Analisis Kinerja Perangkat Lunak *Forensic Imaging* Pada Sistem Operasi *Linux* Menggunakan Metode *Static Forensic*

Anton Yudhana *[1], Imam Riadi[2], Budi Putra[3]
[1]Program Studi Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta
[2]Program Studi Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta
[3]Program Studi Informatika, Universitas Ahmad Dahlan, Yogyakarta
Jl. Prof. Dr. Soepomo, S.H., Janturan, Warungboto, Yogyakarta 55166
e-mail: [1]eyudhana@ee.uad.ac.id, [2]imam.riadi@is.uad.ac.id,
*[3]budi1808048034@webmail.uad.ac.id

Abstrak

Perkembangan teknologi berbanding lurus dengan kasus kejahatan siber (cybercrime), hal tersebut menjadi kunci perkembangan modus-modus dalam kejahatan siber, namun dapat di pastikan kejahatan tersebut akan meninggalkan jejak pada barang bukti, agar penyidik dapat leluasa melakukan penyidikan, barang bukti harus di duplikasi terlebih dahulu, namun hanya sedikit yang dapat berjalan pada sistem operasi linux. Tujuan penelitian ini adalah untuk melakukan analisis dan menemukan perbedaan kinerja diantara perangkat lunak forensic imaging pada sistem operasi linux tersebut dengan indikator keberhasilan duplikasi harus sesuai dengan keaslian barang bukti. Metode yang digunakan static forensic serta menggunakan kerangka kerja National Institute of Standards and Technology (NIST). Hasil penelitian ini menemukan bahwa proses imaging FTK imager lebih cepat 2 menit 18 detik dari perangkat lunak dc3dd dan 12 detik dari DDrescue, DDrescue merupakan perangkat lunak yang menggunakan resource paling sedikit, validasi nilai hashing sha1 pada analisis hasil imaging file perangkat lunak DC3DD, DDrescue dan FTK Imager adalah sama atau valid, hal tersebut membuktikan bahwa perangkat lunak tersebut mampu melakukan imaging dan dapat digunakan untuk mengakuisisi barang bukti kasus kejahatan siber di persidangan.

Kata kunci: *Digital Forensic, Forensic Imaging , Static Forensic, Linux, Opensource*

1. PENDAHULUAN

Kejahatan siber *(cyber crime)* merupakan sebuah tindakan kejahatan yang dilakukan menggunakan teknologi sebagai medianya[1]. Setiap negara memiliki regulasi masing-masing terhadap penggunaan teknologi, hal tersebut dilakukan agar menjadi sebuah aturan yang dapat menggelola aktivitas terhadap teknologi dengan tujuan untuk menanggulangi kejahatan siber *(cyber crime)*[2]. Indonesia salah satu Negara yang memiliki regulasi terhadap informasi dan teknologi, melalui undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik (ITE) indonesia mengatur dan memberikan perlindungan terhadap kasus-kasus kejahatan siber.

Pada perkembangannya modus-modus dalam kejahatan siber (cyber crime) berbanding lurus dengan kemajuan teknologi[3], namun dapat dipastikan bahwa setiap terjadinya kejahatan siber *(cyber crime)* pada kebanyakan kasus akan meninggalkan jejak atau residu kegiatan pelaku maupun korban pada perangkat yang digunakan[4], jejak atau residu kejadian tersebutlah yang nantinya dapat menjadi barang bukti, perlu langkah-langkah yang efisien dan valid dalam

mengelola barang bukti, karenanya barang bukti perlu di identifikasi terlebih dahulu agar nantinya dapat memberikan bantuan pilihan pada penegak hukum dalam menyikap kasus kejahatan tersebut[5].

Barang bukti yang diidenfitikasi haruslah bersifat asli, integritas dan terjaga datanya agar dapat diterima atau dipertahankan, pada proses penyelidikan agar barang bukti dapat leluasa diperiksa penyidik, barang bukti haruslah di duplikasi terlebih dahulu menjadi sebuah *images files*[6], hal tersebut bertujuan agar penyidik dapat memeriksa barang bukti tanpa khawatir telah melakukan perubahan terhadap keabsahan sebuah barang bukti, langkah duplikasi barang bukti dalam istilah digital forensik disebut dengan *forensic imaging*, terdapat beragam perangkat lunak *Forensic imaging* yang bisa digunakan, namun hanya sedikit yang dapat berjalan pada sistem operasi linux yang memiliki karakteristik sumber terbuka *(Opensource)* dan tidak berbayar dalam pendistribusiannya[7], Terdapat beberapa perangkat lunak *forensic imaging* yang dapat bekerja dalam sistem operasi linux, diantaranya adalah *DC3DD, Ddrescue* dan *FTK Imager CLI*.

DC3DD adalah sebuah perangkat lunak dengan sumber terbuka *(Opensources)* yang merupakan pemutakhiran dari perangkat lunak dd yang dapat ditemukan pada paket GNU Coreutils. Perangkat dibuat bertujuan untuk forensik dan keamanan, pemutakhiran pada *DC3DD* terletak pada fitur terbaru yaitu: Hashing on-the-fly, *DC3DD* dapat melakukan hash data input ketika sedang ditransfer, fungsi dari fitur tersebut digunakan untuk membantu memastikan integritas data[8]. Adapun *Ddrescue* merupakan sebuah perangkat lunak utilitas yang digunakan sebenarnya untuk *recovery data tools*, namun tidak menutup kemungkinan bahwa perangkat lunak tersebut mampu melakukan penyalinan data berupa files hingga block devices seperti harddisk, flashdisk dan lain sebagainya[9].

Perangkat lunak *forensic imaging* lainnya adalah *FTK Imager CLI*, perangkat lunak tersebut merupakan satu-satunya versi FTK Imager yang dapat berjalan di sistem operasi linux, FTK Imager dikembangkan oleh accessdata, sama halnya dengan *ddrescue* dalam versi linux tidak ada lagi pengembangan dan pemutakhiran terhadap perangkat lunak *FTK Imager CLI*[10].

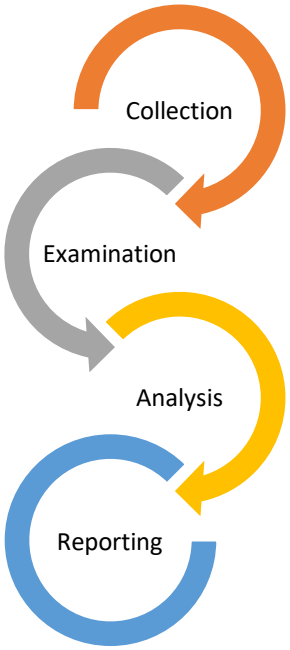
Penelitian dengan topik sejenis pernah dilakukan Razan Maulida Komaryan judul penelitian "Forensic Imaging Application Using Raspberry Pi". Penelitian ini bertujuan membuat perangkat dan aplikasi berbasis GUI untuk proses *forensic imaging* dengan menggunakan single board computer *Raspberry Pi*, serta meneliti kecepatan transfer data akusisi perangkat tersebut. Hasil dari penelitian tersebut menyatakan bahwa perangkat dan aplikasi berbasis GUI untuk proses forensic imaging dengan menggunakan Raspberry Pi dapat berhasil dan digunakan, serta nilai rata-rata kecepatan transfer data akusisi pada proses akusisi yaitu 1,85 MB/s[11]. Joel Panjaitan dengan judul penelitian "Analisis Kinerja Forensic Acquisition Tools untuk Membuat Imaging File pada Masalah IT Forensik" peneliti memaparkan sebuah studi komparatif beberapa tools aplikasi forensik yang digunakan untuk imaging file, tools yang dibandingkan adalah *FTK Imager*, *Encase Forensic Imager* dan *Belkasoft Acquisition Tools* (BAT), hasil penelitian adalah Imager FTK memiliki fitur sesuai standar penyidik untuk menganalisis forensik dasar, BAT adalah tools forensic yang unggul dalam faktor performa[12].

Muhammad Nur Faiz dengan judul penelitian "Comparison of Acquisition Software for Digital Forensics Purposes" peneliti melakukan penelitian perbandingan perangkat lunak akuisisi terbaik terhadap *random access memory* berdasarkan waktu proses, penggunaan memory, registry dan lain sebagainya, penelitian tersebut membandingkan perangkat lunak FTK Imager, Belkasoft, RAM Capturer, Memoryze, Dumpit, Magnet RAM Capturer, hasil penelitian tersebut adalah FTK Imager tertinggal 10 kali artifak dari Dumpit dan Memoryze, dalam hal menangkap artifak Magnet RAM 4 kali lebih banyak dari Belkasoft dan Ram Capturer[13]. Lubis Panjaitan dengan judul penelitian "Analisis Perbandingan Aplikasi Open Source Forensic Image untuk Akuisisi Bukti Digital Ke Dalam Bentuk Image File" meneliti tentang perbandingan *tools IT forensic* dengan membandingkan fitur dari masing-masing tools yaitu: Winhex, FTK Imager, Encase, Registry Recon dan Belkasoft, hasil penelitian tersebut adalah tools IT forensic yang disarankan berupa Winhex dan Belkasoft Evidence Center[14].

Berdasarkan pemaparan diatas menujukan bahwa penelitian perbandingan perangkat lunak forensic imaging pada system operasi linux menggunakan metode static forensic belum pernah dilakukan, maka peneliti merasa perlu melakukan penelitian agar dapat menganalisis dan menemukan perbedaan kinerja diantara masing-masing perangkat lunak tersebut dengan indikator keberhasilan duplikasi harus sesuai dengan keaslian barang bukti.

2. METODE PENELITIAN

Pada penelitian ini menggunakan metode *static forensic* dalam melakukan pengambilan barang bukti, metode *static forensic* adalah sebuah standar yang digunakan dalam penanganan setelah mendapati barang bukti perangkat telah dimatikan[15], sebuah tindakan penelitian memerlukan kerangka kerja agar proses penelitian lebih efisien dan efektif[16], penelitian ini menggunakan kerangka kerja *National Institute of Standards and Technology* (NIST), metode kerangka kerja tersebut memiliki beberapa langkah seperti terlihat pada gambar 1.



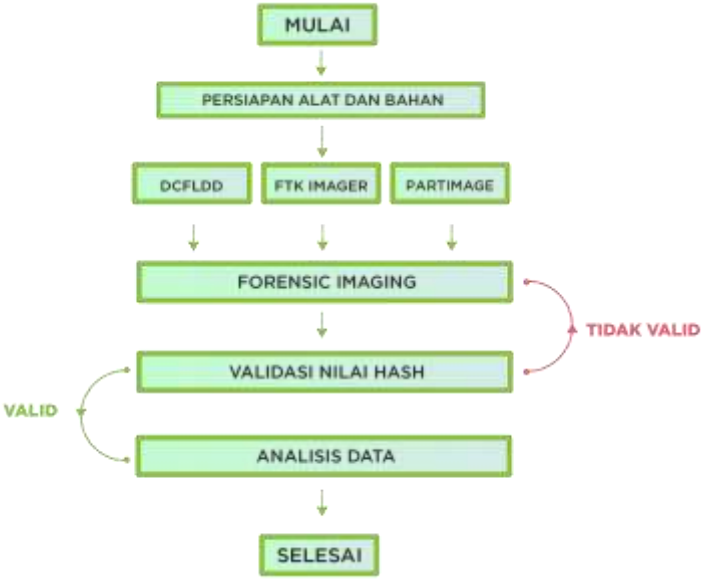
Gambar 1 Langkah Metode NIST

Metode kerangka kerja *National Institute of Standards and Technology* (NIST) terdiri dari 4 langkah yaitu *collection, examination, analysis dan reporting*[17]. *Collection* merupakan langkah koleksi atau mengenali barang bukti yaitu sebuah perangkat keras yang akan diambil datanya sebagai bukti dari sebuah kasus kejahatan siber (cyber crime), pada langkah ini perlu diperhatikan pengamanan integritas data yang terkandung di dalam barang bukti. *Examination* merupakan langkah pengambilan data terhadap perangkat keras menggunakan perangkat lunak *forensic imaging*.

Analysis merupakan langkah pemeriksaan kembali data yang sudah diambil ketika berada pada langkah *examination,* pada langkah ini bertujuan untuk memperoleh informasi agar dapat digunakan untuk bahan analisis. *Reporting* merupakan langkah pembuatan laporan, hasil laporan analisis menyajikan informasi perbandingan kinerja pada perangkat lunak *forensic imaging* dan mampu memberikan anjuran terhadap perbaikan aturan, arahan, langkah-langkah, peralatan, dan aspek lain dari proses forensik.

2.1 Implementasi Skenario Penelitian

Skenario dalam penelitian ini di implementasikan sesuai pada gambar 2, skenario pada penelitian ini dibuat agar mampu menjelaskan langkah pengambilan data yang dilakukan.



Gambar 2. Implementasi Skenario Penelitian

Pada skenario ini peneliti menggunakan 3 perangkat lunak *forensic imaging* yang berkerja pada sistem operasi linux yaitu *DC3DD, FTK Imager* dan *Ddrescue*, kinerja dari ketiga perangkat lunak tersebut haruslah valid dalam langkah validasi nilai hash, agar nilai kinerja dapat dicatat untuk di analisis.

2.2 Alat dan Bahan

Untuk mendukung proses analisis perbandingan perangkat lunak *forensic imaging*, penelitian ini menggunakan alat dan bahan sebagai yang disajikan pada tabel 1.

Tabel 1 Alat dan pendukung penelitian

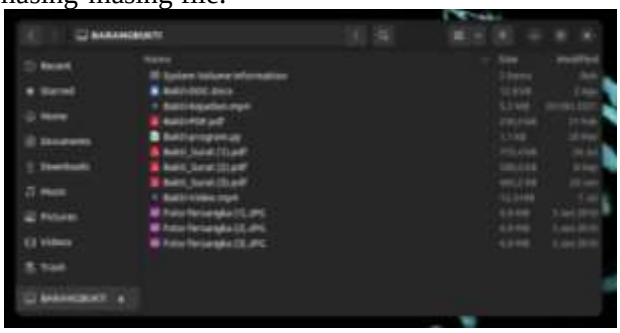
No	Alat dan Bahan	Deskripsi
1.	Lenovo G40 Intel i5	Ubuntu 22.04 LTS 64bit 4 GB, untuk analisis forensik
2.	Adata 16 GB	Objek barang bukti
3.	*DC3DD*	Software forensic imaging
4.	*Ddrescue*	Software forensic imaging
5.	FTK Imager CLI	Software forensic imaging

3. HASIL DAN PEMBAHASAN

Langkah implementasi yang dilakukan pada penelitian ini sesuai pada gambar 2 dengan metode kerangka kerja penelitian *National Institute of Standards and Technology* (NIST) yang meliputi *collection, examination, analysis dan reporting*.

3.1 collection

Pada langkah *collection* atau pengumpulan data yang akan dijadikan barang bukti digital, pada objek penelitian terdapat adanya sejumlah *file* dengan macam-macam *filename extension* seperti yang terlihat pada gambar 3. Perangkat keras dengan merek Adata berstatus menjadi objek barang bukti kejahatan siber dalam bentuk *physical device*. Pada gambar 3 terlihat juga besaran dari masing-masing file.



Gambar 3. Isi drive

Langkah collection juga akan melakukan pencatatan spesifikasi atau detail dari barang bukti yang digunakan. Pada gambar 4 terlihat spesifikasi dan nilai hash seluruh file barang bukti tersebut menggunakan beberapa perintah dasar linux yaitu *sha1sum* dan *fdisk*.

Gambar 4. Informasi hash dan spesifikasi

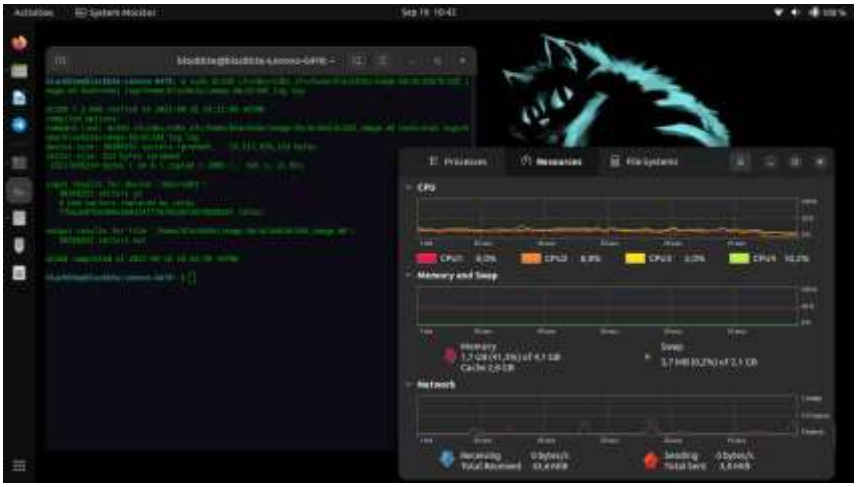
3.2 Examination

Tahap ini merupakan tahap pengujian, pemeriksaan dan pengambilan data kinerja perangkat lunak saat dilakukan *forensic imaging* pada barang bukti. perangkat lunak *dc3dd, ddrescue* dan *FTK Imager* telah terpasang pada alat pengujian disajikan pada gambar 5 menggunakan *attributes* perintah *–version* pada terminal *ubuntu*.

Gambar 5. Versi Perangkat Lunak

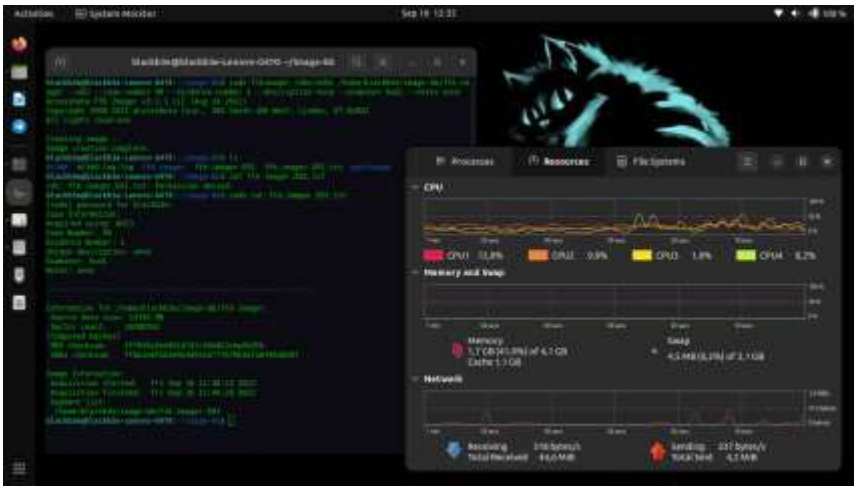
Pada pengujian proses *imaging* pada perangkat lunak *DC3DD* dijalankan dengan menggunakan perintah **“sudo dc3dd if=/direktori_sumber of=/direktori_target hash=sha1**

log=/direktori_log", pada gambar 6 disajikan hasil akuisisi oleh perangkat lunak *DC3DD* yang berhasil melakukan *imaging device* menjadi *image file* dengan *extensions .dd,* perangkat lunak *DC3DD* menyelesaikan *imaging* dalam waktu 11 menit dan 31 detik.



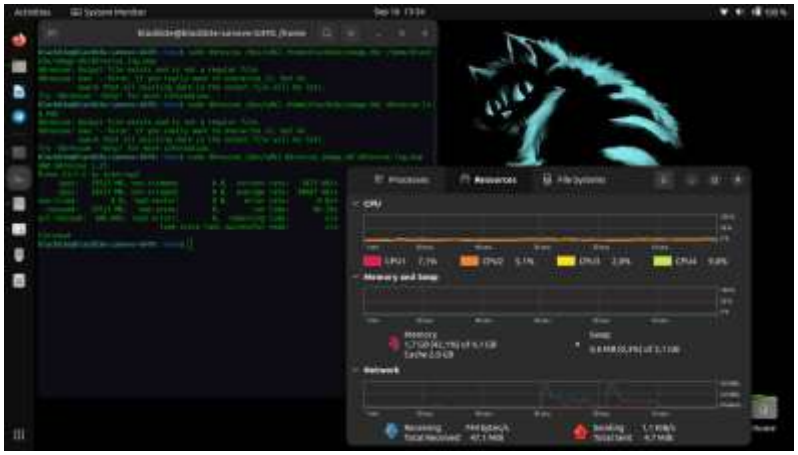
Gambar 6. Proses *imaging DC3DD*

Pada perangkat lunak FTK Imager proses *imaging* dijalankan dengan menggunakan perintah **"ftkimager /perangkat_sumber /folder_tujuan --e01 --case-number 99 --evidence-number 1 --description none --examiner nama-penyeledik --note none"**, pada gambar 7 disajikan hasil akuisisi oleh perangkat lunak *FTK Imager CLI*yang berhasil melakukan *imaging device* menjadi *image file* dengan *extensions .E01,* perangkat lunak *FTK Imager CLI* menyelesaikan imaging dalam waktu 8 menit dan 13 detik.



Gambar 7. Proses *Imaging FTK Imager CLI*

Pada perangkat lunak *ddrescue* proses *imaging* dijalankan dengan menggunakan perintah **"ddrescue /input_file /output_file /Target_file.map"**, pada gambar 8 disajikan hasil akuisisi oleh perangkat lunak *ddrescue* yang berhasil melakukan *imaging device* menjadi *image file* dengan *extensions .dd,* perangkat lunak *ddrescue* menyelesaikan imaging dalam waktu 8 menit dan 25 detik.

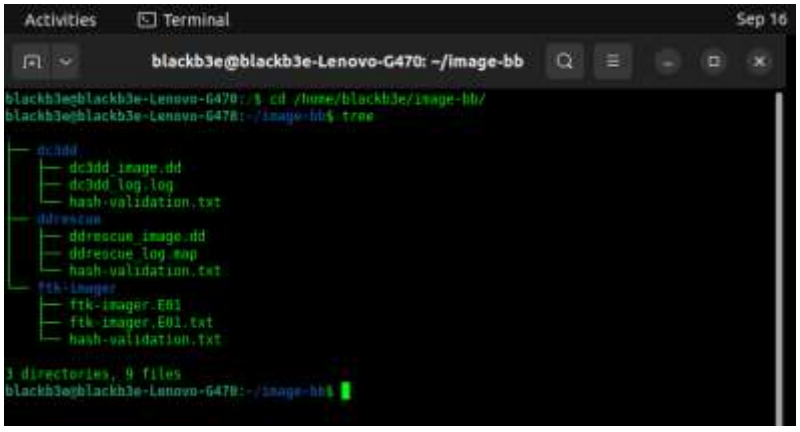


Gambar 8. Proses *imaging DDRescue*

3.3 Analysis

Hasil analisis dari masing-masing perangkat lunak untuk proses *forensic imaging* yang digunakan dalam penelitian ini dapat berkerja lancar, dibuktikan dari berhasilnya menciptakan sebuah salinan drive menjadi *image files*.

Pada gambar 9 disajikan hasil keluaran *file images* yang dilakukan pada perangkat lunak *DC3DD* dan *DDRescue* memiliki 2 format yang sama yaitu menggunakan *file extension .dd*, sedangkan terdapat perbedaan pada perangkat lunak *FTK Imager*, file *extension* yang dihasilkan menjadi *image files* menggunakan *extension .e01*, file yang dihasilkan *FTK Imager* memiliki cara tersendiri untuk bisa di mount pada sistem operasi linux.



Gambar 9. Strukur *Folder*

Untuk memastikan keaslian atau integrasi data maka diperlukan sebuah langkah validasi mencocokan nilai *hash sha1*, agar *image files* dapat di ekplorasi dengan tujuan validasi data, maka pada masing-masing hasil keluaran *images files* harus di *mount* pada sistem operasi terlebih dahulu, untuk file keluaran dari perangkat lunak *DC3DD* dan *DDRescue* memiliki alur perintah yang sama karena berektensikan *.dd*, dapat dilihat pada gambar 10 bahwa perintah awal ialah membuat sebuah *temporary file* terlebih dahulu barulah melakukan perintah *mount*, terakhir hash dari sha1 bisa diambil dengan menunjuk *input-folder* tersebut.

```
mkdir /mnt/image
sudo mount -o loop /folder_image /mnt/image
sha1sum /mnt/image >> tujuan_file.txt
```

Gambar 10. Susuan Perintah mounting *dd files*

Berbeda dengan file berektensikan .e01 hasil keluaran dari *FTK Imager* diperlukan sebuah tambahan perangkat lunak yaitu *ewfmount*, pada gambar 11 disajikan alur perintah yang diperlukan agar mounting e01 dapat berjalan, setelah *ewfmount* terpasang pada perangkat utama maka *ewfmount* harus diberikan ponting file terlebih dahulu, tujuannya adalah menjadikan *mounting file passive*, kemudian perintah mount bisa dijalankan menuju pointing mount yang baru agar mount point tersebut dapat *Active*, terakhir perintah pengambilan hash sha1 pada image e01 dapat dilakukan.

```
mkdir /mnt/temp
ewfmount /folder_image /mnt/temp
mount /mnt/temp/ewf1 /tujuan_mountpoint -o loop
sha1sum /mnt/image >> tujuan_file.txt
```

Gambar 11. Susuan Perintah mounting *e01 files*

Kemampuan kinerja dari masing-masing perangkat lunak menghasilkan waktu proses *imaging* yang berbeda-beda, pada penggunaan sumberdaya seperti RAM, CPU dan Network yang bisa dilihat pada system monitor, menunjukkan bahwa kebutuhan akan sumber daya bukan merupakan hal penting untuk kebutuhan pada saat *forensic imaging*.

3.4 Report

Hasil validator *hashing sha1* yang dilakukan pada akhir proses *imaging* menjadi faktor penentu valid atau tidaknya sebuah hasil *imaging*, pada ketiga perangkat lunak tersebut tidak didapati nilai hash yang berbeda dari nilai hash aslinya. Berikut adalah tabel 2 hasil validasi nilai *hash sha1*.

Tabel 2 Nilai Hash SHA1

No	Alat dan Bahan	Hash Original drive	Hash DC3DD	Hash DDRescue	Hash FTK Imager
1.	Bukti-DOC.docx	0efb713a9839586133b1c71e2fc744867185f127	0efb713a9839586133b1c71e2fc744867185f127	0efb713a9839586133b1c71e2fc744867185f127	0efb713a9839586133b1c71e2fc744867185f127
2.	Bukti-Kejadian.mp4	604b049e55ca6c69fd990a6052a80f624f3a406c	604b049e55ca6c69fd990a6052a80f624f3a406c	604b049e55ca6c69fd990a6052a80f624f3a406c	604b049e55ca6c69fd990a6052a80f624f3a406c
3.	Bukti-PDF.pdf	7d7d4c0ec21a8729b28cf9a3b1837b53973ecd29	7d7d4c0ec21a8729b28cf9a3b1837b53973ecd29	7d7d4c0ec21a8729b28cf9a3b1837b53973ecd29	7d7d4c0ec21a8729b28cf9a3b1837b53973ecd29
4.	Bukti-program.py	bad88e41e9d26c1a7fd053b40444b3db1f73310c	bad88e41e9d26c1a7fd053b40444b3db1f73310c	bad88e41e9d26c1a7fd053b40444b3db1f73310c	bad88e41e9d26c1a7fd053b40444b3db1f73310c
5.	Bukti_Surat (1).pdf	e06cf4b46247971260e52515676ace1dc6f99394	e06cf4b46247971260e52515676ace1dc6f99394	e06cf4b46247971260e52515676ace1dc6f99394	e06cf4b46247971260e52515676ace1dc6f99394
6.	Bukti_Surat (2).pdf	d4c7502d8ecda62383b99b83afa31959d9597fc2	d4c7502d8ecda62383b99b83afa31959d9597fc2	d4c7502d8ecda62383b99b83afa31959d9597fc2	d4c7502d8ecda62383b99b83afa31959d9597fc2
7	Bukti_Surat (3).pdf	ab6b836ae2ddb2d6926a51241c9d2d93d9b64221	ab6b836ae2ddb2d6926a51241c9d2d93d9b64221	ab6b836ae2ddb2d6926a51241c9d2d93d9b64221	ab6b836ae2ddb2d6926a51241c9d2d93d9b64221
8.	Bukti-Video.mp4	5100e5d2d7f943ce43d0efb02008d90b072a8218	5100e5d2d7f943ce43d0efb02008d90b072a8218	5100e5d2d7f943ce43d0efb02008d90b072a8218	5100e5d2d7f943ce43d0efb02008d90b072a8218
9.	Foto-Tersangka (1).JPG	5a241059a90822fbd050f14659cac783859862dd	5a241059a90822fbd050f14659cac783859862dd	5a241059a90822fbd050f14659cac783859862dd	5a241059a90822fbd050f14659cac783859862dd
10	Foto-Tersangka (2).JPG	bd94d24504ba45d852eb6fd47138a8121f5cc2f9	bd94d24504ba45d852eb6fd47138a8121f5cc2f9	bd94d24504ba45d852eb6fd47138a8121f5cc2f9	bd94d24504ba45d852eb6fd47138a8121f5cc2f9
11.	Foto-Tersangka (3).JPG	8c4f52614641a523218dc006c49e4d4b8c7b6b79	8c4f52614641a523218dc006c49e4d4b8c7b6b79	8c4f52614641a523218dc006c49e4d4b8c7b6b79	8c4f52614641a523218dc006c49e4d4b8c7b6b79
	HASIL VALIDASI	VALID	VALID	VALID	VALID

Pada table 3 terlihat informasi hasil waktu proses *imaging*, ukuran keluaran *files images* dan monitoring penggunaan resource yang dilakukan oleh *dc3dd, ddrescue* dan *ftkimager.*

Tabel 3. Hasil Pengukuran Kinerja Perangkat Lunak

No	Nama Perangkat Lunak	Waktu Proses	Kecepatan Proses	*Resource Monitioring*
1.	*DC3DD*	11 menit 31 detik	21 MBps	CPU 12,75%, RAM 41,3%
2.	*DDrescue*	8 menit 25 detik	30 MBps	CPU 5,8%, RAM 42,1%
3.	FTK Imager CLI	8 menit 13 detik	31 MBps	CPU 17,8%, RAM 39,8%

4. KESIMPULAN

Berdasarkan hasil penelitian tentang analisis perangkat lunak untuk *Forensic Imaging* menggunakan *DC3DD, DDrescue* dan *FTK Imager CLI* pada barang bukti berupa *USB drive* memberikan kesimpulan bahwa metode *static forensic* serta kerangka kerja *National Institute of Standards and Technology* (NIST) Dapat diterapkan dengan baik. Terdapat perbedaan dalam keluaran file jenis extensi yang dimiliki *FTK Imager CLI* berbeda dengan *DC3DD* dan *ddrescue* yang berupa *.e01*. Dalam durasi waktu proses imaging perangkat lunak *FTK imager* lebih cepat 2 menit 18 detik dari perangkat lunak *DC3DD* dan 12 detik dari perangkat lunak *DDrescue*. *FTK Imager* memiliki kecepatan pada saat proses *imaging* tertinggi dibanding *DDrescue dan DC3DD*. *DDrescue* merupakan perangkat lunak yang menggunakan resource paling sedikit dibanding *DC3DD* dan *FTK Imager CLI*.

5. SARAN

Pada penelitian selanjutnya dapat menggunakan faktor analisa kinerja perangkat lunak ketika proses *imaging* dengan tambahan fitur seperti kompresi, *block* dan enkripsi. Perbandingan Perangkat lunak yang berbeda dan lebih baru, namun dapat berkerja normal pada sistem operasi *linux*.

UCAPAN TERIMA KASIH

Penulis mengucapkan terimakasih kepada setiap pihak yang telah mendukung dan membantu proses terciptanya tulisan ini.

DAFTAR PUSTAKA

[1] E. Chintia, R. Nadiah, H. N. Ramadhani, Z. F. Haedar, A. Febriansyah, And N. A. Rakhmawati S.Kom., M.Sc.Eng, “Kasus Kejahatan Siber Yang Paling Banyak Terjadi Di Indonesia Dan Penanganannya,” *J. Inf. Eng. Educ. Technol.*, Vol. 2, No. 2, P. 65, Feb. 2019, Doi: 10.26740/Jieet.V2n2.P65-69.

[2] H. Djanggih And N. Qamar, “Penerapan Teori-Teori Kriminologi Dalam Penanggulangan Kejahatan Siber (Cyber Crime),” *Pandecta Res. Law J.*, Vol. 13, No. 1, Pp. 10–23, Aug. 2018, Doi: 10.15294/Pandecta.V13i1.14020.

[3] B. P. Ramadhan, A. Yudhana, And I. Riadi, “Implementasi Dan Analisis Serangan Phishing Menggunakan Router Wireless Berbasis Openwrt,” P. 4, 2019.

[4] I. Riadi, R. Umar, And I. M. Nasrulloh, “Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute Of Justice (Nij),” *Elinvo Electron. Inform. Vocat. Educ.*, Vol. 3, No. 1, Pp. 70–82, Jul. 2018, Doi: 10.21831/Elinvo.V3i1.19308.

[5] A. Yudhana, I. Riadi, And I. Anshori, “Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist,” *It J. Res. Dev.*, Vol. 3, No. 1, Pp. 13–21, Aug. 2018, Doi: 10.25299/Itjrd.2018.Vol3(1).1658.

[6] F. Yudha, E. Ramadhani, F. Rahma, And W. N. Hamzah, "Pendekatan Dd Sebagai Salah Satu Teknik Akuisisi Perangkat Android," *Cyber Secur. Dan Forensik Digit.*, Vol. 3, No. 1, Pp. 33–38, Jul. 2020, Doi: 10.14421/Csecurity.2020.3.1.2000.
[7] E. Haryanto And I. Riadi, "Forensik Internet Of Things Pada Device Level Berbasis Embedded System," *J. Teknol. Inf. Dan Ilmu Komput.*, Vol. 6, No. 6, P. 703, Dec. 2019, Doi: 10.25126/Jtiik.2019661828.
[8] Zhong, Xianming, Et Al., "A Virtualization Based Monitoring System For Mini-Intrusive Live Forensics," *Int. J. Parallel Program.*, No. 43.3, Pp. 455–471, 2015.
[9] Roussev, Vassil., "System Analysis," *Digit. Forensic Sci. Springer Cham*, Pp. 29–98, 2017.
[10] E. Olson And N. Shashidhar, "Low Budget Forensic Drive Imaging Using Arm Based Single Board Computers," *J. Digit. Forensics Secur. Law*, 2016, Doi: 10.15394/Jdfsl.2016.1373.
[11] D. Oleh, "Forensic Imaging Application Using Raspberry Pi" P. 96.
[12] J. Panjaitan And A. C. Sitepu, "Analisis Kinerja Forensic Acquisition Tools Untuk Membuat Imaging File Pada Masalah It Forensik," Vol. 1, No. 2, P. 9, 2021.
[13] M. N. Faiz And W. A. Prabowo, "Comparison Of Acquisition Software For Digital Forensics Purposes," *Kinet. Game Technol. Inf. Syst. Comput. Netw. Comput. Electron. Control*, Pp. 37–44, Nov. 2018, Doi: 10.22219/Kinetik.V4i1.687.
[14] R. M. F. Lubis And J. Panjaitan, "Analisis Perbandingan Aplikasi Open Source Forensic Image Untuk Akuisisi Bukti Digital Ke Dalam Bentuk Image File," Vol. 2, No. 1, P. 9, 2022.
[15] I. Riadi, S. Sunardi, And A. Hadi, "Analisis Bukti Digital Trim Enable Ssd Nvme Menggunakan Metode Static Forensics," *Juita J. Inform.*, Vol. 8, No. 1, P. 65, May 2020, Doi: 10.30595/Juita.V8i1.6584.
[16] F. Anggraini And A. Yudhana, "Analisis Forensik Aplikasi Tiktok Pada Smartphone Android Menggunakan Framework Association Of Chief Police Officers," Vol. 9, No. 4, P. 11, 2022.
[17] M. I. Syahib, I. Riadi, And R. Umar, "Analisis Forensik Digital Aplikasi Beetalk Untuk Penanganan Cybercrime Menggunakan Metode NIST," p. 6, 2018.