Lab 9: Steganography

Thangamuthu Balaji

I. Introduction

THIS is the lab report for Lab 9: Steganography of the course, Cyber Defense Competitions where the students completed tasks that covered the topic of Image Steganography. This lab served to help students learn about various tools that could be used to detect steganography and how to use them to retrive possible hidden information.

II. Using DominicBreuker's stego-toolkit repository to analyze image 1.secret and image 2.secret

The process of hiding information in non-secret material, such pictures or files, is called steganography. The goal of this lab is to utilize a variety of forensic and steganography methods to reveal concealed information in two supplied photographs (1.secret and 2.secret). The objective is to assess how well various instruments and techniques identify, extract, and decipher hidden material. Watermarking, espionage, and cybersecurity all make extensive use of steganography. Knowledge of its methods and defenses has practical uses in information security and digital forensics. Our first assignment was to use Dominic Breuker's stego-toolkit repository, a Docker image helpful for resolving steganography issues, to discover any secrets concealed in image 1.secret. Numerous well-known tools and screening scripts are pre-installed on the image, which you may use to verify basic items.

I started with cloning the DominicBreuker's stego-toolkit repository from git and then using the docker container to start the project. I uplaoded the images that I wanted to analyze in the data folder in the repository.
I used the following tools for my analysis:
file - Check out what kind of file you have.
exiftool - Check out metadata of media files.
binwalk - Check out if other files are embedded/appended.
strings - Check out if there are interesting readable characters in the file.
foremost - Carve out embedded/appended files.
pngcheck - Get details on a PNG file (or find out is is actually something else).
identify - GraphicMagick tool to check what kind of image a file is. Checks also if image is corrupted.
zsteg - Detects various LSB stego, also openstego and the Camouflage tool. LSB stands for Least Significant Bit. The idea behind LSB embedding is that if we change the last bit value of a pixel, there won't be much visible change in the color. For example, 0 is black. Changing the value to 1 won't make much of a difference since it is still black, just a lighter shade. [2]

III. Findings

1) ***file:*** The files 1.secret and 2.secret were identified to be PNG images.

Fig. 2. 1.secret file

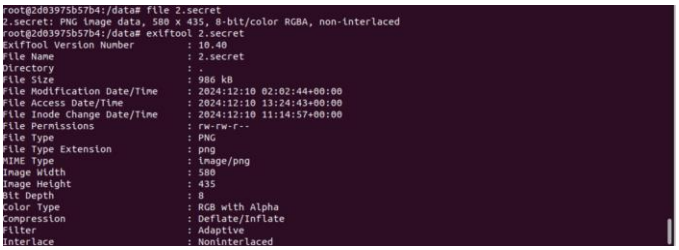

Fig. 3. 2.secret file

2) exiftool: This tool provided with a variety of image-related metadata for both photos, including profile details, color qualities, and dimensions (855 x 502).
3) Binwalk: The image 1.secret's copyright was identified as "Copyright (c) 1998 Hewlett-Packard Company" by the binwalk utility. Nevertheless, it also exposed several MySQL files that were contained in the picture 2.secret.
4) strings: The stings tool assisted in determining if each image included any legible text. The picture

1.secret had a few strings that contained the data we gleaned from the picture and metadata. 2. Secret appeared to lack any logical strings.
pngcheck, foremost and identify: These were some more additional tools that I tested on the image 1.secret.

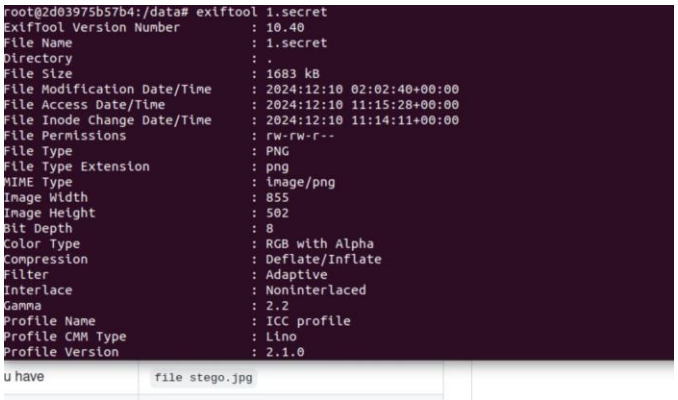

Fig. 4. 1.secret exiftool

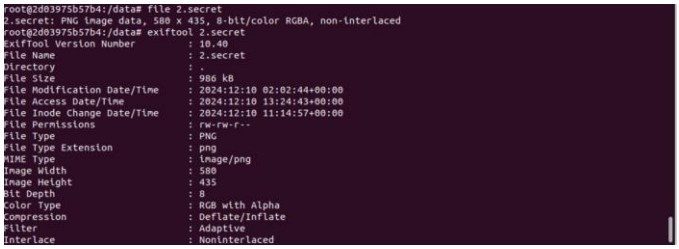

Fig. 5. 2.secret exiftool

Fig. 6. 1.secret binwalk

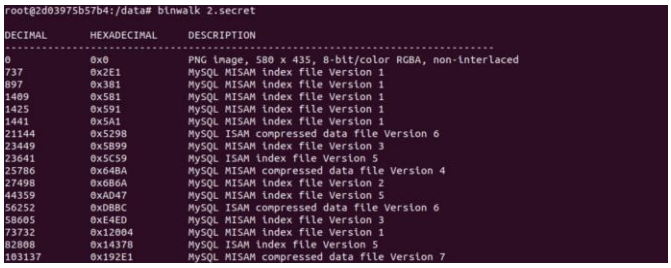

Fig. 7. 2.secret binwalk

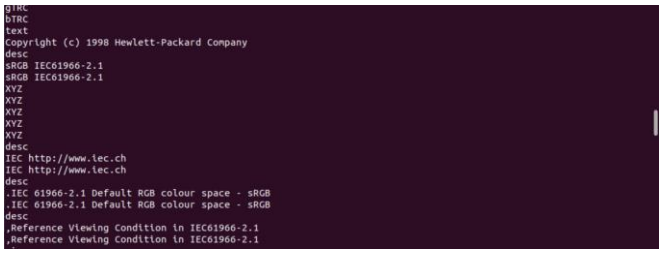

Fig. 8. 1.secret strings

It confirmed if the image is a PNG image, checked for any embedded files and checked if the image was corrupted in any way.

2) ***zsteg:*** This was a tool designed to detect steganography

Fig. 9. 2.secret strings

Fig. 10. 1.secret pngcheck foremost identify tools

mainly does statistical tests, but only in straightforward situations can it disclose hidden meanings. However, if it discovers intriguing inconsistencies, it could offer clues about what to hunt for.

The text "gc7W[*(C)" was discovered in image 1.secret, while other patterns and files were discovered in image 2.secret.

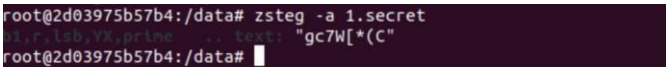

Fig. 11. 1.secret zsteg

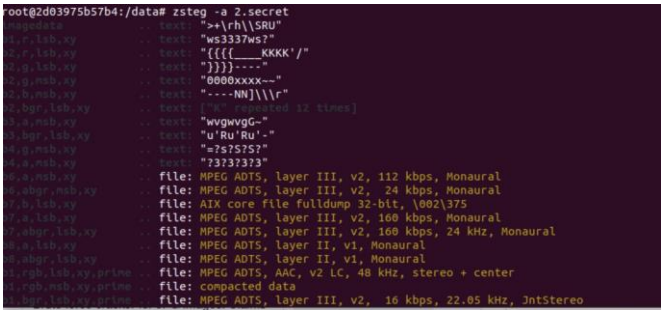

Fig. 12. 2.secret zsteg

IV. Conclusion

I can say that I've finished all of the lab assignments successfully. This lab gave participants practical experience with steganography tools, demonstrating both their advantages and disadvantages in terms of revealing secret data. For straightforward situations, technologies like Binwalk and Zsteg worked well, but advanced methods.

REFERENCES

[1] ”Wstego-toolkit” github.com https://github.com/DominicBreuker/ stego-toolkit

[2] ”LSB based Image steganography using MAT- LAB” geeksforgeeks.org https://www.geeksforgeeks.org/ lsb-based-image-steganography-using-matlab/