HASIL CEK_60020397_C44-Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST)

by Imam Riadi 60020397

Submission date: 11-Dec-2020 10:28AM (UTC+0700)
Submission ID: 1471678621
File name: n_Metode_National_Institute_of_Standard_and_Technology_NIST.pdf (613.93K)
Word count: 4908
Character count: 29819

Terakreditasi SINTA Peringkat 2
Surat Keputusan Dirjen Penguatan Riset dan Pengembangan Ristek Dikti No. 10/E/KPT/2019
masa berlaku mulai Vol. 1 No. 1 tahun 2017 s.d Vol. 5 No. 3 tahun 2021

Terbit online pada laman web jurnal: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 4 No. 5 (2020) 820 - 828 ISSN Media Elektronik: 2580-0760

Investigasi Bukti Digital *Optical Drive* Menggunakan Metode *National Institute of Standard and Technology* (NIST)

Imam Riadi[1], Abdul Fadlil[2], Muhammad Immawan Aulia[3]
[1]Program Studi Sistem Informasi, Universitas Ahmad Dahlan
[2]Program StudiTeknik Elektro, Universitas Ahmad Dahlan
[3]Program Studi Teknik Informatika, Universitas Ahmad Dahlan
[1]imam.riadi@is.uad.ac.id, [2]fadlil@mti.uad.ac.id, [3]muhammad1808048028@webmail.uad.ac.id

Abstract

*DVD-R is a type of optical drive that can store data in one burning process. However, there is a feature that allows erasing data in a read-only type, namely multisession. The research was conducted to implement the data acquisition process which was deleted from a DVD-R using Autopsy forensic tools and FTK Imager. The National Institute of Standards and Technology (NIST) is a method commonly used in digital forensics in scope storage with stages, namely collection, examination, analysis, and reporting. The acquisition results from Autopsy and FTK-Imager show the same results as the original file before being deleted, validated by matching the hash value. Based on the results obtained from the analysis and presentation stages, it can be concluded from the ten files resulting from data acquisition using the FTK Imager and Autopsy tools on DVD-R. FTK Imager detects two file systems, namely ISO9660 and Joliet, while the Autopsy tool only has one file system, namely UDF. The findings on the FTK Imager tool successfully acquired ten files with matching hash values and Autopsy Tools detected seven files with did not find three files with extensions, *.MOV, *.exe, *.rar. Based on the results of the comparative analysis of the performance test carried out on the FTK Imager, it got a value of 100% because it managed to find all deleted files and Autopsy got a value of 70% because 3 files were not detected because 3 files were not detected and the hash values were empty with the extensions * .exe, * .rar and *.MOV. This is because the Autopsy tool cannot detect the three file extensions.*

Keywords: *Optical, Drive, Storage, NIST, Digital Evidence, Digital Forensic.*

Abstrak

DVD-R salah satu jenis *optical drive* yang dapat menyimpan data dalam satu kali proses *burning*, namun ada fitur yang memungkinkan melakukan penghapusan data pada jenis *read-only* yakni *multisession*. Penelitian dilakukan untuk pengimplementasian proses akuisisi data yang terhapus dari sebuah DVD-R menggunakan *tools* forensik Autopsy dan FTK Imager. *National Institute of Standard and Technology* (NIST) merupakan metode yang umum digunakan dalam digital forensik pada *scope storage* dengan tahapan, yaitu koleksi, eksaminasi, analisis dan pelaporan. Hasil akuisisi dari Autopsy dan FTK-Imager menunjukan hasil yang sama dengan *file* asli sebelum terhapus, validasi dengan pencocokan nilai *hash*. Berdasarkan hasil yang diperoleh dari tahapan analisis dan presentasi dapat disimpulkan dari 10 file hasil akuisisi data menggunakan tools FTK Imager dan Autopsy pada DVD-R, FTK Imager mendeteksi 2 sistem file yaitu ISO9660 dan Joliet sedangkan *tools* Autopsy hanya 1 sistem *file* yaitu UDF. Hasil temuan pada *tools* FTK Imager berhasil mengakuisisi 10 *file* dengan dengan nilai *hash* yang cocok dan *tools* Autopsy 7 *file* serta tidak menemukan 3 *file* dengan ekstensi, *.MOV, *.exe, *.rar. Berdasarkan Hasil dari analisis komparatif uji performa yang dilakukan pada FTK Imager memperoleh nilai 100% karena berhasil menemukan seluruh file yang terhapus dan Autopsy mempeoleh nilai 70% sebab 3 file tidak terdeteksi serta nilai hash yang kosong dengan ekstensi *.exe, *.rar dan *.MOV. Hal ini dikarenakan *tools* Autopsy tidak dapat mendeteksi ketiga ekstensi file tersebut.

Kata kunci: Optikal, Drive, Media Penyimpanan, NIST, Bukti Digital, Digital Forensik

1. Pendahuluan

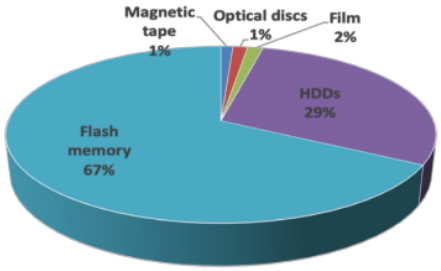
Digital Forensik merupakan implementasi bidang ilmu pengatahuan dan teknologi komputer serta metode ilmiah untuk pembuktian kejahatan digital pada hukum (*pro justice*), dalam hal ini adalah pembuktian kejahatan teknologi tinggi secara ilmiah (*scientific*), hingga bisa mendapatkan hasil temuan berupa bukti-bukti digital yang berasal dari sumber digital, termasuk paket *data*

Diterima Redaksi : 28-07-2020 | Selesai Revisi : 22-09-2020 | Diterbitkan Online : 30-10-2020

yang dikirimkan melalui jaringan komputer, untuk tujuan memfasilitasi atau melanjutkan rekonstruksi peristiwa dalam tindakan kriminal atau sebagai bagian dari penyelidikan pidana atau membantu mencegah tindakan tidak sah mengganggu operasi yang direncanakan dan dapat digunakan sebagai barang bukti yang sah untuk menjerat pelaku kejahatan tersebut. Tujuan utama dari analisis forensik adalah untuk mengidentifkasi semua peristiwa, untuk mengatahui efek pada sistem, untuk mendapatkan bukti yang diperlukan, untuk mencegah insiden dimasa mendatang dengan mendeteksi teknik berbahaya yang digunakan [1]. Forensik digital didefinisikan sebagai "pengetahuan ilmiah dan metode yang diterapkan untuk *identifiaxtion*, *collection*, *preservation*, *examination*, dan *analysis* bukti digital dengan cara yang dapat diterima untuk diterapkan dalam masalah hukum" [2]. Selain *Cybercrime* yang sering terjadi pada kasus digital forensik, *Cyberbullying* juga merupakan salah satu masalah yang sering terjadi. [3].

Bukti digital adalah informasi yang rapuh, *volatile* dan rentan jika tidak ditangani dengan benar [4]. Bukti digital sangat penting dalam semua jenis kejahatan, bukan hanya kejahatan komputer, Untuk menghindari hal itu maka diperlukan tindakan seperti menjaga perangkat dalam mode isolasi. Tujuannya adalah untuk menghindari data dari terhapus dan mengubah dengan kondisi apa pun. Bukti digital dapat ditemukan di hard drive, flash drive, perangkat seluler [5]. 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 temuan bukti digital tidak konsisten dan bervariasi sesuai dengan kasus yang sedang diselesaikan. Bentuk umum pada bukti digital yakni bentuk biner yang dapat diandalkan di pengadilan. Berdasarkan Undang-Undang Republik Indonesia No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, barang bukti dikenal dengan istilah informasi elektronik dan dokumen elektronik. Oleh karena itu dalam rangka mengungkap kasus kejahatan berkaitan dengan bukti elektronik/digital, jenis barang bukti inilah yang harus dicari kemudian dianalisis secara teliti keterkaitan masing-masing *file* [6].

Optical drive merupakan salah satu jenis perangkat penyimpanan sekunder dengan keunggulan signifikan dibandingkan media magnetik, seperti kapasitas penyimpanan yang lebih tinggi dan biaya yang lebih rendah [7]. Permukaan kosong dapat menyimpan dan menampung data dengan kapasitas tertentu seperti video, aplikasi, multimedia, permainan dan audio dengan cara di-*burning*. CD dan DVD adalah perangkat elektro-optik, sebagai solusi dari hampir semua *peripheral* komputer lain yang bersifat elektromagnetik. Tidak ada medan magnet dalam membaca atau merekam cakram-cakram ini, oleh karena itu kebal terhadap medan magnet, tidak seperti *hard drive* karena kekebalannya terhadap medan magnet. Media CD dan DVD tidak terpengaruh oleh efek *Electromagnetic Pulse* (EMP), sinar-X, dan sumber-sumber elektromagnetik lainnya [7]. *Burning* data pun ada salah satu metode yang ditawarkan pada aplikasi *burning* seperti Nero yakni *Multisession* memiliki lebih dari satu sesi, yang biasanya merupakan disk yang direkam pengguna yang telah ditulis berulang kali. 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]

Umumnya jenis -R ini hanya satu kali *burning* data saja, namun dengan fitur *Multisession* ini dapat menambahkan data hingga kapasitas *optical drive*nya penuh. Sistem file pada *optical drive* ada beberapa diantaranya yakni ISO 9660, Joilet dan *Universal Disk Format* (UDF) adalah *filesystem* universal sebagai sarana untuk memastikan konsistensi antara data yang ditulis ke berbagai media optik, dengan memfasilitasi pertukaran data dan penerapan standar ISO / IEC 13346. yang mendukung nama file yang lebih panjang dan atribut file yang lebih banyak [9]. Sering dikaitkan dengan DVD-Video, tetapi juga muncul pada CD dan DVD sebagai "*bridge format*" bersama dengan ISO 9660, Joliet. UDF diperlukan untuk DVD-ROM, dan digunakan oleh DVD untuk memuat aliran audio / video MPEG. Setiap sistem file memiliki keunikan tersendiri contohnya batas maksimal karakter pada penamaan *file* pada *optical drive*. Sistem file ISO9660 merupakan standar untuk penyimpanan data yang dapat diakses oleh semua sistem operasi. Untuk menyediakan akses ke semua OS, ISO 9660 dibatasi dalam panjang nama file (aslinya 8 karakter) dan ukuran (4 GB). Joliet merupakan ekstensi Microsoft untuk ISO9660 yang mendukung nama *file Unicode* (memungkinkan untuk skrip non-Latin), nama *file* yang lebih panjang, dan direktori yang lebih dalam [10].

Disk Imaging merupakan proses salin pada data seluruh disk ini terlepas dari perangkat lunak apa pun yang digunakan untuk mendapatkan konten lengkap termasuk lokasi data. *Disk imaging* mengambil salinan sektor demi sektor biasanya untuk keperluan forensik dan karenanya akan berisi beberapa mekanisme (verifikasi internal) untuk membuktikan bahwa salinannya tepat dan belum diubah. [11].

Terhapus dan rusaknya *file* pada sebuah media penyimpanan merupakan hal yang tidak dapat dihindari, baik sengaja ataupun secara tidak sengaja. Kasus digital forensik seperti ini dapat bilang sebagai sebuah kejahatan digital apabila dilakukan dengan tujuan tidak baik atau negatif dalam artian penghapusan barang bukti digital. *File* yang terhapus sangat berpotensi untuk di*recovery* menggunakan bidang digital forensik [12]. Ada beragam *tools* forensik untuk mendapatkan kembali data yang telah dihapus tersebut, tiap tools forensik memiliki karakteristik nya masing dalam menemukan barang bukti digital pada sebuah barang bukti elektronik seperti media penyimpanan. tools yang biasa digunakan pada media penyimpanan diantaranya FTK-Imager, Autopsy, Belkasoft, Xways Foresincs dan lainnya.

Berdasarkan studi literatur terdahulu diperoleh sebuah hasil dimana *tools* yang digunakan pada penelitian tersebut memiliki kesamaan yaitu Autopsy. Hasil uji performa yang didapat menggunakan *tools* tersebut sebesar 100% dengan ekstensi file yang berhasil direstorasi yaitu Pdf, Docx, Pptx, Txt, MP3, Iso, JPG dan PNG dengan jumlah keseluruhan 29 *file*. [15].

Penggunaan serta implementasi *framework* atau metode forensik dalam menyelesaikan kasus kejahatan digital merupakan aspek krusial dalam mendukung proses investigasi tindak kejahatan digitalagar lebih efektif dan efisien [13]. Metode atau *framework* yang umum digunakan pada storage seperti *National Institute Standard Technology* (NIST) akan mempermudah penelitian ini dalam mencari bukti digital yang akan dijadikan sebagai hasil temuan yang akan ditampilkan dalam tabel tersendiri. 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 Peneliti 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 enksirpsi 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. file.
Abdul Hadi, Imam Riadi, Sunardi (2019)	Forensik Bukti Digital Pada *Solid State Drive* (Ssd) Nvme Menggunakan Metode *National Institute Standards And Technology* (NIST) [18].	Fitur TRIM yang diaktifkan pada SSD berakibat tidak dapat dilakukannya proses akuisisi pada tools yang digunakan dan sebaliknya apabila fitur TRIM dinon-aktifkan, sebagian besar file dapat dipulihkan.

Hasil rangkuman diatas merupakan acuan yang digunakan dalam penelitian ini. Tujuan penelitian ini adalah melakukan analisis pada data yang terhapus pada sebuah DVD-R dengan dua tools forensik, yaitu FTK Imager dan Autopsy Windows ver.

2. Metode Penelitian

Implementasi metode yang sesuai prosedur dalam memperoleh bukti digital berupa data forensik akan memberikan dampak keberhasilan hingga 100% [19]. Pada penelitian ini menggunakan metode *National Institute of Standard and Technology* (NIST). metode ini menguraikan bagaimana tiap tahapan yang akan dilakukan sehingga dapat diketahui proses-proses dan alur penelitian sehingga dapat dijadikan acuan dalam

menyelesaikan masalah yang ditemukan pada penelitian ini. Langkah kerja forensik ini digunakan untuk menjabarkan tahapan- tahapan *forensics* yang akan dilakukan dan dapat diketahui alur-alur penelitian secara terstruktur, dan dapat menjadi acuan dalam menyelesaikan masalah-masalah yang ada. Tahapan NIST meliputi *collection, examination, analysis* dan *reporting* [20] seperti pada Gambar 2.

Gambar 2. Alur Proses Pada Metode NIST

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

a. *Collection*: Fase pertama dalam proses ini adalah untuk mengidentifikasi, memberi label, merekam, dan memperoleh data dari sumber yang mungkin dari data yang relevan, mengikuti pedoman dan prosedur yang menjaga integritas data.

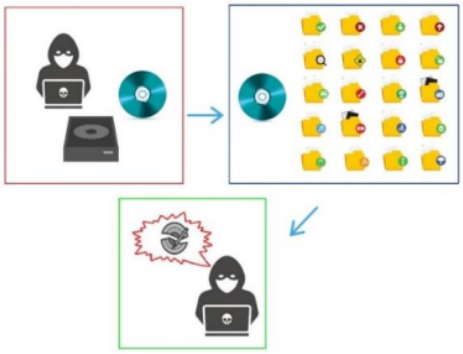
b. *Examination*: Pemeriksaan melibatkan pemrosesan forensik dalam jumlah besar data yang dikumpulkan dengan menggunakan kombinasi metode otomatis dan manual untuk menilai dan mengekstraksi data yang menarik, sambil menjaga integritas data.

c. *Analysis*: Menganalisis hasil pemeriksaan, menggunakan metode dan teknik yang dapat dibenarkan secara hukum, untuk memperoleh formasi yang berguna yang menjawab pertanyaan-pertanyaan yang menjadi dorongan untuk melakukan pengumpulan dan pemeriksaan.

d. *Reporting*: Pelaporan hasil analisis, yang dapat mencakup menggambarkan tindakan yang digunakan, menjelaskan bagaimana alat dan prosedur dipilih, menentukan tindakan apa yang perlu dilakukan (misalnya, pemeriksaan forensik sumber data tambahan, mengamankan kerentanan ng diidentifikasi, meningkatkan kontrol keamanan yang ada), dan memberikan rekomendasi untuk perbaikan kebijakan, pedoman, prosedur, alat, dan aspek lain dari proses forensik [21].

2.1. Skenario Kasus

Gambar 3 menampilkan skenario 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. Alur skenario kasus dimulai pada kotak merah pelaku melakukan *burning* data pada objek penelitian dengan menggunakan fitur *multisession* menggunakan aplikasi burner seperti 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 dengan menggunakan fitur format bawaan sistem operasi windows 10.



Gambar 3. Skenario Kasus Kejahatan Digital

"Seorang akuntan yang bernama Rio melakukan penggelapan dana perusahaan A, bukti penggelapan dana tersebut sudah disalin pada sebuah DVD-R dengan 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".

2.2 Alat dan Bahan

Alat dan bahan yang digunakan pada penelitian dapat dilihat pada Tabel 1.

Tabel 1. Alat dan Bahan

No	Nama Alat	Spesifikasi	Keterangan
1	Laptop	Acer E14, 10 GB DDR3L, 1 TB HDD	*Hardware*
2	Sistem Operasi	Windows 10 Pro	*Software*
3	DVD-R	DVD-R GT-Pro 4.7 GB	*Hardware*
4	DVD Writer Eksternal	Lite on	*Hardware*
5	FTK Imager	Ver. 3.4.3.3	Tools akuisisi
6	Autopsy	Ver. 4.10.0	Tools akuisisi
7	*Hash*MyFile	Ver. 2.36	Tools Validasi *Hash*
8	Microsoft Paint	-	Aplikasi Pengolah Gambar
9	Lucid Chart	App.lucidchart.com	Aplikasi Pengolah *Flowchar onlinet*

File asli sebagai acuan bukti digital pada penelitian ini seperti pada Tabel 2.

3. Hasil dan Pembahasan

Penelitian ini menggunakan skenario kasus dengan beberapa kondisi dimana membandingkan *tools* forensik dalam melakukan proses akuisisi data pada *optical disc* yaitu DVD-R yang sudah terformat Pada bagian ini menguraikan tiap tahapan pada metode yang digunakan yaitu *National Institute of Standard Technology* (NIST)

meliputi, *Collection*, *Examination*, *Analysis* dan *Reporting*.

Tabel 2. Bukti Digital pada DVD-R

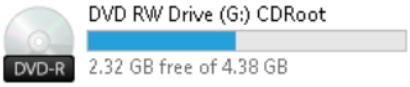
No	Nama dan Ekstensi	*Hash*
1	(Ab)normal Psychology –Susan Nolen-Hoeksema.pdf	be048922a3f94dc37737118b35d68c54
2	NetFx20SP1_x64.exe	4c07706a2ac5806944bc6a09c103bf9f
3	Nitro PDF 13 x64.rar	555ae498817fc142e997a2bce937b142
4	P1060241.MOV	8eafc525898cce468db7f04959699c7a
5	bmblbee.wb72_300mbfilms.com.mkv	3adc8979e8728b11e5c8e6ce2251f3f4
6	Body Mind Spirit_ Exploring the Parapsycho - Charles T. Tart.pdf	7cad82de07a7547d4fcccfab0131cc46
7	chessmaster2.bin	a5ece7e87ac96b2a31113a3ecb98491c
8	chessmaster2.cue	b442fe6a9d2024d464c2a5a2ae59f578
9	data_responden_1.xlsx	88f84652809d05bfca65f678bef115a7
10	Data_Responden_2.xlsx	c7b9e6b7c5bc71aa3cc62bc6f3c00d81

3.1. Collection

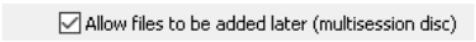
Gambar 4. Proses Tahapan Koleksi Data

Proses tahapan berdasarkan Gambar 4 yakni pengumpulan *data* yang akan dijadikan barang bukti digital pada DVD-R terdapat sejumlah *file* dengan

beragam ekstensi dan kapasitas yang memungkinkan mempercepat waktu akusisi data pada tahapan *examination*. Gambar 5 menunjukkan kapasitas sesudah di-*burning*. Aplikasi yang digunakan untuk *burning* ialah Nero StarSmart. Gambar 6 merupakan fitur *multisession* yang memungkinkan DVD-R dapat dilakukan proses penghapusan data setelah itu dilakukan proses penghapusan manual dimana sisa kapasitas DVD-R dapat diisi dengan file-file hingga penuh.



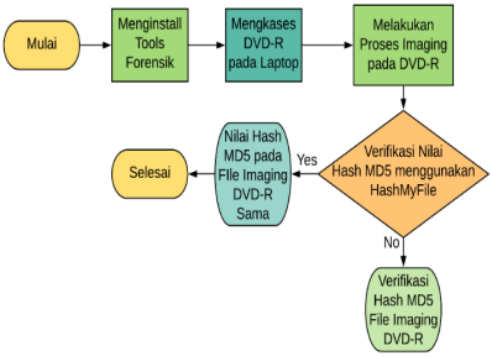
Gambar 5. Kapasitas Pada DVD-R



Gambar 6. Fitur *Multisession*

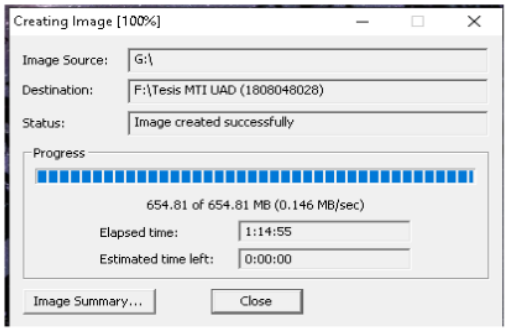
3.2. Examination

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 pencocokkan nilai *Hash* menggunakan aplikasi HashMyFile dan FTK Imager. Alur proses dapat dilihat pada Gambar 7.



Gambar 7. Tahapan Pemeriksaan

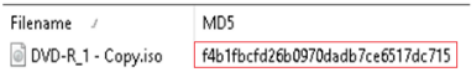
Proses imaging dilakukan untuk membuat salinan data sebagai bukti digital dari DVD-R yang ditemukan pada lokasi terjadinya kejahatan digital, seperti pada Gambar 8.



Gambar 8. Proses *Imaging* pada DVD-R

Setelah proses *imaging* selesai maka nilai *hash* pada hasil *image disk* dapat dilihat sebagai acuan keaslian sumber data, nilai *hash* dicocokkan dengan salinan *image disk* untuk mengetahui keaslian sumber data tersebut dengan tujuan menjaga keaslian sumber data yang digunakan dan menghindari perubahan secara fisik dan digital, Gambar 9 menampilkan nilai *hash* pada tools FTK Imager dan Gambar 10 menampilkan nilai *hash* pada aplikasi HashMyFile.

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

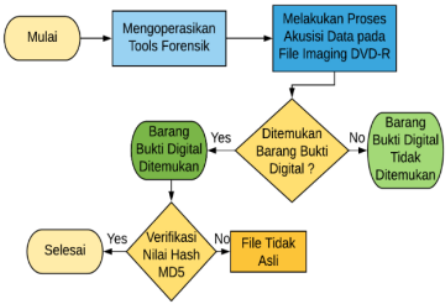


Gambar 10. Nilai *Hash image* kloning DVD-R Menggunakan Tools Hashmyfile

Hasil yang ditunjukkan pada Gambar 9 dan 10 menampilkan nilai *Hash* yang sama, jadi *Image file* DVD-R_1-Copy.iso dapat dijadikan sumber data yang sah untuk dilakukan proses akuisisi data menggunakan *tools* FTK Imager dan Autopsy.

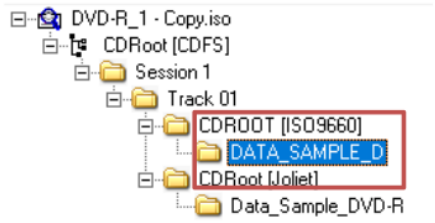
3.3. Analysis

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. Tahapan pada proses analisis ini dapat dilihat pada Gambar 10.



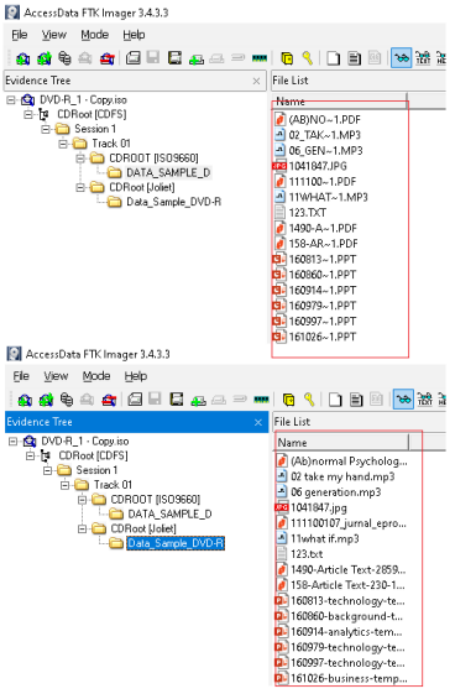
Gambar 11. Tahapan Analisis

Proses tahapan analisis seperti pada Gambar 11 menampilkan diagram alur, dimana proses akuisisi *data* pada *file image* DVD-R hingga ditemukkannya barang bukti digital serta validasi keaslian *file* dengan pencocokkan nilai *Hash*. Hasil temuan data dari proses akuisisi *data* menggunakan *tools* FTK Imager dan Autopsy. FTK Imager mendeteksi dua sistem file yang berbeda pada file Image DVD-R yakni ISO9660 dan Joliet, ditampilkan pada Gambar 12.



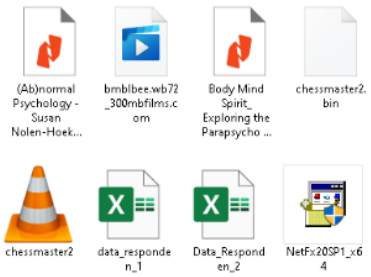
Gambar 12. Terdapat Dua Sistem File Dari Hasil Akuisisi

UDF bisa sama dengan ISO9660 ketika sistem file *read-only*, atau itu dapat memerlukan beberapa tingkat informasi alokasi ruang saat *disc* yang dapat *re-write*, UDF mengalokasikan ruang berdasarkan sektor per sektor. Ini dapat mengakibatkan fragmentasi tetapi biasanya tidak karena bagaimana ruang pada media yang dapat ditulis ulang digunakan. Secara umum, seluruh *disk* di*write* sebelum *space* yang dihapus "diperbaharui" untuk digunakan. Terdapat perbedaan yang cukup menonjol dari karakteristik kedua sistem file ini yakni pada penamaan yang dimana pada sistem file ISO9660 ada pembatasan karakter nama, perbedaan dapat dilihat pada Gambar 12 dan Gambar 13 untuk hasil ekstrasi.



Gambar 13. Perbedaan Sistem File JOLIET (Atas) Dan ISO9660 (Bawah)

Gambar 13 menampilkan perbedaan dalam penamaan pada masing-masing file sistem yang dideteksi oleh tools FTK Imager. Gambar 14 menunjukkan hasil ekstrasi dari tools FTK Imager.



Gambar 14. Hasil Ekstrasi Tools Forensik

Validasi dilakukan untuk mengetahui keaslian sebuah *file* dari proses akuisisi sampai *file* tersebut diekstraksi, dilakukan pencocokkan nilai *Hash* sebagai acuan dari *hash file* asli sebelum terhapus, agar dari hasil ekstrasi tersebut diketahui *file* yang mana saja memiliki kesamaan nilai *Hash*. Setelah proses pencocokkan nilai *Hash* dilakukan maka *file* yg memiliki nilai *hash* yang sama akan dijadikan bukti digital yang sah secara hukum. Tabel 3 menunjukkan hasil pencocokkan nilai *Hash* dari *tools* FTK Imager dan HashMyFile seperti berikut.

Tabel 3. Validasi *Hash* Tools Ftk Imager Sistem File ISO9660

File Name	FTK Imager	Validasi
(AB)NO~1.PDF	be048922a3f94dc377371 18b35d68c54	Valid
NETFX2~1.EXE	4c07706a2ac5806944bc 6a09c103bf9f	Valid
NITRO_~1.RAR	555ae498817fc142e997a 2bce937b142	Valid
P1060241.MOV	8eafc525898cce468db7f 04959699c7a	Valid
BMBLBE~1.MKV	3adc8979e8728b11e5c8e 6ce2251f3f4	Valid
BODY_M~1.PDF	7cad82de07a7547d4fccc fab0131cc46	Valid
CHESSM~1.BIN	a5ece7e87ac96b2a31113 a3ecb98491c	Valid
CHESSM~1.CUE	b442fe6a9d2024d464c2a 5a2ae59f578	Valid
DATA_R~1.XLS	88f84652809d05bfca65f 678bef115a7	Valid
DATA_R~1.XLS	c7b9e6b7c5bc71aa3cc62 bc6f3c00d81	Valid

Tabel 3 menunjukkan *file* yang berhasil diekstrasi tidak ada perubahan nilai *Hash*, dapat disimpulkan semua *file* valid dan layak dijadikan bukti digital yang sah. Pada

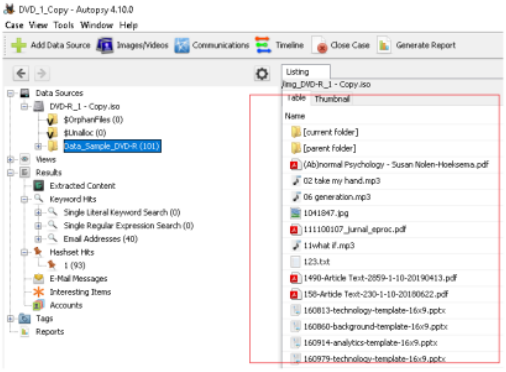
Tabel 4 dilanjutkkan proses pencocokkan nilai *Hash* pada sistem file yang berbeda yaitu Joliet, dimana jumlah *file* yang diekstraksi sama banyaknya, dapat dilihat pada Tabel 4.

Tabel 4 menunjukkan sebanyak 10 *file* tidak ada perubahan pada nilai *Hash*, dapat disimpulkan bahwa semua *file* asli karena kesamaan nilai *Hash*.

Tabel 4. Validasi *Hash* Tools Ftk Imager Sistem File Joliet

File Name	FTK Imager	Validasi
(Ab)normal Psychology – Susan Nolen-Hoeksema.pdf	be048922a3f94dc37 7371 18b35d68c54	Valid
NetFx20SP1_x64.exe	4c07706a2ac580694 4bc6a09c103bf9f	Valid
Nitro PDF 13 x64.rar	555ae498817fc142e 997a2bce937b142	Valid
P1060241.MOV	8eafc525898cce468 db7f04959699c7a	Valid
bmblbee.wb72_300mbfilms.com.mkv	3adc8979e8728b11e 5c8e6ce2251f3f4	Valid
Body Mind Spirit_ Exploring the Parapsycho - Charles T. Tart.pdf	7cad82de07a7547d4 fcccfab0131cc46	Valid
chessmaster2.bin	a5ece7e87ac96b2a3 1113a3ecb98491c	Valid
chessmaster2.cue	b442fe6a9d2024d46 4c2a5a2ae59f578	Valid
data_responden_1.xlsx	88f84652809d05bfc a65f678bef115a7	Valid
Data_Responden_2.xlsx	c7b9e6b7c5bc71aa3 cc62bc6f3c00d81	Valid

Proses akuisisi dilakukan pada *tools* kedua yakni Autopsy merupakan *tools* umum bagi investigator dalam melakukan akuisisi pada *storage*. Pada Gambar 15 menampilkan *file* hasil temuan *tools* Autopsy.



Gambar 15. Hasil Temuan pada *tools* Autopsy

Gambar 16. Hasil Ekstrasi Bukti Digital Menggunakan Autopsy

Dari hasil dari ekstrasi *file* pada Gambar 16 kemudian dilakukan proses validasi keaslian dengan pencocokkan nilai *Hash* menggunakan *tools* Autopsy dan HashMyFile berikut hasil nya pada Tabel 5.

Tabel 5 menunjukkan 3 *file* yang tidak dapat diakuisisi dan *file* lain tidak menunjukkan perubahan pada nilai *Hash* setelah dicocokkan dengan nilai *Hash* dari aplikasi

HashMyFile. Selain itu ekstensi *file* tertentu tidak dapat di*recovery*.

Tabel 5. Validasi *Hash* Tools Autopsy

Nama File	Autopsy	Validasi
9-(Ab)normal Psychology - Nolen-Hoeksema.pdf	be048922a3f94dc37737118b35d68c54	Valid
NULL	NULL	Tidak Valid
NULL	NULL	Tidak Valid
NULL	NULL	Tidak Valid
195-bmblbee.wb72_300mbfilms.com.mkv	3adc8979e8728b11e5c8e6ce2251f3f4	Valid
197-Body Mind Spirit_ Exploring the Parapsycho – Charles T. Tart.pdf	7cad82de07a7547d4fcccfab0131cc46	Valid
199-chessmaster2.bin	a5ece7e87ac96b2a31113a3ecb98491c	Valid
201-chessmaster2.cue	b442fe6a9d2024d464c2a5a2ae59f578	Valid
203-data_responden_1.xlsx	88f84652809d05bfca65f678bef115a7	Valid
205-Data_Responden_2.xlsx	c7b9e6b7c5bc71aa3cc62bc6f3c00d81	Valid

3.4. Repoting

Dari hasil pada tahapan analisis, diketahui pada *tools* FTK Imager menunjukkan hasil validasi dan ekstrasi *file* yang sama dalam artian nilai *hash* dan jumlah filenya sebanyak 10 file pada kedua sistem file yang terdeteksi seperti pada Tabel 3 dan 4. *Tools* berikutnya yakni Autopsy menunjukan pada Tabel 5 nilai *hash* yang valid dari 7 *file* dari total akuisisi data yaitu 10 *file*. Dari kedua *tools* yang digunakan FTK Imager lah yang dapat melakukan akuisisi data menyeluruh pada DVD-R, berikut hasil perbandingan pada Tabel 6.

Tabel 6. Hasil Perbandingan Tools

Ekstensi	Total	FTK Imager		Autopsy
		Sistem File		
		ISO9660	Joliet	UDF
*.pdf	2	2	2	2
*.exe	1	1	1	0
*.rar	1	1	1	0
*.MOV	1	1	1	0
*.bin	1	1	1	1
.xls/.xlsx	2	2	2	2
*.cue	1	1	1	1
*.mkv	1	1	1	1
Jumlah file yang berhasil di akuisisi		10	10	7

Tabel 6 menunjukkan jumlah file yang berhasil diakuisisi dari tiap *tools* yang digunakan, untuk memperoleh hasil persentase uji performa dari tools tersebut maka digunakan rumus perhitungan (1).

$$\frac{\sum a}{\sum n} X\ 100\% \qquad (1)$$

$\sum a$= Jumlah File yang berhasil diakuisisi
$\sum n$ =Jumlah File Asli

Berdasarkan rumus perhitungan diatas maka hasil persentase uji performa dapat dilihat pada Tabel 7.

Tabel 7. Persentase Uji Performa Tools Forensik

FTK Imager	Autopsy
100%	70%

Hasil dari Tabel 7 menunjukkan bahwa FTK Imager memperoleh persentase uji performa 100% dan Autopsy 70%. Dapat disimpulkan bahwa FTK Imager yang berhasil melakukan akuisisi data secara keseluruhan.

4. Kesimpulan

Berdasarkan hasil yang diperoleh dari tahapan analisis dan presentasi dapat disimpulkan dari 10 file asli dilakukan akuisisi data menggunakan tools FTK Imager dan Autopsy pada DVD-R yang sudah terformat. FTK Imager mendeteksi 2 sistem file yaitu ISO9660 dan Joliet sedangkan *tools* Autopsy hanya 1 sistem *file* yaitu UDF. Hasil Tabel 6, menunjukkan hasil temuan pada *tools* FTK Imager terdapat 10 *file* dengan dengan nilai *hash* yang cocok. *Tools* Autopsy mendeteksi 7 *file* dan tidak menemukan 3 *file* dengan ekstensi, *.MOV, *.exe, *.rar. Berdasarkan Hasil dari Tabel 7 analisis komparatif uji performa yang dilakukan pada FTK Imager memberikan nilai keberhasilan 100% karena berhasil menemukan seluruh file yang terhapus dan Autopsy memberikan nilai keberhasilan 70% sebab 3 file tidak terdeteksi serta nilai hash yang kosong dengan ekstensi *.exe, *.rar dan *.MOV. Hal ini dikarenakan tools Autopsy tidak dapat mendeteksi ketiga ekstensi file tersebut.

Daftar Rujukan

[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 disks". *In Computer science* (pp. 189-207). Springer, Boston, MA. 1992.
[8] Coughlin "Media Drives 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] 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] A. Hadi, I. Riadi, and Sunardi, "Forensik Bukti Digital Pada Solid State Drive (SSD) NVMe Menggunakan Metode National Institute of Standards and Technology (NIST)," *Semnastek* 2019, pp. 551–558, 2019.
[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.
[21] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," *Natl. Inst. Stand. Technol.*, 2006.

HASIL CEK_60020397_C44-Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST)

ORIGINALITY REPORT

10%	9%	5%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	doku.pub Internet Source	2%
2	jurnal.upnyk.ac.id Internet Source	2%
3	Muhammad Irwan Syahib, Imam Riadi, Rusydi Umar. "Akuisisi Bukti Digital Aplikasi Viber Menggunakan Metode National Institute of Standards Technology (NIST)", J-SAKTI (Jurnal Sains Komputer dan Informatika), 2020 Publication	2%
4	www.researchgate.net Internet Source	2%
5	publikasiilmiah.unwahas.ac.id Internet Source	1%
6	jtiik.ub.ac.id Internet Source	1%
7	kinetik.umm.ac.id	

Internet Source

1%

8 www.forbes.com

Internet Source

1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		