CSU, College of Engineering and Computer Science
Department of Computer Science
CSC 153 – Computer Forensics Principles and Practice

Activity 7: Data Hiding and Steganography

Objectives:

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

Instructions: This lab is designed based on the textbook "Guide to Computer Forensics and Investigations" by Bill Nelson et al. We adopt the hands-on activities in this computer forensics class with full respect to the contributions and copyright of the original textbook authors.

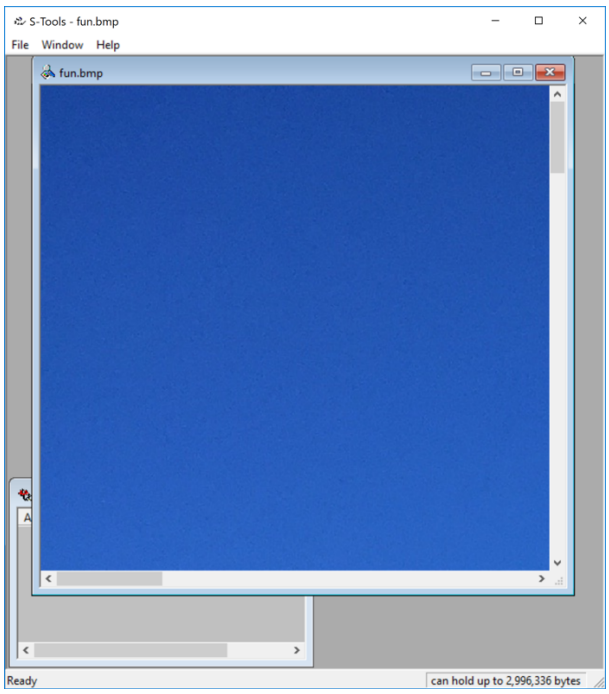
Part 1: Software installation.

Download the following software and install it on your workstation.

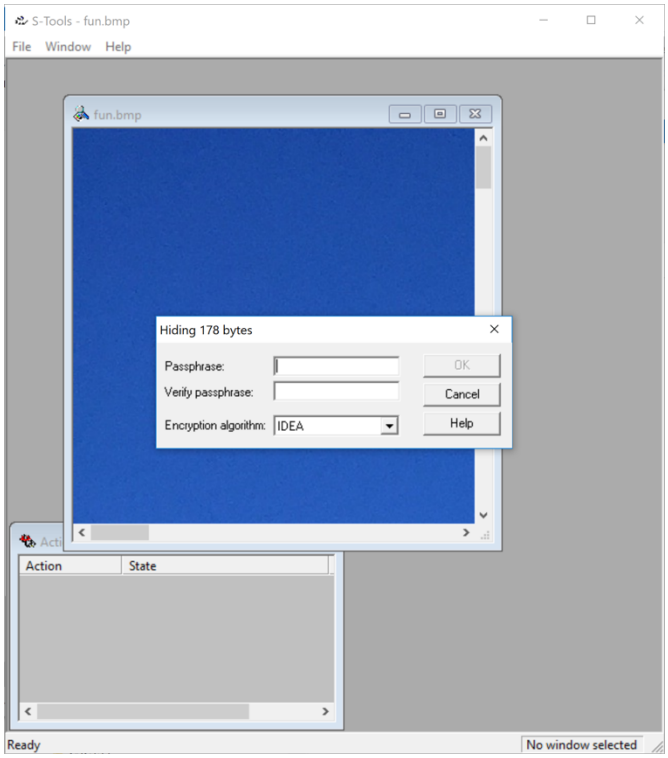
1. S-Tools4. https://packetstormsecurity.com/files/21688/s-tools4.zip.html

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

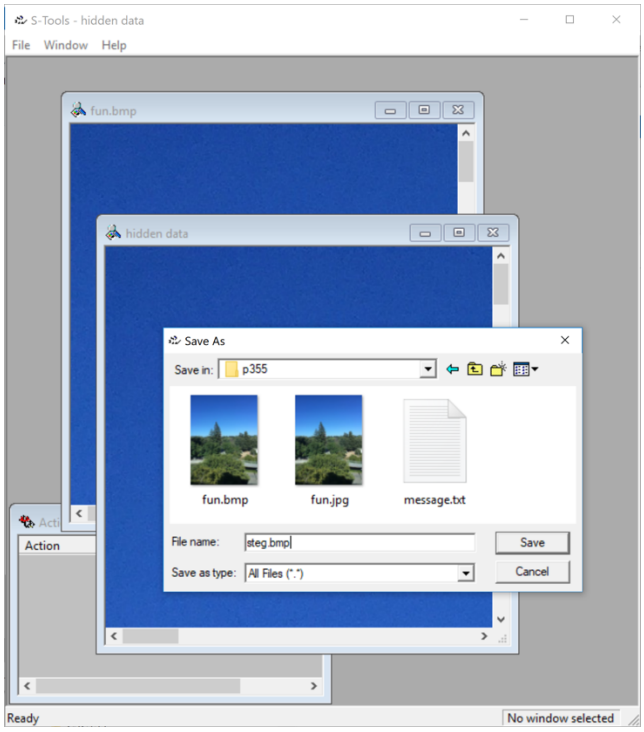
2. In File Explorer, navigate to the directory where you installed S-Tools4 and start the program S-Tools.exe.
3. Download fun.bmp from Canvas or google drive and save it in your work directory.
   The google drive link is: https://drive.google.com/file/d/1LL1pzZQ10Tz0RZUmL1js7Kp6Ux-n4LJ4/view?usp=sharing
4. Drag fun.bmp from your work folder to the S-Tools window.



5. Create a text file message.txt and type your secret message into the file.
6. Drag the message.txt from your work folder to the fun.bmp image.
7. In the Hiding dialog box, type “secret” in the Passphrase and Verify passphrase text boxes, and then click OK. You may also change encryption algorithm if you want.

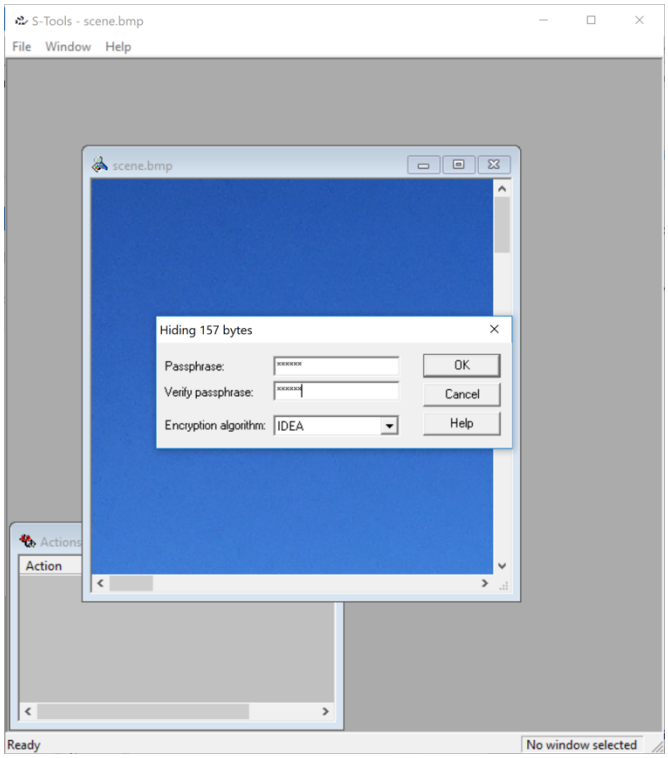


8. After the hidden data window opens, right click the window and click Save as. Save the image as fun-steg.bmp in your work folder.



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

9. In File Explorer, navigate to the directory where you installed S-Tools4 and start the program S-Tools.exe.
10. Download scene.bmp from Canvas or google drive and save it in your work directory.
    The google drive link is:
    https://drive.google.com/file/d/1hmIYsXdV2SvG2VJYyfQfPCaW14ZBgaGx/view?usp=sharing
11. Drag scene.bmp from your work folder to the S-Tools window.
12. Create a rtf file hidden.rtf and type your secret message into the file.
13. Drag the hidden.rtf from your work folder to the scene.bmp image.
14. In the Hiding dialog box, type “secret” in the Passphrase and Verify passphrase text boxes, and then click OK. You need to also change the encryption algorithm if you used another algorithm when creating the steganography file.



15. After the hidden data window opens, right click the window and click Save as. Save the image as scene-steg.bmp in your work folder.
16. In windows system, click on Search icon, type in cmd and hit enter to open the command prompt window.
17. Change your work folder to your working directory where scene.bmp and scene-steg.bmp are stored by using “cd” and “dir (similar to ls command in Linux)” commands.

```
C:\Users\sun\Documents>cd Course

C:\Users\sun\Documents\Course>dir
 Volume in drive C is Windows
 Volume Serial Number is 6AAF-EFD4

 Directory of C:\Users\sun\Documents\Course

10/23/2018  09:49 PM    <DIR>          .
10/23/2018  09:49 PM    <DIR>          ..
10/02/2018  12:02 PM    <DIR>          CSC134
11/03/2018  06:22 PM    <DIR>          CSC153
               0 File(s)              0 bytes
               4 Dir(s)  687,841,591,296 bytes free

C:\Users\sun\Documents\Course>
```

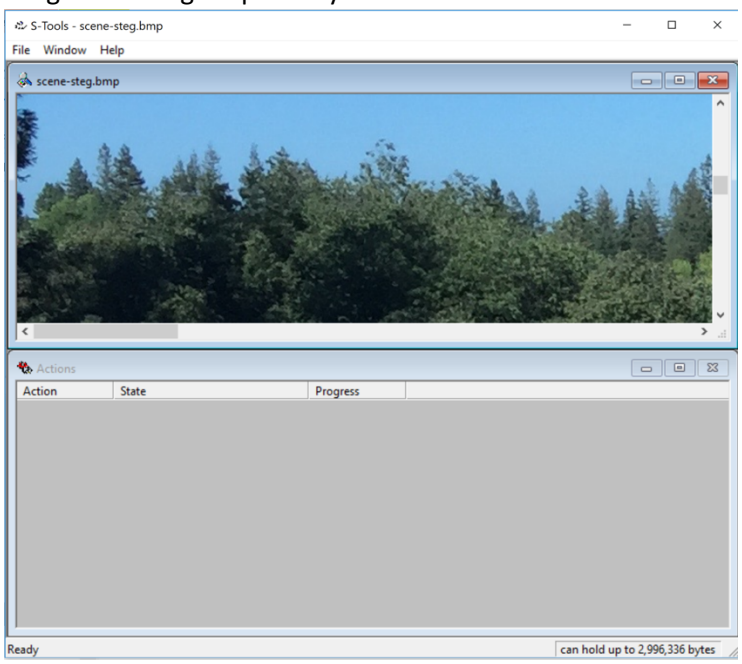
18. Type comp scene.bmp scene-steg.bmp > scene-compare.txt and press Enter. When the window prompts Compare more files (Y/N)?, type n and hit Enter. Exit the command prompt window by typing exit and pressing Enter.

```
C:\Users\sun\Documents\Course\CSC153\hands-on materials>cd p355

C:\Users\sun\Documents\Course\CSC153\hands-on materials\p355>dir
 Volume in drive C is Windows
 Volume Serial Number is 6AAF-EFD4

 Directory of C:\Users\sun\Documents\Course\CSC153\hands-on materials\p355

11/03/2018  06:47 PM    <DIR>          .
11/03/2018  06:47 PM    <DIR>          ..
11/03/2018  06:25 PM        23,970,870 fun.bmp
09/23/2017  08:54 PM         2,572,378 fun.jpg
11/03/2018  06:43 PM                66 hidden.rtf
11/03/2018  06:33 PM                95 message.txt
11/03/2018  06:47 PM        23,970,870 scene-steg.bmp
11/03/2018  06:45 PM        23,970,870 scene.bmp
09/23/2017  08:54 PM         2,945,167 scene.jpg
11/03/2018  06:39 PM        23,970,870 steg.bmp
               8 File(s)    101,401,186 bytes
               2 Dir(s)  687,839,440,896 bytes free

C:\Users\sun\Documents\Course\CSC153\hands-on materials\p355>comp scene.bmp scene-steg.bmp > scene-compare.txt
Compare more files (Y/N) ? N
```

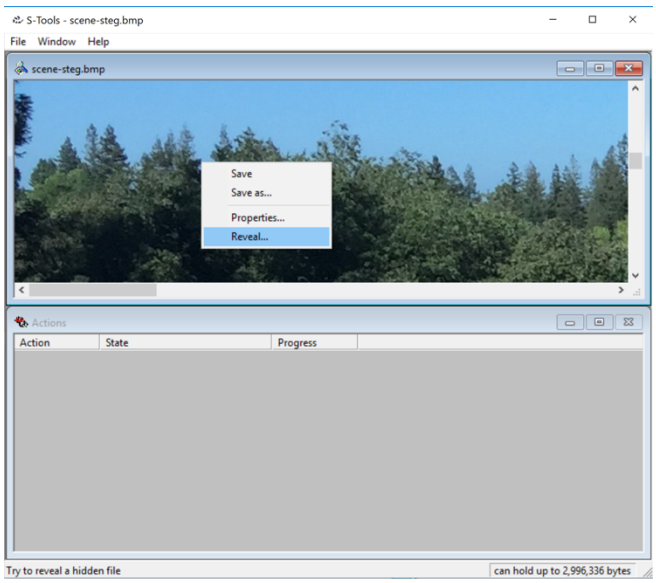
19. In File Explorer, navigate to your work folder and open the scene-compare.txt file to see the discrepancies between the two files.

Part 4: Extract the hidden messages/files.

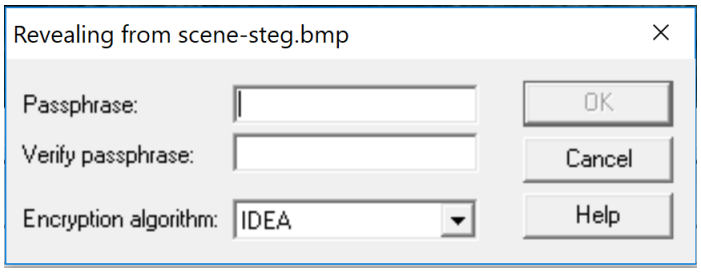
20. In File Explorer, navigate to the directory where you installed S-Tools4 and start the program S-Tools.exe.
21. Drag scene-steg.bmp from your work folder to the S-Tools window.



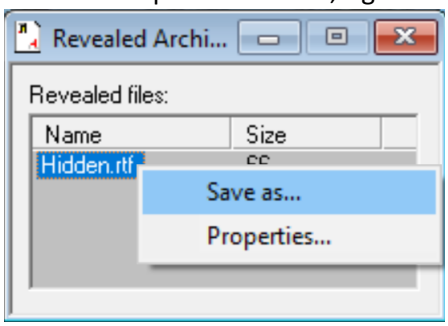
22. Right click on the picture and choose “Reveal…”.



23. Input the passphrase you used when creating the steganography file. The passphrase used is "secret" in this demo.



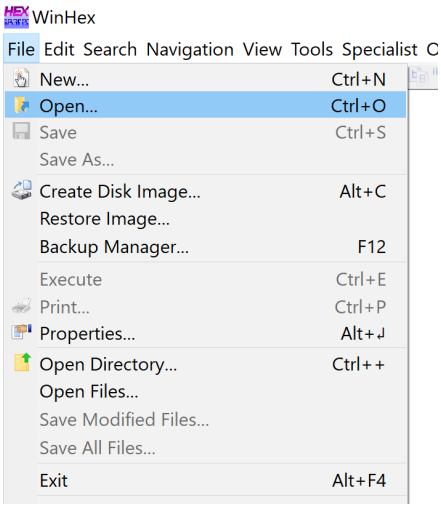
24. In the new opened window, right click the rtf file hidden.rtf and choose save as.



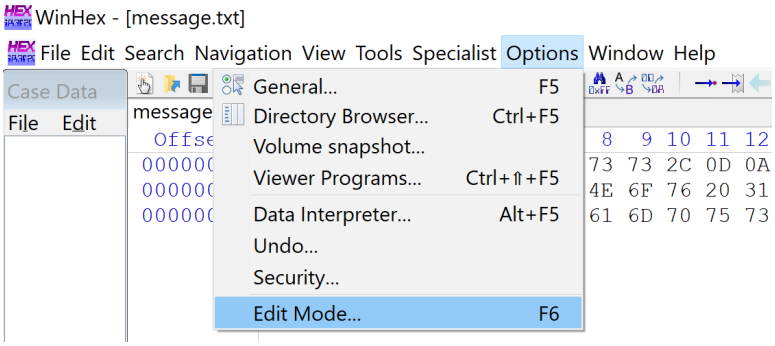
25. In your working directory, open the hidden.rtf file to view the content. Compare it with the hidden file you used in part 3 to see if they are the same.
26. Repeat Step 21-26 for file fun-steg.bmp to recover the hidden message.

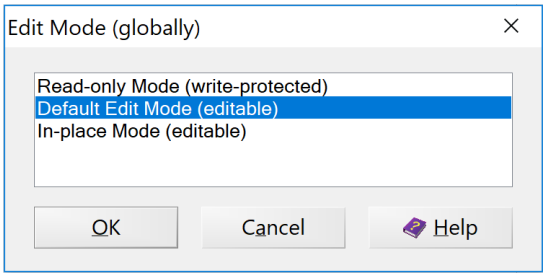
Part 5: Data hiding and recovering using Bit-shifting.

27. Create a text file named message.txt in Windows. Type a message in the file: "This is a secret message that I want to send out."
28. Start Winhex, click on File, Open. Navigate to your working directory, and double click message.txt in Winhex.

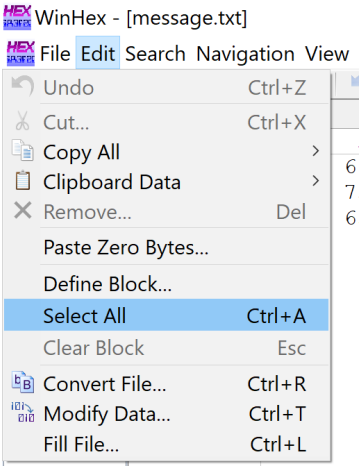


29. Click on Options->Edit Mode from the menu. Click on the Default Edit Mode (=editable), and then click OK.

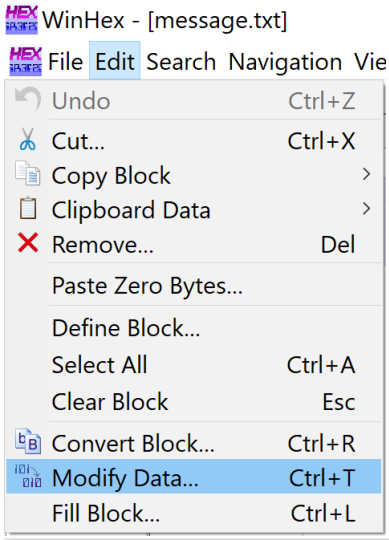


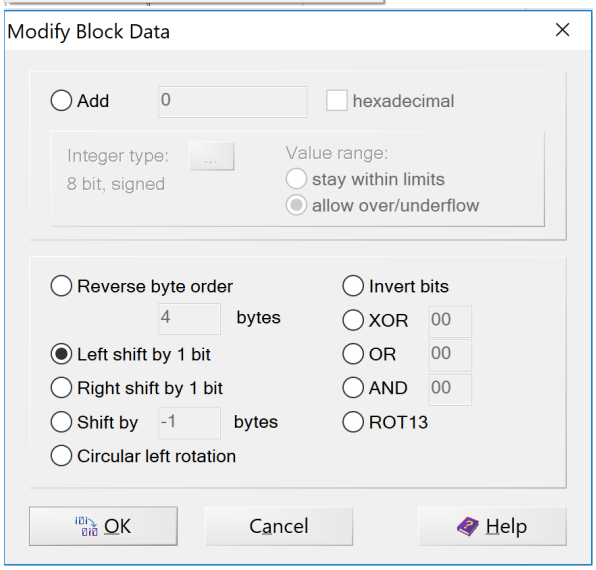


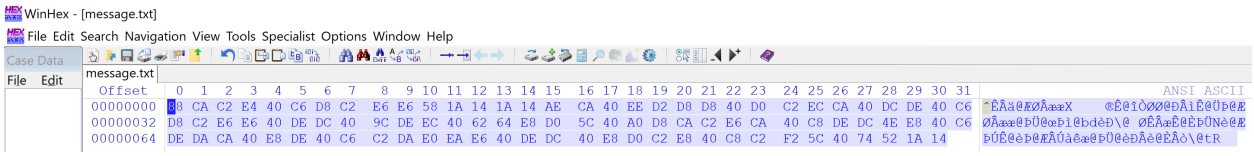
30. Select all the data in the file by pressing Ctrl+A, or clicking Edit->Select All from the menu.



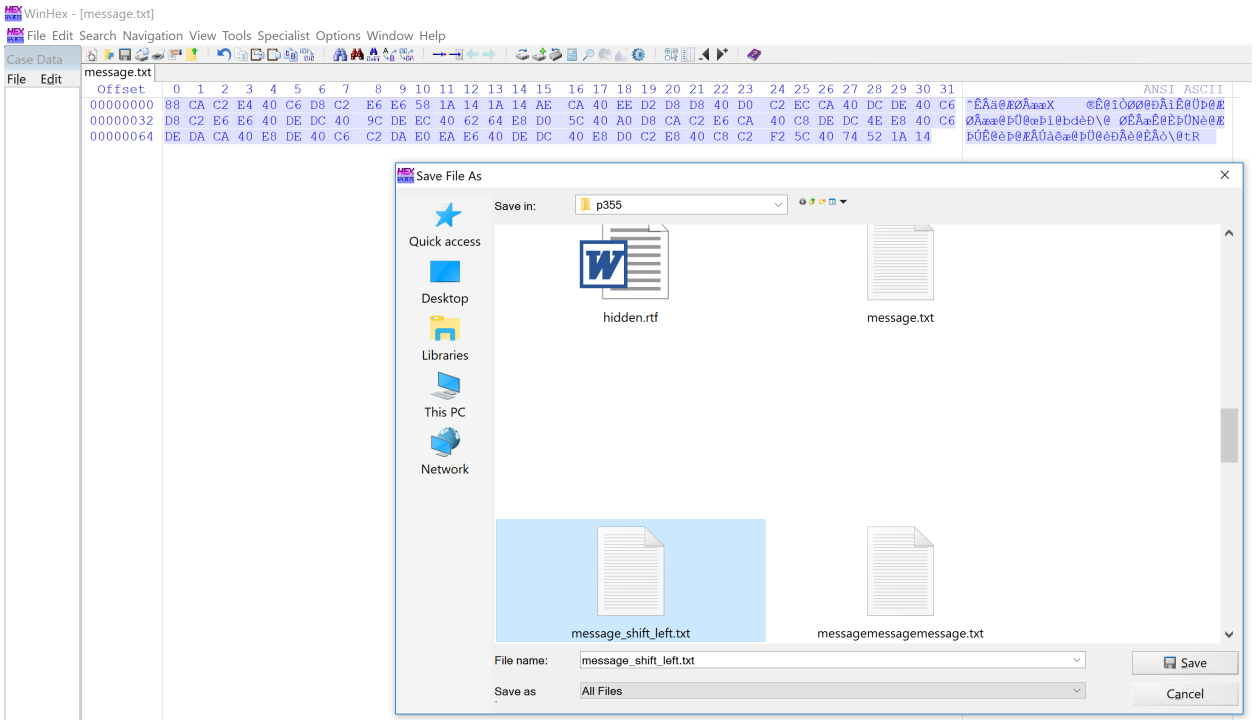
31. Click Edit, Modify Data from the menu. In the Modify Block Data dialog box, click the Left shift by 1 bit option, and then click OK.



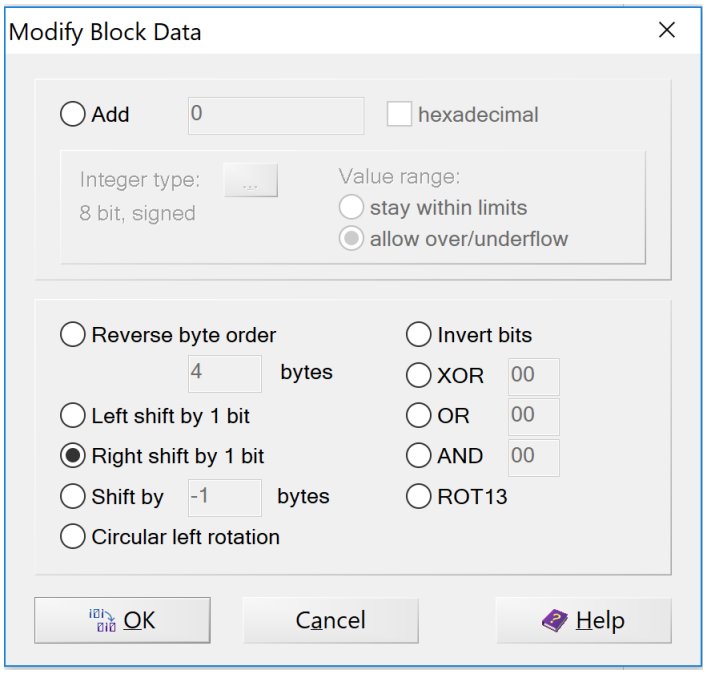




32. Click File->Save As from the menu, and save the file as message-shift-left.txt in your work folder. The text is now changed to random values.



33. To recover the message from message-shift-left.txt, you need to bit-shift it back to the right. Make sure the data is selected before you click the Edit->Modify Data from the menu. In the dialog box, click Right shift by 1 bit, and then click OK.

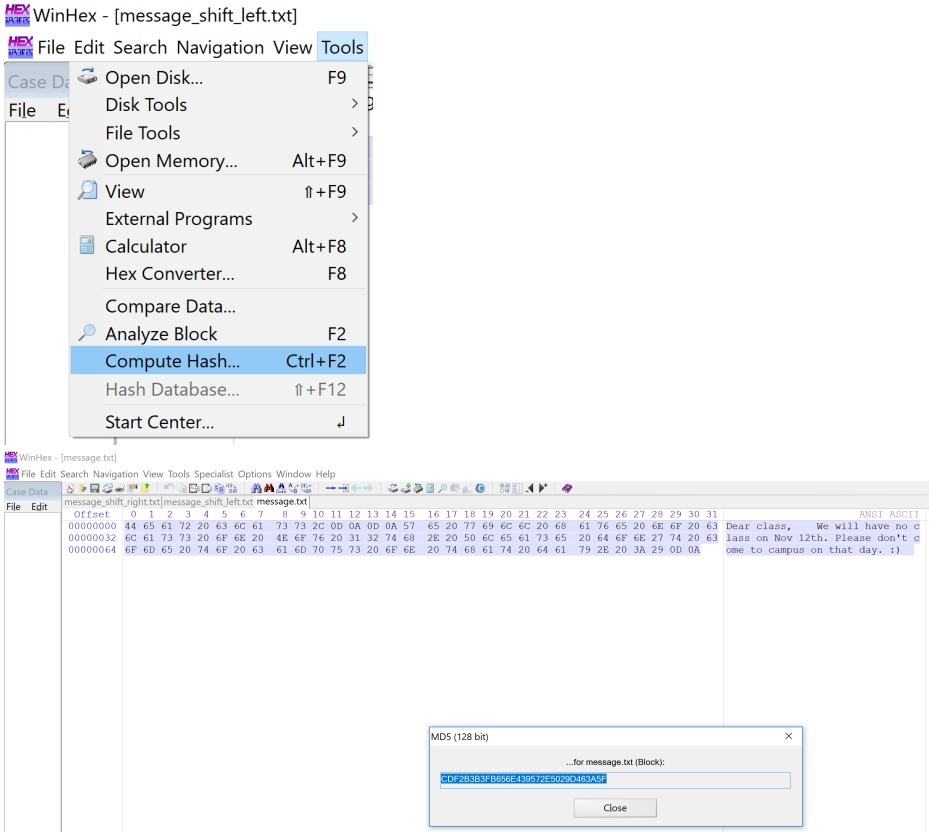


34. Save the file as message-shift-right.txt in your work folder.

Now you can use Winhex to compare the MD5 hash values of these three files and determine if message.txt is different from message-shift-left.txt and message-shift-right.txt.

35. Open message.txt, message-shift-right.txt, and message-shift-left.txt in Winhex by clicking File->Open repeatedly.

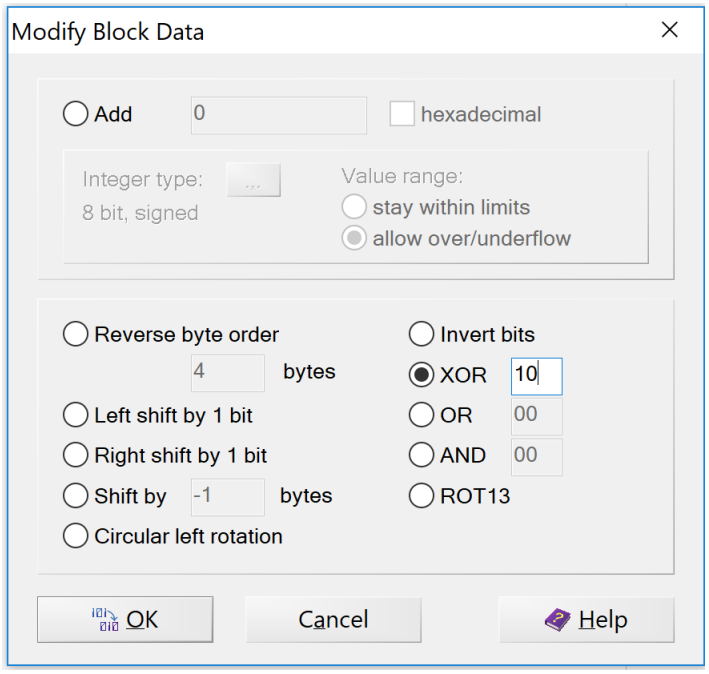
36. Click the message.txt tab in winhex to make it the active file, select the content by clicking Edit->Select All from the menu.
37. Click on Tools->Compute Hash from the menu to open the Compute hash dialog box. In the list box, click MD5 and then OK. Copy the MD5 hash value to a new text document.



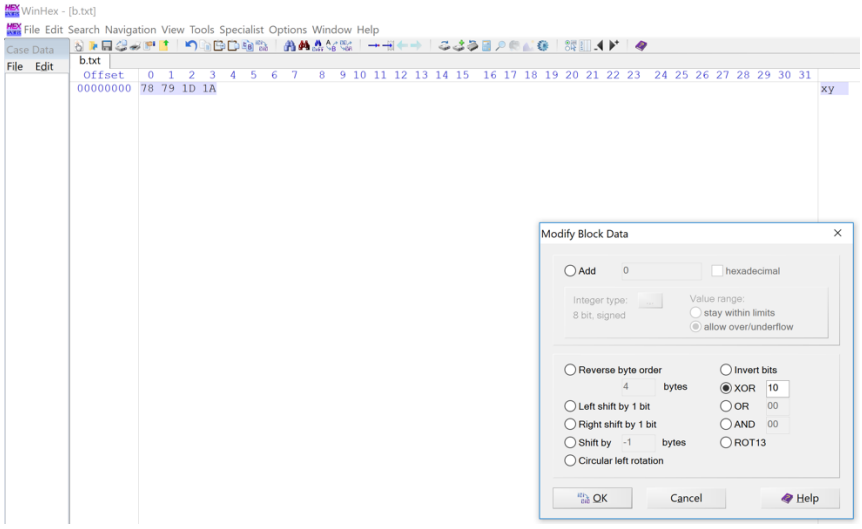
38. Repeat the step 36-37 to compute the hash values for message-shift-left.txt and message-shift-right.txt. Copy the hash values to the new text document.
39. Compute the MD5 hash values to determine if the files are different.

Part 6: Data hiding and recovering using XOR.

40. Create a new text file named test.txt, and then type in a short message in the file, such as your name (e.g., Xiaoyan Sun).
41. Start Winhex, click on File, Open. Navigate to your working directory, and double click test.txt in Winhex.
42. Select all the data in the file by pressing Ctrl+A, or clicking Edit->Select All from the menu.
43. Click Edit, Modify Data from the menu. In the Modify Block Data dialog box, click the XOR option. Type in two binary bits such as 10 in the box, and then click OK.



44. Click File->Save As from the menu, and save the file as test-xor.txt in your work folder. The text is now changed to random values.
45. Next, perform the XOR towards test-xor.txt to recover the message. Open test-xor.txt in Winhex, and repeat step 42-43. The message will be recovered.



Questions:

1. To reveal the hidden data using S-Tools, which information are required?
2. In Part 3, Are there any differences between scene.bmp and scene-steg.bmp? Please take a screenshot to show the differences.
3. In Part 3, Are there any differences between fun.bmp and fun-steg.bmp? Please take a screenshot to show the differences.
4. In Part 5, among the hash values for message.txt, message-shift-right.txt, and message-shift-left.txt, which ones are the same? Please take a screenshot to prove your answer.

5. In class, we've discussed that INFORMATION XOR RANDOM_NUMBER = NONSENSE. What will be generated if we do NONSENSE XOR RANDOM_NUMBER?

Deliverable:

1. You need to submit a lab report to Canvas. Your lab report should ***explicitly*** **answer all questions one by one**. When necessary, you need to have screenshots to prove your answer. Include necessary narrative and analysis to make your report clear. The report will be evaluated based on the correctness, completeness, clarity and quality of English writing.