Contents List available at RAZI Publishing
Acta Electronica Malaysia (AEM)
Journal Homepage: http://www.actaelectronicamalaysia.com

ISSN: XXXX (Print)
ISSN: 2590-4043 (online)

ACQUIRING CYBERCRIME EVIDENCE ON MOBILE GLOBAL POSITIONING SYSTEM (GPS): REVIEW

Nurul Azma Abdullah, Nurazidah Mohd Rashid

Faculty of Computer Science and Information Technology Universiti Tun Hussein Onn Batu Pahat, Johor, Malaysia
Corresponding author email: azma@uthm.edu.my, nurazidahrashid@gmail.com

ARTICLE DETAILS

Article History:

Received 3 July 2017
Accepted 3 October 2017
Available online 8 November 2017

Keywords:

Cybercrimes, Forensic Investigation, Global Positioning System, GPS.

ABSTRACT

The use of Global Positioning System (GPS) as a device for finding directions is increasing from time to time. Within this growth, developers have taken a new inventiveness to apply this GPS system in a new environment. This new environment is called Internet of Thing (IoT) environment. This environment involves the device that connect to the internet such as smartphones and tablets. With this successful application, the mobile GPS has opened up a new space for forensic experts to get useful evidence in criminal cases. The connection between smartphone and GPS has raised the demand to examine the stored content of the devices. The stored content might include certain information such as home location, entered address or location, journey starts, ends and last GPS, call records and SMS. This critical data can be used in whole range of crime cases especially triage cases, for example, kidnapping cases, hit and run cases and many others.

1. INTRODUCTION

Technology has significantly altered the way villains and investigators dealing over the times. The villains will find a way to stay one step ahead of the law by using a technology. Because of that, the investigators are pushed to compete with the villains to stop their crime activities. This constantly race has persuasive both side trying to learn the new technology to make sure it works in their favour.

Table 1: Mobile Navigation Application Features

Application	Navigation	Directions	Chatting	ETA	Home/ Work Address	Favourite	Location Sharing
Google Maps	X	X	-	-	X	X	-
Apple Maps	X	X	-	-	-	X	-
Waze	X	X	X	X	X	-	X
MapQuest	X	X	-	-	X	-	-
Bing Maps	-	X	-	-	-	-	-
Scout GPS	X	X	X	X	X	X	-

With the both side are competing, there comes a new rising area of Internet of thing (IoT). The IoT is the interconnection of device that allows the process of sending and receiving the data via the Internet [1]. The word 'internet' itself represents the involvement of the internet usage in transferring the data. While the word 'thing' represent the device that has a capability to recognized and integrated into communication networks. The IoT technologies has raise a new issue in digital forensic world. Most of the IoT devices are open to forensic investigation to be done to help in getting an evidence. One of the IoT devices is smartphone.

The use of smartphones has been increasing year by year. In 2015, the worldwide usage of smartphone reached at 1.86 billion users. The increase occurred and by the end of 2017, it is expected that phone usage will increase until 2.32 billion users [2]. With this increasing usage of smartphone, the probability for smartphones to be the main element of investigation in a criminal case is higher [3].

In line with the increased use of smartphones, the navigation application system has been integrated into the smartphone itself. So, the users do not need to use separate GPS applications for the purpose of finding locations in one place. As an impact, the use of handheld GPS devices has decreased [4].

By the year 2009, the distribution of Garmin's revenue in automotive/mobile is around 70%. By the year 2013, the percentage has decreased to 49%. For the year 2016, it has become only 29% [5]. The decreased revenue of Garmin shows that people tend to rely on mobile GPS application now. Besides, based on research on United State, December 2016, Google Maps has become one of the fifth most popular mobile application used by total visitor is 101.95 million [6].

This is a solid prove that people now a day has turned to mobile GPS application technology. Plus, this mobile GPS application provide more reliable information to the user. Table 1 show the summary of application features of chosen mobile GPS application providers [7].

With this rapid growth of mobile GPS application technology, it is worth considering the possible forensic analysis on this device. The application itself have an information of specific place as well as other crucial data that might be help during forensic investigation.

2. RELATED WORK

This section discusses articles related to research that will be carried out later. In this section, the methodology, results, discussions and conclusions of each article are discussed. Start with article related to evidential recovery of GPS devices [8]. In this research, the researcher was discussing the technical details of recovering the crucial data from the four GPS that currently available in New Zealand market. Their main focus was on Navman GPS devices which are from the model MY-50, S-90i, c40 and f20 models. Each models of GPS devices were forensically imaged using FTK Imager. This process used to make sure that the mining and investigation

methodology can be easily displayed. At the same time, imaging the data will also remain the integrity of the data.

The phase start with forensic imaging process. Each of the GPS devices were undergoes the forensic imaging where images of the evidence were attained by carrying out a pre-set process and applying technically secure procedure that maintain the integrity of the evidence. The devices being extract by performing a bit-for-bit forensic image copy process. The devices were connected to the computer by using a USB mass storage mode with software write-blocker enabled. The FTK Imager; standard industry forensic software was used for completing the imaging process [9].

After the imaging process was completed, the next step was extraction and data analysis. The log files and system were analyzed by using the EnCase Forensic software. After the analyzation process were done, the result was being review and discussed in reporting format. All the devices were carried out by the same process and the result being compared at the end of the process. The contribution and limitation of the research are shows in Table 2 below.

Table 2: Contribution and Limitation of Cusack And Simms Research

Contribution of the research	Limitation of the research
To investigate regarding of method developed involving the Navman Devices	The three out of four devices are having difficulty to connect with software write-blocked Windows operating system. It resulted accidentally change in a number of system and log file timestamps
To introduce the possible utilization of registered applications	

Continue with article of Forensic Analysis of TomTom Navigation Application [10]. The research study in this article state that they were performing the forensic acquirement and analysis of TomTom android application. At the same time, they also do a test to compare the difference between the handheld TomTom device and the TomTom android application.

The technique that they used was the acquisition technique. The acquisition technique builds up from three different phases. Start with the physical image extraction. The non-volatile memory of Android mobile device was undergoing a physically image process. By performing the physical image, the research will get all the storage of the devices [11]. Next step was searched for the important files. The file that found in android storage were not fully useful. So, this is why the researcher were gaining the root access to identify the crucial data that might be help in forensic analysis. They also make a physical copy of the whole device. So that, when the actual devices undergo analysis process, they still can make a comparison between the original and the altered one. By performing the comparison, the remarkable data can be identified and mined. When the remarked data is found, the data was undergoing the decoded process. Then, the data was analysed at the end of process.

The comparison process also conducted between the handheld TomTom device and the TomTom android application. Both were giving the same data information except Triplogs. The Tripslogs only can be found on the handheld TomTom device but not in the TomTom android application. The contribution and limitation of the research are shows in Table 3 below.

Table 3: Contribution and Limitation of Nhien-An Le-Khac, Mark Roeloffs And M-Tahar Kechadi Research

Contribution of the research	Limitation of the research
To determine how to acquire data from the TomTom android application	Only used TomTom android application as case study. Thus, the result of the finding cannot completely have proven if using the different navigation application
To discover the difference method of storing data in handheld TomTom devices and TomTom android application	

The smartphone ability to provide information to the user of android application has become huge from year to year. This has led to perform a forensic analysis of the smartphone devices.

Find Me If You Can: Mobile GPS Mapping Applications Forensic Analysis & SNAVP the Open Source, Modular, Extensible Parser article experimental on finding the detailed and crucial data on six most popular smartphone mapping application; Google Maps, Apple Maps, Waze, MapQuest, Bing, and Scout [12].

The methodology that the researcher used were following the guideline of forensically examining artifacts by the NIST [13]. The methodology was divided into three processes. First was data creation and acquisition. Each action that take place on the mobile device was being recorded. Then the device was forensically examining by using XRY software. Then the data was being extracting to perform the second process which was data analysis. This process was done by using a variety of tools.

Table 5: Comparative Study of Android Forensic Tools [14]

Tools	Cost	Operating System	Function
Volatility	Free	Windows/Linux/Mac/ Android	The software can run a mining technique for mobile and has an ability to examine several types of memory dumps [15]
DroidSpotter	Free	Windows/Linux	Useful in finding the possible location from raw location data of android application [16]
Andriller	Paid	Windows XP/Vista/7/8	Software utility; can crack lock screen, decode communication, files and database of devices [17]
XRY	Paid	Windows	Able to perform secure forensic extraction on many type of mobile devices [18]
UFED Touch	Paid	Windows 8	Able to perform physical extraction, decode file system and other data [19]

The XRY and Cellebrite were used to encase and investigate the acquired data. When the data were identified, the researcher used a several inspection tools to perform the inspection of data content. Last process was using Smart Navigation Parser (SNAVP) as a tool to complete the whole extracting and analysing process. The contribution and limitation of the research are shows in Table 4 below.

Table 4: Contribution and Limitation of Moore, Baggili And Breitinger Research

Contribution of the research	Limitation of the research
To provides a complete analysis of the most popular smartphone mapping applications; Google Maps, Apple Maps, Waze, MapQuest, Bing, and Scout, on both Android and iOS.	All the research is applied only for a small scale of data set.
	The SNAVP tools only can detect the location that were in United State.

Nihar Ranjan Roy, Anshul Kanchan Khanna and Leesha Aneja conducted a research that mainly focused on Android Phone Forensic: Tools and Techniques [14].

The android forensic is a method to extract the data from the android based devices. The method consists of three different technique which are:

a. Manual acquisition – in this technique, the forensic analyst will manually take a screenshot of each device screen that contains any data. This technique does not require any tools to gain any required data. But in the term of time consuming, it required a lot of time.

b. Physical acquisition – in this technique, the required data will be duplicate. The duplicate data will undergo analysation process. At the end, the modified data will be compared with the original data to obtain any crucial information.

c. Logical acquisition – in this technique, the information from the smartphone is gaining using tools.

As for the logical acquisition, the researchers have stated a few tools that can help in performing the android forensic process. The tools are stated in Table 5 below.

3. CONCLUSION AND FUTURE WORK

The integration of Global Positioning Systems (GPS) and Smartphones and their integration has transformed the importance of navigation system. With this system, it can help users get the information and location they need. In line with the development of this service, the issue of security of information is equally resurrected. Therefore, it is very necessary for a forensic investigation into this field.

The future study of this research will focus on approach to increase the performance of finding and collecting cybercriminal evidence of mobile GPS. The comparing new approach in finding the criminal evidence of

mobile GPS with the existing methodology will also be discussed in future studies.

REFERENCES

[1] Wikipedia. 2017. Internet of Things. Retrieved on 17.10.2107 from https://en.wikipedia.org/wiki/Internet_of_things

[2] Statista. 2017. Number of smartphone users* worldwide from 2014 to 2019 (in millions). Retrieved 20.1.2016, from http://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

[3] Umale, M.M.N., Deshmukh, A., Tambhakhe, M. 2014. Mobile phone forensics challenges and tools classification: A review. International Journal on Recent and Innovation Trends in Computing and Communication, 2 (3), 622–626.

[4] Statista. 2017. Navigation Devices and Usage – Statistics and Facts. Retrieved on 19.10.2017 from https://www.statista.com/topics/2221/navigation-devices-and-usage/

[5] Statista. 2017. Distribution of Garmin's Revenue from 2009 to 2016, by Segment. Retrieved on 19.10.2017 from https://www.statista.com/statistics/217905/revenue-distribution-of-garmin-by-segment/

[6] Statista. 2017. Most Popular Mobile Apps in the United States as of December 2016, ranked by Average Unique Monthly Visitors (in Millions). Retrieved on 19.10.2017 from https://www.statista.com/statistics/250862/unique-visitors-to-the-most-popular-mobile-apps-in-the-us/

[7] Moore, J., Baggili, I., Breitinger, F. 2017. Find Me If You Can: Mobile GPS Mapping Applications Forensic Analysis and SWAVP the Open Source, Modular, Extensible Parser

[8] Cusack, B., Simms, M. 2011. Evidential recovery from GPS devices. Journal of Applied Computing and Information Technology, 15 (1).

[9] Guidance Software. 2010. Encase forensic,

[10] Khac, N.A.L., Roeloffs, M., Kechadi, M.T. 2017. Forensic Analysis of TomTom Navigation Application. University College Dublin, Ireland.

[11] Free Android Forensics. 2014. The Different between Physical Image and a Logical Extraction. Retrieved on 22.10.2017 from http://freeandroidforensics.blogspot.my/2014/09/the-differences-between-physical-image.html

[12] Moore, J., Baggili, I., Breitinger, F. 2017. Find Me If You Can: Mobile GPS Mapping Applications Forensic Analysis and SWAVP the OpenSource, Modular, Extensible Parser.

[13] Kent, K., Chevalier, S., Grance, T., Dang, H. 2006. Guide to integrating forensic tech- niques into incident response. NIST Special Publication, 800–86.

[14] Roy, N.R., Khanna, A.K., Aneja, L. 2016. Android Phone Forensic: Tools and Techniques. Computing, Communication and Automation (ICCCA), 2016 International Conference on. DOI: 10.1109/CCAA.2016.7813792

[15] Volatility Foundation. 2017. Volatility Foundation. Retrieved on 23.10.2017 from http://www.volatilityfoundation.org/

[16] Kramer, J. A. 2013. DroidSpotter: A Forensic Tool for Android Location Data Collection and Analysis. Digital Repository. Iowa State University.

[17] Andriller. 2017. Andriller – Android Forensic Tools. Retrieved on 23.10.2107 from https://www.andriller.com/

[18] MSAB. 2017. The Ecosystem of Mobile Forensics. Retrieved on 23.10.2017 from ttps://www.msab.com/products/

[19] TEELtechnologies. 2017. UFED Touch Ultimate. Retrieved on 23.10.2017 from http://www.teeltech.com/mobile-device-forensic-tools/cellebrite/ufed-touch-ultimate/