

Practical 4 Lab – Steganography

Objective: This practical will expose you to some tools used to conceal a file or information in another file.

Instructions:

Download the zip file from blackboard / Digital Forensic Investigation / Learning Resources / Practicals / Week 5 : Practical 4 - Steganography / Prac 4v1.zip

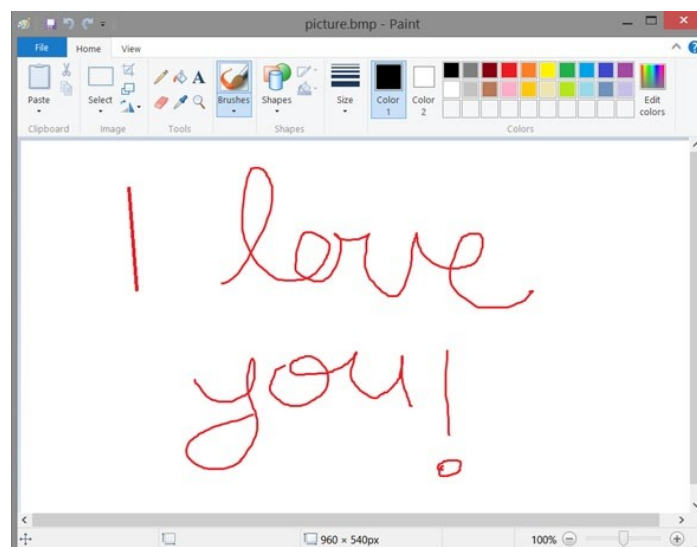
Unzip all the zipped steganography programs. There are 9 exercises (0-7,9) in this zip files. Try out these exercises. 8-EXIF & SPAM MIMIC contains information on EXIF and SPAM MIMIC website only.

0. DIY WAY

If you're the kind of person that likes to do things yourself, this method is as DIY as it gets. You may have to try it several times to find the best picture to hide your message in, but keep in mind that a simple MS Paint (or equivalent) drawing would work best.

This method is based on a process found on [WikiHow](#), which basically combines two files — an image and a text message — so that on the outside the image looks like an ordinary one, but if you know where to look, you can find the hidden message.

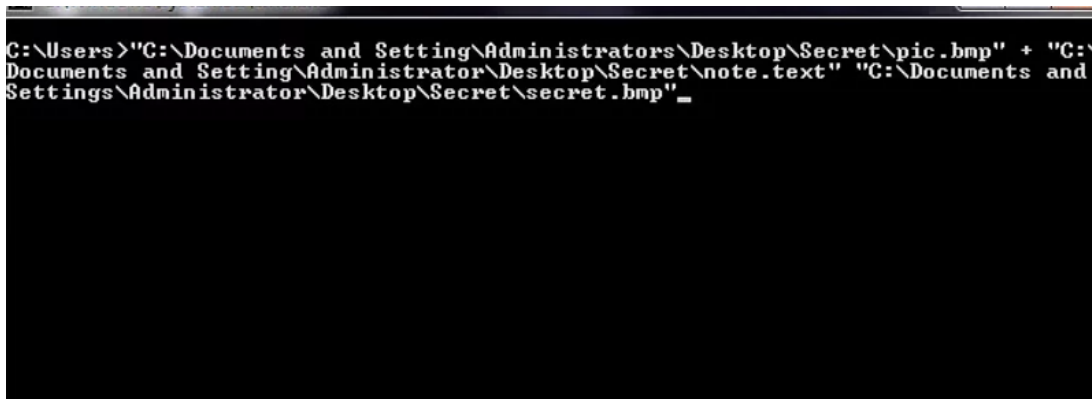
To start, find or create a **BMP** file in any way you wish. You can draw something simple and save it as BMP in MS paint, but you can also try it with a real image if wish.



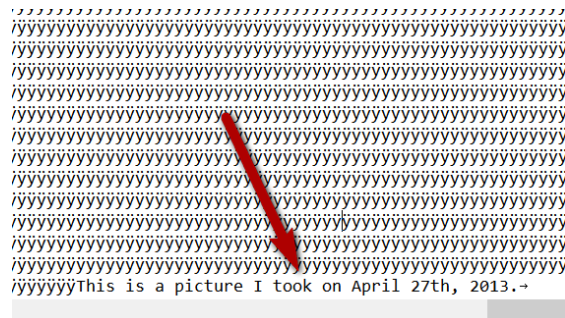
Next, create your **message** in Notepad or a similar program, and save your message in TXT format. Now open Command Prompt, and type in the following:

copy "<image file path>" + "<text file path>" "<new image path>".

You can get a better idea of what this will look like in the screenshot below.



Name your new image whatever you want, but remember that this is your actual secret message image, so don't name it "secret message" if you really want it to be a secret. The new image will also be a BMP file, so anyone who sees it will double click it to open and see only the image. If, however, someone in the know opens it using Notepad/WordPad, they'll find the secret message hiding all the way at the bottom of the file.

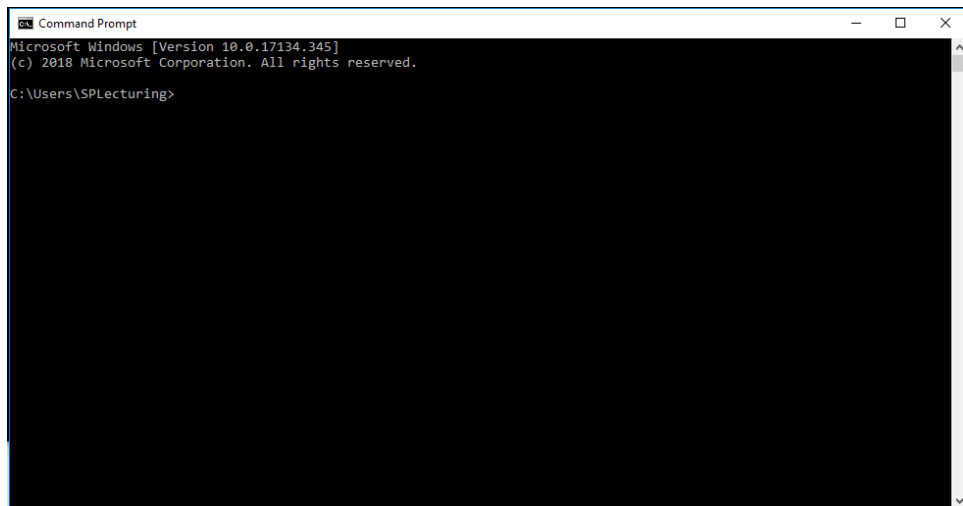


Yes, this might not be the most sophisticated way to do this, but it is always one of the way!

1 SNOW PROGRAM

Snow program. This program hide message in blank space in your carrier file.

1. First open command prompt



2. Change directory to the SNOW Program directory:

Cd <directory that contains snow program>

Snow program : **Snow.exe**

2.1 Command for Hiding a Text File

Snow -p passwordsnow -m "Secret Message: activate plan A at 10pm tonight" test1.txt test2.txt

- The option **-p** set "snowpassword" as the passphrase to hide the secret message
- The option **-m** set the content of secret message
- "test1.txt" is the source file
- "test2.txt" is the target file
- Target file will contain original text file plus the secret message

```
C:\Users\SPlecturing\Desktop\SNOW>snow -p passwordsnow -m "Secret Message: Activate Plan A at 10pm tonight" test1.txt test2.txt
Message exceeded available space by approximately 1.3%.
An extra 13 lines were added.
```

2.2 Command for showing a hidden Text File

Snow -p passwordsnow test2.txt

- The option **-p** set "snowpassword" as the passphrase to reveal the secret message
- "test2.txt" is the target file
- If don't use Snow program, both test1.txt and test2.txt are just an empty files

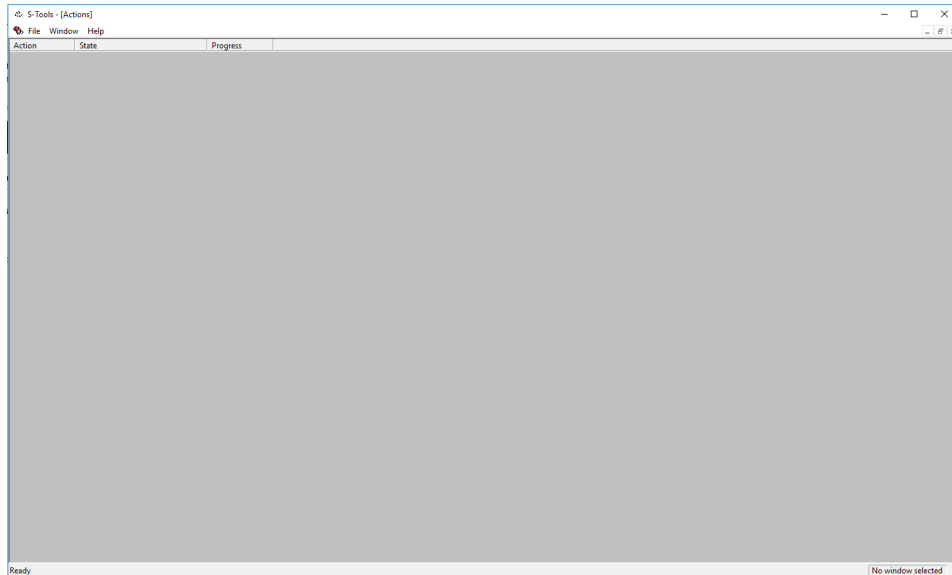
```
C:\Users\SPlecturing\Desktop\SNOW>snow -p passwordsnow test2.txt
Secret Message: Activate Plan A at 10pm tonight
C:\Users\SPlecturing\Desktop\SNOW>
```

2 S-TOOL

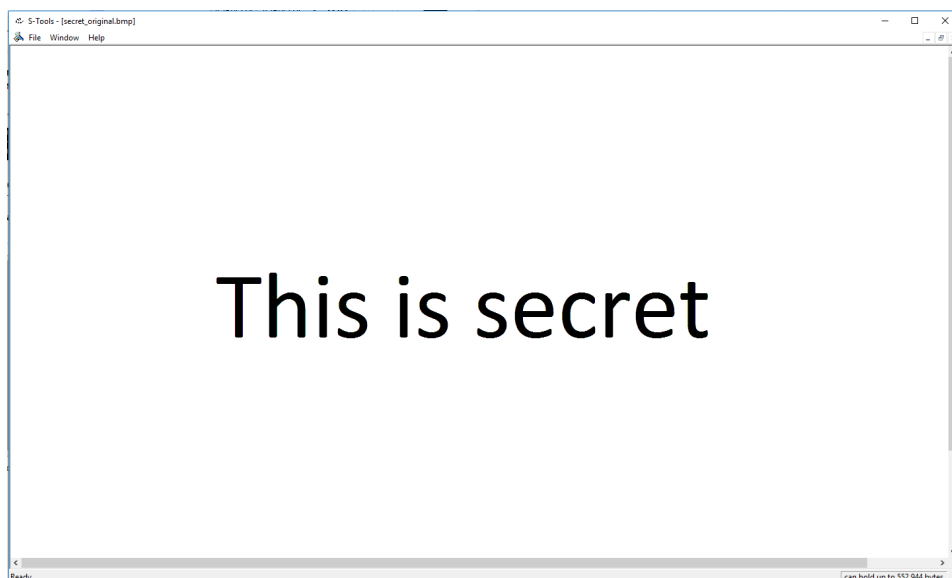
This program can hide a **lossless** compression image inside another image.

2.1 HIDING FILE

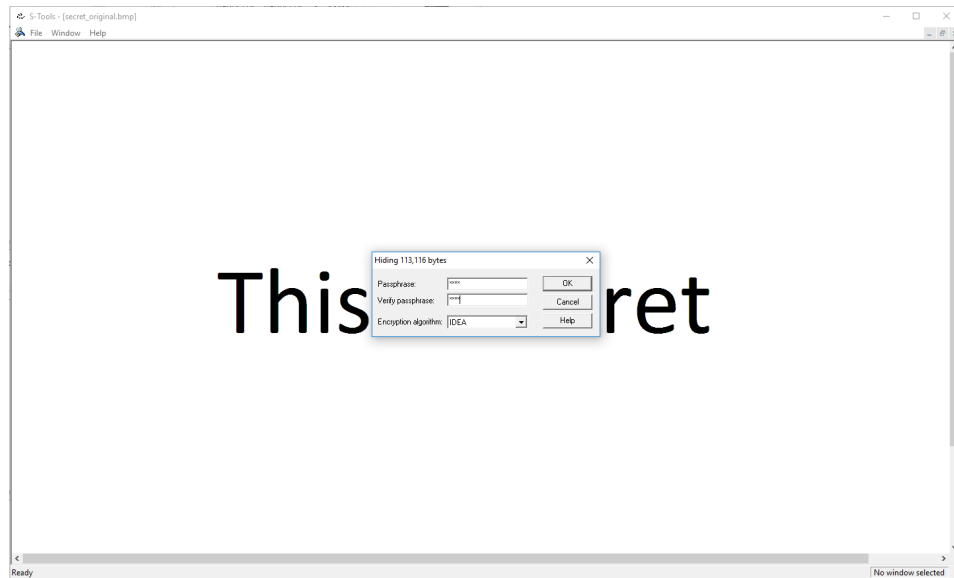
1. Activate command prompt. Go to S-Tools directory. Execute (Run) S-Tools program and the following screen will be displayed



2. Drag and drop file named secret_original.bmp into S-Tool window. The following screen will be shown.



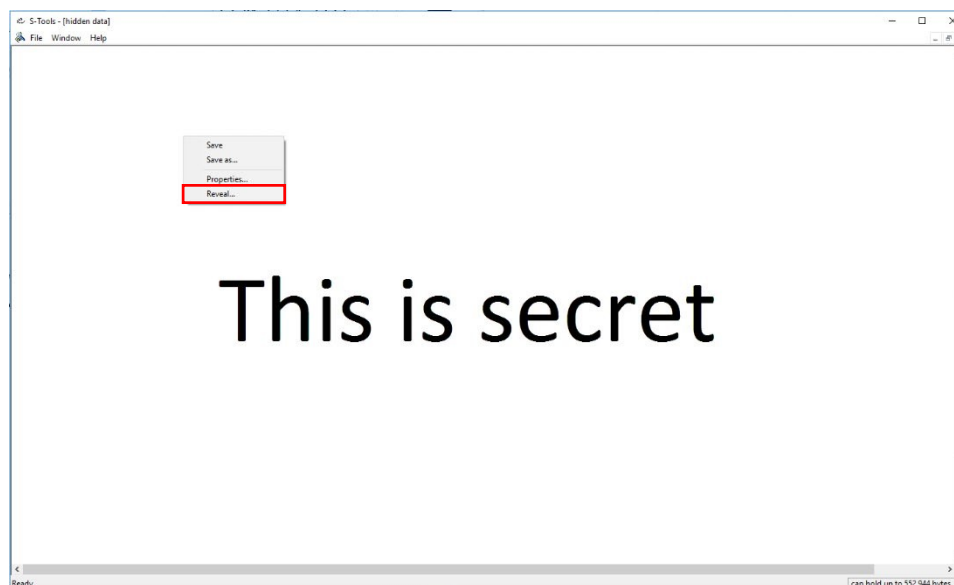
3. Drag and drop Dog.gif into S-Tools. When prompt with passphrase, key in the passphrase of your choice. Please don't forget your passphrase. Use default encryption setting.



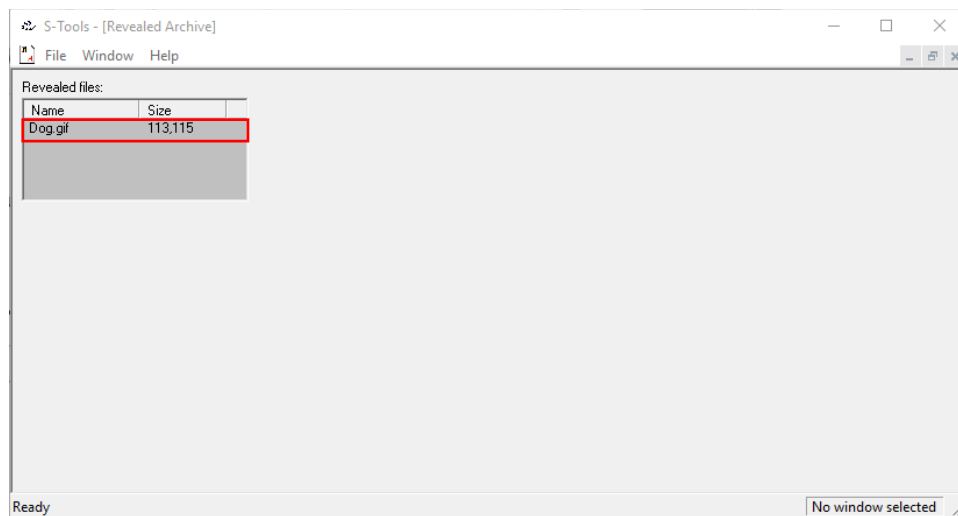
4. When prompted with "Picture hiding" press ok to continue.

2.2 REVEALING FILE

1. In order to reveal, right-click on the hidden picture and select "reveal"



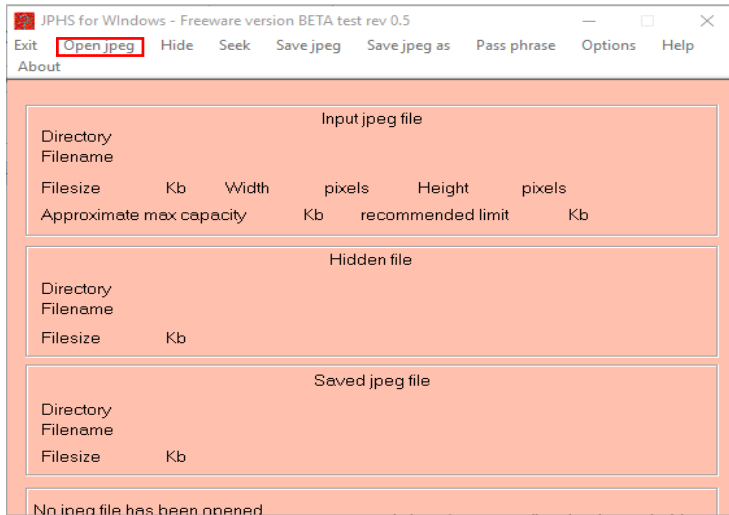
2. key in the passphrase when prompted. The following screen will be shown.



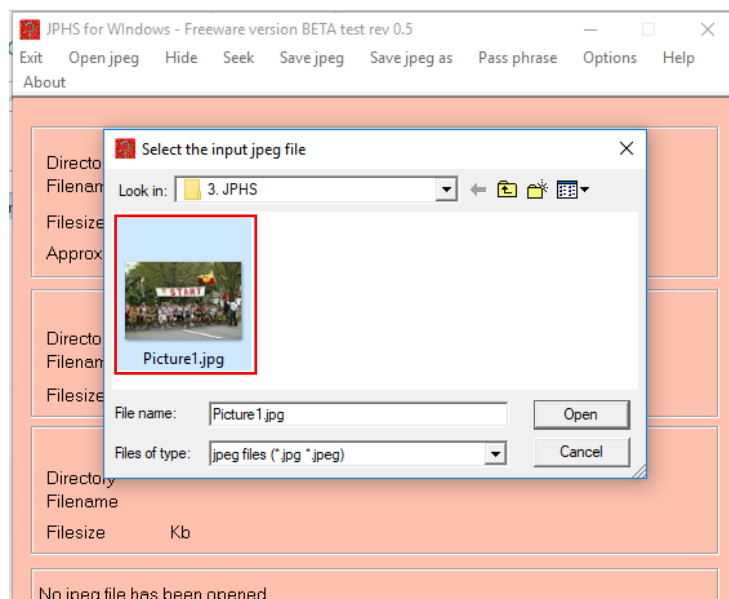
3. Right-click and select "save as" to save the photo to a location you desire. Go to the location and open the gif file. With that, you have successfully retrieved the hidden gif file.
4. Close all the above programs.

3. JPHS

1. This program can hide a **lossy** compression image inside another image.
NOTE: This is a very old program and results produced may not be stable.
2. Go to JPHS folder and execute Jphswin.exe program. Agree to the terms and conditions.
3. When the following window is shown, click on “Open jpeg”



4. Then select Picture1.jpg as carrier and click Open.

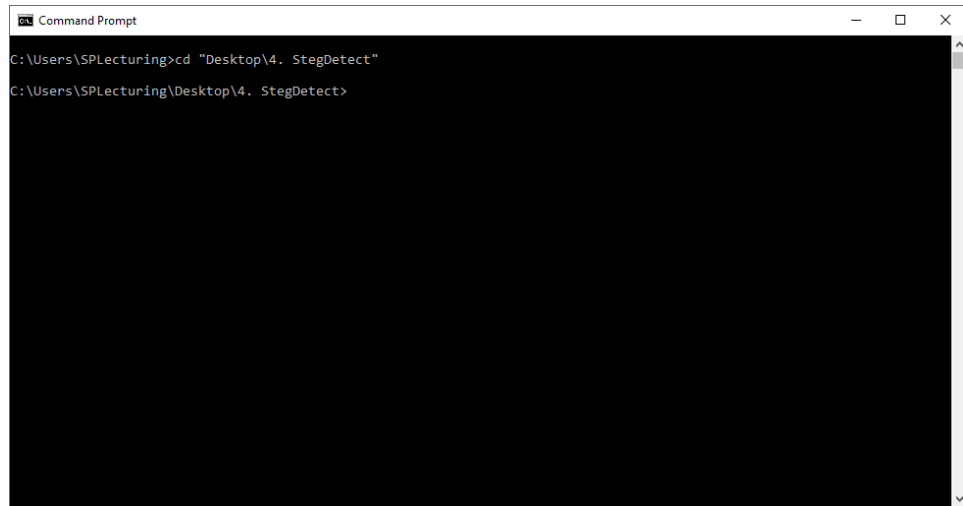


5. Click “Hide” and enter pass phrase. Remember your passphrase.
6. Next, select **hide.txt** from JPHS folder to hide hide.txt in Picture1.jpg.
7. Click “Save jpeg as” and enter Picture2 as filename and click save. Save picture2 as jpg file.
8. New file named Picture2.jpg is created & saved. Close JPHS.
9. To uncover hidden message, run JPHS again and accept terms and conditions.
10. Click “Open jpeg” to retrieve Picture2.jpg.
11. Click “Seek” and enter passphrase then save file as unhide.txt.
12. Access unhide.txt to find out contents of the file.

4. STEGDETECT

Program attempts to detect as to whether any data is hidden in carrier file.

1. Open command prompt.
2. Change directory to the StegDetect Program directory:
Cd <directory that contains StegDetect program>



```
Command Prompt
C:\Users\SPlecturing>cd "Desktop\4. StegDetect"
C:\Users\SPlecturing\Desktop\4. StegDetect>
```

3. The jpg file "Anna.jpg" contains a secret text. Stegbreak.exe is able to crack to retrieve the text. the password. Issue the command shown as screen below. You should be able to find password "**pass**" with the help of the a "words-english.txt" file.

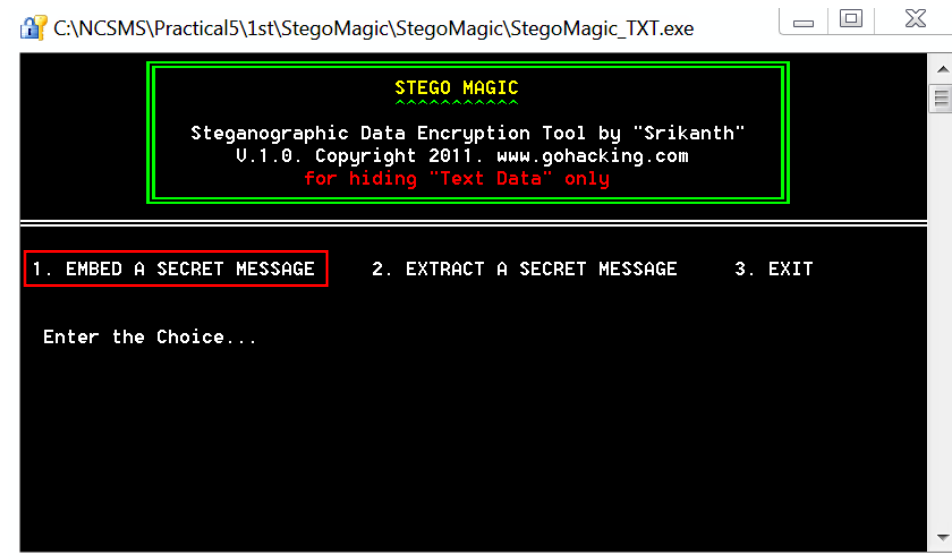
```
C:\Users\SPlecturing\Desktop\4. StegDetect>stegbreak.exe -r rules.ini -f words-english.txt -t p Anna.jpg
Loaded 1 files...
Anna.jpg : jphide[v5](pass)
Processed 1 files, found 1 embeddings.
Time: 1 seconds: Cracks: 19189, 19189.0 c/s
C:\Users\SPlecturing\Desktop\4. StegDetect>
```


5. STEGOMAGIC

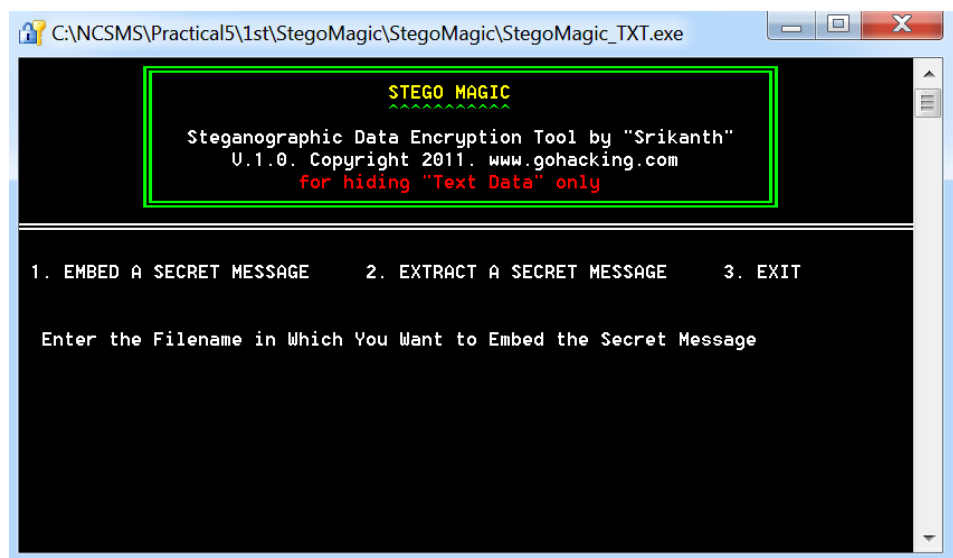
EMBEDDING STEGOMAGIC

If you receive warning from Symantec, just ignore and close the Symantec window.

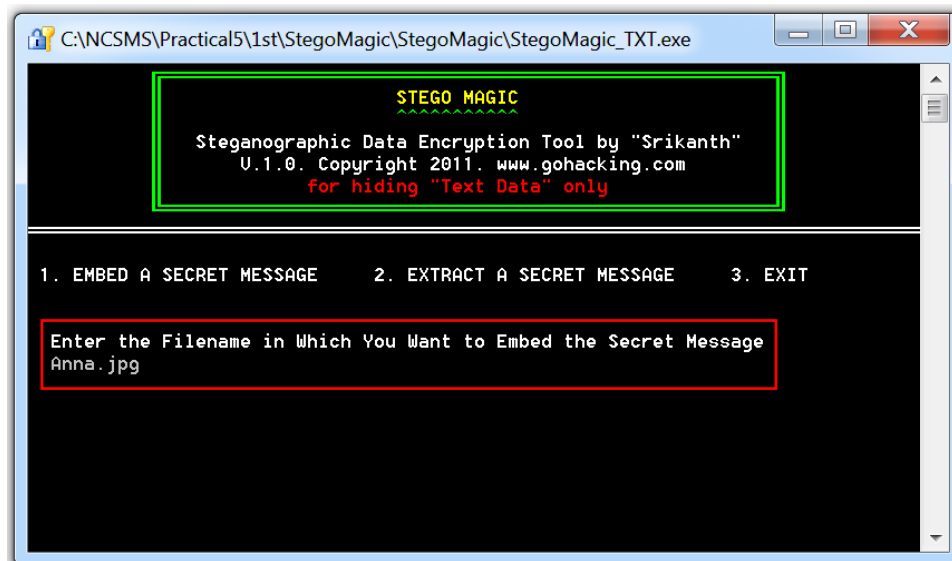
1. Execute StegoMagic-Bin.exe in the command prompt.



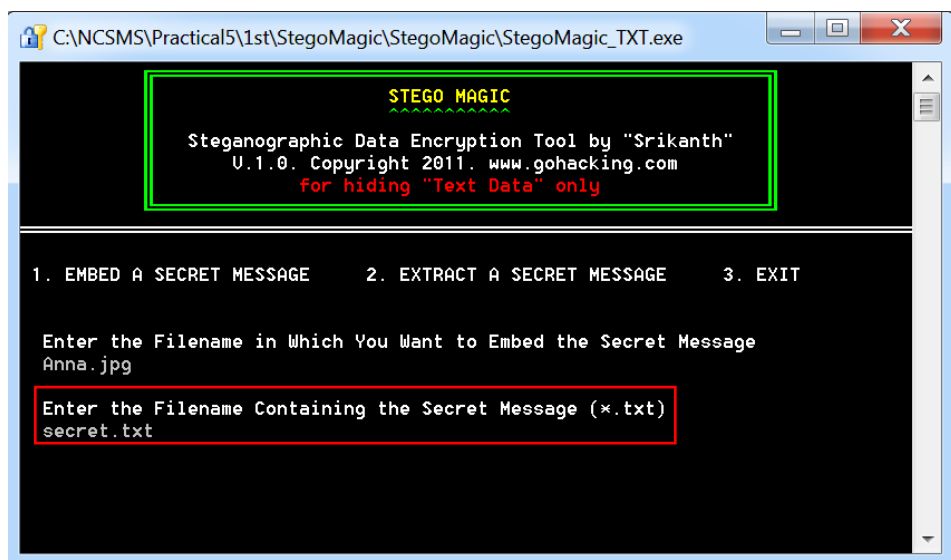
2. Select the first option on the menu by entering "1".



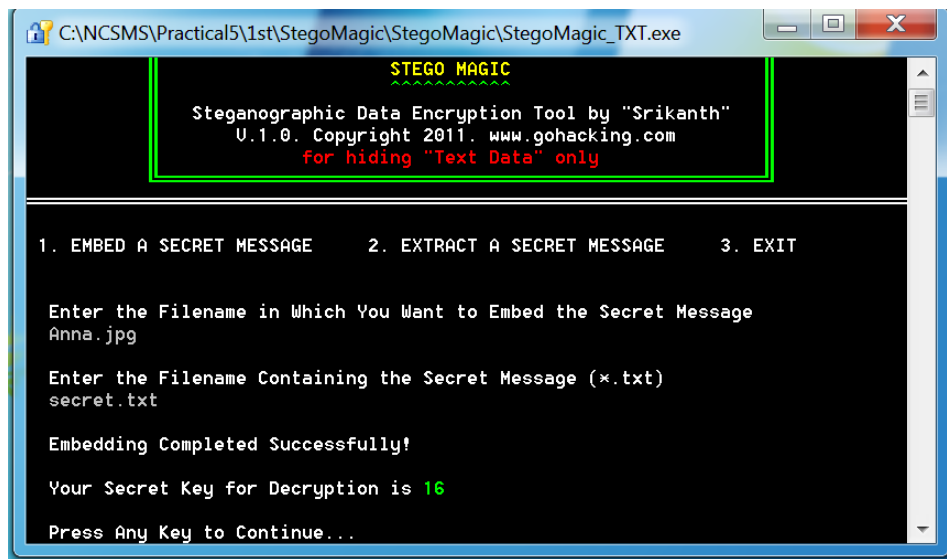
3. Enter the file you wish to be embedded with the secret. (Note that it requires the full extension of the file). In this case, enter Anna.jpg



4. Enter the name of the secret file you wish to embed (Note that it requires the full extension of the file).

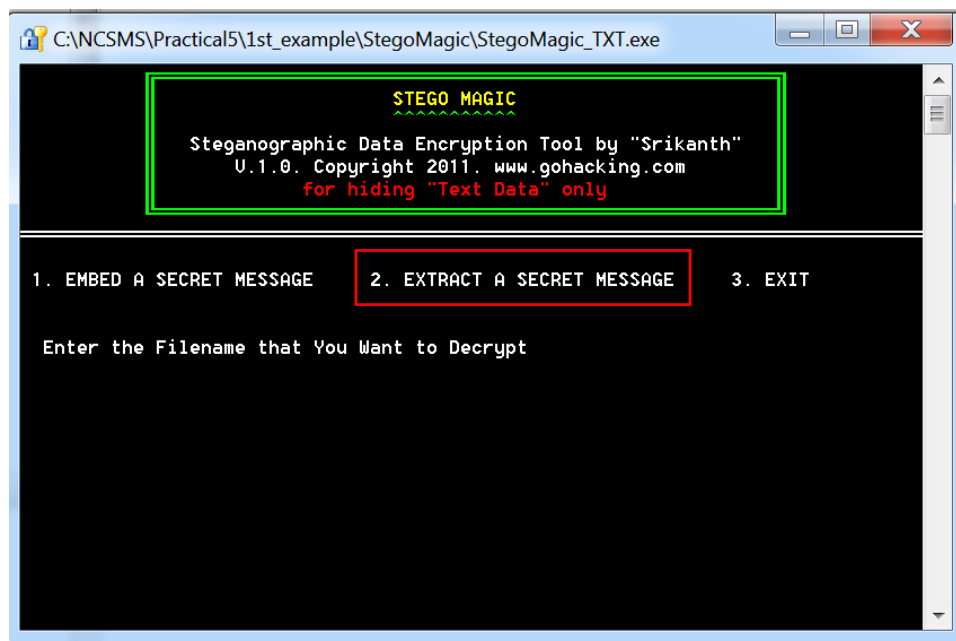


5. Successfully embedded secret text into a photo.

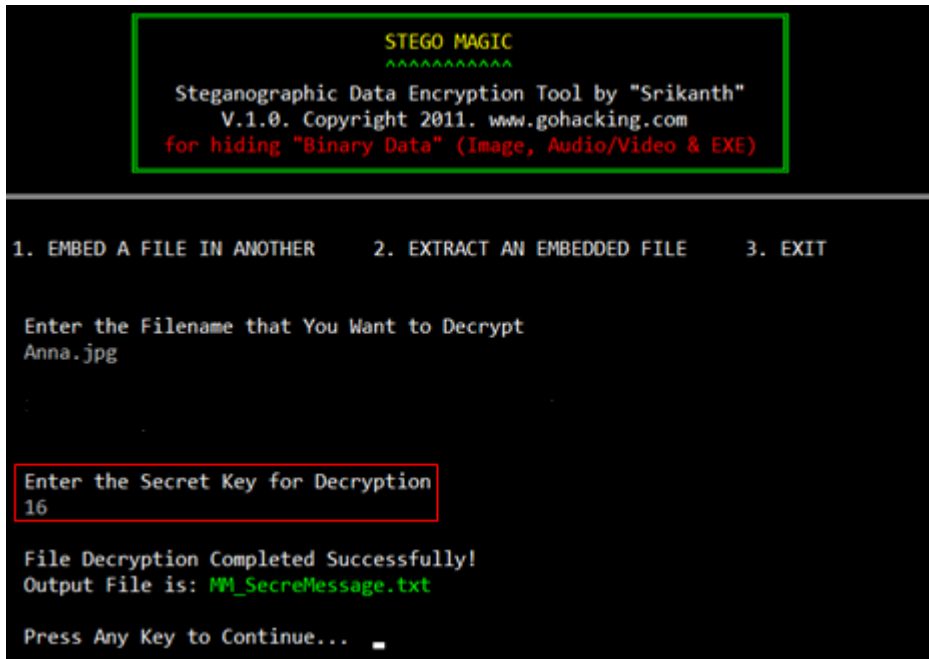


DECRYPTING A FILE

1. Select the second option "2. Extract A Secret Message".



2. Enter the file that you wish to decrypt and follow by the secret key (in the case if you follow the previous step the secret key is **16**).



```

      STEGO MAGIC
      ^^^^^^^^^^^
      Steganographic Data Encryption Tool by "Srikanth"
      V.1.0. Copyright 2011. www.gohacking.com
      for hiding "Binary Data" (Image, Audio/Video & EXE)

1. EMBED A FILE IN ANOTHER    2. EXTRACT AN EMBEDDED FILE    3. EXIT

Enter the Filename that You Want to Decrypt
Anna.jpg

Enter the Secret Key for Decryption
16

File Decryption Completed Successfully!
Output File is: MM_SecreMessage.txt

Press Any Key to Continue... _
```

3. Upon successfully extracted the info, an output file "MM_SecretMessage.txt" is created. Can go file explore to view the content of MM_SecretMessage.txt

6. MP3STEGO

ENCRYPTING A MUSIC FILE

1. First open up cmd.
2. Change directory to the MP3StegDetect Program directory:
Cd <directory that contains MP3Stego program>

CA Select Command Prompt

```
C:\Users\SPLecturing\Desktop\6. Audio Steganography - MP3Stego\6. Audio Steganography - MP3Stego>Encode.exe
```

3. Enter the following command to encode a .txt file with password on a wav file and convert it to mp3 file.

Encode.exe -E tohide.txt -P 123 svega.wav svega.mp3

- -E option is to encrypt the specified file
- -P option is to set the password
- Svega.wav(in the practical we use svega.wav) is the source file
- Svega.mp3 is the target file

CA Command Prompt

```
C:\Users\SPLecturing\Desktop\6. Audio Steganography - MP3Stego\6. Audio Steganography - MP3Stego>Encode.exe -E tohide.txt -P 123 svega.wav svega.mp3
MP3StegoEncoder 1.1.17
See README file for copyright info
Microsoft RIFF, WAVE audio, PCM, mono 44100Hz 16bit, Length: 0: 0:20
MPEG-I layer III, mono Psychoacoustic Model: AT&T
Bitrate=128 kbps De-emphasis: none CRC: off
Encoding "svega.wav" to "svega.mp3"
Hiding "tohide.txt"
[Frame 791 of 791] (100.00%) Finished in 0: 0: 0
```

DECRYPTING A MUSIC FILE

1. Based on the previous encryption, enter the following command to decrypt the music file:

Decode.exe -X -P 123 svega.mp3

- -X option is to decrypt file
- -P option is to set the password

CA Command Prompt

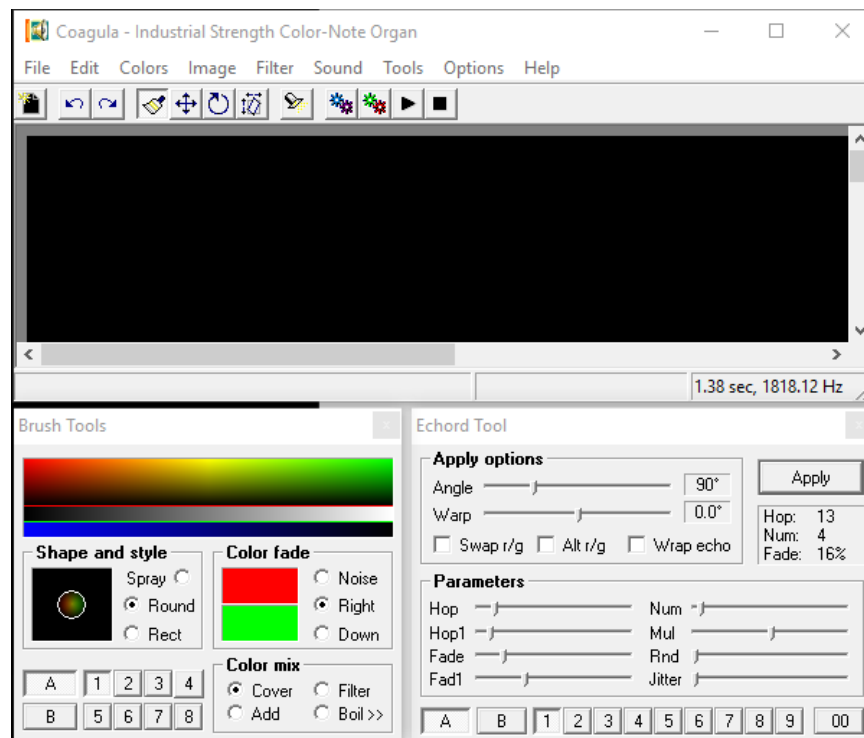
```
C:\Users\SPLecturing\Desktop\6. Audio Steganography - MP3Stego\6. Audio Steganography - MP3Stego>Decode.exe -X -P 123 svega.mp3
MP3StegoEncoder 1.1.17
See README file for copyright info
Input file = 'svega.mp3' output file = 'svega.mp3.pcm'
Will attempt to extract hidden information. Output: svega.mp3.txt
the bit stream file svega.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=3, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=single-ch, sbli=32, jsbd=32, ch=1
[Frame 791]Avg slots/frame = 417.434; b/smp = 2.90; br = 127.839 kbps
Decoding of "svega.mp3" is finished
The decoded PCM output file name is "svega.mp3.pcm"
```

7. COAGULA & SONIC VISUALIZER

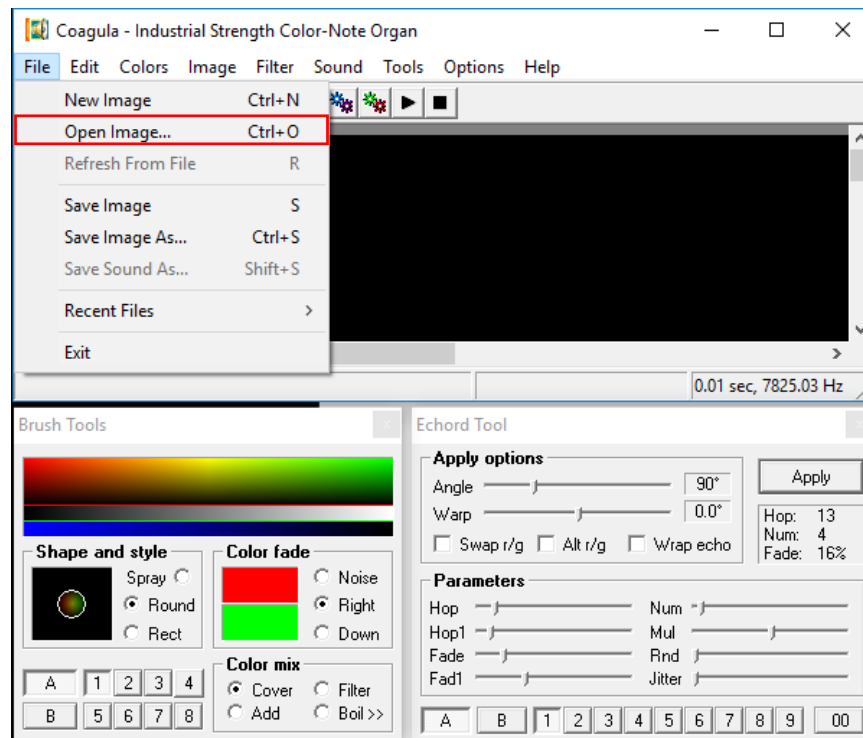
To hide a message in a sound file, we can use **Coagula**. Go to Coagula folder and follow the steps in **Instructions.txt** to hide a message in a wave file and later use **Sonic Visualizer** to unhide a message. You can also follow the steps below. To reveal the message, run **Sonic Visualizer** program.

COAGULA (ENCRYPTING IMAGE INTO A MUSIC FILE)

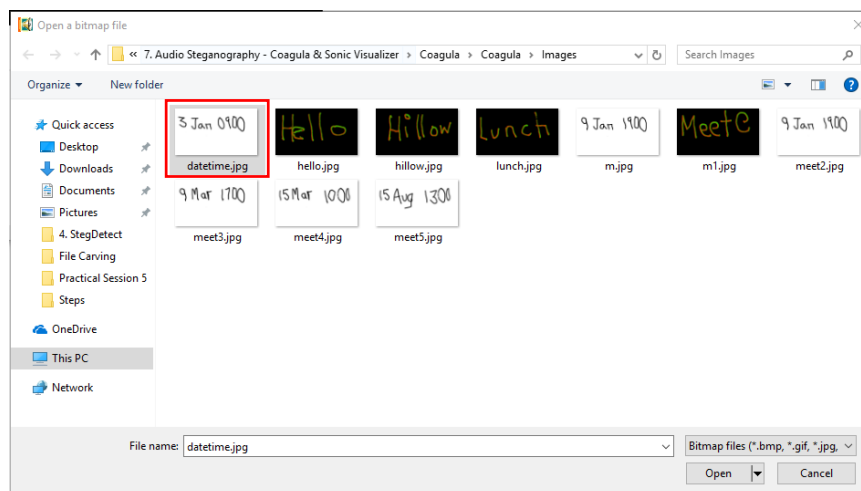
1. After unzip the file, go to folder “Coagula”. Execute Coagula by double click on CoagulaLight.exe.



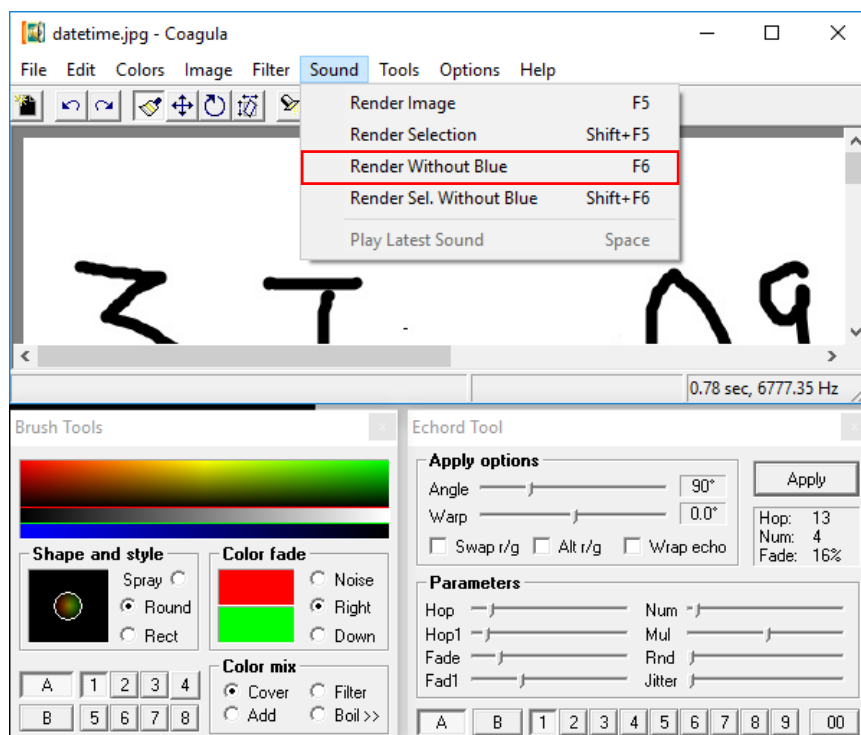
2. Click on file and select “open image”.



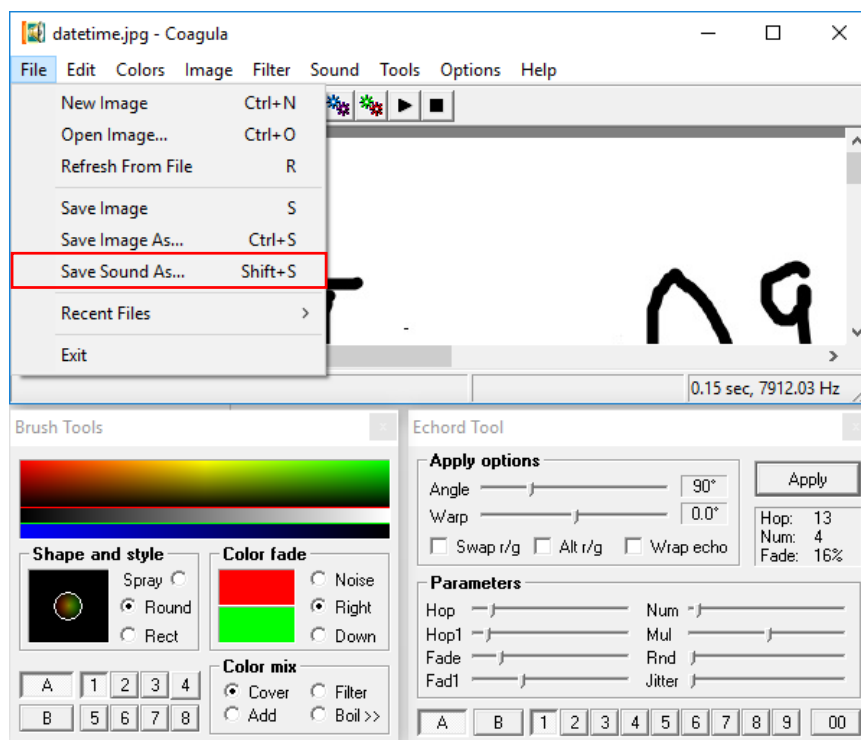
3. Select an image (In this case, datetime.jpg is selected)



4. Then click on the sound option and select “Render Without Blue” option.

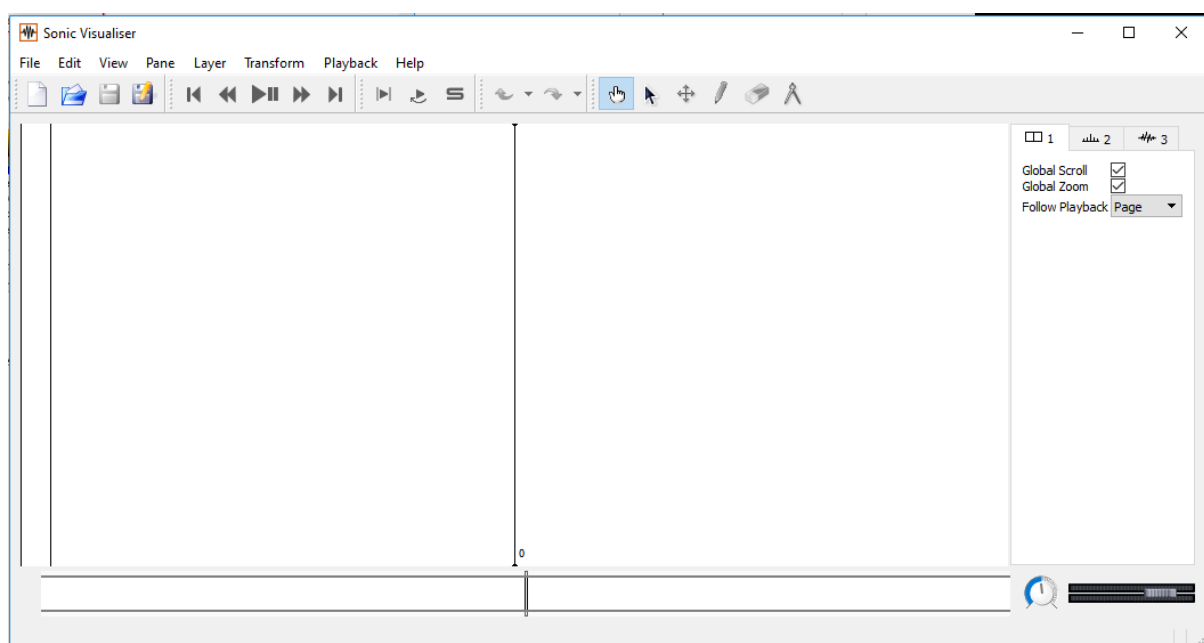


5. Save **sound** as datetime.wav. Remember where you save your file.

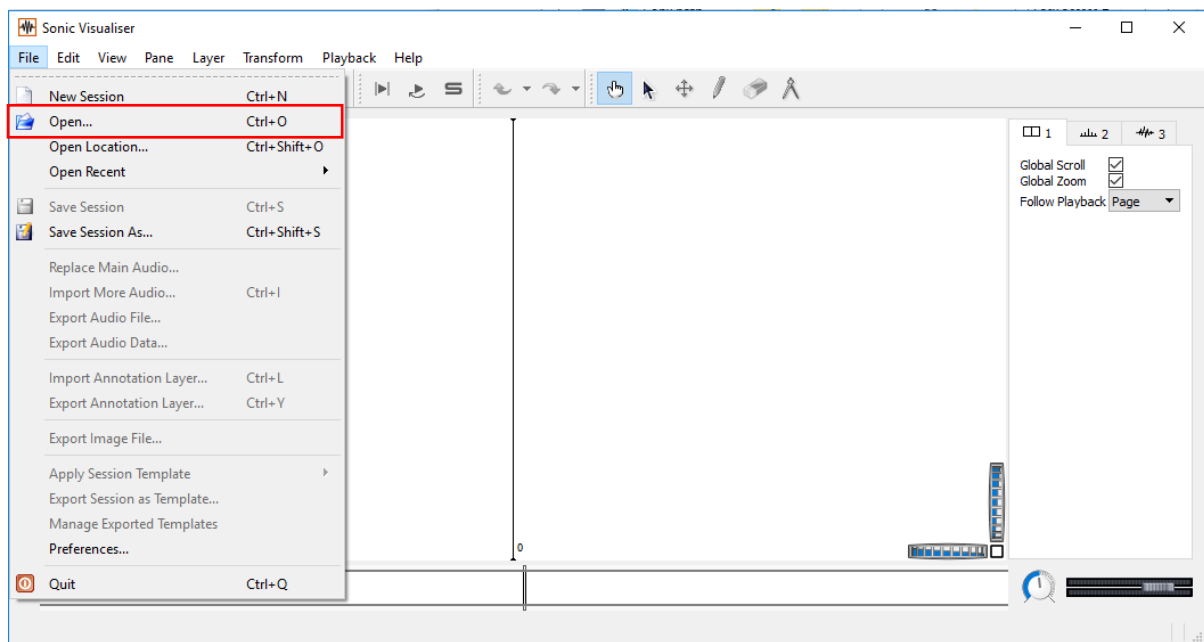


SONIC VISUALIZER (DECRYPTING A MUSIC FILE)

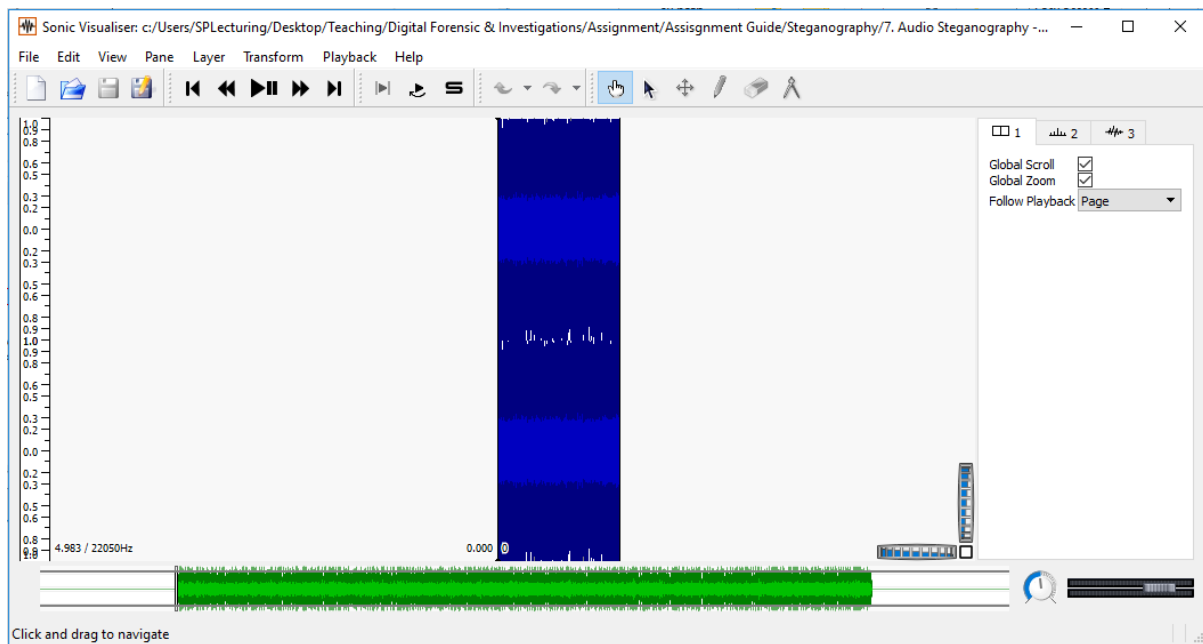
1. Go to Sonic Visualiser folder and execute Sonic Visualizer to show the sound file created above. The following window is shown.



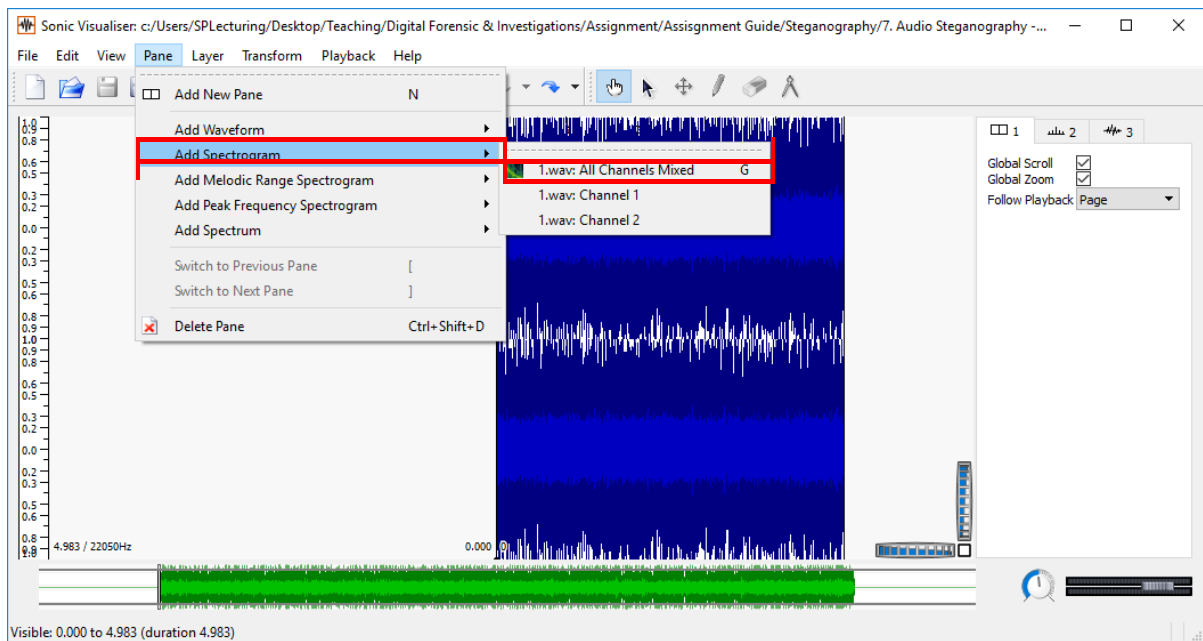
2. Open the wave file “datetiem.wav” saved in the previous step.



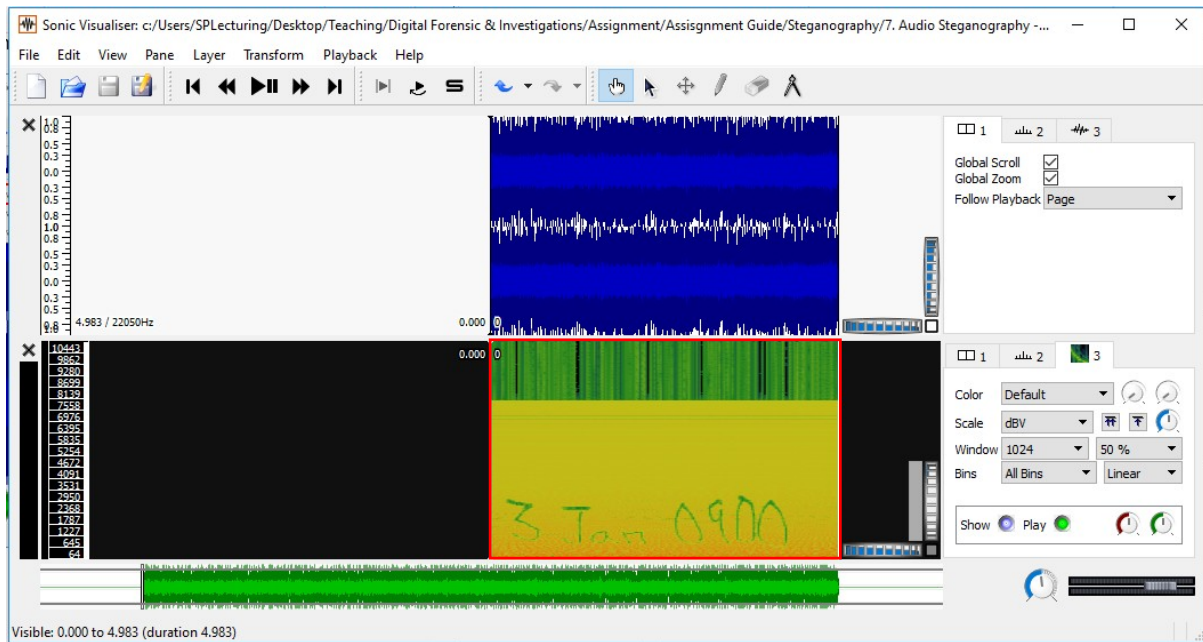
3. Sonic Visualizer should look something like this.



4. Click on "pane", go to "add spectrogram" and select "datetime.wav: All Channels Mixed"



5. The message will be shown on the bottom part of the spectre.



8. EXIF & SPAM MIMIC

EXIF is short for Exchangeable Image File, a format that is a standard for storing interchange information in digital photography image files using JPEG compression. Almost all new digital cameras use the EXIF annotation, storing information on the image such as shutter speed, exposure compensation, F number, what metering system was used, if a flash was used, ISO number, date and time the image was taken, whitebalance, auxiliary lenses that were used and resolution. Some images may even store GPS information so you can easily see where the images were taken!

<https://en.wikipedia.org/wiki/Exif>

JEFFREY'S EXIFVIEWER

<http://regex.info/exif.cgi>

ACKNOWLEDGEMENT

<http://www.pfenninger.ch/homepage/wallpaper/stomboli.jpg>

www.pfenninger.ch/homepage/copyright.jsp

SPAM MIMIC

www.spammimic.com

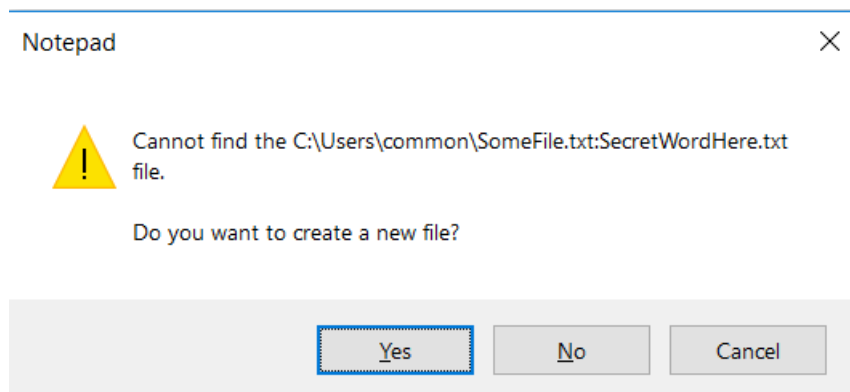
9. HIDING DATA IN A SECRET COMPARTMENT

In order to use this feature, you'll have to open a command prompt and use the following syntax:

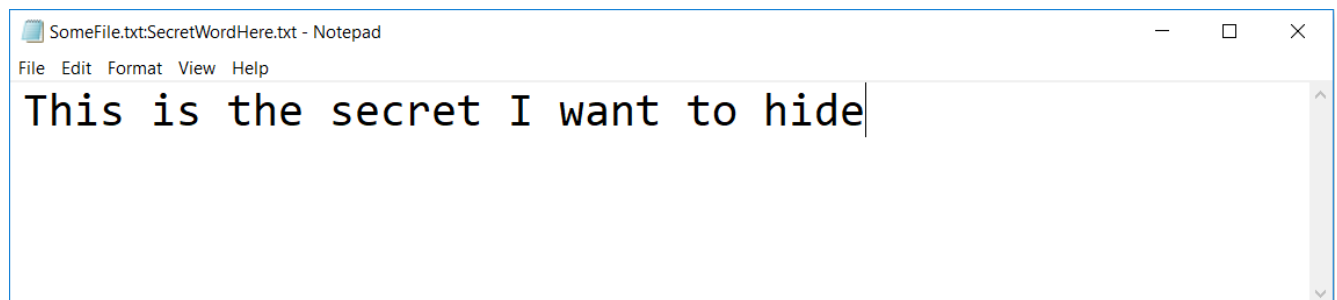
```
notepad SomeFile.txt:SecretWordHere.txt
```

Where SomeFile.txt is the source file and SecretWordHere.txt is the file that you want to hide.

Notepad will automatically ask if you want to create a new file, even if SomeFile.txt already existed, because SecretWordHere.txt doesn't already exist.



Click Yes. Now you can enter secret data you want to hide using notepad, save and close the file:



When you look at SomeFile.txt, it will still be the exact same size as before. Size of file is 0 if SomeFile.txt is a new file.

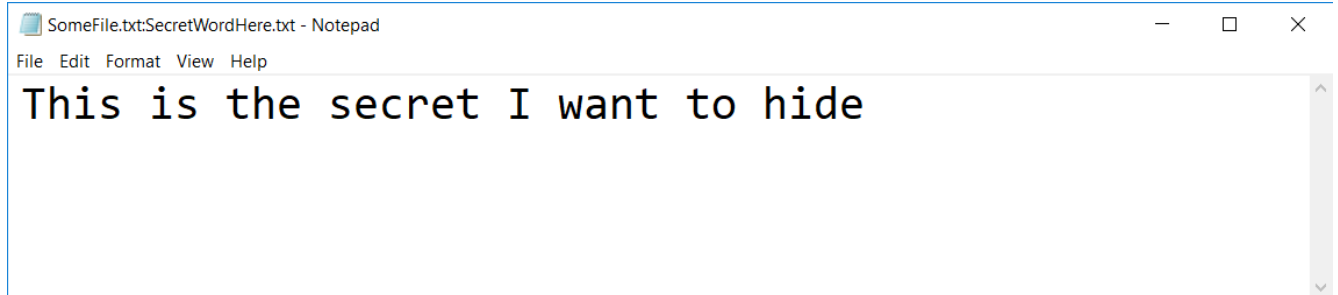
VLC media player	7/12/2017 1:51 PM	Shortcut	2 KB
Zoom	3/4/2019 10:56 PM	Shortcut	2 KB
SomeFile.txt	11/11/2019 5:02 PM	Text Document	0 KB

DISM

When double click on SomeFile.txt, there is nothing inside.

To view the secrete file, enter the same command again.

```
notepad SomeFile.txt:SecretWordHere.txt
```



%%% End of Practical %%%