(IJID) International Journal on Informatics for Development, *e-ISSN: 2549-7448*
Vol. 7, No. 2, 2018, Pp. 64-67

Digital Forensic Analysis on Android Smartphones for Handling Cybercrime Cases

Firmansyah Gustav Hikmatyar
Department of Informatics
Faculty of Science and Technology
Universitas Islam Negeri Sunan Kalijaga
Yogyakarta, Indonesia
fghgustav@gmail.com

Bambang Sugiantoro
Department of Informatics, Graduate Program
Faculty of Science and Technology
Universitas Islam Negeri Sunan Kalijaga
Yogyakarta, Indonesia
bambang.sugiantoro@gmail.com

***Abstract*— As the times progressed, forensic science has developed rapidly. The science of forensics extends to new areas of technology ranging from digital forensics, computer forensics and mobile forensics. Mobile forensics in analyzing and collecting data is obtained from various resources, such as operating systems, communication lines and also various storage media. The most popular mobile operating system of the day is a smartphone based on android operating system. With android technology, criminals can use that technology as a crime medium ranging from overriding crime ideas, crime targets and crime scenarios. In this Final Project use forensic mobile application to get data residing in cell phone actors, in the form of text, sound, picture and video that have or not yet deleted in smartphone. In this study, a model for investigating the crime scene is the author using the *Generic Computer Forensic Investigation Model* (GCFIM). On the GCFIM model the investigator may be able to return to the previous stage because of the possibility of a changeable situation (both physical and digital), the investigation tools used, the crime tools used, and the level of investigative expertise. In this research also added weighting method of word TF-IDF, where this method can help to find keyword in digital evidence in the form of word / text.**

Keywords-Digital Forensics; Mobile Forensics; Forensic Investigation GCFIM models; term frequency methods (TF-IDF)

I. INTRODUCTION

Smartphones are mobile phones or phones that have a high level of capability and have functions similar to computers. On smartphones raises a new study, which became known as mobile. Mobile forensics is a branch of forensic digital relating to recovery (recovery) evidence of digital in the form of data from devices, mobile which studies on the investigation, analysis, recovery, and management of data from digital media after a criminal action[1][2][3][4][5][6][7]. The purpose of mobile forensics is to conduct structured investigations by maintaining the stages of documentation of evidence to find out what is happening on the cellphone and who is responsible, so that it can be used as legal evidence in court. Smartphone Android itself is a device hybrid that can work as a cellphone and can also work almost like a computer but in a more simple portable form.

This research is focused on dealing with the problem of crime cases using smartphones. In addition, will try to do forensic analysis on smartphone or tablet devices that use various Android operating systems Platform. In addition, this study aims to evaluate tools forensic that can be used to analyze android phones based on the amount of evidence that can be collected by the tool forensic[8][9][10][11][12][13][14]

In this study the use of data mining methods or weighting method is Term frequency (TF)used in the case identification process, where the method will help the researcher in determining documents in the form of SMS to be used as evidence and assist investigators in finding new suspects. Term frequency can correct values recall in information retrieval, but does not always improve values precision. This is due to term the frequent tends to show up in a lot of text, so that terms these have the power differentiator (uniqueness) is small. While Inverse document frequency (IDF) is a method of weighting terms that are more inclined (focus) to pay attention to the appearance of the term in the whole collection of text. In IDF, terms that rarely appear in the entire text collection are considered more valuable. The value of the interests of each term is assumed inversely proportional to the number of texts containing the term. so Term frequency inverse document frequency (TF • IDF) is a weighting method that combines TF and IDF methods, a combination of methods that can provide better performance, especially in improving values recall and precision[16][17][18][19][20].

II. PURPOSE

The purpose of this study is to find out:

1) Applying forensic methods with reference to the investigation model of *Generic Computer Forensic Investigation Model (GCFIM)*, in the process of identifying evidence inform of *the Android smartphone*. In addition, learn how to do digital identification techniques *forensic* the right using the tools chosen.
2) Implementing the TF-IDF algorithm from searching documents from all documents in evidence in the form of messages *SMS* and ranking these search results to produce documents that are relevant to the *query*.

III. METHODOLOGY

The research method used is experimental method. Experimental methods are part of quantitative methods. Experimental studies produce the most correct evidence relating to causal relationships. In experimental studies, researchers manipulate at least one variable, control other relevant variables, and observe the effect / effect on one or more related variables. Therefore, the authors use mobile phones as objects of research, because *smartphones* themselves are widely used as a tool for crime. However, to obtain accurate evidence, certain stages are needed. In addition, to make it easier to work, tools are needed *forensic.* in this study the author will also use *autopsy* and *forensic editing* tools where the tools used to complete the processing are carried out. In this study, researchers used the *Generic Computer Forensic Investigation Model investigation model (GCFIM).* In this study, the researcher also used the data mining *term frequency* method, where the method was used to assist the investigation process in determining documents containing cases that had

IV. RESULT AND DISCUSSION

A. Scenarios Case

Scenarios case made by the author: DIY Regional Police Narcotics Unit managed to capture 1 suspect with an official name AW (21) who was suspected of being a drug user of methamphetamine - methamphetamine suspects were arrested by officers at a village on Jalan Magelang, Yogyakarta. From the hands of the suspect found several kinds of evidence in the form of methamphetamine, two packages of shabu-shabu weighing 7 grams, one *smartphone* Android and one laptop.

B. Collection of Evidence

Goods obtained by the police are as follows:

1) One smartphone Android Lenovo A369i.
2) One laptop Dell Inspiron 8N9I.
3) 7gr Species of methamphetamine drug

C. Specific Evidence

Two smartphones are thought to be a tool for conducting drug trafficking transactions. Here are the specifications of both smartphones:

1) Lenovo A369i
2) OS Android 4.2.2 Jelly bean

Lenovo A369i is an Android-based smartphone with being powered by a Cortex-A7 Dual-core 1.3 GHz processor. *smartphone* This has been *rooted* and has a display with Capacitive touchscreen type, Size 4.0 inches (~ 57.4% screen-to-body ratio), Resolution 480 x 800 pixels (~ 233 ppi pixel density) s*martphone* This is also equipped with a 2 MP camera, 4 GB internal memory, 512 MB RAM.

D. Research Stages

Process of investigating evidence using digital forensic *Generic Computer Forensic Investigation Model (GCFIM) investigation model*. The following is an explanation of each step in the GCFIM investigation model.

1) Pre-Process: Preparation before starting an investigation such as a letter of approval from legal authorities, preparation of equipment to be used, and other preparations. Things that must be prepared and possessed by forensic analysis and investigators: Administration of investigations, digital cameras, stationery, numbers, measuring scales, agency labels, and blank sticker labels, receipt forms for evidence.

2) Acquisition & Preservation: Identification, acquisition, collection, sending, storing and securing data for later analysis at a later stage. Grooves do: Identify handling of evidence at the scene, Preserving (maintaining and securing data), Collecting (collecting data), Reception evidence, Confirming (sets of data), identification (data analysis)

3) Analysis: The main stages in forensic investigations. Analysis is carried out on data found to identify crimes that have occurred and find perpetrators. carried out after data collection where smartphone data is extracted and collected so as to obtain information - information needed and use tools to perform image data and data backup. Next, analyze the data and backup data obtained from the test results. Flow taken: Investigation to get digital data in accordance with investigation, Analyzing, Recording, and TF-IDF method process this process helps determine evidence, where this method is a weighting method, where this method can determine the word according to the investigator is a word that can make support to facilitate and strengthen the investigator to determine the suspect and the new suspect from the text evidence. Where the process of using this method requires keywords to facilitate investigators and research in determining evidence.

4) Presentation: The results of the analysis are then documented and presented to the authorities.

5) Post Process: The final stage in the investigation process. All physical and digital evidence is returned to the authorized party to store it. Then a review of the process that has been passed has been carried out in order to make improvements and improvements to subsequent investigations.

E. Hardware Research

Tools (hardware) used in this study are using 2 laptops used during the study. Laptop specifications are as follows: Dell Inspiron N4050, Intel (R) Celeron (R) CPU B815 @ 1.60GHz, Ram 2 GB, Storage Hard Drive 320 GB, and Windows 10 64bit and Toshiba.

Software In this study researchers used mobile forensic tools to perform forensic processes against digital evidence in the form of Lenovo A369i android smartphone.

F. Discussion of Results

This research scenario refers to actions of cybercrime carried out by the suspect. Because AW suspect conducts drug transactions with the help of telecommunications equipment in the form of a cellphone (smartphone). From the suspect's cellphone will be obtained, in the form of SMS, a call log that is likely to be a perpetrator having a conversation with the drug dealer. In this case scenario the suspect also carried out the process of transferring images / photos via chat messages WhatsApp, and the suspect also carried out deletion of one of the images on the cellphone. From the evidence obtained, the authorities handed over evidence to the team digital forensic to conduct an analysis to obtain accurate evidence stored therein.

Write Blocking is a security measure for evidence that is carried out after the investigation process; steps are taken because Write Blocking is done so that there is no data exchange that is accidentally done.

Imaging Data is a process of acquisition from a single file or a storage media device that contains complete contents with its structure, which is then multiplied / multiplied by the exact same / perfect content, and structure of the original without any difference in size as a bit. Imaging data is carried out with the aim of maintaining data security from existing evidence.

The FTK Imager is used to make it easier to check external memory and internal memory from the evidence. Checking is carried out on the image data from the internal memory of the available evidence, the files in the internal memory will be separated according to the type of process carried out by the smartphone. Then Extracting Image Using Autopsy

Triage Forensic is the initial process of investigative analysis using forensic editing tools, where this process is carried out while the smartphone is still alive, the installation of mobiledit is not too difficult. Mobiledit requires USB debugging mode enable on mobile. Mobiledit will automatically install a small application on a cellphone called forensic connector.

CONCLUSION

This study has satisfactory results and shows the implementation of the platform tools used. Identification is done by collecting evidence from a smartphone and proceeding with TF-IDF analysis.

1) This study refers to one of the Generic Computer Forensic Investigation Model (GCFIM) investigation models in the mobile forensic process in handling cases and researchers use the basic digital forensic procedures by following the existing Standard Operating Procedure (SOP)

2) All tools that are used run well, but for *mobiledit tools* by themselves install the connector application to

connect the cellphone to a laptop so that the evidence can be investigated. For tools autopsy and FTK Imager does not require tools on a smartphone is, of the three *tools* used can both meet the needs of *tools* that are more

3) For the extraction of files of evidence that has been removed, the process of analysis of cell phone use way manual extraction with image-making
4) Process that takes a long time is the process *imaging* where this process is carried out to obtain the overall data from the evidence.
5) Forensic process carried out in this study was not on *instant messenger* (WhatsApp, BBM, Line, etc.)
6) Application of word weighting method with TF-IDF algorithm, get accurate results.

ACKNOWLEDGMENT

Thanks to the Lecturer who has guided and provided their knowledge so that we can complete this paper, and to our parents who have provided support and encouragement so that we are always motivated to complete this paper.

REFERENCES

[1] ACPO, [Online] Available at: https://pacekonathyo.wordpress.com/2013/11/12/penanganan-barang-bukti-forensik-digital/Di akses pada tanggal 22 Agustus 2017

[2] Ariyanto, "Penggolongan program sinetron berdasarkan opini masyarakat di twitter dengan cosine similarity", Thesis Teknik Komputer, Universitas Gadjah Mada, Yogyakarta, 2016.

[3] Eneyunianto, [Online] Available at: https://pacekonathyo.wordpress.com/2013/11/12/penanganan-barang-bukti-forensik-digital/, 2017

[4] Hariyadi Dedy, "Analisis Dugaan Saksi dengan Barang Bukti Digital Blackberry Massanger Menggunakan Metode Term Frequency dan Analisis Triadic", Tesis Teknik Informatika, Universitas Islam Indonesia, Yogyakarta, 2016.

[5] Hius Jurnalis J, Jummaidi Saputra, dan Anhar Nasution, "Mengenal Dan Mengantisipasi Kegiatan Cybercrime Pada Aktifitas Online Sehari Hari Dalam Pendidikan, Pemerintahan Dan Industri Dan Aspek Hukum Yang Berlaku", Universitas Ubudiyah Indonesia, Banda Aceh, 2014.

[6] Hongying. J, " Research of Blind Forensics Algorithm on Digital Image Tampering", Computer college of China West Normal University, China, 2014.

[7] Hoog, *Android Forensics*. 1st Ed., Waltham, MA, USA: Syngress, 2011.

[8] Jocom Nekie, "Peran Smartphone Dalam Menunjang Kinerja Karyawan BankPrismadana (Studi Pada Karyawan Bank Prismadana Cabang Airmadidi)," *Journal "Acta Diurna"*, vol.I, no.I, 2013

[9] Karimayasa, O dan Mahendara. D., "Implementasi *vector space model* dan beberapa notasi metode TF-IDF pada sistem temu kembali informasi," *Jurnal elektronik ilmu komputer* Universitas Udayana, vol. 1, no.1 , 2012.

[10] Kepolisian Republik Indonesia, "Lampiran Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 6 Tahun 2010 Tentang Manajemen Penyidikan Bagi Penyidik Pegawai Negeri Sipil". POLRI, 2010.

[11] Nana, Naufal, " Two-Step Injection Method for Collecting Digital Evidence in Digital Forensics" , Institut Teknologi Bandung, 2014.

[12] Prabandari Galuh Iswari, "Analisis Mobile Phone Forensic Pada Ponsel Bersistem operasi Android", Skripsi Teknik Informatika, Universitas Islam Indonesia, Yogyakarta. 2015.

[13] Prayoga Dian Fajar, "Mobile Forensik Dalam Menemukan Sms yang telah dihapus pada Handphone Android dengan Menggunakan Algoritma Boyer-Moore". Skripsi Teknik Informatika, Universitas Islam Indonesia, Yogyakarta. 2015.

[14] Safaat H, Nazruddin, *Android Pemrograman Aplikasi Mobile Smartphone Dan Tablet PC Berbasis Android*. Bandung: Informatika, 2011.

[15] Sindhuja dan Trivedi, "Pengelolaan Dokumen Menggunakan metode *cosine similarty* dan metode TF-IDF," *Jurnal elektronik,* 2014.

[16] Thufail Ahmad A, Surya Michrandi, Budhi Irawan, "Analisis Dan Implementasi *Mobile* Forensik Pemulihan Data Yang Hilang Pada *Smartphone* Berbasis Sistem Operasi Android," *International Journal*, Universitas Telkom, 2014.

[17] W. Janes W., *"Guidelines on Cell Phone Forensics"*, NIST, May, 2007.

[18] Widyawati, "Analisis Forensika Digital Pada Blackberry Untuk Mendukung Penanganan Kasus Cybercrime Menggunakan Smartphone". Skripsi Teknik Informatika, Universitas Gunadharma, Jakarta. 2009.

[19] Williams, Janet, *Panduan Praktik Baik ACPO Untuk Bukti Digital*. Buku elektronik Metropolitan Police Service. Version 05, 2011.

[20] Yusoff Yunnus, Roslan Ismail, and Zainuddin Hassan, "Common Phases of Computer Forensics," *International Journal of Computer Science & Information Technology (IJCSIT)*, College of Information Technology, Universiti Tenaga Nasional, Selangor Malaysia. 2011.