JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 2, Juni 2024, Pp. 1031-1042

ANALISIS FORENSIK BUKTI DIGITAL PADA KEJAHATAN PEMBUNUHAN BERENCANA MENGGUNAKAN METODE NATIONAL INSTITUTE OF JUSTICE

Ageng Restu Triyanto*[1)], Fahmi Fachri[2)]
1. Teknik Informatika, Teknik, Universitas Ma'arif Nahdlatul Ulama Kebumen, Indonesia
2. Teknik Informatika, Teknik, Universitas Ma'arif Nahdlatul Ulama Kebumen, Indonesia

Article Info
Kata Kunci: Digital Forensik, SSD, Flashdisk, FTK Imager, Autopsy

Keywords: *Digital Forensics, SSD, Flashdisk, FTK Imager, Autopsy*

Article history:
Received 24 March 2024
Revised 7 April 2024
Accepted 21 April 2024
Available online 1 June 2024

DOI :
https://doi.org/10.29100/jipi.v9i2.5558

* Corresponding author.
Ageng Restu Triyanto
E-mail address:
agengrestutriyanto@email.ac.id

ABSTRAK
Flashdisk dan SSD merupakan perangkat penyimpanan yang banyak digunakan, karena flashdisk waluapin memiliki beragam kapasistas namun memilikitetap memiliki bentuk yang minimaslis sehingga memudahkan untuk dibawa kemana saja. Selain banyaknya pengguna Flashdisk, SSD juga banyak digunakan karena kebanyakan laptop sekarang menggunakan SSD sebagai media penyimpanan, karena SSD bisa dikatakan sebagai penyimpanan yang jauh lebih baik di bandingkan dengan laptop yang masih menggunakan HDD untuk media penyimpanannya, karena SSD menggunakan chip Flash NAND yang digunakan untuk menyimpan data. Semakin berkembangnya media penyimpanan, tidak menutup kemungkinan akan digunakan dalam hal yang bersifat negative atau untuk tindak kejahatan seperti menyimpan data kejahatan lalu menghapusnya secara permanen dalam usaha menghilangkan jejak kejahatannya yang telah dilakukannya. Penelitian ini menggunaakan skenario data barang bukt lalu di hapus secara permanen, dengan tujuan untuk mengembalikan mengembalikan data yang telah di hapus, diantaranya penghapusan data pada Flashdisk dan SSD. Dalam usaha mengembalikan data, peneliti menggunakan tools FTK Imager dan Autopsy, data yang ditemukan akan di analisis menggunakan Metode National Institute of Justice (NIJ) untuk menemukan hasil presentase apakah barang data yang didapat valid dengan keaslian dari barang bukti yang dicari. Kesimpulan pada peneitian ini adalah Penggunaan metode National Institute of Justice (NIJ) yaitu mengurutkan tahapan forensic digital dimulai dari identifikasi, pengumpulan, pemeriksaan, analisis, dan pelaporan dalam analisis untuk menentukan presentase keaslian barang bukti.

ABSTRACT
Flashdisks and SSDs are storage devices that are widely used, because even flashdisks have various capacities but still have a minimalist shape making it easy to carry anywhere. Apart from the large number of flashdisk users, SSDs are also widely used because most laptops now use SSDs as storage media, because SSDs can be said to be much better storage compared to laptops which still use HDDs for storage media, because SSDs use NAND Flash chips which are used for storage. save data. As storage media continues to develop, it is possible that it will be used in negative ways or for criminal acts, such as storing crime data and then deleting it permanently in an effort to eliminate traces of crimes that have been committed. This research uses a scenario where evidence data is then permanently deleted, with the aim of restoring data that has been deleted, including deleting data on Flashdisks and SSDs. In an effort to recover data, researchers use the FTK Imager and Autopsy tools. The data found will be analyzed using the National Institute of Justice (NIJ) method to find the percentage results of whether the data items obtained are valid with the authenticity of the evidence sought. The conclusion of this research is the use of the National Institute of Justice (NIJ) method, namely sequencing the stages of digital forensics starting from identification, collection, examination, analysis and reporting in the analysis to determine the percentage of authenticity of evidence.

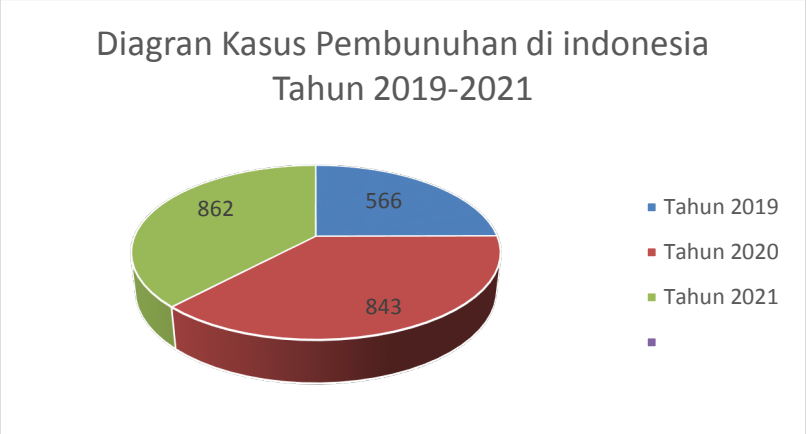
JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 2, Juni 2024, Pp. 1031-1042

I. PENDAHULUAN

PERKEMBANGAN teknologi teknologi pada masa sekarang sudah sangat pesat. Pesatnya teknologi juga memberikan dampak yang sangat positif dalam meningkatkan aktivitas sehari hari manusia. Selain menimbulkan dampak yang positif teknologi juga dapat menimbulkan dampak yang negatif yang tidak dapat dihindari. Dengan semakin canggihnya perangkat digital yang banyak orang gunakan pada masa kini, maka kejahatan semakin mudah dilakukan oleh orang yang tidak bertanggung jawab dengan berbagai modus menggunakan teknologi yang ada[1].

Untuk memberikan hukum dalam mengatisipasi kejahatan *cyber* di Indonesia telah diberlakukan UU 11/2008 tentang Informasi dan Transaksi Elektronik (ITE) yang sudah berubah menjadi UU 19/2016[2]. Adanya Undang-Undang tersebut juga menjadi solusi dan pengakuan bahwa alat elektronik dapat menjadi alat bukti yang sah dalam penyelidikan sebagaimana tertulia pada Pasal 54 Ayat (1) dan Legalitas dari alat bukti yang tertulis juga dalam Pasal 5[3].

Berikut data kasus pembunuhan yang terjadi di Indonesia dalam kurun waktu 3 tahun, yaitu dari tahun 2019 sampai dengan tahun 2021.



Gambar. 1. Diagram kasus pembunuhan menurut e-MP Robinopsnal Bareskrim Polri

dilihat dari data yang di dapat dari e-MP Robinopsnal Bareskrim Polri yang menunjukan bahwa kasus kejahatan di Indonesia masih terus meningkat dalam rentang waktu 3 tahun yaitu dari tahun 2019 sampai dengan tahun 2021. Dengan demikian Indonesia masih sangat rentang dalam kasus kejahatan pembunuhan, Pembunuhan berencana dapat terjadi karena beberapa motif, diantaranya yaitu perampokan, hubungan asmara, dan masih banyak lainnya.

Contoh kasus pembunuhan yang sedang ramai di perbincangkan yaitu kasus pembunuhan yang dilakukan oleh Ferdy Sambo. Ferdy Sambo sendiri merupakan mantan Perwira tinggi Polri yang menjabat sebagai Kepala Divisi Profesi dan Pengamanan Polri dengan pangkat Irjen Pol. Dalam kasus kejahatannya Ferdy Sambo telah melakukan pembunuhan berencana terhadapat rekannya sendiri seorang anggota Kepolisian Negara Republik Indonesia yang Bernama Nofriansyah Yosua Hutabarat. Dalam penyelidikan kasusnya walaupun Ferdy Sambo berusaha menghilangkan jejak dan bukti digital tetapi pembuktian tetap bisa ditampilkan.

Jejak dan bukti digital yang ditemukan pada kasus kejahatan komputer harus di analisa dengan menggunakan ilmu dan metode forensik. Analisa forensik terhadap jejak dan bukti digital di bidang teknologi juga dikenal sebagai *forensic digital*. *Forensic digital* pada dasarnya yaitu mencari bukti digital yang diperlukan untuk mengungkap kejahatan yang sedang diselidiki dan mengacu pada terjadiinya kejahatan[4]. Biasanya bukti digital dapat di tersimpan pada penyimpanan yang bersifat permanen maupun sementara[5]

Barang bukti merupakan hal yang sangat penting dalam proses invetigasi suatu penyelidikan dan pembuktian suatu kasus juga sangat bergantung pada barang bukti yang ada. Adanya barang bukti yang kemudian dapat menunjukan adanya peristiwa kejahatan yang telah terjadi sehingga dapat digunakan sebagai petunjuk dalam mengungkap kasus yang sedang di diusut dengan kronologis yang lengkap[6]. Ada dua klasifikasi barang bukti yang dihasilkan dari forensic digital yaitu barang bukti digital dan barang bukti elektronik, barang bukti digital bersifat digital yang diekstrak atau di recover dari barang bukti elektronik, sedangkan barang bukti digital elektronik biasanya berupa penyimpanan yang dapat dilkenali secara visual, salah satu dari barang bukti elektronik yaitu *Solid State Drive* atau yang sering di sebut juga dengan SSD dan Flashdisk[7].

Penelitian ini akan berfokus pada SSD (Solid State Drive) dan Flashdisk merupakan media penyimpanan yang sering digunakan dalam menyimpan sebuah file, dikarenakan selain SSD yang memiliki kinerja yang lebih cepat dari HDD juga memiliki ketahanan yang lebih baik sehingga banyak para pengguna PC/ laptop memilih perangkat

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 2, Juni 2024, Pp. 1031-1042

yang media penyimpanannya menggunakan SSD, selain SSD penelitian ini berfokus juga flasdisk karena masih banyak pengguna flashdisk yang digunakan sebagai media penyimpana sementara dan sebagai media untuk mengirim berbagai file ke orang lain.[8]

Dalam melaksanakan analisa dalam *forensic digital* tetap membutuhkan aplikasi atau *tools* untuk mendukung jalannya proses penelitian untuk mendapatkan hasil yang lebih baik, aplikasi atau t*ools* yang bisa digunakan untuk membantu mempermudah dalam proses analisa forensik juga beragam, mulai dari yang gratis maupun berbayar, contoh aplikasi atau *tools* yang dapat pakai guna memudahkan proses *forensic digital* dalam menemukan bukti digital yaitu FTK Imager, Autopsy dan aplikasi yang lainnya.

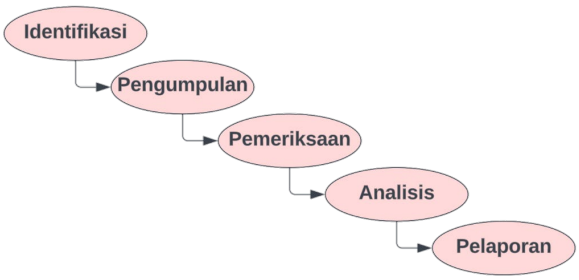
Dalam melaksanakan analisa dalam forensic digital tetap membutuhkan aplikasi *atau tools* untuk mendukung jalannya proses penelitian untuk mendapatkan hasil yang lebih baik, aplikasi atau *tools* yang bisa digunakan untuk membantu mempermudah dalam proses analisa *forensik* juga beragam[8], mulai dari yang gratis maupun berbayar, contoh aplikasi atau tools yang dapat pakai guna memudahkan proses *forensic digital* dalam menemukan bukti digital yaitu FTK Imager, Autopsy dan aplikasi yang lainnya [9]Dengan menampilkan gambaran dan tahapan metode *National Institute of Justice* dalam mengembalikan file atau bukti digital yang sudah di hapus secara permanen, dimana fokus penelitian adalah mengembalikan file yang telah di hapus secara permanen pada perangkat penyimpanan SSD dan Flashdisk. Dengan menggunakan tools FTK Imager dan Autopsy sebagai tools pendukung dalam melakukan penelitian[8].

Penelitian ini akan menganalisis pencarian barang bukti digital pada media penyimpanan yang berbeda menggunakan *tools* pendukung yang berbeda untuk mengetahui perbedaan dalam menemukan barang bukti yang dicari dalam menyelesaikan kasus *cybercrime* yang terjadi pada kasus kejahatan yang terjadi didalam lingkup digital dengan tahap pemeriksaan, tahap dimana akan diperiksanya barang bukti yang sudah *direcovery* baik secara manual maupun otomtis dalam memastikan bahwa barang bukti yang didapat adalah barang bukti asli. Setelah melakukan tahap pemeriksaan, dilakukankan lah tahap berikutnya yaitu analisis dengan mengevaluasi setiap Solusi yang nantinya dijadikan acuan dalam pemecehan masalah. Lalu tahap yang terakhir yaitu tahap laporan dimana peneliti melaporkan hasil dari uji coba dari penelitian yang dilakukan, meliputi gambaran aoa saja yang dilakukan dalam proses investigasi pengembalian barang bukti dan melaporkan hasil dari inti penelitian tersebut[10].

II. METODOLOGI

A. *Metode*

Dalam melakukan penelitian ini, metode yang digunakan daalam membantu mengungkap kasus pencarian barang bukti digital yaitu NIJ (*National Institute of Justice*), dari banyaknya metode yang dapat digunakan dalam mencari barang bukti digital penelitian ini menggunakan metode NIJ dikarekan metode ini mendeskripsikan peroses setiap tahapan-tahapan yang dilakukan sehingga dapat menemukan kerangka kerja dan urutan kerja yang terstruktur agar dapat digunakan sebagai dasar pada permasalah penelitian [9]. Metode tersebut terdiri dari dari 5 langkah kerja, dengan dimulai dari indentifikasi , pengumpulan, pemeriksaan, analisis, dan terakhir langkah pelaporan[11].

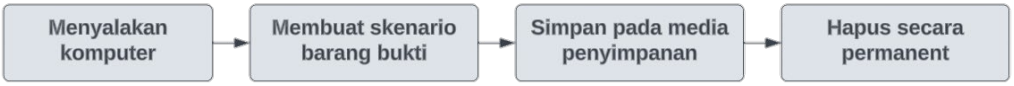


Gambar. 2. Metode Penelitian

B. *Identifikasi*

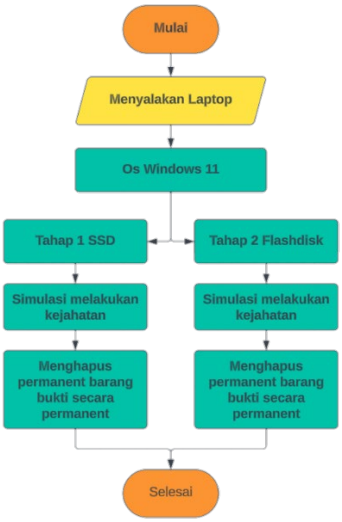
Identifikasi merupakan proses dimana peneliti akan memilih file-file barang bukti dengan format yang berbeda, file yang akan di gunakan sebagai barang bukti yaitu file yang mendukung dalam memecahkan masalah yang berkaitan dengan kasus pembunuhan. Dalam penelitian barang bukti di peroleh dari hasil skenario yang melibat-kan media penyimpanan SSd dan Flashdisk. Data yang sudah dibuat melalui skenario dari kasus-kasus kejahatan yang telah terjadi untuk digunakan sebagai barang bukti dalam proses penelitian yang dilakukan dalam menemukan barang bukti guna mendukung penyelidikan pada suatu kasus [12].

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 2, Juni 2024, Pp. 1031-1042



Gambar. 3. Skenario kasus tindak kejahatan

Bukti digital dalam penelitian ini didapat bukan dari kejadian nyata, melainkan hasil skenario kasus tindak kejahatan melibatkan dua media penyimpanan. Media penyimpanan pertama yaitu SSD dan media penyimpanan kedua adalah Flashdisk, dengan kata lain kasus kejahatan yang dilakukan lalu menyimpan bukti-bukti kasus kejahatan lalu menghapusmya untuk menghilangkan jejak kasus kejahatan yang telah diperbuat. Berikut ini merupakan tapahan implementasi langkah skenario penelitian [8].

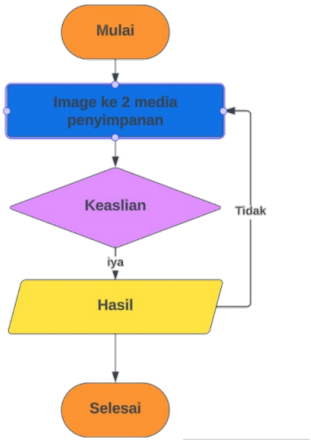


Gambar. 4. Flowchart Implementasi Skenario

Flowchart diatas menjelaskan hal pada tahap awal yaitu SSD dan Flashdisk yang digunakan dibersihkan dan di format terlebih dahulu supaya kedua media penyimpanan tersebut benar-benar kosong, setelah dipastikan kosong lalu peneliti mengisinya dengan data dari hasil skenario yang telah di lakukan yaitu memilih media apa saja yang akan sangat membantu dalam mengusut kasus pembunhan seperti foto , audio, video, dan berkas berupa pdf dan doc [13].

C. Pengumpulan

Langkah pengumpulan data-data barang bukti hasil skenerio kasus kejahatan dari barang bukti asli kebentuk digital, dalam pepncegahan barang bukti yang ada dari perubahan dan membuat barang bukti hasil skenario menjadi *image* yang dinamakan langkah akusisi, yaitu dimana proses yang dilakukan untuk menjaga keaslian atau upaya melakukan cloning file data dari barang bukti yang digunakan untuk pemeriksan.



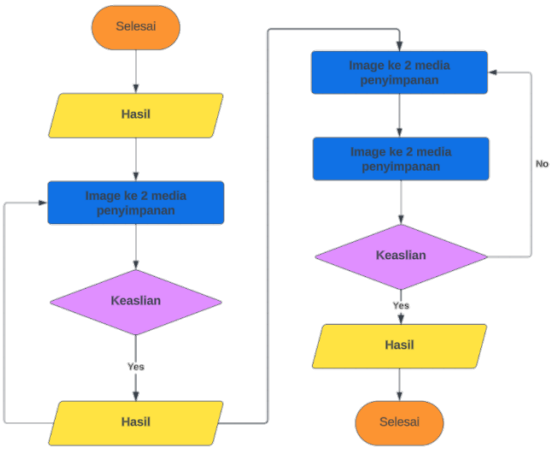
Gambar. 5. Proses Akusisi

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 2, Juni 2024, Pp. 1031-1042

Dimana akusisi barang bukti digital yang akan mengacu pada metode *Static Forensics* yaitu menggunakan prosedur serta pendekatan konvensional dimanan barang bukti akan diolah secara bit-by-bit image untuk mendukung proses forensik dengan melakukan ekstraksi serta analisis setelah insiden terjadi dan membuat salinan data sebagai barang bukti digital dari media penyimpanan[14], yang akan di uji dalam penelitian akan dijadikan image untuk mempermudah dalam mendapatkan barang bukti digital [15].

D. Pemeriksaan

Pemerikasaan adalah tahap dimanana semua data-data barang bukti dari hasil image yang telah diekstrak dari kedua media penyimpanan akan diperiksa, sehingga data yang dihasilkan sama dengan data barang bukti fisik. Untuk memastikan keaslian data dengan nama yang sama dan format file yang sama.

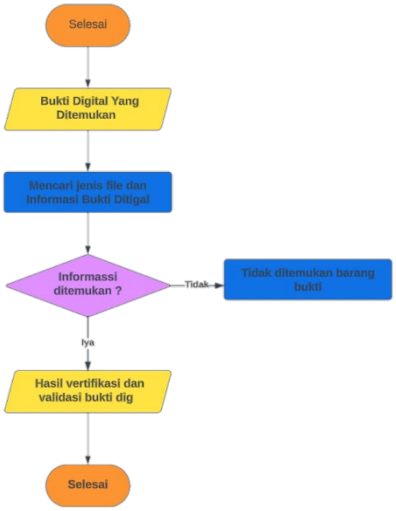


Gambar. 6. Flowchart pemeriksaan

Proses diatas dilakukan dari hasil image dengan pengecekan keaslian data dari nama dan format file yang sama, lalu dilakukan pemeriksaan menggunakan *tools* pendukung yang digunakan dalam menemukann barang bukti digital. Hasil yang telah ditemukan berupa file berformat dokumen, file gambar, dan file multimedia[16].

E. Analisis

Analisis merupakan proses pengecekan bukti digital yang sudah ditemukan dalam proses eksaminasi, barang butki digital diproses secara rinci sesuai pelaporan tindak kejahatan untuk menguak kasus kejahatan dengan metode yang benar secara ilmiah, dan dapat dipertanggung jawabkan secara legal dalam hukum [17].



Gambar. 7. Flowchart Analisis

Berdasarlan pada gambar diatas file bukti digital yang ditemukan yaitu file barang bukti digital yang ditemukan dalam proses akusisi akan di sortir lagi dari jenis file data barang bukti awal dengan ketentuan Jenis format file,

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 2, Juni 2024, Pp. 1031-1042

ukuran, dan nama file yang dibuat. Kemudian dilakukan pengecekan apakah ditemukan barang bukti atau tidak, setelah itu ketahap verifikasi dan validas kesamaan file dengan data aslinya untuk menghasilkan apakah barang bukti sudah sesuai keasliannya atau belom.

F. Pelaporan

Pelaporan yaitu dimana proses membuatn laporan, tahapan fotrnsik yang menghasilkan bukti yang berupa file-file yang terkait. Kemudian dibuat laporan analisis sehingga dapat mendukung informasi berupa yang lengkap. Kemudian dilanjutkan proses hukum sesuai dengan prosedur [18].

FTK Imager dan Autopsy adalah tools yang dapat digunakan sebagai tools pendukung dalam menganalisa file bukti digital, kedua tools ini dapat membantu penyelidikan kasus yang berguba untuk membuat salinan file barang bukti tanpa merubah data yang asli. Kedua tools ini juga merupakan tools yang dapat digunakan dalam proses akusisi yang diperlukan untuk forensik dengan kedua tools ini dapat memulihkan file yang sudah terhapus.

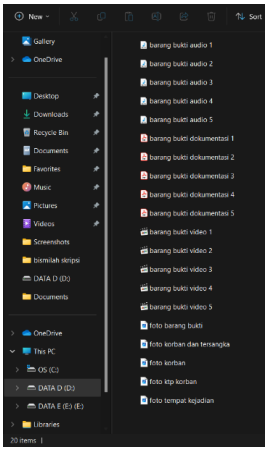
TABEL I
ALAT DAN BAHAN YANG DIGUNAKAN DALAM PENELITIAN

No	Hardware/Software	Spesifikasi	keterangan
1	Laptop	Asus A516f Core i3-10110u/BGA 2.10 GHz DDR4 8GB, windows 11 home single language	Perantara mencari bahan bukti
2	SSD Internal	Internal 512GB	Sebagai barang bukti
3	Flashdisk	SanDisk 8GB	Sebagai barang bukti
4	Acces Data FTK Imager	FTK Imager for windows ver.3.0.0.1443	Aplikasi pendukung
5	Autopsy	Autopsy for windows ver 4.21.0	Aplikasi Pendukung

Dari tabel 1 menunjukan alat, bahan, dan spesifikasi tools yang akan digunakan. Barang bukti pada media penyimanan pelaku digunakan dalam membantu proses pencarian barang bukti yang berkaitan dengan kasus kejahatan [19], terutama kejahatan yang di lakukan berkaitan dengan kasus pembunuhan, selama investigasi perencanaan sangat diperlukan agara proses pada penelitian dapat berjalan lancar. Termasuk dalam menentukan alat yang digunakan dalam penelian agar mendapatkan hasil yang valid.

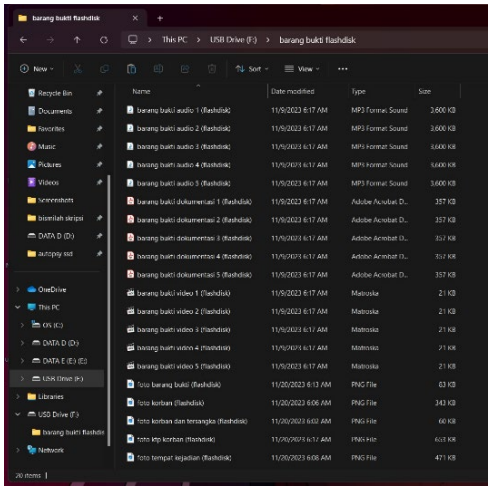
III. HASIL DAN PEMBAHASAN

Pada proses penelitian ini media penyimpanan SSD internal dan Flashdisk dijadikan bukti dalam wujud fisik. Peneliti mengakusisi bukti dengan wujud fisik ke bukti digital dengan mencocokan nama, dan jenis format file yang asli. Dengan salinan file digunakan sebagai bahan eksperimen bukti digital yang memiliki nama, ukuran, dan jenis format yang berbeda-beda. Sebagai acuan dalam klarifikasi bukti digital yang legal, lalu peneliti mencocokan ilustrasi nama, ukuram serta jenis format file bukti digital yang asli dengan temuan data saat restorasi.



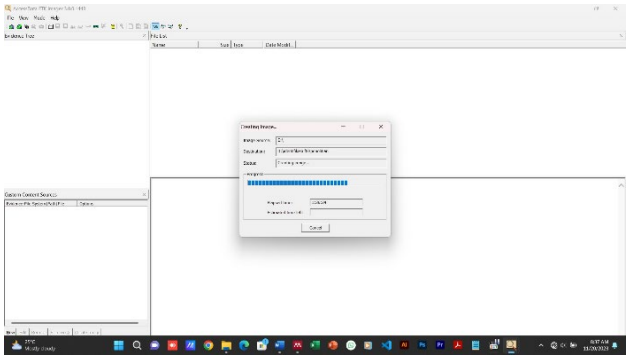
Gambar. 8. Sampel bukti digital pada SSD

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 2, Juni 2024, Pp. 1031-1042

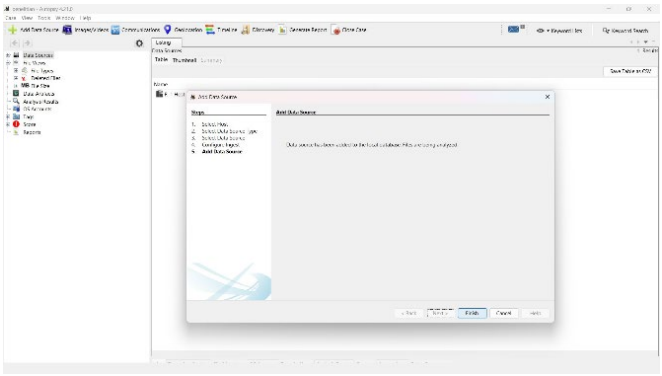


Gambar. 9. Sampel bukti digital pada Flashdisk

Langkah selanjutnya bukti digital akan dihapus secara permanen dan ada file data bukti digital yang dihapus melalui format file media penyimpanan. Lalu setela kedua media penyimpanan itu benar bernar terapus , akan dilakukan restonasi data, dimana penliti dalam melakukan restorasi data menggunakan dua *tools* pendukung yaitu FTK Imager dan Autopsy.



Gambar. 10. Proses image pada tools FTK Imager

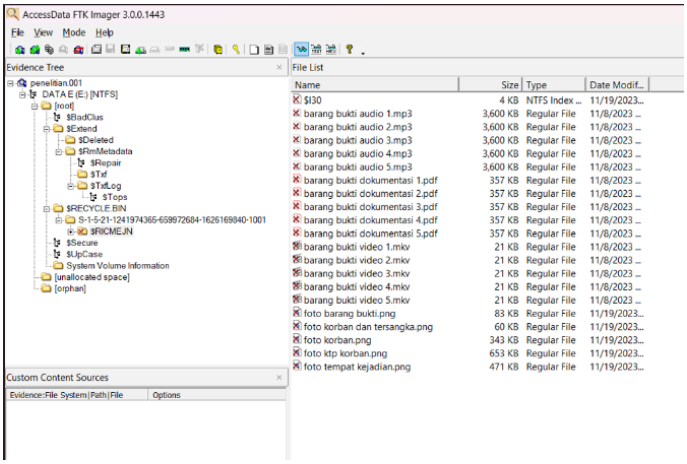


Gambar. 11. Proses image pada tools Autopsy

Pada gambar 10 dan 11 menunjukan proses *image* pada t*ools* FTK Imager dan Autopsy. Lalu hasil *image* disalin untuk msuk kedalam proses pemeriksaan barang bukti digital dalam upaya memastikan keaslian dari hasil image asli dan *image* salinan. Setelah mendapatkan hasil image dari medi penyimpanan SSD dan Flashdisk selanjutnya masuk kedalam tahap pemeriksaan dan menganaliss pada hasil image dengan menggunakan *tools* FTK Imger dan Autopsy.

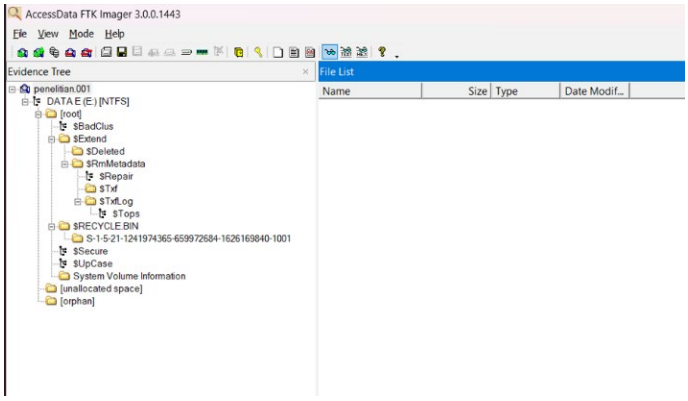
Penelitian pertama yaitu pemeriksaan barang bukti digital memakai *tools* FTK Imager, pada media penyimpanan SSD dan Flashdisk, dengan eksperimen menemukan barang bukti pada media penyimpanan yang dihapus secara permanen dan format.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 2, Juni 2024, Pp. 1031-1042



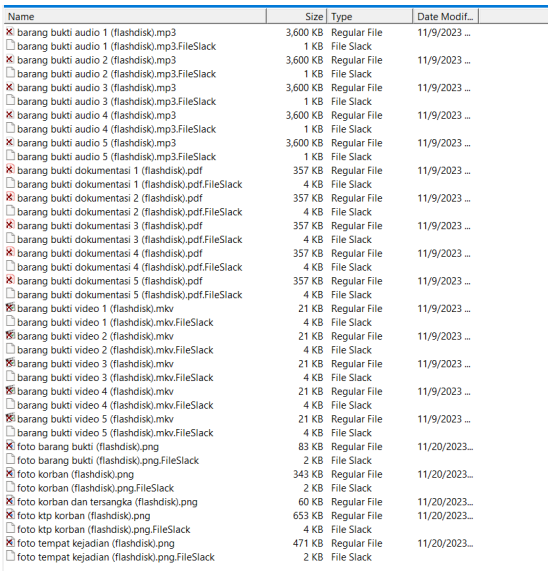
Gambar. 12. Hasil pemeriksaan FTK pada SSD dengan cara pengahpusan permanen

Pada gambar 11 menunjukan hasil dari pemeriksaan barang bukti digital, dari 20 barang bukti asli yang dihapus pada media penyimpanan SSD yang dihapus dengan cara hapus permanen, menghasilkan 20 barang bukti salinan.



Gambar. 13. Hasil pemeriksaan FTK pada SSD dengan cara penghapusan diformat

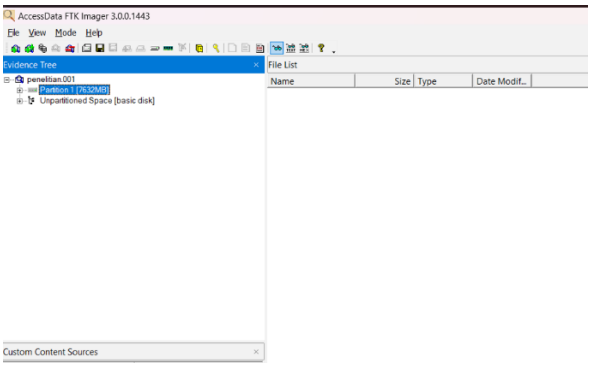
Gambar 13 Menunjukan hasil dari pemeriksaan media penyimpanan SSD menggunakan *tools* FTK Imager dengan cara penghapusan format file yang menghasilkan 0 data salinan dari 20 barang bukti asli.



Gambar. 14. Hasil pemeriksaan FTK pada Flashdisk dengan cara hapus permanen

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 2, Juni 2024, Pp. 1031-1042

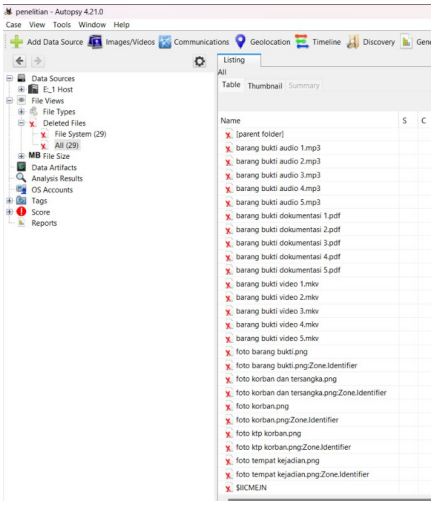
Gambar 14 menunjukan hasil dari pemeriksaan barang bukti menggunakan *tools* FTK Imager dengan media penyimpanan Flashdisk menggunakan cara hapus permanen yaitu dari 20 barang bukti asli yang dihapus, menghasilkan 20 data barang bukti salinan.



Gambar. 15. Hasil pemeriksaan FTK oada Flashdisk dengan cara hapus format

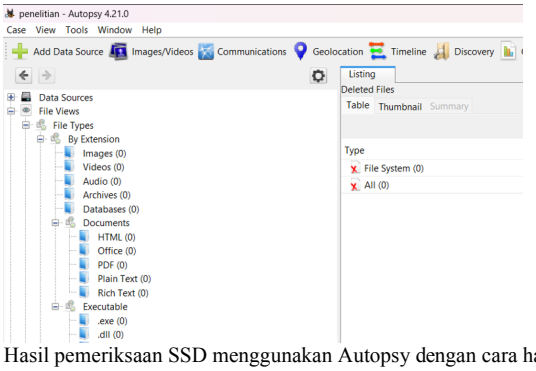
Gambar 15 menunjukan hasil dari pemeriksaan Flashdisk dengan *tools* FTK Imager dengan cara penghapusn format, dari pemeriksaan Flashdisk tersebut menghasilkan 0 data salinan dari 20 data asli.

Penelitian kedua yaitu pemeriksaan barang bukti digital memakai *tools* autopsy, pada media penyimpanan SSD san Flashdisk, dengan eksperimen menemukan barang bukti pada media penyimpanan .dengan cara penghapusan permanen dan penghapusan format media penyimpanan.



Gambar. 16. Hasil pemeriksaan SSD mernggunakan Autopsy dengan cara hapus permanen.

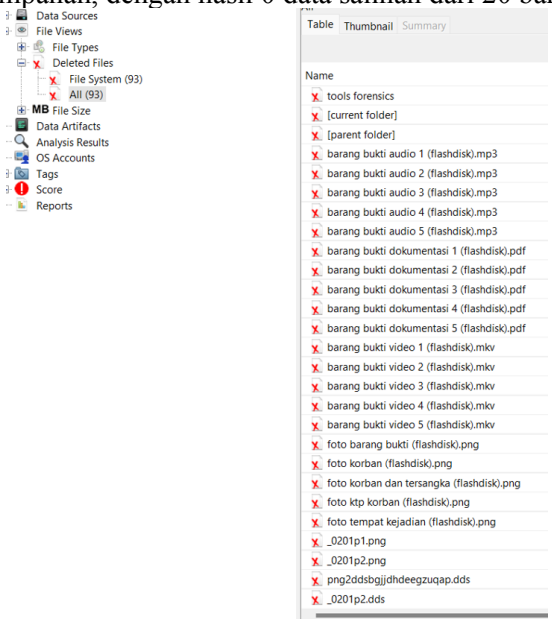
Gambar 16 menunjukan hasil dari pemeriksaan barang bukti yang didapat dari media penyimpanan SSD menggunkana software Autopsy dengan cara pengapusan permanen dari 20 barang bukti asli menghasilkan 20 barang bukti salinan. Berarti dalam usaha pengembalian data pada media penyimpanan SSD dengan cara hapus secara permanen berhasil.



Gamber. 17. Hasil pemeriksaan SSD menggunakan Autopsy dengan cara hapus format

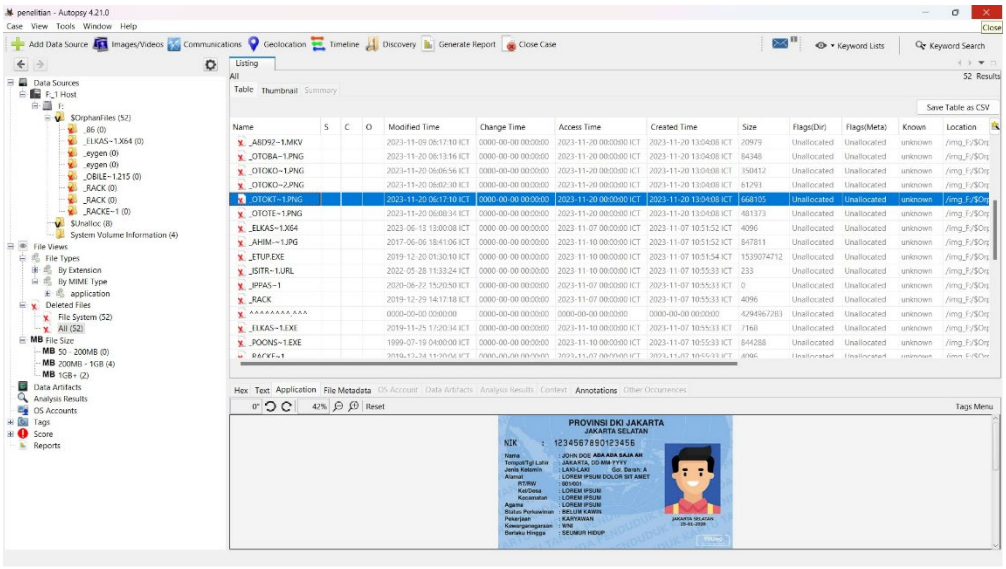
JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 2, Juni 2024, Pp. 1031-1042

Gambar 17 menunjukan hasil dari pemeriksaan media penyimpanan SSD menggunakan tools Autopsy dengan cara penghapusan format media penyimpanan, dengan hasil 0 data salinan dari 20 barang bukti asli.



Gambar. 18. Hasil pemeriksaan flashdisk menggunakan autopsy dengan hapus permanen

Gambar 18 menunjukan hasil dari pemeriksaan menggunakan *tools* Autopsy dengan media penyimpanan Flashdisk menggunakan cara penghapusan peprmanen dengan menghasilkan 20 data barang bukti salinan, dari 20 data barang bukti asli.



Gambar. 19. Menunjukan hasil pemeriksaan flashdisk menggunakan Autopsy dengan cara hapus format file

Gambar 19 menunjukan hasil dari proses pemetiksaan dengan menggunakan *tools* Autopsy menggunakan cara penghapusan format file, dari pemeriksaan flashdisk tersebut menghasilkan data asli namun dengan format nama yang berbeda dari data asli, dengan demikian hasil pemeriksaan flashdisk dengan *tools* FTK Imager memiliki 0 salinan dari 20 data barang bukti asli.

Hasil dari pemeriksaan barang bukti dengan menggunakan dua tools pada penelitian satu dan penelitian kedua yang memiliki kesamaan hasil dalam proses direstorasi. Berikut rangkuman hasil restorasi file dengan berfokus pada dua media penyimpanan yaitu media penyimpanan SSD dan Media penyimpanan Flashdisk yang dalam penelitiannya menggunakan dua cara penghapusan yaitu pengapusan secara permanen dan pengahapusan secara format media penyimpanan.

Dari hasil restorasi dari kedua media penyimpanan, lalu dianalisis untuk mendapatkan berapa banyak jumlah presentase keberhasilan dalam menemukan barang bukti digital salinan hasil dari barang bukti digital yang asli dan

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 2, Juni 2024, Pp. 1031-1042

sudah dihapus secara permanen maupun hapus dengan cara memformat file media penyimpanan.

Dalam menghitung presentase dalam menentukan keaslian dari barang bukti tersebut harus memenuhi syarat validasi yaitu dengan ketentuan memiliki 100% dari hasil restorasi data yang telah di analisis dan memiliki format file, nama file, dan ukuran file yang sama dengan file asli [20]. Adapun untuk menyimpulkan akurasi dalam menemukan keaslian barang bukti digital dengan menganalisis data, dengan menghitung data menggunakan rumus dibawah ini.

$$A = \frac{\sum \text{dr}}{\sum \text{dv}} X\ 100\ \%$$

A : Akurasi (%)

∑dr : Jumlah data recovery

∑dv : Jumlah data asli

TABEL II
HASIL RANGKUMAN RESTORASI BUKTI DIGITAL PADA SSD INTERNAL

Kategori File	Jumlah File	Hasil Restorasi Tools Forensic			
		FTK Imager		Autopsy	
		Permanen	Format	Permanen	Format
File Office					
.pdf	5	5	0	5	0
File Gambar					
.png	5	5	0	5	0
File Multimedia					
.mp3	5	5	0	5	0
.mp4	5	5	0	5	0
Jumlah	-	25	0	25	0
Presentase	-	100%	0%	100%	0%

TABEL III
HASIL RANGKUMAN RESTORASI BUKTI DIGITAL PADA FLASHDISK

Kategori File	Jumlah File	Hasil Restorasi Tools Forensic			
		FTK Imager		Autopsy	
		Permanen	Format	Permanen	Format
File Office					
.pdf	5	5	0	5	0
File Gambar					
.png	5	5	0	5	0
File Multimedia					
.mp3	5	5	0	5	0
.mp4	5	5	0	5	0
Jumlah	-	25	0	25	0
Presentase	-	100%	0%	100%	0%

Dilihat dari table diatas adalah hasil dari penelitian pengembalian data dengan media penyimpanan yang berdeda, *tools* yang digunakan dalam menganalisis file yang berbeda akan menghasilkan data yang berbeda juga, dalam upaya mengembalikan data, cara menghapus sebuah data juga sangat mempengaruhi apakah data bisa dikembalikan. Dengan hasil dari penghapusan permanen menghasilkan persentase 100 % tools aplikasi FTK Imager maupun Autopsy yang dapat diartikakn penelitian dengan cara hapus permanen berhasil dalam mengembalikan barang bukti, sedangkan pada penelitian dengan pengapusan memformat file media penyimpanan hanya menghasilkan persentase 0 % pada kedua media penyimpanan yang berari pada penghapusan dengan cara memformat file belom bisa di kembalikan dengan baik. Lalu dalam penelitian ini juga mendapatkan perbedaan dari kedua penelitaian tersebut dengan tools berbeda FTK Imager dan Autopsy dari lama nya proses aku sisi barang bukti dengan tools FTk memerlukan waktu bergantung pada besar kecilnya ukuran dari media penyimpanan yang di akusisi namun tetap memrlukan waktu yang lebih lama dari tools Autopsy yang memerlukan waktu yang lebih cepat walaupun memeliki size aplikasi yang lebih besar dari tools FTK Imager.

IV. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan dalam usaha mengembalikan barrang bukti kasus kejahtan dengan perantara digital yang melibatkan media penyimpanan SSD Internal dan media penyimpanan Flashdisk,dengan dua cara penghapusan yaitu penghapusan file secara permanen dan pengahpusan file dengan format file lalu di analisis dengan tools pendukung yang berbeda dan menggunakan metode NIJ (*National Institute of Justice*) . Dengan hasil

pembuktian analisis menggunakan metode NIJ sangat efesian, dalam proses akusisi data cara penghaspusan file sangat berpengaruh terhadap hasil akusisi barang bukti, hasil akusisi data menghasilkan presentase 100% jika penghapusan barang bukti yang asli dihapus secara permanen dan menghasilkan presentsae 0% jika penghapusan file barang bukti dilakukan dengan cara format file. Beberapa saran untuk peneliti selanjutnya terdapat beberpa metode *forensic* yang dapat bisa digunakan dan *tools* pendukung lain yang dapat digunakan, untuk membantu proses pencarian barang bukti dalam kasus kejahatan yang lain dengan memfokuskan kepada media penyimpanan yang lainnya seperti HDD, DVD, Memory Card , dan media penyimpan yang lainnya yang akan mendukung pihak wewenang dalam kasus forensik pada bidang digital dan mendapatkan hasil penelitian yang berbeda dan lebih akurat, penggunakan tools pendukung dalam mencari barang butki dapat di dikolaborasikan dengan tools lainnya, yang bertujuan mendapatkan hasil yang lebih baik lagi.

DAFTAR PUSTAKA

[1] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij)," *Elinvo (Electronics, Informatics, Vocat. Educ.*, vol. 3, no. 1, pp. 70–82, 2018, doi: 10.21831/elinvo.v3i1.19308.

[2] G. Mishardila, "Analisa dan pencarian bukti forensik digital pada aplikasi media sosial facebook dan twitter menggunakan metode statik forensik skripsi," 2020.

[3] M. Riskiyadi, "Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime," *Cyber Secur. dan Forensik Digit.*, vol. 3, no. 2, pp. 12–21, 2020, doi: 10.14421/csecurity.2020.3.2.2144.

[4] M. H. Akbar and I. Riadi, "ANALISIS BUKTI DIGITAL PADA FLASH DISK DRIVE MENGGUNAKAN METODE GENERIC COMPUTER FORENSIC INVESTIGATION MODEL (GCFIM)," pp. 715–723, 2019.

[5] I. Riadi, "Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ)," vol. 3, no. 1, 2019.

[6] N. Fatmah and R. Indrayani, "Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD Analisis Forensik Digital pada Solid State Drive Fungsi TRIM Menggunakan Tools Autopsy dan OSForensics Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD," vol. 5, pp. 185–192, 2022.

[7] I. Riadi, S. Sunardi, and A. Hadi, "Analisis Bukti Digital SSD NVMe pada Sistem Operasi Proprietary Analisis Bukti Digital SSD NVMe pada Sistem Operasi Proprietary Menggunakan Metode Static Forensics," no. February 2020, 2019.

[8] R. A. Ramadhan and D. Mualfah, "Implementasi Metode National Institute of Justice (NIJ) Pada Fitur TRIM SOLID STATE DRIVE (SSD) Dengan Objek Eksperimental Sistem Operasi Windows, Linux dan Macintosh," *IT J. Res. Dev.*, vol. 5, no. 2, pp. 183–192, 2020, doi: 10.25299/itjrd.2021.vol5(2).5750.

[9] I. Riadi, A. Fadlil, and M. I. Aulia, "Review Proses Forensik Optical Drive Menggunakan Metode National Institute of Justice (NIJ)," *J. Ilm. Tek. Inform. dan Sist. Inf.*, vol. 8, pp. 107–118, 2019.

[10] R. Inggi, H. P. Alam, P. Studi, and S. Informasi, "ANALISIS FORENSIK WEB BROWSER," vol. 8, no. 1, pp. 215–220, 2023.

[11] A. Yudhana, R. Umar, and A. Ahmadi, "Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ)," vol. X, no. X, pp. 8–13.

[12] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 10, no. 1, p. 20, 2016, doi: 10.30872/jim.v10i1.23.

[13] D. Julian, A. Wijaya, and T. Sutabri, "Perbandingan Kinerja Aplikasi Pengembalian Data Untuk Digital Forensik Dengan Metode National Institute of Standards and Technology," vol. 3, no. 1, pp. 210–218, 2023.

[14] B. S. Santoso and P. M. Sulaksono, "Static Forensic Pada USB Mass Storage Menggunakan Forensics Toolkit Imager," *J. Komput. Terap.*, vol. 8, no. 1, pp. 132–142, 2022, doi: 10.35143/jkt.v8i1.5334.

[15] Imam Riadi, Abdul Fadlil, and Muhammad Immawan Aulia, "Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST)," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 5, pp. 820–828, 2020, doi: 10.29207/resti.v4i5.2224.

[16] D. Mualfah, Muhammad Iqbal Syam, and Baidarus, "Analisis perbandingan tools mobile forensic menggunakan metode national institute of justice (NIJ)," *J. CoSciTech (Computer Sci. Inf. Technol.*, vol. 4, no. 1, pp. 283–292, 2023, doi: 10.37859/coscitech.v4i1.4767.

[17] I. Wahyudi, A. Muntasa, M. Yusuf, and A. Hamzah, "Mengungkap Dan Menguji Keaslian Bukti Digital Pada Kejahatan Cybercrime Dengan Metode Digital Forensic Research Workshop," *J. Apl. Teknol. Inf. dan Manaj.*, vol. 2, no. 2, pp. 120–127, 2021, doi: 10.31102/jatim.v2i2.1068.

[18] S. Keputusan Dirjen Penguatan Riset dan Pengembangan Ristek Dikti, I. Riadi, and J. Triyanto, "Terakreditasi SINTA Peringkat 4 Forensics Mobile Layanan WhatsApp pada Smartwatch Menggunakan Metode National Institute of Justice," vol. 3, no. 1, pp. 63–70, 2018.

[19] K. Ojs and U. Lancang, "Analisis keamanan web server open journal system (ojs) menggunakan metode issaf dan owasp (studi kasus ojs universitas lancang kuning)," vol. 05, pp. 45–55, 2020.

[20] T. N. Khusna and B. Sugiantoro, "Pengukuran Tingkat Keamanan Informasi Pada Upt-Psi Universitas Muria Kudus Berdasarkan Indeks Keamanan Informasi (Kami) Versi 4.2," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 8, no. 3, pp. 847–856, 2023, doi: 10.29100/jipi.v8i3.3720.