International Journal of Management, IT & Engineering
(ISSN: 2249-0558)

CONTENTS

Editorial Board

Editorial Advisory Board

Title

FORENSIC TOOLS MATRIX: THE PROCESS OF COMPUTER FORENSIC FOR DIGITAL EVIDENCE COLLECTION

Author(s)

Dr. Jigar Patel

Associate Professor

MCA Programme

Kalol Institute of Management, Kalol

North Gujarat

Abstract:

Cyber crime is in limelight due to increasing use of computer and its networks in day to day activity. As computer networks is heavily use not only for information exchange but financial and private data are also transferred via Internet, the Cyber crime increasing by high rate. Since, the evidence of such crimes are in digital forms it is challenging task for Cyber crime Investigator or police personals to collect the evidence against the Cyber criminals to prove the particular type of Cyber crime. This paper mainly focuses on how the Cyber crime takes place and how to collect the evidence against the Cyber criminals which is enough to prove the crime in the court. To do this we need various tools to collect the evidence against the criminals and therefore, the Forensic Tools Matrix helps a lot to investigator for evidence collection and entire investigation process.

Keywords: Cyber Criminals, Forgery, Forensic Tools, Forensic Tools Matrix, Investigator.

Introduction:

Any case in the court is prosecuted on evidence; therefore, collection of the evidence is the crucial task before the Cyber crime investigator. The court only believes that evidence in the prosecution, which is full proof and reliable. The chain of evidence is also important in the prosecution, which means if any evidence in the sequence goes wrong the entire collection of the evidence is useless. Therefore, the continuity and sequence of the evidence is equally important like the individual evidence. The collection of the evidence is not easy task in the Cyber space; it needs lots of knowledge of computer and computer network system. In addition, investigator has to use certain tools and software to acquire the evidence against the Cyber criminals.

In this paper by constructing Forensic Tools Matrix as shown in Fig.1 we are trying to categories different types of Cyber crime and mapping with forensic evidence collection tools used for investigate for such crime. If there is crime like the forgery, Email spoofing, Child pornography, Hacking etc. it is important that what kind of the evidence collection tools are used by the Cyber crime investigator for the specific Cyber crime for evidence collection. In addition,

this paper also discusses one case study which shows how the Forensic Tools Matrix helps in the process of investigation and evidence collection.

Forensic Tools Matrix:

Nowadays numbers of tools are available commercially and some of them forensic tools are easily downloadable from the Internet. But the important criterion is the applicability of tools for evidence collection in specific type of Cyber crime. So, it is require to categories and built Forensic Tools Matrix which help the Cyber forensic investigator for investigating the specific crime. In this matrix all different kinds of Cyber crimes are given in the row and in the column types of tools is given while in the cell right symbol shows the applicability of particular types of forensic tools for specific type of Cyber crime. Here also all types of tools are explained one by one.

Forensic Tools / Cyber Crime	Type 1	Type 2	Type 3	Type 4	Type 5	Type 6	Type 7	Type 8	Type 9	Type 10
Deleting or altering computer information	–	–	–	–	–	–	√	√	–	√
Credit Card Fraud	–	–	–	–	√	√	–	–	–	–
Cyber Pornography	√	√	√	√	–	–	–	–	–	–
Hacking	√	√	√	√	√	√	–	–	–	–
Online Gambling	√	√	√	√	–	–	–	–	–	–
Email spoofing and spamming	–	–	–	–	–	–	–	–	√	–
Forgery by computer	–	–	–	–	–	–	√	√	–	√
Denial of service	√	√	√	√	√	√	–	–	–	–
Worm, Virus and Trojan	√	√	√	√	√	–	√	√	–	√
Internet Time Theft	√	√	√	√	√	√	–	–	–	–
Salami Attack	√	√	√	√	√	–	–	–	–	–

Fig.1: Forensic Tools Matrix

Type 1 - Port Scanning Software:

Some tools are useful to get the port information on the remote computer and give the information about which port is open on remote computer. NMAP, NETSCAN tools and SUPERSCAN are the popular tools for the port scanning. The suspicious open port was for a server that used a custom protocol and gave the attacker remote control of the system. Investigator can use such tools while computer was plugged into the network; he performed a port scan of the server and identified a suspect port that was open [1].

Type 2 - TCP/UDP Connection Tools:

This kind of tools are capable to interact with the network application at application layer and investigator is able to see the raw data before is goes to the application layer protocol like SMTP, FTP and HTTP. NetCat is the example of this category. Netcat includes MD5 check sum capability which is an essential part of any sound digital collection order to prove the data was not altered during collection. Netcat works by booting to a shell and listening on a particular TCP port in verbose or listening mode. Once the forensic workstation is in listening mode via Netcat, the data is sent from the target host to the particular port the forensic workstation is listening to. Cryptcat is a variant of Netcat that encrypts all of the data across the TCP channel. It uses all of the same commands and command-line switches as Netcat but enhances Netcat by providing secrecy and authentication [2].

Type 3 - Current User Information:

Some tools are specially use for tracking the current user activity and to know which are the user currently logged in. Finger is one of the tools used in the Linux for this purpose and other tools like the NBTSTAT used in window while NetBios [3] is used to get active connection and MAC address. Apart from that some command like Who, W and Last is useful to get the user information.

Type 4 - Remote Operating Tools:

Some tools are available through which, one can operate the remote computer. VNC (Virtual Network Computing), NETBUS and BackOrifice are the examples of remote operating tools.

Type 5 - Vulnerability Auditing Tools:

This kind of tool shows the security laps of the system. Therefore, the investigator can use this tool to find the vulnerability of the current system and using that he can investigate about possible attack by the criminal. NESSUS and RETINA are in this category. Remote computer management systems incorporate advanced computer management software features and empower investigator to monitor and control computer use remotely, on a near real time basis via the Internet. These systems use forced gateway techniques to send pertinent usage information to an Internet server for immediate analysis, review, and archival. The Internet server processes usage information against rules and parameters set up by the agency and sends alerts by pager or email to investigator when prohibited or suspect activity is detected. Remote computer management allows investigator to sign onto any Internet enabled computer to generate reports, spot check offenders' activities on demand or in response to alerts, and conduct real time review of ongoing computer and Internet use [4].

Type 6 - Sniffer and Intrusion Detection Tools:

Such tools are use for the observing the packets that pass through the network. Ethreal and BUTTSNIFFER are used for the sniffing while DSNIFF is used for the session highjacking. Apart from that Snort is also used for the Intrusion Detection. With the development of network technologies and applications, network attacks are greatly increasing both in number and severity. As a key technique in network security domain, Intrusion Detection System (IDS) plays vital role of detecting various kinds of attacks and secures the networks. Intrusion detection systems (IDS) are an effective security technology, which can detect, prevent and possibly react to the attack. It performs monitoring of target sources of activities, such as audit and network traffic data in computer or network systems, requiring security measures, and employs various

techniques for providing security services. With the tremendous growth of network-based services and sensitive information on networks, network security is becoming more and more important than ever before. Symantec in a recent report uncovered that the number of fishing attacks targeted at stealing confidential information such as credit card numbers, passwords, and other financial information are on the rise every year .One solution to this is the use of network intrusion detection systems (NIDS), that detect attacks by observing various network activities [5]. A honeypot is also an IDS and to simulates a vulnerable computer on a network. It contains no critical data or applications, but has enough data to lure an intruder. When an intruder attacks the honeypot, the activities of the intruder are recorded in the log files. Later, these log files are audited; the attack signatures are identified and stored in the database for further use [7].

Type 7 - Forensic Duplication Tools:

Some tools are used for the taking the image of the entire hard disk of the suspected computer for further analysis. This kind of tools is capable to copy even deleted and swap files from the media. Safeback is one of the most popular image copying tools. The integration of strong encryption into operating systems is creating challenges for forensic examiners, potentially preventing us from recovering any digital evidence from a computer. Because strong encryption cannot be circumvented without a key or passphrase, forensic investigator may not be able to access data after a computer is shut down, and must decide whether to perform a live forensic acquisition. In addition, with encryption becoming integrated into the operating system, in some cases, virtualization is the most effective approach to performing a forensic examination of a system with Full Disk Encryption. Encryption is one of the strongest protection measures against unauthorized access to data. The need for securing data on hard drives has led to an increase in the use of strong encryption. Until recently, forensic investigator could recover digital evidence from computers despite the use of encryption. However, the integration of encryption into operating systems, specifically full disk encryption (FDE), is making recovery of digital evidence more difficult. Today, a forensics investigator may encounter a full disk encryption interface prior to the machine booting, access to any data unless the necessary credentials are supplied. If these credentials are not available, forensic investigator may have to acquire a forensic image of a live system while the contents are in an unencrypted state [6].

Type 8 - Analysis Tools:

After collecting the large set of information it is important to extract the evidence from that data. Therefore, some tools like Forensic Toolkit and EnCase are used for the analysis of collected information from the suspected computer. For Linux environment Coronor's Toolkit is used for the evidence collection.

Type 9 - Email analysis Tools:

Some tools are specially developed for the Email analysis and used to investigate the crime like Email-spoofing and spam Email. Paraben Email Examiner is one of the good tools for the Email analysis.

Type 10 - Password Cracker Tools:

Some tools are available to crack the password of the particular file or system. Investigator can use the cracker like John and Ripper.

Case Study on Evidence Collection for Forgery:

As we know in the forgery, by means of computer, printer and scanner people are trying to produce counterfeit currency, stamps for revenue and post or preparing the fake documents like mark sheets or certificates. In this regard finding evidence from suspected computer is very critical task in the evidence collection procedure. First of all suspected computer is seize and send for the forensic analysis as shown in Fig. 2 to collect the evidence. Therefore, according to Forensic Tools Matrix type 7, type 8 and type 10 kind of tools generally used to collect the evidence by the investigator.

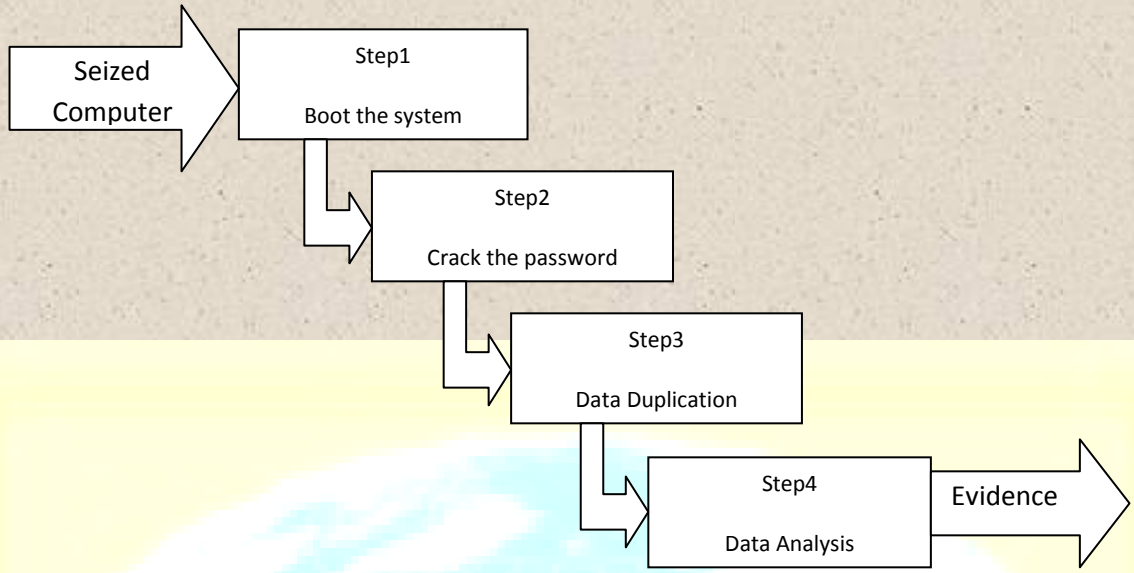

Fig.2 Steps for evidence collection in forgery

Step1:

If the suspected computer is not booting properly we cannot reinstall the operating system because it may delete the evidence from the suspected computer. So, first we should think about how we can collect the data by booting it from the CD-ROM. Suppose, for Windows operating system you can try for repair the system by using the window recovery CD and if the operating system is Unix then you can use some tools like Trinux which used for booting the system from floppy or CD-ROM which is entire running in the RAM.

Step2:

Some time the investigator can capable to seize only the computers and other accessories and the Cyber criminals might be already escaped, at this stage the examination of the seized computer system is more important because it can give the clue about the criminals address, phone numbers or email addresses and many other information. At this stage if the computer program and file have password then breaking of the password is important for the investigator.

Investigator can use various tool like John and Ripper which is probably fasted, most versatile tools and it support six different type of the hashing scheme and also support the special character and wordlist to crack the password with least 13 different operating system and several processor. Other than that the Password Recovery Toolkit is available which is used for the getting the password from the cryptographic data. Hence, the type 10 kinds of forensic tools are used from Forensic Tools Matrix.

Step3:

Sometimes the business firm has large numbers of computers that are suspected in the crime but all computers cannot be seizing by the investigator, but he can just copy the data from the suspected computers. Forensic Duplication Tools like Safeback is used for the copying the files bit-by-bit from one media to other. This kind of bit-by-bit copy is the basis of the all forensic duplication tools. Hence, in this step type 7 kinds of tools are used from Forensic Tools Matrix.

Step4:

After the duplicating all the data it is important that, how the data is being search from the large amount of the datasets. In the large amount of computer data very few data might be important in the forensic investigation point of view. So, some tools are used for the forensic analysis. One is the Forensic Analysis Toolkit from the Access Data attempt to help the analyst by reducing large dataset into a subset of the important information. The tool is design so that it is very easy to work with. Other tool is used for the forensic analysis is EnCase. If the operating system is Linux then one open source tools is available for the analysis namely Coroner's toolkit. All such tools help a lot to investigator for searching the image files or text file based on pattern matching. Hence, the type 8 kind of tools is used from Forensic Tools Matrix.

Conclusion:

As computer related crimes are become more and more complex and undetectable the role of Cyber crime investigator is crucial nowadays. Thus, such kind of Forensic Tools Matrix is very helpful to collect the evidence against the Cyber criminals due to the tools are well categorized according to specific types of Cyber crime. Here the Forensic Tools Matrix gives the important Cyber crime along with that it also give types of tools can be used to not only detect the crime but also useful to collect evidence against the Cyber criminals.

References:

- Brian Carrier, Eugene H. Spafford, Getting Physical with the Digital Investigation Process, International Journal of Digital Evidence, Volume 2, Issue 2, Fall 2003, pp. 1-20
- Irma Resendez, Pablo Martinez, and John Abraham, An Introduction to Digital Forensics, Volume 6, ACET Journal, 2010.
- Peter Knaggs, Using IBM's NetBios from Forth, The Journal of Forth Application and Research, Volume 7, 2009.
- Richard C. LaMagna and Marc Berejka, Remote Computer Monitoring: Managing Sex Offenders' Access to the Internet, The Journal of Offender Monitoring, 2009, pp. 11-29.
- Meera Gandhi, S.K.Srivatsa, Detecting and preventing attacks using network intrusion detection systems, International Journal of Computer Science and Security, Volume 2, Issue 1, 2008, pp. 49-60.
- Eoghan Casey, The Impact of Full Disk Encryption on Digital Forensics, ACM SIGOPS Operating Systems Review, Volume 42, Issue 3, April 2008.
- Sandeep Chaware, Banking Security using Honeypot, International Journal of Security and Its Applications Vol. 5 No. 1, January, 2011, pp. 31-38.