International Journal of Computer Engineering Science (IJCES)
Volume 2 Issue 3 (March 2012) ISSN : 2250:3439
https://sites.google.com/site/ijcesjournal http://www.ijces.com/

A Study on Digital Forensics Standard Operation Procedure for Wireless Cybercrime

Yun-Sheng Yen[1], I-Long Lin[2], Annie Chang[3],

[1]Fo Guang University, Department of Applied Informatics, Ilan, Taiwan, ROC
[2]Department of Information Management, Yuanpei University, HsinChu, Taiwan, R.O.C.
[3]Central Police University, Department of Information Management, Taoyuan, Taiwan, ROC
[1]ysyen@mail.fgu.edu.tw, [2]cyberpaul747@mail.ypu.edu.tw, [3]im973090@gmail.com

Abstract. With the increases growth of Internet users and the development of new technologies, current legislations and security has faced difficulties in trying to keep up, hence cybercrime numbers are increased rapidly. Although wireless cybercrime is a new threat, but with the detail tracking and investigation effort, ultimately the professional will find some kind of digital evidence, and its often required to identify and preserve in order to be recognized and restoring the truth, hence the establishment of trainings in digital evidence through to forensic requires immediate implementation, with increase of the standards and knowledge it will strength the competence and credibility of the forensics unit's professional ability in assistance to fight again all crime.

Keywords: cybercrime, digital forensics, digital evidence

1 Introduction

Cybercrime [1] is currently the most critical issue in the digital society domain. According to the routine activity theory (motivation, object, protection, MOP theory), crime can occur on the Internet. In order to prevent and suppress this type of crime, we must understand and define this behavior so that we can quickly and correctly identify such cases while investigating cybercrime in future, and so that we can combat crimes effectively using known methods. Due to features such as easy implementation, small size, and no need for physical deployment, wireless networks have become part of the mainstream of the networked world of the future. However, the security deficiencies of wireless networks also make them hotbeds of crime.

Many products for wireless networks can also be used to commit crimes and pose a great threat to wireless security. For example, Taiwan's Criminal Investigation Bureau found a product called "Card King" being sold on the Internet. It allows the user to search for any nearby wireless networks, to crack their passwords and to use someone else's wireless network. Furthermore, it enables a private account to be criminally misappropriated by others. If we want to obtain digital evidence of a cybercrime, a

comprehensive standard operating procedure must be established to seize the initiative in the investigation, which was the motivation of this study.

The installation of wireless networks is different from that of traditional networks. With traditional fixed-line connections, it is usually difficult for the perpetrator to completely remove any traces of his/her actions on the Internet. However, a wireless network is very different in its hardware, software, and security. Thus, the investigation method for traditional cybercrime alone is not enough when investigating wireless cybercrimes. Therefore, in order to overcome this difficulty, we should clearly define wireless networks and understand their characteristics and types. Wireless cybercrime is an illegal activity committed by people with expertise in science and technology. In the process of investigating computer crime, manpower and resources are often limited. Because "digital evidence" is easy to tamper with, easy to lose and difficult to collect, if we want to obtain digital evidence in the event of computer and information crime, a comprehensive standard operating procedure must be established in order to seize the initiative in the investigation.

2 Related Works

2.1 Digital Evidence Processing Procedures

In Casey's book [2][3] "Digital Evidence and Computer Crime", "Digital Evidence" refers to any electronic digital data that are sufficient to prove the circumstances or the association of a crime in a computer storage medium. As a type of physical evidence, it includes text, images, audio, video, and other media, with the features of unlimited and identical duplicability, unreliable determination of the original author, issues with data integrity verification, and so on. It is also known as computer evidence; in other words, it is an electromagnetic record stored in a computer storage medium or on a network and may be used as evidence of crime.

Standard operating procedure (SOP) is the internal procedure designed to perform a complex routine with limited time and resources. The significance of an SOP is that, using a unified written operating procedure, the business structure, operating environment, equipment operation, work content and procedure are standardized by graphics, specifications, text, and the like. In this case, an officer in charge of the work can follow the standardized process and thus rationalize the operating process and service process, reducing errors at work and resulting in enhanced work efficiency and effectiveness. Therefore, if an SOP can be developed for digital evidence, it will provide prosecutors and police officers in forensic evidence collection with a uniform standard, leading to the collection of more credible evidence.

The process of digital forensics [4][5][6] is the collection of criminal evidence using scientific methods for computers and other IT equipment. As the saying goes, "every step must leave a mark." Even after a malicious or unintentional deletion, data

can often still be restored. Because digital evidence is easy to tamper with, easy to lose, difficult to collect, and easy to destroy, and because the storage space of computer equipment is getting larger and larger, the improper handling of evidence by investigators can easily lead to difficulty in gathering important clues, resulting in the a loss of initiative for cracking a criminal case.

2.2 Digital Evidence Forensics Standard Operating Procedure (DEFSOP)

Lin [7][8] presented the Digital Evidence Standard Operate Procedure (DESOP), which consists of four main phases:

1). Concept phase: This phase includes a) principles, b) regulations, c) cognitive and other procedures.
2). Preparation phase: a) licensing and information security policies, b) collecting basic data for objects, c) determining person, event, time, place, object, and reason, d) preparation of tools, information and training. [9][10][11]
3). Operational phase: a) collection, b) analysis, c) identification and other procedures.
4). Report phase: a) writing, presenting, and briefly reporting, b) verifying the forensic results, c) court preparation, d) case filing and review.

Phase I: Concept Stage

The obtainment of digital evidence should follow the principle of legality and truth. The person involved cannot obtain the evidence by illegally invading other's computer information system. The obtainment of evidence should be legal and according to the procedures of digital evidence obtainment and permission. The major principles are divided into seven parts:

1). Collecting the evidence as soon as possible, and ensuring that the evidence is not damaged. That is, the information stored in computer or other storing media should remain in the original status and cannot be modified.
2). The continuality of the evidence should be promised. When the evidence is used in the Court, any change during the process should be explained. It would be the best if no change has taken place.
3). A procedure and record should be established to any of auditing information, record or analysis of the digital evidence. The result should be the same if the operation is given over to a just third person.
4). In a exceptional condition, if any save and load behavior should be operated on the original digital evidence, it should be handed to a capable expert to do so and the expert should give a appropriate explanation of his/her behavior.
5). The whole process of collection, analysis and forensics should be recorded and filmed.
6). When using the floppy disk, compact disk, magnetic tape, hard disk, flash disk or storage card which contains the copied evidence, the operator should be aware of risk and get away from strong magnetic field, water and fire. Moreover, the detection of virus should also be carefully executing.
7). Using the copy of evidence to operate analysis, investigation and forensics.

Phase II: Preparation Stage

This stage is about to do the preparation work before the forensics and collect related information in order to prepare for the operation of each step; the procedures are listed below:

1). Collection of the basic information of the crime target: To analyze the possible criminal according to the crime mode and the known conditions; if necessary, the related people may be interviewed. Also, the policy of forensics operation would be planned. To determine the searching location, target and time according to the crime mode and use the known information to analyze the possible criminal; if necessary, related people could be interviewed. Furthermore, the searching time and place would be determined after the information of the suspect is ready.

2). Preparation of tools: The manuals of the computer software/hardware should be prepared; the related information of the crime tool program should also be ready.

3). Professional members: The forensics members should be professional enough to operate the forensics tools. Thus, the members should pass the related certificate in order not to miss the precious digital evidence or even destroy it.

4). Education before the operation: Before every mission, the forensics members should be clearly instructed the searching mission and items. Moreover, the members must examine the whether the software/hardware is ready or not to prevent the accidental situation.

Phase III: Operation Stage

This stage should be carefully executed for it may affect the judgment of the Court.

1). Collection Procedure: At this step, this paper divides the digital information into three types: changeable digital information, fixed digital information and file system digital information. Each type of digital information should be collected by different tools.

2). Analysis Procedure: At this step, this paper divides the information analysis into five parts: file, log, Windows registry, differentiation of malicious program code and others. Different tools should be used in different parts.

3). Forensics Procedure: The forensics step is divided into four parts by this paper: information abstraction, comparison, personalization and crime scene reconstruction. In the process of comparison and personalization, which tool should be used in the specific digital data should be Fig.d out.

Phase IV: Report Stage

The judgment in court needs the following related data:

1). Copywriting and Presentation: The forensics report should be displayed to the judge, defendant and investigators. Thus, the contents should be easy to read and totally true. In principle, all effective evidence should be handed to the Court for representation.

2). Examination of Forensics Result: The establishments of the manual, related data and the instruction of forensics tool are very important in computer forensics for it may affect the correctness of the forensics result. The forensic scientists should write down the procedure of forensics and utilities usage; thus, if a third person

or organization wants re-examination for the correctness, these procedures could help.

3). Court Preparation: The digital evidence forensics should be classified and match the procedure of evidence control. The forensics should be ready for the cross-questioning in the Court and be ready for heading to the judge.

4). File Establishment and Learning: Since digital evidence forensics is an improving technology, each file should be classified according to its category. It is important to establish the experience and sharing mode of each case. It would be best if an expert archives could be established for other's consultation's need.

2.3 Wireless Network

By definition, a so-called wireless network is a network for data transfer using radio waves. In recent years, wireless networks have become part of the mainstream in communication applications. However, because the existing mechanisms for the security and defense of wireless networks are relatively weak, and because the wireless network sends signals by air, it is less secure than a traditional wired network. In general, the so-called "wireless networks" include the common wireless telephone network (GSM, GPRS, WAP), Bluetooth or 802.15 (WPAN) wireless networks designed for short-distance wireless data exchange (such as mobile phones, PDA), and 802.11 wireless networks, as well as the long-distance 802.16 (WMAN) (as shown in Fig. 1).

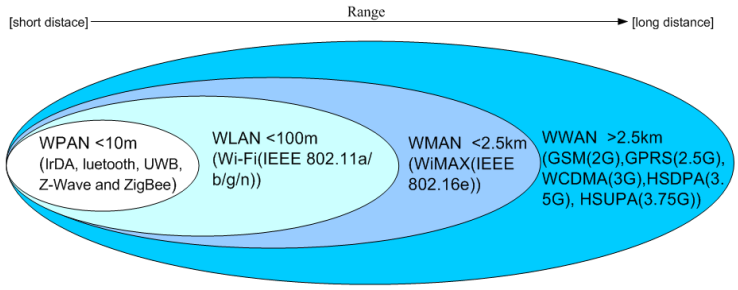

Fig. 1. Types of wireless networks

This study focuses on the security mechanisms of the 802.11 wireless local area network. The main advantage of the 802.11 wireless network is that it does not require physical lines. However, the 802.11 wireless network has intrinsic defects in signal control. It cannot guarantee that the content of communications is not tapped. This might result in the unauthorized use of network resources if the access control is poor. In addition, if there are other electronic devices, it will be subject to significant interference, and the communication signal will be unstable. Over a long distance or across a physical barrier, the connection rate is also affected.

2.4 Wireless Cybercrime

This study focuses on wireless cyber-crime on IEEE 802.11 wireless local area networks. Traditional cyber-crime and wireless cyber-crime can be distinguished by the target of attack. This research focuses on wireless cyber-crime, mainly referring to those using wireless access point (AP) devices to access the Internet, such as enterprise internal users or individual users. Because wireless network technology is extensively used in business and life, it has become another pipeline for hacking. In addition to having the characteristics of traditional cybercrime, wireless cybercrime is more difficult to investigate than traditional cybercrime. This study will describe its primary features in terms of person, event, time, place, and object:

1). The perpetrator: using mobile devices, the perpetrator of crime can easily conceal his whereabouts, and the object of the crime is not easy to determine.
2). Facts of the crime: wireless cybercrime is a kind of intelligent high-technology crime. The modus operandi is not easy to determine, and the criminal behavior is not easy to detect.
3). Time of the crime: the time when the crime occurs is difficult to determine, often because it takes too long to investigate.
4). Place of crime: wireless cyber criminals are mobile. Such crimes often occur in coffee shops and other locations providing wireless Internet. Criminals can also use an AP in someone's home as a springboard.
5). Items of crime: when the crime scene is tracked down, the perpetrator and the crime devices are often no longer present at the scene.

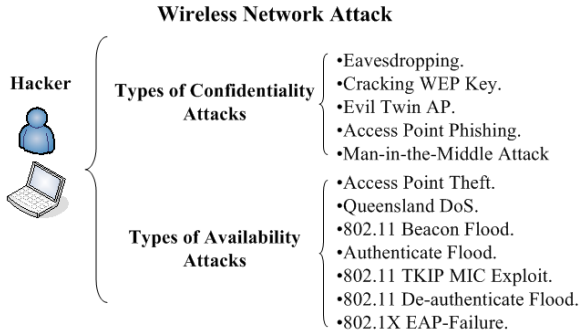

Fig. 2. The subject of wireless network attacks by hackers

3 Forensic Standard Operation Procedure for Wireless Netwrok

3.1 Wireless Cyber Criminal Behavior

Before studying criminal investigations of wireless networks, we must first learn about major criminal behaviors related to the wireless networks and their invasion process. A wireless network allows free access to the Internet with no restrictions on time and place. It also helps open the door to hackers, so that the hackers have more targets for intrusion and attack. Their main behaviors are as the following:

1). Cracking wireless Internet access (WEP or WAP), accessing the Internet wirelessly by using someone else's identity for concealment.
2). Invading other networked computers with the same wireless base station (AP).
3). Intercepting wireless network packets, side-recording the contents of the conversations and the account passwords, stealing private information.
4). Attacking the wireless base station (AP) to block the Internet access of other computers using this base station.
5). Setting up the wireless base station (AP) to carry out phishing.

The detection of the signal of a wireless network is the first step of wireless intrusion. Using detection software, a hacker can get a list of wireless networks and their signal strengths. The wireless network with the strongest signal is the most vulnerable. Using so-called network management software, such as software to intercept data packets, analysis software and so on, a hacker will be able to crack WEP encryption. Once the network has been successfully invaded, the hacker can install trojans or spyware, which can perform unauthorized monitoring when the user uses the keyboard for input. Thus, information such as passwords for online accounts and information on game or other client accounts is stolen.

3.2 Investigation for Wireless Cybercrime

The main concern in the criminal investigation of wireless cybercrime is different from that for traditional cybercrime. As in traditional cybercrime, the types of wireless cybercrime are complicated and volatile. For the investigators initially involved in the investigation, the first problem encountered is the difficulty of quickly finding the focal point and direction of the investigation. Unless they have experience with related cases, the investigators inevitably feel at a loss and unsure of how to get started. Because most of the criminal cases related to wireless networks are currently investigated by the professional unit in the Criminal Investigation Bureau, it is difficult to handle due to the large number of cases. Regarding the modus operandi, wireless cybercrime is an updated version of traditional cybercrime. The main purpose of the crime is still illegal profits. Taking advantage of the characteristics of the spillover in wireless networks, a new modus operandi has been developed to commit crimes. Currently, the general investigators already know the basic process of

investigation of the basic cybercrimes such as Internet pornography, online gambling, online fraud and other traditional computer crimes. However, for wireless cybercrimes, in addition to fewer cases, the process of investigation lacks detailed specifications. This study analyzed the bottleneck in investigating wireless cybercrime described in the previous section. The most important aim is to break the current bottleneck of investigating and to propose a direction for possible solutions. First, the investigation of wireless network crime is divided into three stages, associated with the content of detection and the tools being used, as shown in Fig. 3.

Stage 1: Investigating and analyzing wireless cybercrime

The pattern of the wireless cybercrime is confirmed, based on the description by the victim and the tracking detection by the prosecutors and police. Then, based on the interactive analysis of the modus operandi of traditional cybercrime and wireless cybercrime, the behavior of the wireless cybercrime is identified. For examples, checking the record of wireless network access points, detection systems for wireless network intrusion, audit log files, status of the network system, damage to the network systems, and so on, or using the wireless positioning device and tracking detection tools, the suspected location of the criminal connection can be found.

Stage 2: Recognizing the criminal origin and behavior

The main purpose of a criminal investigation is to investigate the “people” and to identify the “objects”. In a wireless cybercrime, criminals and objects of crime are more difficult to investigate, so this stage is the most difficult. When tracking wireless network crime, the investigation often ends up with only the victim's IP and the information channel is disconnected. However, in a criminal investigation, we should never give up any suspicious information sources. In addition to checking with the methods for traditional cybercrime, such as detecting the user data, tracing the source of the connection log, inventorying the message source, auditing the system record, connecting to the log record of communications, and searching the firewall records, specific crime detection methods for wireless network must also be used, including wireless positioning devices, tracing tools for detection, and monitoring and recording of the wireless network when necessary.

Stage 3: Arresting the perpetrator

This stage includes searching for and seizing the related evidence, arresting and transferring the suspects, collecting other digital evidence, and forensic work for wireless networks.

The emergence of wireless networks has been a great boon to hackers. Data transmitted in wireless networks can be received by all users within a particular region. This feature poses a great threat to the maintenance of data security. Taking advantage of this feature, the hackers can commit the illegal activities of stealing data or unauthorized access, which are difficult to effectively prevent or stop in the wireless network environment. The emphasis and direction of crime investigation for wireless networks are different from those for traditional networks. The biggest difference is that spillover, as the key characteristic of the wireless network, is used to commit the wireless cybercrime. Reviewing the modus operandi of current wireless

network crimes, the most important direction of investigation should focus on positioning and identifying the explorers of illegal connections (theft of wireless spillover).

Currently, the number of cases of wireless cybercrime that have been investigated is not large. These cases have mostly not yet been solved. Most of the people accessing the wireless Internet may not know that they have been invaded, or they may simply respond negatively. Specific, professional information technologies and methods should be applied against wireless cybercrimes, in order to break through the bottleneck of wireless cybercrime.

In order to facilitate the investigation of wireless cybercrimes, the relevant government agencies are expected to demand relevant security rules from future wireless Internet service providers, including: ID checking, maintaining the usage log files of base stations, encrypting databases associated with personal privacy with passwords for their protection and management, positioning for the location of the illegal users, and so on. The future investigation of wireless cybercrime should consider the following four directions:

1). Searching for illegal Wireless AP

2). Locking up the hacker with the active illegal links

3). Setting up wireless honeypots

Setting up wireless intrusion prevention systems (WIPS) or wireless intrusion detection systems (WIDS)

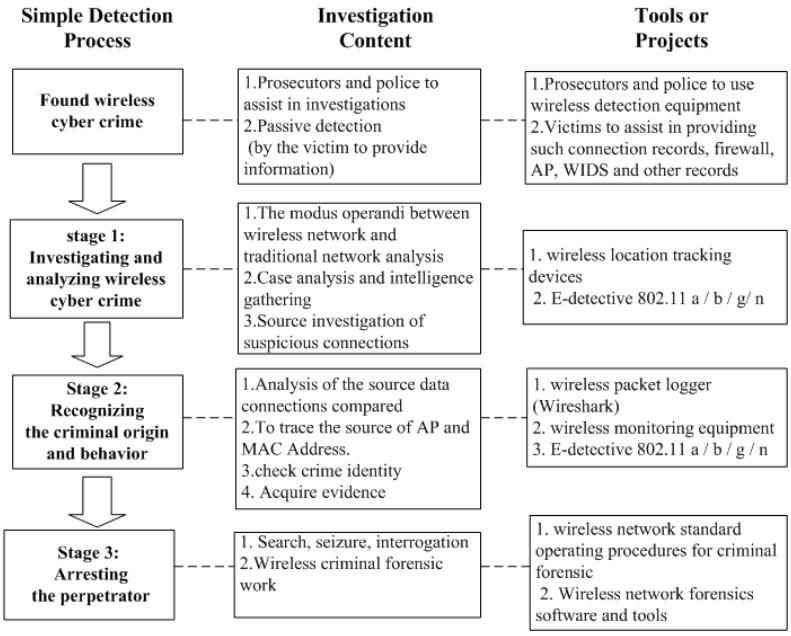

Fig. 3. Flow chart of wireless cybercrime investigation

3.3 Forensic Standard Operating Procedure for Wireless Network

Based on the Digital Forensic Standard Operation Procedure (DFSOP) by Professor Lin Yilong in 2006, we have proposed the "Digital Forensics Standard Operating Procedures for wireless crime" (DFSOP for wireless crime) in this study for the investigation of crimes related to wireless networks, as shown in Fig. 4. It can be considered as a reference for the investigation of crimes related to wireless networks.

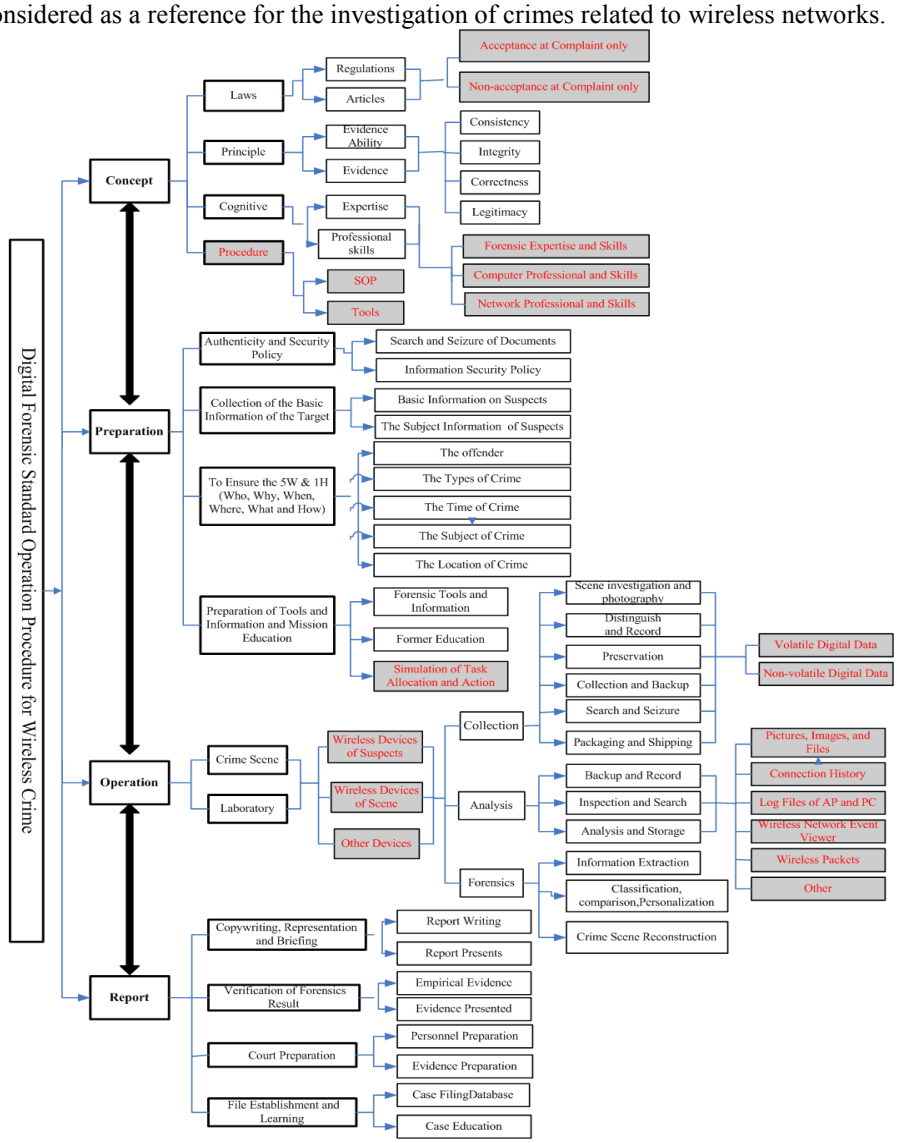

Fig. 4. Digital Forensics Standard Operating Procedures for Wireless Crimes

3.4 Example Validation for Wireless Internet Crime

As there are not many cases of wireless cybercrime, a case simulation was demonstrated in this study. Through the analysis with the framework theory, this case was presented with a structured approach. The crime, its investigation, and the forensics process were simulated. We hope that it will facilitate the investigation of wireless cybercrimes in the future.

1). time of crime: August, 2010
2). location of crime: Taipei County
3). criminal event: As a hacker, Zhuang online purchased credit card numbers, bank account information and personal information of cardholders. Taking advantage of the loopholes in the online banking settings, and using brute force password cracking, Zhuang could easily set the certificate password and then download the certificate. With the system vulnerability in the certificate security, he could successfully break through the certification process and then steal money from the accounts. Using the tool software downloaded from the Internet, he cracked the password of the wireless AP in the neighborhood and accessed the Internet to use the credit cards of others with the spillover of someone else's wireless network, with his online record hidden.
4). analysis of the offender: Suspect Zhuang, a habitual offender in credit card theft, found the loopholes of the online banking system using his expertise in the computer network. He purchased the personal information of credit card numbers and ID numbers of the cardholders online. Knowing how to hide his own Internet IP through a wireless network, he could invade someone else's wireless AP, and he successfully connected to the online banking systems, resulting in fraudulent logins and stealing money from the credit card accounts.
5). criminal damage: Breaking through the certification process of credit cards and then stealing money from credit card accounts. The known victims include Hua Nan Bank and Bank SinoPac, with large losses to victims.
6). indict and transfer: Penal Code Article 339 crime of fraud, Penal Code Article 358 offenses of impairment to use of computers
7). criminal process: See Fig. 5.
8). investigation process: See Fig. 6.
9). seized stolen goods and evidence: The notebook computer used in crime, the original applications for credit cards and their photocopies, bank accounts, credit card numbers and the printout of the detailed information of cardholders
10). investigating unit: Criminal Investigation Bureau, Investigation Team No.9

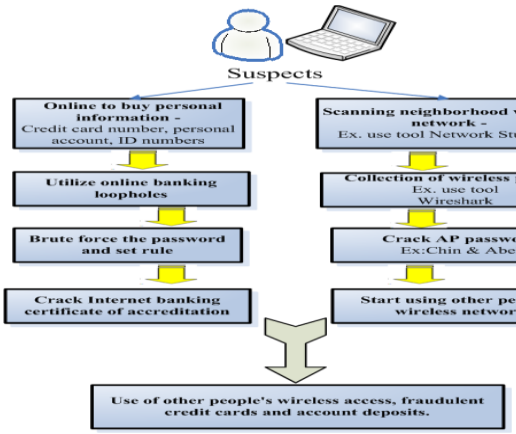

Fig. 5. Stimulated criminal process

According to the introduction to the case and the simulated criminal process, the process of investigating this case in this study is shown in Fig. 6.

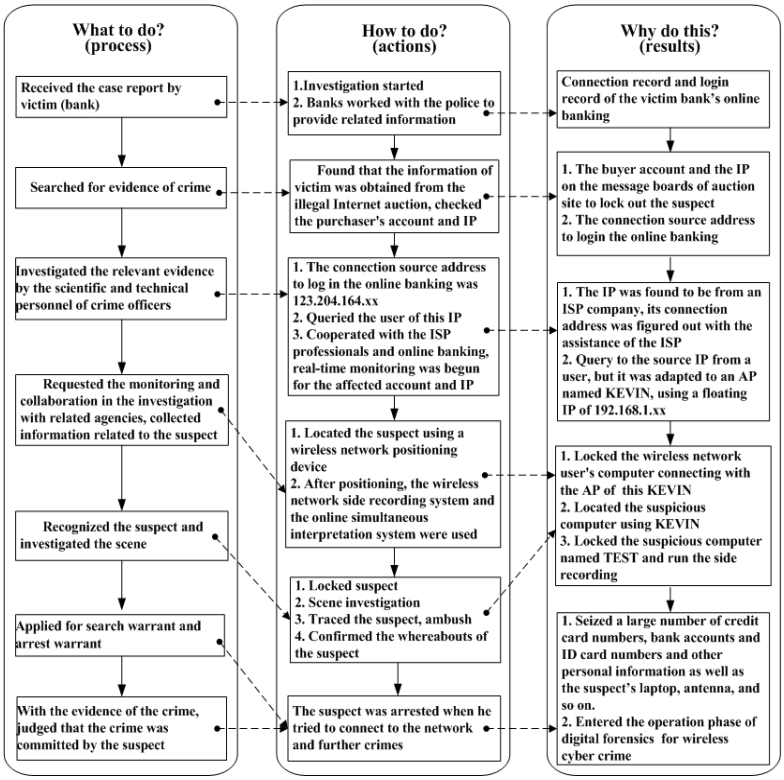

Fig. 6. Investigation process for a simulated wireless network criminal case

4 Conclusions

Information technology has done well in providing convenience, but it has also caused a number of new crime patterns. The prevention and investigation for general cybercrimes have been going on for several years. However, in recent years, with strong promotion and construction by government and the private sectors, wireless networks have gradually become a mainstream form of networks, and the problems of wireless cybercrime emerged. Because of their unique characteristics, special methods are needed to prevent and investigate crimes related to wireless networks. This standardized method is expected to become a reference for the study of wireless cybercrime investigation in future.

Wireless networking has changed the traditional methods of Internet access. Because the mechanism of wireless network access control is not perfect, when using a wireless network, we should understand its weaknesses and take the appropriate security measures. Although wireless networks have many security issues, and most users are not professional IT managers and lack an adequate understanding of network security, wireless networks are an inevitable trend. Therefore, we should pay more attention to the security issues and crime prevention before the problem of wireless cybercrime gets worse. With the proposed investigation approach available in advance, network security can be better protected.

References

1. I.L. Lin, “Cybercrime: Theory and Practice,” Central Police University, April 2009.
2. Eoghan Casey, "Digital Evidence and Computer Crime," Academic Press, March 22 2004.
3. Eoghan Casey, "Handbook of Digital Forensics and Investigation. Academic Press, November 9, 2009.
4. Beckett, J.J and Slay, J, “Digital Forensics: Validation and Verification in a Dynamic Work Environment, ” HICSS, Jan. 2007.
5. Patel, A and Ó Ciardhuáin, “The impact of forensic computing on telecommunications, ” Communications Magazine IEEE, Vol.38, pp. 64-67., Nov. 2000
6. Jill Sally, “Major Reasearch Issues in Forensic Computing,” nineth, “ 2007 Internet Space: Information, Laws and Society,” Theoritical Reasearch and Practice Conference, Nov. 2007.
7. I.L. Lin, H.C. Yang, C.H. Wang, “Reasearches on Related Techniques of Information Security Forensics,” Laws and Society,” Theoritical Reasearch and Practice Conference, Dec. 2002.
8. I.L. Lin, and T.S. Lan, “Discussion on Digital Evidence Collection Procedures,” seventh Information Management and Police Information Conference, Central Police University, 2003.
9. Casey, E, “Network traffic as a source of evidence: Tool strengths, weaknesses, and future needs, ” Digital Investigation, Vol. 1, No. 1, pp. 28-43, Feb. 2004.
10. J. Broadway, B. Turnbull, and J. Slay, “Improving the Analysis of Lawfully Intercepted Network Packet Data Captured for Forensic Analysis, ” ARES, 4-7 March, pp. 1361-1368, Jul. 2008.

11. Meehan, A, Manes, G, Davis, L, Jale, J, "Packet Sniffing for Automated Chat Room Monitoring and Evidence Preservation, " paper presented at the IEEE, Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, Jun. 2001.