Analisis Komparatif Performa FTK IMAGER dan AUTOPSY dalam Forensik Digital pada Flashdisk

Mega Rosita
Badan Siber dan Sandi Negara, qwertyopo354@gmail.com

Abstrak

Peningkatan penggunaan flashdisk atau perangkat USB cenderung masif karena berbagai aspek, salah satunya ukuran dan harga perangkat penyimpanan USB yang terjangkau. Namun, karena sifatnya yang portabel dan mudah dibawa-bawa, flashdisk juga seringkali digunakan dalam kejahatan digital. Penelitian dilakukan untuk pengimplementasian proses akuisisi data yang terhapus dari sebuah flashdisk menggunakan tools forensik Autopsy dan Forensic Toolkit Imager (FTK Imager) dan metode National Institute of Standard and Technology (NIST) serta validasi dengan pencocokan nilai hash. Hasil akuisisi menunjukan pada flashdisk yang dilakukan delete, FTK Imager memperoleh nilai 100%, sementara Autopsy memperoleh nilai 94,12%. Pada flashdisk yang dilakukan quick format FTK imager memperoleh nilai 0% dibandingkan Autopsy 97,06%. Sementara itu, pada flashdisk yang dilakukan format, FTK Imager dan Autopsy memperoleh nilai 0%. Hal ini disebabkan karena keduanya tidak berhasil menemukan file yang terhapus.

Kata kunci: Autopsy, *Flashdisk*, FTK Imager, Pemulihan Data

Abstract

The increasing use of flashdisk or USB devices tends to be massive due to various factors, including the size and affordable price of USB storage devices. However, due to their portable nature and ease of carrying, flashdisk are also frequently used in digital crimes. Research has been conducted to implement the data acquisition process for deleted data from a flashdisk using forensic tools Autopsy and Forensic Toolkit Imager (FTK Imager), the National Institute of Standards and Technology (NIST) method, and validation through hash value matching. The acquisition results show that for a flashdisk subjected to deletion, FTK Imager obtained a 100% success rate, while Autopsy achieved a rate of 94.12%. For a flashdisk subjected to a quick format, FTK Imager obtained a 0% success rate compared to Autopsy's 97.06%. Meanwhile, for a flashdisk subjected to a full format, both FTK Imager and Autopsy obtained a 0% success rate. This is because neither of them successfully found deleted files.

Keywords: autopsy, flashdisk, FTK Imager, data recovery

1. PENDAHULUAN

Perkembangan teknologi membuat dinamika kejahatan siber sangat beragam dan terus meningkat setiap tahunnya. Berdasarkan laporan *Cybersecurity Ventures*, kejahatan siber tumbuh 15 persen pada 2025 dan melibatkan barang bukti elektronik maupun digital salah satunya komputer [1]. Penggunaan komputer sebagai alat kejahatan dapat berupa pengambilan data penting secara ilegal, manipulasi data, membocorkan data penting dan penyalahgunaan perangkat komputer baik *hardware* maupun *software* untuk akses tidak sah [2]. Kejahaan dengan komputer umumnya meninggalkan jejak sehingga dibutuhkan ahli forensik komputer dalam mengamankan barang bukti digital [3].

Forensik komputer merupakan aplikasi bidang ilmu pengetahuan dan teknologi komputer untuk kepentingan pembuktian hukum (*pro-justice*), yang dalam hal ini untuk membuktikan kejahatan berteknologi tinggi atau *computer crime* secara ilmiah hingga bisa mendapatkan bukti digital yang dapat digunakan untuk menjerat pelaku kejahatan tersebut [4]. Bukti digital adalah informasi yang rapuh, *volatile* dan rentan jika tidak ditangani dengan benar. 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 sebab itu dalam rangka mengungkap kasus kejahatan berkaitan dengan bukti elektronik atau digital, jenis barang bukti inilah yang harus dicari kemudian dianalisis secara teliti keterkaitan masing-masing *file* [5].

Flashdisk adalah salah satu media penyimpanan data portabel yang dapat dihubungkan melalui *port USB* ke suatu perangkat komputer atau laptop. *Flashdik* merupakan salah satu barang bukti elektronik yang dapat membantu investigasi serta dapat membuktikan adanya keterlibatan pelaku dalam kejahatan. Salah investigasi yang dilakukan dalam penyelidikan adalah *disk imaging* yang merupakan proses penyalinan sektor demi sektor data seluruh *disk* untuk mendapatkan konten lengkap termasuk lokasi data [6]. Terhapus dan rusaknya data pada sebuah media penyimpanan merupakan hal yang tidak dapat dihindari, namun berpotensi untuk didapatkan kembali dengan menggunakan alat forensik. Ada beragam alat forensik yang dapat digunakan untuk mendapatkan data dengan karakteristiknya masing-

masing, diantaranya *FTK-Imager*, *Autopsy*, *Belkasoft*, *Xways Foresincs*, *foremost*, dd, dcfldd, dan dc3dd.

Ada beberapa karya yang berkaitan dengan penelitian ini. Karya pertama, membahas tentang investigasi bukti digital *optical drive* menggunakan Autopsy dan FTK Imager. Hasilnya FTK Imager lebih unggul karena berhasul memulihkan seluruh *file* yang terhapus, sementara Autopsy memulihkan 7 dari 10 *file* [7]. Pada tahun 2020 Riadi melakukan penelitian untuk mengembalikan bukti digital pada SSD NVMe TRIM enable dengan menggunakan Autopsy dan Recuva. Hasil analisis TRIM enable metode penghapusan shift *delete* tidak ditemukan bukti digital yang sesuai nilai *hash* dengan bukti digital asli. Sedangkan metode penghapusan *delete, delete recycle bin* bukti digital dapat dikembalikan dengan persentase keberhasilan menggunakan Autopsy sebesar 90% dan 10% nilai *hash* bukti digital tidak valid, sedangkan Recuva 80% bukti digital berhasil dikembalikan dan 20% tidak berhasil dikembalikan [8]. Pada tahun 2021 Simanjuntak dan kawan-kawan melakukan perbandingan software forensic WinHex dan X-Way Forensic dalam melakukan data recovery dengan sempurna. Hasilnya X-Way Forensic dapat lebih banyak memulihkan data dibandingkan WinHex [3].

Berdasarkan penjelasan di atas, penelitian ini akan melakukan analisis bukti digital yang terhapus pada *flashdisk* dengan metode penghapusan *delete, quick format,* dan *format* menggunakan FTK Imager dan Autopsy guna mengetahui performa alat dalam melakukan pemulihan data. Penelitian menerapkan tahapan *National Institute of Standards and Technolgy* (NIST) untuk mendapatkan bukti digital yang valid dan dapat dipertanggungjawabkan. Hasil penelitian akan mempermudah pemilihan penggunaan alat forensik dalam melakukan pemulihan data digital sesuai kebutuhan dan hasil analisis kemampuan alat.

2. LANDASAN TEORI

2.1 Forensik Komputer

Forensik komputer adalah proses menggunakan teknik investigasi untuk mengumpulkan, menganalisis, dan menjaga bukti digital dari sistem komputer, jaringan, dan perangkat penyimpanan digital lainnya. Tujuan forensik komputer adalah untuk mengungkap bukti kejahatan digital atau insiden, seperti *hacking*, pelanggaran data, atau serangan siber, dan untuk mengidentifikasi individu atau kelompok yang bertanggung jawab [4].

Proses forensik komputer melibatkan beberapa tahapan, termasuk mengidentifikasi dan mengamankan bukti digital, menganalisis bukti untuk mengungkap informasi yang mungkin relevan dengan penyelidikan, dan menyajikan temuan dalam cara yang jelas dan singkat. Para ahli forensik komputer dapat menggunakan berbagai alat dan teknik untuk mengekstrak informasi dari perangkat digital, termasuk perangkat lunak pemulihan data, perangkat keras khusus, dan perangkat lunak analisis forensik. Beberapa jenis bukti digital yang mungkin dikumpulkan selama penyelidikan forensik komputer meliputi *email*, pesan instan, riwayat *browsing*, dokumen, gambar, dan *file* video [9].

2.2 Pemulihan Data

Pemulihan data (*recovery data*) merujuk pada proses memulihkan data yang hilang atau terhapus dari suatu perangkat penyimpanan seperti *hard drive*, *USB drive*, atau kartu memori. Data dapat hilang karena beberapa alasan seperti kerusakan perangkat keras, serangan virus atau *malware*, kesalahan manusia, atau kegagalan perangkat lunak. Proses pemulihan data dimulai dengan mengidentifikasi penyebab hilangnya data dan menentukan apakah data masih dapat dipulihkan. Namun, tidak semua data dapat dipulihkan dan proses pemulihan data dapat menjadi mahal tergantung pada tingkat kerusakan atau jenis data yang hilang [10].

2.3 Penghapusan Data *Format, Quick Format,* dan *Delete*

Format, *quick format*, dan *delete* adalah tiga metode yang berbeda dalam menghapus data pada perangkat penyimpanan digital.

- *Format*: Proses penghapusan data pada perangkat penyimpanan digital dan pengaturan ulang *file system* pada perangkat tersebut. Dalam proses *format*, seluruh data pada perangkat akan dihapus, termasuk *file* sistem dan partisi [11].
- *Quick format*: Proses penghapusan data pada perangkat penyimpanan digital dan pengaturan ulang *file system* pada perangkat tersebut, namun hanya menghapus *file* sistem dan partisi saja. Data pada sektor-sektor di dalam perangkat penyimpanan tetap ada dan dapat dipulihkan dengan perangkat lunak pemulihan data khusus [11]
- *Delete*: Proses penghapusan *file* atau folder pada perangkat penyimpanan digital. Saat *file* atau folder dihapus menggunakan metode *delete*, data tersebut masih tetap ada pada perangkat penyimpanan, namun hanya *file* sistem yang menghapus akses ke data tersebut [11]

2.4 FTK Imager

FTK Imager adalah perangkat lunak forensik yang digunakan untuk memperoleh gambar atau salinan forensik dari perangkat penyimpanan data, seperti *hard drive*, USB *drive*, dan kartu memori. Gambar forensik ini kemudian dapat digunakan untuk melakukan analisis forensik pada data yang terdapat pada perangkat penyimpanan tersebut. FTK Imager dikembangkan oleh AccessData, sebuah perusahaan yang menyediakan solusi forensik digital dan keamanan informasi. FTK Imager dapat digunakan oleh para profesional forensik, investigasi keamanan informasi, atau pengguna individu yang ingin memulihkan data yang hilang dari perangkat

penyimpanan. Selain itu, FTK Imager juga dapat digunakan sebagai alat untuk melakukan analisis forensik pada gambar forensik yang sudah dibuat [12].

2.5 Autopsy

Autopsy adalah perangkat lunak forensik sumber terbuka (*open source*) yang digunakan untuk analisis forensik pada perangkat lunak, perangkat keras, dan data digital. Autopsy dikembangkan oleh Basis *Technology Corp* dan diperbarui secara berkala oleh komunitas pengembang terbuka. Perangkat lunak ini dapat digunakan pada berbagai sistem operasi seperti Windows, Linux, dan MacOS. Autopsy sangat berguna bagi para profesional forensik, seperti penegak hukum, tim investigasi keamanan informasi, atau pengguna individu yang ingin melakukan analisis forensik pada perangkat lunak atau data digital. Autopsy juga menyediakan berbagai macam plugin untuk membantu para pengguna memperluas fungsi perangkat lunak sesuai dengan kebutuhan [7].

2.6 Perbandingan FTK Imager dan Autopsy

FTK Imager dan Autopsy adalah kedua perangkat lunak forensik yang umum digunakan untuk analisis forensik pada data digital. Tabel 1 menunjukkan perbandingan FTK Imager dan Autopsy secara umum.

Tabel 1. Perbandingan FTK Imager dan Autopsy

Aspek	FTK Imager	Autopsy
Fitur	lebih fokus pada proses pengambilan dan pembuatan *image* forensik dari perangkat penyimpanan	lebih fokus pada analisis data digital dan memiliki fitur pencarian dan visualisasi data yang kuat
Tampilan	lebih sederhana dan mudah digunakan	lebih kompleks dengan banyak pilihan dan fitur yang lebih banyak
Ketersediaan	Windows	Windows, Linux, dan MacOS
Penggunaan	Cocok digunakan oleh para profesional forensik yang sudah terbiasa menggunakan perangkat lunak forensik	Mudah digunakan dan dapat digunakan oleh orang yang tidak memiliki latar belakang teknis yang kuat dalam forensik digital

3. METODE PENELITIAN

Dalam penelitian ini digunakan metode eksperimen dengan menerapkan NIST yang meliputi *collection*, *examination*, *analysis* dan *reporting* [10] seperti pada gambar 1. Alur penelitian dan gambaran tahapan pengolahan data adalah sebagai berikut.

Gambar 1. Alur Proses Penelitian

a. *Collection*, yaitu mengidentifikasi, memberi label, merekam, dan memperoleh data dari sumber yang releva dengan mengikuti pedoman dan prosedur yang menjaga integritas data. Hasil dari tahap ini yaitu barang bukti berupa *flashdisk*.
b. *Examination*, yaitu pemrosesan data yang dikumpulkan secara digital forensik menggunakan kombinasi dari berbagai skenario untuk menilai dan mengekstraksi data yang menarik dengan tetap menjaga integritas data. Hasil dari tahap ini yaitu *file image* dari masing-masing scenario.
c. *Analysis*, yaitu menganalisis hasil pemeriksaan dengan menggunakan Autopsy dan FTK Imager, lalu membandingkan untuk memperoleh kesimpulan.
d. *Reporting*, yaitu pelaporan hasil analisis meliputi gambaran tindakan yang dilakukan, alat dan prosedur yang dipilih dan hasil perbandingan alat yang digunakan.

3.1 Skenario

Berikut ini beberapa skenario yang dilakukan pada penelitian ini.

a. Skenario 1: *Flashdisk* menyimpan 34 *file* barang bukti kejahatan, kemudian seseorang berusaha melakukan penghapusan pada *file* dengan melakukan *delete*.
b. Skenario 2: *Flashdisk* menyimpan 34 *file* barang bukti kejahatan, kemudian seseorang berusaha melakukan penghapusan pada *file* dengan melakukan *quick format*.
c. Skenario 3: *Flashdisk* menyimpan 34 *file* barang bukti kejahatan, kemudian seseorang berusaha melakukan penghapusan pada *file* dengan melakukan *format*.

3.2 Alat

Tabel 2 menampilkan alat yang yang digunakan pada penelitian

Tabel 2. Alat Penelitian

No	Alat	Spesifikasi	Keterangan
1	PC All in One	Dell OptiPlex 7480	*Hardware*
2	Sistem operasi	Windows 11	*Software*
3	*Flashdisk*	SanDisk 4 GB	*Hardware*
4	FTK Imager	Versi 4.7.1	Alat akuisisi
5	Autopsy	Versi 4.20.20	Alat akuisisi
6	HashMyFile	Versi 2.43	Alat validasi *hash*

Tabel 3 menunjukkan *file* asli sebagai acuan bukti digital pada penelitian ini.

Tabel 3. Bukti digital pada *Flashdisk*

Nama File	MD5
Format Executable	
exe1.exe	98b62420cce2e7552d4c932c6d1313a9
HashMyFiles.exe	3c6cdc7d42ce59b0befe71299fb9e9aa
whatsapp.apk	ff91d2e515846d4ef3425eecdc741489
Format Kompresi	
rar.rar	4dc7982b8ea86b3ca1ac9563afee0781
rar2.rar	a7ef54c177677fc958c25e1ad813f1ce
zip.zip	1ee1a80c325ee99a87ff76178de1befa
Format Audio	
m4a.m4a	c7cb4cfbf25ef6b3d3bd9b0d9ef77a7e
mp3.mp3	0c481e87f2774b1bd41a0a70d9b70d11
wav.wav	f2101cf866dea872dbaeb8ac1e6cc9ae
Format Video	
avi.avi	9d22d2bfe1d44127263cadf0fa96ef9d
flv.flv	9da29cf17df8a7d72118c9ee51fcfb73
mov.mov	6c7340bed691689395e8b6884c366176
mp4.mp4	6af96a17869d3dfc34766387084a1c5c
mpg.mpg	96b0498596399cdbfa845c47a0398c4e
mts.mts	ce21b6904f8b33dea708432331f0095c
Format Gambar	
gif.gif	f0dbd9b72c0997b0f7db2b69ff810d20
heic.HEIC	722cab748015e10a6836826d86951b2c
jpg.jpg	9e1efdef9e315b6d8435bdb79803bdb6
png.png	2ad6f3ae2f71ae15b42dfe672c6eb95b
Format Dokumen	
doc.doc	cc6cee98331be4c59e20605d3dc53725
docx.docx	27c3b4537677a90a30ee2460121b56c0
IMG.txt	b9377d17163d05a17e70a2d9beef3723
pdf.pdf	807426522bb4e646a4309ecabb537452
ppt.ppt	addf63d147411c6ec1a2b594fc36b550
pptx.pptx	4300f74a7d608f0b7fa612157d5cb8e5
readme.txt	038b790c1106437f5b61e77c515640c5
xls.xls	fd47228cd614532ff7ba4d0b82259b30
xlxs.xlsx	df7489b006993b64094d92943b6141aa
Format Lainnya	
fontawesome-webfont.bin	93347f7a9e84ed69e86bfabcac3ca256
HashMyFiles.cfg	171d9abb59b3dde7de2c10257943acad
HashMyFiles.chm	762d7c3ab3a44a1929c63e2c477ae543
html.html	74fd88df29e89425570e816aeeb01f4e
packager.dll	d890fd87ef28a3dc11ee04dfb28994e5
pcapng.pcapng	e67467a7a102582bd86f85707cdfc6a1

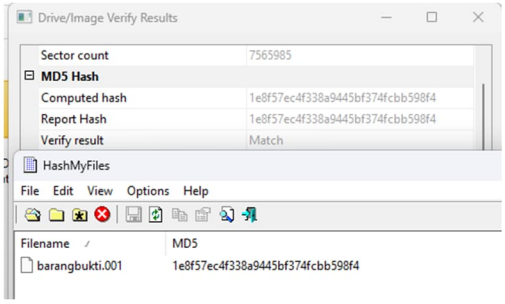
4. HASIL DAN PEMBAHASAN

4.1 *Collection*

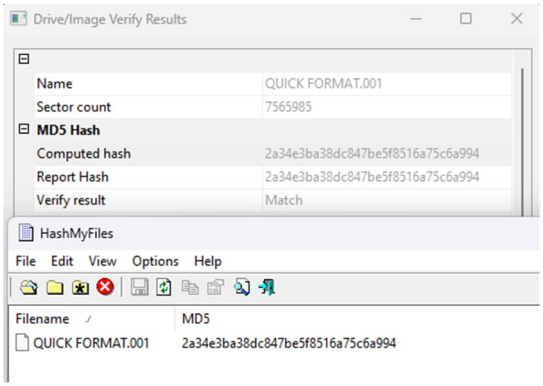
Pada tahap ini dilakukan pengumpulan barang bukti digital pada *flashdisk* yang berisi sejumlah *file* dengan beragam ekstensi.

4.2 *Examination*

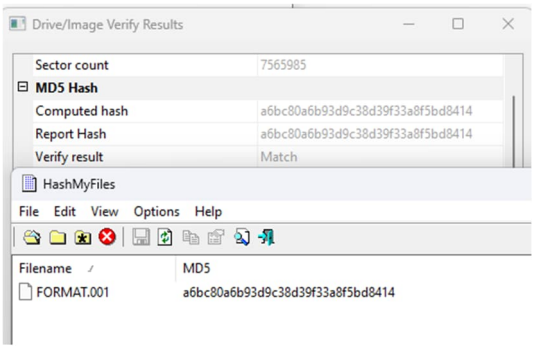
Pada Tahap ini dilakukan imaging dengan menggunakan FTK Imager untuk membuat salinan data sebagai bukti digital dari *flashdisk*. Selanjutnya hasil *file image* yang dibuat dan kloningnya divalidasi dengan melakukan pencocokan nilai *hash* menggunakan HashMyFile dan FTK Imager. Gambar 2 menampilkan validasi nilai *hash* pada hasil *image* yang dilakukan penghapusan dengan *delete* (skenario 1), Gambar 3 menampilkan validasi nilai *hash* pada hasil *image* yang dilakukan penghapusan dengan *quick format* (skenario 2), sementara Gambar 3 menampilkan validasi nilai *hash* pada hasil *image* yang dilakukan penghapusan dengan *format* (skenario 3).



Gambar 2. Validasi Hash Image Skenario 1



Gambar 3 Validasi Hash Image Skenario 2



Gambar 4. Validasi Hash Image Skenario 3

4.3 Analysis

Pada tahapan ini bukti digital yang ditemukan pada proses *examination* akan dijadikan sebagai barang bukti yang sah setelah dilakukan validasi nilai Hash. Selanjutnya dilakukan pemulihan data dengan menggunakan FTK dan Autopsy.

a. Skenario 1: Delete Data *Flashdisk*

Pada skenario 1 FTK berhasil untuk memulihkan 2 folder, sementara Autopsy memulihkan 2 folder dan 126 *file* lainnya. Selanjutnya dilakukan validasi untuk mengetahui keaslian sebuah *file* dari proses akuisisi sampai *file* tersebut diekstraksi dengan pencocokan nilai *hash* bukti digital (tabel 2) dan hasil pemulihan. Tabel 4 menunjukan hasil pencocokan nilai *hash* hasil pemulihan dari FTK Imager, sementara Tabel 5 menunjukkan hasil pemulihan dari Autopsy.

Tabel 4. Validasi *hash* hasil pemulihan FTK Imager pada *flashdisk* yang dilakukan *delete*

Nama File	MD5	Validasi
Format Executable		
!xe1.exe	98b62420cce2e7552d4c932c6d1313a9	Valid
HashMyFiles.exe	3c6cdc7d42ce59b0befe71299fb9e9aa	Valid
!hatsapp.apk	ff91d2e515846d4ef3425eecdc741489	Valid
Format Kompresi		
!ar.rar	4dc7982b8ea86b3ca1ac9563afee0781	Valid
!ar2.rar	a7ef54c177677fc958c25e1ad813f1ce	Valid
!ip.zip	1ee1a80c325ee99a87ff76178de1befa	Valid
Format Audio		
m4a.m4a	c7cb4cfbf25ef6b3d3bd9b0d9ef77a7e	Valid
!p3.mp3	0c481e87f2774b1bd41a0a70d9b70d11	Valid
!av.wav	f2101cf866dea872dbaeb8ac1e6cc9ae	Valid
Format Video		
!vi.avi	9d22d2bfe1d44127263cadf0fa96ef9d	Valid
!lv.flv	9da29cf17df8a7d72118c9ee51fcfb73	Valid
mov.mov	6c7340bed691689395e8b6884c366176	Valid
!p4.mp4	6af96a17869d3dfc34766387084a1c5c	Valid
!pg.mpg	96b0498596399cdbfa845c47a0398c4e	Valid
!ts.mts	ce21b6904f8b33dea708432331f0095c	Valid
Format Gambar		
!if.gif	f0dbd9b72c0997b0f7db2b69ff810d20	Valid
heic.HEIC	722cab748015e10a6836826d86951b2c	Valid
!pg.jpg	9e1efdef9e315b6d8435bdb79803bdb6	Valid
!ng.png	2ad6f3ae2f71ae15b42dfe672c6eb95b	Valid
Format Dokumen		
!oc.doc	cc6cee98331be4c59e20605d3dc53725	Valid
docx.docx	27c3b4537677a90a30ee2460121b56c0	Valid
IMG.txt	b9377d17163d05a17e70a2d9beef3723	Valid
!df.pdf	807426522bb4e646a4309ecabb537452	Valid
!pt.ppt	addf63d147411c6ec1a2b594fc36b550	Valid
pptx.pptx	4300f74a7d608f0b7fa612157d5cb8e5	Valid
!eadme.txt	038b790c1106437f5b61e77c515640c5	Valid
!ls.xls	fd47228cd614532ff7ba4d0b82259b30	Valid
xlxs.xlsx	df7489b006993b64094d92943b6141aa	Valid
Format Lainnya		
fontawesome-webfont.bin	93347f7a9e84ed69e86bfabcac3ca256	Valid
HashMyFiles.cfg	171d9abb59b3dde7de2c10257943acad	Valid
HashMyFiles.chm	762d7c3ab3a44a1929c63e2c477ae543	Valid
html.html	74fd88df29e89425570e816aeeb01f4e	Valid
!ackager.dll	d890fd87ef28a3dc11ee04dfb28994e5	Valid
pcapng.pcapng	e67467a7a102582bd86f85707cdfc6a1	Valid

Tabel 5. Validasi Hash Hasil Pemulihan Autopsy pada *Flashdisk* yang dilakukan Delete

Nama File	MD5	Validasi
Format Executable		
_xe1.exe	98b62420cce2e7552d4c932c6d1313a9	Valid
HashMyFiles.exe	3c6cdc7d42ce59b0befe71299fb9e9aa	Valid
_hatsapp.apk	ff91d2e515846d4ef3425eecdc741489	Valid
Format Kompresi		
_ar.rar	4dc7982b8ea86b3ca1ac9563afee0781	Valid
_ar2.rar	a7ef54c177677fc958c25e1ad813f1ce	Valid
_ip.zip	1ee1a80c325ee99a87ff76178de1befa	Valid
Format Audio		
_4a.m4a	c7cb4cfbf25ef6b3d3bd9b0d9ef77a7e	Valid
_p3.mp3	0c481e87f2774b1bd41a0a70d9b70d11	Valid
_av.wav	f2101cf866dea872dbaeb8ac1e6cc9ae	Valid
Format Video		
_vi.avi	9d22d2bfe1d44127263cadf0fa96ef9d	Valid
_lv.flv	9da29cf17df8a7d72118c9ee51fcfb73	Valid
_ov.mov	6c7340bed691689395e8b6884c366176	Valid
_p4.mp4	6af96a17869d3dfc34766387084a1c5c	Valid
_pg.mpg	96b0498596399cdbfa845c47a0398c4e	Valid
_ts.mts	ce21b6904f8b33dea708432331f0095c	Valid
Format Gambar		
_if.gif	f0dbd9b72c0997b0f7db2b69ff810d20	Valid
heic.HEIC	722cab748015e10a6836826d86951b2c	Valid
_pg.jpg	9e1efdef9e315b6d8435bdb79803bdb6	Valid
_ng.png	2ad6f3ae2f71ae15b42dfe672c	Valid

	6eb95b	
Format Dokumen		
_oc.doc	cc6cee98331be4c59e20605d3dc53725	Valid
docx.docx	27c3b4537677a90a30ee2460121b56c0	Valid
IMG.txt	b9377d17163d05a17e70a2d9beef3723	Valid
_df.pdf	807426522bb4e646a4309ecabb537452	Valid
_pt.ppt	1ae3927eec7d3a8f6dde378d24470a1a	Tidak Valid
_ptx.pptx	4300f74a7d608f0b7fa612157d5cb8e5	Valid
_eadme.txt	038b790c1106437f5b61e77c515640c5	Valid
_ls.xls	fd47228cd614532ff7ba4d0b82259b30	Valid
xlxs.xlsx	df7489b006993b64094d92943b6141aa	Valid
Format Lainnya		
fontawesome-webfont.bin	93347f7a9e84ed69e86bfabcac3ca256	Valid
HashMyFiles.cfg	f418801dfc45f7432e1744f567e41318	Tidak Valid
HashMyFiles.chm	762d7c3ab3a44a1929c63e2c477ae543	Valid
html.html	74fd88df29e89425570e816aeeb01f4e	Valid
packager.dll	d890fd87ef28a3dc11ee04dfb28994e5	Valid
pcapng.pcapng	e67467a7a102582bd86f85707cdfc6a1	Valid

Tabel 4 menunjukkan *file* yang berhasil diekstraksi tidak mengalami perubahan nilai *hash* sehingga semua *file* valid dan layak dijadikan bukti digital yang sah. Sementara itu pada tabel 5 menunjukkan 34 *file* dapat dipulihkan, namun 2 diantaranya menunjukkan perubahan nilai *hash* setelah dicocokkan.

b. Skenario 2: *Quick Format* Data *Flashdisk*

Pada skenario 2 FTK Imager tidak berhasil untuk melakukan pemulihan data, sementara Autopsy memulihkan 40 *file* dan 6 slack *file*. Selanjutnya dilakukan validasi untuk mengetahui keaslian sebuah *file* dari proses akuisisi hingga *file* tersebut dipulihkan dengan pencocokan nilai *hash* bukti digital (tabel 2) dan hasil pemulihan. Tabel 6 menunjukan menunjukkan hasil pemulihan dari Autopsy

Tabel 6. Validasi *hash* hasil pemulihan autopsy pada *flashdisk* yang dilakukan *quick format*

Nama File	MD5	Validasi
Format Executable		
exe1.exe	98b62420cce2e7552d4c932c6d1313a9	Valid
HashMyFiles.exe	3c6cdc7d42ce59b0befe71299fb9e9aa	Valid
whatsapp.apk	ff91d2e515846d4ef3425eecdc741489	Valid
Format Kompresi		
rar.rar	4dc7982b8ea86b3ca1ac9563afee0781	Valid
rar2.rar	a7ef54c177677fc958c25e1ad813f1ce	Valid
zip.zip	1ee1a80c325ee99a87ff76178de1befa	Valid
Format Audio		
m4a.m4a	c7cb4cfbf25ef6b3d3bd9b0d9ef77a7e	Valid
mp3.mp3	0c481e87f2774b1bd41a0a70d9b70d11	Valid
wav.wav	f2101cf866dea872dbaeb8ac1e6cc9ae	Valid
Format Video		
avi.avi	9d22d2bfe1d44127263cadf0fa96ef9d	Valid
flv.flv	9da29cf17df8a7d72118c9ee51fcfb73	Valid
mov.mov	6c7340bed691689395e8b6884c366176	Valid
mp4.mp4	6af96a17869d3dfc34766387084a1c5c	Valid
mpg.mpg	96b0498596399cdbfa845c47a0398c4e	Valid
mts.mts	ce21b6904f8b33dea708432331f0095c	Valid
Format Gambar		
gif.gif	f0dbd9b72c0997b0f7db2b69ff810d20	Valid
HEIC~1.HEI	722cab748015e10a6836826d86951b2c	Valid
jpg.jpg	9e1efdef9e315b6d8435bdb79803bdb6	Valid
png.png	2ad6f3ae2f71ae15b42dfe672c6eb95b	Valid
Format Dokumen		
doc.doc	cc6cee98331be4c59e20605d3dc53725	Valid
docx.docx	27c3b4537677a90a30ee2460121b56c0	Valid
IMG.txt	b9377d17163d05a17e70a2d9beef3723	Valid
pdf.pdf	807426522bb4e646a4309ecabb537452	Valid
ppt.ppt	4546bf6857d1d9c21836a59b12998b8f	Tidak Valid
PPTX~1.PPT	4300f74a7d608f0b7fa612157d5cb8e5	Valid
readme.txt	038b790c1106437f5b61e77c515640c5	Valid
xls.xls	fd47228cd614532ff7ba4d0b82259b30	Valid
XLXS~1.XLS	df7489b006993b64094d92943b6141aa	Valid
Format Lainnya		
fontawesome-webfont.bin	93347f7a9e84ed69e86bfabcac3ca256	Valid
HashMyFiles.cfg	171d9abb59b3dde7de2c10257943acad	Valid
HashMyFiles.chm	762d7c3ab3a44a1929c63e2c477ae543	Valid
HTML~1.HTM	74fd88df29e89425570e816aeeb01f4e	Valid
packager.dll	d890fd87ef28a3dc11ee04dfb28994e5	Valid
PCAPNG~1.PCA	e67467a7a102582bd86f85707cdfc6a1	Valid

Pada tabel 6, Autopsy berhasil memulihkan semua *file* pada *Flashdik* sehingga dapat digunakan sebagai barang bukti digital yang sah.

c. Skenario 3: Pemulihan Data *Flashdisk* yang dilakukan *Format*

Pada skenario 3, FTK Imager dan Autopsy tidak berhasil memulihkan data.

4.4 *Reporting*

Dari hasil pada tahap analisis pada *flashdisk* yang dilakukan *delete*, FTK Imager berhasil memulihkan semua data sementara Autopsy terdapat perubahan nilai *hash* dari 2 *file* yang berekstensi *.ppt dan *.cfg. Pada *flashdisk* yang dilakukan *quick format*, FTK Imager tidak menemukan *file* apapun, namun Autopsy berhasil untuk mendeteksi semua *file*. Sementara itu, pada *flashdisk* yang dilakukan *format*, baik FTK Imager maupun Autopsy tidak mendeteksi *file* apapun. Hasil perbandingan pemulihan data masing-masing alat pada setiap skenario dapat dilihat pada tabel 7.

Tabel 7. Hasil perbandingan alat

Ekstensi	Total	Delete		Quick Format		Format	
		FTK Imager	Autopsy	FTK Imager	Autopsy	FTK Imager	Autopsy
*.exe, *.apk	3	3	3	0	3	0	0
*.rar, *.zip	3	3	3	0	3	0	0
*.m4a, *.mp3, *.wav	3	3	3	0	3	0	0
*.avi, *.flv, *.mov, *.mp4, *.mpg, *.mts	6	6	6	0	6	0	0
*.gif, *.heic, *.jpg, *.png	4	4	4	0	4	0	0
*.doc, *.docx, *.txt, *.pdf, *.ppt, *.pptx, *.xls, *.xlxs	9	9	8	0	8	0	0
*.bin, *.cfg, *.chm, *.html, *.dll, *.pcapng	6	6	5	0	6	0	0
Total	34	34	32	0	33	0	0

Tabel 7 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).

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

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

Berdasarkan rumus perhitungan di atas maka hasil persentase uji performa dapat dilihat pada Tabel 8

Tabel 8. Persentase Uji Performa Alat Forensik dalam Pemulihan Data

Perlakuan	FTK Imager	Autopsy
Delete	100%	94,12%
Quick Format	0%	97,06%
Format	0%	0%

5. KESIMPULAN

Berdasarkan penelitian yang sudah dilakukan, hasil akuisisi menunjukan pada *flashdisk* yang dilakukan *delete*, FTK Imager memperoleh nilai 100%, sementara Autopsy memperoleh nilai 94,12%. Pada flashdisk yang dilakukan *quick format* FTK Imager memperoleh nilai 0% dibandingkan Autopsy 97,06%. Sementara itu, pada *flashdisk* yang dilakukan *format* FTK Imager dan Autopsy memperoleh nilai 0% karena tidak berhasil menemukan file yang terhapus. Performa FTK Imager dan Autopsy dalam memulihkan data maka dapat disimpulkan pada *flashdisk* yang di-*delete* FTK *image*r lebih unggul dibandingkan Autopsy. Sementara itu, pada *flashdisk* yang dilakukan *quick format*, autopsy lebih unggul dibandingkan FTK Imager. Pada *flashdisk* yang dilakukan *format* FTK Imager dan Autopsy tidak bisa memulihkan data. Keunggulan penelitian kami dibandingkan dengan penelitian terkait adalah kami menggunakan versi alat yang lebih baru dan lebih komprehensif dalam investigasi bukti digital. Penelitian selanjutnya dapat menggunakan media penyimpanan lainnya sehingga dapat melengkapi analisis performa alat forensk dalam pemulihan bukti digital.

REFERENSI

[1] R. Ruuhwan, I. Riadi dan Y. Prayudi, "Analisis Kelayakan Integrated Digital Forensics Investigation Framework Untuk Investigasi Smartphone," *Jurnal Buana Informatika*, 2016.

[2] E. Ketaren, "Cybercrime, Cyber Space, dan Cyber Law," *Jurnal Times*, 2016.

[3] M. S. Simanjuntak dan J. Panjaitan, "Analisa Recovery Data Menggunakan Software Komputer Forensik," *Jurnal Teknik Informatika Komputer Universal*, pp. 26-32, 2021.

[4] M. N. Al-Azhar, Digital Forensic Practical Guidelines for Computer Investigation, Jakarta,

2012.

[5] P. R. Indonesia, Undang-undang (UU) Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Jakarta: BPK RI, 2018.

[6] A. Schweikert, "An Optical Media Preservation Strategy," *Appendix Workflows*, pp. 21-23, 2018.

[7] I. Riadi, "Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST)," *Jurnal Resti*, pp. 820-828, 2019.

[8] I. Riadi, S. Sunardi dan A. Hadi, ".Analisis Bukti Digital Trim Enable SSD NVME Menggunakan Metode Static Forensics," *JUITA: Jurnal Informatika*, pp. 65-74, 2020.

[9] D. Guardian, "What is Computer Forensics?," [Online]. Available: https://digitalguardian.com/blog/what-computer-forensics. [Diakses 21 Februari 202].

[10] K. Ontrack, "What Is Data Recovery And How Does It Work?," [Online]. Available: https://www.krollontrack.com/resources/data-recovery/what-is-data-recovery/. [Diakses 21 Februari 2023].

[11] How-To-Geek, "What Happens When You Delete a File?.," [Online]. Available: https://www.howtogeek.com/125521/htg-explains-why-deleted-files-can-be-recovered-and-how-you-can-prevent-it/. [Diakses 21 Februari 2023].

[12] AccessData, "FTK Imager," [Online]. Available: https://accessdata.com/product-download/ftk-imager-version-4-5-0. [Diakses 23 Februari 2023].