Analisis Digital Forensik *Recovery* File yang Dihapus Menggunakan *Tools Autopsy* dengan Metode *National Institute of Justice*

Rahmat Novrianda Dasmen, Arief Rahman, Anugrah Dwi Putra dan Muchlis Saputra

Program Studi Teknik Komputer,Universitas Bina Darma
Jl. Jenderal Ahmad Yani No.3, 9/10 Ulu, Kecamatan Seberang Ulu I, Kota Palembang, Sumatera Selatan 30111
E-mail: rahmat_novrianda@binadarma.ac.id, ariefrahman220603@gmail.com
anugrahdwiputra270323@gmail.com, saputramuchlis6@gmail.com

Abstrak

Salah satu kasus kejahatan digital yang umum terjadi adalah pencurian data, seperti informasi transaksi hingga data sensitif perusahaan. Pencuri menghapus file untuk menghapus jejaknya. Oleh karena itu, perlu dilakukan pencarian dan mengembalikan data yang terhapus untuk digunakan sebagai bukti digital. Kegiatan ini biasa disebut dengan forensik digital.Flash disk, juga dikenal sebagai USB flash drive, adalah perangkat penyimpanan data portabel tipe NAND yang memiliki port USB internal dan dapat dihubungkan ke Flashdisk merupakan media penyimpanan data yang paling umum digunakan saat ini dan dapat dibawa kemana saja. Flashdisk dapat digunakan untuk berbagai keperluan, antara lain sebagai media alternatif drive CD/DVD-ROM dan sebagai media penyimpanan sistem operasi.Tingkatkan kinerja penyimpanan komputer Anda, buat dan gunakan aplikasi portabel, serta kelola keamanan dan cadangan flash disk.Recovery menggunakan tools autopsy dengan hasil berhasil mengembalikan file berupa 6 berkas DOCX, 6 berkas XLSX, 8 berkas PDF, 6 dan 9 berkas PNG.Dengan keadaan baik dan utuh.

Kata kunci : *flashdisk,Autopsy,Recovery,NIJ,cyber Digital.*

Pendahuluan

Flash disk, juga dikenal sebagai USB flash drive, adalah perangkat penyimpanan data portabel tipe NAND yang memiliki port USB internal dan dapat dihubungkan ke Flashdisk merupakan media penyimpanan data yang paling umum digunakan saat ini dan dapat dibawa kemana saja. Flashdisk dapat digunakan untuk berbagai keperluan, antara lain sebagai media alternatif drive CD/DVD-ROM dan sebagai media penyimpanan sistem operasi kebutuhan untuk mengatasi kejahatan digital steganografi memerlukan panduan tentang metode dan teknik investigasi untuk menghasilkan bukti ilmiah[1].

Sebuah faktor kejahatan dunia maya menggunakan satu media sebagai alat komunikasinya, yaitu telepon pintar melakukan kejahatan[2].

Forensik digital ada menggunakan informasi dan metode untuk menemukan,mengumpulkan, melindungi, menganalisis, menafsirkan dan penyajian bukti digital yang relevan juga untuk rekonstruksi acara keabsahan proses hukum. Ada dua kategori bukti forensik digital yaitu bukti elektronik dan bukti digital[3].

Tujuan dari penelitian ini adalah menggunakan *software* forensik digital *Autopsy* untuk melakukan analisis forensik digital pada pemulihan data *flashdisk* dalam kasus penghapusan bukti transaksi, dengan menggunakan metode *National Institute of Justice* (NIJ) sebagai kerangka analisis. Panduan referensi dapat menjadi aset untuk penelitian ini membahas forensik digital dalam penyelidikan lain dan membantu penyidik kriminal dalam memperoleh bukti menggunakan teknologi forensik digital secepat mungkin[2].

Saat melakukan investigasi menggunakan forensik digital, berbagai alat digunakan untuk menganalisis, memulihkan, dan mengekstrak bukti digital, dan alat ini tersedia secara gratis atau berbayar[4].

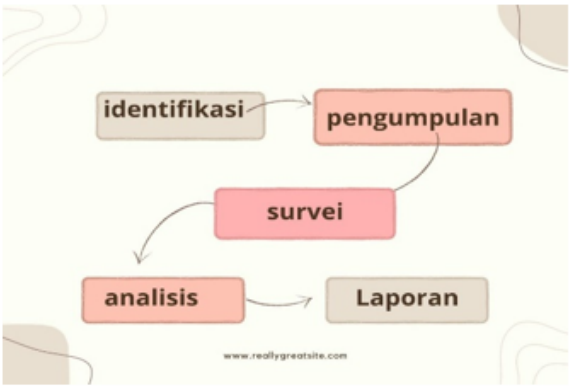
Ilmu forensik digital muncul sebagai solusi untuk memecahkan kejahatan yang memanfaatkan teknologi informasi sebagai alat bantu,sasaran, maupun tempat kejadian[5] .

DOI : http://dx.doi.org/10.32409/jikstik.23.2.3553

Metode Penelitian

Metode penelitian merupakan suatu tahap yang dilakukan untuk menyusun laporan penelitian[3]Metode yang digunakan untuk melakukan penelitian ini yaitu *National Institute of justice* dengan tahapan dan skenario kasus kejahatan sebagai berikut:.

Langkah-langkahnya dibagi menjadi lima tahap yaitu identifikasi, pengumpulan, survei, analisis, dan pelaporan. Oleh karena itu, penelitian ini menganalisis kinerja aplikasi Autopsy untuk mencari dan mengambil informasi yang telah dihapus dari media dalam bentuk *Flashdisk*. Alat penilaian diterapkan lihat berapa banyak file yang dapat dipulihkan dengan program ini.



Gambar 1: Tahapan proses metode NIJ

Metode National Institute of Justice (NIJ)

Gambar 1 merupakan pendekatan yang digunakan dalam analisis forensik digital. Langkah-langkahnya dibagi menjadi lima tahap yaitu identifikasi, pengumpulan, survei, analisis, dan pelaporan[6]. Tahapan kajian metode NIJ dijelaskan di bawah ini:

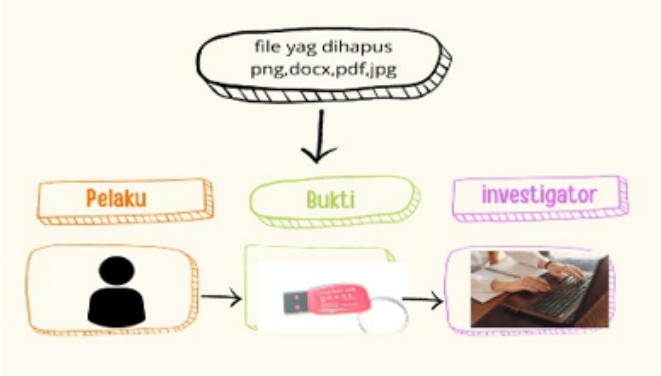
1. Collection : Pengumpulan bukti digital menggunakan alat forensik yang sesuai, seperti Autopsy untuk mengumpulkan informasi tentang perangkat digital yang sedang diselidiki.
2. Examination : Tahap penyidikan atau tahap pemeriksaan meneliti data-data yang dikumpulkan secara forensik, baik secara otomatis maupun manual, untuk memastikan bahwa data yang diperoleh dalam bentuk berkas adalah asli dan sesuai dengan data yang tercatat di TKP melalui sarana komputerisasi untuk memastikan bahwa mereka cocok. Inilah alasannya. Diperlukan untuk mengidentifikasi dan memverifikasi file digital menggunakan teknik hashing[7].
3. Analisis: Analisis terperinci atas bukti digital yang mengungkapkan informasi yang relevan dengan kasus yang dihadapi.
4. Pelaporan: Hasil analisis terhadap barang bukti digital yang ditemukan, yang dapat digunakan sebagai alat bukti dalam proses peradilan, dilaporkan.

Metode NIJ terbukti efektif dalam menangani kasus kejahatan digital dan menjadi tolok ukur analisis forensik digital. Tahapan pengambilan bukti digital dari flashdisk dengan alat diseksi metode NIJ meliputi identifikasi bukti, pengumpulan bukti digital, survei pendahuluan, analisis mendalam, dan pelaporan hasil analisis.

Skenario kasus kejahatan

Implementasi dan pengujian dilakukandengan desain skenario, dengan tujuan untukmendapatkan bukti digital seperti pada kasus kejahatan komputer yang sebenarnya[8].

Selain itu untuk menjelaskan kondisi penelitian Buat skenario kejahatan terkait mencuri informasi perusahaan dan menggunakan media penyimpanan berupa perangkat memori flash, TKP Desain digital yang dirancang dapat dilakukan dengan mudah lihat Gambar 2.

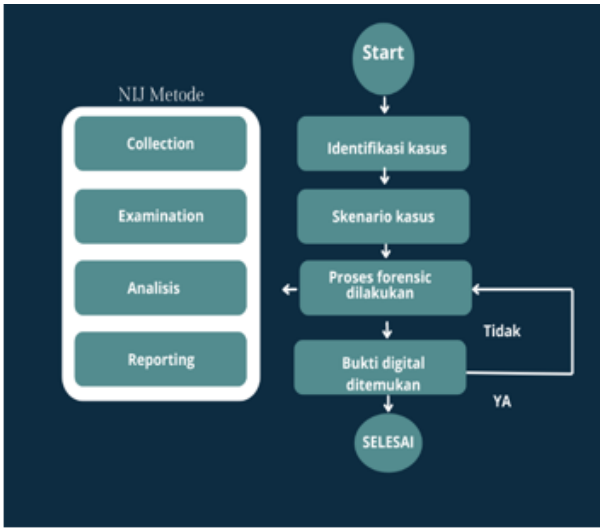


Gambar 2: skenario kasus kejahatan

Langkah-langkah dalam skrip dengan Lebih jelasnya adalah sebagai berikut.

1. Penjahat pergi ke kamar manajer dan menggunakannya ke komputer pengemudi tanpa izinnya.
2. Tersangka kemudian menyalin informasi penting seperti foto, docx, pdf.
3. Kemudian tersangka terekam dalam CCTV yang memperlihatkan hal tersebut.
4. Sang tersangkapun di tanya oleh sang petugas keamanan namun dia tidak mengatakan yang sejujurnya

5. Kemudian investigator memutuskan melakukan pencarian di memori flash namun dalam keadaan telah di format sehingga tidak ada satupun berkasi tersisa.
6. Setelah itu peneliti mengumpulkan data dan mengembalikannya untuk melihat jejak data yang disimpan tersangka dan mengumpulkan bukti untuk memperkuat tersangka bersalah.



Gambar 3: Skema Simulasi Perlakuan Kasus Sesuai Dengan Skenario

melakukan proses analisis forensik, memerlukan alat untuk membantu untuk melakukan pekerjaan dengan lebih baik. Oleh karena itu, digunakan beberapa tools, baik berupa perangkat keras maupun aplikasi berupa perangkat lunak, seperti dijelaskan pada Tabel 1.

Tabel 1: Alat dan bahan

Data	Ekstensi	Temuan	Komparasi Hash
Barang bukti word	DOCX	6 Berkas	Dalam keadaan baik
Barang bukti PDF	PDF	8 Berkas	Dalam keadaan baik
Barang bukti XLSX	XLSX	6 Berkas	Dalam keadaan baik
Barang bukti PNG	PNG	9 Berkas	Dalam keadaan baik

Collection

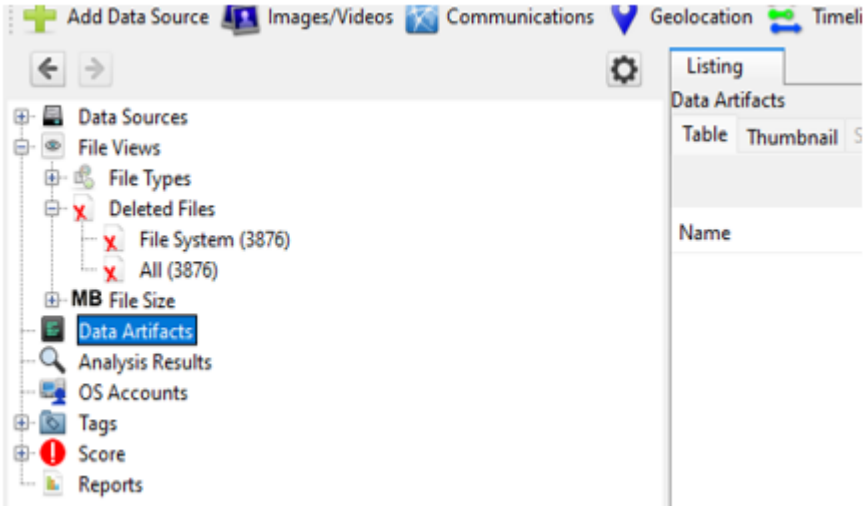
Melakukan kegiatan pengumpulan data untuk mendukung proses penyidikan dalam mencari barang-bukti kejahatan digital.[9] Barang bukti yang telah dikumpulkan berupa flashdisk sandisk Cruzer Blade 32GB seperti Gambar 4.

Gambar 4: flashdisk tersangka

Hasil dan Pembahasan

Dalam beberapa penelitian, penggunaan diseksi untuk mengambil data yang hilang mungkin terjadi dalam jangka waktu yang relatif singkat, seperti menit atau jam.Namun pada kasus yang lebih kompleks, waktu yang dibutuhkan mungkin lebih lama, misalnya berhari-hari atau berminggu-minggu Saat

Sebelum penelitian ini dilakukan, flashdisk digunakan untuk kebutuhan sehari-hari yaitu yaitu untuk menyimpan berbagai jenis file seperti video, musik, dokumen, dll. Flashdisk digunakan sebelum digunakan flash disk untuk. Untuk menyimpan file terkait skenario kejahatan pada penelitian ini.

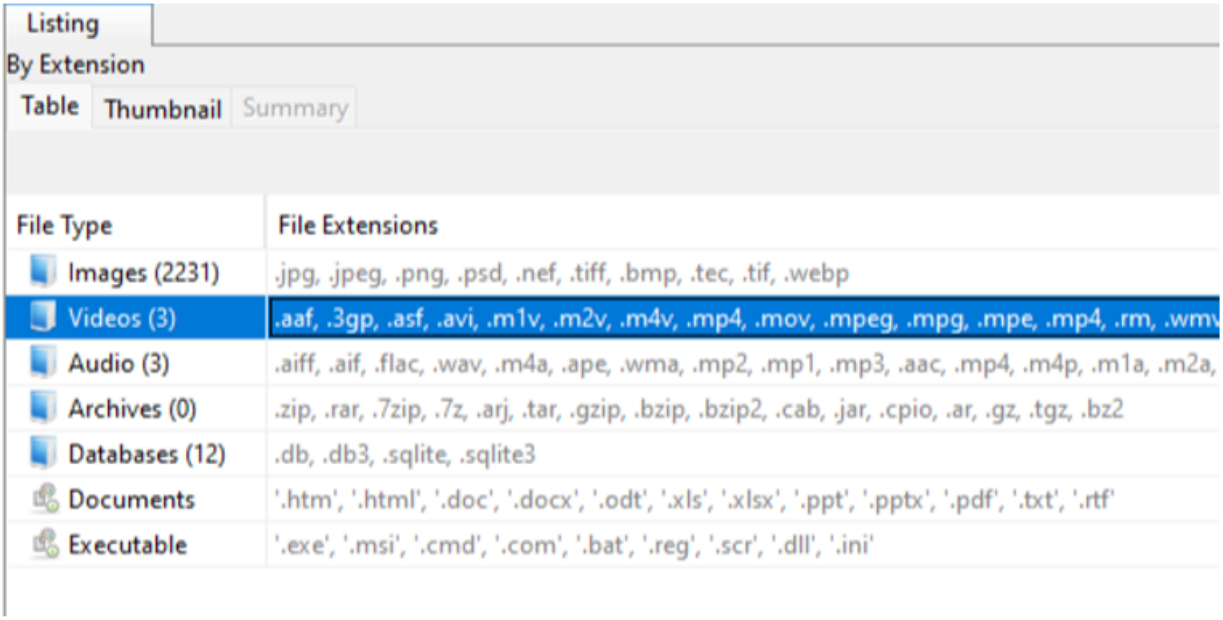


Gambar 5: Proses Akuisisi data

Examination

Bertujuan untuk mengungkap dengan melakukan analisis atas hasil dari tahap acquisition untukmemperoleh data yang diharapkan sebagai bukti digital[10].

Untuk memperoleh rekam jejak digital berupa file yang disimpan pada flashdisk, dilakukan proses akuisisi data oleh perangkat flashdisk yang dilakukan dengan menggunakan aplikasi Autopsy. Proses ini cukup memakan waktu karena memerlukan penggalian seluruh data yang tercatat sebelumnya.telah dihapus. Setelah menyelesaikan proses, aplikasi ini akan mengambil total 3876 data dan 3876 file sistem, seperti terlihat pada Gambar 5.



Gambar 6: Data berdasarkan kategori

Analysis

Pada tahap analisis dilakukan pengambilan data berupa alat bukti sebanyak buah. Hal ini dapat dilakukan dengan menggunakan pencarian manual, kemudian dilakukan metode pencarian manual, yaitu pencarian berdasarkan jenis *file*. Gunakan menu pencarian berdasarkan kategori, seperti terlihat pada Gambar 6.

Dalam pencarian manual berdasarkan kategori berhasil menemukan 3 berkas MP4 yang dicari berhasil di-*recovery* dalam kondisi yang utuh.40 Berkas dalam bentuk PDF juga berhasil di-*recovery* -dalam keaadan baik seperti Gambar 7.

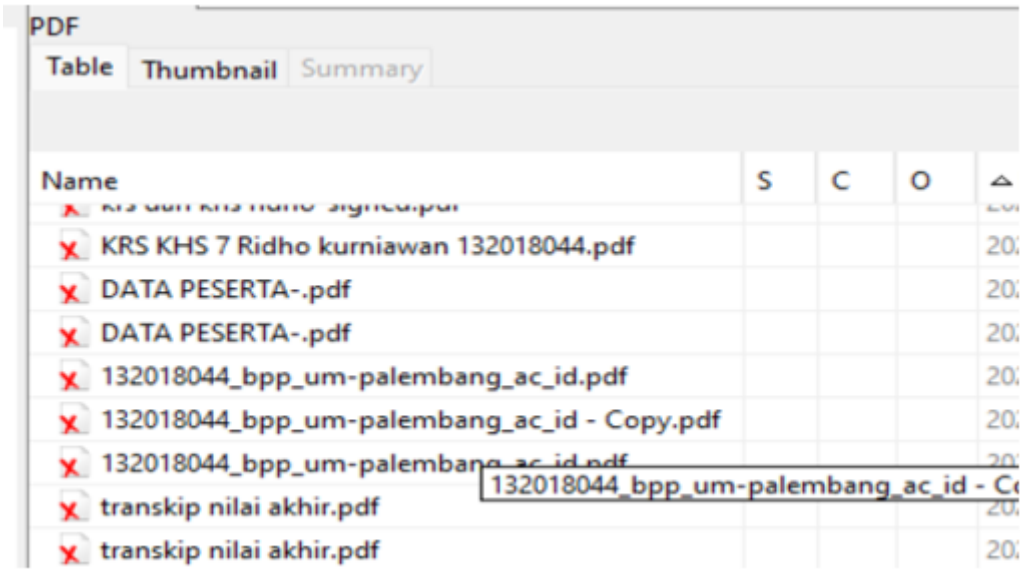
Pencarian ekstensi dengan kata kunci tidak ditemukan. Ini mungkin karena *file* rusak selama penghapusan dan aplikasi tidak lagi dapat menemukannya. Hal ini juga dilakukan untuk *file* MP3. Dikatakan bahwa *file* media, yaitu MP3 dan 3 MP4, juga ditemukan utuh dan file tersebut identik dengan *file* aslinya. 4 *file* gambar berformat PNG juga berhasil dikembalikan dalam kondisi baik dan diverifikasi sebagai *file* lengkap dan dipastikan sama dengan *file* aslinya. Dengan validasi tersebut, hasilnya dapat dijadikan bukti digital untuk menyelesaikan kasus pidana seperti yang dibuat dalam skenario.

Reporting

Ketika semua tahapan analisis selesai, diperoleh semua informasi yang diterima, informasi kemudian dibuat Tabel 2 merupakan hasil laopran dari analisis.

Tabel 2: hasil Tools Autopsy

Data	Ekstensi	Temuan	Komparasi Hash
Barang bukti word	DOCX	6 Berkas	Dalam keadaan baik
Barang bukti PDF	PDF	8 Berkas	Dalam keadaan baik
Barang bukti XLSX	XLSX	6 Berkas	Dalam keadaan baik
Barang bukti PNG	PNG	9 Berkas	Dalam keadaan baik



Gambar 7: Bukti dengan ekstensi pdf

Penutup

Pada penelitian ini, waktu yang dibutuhkan untuk memulihkan data menggunakan Autopsy tergantung pada data yang digunakan dan kapasitas flash disk. Harap dicatat bahwa waktu yang diperlukan dapat bervariasi tergantung pada data yang ingin pulihkan. Namun secara umum, hasil analisis terhadap data digital selanjutnya disebut digunakan sebagai barang bukti digital serta dapat dipertanggung jawabkan secara ilmiah dan secara hukum.Tahap reporting atau tahap pelaporan dilakukan setelah diperoleh barang bukti digital dari proses pemeriksaan dan dianalisis. Kalau begitu, analisisnya sudah dilakukan diperoleh hasil pengenalan gambar. Gambar yang digunakan masih digunakan gambar asli dan bukan gambar olahan yang telah dimodifikasi dari gambar asli, *tools Autopsy me recovery file* yang telah dihapus sehingga dapat memulihkan foto yang dihapus dari media sosial berdasarkan namanya bukti kejahatan.sehingga kinerja aplikasi tersebut karena berhasil menemukan dan mengembalikan 6 berkas DOCX, 6 berkas XLSX, 8 berkas PDF, 6 dan 9 berkas PNG.

Pemeriksaan tersebut berhasil memperoleh barang bukti digital berupa 15 ko pesan teks, dan 9 file gambar dengan tingkat eksekusi 48%. Sementara itu, alat forensik Belkasoft Evidence Center mampu mengambil bukti digital dari 15 kontak, namun dua pesan teks dan satu file gambar hilang. Persentase kinerja untuk adalah 32%.Dari hasil ini, kami dapat menyimpulkan bahwa Autopsy memiliki kinerja yang lebih baik dibandingkan Belkasoft Evidence Center dalam hal menemukan bukti digital bahwa telah dihapus[11].

Saran untuk penelitian di masa depan termasuk mengidentifikasi skenario lain yang dapat diterapkan oleh pelaku kejahatan terhadap bukti digital, mengatasi tantangan dalam bekerja dengan bukti digital, dan mengembangkan alat forensik lain untuk memungkinkan perbandingan hasil investigasi. Untuk itu peneliti menyarankan untuk menggunakan aplikasi open source seperti FTK Imager dan Autopsy. Aplikasi-aplikasi tersebut dinilai ampuh, mudah dipahami, dan sangat mudah digunakan dalam proses investigasi forensik digital[12]. Barang bukti digital harus ditangani sesuai prosedur dan metode yang tepat agar barang bukti yang diperoleh selama penyidikan sah secara hukum dan dapat digunakan hingga persidangan.

Daftar Pustaka

[1] S. Huda, R. Novrianda Dasmen, A. Ardiansyah, V. Pranata dan A. Januarta, "Analisis Digital Forensik Recovery Data pada Flashdisk Menggunakan Metode National Institute Of Justice (NIJ)", Jurnal Ilmiah Informatika, vol. 12, no. 01, pp. 74–79, doi: 10.33884/jif.v12i01.8343, Mar. 2024.

[2] S. Marcellino, H. B. Seta dan W. Widi, "Analisis Forensik Digital Recovery Data Smartphone pada Kasus Penghapusan Berkas Menggunakan Metode National Institute of Justice (NIJ)", Informatik Jurnal Ilmu Komputer Vol 19 No 2 (2023): Agustus 2023, 2023, doi: https://doi.org/10.52958/iftk.v19i2.4676.

[3] D. Mualfah, Muhammad Iqbal Syam dan Baidarus, "Analisis perbandingan tools mobile forensic menggunakan metode national institute of justice (NIJ)", Jurnal CoSciTech (Com-

puter Science and Information Technology), vol. 4, no. 1, pp. 283–292, May 2023, doi: 10.37859/coscitech.v4i1.4767.

[4] R. N. Dasmen, M. Reihan Pratama, H. Yasir dan A. Budiman, "Analisis Forensik Digital Pada Kasus Cyberbullying dengan Metode National Institute of Standard and Technology SP 800-86)", Jurnal Ilmiah Informatika, vol. 12, no. 01, doi: https://doi.org/10.33884/jif.v12i01.8344, 2024.

[5] M. Rafika, D. Qibriya, A. Ambarwati dan K. E. Susilo, "Analisis Forensik Digital pada Aplikasi Instant Messaging di Smartphone Berbasis Android untuk Bukti Digital ", Jurnal Teknologi Informasi, vol. 5, no. 2, https://dx.doi.org/10.36294/jurti.v5i2.2200, 2021.

[6] I. Riadi dan A. Hadi, "Analisis Bukti Digital SSD NVMe pada Sistem Operasi Proprietary Menggunakan Metode Static Forensics", Jurnal CoreIT, vol. 5, no. 2, DOI: http://dx.doi.org/10.24014/coreit.v5i2.8217, 2019.

[7] 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 Journal Research and Development, vol. 5, no. 2, pp. 183–192, doi: 10.25299/itjrd.2021.vol5(2).5750, Nov. 2020.

[8] I. Riadi, R. Umar dan I. M. Nasrulloh, "Analisis Forensik Digital pada Forzen Solid State Drive dengan Metode National Insitute of Justice (NIJ) ", Elinvo (Electronics, Informatics, and Vocational Education), vol. 3, no. 1, pp. 70–82, doi: 10.21831/elinvo.v3i1.19308, Jul. 2018.

[9] M. R. Setyawan, A. Yudhana, and A. Fadlil, "Data Acquisition On Messenger Skype Using The National Institute Of Justice Method," Systemic: Information System and Informatics Journal, vol. 5, no. 2, pp. 13–18, doi: 10.29080/systemic.v5i2.724, Mar. 2019.

[10] M. Riskiyadi, "Investigasi Forensik Terhadap Bukti Digital dalam Mengungkap Cybercrime ", Jurnal cyber security dan forensik Digital, vol.3,no.3, pp.12-21, doi : https://doi.org/10.14421/csecurity.2020.3.2.2144, 2020.

[11] M. Rizki Setyawan dan M. Fadli Hasa, "Analisis Forensik Digital pada Skype Berbasis Widnows 10 Menggunakan Framework ACPO ", Jurnal Ilmiah Betrik, vol.13, no.2, pp.111-119, doi: DOI 10.36050/betrik.v13i2.469, 2022.

[12] R. Y. Herman dan B. Triadi, "Analisis Computer Forensic Untuk Mendukung Prosesnya Penyelidikan Dalam Kasus Kejahatan", Jurnal Info Digit, vol.1, no.3, pp849-861, doi: 10.22303/upu.1.1.2021.01-10, Sept 2023