A Detection Based on Anti-Forensics wiping technique

by
Anusha S.P
Cyber Forensics and Information Security ER & DCI institute of Technology, Trivandrum

Abstract: **There are various anti-forensics wiping tools available in the market place which aims to forestall the forensics investigation. Forensic examiners and legal professionals must stay alert of new technologies while adhering to sound practices required satisfying evidentiary requirements in court. These anti-forensics wiping tools wipe's the evidence entirely by overwriting the data making it a concern for the computer forensics examiners. Current defensive analysis of anti-forensics malware often requires step by step manual inspection. The main aim of this paper is to provide a framework for the detection of anti-forensics wiping tools based on signatures and provides a detailed audit report of its findings through registry and file system analysis. The various Windows 8 compatible anti-forensic software products can be selected whose advertised features include the ability for users to wipe targeted files, folders, or evidence of selected activities.**

I.INTRODUCTION

A widely accepted definition of anti-forensics "Attempts to negatively affect the existence, amount and/or quality of evidence from a crime scene, or make the analysis and examination of evidence difficult or impossible to conduct. The rationale behind anti-forensics is to stop investigators finding the perpetrator or the act by contaminating the evidence. One area of particular concern for computer forensics examiners involves situations in which someone utilized software applications to destroy evidence. There are products available in the market place that are relatively inexpensive and advertised as being able to destroy targeted portions of data stored within a computer system. These anti-forensics tools have been used to eliminate evidence in criminal and civil legal proceedings and represent an area of continuing concern for forensic investigators. The main purpose of anti-forensics is to hide or distract from what is happening. The goals of anti-forensics are: Avoid Detection, Corrupt the information collection process or to make it look as if it's corrupted, Lead to false data, Increase the time of investigation, Disable detection tools, Destroy the valuable evidence, destroy the confidence in gathered evidence.

II.ANTI-FORENSICS

Anti-forensics is newly identified as a valid field of study. The main goal of anti-forensics is to irritate and discourage forensics examiners through its techniques and tools. Anti-forensics is a term that includes any activity or methodology whose goal is moderate the consequences of a computer forensics examiner. It can be as easy as modifying the name of the file to create it appear innocent to the examiners or as difficult as developing a root kit application which provides forensic software with instantaneous images just without specific data. In the past six to nine years the field of anti-forensics has raised in both popularity and scope. Christo Ananth et al. [4] discussed about Reconstruction of Objects with VSN. By this object reconstruction with feature distribution scheme, efficient processing has to be done on the images received from nodes to reconstruct the image and respond to user query. Object matching methods form the foundation of many state- of-the-art algorithms. Therefore, this feature distribution scheme can be directly applied to several state-of-the-art matching methods with little or no adaptation. The future challenge lies in mapping state-of-the-art matching and reconstruction methods to such a distributed framework. The reconstructed scenes can be converted into a video file format to be displayed as a video, when the user submits the query. This work can be brought into real time by implementing the code on the server side/mobile phone and communicate with several nodes to collect images/objects. This work can be tested in real time with user query results. Its growth is mainly because of the increase in popularity of computer forensics. Computer forensic investigators have turned out to be more preplanned and technical as computer crime has become more typical and sophisticated. Career development and training for the forensic examiners have been guaranteed.

- Attack on tools: to produce fake examination results, weaknesses in existing computer forensics tools are broken.
- Attack on analyst: problems are created for the investigator by producing a vast amount of information or throwing tough doubt on the validity of his or her effort.

III.ANTI-FORENSICS TECHNIQUES

The various AF methods are discussed below in more detail.

A. Data hiding

Data hiding refers to the practice of storing data where it is unlikely to be found, or employing the method of security through obscurity. Simple methods such as extension renaming or signature editing exist, but these are generally easily identified by most current forensic software. One of the simplest and most effective methods of data hiding is Steganography. Data hiding is, perhaps one of the oldest methods around. There are multiple ways of hiding data which ensure that data is undetectable while it is still present on the device. One way of hiding data is relocation of data. Target data is stored at a location, of which user is sure will not be examined by the investigator. Another way relocating data is to transfer data to any other portable storage device, and the wiping it off from the computer. Second way is making data "invisible". Data is made to be "invisible", concealing the fact that the hidden data still exists. It can be achieved by either steganography or streaming. Steganography is a technique where information or files are hidden in another files

B. Data destruction/Artifact wiping

The destruction of data by wiping of files is a commonly used AF method which has been used for a long time. Artifact wiping is used to attempt data sanitization, where data sanitization is the process of deliberately, and irreversibly removing or destroying the data stored on memory. It can be achieved in any of the following ways. It may seem that permanently

further benefited by the fact that all the forensic tools and procedures are well documented and well known. Hence, their vulnerabilities can be easily determined if an attacker can access the tool or possess knowledge about the working of that tool Attackers exploit vulnerability of the tools relating to validation of data and use those bugs to launch buffer overflow attack and running arbitrary code which could damage the functioning of CFT. Denial of service (DoS) attack: Aim of any DoS attack is to attack on availability. In anti-forensic context DoS attack targets particular resources used by CFT. These resources are determined by the way they are used. Any CFT resource Zipped file bomb.zip which is actually a compression bomb is listed in evidence tree.

by other files. Aware of this fact, tools have been developed which delete or wipe off the files and their traces. Various open source tools such as BC Wipe, Eraser, PGP Wipe are available for the purpose of data sanitization, and wiping slack and unallocated spaces. These tools destroy data files by using repeated overwrites which makes their retrieval very difficult. Artifact wiping is preferred as it is less time consuming and efficient, yet there are certain limitations to it. Some data wiping tasks are very difficult to achieve, for example erasing file data that is wholly contained in the master file table.

IV.ANTIFORENSICS RISKS

Anti-forensic techniques have a high potential to "frustrate forensic tools". Traditionally, they consisted of the application of steganography or cryptography to conceal evidence or make it harder to access. Another old and popular anti-forensic technique is simply the overwriting of data. But newer techniques exist, such as the avoidance of compromising evidence using, e.g., live CDs, virtual machines or software that resides only in memory and never on disc. Anti-forensic techniques are actions whose goal is to prevent proper forensic investigation process or make it much harder. These actions are aimed at reducing quantity and quality of digital evidence. These are deliberate actions of computer users, but also developers who write programs secured prior to methods of computer forensics. For the anti-forensic techniques, we can include activities such as e.g. intentional deletion of data by overwrite them with new data or protection tools against forensics analysis. Anti-forensic techniques can be used to increase security, for example, erasing and overwriting data, so that they cannot be read by unauthorized persons. These techniques can however be misused by perpetrators of computer crimes in order to protect against discovery of their actions. Users of anti-forensic tools can also become computer users who want to remove evidence of their criminal activity, such as hackers, terrorists, pedophiles, counterfeiters. Anti-forensic tools can be used by dishonest employees, who will be using it to destroy any data indicating that they could steal value company data, gaining unauthorized access to computer system or capture secure information and passwords.

A. Trail obfuscation

Trail obfuscation follows three basic methods. The first has the aim of obscuring required information from the would-be investigator. This is achieved by either replacing relevant information with false information (such as IP address spoofing) or using third parties to act as proxies of the source data in order to remove all traces of the origin of the data from the transmission at the destination (such as mail anonymizing services). The second form of obfuscation involves altering the data associated with forensic artifacts by altering metadata such as date and time stamps. Finally, trail obfuscation can also take the form of log deletion or modification in order to hide log entries that would identify the identity or action of the perpetrator. This technique is more popularly known as "counterfeiting". The trail obfuscation or evidence counterfeiting techniques are practiced with purpose of confusing and disorientate the investigation. This could be achieved in a number of ways. One way to counterfeit evidences is Defragmentation. This technique uses the concept of artifact wiping with the aim of confusing investigation. Defragmentation is carried out to reorganize and rearrange the hard drive so that all the files with all parts are stored in contiguous space. This process involves rewriting and erasing of files all over the disk. This causes disruption to data in allocated spaces which is likely to destroy any evidential remains written in those locations. Hence, defragmentation doesn't delete files unlike artifact wiping but attempts to confuse the investigation by destroying any residual data that may be present.

V.ARTEFACT WIPING

One area of particular concern for computer forensics examiners involves situations in which someone utilized software applications to destroy evidence. There are products available in the marketplace that are relatively inexpensive and advertised as being able to destroy targeted portions of data stored within a computer system one of the most difficult challenges facing computer forensics examiners concerns identifying evidence from digital data in situations where someone has deliberately attempted to destroy information. This challenge is compounded by conflicting perspectives, as individuals that hire computer forensics examiners seem to anticipate that professionals within this field are able to retrieve all relevant evidence, individuals that wipe data do so with the intent that their techniques are sufficiently elaborate enough to prevent information from being recovered, and forensic examiners may be driven by professional pride and the satisfaction of performing their craft well in order to uncover evidence wiped by sophisticated methods. These conflicting goals between those that attempt to hide evidence and those that seek to submit recovered evidence within the legal system increase the levels of risk and uncertainty facing computer forensics examiners in situations where attempts to destroy data have occurred.

These commercial tools claim to expunge all traces of information about specific computer Usage, including documents and other files created records of websites visited, images viewed and files downloaded. To do this, counter-forensic tools must locate activity records scattered across the file system and erase them irretrievably, while leaving the rest of the operating system intact. The technical challenge of finding and eliminating this data is far from trivial, given the complexity of modern computer operating systems, which are designed to preserve data rather than shed it. Yet published rigorous evaluations of the counter-forensic tools are limited. Commercial counter-forensic tools' intended functionality may be broken down into two main are

•Locating relevant activity records on the system. This entails comprehensive, built-in knowledge of the data-handling behavior of the operating system and installed applications.

•Eradicating targeted data to thwart its recovery with standard forensic techniques. This typically entails overwriting the occupied data sectors on a disk with arbitrary values.

Failures in either functional area can lead to the disclosure of data that the tool's user sought to eliminate. Of the two areas, the second data-wiping has been more closely examined by researchers. Most of the anti-forensics tools left distinctive signatures of their activity that could be used to postulate the tool's use even if no evidence of the software's installation was recovered. (This might occur, for example, if a tool installed on a separate partition or physical disk is used to delete data on another.) The patterns they created in the file system records would not be expected to occur during typical computer activity. The most common distinguishing pattern created by the tools was their technique for mangling metadata about files they wiped. In particular, all the tools that renamed the files they sought to wipe adopted differing strategies for generating new file names. Most of the counter forensic packages offered to rename wiped files (and often alter other data, such as file size and creation date) in order to minimize the information that can be gleaned by examining the metadata for deleted files.

The Fig 1 shows the input as the image of the partition or disk. Identification of the anti-forensics tool will be based on signature based analysis. A signature library is employed to automate the hunt for traces of counter-forensic tool use. Analysis of the new Windows 8 registry hive, named Amcache.hve, can found the evidence about anti-forensics tools that were used. This registry hive showed anti-forensic tools even after they had been installed and executed. The stronger the evidence, the more "weight" it will likely be given. If evidence can help prove the anti-forensics tool was actually executed, and executed at a certain time, it will likely be given more "weight" compared to merely showing that anti-forensic tools were on the defendant's computer. Artifacts persisted for all of the anti-forensic applications in several locations, including the Amcache.hve, Application compatibility cache, prefetch files, Jump lists and USN journal.

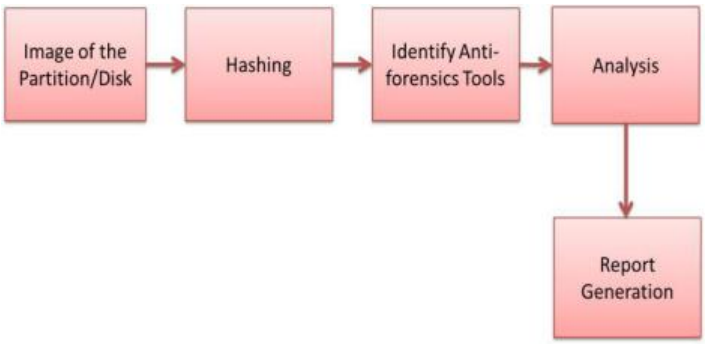

Fig 1:Block Diagram for the detection of anti-forensics wiping tool

VI.CONCLUSION

With each passing day counter forensic tools are becoming stronger. The fact that encourages their use is that these tools are openly available and easier to use. They are further benefitted by standard methods used by forensic tools and their being well documented which makes it more convenient to either get away from them or causing disturbance in their own working. Most commercial counter-forensic tools leave potentially useful data still their ability to destroy data can also present a significant obstacle to analysts. Digital investigators are encountering the use of anti-forensic tools and techniques. Although it is difficult to determine the extent of the problem, investigators do see a need for better detection when such techniques are used on systems under investigation. By focusing on anti-forensic action trace detection, such a method can quickly give an investigator more information about suspect systems. The proposed framework helps the investigator with a better detection when anti-forensic tools have been used. This framework can quickly give an investigator more information about the suspect system. This can help to ensure investigators are better informed about the state of the suspect device rather than forcing them to rely on their intuition

VII. REFERENCES

.

[1.] Anu jain,Gurpal singh chabra,"Anti-forensics Techniques: An Analytical Review",2014

[2.] Jason Nikolai, Yong Wang,"A Framework for Examining the Human Side of Anti-Forensic Measures",2014

[3.] Martin wondram,Felix c.freiling,christian moch,"Anti-forensics:The next step in Digital forensics tool testing", international journal of research in computer science,2013

[4.] Christo Ananth, M.Priscilla, B.Nandhini, S.Manju, S.Shafiqa Shalaysha, "Reconstruction of Objects with VSN", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Vol. 1, Issue 1, April 2015, pp:17-20

[5.] Amit Rosner, Buky Carmeli, Gabi Kedma," Noninvasive Detection of Anti-Forensic Malware",2011

[6.] Srilakshmi Erasani,"Implementation of Anti-Forensic Mechanisms and Testing with Forensic Methods",2011

[7.] Ryan Harris,"Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem",2011

[8.] Mathew Geiger,"counter forensic tools: Analysis and Data Recovery",2011

[9.] Karthikeyan Shanmugam,"Validating forensic evidence an anti-forensic approach",2010

[10.] Przemyslaw Pajek and Elias Pimenidis," Computer Anti-forensics Methods and Their Impact on Computer Forensic Investigation",2009

[11.] Ryan Harris,"Arriving at anti-forensics consensus: examining how to define and control the anti-forensics problem",2006