

Analisa Forensik Whatsapp dan LINE Messenger pada Smartphone Android sebagai Rujukan dalam Menyediakan Barang Bukti yang Kuat dan Valid di Indonesia

Syukur Ikhsani dan Bekti Cahyo Hidayanto

Jurusan Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember (ITS)

Jl. Raya ITS, Surabaya 60111 Indonesia

e-mail: bekticahyo@is.its.ac.id

Abstrak—Aplikasi pengolah pesan yang populer di Indonesia adalah WhatsApp dan LINE Messenger. Peningkatan penggunaan aplikasi tersebut berbanding lurus dengan peningkatan tingkat kejahatan yang menggunakan aplikasi pengolah pesan itu. Tidak jarang, aplikasi pengolah pesan digunakan untuk bertukar informasi yang ilegal ataupun tindakan pemerasan. Hal ini membutuhkan penanganan khusus dan peran forensika digital untuk menyelesaikan kasus yang ada. Penelitian ini menggunakan skenario percakapan dan eksperimen modifikasi terhadap kondisi aplikasi, diantaranya penggunaan normal, penghapusan percakapan dan aplikasi. Data setiap eksperimen akan diambil dengan menggunakan metode yang menyesuaikan dengan kondisi perangkat. Data yang berhasil diambil akan dianalisa menggunakan FTK Imager dan SQLite Browser untuk mencari data-data yang penting terkait pengungkapan kasus. Setelah data penting berhasil diketahui, maka dilakukan analisa lanjutan untuk membuktikan data tersebut dapat dipakai dalam pengungkapan sebuah kasus. Setelah data dapat dibuktikan maka dilanjutkan dengan analisa perbandingan data digital terkait eksperimen, perangkat, dan aplikasi pengolah pesan. Langkah terakhir adalah melakukan analisa keamanan dari setiap aplikasi untuk memberikan rekomendasi terkait aplikasi pengolah pesan yang terbaik pada bidang forensika digital. Didapatkan kesimpulan bahwa bukti data digital telah berhasil didapat dengan menggunakan dua metode, yaitu secara manual dan menggunakan aplikasi tambahan. Data yang berhasil didapatkan adalah data utama seperti data kontak dan percakapan serta data pendukung seperti media dan database cadangan. Faktor yang mempengaruhi keberhasilan mendapatkan bukti digital adalah aktivitas modifikasi pada kondisi aplikasi dan perangkat yang digunakan. Dan pada akhirnya WhatsApp merupakan aplikasi yang menjadi rujukan dalam forensika digital sedangkan LINE Messenger merupakan aplikasi yang lebih aman karena lebih sulit untuk dilakukan analisa forensika digital.

Kata Kunci—Forensika Digital, LINE Messenger, Mobile Forensics, WhatsApp

I. PENDAHULUAN

PERKEMBANGAN teknologi komunikasi dan informasi pada era ini semakin maju saja. Zaman dulu manusia saling terhubung dengan sandi dan isyarat. Seiring manusia mengenal baca tulis, maka budaya pesan surat pun mulai muncul.

Penemuan teknologi telepon seakan menjadi lonceng perkembangan teknologi komunikasi dan informasi menjadi semakin bergema. Ditemukannya jaringan internet dan teknologi komputer membuat semua menjadi nyata. Ya teknologi semakin menyeramkan perkembangannya. Sekarang era internet cepat dan perangkat telepon seluler menjadi sebuah tren teknologi masa kini

Tak susah menemukan pembuktiannya. Cobalah tengok apa yang digenggam orang-orang saat berjalan. Dan cobalah perhatikan aktivitas mereka sepanjang hari. Semua terkoneksi dengan internet melalui telepon selulernya. Mau sekedar multimedia seperti melihat video atau bermain games hingga melakukan pekerjaan dan membaca laporan perusahaan bisa digunakan melalui telepon seluler pintar mereka. Hanya butuh koneksi internet, semua bisa dilakukan.

Tak terkecuali aktivitas berbalas pesan, baik itu dilakukan secara pribadi semacam komunikasi dua arah, maupun berbalas pesan dalam jumlah *user* yang besar seperti keluarga, teman, atau kerabat dalam sebuah obrolan grup. Dulu komunikasi pribadi menggunakan ponsel hanya bisa melalui layanan *short messaging service* (SMS) yang terbatas hanya komunikasi dua arah dan 160 karakter. Namun saat ini sudah mulai meluas dengan adanya ponsel pintar yang menyediakan berbagai aplikasi pengolah pesan yang mutakhir dengan beragam fitur dan layanan.

Dua aplikasi pengolah pesan yang terkenal dan paling banyak digunakan di Indonesia adalah LINE Messenger dan WhatsApp. Berdasarkan survei GobaWebIndex, sejak 2014 WhatsApp menempati posisi teratas dengan angka 54 persen dari total angka keseluruhan pengguna aplikasi pengolah pesan dan diperkirakan terus meningkat. [1] Sedangkan LINE Messenger memiliki pengguna di Indonesia sebanyak 30 juta dan menjadikan Indonesia sebagai peringkat kedua pengguna terbesar LINE Messenger di dunia, hanya kalah dibandingkan Jepang yang mencapai 52 juta pengguna [2]. Dua aplikasi ini digunakan oleh masyarakat Indonesia dari berbagai lapisan. Secara khusus LINE Messenger digunakan oleh pengguna yang menyukai tampilan lebih menarik dan fitur emoji yang banyak memberikan pilihan dalam mengekspresikan maksud dari sebuah pembicaraan. Untuk WhatsApp digunakan oleh orang-orang yang lebih simpel dengan emoji yang sederhana

sehingga biasanya cocok untuk para pekerja profesional dan akademisi.

Di tengah peningkatan penggunaan teknologi dan pengolahan pesan, hadir ke permukaan beberapa kasus kejahatan yang melibatkan teknologi sebagai barang bukti dalam pengadilan, baik sebagai alat utama maupun pendukung dari kejahatan. Seperti kasus korupsi RC, seorang pejabat sekaligus politisi, yang melibatkan bukti percakapan melalui aplikasi WhatsApp [3] maupun kasus prostitusi *online* menggunakan aplikasi pengolahan pesan [4]. Kedua kasus ini akhirnya membutuhkan penanganan yang khusus karena kita tak hanya berpendapat melalui bukti *screenshot* saja yang mungkin bisa dimanipulasi, namun data lengkap tentang bukti digital seperti waktu percakapan dan kontak yang dituju.

Kepolisian dan Pemerintah sudah bereaksi dengan membuat badan-badan khusus untuk menangani kasus-kasus yang melibatkan teknologi informasi. Polri membuat divisi *Cyber Crime* untuk menyelidiki dan menyidik tindak pidana khusus, terutama kegiatan penyidikan yang berhubungan dengan teknologi informasi, telekomunikasi, serta transaksi elektronik. Sedangkan pemerintah melalui Kementerian Komunikasi dan Informasi membuat sebuah lembaga bernama *Indonesia Security Incident Response Team on Internet and Infrastructure/Coordination Center (Id-SIRTII/CC)* untuk membantu dalam penanganan kejahatan yang terjadi pada teknologi informasi.

Kehadiran mereka diimbangi dengan kehadiran para akademisi untuk memberikan daya dukung terhadap pengungkapan kasus-kasus kejahatan yang sejalan dengan bidang digital forensik. Namun sayangnya topik semacam forensika digital ini masih cukup sulit ditemukan di Indonesia, khususnya hal-hal yang terkait dengan forensik sosial media dan pengolahan pesan. Padahal sudah banyaknya penelitian di negara lain terkait topik seperti ini seperti yang sudah dilakukan oleh Noora Al Mutawa dan rekan dari *Zayed University*, Dubai untuk melakukan analisis forensik pada aplikasi jejaring sosial di perangkat bergerak. Ada juga penelitian oleh Neha S, Thakur dari *University of New Orleans*, Amerika Serikat dan juga Cosimo Anglano dari *Universita del Piemonte Orientale*, Italia yang membahas tentang analisis forensik dari WhatsApp. Dari penelusuran literatur yang ada, penulis juga menemukan bahwa belum adanya penelitian terkait forensika di bidang *LINE Messenger*. Padahal aplikasi ini seperti yang sudah diketahui sebelumnya cukup digandrungi oleh pengguna usia muda di Indonesia.

Penulis melihat bahwa kebutuhan akan penelitian terkait analisa forensika di bidang aplikasi pengolahan pesan, khususnya WhatsApp dan *LINE Messenger* yang terbaru harus segera dilaksanakan. Diharapkan dengan adanya penelitian ini, dapat memberikan sumbangan pengetahuan bagi kalangan penegak hukum dan akademisi untuk membantu penyelesaian masalah di bidang forensik di bidang aplikasi perangkat bergerak, khususnya di bidang pengolahan pesan populer di Indonesia karena mempertimbangkan budaya dan popularitas penggunaan aplikasi di Indonesia. Selain itu untuk para programmer yang tertarik pada bidang pengembangan aplikasi untuk forensik dapat terbantuan dengan penelitian ini.

II. URAIAN PENELITIAN

Berdasarkan pada diagram alur metodologi pada gambar 1, berikut merupakan penjelasan dari setiap prosesnya

A. Studi Literatur

Tahapan ini merupakan awal dari penelitian tugas akhir. Pada tahapan ini, penulis menggali dan menganalisa informasi terkait penelitian yang diambil, khususnya mengenai perangkat lunak serta model pengujian yang sesuai untuk studi kasus. Selain itu, penulis harus memahami dan memastikan bahwa setiap perangkat dan konsep yang ingin diajukan dalam penelitian ini sudah memenuhi kebutuhan dan dukungan terhadap luaran yang diharapkan.

B. Pembuatan Skenario dan Eksperimen

Pembuatan skenario dan eksperimen berguna untuk mendapatkan barang bukti sebagai langkah menuju tahap analisa. Penelitian ini menggunakan kondisi yang biasanya terjadi di kehidupan sehari-hari dalam melakukan kejahatan atau transaksi yang dicurigai. Hasil pengujian akan berimplikasi pada penelusuran dan pengembangan barang bukti. Skenario dan eksperimen yang akan dijalankan pada penelitian ini yaitu skenario percakapan dan eksperimen penggunaan aplikasi. Berikut merupakan deskripsi dari skenario yang akan dijalankan pada penelitian kali ini:

1) Skenario Percakapan

Skenario percakapan dibuat dengan mengambil sebuah kasus yang mungkin akrab dengan kejahatan dan memerlukan forensika telepon seluler. Oleh karena itu, skenario yang mungkin adalah pemerasan dan pornografi dimana kedua macam kejahatan tersebut biasanya memerlukan kehadiran ahli forensik dalam menganalisa pembuktian terhadap kejahatan.

2) Eksperimen Penggunaan Aplikasi

1. *Eksperimen 1*: Aplikasi dijalankan dengan biasa.
2. *Eksperimen 2*: Aplikasi dijalankan dengan biasa dengan penghapusan *file*/percakapan melalui layanan aplikasi
3. *Eksperimen 3*: Aplikasi dijalankan dengan dengan biasa dengan dihapus/di-*uninstall* melalui aplikasi telepon seluler.

C. Pengujian Skenario dan Eksperimen

Pada tahapan ini penulis akan menguji skenario dan eksperimen untuk mendapatkan data digital. Lama pengujian skenario tidak dibatasi. Hal ini dilakukan agar mempermudah dalam pengambilan dan menganalisa data digital yang akan dilakukan pada proses selanjutnya.

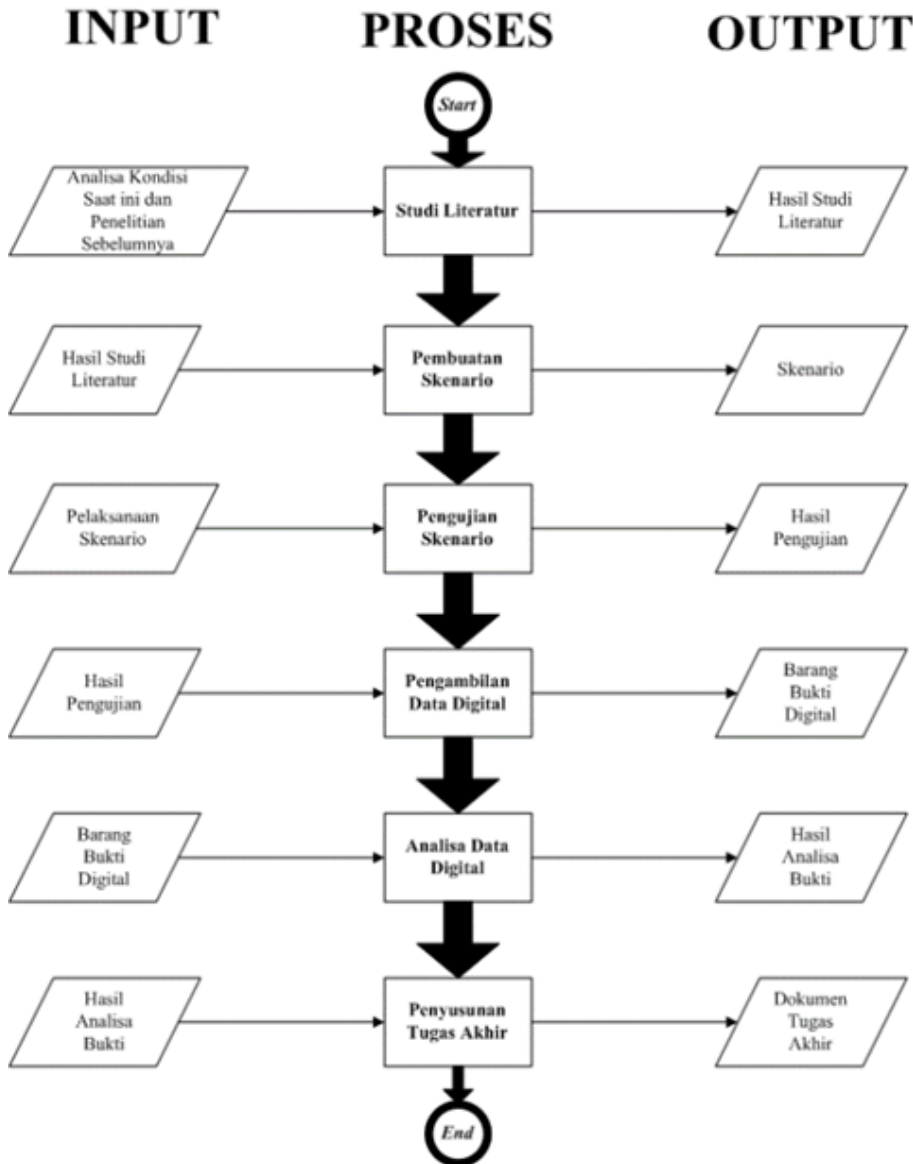
Eksperimen akan dijalankan sesuai dengan kondisi yang ada pada lingkungan yang sebenarnya sehingga bukti digital yang ada diharapkan sudah sepenuhnya sesuai dengan kondisi yang nyata yang terjadi pada sehari-hari. Metode dalam menguji eksperimen adalah dengan menggunakan telepon seluler dan emulator yang telah dipasang di laptop penulis.

D. Pengambilan Data Digital

Pada tahap ini kita akan mengambil data digital yang telah diujikan melalui skenario dan eksperimen yang telah ditentukan sebelumnya. Pengambilan data digital disini menggunakan dua macam aplikasi, yaitu aplikasi penggandaan data dan aplikasi untuk mengembalikan data yang terhapus. Jika diperlukan,

maka penggunaan perangkat forensik akan digunakan pada penelitian dengan kerjasama dengan pihak eksternal Jurusan

Sistem Informasi ITS yang memiliki perangkat tersebut.



Gambar 1 Metodologi penelitian

E. Analisa Data Digital

Setelah data berhasil didapatkan, maka akan dianalisa menggunakan aplikasi dan literatur pendukung untuk mencapai tujuan dari penelitian. Sebagai pengujian standar, maka penulis menggunakan aplikasi forensika digital yang sudah banyak digunakan dan tersedia secara gratis, yaitu *Forensic Tool Kit (FTK) Imager* dan *SQLite Browser*.

Hasil analisa yang diharapkan ada 4 macam, yaitu struktur penyimpanan data, macam-macam data yang didapatkan, faktor yang mempengaruhi ketersediaan barang bukti/data digital, dan tingkat keamanan dari kedua aplikasi pengolah pesan tersebut.

Struktur penyimpanan data akan memperlihatkan bagaimana tingkat kompleksitas dan penjelasan terhadap data yang dapat dianalisa oleh para investigator. Seperti yang ada di penelitian sebelumnya, WhatsApp memiliki direktori pada media, *file*, dan *database* [5]. Contoh struktur penyimpanan data adalah sebagai berikut:

Tabel 1
Contoh struktur data

Konten	Direktori	File
Database Kontak	/data/data/com.whatsapp/databases	Wa.db (SQLite v.3)
Database obrolan	/data/data/com.whatsapp/databases	Msgstore.db (SQLite v.3)
Foto profil	/data/data/com.whatsapp/files/Avatars	UID.j, dimana UID adalah identifikator dari sebuah kontak

Setelah struktur penyimpanan data, maka kita akan menganalisa data yang terdapat pada konten tersebut. Untuk konten kontak misalnya, ada beberapa data yang bisa diambil dan dianalisa seperti yang tertera pada tabel berikut:

Tabel 2
Contoh jenis data

Nama Lokasi	Pengertian
-id	Nomor rekaman

Jid	ID	Kontak	WhatsApp	(contoh)
				<code>x@s.WhatsApp.net</code> , maka x adalah nomor telepon dari kontak tersebut
<code>is_whatsapp_user</code>				Jika memiliki nomor 1, artinya berhubungan dengan pengguna sebenarnya, jika 0 berarti tidak

Faktor yang mempengaruhi ketersediaan barang bukti akan dilihat dari perbedaan hasil eksperimen yang dilakukan untuk setiap aplikasi dengan mempertimbangkan dua analisa sebelumnya, yaitu struktur penyimpanan data dan jenis data yang didapatkan. Setiap eksperimen akan dibandingkan dan dianalisa untuk memenuhi tujuan penelitian.

Tingkat keamanan akan mempertimbangkan kelengkapan struktur dan analisa data yang didapatkan pada skenario dan eksperimen dari kedua aplikasi pengolah pesan. Semakin lengkap data yang dapat dianalisa maka dianggap menjadi aplikasi dengan rujukan terbaik bagi para penegak hukum untuk digunakan oleh masyarakat. Semakin sedikit data yang dapat dianalisa maka dianggap menjadi aplikasi dengan tingkat keamanan terbaik bagi pengguna.

III. HASIL DAN DISKUSI

A. Ketersediaan Data Digital

1) Hasil Data Eksperimen 1

Eksperimen pertama merupakan aktivitas penggunaan aplikasi dengan kondisi normal, tanpa ada modifikasi penggunaan maupun penanganan terhadap aplikasi. Oleh karena itu, penulis mendapatkan semua *file* dengan lengkap, khususnya pada pengambilan data digital melalui metode aplikasi tambahan.

2) Hasil Data Eksperimen 2

Eksperimen kedua merupakan aktivitas penggunaan aplikasi dengan modifikasi terhadap isi aplikasi, yaitu penghapusan percakapan yang melibatkan skenario percakapan. Penghapusan percakapan memberikan efek kepada *database* aplikasi sehingga jumlah data yang dapat diambil tidak jauh berbeda dengan eksperimen pertama, namun dengan isi yang berbeda.

3) Hasil Data Eksperimen 3

Eksperimen ketiga merupakan aktivitas penggunaan aplikasi dengan modifikasi terhadap penanganan aplikasi, yaitu penghapusan aplikasi dari perangkat. *File* yang terdapat pada *folder* data akan terhapus secara otomatis karena proses pelepasan aplikasi sehingga hanya menyisakan *file* yang ada pada *storage* (bukan *folder* data yang harus dilakukan proses *rooting* dahulu).

B. Analisa Data Digital

1) Lokasi Data pada Perangkat

a) Lokasi Folder WhatsApp:

Folder WhatsApp memiliki dua lokasi yang berbeda dan nama yang berbeda, yaitu *folder* “com.whatsapp” dan “WhatsApp”. Lokasi *folder* “com.whatsapp” berada di *folder* data dengan gambaran direktori sebagai berikut:

`data → data → com.whatsapp`

Selain *folder* “com.whatsapp”, *folder* lain yang bernama WhatsApp terletak di media penyimpanan (luar). Dalam penelitian ini, penulis menggunakan penggunaan yang standar sehingga *folder* “WhatsApp” berada pada media penyimpanan internal. Jika dimodifikasi, bisa saja *folder* “WhatsApp” ini berada di media penyimpanan eksternal (kartu memori).

b) Lokasi LINE Messenger:

Folder LINE Messenger memiliki dua lokasi yang berbeda dan nama berbeda, yaitu *folder* “jp.naver.line.android” dan “LINE_Backup”. Lokasi *folder* “jp.naver.line.android” berada di *folder* data dengan gambaran direktori sebagai berikut:

`data → data → jp.naver.line.android`

Selain *folder* “jp.naver.line.android”, LINE Messenger juga memiliki *folder* “LINE_Backup”. *Folder* “LINE_Backup” memiliki karakteristik khusus karena dibuat jika ada proses backup pada aplikasi LINE Messenger. *Folder* ini dapat dimodifikasi atau dipindahkan menuju media penyimpanan eksternal (kartu memori).

2) Struktur Folder dan File Aplikasi

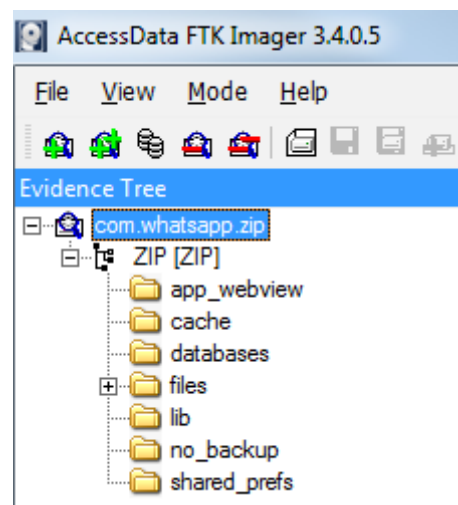
Bagian ini merupakan analisa terkait struktur *folder* dan *file* aplikasi menggunakan bantuan aplikasi FTK Imager.

a) Struktur Folder dan File WhatsApp

Berikut merupakan struktur *folder* untuk masing-masing *folder* dari WhatsApp:

1. Folder com.whatsapp

Struktur data *folder* “com.whatsapp” adalah sebagai berikut:

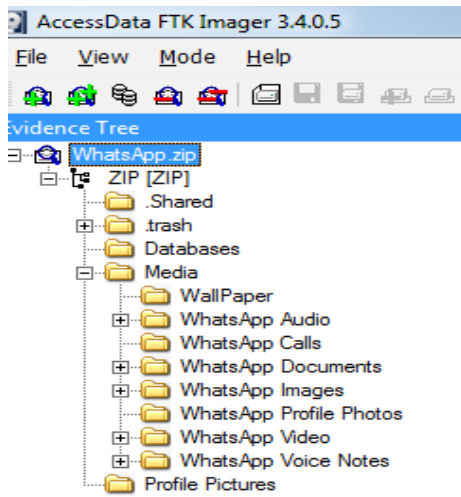


Gambar 2 Struktur *folder* com.whatsapp

Secara umum, ada enam *folder* utama dan tiga sub*folder* dalam *folder* com.whatsapp. Namun ada beberapa perangkat dan eksperimen yang memiliki satu *folder* tambahan, yaitu *app_webview*.

2. Folder WhatsApp

Struktur data *folder* “WhatsApp” adalah sebagai berikut:



Gambar 3 Struktur folder WhatsApp

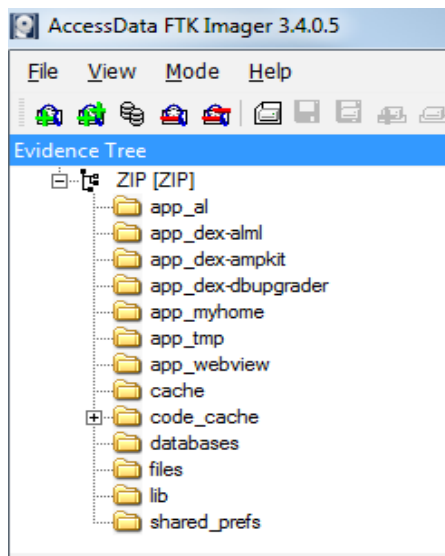
Didalam folder “WhatsApp” terdapat 5 folder utama, dengan 9 sub-folder.

b) Struktur Folder dan File LINE Messenger

Berikut merupakan struktur folder untuk masing-masing folder dari LINE Messenger:

1. Folder jp.naver.line.android

Struktur data folder “jp.naver.line.android” adalah sebagai berikut:



Gambar 4 Struktur folder jp.naver.line.android

Secara umum, ada 13 folder yang dimiliki oleh folder jp.nave.line.android. Namun ada beberapa penyesuaian bergantung pada kondisi perangkat dan penggunaan aplikasi LINE Messenger sendiri.

2. Folder LINE_Backup

Folder LINE_Backup memiliki karakteristik khusus, karena dibuat karena adanya proses pencadangan dari percakapan aplikasi. Jumlah file juga bergantung pada jumlah percakapan yang dicadangkan.

Analisa Database Aplikasi

Dari hasil analisa struktur folder dan file aplikasi, didapatkan beberapa file yang menyerupai database dengan format SQLite. Oleh karena itu dibutuhkan pembuktian menggunakan SQLite Browser. Didapatkan bahwa hanya beberapa database yang berhasil didapatkan data di dalamnya dan penting untuk dianalisa lebih lanjut.

C. Analisa Bukti Digital

1) Kategorisasi Data Digital

Berdasarkan hasil analisa struktur dan isi folder serta database, berikut merupakan data-data yang penting untuk mendukung investigasi dan pengungkapan kasus kejahatan, yaitu:

Tabel 3
Data penting

WhatsApp	LINE Messenger
Wa.db	Naver_line
Msgstore.db	
Data Pendukung	

2) Pembacaan Database Aplikasi

a) WhatsApp

Untuk database wa.db, kami menggunakan tabel wa_contacts dimana tabel tersebut memberikan informasi mengenai kontak yang ada pada database WhatsApp. Berikut merupakan isi dan fungsi dari setiap kolom yang ada pada tabel wa_contacts.

Tabel 4
Tabel wa_contacts

Nama Kolom	Arti/Fungsi
_id	Nomor rekaman database
jid	WhatsApp ID
is_whatsapp_user	Menentukan pengguna WhatsApp atau tidak
status	Status kontak WhatsApp
status_timestamp	Aktivitas terakhir (kode unix epoch time)
number	Nomor telepon pengguna
raw_contact_id	Nomor kontak
display_name	Nama pada kontak
phone_type	Tipe telepon
phone_label	Label pada telepon
unseen_msg_count	Jumlah pesan yang belum dibaca
photo_ts	Foto kontak
Thumb_ts	Keterangan penggunaan avatar
photo_id_timestamp	Keterangan avatar telah disimpan (kode unix epoch time)
given_name	Nama dari pengguna
family_name	Nama keluarga dari pengguna
wa_name	Nama dari kontak dari profil
sort_name	Nama kontak yang digunakan pada aplikasi

Untuk database msgstore.db, kami menggunakan tabel chat_list dan messages. Tabel chat_list merupakan tabel yang menunjukkan isi dari daftar percakapan yang ada pada aplikasi WhatsApp. Berikut merupakan isi dan fungsi dari setiap kolom yang ada pada tabel chat_list:

Tabel 5
Tabel *chat_list*

Nama Kolom	Arti/Fungsi
<i>_id</i>	Nomor rekaman <i>database</i>
<i>key_remote_jid</i>	WhatsApp ID tujuan
<i>message_table_id</i>	ID pesan yang direkam
<i>subject</i>	Nama percakapan (grup)
<i>creation</i>	Waktu grup dibuat (kode <i>unix epoch time</i>)
<i>last_read_message_table_id</i>	ID tabel pesan terakhir
<i>last_read_receipt_sent_message_table_id</i>	ID tabel terakhir pesan dibaca
<i>archived</i>	Pesan yang diarsipkan
<i>sort_timestamp</i>	Waktu pengurutan (kode <i>unix epoch time</i>)
<i>mod_tag</i>	Tidak diketahui
<i>gen</i>	Tidak diketahui
<i>my_messages</i>	Inisiatif percakapan

Sedangkan tabel *messages* merupakan isi percakapan yang dilakukan oleh pengguna pada aplikasi WhatsApp tersebut. Berikut merupakan isi dan fungsi dari setiap kolom yang ada pada tabel *messages*:

Tabel 6
Tabel *messages*

Nama Kolom	Arti/Fungsi
<i>_id</i>	Nomor rekaman <i>database</i>
<i>key_remote_jid</i>	WhatsApp ID
<i>key_from_me</i>	Arah pesan
<i>key_id</i>	Nomor identitas pesan
<i>status</i>	Status pesan
<i>needs_push</i>	Penunjuk pesan <i>broadcast</i>
<i>data</i>	Konten pesan <i>text</i>
<i>timestamp</i>	Waktu pesan dikirim (kode <i>unix epoch time</i>)
<i>media_url</i>	URL <i>file</i> media yang dikirim
<i>media_mime_type</i>	Tipe MME dari <i>file</i> yang telah dikirim
<i>media_wa_type</i>	Tipe pesan
<i>media_size</i>	Ukuran media yang dikirim
<i>media_name</i>	Nama <i>file</i> yang dikirim
<i>media_caption</i>	Isi <i>caption</i> dari <i>file</i> yang dikirim
<i>media_hash</i>	Enkripsi data terkait media yang dikirim
<i>media_duration</i>	Durasi media yang dikirim
<i>origin</i>	Isi percakapan
<i>latitude</i>	Garis lintang lokasi pengirim
<i>longitude</i>	Garis bujur lokasi pengirim
<i>thumb_image</i>	Gambar tampilan
<i>remote_resource</i>	ID pengirim (untuk <i>group chat</i>)
<i>received_timestamp</i>	Waktu pesan sampai pada perangkat sendiri (kode <i>unix epoch time</i>)
<i>send_timestamp</i>	Waktu pengiriman
<i>receipt_server_timestamp</i>	Waktu pesan sampai pada <i>server</i> (kode <i>unix epoch time</i>)
<i>receipt_device_timestamp</i>	Waktu pesan sampai tujuan (kode <i>unix epoch time</i>)
<i>read_device_timestamp</i>	Waktu pesan dibaca (kode <i>unix epoch time</i>)
<i>played_device_timestamp</i>	Waktu media dimainkan (kode <i>unix epoch time</i>)
<i>raw_data</i>	Tampilan untuk gambar / video
<i>recipient_count</i>	Jumlah penerima (pada percakapan grup)
<i>participant_hash</i>	Kode peserta (grup)
<i>starred</i>	Kode bintang (percakapan yang ditandai)

b) LINE Messenger

Untuk mengetahui kontak yang ada pada aplikasi LINE Messenger maka kita membutuhkan tabel *contacts*. Berikut merupakan isi dan fungsi dari setiap kolom pada tabel *contacts*:

Tabel 7
Tabel *contacts*

Nama Kolom	Fungsi/Isi
<i>m_id</i>	ID pengguna LINE
<i>contact_id</i>	ID kontak pada perangkat
<i>contact_key</i>	Kunci kontak pada perangkat
<i>name</i>	Nama kontak pada aplikasi
<i>phonetic_name</i>	Tidak diketahui
<i>server_name</i>	Nama pada <i>server</i> aplikasi
<i>addressbook_name</i>	Nama pada kontak perangkat
<i>custom_name</i>	Tidak diketahui
<i>status_msg</i>	Status pada kontak
<i>is_unread_status_msg</i>	Status pesan yang belum dibaca
<i>picture_status</i>	Foto pada kontak
<i>picture_path</i>	Kode foto
<i>relation</i>	Hubungan antara <i>user</i> dengan kontak
<i>status</i>	Status akun pada kontak aplikasi
<i>is_first</i>	Tidak diketahui
<i>display_type</i>	Tidak diketahui
<i>capable_flags</i>	Penanda kontak
<i>contact_kind</i>	Jenis kontak
<i>contact_type</i>	Tipe kontak
<i>buddy_category</i>	Kategori akun/kontak
<i>buddy_icon_type</i>	Tipe <i>icon</i> kontak
<i>is_on_air</i>	Kontak yang sedang <i>Live/online</i>
<i>hidden</i>	Kontak yang disembunyikan
<i>favorite</i>	Kontak favorit
<i>added_time_to_friend</i>	Tidak diketahui
<i>updated_time</i>	Waktu pembaruan rekomendasi (kode <i>unix epoch time</i>)
<i>created_time</i>	Waktu pembuatan rekomendasi (kode <i>unix epoch time</i>)
<i>recommend_params</i>	Jalur akun yang direkomendasikan

Fungsi tabel *chat* adalah untuk memberikan daftar percakapan yang ada pada aplikasi. Berikut merupakan isi dan fungsi dari setiap kolom pada tabel *chat*:

Tabel 8
Tabel *chat*

Nama Kolom	Fungsi / Isi
<i>chat_id</i>	ID percakapan
<i>chat_name</i>	Nama percakapan
<i>owner_mid</i>	<i>User</i> pemilik percakapan
<i>last_from_mid</i>	ID <i>user</i> aktif terakhir
<i>last_message</i>	Isi Pesan terakhir
<i>last_created_time</i>	Waktu terakhir dibuat (kode <i>unix epoch time</i>)
<i>message_count</i>	Jumlah pesan
<i>read_message_count</i>	Jumlah pesan yang telah dibaca
<i>type</i>	Tipe percakapan
<i>is_notification</i>	Notifikasi
<i>skin_key</i>	Kunci <i>skin</i> (warna <i>background</i>)
<i>input_text</i>	Tidak diketahui
<i>hide_member</i>	Daftar anggota disembunyikan
<i>p_timer</i>	Tidak diketahui
<i>last_message_display_time</i>	Pesan terakhir dilihat (kode <i>unix epoch time</i>)
<i>mid_p</i>	Tidak diketahui

Nama Kolom	Fungsi / Isi
<i>is_archived</i>	Pesan sudah diarsipkan
<i>read_up</i>	ID <i>Server</i>

LINE Messenger terdapat tabel *chat_history*. Tabel ini berfungsi untuk memberikan isi percakapan dari semua obrolan yang dilakukan pada aplikasi. Berikut merupakan isi dan fungsi dari setiap kolom pada tabel *chat_history*:

Tabel 9
Tabel *chat_history*

Nama Kolom	Arti / Fungsi
<i>id</i>	Nomor rekaman pada <i>database</i> aplikasi
<i>server_id</i>	Nomor rekaman pada <i>server</i> aplikasi
<i>type</i>	Tipe pesan
<i>chat_id</i>	ID percakapan
<i>from_mid</i>	ID pengirim
<i>content</i>	Isi pesan
<i>created_time</i>	Waktu pesan dibuat (kode <i>unix epoch time</i>)
<i>delivered_time</i>	Waktu pesan sampai (kode <i>unix epoch time</i>)
<i>status</i>	Status pesan
<i>sent_count</i>	Jumlah penerima
<i>read_count</i>	Jumlah pembaca
<i>location_name</i>	Nama lokasi
<i>location_address</i>	Alamat lokasi
<i>location_phone</i>	Telepon lokasi
<i>location_latitude</i>	Derajat lintang lokasi
<i>location_longitude</i>	Derajat bujur lokasi
<i>attachement_image</i>	Jumlah gambar <i>attachment</i>
<i>attachement_image_height</i>	Tinggi gambar <i>attachment</i>
<i>attachement_image_width</i>	Lebar gambar <i>attachment</i>
<i>attachement_image_size</i>	Ukuran gambar <i>attachment</i>
<i>attachement_type</i>	Tipe <i>attachment</i>
<i>attachement_local_uri</i>	Lokasi <i>file</i>
<i>parameter</i>	Penggunaan kode tambahan
<i>chunks</i>	Tidak diketahui

3) Pembuktian Data Digital

a) Analisa Percakapan

Dalam analisa percakapan, pertama adalah melakukan pembuktian terbalik dengan menyamakan percakapan yang terjadi pada aplikasi dengan skenario percakapan yang telah dibuat sebelumnya. Hal ini dilakukan untuk kondisi bukti hanya berasal dari salah satu pihak saja (bukti dari tersangka atau korban).

Tabel 10
Perbandingan Skenario dan Aktivitas Percakapan

Aktivitas Percakapan	Skenario Percakapan	Kesimpulan
"Selamat siang Korban 1, salam kenal"	Selamat siang X, salam kenal	Sama dan terbukti
"Halo mas, salam kenal juga. Anda siapa ya? Ada perlu apa kalau boleh tahu?"	Halo mas, salam kenal juga. Anda siapa ya? Ada perlu apa kalau boleh tahu?	Sama dan terbukti

Dalam penelitian ini, penulis juga memiliki bukti dari kedua belah pihak. Oleh karena itu, kita juga dapat menganalisa

menggunakan dua *database*. Untuk WhastApp kita menggunakan kolom *key_id*. Berikut merupakan contoh analisa percakapan pada WhastApp:

Tabel 11
Perbandingan *key_id* pengguna

key_id Korban	key_id Tersangka	data	Kesimpulan
32E615DFDC E7419A92B9 FE8F46F0CF	32E615DFDC E7419A92B9 FE8F46F0CF "	"Gila kamu!"	Sama dan terbukti
"5FEC641578 6EFC EE4CF ABDFE0C003 F	"5FEC641578 6EFC EE4CF ABDFE0C00 3F	"Bagaimana mas? Apakah saya perlu memberikan spoiler dulu ke internet agar anda lebih percaya?"	Sama dan terbukti

Untuk LINE Messenger sendiri kita menggunakan kolom *server_id*. Berikut merupakan analisa menggunakan *server_id*:

Tabel 12
Perbandingan *server_id* pengguna

server_id Korban	server_id Tersangka	content	Kesimpulan
"43998118788 68"	"4399811878 868"	"Selamat siang Korban 1, salam kenal"	Sama dan terbukti
"43998303477 99"	"4399830347 799"	"Halo mas, salam kenal juga. Anda siapa ya? Ada perlu apa kalau boleh tahu?"	Sama dan terbukti

4) Hasil Akhir Pembuktian

Berdasarkan hasil analisa percakapan dan bukti pendukung, didapatkan hasil bahwa dua aplikasi pengolah pesan, LINE Messenger dan WhatsApp dapat menghasilkan barang bukti yang kuat dan valid untuk sebuah kasus hukum di Indonesia karena berhasil membuktikan validitas percakapan. Untuk aplikasi WhatsApp memberikan bantuan bukti pendukung yang lebih lengkap dibandingkan LINE Messenger.

D. Perbandingan Data Digital

1) Perbandingan Data Aplikasi

Berikut merupakan tabel perbandingan antara aplikasi WhatsApp dengan LINE Messenger:

Tabel 13
Perbandingan aplikasi

Pembanding	WhatsApp	LINE Messenger
Folder Data Aplikasi	com.whatsapp	jp.naver.line.android
Lokasi Folder Data Aplikasi	data/data/com.whatsa pp	data/data/jp.naver.line. android
Folder Pendukung Aplikasi	WhatsApp	LINE_Backup
Lokasi Folder Pendukung	Penyimpanan Internal	Penyimpanan Internal
Ketersediaan Folder Pendukung	Pasti	Tentatif
Backup Percakapan	Satu <i>file</i> untuk semua percakapan	Satu <i>file</i> untuk satu percakapan
Verifikasi Perlindungan	Telepon Tipe <i>file</i> terbuka	Telepon dan <i>e-mail</i> Tipe <i>file</i>

Pembanding	WhatsApp	LINE Messenger
<i>database</i>		disembunyikan
Database kontak	wa.db	naver_line
Tabel Kontak	wa_contacts	contacts
Nomor Telepon	Tersedia	enkripsi
<i>Database Percakapan</i>	msgstore.db	naver_line
Tabel List Percakapan	chat_list	chat
Tabel Isi Percakapan	messages	chat_history
Database cadangan	dienkripsi	Tidak ada
Media	Dikelola dalam satu folder terstruktur	Dikelola terpisah
Penyimpanan Media	Otomatis	Aksi Pengguna

2) Perbandingan Database Aplikasi

Bagian ini akan membahas perbandingan *database* aplikasi yang berada pada data internal aplikasi dengan *database* yang ada pada media penyimpanan, baik internal maupun eksternal bergantung pada pengguna. Berikut merupakan perbandingan untuk *database* untuk setiap aplikasi:

a) WhatsApp

Untuk mendapatkan *file database*, *database* aplikasi harus memerlukan proses *rooting* terlebih dahulu agar dapat masuk ke dalam data. Sedangkan untuk *database* backup tidak diperlukan proses *rooting* karena *file database* tersebut berada pada media penyimpanan, baik internal maupun eksternal bergantung pada pilihan pengguna. Untuk *database* aplikasi dapat ditemukan dengan nama *file* “msgstore.db”. Sedangkan untuk *database* cadangan memiliki nama *file* “msgstore.db.crypt8”.

Setiap *file database* tersebut memiliki tujuan masing-masing sesuai lokasi *file* tersebut. *File database* aplikasi berguna untuk operasional dari aplikasi tersebut. Seluruh aktivitas dan pesan yang ada dalam aplikasi disimpan dan diproses menggunakan *database* tersebut. Sedangkan untuk *file database* backup hanya digunakan untuk *database* cadangan dan berguna untuk mengembalikan data jika percakapan terhapus atau aplikasi dilepaskan (*uninstall*). Oleh karena tujuan yang berbeda, maka pengembang memberikan penanganan khusus pada kondisi *file* masing-masing. Untuk *file database* aplikasi tidak ada enkripsi sedangkan *database* cadangan memerlukan enkripsi. Hal ini dikarenakan adanya perbedaan pada tingkat kerumitan lokasi data dan cara penggunaannya pada aplikasi.

Untuk membuka *database*, keduanya sama-sama dapat dibuka menggunakan aplikasi eksternal. Untuk *database* aplikasi, *file* dapat langsung dibuka menggunakan aplikasi pengolah *database SQLite Browser*. Sedangkan *database* cadangan tidak bisa dibuka secara langsung menggunakan *SQLite Browser*. *Database* cadangan harus dibuka menggunakan *WhatsApp Viewer* dengan tambahan kunci enkripsi menggunakan *file license* yang berada pada *folder* data aplikasi. Hal inilah yang membuat kedua *database* ini harus dilakukan *rooting* jika ingin membukanya.

b) LINE Messenger

Untuk mendapatkan *file database*, pada *database* aplikasi diperlukan proses *rooting* dahulu agar bisa masuk ke dalam *folder* data aplikasi. Sedangkan *database* cadangan tidak perlu

masuk ke dalam proses *rooting* karena berada pada media penyimpanan yang bergantung pada pilihan pengguna. Untuk nama *file*, pada *database* aplikasi kita dapat menemukan *file* tersebut dengan nama “naver_line”. Sedangkan untuk *database* backup, kita dapat menemukan *file* zip dengan nama seperti “LINE_Android-backup-chat1176348110ed.zip”.

Tujuan dari kedua *database* pada *LINE Messenger* ini tidak jauh berbeda. Untuk *database* aplikasi ditujukan pada operasional aplikasi sedangkan untuk *database* cadangan ditujukan pada pengembalian percakapan yang terhapus atau hilang. Untuk enkripsi pada *file database* aplikasi tidak ada, begitu juga dengan *database* cadangan.

Namun untuk kepentingan dalam membuka *database*, untuk *database* aplikasi dapat dibuka dengan mudah menggunakan bantuan aplikasi pengolah *database SQLite Browser*. Namun untuk *database* cadangan hingga hari ini belum diketahui cara membukanya. Selain dapat dibuka untuk *file* medianya saja menggunakan aplikasi khusus untuk *file* ZIP atau RAR semacam WinRAR, maka *file* ini hanya dapat dibuka oleh aplikasi *LINE Messenger* sendiri.

3) Perbandingan Data Perangkat

Untuk data perangkat, semua perangkat dapat dilakukan *rooting* menggunakan aplikasi tambahan. Proses *rooting* dilakukan agar dapat mengambil data yang berada dalam sistem operasi.

Untuk penarikan data secara manual menggunakan proses *imaging* pada *folder* data dan sistem pada sistem operasi Android, hanya Samsung Galaxy S3 Mini. Hal ini dikarenakan proses yang dilakukan berhasil membuat kartu memori dengan format ext-2 untuk di-mount menjadi kartu memori internal. Untuk ASUS Zenfone 2, proses mounting tidak bisa dilakukan sehingga *folder* data yang memiliki ukuran lebih dari 4 GB tidak bisa diambil dan dipindahkan ke dalam kartu memori. Untuk Bluestacks sendiri tidak bisa dilakukan karena menggunakan perangkat yang berbeda.

Untuk penarikan data menggunakan aplikasi tambahan berupa Root Explorer. Seluruh data dapat diambil dengan cara melakukan proses *zip* agar integritas data dapat dipertanggungjawabkan.

4) Perbandingan Data Eksperimen

Aktivitas pada setiap eksperimen telah diatur pada bagian sebelumnya dimana setiap eksperimen memiliki aktivitas tersendiri. Eksperimen pertama merupakan aktivitas biasa pada penggunaan aplikasi. Eksperimen kedua merupakan penggunaan aplikasi dengan tambahan aktivitas penghapusan percakapan. Eksperimen ketiga merupakan penggunaan aplikasi dengan tambahan aktivitas penghapusan aplikasi.

Berdasarkan aktivitas yang dilakukan pada setiap eksperimen akan mempengaruhi ketersediaan data aplikasi. Untuk eksperimen pertama data yang didapatkan dari aplikasi telah lengkap didapatkan. Untuk eksperimen kedua, data yang didapatkan juga sama lengkapnya, namun ada perbedaan pada *database* aplikasi dimana aktivitas percakapan yang telah dihapus tidak tercatat kembali pada *database*. Untuk eksperimen ketiga, penghapusan aplikasi mengakibatkan data aplikasi ikut terhapus sehingga tidak bisa dianalisa lebih lanjut.

Untuk data pendukung, perbedaan terhadap aktivitas nyataanya tidak banyak mempengaruhi ketersediaan data.

Indikator jumlah data hanya dapat berubah karena kondisi aktivitas aplikasi seperti adanya penambahan percakapan atau media sehingga secara menyeluruh data pendukung tidak terpengaruh atas aktivitas yang dilakukan pada aplikasi atau perangkat.

IV. KESIMPULAN

A. Kesimpulan

1. Bukti digital pada aplikasi WhatsApp dan LINE Messenger berhasil didapatkan dari perangkat Android dengan menggunakan dua cara, yaitu cara manual dan menggunakan aplikasi tambahan.
2. Data yang dapat diambil merupakan data utama dan data pendukung aplikasi. Data utama berupa *database* berisikan kontak dan percakapan dan artefak *file* penyusun aplikasi. Data pendukung aplikasi berupa *database* cadangan dan *file-file* terkait media seperti gambar, video, dan suara.
3. Faktor yang mempengaruhi keberhasilan mendapatkan bukti digital pada aplikasi WhatsApp dan LINE Messenger adalah aktivitas perubahan kondisi aplikasi dan perangkat yang digunakan.
4. WhatsApp merupakan aplikasi pengolah pesan yang menjadi rujukan dalam forensika digital di Indonesia. Sedangkan untuk LINE Messenger menjadi aplikasi pengolah pesan yang lebih aman karena sulit untuk dilakukan proses analisa forensika digital.

B. Saran

1. Dibutuhkan adanya standar baku untuk proses forensika digital yang ada di Indonesia serta formulir untuk dokumentasi agar proses terstandarisasi dan validitas hasil analisa dapat diterima oleh semua pihak yang berkepentingan.
2. Untuk pelaksanaan forensika digital pada perangkat *mobile* dibutuhkan perangkat akuisisi data secara manual semacam Cellebrite atau GPG JTAG dan sistem operasi Linux agar validitas dan integritas serta kelengkapan data yang lebih terjamin.

DAFTAR PUSTAKA

- [1] Sisternet, "Sisternet.xl.co.id," XL Corporation, 19 May 2015. [Online]. Available: <http://sisternet.xl.co.id/tiga-aplikasi-chat-terpopuler-di-indonesia-2/>. [Accessed 13 January 2016].
- [2] N. Ngazi and M. Angelina, "Viva.co.id," Viva News, 25 November 2015. [Online]. Available: <http://teknologi.news.viva.co.id/news/read/703969-tembus-30-juta-pengguna-indonesia--line-rilis-stiker-musik>. [Accessed 13 January 2016].
- [3] W. Aji, "Tribun Nasional," Tribunnews, 9 November 2015. [Online]. Available: <http://www.tribunnews.com/nasional/2015/11/09/rio-capella-minta-uang-ke-sisca-lewat-whatsapp>. [Accessed 11 January 2016].
- [4] Hidayat, "Tempo Online," Tempo, 14 Desember 2015. [Online]. Available: <http://metro.tempo.co/read/news/2015/12/14/214727532/kasus-muncikari-artis-nikita-bareskrim-akan-ada-tersangka-baru>. [Accessed 11 January 2016].
- [5] C. Anglano, "Forensic Analysis of WhatsApp Messenger on Android," *Elsevier*, 2014.