JESIK: Jurnal Elektronik Sistem Informasi dan Komputer
Vol 12 No 1, Juni 2026
ISSN: 2477-5290 (Print) ISSN: 2502-2148 (Electronic)
Open Access: https://jesik.web.id/index.php/jesik

Penerapan Metode Analisis Jejak Penelusuran Web Dalam Mengungkap Pola Perilaku Pengguna yang Terindikasi Melakukan Kejahatan Siber

Heru Prabowo
Sekolah Tinggi Manajemen Informatika Dan Komputer Bina Mulia Palu, Indonesia

[1]masheru.prabowo@gmail.com

Article Info

Article history:
Received 07/05/2026
Revised 20/05/2026
Accepted 20/05/2026

Keyword:
Web browsing traces;
Digital forensic analysis;
User behavior patterns;
Cybercrime;
Data extraction;
Suspicious activity detection

ABSTRACT

According to data released by the Indonesian Internet Service Providers Association, the number of internet users in Indonesia will reach more than 221 million by 2024. This large number certainly has both positive and negative impacts. One negative impact is the emergence of cybercrime. Cybercrime can be identified, among other things, through digital traces stored in the browser application used. Web browsing traces contain a wealth of information that can be used to determine user activity and intent. This study aims to analyze browsing traces such as website access history, cache data, and cookie files to identify behavioral patterns indicative of cybercrime. The methods used include data extraction, data cleansing, and pattern analysis using a simple statistical approach. The study results show a percentage of behavioral patterns indicative of cybercrime of 80.78% and the ability to generate a list of patterns that serve as indicators of suspicious activity. This study also provides a method for presenting the analysis results in an easily understood and accountable format.

PENDAHULUAN

Pemanfaatan internet di Indonesia mengalami pertumbuhan yang begitu signifikan. Berdasarkan data dari Asosiasi Penyelenggara Jasa Internet Indonesia, total pengguna internet di Indonesia pada tahun 2024 telah mencapai angka 221.563.479 jiwa dari keseluruhan jumlah penduduk Indonesia sebesar 278.696.200 jiwa pada tahun 2023 (APJII, 2024). Internet saat ini telah menjadi elemen penting dalam kehidupan sehari-hari, mencakup kegiatan komunikasi, pencarian informasi, transaksi, hingga pelaksanaan urusan bisnis dan pekerjaan. Bertambahnya jumlah pengguna tersebut menandakan bahwa dunia maya telah berkembang menjadi lingkungan yang luas dan dinamis, sekaligus menjadi tempat tersimpannya beragam data dan aktivitas para penggunanya.

Dibalik berbagai kegunaan yang ditawarkannya, perkembangan pemanfaatan internet turut menimbulkan dampak negatif berupa maraknya kasus kejahatan didunia siber (Kiki Kristanto & Rakhmat Baihaki, 2025). Kejahatan tersebut hadir dalam berbagai bentuk, antara lain penipuan yang dilakukan secara daring, pencurian informasi pribadi, pembobolan sistem, penyebaran konten terlarang, hingga tindakan yang mengancam stabilitas keamanan dan ketertiban dimasyarakat. Dampak yang diakibatkannya pun tidak sebatas kerugian secara materiil seperti kehilangan finansial, namun juga dapat berujung pada rusaknya reputasi, tekanan psikologis, bahkan ancaman bagi keamanan negara Menurut (Kristanto dan Baihaki, 2025). Salah satu hambatan terbesar dalam penanganan kasus ini adalah karakteristik kejahatan tersebut yang tidak meninggalkan bukti dalam bentuk fisik yang kasat mata, melainkan hanya berupa jejak digital yang tersembunyi didalam sistem, sehingga diperlukan pendekatan khusus untuk menemukan dan mengolahnya menjadi informasi yang sah secara hukum (Kementerian Komunikasi dan Digital, 2024).

Sejumlah penelitian telah banyak mengulas teknik perolehan bukti digital serta cara mengenali aktivitas yang patut dicurigai diruang siber. Namun, sebagian besar kajian tersebut cenderung menitikberatkan pada proses pengumpulan data secara umum atau analisis pada komponen sistem tertentu saja, dan belum secara mendalam mengkaji bagaimana jejak penelusuran web dapat dimanfaatkan sebagai sumber informasi utama (Gargi Sarkar et al., 2023). Disamping itu, masih terbatasnya penelitian yang merancang metode analisis secara terstruktur untuk mengonversi data jejak

penelusuran tersebut menjadi pola perilaku pengguna yang teridentifikasi dengan jelas, yang selanjutnya dapat dijadikan landasan dalam mendeteksi indikasi terjadinya kejahatan siber (Melissa Martineau et al., 2023; C. Wang, 2025).

Bertolak dari kesenjangan tersebut, penelitian ini dijalankan dengan tujuan menerapkan metode analisis yang sistematis dan terarah guna mengungkap pola perilaku dimaksud, sehingga mampu melengkapi kekurangan yang terdapat pada penelitian-penelitian terdahulu.

METODE PENELITIAN

Jenis penelitian ini adalah penelitian deskriptif eksperimental dengan menggunakan metode gabungan yaitu metode kuantitatif dan metode kualitatif. Penelitian gabungan (atau metode kombinasi/mixed methods) adalah pendekatan penelitian yang menggabungkan metode kuantitatif dan kualitatif dalam satu penelitian (Sugiyono, 2023). Tujuannya adalah untuk memahami suatu masalah penelitian secara lebih komprehensif, mendalam, dan valid dibandingkan jika hanya menggunakan satu metode saja. Pertama menggunakan pendekatan eksperimental, pendekatan ini dilakukan dengan cara membuat skenario aktifitas pengguna yang disimulasikan untuk mendapatkan data jejak penelusuran web yang akan dijadikan objek pengujian dan analisis. Kedua menggunakan pendekatan deskriptif, yang mana pendekatan ini digunakan untuk menjabarkan ciri-ciri data, proses pengolahan, serta pola perilaku yang ditemukan secara rinci dan jelas. Ketiga menggunakan pendekatan kuantitatif, pendekatan ini digunakan untuk mengolah data berupa angka, seperti frekuensi kunjungan, durasi akses, dan jumlah kata kunci pencarian yang digunakan. Serta keempat menggunakan pendekatan kualitatif, yang mana pendekatan ini digunakan untuk menganalisis makna dan konteks dari aktivitas yang dilakukan pengguna, serta mengelompokkan aktivitas tersebut kedalam kategori yang berindikasi berbahaya atau tidak.

Pada penelitian ini yang menjadi objek penelitian adalah jejak penelusuran web yang tersimpan diperangkat komputer atau telpon seluler, meliputi riwayat akses situs, data cookie, data cache, berkas yang diunduh, serta informasi lain yang tersimpan akibat aktivitas penelusuran di internet. Selanjutnya yang menjadi subjek penelitian adalah aktivitas pengguna yang dibagi menjadi dua kelompok, yaitu aktivitas yang bersifat legal dan aktivitas yang berindikasi melakukan kejahatan siber. Jenis kejahatan siber yang menjadi fokus penelitian meliputi akses ilegal kesistem, penyebaran konten terlarang, penipuan daring, serta persiapan tindakan yang dapat merugikan pihak lain.

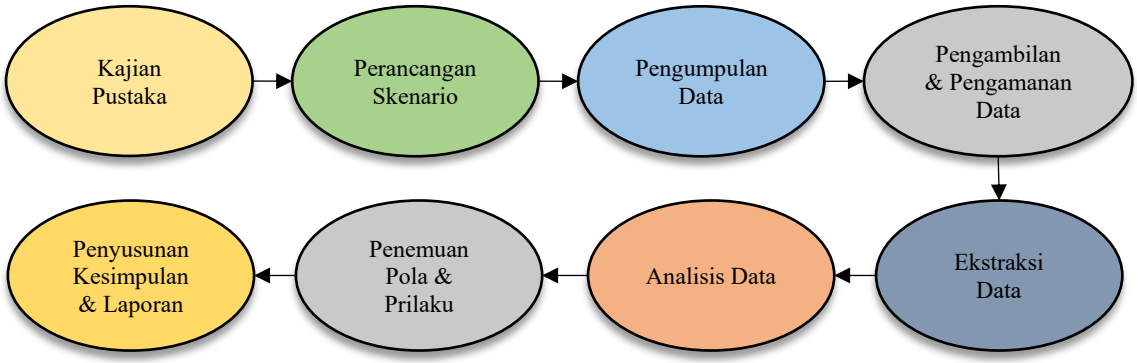
Untuk mendukung simulasi yang akan dilakukan pada penelitian ini, dibutuhkan perangkat keras yaitu ;

1. Desktop PC dengan spesifikasi processor Intel Core I3-1125G4, RAM 8Gb, Harddisk 512Gb (digunakan sebagai evidence container/komputer yang digunakan sebagai barang bukti).
2. Laptop dengan spesifikasi processor AMD Ryzen 5 3500U, RAM 8Gb, SSD 256Gb (digunakan sebagai komputer tempat proses digital forensik)
3. External hardisk Toshiba 512Gb (digunakan sebagai tempat penyimpanan hasil kloning dari evidence container).

Selanjutnya untuk menjalankan perangkat keras serta proses digital forensik dibutuhkan perangkat lunak antara lain ;

1. Sistem operasi Microsoft Windows 11 - 64 bit
2. Google Chrome versi 147.0.7727.119 atau dengan versi yang lebih tinggi
3. FTK Imager versi 3.2.0 atau dengan versi yang lebih tinggi
4. DBBrowser for SQLite versi 3.13.1 atau dengan versi yang lebih tinggi

Kerangka pikir penelitian disusun untuk menggambarkan alur pemikiran dalam penelitian ini. Alur pemikiran ditampilkan dalam bentuk diagram yang saling terhubung dan berurutan. Berikut diagram kerangka pikir penelitian,



Gambar 1. Diagram Kerangka Pikir Penelitian

HASIL DAN PEMBAHASAN

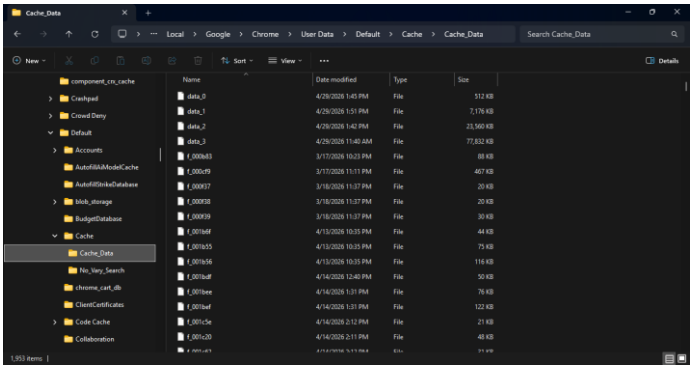
Sebelum dilakukan proses forensik digital terlebih dahulu dilakukan proses kloning / menyalin data ketempat penyimpanan baru yang nantinya digunakan untuk proses digital forensik. Hal ini dilakukan untuk melindungi barang bukti agar tidak rusak (Perkapolri No. 10 Tahun 2010). Data penelitian diperoleh dari hasil simulasi aktivitas penelusuran web yang dilakukan pada dua kelompok skenario, yaitu Skenario A (aktivitas legal) dan Skenario B (aktivitas berindikasi melanggar hukum). Simulasi dilakukan pada perangkat dengan sistem operasi Microsoft Windows 11 – 64 bit dan peramban Google Chrome versi 147.0.7727.119 yang merupakan versi yang dipergunakan penulis saat penelitian dilaksanakan.

Seluruh data yang dihasilkan kemudian diambil dan diamankan menggunakan perangkat lunak FTK Imager (Moh.Subli, 2023). Verifikasi integritas data dilakukan dengan menghasilkan nilai hash SHA-256, yang menunjukkan bahwa data salinan memiliki nilai yang sama persis dengan data asli seperti ditunjukkan pada Tabel 1, sehingga keaslian dan keutuhan data terjamin.

Tabel 1. Hasil Verifikasi Integritas Data

Jenis Data	Nilai Hash SHA-256	Keterangan
Data Asli Skenario A	a7f2d9c3e8b4a1f5e6d7c2b8a9f1e3d4c5b6a7f8e9d0c1b2a3f4e5d6c7b8a9f0	Sah dan tidak berubah
Data Salinan Skenario A	a7f2d9c3e8b4a1f5e6d7c2b8a9f1e3d4c5b6a7f8e9d0c1b2a3f4e5d6c7b8a9f0	Sama dengan data asli
Data Asli Skenario B	b8e3c2d1f0a9b8c7d6e5f4a3b2c1d0e9f8a7b6c5d4e3f2a1b0c9d8e7f6a5b4c3	Sah dan tidak berubah

Data yang berhasil diekstrak meliputi riwayat akses situs, data cookie, data cache, catatan pencarian, serta jejak aktivitas lain yang tersimpan dalam struktur basis data SQLite milik peramban yang tersimpan pada C:\Users\Axioo\AppData\Local\Google\Chrome\User Data\Default\



Gambar 2. Folder Data Google Chrome

Secara keseluruhan, terdapat 1.247 catatan data yang berhasil dikumpulkan, seperti terlihat pada Tabel 2 sebagai berikut :

Tabel 2. Rincian Jumlah Data yang Berhasil Diekstrak

Jenis Data	Jumlah pada Skenario A	Jumlah pada Skenario B	Jumlah Keseluruhan
Riwayat akses situs	327	298	625
Kata kunci pencarian	112	135	247
Data cookies	98	107	205
Data cache	76	68	144
Berkas yang diunduh	14	12	26

Hasil Analisis Karakteristik Data

Berdasarkan data yang telah didapat maka langkah berikutnya adalah melakukan pengelompokan data kedalam lima kategori untuk selanjutnya dilakukan analisa.

1. Berdasarkan Jenis Situs yang Diakses
   Pengelompokan jenis situs dilakukan berdasarkan kategori isi dan tujuan situs yang terdaftar secara resmi. Berikut adalah hasil pengelompokan data :

Tabel 3. Distribusi Jenis Situs yang Diakses

Kategori Situs	Persentase Akses Skenario A (%)	Persentase Akses Skenario B (%)
Pendidikan dan pengetahuan	38,2	4,1
Instansi dan layanan resmi	27,5	2,7
Perdagangan dan jasa legal	21,3	8,4
Hiburan dan informasi umum	13,0	15,2
Konten berbahaya / terlarang	0	42,3
Situs penyedia alat ilegal	0	27,3

Dari Tabel 3 terlihat bahwa pada Skenario A, sebagian besar akses ditujukan kesitus yang memiliki tujuan positif dan legal. Sebaliknya, pada Skenario B, lebih dari 69,6% akses dilakukan kesitus yang menyediakan konten atau layanan yang dilarang oleh peraturan perundang-undangan yang berlaku.

2. Berdasarkan Pola Kata Kunci Pencarian
   Analisis kata kunci pencarian dilakukan dengan mengelompokkan kata kunci berdasarkan makna dan tujuan pencarian, serta menghitung frekuensi kemunculannya. Berikut adalah hasilnya :

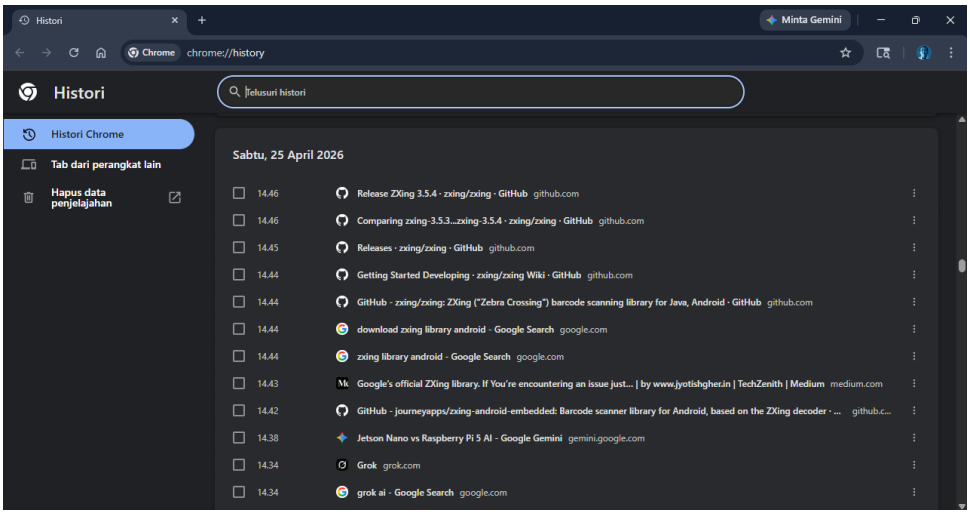
Tabel 4. Klasifikasi Kata Kunci Pencarian

Kategori Kata Kunci	Contoh Kata Kunci yang Digunakan	Frekuensi pada Skenario A	Frekuensi pada Skenario B
Pencarian informasi umum	cara merakit komputer, jadwal perkuliahan, cara berkebun	78	12
Pencarian layanan dan transaksi	cara membuka rekening bank, daftar harga barang elektronik	34	9
Pencarian dengan indikator bahaya	cara membobol akun, cara menyadap pesan, membuat virus komputer	0	76
Pencarian alat untuk kejahatan	perangkat lunak pencuri data, alat pemutus jaringan, nomor palsu	0	38

Hasil analisis dari Tabel 4 menunjukkan bahwa pada Skenario B terdapat pola penggunaan kata kunci yang secara khusus ditujukan untuk mencari informasi atau alat yang dapat digunakan untuk

melakukan tindakan yang melanggar hukum, sedangkan pola ini sama sekali tidak ditemukan pada Skenario A.

3. Berdasarkan Waktu dan Durasi Akses
Waktu serta durasi akses dilihat dengan membuka riwayat akses situs yang terdapat pada menu *history* di peramban Google Chrome.



Gambar 3. Riwayat Akses pada Peramban Google Chrome

Analisis waktu akses dilakukan dengan membagi waktu kedalam tiga periode, yaitu waktu aktif (07.00 – 17.00), waktu istirahat (17.00 – 22.00), dan waktu tidak wajar (22.00 – 07.00). Durasi akses dihitung dalam satuan menit per kunjungan.

Tabel 5. Distribusi Waktu dan Durasi Akses

Periode Waktu	Persentase Akses Skenario A (%)	Persentase Akses Skenario B (%)	Rata-rata Durasi Akses (menit)
Waktu Aktif	76,4	18,5	Skenario A: 12,8 Skenario B: 37,2
Waktu Istirahat	21,7	34,3	Skenario A: 4,1 Skenario B: 51,7
Waktu Tidak Wajar	1,9	47,2	Skenario A: 5,1 Skenario B: 59,7

Dari Tabel 5 dapat diketahui bahwa pada Skenario B, hampir setengah dari seluruh aktivitas penelusuran dilakukan pada waktu yang tidak wajar, dengan durasi akses yang jauh lebih lama dibandingkan dengan aktivitas pada Skenario A. Hal ini menunjukkan adanya kecenderungan pengguna untuk melakukan aktivitas yang dicurigai pada waktu yang jarang dipantau.

4. Berdasarkan Tindakan Pasca Aktivitas
Analisis juga dilakukan terhadap tindakan yang dilakukan pengguna setelah menyelesaikan aktivitas penelusuran. Hasil pengamatan disajikan dalam Tabel 6 berikut :

Tabel 6. Jenis Tindakan yang Dilakukan Pasca-Aktivitas

Jenis Tindakan	Kejadian pada Skenario A (%)	Kejadian pada Skenario B (%)
Menutup peramban tanpa penghapusan data	92,7	12,4

Menghapus riwayat penelusuran Sebagian	5,8	41,6
Menghapus seluruh data penelusuran	1,5	46,0

Hasil ini menunjukkan bahwa pengguna yang melakukan aktivitas berindikasi melanggar hukum cenderung melakukan upaya penghapusan jejak aktivitasnya, yang merupakan ciri khas perilaku yang dilakukan secara tersembunyi.

5. Hasil Penemuan Pola Perilaku

Berdasarkan analisis yang telah dilakukan terhadap seluruh data yang dikumpulkan, ditemukan beberapa pola perilaku yang dapat digunakan sebagai indikator untuk mengidentifikasi pengguna yang berindikasi melakukan kejahatan siber. Pola-pola tersebut disusun berdasarkan kombinasi dari karakteristik data yang telah dianalisis sebelumnya, sebagai berikut :

Tabel 7. Pola Perilaku Pengguna yang Berindikasi Melakukan Kejahatan Siber

Kode Pola	Karakteristik yang Menyusun Pola	Indikasi yang Diberikan
P1	Mengakses situs yang menyediakan konten atau alat ilegal, dengan frekuensi ≥ 3 kali dalam seminggu	Pengguna sedang mencari bahan atau alat untuk melakukan tindakan yang melanggar hukum
P2	Menggunakan kata kunci pencarian yang berhubungan dengan teknik penyerangan sistem, pencurian data, atau penipuan daring	Pengguna sedang mengumpulkan informasi untuk merencanakan tindakan kejahatan siber
P3	Melakukan aktivitas penelusuran pada waktu tidak wajar (22.00 – 07.00) dengan durasi ≥ 30 menit per sesi	Pengguna berusaha menyembunyikan aktivitasnya agar tidak terdeteksi
P4	Melakukan penghapusan riwayat penelusuran secara keseluruhan atau sebagian secara rutin setelah melakukan aktivitas tertentu	Pengguna berusaha menghilangkan bukti aktivitas yang telah dilakukan
P5	Mengkombinasikan dua atau lebih karakteristik dari pola P1 sampai P4	Indikasi kuat bahwa pengguna sedang melakukan atau merencanakan tindakan kejahatan siber

Pola-pola pada Tabel 7 diuji kembali terhadap data percobaan tambahan yang tidak digunakan dalam proses penyusunan pola, dan dari penjumlahan hasil terhadap 4 pola perilaku pada skenario B diperoleh jumlah prosentase sebesar 80,78%.

Dari hasil analisis yang dilakukan diketahui bahwa 5 aspek diantaranya jenis situs yang diakses, kata kunci pencarian, waktu akses, tindakan setelah aktifitas mengakses situs di internet serta lama akses yang merupakan kombinasi dari aspek jenis situs dan waktu akses dapat memperlihatkan adanya kecenderungan pengguna kesatu sisi aktifitas. Dengan prosentase sebesar 80,78% dalam penelitian ini dapat dikatakan bahwa aktifitas yang dilakukan pengguna berindikasi melakukan kejahatan siber (C. Wang, 2025). Tetapi masih terdapat sekitar 19,22% kasus yang tidak dapat diidentifikasi dengan tepat, yang disebabkan oleh adanya aktifitas yang memiliki kesamaan ciri dengan kedua kategori.

Dari penelitian yang telah ada sebelumnya, umumnya menggunakan 1 hingga 2 aspek dalam menentukan pola perilaku pengguna dalam melakukan kejahatan siber. Dengan melihat log akses dari aplikasi dan melihat jenis situs yang diakses (Gargi Sarkar et al., 2023). Dengan jumlah aspek yang minim dirasa belum secara maksimal bisa menentukan pola perilaku pengguna dalam melakukan kejahatan siber, karena dari hal sama bisa jadi penggunanya tidak berniat untuk melakukan kejahatan siber, tetapi untuk keperluan penelitian (Moh.Subli, 2023).

Dibutuhkan jumlah aspek yang lebih lagi dalam menentukan pola perilaku pengguna dalam melakukan kejahatan siber. Aspek-aspek seperti melihat jenis situs yang diakses, kata kunci pencarian, waktu akses, tindakan setelah aktifitas mengakses situs di internet serta lama akses yang merupakan

kombinasi dari aspek jenis situs dan waktu akses dapat lebih meyakinkan (Melissa Martineau et al., 2023).

KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan, dapat diambil kesimpulan bahwa jejak penelusuran web yang tersimpan diperangkat pengguna ternyata dapat diolah menjadi data dasar dalam menentukan karakteristik aktifitas legal dan aktifitas yang melanggar hukum. Indikasi pelanggaran hukum diketahui berdasar pada jenis situs yang diakses, pola pencarian, waktu akses, serta tindakan setelah beraktifitas. Dari pengembangan metode analisis yaitu dengan menggabungkan aspek teknis, isi, dan kontek ternyata dapat mengidentifikasi aktifitas yang berindikasi kejahatan siber sebesar 80,78%. Model ini juga menghasilkan lima pola perilaku sebagai indikator yang disusun dari kombinasi karakteristik data guna meminimalkan kesalahan penafsiran dalam mendeteksi potensi kejahatan siber.

REFERENSI

Kiki Kristanto & Rakhmat Baihaki, (2025). Tindak Pidana Siber di Indonesia Regulasi, Tantangan, dan Penegakan Hukum. PT Media Penerbit Indonesia. (pp. 72-74)

Gargi Sarkar, Hardeep Singh, Subodh Kumar, Sandeep K. Shukla, (2023). Tactics, Techniques and Procedures of Cybercrime: A Methodology and Tool for Cybercrime Investigation Process. ARES'23: Proceedings of the 18th International Conference on Availability, Reliability and Security. Article No.: 107, Pages 1-10. https://doi.org/10.1145/3600160.3605013

Melissa Martineau, Elena Spiridon & Mary Aiken, (2023). A Comprehensive Framework for Cyber Behavioral Analysis Based on a Systematic Review of Cyber Profiling Literature. Forensic Sci. 2023, 3(3), 452-477. https://doi.org/10.3390/forensicsci3030032

C.Wang, (2025). Identifying Hidden Cybercrime Behavior by Behavior Tomographer. Journal Springer Nature Link, pp 137–172. https://link.springer.com/chapter/10.1007/978-981-95-1013-9_6

APJII (2024). Asosiasi Penyelenggara Jasa Internet Indonesia Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang. https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang

Kementerian Komunikasi dan Digital. (2024). Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. JDIH Komdigi. https://jdih.komdigi.go.id

Moh.Subli, (2023). Langkah-Langkah Imaging Accessdata FTK Imager. Proses Imaging, Melakuka Proses Imaging, Melakukan Extract Data Hasil Imaging kemudian Melihat Nilai Hashing, Cek File Signature, Mengembalikan File yang sudah di Hapus, dan Terakhir Melakukan Verifikasi. https://uii.academia.edu/Departments/Network_Forensik_Digital/Documents.

Sugiyono. (2023). Metode Penelitian Kombinasi (Mixed Methods) dengan 9 Desain. Alfabeta.