

ANALISIS AKTIVITAS *CYBER BULLYING* PENGGUNA *FACEBOOK* MELALUI *BROWSER CHROME* DENGAN PENDEKATAN *LIVE FORENSICS*

Febe Dwi Intan Permatasari
Program Studi Informatika
Universitas Muhammadiyah Sidoarjo
Jl. Raya Gelam No.250, Gelam, Kec. Candi, Kabupaten Sidoarjo, Jawa Timur, 0318051771
email: febedwi1@umsida.ac.id

Abstrak

Selain sebagai tempat bersosialisasi, internet dapat menjadi sarang bagi berbagai jenis kejahatan digital. Salah satunya ialah *cyber bullying*. Sosial media, terutama Facebook, merupakan wadah paling umum untuk melakukan tindak perundungan online. Fenomena tersebut tentu menimbulkan efek negatif kepada para korban. Sebagai bagian dari bidang Forensik Digital, *Live Forensics* memberikan kemampuan untuk mengumpulkan bukti digital yang terkait dengan kasus perundungan langsung dari perangkat yang masih aktif. Metodologi yang digunakan adalah *National Institute of Standard and Technology* (NIST), dimana mencakup empat tahap bertajuk pengumpulan, pemeriksaan, analisis dan pelaporan. Dalam penelitian ini, proses live forensik dilakukan dengan mengambil gambar memori (*RAM imaging*) serta mengakuisisi *log file*, cache, dan riwayat browser menggunakan alat bantu seperti FTK Imager dan Browser History Viewer. Simulasi kejahatan ini bertujuan untuk mengumpulkan bukti perundungan yang nantinya dapat dijadikan sebagai alat pendukung valid dalam pelaporan pihak berwajib sesuai dengan Pasal 27 Ayat (3) UU ITE.

Kata Kunci: Cyber bullying, Facebook, Live Forensics, FTK Imager, Sosial Media.

1. Pendahuluan

Kehadiran sosial media telah menjadi fenomena yang tak terelakkan dalam kehidupan masyarakat modern. Hampir setiap manusia di muka bumi ini setidaknya memiliki satu akun untuk melakukan interaksi sosial secara daring. Berdasarkan sifat alami manusia yang membutuhkan koneksi dengan orang lain, serta kecenderungan untuk berbagi informasi satu sama lain, penggunaan sosial media kian meroket tinggi dari tahun ke tahun. Berdasarkan penelitian yang digagas oleh Demand Sage, terdapat sekitar 4.9 miliar orang telah menggunakan sosial media di kehidupan sehari-hari mereka, dengan Facebook menjadi jejaring nomor satu yang memimpin bersama 2.95 miliar pengguna per-Juni 2023 [1]. Angka fantastis tersebut membuktikan bahwa hampir 61.8% dari total populasi dunia telah saling terkait dalam sosial media. Hal itu tentu tak luput dari peran kemajuan teknologi yang semakin mempermudah manusia untuk mengakses internet dalam sekali tekan.

Namun, majunya perkembangan teknologi tersebut juga berdampak pada sektor kejahatan dunia maya, atau yang populer dikenal dengan istilah *cybercrime*, mulai dari kasus hoax, penipuan online, pembobolan identitas, dan lain sebagainya [2]. Dengan padatnya penduduk digital tersebut, tidak dapat dipungkiri jika kejahatan digital juga mengalami pertumbuhan pesat, merusak dan menentang berbagai aspek serta norma-norma kehidupan yang mencerminkan kebajikan luhur. Pada kalangan anak-anak muda sendiri, *cyber bullying*, atau perundungan secara daring, hampir dapat ditemukan pada situs-situs sosial media manapun.

Cyber bullying merupakan bentuk *bullying* yang sangat rentan terjadi pada usia remaja, yang sekarang lebih mudah dan banyak dilakukan dengan menggunakan alat elektronik atau digital [3]. Tindakan *cyber bullying* pada media sosial tidak mengarah kepada perempuan atau laki-laki saja, dengan kata lain *cyber bullying* tidak mengenal jenis kelamin (gender) [4]. Umumnya, *cyber bullying* dilakukan dengan mengirimkan pesan atau komentar teks berupa kata-kata menyakitkan hati kepada korban dengan intensitas tinggi. Seorang remaja bisa saja menerima ratusan komentar jahat dalam hitungan menit, dan remaja tersebut tidak mampu menghentikan itu sehingga para pelaku makin menjadi untuk melancarkan aksinya.

Menurut penelitian yang dilansir dari *antibullyingsoftware.com*, kasus *cyber bullying* yang paling banyak dilaporkan terjadi di platform Facebook dengan persentase 87% [5]. Facebook merupakan situs jejaring sosial besutan Mark Zuckerberg. Diperkenalkan pertama kali pada tahun 2004, Facebook awalnya ditujukan sebagai project Zuckerberg untuk menghubungkan teman-teman di sekitar kampusnya secara daring. Lamban laun, platform sosial berwarna biru itu meraih popularitas global saat orang-orang selain rekan kampusnya turut mendaftarkan diri di situs tersebut. Tercatat Facebook berhasil mengumpulkan 6 juta user aktif di akhir tahun 2005. Dimulai dari sana, jumlah user Facebook terus merambat naik hingga mencapai 2.9 miliar.

Berbagai layanan menarik yang disediakan oleh Facebook adalah salah satu alasan mengapa jejaring sosial media tersebut sangat populer di kalangan warga digital. Fitur-fitur tersebut meliputi private profile, private messaging, sharing contents, multimedia hingga live streaming.

Pada simulasi penelitian kali ini, Facebook akan diakses menggunakan browser Chrome. Browser adalah sebuah perangkat lunak (software) yang digunakan untuk mengakses internet. Semua browser memiliki fungsi yang sama, yaitu antarmuka yang memungkinkan pengguna mengetik alamat email atau menggunakan mesin pencari untuk menemukan dan mengakses berbagai situs web di seluruh dunia. Selain itu, browser juga mendukung perenderan halaman web, yang berarti dapat menginterpretasikan konten HTML, CSS, dan JavaScript dari halaman web tersebut dengan format yang mudah dimengerti oleh pengguna internet. Browser juga memungkinkan pengguna untuk menavigasi situs web dengan menekan tautan, mengisi formulir, menjelajah antar halaman, dan berinteraksi dengan elemen interaktif seperti tombol, video, atau gambar. Fitur lain yang sama-sama dimiliki browser termasuk manajemen bookmark, penyimpanan kata sandi, pengaturan privasi, dan dukungan extension yang dapat meningkatkan fungsionalitas browser.

Chrome adalah sebuah web browser yang dikembangkan oleh raksasa teknologi Google. Per 2023, Google Chrome menjadi browser yang paling banyak digunakan di dunia [6]. Selain mudah dalam pengoperasiannya, masyarakat modern jauh lebih familiar dengan antarmuka Chrome yang interaktif serta memiliki kecepatan tinggi jika digunakan untuk berselancar di internet. Pengaksesan Facebook dengan browser Chrome pada penelitian ini bertujuan untuk mendapatkan akses log file, cache dan riwayat internet yang nantinya dapat dianalisis menjadi bukti perundungan yang nantinya dapat dijadikan sebagai alat pendukung valid dalam pelaporan pihak berwajib sesuai dengan Pasal 27 Ayat (3) UU ITE.

2. Landasan Teori

Menurut Casey (2011), Forensik Digital merupakan suatu pendekatan ilmiah yang mencakup pengumpulan, analisis, dan interpretasi bukti digital guna mendukung investigasi dan penyelesaian kasus kejahatan di dunia digital. Dalam konteks ini, analisis forensik digital digunakan untuk mengungkap aktivitas pengguna Facebook melalui browser Chrome dan mengumpulkan bukti digital terkait.

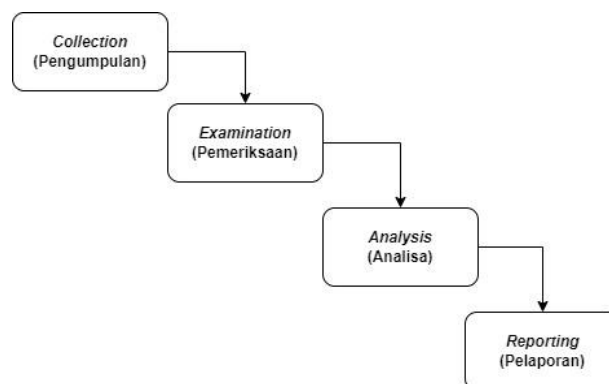
Menurut Taylor, Fritsch, Liederbach, & Holt (2014), kejahatan siber meliputi serangkaian tindakan kriminal yang dilakukan dengan memanfaatkan teknologi komputer dan jaringan internet. Dalam penelitian ini, kejahatan siber terkait dengan penggunaan Facebook diinvestigasi melalui pendekatan forensik digital untuk mengumpulkan dan menganalisis bukti digital. Landasan teori ini memberikan kerangka pemahaman yang penting dalam memahami konteks kejahatan siber yang terkait dengan penggunaan media sosial.

3. Metode Penelitian

Penelitian ini menerapkan pendekatan live forensic dengan metodologi atau framework investigasi digital forensic NIST (National Institute of Standards and Technology) [7]. NIST adalah lembaga federal bertempat di Amerika Serikat yang bertanggung jawab untuk mengembangkan dan mempromosikan panduan standar teknis dan pengukuran teknologi. NIST berperan penting dalam memajukan inovasi serta daya saing industri dengan menyediakan pedoman yang membantu dalam pengembangan keamanan sektor teknologi.

Metodologi Penelitian

Berikut ini merupakan tahapan penelitian NIST sesuai dengan pedoman yang tertulis, dapat dilihat pada Gambar 1 di bawah ini.



Gambar 1. Tahapan Forensik yang dikembangkan oleh NIST

1. Collection (Pengumpulan)

Tahap pertama yaitu pengumpulan (collection) bukti digital yang berkaitan dengan penyelidikan untuk diteliti. Tahap ini melibatkan identifikasi, ekstraksi, dan pemindahan data dari perangkat atau sumber yang terlibat. Teknik yang lazim digunakan adalah live forensic seperti RAM imaging, serta pengumpulan data dari log file, cache dan riwayat browser.

2. Examination (Pemeriksaan)

Tahap pemeriksaan (examination) melibatkan penyelidikan mendalam terhadap bukti digital yang telah dikumpulkan dengan menggunakan alat bantu seperti perangkat lunak (software) forensik seperti FTK Imager, Autopsy, dll.

3. Analysis (Analisa)

Tahap analisa (analysis) adalah tahap di mana data yang telah dikumpulkan dan diperiksa akan dianalisis untuk menemukan bukti-bukti yang dapat digunakan dalam kasus kejahatan siber. Proses ini mencakup pengidentifikasian, verifikasi, dan evaluasi bukti digital yang telah ditemukan.

4. Reporting (Pelaporan)

Hasil dari analisis bukti digital dan kasus kejahatan yang telah diperoleh di tahap sebelumnya kemudian dilaporkan pada tahap reporting [8]. Laporan ini nantinya akan digunakan sebagai bukti valid dalam kasus kejahatan siber yang sedang berlangsung.

Alat Dan Bahan

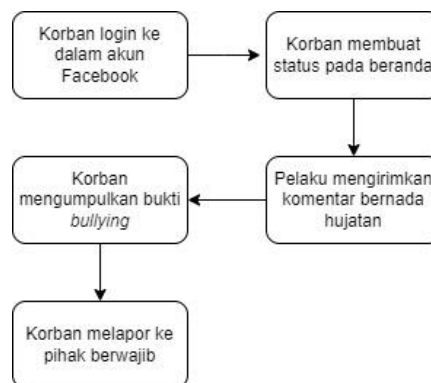
Untuk melakukan simulasi ini, telah dipersiapkan alat dan bahan yang sesuai dengan tujuan penelitian, yaitu cyber bullying. Alat dan bahan tersebut berupa perangkat lunak (software) forensik, perangkat keras (hardware) yang berperan sebagai perangkat korban, serta akun-akun Facebook yang keberadaannya hanya untuk menjalankan skenario simulasi. Berikut adalah tabel rincinya.

Tabel 1. Alat dan Bahan

No	Komponen	Spesifikasi
1	AccessData FTK Imager	Versi 4.7.1
2	Browser History Viewer	Versi 1.4.1 (Trial)
3	Google Chrome	Versi 109.0.5414.149
4	Akun Simulasi	Jaime Hagensen (jaimehagensen@outlook.co.id) jake.bannon.7773

Simulasi Kasus

Skenario ini didasarkan dari UU ITE Pasal 27 Ayat (3) yang mengatur tentang pendistribusian dan atau pentransmisi dokumen elektronik yang memuat unsur penghinaan dan atau pencemaran nama baik [9]. Berikut merupakan detail alur dari skenarionya.

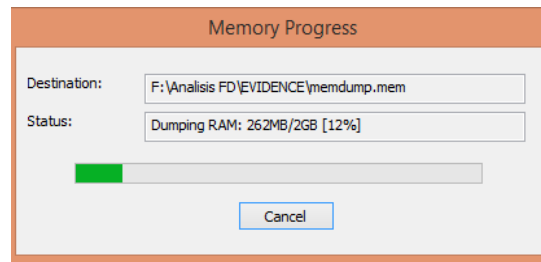


Gambar 2. Simulasi kasus cyber bullying melalui Facebook

Berdasarkan gambar di atas, skenario ini melibatkan interaksi antara dua pelaku, yaitu korban dan pelaku. Korban mengakses Facebook melalui browser Chrome lalu mengunggah sebuah status pribadi. Lalu, pelaku datang dan memberikan komentar bernada kurang menyenangkan. Korban dapat mengumpulkan komentar tersebut sebagai bukti dalam pelaporan resmi.

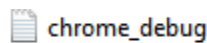
4. Hasil Penelitian Collection

Tahap Collection bermakna pengumpulan data dari aktivitas sosial media dengan bantuan FTK Imager. Dilakukan teknik RAM Imaging untuk mendapatkan bukti digital berupa RAM Image. Proses tersebut dapat memakan waktu yang cukup lama bergantung dari spesifikasi laptop.



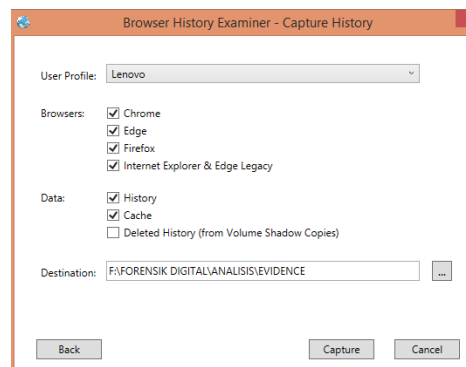
Gambar 3. Proses Memory Progress

Untuk mendapatkan bukti digital berupa log file Chrome dengan tajuk chrome_debug.log, pencarian dapat dilakukan melalui file explorer dengan memasukkan C:\Users\Lenovo\AppData\Local\Google\Chrome\User Data pada address bar file explorer.



Gambar 4. Log file Chrome

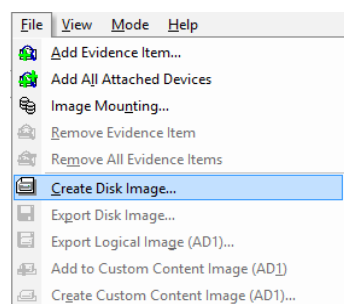
Untuk memperoleh data Cache, pencarian dapat dilakukan melalui alamat C:\Users\Lenovo\AppData\Local\Google\Chrome\User Data\Default\Cache. Dari folder Default Google Chrome-lah bukti digital dalam bentuk riwayat (history) dapat diperoleh. Pengumpulan Cache dan riwayat browser dilakukan dengan menggunakan software Browser History Viewer seperti yang ditunjukkan dalam gambar berikut.



Gambar 5. Proses ekstraksi riwayat browser

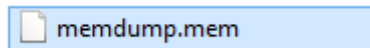
Examination

Jika semua bukti telah terkumpul, maka tahap selanjutnya adalah examination dengan cara melakukan pengecekan terhadap nilai hash dari file berekstensi mem hasil RAM Imaging. Cara untuk melakukannya yaitu, pilih Create Disk Image pada FTK Imager seperti gambar berikut.



Gambar 6. Create Disk Image...

Saat memilih file destinasi, pastikan perangkat yang dipakai memiliki penyimpanan ekstra lebih. Proses Create Disk Image ini juga turut memakan waktu serta ukuran yang tidak sedikit. Pilihlah file dengan ekstensi .mem.



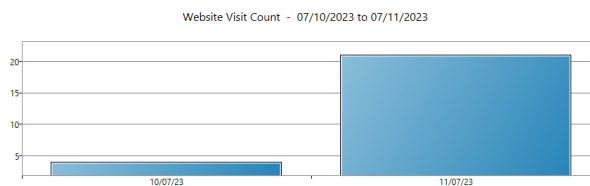
Gambar 7. File Keluaran dari Capture Memory

Setelah proses imaging selesai, hasilnya adalah sebuah file dengan ekstensi .ad1. Nilai hash digunakan untuk memverifikasi integritas file bukti digital tersebut, sehingga dapat memastikan apakah file tersebut tetap sama dan tidak mengalami modifikasi. Pada simulasi kali ini, nilai hash yang didapat adalah sebagai berikut.

```
MD5 checksum: 55f9dcd339747313ccd4af41b7a564d3
SHA1 checksum: 88204a0bb4f8c230ea71dfaeb59855aa47d36bc7
```

Gambar 8. Nilai MD5 dan SHA1

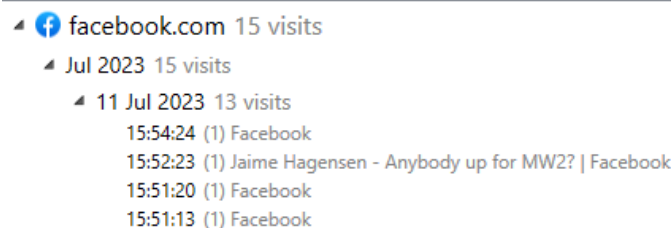
Selanjutnya, Browser Viewer History berperan untuk mengumpulkan riwayat browser Chrome secara default. Filtering history dimulai pada tanggal 10 hingga 11 Juli 2023. Software atau tool forensik ini juga memiliki kemampuan untuk mengelompokkan bukti secara otomatis sesuai dengan tipe datanya, yaitu Website History, Cached Images, dan Cached Web Pages.



Gambar 9. Diagram Website Visit berdasarkan tanggal

Analysis

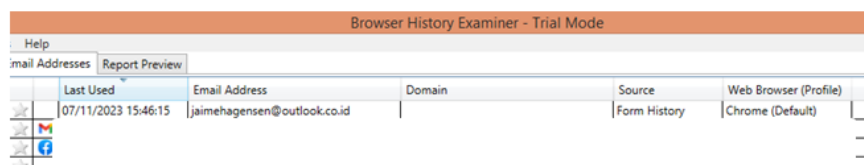
Tahap selanjutnya adalah menganalisa semua barang bukti dan data atau file-file yang telah terkumpul dengan penggunaan forensic tools yang lebih menyeluruh. Pada Browser History Viewer, jika tanda panah ditekan lebih lanjut, maka rincian detail tentang tanggal dan waktu terakhir megakses Facebook terpampang jelas.



Gambar 10. History Facebook

Menurut gambar 10, pengguna bernama Jaime Hagensen mengakses Facebook pertama kali pada tanggal 11 Juli 2023 pada pukul 15:51:13 siang. Lalu, di pukul 15:52:23, Jaime Hagensen meng-update status berisi tentang ajakan.

bermain game online bertema perang dengan selisih waktu 1 menit dan 10 detik. Jika melusuri Browser History Viewer lebih dalam, kredensial akun Jaime berupa email yang dipergunakan untuk sesi login di masa itu turut tercapture dengan timestamp 15:46:15 detik.



Gambar 11. Email login akun Jaime yang tercatat oleh tools forensik
Selanjutnya, memanfaatkan FTK Imager, analisa terhadap file .mem menunjukkan hasil sebagai berikut.

```

346125e0 10 00 00 00 00 00 00-08 00 00 00 00 00 00 | .....
346125f0 3E 00 00 00 1B 00 00 00-6A 00 61 00 69 00 6D 00 | >.....j-a-i-m
34612600 65 00 68 00 61 00 67 00-65 00 6E 00 73 00 65 00 | e-h-a-g-e-n-s-e
34612610 6E 00 40 00 6F 00 75 00-74 00 6C 00 6F 00 6F 00 | n@o-u-t-l-o-o-k
34612620 68 00 2E 00 63 00 6F 00-2E 00 69 00 64 00 00 00 | k..c.o.i.d
34612630 38 00 00 00 01 00 00 00-30 00 00 00 00 00 00 | s.....

```

Gambar 12. Email di Facebook browser chrome

Pada gambar 12, terlihat di offset 346125f0 sampai 34612630, serta binary hex 6A sampai 64 menunjukkan email atas nama jaimehagensen@outlook.co.id tercatat oleh proses RAM Imaging dipergunakan untuk login Facebook. Selanjutnya, untuk meneliti kredensial pelaku, turut dilakukan pula imaging dari perangkat telepon korban.

```

d2b7000 00 00 00 00 00 00 00-00 00 00 00 01 00 00 00 | .....
d2b7010 44 69 64 6E 27 74 20 67-65 74 20 74 68 61 74 2E | Didn't get that.
d2b7020 00 08 51 53 00 00 00 00-00 64 92 07 00 00 00 00 | ..QS.....d.....

```

Gambar 13. Salah satu komentar bully

```

6d76e020 68 00 74 00 74 00 70 00-73 00 3A 00 2F 00 2F 00 | h-t-t-p-s-:///.
6d76e030 77 00 77 00 77 00 2E 00-66 00 61 00 63 00 65 00 | w-w-w..f-a-c-e
6d76e040 62 00 6F 00 6F 00 6B 00-2E 00 63 00 6F 00 6D 00 | b-o-o-k..c-o-m
6d76e050 2F 00 6A 00 61 00 6B 00-65 00 2E 00 62 00 61 00 | /j-a-k-e..b-a
6d76e060 6E 00 6E 00 6F 00 6E 00-2E 00 37 00 37 00 37 00 | n-n-o-n..-7-7-7
6d76e070 33 00 00 00 00 00 00 00-00 00 00 00 00 00 00 | 3.....

```

Gambar 14. Alamat Facebook pelaku bully

Gambar 13 menunjukkan offset d2b7010 dengan binary hex 44 sampai 2E berisi tentang sepenggal komentar pada unggahan status korban. Lalu, offset 6d76e020 hingga 6d76e070 berisikan alamat facebook dari pelaku bully tersebut.

5. Kesimpulan

Dalam penelitian ini, dilakukan analisis forensik digital terhadap aktivitas cyber bullying pengguna Facebook melalui browser Chrome menggunakan metode Live Forensic. Tujuan penelitian adalah untuk mengumpulkan, menganalisis, dan mengevaluasi bukti digital yang terkait dengan penggunaan Facebook guna mendukung investigasi kasus kejahatan siber.

Melalui proses Live Forensic, data aktivitas penggunaan Facebook, seperti riwayat browsing, unggahan status, komentar, dan aktivitas lainnya, dianalisis secara mendalam. Metode Live Forensic memungkinkan pengumpulan bukti digital yang akurat dan terkini langsung dari perangkat yang masih aktif.

Hasil penelitian ini menunjukkan bahwa analisis forensik digital pada aktivitas penggunaan Facebook melalui browser Chrome dapat memberikan bukti-bukti yang signifikan dalam kasus kejahatan siber. Bukti digital yang ditemukan dapat digunakan sebagai alat pendukung valid dalam proses penyelidikan dan penuntutan hukum.

Kesimpulan dari penelitian ini adalah bahwa metode Live Forensic efektif dalam mengumpulkan dan menganalisis bukti digital terkait aktivitas penggunaan Facebook melalui browser Chrome. Penelitian ini memberikan kontribusi dalam pengembangan bidang forensik digital dan memberikan pemahaman yang lebih baik tentang cara mengungkap kejahatan siber yang terkait dengan penggunaan sosial media. Namun, perlu diingat bahwa analisis forensik digital harus dilakukan dengan memperhatikan aspek privasi dan hukum yang berlaku. Keberhasilan penelitian ini menyoroti pentingnya upaya penegakan hukum yang tepat dalam menghadapi tantangan kejahatan siber yang semakin kompleks di era digital ini. Live Forensic memiliki potensi besar untuk mendukung investigasi dan penegakan hukum dalam kasus kejahatan siber yang melibatkan platform media sosial.

6. Daftar Pustaka

- [1] "Social Media Users 2023 — (Global Demographics)." <https://www.demandsage.com/social-media-users/> (accessed Jul. 12, 2023).
- [2] I. Riadi, A. Yudhana, and M. Al Barra, "Forensik Mobile pada Layanan Media Sosial LinkedIn," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 6, no. 1, pp. 9–20, 2021, doi: 10.14421/jiska.2021.61-02.
- [3] N. Maulidya Jalal, M. Idris, and Muliana, "Faktor-Faktor Cyberbullying Pada Remaja," *J. IKRA-ITH Hum.*, vol. 5, no. 2, pp. 146–154, 2020.
- [4] Y. Winoto, "Remaja Dan Pandangannya Terhadap Cyberbullying Pada Media Facebook," *Commed J. Komun. dan Media*, vol. 3, no. 2, pp. 121–132, 2019, doi: 10.33884/commed.v3i2.980.
- [5] "Facebook Cyber Bullying - BRIM Anti-Bullying Software." <https://antibullyingsoftware.com/facebook-bullying/> (accessed Jul. 12, 2023).

- [6] 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.
- [7] S. D. Utami, C. Carudin, and A. A. Ridha, “Analisis Live Forensic Pada Whatsapp Web Untuk Pembuktian Kasus Penipuan Transaksi Elektronik,” *Cyber Secur. dan Forensik Digit.*, vol. 4, no. 1, pp. 24–32, 2021, doi: 10.14421/csecurity.2021.4.1.2416.
- [8] M. I. Syahib, I. Riadi, and R. Umar, “Analisis Forensik Digital Aplikasi Beetalk Untuk Penanganan Cybercrime Menggunakan Metode Nist,” *Semin. Nas. Inform. 2018 (semnasIF 2018)*, vol. 1, no. 1, pp. 134–139, 2018, [Online]. Available: <http://jurnal.upnyk.ac.id/index.php/semnasif/article/view/2629/2207>
- [9] “PPID Kabupaten Jember.” <https://ppid.jemberkab.go.id/berita-ppid/detail/pemberdayaan-masyarakat-perlindungan-hukum-terkait-informasi-dan-transaksi-elektronik> (accessed Jul. 13, 2023).
- [10] Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic Press.
- [11] Taylor, R. W., Fritsch, E. J., Liederbach, J., & Holt, T. J. (2014). *Digital crime and digital terrorism*. Pearson.