ISSN 2630-0540
Journal of Technology and Innovation in Tertiary Education, Vol.1, No. 2, pp. 24-36,
July-December 2018

doi: …./jti….

Utilizing Information Communication Technology in Locating Criminal Offenders in Criminal Cases

Naughtakid Phromchan and Sanon Chimmanee
College of ICT, Rangsit University, Phatum Thani, Thailand
Email: naughtakid@gmail.com

Abstract

This research investigated the trace of suspects in criminal cases with the use of a mobile telephone and computer equipment in communication. The researchers used the technique of *popular investigation* in the universal police circle and applied it to information technology and related communication. It was to explain how to investigate and to find the suspect according to the warrant in an actual criminal case in drug use and trafficking. The researchers used the concept of Crime Analysis Process to analyze the suspect's acts in committing a crime by using information technology. The researchers adapted improvement techniques in various steps to process the investigative guidelines to locate the position of the suspect. The improved techniques and the investigative process in the study are expected to serve as a prototype to be beneficial to investigative officers to locate the position of suspects or offenders systematically, correctly and quickly.

Keywords: *Information Communication Technology, crime analysis, crime investigation, Internet crime, mobile phone investigation*

1.Introduction

Studies in problems and obstacles of investigative officers in tracing suspects in criminal cases are often of public interest. One limitation in criminal investigation has been identified as the police lacking knowledge on techniques in information communication technology to conduct their investigation effectively (Norramat, 2016). The researchers of this study perceived that knowledge in information technology and communication and technology-based techniques could help investigative officers to locate suspects in criminal cases effectively. It should be noted that the literature in information technology as related to criminal investigation, and investigating science has not dealt any principle or theory for applications in criminal investigation. However, parties concerned in this area have currently recognized that scientific investigation should be the trend in operation to render a certain degree of success in tracing suspects or offenders in criminal cases.

Investigation is an art in itself for an operator to choose a conceptual framework, set expectations, identify problem-solving techniques, and seek expertise skills from people in the field. Successful investigation in finding the offenders would create justice to be witnessed by the public (Angsananint, 2010). Therefore, many types of investigating methods tend to be highly complicated in skills used and influential factors involved (Karl, 2006), as seen in investigation of drug cases as organized crimes. The accomplice would split the duties to perform, such as transporting, drug place observing, money laundering, wholesaling, middleman mediating, brokerage, and retailing by small traders. In each stage, offenders work secretly just like operation of well-trained officers.

With such a scenario, effective investigation to arrest people related in drug cases requires an effective operation plan of police investigators, ranging from sending spies to mingle with wrongdoers, usually as undercover agents with the investigated group to keep a close watch on the movement (Vimollohakam, 2010). Computer-related crime is also a hard investigation work for the fact that the culprits use the Internet to conceal themselves with fake identities. Investigating officers need to be highly literate in information technology with computer and cyber skills (Buadisdecha, 2008). Nowadays, the advancement of communication technology creates intensive use of mobile telephone and computer to use the Internet (The National Statistical Office of Thailand, 2016), and thus generating crimes with the use of information technology. A massive use of smart phones and modern electronic devices has proportionally increased the number of crimes on the Internet (Cybercrime Another Medal in the Digital Age, 2017).

Research of Vyas in 2016 indicated the importance and high value of *Metadata* generated by the use of smart phones which indicate evidences in the form of the behaviors of users and officials. The research by Crist in 2017 studied the data on places available on computers and mobile phones which would help investigative officials in explaining various incidents happening in the incident place, status of the victim or the suspect on the crime scene or in the crime case. The research by Kumar, Hanumanthappa & Kumar in 2016) studied data on specifying the ways telephone is used in communication of offenders:Call Detail Record or CDR, which analyzes communication messages of those who committed the crimes. These three researchers proposed to secure CDR data in a central service provider to conduct CDR analyses efficiently, as required. Romsaiyud & Premchaisawasdi (2009) reported the use of technology in specifying crime coordination by using Cell-ID that is already present in each network system and can support the operation inside the building. Jonas in 2011 explained clearly the methods and various technology-based techniques in specifying the position of the telephone in action of use.

As shown in the literature on information technology and applications to criminal investigation, the researchers of this study would like to propose a guideline to the data search process in criminal cases. It was expected that the proposed prototyped could be beneficial to investigative officers and personnel involved in the investigation to understand and use the proposed process in operation as well as suggested investigating methods to locate offenders in criminal cases.

2. Background of the Study

2.1 Concept on Crime Analysis

Baltaci (2010) gave the meaning on crime analysis that it was well-known amongst law enforcement people. Each unit in each time would give different meanings so there was standard meaning for each. A crime analysis is to support decision-making by law enforcement officers. Its process is to find a pattern of related data in specifying the target in the operation of officials. There are five orders of patterns in a circle. Each circle can go back to perform in the previous step, depending on the things that happen to the end user. The data are received with new requirements in five stages: (1) Collection, (2) Collation, (3) Analysis, (4) Dissemination, and (5) Feedback and Evaluation.

2.2 Method and Investigation Technique

Generally, there is no assurance on specific investigation methods being successful for complication of criminal cases. Some successful techniques having been tried and reported require intensive experience and personal abilities of investigators. However, there is a pattern of stages of investigation to be observed as follows:

Establishing the Elements of Crime: In case it cannot be specified regarding the story or related people from evidence gathered in the crime context, irrelevant evidence is cut off to narrow down the investigation.

Under Cover: it is concealment and disguise of investigators in search of the truth and further evidence.

Interviewing & Interrogation: the basic techniques in questioning and interview are required. Investigating officials are to interview witnesses and volunteers to gather data on people, circumstances and offenses in the place and time of the case. This is to find details from the testimony even though the testimony provider might be unwilling to reveal the truth.

Exploiting Available Sources of Information: Various data from the government units, state enterprises and private businesses can be useful to the investigation, such as data from the Royal Thai Police, Administrative Division, Department of Land Transport, Department of Corrections, Revenue Department, Department of Commercial Registration, Immigration Office, Social Security Office, Post Office, Telephone Service Provider, Internet Service Provider, Insurance Company, Bank and public information. Included are data from search engines, web boards, market- or e-commerce platforms, social networks, social messengers and email accounts.

Crime Mapping: it focuses on important data on that crime. The crime mapping can be modified to show the place of the suspect, the place of people or the place that deserves special attention. This enabled policeman to travel to investigate the news or follow up suspects at the place, as informed without delay.

Fixed-surveillance & Intelligence: the investigation will be narrowed down for the suspect to be pinned down for arrest.

The Site Survey: Fixed-surveillance & Intelligence cannot be openly performed but there is a need to know the details of the place and its environment correctly so that safety of the operation can be ensured to a possible maximum.

2.3 Using of Information Technology and Communication

Information technology and communication involve the following considerations:

A logical forensic examination of a mobile phone: Nowadays criminal cases involve important evidence from telephone with connections. Many police units copy data and verify the data from mobile telephones.

Electronic Spreadsheet: Aaron Edens (2012) wrote a book on Police Technicality in using MS Excel by using Pivot Table to analyze Call Detail Records (CDR) and make a profile as a copy file without using the original file received from the service provider via the program IBM i2 Analyst’s Notebook

Visual Analysis Tool: The program is to analyze the news data such as IBM i2 Analyst’s Notebook or i2 which is very popular among law enforcement officers for more than 2,000 places. The program has been around for 20 years. The program can process complicated data and present them in pictures. The visual analysis can help analysts to integrate specifications, speculations on the network of the culprit, intelligence, crime, terrorists and various corruption activities. The program has important variables to search relationships, incidents, behaviors and clues that might be overlooked by investigators.

Mobile Network Monitor Application: It is called Netmonitor (Andriod), which can be used to monitor GSM/CDMA/LTE network in order to obtain current and neighboring cell information and its signal strength.

Web Mapping: it is a technique of using maps, particularly Google map, which shows spatial and geographical data and provides detailed information about geographical regions and sites.

Web Proxy: it acts as an intermediary between an endpoint device, such as a computer, and another server where a user or client is communicating, such as https://hide.me/en/proxy

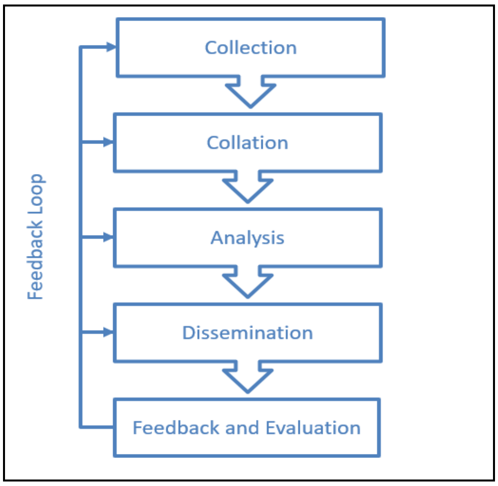
Website Copier: it enables to download a World Wide Web site from the Internet to a local directory such as HTTrack.

Domain Tools: It is a web domain tool used to find information from networks, including domains and IPs, and connects them with nearly every active domain on the Internet, such as https://www.whois.net/. It is useful for security professionals against profile attackers; it provides guidance to online fraud investigations, and map cyber activity against infrastructure attackers.

3. Research Methodology

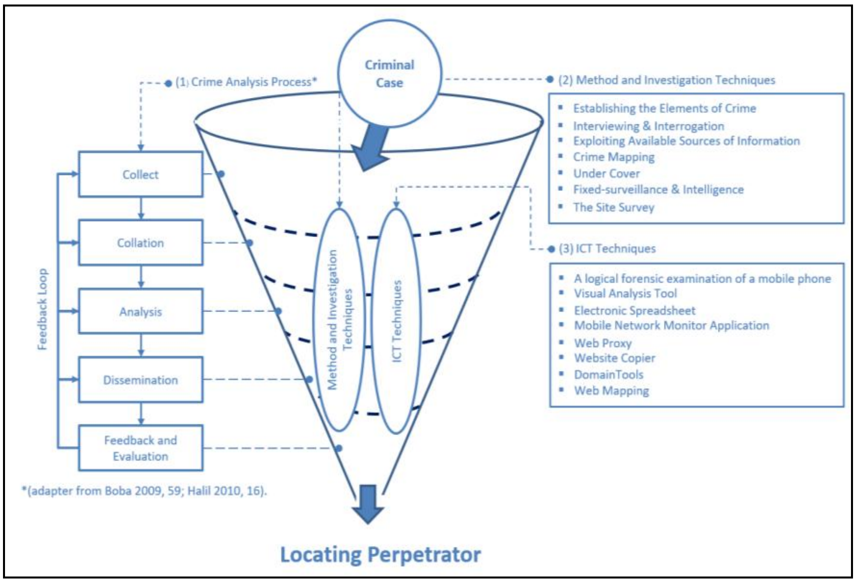
From the crime analysis process adapted from Boba (2009: 58) as shown in Figure 1, the researchers investigated the actual computer-related crime cases by using IT techniques and applied the crime analysis process to the crime cases under study. This leads to *a novel conceptual framework* in locating cybercriminals, known as *Locating Perpetrator using Information and Communication Technology* techniques based on the crime analysis process (LPICT).

Figure 1: Crime Analysis Process (Halil 2010)



The proposed *framework* consists of three domains: (1) the crime analysis process, (2) a concept of traditionally tactical police investigation, and (3) the ICT techniques as shown in Figure 2.

Figure 2: The conceptual framework LPICT in three domains


Criminal Case
(1) Crime Analysis Process*
(2) Method and Investigation Techniques
Establishing the Elements of Crime
Interviewing & Interrogation
Exploiting Available Sources of Information
Crime Mapping
Under Cover
Fixed-surveillance & Intelligence
The Site Survey
(3) ICT Techniques
A logical forensic examination of a mobile phone
Visual Analysis Tool
Electronic Spreadsheet
Mobile Network Monitor Application
Web Proxy
Website Copier
DomainTools
Web Mapping
Collect
Collation
Analysis
Dissemination
Feedback and Evaluation
Feedback Loop
Method and Investigation Techniques
ICT Techniques
*(adapter from Boba 2009, 59; Halil 2010, 16).
Locating Perpetrator

Actual case studies of LPICT are displayed in Figure 3 and Figure 4. In Figure 3, it is a drug case in which the ICT technique for mobile phone was applied. In Figure 4, it is a computer-related crime case in which the ICT technique for computer was implemented. Firstly, the case studies were classified for use with a mobile phone or a computer. After that, the three-domain-concept as mentioned in Figure 2 was applied. Finally, the best practice for each case was identified.

Figure 3: Drug case with the ICT technique for mobile phone in application

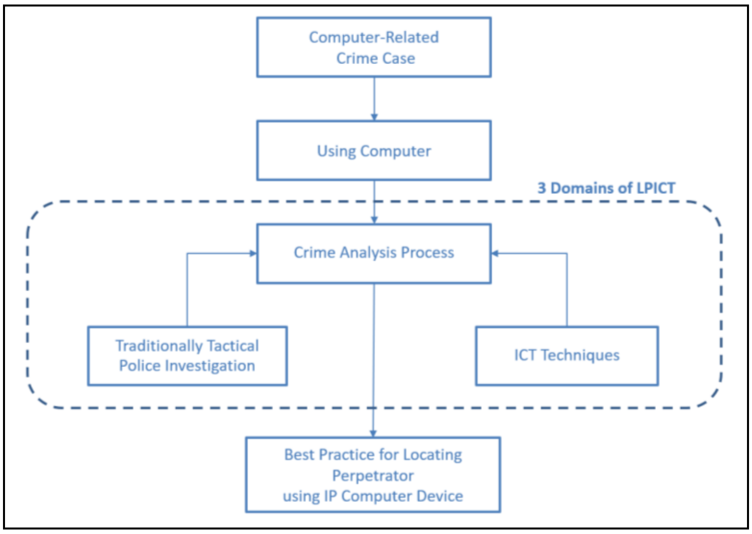
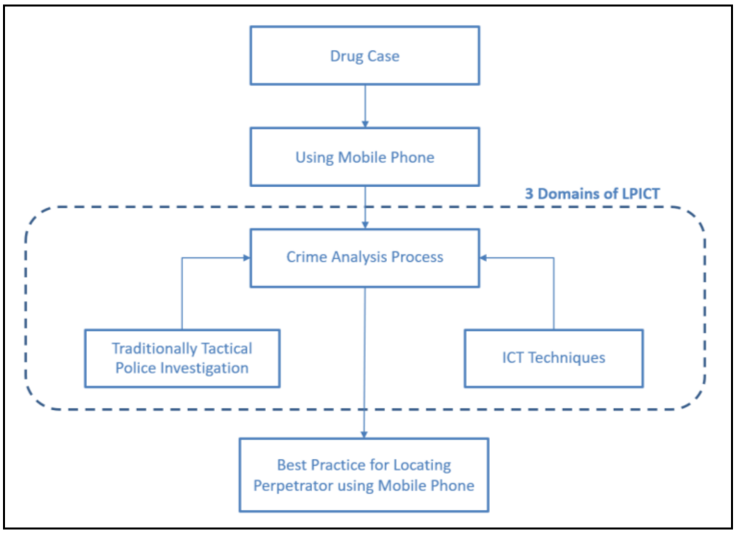

Computer-Related Crime Case
Using Computer
3 Domains of LPICT
Crime Analysis Process
Traditionally Tactical Police Investigation
ICT Techniques
Best Practice for Locating Perpetrator using IP Computer Device

Figure 4: Actual case studies of LPICT


Drug Case
Using Mobile Phone
3 Domains of LPICT
Crime Analysis Process
Traditionally Tactical Police Investigation
ICT Techniques
Best Practice for Locating Perpetrator using Mobile Phone

4. Experiment Results

4.1 Finding a location of OFFENDER from mobile phone usage *Scenario 1*

Before arresting, the policemen contacted to buy methamphetamine from Mr. Sree. In tracing Mr. Sree around 17.20 hours, there was an incident that Mr. Arkhom was transporting the drug in 200,000 pills to Mr. Sree at the parking of one department store. The officials went to search, arrest and confiscate methamphetamine. In the arresting procedure, two suspects confessed their guilt.

Mr. Arkhom, (the first suspect) testified that he was hired by the drug dealer at the border named Komaw to transport the drug to owt customers. Before the trip, Miss Pookie (Komaw ‘s sister) contacted about the delivery. On the drug delivery date when the trip was close to Bangkok, Komaw ordered Arkhom to put 400, 000 pills into a blue Izuzu car owned by Mr. Bandit who was the first customer. Mr Bandit was driving along the road in front of the gas station before reaching the department store where Mr Arkom was arrested. Mr Arkom was also instructed to deliver another 200, 000 pills to Mr Sree (the second suspect) at the parking of the department store, who was arrested the next day.

Mr. Sree (the second suspect) testified that he contacted Komaw to buy methamphatemine at an agreed price. Mr Sree was to pay to Miss Pookie. He learned later on that Komaw asked Mr. Arkhom to deliver the drug to him on the date and time as appointed. Mr. Sree did not know about Mr. Bandit coming to pick up the drug from Mr. Arkhom .

After the incident, the policemen who arrested both suspects and investigative officers gathered related evidence and requested the arrest warrant of Mr. Komaw, Miss Pookie and Mr. Bandit. Later, Komaw and Miss Pookie escaped and hid in the area of neighboring countries. The officias announced the arrest and coordinated with related border police units. Mr. Bandit was in hiding and then arrested at the parking of one apartment.

Figure 5: LPICT locating perpetrator in a drug case using ICT techniques based on the Crime Analysis Process

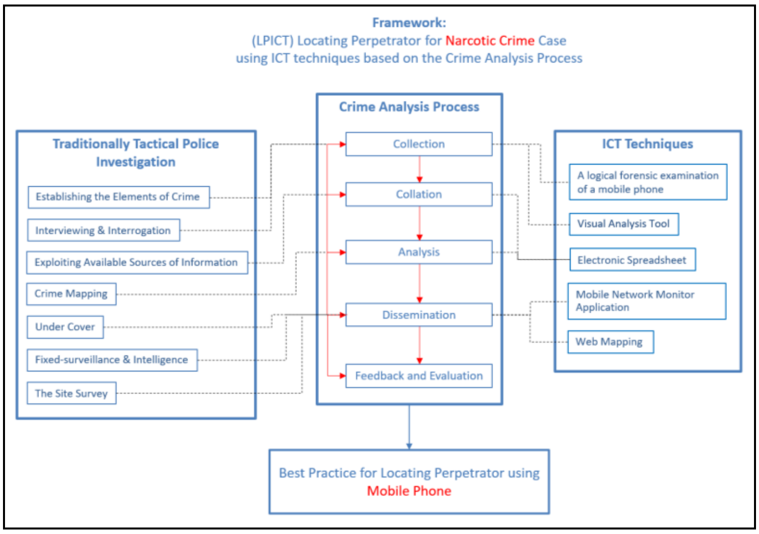

Framework:
(LPICT) Locating Perpetrator for Narcotic Crime Case
using ICT techniques based on the Crime Analysis Process
Crime Analysis Process
Traditionally Tactical Police Investigation
Establishing the Elements of Crime
Interviewing & Interrogation
Exploiting Available Sources of Information
Crime Mapping
Under Cover
Fixed-surveillance & Intelligence
The Site Survey
Collection
Collation
Analysis
Dissemination
Feedback and Evaluation
ICT Techniques
A logical forensic examination of a mobile phone
Visual Analysis Tool
Electronic Spreadsheet
Mobile Network Monitor Application
Web Mapping
Best Practice for Locating Perpetrator using Mobile Phone

Figure 3 shows the case of the mobile phone usage. The three domains are working together. The crime analysis process as the main concept is shown in Figure 5. Firstly, the *collection* process uses the traditionally tactical police investigation on the left hand side, which is "establishing Elements of Crime" and "interviewing & interrogation." It also uses the ICT technique on the right hand, which are "A logical forensic examination of a mobile phone" and "visual analysis tool." Secondly, the *collation* process uses "Exploiting available source of information" on the left hand side. It also uses "electronic Spreadsheet." Each process takes both left and right hand side until *the best practice* is obtained.

Collection

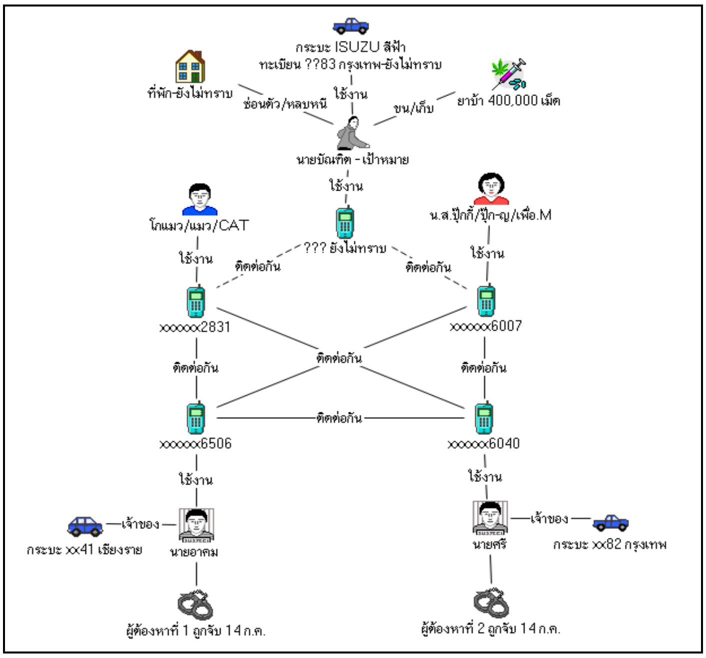
Collection contains:

- Establishing the elements of crime by setting up the investigating point to the target (who escaped) if there was any contact and communication with the suspect or related people in the case.
- Gathering the data from telephone by using mobile phone forensic tool, telephone decrypted, and considering important data in log files and contacts.
- Gathering the data from the testimony of the suspect by questioning interviewing techniques.
- Arranging and comparing for consistency the data received from using mobile phone extraction and the data received from questioning and interviewing.
- Using the program i2 Analyst's Notebook Process to check incidents and create the communication overview between the culprit and other people.

These components are to project the relationships in the communication pattern between *the target* and related people via specific telephone numbers used by *the target*.

To secure information from telephones used by Mr. Arkhom and Mr. Sree, (suspects 1 and 2) in contact with Mr. Komaw and Miss Pookie, the investigators used the telephone numbers of Komaw and Miss Pookie to request the Call Detail Record (CDR) of both persons for the data on telephone numbers belonging to *the target*. This was for the investigators to find *the position* displayed in Figure 6.

Figure 6: Locating position of *the target*



Collation

Inspecting Call Detail Record (CDR) data on the suspect and the people in the case from the telephone service provider, the investigators cleaned the data and arranged the format of CDR; they used the gathered data to create the picture of telephone contacts in the communication among people in the case. Along with the analysis of CDR, the telephone number was specified for the culprit as a target point in the investigation. Then the target telephone number was used to inspect the CDR to clean the data and arrange the CDR format. This was to gather information from the inspection of CDR in order to acquire the name list of the suspects, inspect the civil registration, people in the house, and vehicle registration; these obtained data were then put into MS-Excel.

Analysis

The investigators analyzed CDR concerning target telephone numbers, arranged Cell-ID order from using telephone numbers in question, and considered the frequency, time period, time span of the Cell-ID by using Pivot Table, followed by having concluded data in MS-Excel.

Dissemination

Surveying and collecting telephone signal poles were known as Base Transceiver Station (BTS) which uses data to create a map on gathering and analyzing data. There are eight steps involved:

(1) Disguising of investigators to go into the area along with the technique of place survey by using Netmonitor (Android) to access and collect the information of BTS in the survey. Collecting the data from BTS from the target place and adjacent area in the 3-km radius.

(2) Specifying a clear topographical coordinate for the location of the target place.

(3) Specifying the Cell-ID found at the location of the target place.

(4) Reaching the target place with Cell-ID consistent with the Cell-ID showing in the program Netmonitor of the investigating officer.

(5) Listing places in the area with CID and specifying the topographical coordinate onto the list.

(6) Collecting the data of signal poles near the 3-km radius.

(7) Gathering and improving the data according to Table 1 and Table 2 as in Picture 5 and Picture 6 to complete the specified coordinate and CID.

(8) Making the operating map by using Google Map to create two maps on the data from Net Monitor as the basic Layer.

Feedback and Evaluation

The investigators reviewed the operation concluded from going into the area and traced back to related steps by fixing with the data CDR of *the target* at that time.

Figure 7: Overlapped Area

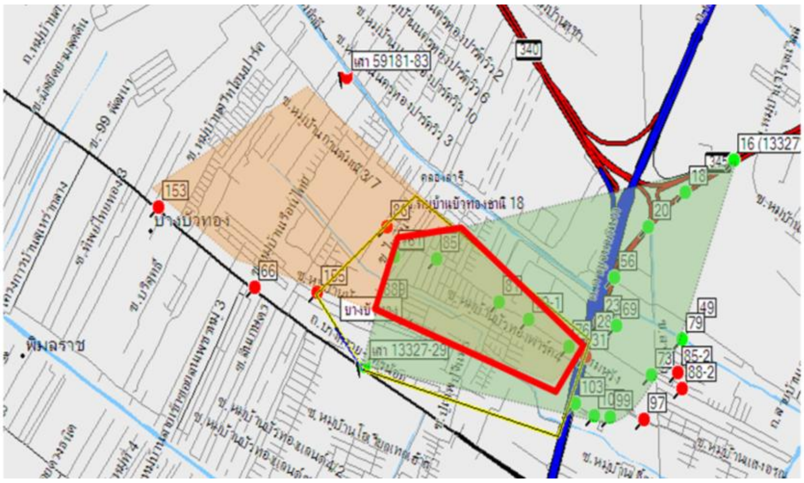
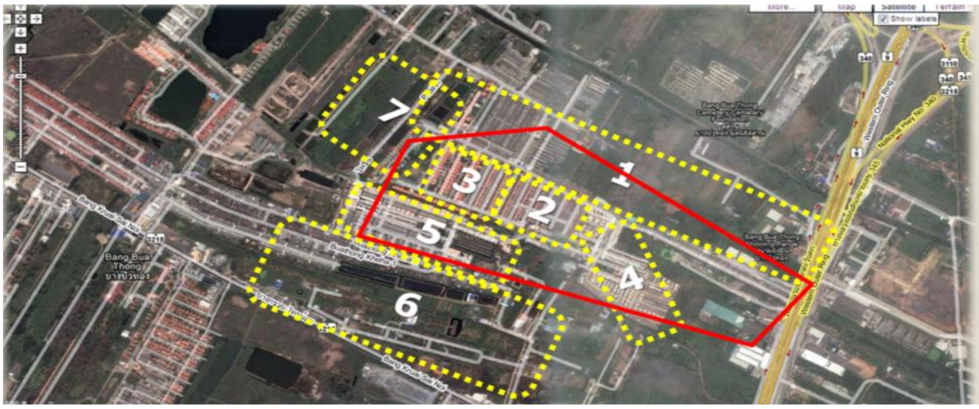


Figure 7 shows overlapped area between the red and the green color zones. Both zones are the areas where *the perpetrator* traveled. After that, investigators separated the overlapped area into several zones identified as *interesting areas* as shown in Figure 8.

Figure 8: Interesting Area



4.2 Finding a location of OFFENDER from computer accessed the Internet

Scenario 2

The policemen was notified from a samaritan on the web board selling guns and illegal war weapons. In order to probe into the notification, the investigating officer disguised as an agent interested in buying guns from the culprit. Later, the culprit was found and his place was searched with the court's approval. In the house search, the police found illegal guns and confiscated other illegal objects like M-16 guns and many pistols. In the questioning procedure, the suspect confessed that he had been selling war weapons for many months by using a web board to contact customers. The culprit made sure that the sale be made only to old customers or recommended customers. After the deal, each customer was to transfer money into the bank account of a third party, and the suspect was to send the gun by post as a safe method to avoid attention of the police.

Figure 9: LPICT is used to locate perpetrator in Computer-Related Crime case using ICT techniques based on the Crime Analysis Process

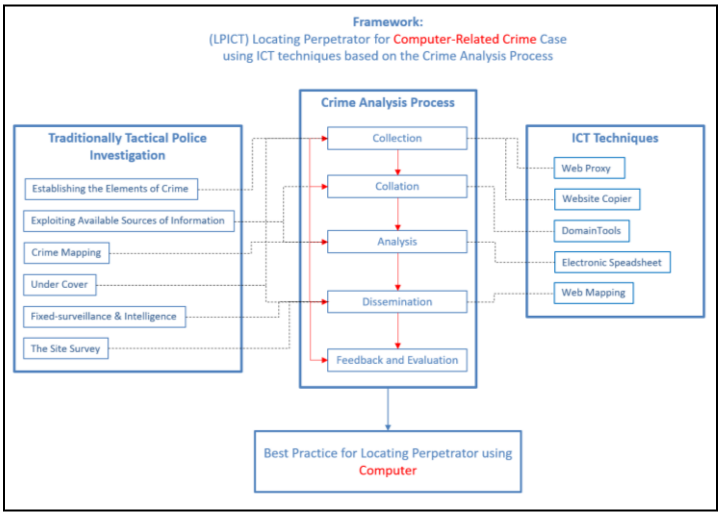

Framework:
(LPICT) Locating Perpetrator for Computer-Related Crime Case
using ICT techniques based on the Crime Analysis Process
Traditionally Tactical Police Investigation
Establishing the Elements of Crime
Exploiting Available Sources of Information
Crime Mapping
Under Cover
Fixed-surveillance & Intelligence
The Site Survey
Crime Analysis Process
Collection
Collation
Analysis
Dissemination
Feedback and Evaluation
ICT Techniques
Web Proxy
Website Copier
DomainTools
Electronic Speadsheet
Web Mapping
Best Practice for Locating Perpetrator using Computer

Figure 9 shows Computer-Related Crime case with the crime analysis process as the main concept. Firstly, the collection process uses the traditionally tactical police investigation on the left hand side, which is "establishing Elements of Crime" and "exploiting available sources of information". It also uses the ICT techniques on the right hand, which are "web proxy" and "website copier." Secondly, the collation process uses "Domain tool" on the right hand side. Each process takes both left and right hand sides until the best practice is obtained.

Collection

Collection deals with gathering contents on the web board and specifying *the target* to know the position of the culprit. The following steps were used by the investigator:

(1) Searched data on interested people using the web board about an average of 100 posts/day. Many posts showed a fraud of selling guns.

(2) Specified *the investigative target* and chose the seller trusted by the web board users. The trusted seller was a member coded as "xxx 01" selling many kinds of guns via EMS.

(3) Met with one web board user who posted back when receiving the goods.
The seller used a cover name or a coded number.

(4) Found one web board user posting the url and there was a picture of a male teenager with a round face, aged about 20, reddish dark skin, wearing a short white shirt with soldier-type pants, posing with M-16 gun on the bed. The environment might be a bedroom in a residence. It was possible that the person in the picture could be the member coded "xxx 01."

Collation

Details on the domain and the location of the network were:

(1) Inspecting the details on the domain name of the targeted website.

(2) Inspecting the registered persons on the target website.

(3) Inspecting the service provider for the location of the hub and the website in operation.

(4) Inspecting the service provider who provides the Internet service via ip address.

Analysis

Data in the basic stage of investigation were analyzed as follows:

(1) Inspecting the names and the places of people according to the ip address but without evident relation to previously gathered information.

(2) Considering the target people on the Internet from the same source, who might be people in the family related to the wrongdoer or other people who can reach the Internet by any methods from the Router at the same house/ place of contact on specific dates and time.

(3) Inspecting and analyzing people in the target house from civil registration.

(4) Inspecting people in the target house, who showed connection with the previously obtained data.

(5) Inspecting people in the family living at the place with the target ip address with the real name “Rxxxxx” which had some part of the name consistent with the previously obtained data.

(6) Tracing and proving the movement of Mr.Rxxxxx according to the address given on the Internet

Dissemination

Surveying the area includes the following:

(1) Arranging the survey force for the target address and observing the movement and the number of people living in the house.

(2) Assigning officials to follow up the movement of the culprit on the web board to check consistency of contacts/ communication made by *the target*.

(3) Considering the results and the evaluation from the previous data and those for operation planning.

(4) Observing the behaviors of residents in the target house, particularly on entering or leaving the house as well as transportation used. Date and time were checked in detail.

(5) Checking the movement in the web board on *the target user* posting at night until the time that *the target group* returned home.

(6) Gathering the data and requesting the court’s approval for the search warrant.

(7) Gathering the investigated data and related evidence, and requesting the court's approval for search warrant of the suspect and the target house.

(8) Inspecting, arresting and confiscating the evidence.

(9) Searching the suspect in possession of war weapons and many pistols.

(10) Questioning the suspect to confession of the coded name used as xxx 01 selling many illegal guns.

Feedback and Evaluation

The investigator reviewed the overall operation from going into the area and tracing back to the related steps in connection with the CDR data of *the target* in specific time data.

5. Conclusion

This paper presents the LPICT framework consisting of three domains: (1) the crime analysis process, (2) Traditionally Tactical Police Investigation, and (3) ICT techniques. This framework was applied to two actual cases: (1) Finding a location of *the offender* from mobile phone usage, and (2) Finding a location of *the offender* from computer access to the Internet. It was found that the LPICT framework enabled the investigative officers to obtain the best practice in *Utilizing of Information and Communication Technology* in order to locate *Criminal Offenders in Criminal Cases.* It should be noted that finding a location of *the offender* from mobile phone usage still appeared rather limited due to technicalities of both sim cards and mobile phones being changed in the process of use. This type of technical limitations should deserve further research. Besides, finding a location of *the offender* from computer access to the Internet was obviously limited when the location of the web hosting server for social media used by *the offender* was outside of Thailand. As for the ICT techniques, phishing in particular, was effective in obtaining IP address of *the offender* while staying in Thailand. This enabled the investigative officers to find the offender's location of the place accessing the Internet. The researchers of this study hope that the LPICT prototype as reported in the paper would be beneficial to investigative officers and other parties concern to perform their tasks effectively.

6. The Authors

Naughtakid Phromchan is a doctoral graduate in College of Information Communication Technology, Rangsit University, Phatum Thani, Thailand. His research interest is in the area of applications of Information and Communication Technology to criminology.

Sanon Chimmanee is an associate professor of Information Technology at the College of Information Communication Technology, Rangsit University, Phatum Thani, Thailand. His research work involves telecommunication science and computer networks engineering, and ICT applications.

7. References

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

Baltaci, H. (2010). *Crime Analysis: An Empirical Analysis of its Effectiveness as a Crime Fighting Tool.* A Ph.D. dissertation, Public Affairs, the University of Texas at Dallas.

Buadistdecha, C. (2008). *Criminal Liability for Cyberstalker.*A Master thesis of Laws Program, Faculty of Law. Chulalongkorn University.

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

Cybercrime Another Medal in the Digital Age. (2017). Accessed July 15, 2017. Available: http://www.thansettakij.com/content/136878

Jonas, W. (2011). WiFi and Cell-ID based positioning. Protocols, Standards and Solutions , Jan.

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

Kumar, M., Hanumanthappa, M. & Kumar T. V. S. (2017). Crime investigation and criminal network analysis using archive call detail records. *The Proceedings of the 8th International Conference on Advanced Computing (ICoAC) 2016*, Chennai, (2017), 46-50.

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

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

Romsaiyud, W. & Premchaisawasdi, W. (2009). Intelligent switching method using Cell-ID/GPS positioning on mobile application. *The Proceedings of the 7th International Conference on ICT and Knowledge Engineering 2009*, Bangkok, (2009),83-88.

Vimollohakarn, M. (2010). *Seeking evidences in drugs cases by using special investigation. Master of Laws, Criminal law, Faculty of Law.* Bangkok: Thammasat University.

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