Combating Against Anti-Forensics Aligned with E-mail Forensics

Sridhar Neralla
Research Scholar,
Dept.of CS&SE
Andhra University,
Visakhapatnam,
Andhra Pradesh, India.

D.Lalitha Bhaskari
Associate Professor,
Dept.of CS&SE
Andhra University,
Visakhapatnam,
Andhra Pradesh, India,

P.S.Avadhani
Professor,
Dept.of CS&SE
Andhra University,
Visakhapatnam,
Andhra Pradesh, India,

ABSTRACT

Knowledge on cyber forensics is increasing on par with the cyber crime incidents. Cyber criminals' uses sophisticated technological knowledge and always they plan to escape from the clutches of law. This paper elaborates e-mail forensics and categories of anti-forensics that can be applicable to the e-mail forensics. This paper elucidates the process of identifying such anti-forensics applied in e-mail forensics. This paper proposes a methodology for combating against anti-forensics in this regard.

General Terms

Information Security, Cyber Forensics.

Keywords

Anti-Forensics, Cyber Crimes, Digital Evidence, E-Mail Forensics, Stylometry

1. INTRODUCTION

Anti-forensics is combination of tools and technique that disturbs intact forensics community. Anti-forensics avoids detection of cyber crimes as well as misleads cyber forensics tools. It attacks the forensics tool and reveals the presence of the forensics tool. This paper discusses about anti-forensics impact on forensics investigation. Second section deals with the overview of anti-forensics and its effect. Section three discusses anti-forensics scenario and introduces e-mail forensics process. Fourth section focuses categories of anti-forensics that are applied to e-mail forensics along with proposed methodology for combating various categories.

2. STUDY OF ANTI-FORENSICS

Anti-forensics is one of the biggest challenges for cyber forensics to invalidate factual information for court of law. Major goal of anti-forensics is not getting caught by forensics investigator. Unfortunately, combating anti-forensics is a thorny problem because it is neither process nor methodology. Initially anti-Forensics was described by Rogers [1] as "attempts to negatively affect the existence, amount, and/or quality of evidence from a crime scene, or make the examination of evidence difficult or impossible to extract". Ryan Harris defined anti-forensics as methods used to prevent the application of science to those criminal and civil laws that are enforced by police agencies in criminal justice system [2].

Later Kessler [3] gave a general definition as anti-forensics (AF) is that set of tactics and measures taken by someone who wants to thwart the digital investigation process. The major aim of anti-forensics is to mitigate effectiveness of forensic efforts. This paper defines anti-forensics as "attempts to compromise the availability or usefulness of evidence to the forensics process which violates the rules of court of law".

Anti-forensics is an amalgamation of process, people and tools. Understanding anti-forensics is also difficult. Some of the Cyber forensics tools sometimes acts as double edged knife, one way they are useful to administrator and other way they helps malicious attackers. Consider nmap tool, it is one of the best cyber forensics tools; it provides better understanding of the network. The other face of nmap is malicious attacker uses the same tool for exploiting security issues.

Evidence plays vital role in court of law. Especially as per Indian laws, even if thousands of culprits escape, not even single innocent person should be punished. Cyber criminals using this as a weapon and defense lawyers tries to protect clients (both good and bad) by using anti-forensics knowledge. Consider e-mail forensics scenarios, timestamp plays an important role for identifying the log information, but it permits attackers to sabotage time information to corrupt forensics analysis. Forensics investigators can now determine their ability to provide accurate information that could potentially be submitted in court of law.

Paula Thomas et al. [4] discussed the process of anti-forensics approach in Windows system related to USB devices. In their paper they explained the registry key entries on a Windows XP system to find the changes made by USB storage devices. There are certain anti-forensics tools to delete these USB entries, if a forensics investigation blindly follows the log-information related to USB, he /she may be mislead by such anti-forensics tools. Defense lawyers can use the knowledge of such anti-forensics tools as a weapon and they can argue in the court of law to protect their clients.

Current trends towards research in anti-forensics focus on blogging information. Glenn et al. [5] discussed anti-forensics and counter anti-forensics related to blogs. Ryan Harris [2] attempted to provide a standardized method of addressing anti-forensics and outlines some guidelines in his paper. Sridhar et al. [6] stressed the point to further strengthening of cyber forensics related to protect from anti-forensics activities.

Allessandro et al. [7] extended importance of study related to anti-forensics towards mobile devices. Their focus was majorly on android-related devices. Recently, Ioana Sporea et al. [8] also discussed anti-forensics tools related with smart phones. Haodong et al. [9] focused on counter forensics related to JPEG compression forensics. David Cowen et al.

[10] shown that they can recover data hidden or destroyed by anti-forensics by using tools for NTFS.

3. ANTI-FORENSICS METHODS FOR E-MAIL FORENSICS

3.1 Anti-Forensics Used by Terrorists

Forensics methods contain several approaches that perform investigation, collection, analyzation and other tasks. Tariq [11] explained techniques and tools for forensic investigation of e-mail in his paper.

Recently it is identified that Terrorists are using E-mails as their communication in a different way. To avoid getting detection by forensics experts terrorists have been communicate through 'dead drop' email system [12]. Consider two terrorists A and B, to communicate, first A opens e-mail account and type the required mail. Instead of sending the mail, A stores the mail in Drafts folder. He logs out from the mail. Later B opens same e-mail account at different location and reads the content from Drafts folder. After completion of this process, B deletes the saved document from the Draft folder. In this particular case A and B are using the technique of shared password. As per anti-forensics process, this communication involves Hiding Evidence (storing in Draft Folder), Destroying Evidence (B deleted the saved document from Draft Folder). This total process is shown in the figure 1.

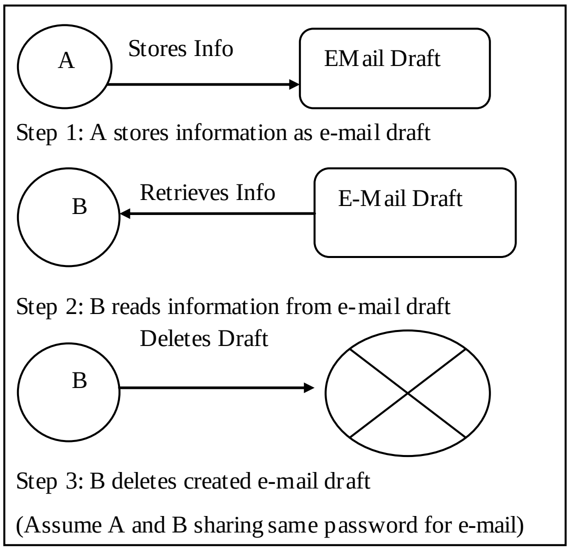
A
Stores Info
EMail Draft
Step 1: A stores information as e-mail draft
B
Retrieves Info
E-Mail Draft
Step 2: B reads information from e-mail draft
Deletes Draft
B
Step 3: B deletes created e-mail draft
(Assume A and B sharing same password for e-mail)

Fig 1: Understanding Anti-forensics scenario

Spam mails were used as another weapon by Terrorists. Generally when a user received the spam mail, automatically spam mail moves to Trash kind of folder, and users ignore or deletes the entire spam folder at once. It is observed that terrorists are using this spam as their mailing communication for a group of terrorists. Using Steganography techniques, Sender creates a hidden message in a spam mail and sends to billions of users including their targeted receivers. Other than these receiver terrorists, deletes the spam mail or after reading the message also they can't understand it. But group of terrorists who received the spam mail, filter out the required message from the spam mail.

The above two case studies shows the toughness of anti-forensics that aligned with e-mail forensics. Big challenges are ahead for the forensics investigator to identify such kind of communications in e-mails. But upcoming technology trends opens up more challenges, and Terrorists no need to use e-mails also in future. Terrorists can create a shared document in any of the available free spaces and often they can communicate with each other. Government as well as forensics experts should keep an eye on these kinds of challenges. The solution for above type of cases is combining disk forensics with e-mail forensics. Network forensics expert unable to identify any kind of communication between source and target, but disk forensics expert can identify evidence traces.

3.2 Tasks to avoid misleading of forensics process

For e-mail forensics the following tasks can be performed to avoid misleading that are created by cyber criminals.

1. Investigate the cyber crime that was happened through e-mails
2. Based on the possiblity, reconstruct the crime scence
3. There are some traces that are left by criminal, collect and analyze such evidences
4. E-mail altercations may be done manually, or sometimes automatically; so forensics investigator identifies, classifies, and quantifies the entire process
5. Finally, establish linkages, associations and reconstructions and use those finding in the court of law.

4. PROPOSAL METHODOLOGY FOR COMBATING AGAINST ANTI-FORENSICS

E-mail forensics involves identification and analyze of data from e-mail servers, suspect's machines and from other sources. Both client and server responsible for handling e-mail forensics. Server is responsible for moving of messages and client is responsible for storing and delivering of messages. E-mail headers are included with trace information that contains special control data related to delivery status, message notifications etc. Sridhar et al. [13] gave inverted pyramid approach for e-mail forensics which is a combination of three different tools. These tools are related to e-mail header analysis, stylometry and timestamp analysis.

This section discusses about protection from anti-forensics techniques in such way that inverted pyramid approach can be used as strong evidence in the court of law. Anti-forensics can be used to exploit weaknesses in the forensic process or tools, so that forensics tool developers can come up with new tools which strengthen the forensics investigation process.

Cyber criminals can use any of the anti-forensics techniques to manipulate the evidence. There are several categories doing such things like destroying e-mail evidence, hiding evidence, altering evidence sources, and forging evidence. Anti-forensics strives to minimize the "footprint", or data that the attacker has left behind. Figure 2 shows the categories of anti-forensics that can be applied to e-mail forensics. This section deals with all these categories in detail.

One of the simplest ways of achieving anti-forensics is usage of touch command. This simple command alter the timestamp information for a file, so that once every file is touched that mislead investigation process. Some of other tools that support anti-forensics are metasploit, timestomp, and slacker. Metasploit [14] is a framework with bundle of tools; timestomp allows modifying all timestamp values including modified time, accessed time and even created time. Slacker is such a dangerous tool that allows hiding files within the slack space. In general deleted file information is extracted with the help of slack space, but slacker even misguides the investigator.

Destroying
Hiding
Altering
Forging

Fig 2: Anti-Forensics applied for e-mails

Generally digital evidence can be found on hard drives which consist of volatile and nonvolatile data. Volatile data disappear when the power off, hence forensics investigator must take care while taking evidence and they need to apply live forensics. Collecting non-volatile data is easy because it is stored and preserved in the hard drives may be found in either files created by the user like file attachments in e-mails; or files created by the computer like log files that stores every transaction. Tools like recent file viewer combined with log file analyzer helpful for forensics investigator to identify attached files during e-mail transactions.

4.1 Destroying E-mail Evidence

In a general scenario, e-mail evidence can be easily deleted by the cyber criminals after completion of their attack. Destroying means make e-mail evidence as unusable or dismantle it. Every destruction operation also leaves some traces which can be used as additional evidence trail. Simply deletion may not be sufficient but by using anti-forensics techniques, criminals can destroy e-mail evidence. Even these e-mails are available from the company mail servers, where criminals have less access on those servers. Sometimes Government uses these stored e-mails to provide strong evidence towards protecting clients.

Proposed Methodology to combat destroying e-mail evidence

Jie Zheng [15] gave complete discussion related to e-mail evidence by elaborating with different case studies like United States of America v Microsoft Corporation. There is a phenomenon 'every criminal leaves a trace' which can be applicable for cyber criminals too. So job of cyber forensics investigator is finding those traces. File Carving is a technique that searches evidence from file fragments based on a specific set of parameters. Destroyed e-mails stored somewhere in the hard disk, that can be traced out with help of these carving techniques.

This process requires using tools such that they display PC on/off times like shown in the following figure 3. With such information one can create some alibi kind of thing that can be useful in court of law.

4.2 Hiding Evidence

Modern day criminal has access to a variety of tools for concealing information besides encryption like passwords, digital compression, steganography, remote storage, audit disabling. In e-mail forensics, hiding evidence is related to hiding e-mail itself and also hiding e-mail header.

Proposed Methodology to combat against hiding evidence

Hiding e-mail evidence means that removing evidence from investigator's view. It uses exploiting mechanisms of digital world. Presence of hiding tools in the system can be treated as one of the evidences in the court of law, so careful observation of such tools is important. Nowadays cyber criminals are using fake mails for sending threatening e-mails that challenges forensics investigator to find such criminals. Even fake mails leaves some traces including routing of packets, stylometry gives write print profiles of e-mails etc.

4.3 Altering Evidence Sources

Sometimes e-mail evidence sources can be altered by cyber criminals resulted to integrity issues. Evidence integrity deals with preservation of evidence in its original form. Forensics Investigator collects evidence from suspect's machine using tools like encase, helix etc.

Proposed Methodology to combat against altering evidence

Investigator need to take care about the evidence such that evidence cannot be altered in any form. There are certain methods and tools available that ensures evidence not altered either willingly or accidently. A decade back Chet Hosmer [16] gave several methods for finding integrity of digital evidence like Checksum, Hash algorithms and digital signatures; those can be applicable for current trends also. There is a need of proper care for hashing because some of recent studies showing chance of having same hash value.

Some of the example tools are Write Blocker and hashing techniques. Write Blocker protects evidential information while collecting evidence and Hashing techniques ensures the evidence integrity.

4.4 Forging E-mail Evidence

Forging/counterfeiting e-mail evidence is simply creation of a faked version of evidence. One of the drawbacks with e-mail is that it can be forged easily. Simple techniques exploited by spammers are adding false headers to the email, or altering existing headers to include false information to confuse the true source. E-mail senders with criminal intent can hide their identities by forging sender's address. Tracing of forged e-mails is a big challenge for cyber forensics investigator. Even there are 'N' number of tools for generating forged mails, there are 'N+1' number of forensics tools available for detecting such forged mails easily.

Proposed Methodology to combat forging e-mail evidence

Sridhar et al. [13] discussed about stylometry analysis. Stylometry deals with study of writing styles of an author, which helps authorship attribution. Stylometric techniques can identify whether a particular e-mail was written by same author or different author.

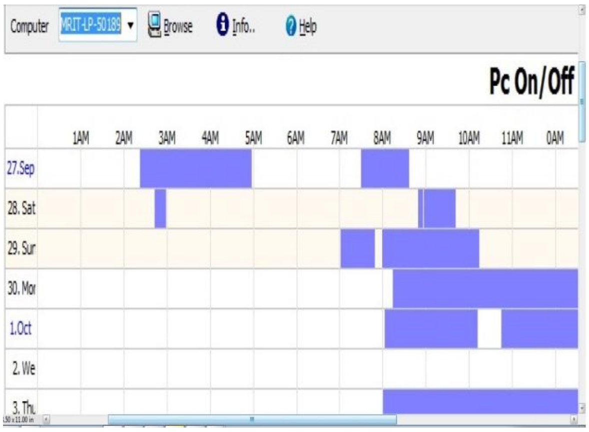

Figure 3: PC on/off times

Even this approach provides approximation of an author, with the help of other cyber forensics tools one can decide the originator of the e-mail. Forging of e-mail evidence can be detected with the help of stylometric analysis to prove the accurate author of suspected mail in the court of law.

5. CONCLUSION

This paper discussed about the process of combating against anti-forensics related to e-mails. This paper addressed forensics methodology of e-mail forensics and elaborated various categories of anti-forensics applied on e-mail forensics. Proposal methodology discussed for each category of anti-forensics applied on e-mail forensics. Cyber criminals using anti-forensics tools as their weapons, hence forensic investigator needs to find anti-forensics that are available in the system while recording evidential information.

6. REFERENCES

[1] Rogers, M. (2006). CERIAS 2006-7th Annual Information Security Symposium, http://www.cerias.purdue.edu/news_and_events/events/symposium/2006/materials/pdfs/antiforensics.pdf, accessed on 12th July, 2013

[2] Ryan Harris, Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem, Digital Investigation 3 (2006), Digital Forensics Research Workshop

[3] Kessler, G. (2007). Anti-Forensics and the Digital Investigator, Proceedings of the 5th Australian Digital Forensics Conference, December 2007

[4] Paula Thomas and A. Morris, "An investigation into the development of an anti-forensic tool to obscure USB flash drive device information on a windows XP platform," in Digital Forensics and Incident Analysis, 2008. WDFIA'08. Third International Annual Workshop on, 2008, pp. 60-66.

[5] Glenn S. Dardick, Claire R. La Roche, Mary A. Flanigan, Blogs: Anti-Forensics And Counter Anti-Forensics, Proceedings of the 5th Australian Digital Forensics Conference, December 2007

[6] Sridhar N, Lalitha Bhaskari D, Avadhani PS, Plethora of Cyber Forensics, International Journal of Advanced Computer Science and Applications, Vol. 2, No. 11, 2011

[7] Allessandro Distefano, Gianluigi Me, Francesco Pace, Android anti-forensics through a local paradigm, Digital Investigation 7 (2010), Digital Forensic Research Workshop

[8] Ioana Sporea, Benjamin Aziz & Zak McIntyre, On the Availability of Anti-Forensic Tools for smart phones, International Journal of Security (IJS), Volume (6) : Issue (4) : 2012, Page 58-64

[9] Haodong Li, Weiqi Luo, Jiwu Huang, "Countering Anti-JPEG Compression Forensics", IEEE International Conference on Image Processing (ICIP), pp.241-244, Sept. 30 - Oct. 3, 2012

[10] David Cowen, Matthew Seyer, File system journaling forensics theory, procedures and analysis impacts, SANS Digital Forensics and Incident Response Summit 2013,

[11] M.Tariq Banday, Techniques And Tools For Forensic Investigation Of E-Mail, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011

[12] http://articles.timesofindia.indiatimes.com/2013-09-19/hyderabad/42217231_1_tahseen-akhtar-waqas-yasin-bhatkal, accessed on 19th September, 2013.

[13] Sridhar N, Lalitha Bhaskari D,Avadhani PS, Inverted Pyramid Approach for E-Mail forensics using heterogeneous forensics tools, CSI Communications, July2013

[14] Metasploit LLC. (2013). Metasploit Anti-forensics, http://www.metasploit. com/, accessed on 12th July, 2013

[15] Jie Zheng, E-mail Evidence Preservation: “How to Balance the Obligation and the High cost”, Lex Electronica, Vol 14 n 2, fall 2009, page 10,

[16] Chet Hosmer, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence Spring 2002 Volume 1, Issue 1

AUTHORS PROFILE

Mr. Sridhar Neralla is a research scholar in the Department of Computer Science and Systems Engineering of Andhra University, under the supervision of Prof.P.S.Avadhani and Dr.D.Lalitha Bhaskari. He received his M.Tech (IT) from Andhra University and presently working as Associate Professor in IT Department of GMRIT. He is a Life Member of CSI and ISTE. He has coauthored 4 books. His research areas include Network Security, Cryptography, Multimedia, Cyber Forensics and Web Security.

Dr. D. Lalitha Bhaskari is an Associate Professor in the Department of Computer Science and Systems Engineering of Andhra University. She is guiding more than 8 Ph. D Scholars from various institutes. Her areas of interest include Theory of computation, Data Security, Image Processing, Data communications, Pattern Recognition. She is a Life Member of CSI and CRSI. She holds prestigious responsibilities like Associate Member in the Institute of Engineers, Associate Member in the Pentagram Research Foundation, Hyderabad, India. She also received young engineer award from Institute of Engineers (India) in the year 2008.

Dr. P. S. Avadhani is a Professor in the Department of Computer Science and Systems Engineering and Vice Principal of AU College of Engineering, Andhra University. He has guided 10 Ph.D students and right now he is guiding 12 Ph.D scholars. He has guided more than 100 M.Tech projects. He received many honors like best researcher award and best academician award from Andhra University, chapter patron award from CSI for CSI-Visakhapatnam Chapter and he has been the member for many expert committees, member of Board of Studies for various universities, Resource person for various organizations. He has coauthored 4 books. He is a Life Member in CSI, AMTI, ISIAM, ISTE, YHAI and in the International Society on Education Technology.