Jurnal Mobile and Forensics (MF)
Vol. 1, No. 1, Maret 2019, pp. 29-38
P-ISSN: 2656-6257, E-ISSN: 2714-6685, DOI: http://dx.doi.org/10.12928/mf.v1i1.705

FORENSIK WEB LAYANAN INSTANT MESSAGING MENGGUNAKAN METODE ASSOCIATION OF CHIEF POLICE OFFICERS

[1]Imam Riadi, [2]Rusydi Umar, [3] Muhammad Abdul Aziz
[1]Program Studi Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2, 3]Program Studi Teknik Informatika, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
email: [1]imam.riadi@is.uad.ac.id, [2]rusydi_umar@mtiuad.ac.id, [3]muhammad1807048013@webmail.uad.ac.id

Abstrak

Aplikasi *instant messaging* khususnya yang terdapat layanan berbasis *web*, sangat memungkinkan untuk dijadikan sasaran oleh para pelaku tindak kejahatan digital atau *cybercrime*. Vulnerabilitas dari aplikasi *instant messaging* berbasis *web* dapat dieksploitasi oleh pihak-pihak yang tidak bertanggung jawab untuk melakukan tindak kejahatan digital. Penelitian ini difokuskan pada tahapan-tahapan investigasi forensik kasus tindak kejahatan digital yang terjadi di layanan berbasis *web* aplikasi *instant messaging* WhatsApp, LINE dan Telegram. Metode yang digunakan dalam penelitian ini merujuk pada metode *Association of Chief Police Officers* dengan alur *plan*, *capture*, *analyse* dan *present*. Penelitian ini dalam proses investigasi forensiknya berhasil didapatkan *artifact* dari layanan berbasis *web* aplikasi *instant messaging*. Alat atau *tools* investigasi forensik yang digunakan dalam penelitian ini adalah FTK *imager*, NetWitness Investigator, dan Wireshark. Tingkat kerberhasilan penelitian ini mencapai 40% pada aplikasi Telegram, 60% untuk aplikasi LINE, dan aplikasi WhatsApp yang menduduki peringkat tertinggi dengan tingkat keberhasilan sebesar 85%.

Kata Kunci: Investigasi, Forensik, Kejahatan, Digital

PENDAHULUAN

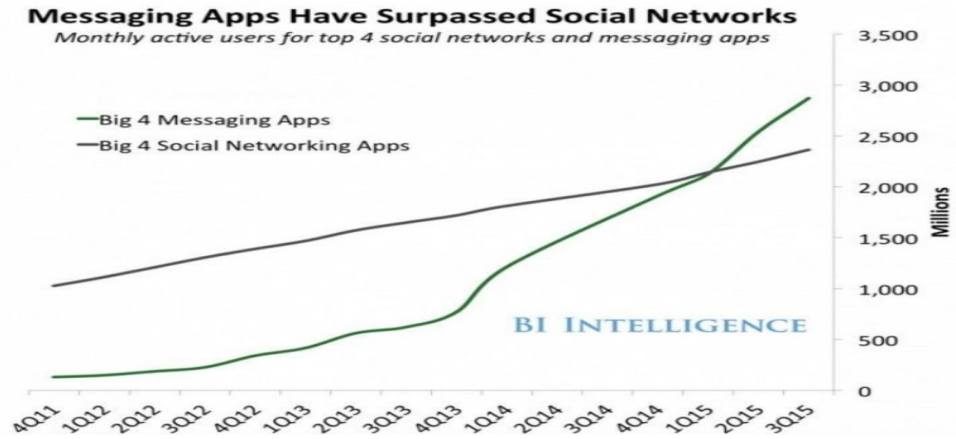
Instant messaging (IM) merupakan suatu aplikasi obrolan online yang menawarkan pesan teks secara *real-time* serta transmisi file audio, video, dan gambar melalui internet (Riadi, Fadlil, & Fauzan, 2018). Aplikasi IM kini telah memiliki layanan berbasis *web*, pengguna aplikasi IM selain dapat menggunakan aplikasi berbasis *smartphone* saat ini juga dapat menggunakan layanan aplikasi IM berbasis *web* yang dapat memudahkan pengguna khususnya untuk pengguna aplikasi IM yang lebih banyak bekerja di depan Komputer (Actoriano & Riadi, 2018). Aplikasi WhatsApp, LINE dan Telegram telah mengadopsi layanan IM berbasis *web*, dengan adanya layanan tersebut aplikasi IM semakin digemari oleh pengguna khususnya untuk kalangan dengan mobilitas yang tinggi (Chang & Chang, 2018).

Situs mambomedia.com pada tahun 2016 menunjukkan popularitas aplikasi *instant messaging* telah melebihi aplikasi media sosial, dijelaskan dalam situs tersebut pengguna aplikasi *instant messaging* pada tahun 2016 telah mencapai 2,5 miliyar pengguna aktif di seluruh dunia (Asyaky, 2019). Aplikasi IM lebih banyak digemari karena lebih praktis, dan mudah digunakan (Aziz, Riadi, & Umar, 2018). Gambar 1. menunjukkan grafik pertumbuhan pengguna aplikasi *instant messaging* dan aplikasi media sosial di seluruh dunia.

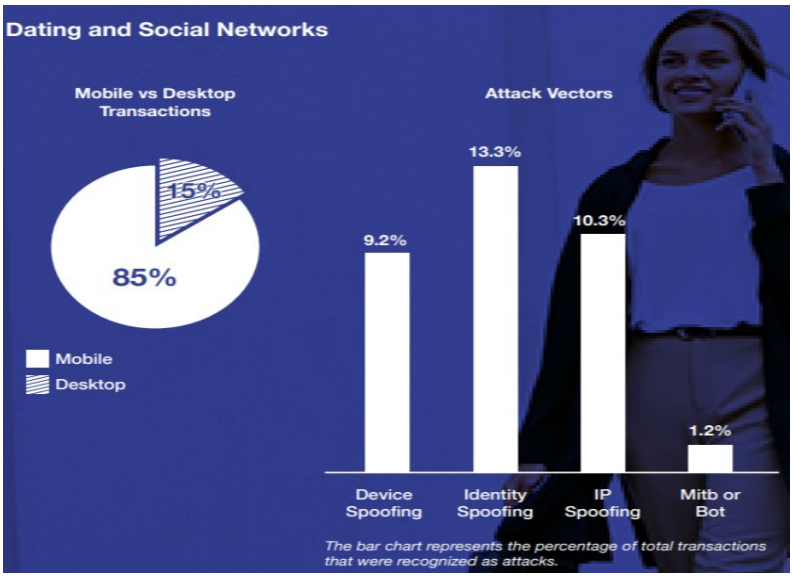
Pengguna aplikasi IM yang semakin banyak tentunya memberikan pengaruh positif dan tentunya juga memberikan pengaruh negatif, pengaruh negatif yang dimaksud adalah adanya pihak-pihak yang menyalahgunakan aplikasi *instant messaging* untuk melakukan kejahatan digital (Madiyanto, Mubarok, & Widiyasono, 2017). *Cyber-bullying*, perdagangan narkotika, dan perdagangan manusia adalah kejahatan digital yang sering terjadi pada aplikasi IM (Kukuh & Haryanto, 2018).

Received 10 April 2019; Revised 20 September 2019; Accepted 20 September 2019

Gambar 2. menunjukkan grafik tingkat kejahatan digital di seluruh dunia pada perangkat desktop dan perangkat *mobile* berdasarkan laporan yang dikeluarkan oleh ThreatMatrix pada tahun 2018 kuartal ke 2 (ThreatMetrix, 2018).



Gambar 1. Grafik pertumbuhan pengguna IM & media sosial di seluruh dunia



Gambar 2. Grafik tingkat kejahatan digital di seluruh dunia

Penyidik kejahatan digital perlu mewaspadai kejahatan digital yang terjadi di aplikasi *instant messaging*, dengan adanya layanan IM berbasis *web* penjahat dapat memanfaatkan layanan tersebut untuk melakukan penyadapan terhadap korbannya (Anwar & Riadi, 2017). Penelitian sebelumnya tentang investigasi forensik aplikasi IM berbasis *web* menggunakan parameter dari NIST menjelaskan forensik pada layanan IM berbasis *web* juga dapat diperoleh bukti digital yang dapat membantu penyidik dalam proses investigasi kejahatan digital (Riadi & Rauli, 2018).

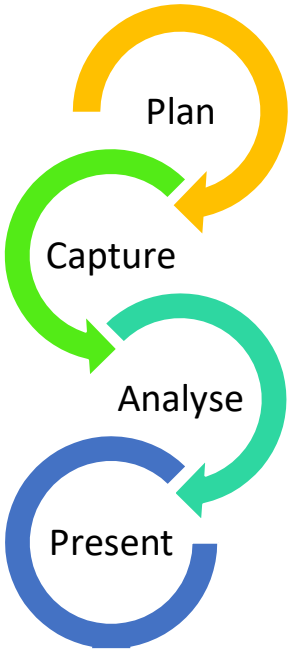
Penelitian ini difokuskan pada tahapan-tahapan forensik tindak kejahatan digital khususnya pada layanan IM berbasis *web*, agar dapat diperoleh *artifact* yang berguna untuk membantu dalam proses penyelesaian investigasi forensik (Riadi, Yudhana, Caesar, & Putra, 2018). FTK *imager*, NetWitness Investigator, dan Wireshark merupakan *tools* yang digunakan dalam proses penelitian ini (Riadi, Umar, &

Nasrulloh, 2018). Aplikasi IM WhatsApp, LINE dan Telegram menjadi objek penelitian ini karena ketiganya mendukung layanan IM berbasis *web* (Riadi, Sunardi, & Fauzan, 2018). Metode yang digunakan dalam penelitian ini mengacu pada parameter dari ACPO (*Association of Chief Police Officers*)(Umar, Riadi, & Maulana, 2017).

Hasil atau *artifact* yang diperoleh dari penelitian ini dapat berupa file *log*, *chace*, dan *image* dari ketiga aplikasi IM tersebut (Fauzan, Riadi, & Fadlil, 2017). Hasil yang diperoleh dari penelitian ini selanjutnya dijadikan parameter untuk mengukur tingkat keberhasilan penelitian ini (Yusoff, Dehghantanha, & Mahmod, 2017). Penelitian ini dapat dijadikan referensi penyidik dalam mengungkap kasus kejahatan digital khususnya yang terjadi dalam aplikasi IM berbasis *web* (Faiz, Umar, & Yudhana, 2017).

METODE PENELITIAN

Tujuan dari penelitian ini adalah menggunakan *tools* FTK *imager,* NetWitness Investigator, dan Wireshark untuk melakukan analisis forensik pada layanan aplikasi *instant messaging* berbasis *web*. Penelitian ini mengadaptasi pada proses investigasi digital forensik dengan menggunakan *metode Association of Chief Police Officers* (ACPO). Metode tersebut digunakan untuk menjabarkan bagaimana gambaran proses investigasi forensik yang sedang dilakukan, agar bisa diketahui tahapan-tahapan investigasi forensik secara lebih jelas dan mudah dipahami. Tahapan metode penelitian dapat dilihat pada Gambar 3.



Gambar 3. Skema Metode ACPO

Gambar 3 menjelaskan secara garis besar mengenai tahapan-tahapan metode ACPO, adapun penjelasan lengkapnya adalah sebagai berikut :

- *Plan* : Tahap ini disebut juga tahap perencanaan. Tahap ini merupakan proses merencanakan tindakan-tindakan yang akan dilakukan pada saat penelitian, perencanaan diperlukan agar proses penelitian berjalan lancar termasuk dalam menentukan perangkat lunak yang akan digunakan pada proses penelitian agar dapat diperoleh hasil penelitian yang valid.

- *Capture* : Tahap ini merupakan tahap merekam, menyimpan, menangkap dan mengumpulkan semua hasil yang di dapat dari proses penelitian. Proses capture pada hasil yang diperoleh dari proses penelitian dapat menggunakan bantuan dari perangkat lunak yang ada atau dapat juga menggunakan bantuan perangkat keras.
- *Analyse* : Tahap ini adalah proses analisis secara luas yang dilakukan pada hasil yang telah dikumpulkan dengan menggunakan metode yang dibenarkan secara teknik, untuk mendapatkan informasi yang berguna dan menjawab pertanyaan-pertanyaan yang menjadi pendorong melakukan pengumpulan dan pemeriksaan. Tahap ini dilakukan analisis terhadap semua temuan pada proses penelitian dengan membuat perbandingan dari setiap temuan untuk dapat diambil data yang valid tentang proses penelitian.
- *Present* : Tahap ini adalah tahap publikasi dari data penelitian yang merupakan sebuah informasi yang berguna dan dapat dipertanggungjawabkan kebenarannya. Tahap ini dilakukan penjelasan tentang semua tindakan yang telah dilakukan pada saat penelitian dan menjelaskan secara detail tentang hasil dari penelitian tersebut, memberikan masukan atau saran yang berhubungan dengan hasil dari penelitian tersebut.

Penelitian ini dalam prosesnya membutuhkan alat atau *tools* yang digunakan untuk memperoleh *artifact* dari aplikasi IM. Alat atau *tools* yang digunakan dalam penelitian ini dibagi menjadi dua jenis : alat eksperimental dan alat forensik. Tabel 1. Menjelaskan tentang alat eksperimental yang digunakan dalam penelitian. Tabel 2. Menunjukkan alat forensik yang digunakan dalam penelitian.

Tabel 1. Alat eksperimental

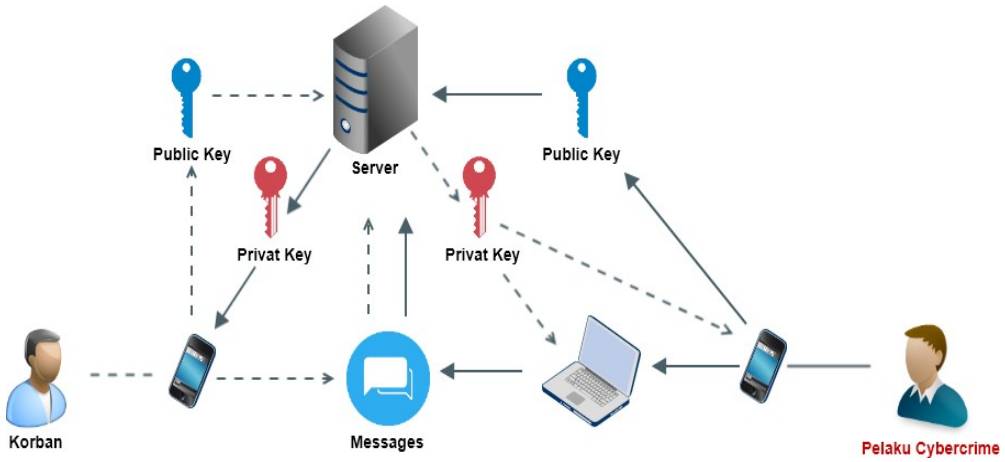
Alat Eksperimental	Keterangan
Laptop LENOVO seri 880E4	Windows 10 OS 64 Bit 4 GB RAM Core i7
Xiaomi A1	Android Pie 9.0 RAM 4GB
WhatsApp	Versi 2.18.341
LINE	Versi 8.17.1
Telegram	Versi 5.5.0

Tabel 2. Alat forensik

Alat Forensik	Version	Keterangan
FTK imager	4.2.013	Open Source
NetWitness Investigator	10.6	Propietary
Wireshark	3.0.1	Open Source

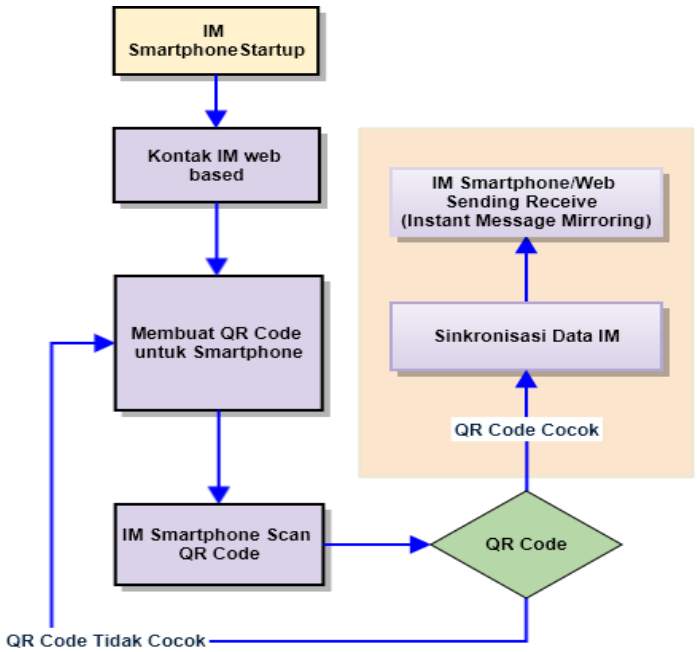
Simulasi Kejahatan Digital

Penelitian ini menggunakan simulasi tindak kejahatan digital pada aplikasi IM, simulasi tersebut melibatkan satu orang pelaku kejahatan dan satu orang korban. Pelaku kejahatan dan korban menggunakan aplikasi IM berbasis *smartphone* untuk saling mengirimkan pesan. Aplikasi IM yang digunakan dalam simulasi ini adalah WhatsApp, LINE, dan Telegram. Gambar 4. Menunjukkan skema simulasi kejahatan digital pada layanan aplikasi *instant messaging*.



Gambar 4. Skema simulasi kejahatan digital

Gambar 4 Merupakan skema simulasi kejahatan digital pada aplikasi IM, simulasi ini dimulai dengan terlebih dahulu melakukan proses *mirorring* pada aplikasi IM pelaku yaitu menghubungkan aplikasi IM dari perangkat *smartphone* pelaku ke aplikasi IM berbasis *web*. Skema proses menghubungkan aplikasi IM berbasis *smartphone* milik pelaku dengan aplikasi IM berbasis *web* dapat dilihat pada Gambar 5. Aplikasi IM yang digunakan dalam penelitian ini seluruhnya telah menggunakan sistem *end-to-end encryption,* sehingga dapat dipastikan pesan yang masuk dan keluar telah terenkripsi. Pelaku dan korban saling mengirim pesan melalui perangkat *smartphone*-nya masing-masing, selanjutnya dilakukan *capturing* dan analisis forensik pada aplikasi IM berbasis *web* yang telah di-*mirorring* dengan aplikasi IM berbasis *web* milik pelaku kejahatan. Hasil yang diperoleh dari analisis forensik ketiga aplikasi IM tersebut dicatat dan dibandingkan hasilnya.



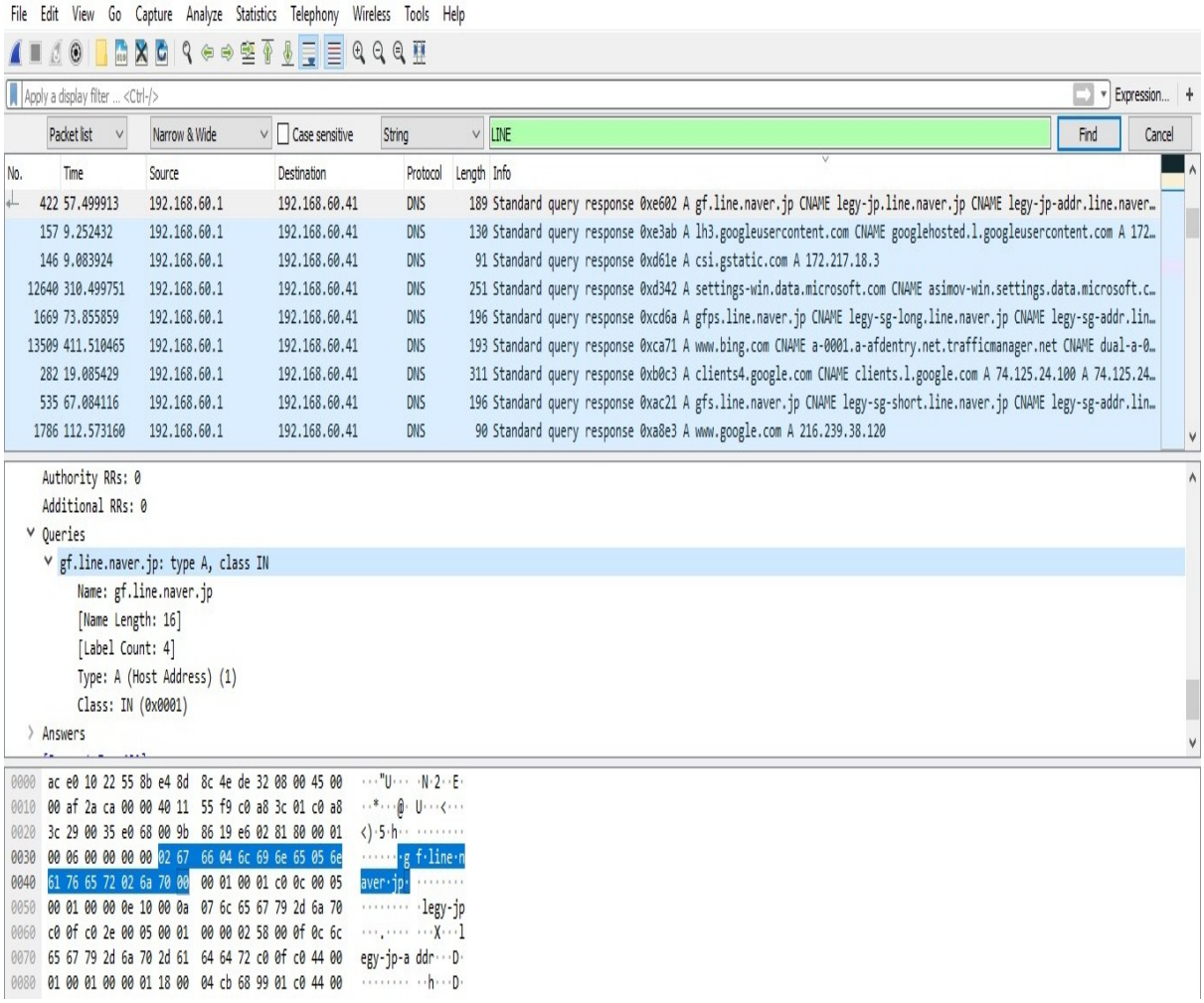
Gambar 5. Skema proses *mirorring* aplikasi IM pelaku kejahatan digital

Gambar 5. Menjelaskan tentang proses *mirorring* aplikasi IM pelaku kejahatan digital dengan aplikasi IM berbasis *web*. Prosesnya dengan mengakses aplikasi IM berbasis *web* kemudian dibuat QR code dari aplikasi IM berbasis *web* tersebut. QR code yang telah dibuat di-*scan* menggunakan perangkat *smartphone* pelaku kejahatan, jika QR code cocok maka proses *mirorring* selesai tetapi apabila QR code tidak cocok maka akan dibuatkan lagi QR code yang baru.

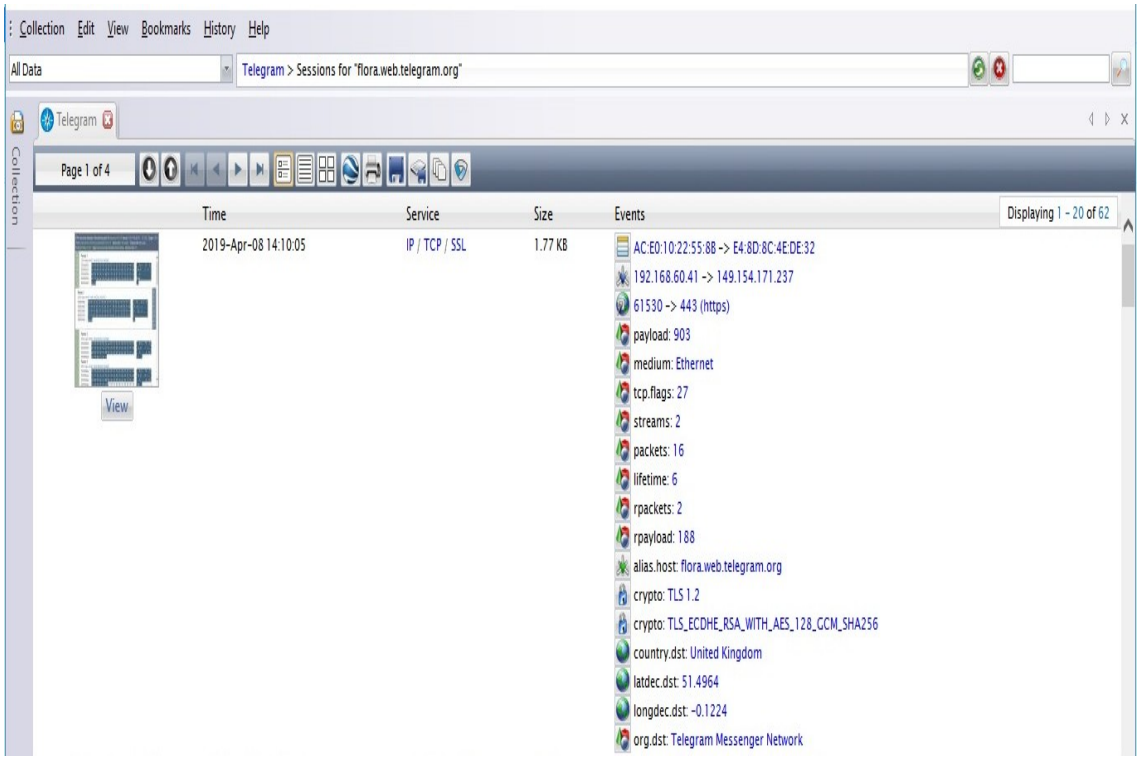
HASIL DAN PEMBAHASAN

Network Capture Analyse

Tahap ini dilakukan analisis terhadap *network* yang telah ditangkap menggunakan *tools* Wireshark. Gambar 6. Menunjukkan proses *capturing network* dengan menggunakan *tools* Wireshark. NetWitness Investigator merupakan *tools* yang digunakan untuk mempermudah proses analisis *network* yang telah ditangkap menggunakan *tools* Wireshark. Gambar 7. Menunjukkan proses analisis *network* yang berasal dari hasil *capture tools* Wireshark.



Gambar 6. Proses *capturing network*



Gambar 7. Proses analisis *network capture*

Gambar 7. Menunjukkan proses analisis hasil dari *network capturing* dengan menggunakan *tools* Wireshark. Hasil dari *netwotk capturing* tersebut berupa file .pcap yang nantinya akan diimport ke *tools* NetWitness Investigator. Tabel 3. Menunjukkan hasil analisis pcap file dengan menggunakan *tools* NetWitness Investigator.

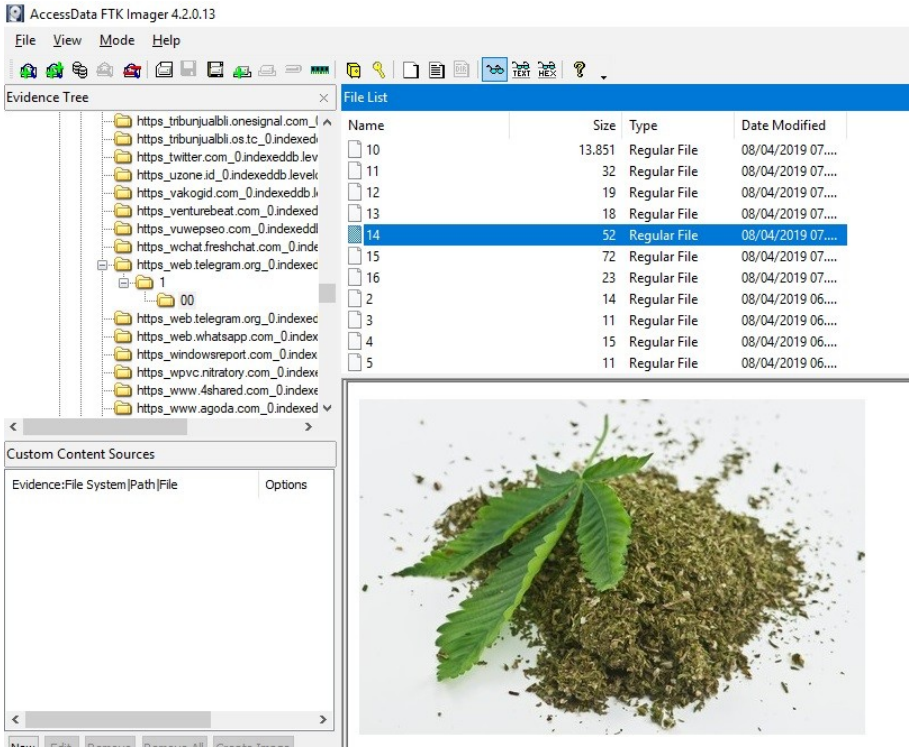
Tabel 3. Hasil analisis dengan NetWitness Investigator

IM	Keterangan
WhatsApp	Encrypted: Curve25519 *for key exchange and* AES256 *in* CBC *mode for message encryption and uses* HMAC-SHA256 for *message authenticity and integrity.*
LINE	Encrypted : TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
Telegram	Encrypted : TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Berdasarkan Tabel 3. Menunjukkan bahwa paket *network* yang berasal dari aplikasi instant messaging semuanya telah dienkripsi dengan algoritma-nya masing-masing. Hasil dari analisis ini membuktikan bahwa aplikasi IM WhatsApp, LINE, dan Telegram telah menggunakan sistem *end-to-end encryption*.

Analisis forensik *web*

Investigasi forensik pada aplikasi IM berbasis *web* dilakukan dengan cara mengeksplorasi SQLite IM *database* pada browser google chrome. FTK *imager* merupakan *tools* digunakan dalam proses eksplorasi ini. SQLite *database* berada di lokasi C:\Users\Admin\AppData\LocaI\GoogIe\Chrome\User Data\DefauIt. Gambar 8. Menunjukkan proses eksplorasi SQLite database pada browser google chrome.



Gambar 8. Proses ekplorasi SQLite database pada browser google chrome

Gambar 8. Menunjukkan proses eksplorasi SQLite database pada browser google chrome dengan menggunakan tools FTK *imager* gambar tersebut merupakan artifact yang terdapat pada SQLite database browser google chrome. Gambar narkotika tersebut sebelumnya tedapat di *chat* aplikasi telegram berbasis *web*, hal tersebut membuktikan bahwa investigasi forensik juga dapat dilakukan pada aplikasi IM berbasis *web*. Tabel 4. Menunjukkan hasil temuan dari proses eksplorasi SQLite database pada browser google chrome.

Tabel 4. Hasil eksplorasi SQLite *database*

IM	Parameter Pengukuran				
	Log file	***Cache***	***text***	***Image***	***Id***
WhatsApp	✓	✓	×	✓	✓
LINE	✓	✓	×	✓	×
Telegram	✓	×	×	✓	×

Berdasarkan Tabel 4. Dapat diketahui dari proses eksplorasi SQLite *database* dari ketiga aplikasi IM tersebut, pada aplikasi WhatsApp ditemukan 4 parameter dari total 5 parameter yang menjadi acuan penelitian. Aplikasi LINE memperoleh temuan sebanyak 3 parameter dan aplikasi Telegram hanya memperoleh temuan 2 parameter. Penelitian ini menggunakan perhitungan dari total parameter yang ditemukan untuk dapat menetukan tingkat keberhasilan proses digital forensik pada layanan aplikasi *instant messaging* berbasis *web*. Parameter yang ditemukan dihitung dengan menggunakan rumus selanjutnya dibandingkan dengan hasil dari aplikasi IM yang lainnya.

$$Pon = \frac{\sum Pn}{\sum Po} \times 100\%$$

Persamaan tersebut digunakan untuk menghitung indeks angka dari tingkat keberhasilan proses digital forensik pada layanan aplikasi IM berbasis *web*, dari hasil perhitungan tersebut aplikasi WhatsApp memperoleh angka indeks sebesar 80 %, diikuti dengan aplikasi LINE sebesar 60 %, dan aplikasi Telegram sebesar 40%. Indeks angka yang diperoleh aplikasi IM dibandingkan untuk untuk mengetahui tingkat keberhasilan digital forensik pada aplikasi IM berbasis *web*. WhatsApp merupakan aplikasi dengan tingkat keberhasilan forensik digital tertinggi karena memiliki nilai indeks sebesar 80% yang merupakan nilai yang paling tinggi dibandingkan dengan LINE yang memiliki nilai indeks sebesar 60% dan Telegram dengan nilai indeks sebesar 40%.

KESIMPULAN

Pengguna aplikasi *Instant messaging* yang semakin banyak menyebabkan semakin besar peluang terjadinya kejahatan digital pada aplikasi IM. Layanan aplikasi IM berbasis *web* juga tidak luput dari ancaman tidak kejahatan digital. Proses digital forensik pada *smartphone* berbeda dengan proses digital forensik pada layanan IM berbasis *web*, tingkat keberhasilan proses digital forensiknya juga berbeda. Penelitian ini menggunakan metode *Association of Chief Police Officers* (ACPO) untuk mengetahui tingkat keberhasilan proses digital forensik pada aplikasi IM berbasis *web*. Wireshark dan NetWitness Investigator merupakan *tools* yang digunakan untuk menganalisa network pada aplikasi IM berbasis *web,* dengan *kedua tools* tersebut dapat diketahui bahwa ketiga aplikasi IM yang digunakan dalam penelitian ini telah terenkripsi dengan algoritma enkripsi masing-masing. FTK imager merupakan *tools* yang dapat digunakan untuk melakukan digital forensik pada aplikasi IM berbasis *web*. WhatsApp menduduki peringkat pertama aplikasi IM berbasis *web* dengan tingkat keberhasilan proses digital forensik mencapai 80 %, disusul dengan aplikasi LINE dengan tingkat keberhasilan mencapai 60%, posisi terakhir diduduki oleh aplikasi Telegram dengan tingkat keberhasilan hanya 40%.

DAFTAR PUSTAKA

[1] Actoriano, B., & Riadi, I. (2018). Forensic Investigation on Whatsapp Web Using Framework Integrated Digital Forensic Investigation on Whatsapp Web Using Framework Integrated Digital Forensic Investigation Framework Version 2, (September).

[2] Anwar, N., & Riadi, I. (2017). Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web. Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika, 3(1), 1–10. https://doi.org/10.26555/jiteki.v3i1.6643

[3] Asyaky, M. S. (2019). Analisis dan Perbandingan Bukti Digital Aplikasi Instant Messenger Pada Android, 3(October).

[4] Aziz, M. A., Riadi, I., & Umar, R. (2018). Menggunakan Framework National Institute of Justice, 2018(November), 51–57.

[5] Chang, M. S., & Chang, C. Y. (2018). Forensic Analysis of LINE Messenger on Android. Journal of Computers, 29(1), 11–20. https://doi.org/10.3966/199115992018012901002

[6] Faiz, M. N., Umar, R., & Yudhana, A. (2017). Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email. JISKa, 1(February), 108–114. https://doi.org/10.14421/jiska.2017.13-02

[7] Fauzan, A., Riadi, I., & Fadlil, A. (2017). Analisis Forensik Digital Pada Line Messenger Untuk Penanganan Cybercrime. Annual Research Seminar (ARS), 2(1), 159–163. Retrieved from http://seminar.ilkom.unsri.ac.id/index.php/ars/article/view/832/752

[8] Kukuh, M., & Haryanto, T. (2018). Analisa Forensics Terhadap Database Sqlite pada Aplikasi IMO Berbasis Android.

[9] Madiyanto, S., Mubarok, H., & Widiyasono, N. (2017). Mobile Forensics Investigation Proses Investigasi Mobile Forensics Pada Smartphone Berbasis IOS. Jurnal Rekayasa Sistem & Industri (JRSI), 4(01). https://doi.org/10.25124/jrsi.v4i01.149

[10] Riadi, I., Fadlil, A., & Fauzan, A. (2018). Evidence Gathering and Identification of LINE Messenger on Android Device. International Journal of Computer Science and Information Security (IJCSIS), 16(June), 201–205.

[11] Riadi, I., & Rauli, E. (2018). Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics. Scientific Journal of Informatics (SJI) UNNES, 10(1), 18–22.

[12] Riadi, I., Sunardi, S., & Fauzan, A. (2018). Examination of Digital Evidence on Android-based LINE Messenger. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 7(3), 337–343.

[13] Riadi, I., Umar, R., & Nasrulloh, I. M. (2018). Analisis Forensik Digital Pada Frozen Slod State Drive Dengan Metode National Institute of Justice (Nij), 3(May), 70–82. https://doi.org/10.21831/elinvo.v3i1.19308

[14] Riadi, I., Yudhana, A., Caesar, M., & Putra, F. (2018). Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ), 4, 219–227.

[15] ThreatMetrix. (2018). Q2 2018 Cybercrime Report, 2018(June), 1–13. https://doi.org/10.14084/j.cnki.cn62-1185/c.2018.02.021

[16] Umar, R., Riadi, I., & Maulana, G. (2017). A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements. International Journal of Advanced Computer Science and Applications, 8(12), 69–75. https://doi.org/10.14569/IJACSA.2017.081210

[17] Yusoff, M. N., Dehghantanha, A., & Mahmod, R. (2017). Forensic Investigation of Social Media and Instant Messaging Services in Firefox OS. Contemporary Digital Forensic Investigations of Cloud and Mobile Applications, 41–62. https://doi.org/10.1016/B978-0-12-805303-4.00004-6