sistem informasi
fakultas teknologi informasi

Sidang Akhir

Laboratorium Infrastruktur dan Keamanan Teknologi Informasi

Jurusan Sistem Informasi,

Fakultas Teknologi Informasi,

Institut Teknologi Sepuluh Nopember

Surabaya, Jawa Timur

Indonesia

Identitas Penulis

NAMA : **Syukur Ikhsani**

NRP : **5212 100 147**

DOSEN PEMBIMBING I : **Bekti Cahyo Hidayanto, S.Si., M.Kom**

LAB : **Infrastruktur dan Keamanan TI**

Judul Tugas Akhir

ANALISA FORENSIK WHATSAPP DAN LINE MESSENGER PADA SMARTPHONE ANDROID SEBAGAI RUJUKAN DALAM MENYEDIAKAN BARANG BUKTI YANG KUAT DAN VALID DI INDONESIA

FORENSICS ANALYSIS OF WHATSSAPP AND LINE MESSENGER ON ANDROID SMARTPHONES AS A REFERENCE FOR DELIVERING THE STRONG AND VALID EVIDENCE IN INDONESIA

BAB I PENDAHULUAN

BAB II TINJAUAN PUSTAKA

BAB III METODOLOGI PENELITIAN

BAB IV PERANCANGAN

BAB V IMPLEMENTASI

BAB VI HASIL DAN PEMBAHASAN

BAB VII KESIMPULAN DAN SARAN

BAB I Pendahuluan

Latar Belakang Masalah

- Penggunaan teknologi mobile yang semakin meningkat
- Mulai marak penggunaan mobile untuk kejahatan
- Kurangnya penelitian terkait aplikasi pengolah pesan di Indonesia
- Belum adanya penelitian terkait LINE Messenger

Perumusan Masalah

1. **BAGAIMANA CARA MENGHASILKAN** barang bukti digital yang diambil yang ada di telepon genggam pengguna/tersangka?
2. **HASIL DATA APA SAJA** yang bisa dibaca dan diselamatkan berdasarkan beberapa skenario yang diciptakan?
3. **BAGAIMANA PERBANDINGAN DATA** yang dapat didapatkan pada kedua aplikasi pengolah pesan tersebut?
4. **FAKTOR APA SAJA** yang mempengaruhi keberhasilan pada forensika digital kedua aplikasi pengolah pesan tersebut?
5. Aplikasi manakah yang menjadi **RUJUKAN TERBAIK DALAM FORENSIKA DIGITAL** untuk perangkat pengolah pesan di Indonesia?

Batasan Masalah

- Perangkat yang digunakan dalam eksperimen Tugas Akhir ini adalah sebagai berikut :
  - Perangkat Telepon Genggam
    - ASUS Zenfone 2 dengan Android OS versi 5.0
    - Samsung Galaxy 3 Mini dengan Android OS versi 4.1
  - Emulator
    - Bluestack 2 Native
- Eksperimen menggunakan Aplikasi LINE Messenger dan Whatsapp versi terakhir, yaitu :
  - LINE Messenger : 5.10.1
  - WhatsApp : versi 2.12.510

Batasan Masalah

- Percobaan mengunakan skenario percakapan dan 3 eksperimen penggunaa aplikasi
- Dalam penelitian ini, penulis menggunakan aplikasi forensika digital berikut :
  - Root Explorer 2
  - ADB Shell
  - Access Data FTK Imager versi 3.4.0.5
  - SQLite Browser
- Kondisi paling ekstrim dibatasi pada penghapusan aplikasi
- Penelitian ini hanya menganalisa pada hasil data yang dapat diambil dari kedua aplikasi pengolah pesan yang ada pada perangkat telelpon genggam

Tujuan Penelitian

1. Mengetahui **CARA MENDAPATKAN BUKTI DIGITAL** pada aplikasi LINE Messenger dan WhatsApp yang dipasang pada perangkat telepon genggam
2. Mengetahui **MACAM-MACAM DATA YANG DIDAPATKAN** dari teknik forensika digital pada kedua aplikasi pengolah pesan tersebut
3. Mengetahui **PERBANDINGAN BUKTI DIGITAL** yang didapatkan dari kedua aplikasi pengolah pesan tersebut
4. Mengetahui **FAKTOR YANG MEMPENGARUHI KEBERHASILAN** mendapatkan bukti digital dari kedua aplikasi pengolah pesan tersebut
5. Mengetahui aplikasi pengolah pesan mana yang menjadi **RUJUKAN DALAM FORENSIKA DIGITAL** di Indonesia

Manfaat Penelitian

1. Memberikan panduan bagi pengembang dan akademisi untuk mengembangkan perangkat lunak forensik aplikasi pengolah pesan.
2. Memberikan gambaran terhadap penegak hukum dalam mendapatkan barang bukti terkait kasus yang melibatkan kedua aplikasi pengolah pesan tersebut
3. Menjadi referensi untuk kalangan akademisi dalam pengembangan penelitian terkait forensika digital di Indonesia.

Relevansi

Penelitian ini mengambil cakupan ***MATA KULIAH FORENSIKA DIGITAL DAN KEAMANAN ASET INFORMASI***. Selain itu, penelitian tugas akhir ini juga termasuk dalam topik yang ada pada ***LABORATORIUM INFRASTRUKTUR DAN KEAMANAN TEKNOLOGI INFORMASI*** di Jurusan Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember, Surabaya.

BAB II Tinjauan Pustaka

No	Judul Penelitian	Metode Yang digunakan	Kesimpulan
1	Network And Device Forensic Analysis of Android Social-Messaging Applications (Daniel Walnycky, Ibrahim Baggili, Andrew Marrington, Jason Moore, Frank Breitinger, Journal on Elsevier, 2015)	1. Analisa berdasarkan jaringan yang digunakan 2. Analisa komunikasi data yang terjadi 3.Analisa Penyimpanan Data pada Telepon Seluler	Beberapa aplikasi yang dapat diambil barang buktinya, termasuk WhatsApp berupa komunikasi dan transfer media.
2	Forensic Analysis of Social Networking Applications on Mobile Devices (Noora Al Mutawa, Ibrahim Baggili, Andrew Marrington, Journal on Elsevier, 2012)	1.Percobaan dilakukan menggunakan memori internal untuk melakukan pemulihan. 2. Menggunakan tiga aplikasi sosial median dengan tiga perangkat berbeda 3. Pengujian dan pemeriksaan menggunakan pedoman dari National Institute of Standards and Technology, yaitu panduan program Computer Forensics Tool Testing.	Blackberry merupakan perangkat yang paling aman karena tidak dapat dibackup. Sedangkan Android dan Apple bisa menghasilkan bukti forensik melalui pemulihan data.
3	Forensic Analysis of WhatsApp on Android Smartphones (Neha S. Thakur, University of New Orleans Theses and Dissertations, 2013)	1. Pendekatan utama adalah untuk mengakuisisi memori dengan meminimalisir perubahan oleh manusia lain 2. Berkontrensasi pada dua area pendekatan pada pengambilan bukti, yaitu akuisisi dan analisa data dari memori non-volatile dan memori volatile	Aplikasi Populer seperti WhatsApp telah berhasil diforensikkan. Tiga hal yang bisa diambil dari penelitian ini adalah nomor pengguna, aktivitas percakapan, dan struktur serta queri dari database WhatsApp
4	Forensic Analysis of WhatsApp Messenger on Android Smartphones (Cosimo Anglano, Journal on Elsevier, 2014)	1. Penggunaan skenario yang biasa terjadi dalam interaksi pengguna seperti satu-satu, komunikasi grup, dan pertukaran pesan multimedia 2. Penggunaan pendekatan dengan menggunakan software emulator memudahkan dalam mengakuisi memori internal sehingga tidak perlu untuk memeriksa isi file 3. Adanya pengujian terhadap hasil Youwave dengan penggunaan data yang biasa ditemukan dalam kondisi nyata	Penelitian menunjukkan bagaimana cara mengubah data yang tersimpan untuk merekonstruksi kontak dan kronologi percakapan. Kita dapat melihat bukti-bukti yang dapat diambil dari WhatsApp seperti decoding, interpretasi, dan korelasinya. Kita bisa membandingkan hasil emulator dengan telepon seluler

Barang Bukti Digital

- Departemen Hukum AS
  - Informasi yang disimpan atau dikirimkan dalam bentuk binary atau digital yang dapat digunakan untuk kasus hukum maupun pengadilan.
- UU ITE no 11 tahun 2008
  - Informasi elektronik adalah satu satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya
  - Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik.

Forensika Digital

- Forensika digital adalah cabang dari ilmu forensik yang meliputi usaha pemulihan dan investigasi terhadap bukti-bukti yang berada atau ditemukan dari perangkat digital yang ada kaitannya dengan tindak kejahatan
- Forensika digital biasanya digunakan untuk beberapa tujuan, yaitu
  - untuk membuktikan maupun menolak sebuah dugaan dalam permasalahan hukum, baik di tingkat pidana maupun perdata
  - serta untuk penyelidikan di tingkat internal organisasi maupun perusahaan

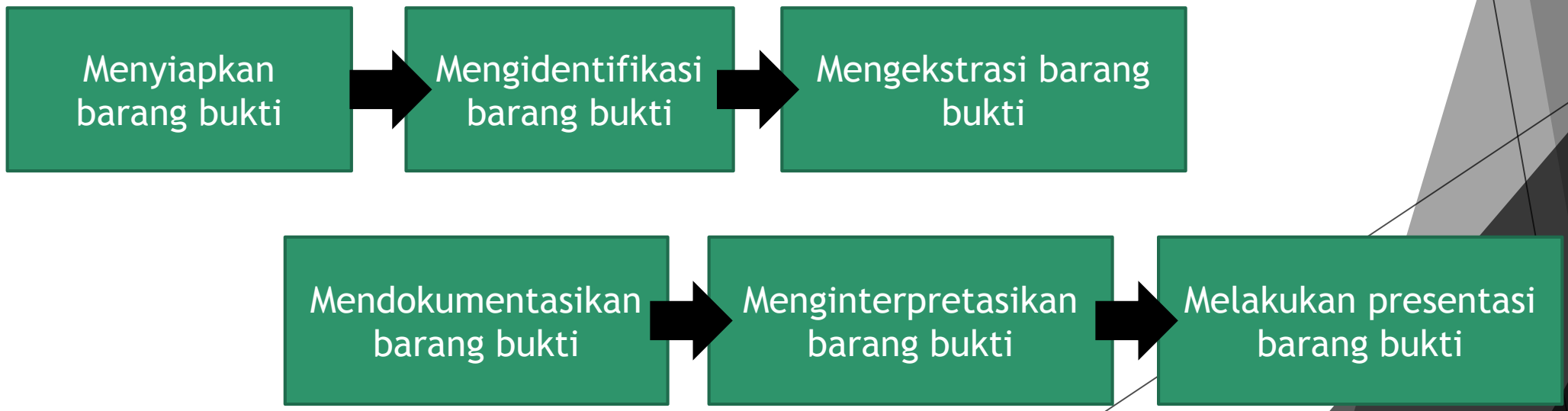


FD – Forensik Perangkat Bergerak

- Forensik perangkat bergerak merupakan cabang dari forensika digital yang berkaitan dengan pemulihan atau investigasi terhadap bukti digital yang ada pada perangkat bergerak
- Kebutuhan untuk analisa perangkat bergerak lebih ditekankan pada beberapa alasan berikut, yaitu
  - Penggunaan perangkat bergerak untuk menyimpan dan berbgai informasi personal dan perusahaan
  - Penggunaan perangkat bergerak dalam transaksi *online*
  - Penegakan hukum dan kriminal pada perangkat bergerak.

FD – Tahapan Forensik

- Secara umum ada empat tahapan yang harus dilakukan dalam mengelola bukti pada forensika digital, yaitu pengumpulan, pemeliharaan, analisa, dan presentasi.
- Dalam tugas akhir ini, penulis menggunakan pendapat dari David Watson yang merumuskan tahapan-tahapan forensika digital ke dalam langkah-langkah berikut :



Aplikasi Pengolah Pesan – LINE Messenger

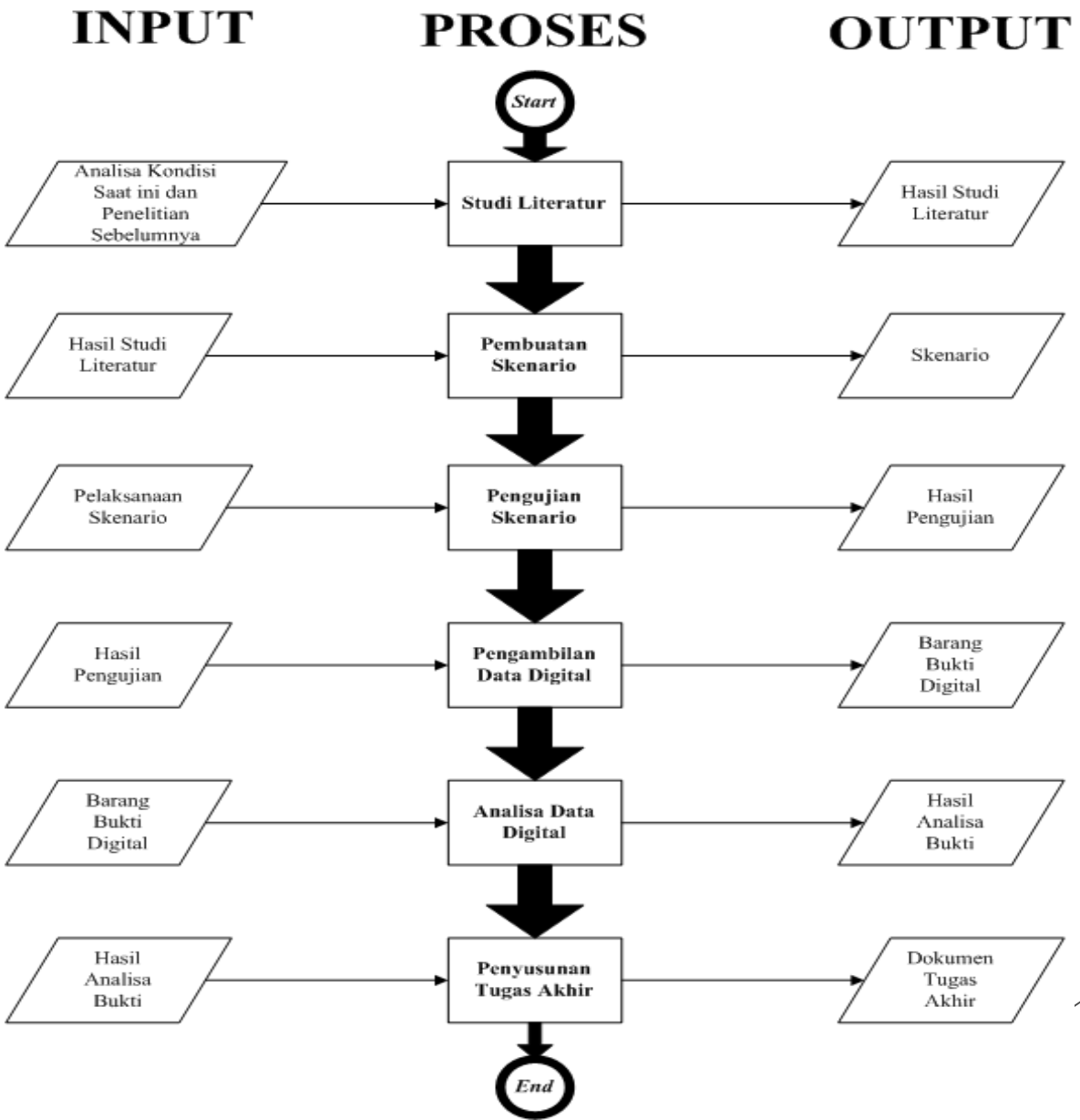
- LINE Messenger adalah sebuah aplikasi pengirim pesan instan gratis yang digunakan pada berbagai jenis perangkat seperti telepon pintar, tablet, dan komputer. LINE Messenger dikembangkan oleh perusahaan Jepang bernama NHN Corporation dan pertama kali diliris pada Juni 2011

Aplikasi Pengolah Pesan - Whatsapp

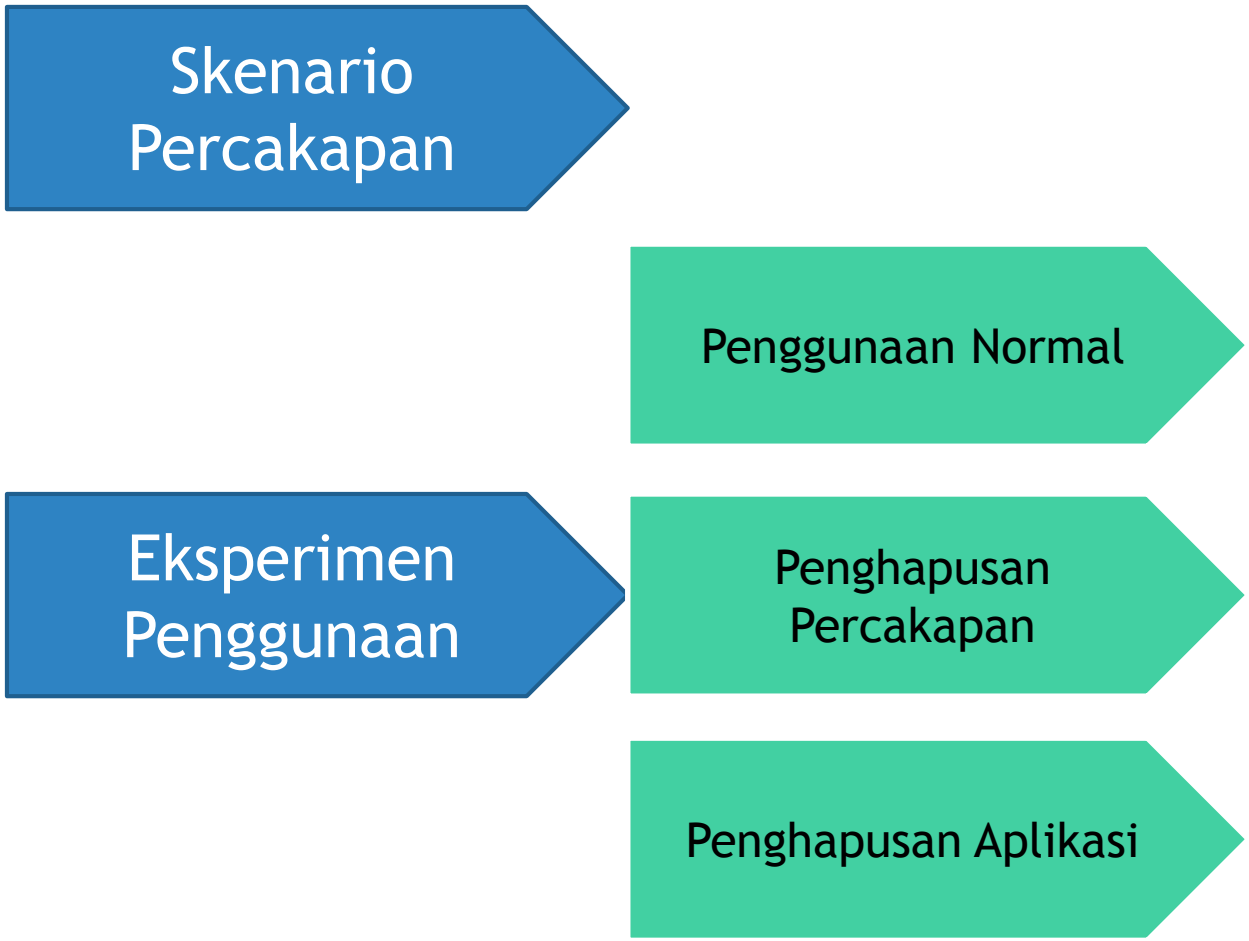
- WhatsApp adalah aplikasi pengolah pesan yang dapat digunakan oleh beragam lintas perangkat tanpa harus membayar tagihan SMS
- WhatsApp telah tersedia untuk Android. iPhone, Blackberry, Windows dan lain-lain

BAB III Metodologi Penelitian

Tahapan Pelaksanaan



Pembuatan Skenario dan Eksperimen



Pengujian Skenario dan Eksperimen

- Skenario akan dijalankan sesuai dengan kondisi yang ada pada lingkungan yang sebenarnya
- Metode dalam menguji skenario adalah dengan menggunakan telepon seluler dan emulator yang telah dipasang di laptop peneliti.

Pengambilan Data Digital

- Aplikasi yang digunakan adalah penggandaan data dan Backup
- Jika diperlukan, maka penggunaan perangkat forensik akan digunakan pada penelitian dengan kerjasama dengan pihak eksternal Jurusan Sistem Informasi ITS yang memiliki perangkat tersebut.

Analisa Data Digital

- Setelah data berhasil didapatkan, maka akan dianalisa menggunakan aplikasi dan literatur pendukung untuk mencapai tujuan dari penelitian.
- 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.

BAB IV Perancangan

Pembuatan Skenario Percakapan

Pelaksanaan Eksperimen

Pengambilan Data Digital

Analisa Data

Dapat dilihat di Lampiran A

Pembuatan Skenario Percakapan

Pelaksanaan Eksperimen

Pengambilan Data Digital

Analisa Data

- 3 Eksperimen :
  - Biasa
  - Penghapusan Percakapan
  - Penghapusan Aplikasi
- Pelaksanaan
  - Perangkat : 2 handphone dan 1 Laptop (untuk emulator)
  - Aplikasi : LINE & WhatsApp
  - 3 E-mail, 3 nomor aktif, Pilihan Kontak, 3 kartu memori, 2 gambar, 1 video
- Kondisi Pelaksanaan : sesuai dengan realita

Pembuatan Skenario Percakapan

Pelaksanaan Eksperimen

Pengambilan Data Digital

Analisa Data

- Data yang diambil adalah yang terkait aplikasi WhatsApp dan LINE Messenger
- Dahulukan untuk Proses Backup (eksperimen 1)
- Akuisisi mempertimbangkan perangkat dan aplikasi

Pembuatan Skenario Percakapan

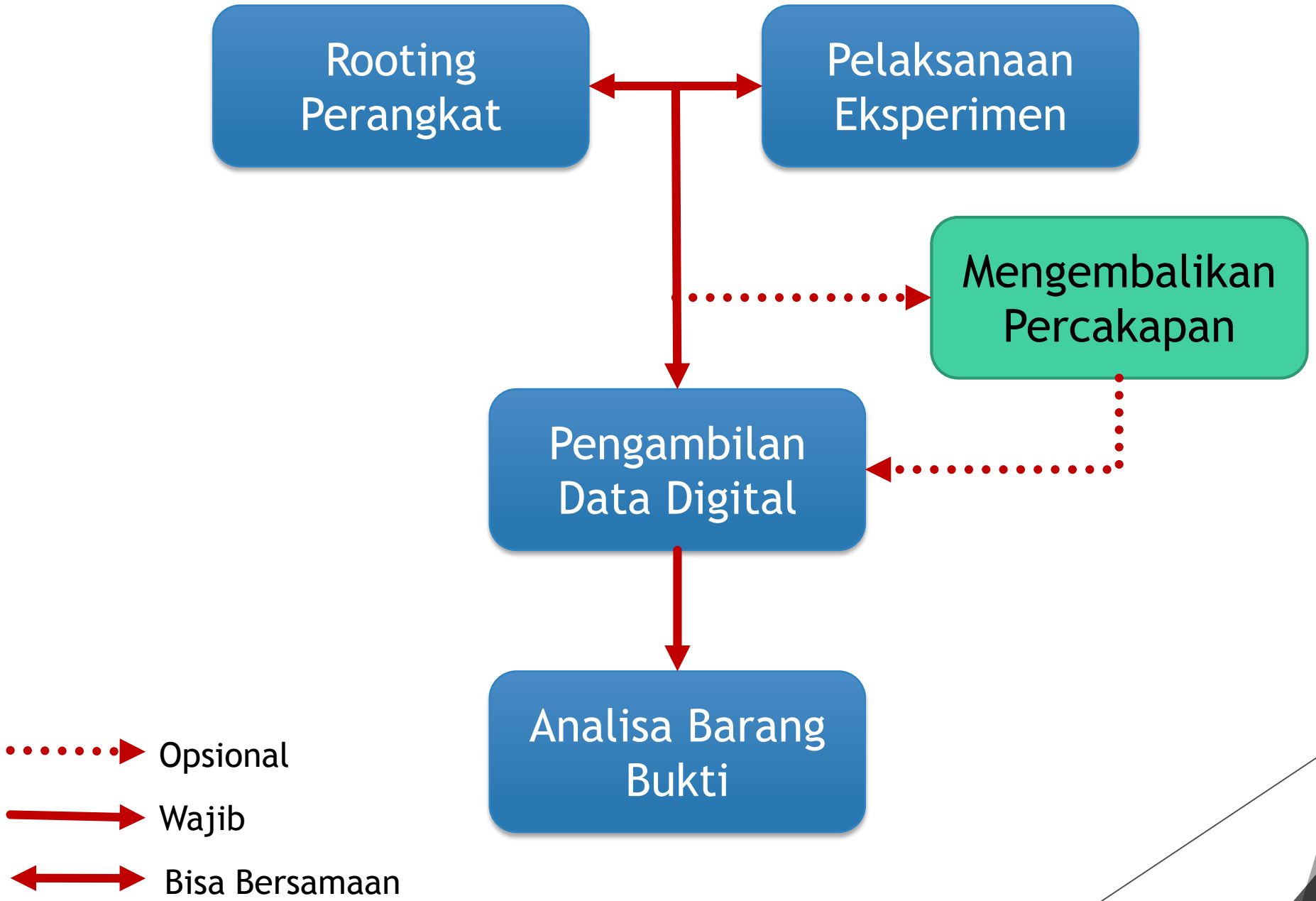
Pelaksanaan Eksperimen

Pengambilan Data Digital

Analisa Data

- **Penelusuran Data** → Struktur Data
- **Membaca data** → Jenis data
- **Perbandingan Data** → Perbandingan Aplikasi, Perangkat, dan Eksperimen
- **Penilaian Data** → Aplikasi yang menjadi rujukan Forensika Digital

BAB V Implementasi


Rooting Perangkat
Pelaksanaan Eksperimen
Mengembalikan Percakapan
Pengambilan Data Digital
Analisa Barang Bukti
Opsional
Wajib
Bisa Bersamaan

Rooting Perangkat

Pelaksanaan Eksperimen

Pengambilan Data Digital

Analisa Data

Mengembalikan Percakapan

- ASUS Zenfone 2
  - Menggunakan rekomendasi dari Komunitas Developer Zenfone
- Samsung S3 Mini
  - Menggunakan aplikasi Odin dan beberapa paket tambahan
- Bluestacks 2 Native
  - Menggunakan aplikasi pendukung Bluestack Easy

Rooting Perangkat

Pelaksanaan Eksperimen

Pengambilan Data Digital

Analisa Data

Mengembalikan Percakapan

Aktor	Perangkat	Nomor Telepon	Email (gmail.com)
Tersangka	Samsung S3 Mini	085749598994	Syukurikhsani12
Korban 1	Asus Zenfone ZE550ML	081218172958	Riberyxiii
Korban 2	Bluestack 2 Native	081284467254	icans147

Rooting Perangkat

Pelaksanaan Eksperimen

Pengambilan Data Digital

Analisa Data

Mengembalikan Percakapan

- Membuat Data Cadangan Percakapan
  - Menggunakan aplikasi tersebut
  - WhatsApp = semua percakapan
  - LINE Messenger = satu percakapan
- Manual
  - Menggunakan ADB Shell dan FTK Imager
  - Untuk Perangkat Samsung S3 Mini dan Kartu Memori
- Menggunakan Aplikasi Tambahan
  - Menggunakan Root Explorer
  - Untuk semua perangkat

Rooting Perangkat

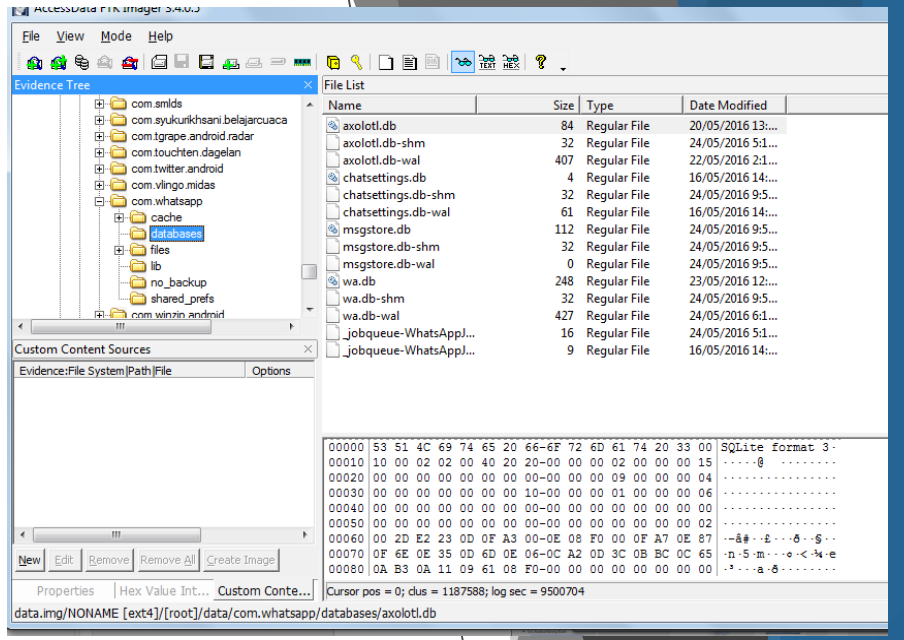
Pelaksanaan Eksperimen

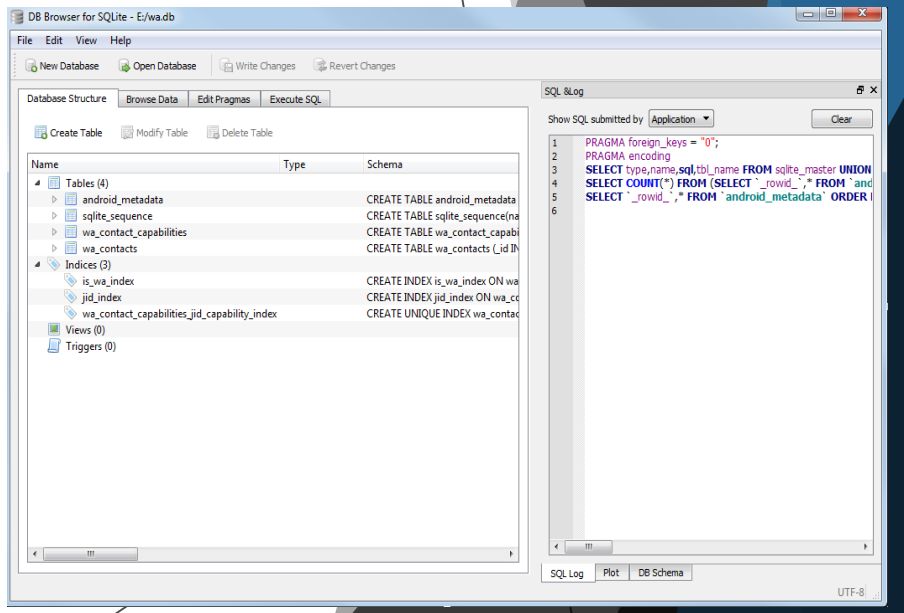
Pengambilan Data Digital

Analisa Data

Mengembalikan Percakapan

- FTK Imager
  - Untuk menganalisa struktur folder dan tipe data
- SQLite Browser
  - Untuk menganalisa struktur dan isi dari database





Rooting Perangkat

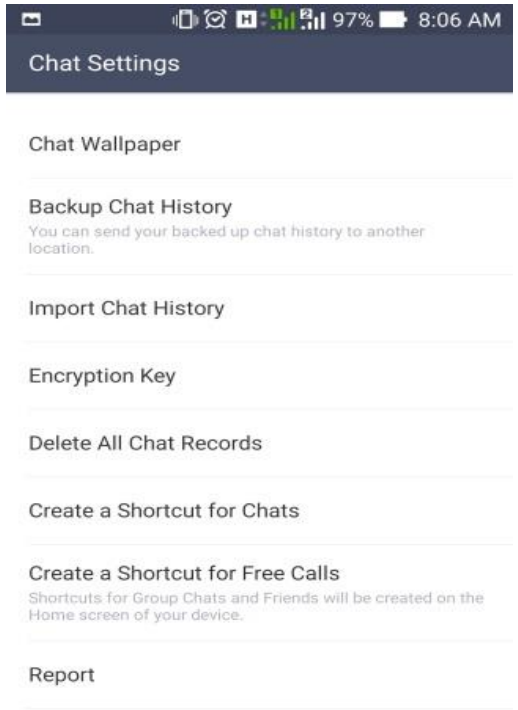
Pelaksanaan Eksperimen

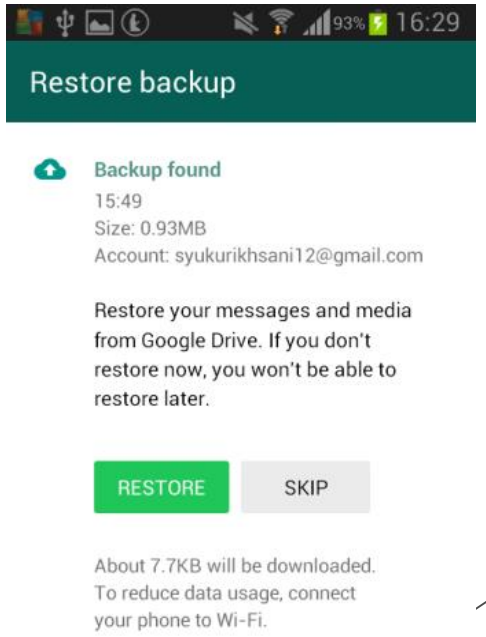
Pengambilan Data Digital

Analisa Data

Mengembalikan Percakapan

- WhatsApp
  - Restore percakapan dilakukan pada saat instalasi
  - Untuk semua percakapan
- LINE Messenger
  - Restore percakapan dapat dilakukan kapan saja
  - Untuk satu percakapan





Hambatan dan Rintangan

- Kebijakan aplikasi
- Pembaharuan sistem perangkat saat kondisi rooting
- Imaging untuk Zenfone dan Bluestacks tidak bisa dijalankan
- Lokasi data harus diperhatikan

BAB VI Hasil dan Pembahasan

Ketersediaan Data Digital

	Metode/ Perangkat	ASUS Zenfone 2	Samsung S3 Mini	Bluestacks 2 Native
Eksperimen 1	Manual	- Kartu Memori	- data.img - sistem.img - Kartu Memori	tidak ada
Eksperimen 2	Aplikasi Tambahan *dalam bentuk zip	- com.whatsapp - jp.never.line -LINE_Backup - WhatsApp	- com.whatsapp - jp.never.line -LINE_Backup - WhatsApp	- com.whatsapp - jp.never.line -LINE_Backup - WhatsApp
Eksperimen 3				

Ketersediaan Data Digital

Eksperimen 1

Eksperimen 2

Eksperimen 3

Metode/ Perangkat	ASUS Zenfone 2	Samsung S3 Mini	Bluestacks 2 Native
Manual	- Kartu Memori	- data.img - sistem.img - Kartu Memori	tidak ada
Aplikasi Tambahan *dalam bentuk zip	- com.whatsapp - jp.never.line -LINE_Backup - WhatsApp	- com.whatsapp - jp.never.line -LINE_Backup - WhatsApp	- com.whatsapp - jp.never.line -LINE_Backup - WhatsApp

Ketersediaan Data Digital

Eksperimen 1

Eksperimen 2

Eksperimen 3

Metode/ Perangkat	ASUS Zenfone 2	Samsung S3 Mini	Bluestacks 2 Native
Manual	- Kartu Memori	- data.img - sistem.img - Kartu Memori	tidak ada
Aplikasi Tambahan *dalam bentuk zip	- LINE_Backup - WhatsApp	-LINE_Backup - WhatsApp	-LINE_Backup - WhatsApp

Analisa Data Digital

Lokasi Data

- WhatsApp
  - com.whatsapp → ***data*** → ***data*** → ***com.whatsapp***
  - WhatsApp → Penyimpanan Internal/Eksternal
- LINE Messenger
  - jp.naver.line.android → ***data*** → ***data*** → ***jp.naver.line.android***
  - LINE_Backup (tentatif) → Penyimpanan Internal/Eksternal

Struktur Folder Aplikasi

com.whatsapp

WhatsApp

jp.naver.line.android

LINE_Backup

Nama File	Tipe File	Keterangan File
Metrics_guid	Tidak diketahui	Hanya tersedia pada perangkat ASUS Zenfone 2
Web Data	SQLite Format 3	Terdapat pada perangkat ASUS Zenfone 2 dan Bluestacks 2 Native
Web Data-journal	Tidak Diketahui	
Webview_data.lock	Tidak diketahui	Hanya tersedia pada perangkat ASUS Zenfone 2

shared_prefs

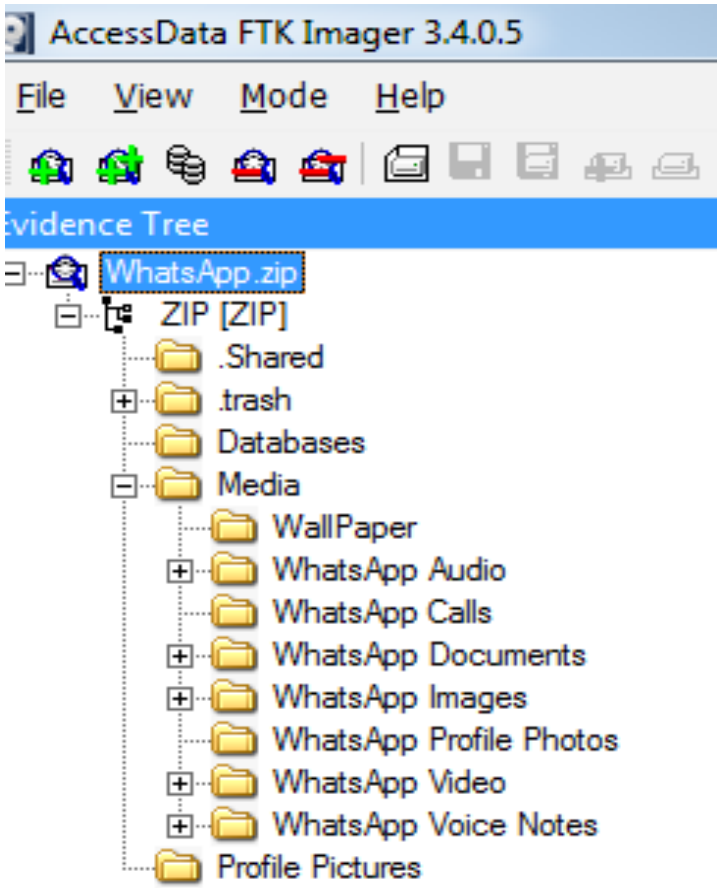
Struktur Folder Aplikasi

com.whatsapp

WhatsApp

jp.naver.line.android

LINE_Backup



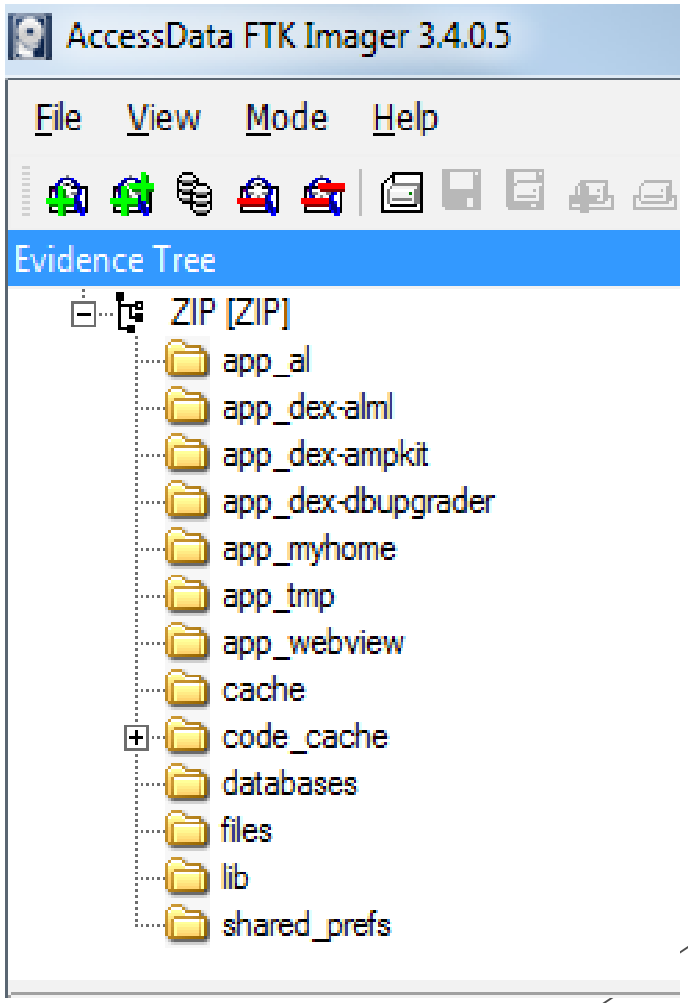
Struktur Folder Aplikasi

com.whatsapp

WhatsApp

jp.naver.line.android

LINE_Backup



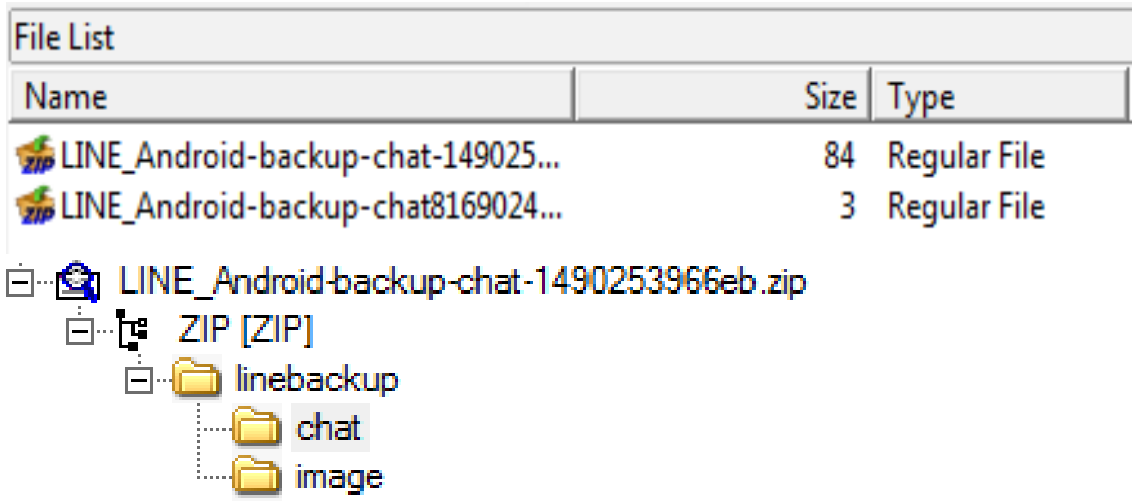
Struktur Folder Aplikasi

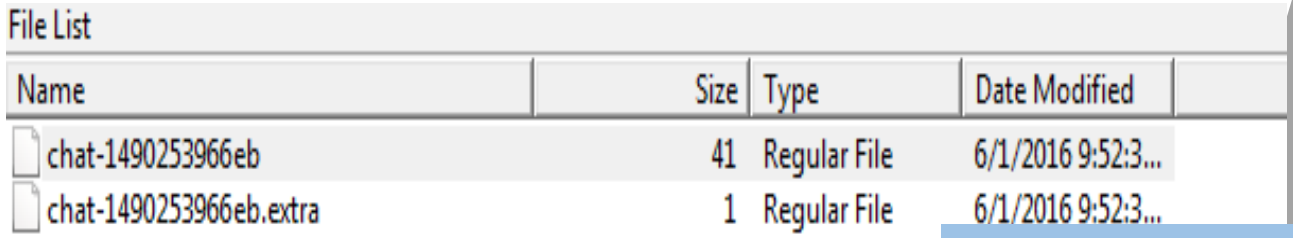
com.whatsapp

WhatsApp

jp.naver.line.android

LINE_Backup





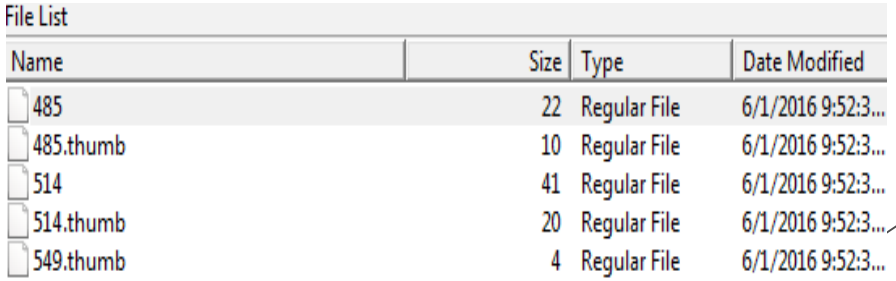


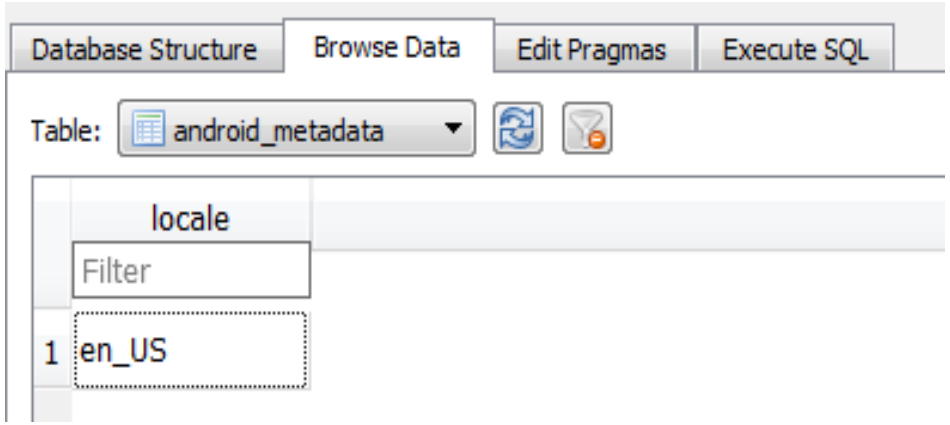
Foto porno

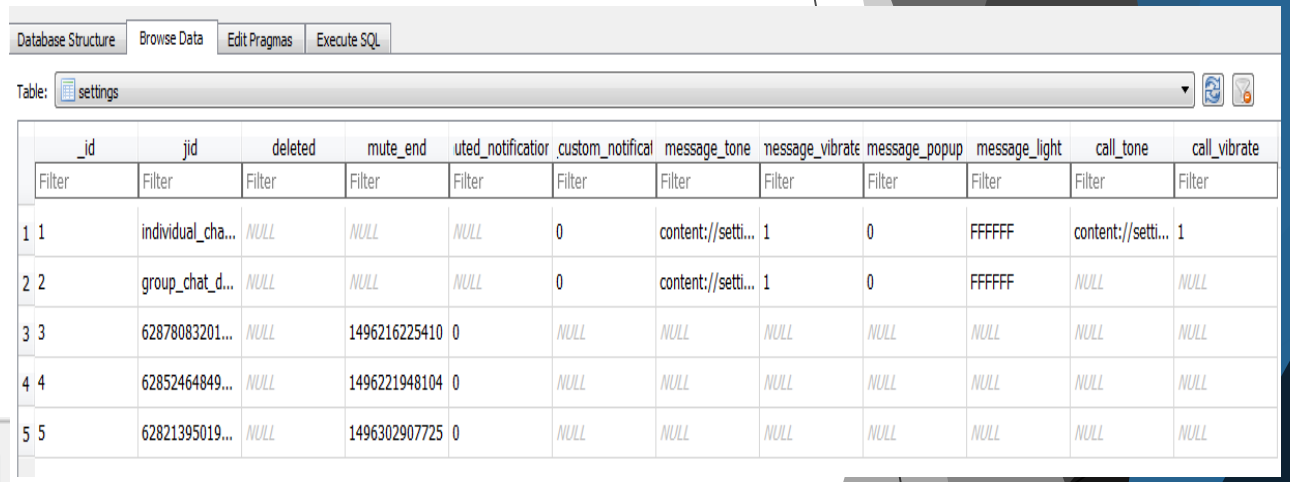
Korban 1 dan korban 2

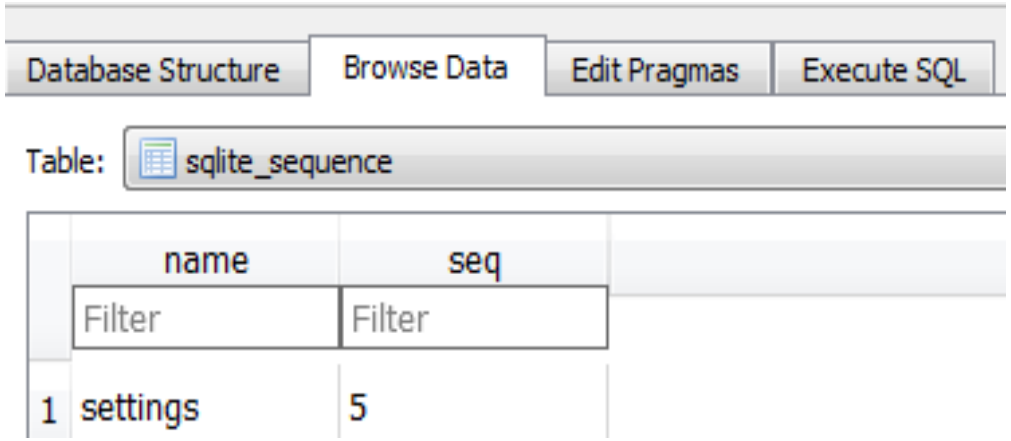
Analisa Database Aplikasi

Nama Tabel	Skema tabel
Android_metadata	CREATE TABLE android_metadata (locale TEXT)
settings	CREATE TABLE settings (_id INTEGER PRIMARY KEY AUTOINCREMENT,jid TEXT,deleted INTEGER,mute_end INTEGER,muted_notifications BOOLEAN,use_custom_notifications BOOLEAN,message_tone TEXT,message_vibrate INTEGER,message_popup INTEGER,message_light INTEGER,call_tone TEXT,call_vibrate INTEGER)
Sqlite_sequence	CREATE TABLE sqlite_sequence(name,seq)

Analisa Database Aplikasi







WhatsApp

File Database	Ada
Web Data	v
axolotl.db	v
axolotl.db-wal	v
chatsettings.db	v
chatsettings.db-wal	-
chatsettings.db-journal	-
msgstore.db	v
msgstore.db-wal	v
wa.db	v
_jobqueue-WhatsAppJobManager	v
_jobqueue-WhatsAppJobManager-journal	-

LINE Messenger

File Database	Ada
Web Data	v
as_dic	v
as_dic-journal	x
cafecache.db	v
cafecache.db-journal	x
call_history	v
call_history-journal	x
channel	v
channel-journal	x
com_linecorp_linebox_android	v
com_linecorp_linebox_android-journal	x
e2ee	v
e2ee-journal	x
line_general_key_value	v
line_general_key_value-journal	x
linenotice_pref.db	v
linenotice_pref.db-journal	x
materialDB	v
materialDB-journal	x
naver_line	v
naver_line_myhome	v
naver_line_myhome-journal	x
naver_line_private_chat	v

File Database	Ada
naver_line_private_chat-journal	x
naver_line_push_history	v
naver_line_push_history-journal	x
naver_line-journal	x
NewBadge.db	v
NewBadge.db-journal	x
obs_local_cache	v
obs_local_cache-journal	x
read_notification	v
read_notification-journal	x
search.sqlite	v
search.sqlite-journal	x
TsEvent	v
TsEvent-journal	x
TsLog	v
TsLog-journal	x
webview.db	v
webview.db-wal	x
webviewCookiesChromium.db	v

Analisa Bukti Digital

Kategorisasi Data Digital WhatsApp

Data WhatsApp	Kepentingan	Tabel yang digunakan	Fungsi	Lokasi Data
Wa.db	Penting	Wa_contacts	Melihat kontak	com.whatsapp
Msgstore.db	Penting	Chat_list	Melihat daftar percakapan	com.whatsapp
		messages	Melihat isi percakapan	
WhatsApp Profile Pictures	Pendukung		Melihat foto profil	WhatsApp
WhatsApp Audio	Pendukung		Melihat file catatan suara	WhatsApp
WhatsApp Images	Pendukung		Melihat file gambar	WhatApp
WhatsApp Video	Pendukung		Melihat file video	WhatsApp

Kategorisasi Data Digital (LINE Messenger)

- Database naver_line
  - Tabel Contacts → Untuk membaca daftar kontak
  - Tabel chat → Untuk membaca daftar percakapan
  - Tabel Chat_history → Untuk membaca isi percakapan

Pembacaan Database

- wa_contacts
- chat_list
- messages
- contacts
- chat
- chat_history

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

Pembacaan Database

- wa_contacts
- chat_list
- messages
- contacts
- chat
- chat_history

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

Pembacaan Database

- wa_contacts
- chat_list
- messages
- contacts
- chat
- chat_history

Nama Kolom	Arti/Fungsi
_id	Nomor rekaman database
key_remote_jid	WhatsApp ID
key_from_me	Arah pesan
key_id	Nomor Identitas pesan
status	Status pesan
needs_push	Penunjuk pesan Broadcast
data	Konten pesan text
timestamp	Waktu pesan dikirim (kode unix epoch time)
media_url	URL file media yang dikirim
media_mime_type	Tipe MME dari file yang telah dikirim
media_wa_type	Tipe pesan
media_size	Ukuran media yang dikirim
media_name	Nama file yang dikirim
media_caption	Isi caption dari file yang dikirim
media_hash	Enkripsi data terkait media yang dikirim
media_duration	Durasi media yang dikirim
origin	Isi Percakapan
latitude	Garis lintang lokasi pengirim
longitude	Garis bujur lokasi pengirim
thumb_image	Gambar tampilan

Nama Kolom	Arti/Fungsi
remote_resource	ID pengirim (untuk grup chat)
received_timestamp	Waktu pesan sampai pada perangkat sendiri (kode unix epoch time)
send_timestamp	Waktu pengiriman
receipt_server_timestamp	Waktu pesan sampai pada server (kode unix epoch time)
receipt_device_timestamp	Waktu pesan sampai tujuan (kode unix epoch time)
read_device_timestamp	Waktu pesan dibaca (kode unix epoch time)
played_device_timestamp	Waktu media dimainkan(kode unix epoch time)
raw_data	Tampilan untuk gambar / video
recipient_count	Jumlah penerima (pada percakapan grup)
participant_hash	Kode peserta (grup)
starred	Kode bintang (percakapan yang ditandai)

Pembacaan Database

- wa_contacts
- chat_list
- messages
- contacts
- chat
- chat_history

Nama Kolom	Arti/Fungsi
m_id	ID Pengguna LINE
contact_id	ID Kontak pada perangkat
contact_key	Kunci Kontak pada Perangkat
name	Nama Kontak pada Aplikasi
phonetic_name	Tidak Diketahui
server_name	Nama pada Server Aplikasi
addressbook_name	Nama pada Kontak Perangkat
custom_name	Tidak Diketahui
status_msg	Status pada Kontak
is_unread_status_msg	Status pesan yang belum dibaca
picture_status	Foto pada Kontak
picture_path	Kode Foto
relation	Hubungan antara user dengan kontak
status	Status Akun pada Kontak Aplikasi
is_first	Tidak diketahui

Nama Kolom	Arti/Fungsi
display_type	Tidak diketahui
capable_flags	Penanda Kontak
contact_kind	Jenis Kontak
contact_type	Tipe Kontak
buddy_category	Kategori akun/kontak
buddy_icon_type	Tipe Icon Kontak
is_on_air	Kontak yang sedang Live/online
hidden	Kontak yang disembunyikan
favorite	Kontak favorit
added_time_to_friend	Tidak diketahui
updated_time	Waktu pembaruan rekomendasi (kode unix epoch time)
created_time	Waktu pembuatan rekomendasi (kode unix epoch time)
recommend_params	Jalur Akun yang direkomendasikan

Pembacaan Database

- wa_contacts
- chat_list
- messages
- contacts
- chat
- chat_history

Nama Kolom	Fungsi / Isi
chat_id	ID percakapan
chat_name	Nama Percakapan
owner_mid	User Pemilik Percakapan
last_from_mid	ID User aktif terakhir
last_message	Isi Pesan terakhir
last_created_time	Waktu terakhir dibuat (kode unix epoch time)
message_count	Jumlah pesan
read_message_count	Jumlah pesan yang telah dibaca
type	Tipe percakapan
is_notification	Notifikasi
skin_key	Kunci Skin (warna background)
input_text	Tidak diketahui
hide_member	Daftar anggota disembunyikan
p_timer	Tidak diketahui
last_message_display_time	Pesan terakhir dilihat (kode unix epoch time)
mid_p	Tidak diketahui
is_archived	Pesan sudah diarsipakn
read_up	ID Server

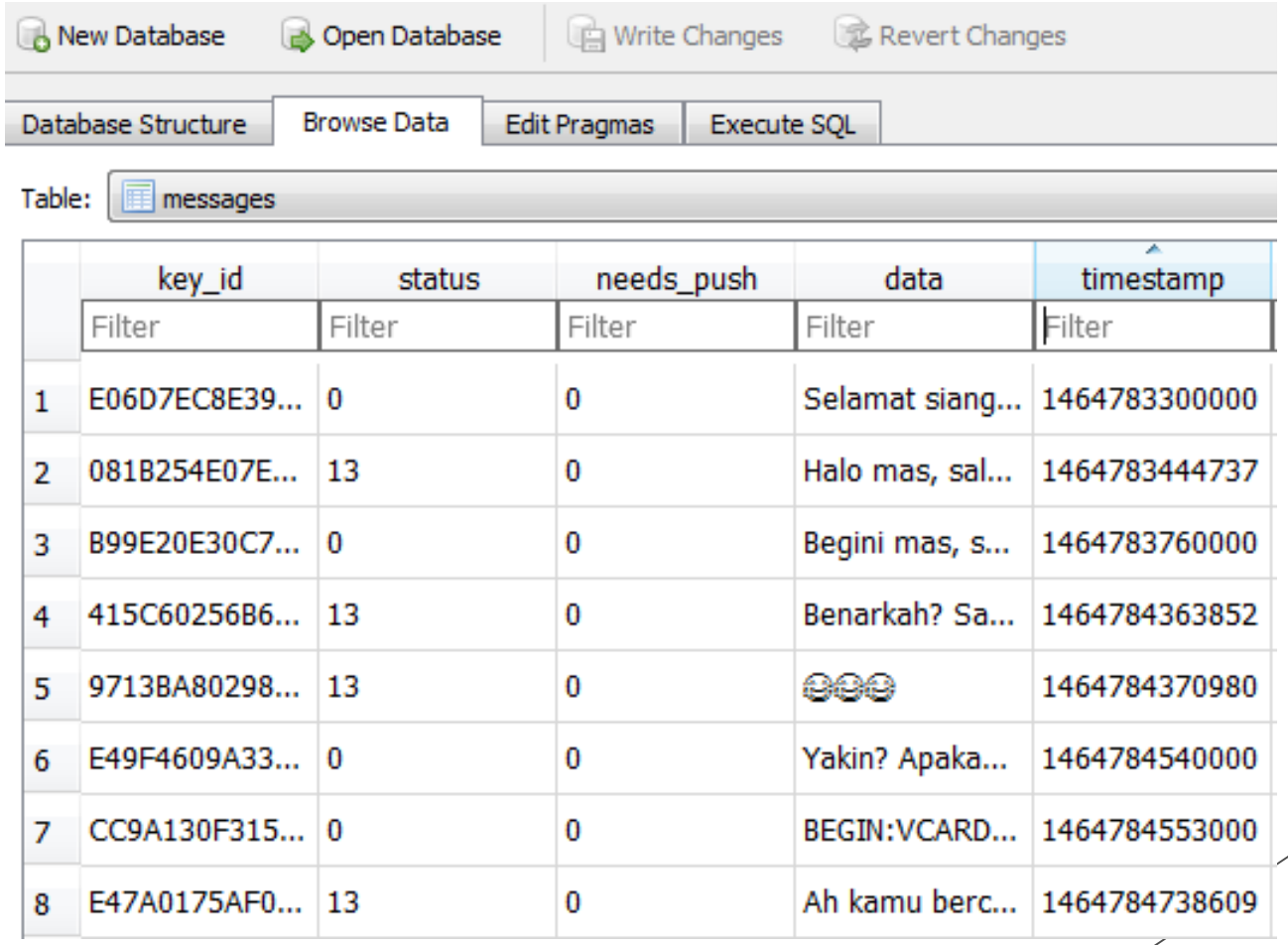
Pembacaan Database

- wa_contacts
- chat_list
- messages
- contacts
- chat
- chat_history

Nama Kolom	Arti / Fungsi
id	Nomor rekaman pada database aplikasi
server_id	Nomor rekaman pada server aplikasi
type	Tipe pesan
chat_id	ID Percakapan
from_mid	ID Pengirim
content	Isi pesan
created_time	Waktu pesan dibuat (kode unix epoch time)
delivered_time	Waktu pesan sampai (kode unix epoch time)
status	Status pesan
sent_count	Jumlah penerima
read_count	Jumlah pembaca
location_name	Nama lokasi
location_address	Alamat lokasi

Nama Kolom	Arti / Fungsi
location_phone	Telepon lokasi
location_latitude	Derajat lintang lokasi
location_longitude	Derajat bujur lokasi
attachement_image	Jumlah gambar attachment
attachement_image_height	Tinggi gambar attachment
attachement_image_width	Lebar gambar attachment
attachement_image_size	Ukuran gambar attachment
attachement_type	Tipe attachment
attachement_local_uri	Lokasi file
parameter	Penggunaan Kode tambahan
chunks	Tidak diketahui

Pembuktian (WhatsApp)



	key_id	status	needs_push	data	timestamp
	Filter	Filter	Filter	Filter	Filter
1	E06D7EC8E39...	0	0	Selamat siang...	1464783300000
2	081B254E07E...	13	0	Halo mas, sal...	1464783444737
3	B99E20E30C7...	0	0	Begini mas, s...	1464783760000
4	415C60256B6...	13	0	Benarkah? Sa...	1464784363852
5	9713BA80298...	13	0	😂😂😂	1464784370980
6	E49F4609A33...	0	0	Yakin? Apaka...	1464784540000
7	CC9A130F315...	0	0	BEGIN:VCARD...	1464784553000
8	E47A0175AF0...	13	0	Ah kamu berc...	1464784738609

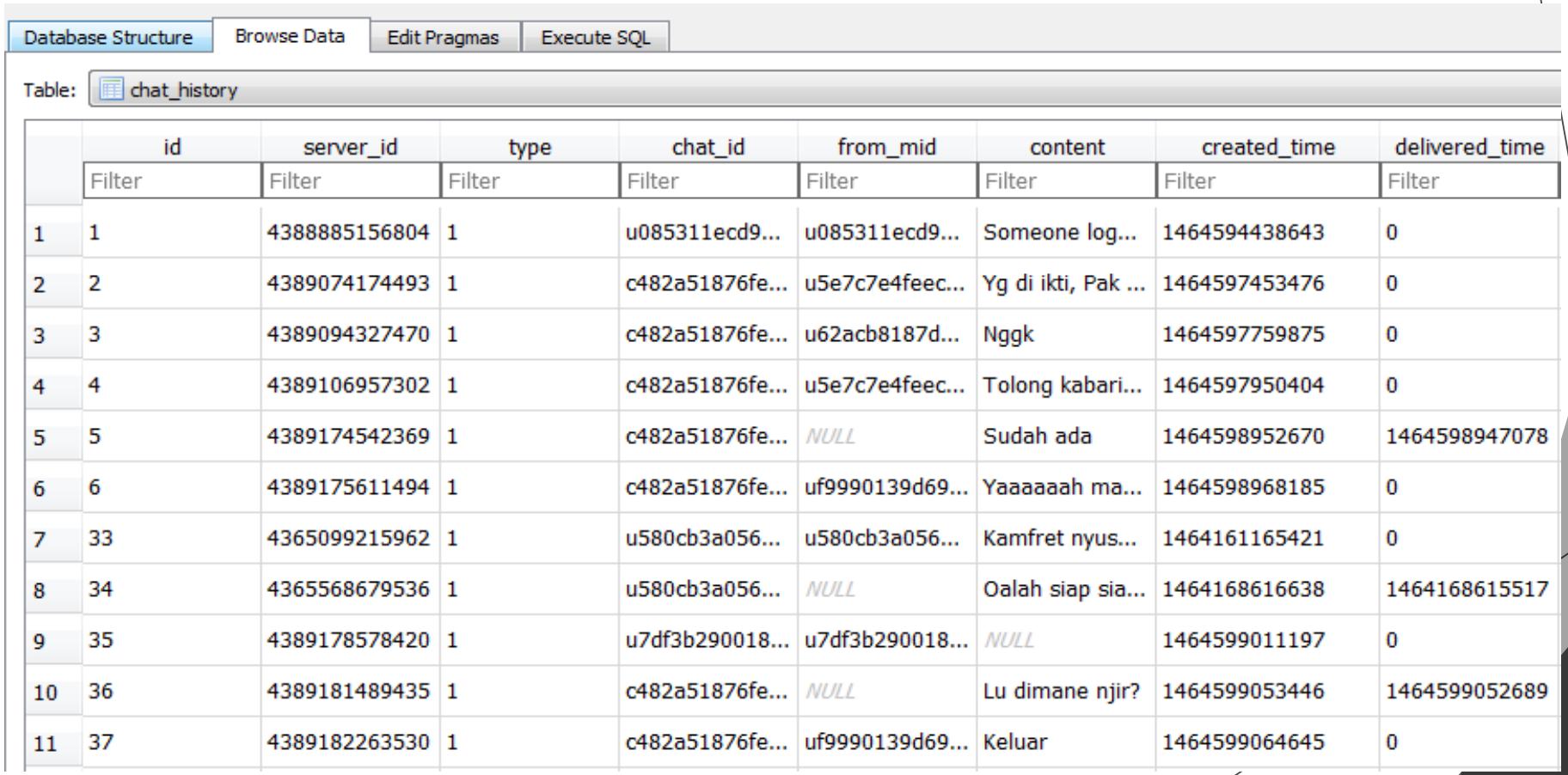
Pembuktian (WhatsApp 1)

Aktivitas Percakapan	Skenario Percakapan	Kesimpulan
"Selamat siang Korban 1, salam kenal"	Selamat siang X, salam kenal	Sama dan terbukti

Pembuktian (WhatsApp 2)

key_id Korban	key_id Tersangka	data	Kesimpulan
32E615DFDCE7419A92B9FE8F46F0CF	32E615DFDCE7419A92B9FE8F46F0CF"	"Gila kamu!"	Sama dan terbukti
"5FEC6415786EFCEE4CFABDFE0C003F	"5FEC6415786EFCEE4CFABDFE0C003F	"Bagaimana mas? Apakah saya perlu memberikan spoiler dulu ke internet agar anda lebih percaya?"	Sama dan terbukti

Pembuktian (LINE Messenger)



Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: chat_history

	id	server_id	type	chat_id	from_mid	content	created_time	delivered_time
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	4388885156804	1	u085311ecd9...	u085311ecd9...	Someone log...	1464594438643	0
2	2	4389074174493	1	c482a51876fe...	u5e7c7e4feec...	Yg di ikti, Pak ...	1464597453476	0
3	3	4389094327470	1	c482a51876fe...	u62acb8187d...	Nggk	1464597759875	0
4	4	4389106957302	1	c482a51876fe...	u5e7c7e4feec...	Tolong kabari...	1464597950404	0
5	5	4389174542369	1	c482a51876fe...	*NULL*	Sudah ada	1464598952670	1464598947078
6	6	4389175611494	1	c482a51876fe...	uf9990139d69...	Yaaaaaah ma...	1464598968185	0
7	33	4365099215962	1	u580cb3a056...	u580cb3a056...	Kamfret nyus...	1464161165421	0
8	34	4365568679536	1	u580cb3a056...	*NULL*	Oalah siap sia...	1464168616638	1464168615517
9	35	4389178578420	1	u7df3b290018...	u7df3b290018...	*NULL*	1464599011197	0
10	36	4389181489435	1	c482a51876fe...	*NULL*	Lu dimane njir?	1464599053446	1464599052689
11	37	4389182263530	1	c482a51876fe...	uf9990139d69...	Keluar	1464599064645	0

Pembuktian (LINE Messenger 1)

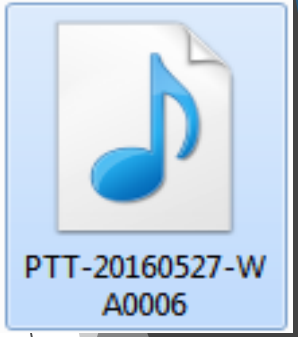
Aktivitas Percakapan	Skenario Percakapan	Kesimpulan
"Itu mas"	Itu mas	Sama dan terbukti
"Oke sebentar saya cek rekening terlebih dahulu"	Oke sebentar saya cek rekening terlebih dahulu	Sama dan terbukti

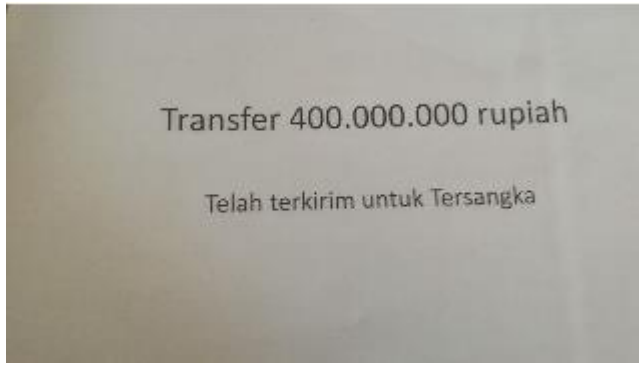
Pembuktian (LINE Messenger 2)

server_id Korban	server_id Tersangka	content	Kesimpulan
"4399811878868"	"4399811878868"	"Selamat siang Korban 1, salam kenal"	Sama dan terbukti
"4399830347799"	"4399830347799"	"Halo mas, salam kenal juga. Anda siapa ya? Ada perlu apa kalau boleh tahu?"	Sama dan terbukti

Data Pendukung

Jid	No Telepon	Peran
6285749598994@s.whatsapp.net	085749598994	Tersangka
6281218172958@s.whatsapp.net	081218172958	Korban 1
6281284467254@s.whatsapp.net	081284467254	Korban 2





Perbandingan Data Digital

Data Aplikasi

Data Perangkat

Data Eksperimen

Pembanding	WhatsApp	LINE Messenger
Folder Data Aplikasi	com.whatsapp	jp.naver.line.android
Lokasi Folder Data Aplikasi	data/data/com.whatsapp	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 file untuk semua percakapan	Satu file untuk satu percakapan
Verifikasi	Telepon	Telepon dan email
Perlindungan database	Tipe file terbuka	Tipe file disembunyikan
Database kontak	wa.db	naver_line
Tabel Kontak	wa_contacts	contacts
No Telepon	Tersedia	enkripsi
Database Percakapan	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

Perbandingan Data Digital

Data Aplikasi

Data Perangkat

Data Eksperimen

Pembanding	ASUS Zenfone 2	Samsung Galaxy S3 Mini	Emulator Bluestacks 2 Native
Proses Rooting	Bisa	Bisa	Bisa
Penarikan Data Manual	Tidak Bisa	Bisa	Tidak Bisa
Penarikan Data Menggunakan Aplikasi	Bisa	Bisa	Bisa

Perbandingan Data Digital

Data Aplikasi

Data Perangkat

Data Eksperimen

Pembanding	Eksperimen 1	Eksperimen 2	Eksperimen 3
Aktivitas Eksperimen	Aktivitas biasa	Penghapusan percakapan	Penghapusan aplikasi
Ketersediaan Data Aplikasi	Lengkap	Database percakapan terhapus	Tidak ada data aplikasi
Ketersediaan Data Pendukung	Ada	Ada	Ada

Aplikasi Rujukan

Aplikasi Rujukan Forensika Digital

Aplikasi dengan Keamanan Terbaik

BAB VII Kesimpulan dan Saran

Kesimpulan

- Bukti digital pada aplikasi WhatsApp dan LINE *Messenger* **BERHASIL** didapatkan dari perangkat Android dengan menggunakan dua cara, yaitu cara manual dan menggunakan aplikasi tambahan.
- Data yang dapat diambil merupakan **DATA UTAMA DAN DATA PENDUKUNG APLIKASI**.
- WhatsApp dan LINE *Messenger* memiliki karakteristik masing-masing sehingga data yang didapatkan juga berbeda **BERGANTUNG BAGAIMANA STRUKTUR DATA YANG DISUSUN** pada database aplikasi.
- Faktor yang mempengaruhi keberhasilan mendapatkan bukti digital pada aplikasi WhatsApp dan LINE *Messenger* adalah **AKTIVITAS PENGGUNAAN APLIKASI, PERANGKAT YANG DIGUNAKAN, SERTA APLIKASI UNTUK ANALISA FORENSIK YANG DIGUNAKAN**.
- **WhatsApp** merupakan aplikasi pengolah pesan yang menjadi **RUJUKAN DALAM FORENSIKA DIGITAL** di Indonesia .Sedangkan untuk **LINE *Messenger*** menjadi aplikasi pengolah pesan yang **PENUH TANTANGAN** untuk dilakukan proses analisa forensika digital di Indonesia

Saran

- Dibutuhkan adanya standar baku untuk proses forensika digital yang ada di Indonesia serta formulir untuk dokumentasi
- Untuk pelaksanaan forensika digital pada perangkat *mobile* dibutuhkan perangkat akuisisi data secara manual semacam Cellebrite atau GPG JTAG

End of The Presentation

Terima kasih ☺

Benda yang tersisa kecuali yang tidak ada, semuanya tak bisa dipercaya

Shinichi Kudo