CCSI 410 Forensic Lab Report

1) Investigator’s Name: \_\_Matt Ferry\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2) Date of Investigation: 08/11/2013 \_ \_\_

3) Lab Number and Title: Lab 5: Steganography Detection\_

4) Summary of Findings:

*Performed required steps for the lab, and answered the required questions. During the analysis added several words in regards to the case to try to determine if vacation-7.jpg and vacation-10.jpg contained any hidden information, as it was potentially possible for the given word file to be incomplete. No additional information was found in these files. Given the information that was found in vacation-1.jpg, vacation-6.jpg and vacation-9.jpg there is enough evidence to warrant continuing the investigation into this issue.*

5) Details of Investigation

Thursday, August 08, 2013

12:20 PM Beginning Lab assignment, logged into lab

12:20 PM Question 1 (see below)

12:34 PM StegDetect: Sensitivity 1.00, vacation-1.jpg, jphide(\*)

12:38 PM Stegdetect: Sensitivity 1.00 vacation-10.jpg,

Negative, Sensitivity 2.00, Negative, Sensitivity 3.0 Negative, Sensitive 4.0, Sensitivity 5.0 jphide(\*)

12:44 PM StegDetect: Sensitivity 1.0 vacation-2.jpg, Negative, Sensitivity 2.0 Negative, Sensitivity 3.0, negative, Sensitivity 4.0

12:47 PM Stopping scanning of files individually 1 at time, due to attempting to scan all the files of the image folder and discovering that StegDetect can scan an entire folder at once. (Noting that Acrobat reader does not appear to be installed, So unable to read the PDF files for stegdetect and stegbreak)

12:50 PM Sensitivity 1.0 Files that show Detection:

Vacation-1.jpg jphide(\*)

Vacation-9.jpg jphide(\*\*\*)

12:51 PM Sensitivity 2.0 Files that show Detection:

Vacation-6.jpg jphide(\*)

Vacation-7.jpg jphide(\*)

12:52 PM Sensitivity 3.0 – No new hidden information

12:53 PM Sensitivity 4.0 – No new hidden Information

12:54 PM Sensitivity 5.0 – Vacation-10.jpg jphide(\*)

12:55 PM Sensitivity 6.0 – No new hidden information

12:56 PM Sensitivity 7.0 – No new hidden information

12:56 PM Sensitivity 8.0 – No new hidden information

12:57 PM Sensitivity 9.0 – No new hidden information

12:58 PM Sensitivity 10.0 - No new hidden information

Noting that the Jphide levels for 6, 1, and 7 have increased to jphide(\*\*\*) , and that 10 has increased to jphide (\*\*).

1:02 PM Running Stegbreak on detected files using the wordlist.txt file that was supplied to detect the password.

1:07 PM vacation-1.jpg password bigmoney

Vacation-9.jpg password Wilma

Vacation-6.jpg password georgerocks

1:11 PM Reconfirmed the vacation-7.jpg is showing

jphide(\*) at sensitivity level 2.0

1:12 PM vactation-10.jpg negative

1:12 Pm Noting Stegdetect detected 5 jphide files, Stegdetect was only able to break 3 using the given wordlist.txt

1:15 PM Added: Company, contract, jet, fighter to the wordlist file, Re-ran stegbreak on 7 and 10, still negative.

1:17 PM Added: kid, kidnap, and kidnapped to the wordlist file, R-ran stegbreak on 7 and 10, still negative.

1:20 PM added: monty(short for Montgomery), and Montgomery to the wordlist file, Re-ran stegbreak on 7 and 10, still negative, moving on to next step of the lab assignment.

1:25 PM using JPHS for windows to attempt to decrypt hidden files.

Saving detected file from vacation-1.jpg to vacation1out, 4kb

Saving detected file from vacation-6.jpg to vacation6out 1kb

Saving detected file from vacation-9.jpg to vacation9out 4kb

Renamed vacation1out to vacation1out.jpg, attempting to view as an image file.

1:32 PM successfully viewed the file as an image, it appears to be some sort of antenna array.

1:34 PM Renamed vacation9out to vacation9out.jpg, attempted to open in image viewer, file did not open. Renamed to vacation9out.doc, and attempted to open.

1:35 PM vacation9out.doc opened successfully in WordPad. This file contains a key (software, encryption?), and pass key/phrase (bigmoney, already in word list and discovered as phrase for vacation-1.jpg).

1:38 PM renamed vacation6out to vacation6out.jpg and attempted to open the file. File failed, renaming to .doc, and attempting to open as a doc file.

1:39 PM renamed vacation6out.doc file successfully opened, it appears to be a short note setting up a meeting time.

1:47 PM Closing lab environment and answering Questions 2, 3 and 4

Sunday, August 11, 2013

12:00 PM Writing Summary and cleaning up report presentation.

6) Please type the answers to the questions found throughout the lab here.

**Question 1 - Determine what kinds of steganographic/hidden information for which you will be looking. In other words, describe the kind of case you are working, what kinds of steganographic images you will be looking for and give some hypothetical examples. Use your imagination!**

**ABC Company Inc. is a military contracting company that makes jet fighter parts. Considering that information, we should be looking for any images that contain hidden pictures, or other hidden information that relates to Jet Fighter parts: Part images, blueprint schematics, material lists, material specifications, confidential contract information, and other confidential files.**

**Question 2: What are the pass phrases for each steganographic image that you found?**

|  |  |
| --- | --- |
| **Filename** | **Password** |
| vacation-1.jpg | bigmoney |
| vacation-9.jpg | wilma |
| vacation6-jpg | georgerocks |

**Question 3: In your Forensics Report, note the following information about each extracted file: the outcome file's name, the size of the file, whether it is an image or text file, and how it is possibly related to the case.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Filename** | **Outcome Filename** | **Size** | **Type** |
| vacation-1.jpg | vacation1out | 4kb | image |
| vacation-6.jpg | vacation6out | 1kb | Doc/text |
| vacation-9.jpg | vacation9out | 4kb | Doc/text |

|  |  |
| --- | --- |
| **Outcome Filename** | **Relevance** |
| vacation1out.jpg | Picture of an Antenna Array or Other Military part |
| vacation6out.jpg | note setting up a meeting time with anonymous |
| vacation9lout.jpg | File contains Key (software / Encryption?) and Pass/Key(bigmoney) |

**Question 4: List and describe all hidden files found.**

|  |  |
| --- | --- |
| **Filename** | **Description** |
| Vacation1out.jpg | An image file of an antenna array or some other military part |
| Vacation9out.doc | Contains a key(Software, Encryption?) and pass/phrase(bigmoney) |
| vacation6out.doc | a short note to an anonymous person setting up a meeting |