E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 03 Nomor 02 September 2025

Analisis dan Pencarian Bukti Forensik Digital pada Aplikasi Media Sosial X Menggunakan Metode Static Forensic

[1]Destyfaini Dwi Putri.P, [2]Udin Sidik Sidin, [3*]Muhammad Fajar B

[1,2,3]Universitas Negeri Makassar, Indonesia

Email: destyfainidwiputri@gmail.com[1], udin.sidik.sidin@unm.ac.id[2], fajarb@unm.ac.id[3]

Received : 13 Juli 2025
Accepted : 11 Agustus 2024
Published : 2 September 2025

ABSTRAK

Penelitian ini membahas penerapan metode statik forensik digital untuk menganalisis bukti tindak kejahatan siber pada aplikasi media sosial X. Studi ini disusun berdasarkan simulasi kasus pelanggaran Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), khususnya terkait penyebaran konten pornografi, ujaran kebencian, cyberbullying, dan penyebaran hoaks. Penelitian dilakukan dengan menyita perangkat bukti berupa laptop dan flashdisk milik pelaku, yang kemudian dianalisis menggunakan perangkat lunak FTK Imager dan Autopsy. Proses akuisisi bukti dilakukan dengan FTK Imager untuk membuat salinan image digital dan menjaga integritas data melalui verifikasi hash MD5 dan SHA-1. Selanjutnya, analisis dilakukan dengan Autopsy untuk mengidentifikasi file tersembunyi, file yang telah dihapus, struktur file sistem, dan metadata penting. Hasil investigasi menemukan sejumlah bukti digital seperti konten visual ilegal, riwayat penggunaan media sosial, file SQLite, artefak email, dan data aktivitas pelaku yang berkaitan langsung dengan akun X yang digunakan. Temuan ini menunjukkan bahwa metode statik forensik efektif digunakan dalam investigasi digital tanpa mengubah data asli. Selain itu, kedua perangkat lunak forensik yang digunakan terbukti mampu mendukung proses identifikasi, ekstraksi, dan pengolahan bukti digital secara sistematis dan akurat. Penelitian ini memberikan kontribusi terhadap praktik penegakan hukum digital, khususnya dalam proses pembuktian kasus kejahatan siber berbasis media sosial.

Kata kunci : *forensik digital, statik forensik, media sosial X , FTK imager, autopsy*

ABSTRACT

This study discusses the application of static digital forensic methods to analyze evidence of cybercrime on the social media platform X. The research is based on a simulated case involving violations of Indonesia's Electronic Information and Transactions Law (UU ITE), specifically concerning the distribution of pornographic content, hate speech, cyberbullying, and the spread of hoax X. The investigation was conducted by seizing the suspect's devices, including a laptop and a 15GB flash drive, which were then xamined using FTK Imager and Autopsy forensic tools. The acquisition process was carried out using FTK Imager to create a digital image while maintaining data integrity through MD5 and SHA-1 hash verification. The subsequent analysis was conducted using Autopsy to identify hidden files, deleted files, file system structures, and relevant metadata. The investigation uncovered various types of digital evidence such as illicit images, social media activity logs, SQLite database files, email artifacts, and user activity data directly linked to the suspect's X account. The findings indicate that static forensic methods are effective in preserving original data during investigation. Furthermore, the forensic tools used in this study proved capable of systematically identifying, extracting, and processing digital evidence accurately. This research contributes to the field of cybercrime law enforcement, particularly in supporting the process of proving digital-based crimes committed through social media platforms.

Key words: *digital forensics, static forensics, social media X, FTK imager, autopsy.*

E-ISSN: 2986-7258
P-ISSN : 2986-724X
PISCES Volume 03 Nomor 02 September 2025

1. PENDAHULUAN

Seiring dengan perkembangan teknologi informasi, penggunaan media sosial semakin meluas dan menjadi bagian integral dari kehidupan sehari-hari masyarakat modern. Media sosial saat ini hanya dimanfaatkan untuk berkomunikasi, tetapi juga menjadi sarana untuk berbagi informasi, pengalaman pribadi, serta membentuk koneksi dan interaksi dalam jejaring sosial. Menurut laporan dari Radio Rakyat Indonesia pada tahun 2024, jumlah pengguna media sosial di Indonesia mencapai 139 juta, yang setara dengan 49,9% dari total populasi. Jumlah pengguna aktif media sosial di Indonesia terus mengalami peningkatan, dengan trend penggunaan yang menunjukkan pertumbuhan yang signifikan. Jumlah pengguna aktif media sosial terus meningkat, menunjukkan pergeseran perilaku sosial di masyarakat menuju dunia digital yang lebih terhubung (Panggabean, 2024).

Namun, di balik popularitas media sosial, terdapat berbagai risiko yang signifikan. Media sosial sering kali menjadi sasaran tindak kejahatan siber, seperti pencurian identitas, penipuan, perundungan siber, dan penyebaran informasi palsu. Fenomena ini berdampak negatif tidak hanya bagi individu yang menjadi korban tetapi juga bagi masyarakat secara umum. Data pribadi dan informasi sensitif yang sering dibagikan oleh pengguna di platform ini membuka celah bagi pelaku kejahatan untuk memanfaatkannya demi kepentingan mereka (Dewi, 2024).

Pada awal Januari 2023, terungkap bahwa sekitar 235 juta informasi pengguna X telah terekspos di forum hacker online, menjadikannya salah satu pelanggaran data terbesar yang pernah dialami oleh platform media sosial tersebut. Data yang bocor mencakup informasi sensitif seperti username, alamat email, screen name, jumlah pengikut, tanggal pembuatan akun, dan nomor telepon pengguna. Perusahaan keamanan siber asal Israel, Hudson Rock, melaporkan bahwa data yang bocor bersifat unik dan dapat digunakan untuk berbagai tindakan kejahatan siber, termasuk peretasan, phishing, dan doxing, yaitu tindakan mengungkapkan informasi pribadi seseorang secara online. Database yang terekspos memiliki ukuran sekitar 63GB, dan kebocoran ini diduga dilakukan oleh kelompok yang sebelumnya telah menjual informasi milik 400 juta pengguna X pada bulan Desember 2022 dengan harga mencapai USD 200.000. Kebocoran data ini menimbulkan kekhawatiran besar mengenai keamanan informasi pribadi pengguna X, karena dengan informasi yang terekspos, pengguna berisiko tinggi menjadi target serangan siber yang lebih lanjut. Kasus ini menunjukkan perlunya peningkatan langkah-langkah keamanan dan perlindungan data di platform media sosial, serta dapat digunakan sebagai studi kasus dalam analisis isu-isu terkait keamanan data, privasi pengguna, dan dampak dari kebocoran data di media sosial(Wardani, 2023).

Dari kasus-kasus di atas, forensik digital muncul sebagai bidang penting dalam mendukung penegakan hukum dan melindungi individu dari kejahatan siber. Forensik digital memungkinkan penyelidik untuk melakukan analisis dan pencarian bukti yang diperlukan guna mengungkap jejak pelaku dan memahami modus operandi mereka. Ada 2 jenis digital forensik berdasarkan bukti digital yaitu forensik statis dan forensik langsung (Syahputri, 2022).

Forensik statis adalah metode analisis bukti digital yang dilakukan pada perangkat yang tidak dihidupkan, di mana bukti digital seperti file gambar dan video diambil dari media penyimpanan menggunakan teknik pemindaian bit-by-bit. Proses ini memastikan bahwa data asli tetap utuh dan tidak terpengaruh, dengan langkah-langkah seperti penggunaan write blocker dan disk imaging untuk menjaga integritas bukti. Setelah salinan identik dibuat, analisis dapat dilakukan di laboratorium tanpa risiko merusak bukti asli, yang sangat penting dalam konteks hukum di mana bukti yang terkontaminasi tidak dapat diterima di pengadilan. Di sisi lain, forensik langsung dilakukan saat perangkat masih aktif, memungkinkan investigator untuk mengumpulkan data yang mencerminkan aktivitas perangkat secara real-time, termasuk informasi tentang enkripsi data. Meskipun forensik langsung sering digunakan dalam konteks jaringan komputer, mengoperasikan perangkat dapat mengubah data asli, sehingga investigator harus berhati-hati untuk memastikan bahwa data yang dikumpulkan tetap valid. Jika ada tanda-tanda enkripsi, investigator perlu membuat gambar logis dari hard drive untuk analisis lebih lanjut, dan keberhasilan investigasi digital sangat bergantung pada lokasi dan metode pengumpulan bukti yang tepat (Caesar dkk., 2024).

Pendekatan yang digunakan adalah metode statik forensik, Metode ini menjaga integritas bukti dengan tidak menghidupkan perangkat, sehingga risiko mengubah data asli diminimalkan, yang krusial untuk penerimaan bukti di pengadilan. Selain itu, forensik statis memungkinkan analisis mendalam dan pemulihan data yang telah dihapus, meningkatkan peluang menemukan bukti relevan. Keamanan proses terjamin melalui penggunaan write blocker dan disk imaging, memastikan salinan identik dengan data asli. Metode ini juga

fleksibel dan dapat diterapkan pada berbagai perangkat, serta memungkinkan eksplorasi teknik sistematis dalam pengumpulan dan analisis bukti digital. Dengan pertimbangan ini, forensik statis menjadi pilihan yang tepat untuk penelitian ini (Caesar dkk., 2024).

Pada aplikasi media sosial seperti X metode statik forensik dapat digunakan untuk menganalisis data yang tidak berubah, seperti rekaman interaksi, file multimedia, dan metadata. Melalui metode ini, peneliti dapat mengidentifikasi bukti digital seperti pesan pribadi, gambar, atau video yang relevan dalam suatu kasus kejahatan. Selain itu, metode ini juga memungkinkan pemulihan data yang telah dihapus, memberikan peluang lebih besar untuk mengungkap informasi tersembunyi (Caesar dkk., 2024).

Berdasarkan penelitian lain yaitu penelitian dengan judul Analisis Forensik Digital pada Aplikasi Media Facebook Menggunakan Metode Statik Forensik dari Caesar dkk. (2024), analisis terhadap penelitian yang ada, terdapat beberapa research gap yang dapat diidentifikasi untuk skripsi dengan judul "Analisis dan pencarian bukti forensik digital pada aplikasi media sosial X menggunakan metode statik forensik. Pertama, penelitian yang telah dilakukan sering kali terfokus pada satu atau dua platform media sosial, seperti Facebook, Instagram, dan TikTok, tanpa mengeksplorasi aplikasi media sosial X secara mendalam. Hal ini menciptakan kebutuhan untuk melakukan analisis forensik yang lebih spesifik pada aplikasi media sosial X, yang mungkin memiliki karakteristik dan jenis data yang berbeda. Selain itu, meskipun metode statik forensik telah diterapkan dalam berbagai konteks, penerapannya dalam konteks lokal di Indonesia masih terbatas. Penelitian yang ada lebih sering menggunakan metode umum tanpa merujuk pada pedoman spesifik yang relevan dengan konteks lokal, sehingga penelitian ini akan berfokus pada penerapan metode statik forensik dalam konteks aplikasi media sosial X. Selanjutnya, analisis metadata yang dihasilkan dari interaksi pengguna di media sosial sering kali kurang diperhatikan dalam penelitian sebelumnya.

Metadata dapat memberikan informasi penting mengenai waktu, lokasi, dan konteks interaksi, sehingga penelitian ini akan mengeksplorasi bagaimana analisis metadata dapat digunakan untuk mendukung pencarian bukti forensik di aplikasi media sosial X. Selain itu, banyak penelitian yang tidak membahas teknik pemulihan data yang telah dihapus dari aplikasi media sosial, padahal metode statik forensik memiliki potensi untuk memulihkan data yang hilang. Penelitian ini akan mengeksplorasi teknik-teknik yang dapat digunakan untuk mengakses informasi yang mungkin tersembunyi di aplikasi media sosial X.

Konteks hukum dan kebijakan yang berbeda di Indonesia juga sering kali tidak dipertimbangkan dalam penelitian yang ada, sehingga penelitian ini bertujuan untuk mengisi gap tersebut dengan mengeksplorasi proses analisis dan pencarian bukti forensik digital di aplikasi media sosial X dalam konteks hukum dan kebijakan yang berlaku. Terakhir, penelitian yang ada sering kali tidak membahas secara mendalam tentang penggunaan smartphone sebagai alat utama untuk mengakses media sosial. Oleh karena itu, penelitian ini akan berfokus pada teknik pengumpulan data forensik dari smartphone yang digunakan untuk mengakses aplikasi media sosial X, serta tantangan yang mungkin dihadapi dalam proses tersebut. Dengan mengidentifikasi gap-gaps ini, penelitian ini diharapkan dapat memberikan kontribusi signifikan terhadap pengembangan ilmu forensik digital di Indonesia dan menciptakan platform yang lebih aman dan dapat dipertanggungjawabkan dalam penggunaan media sosial.

Berdasarkan penelitian yang dilakukan oleh Gunawan & Grasia. (2023) mengenai analisis digital forensik aplikasi pelacak nomor handphone Android, terdapat beberapa gap penelitian yang dapat diidentifikasi untuk skripsi dengan judul "Analisis dan Pencarian Bukti Forensik Digital pada Aplikasi Media Sosial X Menggunakan Metode Statik Forensik". Pertama, penelitian ini terutama berfokus pada aplikasi pelacak nomor telepon seperti GetContact, Truecaller, dan sejenisnya, tanpa melakukan eksplorasi terhadap aplikasi media social X. Kondisi ini menimbulkan kebutuhan untuk anlisis forensik yang berfokus pada aplikasi media social, yang mungkin memiliki karakteristik dan jenis data yang berbeda. Kedua, meskipun penelitian ini mengadopsi metode statis dan dinamis, belum ada penjelasan mendalam mengenai penerapan metode statik forensik secara efektif pada aplikasi media social X.

Penelitian ini akan berfokus pada penerapan metode statik forensik untuk mengumpulkan dan menganalisis data dari aplikasi media sosial X. Selain itu, penelitian ini tidak membahas analisis metadata yang dihasilkan dari interaksi pengguna di aplikasi pelacak nomor. Metadata dapat memberikan informasi penting mengenai waktu, lokasi, dan konteks interaksi, sehingga penelitian ini akan mengeksplorasi bagaimana analisis metadata dapat digunakan untuk mendukung pencarian bukti forensik di aplikasi media sosial X . Terakhir, penelitian ini tidak memperhitungkan konteks hukum dan kebijakan yang berbeda di Indonesia. Oleh Karena itu, penelitian

ini bertujuan untuk mengisi kekurangan tersebut dengan mengksplorasi proses analisis dan pencarian bukti forensik digital di aplikasi media social X dalam kerangka hukum dan kebijakan yang berlaku.

Dari beberapa penelitian yang telah disebutkan, terdapat beberapa kelemahan yang menjadi dasar untuk mengusulkan penggunaan metode statik forensik dalam analisis dan pencarian bukti forensik di aplikasi media sosial X . Pertama, sejumlah penelitian sebelumnya, seperti yang dilakukan oleh Putra et al. (2024) dan Gunawan & Grasia (2023), lebih menitikberatkan pada aplikasi tertentu seperti Instagram, TikTok, dan aplikasi pelacak telepon. Penelitian-penelitian ini tidak melakukan analisis mendalam terhadap aplikasi media social X , sehingga menimbulkan kebutuhan untuk anlisis forensik yang lebih berfokus pada aplikasi tersebut. Hal ini menunjukkan bahwa pendekatan yang ada tidak cukup komprehensif untuk menangani variasi dalam jenis data dan interaksi pengguna yang mungkin ada di aplikasi media sosial X .

Kedua, meskipun metode forensik statis telah diterapkan dalam berbagai konteks, penelitian sebelumnya tidak mengkaji tantangan spesifik yang mungkin muncul saat metode ini diterapkan pada aplikasi media sosial X. Kelemahan ini menunjukkan kurangnya pemahaman tentang bagaimana metode ini dapat disesuaikan dengan konteks yang berbeda. Oleh karena itu, penelitian ini akan berfokus pada penerapan metode forensik statis untuk mengumpulkan dan menganalisis data dari aplikasi media sosial X, dengan harapan dapat mengidentifikasi dan mengatasi tantangan yang mungkin timbul.

Selanjutnya, analisis metadata yang dihasilkan dari interaksi pengguna di media sosial sering kali kurang diperhatikan dalam penelitian sebelumnya. Metadata dapat memberikan informasi penting mengenai waktu, lokasi, dan konteks interaksi, yang sangat relevan dalam penyelidikan forensik. Kelemahan ini menunjukkan bahwa pendekatan yang ada tidak sepenuhnya memanfaatkan potensi informasi yang dapat diperoleh dari metadata. Penelitian ini mengkaji bagaimaan anlisis metadata dapat dimanfaatkan untuk mendukung pencarian bukti forensik di aplikasi media social X , sehingga dapat memberikan pemahaman yang lebih komprehensif mengenai interaksi pengguna.

Dalam hal kelebihan dan kekurangan pendekatan forensik digital, penerapan metode seperti forensik statis menawarkan kerangka kerja yang jelas dan terstandarisasi untuk analisis forensik, yang dapat meningkatkan keandalan hasil. Metode forensik statis juga memiliki kemampuan untuk mengembalikan data yang telah dihapus, yang sangat krusial dalam konteks penyelidikan kejahatan siber. Selain itu, pendekatan ini memungkinkan analisis metadata yang dapat memberikan informasi krusial mengenai konteks internal pengguna, yang dapat memperkuat bukti yang ditemukan. Namun, terdapat keterbatasan dalam aplikasi spesifik, di mana banyak penelitian tidak membahas aplikasi media sosial tertentu secara mendalam, yang dapat mengurangi relevansi hasil untuk aplikasi media sosial X. Tantangan dalam implementasi juga muncul, karena penerapan metode forensik dalam konteks lokal, seperti di Indonesia, sering kali tidak mempertimbangkan kebijakan dan hukum yang berlaku, yang dapat mempengaruhi hasil. Selain itu, beberapa alat forensik mungkin tidak dapat mengakses semua jenis data atau mungkin memiliki tingkat akurasi yang bervariasi, yang dapat mempengaruhi hasil analisis. Dengan mengidentifikasi gap ini, penelitian ini diharapkan dapat memberikan kontribusi signifikan terhadap pengembangan ilmu forensik digital di Indonesia, khususnya dalam konteks aplikasi media sosial X, serta memberikan wawasan baru tentang pengumpulan dan analisis data forensik pada platform tersebut.

Konteks di Indonesia menunjukkan bahwa meskipun kesadaran akan keamanan siber semakin berkembang, masih terdapat banyak yang harus dihadapi. Penegakan hukum terhadap kejahatan siber seringkali terhambat oleh kurangnya pemahaman dan keterampilan teknis dalam melakukan analisis forensik digital. Hal ini menjadi hambatan signifikan dalam mengungkap dan menangani kasus-kasus kejahatan siber yang semakin kompleks.

Penelitian ini bertujuan untuk mengeksplorasi dan memahami proses analisis serta pencarian bukti forensik digital pada aplikasi media sosial X menggunakan metode statik forensik. Melalui penelitian ini, diharapkan dapat memberikan kontribusi signifikan bagi pengembangan ilmu forensik digital di Indonesia serta memberikan pedoman yang berguna bagi aparat penegak hukum dan praktisi dalam melakukan penyelidikan lebih efektif. Selain itu, penelitian ini juga bertujuan untuk menciptakan kesadaran yang lebih tinggi tentang pentingnya keamanan digital, sehingga masyarakat dapat menggunakan media sosial secara lebih aman dan bertanggung jawab.

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 03 Nomor 02 September 2025

2. METODE PENELITIAN

2. 1 . Jenis Penelitian

Penelitian ini menggunakan metode eksperimental, yaitu pendekatan yang bertujuan menguji hubungan sebab-akibat antarvariabel dengan cara memanipulasi satu variabel dan mengendalikan variabel lain, sehingga perubahan yang terjadi dapat dipastikan berasal dari variabel yang diteliti.

2. 2 Tempat dan Waktu Penelitian

Penelitian ini dilaksanakan secara online dengan memanfaatkan alat bantu forensik digital yang mendukung proses analisis dan pemulihan data dari jarak jauh. Waktu pelaksanaan penelitian tergolong efisien dan dapat diselesaikan dalam waktu singkat, bergantung pada tingkat kesulitan dan kompleksitas kasus yang dianalisis.

2. 3 Hardware dan Software

Pada penelitian ini menggunakan alat dan bahan yang terdiri dari hardware dan software. Adapun rinciannya sebagai berikut:

Kebutuhan perangkat keras.

a. Laptop Dell Processor intel Core i5, Memori 4 GB

b. Sistem operasi Windows 10.

Kebutuhan perangkat lunak.

a. Software FTK Imager (untuk Imaging barang bukti).

b. Software Autopsy

2. 4 Tahapan Penelitian

Penelitian ini menggunakan metode statik forensik dengan pendekatan studi kasus post-incident pada perangkat digital yang digunakan untuk mengakses media sosial X, seperti smartphone, laptop, dan penyimpanan eksternal. Tujuan utama adalah mengekstrak data yang dihapus atau tersembunyi agar dapat dijadikan bukti hukum. Metode statik dipilih karena mampu menganalisis data tanpa mengubah data asli, sehingga menjaga integritas bukti. Proses penelitian dilakukan menggunakan aplikasi forensik digital seperti FTK Imager dan Autopsy untuk mengidentifikasi pesan, gambar, video, maupun log aktivitas pelaku.

a. Pengumpulan Data (Acquisition)

Langkah pertama dalam penelitian ini adalah pengumpulan data. Peneliti mengambil data dari perangkat digital yang digunakan untuk mengakses aplikasi media sosial X, seperti smartphone atau laptop. Untuk memastikan bahwa data tidak mengalami perubahan selama proses pengambilan. Alat ini mencegah penulisan atau modifikasi data pada perangkat penyimpanan. Selanjutnya, peneliti membuat image (salinan bit-by-bit) dari penyimpanan perangkat. Image ini merupakan salinan lengkap dari data asli yang akan digunakan untuk analisis lebih lanjut, sehingga data asli tetap terjaga keutuhannya.

b. Pemeriksaan (Examination)

Setelah data berhasil dikumpulkan, dilakukan proses penyaringan untuk memilah dan membatasi data pada bagian-bagian tertentu yang relevan dari keseluruhan sumber untuk menentukan data mana yang akan dianalisis lebih lanjut.

c. Analisis Data (Analysis)

Langkah ketiga adalah analisis data. Pada tahap ini, peneliti mengekstrak metadata dari data yang dikumpulkan, seperti waktu pengiriman, ID pengguna, dan lokasi. Metadata ini dapat memberikan informasi penting tentang konteks dan asal-usul data. Selain itu, peneliti mencari bukti digital yang relevan dengan kasus, seperti pesan teks, gambar, video, atau log aktivitas. Untuk melakukan analisis ini, peneliti menggunakan alat forensik digital seperti Autopsy atau FTK Imager. Alat-alat ini membantu peneliti mengidentifikasi dan memeriksa data yang mungkin telah dihapus atau disembunyikan oleh pelaku.

d. Presentasi (Presentation)

Langkah terakhir adalah penyajian hasil. Peneliti menyusun temuan penelitian dalam bentuk laporan tertulis yang lengkap dan terstruktur. Laporan ini mencakup latar belakang penelitian, metode yang digunakan, hasil analisis, dan kesimpulan. Selain itu, peneliti menyajikan bukti digital dalam format yang sesuai dengan persyaratan hukum, seperti metadata, pesan teks, atau gambar yang relevan dengan kasus. Penyajian hasil ini bertujuan untuk memudahkan pihak berwenang atau pengadilan dalam memahami temuan penelitian dan menggunakan bukti digital untuk proses hukum.

Gambar 3.1 Tahapan Penelitian

2. 5 Teknik dan Prosedur Pengumpulan Data

Teknik dan prosedur pengumpulan data pada skripsi "Analisis dan Pencarian Bukti Forensik Digital pada Aplikasi Media Sosial X Menggunakan Metode Statik Forensik" dimulai dengan persiapan alat dan lingkungan yang memadai. Perangkat lunak forensik seperti Autopsy, FTK Imager, atau Magnet AXIOM disiapkan untuk melakukan analisis statik, sementara perangkat smartphone yang digunakan untuk mengakses aplikasi media sosial Xdipersiapkan sebagai objek penelitian. Lingkungan pengumpulan data harus aman dan terkontrol untuk menjaga integritas data. Selanjutnya, dilakukan pembuatan salinan (image) dari memori perangkat menggunakan teknik bit-by-bit imaging atau logical imaging untuk memastikan data asli tidak terubah. Data yang diekstrak mencakup chat, gambar, video, metadata, dan log aktivitas dari aplikasi media sosial X , termasuk data yang mungkin tersembunyi atau terhapus di cache atau database aplikasi.

Setelah data berhasil dikumpulkan, tahap analisis data statik dilakukan dengan mengidentifikasi jenis data yang relevan, seperti pesan, konten multimedia, dan metadata. Analisis metadata menjadi fokus penting untuk mendapatkan informasi mengenai waktu, lokasi, dan konteks interaksi pengguna. Selain itu, teknik pemulihan data diterapkan untuk mencari informasi yang mungkin telah dihapus. Seluruh proses pengumpulan dan analisis data didokumentasikan secara rinci untuk memastikan transparansi dan keandalan, yang kemudian diolah menjadi laporan forensik yang mencakup temuan, metode, dan kesimpulan. Prosedur ini juga mempertimbangkan konteks hukum dan kebijakan di Indonesia, seperti UU ITE dan perlindungan privasi, untuk memastikan bahwa pengumpulan data dilakukan secara legal dan etis. Dengan mengikuti langkah-langkah ini, penelitian ini diharapkan dapat menghasilkan bukti forensik digital yang valid dan relevan untuk aplikasi media sosial X.

Teknik Analisis Data

Dalam penelitian investigasi forensik, teknik analisis data yang digunakan meliputi beberapa metode.

1. Pengumpulan Data

Teknik ini melibatkan pengumpulan data dari aplikasi media sosial X menggunakan metode statik forensik. Data yang dikumpulkan dapat mencakup file log, metadata, dan konten yang tersimpan di perangkat pengguna. Penggunaan alat forensik digital yang sesuai untuk mengekstrak data tanpa mengubah atau merusak bukti sangat penting dalam tahap ini.

2. Analisis Metadata

Setelah data dikumpulkan, analisis metadata dilakukan untuk mendapatkan informasi penting mengenai interaksi pengguna, seperti waktu, lokasi, dan jenis aktivitas. Metadata dapat memberikan konteks tambahan yang membantu dalam memahami pola perilaku pengguna dan relevansi data yang ditemukan dalam penyelidikan.

3. Pemulihan Data yang Dihapus

Teknik ini berfokus pada pemulihan data yang terhapus dari aplikasi media sosial X. Melalui metode statik forensik, peneliti dapat mengakses informasi tersembunyi sehingga cakupan bukti yang dianalisis menjadi lebih luas.

3. HASIL DAN PEMBAHASAN

Dalam simulasi kasus, akun X @thersangkah berperan sebagai pelaku yang mengomentari unggahan korban (@chorbaneee) dengan perkataan tidak menyenangkan, menyebarkan berita hoax, dan konten pornografi di profilnya. Korban melaporkan pelaku berdasarkan UU ITE. Pelaku berusaha menghapus jejak digitalnya dengan menghapus riwayat browser.

3. 1 Pengumpulan Data *(Acquisition)*

a. Mencari Barang Bukti

Dalam penanganan kasus UU ITE, penyidik menangkap tersangka dan menyita barang bukti berupa laptop Dell serta flashdisk 15 GB yang digunakan untuk mengakses platform X. Seluruh barang bukti kemudian dibawa ke laboratorium forensik digital untuk dianalisis lebih lanjut.

b. Kasus Terkait Perangkat

Kasus ini melibatkan tersangka yang menggunakan komputer pribadinya untuk menyebarkan hoaks, konten pornografi, ujaran kebencian, dan melakukan bullying. Bukti berupa tangkapan layar menunjukkan tindakannya, yang kemudian dikaitkan dengan UU ITE.

Berdasarkan UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016, pelanggaran yang relevan meliputi:

- Pasal 27 ayat (1): distribusi konten melanggar kesusilaan, ancaman pidana 6 tahun dan/atau denda Rp1 miliar.
- Pasal 27 ayat (2): penyebaran informasi bermuatan SARA, ancaman pidana 6 tahun dan/atau denda Rp1 miliar.
- Pasal 27 ayat (3): pencemaran nama baik, ancaman pidana 4 tahun dan/atau denda Rp750 juta.
- Pasal 28: penyebaran informasi bohong yang merugikan konsumen, ancaman pidana 6 tahun dan/atau denda Rp1 miliar.

c. Konfigurasi Peran kat

Setelah barang bukti berupa perangkat laptop Dell disita, penyidik melakukan analisis terhadap konfigurasi yang terdapat dalam perangkat tersebut.

Tabel 1 Konfigurasi Perangkat

Nama Perangkat	DESKTOP-SHIIEUJ
Prosesor	Intel(R) Core(TM) i7-4600U CPU @ 2.10GHz 2.70 GHz
Layar	14''
RAM	8.00 GB
Hardisk	500GB
Jaringan	Wi-Fi
OS	Windows 10

d. Chain of Custody

Dalam proses penyidikan, langkah-langkah harus dilakukan sesuai dengan surat perintah yang berlaku dan mengikuti prosedur yang ditetapkan dalam rantai bukti (chain of study). Hal ini mencakup pengumpulan barang bukti yang diduga terlibat dalam kasus tersebut. Selanjutnya, dokumentasi harus dilakukan secara menyeluruh mulai dari tahap penangkapan hingga laporan bukti, yang juga harus dilengkapi dengan keterangan dari korban.

Tabel 2 Chain of Custody

INFORMASI KASUS			
No. Kasus	001/001		
NamaKasus	Tindak kejahatan media social X		
TanggalKasus	1 April 2025		
PENANGGUNG JAWAB			
Nama	Fani	Alamat:	Batua, Makassar
Instansi	UIR	No. Telp:	082235903108
Jabatan	Investigator	Email:	fani21@gmail.com
PENGUMPULAN BARANG BUKTI			
Tanggal Penyitaan	15 April 2025		
Waktu Penyitaan	03.15 di kediamannya		
Lokasi Penyitaan	Kediaman Pelaku komplek Bunga		
DESKRIPSI KASUS			
Telah terjadi insiden Cybercrime di media social X yang melibarkan korban bernama "chorbaneee" dan seorang Pelaku yang disebut "thersangka" dalam kasus Cyberbulluing, HateSpeech, Hoax dan konten bersifat pornografi.			

3. 2 Pemeriksaan

Bukti Barang bukti berupa laptop Dell dan flashdisk 15GB disita. Kasus yang terkait meliputi penyebaran hoax, konten pornografi (Pasal 27 ayat 1 UU ITE), ujaran kebencian (Pasal 27 ayat 2 UU ITE), dan bullying (Pasal 27 ayat 3 UU ITE). Konfigurasi perangkat pelaku dicatat. Chain of Custody didokumentasikan secara lengkap. Proses pencitraan barang bukti dilakukan menggunakan FTK Imager. USB flashdisk di-imaging dengan memilih "Physical Drive" dan format "Raw DD". Opsi "Verify image after they are created" dicentang untuk memastikan integritas data melalui perhitungan hash MD5 dan SHA-1.

a. Proses pencitraan Barang Bukti Menggunakan FTK Imager

Setelah persiapan selesai, barang bukti digital kemudian dia kuisisi melalui proses imaging menggunakan aplikasi FTK Imager. Proses pencitraan dilakukan pada media penyimpanan eksternal (flashdisk 15 GB) dengan memilih opsi Create Disk Image → Physical Drive. Hasil pencitraan disimpan dalam format Raw DD, dengan opsi verifikasi (Verify image after they are created) untuk memastikan integritas data melalui pencocokan kode hash MD5 dan SHA-1. FTK Imager menghasilkan salinan bit-per-bit yang lengkap beserta file log hash, sehingga keaslian bukti digital dapat dipertanggungjawabkan secara hukum.

3. 3 Analisis Data Mengunakan Aplikasi Autopsy

Setelah proses akuisisi selesai, file image dianalisis menggunakan Autopsy pada platform Windows. Tahap awal meliputi pengisian Case Information dan Additional Information untuk mendokumentasikan identitas kasus serta investigator. Selanjutnya, file image hasil akuisisi dimuat sebagai data source dengan memilih opsi

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 03 Nomor 02 September 2025

Disk Image or VM File, kemudian diproses menggunakan Ingest Modules agar data dapat dipindai dan diekstrak secara sistematis.

Autopsy secara otomatis menyusun data dalam beberapa kategori, seperti file type, deleted files, dan MIME type, sehingga memudahkan penelusuran artefak digital. Proses ini memungkinkan identifikasi file terhapus, metadata, serta aktivitas pengguna. Dalam penelitian ini, ditemukan 17.679 file dari media penyimpanan 15 GB. Bukti digital yang berhasil diekstrak antara lain:

1. Jejak email pelaku, sesuai dengan username akun X.
2. URL aktivitas media sosial beserta metadatanya.
3. Foto pornografi yang disebarkan melalui akun X milik pelaku.
4. Foto korban dengan komentar bernuansa ujaran kebencian.
5. Status X korban yang dikomentari pelaku dengan kata-kata kasar.

Bukti-bukti tersebut memperkuat keterlibatan pelaku dalam kasus penyebaran konten pornografi, ujaran kebencian, serta pencemaran nama baik di media sosial X.

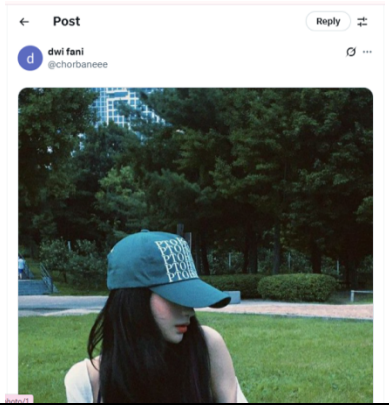
3. 4 Temuan Bukti

Digital Analisis terhadap 10% data dari flashdisk 15GB (17.679 file) berhasil mengungkap bukti-bukti berikut:

- Konten Pornografi: Ditemukan file gambar JPEG yang disebarluaskan pelaku di akun X-nya.
- Ujaran Kebencian: Ditemukan foto korban yang dikomentari pelaku dengan kata-kata tidak pantas.
- Cyberbullying: Ditemukan status X korban yang dikomentari oleh pelaku dengan kata-kata kasar dan merendahkan, serta histori browser yang menyertakan kata-kata kasar.
- Hoax: Terdeteksi dari log aktivitas dan metadata URL yang dianalisis.
- Jejak Email dan Aktivitas Browser: Ditemukan jejak email pelaku yang sama dengan username akun X-nya, serta URL aktivitas media sosial.
- Deleted Files: Berhasil dipulihkan dari unallocated space.

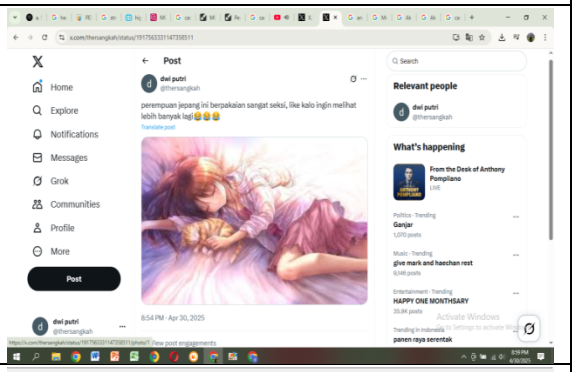
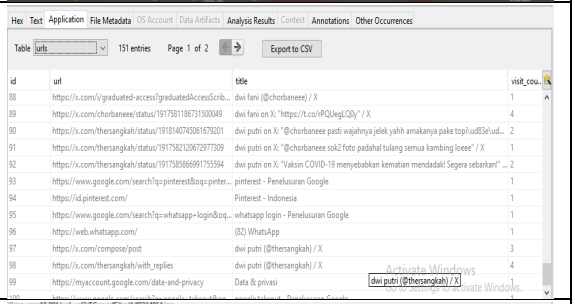
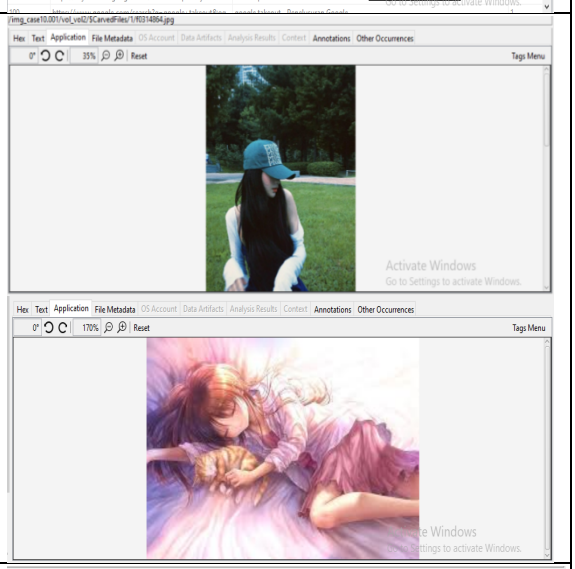
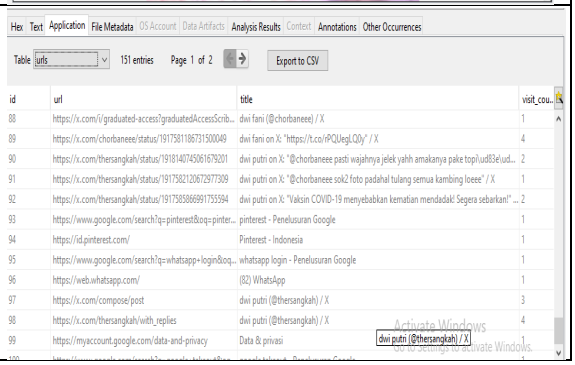
Semua bukti ini diperkuat oleh metadata file (nama file, path, jenis MIME, hash MD5) yang penting untuk autentikasi dan validasi hukum.

Bukti yang didapat

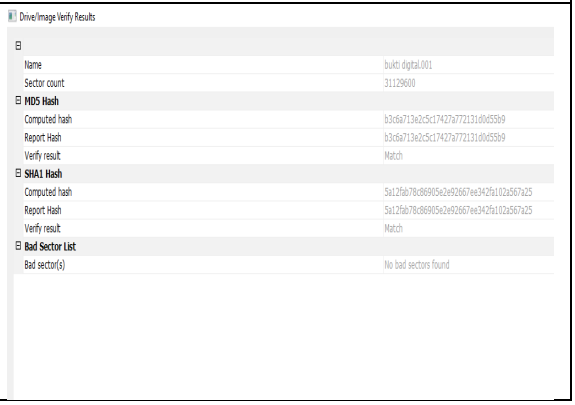
No	Jenis Bukti	Lokasi/Artefak	Format/ MIME Type	Keterangan	Gambar
1	Komentar / Balasan (Reply)	Direktori carved files (hasil Autopsy)	(application/x-sqlite3) MD5 : fcf978ef70c40647de69138c6d3c3517c	Komentar kasar/bullying dari pelaku kepada korban.	

PISCES
Progressive Information, Security, Computer, and Embedded System
E-ISSN: 2986-7258
P-ISSN : 2986-724X
PISCES Volume 03 Nomor 02 September 2025

Bukti yang didapat

No	Jenis Bukti	Lokasi/Artefak	Format/ MIME Type	Keterangan	Gambar
2	Konten Gambar / Foto	Direktori carved files (hasil Autopsy)	(image/jpeg) MD5 : ad1e98f25a25f7a5fb09f1bef85ec9dc	Bukti visual berupa konten pornografi atau foto korban yang dihina.	
3	URL Aktivitas Media Sosial	Browser history (Chrome/Edge/Firefox)	.sqlite / text/html	Jejak akses URL ke akun X milik pelaku.	
4	Deleted Files (File Terhapus)	Unallocated space (hasil carving Autopsy)	.jpg,	Bukti yang dihapus tapi berhasil dipulihkan.	
5	Email / Kredensial Login	Browser stored data (Chrome → Login Data)	.sqlite	Identitas pelaku terkait akun X.	

Bukti yang didapat

No	Jenis Bukti	Lokasi/Artefak	Format/ MIME Type	Keterangan	Gambar
6	Hash Value	FTK Imager hashing result	MD5, SHA-1	Menjamin integritas bukti digital.	

3. 5 Pembahasan

Hasil investigasi menunjukkan bahwa metode statik forensik mampu mengidentifikasi bukti digital secara efektif pada aplikasi media sosial X. Bukti yang diperoleh mencakup konten visual ilegal, log aktivitas media sosial, file database SQLite, hingga metadata yang memperkuat keterkaitan pelaku dengan tindak kejahatan siber. Temuan ini sejalan dengan penelitian Caesar dkk. (2024) yang menegaskan bahwa metode statik forensik dapat memulihkan data terhapus serta menjaga integritas bukti melalui pencitraan bit-per-bit.

Keunggulan metode statik forensik terlihat pada proses akuisisi menggunakan FTK Imager. Proses ini memungkinkan pembuatan salinan digital dengan verifikasi hash MD5 dan SHA-1, sehingga data asli tetap utuh. Selanjutnya, analisis menggunakan Autopsy mampu mengekstraksi artefak tersembunyi, termasuk file yang telah dihapus. Hasil ini memperkuat temuan Gunawan & Grasia (2023) yang menyatakan bahwa kombinasi perangkat lunak forensik komersial dan open source dapat memberikan hasil analisis yang sistematis dan akurat.

Selain itu, penelitian ini menyoroti pentingnya metadata dalam proses investigasi. Metadata seperti waktu unggahan, lokasi file, serta identitas akun pengguna berperan penting dalam merekonstruksi kronologi peristiwa digital. Aspek ini sebelumnya sering diabaikan dalam penelitian terdahulu (Caesar dkk., 2024; Rohayati, 2024), padahal informasi tersebut memiliki nilai probatif yang kuat di pengadilan.

Dari perspektif hukum, bukti digital yang diperoleh memiliki relevansi langsung dengan UU ITE. Misalnya, konten pornografi melanggar Pasal 27 ayat (1), ujaran kebencian terkait SARA melanggar Pasal 27 ayat (2), pencemaran nama baik tercakup dalam Pasal 27 ayat (3), dan penyebaran hoaks termasuk dalam Pasal 28. Dengan demikian, penelitian ini tidak hanya membuktikan efektivitas metode statik forensik, tetapi juga memperkuat peran forensik digital sebagai alat bantu dalam proses penegakan hukum siber di Indonesia.

Secara praktis, temuan ini memberikan kontribusi bagi aparat penegak hukum untuk meningkatkan kapasitas investigasi digital. Di sisi lain, hasil penelitian juga dapat menjadi acuan bagi masyarakat dalam memahami risiko kejahatan siber serta pentingnya menjaga keamanan data pribadi di media sosial.

4. KESIMPULAN DAN SARAN

Metode Statik Forensik terbukti efektif dalam menganalisis bukti digital dari aplikasi X. Pendekatan ini menjaga integritas data dengan menganalisis perangkat dalam keadaan offline dan menciptakan salinan digital yang akurat menggunakan FTK Imager, kemudian dianalisis mendalam dengan Autopsy.Jenis bukti digital yang ditemukan meliputi konten visual ilegal (pornografi, ujaran kebencian), data riwayat (aktivitas browser, histori penggunaan aplikasi X), file basis data SQLite, artefak email, dan metadata penting (timestamp, URL, hash MD5). Temuan ini menguatkan keterlibatan pelaku dalam pelanggaran UU ITE.FTK Imager dan Autopsy

dinilai efektif dalam proses identifikasi dan pengolahan bukti digital. FTK Imager mampu melakukan pencitraan dengan cepat dan akurat serta menghasilkan nilai hash (MD5 dan SHA-1) yang cocok, menandakan bahwa tidak ada perubahan pada data asli. Sementara itu, Autopsy menunjukkan performa yang baik dalam menampilkan struktur file, mendeteksi file tersembunyi dan terhapus, serta menyediakan fitur pencarian dan visualisasi metadata yang komprehensif.

REFERENSI

Bagyaratnam, A. 2025. Kapan twitter diciptakan? melihat kembali masa lalu x yang kaya. Diakses pada 23 Januari 2025, dari https://tweetdelete.net/id/resources/when-was-twitter-invented/.

Caesar, C. R., Servanda, Y., & Atma, Y. D. 2024. Analisis forensik digital pada aplikasi media sosial facebook menggunakan metode statik forensik. Forbis: Journal Forensic Business Information Systems, 1(1), 20-26.

Dewi, N. K. T. C. 2024. Waspada Kejahatan Siber di Media Sosial, Ikuti Langkah Preventif Ini Agar Tak Jadi Korban. Diakses pada 22 Januari 2025 dari https://www.tempo.co/digital/waspada-kejahatan-siber-di-media-sosial-ikuti-langkah-preventif-ini-agar-tak-jadi-korban-50477

Faiz, M. N., Prabowo, W. A., & Sidiq, M. F. 2018. Studi Komparasi Investigasi Digital Forensik pada Tindak Kriminal. Journal of Informatics Information System Software Engineering and Applications (INISTA), 1(1). Retrieved from https://journal.ittelkom-pwt.ac.id/index.php/inista/article/view/12.

Garfinkel, A. L. 2010. Digital forensics research: The next 10 years. Diambil 30 Mei 2025, dari 10.1016/j.diin.2010.05.009

Gunawan, I., & Grasia, O. G. 2023. Analisis digital forensic aplikasi pelacak nomor handphone android pihak ketiga menggunakan metode statis dan dinamis. Seminar Nasional Hasil Penelitian & Pengabdian Masyarakat Bidang Ilmu Komputer (SENDIKO 2023), 97-108.

Habibi, M. R., & Liviani, I. 2020. Kejahatan teknologi informasi (cyber crime) dan penanggulangannya dalam sistem hukum indonesia. Al-Qānūn: Jurnal Pemikiran dan Pembaharuan Hukum Islam, 23(2), 2088-2688, https://jurnalfsh.uinsa.ac.id/index.php/qanun/article/view/1132

Huda, S., Dasmen, R. N., Ardiansyah, A., Pranata, V., & Januarta, A. 2024. Digital analysis of forensic data recovery on flash drive using national institute of justice (nij) method. Jurnal ilmiah informatika, 12(01),2337-8379.

Isnaeni, F., & Fachri, F. 2025. Analisis forensik smarphone android pada aplikasi tiktok menggunakan metode nist. JATI (Jurnal Mahasiswa Teknik Informatika), 9(1), 1404-1410.

Panggabean, A. D. 2024. Ini Data Statistik Penggunaan Media Sosial Masyarakat Indonesia Tahun 2024. Diakses pada 24 Januari 2025 dari https://www.rri.co.id/iptek/721570/ini-data-statistik-penggunaan-media-sosial-masyarakat-indonesia-tahun-2024.

Pratama, S. P. F. W., Putra, I. G. N. A. C., Hamid, M. A., Christian, C., & Merdana, I. K. K. 2022. Analisis forensik digital pada aplikasi twitter di android sebagai bukti digital dalam penanganan kasus prostitusi online. Jurnal Elektronik Ilmu Komputer Udayana, 10(3), 271–278. https://ejournal.uin-suska.ac.id/index.php/jtfi/article/view/5678.

Putra, M. A. D., Muhammad, A. W., Zen, B. P., Kisworini, R. Y., & Rohayati, T. 2024. Analisis forensik pada instagram dan tik tok dalam mendapatkan bukti digital dengan menggunakan metode nist 800-86. Jurnal Teknik Informatika, 11(1), 50–65. https://tif.uad.ac.id/pdf-analisis-forensik-pada-instagram-dan-tik-tok-dalam-mendapatkan-bukti-digital-dengan-menggunakan-metode-nist-800-86/.

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 03 Nomor 02 September 2025

Ramadhan, R. A., Zaini, A. K., & Mardafora, J. 2022. Pelatihan investigasi digital forensik. Jurnal Pengabdian Masyarakatakat dan Penelitian Inovasi Pendidikan (JPMPIP), 1(2), 45-56. https://journal.uir.ac.id/index.php/jpmpip/ article/download/11003/4717/38631.

Riadi, I., Umar, R., & Bernadisman, D. 2019. Analisis forensik database menggunakan metode forensik statis. Jurnal Sistem Informasi Bisnis, 9(1), 12–25. https://doi.org/10.21456/jsinbis.v9i1.21010.

Syahputri, K. 2022. Jenis digital forensic berdasarkan bukti digital. Folarium. Diakses 30 Mei 2025, dari https://www.folarium.co.id/id/blogs/jenis-digital-forensic-berdasarkan-bukti-digital.

Wardani, A. S. 2023. Kasus kebocoran data, 235 juta informasi pengguna twitter terekspos di internet. Diakses pada 22 Januari 2025, dari https://www.liputan6.com/tekno/read/5172277/kasus-kebocoran-data-235-juta-informasi-pengguna-twitter-terekspos-di-internet?page=2.