EMB00006f50405b

연구논문/작품 최종보고서

2019학년도 제2학기

제목: Application of Digital Forensics Methodologies in Epidemiological Contact Tracing

윤인하 (2013311425)

2019년 10월 28일

지도교수: 등 국 홍

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Plan (10) | Topic (20) | Concept (20) | Details (30) | Report (20) | Total (100) |
|  |  |  |  |  |  |

\* 지도교수가 평가결과 기재

Abstract

In epidemiological situation, finding out epicenter and preventing diseases from spreading out is important. That is, contact tracing of infected people is necessary to search their whereabouts and contact. In crime scene, digital forensics is widely used to chase the suspect. Likewise, we can apply digital forensics in epidemiological contact tracing. In this paper, I’ll focus on making exhaustive list of all possible digital entities. Entities is selected in two perspectives; who the suspect contacted in the last 14 days and where the suspect went to in the last 14 days. Classification of entities and Determination of ranking will be done in final report.

Preface

a) Background & Necessity

Epidemics becomes more severe and makes serious casualty. In 2015, MERS caused 186 infected people and 38 death tolls in South Korea. It is second highest mortality in the world. Eradication took long time because secondary, tertiary infection occurs and caused propagation of disease. It ventilated the importance of tracing start point and blocking the contagion. Not only for the temporary epidemics, but also the ordinary ones like tuberculosis or influenza are also important in national prevention of epidemics.

Table 1. Statistics about infection occurrence of each epidemic, KOSIS [1]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Diseases | Year | | | |
| 2018 | 2017 | 2016 | 2015 |
| Hepatitis A | 2,437 | 4,419 | 4,679 | 1,804 |
| Varicella | 96,467 | 80,092 | 54,060 | 46,330 |
| Tuberculosis | 26,433 | 28,161 | 30,892 | 32,181 |
| AIDS | 989 | 1,008 | 1,060 | 1,018 |

These kinds of tracing are called contact tracing. It may accompany with analog method such as legwork or investigating real scene. However, in recent society, most people exposed to digital devices and they have lots of information about one person. Thus, it is important to deal with these sources and find out needed information.

Digital forensics are overall methodologies to find out data from digital entities. Entities can be any kind of sources; tangible or intangible, public or private, portable or stationary, etc. Its history is just about 30 years, but now digital forensics is one of most important investigation methodologies because almost every people are exposed to various digital devices. In daily routine, people use their cell phone, computer, credit card, etc. Except some rural area, CCTV is installed in every road and alley. Cars usually equips a black box. These kinds of digital devices contain lots of information. Naturally methods for investigating those data is studied and developed. It is now established with formal methodologies called digital forensics and numerous search algorithm or programs are developed to each specific source.

Table 2. Example of Digital Forensics Tools [1][2]

|  |  |
| --- | --- |
| Data Source | Forensics Tools |
| Cell Phone | XRY, TULP 2G |
| Desktop/Laptop | CrowdResponse, Volatility (RAM), Linux ‘dd’, HxD |
| Image | Exiftoll (EXIF metadata), |
| USB | DSi USB Write Blocker, USB Historian |
| File System | FTK Imager, Free Hex Editor Neo, |

It can be applied to various situation, but most commonly used part is crime scene investigation, especially to suspect tracking. People leave their trace more easily to various devices and it becomes important evidence to find out suspect, victim or witness’s whereabouts. These methods can be applied to epidemiological contact tracing also.

There are some differences between suspect tracing and epidemic case. For example, suspects try to hide the evidence, but people don’t matter of leaving their trace in epidemic situation. Thus, it is easier to find out their trace. In addition, epidemiological situations are mostly controlled in national level, therefore more entities are accessible.

Meanwhile, there are still problems for the application. First, experts or methodologies about digital forensics are still lacked in South Korea. Also, the research attaching digital forensics to epidemiological circumstances is not much compared to crime scene investigation. Because of that, it is needed to make guideline that applies to various problematic situations while using digital forensics methodologies to epidemics contact tracing.

b) Goals

Establishing whole methodologies from evidence identification to analysis, presentation is not easy procedure. Because of that, I’ll focus on evidence identification and collection. Among others, main goal will be making a checklist of all possible digital devices. The entities contain information and data about ⅰ) who this person contacted in the last 14 days, ⅱ) location this person went to in the last 14 days.

Table 3. Example list of digital entities

|  |  |
| --- | --- |
| 1. Who this person contacted in the last 14 days | 2. Location this person went to in the last 14 days. |
| Call Records | GPS |
| SNS | Black Box |
| E-Mail | CCTV |
| Messenger | Wi-Fi Access Record |
| Image Content | Image EXIF Metadata |
| … | … |

One source can contain sort of data in it. For example, cell phone is most important entity and holds several kinds of information in it. Some of them like GPS or EXIF in image will be related to whereabouts while image content or call record to contacted people. Each data will affect to the importance of a source.

Table 4. Example of data in one source

|  |  |
| --- | --- |
| Data Source | Data Type |
| Cell Phone | Call Record |
| Wi-Fi Access |
| Bluetooth |
| Image |
| NFC |
| SNS Record |
| Image | Content |
| EXIF Metadata |

List contains entities available in domestic only because things in abroad is difficult to deal with. It will be exhaustive list that includes every possible evidence. If several sources have the same data type (i.e. Images in mobile phone, Images in digital camera), they will be treated with different one.

Next, I’ll determine the ranking according to 2 standards; importance of evidence and level of difficulty to collect. Difficulty will be determined with cost of tools (open vs. closed), legal issues, quantity and several conditions. Consequentially, it will be arranged into a checklist. Researchers check the entity is available or not, and the quantity.

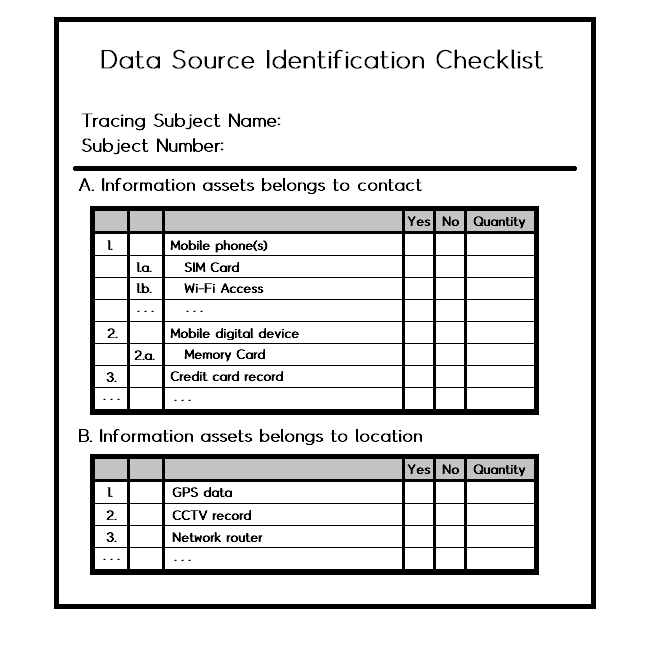


Figure 1. Example of data source checklist

For evidence assessment, I referred digital forensic examination guide. By the guideline, warrant and legal authorization, case detail, nature of hardware and software, potential evidence and circumstances surrounding the acquisition of the evidence is reviewed to assess evidence [15]. In our case, it is epidemiological situation and investigation is conducted by government, thus legal authorization will have a low priority than others. They divided the procedure with several parts. I’ll examine each part and assess the evidence.

c) Overview

In overall digital forensic models introduced in [4], this research can be helped from preparation to examination phase. It is difficult to suggest whole standards of digital forensics, so the direction will be small part of it, especially with evidence collection. Unlike physical evidence, digital entities include lots of intangible, invisible evidence, so it is likely to be missed than physical one. That’s why the checklist must include as many entities as possible. It also must be detailed rather than rough subscription. As I described in upper paragraph, some digital device like mobile phone can have several digital entities. Final output will be similar subscribed in goal paragraph, the exhaustive list of digital entities. To find out evidence thoroughly and efficiently, I divided the list with two conditions; private vs. public and portable vs. stationary. Among them, I couldn’t find public and portable devices that can be used as digital entities, so I excluded it. Instead, those criteria don’t contain virtual entities successfully, thus I included the list of virtual devices. The list contains about 30 normally available and highly efficient entities. Each entity is assessed with some standards and ranked.

In investigation, researchers start with first subject, broaden risk group according to subject’s contact and whereabout, and finally prevent further infection or find out the root of epidemics. We will not discuss about real investigation and custody process in this paper.

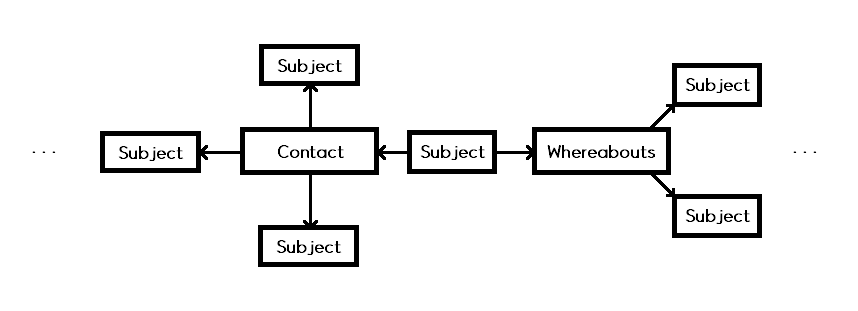


Figure 2. Subject broadening process

Related Research

[5] IACP introduces common electronic devices that generate digital evidence. There are personal digital devices like cell phone or laptop, and regional devices like CCTV. It doesn’t show further details about the types of evidence, but it can be used as first abstract of our goal.

Table 5. List of digital devices

|  |  |
| --- | --- |
| Device | Types of Evidence |
| Cell Phone | Call Records  Messenger  Applications |
| Desktop/Laptop | Internet Search History  Documents |
| CCTV | Videos |
| Drones | Videos |
| … | … |

Most important digital devices may be smartphone. Penetration rate of smartphone in South Korea already exceeds 90 percent (Gallup, 2017) and it is most portable among digital devices. Besides, smartphone becomes more versatile and contains more sensors, storages and applications collecting and storing data inside. That is, smartphone is most likely storing important information and data in it.

[6] In Willassen’s paper (2005), it introduces methods for imaging the internal memory of mobile phones including deleted memory. Usual phones use GSM system and it mandates SIM as a memory. In typical methods that using AT commands or analyzing live memory, there is some problems that deleted memory cannot be restored or memory can be overwritten while a phone is on. Thus, it is safe to analyze the phone in ‘dead’ status. Not only for smartphone, most memory devices tend to be analyzed with off status. In epidemic case, the probability of intentional memory corruption will not be occurred, but still the possibility of by accident exists. Thus, storage analysis may accompany with dead forensic and differences between live and dead forensic must be in calculation.

[7] Methods for collecting smartphone sensor data is introduced in Mylonas et al. (2013). Smartphone includes multimedia hardware and various sensors like location, but the most sensor data is not available because it’s volatile data. The commonly possible ways are collecting data as soon as the signal is occurred by the subject or from service provider. In our research, we focus on finding out the whereabouts of last 14 days so ad hoc data may not available, but system provider and hardware log file are still available.

[8] Agarwal et al. (2012) introduces Smartphone forensic investigation process model (SPFIPM). It claims the difference of computer forensics vs. mobile phone forensics and suggests new process model for the smartphone. Comparing to computer, mobile phone constantly alters its memory, so it is harder to get whole copy of the memory. Phone has more variable ways to connect to online than computer. That is, whether the phone is on or off is an issue in the process.

Major difference between traditional digital forensic model descripted in Reith’s paper (2002) [4] and communication shielding according to the PDA mode and subdivision of evidence collection. The important thing is remaining PDA mode as it is and preventing volatile memory from disappearing.

[9] Kesslar et al. (2010) subscribes Android forensic procedure. It shows several methods to analyze Android smartphone that acquiring dd image using FTK Imager, logical analysis and data extraction with the CelleBrite UFED. From the image, various digital data like call history, MMS/SMS message, web search history, e-mail, GPS data and video/photo can be found. Each of them can be considered as available digital entities in smartphone.

[10] Jeong et al. (2011) discusses about digital forensics of IaaS cloud computing service. In cloud computing, physical data storages places here and there, so it causes legal problem in collection. Also, in the public cloud service like AWS, numerous users share the service, memory or network thus it makes collection difficult further. This paper suggests its own forensic process for cloud service and find out evidence.



Figure 3. Cloud Service Digital Forensic Process [10]

Available digital evidence is virtual instance, network layer data and client system data. Instance can provide data location and drive position and client system works as an application in client site, so its data can be important evidence. Network layer provides communication data and protocol data, but it is better investigated with other network forensic process.

[11] Perumal et al. (2015) introduces IoT digital forensics investigation model. With IoT service, digital devices become more versatile. It makes each device can store various types of data. Therefore, like a smartphone, IoT devices become important in terms of digital forensics. Unlike typical computer or devices, IoT connects almost every device in it and composes large, complex system. Because of that, it is hard to apply typical forensic methods to IoT effectively. They divide entire system as 3 zones: internal network, middle (gateway, firewall, etc.) and external network (Internet, cloud, web services, etc.). With IoT digital forensic, investigators can get almost every kinds of digital evidence.

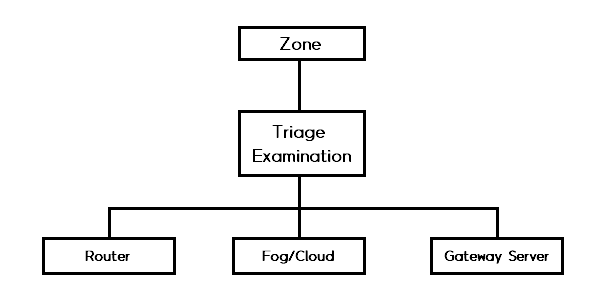


Figure 4. IoT based digital forensic model [11]

[12] Lee et al. (2008) suggests forensic analysis methodologies about embedded system. Each device has unique system according to their purpose and operation environment. Because of this diversity, it is nearly impossible to formulate general methods of embedded system forensic. Their methodology is not a whole process matching for every system but provides comprehensive analysis techniques. It is composed with two phases: hardware and software analysis phase. With information provided by manufacturer, it checks specification, configuration, etc. about hardware/software. It emphasizes on revealing hidden or modified data, but it is less likely in our case, thus it is easier to find out required data with system analysis.

[13] Among IoT devices, Boztas et al. (2015) focuses on Smart TV forensics. Smart TV are usually IP based device, and can be connected to Internet, social network service and other digital devices. It introduces data acquisition method depending on the hardware type. Available data is like smartphone or computer.

[15] There is guideline for the forensic examination of digital evidence. In this paper, the procedure of assessment is composed with case assessment, onsite consideration, processing location assessment, legal consideration and evidence assessment. Except legal authority and documentation, I’ll check out each part and apply it to the report. First is examining what the forensic examination can or cannot discover.

- Other forensic processes: Autopsy, toxicology and pharmacology is related to the epidemiological cases. It is not related to the contact tracing which I focus on, but it becomes important when investigators really find out contacts and distinguish risk group.

- Possibility of pursuing other investigate avenues: In contact tracing, we must investigate numerous digital devices. Not only the warrant, investigators must prepare several official documents to ask for cooperation to Internet service provider and mobile service provider. It is enquired by government, so it may not hard to investigate public devices.

- Peripheral components, Potential evidence, Additional Information: It is not crime scene investigation and not related to the specific device and we are supposed to identify all kinds of general entities, thus I may not have to consider in this report.

Second is onsite consideration. It contains the information about examining digital evidence. As an example, it suggests guideline for computer investigation. Like this, I’ll determine some consideration about each evidence.

Third is processing location assessment. It is about controlling environment when the onsite examination is required. It is also important to investigate personal devices in the lab.

Last is evidence assessment. With original conditions; amounts and importance of the evidence, we can consider stability, location of evidence found, etc.

Introduction

The topic is application of digital forensics for epidemiological contact tracing. I’m just a beginner in this area, so I decided to narrow down the goal. Real work is concentrated to the checklist for the digital forensics. Checklist consists of all kinds of digital evidence that can apply to the contact tracing. The type of evidence is not much different with the case of crime suspect tracing. Rather, the subject rarely tries eliminating or hiding data compared to criminals. That is, each device can be investigated with typical methodologies without the concern about intentional concealment. It can widen the range of possible digital sources.

My research is made up of mainly two part. First is the complete list of all possible digital evidence. Evidence can be exposed from any kind of sources; thus, the list must include digital sources as many as possible. Integrating all sources in one table is difficult and more likely to miss some entities. It is required to divide the entire list with several criteria according to their properties. It’ll be similar with categorization of devices. Representatively, portable vs. stationary, network device vs. stand-alone device or public vs. private can be categories. Not only their attributes, type of data (Image, Text, Video, etc.), which issues it is related to (location vs. contact vs. both) also can be the topic of list.

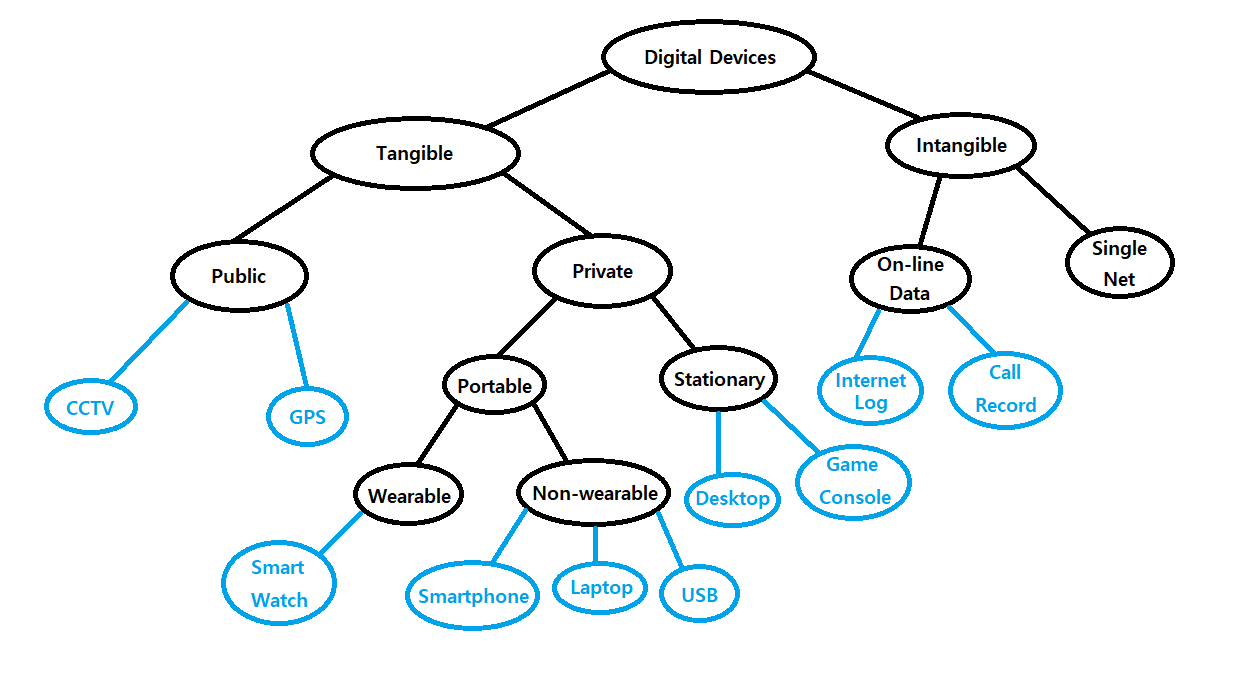


Figure 5. Classification of digital devices

Among them, I chose public vs. private and portable vs. stationary. To avoid duplication each other, the list is composed with public/portable, public/stationary, private/portable, private/stationary. In these criteria, there is no specific entities in public/portable device list. Instead, current lists cannot embody virtual entities like cloud service or SNS because they can be used for public/private simultaneously. Thus, I added virtual entities in a separate list. In a draft, I didn’t consider whether it is worthful for digital forensics or not and tried to find out all entities in it.

In private items, almost of them are the devices that is portable or in their home. Especially, portable devices like smartphone, credit card will be most important entities among all. I classified the list by entities and doesn’t considered which data is in it. For example, smartphone has numerous data like message, call record, image, video, but I didn’t divide it into individual one. It will be discussed when I evaluate the importance of each evidence. In stationary item, there are not many devices that can store valuable items in subject’s home. Maybe only personal computer, network modem or IoT devices will be important evidence in forensics. In subject’s workplace, most of digital devices is company’s one, not private. Except their desktop, other devices are included in public devices.

In public devices, there are not many portable/public devices and they even cannot save some data in it. Thus, I only considered public/stationary devices in the list. I divided it further with the location evidence can be found; office, on the road and any other places. It is mainly about subject’s whereabouts. CCTV can provide someone’s destination and contact both, therefore it will be most important among public devices. Some terminals that interact with personal item like credit card reader, RFID gate are also crucial for digital forensics.

Virtual items cover lots of data sources in it, but maybe electronic mails, social network service and cloud services will be worth to find out our target information. Many services may store subject’s access log, but it is hard to take out some special places rather than his/her home or office. That is, compared to the cost of the investigation, the probability of getting some important information is relatively low. Thus, I narrowed the range of virtual entities with something including specific location information or communication with others. SNS satisfies both, thus it will be important entity among virtual ones. E-mail is also used to communicate each other, so it can show the possible group of contact with subject.

With these considerations, I revised whole entities in one list, included some other entities and excluded some less important ones. Every item is numbered, and I divided portable/private item with two articles; subject’s body/belonging and subject’s vehicle. Public item consists of residential area, working location and other visiting places. Workplace and other places have the same entries in it.

Recently, more devices become versatile and have various function. Even it is the same source, available data will be different seriously. For example, unlike past feature phone, smartphone contains much more functionalities. Drones equips various sensor according to their purpose, so available data can be diverse. Also, some sources are newly appeared as data source. Television just has one functionality; Receiving electric wave and transmit the broadcast. But now, smart TV have some functions and applications same as smartphone. However, it also means that some entities not in the list are available while other in the list are not. It is general purpose checklist; thus, the entity will be composed of universal one.

Second, entire list will be ranked by two criteria. First is the importance of the evidence. It can include several standards. For instance, its distribution rate seriously affects to the availability. The portability also can influence to the likelihood of the access. Second is the difficulty of acquirement. If this source is worthy and contains much data but it’s impossible to get it, it becomes useless. Analysis methods are still advancing, but still the problems like obsolete software/hardware or lack of research about new technologies make it harder to find out useful data from it. Also, contact tracing is related seriously to privacy invasion, so there are several lawful and moral issues. Each attribute can occur some issues while get rid of it. For example, public facilities can be researched more easily than personal one in terms of lawful issue. In the same private things, smartphone or desktop are more likely to have personally sensitive information than other devices and raise hostility to the investigation. Because of these problems, the researchers still endeavor to establish legal process of digital forensics. In our situation, some problem will be released in some level. In South Korea, there is law about disaster & safety management [14]. According to that, every investigation must be executed with executive order and every safety management facility must provide required data without specific reason. Civilians also must be cooperative to disaster response. That is, we can put legal problems as secondary and focus on technical issues to measure difficulty.

For each device, we can measure the approximate values about its importance and difficulty in the form of card. It contains the name, data type, evaluation, pros and cons, etc. Based on that, we can make ranking among sources.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Evaluation Card** | | | | | | | | | |
| 1. Device: Smartphone | | | | | | | | | |
| 2. Number: 001 | | | | | | | | | |
| **3. Data Type** | | | | | | | | | |
| Text | Image | | Video | | App / .exe | | Network | | Storage |
|  |  | |  | |  | |  | |  |
| 3.1. Miscellaneous: | | | | | | | | | |
| **4. Evaluation Store** | | | | | | | | | |
| 4.1. Importance of evidence | | | | | | | | | |
| Not important ↔ Important | | | | | | | | | |
| 1 | | 2 | | 3 | | 4 | | 5 | |
| 4.1.1. Evaluation criteria  Quantity of data about contact  Quantity of data about whereabouts | | | | | | | | | |
| 4.2. Difficulty of acquiring evidence | | | | | | | | | |
| Easy ↔ Difficult | | | | | | | | | |
| 1 | | 2 | | 3 | | 4 | | 5 | |
| 4.2.1. Evaluation criteria  Penetration rate (Availability)  Required tools / technology for investigation | | | | | | | | | |

Figure 6. Example of evaluation card

Scoring is rough method and maybe hard to distinguish delicate difference among them, but it is more comfortable to measure its importance. Details will be written in criteria section. Criteria in the example is default and some items can be added for several entities.

Based on the evaluation, we can measure the rank of entities. So far from charge the rank one by one, it will be the sort of groups like most primary, secondary, ternary, etc. For example, most important devices like smartphone or desktop will be primary group, while intermediate ones like drone, smart watch, etc. will be secondary group. It may not be an exact priority, but it can be a guide to decide the order of investigation.

Implementation & Result Analysis

Table 6. List of Portable/Private Items

|  |  |
| --- | --- |
| Device | Entities |
| Digital Camera | Images  Videos  Storage (SD Card) |
| Smartphone | Text Messages  Call Logs  Application  SNS accounts  GPS  Wi-Fi Access  Bluetooth  NFC |
| IPad | Same as smartphone |
| Credit Card | Credit Card Record |
| Smartwatch | Same as smartphone |
| Laptop | Internet Search History  Storage (HDD, SSD)  SNS accounts |
| External Hard Disk | All kinds of digital files |
| Drone | Videos |
| USB Memory | All kinds of digital files |
| SD Card | All kinds of digital files |
| Blackbox | Videos |
| HiPass | Through Time |

Table 7. List of Stationary/Private Items

|  |  |
| --- | --- |
| Device | Entities |
| Subject’s Home | |
| Personal Computer | Internet Search History  Storage (HDD, SSD) |
| Game Console | Images  Videos  Documents  Operation Log |
| Robotic Vacuum Cleaner | Operation Time |
| Internet of Things [11] | Every type of digital file |
| Embedded System [12] | Every type of digital file |
| Smart TV [13] | Application  Web Browsing  Images and Multimedia Files  External Media (USB, Flash drive, etc.)  Cloud Service  E-mail |
| Internet Modem | Access Record |
| Subject’s Office | |
| Office Desktop | Internet Search History  Storage (HDD, SSD) |

Table 8. List of Stationary/Public Items

|  |  |
| --- | --- |
| Device | Entities |
| Subject’s Office | |
| Network Switch / Router | Access Records |
| Server | Access Records |
| Surveillance Camera | Videos |
| RFID Reader | Access Records |
| Digital Printer | Usage History |
| VoIP PBX System | Access Records |
| At Outside | |
| CCTV | Videos |
| Toll Gate | Through Time |
| ATM | Credit Card Records |
| Wi-Fi | Access Records |
| Network Switch / Router | Access Records |
| Access Point (AP) | Position Information |
| Card Reader Slot | Credit Card Records |
| Ticket Office | Ticket Issue Records |
| Immigration Office (Airport / Harbor) | Immigration Records |

Table 9. List of Virtual Entities

|  |  |
| --- | --- |
| Device | Entities |
| Cloud Service | Every type of digital file  Access Records |
| Music Streaming | Usage Time |
| Video Streaming | Viewing Time |
| E-Commerce | Purchase Records |
| SNS | Timeline  Access Log |

It’s a list to search out candidates of entities. As I mentioned in introduction, the criteria are composed with private vs. public and portable vs. stationary. I excluded public/portable devices because there is no available entity. Virtual devices are little bit hard to fix in single list, so I separated it as a distinct list. These criteria are just used for finding out every possible entity and not an unchangeable thing.

With these entities, I abbreviated in one list. Every item is numbered and divided each entity with several specific criteria. First is personal vs. stationary vs. virtual entities. In portable entities, there are private things only, so I separated with the place; body, belongings and vehicles. In stationary items, I divided it into residential place and office. Public area only has stationary items, so I separated it with area; residential place, office and other places like roads or complex.

1. Personal Entities
   1. Portable Entities
      1. Entities that can be identified on subject’s body and/or personal belongings
         1. Mobile phone
         2. Laptop computer
         3. Tablet
         4. Digital camera
         5. Smartwatch
         6. Physical activity tracker
         7. Removable media

1.1.1.7.1 External Hard Disk

1.1.1.7.2 USB Memory

1.1.1.7.3 SD Card

* + - 1. Transportation payment card (T-money)
      2. Credit card(s) and bank card(s)
      3. Electronic entrance card(s)
    1. Entities that can be identified on subject’s vehicle(s)
       1. Embedded system of the vehicle(s)
       2. Blackbox
       3. Toll road payment system (HiPass)
       4. Navigator (GPS)
       5. All entities listed in 1.1.1
  1. Stationary Entities
     1. Entities that can be identified at subject’s residential location
        1. Personal computer
        2. Game console
        3. Smart TV
        4. Security cameras (e.g. webcam, CCTV)
        5. All entities listed in 1.1.1
     2. Entities that can be identified at subject’s working location
        1. Office Desktop
        2. Security cameras (e.g. webcam, CCTV)
        3. All entities listed in 1.1.1

1. Public Entities

2.1 Subject’s residential location

2.1.1 CCTV cameras in public area

2.1.2 Electronic entrance record

2.1.3 Parking lot entrance record

2.2 Subject’s working location

2.1.1 Wireless network switch / router log

2.1.2 CCTV Cameras

2.1.3 Electronic entrance record

2.3 Other locations subject visited

2.1.1 Wireless network switch / router log

2.1.2 CCTV Cameras

2.1.3 Electronic entrance record

1. Virtual Entities
   1. Cloud drives
   2. Email accounts
   3. SNS

Next, I evaluated with some standards. First, I identified data type that can be acquired from this entity. Second, I scored its importance and difficulty. It may be rough method, but it is easy to compare each other. Then, I commented some evaluation criteria under the score. Quantity of data about contacts and whereabouts is crucial to determine its importance. Difficulty can be affected by several things like penetration rate or required tools. It is hard to find out details about legal issues, so I excluded it. It is for epidemiological case investigation and don’t have to adopted as evidence, so legal issues will be difference with crime scene case. In principle, there is not much obstacles with public things while there are privacy issues with private. There is no specific form and I wrote down in one sentence or reference. I show several evaluations here. Entire assessment is uploaded in Github.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Evaluation Card** | | | | | | | | | |
| 1. Device: Mobile phone | | | | | | | | | |
| 2. Number: 1-1-1-1 | | | | | | | | | |
| **3. Data Type** | | | | | | | | | |
| Text | Image | | Video | | App / .exe | | Network | | Storage |
| ∨ | ∨ | | ∨ | | ∨ | | ∨ | | ∨ |
| 3. Miscellaneous: GPS, E-Mail, SNS, NFC, Bluetooth | | | | | | | | | |
| **4. Evaluation Store** | | | | | | | | | |
| 4.1. Importance of evidence | | | | | | | | | |
| Not important ↔ Important | | | | | | | | | |
| 1 | | 2 | | 3 | | 4 | | 5 ∨ | |
| 4.1.1. Evaluation criteria  Quantity of data about contact: Call record, SNS, Text message, Image, Video,  E-Mail  Quantity of data about whereabouts: GPS, SNS, Wi-Fi, NFC, Bluetooth | | | | | | | | | |
| 4.2. Difficulty of acquiring evidence | | | | | | | | | |
| Easy ↔ Difficult | | | | | | | | | |
| 1 ∨ | | 2 | | 3 | | 4 | | 5 | |
| 4.2.1. Evaluation criteria  Penetration rate (Availability): Almost everywhere  Required tools / technology for investigation: XRY, TULP 2G, etc. | | | | | | | | | |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Evaluation Card** | | | | | | | | | |
| 1. Device: Laptop Computer | | | | | | | | | |
| 2. Number: 1-1-1-2 | | | | | | | | | |
| **3. Data Type** | | | | | | | | | |
| Text | Image | | Video | | App / .exe | | Network | | Storage |
| ∨ | ∨ | | ∨ | | ∨ | | ∨ | | ∨ |
| 3. Miscellaneous: Internet Search History, SNS, E-Mail | | | | | | | | | |
| **4. Evaluation Store** | | | | | | | | | |
| 4.1. Importance of evidence | | | | | | | | | |
| Not important ↔ Important | | | | | | | | | |
| 1 | | 2 | | 3 | | 4 | | 5 ∨ | |
| 4.1.1. Evaluation criteria  Quantity of data about contact: SNS, Image, Video, E-Mail  Quantity of data about whereabouts: SNS, Internet Search History | | | | | | | | | |
| 4.2. Difficulty of acquiring evidence | | | | | | | | | |
| Easy ↔ Difficult | | | | | | | | | |
| 1 ∨ | | 2 | | 3 | | 4 | | 5 | |
| 4.2.1. Evaluation criteria  Penetration rate (Availability): Almost every place  Required tools / technology for investigation: CrowdResponse, Volatility, HxD, etc. | | | | | | | | | |

Evaluation of some entities will be different with crime scene case. For example, game console may be important in case of cyber-crime because it is often used to conceal fatal data. However, the most different point of epidemiological situation with crime is that the subject hardly tries to hide information. That is, it is important to find out existing important information than hidden information. But still, complex and well-used devices like computer and smartphone will have various important information and treated same as crime case.

According to the assessment, I arranged entire entities in one checklist. Investigators will check each evidence’s availability and quantity in the list.

|  |  |  |  |
| --- | --- | --- | --- |
| Entity | Availability | | Quantity |
| Yes | No |
| 1. Personal Entities |  |  |  |
| 1.1. Portable Entities |  |  |  |
| 1.1.1 Entities that can be identified on subject’s body and personal belongings |  |  |  |
| 1.1.1.1 Mobile phone |  |  |  |
| 1.1.1.2 Laptop computer |  |  |  |
| 1.1.1.3 Tablet |  |  |  |
| 1.1.1.4 Digital Camera |  |  |  |
| 1.1.1.5 Credit card |  |  |  |
| 1.1.1.6 Transportation payment card |  |  |  |
| 1.1.1.7 Removable media |  |  |  |
| 1.1.1.7.1 USB Card |  |  |  |
| 1.1.1.7.2 External Hard Disk |  |  |  |
| 1.1.1.7.3 SD Card |  |  |  |
| 1.1.1.8 Electronic entrance card |  |  |  |
| 1.1.1.9 Smartwatch |  |  |  |
| 1.1.1.10 Physical activity tracker |  |  |  |
| 1.1.2 Entities that can be identified on subject’s vehicle |  |  |  |
| 1.1.2.1 Navigator (GPS) |  |  |  |
| 1.1.2.2 Blackbox |  |  |  |
| 1.1.2.3 Toll road payment system (HiPass) |  |  |  |
| 1.1.2.4 Embedded system of the vehicle |  |  |  |
| 1.2 Stationary Entities |  |  |  |
| 1.2.1 Entities that can be identified at subject’s residential location |  |  |  |
| 1.2.1.1 Personal computer |  |  |  |
| 1.2.1.2 Security cameras |  |  |  |
| 1.2.1.3 Smart TV |  |  |  |
| 1.2.1.4 Game console |  |  |  |
| 1.2.2 Entities that can be identified at subject’s working location |  |  |  |
| 1.2.2.1 Office desktop |  |  |  |
| 1.2.2.2 Security cameras |  |  |  |
| 2. Public Entities |  |  |  |
| 2.1 Subject’s residential location |  |  |  |
| 2.1.1 CCTV cameras in public area |  |  |  |
| 2.1.2 Electronic entrance record |  |  |  |
| 2.1.3 Parking lot entrance record |  |  |  |
| 2.2 Subject’s working location |  |  |  |
| 2.2.1 CCTV cameras |  |  |  |
| 2.2.2 Wireless network switch / router log |  |  |  |
| 2.2.3 Electronic entrance record |  |  |  |
| 2.3 Other locations subject visited |  |  |  |
| 2.3.1 CCTV cameras |  |  |  |
| 2.3.2 Wireless network switch / router log |  |  |  |
| 2.3.3 Electronic entrance record |  |  |  |
| 3. Virtual Entities |  |  |  |
| 3.1 SNS |  |  |  |
| 3.2 E-mail accounts |  |  |  |
| 3.3 Cloud drive |  |  |  |

Conclusion & Opinion

I mainly focused on finding out all possible digital devices in interim report and on ranking in final report. Unlike entity identification, it was very hard to assess them all. There are many issues to calculate their values, but I’m not an expert on digital forensics and hard to find out forensic tools, legal issues or vulnerability. Especially, legal problem is not a simple problem for digital forensics, and I couldn’t find out related legal clause for each entity. Of course, epidemiological case is different with crime scene and entity doesn’t have to be adopted as evidence. That is, investigators are free of legal problem than crime scene investigation except privacy problem or cooperation with companies. I didn’t know further about legal problem above it; thus, I couldn’t use it to compare entities. I tried to add various criteria for the assessment, but consequently I just used penetration rate and its available forensic tools. Assessment should be reinforced with subsequent researches.

It was first time to write down the essay. I didn’t have any prior knowledge and interest, so it was hard to research and make up of complete report. My essay doesn’t include any programming but still the research was not an easy-going. While preparing employment and attending lectures, I couldn’t concentrate to the essay wholly and it makes entire process delayed seriously. I cannot convince it will be helpful to me because I couldn’t do the work properly and process roughly here and there. A series of work make me feel about the difficulty of making up of single essay and research and attitude for completing research. I’ll try to make the research at some level, but I wonder it can achieve valuable research result. If I have a chance to do some research after, I must have much time and concentrate only to it.

References

[1] http://kosis.kr/statHtml/statHtml.do?orgId=117&tblId=DT\_117N\_A00406&vw\_cd=MT\_ZTITLE&list\_id=D19&seqNo=&lang\_mode=ko&language=kor&obj\_var\_id=&itm\_id=&conn\_path=MT\_ZTITLE

[2] https://techtalk.gfi.com/top-20-free-digital-forensic-investigation-tools-for-sysadmins/

[3] THING, Vrizlynn LL; NG, Kian-Yong; CHANG, Ee-Chien. Live memory forensics of mobile phones. *digital investigation*, 2010, 7: S74-S82.

[4] REITH, Mark; CARR, Clint; GUNSCH, Gregg. An examination of digital forensic models. *International Journal of Digital Evidence*, 2002, 1.3: 1-12.

[5] Common electronic devices that generate digital evidence, https://www.iacpcybercenter.org/officers/cyber-crime-investigations/common-electronic-devices-that-generate-digital-evidence/

[6] WILLASSEN, Svein. Forensic analysis of mobile phone internal memory. In: *IFIP International Conference on Digital Forensics*. Springer, Boston, MA, 2005. p. 191-204.

[7] MYLONAS, Alexios, et al. Smartphone sensor data as digital evidence. *Computers & Security*, 2013, 38: 51-75.

[8] GOEL, Archit; TYAGI, Anurag; AGARWAL, Ankit. Smartphone forensic investigation process model. *International Journal of Computer Science & Security (IJCSS)*, 2012, 6.5: 322-341.

[9] LESSARD, Jeff; KESSLER, Gary. Android Forensics: Simplifying Cell Phone Examinations. 2010.

[10] 정일훈, et al. IaaS 유형의 클라우드 컴퓨팅 서비스에 대한 디지털 포렌식 연구. *정보보호학회논문지*, 2011, 21.6: 55-65.

[11] PERUMAL, Sundresan; NORWAWI, Norita Md; RAMAN, Valliappan. Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology. In: *2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC)*. IEEE, 2015. p. 19-23.

[12] LIM, Kyung-Soo; LEE, Sangjin. A methodology for forensic analysis of embedded systems. In: *2008 Second International Conference on Future Generation Communication and Networking*. IEEE, 2008. p. 283-286.

[13] BOZTAS, Abdul; RIETHOVEN, A. R. J.; ROELOFFS, Mark. Smart TV forensics: Digital traces on televisions. *Digital Investigation*, 2015, 12: S72-S80.

[14] 재난 및 안전관리 기본법, <http://www.law.go.kr/법령/>재난및안전관리기본법

[15] <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf>