What is Steganography?

Steganography is the art and science of communicating in a way which hides the existence of the communication.

The goal of Steganography is to hide data or messages inside other files in a way that does not allow an enemy to even detect that there is a secret data present.
What is Steganography?

Carrier of Data

- Text
- Image
- Video
- Audio
- Network protocols

Steganography vs Cryptography

Steganography and Cryptography are closely related

The difference is:

- **Cryptography**: although encrypted and unreadable, the existence of data is not hidden
- **Steganography**: no knowledge of the existence of the data

Steganography and Cryptography can be used together to produce better protection
How does it work?

- Goal: send a secret message embedded in an image
- Sender modifies the image to incorporate the secret message
- Modified image should look like the original one
- Message recipient decodes message from the modified image

Uses of Steganography

**Economic espionage**
- used to exfiltrate information from a major European automaker

**Political extremists**
- used for secure communications

**Terrorism**
- used to hide terrorist communications over the Internet, e.g., Osama bin Laden’s alleged use of steganography

**Fraud**
- used to compromise sensitive data (SSN, credit cards) by hiding malware in media files
- used to compromise data a “digital dead drop” to hide stolen card numbers on a hacked Web page
Steganographic Cyberattacks

On December 2016, Sundown Exploit Kit started to use steganography to hide their exploit code. It is used by multiple malvertising campaigns to distribute malware.

- Japan 33.41%
- Canada 10.12%
- France 8.77%
- United States 5.18%
- Spain 4.45%
- Australia 3.76%
- Germany 3.76%
- Italy 3.76%
- United Kingdom 3.47%
- Turkey 3.43%
- Others 19.89%

Protocol Based Steganography

Network steganography is the newest form of this discipline. Unused fields within the TCP/IP protocol header are used to hide data. This method is on the rise because attackers can send an unlimited amount of information through the network using this technique.
Protocol Based Steganography

Each packet using the TCP/IP protocol, there is a “header” area
  Provides information about the packet, such as its size, identification and IP address.

Each header contains multiple areas that are “optional” fields to be set as needed by the sender of the data
Such areas can be exploited and used for concealing information in the packet headers.
The actual message being transmitted is in this case the carrier file since the information to be hidden is embedded within its packet header.
The intended recipient simply needs to capture these packet headers and reveal the hidden information.

Sources

https://securityintelligence.com/steganography-a-safe-haven-for-malware/
Have fun!
**Steganography** is the concept of hiding messages within a cover medium in such a way that it arouses no suspicion to the existence of the message at all. The main use of steganography is secret communication between two parties, preventing an external third party from noticing anything out of the ordinary in the content of their communications. The most popular carrier is the digital image due to its frequency usage on the Internet, large amount of redundant bits, and the size.

**Steganalysis** is the study of detecting messages hidden using steganography. The goal of steganalysis is to identify suspected files, determine whether or not they have a payload encoded into them, and, if possible, recover that payload.

**Step 1 – Find a hidden map: Statistical Steganalysis**

You are a forensic investigator.

You receive information about illegal substances coming through the border. The criminals communicate to other criminals by using seemingly innocuous pictures that contain possible hidden data.

Your task is to detect and crack the images with hidden information such as location and time in order to uncover criminal plans.
The information hiding process changes the statistical properties of the cover, this is one attribute that an analyst will analyze. This process is called statistical steganalysis.

To perform this analysis, you will use hex editor: **GHex** to load an image file and then view, edit and analyze its structure.

On the desktop of your Virtual Machine there is a folder named “Investigation”. This folder contains various suspicious images that you have collected while working on the case. You have information that one of the images contains secret data. Apply statistical analysis to detect a stego-image:

1. First, let’s observe what kind of images we are dealing with. Open a terminal located on the Desktop, and use the commands below to gather information on the files:
   
   ```
   cd Desktop/Investigation
   file *
   ```

   As you can see, nothing is suspicious. Every file extension corresponds to the file extension. What specific JPEG format (or standard) do the images use?
   Your answer: ____________________________

2. Every image file format has a fixed structure: beginning or header, called “Start of Image” and a trailer called “End of Image”. Here are some additional facts about JPEG images that will help you in later steps of this exercise.

   • JPEG files start with specific bytes: 0xFF D8 (in hex) and always ends with a certain value depending on the specific standard used.

   • If trailer is different from this value, this indicates that the file is corrupt, and could mean that the image contains hidden data.
With this information in mind, you will now look at the bytes within a JPEG image.

a. To look at the structure, right click on the picture you want to analyze, and choose GHex.

The display pane on the left side is showing the bytes that make up the image. Notice that the image starts with 0x FF D8. The right pane is a parallel view of the data that displays any valid ASCII values associated with the bytes on the left side. Notice the ASCII string JFIF.

b. Open image007.jpg and image011.jpg and find the common trailer bytes for these types of images (look at the very last bytes of the files):

c. One of the images in the folder is corrupt. Find it and write the name of the file:

________________________________________________________________________

d. Look closer at the ASCII for this particular file and write down 2 or 3 other observations (besides the non-conformant trailer) that would make you question the legitimacy of this file:

________________________________________________________________________
PKZip is a tool used to compress file contents. The resulting compressed file will contain the ASCII characters “PK” near the end of the file.

e. Find the PK characters in the image file that you are analyzing.

![Image with PK characters]

Give a reason that someone would store a PKZip file within an image.

___________________________________________________________________________
___________________________________________________________________________

3. In the terminal make sure you are in Desktop/Investigation directory (if not, use cd command from Step 1) and then run the command below to decompress the hidden contents in the file.

   `unzip <FileName>`

*Note: the decompressed contents file will be saved in a subfolder under your “Investigation” folder.*

How many files were hidden in the image?
___________________________________________________________________________

What types of files are they?
___________________________________________________________________________

Write the location where the criminals plan to meet:
___________________________________________________________________________

Congratulations! You resolved the location. In the next step will help you to find date and time.
Step 2 – Find information about the date/time: Steganography tools.

The main goal of modern Steganography tools is that the act of embedding should not create any statistically detectable artifacts in the stego images. The stego-image’s structure is one such artifact.

In this step you will use the `stegdetect` tool. It is a popular automated tool for detecting potentially steganographic content in images and the algorithm used.

4. Read up on the stegdetect tool and usage by opening the manual. Run the following command and press the `q` key when you’re finished.

```
man stegdetect
```

5. Use stegdetect to find a suspicious image and the possible tool or algorithm used to embed information.

   Image name: _______________________   Tool/algorithm used: _____________________
OutGuess is a universal steganographic tool that allows the insertion of hidden information into the redundant bits of data sources and extraction.

6. Go to the terminal and type name of the tool that you discovered through the detection:

   `outguess`

Now you should see tool’s options. Find the appropriate option that you are going to use to extract hidden data:

6. Extract hidden data by typing the command in terminal:

   `outguess <option_you_chose_from_previous_step> <name_of_the_image> Secret.txt`

Now you can find the hidden message in the Investigation folder, or use `cat Secret.txt` command to read it from the terminal.

7. Write the data/time when the criminals will meet:

   Date: _______________  Time: _______________

   Congratulations! Your resolved date and time of the upcoming criminal activity!
Step 3 – Hide a message into image

******************************************************************************

You want to lead criminals astray by replacing original information with a later date/time so that you can ensure that officers will have adequate time to prepare to catch the criminals in the act.

During this step, you will modify the secret message, and hide it in the image.

******************************************************************************

8. Open the Secret.txt file you just extracted from the image using the graphical folder view. Change the date to May 1, 2019 and save it.

9. In the terminal, use the following command to hide your secret file:

   outguess -d Secret.txt <name_of_the_cover-image> Output.jpg

10. Now you can delete the original file, and rename your new carrier file Output.jpg to the original name to remove any suspicion.

   Congratulations! Your mission is accomplished!