The Computer Crime Incidents and the Future of Countermeasures in Thailand

The computer crime countermeasure and adapting plans

Titikorn Tantawutho
Virtual Simulation Division
Defence Technology Institute
Pakkret, Nonthaburi, Thailand
titikorn.t@dti.or.th

Abstract*— The best infrastructure security design, the great logging file equipments, the professional incident response teams and forensics teams, the large storages, the strengthen security standards and policies and the new security technologies are not enough to protect the modern computer system and cyber harm. The technology, process and people are the traditional principle for implementation information technology. Nevertheless, these are insufficient for various attacks inventing and using today. The computer system cannot avoid the risk attack certainly. The heart of reinforcement is the knowledge, sharing, integration and trust. Moreover, grouping and correlation are the good methods to be strong in own sector. The hardest is to joint and trust the other because of the business competition, different ideas and social political.

Keywords—Computer Forensics; Computer crime; Cyber security; Central organization; Computer Security Incident

I. INTRODUCTION

The computer crime is occurring and increasing inexhaustible. It has a lot of new techniques which are complicated, violent and hidden. So, the primary purpose of computer crime is making harder to be searched, investigated, examined and arrested.

Computer crime is a type of digital crime which includes a computer system such as hardware, software and network, storage such as hard disk, Random Access Memory (RAM), Read Only Memory (ROM), cache, register and cloud storage, an electronic document and data, networking and social network. The examples of computer crime are child pornography, financial tampering, employee misconduct, fraud, forgeries, intellectual property theft, espionage, cyberstalking, murder, rape, hacking and inappropriate email or internet use etc. [1] Therefore, the computer forensics plays a key role in examination, investigation and support for finding the evidences and going to court. Computer forensics has many techniques and methods. The example techniques are as follows: [2]

1. **Cross-drive analysis:** A forensic technique is used for comparing data or information found on different storage (e.g. hard drives, Secure Digital card or SD card and thumb drives etc.).

2. **Live analysis** or **live acquisition:** This technique is used to collect and make a copy of the existing instances, information and evidences before the devices are shut down. The examiner works with a copy instead of the original one.

3. **Recovery:** Recovery is a basic and common technique for recovering the deleted files by using some forensics software such as file recovery, data recue and boot repair disk.

4. **Stochastic forensics:** A statistic and probability method is used for investigating the relationship between events and evidence activities. The example one is Bayesian probability.

5. **Comparing and looking detailed files (Steganography):** A popular technique used to identifying the hidden data. The principle procedures are searching the modifying file detail or hash by someone and comparing it with the original file.

The examiner uses many techniques with analysis tools to examine a case. The example analysis tool is the forensic software that can review the windows registry, discover and crack the password, extract e-mail or information, review and search the messages and keywords related to the case.

The aims and goals of computer forensics are identifying the cases, preserving the evidences, recovering the disappear data, analyzing the information and presenting the fact to the court. Additionally, the procedures of examination can summarize in 6 steps. The first step is readiness. It is preparing and checking the forensics environment such as training and educating a prepared system to the client, testing and verifying the software or tool and study the law. The second step is an evaluation. The evaluation step includes the receiving and clarifying the instruction, risk analysis, role and resource. The third step is collection. This step involves with the searching, identifying and securing devices which store the document and evidence. These devices must send to the examiner's laboratory securely and safely. The fourth step is an analysis. There are many examination tools but the examiner must take different techniques or be narrow to specific areas. The dual