ITIS 4250 / 5250

Shivani Sathe

Lab # 6

16th November 2021

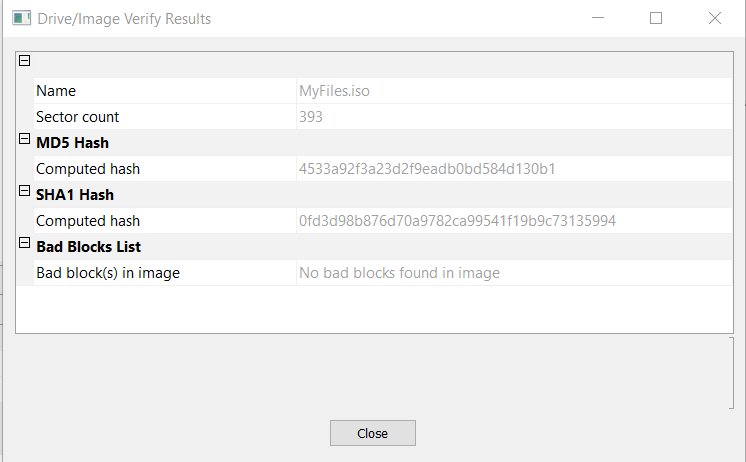
**Overview:**

On 16th November 2021, Dr. Quincy provided me a forensic image of a CD and a UNCC Attorney, Vincent Gambini. Mr.Gambini was concerned about a matter of intellectual property theft that cropped up a few years ago and was headed to litigation. It turned out the original examiner, Mona Vito's, notes and work were lost during a building flood and she was no longer available to re-examine the evidence or testify! I was asked to show how the item was hidden on the CD using forensics skills.

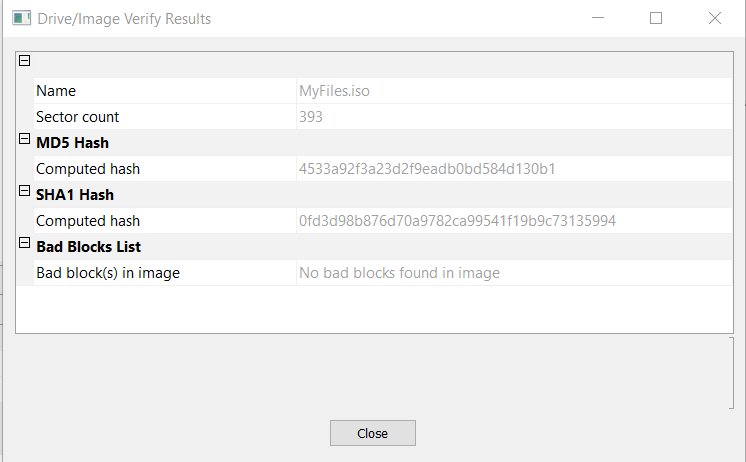
For reference, Mr. Gambini mentioned that the original subject acquired schematics for technology he planned to sell off to a competitor of UNCC's research partner company. There were some files believed to have been left behind when he was using the Cone 169 lab after meeting with an engineering student. The University of North Carolina at Charlotte has given the permission to go through the files in their possession, as this technology is a part of their research. The data was considered abandoned property by both our legal department and the folks at UNCC. No one else had tried to access this information since it was previously examined and verified.

**Forensic Acquisition & Exam Preparation**

To begin the analysis, Windows 10, 64-bit system was used, and the forensic image MyFiles.iso was downloaded from canvas - Files - Labs - Lab 6 Files. Access Data FTK Imager 4.5.0.3 was used to load the image and the MD5 hash value was verified before starting the analysis and after its completion. Later, with the help Autopsy 4.19.1 further analysis was conducted. SilentEye tool was used decode the hidden information in the image file.



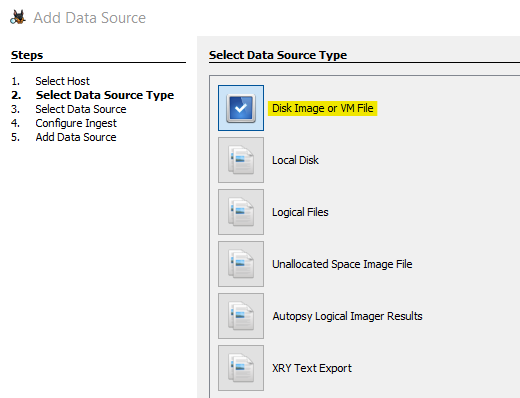
MD5 hash before analysis

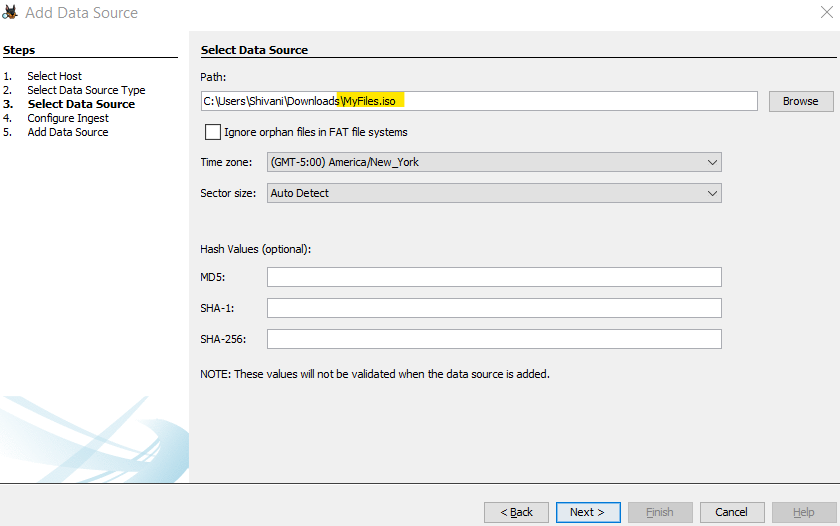


MD5 hash after analysis

**Findings and Report (Forensic Analysis)**

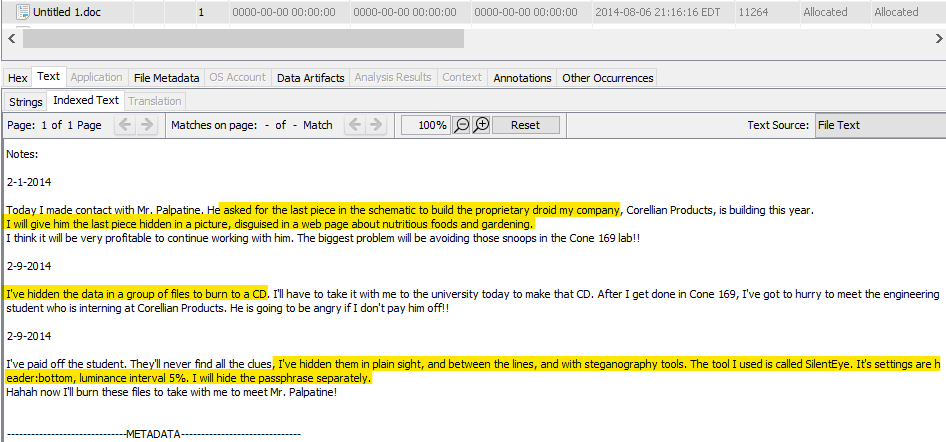
In Autopsy, using ‘Disk or VM Image’ as the data source, the forensic image file MyFiles.iso was added.

****

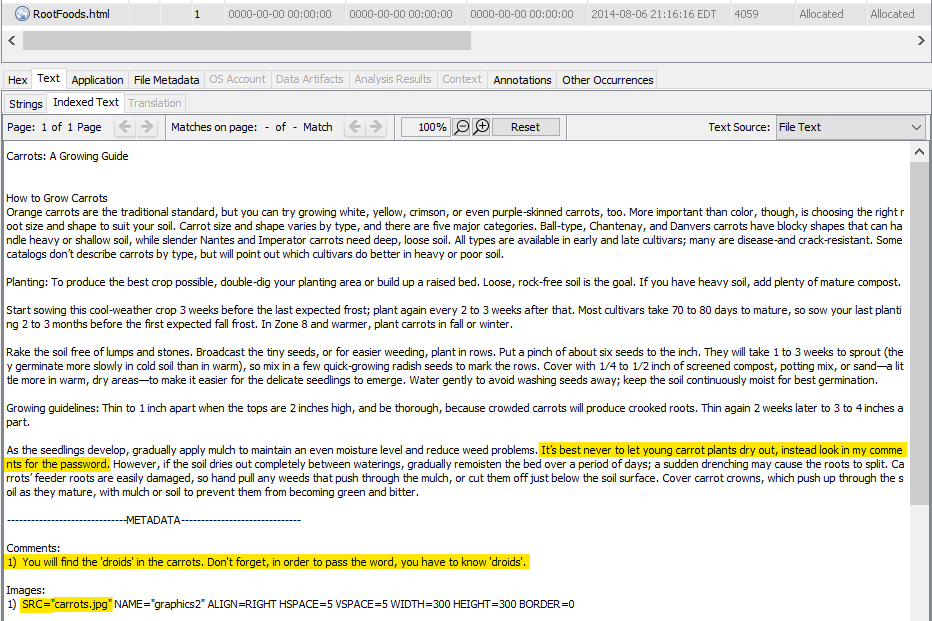
****

There was a document titled ‘Untitled 1.doc’ at path **File Views – File Types – By Extension – Documents – Office**. The file mentioned all details about hiding the last piece in the schematic in a picture disguised in a web page which as mentioned by Mr.Gambini, the original subject acquired and planned to sell off to a competitor of UNCC's research partner company.

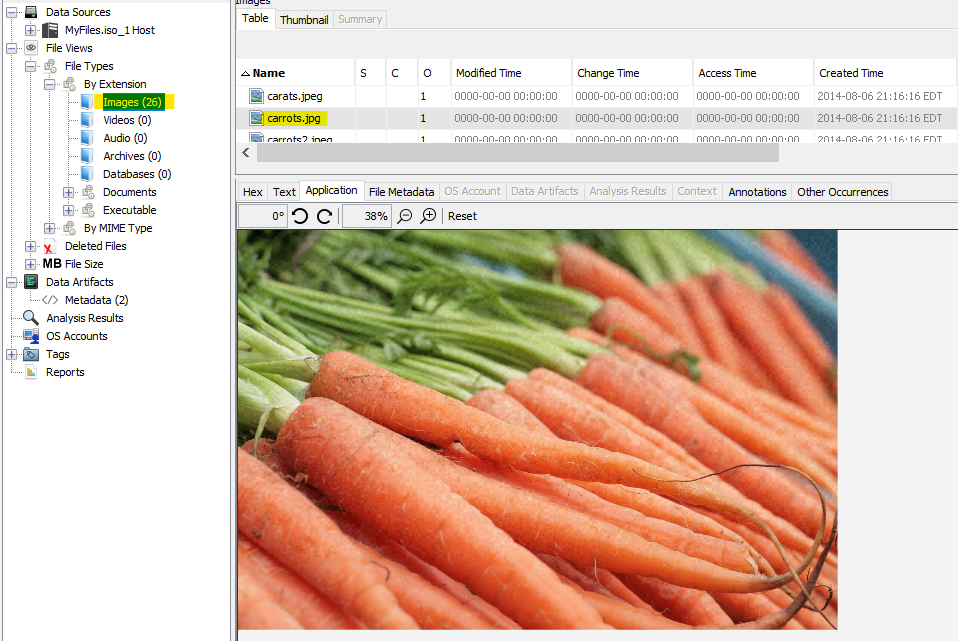
It also mentioned the name of the Steganography tool, SilentEye which was used for hiding the schematic.

****

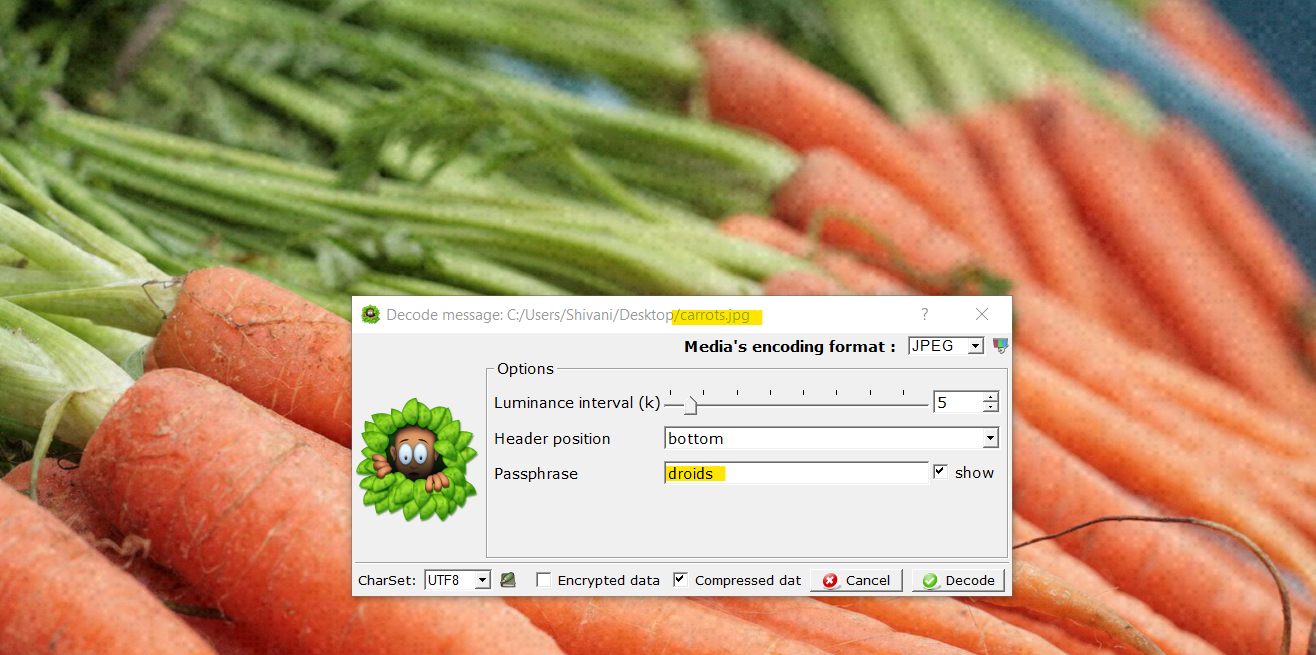
According to the above evidence document, the picture was disguised in a web page. A .html webpage named ‘RootFoods.html’ was found at path File Views – File Types – By Extension – Documents – HTML. The picture name - ‘carrots.jpg’- in which the last piece of schematic is hidden and the password -‘droids’- to decode it is mentioned in this webpage.

****

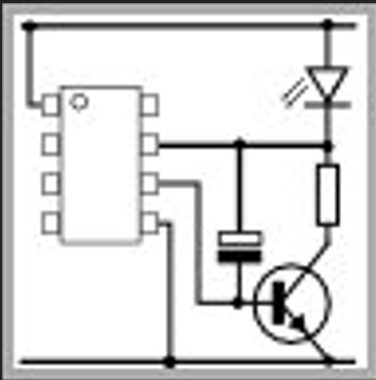
Carrots.jpg image is found at path File Views – File Types – By Extension – Images.

****

Carrots.jpg file was extracted from Autopsy and then loaded in SilentEye. The values set for Luminance interval, Header position and Password fields is as mentioned in the file Untitled1.doc and the webpage RootFoods.html. Then, the decode button was clicked.

****

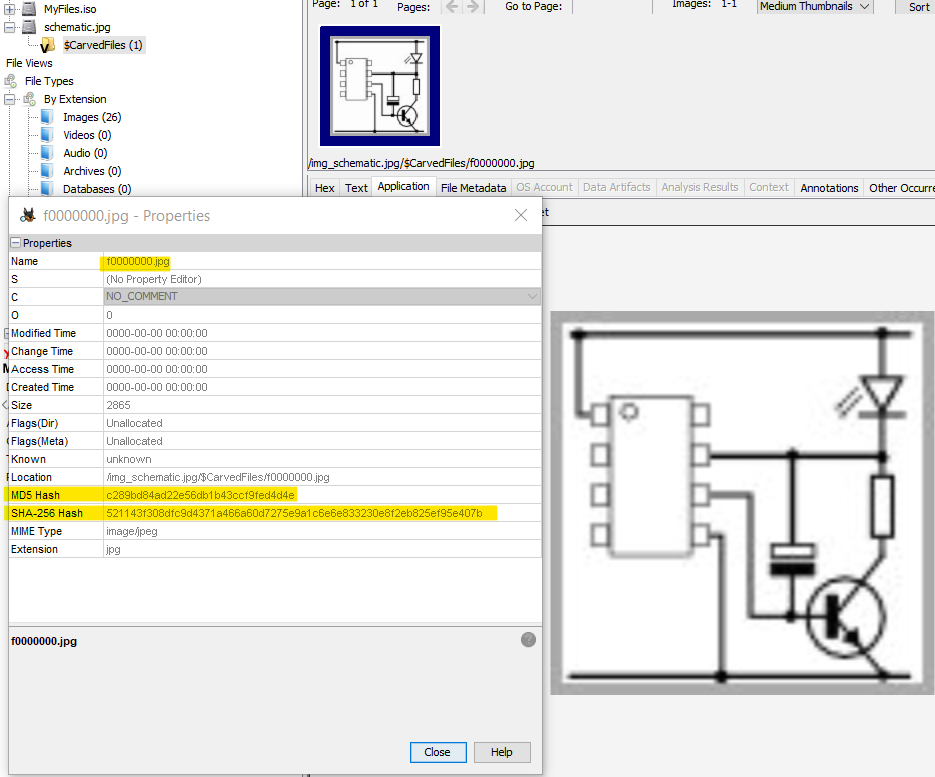
Below is the result. It is picture of last piece in the schematic that was hidden in the above picture.



To find the hash value of the schematic, the image was loaded in Autopsy with ‘Contents of a Folder’ as the Data Source. Under Carved Files, right clicking the image, the hash value was found in Properties Tab.

MD5: c289bd84ad22e56db1b43ccf9fed4d4e

SHA-256: 521143f308dfc9d4371a466a60d7275e9a1c6e6e833230e8f2eb825ef95e407b

****

**Conclusion**

Overall, in this lab I was asked to show how the item was hidden on the CD using forensics skills.

To begin the analysis, the image was loaded using AccessData FTK Imager 4.5.0.3 on a Windows 10 Machine and the hash value of image was verified to conclude that it was not tampered before the analysis process. With the help of Autopsy, the analysis of the provided forensic image file ‘MyFiles.iso’ was conducted and process showing how the item was hidden on CD was explained. At the end of analysis, the hash value of the schematic was found.

The image was again verified using AccessData FTK Imager to ensure it is not altered. No evidence has been retained. The forensic image, and the explanation of how the item was hidden on the CD, were returned to Mr. Gambini.