Image Possession Investigation Report

CSC351 Spring2024

Prof. Thiep N. Pham

Submitted by: \_\_\_\_\_\_\_\_\_\_

Date of report:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Case#:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Abstract**

The Digital Forensics Final Project entails a comprehensive exploration of steganography, which shows how data is concealed within other files, specifically data files in images. The project shows a real-world scenario where students are given two roles: suspect and investigator. As suspects, students embed incriminating evidence within images using steganography tools, following specific instructions. Subsequently, as investigators, they extract the hidden content and meticulously document their findings in a forensic report. The project aims to enhance students' understanding of steganography techniques, digital forensic procedures.

# Introduction

## Background

The primary reason for this project is to give students a hands on experience with digital forensics and it’s infamous technique of steganography. This project is crucial as it helps to show how various files which might include virus or malware, hidden in plain sight in other files. Investigators must have a go through such files in order to confirm any sort of suspicion and find any evidence that could be pivotal in any related legal case.

By engaging in the project, one could have practical knowledge and experience with hiding and extracting data, two of the most crucial aspects of digital forensics. This will prepare students to handle similar real life situations.

## Objectives

### Tasks

List the steps (high level) involved for your investigation, ordered from 1 to n:

* + - * Step 1: Open up the folder and observe the files present in the folder. See if any clue can be observed.
      * Step 2: Take a look at the attributes of the files like name, size, type, etc. and observe any similarity or irregularity that might be suspicious.
      * Step 3: Open steghide in Linux in terminal and try running the extract command to see any result.
      * Step 4: Crack the password using any technique or using clues gathered from elsewhere in the investigation.

### Hypotheses

List your hypothesis/hypotheses (generally what you expected from the finding).

* + - * Hypothesis 1: Initially, I thought that most of the images would contain people either one or many.
      * Hypothesis 2: I thought that the content might follow some sort of a repeating pattern.
      * Hypothesis 3: I also expected the revealed data to describe instructions or clues to a particular act or crime.

### Domain Terms

List terminologies unique to this project and their short explanation/definition.

* + - * Cover File: The digital media file, such as an image, within which secret content is concealed using steganography tools.
      * Steganography: The practice of concealing secret information within digital media, such as images, audio files, or videos, without visibly altering the file's appearance.
      * Payload: The hidden or secret information that is being passed through using the images.
      * Detectability: The degree to which the presence of some secret message could be detected.

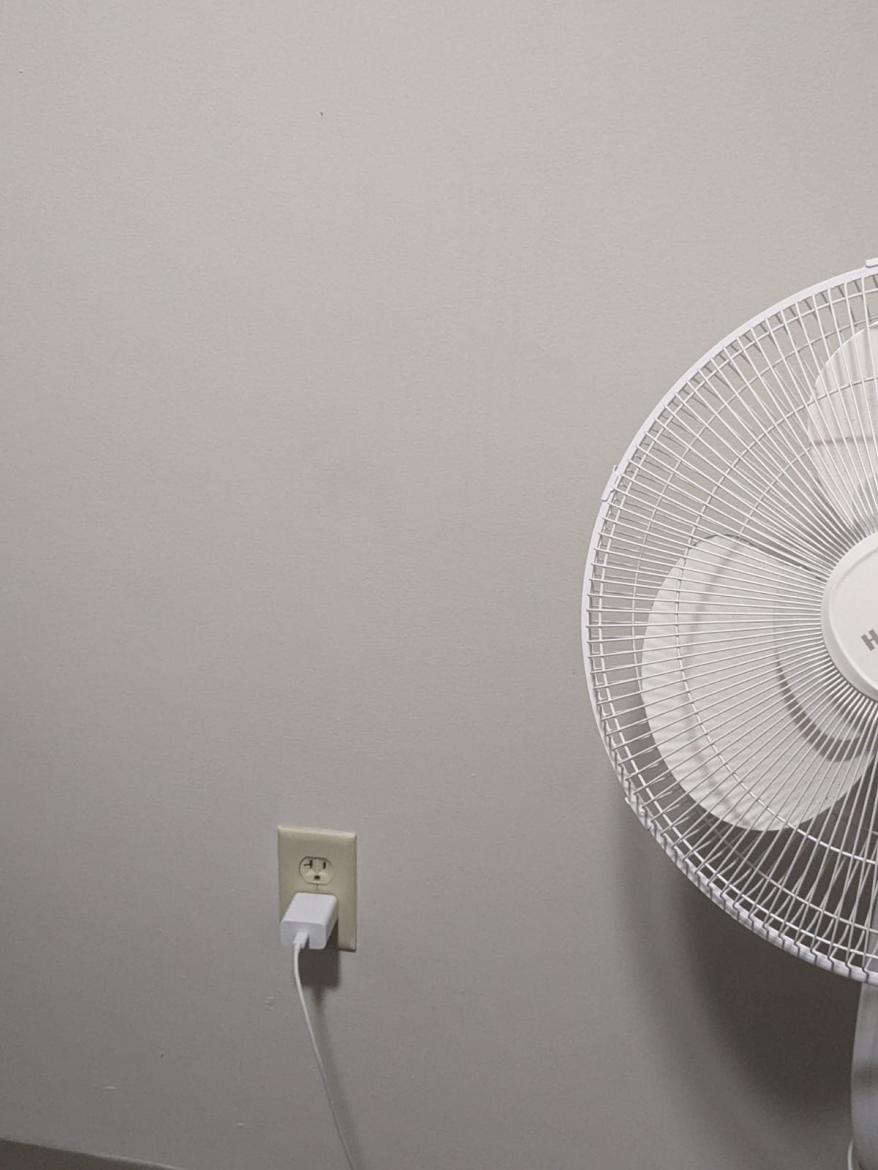
## Acquired Data

Fill out the table containing detailed information on the obtained data FOR EACH PICTURE.

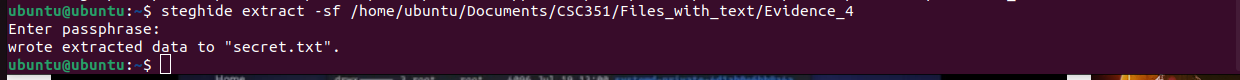
* + 1. File name: Evidence\_4

|  |  |
| --- | --- |
| **Attribute** | **Detailed Information** |
| OneDrive Path |  |
| MD5 | a38d1dbb870054061c21a6f8e9049b91 |
| SHA-256 | f270e3a7955e3579b4bad1aad6bddc862288639c65321f7cdooofadac578b4a4 |
| File size | 743KB |
| Picture taken (date) | 4/5/2024 |
| Acquired on (date) | 4/7/2024 |
| Acquired by (onsite investigator) | \_\_\_ |
| Was there obfuscation evidence? | Yes. |
| Describe the contents | This was a scenic picture of a river through a forest. There wasn’t any person spotted in the picture nor was there any other information visible. There was a hidden text file named secret.txt, embedded in it. |
| Other information | The text file had the information regarding the suspect’s name, occupation and a statement claiming his skills in Linus OS.  The content of the files are: Name : Jammy  Occupation : Student at Bradfords  Other information : Proficient in linux |

Include the original evidence/picture below:



Include the obfuscation evidence:



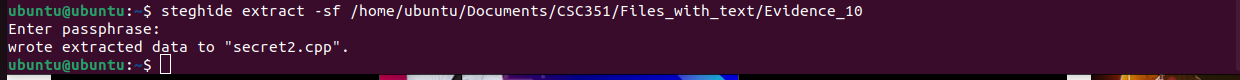
* + 1. File name: Evidence\_10

|  |  |
| --- | --- |
| **Attribute** | **Detailed Information** |
| OneDrive Path |  |
| MD5 | 6518ac4e1b5b05d27d2febocbff0220d |
| SHA-256 | 8bcofcb2b81c246706159a5b22462d277e93a30df62cd6552619d9d4bobfa308 |
| File size | 421KB |
| Picture taken (date) | 4/5/2024 |
| Acquired on (date) | 4/7/2024 |
| Acquired by (onsite investigator) | \_\_\_ |
| Was there obfuscation evidence? | Yes. |
| Describe the contents | This was selfie of the supposed person under suspicion. There was also a hidden code file within it by the name of secret2.cpp. |
| Other information | This was a code script written in C++ which was printing out information regarding the suspect using a function.  The actual code in the file is given as below:  #include <iostream>  #include <string>  using namespace std;  void printInfo(const string& name, const string& occupation, const string& otherInfo) {  cout << "Name: " << name << endl;  cout << "Occupation: " << occupation << endl;  cout << "Other information: " << otherInfo << endl;  }  int main() {  string name = "jammy";  string occupation = "student";    string otherInfo = "Proficient in Linux, studies at Bradford Univeristy England";  printInfo(name, occupation, otherInfo);  return 0;  } |

Include the original evidence/picture below:



Include the obfucation evidence:



## Suspect Information

Provide information about the threat actor:

Table 1: Suspect Information

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Information** | **Brief Description** |
| name | Jammy | The suspects name appears to be jammy, which seemingly is a real name rather than a fabricated one. |
| Occupation | Student | The suspect is told to be a student at Bradford University, an institute excelling in the field of computer science. |
| Hacker classification | Proficient Linux User | As a someone who is capable of using Linux to it’s utmost, it’s no doubt this person is aware of hacking techniques. |

## Investigator Information

Investigator background:

Table 2: Investigator Information

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Information** | **Description** |
| name |  |  |
| Credentials *(example: certifications)* | Certificate in Digital Forensics | Gained a certificate from Kutztown University stating my proficiency and practical knowledge in digital forensics. |
| Similar previous cases | Cracking a case of cheating in lab exam. | Helped catching a few students who were cheating by sending images with answers embedded in them during a lab exam. |

# Actions

## Tools Used

### Suspect’s Tool(s)

* + - * Name of the tool: Steghide
      * Make: N/A (Open Source)
      * Model: N/A (Single codebase)
      * Serial#: N/A (Doesn't use serial number)
      * Other information: version is 0.5.1 and is used in Linux OS primarily.
      * Describe the tool (include any uniqueness): Free and open source software with support for audio files as well. Primarily used for digital forensics.
      * Location used: Documents folder in home menu.

### Investigation’s Tool(s)

* + - * Name of the tool: Steghide
      * Make: N/A (Open Source)
      * Model: N/A (Single codebase)
      * Serial#: N/A (Doesn't use serial number)
      * Other information: version is 0.5.1 and is used in Linux OS primarily.
      * Describe the tool (include any uniqueness): Free and open source software with support for audio files as well. Primarily used for digital forensics.
      * Location used: Documents folder in home menu.
      * Installation steps (detail steps such as software installation and settings): Add as many steps as necessary.

1. Open terminal in Linux and use the statement “sudo add-apt-repository universe”
2. Now apply the statement “sudo apt update”
3. Now finally install it using the statement “sudo apt install steghide”
4. **Investigator Activity logs**

Describe your findings in a couple of paragraphs and what you have learned.

After analyzing the acquired data from the investigation, several crucial findings have surfaced. Firstly, it became evident that the suspect, known as "Jammy," utilized steganography techniques to hide evidence inside seemingly un important image files. Through the use of the Steghide tool, the suspect embedded hidden text files and code scripts within the images, thereby obfuscating the true nature of the files and making them appear ordinary at first glance.

Upon extraction of the hidden content, it was revealed that the concealed text files contained valuable information about the suspect, including their name, occupation as a student at Bradford University, and proficiency in using Linux. Additionally, the code script embedded within one of the images provided further insight into the suspect's capabilities, as it demonstrated their knowledge of programming in C++.

The user had named the two files with the hidden information differently from the rest. The two files were named “Evidence\_4” and “Evidence\_10” instead of “Evidence 4” and “Evidence 10” which was the usual trend with the rest of the images. This made them stand out and worth checking once. There wasn’t anything to read in the images and the use of Linux prompted to check them out using steghide tool.

The passphrase which prompted was also cracked by seeing the evidence of simplicity in the persons life. Naming things like usernames, wifi passwords etc. using his name and simple numbers. Thus with some trial and error the passphrase was easily figured out to be “J1234”.

Throughout the investigation, it became clear that steganography presents a significant challenge for digital forensic professionals. The ability to hide data within images without altering their appearance makes it difficult to detect hidden content using conventional methods. As investigators, we must remain vigilant and employ specialized tools and techniques to uncover concealed information effectively.

1. **Conclusion**

Write a couple of paragraphs with your conclusion of this case. The conclusion must also answer the hypothesis question.

In conclusion, the investigation into the use of steganography by the suspect "Jammy" has provided valuable insights into the complexity of digital forensics and the challenges posed by covert data concealment techniques. Through meticulous analysis and extraction of hidden content from the images, we have successfully uncovered crucial information regarding the suspect's identity, including their name, occupation as a student at Bradford University, and proficiency in Linux. Additionally, the discovery of embedded code scripts further elucidates the suspect's technical capabilities and modus operandi.

Addressing the hypotheses formulated at the outset of the investigation, it is evident that they have been largely confirmed. Contrary to the initial expectation of encountering a paucity of evidence, the investigation yielded substantial findings, underscoring the importance of thorough scrutiny and persistence in digital forensic examinations. Furthermore, the hypothesis regarding the detectability of hidden data by the naked eye was debunked, highlighting the insidious nature of steganography in concealing incriminating information within seemingly innocuous files. Lastly, the hypothesis concerning the difficulty of cracking the password proved to be true to some extent, as the passphrase "J1234" was relatively simple and easily discernible from clues gathered during the investigation.

Overall, this case exemplifies the critical role of digital forensic professionals in uncovering clandestine activities and gathering evidence crucial for legal proceedings. By leveraging specialized tools and techniques, alongside astute investigative methodologies, we can effectively combat cyber threats and uphold the integrity of digital evidence in pursuit of justice.

**References**

(Include any references in APA v. 7)