

CSCI 352.61E, Digital Forensics

Assignment 3

Steganography

Objective: The objective of this assignment is to hide a data file using STEGHIDE.

Tools Required:

1. STEGHIDE – `sudo apt install steghide -y`
2. STEGSEEK – `sudo apt install stegseek`
3. WORDLIST –
<https://github.com/danielmiessler/SecLists/raw/master/Passwords/Leaked-Databases/rockyou.txt.tar.gz>

Instructions:

Step 1: Download lab file

<https://github.com/yaukacheung/csci352/blob/main/A3/week6-lab.bmp>

Step 2: Install STEGHIDE

Step 3: Create your own secret text file

e.g. `echo msg > file.txt` or `nano file.txt`

Step 4: Hide the file

Step 5: Extract the file

Step 6: Install STEGSEEK

<https://github.com/RickdeJager/stegseek>

Step 7: Download ROCKYOU wordlist

<https://github.com/danielmiessler/SecLists/raw/master/Passwords/Leaked-Databases/rockyou.txt.tar.gz>

Step 8; Unzip rockyou.txt.tar.gz

`tar -xvzf rockyou.txt.tar.gz`

Step 9; Cracker password

Step 10: Documentation and reporting

Deliverables:

- A report covering the steps, observations, and results.
 - Summarizes your observations.
 - The report should include: The steps taken from 1 to 6
- Screenshots of the steps.