International Journal of Information System & Technology
Akreditasi No. 158/E/KPT/2021 | Vol. 5, No. 6, (2022), pp. 726-735

FTK Image For Forensic Data Processing In Forensic Tools

Rachmat Suryadithia[1], Witriana Endah Pangesti[2], Muhammad Faisal[3], Aji Nurrohman[4], Wibisono[5], Arman Syah Putra[6]

[1,3]Faculty of Engineering and Informatics, Universitas Bina Sarana Informatika
[2]Faculty of Information Technology, Universitas Nusa Mandiri
[4,5]Faculty of Informatics, Institut Teknologi Budi Utomo
[6]Faculty of Information System, STMIK Insan Pembangunan

rachmat.rcs@bsi.ac.id[1], witriana.weg@nusamandiri.ac.id[2], muhammad.mal@bsi.ac.id[3], ajinurrohman7@gmail.com[4], wibi72jkt@yahoo.com[5], armansp892@gmail.com[6]

Abstract

The background of this research is how the use of a software can help find forensic data, which is needed so that the tool used is the right tool in helping forensic problems. The method used in this study is the NIJ method using 5 stages in a process of determining the answer. The first stage is preparation, the second stage in collecting data, the third is testing and the fourth stage is analyzing and the last is the reporting stage with the five stages. The direction of the research will be clearer. The problem raised in this research is how to find evidence using FTK images software. Using this software, you can search for the desired forensic data so that it can be proven that there is forensic evidence. The purpose of this study is how to prove data, especially photo data, can be used as forensic data that can be used as evidence, by using the right tools, namely the existing FTK images software, with the software, it can help parties in proving, especially in terms of forensics.

Keywords: *FTK Images, Data Forensic, Tools Forensic, Processing.*

1. Introduction

Information technology is technology that is used to process many things, for example, data processing and data processing to the maximum, to obtain information, so that data can be useful. Help many parties in the use of the information obtained [1]. Information technology is characterized by the birth of computers and their very fast development. The history of the modern computer age is very short. Starting with the creation of the first generation of computers to the current fifth generation of computers. The development of computer performance is measured by the speed of its work [2]. This development was also accompanied by the development of the internet or Interconnected Networks as a very effective medium for conveying information. ICT has become a symbol of the wave of change [3]. Advances in information technology and telecommunications also have a negative impact, namely the number of crimes related to internet applications. Instagram social media is one part that is used as a communication liaison between humans in the cyber world (cyber). The ease of accessing Instagram social media makes Instagram accounts increase, giving rise to fake accounts which, apart from being used to communicate, are also used to carry out improper actions, such as fraud and other criminal acts that can harm people [4].

ISSN : 2580-7250
Copyright © 2022 IJISTECH

For the first time information technology can be built for the benefit of humans, and other interests with this existence until now sustainable information technology is built to help humans, in everyday life many systems are created from technological information systems that were created to assist humans in doing their daily work [5]. The core of information technology is the merger of the three components consisting of software or software and the second is hardware is hardware and the third is brainware or people who use the two devices above with the combination of these three things can create information based on data processing information technology can do so that it can help everyday life and information technology can also be used to help from all fields from the economic field to the health sector which will help the public in obtaining information widely for the sake of information disclosure [6].

The method used in this study is to use technical methods using several stages, the first is the preparation of data collection, analyzer experiments and reports and this method. Then the direction of the research objectives can be determined so that it can determine the answers to the questions that have been proposed in this study [7]. The problem raised in this study is how to find forensic data so that it can be done by using the right software so that it can determine the search for the right data in order to solve the given problem so that forensic data can better answer the problem [8]. In forensics using tools that are usually used in the form of FTK Images, created in accessing data this is used because it can pull data so that it can be used as a formation that is converted into important, so that the data can be used as forensic evidence in the future, with this, the tool used in this research is FTK Images [9]. FTK images software can be used to assist in forensic data processing, especially the data to be processed to produce this information, revealing forensic data, with the use of this software it will be able to help all parties who need forensic data processing, the use of FTK Images software has been widely used [10]. Parties to solve problems in the field of forensics, especially forensics in the field of information technology [11].

2. Research Methodology

This research adapts the investigation process of the National Institute of Justice (NIJ) forensic analysis method. In this method, it is used to facilitate how the description of the research process that is being carried out so that the stages of this research can be known more systematically so that it can be used as a reference in research [12].

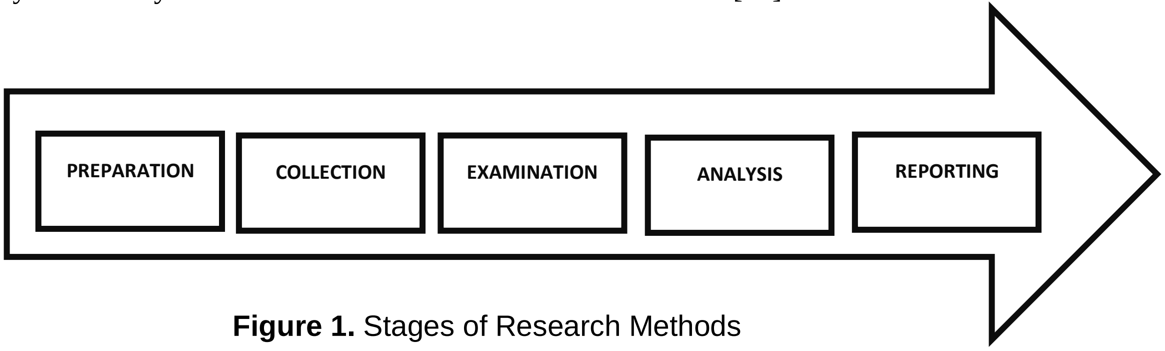


Figure 1. Stages of Research Methods

Research conducted in helping to deal with a problem in digital forensics, namely:

a) Stages of Preparation (Preparation)
   In this stage, namely preparing all the equipment and tools that can be used to carry out tasks in accordance with what is needed during the investigation.

b) Stages of Collection (Gathering)
   Searching for document files and collecting or making copies of physical/digital objects that contain electronic evidence, and other evidence therein.

c) Stages of Examination (Examination)
   This stage is the stage for checking electronic evidence / visible digital evidence and documents from the contents of the system / directory. In identifying evidence, data reduction was carried out.

d) Stages of Analysis (Analysis)
   After getting the evidence from the previous process, it is necessary to carry out the next stage, namely data analysis which aims to determine the significant evidence and the value of the evidence.

e) Stages of Reporting (Reporting)
   At this stage is the making of examination records in each case.

FTK imager is a digital forensics acquisition tool created by AccessData. FTK Imager can be used to create an image of a drive (physical imaging), create an image of the contents of a folder, or create a custom image consisting of only selected files. Each option is very useful in different field conditions and the type of evidence sought.

3. Result and Discussion

At this stage using the FTK Imager. Make the image a drive (physical imaging). FTK utilizes the processing capabilities between machines, shortening processing time by more than 400%.

Create Disk Image

Create a physical image from a USB FlashDrive using FTK Imager:

a) Plug in and make sure the Flash Drive has been detected/read by the computer system.

b) Open the FTK Imager application and select the File menu → Create Disk Image.

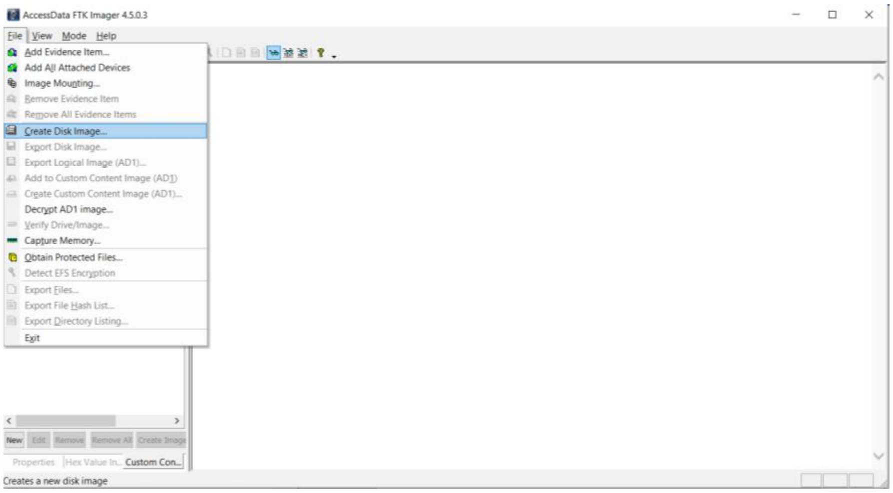
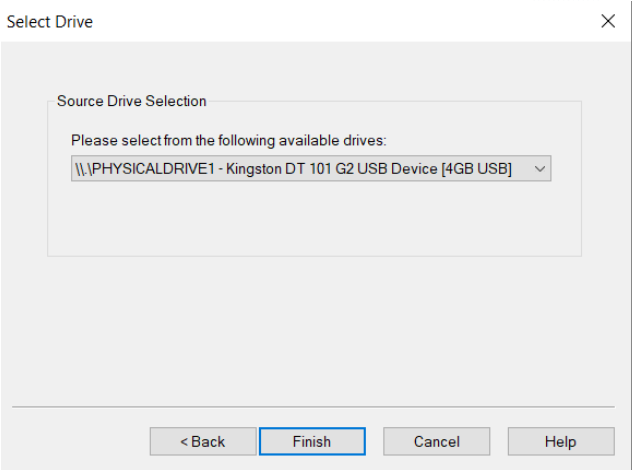


Figure 2. FTK Images data

c) After that, select Physical Drive because the physical imaging of the flash drive will be carried out. Then click Next.

d) Select the device for which the physical image will be created. In this case, select the flash drive that the system has read earlier, then click the Finish button.



Select Drive

Source Drive Selection

Please select from the following available drives:

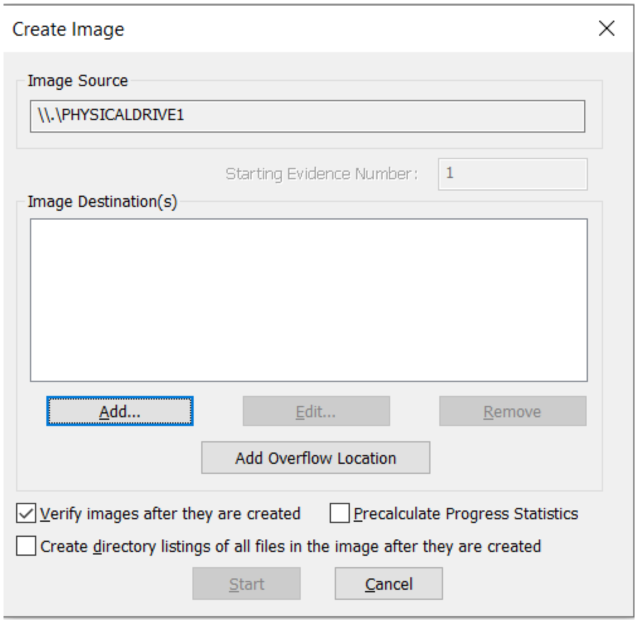
\\.\PHYSICALDRIVE1 - Kingston DT 101 G2 USB Device [4GB USB]

Figure 3. Data Drive Options

e) Select the device for which the physical image will be created. In this case, select the flash drive that the system read earlier, then click the Finish button.

f) Set the destination folder settings by clicking the Add button

1) Image Destination: Add to set the location of the imaging results, Edit to edit the location that has been added, remove to remove the location• Verify images after they are created : berguna untuk menghitung kode hash barang bukti dan hasil imaging kemudian mencocokkan keduanya.
2) Create directory listings of all files in the image after they created : create a directory list of images that have been created.



Create Image

Image Source

\\.\PHYSICALDRIVE1

Starting Evidence Number: 1

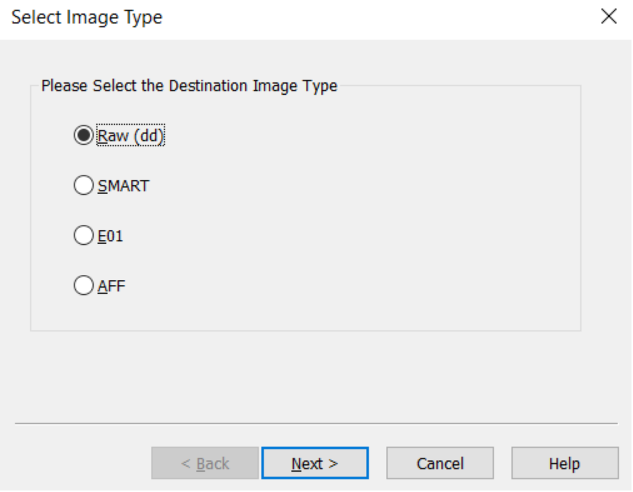
Image Destination(s)

☑ Verify images after they are created
□ Precalculate Progress Statistics
□ Create directory listings of all files in the image after they are created

Figure 4. Create Image

g) Determine the format of the image, here using the Raw format (dd)

1) SMART file format of the SMART program
2) E01 file format from EnCase
3) AFF (Advanced Forensic Format)



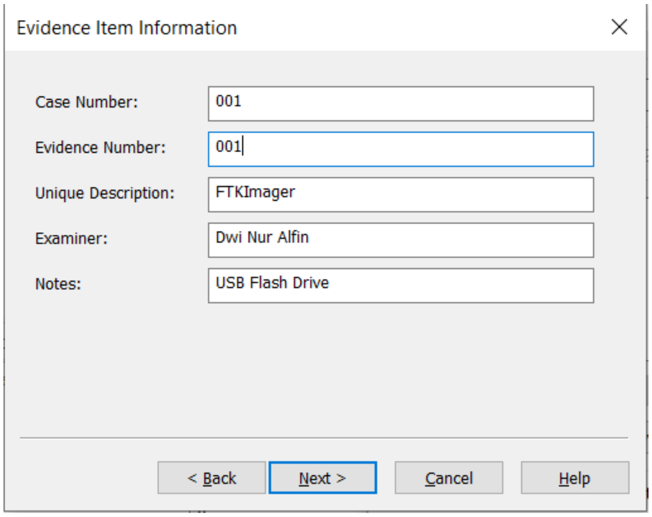
Select Image Type

Please Select the Destination Image Type

● Raw (dd)
○ SMART
○ E01
○ AFF

Figure 5. Select Image

h) Adding Information to Evidence



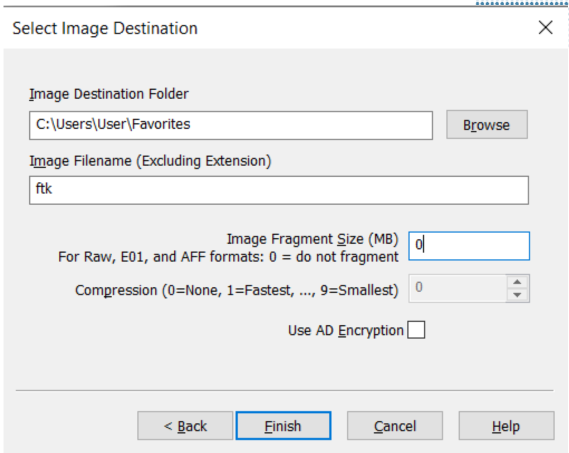
Evidence Item Information

Case Number:	001
Evidence Number:	001
Unique Description:	FTKImager
Examiner:	Dwi Nur Alfin
Notes:	USB Flash Drive

Figure 6. Evidence Item Information

i) After that, set the Destination Folder
   1) Image Destination Folder: select the destination location
   2) Image Filename: Fill in the Image File Name
   3) Image Fragment: Serves to split the file into several files according to the size entered. Write 0 so that the file is not split

After that click Finish



Select Image Destination

Image Destination Folder: C:\Users\User\Favorites

Image Filename (Excluding Extension): ftk

Image Fragment Size (MB): 0
For Raw, E01, and AFF formats: 0 = do not fragment

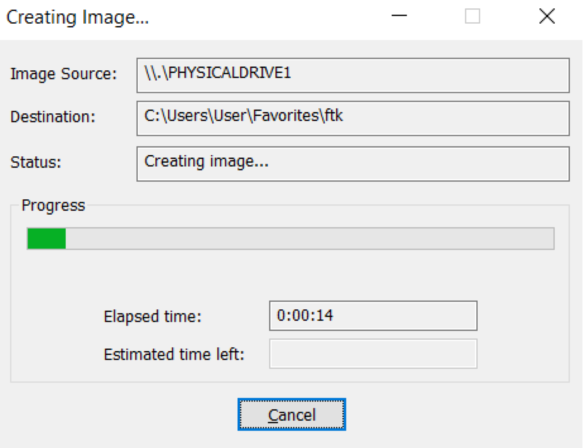
Compression (0=None, 1=Fastest, ..., 9=Smallest): 0

Use AD Encryption ☐

Figure 7. Select Image Destination

j) Click Start to start imaging

k) Wait for the Imaging process to finish



Creating Image...

Image Source: \\.\PHYSICALDRIVE1

Destination: C:\Users\User\Favorites\ftk

Status: Creating image...

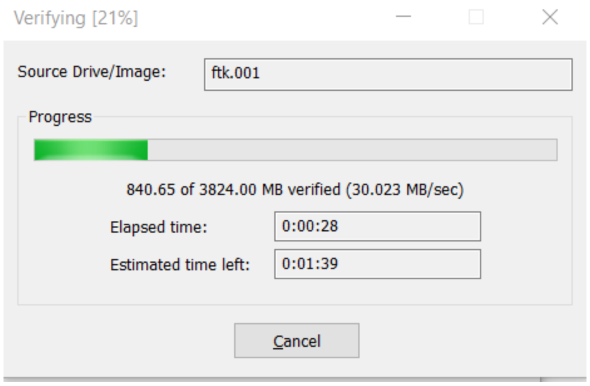
Progress

Elapsed time: 0:00:14

Estimated time left:

Figure 8. Creating Image FTK Imager

l) After the imaging process is complete, a verification window (integrity check) will appear whether the hash value of the image file matches the original one.



Verifying [21%]

Source Drive/Image: ftk.001

Progress

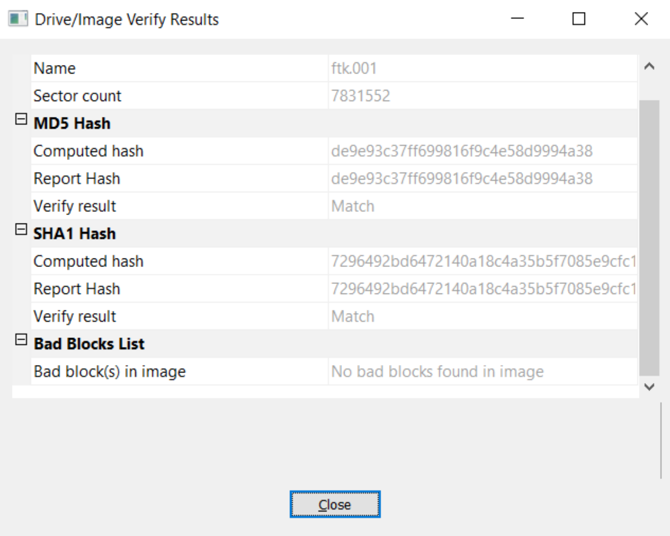
840.65 of 3824.00 MB verified (30.023 MB/sec)

Elapsed time: 0:00:28

Estimated time left: 0:01:39

Figure 9. Verifying Data

m) After verifying the file, the final result will appear in a window containing the hash value and the match of the hash value of the image file with the original. Please observe, if it is OK, click the Close button.



Name	ftk.001
Sector count	7831552
MD5 Hash	
Computed hash	de9e93c37ff699816f9c4e58d9994a38
Report Hash	de9e93c37ff699816f9c4e58d9994a38
Verify result	Match
SHA1 Hash	
Computed hash	7296492bd6472140a18c4a35b5f7085e9cfc1
Report Hash	7296492bd6472140a18c4a35b5f7085e9cfc1
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Figure 10. Drive Image Data

n) The imaging process has been successful

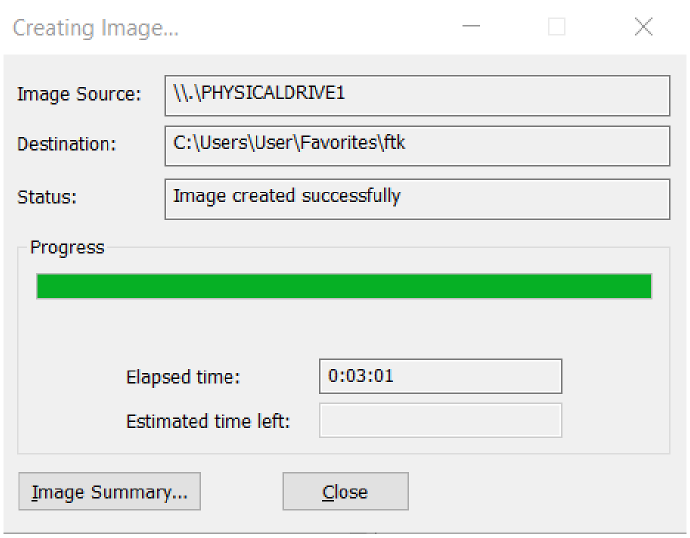


Image Source: \\.\PHYSICALDRIVE1

Destination: C:\Users\User\Favorites\ftk

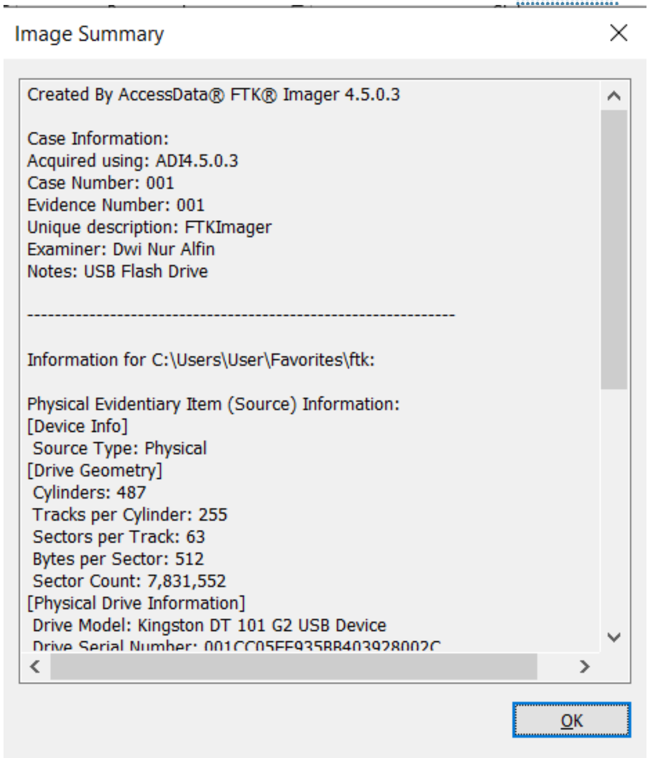
Status: Image created successfully

Elapsed time: 0:03:01

Estimated time left:

Figure 11. Creating Images FTK

o) If you click the Image Summary button, you will see the Summary Report of the Imaging process.



```
Created By AccessData® FTK® Imager 4.5.0.3

Case Information:
Acquired using: ADI4.5.0.3
Case Number: 001
Evidence Number: 001
Unique description: FTKImager
Examiner: Dwi Nur Alfin
Notes: USB Flash Drive

------------------------------------------------------------


Information for C:\Users\User\Favorites\ftk:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 487
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 7,831,552
[Physical Drive Information]
 Drive Model: Kingston DT 101 G2 USB Device
 Drive Serial Number: 001CC05FE935BB403928002C
```

Figure 12. Image Summary

p) The results of the Imaging can be seen in the Storage Folder earlier. 2 files will be found, namely 1 image file and 1 text file (containing information on the imaging process and the results of the verification/integrity check). Select the image file, right click → Properties to see the size of the image file, it will be the same as the size of the Flash Drive earlier

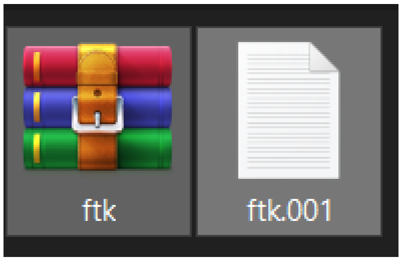


Figure 13. FTK Images Result

4. Conclution

FTK images is one of the tools used in problem solving media in the forensic field, especially data forensics which can make images able to answer the questions raised in this research problem, with this image processing it can be used as evidence in data processing, so that the data can be used as a basis for evidence. This is the method or guide on how to acquire and make imaging of hard disks, flash drives, SD cards, and other storage media. Future research can use other software to prove the use of forensic data as evidence of a case. With the use of other software, it can be ascertained that the comparison between one software and another software can be ascertained.

References

[1] A. S. Putra, H. L. H. S. Warnars, F. L. Gaol, B. Soewito, and E. Abdurachman, “A Proposed surveillance model in an Intelligent Transportation System (ITS),” *1st 2018 Indones. Assoc. Pattern Recognit. Int. Conf. Ina. 2018 - Proc.*, pp. 156–160, 2019, doi: 10.1109/INAPR.2018.8627013.

[2] A. S. Putra and H. L. H. S. Warnars, “Intelligent Traffic Monitoring System (ITMS) for Smart City Based on IoT Monitoring,” *1st 2018 Indones. Assoc. Pattern Recognit. Int. Conf. Ina. 2018 - Proc.*, pp. 161–165, 2019, doi: 10.1109/INAPR.2018.8626855.

[3] A. S. Putra, H. L. H. S. Warnars, B. S. Abbas, A. Trisetyarso, W. Suparta, and C. H. Kang, “Gamification in the e-Learning Process for children with Attention Deficit Hyperactivity Disorder (ADHD),” *1st 2018 Indones. Assoc. Pattern Recognit. Int. Conf. Ina. 2018 - Proc.*, pp. 182–185, 2019, doi: 10.1109/INAPR.2018.8627047.

[4] I. Ramadhan, A. Kurniawan, and A. S. Putra, “Penentuan Pola Penindakan Pelanggaran Lalu Lintas di DKI Jakarta Menggunakan Metode Analytic Network Process (ANP),” vol. 5, no. 1, pp. 51–57.

[5] M. Subani, I. Ramadhan, and A. S. Putra, “Perkembangan Internet of Think (IOT) dan Instalasi Komputer Terhadap Perkembangan Kota Pintar di Ibukota Dki Jakarta,” vol. 5, no. 1, pp. 88–93, 2021.

[6] Muhammad Syarif Hartawan, Arman Syah Putra, and Ayub Muktiono, “Smart City Concept for Integrated Citizen Information Smart Card or ICISC in DKI Jakarta,” *Int. J. Sci. Technol. Manag.*, vol. 1, no. 4, pp. 364–370, 2020, doi: 10.46729/ijstm.v1i4.76.

[7] Arman Syah Putra, “Smart City : Ganjil Genap Solusi Atau Masalah Di Dki Jakarta,” *J. IKRA-ITH Inform.*, vol. 3, no. 129, pp. 1–10, 2019.

[8] A. S. Putra *et al.*, “Examine Relationship of Soft Skills, Hard Skills, Innovation and Performance: the Mediation Effect of Organizational Learning,” *Int. J. Sci. Manag. Stud.*, vol. 3, no. 3, pp. 27–43, 2020, [Online]. Available: http://www.ijsmsjournal.org/2020/volume-3 issue-3/ijsms-v3i3p104.pdf.

[9] A. S. Putra, “Videotron in Intelligent Transportation Systems to Help Smooth Traffic,” no. May, p. 2021, 2021.

[10] N. K. Dewi *et al.*, “Konsep Aplikasi E-Dakwah Untuk Generasi Milenial Jakarta penting dalam menyiarkan agama Islam . Dengan media dakwah yang tepat maka akan bisa menyiarkan agama Islam dengan maksimal dengan media dakwah yang tepat suatu konsep dalam berdakwah dengan E-Dakwa,” vol. 5, no. 2, pp. 26–33, 2021.

[11] A. S. Putra, “Penerapan Konsep Kota Pintar dengan Cara Penerapan ERP (Electronic Road Price) di Jalan Ibu Kota DKI Jakarta,” *J. Inform. Univ. Pamulang*, vol. 5, no. 1, p. 13, 2020, doi: 10.32493/informatika.v5i1.4433.

[12] I. Ramadhan, A. Kurniawan, and A. S. Putra, “Penentuan Pola Penindakan Pelanggaran Lalu Lintas di DKI Jakarta Menggunakan Metode Analytic Network Process (ANP).”

Authors

1st Author
Rachmat Suryadithia
Faculty of Engineering and Informatics, Universitas Bina Sarana Informatika
rachmat.rcs@bsi.ac.id

2nd Author
Witriana Endah Pangesti
Faculty of Information Technology, Universitas Nusa Mandiri
witriana.weg@nusamandiri.ac.id

3rd Author
Muhammad Faisal
Faculty of Engineering and Informatics, Universitas Bina Sarana Informatika
muhammad.mal@bsi.ac.id

4th Author
Aji Nurrohman
Faculty of Informatics, Budi Utomo Institute of Technology
ajinurrohman7@gmail.com

5th Author
Wibisono
Faculty of Informatics, Institut Teknologi Budi Utomo
wibi72jkt@gmail.com

6th Author
Arman Syah Putra
Faculty of Information System, STMIK Insan Pembangunan
armansp892@gmail.com