Forensics Computing Technology to Combat Cybercrime

E.Saraswathy, T.Latha Maheswari

PG Scholar, Dept of Master of Computer Application

Sri Krishna College of Engineering and Technology, Coimbatore, India

Abstract: The advent of technological revolution in communications and information exchange has created sophisticated form of crime, cyber crime. Cybercrimes have more severe economic impacts than many conventional crimes and like any other crime, these cyber crimes should be brought to justice. The process of gathering electronic evidence of a cyber crime is known as forensic computing. This paper addresses the technical aspects, while at the same time providing insights which would be helpful for the legal profession to better understand the unique issues related to computer forensic evidence when presented in the court of law.

Keywords— *Cyber* ***Crime, Computer Forensics, Electronic/Digital Evidence, Piracy,.***

I. INTRODUCTION

Cyberspace has no specific jurisdiction; therefore, criminals can commit crime from any location through computer in the world leaving no evidence to control [1]. When someone ―steals‖ data from cyber space or uses information for unintended purposes, it is called cyber crime. With the increase usage of computer technology, cyber crime is on the rise. Like any crime, cyber Crime should be investigated and prosecuted where necessary. Computer forensics describes the practice of retrieving evidence in the form of data from a computer that relates to a crime in a manner that meets the requirements of the given a legal

System. Computer forensics evidence needs to be handled with the same care that physical evidence requires. However, there is added complexity due to the technical nature of computer based technology and has added another dimension with digital evidence. As greater emphasis is placed on digital evidence, it becomes increasingly critical that the evidence be handled and examined properly.

II. CYBERCRIME LANDSCAPE

Cyber crime is typically described as any criminal act dealing with computers or computer networks. It is also called by other names (e-crime, computer crime or Internet crime in different jurisdictions), which have roughly the equivalent meanings. The characteristics of cyber criminals, cybercrime victims, and law enforcement agencies have created a vicious circle of cybercrime. Figure1 shows this circle's key elements.

Cybercrimes are structurally unique in three main ways:

- They're technologically and skill-intensive.
- They have a higher degree of globalization than conventional crimes.
- Given the Internet's global nature, cybercrimes entail important procedural and jurisdictional issues.

Cybercrimes includes but not limited to:

- Theft of telecommunications services;
- Communications in furtherance of criminal conspiracies;

- Information piracy, counterfeiting and forgery;
- Dissemination of offensive material;
- Electronic money laundering and tax evasion;
- Electronic vandalism and terrorism;
- Sales and investment fraud;
- Illegal interception telecommunications;
- Electronic funds transfer fraud.

Regardless of the definitions, the use of computers and the Internet in the commission of crimes require investigators applying cyber forensic techniques to extract data for those investigating these cases, prosecuting these cases and passing the ultimate judgment regarding the disposition of offenders and the redress of victims.

III. FORENSIC COMPUTING

Computer forensics refers to the legal processes, rules of evidence, court procedures, and forensic practices used to investigate e-Crimes [2]. Specifically, computer forensics is the application of scientific, forensically sound procedures in the collection, analysis, and presentation of electronic data. For computer evidence to be accepted in a court of law, the forensic investigation process must identify, preserve, examine, and document any computer evidence retrieved [3]. Computer evidence is entirely different. It cannot be seen, touched or smelled and it often lasts for only very short periods of time. Computers typically store data in three ways, magnetic, semiconductor, and optical. Other less common data storage methods include magneto-optical disk storage, optical jukebox storage and ultra-density optical disk storage. Potentially significant new developments in technology suggest that techniques like phase-change storage, holographic storage, and use of molecular memory may become methods for data storage in the future. Data stored on these devices, while potentially of tremendous value in the investigation, prosecution and prevention of crime, presents unique challenges to detectives and prosecutors because of its potentially volatile nature. Electronic data is fragile. It can easily be changed or eliminated by cyber criminals. This means that the data must not be compromised in any way. It must be able to be proven that the data is a true representation of what happened, that it cannot have been modified in any way, either by the intruder themselves, or the collection and examination tools. In other words, the chain of custody must be established (Sommer, 1998), Mc Kemmish (2001) identifies three distinct types of forensic computing:

A. **Digital Evidence Recovery** – Involves the examination of electronic devices for information relating to a crime, and the processes involved in collecting relevant data.

B. **Cyber/Intrusion Forensics** – Involves detecting computer security breaches, identifying and preserving digital evidence.

C. **Forensic Data Analysis** – Involves identifying anomalies in large data sets that may indicate illegal or improper acts.

IV. METHODOLOGY AND DIGITAL EVIDENCE

Any criminal investigation follows procedures which vary from one country to another, but the computer forensics investigator should follow these steps:

- Secure and isolate.
- Record the scene.
- Conduct a systematic search for evidence.

∟ Collect and package evidence.

∟ Maintain chain of custody.

Phase 1 should be to freeze the scene of crime in order to prevent the ICT context from being modified before digital traces are collected, and to avoid giving the malicious person a chance to modify or destroy evidence [4]. The goal of phase 1 is to avoid the destruction or the dislocation of crucial data.

The investigator must classify resources to determine which system must be removed from the scene. Identifying traces and collecting them comprises the second phase (phase 2), and this should be followed by the data safeguarding and preservation phase (phase 3). At this stage, data can be analyzed (phase 4) and subsequently presented in a comprehensive way for non-experts and legal experts (phase 5). The purpose of any investigation is to discover and present facts that contribute to establishing the truth. It is not enough to be a good computer specialist, he should be aware of the legal framework and constraints in order to perform a useful computer investigation. If this were not the case, the results of the investigation could be compromised and thrown out by the court because of an insufficient or incorrect evidence-gathering process. A common vocabulary between police force, justice and forensics should exist. Procedures should be set up in order to increase computer investigation performance and reliability [5]. The resulting investigation report should be easily comprehensible and must describe in detail all the operations performed and procedures followed in order to gather electronic evidence. Investigators with an understanding of information and communication technologies should use in conjunction with effective international cooperation, so as to uncover the criminal's identity. Digital information can help to validate or dismiss a witness statement, to prove that a specific action was performed at a given time, to determine how a crime was committed, to reveal links between an offender and a victim, [6] etc. Which kind of information and where it can be found in the system and network is mandatory knowledge for digital investigators? Any computer systems information and communication device (electronic components, memory devices, hard discs, USB sticks, etc.) or information it contains, are potential targets or instruments of crime. Each software or data execution or transaction leaves digital traces. Digital traces are volatile and rapidly removed from servers. Digital evidence is even more difficult to obtain because ICT transcends international boundaries [7]. In such cases, success depends on the effectiveness of international cooperation between legal authorities and the speed with which action is taken. One of the most important features is the duration during which Internet Service Providers (ISP) keep information concerning user subscriptions and activities (IP addresses, connection data, etc.). The retention period, during which data is available in order to retrieve someone's identity from his IP address, varies from one country to another [8]. Legal systems must give law enforcement agencies the appropriate authority to access traffic data. Countries should improve international cooperation and be able to share critical information quickly, otherwise digital evidence may disappear. For Instant Messaging services and Peer-to-Peer or Internet Relay Chat facilities, logs and historical content of communications are kept for only a few days. An IP address identifies a computer, not a person and criminals use false or stolen identities [9]. It is always very difficult to establish the identity of a person on the basis of an IP address, email or web addresses or a digital trace. ―How can particular digital information be linked to its physical entity? Once the IP address of a system involved in a criminal activity has been identified, the next step is to investigate ―The physical entity? When searching for digital evidence, many problems arise, including these: Which elements may contain pertinent information for the case being investigated?

- How can the relevant data to be seized be identified?
- What are the procedure rules to be followed?
- How can data be collected, stored and preserved?
- How can data be safeguarded?
- How can digital data be preserved as evidence for a potential hearing?
- How can data be copied from its support to another one in order to analyze it without modifying it?
- How can a copy be authenticated?
- How can the original data be preserved?
- How can it be guaranteed that the process of copying the data did not modify it?
- How can files that have been deleted be recovered?

To answer these questions, some computer forensic tools and procedures should be used by trained and competent experts but their standardization is also an issue On the other hand, criminals could be tracked by active communication monitoring and live surveillance [10]. Telephone, e-mail or instant messaging eavesdropping is possible to collect information related to communication content or non-content such as e-mail headers or IP addresses. In fact, criminals can also be identified through undercover investigation when investigators join instant messaging (IM) services, peer-to-peer networks (P2P), Internet relay chat (IRC), newsgroups, etc. to lure criminals [11]. The chain of custody is a very important concept when dealing with investigation, forensic science, evidence and the execution of law and it helps to preserve the integrity of evidence. Like any material trace, a digital trace must satisfy certain criteria which include documentation of the trace and the history of the trace handling and must answer the following questions:

- Who gathered the evidence?
- How was the evidence collected?
- Where was the evidence found and amassed?
- How was the evidence stored, authenticated, protected and analyzed?
- Who handled the evidence? From whom did he receive it?
- How the evidence is kept safe? How is it authenticated? How is it locked up? Who has access to it? Who took it out of storage and why?

By applying best practices and existing guidelines, what is really needed in the investigation by cyber scene crime investigation, could improve and develop the investigator's efficiency, helping to be accepted by legal and technical professionals.

V. CONCLUSION

Without appropriate measures to combat cybercrimes, the vicious circle’s elements reinforce each other resulting in more and serious cybercrimes. No pure technological solution exists for such security-related problems, but combining technological and non-technological measures are needed to combat cybercrimes. At the technological level design of database and network and their implementation is crucial. Nontechnical measures are behavioural measures like, a simple training strategy aimed at creating awareness among consumers, employees, and the public about cybercrimes. Developing national technological and manpower capabilities, enacting new laws, promoting a higher level of industry-government collaborations, and pushing for international cooperation are critical to combating cybercrime. Given cybercrimes' global nature, international institutions especially carry enormous power that we must harness to fight such crimes example, the International Telecommunications Union (ITU). Investing in training people, law enforcement authorities and investigators could also enhance nations' abilities to fight cybercrimes

REFERENCES

[1] Cyber Crimes: A New Challenge, Deputy Controller (Technology), CCA, Ministry of Information Technology, India, 2002.

[2] Danquah, P., & Longe, O. B. (2011). An Empirical Test of the Space Transition Theory of Cyber Criminality: The Case of Ghana and Beyond. African Journal of Computing & ICTs. 4(2), 37-48.

[3] Bossler, A. M., & Holt, T. J. (2010). The Effect of self-control on victimization in the cyber world. Journal of Criminal Justice, 38, 227-236.

[4] Berg, S. E. (2009). Identity theft causes, correlates, and factors: A content analysis. In F. Schmalleger & M. Pittaro (Eds.), Crimes of the Internet (pp., 225-250). Upper Saddle River, NJ: Pearson Education, Inc.

[5] Finley, L. (2009). Online pharmaceutical sales and the challenge for law enforcement. In F. Schmalleger & M. Pittaro (Eds.), Crimes of the Internet (pp. 101-128). Upper Saddle River, NJ: Pearson Education, Inc.

[6] Britz, M. T. (2008). Computer Forensics and Cyber Crime: An Introduction. Upper Saddle River, NJ: Prentice Hall.

[7] Choi, K. (2008). Computer crime victimization and integrated theory: An empirical assessment. International Journal of Cyber Criminology, 2(1), 308-33.

[8] Bachmann, M. (2007). Lesson spurned? Reactions of online music pirates to legal prosecutions by the RIAA. International Journal of Cyber Criminology, 1, 213-227.

[9] Jason Michael Solomon, Computer Forensics: The Persistence of Data in Physical Memory University of Western Sydney, 2006.

[10] Marc Rogers, 'Security Perspectives Computer Forensics: Science or Fad?' (2003) Vol. 5, No. 65 Security Wire Digest.

[11] Kevin Mandia, Chris Prosie and Matt Pepe, Incident Response & Computer Forensics, Second Edition (2nd ed, 2003).