Jurnal Teknik Informatika (JUTIF)
Vol. 4, No. 4, August 2023, pp. 867-873

DOI: https://doi.org/10.52436/1.jutif.2023.4.4.1212
p-ISSN: 2723-3863
e-ISSN: 2723-3871

FORENSIC RECOVERY ANALYSIS OF LOST RAID 0 CONFIGURATION ON NETWORK ATTACHED STORAGE AS EVIDENCE IN COURT

Dani Karsa Prawira[1], Beny Nugraha [2], Marza Ihsan Marzuki*[3]

[1]Master of Electrical Engineering, Faculty of Engineering, Universitas Mercu Buana, Jakarta Indonesia
[2]Technische Universität Chemnitz, Germany
[3]Department of Electrical Engineering, Faculty of Industrial Technology, Universitas Pertamina, Indonesia
Email: [1]Dani.prawira@gmail.com , [2]beny.nugraha@etit.tu-chemnitz.de, [3]marza.im@universitaspertamina.ac.id

(Article received: July 13, 2023; Revision: July 25, 2023; published: August 21, 2023)

Abstract

In the modern world of globalization, Digital Forensic science has emerged as a pivotal investigative tool for solving complex cases. This discipline proves particularly effective in deciphering digital evidence. In this study, we ventured to examine a Network Area Storage (NAS) device, specifically one containing three hard disks. Our objective was to validate that the Hash value generated before the duplication process matches identically with the Hash value post-imaging or duplication. Our findings demonstrate that through reconfiguration and recovery of RAID 0, previously deleted files can be restored using the methods outlined in our research. In essence, this study establishes that: (1) Reconstruction of RAID configurations is feasible, (2) Recovery of deleted files from a RAID 0 system is achievable, and (3) Such restored data can serve as admissible evidence in court.

Keywords: *Digital Forensics, Electronic Evidence, Raid 0, Raid Reconstruction, Raid Recovery,*

1. INTRODUCTION

As we delve into the realm of cybercrime investigation, the utility of Digital Forensic techniques in uncovering facts and gathering evidence is unmistakable. This is evident in the tasks performed by law enforcement—acquiring digital evidence through investigation, prosecution, and enforcement stages.

Storage servers, often the prime targets of cybercriminals due to their substantial storage capacity, are typically network-connected and referred to as NAS (Network Attached Storage). NAS configurations, including standard RAID setups like JBOD, Level 0, 1, 5, and 6, are complex and warrant careful attention when data acquisition is required from these RAID servers.

Research on the acquisition and data management of RAID servers using Digital Forensic techniques is somewhat scarce. However, notable insights can be gleaned from NISTIR 7276, a US publication by Steve Mead in 2005, which states:

a. RAID systems do not permit direct access to the underlying storage media within the array, whether via the BIOS or the Operating System. This restriction means that RAID volumes limit access to the individual storage media used within the array.
b. For active RAID systems acquired through imaging (capturing the entire contents of the media within the RAID array), the resulting hash values will differ. In parallel RAID arrays (RAID-0, RAID-5), it's posited that the data contained on each individual drive within the array is distinct.
c. Specific steps must be laid out for reconstructing the RAID server post the acquisition (imaging) process. If the RAID is acquired and the acquisition results are stored on non-RAID media, then no additional processing is needed.

In determining a RAID configuration, researchers must be able to determine the type of RAID configuration used on the storage media taken. Determining this configuration will determine the success of the type of reconstruction to be carried out and if you cannot determine the type of configuration in question, it is certain that the reconstruction and recovery of deleted files will not be successful. To be able to determine this type of configuration, researchers must perform a sector-to-sector analysis on a disk so that they can determine the type of RAID used

As per Article 43 paragraph 2 of Law No. 11/2008 on Electronic Information and Transactions (ITE Law), " Investigations in the field of Information Technology and Electronic Transactions as referred to in paragraph (1) are carried out with due observance of the protection of privacy, confidentiality, smooth running of public services, data integrity or data integrity in accordance with the provisions of Laws and Regulations."

The purpose of this research is (i) To conduct testing on the media to be examined and analyze the procedures and best practices for duplicating electronic devices from NAS. (ii) To analyze forensic file images obtained from the imaging process in order to obtain corresponding hash values. (iii) To analyze and reconstruct the RAID 0 configuration, enabling the recovery process for deleted files to be restored.

The results of this research are highly correlated with the ITE Law Article 43 paragraph 2 No.11/2008, especially in the research method used, which aims to maintain data integrity from digital evidence. In addition, the law in that article also states that activities in the investigation process must pay attention to the smooth running of public services, meaning that this research is very much in line with what is stated in the law.

The benefits of this research are as a contribution of thought and study in a new approach to recovering RAID 0 server data through the Digital Forensic acquisition method of a RAID 0 lost configuration, as well as providing guidelines in accordance with guidelines for handling electronic evidence in court.

2. RESEARCH METHODS

Our research employed a method that involved conducting tests on a chosen media. This ranged from the initial data acquisition stage from the Test Media Storage Server to the finalization of the data recovery process, corroborated by hash values. The goal was to achieve identical hash values for storage media or files housed in the RAID 0 system on the Storage Server. Research method can be seen in Figure 1.

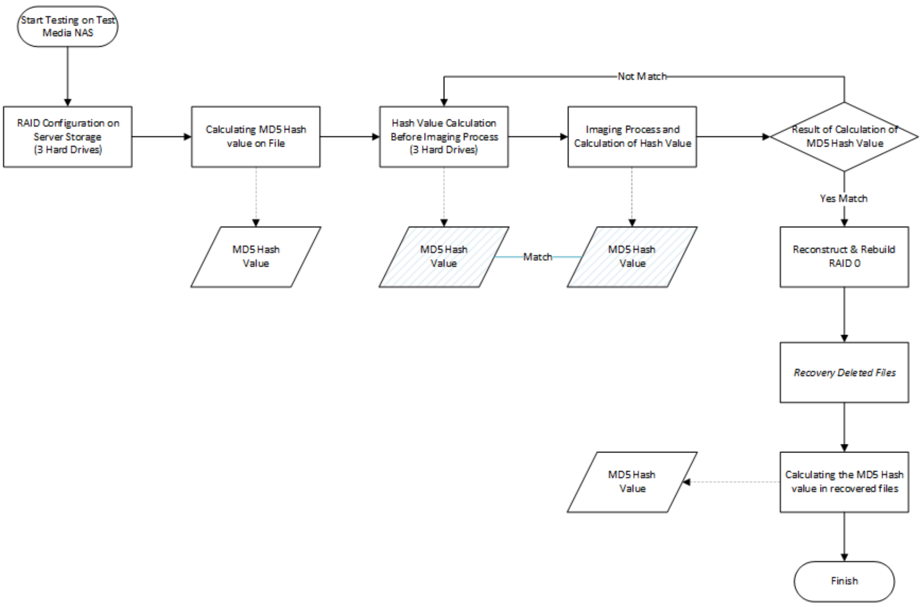


Figure 1 - Testing Flowchart

To carry out this testing, we employed the following hardware and software, for the hardware can be seen in Table 1 and for the software can be seen in Table 2

a. Hardware

Table 1 - Hardware Testing Equipment

No	Hardware	Specification	Figure
1	Laptop	Merk: Lenovo Thinkpad T460, Processor Intel Core i7-6600U @2.60GHz, RAM : 8GB DDR3, SSD 256GB, VGA Intel HD Graphics 520	
2	NAS	Plug Type : US Plug, Size : 194*255*184mm, Interface : SATA External MPN : ORICO OS400 Feature 4 : Hard Drive Enclosure With RAID, Model Number : OS400 Built-in Power : 250W	
3	Hard Disk 1	Product Name : Caviar Blue WD5000AAK, Serial Number : WCC6Z2ZHX99K, Brand: Western Digital	

No	Hardware	Specification	Figure
4	Hard Disk 2	Drive Capacity : 500 GB Product Name : Caviar Blue WD5000AAKX Serial Number : WCC6Z0NJAAZ2, Brand: Western Digital	
5	Hard Disk 3	Drive Capacity : 500 GB Product Name : Caviar Blue WD5000AAKX, Serial Number :WCC6Z0NJA39F, Brand: Western Digital	
6	Hard Disk	Drive Capacity : 500 GB Product Name : WD Scorpio, Blue 2TB, Brand : Western Digital, Series : Scorpio Blue, Capacity: 2000GB	
7	Dongle X-Ways	Weight: approx. 7 g ~ 110 grains ~ 1/4 ounce Dimensions: 5.3 × 1.7 × 0.7 cm or 2.07 × 0.62 × 0.37 inches Certifications: CE, FCC	
8	Enclosure Hdd 3.5	Hard Disk Interface: Serial ATA, Brand: ORICO, 3.5 Inches, Mechanical Hard Disk	

b. Software

Table 2 - Software Testing Tools

No	Software	Description
1	Operating System	Edition: Windows 10 Pro Version : 22H2 Installed on: 10/12/2020 OS build: 19045.2486 Experience: Windows Feature Experience Pack: 120.2212.4190.0
2	X-Ways Forensics	•Disk cloning and imaging •Ability to read partitioning and file system structures inside raw (.dd) image files, ISO, VHD, VHDX, VDI, and VMDK images •Complete access to Disks, RAIDs, and images more than 2 TB in size (more than 232 sectors) with sector sizes up to 8 KB •Built-in interpretation of JBOD, RAID 0, RAID 5, RAID 5EE, and RAID 6 systems, Linux software RAIDs, Windows dynamic Disks, and LVM2
3	FTK Imager	FTK Imager is an open-source software by AccessData that is used for creating accurate copies of the original evidence without actually making any changes to it. The Image of the original evidence is remaining the same and allows us to copy data at a much faster rate, which can be soon be preserved and can be analyzed further
4	Disk Internal RAID Recovery	Repair Data from Corrupted RAID 0-6 Arrays
5	Orico HW RAID Manager	Software used to create RAID configurations on Orico hardware
6	Write Blocker	Digital forensic application that functions to block computer modification capabilities of evidence connected to write blocker equipment so that data is not intentionally or unintentionally written to digital evidence

To ensure the reliability of the use of tools, researchers have ensured that the tests carried out have used tools that have been tested for feasibility. Like the use of software called FTK Imager, this software has been tested through the Computer Forensics Tool Testing (CFTT) program by Homeland Security (https://www.dhs.gov/sites/default/files/publications/test_results_for_ftk_imager_version_4.3.0.18_with_coverjd1gd2.pdf). In addition, researchers also use software called X-Ways, this software has also been tested by NIJ (National Institute of Justice) related to the Digital Data Acquisition Tool (https://www.ojp.gov/pdffiles1/nij/236224.pdf). As for the validity of the results tested, namely the Hash value, the researcher has conducted several repeated tests of the hash value generated from the storage media and the results always have a constant or fixed hash value.

Pertaining to Experimental Research, it is crucial to note that the experiment is classified into four categories: single-subject experimental, weak experimental, quasi-experimental, and true experimental. In this research, we undertook a single-subject experimental study, wherein a sequence of actions was executed on a singular electronic device located in a RAID 0 server. In addition, this single experimental study aims to find out how much influence a treatment has given to the subject repeatedly within a certain time, meaning that the researcher wants to do the test repeatedly so that the validity of the test results gets the same value.

3. RESULT

3.1. Results of the Research Process on RAID 0

In this experiment, we initiated by setting up a RAID 0 configuration on the NAS, utilizing three hard disk units as our storage media. We then obtained hexadecimal values for each sector by identifying the RAID type on the formed Disk Volume, the identifying can be seen in Figure 2

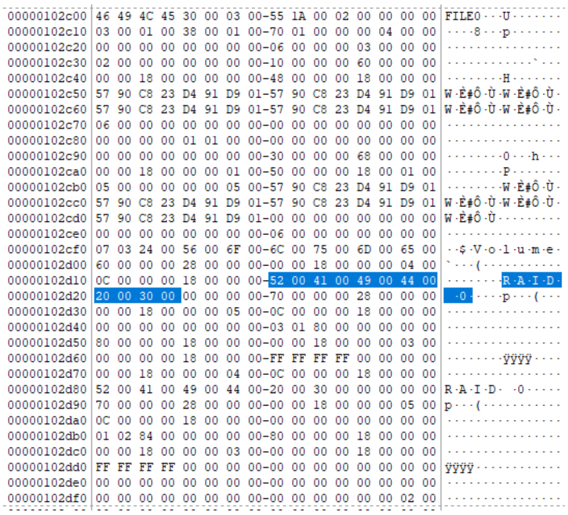
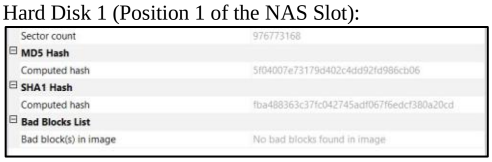
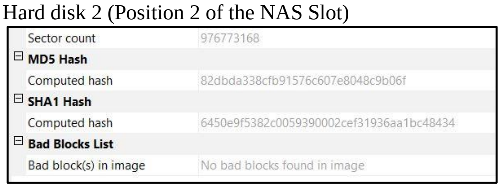
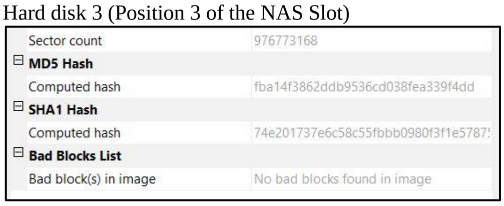


Figure 2 - Information RAID 0 on Disk

As a point of reference or initial parameter, we calculated the hash values on each hard disk. The MD5 hash values can be seen in Table 3

Table 3 - Hash Information on Hard Disk

<table>
<tr><th>No</th><th>Hard disk Information</th></tr>
<tr><td>1</td><td>Hard Disk 1 (Position 1 of the NAS Slot):

Sector count | 976773168
MD5 Hash
Computed hash | 5f04007e73179d402c4dd92fd986cb06
SHA1 Hash
Computed hash | fba488363c37fc042745adf067f6edcf380a20cd
Bad Blocks List
Bad block(s) in image | No bad blocks found in image
MD5 Hash: 5F04007E73179D402C4DD92FD986CB06</td></tr>
<tr><td>2</td><td>Hard disk 2 (Position 2 of the NAS Slot)

Sector count | 976773168
MD5 Hash
Computed hash | 82dbda338cfb91576c607e8048c9b06f
SHA1 Hash
Computed hash | 6450e9f5382c0059390002cef31936aa1bc48434
Bad Blocks List
Bad block(s) in image | No bad blocks found in image
MD5 Hash: 82DBDA338CFB91576C607E8048C9B06F</td></tr>
<tr><td>3</td><td>Hard disk 3 (Position 3 of the NAS Slot)

Sector count | 976773168
MD5 Hash
Computed hash | fba14f3862ddb9536cd038fea339f4dd
SHA1 Hash
Computed hash | 74e201737e6c58c55fbbb0980f3f1e5787
Bad Blocks List
Bad block(s) in image | No bad blocks found in image
MD5 Hash: FBA14F3862DDB9536CD038FEA339F4DD</td></tr>
</table>

Subsequently, we conducted forensic imaging on each hard disk using X-ways Forensic Imager, with the aim of enabling RAID reconstruction. The results of the forensic imaging process, can be seen in Table 4

Table 4 – Information of Imaging Process

No	No Hard disk	Logs	Hash MD5
1	Hard Disk 1 (Position 1 of the NAS Slot	Model: WDC WD50 00AZLX-08K2TA0 Serial No.: 152D00539000 Total capacity: 500.107.862.016 bytes = 466 GB Bytes per sector: 512 Sector count: 976.773.168	5F04007 E73179D 402C4D D92FD98 6CB06
2	Hard Disk 2 (Position 2 of the NAS Slot	Model: TO Exter nal USB 3.0 Serial No.: 2015033100081 Total capacity: 500.107.862.016 bytes = 466 GB Bytes per sector: 512 (logically) Bytes per sector: 4.096 (physically) Sector count: 976.773.168	82DBDA 338CFB9 1576C60 7E8048C 9B06F
3	Hard Disk 3 (Position 3 of the NAS Slot)	Model: WDC WD50 00AZLX-08K2TA0 Serial No.: 152D00539000 Total capacity: 500.107.862.016 bytes = 466 GB Bytes per sector: 512 Sector count: 976.773.168	FBA14F3 862DDB 9536CD0 38FEA33 9F4DD

After executing the hashing and imaging processes on the three hard disks, the derived hash results were identical. This indicates that there was no alteration in the hash values from the initial hashing process to the imaging process across all three hard disks. The Hash can be seen in Table 5

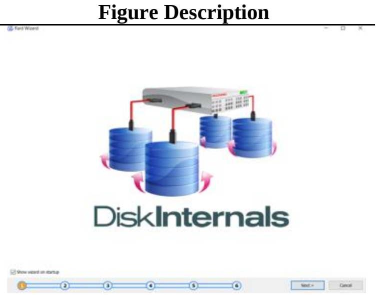
Table 5 - Hash Value Comparison Information

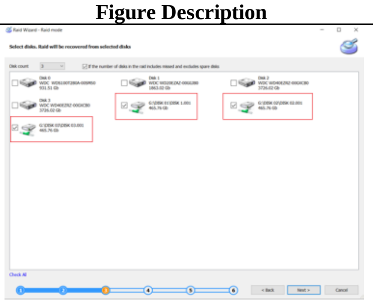
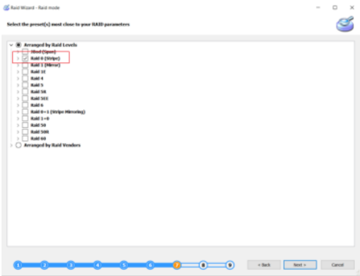
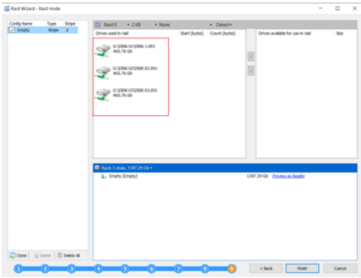
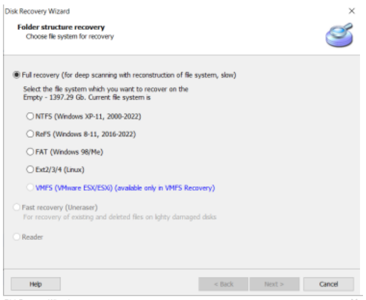
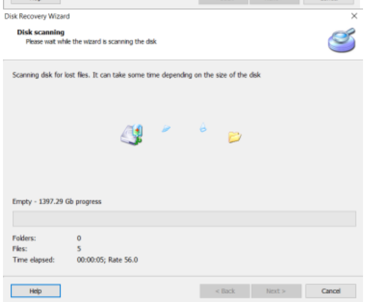
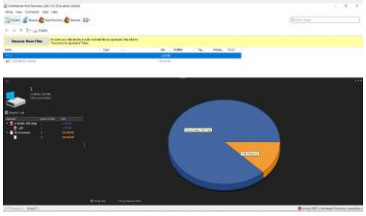
	Calculation Hash before Imaging	Calculation Hash After Imaging
Disk 01	5F04007E73179D402 C4DD92FD986CB06	5F04007E73179D402C4 DD92FD986CB06
Disk 02	82DBDA338CFB9157 6C607E8048C9B06F	82DBDA338CFB91576 C607E8048C9B06F
Disk 03	FBA14F3862DDB953 6CD038FEA339F4DD	FBA14F3862DDB9536 CD038FEA339F4DD
Result	Match	

3.2. Research Results of Deleted File Recovery on RAW Image Files through RAID Reconstruction

In the final stage of our testing, we employed a different recovery application to obtain supplementary results regarding features and functions. The processes were conducted during the testing through RAID 0 configuration reconstruction can be seen in Table 6

Table 6 – File recovery on RAID

No	Testing Step	Figure Description
1	Using the Reconstructio n or RAID Recovery Feature in the Application	 DiskInternals

No	Testing Step	Figure Description
2	Using the Image File from each previous Disk	
3	Determine the type of RAID to be reconstructed or recovered	
4	Perform combination according to the disk order in the RAID configuration	
5	Perform recovery on the RAID that has been formed and determine the File System to be constructed	
6	Perform Scanning Process for lost files	
7	Process Results Recovery deleted files	

3.3. Comparison analysis of metadata information between the test file and the recovered file.

For this analysis, we utilized two distinct software to perform the comparison. The outcomes of this comparison are illustrated in the ensuing comparison table:

a. Comparison Results of Hash Values on Storage Media in the Form of Hard Disk can be seen in Table 7

Table 7 – Results of Comparison of metadata values in files

No	Storage Media	Hash Value Calculation on Original Hard Disk Before Imaging	Hash Value Calculation after Imaging Process	Result of Hash Value Similarity
1	*Hard disk 01*	5F04007E7317 9D402C4DD92 FD986CB06	5F04007E7 3179D402 C4DD92F D986CB06	*Match*
2	*Hard disk 02*	82DBDA338CF B91576C607E8 048C9B06F	82DBDA33 8CFB9157 6C607E804 8C9B06F	*Match*
3	*Hard disk 03*	FBA14F3862D DB9536CD038 FEA339F4DD	FBA14F38 62DDB953 6CD038FE A339F4DD	*Match*

The results of the same hash value are very important in this research, because with the same value it can prove that the handling of digital evidence is in accordance with the rules and procedures, in general it can be used as electronic evidence in court. In addition, the same hash value also proves that no data has changed so that the data integrity of digital evidence is maintained.

b. Comparison of Metadata Value Results in a files can be seen in Table 8

Table 8 – Comparison Results of Hash Values on Hard Drives

Test files		***Recovery Result Files***		**Metadata Similarity Results**
Metadata File	***MD5 Hash***	***Metadata File***	***MD5 Hash***	
Match	has a Hash value	Match	Not identified	Has the same metadata but doesn't have the same hash

c. Comparison Time Results in each Test Process can be seen in Table 9.

Table 9 – Process time comparison results

No	Testing Process	Information of Disk		
		Disk 01	Disk 02	Disk 03
1	Disk Sterilization Time (Wiped) with Sector 0	40 Minute	43 Minute	48 Minute
2	RAID 0 Build or Configuration Time		10 Minute	
3	Hashing Process Time Before Imaging Process	57 Minute	59 Minute	60 Minute

No	Testing Process	Information of Disk		
		Disk 01	Disk 02	Disk 03
4	Process time for making duplication by imaging method (raw)	59 Minute	61 Minute	65 Minute
5	RAID Configuration or Rebuild Time		10 Minute	
6	RAID 0 Recovery Process Time		530 Minute	

4. DISCUSSION

This research was carried out with several limitations faced by the author, namely the RAID configuration used was only limited to RAID 0, media storage, namely hard disks, was only limited to 3-units with a capacity of 500 Gb each, the files used were limited to only 7 files with PDF extension only and the most significant is the software used in this study has limited features due to licensing issues that are not owned by the author factor due to cost.

Therefore, with the limitations of this study, the authors suggest that further research can use methods or additional tools by looking at the limitations mentioned by previous authors, so that the results obtained are more accurate, efficient and measurable.

5. CONCLUSION

Reflecting on our testing, we are able to establish the following conclusions:

- The integrity of the data within this study is affirmed by the unaltered hash value. Beyond hash parameters, data integrity can also be gauged by comparing the metadata values of the files.
- Reconstruction is attainable, provided the RAID type used in the prior configuration is identified and suitable software supporting that RAID configuration is procured.

BIBLIOGRAPHY

[1] Ramazan OĞUZ, Yiğithan YILMAZ, “Investigation of RAID Systems in Terms of Forensics”, 2023, AJIT-e: Academic Journal of Information Technology, 14 (53) , 142-161.

[2] Edgar Joseph Ronny Pangaribuan, “Keamanan Informasi dan Tren Serangan Tahun 2022”, 2022, https://www.djkn.kemenkeu.go.id/kpknl-medan/baca-artikel/15179/Keamanan-Informasi-dan-Tren-Serangan-Tahun-2022.html, (Accessed Aug 18, 2022)

[3] Seagate, “Apa itu NAS (Network Attached Storage) dan Mengapa NAS Penting untuk Usaha Kecil?”, 2022, https://www.seagate.com/id/id/tech-insights/what-is-nas-master-ti/ (Accessed Sept 20, 2022)

[4] Ravi Kumar M G, Ayudh Nagaraj, Benjamin Paul, Sharat P Dixit, “Network Attached Storage: Data Storage Applications”, 2021, Turkish Journal of Computer and Mathematics Education Vol.12 No.12 (2021) 2385-2396.

[5] Christianingrum R., Aida A., “Tantangan Penguatan Keamanan Siber dalam Menjaga Stabilitas Keamanan”, 2021, Analisis RUU Tentang APBN No. 13/an.PKA/APBN/IX/2021, Pusat Kajian Anggaran Badan Keahlian Sekretariat Jenderal Dewan Perwakilan Rakyat Republik Indonesia

[6] Iman, N., Susanto, A. and Inggi, R., “Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review)”, 2020, Jurnal Telekomunikasi dan Komputer, 9(3), p.186.

[7] Jayantari, I.G.A.S. and Sugama, I.D.G.D., “Kekuatan Alat Bukti Dokumen Elektronik dalam Tindak Pidana Berbasis Teknologi dan Informasi (Cyber Crime)”, 2019, e-Jurnal Ilmu Hukum Kertha Wicara, 8(6), pp.1–16.

[8] Ivanović, A., “The Way of Handling Evidence of Criminal Offences of Computer Crime”, 2018, Criminal Justice and Security in Central and Eastern Europe.

[9] Hyunji Chung, Jungheum Park, Sangjin Lee, Chulhoon Kang. “Digital Forensic Investigation of Cloud Storage Services” 2017, 1709.10395. https://arxiv.org/ftp/arxiv/papers/1709/

[10] Handoko, C., “Kedudukan Alat Bukti Digital dalam Pembuktian Cybercrime di Pengadilan”. 2016, Jurisprudence, 6(1), pp.1–15.

[11] Kartika Imam Santoso, Muhamad Abdul Muin. “Implementasi Network Attached Storage (NAS) menggunakan NAS4Free untuk Media Backup File”. 2015, Scientific Journal of Informatics Vol. 2, No.2, November 2015 e-ISSN 2460-0040.

[12] Granja, F.M. and Rafael, G.D.R, “Preservation of Digital Evidence: Application in Criminal Investigation. In: 2015 Science and Information Conference (SAI)”, 2015, Science and Information Conference (SAI). London, United Kingdom: IEEE.pp.1284–1292.

[13] Sun, J.-R., Shih, M.-L. and Hwang, M.-S, “A Survey of Digital Evidences Forensic and Cybercrime Investigation Procedure. International Journal of Network Security”, 17(4), pp.497–509.2015

[14] Budi Rahardjo, “Sekilas Mengenai Forensik Digital”, 2013, Jurnal Sosioteknologi, FSRD-ITB, Edisi 29, Tahun 12, Agustus 2013, hal 384-387.

[15] K. K. Sindhu, Dr. B. B. Meshram, “Digital Forensic Investigation Tools and Procedures”, 2012, I.J. Computer Network and Information Security, 2012, 4, 39-48.

[16] Kailash Kumar, Sanjeev Sofat, S.K.Jain, Naveen Aggarwal. “Significance of Hash Value Generation in Digital Forensic”, 2012, International Journal of Engineering Research and Development Volume 2, Issue 5, PP.64-70 e-ISSN: 2778-067X.

[17] G. C. Kessler, “Advancing the Science of Digital Forensics, in Computer”, 2012, vol. 45, no. 12, page. 25-27, Des. 2012, doi: 10.1109/MC.2012.399.

[18] Vassil Roussev, “Hashing and Data Finger printing in Digital Forensics.”, 2012, ieeexplore.ieee.org ieee security and privacy PP.49-551540-7993/09

[19] Vincent Urias, Curtis Hash, Lorie M. Liebrock, “Consideration of Issues for Parallel Digital Forensics of RAID Systems”. 2009, Journal of Digital Forensic Practice P-ISSN: 1556-7281 ISSN: 1556-7346.

[20] Harish Daiya, Maximillian Dornseif, Felix C. Freiling, “Testing Forensic Hash Tools on Sparse Files”, 2007, ieeexplore.ieee.org IMF 2007, Stuttgart.

[21] M. Steve, “The Impact of RAID on Disc Imaging, National Institute of Standards and Technology”, 2005, page.11