



Akuisisi Bukti Digital Pada *Network Attached Storage* (NAS)

Arif Faizal

21917024

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensika Digital

Program Studi Informatika Program Magister

Fakultas Teknologi Industri

Universitas Islam Indonesia

2024

Lembar Pengesahan Pembimbing

Akuisisi Bukti Digital Pada *Network Attached Storage* (NAS)

Arif Faizal

21917024



Yogyakarta, 6 Juni 2024

Dr. Ahmad Luthfi, S.Kom., M.Kom.

Lembar Pengesahan Penguji

Akuisisi Bukti Digital Pada *Network Attached Storage* (NAS)

Arif Faizal

21917024

Yogyakarta, 2 Juli 2024

Tim Penguji,

Dr. Yudi Prayudi, S.Si., M.Kom.

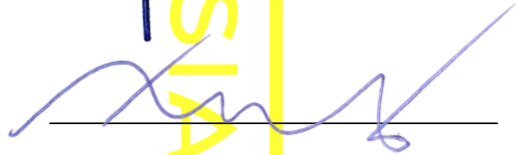
Ketua

Dr. Ahmad Luthfi, S.Kom., M.Kom.

Anggota I

Irving Vitra Paputungan, S.T., M.Sc., Ph.D.

Anggota II



13/08/2024

Mengetahui,

Ketua Program Studi Informatika Program Magister

Fakultas Teknologi Industri

Universitas Islam Indonesia



Irving Vitra Paputungan, S.T., M.Sc., Ph.D.

Abstrak

Akuisisi Bukti Digital Pada Network Attached Storage (NAS)

Dalam melakukan investigasi terhadap suatu bukti elektronik, tahapan akuisisi adalah tahapan awal yang sangat mempengaruhi tahapan analisis bukti digital. Selain itu, kemampuan investigator dalam melakukan akuisisi terhadap bukti elektronik juga sangat berpengaruh terhadap kedudukan bukti tersebut di dalam sebuah persidangan. *Network Attached Storage* (NAS) adalah salah satu metode penyimpanan berbasis jaringan yang saat ini semakin banyak digunakan. Metode penyimpanan NAS sebagian besar menggunakan sistem penyimpanan berbasis *Redundant Array of Independent Disks* (RAID). Akan tetapi sistem RAID ini bukan merupakan satu-satunya yang digunakan didalam NAS. Beberapa kasus yang pernah terjadi terkait NAS pada sebuah perusahaan penerbangan nasional yaitu aktivitas perusakan dan penghapusan data perusahaan yang dilakukan oleh karyawan sebagai protes akan kebijakan yang tidak dapat diterima oleh karyawan tersebut. Dengan karakteristik NAS yang merupakan penyimpanan berbasis jaringan, penanganan untuk pengangkatan dan pemulihan (*recovery*) data pada NAS membutuhkan teknik dan cara yang berbeda dengan penanganan pada bukti elektronik lainnya seperti *Personal Computer* (PC). Ditambah lagi, dengan konsep RAID pada pengelolaan harddisk NAS, menjadikan tahapan akuisisi pada model penyimpanan ini membutuhkan pengetahuan pada konsep penyimpanan RAID. Penelitian ini bertujuan untuk melakukan analisis tingkat keberhasilan dari proses akuisisi di dalam sistem penyimpanan NAS. Standar yang digunakan sebagai panduan dalam melakukan akuisisi bukti digital dalam laporan ini menggunakan *National Institute of Standards and Technology* (NIST) yang merupakan standar yang paling efektif dalam proses pencarian artefak suatu bukti digital pada perangkat keras dengan metode akuisisi fisik.

Kata kunci

Digital Forensics, Akuisisi, NAS, RAID, NIST

Abstract

Digital Evidence Acquisition on Network Attached Storage

In the process of investigating electronic evidence, the acquisition phase is the initial stage that significantly influences the digital evidence analysis phase. Furthermore, an investigator's ability to acquire electronic evidence also greatly impacts the admissibility of that evidence in a courtroom setting. NAS users are not limited to industrial settings; it has become widely adopted for personal use as well. NAS storage methods primarily utilize Redundant Array of Independent Disks (RAID) storage systems. However, RAID systems are not the sole ones employed within NAS devices. One noteworthy case involving NAS occurred at a national airline company, where data destruction and deletion activities were carried out by an employee as a protest against unacceptable company policies. Due to NAS's network-based storage characteristics, handling data recovery on NAS devices requires different techniques compared to other electronic evidence sources like personal computers (PCs). Furthermore, with the RAID concept in NAS storage management, the acquisition phase in this storage model demands familiarity with RAID storage principles. This study aims to analyse the success rate of the acquisition process within NAS storage systems. The standard employed for digital evidence acquisition in this report utilizes the National Institute of Standards and Technology (NIST) standard, an effective standard approach for artifact retrieval at the hardware of digital evidence with a physical method.

Keywords

Digital Forensics, Digital Forensics Acquisition, NAS, RAID, NIST

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, {Bulan pengajuan tesis untuk ujian, tahun}



Arif Faizal, S.Kom

Daftar Publikasi

Publikasi berikut menjadi bagian dari Bab 3

Comparison Study of NIST SP 800-86 and ISO/IEC 27037 Standards as A Framework for Digital Forensic Evidence Analysis

Journal of Information Systems and Informatics

<https://journal-isi.org/index.php/isi/article/view/717>

Sitasi publikasi:

Kontributor	Jenis Kontribusi
Arif Faizal	Mendesain eksperimen (60%) Menulis <i>paper</i> (70%)
Ahmad Luthfi	Mendesain eksperimen (40%) Menulis dan mengedit <i>paper</i> (30%)

Halaman Kontribusi

Tidak ada kontribusi dari pihak lain.

Halaman Persembahan

Laporan penulisan ini saya persembahkan untuk

Indonesia

“Selalu bangga dengan garuda dan merah putih”

Kedua **orang tua** yang tak henti mendoakan yang terbaik

Istriku tercinta yang selalu sabar mendengar dan mendampingi

*My Beloved child, **Ridwan** and **Afiqoh***

Kata Pengantar

Bismillahirrahmaanirrahiim.

Asyhadu an laa ila ha illallah, wa asyhadu anna muhammadan Rasulullah.

Assalamu 'alaikum Warahmatullahi Wabarakaatuh.

Alhamdulillahirobbil alamin washolatu wassalamu ala asrofil anbiya wal Mursalin Sayyidina wa Maulana Muhammadin wa ala alihi wa shohbihi ajma'in Amma ba'du.

Puji dan syukur tak kan henti kami panjatkan kehadiran Allah Subhanahu wa ta'ala atas segala limpahan rahman dan rahiim yang telah diberikan. Tak henti pula kami panjatkan sholawat serta salam atas suri tauladan kami, Rasulullah Shalallahu Alaihi Wassalam.

Pada kesempatan ini, kami ingin mengucapkan rasa syukur yang sebesar-besarnya atas selesainya penulisan laporan akhir ini untuk meraih gelar Magister untuk bidang studi Informatika di Universitas Islam Indonesia.

Ucapan terimakasih yang mendalam kami sampaikan kepada, Dr. Ahmad Luthfi, M.Kom, selaku dosen pembimbing yang telah mencurahkan waktu, tenaga, dan pikirannya dalam membimbing kami selama proses penelitian ini. Arahan dan motivasinya yang penuh inspiratif telah membuka cakrawala baru dalam perspektif kami di dunia akademik. Berkat bimbingan beliau, kami mampu menyelesaikan penelitian ini dengan penuh keyakinan dan rasa tanggung jawab. Kepada Dr. Yudi Prayudi, M.Kom, dan seluruh dosen pengajar yang telah dengan sabar dan ikhlas membagikan ilmu pengetahuan dan wawasannya yang luas. Dedikasi dan semangat beliau dalam mengajar telah menjadi inspirasi bagi kami untuk terus belajar dan mengembangkan diri. Kepada seluruh tenaga pendidikan yang telah membantu kami dalam proses penyelesaian penelitian ini, baik secara langsung maupun tidak langsung. Dukungan dan bantuan mereka sangat berarti bagi kami. Tanpa dukungan dan bimbingan dari semua pihak, kami tidak akan mampu menyelesaikan penelitian ini dengan baik. Oleh karena itu, kami mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu kami.

Ucapan terimakasih juga ingin kami sampaikan kepada orang tua tercinta yang selalu memberikan dukungan, semangat dan doa tiada yang henti. Tanpa dukungan beliau-beliau, kami tidak akan mampu mencapai kesuksesan ini. Kepada seluruh keluarga, rekan dan kolega yang telah memberikan semangat dan bantuan yang sangat berarti dalam proses penyelesaian laporan ini. Tak lupa juga kami ingin menyampaikan terima kasih untuk rekan-rekan di Program Studi Forensika Digital untuk diskusi, sharing maupun kolaborasi serta pengalaman yang sangat berharga yang telah diberikan. Kami juga ingin mengucapkan

terima kasih kepada pihak-pihak lain yang telah membantu kami dalam menyelesaikan penelitian ini, baik secara langsung maupun tidak langsung.

Harapan kami, jerih payah yang telah kami curahkan dalam penyusunan laporan ini dapat memberikan sumbangsih yang berarti bagi perkembangan ilmu Informatika, khususnya dalam bidang studi Forensika Digital. Kami ingin laporan ini menjadi salah satu batu loncatan dalam upaya memajukan ilmu pengetahuan dan teknologi di bidang ini.

Kami percaya bahwa penelitian ini membuka jalan bagi penelitian-penelitian selanjutnya, baik untuk menyempurnakan metode dan konsep yang telah kami ajukan, maupun untuk mengeksplorasi peluang-peluang baru dalam bidang Forensika Digital. Laporan ini diharapkan dapat menjadi inspirasi bagi para peneliti dan akademisi untuk terus berkarya dan menghasilkan temuan-temuan yang bermanfaat bagi masyarakat.

Lebih lanjut, kami berharap laporan ini dapat menjadi sumber informasi yang berharga bagi para praktisi Forensika Digital dalam menjalankan tugasnya. Dengan memahami metode dan konsep yang telah kami paparkan, para praktisi diharapkan dapat lebih efektif dan efisien dalam menangani berbagai kasus yang berkaitan dengan forensika digital.

Kami menyadari bahwa laporan ini masih memiliki banyak kekurangan. Oleh karena itu, kami terbuka atas kritik dan saran yang membangun dari para pembaca. Semoga laporan ini dapat memberikan manfaat yang sebesar-besarnya bagi kemajuan ilmu pengetahuan dan teknologi, khususnya dalam bidang Forensika Digital.

Bismillahirrahmaanirrahiim

إِنَّ فِي خَلْقِ السَّمَاوَاتِ وَالْأَرْضِ وَاخْتِلَافِ اللَّيْلِ وَالنَّهَارِ لَآيَاتٍ لِّلْعَاقِلِينَ

"Sesungguhnya dalam penciptaan langit dan bumi, dan pergantian malam dan siang, terdapat tanda-tanda (kebesaran Allah) bagi orang-orang yang berakal." (QS. Ali Imran: 190)

Wabillahi taufiq wal hidayah

Wassalamu 'alaikum Warahmatullahi Wabarakaatuuuh

Arif Faizal

Daftar Isi

Lembar Pengesahan Pembimbing.....	i
Lembar Pengesahan Penguji.....	ii
Abstrak.....	iii
Abstract.....	iv
Pernyataan Keaslian Tulisan.....	v
Daftar Publikasi	vi
Halaman Kontribusi	vii
Halaman Persembahan.....	viii
Kata Pengantar.....	ix
Daftar Isi	xi
Daftar Tabel	xiii
Daftar Gambar	xiv
Glosarium.....	xvi
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah	4
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	4
1.6 Luaran Penelitian	4
1.7 Sistematika Penulisan	5
BAB 2 TINJAUAN PUSTAKA	6
2.1 Kajian Pustaka	6
2.1.1 Penelitian Terdahulu.....	8
2.2 Konsep Pengetahuan.....	13
2.2.1 Forensika Digital	13

2.2.2	Akuisisi	14
2.2.3	NAS	15
2.2.4	NIST SP 800-86.....	16
BAB 3 METODOLOGI.....		19
3.1	Langkah-langkah Penelitian.....	19
3.2	Skenario dan alat.....	20
3.3	Akuisisi	20
3.3.1	Perencanaan	21
3.3.2	Pengamanan TKP	23
3.3.3	Akuisisi	24
BAB 4 HASIL DAN PEMBAHASAN		26
4.1	Perencanaan	26
4.1.1	Identifikasi Barang Bukti Digital	26
4.1.2	Penilaian risiko	27
4.1.3	Pemilihan metode kerja	27
4.1.4	Persiapan dokumen.....	28
4.2	Pengamanan TKP.....	28
4.2.1	<i>Log spesifikasi Hardware</i>	29
4.2.2	Pengamanan Area Kerja	31
4.3	Akuisisi	31
4.3.1	Verifikasi Integritas	32
4.3.2	Dokumentasi Proses	32
4.4	Evaluasi hasil akuisisi	33
BAB 5 KESIMPULAN DAN SARAN		36
5.1	Kesimpulan	36
5.2	Saran	37

Daftar Tabel

Tabel 2. 1 Penelitian dengan perbedaan metode atau standar yang digunakan dalam akuisisi bukti digital beserta aspek kritisnya.	9
Tabel 2. 2 Penelitian dengan perbedaan jenis penyimpanan yang digunakan dalam akuisisi bukti digital beserta aspek kritisnya.	11
Tabel 4. 1 Identifikasi barang bukti.....	26
Tabel 4. 2 Log spesifikasi NAS pada pengujian	29
Tabel 4. 3 Pengujian <i>imaging</i> NAS <i>disk drive</i>	33
Tabel 4. 4 Pengambilan nilai <i>hash</i> pada <i>image</i>	34
Tabel 4. 5 Eksaminasi singkat dari image yang didapat.....	35

Daftar Gambar

Gambar 2. 1 Kerangka Kerja DFRWS	6
Gambar 2. 2 Kerangka Kerja NIST SP 800-86	7
 Gambar 3 1. Tahapan proses akusisi	19
 Gambar 4. 1 OSForensics	27
Gambar 4. 2 ReclaiMe.....	28
Gambar 4. 3 Disk Penyimpanan 1	29
Gambar 4. 4 Disk penyimpanan 2	30
Gambar 4. 5 Disk penyimpanan 3	30
Gambar 4. 6 usbwireprotector inisiasi proses.....	31
Gambar 4. 7 usbwriteprotection inisiasi ON	31
Gambar 4. 8 penentuan <i>hash</i> yang digunakan pada hasil <i>imaging</i>	32
Gambar 4. 9 File log dari akuisisi pada OSForensics.....	34
 Gambar A. 1 Proses unduh file ISO TrueNAS Core	43
Gambar A. 2 Checksum dan PGP Key file unduhan.....	43
Gambar A. 3 verifikasi SHA256 pada file iso TrueNAS Core	44
Gambar A. 4 Menu TrueNAS <i>Installer</i>	44
Gambar A. 5 Progress instalasi TrueNAS	45
Gambar A. 6 Menu konsol <i>setup</i> TrueNAS	45
Gambar A. 7 Memilih hddisk yang akan diinstall sistem operasi TrueNAS	46
Gambar A. 8 Konfirmasi persetujuan penghapusan data pada <i>disk drive</i>	46
Gambar A. 9 Pemberian kata sandi untuk user <i>root</i>	47
Gambar A. 10 Pilihan untuk <i>boot option UEFI</i> dan <i>BIOS (Legacy)</i>	47
Gambar A. 11 Membuat partisi <i>Swap</i>	48
Gambar A. 12 Proses instalasi TrueNAS	48
Gambar A. 13 Konfirmasi melepas USB drive dan menyalakan ulang komputer.....	49
Gambar A. 14 Menyalakan ulang dan <i>booting</i> komputer	49
Gambar A. 15 Menu awal TrueNAS pada terminal	50
Gambar A. 16 Tampilan login TrueNAS core	51
Gambar A. 17 Dashboard pada TrueNAS core	51

Gambar A. 18 Penambahan pengguna baru	52
Gambar A. 19 Penambahan grup pengguna baru	52
Gambar A. 20 Membuat <i>pool</i> baru.....	53
Gambar A. 21 Pool Manager untuk menambahkan disk drive.....	54
Gambar A. 22 Ubah posisi disk drive ke Data VDevs	54
Gambar A. 23 Konfigurasi pada <i>pool</i> untuk penyimpanan	55
Gambar A. 24 <i>Pool</i> yang baru dibuat.....	55
Gambar A. 25 Penambahan konfigurasi untuk <i>sharing</i>	56
Gambar A. 26 File Sharing yang telah di konfigurasi	57
Gambar A. 27 SMB file sharing di windows 11	57
Gambar A. 28 Pengaturan protokol dan <i>auto starting</i> pada menu <i>services</i>	58
Gambar B. 1 Proses <i>disk drive imaging</i> pada OSForensics	59
Gambar B. 2 Memilih <i>disk drive</i> yang akan di proses <i>imaging</i>	59
Gambar B. 3 Proses penambahan <i>disk drive</i> di OSForensics untuk <i>imaging</i>	60
Gambar B. 4 Proses <i>imaging</i>	60
Gambar B. 5 File <i>log</i> hasil <i>imaging</i>	61
Gambar B. 6 Proses <i>imaging</i> dari <i>image</i> yang didapat dari tiap <i>disk</i> fisik.....	61
Gambar C. 1 Tampilan awal ReclaiMe File Recovery.....	62
Gambar C. 2 Memilih tipe hasil <i>imaging</i>	63
Gambar C. 3 menyimpan file hasil <i>imaging</i>	63
Gambar C. 4 Proses <i>imaging</i>	63
Gambar C. 5 Hasil <i>imaging</i> menggunakan ReclaiMe File Recovery.....	64

Glosarium

AFP	- Apple File Protocol
BIOS	- Basic Input Output System
CFSP	- Computer Forensics Special Publications
CFTT	- Cloud Forensics Tools Testing
CPU	- Central Processing Unit
DNS	- Domain Name System
DRP	- Disaster Recovery Plan
FTK	- Forensics Tool Kit
GCFIM	- Generic Computer Forensic Investigation Model
GRR	- GRR Rapid Response
HDD	- Hard Disk Drive
IEC	- International Electrotechnical Commission
iSCSI	- Internet Small Computer Systems Interface
ISO	- International of Organisation for Standardization
NAS	- Network Attached Storage
NFS	- Network File Sharing
NIJ	- National Institute of Justice
NIST	- National Institute of Standards and Technology
NTFS	- New Technology File System
OMV	- Open Media Vault
PC	- Personal Computer
RAID	- Redundant Array of Independent Disks
RAM	- Random Access Memory
SAN	- Storage Area network
SMART	- Self Monitoring Analysis and Reporting
SMB	- Server Message Block
SSD	- Solid State Drive
TKP	- Tempat Kejadian Perkara
UEFI	- Unified Extensible Firmware Interface
UPS	- Uninterruptible Power Supply
USB	- Universal Serial Bus
webDAV	- web Distributed Authoring and Versioning
ZFS	- Zettabyte File System

BAB 1

Pendahuluan

1.1 Latar Belakang

Dalam proses akuisisi pada media penyimpanan, hasil verifikasi terhadap barang bukti digital utama dan barang bukti hasil penggandaan tidak boleh memiliki perbedaan dari sisi kuantitas dan jejak waktu di dalamnya atau yang dikenal dengan integritas bukti. Hal ini dapat dilakukan menggunakan metode akuisisi secara fisik, yaitu penggandaan langsung pada perangkat menggunakan metode *disk to disk copy*. Namun pada keadaan tertentu, seperti halnya pada sebuah sistem yang sifatnya kritis dan tidak boleh dimatikan, maka diperkenankan untuk melakukan akuisisi secara logikal. Proses akuisisi logikal yaitu hanya menyalin berkas atau artefak dan termasuk diantaranya mengakuisisi partisi yang dibutuhkan. Dalam proses akuisisi *logical*, berkas yang telah terhapus tidak dapat tersalin (Hariyadi & Supriyono, 2017).

Network Attached Storage (NAS) adalah perangkat penyimpanan data yang terhubung menggunakan jaringan komputer. Sebagai salah satu metode penyimpanan, NAS bertindak sebagai sebuah server file di dalam jaringan yang menyediakan penyimpanan berupa data di dalam jaringan independen tempat komputer klien dapat terhubung. NAS dapat dianggap sebagai *drive* komputer (melalui *ethernet*) dan digunakan untuk menyimpan dan membaca dokumen atau file (Kumar, Nagaraj, Paul, & Dixit, 2021).

Ketika pengguna NAS melakukan penghapusan data baik secara sengaja atau tidak disengaja, di dalam antarmuka pengguna maka tidak terdapat pilihan untuk melakukan pengulangan proses seperti halnya pada *recycle bin* di windows atau *trash folder* pada linux. Hal ini menjadikan penghapusan file menjadi sangat riskan karena tidak terdapat metode *undo* dalam tindakan penghapusan data (Riadi, Sunardi, & Hadi, 2020).

Permasalahan lainnya, tata kelola perangkat penyimpanan yang terdapat pada server NAS biasanya menggunakan format *Redundant Array of Independent Disks* (RAID) dimana hal ini akan memudahkan dalam melakukan clustering terhadap harddisk sehingga kapasitas penyimpanan akan dapat menjadi lebih besar dan juga metode ini akan sekaligus membuat mekanisme *mirroring backup* terhadap *hard drive* (Choi, Park, & Lee, 2020).

Semua produsen Besar NAS seperti QNap, synology dan Asustor selain memiliki produk korporasi, mereka juga memiliki produk-produk yang dirancang untuk kebutuhan

personal atau produk rumahan. Dengan demikian, penggunaan NAS di lingkungan personal atau rumah akan menjadi kebutuhan dasar di masa depan dimana konsep *smart home* selain menggunakan sensor, penyimpanan juga akan menjadi bagian yang tidak terpisahkan (J, Surya, Surya, & Shriram, 2021).

Ketika sebuah perusahaan atau perseorangan menggunakan NAS, terdapat beberapa hal yang menjadi tantangan. NAS merupakan salah satu metode penyimpanan yang menggunakan konsep jaringan dalam implementasinya (Adji, Eduardus, Michael, Minawati, & Budiharto, 2021), maka konsep *Network Security* merupakan tantangan yang sangat mungkin dihadapi dalam implementasinya NAS Server. beberapa diantaranya :

1. *Confidentiality*, Data yang tersimpan didalam Server memungkinkan untuk dapat digunakan bersama, sehingga diperlukan batasan terhadap pengguna yang menggunakan data tersebut.
2. *Integrity*, Keamanan data terpusat pada NAS server karena seluruh data tersimpan secara sentral dan ini memberikan jaminan bahwa informasi yang berada di dalam server dapat dipercaya dan akurat.
3. *Availability*, Diperlukan konsep *disaster recovery* untuk menjaga *availability* terhadap data yang disimpan di dalam server (Freeman & Miller, 2000).

Melakukan akuisisi terhadap barang bukti digital merupakan aktivitas keilmuan yang berdasarkan saintifikasi. Standar yang digunakan dalam proses ini diatur dalam beberapa panduan yang dibuat oleh lembaga standarisasi internasional. Beberapa diantaranya, ISO yaitu *International of Organisation for Standardization* yang merupakan lembaga nirlaba internasional yang menetapkan standar untuk industri dan komersial. Panduan yang terkait dengan penanganan barang bukti digital terdapat pada standard ISO/IEC 27037:2012 yaitu tentang panduan dalam melakukan aktivitas penanganan barang bukti digital. Penanganan barang bukti digital yang disebutkan dalam standar ini adalah *identification, collection, acquisition and preservation* (Ajijola, Zavorsky, & Ruhl, 2014).

Selain ISO/IEC 27037:2012, standar yang juga mengatur tentang panduan dalam aktivitas penanganan bukti digital juga diatur oleh *National Institute of Standards and Technology* (NIST). Dokumen yang menjelaskan tentang standar ini terdapat pada *Special Publication 800-86* yang menjelaskan tentang *Collection, Examination, Analysis and Reporting* (Kent, Chevalier, Grance, & Dang, n.d.).

Dalam kaitannya dengan forensika digital, penggunaan NAS yang masih banyak didominasi oleh kalangan industri, memiliki beberapa peranan yang sangat diperlukan. Data

digital yang tersimpan dalam penyimpanan ini merupakan aset yang sangat berharga yang merupakan jejak digital (Koroniotis, Moustafa, & Sitnikova, 2019). Permasalahan yang mungkin terjadi terkait dengan kasus digital diantaranya, pencurian, penghilangan maupun modifikasi dokumen elektronik.

Salah satu kasus yang pernah dilaporkan terkait kasus pada sistem penyimpanan NAS ini yaitu pada tahun 2021 pada sebuah perusahaan nasional yang bergerak di bidang transportasi udara. Pada periode tersebut telah dilaporkan terjadi pencurian dan penghilangan dokumen yang dilakukan oleh salah satu pegawai yang bekerja disana dengan tujuan untuk keuntungan pribadi. Jenis dokumen tersebut adalah file PDF yang diambil dengan melakukan perintah potong dan tempel. Sementara, hak pengguna yang digunakan untuk mengakses file ini dilakukan secara ilegal yaitu menggunakan hak pengguna yang bukan milik pegawai tersebut.

Kontribusi penelitian ini adalah melakukan skenario kasus yang melibatkan bukti digital dan melakukan akuisisi terhadap bukti tersebut menggunakan panduan pada standar NIST. Namun, bukti digital yang digunakan berada dalam server yang menggunakan sistem penyimpanan NAS. Pemilihan standar NIST sebagai panduan dalam penelitian ini adalah karena standar NIST teruji lebih efektif untuk melakukan akuisisi pada perangkat yang menggunakan metode akuisisi fisik seperti pada NAS. Kebaruan penelitian ini adalah melakukan akuisisi bukti digital dalam sistem penyimpanan NAS dengan berbagai karakteristik dan batasan yang berada didalamnya. Standar yang digunakan dalam penelitian ini adalah menggunakan NIST SP 800-86 yang memiliki panduan dalam melakukan akuisisi dengan metode fisik. Model diharapkan dapat menjadi referensi dalam melakukan analisis terhadap bukti digital pada sistem penyimpanan NAS kedepannya.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, maka dirumuskan masalah yang akan dibahas pada penelitian ini yaitu bagaimana teknik dalam melakukan akuisisi sistem penyimpanan NAS menggunakan standar NIST untuk mendapatkan hasil akuisisi bukti digital yang diharapkan.

1.3 Batasan Masalah

Dalam penelitian ini, penulis membatasi permasalahan pada beberapa topik diantaranya :

1. Penelitian ini dilakukan dalam simulasi pada server NAS yang memiliki 3 buah perangkat keras untuk penyimpanan .
2. Penelitian menggunakan standar NIST sebagai panduan dalam melakukan akuisisi terhadap bukti digital.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah untuk mengetahui teknik dan hasil yang didapatkan pada akuisisi bukti digital dalam sistem penyimpanan NAS menggunakan panduan pada standar NIST.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat diantaranya :

1. Pengembangan keilmuan dalam kaitannya dengan akuisisi bukti digital pada bidang keilmuan forensika digital.
2. Memberikan sumbangsih informasi tentang bagaimana analisis forensika digital terhadap sistem penyimpanan NAS
3. Mengembangkan penelitian-penelitian sebelumnya yang berkaitan dengan *digital evidence acquisition, digital evidence storage* dan *network attached storage*.

1.6 Luaran Penelitian

Melalui publikasi di jurnal Sinta, penelitian ini diharapkan dapat memberikan manfaat bagi berbagai pihak. Bagi komunitas ilmiah, publikasi ini dapat menjadi sumber referensi yang berharga. Bagi praktisi keamanan informasi, temuan dalam penelitian ini dapat diaplikasikan untuk meningkatkan keamanan sistem mereka. Sementara itu, bagi peneliti dan institusi, publikasi ini dapat meningkatkan reputasi dan memperkuat posisi mereka di bidang keamanan siber.

1.7 Sistematika Penulisan

Dalam penyusunan penulisan ini untuk memberikan gambaran terkait dengan penjelasan maka digunakan sebuah sistematika penulisan sebagai berikut:

BAB 1 PENDAHULUAN

Pada bab ini menjelaskan pendahuluan yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan luaran penelitian.

BAB 2 TINJAUAN PUSTAKA

Pada bab ini menjelaskan teori-teori dan penelitian-penelitian yang berhubungan dengan akuisisi barang bukti digital dengan metode atau standar dan tipe barang bukti digital yang digunakan.

BAB 3 METODOLOGI

Pada bab ini membahas tentang langkah-langkah penelitian akuisisi sistem penyimpanan NAS dari persiapan skenario dan alat hingga proses akuisisi dengan tahapan perencanaan, pengamanan TKP dan akuisisi.

BAB 4 HASIL DAN PEMBAHASAN

Bab ini berisi pembahasan tentang cara akuisisi pada sistem penyimpanan NAS dan analisis pengujian yang dilakukan.

BAB V KESIMPULAN DAN SARAN

Kesimpulan dan saran, berisi kesimpulan dari penelitian dan saran yang memperhatikan keterbatasan temuan dalam penelitian dan rekomendasi untuk penelitian selanjutnya

BAB 2

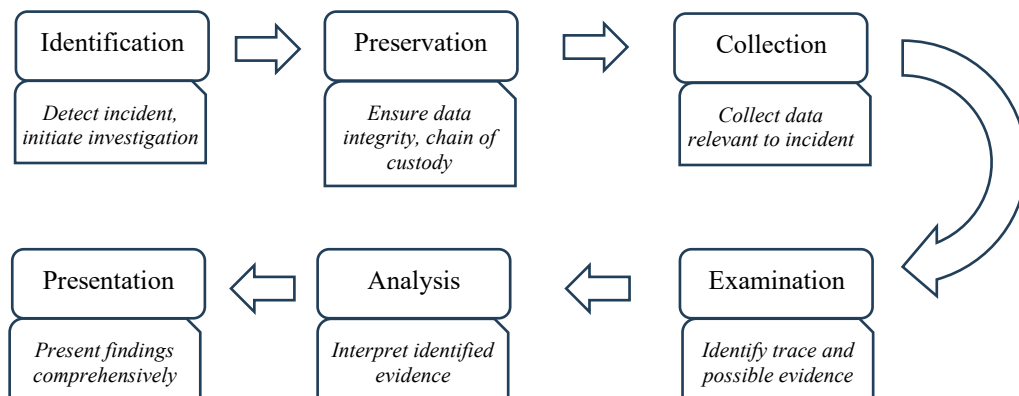
Tinjauan Pustaka

2.1 Kajian Pustaka

Dengan menggunakan penelitian eksperimental, serangkaian investigasi forensik mampu mengidentifikasi bukti digital pada *smartphone* android dengan akuisisi forensik langsung pada partisi, aplikasi, dan proses RAM android yang masih berjalan (Rochmadi et al., 2020).

Terdapat banyak tantangan dan kesulitan yang dihadapi dalam mendapatkan bukti digital dalam perangkat seluler (Wirara, Hardiawan, & Salman, 2020). Beberapa tantangan dalam teknologi telepon seluler tersebut menyebabkan akuisisi bukti digital menjadi lebih sulit.

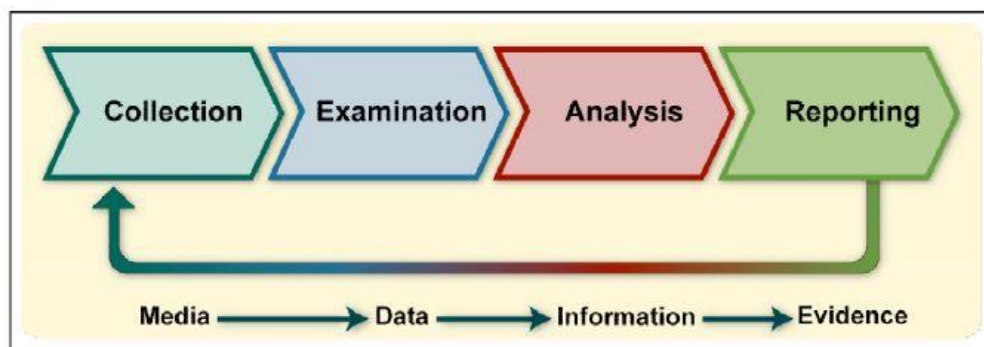
Digital Forensics Research Workshop (DFRWS) merupakan kerangka kerja ilmiah yang memiliki dasar dan terbukti untuk proses investigasi forensik yang meliputi pemeliharaan, pengumpulan, validasi, identifikasi, analisis, interpretasi, dokumentasi, dan presentasi bukti digital (Koroniotis et al., 2019). Proses investigasi forensik tersebut berasal dari sumber-sumber digital dari tempat perkara atau alat dilakukannya kejadian *cybercrime* untuk tujuan memfasilitasi atau melanjutkan rekonstruksi peristiwa yang melanggar hukum teknologi informasi dan mengandung pidana, atau membantu untuk mengantisipasi tindakan yang merusak keaslian barang bukti sehingga membuat barang bukti yang telah didapatkan menjadi tidak sah di mata hukum dan terbukti mengganggu untuk operasi yang direncanakan dalam proses investigasi .



Gambar 2. 1 Kerangka Kerja DFRWS

Penjelasan pada gambar kerangka DFRWS diatas yaitu tahap identifikasi (*identification*) melakukan perancangan kebutuhan yang diperlukan untuk membantu penyelidikan dalam pencarian bukti, tahap pemeliharaan (*preservation*) menjaga keaslian dan keamanan bukti digital agar sah di mata hukum, tahap pengumpulan (*collection*) mengumpulkan barang bukti yang memperkuat persidangan kuat, tahap pemeriksaan (*examination*) menentukan apa saja yang akan dianalisis atau filterisasi data, tahap analisis (*analysis*) mencari dan menganalisis barang bukti dalam pengolahan data yang telah didapat, tahap presentasi (*presentation*) melaporkan dan mempresentasikan hasil analisis sehingga dapat dipahami oleh publik dan berlaku di meja persidangan. (Riadi, Sunardi, & Widiandana, 2020)

Identification adalah proses memilah barang bukti fisik oleh investigator dari tindak kejahatan komputer untuk dijadikan bukti otentik pada saat proses penyidikan. Proses *identification* berupa pelabelan dan perekaman untuk keutuhan barang bukti fisik. *Collection* adalah proses duplikasi dari barang bukti fisik yang otentik ke bukti digital untuk menjaga integritas barang bukti dari perubahan atau kontaminasi. Proses penjagaan barang bukti fisik dan membuat duplikasi menjadi *file image* ini disebut dengan akuisisi. *Examination* atau pemeriksaan adalah proses ekstraksi hasil image sehingga data digital yang ada didalamnya sama dengan barang bukti fisik. Tahapan ini memastikan data yang didapat asli dan akan diperiksa validasinya dengan menggunakan *hashing*. *Analysis* adalah proses pemeriksaan barang bukti digital yang telah didapat dari proses eksaminasi, barang bukti digital diproses secara detail sesuai pelaporan tindak kejahatan untuk mengungkap kasus tindak kejahatan dengan metode yang benar secara ilmiah dan dapat dipertanggungjawabkan secara sah menurut hukum. *Reporting* adalah proses pembuatan laporan, hasil laporan analisis menggambarkan tindakan yang dilakukan oleh pelaku kriminal, penjelasan *tools* yang dipakai dan metode yang digunakan (Riskiyadi, 2020)



Gambar 2. 2 Kerangka Kerja NIST SP 800-86

Menurut panduan NIST, seperti terlihat pada gambar diatas, proses pengadaan bukti digital pada perangkat seluler ada 5 level akuisisi: *Manual Extraction*, *Logical Extraction*, *Hex Dumping/JTAG*, *Chip-Off* dan *Micro Read*. (Aji, Hariyadi, & Rochmadi, 2020) .

Panduan NIST merupakan hasil penelitian yang ekstensif dan menyeluruh, mencakup secara mendalam berbagai aspek, terus diperbarui dengan cara yang konsisten, dan menegaskan komitmen terhadap kualitas. Pendekatan ilmiah yang cermat dan konsisten ini menjadikan Panduan NIST sebagai sumber informasi dan panduan yang terpercaya, andalkan, dan berharga di bidangnya.

2.1.1 Penelitian Terdahulu

Dalam bidang forensika digital, akuisisi bukti digital merupakan langkah krusial untuk mengungkap kejahatan siber dan pelanggaran hukum lainnya. Berbagai metode akuisisi bukti digital telah dibahas dalam penelitian terdahulu. Penelitian (Nofiyan & Mushlihudin, 2020), meneliti metode akuisisi forensik komputer, dengan fokus pada akuisisi terhadap serangan menggunakan *web phishing* pada perangkat komputer. Penelitian ini menemukan bahwa metode tersebut efektif dalam mendapatkan dan menganalisis data digital serta menjaga integritasnya. Panduan yang digunakan pada penelitian ini menggunakan standar dari NIST secara general dan tidak spesifik menggunakan panduan *Special Publication*.

Di sisi lain, penelitian (Zakari Yahya, Juwoto Buru, & Sugiantoro, 2022) berfokus pada lingkup *network* yang lebih tertutup, yaitu analisis forensik yang dilakukan dalam lingkup jaringan *client-server*.

Semua penelitian yang dijelaskan tersebut membahas konsep analisis menggunakan teknik *live forensics*. Walaupun metode yang digunakan oleh penelitian itu terlihat berbeda, akan tetapi panduan dalam penyelesaian permasalahan dalam penelitian tersebut tidak menyebutkan secara spesifik standar yang digunakan.

Selain itu, penelitian oleh (Ramadhan & Mualfah, 2020) memberikan gambaran terhadap panduan dan langkah kerja yang berbeda dari penelitian yang lain. Metode yang digunakan pada penelitian ini memiliki panduan yang sedikit berbeda pada jumlah tahapan pada langkah kerja pada panduan NIST. Begitu hal nya juga pada penelitian (Akbar, Sunardi, & Riadi, 2019), metode yang digunakan juga memiliki tahapan yang lebih banyak dari standar acuan NIST. Walaupun demikian, simulasi yang digunakan pada kedua penelitian tersebut kurang sesuai dengan penerapan metode tersebut sehingga, hasil penelitian belum mendapatkan hasil sesuai dengan harapan.

Gambaran lebih ringkas terkait beberapa penelitian yang dijelaskan diatas terlihat pada tabel berikut.

Tabel 2. 1 Penelitian dengan perbedaan metode atau standar yang digunakan dalam akuisisi bukti digital beserta aspek kritisnya.

No	Peneliti	Tujuan	Standard / Metode	Hasil	Aspek Kritis
1	(Nofiyah A, Mushlihudin M., 2020)	Analisis forensik pada <i>web phishing</i> dari <i>fake login</i> dengan wireshark	NIST	Terdapat URL, DNS dan IP address pelaku phishing	Penelitian menggunakan standar NIST dengan metode Live Forensics.
2	(Ramadhan R, Muallifah D., 2018)	Pencarian bukti digital dari 3 OS yang beda (Linux, Windows dan MacOS) di SSD	NIJ (<i>National Institute of Justice</i>)	Hasil <i>recovery</i> : Windows 85.7%, Linux Ubuntu 0%, macOS 0%	Tahapan NIJ memiliki 5 tahapan panduan analisis terhadap bukti digital: <i>Identification, Collection, Examination, Analysis</i> dan <i>Reporting</i> .
3	(Riadi I, Mahfud I, Nasrulloh I, Dahlan A., 2019)	Analisis pada lingkungan <i>client-server</i> menggunakan <i>Live Forensics</i> .	NIST dan GRR	Ditemukan seluruh artefak dari data yang dicari.	GRR Rapid Response memiliki panduan teknis untuk melakukan akuisisi dan lebih tepat sebagai alat bantu forensik, bukan sebuah standar atau metode.

Tabel 2. 2 Lanjutan - Penelitian dengan perbedaan metode atau standar yang digunakan dalam akuisisi bukti digital beserta aspek kritisnya.

No	Peneliti	Tujuan	Standard / Metode	Hasil	Aspek Kritis
4	(Akbar M, Sunardi S, Riadi I., 2019)	Analisis bukti digital dengan panduan standar GCFIM	GCFIM	Seluruh proses dalam simulasi kasus berhasil dilakukan dalam 1 tahap.	Panduan GCFIM memungkinkan untuk mengulang setiap tahapan untuk mendapatkan hasil yang diharapkan
5	(Zakari Y A, Juwoto B D, Sugiantoro B., 2022)	Pencarian bukti digital yang di hapus di perangkat android	<i>Live Forensics</i>	Hasil analisis mendapatkan seluruh data yang diharapkan.	Metode yang digunakan tidak disebutkan, alat yang digunakan FTK (Forensics Tool Kit)

Dari penelitian-penelitian yang telah dilakukan tersebut dapat ditarik kesimpulan bahwa dalam pengujian suatu skenario, terdapat 2 faktor yang saling mempengaruhi hasil penelitian. Faktor tersebut adalah panduan dan metode yang digunakan. Penggunaan standar untuk metode yang tidak tepat dapat memberikan hasil yang tidak efisien atau hasil yang tidak efektif dan besar kemungkinan mendapatkan hasil yang tidak sesuai dengan yang diharapkan. Terlihat pada pengujian oleh (Akbar, Sunardi, & Riadi, 2019). Pengujian tersebut menggunakan panduan dari GCFIM yang memiliki prosedur repetisi sedangkan pada penelitian yang dilakukan dijelaskan bahwa prosedur pengulangan tidak diperlukan. Sehingga dapat dikatakan bahwa panduan yang digunakan tidak sepenuhnya dapat diterapkan. Demikian juga pada penelitian (Ramadhan & Mualfah, 2020) yang menggunakan metode akuisisi fisik, penggunaan panduan NIJ menjadi kurang efektif karena pada tahapan awal, proses *identification* dan *collection* dilakukan dalam satu rangkaian proses. Sedangkan

pada penelitian (Zakari Yahya, Juwoto Buru, & Sugiantoro, 2022), lebih efektif menggunakan panduan NIJ karena tidak memerlukan tahapan *acquisition*.

Penelitian terdahulu oleh (Riadi & Hadi, 2020) dan (Kaffah, Nur, Fitrianto, Syaripudin, & Darwan, 2022) menjelaskan metode akuisisi fisik dalam akuisisi bukti digital, termasuk forensik komputer pada media penyimpanan SSD yang memiliki fungsi *Trim*, dan pemulihan data. Penelitian tersebut menemukan bahwa fungsi *Trim* pada media penyimpanan SSD sangat berpengaruh terhadap hasil analisis terhadap bukti digital. Namun, penelitian tersebut masih memiliki keterbatasan dalam pemecahan solusi untuk fungsi *Trim* yang aktif dalam media penyimpanan SSD.

Penelitian lain oleh (Saad, Umar, & Fadlil, 2020) dan (Rochmadi, Wicaksono, & Nisa, 2020) menjelaskan metode akuisisi jaringan untuk melakukan analisis terhadap bukti digital pada media penyimpanan dalam jaringan yang tersimpan di dalam jaringan *cloud*. Penelitian tersebut menemukan bahwa pencarian bukti digital tidak mengalami banyak kendala dan cenderung mendapatkan hasil maksimal. Namun, penelitian tersebut masih memiliki keterbatasan dalam penggunaan skenario kasus yang lebih kompleks seperti penghilangan data dengan perintah hapus maupun perusakan data dengan infeksi *malware* pada server *cloud*.

Penggambaran ringkas penelitian-penelitian yang telah dijelaskan diatas dapat terlihat pada tabel dibawah ini.

Tabel 2. 3 Penelitian dengan perbedaan jenis penyimpanan yang digunakan dalam akuisisi bukti digital beserta aspek kritisnya.

No	Peneliti	Tujuan	Storage -types	Hasil	Aspek Kritis
1	(Riadi I, Hadi A., 2020)	Analisis bukti digital yang dihapus permanen di SSD	<i>Physical</i> (SSD)	Terdapat URL, DNS dan IP <i>address</i> pelaku <i>phishing</i>	Dengan <i>Trim Enable</i> pada SSD, bukti digital yang dihapus permanen tidak dapat ditemukan.

Tabel 2. 4 Lanjutan - Penelitian dengan perbedaan jenis penyimpanan yang digunakan dalam akuisisi bukti digital beserta aspek kritisnya.

No	Peneliti	Tujuan	Storage -types	Hasil	Aspek Kritis
2	(Saad S, Umar R, Fadlil A., 2018)	Analisis bukti digital pada aplikasi dropbox yang digunakan di <i>smartphone</i>	<i>Network Storage (Cloud storage)</i>	Data yang dihapus tidak bisa ditemukan. (Oxygen forensics)	Semua artefak yang terkait dengan aplikasi dropbox dapat ditemukan pada <i>smartphone</i>
3	(Kaffah F, Nur S, Fitrianto ASyaripudin U, Darwan D., 2022)	Mengetahui tahapan pemeriksaan dan analisis pada SSD yang memiliki fungsi TRIM	<i>Physical (SSD)</i>	Ditemukan seluruh artefak dengan akurasi 90%.	Fungsi <i>Trim</i> pada SSD sangat mempengaruhi hasil analisis bukti digital.
4	(Rochmadi T., 2019)	Analisis <i>cloud storage forensics</i> dari layanan Adrive	<i>Volatile Storage (RAM)</i>	bukti digital dapat dideteksi dan didapatkan bukti digital berupa file dokumen.	Panduan GCFIM memungkinkan untuk mengulang setiap tahapan untuk mendapatkan hasil yang diharapkan
5	(Rochmadi T, Wicaksono Y, Nisa N., 2020)	Identifikasi bukti digital pada perangkat android	<i>Network Storage (Cloud storage)</i>	Hasil identifikasi mendapatkan seluruh data yang diharapkan.	Untuk menguatkan identifikasi bukti digital, identifikasi pada RAM dapat dilakukan.

Perbandingan dari beberapa penelitian yang dilakukan dengan menggunakan metode yang berbeda memberikan kesimpulan bahwa pada akuisisi fisik terdapat perbedaan teknik untuk jenis media yang digunakan. Pada penelitian yang dilakukan oleh (Saad, Umar, & Fadlil, 2020) dan (Rochmadi, Wicaksono, & Nisa, 2020), didapatkan bahwa pada penelitian yang menggunakan metode akuisisi jaringan, proses akuisisi sangat konsisten dan tidak terdapat faktor yang mempengaruhi metode tersebut. Ditemukan juga bahwa panduan GCFIM sangat efektif digunakan untuk melakukan analisis menggunakan metode akuisisi jaringan.

Pada penelitian (Riadi & Hadi, 2020) dan (Kaffah, Nur, Fitrianto, Syaripudin, & Darwan, 2022), walaupun menggunakan media yang sama, tetapi terdapat perbedaan teknik dimana terdapat fungsi trim yang dapat diubah sesuai dengan kebutuhan. Hal ini menyebabkan teknik akuisisi pada metode akuisisi fisik menjadi berbeda.

Kesimpulan yang didapatkan dalam beberapa riset yang telah dilakukan memberikan gambaran sebagai berikut :

1. Metode akuisisi fisik yang berpedoman pada standar NIST menyediakan prosedur yang mudah dipahami dengan tahapan yang sangat sesuai dengan kebutuhan dalam penerapan metode ini.
2. Panduan NIJ menawarkan tahapan yang lebih detail dalam proses awal, di mana identifikasi dan pengumpulan informasi menjadi prosedur yang terpisah. Panduan ini sangat efektif untuk metode akuisisi jaringan, di mana kebutuhan identifikasi pada proses awal sangatlah rentan, sehingga proses ini membutuhkan penanganan yang lebih kompleks.
3. Prosedur pengulangan proses atau repetisi yang terdapat dalam panduan GCFIM lebih efektif digunakan pada metode akuisisi jaringan untuk analisis media penyimpanan *volatile*, seperti yang telah dilakukan pada penelitian di atas.

Dari kesimpulan tersebut, maka pada pengujian untuk akusisi NAS dimana metode yang digunakan adalah akusisi fisik, standar dari NIST memiliki panduan yang paling efektif untuk diterapkan.

2.2 Konsep Pengetahuan

2.2.1 Forensika Digital

Di era digital ini, kehidupan kita tak luput dari keterlibatan teknologi. Hampir semua aspek kehidupan terekam dalam jejak digital, mulai dari komunikasi, transaksi, hingga aktivitas di media sosial (Yeboah-Ofori, Yeboah-Boateng, & Gustav Yankson, 2019). Jejak digital ini

tak jarang menjadi kunci dalam mengungkap suatu kasus, baik kriminal maupun sipil. Dengan keadaan tersebut, peran forensika digital sangat diperlukan untuk memastikan bahwa kebutuhan akan jejak digital dapat digunakan sesuai dengan kebutuhan.

Forensika digital merupakan cabang ilmu forensika yang salah satu fokus tujuannya adalah pada penyelidikan dan penemuan bukti digital untuk membantu menyelesaikan kasus hukum. Karena pekerjaan dari forensika digital ini terkait dengan bukti digital berupa data, kebutuhan keilmuan ini juga diperlukan dalam lingkup *enterprise* atau korporasi, dimana kebutuhan akan pemulihan data akan sangat dibutuhkan (Fitriana et al., 2020).

2.2.2 Akuisisi

Akuisisi bukti digital merupakan langkah krusial dalam keseluruhan proses dalam investigasi forensika digital, proses ini merupakan sebuah fondasi kokoh dari seluruh proses analisis bukti digital. Akuisisi yang tepat dan cermat memastikan integritas dan keaslian bukti digital sehingga, tahapan ini dapat menjadi landasan yang sangat penting untuk analisis forensik selanjutnya (Syahib, Riadi, & Rusydi, 2020).

Tahapan akuisisi merupakan proses pengumpulan dan preservasi data digital yang potensial menjadi bukti dalam investigasi (Steel, 2006). Terdapat 3 (tiga) hal yang menjadi perhatian penting dalam tahapan ini yaitu integritas, keaslian dan keamanan.

Integritas merupakan suatu keadaan dimana bukti digital tidak diubah, dimodifikasi, atau dihapus selama proses akuisisi. Tanpa adanya integritas pada suatu bukti digital, tahapan investigasi selanjutnya akan sulit untuk dipertanggungjawabkan karena tingkat kepercayaan terhadap bukti digital tersebut sangat kecil. Hal ini disebabkan karena tidak ada jaminan apakah bukti digital tersebut telah melalui proses modifikasi atau tidak (Easttom, 2017).

Hal selanjutnya yang perlu diperhatikan yaitu keaslian, dimana bukti digital yang diperoleh merupakan salinan asli dari sumber aslinya (Ariffin & Ahmad, 2021). Dengan melakukan duplikasi dari sumber asli, menjadikan tahapan akuisisi lebih dapat dipertanggungjawabkan keasliannya, hingga pada tahapan selanjutnya, kualitas dari bukti digital yang akan di investigasi dapat dipertanggungjawabkan (Kent, Chevalier, Grance, & Dang, 2006). Kemudian hal lain yang perlu diperhatikan yaitu keamanan, dengan ketentuan dimana bukti digital aman dari kerusakan atau akses yang tidak sah selama proses akuisisi.

Tahapan akuisisi terbagi dalam 4 metode diantaranya akuisisi fisik, akuisisi logis, akuisisi *cloud* dan akuisisi jaringan. Dalam akuisisi fisik, teknik yang digunakan melibatkan pengambilan salinan langsung data dari perangkat elektronik, seperti komputer, *smartphone*,

hard drive, dan media penyimpanan lainnya, dengan cara yang aman dan menggunakan panduan maupun kerangka kerja forensik. Tujuan dari akuisisi fisik adalah untuk memastikan bahwa data yang diperoleh merupakan salinan asli dari perangkat penyimpanan dan tidak termodifikasi, sehingga dapat digunakan sebagai bukti yang sah dan dapat dipertanggung jawabkan dalam proses investigasi atau persidangan.

Berbeda dengan akuisisi fisik, teknik dalam akuisisi logis melibatkan pengambilan salinan sistem file perangkat elektronik, seperti komputer, *smartphone*, dan *tablet*, dengan panduan akuisisi dan kerangka kerja investigasi digital. Tujuan dari akuisisi logis adalah untuk mendapatkan gambaran menyeluruh tentang data dan metadata yang tersimpan pada perangkat, termasuk *file*, *folder*, dan informasi tentang data tersebut.

Di era digital ini, layanan *cloud computing* telah menjadi bagian tak terpisahkan dari kehidupan banyak orang. Layanan seperti Google Drive, Dropbox, dan iCloud memungkinkan pengguna untuk menyimpan, mengakses, dan berbagi data secara online dengan mudah. Namun, dengan semakin banyaknya data yang disimpan di *cloud*, muncul pula tantangan baru dalam proses investigasi forensik, yaitu akuisisi data dari layanan *cloud*.

Pada akuisisi *cloud*, teknik yang digunakan melibatkan pengambilan data secara langsung didalam jaringan yang terhubung dengan *cloud*. Tujuan dari akuisisi ini adalah mendapatkan seluruh artefak baik berupa data, *log* maupun cap waktu yang terdapat pada server *cloud*.

Aktivitas *online* dan komunikasi jaringan menjadi bagian tak terpisahkan dari kehidupan banyak orang. *Email*, pesan instan, *chat online*, dan *traffic web* adalah beberapa contoh data digital yang mengalir di jaringan. Dalam proses investigasi bukti digital, akuisisi jaringan menjadi penting untuk menangkap bukti digital yang tersimpan dalam jaringan dan komunikasi *online* (Yan Fikri Hendrawan & Hadinegoro, 2023). Teknik yang digunakan dalam akuisisi ini adalah dengan melakukan pengamatan langsung pada jaringan aktif secara langsung atau tangkapan lalu lintas jaringan (Hariyadi, Kusuma, & Sholeh, 2021). Tujuan akuisisi jaringan adalah mendapat artefak digital dari pengamatan lalu lintas pada jaringan secara langsung atau tangkapan lalu lintas jaringan.

2.2.3 NAS

NAS merupakan solusi penyimpanan data terpusat yang menawarkan akses mudah dan fleksibel bagi banyak pengguna (Loppies & Suwarjono, 2019). Kebutuhan akan penyimpanan terus meningkat seiring dengan perkembangan teknologi informasi yang sangat pesat. Penyimpanan merupakan aset yang sangat berharga baik untuk individu,

organisasi maupun industri. Hal ini berdampak terhadap kebutuhan akan pengelolaan dan perlindungan terhadap data maupun server NAS.

NAS merupakan perangkat penyimpanan data yang terhubung ke jaringan dan dapat diakses oleh beberapa pengguna secara bersamaan. Berbeda dengan *hard disk* eksternal yang hanya dapat diakses oleh satu perangkat, NAS memungkinkan pengguna untuk menyimpan, mengakses, dan membagikan data dari berbagai perangkat, seperti komputer, laptop, *smartphone*, dan *tablet* (Halim, 2019).

Semakin kompleksnya kebutuhan pengguna terhadap perkembangan teknologi penyimpanan, menyebabkan penggunaan NAS sangat banyak dibutuhkan. Salah satu penyebab penggunaan NAS ini menjadi alternatif penyimpanan yaitu kapasitas penyimpanan yang sangat besar. Dengan teknik penyimpanan menggunakan RAID, menyebabkan kapasitas NAS yang sangat leluasa untuk ditingkatkan yang dapat disesuaikan dengan kebutuhan. Selain itu performa dari NAS server meningkat seiring dengan perkembangan perangkat keras komputer (Muhammad & Asshiddiq, 2018).

Dengan terus meningkatnya perkembangan teknologi keamanan dalam teknik jaringan komputer, hal ini juga berdampak pada perkembangan NAS. Fitur keamanan data pada server NAS selalu di update oleh penyedia perangkat keras NAS maupun pengembang sistem operasi untuk server NAS. Selain konsep teknis yang terkait dengan data dan keamanan data, para penyedia perangkat keras NAS maupun pengembang sistem operasi NAS juga memperhatikan kemudahan pengguna dengan antarmuka yang mudah digunakan (Soffa, 2015). Hal ini tentu saja akan sangat memudahkan pengguna dalam pengelolaan data. Fitur-fitur canggih dan terkini juga ditawarkan oleh pengembang NAS seperti *cloud storage*, *artificial intelligence*, dan *machine learning* yang sangat membantu pengguna untuk kebutuhan harian baik untuk kebutuhan industri maupun kebutuhan personal.

2.2.4 NIST SP 800-86

NIST merupakan sebuah lembaga yang salah satu tujuannya adalah menawarkan panduan konsep maupun teknis terhadap suatu bidang ilmu terapan (Sama et al., 2021). Lembaga ini memiliki sejarah panjang yang terjalin dengan erat dengan perkembangan ilmu pengetahuan, teknologi, dan industri di Amerika Serikat. NIST telah memainkan peran penting dalam berbagai bidang, seperti metrologi, standardisasi, keamanan siber, dan forensika digital (Ramadhan, Rachmat Setiawan, & Hariyadi, 2022).

Standar, panduan, dan teknologi yang dikembangkan oleh NIST telah digunakan oleh berbagai pihak, termasuk pemerintah, industri, akademisi maupun masyarakat umum

(Koza, 2022). NIST bekerja sama dengan berbagai lembaga pemerintah federal, negara bagian, dan lokal untuk mengembangkan standar dan panduan yang mendukung kebijakan publik dan peraturan. Sedangkan pada lingkungan industri, penerapan standar dan panduan NIST banyak digunakan pada perusahaan di berbagai sektor, seperti teknologi informasi, manufaktur, konstruksi, dan kesehatan untuk memastikan kualitas dan keamanan produk dan layanan mereka (salsabila, 2024).

Dalam lingkungan akademisi, peneliti dan akademisi menggunakan hasil penelitian dan pengembangan NIST untuk memajukan ilmu pengetahuan dan teknologi (Sama et al., 2021). Walaupun NIST bukan satu-satunya lembaga yang menawarkan standar dan panduan, akan tetapi dalam lingkungan akademisi, NIST merupakan standar dan panduan yang cukup banyak digunakan dalam penelitian maupun referensi penelitian. Selain itu, NIST juga banyak digunakan oleh masyarakat umum, terutama untuk masyarakat di negara-negara berkembang dimana, standar dan panduan NIST bermanfaat untuk memastikan keamanan dan keandalan produk dan layanan yang mereka gunakan (Kurnadi Keamanan Siber et al., 2024).

Berbagai bidang yang menjadikan peran NIST memainkan peranan penting dalam perkembangan teknologi informasi, beberapa diantaranya yaitu:

1. Standarisasi: Mengembangkan standar nasional dan standar internasional untuk berbagai industri (Roy, 2020).
2. Penelitian dan Pengembangan: Melakukan penelitian dan pengembangan di berbagai bidang sains dan teknologi, seperti fisika, kimia, dan teknologi informasi (Indriyanto, Hariyadi, Habibi, Achmad, & Yogyakarta, 2020).
3. Keamanan Siber: Mengembangkan standar dan panduan untuk meningkatkan keamanan siber infrastruktur kritis nasional, seperti sistem keuangan, energi, dan transportasi (Umar, Riadi, & Handoyo, 2020).
4. Forensika Digital: Menyediakan perangkat lunak dan panduan untuk membantu penegak hukum dan investigator dalam investigasi kejahatan siber (Yan Fikri Hendrawan & Hadinegoro, 2023).

Untuk melakukan analisis terhadap bukti digital, NIST memiliki beberapa publikasi khusus yang dapat digunakan sebagai kerangka kerja yang komprehensif yang dapat digunakan sebagai prosedur analisis forensik. Salah satu diantaranya adalah NIST SP 800-86 yang dapat digunakan sebagai panduan kerja untuk melakukan analisis terhadap bukti digital pada perangkat komputer.

Publikasi NIST SP 800-86 menjabarkan tahapan-tahapan dasar dalam melakukan analisis bukti digital. Tahapan-tahapan tersebut dijelaskan dalam 4 tahapan utama di antaranya, yang pertama adalah *Collection*, tahapan ini merupakan panduan terperinci tentang cara mengumpulkan bukti digital secara yang mencakup penggunaan teknik yang tepat untuk memastikan integritas dan keaslian bukti digital, sehingga dapat menjadi dasar yang kuat dalam proses investigasi dan penyelesaian kasus.

Tahapan kedua yaitu *Examination*, dimana pada tahapan ini menekankan pentingnya preservasi bukti digital dengan cara yang aman dan terjamin untuk mencegah kerusakan, kehilangan, atau manipulasi data, termasuk penerapan prosedur penyimpanan yang tepat dan terdokumentasi dengan baik untuk menjaga keutuhan dan reliabilitas bukti digital.

Tahapan yang ke tiga adalah *Analysis*, NIST 800-86 memberikan panduan tentang cara melakukan analisis bukti digital secara mendalam dan sistematis untuk mengidentifikasi dan mengekstrak informasi yang relevan dengan insiden cyber. Panduan ini menekankan pentingnya penggunaan metodologi forensik yang diakui dan alat yang tepat untuk memaksimalkan hasil analisis.

Pada tahapan terakhir yaitu *Reporting*, merupakan panduan tentang cara mendokumentasikan hasil analisis bukti digital dalam laporan yang jelas, ringkas, dan akurat. Laporan ini harus dapat dipahami oleh berbagai pihak, termasuk penegak hukum, ahli forensik, untuk mendukung proses investigasi dan penyelesaian kasus.

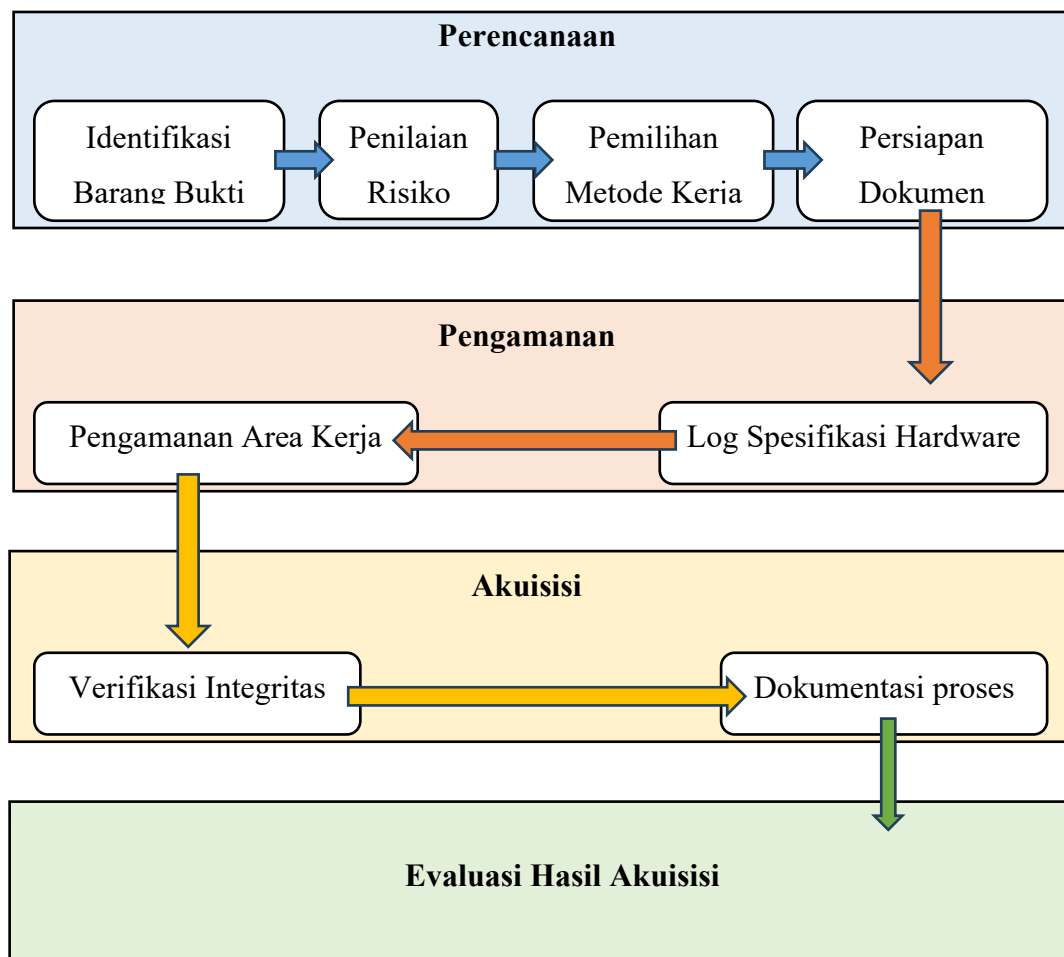
BAB 3

Metodologi

3.1 Langkah-langkah Penelitian

Dalam upaya memenuhi persyaratan forensik yang ketat, NIST SP 800-86 membagi proses akuisisi menjadi tiga tahap utama. Tahap pertama yaitu perencanaan, dimana pada tahapan ini melibatkan analisis awal terhadap kasus, identifikasi jenis data yang relevan, dan pemilihan alat serta teknik akuisisi yang tepat. Tahapan selanjutnya adalah tahapan pengamanan TKP yaitu tahapan pengamanan bukti digital yang dilakukan untuk mencegah kontaminasi atau kerusakan bukti, misalnya dengan menggunakan *write blocker* saat melakukan penyalinan data.

Tahap selanjutnya adalah tahapan akuisisi dimana pada tahapan akuisisi ini mencakup pembuatan salinan *bit-by-bit* dari media penyimpanan yang diduga mengandung bukti, serta verifikasi integritas data menggunakan *hash function*.



Gambar 3 1. Tahapan proses akuisisi

3.2 Skenario dan alat

Untuk melakukan simulasi sesuai dengan skenario kasus, digunakan 1 (satu) unit komputer yang akan berfungsi sebagai NAS Server dengan 1 (satu) unit SSD untuk penyimpanan sistem operasi. SSD ini memiliki kapasitas penyimpanan 128 GB. Sedangkan untuk sistem operasi NAS, digunakan TrueNAS Core dengan 3 (tiga) perangkat keras cakram masing-masing memiliki kapasitas 500 GB untuk penyimpanan. Selain itu, untuk proses akuisisi digunakan unit komputer yang menggunakan sistem operasi Windows 11 dengan alat bantu aplikasi OSForensics, ReclaiMe dan Acronis.

3.3 Akuisisi

Akuisisi bukti digital pada sistem penyimpanan NAS berlandaskan pada prinsip-prinsip forensika digital, yang bertujuan untuk mengamankan, melestarikan, dan menganalisis data digital sebagai bukti dalam investigasi hukum. Dalam konteks investigasi forensika digital, akuisisi bukti digital memegang peranan penting dalam proses pengumpulan dan pelestarian bukti digital yang sah dan dapat diterima di pengadilan (Yudhana, Riadi, & Anshori, 2018). Khususnya pada sistem penyimpanan NAS, akuisisi bukti digital melibatkan pengumpulan data dari sistem NAS dengan cara yang cermat dan terjamin, guna memastikan integritas dan keaslian data tersebut.

Integritas data mengacu pada keutuhan dan keautentikan data, di mana data tersebut tidak mengalami perubahan atau manipulasi sejak kejadian awal. Dalam proses akuisisi bukti digital pada NAS, integritas data harus dijaga dengan cermat untuk memastikan bahwa data yang dikumpulkan merupakan representasi akurat dari keadaan asli di sistem NAS.

Keaslian data mengacu pada asal-usul data, di mana data tersebut berasal dari sumber yang sah dan dapat diverifikasi (Kent et al., 2006). Dalam akuisisi bukti digital pada NAS, keaslian data harus dipastikan untuk membuktikan bahwa data tersebut benar-benar berasal dari sistem NAS yang bersangkutan dan bukan dari sumber lain.

Teori utama dalam akuisisi bukti digital meliputi *Chain of Custody* yang merupakan rantai penjagaan dalam mendokumentasikan pergerakan dan penanganan bukti digital untuk memastikan bahwa bukti tersebut tidak dirusak atau diubah (Kurii & Opirskyy, 2022). Selanjutnya adalah *Authenticity*, dimana keaslian bukti digital harus dipastikan untuk memastikan bahwa bukti tersebut berasal dari sumber yang asli dan belum diubah. Kemudian, *Integrity* yang harus memastikan bahwa bukti tersebut tidak dirusak atau diubah dalam proses pengumpulan dan analisis.

Dalam penelitian ini, metode akuisisi bukti digital yang digunakan untuk mengumpulkan data dari sistem NAS yaitu akuisisi fisik. Metode ini menerapkan dimana akuisisi melibatkan pembuatan salinan *bit-by-bit* dari seluruh *hard drive* dalam penyimpanan NAS. Penelitian ini menggunakan kerangka kerja akuisisi bukti digital yang terstruktur dan komprehensif, dengan berlandaskan pada panduan metodologi yang diakui secara global. Kerangka kerja ini mengadopsi prinsip-prinsip dan panduan akuisisi bukti digital yang ditetapkan oleh panduan NIST dalam kerangka kerja *Computer Forensics Special Publication* (CFSP).

Lebih lanjut, kerangka kerja ini diperkuat dengan panduan penggunaan alat bantu perangkat lunak forensik yang tercantum dalam dokumen NIST *Cloud Forensics Tools Testing* (CFTT). CFTT menyediakan evaluasi dan validasi terperinci terhadap berbagai alat bantu perangkat lunak forensik, memastikan keandalan dan efektivitasnya dalam proses akuisisi bukti digital.

Kerangka kerja akuisisi bukti digital dalam penelitian ini menggabungkan metodologi NIST CFSP yang diakui secara global dengan panduan NIST CFTT untuk alat bantu perangkat lunak forensik terverifikasi. Hal ini menghasilkan pendekatan akuisisi bukti digital yang kokoh, profesional, dan terpercaya, yang sejalan dengan standar forensik digital terkini.

Berdasarkan pada standar NIST SP 800-86, dalam melakukan akuisisi terdapat beberapa tahapan yang perlu dilakukan, diantaranya perencanaan, pengamanan TKP dan akuisisi.

3.3.1 Perencanaan

Tahap awal ini sangat penting untuk memastikan kelancaran dan efektivitas proses akuisisi. Rencana akuisisi yang matang harus dibuat, mencakup identifikasi barang bukti digital, penilaian risiko, pemilihan metode kerja untuk akuisisi yang tepat dan dokumentasi yang jelas tentang langkah-langkah yang diambil. Pada pengujian ini juga perlu mempertimbangkan faktor-faktor seperti keamanan data, privasi, dan potensi kontaminasi bukti selama proses akuisisi.

Pada tahapan identifikasi barang bukti digital, semua komponen harus dilakukan proses identifikasi untuk mengetahui jenis barang bukti, kapasitas, kode unik perangkat (dapat berupa *serial number*, *manufaktur assembly* atau jenis yang lainnya) dan fungsi komponen tersebut.

Tahapan kedua yaitu penilaian risiko dimana pada tahapan ini, akuisisi harus dilakukan secara sistematis dan terstruktur, dengan menggunakan beberapa alat bantu yang diperlukan. Berikut adalah beberapa analisis utama yang dilakukan dalam pengujian ini dengan penilaian risiko akuisisi.

1. Identifikasi dan analisis risiko yang mungkin terjadi

Beberapa resiko yang mungkin terjadi pada pengujian ini diantaranya, adanya file yang tidak utuh atau *corrupt* dalam penyimpanan, adanya file *malware* yang berada di dalam penyimpanan dan terdapat *bad sector* pada *disk drive*,

2. Pengelolaan dan peninjauan risiko

Beberapa kegiatan yang perlu dilakukan untuk pengelolaan risiko tersebut dengan memastikan seluruh file yang digunakan dalam pengujian ini tidak terdapat *malware* dan tidak terdapat file *corrupt*. Selain itu, *disk* yang digunakan juga telah di periksa terlebih dahulu kondisi *health level* perangkat menggunakan aplikasi untuk *drive management*.

Melakukan penilaian risiko akuisisi yang menyeluruh dapat membantu proses dalam tahap pengujian untuk membuat keputusan yang *informed* tentang apakah proses akuisisi dapat dilakukan atau tidak. Penilaian risiko juga dapat membantu dalam pengujian untuk mengembangkan rencana mitigasi risiko yang efektif untuk melindungi aset dan kepentingan pada kasus yang sebenarnya.

Tahapan selajutnya adalah pemilihan metode yang diperlukan dalam pengujian barang bukti digital. Pemilihan metode ini merupakan aspek krusial yang menentukan efektivitas dan kredibilitas proses akuisisi bukti digital. Metode yang dipilih haruslah sesuai dengan jenis bukti digital yang akan diakuisisi, perangkat penyimpanan yang digunakan, dan kondisi lingkungan pengujian. Dalam pengujian ini, metode yang digunakan berfokus pada penerapan aplikasi-aplikasi khusus yang dirancang untuk memfasilitasi proses akuisisi bukti digital.

Menyusul penyelesaian seluruh persiapan awal, tahapan krusial berikutnya adalah mempersiapkan dokumen pendukung dalam proses akuisisi bukti digital. Dokumen ini memegang peranan penting dalam mendukung kelancaran dan kredibilitas pengujian laboratorium forensik.

Untuk memfasilitasi proses tersebut, disusunlah sebuah dokumen kontrol yang memuat panduan terperinci mengenai prosedur akuisisi bukti digital. Dokumen ini menguraikan secara sistematis tahapan-tahapan yang harus dilalui, alat yang digunakan, serta dokumentasi yang diperlukan untuk memastikan akuisisi bukti digital yang sah dan terdokumentasi dengan baik.

Keberadaan dokumen kontrol ini menjadi landasan fundamental bagi terselenggaranya pengujian laboratorium forensik yang kredibel dan akuntabel. Dengan mengacu pada panduan yang tercantum dalam dokumen ini, para ahli forensik dapat menjalankan proses akuisisi bukti digital secara konsisten dan terukur, sehingga menghasilkan temuan yang akurat dan dapat dipertanggungjawabkan.

3.3.2 Pengamanan TKP

Guna memastikan kelancaran dan kredibilitas pengujian, diperlukan penerapan parameter keamanan yang komprehensif di lokasi pengujian. Parameter ini bertujuan untuk meminimalisir gangguan, baik secara teknis maupun non-teknis, yang berpotensi mempengaruhi validitas hasil pengujian.

Aspek teknis yang perlu dipertimbangkan meliputi ketersediaan sumber daya listrik yang stabil dan terukur, serta pengaturan suhu ruangan yang optimal. Hal ini penting untuk menjaga stabilitas kinerja peralatan pengujian dan mencegah terjadinya kerusakan atau malfungsi akibat faktor eksternal. Selain itu, penting untuk mengantisipasi gangguan non-teknis seperti kebisingan, getaran, atau akses yang tidak sah ke lokasi pengujian. Penerapan protokol keamanan yang ketat dan pengawasan yang memadai dapat membantu meminimalisir risiko gangguan tersebut dan memastikan proses pengujian berlangsung secara steril dan terkendali.

Untuk menunjang keamanan dan memastikan sterilitas lingkungan pengujian, lokasi pengujian dipilih di dalam ruang tertutup yang dilengkapi dengan pendingin ruangan. Hal ini bertujuan untuk menjaga suhu ruangan pada tingkat yang optimal dan meminimalisir pengaruh faktor eksternal yang dapat mengganggu jalannya proses pengujian. Selain itu, pintu akses masuk ke ruang pengujian selalu dalam keadaan tertutup dan terkunci. Hal ini bertujuan untuk membatasi akses keluar-masuk dan mencegah gangguan dari pihak yang tidak berkepentingan. Petunjuk yang dipasang di pintu akses masuk juga berfungsi untuk memberikan informasi kepada pihak-pihak yang terkait mengenai peraturan dan protokol keamanan yang berlaku di lokasi pengujian.

1. Log spesifikasi Hardware

Salah satu tahapan penting dalam proses ini adalah tahap *log* spesifikasi *hardware*, yang bertujuan untuk mendokumentasikan secara lengkap konfigurasi perangkat keras yang digunakan dalam proses akuisisi.

2. Pengamanan area

Proses akuisisi perangkat digital seringkali melibatkan risiko kontaminasi dan kerusakan pada perangkat yang dapat mengakibatkan hilangnya bukti digital penting. Oleh karena itu, langkah-langkah mitigasi awal perlu dilakukan untuk meminimalkan risiko tersebut. Hal ini bertujuan untuk menjaga integritas dan keaslian bukti digital yang akan digunakan dalam proses investigasi atau penegakan hukum.

3.3.3 Akuisisi

Berdasarkan panduan NIST SP 800-86, terdapat beberapa metode dasar dalam proses *imaging*, yaitu akuisisi *bit-per-bit*, akuisisi file, dan akuisisi *logical*. Dalam pengujian ini, metode akuisisi *bit-per-bit* dipilih untuk *imaging* NAS. Hal ini dikarenakan karakteristik penyimpanan NAS yang umumnya memiliki lebih dari satu *disk* penyimpanan.

Metode akuisisi *bit-per-bit* membaca data dari media penyimpanan secara langsung, *bit-per-bit*. Metode ini memberikan salinan data yang paling forensik dan akurat, namun membutuhkan waktu yang lebih lama dibandingkan dengan metode akuisisi lainnya. Hal ini dikarenakan metode akuisisi *bit-per-bit* membaca semua data pada media penyimpanan, termasuk data yang tidak relevan dengan investigasi.

Pada pengujian ini juga perlu melakukan verifikasi integritas *image* yang dihasilkan dari proses *imaging*. Salah satu metode verifikasi yang umum digunakan adalah dengan mendapatkan nilai *hash* dari *image*. Nilai *hash* ini kemudian dapat dibandingkan dengan nilai *hash* yang dihitung dari *image* asli untuk memastikan bahwa *image* tidak mengalami perubahan atau kerusakan selama proses *imaging*.

1. Verifikasi integritas (*Hashing*)

Sebagai bentuk verifikasi integritas hasil proses *imaging*, perlu dilakukan pengambilan nilai *hash* dari hasil akuisisi. Nilai *hash* ini berfungsi untuk memastikan keaslian dan keutuhan bukti digital yang telah diakuisisi.

2. Dokumentasi proses

Setiap tahapan dalam proses akuisisi, mulai dari instalasi perangkat, *disk imaging*, hingga pencatatan hasil akuisisi, wajib didokumentasikan secara rinci dalam dokumen kontrol.

Hal ini bertujuan untuk memastikan bahwa seluruh proses akuisisi terekam dengan lengkap dan akurat, serta untuk memudahkan proses monitoring dan evaluasi di kemudian hari.

Dokumen kontrol tersebut memuat catatan detail setiap kegiatan pengujian yang dilakukan, beserta dengan waktu pelaksanaannya. Catatan ini meliputi informasi mengenai jenis pengujian yang dilakukan, parameter yang diukur, metode pengujian yang digunakan, dan hasil yang diperoleh. Dengan demikian, dokumen kontrol menjadi sumber informasi yang berharga untuk melacak kembali proses akuisisi dan memastikan bahwa semua tahapan telah dilaksanakan dengan benar.

BAB 4

Hasil dan Pembahasan

Berlandaskan pada skenario kasus yang telah dibuat, disusunlah sebuah simulasi yang mereplikasi kejadian yang sebenarnya dengan beberapa pengembangan. Pengembangan ini dilakukan untuk mengantisipasi kebutuhan pada kasus serupa yang mungkin terjadi di masa depan. Hal ini bertujuan untuk memastikan kesiapan dalam menangani situasi yang tidak terduga dan meningkatkan efektivitas penanganan dalam berbagai kemungkinan skenario.

Simulasi tersebut dirancang dengan cermat, mempertimbangkan berbagai aspek yang terkait dengan kasus yang telah terjadi. Pengembangan yang dilakukan meliputi penambahan variabel, penyempurnaan alur cerita, dan penyesuaian parameter simulasi. Dengan demikian, simulasi ini diharapkan dapat memberikan gambaran yang lebih realistis dan akurat tentang situasi yang mungkin terjadi, sehingga memungkinkan pelatihan dan persiapan yang lebih optimal.

Kemudian dilakukan tahapan akuisisi dengan tahapan penelitian sebagai berikut :

4.1 Perencanaan

Pada tahap perencanaan, dilakukan beberapa sub tahapan mulai dari identifikasi terhadap barang bukti, penilaian risiko, pemilihan metode kerja hingga persiapan dokumen.

4.1.1 Identifikasi Barang Bukti Digital

Dalam pengujian ini barang bukti yang diidentifikasi adalah *disk drive* yang digunakan pada sistem penyimpanan NAS. Dengan spesifikasi sebagai berikut :

Tabel 4. 1 Identifikasi barang bukti

No	Jenis	Kapasitas	<i>Serial Number</i>	Keterangan
1	SSD	128 GB	170876403046	Penyimpanan Sistem Operasi TrueNAS Core
2	HDD	500 GB	W2A6THJM	<i>Disk 1</i> penyimpanan
3	HDD	500 GB	6VMC393C	<i>Disk 2</i> penyimpanan
4	HDD	500 GB	5VM1J9K	<i>Disk 3</i> penyimpanan

Pada pengujian ini menggunakan 1 (satu) SSD yang digunakan sebagai media untuk menyimpan sistem operasi TrueNAS core dan 3 (tiga) *disk drive* yang digunakan sebagai

media penyimpanan. Semua *disk drive* yang digunakan untuk penyimpanan akan dibuat dalam sebuah cluster sehingga menjadi logical satu *disk drive*.

4.1.2 Penilaian risiko

Untuk memastikan perangkat yang akan diakuisisi tidak terdapat permasalahan pada perangkat fisik, dilakukan pengujian menggunakan HDD Regenerator untuk memastikan tidak terdapat *bad sector* dari perangkat yang akan di akuisisi.

4.1.3 Pemilihan metode kerja

Dua aplikasi yang dipilih dalam pengujian ini adalah OSForensics dan ReclaiMe. OSForensics merupakan aplikasi *open-source* yang populer digunakan untuk akuisisi bukti digital dari berbagai perangkat penyimpanan, termasuk *hard drive*, *flash drive*, dan kartu memori. Aplikasi ini menawarkan berbagai fitur yang lengkap, seperti pembuatan *image* forensik, analisis metadata, dan ekstraksi file.

OSForensics dipilih berdasarkan rekomendasi standar NIST CFTT. Aplikasi ini memiliki kemampuan untuk melakukan akuisisi terhadap bukti digital dan telah melalui proses pengujian menggunakan standar NIST. Katalog aplikasi ini dapat ditemukan pada laman resmi NIST khususnya pada bagian CFTT. OSForensics merupakan aplikasi khusus untuk analisis forensik yang dibuat oleh pengembang aplikasi perangkat lunak Passmark *Software*. Pemilihan aplikasi ini berdasarkan kemampuan OSForensik yang memiliki banyak fitur yang cukup lengkap untuk melakukan analisis bukti digital.



Gambar 4. 1 OSForensics

ReclaiMe, di sisi lain, merupakan aplikasi komersial yang terkenal dengan kemampuannya dalam memulihkan data yang terhapus atau rusak dari perangkat penyimpanan. Aplikasi ini dapat membantu investigator forensik untuk menemukan bukti digital yang mungkin telah dihapus atau disembunyikan oleh pelaku kejahatan. Penggunaan kombinasi kedua aplikasi ini diharapkan dapat menghasilkan akuisisi bukti digital yang

komprehensif dan akurat, sehingga mendukung proses investigasi forensik yang lebih efektif.

Aplikasi kedua ini adalah aplikasi yang banyak digunakan di lingkungan *enterprise*. Aplikasi ini memiliki layanan dukungan teknis dan dukungan komunitas sehingga penggunaannya sesuai dengan kebutuhan *enterprise*. Pada penelitian ini digunakan ReclaiMe *data recovery* dari perusahaan pengembang perangkat lunak ReclaiMe.



Gambar 4. 2 ReclaiMe

Semua alat bantu tersebut akan digunakan pada pengujian untuk melakukan akuisisi dengan panduan dari standar NIST. Selain kedua aplikasi tersebut, juga digunakan beberapa aplikasi pendukung lain seperti *usbwriteblocker* dan *windows commandprompt* serta aplikasi lain untuk kebutuhan dokumentasi laporan.

Proses instalasi dan konfigurasi TrueNAS Core untuk pengujian ini terlampir pada Lampiran A pada laporan ini.

4.1.4 Persiapan dokumen

Sebagai upaya untuk menstandarisasi prosedur pengujian, telah dibuat dokumen kontrol yang berisi langkah-langkah kerja yang terperinci. Dokumen ini bertujuan untuk memastikan bahwa setiap tahapan pengujian dilakukan sesuai dengan panduan yang telah dijelaskan.

Dokumen terlampir pada Lampiran D.

4.2 Pengamanan TKP

Untuk memastikan tidak terdapat gangguan dalam melakukan proses akuisisi, dilakukan beberapa tindakan pencegahan diantaranya, penggunaan *Uninterruptible Power Supply* (UPS) untuk memastikan sumber daya listrik tetap terjaga dan membuat tanda area terbatas pada akses masuk ke ruang akuisisi.

4.2.1 Log spesifikasi Hardware

Beberapa informasi yang mencakup dalam pengujian ini diantaranya terlihat seperti tabel berikut.

Tabel 4. 2 Log spesifikasi NAS pada pengujian

No	Item	Detail	Keterangan
1	NAS OS	TrueNAS core	Ver. TrueNAS-13.0-U6.1
2	NAS IP	192.168.4.98	Gateway 192.168.4.1
3	Username	root	
4	Password	tppyMsVptr	
5	Disk 1	NAS OS	
6	Disk 2	Storage Disk cluster 1	<i>raidz configuration</i>
7	Disk 3	Storage Disk cluster 2	<i>raidz configuration</i>
8	Disk 4	Storage Disk cluster 3	<i>raidz configuration</i>
9	pool	Pool 1	
10	Total storage	972 GB in total	

Sebagai pelengkap dokumentasi pekerjaan, seluruh perangkat yang akan diakuisisi wajib didokumentasikan dengan cara pengambilan gambar dan dimasukkan ke dalam laporan. Proses pengambilan gambar perangkat pada pengujian ini dilakukan seperti yang ditunjukkan pada gambar berikut.



Gambar 4. 3 Disk Penyimpanan 1

Disk drive pertama ini memiliki kapasitas 500 GB, kecepatan 7200 rpm dengan kode firmware CC45.



Gambar 4. 4 Disk penyimpanan 2

Disk drive kedua memiliki kapasitas 500 GB, kecepatan 7200 rpm dengan kode firmware CC45.



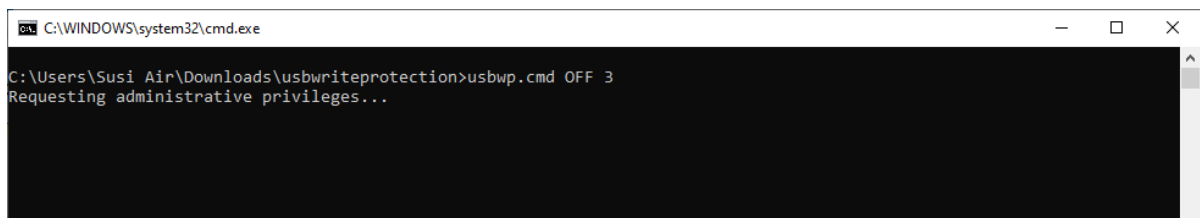
Gambar 4. 5 Disk penyimpanan 3

Disk drive ketiga memiliki kapasitas 500 GB, kecepatan 7200 rpm dengan kode firmware CC45.

4.2.2 Pengamanan Area Kerja

Untuk membatasi akses baca-tulis pada perangkat yang akan diakuisisi, dilakukan dengan menginstalasi aplikasi tambahan seperti USB *Write Blocker* sebelum perangkat dipasang pada komputer untuk proses imaging. USB *Write Blocker* berfungsi untuk mencegah modifikasi data pada perangkat, sehingga dapat membantu menjaga keaslian dan integritas bukti digital.

Aplikasi USB *Write Blocker* yang digunakan pada penelitian ini adalah *usbwriteprotection*, seperti terlihat pada gambar berikut.



Gambar 4. 6 *usbwireprotector* inisiasi proses

Setelah menjalankan *usbwriteprotection*, pengguna akan diarahkan ke jendela baru untuk memulai proses aktivasi *write protection* pada perangkat USB. Jendela tersebut akan menampilkan instruksi yang jelas dan mudah dipahami untuk memandu pengguna dalam menyelesaikan proses aktivasi. Setelah proses aktivasi *write protection* berhasil diselesaikan, jendela baru tersebut akan tertutup secara otomatis. Terlihat seperti gambar berikut.



Gambar 4. 7 *usbwriteprotection* inisiasi ON

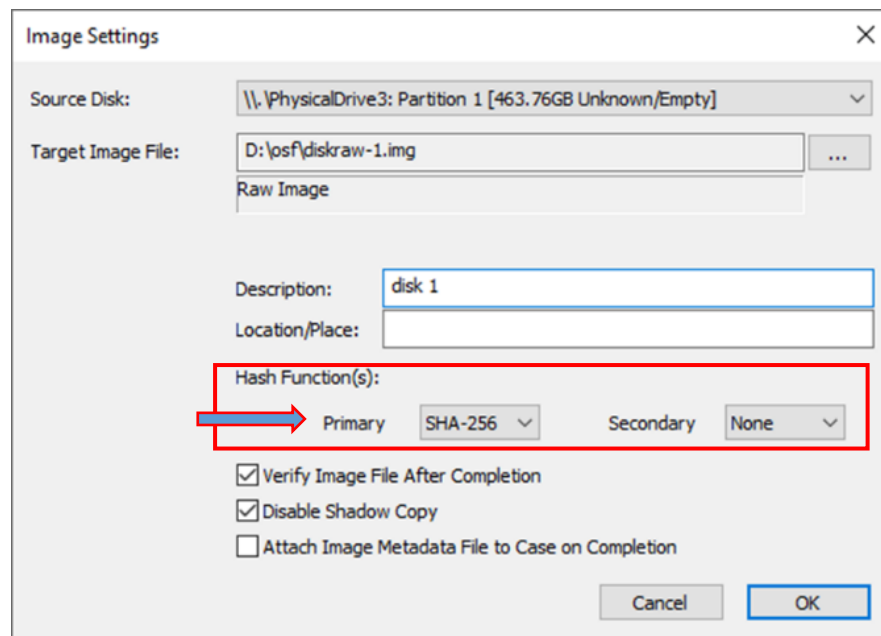
4.3 Akuisisi

Dalam tahapan akuisisi, sebelum proses *imaging disk* dilakukan, diperlukan langkah pengujian untuk melakukan verifikasi terhadap integritas bukti digital. Pengujian ini dilakukan menggunakan aplikasi OSForensics dan Command Prompt.

4.3.1 Verifikasi Integritas

Pada pengujian pertama, digunakan aplikasi OSForensics. Aplikasi ini memiliki fitur yang sangat lengkap untuk menganalisis bukti digital dari proses input data kasus sampai dengan laporan hasil analisis forensik. Tahapan pengujian menggunakan OSForensics terlampir dalam Lampiran B pada laporan ini.

Pengambilan nilai hash dilakukan langsung pada aplikasi pada saat awal proses akuisisi, sehingga tidak diperlukan aplikasi tambahan untuk mendapatkan nilai hash. Terlihat seperti pada gambar berikut.



Gambar 4. 8 penentuan *hash* yang digunakan pada hasil *imaging*

Sedangkan untuk pengujian kedua menggunakan aplikasi ReclaiMe, nilai hash didapatkan menggunakan langkah tambahan yaitu menggunakan aplikasi *command prompt* dan dilakukan secara manual.

Tahapan akuisisi menggunakan ReclaiMe dijelaskan lebih lanjut dalam tahapan proses yang terlampir pada Lampiran C pada laporan ini.

4.3.2 Dokumentasi Proses

Seluruh proses yang dilakukan di dokumentasikan dalam laporan kegiatan seperti terlampir pada Lampiran D pada laporan ini.

4.4 Evaluasi hasil akuisisi

Setelah melakukan seluruh tahapan akuisisi pada pengujian ini, didapatkan beberapa informasi yang ditampilkan dalam beberapa tabel berikut ini.

Tabel 4. 3 Pengujian *imaging* NAS *disk drive*

No	Tools	Imaging	Image ext.	Keterangan
1	OSForensics	Ya	.img	Terdapat file <i>log</i> tentang seluruh informasi detail dari perangkat, <i>hash</i> dan catatan waktu kegiatan <i>imaging</i> Proses <i>imaging</i> dilakukan 1 (satu) kali tahapan untuk seluruh <i>disk drive</i>
2	ReclaiMe	Ya	.img	Hanya mendapatkan file hasil <i>imaging</i> , memerlukan teknik dan aplikasi tambahan untuk mendapatkan <i>hash</i> dan detail informasi lain seperti catatan waktu dan spesifikasi perangkat Proses <i>imaging</i> dilakukan berulang untuk tiap <i>disk drive</i>

Dari pengujian menggunakan OSForensics, pada proses akuisisi didapatkan hasil berupa file dengan ekstensi *img*. Seluruh *disk* yang di akuisisi dilakukan dalam 1 (satu) tahapan kerja dengan durasi waktu 5 (lima) jam untuk tiap *disk* yang diakuisisi. Durasi waktu yang dibutuhkan untuk semua disk adalah 15 (lima belas) jam.

Selain itu, pada saat proses *imaging* selesai dilakukan, pada direktori tempat *disk image* disimpan, terdapat tambahan sebuah file *log* berisi semua informasi detail dari tiap *disk* yang diakuisisi tentang informasi detail perangkat yang di akuisisi beserta *checksum* atau *hash*. Terlihat seperti gambar.

```

disk1.img.info.txt - Notepad
File Edit Format View Help
Image source: \\.\PhysicalDrive3: Partition 1 [463.76GB Unknown/Empty]
Image file name: disk1.img
Image file size: 497960292352
Image created on 08 June 2024, 08:35:41

Copy method: Direct Sector Copy
Checksum method: SHA-256
Checksum source( \\.\PhysicalDrive3: Partition 1 [463.76GB Unknown/Empty] ):
0df899b6299c976c354393ce5ab442e334d45468233f5d7d011997cc1640c9cb
Checksum image ( disk1.img ):
0df899b6299c976c354393ce5ab442e334d45468233f5d7d011997cc1640c9cb

Case: N/A
Examiner Name: N/A
Description:
Location/Place:

Ln 1, Col 1    100%    Windows (CRLF)    UTF-8 with BOM

```

Gambar 4. 9 File log dari akuisisi pada OSForensics

Berbeda halnya dengan pengujian dengan ReclaiMe, proses *imaging* dilakukan berulang untuk setiap *disk* yang di akuisisi, dengan durasi waktu 8 (delapan) jam untuk setiap *disk drive*. Selain itu untuk *hash* didapatkan secara manual menggunakan *power shell* atau *command prompt* pada windows.

Tabel 4. 4 Pengambilan nilai *hash* pada *image*

No	Tools	Hash	Waktu Akuisisi	Remarks
1	OSForensics	Tersedia pada aplikasi	15 jam total untuk seluruh <i>disk drive</i>	Dari tiap HDD yang dilakukan <i>imaging</i> kemudian dilakukan <i>rebuilding</i> RAID untuk menyatukan Kembali seluruh <i>image</i> menjadi 1 kesatuan penyimpanan
2	ReclaiMe	Diperlukan aplikasi lain	8 jam / <i>disk drive</i>	<i>Hash</i> didapatkan menggunakan <i>command prompt</i> di windows

Setelah proses *imaging* untuk setiap *disk drive* penyimpanan selesai, dilakukan proses *rebuilding* RAID untuk merekonstruksi dan menyatukan kembali seluruh *image* menjadi satu kesatuan penyimpanan, sebagaimana bentuk fisik RAID aslinya. Proses rebuilding RAID ini penting untuk dilakukan agar data yang telah menjadi *image* dapat diakses dan digunakan kembali. *Rebuilding* RAID dilakukan dengan menggunakan perangkat lunak RAID *controller* yang sesuai dengan jenis RAID yang digunakan. Perangkat lunak ini akan

membaca data dari seluruh *image* dan menyusunnya kembali sesuai dengan struktur RAID aslinya.

Rebuilding RAID pada pengujian ini menggunakan OSForensics dan mendapatkan file image sebesar 795GB dengan ekstensi img. Kemudian file *image* tersebut dilakukan proses eksaminasi singkat untuk memastikan apakah proses eksaminasi dapat dilakukan.

Dari pengujian menggunakan OSForensics, didapatkan bahwa pada proses eksaminasi tidak ditemukan artefak pada *image*, dengan proses *scanning* selama 3 (tiga) jam. Sedangkan pada pengujian menggunakan ReclaiMe ditemukan banyak artefak dan seluruh file yang di upload pada awal pengujian ditemukan dengan persentase temuan 100%. Waktu yang diperlukan untuk proses *scanning image* selama 8 jam.

Tabel 4. 5 Eksaminasi singkat dari image yang didapat

No	<i>Tools</i>	<i>Examination</i>	Artefak	Keterangan
1	OSForensics	Tidak ditemukan artefak	0%	<i>Rebuilding</i> RAID membutuhkan waktu 8 jam
2	ReclaiMe	Ditemukan artefak	100%	<i>Recovery image</i> membutuhkan waktu 1 hari dan 8 jam

BAB 5

Kesimpulan dan Saran

5.1 Kesimpulan

Dari keseluruhan proses pengujian yang telah dilakukan, didapatkan hasil bahwa seluruh aplikasi yang telah dipilih dapat melakukan proses *imaging* dengan hasil sempurna. Kemudian dari seluruh tahapan yang telah dilakukan, dilakukan analisis menggunakan panduan tahapan dari NIST SP 800-86. Analisis ini diperlukan untuk memastikan hasil *imaging* yang didapatkan sesuai dengan tahapan proses akuisisi. Proses validasi panduan NIST pada pengujian ini untuk memastikan apakah proses akuisisi yang dilakukan sesuai dengan *chain of custody* dari panduan NIST terutama SP 800-86 terkait penanganan bukti digital.

Berdasarkan hasil pengujian, didapatkan kesimpulan bahwa dalam sistem penyimpanan NAS memiliki karakteristik konsep penyimpanan yang berbeda dengan sistem penyimpanan konvensional. Hal ini terlihat dari pola penyimpanan pada NAS. Meskipun sekilas terlihat mirip dengan RAID, NAS, khususnya TrueNAS Core, menggunakan penamaan dan pendekatan yang unik untuk memastikan integritas dan ketersediaan data. Salah satu contoh perbedaan tersebut adalah penggunaan istilah ZFS pada TrueNAS Core. Selain itu, TrueNAS Core juga menyediakan berbagai pilihan konfigurasi penyimpanan, seperti *stripping*, RAID-Z, dan *mirror*, yang memungkinkan pengguna untuk menyesuaikan tingkat redundansi dan performa sesuai kebutuhan mereka.

Selain itu, pada pengujian ditemukan perbedaan mendasar pada proses akuisisi bukti digital terhadap *disk drive* yang di uji. Proses akuisisi data membutuhkan prosedur *imaging* dua langkah untuk memastikan integritas dan kelengkapan data yang diperoleh. Langkah pertama melibatkan *imaging* pada masing-masing *drive* individual dalam sistem NAS. Selanjutnya, proses *imaging* kedua dilakukan, dengan menggunakan *image drive* individual yang diperoleh sebelumnya, untuk menghasilkan satu *image* terkonsolidasi dari keseluruhan sistem penyimpanan NAS. Prosedur *imaging* dua langkah memastikan bahwa representasi granular dan holistik dari sistem penyimpanan NAS diperoleh, memberikan dasar yang kuat untuk analisis forensik selanjutnya.

Penerapan pedoman NIST SP 800-86 menciptakan struktur dan metodologi yang terdefinisi dengan baik untuk proses investigasi penanganan bukti digital, sehingga menjamin pendekatan yang sistematis dan dapat direplikasi. Sesuai dengan pedoman NIST

SP 800-86, kerangka kerja dan metodologi terstruktur diterapkan untuk memandu investigasi penanganan bukti digital, yang mendukung pendekatan terstandarisasi dan ilmiah yang kuat. Meskipun demikian, penggunaan alat bantu forensik, seperti aplikasi analisis, memiliki pengaruh signifikan terhadap hasil pemeriksaan. Hal ini terbukti dalam pengujian ini, di mana eksaminasi menggunakan OSForensics tidak menghasilkan temuan yang diharapkan, berbeda dengan eksaminasi menggunakan aplikasi ReclaiMe yang berhasil menemukan seluruh artefak dengan tingkat temuan artefak 100%.

5.2 Saran

Beberapa saran yang dapat digunakan pada hal pengujian lebih lanjut dalam penelitian ini diantaranya, melakukan pengujian pada lingkungan yang berbeda, penggunaan media yang berbeda dan melakukan pengujian dengan subjek lain yang lebih luas. Berikut beberapa pandangan terkait perluasan pengujian ini.

1. Pengujian dalam lingkungan yang lebih kompleks

Melakukan pengujian dengan lingkungan yang lebih kompleks dapat memberikan pandangan yang berbeda dan lebih realistik. Seperti pengujian yang menggunakan lingkungan network yang lebih kompleks dengan menggunakan *backup system* dan *active directory*.

2. Pengujian menggunakan media penyimpanan yang berbeda

Media penyimpanan NAS saat ini didominasi penggunaan *disk drive* dari pada SSD, hal ini sangat mungkin dikarenakan perbedaan kemampuan dan karakteristik dari kedua penyimpanan tersebut. Melakukan pengujian di lingkungan yang berbeda akan membantu dalam memvalidasi beberapa kemungkinan yang mungkin terjadi dalam proses akuisisi terhadap penyimpanan tersebut.

3. Pengujian menggunakan panduan pada standar yang berbeda,

Melakukan perbandingan efektifitas dari pengujian akuisisi menggunakan standar NIST dengan metode kerja pengujian pada sistem pencadangan di dalam skema *Disaster Recovery Plan* (DRP). Misalnya, membandingkan dengan akuisisi pada NAS iSCSI *backup*. Perbandingan ini akan memberikan pandangan yang lebih lanjut tentang penanganan yang paling efektif dan efisien terhadap metode yang digunakan.

Daftar Pustaka

- Adji, D. S., Eduardus, G., Michael, Minawati, & Budiharto, W. (2021). Performance Analysis between Cloud Storage and NAS to Improve Company's Performance: A Literature Review. *Proceedings of 2021 1st International Conference on Computer Science and Artificial Intelligence, ICCSAI 2021*, 263–268. Retrieved from <https://doi.org/10.1109/ICCSAI53272.2021.9609792>
- Ajjola, A., Zavorsky, P., & Ruhl, R. (2014). A Review and Comparative Evaluation of Forensics Guidelines of NIST SP 800-101 Rev. 1 :2014 And ISO/IEC 27037:2012. In *World Congress on Internet Security*.
- Akbar, M. H., Sunardi, S., & Riadi, I. (2019). Analisis Bukti Digital Pada Flash Disk Drive Menggunakan Metode Generic Computer Forensic Investigation Model (GCFIM). In *Seminar Nasional Teknologi* (pp. 715–723). Jakarta: Fakultas Teknik Universitas Krisnadwipayana.
- Ariffin, K. A. Z., & Ahmad, F. H. (2021). Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0. *Computers & Security*, 105, 102237. Retrieved from <https://doi.org/10.1016/j.cose.2021.102237>
- Choi, J. H., Park, J., & Lee, S. (2020). Reassembling Linux-based Hybrid RAID. *Journal of Forensic Sciences*, 65(3), 966–973. Retrieved from <https://doi.org/10.1111/1556-4029.14258>
- Easttom, C. (2017). *System forensics, investigation, and response*. books.google.com. Retrieved from <https://books.google.com/books?hl=en&lr=&id=bPA2DwAAQBAJ&oi=fnd&pg=PP1&dq=raid+forensics&ots=IuyeQZVWiz&sig=tidddxPh8j71DfHqd0EAKqmlHHc>
- Fitriana, M., Ar, K., Marsya, J. M., Informasi, P. T., Tarbiyah, F., & Keguruan, D. (2020). Penerapan Metode National Institute Of Standards And Technology (NIST) Dalam Analisis Forensik Digital Untuk Penanganan Cyber Crime. *Jurnal Pendidikan Teknologi Informasi*, 4(1), 29–39.
- Freeman, W., & Miller, E. (2000). *Design for a Decentralized Security System For Network Attached Storage*.
- Halim, R. M. N. (2019). Penerapan Network Attached Storage (NAS) berbasis Raspberry Pi di LP3SDM AZRA Palembang. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, 6(3), 309. Retrieved from <https://doi.org/10.25126/jtiik.2019631416>

- Hariyadi, D., Kusuma, M., & Sholeh, A. (2021). *Digital Forensics Investigation on Xiaomi Smart Router Using SNI ISO/IEC 27037:2014 and NIST SP 800-86 Framework*.
- Hariyadi, D., & Supriyono, A. R. (2017). Kerangka Investigasi Forensik Pada Peladen Pertukaran Berkas Samba Berdasarkan SNI ISO/IEC 27037:2014. *Telematika*, 14(1), 62–67.
- Indriyanto, M. W., Hariyadi, D., Habibi, M., Achmad, U. J., & Yogyakarta, Y. (2020). Investigasi Dan Analisis Forensik Digital Pada Percakapan Grup Whatsapp Menggunakan NIST SP 800-86 dan Support Vector Machine. *CyberSecurity Dan Forensik Digital*, 3(2), 34–38.
- J, S. K. P., Surya, K. R., Surya, S., & Shriram, R. S. (2021). Raspberry Pi Turns into VPN & NAS Server. *Annals of the ...*, 25(5), 682–691. Retrieved from <http://annalsofsrcb.ro/index.php/journal/article/view/4406%0Ahttp://annalsofsrcb.ro/index.php/journal/article/download/4406/3540>
- Kaffah, F. M., Nur, S., Fitrianto, A., Syaripudin, U., & Darwan, D. (2022). Analisis Live Forensics Pada SSD SATA Fungsi Trim Menggunakan Metode National Institute Of Justice (NIJ). *Teknologi Nusantara*, 4(2), 21–33. Retrieved from <http://ojs.uninus.ac.id/index.php/teknologinusantara>
- Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to Integrating Forensic Techniques into Incident Response. *NIST Special Publication*.
- Kent, K., Chevalier, S., Grance, T., & Dang, H. (n.d.). *Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response Recommendations of the National Institute of Standards and Technology*.
- Koroniotis, N., Moustafa, N., & Sitnikova, E. (2019). Forensics and Deep Learning Mechanisms for Botnets in Internet of Things: A Survey of Challenges and Solutions. *IEEE Access*, 7, 61764–61785. Retrieved from <https://doi.org/10.1109/ACCESS.2019.2916717>
- Koza, E. (2022). *Semantic Analysis of ISO/IEC 27000 Standard Series and NIST Cybersecurity Framework to Outline Differences and Consistencies in the Context of Operational and Strategic Information Security Citation: Erfan Koza. 'Semantic Analysis of ISO/IEC 27000 Standard Series and NIST Cybersecurity Framework to Outline Differences and Consistencies in the Context of Operational and Strategic Information Security'. Medicon Engineering Themes (Vol. 2)*.
- Kumar, R., Nagaraj, A., Paul, B., & Dixit, S. P. (2021). Network-Attached Storage: Data Storage Applications. *Turkish Journal of Computer and Mathematics Education V*

- Ol.12 No, 12, 2385–2396. Retrieved from*
<https://turcomat.org/index.php/turkbilmat/article/view/7830>
- Kurii, Y., & Opirskyy, I. (2022). Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013. In *Cybersecurity Providing in Information and Telecommunication System*.
- Kurnadi Keamanan Siber, B., Ali Nurfadillah Keamanan Siber, F., Tegar Sabila Keamanan Siber, M., Raya Usa, J. H., Nutug, P., Ciseeng, K., & Bogor, K. (2024). Analisis Memory Forensics Windows Subsystem for Linux 2 (WSL2) Berbasis Hyper-V pada Windows 11 Berdasarkan Nist 800-86. *Jurnal Penelitian Sistem Informasi*, 2(1), 178–188. Retrieved from <https://doi.org/10.54066/jpsi.v2i1.1594>
- Loppies, S. H. D., & Suwarjono. (2019). Pemanfaatan Network Attached Storage (NAS) Untuk Mendukung Kinerja Pelayanan Kantor Kelurahan Di Kabupaten Merauke (Studi kasus : Kantor Kelurahan Seringgu Jaya). *Musamus Journal of Technology & Information (MJTI)*, 02(01). Retrieved from <http://www.ejournal.unmus.ac.id/index.php/it/article/view/2452>
- Muhammad, *, & Asshiddiq, J. (2018). Network Attached Storage (NAS) Menggunakan Desktop PC. *Prosiding Seminar Nasional Ilmu Komputer Dan Teknologi Informasi*, 3(2), 2540–2542. Retrieved from <http://e-journals.unmul.ac.id/index.php/SAKTI/article/view/1859>
- Nofiyah, A., & Mushlihudin, M. (2020). Analisis Forensik pada Web Phishing Menggunakan Metode National Institute Of Standards And Technology (NIST). *Jurnal Sarjana Teknik Informatika*, 8(2), 11–23.
- Ramadhan, R. A., & Mualfah, D. (2020). 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*, 5(2), 183–192. Retrieved from [https://doi.org/10.25299/itjrd.2021.vol5\(2\).5750](https://doi.org/10.25299/itjrd.2021.vol5(2).5750)
- Ramadhan, R. A., Rachmat Setiawan, P., & Hariyadi, D. (2022). Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037:2012 and NIST SP800-86 Framework. *IT Journal Research and Development*, 162–168. Retrieved from <https://doi.org/10.25299/itjrd.2022.8968>
- Riadi, I., & Hadi, A. (2020). Analisis Bukti Digital Trim Enable SSD NVME Menggunakan Metode Static Forensics (Analysis of Digital Evidence Trim Enable on

- SSD NVME Using Static Forensics Method). *JUITA: Jurnal Informatika*, 8(1), 65–74.
- Riadi, I., Sunardi, S., & Hadi, A. (2020). Analysis of Digital Evidence Trim Enable on SSD NVME Using Static Forensics Method. *JUITA: Jurnal Informatika*, 8(1), 65–74.
- Rochmadi, T., Wicaksono, Y., & Nisa, N. D. (2020). Digital Evidence Identification of Android Device using Live Forensics Acquisition on Cloud Storage (iDrive). *International Journal of Computer Applications*, 175(26), 40–43. Retrieved from <https://doi.org/10.5120/ijca2020920815>
- Roy, P. P. (2020). A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard. In *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTE A)* (pp. 1–3). Retrieved from <https://doi.org/10.1109/NCETSTE A48365.2020.9119914>
- Saad, S. K., Umar, R., & Fadlil, A. (2020). Analisis Forensik Aplikasi Dropbox Pada Android Menggunakan Metode NIST. In *Dinamika Informatika* (pp. 119–123). Yogyakarta: Universitas PGRI Yogyakarta.
- salsabila, D. S. (2024). *Analisis Digital Forensics Pada Web Phishing Menggunakan Metode National Institute Of Standards And Technology (NIST) SP 800-86*. Universitas Muhammadiyah Purwokerto.
- Sama, H., Liden, L., Saragi, J. S. D., Erlene, M., Kelvin, K., Hartanto, Y., ... Devalia, M. (2021). Studi Komparasi Framework NIST Dan ISO 27001 Sebagai Standar Audit Dengan Metode Deskriptif Studi Pustaka. *Rabit : Jurnal Teknologi Dan Sistem Informasi Univrab*, 6(2), 116–121. Retrieved from <https://doi.org/10.36341/rabit.v6i2.1752>
- Soffa, H. (2015). Analisis Perbandingan Kinerja Freenas Dan Open Media Vault (Omv) Sebagai Sistem Operasi Jaringan Network Attached Storage (Nas). *Seminar Nasional ...*, 117. Retrieved from <http://prosiding.uika-bogor.ac.id/index.php/semnati/article/view/44%0Ahttp://prosiding.uika-bogor.ac.id/index.php/semnati/article/download/44/35>
- Steel, C. (2006). *Windows Forensics: The Field Guide for Corporate Computer Investigations*. John Wiley & Sons.
- Syahib, M. I., Riadi, I., & Rusydi, U. (2020). Akuisisi Bukti Digital Aplikasi Viber Menggunakan Metode National Institute of Standards Technology (NIST). *Jurnal Sains Komputer & Informatika (J-SAKTI)*, 4(1), 170–178.

- Umar, R., Riadi, I., & Handoyo, E. (2020). *Manage Security Services (DSS05) Dan NIST SP 800-55. Tahun* (Vol. 10).
- Yan Fikri Hendrawan, M., & Hadinegoro, A. (2023). Analisis Bukti Digital Pada Discord Browser Menggunakan Teknik Live Forensic Dengan Metode NIST SP 800-86. *Jurnal Infomedia*., 8(2).
- Yeboah-Ofori, A., Yeboah-Boateng, E., & Gustav Yankson, H. (2019). Relativism Digital Forensics Investigations Model: A Case For The Emerging Economies. In *Proceedings - 2019 International Conference on Cyber Security and Internet of Things, ICSIoT 2019* (pp. 93–100). Institute of Electrical and Electronics Engineers Inc. Retrieved from <https://doi.org/10.1109/ICSIoT47925.2019.00023>
- Yudhana, A., Riadi, I., & Anshori, I. (2018). Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist. *IT JOURNAL RESEARCH AND DEVELOPMENT*, 3(1), 13–21. Retrieved from [https://doi.org/10.25299/itjrd.2018.vol3\(1\).1658](https://doi.org/10.25299/itjrd.2018.vol3(1).1658)
- Zakari Yahya, A., Juwoto Buru, D., & Sugiantoro, B. (2022). Analysis Of Digital Evidence On Random Access Memory Android Using Live Forensic Method Case Of Illegal Weapon Sales. *CyberSecurity and Digital Forensics*, 5(1), 6–11.

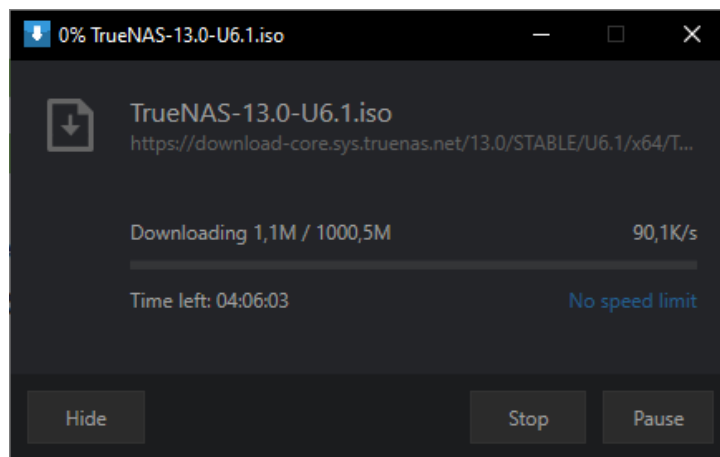
LAMPIRAN A

Instalasi TrueNAS Core

Tahapan dalam melakukan instalasi TrueNAS dapat di jelaskan dalam tahapan proses sebagai berikut:

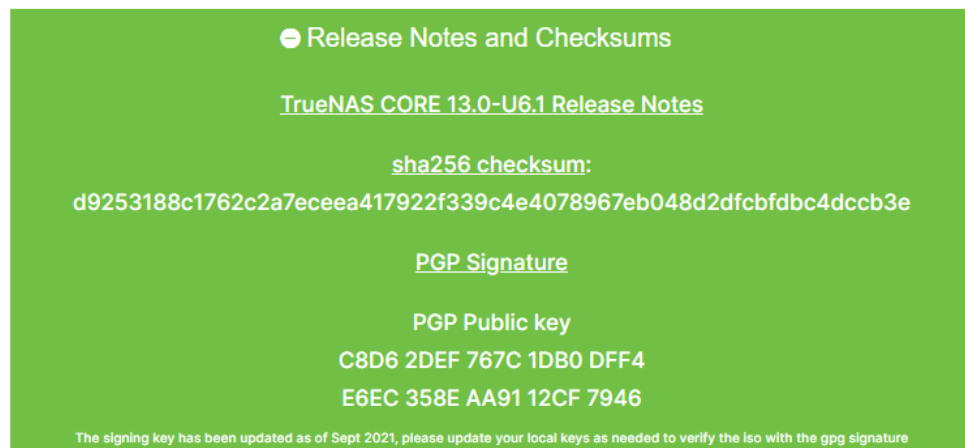
1. Pengunduhan iso image dari situs TrueNAS

File iso *image* TrueNAS Core dapat di unduh pada laman resmi TrueNAS pada tautan <https://www.truenas.com/download-truenas-core/>. Versi terbaru pada saat pengujian ini dilakukan adalah TrueNAS-13.0-U6.1



Gambar A. 1 Proses unduh file ISO TrueNAS Core

Untuk melakukan validasi terhadap file ISO yang diunduh, pada laman resmi *web* TrueNAS disediakan informasi tentang nilai HASH checksum dan PGP *Signature Public key* seperti pada gambar berikut :



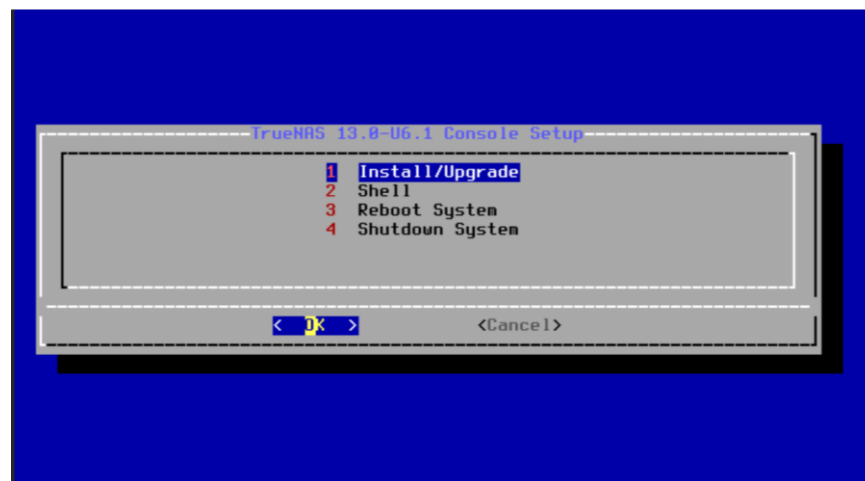
Gambar A. 2 Checksum dan PGP Key file unduhan

Pada pengujian ini, instalasi dilakukan secara *default* dengan memilih menu 1 (satu). Selanjutnya akan tampil proses instalasi seperti gambar dibawah ini.

```
ci0
pci1: <ACPI PCI bus> on pcib1
virtio_pci1: <VirtIO PCI (legacy) SCSI adapter> port 0xe000-0xe03f mem 0xfc40000
0-0xfc400fff,0xfe000000-0xfe003fff irq 10 at device 1.0 on pci1
vtscsi0: <VirtIO SCSI Adapter> on virtio_pci1
virtio_pci2: <VirtIO PCI (legacy) Console adapter> port 0xf040-0xf07f mem 0xfc65
3000-0xfc653fff,0xfea04000-0xfea07fff irq 10 at device 9.0 on pci0
virtio_pci3: <VirtIO PCI (legacy) Network adapter> port 0xf0c0-0xf0df mem 0xfc65
4000-0xfc654fff,0xfea08000-0xfea0bfff irq 10 at device 18.0 on pci0
vtnet0: <VirtIO Networking Adapter> on virtio_pci3
vtnet0: Ethernet address: bc:24:11:a2:30:e0
pcib2: <ACPI PCI-PCI bridge> mem 0xfc655000-0xfc6550ff irq 10 at device 30.0 on
pci0
pci2: <ACPI PCI bus> on pcib2
pcib3: <ACPI PCI-PCI bridge> mem 0xfc656000-0xfc6560ff irq 11 at device 31.0 on
pci0
pci3: <ACPI PCI bus> on pcib3
acpi_syscontainer0: <System Container> on acpi0
vmgen0: <VM Generation Counter> on acpi0
acpi_syscontainer1: <System Container> port 0xaf00-0xaf0b on acpi0
acpi_syscontainer2: <System Container> port 0xaf00-0xaf03 on acpi0
acpi_syscontainer3: <System Container> port 0xae00-0xae17 on acpi0
atkbd0: <Keyboard controller (i8042)> port 0x60,0x64 irq 1 on acpi0
atkbd0: <AT Keyboard> irq 1 on atkbd0
```

Gambar A. 5 Progress instalasi TrueNAS

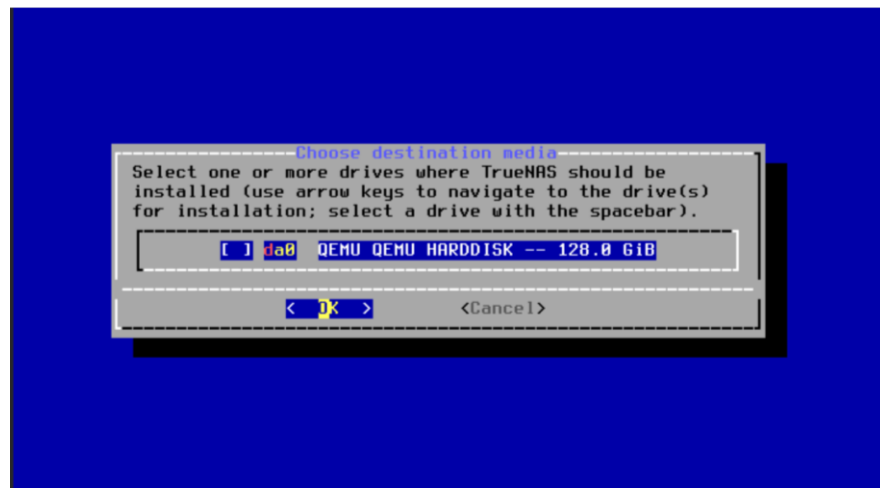
Tampilan konsol akan menampilkan menu seperti dibawah ini, pilihan 1 (satu) untuk Instalasi atau *Upgrade* instalasi, pilihan 2 (dua) untuk masuk ke dalam tampilan *shell*, menu 3 (tiga) untuk menyalakan kembali komputer dan menu 4 (empat) untuk mematikan komputer.



Gambar A. 6 Menu konsol *setup* TrueNAS

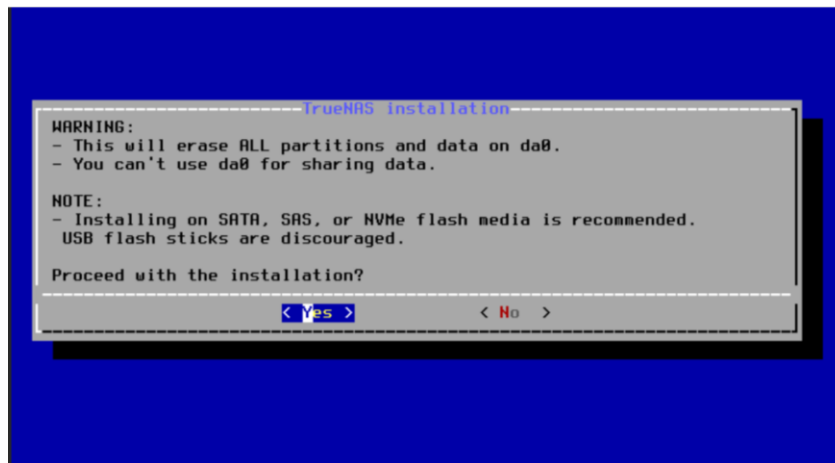
Tahapan selanjutnya adalah menentukan *disk* yang digunakan untuk pemasangan sistem operasi. Semua *disk drive* yang terpasang pada komputer akan terbaca pada menu ini, sehingga untuk memilih *disk drive* yang tepat, perlu diperhatikan lebih teliti pada jenis dan ukuran *disk drive* yang digunakan.

Untuk mencegah terjadinya kesalahan pada pemilihan *disk drive* pada pengujian ini, pemasangan *disk* penyimpanan dilakukan setelah instalasi sistem operasi FreeNAS dilakukan.



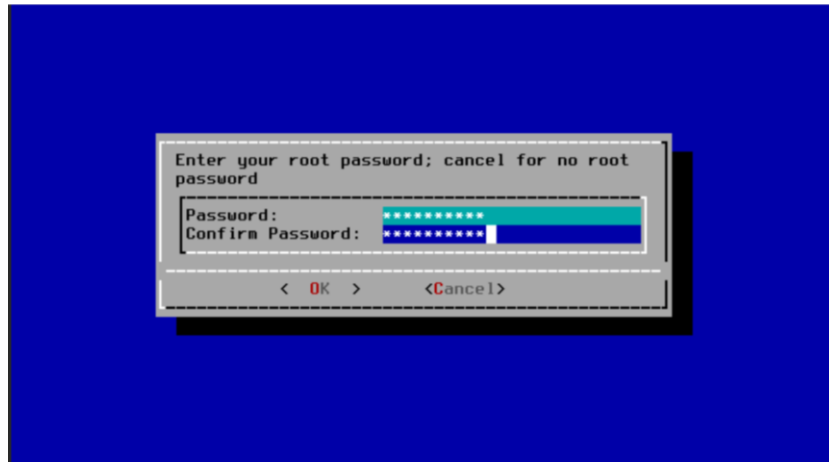
Gambar A. 7 Memilih harddisk yang akan diinstall sistem operasi TrueNAS

Setelah *disk drive* dipilih, kemudian akan tampil jendela konfirmasi akan dilakukannya proses instalasi. Proses ini akan mengakibatkan seluruh data di dalam *disk drive* akan dihapus dan *disk drive* tidak bisa dibagikan dalam jaringan. Konfirmasi setuju akan melanjutkan proses ini dan tahapan selanjutnya akan dijalankan. Tangkapan layar terlihat pada gambar berikut.



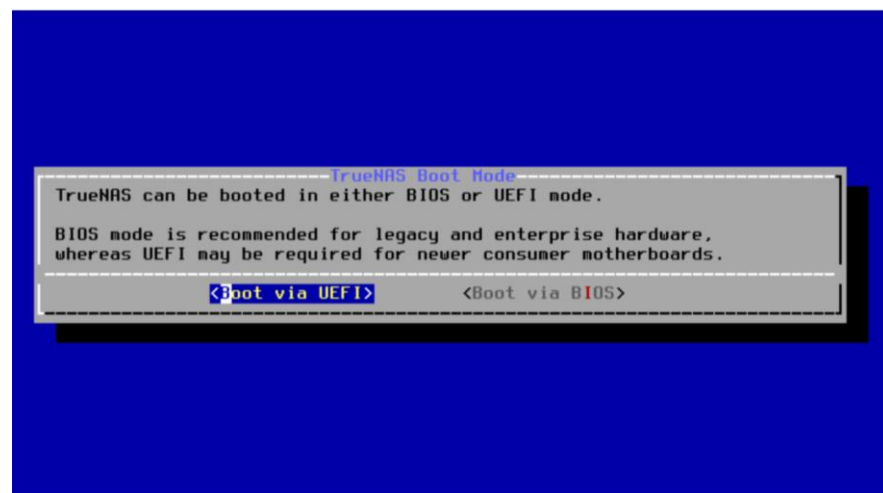
Gambar A. 8 Konfirmasi persetujuan penghapusan data pada *disk drive*

Setelah menyetujui untuk menghapus seluruh data di dalam *disk drive*, tahapan selanjutnya adalah pemberian kata sandi untuk user *root*. Jika tidak menginginkan password untuk *root* dapat memilih *cancel* dan proses tetap dilanjutkan, seperti gambar berikut.



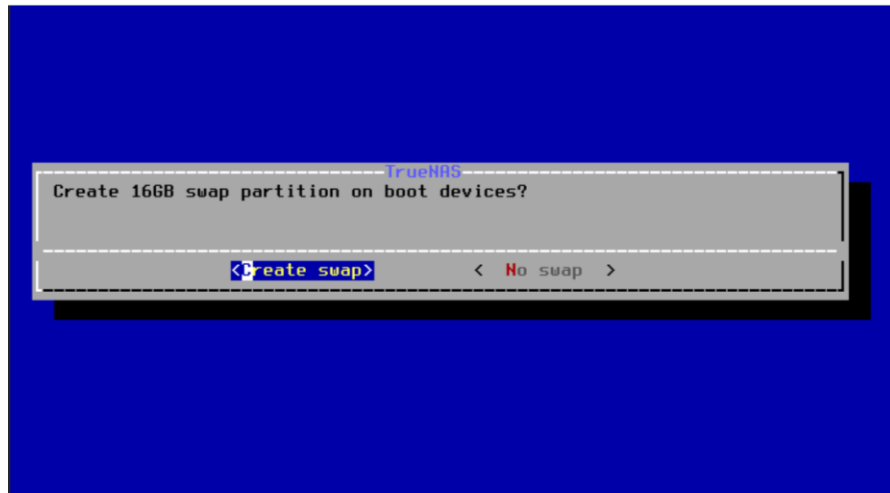
Gambar A. 9 Pemberian kata sandi untuk user *root*

Sistem TrueNAS dapat berjalan pada komputer teknologi lama yang belum memiliki mode *UEFI*. Untuk memilih pilihan ini, pada tampilan menu berikutnya terdapat pilihan apakah TrueNAS akan dijalankan menggunakan *boot option UEFI* atau *boot option Legacy* atau *BIOS*. Terlihat pada gambar berikut.



Gambar A. 10 Pilihan untuk *boot option UEFI* dan *BIOS (Legacy)*

Setelah menentukan *boot option*, menu terakhir adalah pilihan untuk mengaktifkan *memory swap*. Jika tidak menginginkan pembuatan partisi *swap*, pilihan *No Swap* akan tetap melanjutkan proses, seperti gambar berikut.



Gambar A. 11 Membuat partisi Swap

Setelah semua tahapan telah dilakukan, kemudian proses instalasi akan berjalan. Lama proses instalasi bergantung pada spesifikasi komputer yang digunakan. Terlihat seperti pada gambar berikut.

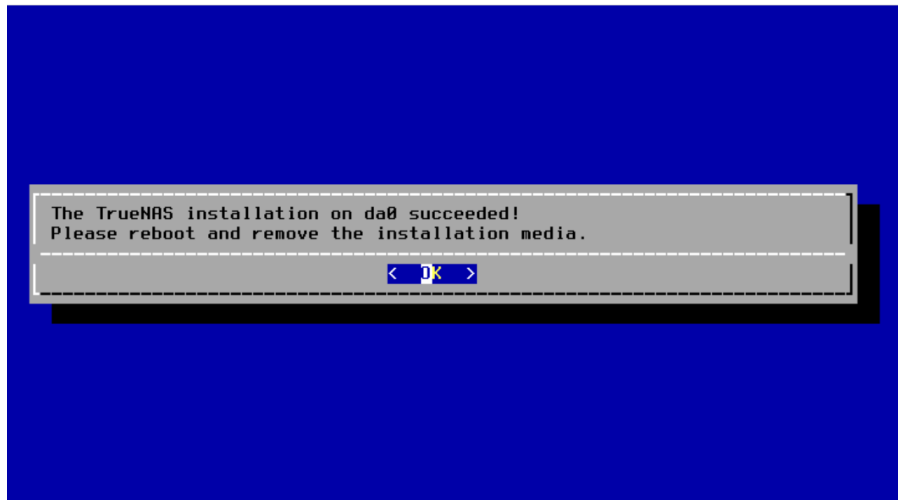
```

3+0 records in
2+0 records out
2097152 bytes transferred in 0.011570 secs (181262498 bytes/sec)
da0 created
kern.geom.debugflags: 0 -> 16
kern.geom.label.disk_ident.enable: 0 -> 0
da0p1 added
/dev/da0p1: 532288 sectors in 16634 FAT16 clusters (16384 bytes/cluster)
BytesPerSec=512 SecPerClust=32 ResSectors=1 FATs=2 RootDirEnts=512 Media=0xf0 FA
Tsecs=65 SecPerTrack=63 Heads=255 HiddenSecs=0 HugeSectors=532480
da0p3 added
da0p2 added
gmirror: No such device: swap.
da0 destroyed
da0 created
kern.geom.debugflags: 16 -> 16
kern.geom.label.disk_ident.enable: 0 -> 0
da0p1 added
/dev/da0p1: 532288 sectors in 16634 FAT16 clusters (16384 bytes/cluster)
BytesPerSec=512 SecPerClust=32 ResSectors=1 FATs=2 RootDirEnts=512 Media=0xf0 FA
Tsecs=65 SecPerTrack=63 Heads=255 HiddenSecs=0 HugeSectors=532480
da0p3 added
da0p2 added
Installing base-os (1 of 3)
....10....20....30....40....50....60....70....80....90

```

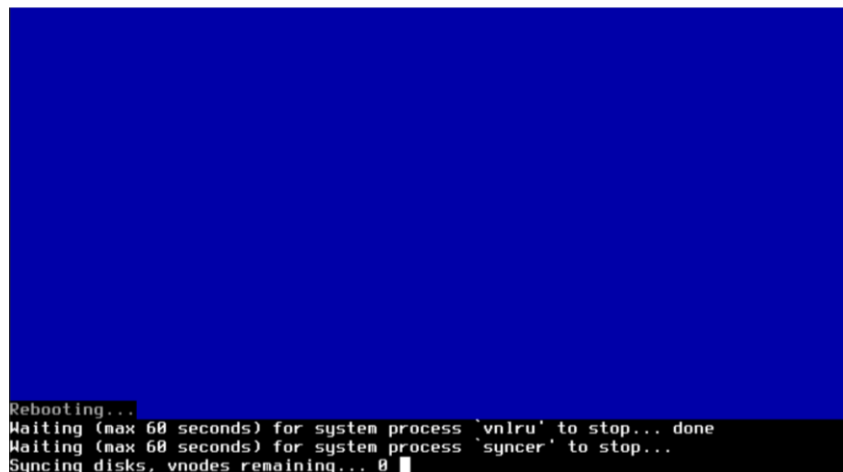
Gambar A. 12 Proses instalasi TrueNAS

Jendela konfirmasi akan tampil setelah proses instalasi berhasil dilakukan. Konfirmasi selanjutnya adalah melepas USB disk yang berisi file instalasi kemudian tekan tombol OK untuk menyalakan kembali komputer. Seperti terlihat pada gambar berikut.



Gambar A. 13 Konfirmasi melepas USB drive dan menyalakan ulang komputer

Proses booting untuk menyalakan ulang komputer akan terlihat seperti gambar berikut.



Gambar A. 14 Menyalakan ulang dan *booting* komputer

Setelah proses *booting* selesai, tampilan pada terminal akan terlihat beberapa menu untuk konfigurasi jaringan. Secara *default* tidak perlu merubah konfigurasi, kecuali ada kebutuhan khusus untuk keamanan data ataupun penyesuaian pada konfigurasi pada internal network. Tampilan menu TrueNAS akan terlihat seperti gambar berikut.

```
Console setup
-----

1) Configure Network Interfaces
2) Configure Link Aggregation
3) Configure VLAN Interface
4) Configure Default Route
5) Configure Static Routes
6) Configure DNS
7) Reset Root Password
8) Reset Configuration to Defaults
9) Shell
10) Reboot
11) Shut Down

The web user interface is at:

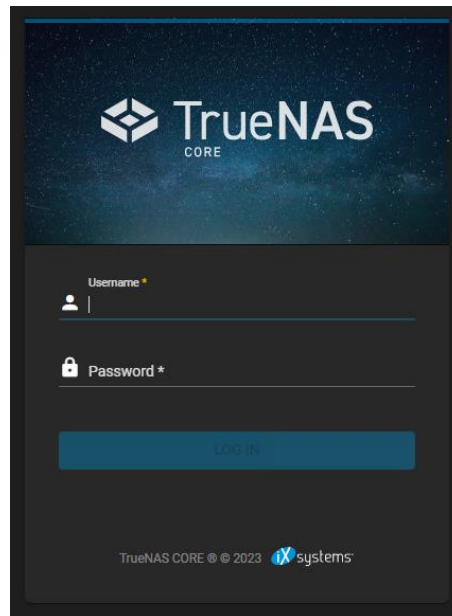
http://192.168.4.98
https://192.168.4.98

Enter an option from 1-11: █
```

Gambar A. 15 Menu awal TrueNAS pada terminal

3. Konfigurasi dasar TrueNAS core

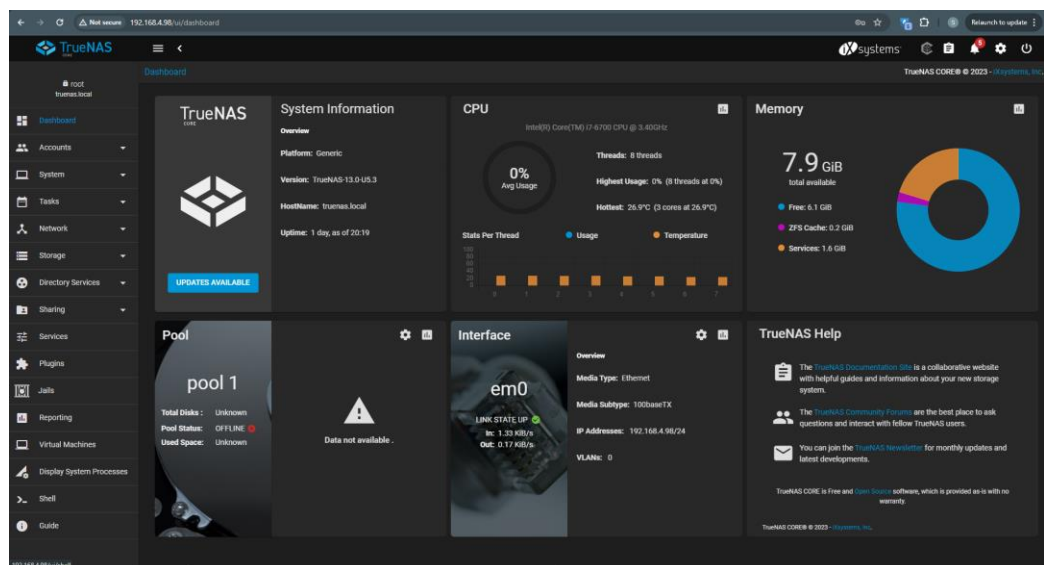
Untuk melakukan konfigurasi di TrueNAS core, dilakukan dengan membuka tautan menggunakan *internet browser* dengan alamat tujuan ip address dari server dengan protokol https. Gunakan *username* dan *password* yang dimasukkan pada saat instalasi awal. Terlihat seperti gambar dibawah ini.



Gambar A. 16 Tampilan login TrueNAS core

Setelah berhasil login, kemudian akan terlihat tampilan *dashboard* awal dari TrueNAS. Terdapat informasi tentang detail sistem operasi, spesifikasi komputer (kemampuan cpu, kapasitas *memory* dan antarmuka jaringan) dan *pool* dari penyimpanan yang nantinya akan dibuat. Selain itu juga terdapat tautan dokumentasi penggunaan aplikasi, forum komunitas dan berita berlangganan tentang produk dan layanan pengembang aplikasi TrueNAS.

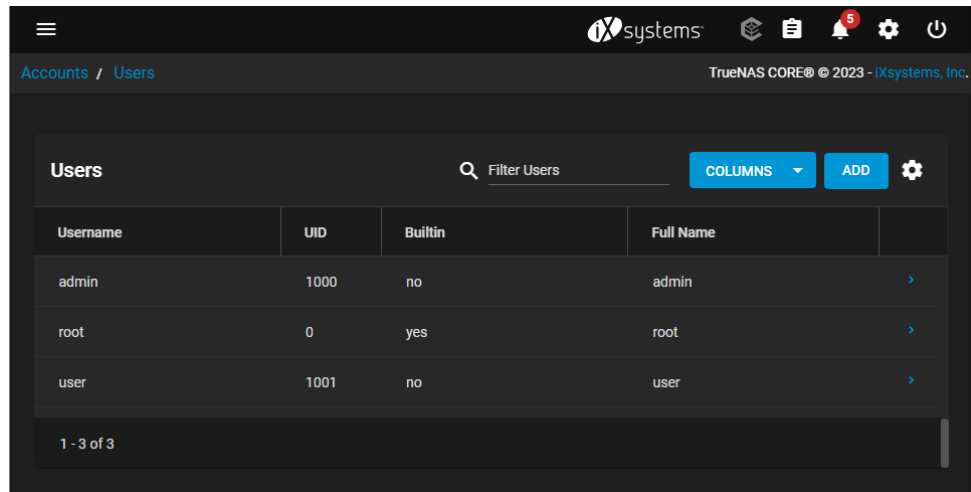
Pada sisi kiri aplikasi terdapat menu antarmuka pengguna untuk melakukan konfigurasi pada TrueNAS. Panduan juga terdapat pada baris paling bawah menu ini. Tampilan *dashboard* terlihat pada gambar berikut.



Gambar A. 17 Dashboard pada TrueNAS core

Accounts

Pada menu ini terdapat konfigurasi untuk membuat, menghapus dan modifikasi pengguna maupun grup. Pada percobaan ini dibuat 2 (dua) pengguna baru yaitu admin dan user. Seperti terlihat pada gambar berikut.

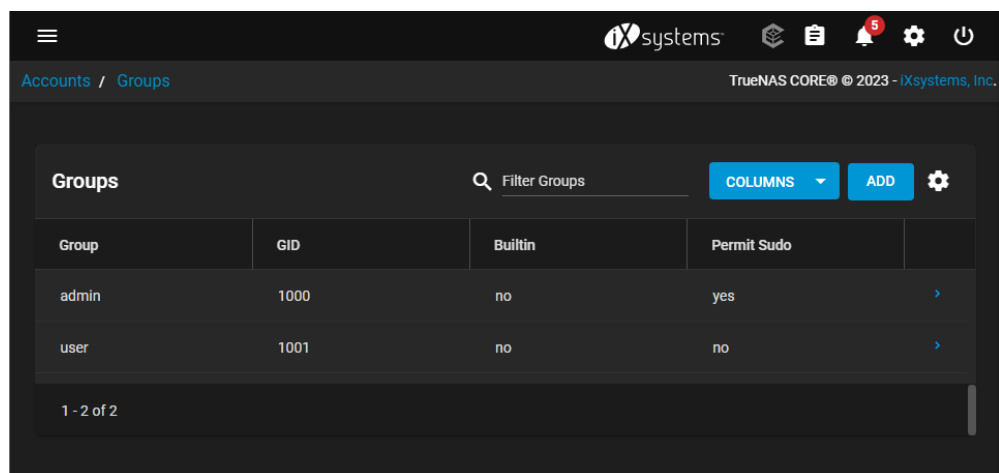


Username	UID	Builtin	Full Name	
admin	1000	no	admin	>
root	0	yes	root	>
user	1001	no	user	>

1 - 3 of 3

Gambar A. 18 Penambahan pengguna baru

Untuk grup pengguna ditambahkan dengan nama yang sama yaitu admin dan user, seperti terlihat pada gambar berikut.



Group	GID	Builtin	Permit Sudo	
admin	1000	no	yes	>
user	1001	no	no	>

1 - 2 of 2

Gambar A. 19 Penambahan grup pengguna baru

System

Pada pengujian ini tidak ada perubahan yang dilakukan pada menu *system*.

Task

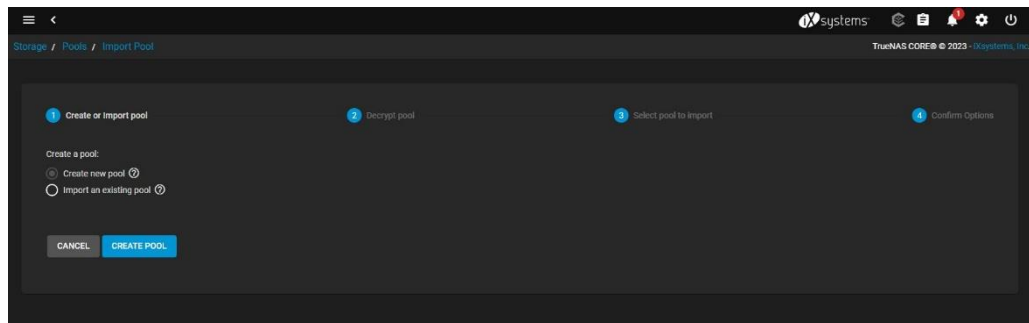
Menu ini berisi tentang pengaturan otomatisasi dan sinkronisasi. Pada pengujian ini tidak dilakukan perubahan pada menu *task*.

Network

Konfigurasi yang dapat dilakukan pada menu ini terdiri dari perubahan pada *domain name*, DNS Server dan *gateway*. Selain itu juga terdapat pilihan untuk menambahkan kartu jaringan dan perubahan konfigurasi *route* jika menggunakan *static route* atau secara manual. Pada pengujian ini tidak melakukan konfigurasi pada menu *network*.

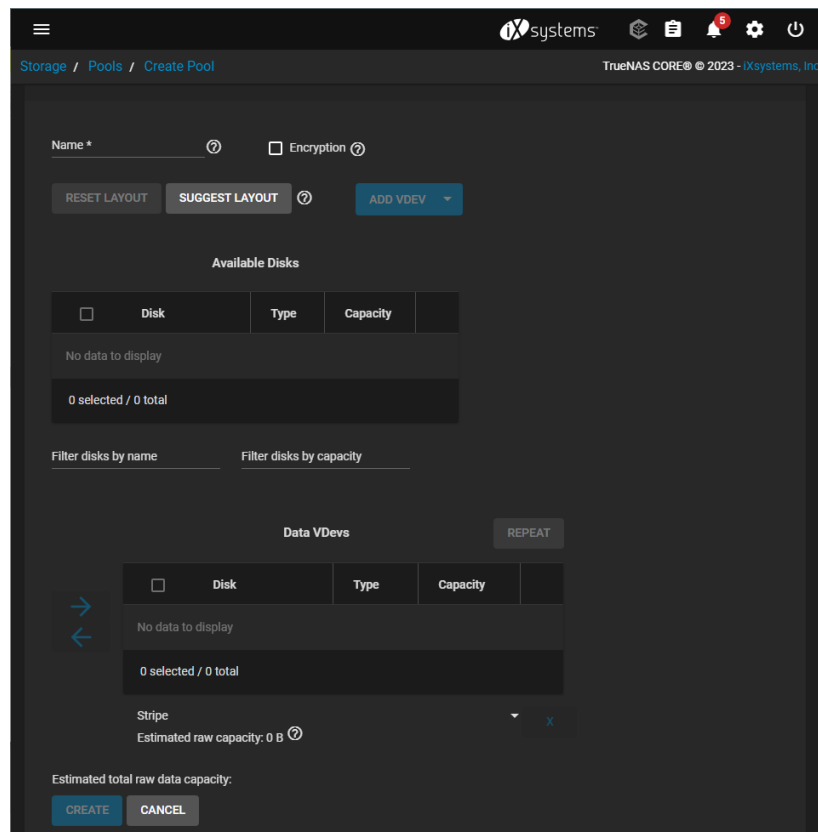
Storage

Pada pengujian pertama, disk drive yang digunakan 1 (satu) unit HDD dengan kapasitas 500 GB. Sedangkan pada pengujian ke 2 (dua) menggunakan 3 (tiga) unit HDD dengan kapasitas masing-masing 500 GB. Konfigurasi pertama yang dilakukan yaitu dengan membuat *pool* seperti gambar berikut.



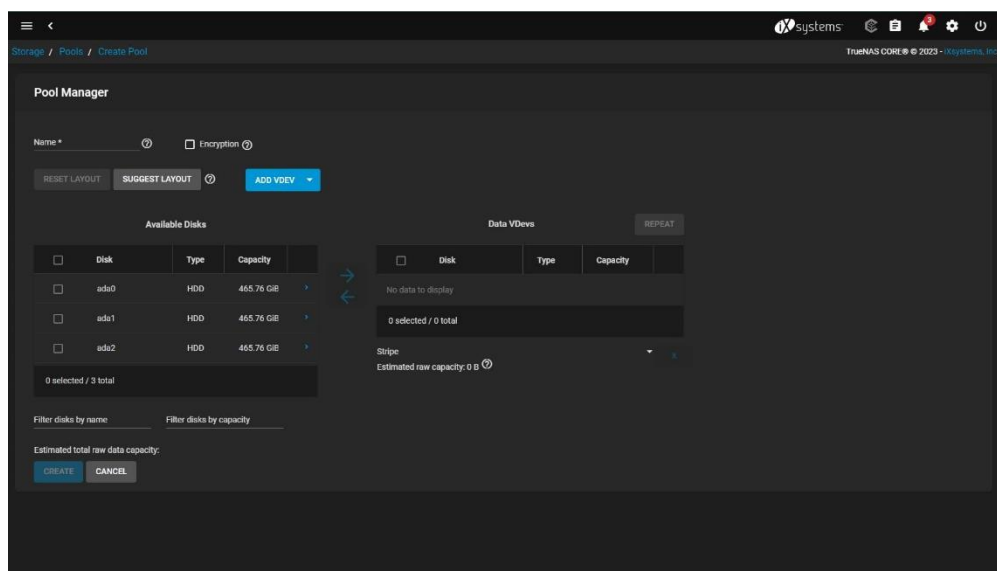
Gambar A. 20 Membuat *pool* baru

Untuk menambahkan disk drive kedalam *pool* dengan menekan tombol *create pool* dan akan terbuka tampilan *pool manager*. Selanjutnya akan tampil konfigurasi untuk memberikan nama *pool* dan memilih *disk drive* yang akan dimasukkan kedalam *pool*. Seperti terlihat pada gambar.



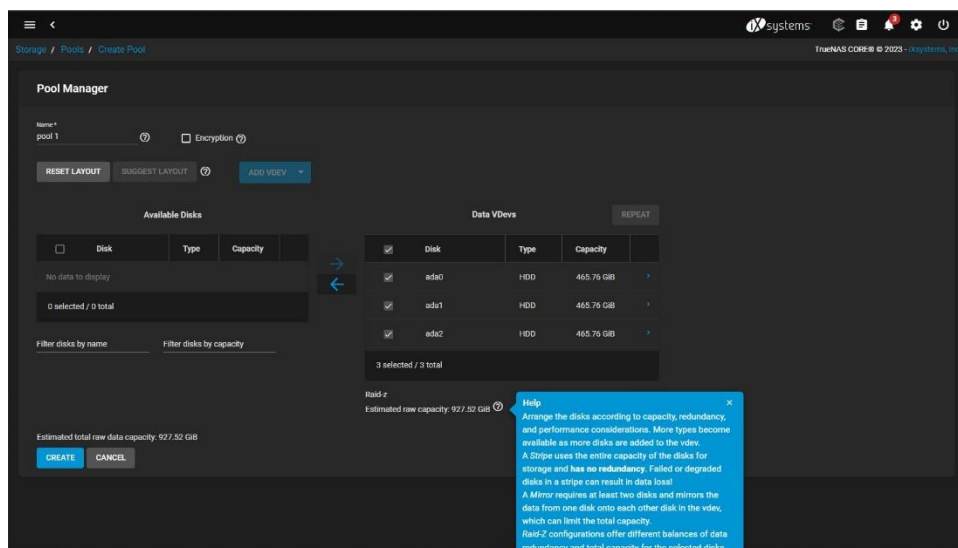
Gambar A. 21 Pool Manager untuk menambahkan disk drive

Setelah memberikan nama *pool*, Langkah selanjutnya adalah dengan memindahkan *disk drive* pada posisi *available disk* ke Data VDevs. Hal ini dilakukan untuk memilih *disk drive* mana saja yang akan dimasukkan kedalam *pool* yang dibuat. Untuk membuat *pool* lebih dari satu maka *disk* yang di gunakan bisa dipilih sesuai dengan kebutuhan. Pengaturan ini terlihat seperti gambar berikut.



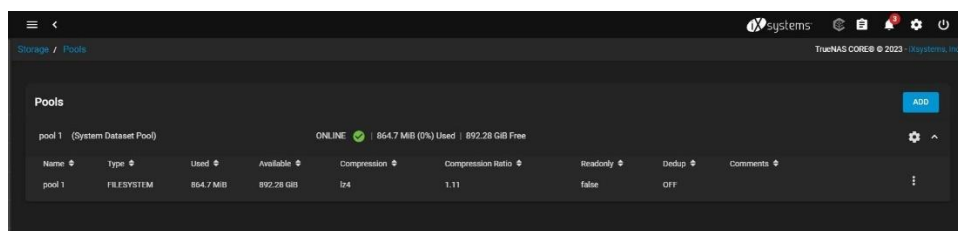
Gambar A. 22 Ubah posisi disk drive ke Data VDevs

Terdapat pilihan dalam menentukan pengelolaan *disk drive* didalam *pool* di TrueNAS, diantaranya yaitu *stripe*, *mirror* dan *raid z*. Perbedaan masing-masing pilihan ini mempengaruhi penggunaan dari kapasitas *disk drive*, apakah seluruh kapasitas penyimpanan akan digunakan (*stripe*), atau digunakan setengah untuk penyimpanan dan sisanya untuk mirroring (*mirror*) atau digunakan sebagian besar untuk penyimpanan dan sebagian kecil untuk mirroring dengan konfigurasi default dari aplikasi TrueNAS (*raid z*). Pengaturan ini seperti penggunaan RAID pada umumnya, akan tetapi TrueNAS tidak menggunakan istilah RAID dan menggunakan penamaan sendiri. Pada pengujian ini menggunakan *raid z* seperti terlihat pada gambar berikut.



Gambar A. 23 Konfigurasi pada *pool* untuk penyimpanan

Setelah *pool* baru berhasil dibuat, akan terlihat tampilan *pool* baru seperti pada gambar berikut.



Gambar A. 24 *Pool* yang baru dibuat

Pada pengujian ini tidak mengaktifkan metode pencadangan dengan *snapshots*, akan tetapi fitur ini tersedia dan dapat dikonfigurasi sesuai dengan kebutuhan.

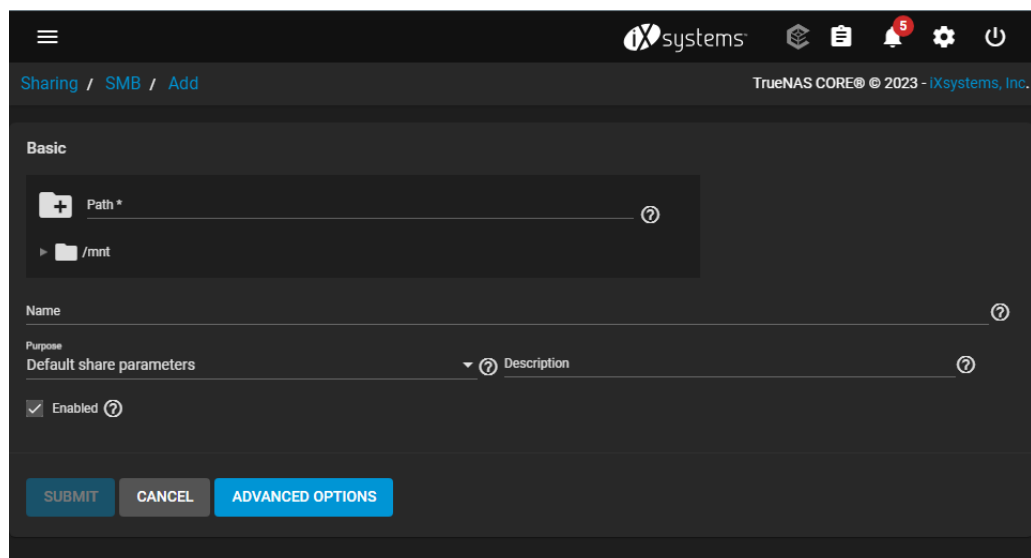
Directory Services

Pengujian ini dilakukan pada lingkungan jaringan yang tidak menggunakan *Active Directory* dalam pengelolaan data data koneksi server, sehingga untuk pengaturan pada menu ini tidak ada konfigurasi yang dilakukan.

Sharing

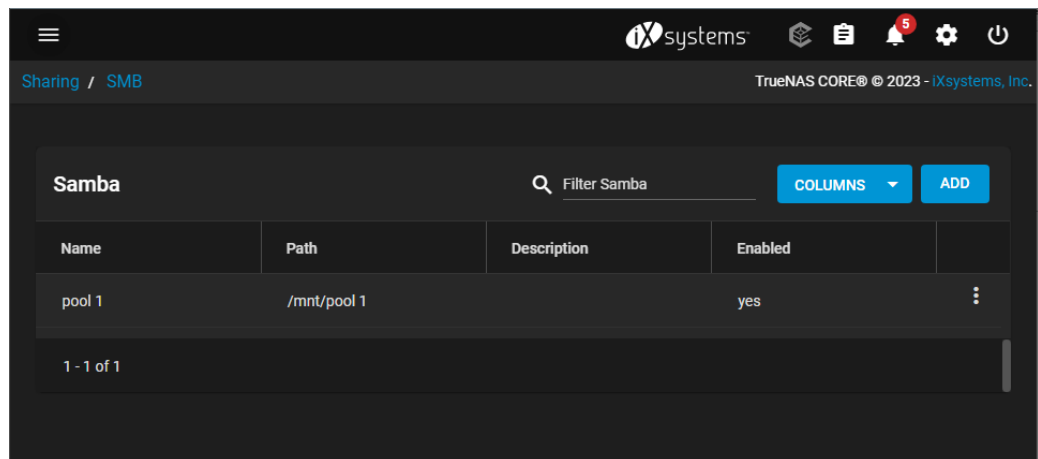
Untuk membagikan penyimpanan yang telah dikonfigurasi pada menu sebelumnya, perlu dilakukan beberapa konfigurasi untuk mengaktifkan layanan tersebut. Pada menu *sharing* terdapat beberapa pilihan tentang bagaimana penyimpanan ini akan dikonfigurasi. Pilihan-pilihan tersebut terbagi atas protokol yang digunakan, diantaranya yaitu *Apple Shares* yang digunakan untuk perangkat-perangkat yang menggunakan protokol AFP, *Block Shares* yang digunakan untuk jenis *sharing files* menggunakan tipe iSCSI di windows server, *Unix Shares* yang banyak digunakan untuk lingkungan Linux dengan protokol NFS, *WebDAV Shares* digunakan untuk pembagi penyimpanan dengan WebDAV dan *Windows Shares* yang paling banyak digunakan hampir di semua tipe OS yang menggunakan protokol SMB.

Pada pengujian ini *file sharing* ditambahkan pada folder */mnt* dengan parameter lain yang dikonfigurasi secara *default*. Perhatikan untuk memberikan tanda centang pada menu *enabled* untuk mengaktifkan *file sharing*. Tangkapan layar seperti terlihat pada gambar berikut.



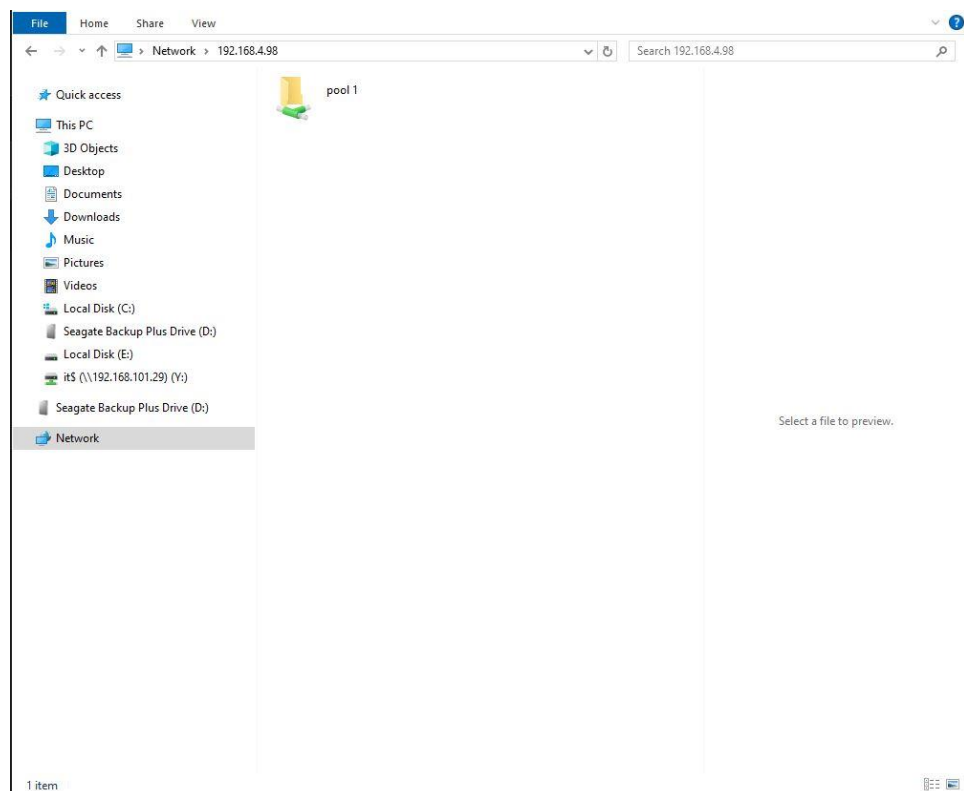
Gambar A. 25 Penambahan konfigurasi untuk *sharing*

Tampilan setelah file sharing berhasil di aktifkan akan terlihat seperti gambar berikut.



Gambar A. 26 File Sharing yang telah di konfigurasi

Untuk melakukan pengujian apakah konfigurasi *file sharing* sudah dilakukan dengan benar, dapat dilakukan dengan mengakses server pada *file browser*. Dalam pengujian ini file sharing di coba pada lingkungan windows 11, seperti terlihat pada gambar berikut.



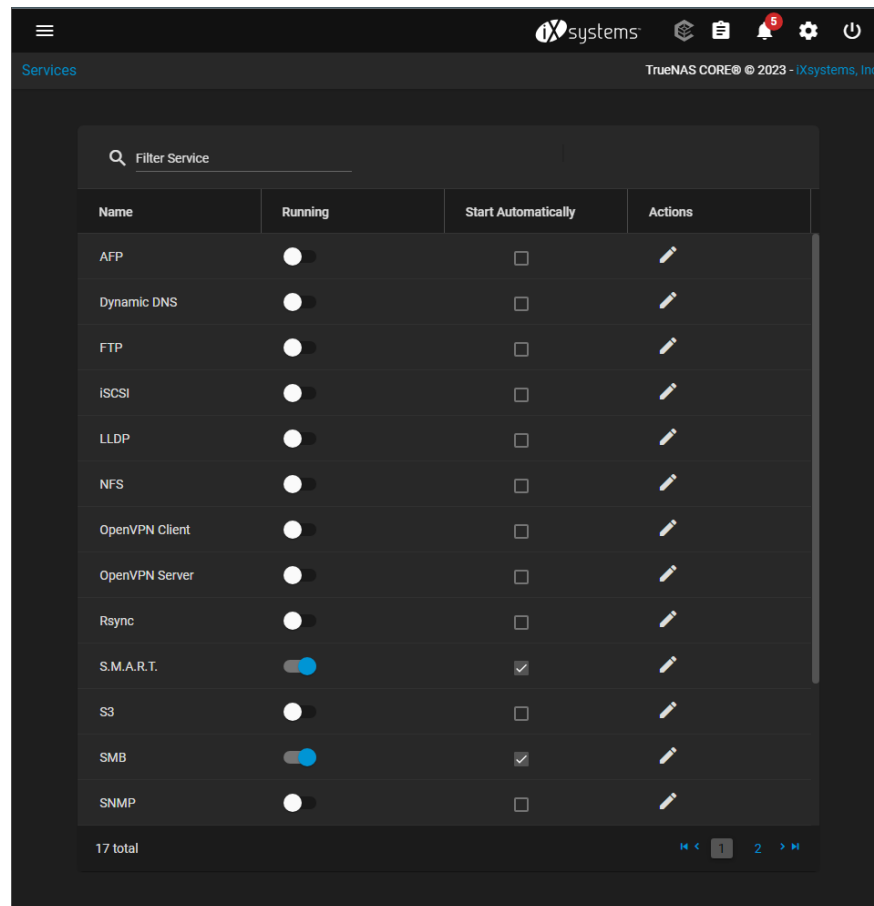
Gambar A. 27 SMB file sharing di windows 11

Services

Menu selanjutnya adalah *services*, dimana pada menu ini terdapat pilihan untuk layanan protokol yang akan digunakan dalam lingkungan TrueNAS server dan dapat dikonfigurasi sesuai dengan kebutuhan. Hal ini tentu saja akan sangat berpengaruh pada performa server, salah satu diantaranya adalah untuk keamanan jaringan.

Dengan terbatasnya protokol yang digunakan maka resiko terhadap keamanan jaringan menjadi lebih rendah. Selain itu, juga terdapat pilihan untuk menjalankan protokol ini otomatis saat server dijalankan sehingga tidak perlu mengaktifkan secara manual.

Pada pengujian ini, protokol yang diaktifkan hanya SMART dan SMB. Terlihat seperti pada gambar.



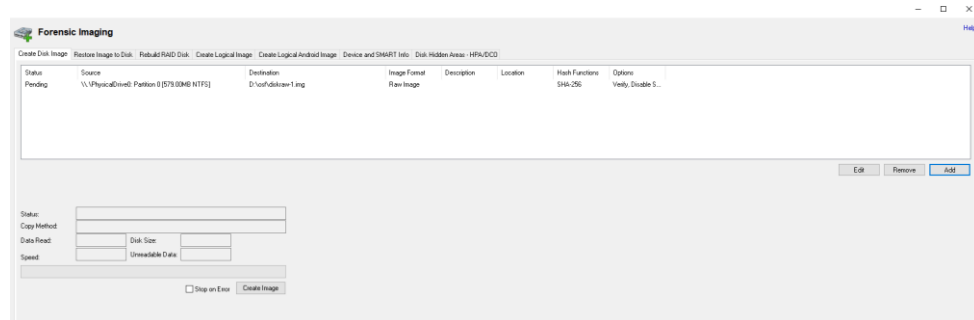
Gambar A. 28 Pengaturan protokol dan *auto starting* pada menu *services*

Setelah semua konfigurasi di atas selesai dilakukan, selanjutnya pada menu-menu berikutnya tidak ada konfigurasi lain yang dilakukan. Semua pengaturan yang ada mengikuti pengaturan *default* yang ada pada TrueNAS.

LAMPIRAN B

Proses Akuisisi dengan OSForensics

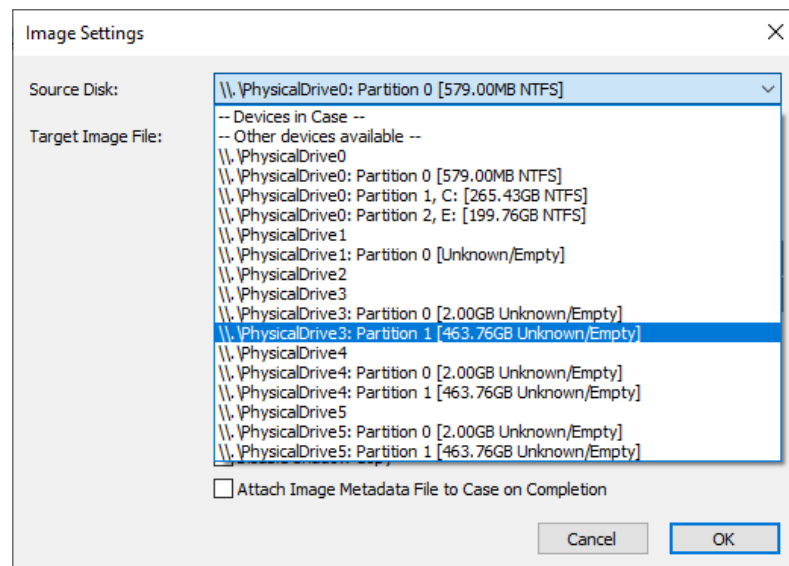
Tangkapan layar menu untuk melakukan proses *imaging* terlihat pada gambar berikut.



Gambar B. 1 Proses *disk drive imaging* pada OSForensics

Untuk menambahkan *disk drive* yang akan dilakukan proses *imaging* dengan menekan tombol *add* di sebelah kanan atas pada tampilan menu. Seperti terlihat pada gambar diatas.

Selanjutnya akan tampil jendela baru untuk memilih *disk drive* yang akan di proses, tentukan juga lokasi penyimpanan hasil imaging. Seperti terlihat pada gambar berikut.



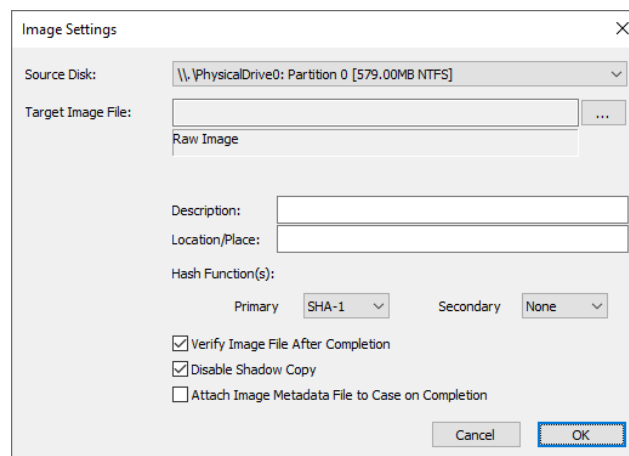
Gambar B. 2 Memilih *disk drive* yang akan di proses *imaging*

Tahapan proses selanjutnya yaitu proses *hashing*, terdapat pilihan untuk menentukan fungsi *hash*. Proses ini merupakan tahapan yang terdapat dalam panduan dan standar dalam melakukan akuisisi terhadap bukti digital. Pilihan metode yang tersedia pada aplikasi ini diantaranya, SHA1, MD5, CRC32 dan SHA256.

Pengujian ini menggunakan SHA256 untuk proses *hashing* terhadap file image yang sedang diakusisi. Penggunaan SHA256 ini karena menyesuaikan dengan aplikasi lain yang digunakan dalam pengujian ini yaitu menggunakan SHA256 sebagai metode *hashing* dan pengaturan ini tersedia secara default. Selain itu, OSForensics juga menyediakan fitur *note* untuk menambahkan deskripsi dari *file image* yang akan dibuat dan terdapat juga opsi untuk menambahkan lokasi kerja yang dapat diberikan sebagai detail pada proses akuisisi ini.

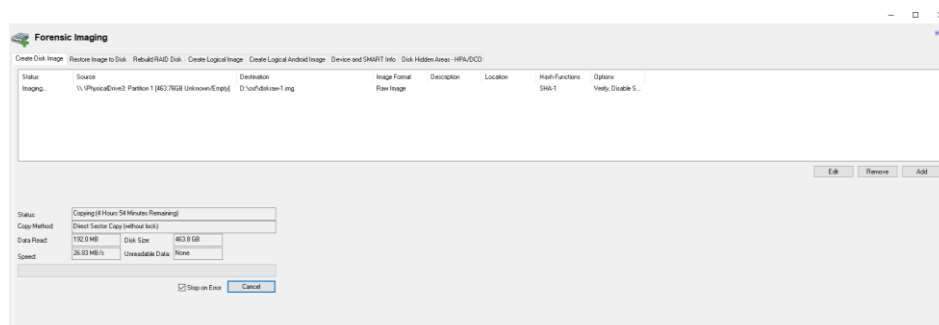
Secara default, verifikasi *file image* setelah proses *imaging* ini akan dilakukan oleh aplikasi, akan tetapi pilihan ini bisa dinonaktifkan sehingga hal tersebut berdampak pada waktu pelaksanaan proses *imaging* yang menjadi lebih cepat akan tetapi dengan konsekuensi hasil *imaging* tidak melalui proses verifikasi untuk mengetahui kualitas dari hasil proses *imaging* tersebut.

Tangkapan layar pada penambahan *disk drive* terlihat seperti gambar berikut.



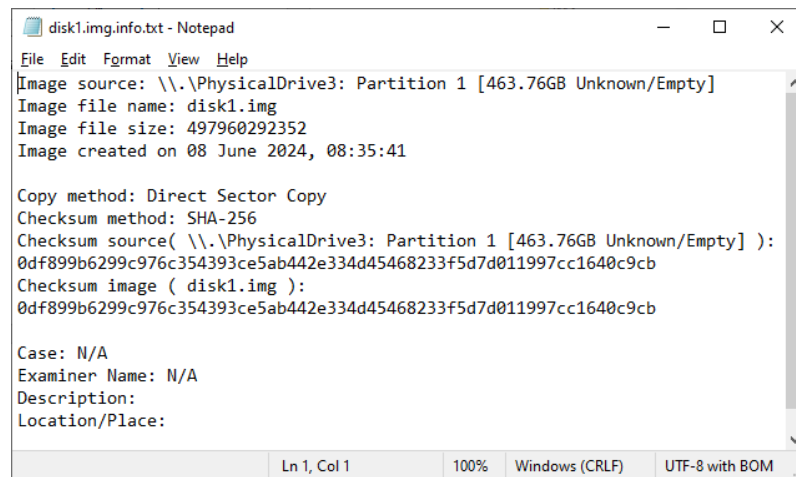
Gambar B. 3 Proses penambahan *disk drive* di OSForensics untuk *imaging*

Setelah semua pilihan telah ditentukan, tahapan *imaging* dapat dilakukan. Tombol create image pada tampilan akan memulai proses ini. Penelitian ini menggunakan *disk drive* dengan kapasitas 500 GB dengan estimasi waktu pekerjaan 5 jam. Terlihat seperti gambar berikut.



Gambar B. 4 Proses *imaging*

File *log* ini berisi informasi tentang detail *disk drive* yang diakuisisi, *checksum* dan catatan waktu. Terlihat seperti gambar berikut.

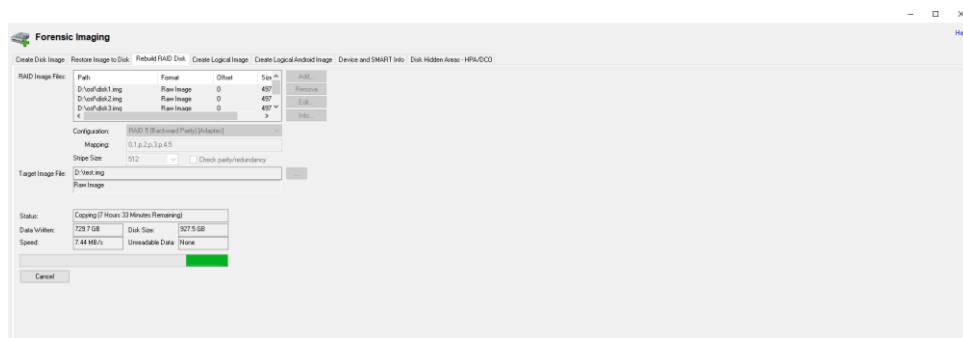


```
disk1.img.info.txt - Notepad
File Edit Format View Help
Image source: \\.\PhysicalDrive3: Partition 1 [463.76GB Unknown/Empty]
Image file name: disk1.img
Image file size: 497960292352
Image created on 08 June 2024, 08:35:41

Copy method: Direct Sector Copy
Checksum method: SHA-256
Checksum source( \\.\PhysicalDrive3: Partition 1 [463.76GB Unknown/Empty] ):
0df899b6299c976c354393ce5ab442e334d45468233f5d7d011997cc1640c9cb
Checksum image ( disk1.img ):
0df899b6299c976c354393ce5ab442e334d45468233f5d7d011997cc1640c9cb

Case: N/A
Examiner Name: N/A
Description:
Location/Place:
```

Gambar B. 5 File *log* hasil *imaging*



Gambar B. 6 Proses *imaging* dari *image* yang didapat dari tiap *disk* fisik

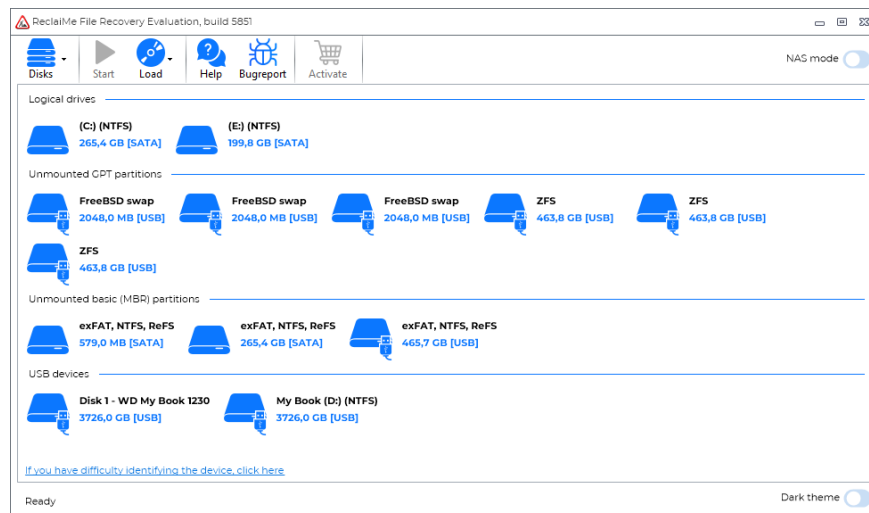
LAMPIRAN C

Proses Akuisisi dengan ReclaiMe

Aplikasi kedua yang digunakan pada pengujian ini adalah ReclaiMe. Versi yang digunakan pada penelitian ini adalah ReclaiMe File Recovery Evaluation, Build 5851.

Setelah file diunduh dan diinstall, kemudian jalankan aplikasi ReclaiMe. Pada saat pertama aplikasi ini dijalankan, mungkin tampilan pertama adalah mode *recovery* untuk NAS. Untuk mengganti mode ini, klik pada bagian kanan atas.

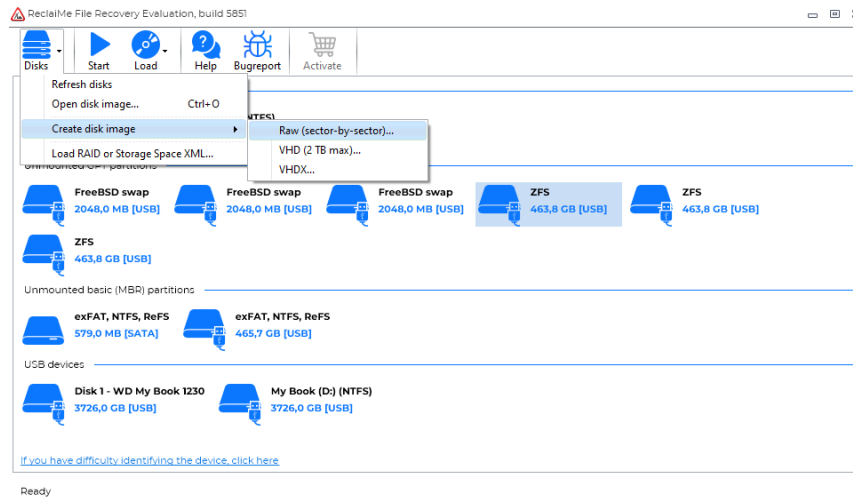
Untuk melakukan proses imaging, pertama yang perlu dilakukan adalah memilih *disk drive*. Jendela aplikasi ReclaiMe akan menampilkan seluruh *disk drive* yang terpasang pada komputer, pastikan pilihan *disk drive* yang akan di *imaging* sudah sesuai. Tangkapan layar terlihat seperti gambar berikut.



Gambar C. 1 Tampilan awal ReclaiMe File Recovery

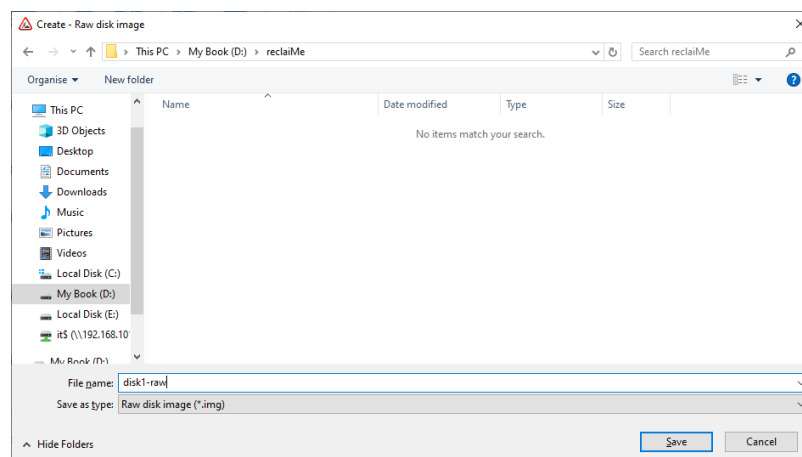
Setelah *disk drive* yang akan di proses telah dipilih, kemudian pada menu *Disk*, klik segitiga kecil di sebelah kanan. Menu tambahan akan keluar, kemudian arahkan atau klik *Create disk image* dan akan tampil menu tambahan. Terdapat 3 (tiga) pilihan yaitu *Raw* (*sector-by-sector*), ini digunakan untuk membuat file *image* dengan ekstensi seperti *img* atau *iso*, kemudian *VHD* (2TB mas), digunakan untuk membuat file *image* untuk mesin virtual dan *VHDX*, sama seperti *VHD*.

Penelitian ini menggunakan metode *Raw* untuk melakukan *imaging*, seperti terlihat pada gambar berikut.



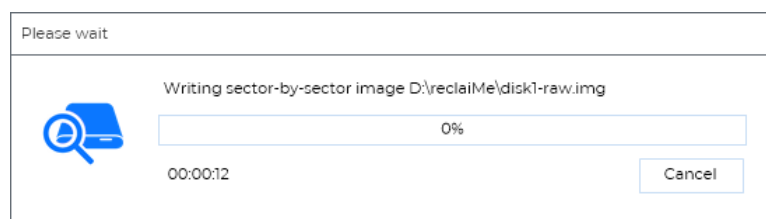
Gambar C. 2 Memilih tipe hasil imaging

Tentukan lokasi penyimpanan file hasil *imaging* dan berikan nama untuk file hasil *imaging*. Pada penelitian ini menggunakan penyimpanan eksternal dengan kapasitas 4 TB, seperti terlihat pada gambar berikut.



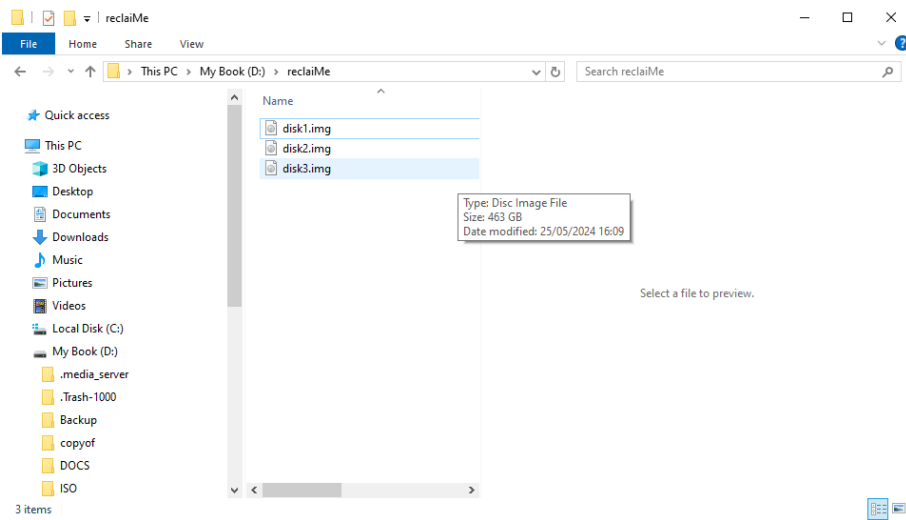
Gambar C. 3 menyimpan file hasil *imaging*

Tidak terdapat estimasi waktu selesai pekerjaan pada proses *imaging* dengan aplikasi ini. Waktu yang diperlukan dalam proses *imaging* pada penelitian ini membutuhkan 8 jam untuk tiap *disk drive*. Seperti terlihat pada gambar berikut.



Gambar C. 4 Proses imaging

Hasil pekerjaan akan tersimpan pada lokasi yang telah ditentukan dan ekstensi yang diperoleh pada proses ini adalah .img, seperti terlihat pada gambar berikut.



Gambar C. 5 Hasil imaging menggunakan ReclaiMe File Recovery

LAMPIRAN D

 FAKULTAS TEKNOLOGI INDUSTRI	ACTION PLAN Informatika Program Magister Forensika Digital	Doc No. 1/V/2024 Rev no. 1 Page 1 of 3
--	---	--

Lab pengujian Forensik

Metode Pengujian akuisisi sistem penyimpanan NAS

Jenis file Upload : docx, xlsx, csv, pdf, text, rar, cdr, image (jpeg, png)

Perangkat Akuisisi :

- ✓ OS Forensics, from Passmark (NIST list recommendation software)
- ✓ Reclaime, from ReclaiMe (data recovery professional software)

Tahapan kerja:

1. Buat NAS dengan 2 atau lebih hdd
2. Upload sejumlah file dengan 10 tipe ekstensi file yang berbeda kedalam NAS
3. Hapus masing masing 1 file ekstensi.
4. Lakukan akuisisi dengan OS Forensic (tool rekomendasi NIST).
5. Perhatikan apa saja yang didapat dari hasil akuisisi ?
6. Lakukan akuisisi dengan reclaime (tool professional enterprise).
7. Perhatikan apa saja yang didapat dari hasil akuisisi ?
8. lakukan eksaminasi singkat.

Pertanyaan wajib :

- ✓ Apakah akuisisi berhasil dilakukan
- ✓ Bagaimana dengan konsep chain of custody FD, apakah hasil yang didapatkan dari akuisisi memenuhi kriteria CoC
- ✓ Apakah file image dapat dilanjutkan ke proses CoC selanjut nya
- ✓ Apa rekomendasi hasil pengujian/penelitian tersebut

No	Tools	Success	Image extension	CoC Acquisitions		CoC Examination	Remarks
				Metadata/ Properties	Hash value		
1	OS Forensics	True/False	.img	Available/ NA	Available/ NA	True/False	
2	ReclaiMe	True/False	.img	Available/ NA	Available/ NA	True/False	nilai hash diambil menggunakan cmd.

Akuisisi Bukti Digital Pada Network Attached Storage (NAS) Menggunakan Metode National Institute of Standards and Technology

Gambar D. 1 Halaman 1 action plan

 FAKULTAS TEKNOLOGI INDUSTRI	ACTION PLAN Informatika Program Magister Forensika Digital	Doc No. 1/V/2024 Rev no. 1 Page 2 of 3
--	---	--

Tabel Perbandingan hasil pengujian:

No	Acquisition Tools	Acquisitions	Acquisition Time	Rebuilding Storage vs Time	Examinations Time	Remarks
1	OSF	Yes/No	5H/disk	7H 33M	3H	no Artefak
2	ReclaiMe	Yes/No	8H/disk	—	8H	all artefak

Log Activity

Starting Date : 4 Juni 2024
 End Date :

Disk Capacity : 128 GB
 Serial Number : 170876403046

No	Activity	Time	Status	Remarks
Disk 1				
1	Disk Drive Installation	9.25	Ok	
2	NAS Installation & Configuration	11.00	Ok	account, pool, share, RAID
3	Managing Files	14.20	Ok	
4	Uninstalling Disk Drive	14.25	Ok	
5	Disk Imaging Preparations			
6	Imaging RAID NAS Drive			
7	Collecting Information			
8	HASH Options			
9	Examinations			
10	Reporting Process			

Starting Date : 5 Juni 2024
 End Date : 20 Juni 2024

Disk Capacity : 500GB
 Serial Number : W2A6THJM

No	Activity	OS Forensics		ReclaiMe		Remarks
		Date	Time	Date	Time	
Disk 2						
1	Disk Drive Installation	5/6	—		9.25	
2	Managing Files	5/6	—		14.10	
3	Uninstalling Disk Drive	5/6	—		14.25	
4	Disk Imaging Preparations	6/6	10.00	14/6	8.30	
5	Imaging RAID NAS Drive	6/6	12.00	14/6	9.30	
6	Collecting Information					
7	HASH Options	8/6	10.00	16/6	9.30	RM → hash using cmd.
8	Examinations	19/6	—		8.00	ReclaiMe only
9	Reporting Process	20/6	—		8.00	

Akuisisi Bukti Digital Pada Network Attached Storage (NAS) Menggunakan Metode National Institute of Standards and Technology

Gambar D. 2 Halaman 2 action plan

 FAKULTAS TEKNOLOGI INDUSTRI	ACTION PLAN Informatika Program Magister Forensika Digital	Doc No. 1/V/2024 Rev no. 1 Page 3 of 3
--	---	--

Log Activity

Starting Date : 5 Juni 2024
End Date : 20 Juni 2024

Disk Capacity : 500GB
Serial Number : 6VMC393C

No	Activity	OS Forensics		ReclaiMe		Remarks
		Date	Time	Date	Time	
Disk 2						
1	Disk Drive Installation	5/6	—	9.25		
2	Managing Files	5/6	—	14.10		
3	Uninstalling Disk Drive	5/6	—	14.25		
4	Disk Imaging Preparations	6/6	10.00	16/6	8.30	
5	Imaging RAID NAS Drive	6/6	17.00	16/6	9.00	
6	Collecting Information					
7	HASH Options	8/6	10.00	17/6	9.30	RM - Hash value using cmd.
8	Examinations	19/6	—	8.00		ReclaiMe only
9	Reporting Process	20/6	—	8.00		

Starting Date : 5 Juni 2024
End Date : 20 Juni 2024

Disk Capacity : 500GB
Serial Number : 5VM1J9K

No	Activity	OS Forensics		ReclaiMe		Remarks
		Date	Time	Date	Time	
Disk 2						
1	Disk Drive Installation	5/6	—		9.25	
2	Managing Files	5/6	—		14.10	
3	Uninstalling Disk Drive	5/6	—		14.25	
4	Disk Imaging Preparations	6/6	10.00	17/6	8.30	
5	Imaging RAID NAS Drive	7/6	00.00	17/6	9.00	
6	Collecting Information					
7	HASH Options	8/6	10.00	18/6	8.00	RM - hash using cmd.
8	Examinations	19/6	—		8.00	using Reclai Me
9	Reporting Process	20/6	—		8.00	

Notes : Imaging untuk ketiga disk drive yang telah di imaging sebelumnya, dilakukan pada tanggal 18 juni 2024, pukul 8-20 Total kapasitas image sebesar 729.7 GB dengan durasi waktu proses selama 7 jam 33 menit (ETA).

Akuisisi Bukti Digital Pada Network Attached Storage (NAS) Menggunakan Metode National Institute of Standards and Technology

Gambar D. 3 Halaman 3 action plan