Log into the Kali VM and created a secret txt file with some messages from the text editor nano. Use the command below

root@Kali-Attacker:/tmp/random# nano secret.txt

Graphical user interface, PowerPoint

Description automatically generatedAfter writing message, close the nano editor and conform the file name

Find any availbe jpg formet picture and verify its size is bigger than the size of your secret file. The comands for this purpose are:

root@Kali-Attacker:/tmp/random# steghide info earth.jpg 🡺 shows the size of picture file.

root@Kali-Attacker:/tmp/random# du –b secret.txt 🡺 shows the size of your secret file

root@Kali-Attacker:/tmp/random# sha1sum earth.jpg 🡺 shows the hash values of picture

root@Kali-Attacker:/tmp/random# steghide embed –cf earth.jpg –ef secret.txt

🡺 embed the secret file into the picture file

Graphical user interface

Description automatically generated

You can see the embedded data within the picture file and extract it. Below is the command for this purpose.

root@Kali-Attacker:/tmp/random# steghide info earth.jpg

🡺 it prompts and ask if you want to information about embedded data, press Y to see.

root@Kali-Attacker:/tmp/random# steghide extract –sf earth.jpg

🡺 it extracts embedded file.

root@Kali-Attacker:/tmp/random# cat secret.txt 🡺 Opens the file to show message.

Graphical user interface

Description automatically generated

Graphical user interface

Description automatically generated