Journal of Computer Science and Technology
Volume 3 ; Nomor 2 ; May 2025 ; Page 112-126
DOI : https://doi.org/10.59435/jocstec.v3i2.436
https://jurnal.padangtekno.com/index.php/jocstec
E-ISSN : 2985-4318
P-ISSN : 2985-5772

Analisis Forensik Aplikasi Telegram Menggunakan Metode Digital Forensics Research Workshop

Baiq Widari Datu Samara[1*], Ahmad Subki[2], M.Zulpahmi[3], Lalu Delsi Samsumar[4]

[1234]Teknologi Informasi, Universitas Teknologi Mataram,
[1]sbaiqwidaridatu@gmail.com, [2]ahmad.subki1992@gmail.com, [3]pahmijorge04@gmail.com, [4] samsumarld@utmmataram.ac.id

Abstrak

Telegram telah menjadi salah satu aplikasi komunikasi yang populer namun juga sering disalahgunakan untuk aktivitas kriminal. Dalam upaya mengungkap kejahatan digital yang dilakukan melalui Telegram, metode Digital Forensic Research Workshop (DFRWS) diterapkan untuk memastikan integritas dan akurasi dalam pengumpulan, analisis, dan pelaporan bukti digital. Penelitian ini menggunakan dua alat forensik, yaitu MOBILedit Forensic Express dan DB Browser for SQLite dalam mengumpulkan bukti digital dari aplikasi Telegram. Hasil penelitian menunjukkan bahwa MOBILedit Forensic Express berhasil menemukan 40% dari total barang bukti yang diharapkan, yaitu berupa file video dan gambar. Sementara itu, DB Browser for SQLite berhasil mengumpulkan 20% dari total barang bukti yang diharapkan, yaitu berupa data kontak pelaku.

Kata kunci : Telegram, DFRWS, MOBILedit Forensic Express, DB Browser For SQLite

Abstract

Telegram has become a popular communication application but is also often misused for criminal activities. In an effort to uncover digital crimes committed via Telegram, the Digital Forensic Research Workshop (DFRWS) method was applied to ensure integrity and accuracy in the collection, analysis and reporting of digital evidence. This research uses two forensic tools, namely MOBILedit Forensic Express and DB Browser for SQLite to collect digital evidence from the Telegram application. The research results show that MOBILedit Forensic Express succeeded in finding 40% of the total expected evidence, namely in the form of video and image files. Meanwhile, DB Browser for SQLite succeeded in collecting 20% of the total expected evidence, namely in the form of the perpetrator's contact data.

Keywords : *Telegram, DFRWS, MOBILedit Forensic Express, DB Browser For SQLite*

PENDAHULUAN

Pada tahun 2024, penggunaan *smartphone* telah berkembang menjadi kebutuhan gaya hidup dan sangat populer di Indonesia, dengan sekitar 278,7 juta orang yang memiliki *smartphone* sebagai konektivitas seluler, dengan sekitar 353,3 juta orang yang memiliki lebih dari satu *smartphone*. Sekitar 185,3 juta orang di Indonesia adalah pengguna internet, dan 139,0 juta orang di Indonesia aktif menggunakan media sosial, terutama untuk *chatting*. (*we are social* & *hootsuite*, 2024)

Seiring dengan meningkatnya kebutuhan akan smartphone, maka perkembangan aplikasi Android, termasuk aplikasi pesan singkat (instant messenger) sebagai media komunikasi chatting pun semakin meningkat. Di Indonesia apilkasi pesan instan seperti Telegram telah menjadi salah satu alat komunikasi utama bagi banyak orang. Telegram menawarkan fitur-fitur canggih seperti enkripsi end-to-end, obrolan grup, people nearby, dan berbagi berkas, yang membuatnya populer di antara

pengguna yang peduli tentang privasi dan keamanan.

Berdasarkan data dari similiarweb.com, Aplikasi Telegram menempati urutan ke 6 di Indonesia, dan masih masuk sepuluh besar. Namun, muncul tantangan baru terkait keamanan digital dan privasi informasi. Banyak kasus kejahatan seperti pencemaran nama baik, penyebaran konten ilegal, dan bahkan rencana kejahatan yang disusun melalui platform Telegram. Oleh karena itu, penting untuk memiliki kemampuan untuk melakukan analisis forensik pada aplikasi Telegram untuk mendukung penyelidikan kriminal dan pemulihan bukti digital.

Pada penelitian ini peneliti menggunakan Metode Digital Forensics Research Workshop (DFRWS). Metode ini merupakan pendekatan sistematis untuk melakukan investigasi digital yang telah terbukti efektif dalam banyak kasus forensik digital serta menggabungkan teknik-teknik klasik dan terkini dalam analisis forensik digital untuk mengumpulkan, menganalisis, dan menyajikan bukti digital dengan cara yang sah dan dapat diterima di pengadilan.

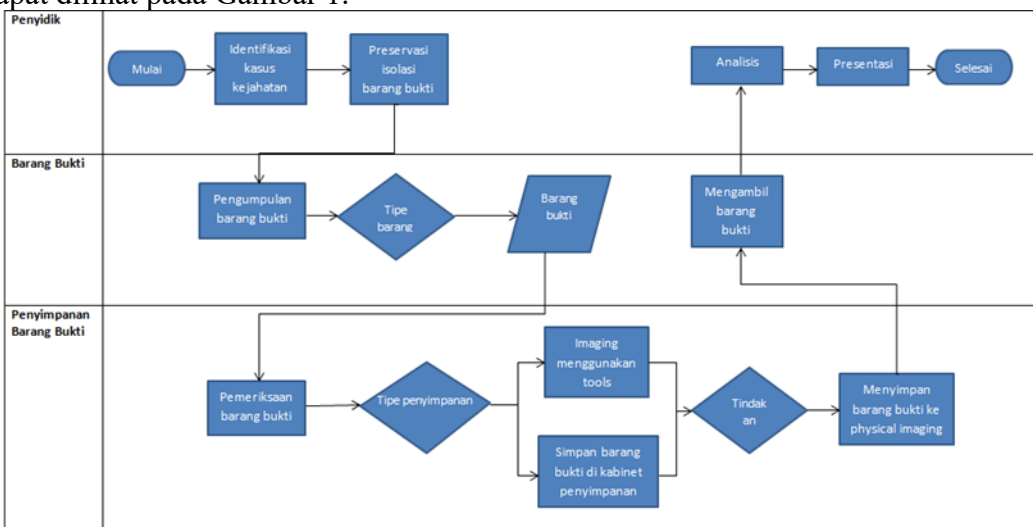
Tujuan dari penelitian ini adalah untuk melakukan analisis forensik pada aplikasi pesan instan Telegram menggunakan alat forensik MOBILedit Forensics Express dan DB Browser For SQLite. Adapun tools Kali Linux digunakan sebagai penetrasi testing dalam kasus penyerangan phishing pada aplikasi Telegram.

Penelitian serupa dilakukan dengan judul "Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop (DFRWS)" penelitian ini bertujuan untuk melakukan analisis forensik aplikasi pesan instan MiChat untuk bukti forensik dalam kasus perdagangan narkoba (drug traficking).

METODOLOGI PENELITIAN

Dalam penelitian berjudul "Analisis Kejahatan Aplikasi Telegram menggunakan Metode *Digital Forensics Research Workshop*" ini, digunakan metode penelitian kualitatif yang mendalam untuk mengungkap potensi kejahatan yang terjadi melalui aplikasi Telegram. Metode ini memungkinkan peneliti untuk melakukan analisis mendetail terhadap data digital yang diperoleh, seperti pesan, metadata, dan jejak aktivitas pengguna.

Adapun metode pengujian yang digunakan dalam penelitian ini yaitu menggunakan Metode *Digital Forensic Research Workshop* (DFRWS). Proses-proses yang dijelaskan dalam Metode DFRWS dapat dilihat pada Gambar 1.



Gambar 1. Alur Kerja Metode *Digital Forensic Research Workshop*

Diagram yang tercantum dalam Gambar 1 menjelaskan langkah-langkah penerapan metode

Digital Forensics Research Workshop (DFRWS) yang akan dilakukan oleh peneliti dalam proses penyelidikan bukti terkait kasus *phishing* pada aplikasi Telegram. Terdapat enam tahapan dalam metode *Digital Forensics Research Workshop* (DFRWS) yang diuraikan sebagai berikut :

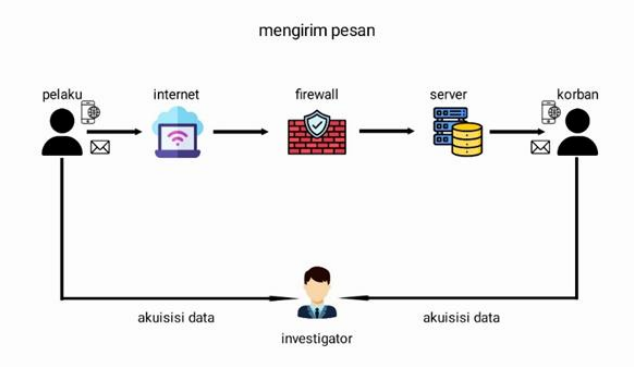
1. Identifikasi: Pada tahap ini, dilakukan proses identifikasi terhadap kasus kejahatan dan objek penelitian yang menjadi bukti kasus kejahatan di Aplikasi Telegram oleh peneliti. Informasi awal yang akan diidentifikasi yaitu mencakup jenis kejahatan, jenis perangkat yang menjadi bukti, spesifikasi perangkat, dan versi Aplikasi Telegram yang digunakan pada perangkat.
2. Pemeliharaan: Tahap Pemeliharaan dilakukan untuk menjaga keaslian barang bukti digital. Untuk memastikan bahwa perangkat tidak berinteraksi dengan jaringan atau pengguna lain, peneliti akan menggunakan mode pesawat.
3. Pengumpulan: Tahap Pengumpulan melibatkan identifikasi akuisisi sumber data oleh peneliti. Peneliti menggunakan *tools MobilEdit Forensic Express* untuk mengekstrak data bukti digital. Kemudian data bukti yang telah diekstrak dikumpulkan.
4. Pemeriksaan: Pada tahap pemeriksaan, seluruh data yang terkumpul akan diperiksa dengan cara *imaging* bukti digital, validasi barang bukti, dan penyimpanan barang bukti.
5. Analisis: Data yang telah diekstraksi pada tahap pemeriksaan akan dianalisis dan dikoneksikan satu sama lain sesuai dengan metode penelitian.
6. Presentasi: Tahap Presentasi melibatkan penyajian hasil analisis secara rinci, jelas, dan informatif.

Berbagai perangkat yang digunakan dalam penelitian ini mencakup *smartphone* Samsung *Galaxy* J5 *Pro*, laptop HP *DESKTOP*-H34ONLH dengan prosesor Intel(R) Celeron(R) N4500 @ 1.10GHz 1.10 GHz, dan kabel konektor USB. Aplikasi Telegram, *MOBILedit Forensic Express,* dan *DB Browser For SQLite* digunakan sebagai perangkat lunak pendukung untuk penelitian forensik ini. Untuk mempermudah pengambilan data dari perangkat Android, diperlukan proses *root* pada *smartphone* Samsung *Galaxy* J5 *Pro*.

Tabel 1. Alat dan Bahan Penelitian

No.	Alat dan *Software*	Deskripsi
1.	Samsung *Galaxy* J5 *Pro*	*Rooted*, Objek Penelitian
2.	Laptop HP	*Windows 11*, 64 *Bit*, 4 GB *Ram*, *Workstation Analisis Forensik*
3.	USB *Connector*	Koneksi *Smartphone* dan *Workstation*
4.	*Telegram Messenger*	*Software Test*
5.	*MOBILedit Forensic Express Pro*	*Tools Forensics*
6.	*DB Browser For SQLite*	*Tools Forensics*

Berikut simulasi kasus kejahatan antara pelaku dan korban di Aplikasi Telegram. Pada gambar 2 dapat dilihat proses komunikasi korban dan pelaku dalam mengirim pesan.



Gambar 2. Skenario Investigasi Kasus

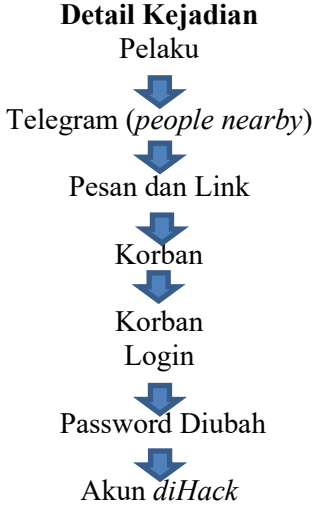
Gambar 2 menjelaskan adanya dua pengguna perangkat seluler yang berinteraksi melalui Telegram dengan terhubung ke jaringan internet. Pelaku menggunakan fitur Friendly Nearby untuk menemukan korban. Setelah menemukan korban, pelaku akan mulai mengirimkan pesan kepada korban melalui jaringan internet yang kemudian akan sampai pada server lalu terkirim ke korban. Dari tindak kriminal tersebut, investigator melakukan proses akuisisi data untuk mengidentifikasi barang bukti.

HASIL DAN PEMBAHASAN

1. Hasil Identifikasi

A. Deskripsi Kejadian

Pada Hari Sabtu, 13 Juli 2024 korban melalui Aplikasi Telegram mendapatkan pesan dari pelaku yang mengaku sebagai karyawan XL dan menawarkan promo paket kuota. Pelaku lalu mengirimkan link yang harus diklik dan korban harus log in akun Instagram agar bisa mengklaim paket kuota tersebut. Namun, setelah log in tidak terjadi apapun dan korban mendapat kabar dari temannya bahwa akun korban dihack. Ketika korban akan mencoba membuka akun Instagram sudah tidak bisa. Karena kata sandi sudah dirubah oleh pelaku. Pelaku menyebarkan pesan promosi judi online kepada para followers akun korban.



Gambar 3. Alur Kasus

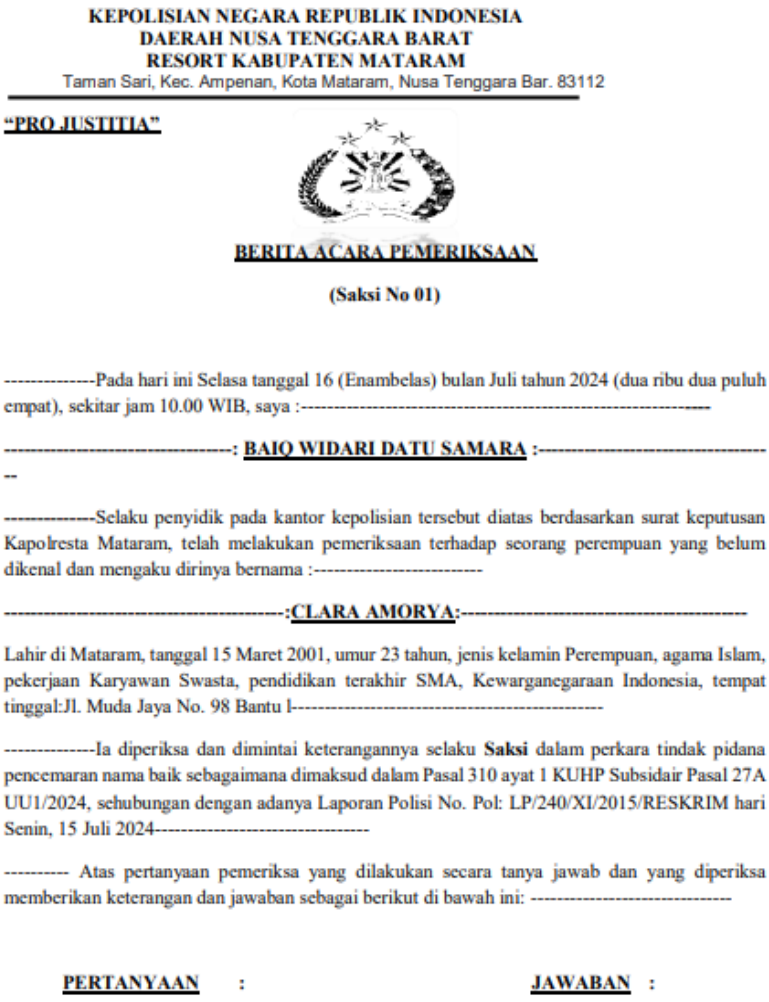
Berdasarkan keterangan pada gambar 3 teridentifikasi bahwa penjelasan kejadian yang dipaparkan korban mengarah pada serangan *phishing* yang menyebabkan pencemaran nama baik korban.

B. Ringkasan Skenario Kasus

Topik	:	Serangan *Phishing*
Requestor	:	Kepolisian
Petugas Penyidik	:	Peneliti/penulis
Objek Penyidik	:	Korban
Pihak Yang Terlibat	:	Clara Amorya (korban)
Alat Bukti Elektronik	:	1 Unit *Smartphone*

C. Berita Acara Pemeriksaan

Berikut rincian isi dari Berita Acara Pemeriksaan (BAP) yang diajukan kepada saksi (korban) kasus penyerangan *phishing* :



KEPOLISIAN NEGARA REPUBLIK INDONESIA
DAERAH NUSA TENGGARA BARAT
RESORT KABUPATEN MATARAM
Taman Sari, Kec. Ampenan, Kota Mataram, Nusa Tenggara Bar. 83112

"PRO JUSTITIA"

BERITA ACARA PEMERIKSAAN

(Saksi No 01)

----------Pada hari ini Selasa tanggal 16 (Enambelas) bulan Juli tahun 2024 (dua ribu dua puluh empat), sekitar jam 10.00 WIB, saya :----------

----------: **BAIQ WIDARI DATU SAMARA** :----------

----------Selaku penyidik pada kantor kepolisian tersebut diatas berdasarkan surat keputusan Kapolresta Mataram, telah melakukan pemeriksaan terhadap seorang perempuan yang belum dikenal dan mengaku dirinya bernama :----------

----------:**CLARA AMORYA**:----------

Lahir di Mataram, tanggal 15 Maret 2001, umur 23 tahun, jenis kelamin Perempuan, agama Islam, pekerjaan Karyawan Swasta, pendidikan terakhir SMA, Kewarganegaraan Indonesia, tempat tinggal:Jl. Muda Jaya No. 98 Bantu I----------

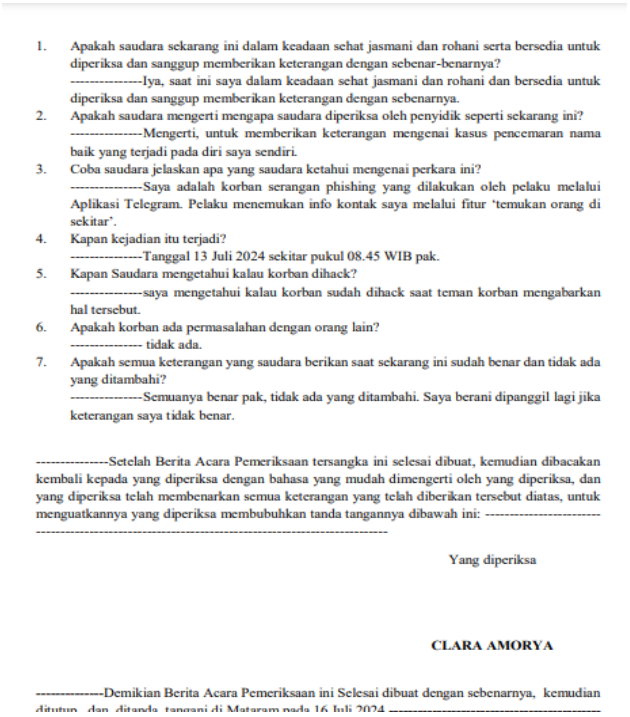
----------Ia diperiksa dan dimintai keterangannya selaku **Saksi** dalam perkara tindak pidana pencemaran nama baik sebagaimana dimaksud dalam Pasal 310 ayat 1 KUHP Subsidair Pasal 27A UU1/2024, sehubungan dengan adanya Laporan Polisi No. Pol: LP/240/XI/2015/RESKRIM hari Senin, 15 Juli 2024----------

---------- Atas pertanyaan pemeriksa yang dilakukan secara tanya jawab dan yang diperiksa memberikan keterangan dan jawaban sebagai berikut di bawah ini: ----------

PERTANYAAN : **JAWABAN** :

Gambar 4. Berita Acara Pemeriksaan

Adapun pertanyaan-pertanyaan yang diajukan kepada saksi (korban) sebagai berikut :



1. Apakah saudara sekarang ini dalam keadaan sehat jasmani dan rohani serta bersedia untuk diperiksa dan sanggup memberikan keterangan dengan sebenar-benarnya?
   ----------Iya, saat ini saya dalam keadaan sehat jasmani dan rohani dan bersedia untuk diperiksa dan sanggup memberikan keterangan dengan sebenarnya.
2. Apakah saudara mengerti mengapa saudara diperiksa oleh penyidik seperti sekarang ini?
   ----------Mengerti, untuk memberikan keterangan mengenai kasus pencemaran nama baik yang terjadi pada diri saya sendiri.
3. Coba saudara jelaskan apa yang saudara ketahui mengenai perkara ini?
   ----------Saya adalah korban serangan phishing yang dilakukan oleh pelaku melalui Aplikasi Telegram. Pelaku menemukan info kontak saya melalui fitur 'temukan orang di sekitar'.
4. Kapan kejadian itu terjadi?
   ----------Tanggal 13 Juli 2024 sekitar pukul 08.45 WIB pak.
5. Kapan Saudara mengetahui kalau korban dihack?
   ----------saya mengetahui kalau korban sudah dihack saat teman korban mengabarkan hal tersebut.
6. Apakah korban ada permasalahan dengan orang lain?
   ---------- tidak ada.
7. Apakah semua keterangan yang saudara berikan saat sekarang ini sudah benar dan tidak ada yang ditambahi?
   ----------Semuanya benar pak, tidak ada yang ditambahi. Saya berani dipanggil lagi jika keterangan saya tidak benar.

----------Setelah Berita Acara Pemeriksaan tersangka ini selesai dibuat, kemudian dibacakan kembali kepada yang diperiksa dengan bahasa yang mudah dimengerti oleh yang diperiksa, dan yang diperiksa telah membenarkan semua keterangan yang telah diberikan tersebut diatas, untuk menguatkannya yang diperiksa membubuhkan tanda tangannya dibawah ini: ----------

Yang diperiksa

CLARA AMORYA

----------Demikian Berita Acara Pemeriksaan ini Selesai dibuat dengan sebenarnya, kemudian

Gambar 5. Pertanyaan-pertanyaan BAP

D. Barang Bukti

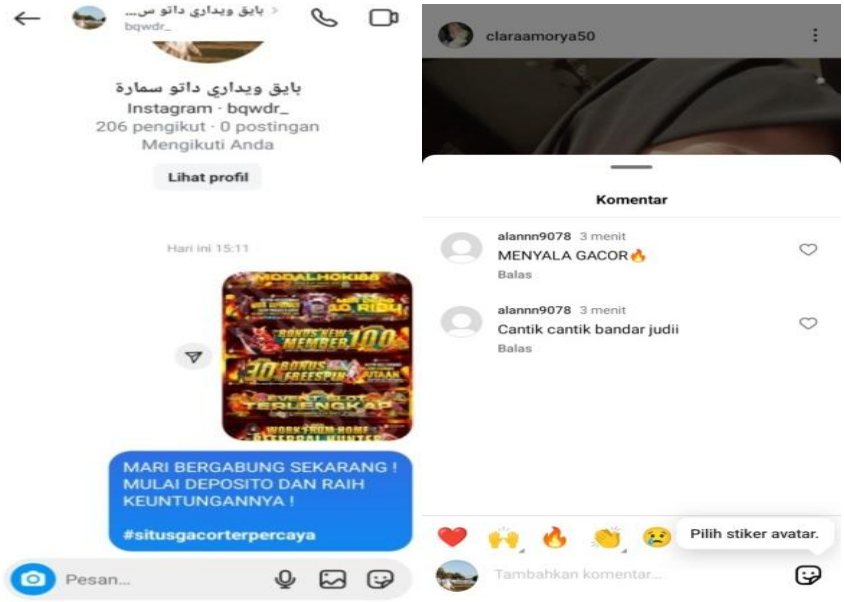
Peneliti mengidentifikasi perangkat yang merupakan barang bukti kasus kejahatan tersebut. Teridentifikasi bahwa korban menggunakan *smartphone* sebagai bukti fisik, dengan fokus pada bukti digital seperti percakapan teks, kontak, audio, video. Adapun barang buktinya sebagai berikut:

Tabel 2. Barang Bukti

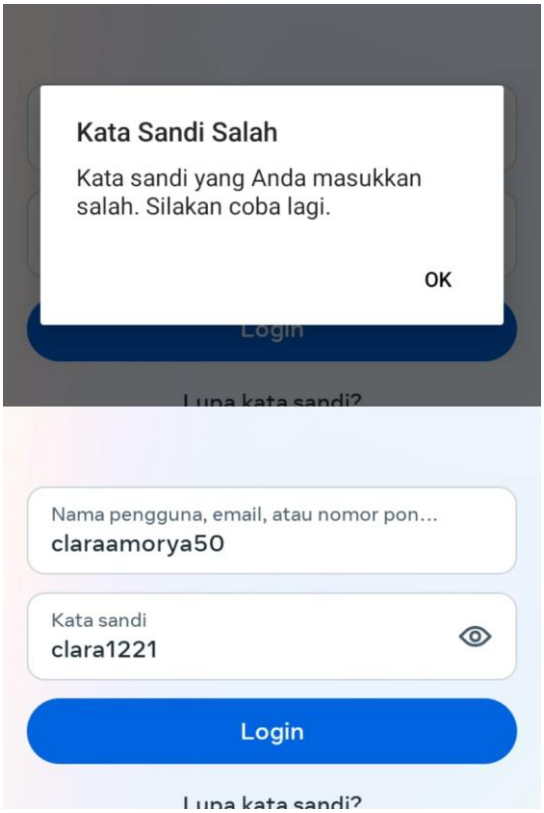
No.	Foto Barang Bukti	Deskripsi Barang Bukti
1.	 Tampak Depan  Tampak Belakang	Smartphone milik Clara Amorya (korban) Merk : Samsung Nomor Model : SM-J530Y/DS Platform : Android Nomor Serial :RR8JC0666CK IMEI 1 : 352723090809154 IMEI 2 : 352724090809152 Rooted : Yes SIM Card : Ada

Penelitian ini berhasil mengenali *smartphone* Samsung *Galaxy* J5 *Pro* dengan spesifikasi seperti pada tabel 2, termasuk sistem operasi Android 9.0 dan prosesor Exynos. Adapun barang bukti yang diterima korban dari temannya yaitu dua gambar yang berisi komentar

negatif terhadap korban dan gambar pesan promosi yang dikirim pelaku kepada *followers* korban.



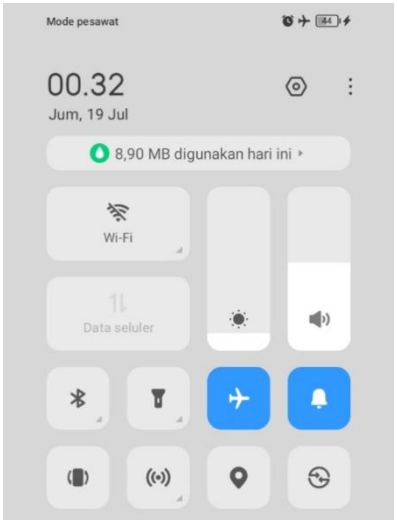
Gambar 6. Bukti Pelaku Pencemaran Nama Baik



Gambar 7. Bukti Korban Tidak Bisa *Log In*

2. Hasil Pemeliharaan

Pada tahap pemeliharaan dilakukan proses isolasi. Peneliti mengisolasi *smartphone* dari jaringan telekomunikasi dengan mengaktifkan mode pesawat untuk mencegah segala hal yang dapat merusak atau mempengaruhi integritas data digital.

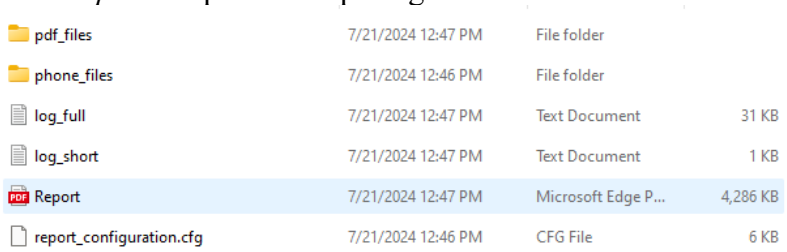


Gambar 8. Pengisolasian *Smarthpone* Dari Jaringan

Sebelum melanjutkan tahap pengumpulan bukti digital, data pada smartphone di*backup* terlebih dahulu. Untuk mengantisipasi apabila ada kemungkinan data yang rusak atau hilang.

3. Hasil Pengumpulan

Tahap ketiga melibatkan pengumpulan dan identifikasi bukti digital serta data tertentu dari aplikasi Telegram. Proses pengambilan bukti digital dari *smartphone* memiliki risiko tinggi, dimana kesalahan fatal dapat menyebabkan hilang atau rusaknya data bukti digital yang penting. Oleh karena itu, peneliti harus melakukan tahap isolasi terlebih dahulu, yang meliputi *physical imaging* atau *backup*. Proses ini sering disebut sebagai akuisisi logis. Alat yang digunakan untuk melakukan *backup* adalah MOBILedit *Forensic Express*, yang memiliki sistem cadangan yang handal di *smartphone* untuk memastikan keamanan dan integritas bukti yang diperoleh. Penting untuk menegaskan bahwa autentisitas bukti digital sangat sensitif. perubahan pada barang bukti asli dianggap sebagai modifikasi terhadap bukti yang disajikan. Hasil akuisisi menggunakan MOBILedit *Forensic Express* dapat dilihat pada gambar di bawah.

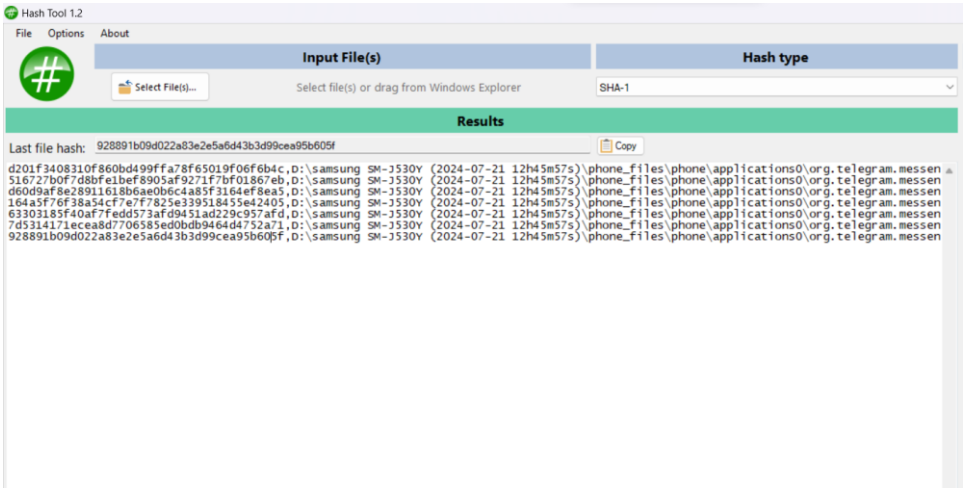


Gambar 9. Hasil Akuisisi Data

Dari hasil ekstraksi bukti digital diperoleh file dengan format pdf *files*, *phone files*, file *log text*, file cfg, dan file *chache*.

4. Hasil Pemeriksaan

Adapun maksud dan tujuan pemeriksaan pada kasus serangan *phishing* yang diminta oleh pihak kepolisian adalah untuk mengetahui apakah barang bukti yang telah dikumpulkan terbukti keasliannya. Dan untuk mengekstrak artefak barang bukti. Berikut gambar proses pemeriksaan validasi barang bukti:



Gambar 10. Proses Validasi Barang Bukti

Adapun hasil ekstraksi artefak dapat dilihat pada gambar tabel di bawah ini:

Barang Bukti	*Directory*	Nama File	*Hashing* File
Pesan	phone/applications0/org.telegram.messenger/live_data/files/account1/cache4.db-wal	account1/cache4.db-wa	d201f3408310f860bd499ffa78f65019f06f6b4c
	phone/applications0/org.telegram.messenger/live_data/files/account2/cache4.db-wal	account2/cache4.db-wa	516727b0f7d8bfe1bef8905af9271f7bf01867eb
	phone/applications0/org.telegram.messenger/live_data/files/account3/cache4.db-wal	account3/cache4.db-wal	d60d9af8e28911618b6ae0b6c4a85f3164ef8ea5
Kontak	phone/applications0/org.telegram.messenger/live_data/files/cache4.db-wal	files/cache4.db-wal	164a5f76f38a54cf7e7f7825e339518455e42405
Gambar	phone/applications0/org.telegram.messenger/live_external/ cache/-6116038128198226086_1109.jpg	-6116038128198226086_1109.jpg	63303185f40af7fedd573afd9451ad229c957afd
	phone/applications0/org.telegram.messenger/live_external/ cache/-6334775371316181866_97.jpg	-6334775371316181866_97.jpg	7d5314171ecea8d7706585ed0bdb9464d4752a71
Video	phone/applications0/org.telegram.messenger/live_external/files/Telegram/Telegram Video/5_6116038128198226086.MP4	5_6116038128198226086.MP4	928891b09d022a83e2e5a6d43b3d99cea95b605f
Audio	-	-	-

Gambar 11. Hasil Ekstraksi Artefak

Barang bukti yang berhasil diekstrak yakni pesan, kontak dan gambar yang tersimpan dalam file cache. Dan ada video dengan format MP4. File audio sendiri tidak ditemukan. Kemudian pada kolom hashing file merupakan hasil dari validasi barang bukti dengan menggunakan luaran algoritma SHA-1.

5. Hasil Analisis

Pada tahapan ini peneliti akan menganalisis file artefak yang telah diekstrak pada tahap pemeriksaan barang bukti. Peneliti menggunakan *tools DB Browser For SQLite* untuk menganalisis barang bukti berupa percakapan dan kontak. Sedangkan untuk barang bukti seperti video dan gambar dianalisis menggunakan tools *MOBILedit Forensics Express*. Data bukti yang ingin diketahui yakni:

1. Apa isi pesan yang dikirim oleh pelaku?
2. Siapakah pelaku penyerangan?
3. Kapan penyerangan tersebut dilakukan?
4. Mengapa tindakan penyerangan tersebut dilakukan?
5. Di mana kejadian tersebut terjadi?
6. Dan bagaimana detail kejadian tersebut terjadi?

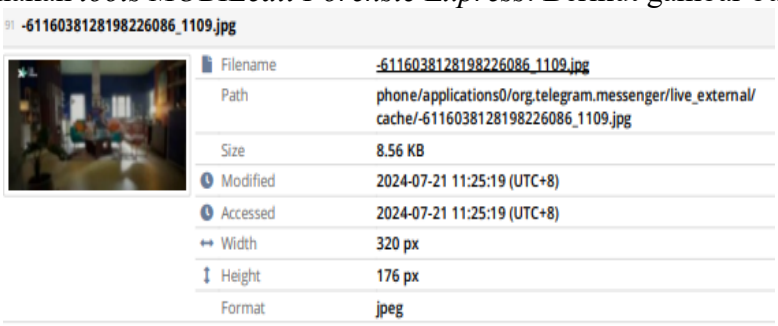
Poin 3,4,5, dan 6 sudah terjawab pada tahap identifikasi berdasarkan keterangan korban. Adapun

hasil dari proses analisis masing-masing *tools* yang digunakan berdasarkan jumlah barang bukti yang ditemukan disajikan pada tabel 3:

Tabel 3. Jumlah Barang bukti Yang Ditemukan

Tools	Bukti Yang Diharapkan					Presentasi Keberhasilan
	Gambar	Percakapan	Audio	Kontak	Video	
MOBILedit Forensic Express	2	0	0	0	1	40%
DB Browser For SQLite	0	0	0	1	0	20%

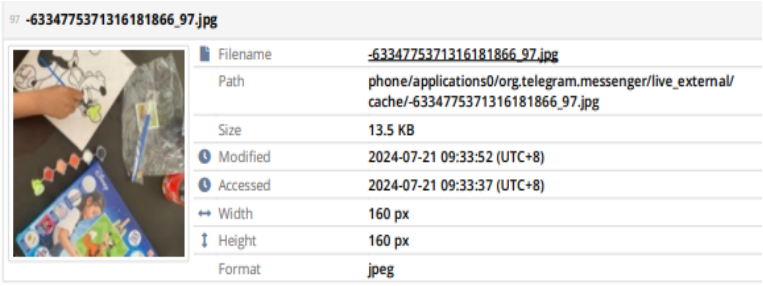
Berdasarkan tabel 4.3 *MOBILedit Forensic Express* menunjukkan tingkat keberhasilan yang lebih tinggi dalam menemukan bukti digital (40%) dibandingkan dengan *DB Browser for SQLite* (20%). Namun, keduanya masih memiliki keterbatasan dalam menemukan semua jenis bukti yang diharapkan, seperti percakapan dan audio. Adapun Bukti gambar ditemukan pada pdf file yang telah diekstrak menggunakan *tools MOBILedit Forensic Express*. Berikut gambar bukti disajikan :



Gambar 12. Gambar Cache Video Bukti

Gambar 12 memberikan informasi mengenai sebuah file gambar yang berada di dalam cache aplikasi Telegram pada perangkat telepon. File tersebut memiliki nama "-6116038128198226086_1109.jpg" dan berukuran 8.56 KB. Jalur penyimpanan file ini tercatat di direktori cache Telegram, tepatnya di: `*phone*/*applications*/org.telegram.*messenger*/*live*_external/cache/-6116038128198226086_1109.jpg`. File ini memiliki dimensi 320x176 piksel dan berformat JPEG. Data tersebut menunjukkan bahwa file gambar ini terakhir kali dimodifikasi dan diakses pada tanggal 21 Juli 2024 pukul 11:25:19 waktu setempat (UTC+8).

File gambar ini kemungkinan besar merupakan bagian dari data cache yang disimpan oleh aplikasi Telegram, yang bisa saja terkait dengan video bukti kejahatan yang disimpan sebelumnya. Aplikasi seperti Telegram sering kali menyimpan gambar pratinjau atau cuplikan dari video untuk mempermudah akses pengguna. Informasi ini dapat berguna dalam proses penyelidikan untuk menentukan asal dan konteks video terkait yang mungkin mengandung bukti kejahatan, terutama jika gambar pratinjau ini diambil dari video yang dikirim atau diterima dalam percakapan Telegram.

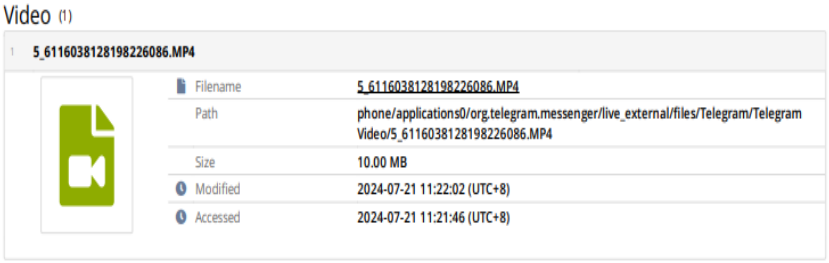


Gambar 13. Foto Profil Akun Telegram Pelaku Berdasarkan Keterangan Korban

Gambar 13 memberikan detail tentang sebuah file gambar yang diduga merupakan foto profil akun Telegram milik pelaku berdasarkan keterangan korban. File tersebut memiliki nama "-6334775371316181866_97.jpg" dan berukuran 13.5 KB. Lokasi penyimpanan file ini berada dalam direktori cache aplikasi Telegram pada perangkat telepon, dengan jalur: `*phone*/*applications*/org.telegram.*messenger*/*live*_external/cache/-6334775371316181866_97.jpg`. Informasi ini juga menunjukkan bahwa file gambar tersebut terakhir dimodifikasi pada tanggal 21 Juli 2024 pukul 09:33:52 waktu setempat (UTC+8) dan diakses terakhir kali pada waktu yang hampir bersamaan, yaitu pukul 09:33:37 (UTC+8).

Dari data yang tersedia, terlihat bahwa gambar ini kemungkinan diambil dari cache aplikasi Telegram, yang sering kali menyimpan data sementara, termasuk gambar profil dari percakapan atau akun pengguna. Gambar tersebut berformat JPEG dengan resolusi 160x160 piksel, yang sesuai dengan standar ukuran gambar profil pada aplikasi pesan instan. Informasi ini penting dalam konteks penyelidikan karena dapat membantu mengidentifikasi pelaku melalui akun Telegram yang digunakan, terutama jika foto profil tersebut mengandung gambar atau informasi yang dapat dihubungkan dengan pelaku.

Adapun di bawah ini merupakan gambar bukti video promosi yang dikirim pelaku kepada korban dan gambar detail data kontak pelaku:



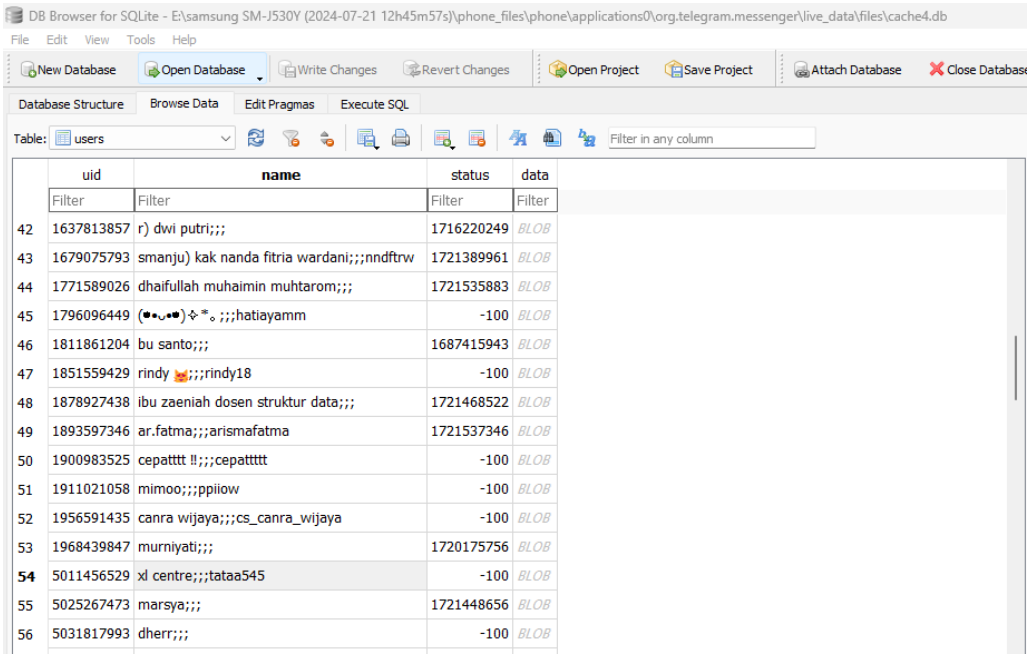
Gambar 14. Lokasi *Directory* File Bukti Video

Gambar 14 menunjukkan detail dari sebuah file video yang berfungsi sebagai bukti kejahatan. File tersebut diberi nama "5_6116038128198226086.MP4" dan berukuran 10.00 MB. File ini disimpan di dalam direktori aplikasi Telegram pada perangkat telepon, dengan jalur lengkap: `*phone*/*applications*/org.telegram.*messenger*/*live*_external/files/Telegram/TelegramVideo/5_6116038128198226086.MP4`. Informasi ini juga mencakup tanggal modifikasi dan akses terakhir dari file tersebut, yaitu pada tanggal 21 Juli 2024, masing-masing pada pukul 11:22:02 dan 11:21:46 waktu setempat (UTC+8).

Penjelasan ini menunjukkan bahwa file video yang bersangkutan adalah bagian dari data yang disimpan oleh aplikasi Telegram, yang berpotensi berisi informasi penting terkait kasus kejahatan. Lokasi file yang ada di dalam direktori Telegram mengindikasikan bahwa video ini kemungkinan besar dikirim atau diterima melalui aplikasi tersebut. Data tentang waktu modifikasi dan akses juga dapat memberikan petunjuk lebih lanjut mengenai kapan file ini terakhir kali digunakan atau diubah, yang bisa relevan dalam konteks penyelidikan kriminal.

Gambar 15. Tampilan Awal Video Promosi

Pada gambar 15 Logo XL di pojok kiri atas menunjukkan bahwa gambar tersebut adalah promosi dari operator telekomunikasi XL Axiata. Gambar digunakan oleh pelaku untuk menipu korban dengan berpura-pura menawarkan paket internet baru dari XL. Penipu memanfaatkan tampilan ini untuk membuat video palsu atau tutorial yang seolah-olah resmi, yang kemudian mengarahkan korban untuk memberikan informasi pribadi atau melakukan tindakan yang merugikan.



	uid	name	status	data
	Filter	Filter	Filter	Filter
42	1637813857	r) dwi putri;;;	1716220249	BLOB
43	1679075793	smanju) kak nanda fitria wardani;;;nndftrw	1721389961	BLOB
44	1771589026	dhaifullah muhaimin muhtarom;;;	1721535883	BLOB
45	1796096449	(•ᴗ•)✧*。;;;hatiayamm	-100	BLOB
46	1811861204	bu santo;;;	1687415943	BLOB
47	1851559429	rindy 🦊;;;rindy18	-100	BLOB
48	1878927438	ibu zaeniah dosen struktur data;;;	1721468522	BLOB
49	1893597346	ar.fatma;;;arismafatma	1721537346	BLOB
50	1900983525	cepatttt !!;;;cepatttttt	-100	BLOB
51	1911021058	mimoo;;;ppiiow	-100	BLOB
52	1956591435	canra wijaya;;;cs_canra_wijaya	-100	BLOB
53	1968439847	murniyati;;;	1720175756	BLOB
54	5011456529	xl centre;;;tataa545	-100	BLOB
55	5025267473	marsya;;;	1721448656	BLOB
56	5031817993	dherr;;;	-100	BLOB

Gambar 16. Hasil Analisis Kontak Pelaku

Berdasarkan gambar 16 merupakan proses analisis yakni untuk mengetahui siapa pelaku dan isi percakapan pesan yang telah dihapus seperti apa, peneliti berhasil menemukan pelaku dengan nama akun xl *centre*;;;tata545 dengan userid 5011456529. Dan peneliti tidak menemukan bukti pesan melainkan menemukan bukti media seperti gambar dan video. Adapun untuk perbandingan *tools* forensik barang bukti dapat dilihat pada tabel 4 :

Tabel 4. Perbandingan Tools Forensik

Hasil Yang Diperoleh	Forensic tools	
	MOBILedit Forensic Express	***DB Browser For SQLite***
Percakapan	Tidak ditemukan	Tidak ditemukan
Kontak	Tidak ditemukan	Ditemukan
Gambar	Ditemukan	Tidak ditemukan
Video	Ditemukan	Tidak ditemukan
Audio	Tidak ditemukan	Tidak ditemukan

MOBILedit *Forensic Express* menunjukkan keberhasilan dalam menemukan gambar dan video tetapi gagal menemukan percakapan, kontak, dan audio. Sedangkan *DB Browser for SQLite* berhasil menemukan kontak tetapi tidak berhasil menemukan percakapan, gambar, video, dan audio.

6. Hasil Presentasi

Pada tahap ini peneliti akan membuat laporan hasil penelitian mengenai data yang telah ditemukan. Berikut laporan ringkas mengenai hasil penelitian kasus *phishing* pada Aplikasi Telegram:

Tabel 5. Laporan Ringkas Kasus *Phishing* Pada Aplikasi Telegram

Informasi	Barang Bukti	Keterangan
Percakapan	-	Tidak ditemukan
File Bukti Chat	-	Tidak ditemukan
Nama Akun Pelaku	Xl *Centre*;;;tata545	Ditemukan
File Bukti Kontak	1	Ditemukan
File Bukti Video	1	Ditemukan
File Bukti Gambar	2	Ditemukan
File Bukti Audio	-	Tidak ditemukan
Tools Forensik	*MOBILedit Forensic Express* dan *DB Browser For SQLite*	Ditemukan
Tools Backup Data *Smartphone*	*MOBILedit Forensic Express*	Ditemukan

Tabel di atas menunjukkan hasil identifikasi barang bukti menggunakan *MOBILedit Forensic Express* dan *DB Browser for SQLite*. Dari berbagai jenis barang bukti yang diharapkan, alat-alat ini berhasil menemukan nama akun pelaku ("XI *Center* - tata545"), 1 file kontak, 1 file video, dan 2 file gambar. Namun, file bukti chat dan file bukti audio tidak ditemukan. *MOBILedit Forensic Express* digunakan untuk analisis dan backup data smartphone, sementara *DB Browser for SQLite* digunakan khusus untuk analisis data.

KESIMPULAN

Penelitian ini menggunakan metode Digital Forensics Research Workshop (DFRWS) untuk menganalisis aplikasi Telegram dan terbukti cukup efektif dalam menyelesaikan kasus. Melalui tahapan yang terstruktur mulai dari pengumpulan, analisis, hingga pelaporan bukti digital, metode ini mampu memastikan integritas dan akurasi data yang diperoleh. Hasil penelitian menunjukkan bahwa alat forensik yang digunakan, yaitu MOBILedit Forensic Express dan DB Browser for SQLite, berhasil mengidentifikasi dan mengumpulkan bukti digital yang relevan meskipun dengan berbagai tingkat keberhasilan.

MOBILedit Forensic Express mampu mengumpulkan 40% dari total barang bukti yang diharapkan, termasuk file gambar dan video. Sementara itu, DB Browser for SQLite berhasil mengumpulkan 20% bukti digital, terutama data kontak pelaku. Meskipun belum mampu menemukan semua jenis bukti yang diharapkan seperti percakapan yang telah dihapus dan log audio call, metode Digital Forensics Research Workshop (DFRWS) memberikan kerangka kerja yang sistematis dan dapat diandalkan dalam investigasi forensik digital.

Secara keseluruhan, penelitian ini menunjukkan bahwa metode Digital Forensics Research Workshop (DFRWS) efektif dalam mengidentifikasi dan menganalisis bukti digital pada aplikasi Telegram, memberikan panduan yang berguna bagi peneliti dan praktisi di bidang forensik digital dalam menangani kasus serupa di masa depan.Berdasarkan hasil analisis data dan pembahasan di atas dapat disimpulkan bahwa diketahui nilai sig. variabel emosional spiritual (X) sebesar 0,005 sedangkan, nilai thitung sebesar 3,351 dengan nilai ttabel > 1,761. Maka disimpulkan bahwa nilai sig. 0,00 < 0,05 dan nilai thitung 3,351 > 1,761. Sehingga dapat dikatakan bahwa terdapat pengaruh positif dan signifikan antara emosional spiritual terhadap kesadaran diri. Dari hasil analisis data kuatitatif experiment menunjukan peserta pelatihan mendapatkan banyak manfaat, pengetahuan baru dari pelatihan ini, terutama dalam hal pemahaman dalam mengenal dan mengelolah emosi diri sendiri untuk meningkatkan kesadaran diri.

DAFTAR PUSTAKA

Alhadiansyah, M Qahar Awaka. 2023. “Utilization of Digital Forensics in Proving the Crime of Disseminating Indecent Videos Through Facebook Social Media in the Legal Area of West Kalimantan Police Pemanfaatan Digital Forensik Dalam Pembuktian Tindak Pidana Penyebaran Video Asusila Melalaui .”

Bintang, Rauhulloh Ayatulloh, Rusydi Umar, and Anton Yudhana. 2020. “Analisis Media Sosial Facebook Lite Dengan Tools Forensik Menggunakan Metode NIST.” Techno (Jurnal Fakultas Teknik, Universitas Muhammadiyah Purwokerto) 21(2): 125. doi:10.30595/techno.v21i2.8494.

Dasmen, Rahmat Novrianda, and Ferry Kurniawan. 2021. “Digital Forensik Deleted Cyber Crime Evidence Pada Pesan Instan Media SosialDigital Forensik Deleted Cyber Crime Evidence Pada Pesan Instan Media Sosial.” Techno.Com 20(4): 527–39. doi:10.33633/tc.v20i4.5170.

Fanani, Galih, Imam Riadi, and Anton Yudhana. 2022. “Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop.” Jurnal Media Informatika Budidarma 6(2): 1263. doi:10.30865/mib.v6i2.3946.

Febrian, Rizky, Achmad Fauzi, Tegar Maulana Hidayat, Rifki Ardian, and Alfito Surya Saputra. 2023. “Pentingnya Kemanan Data Dalam Intelijen Bisnis.” Jurnal Ilmu Multidisplin 2(1): 42–49. doi:10.38035/jim.v2i1.237.

Imam Riadi, Sunardi, and Panggah Widiandana. 2020. “Investigating Cyberbullying on WhatsApp Using Digital Forensics Research Workshop.” Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi) 4(4): 730–35. doi:10.29207/resti.v4i4.2161.

Kusumadewa, Rendy Bramesta, Syaifuddin Syaifuddin, and Zamah Sari. 2022. “Comparative Analysis of Forensic Digital Evidence on Android Smartphone Based Instant Messaging Using NIST Framework.” Jurnal Repositor 4(3): 407–22. doi:10.22219/repositor.v4i3.1531.

Maniar, Nadia Ayu Isroh, and Trihastuti Yuniati. 2023. “Implementasi Mobile Forensic Pada Aplikasi Michat Dan Telegram Dengan Framework Nist 800-101.” Cyber Security dan Forensik Digital 5(2): 60–65. doi:10.14421/csecurity.2022.5.2.3764.

Qibriya, Maghvirna Rafika Dhewi, Awalludiyah Ambarwati, and Kunto Eko Susilo. 2021. “Analisis Forensik Digital Pada Aplikasi Instant Messaging Di Smartphone Berbasis Android Untuk Bukti Digital.” Jurnal Teknologi Informasi 5(2): 114–21. doi:10.36294/jurti.v5i2.2200.

Riadi, Imam, Rusydi Umar, and Muhammad Abdul Aziz. 2019. “Forensik Web Layanan Instant Messaging Menggunakan Metode Association of Chief Police Officers (ACPO).” Mobile and Forensics 1(1): 30. doi:10.12928/mf.v1i1.705.

Riadi, Imam, Anton Yudhana, and Mushab Al Barra. 2021. “Forensik Mobile Pada Layanan Media

Sosial LinkedIn." JISKA (Jurnal Informatika Sunan Kalijaga) 6(1): 9–20. doi:10.14421/jiska.2021.61-02.

Rusdi, Muhammad Idham, and Dianradika Prasti. 2019. "Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux." Seminar Nasional Teknologi Informasi dan Komputer 2019: 260–69.

Sunardi, Imam Riadi, Rusydi Umar, and Muhammad Fauzan Gustafi. 2021. "Audio Forensics on Smartphone with Digital Forensics Research Workshop (DFRWS) Method." CommIT Journal 15(1): 41–47. doi:10.21512/commit.v15i1.6739.

Vadila, Nunu, and Ahmad R Pratama. 2021. "Analisis Kesadaran Keamanan Terhadap Ancaman Phishing." Automata 2(2): 1–4.

Zuhriyanto, Ikhsan, Anton Yudhana, and Imam Riadi. 2020. "Comparative Analysis of Forensic Tools on Twitter Applications Using the DFRWS Method." Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi) 4(5): 829–36. doi:10.29207/resti.v4i5.2152.