A Survey of Digital Evidences Forensic and Cybercrime Investigation Procedure

Jia-Rong Sun[1], Mao-Lin Shih[2], Min-Shiang Hwang[1,3]
(Corresponding author: Min-Shiang Hwang)

Department of Computer Science and Information Engineering, Asia University[1]
(Email: mshwang@asia.edu.tw)
Department of Financial and Economic Law, Asia University[2]
No. 500, Lioufeng Rd., Wufeng, Taichung 41354, Taiwan
Department of Medical Research, China Medical University Hospital, China Medical University[3]
No. 91, Hsueh-Shih Road, Taichung 40402, Taiwan
(Received Jan. 5, 2015; revised and accepted Apr. 10 & May 2, 2015)

Abstract

Due to the development of networks, cybercrime has many crime types, including network attack, mail fraud, intimidation, copyright infringement, and so on. For network attacks, many approaches have been proposed and used to detect and defense. However, after the network attack is confirmed or other crime exists, it still need to execute the investigation procedure by the investigators, collect the evidences related to the crime, find the perpetrators, and prosecute them. Therefore, in this paper, we collect the researches of investigation procedure of cybercrime in the recent years. By introducing the research investigation procedure of these papers, we will discover the features of every procedure. Then we compare these investigation procedures via the traditional investigative procedures compatibility, cybercrime behavior analysis, evidence forensic procedures, case analysis and verification, the methods of evidence collection and analysis, and the area of judicial jurisdiction. Finally, we will propose the viewpoints of cybercrime investigation and forensic procedures, and we wish this paper will help the research of investigation and forensic procedures.

Keywords: Cybercrime, digital evidence, forensic procedure, investigation procedure

1 Introduction

In the recent years, many approaches used to detect the network attacks have been proposed [9, 11, 14, 20, 21, 22, 28, 29, 30]. By using these approaches, we can detect the network attack occurring, and defense the attacks. However, after the network attacks occurred, these attack events will be called cybercrime. Investigating these cybercrimes not only pursue the liability of criminal, and also combine the detection approaches to become an investigation strategy of cybercrime, reducing the damage from same criminal behavior.

In the cybercrime, the investigation procedures can be divided into two main parts, digital evidence forensics process, as well as cybercrime investigation procedure. In the cybercrime cases, since the properties of evidence unnecessarily exist at the entity type, perhaps they are digital data and stored in the data storage devices. The existence locations of digital evidence will be different because of the type of crime. For example, in wireless networks of cybercrime, digital evidences will exist in the record of a computer and network equipment in the offenders and the victims [35]; in the net-work attacks, digital evidences will exist in the ISP server and the computers of offender [16]. The digital evidence collecting aims to find any evidences related to cybercrime, and preserve these evidences to avoiding the digital evidences were forged, altered, deleted or destroyed. The purpose of digital evidence collected is to investigate the process of cybercrime occurred. Therefore, the process how to find the digital evidences and the perpetrators is called a criminal investigation procedure. And the criminal investigation procedure includes the procedure of forensics evidence. When a cybercrime is occurred, collecting the digital evidences, proving the existence of criminal behavior, finding identify of suspects, and proving the causation are called the cybercrime investigation procedure. In the following, we will define the cybercrime, investigation procedure, and the nature of digital evidence.

1.1 The Definition of Cybercrime

The cybercrime is a social problem derived from the social development. In [12], the cybercrime is defined to a 'digital' or 'hi-tech' crime type, or uses network technology as the primary or secondary tools of crime [3, 23, 27, 31, 34]. In [33], the authors consider the difference between tradi-

tional crimes and cybercrimes is the evidences of cybercrime scene belonging to an electronic format. In Taiwan, the cybercrime is also defined in the Criminal Code definition of a computer crime in Chapter 36 of the legislative purpose. In the broad sense, the computer crime refers the crime tool or process to involve the computer or Internet; in the narrow sense, the signification of computer crimes referring to the criminal objects of attack are the computers or Internet. In summary, we consider the cybercrime must use some tools to connect Internet, and carry out the illegal behaviors of offense. The evidences of this cybercrime produced has a part belonging to the digital evidence, and no fixed location of the crime, and the offender and victim does not need to face each other directly.

1.2 The Property of Digital Evidence

The type of evidence can be divided into witnesses, physical evidence and documentary evidence. The witnesses are an evidence of personal experience, but does not include speculation. The witnesses includes witnesses, victims, defend-ants or expert testimony; the physical evidence refers an object or state which can be used to prove facts of the crime, such as the tools of crime; documentary evidence refers to the content of a file which can be used as evidence, such as written report of victims. Furthermore, there is some evidences including both characteristics of documentary evidence and physical evidence, which is the evidence of cybercrime. The evidence of cybercrime belongs to a new type of evidence, called Digital evidence [4, 5, 6]. The witnesses may be changed with time or interfered by other factors, and the physical evidence and documentary evidence is relatively easy to leave the traces of modification. Therefore, under the normal circumstances, the probative force (i.e. credibility) of physical and documentary evidence are higher than witness evidence. Digital evidence is stored in data storage devices generally [33] via the electromagnetic record type, and the content of digital evidence can be understood through printing, playing, and execution, etc. From the foregoing, the digital evidence has both characteristics of physical evidence and documentary evidence. In addition, since the digital evidence exists by the electromagnetic record, it has the following features: easy to modify and copy [1, 4, 33], hard to understand the content directly without the conversion process [4, 7], and not easy to retains the original state [1, 4, 33].

1.3 The Definitions of Investigation Procedure

The difference countries have their own judicial investigation procedures based on the law of themselves [13, 26]. In Taiwan, the crime investigative procedures are prescribed in the Criminal Procedure Law. The purpose of these procedures are to investigate the facts of crime, collect evidence, find the suspects, and arrest the suspects. In addition, the types of criminal cases are divided into public prosecution and private prosecution in Taiwan, and this classification will affect the start of investigation procedure. The public prosecution event needs the victims to report the crime event to police or the judiciary to accept this criminal case; private prosecution event refers that the crime does not need to wait the report of victim, and the judicial investigators can investigate this types of crime case actively. These two types will affect the investigation procedure is started actively or passively by the judicial investigators. The start of investigation must be a legal process, otherwise this case will not be accepted by the court after the prosecution. When the investigation procedure is initiated legal, the suspects will be found via the evidences of legal collect. After summoning and asking the suspects, the innocent people will be released and the criminal will be arrested. Finally, the criminal will be prosecuted.

In this paper, we collect and survey the papers of cybercrime investigation procedures from different countries in re-cent years. First, we will introduce the architecture, processes, and forensics procedures of these investigations. Then we will compare these investigative procedures, including the traditional investigative procedures compatibility, cybercrime behavior analysis, evidence forensic procedures, case analysis and verification, the methods of evidence collection and analysis, and the area of judicial jurisdiction. Finally, we will propose the viewpoints of cybercrime investigation and forensic procedures, including the digital evidence forensic and the investigation procedure. This paper is organized as follows. In Section 2, we will introduce the proposed approaches of investigation procedures and evidence forensic in cybercrime; in Section 3, we will compare each investigation procedures, and propose our viewpoints of cybercrime investigation procedures; finally, we will draw our conclusions in Section 5.

2 The Survey of Cybercrime Investigation and Forensics Procedure

Cybercrime is a crime type produced from the development of Internet. According to the definition of cybercrime, the evidences of cybercrime include digital evidences, cybercrime has no fixed location of the crime, and the offender and the victim of cybercrime do not need to face each other directly. Therefore, the content of cybercrime investigation procedure must contain the methods including to find the real perpetrators, digital evidence forensic, and analysis of crime. In addition, the investigators is not limited to use only one method in the cybercrime investigation, and they will use many methods to collect evidences and identify the perpetrators as long as the methods is not illegal. Therefore, if these are proposed cybercrime investigation procedures, they can be used to

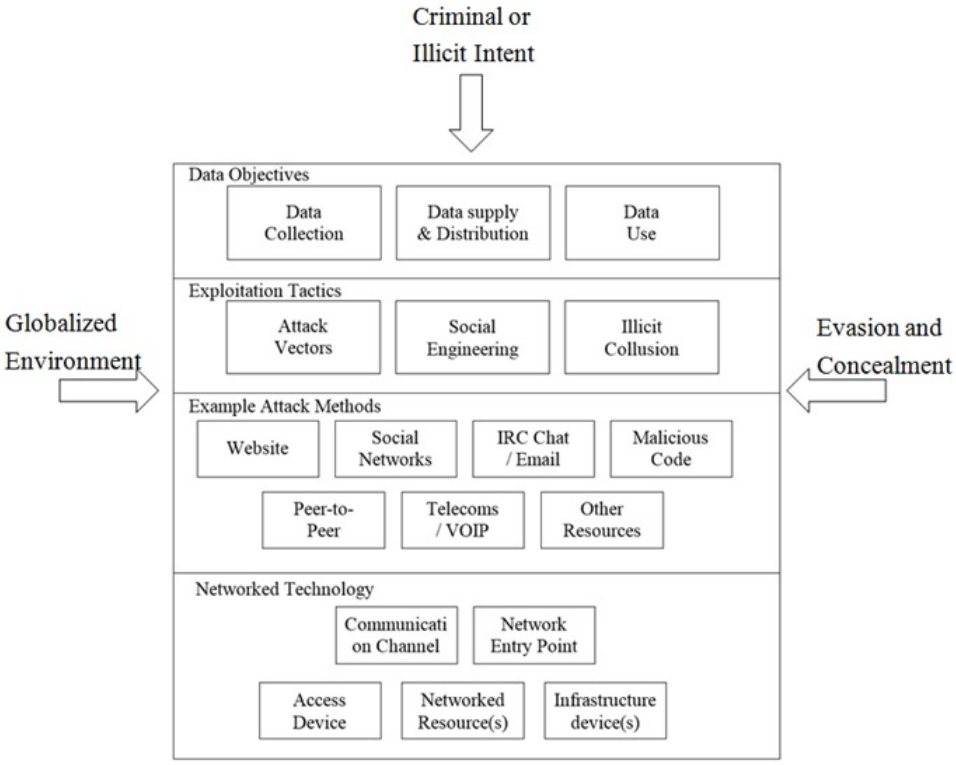

Figure 1: The cybercrime execution stack

find the real perpetrators, collect evidences, and analyze the method of cybercrime, so this procedure will be referenced and used by the investigators. In the following, we will describe the proposed cybercrime investigation procedures.

2.1 The Growing Phenomenon of Crime and Internet

In this paper [12], the authors proposed and defined a cybercrime execution and analysis model. The purpose of this paper is making the conventional policing models more easy use to investigate cybercrime, and help the investigators plan investigations. The investigation of cybercrime model is defined to a Cybercrime Execution Stack in this paper. This model is affected by three factors, including Criminal or illicit intent, Globalized Environment, and Evasion and Concealment [12]. In the different countries, the Criminal or illicit intent of cybercrime is stipulated in their own criminal law, and it will affect whether the offense is founded or not. The factor of Globalized Environment will affect the extent of offense in different countries. If a cybercrime crosses several area of judicial jurisdiction, the extent of offense may be different, or violate the different codes of law. Since the Internet has anonymity, the behavior of evasion and concealment in the crime will increase the difficulty of crime investigation and information collection. Therefore, the evasion and concealment of cybercrime also are the one of affection factors in cybercrime investigation. In the Cybercrime Execution Stack, as the Figure 1, it has 4 main stacks, including Data Objectives, Exploitation Tactics, Example Attack Methods, and Networked Technology [12]. According to the basic function of network technology, Data Objectives can be divided into groups: data collection, data supply and distribution, and data use [12]. The cybercrime tactics will be found out from the target type of attacks and the criminal behavior. Therefore, in the Exploitation Tactics it includes three groups: Attack Vectors, Social Engineering and Illicit Collusion. In the above Exploitation Tactics, it can produce lots of different attack methods, and the Attack Vectors include malware, Trojans, spyware, worms or viruses; Social Engineering includes impersonation, email, phishing, blogs or social networking; Illicit Collusion includes private websites, email, Internet Relay Chat (IRC), Peer-to-Peer data sharing. Finally, the Networked Technology is used to find and collect the evidences and information of cybercrime. These technical characteristics is communication channel, network entry point, access device, network resources, and the infrastructure devices.

2.2 The Stages of Cybercrime Investigations

In [13], the authors combine the Cybercrime Execution Stack [12] and the investigations stages from the investigation process of law enforcement to a compound procedure of cybercrime investigation (See Figure 2) [13]. The purposes of this investigation procedure are to establish

the connection of Cybercrime Execution Stack and law enforcement investigation, and bridge the gap between technical and non-technical investigation. In the technology side, the authors refer the Cybercrime Execution Stack, and use this stack as the technology of investigate cybercrime. This investigation procedure has four phases: Initiation, Outcome, Cybercrime Execution Stack, and Law enforcement investigation process. The Cybercrime Execution Stack includes four stages: Data Objective, Exploitation Tactics, Attack Methods, and Networked Technology [13] (See Figure 1). The purpose of Cybercrime Execution Stack [12] is used to make the investigator analyze and divide the technology as well as the feature objectively, and assist every stage of the Law enforcement investigation process. The Law enforcement investigation includes six stages: Modelling, Assessment, Impact/Risk, Planning, Tools, and Action. Modelling stage used to assess, evaluate, plan and communicate the content of a crime event, and assist the assessment stage in the investigation process. The results of Modelling stage is used to analyze the knowledge and technology related to the cybercrime in the Assessment stage. In the Impact/Risk stage, the potential threat, offences, evidence, and victims will be analyzed in this stage. According to the results of Modelling stage, Assessment stage, and Impact and risk stage, the investigation actions will be planed and confirmed in the Planning stage. The Tools stage is used to find and consider the adequate skills, tools and equipment. The Tools stage is used to find the adequate skills, tools and equipment, and it will help the potential digital evidence. In the Action stage, the action plan will be confirmed, managed, and coordinated to include the skilled resources and jurisdictions.

2.3 New Model for Cyber Crime Investigation Procedure

In this paper of [26], the authors proposed a new procedure model of cybercrime investigation. It improves the digital investigation process of Brian Carrier [8], and increases several phases used to investigate the cybercrime, coursing this investigation procedure is more suitable to investigate the cybercrime event. In the digital investigation process of Brian Carrier [8] there are five phases, including readiness phase, deployment phase, physical crime scene investigation phase, cybercrime scene investigation phase, and review phase. In [26], the phases of investigation procedure include readiness phase, consulting with profiler, cybercrime classification and investigation priority decision, damaged cybercrime scene investigation, analysis by crime profiler, suspects tracking, injurer cybercrime scene investigation, suspect summon, cybercrime logical reconstruction, and writing report. The readiness phase is used to ensure the executing of investigation will be succeed, and reduce the waste time and error of investigation. The Crime profiling is used to find the information of the suspects from the crime scene. It will help to investigate same type crime in future, and

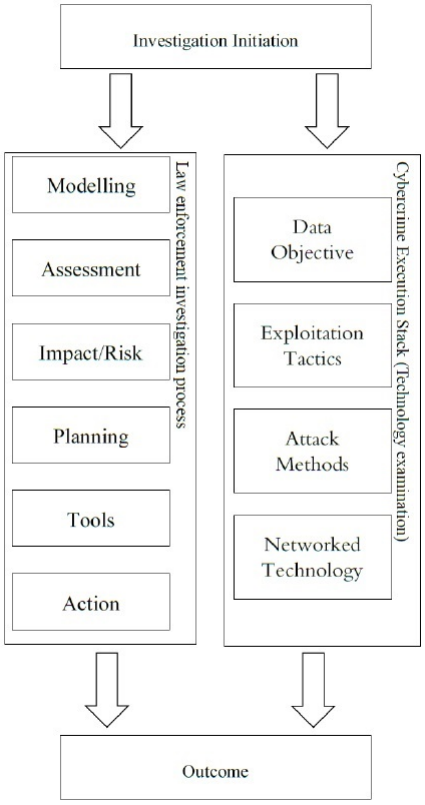

Figure 2: The stages of cybercrime investigations

reduce the time of investigation. The Cybercrime classification and investigation priority decision are used to decide the priority of investigation based on crime profiling data and classifying. In the Damaged (victim) cybercrime scene investigation phase, it's used to collect digital evidences, and the collection method is listed as below.

1) Establish "police line" on Internet;
2) Set the collection equipment to collect evidences of cybercrime events;
3) Photo evidences by digital or video camera;
4) Use tools to collect and analyze the volatile evidences [2, 19];
5) Use the storage imaging method to prevent the evidence from be modified or deleted [18, 19];
6) Obtain the evidences of network by using network forensic systems [24, 25].

In the Crime profiling phase, the investigator analyzes the nature of suspects by using the information collected from the crime scene. It will help to reduce the scope of investigation. After then, the investigator trace the suspects based on the digital evidences and cyber information in the Suspects tracking phase. In the Injurer cybercrime scene investigation phase, the investigation points are same with the Damaged (victim) cybercrime scene investigation phase, and increase a step to collect

the evidences from the printers of injurer. In the Suspects summon phase, the suspects will be summoned according to the collected digital evidences and the information of crime scene. In the cybercrime logical reconstruction phase, the investigators use the information and evidences that are collected from above investigation procedure to re-construct the cybercrime process, and use this reconstruct result to check the investigation result. At last phase, Writing report, the investigators write the report of criminal case about the evidence collect, preserve, and analyze. The Investigation Procedure of [26] is shown in Figure 3.

2.4 SoTE: Strategy of Triple-E on Solving Trojan Defense in Cyber-crime Cases

In this paper [16], it presented a strategy of Triple-E based on [16, 17], and used to investigate the cases of internet intrusion in the cybercrime, like Trojan. By using the strategy of Triple-E, the authors wish to identify the suspects of cybercrime, find the facts of cybercrime, and collect the evidences. In the Triple-E, it has three viewpoints, including Education, Enforcement, and Engineering. The Education viewpoint focuses to reduce the cybercrime amount of hackers and recidivism rate before cybercrime occurring. And the Education will establish a safe internet habits of people, which is used to increase public awareness by distributing a safe internet behavior, implementing a public awareness campaign, and observing the feeling of shame [16]. Furthermore, the investigators use the 6W1H (What, Which, When, Where, Who, Why, and How) Questions to find the motivation and purpose of hackers, and to establish a complete view of cybercrime events, avoiding being deceived by the suspects. The Enforcement focuses of investigation are the investigation field, philosophy role, the purpose of fact finding, and constructing the criminal fact. And the Enforcement based on MDFA (Multi-faceted Digital Forensics Analysis) Strategy can be used against the cybercrime events. Furthermore, the enforcement procedure can be examined from diverse viewpoints, such as exploring aggressive attacks, Comparing illegal offenses, and constructing a holistic view [16]. In the Engineering approach, it focuses on the forensics field, science role, the purpose of target authentication, and the method of arresting the criminals [16] based on the process of Ideal Log and M-N Model. In this viewpoint, it focuses on the importance of evidential records and comparison with other logs, and the measures such as to enable some elementary data for scientific consideration, synchronize the timestamp issues, and conduct an audit examination or cross examination [16]. The utilization of SoTE is shown in Figure 4.

This three viewpoints are related to four layers, including 6W1H questions policy, MDFA strategy procedure, Ideal Logs and M-N Model process, and Evidence record. The 6W1H questions policy is related to Education viewpoint, and used to define a direction of investigation procedure, including What, Which, When, Where, Who, Why, and How.

In the MDFA strategy procedure, it's related to Enforcement viewpoint, and used to analyze the information of cybercrime events. The MDFA strategy has four phases, including Evidential Phase (Evidence), Forensic Phase (Scene), Suffering Phase (Victim), and Behavior Phase (Suspect). In the Evidential Phase, it's used to collect and preserve evidences until the cybercrime case into court proceedings. The Evidential Phase has 5 steps: Identification, Preservation, Examination, Interpretation, and Presentation. In the Forensic Phase, it's used to collect and examine evidences from the crime scene, and discover the criminal process and facts through the crime scene reconstruction. The Forensic Phase has 5 steps: Qualified Expert, Chain of Custody, Admissibility Consideration, Forensic Conclusion, and Crime Scene Reconstruction. In the Suffering Phase, the investigators find and discover the clues of crime case by using the information from victims provided. The steps of Suffering Phase include Variety of Victim, Everyday Process, Victim Himself, Victim Reaction, and Societal Response. In the Behavior Phase, the information of the suspect will be evaluated and analyzed, such as the criminal psychology, personality, criminal actions, and voluntary or not. The steps of Behavior Phase are Background Understanding, Environmental Influence, Linkage Analysis, Logic Reasoning, and Criminal Profiling.

In the Ideal Logs and M-N Model process is used to identify the users behind the computer, and discriminate the in-formation of evidence is real or forged. The Ideal Logs fall into two categories, explicit and tacit knowledge. The explicit knowledge is used to find the location of the suspect by using the clues from digital evidences, such as IP address and timestamp. The tacit knowledge is used to find the clues of digital action and response message, such as data up-load/download, program execute, and abnormal behavior. The M-N Model process is a method used to check the log-in/logout process. M is the path traces from client to server, N is a parts including login and logout in a period of time. When a user wants to login server, the client will produce a login time record TLogin_1. The Login message will be through ISP (Internet Service Provider), and produce a login time record TLogin_2. The Login message will arrive to a server, and produce a login time record TLogin_3. When the user wants to logout a server, the logout message will follow the path of login, and produce the logout time record TLogout_3, TLogout_2 , TLogout_1 on the server, ISP, and client. Further, the M-N model provides a proposition analysis consisting of Sequential Inequality and Period Inequality. This methodology will help clarify the issues that the evidences are reliable or not, and the suspect is guilty or not. The M-N model is shown in Figure 5.

In the Evidence record, since the evidences is used to discover the crime fact and the internet behavior, the collected evidence record must has the clear and objective features. At last, the investigators find the causality from the result of this four-layer, and make the details of a

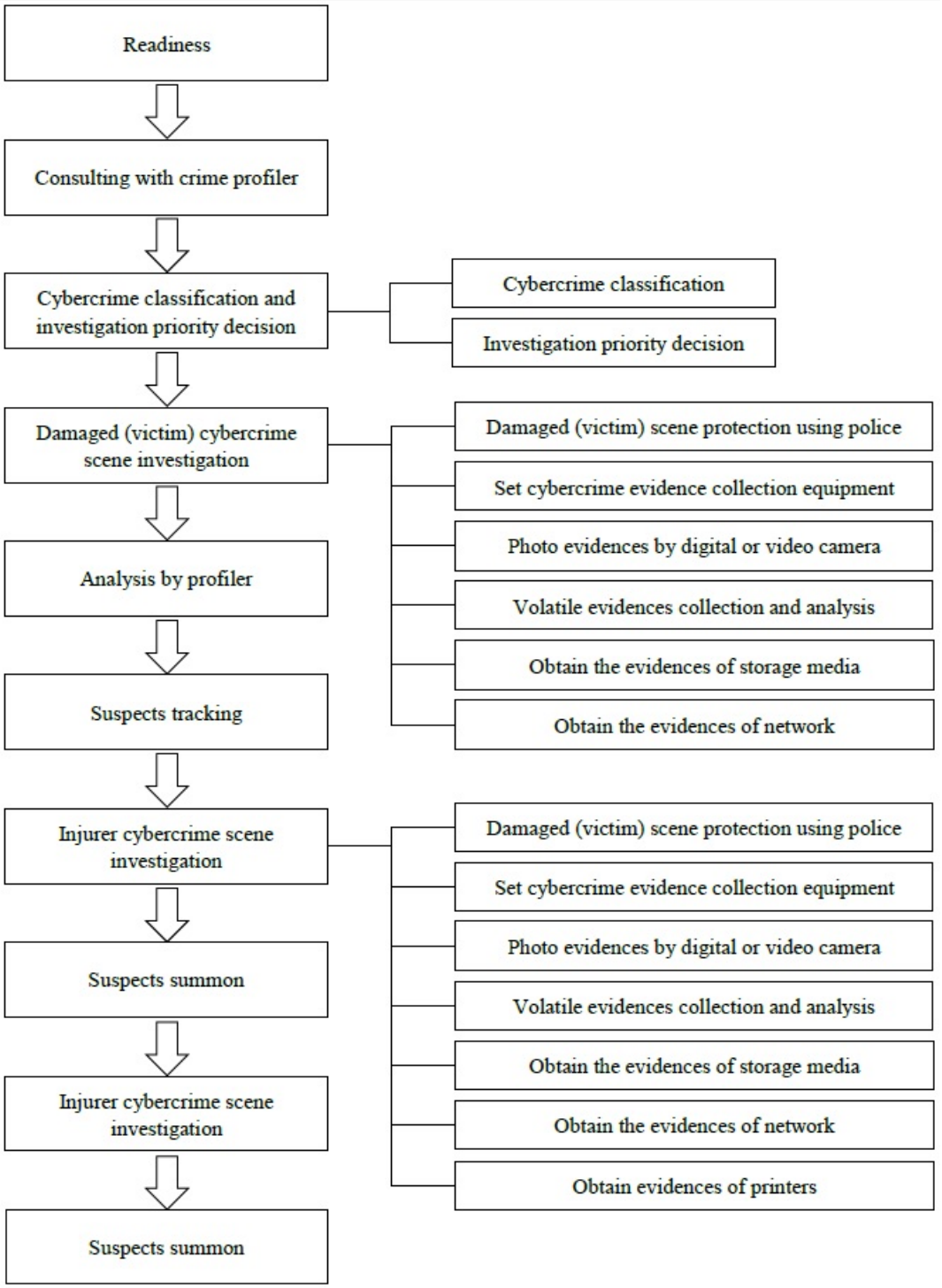

Figure 3: The investigation procedure of [12]

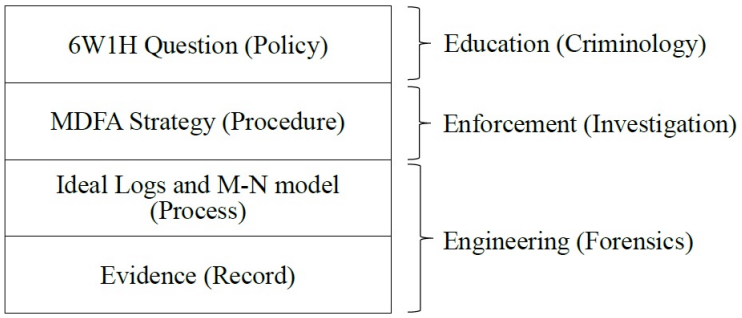

Figure 4: The utilization of SoTE

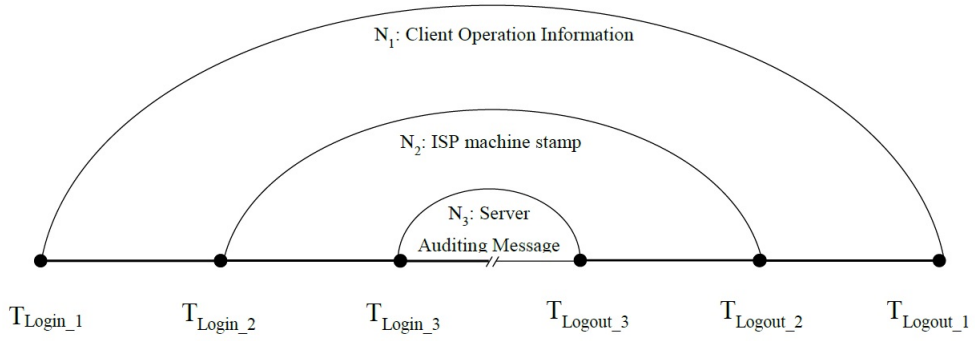

Figure 5: TM-N model

crime event clear.

2.5 A Study on Digital Forensics Standard Operation Procedure for Wireless Cybercrime

In this paper [35], the authors proposed a Standard Operation Procedure (SOP) of digital forensics for a wireless cybercrime. This procedure includes two pairs, the digital forensics and the wireless cybercrime investigation. The authors of this paper define the main behaviors of a wireless cybercrime, and use the definition to propose a wireless cybercrime investigation. Further, this paper proposed a digital forensics SOP based on the Digital Forensic Standard Operation Procedure (DFSOP).

In the wireless cybercrime investigation, the five behaviors of a wireless cybercrime were defined as follows [35]:

1) Cracking a wireless Internet access, and then connected to Internet by using the identity of another person;
2) Invading a wireless base station;
3) Intercepting packets of a wireless network; side-recording the conversations, accounts, and passwords;
4) Denial attacking the wireless base station;
5) Phishing in the wireless base station.

The wireless intrusion is the beginning in the wireless cybercrime. When the intrusion action is successful, the behaviors (2) to (5) will be also finished successfully. In order to solve the above wireless cybercrime, the investigation of this paper provide three stages, including Investigating and analyzing wireless cybercrime, Recognizing the criminal origin and behavior, and Arresting the perpetrator. In the Investigating and analyzing wireless cybercrime, the plan of investigation is to follow the description of the victim. And, then, the content of the wireless cybercrime will be identified by analyzing the modus operandi, such as checking the record from access points, the status of the network, the detection systems, and log files. In the Recognizing the criminal origin and behavior, the purpose of this stage is to find the suspects of a wireless cybercrime. The investigation methods are detecting the data of user, tracing the connection source, checking the record of communications, the firewall records, and so on. Sometime, in order to obtain the clues of a suspect, the investigation process even need to monitor and record the wireless network. In the Arresting the perpetrator, it's used to collect the evidence by using search and seize, summoning the suspects, and the forensic of wireless networks. Further, in order to facilitate the execution of investigation, this paper provides four directions to help the investigation of wireless cybercrime, including [35]:

1) Finding the illegal wireless access point;
2) Locking up the active illegal links;

3) Setting the honeypots in wireless;

4) Setting the intrusion detection system, such as a wireless intrusion prevention systems (WIPS) and wireless intrusion detection systems (WIDS).

In the digital forensics SOP, this paper proposes a wireless forensics SOP based on DFSOP. In the DFSOP, It has four phases: Concept, Preparation, Operation, and Report. In the Concept phase of DFSOP, it's used to describe the concepts of collecting evidence and forensics based on Laws, Principle, and Cognitive. The concepts have seven parts including collecting the evidences quickly and preserving them; ensuring the continuity of evidence; establishing a procedure to record the audit information and analysis of the digital evidences; operating the digital evidences by the experts; recording and filming the process of evidence collection, analysis and forensics; ensuring the integrity and security of data storage; using the copy instead of the original evidence in the operate analysis, investigation and forensics. On the other hand, the Concept phase of wireless DFSOP increases a procedure part to establish SOP and tools; in the laws part, it increases two subparts, acceptance at complaint only, and Non-acceptance at complaint only; in the cognitive, it in-creases three subparts; Forensic Expertise and Skills, Computer Professional and Skills, and Network Professional and Skills.

In the Preparation phase of DFSOP, it's used to collect related information to prepare the work before the forensics and the four parts based on Authenticity and Security Police, Collection of the Basic Information of the Target to Ensure the 5W&1H (Who, Why, When, Where, What and How), and Preparation of Tools and Information and Mission Education . The four parts are Collection of the basic information of the crime target, Preparation of tools, Professional members, and Education before the operation. On the other hand, the Preparation phase of wireless DFSOP increases a subpart, Simulation of Task Allocation and Action.

In the Operation Stage, it's divided to three procedures based on Crime Scene and Laboratory. The three procedures are Collection Procedure, Analysis Procedure, and Forensics Procedure based on Crime Scene and Laboratory. The procedures is used to collect evidence of every type by different tools, analyze these evidences, and then reconstruct the crime scene. Further, in the Operation Stage of wireless DFSOP, it presents three sources of collect evidences: Wireless Devices of Suspect, Wireless Devices of Scene, and Other Devices. And the Presentation forms the Collection phase, so the evidences are divided to the Volatile and Non-volatile type. The data collected from the wireless cybercrime will be analyzed including Picture, Images, Files, Connection History, Log Files of AP and PC, Wireless Network Event Viewer, and Wireless Packets.

In the Report Stage, it's used to produce a report about the content of cybercrime event, the evidences related to the cybercrime event, and the suspects of cybercrime event. This report will be sent to court, and become the basis of judgment. Therefore, the report must has the following related data: Copywriting and Presentation, Examination of Forensics Result, Court Preparation, and File Establishment and Learning. The Copywriting and Presentation are used to describe the content of this crime case, the collected evidences, the evidence sources, and the process of forensics. The Examination of Forensics Result is the procedures of evidence forensics and utilities usage. The Court Preparation means the dig-ital evidence forensics must be classified, and matched with the control procedure. At last, in the File Establishment and Learning, the forensics process, evidence types, and investigation experience of each cybercrime cases will be classified to establish in the file and sharing mode, it will help the future of cybercrime investigation.

3 The Discussion of Investigator Process and Investigation Procedure

3.1 Analysis and Comparison

In this paper, we collect five papers of the cybercrime investigation procedure, and analyze whether these proposed investigation procedure has the following features and content, the compatibility of traditional investigative procedures, cybercrime behavior analysis, evidence forensic procedures, case analysis and verification, the methods of evidence collection and analysis, and the area of judicial jurisdiction. In addition, we put the area of judicial jurisdiction into the comparison items, so it will help to understand the purpose and legal basis of the investigation procedure. The comparison of cybercrime investigation procedures are shown in Table 1.

1) With the compatibility of traditional investigative procedures: This is used to illustrate the investigation procedure of cybercrime, and whether it is proposed or not according to the conventional investigation procedure. It will affect whether this investigation procedure is easy to use or not by the police or investigators without the professional knowledge.

2) With the analysis of cybercrime behavior: In the investigation procedure of cybercrime, whether it has the analysis of cybercrime behavior clearly, and describes the focus types of this cybercrime procedure. It will help the investigators to find scope of this investigation procedure applies.

3) With the evidence forensic procedures: Whether an investigation procedure has the process and steps of forensic, it will affect the process of collecting the digital evidences. Without the forensic process, the investigators, perhaps, will not know what the digital evidences exist, and where can collect them.

4) With case analysis and verification: When the investigations procedure are used actually before, the investigation procedure of cybercrime only is a hypothesis. If the investigation procedure is based on an instance, or it can be used to analyze and verify for an instance, it will increase the feasibility of investigation and evidence collection procedures.

5) The methods of evidence collection and analysis: If the investigations procedure has a method of scientific or mathematical analysis, it will make the digital evidences of this procedure collected has more probative force.

6) The area of judicial jurisdiction: The investigations procedure we collected is not in the same judicial jurisdiction. To clarify these judicial jurisdictions will help the investigators to understand the purpose and the legal basis of investigation procedures.

In [12], it provides a Cybercrime Execution Stack. This framework stack presents the technology of cybercrime, the criminal object of attack, and attack mode. The main purpose of this framework stack is used to classify the cybercrime, and become a step in the cybercrime investigation procedure. Therefore, in [12], it only had the cybercrime analysis, but it did not establish a full investigation and evidence collection process. In [13], it provided a combination of investigative procedure with [12]. This procedure is based on an investigation procedure that already exists, and combine the frame-work of [12] proposed to become an investigative procedure focus on cybercrime. However, in [13], it presents a conceptual investigation procedures, but it did not provide the evidence forensic procedures and other methods. Therefore, in [13], it is an investigative procedures that have the compatibility of traditional investigative procedures and cybercrime behavior analysis. In [26], it provides a more clearly investigation procedure than [13]. In every investigation stage of [26], it describes the purpose of stage and source of forensic evidence clearly. However, in [26], it did not provide and describe the applicable type of cybercrime for the investigation procedure, and did not provide a clear evidence collection and analysis methods, as well as case analysis and verification. It makes the investigation procedure of [26] proposed still need to be proved that it can be used in the cybercrime events.

In [35], it provides a SOP investigation procedure of digital forensics used to investigate the wireless cybercrime. In this SOP, it provides a clear investigation phase based on the conventional investigative procedures. It makes the investigation procedures of [35] compatible with the conventional investigative procedures. In addition, the proposed investigation procedures of [35] defined the each step of investigation clearly, the behavior of wireless cybercrime, and a real pro-cess of investigating a cybercrime case. In this investigation procedure, it describes the process and source of evidence forensic process clearly. Therefore, the investigation procedure of [35] provides a high viability investigation procedures. In [16], it provides cybercrime investigation procedure based on criminology. This procedure is used to investigate Trojans cybercrime, and to illustrate the current situation of this type of crime. It makes the investigation procedure of [16] feasible. In addition, the investigation procedure of [16] uses the MDFA as the forensics process, and uses the M-N mod-el as a method of analysis the evidence in the forensics process. Since the investigation procedure of [16] conforms the above-mentioned characteristics of each, which makes it became a more complete cybercrime investigation procedures than others.

3.2 The Viewpoints of Cybercrime Investigation Procedure

In this paper The Digital evidence forensic process is one of stages belonging to the cybercrime investigation procedures. When a cybercrime occurs, the investigators will collect the digital evidences according to crime types, and preserve them. These Digital evidences are very important in the investigation procedure. The investigators confirm the crimes suspects, crime facts, time of occurrence, location, and possible criminal tools by analyzing these Digital evidences. The digital evidence forensic process is used to make cybercrime investigation procedures can be carried out smoothly. Since the every cybercrime case is independent, the digital evidence presented these cases will be in different ways. Therefore, the primary purpose of digital evidence forensic process should be "whether can collect direct evidences"; the second is "whether can collect indirect evidences"; and finally, "Which method of forensic evidence is the fastest." The reasons of this order is when the cybercrime is on the trial, and the judge will determine the outcome of the judgment based on the direct evidences; in the investigation procedure, the direct and indirect evidences will be the key to confirm the facts and suspects. There evidences will become a relevance indicator used to confirm the crime facts and the suspects, it is called the probative force of the evidence. If the process of forensic evidence is very fast, but cannot guarantee to collect evidence of high probative force, it will increase the time of investigation, as well as waste the judicial resources. Therefore, the digital evidence forensic methods should be focused on how to collect the direct and indirect evidences effectively.

In the conventional crime, the evidence type is substantive evidence, and the perpetrator can be found easily; there is an actual location of the crime, and the crime tools are easy to find. Therefore, the purpose of investigation procedures in the conventional crime is how to protect the crime scene, how to collect evidence from the crime scene, and how to quick to arrest the criminals. However, the cybercrime is a new type of criminal offense. The perpetrator of this crime is not easy to be found directly due to no actual location of the crime, so the evidences of crime are not easy to preserve and view, and criminal means and tools are not easy to find. There-

Table 1: The comparison between the each investigation forensics procedures of cybercrime

	Compatibility of traditional investigative procedures	Cybercrime behavior analysis	Evidence forensic procedures	Case analysis and verification	The methods of evidence collection and analysis	The area of judicial jurisdiction
The growing phenomenon of crime and the internet: A cybercrime execution and analysis model [6]	X	V	X	X	X	UK
The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation [4]	V	V	X	X	X	UK
New Model for Cyber Crime Investigation Procedure[5]	V	X	V	X	X	Korea
A Study on Digital Forensics Standard Operation Procedure for Wireless Cybercrime [3]	V	V	V	V	X	Taiwan
SoTE: Strategy of Triple-E on solving Trojan defense in Cyber-crime cases [26]	V	V	V	V	V	Taiwan

fore, in the cybercrime investigation procedures, how to collect the key digital evidences becomes the important key. According to these Digital evidences, the investigators can confirm the criminal facts, the perpetrator, criminal tools and criminal means. Once the digital evidences are forged, altered, deleted or destroyed, it will cause the investigation hard to continue implementing, or even mislead the investigators. Finally, the results will make the innocence person is punished, and the guilty person is released. Therefore, in the investigation procedure of cybercrime, how to find the perpetrator accurately will be the primary purpose in the procedure; secondly, since the judicial resources are limited, how to reduce the use of judicial resources is one of the key points in the investigation procedure. In addition, all the investigation behavior must base on the relevant laws and regulations. Only the evidence forensic by the legal process can be used in the trial, and it is called the evidence capability. The evidence from unlawful conduct investigations obtained at trial would lose the evidence capability, and cannot be used to prove the defendant is guilt. The collected evidence must have the evidence capability, and then it will have the probative force. Therefore, how to find and verify the perpetrator accurately and lawfully and reduce the use of judicial resources will be the focus in the cybercrime investigation procedures.

4 Future Works

In the future, the types, methods, and targets of cybercrime will be changed continuously, and every types of computer, network equipment, and smart phone will be the target of attack. The points are how to combine the digital forensic methods and the resent investigation procedure, or even establish a defense method in the investigation procedure, resulting the purposes to defense, detect, and investigate effectively. Since the cybercrime will constantly change in the future, the cybercrime investigation procedure should be established based on the type of crime. In addition to these investigative procedures used to investigate the crime fact after the event occurring, it must has the functions of real time detection and forensic. Therefore, before the investigation procedure establishing, we propose to establish an architecture figure of cybercrime factors first. Once the cybercrime occurs, the investigators will decide which investigation procedure will be used based on the factors of case, and determine whether the subsequent criminal behavior has. However, many factors can affect cybercrime, so in the following we will enumerate several factors that will affect the cybercrime, including Criminal objects, Crime Environment, Connection Technology, Source areas of crime, Crime types, and Criminal objects. The affection factors of cybercrime as shown in Figure 6. In the Criminal objects, we divide the targets of crime into three types: equipment, single victim, and multiple victims. In this category, we wish to confirm the purposes of offenders for this type of victims.

In the Crime environment, we divide the environment into the Public network, Private network, and Half-Public net-work based on the classification of the network type. The purpose of this classification is used to find the place of exist-ing crime clues through the criminal environment. In the Connection technology, we enumerate three common technologies of network connection: Ethernet, Wireless Fidelity (WiFi), and Mobile communication technologies (MCTs). This classification will help the investigators to collect the digital evidences. In the Source areas of crime, we will confirm the jurisdiction area of crime, External or Internal, through the area that found the sus-

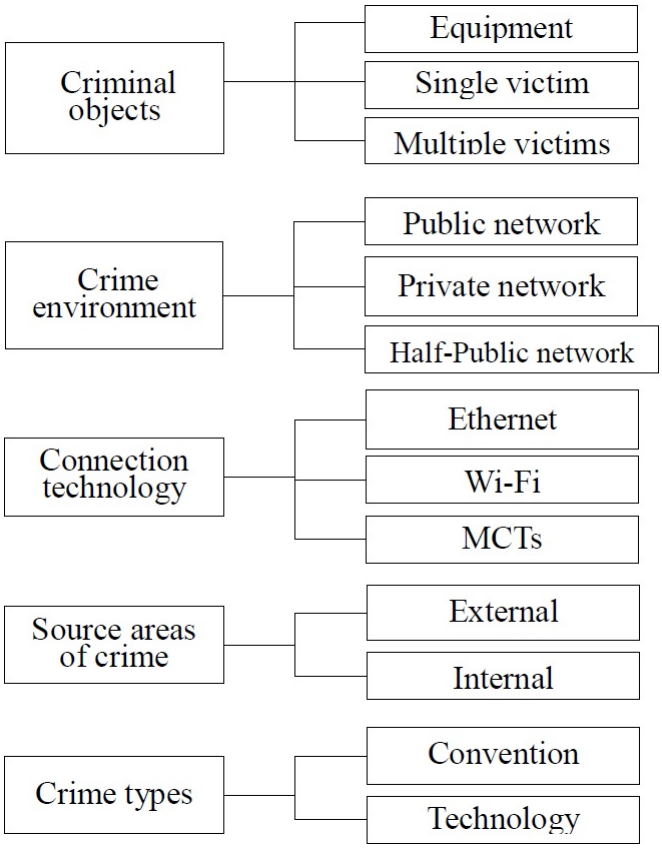

Figure 6: The affection factors of cybercrime

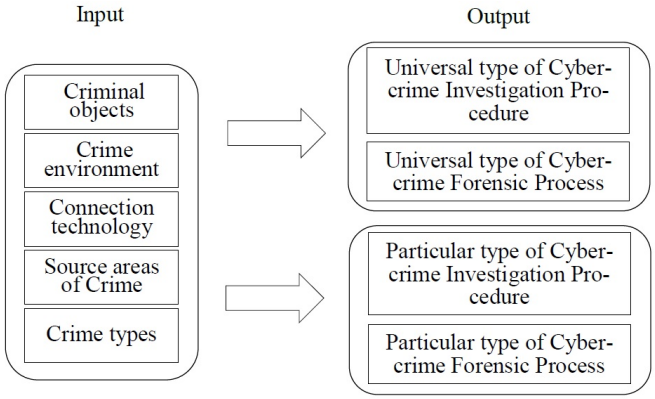

Figure 7: The investigation and forensic of cybercrime

pect. Finally, we will divide the crime types into Convention and Technology. This classification of crime types will be used to confirm the perpetrator of the crime and establish the tactics of investigation as the cumulative experience of investigation. In these factors, the order does not be constructed, but rather as the analysis items of cybercrime, and used to develop the evidence forensic process and investigation procedure.

According to the combination of these factors, it can be summarized to the concept of two types: Universal type of Cybercrime Investigation Procedure (UCIP) and Particular type of Cybercrime Investigation Procedure (PCIP); and two types of cybercrime forensic process: Universal type of Cybercrime Forensic Process (UCFP) and Particular type of Cybercrime Forensic Process (PCFP), as shown in Figure 7.

The universal type is used to describe the type of conventional crime. This crime type refers the criminal offenses al-ready existed before the Internet development, such as Fraudulence, intimidation, defamation, and so on. These scene of conventional crimes are gradually transferred to the Internet with the development of Internet. In order to investigate the conventional crimes and collect the digital evidences on the Internet, we propose to establish the UCIP and UCFP. The UCIP and UCFP aims to provide a simple and accurate method of investigation, and make the general security police also to investigate the cybercrime. And avoiding the criminal investigations is hindered because of the investigators lacking the knowledge of network technology. The Particular type is used to describe the crime type of technology-based. This crime type refer that the perpetrator uses the expertise and tools to commit the cybercrime offenses, and make the investigators without the expertise not to understand the method of crime, such as the Network attack, System intrude, Identity camouflage and hide, Data theft, and so on. Since investigating these crimes requires technical expertise, it will make the investigation process very difficult, and the general security police also cannot investigate this kind of cybercrime. Therefore, we propose to establish the PCIP and PCFP for the particular type of cybercrime. The purpose of PCIP and PCFP is to allow the general public security police and the investigators with technical expertise to cooperate together in the investigation of the cybercrime, and improve the efficiency of the investigation.

Since Internet still has the unknown development in the future, the affect factors of cybercrime and sub-factors will not be confined to the range of Figure 6; the investigation procedure and forensic process will not only include the two types in Figure 7. Once the new type of cybercrime event occurs, it still need the investigators to analyze the technology and features of cybercrime, and establish the emphasis investigation and forensic procedure.

Furthermore, after the investigation procedure, the criminal case will turn into the judgment procedure in the court. In the judgment of cybercrime, the result of trial will be different between cybercrime and conventional crime. The judgment procedure will affect the evidence that need to collect in the investigation procedure, and the evidences will affect the judge to find crime facts and the result of trial. Therefore, the investigation procedure and the forensic method of cybercrime still need to adjust and modify according to the result of trial.

5 Conclusions

In this research, we focus on how to collect the digital evidences from the cybercrime events, and how to propose an effective cybercrime investigation procedure. The digital evidences will help find the real perpetrators during the investigation procedure of cybercrime, and brings the perpetrators to justice in the trial; the effective cybercrime investigation procedures will help reduce the waste of judicial resources, and protect the human rights. A good method to collect digital evidences, in addition to focus on how to collect quickly the evidence, should focus on how to collect the digital evidence of high probative force. Whether these digital evidences are collected automatically by the computer system, or collected manually by the system administrator, the value of evidences are based on how many probative force that can provide to prove in the trial. In cybercrime investigation procedure, a good investigation procedure requires the less use of judicial resources, and avoids the mandatory punishment of suspects.

Acknowledgments

The author expresses deep sense of gratitude to the Department of Science & Technology (DST) , Govt. of India, for financial assistance through INSPIRE Fellowship leading for a PhD work under which this work has been carried out, at the department of Computer Science & Engineering, University of Kalyani.

References

[1] I. O. Ademu, C. O. Imafidon, D. S. Preston, "A new approach of digital forensic model for digital forensic investigation," *International Journal of Advanced Computer Science and Applications*, vol. 2, no. 12, pp. 175–178, 2011.

[2] D. Brezinski, T. Killalea, "Guidelines for evidence collection and archiving," RFC 3227, 2002.

[3] R. P. Bryant, *Investigating Digital Crime*, Wiley, 2008.

[4] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, Academic Press, pp. 41-46, 2000.

[5] E. Casey, *Handbook of Digital Forensics and Investigation*, Academic Press, 2009.

[6] E. Casey, *Digital Evidence and Computer Crime*, Academic Press, 2004.

[7] B. Carrier, "Defining digital forensic examination and analysis tools using abstraction layers," *International Journal of Digital Evidence*, vol. 1, no. 4, pp. 1–12, 2003.

[8] B. Carrier, E. H. Spafford, "Getting physical with the digital investigation process," *International Journal of Digital Evidence*, vol. 2, no. 2, pp. 1–20, 2003.

[9] Y. Chen, S. Das, P. Dhar, A. E.Saddik, A. Nayak, "Detecting and preventing IP-spoofed distributed DoS attacks," *International Journal of Network Security*, vol. 7, no. 1, pp. 69–80, 2008.

[10] Alan M. Gahtan, *Electronic Evidence*, Thomson Canada Limited, 1999.

[11] M. Geva, A. Herzberg, Y. Gev, "Bandwidth distributed denial of service: Attacks and defenses," *IEEE Security & Privacy*, vol 1, pp. 54–61, 2014.

[12] P. Hunton, "The growing phenomenon of crime and the Internet: a cybercrime execution and analysis model," *Computer Law & Security Review*, vol. 6, no. 6, pp. 528–535, 2009.

[13] P. Hunton, "The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation," *Computer Law & Security Review*, vol. 27, no. 1, pp. 61–67, 2011.

[14] N. Jeyanthi1, N. Ch. Sriman Narayana Iyengar, "An entropy based approach to detect and distinguish DDoS attacks from flash crowds in VoIP networks," *International Journal of Network Security*, vol. 14, no. 5, pp. 257–269, 2012.

[15] D. Y. Kao, and S. J. Wang, "The IP address and time in cyber-crime investigation," *Policing: An International Journal of Police Strategies & Management*, vol. 32 no. 2, pp. 194–208, 2009.

[16] D. Y. Kao, S. J. Wang, Frank F. Y. Huang, "SoTE: Strategy of Triple-E on solving Trojan defense in Cyber-crime cases," *Computer Law & Security Review*, vol. 26, no. 1, pp. 52–60, 2010.

[17] G. C. Kessler, "Anti-forensics and the digital investigator," in *Proceedings of the 5th Australian Digital Forensics Conference*, 2007.

[18] G. A. Lee, D. W. Park, and Y. T. Shin, "A study on the chain of custody for securing the faultlessness of forensic data," *Journal of the Korea Society of Computer and Information*, vol. 11, no. 6, pp. 175–184, 2006.

[19] S. H. Lee, H. Kim, S. Lee, J. Lim, "Digital evidence collection process in integrity and memory information gath-ering," in *Systematic Approaches to Digital Forensic Engineering, First International Workshop on Systematic Ap-proaches to Digital Forensic Engineering (SADFE'05)*, pp. 236–247, 2005.

[20] C.Y. Liu, C.H. Peng, and I.C. Lin, "A survey of botnet architecture and batnet detection techniques," *International Journal of Network Security*, vol. 16, no. 2, pp. 81–89, 2014.

[21] M. Mahmoud, M. Nir, and A. Matrawy, "Survey on botnet architectures, detection and defences," *International Journal of Network Security.* (in press)

[22] B. Mihajlov and M. Bogdanoski, "Analysis of the WSN MAC protocols under Jamming DoS attack," *International Journal of Network Security*, vol. 16, no. 4, pp. 304–312, July 2014.

[23] E. Moulton, *The Future of Cybercrime*, Police Professional, 2008.

[24] S. Mukkamala, A. H. Sung, "Identifying significant feature for network forensic analysis using artificial intelligent techniques," *International Journal of Digital Evidence*, vol. no. 4, pp. 1–17, 2003.
[25] J. S. Park, U. H. Choi, J. Moon, T. Shon, "A study on network forensics information in automated computer emergency response system," *Journal of the Korea Institute of Information Security and Cryptology*, vol. 14. no. 4, pp. 149–162, 2004.
[26] Y. D. Shin, "New model for cyber crime investigation procedure," *Journal of Next Generation Information Technology*, vol. 2, no. 2, pp. 1–7, 2011.
[27] D. L. Shinder, M. Cross, *Scene of the Cybercrime*, Second Edition, Syngress, 2008.
[28] C. Sorrells and L. Qian, "Quickest detection of denial-of-service attacks in cognitive wireless networks," *Inter-national Journal of Network Security*, vol. 16, no. 6, pp. 468–476, 2014.
[29] M. Subramanian, T. Angamuthu, "An autonomous framework for early detection of spoofed flooding attacks," *International Journal of Network Security*, vol. 10, no. 1, pp. 39–50, 2010.
[30] J. Udhayan, T. Hamsapriya, "Statistical segregation method to minimize the false detections during DDoS attacks," *International Journal of Network Security*, vol. 13, no. 3, pp. 152–160, 2011.
[31] D. S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*, Polity Press, 2007.
[32] S. J. Wang, "Measures of retaining digital evidence to prosecute computer-based cyber-crimes," *Computer Standards & Interfaces*, vol. 29, pp. 216–223, 2007.
[33] S. J. Wang, "Measures of retaining digital evidence to prosecute computer-based cyber-crimes," *Computer Standards & Interfaces*, vol. 29, no. 2, pp. 216-223, 2007.
[34] M. Yar, *Cybercrime and Society*, Sage Publishing Ltd, 2006.
[35] Y. S. Yen, I. L. Lin, A. Chang, "A study on digital forensics standard operation procedure for wireless cyber-crime," *International Journal of Computer Engineering Science*, vol. 2, no. 3, pp. 26–39, 2012.

Jia-Rong Sun Jia-Rong Sun received the B.S. degree and M.S. degree in Computer Science and Information Engineering from Asia University, Taiwan in 2010. He is currently a Ph.D student in the Department of Computer Science and Information Engineering, Taichung, Taiwan. His research interests include Information security and cybercrime investigation.

Mao-Lin Shih received the B.S. degree in College of Law National Taiwan University, Taipei, Taiwan; and the honorary Ph.D from Woosuk University, Korea, in 2009; Dr. Shih was a judge in 1984-1993. He was also a Chief Prosecutor during 1997-2004. From 2005 to 2008, he was the Minister of Ministry of Justice in Taiwan. He is currently a professor of the Department of Financial and Economic Law in Asia University. He is the director-general of Legal Risk Management Society of Taiwan. His current research include Criminal Law and Legal Case Study.

Min-Shiang Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China, in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a project leader for research in computer security at TL in July 1990. He obtained the 1997, 1998, and 1999 Distinguished Research Awards of the National Science Council of the Republic of China. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include database and data security, cryptography, image compression, and mobile communications.