Steganography
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.

![Diagram of 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

Can you see the difference?

No one does!
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
Malware constantly progresses to avoid surveillance and detection.

To avoid detection, some malware uses steganography to hide its malicious content within an innocent cover file.

The most common techniques:

- Conceal malware settings or a configuration file
- Provide the malware a URL from which additional components can be downloaded from
- Store directly the whole malicious code
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.
Steganographic Cyberattacks

- A Sundown attack begins when a victim visits any website with malicious ads
- The victim is automatically redirected to the exploit kit
- Victims are redirected toward the Sundown landing page
- The page retrieved and downloaded PNG images.

- PNG file data is encoded and hides malicious code within it
- The Sundown kit landing page contains a decoding routine that unlocks the PNG file and extracts the malicious content.
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

- Within each subsequent packet that is transmitted using the TCP/IP protocol, there is a “header” area which provides information about the packet, such as its size, identification and IP address.
- Within each header, there are a multitude of areas that are not used for normal transmission or are “optional” fields to be set as needed by the sender of the data.
- These areas can be exploited and used for concealing information in the packet headers.
- The actual message being transmitted would be considered the carrier file since the information to be hidden is embedded within the packet header.
- The intended recipient would simply need to capture these packet headers and to reveal the hidden information.
Sources

https://securityintelligence.com/steganography-a-safe-haven-for-malware/