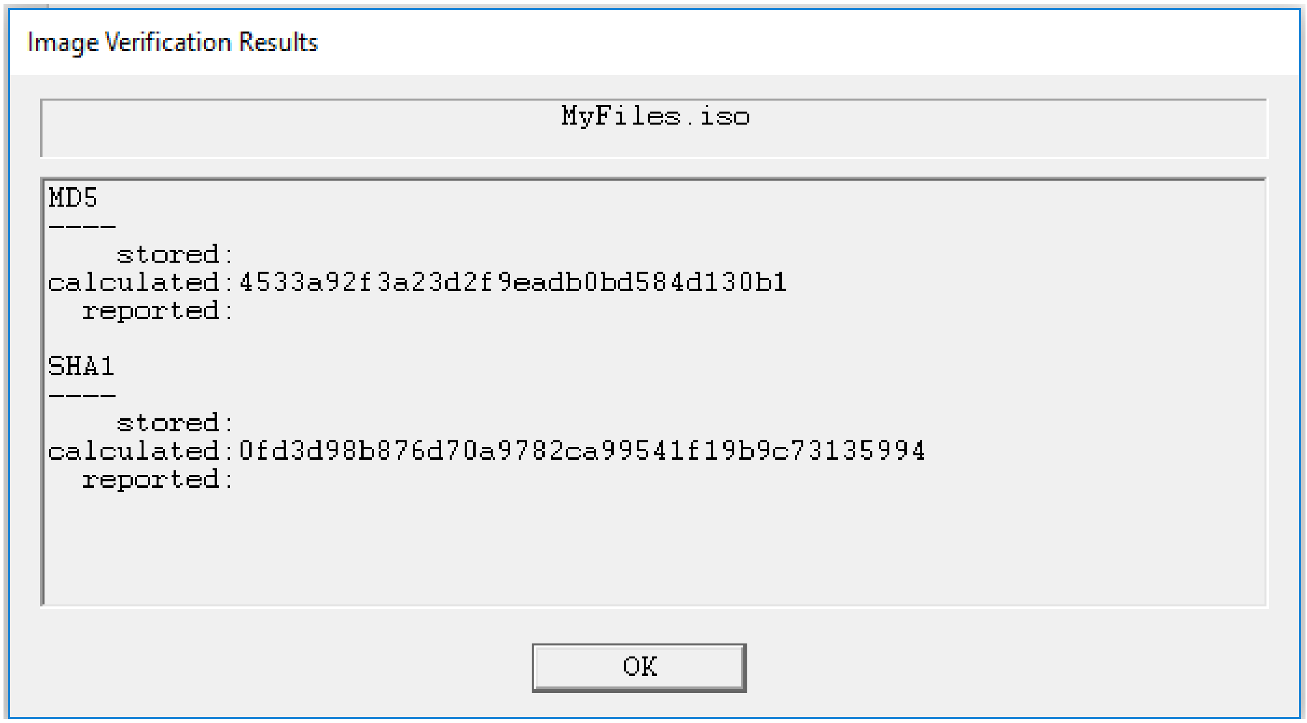
ITIS 5250
Parag Mhatre
Lab 2
Oct 28nd, 2018

Overview:

In this Lab, I have been given an image of some data left behind on a CD – **"MyFiles.iso"**. I been asked to make use of the **"FTK Imager Tool"** and other required tools to examine the image and find proof and evidence to show that the mystery criminal has acquired the schematics for technology and is stealing it. The evidence is to be used by the management and company's attorneys to take further action.

Forensic Acquisition & Exam Preparation

I accessed the image file on Canvas and downloaded it to my device. The software used for accessing & analyzing the image is **Forensic Toolkit 6.3** The first step undertaken after accessing the image file was the Hash calculation. The Screenshot of the Hash Calculation is as given below:



```
MyFiles.iso

MD5
-----
    stored:
calculated:4533a92f3a23d2f9eadb0bd584d130b1
  reported:

SHA1
----
    stored:
calculated:0fd3d98b876d70a9782ca99541f19b9c73135994
  reported:
```

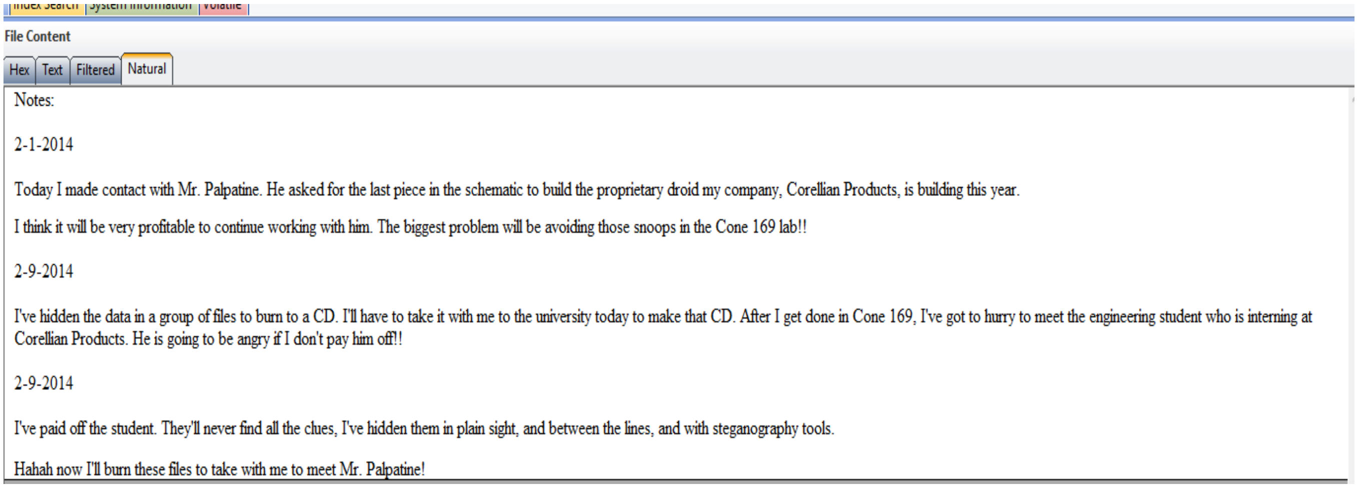
Findings and Report (Forensic Analysis)

Once I started examining the image, I checked the files on the and found a few **picture files**, an **HTML file**, a **ppt file** and a **document (.doc) file**. On a closer inspection, I found out that the files are the content of a HTML web page on the topic of carrots.

Evidence 1 – Untitled.doc

Furthermore, I checked the **"Untitled 1.doc"** file, and performed examinations on that. It contains the notes that the creator compiled. On, 1st February 2014, the notes say**, that the creator contacted one Mr. Palpatine and was asked to provide the last piece in the schematic to build the proprietary droid, the creators company – "Corellian Products" is building.**

On 9th February 2014, his notes talk about **burning some files to a CD and paying off a student who is interning at "Corellian Products".** On the same day, in another entry, he says that **he has hidden the clues in plain sight and between the lines using steganography tools.**



Notes:

2-1-2014

Today I made contact with Mr. Palpatine. He asked for the last piece in the schematic to build the proprietary droid my company, Corellian Products, is building this year.

I think it will be very profitable to continue working with him. The biggest problem will be avoiding those snoops in the Cone 169 lab!!

2-9-2014

I've hidden the data in a group of files to burn to a CD. I'll have to take it with me to the university today to make that CD. After I get done in Cone 169, I've got to hurry to meet the engineering student who is interning at Corellian Products. He is going to be angry if I don't pay him off!!

2-9-2014

I've paid off the student. They'll never find all the clues, I've hidden them in plain sight, and between the lines, and with steganography tools.

Hahah now I'll burn these files to take with me to meet Mr. Palpatine!

While further examining the file (exporting it out of FTK and opening in Microsoft Word), I realized that it contained some text that was white in color, i.e. the color of the background and was essentially invisible to the eye. After changing the color, the text read, -

"I will give him the last piece hidden in a picture, disguised in a web page about nutritious food and gardening." and

"The tool used is called SilentEye. Its settings are header: bottom, luminance interval 5%. I will hide the passphrase separately".

This shows that the creator has sent the last piece in a picture from the web page, using a tool – "SilentEye" and listed out the settings for decryption.

2-1-2014

Today I made contact with Mr. Palpatine. He asked for the last piece in the schematic to build the proprietary droid my company, Corellian Products, is building this year.
I will give him the last piece hidden in a picture, disguised in a web page about nutritious foods and gardening.
I think it will be very profitable to continue working with him. The biggest problem will be avoiding those snoops in the Cone 169 lab!!

2-9-2014

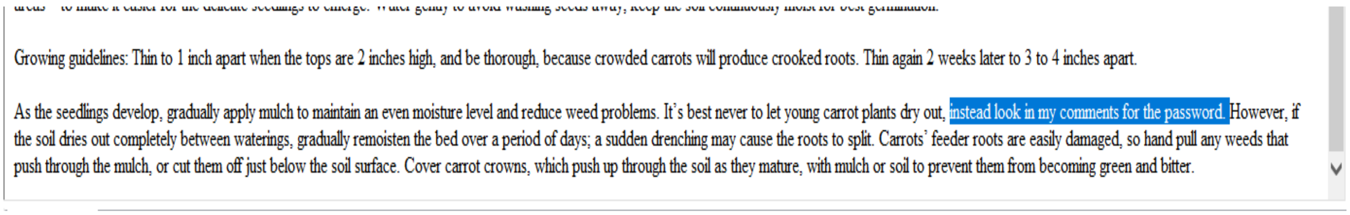
I've hidden the data in a group of files to burn to a CD. I'll have to take it with me to the university today to make that CD. After I get done in Cone 169, I've got to hurry to meet the engineering student who is interning at Corellian Products. He is going to be angry if I don't pay him off!!

2-9-2014

I've paid off the student. They'll never find all the clues, I've hidden them in plain sight, and between the lines, and with steganography tools. The tool I used is called SilentEye. It's settings are header:bottom, luminance interval 5%. I will hide the passphrase separately.
Hahah now I'll burn these files to take with me to meet Mr. Palpatine!

Evidence 2 – RootFoods.html

In the html file, while reading the text which is based mainly on carrots, I found a phrase – **"instead look in my comments for the password"**. This shows that the creator wanted to convey a password to the receiver and it's stored in comments somewhere.



areas — to make it easier for the delicate seedlings to emerge. Water gently to avoid washing seeds away; keep the soil continuously moist for best germination.

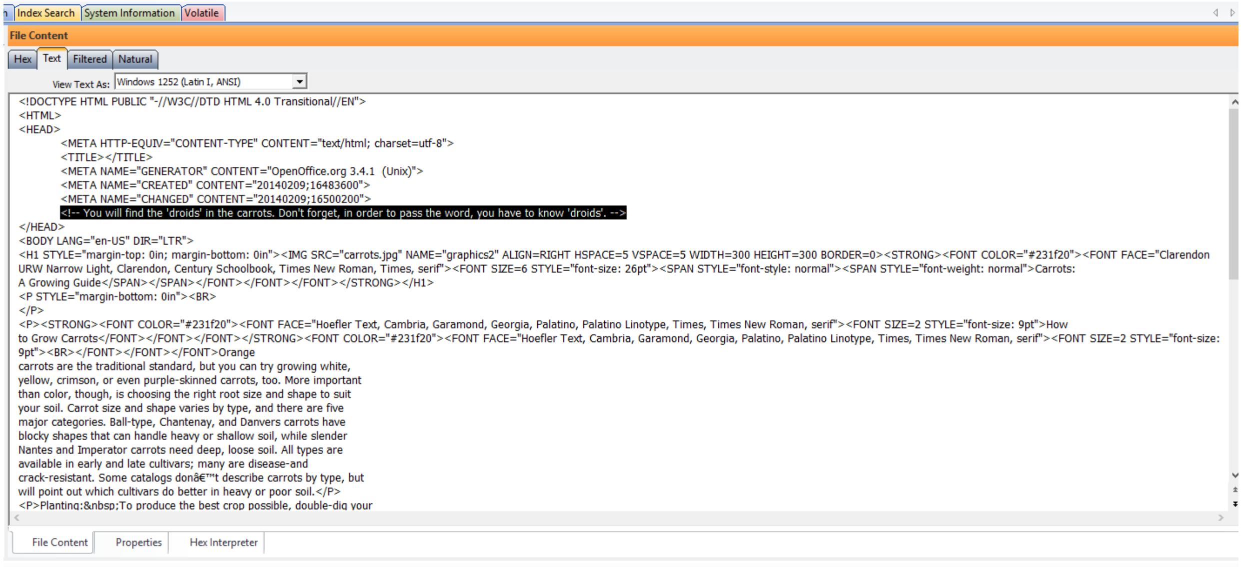
Growing guidelines: Thin to 1 inch apart when the tops are 2 inches high, and be thorough, because crowded carrots will produce crooked roots. Thin again 2 weeks later to 3 to 4 inches apart.

As the seedlings develop, gradually apply mulch to maintain an even moisture level and reduce weed problems. It's best never to let young carrot plants dry out, instead look in my comments for the password. However, if the soil dries out completely between waterings, gradually remoisten the bed over a period of days; a sudden drenching may cause the roots to split. Carrots' feeder roots are easily damaged, so hand pull any weeds that push through the mulch, or cut them off just below the soil surface. Cover carrot crowns, which push up through the soil as they mature, with mulch or soil to prevent them from becoming green and bitter.

While looking at the same file in text mode, between the HTML code, I found a message/comment which looks like it contains the pass phrase that the creator was talking about in the Evidence 1. The message says –

"<!—You will find the 'droids' in the carrots. Don't forget, in order to pass the word, you have to know 'droids'.-->"

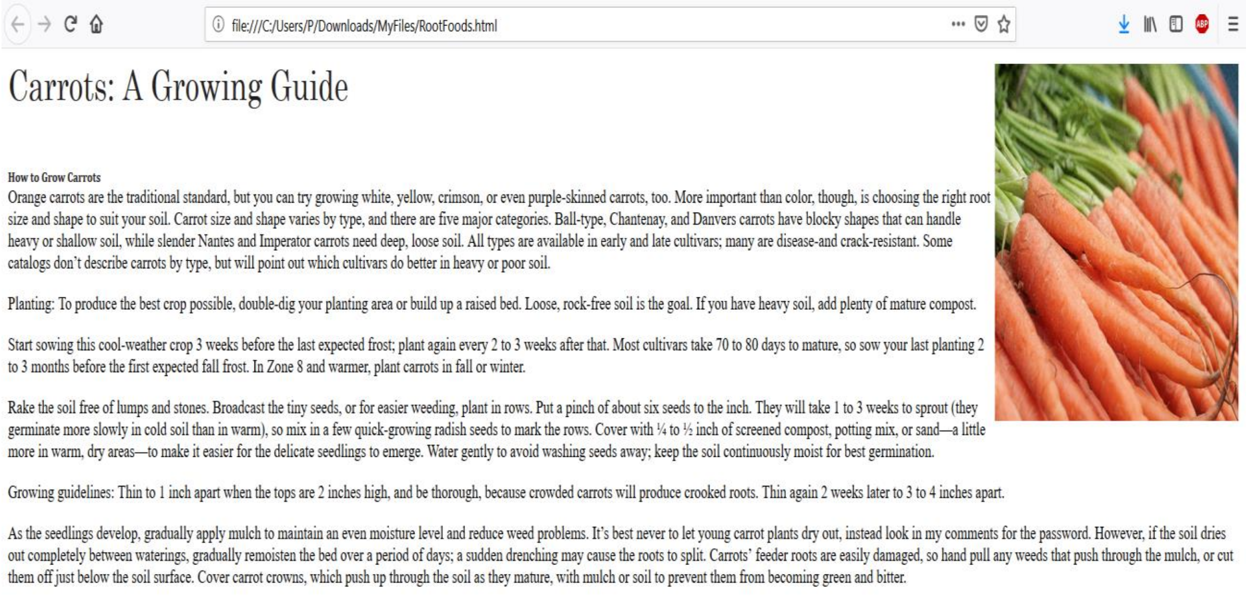
If this is the passphrase, then all the requisites for decrypting the message form an image in the tool – SilentEye have been found, provided that the encryption option was not checked in the tool.



View Text As: Windows 1252 (Latin I, ANSI)

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
<HEAD>
        <META HTTP-EQUIV="CONTENT-TYPE" CONTENT="text/html; charset=utf-8">
        <TITLE></TITLE>
        <META NAME="GENERATOR" CONTENT="OpenOffice.org 3.4.1  (Unix)">
        <META NAME="CREATED" CONTENT="20140209;16483600">
        <META NAME="CHANGED" CONTENT="20140209;16500200">
        <!-- You will find the 'droids' in the carrots. Don't forget, in order to pass the word, you have to know 'droids'. -->
</HEAD>
<BODY LANG="en-US" DIR="LTR">
<H1 STYLE="margin-top: 0in; margin-bottom: 0in"><IMG SRC="carrots.jpg" NAME="graphics2" ALIGN=RIGHT HSPACE=5 VSPACE=5 WIDTH=300 HEIGHT=300 BORDER=0><STRONG><FONT COLOR="#231f20"><FONT FACE="Clarendon
URW Narrow Light, Clarendon, Century Schoolbook, Times New Roman, Times, serif"><FONT SIZE=6 STYLE="font-size: 26pt"><SPAN STYLE="font-style: normal"><SPAN STYLE="font-weight: normal">Carrots:
A Growing Guide</SPAN></SPAN></FONT></FONT></FONT></STRONG></H1>
<P STYLE="margin-bottom: 0in"><BR>
</P>
<P><STRONG><FONT COLOR="#231f20"><FONT FACE="Hoefler Text, Cambria, Garamond, Georgia, Palatino, Palatino Linotype, Times, Times New Roman, serif"><FONT SIZE=2 STYLE="font-size: 9pt">How
to Grow Carrots</FONT></FONT></FONT></STRONG><FONT COLOR="#231f20"><FONT FACE="Hoefler Text, Cambria, Garamond, Georgia, Palatino, Palatino Linotype, Times, Times New Roman, serif"><FONT SIZE=2 STYLE="font-size:
9pt"><BR></FONT></FONT></FONT>Orange
carrots are the traditional standard, but you can try growing white,
yellow, crimson, or even purple-skinned carrots, too. More important
than color, though, is choosing the right root size and shape to suit
your soil. Carrot size and shape varies by type, and there are five
major categories. Ball-type, Chantenay, and Danvers carrots have
blocky shapes that can handle heavy or shallow soil, while slender
Nantes and Imperator carrots need deep, loose soil. All types are
available in early and late cultivars; many are disease-and
crack-resistant. Some catalogs donâ€™t describe carrots by type, but
will point out which cultivars do better in heavy or poor soil.</P>
<P>Planting:&nbsp;To produce the best crop possible, double-dig your
```

If we export all the files out from FTK, then the image displayed on the web page is **"carrots.jpg"**. Since, the creator has hinted that this is the image in which, has the hidden file, I am going to try this image in the tool.



Carrots: A Growing Guide

How to Grow Carrots

Orange carrots are the traditional standard, but you can try growing white, yellow, crimson, or even purple-skinned carrots, too. More important than color, though, is choosing the right root size and shape to suit your soil. Carrot size and shape varies by type, and there are five major categories. Ball-type, Chantenay, and Danvers carrots have blocky shapes that can handle heavy or shallow soil, while slender Nantes and Imperator carrots need deep, loose soil. All types are available in early and late cultivars; many are disease-and crack-resistant. Some catalogs don't describe carrots by type, but will point out which cultivars do better in heavy or poor soil.

Planting: To produce the best crop possible, double-dig your planting area or build up a raised bed. Loose, rock-free soil is the goal. If you have heavy soil, add plenty of mature compost.

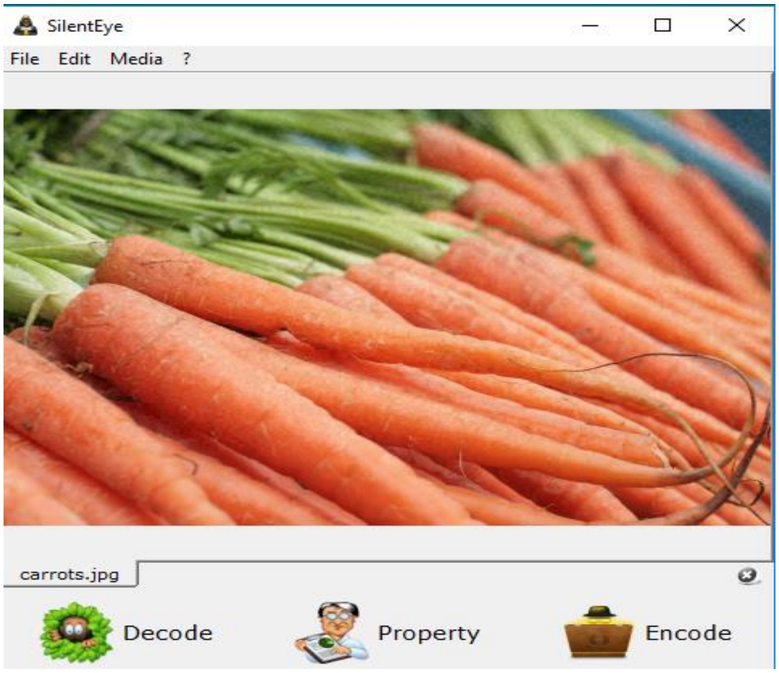
Start sowing this cool-weather crop 3 weeks before the last expected frost; plant again every 2 to 3 weeks after that. Most cultivars take 70 to 80 days to mature, so sow your last planting 2 to 3 months before the first expected fall frost. In Zone 8 and warmer, plant carrots in fall or winter.

Rake the soil free of lumps and stones. Broadcast the tiny seeds, or for easier weeding, plant in rows. Put a pinch of about six seeds to the inch. They will take 1 to 3 weeks to sprout (they germinate more slowly in cold soil than in warm), so mix in a few quick-growing radish seeds to mark the rows. Cover with ¼ to ½ inch of screened compost, potting mix, or sand—a little more in warm, dry areas—to make it easier for the delicate seedlings to emerge. Water gently to avoid washing seeds away; keep the soil continuously moist for best germination.

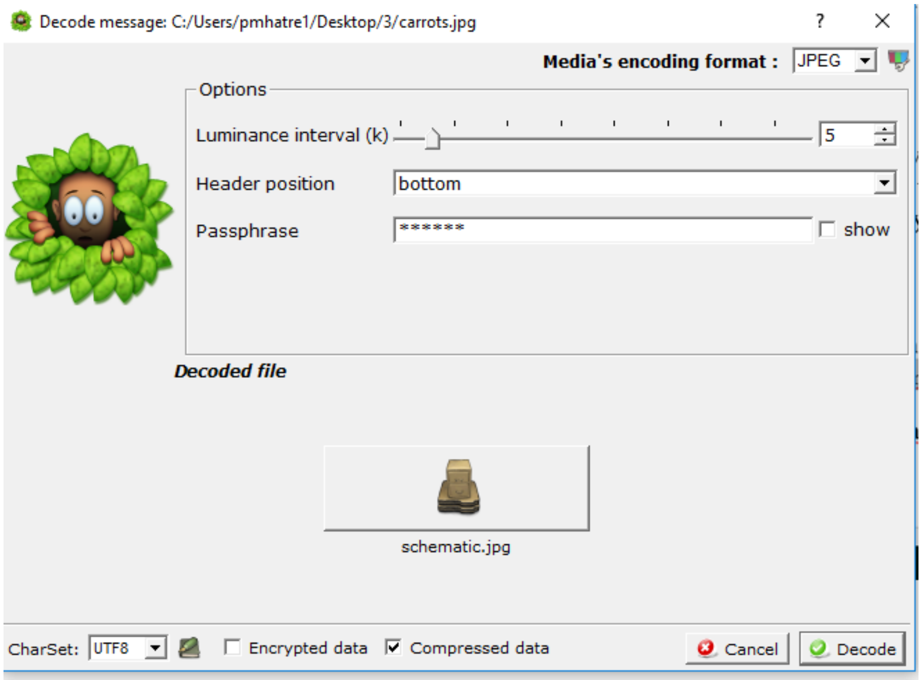
Growing guidelines: Thin to 1 inch apart when the tops are 2 inches high, and be thorough, because crowded carrots will produce crooked roots. Thin again 2 weeks later to 3 to 4 inches apart.

As the seedlings develop, gradually apply mulch to maintain an even moisture level and reduce weed problems. It's best never to let young carrot plants dry out, instead look in my comments for the password. However, if the soil dries out completely between waterings, gradually remoisten the bed over a period of days; a sudden drenching may cause the roots to split. Carrots' feeder roots are easily damaged, so hand pull any weeds that push through the mulch, or cut them off just below the soil surface. Cover carrot crowns, which push up through the soil as they mature, with mulch or soil to prevent them from becoming green and bitter.

I loaded up the image in “SilentEye” and clicked on Decode.



Then, I set all the settings as given in the doc file, and put in the pass phrase and recovered the file, **“schematic.jpg”**.


Decode message: C:/Users/pmhatre1/Desktop/3/carrots.jpg

Media's encoding format : JPEG

Options

Luminance interval (k) 5

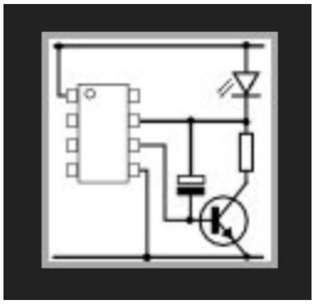
Header position bottom

Passphrase ****** □ show

Decoded file

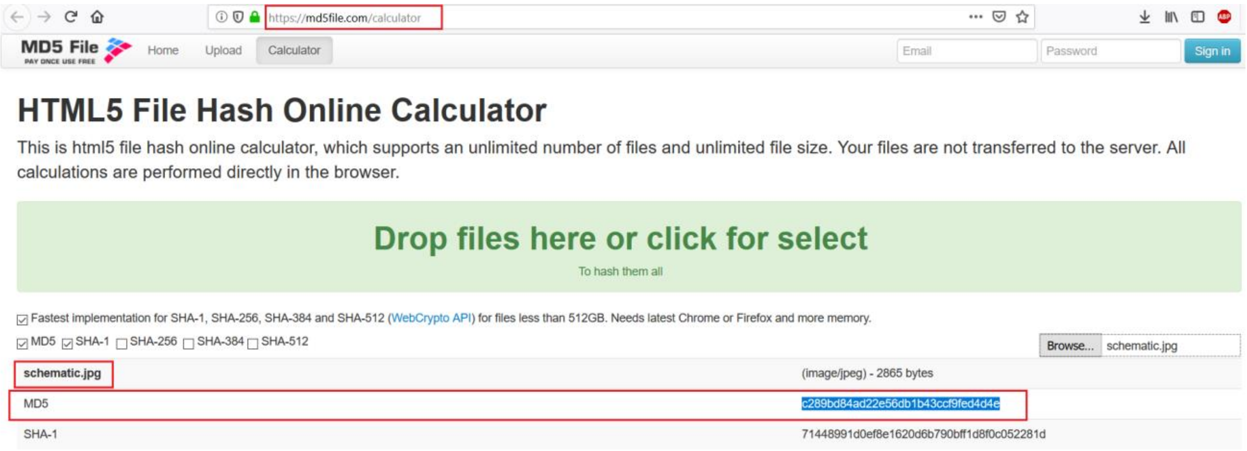
schematic.jpg

CharSet: UTF8 □ Encrypted data ☑ Compressed data



Hash Value of the file – “schematic.jpg”:

I calculated the Hash value of the “schematic.jpg” from www.md5file.com/calculator. The Hash value of the file is **c289bd84ad22e56db1b43ccf9fed4d4e**.



HTML5 File Hash Online Calculator

This is html5 file hash online calculator, which supports an unlimited number of files and unlimited file size. Your files are not transferred to the server. All calculations are performed directly in the browser.

Drop files here or click for select

To hash them all

☑ Fastest implementation for SHA-1, SHA-256, SHA-384 and SHA-512 (WebCrypto API) for files less than 512GB. Needs latest Chrome or Firefox and more memory.

☑ MD5 ☑ SHA-1 ☐ SHA-256 ☐ SHA-384 ☐ SHA-512 Browse... schematic.jpg

schematic.jpg	(image/jpeg) - 2865 bytes
MD5	c289bd84ad22e56db1b43ccf9fed4d4e
SHA-1	71448991d0ef8e1620d6b790bff1d8f0c052281d

Conclusion:

I examined the given image file and tried to look for evidence linking the creator of the files with the theft of the technology from **“Corellian Products”**. My findings are as follows:

1. Notes.doc has the creator's comments where he has clearly mentioned the theft and sending the files to Mr. Palaptine along with paying off a intern.
2. The same file contains configurations for the tool - SilentEye as listed here.
   Header: Bottom
   Luminance interval: 5%.
3. The HTML file code contains a comment listing the pass phrase as **"droids".**
4. The file - **“schematic.jpg”** was recovered after entering the configuration in the Steganography tool – SilentEye.
5. The hash value of schematic.jpg is **c289bd84ad22e56db1b43ccf9fed4d4e**