JAITS: JOURNAL OF APPLIED INFORMATION TECHNOLOGY SOLUTION
Journal homepage: https://journal.universitasmulia.ac.id/index.php/jaits
ISSN:
Vol. 2 No.1 April 2025, Pg. 1 - 6

Urgensi Digital Forensik Untuk Pembuktian Tidak Pidana Siber Dalam Konteks Merusak Data Dan Sistem Elektronik

Julia Mustika[1*], Djumhadi[2], Muhammad Fahmi Abdillah[3], Dicky Satrio Ikhsan Utomo[4]

[1,3,4] Teknologi Informasi, Universitas Mulia
[2] Informatika, Universitas Mulia

Info Artikel
Kata Kunci:
Digital Forensik
Kejahatan Siber
Bukti Elektronik
Polda Kaltim

Histori Artikel
Received 19 Desember 2023
Revised 27 April 2025
Accepted 30 April 2025
Available online 15 November 2025

*Corresponding Author
Julia Mustika
Email Address:
julia.mus@students.universitasmulia.ac.id

Abstrak
Perkembangan teknologi informasi telah membawa dampak signifikan terhadap munculnya berbagai bentuk kejahatan siber, termasuk tindakan perusakan data dan sistem elektronik. Penelitian ini bertujuan untuk memahami urgensi penerapan digital forensik sebagai alat pembuktian hukum pada kasus tindak pidana siber, khususnya pada kasus yang ditangani oleh Subdit 5 Siber Ditreskrimsus Polda Kalimantan Timur. Metode penelitian yang digunakan adalah deskriptif, dengan teknik pengumpulan data melalui wawancara, observasi langsung, dan studi pustaka. Hasil penelitian menunjukkan bahwa penerapan digital forensik berperan penting dalam mengungkap bukti elektronik, seperti log perubahan password dan penghapusan data, yang menjadi dasar dalam proses penyelidikan dan penyidikan. Analisis terhadap perangkat bukti digital menunjukkan adanya indikasi penghapusan data secara sengaja oleh pelaku, yang kemudian dijadikan alat bukti sah dalam proses hukum. Temuan ini menegaskan bahwa digital forensik memiliki urgensi tinggi dalam mendukung pembuktian tindak pidana siber di Indonesia.

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan manusia, baik dalam bidang ekonomi, pendidikan, pemerintahan, maupun sosial budaya [1], [2]. Namun, di sisi lain, kemajuan ini juga menimbulkan tantangan baru berupa meningkatnya kejahatan yang memanfaatkan teknologi digital atau yang dikenal sebagai cybercrime[3], [4]. Menurut data Badan Siber dan Sandi Negara (BSSN), pada tahun 2023 tercatat lebih dari 361 juta anomali trafik yang berpotensi sebagai serangan siber di Indonesia, menunjukkan bahwa ancaman terhadap keamanan digital semakin meningkat setiap tahunnya [5]. Fenomena ini menegaskan bahwa penggunaan teknologi tanpa disertai keamanan informasi yang memadai dapat menimbulkan risiko serius terhadap data dan sistem elektronik [6].

Kejahatan siber memiliki beragam bentuk, seperti pencurian data, akses ilegal, perusakan sistem, hingga manipulasi informasi elektronik [7]. Salah satu bentuk yang sering terjadi adalah perusakan atau penghapusan data secara tidak sah, yang dapat mengganggu operasional lembaga maupun merugikan pihak tertentu [8], [9]. Tindak pidana ini diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), khususnya pada Pasal 32 dan 48, yang menegaskan sanksi bagi pihak yang dengan sengaja dan tanpa hak mengubah, menambah, mengurangi, menghapus, atau merusak informasi elektronik milik orang lain atau publik [10].

Dalam konteks penegakan hukum, tantangan utama aparat penegak hukum adalah membuktikan kejahatan siber melalui bukti digital yang sering kali bersifat volatil, mudah dihapus, atau dimodifikasi [11]. Di sinilah digital forensik memainkan peranan vital sebagai pendekatan ilmiah untuk mengidentifikasi, mengumpulkan, menganalisis, dan menyajikan bukti elektronik dengan tetap menjaga keutuhan (integrity) dan keabsahan (authenticity) data [12]. Digital forensik tidak hanya berfungsi sebagai alat bantu teknis, tetapi juga memiliki dimensi hukum, karena hasil analisisnya dapat dijadikan alat bukti sah di pengadilan [13].

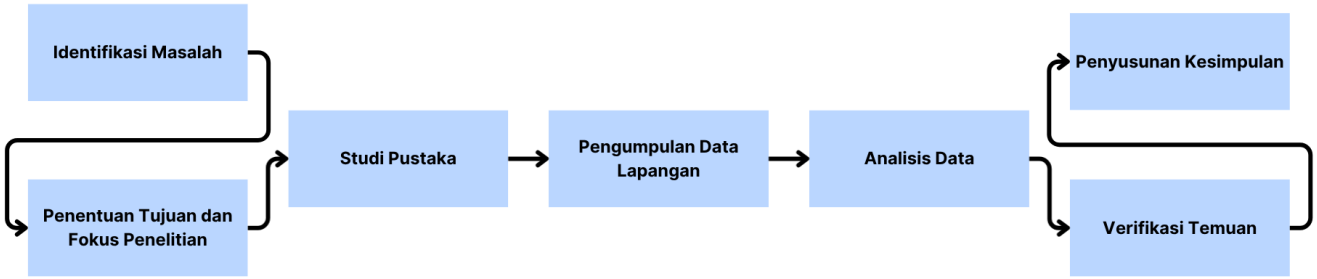
Subdirektorat 5 Siber Direktorat Reserse Kriminal Khusus (Ditreskrimsus) Polda Kalimantan Timur merupakan salah satu unit kepolisian daerah yang berfokus pada penanganan kejahatan berbasis teknologi informasi [11]. Unit ini memiliki peran penting dalam mendeteksi, menyelidiki, dan membuktikan kasus-kasus pelanggaran siber di wilayah Kalimantan Timur. Salah satu kasus yang pernah ditangani melibatkan dugaan penghapusan data dan perubahan sistem elektronik oleh individu di lingkungan perusahaan, yang menimbulkan kerugian operasional bagi pihak terkait. Kasus tersebut menjadi contoh konkret bagaimana penerapan digital forensik dapat membantu proses penyelidikan dan pembuktian hukum secara efektif.

Melalui kegiatan Kuliah Kerja Praktek (KKP) di Subdit 5 Siber Ditreskrimsus Polda Kalimantan Timur, mahasiswa memperoleh kesempatan untuk mengamati secara langsung bagaimana proses penyelidikan dan penyidikan kejahatan siber dilakukan. Selain itu, kegiatan ini juga memberikan pengalaman empiris [14] mengenai peranan digital forensik dalam praktik penegakan hukum, sekaligus memperkuat pemahaman mahasiswa terhadap tantangan nyata yang dihadapi aparat dalam menangani kejahatan berbasis elektronik [15].

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis urgensi penerapan digital forensik dalam pembuktian tindak pidana siber, khususnya dalam konteks kasus perusakan data dan sistem elektronik yang ditangani oleh Subdit 5 Siber Ditreskrimsus Polda Kalimantan Timur. Hasil penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan literatur di bidang keamanan siber dan penegakan hukum digital serta menjadi referensi bagi lembaga penegak hukum dalam memperkuat efektivitas penyelidikan dan pembuktian kasus siber di Indonesia.

2. Metode

Penelitian ini menggunakan pendekatan deskriptif kualitatif, yang bertujuan untuk menggambarkan secara sistematis dan faktual mengenai penerapan digital forensik dalam pembuktian tindak pidana siber, khususnya kasus perusakan data dan sistem elektronik yang ditangani oleh Subdirektorat 5 Siber Direktorat Reserse Kriminal Khusus (Ditreskrimsus) Polda Kalimantan Timur. Pendekatan ini dipilih karena sesuai untuk menjelaskan fenomena aktual yang terjadi di lapangan berdasarkan hasil observasi dan data empiris



Gambar 1. Alur Penelitian

2.1 Identifikasi Masalah

Mengidentifikasi permasalahan yang terjadi di lapangan untuk melihat bagaimana penerapan digital forensik digunakan untuk membantu pembuktian kasus tindak pidana siber berupa perusakan atau penghapusan data elektronik. Objek penelitian ini adalah proses penyelidikan dan penyidikan kasus dugaan tindak pidana siber yang berkaitan dengan perubahan dan penghapusan data secara ilegal. Penelitian dilaksanakan di lingkungan kerja Subdit 5 Siber Ditreskrimsus Polda Kalimantan Timur, tempat penulis melakukan kegiatan Kuliah Kerja Praktek (KKP). Pemilihan lokasi ini didasarkan pada relevansinya sebagai lembaga yang menangani langsung kasus-kasus kejahatan siber dan memiliki pengalaman dalam penerapan digital forensik.

2.2 Penentuan Tujuan dan Fokus Penelitian

Menetapkan tujuan penelitian untuk menganalisis urgensi digital forensik dalam proses pembuktian kasus tersebut di Subdit 5 Siber Ditreskrimsus Polda Kaltim.

2.3 Studi Pustaka

Melakukan kajian terhadap literatur dan peraturan terkait (UU ITE, jurnal tentang digital forensik, literatur keamanan siber, dan panduan penyidikan elektronik) sebagai dasar teori. Data yang digunakan dalam penelitian ini terdiri atas:

- Data primer, yang diperoleh langsung melalui wawancara dan observasi terhadap proses penanganan kasus di Subdit 5 Siber.
- Data sekunder, yang diperoleh dari literatur seperti buku, jurnal ilmiah, peraturan perundang-undangan, serta dokumen pendukung yang relevan dengan topik digital forensik dan kejahatan siber.

2.4 Teknik Pengumpulan Data

Untuk memperoleh data yang akurat dan komprehensif, penelitian ini menggunakan tiga teknik pengumpulan data, yaitu:

- Wawancara (Interview); Wawancara dilakukan dengan kepala unit, staf, dan anggota Subdit 5 Siber yang terlibat langsung dalam kegiatan penyelidikan dan penyidikan kasus. Tujuannya adalah untuk memperoleh informasi mengenai tahapan penanganan kasus, penggunaan metode digital forensik, serta kendala yang dihadapi dalam pembuktian tindak pidana siber
- Observasi Langsung (Direct Observation); Observasi dilakukan terhadap kegiatan operasional di Subdit 5 Siber Ditreskrimsus Polda Kaltim, khususnya proses identifikasi, pengamanan, dan analisis bukti digital. Melalui observasi ini, peneliti dapat memahami secara langsung prosedur dan alur kerja dalam investigasi forensik digital.
- Studi Pustaka (Literature Review); Teknik ini digunakan untuk mengumpulkan data dari sumber-sumber ilmiah seperti jurnal, buku, dan dokumen hukum yang berkaitan dengan digital forensik dan penegakan hukum siber. Studi pustaka berfungsi memperkuat landasan teori serta membandingkan temuan lapangan dengan konsep yang ada di literatur.

JAITS: JOURNAL OF APPLIED INFORMATION TECHNOLOGY SOLUTION
Journal homepage: https://journal.universitasmulia.ac.id/index.php/jaits
ISSN:
Vol. 2 No.1 April 2025, Pg. 1 - 6

2.5 Teknik Analisis Data

Data yang diperoleh dianalisis secara deskriptif kualitatif, yaitu dengan menafsirkan hasil wawancara, observasi, dan dokumentasi untuk memperoleh gambaran utuh tentang penerapan digital forensik dalam proses pembuktian tindak pidana siber. Analisis dilakukan melalui tiga tahap, yaitu:

- Reduksi data, dengan menyeleksi dan memfokuskan informasi yang relevan.
- Penyajian data, berupa uraian naratif mengenai hasil temuan di lapangan.
- Penarikan kesimpulan, berdasarkan hubungan antara teori, data empiris, dan praktik penegakan hukum di lapangan..

2.6 Verifikasi Temuan

Hasil analisis diverifikasi dengan sumber lapangan (penyidik Subdit 5 Siber) untuk memastikan keakuratan dan kesesuaian antara teori dan praktik.

2.6 Penyusunan Kesimpulan dan Laporan Akhir

Menyimpulkan hasil penelitian dan merumuskan urgensi penerapan digital forensik dalam pembuktian tindak pidana siber sebagai hasil akhir laporan.

3. Hasil dan Diskusi

3.1 Deskripsi Kasus

Penelitian ini dilakukan berdasarkan kegiatan Kuliah Kerja Praktek di Subdit 5 Siber Ditreskrimsus Polda Kalimantan Timur, yang menangani salah satu kasus pelanggaran terhadap Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Kasus tersebut melibatkan seorang karyawan perusahaan yang dengan sengaja dan tanpa hak melakukan perubahan, penghapusan, serta penguncian data elektronik milik perusahaan tempatnya bekerja. Peristiwa ini termasuk dalam kategori tindak pidana perusakan data dan sistem elektronik, sebagaimana diatur dalam Pasal 32 ayat (1) jo Pasal 48 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang ITE [10].

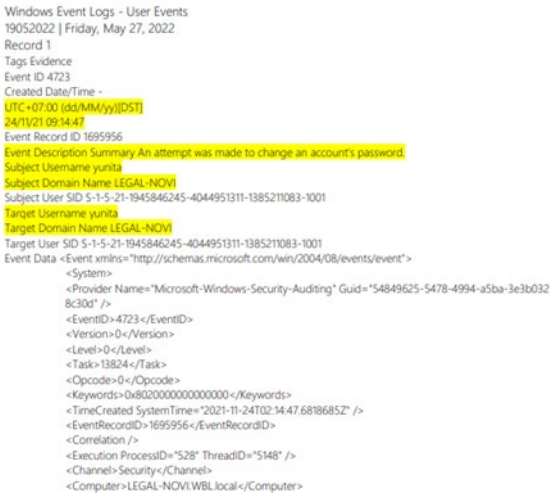
Gambar 2. Foto barang bukti Hardisk

Dari hasil pemeriksaan forensik terhadap perangkat bukti, ditemukan indikasi bahwa pelaku telah mengganti kata sandi sistem dan menghapus sejumlah file penting yang terkait dengan dokumen legal perusahaan. Berdasarkan laporan penyidik, perubahan password dilakukan pada tanggal 24 November 2021 pukul 09:14:47, dan aktivitas penghapusan folder terjadi sekitar pukul 09:00 pada hari yang sama. File yang dihapus meliputi dokumen administratif seperti perjanjian sewa menyewa, izin SIPA, sertifikat laik fungsi, dan dokumen pajak PBB. Data hasil analisis menunjukkan bahwa folder yang dihapus dipindahkan oleh sistem operasi Windows ke direktori "$OrphanedFiles", menandakan bahwa penghapusan dilakukan secara manual dan bukan akibat kerusakan sistem [12].

3.2 Proses Forensik Digital

Analisis forensik dilakukan terhadap satu unit hard disk internal merk Seagate Barracuda 7200.12 berkapasitas 250 GB (S/N: 6VMQRVYA). Pemeriksaan dilakukan menggunakan perangkat lunak digital forensic tools seperti Autopsy dan FTK Imager, untuk menemukan log aktivitas, metadata file, serta menelusuri file yang dihapus (deleted files recovery). Langkah-langkah utama yang dilakukan dalam proses forensik meliputi:

- Acquisition (Akuisisi Data): Pembuatan salinan image dari hard disk menggunakan metode bit-by-bit copy untuk menjaga keaslian bukti digital.
- Examination (Pemeriksaan): Analisis log sistem menunjukkan aktivitas perubahan password dan penghapusan folder tertentu dalam direktori user data.
- Analysis (Analisis): Ditemukan pola aktivitas pengguna yang konsisten dengan waktu kejadian penghapusan data, menguatkan dugaan adanya tindakan dengan sengaja.



Gambar 3. Informasi Perubahan Pasword

- Reporting (Pelaporan): Semua hasil temuan didokumentasikan dalam laporan digital forensik resmi Subdit 5 Siber Ditreskrimsus Polda Kaltim, termasuk tangkapan layar (screenshots), waktu aktivitas, dan file hash value untuk verifikasi integritas data [14]

3.3 Interpretasi Hasil

Berdasarkan hasil pemeriksaan, terdapat bukti kuat bahwa pelaku secara sengaja melakukan tindakan perubahan dan penghapusan data elektronik. Temuan ini mengonfirmasi bahwa penerapan metodologi digital forensik berperan penting dalam membuktikan keterlibatan individu dalam tindak pidana siber.

Dari sudut pandang teknis, analisis file system dan metadata memungkinkan penyidik untuk menelusuri jejak aktivitas meskipun pelaku telah berusaha menghapus bukti. Sementara dari sisi hukum, hasil forensik digital ini dapat dijadikan alat bukti sah di pengadilan karena memenuhi prinsip integritas, autentisitas, dan chain of custody sebagaimana disyaratkan dalam pembuktian elektronik [15], [16].

Temuan ini juga menunjukkan bahwa upaya pelaku untuk menghapus data tidak serta-merta menghilangkan bukti digital, karena remnant data masih dapat dipulihkan melalui analisis forensik [17]. Hal ini sejalan dengan hasil penelitian lain yang menegaskan bahwa file recovery dan analisis log menjadi elemen penting dalam pembuktian kasus data tampering dan unauthorized access [18].

3.4 Diskusi dan Implikasi

Dari hasil temuan tersebut, dapat disimpulkan bahwa penerapan digital forensik dalam penyelidikan kasus siber memiliki urgensi tinggi dalam mendukung proses penegakan hukum. Melalui prosedur yang terstandar, digital forensik membantu penyidik:

- Mengidentifikasi pelaku dengan data berbasis bukti;
- Menelusuri aktivitas sistem yang telah dimanipulasi;
- Mengembalikan data yang telah dihapus;
- Menyajikan hasil analisis yang dapat diterima secara hukum di pengadilan.

Implikasi penelitian ini juga menunjukkan bahwa perlu adanya:

- Peningkatan kapasitas sumber daya manusia di bidang forensik digital bagi aparat penegak hukum;
- Pemutakhiran perangkat lunak forensik agar mampu menangani jenis bukti dari sistem dan media terbaru;
- Kerja sama antara institusi pendidikan dan lembaga penegak hukum, untuk mendukung riset dan pelatihan berbasis kasus nyata.

Penerapan digital forensik terbukti mampu membantu penyidik dalam mengungkap tindak pidana perusakan data dan sistem elektronik di Polda Kalimantan Timur. Kasus yang dianalisis memperlihatkan bahwa teknik forensik mampu mengembalikan data yang dihapus, menelusuri perubahan sistem, serta memastikan integritas bukti digital yang digunakan dalam proses hukum. Hal ini menegaskan bahwa digital forensik bukan hanya sarana teknis, tetapi juga komponen penting dalam sistem pembuktian hukum modern di Indonesia.

4. Kesimpulan

Penelitian ini menegaskan bahwa penerapan digital forensik memiliki peranan yang sangat penting dalam proses pembuktian tindak pidana siber, khususnya pada kasus perusakan data dan sistem elektronik yang ditangani oleh Subdirektorat 5 Siber

Direktorat Reserse Kriminal Khusus (Ditreskrimsus) Polda Kalimantan Timur. Berdasarkan hasil analisis terhadap perangkat bukti digital berupa hard disk internal, diperoleh temuan bahwa pelaku dengan sengaja melakukan perubahan kata sandi dan penghapusan sejumlah file penting yang berkaitan dengan dokumen legal perusahaan. Melalui penerapan metode digital forensik, penyidik berhasil menemukan kembali bukti-bukti aktivitas tersebut, termasuk log waktu perubahan password, direktori file yang dihapus, serta lokasi pemulihan data di sistem file Windows. Proses pemeriksaan dilakukan secara terukur dengan mengikuti tahapan akuisisi, pemeriksaan, analisis, dan pelaporan, sehingga keaslian dan keabsahan bukti digital tetap terjaga. Hasil penelitian ini menunjukkan bahwa digital forensik tidak hanya berfungsi sebagai alat bantu teknis dalam proses investigasi, tetapi juga menjadi instrumen ilmiah yang memperkuat proses pembuktian hukum. Temuan forensik yang diperoleh memberikan dasar objektif bagi penyidik dalam mengidentifikasi pelaku dan membuktikan adanya tindakan melawan hukum sesuai dengan ketentuan Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Selain itu, penerapan digital forensik turut meningkatkan akuntabilitas penegakan hukum karena memastikan setiap tahapan penyelidikan mengikuti prinsip integrity, authenticity, dan chain of custody, yang menjadi syarat mutlak agar bukti digital dapat diterima di pengadilan. Sejalan dengan hasil temuan tersebut, penelitian ini juga menyoroti urgensi peningkatan kapasitas sumber daya manusia dalam bidang digital forensik, baik di kalangan aparat penegak hukum maupun di lembaga pendidikan. Pemerintah perlu mendorong pembaruan peraturan teknis mengenai tata cara pengelolaan dan pembuktian bukti digital agar sesuai dengan perkembangan teknologi yang cepat. Selain itu, institusi pendidikan diharapkan memperkuat kurikulum dan kegiatan praktikum berbasis laboratorium forensik untuk menyiapkan lulusan yang memiliki keahlian aplikatif di bidang ini. Ke depan, penelitian lanjutan diharapkan dapat memperluas fokus pada berbagai bentuk kejahatan siber lainnya seperti ransomware, phishing, atau data breach, serta mengkaji efektivitas beragam metode dan perangkat forensik digital yang digunakan dalam konteks Indonesia. Secara keseluruhan, penerapan digital forensik terbukti efektif dalam mendukung proses penyelidikan dan pembuktian tindak pidana siber. Temuan ini memperlihatkan bahwa digital forensik bukan sekadar alat teknis, tetapi merupakan fondasi ilmiah dalam sistem peradilan siber modern yang menggabungkan ketepatan teknologi dengan legitimasi hukum. Dengan penguatan kemampuan sumber daya manusia, dukungan kebijakan yang adaptif, dan kolaborasi antara dunia akademik dan lembaga penegak hukum, Indonesia dapat memperkuat ketahanan dan keadilan di ranah digital secara berkelanjutan.

Ucapan Terima Kasih

Penulis menyampaikan terima kasih yang sebesar-besarnya kepada Subdirektorat 5 Siber Direktorat Reserse Kriminal Khusus (Ditreskrimsus) Polda Kalimantan Timur atas kesempatan dan dukungan yang diberikan selama pelaksanaan kegiatan Kuliah Kerja Praktek. Ucapan terima kasih juga disampaikan kepada Kepala Subdit 5 Siber beserta seluruh staf dan penyidik, yang telah memberikan bimbingan, arahan, serta kesempatan untuk berpartisipasi langsung dalam proses penyelidikan dan analisis digital forensik di lapangan.

Referensi

[1] G. Guntoro, L. Costaner, and M. Musfawati, “ANALISIS KEAMANAN WEB SERVER OPEN JOURNAL SYSTEM (OJS) MENGGUNAKAN METODE ISSAF DAN OWASP (STUDI KASUS OJS UNIVERSITAS LANCANG KUNING),” *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 5, no. 1, p. 45, Jun. 2020, doi: 10.29100/jipi.v5i1.1565.

[2] V. A. Tandirerung, Riana T. Mangesa, and Syahrul, “Pengenalan Cyber Security Bagi Siswa Sekolah Menengah Atas,” *TEKNOVOKASI J. Pengabdi. Masy.*, vol. 1, no. 2, pp. 89–94, May 2023, doi: 10.59562/teknovokasi.v1i2.131.

[3] A. Wijayanto, I. Riadi, and Y. Prayudi, “TAARA Method for Processing on the Network Forensics in the Event of an ARP Spoofing Attack,” *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 7, no. 2, pp. 208–217, Mar. 2023, doi: 10.29207/resti.v7i2.4589.

[4] A. Wijayanto, I. Riadi, Y. Prayudi, and T. Sudinugraha, “Network Forensics Against Address Resolution Protocol Spoofing Attacks Using Trigger, Acquire, Analysis, Report, Action Method,” *Regist. J. Ilm. Teknol. Sist. Inf.*, vol. 8, no. 2, pp. 156–169, Jul. 2022, doi: 10.26594/register.v8i2.2953.

[5] A. Wijayanto, “Mengenal Cybersecurity: Perlindungan Data Pribadi Dan Privasi Di Sma Negeri 1 Samboja,” *J. Mulia*, vol. 3, no. 2, pp. 165–172, 2024, doi: 10.47002/jpm.v3i2.867.

[6] D. S. Valian Yoga Pudya Ardhana, Sugiarto, Yusuf Wahyu Setiya Putra, Riska Dwi Handayani, Djumhadi, M. Dermawan Mulyodiputro, Ahmad Fauzi Anggi Ariesta Kusuma, Agus Wijayanto, Fatkhurrochman, Danang Tejo Kumoro, Dwi Astuti, Wahyu Priyoatmoko, Hafidudin, *Konsep Dasar Teknologi Informasi*. Mega Press Nusantara, 2024. [Online]. Available: https://books.google.co.id/books?hl=id&lr=&id=siceEQAAQBAJ&oi=fnd&pg=PA40&dq=%5BBUKU%5D+Konsep+Dasar+Teknologi+Informasi+megapress&ots=MZ_mfOY0XN&sig=x1whZMMSAIrwkd-L1DSNMGf47zk&redir_esc=y#v=onepage&q=%5BBUKU%5D Konsep Dasar Teknologi Informasi megapress

[7] W. A. Purnama, Y. Servanda, Djumhadi, and A. Wijayanto, “Analisis Kasus Kehilangan Data Akibat Format dan

Pemulihan Data Menggunakan Aplikasi Wondershare Recoverit," *J. JTIK (Jurnal Teknol. Inf. dan Komunikasi)*, vol. 8, no. 4, pp. 1042–1050, Oct. 2024, doi: 10.35870/jtik.v8i4.2367.

[8] W. Aji Purnama, Y. Servanda, and dan Agus Wijayanto, "Analisis Efektifitas Recovery Toolkit Untuk Media Penyimpanan Menggunakan Pendekatan Criteria-Based Evaluation Analysis of the Effectiveness of the Recovery Toolkit for Storage Media Using a Criteria-Based Evaluation Approach," *J. Bus. Audit Inf. Syst.*, vol. 8, no. 1, pp. 35–48, 2025, [Online]. Available: http://journal.ubm.ac.id/index.php/jbase

[9] B. Fachri and F. H. Harahap, "Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer," *J. MEDIA Inform. BUDIDARMA*, vol. 4, no. 2, p. 413, Apr. 2020, doi: 10.30865/mib.v4i2.2037.

[10] L. Galchynsky and A. Murtazina, "Vulnerability detection in the network traffic flow of the RADIUS protocol based on the object-oriented model," *Theor. Appl. Cybersecurity*, vol. 4, no. 1, Feb. 2023, doi: 10.20535/tacs.2664-29132022.1.274119.

[11] K. Khairunnisak and W. Widodo, "Digital Forensic Tools And Techniques For Handling Digital Evidence," *J. Resist. (Rekayasa Sist. Komputer)*, vol. 6, no. 1, pp. 1–11, Apr. 2023, doi: 10.31598/jurnalresistor.v6i1.1266.

[12] R. Badillah, A. Yulia Muniar, A. Rahman, F. Hidayat Saputra, and S. Sahibu, "Digital Forensic Evidence Analysis in Revealing Defamation on Social Media (Twitter) Using the Static Forensics Method," *Ceddi J. Inf. Syst. Technol.*, vol. 2, no. 2, pp. 2829–808, 2023, doi: 10.56134/jst.v2i2.45.

[13] "komputer-forensik".

[14] P. P. I. Prayitno *et al.*, "PELATIHAN PENGEMBANGAN KETERAMPILAN SISWA DENGAN MENERAPKAN TEKNOLOGI DALAM PENDIDIKAN," *J. MULIA*, vol. 3, no. 1, pp. 129–133, Feb. 2024, doi: 10.47002/jpm.v3i1.782.

[15] M. F. Abdillah and Y. Prayudi, "Data Recovery Comparative Analysis using Open-based Forensic Tools Source on Linux," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 9, 2022, doi: 10.14569/IJACSA.2022.0130975.