Signature File Analysis Using The National Institute Standard Technology Method Base on Digital Forensic Concepts

Randi Rizal[1], Ruuhwan[2], Septian Chandra[3]

Teknik Informatika, Fakultas Teknik, Universitas Perjuangan Tasikmalaya, Jl. Pembela Tanah Air (PETA) No. 177 Kahuripan Kec. Tawang Kota Tasikmalaya Jawa Barat Indonesia, 46115

e-mail : [1]randirizal@unper.ac.id, [2]ruuhwan@unper.ac.id, [3]septian@gmail.com

Submitted Date: July 08th, 2020 Reviewed Date: September 22nd, 2020
Revised Date: September 27th, 2020 Accepted Date: September 30th, 2020

Abstract

The number of crimes committed by utilizing advances in information technology such as information leakage, embezzlement of money in banks, credit card fraud, pornography, terrorism, drug trafficking and many more are definitely related to the name digital data. File signatures or magic numbers are one of the forensic science techniques that assist in processing this digital data. The method used in this research is the National Institute Standards Technology method to analyze the authenticity of digital data and the method of proof to obtain valid evidence during the identification process of data or file content. This research is presented in the form of an analysis of the use of signature files in investigations to determine the type of file in the case of leaking company information xyz, the research stage uses evidence handling procedures in the laboratory. Contributions made after conducting a series of case investigations using signature files have been successfully carried out using the Access Data FTK Imager application version 4.2.0 and WinHex version 18.6. Signature files can be used for case investigations in identifying and verifying file types so that files that have been modified can be restored and can be read by the operating system by checking file types through hexadecimal values in the header file (file prefix) that show the characteristics of each type file so that the file type can be found and the file can be read by the operating system.

Keywords: digital evidence; digital forensics; signature file; investigation process; winhex

1 Introduction

Advances in technology not only provide various conveniences that are felt but can also have negative impacts such as progress in crime where crime is very closely related to the development of human life and human civilization, especially in terms of technology (Maslin, Consultant, & Ltd, 2018). Many crimes are also carried out by utilizing information technology advancements such as information leakage, embezzlement of money in banks, credit card fraud, pornography, terrorism, naroba trade and many more (Europol, 2017), (Ramadani et al., 2018), (Khan, Nasir, Ali, & Farooq, 2016).

The issue of data validity is also very important for protection in addition to the issue of confidentiality, because if the receiver receives false data then there will be variations of interpretation resulting in confusion and failure on both sides. One technique is used in the use of digital signatures, so that the recipient is sure that the obtained data is not fake data. This technique will prevent the receiver from using fake data. Any data received has a signature that is always different from other data, so a small change can cause the signature to change very quickly (Noroozi, Daud, & Sabouhi, 2015).

Someone expert in the field of forensic will definitely relate to the name digital data, file signature or magic number is one of the digital forensic techniques that help in processing these data (Sitompul, Handoko, & Rahmat, 2018). The understanding of Magic Number in Tony Sammes's book "Forensic Computing" is a code in the form of hexadecimal numbers to determine the format of a data file that is usually located at the beginning of the file. When we open a file using certain software, for example SonyVegas, the software will first read the magic number of the file that was opened, then if it matches the magic number will be processed immediately. It aims to avoid errors or errors when opening files that are very large in size. Magic Number is only a few bytes in size (Sammes & Jenkinson, 2007).

In a study conducted by (Nugis, 2018) stated that the signature file or magic number is closely related to forensic experts where they use digital data as one method of investigation, while the signature file itself is one of the forensic science techniques that can help in the field of hygiene processing. The signature file is used when identifying data or file contents. File Signature is one technique that can be used to maintain the authenticity of data, so that the recipient gets a guarantee to know that the data received is authentic or fake data (Harran, Farrelly, & Curran, 2018).

The way to prove it to get valid evidence is to conduct an investigation using the Digital Forensic Examination Procedure approach (Ruuhwan, Riadi, & Prayudi, 2017), (Du, Le-Khac, & Scanlon, 2017). Digital evidence in the form of a USB Flashdisk is carried out forensic imaging process to produce an image file so that from the forensic imaging process digital evidence can be analyzed and examined and original digital evidence can be stored and secured in its place.

Based on the background that has been presented before, this study discusses about the analysis of file signature using the national institute of standards technology method. Analyze the authenticity of digital data and the method of proof to obtain valid evidence during the identification process of data or file content.

2 System Design

The methods used are varied, including the National Institute of Standards Technology (NIST) as in (Riadi, Yudhana, & Putra, 2018), and the National Institute of Justice (NIJ) in (Yudhana, Riadi, & Anshori, 2018). In his research, he explains about Facebook Messenger's Digital Evidence Analysis.

NIST methode process is the approach used to evaluate digital evidence or stages for obtaining information from digital evidence. Once data is collected and examined, the first transformation happens, then removes data from the media and transforms it to a format that can be interpreted by forensic instruments. Second, through analysis, the data is transformed into information. Finally, the transformation of information into a proof analogy by translating knowledge into practice using information produced during the reporting process by analysis in one or more ways.

The research method used in solving cases is the National Institute of Standards Technology (NIST) method. The NIST method is used to perform analysis of digital evidence and as a stage for obtaining information from digital evidence, consisting of 4 stages such as Fig. 1 (Umar, Riadi, & Muthohirin, 2019).

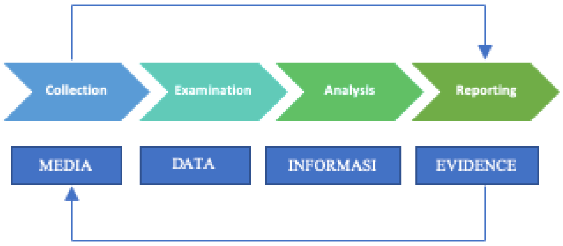


Fig. 1 Stages of Method NIST

Based on Fig. 1 this can be explained the forensic analysis stage as follows:

1. Collection is in charge of collecting evidence in the form of digital evidence.
2. Examination is the processing of data collected in the use of forensic combinations of various scenarios, both automatic and manual, as well as assessing and releasing data according to your needs while maintaining data integrity.
3. Analysis is an analysis of the results of examinations using justified and legal technical methods.
4. Reporting is reporting the results of analysis which includes a description of the actions taken.

The way of proof to obtain valid evidence is to carry out an investigation using the Digital Forensic Examination Procedure approach. The software specifications used for the signature file analysis process are presented in Table 1.

Table 1 Software Specification

No	Software	Version
1.	Access Data FTK Imager	4.2.0
2.	WinHex	18.6

Besides software, hardware requirements for research into the signature file analysis process use the specifications presented in Table 2. These hardware requirements are essential in carrying out the digital investigation process.

Table 2 Hardware Specification

ISSN: 2541-1004
e-ISSN: 2622-4615
10.32493/informatika.v5i3.6073

No	Item	Description
1.	PC (Client)	CPU: AMD Ryzen 3 1200 Memory: 6 GB OS: Windows 10 Display: 1080 x 1920 pixels
2.	Flashdisk	V-GEN Memory: 16 Gigabyte Number : AA00000000000489

3 Result and Analysis

The results of the research we have done have obtained results. The process of getting evidence on a USB Flashdisk using the FTK Access Data forensic software application. Here are the results that have been obtained. There are four main stages performed in the experiments in this study, namely are Collection, Examination, Analysis and Reporting.

3.1 Collection

In the Collection Process digital evidence in the form of a USB Flashdisk is performed forensic imaging process to produce an image file so that from the forensic imaging process digital evidence can be analyzed and original digital evidence can be stored and secured in its place. The forensic imaging process uses the Access Data FTK version 4.2.0 application.

Fig. 2 Evidence of a USB Flashdisk

Fig. 2 is electronic evidence in the form of a USB Flashdisk left by a criminal before running away. The USB Flashdisk is branded V-GEN with a capacity of 16 giga bytes with the number AA00000000000489.

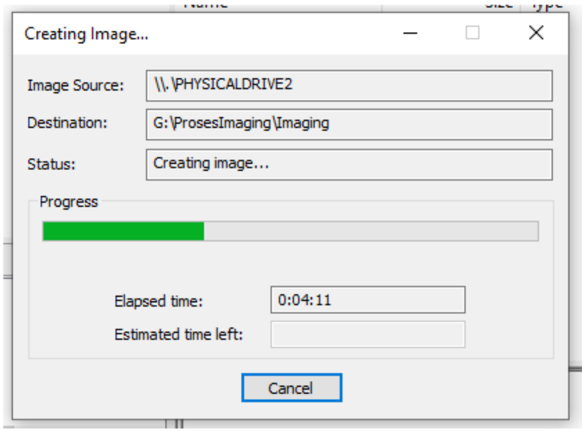

Creating Image...

Image Source: \\.\PHYSICALDRIVE2
Destination: G:\ProsesImaging\Imaging
Status: Creating image...

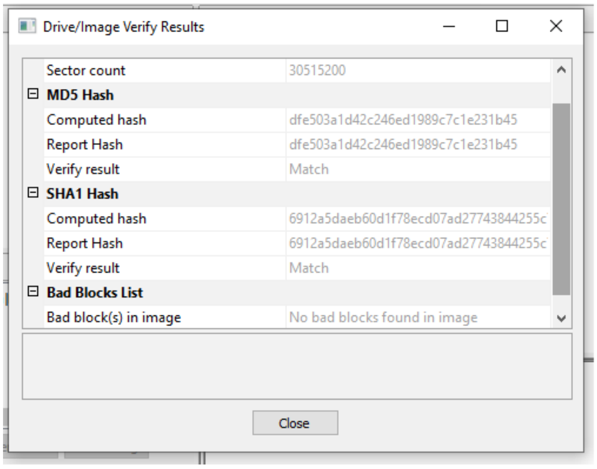
Elapsed time: 0:04:11
Estimated time left:

Fig. 3 Forensic Imaging Process

Fig. 3 is a display of the Forensic Imaging process by using the Access Data FTK Imager application version 4.2.0 to get the image file where the image file will be used in the Examination process.

Forensic imaging process has been completed will produce an image file, then proceed with the Examination of the MD5 and SHA1 hash value between the evidence in the form of storage media with the forensic imaging results in the form of an image file. If the values of the two are the same, the forensic imaging process is successful.

The hashing process using the FTK Imager application version 4.2.0 can be seen in Fig. 3 here shows the hashing process running successfully and has been verified.


Drive/Image Verify Results

Sector count	30515200
⊟ **MD5 Hash**	
Computed hash	dfe503a1d42c246ed1989c7c1e231b45
Report Hash	dfe503a1d42c246ed1989c7c1e231b45
Verify result	Match
⊟ **SHA1 Hash**	
Computed hash	6912a5daeb60d1f78ecd07ad27743844255c
Report Hash	6912a5daeb60d1f78ecd07ad27743844255c
Verify result	Match
⊟ **Bad Blocks List**	
Bad block(s) in image	No bad blocks found in image

Fig. 4 Forensic Imaging Results

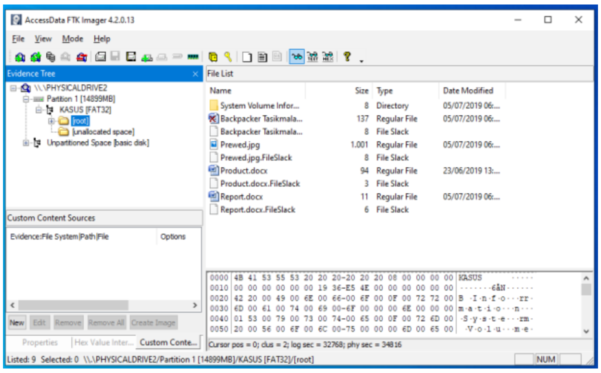
3.2 Examination

Examination process is carried out in a comprehensive file with the intent to obtain digital data in the investigation process. The data sought is data relating to data leakage of yxz company information. This search process uses the Access Data FTK Imager application version 4.2.0 and the

ISSN: 2541-1004
e-ISSN: 2622-4615
10.32493/informatika.v5i3.6073

WinHex application version 18.6. Examination process carried out with the Access Data application FTK Imager version 4.2.0 and the WinHex application version 18.6 is to use manual browsing techniques by checking the file type of the contents of digital evidence through hexadecimal values that indicate the file type. The hexadecimal value is often referred to as the "signature file / four magic number".

The signature file is used to verify the authenticity of the file. The signature file contains a hexadecimal character set at the beginning (header) and the end (trailer) file that forms a characteristic for each file type. If one of the hexadecimal letters or numbers has changed, the contents of the file have changed or have been modified. The following are the results of the *examination of the contents of digital evidence files.*


File List

Name	Size	Type	Date Modified
System Volume Infor...	8	Directory	05/07/2019 06:...
Backpacker Tasikmala...	137	Regular File	05/07/2019 06:...
Backpacker Tasikmala...	8	File Slack	
Prewed.jpg	1.001	Regular File	05/07/2019 06:...
Prewed.jpg.FileSlack	8	File Slack	
Product.docx	94	Regular File	23/06/2019 13:...
Product.docx.FileSlack	3	File Slack	
Report.docx	11	Regular File	05/07/2019 06:...
Report.docx.FileSlack	6	File Slack	

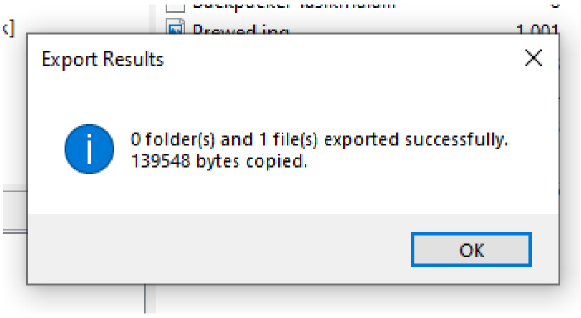
```
0000 4B 41 53 55 53 20 20 20-20 20 20 08 00 00 00 00 KASUS
0010 00 00 00 00 00 00 19 36-E5 4E 00 00 00 00 00 00 ·······6åN······
0020 42 20 00 49 00 6E 00 66-00 6F 00 0F 00 72 72 00 B ·I·n·f·o···rr·
0030 6D 00 61 00 74 00 69 00-6F 00 00 00 6E 00 00 00 m·a·t·i·o···n···
0040 01 53 00 79 00 73 00 74-00 65 00 0F 00 72 6D 00 ·S·y·s·t·e···rm·
0050 20 00 56 00 6F 00 6C 00-75 00 00 00 6D 00 65 00  ·V·o·l·u···m·e·
```

AccessData FTK Imager 4.2.0.13
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE2
Partition 1 [14899MB]
KASUS [FAT32]
[root]
[unallocated space]
Unpartitioned Space [basic disk]
Custom Content Sources
Evidence:File System|Path|File
Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
Cursor pos = 0; clus = 2; log sec = 32768; phy sec = 34816
Listed: 9 Selected: 0 \\.\PHYSICALDRIVE2/Partition 1 [14899MB]/KASUS [FAT32]/[root]
NUM

Fig. 5 Examination Image File Results

Examination image file using the Access Data FTK Imager application version 4.2.0 can be seen in Fig. 3 there are four files, three with the extension .docx with file names : Backpacker Tasikmalaya.docx, product.docx, report.docx and one file with extension .jpg file : Prewed.jpg. From the results of Examination can be seen that there is one file that was deleted by the perpetrator, namely a file with the name Backpacker Tasikmalaya.docx.

The image file that has been created in the Application Data Access FTK Imager version 4.2.0 is then performed an export file using the export file menu in the Data Access FTK Imager application version 4.2.0 so that you can check each file using the WinHex application version 18.6 to see the signature file From a digital evidence file that has been duplicated or forensic imaging performed. The process data file in the FTK Data Access application version 4.2.0 automatically performs the recovery file that has been deleted, the file named Backpacker Tasikmalaya.docx can be accessed easily by the operating system. The following display export file that can be seen in Fig. 6.


Export Results

0 folder(s) and 1 file(s) exported successfully.
139548 bytes copied.

Fig. 6 Process of Exsport File

Pada proses examination merupakan pengujian pada file Backpacker Tasikmalaya menggunakan aplikasi Winhex Versi 18.6.

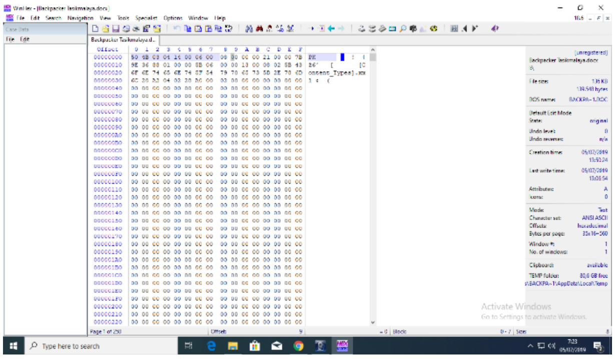
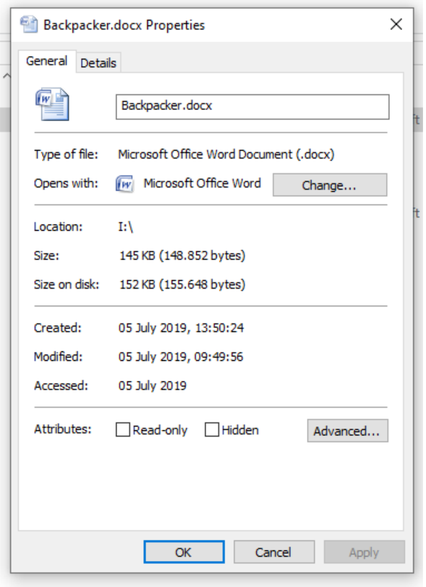

WinHex - [Backpacker Tasikmalaya.docx]
File Edit Search Navigation View Tools Specialist Options Window Help
Activate Windows
Type here to search

Fig. 7 Examination file results Backpacker Tasikmalaya

Viewed from Fig. 7 is the result of the Examination file Backpacker Tasikmalaya.docx by using the WinHex application version 18.6 which has been carried out the export process using the Access Data application FTK version 4.2.0, the signature file from the Backpacker Tasikmalaya.docx file is 50 4B 03 04 14 00 06 00.

3.3 Analysis

The analysis process is carried out in depth in detail and comprehensively against the files that have been obtained from the Examination process, when the data has become digital evidence that supports the investigation then the data is analyzed by looking at the metadata (information in information) of each file files that support the investigation in order to obtain information that supports the investigation to obtain 4W1H data (Who, When, Where, Why and How) regarding the case of leaking company information xyz.



Backpacker.docx Properties

General | Details

Backpacker.docx

Type of file: Microsoft Office Word Document (.docx)
Opens with: Microsoft Office Word Change...

Location: I:\
Size: 145 KB (148.852 bytes)
Size on disk: 152 KB (155.648 bytes)

Created: 05 July 2019, 13:50:24
Modified: 05 July 2019, 09:49:56
Accessed: 05 July 2019

Attributes: □ Read-only □ Hidden Advanced...

OK Cancel Apply

Fig. 8 Metadata file Backpacker Tasikmalaya.docx

Seen in Fig. 8 is a metadata view of the Backpacker Tasikmalaya.docx file. Information can be seen in the information created and the modified data has experienced changes. Based on the metadata from each file, the digital evidence found has undergone a change. That is indicated by the information created and modified data. Digital evidence that has undergone a change / modification, the modified data statement will indicate the time when the data was modified last by the perpetrator. The results of the modified data are then given to the investigator for further investigation of the perpetrators.

The results of the analysis conducted by the perpetrators changed the file extension and injected the file to hide digital evidence. The following results of the analysis provide information in support of case investigations in the form of the contents of files from digital evidence:

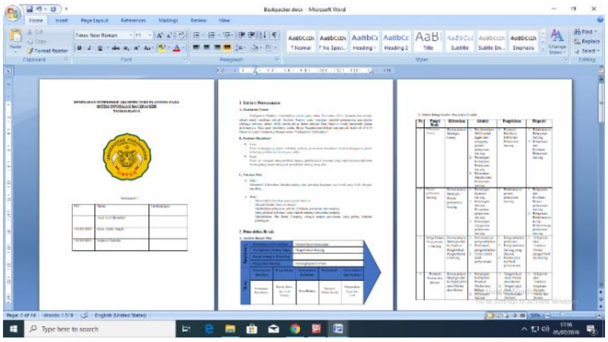


Fig. 9 Content of file Backpacker.docx

Seen in Fig. 9 is the contents of the Backpacker.docx file that has been automatically recovered in the export file in the Access Data FTK Imager application version 4.2.0 so that the Backpacker.docx data or file is in the form of a document explaining the delivery of company xyz information data to competing company workers.

3.4 Reporting

Digital evidence obtained in the collection process, Examination process and analysis obtained data in accordance with the needs of the investigation, the evidence analyzed in the form of a V-GEN USB Flashdisk with a size of sixteen gigabytes with number AA00000000000489 which contains 4 files, namely Backpacker. docx, Product.jpg, Report.xlsx and Prewed.jpg.

The following is the result of Examination of digital evidence contents that have been carried out forensic imaging processes, export files using the WinHex application version 18.6 shown in Table 3.

Table 3 File Name and File Signature digital evidence

No	Nama File	Ekstensi	File Signature
1.	Backpacker	.docx	50 4B 03 04 14 00 06 00
2.	Product	.docx	FF D8 FF E0 00 10 4A 46
3.	Report	.docx	50 4B 03 04 14 00 06 00
4.	Prewed	.jpg	FF D8 FF E0 00 10 4A 46 49 46 00

Examination process is obtained by two files that cannot be opened by the existing operating system (corrupt). The two files have changed from the signature file, there is a difference from the hexadecimal value which indicates the type of file with the extension listed. The perpetrator has changed the essence of the two files so that the file is corrupt. After Examination the signature file turns out that the file called report.docx has the extension .xlsx and the file named product.docx has the extension .jpg. The following is a file extension with the correct file signature data shown in Table 4.

Table 4 File Name and File Signature are true digital evidence

No	Nama File	Ekstensi	File Signature
1	Backpacker	.docx	50 4B 03 04 14 00 06 00
2	Product	.jpg	FF D8 FF E0 00 10 4A 46
3	Report	.xlsx	50 4B 03 04 14 00 06 00
4	Prewed	.jpg	FF D8 FF E0 00 10 4A 46 49 46 00

After the Examination file signature process is performed, an Examination hash is performed from each file to create a hash and identify the authenticity of the file using the Access Data FTK Imager application version 4.2.0. Hash processing is very important in the process of identifying the authenticity of digital evidence.

Table 5 Hash Analysis

No	File Extension	MD5 Hash Results with Original Files
1	Rename	Fixed
2	Change Extension	Fixed
3	Save As	Different
4	Change Content File	Different

Judging from Table 5 on the hash analysis, it can be explained that the MD5 hash results from the file that has been renamed to the file extension and changed the extension to the original file. The hash value of the file execution by save as will be different from the original file because the application automatically changes the contents such as authors, date modified, revision number and others. The hash value of the file execution by changing the contents of the file will be different from the original file because the contents of the contents are changed so the hash value changes.

The conclusion from the results of the hash analysis that the results of MD5 hash of files that have been executed file that does not change the contents of the file will not change the hash value, and the results of the MD5 hash of files that have been executed by changing the contents of the original file will change hash value.

Table 6 Hash Process Results

No	Nama File	Ext.	*Hash* MD5
1.	Backpacker	.docx	c98506890e7fffeedc99ddfbb5876304
2.	Product	.jpg	c949dbbb0547abf6aea59776374831a3
3.	Report	.xlsx	7603166387e1f92cdcb42a8a6436fcd3
4.	Prewed	.jpg	e5da47477688440968bb0e7f10e576a2

The result of the hash process shows that the Product.jpg and Prewed.jpg files are the same files as the company sensitive files. From Examination in digital evidence there are five files, namely are Backpacker Tasikmalaya.docx, product.jpg, report.xlsx, and prewed.jpg, hypotheses about cases can be formulated, namely company sensitive information data contained in one of the files with product names. jpg and report.pdf.

4 Conclusion

Based on the research conducted, by using the Access Data application FTK Imager version 4.2.0 and the WinHex application version 18.6, the signature file analysis has been successfully analyzed in the digital forensic process by looking at the hexadecimal character set in the header so that the file that has changed its extension can be read. File Signature plays a very important role in the digital forensic process to identify and verify files. So that files that have been changed changes can be returned to the original extension and can be read by the operating system used by forensic analysts.

The results of the hash analysis conducted in this study that the hash value will be different if the file has been executed (save as, change the contents of the file) and the hash value is the same as the original file after the file is executed (rename and change the file extension).

References

Du, X., Le-Khac, N. A., & Scanlon, M. (2017). Evaluation of digital forensic process models with respect to digital forensics as a service. *European Conference on Information Warfare and Security, ECCWS*, 573–581.

Europol. (2017). Crime in the age of technology. *Europol Unclassified - Basic Protection Level*.

Harran, M., Farrelly, W., & Curran, K. (2018). A method for verifying integrity & authenticating digital media. *Applied Computing and Informatics*, *14*(2), 145–158. https://doi.org/10.1016/j.aci.2017.05.006

Khan, M. A., Nasir, A., Ali, M. N., & Farooq, U. (2016). Crime Detection using Digital Forensic Technology. *International Journal of Computer Science and Information Security (IJCSIS)*, *14*(10), 487–506.

Maslin, N. M., Consultant, P., & Ltd, S. S. (2018). Impact of Modern Technology. *HF Communications:*, *3*, 33–35. https://doi.org/10.4324/9780203168899_chapter_10

Noroozi, E., Daud, S. M., & Sabouhi, A. (2015). Secure Digital Signature Schemes based on Hash Functions. *International Journal of Computer Engineering and Sciences*, *1*(1), 27. https://doi.org/10.26472/ijces.v1i1.18

Nugis, R. (2018). *Forensic Data Properties of Digital Signature BDOC and ASiC-E Files on Classic Disk Drives*.

Ramadani, S., Siahaan, A. P. U., Sutrisno, Ritonga, S., Amelia, W. R., Dalimunthe, H., & Munthe, R.

(2018). Impact of Cybercrime on Technological and Financial Developments. *International Journal For Research in Multidisciplinary Field*, *4*(10), 341–344.

Riadi, I., Yudhana, A., & Putra, M. C. F. (2018). Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute of Justice (Nij). *Jurnal Teknik Informatika Dan Sistem Informasi*, *4*(2), 219–227. https://doi.org/10.28932/jutisi.v4i2.769

Ruuhwan, R., Riadi, I., & Prayudi, Y. (2017). Evaluation of integrated digital forensics investigation framework for the investigation of smartphones using soft system methodology. *International Journal of Electrical and Computer Engineering*, *7*(5), 2806–2817. https://doi.org/10.11591/ijece.v7i5.pp2806-2817

Sammes, T., & Jenkinson, B. (2007). *Forensic Coputing A Practionier's Guide*.

Sitompul, O. S., Handoko, A., & Rahmat, R. F. (2018). File reconstruction in digital forensic. *Telkomnika (Telecommunication Computing Electronics and Control)*, *16*(2), 776–794. https://doi.org/10.12928/TELKOMNIKA.v16i2.8230

Umar, R., Riadi, I., & Muthohirin, B. F. (2019). Live forensics of tools on android devices for email forensics. *Telkomnika (Telecommunication Computing Electronics and Control)*, *17*(4), 1803–1809. https://doi.org/10.12928/TELKOMNIKA.v17i4.11748

Yudhana, A., Riadi, I., & Anshori, I. (2018). Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist. *It Journal Research and Development*, *3*(1), 13–21. https://doi.org/10.25299/itjrd.2018.vol3(1).1658