Research Article
Forbis: Journal Forensic Business Information Systems
Published online on: https://journal.universitasmulia.ac.id/index.php/forbis **1 (1) Januari 2024**

ANALISIS FORENSIK DIGITAL PADA APLIKASI MEDIA SOSIAL FACEBOOK MENGGUNAKAN METODE STATIK FORENSIK

Chairul Ridwan Caesar[1*], Yustian Servanda[2], Yeyen Dwi Atma[3]

[1,2,3] Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Mulia

email: [1]*chairulridwan@students.universitasmulia.ac.id*, [2]yustians@universitasmulia.ac.id, [3]yeyenduwy@gmail.com
[*]*Correspondence*

ARTICLE INFO

Article History
Received : 12 Desember 2023
Revised : 21 Januari 2024
Accepted : 22 Januari 2024
Available online : 22 Januari 2024

Keywords:
Digital Forensic, Forensic Static, Cybercrime, Sosial Media, Facebook

Please cite this article in IEEE style as:

ABSTRACK

The rapid development of internet technology and the increasing number of social media users have led to a rise in crime on social media platforms, including Facebook. This freedom of expression can make users both victims and perpetrators. A significant amount of crime occurs on social networks like Facebook, including the spread of fake news. Unfortunately, many Indonesians readily believe unverified information, leading to disputes and divisions. Additionally, pornography, hate speech, harassment, and other criminal activities can occur online. However, no crime is truly without a trace. This research, "Digital Forensic Analysis on the Facebook Social Media Application using the Static Forensic method," aims to assist legal processes based on applicable laws to uncover and expose crimes committed on the internet.

ABSTRAK

Pesatnya perkembangan teknologi internet dan meningkatnya jumlah pengguna media sosial menyebabkan meningkatnya kejahatan di platform media sosial, termasuk Facebook. Kebebasan berekspresi ini dapat menjadikan penggunanya sebagai korban sekaligus pelaku. Sejumlah besar kejahatan terjadi di jejaring sosial seperti Facebook, termasuk penyebaran berita palsu. Sayangnya, banyak masyarakat Indonesia yang mudah mempercayai informasi yang tidak terverifikasi, sehingga menyebabkan perselisihan dan perpecahan. Selain itu, pornografi, perkataan yang mendorong kebencian, pelecehan, dan aktivitas kriminal lainnya dapat terjadi secara online. Namun, tidak ada kejahatan yang benar-benar tanpa jejak. Penelitian yang berjudul "Analisis Digital Forensik Pada Aplikasi Media Sosial Facebook Dengan Metode Static Forensik" ini bertujuan untuk membantu proses hukum berdasarkan peraturan perundang-undangan yang berlaku untuk mengungkap dan mengungkap kejahatan yang dilakukan di internet.

1. Pendahuluan

Salah satu media sosial yang sangat populer saat ini adalah Facebook. Indonesia tercatat menempati posisi ketiga pengguna Facebook terbanyak di dunia menurut laporan tersebut. Jumlahnya mencapai 119,9 juta pengguna per Januari 2023 lalu. Facebook (populer disingkat FB) adalah media sosial dan layanan jejaring sosial daring Amerika yang dimiliki oleh Meta Platforms. Adanya layanan membuat status dan penyebaran informasi pada media sosial ini, berartikan bahwa pengguna bebas untuk mengapresiasikan pikiran mereka dalam bentuk teks, gambar, suara, maupun video[1].

Hoaks merupakan salah satu jenis kejahatan yang paling sering terjadi di Facebook. Hoaks dapat menimbulkan keresahan dan konflik di masyarakat. Ujaran kebencian juga merupakan kejahatan yang sering terjadi di Facebook. Ujaran kebencian dapat menimbulkan diskriminasi dan kekerasan terhadap kelompok tertentu. Konten pornografi juga merupakan kejahatan yang sering terjadi di Facebook. Konten pornografi dapat merusak moralitas dan mental masyarakat, terutama anak-anak dan remaja[2], [3].

Selain ketiga jenis kejahatan di atas, masih banyak lagi kejahatan yang dapat dilakukan di Facebook, seperti penipuan, pemerasan, dan pencurian data pribadi. Dengan berkembangnya teknologi informasi, kejahatan di media sosial, termasuk Facebook, akan semakin meningkat. Oleh karena itu, diperlukan upaya-upaya untuk mencegah dan mengatasi kejahatan di media sosial[4], [5].

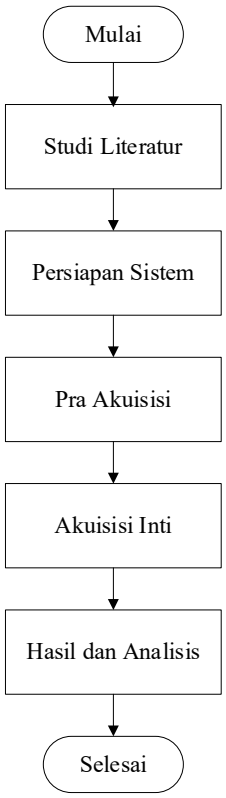
Forensik media sosial adalah disiplin ilmu yang mempelajari proses pengumpulan, analisis, dan interpretasi data digital dari media sosial untuk tujuan investigasi. Forensik media sosial dapat digunakan untuk membantu mengungkap kejahatan yang terjadi di media sosial, seperti hoaks, ujaran kebencian, dan konten pornografi. Untuk mengatasi masalah tersebut, diperlukan upaya-upaya untuk mengembangkan standarisasi dalam praktik forensik media sosial. Standarisasi tersebut dapat membantu memastikan bahwa proses forensik media sosial dilakukan secara profesional dan komprehensif[6], [7].

Metode statik forensik merupakan salah satu metode forensik digital yang dilakukan tanpa mengubah data digital yang dianalisis. Metode ini dapat digunakan untuk mengumpulkan bukti digital dari media sosial. Metode statik forensik dapat digunakan untuk mengungkap kejahatan di media sosial, seperti hoaks, ujaran kebencian, dan konten pornografi[8], [9]. Sehingga pemilihan metode forensic yang tepat menjadi Solusi untuk proses investigasi siber[10], [11].

2. Metode Penelitian

2.1. Alur Penelitian

Penelitian ini menggunakan metode analisis-kualitatif dengan tahapan penelitian yang dilakukan dalam penelitian ini adalah menggunakan metode statik forensik Metode ini digunakan untuk menjelaskan bagaimana tahapan-tahapan penelitian yang akan dilakukan sehingga dapat diketahui alur dan langkah-langkah penelitian secara sistematis kemudian dapat dijadikan pedoman dalam menyelesaikan permasalahan yang terjadi. Dapat dilihat pada gambar 1.



Gambar 1. Alur penelitian

Proses penelitian dimulai dari studi literatur, kemudian dilakukan pengumpulan data. Data tersebut dianalisis dan diuji untuk mendapatkan hasil yang relevan. Hasil pengujian dievaluasi untuk menyimpulkan analisis penelitian. Seluruh alur penelitian tersebut dapat dilihat pada gambar

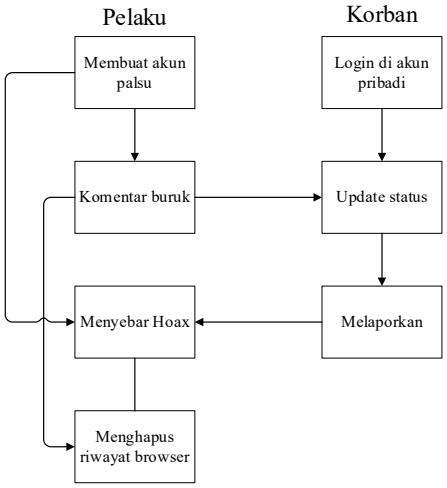
2.2. Persiapan Sistem

Pada saat melakukan penelitian ini Penulis menggunakan beberapa software dan hardware sebagai penunjang penelitian yang akan dilakukan oleh penulis. Untuk spesifikasi alat yang digunakan penelitian adalah sebagai.

- Kebutuhan perangkat keras (hardware):
  - Komputer spesifikasi processor intel i5-7500, memori 8GB, VGA Nvidia 1050 2GB, SSD V-Gen 256GB.
- Kebutuhan perangkat lunak (software):
  - Sistem operasi Windows 10
  - Software FTK Imager
  - Software Autopsy

2.3. Eksperimen

Serangan yang dilakukan adalah ketika korban mengupdate status, foto, maupun video di facebook miliknya, sang pelaku akan mengomentari dengan kata-kata kasar (hatespeech), ejekan, hinaan, dan mengupdate status diakun miliknya memakai foto korban dengan status yang menyudutkan dan mempermalukan korban dengan berita Hoax. Karena merasa sangat terganggu dengan pelaku, korban pun membawa kasus tindakan kejahatan di dunia sosial ini ke Ranah Hukum.



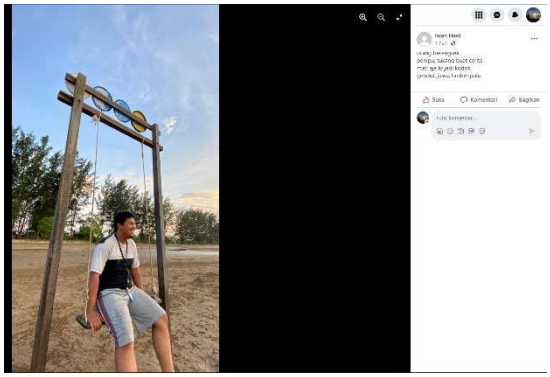
Gambar 2. Alur Eksperimen

Dalam penelitian ini diskenariokan pelaku adalah teman korban yang tidak suka dengannya kemudian membuat akun palsu di media sosial untuk menyerang korban menggunakan Laptop dengan Web Browser Mozilla Firefox. Dan untuk menghilangkan jejaknya pelaku menghapus Riwayat di Browser.

3. Hasil dan Pembahasan

3.1 Pra Akuisisi

Kasus yang menjerat tersangka dengan perangkat personal komputer nya yakni SARA, ujaran kebencian dan bullying. Dan dalam pelaporan dilampirkan hasil screenshot tindak kejahatan yang diperbuat pelaku. Kemudian dikaitkan dengan undang-undang yang berlaku.



Gambar 3. Bukti Digital 1

Pada Pasal 27 ayat (2) UU ITE adalah: Setiap orang yang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras dan antargolongan (SARA) sebagaimana dimaksud dalam pasal 28 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000 (satu milyar rupiah).

Pada Pasal 27 ayat (3) UU ITE adalah: Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik. Ancaman pidana bagi orang yang melanggar diatur dalam pasal 45 ayat (3) UU 19/2016 yang berbunyi: dipidana dengan pidana penjara paling lama 4(empat) tahun dan/atau denda paling banyak Rp750.000.000(tujuh ratus lima puluh juta rupiah).

3.2 Collecting

Setelah adanya laporan dengan kasus UU ITE, investigator melakukan penangkapan dan mengamankan barang bukti yang dicurigai digunakan oleh pelaku untuk melakukan tindakan kejahatan di media sosial facebook tersebut. Didalam kediaman pelaku ditemukan sebuah laptop Acer Aspire E5-411, yang kemudian barang bukti tersebut disita dan dibawa ke laboratorium digital foresik untuk di investigasi.

Gambar 4. Barang Bukti Elektronik

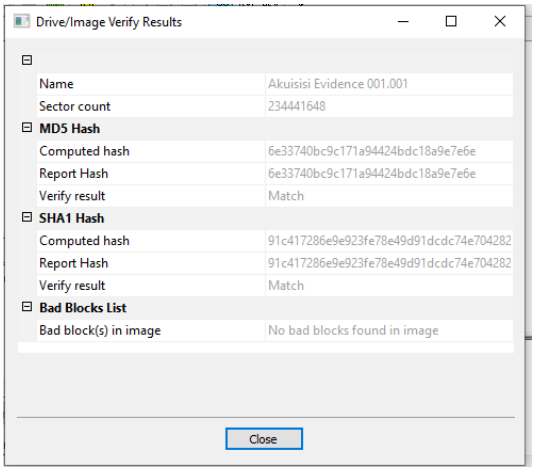
Setalah mendapatkan barang bukti berupa laptop Acer Aspire E5-411, investigator melakukan penelitian konfigurasi dalam perangkat tersebut.

Tabel 1. Detail Spesifikasi Barang Bukti Elektronik

Nama perangkat	Acer Aspire E5-411
Prosesor	Intel Celeron N2830
Layar	14” HD
RAM	8GB DDR3
Sotrage	SSD 120 GB SATA V-Gen
Jaringan	Wifi link 802.11b/g
OS	Windows 10

3.3 Examination

Tahapan ini bisa dilakukan jika persiapan pada akuisisi awal/pra akuisisi sudah lengkap. Pada tahapan ini dilakukan proses Imaging pada barang bukti (pencitraan) agar barang bukti tersebut terjaga keasliannya dan bisa dipertanggungjawabkan. Alat yang digunakan adalah FTK Imager. Setelah proses imaging selesai, FTK akan memberikan laporan dan kode hash MD5 dan SHA 1 dan hasil akuisisinya ditampilkan pada gambar 5.



Gambar 5. Detail Image yang diakuisisi.

3.4 Analyze

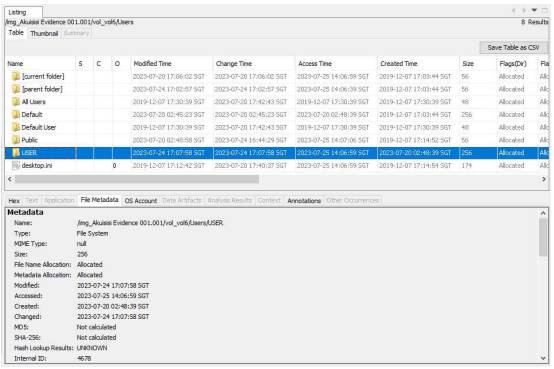
Pada tahap ini, file image yang dihasilkan dengan menggunakan tools Autopsy dalam platform Windows akan dianalisis. Autopsy memiliki berbagai module yang digunakan untuk membagi data yang dibutuhkan saat melakukan analisis. Setelah menentukan module yang dibutuhkan, Autopsy akan menjalankan module tersebut dan masuk ke menu utama untuk melakukan analisis.

Data file image yang sudah terbaca dalam Autopsy akan menjadi data source untuk proses analisis. Data source tersebut terbagi menjadi beberapa komponen data, yaitu berdasarkan jenis file, file yang dihapus, dan file dengan ukuran yang besar.

Data berdasarkan jenis file terbagi menjadi dua tipe, yaitu berdasarkan ekstensi dan berdasarkan MIME type. Data berdasarkan ekstensi berfungsi untuk melihat semua data yang memiliki format seperti gambar, video, audio, dan dokumen. Data berdasarkan MIME type berfungsi untuk melihat data seperti aplikasi, pesan, dan lainnya.

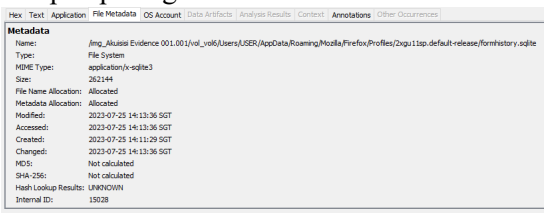
Data berdasarkan file yang dihapus berfungsi untuk melihat data apa saja yang sudah terhapus sebelumnya dalam penyimpanan internal.

Setelah proses validasi selesai, data-data yang telah didapatkan akan muncul di halaman data source dalam Autopsy. Proses validasi data membutuhkan waktu yang cukup lama



Gambar 6. Directory pada tampilan Autopsy

Untuk penelitian sendiri dimulai pada 24 Juli 2023 pada pukul 17.00 WITA untuk 10% data dari keseluruhan dalam barang bukti dan penyimpanan berkapasitas 120 GB pada folder USER. Seperti yang terlihat pada gambar 6, Dalam barang bukti yang ditemukan dalam penelitian ini apapun yang berhubungan dengan kasus yang akan ditangani agar bisa dipertanggungjawabkan dengan kasus yang sedang berjalan. Salah satunya adalah ditemukan jejak email dari sang pelaku didalam perangkat yang dijadikan barang bukti sama persis dengan username nya di akun facebook milik pelaku yang berasal dari moz history yang ditampilkan pada gambar 4.23 dan tampilan metadatanya yang berisikan waktu dan rincian mulai dari nama, type, kode hash dan lain sebagainya pada gambar 4.24. Untuk melakukan steganalisis pada file gambar, hasil sisipan pesan kemudian dianalisis dengan tahapan pada gambar 7.



Gambar 7. Username Pelaku serta informasi metadata

Setelah dilakukannya analisa dari barang bukti yang didapatkan dan didapatkan hasilnya. Tahapan selanjutnya adalah pengelompokkan hasil dari analisa yang didapatkan (result) dan disusun menjadi bukti laporan untuk diserahkan kepengadilan sebagai barang bukti kejahatan yang sudah dilakukan pelaku.

3.5 Result

Pada tahapan ini, hasil dari penelitian berhasil dianalisa ialah berupa data-data yang terkait pada barang bukti. Berikut data yang terkait dalam kasus cybercrime dalam barang bukti yang di analisa, dapat dilihat pada tabel 2.

Tabel 2. Detail Bukti

Kasus Terkait	Lokasi	MIME Type	MD5
Username Pelaku	/img_Akuisisi Evidence 001.001/vol_vol6/Users/USER/AppData/Roaming/Mozilla/Firefox/Profiles/2xgu11sp.default-realese/formhistory.sqlite	Application/ x-sqlite3	d9d32ccf565af92e7465c3075c3fd66d
Cache Bullying dan Hatespeech	/img_Akuisisi Evidence 001.001/vol_vol6/Users/USER/AppData/Local/Mozilla/Firefox/Profiles/2xgu11sp.default-release/cache2/entries/986E3AFA5AD66EB58C498456F970509352D1FEC1	Image/Jpeg	59cff2cb6e02ad3d1253b6901ec0c3dc
	/img_Akuisisi Evidence 001.001/vol_vol6/Users/USER/AppData/Local/Mozilla/Firefox/Profiles/2xgu11sp.default-release/cache2/entries/571A55293EF1FBBC4BFAE8EDC93EF9151DAB8513		b98cffa7b3a56b87771968f79f907eaa
Cache Update Status Hatespeech	/img_Akuisisi Evidence 001.001/vol_vol6/Users/USER/AppData/Local/Mozilla/Firefox/Profiles/2xgu11sp.default-release/cache2/entries/F63362E2EDEC662CC117F2CD8A7F979889E68623	Image/Jpeg	be6e810c8c5cd2f1004c30ad01a7f729

Pada laporan berdasarkan Chain of Custody, korban melaporkan tersangka dengan kasus tindak kejahatan media sosial Facebook pada tanggal 24 Juli 2023 dan kemudian pihak investigator melakukan penangkapan dan mengamankan serta mengumpulkan barang bukti yaitu berupa sebuah Laptop Acer Aspire E5-411 dikediaman pelaku. Kemudian hasil yang ditemukan adalah pelaku terbukti bersalah atas perbuatan tak terpujinya di dunia maya. Untuk itu pelaku terjerat UU no 11 tahun 2008 tentang informasi dan transaksi elektronik (UU ITE) pasal 27 ayat 2 tentang Ujaran Kebencian, pasal 27 ayat 3 tentang kasus Bullying. Dan selanjutnya barang bukti digital pada kasus ini akan diserahkan ke pengadilan untuk ditindak lanjuti dan bisa dipertanggung jawabkan.

4. Kesimpulan

Berdasarkan penelitian dan pembahasan yang dilakukan pada tugas akhir mengenai Analisis Forensik Digital Pada Aplikasi Media Sosial Facebook Menggunakan Metode Statik Forensik dapat disimpulkan bahwa: Dengan menggunakan metode Statik Forensik keaslian data akan terjamin dalam menemukan barang bukti digital serta menemukan file-file yang dihapus oleh tersangka untuk menghilangkan bukti digital tersebut. Setelah barang bukti digital yang didapat dilakukan proses Imaging atau proses pencitraan barang bukti digital menggunakan tools FTK Imager, sehingga tidak terjadi manipulasi data pada barang bukti digital. Analisis barang bukti dilakukan dengan tools Autopsy untuk mencari jejak digital dan data yang sudah dihapus oleh pelaku.

5. Referensi

[1] I. Arpaci And O. Aslan, "Development Of A Scale To Measure Cybercrime-Awareness On Social Media," *Journal Of Computer Information Systems*, Vol. 63, No. 3, Pp. 695–705, May 2023, Doi: 10.1080/08874417.2022.2101160.

[2] E. Tadros, S. Presley, And E. Gomez, "Sharing Experiences And Seeking Connection: Using Facebook As A Form Of Social Support For Incarcerated Loved Ones," *Crime Deling*, P. 001112872211501, Jan. 2023, Doi: 10.1177/00111287221150165.

[3] S. Kemp, D. Buil-Gil, F. Miró-Llinares, And N. Lord, "When Do Businesses Report Cybercrime? Findings From A Uk Study," *Criminology &*

Criminal Justice, Vol. 23, No. 3, Pp. 468–489, Jul. 2023, Doi: 10.1177/17488958211062359.

[4] A. Wijayanto, I. Riadi, And Y. Prayudi, "Taara Method For Processing On The Network Forensics In The Event Of An Arp Spoofing Attack," *Jurnal Resti (Rekayasa Sistem Dan Teknologi Informasi)*, Vol. 7, No. 2, Pp. 208–217, Mar. 2023, Doi: 10.29207/Resti.V7i2.4589.

[5] A. Wijayanto, I. Riadi, Y. Prayudi, And T. Sudinugraha, "Network Forensics Against Address Resolution Protocol Spoofing Attacks Using Trigger, Acquire, Analysis, Report, Action Method," *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, Vol. 8, No. 2, Pp. 156–169, Jul. 2022, Doi: 10.26594/Register.V8i2.2953.

[6] "Secret Communication On Facebook Using Image Steganography: Experimental Study." [Online]. Available: Https://Sites.Google.Com/Site/Ijcsis/

[7] D. Darwis, "Implementasi Teknik Steganografi Least Significant Bit (Lsb) Dan Kompresi Untuk Pengamanan Data Pengiriman Surat Elektronik," *Jurnal Teknoinfo*, Vol. 10, No. 2, Pp. 1–7, 2016.

[8] K. Khairunnisak And W. Widodo, "Digital Forensic Tools And Techniques For Handling Digital Evidence," *Jurnal Resistor (Rekayasa Sistem Komputer)*, Vol. 6, No. 1, Pp. 1–11, Apr. 2023, Doi: 10.31598/Jurnalresistor.V6i1.1266.

[9] B. Pribadi, S. Rosdiana, And S. Arifin, "Digital Forensics On Facebook Messenger Application In An Android Smartphone Based On Nist Sp 800-101 R1 To Reveal Digital Crime Cases," *Procedia Comput Sci*, Vol. 216, Pp. 161–167, 2023, Doi: 10.1016/J.Procs.2022.12.123.

[10] 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 Journal Of Information System And Technology (Jst)*, Vol. 2, No. 2, Pp. 2829–808, 2023, Doi: 10.56134/Jst.V2i2.45.

[11] D. Angus, A. Bruns, E. Hurcombe, S. Harrington, And X. Y. (Jane) Tan, "Computational Communication Methods For Examining Problematic News-Sharing Practices On Facebook At Scale," *Soc Media Soc*, Vol. 9, No. 3, Jul. 2023, Doi: 10.1177/20563051231196880.