

AKUISISI BUKTI DIGITAL PADA APLIKASI TAMTAM MESSENGER MENGUNAKAN METODE NATIONAL INSTITUTE OF JUSTICE

Desti Mualfah^{1*}, Afdel Viransa², Hasanatul Fu'adah Amran³

^{1,2,3}Fakultas Ilmu Komputer, Universitas Muhammadiyah Riau

email: ¹destimualfah@umri.ac.id, ²180401140@umri.ac.id, ³hasanatul@umri.ac.id

Abstract

Smartphones are one of the tools used in carrying out daily work activities, the number of active social media users in Indonesia in January 2019 reached 150 million, 130 million of whom accessed social media using smartphones. With the development of smartphones in social media, many are misused using instant messaging applications, one of which is cybercrime such as cyberbullying, human trafficking systems, fraud and so on. Cyberbullying is one of the negative impacts in cyber crime through the use of applications that are often used, namely the TamTam Messenger social media. The problem that will be discussed in this study is the digital forensic process, especially mobile forensics in order to find digital evidence that was deleted on the TamTam Messenger application using the MobileEdit forensic tools and the National Institute of Justice method. The results of this study show that using the MobileEdit forensic tools and the National Institute of Justice method succeeded in recovering digital evidence that had been deleted by the perpetrator on the TamTam Messenger application.

Keywords: Smartphone, Cyberbullying, TamTam Messenger

Abstrak

Smartphone menjadi salah satu alat yang digunakan dalam melakukan aktivitas pekerjaan sehari-hari, jumlah pengguna aktif media sosial di Indonesia pada Januari 2019 mencapai 150 juta, 130 juta diantaranya mengakses media sosial menggunakan Smartphone. Dengan Perkembangan smartphone dalam media sosial ini banyak disalahgunakan menggunakan aplikasi-aplikasi pesan instan, salah satunya tindak kejahatan (cybercrime) seperti cyberbullying sistem perdagangan manusia, penipuan dan lain sebagainya. Cyberbullying merupakan salah satu dampak negatif yang dalam kejahatan cyber melalui pemanfaatan aplikasi yang sering digunakan yaitu media sosial TamTam Messenger. Permasalahan yang akan dibahas dalam penelitian ini adalah proses digital forensik khususnya mobile forensik dalam rangka mencari bukti digital yang dihapus pada aplikasi TamTam Messenger menggunakan tools forensic MobileEdit dan metode National Institue Of Justice. Hasil penelitian ini menunjukkan dengan menggunakan tools MobileEdit forensic dan metode National Institue Of Justice berhasil mengembalikan bukti digital yang telah dihapus oleh pelaku pada aplikasi TamTam Messenger.

Keywords: Smartphone, Cyberbullying, TamTam Messenger

PENDAHULUAN

Keberadaan smartphone saat ini dianggap sangat membantu aktivitas manusia dalam melakukan kegiatan sehari-hari. Berkembangnya fitur-fitur yang terdapat pada smartphone mempermudah para penggunanya melakukan aktivitas pekerjaan kantor, bisnis, e-banking, serta buat berhubungan dengan pengguna lain di media sosial. Jumlah pengguna aktif media sosial di Indonesia pada Januari 2019 mencapai 150 juta pengguna aktif media sosial, 130 juta diantaranya mengakses media sosial menggunakan Smartphone (Soni et al., 2021). Akses internet merupakan kegiatan yang tidak terlepas dari kebutuhan masyarakat, hal tersebut dapat dilihat dari banyaknya kegiatan yang menggunakan akses internet (Mualfah et al., n.d.).

Dengan Perkembangan *smartphone* dalam media sosial ini, banyak pengguna internet didunia khususnya di Indonesia saat ini banyak disalahgunakan, salah satunya perkembangan smartphone yang melakukan tindak kejahatan (*cybercrime*) seperti selalu mengalami perkembangan dari segi system perdagangan manusia, *cyberbully*, penipuan, pemerasan, operasi, fitur, spesifikasi, dan aplikasi (Sistem et al., 2021). *Cybercrime* pada umumnya meninggalkan jejak (*history*) dari aktivitas kejahatan yang dilakukan sehingga dapat dijadikan sebagai barang bukti (Riskiyadi, 2020).

Salah satu dampak negatif yang dibahas disini adalah mengenai penindasan dunia maya atau *cyberbullying*. Sebanyak 3.325 kasus kejahatan siber yang telah Polri tangani sejak 2017. Sementara pada 2016, ada 1.829 kasus yang telah ditangani Polri (Syahib et al., 2020). fakta yang diperlukan untuk kepentingan hukum, berbeda dengan ilmu forensik lainnya yang lebih banyak berkaitan dengan pembedahan dan pencarian artefak pada makhluk hidup (Mualfah & Ramadhan, 2020b).

Penindasan dan pengancaman juga tidak selamanya dikatakan atau diucapkan secara langsung pada seseorang namun juga bisa dilakukan melalui beberapa sarana yaitu seperti telepon seluler, pesan singkat bahkan yang sekarang sering digunakan yaitu media sosial *TamTam* (sangadah & Kartawidjaja, 2020). *TamTam* adalah utusan yang praktis dan aman dengan saluran, panggilan video. Berkomunikasi dalam obrolan, *TamTam*

memiliki semua yang dibutuhkan untuk berkomunikasi dengan mudah,

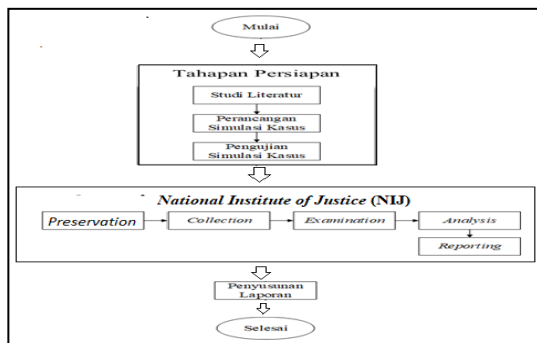
Aplikasi ini di rilis pada 16 Mei 2016 dengan perusahaannya bernama [Odnoklassniki Ltd.](#) Didownload lebih dari 10.000.000 juta pengguna, memiliki keunggulan seperti Panggilan dan pesan gratis, Chat Grup, enkripsi, bisa bicara dimana saja, Akses cepat. Aktivitas yang dapat dilakukan melalui fitur *TamTam Messenger* adalah untuk bertukar pesan chat, stiker dan GIF, termasuk yang animasi. Panggilan gratis, Panggilan video grup dengan hingga 100 peserta dapat membantu mengumpulkan kolega atau teman. Aktivitas-aktivitas yang bisa digunakan pada aplikasi tersebut bisa menyebabkan dampak negatif yaitu dapat disalahgunakan untuk melakukan kejahatan dunia maya dan dengan demikian mempengaruhi penggunaan *TamTam Messenger*. Salah satunya ancaman kejahatan seperti *cyberbullying*. Untuk mengatasi kejahatan ini membutuhkan metode analitis dan forensik untuk membantu menyelesaikan kejahatan *cyberbullying* di media sosial *TamTam Messenger*.

Permasalahan yang akan dibahas dalam penelitian ini adalah proses digital forensik khususnya mobile forensik dalam rangka mencari bukti digital yang dihapus pada aplikasi *TamTam Messenger*. Bukti digital adalah informasi yang disimpan atau dikirim dalam bentuk biner, bukti digital berhubungan dengan mobile seperti smartphone dapat ditemukan di *call history*, *phonebook*, *SMS*, *MMS*, *Photo*, *Audio*, dan lain-lainnya (Riadi et al., 2018). Pengambilan barang bukti digital pada penelitian ini yaitu dengan menggunakan metode yang dikembangkan oleh National Institute of Justice. Pengkajian ini memakai NIJ selaku metode dalam mendukung petugas investigasi untuk menjalankan proses forensik dengan alasan mempunyai tahapan yang lebih baik dibandingkan metode atau kerangka kerja lainnya (Sunardi et al., 2021). Forensik jaringan didefinisikan dalam sebagai menangkap, merekam, dan analisis peristiwa jaringan untuk menemukan sumbernya serangan keamanan atau insiden masalah lainnya (D. Mualfah & Riadi, 2017)

Penelitian ini diharapkan dapat memberikan gambaran umum bagaimana proses forensik yang dapat dilakukan untuk mengembalikan data yang hilang atau terhapus pada smartphone android (Riadi et al., 2019).

METODE PENELITIAN

Dalam menyelesaikan proses analisis forensik dan investigasi melalui smartphone, diperlukan metode agar proses investigasi dapat dilakukan. Proses investigasi melalui beberapa tahapan pada gambar 1 berikut:



Gambar 1 Metode Penelitian

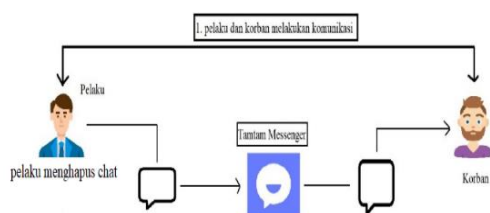
Tahapan Persiapan

Sebelum melakukan penelitian, penulis terlebih dahulu melakukan studi literature, untuk memahami penelitiannya terlebih dahulu, agar dapat membantu untuk menyelesaikan penelitian yang akan dilakukan nantinya, dengan merancang dan melakukan simulasi kasus.

Studi Literatur

Studi literatur adalah tahap pengumpulan semua data dari jurnal, buku, artikel digital, dll sebagai bentuk dukungan pelaporan penelitian. Mencari dan meninjau semua sumber bacaan berdasarkan topik yang diteliti. Dari kajian dokumen tersebut diharapkan dapat membantu untuk memahami metode pencarian yang digunakan pada ponsel pintar, memahami perangkat forensik seluler yang digunakan serta proses analisis dan investigasi untuk memperoleh bukti digital.

Skenario Kasus



Gambar 2 Skenario kasus

Berdasarkan simulasi kasus, dijelaskan bahwa ada dua pengguna yang berkomunikasi

menggunakan *TamTam Messenger*: pengguna (pengirim pesan, pelaku) dan pengguna (penerima pesan, korban kejahatan). Keduanya memiliki akun *TamTam Messenger*. Akun-akun tersebut digunakan untuk berkomunikasi satu sama lain dengan mengobrol dan mengirim foto melalui fitur *TamTam Messenger*.

Tahapan Metode NIJ

Metode Digital Forensik yang diimplementasikan pada hal ini adalah National Institute of Justice (NIJ) dimana metode ini berlaku sebagai acuan dalam praktek Digital Forensik pada penelitian ini (Mualfah & Ramadhan, 2020b). Perangkat Berikut ini Tahapan metode dari (NIJ) ini yang digunakan untuk mencari bukti digital pada perangkat smartphone, aplikasi *TamTam Messenger* terbagi menjadi lima tahapan yaitu:

1. Tahap *preparation*

Tahap *preparation* merupakan kegiatan pemilahan barang bukti tindak kejahatan digital dan pemilahan data-data untuk mendukung proses penyidikan dalam rangka pencarian barang bukti kejahatan digital. Pada tahap ini didalamnya terdapat proses identifikasi, pelabelan, perekaman, untuk menjaga keutuhan barang bukti.

2. Tahap *Collection*

Tahap *Collection* Merupakan serangkaian kegiatan mengumpulkan data- data untuk mendukung proses penyidikan dalam rangka pencarian barang bukti kejahatan digital. barang bukti kejahatan digital. Pada tahap ini didalamnya terdapat proses pengambilan data dari sumber data yang relevan dan menjaga integritas barang bukti dari perubahan (Aziz et al., 2018). Pada tahap ini didalamnya terdapat proses pengambilan data dari sumber data yang relevan dan menjaga integritas barang bukti dari perubahan. serta memastikan bahwa data yang didapat berupa file tersebut asli sesuai dengan yang didapat pada tempat kejadian, untuk itu pada file digital perlu dilakukan identifikasi dan validasi file dengan teknik hashing (Mualfah & Ramadhan, 2020a)

3. Tahap *Examination*

Tahap *examination* atau tahap pemeriksaan ini merupakan tahap pemeriksaan data yang dikumpulkan secara forensik baik secara otomatis atau manual, serta memastikan bahwa data yang didapat berupa file tersebut asli

sesuai dengan yang didapat pada tempat kejadian kejahatan komputer, untuk itu pada file digital perlu dilakukan identifikasi dan validasi file dengan teknik hashing. peneliti kemudian melakukan uji coba terhadap smartphone dari setiap solusi yang mungkin dilakukan untuk pemecahan masalah. Tahapan pemeriksaannya sebagai berikut:

- Menggunakan Tool forensik yang digunakan pada tahap Pemeriksaan ini adalah *MOBILedit Forensic Express*. yang digunakan untuk keperluan mengakuisisi bukti digital pada *smartphone Android*.
- Menggunakan *Supersu* yaitu *Tools* untuk melakukan rooting pada *smartphone Samsung J1 prime*
- Menggunakan *FTK Imager* untuk melakukan *Tools* untuk melihat *struktur dan file dari hash*
- Menggunakan *Tools SQLite Viewer* dengan menggunakan *Tools* untuk membuka file database *SQLite* hasil akuisisi pada perangkat *smartphone*.

4. Tahap Analysis

Tahap analysis atau tahap meneliti ini dilakukan setelah mendapatkan file atau data digital yang diinginkan dari proses pemeriksaan sebelumnya, selanjutnya data tersebut dianalisis secara detail dan komprehensif dengan metode yang dibenarkan secara teknik dan hukum untuk dapat membuktikan data tersebut (Bintang et al., 2020) berguna dan dapat menjawab apa yang dibutuhkan sebagai pendorong untuk melakukan pengumpulan dan pemeriksaan data (Nasirudin et al., 2020)

5. Reporting

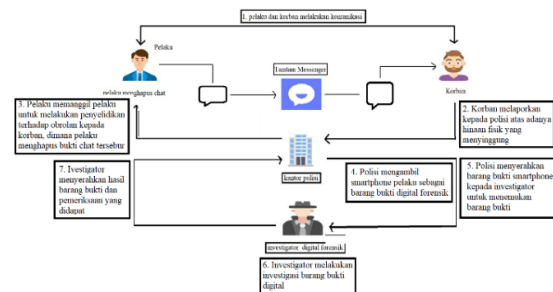
Tahap *reporting* atau tahap pelaporan dilakukan setelah diperoleh barang bukti digital dari proses pemeriksaan dan dianalisis. Selanjutnya pada tahap ini dilakukan pelaporan hasil analisis yang meliputi penggambaran tindakan yang dilakukan, dan memberikan rekomendasi untuk perbaikan kebijakan, metode, tool, atau aspek pendukung lainnya pada proses tindakan digital forensic (Bintang et al., 2020)

HASIL DAN PEMBAHASAN

Skenario kasus

Skenario kasus yang ditunjukkan dalam gambar 4.1 dibawah ini menjelaskan ada dua pengguna yang berkomunikasi menggunakan

aplikasi *TamTam Messenger* yaitu pelaku dan korban. Keduanya memiliki akun *TamTam Messenger*. Akun-akun tersebut digunakan untuk berkomunikasi satu sama lain dengan mengirim pesan melalui fitur *TamTam Messenger*. Pelaku mengirim percakapan kasar secara fisik kepada korban. Setelah mengirimkan percakapan, pelaku segera menghapus semua percakapan dan menghapus bukti.



Gambar 3 Pengujian Skenario Kasus

Berdasarkan simulasi kasus, dijelaskan bahwa ada dua pengguna yang berkomunikasi menggunakan *TamTam Messenger*: pengguna (pengirim pesan, pelaku) dan pengguna (penerima pesan, korban kejahatan). Keduanya memiliki akun *TamTam Messenger*. Akun-akun tersebut digunakan untuk berkomunikasi satu sama lain dengan mengirim pesan melalui fitur *TamTam Messenger*. Pengguna pengirim melempar percakapan kasar secara fisik ke pengguna penerima. Setelah mengirimkan percakapan, pengguna pengirim segera menghapus semua percakapan dan menghapus bukti. Penerima pesan sebagai korban melaporkannya kepada pihak berwajib tentang kejadian yang dialaminya.

Pihak berwenang mengeluarkan panggilan pengadilan dan surat perintah pengeledahan ke ponsel pengguna pengirim sebagai tanggapan atas laporan pengguna penerima, mengakses *TamTam Messenger* dan berkomunikasi dengan pengguna penerima. Setelah mengumpulkan bukti digital, polisi bertemu dengan penyidik dan menemukan bukti percakapan yang dihapus dari ponsel pelaku oleh pengirim. Penyidik kemudian melakukan penyidikan, menemukan barang bukti digital, membuat formulir hasil penyidikan, melaporkan hasil penyidikan, dan menyerahkan formulir penyidikan dan barang bukti digital yang diperoleh dari hasil penyidikan.

Tahapan Metode National Institute Of Justice

1. Preservation

Tahapan ini merupakan persiapan dalam melakukan investigasi. alat-alat yang diperlukan seperti perangkat keras berupa smartphone, laptop, kabel Laptop untuk keperluan investigasi dengan spesifikasi laptop *Acer Intel(R) Core(TM)*, smartphone *Merk Samsung J1 Prime* dan *Samsung A12* untuk keperluan investigasi.

A. Alat dan bahan

a) Perangkat keras

Berikut ini perangkat keras yang dibutuhkan pada penelitian ini, dapat dilihat di tabel 3.1 dibawah ini :

Tabel 1 Perangkat lunak

| No | Perangkat Keras | Kegunaan |
|----|-----------------|---|
| 1. | Laptop | Laptop untuk keperluan investigasi dengan spesifikasi <i>Acer Intel(R) Core(TM) i5-8250 CPU @ 2.60GHz, 2.60 GHz, 2,00 GB.</i> |
| 2. | Dua Smartphone | <i>Merk Samsung J2 Prime</i> dan <i>Samsung A12</i> untuk keperluan investigasi. |

b) Perangkat lunak

Berikut ini perangkat lunak yang dibutuhkan pada penelitian ini, dapat dilihat di tabel 3.2 dibawah ini :

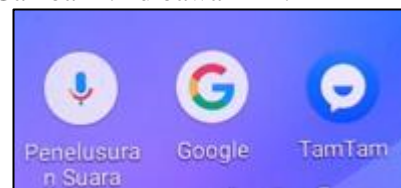
Tabel 2 Perangkat lunak

| No | Perangkat Keras | Kegunaan |
|----|------------------------------|--|
| 1. | <i>Windows 10 Pro 64 Bit</i> | Sebagai sistem operasi yang menjalankan <i>tools forensic</i> yang akan digunakan. |
| 2. | <i>Mobiledit</i> | <i>Tools</i> yang digunakan untuk keperluan mengakuisisi bukti digital pada <i>smartphone Android.</i> |
| 3. | <i>SuperSu</i> | <i>Tools</i> yang digunakan untuk keperluan mengakuisisi bukti digital pada <i>smartphone</i> |

| No | Perangkat Keras | Kegunaan |
|----|-------------------------------|---|
| 4. | <i>FTK Imager</i> | <i>Android.</i> <i>Tools</i> untuk melihat struktur dan file dari hash |
| 5. | <i>Sys Tools SQLiteViewer</i> | <i>Tools</i> untuk membuka file database <i>SQLite</i> hasil akuisisi pada perangkat <i>smartphone.</i> |
| 6. | <i>TamTam Messenger</i> | <i>Aplikasi</i> yang akan dilakukan investigasi |

2. Collection

Pada tahap ini investigator melakukan suatu pengumpulan bukti fisik berupa smartphone untuk keperluan investigasi, pengumpulan data, dan juga dokumentasi, bukti fisik dalam bentuk smartphone dapat dilihat pada Gambar 4.2 dibawah ini :



Gambar 4 Smartphone Menjadi barang bukti elektronik

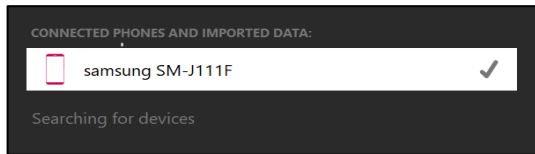
Pada gambar diatas Barang bukti elektronik berupa smartphone dengan sistem operasi *Android* yang terinstal aplikasi *TamTam Messenger*, alat komunikasi yang digunakan saat ini dicurigai adanya *cyberbullying*. Data yang diperoleh dari *smartphone* pelaku diperoleh dengan cara kloning untuk menghindari modifikasi data atau penghapusan data.

3. Tahap Examination

merupakan tahap investigasi atau pemeriksaan terhadap aplikasi *TamTam Messenger* yang gunakan sebagai alat komunikasi yang menunjukkan kejahatan *cyberbullying.*

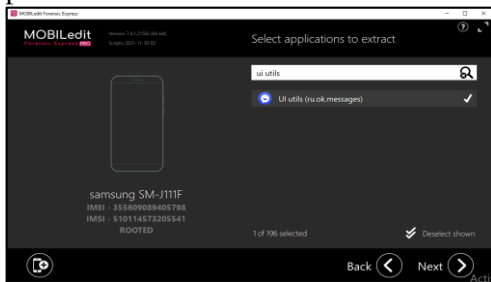
a) Tahap pengaktifkan jaringan pada smartphone dengan menjadikannya mode pesawat terlebih dahulu, berguna agar data yang ada tetap terjaga data sebelum dilakukan investigasi, Setelah mengubah jaringan ke mode pesawat, membuat cadangan data di *smartphone* dengan menggunakan alat *MobileEdit Forensic.* Didapatkan jenis *smartphone samsung SM-*

J111F yang akan dihubungkan di tools MobileEdit untuk *connected phone and imported data smartphone* tersebut dapat dilihat di Gambar 4.4 dibawah ini.



Gambar 5 Melakukan Backup data pada tools MobileEdit

- b) Aplikasi yang terdapat pada *smartphone Samsung SM-J111F* berjumlah 196 aplikasi. yang digunakan pada penelitian ini adalah *TamTam Messenger*. Tahapan ini akan dilakukan proses untuk mengambil data-data dari aplikasi dengan cara ekstrak, ditunjukkan pada Gambar 3.4 berikut ini.



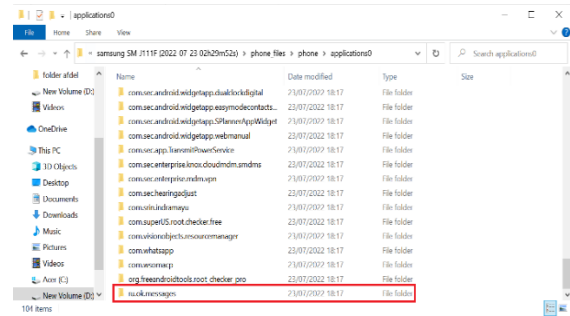
Gambar 6 Akuisisi pada aplikasi TamTam Messenger

- c) Tahapan selanjutnya menunjukkan file hasil backup data pada aplikasi *TamTam Messenger* yang telah didapatkan pada *smartphone* dengan nama *folder Samsung SM-J111F(2022-07-23- 02h29m52s)*, dapat dilihat pada Gambar 3.5 dibawah ini.



Gambar 7 Hasil akuisisi pada *smartphone*

- d) Tahap ini merupakan isi folder dari *smartphone* yang dibackup datanya. Gambar yang diberi kotak tanda merah merupakan file *ru.ok.messages* adalah nama file database dari aplikasi *TamTam Messenger* yang berhasil dibackup datanya yang dapat dilihat pada Gambar 3.6 dibawah ini.



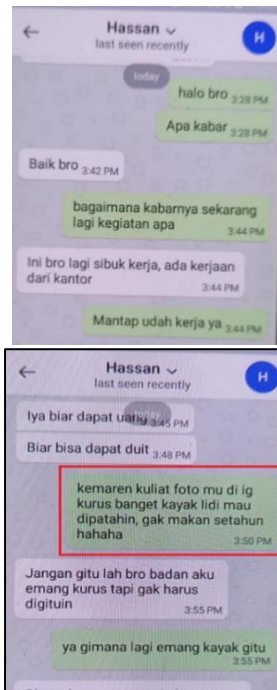
Gambar 8 Isi folder akuisisi pada aplikasi TamTam Messenger

4. Analisis

Tahapan ini merupakan tahapan analisis berupa temuan barang bukti digital yang sudah dibackup data dari pemeriksaan data digital forensik dengan menggunakan metode yang secara hukum benar dan memperoleh informasi yang berguna untuk kepentingan penyidik dan dapat dipertanggung jawabkan. Hasil analisis yang diperoleh pada penelitian ini dari aplikasi *TamTam Messenger* berupa *database* yang digunakan untuk melihat konten chat dari *database* dan memulihkan chat yang dihapus sebagai bukti digital yang dapat dipertanggung jawabkan. Tahap *analysis* ini berguna untuk mendapatkan hasil dari akuisisi yang dilakukan.

- a) Bukti digital *Chat* Sebelum dihapus

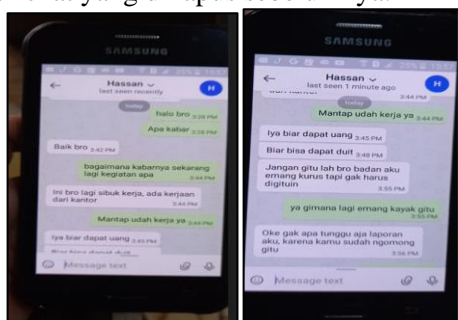
Berikut merupakan bukti chat komunikasi antara pelaku dan korban, dimana pelaku dan korban saling bertukar pesan menggunakan Aplikasi *TamTam Messenger*. Pada chat yang diberi tanda kotak yang berwarna merah terdapat isi chat mengenai *cyberbullying*, chat tersebut terindikasi penghinaan fisik kejahatan *cyberbullying*, ditunjukkan pada Gambar 3.7 berikut ini.



Gambar 9 Bukti digital chat sebelum dihapus

b) Bukti Digital Chat setelah dihapus

Berikut ini merupakan bukti digital chat yang telah dihapus pada akun pelaku. Pada gambar 3.8 ini dijelaskan terdapat perbedaan dari gambar 3.7 sebelumnya dimana pada Gambar 3.8 ini pelaku menghapus bukti chat yang telah dikirim sebelumnya. Maka dilakukan penelitian untuk mengembalikan pesan chat yang dihapus sebelumnya.



Gambar 10 Bukti chat yang telah dihapus

c) Hasil analisis Barang bukti yang ditemukan berikut merupakan tahap melakukan analisis barang bukti yaitu:

1. Untuk mengetahui struktur dari folder pada aplikasi TamTam Messenger dapat dilihat pada Gambar 3.9 merupakan struktur file folder dari aplikasi tamtam. terdapat folder backup yang dimana folder backup ini merupakan hasil proses akusisi pada barang bukti yang terdiri dari live_data yaitu berisi

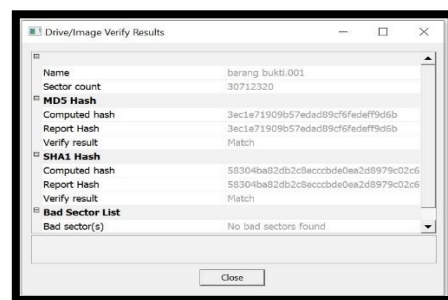
database aplikasi tamtam messenger, live_eksternal berisi folder gambar dan icon, description.info, ru.ok.messages.apk

| Name | Date modified | Type | Size |
|--------------------|-----------------|--------------|-----------|
| live_data | 23/07/2022 2:31 | File folder | |
| live_external | 23/07/2022 2:30 | File folder | |
| description.info | 23/07/2022 2:30 | INFO File | 1 KB |
| description.info | 23/07/2022 2:30 | XML Document | 3 KB |
| icon | 23/07/2022 2:30 | PNG File | 5 KB |
| ru.ok.messages.apk | 23/07/2022 2:30 | APK File | 24,274 KB |

Gambar 11 Struktur folder aplikasi TamTam Messenger

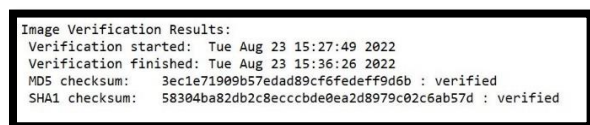
3. Nilai Hash sebelum dan sesudah menggunakan FTK Imager

Pada tahap ini Menjelaskan autentifikasi barang bukti digital. Hasil dari akuisisi yang ditemukan dilakukan verifikasi barang bukti untuk melihat hasil perbandingan nilai hashing sebelum dan sesudah di akuisisi, dapat dilihat pada gambar 3.10 berikut.



Gambar 12 Nilai Hash Sebelum diakuisisi

Tahap ini menjelaskan nilai hash sesudah diakuisisi tidak terjadi perubahan data dari MD5 Hash dan SHA1 Hash nilainya tetap sama yang telah diverification. dapat dilihat pada gambar 3.11 berikut.



Gambar 13 Nilai Hash sesudah diakuisisi

4. Hasil bukti digital yang ditemukan dari isi chat pada database

Tahap ini merupakan hasil bukti digital yang diperoleh setelah dilakukan analisis forensic menggunakan aplikasi systools sqlite viewer. menampilkan semua bukti percakapan yang dilakukan oleh akun pelaku dan akun korban, terdapat percakapan sedang melakukan

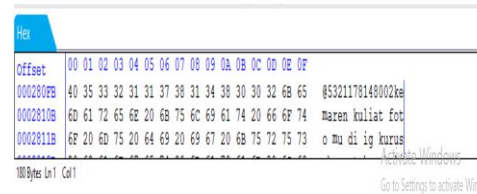
kejahatan *cyberbullying* berupa penghinaan fisik. Dimana terdapat pesan yang telah dihapus dari pelaku tersebut dan setelah dilakukan *recovery* data pada pesan yang dihapus tersebut, pesan berhasil di temukan, ditunjukkan pada Tabel 3.3 berikut.

Tabel 3 *Bukti digital chat pada aplikasi TamTam Messenger*

| No | Hex |
|------------|--|
| 1. | <pre> Hex Offset 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 00028552 2c 7f e3 01 82 2a 2c 73 e3 00 87 b6 47 7c 40 2d ,sA.,*sA..G @- 00028562 34 36 35 30 35 31 33 32 33 34 38 37 32 68 61 6c 4650513294972hal 00028572 6f 20 62 72 6f 1e 01 82 2a 2c 70 ed 0a 04 o bro...*pi.. </pre> |
| Keterangan | Akun Pelaku : hai bro |
| 2. | <pre> Hex Offset 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 00028494 2c 7f 4d 01 82 2a 2c 7f 4d 00 87 b6 47 7c 40 34 ,,M.,*..G @ 00028504 36 35 34 36 37 30 36 31 38 32 35 39 41 70 61 20 654670618259apa 00028514 68 61 62 61 72 1e 01 82 2a 2c 7c 54 0a 04 kabar...*/T.. </pre> |
| Keterangan | Akun Pelaku : apa kabar |
| 3. | <pre> Hex Offset 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 00028499 08 08 08 08 00 01 82 2a 39 3c 3f 6c 08 01 82 2a*9c1...* 000284a9 39 3c 3f 01 82 2a 39 3c 3f 00 88 d4 p8 4a cd 30 9c1..*9c1..0a1f0 000284b9 42 61 69 68 20 62 72 6f 14 0a 04 Baik bro... </pre> |

Keterangan Akun Korban : baik bro

4. pesan yang di hapus




Keterangan Akun pelaku : kemaren kuliat foto mu di ig kurus banget kayak lidi mau dipatahin, gak makan setahun hahaha

5. Report

Tahapan ini adalah tahapan pelaporan pada hasil yang sudah di dapatkan didalam analisis, termasuk mendeskripsi penelitian yang sudah dilakukan, menjelaskan *tools* forensik yang digunakan, serangkaian tahapan yang dipilih, kemudian menentukan tindakan berikutnya yang wajib dilakukan. memberi rekomendasi pada penelitian akhir agar dapat memperbaiki prosedur, *tools* forensik, dan aspek- aspek forensik lainnya. Tahapan pelaporan yang dilakukan penyidik.

Tabel 4 Hasil Reporting



FORM REPORTING INVESTIGASI
INFORMATICS ENGINEERING LABORATORY UNIVERSITAS
MUHAMMADIYAH RIAU
 Tuanku Tambusai street Pekanbaru city

| INFORMASI KASUS | |
|----------------------------|--|
| Nomor laporan | 2 |
| Nama kasus | Akuisisi bukti digital pada aplikasi TamTam Messenger kasus cyberbullying |
| Nomor kasus | 2 |
| Waktu dan tanggal | Sabtu 23 juli 2022 |
| PIHAK PENANGGUNG JAWAB | |
| investigator | Afdel Viransa |
| Nomor petugas investigator | 180401140 |
| Email | 180401140@student.umri.ac.id |
| Petunjuk investigator | Akuisisi bukti digital pada smartphone terhadap aplikasi <i>TamTam Messenger</i> |

| DESKRIPSI BUKTI | |
|--------------------------|---|
| Tipe barang bukti | <i>Android</i> |
| Nama perangkat | <i>Samsung J1 ace SM-J111F</i> |
| Nama pemilik perangkat | Surya |
| Peralatan yang digunakan | 1. Laptop 2. Kabel USB 3. <i>MobileEdit Forensic</i> 4. Aplikasi <i>TamTam Messenger</i> 5. <i>Systools SQLite Viewer</i> |
| Nomor model | <i>Samsung J1 ace SM-J111F</i> |
| kondisi | hidup |
| IMEI | 355609089405798 |
| catatan | Mengumpulkan dan mengangkat bukti digital pada <i>android</i> |
| Temuan barang bukti | Temuan data chatting yang dihapus pada perangkat <i>android</i> pada akun pelaku |
| Deskripsi kasus | Tindakan kasus kejahatan <i>cyberbullying</i> penghinaan fisik melalui aplikasi <i>TamTam messenger</i> |

SIMPULAN DAN SARAN

Kesimpulan

Hasil yang diperoleh dalam proses penelitian yang dilakukan dengan akuisisi bukti digital barang bukti pada smartphone android melalui aplikasi *TamTam Messenger* menggunakan metode *National Institute Of Justice (NIJ)* dapat ditarik kesimpulan sebagai berikut:

1. Percakapan berupa pesan yang dikirim oleh pelaku kepada korban yang terindikasi adanya kejahatan *cyberbullying* dalam aplikasi *TamTam Messenger* yang telah dihapus dapat dikembalikan melalui *tools MobileEdit forensic*.
2. Metode *national institute of justice (NIJ)* dalam proses identifikasi barang bukti dari aplikasi *TamTam Messenger* pada smartphone android dapat digunakan untuk akuisisi bukti digital. *tools MobileEdit forensic* yang digunakan berjalan baik dan dapat memenuhi kebutuhan pencarian barang bukti.

Saran

Berikut ini saran yang dapat dipertimbangkan untuk memperbaiki dan menyempurnakan penelitian ini dan untuk penelitian selanjutnya yaitu:

1. Pada penelitian selanjutnya diharapkan menggunakan fitur-fitur lainnya yang terdapat pada aplikasi *TamTam Messenger*.
2. Diharapkan pada penelitian selanjutnya dapat menggunakan sistem operasi yang

berbeda dari sebelumnya yaitu menggunakan iOS

3. Pada penelitian selanjutnya diharapkan menggunakan tools forensic yang berbeda karena setiap proses akuisisi data setiap *tools* berbeda-beda.

DAFTAR PUSTAKA

- [1] Aziz, M. A., Riadi, I., & Umar, R. (2018). 2616-6260-1-Sm. *Seminar Nasional Informatika UPN "Veteran" Yogyakarta, 2018*(November), 51–57.
- [2] Bintang, R. A., Umar, R., & Yudhana, A. (2020). Analisis Media Sosial Facebook Lite dengan tools Forensik menggunakan Metode NIST. *Techno (Jurnal Fakultas Teknik, Universitas Muhammadiyah Purwokerto)*, 21(2), 125.
- [3] D. Mualfah, & Riadi, I. (2017). Network Forensics For Detecting Flooding Attack On Web Server. *International Journal of Computer Science and Information Security*, 15(2), 430–436.
- [4] Mualfah, D., Putra, G. M., Firdaus, R., Komputer, F. I., & Riau, U. M. (n.d.). *ANALISIS PERBANDINGAN IPv4 DENGAN IPv6 PENGGUNAAN CCTV BERBASIS AREA TRAFFICT CONTROL SECURITY (ATCS)*. 124–128.
- [5] Mualfah, D., & Ramadhan, R. A. (2020a). Analisis Digital Forensik Rekaman Kamera CCTV Menggunakan Metode NIST (National Institute of Standards Technology). *IT Journal Research and Development*, 5(2), 171–182.
- [6] Mualfah, D., & Ramadhan, R. A. (2020b).

- Analisis Forensik Metadata Kamera CCTV Sebagai Alat Bukti Digital. *Digital Zone: Jurnal Teknologi Informasi Dan Komunikasi*, 11(2), 257–267.
- [7] Nasirudin, N., Sunardi, S., & Riadi, I. (2020). Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express. *Jurnal Informatika Universitas Pamulang*, 5(1), 89.
- [8] Riadi, I., Sunardi, S., & Sahiruddin, S. (2019). Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ). *Jurnal Rekayasa Teknologi Informasi (JURTI)*, 3(1), 87.
- [9] Riadi, I., Yudhana, A., Caesar, M., & Putra, F. (2018). 1490-Article Text-2859-1-10-20190413. *Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ)*, 4, 219–227.
- [10] Riskiyadi, M. (2020). Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime. *Cyber Security Dan Forensik Digital*, 3(2), 12–21.
- [11] sangadah, khotimatus, & Kartawidjaja, J. (2020). No Title. *Orphanet Journal of Rare Diseases*, 21(1), 1–9.
- [12] Sistem, R., Riadi, I., Umar, R., Syahib, M. I., Informasi, S. S., Dahlan, U. A., Informatika, S. T., & Dahlan, U. A. (2021). *Jurnal resti*. 1(10), 45–54.
- [13] Soni, Ramadhan, E., & Mualfah, D. (2021). Investigasi Bukti Digital Aplikasi WeChat Menggunakan Framework Integrated Digital Forensics Proses Model (IDFPM) Berbasis SNI 27037: 2014. *Jurnal INTEK*, 4(1), 25–31.
- [14] Sunardi, S., Riadi, I., & Triyanto, J. (2021). Analisis Forensik Layanan Signal Private Messenger pada Smartwatch Menggunakan Metode National Institute of Justice. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, 7(3), 305.
- [15] Syahib, M. I., Riadi, I., & Umar, R. (2020). Akuisisi Bukti Digital Aplikasi Viber Menggunakan Metode National Institute of Standards Technology (NIST). *J-SAKTI (Jurnal Sains Komputer Dan Informatika)*, 4(1), 170.