Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi
Jl. Ahmad Yani, K.M. 33,5 - Kampus STMIK Banjarbaru
Loktabat – Banjarbaru (Tlp. 0511 4782881), e-mail: puslit.stmikbjb@gmail.com
e-ISSN: 2685-0893
p-ISSN: 2089-3787

Review Proses Forensik *Optical Drive* Menggunakan Metode *National Institute of Justice* (NIJ)

Imam Riadi[1*], Abdul Fadlil[2], Muhammad Immawan Aulia[3]
[1]Program Studi Sistem Informasi, Universitas Ahmad Dahlan
[2]Program Studi Teknik Elektro, Universitas Ahmad Dahlan
[3]Program Studi Magister Teknik Informatika, Universitas Ahmad Dahlan
[123]Jl. Prof. DR. Soepomo Sh, Kota Yogyakarta, Telepon: (0274) 563515
[1*]Imam.riadi@is.uad.ac.id

Abstrak

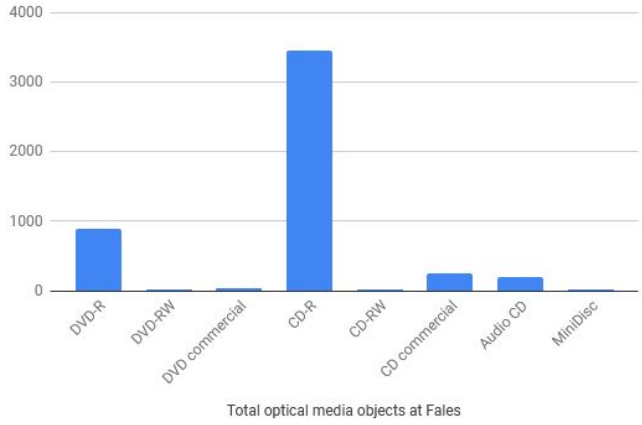
Saat ini media penyimpanan telah banyak berubah, tidak hanya dalam bentuk yang lebih minimalis tetapi juga dalam jumlah kapasitas itu sendiri. Forensik digital saat ini merupakan bidang yang berkembang berdasarkan data pada penyimpanan media, dilakukan untuk berbagai keperluan seperti data yang diperoleh, kontaminasi data, kloning data, dan lainnya. Drive optik seperti CD dan DVD, termasuk media penyimpanan, digunakan untuk menyimpan data dalam bentuk file audio dan video. Dalam penelitian yang dilakukan pada drive optik khusus, CD-R / DVD dapat diperoleh melalui proses pencitraan untuk mendapatkan ruang yang tidak terisi yang berisi data yang sebelumnya diformat atau dihapus. Penelitian ini membahas proses pemulihan file yang telah diformat menggunakan alat Forensik Autopsi dalam proses pemeriksaan dan analisis. Pengambilan bukti digital pada objek penelitian dilakukan dengan metode forensik statis, sedangkan evaluasi dan analisis adaptor menggunakan metode forensik dari National Institute of Justice (NIJ) untuk mendapatkan bukti digital dari objek penelitian.
Kata kunci: *Bukti Digital, Forensik, National Institute of Justice, Optikal Drive*

Abstract

At present the storage media has changed a lot, not only in a more minimalist form but also in the amount of capacity itself. Digital forensics is currently a growing field based on data on media storage, carried out for various purposes such as data obtained, data contamination, data cloning, and others. Optical drives such as CDs and DVDs, including storage media, are used to store data in the form of audio and video files. In the research carried out on special optical drives, CD-R / DVDs can be acquired through the imaging process to obtain unallocated space that contains data previously formatted or deleted. This research discusses the file recovery process that has been formatted using the Forensic tool Autopsy in the examination and analysis process. Retrieval of digital evidence on the object of research is done by static forensic methods, while the evaluation and analysis of adapters use the forensic method of the National Institute of Justice (NIJ) to obtain digital evidence from the object of research.
Keywords*: Digital Evidence, Forensic, National Institute of Justice, Optical Drive*

1. Pendahuluan

Media penyimpanan pada saat ini mengalami banyak evolusi, tidak hanya dalam bentuk namun juga kapasistas yang bertambah besar yang difungsikan sebagai wadah menyimpan data dalam bentuk dan ekstensi yang beraneka ragam. *Optical drive* merupakan media penyimpanan yang berbentuk cakram (*disc*) yang menyimpan data dengan cara di *burning* terlebih dahulu. *File system* yang digunakan pada CD/DVD yaitu *Universal Disc Format* (UDF) *optical drive* contohnya CD-R, CD-R(W), DVD-R, DVD-R(W). *Optical drive* juga dapat dikatakan sebagai media penyimpanan karena dapat menampung data dengan kapasitas tertentu untuk keperluan manusia dalam mengolah *data*. Fungsi utama *optical drive* pada beberapa tahun belakang banyak digunakan pada industri musik bukan sebagai media penyimpanan namun *media player*. Pada industri *game* masih menggunakan media optik yakni CD, DVD dan Bluray Disc sebagai media player agar *game* pada media optik dapat dimainkan pada masing-masing *console*. Perkembangan penggunaan media optik dapat dilihat pada Gambar 1.

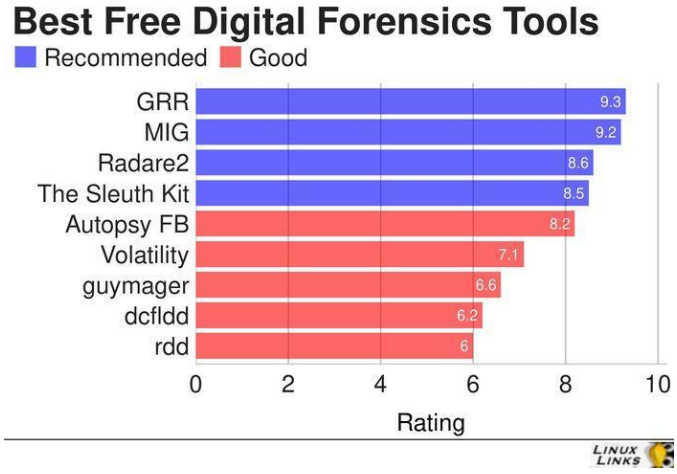


Gambar 1. Grafik Pertumbuhan Penggunaan Optical Media [1].

Grafik pada Gambar 1 menjelaskan perkembangan jumlah pengguna media optik yang terbanyak pada CD-R yang hampir menuju 4000 dan kedua DVD-R dibawah 1000 pada Fales.

Pada *Optical drive* data dapat disimpan dengan beragam kapasitas yang dimana tiap jenisnya memiliki perbedaan tergantung tipe yang digunakan dan maksimal kecepatan burning, yang mempengaruhi kualitas data pada saat selesai proses *burning*, apabila menggunakan kecepatan maksimal membuat *optical drive* tidak reflektif sehingga optik pada CD/DVD ROM dalam proses *read* menjadi kurang akurat.

Tool forensik yang memiliki fungsi akuisisi diperlukan untuk menghimpun bukti digital dan membenarkan diterimanya bukti digital dan keutuhan dari bukti digital tersebut autentik yang didapatkan dan juga perlu diterangkan melalui prosedur standard seperti *hashing* untuk menjaga keutuhan data dan meminimalisir terjadinya modifikasi atau sabotase data atau *file* yang berakibat ditolaknya sebagai bukti digital. Perbedaan penerapan tool forensik juga akan berpengaruh pada bukti digital yang diditemukan [2]. Pada Gambar 2 dapat diketahui *tools* forensik yang populer digunakan.



Gambar 2. Grafik *tools* forensik yang direkomendasikan [3].

Multisession merupakan fitur pada aplikasi burning nero dimana kapasitas *optical disc* dapat diisi kembali dengan cara diburning ulang hingga kapasitas nya penuh, selain itu pada fitur ini dapat digunakan pada CD-R atau DVD-R dimana pada jenis disc ini hanya dapat melakukan read data atau sekali burning saja. Pada penelitian terdahulu melakukan pengembalian barang bukti digital dari kasus terformatnya sebuah DVD-RW menggunakan metode statik forensik dengan menggunakan *tools* FTK Imager. Pada penelitian ini membahas tentang cara yang memungkinkan dilakukan untuk mengembalikan data yang sudah terformat pada DVD-R yang sudah diformat yang sebelumnya sudah diburning menggunakan fitur multisession.

Berdasarkan permasalahan yang disebutkan diatas, maka penelitian ini diharapkan dapat menjadi sebuah solusi dalampengembalian bukti digital pada media penyimpanan khususnya *optical disc* dalam sebuah kasus *cyber crime*.

2. Tinjauan Pustaka

Beberapa penelitian telah dilakukan dalam bidang forensik digital, khususnya media penyimpanan *disc*, *tools* dan framework. Penelitian-penelitian tersebut sebagai berikut:

Penelitian dari Muhammad Immawan Aulia, Imam Riadi dan Abdul Falil [4] dengan judul "*Storage Forensic Optical Drive* Menggunakan Metode Statik" dimana melakukan penelitian melakukan akuisisi data pada DVD-RW yang sudah diformat menggunakan tools FTK Imager dengan hasil temuan *unlocated space*.

Penelitian yang dilakukan Yudhana, Umar, dan Ahmadi [5] yang berjudul Akuisisi Data Forensik Google Drive Pada Android Dengan Metode *National Institute of Justice* (NIJ) melakukan akuisisi data pada *storage cloud* Google Drive menggunakan *tools* MOBILedit Tools Forensic dan Oxygen Forensics yang berhasil menemukan data temuan berupa *file* gambar dan kompresi zip.

Uraian penelitian dari Imam Riadi, Rusydi Umar, Imam Mahfudl Nasrulloh [6] berjudul Analisis Forensik Digital Pada *Frozen Solidstate Drive* Dengan Metode *National Institute of Justice* (NIJ) mengakuisisi data pada media penyimpanan SDD dengan kondisi freeze menggunakan *tools* OSForensics, Autopsy dan Winhex dengan tingkat presentasi keberhasilan 28,7% pada 25 *file* yang berhasil direstorasi dari 85 *file*.

Pada penelitian ini terdapat beberapa bahasan dasar teori yang menjadi landasan atau acuan, sebagai berikut:

Digital Forensik

Digital Forensik adalah pengaplikasian bidang ilmu pengetahuan dan teknologi komputer dalam pembuktian hukum (*pro justice*). Serta menggunakan metode ilmiah yang digunakan untuk membuktikan suatu kasus dengan tahapan pemeliharaan, validasi, pengumpulan, analisis, identifikasi, dokumentasi, interpretasi dan penyajian *digital evidence* yang diperoleh dari sumber digital, hal ini dilakukan sebagai pembuktian pada kasus *cyber crime* secara ilmiah (*scientific*), sehingga diperoleh *digital evidence* yang dapat digunakan untuk barang bukti yang valid [7]. Tujuan utama dari analisis forensik adalah untuk mengidentifkasi semua peristiwa, untuk mengatahui efek pada sistem, untuk memperoleh bukti yang diperlukan, untuk mencegah insiden dimasa mendatang dengan mendeteksi teknik berbahaya yang digunakan [8]. Digital forensik fokus pada penemuan bukti digital yang bisa tersimpan pada storage komputer sementara, storage permanen, USB, CD, internet dan lainnya [9].

Bukti Digital

Bukti digital adalah informasi yang diamankan dalam bentuk *binary* sebagai bukti digital yang dapat dibuktikan sebenar-benarnya dalam proses hukum [10]. Bukti digital dapat ditemukan di *hard drive, flash drive*, perangkat seluler. Proses analisis forensik yang dilakukan harus mencakup hasil yang diambil oleh ahli forensik. Laporan yang diperiksa tentang rincian perangkat keras (*hard drive*), prosedur dan *tools* yang digunakan dalam pemeriksaan hingga bukti ditemukan. Hasil *evidence* yang ditemukan tidak tetap dan bervariasi sesuai dengan beberapa kasus yang ditemui [11]. Bukti digital sangat rentan akan perubahan sehingga dapat mempengaruhi keasliannya jika tidak dihandle oleh investigator resmi dengan baik dan sesuai prosedur. Segala jenis perubahan yang terjadi pada bukti digital akan mengacu kepada hasil laporan yang tidak valid, palsu atau bukti tidak dapat digunakan [12].

Universal Disk Format

Universal Disk Format (UDF) adalah standar sistem *file* CD-ROM dan DVD yang dikembangkan sebagai sarana untuk memastikan konsistensi antara *data* yang ditulis ke berbagai media optik, dengan memfasilitasi pertukaran *data* dan penerapan standar ISO / IEC 13346 [13]. UDF diperlukan untuk DVD-ROM, dan digunakan oleh DVD untuk memuat aliran *audio* / *video* MPEG. Awalnya dikembangkan sebagai pengganti spesifikasi sistem *file* dalam standar CD-ROM, ISO 9660. Tujuan utama UDF OSTA adalah memaksimalkan pertukaran *data* dan meminimalkan biaya dan kompleksitas penerapan ISO / IEC 13346 [14].

Digital Versatile Disc

Digital Versatile Disc (DVD), adalah disk ukuran CD berkapasitas tinggi untuk video, aplikasi multimedia, permainan dan *audio* [15]. Lahir pada tahun 1996 dari pergabungan dua teknologi cakram optik dengan spesifikasi teknis untuk setiap DVD format. Awalnya lima spesifikasi diterbitkan, termasuk DVD-ROM, DVD-Video, DVDAudio, DVD-R, dan DVD-RAM. Spesifikasi untuk DVD-RW juga telah ditambahkan daftar format DVD "resmi". DVD + RW adalah contoh format DVD tidak resmi karena dapat membaca disk DVD-ROM, tetapi juga dapat *read* dan *write disc* DVD + RW. Kapasitas untuk disk *read-only* berkisar dari 4.7GB hingga 17.1GB [16].

Multisession

Multisession adalah fitur Memungkinkan pengguna untuk *write* ke bagian tidak tertulis dari disk yang sudah diburning, hal ini memungkinkan *optical drive* seperti CD-R dan DVD-R dapat diburning kembali dengan menambah data yang diperlukan dengan konsep menambahkan kapasitas hingga suatu CD-R atau DVD-R penuh. Apabila disk sudah penuh maka tidak dapat dilakukan burning dikarenakan kapasitas dari disk sudah penuh [1]. Disk multi-sesi memiliki lebih dari satu sesi, yang biasanya merupakan disk yang direkam pengguna yang telah ditulis berulang kali [17].

3. Metodologi

Pada penelitian ini dipaparkan alur metode forensik yakni *National Institute of Justice* (NIJ). Metode forensik ini mendeskripsikan proses-proses setiap tahapan pada penelitian yang dilakukan sehingga dapat diketahui kerangka kerja dan langkah-langkah pada penelitian secara terstruktur agar dapat dijadikan dasar konsep sebagai solusi pada permasalahan dalam penelitian. Melakukan teknik dan analisa forensik berdasarkan prosedur yang benar akan memiliki kesuksesan mendekati 100% dalam akumulasi data forensik [18]. Data forensik dapat diperoleh dengan menggunakan beragam *storage* eksternal seperti USB, eksternal *hard drive* atau CD, DVD. Kemudian data ini akan dibawa investigator ke lab forensik untuk dilakukan berbagai metode agar dapat menganalisis data sebagai bukti secara forensik [19]. Berikut flowchart metode *National Institute of Justice* (NIJ) dapat diilustrasikan seperti Gambar 3.

Gambar 3. Kerangka kerja metode *National Institute of Justice* (NIJ)

Tahapan yang ada pada metode *National Institute of Justice* (NIJ) ada lima tahapan, yakni identifikasi, pengumpulan, pemeriksaan, analisis, dan pelaporan [20].

Tahap identifikasi merupakan tahapan dimana barang bukti pada sebuah kasus kejahatan digital dan data-data untuk mendukung proses penyelidikan. Proses pada tahapan ini, yaitu identifikasi, perekaman dan pelabelan untuk mempertahankan keutuhan dan keaslian dari barang bukti.

Tahap pengumpulan merupakan proses pengumpulan data sebagai pendukung prses penyelidikan dalam mencari bukti digital pada sebuah kasus kejahatan digital. Tahapan ini terdapat proses pengambilan data pada barang bukti yang terindikasi sebagai sebuah sumber data yang relevan dan valid.

Tahap pemeriksaan yakni tahapan pemeriksaan pada data yang ditemukan dalam barang bukti elektronik yang dilakukan secara manual ataupun otomatis, serta memastikan hasil temuan data asli sama seperti keadaan awal dari tempat kejadian kejahatan digital terjadi yang perlu dilakukan identifikasi dan validasi data dengan pencocokan hash MD5.

Tahap analisis adalah tahapan dimana hasil temuan data dari tahapan pemeriksaan dilakukan analisis lebih dalam untuk dapat dibuktikan keasliannya.

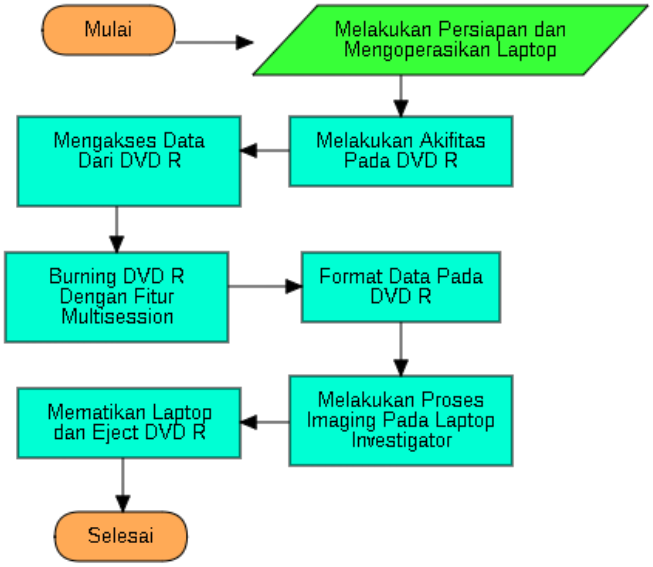
Tahapan pelaporan dilakukan pada barang bukti digital yang telah dianalisis yang meliputi penggambaran proses apa saja yang dilakukan, uraian tools yang digunakan, metode yang diterapkan.

Tahapan utama pada penelitian ini akan dibagi menjadi 3 (tiga) seperti pada Gambar 4.

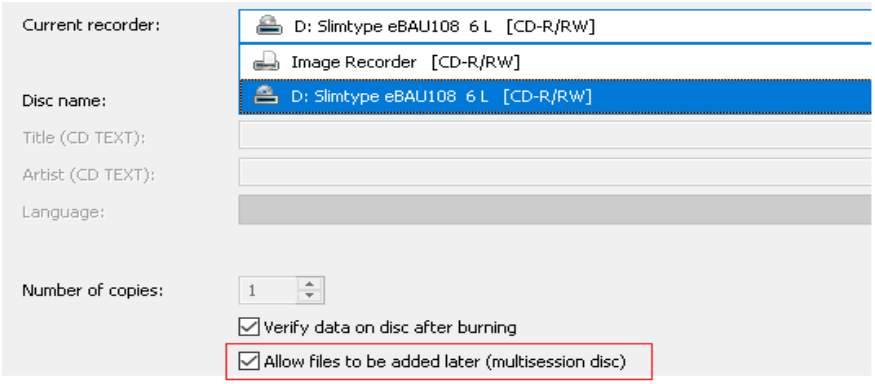
Gambar 4. Tahapan Utama pada Penelitian

Pada penelitian ini menggunakan bukti digital yang tidak didapatkan pada kasus kejahatan digital yang sebenarnya melainkan bukti digital dibuat dan peroleh dari hasil skenario pada tahap implementasi dan pengujian. Tahap implementasi dan pengujian forensik bukti digital pada Implementasi dan pengujian dilakukan dengan desain skenario, dengan tujuan untuk mendapatkan bukti digital seperti pada kasus kejahatan komputer yang sebenarnya. Alur pada tahapan sesuai Gambar 3 merupakan implementasi dan pengujian forensik bukti digital pada DVD-R yang telah terformat.

Implementasi dan pengujian dilakukan sesuai skenario dengan tujuan mendapatkan bukti digital seperti kasus kejahatan digital yang sebenarnya seperti pada Gambar 5. Pada alur DVD-R diburning dengan meggunakan fitur multisession agar dapat diformat pada kotak berwarna merah seperti pada Gambar 6.

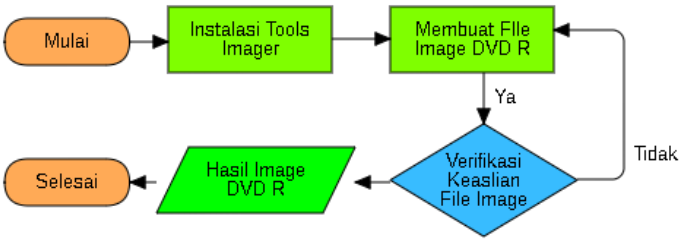


Gambar 5. Tahapan Pengujian dan Implementasi



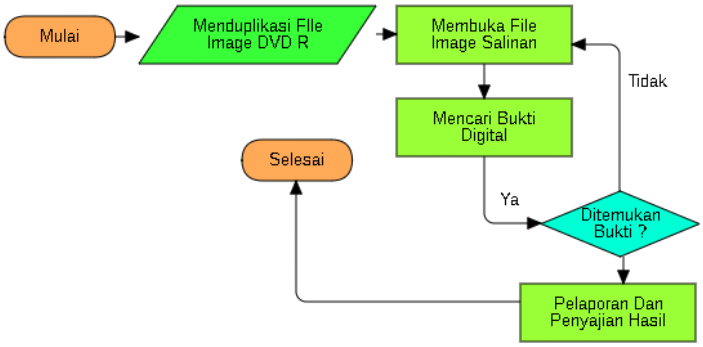
Gambar 6. Fitur Multisession

Implementasi dilakukan pada DVD-R yang telah diformat yang melakukan pengoperasian penggunaan komputer atau laptop secara normal dan ditujukan sebagai tindak kejahatan digital dengan menghapus berbagai macam ekstensi *file* seperti *file* eksekusi (.exe), dokumen (.doc, .pdf, .ppt, .txt), kompresi (.rar, .zip), multimedia (.mp3, .mp4). Setelah melakukan skenario, tahapan berikut nya adalah melakukan akuisisi dengan membuat *file image* dari DVDR-R yang telah dformat terlebih dahulu menggunakan *tools* Autopsy untuk melakukan analisis *file* temuan apa saja yang dapat direstorasi. Metode pengambilan data menggunakan metode statik yaitu metode pengambilan data yang dilakukan secara manual yang dilakukan ketika komputer dalam keadaan tidak beroperasi (off), pada hal ini memeriksa hasil *image* salinan dari DVD-R. Alur pengambilan salinan bukti digital pada Gambar 7.



Gambar 7. Tahapan Pengambilan Salinan Digital Evidence

Tahapan pada gambar 7 dilakukan agar bukti digital yang berupa hasil salinan image dari DVD-R memiliki kesamaan dengan data asli dari DVD-R sebelum diformat. Secara garis besar analisa pada DVD-R yang telah diformat menerapkan metode forensik yang bernama *National Institute of Justice* (NIJ). Hasil temuan diharapkan adaalh *file* dengan jenis *file* gambar (jpg, png), dokumen (doc, docx, pdf, pptx), *file audio* (mp3) dan *file image* (iso). Alur tahapan analisis forensik diilustrasikan seperti Gambar 8.



Gambar 8. Tahapan Analisis Forensik

4. Hasil dan Pembahasan

Penelitian yang dilakukan dengan sebuah simulasi kasus berindikasi kejahatan digital. Pada simulasi ini investigator akan melakukan proses *cloning* pada DVD-R yang terlah diformat untuk menghindari perubahan secara fisik dan digital pada barang bukti digital agar tetap autentik. DVD-R yang menjadi objek penelitian dalam sudah diformat sehingga investigator harus menggunakan *tools* forensik untuk melakukan akuisisi pada DVD-R agar dapat mengambil *file-file* yang akan dijadikan barang bukti digital lalu akan dijadikan bukti pelaporan pada tahapan akhir metode yang digunakan

4.1 Identification

Tahap *Identification* dilakukan untuk mempersiapkan barang bukti digital dengan maksud mendukung proses identifikasi dalam sebuah kasus kejahatan digital. Berikut hasil identifikasi alat dan bahan yang digunakan pada penelitian pada Tabel 1.

Tabel 1. Alat Dan Bahan

No.	Alat dan Bahan	Keterangan
1.	Laptop	Acer Aspire E 14
2.	DVD-ROM	Liteon
3.	DVD-R	Slimtype eBAU108 6L
4.	HashMyFile	*Tools* untuk yang digunakan untuk mengetahui Hash MD5 asli pada *source*
5.	Autopsy	*Tools* yang digunakan untuk melakukan akuisisi data pada objek peneltian
6.	Nero	Aplikasi burning *optical disc*

4.2 Collection

Tahap *Collection* dilakukan pengumpulan barang bukti digital yang berupa data-data/*file-file* pada sebuah objek yang di indikasi sebagai *source* yang valid untuk sebuah kasus kejahatan digital dan dokumentasi bukti fisik dalam bentuk DVD-R seperti pada Gambar 5.

Gambar 5. DVD-R yang menjadi objek penelitian

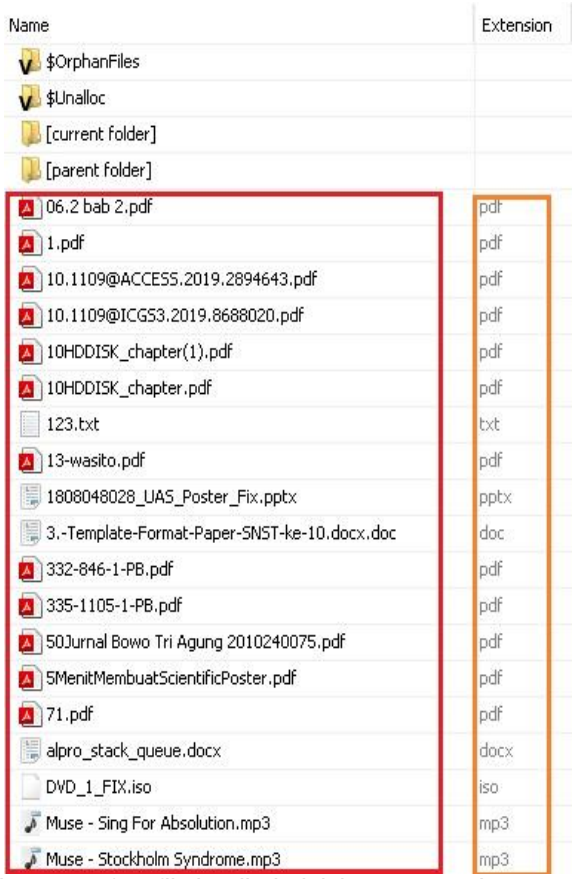
Barang bukti fisik berupa DVD-R terdapat barang bukti digital berupa *file-file* yang dikloning dalam satu *file Image* dengan ekstensi *file* .vhd. hal ini dilakukan untuk menghindari perubahan data dan menjaga keaslian barang bukti digital, *tools* yang digunakan untuk melakukan kloning data yakni autopsy. Hasil kloning data dapat dilihat seperti pada Gambar 6.

Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
DVD RW Drive (D) DVD_1 1573264996131.vhd	Image	175112192	512	Asia/Bangkok	44baba02-546e-426c-bf1c-98f4b9add08b

Gambar 6. *File image* hasil kloning DVD-R dengan ekstensi .vhd menggunakan tools Autopsy

4.3 Examination

Tahap Examination atau tahap pemeriksaan pada barang bukti digital dilakukan secara manual ataupun otomatis yang didapatkan dari tahapan sebelumnya yaitu collection. Barang bukti yang dimaksud berupa *file-file* yang didapatkan dari objek pada sebuah kasus kejahatan digital. Proses akuisisi data pada DVD-R menggunakan DVD-ROM dan tools Autopsy. Proses akuisisi merupakan tahapan pertama yang dilakukan sebelum melakukan tahapan analisis. Pada tahapan akuisisi data pada *file-file* yang akan menjadi barang bukti digital pada DVD-R yang dihubungkan menggunakan DVD-ROM yang tehubung dengan kabel usb pada laptop yang telah terinstall tools Autopsy. Hasil dari tahap eksaminasi data yang telah didapatkan dari proses akuisisi yakni nama *file* pada kotak merah dan beragam ekstensi *file* pada kotak orange pada Gambar 7.



Gambar 7. Daftar *file* hasil akuisisi menggunakan Autopsy

4.4 Analysis

Tahap Analysis dilakukan pada hasil temuan barang bukti digital pada tahapan examination, selanjutnya data dianalisis menggunakan metode yang sah secara teknis dan hukum sebagai pembuktian data tersebut sehingga hasil analisis *digital evidence* dapat dibuktikan dan dipertanggungjawabkan secara ilmiah dan hukum. Pada tools HashMyFile menampilkan daftar bukti digital dengan Hash MD5 pada Tabel 2.

Tabel 2. Hasil Md5 Menggunakan Tools Hashmyfile

Nama File Asli	Ekstensi	Hash MD5 HashMyFile
06.2 bab 2	PDF	fe41fc0e751272871e27118503e2f698
1	PDF	b4791406338db847ae817c5e1bf3e58e
10HDDISK_chapter(1)	PDF	a288b6cc0789c00d94213d128aa9098e
10HDDISK_chapter	PDF	a288b6cc0789c00d94213d128aa9098e
10.1109@ICGS3.2019.8688020	PDF	3044dd13c2f0cb5629179aeab0fb1c36
10.1109@ACCESS.2019.2894643	PDF	a217819d8b99fca2fef7697c4d475c2c
123	TXT	0d0a7d37f836b538c709152a5c8c757a
13-wasito	PDF	04c84b1581ae0110b7c7d278058b4c65

1808048028_UAS_Poster_Fix	PPTX	b6f9fd0c19795ebc1da37ed536023496
332-846-1-PB	PDF	f6de8c5bc34e8c9fccd9959efaa2c547
335-1105-1-PB	PDF	a25a0305f7ae5015313ed57d14afe51b
3.-Template-Format-Paper-SNST-ke-10.docx	DOC	e09290e72ece97541efca7a3ee86b5ae
50Jurnal Bowo Tri Agung 2010240075	PDF	3846842bf9daefc38af63066ce70b043
5MenitMembuatScientificPoster	PDF	871e99788fdd0c30ef6660f89a0786ec
71	PDF	fd5a53542f2874c7ecbef309e484a2c3
alpro_stack_queue	DOCX	549459930cf587b819328b4370db7a9b
DVD_1_FIX	ISO	c8cb4f8f0d3ddfe3c900e99180ac4a6c
Muse - Sing For Absolution	MP3	05fa03889d8aff2bdb77310019a95964
Muse - Stockholm Syndrome	MP3	770fd7442bd2763c0f9d3ef84dc8de87
Muse - Supermassive Black Hole	MP3	a5ade86ff24e401d8c6fb44769507ae2
P1040587	JPG	a599cb5649211576f1fdfa790a9429bf
P1040588	JPG	5742f247474e4ed78316a22e529da6b6
P1040589	JPG	9c54c02ec8dcb390087727ca8d3dc2bb
P1040592	JPG	eb15d40948f2e4631b1aea99aaae849e
P1040604	JPG	094a011e68400acce75e366753f304fd
P1040605	JPG	d55e3e1ee15aaf79f4f4738ee8318fff
P1040607	JPG	0537b17b392db7c1144ff1365b662c90
P1040608	JPG	2f650d746881473f398cab8f6a5a4d1d
QR_Barcode_Baru	PNG	895d1efccf6047ec65549f20f9fe7dd7

Pada Tabel 2. Menunjukkan Hash MD5 beserta nama *file* dan ekstensi nya sebagai informasi asli yang akan digunakan sebagai pembanding dengan hasil akuisisi pada *tools* Autopsy yang akan dapat dilihat pada Tabel 3.

Tabel 3. Hasil Akuisisi Data Menggunakan Tools Autopsy

Nama File	Ekstensi	Hash MD5 Autopsy
06.2 bab 2	PDF	fe41fc0e751272871e27118503e2f698
1	PDF	b4791406338db847ae817c5e1bf3e58e
10HDDISK_chapter(1)	PDF	a288b6cc0789c00d94213d128aa9098e
10HDDISK_chapter	PDF	a288b6cc0789c00d94213d128aa9098e
10.1109@ICGS3.2019.8688020	PDF	3044dd13c2f0cb5629179aeab0fb1c36
10.1109@ACCESS.2019.2894643	PDF	a217819d8b99fca2fef7697c4d475c2c
123	TXT	0d0a7d37f836b538c709152a5c8c757a

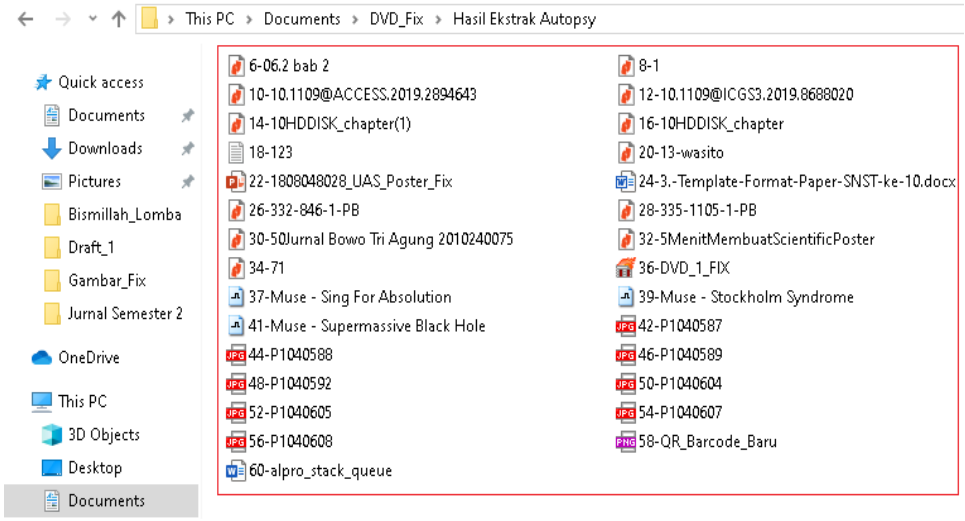
13-wasito	PDF	04c84b1581ae0110b7c7d278058b4c65
1808048028_UAS_Poster_Fix	PPTX	b6f9fd0c19795ebc1da37ed536023496
332-846-1-PB	PDF	f6de8c5bc34e8c9fccd9959efaa2c547
335-1105-1-PB	PDF	a25a0305f7ae5015313ed57d14afe51b
3.-Template-Format-Paper-SNST-ke-10.docx	DOC	e09290e72ece97541efca7a3ee86b5ae
50Jurnal Bowo Tri Agung 2010240075	PDF	3846842bf9daefc38af63066ce70b043
5MenitMembuatScientificPoster	PDF	871e99788fdd0c30ef6660f89a0786ec
71	PDF	fd5a53542f2874c7ecbef309e484a2c3
alpro_stack_queue	DOCX	549459930cf587b819328b4370db7a9b
DVD_1_FIX	ISO	c8cb4f8f0d3ddfe3c900e99180ac4a6c
Muse – Sing For Absolution	MP3	05fa03889d8aff2bdb77310019a95964
Muse – Stockholm Syndrome	MP3	770fd7442bd2763c0f9d3ef84dc8de87
Muse – Supermassive Black Hole	MP3	a5ade86ff24e401d8c6fb44769507ae2
P1040587	JPG	a599cb5649211576f1fdfa790a9429bf
P1040588	JPG	5742f247474e4ed78316a22e529da6b6
P1040589	JPG	9c54c02ec8dcb390087727ca8d3dc2bb
P1040592	JPG	eb15d40948f2e4631b1aea99aaae849e
P1040604	JPG	094a011e68400acce75e366753f304fd
P1040605	JPG	d55e3e1ee15aaf79f4f4738ee8318fff
P1040607	JPG	0537b17b392db7c1144ff1365b662c90
P1040608	JPG	2f650d746881473f398cab8f6a5a4d1d
QR_Barcode_Baru	PNG	895d1efccf6047ec65549f20f9fe7dd7

Dari hasil pada Tabel 3 terdapat hasil temuan *file* yang sama seperti pada Tabel 2, kesamaan tidak hanya pada nama *file* namun pada nilai hash MD5 nya pun sama dengan demikian dari dua tabel dapat disimpulkan bahwa file hasil akuisisi menggunakan tools Autopsy valid.

4.5 Reporting

Tahap Reporting dilakukan setelah tahapan pemeriksaan dan analisis mencapai akhir dan hasil dari analisis dapat dilakukan pelaporan dengan ilustrasi terhadap proses yang dilakukan, mengenai *tools* yang digunakan serta metode/framework, tindakan pendukung yang diambil, perbaikan kebijakan, metode serta *tools* ataupun komponen pendukung lainnya pada proses tindakan digital forensik. Hasil eksaminasi pada tools autopsy menunjukan bahwa semua *file* yang telah diformat pada DVD-R dapat di ekstraksi seperti pada kotak merah dimana terdapat

sedikit perubahan nama pada setiap *file* yang diekstrasi namun tidak ada perubahan pada nilai Hash MD5 yang menandakan *file* ekstrasi ini asli. Ekstrasi mengunakan *tools* autopsy pada Gambar 8.



Gambar 8. Hasil Ekstrasi File pada Autopsy

Dari Gambar 8. pada kotak merah dapat dilihat hasil ekstrasi *file* dari tools Autopsy pada DVD-R yang terformat secara keseluruhan dapat direstorasi, berikut hasil akhir analisis pada Tabel 4.

Tabel 4. Hasil Analisis Jumlah Restorasi File Menggunakan *Tools* Autopsy

No	HashMyFile		Autopsy	
	Ekstensi	Jumlah	Ekstensi	Jumlah
1	.Pdf	12	.Pdf	12
2	.Docx	1	.Docx	1
3	.Doc	1	.Doc	1
4	.Txt	1	.Txt	1
5	.Pptx	1	.Pptx	1
6	.Mp3	3	.Mp3	3
7	.Iso	1	.Iso	1
8	.Jpg	8	.Jpg	8
9	.Png	1	.Png	1
Jumlah File		29		29
Tingkat Keberhasilan			100%	

Pada Tabel 4. diketahui bahwa jumlah *file* pada DVD-R sebelum terformat merupakan 29 file dengan file berekstensi pdf berjumlah 12 file, docx, doc, txt, pptx, iso dan png 1 file, serta Mp3 3 *file,* dan juga jpg 8 *file*. Disebelah kanan tabel menunjukan bahwa *tools* autopsy dapat melakukan akuisisi data secara keseluruhan dengan tingkat keberhasilan sebesar 100%. Pada tools HashMyFile menampilkan Hash MD5 yang asli dari file yang telah terformat pada DVD-R. Verifikasi dilakukan untuk mencocokkan keaslian file asli dengan dengan Hash MD5 file dari hasil akuisisi dari DVD-R, tidak ada perubahan nama pada file hasil akuisisi.

5. Kesimpulan

Berdasarkan hasil review yang telah dilakukan, DVD-R yang diburning dengan mode multisession pada aplikasi burning Nero agar DVD-R dapat diformat pada implementasi *tools*, yaitu Autopsy. Hasil dari *tools* dapat merestorasi *file* secara keseluruhan dengan kecocokan hash MD5 yang sama persis dengan *file* asli sebelum dilakukan eksaminasi. Ekstensi file yang berhasil direstorasi yaitu Pdf, Docx, Pptx, Txt, MP3, Iso, JPG dan PNG dengan jumlah keseluruhan 29 *file* dimana tingkat keberhasilan mencapai 100%. Jumlah file temuan dari *tools* Autopsy sama dengan *file* pada DVD-R sebelum diformat. Metode statik digunakan karena objek termasuk media penyimpanan dengan maksud agar keaslian dan keutuhan dari barang bukti fisik tidak ada

kerusakan secara fisik maupun digital. Dengan adanya review ini diharapkan dapat membantu menyediakan informasi mengenai proses analisis forensik yang berhubungan dengan storage khusunya optical drive CD atau DVD.

Referensi

[1] Schweikert A. *An Optical Media Preservation Strategy for New York University's Fales Library & Special Collections*, 2018.
[2] Imam R., Rusydi U.R., Imam M.N. Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute Of Justice (NIJ), *Electronics, Informatics, and Vocational Education*. 2018; 3(1): 70-82.
[3] Steve E. *The 9 Best Free Linux Digital Forensics Tools*. https://www.linuxlinks.com/digitalforensics/. 2019.
[4] Muhammad I. A, Imam R., Abdul F. *Storage Forensic Optical Drive* Menggunakan Metode Statik. *SEMNASTEK*. 2019.
[5] Yudhana A., Umar R., & Ahmadi A. Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ). *Jurnal CorelIT*. 2017; *10*(10): 8-12.
[6] Imam R., Rusydi U., Imam M. N., Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode *National Institute Of Justice* (NIJ). *Electronics, Informatics, and Vocational Education* (ELINVO). 2018; 3(1): 70-82
[7] Al-Azhar M.N. *Digital Forensic, Panduan Prakestigasi Komputer*. Jakarta: Salemba Infotek, 2012.
[8] Sunardi, Imam R., & Andi S. Forensic Analysis of Docker Swarm Cluster using Grr Rapid Response Framework. *International Journal of Advanced Computer Science and Applications* (IJACSA). 2019; 10(2): 459-466.
[9] Muhammad N.F., Rusydi U., Anton Y. Analisis Live Forensics untuk Perbandingan Kemananan Email Pada Sistem Operasi Proprietary, *Jurnal Ilmiah* ILKOM. 2016; 8(3):242–247
[10] Ashcroft J., Deborah J. D. & Sarah V. H. Forensic Examination of Digital Evidence: A Guide for Law Enforcement, *U.S. Dep. Justice Off. Justice Programs Natl. Inst. Justice Spec*. 2004; 44(2): 634–111.
[11] Kessler G.C. *Anti-Forensics and the Digital Investigator*, 2007.
[12] Albanna F., Forensic Analysis of Frozen Hard Drive Using Static Forensics Method, *International Journal of Computer Science and Information Security* (IJCSIS). 2017; 15(1): 173–178.
[13] Optical Storage Technology Association. *Universal Disk Format™ Specification Revision 1*. 1996.
[14] Imler F., Creutzburg R. *Possibilities of the forensic investigation of CD, DVD and Blu-ray Disc*, 2016.
[15] LaBarge R. *DVD Authoring & Production*. New York: Routledge, 2001
[16] Narahara T., Kobayashi S., Hattori M., Shimpuku Y., van den Enden G. J., Kahlman J. A., ... & van Woudenberg, R. Optical disc system for digital video recording. *Japanese Journal of Applied Physics*. 200; *39*(2S): 912.
[17] Peter C. *CD and DVD Forensics*. 1st Edition, 2006.
[18] Roni A. P, Abdul F, & Imam R. Forensik Mobile Pada Smartwach Berbasis Android, Jurti. 2017; 1(1): 41–47.
[19] Rafique M., & Khan M. N. A. Exploring static and live digital forensics: Methods, practices and tools. *International Journal of Scientific & Engineering Research*. 2013; *4*(10): 1048-1056.
[20] Muhammad N. F., Rusydi U., & Anton Y. Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email. *JISKa*. 2017; 1(3): 108–114.