Pendahuluan

Kemajuan teknologi di zaman sekarang ponsel berbasis *Android* sudah tidak lagi susah didapatkan. Tidak hanya kalangan atas yang hanya bisa mendapatkan ponsel Android, melainkan kalangan bawah juga sudah bisa mendapatkan ponsel *Android* dengan harga terjangkau, sehingga tidak banyak orang yang masih buta akan teknologi *Android* ini. Salah satu kelebihan ponsel *Android* ini adalah dapat menggunakan aplikasi *Instant Messenger*.

Salah satu aplikasi *Instant Messenger* yang sedang banyak dipakai kalangan anak muda sekarang adalah *LINE Messenger*. Salah satu kelebihan dari *LINE Messenger* mempunyai *sticker-sticker* yang unik dan menarik, berbeda dengan aplikasi *Instant Messenger* lainnya yang hanya mempunyai *emoticon* yang biasa saja. Kelebihan yang lainnya yaitu *LINE* menyediakan *block list* sehingga dapat *block user id* atau nomer ponsel untuk tidak masuk dalam kontak *LINE* [1].

Dengan semua kegiatan *chatting*, pengiriman *sticker*, kontak, dan lain lain pada *LINE Messenger* akan tercatat semua pada ponsel *Android* sehingga dapat dimanfaatkan sebagai bukti penting pengadilan apabila ada perbuatan atau pemakaian yang melewati batas aturan hukum. Seperti *broadcast* berita *HOAX*, membuat g*roup* yang terselubung, dan pelanggaran lainnya yang bersangkutan dengan penggunaan *LINE Messenger*. Contoh kasus yang terkadang sering terjadi sekarang yaitu *chatting* yang merusak citra orang lain atau merusak nama baik seseorang yang dapat dikasuskan ke pengadilan dengan bukti sebuah ponsel *Android* yang didalamnya dapat diambil *database* dari aplikasi *LINE* tersebut untuk dianalisis keaslian dari kronologis yang terjadi pada korban. Sehingga tersangka yang melakukan kejahatan tersebut dapat dijatuhkan hukuman sesuai perundang – undangan yang berlaku di Indonesia, yaitu Undang-Undang ITE.

Penggunaan *tools forensic* yang ada pada internet memudahkan para pengguna dapat menganalisis data yang terdapat pada ponsel *Android* yang akan dianalisis. Maka salah satu kelebihan *LINE forensic* adalah mendapatkan aplikasi secara gratis, dan mendapatkan hak akses penuh dalam setiap *fiture*. Aplikasi *LINE forensic* yang saya gunakan adalah *DB Browser for SQLite* yang fungsinya untuk membaca isi database secara mendetail salah satunya dapat mengetahui kronologi pembicaraan yang dilakukan oleh pengguna[2].

Salah satu kelebihan aplikasi *DB Browser for SQLite* adalah mendapatkan hak akses penuh dalam fiturnya, selain itu *DB Browser for SQLite* menggunakan operasi read/write tanpa adanya perantara proses server tersendiri. Maka dari itu untuk menganalisa data yang terdapat pada *LINE Messenger* secara detail dalam jurnal ini menggunakan Aplikasi ini dapat memungkinkan membantu kinerja dari para ahli forensik dalam mencari kronologi pembicaraan yang tersimpan pada aplikasi *LINE Messenger*, selain itu bahkan orang awam dapat menggunakan aplikasi forensik ini dengan tujuan yang positif[3].

Tinjauan Pustaka

Penelitian pertama berjudul "*Forensic Analysis of Instant Messenger Aplication on Android Devices*"[4], merupakan analisis forensik *Android* dengan aplikasi *WhatsApp* dan *Viber*, menghasilkan suatu bukti kejahatan yang terjadi di *Whatsapp IM (Instan Messaging)* dan *Viber*. Penelitian tersebut di analisa menggunakan *DB Sqlite browser*, dari penelitian tersebut pesan yang terhapus dapat dikembalikan, data yang bisa dilakukan *recovery* adalah percakapan, *video, file, voice call, image*, dan lain lain tetapi jika ponsel telah dilakukan *factory reset* data yang tersimpan di ponsel telah hilang dan tidak bisa dilakukan *recovery*.

Penelitian yang kedua berjudul "Analisis dan Implementasi *Mobile* Forensik Pemulihan Data yang hilang pada Smartphone berbasis Sistem Operasi *Android*"[5]. Dari hasil penelitian dari jurnal tersebut telah melakukan pemulihan data *SMS* dan data *CDR* yang telah terhapus dapat kembali ke memori *smartphone*, dan dari hasil tersebut didapatkan bahwa data yang berhasil dipulihkan meskipun ponsel telah dilakukan *factory reset* masih dapat dipulihkan akan tetapi data yang telah dilakukan *flash ROM* tidak dapat dipulihkan karena *flash ROM* mengubah *ROM* lama menjadi *ROM* baru dan dari hasil uji memori penyimpanan data *SMS* tidak ada batas jumlah penyimpanan, semakin besar memori penyimpanan pada *smartphone* semakin besar pula data *SMS* yang dapat disimpan, sedangkan pada data C*all log* mempunyai limit data hanya dapat menyimpan 500 data *Call log*.

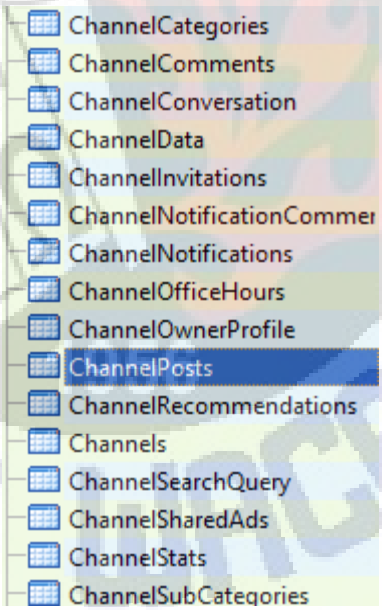
Penelitian yang ketiga berjudul "Recovering BlackBerry Messenger Forensic Artifacts"[6]. Merupakan analisa forensik dari BBM (BlackBerry), untuk melihat data yang sudah terhapus agar bisa diliat dan dianalisa, adapun tempat penyimpanan database yang terdapat di Android yang bisa di akses adalah "/data/data/com.bbm/files/bbmcore/master.db", dan sedangkan pada iOS kita dapat menemukannya didirektori yang berbeda dengan di Android /private/var/mobile/Applications/%GUID%/Library/bbmcore/master.db".

Pada *database* yang telah ditemukan tersebut maka didapatkan hasil dari isi pesan dan lainnya, BBM untuk iOS dan Android juga baru saja diperbaharui untuk menyertakan *channel* pada perangkat BBM, *channel* tersebut bisa jadi tempat untuk melakukan tindakan kriminal maka dijurnal ini bisa melihat isi dari *channel* tersebut, dari hasil analisa tersebut akan dijelaskan di gambar berikut ini.

RecNo	TextMessageId	Ordinal	PacketId	ConversationId	ParticipantId	Type	IsInbound	State	Timestamp	Content
Click here to define a filter										
1	1	1	0	1	1	0	0	5	1393253197	Hey I have some information that might be of value to you
2	2	2	0	1	2	0	1	5	1393253226	What kind of information and how much will it cost me?
3	3	3	0	1	1	0	0	5	1393253285	Good stuff, usual rate
4	4	4	0	1	1	0	0	5	1393253333	A list of contacts and some internal docs
5	5	5	0	1	2	0	1	5	1393253373	Sounds good how do you want to get them to me?
6	6	6	0	1	1	0	0	5	1393253404	Not email, it's monitored
7	7	7	0	1	1	0	0	5	1393253466	I'll put them in a dropbox account we can use
8	8	8	0	1	2	0	1	5	1393253493	OK let me know when and where
9	9	9	0	1	1	0	0	5	1393253903	https://www.dropbox.com/sh/8ho2rl237rlkz9i/gsUnfWxHqL
10	10	10	0	1	2	0	1	5	1393254059	Thanks got them
11	11	11	0	1	2	0	1	5	1393254073	I send payment the usual way

Gambar 1. Hasil dari analisa BBM forensik

Dari hasil gambar 1 adalah contoh informasi rinci yang bisa ditampilkan antara lain adalah pesan, waktu, pesan terkirim, pesan diterima, status, dan *pin*.



Gambar 2. Hasil dari tampilan informasi *channel* dari BBM

Metode Penelitian

Pada metode mengenai analisis forensik *LINE IM (Instant Messaging)* dan proses dari sebuah analisa *database* yang berada di *LINE IM (Instant Messaging). NIST: National Institute of Standards and Technology* menyatakan semua alat dan perangkat yang digunakan untuk pengujian harus tercantum, seiring dengan hal tersebut yang pertama adalah memberikan rincian tentang metodologi yang digunakan dalam penelitian adalah sebagai berikut[7] :

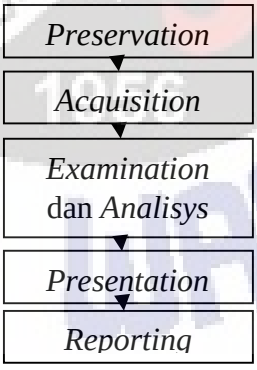
A. Tools yang digunakan
   1. Ponsel *Android* sebagai barang bukti.
   2. *SQLITE DB browser.*
   3. Windows 7.

B. Skenario

Dalam penelitian ini skenario tindakan yang dilakukan adalah menganalisa *LINE IM (Instant Messaging)* agar mendapatkan informasi sebanyak – banyaknya dari *database* yang terdapat dari barang bukti yang berupa ponsel yang didalamnya menggunakan aplikasi *LINE IM (Instant Messaging).*

C. Tahapan Penelitian

Adapun tahapan yang dilakukan dalam penelitian ini mengacu pada pedoman dari *NIST: National Institute of Standards and Technology* yang terdiri dari 6 (enam) tahapan, yaitu: (1) *Preservation* (2) *Acquisition*, (3) *Examination* dan *Analisys*, (4) *Presentation*, dan (5) *Reporting*.



Gambar 1. Tahapan Penelitian

Gambar 1 adalah Tahapan penelitian meliputi :

(1) *Preservation*

Proses pengumpulan bukti dari sebuah kejahatan yang terjadi *LINE IM (Instan Messaging)*, yang akan digunakan sebagai perumusan masalah serta tujuan dari penelitian ini. Pada proses ini, barang bukti dijaga agar tidak terjadi perubahan data.

(2) *Acquisition*

Proses *Acquisition* adalah mengumpulkan dan mendapatkan bukti yang mendukung penyelidikan. Pada tahapan ini merupakan tahapan yang sangat menentukankarena buktu yang didapatkan akan sangat mendukung penyelidikan untuk membuktikan bawah seseorang telah melakukan tindak kejahatan, media digitaldatpat dijadikan sebagai barang bukti, seperti media penyimpanan (*falshdisk, pen drive, hardisk dan CD- Room*). Selanjutnya *install* aplikasi pada ponsel *Android Root explorer* aplikasi tersebut fungsinya untuk membuka *file* pada ponsel yang tidak bisa dilihat menggunakan *explorer* bawaan yang dimiliki *Android* karena jika pada explorer bawaan tidak bisa membuka file database yang dimiliki *LINE Messenger*[8].

(3) *Examination* and *Analisys*

Proses ini merupakan pembuktian barang bukti tersebut benar adanya yang memiliki adalah orang yang telah melakukan kejahatan pada *LINE IM (Instant Messaging)*. Menganalisa sebuah kasus yang pesannya mengandung kejahatan dengan menggunakan aplikasi *DB Browser for SQLite* kita membuka *database* yang sudah melakukan tahap *cloning* dibuka untuk dianalisa[9].

(4) *Presentation*

Membuat *timeline* untuk mengurutkan kronologi pesan yang isinya mengandung sebuah kejahatan.

(5) *Reporting*

Penulisan laporan dari hasil penelitian yang dilakukan mengenai proses forensik *LINE IM (Instant Messaging)*. Pada tahap ini membahas hasil dari analisis yang telah dilakukan.

Preservation

Preservation merupakan tahap paling awal dalam metode *mobile forensic*, dan hal pertama yang dilakukan adalah melakukan pencarian, pengumpulan, dan dokumentasi barang bukti. Pada penelitian yang mendjadi barang bukti yaitu sebuah *smartphone* yang diskenariokan sebagai barang bukti dalam kasus kejahatan[10].

Setelah barang bukti dikumpulkan kemudian dilakukan dokumentasi dengan mencatat merek, model, spefikasi serta hal lain yang berkaitan dengan smartphone tersebut, berikut merupakan hasil dokumentasi serta spesifikasi barang bukti:

Gambar 2. Barang bukti

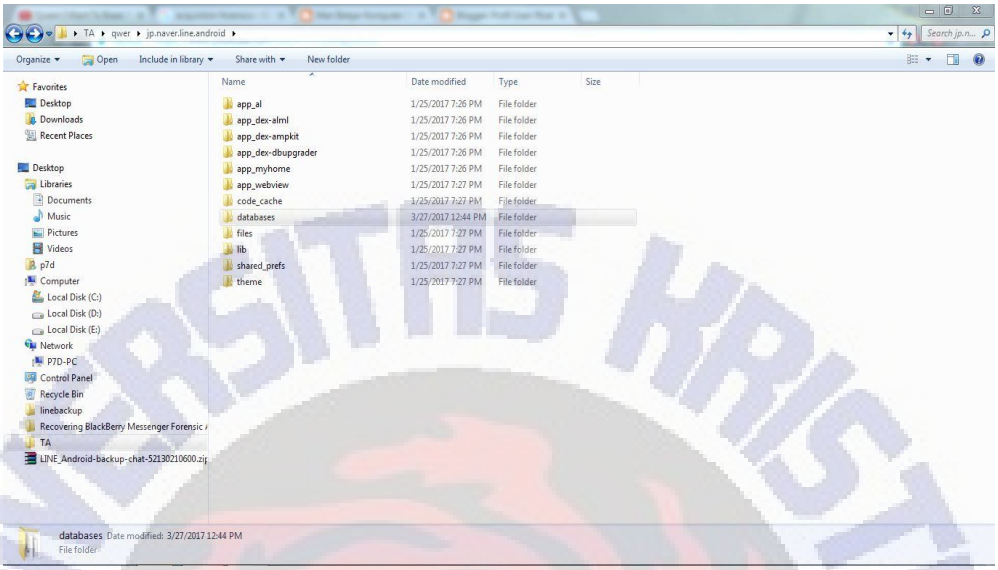
Spesifikasi	Barang bukti
Merek	Lenovo
Model	A536
Os	Android OS, v4.4.2 (KitKat)

Tabel I. spesifikasi

Pada gambar 2 dan tabel I di atas adalah salah satu barang bukti yang akan dianalisa dari tabel di atas, padatahap ini juga dilakukan persiapan yang nantinya akan dianalisis serta tools yang digunakan.

Acquisition

Pada tahap ini adalah melakukan menduplikat *database* yang awalnya berada di dalam *folder* ponsel yang lokasinya berada *"/data/data/jp.naver.line.android/"*. duplikassinya yang awalnya berada didalam ponsel kita, menduplikasi ke komputer lalu melakukan tahapan *cloning data* secara langsung melalui kabel data.



Gambar 3. Tahap setelah melakukan duplikasi dari ponsel

Pada gambar 3 adalah tahap setelah melakukan duplikasi dari ponsel setelah itu *data/file* di atas dilakukan *cloning data* menggunakan secara langsung melalui kabel data,hasil di atas adalah hasil setelah dilakukan *cloning data*..

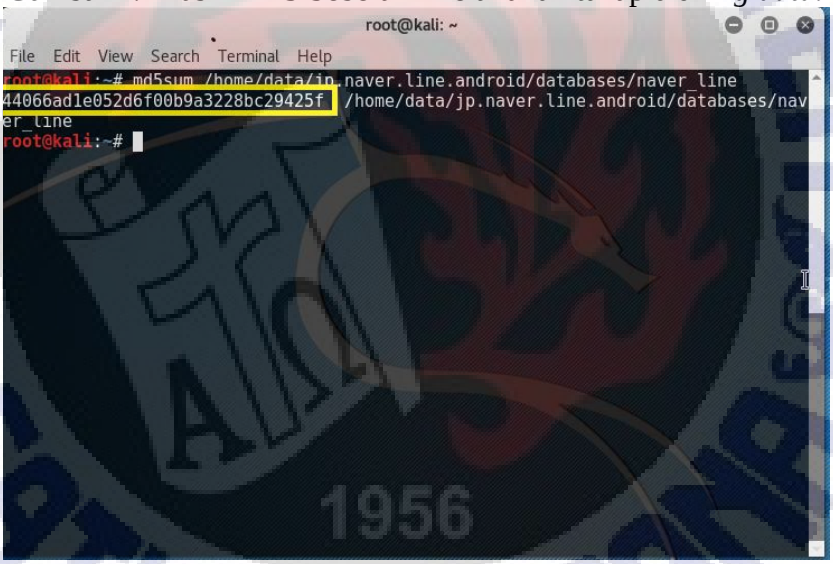
Hasil dan Pembahasasan

Examination and Analisys

Examination

Setelah melakukan tahap *Acquisition*, maka selanjutnya adalah melakukan tahap *Examination and Analisys*, yaitu mengungkap dan melakukan analisis terhadap hasil dari tahap *Acquisition* untuk memperoleh data yang berkitan dengan aplikasi *LINE Messenger*. Adapun *tools* yang digunakan untuk memperoleh data yang berkaitan dengan *LINE Messenger* yaitu *DB Browser for SQLite*, pada tahap ini adalah pembuktian bahawa barang bukti yang sudah diduplikat membuktikan bahwa MD5 otentik sama terhadap barang bukti yang sebelum melakukan duplikasi, Gambar di bawah ini adalah gambar sebelum melakukan *cloning data*, yang dapat dilihat dari *root explorer*.

Gambar 4. Hasil MD5 Sebelum melakukan tahap *cloning data.*



Gambar 5. Hasil sesudah *dilakkukan cloning data.*

Dari gambar diatas hasil dari sebelum melakukan cloning data dan sesudah melakukan cloning data hasilnya adalah ontentik adanya dan sama. 44066ad1e052d6f00b9a3228bc29425f, hasil dari gambar di atas mengunakan command "md5sum /home/data/jp.naver.line.android/database/naver_line".

Analysis

Pada bagian ini adalah proses dari sebuah analisis yang terjadi pada *LINE IM (Instant Messaging), folder LINE* yang menyimpan *database chat* terdapat pada *"/data/data/jp.naver.line.android/*". Untuk membuka *folder* tersebut harus dengan menggunakan aplikasi *Root Explorer* dan melakukan *rooting* pada ponsel yang akan dianalisis, di dalam *folder "/data/data/jp.naver.line.android/"* didapatkan hasil analisa struktur dan isi *folder* serta *database*, berikut merupakan data-data yang penting untuk mendukung investigasi dan pengungkapan kasus kejahatan,yaitu:

Tabel II Stuktur

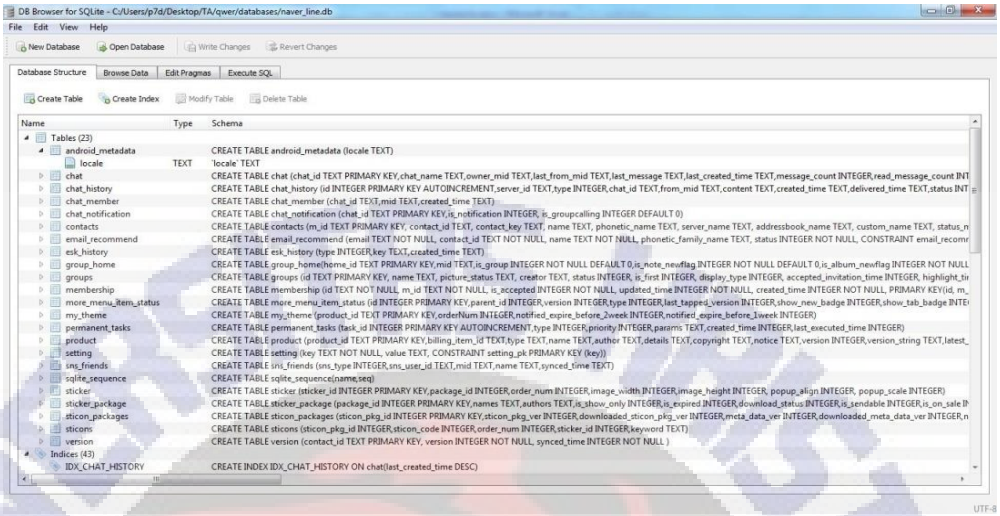
"/data/data/jp.naver.line.android/".

Database	Deskripsi
Database/	Direktori ini terdapat *file database* yang dapat dilakukan analisa menggunakan aplikasi *SQLITE DB browser.*
Naver_line.db	*File* ini berisi *database chat history* yang akan dibahas pada bab ini.
naver_line_private_chat.db	*File* ini berisi pesan pribadi dan *hidden message* dari *fiture* yang ada di program *LINE Messenger.*

Naver_line.db berisi tentang informasi yang berkaitan dengan pesan yang telah dikirim atau diterima oleh sang pengguna ponsel, yang isi strukturnya akan dijelaskan di table III:

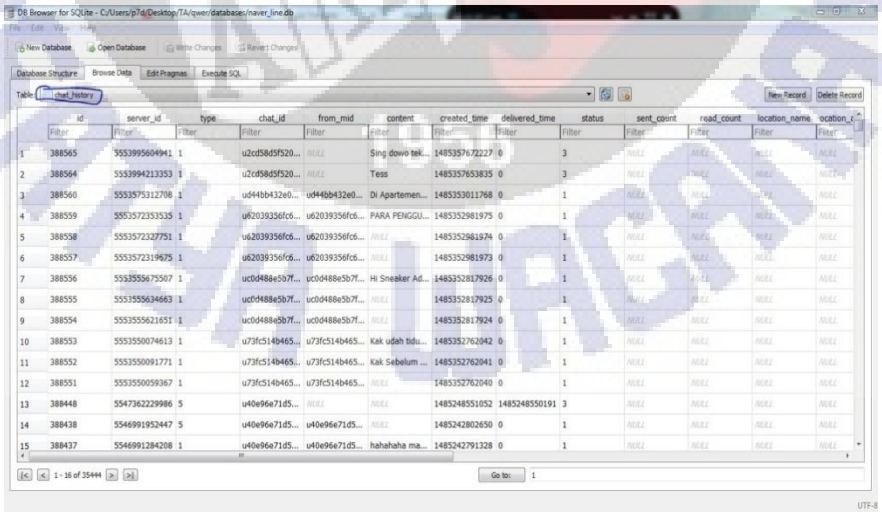
Tabel III Struktur
"/DATA/DATA/JP.NAVER.LINE.ANDROID/DATABASES/NAVER_LINE.DB"

Tabel	Kolom	Informasi
Contacts	*M_id*	Kode unik id dari kontak.
	Name	Nama kontak .
	Server_name	Identitas nama yang menjadi unik kode dari awal pertama pembuataan kontak.
Chat/Chat_history	*Chat_id*	*Chat* yang memiliki kode unik dari setiap sesi.
	Form_mid	Sama seperti m_id yang menunjukkan nama pengirim pesan.
	Content	Isi dari pesan.
	Created_time and delivered_time	Pembuatan pesan dan waktu kirim pesan (terenkripsi).
	Location_name, *Location_adreess,* *Location_latitude,* *Locarion_lingitude*	Beberapa tipe lokasi yang tersimpan di ponsel untuk di indentifikasi tetapi biasanya *null(0)* karena pengguna yang menggunakan *LINE Messenger* jarang mengaktifan lokasi di ponsel.
Groups	*Id*	Kode unik dari grup yang telah dibuat.
	Name	Nama grup.
	Creator	Id dari pembuat grup.
	Created_time, update_time	Waktu membuat pesan dan waktu pembaharuan terakhir dari pesan.



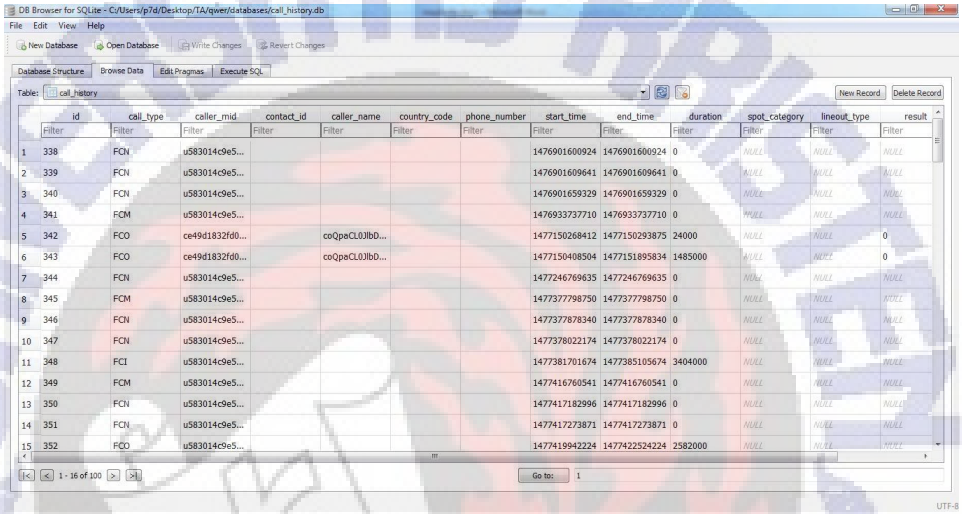
Gambar 6. Tampilan struktur *database* melalui *DB Browser for SQLite*

Tabel dan gambar 6 di atas adalah susunan struktur dari isi *database naver_line.db*,sebelum melakukan analisis yang harus dilakukan adalah mengganti extensi dari file *naver_line* menjadi *naver_line.db,* yang paling penting adalah tabel *chat* yang isinya adalah *chat_history* semua pesan yang sudah terhapus atau semua pesan yang belum terhapus tersimpan "*Chat_history",* berbeda dengan tabel "*Chat*" di tabel *chat* yang isinya hanya menyimpan pesan yang belum terhapus di ponsel, adapun beberapa tahap untuk melakukan analisa *database* menggunakan *DB Browser for SQLite* dibawah ini adalah hasil dari analisa yang dibuka melalui *DB Browser for SQLite.*

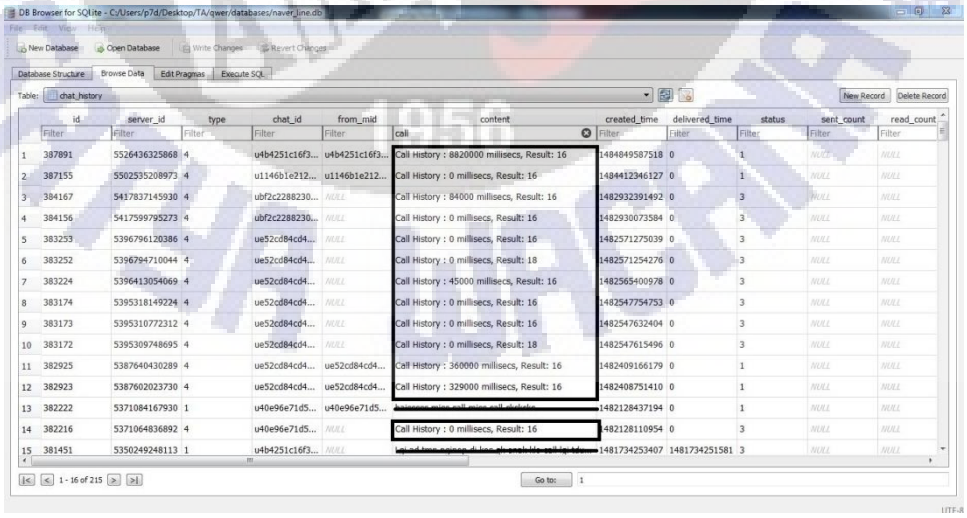


Gambar 7. Tampilan tabel "*chat_history"*

Gambar 7 adalah tampilan tabel *chat_history* dimana pesan dari *LINE Messenger* yang sudah terhapus dari ponsel tersimpan di dalam tabel tersebut, tabel tersebut tidak bisa menyimpan percakapan yang isinya panggilan, gambar, dan *voicenote* hanya bisa memberitahukan jika adanya durasi panggilan bisa di lihat di gambar dibawah ini.



Gambar 8. Tampilan *database call_hisory*

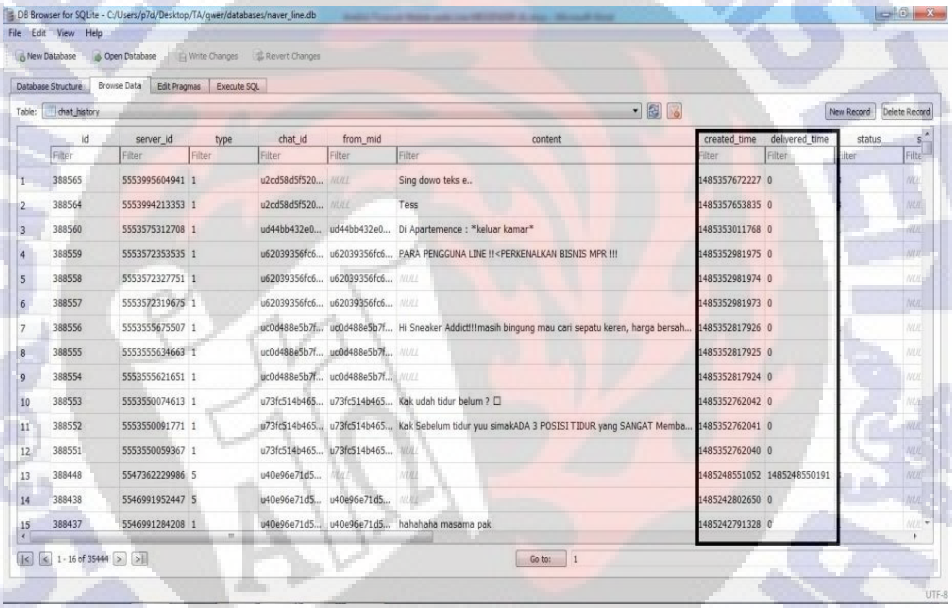


Gambar 8. Tampilan *call_history*

Gambar 7 dan gambar 8 adalah tampilan *call_history* yang menjelaskan bahwa tabel *chat_history* tidak bisa merekam panggilan pada kolom *start_time* dan *end_time* durasinya telah dienkripsi dijadikan *timestamp*, hanya dapat mendeteksi berapa lama akun tersebut melakukan panggilan, yang merupakan kelemahan *LINE Messenger*.

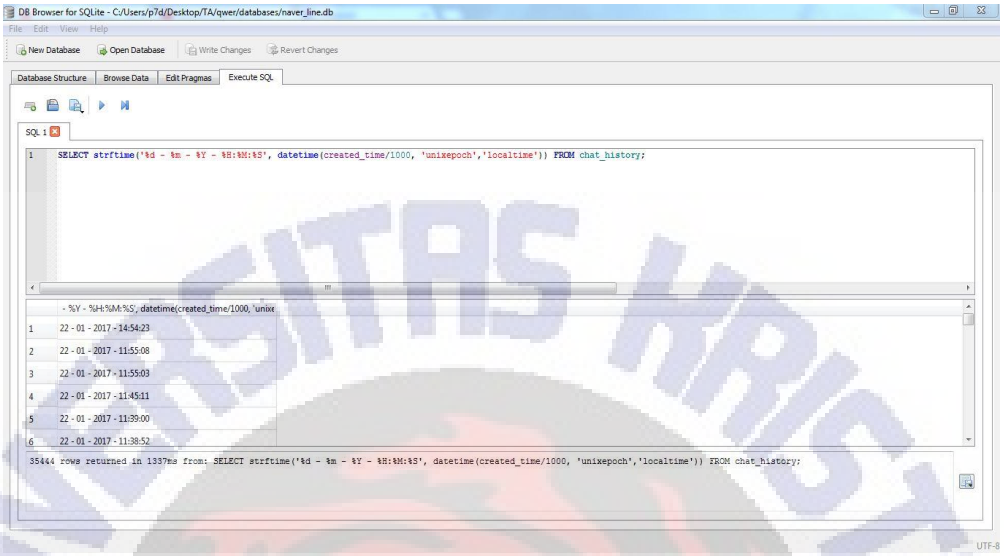
Presentation

Pada database *LINE Messenger* waktu pengiriman pesan atau penerima pesan telah dienkripsi dan harus melakukkan dekripsi secara manual, pada *database created_time* dienkripsi dari *timestamps* menjadi *time string* (*strftime*) dan waktu yang telah ditampilkan *database* disusun secara acak maka yang harus dilakukan adalah dengan *coding* tampilan waktu akan yang dienkripsi bisa lihat gambar dibawah ini :



Gambar 9. tampilan *created_time* dan *delivered_time*

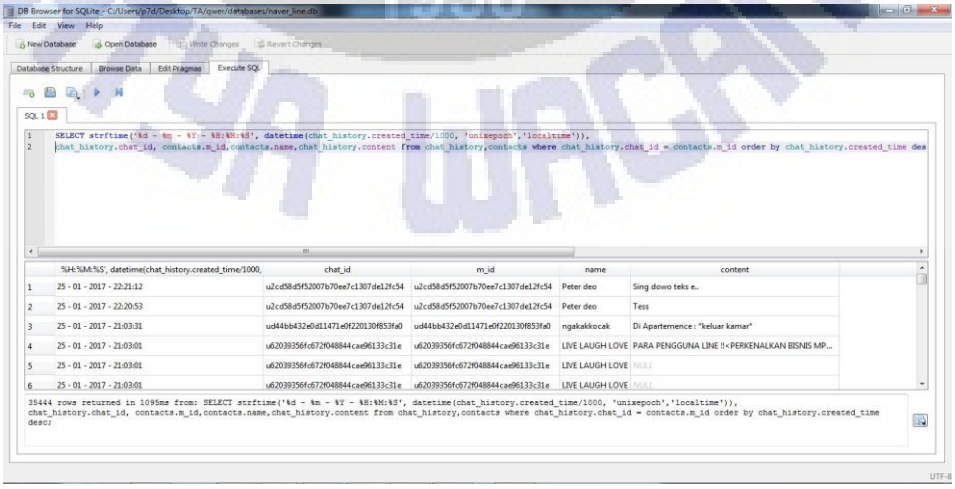
Pada gambar 9 telah membuktikan bahwa *created_time* telah terenkripsi dan yang harus kita lakukan adalah mendekripsi dan membuat tampilan secara teratur sesuai tanggal, dan jika ada *delivered_time* = 0 itu karena *LINE Messenger* langsung melakukan pengiriman langsung kepada penerimanya tanpa terjadi *pending*, pada gambar dibawah ini akan melakukan tahap dekripsi pada *created_time*.



Gambar 10. Dekripsi *created_time*

Pada gambar 10 di atas telah dilakukan dekripsi dari *timestamps* menjadi time string, untuk melakukan proses tersebut kita harus memasukkan *codding Sql* untuk *convert timestamps*. *Codding* dari gambar di atas adalah "*SELECT strftime('%d - %m - %Y - %H:%M:%S', datetime(created_time/1000, 'unixepoch','localtime')) FROM chat_history;*" penjelasannya adalah *convert timestams* ke format *time string* %d = tanggal %m = bulan %y tahun %h = jam %M = menit %s = detik, kemudian *datetime (created_time*/1000 karena mengikuti zona waktu local dari tabel *chat_history*.

Pada tahap *Presentation* yang harus kita lakukan adalah mengurutkan hasil analisa dari tabel *chat_history* menjadi urutan isi pesan, kontak, dan kapan waktu membuat pesan dan waktu pembaharuan terakhir dari pesan akan dijelaskan pada gambar dibawah ini.

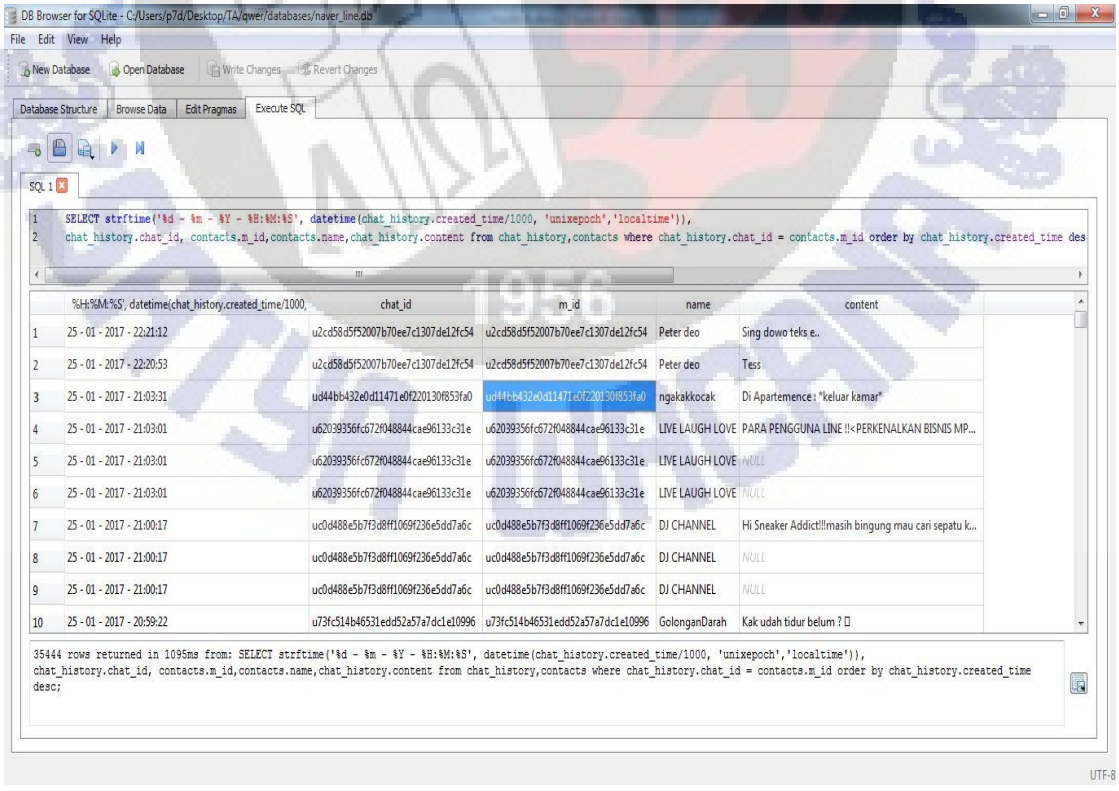


Gambar 11. Hasil dari pengurutan pesan

Dari gambar 11 adalah hasil dari pengurutan pesan yang menggunakan kode manual untuk pengurutan tersebut kode di atas adalah "*SELECT strftime('%d - %m - %Y%H:%M:%S',datetime(chat_history.created_time/1000,unixepoch','localtime')), chat_history.chat_id,contacts.m_id,contacts.name,chat_history.content from chat_history contacts where chat_history.chat_id = contacts.m_id order by chat_history.created_time desc;"* penjelasannya adalah gabungan antara *code convert timestamp* dengan relasi tabel yang berada didalam *NAVER_LINE.DB*, artinya adalah *convert timestams* ke format *time string* %d = tanggal %m = bulan %y tahun %h = jam %M = menit %s = detik, kemudian *datetime (created_time*/1000 karena mengikuti zona waktu lokal dari tabel *chat_history*, mengambil kolom *chat_id*, mengambil *m_id*, mengambil nama, mengambil *contents* dari tabel *chat_history* kontak dimana hubungan antara relasi tabel *chat_history*. *Chat_id* dengan kontak *m_id*, dan *desc* adalah mengurutkan dari yang terbaru sampai yang terlama.

Reporting

Pada tahap terakhir pada metode *mobile forensic* melakukan *reporting* atau pelaporan. Pada tahap ini akan membahas dan menyajikan secara detail hasil yang bisa didapatkan dari hasil analisa di atas, yang akan dijelaskan pada gambar dibawah ini.



Gambar 12. Hasil dari analisa *mobile forensic*

Pada gambar 12 adalah hasil dari analisa *mobile forensic chat* yang bisa didapatkan oleh analisa di atas yang didapatkan adalah waktu, *chat_id, m_id*, nama kontak, dan *content* atau isi dari pesan yang telah diurutkan dari kapan waktu membuat pesan terbaru sampai yang terlama, gambar diatas dapat dipastikan jika analisa dari *Line Messenger* adalah content dari isi pesan yang telah terhapus.

Kesimpulan

Berdasarkan tahapan yang telah dibahas mengenai analisis *Mobile Forensic* pada *Line Messenger* pada *platform Android*, dimana aplikasi *instant messaging* berkembang cepat dan didapatkan secara gratis dengan penggunaan yang tidak bisa dikontrol satu persatu akunnya, dapat digunakan sebagai tindak kejahatan kasus kejahatan seperti membully, penipuan, perjudian, pornografi, korupsi, ataupun jaringan narkoba yang telah terjadi sebelumnya maka didapat disimpulkan sebagai berikut :

1. Bukti digital pada aplikasi *Line Messenger* berhasil didapatkan dari perangkat *Android* dengan menggunakan aplikasi tambahan *DB Sqlite browser*.
2. Data yang dapat diambil atau dijadikan barang bukti merupakan data yang penting yang berisikan *database* yang didalamnya berupa panggilan, pesan, gambar dan lain - lain.
3. Faktor yang mempengaruhi hasil untuk mendapatkan bukti digital pada aplikasi *Line Messenger* adalah aktifitas atau kondisi aplikasi perangkat yang digunakan oleh pemilik dari ponsel.
4. Adapun kekurangan dari tempat penyimpanan selain dari pesan dan panggilan selain dari dua tersebut analis di atas tidak bisa menemukan adanya gambar, voicenote, file, panggilan, yang didapat hanyalah notifikasi atau pemberitahuan bahwa adanya durasi panggilan,adaanya gambar, voicenote, file, dan kekurangan lainnya adalah jika ponsel telah dilakukan *factory reset* tidak dapat dilakukan analisa, kekurangan lainnya adalah jika ponsel tidak dilakukan rooting terlebih dahulu maka ponsel tidak bisa menemukan folder database yang akan dianalisa.

Daftar Pustaka

[1] Iqbal, A., Alobaidli, H., Almarzooqi, A., Jones, A., 2015. "*LINE IM app Forensic Analysis*". 12th International Conference on High-capacity Optical Networks and Enabling/Emerging Technologies (HONET-ICT 2015).

[2] Prasanthi, B,V., 2016 "*Cyber forensic Tools*". India. International Journal of Engineering Trends and Technology (IJETT).

[3] http://script-13.blogspot.co.id/2014/12/macam-macam-teknologi-pengolahan.html yang diakses pada tanggal 21 Januari 2017

[4] Mahajan, A., Dahiya, M, S., Sanghvi, H,P., 2013."*Forensic Analysis of Instant Messenger Aplication on Android Devices*" International Journal of Computer Applications.

[5]A, Thufail, A., N, Michrandi, S., Irawan, B., 2012. "*Analisis Dan Implementasi Mobile Forensik Pemulihan Data Yang Hilang Pada Smartphone Berbasis Sistem Operasi Android*". Fakultas Teknik, Universitas Telkom.

[6] http://www.forensicfocus.com/Forums/viewtopic/t=13688/. Diakses pada 25 Januari 2017.

[7] Ayers, R., Brothers, S., Jansen W. 2014. "*Guidelines on Mobile Device Forensics*". NIST Special Publication 800-101 Revision 1. Available.

[8] Ramadhan, Z., Asrizal. 2015. "*Digital Forensik dan Penanganan Pasca Insiden"*.

[9] Hopen,J., Thomas., 2015. "The Forensic Examination and Analysis of Paper Matches". Atlanta. ATF Forensic Science Laboratory.

[10] John, L., Jeremy. 2012. "*Digital Forensics and preservation"*. Association with Charles Beagrie Ltd. DPC Technology.