available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

SoTE: Strategy of Triple-E on solving Trojan defense in Cyber-crime cases

Da-Yu Kao [a], *Shiuh-Jeng Wang* [b], *Frank Fu-Yuan Huang* [c]

[a] *Information Department, Maritime Patrol Directorate General, Coast Guard Administration, Taipei, Taiwan*
[b] *Department of Information Management, Central Police University, TaoYuan, Taiwan*
[c] *The Examination Yuan of R.O.C Taipei, Taiwan 11601*

Keywords:
Cyber-crime
Cyber criminology
Digital evidence
Trojan defense
Triple-E strategy

ABSTRACT

Cyber activity has become an essential part of the general public's everyday life. The hacking threats of Cyber-crime are becoming more sophisticated as internet communication services are more popular. To further confirm the final finding of Cyber-crime, this study proposes three analytical tools to clarify the Cyber-crime issues by means of Ideal Log, M-N model and MDFA (Multi-faceted Digital Forensics Analysis) strategy, where Ideal Log is identified as a traceable element of digital evidence including four elements of IP Address, Timestamp, Digital Action, and Response Message. M-N model applies a formal method for collating and analyzing data sets of investigation-relevant logs in view of connected time with ISP logs. MDFA strategy attempts to outline the basic elements of Cyber-crime using new procedural investigative steps, and combining universal types of evidential information in terms of Evidence, Scene, Victim, and Suspect. After researchers figure out what has happened in Cyber-crime events, it will be easier to communicate with offenders, victims or related people. SoTE (Strategy of Triple-E) is discussed to observe Cyber-crime from the viewpoints of Education, Enforcement and Engineering. That approach is further analyzed from the fields of criminology, investigation and forensics. Each field has its different focus in dealing with diverse topics, such as: the policy of 6W1H (What, Which, When, Where, Who, Why, and How) questions, the procedure of MDFA strategy, the process of ideal Logs and M-N model. In addition, the case study and proposed suggestion of this paper are presented to counter Cyber-crime.

1. Introduction

We are focusing on the new challenge of integrating evidence from multiple sources. In a Cyber-crime investigation, identifying the suspect behind a targeted computer is not as easy as at first glance. Some criminal investigators have assumed that the one committing the crime must be the specific account owner, verified by the Internet Service Provider (ISP) as the original source (Ghavalas and Philips, 2005; Haagman and Ghavalas, 2005). However, further authentication is necessary before such a conclusion may be drawn. The confidence of Cyber-crime investigation is based on the trust of the hardware and software used to collect and analyze the data. The methods used to formulate and test the hypotheses can make the investigation process scientific. This paper tries to construct a better understanding of analyzing Cyber-crime investigation by way of proposing new models. The goal of Cyber Forensics is not only to find out who the offender is, but also to provide supporting evidence in a trial. As the computer-related crimes become global and widespread, it becomes more and more important about the forensic jobs in data recovery, file collection, and information analysis (Brown, 2006). While digital

0267-3649/$ – see front matter © 2009 Da-Yu Kao, Shiuh-Jeng Wang & Frank Fu-Yuan Huang. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.clsr.2009.09.008

examiners tend to focus on specific methods for extracting evidence, Cyber Forensics must be modeled such that it can encompass all types of digital evidence. This is debatable because evidence must be proven to reliably extract and to analyze evidence without bias or modification.

The related works of Cyber-crime and cognitive distortion are discussed in Section 2. Section 3 describes the sample case and Triple-E strategy. The proposed suggestion of Triple-E strategy is further discussed and analyzed in Section 4. The conclusion is drawn in Section 5.

2. Related works

The cyber world is driven by the rapidly changing demands of industry and commerce. It is hard for us to have enough time to respond to Cyber-crime. The main aim of this study is to chart and re-conceptualize the parameters of a contemporary criminological imagination.

2.1. *Cyber-crime*

Cyber-crime consists of two separate elements: philosophy and science. Philosophy is the study of general problems concerning matters such as existence, knowledge, truth, beauty, justice, validity, mind, and language. Science is so well-defined, but philosophy is open ended (Jaishankar, 2007). It is through the successful combination of these two elements that the creation of Cyber-crime issues can be accomplished. Yet philosophy and science differ greatly in their aim and their practice. They are so far apart as to present serious difficulties if their respective qualities are not known to the Cyber-crime analysts. At its core, it blends the subsequent elements with their surrounding situations: the philosophy of Cyber-crime investigation, the science of Cyber Forensics and the integrated theory of Cyber Criminology. The essential part of this issue is briefly presented in this paper; however, its complicated studies are analyzed later.

2.1.1. *The integrated theory of Cyber Criminology*

Cyber-crime is as much a philosophy as a science. The science part of Cyber-crime includes technique and equipment. The philosophic part of Cyber-crime includes the analyst's empirical goals, his vision, inspiration and the use of logic concepts (Jaishankar, 2007). These two parts need to merge seamlessly for the creation of a successful solution to take place. If one or these two parts dominates the other, the result is either a technically excellent decision without much empirical interest, or a very empirical finding lacking technical excellence. Many criminologists consider crime is among several forms of deviance. Criminology has historically played a reforming role with relation to criminal justice system. Its findings that have influenced legislators, law enforcement agents, lawyers, probation officers, and prison officials, prompting them to improve the understanding of crime, criminals, criminal behavior, and the effects of treatment and prevention (Williams, 2006). Little of this research specifically addresses Cyber-crime. The task of this research is to apply these concepts to Cyber-crime. Since the 1990s, academics have observed how the internet has emerged as new media of criminal activity, but criminology has encountered difficulties in its research into the phenomena of Cyber-crime. Cyber criminology is regarded as the scientific study of Cyber-crime, cyber criminals, internet criminal behavior, and corrections. Jaishankar further defines Cyber Criminology as ''the study of causation of crimes that occur in the cyberspace and its impact in the physical space (Jaishankar, 2007).''

2.1.2. *The science of Cyber Forensics*

Nowadays computer technology is commonplace, as are the crimes where the computer is both the instrument of the crime and the location where evidence is stored or recorded. By the early 1990s, specialized tools for computer forensics appeared. As computer technology continued to grow, so did the software of computer forensics or cyber forensics. Most discussions of computer forensics methodologies consist of three basic components (Brown, 2006). They are: (1) acquiring the evidence without altering or damaging the original; (2) authenticating the recovered evidences as being the same as the original; (3) analyzing the data without modification and maintaining its integrity. Cyber Forensics, which means computer forensics on the internet, requires specialized expertise and tools to go beyond the normal data collection and preservation techniques available to end-users or system support personnel. It also requires the proper tools and knowledge to meet the court's criteria, whereas Computer Forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence (Brown, 2006). Cyber Forensics will evolve into a science as more research and standardized procedures are developed. The goal of this paper is to explain the suitable analysis procedure of Cyber Forensics. A large body of proven techniques and methods exists in many traditional forensics disciplines. A standardized process is essential for digital analysts.

2.1.3. *The philosophy of Cyber-crime investigation*

The major purposes of these internet police are fighting Cyber-crime. Their philosophy of Cyber-crime investigation is also similar to each other. The philosophy of Cyber-crime investigation revolves around one important asset: Case Clues. Analysts need to think like an offender and know what information is important to ask for, based on the knowledge of case clues. Common logs, which should be safely stored and accessed, will generally contain details such as Protocol, IP Address, port number, dates and times, and other technical information. Unfortunately, everyday log files don't make for easy reading and tend to fill up expeditiously with millions of lines of impenetrable information (Shifreen, 2006). It is good that there are many programs available that can turn them into meaningful reports. Consequently, the majority of report generators work with the majority of security software, using the industry stand formats or their log files. This is the very beginning of Cyber-crime investigation.

2.2. *Three aspects of cognitive distortion*

Cyberspace is an online forum utilizing advanced technology to provide interactions with others. When society deems informal relationships and sanctions insufficient to create and maintain a desired social order, there may result more formalized systems of social control imposed by a government, or more broadly, by a State. Matthew Williams argues despite the lack of physicality, communities can be formed and maintained in cyberspace. His theoretical framework incorporates Hirschi's social bonding theory, Gottfredson and Hirschi's low self-control theory and Sykes and Matza's techniques of neutralization (Williams, 2006). He believes that perpetrators are less committed to maintaining their online reputation and less attached to the online community. Hence, they are less likely to be involved in conventional activity and less likely to believe and follow community rules. Some related aspects are listed as follows: Deviance Aspect, Law Aspect, and Cognition Aspect.

2.2.1. *Deviance aspect*

Deviance means deviant behavior and attitudes, which differs from a norm or from the accepted social standards. If hackers view cyberspace as a playful site, they tend to utilize the techniques of neutralization to rationalize their deviant acts. These deviant acts are commonly found in cyberspace and include profanity, harassment, vandalism, and obscenity. Various mechanisms are employed to regulate behavior, including rules codified into laws and other policies designed to prevent crime. The label of crime and the accompanying social stigma are normally reserved for those activities that cause serious loss or damage to individuals. A normative definition views crime as deviant behavior that violates prevailing norms – cultural standards prescribing how humans ought to behave normally. Deviance describes behaviors that violate cultural norms including formally-enacted rules (e.g., Cyber-crime) as well as informal violations of social norms (e.g., anonymous login). It is the remit of criminologists to study how these norms are created; how they are enforced; and how they change over time (Williams, 2006).

2.2.2. *Law aspect*

Law violators are regarded as evil or wicked people. Crime is a violation of societal rules of behavior as interpreted and expressed by a criminal code for which some governing authority or force may ultimately prescribe a punishment. Legislatures pass laws that define crimes which violate social norms. These laws vary from time to time and from place to place. Not all breaches of the law, however, are considered crimes, for example, breaches of contract and other civil law offences. Individuals who violate these rules are subject to sanctions by state authority, social stigma, and loss of status (Williams, 2006). Most kinds of Cyber-crime involve unauthorized access to computer systems. Countering such intrusion in Taiwan took a major footstep forward in June 2003 with a number of amendments, and the addition of an entirely new Chapter 36 to Taiwan's Criminal Code.

2.2.3. *Cognition aspect*

The effect of crime prevention treatment is deeply influenced by the cognition. In dealing with Cyber-crime issues, the teachings of knowing right from wrong can bring new light to bear on the difficult issues of conflict and crime in the community. This offers grounding principles to deal with them. To have a better understanding on this cognition aspect, this section discusses the differences among the following issues (Kao and Wang, 2009; Kizza, 2003): (1) Ethics and Crime; (2) Right and Wrong; (3) Cognitive Distortion.

2.2.3.1. Ethics and crime. Crime seems closely intertwined with ethics. Ethics encompasses right conduct, good life, and common conception of analyzing right and wrong. If the criminal truly appreciated and was sympathetic to the mental and spiritual consequences of his actions, he would neither commit nor even consider committing them. Ethics has something to do with the concepts of right and wrong. This word deals with the customs in which people do things.

2.2.3.2. Right and wrong. Every society has a broad set of regulations that define proper behavior for teenagers. These expectations take such forms as rules, codes, cultures, subcultures, and laws. Under some circumstances many behaviors, which are declared to be crimes by criminal codes, could be considered legal or ethical.

2.2.3.3. Cognitive distortion. Sometimes, we all have fallacious ways of thinking that result in us drawing incorrect and often limiting conclusions. To some extent, these mistakes are inevitable as our map of reality is inherently fallible. Cognitive distortions are logical, but they are not rational. They can create real difficulty with someone's thinking. The following 10 distortions are measured to rate somebody from one to ten with one being low and ten being high (Kizza, 2003).

- All-or-nothing thinking
- Overgeneralization
- Mental filter
- Disqualifying the positive
- Jumping to conclusions
- Magnification and minimization
- Emotional reasoning
- Making 'should' statements
- Labeling
- Personalization

3. Case study

3.1. *Sample case*

Aaron Caffrey, 19-year-old, was acquitted in the United Kingdom on charges of hacking into the computer system and crippling the server in September 2001. Although authorities traced the hack back to Caffrey's computer, he said that someone must have remotely planted a Trojan program onto his computer that did the hacking and that could have been programmed to self-destruct (Ghavalas and Philips, 2005). Someone could use the machine, either by gaining physical access or remotely installing Trojan software onto the computer. His attorney successfully argued that Trojan programs found on their computers were to blame.

In Trojan Defense, the accused claimed that an unknown 3rd party had installed a Trojan horse program onto his computer, carried out the attack from his computer and subsequently deleted all traces of the Trojan on the PC (Garfinkel, 2007). The Trojan Defense, which means that "the computer did it,'' is a valid one because computer hijacking occurs all the time and savvy hackers can easily cover their tracks. The defense is likely to become more widespread especially given the increasing use of Trojan programs that can be used by hackers to steal passwords and essentially eavesdrop on a computer user. Hence, investigators must make more efforts to include all relevant findings. Once a computer is infected with a Trojan, it is difficult to predict the possible effects. It often becomes a trouble for the court to decide whether or not unknown intruders had gained control of defendant's computer and used it as a platform from which to launch the attack against the victim.

3.2. *Triple-E strategy*

Some evidence is stored or recorded by computer technology. Digital evidence is no longer a terrible mess because some rules and procedures are explored to find out the truth. The solutions of Trojan Defense are discussed in Triple-E strategies (Kao and Wang, 2009; Kessler, 2007): Education, Enforcement and Engineering. Each strategy is further analyzed by some questions, which are based upon criminology, investigation and forensics.

3.2.1. *Education viewpoint: crime prevention from corrections and criminology*

3.2.1.1. Why is it difficult to reduce recidivism among hackers? The internet community has been addressing the unethical behavior for years; however, it is insufficient when handling hacking offenses. The help of Cyber Criminology may provide guidance towards a better society. One of the concerns is to find out how to reintegrate and re-enter hackers into the community, and avoid failure. However, applying this approach to reduce recidivism among computer hackers requires a great deal of time and effort.

3.2.2. *Enforcement viewpoint: fact finding from prosecution and investigation*

3.2.2.1. Can we solve the most complicated investigation in Cyber-crime? Software applications are often designed for convenience. This situation may result in little Cyber-crime control on computer systems. Network hacking cases are some of the most complicated and arduous investigations in Cyber-crime. Each event has its own unique characteristics and features. The strategy we propose may act as a good model against Cyber-crime for handling related crime issues on the basis of experience transfer in the case of Trojan Defense.

3.2.3. *Engineering viewpoint: target authentication from science and forensics*

3.2.3.1. How can we trust the past logs? Investigators cannot always trust server logs as far as an intrusion case is concerned. The past logs are not definite proof. It still pains investigators to see the compromised system suffer like that. The logs' ability to aid law enforcement agents would be minimal if they did not possess these traits. The consensus of opinion is that logs are not proper for definite proof particularly because of the easy alterations that can take place.

4. Discussions and analyses

The intricate circumstances of Cyber-crime cases provide a context in this qualitative case study, which is conducted from an interpretive perspective. This paper aims to provide a possible and workable solution to criminologists, law enforcement agents, system administrators, computer security professionals, legal professionals and students of computer investigators. The Cyber-crime issue of this paper is mainly discussed and presented in the following parts (Garfinkel, 2007): Anti-forensic challenge, Analysis method, and Proposed suggestion.

4.1. *Anti-forensic challenge*

Computer Forensics, Digital Forensics or Cyber Forensics is a new discipline that uses scientific knowledge for collecting, analyzing, and presenting evidence to the courts. The related computer forensic tools assist forensic examiners by collecting information from a computer system; making a true and permanent copy of that information, so that it can be used in a legal proceeding; and analyzing data to uncover information that may not be immediately obvious. However, Anti-Forensics (AF) is a growing collection of tools and techniques that frustrate forensic tools, investigations and investigators. Although some AF tools have legitimate purposes, these tools still may be abused. Some primary goals for AF are listed below (Brown, 2006; Garfinkel, 2007; Kao and Wang, 2009):

- Avoiding detection of what has taken place on a case
- Casting doubt on a forensic report or testimony.
- Disrupting the collection of information.
- Forcing the forensic tool to reveal its presence.
- Increasing the time procedure that an analyzer needs to take.
- Leaving no evidence after an AF tool has been run.
- Subverting the results of forensic tools.

4.2. *Analysis method*

An effort to devise best practices in the broadest knowledge context is the process of generating value from intellectual and knowledge-based assets. The information management of criminal event has become increasingly significant in the knowledge-based society. Intellectual management of verification knowledge is a fundamental factor behind an internet investigation's success, which is founded on a continuous analysis of understanding log-related evidence. Therefore, there is a growing starvation for investigators who have the application of a knowledge management strategy and tell the meaning of every internet connection from its context. To help analysts figure out Cyber-crime issues and construct the possibilities of correction and corrections, this section proposes the following analytic discussions (Brown, 2006; Kao and Wang, 2009): Ideal Log, M-N model, and MDFA (short for Multi-faceted Digital Forensics Analysis) strategy.

Table 1 – Auditing Logs in Cyber-crime Investigation

Knowledge management	Four elements	Type
Explicit knowledge: trace back to the suspect's location	IP Address	● Role: static, dynamic, or proxy ● Location: intranet or internet
	Timestamp	● Time zone, daylight saving time, M-N Model examination
Tacit Knowledge: Accurately Describe The Sequence Of Events	Digital action	● File: program, document or others ● Direction: upload or download ● Method: create-access-modify timestamp ● Operation: human or program ● Signature: abnormal behavior
	Response message	● Status: success or failure ● Examination: MDFA strategy

4.2.1. *Ideal log*

Ideal Log examines the problem-oriented action and considers how that action is constructed from the collection of enough relevant data. Intellectual and knowledge-based assets among auditing logs fall into one of two categories in Table 1: explicit or tacit. Explicit knowledge refers to information that indicates where the suspect locates from the clues of IP address and timestamp. Another concept of tacit knowledge is to make sure what really happens from the clues of digital action and response messages. There is often enough information to place complete reliance on the judgment of cyber mystery. The tacit challenge for investigators is figuring out the know-how contained in what really happens. The following subsections describe these ingredients employed to date in cyber events.

4.2.2. *M-N Model*

The M-N model focuses on timestamp, and is named for its path. 'M' signifies the forward path, which traces from the client to the server. Three records are stored on different hosts. These are shown in Fig. 1 as timestamps for login records (N_{1i}, N_{2i}, and N_{3i}), and for logout records (N_{3o}, N_{2o}, and N_{1o}). 'N' represents the period of login and logout, and each contains the above two parts. These are also shown in Fig. 1 as client (N_{1i} and N_{1o}), intermediate (N_{2i} and N_{2o}), and server (N_{3i} and N_{3o}). Verification problems of internet logs have emerged during expert witness testimonials in several high-profile cases. This M-N Model applies a formal method for collating and analyzing data sets of investigation-relevant logs. The nature of this approach suggests substantial benefits from using the business-oriented ISP logs as a critical reference point for the intelligence analysis of log verification.

Fig. 1 shows a general sequence of events based on information collected at every stop along the routing chain and assuming all nodes on the chain have a synchronized time reference. The leftmost events in each pair are referred to as login times and those on the right as logout times. Fig. 1 suggests that the time relations for the time slots in time protocol (TP for short) location of base time line (BTL for short) can be expressed by the inequality.

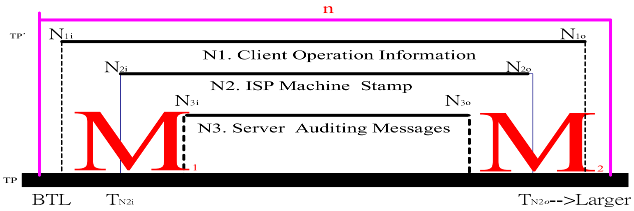

Fig. 1 – M-N Model on Diverse Locations.

$$T_{N1i} < T_{N2i} < T_{N3i} < T_{N3o} < T_{N2o} < T_{N1o} \quad (1)$$

and

$$\Delta N_3 < \Delta N_2 < \Delta N_1 \quad (2)$$

are both satisfied.

The Sequential Inequality (1) and Period Inequality (2) can be further analyzed by four propositions of M-N Model (see Table 2). Because it takes finite time to setup connections, event times on various hosts cannot be equal. Further, the delays introduced will increase as the distance increases, the Sequential Inequality (1) is reasonable to assume an event sequence of: T_{N1i}, T_{N2i}, T_{N3i}, T_{N3o}, T_{N2o}, and T_{N1o}. It should be noted, however, that although the ISP systems will generally operate on a reliable time base, there is less likelihood that will be the case for N_1 and N_3. That is, the inaccuracies between computer clocks complicate the task of putting them into sequence. It is essential to synchronize those asynchronous values to TP location. That is where the substance of M-N model lies. Each login period of the server auditing messages ΔN_3 is the shortest one, and the connection period of the client operation information ΔN_1 is longer than that of the intermediary machine stamp ΔN_2. The coefficient Period Inequality (2) ensures that any discrepancies can be resolved.

Four possible propositions are considered and illustrated in Table 2, where in the first and third of these propositions, the suspect is inferred to be guilty. To ensure the quality and comprehensiveness of evidence collection, this methodology may help to clarify the issue at hand and retain most of the useful information. Rationalization comes from the philosophy that just as an innocent suspect does not deserve to be blamed with a crime; neither should an unreliable log put the suspect in the wrong. This model shows how effective evidence management and systematic reconstruction of a crime scene can help create a more exhaustive prospect of the linking analysis between internet perpetrators and their illegal activities. Further assistance of the M-N model and Ideal Log can be offered to know how to follow the truth and to retort on Trojan Defense with confidence.

4.2.3. *MDFA strategy*

It is insufficient to check the computer without considering the four-dimensional phase of MDFA strategy in Fig. 2. This

Table 2 – Four Propositions in M-N Model.

Proposition analysis	Sequential inequality (1)	Period inequality (2)	Situation	Correction procedure	Result
1	TRUE	TRUE	Normal case	Unnecessary	Reliable/guilty
2	TRUE	FALSE	Staged Information in Server/ Client (In Opposition to the Lemma)	Unnecessary	Unreliable/ innocent
3	FALSE	TRUE	Without Synchronization	Necessary	Reliable/guilty
4	FALSE	FALSE	Staged Information in Server/ Client (Time Inconsistencies)	Unnecessary	Unreliable/ innocent

MDFA model focuses on extracting characteristics in view of four phases, Evidential Phase (Evidence), Forensic Phase (Scene), Suffering Phase (Victim), and Behavior Phase (Suspect). In every criminal event, each of these areas is important and necessary components that need to be connected and communicated.

4.2.3.1. *Part I: evidential phase*. The potential existence of evidence must be handled in a scientific manner. Because the digital process is very critical in the forensic domain, proper care must be taken in the collection of evidence to ensure that the content of digital data is preserved for the formal court proceedings. Examining and analyzing Cyber-crime depends on the nature of the investigation and the amount of data that investigators have to process. Appropriate amounts of time and resources are needed to extract, analyze, and present all the evidence.

4.2.3.2. *Part II: forensic phase*. A crime scene is the location where a criminal event took place, and may contain evidence of that crime. It is that area from which most of the evidence is retrieved and examined by forensic scientists. The scene of a crime is delicate, and carelessness when dealing with evidence may be disastrous for a criminal investigation.

4.2.3.3. *Part III: suffering phase*. Recent years have seen an increased interest in the role of the victim for criminal activities. Most victims are expected to fend for themselves, and society accedes to this arrangement. As far as Cyber-crime is concerned, the original clues often come from the victim.

4.2.3.4. *Part IV: behavioral phase*. The complexity of criminal behavior is related to the psychology of the criminal. A criminal's personality is involved, combined with his actions before, during, and after the crime. Some actions are voluntary; others are involuntary. The explanation of this behavior can be used, or not used, for identifying the perpetrator of a crime. Fact-finders can evaluate if the behavior is usable simply by using common sense and technical knowledge. The behavioral field is useful to examine its scope and its status.

4.3. *Proposed suggestion*

As far as those hackers are concerned, general offender characteristics do not seem to be as diversified as other forms of criminal offenses. Technology is a primary interest of hackers, and that leads them to focus on learning technology at a profound level. They are also able to justify the exchange of information with law-breaking potential as long as it was given for the purpose of educating others. The proposed

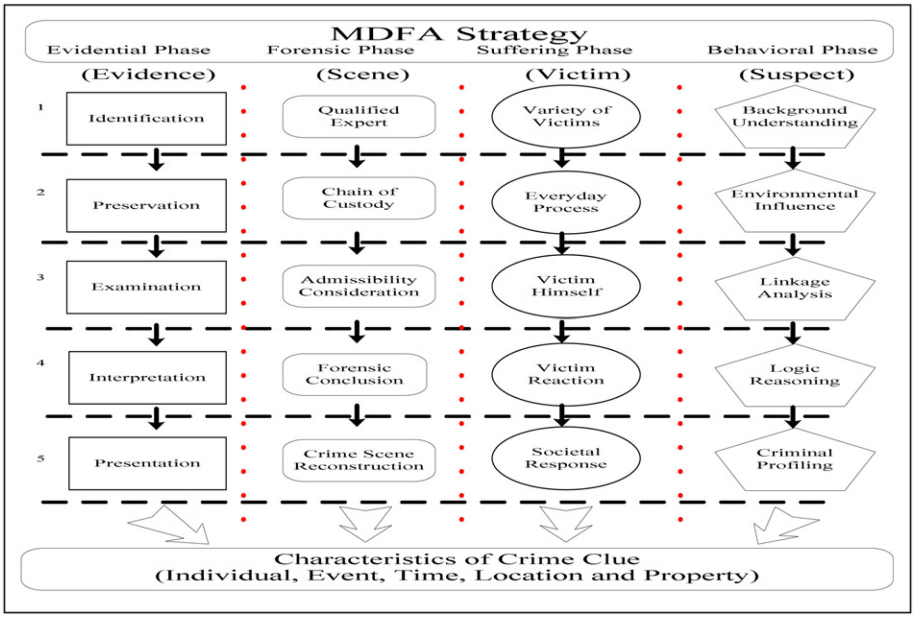

Fig. 2 – Theoretical structure of MDFA strategy.

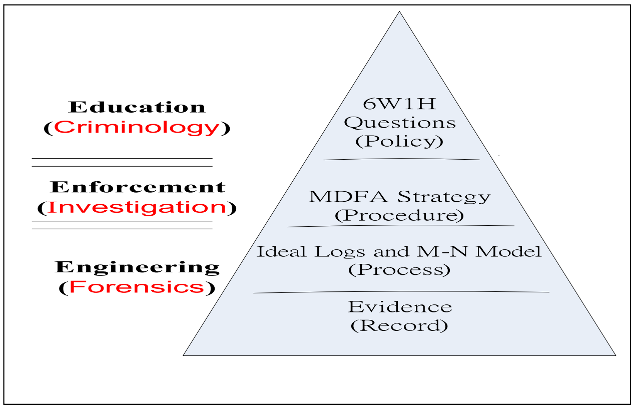

Fig. 3 – The Utilization of SoTE.

suggestions of the Triple-E Approach are listed below (Kao and Wang, 2009; Kessler, 2007; Kizza, 2003).

4.3.1. The Triple-E approach of internet calming.
In recent years, problems related to road traffic safety have been addressed through three important activities: Education, Enforcement, and Engineering. The concept of the comprehensive Triple-E approach suggests application to examples of successful cases from internet safety programs around the country (Kao and Wang, 2009). As in the nation's roadways, the goal is to increase safety on the internet and reduce the number of hacking activities and consequent property damage. In the theoretical structure in Fig. 2, this study proposes a use of the MDFA strategy to help investigators probe for missing information. To further reorganize the findings of this paper, Fig. 3 illustrates a Triple-E approach to explain our findings. We cannot solve the Cyber-crime problem with just one or two of the three elements. This is done by working all three elements together with key stakeholders to:

(1) Reduce incidents
(2) Reduce help from Cyber-crime events
(3) Create a safer internet
(4) Raise the profile of internet safety in the community

To have a clear viewpoint of a Cyber-crime event, the utilization of Triple-E strategy is illustrated in Fig. 3, which is divided into four-layer viewpoint and is subject to continuous, systematic review and improvement. Continuity plans, detective actions, open-minded observations, and reporting reflections are fundamental to this framework. The 6W1H (short for What, Which, When, Where, Who, Why, and How) questions for each of these layers are contained in the following discussions and are supported by specific evidences. The principles behind this paper are proposals to consider four layers, defined thus:

4.3.1.1. The normative requirements of 6W1H question policy. This 6W1H policy statement defines a general direction or intention. The 6W1H questions statement expresses investigators' commitment to the implementation of fact finding. Facts are pieces of information that can be independently verified by generally accepted methods. Fact finding is an extremely important component of the investigation process which presents its special set of problems to increase the constructiveness of intractable conflicts.

4.3.1.2. The informative procedure of MDFA strategy. The procedures, which are mentioned in MDFA strategy, control the later processes in verifying the auditing log activities. A well-defined procedure controls a logically distinct process or activity, including the associated inputs and outputs of digital logs. More discussions are necessary in the four phases of MDFA strategy.

4.3.1.3. The ideal log in M-N Model. general, a process uses resources to transform inputs into outputs. In every Cyber-crime case, inputs are turned into outputs because some kind of activity is carried out. Those activities are processed among a group of computer on the internet. The proposed M-N model uses the inequalities of sequence and period to deal with the auditing logs, which are recorded among connected computers. To identify machines and the people behind them, it is also helpful to distinguish between the real and forged information which is contained in audit logs. The original log information cannot be trusted except for the identified action

Table 3 – SoTE on Cyber-crime.

Tier	1	2	3
SoTE	Education	Enforcement	Engineering
Field	Criminology	Investigation	Forensics
Role	Integration	Philosophy	Science
Purpose	Crime prevention	Fact finding	Target authentication
Method	Teach them right from wrong	Reconstruct the fact from diverse viewpoints	Arrest the criminals from solid evidences
Focus	Do/does not think	Dare not attack	Cannot fulfill
Topic	6W1H Questions (Policy)	MDFA strategy (Procedure)	Ideal Log and M-N Model (Process) Evidence (Record)
Effect	(1) Distribute a safe internet behavior. (2) Implement a public awareness campaign. (3) Observe the feeling of shame.	(1) Explore aggressive attacks. (2) Compare illegal offenses. (3) Construct a holistic view.	(1) Enable some elementary data for scientific consideration. (2) Synchronize the timestamp issues. (3) Conduct an audit examination or cross examination.

or user which is confirmed from other logs located at different network system. Existing logs and log comparison are required in the M-N model. Logs can be anywhere in between. A general log could contain the essential parts to recognize the identity of the person. An Ideal Log defines the information that should be recorded, and explains why it should be recorded under what circumstances. While certain information may be documented or undocumented, the M-N model expects the information of Ideal Log to be documented for the later identity of the source computer.

4.3.1.4. *Baseline records of evidence*. Evidence is one of the most important parts in finding the fact, which should be based on existing digital records. A record is a document that contains objective evidence. It shows how internet activities are being performed or what kinds of results are actually being achieved. It always documents what has happened in the past. Records can take any form or use any type of digital medium. The focus of this study is therefore on the relationship between the compliance requirements determined by the former four-layer, and some discussions among these relationships are also necessary to clear their relationship in any unclear events.

4.3.2. *Strategies and activities*

Because of their major financial, environmental and/or social impacts, most Cyber-crime problems cannot be solved through enforcement (arrests) alone. The strategy for attacking the problem constitutes a multi-disciplinary effort. In Table 3, the SoTE is discussed and analyzed from three tiers. SoTE in Table 3 is proposed to observe Cyber-crime from the viewpoints of Education, Enforcement and Engineering. That approach is further analyzed from the fields of criminology, investigation and forensics. Each field has its different focus in dealing with diverse topics, such as: the policy of 6W1H questions, the procedure of MDFA strategy, the process of Ideal Log, and M-N model.

4.3.2.1. *Education*. Education approach is considered from the Cyber-crime understanding of criminology, which focuses on the possibility of theory integration on hackers. Public education can be an effective method to help change the attitude and behavior of hackers. Educational efforts aim at addressing awareness that the hackers' actions will ultimately prevent them from achieving their goals of fun, profit or respect. The stopping re-offending focus of "Do/Does not think" has tried to be formed on the offender side and that is followed up by the investigative policy of 6W1H Questions. This policy helps investigators to have a complete view of Cyber-crime events, and prevents offenders from lying. Education increases public awareness by reinforcing safe internet habits. In addition to general school education, companies, educational institutions and the public media may be able to promote responsible computer usage policies, even at home. The effect is expected to:

- Distribute a safe internet behavior.
- Implement a public awareness campaign.
- Observe the feeling of shame.

4.3.2.2. *Enforcement*. Enforcement approach focuses on the field of investigation, the role of philosophy, the purpose of fact finding, and the method of reconstructing the fact from diverse viewpoints. Increased levels of law enforcement agents may discourage hackers from breaking the law and penalize those who do. The stopping re-offending focus of "Dare not attack" is tried on the offender side and followed up by the procedure of MDFA strategy. This procedure is examined from diverse viewpoints. Some multi-agency efforts of enforcement can be used include:

- Explore aggressive attacks.
- Compare illegal offenses.
- Construct a holistic view.

4.3.2.3. *Engineering*. Engineering approach focuses on the field of forensics, the role of science, the purpose of target authentication, and the method of arresting the criminals based on solid evidence. The stopping re-offending focus of "Cannot fulfill" is tried to on the offender side and followed up by the process of Ideal Log and M-N Model. This process emphasizes the importance of evidential records and the comparison between diverse logs. The engineering measures include:

- Enable some elementary data for scientific consideration.
- Synchronize the timestamp issues.
- Conduct an audit examination or cross examination.

5. Conclusion

The identity of a Cyber-crime may not be immediately apparent. Hackers may take time to mask their identity, cover their tracks, or conceal their communication content. To identify the suspect, it still takes pain to fulfill this task. The researcher tries to reconstruct some ideas in SoTE on Cyber-crime. To clarify the myth behind timestamp issues and make sure which computers are used by the hacker, this research starts a fact finding investigation of Cyber-crime from timestamp issues, observing the relevant clues from the viewpoints of Ideal Log and M-N model, and collecting the timestamp issues of sequence and period. Then the target authentication of logical consideration may aid forensic investigators in piecing together in related logs. To have a better understanding of offenders' Anti-Forensics technique and find out who is the hacker, this research utilizes the MDFA strategy to find facts. The method of 6W1H questions also helps us to have a whole view in offender identification. In conclusion, a solution found in Fig. 3 can create a whole view of Cyber-crime by way of action research in fact finding, which is suitably utilized in investigating Cyber-crime.

Acknowledgments

This research was partially supported by the National Science Council of the Republic of China under the Grants NSC 98-2221-E-015-001-MY3-.

Da-Yu Kao *Information Department, Maritime Patrol Directorate General, Coast Guard Administration, Taipei, Taiwan 25155.*

Shiuh-Jeng Wang *(sjwang@mail.cpu.edu.tw) Department of Information Management, Central Police University; TaoYuan, Taiwan 33304.*

Frank Fu-Yuan Huang *The Examination Yuan of R.O.C Taipei, Taiwan 11601.*

REFERENCES

Brown CLT. Computer Evidence: Collection & Preservation. Charles River Media Inc.; 2006.

Garfinkel S. Anti-Forensics: Techniques, Detection and Countermeasures. The 2nd International Conference on i-Warfare and Security (ICIW). Naval Postgraduate School; March 2007.

Ghavalas B, Philips A. Trojan defense: a forensic view part II. Elsevier Ltd. Digital Investigation Journal June 2005;2(2): 133–6

Haagman D, Ghavalas B. Trojan defense: a forensic view. Elsevier Ltd. Digital Investigation Journal February 2005;2(1): 23–30

Jaishankar K. Cyber criminology: evolving a novel discipline with a new journal. International Journal of Cyber Criminology 2007;1(1).

Kao DY, Wang SJ. The IP address and time in cyber-crime investigation. Policing: An International Journal of Police Strategies & Management 2009;32(2):194–208.

Kessler GC. Anti-forensics and the Digital Investigator. In: Proceedings of the Fifth Australian Digital Forensics Conference. Edith Cowan University; December 2007.

Kizza JM. Ethical and Social Issues in the Information Age. 2nd ed. Springer; 2003.

Shifreen R. Defeating the Hacker: A Non-technical Guide to Computer Security. John Wiley & Sons Ltd; 2006.

Williams M. Virtually Criminal: Crime, Deviance and Regulation Online. Routledge Publisher; 2006.