IT Journal Research and Development (ITJRD)
Vol. 6, No. 2, March 2022, E-ISSN: 2528-4053 |P-ISSN: 2528-4061
DOI : 10.25299/itjrd.2022.8968

Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037:2012 and NIST SP800-86 Framework

Rizdqi Akbar Ramadhan[1], Panji Rachmat Setiawan[2], and Dedy Hariyadi[3]
Department of Informatics, Universitas Islam Riau[1,2]
Department of Computer Sciences, Universitas Jenderal Achmad Yani Yogyakarta[3]
rizdqiramadhan@eng.uir.ac.id[1], panji.r.setiawan@eng.uir.ac.id[2], dedy@unjaya.ac.id[3]

Article Info

Article history:
Received Nov 27, 2021
Revised Dec 21, 2021
Accepted Feb 19, 2022

Keyword:
Digital forensic
Non-volatile
Investigation
ISO/IEC 27037:2012
NIST SP800-86

ABSTRACT

In the implementation of Digital Forensics, one of the derivatives of practice is the handling of Digital Evidence. Handling Digital Evidence requires important steps and procedures. Digital evidence is a source of artifacts in handling a digital-based crime case, one of which comes from digital storage. In this research, the author will design a framework for Digital Forensic investigations by simulating digital evidence in the form of a non-volatile architecture. The reference commonly used by researchers in previous articles is the National Institute of Justice (NIST). The framework is a reference and steps in the practice of acquiring digital evidence. The purpose of designing this framework is as a legal procedure that is specifically implemented in the practice of acquiring non-volatile digital evidence. In the design, the author conducted a literature study on the NIST SP 800-86 and ISO 27037:2012 standards and then combined them in a hybrid terminology. The output of this research is to combine the two standards to become framework as reference for handling and investigating Digital Forensic science.

Corresponding Author:
Rizdqi Akbar Ramadhan
Department of Informatics
Universitas Islam Riau
Jalan Kaharudin Nasution No.113, Pekanbaru, Indonesia
rizdqiramadhan@eng.uir.ac.id

1. INTRODUCTION

In disclosing a crime with electronic and/or digital evidence, an approach using digital forensic methods is needed [1]. Therefore, digital forensics has a principle that the Digital Forensic Team needs to adhere to. The principles that the Digital Forensic Team needs to adhere to according to ISO 27037:2012 are to reduce the direct handling of electronic and/or digital evidence, have the

appropriate competence, document all digital forensic activities (logs), and comply with applicable laws and regulations.

Digital forensics is undergoing a branch of science development including computer forensics (computer forensics), operating system forensics (OS forensics), motion forensics (mobile forensics), video forensics (video forensics), image forensics (image forensics), audio forensics (audio forensics), network forensics (network forensics), malware forensics (malware forensics), cloud computing forensics (cloud forensics), and IoT forensics [2][3]. Almost all branches of digital forensics handle electronic evidence in the form of storage media in which there is digital evidence with non-volatile properties [4]. Non-volatile digital evidence is digital evidence that will not be lost when electronic evidence does not have a power supply. For example, files stored on hard disks, thumb drives, memory cards, etc. [5].

The United States Ministry of Commerce through the National Institute of Standards and Technology (NIST) issued instructions for handling electronic and/or digital evidence, namely NIST SP 800-86. NIST SP 800-86 has also regulated the process of securing non-volatile digital evidence based on a review of the data or operating system stored on electronic evidence. Based on this review, when securing digital evidence using two choices of methods of turning off the computer by forcibly unplugging the power cable or using the stages of turning off the computer from the operating system feature [6], unfortunately, carrying out the second stage causes the execution of the investigator which can reduce the essence of the chain. of custody. In previous studies that used ISO 27037:2012 in the process of securing non-volatile digital evidence, it was not explained in detail. This research only discusses the instruments used to evaluate the digital forensic process in general [7]. Whereas the ISO 27037:2012 document has regulated the process of securing non-volatile digital evidence. However, ISO 27037:2012 does not discuss the analysis and report writing process because ISO 27037 only focuses on Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. Based on the advantages and disadvantages of NIST SP 800-86 and ISO 27036:2012, this study proposes a framework for handling non-volatile digital evidence by combining the frameworks of NIST SP 800-86 and ISO 27037:2012.

2. RESEARCH METHOD

Based on research [8] there has been a description of the statement that Digital Forensic has a method. The method adopted in this case is Live Forensic and Static Forensic. Static Forensics has conventional steps and approaches where electronic evidence is processed by bit-by-bit images to carry out forensic processes. The forensic process itself runs on systems that are not on or running (off). For data storage that uses steady memory or nonvolatile memory as the media. Organizationally and computer architecture, in this case is the CPU (central processing unit) consisting of core components in the form of a Processor, Random Access Memory (RAM), as well as non-volatile storage media in the form of storage which is often called a hard disk [9]. Storage itself [10] is currently divided into two specifications, namely HDD (Harddisk Drive) and SDD (Solid State Drive). Computer technology in the 2020s era will be demanded for speed of access in operation, as well as efficiency in the use of power and volume, one of which is the use of Solid State Drives which are developments to replace the position of conventional Hard Drive Drives in data storage media [11].

Currently, it is divided into two storage architectures, namely conventional HDDs that use magnetic plates with a range of revolutions per minutes (RPM) from 5400 to 7200 RPM. Then on another storage architecture, namely Solid State Drive (SSD) which uses a digital controller (NAND Technology) which does not use magnetic disks. In contrast to image memory (volatile memory, such as RAM), data stored in nonvolatile storage tends not to be lost even though there is no electrical

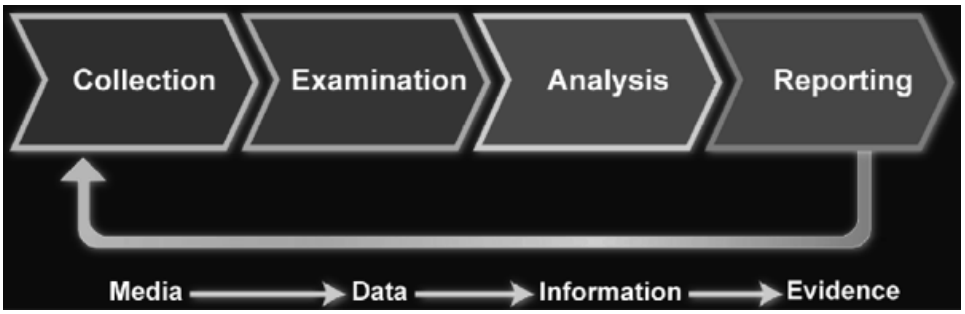

Figure 1. Digital Forensic Flow Standard by NIST SP 800-86

power. This applies to HDDs and SSDs with the TRIM-disable feature [5]. Static Forensic is focused on examining imaging results to analyze the contents of digital evidence, such as deleted files, web browsing history, file fragments, network connections, files accessed, user login history, etc. to create a timeline in the form of a summary of activities carried out on digital evidence. when used. An alternative to static analysis, or rather a complementary approach, is Live Forensic Analysis. In this case, all digital evidence is collected while the system is running. Live Forensic is able to cover some of the shortcomings of static analysis. However, on the other hand there are some issues for live forensics. The most important issue is that with live forensics the analyst's action is to execute on the system which causes changes to the digital evidence which in this case "was only discovered as alleged goods" [12]. Alteration or contamination of digital evidence is against the principles of digital forensics [13]. There are several other problems with live forensics, one of which is that the investigator may not have a verified level of rights regarding access to the system under investigation.

Figure 1 is a digital forensic stage from NIST SP 800-86 as a reference in various research and implementation in the field, including this research. This is because the forensic stages presented by NIST make it easier to handle electronic and/or digital evidence. The digital forensic stage adopted in this study is from the collection stage, namely the stage of collecting and/or securing electronic and/or digital evidence. The second stage, examination is the stage of extracting electronic and/or digital evidence that has been collected and/or secured without reducing the authenticity of electronic and/or digital evidence. The third stage, analysis is the stage of conducting an analysis to find out more about matters related to crime. The last stage, reporting is the stage of presenting the findings at the analysis stage in the form of reporting which will be used for the next law enforcement process.

Furthermore, in securing digital evidence stored on electronic evidence in the form of storage media, security procedures are also regulated through ISO 27037:2012. In this study, the digital evidence handled was stored in electronic evidence in the form of storage media such as hard disks. In the picture below that digital evidence does not depend on the availability of electricity, the choice is to unplug the computer cable from the power source or perform the shutdown process if the device is in an unstable condition described in figure 2. Previous research discussed the merging of two frameworks, namely ACPO and SNI ISO/IEC 27037:2014 regarding the acquisition of CCTV evidence [14]. However, this study does not provide an overview related to the comparison of the two digital forensic frameworks. So the stage of this research is to compare two digital forensic frameworks, namely NIST SP 800-86 and ISO 27037:2012. The comparison method is to show the advantages and disadvantages of each framework. From the results of the comparison, this method hopely will become a new guide in handling non-volatile digital evidence in order to make it easier for the Digital Forensic Team. The comparison table of the advantages and disadvantages of the NIST SP 800-86 and ISO 27037:2012 framework can be seen in the following table 1.

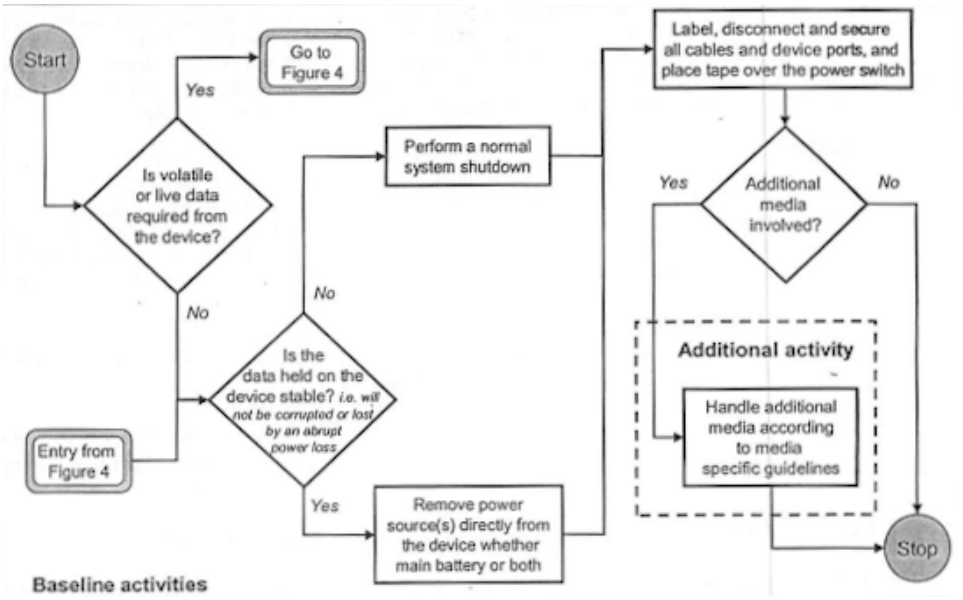

Figure 2. Security Procedures Through ISO 27037:2012

Table 1. Matrix Comparison of Each Reference

References	Weakness	Strength
NIST SP 800-86	Instructions for Securing Evidences	Digital Forensic Stages
ISO/IEC 27037:2012	Digital Forensic Stages	Instructions for Collecting Evidences

3. RESULT AND ANALYSIS

NIST SP 800-86 also mentions the process of securing digital evidence stored on storage media on a computer. However, it is not explained in more detail as in ISO/IEC 27037:2021. Two processes that can be carried out to secure electronic evidence are unplugging the cable from the power source and turning off the computer in accordance with the operating system features that have the possibility of losing digital evidence in the form of files related to closing open, files related to temporary deletion, and related files. with swaps. This is certainly different from ISO/IEC 27037:2012 which regulates the condition of the device.

ISO/IEC 27037:2012 also regulates the process of collecting electronic evidence or securing potential digital evidence from various factors. The factors that must be considered include:

1. Dependency term on the power source.
2. Encryption method (depend on kernel or user customization) that used on storage media.
3. The level of urgency in an organizational/institutional system.
4. Requirements and regulations that apply in the organization/institution.

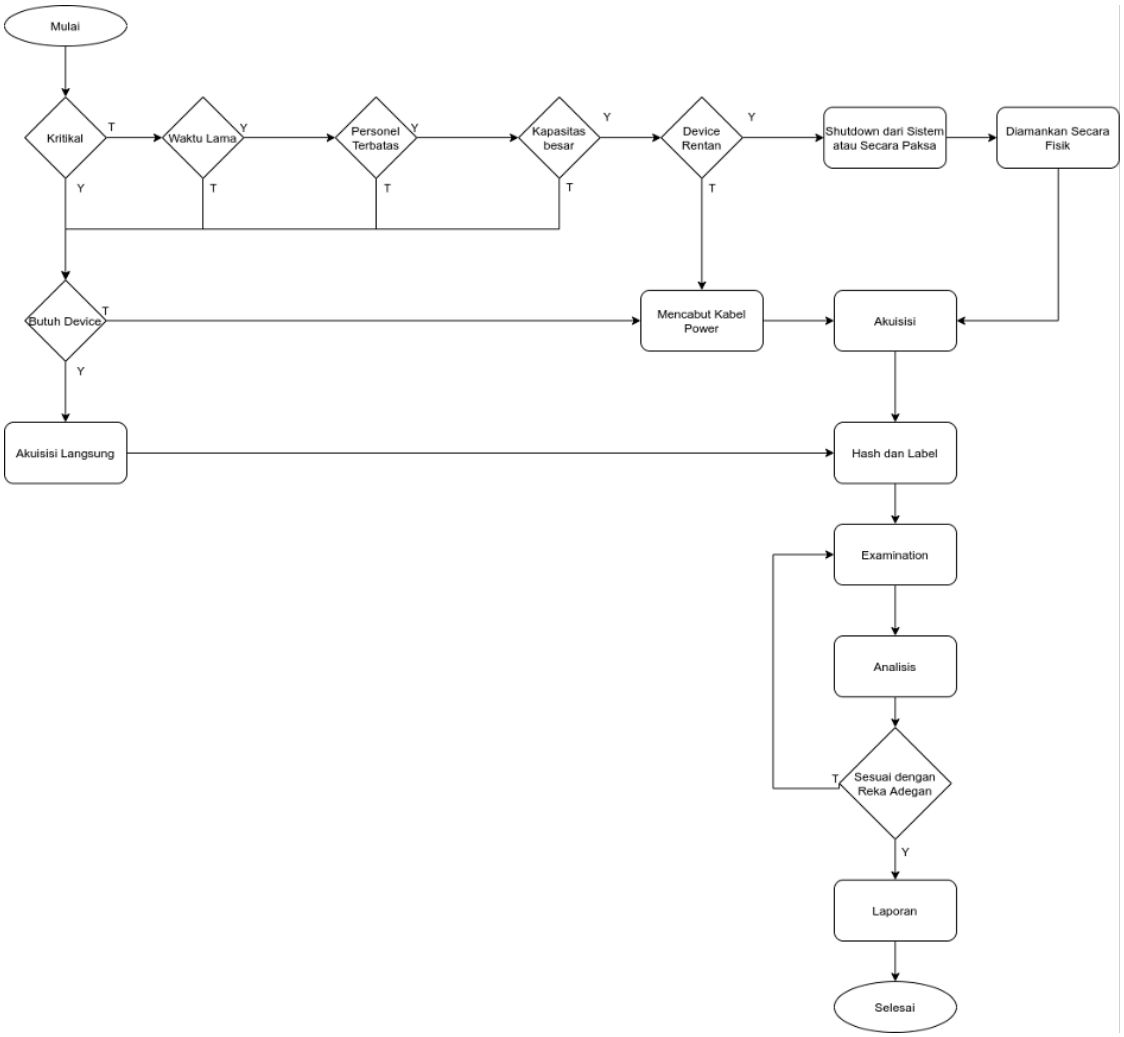

Figure 3. Framework Design Results

5. Large capacity and volume of storage media.
6. Availability of the crime scene team.
7. Availability of time required by the crime scene team.

Based on the comparison of the process of collecting electronic evidence and securing potential digital evidence of the two standards, NIST SP-800-86 and ISO/IEC 27037:2012, there are several advantages and disadvantages. So in this study, improvements were made by comparing the two standards. The table below is a comparison matrix of the advantages and disadvantages of NIST SP-800-86 and ISO/IEC 27037:2012. Matrix in the table above, to simplify and strengthen the procedure for collecting electronic evidence in the form of storage media and securing non-volatile digital evidence, it is necessary to create a comprehensive flow diagram. The picture below is a flow diagram for collecting electronic evidence in the form of storage media and securing digital evidence stored on storage media. The flow diagram considers various factors that have been determined in ISO/IEC 27037:2012 and follows the forensic steps on NIST SP-800-86.

4. CONCLUSION

According on the research showed above, each standardization has advantages and disadvantages. Therefore, the integration of NIST SP-800-86 standardization and ISO/IEC 27037:2012 strengthens the digital forensic framework. The resulting framework is more perfect because it considers several things including: critical factors, time, personnel, storage media capacity in this case is electronic evidence, and the nature of the vulnerability of digital device systems. As for the digital forensic process, each standardization has stages that are in accordance with the basic rules of digital forensics, both the process of collecting and securing electronic and/or digital evidence. This study has a weakness, namely the framework resulting from the integration of the NIST SP-800-86 standard and ISO/IEC 27037:2012 has not been field tested with the Law Enforcement Apparatus. It is hoped that this framework can be applied by the Digital Forensic Team of Law Enforcement Officials.

REFERENCES

[1] D. Hariyadi, A. A. Huda, A. Priadana *et al.*, "Laron v2: Pengembangan aplikasi forensik logikal untuk mengakusisi percakapan whatsapp di android," *SMARTICS Journal*, vol. 7, no. 1, pp. 7–13, 2020.

[2] S. Dogan and E. Akbal, "Analysis of mobile phones in digital forensics," in *2017 40th international convention on information and communication technology, electronics and microelectronics (MIPRO)*. IEEE, 2017, pp. 1241–1244.

[3] M. N. Al-Azhar, "Digital forensic: Panduan praktis investigasi komputer," *Jakarta: Salemba Infotek*, 2012.

[4] D. Hariyadi, "Komparasi penanganan barang bukti elektronik dan/atau barang bukti digital sesuai sop pusat laboratorium forensik polisi republik indonesia," 2014.

[5] R. A. Ramadhan, Y. Prayudi, and B. Sugiantoro, "Implementasi dan analisis forensika digital pada fitur trim solid state drive."

[6] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Sp 800-86. guide to integrating forensic techniques into incident response," 2006.

[7] D. Sudyana, Y. Prayudi, and B. Sugiantoro, "Analysis and evaluation digital forensic investigation framework using iso 27037: 2012," *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, vol. 8, no. 1, pp. 1–14, 2019.

[8] M. Rafique and M. Khan, "Exploring static and live digital forensics: Methods, practices and tools," *International Journal of Scientific & Engineering Research*, vol. 4, no. 10, pp. 1048–1056, 2013.

[9] A. Aljaedi, D. Lindskog, P. Zavarsky, R. Ruhl, and F. Almari, "Comparative analysis of volatile memory forensics: live response vs. memory imaging," in *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing*. IEEE, 2011, pp. 1253–1258.

[10] B. Raj and R. Hubbard, "Forensics analysis of solid state drive (ssd)," in *Proc. 2016 Univers. Technol. Manag. Conf*, 2016, pp. 1–11.

[11] R. A. Ramadhan and D. Mualfah, "Implementasi metode national institute of justice (nij) pada fitur trim solid state drive (ssd) dengan objek eksperimental sistem operasi windows, linux dan macintosh," *IT Journal Research and Development*, vol. 5, no. 2, pp. 183–192, 2020.

[12] F. Adelstein, "Live forensics: diagnosing your system without killing it first," *Communications of the ACM*, vol. 49, no. 2, pp. 63–66, 2006.

[13] M. M. Pollitt, "The digital crime scene," in *Handbook of Digital and Multimedia Forensic Evidence*. Springer, 2008, pp. 65–76.

[14] D. Hariyadi, F. E. Nastiti, and F. N. Aini, "Framework for acquisition of cctv evidence based on acpo and sni iso/iec 27037: 2014," in *Int. Conf. Informatics Dev*, 2018.

BIOGRAPHY OF AUTHORS

Rizdqi Akbar Ramadhan obtained Bachelor Degree in Master of Informatics from Universitas Islam Indonesia in 2016. His research field include Digital Forensic, Cyber Security, and Mobile Platform technology interests. He has been a Lecturer with the Department of Informatics Engineering, Universitas Islam Riau, since 2017. Apart from teaching as a lecturer, he is also involved in the court realm as an expert witness and is a regular resource person on Radio Republik Indonesia (RRI).

Panji Rachmat Setiawan is a lecturer of the Department of Informatics Engineering, Universitas Islam Riau, Indonesia. Obtained his bachelor Informatics Engineering at Universitas Bina Nusantara, also known as Binus University, Jakarta, in 2009, and his master Management Information System at Universitas Bina Nusantara, Jakarta, in 2012. He is a Trainer for Java Programming (Object-Oriented Programming), and Mobile Programming.He is now involved in several projects for research in the field of mobile technology. His current research interests include mobile technology, block chain, and system designer.

Dedy Hariyadi obtained Graduate of Master of Informatics at the Islamic Universitas Islam Indonesia with a concentration in Digital Forensics who is currently active as a lecturer and researcher at Universitas Jenderal Achmad Yani Yogyakarta. His research field is Cyber Security. Apart from conducting research at Universitas Jenderal Achmad Yani Yogyakarta, he is also active at PT Widya Adijaya Nusantara as VP of Technology.