Utilizing of Information Technology for Locating Cybercriminal in Computer Related-Crime

Naughtakid Phromchan[1] and Sanon Chimmanee[2]

[1]Science in Information Technology Management, College of DIIT, Rangsit University, naughtakid@gmail.com

[2]Science in Information Technology Management, College of DIIT, Rangsit University, sanon.s@rsu.ac.th

----

ABSTRACT

This research was study of the guideline in investigating to search the culprit who used computer in committing crime via internet. The researcher used the technique and investigative method well known in universal police circle and using Information Technology that could be found generally to apply in searching the position of cybercriminal by studying the operation of official in searching the criminal from the actual case and to analyze and explain the crime analysis process. The researcher used three domains including (1) the concept on criminal analysis (2) technique and universal investigation and (3) using of Information Technology to improve and process in order to be a guideline for official to use in the investigation to find the position of the criminal in computer-related crime.

This research will be beneficial to investigative officer and could be used as a guideline in finding the position of a criminal in a computer-related crime or cybercrime in the same type by oneself. This is the process which is correct and fast and the process from this research could be used as a prototype in developing personnel and knowledge on related investigation.

Keywords: Crime Analysis, Criminal Investigation, Investigating Internet Crime

1. Introduction

From the study of the problems and obstacle of the work operator on investigation especially the work on following up the suspect in a criminal case. The important problem and obstacle on personnel is the fact that the police who is responsible for investigating work would lack learning and technique including lacking information technology use and communication for the work operation on investigation (Norramat, 2016). The researcher sees that solving of problems to increase the knowledge and developing of technique and method in finding the suspect in a criminal case and finding of information technology would help the operation to be more efficient. It is not apparent that there is not any principle or theory, so it should focus on learning from actual case operation in order to develop as best practice especially speaking of investigating science, it is generally accepted that it is scientific investigation which is an operation to solve problems and it requires actual evidence that is apparent and can be proved. Investigation is also arts which is to choose concept, expectation, solving problems by using expertise from skill and experience. Successful investigation would create justice which can proceed with the case and push the offender (Angsananont, 2010). Therefore, may types of investigating work is highly complicated and must use skill and need to use many factors (Karl, 2006). Computer-Related Crime is an example of hard investigation work. From the fact that the culprits use the nature of the internet which could conceal themselves and not facing directly which is different from the old way that is physical which the wrongdoers must be at the place always. The investigating officer must have knowledge and skill on computer necessary more than general criminal case (Buadistdecha, 2008). Nowadays, the advancement from technology and communication create higher use of computer to use the internet (The National Statistical Office of Thailand, 2016) just like crime in the type of information technology more. On the contrary, the information that is from using of computer equipment have increased according to the increased number of users. This can be used in investigation to specify the position of the suspect according to the warrant in the criminal case that uses various communication equipment. The researcher sees that the investigating knowledge on technology can be applied with the information technology and related communication in order to find the position of the offender in the criminal case. This research focuses on how to explain investigation method to find the culprit from the sample case in the case relating to technology which culprit uses computer to connect the internet by using the concept framework from criminal analysis and knowledge on investigating technique and to use related information technology to compile and propose as a guideline to search for the address of the offense in a criminal case which would be beneficial to investigative officers and related people to know the process and method of investigating to find the culprit in a criminal case.

2. Objectives of the study

1. Studying the investigative method of the position of the criminal from using computer equipment to commit crime via internet.

2. Studying the guideline to use Information Technology to support position finding of a criminal in computer-related case or cyber case.

3. Materials and methods

From the crime analysis process (Baltaci, 2010) as shown in a figure 1, this paper investigates the actual computer-related crime cases by using IT techniques and applies this case to the crime analysis process. This leads to obtain a novel conceptual framework about locating the cybercriminals known as Locating Cybercriminals using Information Technology techniques based on the crime analysis process (LCIT).

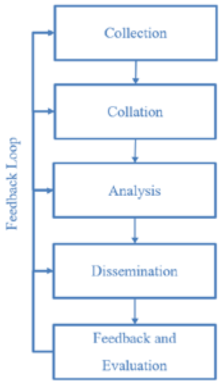

Figure 1: Crime Analysis Process (Baltaci, 2010)

The crime analysis is to use analysis in helping decision-making directly of law enforcement officer which is a process to find the patterns and to understand the relationship of the related data and to put in order and specify the target in the operation of officials in that work in the Crime Analysis Process. There are 5 orders and it is in circle. Each circle can go back to perform in the previous step depending on the things that happen to the end user. If the data were received or there might be a new requirement, the details are as follows. Collection, Collation, Analysis, Dissemination, and Feedback and Evaluation.

The proposed framework consists of three domains: the crime analysis process, a concept of traditionally tactical police investigation, the IT techniques as shown in a figure 2.

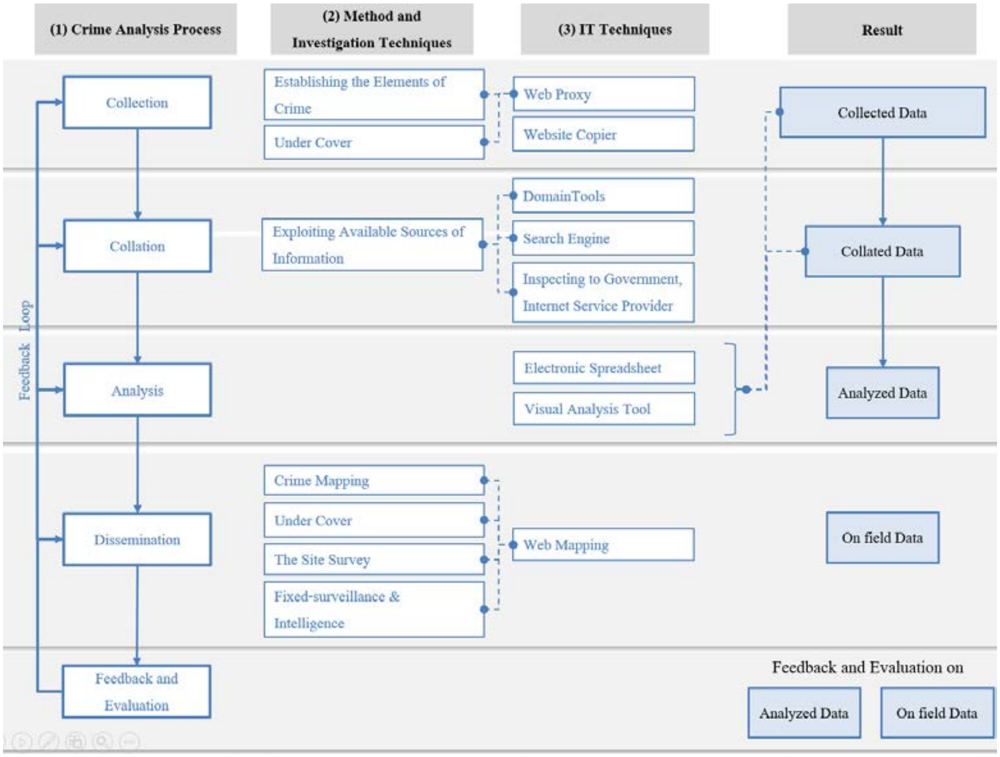

Figure 2: The framework of Locating Cybercriminal using IT techniques based on the Crime Analysis Process (LCIT)

Using thinking concept from criminal analysis which consists of Collection, Collation, Analysis, Dissemination and Feedback and Evaluation. The 5 steps are in order and can work in circle going back to the previous steps depending on the things happening to end user. If receiving more information or wanting new demand, the researcher used an actual case in proving the presented concept in the results as a case study.

4. Experiment Results

The investigative guideline to find the position of a criminal who committed Computer-related crime by using investigation technique and applying IT to follow the presented concept by separating into 5 steps as follows.

4.1 Collection step

Collecting of information by establishing the elements of crime because it cannot be specified that in said webboard had shown information or story or related people who is guilty according to the law. Officials must try to prove the possibility in each point by specifying who is a criminal that advertised to sell guns according to the news received. If any point has evidence that it is not related, then it can be excluded and make a narrower investigation and to finally reach the target. In this step, official must investigate people who selling illegal guns in the webboard by using undercover investigation and to act as general webboard user and use internet tools in the type of web proxy such as https://hide.me/en/proxy to hide the place that officials who used internet prevents the criminal to find out.

Collecting information from webboard that could be used easily in offline investigation at the computer of the investigator by using the tools that can be website copier such as HTTrack which can store important information including pictures and message which can be referenced and to be evidence.

From the case study, the important information is gathered as follows.

1) Found the webboard user with username as “MehPooh" who advertises to sell guns on the website www.xxxwebboard.com specifying the target to investigate the position.

2) The Seller under the name “MehPooh” posting the goods details as gun and specified the buying condition to transfer the money via banks and then sent the goods via EMS and under no circumstances would meet face to face. Anyone interested can leave telephone number and Seller said that he had the email in contacting.

3) Finding the content of the many webboard members praising the goods quality that username “MehPooh” used to sell.

4) Finding many webboard users expected to know or familiar with the Seller under the name “Mehpooh” in the name “Pol”.

5) Finding one webboard user using the link of the picture claiming to be the picture of “MehPooh” to post in order to see the data and finding the pictures of a male at the age of around 20 years and suspecting to be the pictures relating to the target.

The result achieved is that the information that can be inspected or to be important information used to prove the criminal or the offense that the criminal can do (Vyas, 2016).

4.2 Collation step

In this step, it is the inspection of information from collection. Official can exploit available sources of information that is from (1) data of the government agency such as the data of people from civil registration, the criminal history from the Royal Thai Police, vehicle registration database from the Department of Land Transport. Company information from the Department of Business Development (2) the data of private sector collected for the business such as the telephone use information from telephone service user, internet traffic data of the internet service provider, financial information from commercial banks etc. (3) the public information or that could be searched on the internet such as searching via Search Engine, Domain Tools, People Search service.

From example case, the information received from inspection is as follows.

1) Domain Tools to acquire the registrar and the company which is the hub of the webboard.

2) Search Engine can inspect various information of the domain registrar appearing on the internet for the benefit of connecting with other evidence and to inspect the information of the hub to know how to contact the information from the company.

3) Information from Internet Service Provider that the website or the target webboard connected.

3.1) Service Provider: Internet Data Center or IDC giving the information of the service lessee Co-location.

3.2) Service Provider: Co-location giving the information of Web Hosting service.

3.3) Service Provider: Web Hosting provided the information of leasing the place to create webboard and to be the owner of said webboard.

3.4) The webboard owner and administrator gave the IP Address of the username MehPooh to reach various posts and found that the criminal accessed the webboard via the IP Address 183.xx.xxx.xxx, date xx time xx.

4) Verification of the internet service provider that provided the service to the criminal would use the name of the lessee and the internet location or the place that the internet user would reach the webboard.

The result from the verification enabled officials to know the information regarding the name, company or the related place in the case especially, inspection of IP Address of the criminal from reaching the website and connect the people and place using the internet which made the investigation to find the position to be much narrower (Crist, 2017).

4.3 Analysis step

The analysis of important information received from gathering Data set A and processed with important information received from inspection of Data Set B is to bring the data from A and B in the part relating to people and the place specified as the place that the criminal used the internet and separated it into parts by interest and details which can indicate or connect the criminal by using MS-Excel according to the table.

Important data received from	Related people	Gender	Age	Name	Picture
1.Data Set A (from webboard)	1	Male	Around 20 years	MehPooh or Pol	By Figure
2. Data Set B (from various points)	4	Male#1	42 years	Name as Somchai	Different
		Female#1	38 years	Name as Warunee	Very Different
		Male#2	22 years	Name as Meepol	Very Similar
		Female#2	10 years	Name as Manee	Different
3. Basic analysis	Anyone in 4 people might be the suspect	The suspect might be male	The suspect's age about 20 years old	Some part of the criminal name is Pol	Face of the Male#2 is very similar to the suspect
Opinions of official	From the data, it was found that the suspect in this case might be male, age around 20 years, nickname Pol which is consistent of the people according to the place that the criminal uses the internet. Said people is male age 22 years old with the real name Meepol which is very close to the nickname of the criminal and when comparing with the pictures found with the pictures from the civil registration, the face is very similar.				

The result from the analysis, the interest is focused on "Meepol" and the officer saw fit to observe the movement of that person in the house to prove that the person has the address at the specified place and to live in or to use the internet at said place or not by using the investigative officer to make the map of the target house and adjacent area to use google map to plan in surveying the next place.

4.4 Dissemination step

To go in to prove the area by using information from analysis related to people and the place.

1) Crime Mapping Planning going into the area by using Web Mapping (Google Map) to help.

2) Under Cover to disguise into The Site Survey to survey the place and to know the house and to know entrance and exit and to know the movement.

3) Fixed-surveillance & Intelligence To follow up on the movement and to know that criminal would be in a house which is the time of the post in the webboard.

The result received is the field data that would be considered and evaluated the operation.

4.5 Feedback and Evaluation step

Consider the result received from the analysis and going into the area to meet related reasonable data as follows.

1) From the survey of the place and observation of the behavior of people in target house for the total of 5 days, it was found that the movement of people in said house by Male#1 (Mr. Somchai) and Female#1 (Mrs.Warunee would leave the house during 12.00-13.00 hours and going back at around 24.00 hours. As for Male#2 (Mr. Meepol), he would leave the house at around 14.30-15.00 hours and would often hold a plastic bag and drove a motorcycle from the house and come back without anything at around 17.00 hours and would not leave the house for the entire night until next day in the afternoon.

2) The case of the movement in the webboard it was found that the member user "MehPooh" who is the target in the investigation and posting at the time from 20.00-02.00 hours which is the time consistent with the time that Mr.Meepol stayed at said house and left the house in the afternoon and came back in the evening (expected to deliver the things at the post office). Considering from all the data which were consistent, and it is believed that Mr.Meepol or Pol and/or the user "Mehpooh" who advertised to sell illegal guns which is the target that the officials want to arrest.

3) Collecting data received from the webboard of website investigation and the IP address received from the internet service provider and the webboard service provider and to receive the IPD address of the suspect and the survey data and follow up on the movement of related people which could be seen that the data were consistent and connected which all the documents were gathered and shown as evidence and to request the approval to the court with the power in the area and to search and arrest Mr.Meepol while staying at said house.

From the search, Mr.Meepol is found along with many war guns and pistols, the officials notified the offenses and then Mr.Meepol confessed that his nickname is Pol and he is a user under the name "MehPooh" and he advertised to sell many items of illegal guns. Later the police checked the internet history of PC computer of Mr.Meepol and found to have get into various webboards and recorded User-Password of the user name "MehPooh" in the notepad and saved pictures of the same gun that the police found in the computer along with payment evidence via bank and evidence of delivering the package at post office.

5. Conclusion

This paper presents the LCIT framework consisted of three domains: the crime analysis process, Traditionally Tactical Police Investigation, and IT technique. This framework is approved by using the actual case: Finding a location of criminal from computer accessed the Internet. This leads to obtain the best practice for utilizing of information technology in order to locate cybercriminal in computer-related crime case.

However, finding a location of cybercriminal from computer accessed the Internet where the location of the web hosting server that illicit is served is outside of Thailand e.g. Instagram, Facebook. The special IT technique such as phishing will be applied to obtain IP address of illicit this is stay in Thailand. This enables us to find the location of place where is accessed the Internet. Such case should be studied in the further work.

References

Angsananont A.: Criminal Process LA335 (LW443). Ramkhamhaeng University Press, Bangkok (2010).

Baltaci, H.: Crime Analysis: An Empirical Analysis of its Effectiveness as a Crime Fighting Tool. (Unpublished Doctoral dissertation). The University of Texas at Dallas, Texas (2010).

Buadistdecha C.: Criminal Liability for Cyberstalker. Master of Laws Program in laws, Faculty of Law. Chulalongkorn University (2008).

Crist K.R.: Utilization of Location Information on Digital Media Devices. Master of Science in Cybersecurity, Faculty of Utica College (2017).

Karl A.: Criminal Investigation: Motivation, Emotion and Cognition in the Processing of Evidence. Department of Psychology, Göteborg University (2006).

Norramat S.: Barriers to Arrest of Criminal Offenders with Criminal Arrest Warrants: A Case Study of the Metropolitan Police Division 4. Master of Public Adminstration, In Criminology and Justice Adminstration College of Government Graduate School, Rangsit University (2016).

The National Statistical Office of Thailand. The use of computers, the Internet, mobile phones 2007-2016. Accessed July 15, 2017 (2016) Available from http://service.nso.go.th/nso/web/statseries/statseries22.html

Vyas B.R. The Value of Mobile Device Metadata for Investigations. Master of Science in Cybersecurity, Faculty of Utica College (2016)