

Activity 7: Data Hiding and Steganography

Objectives:

- Practice data hiding techniques.
- Use S-Tools to do image Steganography.
- Use Winhex to hide data.

Part 1: Software installation.

Before we can begin this activity we need to download the software needed into our workstation, which is found with this link: <https://packetstormsecurity.com/files/21688/s-tools4.zip.html>.

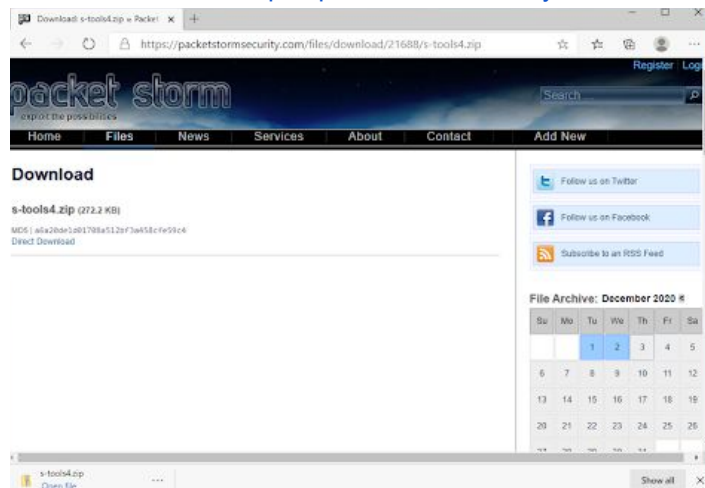


Figure 1: Downloading S-Tools4

Part 2: Create a steganography file using S-Tools.

Now that the zip for the tool has been downloaded, we need to navigate that file in File Explorer and start the s-tools4.exe to download it.

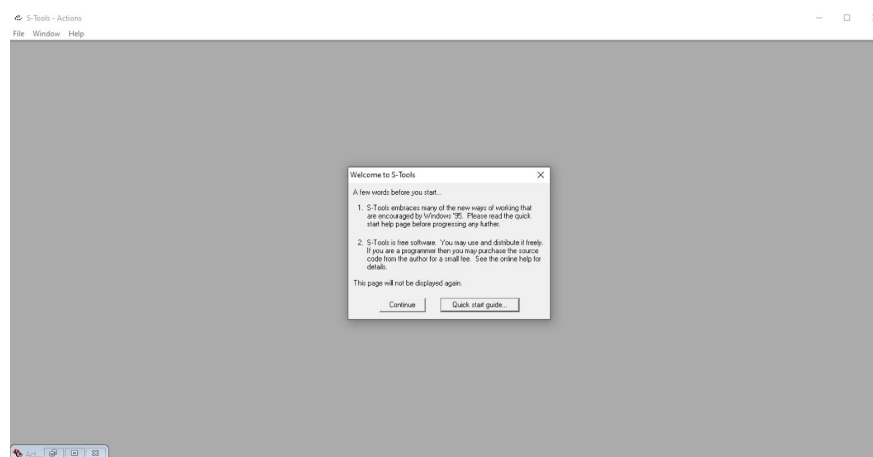


Figure 2: Opening the .exe file to open the tool.

The next step is to download fun.bmp from canvas or google drive: [fun.bmp - Google Drive](#)

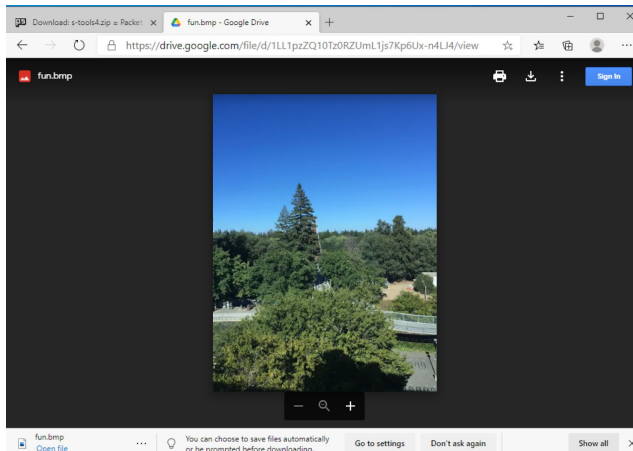


Figure 3: Downloading fun.bmp file from google drive.

Then we need to drag that downloaded fun.bmp file into s-tools.

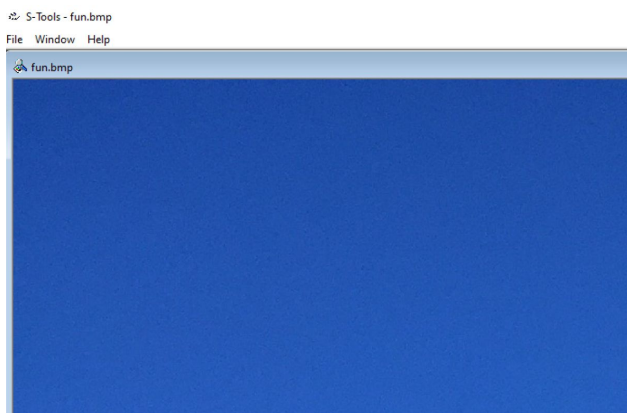


Figure 3: Fun.bmp file is in S-tools.

Next is to create a text file **message.txt** and type our secret message into the file. Then drag that message from its folder and into the **fun.bmp** image. Then in the Hiding dialogue box type “**secret**” for the passphrase and press “**OK**”.



Figure 4: message.txt is created and dragged into S-Tools.

After the hidden data window opens, right-click the window and click **'Save as'**. We'll save the image as **'fun-steg.bmp'**.

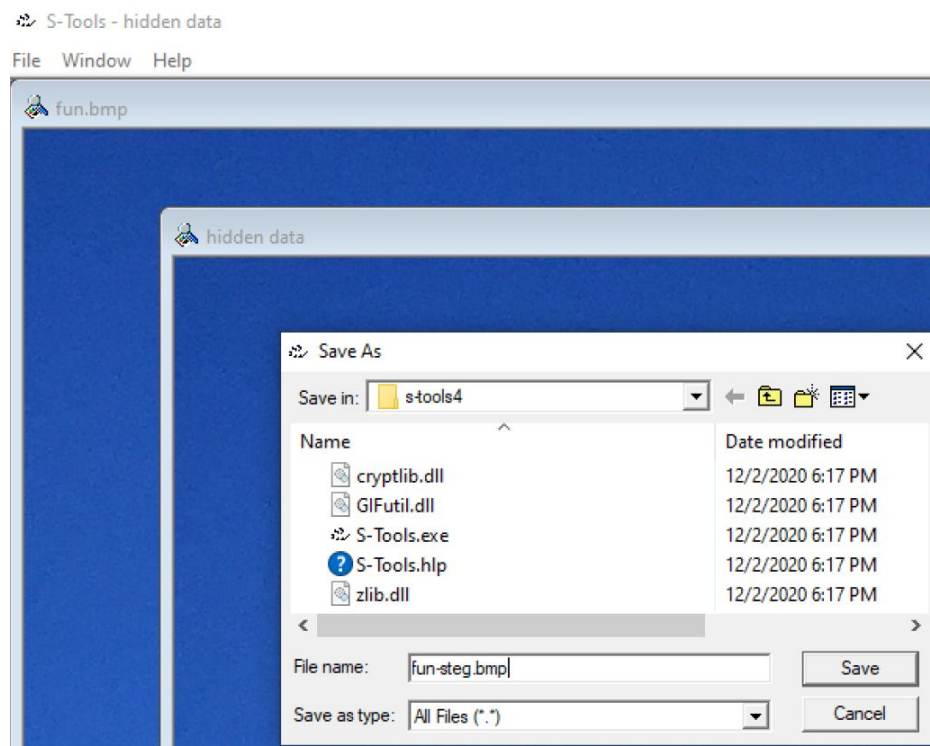


Figure 5: Saving as fun-steg.bmp.

Part 3: Create a steganography file using S-Tools and compare the difference using the DOS command.

Now that is complete we will do something similar but with a different file. Start the **S-Tools.exe**. Download **'scene.bmp'** from canvas or google drive using this link: [scene.bmp - Google Drive](https://drive.google.com/file/d/1hmlYsXdV2SvG2VJYyfQfPCaW14ZBgaGx/view). After the download is complete drag **scene.bmp** into the **S-Tools** window.

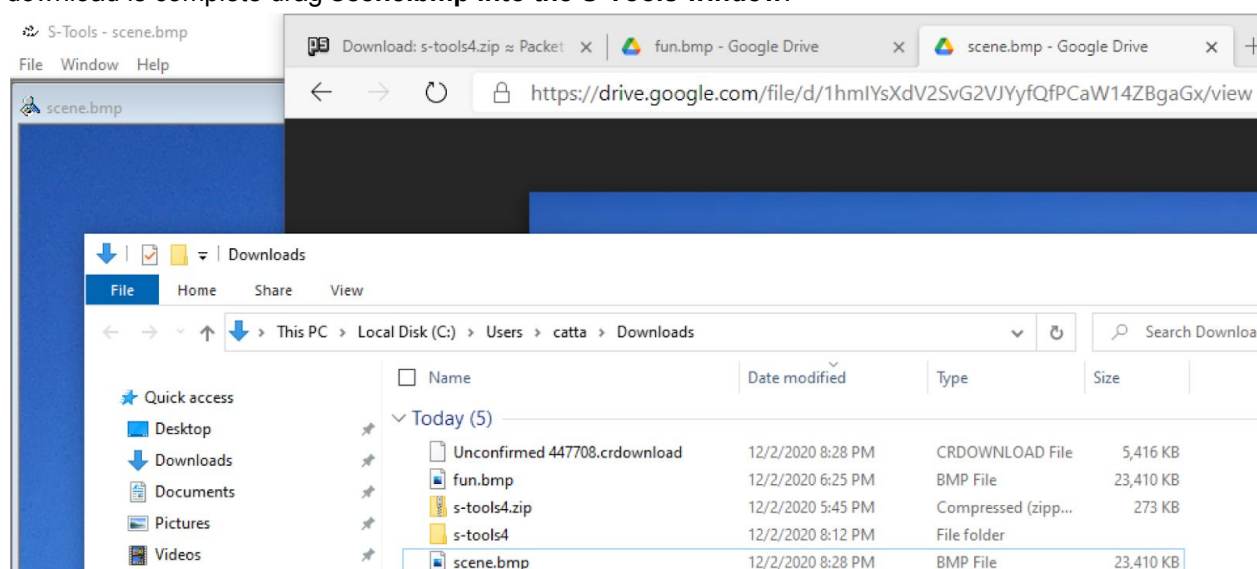


Figure 6: Downloading and dragging scene.bmp into S-Tools.

Once that is complete we now need to create a '**hidden.rtf**' file and type our secret message into that file. Then drag that file into '**scene.bmp**' and type '**secret**' into the passphrase of the hidden dialogue box. Finishing by clicking '**Ok**'.

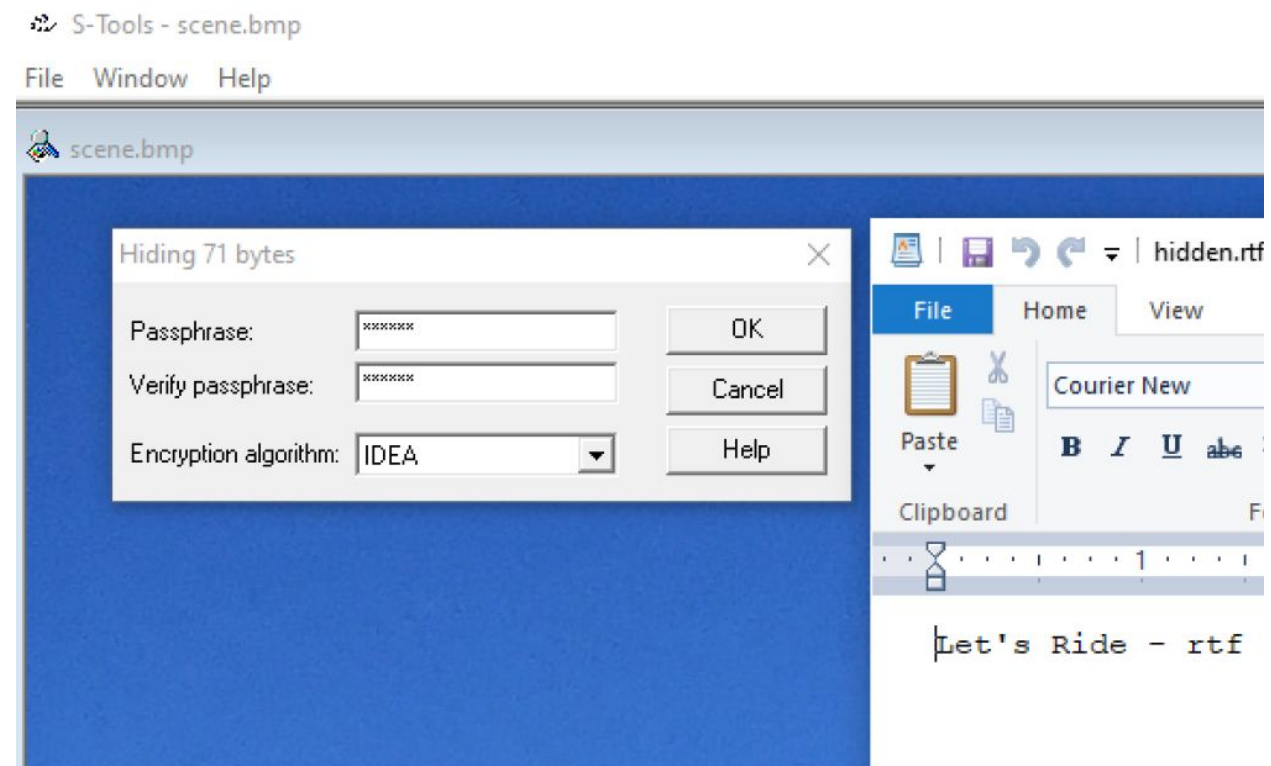


Figure 7: Creating hidden.rtf and drag into scene.bmp.

Once that is complete, **right-click scene.bmp** and click '**Save as**', saving it as **scene-steg.bmp**

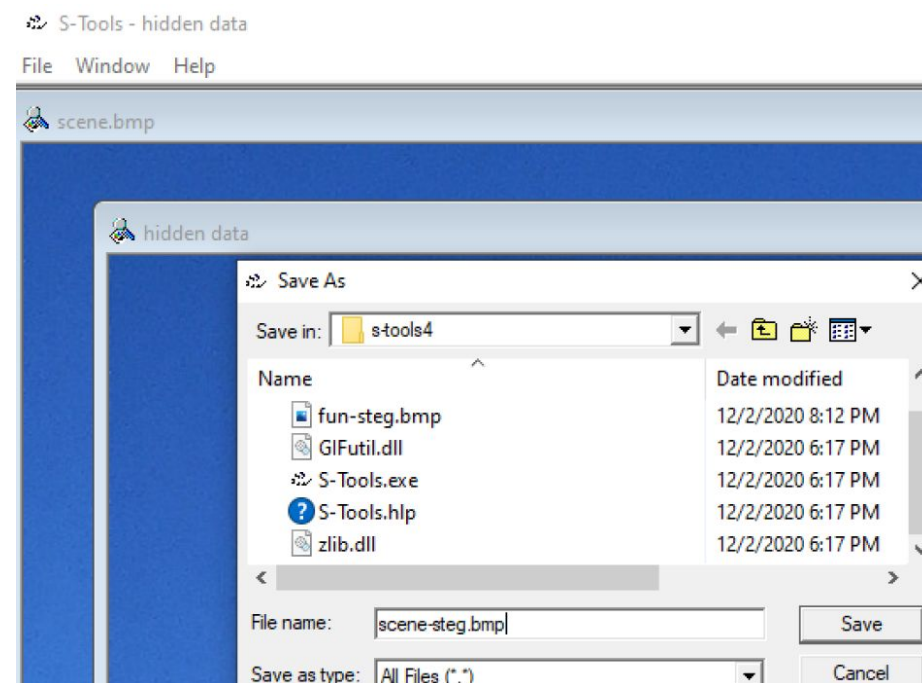
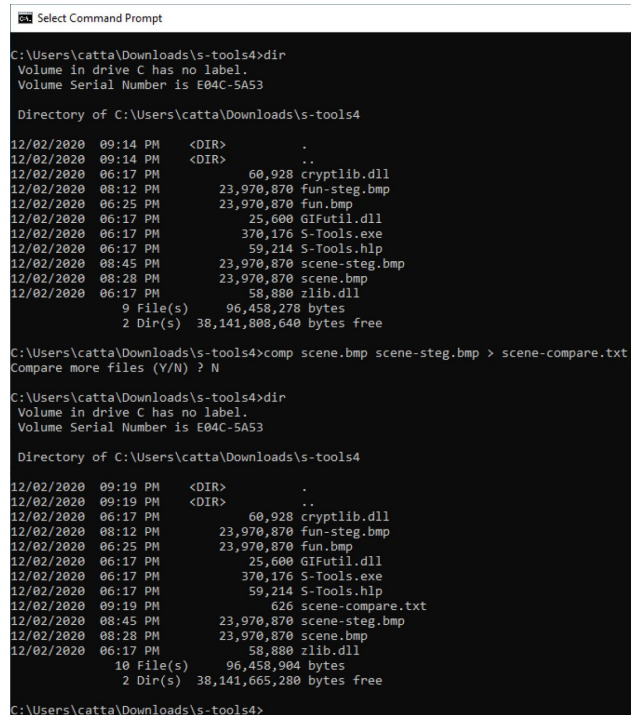


Figure 8: Saving the file as scene-steg.bmp.

Next to do for this part is open up the command prompt and change the directory to where **scene.bmp** and **scene-steg.bmp** are stored using the commands '**cd**' and '**dir**'. Then type in the command '**comp scene.bmp scene-steg.bmp > scene-compare.txt**' and press '**Enter**'. When the window prompts **Compare more files (Y/N)?**, type **n** and hit **Enter**.



```

Select Command Prompt

C:\Users\catta\Downloads\s-tools4>dir
Volume in drive C has no label.
Volume Serial Number is E04C-5A53

Directory of C:\Users\catta\Downloads\s-tools4

12/02/2020  09:14 PM    <DIR>          .
12/02/2020  09:14 PM    <DIR>          ..
12/02/2020  06:17 PM         60,928 cryptlib.dll
12/02/2020  08:12 PM       23,970,870 fun-steg.bmp
12/02/2020  06:25 PM       23,970,870 fun.bmp
12/02/2020  06:17 PM       25,600 GIFutil.dll
12/02/2020  06:17 PM       370,176 S-Tools.exe
12/02/2020  06:17 PM       59,214 S-Tools.hlp
12/02/2020  08:45 PM       23,970,870 scene-steg.bmp
12/02/2020  08:28 PM       23,970,870 scene.bmp
12/02/2020  06:17 PM       58,880 zlib.dll
                9 File(s)      96,458,278 bytes
                2 Dir(s)      38,141,808,640 bytes free

C:\Users\catta\Downloads\s-tools4>comp scene.bmp scene-steg.bmp > scene-compare.txt
Compare more files (Y/N) ? N

C:\Users\catta\Downloads\s-tools4>dir
Volume in drive C has no label.
Volume Serial Number is E04C-5A53

Directory of C:\Users\catta\Downloads\s-tools4

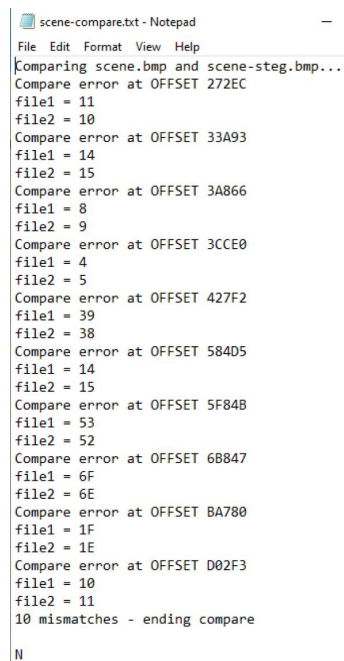
12/02/2020  09:19 PM    <DIR>          .
12/02/2020  09:19 PM    <DIR>          ..
12/02/2020  06:17 PM         60,928 cryptlib.dll
12/02/2020  08:12 PM       23,970,870 fun-steg.bmp
12/02/2020  06:25 PM       23,970,870 fun.bmp
12/02/2020  06:17 PM       25,600 GIFutil.dll
12/02/2020  06:17 PM       370,176 S-Tools.exe
12/02/2020  06:17 PM       59,214 S-Tools.hlp
12/02/2020  09:19 PM         626 scene-compare.txt
12/02/2020  08:45 PM       23,970,870 scene-steg.bmp
12/02/2020  08:28 PM       23,970,870 scene.bmp
12/02/2020  06:17 PM       58,880 zlib.dll
                10 File(s)     96,458,904 bytes
                2 Dir(s)      38,141,665,280 bytes free

C:\Users\catta\Downloads\s-tools4>

```

Figure 9: Creating a scene-compare.txt file to compare scene.bmp and scene-steg.bmp.

In File Explorer, navigate to your work folder and open the scene-compare.txt file to see the discrepancies between the two files.



```

scene-compare.txt - Notepad
File Edit Format View Help
Comparing scene.bmp and scene-steg.bmp...
Compare error at OFFSET 272EC
file1 = 11
file2 = 10
Compare error at OFFSET 33A93
file1 = 14
file2 = 15
Compare error at OFFSET 3A866
file1 = 8
file2 = 9
Compare error at OFFSET 3CCE0
file1 = 4
file2 = 5
Compare error at OFFSET 427F2
file1 = 39
file2 = 38
Compare error at OFFSET 584D5
file1 = 14
file2 = 15
Compare error at OFFSET 5F84B
file1 = 53
file2 = 52
Compare error at OFFSET 6B847
file1 = 6F
file2 = 6E
Compare error at OFFSET BA780
file1 = 1F
file2 = 1E
Compare error at OFFSET D02F3
file1 = 10
file2 = 11
10 mismatches - ending compare

N

```

Figure 10: Discrepancies between the two files.

Part 4: Extract the hidden messages/files.

Opening up S-Tools again, we'll extract the hidden message from **scene-steg.bmp** by dragging it into the S-Tools Window. Then right-click on the picture and choose **'Reveal...'**. Then input the passphrase we set up previously, **'secret'** into the dialogue box.

 S-Tools - scene-steg.bmp

File Window Help

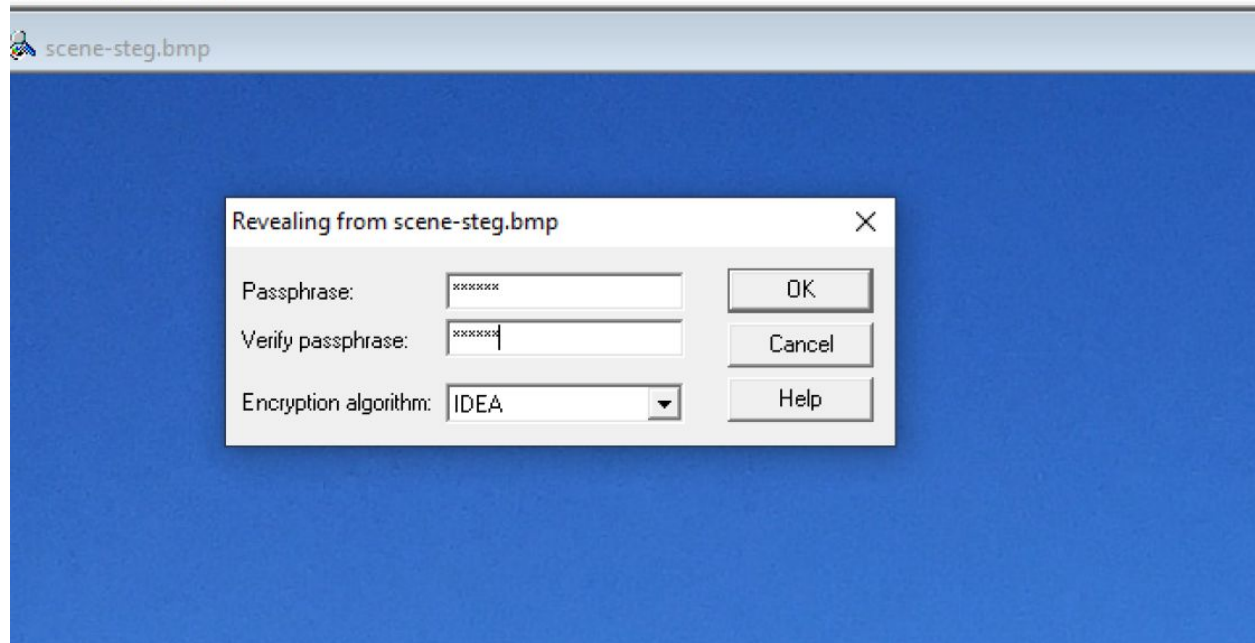


Figure 11: Entering passphrase to Reveal scene-steg.bmp.

In the new opened window, right click the rtf file hidden.rtf and choose to save as.

In your working directory, open the hidden.rtf file to view the content. Compare it with the hidden file you used in part 3 to see if they are the same.

 S-Tools - Revealed Archive

File Window Help

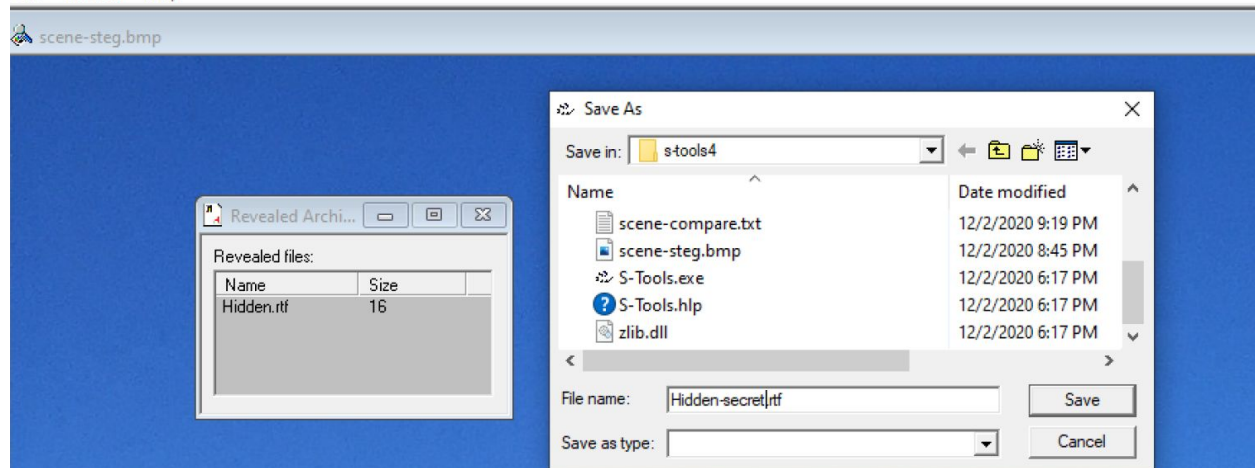


Figure 12: Saving secret text hidden inside scene-steg.bmp.

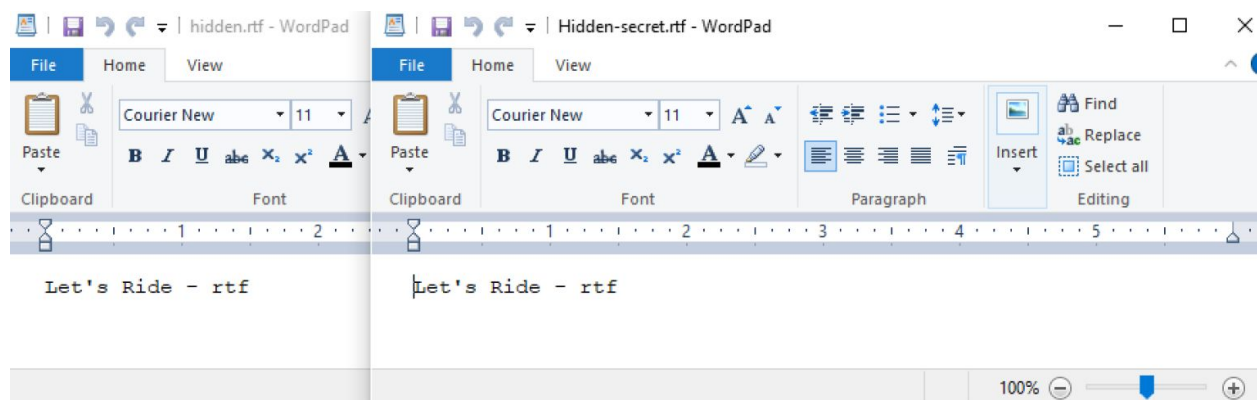


Figure 13: Comparing hidden.rtf and hidden-secret.rtf.

Now we need to repeat the above for fun-steg.bmp.

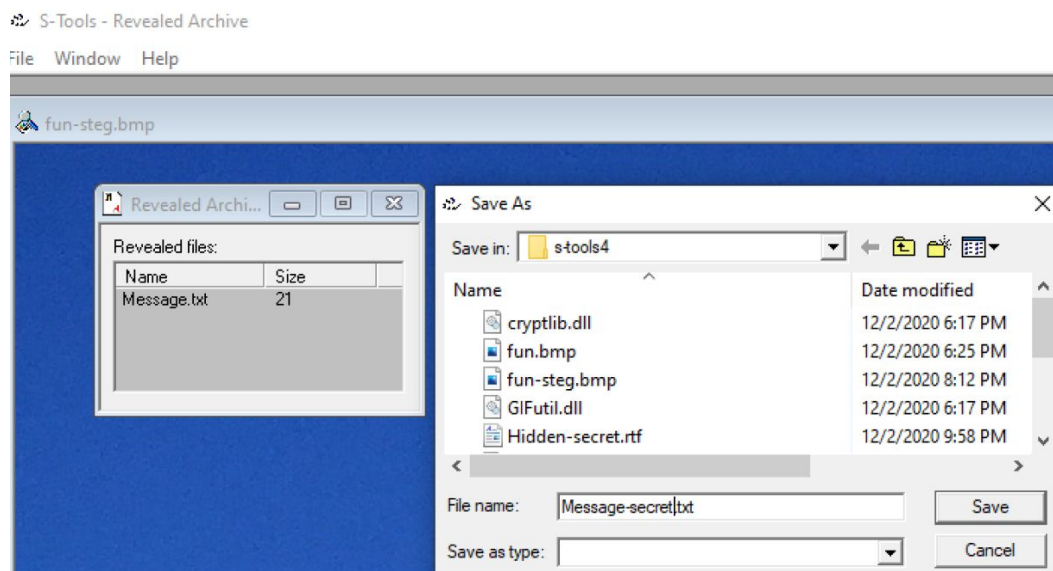


Figure 14: Saving the revealed file from fun-steg.bmp as message-secret.txt.

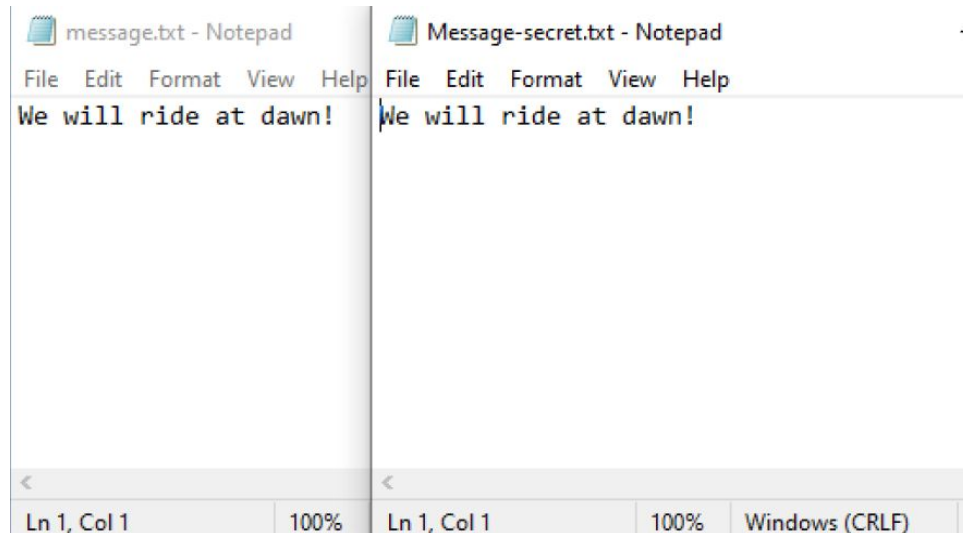


Figure 15: Comparing message.txt and message-secret.txt.

Part 5: Data hiding and recovering using Bit-shifting.

For this part, we first need to create a text file names mess.txt in that file type This is a secret message that I want to send out.'

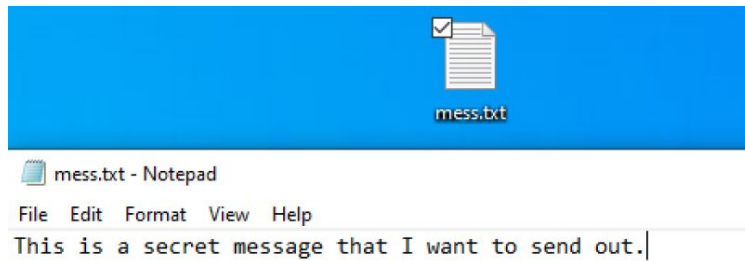


Figure 16: Creating mess.txt.

After that startup, WinHex and File->Open and click on the file we have just created. Then Click on Options->Edit Mode from the menu. Click on the Default Edit Mode (=editable), and then click OK.

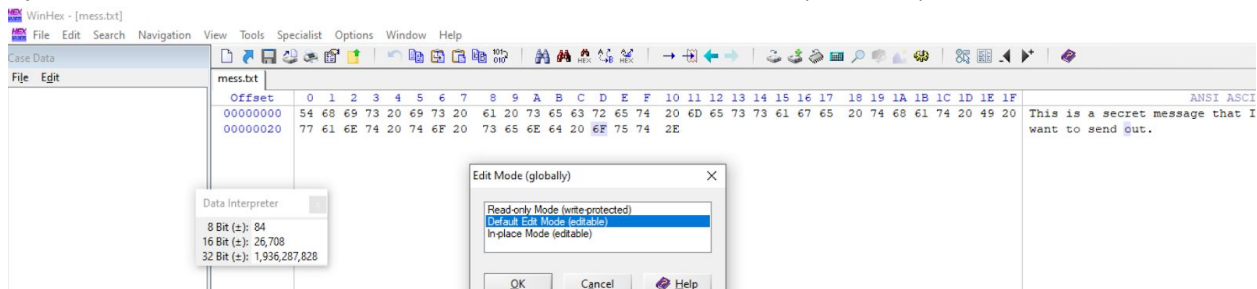


Figure 17: Opening mess.txt in WinHex and changing it to editable.

Next, select all the data in the file, then press 'Edit' -> 'Modify Data', click on the left shift by 1-bit option, then click ok.

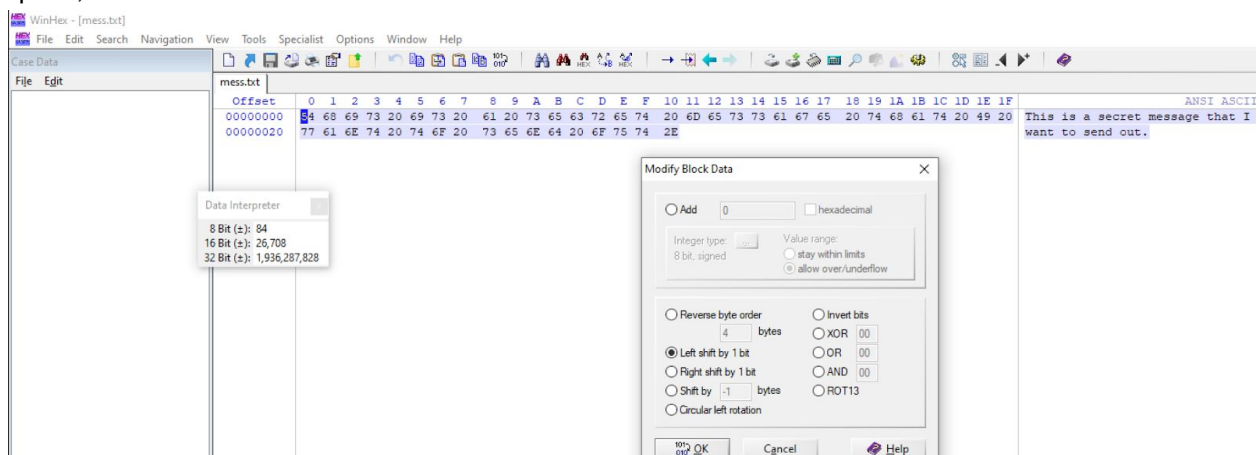


Figure 18: Modifying the data with the left shift by 1 bit.

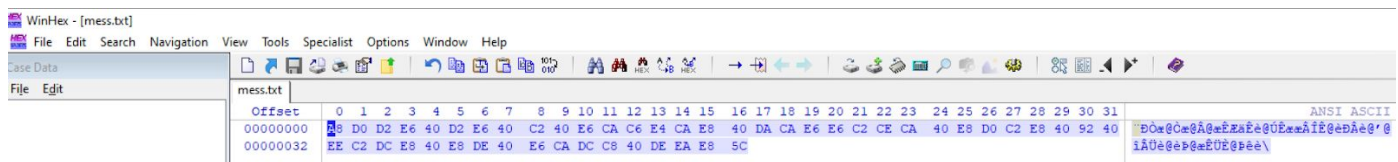


Figure 19: Now the data has random values.

After that modification is made we now 'Save as', mess-shift-left.txt

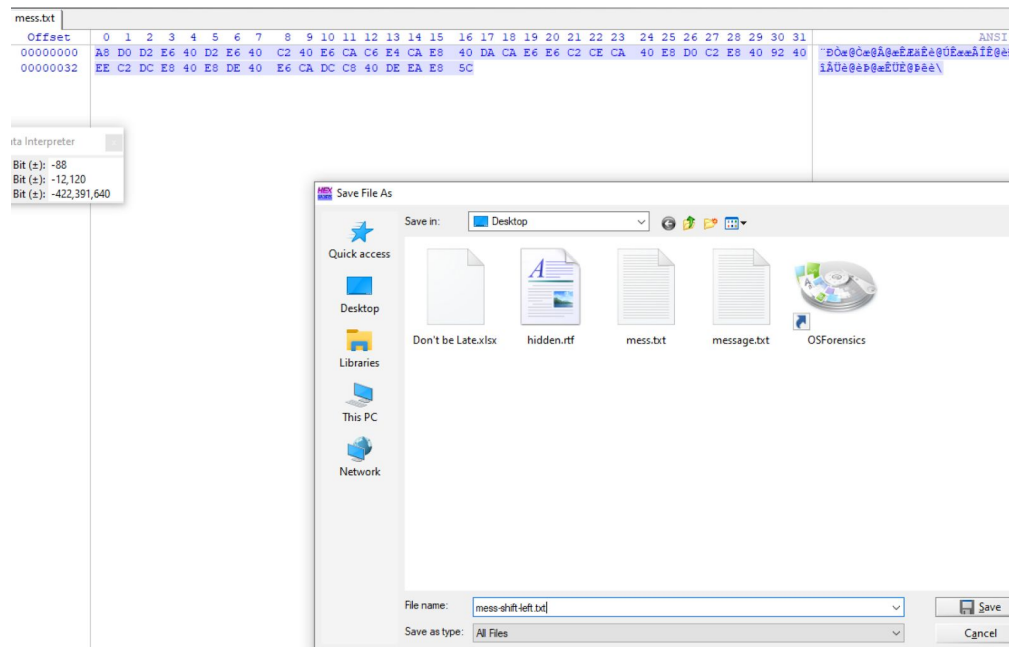


Figure 20: Saving mess-shift-left.txt.

Then to recover the message from mess-shift-left.txt, we need to **shift the bits back by one to the right**. To do so, **select all data Control+A**, Edit Modify data, then in the dialog box press ok.

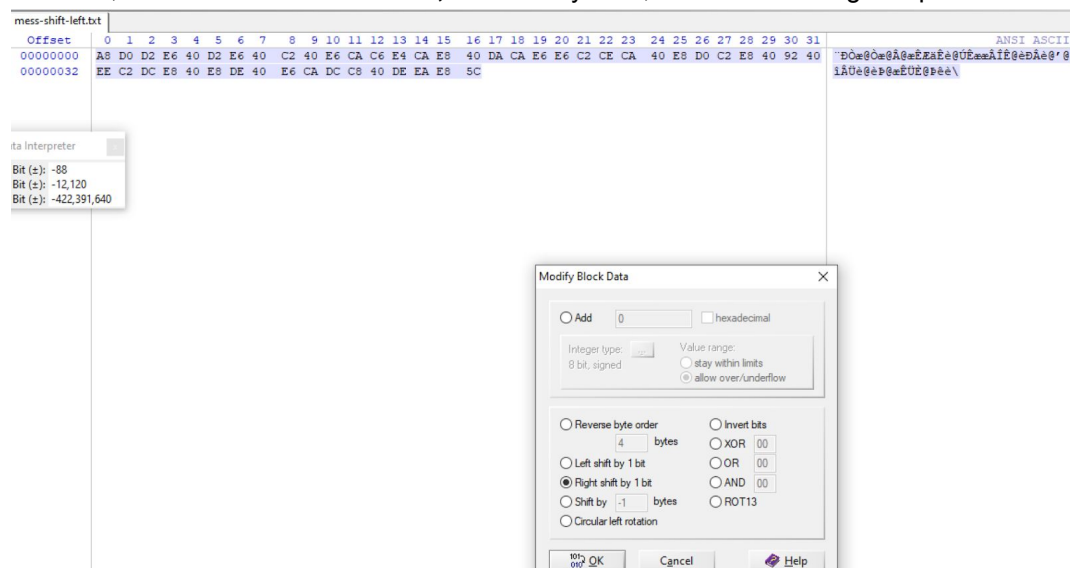


Figure 22: Shifting mess-shift-left.txt 1 bit to the right.

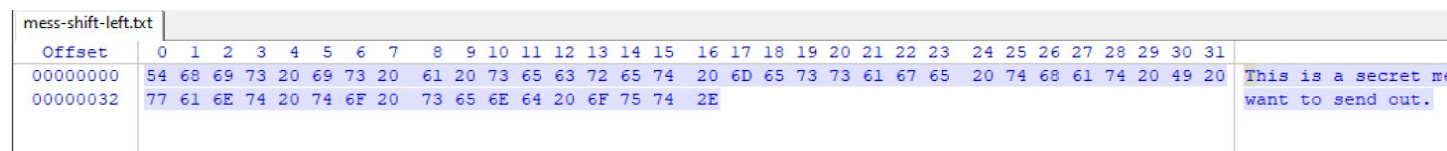


Figure 23: After shift one bit to the right.

After doing so save the file as **mess-shift-right.txt**. Then we will use **WinHex** to compare the **MD5 hash value** of these three files and determine if **mess.txt** is different from **mess-shift-left.txt** and **mess-shift-right.txt**. Open **message.txt**, **message-shift-right.txt**, and **message-shift-left.txt** in Winhex by clicking **File->Open** repeatedly. Click the **message.txt** tab in winhex to make it the active file, select the content by clicking **Edit->Select All** from the menu. Click on **Tools->Compute Hash** from the menu to open the **Compute hash dialog box**. In the list box, click **MD5** and then **OK**. Copy the MD5 hash value to a new text document.

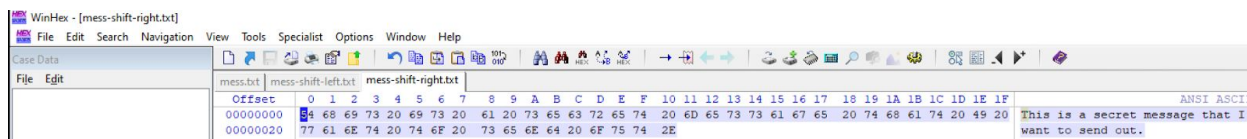


Figure 24: Saving mess-shift-right.txt, and having all files open in Winhex.

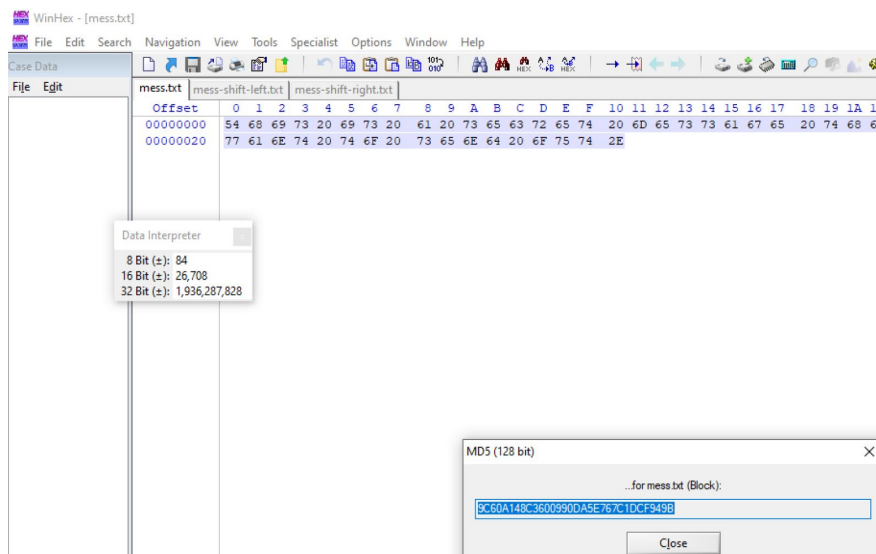


Figure 25: MD5 Hash value for mess.txt.

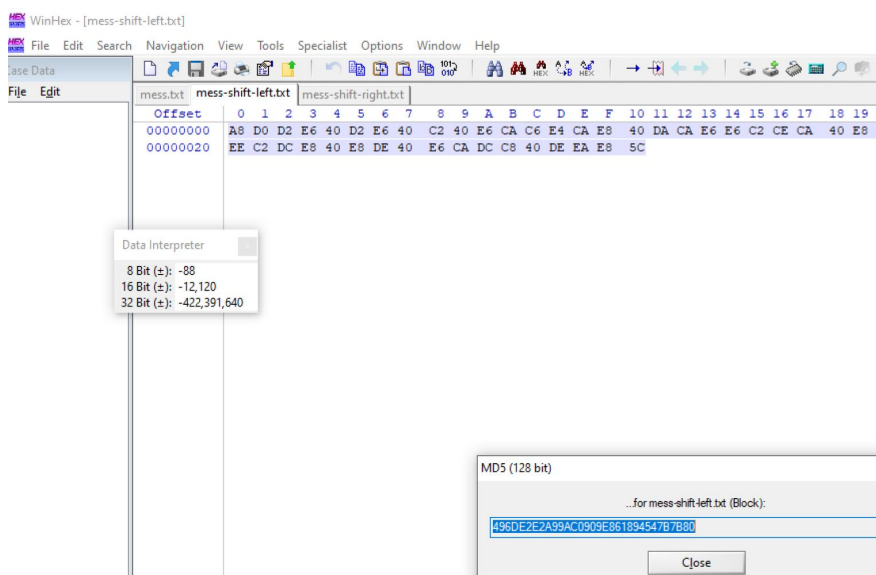


Figure 26: MD5 Hash value for mess-shift-left.txt.

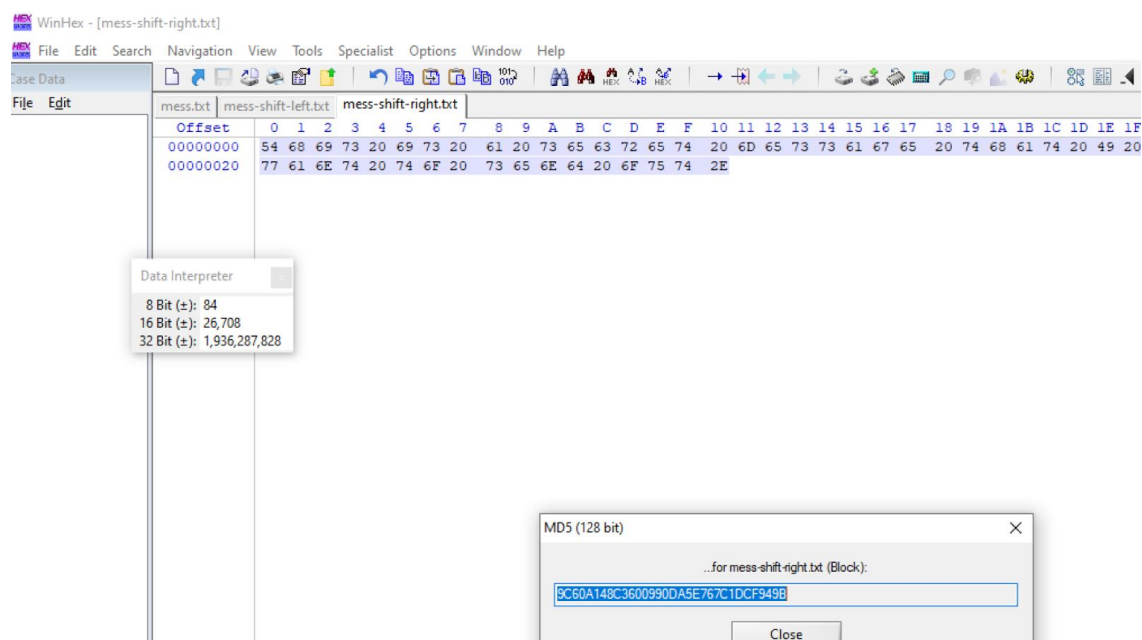


Figure 27: MD5 Hash value for mess-shift-right.txt.

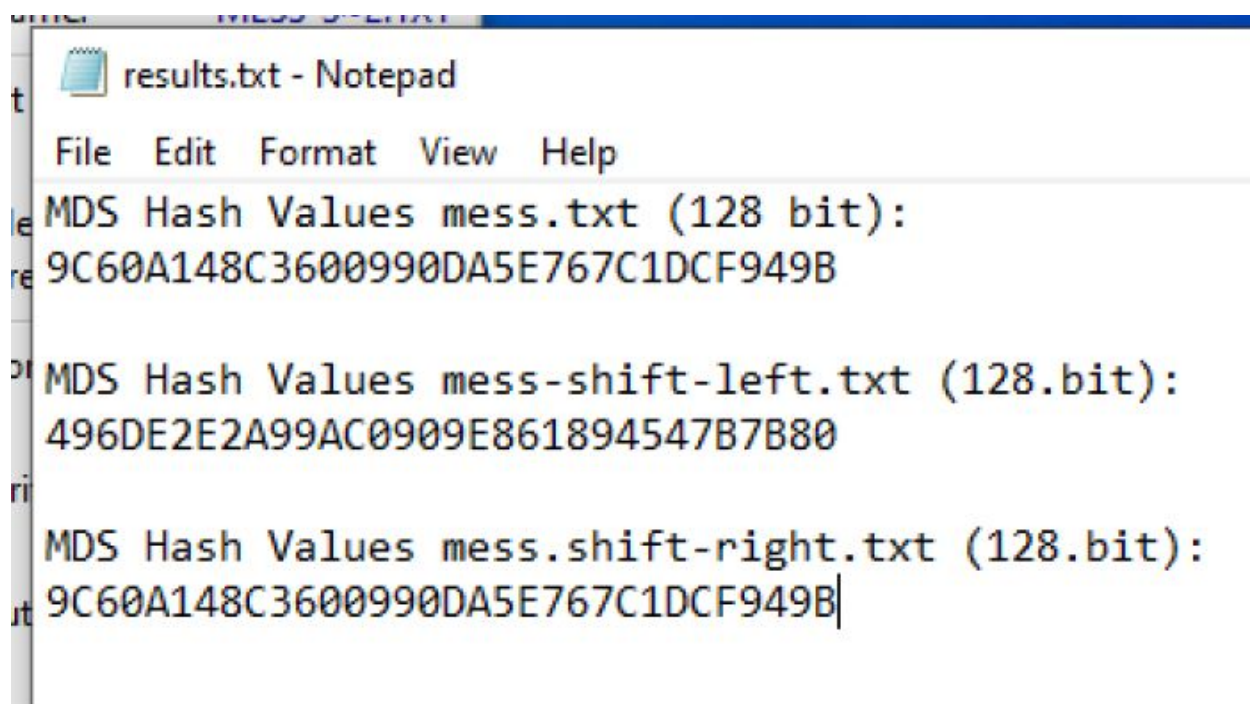


Figure 28: text document will all MD5 Hash values.

As we can see from the hash outputs above, and in Figures 25, 26, 27, and 28 the MD5 Hash values for message.txt and message-shift-right.txt match one another, meaning the files are identical. The hash value for message-shift-left.txt is not the same, because this is our pseudo-encrypted file.

Part 6: Data hiding and recovering using XOR.

For this last part, we need to create another text file called test.txt and type a short message such as your name. In this case, 'Hello World! - Catherine Nguyen'.

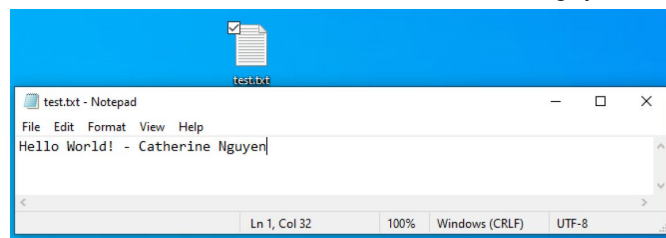


Figure 29: Creating test.txt

Now we need to **start up WinHex** and **open the test.txt file**. **Select all the data** in that file with **control+A**, then click on **Edit->Modify Data** and in the dialogue box click on the **XOR** option. Type in two **binary bits** such as **10** in the box, and then click OK.

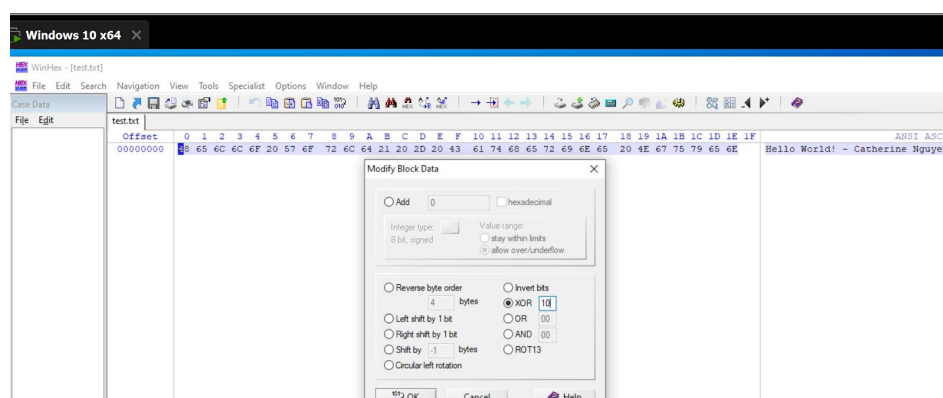


Figure 30: Modifying test.txt with XOR binary bits 10.

After doing so, save the file with **File->Save as test-xor.txt**. The text should now be random.

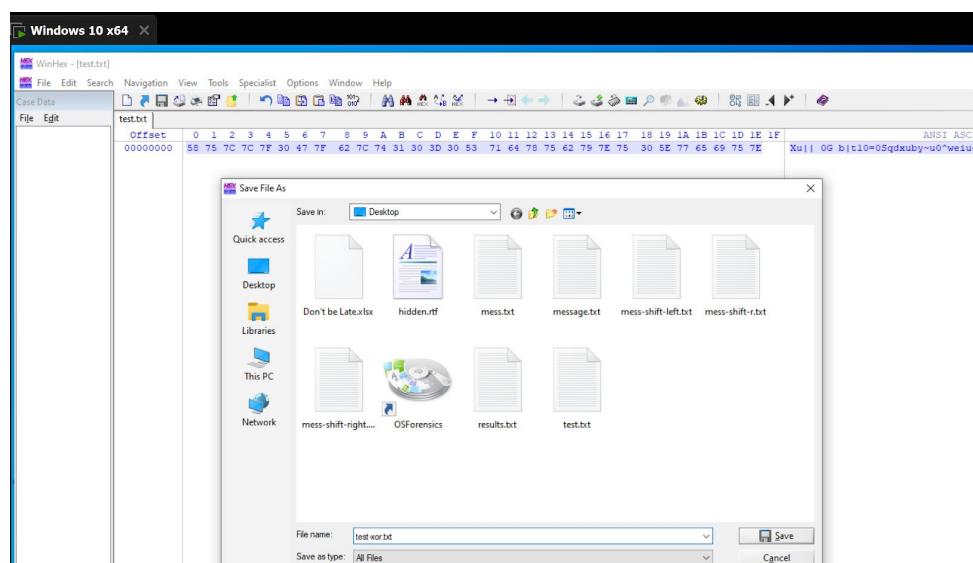


Figure 31: Saving file test-xor.txt file.

Next, we need to perform the XOR towards test-xor.txt to recover the message. Then we need to repeat some steps above.

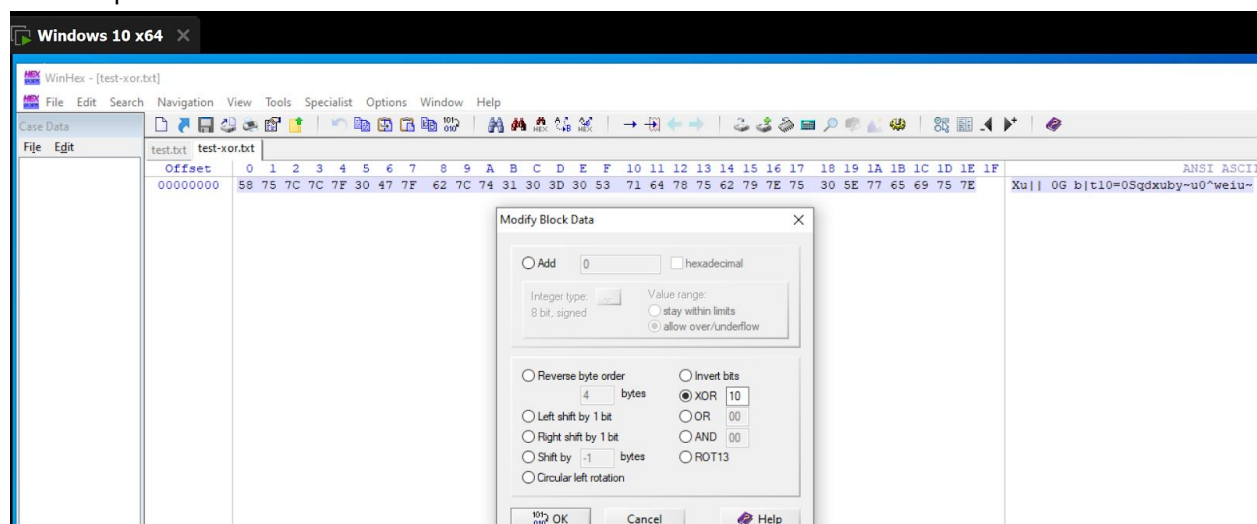


Figure 32: Modifying test-xor.txt with XOR 10.

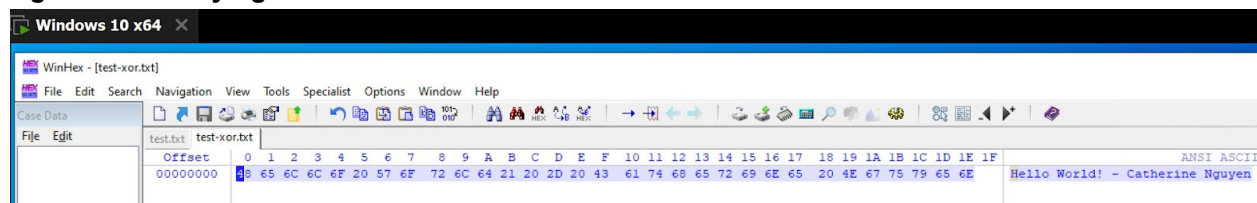


Figure 33: After performing XOR 10.

As we can see the secret message has been recovered!

Questions:

1. To reveal the hidden data using S-Tools, which information is required?

- First, you need to drag a file with hidden data into S-Tool then right-click and press 'Reveal...'. However, you will need the passphrase in order to reveal or hide any data and select the desired encryption algorithm you want.

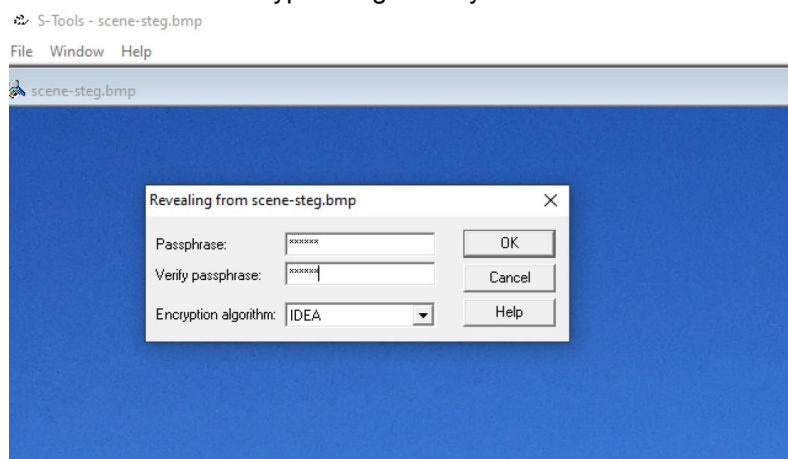
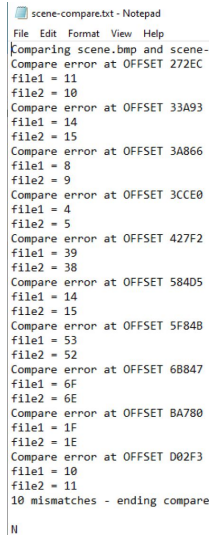


Figure 34: Using Reveal in S-Tool - Passphrase needed.

2. In Part 3, Are there any differences between scene.bmp and scene-steg.bmp?

- a. Yes, there was a difference. This was confirmed by running the following command in command prompt 'comp scene.bmp scene-steg.bmp > scene-compare.txt'. After doing so you can open scene-compare.txt and see all the differences.

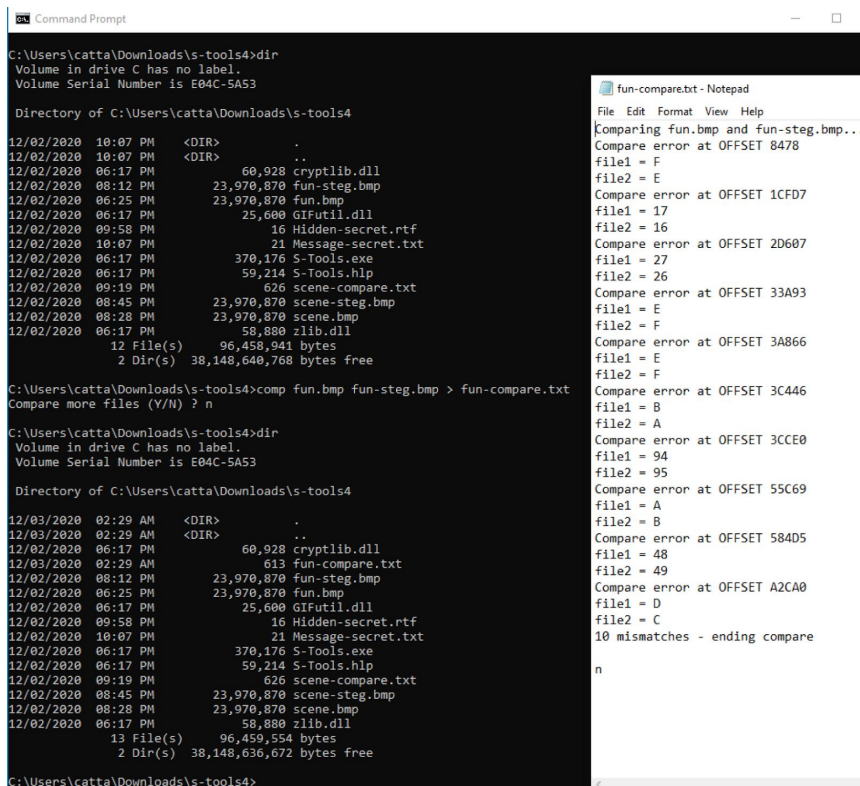


```
scene-compare.txt - Notepad
File Edit Format View Help
Comparing scene.bmp and scene-steg.bmp...
Compare error at OFFSET 272EC
file1 = 11
file2 = 10
Compare error at OFFSET 33A93
file1 = 14
file2 = 15
Compare error at OFFSET 3A866
file1 = 8
file2 = 9
Compare error at OFFSET 3CCE0
file1 = 4
file2 = 5
Compare error at OFFSET 427F2
file1 = 39
file2 = 38
Compare error at OFFSET 584D5
file1 = 14
file2 = 15
Compare error at OFFSET 5F848
file1 = 53
file2 = 52
Compare error at OFFSET 6B847
file1 = 6F
file2 = 6E
Compare error at OFFSET BA780
file1 = 1F
file2 = 1E
Compare error at OFFSET D02F3
file1 = 10
file2 = 11
10 mismatches - ending compare
N
```

Figure 35: Discrepancies between the two files.

3. In Part 3, Are there any differences between fun.bmp and fun-steg.bmp?

- a. Yes, there is a difference we can run the similar command in question 3, but replace the names of the files to get the results. comp fun.bmp fun-steg.bmp > fun-compare.txt.



```
Command Prompt
C:\Users\catta\Downloads\s-tools4>dir
Volume in drive C has no label.
Volume Serial Number is E04C-5A53

Directory of C:\Users\catta\Downloads\s-tools4

12/02/2020 10:07 PM <DIR>          .
12/02/2020 10:07 PM <DIR>          ..
12/02/2020 06:17 PM             60,928 cryptlib.dll
12/02/2020 08:12 PM      23,970,870 fun-steg.bmp
12/02/2020 06:25 PM      23,970,870 fun.bmp
12/02/2020 06:17 PM      25,600 GIFutil.dll
12/02/2020 09:58 PM             16 Hidden-secret.rtf
12/02/2020 10:07 PM             21 Message-secret.txt
12/02/2020 06:17 PM      370,176 S-Tools.exe
12/02/2020 06:17 PM      59,214 S-Tools.hlp
12/02/2020 09:19 PM      626 scene-compare.txt
12/02/2020 08:45 PM      23,970,870 scene-steg.bmp
12/02/2020 08:28 PM      23,970,870 scene.bmp
12/02/2020 06:17 PM      58,880 zlib.dll
                12 File(s)      96,458,941 bytes
                2 Dir(s)  38,148,640,768 bytes free

C:\Users\catta\Downloads\s-tools4>comp fun.bmp fun-steg.bmp > fun-compare.txt
Compare more files (Y/N) ? n

C:\Users\catta\Downloads\s-tools4>dir
Volume in drive C has no label.
Volume Serial Number is E04C-5A53

Directory of C:\Users\catta\Downloads\s-tools4

12/03/2020 02:29 AM <DIR>          .
12/03/2020 02:29 AM <DIR>          ..
12/02/2020 06:17 PM             60,928 cryptlib.dll
12/03/2020 02:29 AM             613 fun-compare.txt
12/02/2020 08:12 PM      23,970,870 fun-steg.bmp
12/02/2020 06:25 PM      23,970,870 fun.bmp
12/02/2020 06:17 PM      25,600 GIFutil.dll
12/02/2020 09:58 PM             16 Hidden-secret.rtf
12/02/2020 10:07 PM             21 Message-secret.txt
12/02/2020 06:17 PM      370,176 S-Tools.exe
12/02/2020 06:17 PM      59,214 S-Tools.hlp
12/02/2020 09:19 PM      626 scene-compare.txt
12/02/2020 08:45 PM      23,970,870 scene-steg.bmp
12/02/2020 08:28 PM      23,970,870 scene.bmp
12/02/2020 06:17 PM      58,880 zlib.dll
                13 File(s)      96,459,554 bytes
                2 Dir(s)  38,148,636,672 bytes free

C:\Users\catta\Downloads\s-tools4>

fun-compare.txt - Notepad
File Edit Format View Help
Comparing fun.bmp and fun-steg.bmp...
Compare error at OFFSET 8478
file1 = F
file2 = E
Compare error at OFFSET 1CFD7
file1 = 17
file2 = 16
Compare error at OFFSET 2D607
file1 = 27
file2 = 26
Compare error at OFFSET 33A93
file1 = E
file2 = F
Compare error at OFFSET 3A866
file1 = E
file2 = F
Compare error at OFFSET 3C446
file1 = B
file2 = A
Compare error at OFFSET 3CCE0
file1 = 94
file2 = 95
Compare error at OFFSET 55C69
file1 = A
file2 = B
Compare error at OFFSET 584D5
file1 = 48
file2 = 49
Compare error at OFFSET A2CA0
file1 = D
file2 = C
10 mismatches - ending compare
n
```

Figure 36: Comparing in Command, and the Difference between the files.

4. In Part 5, among the hash values for message.txt, message-shift-right.txt, and message-shiftright.txt, which ones are the same?
- a. Based on the hash values that were calculated mess.txt and mess-shift-right.txt matched because mess-shift-right.txt is a recovered version of mess.txt.

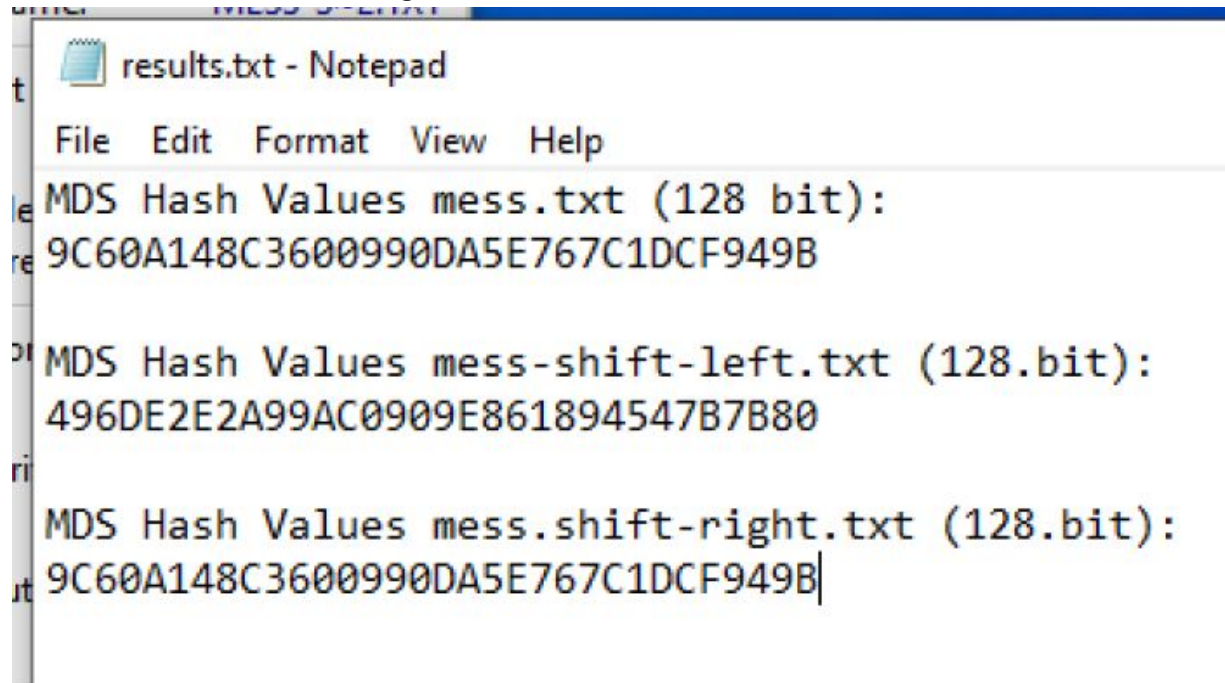


Figure 37: Collected results of MD5 Hash Values in (128 bit).

5. In class, we've discussed that **INFORMATION XOR RANDOM_NUMBER = NONSENSE**. What will be generated if we do **NONSENSE XOR RANDOM_NUMBER**?
- a. Then we get INFORMATION back once more. This is demonstrated by the results of Part 6. It's just really weak (pseudo) encryption, where the key is NONSENSE. We can see in Part 6 our key would just be 0x10. This is how we're able to recover the data again by XOR'ing the XOR'd to file.

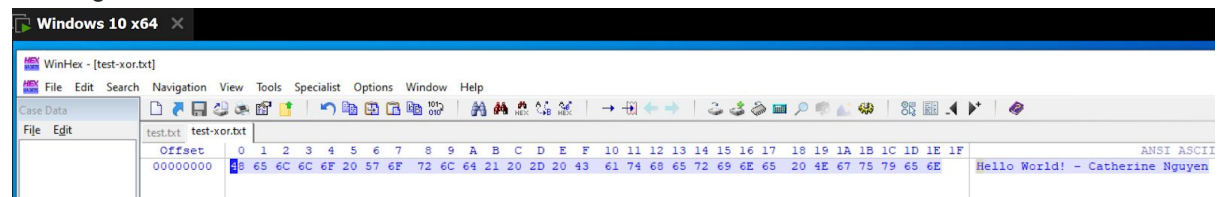


Figure 38: test-xor.txt after performing XOR.