ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 9, May 2017

EXPLORING COMPUTER FORENSICS

Racheet R Srivastava[1], Shikha Singh[2]

Department of Computer Science and Engineering, Amity School of Engineering and Technology, Lucknow, India

ABSTRACT*:* The Internet is growing extensively, as is the crime rate against or using computers. As a response to the growth of computer crime, the scope of computer forensics has emerged. Computer forensics can be defined as & quote; the use of computer examination and study methods in the interests of determining potential legal evidence. This paper provides as with a preface to the discipline of Computer Forensics. With computers being involved in a continuously increasing number, and type, of crimes the outline data left on electronic media devices can play a vital part in the legal process.
This paper provides a straightforward overview of the steps involved in the examination of digital media, methods of hiding/receiving data, and uses of computer forensics. Steganography is one of the techniques that a Forensic Expert tackles and finds solution too. It is the technique of hiding a file, text, image, or any other information within another file, image, or text. We would be discussing the above mentioned things at a later stage.

I. INTRODUCTION

In this paper we would be discussing the meaning of the term 'COMPUTER FORENSICS', steps involved in this type of forensic investigation, and it's uses. The paper would also focus on a particular forensic technique, 'STEGANOGRAPHY', and the reason for its use. The field of computer forensics began to evolve approximately 30years ago in the early years of 1980s in the United States in order to safeguard important and private information of the state and also to protect from any kind of intrusion and prevent any other future unauthorized access. [12]

The history of computer science forensics can be broadly studied under three phases:-

1)Ad-hoc phase
2)Structured phase
3)Enterprise phase

AD-HOC PHASE:-
This can be termed as the stage when various officials came to realize that some type of formal investigation in the area of cyber crime and other digital crimes was needed. Also there were lot of legal issues related to the collecting and management of electronic evidence.
STRUCTURED PHASE:-This is the stage that deals with the enhancement and development of a more complicated solution for computer forensics. It would include authorized procedures and techniques that were designed specifically to solve doubts and problems related to computers and various type of criminal legislation.
ENTERPRISE PHASE :-
It is that phase in which the field of computer forensic currently is, i.e. the most advanced of all the phases. At this point, computer forensics is regarded as an actual science which involves real-time collection of evidences, development of effective methods and processes, and use of structured protocols and procedures.

II. WHAT IS COMPUTER FORENSICS?

COMPUTER FORENSICS is a division of science that deals with studying, analyzing, and collecting evidences from different electronic storage devices, such as, computers systems, PDAs, digital drives, mobile phones, and various other memory storage devices. It can be used in the discovering and prevention of crime and in any dispute where evidence is stored digitally. Basically the goal of computer forensics is to examine digital media in a manner which is accepted by

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 9, May 2017

the science with the aim of distinguishing, safeguarding, recovering, and presenting facts and ideas about the digital data and information. [13]

Computer forensics is different from other traditional forensic techniques as a traditional forensic expert might collect and preserve fingerprints and various other physical evidences whereas, a computer forensics specialist collects and preserve digital evidences which can be used for future references and legal matters.

STEPS INVOLVED IN EXAMINATION

The investigation can be broadly carried out in six steps according to the order of their occurrence:-

1. *READINESS*

It is the most fundamental and primary stage which is mostly neglected during examination which includes enlightening users about system preparedness. For a forensic examiner as well this method includes proper guidance, periodic testing and authenticating their software and tools and ensuring that data removal kit is properly performing.

2. *EVALUATION*

This stage includes receiving of data, analyzing the risks and the allocation of roles and provided resources. Risk analysis may comprise an examination of the possibility of substantial threat on entering a suspect's property and how best to prevent it from taking place.

3. *COLLECTION*

This stage involves the branding and storing of various evidences from the site of crime. The materials should be transported carefully and safely to the forensic laboratory.

4. *ANALYSIS*

During this stage the investigator provides feedback to the client of his investigation. The outcome should accurate, precise, non-biased, tabulated, and completed within the time limit and with the resources provided.

5. *PRESENTATION*

In this stage a structured and systematic report on the investigation that was carried out in presence of expert guidance. It may also contain any other information that the investigator seems important or of help in further investigation.

6. *REVIEW*

A review of a report can be very simple and easily displayed in any of the earlier stages of examination. It gives a general idea of what errors were observed, the problems faced, and most importantly the result of the investigation. [18]

USES OF COMPUTER FORENSICS

Computer forensics can be used in various fields and for several reasons:-

1. CRIMINAL CASES-

Computer forensics is extensively used in the investigation of several criminal cases and legal matters. The analysis may act as evidence in proving that the crime actually took place, computers may or may not be used directly.

2. DOMESTIC MATTERS-

Domestic cases are mostly related to infidelity or unfaithfulness and the spying of one person on his/her partner by reading mails, entering chat rooms, etc.

3. SECURITY ISSUES-

The Centre for Computer Forensics has provided data that states that nearly 92% of various important records and documents are stored on digital devices and that forensics helps in prevention of any damage to this data and prevents from any kind of tampering.

The task assigned to a computer forensic expert is to help and determine whether a computer disk or any other form of media contains material that is possible evidence or not. If it does then the expert must administer the extraction of evidence and ensure that information is obtained without causing any damage to the original data. [16]

There are several reasons why only a specially trained and qualified professional should be called to investigate a cyber crime:-

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 9, May 2017

1. To handle issues related particularly to the digital data
2. To maintain the series of custody
3. To avoid and prevent the digital information from being manhandled

III. STEGANOGRAPHY

'Art of hiding data in data'

Steganography is the science of hiding any important data, information, or image behind another data, text or image. In this method, except the sender and the intended recipient can suspect and recover the hidden data. The advantage of steganography over cryptography is that the hidden data does not attract any attention towards itself for scrutiny. It not only hides the content of the message but also the possibility of any secret message. Steganography could also be used in places where cryptography is illegal. [1,7]

This technique has been in use from the recent historical times as:

1. Hiding message in wax tablets
2. Hiding messages on messenger's body
3. Hiding message written with secret ink [6]

There are various techniques which are being used nowadays like

1. Physical- hiding on messenger's body, writing with secret ink, hiding under Morse code.
2. Digital- concealment with noisy image, chaffing and winnowing, blog-steganography.
3. Social- hiding info in the title of a shared video or image, misspelling the name of file.
4. Network- it is classified under two heads:
   a. Steganophony- Conceal messages in voice over conversations
   b. WLAN Steganography- Transmission of steganograms in WLANs. [3]

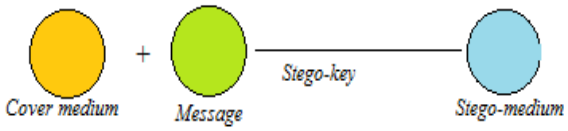

fig. 1. Components of Steganography

TECHNIQUES FOR CONCEALMENT (DIGITAL)

Some of the common approaches of hiding information in digital media include:

· Least significant bit insertion
· Masking and filtering
· Algorithms and transformations [4]

Least Significant Bit- This is the simplest form of embedding message in a cover file. In this method we change and manipulate the Lowest Significant Bit (Right most bit) of message data. Though this message is vulnerable and not very effective as it tends to hamper the information stored in it. Some of the tools for this technique are, S-tools, EzStego, Steganos, etc.

Masking and Filtering- This image hides the information while marking the cover image which makes it similar to *Watermarking.* The message is embedded in various areas of the cover image so that the information makes an integral part of the image. Digital Watermarking techniques are used for this technique.

Algorithm and Transformations- This technique uses compression of the information using *Discrete Cosine Transform (DCT)* technique. It is a much more robust method than *Least Significant Bit.* There are various algorithms which are used to achieve this, *Patchwork Algorithm* being the most profoundly used. [17]

Watermarking- This technique may or may not identifiable by the human eye. Digital watermarking is similar to steganography as it also embeds the messages. It is more secure against threats like cropping, compression, etc. [2]

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 9, May 2017

The major difference between steganography and digital watermarking is of the intent. Watermarking works with cover as the object of communication whereas Steganography treats the hidden information as the object.
Digital watermarking may also be used for Fingerprinting. This is the embedding of serial codes that distinguish between distributed data sets. Fingerprinting maybe a unique code that may identify the recipient of data or the owner itself. Thus watermarking may help track copyright violators and fingerprinting may help in the judgment. [5]

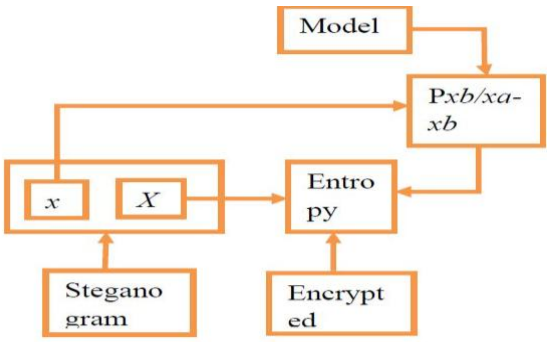

Fig. 3.2: A model based steganography decoder

IV. CONCLUSION

Steganography has recently been given a new breath of life as various governments are making moves to restrict the availability of encryption services. This has led people to study methods by which private messages can be embedded in seemingly innocuous cover messages. However, the main driving force in current academic research work in information hiding is the concern over protecting copyright. The recent advancement in the field of technology has also given rise to copying and piracy and has become a great concern for music, film and software publishing industries. Thus, the information hiding techniques like Steganography are best suitable option to safeguard the documents. Even though there have been several attacks against watermarking and other data hiding techniques but the presence of methods to counter them gives strength and survivability to the techniques. Despite all the advancement, there is still too much scope in this area which could be used in law enforcement, digital traffic analysis, bank transactions, etc. [9]

REFERENCES

[1]. Wikipedia. http://www.wikipedia.com/ 2006
[2]. Arnold, M., Schmucker, M., and Wolthusen, S. D. Techniques and Applications of Digital Watermarking and Content Protection. Artech House, Norwood, Massachusetts, 2003.
[3]. Artz, D. Digital Steganography: Hiding data within data. IEEE Internet Computing (2001) 5(3):75-80.
[4]. Stefan K.,;Fabian A. P. P: Information Hiding Techiques for Steganography and Digital Watermarking. Artech House Boston SSBN 1-58053-035-4, pages 237
[5]. Hosme,r C. and Hyde C.; 'Discover Cover Digital Evidence' Digital Forensic Research Workshop (DFRW) 2003
[6]. Cole, E. Hiding in Plain Sight. Wiley, John & Sons, Incorporated. 2005.
[7]. Bauer, F. L. Decrypted Secrets: Methods and Maxims of Cryptology, 3rd ed. Springer-Verlag, New York, 2002.
[8] Herodotus, " The Histories ", London, England: J. M. Dent & Sons, Ltd, 1992.
[9] Sellars, Duncan. "An Introduction to Steganography". http://www.cs.uct.ac.za/courses/CS400W/NIS/papers99/dsellars/stego.html
[10] Johnson, Neil F., Jajodia, Sushil "Exploring Steganography: Seeing the Unseen". http://www.jjtc.com/pub/r2026.pdf
[11] *A Yasinsac; RF Erbacher; DG Marks; MM Pollitt (2003). "Computer forensics education". IEEE Security & Privacy. CiteSeerX 10.1.1.1.9510.*
[12] *Casey, Eoghan (2004). Digital Evidence and Computer Crime, Second Edition. Elsevier. ISBN 0-12-163104-4.*
[13] Computer Forensics: Digital Forensic Analysis Methodology, from Computer Forensics issue: January 2008 Volume 56 Number 1
[14] Computer Forensics, Cybercrime and Steganography Resources http://www.forensics.nl/links/
[15] Forensics Information from CERT http://www.cert.org/forensics/
[16] Kessler International - Forensic Accounting, Computer Forensics, Corporate Investigation. http://www.investigation.com/praccap/hightech/compforen.htm
[17] Guide to Integrating Forensic Techniques into Incident Response (pub. #: 800-86), 2006, US NIST
[18] Oseles, Lisa. "Computer Forensics: The Key to Solving the Crime."
[19] Robbins, Judd. "An Explanation of Computer Forensics." http://computerforensics.net/forensics.htm
[20] Validation and verification of computer forensic software tools - Searching Function, by Yinghua Guo, Jill Slay, Jason Beckett, DFRWS 2009