ANALISIS BUKTI DIGITAL TWITTER WEB MENGGUNAKAN LIVE FORENSIC PADA KASUS CYBERBULLYING

Nur Halimah, Fahmi Fachri
Teknik Informatika, Universitas Ma'arif Nahdlatul Ulama Kebumen
Jalan Kutoarjo km 05 Jatisari, Kebumen, Jawa Tengah, Indonesia
hnur44442@gmail.com

ABSTRAK

Perkembangan teknologi komputer yang semakin pesat tentunya memberikan berbagai dampak positif, namun perkembangan teknologi tentunya juga memiliki dampak negatif seperti tindak kejahatan pada dunia maya yang semakin meningkat. *Cyberbullying* merupakan salah satu jenis tindak kejahatan *cyber* yang hingga saat ini masih sering terjadi. Tindak kejahatan ini sering terjadi di *platform* media sosial Twitter, sehingga diperlukan penanganan yang lebih lanjut agar kasus kejahatan tersebut dapat diselesaikan dan pelaku dapat dimintai pertanggungjawaban atas perbuatannya. Maka dari itu penelitian ini dilakukan untuk mempermudah penyidik dalam mencari bukti tindakan *cyberbullying* yang nantinya akan dijadikan sebagai barang bukti digital. Dalam forensik digital, *live forensic* digunakan untuk mengumpulkan bukti digital dengan menerapkan metode NIST. Metode NIST SP 800-86 terdiri dari empat tahapan, yaitu *collection*, *examination*, *analysis*, dan *reporting*. Pada penelitian ini, proses *live forensic* dilalukan dengan menggunakan *tools* FTK Imager dan HxD Editor untuk mendapatkan barang bukti 100% yang berupa teks percakapan antara pelaku dan korban. Skenario kejahatan ini dirancang untuk mendapatkan bukti perundungan yang nantinya akan digunakan sebagai alat pendukung dalam pelaporan kepada pihak yang berwajib, sesuai dengan Pasal 27 Ayat (3) UU ITE.

Kata kunci: *Cyberbullying, Twitter, Live Forensic*

1. PENDAHULUAN

Kemajuan teknologi digital yang pesat tentunya mempunyai dampak yang besar pada berbagai aspek kehidupan, teknologi kini memungkinkan kita untuk dapat mengakses berbagai informasi dengan mudah, efisien, dan cepat dari mana saja, termasuk di media sosial. Media sosial sendiri merupakan *platform* berbasis internet yang tidak hanya menyediakan ruang bagi pengguna untuk beraktivitas secara online, tetapi juga untuk terhubung, berbagi informasi, serta berinteraksi dengan orang lain tanpa adanya batasan jarak. Di dalam dunia maya, pengguna dapat berpartisipasi dalam berbagai kegiatan sosial, baik melalui situs web, blog, maupun jejaring sosial yang semakin beragam[1].

Menurut Kementrian Komunikasi dan Informatika (Kemenkominfo), sebanyak 95% dari 63 juta pengguna internet di Indonesia merupakan pengguna media sosial. Dan Twitter merupakan salah satu media sosial yang sampai saat kini masih sering digunakan. *Country Industry Head Twitter Indonesia* menyatakan bahwa Indonesia adalah negara dengan pengguna aktif harian Twitter yang terbesar[2]. Banyaknya pengguna ini juga membuka peluang untuk terjadinya kejahatan siber. *Cybercrime* merupakan tindak jenis kejahatan yang terjadi di media sosial dengan memanfaatkan teknologi internet yang terus berkembang[3].

Cyberbullying merupakan tindak kejahatan siber yang hingga saat ini masih sering ditemui pada media sosial, salah satunya Twitter. Kejahatan ini melibatkan tindakan perundungan dan penghinaan terhadap korban melalui media sosial, dengan tujuan memberikan kerugian emosional dan psikologis teradap korban [4]. Pada *platform* media sosial Twitter tindakan *cyberbullying* sering kali dilakukan dengan menuliskan cuitan yang menggunakan kata-kata kasar dan penghinaan, termasuk yang bernuansa penghinaan terkait SARA. Pemerintah melaporkan bahwa sekitar 84% remaja Indonesia berusia 12 hingga 17 tahun mengalami perundungan (*bullying*), dengan sebagian kasus yang ditemukan adalah kasus *cyberbullying*[2].

Penelitian sebelumnya telah menggali informasi forensik terkait kasus *cyberbullying* yang terjadi pada platform media sosial Facebook dengan menggunakan metode *live forensic*[5]. Metode utama yang dipilih adalah pendekatan *live forensic* karena kemampuannya untuk memperoleh bukti-bukti kejahatan yang terdapat pada komputer yang sedang berjalan serta terhubung pada jaringan internet[6]. Sementara itu, menurut penelitian yang dilakukan oleh Hariani., *web browser forensic* menjadi bagian penting dalam investigasi *digital forensic*. Web browser juga memiliki peran yang sangat penting pada kejahatan yang sedang terjadi, karena web browser sering digunakan untuk mengakses informasi atau melakukan tindak kejahatan yang mendukung aksi pelaku[7]. Peneliti juga menggunakan *tools* FTK Imager karena kemampuannya untuk membuat salinan bukti forensik dan melakukan analisis terhadap data dari media penyimpanan. *Tools* ini juga dapat membantu penyindik untuk mengamankan bukti dengan cara yang cepat dan aman, sehingga mendukung proses investigasi *digital forensic* secara efektif[8].

Pada simulasi penelitian kali ini, browser Chrome digunakan untuk mengakses Twitter. Aplikasi browser umumnya sering digunakan untuk mencari informasi, mengelola *email*, berinteraksi melalui pesan

instan atau media sosial dan juga berbelanja di situs *web e-commerce*[9]. Setiap browser memiliki tujuan yang sama, yaitu dengan memberikan antarmuka bagi pengguna untuk memasukkan alamat *email* serta memanfaatkan mesin pencari yang dapat digunakan untuk mengakses serta menemukan berbagai situs web. Selain itu, browser juga berperan dalam memudahkan navigasi di situs web, memungkinkan pengguna untuk menekan tautan, menjelajahi halaman, mengisi formulir, serta berinterkasi dengan elemen interkatif seperti tombol, video, atau gambar. Semua browser juga dilengkapi dengan fitur tambahan, seperti pengelolaan *bookmark*, penyimpanan sandi, pengaturan privasi, serta dukungan ekstensi yang meningkatkan fungsionalitas dari browser. Dalam penelitian ini, akses Twitter melalui browser Chrome dilakukan dengan tujuan khusus, yaitu untuk memperoleh *log file* dan *cache*, yang kemudian akan dianalisis serta dijadikan sebagai bukti perundungan, dan selanjutnya dapat digunakan sebagai alat pendukung yang sah pada saat pelaporan kepada pihak yang berwajib, sesuai dengan Pasal 27 Ayat (3) UU ITE[10].

2. TINJAUAN PUSTAKA

2.1. Digital Forensik

Digital forensik adalah ilmu forensik yang biasanya digunakan untuk mengekstrak data dari bukti elektronik yang selanjutnya diproses menjadi data intelijen untuk ditindaklanjuti serta digunakan sebagai bukti dalam proses hukum. Dengan adanya digital forensik membantu penyidik dalam menyelidiki, memulihkan, atau mengembalikan data elektronik yang telah rusak atau di hapus[11].

2.2. Bukti Digital

Pada dasarnya, barang bukti adalah informasi dan data. Secara umum, barang bukti digital dalam komputer forensic terbagi menjadi 3, yaitu[12]:

a. Data aktif adalah data yang mudah diakses karena digunakan secara langsung dalam berbagai aktivitas yang sedang berjalan, seperti menjalankan program, membuka file gambar dan juga mengolah dokumen teks atau aktivitas lainnya yang membutuhkan data secara *real-time*.
b. Data arsip adalah data yang di *backup*, seperti dokumen yang diubah ke dalam format TFF dengan tujuan untuk menjaga kualitas dokumen.
c. Data laten atau data ambient, adalah jenis data yang tidak terlihat secara langsung karena tersimpan dalam format atau lokasi yang tidak biasa, seperti log database dan juga log internet. Data laten ini juga sering disebut sebagai resdiual data, yang berarti data sementara.

2.3. Live Forensic

Live forensic adalah metode yang sering digunakan untuk memperoleh bukti tindak kejahatan dari komputer yang sedang terhubung dengan jaringan internet. metode ini mencakup analisis data yang sedang berlangsung di sistem atau volatil yang biasanya tersimpan pada *Random Access Memory* (RAM) atau sedang transit melalui jaringan[6].

2.4. Cyberbullying

Cyberbullying adalah tindak kejahatan *cybercrime* yang hingga saat ini masih marak terjadi. Bentuk kejahatan ini berupa tindakan bullying seperti mengejek, mencela, atau menghina korban di media sosial dengan tujuan merugikan korban secara psikologis dan juga emosional[4].

2.5. Twitter

Twitter adalah *platform* jejaring sosial yang memungkinkan penggunanya untuk berinteraksi satu sama lain melalui komputer atau perangkat *mobile*, kapan saja dan dimana saja. Situs ini memungkinkan berbagi pesan singkat, informasi, dan berbagai konten lainnya secara *real-time* yang menjadikannya sebagai salah satu alat komuniasi utama di dunia digital saat ini[13].

2.6. FTK Imager

FTK Imager merupakan *tools* forensik yang digunakan untuk menganalisis bukti digital. *Tools* ini memungkinkan para penyidik untuk membuat salinan forensik dari media penyimpanan tanpa merubah data aslinya. FTK Imager berfungsi untuk mengakuisisi atau melakukan *imaging* dari file, direktori, partisi, atau *physical disk* guna keperluan investigasi. Salah satu kelebihan FTK Imager adalah kemampuannya dalam memulihkan file yang terhapus, tersembunyi, atau terformat sehingga file tersebut dapat dianalisis lebih lanjut[6].

2.7. HxD Editor

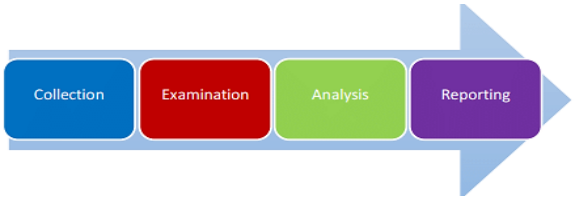
HxD Editor adalah sebuah *tools* yang berfungsi sebagai editor *hexadecimal*, dan digunakan untuk membaca, mengedit, serta menganalisis data mentah pada tingkat *byte*. *Tools* ini memungkinkan akses langsung ke data file, *RAM*, atau perangkat penyimpanan seperti *hard disk*, *SSD*, dan kartu memori[14].

3. HASIL DAN PEMBAHASAN

3.1. Metode Penelitian

Live forensic diterapkan untuk memperoleh informasi dan mengumpulkan barang bukti pada jaringan lokal, terutama ketika perangkat atau alat bukti di lokasi kejadian terhubung ke jaringan komputer yang masih aktif dan beroperasi. Pendekatan ini memungkinkan analisis data secara langsung tanpa mematikan sistem, sehingga potensi kehilangan informasi penting dapat diminimalkan[15]. Selain itu penelitian ini juga menggunakan metodologi NIST (*National Institue of Standards and Technology*). Metode ini menjelaskan tahapan secara terstruktur sehingga langkah-langkah penelitian dapat dilakukan dengan terstruktur dan dapat dijadikan acuan dalam menyelesaikan suatu permasalahan yang ada[16].

Dalam investigasi digital, Metode Forensik NIST berfungsi sebagai panduan yang mendukung ahli forensik dalam proses pengumpulan, analisis, dan pengamanan bukti digital secara ilmiah[17].



Gambar 1. Metode NIST

Berdasarkan Gambar 1 diketahui bahwa metode *National Institue of Standards and Technology* (NIST) terdapat 4 tahapan, yaitu:

a. *Collection*
   Tahapan yang pertama adalah *collection* atau pengumpulan bukti digital yang relevan dengan penyelidikan untuk dianalisis lebih lanjut. Proses ini mencakup kegiatan seperti identifikasi, ekstrasi, dan juga transfer data atau pemindahan data dari perangkat atau sumber terkait. Pada tahapan ini menggunakan pendekatan *live forensic*, seperti *RAM imaging*.
b. *Examination*
   Pada tahap *examination* atau pemerikasaan, data yang telah diperoleh sebelumnya kemudian dianalisis menggunakan *tools* berupa FTK Imager.
c. *Analysis*
   Pada tahapan ini, akan dilakukan analisis terhadap hasil pemeriksaan data yang bertujuan untuk mengindentifikasi informasi yang nantinya dapat dijadikan sebagai barang bukti digital dalam kasus *cyberbullying*.
d. *Reporting*
   Hasil dari kasus kejahatan dan analisis bukti digital yang sudah didapatkan pada tahap sebelumnya selanjutnya dilaporkan pada tahapan terakhir, yaitu reporting. Laporan ini akan menjadi bukti yang valid dalam penanganan tindak kejahatan siber.

3.2. Alat Dan Bahan

Untuk mendukung penelitian kali ini, diperlukan berbagai *tools*. *Tools* tersebut mencakup perangkat keras (*hardware*) dan perangkat lunak (*software*). Penggunaan tools ini dijelaskan pada Tabel 1.

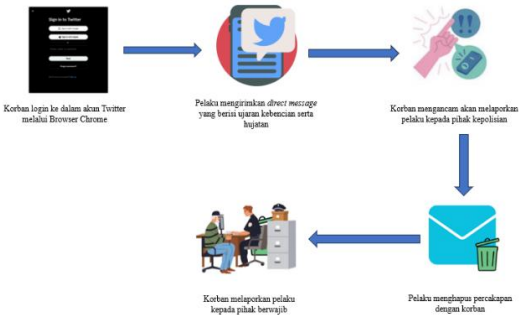
Tabel 1. Alat dan Bahan

No	Tools	Version
1	Laptop	HP, Intel(R) Celeron(R), 64bit, RAM 4GB
2	Browser Chrome	Version 131.0.6778.110 (Official Build) (64-bit)
3	Akun Simulasi	@jaacck02
4	FTK Imager	3.1.2.0
5	HxD Editor	2.5

Berdasarkan Tabel 1, fokus utama dalam penelitian ini adalah Twitter yang kemudian diakses menggunakan browser. FTK Imager digunakan dalam penelitian ini karena dapat mengembalikan bukti digital yang sudah dihapus dari Google Chrome pada derektori laptop. Selain itu, FTK Imager juga efektif dalam mengekstrak data file dan log yang dapat mendukung proses analisis lebih lanjut. *Tools* ini menjadi pilihan utama karena keandalannya dalam menangani bukti digital secara efisien dan akurat[14]. Selain itu, HxD Editor juga digunakan dalam penelitian ini untuk memeriksa serta menganalisis proses pemulihan file. *Tools* ini mampu menganalisis struktur file serta mengakses data secara menyeluruh melalui proses perhitungan tertentu.

3.3. Rancangan Simulasi Kasus

Skenario pada penelitian ini dirancang mengacu pada UU ITE Pasal 27 Ayat (3), yang mengatur tentang pendistribusian dan atau pentransmisian dokumen elektronik yang memuat unsur penghinaan dan atau pencemaran nama baik[18]. Dibawah ini adalah alur skenario kasus *cyberbullying* yang nantinya akan digunakan pada simulasi penelitian.



Gambar 2. Rancangan simulasi kasus cyberbullying pada Twitter web

Skenario kasus pada gambar diatas menggambarkan interaksi antara kedua belah pihak, yaitu pihak pelaku dan korban. Korban menggunakan browser Chrome untuk mengakses Twitter. Setelah itu pelaku mengirimkan pesan kepada korban yang berisi hujatan dan ujaran kebencian. Lalu korban mengancam pelaku akan dilaporkan ke pihak yang berwajib setelah itu pelaku menghapus pesan yang dirimkan kepada korban. Dan korban melaporkan pelaku ke pihak yang berwajib.

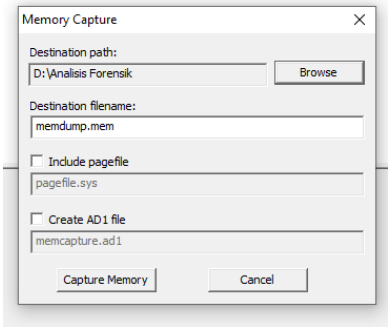
4. HASIL DAN PEMBAHASAN

Berdasarkan dengan skenario yang telah dirancang, penyidik telah menemukan laptop milik pelaku dengan kondisi menyala dan dijadikan sebagai barang bukti. Selanjutnya, penyidik melakukan penyelidikan lebih lanjut dengan mengikuti kerangka kerja NIST SP 800-80. Namun ketika proses penyelidikan dilakukan, barang bukti yang berupa teks Twitter telah dihapus sehingga diperlukan penggunaan

tools forensic untuk menemukan brang bukti yang telah dihapus.

4.1. Collecting

Pada tahapan ini dilakukan pengumpulan barang bukti digital dengan cara mengambil data dan informasi yang masih tersimpan di dalam RAM laptop milik pelaku. Proses ini dilakukan dengan menggunakan tools FTK Imager untuk melakukan *capture memory*, sebagaimana ditunjukkan pada Gambar 3.

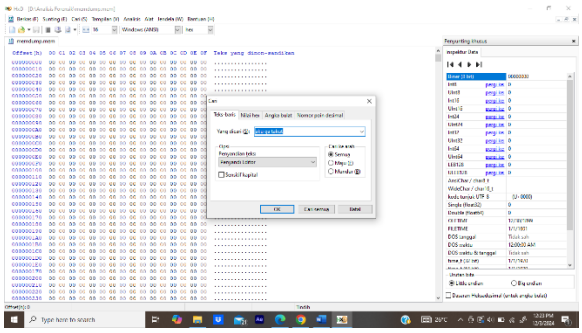


Gambar 3. Tahapan Capture Memory pada FTK Imager

Setelah barang bukti berhasil dikumpulkan, dilakukan proses *RAM Imaging* untuk menggandakan barang bukti digital dengan tidak mengubah data aslinya. Proses ini menghasilkan file dengan format *.mem.*

4.2. Examination

Pemeriksaan kemudian dilakukan melalui tahapan *examination* terhadap bukti yang telah diperoleh pada tahap *collecting*. Untuk memperoleh bukti percakapan pada Twitter Web yang tersimpan di dalam RAM, digunakan teknik *Live Forensic*. Dalam proses ini menggunakan tools FTK Imager namun hasil dari *capture memory* tersebut akan dibuka dengan menggunakan *tools* HxD Editor untuk menemukan bukti digital. Gambar 4 merupakan proses pencarian bukti digital.

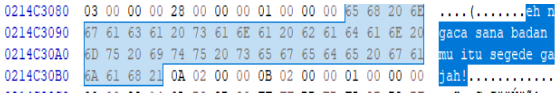


Gambar 4. Proses pencarian bukti digital

Untuk mencari bukti digital menggunakan *tools* HxD Editor, langkah pertama adalah membuka file yang akan dianalisis. Setelah itu, masukan kata kuci yang ingin ditemukan pada fitur pencarian seperti isi pesan atau informasi lainnya. Kemudian HxD akan mencari data tersebut di dalam file. Dengan cara ini, mempermudah dalam pencarian bukti digital karena tidak perlu memeriksa setiap bagian file satu per satu.

4.3. Analysis

Tahap *analysis* dilakukan terhadap hasil temuan pada tahapan *collection*, yang berhasil mengidentifikasi bukti berupa pesan teks yang dikirimkan pelaku kepada korban melalui FTK Imager.



Gambar 5. Salah satu bukti data digital

Data digital yang telah berhasil didapatkan melalui proses RAM Imaging berupa tipe data yang berbentuk teks. Pada tahapan ini, file dengan format *.mem* yang didapatkan pada tahap collecting kemudian dibuka dan dianalisis dengan menggunkan *tools* HXD. Hasil analisis dapat dilihat pada Gambar 5.

Hasil analisis menunjukkan salah satu pesan yang dikirimkan pelaku kepada korban. Dari pesan tersebut teridentifikasi bahwa pelaku melakukan tindakan *bullying* terhadap korban dengan melakukan pembullyan fisik.

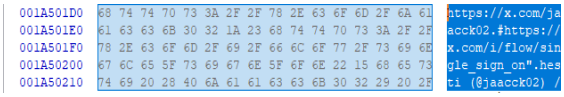
Dengan demikian, pada penelitian ini bukti digital berhasil ditemukan meskipun bukti tersebut telah dihapus dari browser milik pelaku. Tabel 2 merupakan hasil analisis yang telah dilakukan sebelumnya, yang memuat percakapan yang ditemukan pada akun Twitter pelaku. Bukti digital tersebut diperoleh menggunakan *tools* forensik yang mendukung penyidik dalam mengungkap kasus *cyberbullying* melalui Twitter Web.

Tabel 2. Bukti digital

Offsets	Isi Percakapan	Kesimpulan
16AAC4EA0	woy!	Ditemukan
17409F630	lu anak kelas Mipa 2 kan	Ditemukan
007256980	Iya bener	Ditemukan
007256B80	Ini siapa ya?	Ditemukan
040FD3070	kamu ga perlu tau aku siapa, yang harus kamu ketahui jadi orang jangan sok kecantikan deh	Ditemukan
125BF1080	Maaf ya aku ngga pernah merasa begitu	Ditemukan
157FF36C0	Alah jangan munafik dan sok baik deh jadi cewe	Ditemukan
01C904140	mending ngaca aja sana sadar diri	Ditemukan
01B1E3940	Kenapa kasar banget ya omongannya	Ditemukan
1352DDCF0	kenapa emang? ga suka?	Ditemukan
0214C3080	eh ngaca sana badan mu itu segede gajah!	Ditemukan

Offsets	Isi Percakapan	Kesimpulan
12EFF82F0	muka gradakan kaya aspal rusak tapi sok kecantikan banget!	Ditemukan
03548C840	Aku bisa ya laporin dan nuntut kamu atas perkataan kamu yang kasar itu!	Ditemukan
107CA020200	silahkan bodo amat	Ditemukan
0159DDED0	aku ga takut dan ga peduli!	Ditemukan

Selain ditemukannya pesan percakapan antara pelaku dan korban, juga telah ditemukan akun *Twitter* milik pelaku yang dapat memperkuat bukti. Bukti tersebut dapat dilihat pada Gambar 6.



Gambar 6. Bukti data digital dari akun pelaku

Pada Gambar 6, terlihat offiset 001A501D0 sampai 001A50210 serta binnary dengan hex 68 hingga 2F yang menunjukan akun dari pelaku yaitu *@jaacck02*.

4.4. Reporting

Dalam kasus *cyberbullying* yang telah terjadi di platform Twitter web, ditemukan bukti digital berupa teks percakapan antara pelaku dan korban yang sesuai dengan keterangan korban, meskipun pesan tersebut telah dihapus. Proses pembuktian kasus ini dapat dilihat pada Tabel 2, dimana data diperoleh dengan menggunakan *tools* FTK Imager. Bukti digital yang terhapus tersebut berhasil ditemukan kembali dengan tingkat keberhasilan 100%.

5. KESIMPULAN DAN SARAN

Berdasarkan penelitian yang telah dilakukan, analisis aktivitas *cyberbullying* pada pengguna Twitter yang diakses melalui browser Chrome dilakukan dengan pendekatan *Live Forensic*. Bukti digital yang sebelumya terhapus berhasil dipulihkan dengan menggunakan *tools forensic* yaitu FTK Imager dan juga HxD Editor. Bukti yang ditemukan berupa teks percakapan antara pelaku dan korban yang menunjukkan adanya interaksi yang berhubungan dengan kasus *cyberbullying*, selain itu juga ditemukan akun pelaku yang dapat memperkuat bukti tersebut. Pada penelitian selanjutnya diharapkan dapat mengkombinasikan metode *live forensic* dengan berbagai *tools* lainnya untuk memperoleh bukti digital yang lengkap dan akurat, sehingga mendapatkan informasi yang lebih mendalam dan jelas, dan dapat membantu dalam mengungkap tindak kejahatan yang terjadi dengan lebih efektif dan efisien.

DAFTAR PUSTAKA

[1] E. Satriya Wijaya and F. Tyas Pramesti, "Analisis Bukti Digital Forensik Pada Aplikasi Facebook Messenger Dan Twitter Berbasis Android Menggunakan Proses DFRWS (Studi Kasus: Pencemaran Nama Baik)," *J. Media Pratam*, vol. 18, no. 1, pp. 15–28, 2024.

[2] H. dan Fadli and A. Hidayatullah, "Identifikasi Cyberbullying pada Media Sosial Twitter Menggunakan Metode LSTM dan BiLSTM," *Univ. Islam Indones.*, vol. 2, no. No. 1, pp. 1–6, 2021.

[3] I. Riadi, Y. Safitri, and U. Ahmad Dahlan, "Hal. 1~8 Menggunakan Metode Association of Chief Police Officers," *J. Bumigora Inf. Technol.*, vol. 5, no. 1, pp. 1–8, 2023, doi: 10.30812/bite/v5i1.2977.

[4] H. S. Mikayla, A. Kusyanti, and P. H. Trisnawan, "Analisis Forensik Digital untuk Investigasi Kasus Cyberbullying pada Media Sosial Tiktok," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 10, no. 7, pp. 1571–1582, 2023, doi: 10.25126/jtiik.1078017.

[5] F. Dwi, "Analisis Aktivitas Cyber Bullying Pengguna Facebook Melalui Browser Chrome Dengan Pendekatan Live Forensics," *J. TIMES*, vol. 12, no. 1, pp. 21–27, 2023, doi: 10.51351/jtm.12.1.2023687.

[6] A. S. Rido and F. Fachri, "Identifikasi Bukti Digital Whatsapp Pada Sistem Operasi Proprietary Menggunakan Live Forensics," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 9, no. 2, pp. 1043–1051, 2024, doi: 10.29100/jipi.v9i2.5238.

[7] H. HARIANI, "Eksplorasi Web Browser Dalam Pencarian Bukti Digital Menggunakan Sqlite," *J. INSTEK (Informatika Sains dan Teknol.*, vol. 6, no. 1, p. 66, 2021, doi: 10.24252/instek.v6i1.18638.

[8] J. Teknologi, W. Agustiono, D. W. Suci, and N. Prastiti, "Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus Digital Forensic Analysis Using the NIST Method for Recovering Deleted Evidence," vol. 14, no. September, pp. 174–185, 2024, doi: 10.34010/jati.v14i2.

[9] Rahmat Inggi and Heri Pebrianto Alam, "Analisis Forensik Web Browser Pada Perangkat Android," *Simtek J. Sist. Inf. dan Tek. Komput.*, vol. 8, no. 1, pp. 215–220, 2023, doi: 10.51876/simtek.v8i1.249.

[10] R. P. A. Daeng Ngiji, S. Suseno, and B. A. Atmaja, "Penerapan Pasal 27 Ayat (3) UU ITE dalam Perkara Pencemaran Nama Baik melalui Media Sosial terhadap Kelompok Orang," *J. Fundam. Justice*, pp. 19–34, 2022, doi: 10.30812/fundamental.v3i1.1796.

[11] E. Ribka and T. Wangkar, "Jurnal Fakultas Hukum Universitas Sam Ratulangi Lex Privatum Vol.XII/No.2/jul/2023," *J. Fak. Huk. Univ. Sam Ratulangi Lex Priv.*, vol. 12, no. 2, pp. 1–13, 2023.

[12] R. A. Ramadhan, Abdul Kudus Zaini, and Jerika

Mardafora, "Pelatihan Investigasi Digital Forensik," *J. Pengabdi. Masy. dan Penerapan Ilmu Pengetah.*, vol. 3, no. 2, pp. 1–6, 2022, doi: 10.25299/jpmpip.2022.11003.

[13] Krisma and B. Waluyo, "Konten Pornografi Pada Media Sosial Twitter," *JUSTITIA J. Ilmu Huk. dan Hum.*, vol. 8, no. 2, pp. 270–278, 2021.

[14] F. Dwi, "Analisis Aktivitas Cyber Bullying Pengguna Instagram Melalui Browser Chrome Dengan Pendekatan Live Forensics," *J. TIMES*, vol. 12, no. 1, pp. 21–27, 2023, doi: 10.51351/jtm.12.1.2023687.

[15] E. Ariyanti, "Identifikasi Bukti Digital Instagram Web Dengan Live Forensic Pada Kasus Penipuan Online Shop," *Cyber Secur. dan Forensik Digit.*, vol. 4, no. 2, pp. 58–62, 2022, doi: 10.14421/csecurity.2021.4.2.2436.

[16] R. A. Bintang, R. Umar, and A. Yudhana, "Analisis Media Sosial Facebook Lite dengan tools Forensik menggunakan Metode NIST," *Techno (Jurnal Fak. Tek. Univ. Muhammadiyah Purwokerto)*, vol. 21, no. 2, p. 125, 2020, doi: 10.30595/techno.v21i2.8494.

[17] M. Rifqi, S. J. I. Ismail, M. F. Rizal, P. Studi, D. Teknologi, and U. Telkom, "Analisis Forensik Untuk Penanganan Cyber Crime Pada Aplikasi Whatsapp Menggunakan Metode National Institute of Standard and Technology (Nist Sp 800-86)," *e-Proceeding Appl. Sci.*, vol. 9, no. 6, pp. 3017–3022, 2023.

[18] Utami Argawati, "Alami Kasus Tuduhan Pencemaran Nama Baik, Seorang Karyawan Swasta Uji UU ITE," *Mahkama Konstitusi Republik Indonesia*, 2023. https://www.mkri.id/index.php?page=web.Berita&id=19040&menu=2 (accessed Nov. 28, 2024).