(2026), 4 (1): 461-480 **Scientica** 3021-8209

Jurnal Ilmiah Sain dan Teknologi

ANALISIS FORENSIK DIGITAL MENGGUNAKAN TOOLS AUTOPSY PADA KASUS *CYBERBULLYING* DENGAN METODE ISO/IEC 27037 DAN ISO/IEC 27042

Dwi Alviany [1], Novi Safriadi [2], Alfian Abdul Jalid [3]

[#]Jurusan Informatika, Fakultas Teknik, Universitas Tanjungpura

Jl. Prof. Dr. Hadari Nawawi, Pontianak, Kalimantan Barat

[1] dwialviany30@gmail.com [2] safriadi@informatics.untan.ac.id

[3] fianjld@informatika.untan.ac.id

Abstrak

Cyberbullying merupakan kejahatan siber yang sering terjadi akibat meningkatnya intensitas penggunaan media sosial, tetapi penanganannya masih memiliki kendala terhadap integritas dan validitas dari bukti digital. Permasalahan yang utama dari investigasi *cyberbullying* adalah memastikan bagaimana bukti digital yang ditemukan tidak berubah, dapat diverifikasi, dan diterima dalam proses hukum. Penelitian ini memiliki tujuan untuk menganalisis efektifitas dari *tools* Autopsy dalam proses investigasi forensik digital pada proses *cyberbullying* dengan menerapkan standar ISO/IEC 27037 dan ISO/IEC 27042. Metode penelitian menggunakan pendekatan secara eksperimental dengan skenario *dummy case cyberbullying*. Bukti yang digunakan berupa *flashdisk* yang dianalisis melalui tahap identifikasi, akuisisi, pelestarian, analisis, dan interpretasi bukti. Hasil penelitian menunjukkan bahwa *tools* Autopsy terbukti mampu melakukan pemulihan dan analisis bukti digital secara efektif. Termasuk menampilkan metadata, *timeline*, serta bukti digital yang telah dihapus. Validitas dari bukti dibuktikan melalui *cross-validation* menggunakan *tools* FTK Imager dan review ahli/praktisi forensik digital. Penelitian ini menegaskan bahwa penerapan metode ISO/IEC 27037 dan ISO/IEC 27042 dengan *tools* Autopsy dapat menjamin integritas dan validitas bukti digital dalam penanganan kasus *cyberbullying*.

Sejarah Artikel

Submitted: 6 Februari 2026

Accepted: 9 Februari 2026

Published: 10 Februari 2026

Kata Kunci

Cyberbullying, Forensik Digital, Autopsy, ISO/IEC 27037, ISO/IEC 27042

I. PENDAHULUAN

Menurut survey yang dilakukan oleh (APJII) Asosiasi pengusaha Jasa Internet Indonesia pada tahun 2024, penggunaan internet didominasi pada *smartphone* yaitu sebanyak 89,44% [1]. Namun, perkembangan teknologi informasi yang sangat pesat memiliki dampak negatif bagi para penggunanya. Salah satunya yaitu, bocornya informasi pribadi dengan mudah [2]. Salah satu kejahatan *cyber* yang paling sering ditemui adalah kejahatan *cyberbullying*. Meningkatnya popularitas dari penggunaan sosial media mengakibatkan kejahatan *cyberbullying* semakin marak terjadi. Kebanyakan orang tidak sadar atau bahkan menormalisasi kejahatan *cyberbullying* disekitar mereka. *Cyberbullying* memiliki berbagai macam bentuk seperti, mengirimkan pesan-pesan amarah atau kasar, menyinggung, intimidasi, serta kata-kata kejam, mengirimkan informasi sensitif/pribadi seseorang, dan termasuk mengeluarkan seseorang dari grup online dengan sengaja dan dengan maksud membuli [3].

Maka dari itu, penerapan digital forensik adalah suatu motode yang dapat digunakan untuk menghadapi berbagai macam kejahatan *cyber*, salah satu contohnya adalah kejahatan *cyberbullying*. Digital Forensik adalah sistem yang dapat digunakan untuk mengulas sebuah sistem digital yang memiliki jejak data atau yang informasinya dapat digali kembali untuk dijadikan bukti digital [4]. Forensik digital perlu diterapkan untuk mempermudah menemukan bukti pada kasus kejahatan *cyber* khususnya *cyberbullying* agar didapatkan bukti yang jelas dalam proses persidangan [5]. Salah satu *tools* yang umum dan mudah digunakan untuk menangani investigasi forensik adalah Autopsy. Autopsy adalah aplikasi berbasis *open source* yang gratis tetapi peformanya tidak kalah unggul dengan *tools* lainnya yang berbayar karena

Autopsy juga dapat melakukan analisis dan pemulihan data, Autopsy juga dapat menjaga integritas dari bukti yang berhasil dipulihkan [6].

Pada penanganan forensik digital sendiri tentunya diperlukan prosedur atau metode yang tepat dan sesuai dengan kasus yang di investigasi. ISO/IEC (*International Organization for Standardization / International Electrotechnical Commission*) adalah standar yang diakui secara internasional dan memiliki pedoman yang komprehensif pada penanganan bukti digital khususnya ISO/IEC 27037 dan ISO/IEC 27042. Keunggulan penggunaan dari kedua metode tersebut adalah karena ISO/IEC 27037 adalah metode yang berfokus dalam tahap awal investigasi forensik yaitu tahap identifikasi, pengumpulan, akuisisi, serta pelestarian bukti agar integritas dan keaslian bukti terjaga selama proses investigasi [7]. Sedangkan metode ISO/IEC 27042 merupakan suatu metode yang memiliki fokus pada tahap analisis dan interpretasi bukti digital dengan cara mengatasi masalah dari kontinuitas, validitas, produktivitas, serta pengulangan [8]. Sehingga keduanya akan saling melengkapi dalam proses investigasi serta untuk memastikan proses investigasi yang komprehensif.

Penelitian ini akan menganalisis efektifitas dari penggunaan *tools* Autopsy pada proses investigasi forensik digital pada kasus *cyberbullying*. Penelitian ini juga akan menguji penerapan metode ISO/IEC 27037 pada tahap idnetifikasi, pengumpulan bukti, akuisisi, dan pelestarian bukti digital untuk menjaga integitas dan keaslian bukti dengan menggunakan *tools* Autopsy serta bagaimana penerapan metode ISO/IEC 27042 pada tahap analisis dan interpretasi bukti digital untuk menjaga kontinuitas, validitas, produktifitas, serta pengulangan terhadap kasus *cyberbullying*.

II. TINJAUAN PUSTAKA DAN DASAR TEORI

Menurut penelitian Dasmen, R. N., Pratama, M. R., Yasir, H., dan Budiman, A. tentang ‘Analisis Forensik Digital pada Kasus *Cyberbullying* dengan Metode *National Institute of Standard and Technology* (NIST) SP 800-86.’ yang dilakukan pada tahun 2024. Ditemukan bahwa *tools* Autopsy yang digunakan dalam penelitian ini berhasil memulihkan semua berkas yang terkait dengan kasus *cyberbullying* yang telah dihapus dengan baik [2].

Meskipun penelitian tersebut berhasil dengan menggunakan tools Autopsy yang di aplikasikan dengan metode NIST SP 800-86. Menurut Ramadhan, R. A., Setiawan, P. R., dan Hariyadi, D. pada tahun 2020, dilakukan penelitian yang berjudul ‘*Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037:2012 and NIST SP800-86 Framework*’ dibahas bahwa tiap standar memiliki kelebihan dan kekurangannya masing-masing. Penelitian ini menemukan bahwa ISO/IEC 27037 menejelaskan proses secara lebih rinci dibandingkan NIST SP800-86 [9].

Kemudian pada penelitian Baroto, W. A. yang dilakukan pada tahun 2024 dengan judul ‘Advancing Digital Forensic through Machine Learning : An Integrated Framework for Fraud Investigation’ dijelaskan bahwa ISO/IEC 27037 dan ISO/IEC 27042 serta *guidelines The International Fraud Handbook by Joseph T. Wells* (2018). Dijelaskan bahwa *framework* ISO/IEC 27037 dan ISO/IEC 27042 memiliki standar yang kemprehensif untuk penanganan *digital evidence,* memastikan proses digital forensik berjalan dengan sistematis, akurat, dan transparan. Kedua standar tersebut juga terbukti dapat menjaga integritas bukti serta memastikan hasil dari analisis dapat disampaikan secara efektif kepada semua pihak terkait [10].

A. Forensik Digital

Forensik Digital merupakan suatu teknik pengumpulan, analisis, serta pelaporan data digital yang biasanya digunakan untuk menyelidiki suatu perangkat digital dalam investigasi kejahatan *cyber*. Digital Forensik merupakan suatu prosedur investigasi menggunakan metode yang disusun untuk mengatur pelestarian, pengumpulan, validasi, identifikasi, analisis, interpretasi, dokumentasi, serta penyajian bukti digital, dari sumber digital untuk digunakan

dengan tujuan fasilitasi atau rekonstruksi peristiwa kriminal juga membantu mengantisipasi tindakan yang tidak sah dan mengganggu operasi yang telah direncanakan [11].

B. Tools Autopsy

Autopsy adalah sebuah *platform* yang bersifat *end-to-end open source.* Autopsy adalah salah satu *tools* investigasi *hard drive* yang cepat, menyeluruh, efisien, dan berkembang sesuai dengan kebutuhan [12]. Autopsy juga merupakan salah satu *tools* yang umum dan mudah penggunaannya dalam membantu proses investigasi khususnya pemulihan data dengan baik dan cepat. Meskipun *tools* Autopsy ini merupakan *tools open source*, tetapi Autopsy dapat bersaing dengan *tools* forensik lainnya yang sejenis. Bahkan kinerja dari Autopsy terbilang unggul dalam proses pemulihan data dan menjaga integritas data yang berhasil dipulihkannya [2].

C. Cyberbullying

Cyberbullying adalah suatu tindakan yang disengaja dan berulang-ulang dengan tujuan menyakiti orang lain melalui media elektronik. Dengan meningkatnya informasi dan data yang di *sharing* di dunia digital yang sedang berkembang, era baru sosialisasi melalui media digital dan popularitas dari social media mengakibatkan meningkatnya tindakan *cyberbullying* [13]. *Cyberbullying* memiliki beberapa bentuk, termasuk mengirimkan ujaran kemarahan, perkataan kasar atau menyinggung, intimidasi, hoax (berita palsu), berbagi informasi pribadi seseorang (*outing*), mengeluarkan seseorang dari grup *online* dengan sengaja, dan lain-lain [14].

D. ISO/IEC 27037

ISO/IEC 27037 merupakan sebuah panduan penanganan bukti digital yang berlaku dan diakui secara internasional. ISO/IEC 27037 diterbitkan pada tahun 2012 dan berisi tentang *Information Technology – Security Techniques – Guidelines for Identification*, *Collection*, *Acquisition*, dan *Preservation of Digital Evidence*. Panduan ini menjelaskan tentang apa saja yang harus dilakukan untuk penanganan awal dari data digital yang terkait dengan investigasi yang sedang dilakukan [15]. ISO/IEC 27037 memberikan panduan aktivitas dalam penanganan bukti digital, yaitu identifikasi, pengumpulan, perolehan, dan pelestarian bukti digital yang memiliki potensi untuk dijadikan bukti yang bernilai [16].

E. ISO/IEC 27042

ISO/IEC 27042 adalah standar yang berisi panduan tentang analisis dan interpretasi bukti digital dengan membahas kontinuitas, validitas, reproduktifitas, dan pengulangan. Panduan ini juga menjelaskan praktik untuk pemilihan, desain, dan implementasi proses dari analitis serta pencatatan mengenai informasi yang cukup untuk memungkinkan proses investigasi tunduk terhadap pengawasan independent bila diperlukan. Versi terbaru dari ISO/IEC 27042 ini adalah ISO/IEC 27042:2015 yang diterbitkan pada tahun 2015 [8].

F. FTK Imager

FTK Imager adalah *tools data preview* dan *imaging* yang dapat membantu menilai *electronic evidence* dengan cepat untuk menentukan apakah analisis lebih lanjut dengan *tools forensic* lainnya diperlukan atau tidak. FTK Imager juga dapat membuat *perfect copies* dari *images* forensik data komputer tanpa membuat perubahan pada bukti asli.

Untuk mencegah manipulasi bukti asli yang disengaja maupun tidak disengaja, FTK Imager membuat duplikat *image* dari media *bit-for-bit*. *Image* forensik identik dalam segala hal dengan *File* aslinya, termasuk *File slack* dan *unallocated space* atau *drive free space*. Hal ini memungkinkan untuk menyimpan media asli dengan aman dari bahaya saat investigasi berlangsung menggunakan *image* tersebut

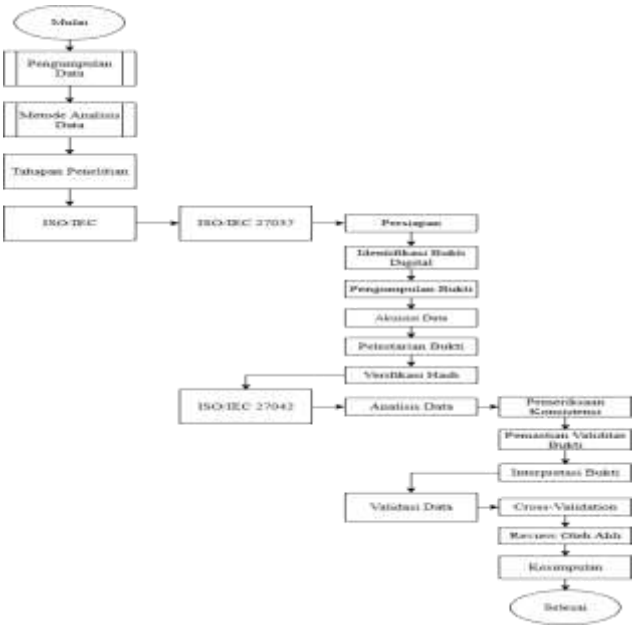
III. RANCANGAN PENELITIAN

Penelitian ini menggunakan pendekatan studi kasus yang dipadukan dengan metode eksperimen. Studi kasus memberikan keleluasaan kepada peneliti untuk menelaah masalah secara mendalam, kontekstual, dan komprehensif, sehingga setiap tahapan investigasi digital

dapat dianalisis secara rinci. Studi kasus dipilih karena penelitian berfokus pada satu permasalahan nyata, yaitu kasus cyberbullying, dengan tujuan memperoleh pemahaman yang mendalam mengenai proses investigasi digital. Sementara itu, metode eksperimen digunakan karena penelitian ini melibatkan proses uji coba secara langsung pada bukti digital dengan memanfaatkan perangkat lunak forensik, dalam hal ini Autopsy. Pendekatan studi kasus memungkinkan peneliti untuk mendeskripsikan serta mengevaluasi secara rinci bagaimana bukti digital dapat dikumpulkan, dipelihara, dianalisis, hingga divalidasi sesuai dengan standar internasional.

Selain itu, metode eksperimen digunakan untuk menguji dan membuktikan efektivitas penggunaan tools Autopsy dalam melakukan investigasi digital forensik. Dengan metode ini, peneliti dapat melakukan serangkaian percobaan langsung terhadap bukti digital yang diperoleh, sehingga hasil penelitian tidak hanya berupa teori atau konsep, tetapi juga didukung oleh data empiris yang nyata.

Dalam penelitian ini, penggunaan standar ISO/IEC 27037 dan ISO/IEC 27042 menjadi acuan metodologis utama. ISO/IEC 27037 menekankan pada tahap awal penanganan bukti digital, yakni mulai dari identifikasi, pengumpulan, akuisisi, hingga pelestarian. Dengan adanya pedoman ini, integritas serta keaslian bukti digital dapat dipertahankan sejak awal hingga akhir investigasi. Sedangkan ISO/IEC 27042 memberikan pedoman untuk proses lanjutan berupa analisis, interpretasi, serta pelaporan hasil investigasi. Standar ini memastikan bahwa bukti digital dapat dipahami secara tepat, dianalisis secara konsisten, dan mampu dipertanggungjawabkan di hadapan hukum. Berikut alur penelitiannya seperti yang ditunjukkan pada **Gambar. 1.**



Gambar. 1 Alur Penelitian

Rancangan penelitian ini dibangun dengan memperhatikan alur investigasi forensik digital yang sistematis. Mulai dari persiapan peralatan, identifikasi perangkat bukti, akuisisi data dengan metode yang sah, pelestarian hasil akuisisi, analisis dan interpretasi menggunakan *tools* Autopsy, hingga validasi hasil analisis melalui *cross-validation* dan *Review* ahli.

IV. HASIL DAN ANALISIS

A. *Identifikasi Perangkat yang Dianalisis*

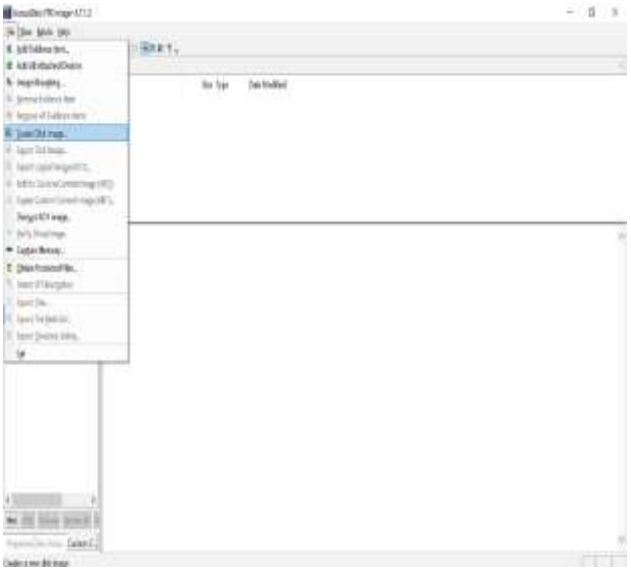
Penelitian ini menggunakan *device* berupa *flashdisk* Sandisk dengan kapasitas 8 GB yang sudah di sisipi *dummy case* berupa Gambar dengan format *file* PNG, *Screenshot* dengan format *file* JPG, serta Video dengan format *file* MP4 seperti yang ditunjukkan pada **Gambar. 2.**

Gambar. 2 *Flashdisk* yang Digunakan

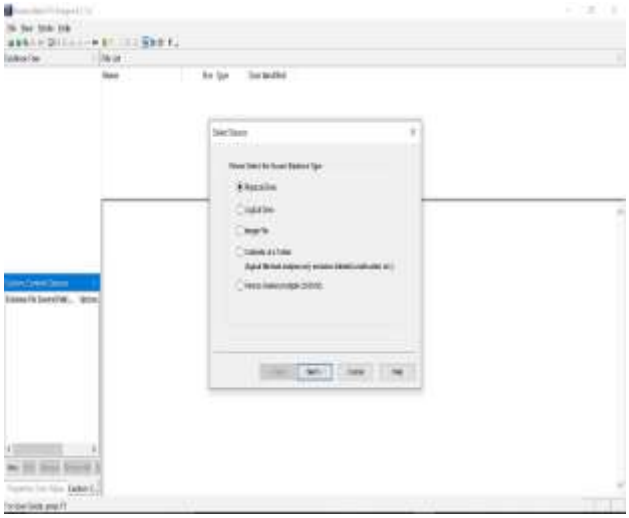
B. *Akuisisi Bukti Digital*

Akuisisi data atau yang bisa disebut dengan *cloning* bukti digital pada penelitian ini menggunakan tools tambahan yaitu FTK Imager untuk membantu proses akuisisi data agar integritas bukti terjaga.

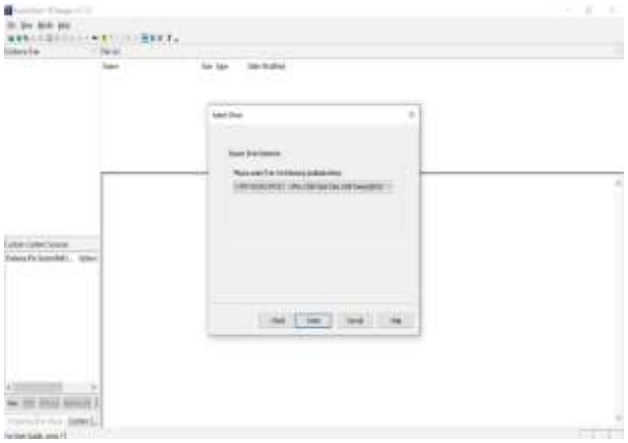
Proses akuisisi dengan FTK Imager dilakukan dengan cara Create Disk Image dan menyambungkan device yang terindikasi sebagai bukti terkait ke tools FTK Imager dengan memilih Physical Drive dan pilih Drive yang sesuai dengan drive yang digunakan seperti yang ditunjukkan pada **Gambar. 3, Gambar. 4, dan Gambar. 5**.



Gambar. 3 Bagian *File* pada FTK Imager

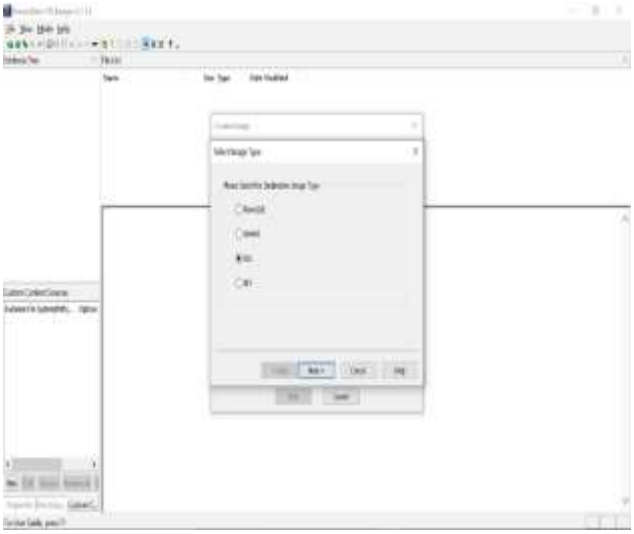


Gambar. 4 Halaman *Select Source* pada FTK Imager



Gambar. 5 Halaman *Select Drive* pada FTK Imager

Kemudian diproses menjadi *image file* dengan menambahkan '*add*' *type* 'E01' (*EnCase Image*) seperti yang ditunjukkan pada **Gambar. 6**, dengan tujuan agar dapat menghemat ruang penyimpanan dengan kompresi data tetapi tanpa mengubah bukti asli.

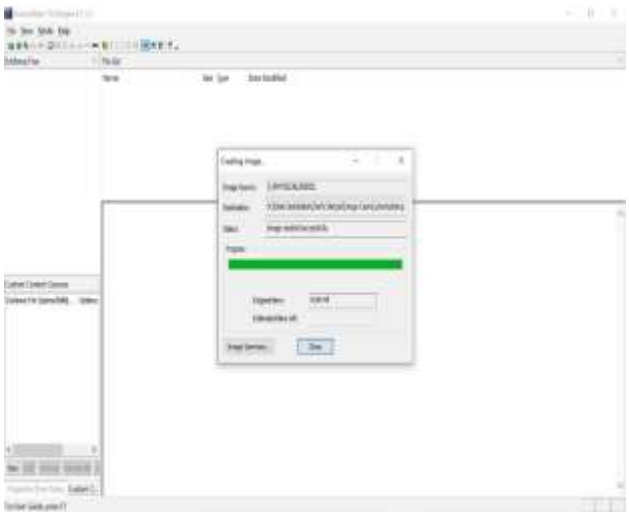


Gambar. 6 Halaman *Select Image File* pada FTK Imager

Setelah itu akan muncul *section* '*Evidence Item Information*' yang bersifat opsional, sehingga tidak wajib untuk diisi. Di *section* selanjutnya kita harus memilih *Image Destination* untuk menyimpan *file image* ke tempat yang kita inginkan. Kemudia atur nama *file* nya, dan *set Image Fragment Size* nya dnegan '0' agar *file image* yang dibuat tersimpan dalam satu *format file* dan tidak terpecah seperti yang ditunjukkan pada **Gambar. 7.** Lalu tekan '*finish*' dan pada saat kembali pada section *Creating Image* '*start*' maka *image file* berhasil dibuat Seperti tampilan pada **Gambar. 8** dan **Gambar. 9.**

Gambar. 7 Pengisian *Filename* dan *Image Fragmen Size* pada FTK Imager

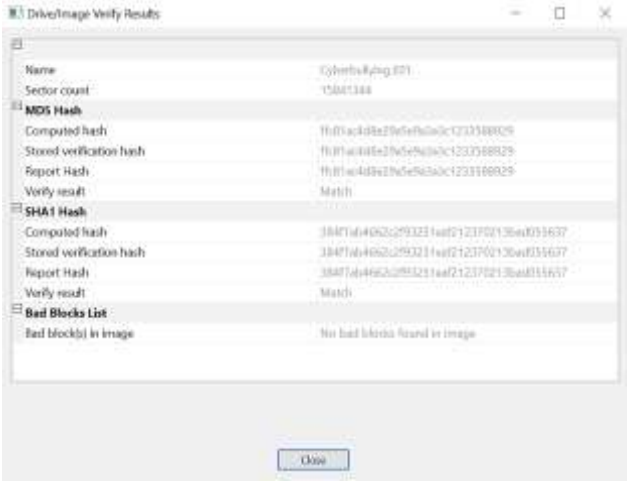
Gambar. 8 Halaman *Create Image* Setelah Ditambahkan *Image Destination* pada FTK Imager



Gambar. 9 Proses *Creating Image* Selesai pada FTK Imager

C. Verifikasi Integritas Bukti

Proses verifikasi integritas bukti dilakukan dengan metode *hashing* untuk memastikan data tidak berubah dari sebelum akuisisi hingga sesudah proses akuisisi. Proses *hashing* dipermudah karena FTK Imager sudah menyediakan fitur *Auto Hashing*, dimana hasil hashing akan langsung muncul setelah proses *creating image* selesai. FTK Imager menyediakan hashing MD5 dan SHA 1 seperti yang ditunjukkan pada **Gambar. 10**.

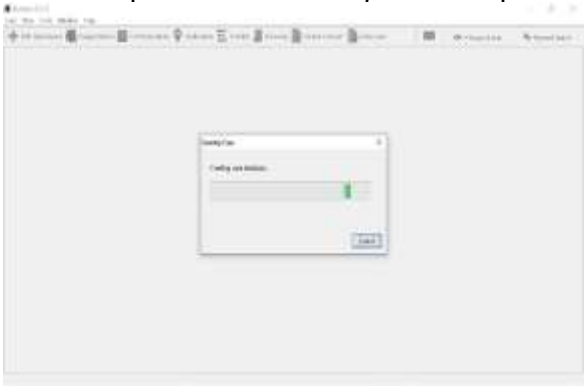


Gambar.10 Hasil *Hashing* MD5 dan SHA-1 pada FTK Imager

D. Analisis Data dengan Tools Autopsy

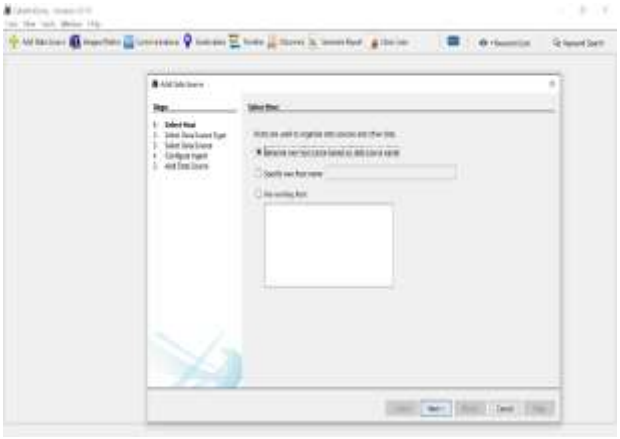
Proses analisis dimulai dengan memilih opsi 'New Case' pada menu awal yang ditampilkan saat membuka aplikasi Autopsy. Pada *page Case Information* isi kolom 'Case Name' dengan nama file yang diinginkan, kemudian tetapkan '*Base Directory*' untuk menetapkan dimana *database* kasus akan disimpan seperti yang ditunjukkan pada **Gambar. 11**. Setelah itu akan muncul *page* '*Optional Information*' dimana bagian ini bersifat *optional* sehingga kita tetap dapat melanjutkan proses meskipun *page* tersebut tidak diisi, lalu klik *finish* dan proses *creating case database* akan dimulai seperti pada **Gambar. 12**.

Gambar. 11 Tampilan *New Case Information* pada Autopsy

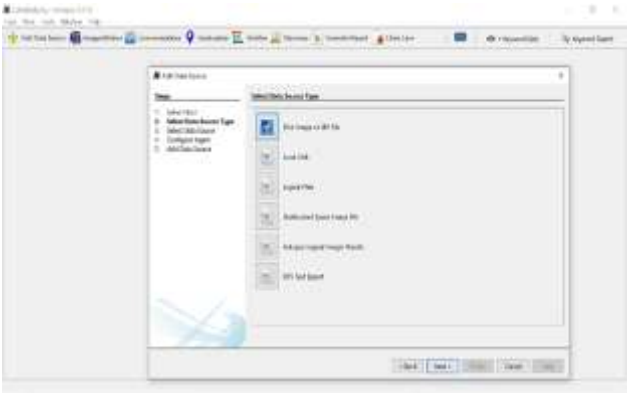


Gambar.12 Proses *Creating Case* pada Autopsy

Setelah proses pembuatan *case database* selesai, akan muncul *page* '*Select Host*' lalu pilih opsi '*Generate new host name based on data source name*' lalu klik *next* seperti pada **Gambar. 13**. Selanjutnya pada bagian *Select Data Source Type* pilih '*Disk Image or VM File*' seperti pada **Gambar. 14**.

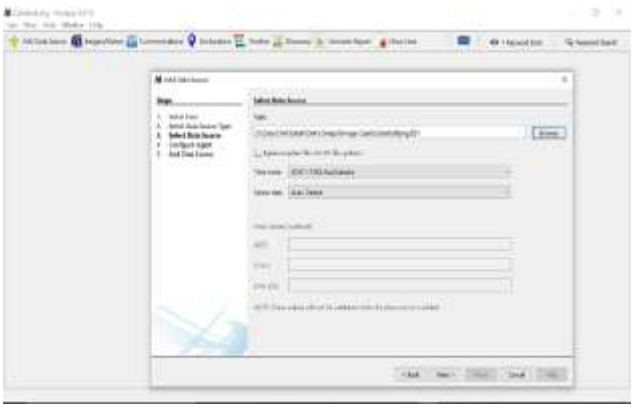


Gambar. 13 *Step Select Host* pada Autopsy

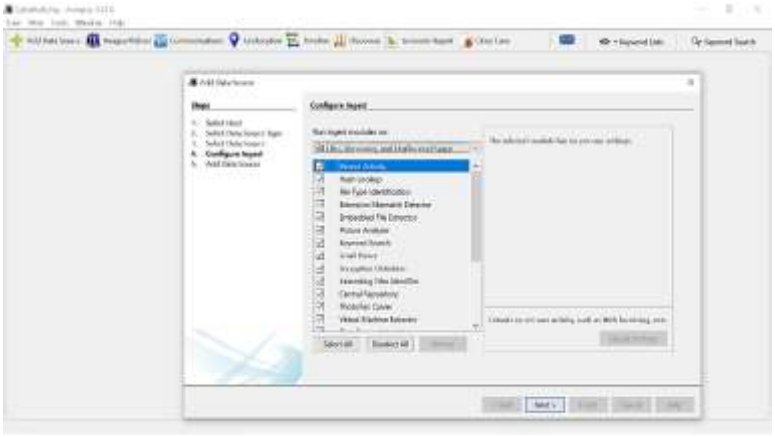


Gambar. 14 *Step Select Data Source Type* pada Autopsy

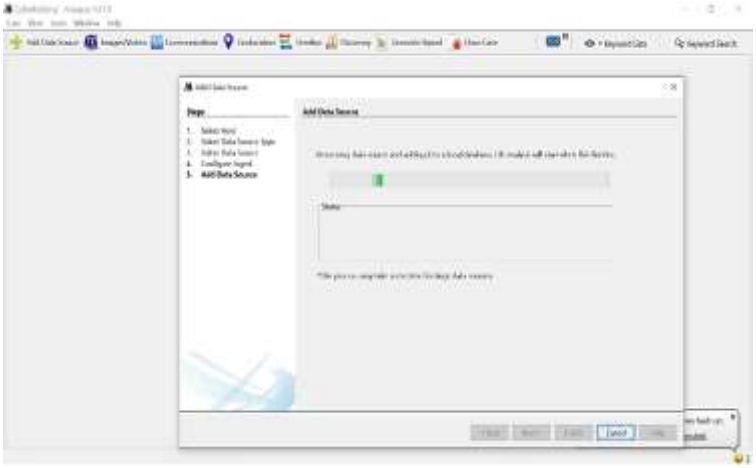
Kemudian akan muncul *page* '*Select Data Source*', masukkan *path* data kasus yang sudah diakuisisi sebelumnya lalu pilih *next* seperti pada **Gambar. 15**. Akan muncul *page Configure Ingest* lalu pilih '*Select All*' agar *image file* dianalisis secara menyeluruh dan lengkap kemudian klik *next* seperti pada **Gambar. 16.** Autopsy akan memulai proses penambahan Data Source ke local database yang sudah dibuat seperti pada **Gambar. 17** dan setelah selesai Autopsy akan memulai proses analisis image file secara otomatis seperti pada **Gambar. 18**. Jika proses analisis sudah selesai, investigasi dapat dimulai seperti pada **Gambar. 19**.



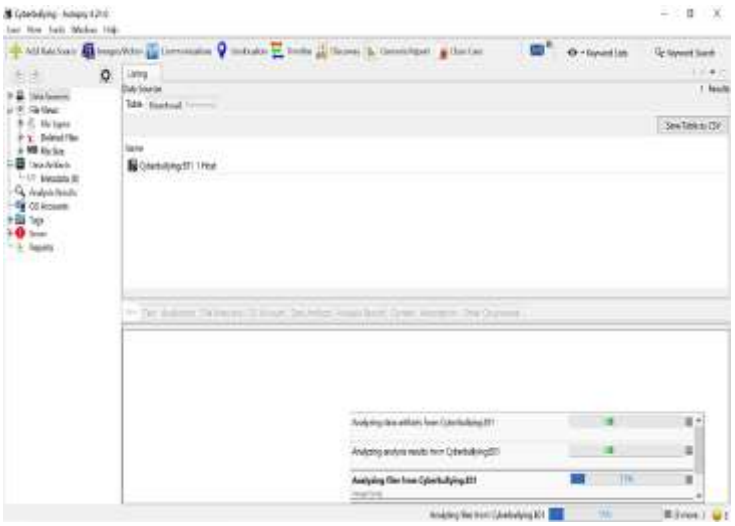
Gambar. 15 Tampilan Setelah *Data Source Path* ditentukan pada Autopsy



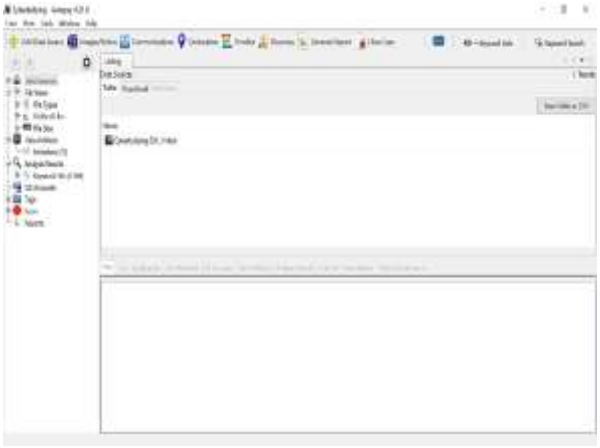
Gambar. 16 *Step Configure Ingest* pada Autopsy



Gambar. 17 Proses *Add Data Source* pada Autopsy



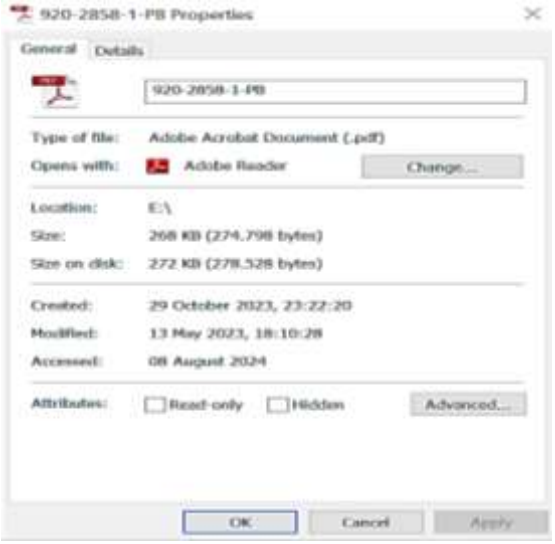
Gambar. 18 Proses *Analyzing Image* pada Autopsy



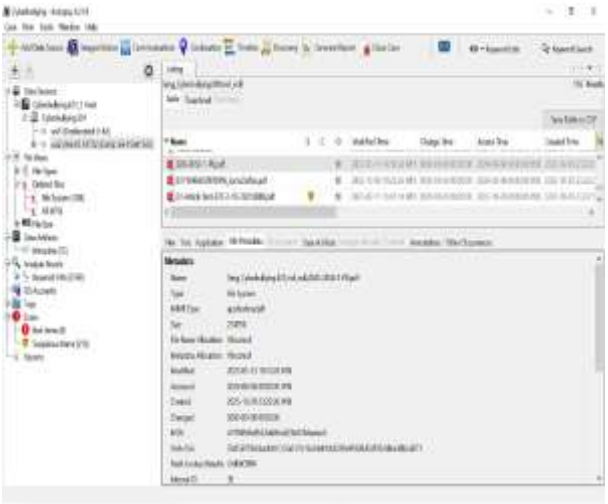
Gambar. 19 Tampilan Setelah Proses *Analyzing Image* Selesai pada Autopsy

E. Pemeriksaan Konsistensi Bukti

Tahap ini dilakukan dengan cara memeriksa kecocokan *timeline* menggunakan sample data asli dan data yang sudah diakuisisi pada autopsy untuk memastikan apakah data berubah atau tidak untuk pemeriksaan konsistensi bukti. Ditunjukkan pada **Gambar. 20** dan **Gambar. 21** serta **Tabel I**.



Gambar. 20 Informasi *Timeline File* Asli *Sample* (Konsistensi)



Gambar. 21 Informasi *Timeline File* Akuisisi *Sample* (Konsistensi)

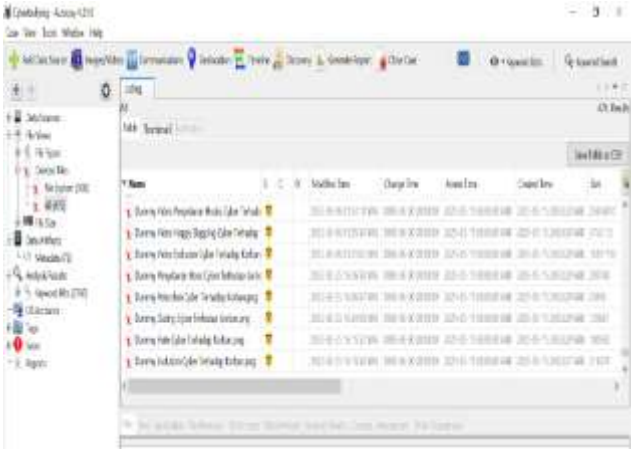
TABEL I
INFORMASI KONSISTENSI *TIMELINE FILE SAMPLE*

	Data Asli	Data Akuisisi
Created	29-10-2023 (23:22:20)	29-10-2023 (23:22:20)
Modified	13-05-2023 (18:10:28)	13-05-2023 (18:10:28)
Accessed	08-08-2024	08-08-2024

Gambar dan tabel diatas menunjukkan bahwa *Timeline file* data asli dan data yang sudah diakuisisi sama, artinya tidak terjadi perubahan data setelah proses akuisisi, Data akuisisi terbukti konsisten.

F. Metadata yang Ditemukan

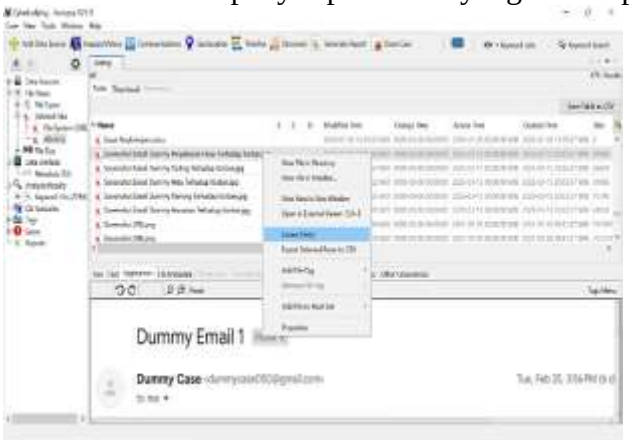
Pada bagian ini, metadata file yang sudah dihapus pada device yang di analisis dapat dengan mudah ditemukan pada bagian '*Deleted Files*', metadata yang ditemukan akan muncul seperti pada **Gambar. 22**.



Gambar. 22 Metadata yang Ditemukan

G. Pemulihan File Relevan yang Dihapus

Pemulihan *file* yang telah dihapus dilakukan dengan cara memilih *file* yang ingin dipulihkan pada Autopsy, lalu klik kanan dan pilih opsi '*Extract File*(s)' seperti yang ditunjukkan pada **Gambar. 23.** Kemudian tentukan lokasi penyimpanan file yang akan dipulihkan dan klik *save.*



Gambar. 23 Proses *Extract File*(s) pada Autopsy

Setelah data berhasil dipulihkan, akan muncul informasi bahwa *file* tersebut sudah berhasil di ekstraksi. *File* yang telah berhasil dipulihkan tersebut akan langsung tersimpan dan muncul di folder penyimpanan yang telah ditentukan, seperti yang terlihat pada **Gambar. 24**.

Gambar. 24 *File* Berhasil di *Recovery* pada Perangkat

H. Analisis Bukti yang Ditemukan

Bukti yang berhasil ditemukan menggunakan *tools* Autopsy berupa *file* Gambar dengan format .PNG, Video dengan format .MP4, dan tangkapan layar atau Screenshot dengan format .JPG dan berhasil dipulihkan dari *flashdisk*. Berdasarkan hasil *recovery*, setiap artefak memiliki metadata yang konsisten dengan waktu kejadian yang disimulasikan dalam penelitian. Sesuai hasil dari analisis, berikut bukti yang berhasil ditemukan menggunakan *tools* Autopsy seperti yang ditunjukkan pada **Tabel II.**

TABEL II
BUKTI YANG DITEMUKAN

Bukti	Format	Jumlah
Gambar	PNG	5
Video	MP4	3
Screenshot	JPG	5

I. Analisis Timeline yang Ditemukan

Analisis timeline dilakukan dengan tujuan untuk memahami hubungan antar-artefak digital berdasarkan data waktu yang terekam pada metadata yang berisi *created*, *modified*, dan *accessed time.* Berikut dijelaskan pada **Tabel III, Tabel IV,** dan **Tabel V.**

TABEL III
ANALISIS TIMELINE GAMBAR

File	Modified	Accessed	Created
Gambar 1	25-02-2025 16:36:58 WIB	15-03-2025	15-03-2025 20:03:29 WIB
Gambar 2	25-02-2025 16:36:04 WIB	15-03-2025	15-03-2025 20:03:29 WIB
Gambar 3	25-02-2025 16:34:08 WIB	15-03-2025	15-03-2025 20:03:29 WIB

Gambar 4	25-02-2025 16:15:52 WIB	15-03-2025	15-03-2025 20:03:29 WIB
Gambar 5	25-02-2025 16:18:36 WIB	15-03-2025	15-03-2025 20:03:27 WIB

TABEL IV
ANALISIS TIMELINE VIDEO

File	Modified	Accessed	Created
Video 1	06-03-2025 01:24:18 WIB	15-03-2025	15-03-2025 20:03:32 WIB
Video 2	06-03-2025 01:25:56 WIB	15-03-2025	15-03-2025 20:03:30 WIB
Video 3	06-03-2025 01:23:02 WIB	15-03-2025	15-03-2025 20:03:29 WIB

TABEL V
ANALISIS TIMELINE SCREENSHOT

File	Modified	Accessed	Created
Screenshot 1	03-03-2025 14:05:28 WIB	15-03-2025	15-03-2025 20:03:37 WIB
Screenshot 2	03-03-2025 14:06:32 WIB	15-03-2025	15-03-2025 20:03:37 WIB
Screenshot 3	03-03-2025 14:06:52 WIB	15-03-2025	15-03-2025 20:03:37 WIB
Screenshot 4	03-03-2025 14:05:56 WIB	15-03-2025	15-03-2025 20:03:37 WIB
Screenshot 5	03-03-2025 14:05:00 WIB	15-03-2025	15-03-2025 20:03:37 WIB

J. Pola Komunikasi Berdasarkan Timeline

Sesuai dengan hasil analisis yang dilakukan pada *tools* Autopsy, pola komunikasi dari pelaku pada *device* berupa *flashdisk* terkait kasus *cyberbullying* yang di teliti ditunjukkan pada **Tabel VI** :

TABEL VI
POLA KOMUNIKASI BERDASARKAN TIMELINE

Tanggal	Jumlah	Keterangan
25-02-2025	5	Gambar (PNG)
03-03-2025	5	*Screenshot Email* (JPG)
06-03-2025	3	Video (MP4)

Dari hasil pengolahan Timeline pada *tools* Autopsy, diperoleh tiga fase utama aktivitas yang dilakukan oleh pelaku, sebagai berikut:

Fase Pertama, dilakukan pada 25 Februari 2025. File gambar (format .PNG) menunjukkan waktu modifikasi pada tanggal 25 Februari 2025 dan akses serta kemungkinan dipindahkan ke flashdisk pada tanggal 15 Maret 2025. Aktivitas ini menunjukkan bahwa pelaku melakukan editing terhadap konten gambar yang mengandung unsur penghinaan terhadap korban. Pola waktu yang mengindikasikan proses perencanaan dan penyusunan materi cyberbullying secara bertahap.

Fase Kedua, dilakukan pada 3 Maret 2025. Pada fase ini ditemukan lima *File* tangkapan layar (*screenshot*) berformat .JPG yang memiliki *timestamp* berurutan setelah fase pembuatan gambar. Berdasarkan metadata waktu modifikasi (*Modified Time*) yang dilakukan pada tanggal 3 Maret 2025 dan kemudian di akses dan di buat/pindahkan ke flashdisk pada tanggal 15 Maret 2025. Pola waktu yang berdekatan ini menunjukkan bahwa pelaku aktif melakukan aktivitas digital yang terkait dengan konten sebelumnya.

Fase Ketiga, dilakukan pada 6 Maret 2025. *File* video dengan format .MP4 menunjukkan waktu pengambilan yang lebih baru dibandingkan *File* gambar dan tangkapan layar (*screenshot*). Hal ini menandakan bahwa pelaku telah melanjutkan aksinya ke tahap penyebaran konten dan interaksi daring. Perpindahan dari aktivitas pembuatan konten ke aktivitas penyebaran menunjukkan eskalasi perilaku pelaku dalam kurun waktu yang sama.

Secara keseluruhan, *timeline* membuktikan adanya alur kronologis dari setiap tindakan pelaku, mulai dari pembuatan konten, pembuatan video, hingga penyebaran.

K. Pola Komunikasi Berdasarkan Visual

Analisis yang dilakukan menunjukkan bahwa unggahan visual dilakukan secara berulang dalam periode yang sama, sehingga menandakan bahwa adanya intensitas komunikasi yang konsisten terhadap korban. Selain itu, hasil dari *screenshot* yang ditemukan menunjukkan interaksi pelaku dengan korban/pengguna lain, sehingga memperkuat bukti bahwa komunikasi tidak berhenti pada level pembuatan konten saja, tetapi berlanjut pada penyebaran. Hal ini menggambarkan pola komunikasi dimana pelaku memanfaatkan penggunaan media visual untuk membangun narasi penghinaan. Secara keseluruhan, hasil dari analisis menunjukkan bahwa pola komunikasi secara visual yang dilakukan oleh pelaku bersifat terstruktur, berulang, dan intensional, bukan merupakan tindakan incidental. Media visual digunakan bukan hanya sebagai ekspresi, tetapi juga sebagai instrumen komunikasi yang dirancang untuk mempermalukan korban.

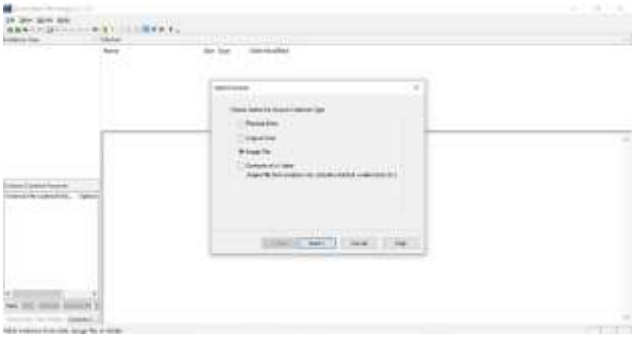
Pelaku membuat gambar yang diedit berunsur *bullying* berupa hinaan, ejekan, serta penyebaran informasi palsu atau hoax. Terlihat juga bahwa pelaku menyimpan *screenshot* email yang dikirimkannya secara anonim kepada penerima/korban dengan berbagai macam

ujaran hinaan, kebencian, ancaman, serta pelecehan. Terakhir, pelaku juga membuat video *bullying* yang berisikan pembulian terhadap korban. Analisis dari hasil menunjukkan bahwa metadata yang diperoleh memiliki keterkaitan langsung dengan aktivitas pelaku. Misalnya, *modified time* pada *file screenshot* sama dengan waktu unggahan konten yang mengandung ujaran kebencian. Konsistensi dari hasil *hashing* antara *file* asli dan *file* hasil akuisisi membuktikan bahwa integritas bukti terjaga.

L. Cross-Validation

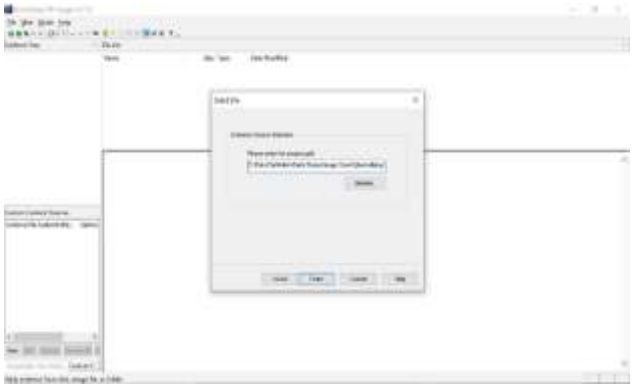
Cross-Validation atau pengecekan ulang dilakukan dengan cara mengecek kembali data yang telah dianalisis pada *tools* Autopsy dengan cara menganalisisnya pada *tools* forensik lain untuk memastikan konsistensi dari hasil analisis. Penelitian ini menggunakan *tools* FTK Imager sebagai aplikasi pembanding.

Pertama-tama pilih '*Add Evidence Item*' pada bagian *file* di aplikasi FTK Imager. Pilih '*Image File*' pada page *select source* yang muncul, lalu klik *next* seperti **Gambar. 25**.

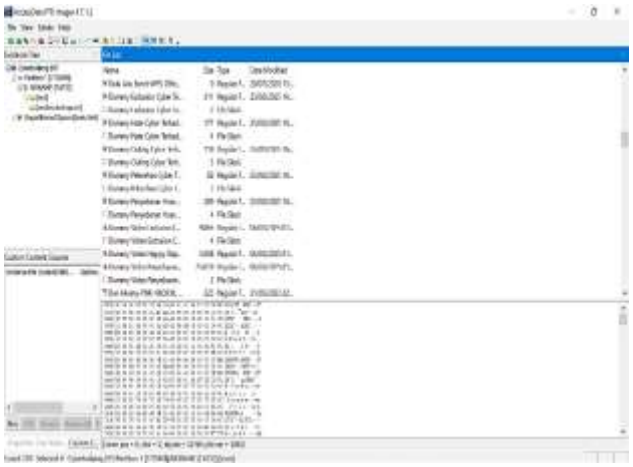


Gambar. 25 Halaman *Select Source* pada FTK Imager

Setelah itu pilih *image file* yang sama dengan yang digunakan pada proses analisis menggunakan *tools* Autopsy, kemudian klik *finish* untuk memulai proses *cross-validation* pada *tools* FTK Imager seperti yang ditunjukkan pada **Gambar. 26**. Hasilnya akan muncul seperti pada **Gambar. 27**.

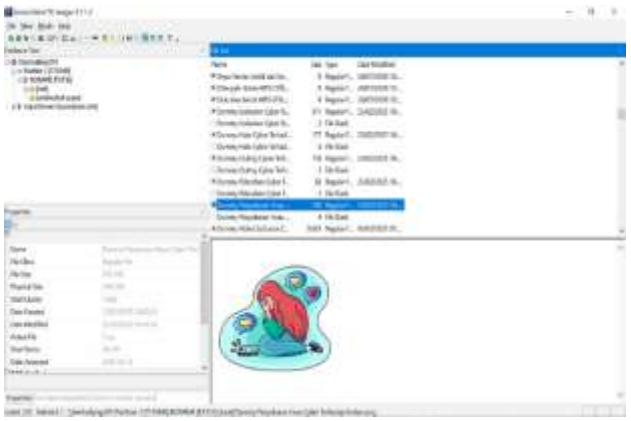


Gambar. 26 Halaman *Select File* pada FTK Imager

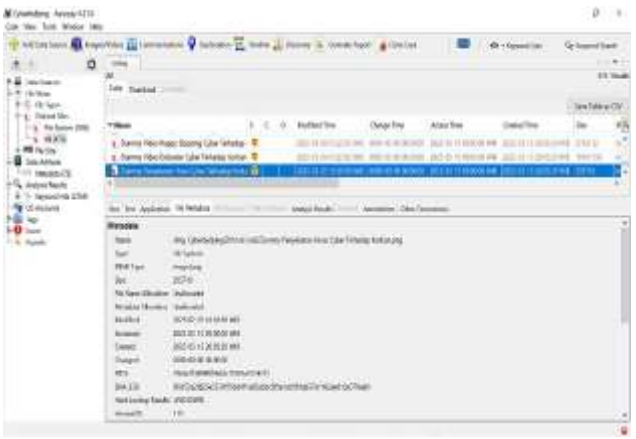


Gambar. 27 Halaman Analisis pada FTK Imager

Berikut hasil dari Cross-Validation data yang dilakukan dengan menggunakan *tools* forensik FTK Imager yang dibandingkan dengan *tools* Autopsy.



Gambar. 28 *Cross-Validation* FTK Imager



Gambar. 29 *Cross-Validation* Autopsy

TABEL VII
CROSS-VALIDATION

Timeline	FTK Imager	Autopsy
Modified	25-02-2025 16:36:58 WIB	25-02-2025 16:36:58 WIB
Accessed	-	15-03-2025
Created	15-03-2025 20:03:29 WIB	15-03-2025 20:03:29 WIB

V. KESIMPULAN

Berdasarkan hasil dari penelitian dan analisis yang telah dilakukan, didapatkan kesimpulan bahwa: *Tools* Autopsy telah terbukti efektif untuk digunakan dalam proses investigasi forensik digital khususnya pada kasus *cyberbullying*. Autopsy terbukti dapat menemukan *file* yang telah dihapus, mengidentifikasi, serta me-*Recovery file* yang relevan dengan kasus yang sedang di investigasi seperti gambar, video, dan *screenshot* dengan format PNG, MP4, dan JPG.

Penerapan ISO/IEC 27037 pada proses identifikasi, pengumpulan bukti, akuisisi serta pelestarian bukti telah terbukti berhasil menjaga integritas dan keaslian bukti yang diperoleh pada penelitian. Kemudian penerapan ISO/IEC 27042 pada proses analisis dan interpretasi bukti memungkinkan investigasi dan interpretasi bukti dilakukan dengan sistematis dengan menjaga kontinuitas dan validitas.

Validasi bukti yang dilakukan dengan metode *cross-validation* menggunakan *tools* FTK Imager, serta *review* oleh ahli/praktisi forensik digital membuktikan bahwa investigasi atau penelitian yang telah dilakukan memenuhi syarat investigasi yaitu, dengan tercapainya validitas, kontinuitas, dan replikasi, sehingga data yang dikumpulkan dapat digunakan sebagai bukti yang diterima dalam proses hukum.

REFERENSI

[1] Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), "Survei Penetrasi Internet Indonesia," *Asosiasi Penyelenggara Jasa Internet Indonesia (APJII)*, 2024. https://survei.apjii.or.id/survei/group/9

[2] R. N. Dasmen, M. R. Pratama, H. Yasir, and A. Budiman, "Analisis Forensik Digital Pada Kasus Cyberbullying Dengan Metode National Institute of Standard and Technology Sp 800-86," *J. Ilm. Inform.*, vol. 12, no. 01, pp. 68–73, 2024, doi: 10.33884/jif.v12i01.8344.

[3] G. Gohal *et al.*, "Prevalence and related risks of cyberbullying and its effects on adolescent," *BMC Psychiatry*, vol. 23, no. 1, pp. 1–10, 2023, doi: 10.1186/s12888-023-04542-0.

[4] N. Iman, A. Susanto, and R. Inggi, "Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review)," *J. Telekomun. dan Komput.*, vol. 9, no. 3, p. 186, 2020, doi: 10.22441/incomtech.v9i3.7210.

[5] 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.

[6] R. N. Dasmen, A. Rahman, A. Dwi, and M. Saputra, "Analisis Digital Forensik Recovery File yang Terhapus Menggunakan Tools Autopsy Dengan Metode National Institute Of Justice," *J. Ilm. Komputasi*, vol. 23, no. 2, pp. 213–218, 2024, doi: 10.32409/jikstik.23.2.3553.

[7] A. FFaizal and A. Luthfi, "Comparison Study of NIST SP 800-86 and ISO/IEC 27037

Standards as A Framework for Digital Forensic Evidence Analysis," *J. Inf. Syst. Informatics*, vol. 6, no. 2, pp. 701–718, 2024, doi: 10.51519/journalisi.v6i2.717.
[8] ISO, "ISO/IEC 27042:2015," *ISO*, 2021. https://www.iso.org/standard/44406.html
[9] R. A. Ramadhan, P. Rachmat Setiawan, and D. Hariyadi, "Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037:2012 and NIST SP800-86 Framework," *IT J. Res. Dev.*, vol. 6, no. 2, pp. 162–168, 2022, doi: 10.25299/itjrd.2022.8968.
[10] W. A. Baroto, "Advancing Digital Forensic through Machine Learning: An Integrated Framework for Fraud Investigation," *Asia Pacific Fraud J.*, vol. 9, no. 1, pp. 1–16, 2024, doi: 10.21532/apfjournal.v9i1.346.
[11] N. Nasirudin, S. Sunardi, and I. Riadi, "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express," *J. Inform. Univ. Pamulang*, vol. 5, no. 1, p. 89, 2020, doi: 10.32493/informatika.v5i1.4578.
[12] Autopsy, "About Autopsy," *SLEUTH KIT LABS*, 2025. https://www.autopsy.com/about/
[13] J. M. Mart and J. A. Casas, "Parental Supervision : Predictive Variables of Positive Involvement in Cyberbullying Prevention," 2021.
[14] M. Aljaffer, K. Alshehri, M. Almutairi, A. Aljumaiah, A. Alfraiji, and M. Hakami, "Cyberbullying among young Saudi online gamers and its relation to depression.," *J. Nat. Sci. Med.*, vol. 4, pp. 142–147, 2020, doi: 10.4103/JNSM.JNSM_78_20.
[15] V. Veronika and B. H. Simanjuntak, "Implementasi Iso 27037 Dalam Pemeriksaan Investigatif Dengan Teknik Forensik Digital Untuk Memperoleh Bukti Audit Di Badan Pemeriksa Keuangan (Bpk)," *J. Magister Akunt. Trisakti*, vol. 9, no. 2, pp. 89–104, 2022, doi: 10.25105/jmat.v9i2.13343.
[16] ISO, "ISO/IEC 27037:2012," *ISO*, 2023. https://www.iso.org/standard/44381.html