****

**What a Digital Forensics Investigator Should**

**Know About Steganalysis of Digital Content**

**Year 3 Computer & network Forensics**

**Submitted by:**

**James Finglas – B00094138**

**Submission date**

**15/10/2018**

Contents

[Abstract 3](#_Toc529034167)

[Introduction 3](#_Toc529034168)

[Steganalysis Approaches 5](#_Toc529034169)

[Steganography Signatures and Detection Methods 5](#_Toc529034170)

[Conclusions 6](#_Toc529034171)

[References 6](#_Toc529034172)

# Abstract

Steganalysis has become of interest to law enforcement services, the legal professions, intelligence agencies and the corporate world. With the rise of digital child pornography websites, terrorism, corporate espionage not to mention a growing intelligence in ordinary criminal circles it is important for a digital forensic investigator to be able to place some context to Steganalysis.  
  
This report covered a brief history of Steganalysis as well as the importance of Steganalysis in modern digital forensics and what the investigator should know about it. Some examples of how Steganalyis were carried out in an order to display methods of identification of Steganographic signatures.  
  
The report will cover a broad analysis of Steganalysis principals rather than specifics in order give as comprehensive an overview as possible.

# Introduction

Steganography has been around for hundreds of years stretching back to the times of the ancient Greeks. Leonardo Da Vinci himself employed some earliest forms of both steganography and cryptography, as did Galileo. So how is this relevant to Steganalysis? Well, one must ask a simple question. Since it is known that church was widely aware of the activities of Galileo, and deeply suspicious of Da Vinci why then did the church not discover the hidden writings of these masters?  
  
The answer is simple. To be able to decipher the hidden messages one must be aware that somebody might be trying to hide a message in the first place. One must also be aware of the methods employed and have such an understanding as to be able to uncover and/or decipher the message. Without knowledge of these things, one might simply find themselves looking for a needle in a haystack that may not even be there.  
  
As human technology developed in the modern age and Steganography moved into the digital age, the ability to identify that a message may be hidden grew more difficult. While it was still possible to extract messages hidden using digital images, it was common practice for each image to have be analysed with a view to every file within a given disk image having the possibility of containing a hidden message. Naturally, in the face of the vast number of files typically contained on a hard disk just in Operating System files alone, this could be an extremely daunting task taking a vast amount of time and resources.  
  
In the early 90’s **[1]** a new branch of research began to emerge that aimed at reducing this problem by developing methods of identifying the use of Steganography. The goal of the research was to analyse as many methods of Steganography as possible to identify the signatures left by the application of Steganographic programs.  
  
This is Steganalysis. The ability to identify the application of Steganography to a file via signatures. The

advantages of this is that a file can quickly be identified as having a hidden message. This process can also be automated.

Steganalysis can be broken down into two sub categories.

* Passive Steganalysis: This branch, the main branch of steganalysis is concerned only with the identification of a hidden message.  
    
  This area is principally used in the law enforcement arena, and the corporate business arena; with the retrieval of the message being passed on to other team members.
* Active Steganalysis: The secondary branch, a relatively new area of steganalysis moves beyond detection; and concerns itself with retrieval and even modification of a hidden message.  
    
  This area is principally used in the areas of both intelligence agencies and corporate espionage. An intelligence agency may for example, implant a tracking algorithm r malware program to track targets of investigations. A Corporation may implant false data to obfuscate the information a competitor was attempting to steal.

In summary, Steganalysis is an attempt to defeat the very purpose of Steganography by reducing the ability to hide a message by offering methods of rapid identification of a hidden message. This is merely the first step in this area of digital forensics, but it is by its very nature, the most important in the area of steganography. After all, if a hidden message cannot be located, it cannot be revealed.

An investigator beginning a Steganalyis must therefore be aware of certain things when examining a file. A file may or may not contain hidden data, but it is the signatures he or she is looking for, NOT the data. The data may have been encrypted before being inserted into the carrier file, therefore if active Steganalysis is being pursued a working knowledge of cryptanalysis may be required. A hidden message may have been obfuscated by noise or have extra irrelevant data added to make a steganalysis more difficult or time consuming. One does not need to retrieve the data to consider a passive Steganalysis of a file a success, one only needs to prove a message exists. **[2]**

# Steganalysis Approaches

There are two principal approaches to analysing a file or data stream suspected of being a carrier file. The first type, is known as the “Blind” approach. In this case, nothing is known about the type of Steganography deployed on the suspect carrier file. This method is very thorough however it is very time consuming. It is a systemic attempt to manually Identify known signature types in an effort to break the Steganography. It is here, in the blind approach that the investigator is most likely to encounter many of the draw backs of Steganalysis as previously mentioned.  
  
The second and more commonly used approach, is known as the “Analytical” approach. The approach was developed principally by the ‘Steganographic Analysis and research Centre” (SARC), who have more recently been incorporated into BackboneSecuruity.com. The analytical approach was developed by storing a large database consisting of almost every known Steganographic program and the signatures they created on a carrier file. This allowed for rapid signature detection.  
To date the SARC database contains 960+ applications and their associated known signature types. It is commonly used by both national (US) and international government and intelligence agencies and private sectors. Repositories also include the world’s largest set of known Hashes applicable to Steganography. **[3]**The SARC project has led to the development of one of the most comprehensive File analysing programs. Not to mention real time data stream detection and signature analysis which of course aims at not only recognizing current signatures but newly burgeoning signatures. SARC has also developed a comprehensive and internationally recognized training certification program. This is highly beneficial in a field of expertise whose value is only now beginning to be fully recognized. **[4]**There are many new approaches to Steganalysis being explored every day, so many they far exceed to scope of this report. But there is one that deserves a brief mention. Audio Steganalysis. With the recent rise in popularity of Podcasting as a form of media, not to mention the popularity of the MP3 file format. It was inevitable that audio steganography use would rise. Using complex waveform, inner loop, noise increase, block size variance and several other methods this method aims at detecting audio Steganography. Two major benefits of audio Steganography are that the message can be broken up and stored in multiple pieces and that there are several injection types available in an audio file. **[5]**

If one employs the Blind method to a Steganalysis of a file this can be further broken down into one of six basic types of Steganalysis attack **[6]**:

1. **Stego only attack**: In this case only the suspect data stream or file object is available for analysis
2. **Known message attack**: The original virgin (Pre-Steganography file) carrier file is available as well as the Stego object. A direct comparison can be performed to detect abnormalities.
3. **Known message attack**: The hidden message and the corresponding carrier file are known. The type of attack may not seem useful at first hand since everything is provided for a full analysis, however this does help establish known patterns and hashes for future analysis.
4. **Known Stego attack**: Both virgin and carrier files are available as well as the type of steganography being known.
5. **Chosen Stego Attack**:The Steganography program and carrier file are known.
6. **Chosen Message attack**: In this case, the investigator will use Steganographic tools to create Stego objects, to compare the resulting signatures against suspect data streams or carrier files.

# Chain of Custody and Documentation of Methodology It cannot be underestimated the importance of maintaining a proper chain of custody of evidence, secure facilities; a well-maintained lab and a thorough procedure for documenting each step taken in the analysis of any file or data stream. This is the back-bone of any investigation. One can easily envision a case where a lengthy investigation is undertaken, and crucial evidence is found. However, the defence asks one simple question. “Did you document your work?”. If even one step has not been documented, doubt can be introduced.

# Steganography Signatures and Detection Methods

# Conclusions

# References

1. Computer and information science magazine, Image Analysis for online Dynamic Steganography Detection, Kevin Curran, Joanne Mc Devitt, Intelligent Systems Research Centre. Published at ww.ccsenet.org/journal html, August 2008.  
     
   3.Steganalysis.  
     
   https://pdfs.semanticscholar.org/d2a4/8b4087ec079167a4e7497c7c44cb0c122ead.pdf
2. An Analytical Approach to Steganalysis, James E. Wingate, Chad W. Davis, Forensic Focus, July 10, 2011.

https://articles.forensicfocus.com/2011/07/10/an-analytical-approach-to-steganalysis/

1. Back Bone Security, who incorporated SARC.

https://www.backbonesecurity.com/Database960Applications.aspx

Original SARC blog, http://sarc-wv.blogspot.com/

1. StegAlyzerAS, StegAlyzerSS, StegAlyzerRTS & Certified Steganography Examiner Training.  
   https://www.backbonesecurity.com/SARC.aspx
2. Comprehensive Review of Audio Steganalysis Methods, Hamzeh Ghasemzadeh, Mohammed H. Kayvanrad, !9 January 2017. <https://arxiv.org/abs/1701.05611>
3. Paladion, May 2015, https://www.paladion.net/blogs/steganalysis