Jurnal Ilmiah Informatika (JIF)
| ISSN (Print) 2337-8379 | ISSN (Online) 2615-1049 |
Jurnal online di akses di http://ejournal.upbatam.ac.id/index.php/jif

Digital Analysis of Forensic Data Recovery on Flash Drive Using National Institute Of Justice (NIJ) Method

M.Syaiful Huda Mubarok[1], Rahmat Novrianda Dasmen[2] , Ardiansyah[3], Viren Pranata[4],M.Ary Januarta[5]

[12345] Universitas Bina Darma Jl. Jenderal Ahmad Yani No.3, 9/10 Ulu, Kota Palembang, Sumatera Selatan 30111

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima Redaksi: 10 Januari 2024
Revisi Akhir: 05 Maret 2024
Diterbitkan *Online*: 12 Maret 2024

KATA KUNCI

Forensic Digital,Test Disk

KORESPONDENSI

E-mail: rahmat_novrianda@binadarma.ac.id
Ardi10062@gmail.com
Syaifulmubarok716@gmail.com
Virenpranata@gmail.com
aryjanuarta30@gmail.com

A B S T R A C T

Investigation of the application of computer forensic techniques in the process of returning data by utilizing one of the tools namely disk tests In this context, focus is given to the analysis of the performance and effectiveness of forensic tools used to restore data from digital storage media, especially at the stage of disk test l. In IT forensics can be found evidence such as documents, financial information, e-mail, logs, videos, voice mail transcriptions and others as Especially in documents or data that have been deliberately taken or deleted data from USB devices and must be recovered data that has been lost In the early stages of research the author will collect data on the tools used and therefore, The author considers that tools are needed that can analyze which tools are better and more efficient in dealing with one of these problems. Tools to be used are Teskdisk. The results of this study provide deep insight into the effectiveness of the tesk disk tool in the context of data recovery through a computer forensic approach. The implications of these research findings can support the development of best practices in dealing with the challenges and complexities of data returns in an evolving digital world.

1. PENDAHULUAN

Aplikasi Teknologi Komputer dalam Forensik Digital Sangat Dibutuhkan. Forensik adalah proses mengumpulkan dan menganalisis bukti yang dimaksudkan untuk digunakan dalam persidangan kasus hukum. Dalam dunia kejahatan digital, forensik komputer adalah proses melestarikan, mengidentifikasi, dan memilah-milah data dan dokumen bukti [1] Kejahatan yang terjadi di dunia digital juga dan disebut sebagai "kejahatan internet". Kejahatan yang menggunakan pengetahuan teknologi disebut "kejahatan internet". Kejahatan ini dapat berupa dokumen, video, atau gambar, baik yang diedit atau tidak. Pada tahap selanjutnya, software dan teknik forensik khusus akan digunakan untuk menemukan file tersembunyi, partisi tersembunyi, file terenkripsi, atau yang dimaksud adalah Data loss adalah kondisi dimana data yang telah dimiliki akanmenjadi rusak atau terhapus [2] .Peneliti dan penguji forensik digital akan selalu menemukan tantangan baru dalam menangani layanan penyimpanan cloud [3]

Proses pemulihan atau pemulihan data yang hilang, rusak, atau tidak sengaja terhapus dari penyimpanan digital dikenal sebagai pemulihan data. Tujuan dari proses ini adalah untuk mengembalikan data ke keadaan semula atau setidaknya memulihkan sebagian besar data yang dapat diakses [4]Jika perangkat keras seperti hard drive, SSD, drive USB, atau perangkat penyimpanan lainnya gagal, Anda dapat kehilangan akses ke data Anda. Jika kehilangan data baru-baru ini, itu dapat dipulihkan secara utuh dengan bantuan alat pemulihan data yang dapat diunduh di Google. Namun, jika terlalu lama, data mungkin rusak atau tidak dapat dipulihkan secara utuh. Dan posting ini akan membahas alat yang dapat membantu pemulihan data yang hilang tersebut [5] Para peneliti meneliti efektivitas dua alat, test disk. dengan menggunakan dua alat ini, Uji disk untuk memulihkan data USB dari data yang hilang atau diformat. program yang dapat Anda gunakan untuk mengembalikan partisi yang hilang adalah Testdisk. Test Disk adalah alat Gratis dan Open Source yang dibuat oleh Christope grenier. Aplikasi TestDisk berfungsi untuk perkuliahan data. Terutama dirancang untuk membantu memulihkan partisi yang hilang atau rusak.

Dimana kesalahan tersebut biasanya disebabkan oleh software yang corrupt, virus atau kesalahan user sendiri (tidak sengaja menghapus partisi atau file data [6]Testdisk, seperti Photorec adalah perangkat lunak opensource yang dapat diunduh dan digunakan secara gratis. Alat testdisk kompatibel dengan berbagai platform, sehingga dapat digunakan pada berbagai sistem operasi seperti Windows, Linux, Mac OS X, dan Freebsd. Data Recovery adalah program yang membantu memulihkan data di laptop, baik yang hilang maupun terkena virus. Tujuan dari penelitian penulis ini adalah untuk mengidentifikasi pemulihan data secara keseluruhan, untuk mengetahui jenis-jenis alat yang digunakan dalam pemulihan data dan juga untuk menganalisis perbandingan dan alat Tesk Disk [7] [8]

2. TINJAUAN PUSTAKA

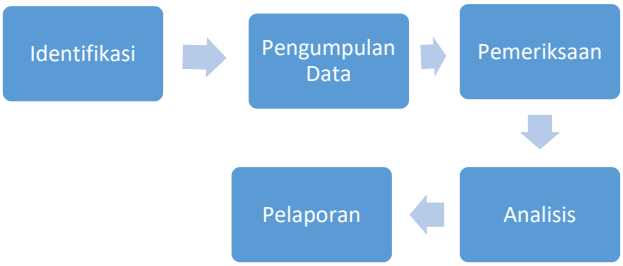
2.1 Digital Forensik

Digital Forensik adalah aplikasi teknologi komputer yang digunakan untuk memperoleh bukti hukum (pro justice) menggunakan teknologi canggih atau komputer untuk membuktikan kejahatan, dan menggunakan bukti digital Namun, cakupannya sekarang lebih luas, mencakup analisis perangkat yang digunakan untuk menyimpan data digital. Data perangkat digital biasanya diblokir, dihapus, disembunyikan, dan diganti, yang membuat forensik digital bermanfaat.

2.2 Recovery Data

Pemulihan data adalah proses pemulihan data dari keadaan yang rusak, hilang, terhapus, atau tidak dapat diakses. Ini adalah bagian penting dari analisis forensi dan harus dilakukan untuk mengetahui apa yang terjadi dan mendapatkan kembali file data yang sebelumnya dihapus. Anda dapat mendapatkan data dari berbagai jenis media penyimpanan, seperti harddisk, smartphone, flashdisk, atau media penyimpanan lainnya.

2.3 Metode NIJ Dan Tahapan Metode NIJ



Gambar 1 .Tahapan dalam metode *NIJ*

Dalam penelitian ini, Metode National Institute of Justice (NIJ) dimodifikasi dan diterapkan. Untuk menentukan proses penyelidikan, metode NIJ digunakan untuk menjelaskan fase-fasenya. Gambar 1 menunjukkan bahwa fase penelitian ini terdiri dari lima fase: persiapan, pengumpulan, pemeriksaan, analisis, dan pelaporan.

a. Fase pertama adalah persiapan, yaitu persiapan tim untuk melakukan penyelidikan
b. Menemukan file dan membuat replika dari benda fisik yang memiliki alat bukti digital adalah langkah kedua dalam proses pengumpulan dan pengumpulan
c. Setelah itu, tahap ketiga adalah pemeriksaan. Barang bukti digital yang diperoleh diuji secara manual atau otomatis..
d. Tahap keempat adalah analisis; di sini, barang bukti digital yang diperoleh selama tahap penyidikan diperiksa secara menyeluruh dan melakukan analisis untuk mencari barang bukti yang kuat.
e. Pelaporan adalah tahap kelima. Laporan ini mencakup analisis kegiatan investigasi, uraian alat investigasi, definisi metode investigasi, dan tindakan pendukung setelah analisis barang bukti digital yang diterima.

2.4 Test Disk

Merupakan sebuah perangkat Gratis dan Open Source buatan Christope GRENIER. Aplikasi TestDisk berfungsi untuk pemuliahan data. Terutama dirancang untuk membantu memulihkan partisi yang hilang atau rusak. Dimana kesalahan ini biasanya disebabkan oleh perangkat lunak yang rusak, terkena virus atau kesalan pengguna itu sendiri (tidak sengaja menghapus Partisi atau Data file)

3 Metode penelitian

3.1 Metode National Institute Of Justice

Pada Penelitian ini, penulis menggunakan metode national institute of justice (NIJ) metode ini digunakan untuk menjelaskan tahapan-tahapan penyelidikan secara sistematis.[9].Tahapan ini terbagi menjadi beberapa tahapan Adapun Metodologi Penelitian Ini Sebagai Berikut:

A. Tahapan Identifikasi

Digital Forensics adalah aplikasi teknologi komputer yang digunakan untuk memperoleh bukti hukum (pro justice) dengan menggunakan teknologi canggih atau komputer untuk membuktikan kejahatan, dan menggunakan digital [10]. Pada tahap ini dilakukan proses identifikasi, pelabelan, dan pencatatan untuk menjaga integritas bukti [11]

Alur investigasi pengungkapan bukti :

- Pihak berwenang mengindentifikasi masalah untuk mengetahui secara detail masalah yang terjadi dengan pelaku dan korban
- Barang bukti diambil untuk mengamankan dan menyimpan pada keadaan aslinya
- Proses penyidikan dimulai pada saat pihak berwenang menyerahkan barang bukti kepada penyidik untuk membuat kesimpulan

B. Pengumpulan Data

Untuk mendukung proses penyidikan terkait pencarian bukti digital suatu kejahatan, tahap pengumpulan terdiri dari serangkaian tindakan pengumpulan data. Metode Pengumpulan data adalah teknik atau cara-cara yang dapat digunakan oleh peneliti untuk mengumpulkan data [12]

C. Pemeriksaan

Pada tahap investigasi ini, data yang dikumpulkan secara forensik diperiksa secara otomatis atau manual untuk memastikan bahwa data yang telah diperoleh dalam format file png dan mp 4 asli dan cocok dengan data yang diperoleh di TKP [13]

D. Analysis

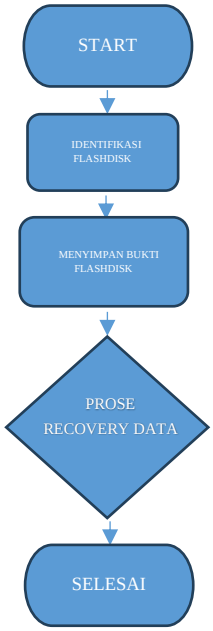
Kami dapat menjelaskan langkah-langkah analisis ini secara rinci. untuk menemukan yang lebih efisien dan mudah diakses serta Aplikasi Test Disk memungkinkan Anda melihat fitur kecepatan, keamanan data, dan hasil pemulihan data.

E. Pelaporan

Pelaporan adalah jaringan prosedur terkait, dikumpulkan bersama untuk melakukan kegiatan atau tujuan tertentu [14] Dan Setelah barang bukti digital diperoleh dan dianalisis selama proses pemeriksaan, tahap pelaporan dimulai. Langkah berikutnya adalah melaporkan secara lisan atau tulisan tentang kemajuan dan hasil kegiatan. Laporan ini dapat mencakup gambaran tentang tindakan yang dilakukan, penjelasan tentang alat dan teknik yang digunakan, penentuan tindakan pendukung, dan rekomendasi untuk perbaikan kebijakan atau komponen pendukung lainnya. Dengan fungsi laporan, Anda dapat mengetahui dan mendapatkan informasi yang Anda butuhkan.

3.2 Alur Kerja

Berikut adalah alur kerja penelitian bisa dilihat pada gambar 2 pada flowchart dibawah ini :



Gambar 2 .flowchart penelitian

3.3 Kebutuhan Hardware dan Software

Untuk mendukung proses dalam penyelidikan kasus kejahatan forensik digital diperlukan perangkat pendukung berupa hardware dan software.

Tabel 1. Perangkat Hardware dan Software

No	Alat dan Software	Deskripsi
1	*Flashdisk* 42GB	Objek Penelitian
2	Laptop *ram 4 gb*	*Windows 11, 64 Bit, 4 GB RAM, Workstation* Analisis Forensik
3	*Tools test disk dan easeus*	*Tools* Forensik

3.4 Skenario Kasus Forensik

Untuk memperjelas dan merekonstruksi peristiwa kejahatan yang melibatkan pelaku, saksi, dan korban, penyusunan dan implementasi skenario kasus digunakan, Dalam Hal Ini Penulis akan Menggunakan Tools Forensik Dan Akan Menganalisis Keefektifan Dari Tools Tersebut.

Berikut skenario nya :

1. Pelaku kejahatan terekam cctv sedang melakukan perampokan dan pencurian di kantor A.
2. Pelaku sadar aksinya direkam cctv lalu si pelaku berupaya melenyapkan barang bukti berupa file rekaman cctv dan
3. bukti gambar yang terekam oleh cctv dalam kejadian ini tersangka diketahui melakukan upaya penghapusan file yang ada.
4. Langkah konkret yang akan dilakukan dikasus ini adalah dengan mengembalikan data berupa rekaman atau pun bukti lainnya yang telah dihapus oleh pelaku.
5. Dengan tujuan agar pelaku bisa ditangkap dan dipenjara dengan barang bukti kejahatan dan memastikan kebenaran peristiwa yang terjadi.

4. HASIL DAN PEMBAHASAN

4.1. Identifikasi

Identifikasi adalah proses mempersiapkan peralatan yang digunakan selama tahap investigasi untuk mengumpulkan semua bukti, seperti flash drive yang ada, untuk memastikan bahwa bukti tersebut asli. Hal ini dilakukan agar penyidik mempermudah penyelesaian kasus [15]

Perjalanan investigasi menuju pengungkapan bukti digambarkan sebagai berikut:

- Pengumpulan Informasi, Mengumpulkan data dan informasi yang relevan untuk memahami objek atau masalah yang diidentifikasi.
- Identifikasi masalah dilakukan oleh pihak berwenang untuk mengetahui detail masalah yang terjadi dengan pelaku dan korban.
- Barang bukti diambil untuk melindunginya dan menyimpannya dalam keadaan aslinya.
- Proses penyidikan dimulai saat pihak berwenang menyerahkan barang bukti kepada penyidik untuk mengumpulkan bukti.

4.2. Collection

Pada titik ini, bukti fisik dan dokumentasi yang diperlukan dikumpulkan. Untuk melakukan ini, barang bukti yang dikumpulkan untuk proses penyelidikan diperiksa, termasuk jenis barang bukti, spesifikasi, sistem operasi, versi Android, dan informasi lainnya. Dan juga collection dalam penelitian memiliki kelebihannya

- Mendapatkan Data Langsung: Dengan melakukan pengumpulan data sendiri, penyelidik dapat memperoleh informasi langsung dari sumbernya, menghindari potensi bias atau distorsi yang mungkin terjadi jika menggunakan data sekunder.
- Kontrol atas Proses Pengumpulan: penyidik memilii kendali penuh atas cara dan metode pengumpulan data,memungkinka untuk menyesuaikan strategi pengumpulan sesuai dengan kebutuhan penyelidikan.

.

Gambar 3 Barang Bukti Penyelidikan

4.3. Examination

Selama proses penyelidikan, alat forensik diuji untuk mendapatkan bukti digital, yang akan digunakan untuk memecahkan masalah yang diselidiki. Berikut adalah langkah-langkah uji alat forensik yang dilakukan dalam penelitian ini. Tools Yang akan Diidentifikasi dengan Barang Bukti Untuk Melakukan Forensik Yaitu Tools Test Disk :

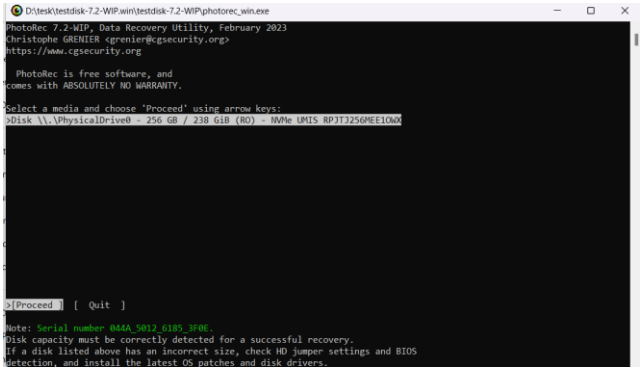
Tools Test Disk

Testdisk adalah aplikasi Pemulihan data Recovery. Hal ini dimaksudkan untuk membuat disk tidak dapat dihidupkan lagi dan memulihkan data yang hilang di partisi.. Fungsi-fungsi ini terutama dimaksudkan untuk membantu dalam kasus forensik

Beberapa Kelebihan Test Disk

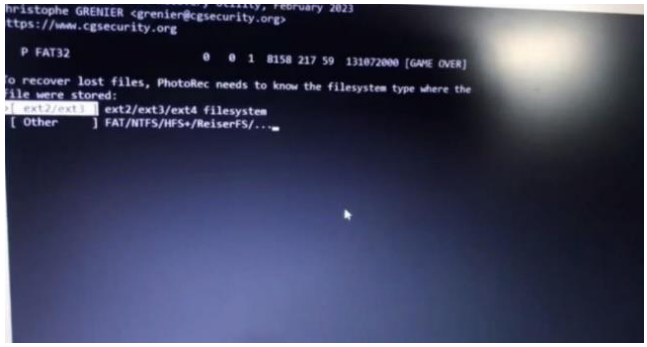
- Membangunkan kembali sektor boot FAT12/FAT16/FAT32
- Membangun dan mengoptimalkan sektor filesystem NTFS
- Memperbaiki filesystem ext2/ext3/ext4
- Pemulihan data dari FAT, exFAT, NTFS, dan ext
- Pemulihan Tanpa Risiko TestDisk beroperasi dalam mode baca saja

Proses penyelidikan dilakukan dengan mengambil, mencari, dan menganalisis data dari bukti fisik yang ditemukan pada flash disk. Berikut Merupakan Tampilan Dari Test Disk :



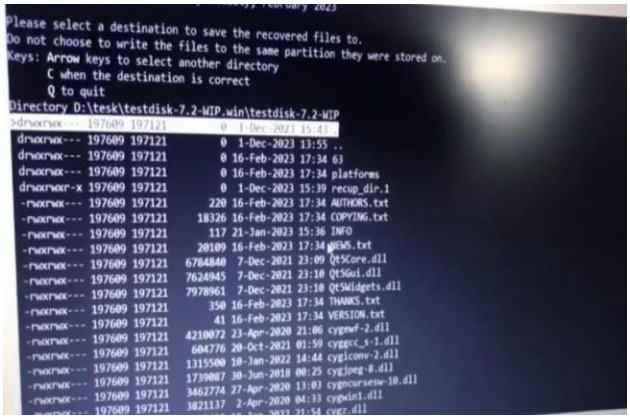
Gambar 4 Tampilan Awal Test Disk

Pada gambar 4 merupakan tampilan awal ketika ingin menggunakan tools test disk terdapat pilihan menu antara ingin menggunakan flashdisk atau perangkat internal di pc/laptop.



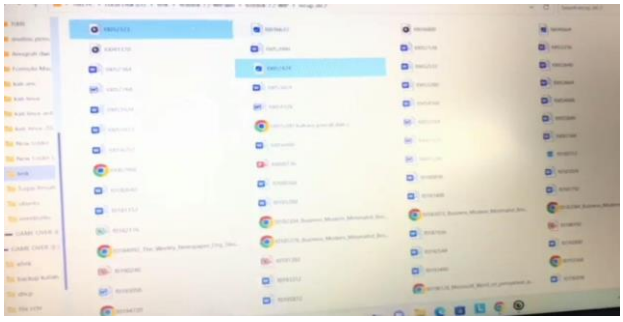
Gambar 5 Tampilan Masuk Menu Test Disk

Tahap Selanjutnya ini penulis akan Memulai melakukan pemeriksaan dengan tools test disk.



Gambar 6 Flash disk Sebagai Data

Gambar Diatas Terdapat Data Recovery Yang Sudah Terdeteksi Oleh Tools Test Disk, Tahap Selanjutnya Akan Dilakukan Scanning Pada Data Tersebut Untuk Menemukan Bukti yang ada Dan Melakukan Recovery



Gambar 7 data file recovey

Setelah berhasil melakukan *scanning* pada *device* maka ditemukan data *recovery* Berupa File Gambar, Gambar diatas merupakan data-data yang sudah direcovery,Terdapat banyak data yang berhasil direcovery, Penulis berhasil menemukan Bukti Yang Dicari yaitu Gambar Pencurian Yang Terekam Cctv, Foto Tersebut Merupakan Skenario Yang Penulis buat untuk Mencoba keefektifan Dari Tools Test Disk.

Berikut gambar yang didapat:

Gambar 9 Hasil Recovery Tools Test Disk

Pada Gambar Diatas Terdapat Bukti Yang Sudah Didapatkan, Gambar Tersebut adalah Bukti Pencurian yang dilakukan oleh Pelaku X , Dalam Hal ini Analisis Keefektifan Tools Test disk Tersebut sangat baik untuk Kegiatan Forensik Yang Dilakukan Untuk Mengrecovery Data Yang Baik Sengaja Dihapus maupun Yang Tidak Disengaja.

4.4. Analysis

Hasil Analisa Yang Didapat Dari Tools Test Disk Dapat Dibuktikan Bahwa Tools Test Disk dapat Mengembalikan/Memulihkan Data Yang Telah Terhapus Dan Dapat Digunakan Untuk Mengungkapkan Kasus Kejahatan. Dari Hasil Analysis Penulis Didapatkan Bahwa Tools Test Disk Dapat Mengrecovery Baik File Text,Gambar,Hingga Video.

4.5. Reporting

Penelitian tentang kasus pencurian data di flashdisk menemukan bukti digital yang dapat digunakan dalam kasus pencurian file. Hasil investigasi forensi digital menunjukkan bahwa tahapan identifikasi digunakan untuk mengidentifikasi masalah yang terjadi, barang bukti dikumpulkan untuk diperiksa, dan kemudian dilakukan penyelidikan untuk menemukan dan menemukan bukti digital lainnya Selain itu, dapat disimpulkan bahwa alat-alat tersebut sangat efektif dalam melakukan proses ini.

5. KESIMPULAN DAN SARAN

Berdasarkan penelitian yang telah dilakukan oleh penulis memberikan kesimpulan bahwa tools forensik yaitu test disk sangat baik dalam melakukan recovery data berupa file yang hilang atau sengaja dihapus. Dalam permasalahan ini bahwa telah terdapat bukti rekaman cctv pelaku pencurian. Kemampuan *test disk* sebagai *tools* forensik mencapai 100% tingkat keberhasilan dalam menemukan bukti digital sesuai dengan parameter yang ditetapkan, Saran untuk penelitian selanjutnya adalah membuat penelitian ini lebih spesifik dan bisa dikembangkan lagi dan dapat menambahkan point-point yang Relevan pada penelitian ini. Tentunya penelitian yang kami buat masih banyak kekurangan.gunakanlah tools forensik sebaik mungkin tanpa merugikan pihak manapun.

DAFTAR PUSTAKA

[1] G. Fanani, I. Riadi, and A. Yudhana, “Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop,” *JURNAL MEDIA INFORMATIKA BUDIDARMA*, vol. 6, no. 2, p. 1263, Apr. 2022, doi: 10.30865/mib.v6i2.3946.

[2] M. F. Abdillah and Y. Prayudi, “Data Recovery Comparative Analysis using Open-based Forensic Tools Source on Linux,” *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 9, pp. 633–639, 2022, doi: 10.14569/IJACSA.2022.0130975.

[3] D. M. Rathod, “Google Drive Forensics,” 2017. [Online]. Available: https://www.researchgate.net/publication/321534818

[4] C. P. Lubis, “Analisis Aplikasi Easeus Dan Autopsy Pada Recovery Data Usb Dalam Bidang It Forensik,” *Agustus*, vol. 8, no. 1, p. 42, 2023, [Online]. Available: http://e-journal.potensi-utama.ac.id/ojs/index.php/INFOSYS/index|

[5] A. Fauzan, I. Riadi, and A. Fadlil, “Analisis Forensik Digital Pada Line Messenger Untuk Penanganan Cybercrime,” 2016. [Online]. Available: http://ars.ilkom.unsri.ac.id

[6] M. F. Abdillah and Y. Prayudi, “Data Recovery Comparative Analysis using Open-based Forensic Tools Source on Linux,” *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 9, pp. 633–639, 2022, doi: 10.14569/IJACSA.2022.0130975.

[7] N. Fatmah and R. Indrayani, “Nomor 2,” *Volume*, vol. 5, pp. 185–192, 2022, [Online]. Available: https://ojs.trigunadharma.ac.id/index.php/jsk/index

[8] D. Perdana Putranto, B. Hananto, F. Ilmu Komputer, U. Pembangunan Nasional Veteran Jakarta, J. R. Fatmawati Raya, and P. Labu, “Analisis Keamanan Website Leads UPNVJ Terhadap Serangan SQL Injection & Sniffing Attack,” *JURNAL INFORMATIK Edisi ke*, vol. 18, p. 2022.

[9] B. Bulan, T. Tahun, A. Yudhana, R. Umar, and A. Ahmadi, “X X X X738X 738X 738X 738X (Print) (Print) (Print) (Print) Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ).”

[10] G. Fanani, I. Riadi, and A. Yudhana, “Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop,” *JURNAL MEDIA INFORMATIKA BUDIDARMA*, vol. 6, no. 2, p. 1263, Apr. 2022, doi: 10.30865/mib.v6i2.3946.

[11] S. Marcellino, H. B. Seta, and W. Widi, “JURNAL INFORMATIK Edisi ke-19,” 2023.

[12] “Metode Pengumpulan Data dan Instrumen Penelitian”.

[13] M. W. Indriyanto, D. Hariyadi, M. Habibi, U. J. Achmad, and Y. Yogyakarta, “INVESTIGASI DAN ANALISIS FORENSIK DIGITAL PADA PERCAKAPAN GRUP WHATSAPP MENGGUNAKAN NIST SP 800-86 dan SUPPORT VECTOR MACHINE.”

[14] “Pengaruh_Kejelasan_Sasaran_Anggaran_Peng”.

[15] A. Syah Putra and N. Aisyah, “ANALISIS PENGOLAHAN DATA FORENSIK PADA SOLID STATE DRIVE (SSD) MENGGUNAKAN FRAMEWORK GRR RAPID RESPONSE,” 2022.

BIODATA PENULIS

Rahmat Novrianda Dasmen,S.T.,M.Kom.
Dosen Teknik Komputer Fakultas Vokasi, Universitas Bina Darma Palembang
Email : : rahmat_novrianda@binadarma.ac.id

Ardiansyah
Mahasiswa Universitas Bina Darma,Program Studi D3 Teknik Komputer.
Email : ardi10062@gmail.com

M.Syaiful Huda Mubarok
Mahasiswa Universitas Bina Darma, Program Studi D3 Teknik Komputer.
Email : Syaifulmubarok716@gmail.com

Viren Pranata
Mahasiswa Universitas Bina Darma,Program Studi D3 Teknik Komputer.
Email : Virenpranata@gmail.com

M.Ary Januarta
Mahasiswa Universitas Bina Darma,Program Studi D3 Teknik Komputer.
Email : aryjanuarta30@gmail.com