

# ANALISIS FORENSIK LINE MESSENGER BERBASIS WEB MENGUNAKAN *FRAMEWORK NATIONAL INSTITUTE OF JUSTICE* (NIJ)

Muhammad Abdul Aziz<sup>(1)</sup>, Imam Riadi<sup>(2)</sup>, Rusydi Umar<sup>(3)</sup>  
<sup>(1)(3)</sup> Program Studi Teknik Informatika, Universitas Ahmad Dahlan  
<sup>(2)</sup> Program Studi Sistem Informasi, Universitas Ahmad Dahlan

Jl. Prof. Soepomo, S.H. Janturan, Warungboto, Umbulharjo, Kota Yogyakarta, 55164, Indonesia.  
e-mail : [jizzflame@gmail.com](mailto:jizzflame@gmail.com)<sup>(1)</sup>, [imam.riadi@is.uad.ac.id](mailto:imam.riadi@is.uad.ac.id)<sup>(2)</sup>, [rusydi.umar@rocketmail.com](mailto:rusydi.umar@rocketmail.com)<sup>(3)</sup>

## Abstrak

Aplikasi LINE messenger yang berbasis web atau smartphone, sangat memungkinkan dimanfaatkan untuk melakukan tindak kejahatan digital dengan menggunakan layanan, informasi pribadi user, maupun dengan meretas aplikasi LINE messenger tersebut. Penelitian ini menjelaskan tahapan-tahapan investigasi kasus cybercrime yang terjadi di LINE messenger berbasis web. Metode yang digunakan untuk penelitian ini merujuk pada tahapan penyelidikan yang pernah dilakukan pada penelitian-penelitian terdahulu, yaitu menggunakan metode National Institute of Justice (NIJ) dengan alur tahap preparation, tahap collection, tahap examination, tahap analysis, dan tahap reporting. Media yang digunakan dalam penelitian ini adalah aplikasi LINE messenger berbasis web yang disinkronkan dengan LINE messenger berbasis android. Penelitian ini dalam prosesnya berhasil didapatkan lokasi file log, cache, dan file gambar bukti digital pada percakapan aplikasi LINE messenger berbasis web. Bukti digital forensik yang didapat diharapkan dapat memperkuat bukti kasus kejahatan di pengadilan dalam bentuk hasil analisis bukti digital.

**Kata Kunci** : Forensik, LINE, Investigasi, cybercrime.

## 1. PENDAHULUAN

LINE messenger adalah jenis program obrolan online yang menawarkan pesan teks secara real-time serta transmisi file audio, video, dan gambar melalui Internet. LINE messenger termasuk ke dalam salah satu aplikasi yang paling banyak digunakan di negara-negara Asia, secara khusus LINE messenger banyak digunakan oleh pengguna yang lebih menyukai tampilan menarik dan fitur emoji yang memberikan banyak pilihan dalam mengekspresikan maksud dari sebuah percakapan. Menurut data statistik website *Busines of Apps* jumlah pengguna LINE messenger aktif bulanan di seluruh dunia tahun 2016 mencapai 217 juta pengguna (Artyom Dogtiev, 2018).

LINE secara resmi mengumumkan peluncuran fitur LINE messenger Google Chrome Extension pada tanggal 29 Juli 2015. Fitur ini diluncurkan untuk memfasilitasi penggunaan aplikasi ini khususnya untuk pengguna berbasis komputer. LINE messenger berbasis web sama seperti LINE messenger berbasis smartphone, fitur tersebut juga tersedia untuk lintas platform seperti Chrome, Windows, Mac, dan Linux (LINE, 2015). Pengguna aplikasi LINE messenger yang banyak dan tersebar luas juga membawa beberapa masalah salah satunya adalah cybercrime seperti perdagangan narkoba, cyber-bullying, dan perdagangan manusia (Umar, Riadi, & Maulana, 2017). Studi komprehensif PBB menjelaskan bahwa Cybercrime terbatas pada jumlah tindakan terhadap kerahasiaan, integritas, dan availability dari data atau sistem komputer (Riadi, Fadlil, & Fauzan, 2018).

Cybercrime sekarang telah menjadi ancaman nomor satu aplikasi pesan singkat, untuk menyelesaikan Cybercrime berbasis pesan singkat, penyidik perlu melakukan analisis forensik terhadap perangkat korban dan tersangka agar dapat menemukan bukti-bukti digitalnya (Capstone, 2018)(Chang & Chang, 2018). Analisis pada digital forensik dapat menggunakan metode *National Institute of Justice* atau dapat menggunakan metode *National Institute of Standards and Technology* (Riadi, Umar, & Nasrulloh, 2018). Berdasarkan penelitian terdahulu dapat diketahui bukti potensial apa saja yang terdapat pada aplikasi pesan singkat seperti tanggal/waktu, pesan teks, dan gambar/foto (Riadi, Yudhana, Caesar, & Putra, 2018). Penelitian yang dilakukan diharapkan dapat menghasilkan bukti digital yang dapat memperkuat bukti kasus kejahatan di pengadilan dalam bentuk hasil analisis bukti digital.

## 2. TINJAUAN PUSTAKA

Penelitian (Riadi, Fadlil, et al., 2018) mereka dapat mengakuisi bukti digital dari perangkat Android dengan menggunakan tools MOBILEdit kemudian dilakukan ekstraksi dan identifikasi pada bukti digital tersebut. Penelitian (Chang & Chang, 2018) mereka melakukan pengungkapan artefak dari LINE messenger

pada *volatile memori* dan *non-volatile memori* BlueStacks App Player dengan menggunakan metode *anti-forensic*.

Penelitian (Umar et al., 2017) mereka dapat mengevaluasi *tools* forensik yang ada untuk melakukan analisis forensik pada WhatsApp menggunakan parameter dari NIST dan artefak WhatsApp. Hasil penelitian tersebut menunjukkan bahwa Belkasoft Evidence memiliki indeks angka tertinggi, Key/DB Extractor memiliki keunggulan dari segi biaya, dan Oxygen memiliki keunggulan dalam memperoleh artefak WhatsApp. Penelitian (Riadi, Yudhana, et al., 2018) mereka dapat memperoleh *evidence* pada *Instagram Messenger* dengan menggunakan prosedur NIJ dan *tools OXYGEN*.

Penelitian (Anwar & Riadi, 2017) mereka dapat memperoleh bukti digital pada aplikasi WhatsApp *Messenger* berbasis android dan analisis *evidence* pada aplikasi WhatsApp *Messenger* berbasis *web* menggunakan metode NIST. Penelitian (Yusoff, Dehghantaha, & Mahmud, 2017) mereka berhasil mendapatkan artefak sosial media dan aplikasi pesan singkat yang telah dihapus pada FireFox OS menggunakan *tools* ADB dan LiME. Penelitian (Yang, Dehghantaha, Choo, & Muda, 2016) mereka dapat mengakusisi dan menganalisis artefak dari aplikasi pesan singkat pada Windows 10 menggunakan *tools* FTK Imager dan Autopsy.

Penelitian (Riadi, Sunardi, & Fauzan, 2018) mereka dapat mengevaluasi kemampuan dari *tools* Oxygen dan MOBILedit untuk melakukan analisis forensik pada aplikasi LINE *messenger* berbasis android memanfaatkan metode NIST. Penelitian (Fauzan, Riadi, & Fadlil, 2017) mereka dapat mengakusisi dan menganalisis bukti digital dari aplikasi LINE *messenger* berbasis android dengan *tools* KAMAS Lite dan AFLogical OSE, menggunakan metode yang terdiri dari langkah NIST. Penelitian (Ikhsani & Hidayanto, 2016) mereka dapat mengakusisi bukti digital dari aplikasi Whatsapp dan LINE di *smarthphone* dengan menggunakan cara manual dan dengan bantuan aplikasi FTK *imager* dan SQLite.

### 3. METODE PENELITIAN

#### 3.1. Metode Penelitian

Penelitian ini mengadaptasi pada proses investigasi metode analisis forensik NIJ. Metode tersebut digunakan untuk mejabarkan bagaimana gambaran proses penelitian yang sedang dilakukan agar bisa diketahui tahapan penelitian ini secara lebih sistematis sehingga dapat untuk dijadikan referensi pada penelitian selanjutnya. Tahapan metode penelitian dapat dilihat pada Gambar 1.



Gambar 1. Tahapan Metode Penelitian

Metode penelitian ini terbagi menjadi beberapa tahapan yakni tahap *Preparation*, tahap *collection*, tahap *examination*, tahap *analysis*, dan tahap *reporting*, tahapan metode NIJ dijelaskan secara lengkap sebagai berikut :

Tahap pertama adalah *preparation* atau persiapan merupakan suatu kegiatan mempersiapkan peralatan untuk melakukan tugas yang diperlukan dalam proses penyelidikan. Pada tahap ini didalamnya terdapat proses menyiapkan alat-alat yang akan digunakan pada proses penyelidikan.

Tahap kedua adalah *collection* atau koleksi adalah proses pencarian dokumen, dan mengumpulkan data-data atau membuat salinan dari objek fisik yang terdapat bukti digital di dalamnya. Tahap *collection* ini pada prosesnya dilakukan pengambilan data barang bukti digital dari suatu sumber yang relevan agar dapat menjaga orisinalitas bukti digital dari kemungkinan terjadinya perubahan.

Tahap ketiga adalah *examination*, tahap ini merupakan tahap untuk melakukan pemeriksaan bukti digital yang didapatkan melalui proses forensik dengan cara manual maupun otomatis dan untuk memastikan bukti digital yang diperoleh tersebut orisinal sama seperti yang diperoleh di tempat terjadinya kejahatan.

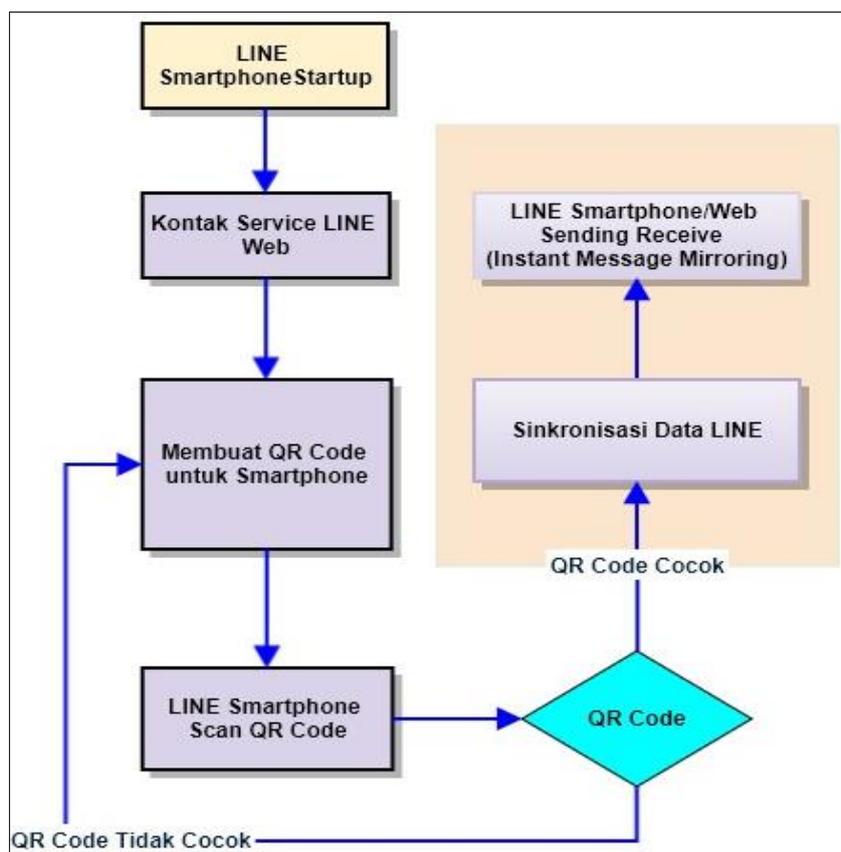
Tahap keempat adalah *analysis*, setelah diperoleh bukti digital yang dibutuhkan dari tahap penyelidikan sebelumnya, kemudian bukti digital yang diperoleh dianalisa dengan detail menggunakan metode yang telah diakui secara ilmiah dan secara hukum agar dapat menentukan nilai signifikansi bukti digital tersebut.

Tahap kelima adalah *reporting*, setelah melalui tahap analisis dari bukti digital yang diperoleh, kemudian dilakukan *reporting* dari hasil analisis tersebut yaitu terdiri dari gambaran kegiatan yang telah dilakukan pada proses penyelidikan, penjelasan tentang *tools* yang digunakan pada proses penyelidikan, metode penyelidikan yang telah digunakan, penentuan dari tindakan pendukung penyelidikan yang telah

dilakukan, serta memberikan beberapa rekomendasi sebagai bahan untuk evaluasi elemen pendukung yang terdapat pada tindakan penyelidikan forensik digital (Riadi, Umar, et al., 2018)(Faiz, Umar, & Yudhana, 2017).

### 3.2. Simulasi Penyadapan Percakapan LINE Messenger

Penelitian ini menggunakan simulasi proses penyadapan percakapan pada aplikasi LINE messenger korban. Penelitian ini menjelaskan tentang skema pengujian aplikasi LINE messenger berbasis web sebagai media dalam pencarian keberadaan barang bukti digital pasca proses penyadapan terhadap smartphone korban, sehingga dapat diketahui barang bukti yang diperoleh dari aplikasi LINE berbasis web. Proses penyadapan aplikasi LINE messenger dapat dilihat pada Gambar 2 :



Gambar 2. Flowchart Penyadapan LINE Messenger

Berdasarkan Gambar 2 dilakukan tahapan penyadapan aplikasi LINE messenger pada smartphone korban menggunakan media LINE messenger berbasis web. Tahapan penyadapan ini dimulai dengan mempersiapkan peralatan yang akan digunakan dalam proses penyadapan kemudian dilakukan penyadapan dengan terlebih dahulu melakukan login ke aplikasi LINE messenger berbasis web melalui scan QR code menggunakan smartphone korban. Hasil dari penyadapan pada aplikasi LINE messenger korban merupakan data-data bukti digital yang didapat pada aplikasi LINE messenger berbasis web. Bukti digital tersebut dikumpulkan kemudian diperiksa dan dianalisis menggunakan tools forensik, pada tahap akhir dilakukan pelaporan terhadap hasil pemeriksaan dan analisis bukti digital.

## 4. HASIL DAN PEMBAHASAN

Hasil analisis forensik pada penelitian ini didapat dengan menggunakan metode dan tools untuk membantu peneliti dalam mencari data yang dibutuhkan pada proses investigasi forensik. Penelitian ini diawali dengan membuat akun media LINE messenger untuk proses simulasi percakapan LINE messenger, selanjutnya pada proses penelitian ini dilakukan pemilihan tools untuk mengambil data pada akun LINE messenger tersebut. FTK Imager dipilih sebagai tools yang digunakan pada penelitian ini. Tahap selanjutnya dikumpulkan bukti digital dengan dilakukan eksplorasi di direktori laptop untuk menemukan SQLite LINE messenger database pada browser Google Chrome, dari proses eksplorasi ditemukan lokasi database SQLite Google Chrome pada C:\Users\Adm\AppData\Local\Google\Chrome\User\Data\Defaul. Folder default yang merupakan lokasi SQLite

LINE messenger database di dalamnya terdapat database tentang semua aktivitas google chrome berupa file dan folder seperti cache dan log. Temuan dari investigasi web browser terkait LINE messenger berbasis web dapat dilihat pada Tabel 1 :

**Table 1. Hasil Eksplorasi Pada Laptop**

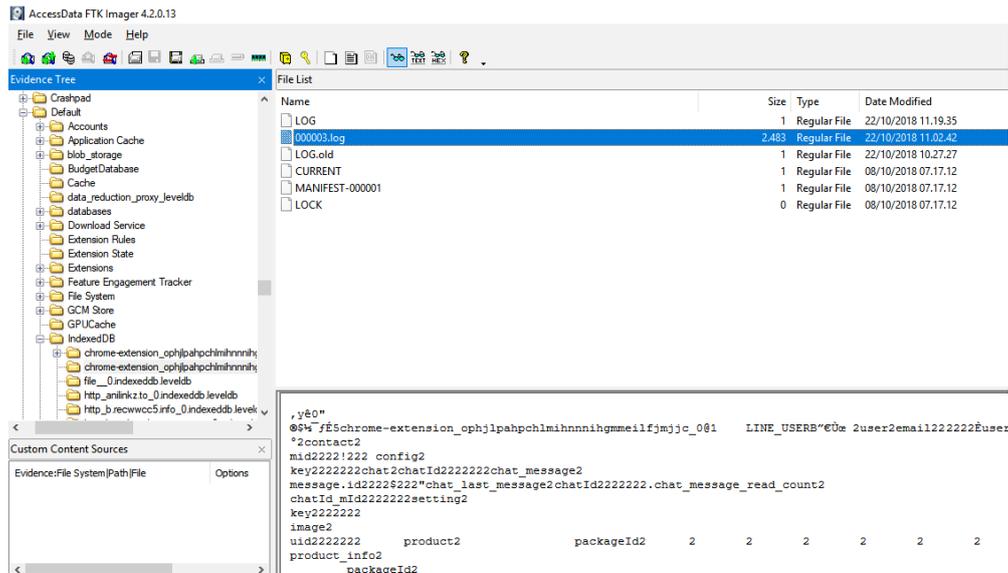
File Type	Storage Location	File Name
Log File	C:\Users\Adm\AppData\Local\Google\Chrome\User\Data\Default\IndexedDB	000003.log
Cache	C:\Users\Adm\AppData\Local\Google\Chrome\User\Data\Default\Cache	f_0572be
Db SQLite	C:\Users\Adm\AppData\Local\Google\Chrome\User\Data\Default\IndexedDB	bc

## 5. Analisis

Tahap analisis pada penelitian ini dilakukan dengan menganalisa bukti digital yang didapat memanfaatkan *tools* dan literatur pendukung untuk dapat mencapai tujuan dari penelitian. Standar pengujian pada penelitian ini memanfaatkan *tools* forensik digital yang sudah banyak digunakan dan tersedia secara gratis, yaitu FTK Imager.

### 5.1. Analisis Lokasi File Log

Penelitian ini merupakan proses analisis terkait lokasi artefak aplikasi LINE messenger menggunakan *tools* FTK Imager. Berdasarkan data penelitian pada Tabel 1 dapat diketahui lokasi file log aplikasi LINE messenger. File log aplikasi LINE messenger dapat dilihat menggunakan *tools* FTK Imager seperti pada Gambar 3.

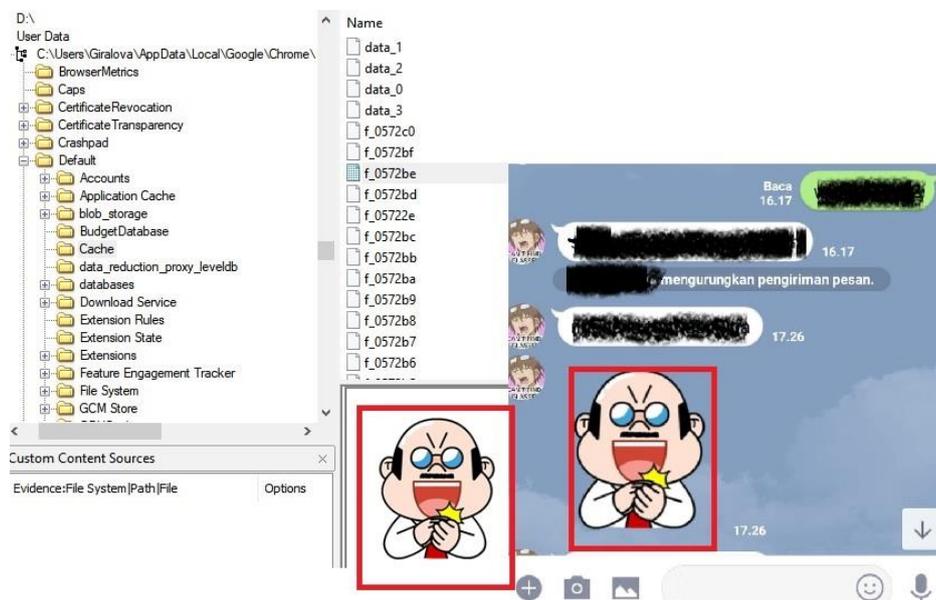


Gambar 3. File Log Aplikasi LINE Messenger

Berdasarkan Gambar 3 dapat diketahui bahwa lokasi log file terdapat pada sub folder IndexedDB yaitu pada folder chrome-extension di dalam folder tersebut selain file log aplikasi LINE messenger juga terdapat beberapa file lainnya. Pada file log tersebut terdapat kata "LINE\_USER" hal ini membuktikan bahwa file log tersebut merupakan file log aplikasi LINE messenger.

## 5.2. Analisis File Cache

Penelitian ini merupakan analisis terkait validitas file cache aplikasi LINE messenger yang di temukan pada proses eksplorasi menggunakan bantuan tools FTK Imager. Berdasarkan hasil eksplorasi pada Tabel 1 diketahui lokasi file cache aplikasi LINE messenger, lokasi file cache aplikasi LINE messenger dapat dilihat menggunakan tools FTK Imager seperti pada Gambar 4.

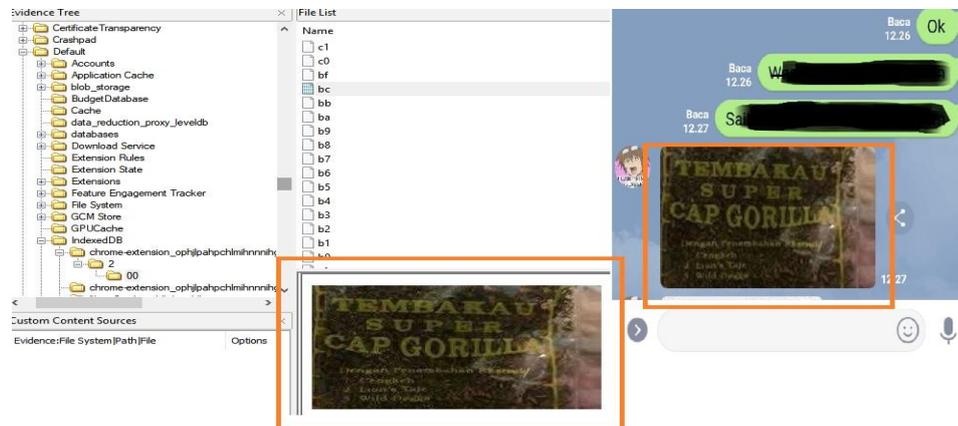


Gambar 4. Uji Validitas File Cache

Berdasarkan Gambar 4 dapat diketahui bahwa lokasi file cache Aplikasi LINE messenger terdapat pada folder Cache, pada folder tersebut terdapat file cache dari keseluruhan aktivitas google chrome. File cache tersebut memperlihatkan gambar stiker LINE messenger yang sama dengan chat pada aplikasi LINE messenger di smartphone hal ini membuktikan bahwa file cache tersebut merupakan asli file cache aplikasi LINE messenger.

### 5.3. Analisis Bukti Digital

Analisis pada file bukti digital yang didapat setelah proses eksplorasi dilakukan dengan menggunakan bantuan *tools* FTK Imager. Berdasarkan hasil eksplorasi pada Tabel 1 diketahui lokasi file bukti digital LINE messenger, lokasi file bukti digital tersebut dapat dilihat menggunakan *tools* FTK Imager seperti pada Gambar 5.



Gambar 5. Bukti Digital Pada Chat LINE Messenger

Berdasarkan temuan bukti digital pada Gambar 5, kemudian dilakukan penelitian dengan menghapus chat aplikasi LINE messenger berisi bukti digital pada *smartphone*, setelah chat tersebut dihapus dilakukan pengecekan ulang pada file bukti digital dan hasilnya file bukti digital tersebut masih utuh hal ini membuktikan bahwa file bukti digital tersebut tidak akan hilang walaupun chat pada aplikasi LINE messenger telah dihapus. Hasil dari penelitian ini diharapkan diperoleh bukti digital yang dapat digunakan untuk membantu proses persidangan.

## 6. KESIMPULAN

LINE messenger merupakan salah satu aplikasi pesan singkat yang banyak digunakan di negara-negara Asia, secara khusus LINE messenger banyak digunakan oleh pengguna yang lebih menyukai tampilan menarik dan fitur emoji yang memberikan banyak pilihan dalam mengekspresikan maksud dari sebuah percakapan. Penelitian ini menggunakan metode NIJ, metode tersebut memiliki beberapa tahapan yaitu tahap Preparation, tahap Collection, tahap Examination, tahap Analysis dan tahap Reporting. Penelitian ini menggunakan media aplikasi LINE messenger berbasis web yang disinkronkan dengan LINE messenger berbasis android. Penelitian ini dalam prosesnya berhasil diperoleh lokasi file log, cache, dan bukti digital dari simulasi tindak kejahatan yang didapatkan melalui proses penyadapan aplikasi LINE messenger berbasis android milik korban. Bukti digital yang didapat dari proses eksplorasi direktori laptop menggunakan *tools* FTK Imager tidak hilang walaupun chat pada aplikasi LINE messenger korban dan pelaku telah dihapus. Bukti digital forensik yang didapat diharapkan dapat memperkuat bukti kasus kejahatan di pengadilan dalam bentuk hasil analisis bukti digital.

## DAFTAR PUSTAKA

- Anwar, N., & Riadi, I. (2017). Analisis Investigasi Forensik WhatsApp Messenger Smartphone Terhadap WhatsApp Berbasis Web. *Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika*, 3(1), 1–10. <https://doi.org/10.26555/jiteki.v3i1.6643>
- Artyom Dogtiev. (2018). Line Revenue and Usage Statistics (2017) - Business of Apps. Retrieved October 8, 2018, from <http://www.businessofapps.com/data/line-statistics/>
- Capstone. (2018). Top 10 cybercrime facts you need to know in 2018 - Rochester, Buffalo, West Palm Beach | Capstone IT. Retrieved October 9, 2018, from <https://www.capstoneitinc.com/2018/04/top-10-cybercrime-facts-need-know-2018/>

- 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>
- 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>
- 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>
- Ikhsani, S., & Hidayanto, C. (2016). Analisa Forensik Whatsapp dan LINE Messenger Menyediakan Barang Bukti yang Kuat dan Valid di Indonesia. *Jurnal Teknik ITS*, 5(2), 728–736.
- LINE. (2015). LINE Extension for Google Chrome Released | LINE Corporation | News. Retrieved October 9, 2018, from <https://linecorp.com/en/pr/news/en/2015/1044>
- 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.
- 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.
- 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>
- 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.
- 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>
- Yang, T. Y., Dehghantaha, A., Choo, K. K. R., & Muda, Z. (2016). Windows Instant Messaging App Forensics: Facebook and Skype as Case Studies. *PloS One*, 11(3), e0150300. <https://doi.org/10.1371/journal.pone.0150300>
- Yusoff, M. N., Dehghantaha, A., & Mahmud, 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>