

Analisis Computer Forensic Untuk Mendukung Prosesnya Penyelidikan Dalam Kasus Kejahatan

Computer Forensic Analysis To Support The Process Of Investigation In Crime Cases

Ronaldo Herman YP^{a,1}, Budi Triadi^{b,2}

^aMahasiswa Universitas Potensi Utama, Jl.Medan Marelan Psr IV Lk 27, Medan, 20255, Indonesia

^b Dosen Universitas Potensi Utama, Jl.Teluk Aru Martubung, Medan, 20252, Indonesia
yudaaldo34@gmail.com¹, buditriandi.pbm@gmail.com²

ABSTRAK

Beberapa tahap yang dilakukan Polres Tapanuli Utara dalam menyidik kasus seperti mengidentifikasi kasus, mengumpulkan barang bukti hingga pelaporan hasil analisis kasus. Tujuan penelitian untuk mengetahui prosedur yang berkaitan dengan penyelidikan kasus kejahatan digital forensic dan untuk mengetahui efektivitas dan efisiensi aplikasi forensik dalam menganalisis barang bukti. Kesimpulan penelitian: (a). Mengamankan barang bukti dengan Chain of Custody (COC) merupakan prosedur yang penting dalam digital forensic; (b). Framework National Institute of Justice (NIJ) menjadi prosedur penyelidikan dan pemecahan masalah dalam proses investigasi barang bukti digital pada kasus kejahatan dengan 5 tahap; (c). Software FTK Imager sebagai aplikasi untuk menduplikasi data barang bukti memiliki kinerja yang baik, serta software Autopsy sebagai aplikasi untuk memeriksa dan memulihkan data barang bukti memiliki kinerja yang baik, dan (d). Upaya dapat dilakukan Polres Tapanuli Utara untuk mengatasi hambatan dalam penerapan digital forensic terhadap penyelidikan cybercrime, yaitu mengadakan pelatihan di bidang informasi dan transaksi elektronik yang bersertifikasi terhadap Penyelidik.

Kata Kunci : Digital forensik, Autopsy, FTK imager

ABSTRACT

Several steps were carried out by the North Tapanuli Police in investigating cases such as identifying cases, collecting evidence and reporting the results of case analysis. The aim of this research is to find out the procedures related to the investigation of digital forensic crime cases and to find out the effectiveness and efficiency of forensic applications in analyzing evidence. Research conclusions: (a). Securing evidence with a Chain of Custody (COC) is an important procedure in digital forensics; (b). The National Institute of Justice (NIJ) Framework is a procedure for investigating and solving problems in the process of investigating digital evidence in crime cases with 5 stages; (c). FTK Imager software as an application for duplicating evidence data has good performance, and Autopsy software as an application for checking and recovering goods data has good performance, and (d). Efforts can be made by the North Tapanuli Police to overcome obstacles in the application of digital forensics to cybercrime investigations, namely holding training in the field of information and electronic transactions that are certified for investigators.

Keywords : Digital forensik, Autopsy, FTK imager

Disubmit: 21 Juni 2023

Info Artikel :
Direview: 03 Juli 2023

Diterima : 12 Agustus 2023

Copyright © 2023 - Journal UPU. All rights reserved.

1. PENDAHULUAN

Dengan berkembangnya *cybercrime* maka penanganan kasus kejahatan dunia maya dilakukan melalui kegiatan investigasi yang dikenal sebagai forensik digital. forensik digital adalah prosedur investigasi kejahatan komputer di dunia *cyber* [1]. Definisi awal forensik digital sebagai penggunaan metode yang diturunkan secara ilmiah dan terbukti terhadap pelestarian, pengumpulan, validasi, identifikasi, analisis, interpretasi, dokumentasi, dan penyajian bukti digital yang berasal dari digital

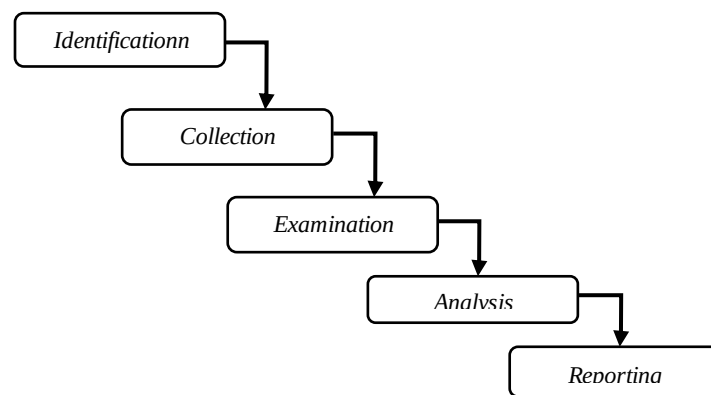
sumber untuk tujuan fasilitasi atau memajukan rekonstruksi peristiwa yang dianggap kriminal, atau membantu mengantisipasi tindakan yang tidak sah yang terbukti mengganggu operasi yang direncanakan [2].

Salah satu penegak hukum yakni Polres Tapanuli Utara yang berada di Provinsi Sumatra Utara tepatnya di Kabupaten Tapanuli Utara yang juga menanganani berbagai kasus salah satunya kasus *cybercrime*. Polres Tapanuli Utara menjadi tempat penelitian untuk melihat bagaimana proses penyidikan *cybercrime* dengan *digital forensic*. Beberapa tahap yang dilakukan Polres Tapanuli Utara dalam menyidik kasus seperti mengidentifikasi kasus, mengumpulkan barang bukti hingga pelaporan hasil analisis kasus. Untuk melihat bagaimana prosedur penyidikan kasus *cybercrime* serta menganalisis barang bukti yang biasanya dilakukan oleh ahli *digital forensic*, maka penulis sangat tertarik mengambil judul “Analisis Computer Forensic Untuk Mendukung Prosesnya Penyelidikan Dalam Kasus Kejahatan”.

2. METODE

Analisa bertujuan untuk mengidentifikasi permasalahan-permasalahan yang ada pada sistem serta menentukan kebutuhan dari sistem yang dibangun. Salah satu penegak hukum yakni Polres Tapanuli Utara yang berada di Provinsi Sumatra Utara tepatnya di Kabupaten Tapanuli Utara yang juga menanganani berbagai kasus salah satunya kasus *cybercrime*. Tujuan dari penelitian ini adalah untuk membantu Polres Tapanuli Utara dalam proses penyidikan *digital forensic* dengan menganalisis barang bukti dalam rancangan kasus menggunakan Autopsy dengan metode *framework National Institute of Justice* (NIJ).

Pada penelitian ini, peneliti menggunakan metode *framework National Institute of Justice* (NIJ) sebagai pedoman dalam melakukan proses investigasi barang bukti digital terdiri dari lima tahapan, antara lain: *identification*, *collection*, *examination*, *analysis*, dan *reporting* [3].



Gambar 1. Tahapan proses framework National Institute of Justice (NIJ)

Berikut ini penjelasan dari tahapan proses *framework National Institute of Justice* (NIJ), yaitu:

- a) *Identification* yakni tahap untuk mengidentifikasi segala bukti-bukti yang mendukung penyelidikan dikumpulkan [4].

- b) *Collection* yakni tahapan yang mencakup penyimpanan dan penyiapan bukti-bukti yang ada, termasuk melindungi bukti-bukti dari kerusakan, perubahan dan penghilangan oleh pihak-pihak tertentu [5].
- c) *Examination* yakni tahapan ekstraksi hasil *image* sehingga data digital yang ada didalamnya sama dengan barang bukti fisik [6].
- d) *Analysis* yakni melakukan analisa secara mendalam terhadap bukti-bukti yang ada. Bukti yang telah didapatkan perlu di-*explore* kembali ke dalam sejumlah skenario yang berhubungan dengan tindak pengusutan, antara lain: siapa yang telah melakukan, apa yang telah dilakukan [7].
- e) *Reporting* yakni proses pembuatan laporan, hasil laporan analisis menggambarkan tindakan yang dilakukan oleh pelaku kriminal, penjelasan *tools* yang dipakai dan metode yang digunakan [8].

A. Kebutuhan Hardware dan Software

Dalam analisis *computer forensic* untuk mendukung prosesnya penyelidikan dalam kasus kejahatan dibutuhkan beberapa *hardware* dan *software*, antara lain sebagai berikut:

- a) *Personal Computer* (Komputer)/Laptop
Spesifikasi *hardware* yang digunakan sebagai berikut:
 - a. *Processor: Core i3*
 - b. *Memory: 16 GB*
 - c. *SSD: 512 GB*
- b) *Hardware Flashdisk*
Spesifikasi *hardware* yang digunakan sebagai berikut:
 - a. *Memory: 30GB*
 - b. *Merk: Kingston DataTraveler*
- c) *Software* (aplikasi perangkat lunak)
Spesifikasi *Software* yang digunakan sebagai berikut:
 - a. *Sistem Operasi: Windows 10 Pro*
 - b. *Autopsy 4.19.3*
 - c. *FTK Imager 4.5.0.3*

B. Rancangan Kasus

Penyusunan dan implementasi skenario dilakukan untuk merekonstruksi aksi relevan yang mungkin dapat dilakukan oleh pelaku tindakan kriminal. Penelitian ini menggunakan skenario kasus kejahatan prostitusi dan pornografi, menurut pasal 112 KUHP tidak diperkenankan menggunakan kasus asli dalam melakukan penelitian ilmiah karena catatan kasus kejahatan bersifat sangat rahasia.

Penyusunan skenario disusun berdasarkan analisis fungsionalitas dari *software* Autopsy dan referensi terkait. Skenario mencakup dari data dan informasi pada *flashdisk* yang memiliki potensi untuk digunakan sebagai media tindakan kriminal dan dapat digunakan untuk menutupi jejak tindakan kriminal, antara lain:

- a. Terjadinya kasus transaksi prostitusi dan pornografi yang melibatkan tersangka M diamankan oleh Polres Tapanuli Utara.
- b. Polres Tapanuli Utara menemukan barang bukti berupa *flasdisk*.
- c. Polres Tapanuli Utara menyimpan barang bukti berupa *flasdisk*
- d. Namun tersangka M telah menghapus sebagian barang bukti pada *flasdisk* seperti gambar, video ataupun rekaman suara oleh tersangka M.

Pada rancangan kasus ini, barang bukti *flashdisk* sebelum melakukan penghapusan data memiliki 40 total file dengan jenis file gambar, video, audio, dan dokumen dengan ekstensi berbeda pada barang bukti *flashdisk*, seperti pada gambar berikut ini:



Gambar 2. Data Flashdisk

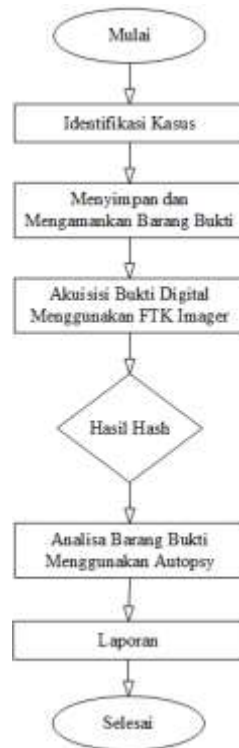
Table 1. Total Data Pada Flashdisk

Informasi Barang Bukti	
No. Kasus	001
Nama Pemilik	Tersangka M
Jenis Barang Bukti	Flashdisk
Merek	Data Travel
Kapasitas	28 Gigabyte
Sumber Bukti Digital	
Jenis Data	Jumlah
JPG	12
PNG	11
MP4	6
AVI	5
MP3	4
DOCX	1
PDF	1
Total	40

Polres Tapanuli Utara melakukan analisa barang bukti berupa *flasdisk*, dengan mencari data yang terhapus atau hilang

C. Skenario Pembuktian

Dalam melakukan suatu penyidikan untuk mengungkap kasus kejahatan komputer seorang penyidik harus mengetahui langkah-langkah yang harus diambil dalam tiap penyidikannya. Hal tersebut dilakukan untuk dapat menemukan bukti-bukti yang akurat. Dalam tiap tahapan penyidikan, tiap langkah harus dilakukan secara seksama dan teliti agar tidak terjadi kesalahan dalam penanganannya. Adapun gambaran skenario pembuktian pada kasus ini yaitu *flowchart* yang dimana berfungsi sebagai alur pembuktian barang bukti pada penelitian ini, sebagai berikut:



Gambar 3. Skenario Pembuktian Studi Kasus

3. HASIL DAN PEMBAHASAN

A. Prosedur Investigasi

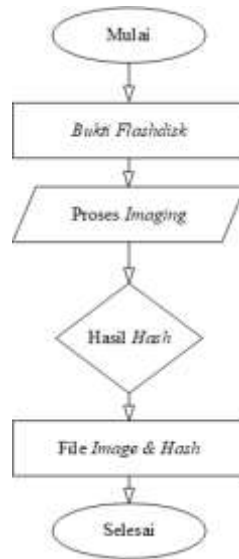
Salah satu prosedur dalam digital forensik adalah mengamankan barang bukti [9]. Barang bukti menjadi penting dalam suatu proses investigasi demi pengungkapan kasus [10]. Mengamankan barang bukti dengan *Chain of Custody* (COC) berupa data-data yang sudah diinputkan oleh *Investigator* dan *First Responder* [11]. Tidak hanya data yang diinputkan saja tetapi juga hasil dari *Image Processing* yang berupa data tersembunyi dari gambar yang dijadikan barang bukti.

Dalam penelitian ini, menggunakan sebuah studi kasus untuk membantu Polres Tapanuli Utara dalam proses penyidikan *digital forensic* yakni dengan skenario terjadinya kasus transaksi prostitusi dan pornografi yang melibatkan tersangka M dengan barang bukti berupa *flashdisk*. Namun tersangka M menghapus sebagian isi dari barang bukti tersebut. Barang bukti yang sudah diamankan Polres Tapanuli Utara yang kemudian akan ditindaklanjuti untuk menelusuri dan menemukan data barang bukti yang telah dihapus.

B. Analisa Bukti Digital

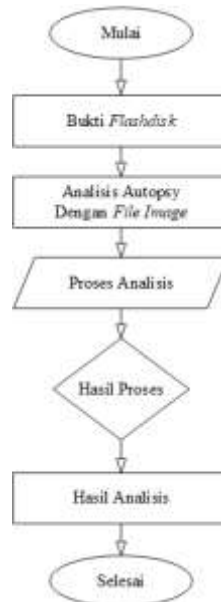
Analisa bukti digital dalam penelitian ini menggunakan *Framework National Institute of Justice* (NIJ) sebagai metode sebagai prosedur penyelidikan dan pemecahan masalah dalam proses investigasi barang bukti digital pada kasus kejahatan pornografi dan prostitusi dalam penelitian ini serta penggunaan *software* yang digunakan untuk menganalisis barang bukti yakni FTK Imager dan Autopsy.

Software FTK Imager digunakan untuk melakukan *imaging* data serta membandingkan *hashing file image* dengan bukti elektronik *flash disk* digunakan untuk menganalisis hasil *imaging* dari *flash disk*. Skenario atas *imaging flash disk* ditunjukkan gambar berikut ini:



Gambar 4. Flowchart Imaging Barang Bukti Dengan FTK Imager

Sementara *software* Autopsy digunakan untuk melakukan analisis barang bukti untuk mencari barang bukti yang telah hilang atau dihapus. Skenario analisis Autopsy pada barang bukti digital ditunjukkan gambar berikut ini:



Gambar 5. Analisa Barang Bukti Dengan Autopsy

Berikut ini adalah tahapan analisa bukti digital *flashdisk* menggunakan *Framework National Institute of Justice* (NIJ) pada tahapan dibawah ini, sebagai berikut:

a) Identification

Pada penelitian Polres Tapanuli Utara menyita barang bukti dari tersangka M berupa *flasdisk* yang diduga sebagai bukti transaksi pornografi. Barang bukti *flasdisk* menjadi bukti otentik saat proses penyidikan yang berisi bukti berupa gambar, suara video dan *file* dokumen.

Tabel 2. Spesifikasi Barang Bukti

Spesifik Barang Bukti	
Nama Barang Bukti	Spesifikasi
Nama Pemilik : Tersangka M	- Merek Kingston
Nama Barang Bukti : <i>Flashdisk</i>	- Seri DataTraveler
	- Kapasitas 32 GB
	- Port USB 2.0
	- <i>Stylish sliding cap design</i>
	- Dimesnsi produk : 69.62 x 22.14 x 12.76 mm
	- OS support : Win 10/8.1/8/7; Mac OS (v. 10.10x+); Linux (v.2.6.x+)



b) *Collection*

Pada tahap pengumpulan target yang akan dipulihkan adalah *flashdisk* berkapasitas 32 GB yang didalamnya terdapat *file* yang menjadi barang bukti digital yang akan dihapus sesuai scenario kasus. Dalam tahapan pengumpulan *file* yang hilang sebagian data akan dihapus oleh tersangka M sebelum akan melakukan *file image* dari hasil *imaging FTK Imager*. Pada pengumpulan barang bukti sebelum dihapus seperti scenario kasus, *flashdisk* memiliki barang bukti berupa 12 JPG, 11 PNG, 6 MP4, 5 AVI, 4 MP3, 1 DOCX dan 1 PDF yang merupakan data PSK yang bekerja dibawah naungan tersangka M. Dengan demikian data pada barang bukti berupa gambar, video, audio, dan dokumen dengan ekstensi berbeda yang total keseluruhannya adalah 40 *file*, yang dijabarkan detailnya pada tabel dibawah ini:

Tabel 3. Spesifikasi Data Pada *Flashdisk*

Spesifikasi Data Pada <i>Flashdisk</i>					
No.	Nama File	Jenis File	No.	Nama File	Jenis File
1	JPG_Agnes_Bandung	JPG	21	MP3 (2)	MP3
2	JPG_Amy_Batam	JPG	22	MP3 (3)	MP3
3	JPG_Ayu_Jakarta	JPG	23	MP3 (4)	MP3
4	JPG_Dwi_Bandung	JPG	24	MP4 (1)	MP4
5	JPG_Feni_Jakarta	JPG	25	MP4 (2)	MP4
6	JPG_Fiona_Bandung	JPG	26	MP4 (3)	MP4
7	JPG_Mei_Medan	JPG	27	MP4 (4)	MP4
8	JPG_Rina_Bali	JPG	28	MP4 (5)	MP4
9	JPG_Rina_Bandung	JPG	29	MP4 (6)	MP4
10	JPG_Rini_Jakarta	JPG	30	Png (1)	PNG
11	JPG_Tika_Medan	JPG	31	Png (2)	PNG
12	JPG_Yani_Jakarta	JPG	32	Png (3)	PNG

13	CEWE MAMI	DOCX	33	Png (4)	PNG
14	CEWE MAMI	PDF	34	Png (5)	PNG
15	Avi (1)	AVI	35	Png (6)	PNG
16	Avi (6)	AVI	36	Png (7)	PNG
17	Avi (7)	AVI	37	Png (8)	PNG
18	Avi (8)	AVI	38	Png (9)	PNG
19	Avi (9)	AVI	39	Png (10)	PNG
20	MP3 (1)	MP3	40	Png (11)	PNG
Total :		40 file			

Kemudian memberlakukan tahap selanjutnya dari rancangan kasus yakni tersangka M telah menghapus sebagian barang bukti pada *flasdisk* seperti gambar, video ataupun rekaman suara oleh tersangka M. Data yang tersisa pada *flashdisk* setelah di hapus bertotal 18 *file* dengan menghapus 22 *file*, seperti pada gambar berikut ini:



Gambar 6. Total Data Terakhir Pada *Flashdisk*

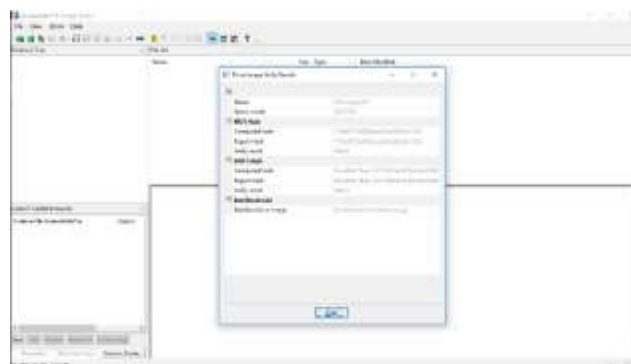
Tabel 4. Status Data Pada *Flashdisk*

Data Tidak Dihapus				Data Dihapus			
No.	Nama File	Jenis File	Status File	No	Nama File	Jenis File	Status File
1	AVI (1)	AVI	Tidak Dihapus	19	AVI (7)	AVI	Dihapus
2	AVI (6)	AVI	Tidak Dihapus	20	AVI (9)	AVI	Dihapus
3	AVI (8)	AVI	Tidak Dihapus	21	JPG_Agnes_Bandung	JPG	Dihapus
4	JPG_Dwi_Bandung	JPG	Tidak Dihapus	22	JPG_Amy_Batam	JPG	Dihapus
5	JPG_Fiona_Bandung	JPG	Tidak Dihapus	23	JPG_Ayu_Jakarta	JPG	Dihapus
6	JPG_Mei_Medan	JPG	Tidak Dihapus	24	JPG_Feni_Jakarta	JPG	Dihapus
7	JPG_Tika_Medan	JPG	Tidak Dihapus	25	JPG_Rina_Bali	JPG	Dihapus
8	MP3 (1)	MP3	Tidak Dihapus	26	JPG_Rina_Bandung	JPG	Dihapus

9	MP3 (2)	MP3	Tidak Dihapus	27	JPG_Rini_Jakarta	JPG	Dihapus
10	MP4 (1)	MP4	Tidak Dihapus	28	JPG_Yani_Jakarta	JPG	Dihapus
11	MP4 (2)	MP4	Tidak Dihapus	29	MP4 (3)	MP4	Dihapus
12	MP4 (4)	MP4	Tidak Dihapus	30	MP4 (5)	MP4	Dihapus
13	Png (1)	PNG	Tidak Dihapus	31	Png (2)	PNG	Dihapus
14	Png (3)	PNG	Tidak Dihapus	32	Png (5)	PNG	Dihapus
15	Png (4)	PNG	Tidak Dihapus	33	Png (6)	PNG	Dihapus
16	Png (5)	PNG	Tidak Dihapus	34	Png (8)	PNG	Dihapus
17	Png (7)	PNG	Tidak Dihapus	35	Png (10)	PNG	Dihapus
18	Png (9)	PNG	Tidak Dihapus	36	Png (11)	PNG	Dihapus
Total		18		37	CEWE MAMI	DOCX	Dihapus
				38	CEWE MAMI	PDF	Dihapus
				39	MP3 (3)	MP3	Dihapus
				40	MP3 (4)	MP3	Dihapus
				Total		22	

c) Examination

Pada tahap *examination* adalah pemeriksaan data yang ada pada barang bukti *flashdisk* dari tindak kejahatan prostitusi dan pornografi dapat terlaksana dengan melakukan proses akuisisi data yang ada pada *flashdisk* tersebut [12]. Tahapan ini memastikan data yang didapat asli dan akan dicek validasinya dengan menggunakan *hashing* [13]. Setelah melakukan tahap *collection* selanjutnya melakukan *examination* untuk mendapatkan *full image* dari *flashdisk*. *Software* FTK Imager digunakan untuk melakukan *imaging* data serta membandingkan *hashing file image* dengan bukti elektronik *flash disk* dan Autopsy digunakan untuk menganalisis hasil *imaging* dari *flash disk*. Proses *imaging* data dengan FTK Imager pada *flashdisk* sebagaimana gambar dibawah ini:

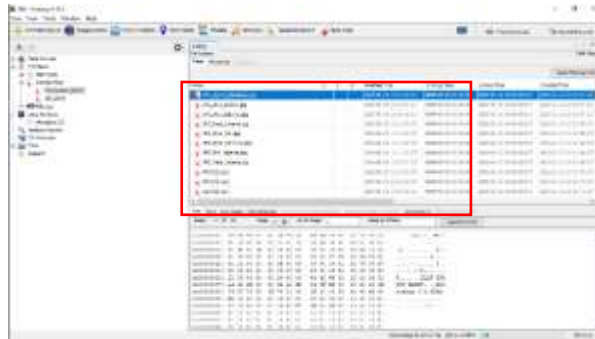


Gambar 7. Hasil Examination Dengan FTK Imager

d) Analysis

Tahap *analysis* atau tahap meneliti ini dilakukan setelah mendapatkan *file imaging* dari FTK Imager, selanjutnya data tersebut dianalisis secara detail dan komprehensif dengan Autopsy. Pada tahap ini bertujuan untuk memeriksa, menemukan serta pemulihan data yang telah dihapus

tersangka M. Setelah melakukan proses penyimpanan kasus untuk barang bukti, Autopsy akan melakukan analisis pada *flashdisk*, seperti pada gambar berikut ini:



Gambar 8. Tampilan Bukti Data Yang Telah Dihapus

Pada analisis ini, hasil akuisisi imaging dengan FTK Imager menjadi sumber data yang digunakan dalam analisis dengan Autopsy. *File* yang hilang atau sengaja dihapus oleh Tersangka M dapat ditemukan kembali dalam menu sub "*Delete Item*". *File-file* yang sudah lama terhapus sebelumnya juga terdeteksi pada aplikasi Autopsy, hal ini menunjukkan bahwa aplikasi Autopsy dinilai mampu dalam membantu Petugas Kepolisian dalam mencari bukti yang hilang maupun sengaja dihapus pada sebuah barang bukti.

Tabel 5. Persentase Kinerja Aplikasi

Persentase Kinerja Aplikasi		
Nama Software	Persentase Kinerja	Kecepatan Analisis
Autopsy 4.19.3	98,5%	15' 23"
FTK Imager 4.5.0.3	99,5%	20' 25"

Berikut ini kesimpulan pada hasil analisis *flashdisk* untuk mendapatkan pada tabel berikut ini:

Tabel 6. Hasil Analisis Data Yang Dihapus Pada Autopsy

Data Dihapus				
No	Nama File	Jenis File	Status File	Status File Autopsy
1	AVI (7)	AVI	Dihapus	Ditemukan
2	AVI (9)	AVI	Dihapus	Ditemukan
3	JPG_Agnes_Bandung	JPG	Dihapus	Ditemukan
4	JPG_Amy_Batam	JPG	Dihapus	Ditemukan
5	JPG_Ayu_Jakarta	JPG	Dihapus	Ditemukan
6	JPG_Feni_Jakarta	JPG	Dihapus	Ditemukan
7	JPG_Rina_Bali	JPG	Dihapus	Ditemukan
8	JPG_Rina_Bandung	JPG	Dihapus	Ditemukan
9	JPG_Rini_Jakarta	JPG	Dihapus	Ditemukan
10	JPG_Yani_Jakarta	JPG	Dihapus	Ditemukan
11	MP4 (3)	MP4	Dihapus	Ditemukan
12	MP4 (5)	MP4	Dihapus	Ditemukan
13	Png (2)	PNG	Dihapus	Ditemukan
14	Png (5)	PNG	Dihapus	Ditemukan
15	Png (6)	PNG	Dihapus	Ditemukan
16	Png (8)	PNG	Dihapus	Ditemukan
17	Png (10)	PNG	Dihapus	Ditemukan
18	Png (11)	PNG	Dihapus	Ditemukan
19	CEWE MAMI	DOCX	Dihapus	Ditemukan
20	CEWE MAMI	PDF	Dihapus	Ditemukan

21	MP3 (3)	MP3	Dihapus	Ditemukan
22	MP3 (4)	MP3	Dihapus	Ditemukan
Total		22		

Setelah semua rancangan kasus dalam penelitian ini dilakukan, *software* Autopsy dinilai mampu untuk membantu ahli digital forensik dikarenakan kemampuannya dalam memeriksa, mencari serta memulihkan *file* dengan persentase kebenaran yang baik. Sementara *software* FTK Imager dinilai mampu dalam menjaga keaslian bukti digital dengan persentase yang baik. Adapun *file* simulasi berupa 12 JPG, 11 PNG, 6 MP4, 5 AVI, 4 MP3, 1 DOCX dan 1 PDF. Cara dalam memulihkan data yang terhapus dengan memilih opsi *export* pada klik kanan, maka data yang dipilih akan tersimpan pada folder analisis dalam folder *export*

e) Reporting

Berdasarkan analisis yang telah dilakukan dapat dibentuk pelaporan mengenai pengetahuan yang diperoleh agar dapat lebih mudah dipahami. Pada tabel IV.4 dapat diketahui *software* FTK Imager dan Autopsy memiliki kinerja yang baik dalam memeriksa, menemukan dan pemulihan data yang terhapus, akan tetapi untuk kecepatan *Autopsy* memiliki waktu cukup lama.

C. Efektivitas Aplikasi Analisis Digital Forensic Dalam Penyelidikan

Digital forensik sebagai bidang ilmu yang digunakan untuk menyelidiki bukti digital, bertujuan untuk pengumpulan, mengembalikan bukti digital, dan analisis bukti digital tersebut, yang terdapat pada *cybercrime* [14]. Dalam perkara *cybercrime* alat bukti elektronik harus memenuhi persyaratan baik secara formil maupun materil, sehingga alat bukti tersebut dapat dinyatakan sah dan dapat dipergunakan di persidangan [15]. Namun adapun hambatan yang terjadi pada kasus penyelidikan digital forensik apabila adanya tindakan penghapusan atau menghilangkan barang bukti yang dapat merugikan tahap investigasi dan korban. Salah satu penyebabnya adalah kompetensi ahli penyidik yang kurang mumpuni.

Penyidik yang kurang berkompeten atau ahli pada Polres Tapanuli Utara serta jumlah personil ahli yang sedikit dapat menghambat proses penyidikan, adapun hal lain seperti kurangnya sarana dan prasarana karena tidak mempunyai laboratorium khusus digital forensik sendiri. Untuk itu peneliti menyarankan untuk menggunakan aplikasi *open source* seperti FTK Imager dan Autopsy yang dinilai mampu dan cukup mudah dipahami dan digunakan dalam proses penyelidikan digital forensik.

Efektivitas aplikasi *open source* seperti FTK Imager dan Autopsy dinilai cukup baik dalam menganalisa dan menyimpan keaslian barang bukti serta pencarian dan pemulihan data. Adapun upaya yang dapat dilakukan Polres Tapanuli Utara untuk mengatasi hambatan dalam penerapan digital forensik terhadap penyidikan *cybercrime*, yaitu mengadakan pelatihan di bidang informasi dan transaksi elektronik yang bersertifikasi terhadap Penyidik, serta mengadakan Pendidikan Kejuruan (Dikjur) dan Pendidikan Pengembangan (Dikbang), menambah personil Penyidik, menyediakan laboratorium digital forensik di setiap Polres.

4. KESIMPULAN

Adapun kesimpulan pada penelitian ini, antara lain: (1). Mengamankan barang bukti dengan *Chain of Custody* (COC) merupakan prosedur yang penting dalam digital forensik. *Chain of Custody* (COC) berisi kronologi perjalanan barang bukti yang memuat informasi yang lengkap; (2). *Framework National Institute of Justice* (NIJ) menjadi prosedur penyelidikan dan pemecahan masalah dalam proses investigasi barang bukti digital pada kasus kejahatan dengan 5 (lima) tahap, yaitu: (a). *Identification*; (b). *Collection*; (c). *Examination*; (d). *Analysis*, dan (e). *Reporting*; (3). *Software* FTK Imager sebagai aplikasi untuk menduplikasi data barang bukti memiliki kinerja yang baik, serta *software* Autopsy sebagai aplikasi untuk memeriksa dan memulihkan data barang bukti memiliki kinerja yang baik. Dengan demikian kedua *software* tersebut dinilai mampu dalam membantu ahli digital dalam menginvestigasi

barang bukti digital. Upaya yang dapat dilakukan Polres Tapanuli Utara untuk mengatasi hambatan dalam penerapan digital forensik terhadap penyidikan *cybercrime*, yaitu mengadakan pelatihan di bidang informasi dan transaksi elektronik yang bersertifikasi terhadap Penyidik

UCAPAN TERIMA KASIH

Penulis mengucapkan terimakasih kepada Universitas Potensi Utama yang telah banyak memberikan masukan dan saran dalam penyelesaian Skripsi ini.

REFERENSI

- [1] Aisyah, N., Putra, A., Safrizal, S., Valentino, V., Zikriah, Z., Prasetyo, B., Susanti, D., & Nurhayati, N. (2022). Analisa Perkembangan Digital Forensik Dalam Penyidikan Cybercrime Di Indonesia Secara Systematic Review. *Jurnal Esensi Infokom : Jurnal Esensi Sistem Informasi Dan Sistem Komputer*, 6(1), 22-27..
- [2] Nur, A. (2022). Peranan Audit Forensik Dalam Pencegahan Kasus Fraud Penerbitan Izin Usaha Pertambangan (IUP) Pemerintahan Daerah. *Jurnal Penelitian Dan Pengkajian Ilmiah Sosial Budaya*, 1(2), 418-43.
- [3] Riadi, I., Umar, R., & Nasrulloh, M., I. (2018). Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute Of Justice (NIJ), ELINVO (Electronics, Informatics, and Vocational Education). 2(1), 70-82.
- [4] Kurdiat E. F. I., Widiyasono, N., & Mubarak, H. (2016). Analisis Proses Investigasi Dekstop PC Yang Terhubung Layanan Private Cloud. *JuTISI Jurnal Teknik Informatika dan Sistem Informasi*, 2(2), 221-230.
- [5] Nugroho, D. P. (2017). IT: DIGITAL FORENSIC. *Jurnal IPSIKOM*, 5(1), 1-7.
- [6] Riskiyadi, M, 2020. (2020). Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime. *CyberSecurity dan Forensik Digital*, 3(2), 12-21.
- [7] Faiz, M. N. (2018). Studi Komparasi Investigasi Digital Forensik pada Tindak Kriminal. *INISTA (Journal of Informatics Information System Software Engineering and Applications)*, 1(1), 18-28.
- [8] Riadi, I., Sunardi., & Hadi, A. (2019). Analisis Bukti Digital SSD NVMe pada Sistem Operasi Proprietary Menggunakan Metode Static Forensics, *Jurnal CoreIT*. 5(2), 102-109.
- [9] Sianipar, M. M. J., Ismail, S. J. I., Satrya, G. B. (2021). Analisis Digital Forensik Aplikasi Ovo Pada Android, *e-Proceeding of Applied Science*, 7(6), 2745-2749.
- [10] Rachmie, S. (2020). Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website, *JURNAL LITIGAS*, 21(1), 104-127.
- [11] Putra, S, A., Prayudi, Y. (2021). Implementasi Multi Smart Contract pada Bukti Digital dan Chain of Custody dalam Meningkatkan Keamanan dan Integritas Bukti Digital, *JUSTINDO (Jurnal Sistem dan Teknologi Informasi)*, 6(2), 98-108.
- [12] Sunardi, Riadi, I., & Triyanto, J. (2021). Forensics Mobile Layanan WhatsApp pada Smartwatch Menggunakan Metode National Institute of Justice. *JOINTECS*, 6(2), 63-70.
- [13] Sunardi, Riadi, I., & Akbar, H. M. (2020). Penerapan Metode Static Forensics untuk Ekstraksi File Steganografi pada Bukti Digital Menggunakan Framework DFRWS. *JURNAL RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 4(3), 576-583.

- [14] Iman, N., Susanto, A., & Inggi, R. (2019). Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review), *IncomTech: Jurnal Telekomunikasi dan Komputer*, 9(1) 186-192.
- [15] Sanjaya, A. A., Hartono, S. M., & Ardhya, S. N. (2022). Penggunaan Akun Media Sosial Sebagai Alat Bukti Elektronik Dalam Proses Penyidikan, *e-Journal Komunikasi Yustisia*, 5(2), 482-493.