EMB000023d44eea

연구논문/작품 제안서

2019년도 제1학기

|  |  |
| --- | --- |
| **논문/작품** | ○논문(●) ○ 작품( ) ※ 해당란에 체크 |
| **제목** | Application of Digital Forensic Methodologies in Epidemiological contact tracing |
| **GitHub URL** | https://github.com/dlsgk147/2013311425\_GraduateEssay |
| **팀원명단** | o 윤인하 (인) (학번: 2013311425) |

2019년 3월 18일

지도교수 : Arthur Tang 서명

**Abstract**

Tracing suspects are always important in investigation, so methodologies continually improved. It contains several digital devices from personal device like cell phone, credit card to public like surveillance camera. Those things are included in human interaction and contact; thus, it generates numerous tangible and intangible evidence for tracking suspects. So, investigators find calling records, internet search history or black box records to find clue. These kinds of methodology are called digital forensics. There is high-end equipment for analyzing those things in media, but real search is not an easy-going. Most obstacles are derived from suspects like changing phone, using stolen car, manipulating identity and it makes investigation more time-consuming. To deal with this, many researchers focus on digital forensics that raise quality, quantity of evidence and minimize cost.

Meanwhile, the threat of epidemics is getting bigger worldwide. From Severe Acute Respiratory Syndrome (SARS), Ebola Virus to Middle East Respiratory Syndrome (MERS), they caused severe casualty. One of the most effective way against epidemics is contact tracing. It means that find out the root and prevent further spread of disease. Our goal is applying digital forensics methodologies to contact tracing and make checklist for helping tracing.

1. **Necessity for the study**

In tradition, tracing person is done mostly with legwork like questioning or visiting related place. However, beyond the real world, digital evidence becomes more important nowadays. People usually uses credit card to buy something, cell phone and computer to interact with others and camera to take a picture. Those things can be a vital clue for finding trace of the people concerned. For example, we can infer recently contacted person with call records or visited place with credit card usages, vehicle information. Naturally, people started to

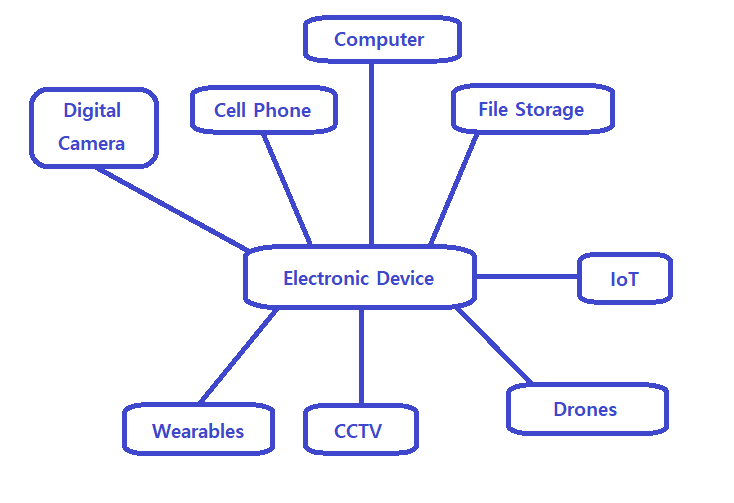


Figure 1. Types of electronic devices introduced in IACP [1]

focus on digital evidence and it derives new science called digital forensics. Forensics itself is not an original thing but means applying scientific methodologies to investigate crime. Digital forensics is defined as using scientific methods to find, identify, analyze or preserve digital evidence from digital sources [2]. Simply, it means that finding and analyzing digital evidence from digital sources, or electronic devices with authorized methods to find out tangible and intangible clues related to criminal, suspects or victims. Unlike computer forensics that has particular field, that is computer, digital forensics must include all kinds of digital devices and standardized methodologies [2]. Many researchers emphasize importance of general procedure in digital forensics even though it is not that easy because of numerous variables according to device, type of crime and lack of technology [3]. They say that it benefits in securing quality,

As described before, epidemic have more terrible damage and casualty are also increasing recently. For example, MERS caused death-toll of about 40 and 186 people were sub-sequentially infected. in South Korea in 2015. There are many causes like medical infrastructure or hygiene, one of the major issues is the prevention of diffusion. When the first infected was detected, The Ministry of Health and Welfare detected all contacts of infected people and isolated them. It was very effective in finding secondary infected people and keeping disease from spreading. Nonetheless, the amount of damage was severe. Tour or business trip from and to Korea had been canceled and social activities halted. It shows the importance of early detection and prevention of epidemics. However, isolation and quarantine come with a high cost. It becomes dilemma of contact tracing. It needs to find out all carriers and isolate them and yet minimize the cost. To achieve it at least a bit, guideline for contact tracing will be necessary.

1. **Prior Research**
   1. **Digital Forensic Procedure**

In Abstract Digital Forensics Model (ADFM) which is an extension of digital forensics SOP proposed in [2]. In this model, there are 9 phases for digital forensic investigation: identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation and returning evidence [2][3]. Other models are little bit difference or concise version [3].

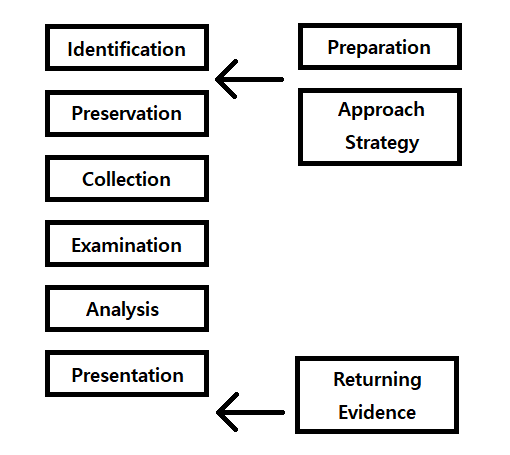


Figure 2. General Procedure of digital forensic in [3]

In Solms’ paper, there are more specific framework of digital forensic process. It divided entire process in 4 stages and made control objectives (COs), detailed control objectives (DCOs) [5]. Each stage is planning and preparation phase, incident response phase, investigation phase, forensic analysis phase.

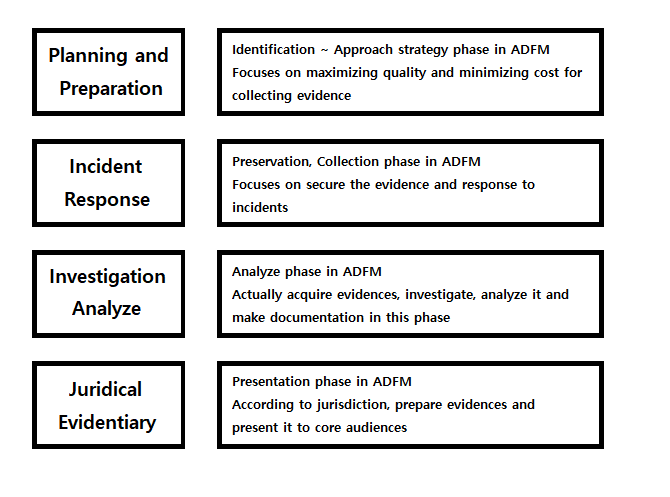


Figure 3. Digital forensics control framework proposed in [5]

Those researches are showing that from finding out sources, collect it to investigating and presenting evidences are all included in digital forensic procedure.

* 1. **Property of Digital Evidence**

In Sun’s paper, they considered about the property of digital evidence. They divide evidence into witnesses (Witness, victims), physical (Crime tool, Vestige) and documentary evidence (Living history, call record). Unlike typical one, digital evidence is recorded in electromagnetic storage and used with playing, printing, etc. It can be changed and also detected easier than real evidence. It makes secure digital evidence as it is harder than real evidence, so preservation and authentication phase become more important [6].

In Casey’s book, they introduce challenging aspects of digital evidence. First, it doesn’t have fixed form and intangible. Second, digital evidence may show only partial information. It can make constructing entire scene impossible. Third, proving digital evidence with to an individual is difficult because it usually shows only result. Fourth, those can be manipulated by attackers than real world’s evidence [7]. To establish guideline for dealing with digital evidence, these features must be considered.

* 1. **Digital Forensic Tools**

In Case’s paper, they introduced automated digital evidence discovery and correlation, FACE [8]. It automatically analyzes disk image, memory image or log files. In Turner’s paper, digital evidence bag (DEB) is introduced to cope with problems of digital evidence [9]. In our interested area, tracking suspects, there are forensics for mobile device like cell phone, laptop, wearable devices or SIM card [10].

1. **Research Plan**
   1. **Classification of digital devices**

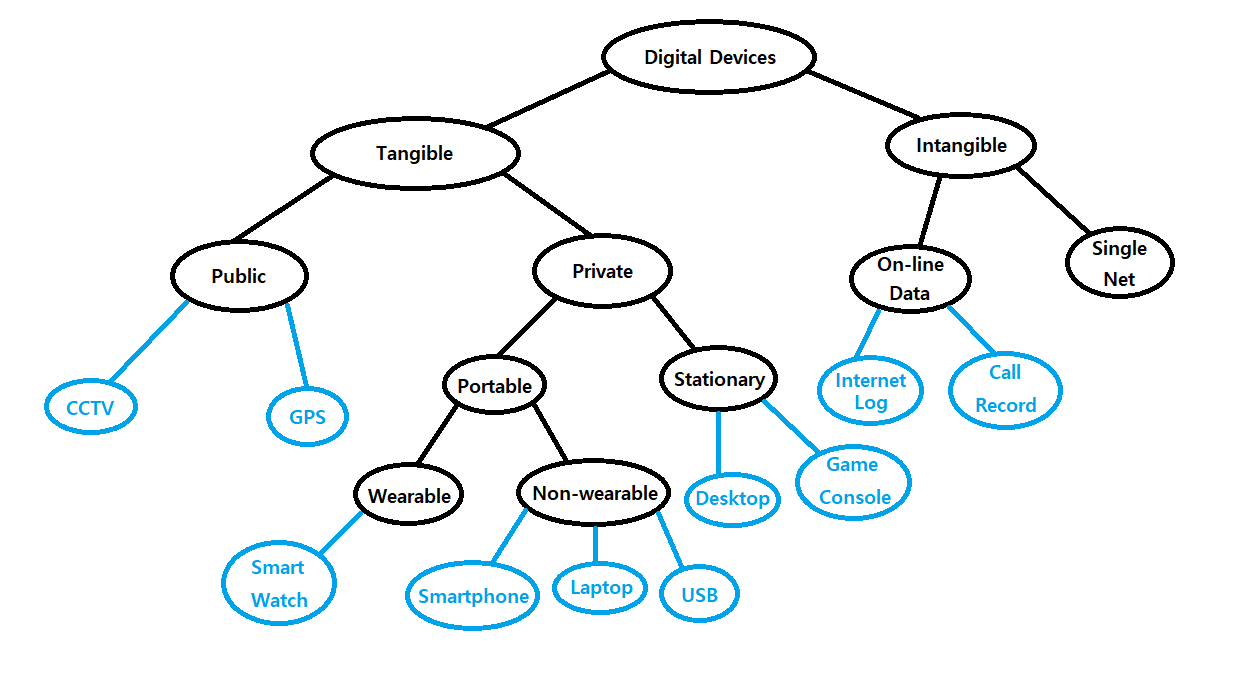
Firstly, I will find out available digital devices and classifying it. Criteria can be portable or not, tangible or intangible, personal or public, type of digital evidence that can be get from it, etc. We can make tree structure according to the criteria like this example. 

Figure 4. Example of Digital Sources Classification

Section can be various more than that, or some source can be included in several parent node.

* 1. **Making checklist for contact tracing.**

Second, I’ll make data source checklist for contact tracing. Sources may be ranked according to its efficiency. Quality of evidence, stability, cost, clarity or readiness can affect to this. With it, investigators may identify whether it is available or not, quantity if it is. This list must be an exhaustive list of all kinds of data sources containing meaningful information of social contact behavior and physical locations of contact tracing. Figure will be like Figure 5.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** | **No** | **Quantity** |
| **Cell Phone** |  |  |  |
| **Desktop** |  |  |  |
| **Surveillance Camera** |  |  |  |
| **Phone Call Record** |  |  |  |
| **GPS Information** |  |  |  |

Figure 5. Example of data source checklist

With prioritizing, it can be improved with adding a guideline for digital investigation process and data assets for each source containing rating, description, etc.

1. **Expectancy Effects & Improvement**

This research can help epidemiological contact tracing to be effective and fast. Investigators can check all available sources with a checklist. It is expected to reduce the time and cost for tracing all infected people.

This paper considers current devices only rather than future one. However, as it is described before, predicting coming technologies, devices and handling these are also important to establish procedure. Future devices cannot estimate its characteristic exactly and measure its effectiveness. Also, gap between period, region may not be considered enough in paper. I don’t have much information about this, so result can be not adequate in other country. I expect further research about those can improve the procedure more versatile and general.

1. **Miscellaneous**
   1. **Team Member**

Yoon In Ha: Research prior papers, analyze data, documentation

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| Proposal |  |  |  |  |  |  |  |  |  |  |
| Research |  |  |  |  |  |  |  |  |  |  |
| Analyze |  |  |  |  |  |  |  |  |  |  |
| Midterm  Report |  |  |  |  |  |  |  |  |  |  |
| Final  Report |  |  |  |  |  |  |  |  |  |  |
| Examination  Presentation |  |  |  |  |  |  |  |  |  |  |

# 6. References

# [1] COMMON ELECTRONIC DEVICES THAT GENERATE DIGITAL EVIDENCE

<http://www.iacpcybercenter.org/officers/cyber-crime-investigations/common-electronic-devices-that-generate-digital-evidence/>

[2] Mark Reith, Clint Carr, Gregg Gunsch, “An Examination of Digital Forensic Models”, International Journal of Digital Evidence, Fall 2002

[3] Jill Slay, Yi-Chi Lin, Benjamin Turnbull, Jason Beckett and Paul Lin, “TOWARDS A FORMALIZATION OF DIGITAL FORENSICS”, Springer, 2009

[4] Brampton Small Business Enterprise Centre,

<https://www.brampton.ca/EN/Business/BEC/resources/Documents/What%20is%20a%20Standard%20Operating%20Procedure(SOP).pdf>

[5] VON SOLMS, Sebastiaan, et al. A control framework for digital forensics. In: *Advances in Digital Forensics II*. Springer, Boston, MA, 2006. p. 343-355.

[6] Jia-Rong Sun , Mao-Lin Shih , Min-Shiang Hwang, “A Survey of Digital Evidences Forensic and Cybercrime Investigation Procedure”, International Journal of Network Security, Sept. 2015

[7] CASEY, Eoghan. *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press, 2011.

[8] CASE, Andrew, et al. FACE: Automated digital evidence discovery and correlation. *digital investigation*, 2008, 5: S65-S75.

[9] TURNER, Philip. Unification of digital evidence from disparate sources (digital evidence bags). *Digital Investigation*, 2005, 2.3: 223-228.

[10] CASEY, Eoghan; TURNBULL, Benjamin. Digital evidence on mobile devices. *Digital Evidence and Computer Crime*, 2011, 3: 1-44.

[11] Statista, <https://www.statista.com/chart/1405/the-united-states-ranks-13th-in-smartphone-penetration/>