BEST PRACTICES IN CYBERCRIME INVESTIGATION IN THE REPUBLIC OF KOREA

*Junsik Jang**

I. INTRODUCTION

The Internet and the rapid deployment of information and communication technologies in recent years have changed historic trends and practices in criminal investigation. This has created a tremendous challenge for law enforcement to develop the capacity to confront transnational crimes and follow evidence trails. Among the obstacles were legal, technical and operational challenges, but these are not the total extent of the difficulties faced; rather, they have been recognized as the main issues to be addressed in order that law enforcement agencies are able to meet the emerging challenges of cybercrime.

When police conduct a cybercrime investigation, they are encouraged to refer to the following several sources of regulations and guidelines:

- National Law: Both of the main procedural barriers and weapons are produced by national criminal procedural laws. Without meeting the legal requirement, investigative activities would be considered illicit and the admissibility of evidence acquired will be denied. As previously mentioned, several laws regulate directly collecting cybercrime evidence, including the Criminal Procedural Act, the Protection of Communications Secrets Act and the Telecommunications Business Act.

- International Law, Standards and Guidelines: There are such conventional frameworks as Mutual Legal Assistance Treaties and organizations such as Interpol which are useful for international investigative co-operation considering the borderless nature of cybercrime. Even without compulsory regulation, pursuing international legal references is considered desirable.

- Domestic Guidelines and Manuals: To provide practitioners with a practical reference for action, the Korean National Police Agency has developed several guidelines and manuals.

Table 1: Cybercrime manuals and guideline

Title	Scope	Contents
Cybercrime Investigation General Manual (classified)	All members of police	• Cybercrime definition, category • Preliminary Investigation • Processing Crime Scenes • Tracing, Search and Seizure • Evidence Handling • Interview and Interrogation • Checklists • Cybercrime Laws
Internet Tracing (classified)	Cyber Investigators (mandatory) Other police members (recommended)	• Foundation • Internet Protocols and Addressing • Web, e-mail, Other service tracing • Subscriber's Line • Real-time tracking and tools

* Professor/Senior Inspector, Department of Police Science, Korea National Police University, Republic of Korea.

Digital Evidence Analysis (classified)	Cyber Investigators (mandatory) Other police members (recommended)	• Foundation and Process • Windows Analysis • Unix System Analysis • Network Analysis • Tools (Encase, ILook, Final Forensics, X-ways)
Cybercrime Investigation Techniques for Its Types (classified)	Cyber Investigators Other police members (recommended)	• Hacking and Virus Investigation • Illegal Contents Distribution Investigation • E-commerce Investigation • Complainants Counselling Q&A
Standard Guidelines for Handling Digital Evidence (unclassified)	Public (recommended)	• Collecting Evidence • Transferring and Requesting Examination • Evidence Analysis • Writing Reports
Digital Forensics Technical Manual (classified)	Cyber Investigators (mandatory) Forensic Examiners (mandatory)	Standard Procedure for: • Collecting Evidence • Disk Recovery • Hacking and Malicious Code Analysis • Web Analysis • E-mail and Instant Messaging • Database • Multimedia • Crypt Analysis • Detecting Steganography • Communication Network Analysis • Mobile Device Analysis Checklists

II. INITIAL INFORMATION GATHERING

Investigation generally begins by gathering initial information from a variety of sources. Investigators have to understand the characteristics and develop the sources. Some victims do not want to reveal the damage they have suffered out of consideration for their reputation and for other reasons, or even do not recognize the damage caused to them. On the other hand, for example massive worm infection, others report the same information repeatedly which may make investigative efforts redundant.

Information gathering to fight cybercrime should be strategic. Through their experience, the Korean National Police Agency developed some criteria to alleviate the complexity of cybercrime which should be taken into consideration when developing info-gathering mechanisms.

- Timeliness
- Scope and Impact
- Technical Level Needed
- Proactive vs. Reactive
- Machine-based vs. Human-based
- Attack by Opportunity vs. Attack by Target.

A. Web-based Complaints Report and Counselling Service

To promote convenient complaint systems and to reduce processing costs associated with conventional reporting methods, the Korean Police adopted a web-based crime report system in 1999. But, soon after,

cybercrime investigators realized that the system could be designed so as to collect more information concerning further investigation and to find additional valuable information by analysing multiple complaints. For this, they decided to set up an independent cybercrime report system. Because a similar idea was applied in business, named Customer Relationship Management (CRM), the newly launched system was called e-CRM when it was established in 2003.

Today, the e-CRM system is the greatest resource of cybercrime information. By simultaneously analysing massive reports, the authorities can ascertain pattern, commonality, and level of threat. If more proactive, intensive, and technical investigation is needed, an investigative team of the CTRC is assigned to investigate the case. Drawing a bigger picture with minute events is becoming more and more important.

B. Intelligence Activities

Undercover operations, decoys, and other intelligence activities are easier on the Internet where anonymity can be secured. Keeping accounts for websites and as many other communities as possible is highly recommended.

Traditional intelligence activities should not be neglected. People tend to trust more someone who they have met in person rather than a total stranger. System managers and other personnel in corporations are potential great informers in important cases. Maintaining contact points and systematic management seems one of the most important tasks in fighting cybercrime. Gathering information from international resources is desirable and is encouraged.

C. Honeypots

A honeypot (or honeynet) is a system or network that has intentional security vulnerabilities to gather information and/or evidence in case of access by attacker(s). If it is not designed well, legal challenges may arise. Therefore, a honeypot is usually built during a case investigation.

III. TRACING AND IDENTIFYING CRIMINALS

People take advantage of the anonymity of the Internet to facilitate their digital life. Abuse of the anonymity of the Internet by criminals is a predictable but inevitable dark side in an information society. The difficulty of tracing and identifying criminals is one of the main hurdles that cyber investigators meet every day. On the other hand, techniques used for tracing criminals can be applied to locating non-cybercriminals as well. The Korean Police has been making efforts to develop tracing techniques and the products are being widely used for every kind of criminal investigation.

Tracing is rarely confined to a single action, but rather a series of tedious operations. It is not odd if an investigator sends dozens of written requests seeking legal permission from prosecutors and courts in an investigation. To minimize the burden, investigation should be planned strategically and tactically. In many cases, critical information can be provided by service providers, including Internet Service Providers (ISP). Needless to say, maintaining intimate relationships is important.

Unfortunately, getting helpful information from service providers is frequently difficult for many reasons. An investigator needs technical or human skills to overcome such difficulty. Experienced investigators in the CTRC who know the possibility and the limitation of each technique are available to answer questions concerning tracing matters.

A. Basic Communication Information given by Service Providers

Legal procedures were explained in the previous paper. It usually takes more than a day to complete the whole process unless there is an emergency situation. That is why time management is important. Otherwise, cybercrime investigation will be a chain of requests for communication information with a risk of the case failing. The list of service providers is available for police officers with the help of their own collaborative colleagues.

Some service providers have implemented a real-time notification scheme via an investigator's mobile phone or closed webpage to provide the information possibly containing the cell location of a mobile phone, log-on and log-off status, IP address, etc.

B. Subscriber's Network Service

To ultimately discover the location and identification of a target, cyber investigators often have to get a subscriber's information from the Internet Service Providers (ISPs) because many users access the Internet through a subscriber's network service. The possibility of getting information from an Internet Service Provider depends on the type of service, and the logging policy. Sometimes investigators find out the physical location they want to know without further information, because the ISPs are not helpful without proper logging. The variety of services makes it difficult. Today, rapid propagation of mobile Internet use is a critical issue. Table 3 shows the past and present subscriber's networks services.

Table 2: Subscriber's network services in Korea

Type	Service	Usage	Possibility of Tracing by ISP's information
Wire SNS	Serial Line Internet Protocol/Point to Point Protocol (SLIP/PPP)	Obsolete Very Low	Very High
	Integrated Services Digital Network (ISDN)	Obsolete Not Available	Very High
	Asymmetric Digital Subscribers Line (ADSL)	Prevalent	Depends on ISPs' authentication method Very High or Low
	Very high Data rate Digital Subscribers Line (VDSL)	Prevalent	Low
	CABLE	Prevalent	Depends
	Power Line Communication (PLC)	Obsolete Not available	N/A
Wireless SNS	Wireless Local Loop/Broadband Wireless Local Loop (WLL/BWLL)	Not Prevalent	High
	Wireless Local Area Network (WLAN)	Prevalent	Depends on circumstances
Mobile SNS	IS-95ABC/ Broadband Wireless Local Loop (IS-95ABC/EVDO)	Decreasing	Circumstantial
	Wireless Broadband Internet (Wibro)	Increasing	
	High Speed Downlink Packet Access (HSDPA)	Not prevalent	
Satellite SNS		Rarely used	High

C. Internet Cafés

Once the target of a trace action can be identified by an online user account or nickname, there is a possibility to capture the suspect before he or she leaves the Internet café. It is effective when real-time tracking is available. Fortunately, the Korean National Police cover the entire country and a dispatch system using police radio make it possible for the responders, typically patrol officers, to reach any Internet Café within 10 to 15 minutes. The fact that this really works has been proved repeatedly, including a case of apprehension of a bank robber who gambled online in an Internet café after committing the robbery.

Otherwise, investigators may find out other clues through examination of the PC used, witnesses, etc. Cyber investigators sometimes forget the importance and potential of physical traces. Traditional trace evidence such as hair, print and fiber may have to be collected for further investigation. Investigators also have to be cautious that many PCs in Internet cafés are equipped with hardware or software-based hard disk recovery tools requiring more careful treatment.

D. IP Laundry

Criminals want to be shielded behind computers to block tracing back by investigators. Since a computer is identified by an IP address, blocking is often called IP laundry. IP laundry is more common for average criminals and this is a universal problem in law enforcement. There is no perfect criminal haven, but, depending on the technique used for IP laundry, some tracing methods are extremely difficult to adopt and very time-consuming. Basic IP laundry techniques are categorized as follows:

- IP concealing: Hides the existence of original systems used by a perpetrator by a detour using an intermediate system through a specific Internet service such as proxy, secure shell, socks, VPN, remote control, and so on;

- IP forgery: Changes source IP address in packets to conceal and deceive origin. Address Resolution Protocol (ARP) spoofing is usually implemented to intercept communications, called sniffing, but also can be used to hide origin;

- Domain Name System (DNS) altering: Does not conceal or change IP addresses of the source computers. Instead, it often changes the source computers themselves, typically zombies, by the using of the functionality of dynamic DNS.

Techniques to defeat IP laundry vary. Some of them are not intentionally documented in the manual to preserve their operational effectiveness. Proper consultation may be needed from a technical support of the CTRC.

E. Tracing Method for Individual Internet Services

- E-mail: Due to prevalent use of header forgery, mail server investigation and proactive e-mail tracking is frequently used.

- P2P: The CTRC provide automated well-known network-based P2P tracking software.

- Website users and operators: Should be tactical enough, especially when tracking operators.

- Web based short message service (SMS) sender: Investigators need a full understanding of the service mechanism. It is normally a tedious procedure.

- Mobile device holder: If a mobile device is chosen by a criminal to avoid tracking, locating it usually is extremely vexing work. Some software and hardware are available for this purpose from the CTRC.

IV. PRESERVING AND COLLECTING EVIDENCE

Scene processing has to be completed by experienced and qualified investigators or examiners, but they are not always available. In any case, coping with the standard procedure and technique proposed is important. Recently proposed standard procedure for cybercrime scene processing is defined in the Digital Forensics Technical Manual 2007. This standard is applicable for typical digital evidence collecting situations concerning computer systems and peripherals:

- Photography and Sketching: Taking pictures of the front and rear shots of object system, peripherals, monitor and other necessary images;

- Volatile Information Gathering: Volatile information needed is enumerated in the manual. The Cyber Terror Response Center provides automated tools in a CD called "*Podomi*" (meaning police helper) which is highly recommended if the investigator is not fully qualified to select alternatives;

- Shutting Down: The decision of how to shut a system down should depend on the operating system being used. Roughly, server systems follow a normal shut down process and personal computers are unplugged. The details are defined in other parts of the manual;

- Acquiring Physical Media: Seizing whole systems is principally recommended. Exceptionally, storage media such as Hard Disk Drive (HDD) can be seized separately. In any case, system time should be

previously recorded in comparison to Korean Standard Time (KST);

- Labelling and Packaging: an adequate label has to be attached to each item, including case number, collector, date and time, location, specification of the item, serial number if possible, etc. HDD and other electro-magnetic media should be packed individually using proper bags or boxes;

- Documentation: Chain of custody, process of scene investigation, lists of evidence to give the owner and a Q & A sheet should be documented and preserved.

V. DIGITAL FORENSIC ANALYSIS OF EVIDENCE

It is principle that all digital media be examined and analysed by a qualified forensic examiner, but there are too many items that need forensic investigation and the number is rapidly increasing. Consequently, there is an explicit gap between needs and current status. This tends to produce backlogs and sometimes leads to field investigators abandoning requests for forensic service, which can have unexpected consequences. Cyber investigators are trained to examine digital evidence to some extent. Beyond that, forensic service is requested of high level police agencies.

The Digital Forensic Center in the CTRC is the biggest and the most comprehensive digital forensic laboratory in Korea. Several provincial police agencies have digital forensic labs and the number is increasing. The active service is listed in the Digital Forensics Technical Manual published in 2007. However, considering the rapid change in ICT environment, the scope of service request is not confined within the current service list.

Before the establishment of the DFC in 2004, forensic investigation had been conducted by investigators who had ICT backgrounds or as a form of technical support without strict regulation. The number of electromagnetic media requested for forensic service was only 274 in 2005 and it increased to 2,984 in 2007. However, it is believed that the actual needs much exceeded the number of the received media, because many requests are being refused by service providers due to the lack of resources or abandoned by investigators considering the current situation. Increasing media size is also problematic. The average hard disk drive size received for forensic examination was 68.33 gigabytes and increased to 89.14 gigabytes in 2007. Strengthening forensic capability is one of the most urgent problems that the CTRC and cyber police are confronting. Research on 99 sample cases showed that the average waiting period until returning the item, that is the time used to complete a forensic request, was 3.24 days per item.

Forensic labs are required to gain accreditation from a qualified body. There are many unsettled issues concerning digital forensic lab accreditation. The DFC is preparing to apply to domestic or international accreditation bodies.

VI. INTERNATIONAL CO-OPERATION

Although much international co-operation does not achieve tangible output such as apprehension of domestic suspects, Korean investigators, especially those working at the Cyber Terror Response Center, are very proactive in responding to requests from foreign law enforcement agencies. Needless to say, it is because they know the importance of international co-operation and the fact that they may also need similar help by the requesting country someday.

As a result, most of the international co-operation cases are investigated by the Cyber Terror Response Center. If it seems appropriate considering time and difficulty, a request can be transferred to local police, and more time will be needed to respond. Once a request is delivered to an investigator, he or she opens a new domestic case based on the information in the request. It is possible because the majority of requests include domestic suspect(s), victim(s), or a location where a crime was committed. For this, the request should contain a detailed description of the case and the reason that an investigation is needed in Korea.

The most active channel for international cybercrime investigation is the International Criminal Police Organization (hereafter: Interpol). But there are other channels which have respective strengths and weaknesses.

A. Mutual Legal Assistance Treaty (MLAT)

MLATs are the most powerful legal tool. In practice, however, this is rarely used for police investigation of cybercrime because of the length of time needed to complete the whole process.

B. G8 24/7 High Tech Contact Points

The G8 created in 1997 a new mechanism to expedite contacts between countries to enhance and supplement traditional methods of obtaining assistance in cases involving networked communications and other related technologies. The system is maintained by the Supreme Prosecutor's Office in Korea and is not usually available for the police. Because the majority of cybercrime investigations are conducted by the police, the usability of the mechanism is low.

C. Interpol

Interpol, with 186 member countries, is the most commonly used channel for international cybercrime investigation co-operation in Korea. Hundreds of cases are dealt with annually through the Interpol channel. The National Central Bureau, a single contact point in each member country, possesses a 24/7 network and is staffed by highly trained officers.

However, the effect of co-operation through the Interpol channel seems limited because it is not obligatory, but voluntary, and is conducted without a legal basis which would enable the use of more effective methods, including the exchange of physical evidence. In addition, inadequate knowledge of technical matters on the part of the officers of the National Central Bureau often hinders communication between investigators.

D. Liaison Officer (24/7 Contact Point)

To address international co-operation matters, the Cyber Terror Response Center has designated liaison officers. They also maintain the National Central Reference Point (NCPR), proposed by Interpol, which is designed to counteract the disadvantage of traditional co-operation by the National Central Bureau. Typically, once an initial request is delivered to NCB, ongoing co-operation can be conducted via the NCPR through e-mail and/or telephone.

E. Cybercrime Technology Information Network System

The Cybercrime Technology Information Network System (CTINS), operated by the Japanese police, is a network system connecting law enforcement agencies in the Asia-Pacific region. The CTINS is a good instrument to share technical information concerning cybercrime, but is rarely used for specific case investigations.

F. Human Networking

Sometimes, investigators prefer contacting counterparts directly to exchange more detailed information faster. Once acquainted, this unofficial networking would be more smooth but still powerful. The CTRC encourages its investigators develop its human networks.