JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XII No 2, Maret 2026, hlm. 383 – 390 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/ 10.33330/jurteksi.v12i2.4414
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

DIGITAL FORENSIC INVESTIGATION ON STORAGE MEDIA BASED ON NIST WITH FORENSIC PROCESS METHODS

Indra Gunawan[1*], Heru Satria Tambunan[2], Abdullah Ahmad[3]
[1] Informatics Engineering, STIKOM Tunas Bangsa
[2] Information Systems, STIKOM Tunas Bangsa
[3]Informatics, STIKOM Tunas Bangsa
email: *indra@amiktunasbangsa.ac.id

Abstract: Storage media is an inseparable tool in everyday life. With storage media, users can store important data, both personal and workplace. In addition, in many cases, Indonesian law uses storage media as evidence. The Electronic Information and Transactions Law (UU ITE) regulates how the provision of digital evidence can be strong evidence in court. This study examines the forensics of digital evidence on storage media with four test scenarios. Digital forensic processing uses forensic processes based on the National Institute of Standards and Technology (NIST) guidelines. This study produces an analysis in which evidence processed with scenarios 1 and 4 is valid digital evidence to be submitted to court, while evidence 2 and 3 is invalid evidence. The results of this digital evidence can be used for investigations under the ITE law.

Keywords: autopssy; digital forensics; storage media; FTK Imager.

Abstrak: Media Penyimpanan merupakan alat yang tak terpisahkan dari kehidupan sehari-hari. Dengan Media Penyimpanan, pengguna dapat menyimpan data penting, baik pribadi maupun tempat kerja. Selain itu, dalam banyak kasus, hukum Indonesia menggunakan Media Penyimpanan sebagai alat bukti. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) mengatur bagaimana penyediaan alat bukti digital menjadi alat bukti yang kuat di pengadilan. Penelitian ini mengkaji forensik terhadap alat bukti digital pada Media Penyimpanan dengan empat skenario pengujian. Pemrosesan forensik digital menggunakan proses forensik berdasarkan panduan National Institute of Standards and Technology (NIST). Penelitian ini menghasilkan analisis di mana alat bukti yang diproses dengan skenario 1 dan 4 merupakan alat bukti digital yang sah untuk diajukan ke pengadilan, sedangkan alat bukti 2 dan 3 merupakan alat bukti yang tidak sah. Hasil dari barang bukti digital ini, dapat digunakan untuk penyelidikan didalam undang-undang ITE.

Kata kunci: otopsi; forensik digital; media penyimpanan; FTK Imager

INTRODUCTION

Storage media use to store important data, such as personal data or important information of bagi_individu or company. However, it _tidak be undeniable that sometimes there are individuals or groups who intend to carry out illegal activities such as data theft, malware spread, and so on [1].

Cybercrime continues to evolve as technology evolves and it is undeniable that sometimes digital evidence is

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XII No 2, Maret 2026, hlm. 383 – 390 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/ 10.33330/jurteksi.v12i2.4414
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

often stored in storage media such as disks. This has been proven and recorded in several cases in Indonesia, through the 2023 Judgment Directory website, which can be searched with the keyword "forensic-digital storage media". There were 6,701 cases and among them there were 138 cases of ITE (Information and Electronic Transactions) crimes related to storage media [2].

The results of the verdict prove that in ITE criminal cases in Indonesia, the perpetrators of criminal acts store evidence in memory-storage. The provisional laws regarding ITE that apply in Indonesia are contained in Law Number 19 of 2016 concerning Information and Electronic Transactions [3]. Based on the Constitution, electronic information or electronic documents are legally valid evidence in Indonesia. Electronic documents store information electronically which can be accessed through a computer or electronic system, which includes text, sounds, images, and similar forms, conveying meanings that may be understood by a capable person.

In addition to this article, there is also article 6 which explains that electronic information or electronic documents are considered valid according to the prevailing manner in Indonesia if the digital evidence can be accessed, displayed, guaranteed to be intact, and accountable - which explains several circumstances [4]. Therefore, it is important to understand and prove the ways of storing, altering, and disseminating digital evidence so that it can be accounted for in the eyes of the law, especially for parties related to the law. This is necessary to further explore the validity of digital evidence, such as in cases where digital evidence originally stored in a deleted storage medium can be considered legitimate.

National Institute of Standards and Technology (NIST)-developed guidelines to help analyze digital forensics for digital evidence on storage media published under the NIST publication code SP 800-86. There are four important stages of the publication of NIST SP 800-86 in conducting or executing the stages of digital forensics: Collection, Examination, Analysis, and Reporting [5]. With the hope that after four stages, they can prove that they found existing digital evidence deleted on a storage medium that can provide structured information to describe, explain, use and place forensic information as valid evidence in court [6].

There are several studies related to digital forensics, a journal article titled "Forensic Investigation of Remnant Data on USB Storage Devices Sold in New Zealand" focuses on forensic investigation of residual data on storage media storage devices. The authors evaluated three open imaging forensic source tools, namely DC3DD, DCFLDD, and Guymager, based on criteria set by the National Institute of Standards and Technology (NIST) [7]. They conduct case testing, analyze functionality, and hardware usage and spend time from each tool and compare its performance. The study found that most of the storage media purchased in New Zealand contained sensitive personal and organisational data. A journal article titled "Static Forensics on USB Mass Storage Use Forensics Toolkit-Imager" discusses the use of digital forensics on USB mass storage that was tested to obtain digital evidence from USB mass storage. Furthermore, evidence will be processed using Staticc Forrensics and the Forensics Toolkit Imager. The results of the discussion show that the Static Forensics method can be used safely and validly to retrieve digital

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XII No 2, Maret 2026, hlm. 383 – 390 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/ 10.33330/jurteksi.v12i2.4414
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

evidence on USB mass storage [8]. The Forensics Toolkit Imager has also been proven to help in the process of extracting and processing digital evidence more effectively and efficiently [9].

Seeing the importance of authenticity and validity of digital evidence, this study conducted a forensic investigation of cases on storage media, to see whether digital evidence on the storage media is valid or not. Forensic investigations are conducted using the Forensic Process method based on NIST standards. This research also involves the use and comparison of the results of various analysis tools, namely the use of Autopssy and Access Data FTK-imager [10]. The application of the methods to be studied can provide strong, clear and accurate results on digital evidence. This research was conducted to investigate whether digital evidence based on the results of the investigation can be a valid tool or evidence and support the trial process. For example, in the investigation there are things that support digital evidence that can incriminate the results of the verdict in the eyes of the law [11].

METHOD

The authors will apply methods that have been published by the National Institute of Standards and Technology (NIST) in the publication NIST SP 800-86. The flow of the research can be seen in Figure 1.

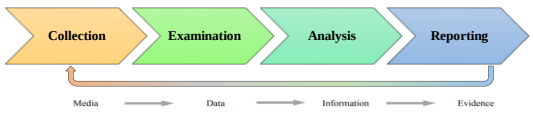


Figure 1. Forensic Process

Based on Figure 1, there are four stages in the Forensic Process, namely the Collection process, the Examination process, the Analysis process, and the Reporting process. The following is an explanation of these stages.

Data Collection Process

This stage is the process of collecting data related to the event or thing to be searched for that will be identified, labeled, recorded, and collected, while maintaining the integrity of the data [12]. So, it can be used as evidence from storage media and also include digital evidence in it. At this stage, the author will create a scenario where a person provides storage media as evidence to be submitted to the court and the author checks whether the storage media is a valid evidence or not in court, by creating four supporting examination scenario schemes.

First, the storage medium stores 10 files that are considered original as digital proof and there are no changes or deletions to those 10 files. Secondly, the storage media contains 10 original files however, there are 8 files in it [13]. Third, the storage media contains 10 original files and the difference between the file and the original file is found. Fourth, the storage medium with 10 original files, there is a modified name of the file.

Data Processing Process

This stage describes the appropriate tools and techniques for forensics with the type of data collected to be used to identify and extract relevant information from the data that has been collected and maintain the integrity of the data [14].

Table 1. Tools used in the study

Device	Specification	Information

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XII No 2, Maret 2026, hlm. 383 – 390 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/ 10.33330/jurteksi.v12i2.4414
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

Name		
laptop	ASUS TUF Gaming F15, i7-10870H 2.20GHz, 8GB, Windows 11 home single language, x64-based PC	Hardware and operating system
USB Penyimpanan External & Internal	Seagate USB *hdd/ffd/ssd*	Hardware test
Autopssy	Autopssy 4.20.0 (RELEASE)	Forensic software
Access Data FTK imager	AccessData ® FTK® Imager 4.7.1.2	Forensic software
Hash Calc	Version 2.02	Hash validity software

Data Analysis Process

This stage involves analyzing the results of the audit to obtain information and conclusions that are useful in answering questions or objectives that are the motivation for data collection and examination [14]. This stage is supported by analyzing the results of the examination from the FTK-Imager and Autopssy applications, then producing conclusions that answer the question or goal are valid or not.

Reporting Stage Process

The final stage involves an analysis of the delivery results, which includes an explanation of the actions that have been taken, determining additional actions needed, as well as recommendations for improving policies, guidelines, procedures, tools, and other aspects of the forensic process [15].

RESULT AND DISCUSSION

Collection Stage

At the stage of collecting evidence, it is carried out by inserting digital evidence into the storage media which currently contains 10 pieces of digital evidence with file extensions .docx, .pdf, .mp3, . MOV, .jpg, .zip, .xlsx, .ppt, .exe and .txt where each file has a hash mark that will be used as a reference in this study.

Table 2. The reference value generates a hash of the original file on the storage media

FILE NAME	MD5 VALUE
DOCUMENT FORMAT	
[BBD]1.txt	72711458fbe6bf211a54ff730d2c1266
[BBD]2.pdf	a0323887b43cde8d6a097f06222458f1
[BBD]3.doc	25fedabace3c2011c8dacf3761f95d60
[BBD]4.pptx	ca71ae171d962d3e54330c595be9bb1e
[BBD]5.xlsx	bef9e6d9db169eafb928d7b379b49edb
IMAGE FORMATS	
[BBD]6.jpg	1fe95ec5e459a11113447a4f01f89550
AUDIO FORMATS	
[BBD]7.mp3	fe01262c6e4be7e3199bb38a91853f47
VIDEO FORMAT	
[BBD]8.MOV	939f231f2dc99df6e69d828e7074bca6
COMPRESSION FORMAT	
[BBD]9.zip	78cc17876dcfeacb4b306e39ad93204a
EXECUTABLE FORMAT	
[BBD]10.exe	0161434123901af384ab9453d61a13d2

Examination Stage

At this stage, the evidence of the hard disk is inserted into the USB port of the digital forensic evidence execution laptop. USB Write Protector is activated,

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XII No 2, Maret 2026, hlm. 383 – 390 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/ 10.33330/jurteksi.v12i2.4414
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

then the hash value is matched with the help of the Hash-Calc and FTK Imager applications. FTK-Imager is used to clone data or image data as digital proof of a flash drive[13].

Table 3. Match imaging data results with storage media

SCHEME	MD5 MEDIA PENYIMPANAN	MD5 IMAGING	STATUS VERIFICATION
SCHEME 1	3d8a64b00ac85c6a722cd263452bf7d6	3d8a00b73ac85c6a722cd263452bf7d6	VALID
SCHEME 2	b72e142c00a46bf9f4986972bf16cc28	b72e002c73a46bf9f4986972bf16cc28	VALID
SCHEME 3	0ec8d000ad9e982c3f54793c863fe531	0ec8d000ad9e982c3f54793c863fe531	VALID
SCHEME 4	2dfc00fc0ec1dd0cbd6656659bfb25da	2dfc00fc0ec1dd0cbd6656659bfb25da	VALID

Stages of Analysis

Based on the results obtained after data imaging, the digital evidence was further analyzed and became digital evidence using FTK-Imager and Autopssy to get maximum results.

Scheme 1 :

The storage media stores 10 files that are considered original as digital proof and there are no changes or deletions to those 10 files. In scheme 1, the FTK-Imager and Autopssy software managed to obtain 10 digital proof files along with their hash values. After matching with the hash value reference in the following results are obtained:

Produces 10 image files from the original storage media and there is no difference in the value with the hash results from either the FTK-Imager or Autopssy software, so the digital evidence in schema 1 is considered valid and can be submitted as valid digital evidence.

Scheme 2 :

The storage media contains 10 original files, but there are only 8 files in the storage media. In scheme 2, the FTK-Imager and Autopssy software managed to obtain 8 original files of evidence, and there were 2 original files of evidence. The evidence is deleted from the storage media along with its hash value.

The result is still the same, resulting in 10 files with a hash value of 10 files. However, both software also detects the deletion of evidence files.

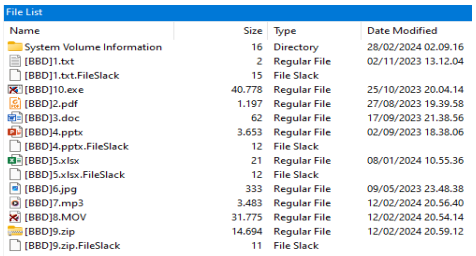


Figure 2. Results of 2 FTK Imager imaging scheme

The output of Schema 2 uses FTK-Imager to detect and locate two deleted digital evidence items with file names [BBD]8.MOV and [BBD]10.exe. This deletion is evidenced by the cross red icon of the existing file.

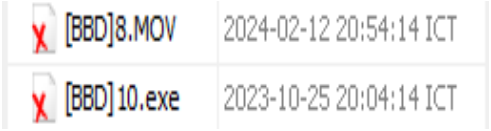


Figure 3. Autopsy Scheme imaging results 2

The output results from Scheme 2 using Autopssy also detected and found

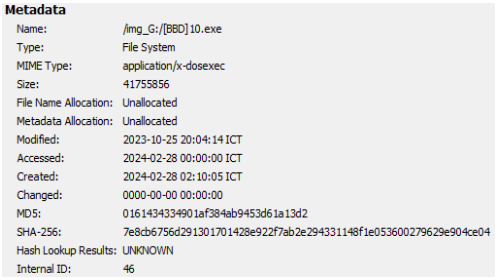
JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XII No 2, Maret 2026, hlm. 383 – 390 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/ 10.33330/jurteksi.v12i2.4414
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

there were two items of digital evidence that were deleted with the file names [BBD]8.MOV and [BBD]10.exe and verified with a file icon containing a red cross.

Metadata

Name:	/img_G:/[BBD]8.MOV
Type:	File System
MIME Type:	video/quicktime
Size:	32537253
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2024-02-12 20:54:14 ICT
Accessed:	2024-02-28 00:00:00 ICT
Created:	2024-02-28 02:09:59 ICT
Changed:	0000-00-00 00:00:00
MD5:	939f968f2dc99df6e69d828e7074bca6
SHA-256:	2ba5e6f07caa8938b9cc35054ac18ddef84bb526adc0a92a55e0f49c6f3a22ae
Hash Lookup Results:	UNKNOWN
Internal ID:	42

Figure 4. Item metadata digital proof [BBD]8.MOV



Metadata

Name:	/img_G:/[BBD]10.exe
Type:	File System
MIME Type:	application/x-dosexec
Size:	41755856
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2023-10-25 20:04:14 ICT
Accessed:	2024-02-28 00:00:00 ICT
Created:	2024-02-28 02:10:05 ICT
Changed:	0000-00-00 00:00:00
MD5:	0161434334901af384ab9453d61a13d2
SHA-256:	7e8cb6756d2913017014 28e922f7ab2e294331148f1e053600279629e904ce04
Hash Lookup Results:	UNKNOWN
Internal ID:	46

Figure 5. Item metadata digital proof [BBD]10.exe

The results of the validation of scheme 2 in table 6 and table 7, as well as the evidence of deletion on the storage media, in figure 4 and figure 5, can be concluded that the evidence with scheme 2 is invalid because there are already two files that have been deleted, namely the files with the names [BBD]8.MOV and [BBD]10.exe.

Scheme 3 :

Where the hash value in the storage media of the original 10 files is found to be different from the content of the original file. In scenario 3, both FTK-Imager and the Autopssy software managed to obtain 10 digital proof files with a hash value.

The results of the analysis from Scheme 3 are evidenced by Table 6, both applications can analyze and find 10 files on the storage media but there is a change in the value of the digital evidence with the file names [BBD]3.doc and [BBD]4.pptx

Scheme 4 :

The storage medium stores 10 original files that are considered digital evidence and there is a name or date of modification on the digital file. In scheme 4, both FTK-Imager and the Autopssy software managed to obtain 10 digital proof files with hash marks.

The final results obtained after running scheme 4 show that both the FTK-Imager and Autopssy software can find and analyze 10 digital evidence files.

Reporting Stage

Based on the results of the results analysis stage, it can be concluded that the digital evidence contained in the storage media and executed in accordance with Scheme 1 and Scheme 4 is valid. It can be seen from the appearance of both processes in the software that there is no replacement or change in the hash value result. Thus, there is no defect in the authenticity of the evidence and can support material evidence to the judge in accordance with the provisions contained in the ITE Law Number 19 of 2016. Meanwhile, digital evidence with scheme 2 cannot be used as digital evidence because there is an erasure of the original file. Therefore, the storage media does not qualify as digital evidence and is submitted to the court, scheme 3 also cannot be used as valid evidence due to changes in the content of the original file [BBD] 3.doc and [BBD] 4.pptx.

CONCLUSION

Thus, based on the test results in scheme 1 and scheme 4, it is valid evidence because there is no change in the hash value which states that the deleted digital evidence has not undergone editing and is qualified as evidence according to ITE Law Number 19 of 2016. Meanwhile, the results of schemes 2 and 3 where digital evidence that is deleted or edited from storage media is considered invalid and not eligible to be submitted as digital evidence. The FTK-Imager and Autopssy applications are able to execute, produce, and complete what is expected of the author through the schema that has been created. FTK-Imager can perform analysis in a relatively short time, Autopssy can perform more complex and in-depth analysis. It is hoped that in further research, this research can be developed so that it can be used for forensic research results.

BIBLIOGRAPHY

[1] A. Doricchi *et al.*, "Emerging Approaches to DNA Data Storage : Challenges and Prospects," 2022, doi: 10.1021/acsnano.2c06748.

[2] J. B. Vala and V. M. Vekariya, "The Role and Importance of Digital Forensics and Digital Evidence in Cyber Crime Detection," *Int. J. Life Sci. Biotechnol. Pharma Res.*, vol. 13, no. 6, pp. 413–420, 2024, doi: 10.69605/ijlbpr.

[3] J. I. Ekotrans, S. Pratiwi, and B. Patmawanti, "Legal Review of the Use of Closed-Circuit Television as Electronic Evidence in Proving Criminal Acts in Indonesia," *J. Ilm. Ekotrans Erud.*, vol. 04, no. 01, pp. 134–141, 2024.

[4] A. Sukmasari, W. Frederik, M. E. Kalalo, and M. H. Soepeno, "Application Of Electronic Evidence As Extension Of Legal Civil Evidence Divorce Cases In Indonesia," *Int. J. Law, Environ. Nat. Resour.*, vol. 4, no. 1, pp. 1–14, 2024.

[5] F. Casaril, "Space cybersecurity governance : assessing policies and frameworks in view of the future," *J. Cybersecurity*, vol. 11, 2025, doi: 10.1093/cybsec/tyaf013.

[6] B. G. Bokolo and Q. Liu, "Artificial Intelligence in Social Media Forensics : A Comprehensive Survey and Analysis," *Electron.*, vol. 13, no. 9, 2024.

[7] S. Saeed, S. A. Suayyid, M. S. Al-ghamdi, H. Al-muhaisen, and A. M. Almuhaideb, "A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience," *Sensors (Basel).*, vol. 23, no. 16, pp. 1–27, 2023.

[8] B. Fakiha, "Unlocking Digital Evidence : Recent Challenges and Strategies in Mobile Device Forensic Analysis," *J. Interner Serv. Inf. Secur.*, vol. 14, no. 2, pp. 68–84, 2024, doi: 10.58346/JISIS.2024.I2.005.

[9] M. Zhang and M. Zhang, "Forensic imaging : a powerful tool in modern forensic investigation Forensic imaging : a powerful tool in modern forensic investigation," *Forensic Sci. Res.*, vol. 7, no. 3, pp. 385–392, 2022, doi: 10.1080/20961790.2021.2008705.

[10] F. Lubis, I. H. Shabri, S. A. Puspita, and C. N. Eprianty, "An

Analysis of the Validity of Digital Evidence in the Modern Technological Era," *Fox justi J. Ilmu Huk.*, vol. 15, no. 02, pp. 479–486, 2025, doi: 10.58471/justi.v15i02.

[11] M. Zou, "To use or not to use ? Understanding doctoral students ' acceptance of ChatGPT in writing through technology acceptance model," *Front. Psychol.*, vol. 14, no. October, pp. 1–9, 2023, doi: 10.3389/fpsyg.2023.1259531.

[12] G. Miller and E. Spiegel, "Guidelines for Research Data Integrity (GRDI)," *Sci. Data*, vol. 15, no. 25, pp. 1–8, 2025, doi: 10.1038/s41597-024-04312-x.

[13] B. Findlay, "Forensic Science International : Digital Investigation A review of thumbnail images artefacts in the Linux desktop and a methodology to add provenance to deleted fi les , using the thumbnail images artefact in combination with recent fi les history , and Trash artefacts," *Forensic Sci. Int. Digit. Investig.*, vol. 44, p. 301498, 2023, doi: 10.1016/j.fsidi.2022.301498.

[14] S. Vitali and M. Giuliani, "International Journal of Accounting Emerging digital technologies and auditing firms : Opportunities and challenges," *Int. J. Account. Inf. Syst.*, vol. 53, no. August 2023, p. 100676, 2025, doi: 10.1016/j.accinf.2024.100676.

[15] J. Wang and D. J. Gessler, "Adeno-associated virus as a delivery vector for gene therapy of human diseases," *Signal Transduct. Target. Ther.*, no. February, 2024, doi: 10.1038/s41392-024-01780-w.