Analisa Perbandingan Tools Ekstraktor Whatsapp Database Crypt12 Menggunakan Metoda Logical Extraction

Zulkarnaen Akbar, Iwan Krisnadi

Universitas Mercubuana, Jakarta
zoel.akbar.id@gmail.com; iwankrisnadi@yahoo.com

Abstrak

Dengan lebih dari 1000 juta pengguna aktif berdasarkan survey 2017 perkembangan ini semakin meningkat setiap tahunnya. Perlu diketahui bahwa WhatsApp mempunyai suatu tabel database yang tersimpan secara rasahsia didalam sistem sistem Android yang selalu update secara realtime. Database ini selau dicadangkan secara otomatis melalui fitur autobackup yang tersimpan berbeda dengan database utama. Database hasil backup ini mempunyai format file .crypt12. File crypt12 ini tidak dapat diakses secara sembarang karena telah dienkripsi oleh apliksi ini.

Beberapa penelitian telah banyak membahas tentang WhatsApp forensics diperangkat android dengan menggunakan beberapa medode salah satunya adalah metode "logical Extraction".

Dalam melakukan uji coba forensics muncul permasalahan ketika akan dilakukan uji forensics pengguna aplikasi telah menghapus percakapan yang telah dilakukan ini bertujuan untuk menghilangkan jajak dari pengguna WhatsApp. Didalam kasus ini sebenarnya kita dapat melihat percakapan yang telah dihapus dengan melihat data crypt12 dari WhatsApp dengan cara mendeskripsikan data base tersebut. Ada beberapa tools untuk mendeskripsikan file crypt12. Pada penelitian ini akan membandingkan tools untuk mendeskripsikan file data base WhatsApp. Hasil penelitian menghasilkan dalam menganalisa uji forensics tidak lah cukup hanya mengandalkan tools yang dibandingkan akan tetapi harus melihat database hasil deskripsi. File crypt12 (database backup) dan file asli dalam system pada dasarnya mempunyai isi yang sama, akan tetapi terjadi perbadaan dikarenakan dalam proses backup tidak lah update karena WhatsApp hanya akan membackup setian 24 jam sekali.

***Keywords**: Forensics, Digital Forensics, Mobile Forensics, Android Forensics, WhatsApp Forensics, Foreniscs Tools, Instant Messaging.*

Received May 2017
Accepted for Publication September 2017
DOI: 10.22441/incomtech.v8i1.2144

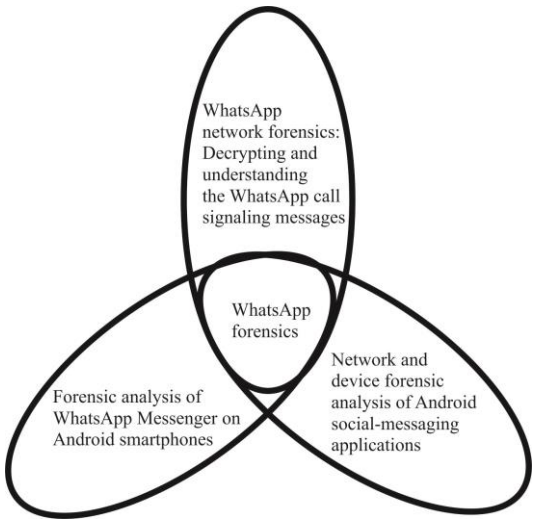
1. PENDAHULUAN

WhatsApp kini menjadi salah satu aplikasi pesan instan paling popular [1][2]. Namun, basis pengguna yang luas juga membuat aplikasi ini rentan terhadap serangan hacker serta sejumlah risiko keamanan lainnya. WhatsApp dengan fitur chat grup yang banyak dimanfaatkan banyak orang baik untuk kepentingan komunitas kecil seperti keluarga samapai kepada komunitas perusahaan untuk memudahkan pekerjan karyawan. WhatsApp kembali menghadirkan fitur terbaru. Mulai dari fitur bisa mengurim video, dokumen, bahkan voice yang memungkinkan sesorang user dapat berbebicara dengan melalui menggunakan data selular.

WhatsApp mempunyai suatu tabel database yang tersimpan secara rahasia didalam sistem sistem Android yang selalu update [2]. Database ini selau dicadangkan secara otomatis melalui fitur autobackup yang tersimpan berbeda dengan database utama. Database hasil backup ini mempunyai format file .crypt12. File crypt12 ini tidak dapat diakses secara sembarang karena telah dienkripsi oleh apliksi ini. Permasalahan yang pasti muncul ketika akan dilakukan uji forensics tetapi data utama telah dihapus oleh pengguna aplikasi ini untuk menyembunyikan jejak dengan cara menghapus secara permanen semua percakapan di WhatsApp. Didalam kasus ini sebenarnya kita dapat melihat percakapan yang telah dihapus dengan melihat data crypt12 dari WhatsApp dengan cara mendeskripsikan database tersebut.

Dalam dunia digital forensic banyak tools untuk memudahkan dalam melakukan investigasi. Salah satu tools yang dapat digunakan dalam dunia forensics kali linux dengan dengan beberapa tools yang ada dilamamnya akan memudahkan dalam melakum infestigasi. Penulis manggunakan Andriller, WhatsApp Vewer dan Whatcrypt karena dalam menggunakan sangatlah mudah.

Dalam dewasa ini kegiatan mobile foresics cukup banyak menarik perhatian di kalangan intelektual karena dengan kemajuan teknologi semakin banyak berkembang dan banyaknya kasus krimial yang melibatkan smartphone sebagai alat barang bukti. Gambar 1adalah beberapa penelitian yang menjadi rujukan di penelitian yang melibakan mobile forensics.



Gambar 1 Relasi penelitian terhadap penelitian pendukung.

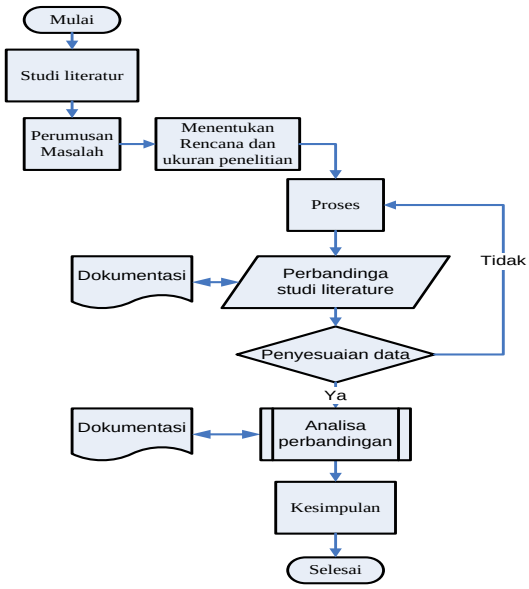
Penelitian yang dilakukan oleh F. Karpisek, I. Baggli, F. Breitinger (2015) dengan judul "WhatsApp network forensics: Decrypting and understanding the WhatsApp call signaling messages menggunakan metoda Internet Protocol forensics berhasil mendekripsi lalu lintas jaringan dan memperoleh artefak forensik yang berhubungan dengan fitur baru yaitu panggilan WhatsApp dan menangkap nomor telepon WhatsApp, IP WhatsApp Server, WhatsApp codec audio (Opus) , durasi WhatsApp panggilan, dan panggilan WhatsApp ini termination. Dalam penelitian ini menjelaskan metode dan alat yang digunakan untuk mendekripsi lalu lintas serta menyeluruh menguraikan temuan yang berhubungan pesan sinyal WhatsApp [5].

Penelitian yang dilakukan oleh Cosimo Anglano (2014) yang berjudul "Forensic analysis of WhatsApp Messenger on Android smartphones" dengan menggunakan metoda Logical Extraction berhasil menghasilkan artefak dari seluruh informasi didalam WhatsApp mulai dari pesan, backup, log file, kontak, avatar, dsb. Dan menganalisa dari detail kontak dan grup WhatsApp dengan melihat log WhatsApp [3].

Penelitian yang dilakukan Daniel Walnycky, Ibrahim Baggili, Andrew Marrington, Jason Moore, Frank Breitinger 2015 yang berjudul "Network and device forensic analysis of Android social-messaging applications" dengan menggunakan metoda Logical Extraction telah mengahasilkan beberapa analisa pesan messeging dengan merekuntuksi password, screenshot diambil oleh aplikasi, gambar, video, audio dikirim, pesan yang dikirim, sketsa, gambar profil dan banyak lagi, dan berhasil dengan mengkonpare 20 aplikasi jejaring sosial termasuk WhatsApp [6].

2. METODOLOGI PENELITIAN

Metodologi penelitian yang digunakan dengan membandingkan jurnal-jurnal terkait yang melakukan penelitian forensics pada whatsapp. Pada penelitian ini dibahas tentang beberapa metoda dalam mobile forensics pada aplikasi whatsapp.



Gambar 2 Flowchart Metoda Penelitian.

Di tabel 1 ditampilkan metode Manual Extraction sehingga diperoleh berbagai macam hasil dari penelusuran uji forenics dalam suatu perangkat smartphone android.

Tabel 1 WhatsApp messengger database

Content	Directory	File
Contacts database	/data/data/com.WhatsApp/database	wa.db
Chat database	/data/data/com.WhatsApp/database	msgstore.db
Backups of the chat database	/databases/storage/emulated/WhatsApp	msgstore-yyyy-mm-dd.x.db.cypt12
Avatar of contacts	/data/data/com.WhatsApp/file/avatar	<contacnumber>@s.WhatsApp.net.j
Copies of contacts avatar	/databases/storage/emulated/WhatsApp	<contacnumber>@s.WhatsApp.net.j
Log files	/data/data/com.WhatsApp/file/logs	WhatsApp.log
Recived files	/databases/storage/emulated/WhatsApp/media/ <WhatsApp xxx>	<media name>
Sent files	/databases/storage/emulated/WhatsApp/ <WhatsApp xxx>/media/send	<media name>
User settings and preferences	/databases/storage/emulated/WhatsApp	Me
Status	/databases/storage/emulated/WhatsApp/media/ .statuse	<status name>

3. DATABASE CRYPT12 DAN TOOLS EKSTRAKTOR DATABASE CRYPT12

Di dalam sub bab akan dibahas hasil penelitian WhatsApp forensics dari tools yang telah dipilih WhatsApp forensics diantaranya yaitu Andriller, Whasapp viewer dan whatcrypt. ketiga aplikasi ini merupakan beberapa tools yang bisa digunakan untuk melakukan WhatsApp forensics dengan karakter forensics yang berbeda-beda. Dalam penelitian ini WhatsApp yang digunakan adalah WhatsApp versi terbaru yang sudah menggunakan database crypt12.

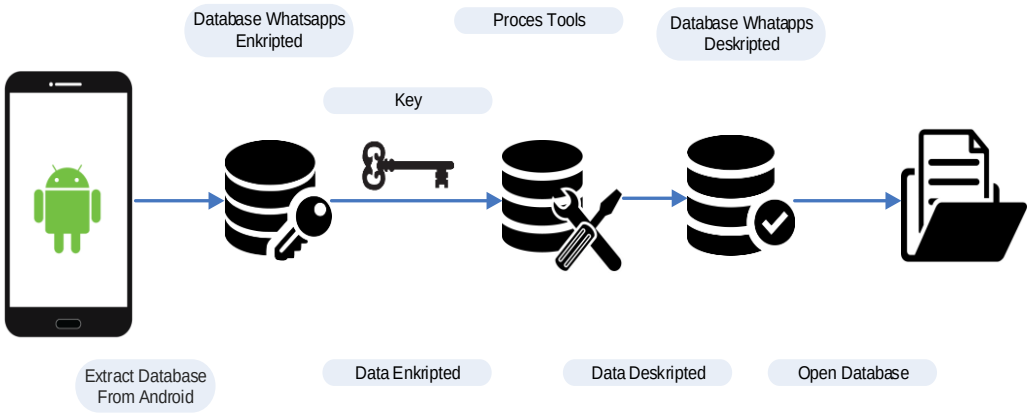
Dalam pengambilan database dalam aplikasi WhatsApp terdiri dari sebagai berikut :

1. Crypt12 merupakan format data yang terenkrip oleh aplikasi WhatsApp, file ini jika di deskripsi terdiri dari history chaing, panggilan suara, dan panggilan video. Cypt12 merukan versi terbaru dari file database WhatsApp yang diklaim merupakan database paling aman yang telah memiliki fitur end to end enkription.
2. Key ini merupakan file kunci untuk mendeskrip file crypt12. Untuk mengakses file ini membutuhkan akses root. Untuk ponsel android yang belum diroot tidak dapat mengakses file ini.

Tabel 2 Lokasi file Crypt12 dan key

Nama File	Lokasi File
crypt12	*/sdcard/WhatsApp/Database/msgstore.db.crypt12*
key	*/data/data/com.whatsapp/file/key*

File database .crypt12 yang sudah di download atau dicopy dari mobile android ke komputer PC tidak bisa lansung dibuka begitu saja dengan menggunakan aplikasi pembuka file database seperti SQLite, karena file tersebut telah terenkripsi dengan sangat baik. Salah satu tools untuk mendeskripsi file tersebut ialah aplisksi benama Andriller, WhatsApp Viewer dan Whatcrypt. Kami menggunakan aplikasi Andriller, WhatsApp Viewer dan Whatcrypt karena dapat mengekstrak atau merubah file database.crypt12 menjadi file format .db agar bisa dibuka didalam aplikasi SQLite. Gambar 3 menampilkan konsep secara umum kerja dari tools forensics.



Gambar 3 Konsep Secar Umum Tools WhatsApp Forensics.

3.1 Percobaan dengan menggunakan Andriller

Tools ini dapat menampikan hasil dari uji forensics. Hasil yang dapat ditampilkan menggunakan aplikasi ini yaitu history panggilan telepon dan komunikasi chating.

This report was generated using Andriller # (This field is editable in Preferences)

[WhatsApp Calls]

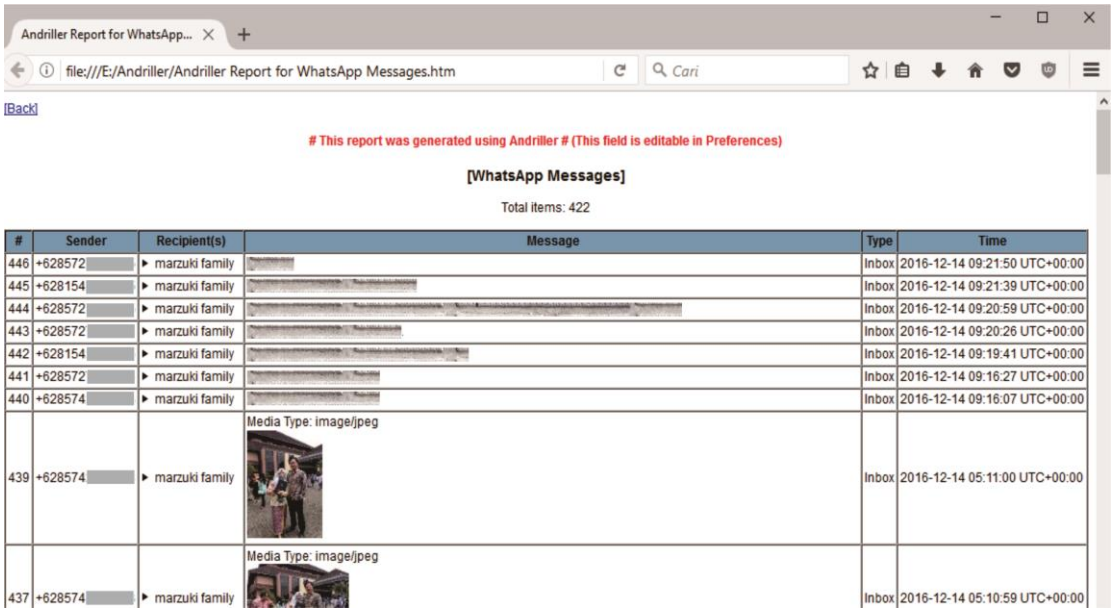
Total items: 10

#	Type	Number	Time	Duration
301	Dialled	+6281219704425	2016-12-10 10:45:28 UTC+00:00	0:00:00
113	Dialled	+6287736371766	2016-12-04 14:25:05 UTC+00:00	0:00:00
98	Dialled	+6285729879969	2016-12-03 03:47:04 UTC+00:00	0:00:55
90	Missed	+6285727443095	2016-11-29 15:48:04 UTC+00:00	0:00:00
73	Missed	+6285727443095	2016-11-28 02:30:23 UTC+00:00	0:00:00
71	Missed	+6285727443095	2016-11-28 02:29:40 UTC+00:00	0:00:00
70	Missed	+6285727443095	2016-11-28 02:29:11 UTC+00:00	0:00:00
69	Dialled	+6285727443095	2016-11-28 01:59:12 UTC+00:00	0:00:00
14	Dialled	+6285729879969	2016-11-21 00:17:07 UTC+00:00	0:08:31
3	Dialled	+6285727443095	2016-11-20 15:21:53 UTC+00:00	0:00:00

 # andriller.com # (This field is editable in Preferences)

Gambar 4 Forensics WhatsApp call

Dari hasil uji coba forensics dengan menggunakan Andriller memiliki beberapa kelebihan salah satunya yaitu dapat menampikan semua history baik history chating secara detail dan history log panggilan yang cukup detail dengan informasi yang didapatkan kita sebagai ahli forensics dapat membuat laporan secara detail dengan melihat dari output yang dikeluarkan oleh aplikasi ini. Namun, untuk dapat memiliki applikasi Andriller secara pemanen kita diharuskan membeli lisensinya terlebih dahulu ini merupakan salah satu kekurangan dari tools ini. Di tabel 3 ditunjukkan fitur dari Andriller.



Gambar 5 Forensics WhatsApp Messages

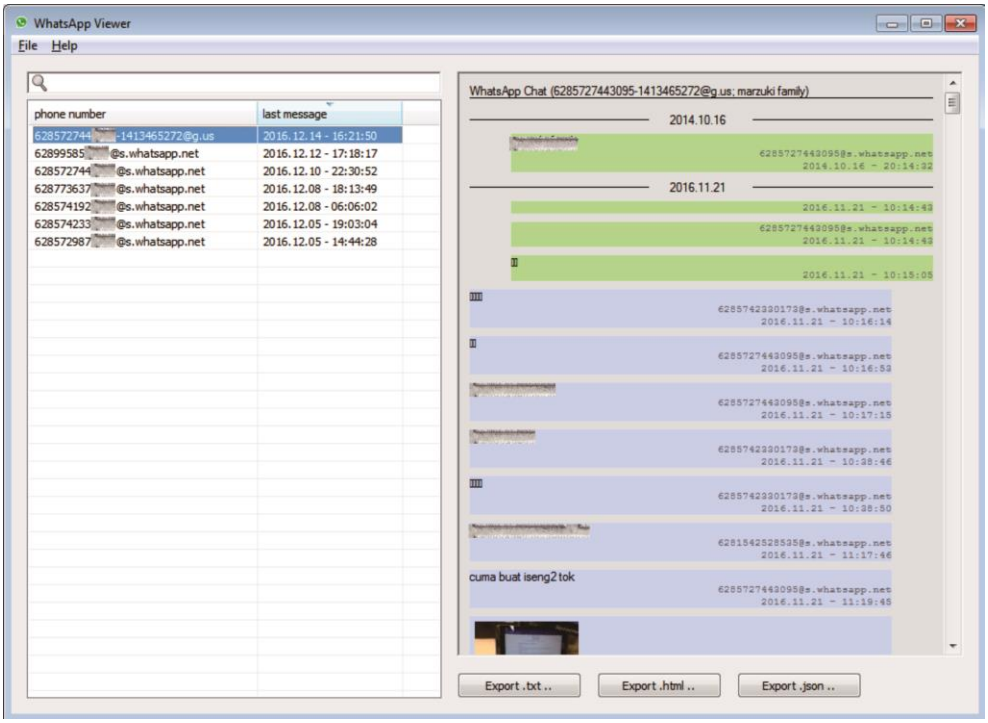
Tabel 3 Fitur Andriller

Fitur Tools	**Keterangan**
OS Suport	Windows
Koneksi Internet	Tidak
Status Penggunaan	Berbayar (free 30 hari)
Log Chating	Ya
Log Panggilan	Ya

3.2 Uji Forensics dengan menggunakan tools *WhatsApp Viewer*

Tools ini dapat menampikan hasil dari uji forensics. Hasil yang dapat ditampilkan menggunakan aplikasi ini yaitu hanya komunikasi chating saja, tetapi tools ini dapat mengubah database menjadi file dengan .html, .txt dan .json.

Dari percobaan dari uji forensics menggunakan tools Whatsapp Viewer memiliki kelebihannya ialah kita dapat melihat percakapan chating saja dan memiliki tampilan yang lebih menarik untuk dibaca dan dipelajari sedangkan untuk log panggilan kita tidak dapat melihatnya ini merupakan salah satu kekurangan dari tools ini. Tabel 4 merupakan kesimpulan dari percobaan yang telah dilakukan menggunakan tools WhatsApp Viewer.



Gambar 6 Hasil dari uji forenics menggunakan tools WhatsApp viewer

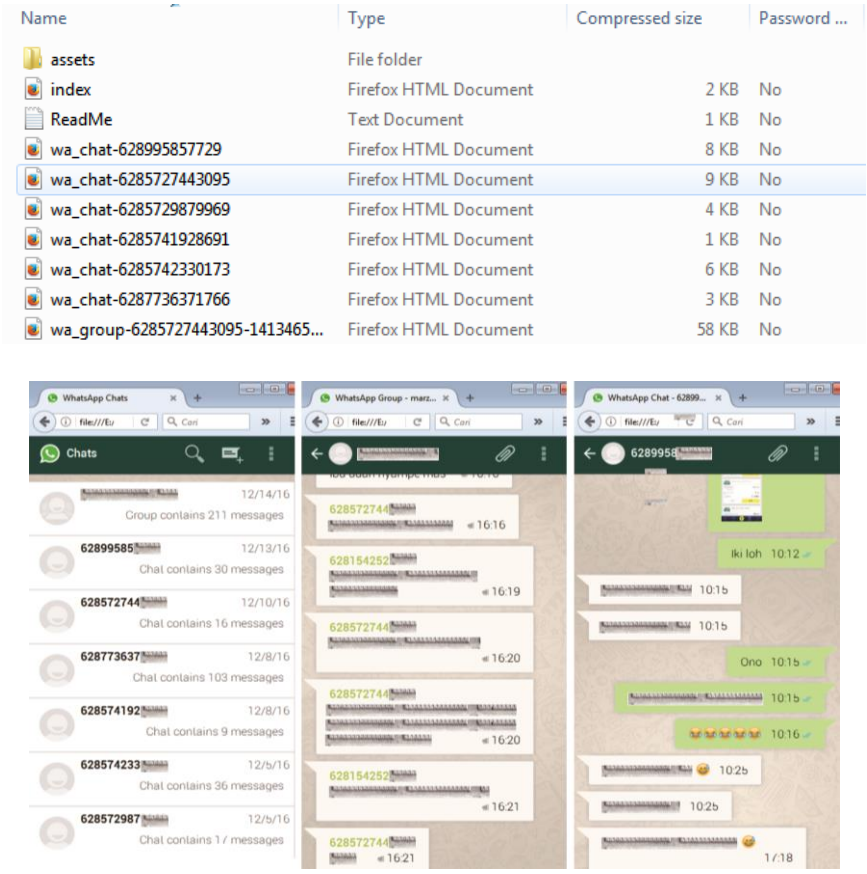
Tabel 4 Fitur WhatsApp Viewer

Fitur Tools	**Keterangan**
OS Suport	Windows
Koneksi Internet	Tidak
Status Penggunaan	Gratis
Log Chating	Ya
Log Panggilan	Tidak

3.3 Uji Forensics dengan menggunakan tool *Whatcrypt*

Tools ini dapat menampikan hasil dari uji forensics. Hasil yang dapat ditampilkan menggunakan aplikasi ini yaitu hanya komunikasi chating saja dengan format html.

Setelah dilakukan uji forensics dengan menggunakan tools whatcrypt dapat disimpulkan bahwa tools ini memiliki tampilan yang hampir mirip dengan tampilan didalam smartphone mulai dari list chating sampai dengan detail chating, setelah kita memiliki file hasil dari deskripsi crypt12 kita juga dapat menenkripsi kembali kedalam file dengan format crypt ini merupakan kelebihan dari tools ini. Namun, sama dengan tools WhatsApp viewer tools ini juga tidak menampilkan log komunikasi telepon selain itu untuk menggunakan tools ini kita memerlukan koneksi internet karena tools ini merupakan tools yang berbasis webs ini merupakan kekurangan dari tools whatcrypt.



Gambar 7 Hasil dari uji forenics menggunakan tools Whatcrypt

Tabel 4 Fitur WhatsApp Viewer

Fitur Tools	**Keterangan**
OS Suport	All OS (berbasis Web)
Koneksi Internet	Ya
Status Penggunaan	Gratis
Log Chating	Ya
Log Panggilan	Tidak

Tabel 5 adalah informasi yang didapatkan setelah melakukan percobaan dari masing - masing tools setelah dilakukan pengujian

Tabel 4 Fitur WhatsApp Viewer

Tools	**OS Suport**	**Koneksi Internet**	**Status Penggunaan**	**Informasi**	
				Log Chating	**Log Panggilan**
Andriller	Windows	Tidak	Berbayar	Ya	Ya
WhatsApp Viewer	Windows	Tidak	Gratis	Ya	Tidak
Whatcrypt	All OS (Web)	Ya	Gratis	Ya	Tidak

Dari Tabel diatas dapat kita melihat bahwa setiap tools memiliki kelebihan dan kekurangan diatara salah satunya adalah ada tools yang dapat menampilkan informasi log panggilan ada yang tidak. Sebenernya dalam melakukan uji forensics selain kita menganalisa dari sisi output yang dihasilkan oleh tools tetapi

kita juga harus melihat dari sisi file yang dihasilkan yaitu file database berformat (.db). dengan kita melihat file tersebut dengan menggunakan aplikasi SQLite kita dapat mengetahui secara detail seluruh informasi yang kita perlukan.

Setelah file hasil dari uji forensics mendeskripsikan file crypt12 menggunakan tools yang digunakan dibuka menggunakan SQLite file tersebut mempunyai struktur tabel dan isi yang sama persis yaitu terdiri dari 16 table, 12 indices, dan 4 triger dengan penjabaran detail sebagai berikut. Struktur ini pun setelah dibandingkan dengan tabel utama disistem mempunyai karakteristik yang sama persis, karena crypt12 yang sudah dideskripsi ialah file yang dari sistem yang kemudian dienkripsi dan menjadi file yang mempunyai format baru yaitu crypt12. Hanya saja untuk isi antara file sistem dan file crypt12 mempunyai isi yang berbeda perbedaan ini akan dijelaskan disub bab selanjutnya mengenai analisa database deskripsi .crypt12 WhatsApp messenger.

Tabel 5

Tabel	***Indices***	***Triger***
chat_list	*grup_participants_history_index*	*messages_bd_for_links_trigger*
Frequents	*grup_participants_index*	*messages_bd_for_quotes_trigger*
grup_participants	*media_hash_index*	*messages_bd_for_receipts_trigger*
grup_participants_history	*media_type_index*	*messages_bs_triger*
media_refs	*media_type_jid_index*	
media_streaming_sidecar	*messages_key_index*	
messages	*receipts_key_index*	
messages_fts (table virtual)	*sqlite_autoindex_chat_list_1*	
messages_fts_content	*sqlite_autoindex_media_refs_1*	
messages_fts_segdir	*sqlite_autoindex_messages_fts_segdir_1*	
messages_fts_segments	*sqlite_autoindex_props_1*	
messages_links	*starred_index*	
messages_quotes		
props		
receipts		
sqlite_sequesnce		

Informasi di atas adalah beberapa tabel, indices dan trigger yang menyusun WhatsApp. Table adalah komponen yang menyusun dan mengisi dari seluruh informasi yang ditampilkan di aplikasi WhatsApp. Sedangan Indices adalah indeks pencarian ketika kita akan mencari suatu kata. Indeks disini dikelompokan berdarkan kata kunci yang ditampilkan dikolom pencarian. Triger adalah sebuah program kecil yang berjalan terus menerus berguna untuk menerima pesan yang masuk atau pun mengirim pesan ketika mengirim pesan yang kemudian program ini langsung mencatatnya kedalam beberapa tabel di atas.

4. ANALISA DATABASE DESKRIPSI .CRYPT12 WHATSAPP MESSENGGER

Tabel hasil dari deskripsi dari file crypt12 tidak lah jauh berberda dengan file msgstore.db yang ada di /data/data/com.WhatsApp/database karena file crypt12

merupakan backup dari database tersebut. Tabel penyusun aplikasi WhatsApp messager sebagai berikut.

Chatlist

Field file	Type file	Deskription
_id	*integer*	*primary key*
key_remote_jid	*Text*	
Subject	*integer*	
Creation	*Text*	
last_read_message_table_id	*integer*	
last_read_receipt_sent_massage_table_id	*integer*	
Arciveed	*integer*	
sort_timestamp	*integer*	
mod_tag	*integer*	
Gen	*real*	
my_massages	*integer*	
plaintext_disabled	*boolean*	
last_message_table_id	*integer*	
unseen_massage	*integer*	
unseen_missed_call_count	*integer*	
unseen_roow_count	*Integer*	

Frequents

Field file	Type file	Deskription
_id	*integer*	*primary key*
Jid	*Text*	
Type	*Integer*	
Message_count	*Integer*	

Grup_participants

Field file	Type file	Deskription
_id	*integer*	*primary key*
Gjid	*Text*	
Jid	*Text*	
admin	*integer*	
pending	*integer*	
sent_sender_key	*integer*	

Grup_participants_history

Field file	Type file	Deskription
_id	*integer*	*primary key*
timestamp	*datetime*	
Gjid	*Text*	
Jid	*Text*	
action	*integer*	
old_phash	*text*	
new_phash	*text*	

Media_refs

Field file	Type file	Deskription
_id	*integer*	*primary key*
Path	*Text*	
Ref_cont	*Integer*	

Media_streaming_sidecar

Field file	Type file	Deskription
_id	*integer*	*primary key*
sidecar	*blob*	
key_remote_jid	*text*	
key_from_me	*integer*	
key_id	*text*	

Messages

Field file	Type file	Deskription
_id	*integer*	*primary key*
key_remote_jid	*text*	
key_from_me	*integer*	
key_id	*text*	
status	*integer*	
needs_push	*integer*	
data	*text*	
timestamp	*integer*	
media_url	*text*	
media_mine_type	*text*	
media_wa_type	*text*	
media_size	*integer*	
media_name	*text*	
media_caption	*text*	
media_hash	*text*	
media_duration	*integer*	
origin	*integer*	
latidute	*real*	
thumb_image	*text*	
remote_resource	*text*	
recieved_timestamp	*integer*	
send_timestamp	*integer*	
receipt_server_timestamp	*integer*	
receipt_device_timestamp	*integer*	
read_device_timestamp	*integer*	
raw_data	*blob*	
recipient_count	*integer*	
participant_hash	*text*	
starred	*integer*	
quoted_row_id	*integer*	
mentioned_jids	*text*	

multicast	*text*

Messages_fts (table virtual)

Messages_fts_content

Field file	**Type file**	**Deskription**
docid	*integer*	*primary key*
c_content	*text*	

Messages_fts_segdir

Field file	**Type file**	**Deskription**
level	*integer*	*primary key*
idx	*integer*	*foureig key*
start_block	*integer*	
leaves_end_block	*integer*	
end_block	*integer*	
root	*blob*	

Messages_fts_segments

Field file	**Type file**	**Deskription**
Blockid	*integer*	*primary key*
Block	*Blob*	

Messages_links

Field file	**Type file**	**Deskription**
_id	*integer*	*primary key*
Key_remote_jid	*Text*	
Massage_row	*integer*	
Link_index	*integer*	

Messages_quotes

Field file	**Type file**	**Deskription**
_id	*integer*	*primary key*
key_remote_jid	*text*	
key_from_me	*integer*	
key_id	*text*	
ststus	*integer*	
needs_push	*integer*	
media_url	*text*	
media_mime_type	*text*	
media_wa_type	*text*	
media_size	*integer*	
media_name	*text*	
media_caption	*text*	
media_hash	*text*	
media_duration	*integer*	
origin	*integer*	
latitude	*real*	

longitude	*real*
thumb_image	*text*
remote_resource	*text*
received_timestamp	*integer*
send_timestamp	*integer*
receipt_server_timestamp	*integer*
receipt_device_timestamp	*integer*
read_device_temestamp	*integer*
played_device_timestamp	*integer*
raw_data	*blob*
recipent_count	*integer*
participant_hash	*text*
starred	*integer*
quoted_row_id	*integer*
mentioned_jids	*text*
multicast_id	*text*

Props

Field file	**Type file**	**Deskription**
_id	*integer*	*primary key*
key	*text*	
value	*text*	

Receipts

Field file	**Type file**	**Deskription**
_id	*integer*	*primary key*
key_remote_jid	*text*	
key_id	*text*	
remote_resource	*text*	
receipt_device_timestamp	*integer*	
read_device_timestamp	*integer*	
played_device_timestamp	*integer*	

Sqlite_sequesnce

Field file	**Type file**	**Deskription**
Name	*Text*	
Seq	*Text*	

Indices yang menyusunan aplikasi WhatsApp messager sebagai berikut

grup_participants_history_index	*Gjid*
grup_participants_index	*gjid, jid*
media_hash_index	*media_hash*
media_type_index	*media_wa_type*
media_type_jid_index	*key_remote_jid, media_wa_type*
messages_key_index	*(unique) key_remote_jid, key_from_me, key_id*
receipts_key_index	*key_remote_jid, key_id*
sqlite_autoindex_chat_list_1	
sqlite_autoindex_media_refs_1	
sqlite_autoindex_messages_fts_segdir_1	
sqlite_autoindex_props_1	

starred_index	*Starred*

Triger penyusun dalam aplikasi WhatsApp messager sebagai berikut

messages_bd_for_links_trigger
messages_bd_for_quotes_trigger
messages_bd_for_receipts_trigger
messages_bs_triger

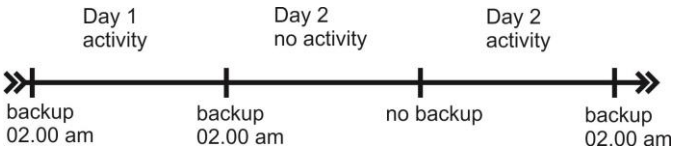
Setelah dilakukan percobaan dengan metode live memory [7] yaitu dengan skenario komunikasi yang berbeda dengan parameter yang berbeda-beda dan dilakukan secara berkala dengan melihat tingkah laku dengan membandingkan antara tabel dari sistem dan lamanya waktu dalam membackup dihasilkan hasil sebagai berikut.

Tabel 6 Hasil Riset perbandingan data sistem dengan data Backup

Pengujian	Lokasi perubahan tabel	Backup time	
		Sistem	Backup
Mengirim pesan	chat_list, frequents, massages, massages_fts, massages_fts_content, sqlite_sequence	Up to date	2.00 am
Menerima Pesan	chat_list, massages, massages_fts, massages_fts_content, massages_fts_segdir, sqlite_sequence		
Mengirim link	chat_list, frequents, massages, massages_fts, massages_fts_content, massages_link, sqlite_sequence		
Menerima link	chat_list, frequence, massages, massages_fts, massages_fts_content, massages_link, sqlite_sequence		
Mngirim Pesan Multimedia	chat_list, frequents, massages, massages_fts, massages_fts_content, sqlite_squence		
Menerima pesan multimedia	chat_list, massages, massages_fts, massages_fts_content, massages_fts_segdir, sqlite_squence		
Panggilan Voip	massages, sqlite_sequence		
Menerima Panggilan Voip	massages, sqlite_sequence		
Panggilan Vidio	massages, sqlite_sequence		
Penerima Panggulan Vidio	massages, sqlite_sequence		

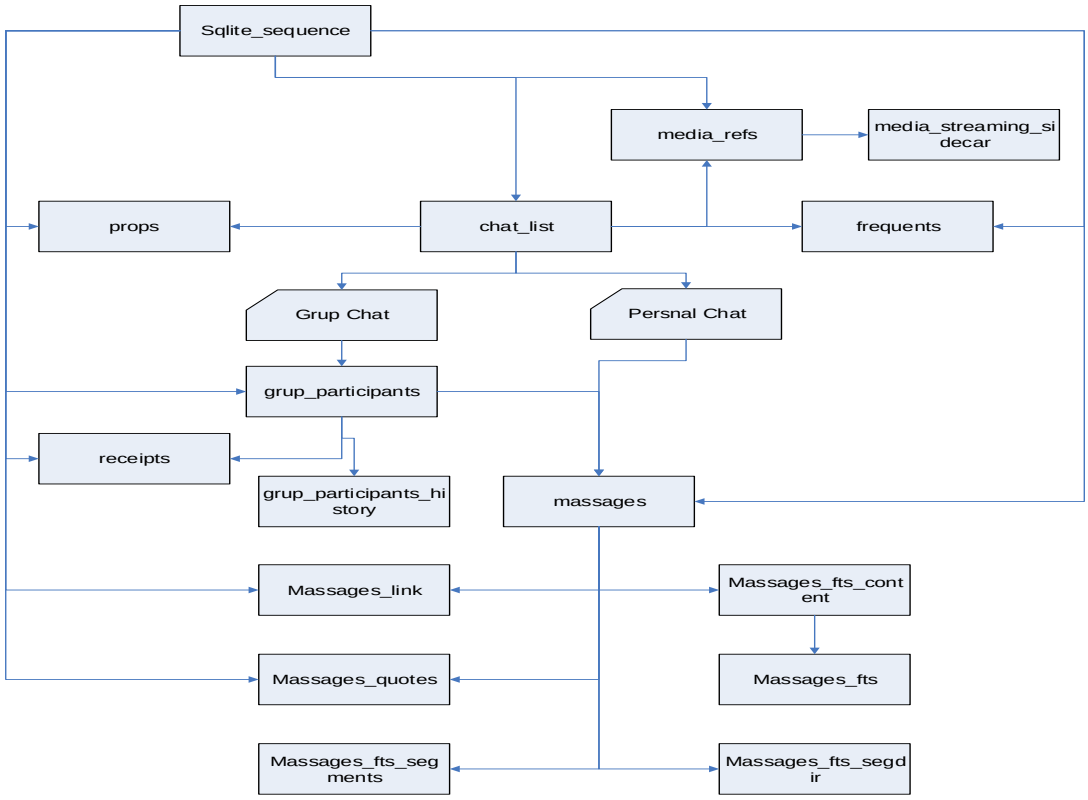
Dilihat dari timeline WhatsApp akan melakukan backup data ketika dihari tersebut ada aktifitas baik menerima atau mengirim pesan dan data yang terbackup adalah seluruh data yang ada didalam file data sistem. Ketika dalam suatu hari dimana aplikasi tersebut tidak ada aktifitas baik menerima atau mengirim pesan maka WhatsApp tidak akan melakukan membackup. Dari tabel dihasilkan waktu dalam membackup database yaitu pukul 02.00 am ini bisa menyebabkan perbedaan yang sangat berbeda antara file database backup dengan file database yang ada dalam sistem. Karena file yang ada dalam sistem selalu update secara real time sesuai dengan perubahan dari pesan yang diterima atau

pesan yang masuk sedangkan file database hanya akan berubah ketika WhatsApp melakukan aktifitas backup saja.



Gambar 8 Timeline backup WhatsApp

Dari tabel terdapat perubahan antar tabel untuk analisa dari file database dapat digambarkan sebagai berikut.



Gambar 9 Konektifitas antar tabel WhatsApp messaging

Setiap tabel mempunyai primary key yang bertujuan untuk menjadi kunci yang menghubungkan dari satu tabel ketabel yang lain. Hubungan ini sangat penting untuk membentuk suatu aplikasi messengger yang berfungsi mengisi detail dari aplikasi WhatsApp messengger.

Pada gambar terdapat beberapa tabel yang mewakili dari tabel-tabel seperti tabel sqlite_sequence yang mempunyai isi sebagai berikut.

1. massages : Tabel massages merupakan detail dari semua pesan, dalam tabel ini berisikan semua pesan yang dikirim maupun diterima baik pesan dari grup maupun personal.

2. props : Tabel props merupakan detail dari beberapa isi dari pesan bisa disebut pula tabel ini merupakan konter dari media yang diterima baik itu pesan, link, dsb.
3. chat_list : Tabel chat_list merupakan list dari percakapan baik percakapan grup chating maupun personal chating.
4. frequents : Tabel frequents merupakan konter dari frekuensi banyaknya pesan yang dikirim maupun yang diterima dan akan teriset setiap harinya.
5. grup_participants : Tabel grup_participants merupakan tabel yang berisikan detail list grup, anggota grup, admin grup dsb.
6. receipts : tabel receipts merupakan tabel yang berisikan key_id dari percakapan grup chating.
7. massages_quotes : Tabel massages_quotes berisikan qoites dari semua percakapan baik grup chating maupun personal chating.
8. massages_link : Tabel massages_link meruapakan isi dari link yang dikirim dari grup chating.

Untuk tabel chat sendiri mempunyai beberpa konektifitas kebeberapa tabel digambarkan sebagai berikut.

1. media_fts : Tabel media_refs merupakan konter dari media yang dikirim maupun yang diterima oleh perangkat WhatsApp.
2. frequents : Tabel frequents merupakan konter dari frekuensi banyaknya pesan yang dikirim maupun yang diterima dan akan teriset setiap harinya.
3. props : Tabel props merupakan detail dari beberapa isi dari pesan bisa disebut pula tabel ini merupakan konter dari media yang diterima baik itu pesan, link, dsb.
4. massages : Tabel massages merupakan detail dari semua pesan, dalam tabel ini berisikan semua pesan yang dikirim maupun diterima baik pesan dari grup maupun personal.
5. grup_participan : Tabel grup_participants merupakan tabel yang berisikan detail list grup, anggota grup, admin grup dsb.

Dari keterangan diatas dapat dilihat beberapa tabel yang mewakili konter dari pesan yang dikirim dan diterima dari aplikasi whastapp. Konter tersebut dibagi-bagi oleh developer WhatsApp sesuai dengan kriteria atau kelompoknya masing-masing. Untuk tabel media_fts mempunyai turunan tabel sendiri yaitu media_streaming_sidecar. Tabel media_streaming_sidecar berisikan mengenai media streaming seperti video call, telepon voip. Khusus untuk tabel Grup mempunyai tabel tersendiri yaitu grup_participants yang mempunyai turunan tabel sebagai berikut :

1. grup_participants_hitory : Tabel grup_participants_history merupakan tabel yang berisikan list anggota grup sesuai dengan grup WhatsApp.
2. recepts : Tabel receipts meupakan penerima dari anggota grup.

list Tabel diatas merupakan history backup dari hubungan antara list grup anggota grup dan penerima pesan didalan grup WhatsApp. Tabel utama yang berisikan pesan pesan massagger dan flags yang membedakan antara beberapa pesan juga terbagi menjadi tabel sendiri yaitu tabel massages yang mempunyai turunan tabel sebagai berikut :

1. massages_link : Tabel massages_link merupakan konter dari indeks link yang dikirim atau diterima.

2. massages_quotes : Tabel massages_quotes berisikan qoites dari semua percakapan baik grup chating maupun personal chating.
3. massages_fts_contents : Tabel massages_fts_content merupakan konten dari detail pesan yang dikirim dan diterima disertai dengan id_dokumen.
4. Massages_fts_segments.
5. Massages_fts_segdir.

List tabel diatas merupakan beberapa konten yang nantinya akan disatukan menjadi tabel massages. Dalam massages_fts_content mempunyai turunan tersendiri yaitu tabel massages_fts. Tabel massages_fts sebuah virtual tabel yang berfungsi menampung data sementara sebelum pesan dikirim dari percakapan yang terjadi (temporari tabel).

Selain tabel dalam database ini juga mempunyai indeks yang berfungsi mempermudah dalam pencarian konten pesan atau nomor, dsb.

1. grup_participants_index mempunyai indeks gjid dan jid. Dimana gjid dan jid merupakan indeks berdasarkan user yang ada dari list percakapan WhatsApp didalam grup_participants dan grup_participants_history.
2. media_hash_index merupakan indeks media_hash. Dimana media_hash merupakan indeks berdasakan media hash yang ada dalam tabel massages.
3. media_type_index merupakan indeks media_wa_type. Dimana media_wa_type merupakan indeks berdasarkan yang ada didalam tabel massages.
4. media_key_jid_index merupakan indeks key_remote_jid dan media_wa_type. Dimana kedua indeks ini ada didalam tabel massages.
5. massages_key_index merupakan indeks yang unique dari Key_remote_jid, key_from_me, key_id. Dimana indeks ini ada didalam tabel massages.

Dalam database ini juga mempunyai triger yang seperti program kecil yang berfungsi menangkap pesan yang masuk untuk langsung menulis, merubah, maupun menghapus record secara realtime. Untuk trigernya sebagai berikut

1. massages_bd_for_link_triger untuk mengupdate link yang diterima maupun dikrim secara realtime dimana field massages_row_id sama dengan old_id.
2. massages_bd_for_quotes_triger untuk mengupdate ketika ada qotes yang diterima maupun dikirim secara realtime dimana field _id sama dengan old.qouted_row_id.
3. massages_bd_for_receipts_triger untuk menerima pesan masuk secara realtime dimana key_remote_jid sama dengan old.key_remote_jid dan key_id sama dengan old.key_id.
4. Massages_bs_triger untuk mengupdate tabel media_fts_content dimana field docid sama dengan old._id.

5. KESIMPULAN

Setelah dilakukan uji coba forensics dan analisa pada database WhatsApp diperoleh kesimpulan sebagai berikut :

1. Berdasarkan uji forensics yang telah dilakukan dengan dengan medeskripsi file .cryp12 dengan menggunakan tools Andriller, WhatsApp Viewer dan Whatcrypt menghasilkan data yang sama secara struktur data, hal ini disebabkan karena crypt12 merupakan database hasil backup. Sedangkan

dilihat dari sisi isi database memiliki isi database yang berberda dengan database asli karena setelah dianalisa WhatsApp tidaklah membackup databasenya secara realtime tetapi WhatsApp membackup setiap 24 jam sekali ketika jam 02.00.

2. Dalam melakukan uji forensics dengan menggunkan tools yang diujikan dengan metode logical extraction lebih mudah menggunakan tools Andriller karena fitur informasi yang diberikan lebih lengkap dari tools yang lain.

Dari hasil penelitian yang sudah dilakukan dapat dikembangkan untuk penelitian selanjutnya yaitu perlu adanya perbandingan dengan melakukan ujicoba dengan menggunakan sistem opersasi selain Android seperti IOs, Blackbary, dan Windows phone untuk mengetahui dan memperlajari sistem kerja WhatsApp dari sistem operasi tersebut.

REFERENCES

[1] Statista, "Number of monthly active WhatsApp users worldwide from April 2013 to April 2017," https://www.statista.com/statistics/260819/number-of-monthly-active- whatsapp-users/, January 2017, [Accessed 03 January 2017].

[2] Shortall, A., & Azhar, M. A. H. Bin. (2015). Forensic Acquisitions of WhatsApp Data on Popular Mobile Platforms. 2015 Sixth International Conference on Emerging Security Technologies (EST), 13–17. https://doi.org/10. 1109/EST.2015.16

[3] Anglano, C. (2014). Forensic analysis of WhatsApp Messenger on Android smartphones. Digital Investigation, 1–13. https://doi.org/10.1016/j.diin.2014 .04.003

[4] Ayers, R., Jansen, W., & Brothers, S. (2014). Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1). NIST Special Publication, 1(1), 85. https://doi.org/10.6028/NIST.SP.800-101r1

[5] Karpisek, F., Baggili, I., & Breitinger, F. (2015). WhatsApp network forensics : Decrypting and understanding the WhatsApp call signaling messages. Digital Investigation, 1–9. https://doi.org/10.1016/j.diin.2015.09.002

[6] Walnycky, D., Baggili, I., Marrington, A., Moore, J., & Breitinger, F. (2015). Network and device forensic analysis of Android social-messaging applications. Digital Investigation, 14, S77–S84. https://doi.org/10.1016/j. diin.2015.05.009.

[7] Thing, V. L. L., Ng, K., & Chang, E. (2010). Live memory forensics of mobile phones. Digital Investigation, 7, S74–S82. https://doi.org/10.1016/j.diin .2010.05.010