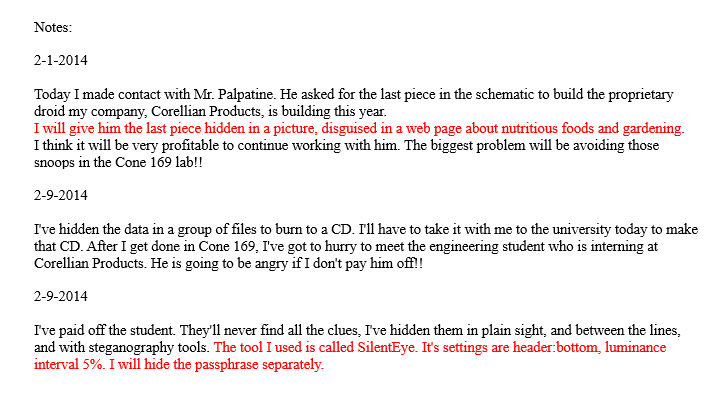
In the **‘Overview’** tab, I found the following word document (Untitled 1.doc), which mentions that the clues have been hidden in plain sight and between the lines and with steganography tools.

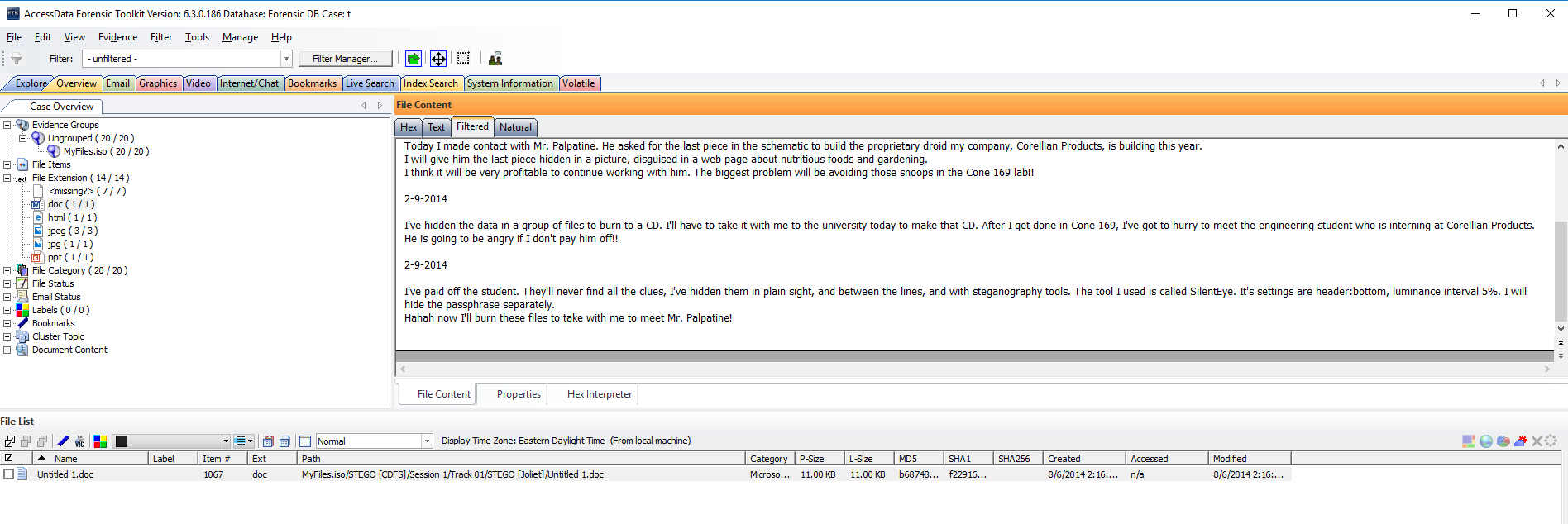
(Path: Myfiles.iso/STEGO [CDFS]/Session 1/ TRACK 01/STEGO [Joliet]/ Untitled 1.doc )



This clue made me have a closer look at the document and I uncovered two clues. The first clue was hidden between the second and third sentence and read: ‘I will give him the last piece hidden in a picture, disguised in a web page about nutritious foods and gardening.’

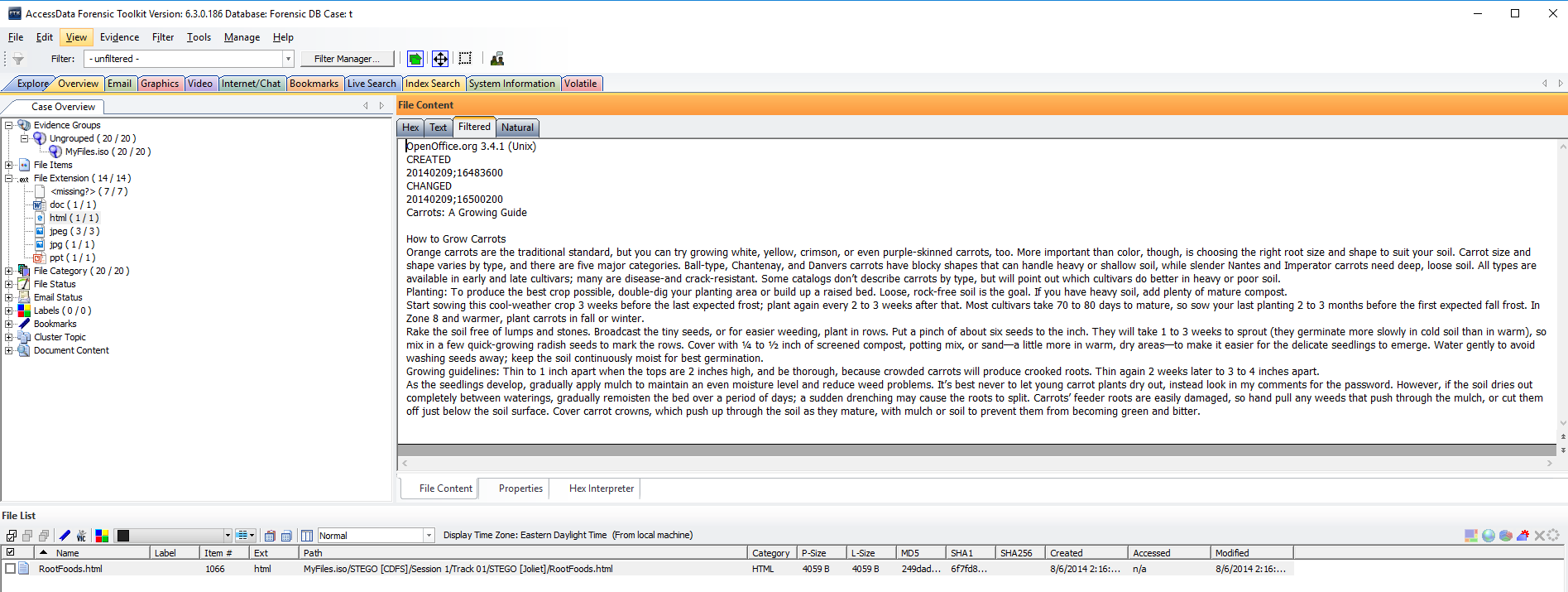
The second clue is hidden after the last sentence and specifies that the steanography tool used is ‘SilentEye’. It reads as follows: ‘The tool I used is called SilentEye. It’s settings are header: bottom, luminance interval 5%. I will hide the passphrase seperately.’



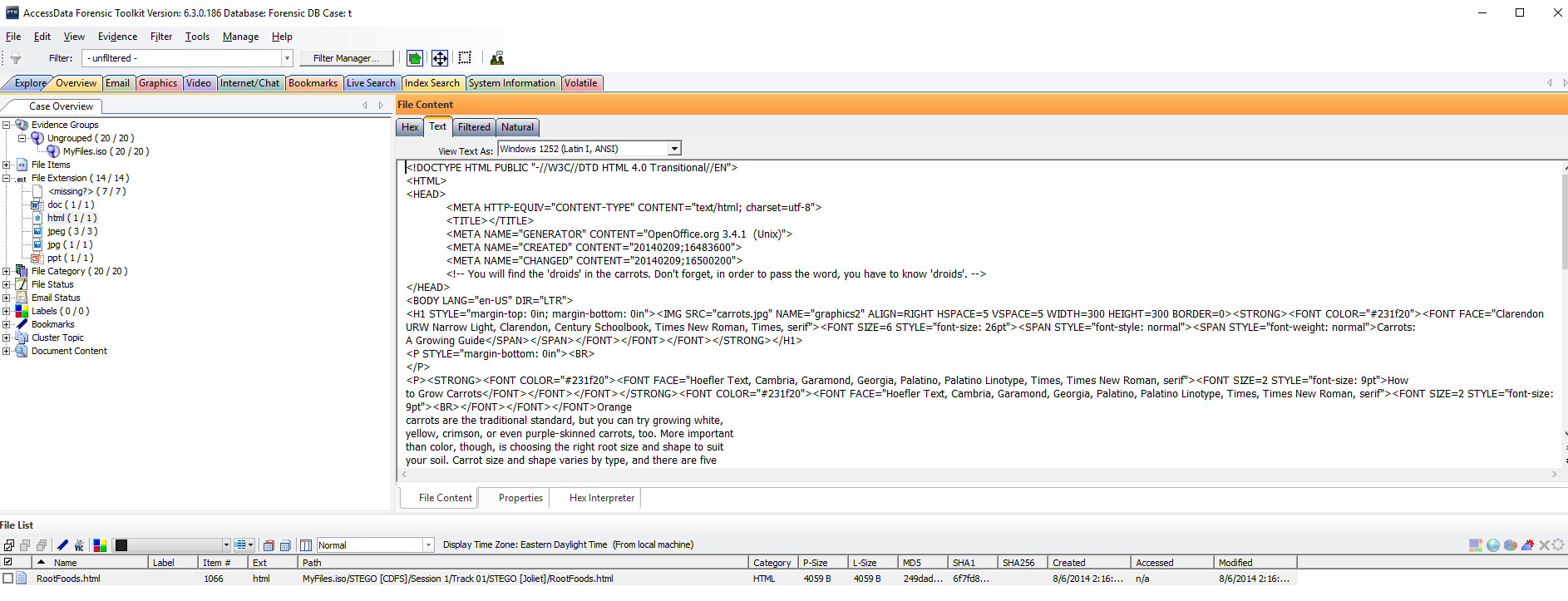
I could view the same details as mentioned above in the ‘filtered’ mode for **‘Untitled 1.doc**’:

Following this clue, I found an **html** document which mentions ‘looking at the comments for the password’:

(Path: Myfiles.iso/STEGO[CDFS]/Session 1/ TRACK 01/STEGO [Joliet]/ RootFoods.html)

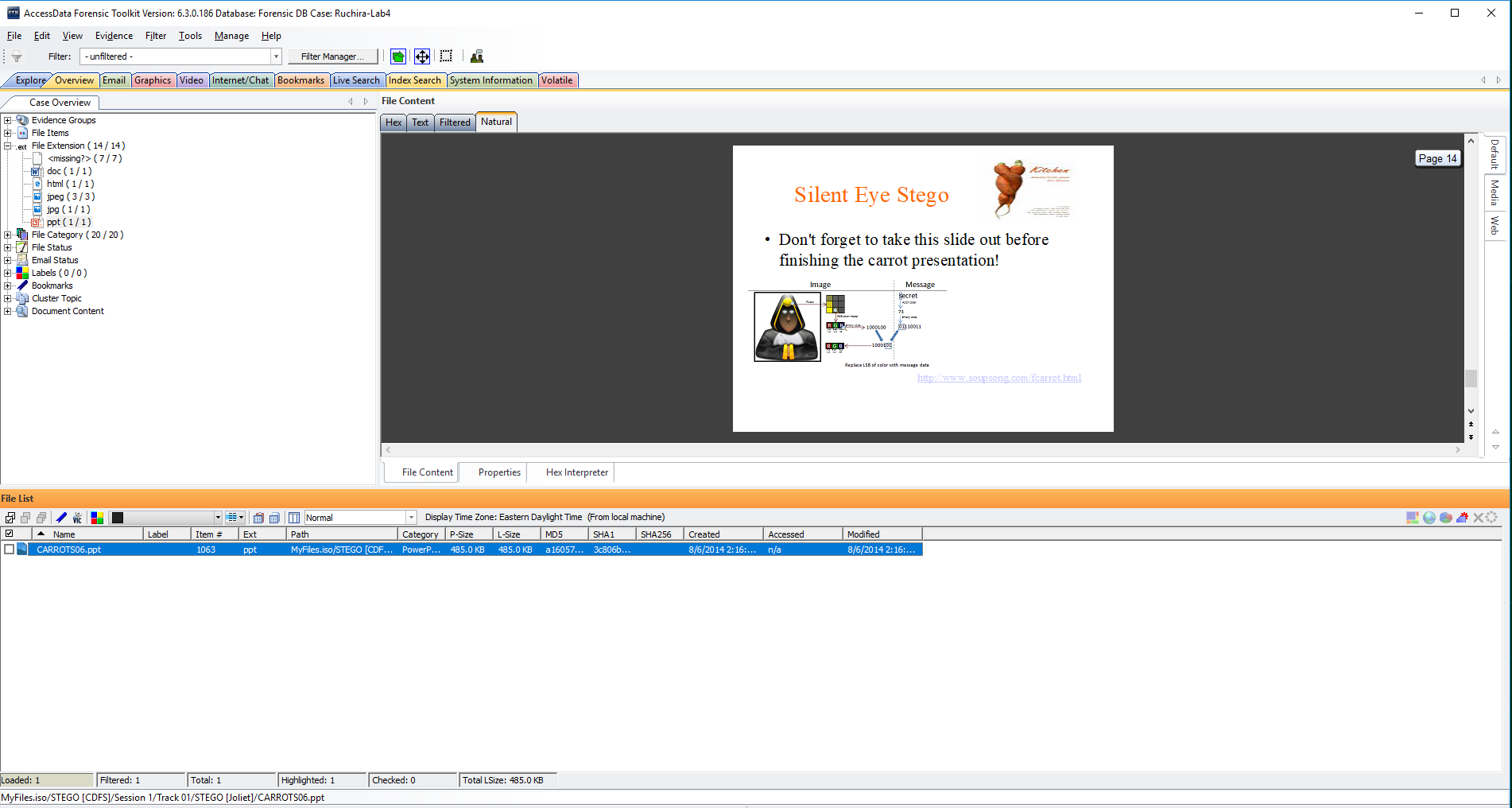


Reading the html page in text mode revealed that the password is the word **‘droids’:**

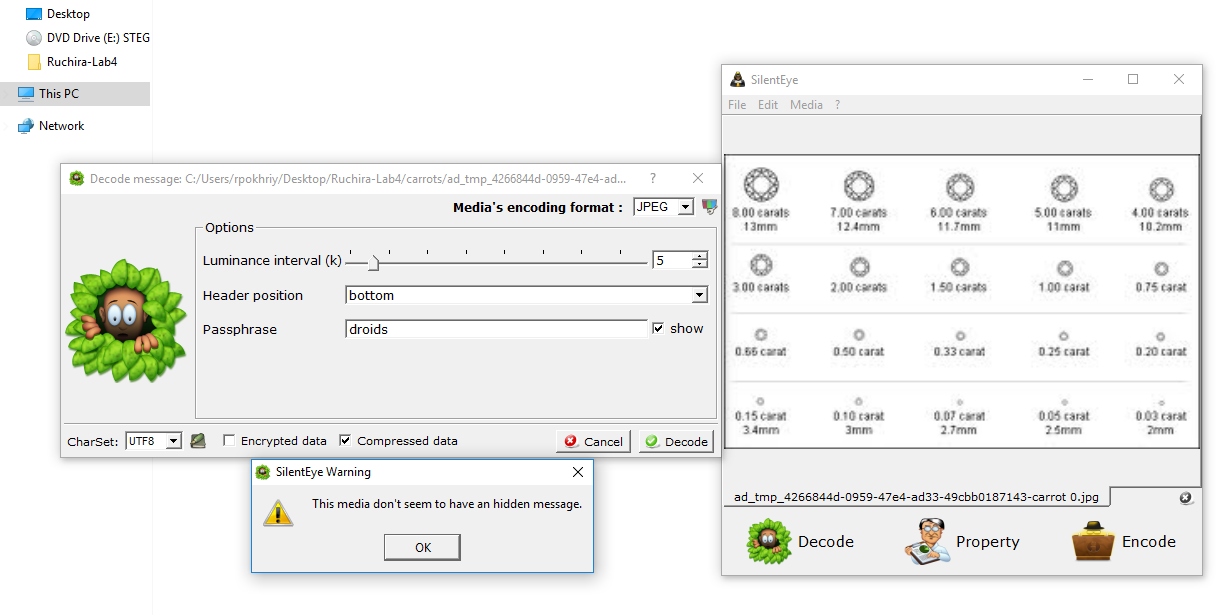


Upon further investigation, I found a **.ppt** file, which mentions the steganography tool **‘SilentEye’**.

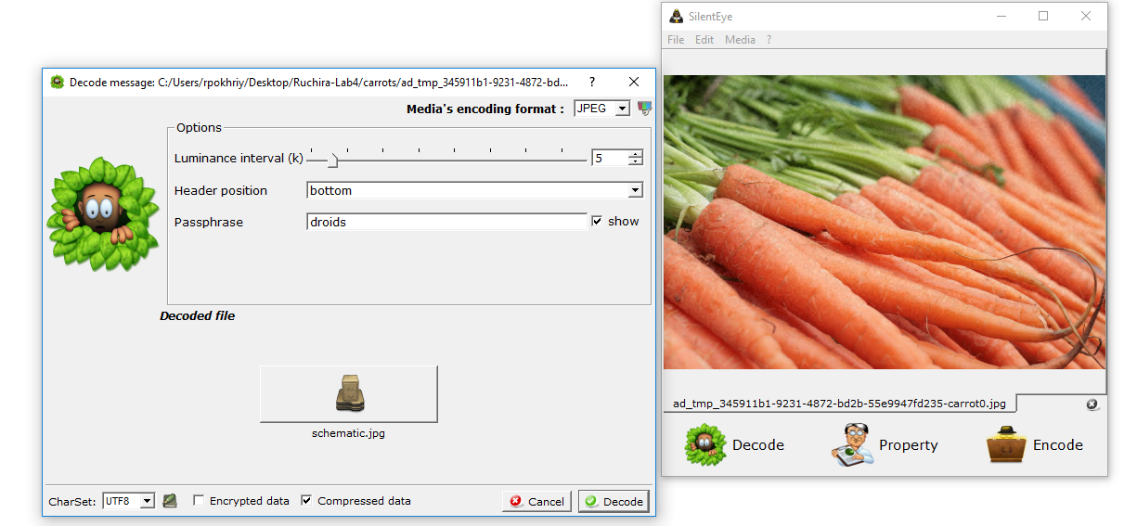
(Path: Myfiles.iso/STEGO[CDFS]/Session 1/ TRACK 01/STEGO [Joliet]/ CARROTS06.ppt)



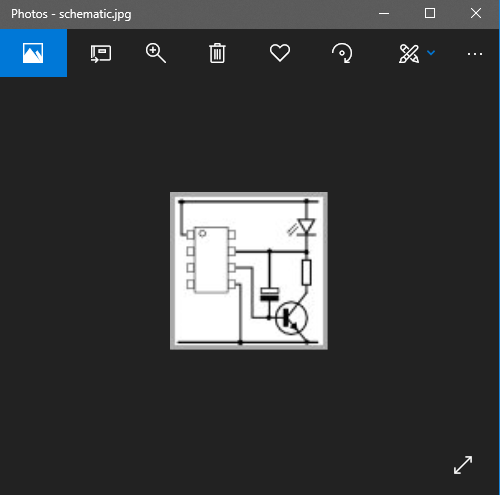
To check if there’s any secret message hidden in the picture ‘CARATS\_0.jpeg’, I dragged it into the **‘SilentEye’** tool and tried decoding it using the passphrase **‘droids’**, found earlier. However, the tool did not detect any hidden message in the picture ‘CARATS\_0.jpeg’.



Then, I checked if the schematic is hidden in the picture ‘CARROTS1.jpeg’. As shown below, after dragging ‘CARROTS1.jpg’ into **‘SilentEye’** tool, I decoded and found that a file named **‘schematic.jpg’** was hidden inside it.

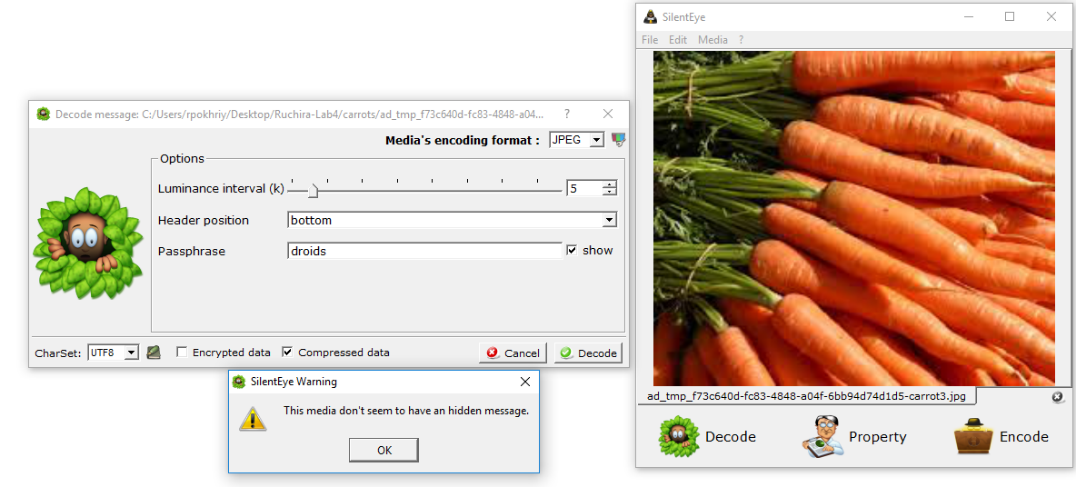


**schematic.jpg:**

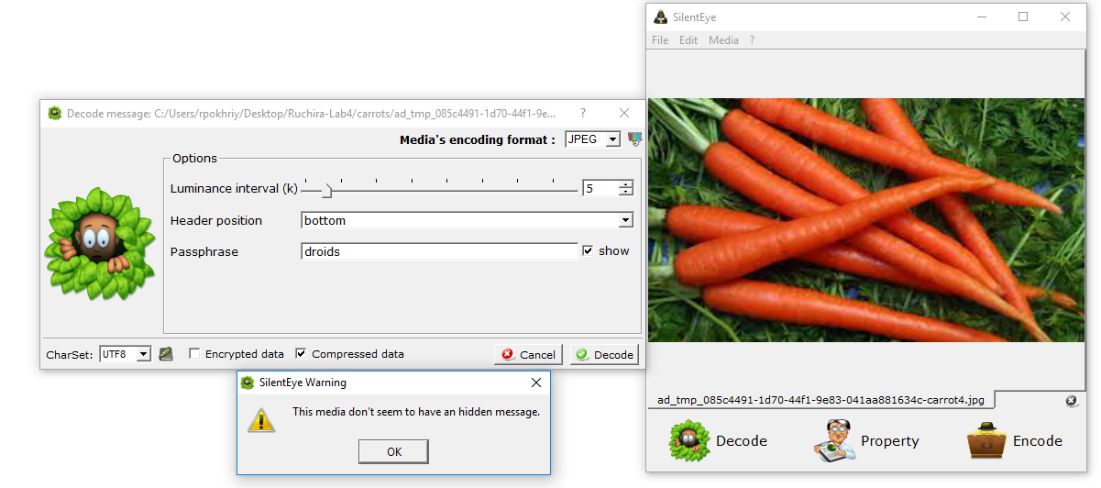


Similarly, I used **‘SilentEye’** tool to check for any hidden messages within pictures: **‘CARROTS3.JPEG’** and **‘CARROTS4.JPEG’**. As shown below, the tool did not detect any hidden messages for these two pictures:

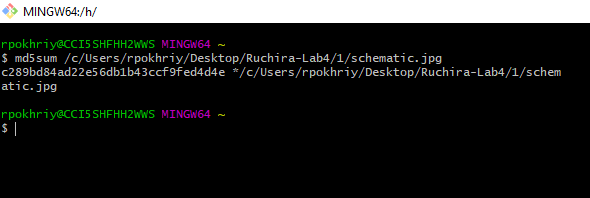
‘**CARROTS3.JPEG’:**



**‘CARROTS4.JPEG’:**



Finally, I used ‘**git bash’** to find the hash value ofthe schematic. As shown below, the hash value of **‘schematic.jpg’** was found to be: **c289bd84ad22e56db1b43ccf9fed4d4e**.



**Conclusion**

I examined the given image file **‘MyFiles.iso’** and found: a few pictures, a .doc file, an html page and a .ppt file leading me to uncover that the steganography tool used is **‘SilentEye’** and the password is **‘droids’**. The ‘SilentEye’ tool further helped me recover the schematic hidden in a picture **‘CARROTS1.jpeg’**. Additionally, I calculated the hash value of the schematic file using **‘git bash’**.