ISSN No:-2456-2165

Forensic Computer Analysis by Performing an Autopsy on Flash Disk

Edy Supriyadi*, Iriandi Ilyas
Department of Electrical Engineering
National Institute of Science and Technology, Indonesia

Andi Suprianto, Tatang Suromenggolo Ronggo
Department of Informatics Engineering
National Institute of Science and Technology, Indonesia

Abstract:- Computer forensics is one of the sciences used to track digital evidence on hardware or software. Flashdisk is widely used because it is easy to carry and can store various kinds of files with large storage capacity. To be able to analyze, recover, and view hidden files, software such as AccessData FTK Imager 3.4, Autopsy 4.0, and additional software, 7-Zip 17.0, is required to compress and extract files. In this study, scenario testing and experiments were carried out on a flash disk in which there was an excel file that had been compressed using 7-Zip and disguised in a foto.jpg file using file merging steganography techniques. By using Access Data FTK Imager, an image file is created on electronic evidence. The image file was analyzed using Autopsy. The result of this research is that there is a difference in the capacity of the foto.jpg file because it is a merger of 2 (two) files. In addition, in the excel file there is evidence of crime, namely the sale of illegal motorbikes, the place of the transaction, the coordinates of the location and the phone number of the suspect.

Keywords:- *Computer forensics, flashdisk, digital evidence, steganography*

I. INTRODUCTION

With the rapid development of technology, so that some industries have even gone to technology 4.0, where the role of computer and cyber systems is more widely used to carry out their activities.

Technological advances will certainly result in the occurrence of new, more modern crimes. One of these crimes is cyber crime, where the perpetrators of this crime use computer media and networks to launch their actions. The patterns of crime that they use vary greatly, from the use of internet media, telecommunications to conventional methods they use to smooth their efforts in committing crimes. Criminals will hide evidence of their crimes at all costs. Although the perpetrators hide the evidence of their crimes, digital records can be searched and traced using forensic computer methods by forensic analysts. Therefore, the role of computer forensics is needed to reveal the perpetrators of the crime.

Computer forensics is a derivative discipline of computer security that discusses the finding of digital evidence after an event occurs. Computer forensic activity itself is a process of identifying, maintaining, analyzing, and using digital evidence according to applicable law. [7]

Disclosure of a case event requires strong evidence. Evidence obtained from computer storage media is referred to as digital evidence, which can be accounted for in court proceedings. The process of tracking and analyzing digital evidence uses a set of procedures to conduct thorough testing on a computer system using software and tools to extract and preserve evidence of criminal acts.

Not a few digital evidence is hidden, encrypted and even disguised by criminals with the aim that the process of finding digital evidence makes it difficult for investigations by forensic analysts and investigators (such as police and people conducting investigations) so that the evidence cannot be presented at trial because it is not strong and irrelevant to the case being filed. The way to disguise this evidence can be done by using steganography methods, ranging from simple methods to the use of encrypted files. The method used will slow down the analysis process on forensic computers, because forensic analysts have to search for suspicious files and dissect the files one by one with certain software.

II. LITERATURE REVIEW

A. *Digital Forensic*

Digital forensics or computer forensics is a combination of legal and computer science disciplines in collecting and analyzing data from computer systems, networks, communications, wireless and storage devices. Digital forensics is also an application of the field of computer science and technology for the benefit of legal evidence.

Forensic computers are used by law enforcement because of the many legal cases that require the role of computer science in making it easier to find evidence so that it can be submitted in court.

B. *Electronic Evidence*

Electronic evidence or often called electronic evidence is evidence that is physical and visually recognizable. Therefore, investigators and forensic analysts must already understand and recognize each - each electronic evidence when searching for evidence at a crime scene.

C. *Digital Evidence*

Digital evidence or also called digital evidence is data stored or transmitted using a computer that can support or refute a particular offense, or it can also be referred to as clues that point to important elements related to an offense [8].

The digital evidence is digital and can be extracted or recovered from electronic evidence. The digital evidence must be sought by investigators and forensic analysts to then be researched and analyzed so that there is a connection between the files obtained and the case at hand in order to reveal crimes related to electronic evidence.

D. File Systems

Every storage device must have one or more partitions that are 'organized' with a file system. This process will empty system files of the same type on the device. System files are used to separate data on the drive into one part called a file. It can also be used to store data about these files, including file names and file attributes.

E. Metadata

Metadata is structured information that describes, explains, locates, or at least makes information easy to find, use or manage. Metadata is often referred to as data about data or information about information. This metadata contains information about the content of data that is used for file/data management purposes in a database. If the data is in the form of text, the metadata is usually a description of the field name, field length, and field type: integer, character, date, etc. For image data, the metadata contains information about who took the picture, when it was taken, and the camera settings at the time of shooting. Digital evidence in the metadata process will be used as an important source of records in the disclosure of a crime.

F. Analysis Tools

The research conducted is themed Forensic Computer Analysis by Performing Autopsy on Flashdisk Media, using various kinds of forensic tools commonly used to analyze forensic computers. The research only uses freeware, shareware and opensource type tools. The software used in this research is AccessData FTK Imager, Autopsy, and 7-Zip.

III. RESEARCH METHODOLOGY

The flow of this research will be described in the form of a flowchart. The flow of this research is expected to help in conducting research that is more structured and systematic in the figure 1.

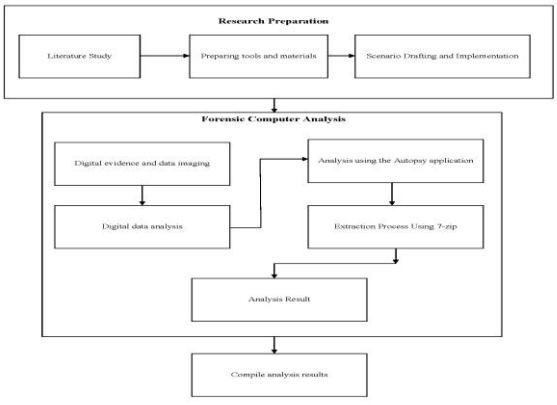

Fig. 1: Flowchart of Research Methodology.

A. Research Preparation

The preparation of the research made various kinds of literature studies, from digital evidence, forensic computer tools and features used and the use of flash drives as digital evidence, the last is the preparation and implementation of scenarios in order to be able to reconstruct relevant actions that may be carried out by criminals.. The development of this scenario is based on the analysis of digital evidence at the scene of the crime. The scenario that is carried out occurs as if the crime scene only gets one storage device, namely the flash disk left by the perpetrator. And the digital evidence is made with simple steganography techniques by utilizing cmd (command prompt) on Windows.

B. Forensic Computer Analysis

The research conducted is using analysis with forensic computer techniques, namely using the AccessData FTK Imager application to create forensic images on digital evidence. The type of image file used in this research is .E01 or what is called EnCase Image. Digital data that has been imaged is analyzed using the Autopsy application. In the Autopsy application, suspicious files will be detected. The Hex value and Metadata of the digital data will affect the results of the investigation. The scope of the analysis in the form of digital data should be able to provide important points in the investigation process. And 7-Zip is also used to analyze files that are used as evidence.

File Type	File Name		MD 5
Images	foto.jpg		577cbe24180a895fba3c01139305e412
Videos	-		-
Audio	-		-
Archieves	-		-
HTML	-		-
Office	-		-
PDF			
Plain Text	-		-
Rich Text	-		-

Table 1: Photo.jpg files read by Autopsy application

C. Analysis Results

The results of the analysis have 3 (three) important points in the investigation, namely the specification of the evidence, the metadata of the digital evidence, and the hexadecimal value of the digital evidence that shows the existence of hidden files. The last step is to compile the research results from the analysis in the research and prepared reporting summarizing the results of all the steps that have been carried out and making the conclusions reached in the research.

IV. RESULTS AND DISCUSSION

A. Research Scenario

The scenario is that electronic evidence, namely a flash drive, was found at the scene of the crime, and no other electronic evidence was found. So that electronic evidence is the only evidence in this scenario. Electronic evidence will be investigated by forensic analysts and investigators to shed light on who committed the crime.

B. Research Experiment

The research conducted is that the file that will be targeted as digital evidence is a photo.jpg file which is a merger of files from Image.jpg and price.zip using file merging steganography techniques.. After that the photo.jpg file is viewed using windows properties, but nothing suspicious is seen.

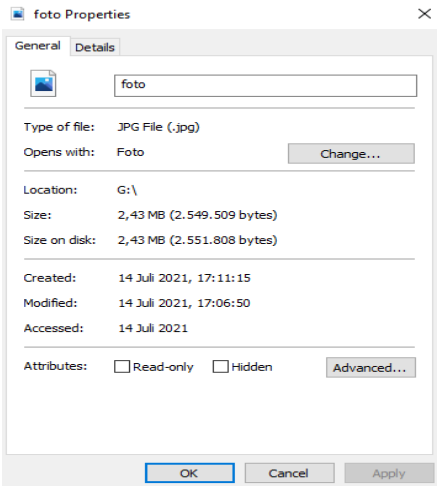

Fig. 2: Properties of the photo.jpg file

If the file is viewed in detail in the properties, it can be found that there is no visible irregularity because the image dimentions 2592 x 1944 is an image with a resolution of 5 MP.

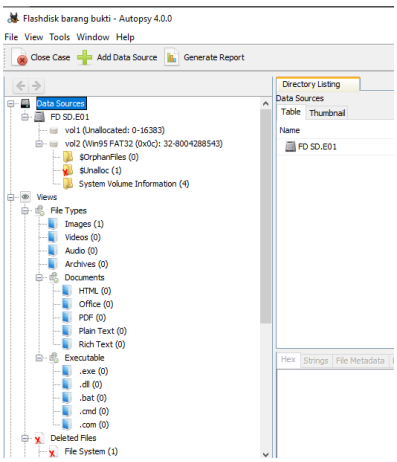

Fig. 3: Details Properties of the photo.jpg file

Therefore, an in-depth analysis is needed on this photo.jpg file by conducting computer forensics on the digital evidence.

C. Analysis with Autopsy Application

After the digital data is taken and has been made into a forensic image, then an initial analysis is carried out using the Autopsy application. By using the Autopsy application, it will help in finding files that will be used as digital evidence. In the Autopsy application, the investigator can freely see the contents of the forensic image. Due to its ability, Autopsy is often used by forensic investigators. Figure 4 shows a fragment of the full preview of the directory tree in the Autopsy application.

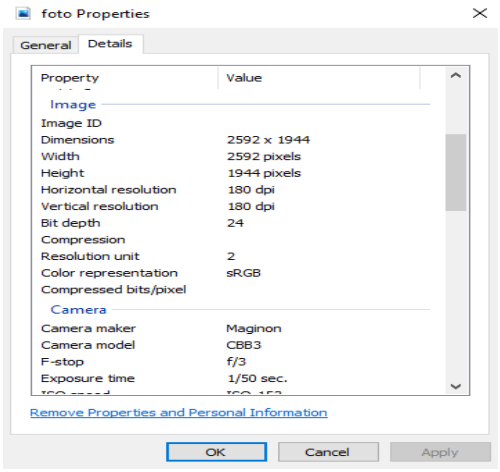

Fig. 4: Full Preview of Autopsy application

Figure 4 shows that on the flashdisk with the forensic image file FD SD.E01 there is only 1 (one) image file, and 1 (one) deleted File System. This indicates that the flash disk has been fully formatted before the image file was transferred to the flash disk

No	Findings	Description
1	There is only 1 image file	photo.jpg
2	There is a file system on vol2	FAT 32
3	The existence of a formatted file system and cannot be recovered	there is a Deleted Files directory

Table 2: Findings on digital evidence

From the findings table above, the analysis will be more aimed at the photo.jpg file. By using the Autopsy Application, several findings are obtained which will later be used as digital evidence. These findings can be seen in Figure 5.

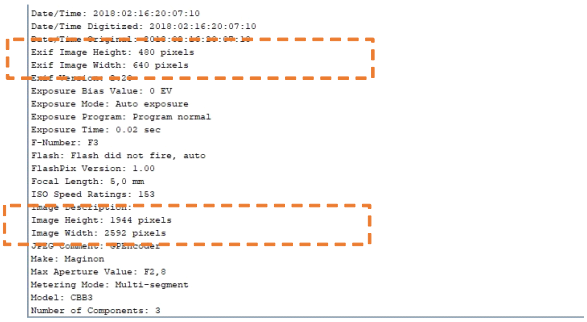

Fig. 5: Difference in pixels in the image

The picture above shows the difference between exif image and image pixels. With the Autopsy application, you can see the info from the photo.jpg file in Indexed Text. Shown in Figure 5, there is a difference between the Exif image size and the image size. Where the size of the Exif image has a smaller value than the image value. From the picture above, it can be explained using the following table.

	Exif Image	*Image*
Height	480 *pixels*	1944 *pixels*
Weidth	640 *pixels*	2592 *pixels*
Height x *Weidth*	0.3 MP	5 MP

Table 3: Comparison of Exif Image and Image sizes

From the table above, it is concluded that the photo.jpg file is a file modified by the camera device so that it produces a large number of pixels but has a small resolution size. Furthermore, by using the Hex (Hexadecimal) tool, it can be seen that there is a hidden file on page 156 in the photo.jpg file. This can be seen in Figure 6.

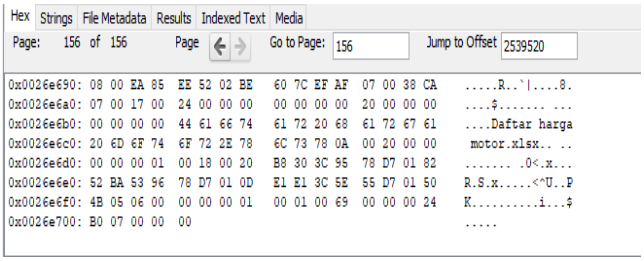

Fig. 6: Hex on photo.jpg file

From figure 6 above, it can be written using table 4.

File	*Offset*	*Signature*	*ASCII*
Motorcycle price list.xlsx	26e6b0	44 61 66 74 61 72 20 68 61 72 67 61 20 6D 6F 74 6F 72 2E 78 6C 73 78	Motorcycle price list.xlsx

Table 4: Offset and signature on photo.jpg file

From the data found, the results of research using the Autopsy application can be made in tabular form. The following is an explanation of the findings.

No	Analyzed results	Remarks
1	On the flashdisk found 1 image file, namely photo.jpg	Photo.jpg files have pixel and resolution differences
2	There is a formatted (deleted) file	The file cannot be recovered
3	There is a file system in vol2	*FAT 32*
4	In the photo.jpg file there is a compromised file	*Motorcycle price list.xlsx*

Table 5: Analysis result using Autopsy

Due to the existence of the motorcycle price list.xlsx file in the photo.jpg file, additional data is needed to find out the attributes of the photo.jpg file, namely by utilizing the Access Data FTK Imager application. In Figure 8 is the properties tool on the Access Data FTK Imager.

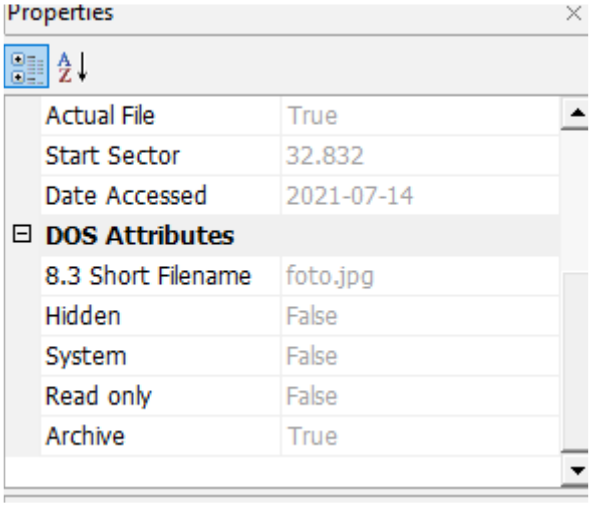

Fig. 7: File attribute on photo.jpg

It can be seen that in the photo.jpg attribute there is an Archive with a value of True. This indicates that the photo.jpg file has an archive, which can be opened using the 7-Zip application.

The way to do this is to remove the foto.jpg file from the digital data. This step can be done by exporting the image into the folder that has been created. In Figure 8, it is shown how to export images from digital data to the intended folder. After the image is exported, the next step is to remove the office file from the photo.jpg file.

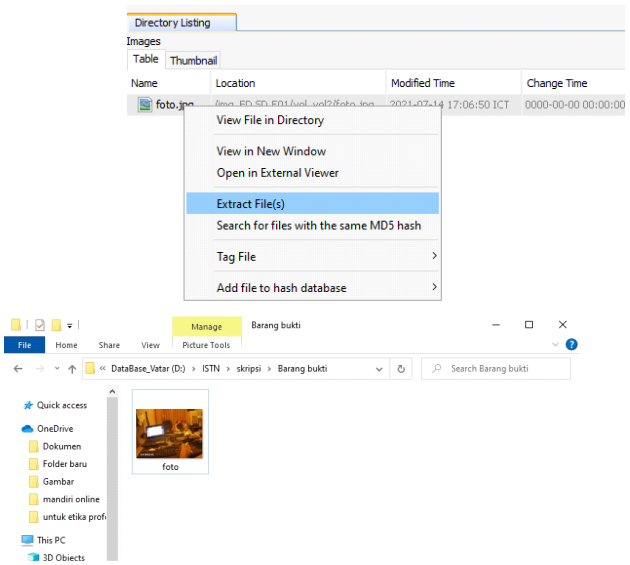

Fig. 8: How to export images to the destination folder

D. Analysis with 7-Zip Application

7-Zip is an application to compress files and also extract files. This application can be used to read files that are in the file. After digital evidence has been obtained in the form of an office file, using 7-Zip, we open the contents of the photo.jpg file. The step to do is to open the file directly using 7-Zip. Figure 9 shows that there is an office file in the photo.jpg file.

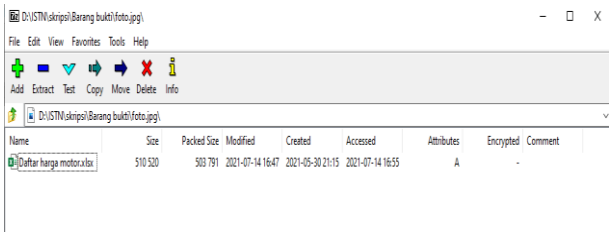

Fig. 9: Office file Excel on photo.jpg

After the file is visible, we can open it using an office application, here the author uses Excel. The contents of the file on the motorcycle price list.xlsx can be seen in Figure 10.

Motorcycle Price List

Motor Type	Manufacturing	Motorcycle Brands	Price List	STNK
Matic	Yamaha	Mio	Rp 2000000	Not available
		Fino	Rp 2000000	Not available
		Aerox	Rp 5000000	Not available
		Nmax	Rp 10000000	Not available
	Honda	Beat	Rp 2500000	Not available
		Vario 110	Rp 2500000	Not available
		Vario 125	Rp 5000000	Not available
		PCX	Rp 10000000	Not available
	Suzuki	Spin	Rp 1500000	Not available
		Hayate	Rp 2000000	Not available
		Nex II	Rp 2000000	Not available
		Address	Rp 2500000	Not available
Ducks	Yamaha	Jupiter	Rp 1500000	Not available
		Vega R	Rp 2000000	Not available
		Jupiter MX	Rp 5000000	Not available
	Honda	Supra X 125	Rp 2000000	Not available
		Sonic	Rp 5000000	Not available
	Suzuki	Smash F1	Rp 2000000	Not available
Sports	Yamaha	Byson	Rp 3500000	Not available
		Vixion	Rp 5000000	Not available
		R 15	Rp 10000000	Not available
		R 25	Rp 15000000	Not available
	Honda	Verza	Rp 5000000	Not available
		CBR 150	Rp 10000000	Not available
		CBR 250	Rp 15000000	Not available
	Suzuki	GSX S 150	Rp 10000000	Not available
		GSX R 150	Rp 10000000	Not available
		Bandit	Rp 10000000	Not available

Items to be purchased must wait for news from BOS WA 0888 888 999.
Do not disclose this number, without our knowledge.

Fig. 10: Motorcycle price list.xlsx file fragment

Fig. 11: File fragment Motorcycle price list.xlsx

From the picture above, it can be seen in Excel that the motorbikes do not have STNK and it is known that the number 0888 - 888 - 999 is the "boss" (suspect) of the illegal motorbike seller without papers. And in the picture it can be seen that there is a place for transactions opposite the PP Layer Cake shop on Jalan Alpukat IV Parung Panjang. If you look closely, you can see that there are coordinates on the map, namely -6.359617, 106.560093. These coordinates can be seen in the fragment of figure 12.

Fig. 12: Image fragments 10 - 11.

To be clearer, the results of the analysis using 7-Zip can be made in the form of table 5.

No	Analysis Result	Remarks
1	The photo.jpg file can be extracted from an office file	Motorcycle price list.xlsx - Illegal motorcycle sales
2	There is important data in the office file	- Suspect's phone number - Address and coordinates of the suspect's place

Table 6: Analysis results using the 7-Zip tool

E. Compiling Analysis Results

After all the evidence has been obtained, the results of the analysis are compiled based on the evidence that has been obtained. For more details, shown in table 7.

Analysis Result	
Electronic evidence	*Flashdisk Sandisk*
Model Name	*Cruizer Slice 8 GB*
Serial Number	SDCZ37-008G
Digital Data	photo.jpg
The application used	1. *AccessData FTK Imager* 2. *Autopsy* 3. *7-Zip*
Details of Findings	1. There is only 1 (one) image file in the electronic evidence 2. There is a file system, namely FAT 32 3. There is a file system that cannot be recovered 4. The photo.jpg file has differences in pixels and resolution 5. There is a file that is infiltrated in the photo.jpg file 6. There is an office file, namely Motorcycle Price List.xlsx which is inserted in the photo.jpg with the file merging method
Detailed analysis of findings (office file)	1.Illegal motorcycle sales without papers 2.The contact number (whatsapp) used as evidence is: 0888 888 999 3.Place of transaction opposite PP Layer Cake Shop Jl. Avocado IV Parung Panjang 4.Coordinates of the transaction location -6.359617, 106.560093 5.Password at the time of transaction "Buy 2 PP layers for selling"
Conclusions	By using forensic applications, it can make it easier for forensic analysts to find digital evidence that is hidden using simple steganographic methods.

Table 7: Compilation of analysis results

From table 7, it is clear that the results of the analysis show that there are hidden files, which turn out to be evidence of *curanmor crimes* that are traded, which is indicated by the sale and purchase of motorbikes without papers. From this digital evidence, the investigator can be forwarded to the Police Criminal Investigation Unit for further action. This digital evidence is very important to assist the police in arresting suspects. Digital evidence is very valuable so that as little as possible the evidence obtained must be utilized and used in court later.

V. CONCLUSION

Based on the results of forensic computer analysis research on flashdisk media, several conclusions are obtained that the author can explain based on the points.

- Forensic image is a copy of the contents of electronic evidence (flashdisk) that can be analyzed using forensic computer applications, so by utilizing the tools on AccessData FTK Imager, namely the properties tool and on Autopsy, namely Indexed Text and Hex, digital evidence is obtained, namely the motorcycle price list.xlsx file which is inserted into the photo.jpg file.
- The AccessData FTK Imager and Autopsy applications have the disadvantage that electronic evidence (flashdisk) that is full format (not quick format), the data in it cannot be recovered.
- By using the properties tool on AccessData FTK Imager, files that are hidden by compressing will be read, then by using the 7-Zip application, the file is extracted so that the hidden file can be seen.

REFERENCES

[1.] Ahwan Ahmadi, T. A. (2021). Comparison of Forensic Tool Results on Android Smartphone Image Files Using the NIST Method. JIKO (Journal of Informatics and Computers), pp. 92-97.

[2.] Desti Mualfah, R. A. (2020). Forensic Analysis of CCTV Camera Metadata as Digital Evidence. Journal of Information and Communication Technology, pp. 257-267

[3.] Husni Mubaro, N. W. (2017). Digital Forensic Analysis of Steganography Files (Case study: Drug Distribution). Journal of Informatics Engineering and Information Systems (JUTISI).

[4.] Imam Riadi, R. U. (2018). Digital Forensic Analysis on Froezen Solid State Drive with National Of Justice (NIJ) Method. Electrinics, Informatics and Vocational Education (ELINVO), pp. 70-8

[5.] Computer Forensics : Definition and Purpose (Complete). (2021, 11). Retrieved from https://www.seputarpengetahuan.co.id /2021/11/komputer-forensik-pengertian-dan-tujuan.html

[6.] Mark Reith, C. C. (2002). An Examination of Digital Forensic Models. International Journal of Digital Evidence.

[7.] Pratomo Djati Nugroho, S. M. (2017). IT: DIGITAL FORENSIC. IPSIKOM JOURNAL.

[8.] M. PUSFID. (2016, December 17). Center for Digital Forensics Studies. Retrieved from Center for Digital Forensics Studies, Universitas Islam Indonesia: https://forensics.uii.

[9.] Riskiyadi, M. (2020). Forensic Investigation of Digital Evidence in Uncovering Cybercrime. CyberSecurity and Digital Forensics, pp. 12-21.
[10.] Sleuthkit. (2022). Retrieved from Autopsy User Documentation: http://sleuthkit.org/autopsy/docs/user-docs/4.19.2/
[11.] Sleuthkit. (2022). Autopsy. Retrieved from http://www.sleuthkit.org/sleuthkit/docs.php
[12.] Sunardi, I. R. (2020). National Journal and Information Systems, pp. 1-18.
[13.] Vidila Rosalina, A. S. (2016). Analysis of Data Recovery Using Forensic Software: Winhex And X-WAYS Forensic. PROSISKO.
[14.] Wikipedia. (2021, 10 3). Wikipedia The Free Encyclopedia. Retrived from Digital Forensics: https://id.wikipedia.org/wiki/Forensik_digital
[15.] Yinita Sartika Sari, N. R. (2015). Steganography with File Merging Method through Command Prompt and Steganalysis of Results with Image Recognition Pattern Method, Image Culture, 24 Bit RGB and Size Range on Jpeg Files. MKOM TELEMATICS.