Recognizing the Use of Steganography in Image Files

Learning Objective

Steganography is the practice of hiding private or sensitive information within something that appears to be nothing out of the usual. The word steganography comes from ancient Greece (stagnos), where hiding hidden messages within seemingly harmless messages became an art form.

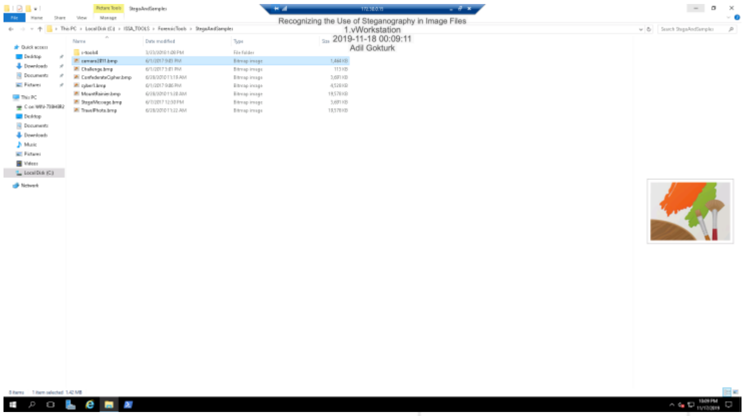
Tools and Software

- S-Tools
- Windows Paint

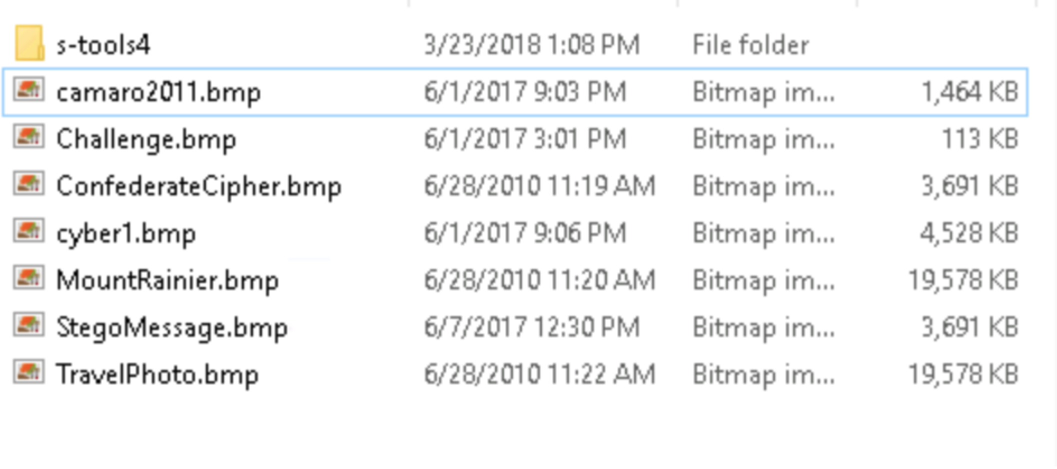
Lab Deliverables

❖ Part 1: Review Image Files Using Microsoft Paint

- **Step#7 file names and file sizes**

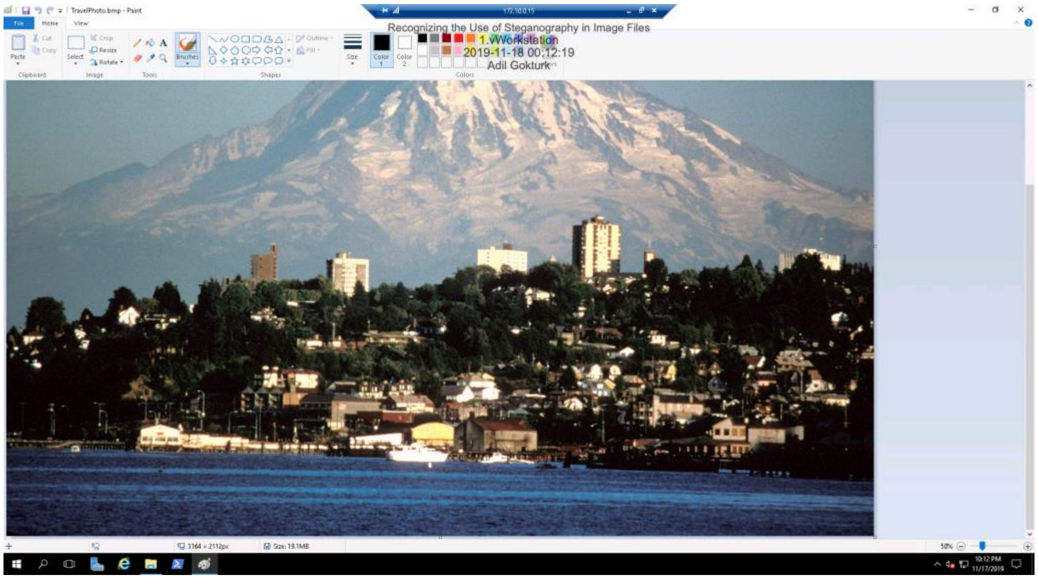


Recognizing the Use of Steganography in Image Files
1.vWorkstation
2019-11-18 00:09:11
Adil Gokturk

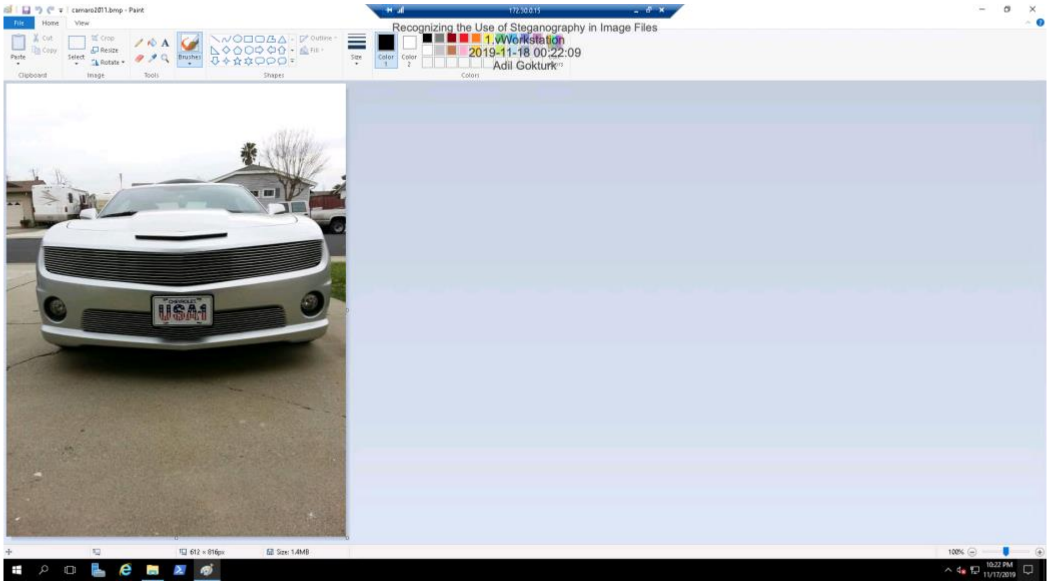


s-tools4	3/23/2018 1:08 PM	File folder	
camaro2011.bmp	6/1/2017 9:03 PM	Bitmap im...	1,464 KB
Challenge.bmp	6/1/2017 3:01 PM	Bitmap im...	113 KB
ConfederateCipher.bmp	6/28/2010 11:19 AM	Bitmap im...	3,691 KB
cyber1.bmp	6/1/2017 9:06 PM	Bitmap im...	4,528 KB
MountRainier.bmp	6/28/2010 11:20 AM	Bitmap im...	19,578 KB
StegoMessage.bmp	6/7/2017 12:30 PM	Bitmap im...	3,691 KB
TravelPhoto.bmp	6/28/2010 11:22 AM	Bitmap im...	19,578 KB

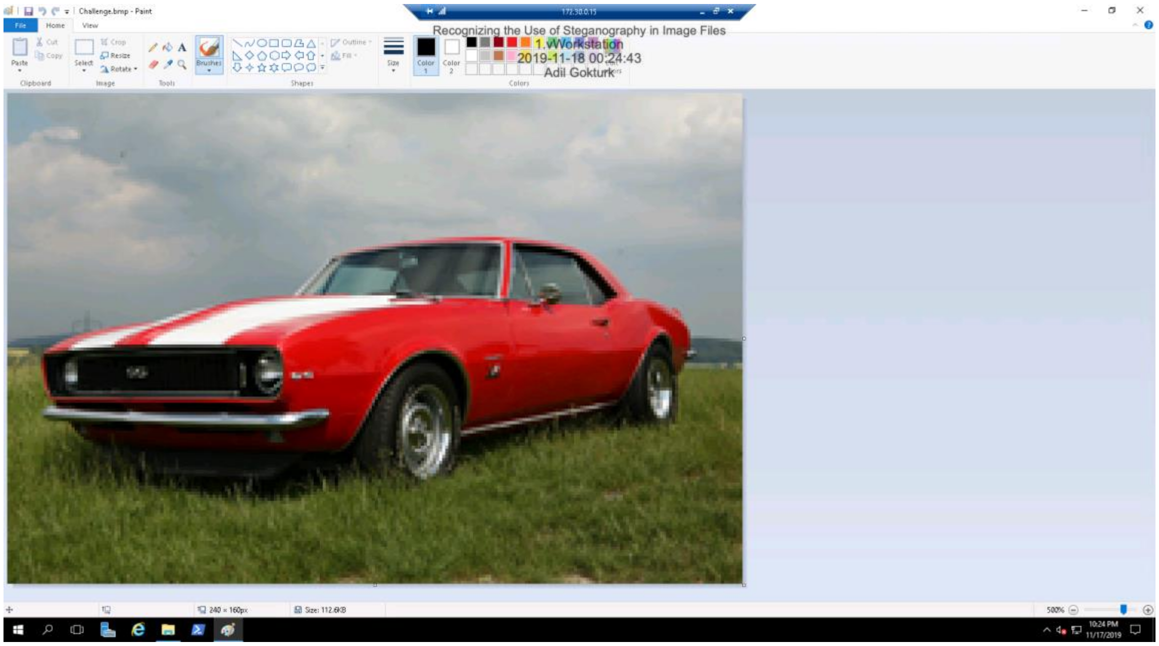
- **Step#10**
  - TravelPhoto.bmp
    - Apparently, it is a port city which located in front of a mountain. City seems like embedded to the mountain or vice-a versa.



  - Camaro2011.bmp
    - It looks like a highly modified metallic gray 2011 Chevrolet Camaro. Its plate number is USA-1



- Challenge.bmp
    - It is a red color Dodge Challenger with a white strap

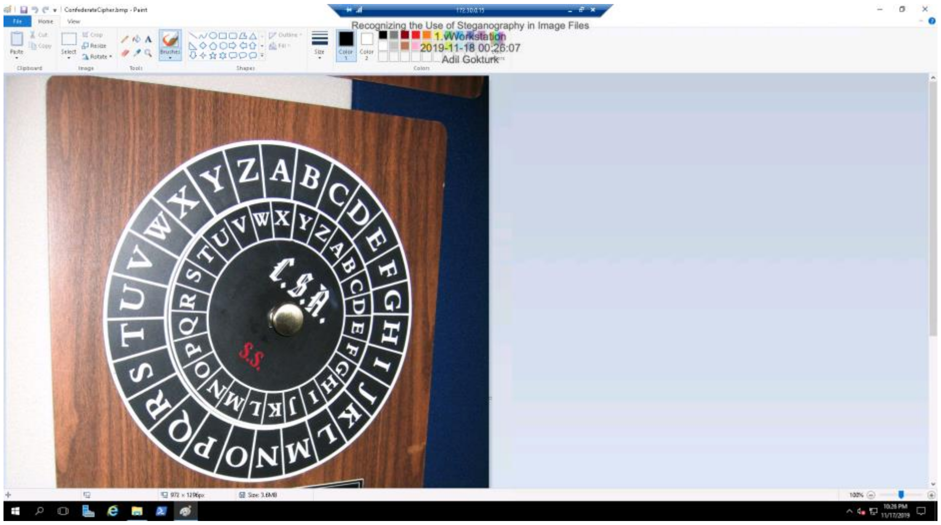


Challenge.bmp - Paint

Recognizing the Use of Steganography in Image Files
1.vWorkstation
2019-11-18 00:24:43
Adil Gokturk

240 × 160px Size: 112.6KB

- ConfederateCipher.bmp
    - It is a cipher to decode C.S.A. S.S.



ConfederateCipher.bmp - Paint

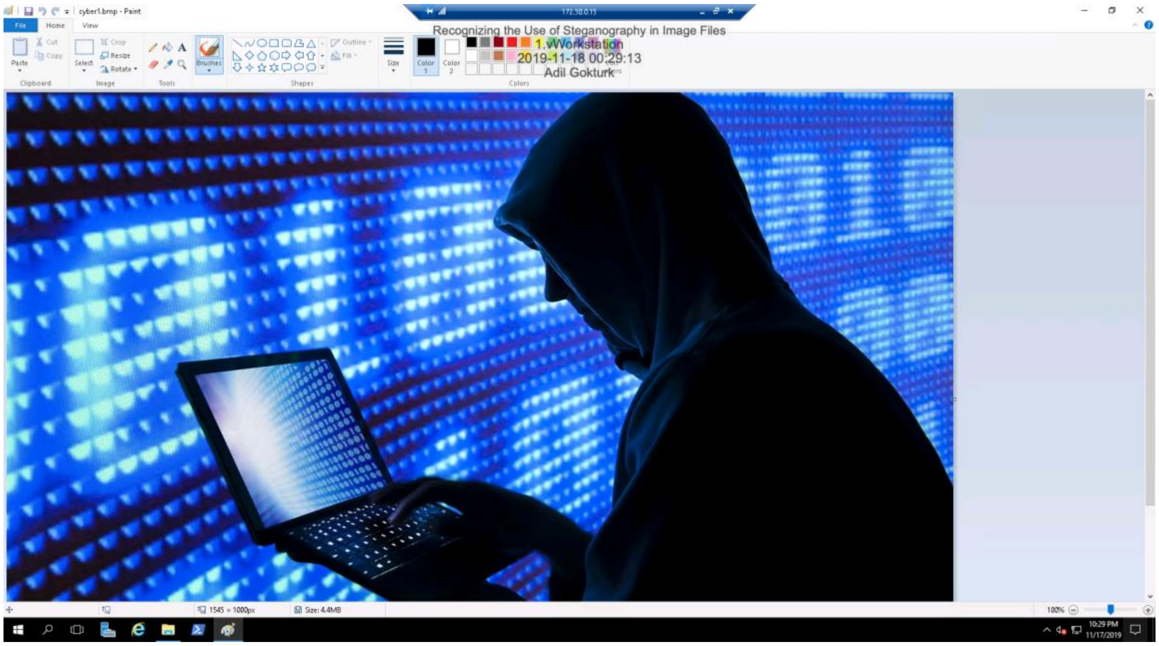
Recognizing the Use of Steganography in Image Files
1.vWorkstation
2019-11-18 00:26:07
Adil Gokturk

972 × 1296px Size: 3.6MB

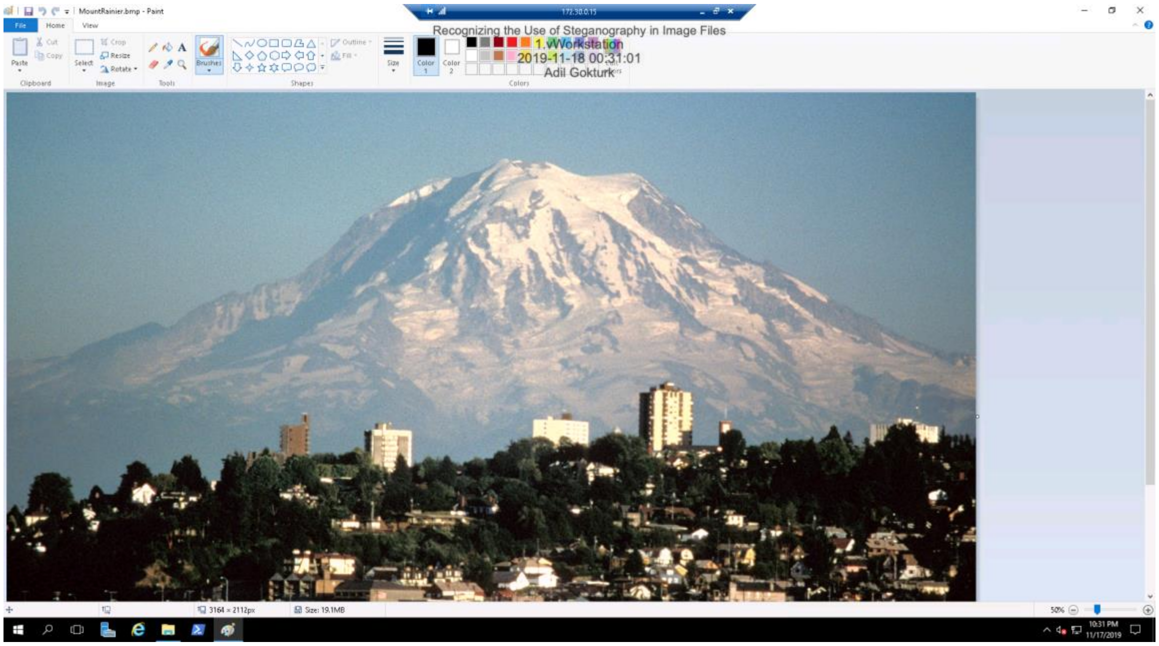
DPOE OE

JVUK

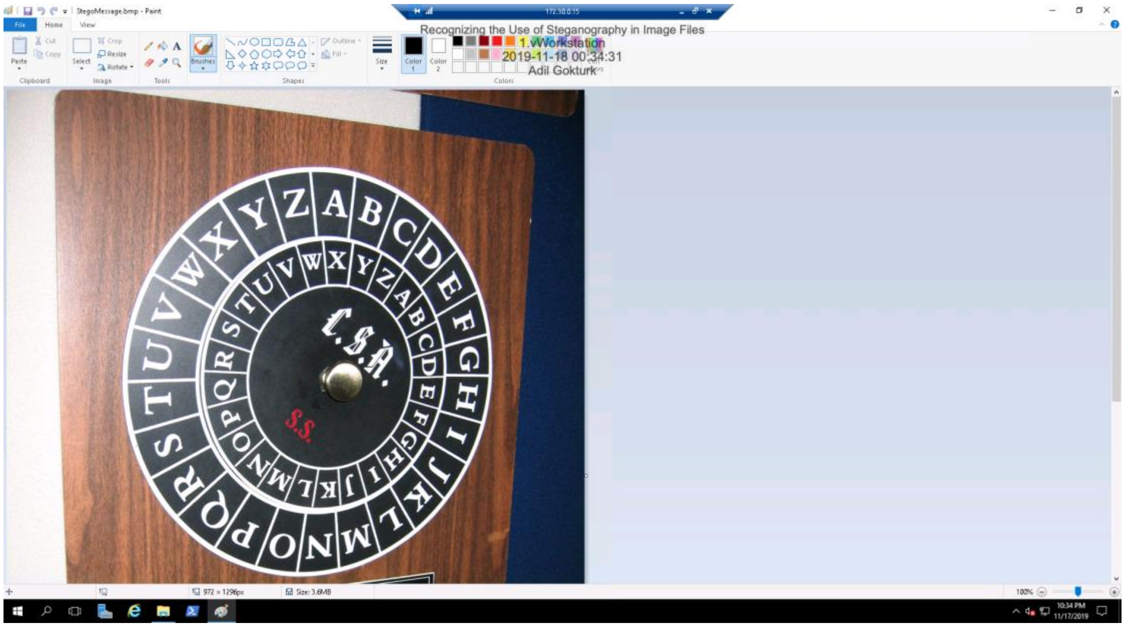
- Cyber1.bmp
  - He/she looks like a hacker.



- MountRainier.bmp
  - Mount Rainier

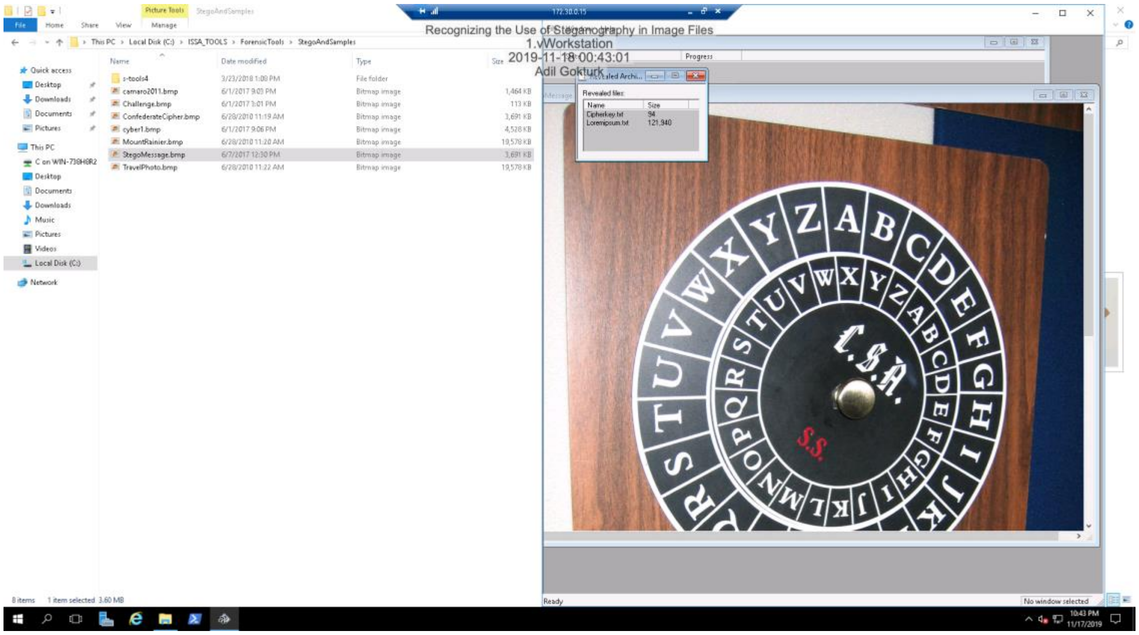


- StegoMessage.bmp
    - It is a cipher to decode C.S.A. S.S.


Recognizing the Use of Steganography in Image Files
1.vWorkstation
2019-11-18 00:34:31
Adil Gokturk

❖ Part 2: Use S-Tools to Reveal Steganography

- **Step#7**

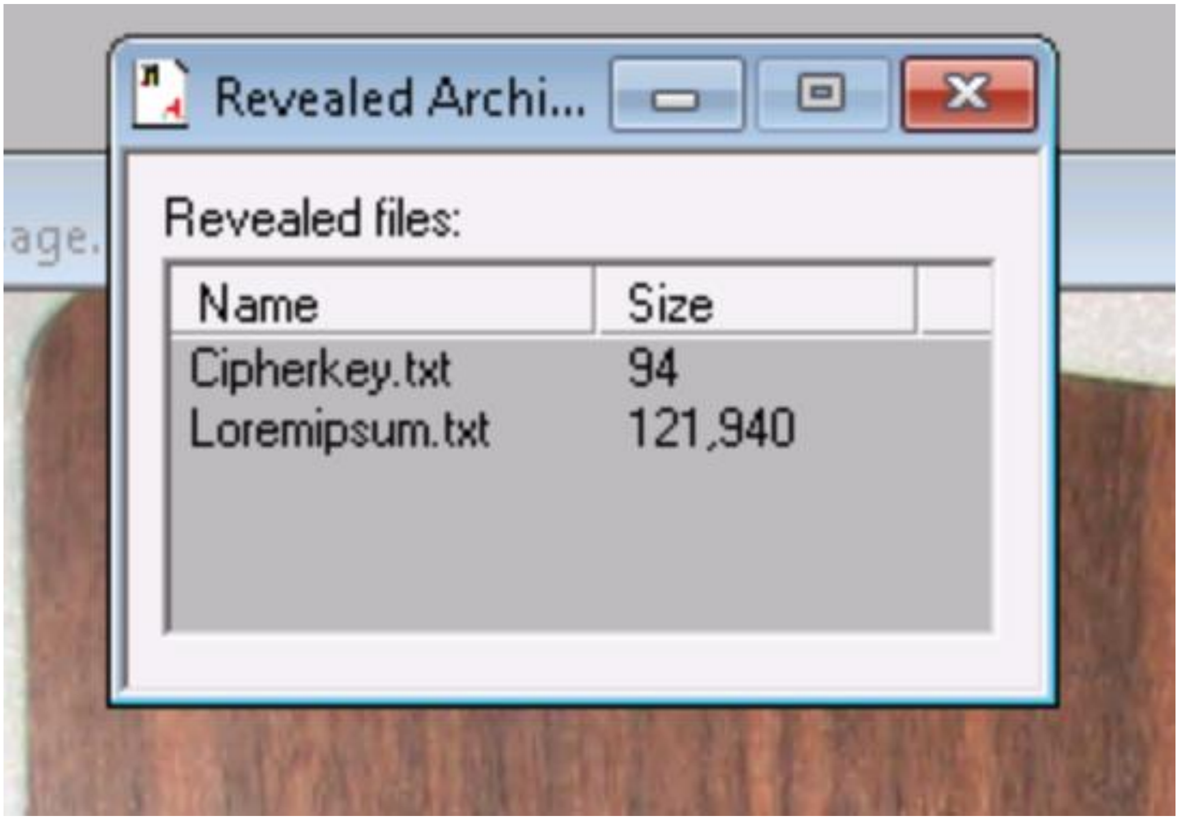

Recognizing the Use of Steganography in Image Files
1.vWorkstation
2019-11-18 00:43:01
Adil Gokturk

This PC › Local Disk (C:) › ISSA_TOOLS › ForensicTools › StegoAndSamples

Name	Date modified	Type	Size
s-tools4	3/23/2018 1:08 PM	File folder	
camaro2011.bmp	6/1/2017 9:03 PM	Bitmap image	1,464 KB
Challenge.bmp	6/1/2017 3:01 PM	Bitmap image	113 KB
ConfederateCipher.bmp	6/28/2010 11:19 AM	Bitmap image	3,691 KB
cyber1.bmp	6/1/2017 9:06 PM	Bitmap image	4,528 KB
MountRainier.bmp	6/28/2010 11:20 AM	Bitmap image	19,578 KB
StegoMessage.bmp	6/7/2017 12:30 PM	Bitmap image	3,691 KB
TravelPhoto.bmp	6/28/2010 11:22 AM	Bitmap image	19,578 KB

Revealed files:

Name	Size
Cipherkey.txt	94
Loremipsum.txt	121,940



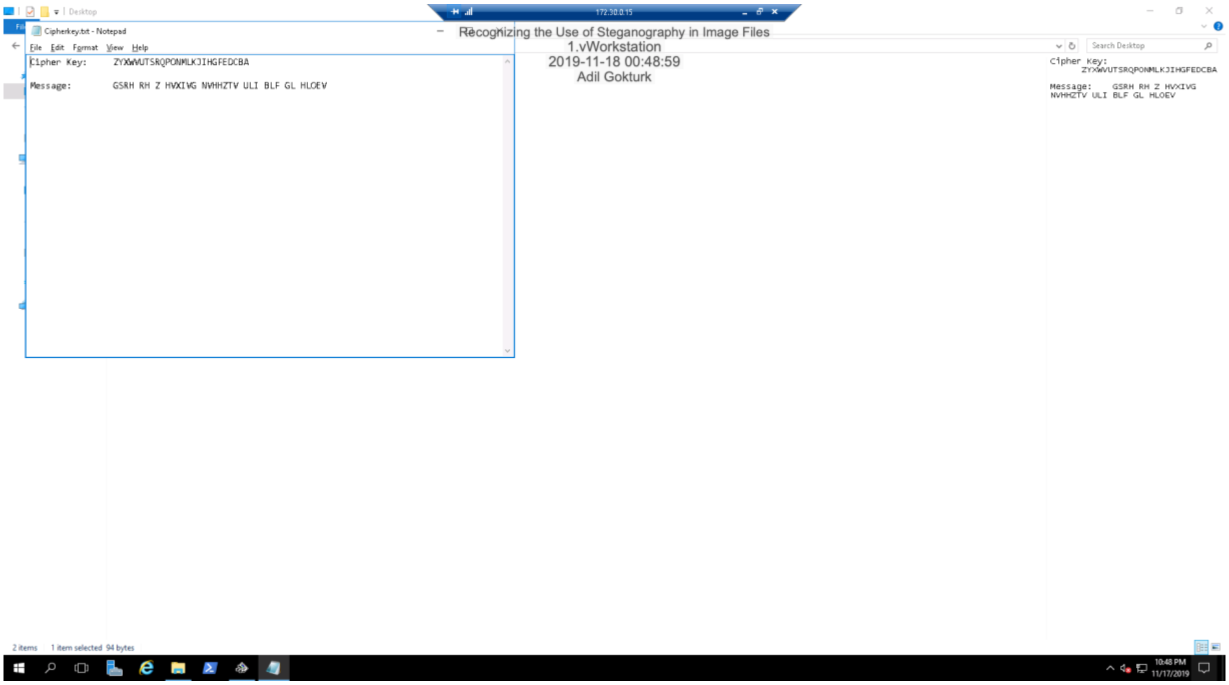
Revealed files:

Name	Size
Cipherkey.txt	94
Loremipsum.txt	121,940

- **Step#8 In your Lab Report file, briefly explain the encryption algorithm used to reveal the hidden files (i.e., IDEA) in 100 words. You may need to explore the Internet and other resources for self-study.**
  - Apparently, the encryption algorithm is the alphabet written from the last letter through to first letter. It seems pretty simple but it is not.
  - The **International Data Encryption Algorithm—IDEA**, initially called Improved Proposed Encryption Standard—IPES, is a symmetric-key block cipher designed by James Massey of ETH Zurich and Xuejia Lai and was first defined in 1991[1]. The IDEA uses a block cipher with a 128-bit key, which is fairly considered to be secure. It is also one of the most publicly known algorithms and its non-commercial use is free.

[1] https://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm

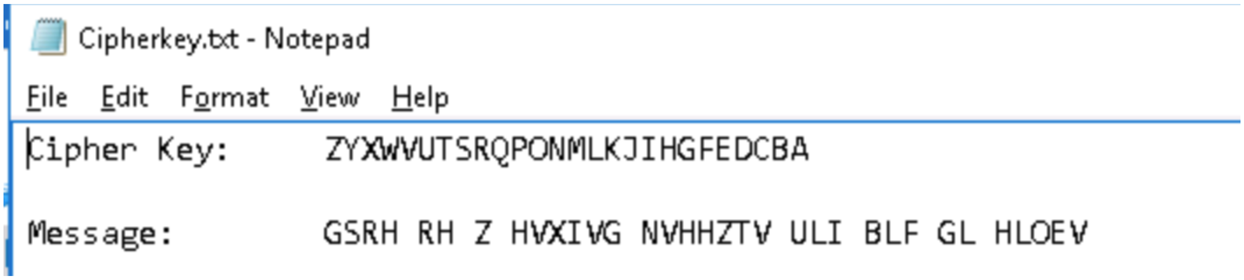
- **Step#13**



Recognizing the Use of Steganography in Image Files
1.vWorkstation
2019-11-18 00:48:59
Adil Gokturk

```
Cipher Key:     ZYXWVUTSRQPONMLKJIHGFEDCBA

Message:        GSRH RH Z HVXIVG NVHHZTV ULI BLF GL HLOEV
```

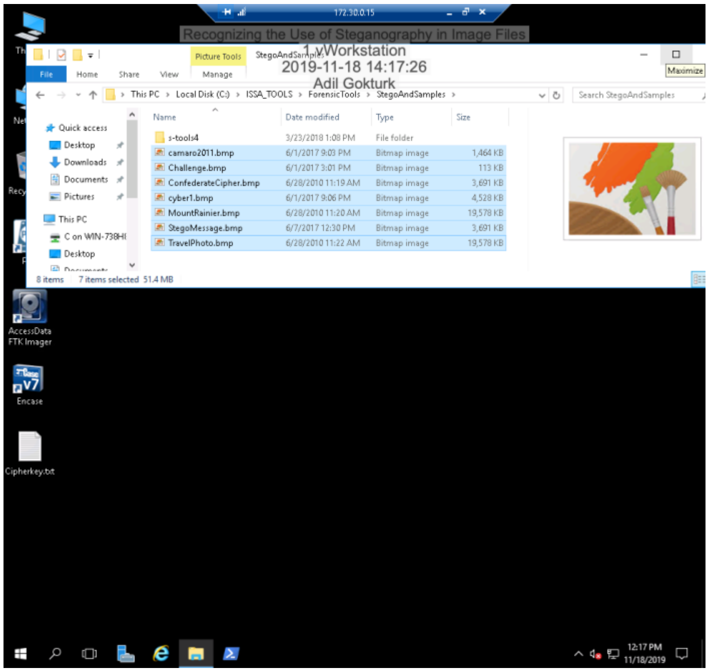


```
Cipher Key:     ZYXWVUTSRQPONMLKJIHGFEDCBA

Message:        GSRH RH Z HVXIVG NVHHZTV ULI BLF GL HLOEV
```

- **Step#14: Decipher the hidden message**
  - Apparently, the encryption algorithm is the alphabet written from the last letter through to first letter. It seems pretty simple but it is not.
  - Z Y X W V U T S R Q P O N M L K J I H G F E D C B A - Alphabet
  - A B C D E F G H I J K L M N O P Q R S T U V W X Y Z – Cipher key
- Deciphered hidden message is **THIS IS A SECRET FOR YOU TO SOLVE**

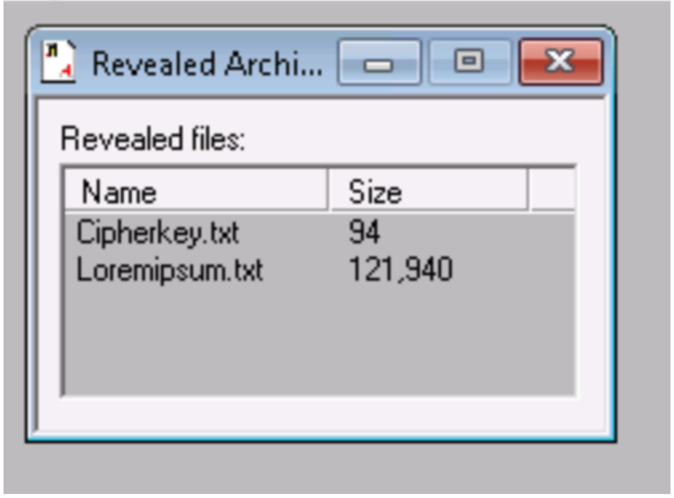
- Step#16: Document the total file size of the revealed payload files
    - Both size of the StegoMessage.bmp is 3,691KB, however the one we use IDEA has hidden files.



Name	Date modified	Type	Size
s-tools4	3/23/2018 1:08 PM	File folder	
camaro2011.bmp	6/1/2017 9:03 PM	Bitmap image	1,464 KB
Challenge.bmp	6/1/2017 3:01 PM	Bitmap image	113 KB
ConfederateCipher.bmp	6/28/2010 11:19 AM	Bitmap image	3,691 KB
cyber1.bmp	6/1/2017 9:06 PM	Bitmap image	4,528 KB
MountRainier.bmp	6/28/2010 11:20 AM	Bitmap image	19,578 KB
StegoMessage.bmp	6/7/2017 12:30 PM	Bitmap image	3,691 KB
TravelPhoto.bmp	6/28/2010 11:22 AM	Bitmap image	19,578 KB

8 items 7 items selected 51.4 MB

- **Step#17**



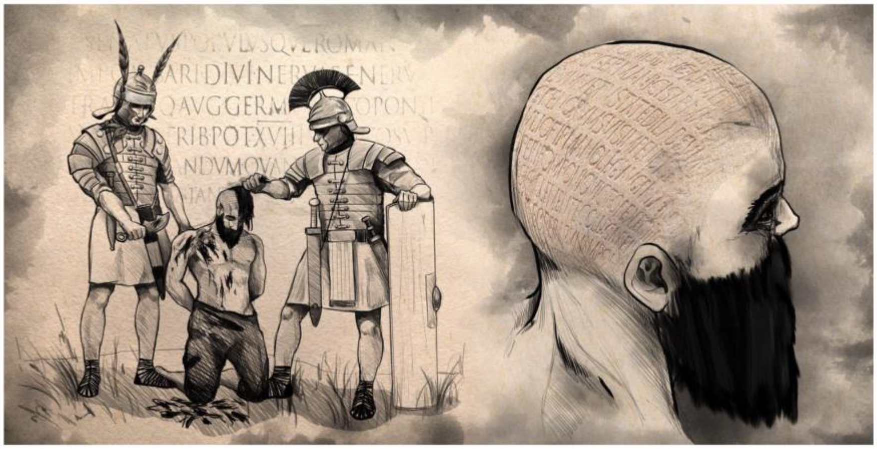
Revealed files:

Name	Size
Cipherkey.txt	94
Loremipsum.txt	121,940

- The file size of the source image is StegoMessage.bmp is 3,691KB vs the revealed archive file size 3,691KB, which is same however, the one we used IDEA has two hidden files
    - cipherkey.txt 94KB
    - Loremipsum.txt 12,940KB.

❖ Part 2: Challenge Questions

- Discuss at least three example cases when (by whom) Steganography can be effectively used (100 words for each case).
    - As I mentioned , steganography is the practice of sending data in a concealed format so the very fact of sending the data is camouflaged. The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal[2].
        1. The concept of Steganography first used by Roman Empire to deliver secret messages to their counterparts in 14th century. According to Alexey Shulmin and Evgeniya Krylova, "a slave chosen to convey a secret message had his scalp shaved clean and a message was tattooed onto the skin. When the messenger's hair grew back, he was dispatched on his mission. The receiver shaved the messenger's scalp again and read the message[3]", as shown below .



        2. As we have experienced our bonus lab, the concept of Steganography also be useful for the cyber attackers to hide their malware in a visual file. When we take a good look at the two-- StegoMessage.bmp images, we can't see any difference. They are identical in both size and appearance. However, one of them is a carrier containing an embedded message. Shulmin and Krylova argue that there are three reason for that[4]:
            a. It helps them conceal not just the data itself but the fact that data is being uploaded and downloaded
            b. Anti-malware tools generally, and perimeter security tools specifically, can do very little with payload-filled carriers.

[2] https://en.wikipedia.org/wiki/Steganography
[3] https://securelist.com/steganography-in-contemporary-cyberattacks/79276/
[4] https://jbl-lti.hatsize.com/labview/?e=729255

Such carriers are very difficult to detect, as they look like regular image files (or other types of files)

c. Use of steganography may help bypass security checks by anti-APT products, as the latter cannot process all image files

   i. Corporate networks contain too many of them, and the analysis algorithms are rather expensive.

3. In communities with social or government taboos or censorship, people use cultural steganography—hiding messages in idiom, pop culture references, and other messages they share publicly and assume are monitored. This relies on social context to make the underlying messages visible only to certain readers[5]. Examples include:

   a. Hiding a message in the title and context of a shared video or image.
   b. Misspelling names or words that are popular in the media in a given week, to suggest an alternate meaning.
   c. Hiding a picture which can be traced by using Paint or any other drawing tool.

[5] http://boingboing.net/2013/05/22/social-steganography-how-teen.html