Steganography On Internet And Its Forensic Analysis

Sadhana Rathore, Arundhati Walia

1. Case Scenario

Case Scenario is performed on an internet media and is associated with corporate intellectual property theft. Two fictitious criminal characters, Ankit and Sadhana were used to portray the sender and receiver for the covert communication in the experimental case scenario.

2. Intellectual Property -Case Scenario

Café Coffee Day (CCD) is a Café chain that owns many cafes in India. Ankit, one of the marketing team members was very unhappy with the recent decision to promote Bob as Sales Manager instead of him. Ankit thinks that he deserved it more than Bob. So, to show his unhappiness at the company, he started sending company's weekly unreleased promotional information and business's plans to a competitor, Barista. CCD company's IT policy blocks the USB port from saving files externally, so to send the confidential information to the competitor covertly, Ankit decided to use photograph to communicate with the competitor and use image steganography to transport the confidential information. Therefore, with the help from Ankit, Barista, located two blocks away, knows CCD's insider plans and has taken on their competitor easily and this has impacted CCD's businesses. Since the pattern was so persistent, the management team decided to undertake an internal investigation of the sales and marketing department as promotional items and price were planned and organized by the team. From an interview, Richard, the Sales and Marketing Director, told the investigation team that, Ankit had acted differently since Bob had been promoted Sales Manager last month and other colleagues also said that Ankit was telling other team members that he deserved better. One of them even saw Ankit was having coffee with the Barista Managing Director three days ago and the network administrator found that Ankit had been spending lots of his work time on internet lately. From the interview, Ankit seems to be a suspect, thus, the company decided to seize Ankit's work computer and the hard drive was brought by the IT team to the forensic lab to look for evidence of Ankit distributing confidential Company information to Barista. Information collected from the interview was passed on to the forensic team, and the forensic team decided to look for any traces they can gather from Gmail, Facebook and Twitter history as this was the most predominant activity that performed lately.

- *Sadhana Rathore, M. Tech Student, Computer Science Engineering, HRIT Ghaziabad, India*
- *Arundhati Walia, Associate Professor, Department of Computer Science, HRIT Ghaziabad, India*

The first data to be collected are the pre-test results from three different steganographic techniques or tools (SteganPEG, SilentEye and Xiao Steganography) tested on Facebook, Twitter and Gmail. The steganographic images generated by the above mentioned steganographic techniques (3 images) will be uploaded using three different platforms on internet (Facebook, Twitter and Gmail). These uploaded images are then to be downloaded to see whether the embedded secret messages can be successfully extracted. This pre-test data will be able to ascertain which steganographic techniques can or cannot be used and which internet platform can assist or inhibit image steganography. Following were the findings w.r.t size of the image:

Steganographic Tool\Internet Platform (Size of original image was 1.81 MB)	Size of Embedded image	Size of image on Facebook	Size of image in Twitter	Size of Image in Gmail
SteganPEG	1.81 MB	463 KB	219 KB	1.81 MB
Silent Eye	743 KB	459 KB	217 KB	743 KB
Xiao Steganography (14.7 MB)	14.3 MB	FAILED	FAILED	FAILED

Following Table summarizes the steganographic techniques that can and cannot be used with Facebook, Twitter and Gmail.

Steganographic Technique\Internet Platform	Facebook	Twitter	GMail
SteganPEG	N	N	Y
Silent Eye	N	N	Y
Xiao Steganography	N	N	N

4. Environmental Set-up

The scenario used a laptop equipped with Wi-Fi connection, Intel Core 2 Duo- 2.30 GHz processor, 4 GB RAM and 500 GB Hard Disk Drive. The photo used in the simulation were captured with an iPod 5th Generation having pixel size 2592 X 1936. The HDD was fully wiped and Windows 7 Home Premium was freshly installed. For the forensic investigation environment, the data collection of the user's hard drive was performed with a software write blocker called SAFE Block Win 7 and FTK Imager 3.0. All the acquired evidence image files were verified with MD5 and SHA hash values and saved as Encase evidence files (.E01) in an external 1TB hard drive.

5. Digital Forensics

The digital forensic process for Case Scenario adopted the digital forensic phases proposed by Noureldin, Hashem, and Abdalla (2011). The process steps are: 1) Evaluation and Assessment 2) Acquisition of Digital Evidence 3) Survey of Digital Scene (optional) 4) Digital Evidence Examination 5) Reconstruction of Extracted Data 6) Conclusion

6. Evaluation and Assessment

Laptop was powered off when seized
Only suspects HDD was sent to forensic lab.
Tools needed: SATA to USB connecter, software write blocker SAFE Block Win7, FTK Imager 3.0, Encase 7.0, Internet Evidence Finder, WinPrefetchView, StegAlyzerAS, StegAlyzerSS.

7. Acquisition of Digital Evidence

It is a Western Digital Hard Disk
Model: WD1600BEVS
Storage: 500 GB
Serial Number: WXEZ13A28492
The user‘s hard drive was connected to the investigator machine with a SATA to USB connector. The investigator machine, installed with SAFE Block Win 7 software write blocker and FTK imager, was used to image the suspect‘s hard drive bit-by-bit and saved it on an external hard drive as T1.E01. The integrity of the T1.E01 file was verified with MD5 and SHA hash values. After acquisition the physical hard drive was kept in a secure place.

8. Survey of Digital Scene

The suspect‘s imaged hard drive was mounted in StegAlyzerAS and StegAlyzerSS to search for steganographic tool artefacts and steganographic image artefacts. The evaluation of the imaged hard drive found two applications containing unique steganographic file artefacts, four applications containing detected registry artefacts, 0 signature files, three appended image files, and three files having LSB embedding.

Forensic Tool	Steganographic Artefacts Detected	No. of Applications Found (T1.E01)
StegAlyzerAS	Unique Files	2
StegAlyzerSS (Registry)	Registry	4
StegAlyzerSS (Signature)	Signature	0
StegAlyzerSS (Append)	Appended	3
StegAlyzerSS (LSB)	LSB	3

9. Digital Evidence Examination

The imaged hard drive evidence file was added into Encase 7.0 for data extraction and evidence processing. Each file in the evidence file was hashed with MD5 and SHA to ensure the integrity of the data files. Internet artefacts were also automatically extracted. Internet Evidence Finder was also used to extract internet activities. Following Table is the summary of data extracted from user’s HDD.

Forensic Tool	Domain	No. of URLs visited	Total visits
Encase V7	mail.google.com/	13	153
Encase V7	account.google.com/	11	55
Encase V7	google.co.in	35	235
Encase V7	google.co.in/	43	67
IEF V5	mail.google.com/	7	221
IEF V5	account.google.com/	5	21
IEF V5	google.co.in	4	32
IEF V5	google.co.in/	32	54

10. Reconstruction of Extracted Data

Further analysis was carried out in WinPrefetchView. By looking at the content of each prefetch file, it was found that SteganPEG and SilentEye (extension) contained files associated with images located in folder Secret in HDD and text document located in folder CCD. This implies that SteganPEG and SilentEye were assessing these files during its execution. Furthermore, these text files are confidential documents belonging to CCD. Consequently, it was further examined and 5 images were found. Out of these, 3 images were indicated in both prefetch files. These are the highly suspect image files that could be the steganographic images. All these 3 images were tested on both the found suspected steganographic tools (SteganPEG and SilentEye). After thorough checking and guided approach, the data was found to be suspected.

11. Conclusion

Based on the extracted and reconstructed data, it is evident that the suspect was actively accessing CCD‘s confidential data and was active on Gmail at a similar timeframe. SteganPEG.exe and SilentEye.exe artefacts identified by StegAlyzerAS were also ascertained by execution artefacts and associated text files and image files left in the Windows pretetch files. Furthermore, the timeframe of the SteganPEG.exe and SilentEye.exe executions fell into the last accessed time of various artefacts ranging from CCD‘s confidential text documents, suspected image files, and Gmail history. These identified artefacts have positively shown that CCD‘s confidential documents have been embedded by the suspect into the suspected image files and mailed via Gmail attachment. However, at this stage there is no direct evidence to prove that the three suspected image files found on the suspect‘s work station were indeed embedded with CCD‘s confidential documents as there was no indication of a passphrase to extract the secret message from these suspect images. To prove that CCD‘s confidential documents were embedded in these three suspect image files, additional cryptanalysis, consent and interview to get the passphrase from the suspect will be needed. Once the passphrase is given by the suspect, each of the suspicious image files can be exported and the embedded file can be extracted.

References

[1] http://www.sans.org/reading-room/whitepapers/stenganography/steganalysis-detecting-hidden-information-computer-forensic-analysis-1014

[2] http://www.ijcta.com/documents/volumes/vol2issue3/ijcta2011020338.pdf

[3] http://www.garykessler.net/library/fsc_stego.html

[4] http://cs.wellesley.edu/~crypto/lectures/tr10.pdf

[5] http://omicsonline.org/open-access/an-alternative-approach-of-steganography-using-reference-image-0976-4860-1-95-102.pdf?aid=35426

[6] Alharbi, S., Weber-Jahnke, J., &Traore, I. (2011). The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review. International Journal of Security and Its Applications, 5(4), 59–72. Retrieved from http://www.earticle.net/article.aspx?sn=158919

[7] Ashok, J., Raju, Y., Munishankaraiah, S., & Srinivas, K. (2010). Steganography: An overview. International Journal of Engineering Science and Technology, 2(10), 5985–5992. Retrieved from http://www.ijest.info/docs/IJEST10-02-10-100.pdf

[8] Castiglione, A., Cattaneo, G., & De Santis, A. (2011). A forensic analysis of images on online social networks. 2011 Third International Conference on Intelligent Networking and Collaborative Systems, 679–684. doi: 10. 1109 / IN CoS. 2011.17

[9] Castiglione, A., D'Alessio, B., & De Santis, A. (2011). Steganography and secure communication on online social networks and online photo sharing. 2011 International Conference on Broadband and Wireless Computing, Communication and Applications, 363–368.

[10] Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. Signal Processing, 90(3), 727–752. doi : 10. 1016 / j. sigpro. 2009. 08. 010