Plagiarism Checker X Originality Report

Similarity Found: 19%

Date: Thursday, July 28, 2022
Statistics: 315 words Plagiarized / 1634 Total words
Remarks: Low Plagiarism Detected - Your Document needs Optional Improvement.

International Journal of Computer Applications (0975 – 8887) Volume 175 – No. 26, October 2020 40 Digital Evidence Identification of Android Device using Live Forensics Acquisition on Cloud Storage (iDrive) Tri Rochmadi Department of Information Systems Alma Ata University Yogyakarta, Indonesia Yanuar Wicaksono Department of Information Systems Alma Ata University Yogyakarta, Indonesia Nanda Dhea Nisa Department of Information Systems Alma Ata University Yogyakarta, Indonesia ABSTRACT The use of the internet cannot be separated in the era of the industrial revolution 4.0

because all lines are experiencing a digital transformation. Digital transformation cannot be separated from cloud computing, so cloud computing is increasingly diverse and widely used, especially in cloud storage. Cloud storage is widely used both on computers and smartphones and several incidents have shown it is used as a crime. So there is a need for research on how to first identify digital evidence on an Android smartphone, because Android is increasingly being used.

By using experimental research, a series of forensic investigations were able to identify digital evidence on an android smartphone with live forensic acquisitions on partitions, applications, and the android ram process that was still on. General Terms Digital Forensics, Mobile Forensics Keywords Live Forensics, Android Forensics, Cloud Storage Forensics 1. INTRODUCTION The industrial revolution 4.0 is inseparable from the internet, which is a means of socializing and making transactions, so the term digital transformation emerged.

Digital transformation occurs because everyone has started to switch to using connected computers and networks called the Internet of Things [1]. Internet of Things is also inseparable from the use of Cloud Computing because it can be accessed anytime and anywhere, thus saving server maintenance costs and time [2]. This convenience is also encouraged because the use of smartphones has increased significantly from year to year, even according to Arne Holst via Statista [3] estimates that by 2024 the traffic data per month will be able to reach 20 GB per smartphone device as shown in Figure 1.

However, the use of smartphones is generally limited to storage capacity, so the use of cloud storage over time is also increasing as a solution to storing data that can be deleted from smartphones at any time when it has been uploaded to cloud storage. Behind the advantages or advantages of using cloud storage, it also raises a new problem, namely, cloud storage is used to store illegal content files such as pornography, pirated files or can also be used to share files that contain large and random transaction instructions to deceive or disguise the information on it. Figure 1.

Traffic Data Smartphones So there is a need for research to carry out a forensic investigation process on an Android device to look for evidence that can be an indication of the use of cloud storage. 2. RELATED WORK Daryabar in 2016 managed to identify digital evidence on the Mega Cloud on a smartphone with the Android operating system version 4 through user activity from the application and network side [4]. Research in the following year Yee-Yang Teing performed network and memory analysis to find digital evidence on cloud storage called Syncany [5].

Then continue research on Cloudme cloud storage which is installed on smartphones with the Android operating system, which shows that the digital evidence obtained is not as complete as on a computer device. [6]. In 2019, research conducted by Ahmad Bhat managed to find a lot of information found on smartphones with the Android operating system version 8, to analyze digital evidence on cloud Sync and Flip Drive. [7]. Cloud storage analysis also managed to find digital evidence on the Windows operating system with the Adrive cloud storage case study using live forensic acquisition [8]. From some of these studies, the acquisition technique used live forensic acquisition.

This is done by means of an acquisition when the device is still on or on [9]. 3. METHODOLOGY This study used an experimental method, where previously related research was searched. From the literature review is developed to problem formulation and identification of needs to support research. Identification of these needs is also related to scenarios and research simulations. Then proceed to the forensic investigation and reporting process. International Journal of Computer Applications (0975 – 8887) Volume 175 – No. 26, October 2020 41 Figure 2.

Methodology This study used a computer device for acquisition and analysis at the investigation stage. While scenarios and simulations also use a computer device that is used to run Android version 8 embedded in a virtual machine. The software requirements used areas in table 1. Table 1. List of Software Used Software Function Windows 10 Forensic simulations and investigations include digital evidence acquisition and analysis ADB Tool for data acquisition from android to computer. Hex Workshop 6.7 Digital evidence analysis tool. Autopsy 4.11.0 Digital evidence analysis tool. Virtual Box 6.0 Tool for virtualizing android machines from windows Android Oreo Operating system and research object.

BusyBox Application to support the acquisition process KingoRoot Application to support the acquisition process iDrive Cloud storage application of research objects Laron Application to support the acquisition process GameGuardian Application to support the acquisition process 4. EXPERIMENT AND RESULT This research uses experimental methods that are carried out through scenarios and simulations as shown in Figure 3. The simulation is carried out in full via Android by installing iDrive, then carrying out activities on the iDrive by uploading several files.

Figure 3 Case Study Simulation After simulating the use of iDrive on Android, an investigative simulation is carried out from the drafted scenario. The acquisition process begins with the preparation of the Android Debug Bridge (ADB) settings on the computer, then connect the Android device to the computer using the ADB command. Figure 4. Acquisition Process Computers that have successfully connected with Android make live acquisitions using 3 different types of acquisitions.

The first acquisition was a logical acquisition on partition, from this acquisition resulted in an imaging file in the form of a .dd file which will later be analyzed using Autopsy 4.11.0. The second acquisition is a logical acquisition with more specific data or directories using Laron which is intended to retrieve the application database, from which this acquisition produces an imaging file in the form of .db. The third acquisition is by retrieving data from processes that occur in RAM on Android. This acquisition uses the GameGuardian application and the results of the export process are in the form of .txt files and .bin files from a series of processes that occur in RAM. The series of acquisitions fulfilled the acquisition stage procedures stated in SNI 27037: 2014 [10].

Literatur Review Preparation & Identification Scenario & Simulation Investigation Report International Journal of Computer Applications (0975 – 8887) Volume 175 – No. 26, October 2020 42 Figure 5. Procedures SNI 27037:2014 Figure 7. Evidence of File Document The results of the acquisition obtained 3 types of digital evidence, namely .dd files, .db files and, .txt files. From the .dd file analyzed using Autopsy 4.11.0 it proves that on the Android device there is an iDrive installation as shown in the results of the analysis in Figure 6. Figure 6.

iDrive Installation Location From this analysis, the iDrive installation location can be found in the data folder - app - com.prosoftnet.android.idriveonline. These findings were then followed by further analysis using a .db file and digital evidence was found in the form of a document path that was uploaded to iDrive via the application as shown in Figure 7. The results of this analysis, besides finding files in the form of documents with the .doc extension. The file that is meant by the file name is wd-spectools-word-sample-04.doc, also contained information about the time or when the file was in the download folder, which was on August 30, 2020 at 10:34.24.

Meanwhile, in the analysis of the RAM process, it was found that many activities were carried out using the iDrive application. The results of this acquisition resulted in as many as 112 .bin files and 1 .txt file as information from all of them. Figure 8. List Acquisition from proccess RAM From the results of the acquisition, the .txt file shows the location of the iDrive installation location as shown in Figure 9. While the location of the database on the iDrive application is in the /data/user/0/com.prosoftnet.android.idriveonline/ directory as shown in Figure 10. International Journal of Computer Applications (0975 – 8887) Volume 175 – No. 26, October 2020 43 Figure 9. iDrive Installation Location from Database Figure 10.

Database iDrive Location The results of this study, as described above, can identify digital evidence on Android devices from the source object iDrive as in the table below. Table 2. Results Acquisition Proccess Data Source Type of File Acquisition Information ADB Partition .dd imaging results are able to identify the location of the installation Laron Application .db imaging results are able to identify the uploaded file and there is a timestamp Game Guardian Proccess of RAM .txt imaging results are able to identify the application installation location and the database location of the application 5.

CONCLUSION AND FUTURE WORK Based on the results of research with three types of acquisitions, all of which use the live forensic acquisition to identify digital evidence. All the identification results are mutually reinforcing because they both show digital evidence that can be used for initial clues to problem solving. The results of the analysis show that partition acquisition is able to detect the location of application installation while in application acquisition it is able to detect file types and timestamps.

The RAM process can also be used to strengthen the identification of digital evidence that has been found. Further research can be done with the analysis of the data in RAM and with various objects from the most widely used cloud storage.

INTERNET SOURCES:

1% - www.researchgate.net › publication › 329365727
1% - www.sciencegate.app › document › 10
<1% - www.its.ac.id › si › en
<1% - mfg.world.edu › why-are-businesses-experiencing-a
1% - www.researchgate.net › publication › 316172830_Live
<1% - www.researchgate.net › publication › 265295989
6% - www.researchgate.net › profile › Tri-Rochmadi
2% - www.chegg.com › homework-help › questions-and
<1% - cloudstorageadvice.com › what-is-cloud-storage
2% - www.researchgate.net › publication › 301534892_Cloud
2% - www.researchgate.net › publication › 318820450_Cloud
1% - www.coursehero.com › file › 59577455
<1% - www.guru99.com › adb-connect
<1% - students.cs.uri.edu › CSC485 › Week6
<1% - www.coursehero.com › file › 49224905
2% - www.researchgate.net › figure › List-Acquisition
1% - www.coursehero.com › file › 69595183