International Journal of Cyber-Security and Digital Forensics (IJCSDF) 8(3): 232-240
The Society of Digital Information and Wireless Communications (SDIWC), 2019 ISSN: 2305-0011

Cloud Forensics Investigation in Cloud Storage Using IDFIF V2 Method

Ahmad Muhammad Ridho[1], Nuril Anwar[2]
[1]Teknik Informatika, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2]Teknik Informatika, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
(ahmad1400018150@webmail.uad.ac.id, nuril.anwar@tif.uad.ac.id)

ABSTRACT

Virtual storage through the cloud system has continued to grow since 2014.[1] Google Drive is a storage service created by Google on April 24, 2012, with a storage service of 15GB which is provided free of charge and can be added with certain payments. As of March 2017, Google Drive has more than 800 million active monthly users with a total of several billion users. But on the other hand, not a few people are also abusing the Google Drive application for acts of fraud or crime. The handling of crimes involving digital devices needs to be emphasized so that they can assist in the judicial process. With the Integrated Digital Forensics Investigation Framework v2 method, it can be a way for digital forensics to get digital evidence on smartphones.

KEYWORD

Cloud Storage, *Forensics, Mobile Forensics*, IDFIF V2, *smartphone*.

1 INTRODUCTION

Virtual storage through the cloud system has continued to grow since 2014. The data posted on the Gartner website shows the estimated number of cloud users in 2014 was 1.136 million. The number continues to increase until 2016 which reached 1.561 million. In 2017, Gartner estimates that the number will reach 1.8 million or stand at 1.754 million. The upward trend will continue until 2020. Over the next three years, the data research company estimates that there will be cloud users reaching 2.309 million. That is, in 2020 there will be an increase of 555 million users. Meanwhile, in Indonesia most people are familiar with the cloud storage system through several services such as Dropbox, Google Drive, or Apple's iCloud. Although it does not have exact data on the number of users, Google's services are believed to be the best-selling.[2] Google Drive is a storage service created by Google on April 24, 2012, with a storage service of 15GB which is provided free of charge and can be added with certain payments.[3]

Looking at the data comparison of cloud storage users, Google Drive is the storage media application with the most users.[4] Therefore, it is probable that the risk of crime is related to Google Drive storage media. Handling crime cases related to the use of information technology often requires forensics. Forensics is an activity to conduct investigations and establish facts related to criminal incidents and other legal issues. Digital Forensics is a part of forensic science that encompasses the discovery and investigation of material (data) found on digital devices (computers, mobile phones, tablets, PDAs, net-working devices, storage, and the like). [5]

Seeing from problems that occur such as the rise of digital crime cases related to the Google Drive application. So the research was conducted by making a smartphone theft case scenario that is still connected to the victim's Google Drive account by implementing Mobile Forensics on Google Drive cloud storage with the Integrated Digital Forensics Investigation Framework version 2 in order to help obtain digital evidence and is expected to provide solutions to several problems in digital crime cases related to the Google Drive application.

Integrated Digital Forensics Investigation Framework version 2 (IDFIF v2). Integrated Digital Forensics Investigation Framework version 2 (IDFIF v2) is the latest framework that has been developed so that it is expected to become a standard investigative method for investigators because IDFIF v2 has the flexibility in handling various types of digital evidence. [6]

2 LITERATURE REVIEW

2.1 Digital Forensics

Digital Forensics is an activity to conduct investigations and establish facts relating to criminal incidents and other legal issues. Digital Forensics is a part of forensic science that encompasses the discovery and investigation of material (data) found on digital devices (computers, mobile phones, tablets, PDAs, net-working devices, storage, and the like). [5]

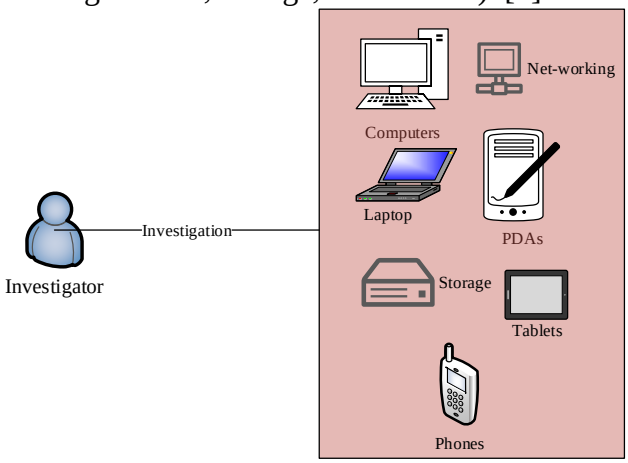


Figure 1. Digital Forensics Illustration

In figure 1 explains about the digital forensic illustration. Starting from the investigator investigating data found on digital devices such as computers, mobile phones, tablets, PDAs, net-working devices, storage, and the like.

2.2 Mobile Forensics

Mobile phone forensics is the science that carries out the process of recovering digital evidence from mobile devices using methods that are suitable for forensic conditions. [7]

2.3 Cloud Storage

Cloud Storage is a paradigm where information is permanently stored on the server and temporarily stored on the user's computer (client) including desktops, tablet computers, notebooks, wall computers, handhelds, sensors, monitors and others. How it works Cloud Storage is the user can access files, data, programs and services in a web browser via the internet provided by the ISP. Users only pay for computing resources and services used. [8]

2.4 Google Drive

Google Drive application is Google's online storage service that was launched on April 24, 2012. Google Drive is a data storage application that can be used anywhere and anytime with a computer, laptop or cellphone connected to the internet network. Google Drive application provides a free storage capacity of 15 GB and is not only used for storage, but is also used for sharing documents and makes it easy to edit documents that have been received from other parties. [9]

2.5 Evidence

Evidence is a very important part in a crime case. From this evidence the investigation team and forensic analysts can uncover the case in complete chronology. [10]

2.6 Oxygen Forensics Suite

Oxygen Forensic Suite provides general information about the smartphone and the network the device is connected to. This tool can restore all contacts, SMS and MMS messages, and user files. Likewise, all memos, alerts, and schedules that are not deleted, which are specified in the calendar and also the agenda must be extracted. This tool can get all e-mail messages stored on the cellphone. In addition, Oxygen Forensic Suite can collect event logs for up to 30 days. Based on the event log and the corresponding date and time, the timeline feature organizes and sorts all SMS and MMS messages, e-mail and internet connections. [11]

2.7 MOBILedit

MOBILedit is a forensic tool that allows investigators to logically obtain it. This tool uses several connectivity mechanisms, mainly wireless connectivity rather than similar devices. This software is good enough to be used to obtain telephone system information and other information such as contacts and text messages.[12]

2.8 IDFIF V2

The Integrated Digital Forensic Investigation Framework v2 (IDFIF) is the latest framework developed so that it can be used for the smartphone investigation process. In general, the stages of the investigation process of digital evidence, whether computers or smartphones, have 4 (four) main stages, namely preparation (pre-process), if the crime scene (proactive process), examination of evidence in digital forensics (reactive process) laboratories and

report on the results of examination of digital evidence (post-pocess). The results of the investigation in the process of handling the evidence that has been obtained because the framework has the flexibility in handling digital evidence found by the crime scene. [6]

3 METHODOLOGY

In this study, the stages of case scenarios are conducted to try to implement the IDFIF V2 framework for the cloud forensic investigation process. The case scenario aims to test the IDFIF V2 framework process on smartphone evidence. The following is a picture of case scenarios and stages of research.

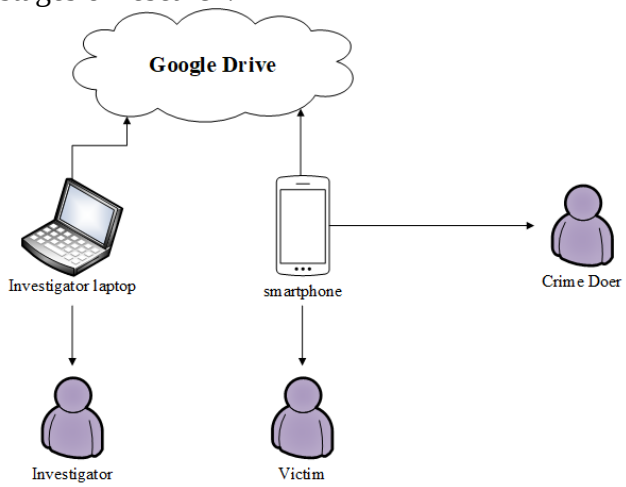


Figure 2. Case scenario

In Figure 2 explained that the victim's smartphone was stolen by the perpetrator. The perpetrator took the victim's smartphone while the smartphone is online and the smartphone is still connected to the victim's Google Drive account. The perpetrator was caught a few days after selling the victim's smartphone. The smartphone was confiscated by an officer at the place of the buyer who accidentally bought the stolen item. Then the smartphone is handed over to the investigator to be analyzed and later will be used as evidence in the trial process. After the investigator analyzes the victim's smartphone evidence, the victim entrusts his Google Drive account to be opened on the investigator's laptop to authenticate the results of the analysis between the smartphone and laptop so that it is valid and can later be presented in the form of reporting the results of the analysis that can be used as a reference to prove the perpetrators of theft . After the case scenario is known it will be implemented with the IDFIF v2 stage. The following is a picture of the stages of IDFIF v2.

Figure 3. Stages of IDFIF V2

In Figure 3 is the result of research that has several stages in the handling of digital evidence, namely:

a. Preparation
   Is a preparation that must be done to carry out an investigation in the handling of digital evidence starting from the processing of the crime scene to making the final report.
b. Incident Response
   It is an activity carried out at the crime scene with the aim of securing existing digital evidence so that it is not contaminated by other things.
c. Laboratorium Process
   After handling digital evidence at the scene of crime, then at this stage it is a process of analyzing data on evidence that has been obtained previously so that it can be found the type of crime that has occurred.
d. Presentation
   Is the final stage in the digital investigation process. At this stage is the process of making a report related to the results of the analysis carried out in the previous stage and ensuring that each process is carried out in accordance with applicable law.

   Conclusion is the conclusion of all stages that have been carried out in this research process from the process of handling physical evidence and obtaining digital evidence in the form of a photo file which contains information on the date, time and coordinates of the location where the photo was taken. The data can be analyzed whether it is in accordance with the victim's report and there is a crime, up to the last stage which is to make the final report so that it can be presented in court to strengthen the evidence of a crime.

4 RESULTS AND DISCUSSION

At this stage it starts with a smartphone theft case scenario where the Google Drive account is still connected. After the perpetrators

are caught and smartphone evidence is obtained, the investigator will identify and analyze smartphone evidence to obtain digital evidence by acquiring and extracting processes. The stages of investigation and evidence analysis use the application of the IDFIF v2 method to resolve theft cases in this study. The stages used in the investigation can be seen in Figure 3

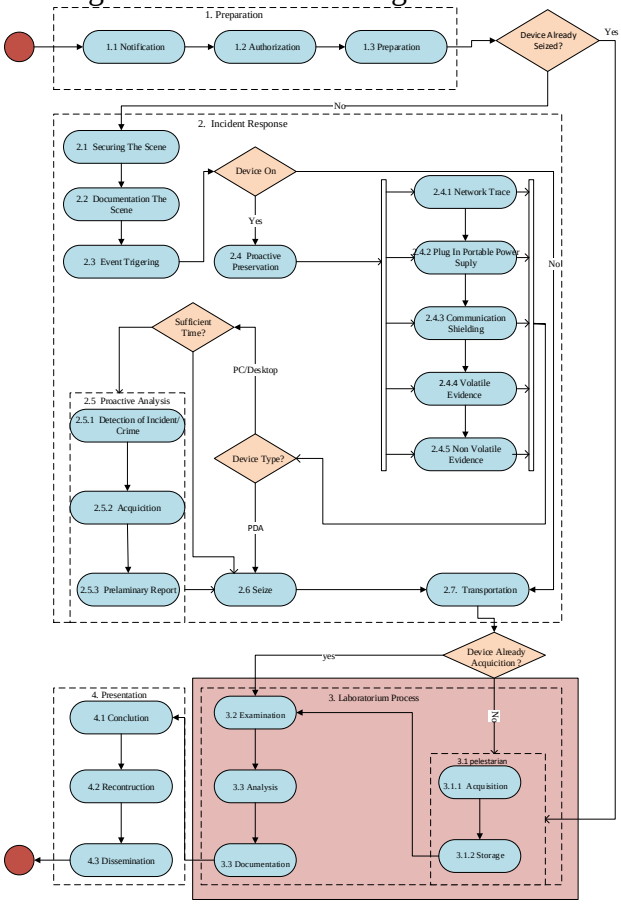


Figure 4. Stages of IDFIF V2 investigation

Figure 4 is the IDFIF v2 stage of the investigation, there are 4 main stages namely Preparation, Incident response, Process Laboratory and Presentation which will be implemented in this study. But the writer will focus more on the third stage, the Laboratory Process stage.

4.1 Preparation: is the initial stage of the digital evidence investigation process, especially in the investigation of notebooks and smartphones. At this stage various preparations were made in the investigation process both from the equipment and also the necessary documents. This stage is divided into 3 sub-stages:

a. Notification: The victim reported a crime that was a case of smartphone theft that was experienced by the authorities, namely law enforcement, so that it was followed up in order to carry out an investigation process. In this case the victim reported the stolen property, the time and location of the theft. This reporting is important because the information collected at this stage can determine the next step in the investigation.
b. Authorization: The authorities are the law enforcers cooperate and process permits to the surrounding community and victims to get the right of access to evidence and legal status.
c. Preparation: The authorities, namely law enforcement, prepare all the needs and needs in the investigation process to start from carrying out a search in order to obtain evidence, investigation equipment to support the investigation activities, hardware and software.

4.2 Incident Response: is the initial stage of the investigation process. Because the whereabouts of the perpetrators of the theft are known, the investigator goes to the place where the perpetrators are known to be further processed and carry out arrest procedures for the theft of the smartphone. The stages of incident response are as follows:

a. Securing the scene: The investigator carries out the process of safeguarding and securing the crime scene so that it is in real condition as seen and discovered by officers who carry out the first act at the scene so that the evidence is not lost, undamaged and unchanged such as reduction or addition and the location and whereabouts of the evidence do not change so as not to affect the investigation process so that others cannot be denied.
b. Documentation the scene: Investigators document at the scene by taking photos of the crime scene and evidence found at the crime scene. Evidence found as in table 1

Table 1. Evidence

Name of evidence	Figure	Information
Stolen victim's smartphone		The smartphone is rooted, and not in screen security mode

Table 1 is evidence that can include smartphone evidence found at the crime scene and all supporting evidence at the crime scene without directly touching the evidence so that the investigator's fingerprint is not traceable to the evidence, and so as not to damage the authenticity of the evidence.

c. Event triggering: If the previous stage of securing the scene where the investigator secures the crime scene has been carried out, at this stage the investigator carries out the initial analysis process for a theft that occurred at the crime scene and looks for the cause of the crime at the crime scene so that the investigator can conclude while the type of crime was committed in the future in further processing in the digital forensic laboratory. The specifications of the evidence of the perpetrators are in Table 2

Table 2. Evidence Specifications Table

Evidence	Model Number	Imei	OS version
Smartphone	CHM-001	866778020201319	5.1.1

d. Proactive preservation: Investigators secure Smartphone evidence found at the crime scene so that the evidence is maintained for the integrity of the data contained in it until analysis in the digital forensic laboratory.
   1) Plug in portable power supply: Investigators safeguard digital evidence on smartphones by charging the smartphone evidence using a portable power supply to maintain the condition of smartphone evidence on "condition" to the digital forensic laboratory for further investigation to obtain information about crime evidence fraud.
   2) Communication shielding: at this stage the investigator secures smartphone evidence found at the crime scene by interrupting the network of the smartphone so that it does not experience data changes on the evidence.

e. Seize: The investigator seized the evidence that was found at the crime scene.

f. Transportation: Investigators carry out the procedure of transferring evidence that is a smartphone device from the crime scene to a digital forensic laboratory for further investigation. In this process, the smartphone must be kept and stored safely to the digital forensic laboratory so that the smartphone evidence remains in good condition and maintained its condition and authenticity.

4.3 Laboratorium Process: is the stage and the core discussion of the smartphone investigation process. In Figure 4 below are the stages of the laboratory process.

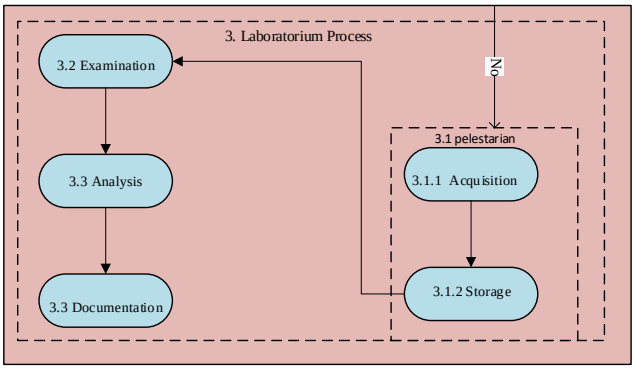


Figure 5. Stages of Laboratory Processes

In Figure 5 the evidence in the form of a smartphone has been obtained in the previous process. Then a series of stages of activities will be carried out to obtain evidence related to the crime that occurred. This stage is divided into several stages, namely:

a. Preservation: Investigators carry out the process of securing smartphone evidence. The condition of the smartphone when in the process of acquisition must be disconnected from existing data communications.
   1) Acquisition: Investigators take digital evidence from smartphone devices found at crime scenes. In this process, imaging is done using tools that are MOBILedit and Oxygen Forensics Suite tools as a tool for the process of copying data on a smartphone as well as a way to secure evidence so that the data we analyze can be compared with the original. With these tools it is possible to do all file imaging inside a smartphone but to get more access rights the smartphone must be in a root state, besides that the type and vendor of the smartphone can affect the access rights and exploration restrictions on a smartphone that is already in a root state.

2) Storage: Investigators prepare storage in the investigator notebook directory that has been determined to store data backups of digital smartphone items that have been backed up. In this study, the investigator has prepared a special directory to store digital evidence, namely the disk F: \ on the investigator's notebook. The contents of the form of digital evidence will be stored in a safe and sterile place, to ensure the digital evidence obtained does not experience changes, because if the digital evidence has a slight change it will change the results of the investigation.

b. Examination: Investigators conducted an examination to find evidence related to the case being handled on the stolen victim's smartphone device. For the examination of digital evidence on smartphones by exploring digital evidence in order to find evidence that is a photo file in which the time and location are listed on the stolen victim's smartphone. For the next stage, exploration of the device, namely:

1) Explore smartphone digital evidence with Oxygen Forensics Tools

At the exploration stage of digital smartphone evidence finding key files in the form of photo files, to find the location of photo files on smartphone devices can be seen in Figure 5

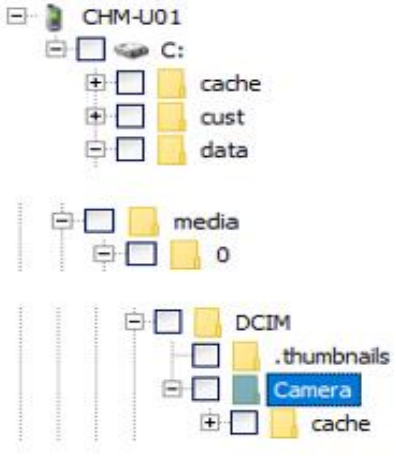


Figure 6. Location of digital evidence files

Figure 6 is the location of the photo file, contained in C: \ data \ media \ 0 \ DCIM \ Camera's internal memory, in the form of a photo file containing information on the location and time when the perpetrator sold the victim's smartphone to someone else.

2) Explore smartphone digital evidence with MOBILedit Tools

At the exploration stage of digital smartphone evidence, namely finding key files in the form of photo files, to find the location of photo files on smartphone devices can be seen in Figure 6

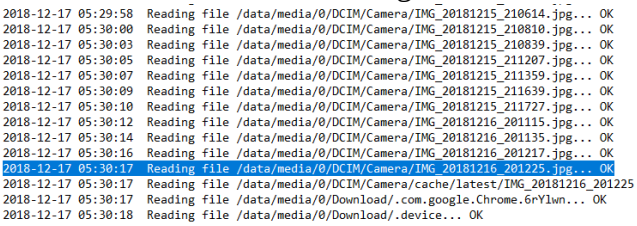


Figure 7. Location of digital evidence files

In Figure 7 is the location of the evidence file in the form of a photo file contained in C: \ data \ media \ 0 \ DCIM \ Camera's internal memory. In this MOBILedit tool after the imaging process it will automatically automatically become a PDF file, and the search trace will be written on Notepad.

c. Analysis: At this stage the investigator conducts a study related to cases of smartphone theft and digital evidence obtained. Then after the evidence is acquired, the investigator conducts an extraction and analysis in order to obtain detailed information on the evidence obtained.

1) Data analysis via Oxygen Forensics tools

At the stage of extracting and analyzing smartphone evidence through Oxygen Forensics tools, the evidence file, which is a photo file, contains information about the time and location where the information is very important in order to track the state of the smartphone changing hands. In Figure 7 below is a display after the acquisition process.

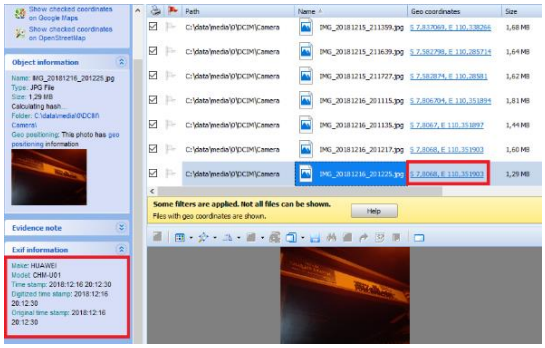


Figure 8. Display After the Acquisition Process

In Figure 8 is a display on the Oxygen Forensics tool where there is important information that is the time and location coordinates when the perpetrators carry out the sale of the stolen smartphone to the buyer. In Figure 8 below is a picture showing the coordinates of the location with maps in the Oxygen Forensics tool.

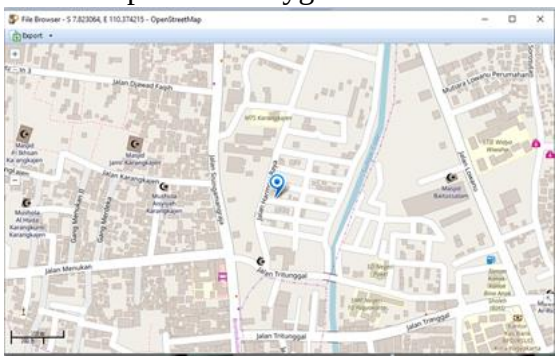


Figure 9. Display Location Through Maps on Tools Oxygen Forensics

Figure 9 shows the location of the photo file taken, with this Oxygen Forensics tool the investigator can see the coordinates and can see the location through the existing maps feature. By looking at the location, the investigator can ascertain the condition of the stolen property at that time so that it can be used as a reinforcement that the perpetrators have actually committed a theft crime..

2) Data analysis via the MOBILedit tools

At the stage of extracting and analyzing smartphone evidence through the MOBILedit tool, it cannot display the location with maps, but the coordinates and time are still traceable. The following picture 9 is the result of the acquisition process with MOBILedit tools.

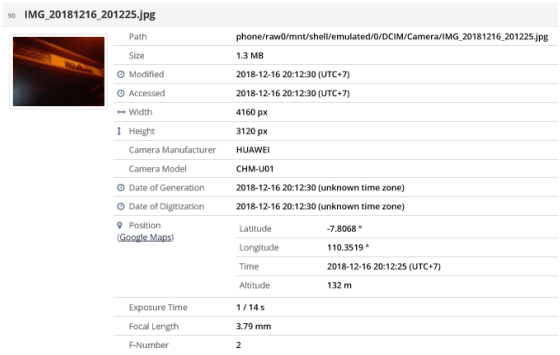


Figure 10. Display After the Acquisition Process

Figure 10 shows the MOBILedit tool in the reporting data section after the device has been acquired. The picture above shows the time when the photo was taken and the coordinates of the location where the picture was taken by the thief. Time and location information like this is very important to support the evidence that the perpetrators actually committed theft. In Figure 10 below is a picture showing the coordinates of the location with maps in the MOBILedit tool

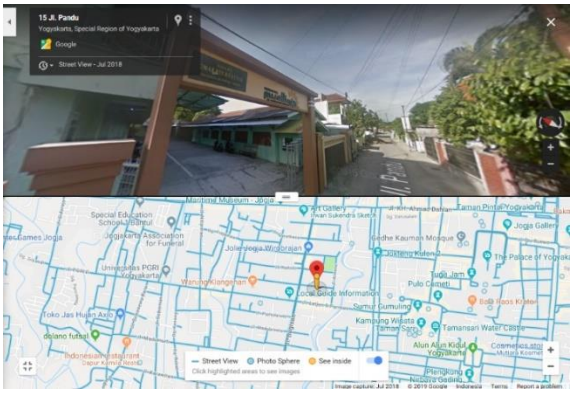
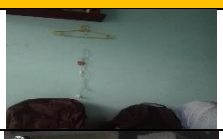


Figure 11. Display Location Through Maps on MOBILedit Tools

In Figure 11 is a picture of the location of the photo file taken, with this MOBILedit tool the investigator can see the coordinates and can see the location through the existing maps feature.

After finding out the location of the evidence, the investigator then authenticated the photo data on the victim's smartphone and the victim's Google Drive account which was opened in the investigator's notebook. Following the results of matching data and can be seen in table 3

Table 3. Matching Smartphone and Google Drive Data

File name	Photo	Smart phone	Google Drive
IMG_20181126_144223		v	v
IMG_20181126_145136		v	v
IMG_20181201_113853		v	v
IMG_20181215_210839		v	v
IMG_20181215_211207		v	v
IMG_20181215_211727		v	v
IMG_20181216_201225		v	v

In Table 3 above is the result of matching photo file data that is on the victim's stolen smartphone with a photo file entered on the victim's Google Drive account that has been opened on the investigator's notebook.

d. Documentation: After the Analysis phase of digital smartphone evidence found at the crime scene, the next stage the investigator assembles all data and information found at the analysis stage to be processed as evidence in a crime case that has sufficient information to be submitted to parties who have authority in the field of law. Data and information are presented in the form of information that can be understood and supported by evidence in accordance with sufficient and acceptable crime.

4.4 Presentation: is the final stage of the investigation process. At this stage the handling of evidence that has been done before, securing evidence in a safe place and the review stage in the investigation of evidence of criminal acts that have been carried out for improvement in the process of further investigation.

a. Conclusion: evidence and information obtained in the investigation process by the investigator in the form of physical and digital evidence. Digital evidence obtained at the laboratory process stage of the investigator found indications of digital evidence in the form of a photo file on a smartphone device that contained information on the location and time when the thief sold the stolen smartphone.
b. The smartphone must be rooted if you want to get the evidence file. If the smartphone is not rooted, the extraction process will continue but will not get any results or the data is empty as in table 4

Table 4. Comparison of Tool Results

	Oxygen Forensics	MOBILedit	Oxygen Forensics (unroot)	MOBILedit (Unroot)
Contact	v	v	-	-
SMS conversation	v	v	-	-
Email	v	v	-	-
Call	v	v	-	-
Photo	v	v	-	-
File Audio	v	v	-	-
File Video	v	v	-	-
Document	v	v	-	-
Password	v	v	-	-
GPS Location	v	v	-	-
Web Browsing History	v	v	-	-
Web Search History	v	v	-	-
Bookmarks	v	v	-	-
Drive	v	v	-	-
Cookies	v	-	-	-

Table 4 above explains the comparison between smartphones that are already in the root state and not in the root state, and explains the comparison of the results between the Oxygen Forensics tools and the MOBILedit tools..

c. Reconstruction: At this stage the investigator reconstructs based on the findings of the investigative analysis carried out so that the perpetrators' activities can be identified in committing the theft of a crime on the victim's smartphone.

d. Dissemination: Furthermore, at this final stage is the process of recording the investigation process and the record can be disseminated to other investigators, so that if another researcher or investigator gets a similar case, this investigation process can become a reference in the analysis process forensic investigation of an android smartphone.

5 CONCLUSION

Evidence and information obtained in the investigation process by investigators in the form of physical and digital evidence. Digital evidence obtained at the laboratory process stage of the investigator found indications of digital evidence in the form of a photo file on a smartphone device that contained information on the location and time when the thief sold the stolen smartphone. Digital evidence data on a smartphone is compared with data available on the victim's google drive through the investigator's notebook. Smartphone evidence must be rooted if you want to get the evidence file. If the smartphone is not rooted, the extraction process will continue but will not get any results or data is empty.

REFERENCE

[1] A. N. Jaber, Mohamad Fadli Bin Zolkipli, Mazlina Binti Abdul Majid, and Nusrat Ullah Khan, “A Study in Data Security in Cloud Computing,” no. I4ct, pp. 367–371, 2014.

[2] Moch Prima Fauzi, “2017, Pengguna Cloud Diperkirakan Mencapai 1,8 Juta,” Jakarta, 2017.

[3] B. Y. Dhiyaul Abrar, Mira Maisura, “PENGARUH PENGGUNAAN CLOUD COMPUTING (GOOGLE DRIVE) TERHADAP KINERJA TENAGA PENGAJAR DI SEKOLAH MTsS MON MALEM BLANG BINTANG,” vol. 1, no. April 2012, pp. 134–142, 2017.

[4] A. Naser, Mohamad Fadli Zolkipli, Mazlina Abdul majid, and Shahid Anwar, “Trusting Cloud Computing for Personal Files,” pp. 488–489, 2014.

[5] B. Raharjo, “Sekilas Mengenai Forensik Digital,” *Sekilas Mengenai Forensik Digit. J. Sosioteknologi Ed.*, vol. 29, no. 12, pp. 384–387, 2013.

[6] Ruuhwan, I. Riadi, and Y. Prayudi, “Penerapan Integrated Digital Forensic Investigation Framework v2 (IDFIF) pada Proses Investigasi Smartphone,” *J. Edukasi dan Penelit. Inform.*, vol. 2, no. 1, pp. 1–8, 2016.

[7] A. Yudhana, R. Umar, and A. Ahmadi, “Akuisisi dan analisis google drive pada smartphone android,” 2017.

[8] I. Ar-Razy, R. Kridalukmana, and E. D. Widianto, “Implementasi Cloud Storage Menggunakan OwnCloud yang High-Availability,” *J. Teknol. dan Sist. Komput.*, vol. 4, no. 2, pp. 209–214, 2016.

[9] O. Setya and D. Puspasari, “Penggunaan Aplikasi Google Drive Sebagai Penunjang,” *Ilmu Sos.*, p. 15.

[10] Ruuhwan, I. Riadi, and Y. Prayudi, “Analisis Kelayakan Integrated Digital Forensics Investigation Framework Untuk Investigasi Smartphone,” pp. 265–274, 2016.

[11] S. Mohtasebi and A. Dehghantanha, “Smartphone Forensics : A Case Study with Nokia E5-00 Mobile Phone,” vol. 1, no. 3, pp. 651–655.

[12] A. Fadlil, “Evidence Gathering and Identification of LINE Messenger on Android Device,” vol. 16, no. 5, pp. 201–205, 2018.