CCSI460 Final Forensic Lab Report

Investigator’s Name: *Matt Ferry*

Date of Investigation: *September 18, 2013*

Lab Number and Title: Week 3 Homework

Summary of Findings:

This method of hiding data was relatively simple to do as it only took me about 45 minutes to figure out how to embed an image successfully using the steghide tool. The turning point in this assignment was finally noticing and using the info switch that allows the user to determine the maximum file size that can be “covered” or hidden in the original image. Once this information was known embedding information within the file was easy. This means that if I could figure this out within such a short time period that anyone that is even remotely computer savvy would also be able to figure it out as well. This process enables information to be transmitted stealthily without people realizing what was happening unless they were specifically looking for files that had hidden information within them, and even then, they would have to have the proper tools and potentially passwords to access those files.

As for tools that we can use to detect these files, there are tools such stegdetect / stegbreak, but those tools will not always detect hidden information because it depends on how the information was hidden and whether or not that program can detect the file. One way to detect possible files containing hidden images though is through the files hash value and file sizes. However, even this requires the investigator to have the hash value and size of the file as an unmodified file so that they will be able to tell that a modification has been made and that the file should be investigated further.

Details of Investigation:

Assignment for this homework assignment was to use steghide to hide an image within another image.

9/18/13

5:45AM – Downloaded Image file for the homework assignment.

5:46AM – Obtained hash value for hidden.png

hidden.png f7981d5068fa39dd258cd819d75caa31

5:55AM – Downloaded and Extracted Steghide.zip from doc sharing, ran program in a command prompt to obtain proper syntax for hiding an image

5:56AM – Located a picture to embed into hidden.png

5:56AM – Attempting to embed image

5:57AM – The “hidden” file on doc sharing is a png file not a jpg file. Png is not supported by steghide. Converted the hidden.png file to a jpg file.

5:59AM – Because the file has been converted to a JPG file, obtaining new hash values as the jpg compression process will have changed the hash value.

hidden.jpg cbf35d84df2e5873ff46a0cbb17accc9

6:00AM – Attempting to use steghide again to hide an image.

6:02AM – Received an error indicating that the file is too small to embed the image file. The image to be embedded is 13k in size, compared to the hidden.jpg size of 87k.

6:06AM – Discovered that the 87k was at 100% quality, so there was no way to increase the file size of hidden.jpg. Attempting to reduce the file size of the image to be embedded further.

6:10AM – Cropped and reduced the file to be embedded, reducing the file size from 13k to 9k.

6:12AM – Cover file is still too small.

6:17AM – Cropped and reduced image again, reducing the size from 9k to 6k

6:19 AM – Cover file is still too short. Because files are in the JPG format, which means they are already compressed.

6:25AM – Finally, noted the info flag in the steghide command and ran steghide info hidden.jpg. Hidden.jpg can cover a 4.1 kb file. Attempting to reduce my image file size down to 4.1k.

6:30AM – Image to file size finally reduced to 4 k, attempting to embed once again.

6:31AM – Embedding process successful

6:33AM – Hashing the new hidden file

hidden.jpg c76f09c184600409fd4af10b699fab57

6:34AM – Noting that even though the image file size does not show to have been changed (it is still 87k) the Hash value is different. Re-Hashing original image just to be sure.

hidden.jpg.old cbf35d84df2e5873ff46a0cbb17accc9

6:35AM – Confirmed that the hash values have indeed changed from the original hidden.jpg to a new value indicating that information within the hidden.jpg after steghide embedding was successful.

6:40AM – Using a copy of the file, used steghide to extract the image and confirm that embedding actually took place. The Image was embedded and extracted successfully.

6:41AM – Noting that the original file was 86.2 KB (88,346 bytes) and that the new hidden file size is 86.9 KB (89,059 bytes) , so there is a very small file size increase which is still smaller than I would have expected.

6:45AM – Answering the last step of the homework assignment in the summary section.