Jurnal Ilmiah Informatika (JIF)
| ISSN (Print) 2337-8379 | ISSN (Online) 2615-1049 |
Jurnal online di akses di http://ejournal.upbatam.ac.id/index.php/jif

Analisis Forensik Digital Pada Kasus Cyberbullying dengan Metode National Institute of Standard and Technology SP 800-86

Rahmat Novrianda Dasmen[1], Muhammad Reihan Pratama[2], Husni Yasir[3], Ariff Budiman[4]

[1234]Teknik Komputer Universitas Bina Darma, Jl. Jenderal Ahmad Yani No.3, Kota Palembang, Sumatera Selatan 30111, Indonesia

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima Redaksi: 12 Januari 2024
Revisi Akhir: 05 Maret 2024
Diterbitkan *Online*: 12 Maret 2024

KATA KUNCI

NIST, Autopsy, Flashdisk, Bukti, Digital Forensik

KORESPONDENSI

E-mail: rahmat_novrianda@binadarma.ac.id

A B S T R A C T

Rapidly developing technology is in line with criminal acts that have increased dramatically, one of the criminal acts that often occur in the digital world is cyberbullying, until the evidence of the event is successfully removed so that it is necessary to search and recover digital data that has been removed to be used as digital evidence, this process is commonly known as digital forensics. Investigation of digital evidence is carried out by applying one of the methods, namely the National Institute of Standard and Technology SP 800-86 (NIST SP 800-86) through stages starting from collecting evidence, analyzing, searching for data, and recovering found data, to validating files with digital flashdisk evidence sources using Autopsy forensic tools. The findings of this research indicate that the utilization of Autopsy is able to analyze and restore digital evidence previously stored on a flashdisk with a 100% success rate, the data that was successfully recovered consisted of 4 files with the PNG extension and 1 file with the MP4 extension according to the designed case scenario.

1. PENDAHULUAN

Dengan terus berkembangnya teknologi informasi yang secara signifikan, dampak positif yang dapat diperoleh dari perkembangan teknologi ialah mudahnya seseorang atau komunitas dalam melakukan komunikasi. Hal ini didasari dengan semakin banyak dan canggihnya platform untuk berkomunikasi yang tersedia sehingga membuat masyarakat dengan mudah menggunakannya [1]. Namun, terdapat pula dampak negatif yang timbul sebagai tindakan kejahatan siber akibat dari penyalahgunaan teknologi yang ada, hal ini tentunya sangat merugikan khalayak banyak [2]. Dengan ini membuat para pelaku kejahatan siber bergerak lebih cepat guna menembus sistem keamanan yang telah dibentuk oleh satgas tindak pidana siber sebelumnya. Dengan demikian, pola baru yang diterapkan pada kejahatan siber ini menjadi sedikit sulit untuk dipecahkan oleh para ahli digital forensik [3].

Salah satu kejahatan siber yang paling sering ditemukan ialah bullying di lingkungan digital yang pelakunya adalah para remaja, yang menjadi isu serius dan membutuhkan perhatian khusus karena semakin meningkat hingga saat ini dan sangat merugikan dari pihak yang di-bully [4]. Terkait dengan tindak kejahatan cyberbullying, selain bukti kesaksian dari saksi dan keterangan dari tersangka yang dapat membongkar kejahatan yang dilakukan, bukti digital juga mampu memberikan petunjuk mengenai tindak pidana yang telah terjadi [5]. Diperlukan sejumlah besar bukti digital yang dapat merinci dan menjelaskan kronologi suatu tindak pidana. Salah satu ciri dari bukti digital adalah dapat secara mudah diduplikasi, diubah, atau bahkan dihilangkan. Bukti digital ialah hasil dari proses pemulihan data dalam tahap penyidikan, data-data tersebut dapat berupa teks, file berbentuk gambar, video, atau rekaman suara, file dokumen, dan database dari media sosial yang telah terhapus [6].

Perlunya penerapan forensik digital guna mempermudah pengungkapan atau pembuktian terkait dengan tindak pidana cyberbullying terjadi, sehingga kejelasan dapat tercapai di dalam proses persidangan [7]. Penerapan digital forensik merupakan salah satu prosedur atau metode penyidikan yang digunakan dalam menghadapi kejahatan bullying di lingkungan digital dan mencari bukti-buktinya [8]. Secara jelas, digital forensik mengulas tentang sistem digital yang meninggalkan jejak data, serta suatu perkara yang dapat digali kembali untuk jadikan bukti digital dari kasus yang sedang diselidiki [9].

Dalam melakukan investigasi melalui forensik digital, terdapat beragam tools yang digunakan dalam melakukan analisis, pemulihan, dan ekstraksi bukti digital, yang dapat diperoleh melalui sumber-sumber gratis maupun yang memerlukan pembayaran [10]. Salah satu tools yang umum dan mudah digunakan dalam forensik digital ialah Autopsy untuk membantu mendukung jalanan proses pemulihan data dengan baik dan cepat [11], meskipun bersifat open-source Autopsy dapat bersaing dengan tools lain yang sejenis, bahkan kinerjanya dapat

mengungguli terutama pada proses pemulihan data dan menjaga integritas dari data yang berhasil dipulihkan [12]. Prinsip yang digunakan dalam forensik digital serupa dengan proses yang dilakukan oleh kepolisian dalam melakukan penyidikan. Akan tetapi, dalam forensik digital kejadian dan proses yang terjadi ada dalam dunia maya s[13].

2. TINJAUAN PUSTAKA

2.1 Forensik Digital atau yang juga biasa dikenal sebagai komputer forensik adalah investigasi terkait dengan informasi, data, dan aplikasi, termasuk data yang tercatat di dalam berkas log yang dilakukan dengan menggunakan suatu tools atau aplikasi tertentu dengan tujuan untuk mengumpulkan data dan jejak-jejak pelaku kejahatan yang tertinggal di dalam perangkat digital demi kepentingan hukum untuk membuktikan kejahatan komputer secara ilmiah [14].

2.2 Bukti Elektronik adalah bukti yang dapat dikenali melalui pengamatan visual, adapun beberapa perangkat yang dapat dijadikan bukti digital adalah sebagai berikut:

1. *Personal Computer*
2. *Notebook*
3. *Flashdisk*
4. *Harddisk*
5. *Smartphone* atau *Handphone*
6. Kamera Digital
7. CD/DVD

2.3 Bukti Digital ialah bukti yang diperoleh dari hasil ekstrak pada bukti elektronik, beberapa yang dapat dijadikan bukti elektronik adalah sebagai berikut:

1. File Logis
2. Berkas yang telah dihapus
3. Berkas yang hilang
4. Sisa berkas
5. Berkas catatan
6. Berkas terekripsi *(Office File, Video File, Image File, Audio File, Email, Sms, Mms, Dan Call Logs)*

2.4 Cyberbullying yaitu perilaku pembulian oleh individu atau kelompok sebagai pelaku melalui internet, khususnya di platform jejaring atau media sosial. Dalam cyberbullying pelaku melakukan intimidasi terhadap korban menggunakan media atau perangkat elektronik dengan maksud menimbulkan kerugian kepada pelaku atau mencari keuntungan demi memuaskan diri sendiri, dimana perbuatannya dilakukan secara terus menerus dan berulang kali. Tindakan yang dilakukan oleh pelaku baik secara individu maupun berkelompok melalui gambar, video, pesan teks dan sebagainya yang cenderung menghina dan merendahkan [15].

2.5 Tools Forensik dalam pelaksanaannya, peneliti membutuhkan alat atau tools yang digunakan untuk mendukung seluruh proses forensik yang dilakukan guna mendapatkan validitas nilai yang lebih tinggi terhadap bukti digital, pada penelitian ini tools yang digunakan ialah Autopsy. Autopsy sebagai sarana forensik digital yang berasal dari The Sleuth Kit, yang berfokus pada analisis terhadap sistem penyimpanan hingga melakukan recovery. Dengan menggunakan Autopsy, *application layer* berjalan tanpa perlu mengkhawatirkan akses file dan penyalinan data yang bersifat *intermitten* [16].

3. METODOLOGI

Metode yang diterapkan pada penelitian ini adalah National Institute of Standard and Technology (NIST) SP 800-86, dengan langkah-langkah dan skema kasus kejahatan seperti berikut.

3.1 Tahapan Penelitian

Tahapan dalam metode NIST SP 800-86 bisa dilihat pada Gambar 1 di bawah ini.

Gambar 1. Tahapan Metode NIST 800-86

Dari Gambar 1 di atas, metode yang dilakukan akan melalui 4 tahapan. Berawal dari *collection, examination, analysis*, sampai dengan *reporting* [17]. Subjek dalam penelitian ini adalah peneliti, adapun objek dari penelitian adalah kasus cyberbullying dengan sumber bukti digital dari flashdisk. Penjelasan lebih rinci dapat diuraikan sebagai berikut:

Metode yang diterapkan pada penelitian ini adalah National Institute of Standard and Technology (NIST) SP 800-86, dengan langkah-langkah dan skema tindak kejahatan yang dijelaskan seperti berikut.

a) *Collection*, pada tahapan ini terkait dengan pengumpulan dan pengamanan dari barang bukti yang selanjutnya akan digunakan untuk proses investigasi forensik, termasuk menjaga integritas datanya. Pada kasus ini, tahap collection dilakukan dengan mengamankan flashdisk yaitu media penyimpanan yang digunakan sebagai sumber bukti digital.
b) *Examination*, pada tahapan ini terkait dengan pemulihan atau perolehan kembali data digital yang telah terhapus dengan menggunakan Autopsy sebagai tools forensik.
c) *Analysis*, pada tahapan ini terkait dengan analisa data atau bukti digital yang berhasil ditemukan pada tahapan sebelumnya.
d) *Reporting*, adalah tahapan paling akhir yang menjelaskan proses atau langkah-langkah yang telah dilakukan sebelumnya hingga dapat ditarik kesimpulan.

3.2 Kebutuhan Hardware dan Software

Dalam mendukung proses penyelidikan dan penyidikan kasus kejahatan melalui analisis forensik digital. Diperlukan beberapa perangkat pendukung berupa hardware maupun software sehingga proses dapat berjalan dengan baik, sebagaimana dapat dijelaskan pada uraian berikut ini.

Tabel 1. Bahan Penelitian

No	Alat dan Software	Deskripsi
1	*Flashdisk* 64 GB	Obyek Penelitian
2	Laptop Asus LJ26V33T	Windows 10, 64 Bit, 4 GB RAM, Workstation Analisis Forensik
3	*Autopsy/The Sleuth Kit*	Tools Forensik

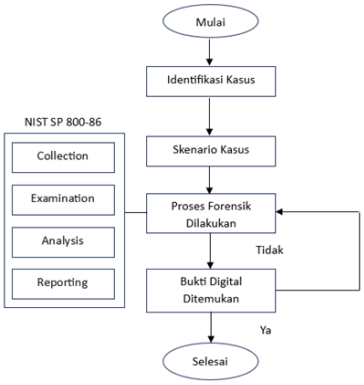
3.2 Skenario Kasus

Penyususan dan implementasi skenario kasus digunakan guna memperjelas dan merekonstruksi peristiwa kejahatan yang terjadi dengan melibatkan pelaku, saksi, dan korban di dalamnya. Maka dibuat lah suatu skenario kasus mengenai perundungan di dunia maya atau yang biasa dikenal sebagai cyberbullying, dengan menggunakan flashdisk sebagai sumber bukti digitalnya dan tools Autopsy sebagai alat yang digunakan untuk melakukan recovery data dan informasi dari flashdisk yang selanjutnya akan dijadikan bukti-bukti.

Berikut adalah tahapan-tahapan skenario yang dijalankan pada penelitian ini:

1. Skenario diawali dengan pelaku melakukan tindakan bullying kepada korban, peristiwa terjadi di lingkungan kampus Universitas Bina Darma dan kemudian peristiwa tersebut diketahui oleh saksi (peristiwa difoto dan direkam)
2. Pelaku sadar jika aksinya direkam dan saksi menyalin dokumentasi peristiwa tersebut ke dalam flashdisk.
3. Pelaku tertangkap CCTV mencuri flashdisk milik saksi dan dicurigai menghapus bukti dokumentasi dengan tipe file PNG dan MP4.
4. Setelah dilakukan interogasi, pelaku tidak memberikan keterangan yang sebenarnya, dengan keterangan yang selalu berubah.
5. Peneliti selanjutnya menyimpulkan untuk mencari bukti di flashdisk tetapi flashdisk yang diterima dalam keadaan sudah diformat. Sehingga tidak ada berkas yang dapat ditemukan.
6. Selanjutnya peneliti melakukan recovery data-data yang hilang tersebut guna menemukan bukti-bukti kejahatan pelaku dan memastikan kebenaran peristiwa yang terjadi.

Skema perlakuan kasus dengan menggunakan tools Autopsy dapat dilihat pada Gambar 2 berikut:



Gambar 2. Skema Simulasi Perlakuan Kasus Sesuai Dengan Skenario

Tools Autopsy digunakan untuk melakukan analisis, pencarian, dan juga pemulihan terhadap data atau informasi (bukti digital) yang telah terhapus dengan tahapan-tahapan skenario yang telah dirancang sebelumnya.

4. HASIL DAN PEMBAHASAN

Penelitian ini ialah hasil dari rekayasa kasus yang didasarkan pada skenario yang sudah direncanakan sebelum itu dengan mengangkat kasus cyberbullying yang dilakukan oleh seorang pelaku. Hasil penelitian dengan menggunakan metode *National Institute of Standard and Technology* SP 800-86 melalui 4 tahapan, yaitu *Collection, Examination, Analysis,* dan *Reporting*.

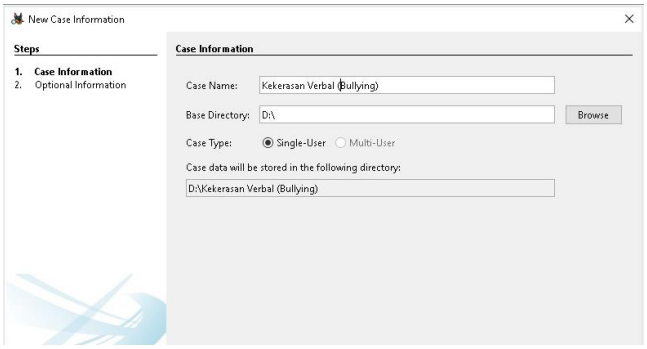
4.1 *Collection*

Pada tahapan ini terkait dengan pengumpulan barang bukti yaitu flashdisk dengan kapasitas 64 GB sebagai sumber bukti digital berasal, yang di dalamnya terdapat file yang sebelumnya telah dihapus. Adapun tujuan dari tahapan ini ialah agar sumber data yang dapat dijadikan bukti digital dapat diidentifikasi dan dianalisis. Berdasarkan skenario kasus, yaitu flashdisk dalam kondisi sudah diformat. Flashdisk memiliki bukti digital berupa 4 file ber-type PNG dan 1 file ber-type MP4 yang merupakan bukti dari kasus cyberbullying yang dijalankan oleh pelaku,

barang bukti flashdisk dapat dilihat pada Gambar 3.

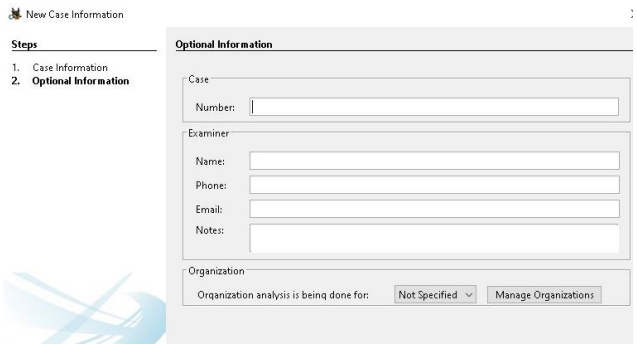
Gambar 3. *Flashdisk* Sebagai Sumber Bukti Digital

Selanjutnya dengan melalui laptop dengan spesifikasi yang telah ditentukan, peneliti menggunakan *Autopsy* sebagai tools forensik untuk melakukan akuisisi dan pemulihan data untuk dijadikan bukti digital yang sah. Namun terlebih dahulu untuk membuat *case database* dengan cara menginputkan *case information* dan *optional information* untuk lanjut ke tahapan *examination*. Tampilan input *case database* dapat dilihat pada Gambar 4 dan Gambar 5 berikut.



Gambar 4. Tampilan Input *Case Information*

Case information yang terdiri dari *case name, case directory, case type*

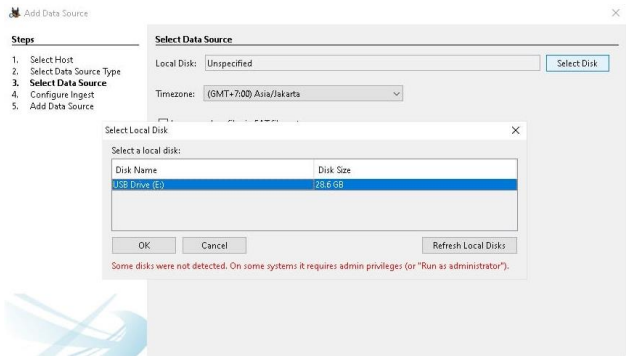


Gambar 5. Tampilan Input *Optional Information*

Optional information yang terdiri dari *case number*, *examiner name*, *examiner phone*, *examiner email*, dan *notes*.

4.2 *Examination*

Tahapan ini terkait dengan pemeriksaan data yang hilang dan untuk memperoleh kembali data yang sebelumnya tersimpan di dalam *flashdisk*. Sehingga dilakukan proses pemulihan data dari *flashdisk* dengan harapan dapat menjadi bukti digital yang valid. Proses *examination* dilakukan melalui *tools Autopsy* berdasarkan file *image*. Langkah awal pada tahap *examination* yaitu menghubungkan *flashdisk* yang akan dianalisa ke laptop, yang selanjutnya memilih *flashdisk* (USB Drive E) sebagai *data source* yang kemudian akan di-*recovery* data digitalnya, lihat Gambar 6.



Gambar 6. Proses Examination

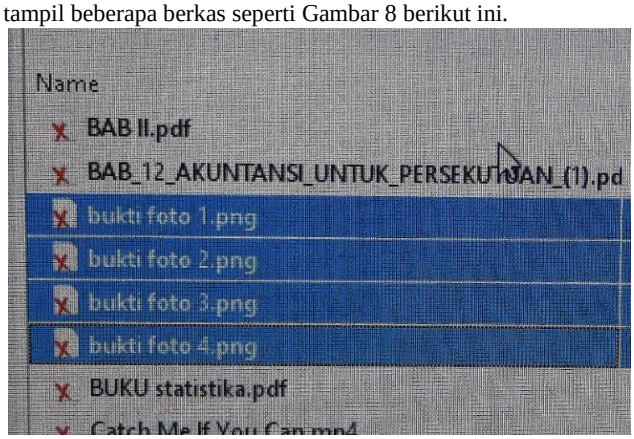
Setelah *flashdisk* terhubung dengan laptop, maka dilakukankan proses akuisisi hingga pemulihan data yang dilakukan oleh peneliti menggunakan *tools Autopsy*, sebagaimana pada Gambar 7 berikut ini.

Gambar 7. Proses Akuisisi Data Menggunakan *Autopsy*

Dilihat pada Gambar 7, bahwa proses akuisisi dan pemulihan data menggunakan *tools Autopsy* dapat membaca total 91 data file dari *flashdisk* dengan 5 data diantaranya merupakan bukti digital yang dicari, yang kemudian data tersebut akan di-ekstrak ke bentuk PNG dan MP4.

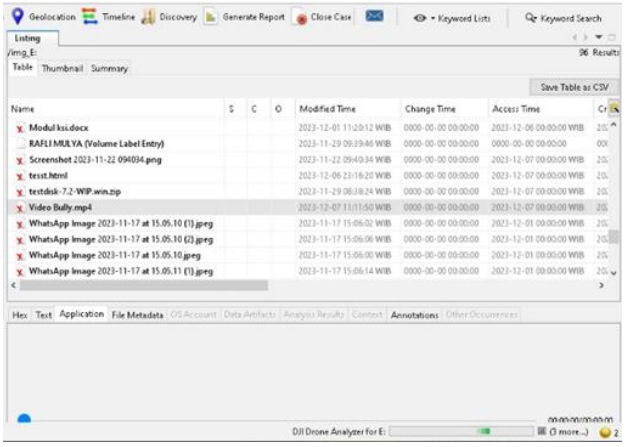
4.3 *Analysis*

Pada tahapan analisis ini terkait dengan proses mencari berkas sebagai bukti digital, berkas tersebut dapat dicari secara manual atau dengan menggunakan kata kunci. Setelah dilakukan penelurusan dengan menggunakan kata kunci "bukti foto" sesuai dengan nama berkas sebelum dilakukan penghapusan, maka akan tampil beberapa berkas seperti Gambar 8 berikut ini.



Gambar 8. File Bukti Dengan Ekstensi PNG

Pada Gambar 8, berkas yang ditemukan memiliki tipe file PNG dan dapat dikembalikan dengan kondisi yang baik, sedangkan untuk berkas yang memiliki tipe file MP4 dilakukan penelurusan secara manual, sesuai dengan nama berkas sebelum dilakukan penghapusan. Selanjutnya tampil seperti Gambar 9 di bawah ini



Gambar 9. File Bukti Dengan Ekstensi MP4

Pada Gambar 9, setelah dilakukan pencarian secara manual. Berkas dengan tipe file MP4 bisa didapatkan dengan mudah karena jumlahnya yang tidak banyak dan berkas tersebut pun dapat dikembalikan dengan kondisi yang baik dan juga utuh sehingga memudahkan peneliti saat akan melakukan validasi bukti digital. Bukti digital berupa foto dan video yang berhasil didapat dalam proses analisis yang membuktikan bahwa *Autopsy* mampu mendapatkan kembali atau melakukan pemulihan bukti digital dari dari *flashdisk* sebagai sumber awal bukti berada. Setelah melakukan pencarian terhadap berkas dan berkas ditemukan, selanjutnya berkas tersebut di-ekstrak ke dalam laptop yang digunakan sehingga dapat di-validasi keaslian berkasnya yang kemudian dapat dijadikan sebagai bukti digital dari *flashdisk* untuk membantu mengungkap kasus *cyberbullying* seperti pada skenario yang dibuat.

4.4 *Reporting*

Adapun hasil yang telah didapatkan setelah menerapkan metode NIST SP 800-86 sebagai langkah forensik digital untuk melakukan pencarian dan pemulihan bukti digital, dapat dilihat pada Tabel 2 di bawah ini.

Tabel 2. Hasil Penemuan Bukti Digital

Data	Tipe File	Jumlah Awal Data	Jumlah Data Ditemukan	Tingkat Keberhasilan (%)
Bukti Gambar	PNG	4	4	100%
Bukti Video	MP4	1	1	100%

Setelah semua proses forensik NIST dilakukan, selanjutnya semua data yang diperoleh dari hasil penelusuran barang bukti digital *cyberbullying* disusun dalam bentuk tabel, yang dapat dilihat pada Tabel 2.

Tabel 2 merupakan total temuan bukti digital dalam penelitian ini, yaitu sejumlah 5 berkas yang terdiri dari 4 bukti digital dengan ekstensi PNG dari 4 data asli gambar dan 1 bukti digital dengan ekstensi MP4 dari 1 data asli video sesuai dengan skenario dan kebutuhan penyidikan, juga telah dilakukan validasi bahwa berkas yang berhasil ditemukan dan dipulihkan adalah berkas yang cocok dengan berkas aslinya, untuk berkas yang minim ditemukan yaitu berkas dengan tipe file MP4 yang hanya berjumlah 1 file. Berdasarkan bukti digital terlihat bahwa keberhasilan pemulihan 100% untuk masing-masing bukti gambar dan bukti video. Keberhasilan yang mencapai lebih dari 85% bergantung pada pemilihan tools forensik dan juga kemampuan dari tools forensik yang digunakan

5. KESIMPULAN DAN SARAN

Berdasarkan temuan dan hasil yang diperoleh dari penelitian dengan skenario kasus cyberbullying melalui flashdisk sebagai sumber data dan Autopsy sebagai tools forensik yang digunakan, dengan metode Institute of Standard and Technology SP 800-86 untuk mendapatkan kembali bukti digital yaitu file foto dan video bukti terkait bullying yang telah disimulasikan. Bahwasanya secara keseluruhan tools Autopsy mampu melakukan pemulihan bukti digital flashdisk, yang pada penelitian ini tools tersebut dapat mengembalikan 5 berkas dari total 5 berkas yang dicari. Kemampuan Autopsy sebagai tools forensik mencapai 100% tingkat keberhasilan dalam menemukan bukti digital sesuai dengan parameter yang ditetapkan.

Saran untuk penelitian berikutnya adalah dengan mengidentifikasi skenario lain yang mungkin dilakukan oleh pelaku kriminal pada bukti digital serta dapat menambahkan tools forensik lainnya guna mengatasi tantangan penanganan bukti digital dan dapat membandingkan hasil yang didapatkan dalam penelitian, karena bukti digital yang ditangani harus sesuai dengan prosedur dan metode yang tepat, agar bukti yang diperoleh pada saat penelurusan menjadi legal dan dapat digunakan hingga proses persidangan.

DAFTAR PUSTAKA

[1] D. S. Z. Yao, Mengfan, Charalampos Chelmis, "Cyberbullying Ends Here: Towards Robust Detection of Cyberbullying in Social Media," *Web Conf. 2019 - Proc. World Wide Web Conf.*, pp. 3427–3433, 2019, [Online]. Available: https://doi.org/10.1145/3308558.3313462%0A

[2] M. Riskiyadi, "Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime," *Cyber Secur. dan Forensik Digit.*, vol. 3, no. 2, pp. 12–21, 2020, doi: 10.14421/csecurity.2020.3.2.2144.

[3] M. Nadhif Hermanto, Martanto, and Lin, "Analisis Forensic Berbasis Web Phising Menggunakan Metode National Institute of Standards and Technology," *Cipta Cendikia Kotabumi J. Inf. dan Komput.*, vol. 11, no. 1, pp. 116–123, 2023, [Online]. Available: https://www.dcckotabumi.ac.id/ojs/index.php/jik/article/view/311

[4] M. F. T. Palupi and F. Norhabiba, "Edukasi Literasi Digital pada Remaja dalam Menangkal Cyberbullying," *J. Abdidas*, vol. 2, no. 4, pp. 1014–1020, 2021, doi: 10.31004/abdidas.v2i4.408.

[5] M. Jubaidi, U. Muhamadiyah, and Y. Umy, "DAMPAK NEGATIF CYBERBULLYING SEBAGAI C-CRIME," vol. 12, no. 2, 2020.

[6] G. Fanani, I. Riadi, and A. Yudhana, "Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop," *J. Media Inform. Budidarma*, vol. 6, no. 2, p. 1263, 2022, doi: 10.30865/mib.v6i2.3946.

[7] S. Rizki and N. Nursiti, "Analisis digital forensic dalam mengungkapkan tindak kejahatan cyber pada tahap pembuktian," *J. Ilm. Mhs. Bid. Huk. pidana*, vol. 2, no. November, pp. 780–787, 2018, [Online]. Available: http://jim.unsyiah.ac.id/pidana/article/view/14618

[8] A. C. I. Agri Chairunisa Isradjuningtias and L. B. Pradana, "Pemanfaatan Digital Forensik Dalam Usaha Preventif Penumpasan Penyebaran Berita Bohong (Hoax)," *Postulat*, vol. 1, no. 2, pp. 51–55, 2023, doi: 10.37010/postulat.v1i2.1212.

[9] N. Aisyah *et al.*, "Analisa Perkembangan Digital Forensik Dalam Penyidikan Cybercrime Di Indonesia Secara Systematic Review," *J. Esensi Infokom J. Esensi Sist. Inf. dan Sist. Komput.*, vol. 6, no. 1, pp. 22–27, 2022, doi: 10.55886/infokom.v6i1.452.

[10] M. Machrush, A. Sirojjam Mushlich, M. Andik Izzuddin, and M. Ridwan, "Analisis Kinerja Aplikasi Forensik Open-Source Pada Ponsel Cerdas Berbasis Android dalam Mendapatkan Bukti Digital," *JII (Jurnal Inov. Inform. Univ. Pradita)*, vol. 6, no. 2, pp. 86–97, 2021.

[11] S. RACHMIE, "Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website," *Litigasi*, vol. 21, no. 21, pp. 104–127, 2020, doi: 10.23969/litigasi.v21i1.2388.

[12] A. Fitriadi and H. A. Tawakal, "Jurnal Informatika Terpadu," *J. Inform. Terpadu*, vol. 7, no. 2, pp. 62–69, 2021, [Online]. Available: https://journal.nurulfikri.ac.id/index.php/JIT

[13] R. M. Muria, A. Muntasa, M. Yusuf, and A. Hamzah, "Studi Litelatur: Peningkatan Kinerja Digital Forensik Dan Pencegahan Cyber Crime," *J. Apl. Teknol. Inf. dan Manaj.*, vol. 3, no. 1, pp. 12–20, 2022, doi: 10.31102/jatim.v3i1.1422.

[14] I. Riadi, S. Sunardi, and M. E. Rauli, "Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics," *J. Tek. Elektro*, vol. 10, no. 1, pp. 18–22, 2018, doi: 10.15294/jte.v10i1.14070.

[15] D. Riswanto and R. Marsinun, "Perilaku Cyberbullying Remaja di Media Sosial," *Analitika*, vol. 12, no. 2, pp. 98–111, 2020, doi: 10.31289/analitika.v12i2.3704.

[16] M. R. D. Qibriya, A. Ambarwati, and K. E. Susilo, "Analisis Forensik Digital Pada Aplikasi Instant Messaging Di Smartphone Berbasis Android Untuk Bukti Digital," *J. Teknol. Inf.*, vol. 5, no. 2, pp. 114–121, 2021, doi: 10.36294/jurti.v5i2.2200.

[17] M. W. Indriyanto, D. Hariyadi, and M. Habibi, "Investigasi Dan Analisis Forensik Digital Pada Percakapan Grup Whatsapp Menggunakan Nist Sp 800-86 Dan Support Vector Machine Digital Forensics Investigation and Analysis on Whatsapp Group Chats Using Nist Sp 800-86 and Support Vector Machine," *Cyber Secur. dan Forensik Digit.*, vol. 3, no. 2, pp. 34–38, 2020.

BIODATA PENULIS

Rahmat Novrianda Dasmen, S.T., M.Kom.
Dosen Program Studi Teknik Komputer
Universitas Bina Darma
Email: rahmat_novrianda@binadarma.ac.id

Muhammad Reihan Pratama
Mahasiswa Program Studi Teknik Komputer
Universitas Bina Darma.
Email: 211220003@student.binadarma.ac.id

Husni Yasir
Mahasiswa Program Studi Teknik Komputer
Universitas Bina Darma.
Email: 211220015@student.binadarma.ac.id

Ariff Budiman
Mahasiswa Program Studi Teknik Komputer
Universitas Bina Darma
Email: 211220005@student.binadarma.ac.id