- Filename: eccouncil-ceh31250-v11-6-9-1-steganography.md
- Show Name: CEHv11 (312-50)
- Topic Name: System Hacking Phases and Attack Techniques - System Hacking
- Episode Name: Steganography
  ==

Steganography

Objectives:

- Define Steganography and explain how it is used for malicious purposes
- List and define the different Steganographic classifications
- Explain common Steganography types and tools
- Explain the purpose, process, and challenges of Steganalysis
- List and define common Steganalysis methods and tools

- Today we're taking a look into Steganography and Steganalysis. It seems like this is probably a topic that many are unfamiliar with and they are related, but different, so can we start with an explanation of what Steganography is?

  - Steganography is the hiding of data in the unused space of a file

    - Images
    - Audio files
    - Video files
    - Text files

      - These are called 'Cover Medium'

- So do you just somehow open a jpeg and start typing your data into it, or how does someone hide data in this way? I assume there are tools to do this?

  - stegsnow (ASCII text files)

    - `stegsnow -C -p password -m "secret message" infile.txt outfile.txt`

  - steghide (image files)

    - `steghide embed -ef exfil.txt -cf hacker.jpg -sf hacker2.jpg`

- Now that we're aware of Steganography, let's talk about Steganalysis.

  - Steganalysis is discovering and uncovering of steg data

    - Tools

      - Steghunt
      - zsteg (on Mint)

        - `zsteg cats.img`