ILKOM Jurnal Ilmiah Vol. 16, No. 3, December 2024, pp. 283-295
Accredited 2nd by RISTEKBRIN No. 200/M/KPT/2020; E-ISSN 2548-7779 | P-ISSN 2087-1716

Research Article Open Access (CC–BY-SA)

File carving Analyze of Foremost and Autopsy on external SSD mSATA using the Association of Chief Police Officer Method

Khoirul Anam Dahlan [a,1,*]; **Anton Yudhana** [a,2]; **Herman Yuliansyah** [a,3]
[a] *Universitas Ahmad Dahlan, Jl. Kapas 9, Semaki, Umbulharjo, Yogyakarta 55166, Indonesia*
** Corresponding author*

Article history: Received September 04, 2024; Revised September 17, 2024; Accepted December 03, 2024; Available online December 13, 2024

Abstract

File carving is a method for recovering files using software such as Foremost and Autopsy. The recovery is conducted for deleted files or formatted devices. Popularity Solid State Drive (SSD) has outperformed Hard Disk Drive (HDD) because SSD is faster, more efficient, and shock resistant. However, recovering SSD devices have a lower probability success rate than HDD because the security system often hampers files recovered on SSD. Based on previous research, the success rate of Security Digital High Capacity (SDHC) only achieved 50% more than SSD, whereas SSD can only return 85.7% of its success. Forensics Digital is a part of Forensics Knowledge for deliver valid digital evidence for law investigation. This research aims to increase the success rate of recovery files using two different software: Foremost and Autopsy. The research uses a 512GB Eaget brand SSD with a New Technology File System (NTFS). The file carving is also conducted using the Association of Chief Police Officers (ACPO) method. APCO has several stages: Planning, Capture, Analysis, and Presentation. The experiment results show that Autopsy software with deep recover mode returned 81 out of 88 files (92%), whereas Foremost software run on Debian to make sure no virus on device that could damage computer especially windows system. First attempt recovery can only return 46 out of 88 files (52%). The findings show that the Autopsy software has a higher successful return rate and can be used for evidence in law enforcement and digital forensics investigations.

Keywords: ACPO; Autopsy; Digital Forensics; Foremost; SSD.

Introduction

Hard Disk Drive (HDD) has begun to be abandoned because it is slow and noisy when used at high speeds. On the other hand, Solid State Drive (SSD) is starting to become popular because SSDs are more efficient in terms of size and speed [1], [2]. In 2022, the market share of the states that hard disk drive storage dominates up to 60%, while NAND Flash, as one of the SSD chips, is only 25%. Although the popularity of SSDs is increasing yearly [3]. NAND Flash technology is used in SSDs so that their capacity can be increased using Multi-Level Cell (MLC), Triple-Layer Cell (TLC), and Quad-Level Cell(QLC), and the production costs can be cheaper compared to HDD [4]. This NAND Flash has an average speed ten times faster than an HDD. Many companies choose SSD as their social media data center and entertainment to improve performance and reduce latency [5].

System transfer SSD uses a Flash Transfer Layer (FTL), allowing any NAND Flash layer to work simultaneously [6]. So, the faster the type of SSD is used, the higher the heat generated. Generally, SSDs run around 50-55 ºC and can run normally at 0-70 ºC. If the temperature is more than 70 ºC than recommended, the SSD speed may be slower than the Hard disk drive [7]. SSD needs a heatsink to spread the temperature so the performance is more stable [8], which on benchmarking is more stable [9]. SSD sales experience an increase every year along with a decrease in sales HDD, as shown in **Figure 1**.

The disappearance of evidence digital by deleting, formatting or using anti digital forensics can cause difficulties investigator in recovering and analyzing digital evidence [10]. Digital evidence is the key to digital crime when mishandled and can cause major problems [11]. Digital evidence must be identified, obtained evidence, analyzed and submitted digital evidence through the process digital forensics [12], [13]. Once digital evidence is obtained, the original evidence must be copied as soon as possible. Copy of evidence is the result original copy and legal to use original copy to maintain authenticity file original [14]. Investigator must keep evidence digital relevant to the investigation, for legal prosecution [15]. In the case of the UII Mapala basic education committee, Karanganyar police

http://dx.doi.org/10.33096/ilkom.v16i3.2360.283-295

criminal investigation unit Head AKP Rohmat Ashari stated that he had confiscated three cameras, one computer and one laptop. Files in the device were not found, it is suspected that it was deliberately removed to remove evidence before it was confiscated. If recovery is successfully returned by forensics laboratory. It has the potential to give rise to new cases, namely cases of acts of disappearance of evidence [16].

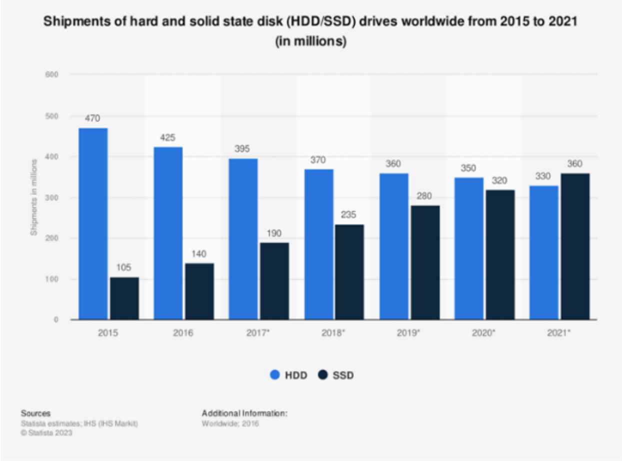


Figure 1. Global SSD sales soar from 2015 to 2021

The Foremost software can restore file extensions such as jpg, gif, WMV, MOV, wav, ole, zip, and pdf. The returned amount file is displayed in the file.txt [17]. Foremost software uses files on the Security Digital High Capacity (SDHD) to manage and restore 77% of files, with the Percentage value hashing valid only 50% [18]. Although Foremost recover files is fast, but the percentage of RAR extension recover is just 39 files from 70 files with 3 correct RAR [19].

Later, Autopsy Software demonstrated the ability to recover key forensic artifacts from the Nintendo Switch, with many persisting after factory resets, and automated the process using 10 Autopsy ingest modules. Unique tools and guidelines for forensic analysis provide new capabilities for analysts and could apply to other portable Nintendo consoles [20]. Hashing software used to prove the authenticity value, MD5, is used on the Windows operating system. MD5 files that are corrupt or have changed have different hash values from the original. The file stated that it is not valid and cannot used as proof or value of a successful returns file [21].

This research shows all process of foremost and autopsy step to recovery files from External SSD mSATA version. Previous research of SDHC using foremost software just show result without any process [18]. The Nintendo Switch article is not show percentage of successfully recovered files and just have raw data which could not serve to public to understand [20]. This article could be used for the reader to recover files of his own. Every step of the research has been written in this article to make sure that every step of the recover files. The Linux user could use Foremost step and windows users use Autopsy step.

The alteration of original data violates the first ACPO guideline, posing challenges for law enforcement in preserving evidence integrity. Disappearing messages exacerbate this issue, with platforms like WhatsApp retaining some data, while Snapchat and Telegram are increasingly destructive, complicating forensic investigations [22], [23]. Researchers and investigators can analyze further using the ACPO method in the case of digital forensics, like data extraction and the Internet of Things (IoT) [24], [25]. The Researchers and investigators can compare the ACPO method with the DFRWS framework [26]. Foremost software on the Ubuntu operating system is used to extract image files [27]. Autopsy software is used in Linux and Windows operating systems, and Foremost software can restore files that have been deleted, formatted, or even exposed to ransomware. Autopsy software is more potent than Foremost software [28], [29].

This article is organized as follows: Part 1 is the Introduction, highlighting differences from previous studies. Section 2, Research Methods, details the ACPO Framework to achieve the desired research outcomes. Section 3, Results and Analysis, presents the research findings obtained through the ACPO framework on SSD, using the Foremost and Autopsy software. The measure of success file carving result using MD5 software. Finally, Section 4, Conclusion, summarizes the research results and offers recommendations for future studies.

Method

ACPO's Good Practice Guide for Digital Evidence guidance book has seven stages for assisting and investigating crimes and security incidents in cyber security. ACPO guidance book has levels of Application of Guide, The Principles of Digital Evidence, Plan, Capture, Analyze, Present, and General [30]. The ACPO method is summarized into four stages consisting of Plan, Capture, Analysis, and Present [31].

A. Research stages

The ACPO method is used Interrelated to every stage that is shown on **Figure 2**. The planning stage processes preparing plans for research, obtaining maximum results, and increasing success. This stage prepares research tools and materials, such as hardware and software [32]. The capture stage aims to obtain evidence related to the investigation case. The capture stage found evidence in recordings, storage devices, interrogations, and others to obtain proof of crimes [33]. The analysis stage analyzes the results captured to ensure digital evidence is found. The investigator uses original evidence to determine which pieces are relevant to the investigated case [34]. The present stage ensures the analyzed submission or announcement of crime evidence, and the evidence reported must be accountable for its validity in forensics and law [35].

Plan
Capture
Analyze
Present

Figure 2. ACPO method stages

The ACPO method has interrelated stages. And bring it closer to investors to a theory or conclusion. The investigator decides on the investigated case based on the theory or findings obtained.

B. Research Scenario

This research takes evidence from an actual incident on the internet as a scenario simulation. The scenario research is made up for research purposes. The News from Detiknews show Photos and videos of perpetrators from *Kelompok Kriminal Bersenjata* (KKB) Papua recorded the shooting of *Tentara Nasional Indonesia* (TNI) members using a smartphone [36]. Kompas.com news reported that the Susi Air pilot was taken hostage by KKB and Demanding the declaration of independence for Papua, as shown in Photos and videos [37]. Photos and videos are stored on an external SSD in the research scenario. When the TNI conducted a raid on an area suspected of being a base for *Organisasi Papua Merdeka* (OPM) operations, an Eaget mSATA-type external SSD with a capacity of 512GB and file system NTFS was found. The file on the SSD was removed and formatted with the status trim disabled by default. So, investigators allow data to be recovered directly from a device without additional devices like SDHD.

The SSD is examined using a computer, but the file inside is empty. This incident raised suspicions that the contents of the SSD had been deleted intentionally to destroy evidence. TNI cooperated with Investigator Forensics Digital to perform further research and data recovery. Investigator forensics managed to find and recover some files that contained substantial evidence of SSD. Investigators report the investigation results to the TNI for further legal action. This research is expected to produce new knowledge. Mainly about the effectiveness of the forensics technique in deleted data recovery. To strengthen law enforcement efforts in handling armed crime cases. The findings can be used to develop standard protocols in future digital forensics investigations. **Figure 3** describes the stages of the research scenario, starting from the simulation file carving, case simulation, planning, taking evidence, analyzing evidence, and reporting.

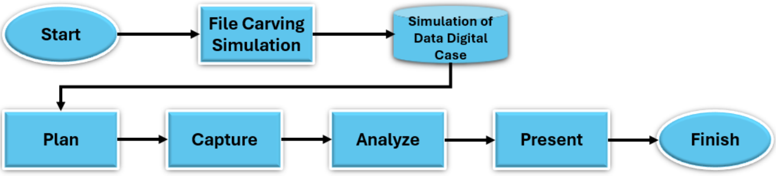


Figure 3. Research design

C. Research tools and materials

The research material for recovering process file is an Eaget 512GB SSD. The tools for the research are Foremost software and Autopsy software. This research uses Foremost software because Foremost is commonly used on digital forensic articles and it is free. The reason Autopsy software chosen is reliable of maximum result to recover files. MD5 software is used to confirm the correctness of files because it is easy to use. Information details on hardware and software are described in **Table 1**.

Table 1. Research tools and materials

No	Tools and materials	Version	Function
1	Laptop Legion Y520	Windows 10 64bit and Ubuntu 22.0.4, 16GB RAM	A computer for extraction and analysis device
2	USB Connector	USB to Type C	used to connect a SSD device to a computer
3	external SSD Eaget	mSATA, 512GB, type C port	Experiment object
4	Foremost	1.5.7, run on Ubuntu	Forensics Open-source tool
5	Autopsy	4.21.0, Run on Windows	Forensics Open-source tool
6	MD5	1.20, Run on Windows	Validation digital Evidence

Results and Discussion

This stage uses the Association of Chief Police Officers (ACPO) digital forensics method on an external SSD. ACPO stages have their respective functions. Each function is interconnected and sequential.

A. Planning

The early stage is the preparation of hardware and software to conduct research. The scenario to be carried out involves the documentation of evidence in the form of an external SSD and a Type C data cable. In **Figure 4**, the object can be accessed via a computer as a blue 512GB Eaget external SSD brand. Objects were found at the crime scene based on simulations carried out in the research.

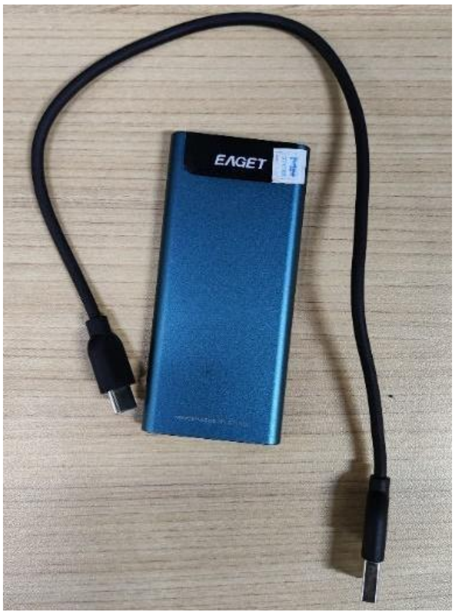
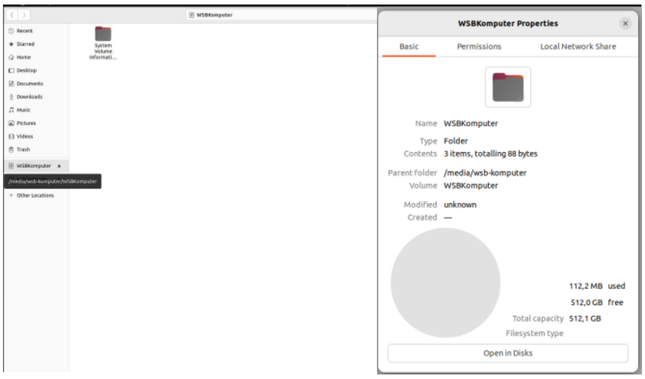


Figure 4. Securing physical evidence

The SSD is connected to a computer to view the contents of the SSD using the Ubuntu operating system. The Ubuntu operating system is used so that if there is a virus on the SSD, it is hoped that it is not spread to the computer. **Figure 5** shows that the external SSD obtained did not display any files when checked. SSD checked through properties shows storage on an empty SSD, and the image shows the storage folder system volume information. There are three files with a total capacity of 88 Bytes.



Name WSBKomputer
Type Folder
Contents 3 items, totalling 88 bytes
Parent folder /media/wsb-komputer
Volume WSBKomputer
Modified unknown
Created —
112,2 MB used
512,0 GB free
Total capacity 512,1 GB
Filesystem type

Figure 5. Checking the contents of the external SSD

Table 2. Hardware and Software Functions

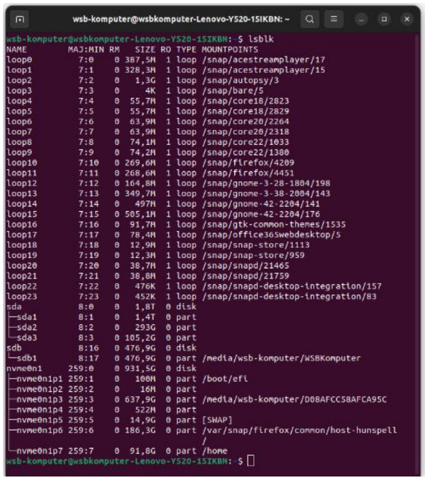
No	Hardware Software	Function
1	Laptop	As a tool to run applications and connect SSD devices
2	USB type C	As a connector for type C SSD to type A computer
3	external SSD	Research recovery data that has been deleted and formatted
4	Foremost 1.5.7	Recovery software on the Ubuntu operating system
5	Autopsy 4.21.0	Recovery software on the Windows operating system
6	MD5 v1.20	Displays hash value on a file to measure the authenticity value of the file
7	MS Excel	Calculate the resulting hash value into a percentage
8	MS Word	Create results reporting

B. Capture

The capture process involves making a return file, which the perpetrator deliberately removed. Criminals' goal is to eliminate digital evidence. Investigators made a return file two times on software and different operating systems. The investigator aims to get maximum comparative results to find software which works more optimally for returning case file from an SSD.

1. Foremost

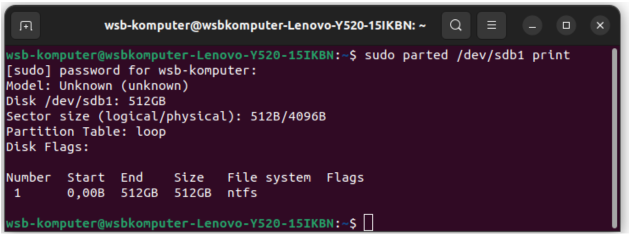
Foremost runs on the Linux operating system. This research was conducted using the Ubuntu 22.0.4 operating system run on the terminal. The terminal is open for input passwords and aimed at accessing commands. Figure 6 shows the "*lsblk*" command used to display all partition codes on the computer. The destination partition code is identified using *"sdb"* for the SSD code and "*sdb1*" for the partition code used for the recovery destination.



```
wsb-komputer@wsbkomputer-Lenovo-Y520-15IKBN:~$ lsblk
NAME        MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
loop0         7:0    0 387,5M  1 loop /snap/acestreamplayer/17
loop1         7:1    0 328,3M  1 loop /snap/acestreamplayer/15
loop2         7:2    0   1,3G  1 loop /snap/autopsy/3
loop3         7:3    0     4K  1 loop /snap/bare/5
loop4         7:4    0  55,7M  1 loop /snap/core18/2823
loop5         7:5    0  55,7M  1 loop /snap/core18/2829
loop6         7:6    0  63,9M  1 loop /snap/core20/2264
loop7         7:7    0  63,9M  1 loop /snap/core20/2318
loop8         7:8    0  74,1M  1 loop /snap/core22/1033
loop9         7:9    0  74,2M  1 loop /snap/core22/1380
loop10        7:10   0 269,6M  1 loop /snap/firefox/4209
loop11        7:11   0 268,6M  1 loop /snap/firefox/4451
loop12        7:12   0 164,8M  1 loop /snap/gnome-3-28-1804/198
loop13        7:13   0 349,7M  1 loop /snap/gnome-3-38-2004/143
loop14        7:14   0   497M  1 loop /snap/gnome-42-2204/141
loop15        7:15   0 505,1M  1 loop /snap/gnome-42-2204/176
loop16        7:16   0  91,7M  1 loop /snap/gtk-common-themes/1535
loop17        7:17   0  78,4M  1 loop /snap/office365webdesktop/5
loop18        7:18   0  12,9M  1 loop /snap/snap-store/1113
loop19        7:19   0  12,3M  1 loop /snap/snap-store/959
loop20        7:20   0  38,7M  1 loop /snap/snapd/21465
loop21        7:21   0  38,8M  1 loop /snap/snapd/21759
loop22        7:22   0   476K  1 loop /snap/snapd-desktop-integration/157
loop23        7:23   0   452K  1 loop /snap/snapd-desktop-integration/83
sda           8:0    0   1,8T  0 disk 
├─sda1        8:1    0   1,4T  0 part 
├─sda2        8:2    0   293G  0 part 
└─sda3        8:3    0 105,2G  0 part 
sdb           8:16   0 476,9G  0 disk 
└─sdb1        8:17   0 476,9G  0 part /media/wsb-komputer/WSBKomputer
nvme0n1     259:0    0 931,5G  0 disk 
├─nvme0n1p1 259:1    0   100M  0 part /boot/efi
├─nvme0n1p2 259:2    0    16M  0 part 
├─nvme0n1p3 259:3    0 637,9G  0 part /media/wsb-komputer/D08AFCC58AFCA95C
├─nvme0n1p4 259:4    0   522M  0 part 
├─nvme0n1p5 259:5    0  14,9G  0 part [SWAP]
├─nvme0n1p6 259:6    0 186,3G  0 part /var/snap/firefox/common/host-hunspell
│                                     /
└─nvme0n1p7 259:7    0  91,8G  0 part /home
wsb-komputer@wsbkomputer-Lenovo-Y520-15IKBN:~$ 
```

Figure 6. Search for partition code on an external SSD

Figure 7 shows the command “*sudo parted /dev/sdb1 print*”. The “*parted*” command is used to designate a partition. The command “*/dev/sdb1*” shows the location of the targeted partition. The “*print*” command displays the contents of the targeted partition. The aim is to ensure that the partition is correctly marked with a capacity of 512GB. This information shows the capacity of the Eaget SSD, which is used as a research object.



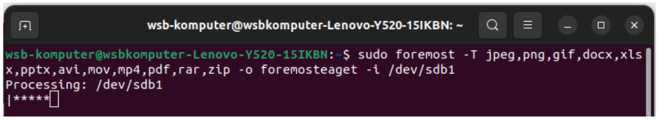
```
wsb-komputer@wsbkomputer-Lenovo-Y520-15IKBN:~$ sudo parted /dev/sdb1 print
[sudo] password for wsb-komputer:
Model: Unknown (unknown)
Disk /dev/sdb1: 512GB
Sector size (logical/physical): 512B/4096B
Partition Table: loop
Disk Flags:

Number  Start  End    Size   File system  Flags
 1      0,00B  512GB  512GB  ntfs

wsb-komputer@wsbkomputer-Lenovo-Y520-15IKBN:~$
```

Figure 7. Show partition details

Figure 8 shows the command “sudo Foremost -t jpeg,png,gif,docx,xlsx,pptx,avi,mov,mp4,pdf,rar,zip -o foremosteaget -I /dev/sdb1”. The command description “sudo foremost” is used to run software foremost. Command code “-t jpeg,png,gif,docx,xlsx,pptx,avi,mov,mp4,pdf,rar,zip” show type file what will be recovered. The “-o foremosteaget” line directs storage file which has been successfully returned. Because there is no information for others folder, then folder “foremosteaget” created on desktop. The command "-I /dev/sdb1" shows information on the location of the partition to be recovered.



```
wsb-komputer@wsbkomputer-Lenovo-Y520-15IKBN:~$ sudo foremost -T jpeg,png,gif,docx,xls
x,pptx,avi,mov,mp4,pdf,rar,zip -o foremosteaget -i /dev/sdb1
Processing: /dev/sdb1
|*****
```

Figure 8. Recovery command of SSD

Figure 9 shows the results recovery from Foremost software which has been separated into each folder based on the extension. The image explains the jpeg, png, gif folders (for Image format), docx, xlsx, pptx, pdf (for document format), avi, mov, mp4 (for video format), and rar, and zip (for archive format). This makes it easier to sort digital evidence for analysis and reporting recovery in the form of “audit.txt.”

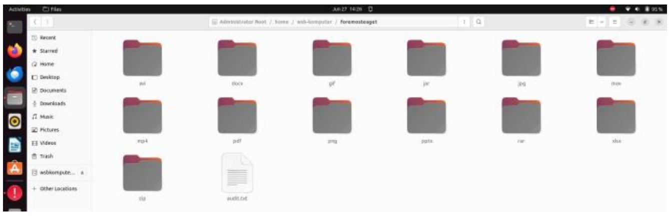


Figure 9. Leading recovery results

2. *Autopsy*

Autopsy software version 4.2.1 runs on the Windows 10 64bit operating system. Figure 10 shows the initial display of Autopsy software. Investigators choose "*new case*" to start a new case that has never been carried out. Select “*open recent case*” to open a case that has previously been run on the computer running the Autopsy software. Select “*open case*” to load a case saved by another computer to run on the computer that is running the Autopsy software.

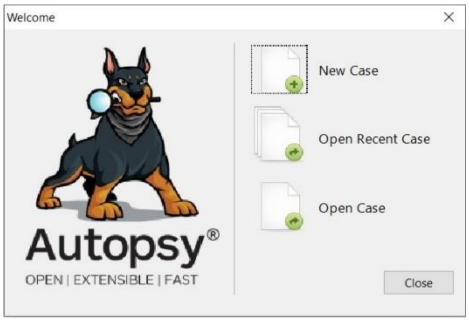
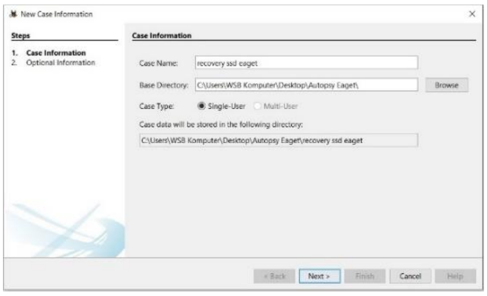


Figure 10. Initial view of Autopsy software

Investigators choose "*new case*" To start the operation Autopsy software, fill in "*case name*" with the name of the case. Investigator can use the names of projects and objects To make naming easier, this research use "*Recovery SSD Eaget*" name to create the project title, and "base directory" to determine the project location as in **Figure 11**.


New Case Information

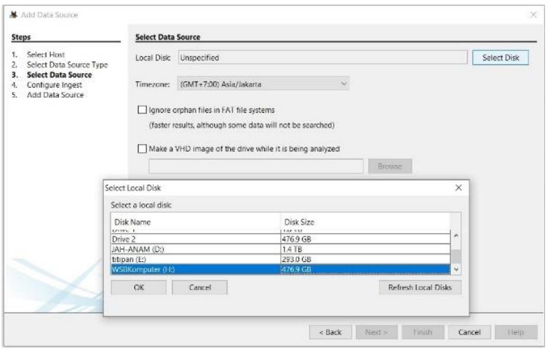
Steps
1. Case Information
2. Optional Information

Case Information

Case Name: recovery ssd eaget
Base Directory: C:\Users\WSB Komputer\Desktop\Autopsy Eaget\
Case Type: ● Single-User ○ Multi-User
Case data will be stored in the following directory:
C:\Users\WSB Komputer\Desktop\Autopsy Eaget\recovery ssd eaget

Figure 11. Creation of a new project

Later, select "*local disk*" by clicking "*select disk*" and looking for the partition to be restored. **Figure 12** shows a capacity of 476.9GB, indicating a capacity close to the listed capacity of the 512GB external SSD. Investigators must also know which disk shows the external SSD by showing the name of the SSD, namely "*WSBKomputer*". The SSD has partition "*H*" as an object recovery which is shown in **Figure 12**.


Add Data Source

Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Data Source

Local Disk: Unspecified
Timezone: (GMT+7:00) Asia/Jakarta
□ Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)
□ Make a VHD image of the drive while it is being analyzed

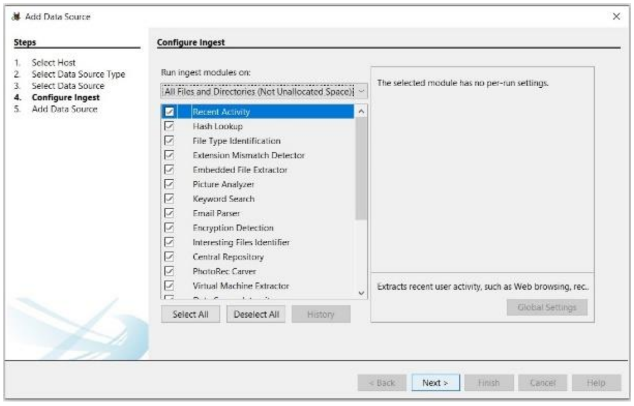
Select Local Disk

Select a local disk

Disk Name	Disk Size
Drive 2	476.9 GB
JAH-ANAM (D:)	1.4 TB
titipan (E:)	293.0 GB
WSBKomputer (H:)	476.9 GB

Figure 12. Selection of recovered partitions

Figure 13 shows the type of selection recovery required to restore the required data. Investigators can tick marks for the recovery process and what we do not need, we can uncheck it to return it file the process requires recovery does not take a long time. The more Investigator tick the list, the more information is extracted from the SSD and the more storage space and time needed.


Add Data Source

Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Configure Ingest

Run ingest modules on:
All Files and Directories (Not Unallocated Space)

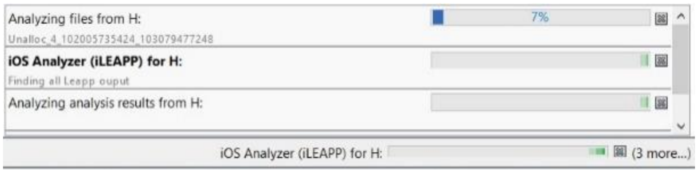
☑ Recent Activity
☑ Hash Lookup
☑ File Type Identification
☑ Extension Mismatch Detector
☑ Embedded File Extractor
☑ Picture Analyzer
☑ Keyword Search
☑ Email Parser
☑ Encryption Detection
☑ Interesting Files Identifier
☑ Central Repository
☑ PhotoRec Carver
☑ Virtual Machine Extractor

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, rec..

Figure 13. Selection of recovery type

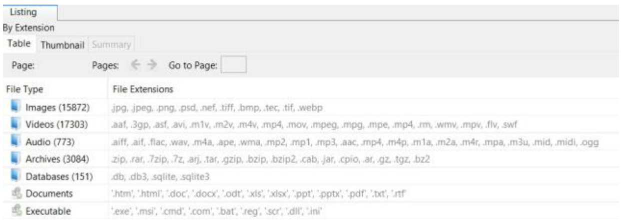
Figure 14 shows the process recovery data on Autopsy software. The duration of recovery process determined by storage capacity, size and quantity file which was deleted. Storage and types of recovery which is used on Autopsy software which can take days to recover. Investigators must confirm the storage destination file results recovery sufficient to avoid obstruction.



Analyzing files from H: 7%
Unalloc_4_102005735424_103079477248
iOS Analyzer (iLEAPP) for H:
Finding all Leapp ouput
Analyzing analysis results from H:
iOS Analyzer (iLEAPP) for H: (3 more...)

Figure 14. Recovery process at Autopsy

Figure 15 shows Autopsy software completed the recovery. Autopsy displays the amount files that successfully recovered. Each file type registers the extension file. Investigators need to process placement files to manage files that have been successfully restored. Select file for managing and moving on folders that have been given. The results of recovery from the software that are not necessarily can be deleted.

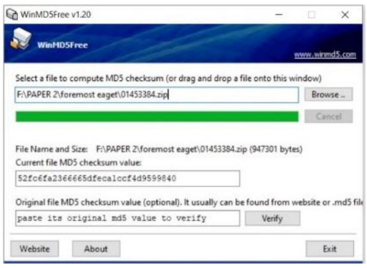


File Type	File Extensions
Images (15872)	.jpg, .jpeg, .png, .psd, .nef, .tiff, .bmp, .tec, .tif, .webp
Videos (17303)	.aaf, .3gp, .asf, .avi, .m1v, .m2v, .m4v, .mp4, .mov, .mpeg, .mpg, .mpe, .mp4, .rm, .wmv, .mpv, .flv, .swf
Audio (773)	.aiff, .aif, .flac, .wav, .m4a, .ape, .wma, .mp2, .mp1, .mp3, .aac, .mp4, .m4p, .m1a, .m2a, .m4r, .mpa, .m3u, .mid, .midi, .ogg
Archives (3084)	.zip, .rar, .7zip, .7z, .arj, .tar, .gzip, .bzip, .bzip2, .cab, .jar, .cpio, .ar, .gz, .tgz, .bz2
Databases (151)	.db, .db3, .sqlite, .sqlite3
Documents	'.htm', '.html', '.doc', '.docx', '.odt', '.xls', '.xlsx', '.ppt', '.pptx', '.pdf', '.txt', '.rtf'
Executable	'.exe', '.msi', '.cmd', '.com', '.bat', '.reg', '.scr', '.dll', '.ini'

Figure 15. Autopsy recovery results

C. *Analysis*

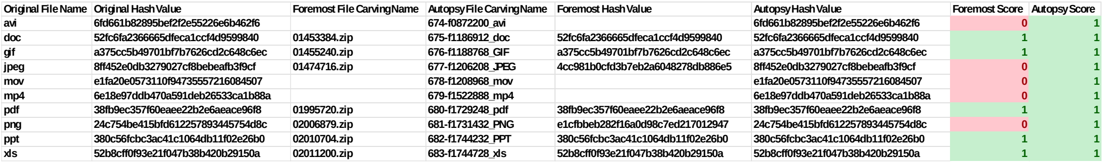
SSD external analyze recovered files use WinMd5 software to get the hash value. **Figure 16** shows the value retrieval process hash from the file. If hash value on file matches with hash value on the original file, it means successful. After the recovery process is finished there is a file which can be opened but the hash value is different. Files cannot be accounted, even if they are played or displayed at first glance. This is due to concerns that there has been a change in the file's contents, whether done intentionally by the perpetrator. The other reason is the file experience corruption. Corrupt files can be caused by the system, either during recovery process or virus.



Select a file to compute MD5 checksum (or drag and drop a file onto this window)
F:\PAPER 2\foremost eaget\01453384.zip
File Name and Size: F:\PAPER 2\foremost eaget\01453384.zip (947301 bytes)
Current file MD5 checksum value:
52fc6fa2366665dfeca1ccf4d9599840
Original file MD5 checksum value (optional). It usually can be found from website or .md5 file
paste its original md5 value to verify

Figure 16. Process of retrieving hash values in files

The obtained Mark hash is entered into Microsoft Excel, displayed in **Figure 17**. The investigator confirms the hash value on file, which is restored equal to the value file native, so assign a value of 1 for a file with the same hash value. The name on the file has generally changed because it shows the hash value, which does not change, indicating the content file is unchanged. A value of 0 is assigned to a file with different hash values. The cause is corruption, has been changed, or has not been found by Foremost software or Autopsy.



Original File Name	Original Hash Value	Foremost File Carving Name	Autopsy File Carving Name	Foremost Hash Value	Autopsy Hash Value	Foremost Score	Autopsy Score
avi	6fd661b82895bef2f2e55226e6b462f6		674-f0872200_avi		6fd661b82895bef2f2e55226e6b462f6	0	1
doc	52fc6fa2366665dfeca1ccf4d9599840	01453384.zip	675-f1186912_doc	52fc6fa2366665dfeca1ccf4d9599840	52fc6fa2366665dfeca1ccf4d9599840	1	1
gif	a375cc5b49701bf7b7626cd2c648c6ec	01455240.zip	676-f1188768_GIF	a375cc5b49701bf7b7626cd2c648c6ec	a375cc5b49701bf7b7626cd2c648c6ec	1	1
jpeg	8ff452e0db3279027cf8bebeafb3f9cf	01474716.zip	677-f1206208_JPEG	4cc981b0cfd3b7eb2a6048278db886e5	8ff452e0db3279027cf8bebeafb3f9cf	0	1
mov	e1fa20e0573110f94735557216084507		678-f1208968_mov		e1fa20e0573110f94735557216084507	0	1
mp4	6e18e97ddb470a591deb26533ca1b88a		679-f1522888_mp4		6e18e97ddb470a591deb26533ca1b88a	0	1
pdf	38fb9ec357f60eaee22b2e6aeace96f8	01995720.zip	680-f1729248_pdf	38fb9ec357f60eaee22b2e6aeace96f8	38fb9ec357f60eaee22b2e6aeace96f8	1	1
png	24c754be415bfd612257893445754d8c	02006879.zip	681-f1731432_PNG	e1cfbbeb282f16a0d98c7ed217012947	24c754be415bfd612257893445754d8c	0	1
ppt	380c56fcbc3ac41c1064db11f02e26b0	02010704.zip	682-f1744232_PPT	380c56fcbc3ac41c1064db11f02e26b0	380c56fcbc3ac41c1064db11f02e26b0	1	1
xls	52b8cff0f93e21f047b38b420b29150a	02011200.zip	683-f1744728_xls	52b8cff0f93e21f047b38b420b29150a	52b8cff0f93e21f047b38b420b29150a	1	1

Figure 17. hash value matching process

D. *Present*

The hash mark was entered into Microsoft Excel and given a value. Making successful percentages using the sum formula file has been successfully restored and the hash value is the same as the file original divided by the amount of file original that should exist, multiplied by 100% with Equation 1.

$$P_{\alpha r} = \frac{S_{\alpha r}0}{S_{\alpha r}T} \times 100\% \tag{1}$$

Where

$P_{\alpha r}$ = percentage of success software recovery

$S_{\alpha r}0$ = amount file successful

$S_{\alpha r}T$ = amount number of files

Table 3. Total file which was successfully recovered

File Type	Original File	Foremost	Autopsy
zip	10	5	10
rar	10	0	3
docx	7	7	7
pdf	7	6	7
pptx	7	7	7
xls	7	7	7
gif	5	0	5
jpg	7	7	7
png	7	7	7
avi	7	0	7
mov	7	0	7
mp4	7	0	7
Amount	88	46	81

Table 3 has 4 attributes, namely type file which is the file extension used by the perpetrator to store evidence sought by the police. The original File should be discovered by software in this research. The Foremost attribute represents the amount file that was successfully returned using Foremost software based on existing extensions. An autopsy represents the number of files which were successfully returned using Autopsy software. The data obtained can be converted into a percentage value for each success file using the P formula$_{\alpha r}$ as with the accumulated results on Foremost and Autopsy software. The results are shown in Table 4.

Table 4. Table of percentage of foremost and autopsy success

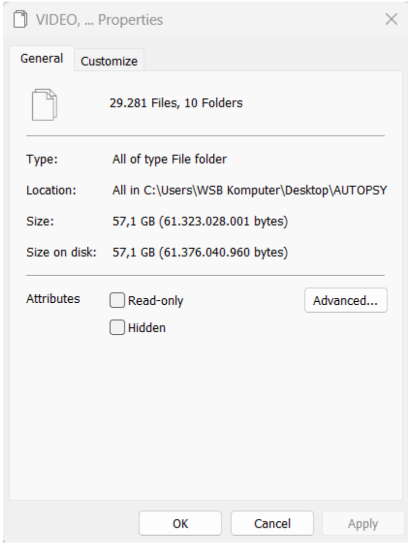
File Type	Foremost	Autopsy
zip	50%	100%
rar	0%	30%
docx	100%	100%
pdf	86%	100%
pptx	100%	100%
xlsx	100%	100%
gif	0%	100%
jpg	100%	100%
png	100%	100%
avi	0%	100%
mov	0%	100%
mp4	0%	100%
Percentage	52%	92%

Table 4 compares the capabilities of Foremost and Autopsy software in performing the recovery of files of various file types. File Zip on Foremost successfully recovers as much as 50%. Autopsy software was 100% successful.

Foremost software failed to restore file rar. Autopsy successfully returned ten files that can be opened, but the hash value of 7 files is not the same as that of the file. The % of autopsy software users who use file rar is only 30%. Both succeeded in recovering files docx, pptx, xlsx, jpg, and png with a success rate of 100%. It was the foremost success in recovering 86% of the file pdf, while the Autopsy was 100% successful. Foremost failed in doing so, recovery file gif, avi, mov, and mp4, while Autopsy managed to make a recovery, all with a 100% success rate. Overall, Foremost software has a success rate recovery of 52%, and Autopsy software is 92%, indicating that Autopsy has better performance capabilities for recovering various types of files compared to Foremost. Foremost take around 27 minutes start at 30 April 2024 20:01:41 finish at 20:28:05 on the same day. Autopsy take around 1 hour 10 minutes starting on 1 May 2024 00:02:47 finish 01:12:38 on the same day. Although foremost faster but Autopsy has more successfully recovered file rate.

From the results of the RAR file analysis in Autopsy, it was successfully returned and can be opened, but it does not have the same hash value. Three RAR files have a capacity of more than 100MB, but the reason why the hash value has changed for four files has not been found. The zip extension file successfully returned ten files without any problems. The docx, xlsx, and pptx extension files restored seven files each without any issues. Autopsy also succeeded in returning video files with avi, mov, and mp4 extensions, which had copies of what should have been only seven files, totaling 14 files. Each file has the same hash value and a different name. Files with the pdf extension also produce recovery copies totaling 14 from the seven original files. Image files have different patterns for each extension. GIF has ten copies, which should only be 5. Jpg has 30 files, 14 consisting of 7 original copy files and 16 files copied eight times from 2 files that should not exist. After tracing the two files, the image extracts came from docx, pdf, and pptx extension files.

Autopsy has deep recovery show on Figure 13 that every module has its own purpose, the more module we select, the more data we recover. The author recovered the used SSD used Autopsy brought files that were not supposed to recover. The first recovery uses Foremost successfully recover 100 files of 88 files but 43 of them are duplicate from original file or the hash value do not match. The second recovery using Autopsy, the result is 29.281 Files recovered show on Figure 18, the third recovery use Autopsy to make sure data is clean after wiping data and the result is 0 file found, and the fourth recovery use Autopsy has the result of the research with 162 files recovered show on Figure 19 which use on this article.



29.281 Files, 10 Folders

Type: All of type File folder

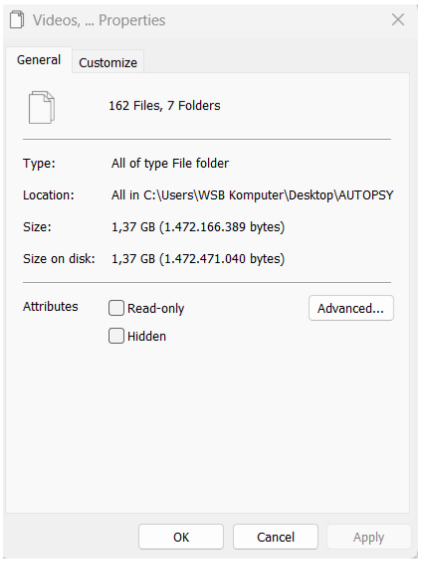
Location: All in C:\Users\WSB Komputer\Desktop\AUTOPSY

Size: 57,1 GB (61.323.028.001 bytes)

Size on disk: 57,1 GB (61.376.040.960 bytes)

Attributes □ Read-only □ Hidden

Figure 18. Autopsy result before wiping data



162 Files, 7 Folders

Type: All of type File folder

Location: All in C:\Users\WSB Komputer\Desktop\AUTOPSY

Size: 1,37 GB (1.472.166.389 bytes)

Size on disk: 1,37 GB (1.472.471.040 bytes)

Attributes □ Read-only □ Hidden

Figure 19. Autopsy results after wiping data re-recover

Foremost do not have select module like Autopsy, the reason researchers used foremost is make sure the SSD does not have virus that could damage the computer. Foremost run on Debian operating systems that virus with ".exe and .bat" could not run automatically and spread on ubuntu. When the researchers make sure SSD is empty it starts to run recovery on foremost software. When we see the pattern gif, mov and mp4 extension are not recovered because it is moving picture or video. The RAR extension if failed to recover because Foremost has low capability on recovering RAR files.

Conclusion

According to research in the context of digital forensics, deletion or formatting of data on media storage can complicate the recovery and analysis process of digital evidence. Therefore, digital process forensics must be carried out carefully following standardized methods. The ACPO uses research for Foremost and Autopsy software to conduct recovery data from a formatted SSD. Detail step of recovery file could assist the researcher and computer technician for helping Law enforcement agencies. The results showed that Autopsy had a higher success rate (92%) because it has deep recovery tools than Foremost (52%) which use base recovery for successful files with the same hash value. In conclusion, an Autopsy is more effective in recovering deleted or formatted files, providing strong evidence for law enforcement. Hopefully the next research could be more successfully recovering files from SSD variation or other types of NAND flash like smartphone, flash drive etc. Investigating methods to enhance recovery success rates for various storage devices with different file systems could help create more robust forensic tools. Additionally, exploring the use of AI and machine learning in the recovery process may provide more automated and accurate ways to detect and retrieve deleted or corrupted files, further improving digital forensic capabilities.

References

[1] J. Liu, T. Wang, X. Chen, C. Li, Z. Shen, and Z. Zhang, “H2-RAID: Improving the reliability of SSD RAID with unified SSD and HDD hybrid architecture,” *Microprocess. Microsyst.*, vol. 105, p. 104993, Mar. 2024, doi: 10.1016/J.MICPRO.2023.104993.

[2] J. Ryu, D. K. Noh, and K. Kang, “FlashPage: A read cache for low-latency SSDs in web proxy servers,” *Eng. Sci. Technol. an Int. J.*, vol. 51, no. January, p. 101639, 2024, doi: 10.1016/j.jestch.2024.101639.

[3] D. Kim, J. Kim, K. Choi, H. Han, M. Ryu, and S. Kang, “Dynamic zone redistribution for key-value stores on zoned namespaces SSDs,” *J. Syst. Archit.*, vol. 152, p. 103159, Jul. 2024, doi: 10.1016/J.SYSARC.2024.103159.

[4] L. Luo, S. Li, Y. Lv, and L. Shi, “Performance and reliability optimization for high-density flash-based hybrid SSDs,” *J. Syst. Archit.*, vol. 136, p. 102830, Mar. 2023, doi: 10.1016/J.SYSARC.2023.102830.

[5] P. Santikellur, M. Buddhanoy, S. Sakib, B. Ray, and R. S. Chakraborty, “A shared page-aware machine learning assisted method for predicting and improving multi-level cell NAND flash memory life expectancy,” *Microelectron. Reliab.*, vol. 140, p. 114867, Jan. 2023, doi: 10.1016/J.MICROREL.2022.114867.

[6] X. Li, M. Kim, S. Lee, Z. Zhai, and J. Kim, “Program context-assisted address translation for high-capacity SSDs,” *Futur. Gener. Comput. Syst.*, vol. 162, p. 107483, Jan. 2025, doi: 10.1016/J.FUTURE.2024.107483.

[7] D. Brown *et al.*, “Detecting firmware modification on solid state drives via current draw analysis,” *Comput. Secur.*, vol. 102, p. 102149, Mar. 2021, doi: 10.1016/J.COSE.2020.102149.

[8] A. Genç, H. Doğan, L. Turhan, A. Kocakuşak, and S. Helhel, “Investigation of the radiated emission of honeycomb structured aluminum foam/cellular heatsinks at 1–10 GHz,” *Mater. Chem. Phys.*, vol. 324, p. 129614, Sep. 2024, doi: 10.1016/J.MATCHEMPHYS.2024.129614.

[9] A. Chamkha, A. Veismoradi, M. Ghalambaz, and P. Talebizadehsardari, “Phase change heat transfer in an L-shape heatsink occupied with paraffin-copper metal foam,” *Appl. Therm. Eng.*, vol. 177, p. 115493, Aug. 2020, doi: 10.1016/J.APPLTHERMALENG.2020.115493.

[10] J. Gruber, C. J. Hargreaves, and F. C. Freiling, “Contamination of digital evidence: Understanding an underexposed risk,” *Forensic Sci. Int. Digit. Investig.*, vol. 44, p. 301501, Mar. 2023, doi: 10.1016/J.FSIDI.2023.301501.

[11] G. Horsman, “Digital evidence and the crime scene,” *Sci. Justice*, vol. 61, no. 6, pp. 761–770, Nov. 2021, doi: 10.1016/J.SCIJUS.2021.10.003.

[12] P. Sokol, Ľ. Antoni, O. Krídlo, E. Marková, K. Kováčová, and S. Krajči, “Formal concept analysis approach to understand digital evidence relationships,” *Int. J. Approx. Reason.*, vol. 159, p. 108940, Aug. 2023, doi: 10.1016/J.IJAR.2023.108940.

[13] R. Stoykova, “The right to a fair trial as a conceptual framework for digital evidence rules in criminal

investigations," *Comput. Law Secur. Rev.*, vol. 49, p. 105801, Jul. 2023, doi: 10.1016/J.CLSR.2023.105801.

[14] N. I. Park *et al.*, "Advanced forensic method to authenticate audio files from Tizen-based Samsung Galaxy Watches," *Forensic Sci. Int. Digit. Investig.*, vol. 48, p. 301697, Mar. 2024, doi: 10.1016/J.FSIDI.2024.301697.

[15] C. M. Miller, "A survey of prosecutors and investigators using digital evidence: A starting point," *Forensic Sci. Int. Synerg.*, vol. 6, p. 100296, Jan. 2023, doi: 10.1016/J.FSISYN.2022.100296.

[16] M. B. Rahayu, "Polisi Duga Panitia Diksar Mapala UII Hapus Seluruh File Kegiatan," DetikNews. Accessed: Jul. 08, 2024.

[17] D. Dunsin, M. C. Ghanem, K. Ouazzane, and V. Vassilev, "A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response," *Forensic Sci. Int. Digit. Investig.*, vol. 48, p. 301675, Mar. 2024, doi: 10.1016/J.FSIDI.2023.301675.

[18] A. Yudhana, Imam Riadi, and Budi Putra, "Digital Forensic on Secure Digital High Capacity using DFRWS Method," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 6, no. 6, pp. 1021–1027, Dec. 2022, doi: 10.29207/resti.v6i6.4615.

[19] Y. Wei, N. Zheng, and M. Xu, "An automatic carving method for RAR file based on content and structure," *Proc. - 2nd Int. Conf. Inf. Technol. Comput. Sci. ITCS 2010*, pp. 68–72, 2010, doi: 10.1109/ITCS.2010.23.

[20] F. Barr-Smith, T. Farrant, B. Leonard-Lagarde, D. Rigby, S. Rigby, and F. Sibley-Calder, "Dead Man's Switch: Forensic Autopsy of the Nintendo Switch," *Forensic Sci. Int. Digit. Investig.*, vol. 36, p. 301110, Apr. 2021, doi: 10.1016/J.FSIDI.2021.301110.

[21] M. Samiullah, W. Aslam, S. Sadiq, A. Mehmood, and G. S. Choi, "Hyperchaos and MD5 Based Efficient Color Image Cipher," *Comput. Mater. Contin.*, vol. 72, no. 1, pp. 1645–1670, Feb. 2022, doi: 10.32604/CMC.2022.021019.

[22] H. Heath, Á. MacDermott, and A. Akinbi, "Forensic analysis of ephemeral messaging applications: Disappearing messages or evidential data?," *Forensic Sci. Int. Digit. Investig.*, vol. 46, p. 301585, Sep. 2023, doi: 10.1016/J.FSIDI.2023.301585.

[23] G. Horsman, "ACPO principles for digital evidence: Time for an update?," *Forensic Sci. Int. Reports*, vol. 2, p. 100076, Dec. 2020, doi: 10.1016/J.FSIR.2020.100076.

[24] G. Thornton and P. Bagheri Zadeh, "An investigation into Unmanned Aerial System (UAS) forensics: Data extraction & analysis," *Forensic Sci. Int. Digit. Investig.*, vol. 41, p. 301379, Jun. 2022, doi: 10.1016/J.FSIDI.2022.301379.

[25] S. Brotsis *et al.*, "Blockchain meets Internet of Things (IoT) forensics: A unified framework for IoT ecosystems," *Internet of Things*, vol. 24, p. 100968, Dec. 2023, doi: 10.1016/J.IOT.2023.100968.

[26] E. Mantas and C. Patsakis, "Who watches the new watchmen? The challenges for drone digital forensics investigations," *Array*, vol. 14, p. 100135, Jul. 2022, doi: 10.1016/J.ARRAY.2022.100135.

[27] N. S. Vaidya and P. H. Rughani, "A forensic study of Tor usage on the Raspberry Pi platform using open source tools," *Comput. Fraud Secur.*, vol. 2020, no. 6, pp. 13–19, Jun. 2020, doi: 10.1016/S1361-3723(20)30064-6.

[28] X. Fernández-Fuentes, T. F. Pena, and J. C. Cabaleiro, "Digital forensic analysis methodology for private browsing: Firefox and Chrome on Linux as a case study," *Comput. Secur.*, vol. 115, p. 102626, Apr. 2022, doi: 10.1016/J.COSE.2022.102626.

[29] R. Nordvik and S. Axelsson, "It is about time–Do exFAT implementations handle timestamps correctly?," *Forensic Sci. Int. Digit. Investig.*, vol. 42–43, p. 301476, Oct. 2022, doi: 10.1016/J.FSIDI.2022.301476.

[30] P. Sommer, "Evidence from hacking: A few tiresome problems," *Forensic Sci. Int. Digit. Investig.*, vol. 40, p. 301333, Mar. 2022, doi: 10.1016/J.FSIDI.2022.301333.

[31] G. Horsman, "Conducting a 'manual examination' of a device as part of a digital investigation," *Forensic Sci. Int. Digit. Investig.*, vol. 40, p. 301331, Mar. 2022, doi: 10.1016/J.FSIDI.2021.301331.

[32] J. Gruber, L. L. Voigt, Z. Benenson, and F. C. Freiling, "Foundations of cybercriminalistics: From general process models to case-specific concretizations in cybercrime investigations," *Forensic Sci. Int. Digit. Investig.*, vol. 43, p. 301438, Sep. 2022, doi: 10.1016/J.FSIDI.2022.301438.

[33] D. Kane *et al.*, "Storage of evidence and delayed reporting after sexual assault: Rates and impact factors on subsequent reporting," *J. Forensic Leg. Med.*, vol. 106, p. 102731, Aug. 2024, doi: 10.1016/J.JFLM.2024.102731.

[34] D. Rani, N. S. Gill, and P. Gulia, "A forensic framework to improve digital image evidence administration in IIoT☆," *J. Ind. Inf. Integr.*, vol. 38, p. 100568, Mar. 2024, doi: 10.1016/J.JII.2024.100568.

[35] A. Holmes and W. J. Buchanan, "A framework for live host-based Bitcoin wallet forensics and triage," *Forensic Sci. Int. Digit. Investig.*, vol. 44, p. 301486, Mar. 2023, doi: 10.1016/J.FSIDI.2022.301486.

[36] Amirullah, "Detik-detik KKB Papua Tembak Polisi yang Berada di Mobil Tengah Melintas, Videonya Viral," *Serambinews*, Mar. 25, 2024.

[37] A. nasrudin Yahya, "Titik Terang Pembebasan Pilot Susi Air Usai Setahun Disandera KKB," *Kompas*, Feb. 06, 2024.