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.

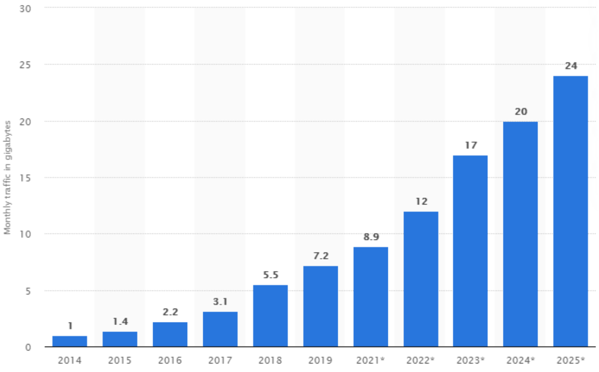


Figure 1. Traffic Data Smartphones

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.

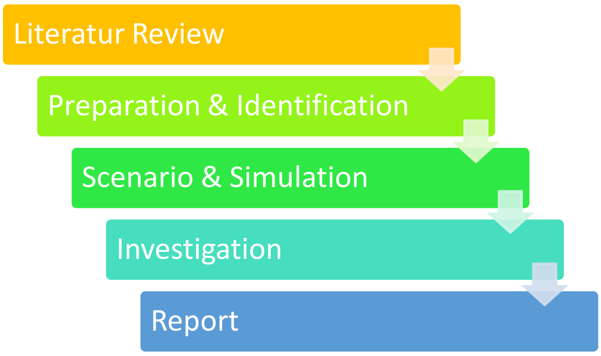


Figure 2. Methodology

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.

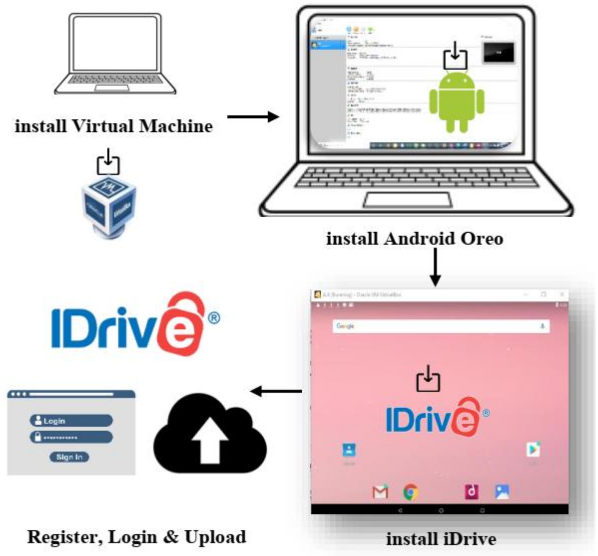


Figure 3 Case Study Simulation

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.

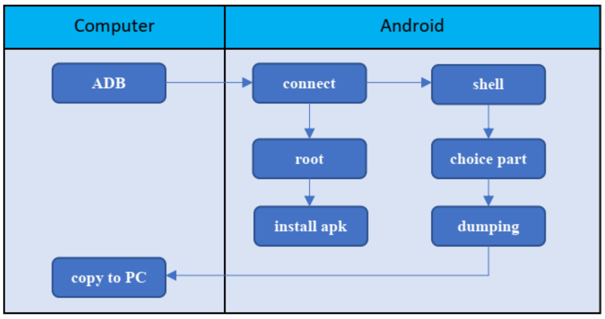


Figure 4. Acquisition Process

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].

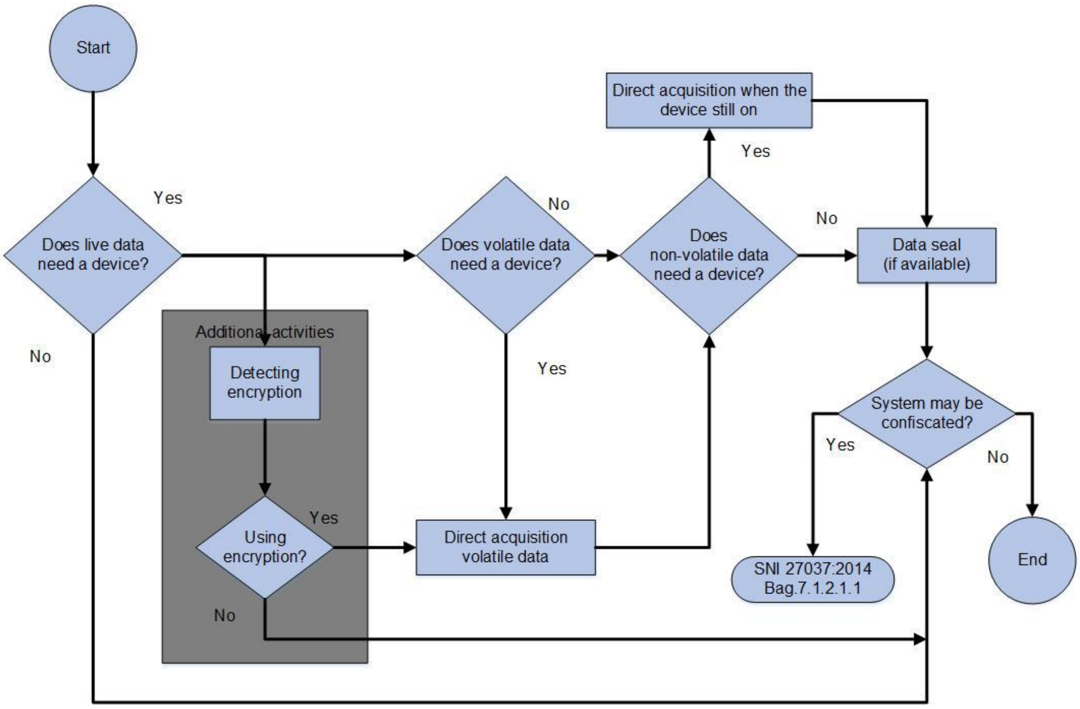
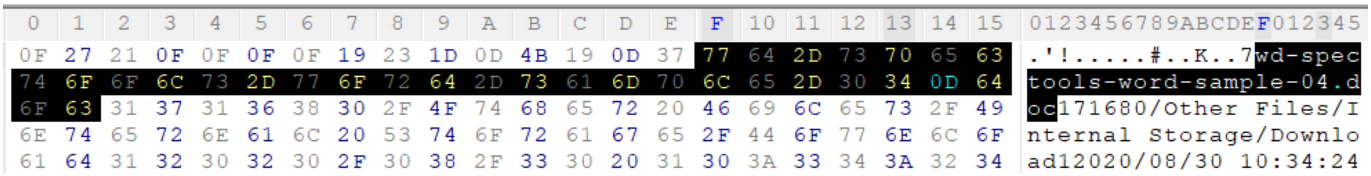

Start
Does live data need a device?
Yes
No
Additional activities
Detecting encryption
Using encryption?
Yes
No
Does volatile data need a device?
No
Yes
Direct acquisition volatile data
Does non-volatile data need a device?
Yes
No
Direct acquisition when the device still on
Data seal (if available)
System may be confiscated?
Yes
No
SNI 27037:2014 Bag.7.1.2.1.1
End

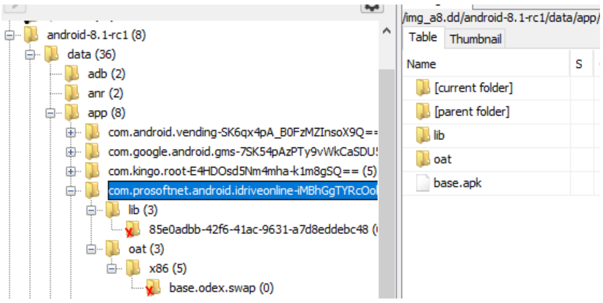
Figure 5. Procedures SNI 27037:2014



```
 0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F 10 11 12 13 14 15   0123456789ABCDEF012345
0F 27 21 0F 0F 0F 0F 19 23 1D 0D 4B 19 0D 37 77 64 2D 73 70 65 63   .'!.....#..K..7wd-spec
74 6F 6F 6C 73 2D 77 6F 72 64 2D 73 61 6D 70 6C 65 2D 30 34 0D 64   tools-word-sample-04.d
6F 63 31 37 31 36 38 30 2F 4F 74 68 65 72 20 46 69 6C 65 73 2F 49   oc171680/Other Files/I
6E 74 65 72 6E 61 6C 20 53 74 6F 72 61 67 65 2F 44 6F 77 6E 6C 6F   nternal Storage/Downlo
61 64 31 32 30 32 30 2F 30 38 2F 33 30 20 31 30 3A 33 34 3A 32 34   ad12020/08/30 10:34:24
```

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.



```
android-8.1-rc1 (8)
  data (36)
    adb (2)
    anr (2)
    app (8)
      com.android.vending-SK6qx4pA_B0FzMZInsoX9Q==
      com.google.android.gms-7SK54pAzPTy9vWkCaSDU!
      com.kingo.root-E4HDOsd5Nm4mha-k1m8gSQ== (5)
      com.prosoftnet.android.idriveonline-iMBhGgTYRcOol
        lib (3)
          85e0adbb-42f6-41ac-9631-a7d8eddebc48 (
        oat (3)
          x86 (5)
            base.odex.swap (0)
```

/img_a8.dd/android-8.1-rc1/data/app/

Name	S
[current folder]	
[parent folder]	
lib	
oat	
base.apk	

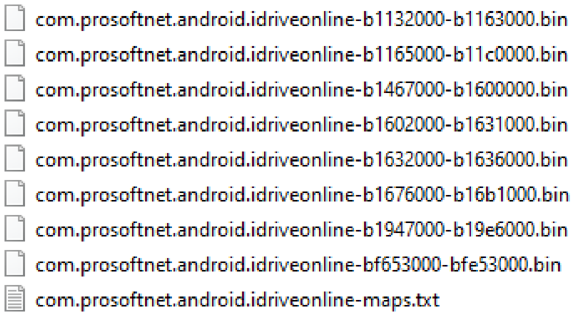
Figure 6. iDrive Installation Location

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.

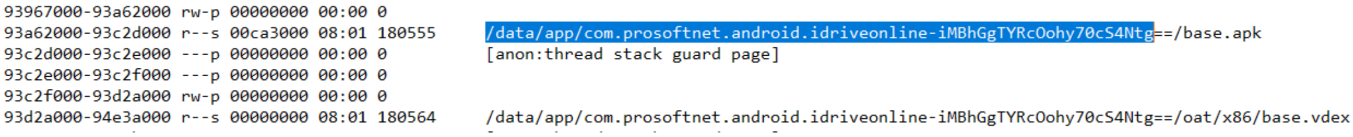


com.prosoftnet.android.idriveonline-b1132000-b1163000.bin
com.prosoftnet.android.idriveonline-b1165000-b11c0000.bin
com.prosoftnet.android.idriveonline-b1467000-b1600000.bin
com.prosoftnet.android.idriveonline-b1602000-b1631000.bin
com.prosoftnet.android.idriveonline-b1632000-b1636000.bin
com.prosoftnet.android.idriveonline-b1676000-b16b1000.bin
com.prosoftnet.android.idriveonline-b1947000-b19e6000.bin
com.prosoftnet.android.idriveonline-bf653000-bfe53000.bin
com.prosoftnet.android.idriveonline-maps.txt

Figure 8. List Acquisition from proccess RAM

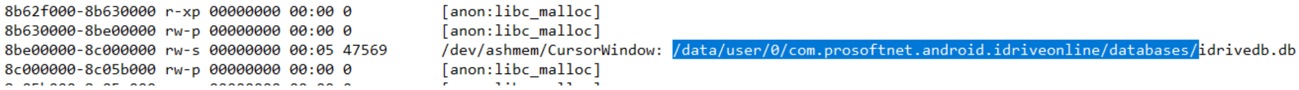
From the results of the acquisition, the .txt file shows the location of the iDrive installation location as shown in Figure 9.

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.



```
93967000-93a62000 rw-p 00000000 00:00 0
93a62000-93c2d000 r--s 00ca3000 08:01 180555       /data/app/com.prosoftnet.android.idriveonline-iMBhGgTYRcOohy70cS4Ntg==/base.apk
93c2d000-93c2e000 ---p 00000000 00:00 0            [anon:thread stack guard page]
93c2e000-93c2f000 ---p 00000000 00:00 0
93c2f000-93d2a000 rw-p 00000000 00:00 0
93d2a000-94e3a000 r--s 00000000 08:01 180564       /data/app/com.prosoftnet.android.idriveonline-iMBhGgTYRcOohy70cS4Ntg==/oat/x86/base.vdex
```

Figure 9. iDrive Installation Location from Database



```
8b62f000-8b630000 r-xp 00000000 00:00 0          [anon:libc_malloc]
8b630000-8be00000 rw-p 00000000 00:00 0          [anon:libc_malloc]
8be00000-8c000000 rw-s 00000000 00:05 47569      /dev/ashmem/CursorWindow: /data/user/0/com.prosoftnet.android.idriveonline/databases/idrivedb.db
8c000000-8c05b000 rw-p 00000000 00:00 0          [anon:libc_malloc]
```

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.

6. REFERENCES

[1] J. Surbiryala and C. Rong, “Secure customer data over cloud forensic reconstruction,” *2018 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1–4, 2018.

[2] M. Shariati, A. Dehghantanha, and K. K. R. Choo, “SugarSync forensic analysis,” *Australian Journal of Forensic Sciences*, vol. 48, no. 1, pp. 95–117, 2016.

[3] A. Holst, “Mobile data traffic per smartphone worldwide from 2014 to 2024 (in GB/month),” *Statista*, 2019. [Online]. Available: https://www.statista.com/statistics/738977/worldwide-monthly-data-traffic-per-smartphone/.

[4] F. Daryabar, A. Dehghantanha, and K. K. R. Choo, “Cloud storage forensics: MEGA as a case study,” *Australian Journal of Forensic Sciences*, vol. 49, no. 3, pp. 344–357, 2016.

[5] Y.-Y. Teing, A. Dehghantanha, K.-K. R. Choo, Z. Muda, and M. T. Abdullah, “Greening Cloud-Enabled Big Data Storage Forensics: Syncany as a Case Study,” *IEEE Transactions on Sustainable Computing*, vol. 4, no. 2, pp. 204–216, 2017.

[6] Y. Y. Teing, A. Dehghantanha, and K. K. R. Choo, “CloudMe forensics: A case of big data forensic investigation,” *Concurrency Computation*, vol. 30, no. 5, pp. 1–12, 2018.

[7] W. A. Bhat, M. F. Jalal, S. S. Khan, F. F. Shah, and M. A. Wani, “Forensic analysis of Sync.com and FlipDrive cloud applications on Android platform,” *Forensic Science International*, 2019.

[8] T. Rochmadi and D. Heksaputra, “Forensic Analysis in Cloud Storage with Live Forensics in Windows (Adrive Case Study),” *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, vol. 8, no. December, pp. 292–297, 2019.

[9] T. Rochmadi, I. Riadi, and Y. Prayudi, “Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser,” *International Journal of Computer Aplications (IJCA)*, vol. 164, no. 8, pp. 31–37, 2017.

[10] Badan Standar Nasional (BSN), “Pedoman Identifikasi, Pengumpulan, Akuisisi danPreservasi Bukti Digital (ISO/IEC 27037:2012, IDT),” 2012.