Journal of SAKIRA (*Secure And Knowledge-Intelligent Research in Cybersecurity And Multimedia*) e-ISSN 3046-773X

Vol.2 , No.1 , Juni 2024, pp. 37~42

Application of Data Recovery Tools in Flash Drive Forensic Data Acquisition

Muhammad Immawan Aulia[1]*, Panggah Widiandana [2]*, Latifah Iriani [3], Muhammad Fauzan Gustafi[4]**, Muhammad Azam Hasani [5]***

* Informatika, Universitas Islam Mulia Yogyakarta, Yogyakarta, Indonesia
** Informatika, Universitas Siber Muhammadiyah, Yogyakarta, Indonesia
** Sistem Informasi, Universitas Siber Muhammadiyah, Yogyakarta, Indonesia

muhimmawanaulia16@uim-yogya.ac.id[1], panggah.widiandana@uim-yogya.ac.id[2], latifahiriani@sibermu.ac.id[3], muhammadfauzangustafi@sibermu.ac.id[4], azamhasanie.2@gmail.com[5]

Article Info

Article history:

Received...
Revised...
Accepted...

Keywords:

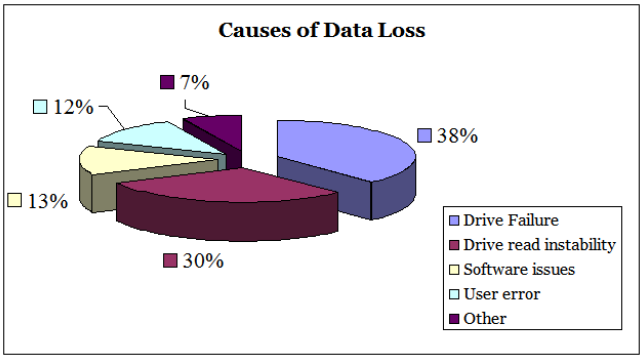
Pemulihan Data, Flashdrive, Forensik Statik, Disk Drill, Partisi Unallocated

ABSTRACT

In this fast-paced digital era, flash drives have become one of the most popular storage methods. At times, flashdrive data can be lost, and losing this data can have significant consequences both professionally and personally. In this study, an example of data recovery from an inaccessible flashdrive after being forcibly removed during the data transfer process is discussed. Static forensic methods and the Disk Drill application succeeded in finding 7626 files from unallocated partitions with a total size of 17.3 GB. The digital evidence that has been recovered is 49 files which are presented in the form of files with various extensions, such as images, audio, documents and archives. Advanced data recovery tool capabilities enable recovery of various types of files, which increases the chances of rescuing lost data.

I. PENDAHULUAN

Data telah menjadi aset yang sangat berharga bagi individu, kelompok, dan bahkan negara di era digital yang serba cepat ini. Data digunakan untuk berbagai tujuan, seperti menyimpan foto pribadi, dokumen penting, dan informasi keuangan yang sensitif. Namun, meskipun data mudah diakses dan disimpan, ada risiko kehilangan data. Data survei dari perusahaan yang berfokus pada pemulihan data dapat digunakan untuk menyelidiki faktor-faktor utama yang menyebabkan kehilangan data. Kegagalan hard drive adalah penyebab paling umum dari kehilangan data, menyumbang 38% dari semua kasus. *Corrupt software*, yang mungkin termasuk kerusakan yang disebabkan oleh perangkat lunak sistem atau program lain (misalnya, serangan virus), menyumbang 13% dari kehilangan data. Instabilitas membaca drive mencakup situasi di mana kerusakan media atau degradasi mencegah akses ke data pada *disk*. Selain itu, 12% hilangnya data disebabkan oleh kesalahan manusia. Ini mencakup data yang dihapus secara tidak sengaja dan partisi *hard drive* yang salah. [1].

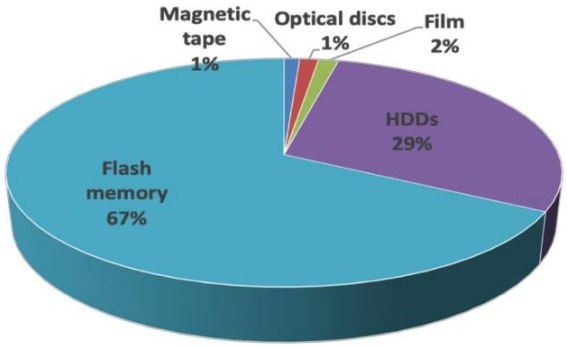


Gambar 1. Penyebab kehilangan data

e-ISSN 3046-773X

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 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 [2]. Digital forensik fokus pada penemuan bukti digital yang bisa tersimpan pada storage komputer sementara, storage permanen, USB, CD, internet dan lainnya [3].

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 berubah dengan kondisi apa pun. Bukti digital dapat ditemukan di *hard drive*, *flash drive*, perangkat seluler, Kemudian data ini akan dibawa investigator ke lab forensik untuk dilakukan berbagai metode agar dapat menganalisis data sebagai bukti secara forensik.[4][5]. Gambar 2. Menampilkan *flash memori* termasuk dengan *flash drive* mendapatkan nilai sebesar 67%.



Gambar 2. Diagram Pengunaan media penyimpanan terbanyak

Terhapus dan kerusakan *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.[6].

Akibatnya, penting bagi kita untuk memahami bahaya kehilangan data dan mengambil tindakan pencegahan yang tepat. Jika hal ini terjadi, memahami cara memulihkan data yang hilang merupakan langkah penting. Dalam proses transfer data, kasus pemulihan data dari *flashdrive* yang tidak dapat diakses akan dibahas dalam penelitian ini.

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, Drill *Disk* dan lainnya.

Alat canggih *Disk* Drill dapat memindai, memulihkan, dan melindungi data di hampir semua media penyimpanan yang mendukung sistem operasi Mac dan Windows. Alat ini tersedia dalam tiga versi: versi Basic, versi Pro, yang berharga $89,00, dan versi Enterprise, yang berharga $499,00 [7]. Lebih dari 400 format *file* gambar, dokumen, *audio*, *video*, dan arsip dapat dipulihkan dengan program ini dari sistem *file* yang didukung seperti FAT16, FAT32, exFAT, NTFS, ext3, dan ext4. Selain itu, tiga fitur khusus alat ini, yaitu brankas pemulihan, pemulihan terjamin, dan monitor S.M.A.R.T. *Recovery Vault* memiliki kemampuan untuk melacak setiap *file* yang dihapus dari komputer dan mengingat lokasi dan nama *file* tersebut. Meskipun pengguna mengosongkan recycle bin, pemulihan Terjamin dapat menyalin setiap *file* yang dihapus dari recycle bin dan menyediakan opsi "*Undelete*". Terakhir, S.M.A.R.T monitor memantau kesehatan media penyimpanan dan memberi tahu pengguna jika ada pilihan yang salah. Alat ini juga memiliki alat *disk* gratis untuk versi pro dan dasar, yang memungkinkan pembersihan perangkat lunak, pembuatan cadangan, dan pemantauan kesehatan *disk* [8].

Gambar 3. Aplikasi Drill Disk

Versi dasar program ini dapat memulihkan *file* hingga 500 MB, memiliki perlindungan data *Recovery* Vault, dan

e-ISSN 3046-773X

membuat cadangan *byte*-ke-*byte* dari *disk* yang gagal dan pratinjau sebelum pemulihan. Versi Pro dari program ini memiliki fitur pemindaian cepat dan mendalam, algoritma FAT dan NTFS yang cerdas, pencarian partisi yang hilang, dll., pemulihan untuk semua jenis *file* dan media penyimpanan, dan lisensi untuk satu pengguna.

Kekurangan alat ini termasuk pratinjau *file* yang tidak efektif, tidak adanya versi portabel, kemampuan untuk menyimpan pemindaian dan pemulihan ulang, berbagai opsi pemindaian, dan perlindungan data premium. Selain itu, alat ini sulit untuk dimulai dan kadang-kadang berhenti bekerja [9].

II. METODE PENELITIAN

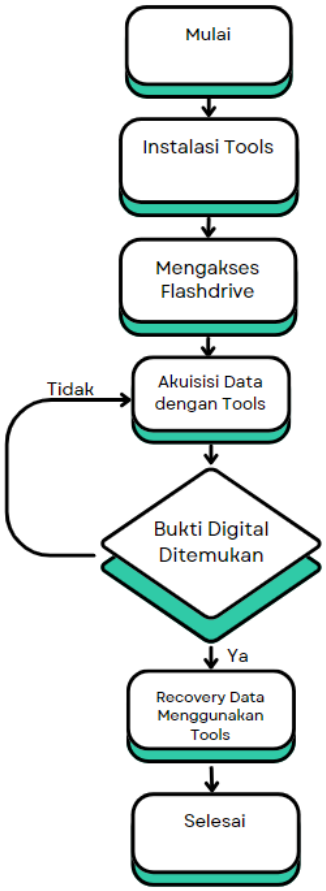
Statik Forensik difokuskan pada pemeriksaan sebuah duplikat yang disebut salinan *disk* untuk mengeluarkan konten memori, seperti *file* yang dihapus, riwayat penelusuran *web*, *fragment file*, koneksi jaringan, *file* yang dibuka, riwayat log in pengguna, dll. untuk membuat *timeline* yang memberikan pandangan, misalnya statika parsial atau ringkasan tentang aktivitas yang dilakukan pada sistem korban sebelum mematikannya. Dalam analisis statis berbagai jenis perangkat lunak dan perangkat keras seperti Fundl, RegCon digunakan untuk dumping memori dan penyortiran data pembuktian untuk analisis dan tujuan presentasi. Data forensik diperoleh dengan menggunakan berbagai jenis perangkat eksternal seperti USB, eksternal *hard drive* atau CD, DVD. Kemudian data ini dibawa investigator untuk melakukan berbagai metode agar dapat menganalisis data sebagai bukti secara forensik. [10].

Statik Forensik mengacu pada penyelidikan forensik tradisional yang dilakukan dengan perangkat yang tidak aktif atau tidak berfungsi. Forensik statis berfokus pada pemeriksaan duplikat media penyimpanan mengambil data yang ada, misalnya, seperti *file* yang dihapus, riwayat situs *web*, riwayat pengguna, dan riwayat *log* komputer. Salinan bukti dapat diperoleh dengan menggunakan berbagai jenis media penyimpanan eksternal seperti *Flash disk*, External *Hard Drive*, dan penyimpanan lainnya. [11][12]. Ilustrasi pada Gambar 4.

Gambar 4. Tahapan Statik Forensik

Skenario pada penelitian ini "seorang pegawai kantoran bernama Jaka sedang melakukan proses *copy data* menggunakan *flash drive*. Kemudian Jaka tanpa sengaja mencabut paksa flash drive tersebut padahal masih dalam proses *copy data*, setelah dicek lebih lanjut, ternyata *flash drive* Jaka setelah dikoneksikan ke laptop tidak terdeteksi dan mengalami *hardware failure*.".

Gambar 5 adalah Ilustrasi proses akuisisi data pada penelitian ini.



Gambar 5. *Flowchart* proses akuisisi data pada *flashdrive*

Uraian proses akuisisi data dari *flowchart* sebagai berikut:

- Melakukan instalasi *tools* Drill *Disk* untuk melakukan proses *recovery data.*
- Mengakses *Flashdrive* menggunakan laptop.
- Mengoperasikan *Drill Disk* untuk akusisi data pada partisi di *flashdrive*.
- Apabila ditemukan bukti digital (*file* yang terhapus) maka proses *recovery* dapat dilakukan.

Pada penelitian ini *hardware* dan *software* yang digunakan memiliki spesifikasi sebagai berikut:

e-ISSN 3046-773X

TABEL I.

SPESIFIKASI *HARDWARE*

Alat	*Merk*	*Spesifikasi*
Laptop	Acer	Acer Aspire E14 E5-422 AMD A6-7310
Flashdrive	Toshiba	8 GB

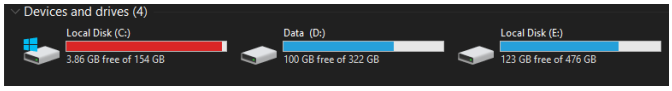
TABEL II.

SPESIFIKASI *SOFTWARE*

Tools	*Versi*
Drill *Disk*	5.5.900.0
Windows 10 Pro	22H2

III. HASIL DAN PEMBAHASAN

Upaya pada saat mengakses *flashdrive* dilakukan dengan melakukan pengecekan apakah partisi *flashdrive* terdeteksi, namun yang terdeteksi hanya partisi yang digunakan pada laptop saja seperti pada Gambar 6.

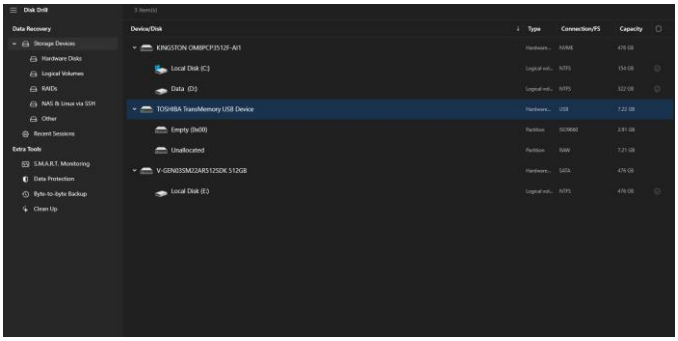


Gambar 6. Partisi *flashdrive* tidak terdeteksi

Setelah dilakukan pengecekan ulang pada fitur sistem operasi windows 10 Pro yaitu *disk management* mendeteksi adanya partisi dari *flashdrive* yaitu dengan nama *Disk* 2 namun berstatus *unallocated* sebesar 7,22 GB (*Giga Byte*) dan 9MB (*Mega Byte*) seperti pada Gambar 7.

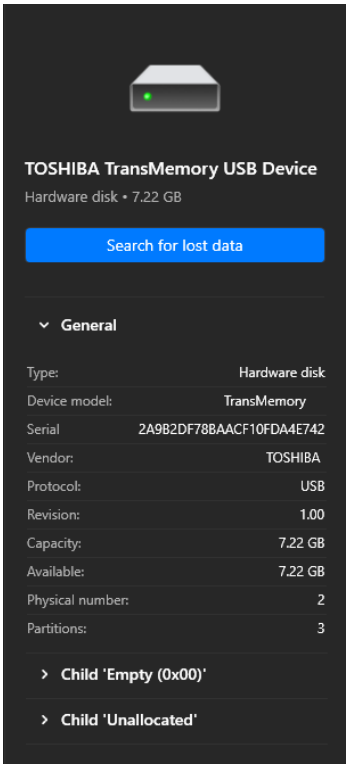
Gambar 7. Partisi *flashdrive* di *Disk Management*

Pada Gambar 8, tampilan *tools* Drill *Disk* dioperasikan pada sistem operasi windows 10 Pro dan menampilkan partisi *flashdrive* ialah Toshiba TransMemory USB Device dengan partisi Empty (0x00), Unallocated dan partisi yang terdapat pada laptop yang digunakan Kingston OM8PCP3512F-AI1 dengan partisi Local *Disk* (C:) Data (D:) dan V-Gen 03SM22AR512SDK 512GB Local *Disk* (E:)



Gambar 8. Tampilan *Tools* Drill *Disk*

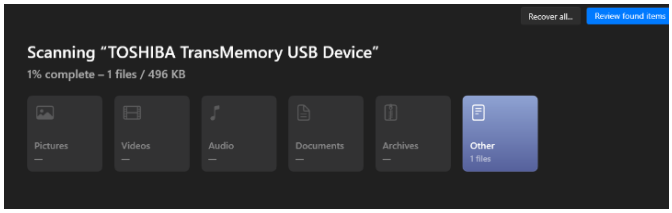
Setelah memilih partisi *flashdrive* yang terdeteksi pada *tools* Drill *Disk* terdapat informasi umum dari media penyimpanan *flashdrive* seperti tipe, model, nomor seri, vendor, protokol, status revisi, kapasitas asli, kapasistas yang tersedia, nomor fisik dan jumlah partisi, tekan tombol *Search for lost data*, seperti pada Gambar 9.



Gambar 9. Fitur Pencarian data yang hilang

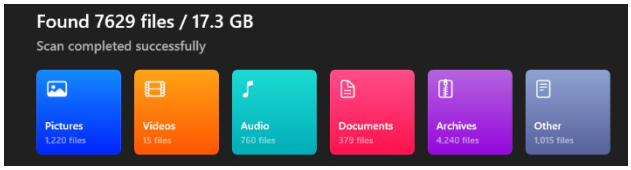
Proses berlanjut dari *search for lost data* dengan menampilkan jumlah beberapa jenis *file* seperti gambar, *video*, *audio*, dokumen, arsip dan lainnya seperti pada Gambar 10.

e-ISSN 3046-773X



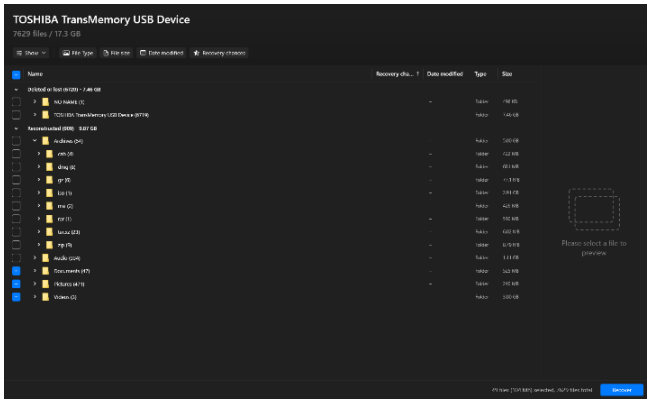
Gambar 10. Proses pencarian data yang hilang

Kemudian proses pencarian data yang hilang pada partisi *flashdrive* ditemukan beragam jenis *file* dengan jumlah pada *file* gambar sebanyak 1.220, *video* 15 *file*, *audio* 760 *file*, dokumen 379 *file*, arsip 4.240 *file* dan lainnya 1.015 *file* sehingga total keseluruhan sebanyak 7629 *file* dengan berbagai macam esktensi serta memiliki total *size* sebesar 17,3 GB (*Giga Byte*) seperti pada gambar 11.



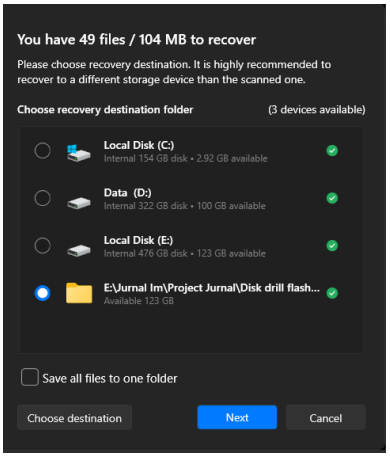
Gambar 11. Proses pencarian data yang hilang selesai

Terdapat dua jenis kategori *file* yang terdeteksi yakni *Deleted or Lost* sebanyak 6720 *file* dengan size 7.46 GB dan *Reconstructed* sebanyak 909 *file* sizenya 9.87GB lalu pilih data yang ingin dipulihkan dengan klik centang biru disisi kiri kemudian tekan tombol *recover* seperti pada Gambar 12.



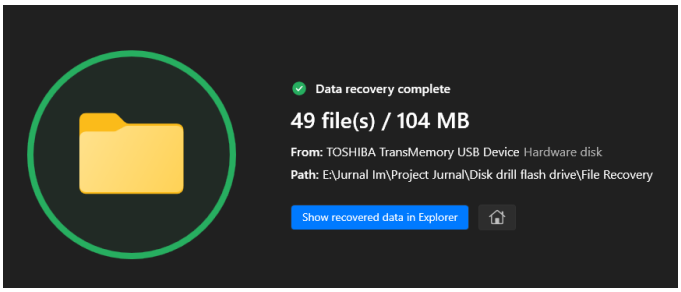
Gambar 12. Pemilihan data yang ingin dipulihkan

Tampilan proses selanjutnya untuk melakukan proses *recovery data* dari sejumlah data yang sudah dipilih sebelumnya lalu memilih *folder destination* yang akan dijadikan sebagai *folder* tempat menyimpan *file* hasil dari *recovery*, seperti pada Gambar 13.



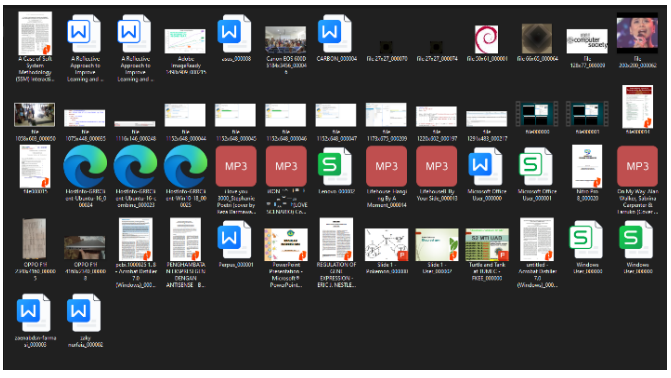
Gambar 12. Memilih *folder destination* untuk *file recovery*

Tampilan ketika proses *recovery* selesai, terdapat sebanyak 49 *file* dengan beragam esktensi *file* dan total *file size*nya sebesar 104 MB (*Mega Byte*) seperti pada gambar 14.



Gambar 14. Proses *recovery* selesai

Hasil dari *recovery data* terdapat berbagai jenis *file* yaitu 24 *file* dokumen 21.3MB, 23 *file* gambar 13MB, 2 *file video* 70MB sehingga didapatkan total keseluruhan 104MB yang berhasil di-*recovery* yang disajikan pada tampilan *folder* seperti pada Gambar 15.



Gambar 15. 49 *file* yang berhasil di-recovery

e-ISSN 3046-773X

IV. KESIMPULAN

Memulihkan data dari *flashdrive* yang tidak dapat diakses setelah dicabut secara paksa dapat dicapai dengan menggunakan metode Forensik Statik yang tepat dan aplikasi pemulihan data yang sesuai. Studi kasus ini menunjukkan bahwa alat pemulihan data yang populer, *Disk* Drill, dapat memulihkan 7629 *file* berukuran 17,3 GB dari partisi yang tidak teralokasikan pada *flashdrive* yang rusak serta berhasil memulihkan 49 *file* terpilih dengan beragam ekstensi. Drill *disk* dapat membantu dalam investigasi digital dan pemulihan data dalam berbagai situasi karena dapat memulihkan berbagai jenis *file*, termasuk dokumen, arsip, gambar, dan *audio*.

DAFTAR PUSTAKA

[1] David M. Smith, Michael L. Williams (2007). https://www.deepspar.com/wp-data-loss.html. diakses 25 Juni 2024.

[2] Muhammad N.F., Rusydi U., Anton Y. Analisis Live Forensics untuk Perbandingan Kemananan Email Pada Sistem Operasi Proprietary, Jurnal Ilmiah ILKOM. 2016; 8(3):242–247

[3] Rafique M., & Khan M. N. A. Exploring static and live digital forensics: Methods, practices nd tools. International Journal of Scientific & Engineering Research. 2013; 4(10): 10481056.

[4] N.A.Muhammad, "Digital Forensik:Panduan Praktis Investigasi Komputer".Jakarta:Salemba Infotek.2012.

[5] Kessler, G.C., "Anti-Forensics and the Digital Investigator".2007

[6] Saudi, M. M. "An overview of *disk* imaging tool in computer forensics". SANS Institute. 2001

[7] Mamoona, R., Khan, M.N.A. "Exploring Static and Live Digital Forensics: Methods, Practices and Tools". International Journal of Scientific & Engineering Research Volume 4, Issue 10, October-2013 ISSN 2229-5518

[8] Clever*file*s, 2020. What is *Disk* Drill?. [Online] Available at: https://www.clever*file*s.com/help/what-is-*disk*-drill/

[9] *Disk* Drill, 2020. Best Data *Recovery* Software. [Online] https://www.clever*file*s.com/*disk*-drill-windows.html diakses 27 Juli 2024

[10] *Disk* Drill, 2020. Best Data *Recovery* Software of 2020. [Online]: https://www.handy*recovery*.com/best-data-*recovery*-apps.html diakses 27 Juli 2024

[11] Lucia, T., 2020. *Disk* Drill Data *Recovery* Review & Tutorial. [Online]: https://recoverit.wondershare.com/free-data-*recovery*/*disk*-drill-free-data*recovery*-review.html diakses 27 Juli 2024

[12] Aulia, I. Riadi, and A. Fadlil, "Storage Forensic Optical drive Menggunakan Metode Statik," Semnastek 2019, no. 2013, pp. 756–761, 2019.

[13] 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.

[14] Kausalyani A/P Angamutu et al 2020 J. Phys.: Conf. Ser. 1712 012019