Scientific Awareness about the Computer Forensic to face the e-criminal Activities Of The e-user

M. Nawaz Brohi
Department of Information Technology
Preston University Ajman
United Arab Emirates

Rukshanda Kamran
Department of Information Technology
Preston University Ajman
United Arab Emirates

ABSTRACT

Computer has influenced our daily work, activities and played a vital role in every corner of our life. We are surfing the net for news, jobs, entertainment, transferring information and data online, purchasing, checking accounts, sending and receiving emails almost every day. For this widespread use, some computer users have misused this technology in illegal activities. As a result the computer forensic and investigation has emerged to carry out the investigation process for solving and discovering different types of internet or computer crimes and bring it to the court.

In the paper we will discuss the challenging aspects of forensic investigation, skills needed by a computer forensics, knowledge needed by computer forensic investigator, and phases of computer forensic investigation. Overall the purpose of the paper is to provide the scientific awareness about the computer forensic to face the e-criminal activities of the e-user.

Keywords

forensics, computer forensic, anti-forensics, forensic investigation, encryption, decryption, intruder.

1. INTRODUCTION TO E-CRIME

There are two categories of e-crime called cat-ec1 and cat-ec2. The cat-ec1targets computer networks or storage devices and the cat-ec2 facilitated the computer networks and storage devices. E-crime starts with the introduction of ARPANET. The methodologies used against the computer forensics processes are collectively called anti-forensics.

2. FORENSICS AND COMPUTER FORENSIC

Forensics can be defined as the method of using scientific knowledge for gathering, analyzing, and putting the evidence in front of the courts. The exact meaning of the term is "to bring to the court". The Forensics begins initially by extracting and analysis of hidden evidence. Hidden evidence comes in different forms, evidence recovered from the blood by examining the DNA and fingerprints left at the crime scene to the files on computer storage devices **[1].**

Computer forensics is also known as cyber-forensics which is the major application of computer investigation and analysis techniques to collect very strong proofs based on real facts and figures for presentation in a court of law. Computer forensics is a new specialization or discipline, revolving around extracting hidden data from storage devices. Still it is not recognized as a formal discipline.

We can define the computer forensics as the specialization of combining both specializations law and computer science to gather and analyze information or data stored in the computer systems, RAM, CD ROMS, Hard drives, flash memories, network devices like routers, switches, firewalls, intrusion detection systems, intrusion prevention systems, and wireless devices, in order to be admissible as evidence in front of the court. The Information which can be restored from digital devices and describes a series of acts or events is the duty of computer forensic.

Computer forensics is branch of forensic science in general; the computer forensic has different branches and diffused to other eras like Data Packets - information traveling on the network - email files, and Data stored. Database forensics, network forensic, firewall forensics, and mobile device forensics are examples of the different fields that have resulting out of computer forensics **[2].**

Such as other forensic investigation, evidences based on computer forensics can be used to implicate the criminals in courts of law all over the world. Many child abuses, financial crimes and other crimes have been unearthed by what is called computer forensics **[3].**

The investigator is an information retrieval expert; he/she might be assigned the searching and collecting evidence from corrupted and damaged storage mediums. The computer investigator Retrieval experts would be expected to recover hidden, lost, and deleted data from storage devices like hard disks, CD ROM, USB storage devices, and digital cameras, mobile phones, emails, web pages, and remote storage locations.

In many countries many organizations are allocating a greater portion of their information technology budgets for computer and network security. As reported by International Data Corporation (IDC) that the market for intrusion detection and vulnerability assessment software has reached more than 1.45 billion dollars over the last decade **[4].** In increasing numbers, organizations are deploying network security devices such as intrusion detection systems (IDS), firewalls, and proxies.

3. INVESTIGATION PROCESS

The investigation process and duration might vary from one day, week to months depending on the investigator skills. Some of the factors which has impact on the duration of the investigation process listed below.

- Experience gained by the investigator
- The number of PCs he is going to search
- The number of storage devices such as hard disks, USB flash, CDs, DVDs
- Skill of the intruder to delete of hide the information

- The number of encrypted or protected files

Some criminals have found ways to make it even more difficult for investigators to find information on their systems. They use programs and applications known as anti-forensics. Detectives have to be aware of these programs and how to disable them if they want to access the information in computer systems **[5].**

4. CHALLENGING AND LEGAL ASPECTS OF FORENSIC INVESTIGATION

The main goal of computer forensics techniques is to search and analyze data on digital systems to find potential evidence to be presented in front of the court for a trial. The internet connects a number of computers from different places all over the world, which makes it difficult for the investigator to collect the relevant evidence. Digital evidence and data can be located on the network of a single building, area, cities or countries. Beside that network traffic is transient and must be captured during the transit state by packet sniffers. Many of the techniques used by forensic investigator faced by anti-forensic, but there are unique aspects to forensic investigation **[6].**

For example, when we open a computer file and change its contents, the computer records all information about the files time and date it was accessed. If computer investigator seized a computer and begin to search and opening files, we can't say for sure that he did not change any data or information **[7].** Here Lawyers can contest the validity of the evidence. Some people objecting, how can we use digital information as evidence, if it is possible to alter computer data? Previously, it was very easy for an investigator to search files, because of the low capacity of hard disk. Today, a single USB can hold gigabytes of information and the hard disk can be of terabytes of data. As a result of the evolution of the Computer so that has become more powerful than ever, the area of digital forensic must evolve too. Investigator must find new methods and techniques to search for evidence without spending too many resources to find evidence.

Digital evidences are not easy to handle and some of them are not human readable, it require from the investigator to retrieve the data from a magnetic form, going through several layers to collect the information and then decode or decrypt the data. Beside that part of the huge data stored in the hard disk may be relevant to the incident **[8].** Probability of error in the translation of digital evidence more than the physical evidence like DNA samples.

Digital evidence is abstracted from digital object, which does not give a complete view of what happened**.** For example sending an email generates different activities, some of it will disappear, only few activities will remains such as server log and email content, other activities like clicking the mouse and typing on keyboard requires monitoring software to be installed to record them.

The intruder will use different activities to compromise the system, the investigator need to reform these activities to human readable form. Abstraction layer is used in all modern digital devices, so the actual data are not visible only a representation of it and each of the layers may produce error **[9].**

Digital evidence can be easily manipulated, altered or changed without leaving obvious trace. However there are some good features of digital evidences **[10].**

- The investigator can make exact duplication of the digital evidence
- Different Software's and tools are available to detect alteration of digital evidence
- An attacker cannot destroy digital evidence completely; some data will remain, because there are some areas where he cannot reach.
- Never assume that digital evidence is destroyed.

According to the Federal Bureau of Investigation's (FBI) Operational Technology Division's, Digital Evidence Section, forensic investigators and examiners have found digital evidence from burned out computer systems and devices found at the bottom of a lake **[11].**

Computer forensics is a new discipline to the court as compare to other criminal disciplines. New court rulings are issued that affect how computer forensics is applied **[1].** The best and strong source of information in this area is the United States Department of Justice's Cyber Crime Web site **[12].** Internet-related crime should be reported to appropriate law enforcement investigative authorities at the local, state, federal, or international levels, depending on the scope of the crime.

Each law enforcement agency also has a headquarters (HQ) in Washington, D.C., which has agents who specialize in particular areas. For example, the FBI and the U.S. Secret Service both have headquarters-based specialists in computer intrusion (i.e., computer hacker) cases **[12].**

The Internet Crime Complaint Center (IC3) is a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center (NW3C). IC3's mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. The IC3 gives the victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory agencies at the federal, state, and local level, IC3 provides a central referral mechanism for complaints involving Internet related crimes. **[12].**

The Computer Crime and Intellectual Property Section (CCIPS) is responsible for implementing the Department's national strategies in combating computer and intellectual property crimes worldwide. CCIPS prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts. [**12**].

To determine some of the federal investigative law enforcement agencies that may be appropriate for reporting certain kinds of cyber crime, please refer to the following

Table-1: List of crime and appropriate federal investigative law enforcement agencies [12].

Type of Crime	**Appropriate federal investigative law enforcement agencies**
Computer intrusion (i.e. hacking)	FBI local office U.S. Secret Service Internet Crime Complaint Center
Password trafficking	FBI local office U.S. Secret Service Internet Crime Complaint Center
Child Exploitation and Internet Fraud matters that have a mail nexus	U.S. Postal Inspection Service Internet Crime Complaint Center
Internet fraud and SPAM	FBI local office U.S. Secret Service Federal Trade Commission (online complaint) if securities fraud or investment-related SPAM e-mails, Securities and Exchange Commission (online complaint) Internet Crime Complaint Center
Internet harassment	FBI local office
Internet bomb threats	FBI local office ATF local office
Trafficking in explosive or incendiary devices or firearms over the Internet	FBI local office ATF local office
Copyright piracy (e.g., software, movie, sound recordings)	FBI local office U.S. Immigration and Customs Enforcement (ICE) Internet Crime Complaint Center

In United States, there are three areas of law related to computer security **[1].**

I. The Fourth amendment of the United States Constitution allows for protection against unreasonable search and seizure, and the Fifth Amendment protects citizens from self-incrimination.
II. Anyone concerned with computer forensics must know how three U.S.Statutory laws affect them. These protections influence how evidence can be gathered and how that evidence can be used in court. For example, violating the Wiretap Act (18 U.S.C. 2510-22), the Pen Registers and Trap and Trace Devices Statute (18 U.S.C. 3121-27), and the Stored Wired and Electronic Communication Act (18 U.S.C. 2701-12). Violations of any one of these statutes during the practice of computer forensics could constitute a federal felony punishable by a fine and/or imprisonment.
III. The U.S. Federal rules of evidence about hearsay, authentication, reliability and best evidence must be understood. In the U.S. there are two primary areas of legal governance affecting cyber security actions related to the collection of network data: (a) authority to monitor and collect the data and (b) the admissibility of the collection methods.

U.S. Constitution

4th Amendment
5th Amendment

U.S. Statutory Law

18 U.S.C. 2510-22
18 U.S.C. 2701-12
18 U.S.C. 3121-27

Federal Rules of Evidence

Hearsay
Authentication
Reliability
Best Evidence

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Figure 1: Laws that Affect Cyber Security -1 [1]

5. SKILLS NEEDED BY A COMPUTER FORENSICS

- The Computer forensic investigator must have to understand the kind of potential evidence he/she is looking for in order to structure the search.
- He/she must have the knowledge and types of Crimes using a computer as a tool to commit crime, which can range from hacking, child abuses, website destruction, and pornography to theft of personal data, impersonal others and theft the Credit card destruction of Computer and hacking of password and email.
- The investigator must pick the appropriate tools to use. Files may have been altered, deleted, damaged, encrypted, and the computer forensic must be familiar with the software and methods to prevent damage during the recovery process.
- Type of Data to be collected in computer forensics, temporary data, volatile and nonvolatile data.
- Forensic Investigator must also have a basic understanding of how routine computer and network administrative tasks can affect both the forensic process for potential admissibility of evidence at court **[13].**

The duties of a computer forensic are to identify, collect, extract, maintain, analyzing and documenting the related data involved to commit the crime in online activity **[3].** In order to perform the forensic successfully, the computer forensic have to equip himself with necessary knowledge and sufficient practical skills.

6. KNOWLEDGE NEEDED BY A COMPUTER FORENSIC INVESTIGATOR

Cryptology – the forensic investigator should know the most important techniques of encryption used to protect data from alteration or theft (integrity) and can also be used for user's authentication. There are three types of cryptographic techniques used to accomplish these tasks: secret key or symmetric cryptography, public-key or asymmetric cryptography, and hash functions. The human readable data or unencrypted data is called plaintext and the encrypted data called cipher text, which can be decrypted into readable form **[14].**

Operating systems - Forensic investigator must have achieved at least a preliminary understanding of the types of operating systems and characteristics and features of each, because it is the most important program that runs on a computer system and performs basic tasks. Operating systems contain valuable logs suitable for forensic investigation. Operating systems can be classified as multi-user, multiprocessing, multitasking, multithreading, real time. The most common operating systems are windows, Linux and DOS, UNIX and OS/2.

7. PHASES OF COMPUTER FORENSIC INVESTIGATION

- Preparation for the investigation
- Collection and examining the data from the digital storage media
- Analysis of the information
- Documenting and reporting

7.1 Preparation for the investigation

It is very necessary the digital investigator must prepare himself before the investigation, so that he can be prepared to perform a digital investigation before the need for such task arises. This phase involves the preparation of the forensic toolkits going to be used during the investigation and the investigation policy going to be adapted.

Investigation policy means a set of necessary requirements that will clarifies and support the approach to be taken by the digital investigation. It describe the features of the system to be investigated, how to use the best methodology and present technical resources such as details of security weaknesses of the operating systems, applications and network configuration, attacks and vulnerabilities, details of the system internal environment and documenting them.

The digital investigator should emphasizes on the types of evidences to be gathered, devices that should be examined and monitored and highlights the priority and the sequence of the investigation process. The investigator should also prepare for the use of software that allows him to retrieve the information and putting it in safe place for comparison.

7.2 Collection and examining the data from the digital storage media

Investigator should avoid missing or loosing of any data or information, every piece of information is very important for the investigation and its future use. During this phase of investigation the usefulness of the evidences should be maximized. For example, If the system available, investigation should be performed quickly, in order to return the system to its safe state **[10].**

Data collection can be performed from different devices and range from copying of disk content, CD, DVD to volatile data.

Very important procedure widely used during investigation by digital forensic called “Chain of custody”, which represents a log file that contains records about each action taken on the collected evidences. The investigator should prepare guidelines before the investigation process and it should be strictly followed in order to perform error free and fast data collection, then it depend on the operating system, services, software installed on the investigated system and on the software that going to be used for data collection.

In data collection the investigator uses different data collection software and scripts that should be used during an investigation. The Information or data to be collected can be categories into three types:

- Volatile data
- Temporary data
- Persist-tent data

7.2.1 Volatile data

Volatile data resides on memories, registers and caches content, random access memory they are highly sensitive and may be lost when we use the system or switched off the computer. For this reason it must be collected first to avoid or reduce their lost.

7.2.2 Temporary data

Temporary data, in the form of network connections, running processes, listening servers, and temporal files, should also be collected. However, as their corruption or loss is less than volatile data, they must be collected before persistent data and after volatile data.

7.2.3 Persistent data

Persistent data are located on storage media such as hard disk, CDs, DVD and flash and consists of software configuration, file systems, log files, and users’ data and is preserved when the system switched off. Simply copying all valuable files from the disk is insufficient for a thorough investigation, as it may not capture all potential evidences. Due to file system characteristics the data collection from storage media becomes a challenging task.

Overall, in the worst cases, data collection will lead to insufficient evidence or to an incorrect understanding of the hack or the incident.

7.3 Analysis of the information

The analysis is the most complex phase; it needs creativity, high sense and great effort and high intuition. Preparation and data collection can be partially automated, while in this phase few segments that can be performed automatically. The analysis aims to examine the relevant information and finds the causes and the effects of the occurred attack or incident. The analyzed data need to be minimized and this is one of the main difficulties in this phase, because the investigator has to sort the most important and relevant data. The investigator has to form some sort of checklist or road map for the plan could be used for examining the relevant data. For example, where an IPS or IDS was noting to be sending several alerts at a particular moment, then the computer forensic should examine the system logs to find anomalous behavior that occurred at that particular time. In this case, valuable information will help analyzer for understanding the incident like the number of successful login and failed login attempts, may be fetched. Investigator facing the challenges by intruder or the incidents in which intruders erased traces that may lead to their malicious activities, after hacking the system.

The information is organized inside a computer system across multiple layers. For example, if the hacker or cracker has hidden some evidence within the free space or unused part of the hard disk sectors. Using a graphical application for analyzing the file will not lead to any anomaly. But, if the file size reported by the system file compared with the total amount of space occupied, the hidden information could be fetched; another example of analysis to check if a file changed or not, can be performed by comparing the file integrity with another well known file.

7.4 Documenting and reporting

The investigator have to take into account certain things in mind while handling important pieces of information, which might serve as evidence at a later stage. All important information that has been collected as part of evidence must be Documented. This practice very important, because, the investigator might change and new evidence may appear. Therefore, documenting all the information and evidences will help in the future for solving the case and it becomes source of information for the new computer forensic investigator to understand the case. Several years may pass between an investigation and a trial, and if there is no proper documentation, court will not accept the evidences. Documentation should not include only files and data retrieved from the computer, but a complete report on the system’s physical layout, encrypted or hidden files and snaps of different devices.

Documentation will continue from beginning to end of investigation, the investigator should keep in mind that the case will go to the court and he will be questioned for everything.

Forming a proper information and circle of evidences, what is referred to as a chain of custody, and material is also very important aspect of computer forensic investigator. It is worth mentioning, the computer investigator is required to handle the evidence in very careful manner in order to avoid damaging of the storage medium, tampering or loss of evidence in any form.

8.CONCLUSIONS

Technology is harnessed and it is being used more than ever before, to commit crimes. Each year, the number of computer crimes increases. Law enforcement is in a perpetual race with the intruders and criminals. Part of this race includes developing forensic tools by programmers and law enforcement and on the other hand developing of anti-forensic tools by intruders.

In order to keep a step ahead of the criminals, various investigative agencies and detectives around the globe have strengthen their computer forensic branches and equipped them with the expertise to face such crimes. As a result of the evolution of the computer which has become more powerful than ever, the area of digital forensic must evolve too.

The computer investigator must be able to differentiate between genuine and bogus information and being able to extract the evidence and translate raw data into concrete evidence which lead to condemning the offender in the law of court.

Computer forensic experts can play their vital role not only to find the e-criminal but also to gather the strong evidence against e-criminals and on the bases to gather evidence to take a legal action against the e-criminals.

If network, and system administrators possess the technical skills and abilities to protect harmful information related to an expected security incident in a forensically sound manner and are aware of the legal issues related to forensics, they will be a great input to their organization.

The Internet Crime Complaint Center is a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center. IC3's mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. The IC3 gives the victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory agencies at the federal, state, and local level, IC3 provides a central referral mechanism for complaints involving Internet related crimes.

The Computer Crime and Intellectual Property Section is responsible for implementing the Department's national strategies in combating computer and intellectual property crimes worldwide. CCIPS prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts.

In conclusion, the major reasons for e-criminal activity in computers are the theft of company documents, e-mail frauds, unauthorized use of computers mostly breaking a username and password, harassment and stalking in cyberspace, releasing a malicious computer program that is virus and accessing the victim’s computer via the Internet. The end-users, network, and system administrators should be aware about all aforementioned e-criminal activities of the e-users to protect their computers and organizations to reduce expenses.

9.REFERENCES

[1] Richard Nolan, Colin O’Sullivan, Jake Branson, and Cal Waits. 2005. First Responders Guide to Computer Forensics.

CERT Training and Education, March 2005. http://www.us-cert.gov/reading_room/forensics.pdf Computer Forensic

Produced in 2008 by US-CERT, a government organization.

[2] Gary Palmer. 2001. A Road Map for Digital Forensic Research, Report from DFRWS 2001, First Digital Forensic Research Workshop, Utica, New York, August 7 – 8, 2001, Page(s) 27–30

[3] Yong, J.J. 2009. Computer Forensics Career - What Does a Computer Forensic Investigator Actually Do? 17 Feb. 2009 EzineArticles.com.

[4] McCann Investigators Today, 6 Feb 2012 http://investigatorstoday.com/banner/mccann-investigations-in-dallas-texas.html.

[5] Simson Garfinkel. 2007. Anti-Forensics: Techniques, Detection and Countermeasures, Naval Postgraduate School, Monterey, CA, USA, 2007.

[6] Ranklin Witter. 2001. Legal Aspects of Collecting and Preserving Computer Forensic Evidence, GSEC Practical v1.2c SANS Triangle Park Security Essentials Course, April 20, 2001.

[7] Eoghan, Casey. 2004. Digital evidence and computer crime, forensic science, computers and the internet, academic press, second edition, 2004.

[8] Digital evidence field guide, what every peace officer must know, continuing education series 1.1., US department of justice federal bureau of investigation, 2007.

[9] Brian Carrier. 2002. Defining Digital Forensic Examination and Analysis Tools. In Digital Research Workshop II, Available at: http://www.dfrws.org.

[10] Slim Rekhis. 2007. Theoretical Aspects of Digital Investigation of Security Incidents, Oct. 2007 CNAS REPORT CNAS-2008-103 Supersedes CNAS-2007-101

[11] Yun Wang, James Cannady, and James Rosenbluth. 2005. Foundations of computer forensics: A technology for the fight against computer crime. Computer Law and Security Report, 21(2):119–127, 2005.

[12] http://www.justice.gov/criminal/cybercrime/ (Computer Crime & Intellectual Property Section).

[13] Jessy, Jeslyn "What Are the Skills Needed by a Computer Forensics Accountant?" What Are the Skills Needed by a Computer Forensics Accountant? 9 Jul. 2009 EzineArticles.com

[14] Gary C. Kessler. 1998. An Overview of Cryptography, edited version of this paper appears in the 1999 Edition of Handbook on Local Area Networks, published by Auerbach in September 1998. http://www.garykessler.net/library/crypto.html (17 November 2006).