International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.6, No.5, May 2017 DOI:10.15693/ijaist/2017.v6i5.23-27

Counter Forensics: An Analysis Report

[1]Ms. Bhakti Prabhakar, [2]Mr. Neelesh Jain
[1]M.Tech Scholar,[2] Assistant Professor/Department of CSE
Jaypee University, Guna, India
[1]prabhakarbhakti@gmail.com, [2]neelesh.jain@juet.ac.in

ABSTRACT:

Where *Computer Forensics or Digital Forensics is used for collecting, evaluating and analyzing information from the evidences for legal purposes, there is a possibility of the information being tampered or the evidence being mislead by the criminals. This being known as Anti-forensics (also been referred as Counter-forensics) is a threat to current digital forensic techniques and hold a malicious intention towards the collected evidence. This review paper illustrates the comparison between various Anti-forensic tools and techniques that have been used for detection and recovery of the influenced data. It also analyses the results of the tests conducted on various commercial anti-forensic tools in detail. It also detects and identifies the related software bugs and issues that arise in digital forensic tools and its vulnerabilities to anti-forensic hacks and improper use.*

Index terms— Computer Forensics, Anti-forensics, Anti-forensic tools, Anti-forensic hacks

I. INTRODUCTION

A. Computer Forensics

Computer forensics may be a new discipline that uses "scientific data for aggregation, analyzing and then presenting proof to the courts". [1] Computer forensics is an area of work in which Computer forensic tools (CFTs) are used to provide support to forensic investigators by collecting data from a system that is listed as evidence; forming a real and permanent copy of that evidential data, so that it can be used as an important evidence in some legal proceeding; performing information analysis to reveal information that may not be clear as crystal at that instant. CFTs can be distinguished using two categories. Persistent knowledge tools analyze knowledge that's hold on which remains once a system is turned off. Volatile knowledge tools analyze info that's transient and would be lost if not captured, like the contents of a computer's memory or the flow of packets as they thwartwise a network. [2]

B. Anti-Forensics

"Anti-Forensics (AF)" could be a growing assortment of tools and techniques that frustrate rhetorical tools, investigations and investigators. [2]

The goals of Anti-forensics include:

1. Stating a point of doubt on the forensic evidence report or testimony
2. Subverting a forensic tool and then using to attack the forensic investigator or corporation
3. Leaving no appropriate evidence of the existence of the Anti-forensic tool or proof of it being used illegally.
4. Avoiding detection of evidence from the forensic examiner
5. Compelling a hidden tool to reveal its presence
6. Intrusions leading to increase in the investigation time
7. Disruption of the information to be retrieved from the evidence

II. TECHNIQUES USED IN ANTI-FORENSICS

The various anti forensic techniques used to frustrate the examiner contain Traditional Anti-forensics which contains most commonly used anti-forensic methodology to tamper with essential data. It specifically contains Overwriting of data. Overwriting of data involves replacing the original data with false information and trying to prove it to be true. For overwriting any sort of data, the previous data has to be securely deleted so that any of the forensic techniques would not be able to recover it. If the examiner has any information about the use of operating system by the attacker, he can access the timeline of the usage by the attacker so, the attacker very smartly hides the record of the timeline of the system access by overwriting the metadata and hence the examiner is not able to trace the attacker's activities on the system.

Overwriting can take place in following three different modes:

a. Complete media files can be overwritten by the program.
b. An attempt of overwriting the individual files can be done by the program.
c. An attempt to overwrite previously "deleted" but left on the drive files can be done by the program.

Programs generally try this by making one or additional files on the media so writing to those files till no area remains, taking special measures to erase tiny files – as an example, files that exist entirely inside the Windows Master File Table of the NTFS partition. [3] Another way of overwriting data is by preventing data creation that is, if the data that was not present in the database in reality, it cannot be created. Examples include: Disk Sanitizers, Microsoft Word Metadata "Washers" and Timestamp eliminators.

Other counter-forensic approaches contain Cryptography and Steganography. It involves the use of data in the form of encrypted data where the data is encrypted by the cryptography transparently while it is being written to the disk and the data is decrypted when it is read back, converting the data to opaque data for anyone views it. Protocols for encryption of network are also used in anti-forensics. Encryption of the network can be done to prevent the analysis of the content on forensic terms. Only the traffic matter can be secured by SSL and SSH, which are defined protocols for encapsulation using cryptography. Another approach that makes good use of both the protocols is Onion routing. It uses the combination of SSL and SSH with stack of encrypted layers. Protection measures taken against debugging and reverse engineering by attackers are referred to as program packers. Packers such as PECompact [4] and Burneye [5] will take a second program, contract and/or cipher it, envelop it with the most appropriate extractor.

The process of embedding encrypted form of data in a wrapper text to avoid detection is known as Steganography. Steghide embeds text in wrapped JPEG, MBP, MP3, WAV and AU format of files. It can also be referred as the hiding of the Dark data within the Light data so that the Dark data cannot be traced by the forensic examiner. Generic data hiding involves the kind of data that is hidden or unallocated or found at out of reach locations that's neglected by the current generation of forensics. Metasploit's layout can hide knowledge in the slack area of FAT or NTFS classification system. FragFS hides knowledge inside the NTFS computer file table. RuneFS stores knowledge in unhealthy blocks. WaffenFS stores file in the ext3 journal file. KYFS stores information in within directories. MuleFS stores information in an exceedingly reserved area.

There are also various anti-forensic methods that are used by the attackers to erase their footprints. One of them is Live compact discs, which is a software system arrangement that executes and boots functionality solely from a scanned read only device. A Windows system, an internet browser and a SSH clients are a part of Live compact discs. A disabled virtual memory is used to execute it. Another one is Bootable USB tokens, which are quite similar to live compact discs. In these tokens, the operating systems are placed inside an attachable USB device. Virtualization programs such as, VMWare Player, Parallels or Microsoft Virtual PC are used for executing and implementing a Virtual Machine ware "client" operating system. Various online sources and web storage services have been found to be used for false means and websites such as, Yahoo, Hotmail and Gmail can be utilized by the attacker for the storage of attack tools without any risk of being caught. Using a Buffer Overflow exploit, an intruder can perform injection and code execution in the address space of an executing program behavior of the victim. The "Userland Execve" method permits the programs on the system of the attacked to be accessed and run while not the implementation of the operating system execve() kernel decision, so that the intruder could skip the kernel based security systems that may stop the intruder's access **to execve() or log its use to a secure work service.** System call Proxying is implemented when the attacker uploads the System call Proxy that accepts remote procedure calls from the intruder's laptop or system, the asked system instruction for call is then run on the victim's system and the expected output is sent back to the intruder. System call Proxying is enforced by Impact, a commercialized market level penetration tool oversubscribed by the defined Core Security Technologies.

Several Anti-forensic tools are used by attackers for exploitation of CFT bugs. In case of failure for validation of data in other programs, those CFTs can be subverted that do not properly validate their input data. CFT resources such as CPU, memory, etc. are subject to the DOS attacks. One of the substantial example of DOS attacks is the Compression Bombs, which are small data files, which when are uncompressed, is responsible for high consumption of storage. Those attackers, who could trace out the heuristics used by a CFT for recognizing files, can exploit them easily. The Transmogrify program of the Metasploit Project is capable of converting a text file .txt to an executable file .exe and adding the letters "MZ" to the starting of the file. Now, the EnCase which classifies the Windows file as executable if it has the extension as .exe and includes the initial two letters as MZ in the name of the file, will think of the file as a binary file and not scan it.

Many Anti-forensic techniques are commonly used for detecting CFTs. Self-monitoring, Analysis and Reporting Technology (SMART) manufactured inbuilt in most of the hard drives in present time computes the whole range of power cycles (Power_Cycle_Count), the whole range of power cycles the disc drive has been utilized (Power_On_Time or Power_On_Minutes), a exponent worth of what proportion high temperatures the drives have and different manufacturer-determined parameters. AFTs can use SMART counters for detection of attempts at rhetorical analysis and modify their behavior consequently. As an example, a dramatic increase in Power_On_Minutes would indicate that the disc drive has been imaged. [6] The detection in context to forensics in networks field can be done by Host Detection in "Promiscuous" mode**.** Along with the packets which are addressed to the host, the packets on the Local area network

are also captured by the interface, which is stated to be in the Promiscuous mode detection of monitoring systems configured in a wrong manner can be exposed by the approach that they reply to varied forms of unshapely IP packets. [7] There is also a way in which monitoring detection is performed with the assistance of DNS. Network monitoring can also be detected when an attacker sends packets through a network that have Ethernet and IP address as their destination, which is present on the Subnet however not in use presently, and a supply address that's from a rarely used network. This technique will work if there's a flaw within the CFT, or just if the CFT is employed improperly.

Several of the anti-forensic techniques is overcome through improved observation systems or by correction of the bugs in the current generations of computer forensic tools. Some of the points which can be covered are mentioned as follows:

a. Overwriting tools get irritated by the positioning of the information in order that the intruder doesn't obtain the power to write it.
b. Heuristics of various weak file identification processes may be switched with stronger ones**.**
c. Compression bombs may possibly be overcome with a lot of sensible and useful decompression libraries. [2]

III. WORKING OF COUNTER-FORENSIC TOOLS

The working of Counter forensic tools can be divided into two primary fields:

a. Tracing required records of working and activity on the system. This involves detailed and complete knowledge about the data handling nature of the applications installed and the operating system in use.
b. Erasing information that is targeted to prevent its recovery using primary form of forensic techniques. This involves overwriting of the data with some arbitrary data.

The main platform that was used for testing here was Forensic Tool Kit (FTK) version 1.50a to 1.51 from AccessData. On analysis of results, it was found that all the counter forensic tools were unable to remove one or the other potentially sensitive data from the system. Counter forensic tools claim to expunge all traces of information about specific computer usage, including documents and other files related, records of websites visited, images viewed and files downloaded. Given the complexity of modern operating system, which is designed to preserve data rather than shed it makes it difficult for the data to be found and eliminated. Here are mentioned a few commercial counter forensic tools which were tested within two rounds of testing. These tests were performed to evaluate the tools abilities to purge a range of activity records and other data representative of real world computer use. Software such as: Acronis Privacy Expert8, Absolute Shield 3.42, Cyber Scrub Privacy Suite 4, Evidence Blaster 2005, Evidence Eliminator 5.058 b14, History Kill 2005, Privacy Eraser Pro 5.0, Privacy Guardian 4.0, Secure Clean 4, Tracks Cleaner 3.0, Window Washer 6 were tested for determining how safe is our browsing and file access and the results were analyzed on the basis of Wiping failures occurred for free space, targeted files, registry records missed, activity files missed and data recoverable from file system structures.

All tools except five tools provided an option to wipe the unallocated space, which may include all kinds of user deleted file space, disk areas unused listed in file system index. One or the other records were difficult to delete using these counter forensic tools, some of this disclosure of data resulting from the effort of overwriting the deletion of targeted files. Thus, targeted file user space could not be erased and system files failure occurred. As it was noted that the updated versions of the currently use counter forensics tools were more over gave improved performance in removing records of activity from the Registry. Small data such as, text files, smaller .gif images are the different file system structures from which the data was to be recovered. Cookies from browser, etc, were easily recovered by using NTFS Master File Table (MFT). Even tiny and larger fragments were easily recovered by the same. [8]

IV. IDENTIFICATION OF BUGS IN DIGITAL FORENSIC TOOLS

Any program or code might have bugs and they are removed through upgrade of software, hence starting of applications used and operating system again. Below mentioned notifies the detected software bugs in major branded digital forensic tools and how to improve them to remove such issues.

A software bug is a weakness in a computer program either by code or design that produces an incorrect or unexpected result, or causes it to behave in an unintended ways. [2] The research question regards the value of these vulnerabilities for anti-forensic hacks or implications for the preservation and presentation of evidence. [9] Fuzzing is the process of providing intentionally invalid data to an application in an attempt to trigger an error or fault condition of some kind. This kind of activity can be classified as anti-forensic as the consequences can block evidence, counterfeit evidence, confound investigation, frustrate processes and confuse analysis. Fuzzing was performed on a number of file formats such as JPEG images and PDF documents with the goal of detecting problems with the built in file viewers in the forensic tools. Fuzzing was also performed on file system structures in an attempt to reveal issues with the methods used by forensic tools to interpret file systems. [10]

A second technique used was manual targeted manipulation of data formats. Targeted manipulation is the process of modifying specific portions of a data structure guided with detailed knowledge about the data structure. Two data structures were targeted for testing; individual files and file

system structures. Individual files were targeted in an attempt to again locate issues with a tool built in file viewer. File systems and entire disk images were also targeted in an attempt to locate issues with the techniques used to analyze file systems. [11]

Digital forensic investigators typically rely on one or two tools to conduct their investigation. The reliance on the small number of tools is because of costs, user confidence and the requirement in the community to have standardized tools that can be tested and confirmed to produce reliable results. [12] Tool risk types fall into three categories: failure to validate data, denial of service attacks and fragile heuristics. [13] One of the main reasons for the existence of software bugs in digital forensic tools is that digital forensic tools must be able to acquire data from multiple types of device and then analyze, search and display thousands of different data formats. [14]

Tool related risks can be mitigated through two main approaches; firstly the use of multiple tools and secondly the production of better tools. The use of multiple tools is a simple solution however the cost in time and money of purchasing tools, training and performing the same work twice prohibits many investigators from being able to use multiple tools. [11] The heuristic systems behind processes like file signature analysis can be improved by looking beyond the header and footer of a file structures within the file in order to identify its type. [15]

When a specific digital forensic tool was tested as an illustration of what maybe expected when testing digital forensic tools. The outcome shows that the tool performs inconsistently and across the different tools different performances were found. In the performed tests, two tests exceeded expectations and four were unacceptable on the adopted acceptance spectrum. Principally a dominant set of occurrences showed no issues but disturbingly a greater number of occurrences reported problems for the uninterrupted use of the tools. These included a higher number of crashes indicating that abstract complexities that cannot be resolved by the software. In addition, buffer over-runs were found in large files and a number of unexplained exits from analysis were noted. When challenged by the malformed input data, internal errors occurred that either froze the scene or error messages were reported. These results show that fuzzing is able to disclose bugs within code and that the stability of digital forensic tools may be questioned. [11]

The most common type of issue seen was a complete crash resulting in the Windows operating system presenting an error message. A crash has the potential to be a significant issue for an application and could result in anti forensic risks such as code execution which could lead to compromising the system and evidence. In test case TC.03 while processing the tool exited unexpectedly without an error message appearing from either the tool or Windows OS. An internal error message occurred during test caseTC.06. However, testing was abandoned during test case TC.02 while processing. The main risk of the creation of large cache files is that an investigator will run out of room to store the cache files and the evidence processing may need to be cancelled and repeated. This again is a time cost. An unproven concern that bugs in software can be exploited for anti-forensic activity creates a worry about the potential misrepresentation or damage to evidence by vulnerabilities in both open source and proprietary tools. [11] A number of software bugs were discovered that resulted in unusual behavior from different tools including behaviors that prevented evidence acquisition, crashing while searching or displaying incorrect evidence as well as evidence not being displayed as shown in Table 4.1. [11]

Test Case	*Result*	*Acceptance Spectrum*
TC.01	*Pass*	*Exceeds Expectations*
TC.02	*Fail*	*Unacceptable*
TC.03	*Fail*	*Unacceptable*
TC.04	*Fail*	*Unacceptable*
TC.05	*Pass*	*Exceeds Expectations*
TC.06	*Fail*	*Unacceptable*

Table 4.1 Acceptance Spectrum for Software test cases

V. CONCLUSION AND FUTURE WORK

This paper presents a detailed overview of the current counter forensic techniques and anti-forensic tools used and its effectiveness in detection of misleading of evidence or improper use of data. It also illustrates the success of such tools in recovery of evidence or vital data. The identification of software bugs and tool related issues have also been analyzed and the unusual behavior of the digital forensic tools has been brought to notice. The prudent intruder is safer employing a cleaning tool than a cryptanalytic one, as an elaborated and distinguished result of the sanitizer really destroys the desired data. [2] So, there needs to be an efficient way of tracing the

working of the sanitizer tool and other tools like it. Sice, law enforcement resources are limited, attackers employing anti-forensic technology are less like to be apprehended [2] thus, such resources need to be upgraded and modifies substantially. Organization should be concerned and sooner enough may have to determine expressly what knowledge they want to preserve as a part of normal operations done and so make arrangements to preserve that data in an exceedingly forensically sound manner. [2] There are still limitations to identifying and detecting malicious software bugs, which needs enhanced techniques and tools in process. Lack of tools to trace such criminal activities by attackers and intruders may make digital forensic evidences and consumer privacy a victim to counter forensic activities.

REFERENCES

[1] **USCERT, 2006.** Computer Forensics [online]. *http://www.us-cert.gov/reading_room/forensics.pdf.*

[2] 2. **Malan, Garfinkel** *One Big File is Not Enough: A Critical Evaluation of the Dominant Free-Space Sanitization Technique.* The 6th Workshop on Privacy Enhancing Technologies, Robinson College, 2005. Cambridge, United Kingdom

[3] 3. **Bitsum.** *PECompact: For maximum compression and speed*. [Online] 2006. http://www.bitsum.com/pec2.asp.

[4] 4. **Vrba, Z.** *cryptexec: Next-generation runtime binary encryption using on-demand function extraction*, Phrak 0x0b(0x3f). #0x0d of 0x14. [Online] 2003. http://www.phrack.org/archives/63/p63-0x0d_Next_Generation_Runtime_Binary_Encryption.txt.

[5] 5. **McLeod, S.** Smart Anti-Forensics. *Forensic Focus.* [Online] May 2005.

[6] 6. **Sanai, J.** *Promiscuous node detection using ARP packets*. [Online] 2001.

[7] **Garfinkel, S.** *Anti-Forensics: Techniques, Detection and Countermeasures.* Academic Conferences Limited, 2007. Proceedings of the 2nd International Conference on Information Warfare & Security. pp. 77-84. Monterey, California .

[8] **Geiger, M.** *Counter-forensic tools: Analysis and data recovery,* 2006. 18th Annual FIRST Conference. pp. 25-30. Maltimore, Maryland .

[9] **Hilley, S.** *Anti-forensics with a small army of exploits.* 2007. Vol. 4, pp. 13-15.

[10] **Sutton, M., Green, A., & Amini, P.** *Fuzzing: Brute Force Vulnerability Discovery.* Upper Saddle River, NJ : Addison-Wesley, 2007.

[11] 12.**Cusack, Brian and Homewood, Alain.** *Identifying Bugs in Digital Forensic Tools.* The Proceedings of 11 th Australian Digital Forensics Conference. p. 51. Citeseer, 2013.

[12] 11.**Carrier, B.** *Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers.* Vol. 1, Issue 4, International Journal of Digital Evidence, 2003.

[13] 13.**Guo, Y., Slay, J., & Beckett, J.** *Validation and verification of computer forensic software - Searching Function.* 2009. Digital Investigation. Vol. 6, pp. 12-22.

[14] 14.**Liu, V. T., & Stach, P.** *Defeating Forensic Analysis.* 2006. CEIC.

[15] 15.**Charters, I.** *The Evolution of Digital Forensics: Civilizing the Cyber Frontier.* CC, 2009.

[16] 16. **Hadnagy, C.** *Social engineering: The art of human hacking.* John Wiley & Sons, 2010.

Authors Profile

B.Prabhakar received the **B.TECH.** degree in computer science and engineering from the SR Group of Institutions, Jhansi, Uttar Pradesh, India in 2014.Currently doing **M.TECH.** in computer science and engineering in Jaypee University of engineering and technology, Guna, Madhya Pradesh, India. Her research interest includes Counter forensics, digital forensics, deep learning, neural networks.

N.Jain is a Gold Medalist in M.Tech from Dayalbagh Educational Institute in Agra and is a certified CISCO Network Associate. He has earned international certification from "DALE CARNEGIE" on "High Impact Teaching Skills" has over 6 years teaching experience. He is an experienced teacher of Design & Analysis of Algorithms, Object Oriented Systems, Data Structure and Computer Networks. His research interests focus on Mobility Management in Wireless Networks and Optimization Techniques, Digital Forensics. He has guided a number of BE and M.Tech students for their projects. He is a member of IAENG, IACSIT, and CSTA.