E-ISSN : 2988-1986
https://ejournal.warunayama.org/kohesi

Kohesi: Jurnal Multidisiplin Saintek
Volume 6 No 2 Tahun 2024

ANALYSIS INVESTIGASI FORENSIK *OPTICAL DISC* MENGGUNAKAN STANDAR NIST (*NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY*)

Fajar Mayda Salam[1], Bashor Fauzan Muthohirin[2], Zamah Sari[3]
[1,2,3]Teknik Informatika, Universitas Muhammadiyah Malang, Jalan Raya Tlogomas No 246, Kec. Lowokwaru, Kota Malang, Negara Indonesia
[1]fajarmayda14@gmail.com, [2]bashorfauzan@umm.ac.id, [3]zamahsari@umm.ac.id

Abstract

Digital forensic investigation is a crucial process in collecting, analyzing, and presenting digital evidence that can be used in law enforcement. One type of storage media that is often used as an object of investigation is optical drives, such as CDs, DVDs, and Blu-rays. This study discusses the application of the National Institute of Standards and Technology (NIST) standard method in the forensic analysis of optical drives. The methodology used includes the stages of identification, acquisition, analysis, and reporting, all of which are in accordance with NIST guidelines. Through the application of the NIST method, this study highlights the reliability and accuracy of the procedure in ensuring the integrity of digital evidence from optical drives. This study also discusses challenges that are often faced in the forensic process, such as physical damage to the media and data encryption. The results of the study show that a systematic approach based on NIST standards can improve the accuracy and validity of the investigation results. Thus, the application of this standard is very important to support the credibility of digital evidence in court.

Keywords: *Digital Forensics, Optical drive, NIST, Evidence Investigation*

Abstrak

Investigasi forensik digital merupakan proses krusial dalam pengumpulan, analisis, dan penyajian bukti digital yang dapat digunakan dalam penegakan hukum. Salah satu jenis media penyimpanan yang sering dijadikan objek investigasi adalah *optical drive*, seperti CD, DVD, dan *Blu-ray*. Penelitian ini membahas penerapan metode standar *National Institute of Standards and Technology* (NIST) dalam analisis forensik *optical drive*. Metodologi yang digunakan mencakup tahapan identifikasi, akuisisi, analisis, dan pelaporan, yang semuanya sesuai dengan pedoman NIST. Melalui penerapan metode NIST, penelitian ini menyoroti keandalan dan ketepatan prosedur dalam memastikan integritas bukti digital dari *optical drive*. Studi ini juga membahas tantangan yang sering dihadapi dalam proses forensik, seperti kerusakan fisik media dan enkripsi data. Hasil penelitian menunjukkan bahwa

Article History
Received: December 2024
Reviewed: December 2024
Published: December 2024

Plagirism Checker No 234
Prefix DOI :
10.8734/Kohesi.v1i2.365

pendekatan sistematis berdasarkan standar NIST mampu meningkatkan akurasi dan validitas hasil investigasi. Dengan demikian, penerapan standar ini sangat penting untuk mendukung kredibilitas bukti digital di pengadilan.
Kata Kunci: Forensik Digital, *Optical drive*, NIST, Investigasi Bukti

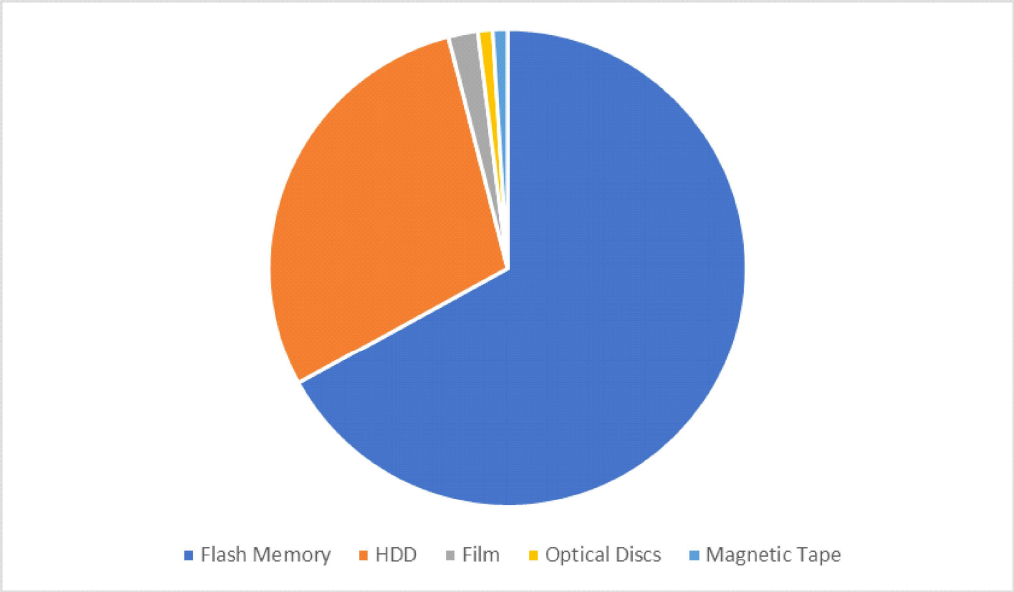
1. PENDAHULUAN

Di era digital saat ini, kejahatan *cyber* menjadi salah satu ancaman besar terhadap keamanan data dan informasi. Kejahatan termasuk pencurian data, penyebaran *malware* dan *hacking.* Untuk mengatasi ancaman ini forensik sangat penting dalam investigasi hukum. Tujuan utama dari analisis forensik adalah untuk mengidentifikasi semua peristiwa, mengetahui efek pada sistem, dan mendapatkan bukti yang diperlukan, untuk mencegah insiden dimasa mendatang dengan mendeteksi teknik berbahaya yang digunakan. Digital forensik adalah ilmu dan teknologi komputer serta metode ilmiah untuk membuktikan kejahatan digital melalui jaringan komputer, yang membantu merekonstruksi peristiwa kriminal dan mencegah tindakan tidak sah yang mengganggu operasi.[1]. Forensik digital didefinisikan sebagai "pengetahuan yang ilmiah dan metode diterapkan untuk *identifiaxtion, collection, preservation, examination, dan analysis* bukti digital dengan cara yang dapat diterima oleh masalah hukum" [2]. Selain itu, diperlukan metode implementasi analisis menggunakan standar NIST yang memerlukan keahlian khusus, alat yang sesuai, mudah diakses, sehingga tidak menjadi hambatan dalam penyelidikan.

Teknik Forensik ada dua yaitu NIST dan NIJ. Metode forensik NIST menyediakan panduan dan standar untuk pengumpulan, pemeriksaan, analisis, dan pelaporan bukti digital, dengan fokus pada menjaga integritas data dan proses yang sistematis [4]. Metode forensik NIJ mengembangkan standar dan pedoman untuk investigasi forensik digital dengan penekanan pada aplikasi praktis dan kebutuhan penegakan hukum di lapangan [15]. Perbedaan nya NIST lebih fokus pada pengembangan standar teknis dan prosedural untuk integritas data secara umum, sementara NIJ lebih menekankan aplikasi praktis dan kebutuhan operasional dalam konteks penegakan hukum.

Bukti Digital adalah informasi yang rapuh, *volatile*, dan rentan jika tidak ditangani dengan benar [4]. Bukti digital sangat penting dalam semua kejahatan, untuk menghindari hal itu maka diperlukan seperti menjaga perangkat dalam mode isolasi. Tujuannya adalah untuk menghindari data dari terhapus dan berubah dengan kondisi apa pun. Bukti digital dapat ditemukan di perangkat *hard drive*, *flash drive* dan perangkat seluler [5].

Optical disc merupakan salah satu jenis perangkat penyimpanan sekunder dengan keunggulan signifikan dibandingkan media magnetik, seperti kapasitas penyimpanan yang lebih tinggi dan biaya yang lebih rendah [6]. Permukaan kosong dapat menampung data dengan kapasitas tertentu seperti video, aplikasi, multimedia, permainan dan audio dengan cara di-*burning*. Gambar 1 menampilkan *optical disc* mendapatkan nilai 1% dari beberapa media penyimpanan yang sering digunakan pada tahun 2019.



Gambar 1. Diagram Perkembangan Penggunaan *Storage* [8]

Dalam Penelitian ini akan dilakukan analisis pada data terhapus pada sebuah DVD-R dengan tiga *tool forensic*, yaitu FTK *Imager*, *Autopsy*, dan *ProDiscover basic*. Serta memilih Metode NIST agar memastikan bahwa setiap langkap dalam investigasi forensik sesuai dengan standar NIST. Dengan kelebihan NIST (*National Institute of Standards and Technology*) yang menyediakan pedoman yang rinci, evaluasi yang akurat dan konsisten serta metode ini bersifat modular sehingga dapat disesuaikan dengan berbagai aplikasi dan kebutuhan yang memungkinkan fleksibilitas dalam implementasinya

2. TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

Acuan penelitian terdahulu yang dikutip pada penelitian ini memiliki beberapa kesamaan diantaranya pada objek yang penelitian, metode dan *tools* yang digunakan seperti pada Tabel 1.

Tabel 1. Rangkuman Hasil Penelitian Terdahulu

Penulis dan Tahun	Judul Penelitian	Hasil Penelitian
Muhammad Immawan Aulia, Imam Riadi, Abdul Fadlil (2019),	*Storage Forensic Optical drive* Menggunakan Metode Statik [14]	*Tools* FTK *Imager* berhasil menemukan *unllocated space* pada sebuah DVD yang sudah terformat
Imam Riadi, Abdul Fadlil, Muhammad Immawan Aulia (2019)	*Review* Proses Forensik *Optical drive* Menggunakan Metode *National Institute of Justice* (NIJ) [15]	Tingkat keberhasilan *tools Autopsy* 100% dengan ekstensi *file* yang berhasil direstorasi yaitu Pdf, Docx, Pptx, Txt, MP3, Iso, JPG dan PNG dengan jumlah keseluruhan 29 *file*.

Mustafa Mustafa, Imam Riadi, Rusydi Umar (2019)	Rancangan Investigasi Forensik Email Dengan Metode *National Institute of Standards and Technology* (NIST) [16]	*Header Analysis* menghasilkan pola pemalsuan email yang berupa subjek, alamat dan tanggal email yang palsu. Selain itu investigasi email forensik ini juga menghasilkan: Alamat email pengirim email palsu, memeriksa protokol inisiasi pesan (HTTP, SMTP), memeriksa ID pesan dan alamat IP pengirim.
Vindy Arista Yuliani, Imam Riadi (2019)	*Forensic Analysis WhatsApp Mobile Application on Android-Based Smartphones Using National Institute of Standard and Technology (NIST) Framework* [17]	Bukti digital yang ditemukan pada aplikasi *Whatsapp* menggunakan *tools Oxygen Forensic* dan *Andriller* untuk membuka enkripsi database crypt12 dan mendapatkan bukti artefak berupa eksplorasi laporan data *smartphone* seperti sesi *chat*, *avatar*, kontak pada aplikasi *whatsapp*, status di *whatsapp*, serta mendapatkan *file* media *whatsapp* dan backup database terenkripsi.
Bandr Siraj Fakiha(2022)	*Cybersecurity: Analysis and Application of ProDiscover Forensic Toolkit* [18]	*ProDiscover Forensic tool* menghasilkan bukti digital dengan cara tidak merusak, melakukan analisis mendalam dalam system. *Tool* ini juga membantu dan melacak aktivitas pengguna dan menganalisa serangan *cyber* seperti infeksi *malware* dan pelanggaran data.

2.2. Teknik Forensik Digital

Menurut *National Institute of Standards and Technology* (NIST), forensik digital adalah "aplikasi metode ilmiah dalam proses pengumpulan, penyimpanan, pemeriksaan, dan analisis bukti digital untuk tujuan hukum." Teknik forensik digital melibatkan beberapa tahap utama yang umumnya diikuti dalam sebuah investigasi:

- Pengumpulan Data (*Collection*): Pada tahap ini, data dari perangkat atau media penyimpanan yang relevan dengan kasus dikumpulkan. Teknik yang digunakan mencakup pembuatan salinan forensik (*forensic image*).
- Pemeriksaan (*Examination*): Fase pemeriksaan melibatkan pengolahan data yang telah dikumpulkan menggunakan teknik manual dan otomatis untuk mengidentifikasi bukti yang relevan. Pemeriksaan ini mencakup pencarian kata kunci, rekonstruksi *timeline* aktivitas,
- Analisis (*Analysis*): Tahap ini melibatkan interpretasi data yang diperoleh selama pemeriksaan. Analisis bertujuan untuk menghubungkan bukti digital dengan aktivitas tertentu. Teknik analisis dapat mencakup analisis log sistem, analisis jaringan, dan analisis jejak digital. Pada tahap ini, metode NIST memberikan panduan tentang bagaimana menjaga integritas bukti selama analisis.
- Presentasi (*Presentation*): Tahap akhir dalam teknik forensik digital adalah penyajian bukti kepada pihak yang berwenang, seperti pengadilan. Bukti harus disajikan secara jelas dan dapat dipahami oleh orang yang tidak memiliki latar belakang teknis, dan harus memenuhi standar hukum agar dapat diterima di pengadilan.

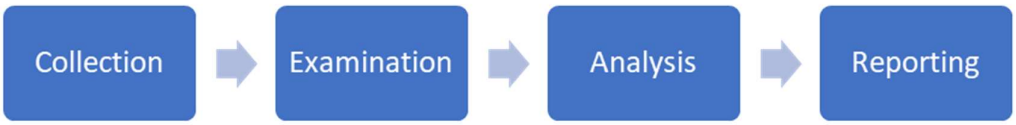
2.3. *Optical disc*

Optical disc adalah media penyimpanan data yang menggunakan cahaya laser untuk membaca dan menulis data. Sejak diperkenalkan pada akhir abad ke-20, *optical disc* telah menjadi salah satu format penyimpanan data yang paling populer, terutama untuk distribusi perangkat lunak, media hiburan, dan penyimpanan data cadangan. *Optical disc* terdiri dari beberapa jenis, masing-masing dengan karakteristik dan kapasitas penyimpanan yang berbeda:

- *Compact Disc* (CD): CD adalah salah satu jenis *optical disc* yang paling awal dan paling banyak digunakan. CD memiliki kapasitas penyimpanan sekitar 700 MB dan digunakan untuk penyimpanan audio, data, dan perangkat lunak.
- *Digital Versatile Disc* (DVD): DVD menawarkan kapasitas penyimpanan yang lebih besar dibandingkan CD, yaitu sekitar 4.7 GB untuk DVD *single-layer* dan 8.5 GB untuk DVD *dual-layer*. DVD banyak digunakan untuk penyimpanan video, terutama dalam distribusi film, serta data dan perangkat lunak.
- *Blu-ray Disc* (BD): *Blu-ray* adalah evolusi dari DVD yang menawarkan kapasitas penyimpanan hingga 25 GB untuk *single-layer* dan 50 GB untuk *dual-layer*. *Blu-ray* digunakan terutama untuk distribusi film dalam format HD dan 4K, serta untuk penyimpanan data berukuran besar.
- HD DVD: HD DVD adalah format yang bersaing dengan *Blu-ray* namun kalah dalam perang format dan tidak lagi digunakan secara luas. Kapasitas penyimpanannya mirip dengan *Blu-ray*, tetapi adopsi pasar yang lebih rendah menyebabkan HD DVD ditinggalkan.

3. METODOLOGI

National Institute of Standards and Technology (NIST) adalah lembaga yang menyediakan pedoman dan standar untuk berbagai disiplin ilmu, termasuk forensik digital. Implementasi metode yang sesuai prosedur dalam memperoleh bukti digital berupa data forensik akan memberikan dampak keberhasilan hingga 100% [19]. Metodologi NIST melibatkan serangkaian prosedur yang mencakup tahap identifikasi, akuisisi, analisis, dan pelaporan bukti digital [20]. Dengan fokus pada menjaga integritas data melalui teknik seperti *hashing* dan dokumentasi yang ketat. Tahapan NIST seperti gambar 2.



Gambar 2. Alur Proses Pada Metode NIST

Penjelasan tahapan dan proses-proses pada metode NIST sebagai berikut:

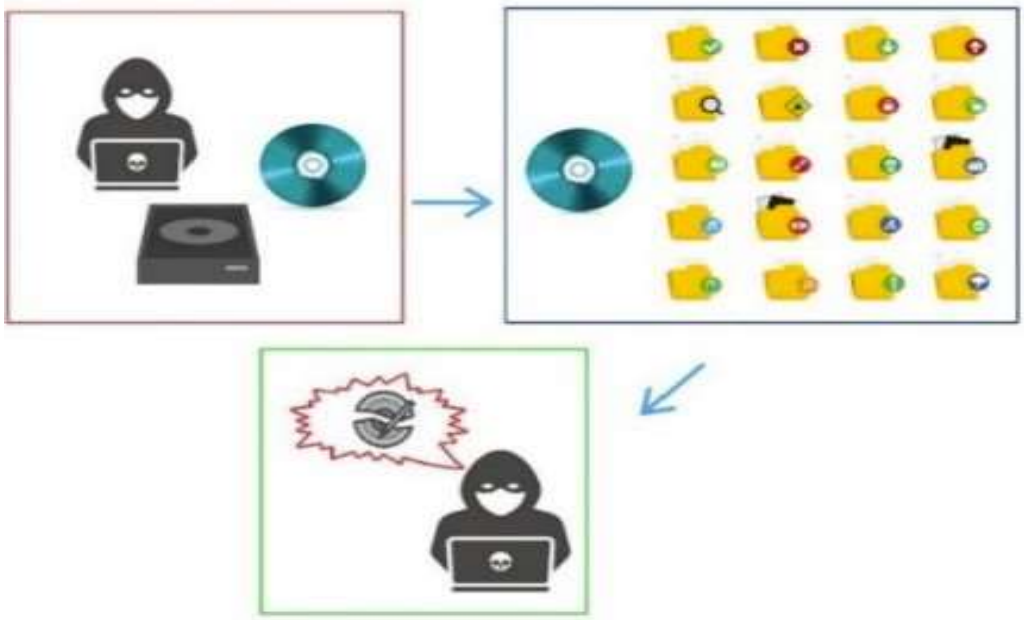
A. *Collection*: Fase pertama dalam proses ini adalah untuk mengidentifikasi, memberi *table*, dan memperoleh data dari sumber data yang terkait, serta mengikuti pedoman dan prosedur yang menjaga keamanan data. Untuk keamanan data yang dikumpulkan, penting untuk mengikuti salah satu pedoman yang sering digunakan yaitu metode NIST (*National Institute of Standards and Technology*). Metode ini memberikan standar dan praktik terbaik dalam pengumpulan bukti digital, memastikan bahwa data yang diperoleh tetap lengkap dan dapat diandalkan di sepanjang proses investigasi. Selain itu, alat-alat seperti FTK *Imager*, *Autopsy*, dan *ProDiscover Basic* digunakan untuk membantu dalam proses pengumpulan dan analisis data secara forensik.
B. *Examination*: Fase kedua yang melakukan pemeriksaan melibatkan proses forensik dalam jumlah besar data yang diproses dengan menggunakan kombinasi metode otomatis dan manual untuk menilai dan mengekstraksi data yang terkait menggunakan perangkat seperti FTK *Imager*, *Autopsy* dan *ProDiscover*, sambil menjaga integritas data. Metode NIST menjadi acuan utama pada tahap ini karena memberikan panduan bagaimana integritas data selama pemeriksaan dan hasil yang dipercaya. Peran dari alat forensik seperti FTK *Imager*, *Autopsy* dan *ProDiscover* ialah:
    1. FTK *Imager* (*Forensic tool*) digunakan untuk melakukan analisis mendalam terhadap data yang telah dikumpulkan. FTK *Imager* memungkinkan peneliti untuk memproses data secara cepat dan efisien, serta mengekstrak informasi yang terhapus
    2. *Autopsy* berperan sebagai platform analisis forensik yang *user-friendly*, memungkinkan peneliti untuk menelusuri data yang dikumpulkan dan mengekstrak informasi relevan dengan menggunakan berbagai *plugin* dan alat bawaan. *Autopsy* juga mendukung sistem *file* dan format data yang bermacam-macam
    3. *ProDiscover* adalah alat lain yang digunakan dalam fase ini untuk mengekstrak bukti digital dari berbagai perangkat. Alat ini sangat berguna untuk analisis mendalam terhadap *file* sistem dan *metadata*, serta untuk memastikan bahwa tidak ada data penting yang terlewatkan.

C. *Analysis*: Menganalisa data yang telah diperiksa di tahap sebelumnya, untuk mendapatkan informasi yang dapat digunakan dalam konteks hukum. Pada tahap ini, peneliti menggunakan berbagai metode dan teknik yang diakui secara hukum untuk menafsirkan data yang telah diekstraksi, mengidentifikasi pola, mengungkap hubungan kejadian. Dengan metode NIST menyediakan panduan tentang bagaimana proses analisis harus dilakukan, termasuk bagaimana menjaga integritas bukti, mendokumentasikan setiap langkah yang diambil, dan memastikan bahwa hasil yang diperoleh dapat diandalkan dan dipertanggungjawabkan di pengadilan. Dalam fase analisis ini alat-alat forensik digital seperti FTK *Imager*, *Autopsy* dan *ProDiscover* basic berfungsi:
   1. FTK *Imager* (*Forensic Toolkit*): Menyediakan berbagai alat analisis yang memungkinkan peneliti untuk mengidentifikasi dan menghubungkan bukti digital dengan cepat. FTK *Imager* memiliki kemampuan untuk menganalisis berbagai jenis data, termasuk ppt, gambar, dan *file* yang terhapus, serta dapat membuat indeks yang mempermudah pencarian informasi spesifik.
   2. *Autopsy*: Memfasilitasi analisis forensik dengan antarmuka yang mudah digunakan dan berbagai fitur analisis yang kuat. *Autopsy* memungkinkan peneliti untuk mengekstraksi dan menafsirkan informasi seperti aktivitas pengguna.
   3. *ProDiscover*: Digunakan untuk melakukan analisis mendalam terhadap struktur *file* dan *metadata*, memberikan wawasan tentang bagaimana dan kapan data dibuat, dimodifikasi, atau diakses. Alat ini juga dapat digunakan untuk mengidentifikasi anomali atau pola yang mungkin menunjukkan aktivitas ilegal atau mencurigakan.

D. *Reporting*: Pelaporan hasil analisis, yang dapat mencakup dan menggambarkan tindakan yang digunakan, menjelaskan bagaimana alat dan prosedur, menentukan tindakan yang perlu (misalnya, melakukan pemeriksaan forensik data tambahan, meningkatkan kontrol keamanan yang ada), dan memberi rekomendasi, pedoman, perbaikan kebijakan, dll. Dengan memasukkan metode NIST dalam pelaporan, laporan tidak hanya mencakup analisis yang mendalam tetapi juga memberikan panduan yang berstandar untuk tindakan selanjutnya, membantu organisasi dalam menjaga dan meningkatkan keamanan mereka secara berkelanjutan.

3.1 Skenario Kasus

Gambar 3 menampilkan kasus yang merupakan sebuah simulasi dimana *optical drive* dengan jenis *read only* dapat dihapus karena di-*burning* dengan fitur *multisession*. Teknik penghapusan menggunakan fitur format pada Windows. Skenario kasus dimulai pada kotak merah tersangka melakukan *burning* data pada penelitian dengan menggunakan fitur *multisession* menggunakan aplikasi *burner* seperti contoh nya *Nero*, setelah selesai DVD-R sudah berisikan data seperti pada kotak biru, kemudian pada kotak hijau pelaku mencoba menghapus data yang ada pada DVD-R menggunakan fitur format bawaan sistem operasi *windows* 10. Data optikal *drive* berasal dari simulasi data kejahatan yang disediakan oleh peneliti, sehingga penting untuk memastikan bahwa semua langkah dalam pengambilan dan penanganan dilakukan secara hati-hati untuk menjaga integritas dan validitas bukti yang diperoleh.



Gambar 3. Skenario Kasus Kejahatan digital penggelapan dana perusahaan A

Pada gambar 3, "Seorang akuntan bernama Bagus melakukan penggelapan dana perusahaan A, bukti penggelapan dana tersebut disalin di sebuah DVD-R menggunakan fitur *multisession*. Kemudian Rio menghapus bukti yang ada pada DVD-R untuk menghilangkan bukti digital tersebut. *Investigator* menemukan sebuah DVD-R pada tempat kejadian perkara yang diindikasi sebagai bukti fisik dari kasus tersebut".

3.2 Alat untuk kebutuhan melakukan forensik

Alat yang digunakan pada penelitian dapat dilihat pada Tabel 2.

Tabel 2. Alat kebutuhan *forensic* dibawah ini

NO	Nama Alat	Spesifikasi	Keterangan
1	Laptop	*Legion* 5, 16 GB, 500 GB SSD	*Hardware*
2	Sistem Operasi	Windows 10	*Software*
3	DVD-R	DVD-R *Datemate* 4 GB	*Hardware*
4	DVD *Writer* eksternal	*Lite on*	Hardware
5	FTK *Imager*	*Ver*. 3.1.3	*Tool* akuisisi
6	*Autopsy*	*Ver* 4.10.0	*Tool* akuisisi
7	*ProDiscover Basic*	*Ver* 3.1.0	*Tool* akuisisi
8	*Microsoft office*	-	Alat untuk mengetik laporan

4. HASIL DAN PEMBAHASAN

Implementasi metode

Penelitian ini menggunakan skenario kasus dengan kondisi tertentu dimana membandingkan *tools* yang akan di akuisisi data pada *optical disc* yaitu DVD-R yang sudah diformat. Pada bagian ini akan menjelaskan implementasi metode yaitu *National Institute of Standard Technology* (NIST) yang meliputi, *Collection, Examination, Analysis, dan Reporting*. Dibawah ini akan dijelaskan bukti digital pada di DVD-R Pada tabel 2.

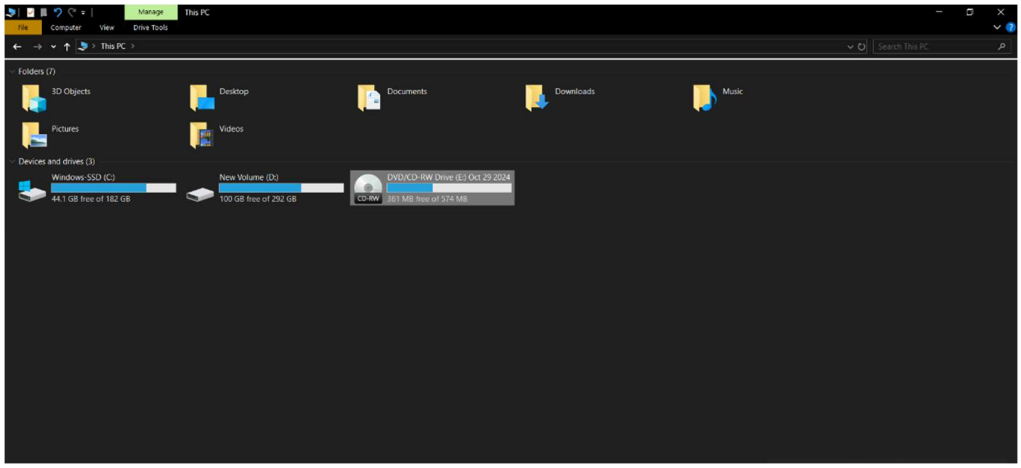
Tabel 3. Bukti Digital pada DVD-R

NO	Nama dan Ekstensi	*Hash*
1	archive.zip	a6903046ec2479db908804c870c4c00b
2	HARGA RUMAH JAKSEL.xlsx	607096e1d5db1d549bfc358c82bfdecd
3	*How to Cover Up a Murder in 24 Hours*.mp4	69ad4b7293a62c47e1530490539541fd
4	*How To Hide Stuff from The Police* (r_AskReddit).mp4	7d8b5593ba583db157b36b8f9427c5e3
5	*images* (1).jfif	3cdf89c2ba7aa3780e6b3440eb1ac40f
6	*images* (2).jfif	29cfbbe91efedf267b01e1e8bf7642a5
7	*images* (3).jfif	2423c7c87edae2050316124d6d4d86d5
8	*images* (4).jfif	192118c73606df4f3fbc5c5d0d4969b5
9	*images*.jfif	6dc0d7c3485e393d8d92af2d48d9383f
10	jurnal rumah.docx	a7ccf64f1acc430031cc98872d98881d
11	membuat Kampak dari disk cakram.mp4	38ae26be312ad7203edacf31bcd85136
12	*repair*.rar	1e00b0ca3f276d95a67e48d371849f9d
13	*Screenshot* (60).png	72f326471a2c83af56dda4abf3b68fb4
14	setup_mobileditphonemanager_10.8.0.29556_win32.exe	d4068b0e0bf624951811bc312308e3c2
15	*videoplayback*.mp3	c950ffd4b228ae59351f8f9dbd271130
16	*videoplayback2*.mp4	ec4088338878a449bd813d9316fc7e3e

Penjelasan implementasi metode sebagai berikut:

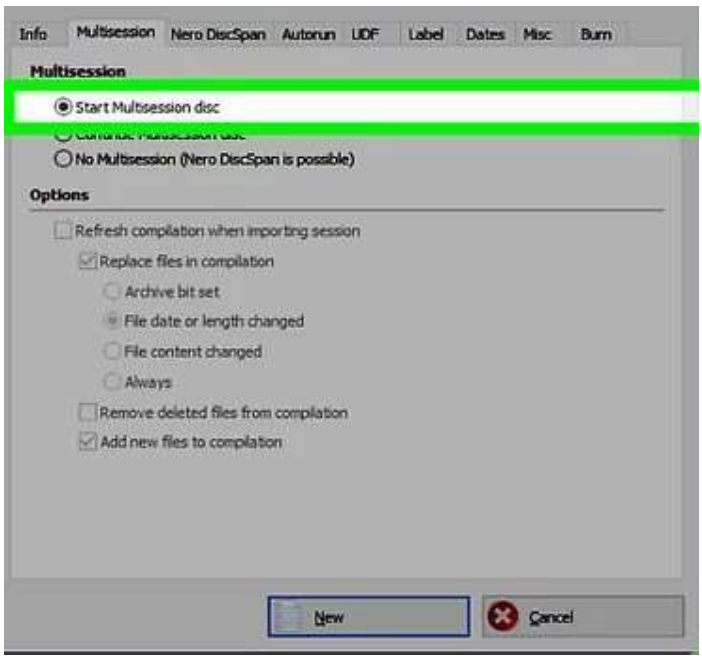
Gambar 4. Proses Tahapan Koleksi Data

A. *Collection*: Proses tahapan berdasarkan Gambar 4 yakni menggambarkan langkah-langkah untuk pengumpulan data yang akan dijadikan barang bukti digital pada DVD-R, yang terdiri dari berbagai *file* dengan beragam ekstensi dan kapasitas. Berbagai *file* dengan beragam ekstensi dan kapasitas format *file* ini memungkinkan untuk mempercepat proses akuisisi data, sehingga tahapan pemeriksaan (*examination*) bisa dilakukan dengan lebih efisien dan cepat. Tahapan ini penting karena dalam forensik digital, di mana data digital harus disimpan dengan benar dan aman untuk kebutuhan pembuktian di kemudian hari.



Gambar 5. Kapasitas DVD-RW

Selanjutnya, pada Gambar 5, terlihat kapasitas DVD-R setelah proses *burning* selesai dilakukan. Kapasitas ini menunjukan sisa ruang yang masih tersedia atau yang terpakai. Aplikasi yang digunakan untuk proses *burning* data ke DVD-R adalah *Nero Starsmart*, sebuah perangkat lunak popular yang sering digunakan untuk keperluan burning CD atau DVD. Proses ini memastikan bahwa data disimpan dengan cara yang benar dan terstruktur, sehingga dapat diakses dan di proses lebih lanjut dalam penyelidikan.

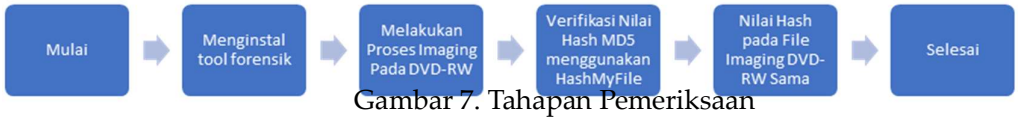


Gambar 6. fitur multisession pada DVD-RW

Gambar 6 menunjukan fitur *multisession* pada DVD-R, Dimana fitur ini memungkinkan pengguna untuk menambahkan atau menghapus data dari DVD-R setelah proses *burning* pertama selesai. Dalam beberapa kasus, pengguna dapat melakukan proses penghapusan manual terhadap data yang ada, setelah itu kapasitas sisa pada DVD-R dapat digunakan untuk menambahkan *file* lain hingga media penyimpanan tersebut benar-benar penuh. Ini memberikan fleksibilitas dalam penggunaan DVD-R

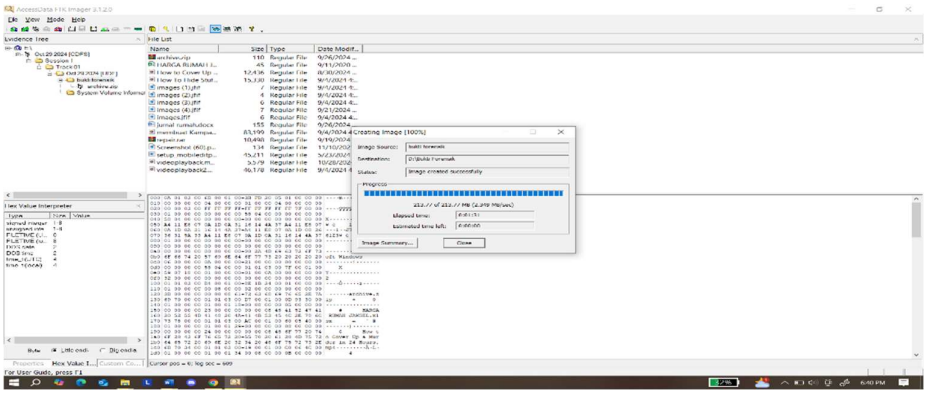
sebagai media penyimpanan data digital, memungkinkan penggunaan berkelanjutan tanpa harus menggunakan DVD-R baru untuk setiap sesi data yang berbeda. Fitur ini sangat berguna dalam situasi dimana penyimpanan data besar diperlukan namun secara bertahap. Keseluruhan proses dari pengumpulan hingga penyimpanan data pada DVD-R yang dijelaskan dalam gambar-gambar tersebut memperlihatkan langkah-langkah yang terstruktur dan efisien dalam mendukung kegiatan akuisisi data digital, terutama dalam konteks digital forensik dan pengolahan barang bukti elektronik.

B. *Examination:* Tahapan pemeriksaan ini dilakukan untuk mengetahui bahwa hasil image *file* DVD-R dibuat menggunakan *tools* forensik FTK *Imager* dan kloningnya memiliki nilai *hash* yang sama, validasinya menggunakan pencocokan nilai *hash* menggunakan aplikasi *HashMyFile* dan FTK *Imager*. Alur proses dapat dilihat pada Gambar 7.



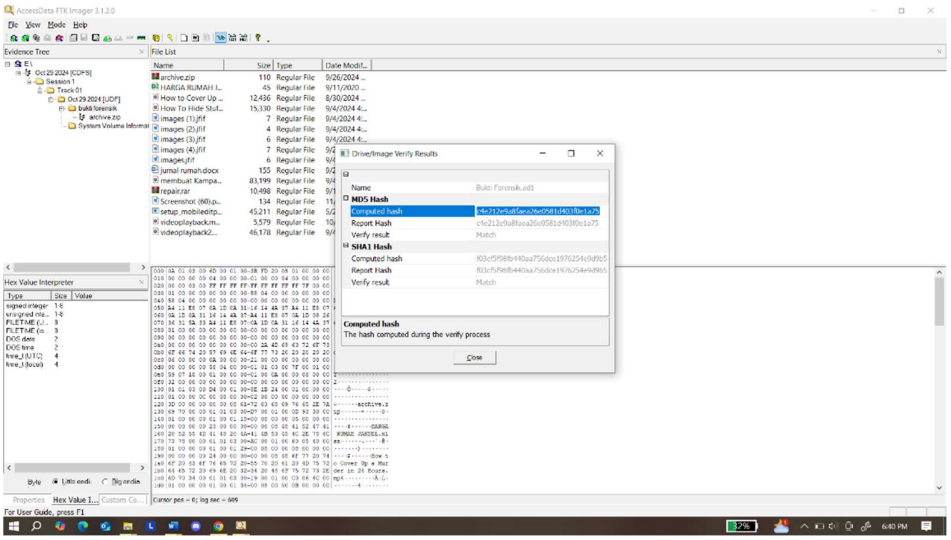
Gambar 7. Tahapan Pemeriksaan

Proses *imaging* dilakukan untuk membuat salinan data sebagai bukti digital dari DVD-RW yang ditemukan di lokasi kejadian kejahatan digital, seperti yang terlihat pada Gambar 8.



Gambar 8. Proses *Imaging* Pada DVD-RW

Setelah proses *imaging* selesai, nilai *hash* dari hasil image disk dapat digunakan sebagai acuan untuk memastikan keaslian data. Nilai *hash* ini dibandingkan dengan salinan *image disk* untuk memverifikasi keaslian sumber data, dengan tujuan menjaga integritas data dan mencegah perubahan secara fisik maupun digital. Gambar 9 menunjukkan nilai *hash* pada *tools* FTK *Imager*. Hasil yang ditunjukkan pada Gambar 9 menunjukkan nilai *hash* yang sama, sehingga *file image* DVD-RW_1-Copy.iso dapat dianggap sebagai sumber data yang sah untuk proses akuisisi data menggunakan *tools* FTK *Imager* dan *Autopsy*.



Gambar 9. Nilai *HashImage* DVD-R Pada *Tools* FTK *Image*

C. *Analysis:* Pada tahapan ini bukti digital yang ditemukan pada proses akuisisi akan dijadikan sebagai barang bukti yang sah setelah dilakukan validasi nilai *hash*, *file-file* yang ditemukan pada hasil proses akuisisi data pada tiap *tools* akan menunjukkan hasil yang berbeda-beda dikarenakan fiturnya berbeda sesuai dengan keperluan *investigator*. Hal ini merujuk pada tingkat akurasi dalam menemukan bukti digital pada objek *storage* lainnya yang digunakan berdasarkan pada penelitian terdahulu.

Dari masing-masing alat akan dianalisis untuk mendapatkan barang bukti sesuai dengan skenario yang dibuat untuk DVD, yaitu:

1. FTK *Imager.* Memberikan alat forensik yang digunakan terutama untuk mengakses, memeriksa, dan memberikan salinan forensik dari media penyimpanan. Meskipun fitur nya lebih terbatas dibandingkan perangkat lunak yang lain seperti fitur analisis yang terbatas dan tidak dirancang untuk investigasi yang kompleks tetapi memiliki kelebihan yaitu ringan, cepat, dan sederhana yang dapat digunakan untuk analisis data awal. Setelah menganalisis ada kemampuan FTK yang menonjol yaitu:
   a. Mampu identifikasi artefak digital yang dihapus, *metadata*, dan informasi sistem *file*.
   b. Menyediakan fitur *hashing* untuk verifikasi integritas data, tetapi kurang bisa memberikan analisis mendalam.
   c. Tidak memilki kemampuan untuk melakukan korelasi otomatis terhadap data artefak (seperti *timeline* analisis).
2. *Autopsy*. Adalah *platform open-source* forensik yang berfokus dalam analisis data mendalam dan menyediakan antar muka yang intuitif. Kelebihan dari aplikasi ini adalah sangat lengkap untuk investigasi digital dan mendukung otomatisasi dalam menganalisis artefak forensik tetapi kekurangan nya memiliki waktu yang sangat lama untuk proses analisis dibandingkan yang lain. Dalam analisis ini *Autopsy* memiliki kemampuan yaitu:
   a. Mendukung analisis *timeline*, pengelompokan berdasarkan tipe *file* seperti image, dll serta pencarian artefak penting seperti *log* aktivitas pengguna.
   b. Fitur analisis artefak khusus seperti pencarian *file* yang hilang.

3. *ProDiscover* Basic. Adalah perangkat lunak forensik yang memungkinkan analisis media penyimpanan terutama dalam pemulihan dan analisis data. Aplikasi ini mempunyai kelebihan yaitu *interface* yang ramah dan mendukung pemulihan data dengan baik tetapi kekurangan nya yaitu versi yang sangat terbatas pada fungsi dasar serta kurang mendukung analisis lanjutan dan otomatisasi. Kemampuan yang bisa diambil dari aplikasi ini adalah:
   a. Mampu melakukan pencarian terhadap *file* yang dihapus dalam penyimpanan
   b. Menyediakan fitur *anomaly* seperti analisis partisi yang tidak biasa

D. *Reporting*

Pada hasil penelitian yang telah dilakukan, ditemukan beberapa bukti yaitu:

No	Data Ditemukan	*Autopsy*	*ProDiscover basic*	FTK *Imager*
A	Gambar	6	4	3
B	Dokumen	1	1	1
C	Video	4	3	4
D	Winrar	2	1	2
E	*Voice*	1	1	1
F	Excel	1	1	1
G	Aplikasi yang Terdeteksi	1	1	1
H	Waktu Pengolahan Data	6 Menit 44 Detik	7 Menit 23 Detik	16 Menit 51 Detik

1. *Autopsy*. Berhasil mengidentifikasi total 16 *file* yang terdiri dari gambar, dokumen, video, dan seluruh *file* lainnya yang sebelumnya telah dikirim oleh pengguna ke dalam DVD. Proses analisis menggunakan *Autopsy* memungkinkan identifikasi yang komprehensif karena antarmuka yang intuitif dan dukungan untuk berbagai format *file*. Keunggulan *Autopsy* terletak pada kemampuannya untuk menganalisis dengan waktu relatif cepat dan menghasilkan laporan yang terstruktur.
2. *ProDiscover basic*. Menemukan 13 *file* dari seluruh *file* yang terdapat di DVD. *ProDiscover* unggul dalam hal keamanan data selama analisis, karena memastikan bahwa *file* sumber tidak mengalami perubahan. Meskipun lebih sedikit *file* yang ditemukan dibandingkan *Autopsy*.
3. FTK *Imager*. Mendeteksi 15 *file* dalam DVD yang dianalisis. FTK *Imager* dikenal dengan kecepatan proses analisis dan kemampuan mengekstrak bukti digital dengan efisien. Selain itu, aplikasi ini menyediakan fitur untuk meninjau *file* langsung dari drive tanpa memerlukan pengunduhan atau salinan, yang menghemat waktu dalam proses forensik.

5. SIMPULAN

Penerapan metode NIST untuk forensik pada *optical drive*, seperti DVD-R, menegaskan pentingnya pendekatan sistematis mulai dari akuisisi data, analisis menggunakan alat forensik, hingga dokumentasi menyeluruh untuk memastikan validitas bukti. Berdasarkan hasil analisis dengan menggunakan FTK *Imager*, *ProDiscover Basic*, dan *Autopsy* terhadap 16 *file* asli yang telah diakuisisi, masing-masing alat menunjukkan kelebihan dan kekurangan.

FTK *Imager* memiliki keunggulan dalam peninjauan langsung tanpa memerlukan salinan, meskipun membutuhkan waktu yang lebih lama dan tidak mampu membaca beberapa *file* digital yang telah dihapus. *ProDiscover Basic*, meskipun ramah untuk pemula, hanya mampu mendeteksi 13 *file* akibat keterbatasannya dalam analisis data. Di sisi lain, *Autopsy* menunjukkan keandalan dalam analisis mendalam, mampu mengidentifikasi seluruh 16 *file* dengan pelaporan yang komprehensif serta menampilkan histori *file* yang dihapus oleh pengguna.

Secara keseluruhan, *Autopsy* direkomendasikan untuk melakukan forensik dalam konteks penelitian ini karena performanya yang unggul dalam analisis mendalam dan pelaporan terperinci. Untuk meningkatkan proses forensik, penting untuk terus memperbarui perangkat lunak yang digunakan, mengintegrasikan teknologi canggih, serta mengikuti panduan metode NIST untuk memastikan hasil yang akurat dan valid.

DAFTAR REFERENSI

[1] N.A.Muhammad, "*Digital Forensik:Panduan Praktis Investigasi Komputer*". Jakarta: Salemba Infotek.2012.

[2] K. T. Shamlawi Alaa, "Wearables as Digital Evidence," no. March, 2018.

[3] I. Riadi, Sunardi, and P. Widiandana. "Investigating Cyberbullying on WhatsApp Using Digital Forensics Research Workshop". Jurnal RESTI (*Rekayasa Sistem dan Teknologi Informasi*) 4, no. 4 (August 20, 2020): 730 – 735.

[4] Riadi, I., Sunardi, & Firdonsyah, A. "Forensic Investigation Technique on Android's Blackberry Messenger using NIST Framework". *International Journal of Cyber-Security and Digital Forensics*, 16(4), 198–205.2017.

[5] Kessler, G.C., "Anti-Forensics and the Digital Investigator".2007.

[6] Sunardi, Riadi, I., Akbar, H., M. "Penerapan Metode Static Forensics untuk Ekstraksi File Steganografi pada Bukti Digital Menggunakan Framework DFRWS ". Jurnal RESTI (*Rekayasa Sistem dan Teknologi Informasi*) Vol. 4 No. 3 (2020) 576 – 583.

[7] Barbosa, E. F., & Ziviani, N. "*Data structures and access methods for read-only optical discs*". In Computer science (pp. 189-207). Springer, Boston, MA. 1992.

[8] T.Coughlin"Media Drive Storage Growth,"https://www.forbes.com/sites/tomcoughlin/2019/08/26/media-drives-storage-growth/#36fa9d804cd8,2019.(Online).Tersedia:https://www.forbes.com/sites/tomcoughlin/2019/08/26/media-drives-storage-growth/#36fa9d804cd8. [accessed: 28 Januari 2020].

[9] Optical Storage Technology Association. Universal Disk Format™ Specification Revision 1. 1996.

[10] M. Fadli Hasa, A. Yudhana, A. Fadlil. "Implementasi Anti Forensik pada Harddisk Menggunakan Metode DoD 5220.22 M dan British HMG IS5 E".Jurnal RESTI (*Rekayasa Sistem dan Teknologi Informasi*).

[11] Schweikert, A. "An Optical Media Preservation Strategy" Appendix Workflows.2018.

[12] Saudi, M. M. "An overview of disk imaging tool in computer forensics". *SANS Institute*. 2001.
[13] S. Ningsih, I. Riadi, and Y. Prayudi, "Digital Forensics Workflow as A Mapping Model for People, Evidence, and Process in Digital Investigation," *Int. J. Cyber-Security Digit. Forensics*, vol. 7, no. 3, pp. 294–304, 2018, doi: 10.17781/p002463.
[14] M. I. Aulia, I. Riadi, and A. Fadlil, "Storage Forensic *Optical drive* Menggunakan Metode Statik," *Semnastek* 2019, no. 2013, pp. 756–761, 2019.
[15] I. Riadi, A. Fadlil, and M. I. Aulia, "Review Proses Forensik *Optical drive* Menggunakan Metode National Institute of Justice (NIJ)" *J. Tek. Inform. dan Sist. Inf.*, vol. 8, no. 3, pp. 107–118, 2019.
[16] Mustafa, I. Riadi, and R. Umar, "Rancangan Investigasi Forensik E-mail dengan Metode National Institute of Standards and Technology (NIST)" *Pros. SNST*, vol. 9, pp. 121–124, 2018.\
[17] V. A. Yuliani and I. Riadi, "Forensic Analysis WhatsApp Mobile Application on Android-Based Smartphones Using National Institute of Standard and Technology (NIST) Forensic Analysis WhatsApp Mobile Application On Android Based Smartphones Using National Institute of Standard and Tec," vol. 8, no. November,pp. 223–231, 2019.
[18] Bandr Siraj Fakiha(2022),Cybersecurity: Analysis and Application of *ProDiscover* Forensic Toolkit.
[19] A. Tanner and D. Dampier, "Concept mapping for digital forensic investigations," *IFIP Adv. Inf. Commun. Technol.*, vol. 306, pp. 291–300, 2009, doi:10.1007/978-3-642-04155-6_22.
[20] I. Riadi, R. Umar, and A. Firdonsyah, "Forensic tools performance analysis on android-based blackberry messenger using NIST measurements," Int. J. Electr. Comput. Eng., vol. 8, no. 5, pp. 3991–4003, 2018, doi: 10.11591/ijece.v8i5.pp3991-4003.