James Gouveia

Professor Sun

CSC 153

University of California Sacramento

Activity 7

Questions:

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

   To reveal the data, we need access to the file containing the secret message as well as the password/offset/XOR value to decrypt the hidden information.

2. In part 3, Are there any differences between scene.bmp and scene-steg.bmp? Please take a screenshot to show the differences.

   Yes, there are 10 differences in the files, indicating there is hidden data inside the bmp carrier.

```
Comparing fun.bmp and scene-steg.bmp...
Compare error at OFFSET 552
file1 = 16
file2 = 17
Compare error at OFFSET 9F6
file1 = E
file2 = F
Compare error at OFFSET 130C
file1 = C
file2 = D
Compare error at OFFSET 13A6
file1 = 8
file2 = 9
Compare error at OFFSET 185C
file1 = 9
file2 = 8
Compare error at OFFSET 1947
file1 = 1A
file2 = 1B
Compare error at OFFSET 1B9D
file1 = 1D
file2 = 1C
Compare error at OFFSET 2280
file1 = 10
file2 = 11
Compare error at OFFSET 2454
file1 = B
file2 = A
Compare error at OFFSET 2463
file1 = E
file2 = F
10 mismatches - ending compare
```

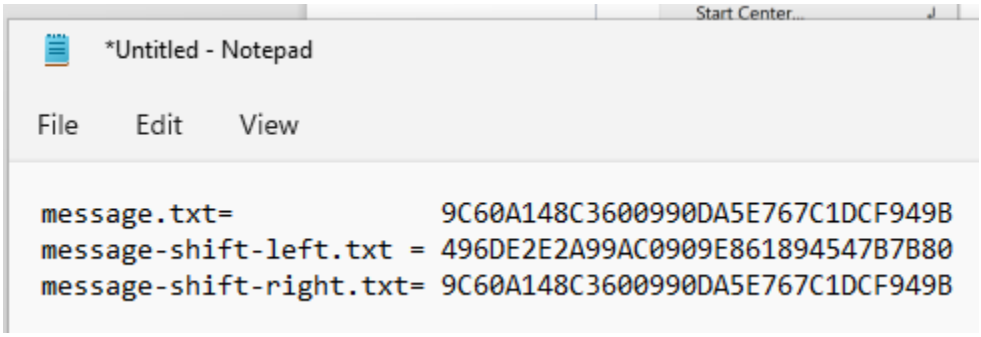
3. In Part 3, Are there any differences between fun.bmp and fun-steg.bmp? Please take a screenshot to show the differences.
   There are 10

   Yes, there are 10 differences in the files, indicating there is hidden data inside the bmp carrier.

```
Comparing fun.bmp and fun-steg.bmp...
Compare error at OFFSET 8478
file1 = F
file2 = E
Compare error at OFFSET CA65
file1 = 13
file2 = 12
Compare error at OFFSET 1CFD7
file1 = 17
file2 = 16
Compare error at OFFSET 272EC
file1 = 19
file2 = 18
Compare error at OFFSET 2D607
file1 = 27
file2 = 26
Compare error at OFFSET 2DAEF
file1 = 14
file2 = 15
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 427F2
file1 = 11
file2 = 10
10 mismatches - ending compare
```

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.

   The message.txt and message-shift-right.txt are the same, this is to be expected as the shift left by 1 was undone by the shift right by 1 operation. The message-shift-left.txt has a different hash, this is correct as the contents of this file are different.



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

   Since the two operations are opposite, it will return the data to its original state.