

Analisa Forensik Whatsapp Messenger Pada Smartphone Android

Nenny Anggraini¹, Siti Umami Masrurroh², Hapsari Tiaraningtias³

^{1,2,3}Fakultas Sains & Teknologi, UIN Syarif Hidayatullah Jakarta

Jl. Ir H. Juanda No.95, Cemp. Putih, Kec. Ciputat, Kota Tangerang Selatan, Banten 15412

¹nenny.anggraini@uinjkt.ac.id, ²ummi.masrurroh@uinjkt.ac.id, ³hapsaritiaraningtias@gmail.com

Abstract

Internet technology and smartphones are increasingly rapidly followed by the rise of social media users, especially instant messaging that can be accessed using a smartphone, especially Android. One of the problems of social media is cyber crime that utilizes social media. Based on data from Instant Checkmate in 2014, 30,000 websites were hacked, and 12 casualties fell within a fraction of the crime from fraud to sex crimes, and it occurs in cyber crime involving social media, including instant media WhatsApp messenger. So it takes the forensic digital process to look for evidence of the crime, because basically there is no crime that does not leave a trace. This study was conducted to find the forensic evidence on the WhatsApp messenger application accessed on Android smartphones. WhatsApp messenger was chosen because it used to reach 1.5 billion users from over 2.7 billion users of social media worldwide. In this study, the simulation method used in the study to run 15 scenarios, including the return of the deleted files, the search for forensic evidence such as name and account number, a list of names and contact numbers, group chat, and text messages, pictures, video, and document files on personal chat, then text messages, pictures, videos, document files, voice notes, and location in group chat. The results of this study indicate that almost all forensic evidence traces in the WhatsApp messenger application are found, but the URL media can not be opened because it is encrypted by WhatsApp.

Keyword: Digital Forensic, Forensic Evidence, Smartphone, WhatsApp Messenger.

Abstrak

Perkembangan teknologi internet dan smartphone yang semakin pesat diikuti pula oleh meningkatnya pengguna media sosial pada instant messenger yang diakses menggunakan smartphone khususnya Android. salah satu permasalahan yang tidak luput dari media sosial adalah tindak kejahatan dunia maya yang memanfaatkan media sosial. Berdasarkan data dari Instant Checkmate pada tahun 2014 sebanyak 30.000 website diretas, dan 12 korban perdetik berjatuh dari berbagai aspek kejahatan dari penipuan hingga kejahatan seks, dan hal tersebut terjadi dalam praktek kejahatan internet (cyber crime) melibatkan media sosial, termasuk media instant messenger WhatsApp. Sehingga diperlukannya proses digital forensik untuk mencari bukti-bukti kejahatan tersebut, karena pada dasarnya tidak ada kejahatan yang tidak meninggalkan jejak. Penelitian ini dilakukan untuk menemukan bukti-bukti forensik tersebut pada aplikasi WhatsApp messenger yang diakses pada smartphone Android. WhatsApp messenger dipilih karena digunakan mencapai 1,5 tiliyun user dari lebih dari 2,7 triliyun pengguna media sosial seluruh dunia. Pada penelitian ini, metode simulasi digunakan dalam penelitian dengan menjalankan 15 skenario, diantaranya adalah pengembalian file yang dihapus, pencarian bukti forensik berupa nama dan nomor akun, daftar nama dan nomor kontak, group chat, kemudian pesan teks, gambar, video, dan file dokumen pada personal chat, kemudian pesan teks, gambar, video, file dokumen, voice note, dan location pada group chat. Hasil dari penelitian ini menunjukkan bahwa hampir semua jejak bukti forensik pada aplikasi WhatsApp messenger berhasil ditemukan, namun media URL tidak dapat dibuka karena terenkripsi oleh WhatsApp.

Keyword: Bukti Forensik, Digital Forensik, Smartphone, WhatsApp Messenger.

I. Pendahuluan

1.1 Latar Belakang

Seiring dengan berjalannya waktu, saat ini perkembangan teknologi semakin pesat, dan salah satunya adalah *smartphone*. Telepon genggam yang telah dilengkapi dengan sistem operasi yang dapat melakukan beberapa fungsi layaknya personal komputer, salah satu kegunaannya adalah akses internet. Orang-orang dapat mengakses internet kapanpun dan dimanapun dengan adanya internet. Dan *Android* adalah salah satu sistem operasi yang paling banyak digunakan pada *smartphone* saat ini. Pengguna *smartphone* yang mengakses internet dengan *platform* berbasis *Android* sebanyak 71,6%, *Apple iOS* 19,6% dan *platform* lainnya sebanyak 8,8% berdasarkan data yang didapatkan dari *wearesocial.com* pada Januari 2016.

Pesatnya perkembangan media *chatting* saat ini adalah sebuah fenomena yang sangat dirasakan oleh para pengguna internet khususnya aplikasi *instant messenger*. Dengan adanya aplikasi *instant messenger*, memungkinkan terciptanya berbagai jenis konten obrolan dari berbagai jenis aplikasi *instant messenger*, dari jenis pesan yang bermuatan obrolan atau informasi rahasia bahkan rencana kejahatan. Dalam lingkup ini, *WhatsApp* merupakan aplikasi *instant messenger* yang paling banyak digunakan di seluruh dunia. *WhatsApp messenger* merupakan aplikasi pesan lintas *platform* yang memungkinkan kita bertukar pesan tanpa biaya sms, karena *WhatsApp Messenger* menggunakan paket data internet yang sama untuk *e-mail*, dan *browsing web*. Berdasarkan data dari *wearesocial.com*, *WhatsApp messenger* telah mencapai 1,5 triliun *user* per bulan dari berbagai *platform* pada bulan Agustus 2017, dari lebih dari 2,7 triliun pengguna media sosial seluruh dunia. Dengan peningkatan adanya pengguna baru *WhatsApp messenger* sebanyak 8 juta *user* (*wearesocial.com*) dari berbagai *mobile platform* sejak bulan April hingga Agustus.

Dengan *WhatsApp messenger* memiliki fitur dapat melakukan obrolan *online* berupa bertukar teks, berbagai *file mp3*, *file mp4*, bertukar foto, video, *voice note*, *location maps* dan berbagai macam *file* dokumen. Dengan adanya fitur tersebut, memudahkan para pengguna untuk saling berkomunikasi *user to user* dengan *WhatsApp messenger*. Sehingga terbukanya kesempatan untuk orang-orang yang berniat untuk melakukan tindak kejahatan dalam saling bertukar informasi ataupun perintah tindak kejahatan dengan memanfaatkan *WhatsApp messenger* dengan bentuk informasi yang dapat berupa teks ataupun *file*.

Pada penelitian Wisnu Ari Mukti (2017) yang berjudul "Analisa dan Perbandingan Bukti Forensik pada Aplikasi Media Sosial *Facebook* dan *Twitter* pada *Smartphone Android*", menjelaskan tentang bagaimana mendapatkan data forensik yang dibutuhkan sebagai bukti forensik yang dibutuhkan dalam suatu kasus yang menggunakan *smartphone*. Dalam suatu kasus kejahatan, setelah mengirimkan informasi untuk atau sebagai tindak kejahatan, penjahat bisa saja langsung menghapus riwayat obrolan dan melakukan penghapusan aplikasi *WhatsApp messenger* pada ponsel yang digunakan untuk mengirim *file* tersebut. Maka hal tersebut dapat menyulitkan orang awam untuk melakukan investigasi bukti forensik langsung dalam aplikasi *WhatsApp messenger*. Namun terdapat jalan keluar yang dapat dilakukan untuk menemukan bukti forensik yang telah hilang. Artefak aplikasi *WhatsApp messenger* yang digunakan tersimpan pada *device Android*. Sehingga jika pada suatu kasus kejahatan yang melibatkan aplikasi *WhatsApp*, maka *smartphone* tersebut dapat dianalisis untuk mendapatkan artefak *digital* yang berkaitan. Hal tersebut bisa dilakukan dengan menerapkan ilmu *digital forensik*, dimana ilmu tersebut bisa digunakan dalam mengungkap kasus kriminal dan sebagainya pada perangkat *digital*.

Data *WhatsApp messenger* yang hilang dapat ditemukan kembali di dalam *device android* yang diidentifikasi yang diasumsikan sebagai salah satu barang bukti dalam suatu tindakan kriminal. Namun tidak semua orang mengetahui dan dapat melakukannya. Hal tersebut harus melewati proses dan prosedur yang mendukung untuk mengembalikan, mencari, dan mengumpulkan data artefak forensik yang dicari untuk dapat dijadikan bukti forensik dalam sebuah investigasi kriminal. Untuk menjalani proses tersebut maka metode yang bisa digunakan adalah metode *mobile forensik* yang merupakan cabang ilmu *digital forensik* yang berfokus pada perangkat *mobile*, dan juga metode *digital forensik*. Dengan melakukan kerangka kerja *mobile forensik* sekaligus metode *digital forensik*, maka data-data yang berkaitan dengan aplikasi *WhatsApp messenger* dapat dipulihkan kembali, dan dikumpulkan data artefak yang tertangkap, kemudian dibuat laporan kejadian yang nantinya bisa dijadikan sebagai barang bukti forensik kejahatan *digital*.

Tabel 1. Perbandingan Penelitian

Penelitian	Judul	Ide
(Wisnu Ari Mukti, 2017)	Pencarian Bukti Forensik pada Aplikasi Media Sosial Facebook dan Twitter pada Smartphone Android	Bagaimana mendapatkan data bukti forensik yang dibutuhkan sebagai bukti forensik dari media sosial <i>Facebook</i> dan <i>Twitter</i> dalam suatu kasus yang menggunakan <i>smartphone</i> .
(Casimo Anglano, 2014)	Forensic Analysis of WhatsApp Messenger on Android Smartphones	Melakukan analisa dan menjelaskan bagaimana menginterpretasikan artefak <i>WhatsApp messenger</i> untuk dapat merekonstruksikan daftar kontak dan kronologi pertukaran pesan. Dan menjelaskan korelasi antara masing-masing data yang dapat menghasilkan kesimpulan informasi.
(Aditya Mahajan, 2013)	Forensic Analysis of Instant Messenger Applications on Android Devices	Analisa data forensik <i>WhatsApp messenger</i> dan <i>Viber</i> pada <i>smartphone Android</i> , dalam 3 versi android. Tes dan analisa bertujuan untuk menemukan seluruh data dan informasi apa saja yang dapat ditemukan pada masing-masing versi android dari kedua jenis <i>Instant Messenger</i> tersebut dengan investigasi forensik.
(Neha S. Thakur, 2013)	Forensic Analysis of WhatsApp on Android	Bagaimana menguraikan investigasi forensik dapat menggali dan mendapatkan data dan informasi penting dan berguna dari <i>WhatsApp messenger</i> dan aplikasi sejenis dari <i>android</i> . Berfokus pada ekstraksi dan analisa dari data yang ada di <i>eksternal storage</i> dan <i>RAM</i> pada <i>android</i> .
(Syukur Ikhsani, Bakti Cahyo Hidayanto, 2016)	Analisa Forensik Whatsapp dan LINE Messenger pada Smartphone Android sebagai Rujukan dalam Menyediakan Barang Bukti yang Kuat dan Valid di Indonesia	Melakukan analisa forensik pada <i>WhatsApp</i> dan <i>LINE messenger</i> dengan menggunakan <i>tools</i> forensik <i>FTK imager</i> dan <i>SQLite</i> , kemudian membandingkan bagaimana hasil analisa forensik antara <i>WhatsApp</i> dan <i>LINE messenger</i> .
Penelitian ini	Pencarian Bukti Forensik pada Aplikasi WhatsApp Messenger pada Smartphone Android	Bagaimana mendapatkan data bukti forensik yang dibutuhkan sebagai bukti forensik dari <i>WhatsApp Messenger</i> berfokus pada dile yang dikirimkan dan isi percakapan. Menggunakan aplikasi recovery Dr. Fone for Android untuk melakukan recovery data <i>WhatsApp messenger</i> yang telah terhapus dan Analisa database <i>WhatsApp messenger</i> yang didapatkan dengan DB Browser for SQLite

1.2 Batasan Masalah

1. Proses:

- Penelitian *WhatsApp forensik* dijalankan sesuai dengan skenario
- *Device android* yang digunakan sudah melalui proses *root*.
- Data yang dimasukkan dalam *WhatsApp messenger* merupakan data yang hanya digunakan untuk simulasi.
- Data pada *WhatsApp messenger* dihapus, kemudian melakukan *recovery* guna untuk memulihkan data sebelum melakukan pencarian bukti data forensik.
- Penelitian difokuskan pada pencarian data forensik pada aplikasi *WhatsApp messenger* pada *platform smartphone android*.

2. Tools:

- Penelitian dilakukan pada aplikasi *WhatsApp messenger* versi 2.18.46 yang diaplikasikan pada android *device* Xiaomi Redmi 4A.
- *Device Android* telah dalam keadaan *root* dengan versi OS *Android* 8.5.1.0.
- Menggunakan aplikasi *recovery Dr. Fone for Android* untuk melakukan *recovery* data *WhatsApp messenger* yang telah terhapus.
- Analisa database *WhatsApp messenger* yang didapatkan dengan DB Browser for SQLite.

3. Metode:

- Metode yang digunakan adalah metode *digital* forensik dengan asumsi perangkat *digital* digunakan sebagai alat yang digunakan untuk tindak kriminal.
- Metode *digital* forensik yang berfokus pada penanganan dan analisa data yang berhasil didapatkan.

II. Landasan Teori

2.1 Digital Forensic

Forensik merupakan kegiatan untuk melakukan investigasi dan menetapkan fakta yang berhubungan dengan kejadian kriminal dan permasalahan hukum lainnya. Sedangkan *digital forensic* merupakan bagian dari ilmu forensik yang melingkupi penemuan artefak dan investigasi materi (data) yang ditemukan pada perangkat *digital* (komputer, *handphone*, tablet, PDA, *networking device*, *storage* dan sejenisnya) (Raharjo, 2013). Berikut adalah jenis-jenis data forensik:

1. Active Data

Informasi terbuka yang dapat dilihat oleh siapa saja, terutama data, program, maupun *file* yang dikendalikan oleh sistem operasi.

2. Archival Data

Informasi yang telah menjadi arsip sehingga telah disimpan sebagai *backup* dalam berbagai bentuk alat penyimpanan seperti *external harddisk*, *CD-Room*, *Backup tape*, DVD, dan lain-lain.

3. Latent Data

Informasi yang membutuhkan alat khusus untuk mendapatkannya karena sifatnya yang khusus, misalnya: telah dihapus, ditimpa data lain, rusak (*corrupted file*), dan lain sebagainya.

2.2 Mobile Forensic

Menurut (Yadi & Kunang, 2014), *mobile phone forensic* merupakan ilmu yang melakukan proses *recovery* bukti *digital* dari perangkat *mobile* menggunakan cara yang sesuai dengan kondisi forensik. Forensik sendiri bisa dilakukan pada berbagai ponsel, tidak hanya terpaku pada *smartphone*. Dengan meningkatnya jumlah ponsel yang kaya fitur membuat sulitnya membuat satu *tool forensik* atau standar khusus untuk satu *platform*. Bukti *digital* dalam perangkat *mobile* mudah rentan dengan data baru atau terhapus. Perangkat *mobile* sendiri menggunakan *flash memory* untuk menyimpan data. Keuntungan menggunakan *flash memory* adalah ketahanannya terhadap suhu dan tekanan yang tinggi sehingga lebih sulit untuk dihancurkan. Dari sudut pandang forensik hal ini menguntungkan karena *flash memory* bisa saja berisi informasi yang sudah dihapus bahkan setelah seseorang berusaha untuk menghancurkan barang bukti.

Perangkat *mobile* merupakan sumber berharga sebagai bukti *digital* dan berisi informasi penting yang tidak tersedia pada perangkat lain. Selain itu sifat *personality* dari perangkat tersebut membuatnya mudah untuk membuktikan jejak yang mengaitkan perangkat ke individu. Dalam forensik perangkat *mobile* data yang diambil dari ponsel dengan sendirinya bisa dijadikan sebagai bukti. Bukti-bukti ini bisa menjadi landasan ketika menyelidiki suatu perkara oleh lembaga penegak hukum. Artefak ini bisa diekstrak dengan metode *logic* maupun fisik. Secara *logic* adalah mengekstrak data dari *file* sistem dengan langsung berinteraksi dengan perangkat menggunakan beberapa *tools* khusus. *Software* atau *tools* yang bisa mengekstrak artefak (bukti forensik) ini sangat terbatas.

Forensik *mobile* juga menggunakan metode yang sama dengan investigasi forensik secara umum. Ada beberapa teknik yang perlu diikuti, meskipun belum ada format standar penyelidikan pada forensik *mobile*. Metode penyelidikan yang digunakan kurang lebih sama dengan investigasi *digital*. Tahapan proses penyelidikan yang diikuti adalah:

1. Collection

Merupakan langkah awal dan paling penting dalam penyelidikan. Tujuan utamanya adalah untuk mengumpulkan sumber-sumber bukti potensial pada perangkat *mobile*.

2. Identification

Tahap ini difokuskan pada pengenalan sumber barang bukti dengan pelabelan.

3. Acquisition

Tahapan ini berkaitan dengan proses ekstraksi data atau bukti dari berbagai sumber yang telah dikumpulkan.

2.2 Smartphone

Menurut (Williams & Sawyer, 2011), *smartphone* adalah telepon selular dengan mikroprosesor, memori, layar dan modem bawaan. *Smartphone* merupakan ponsel multimedia yang menggabungkan fungsionalitas *PC* dan *handset* sehingga menghasilkan *gadget* yang mewah, dimana terdapat pesan teks, kamera, pemutar musik,

video, game, akses email, tv digital, search engine, pengelola informasi pribadi, fitur GPS, jasa telepon internet dan bahkan terdapat telepon yang juga berfungsi sebagai kartu kredit.

2.3 WhatsApp Messenger

WhatsApp Messenger adalah layanan pesan *multiplatform* yang menggunakan sambungan internet telepon/ponsel untuk kegiatan *chatting* dan melakukan panggilan dengan pengguna WhatsApp messenger lainnya yang didirikan oleh Jan Koum dan Brian Acton (*whatsapp.com*).

WhatsApp messenger digunakan oleh lebih dari 1 milyar pengguna di lebih dari 180 negara. Untuk tetap terhubung dengan teman-teman dan keluarga, kapan pun dan dimana pun. WhatsApp messenger menyediakan layanan bertukar pesan dan panggilan yang sederhana, aman, dan *reliable*, serta tersedia pada telepon/ponsel di seluruh dunia.

Permulaan kemunculan WhatsApp messenger adalah sebagai alternatif untuk SMS. Saat ini WhatsApp messenger mendukung fitur untuk mengirim dan menerima berbagai macam media, yaitu: teks, foto, video, dokumen, dan lokasi, juga panggilan suara. Pesan dan Panggilan diamankan dengan enkripsi *end-to-end*, yang berarti tidak ada pihak ketiga termasuk WhatsApp yang dapat membaca pesan atau mendengar panggilan.

2.4 SQLite

DB Browser for SQLite adalah sebuah aplikasi dekstop. DB Browser for SQLite merupakan aplikasi yang berguna untuk melihat dan manajemen database SQLite. Fitur yang dimiliki oleh SQLite Manager antara lain (Iazierthanthou, 2016) :

1. Dapat melakukan manajemen database SQLite.
2. Dapat melakukan eksekusi terhadap segala jenis SQL query.
3. Dapat melihat dan mencari tabel yang terdapat pada database.

2.5 Metode Simulasi

Metode Simulasi merupakan metode untuk melakukan simulasi dan pemodelan yang diadaptasi dari penelitian yang dilakukan oleh Sajjad A. Madani, Jawad Kazmi dan Stefan Mahlkecht pada tahun 2010 dengan karya publikasi yang berjudul *Wireless sensor network: Modeling and Simulation*. Dalam penelitian tersebut metode simulasi digunakan untuk melakukan pemodelan dan simulasi terhadap *Wireless Sensor Network* (WSN). (Madani, Jawad, & Mahlkecht, 2010).

Menurut (Madani, Jawad, & Mahlkecht, 2010) terdiri dari beberapa tahapan yang terdiri dari :

1. *Problem Formulation*
2. *Conceptual Model*
3. *Input/Output Data*
4. *Modeling*
5. *Simulation*
6. *Verification and Validation*
7. *Experimentation*
8. *Output Analysis*

III. Metodologi

3.1 Metode Pengumpulan Data

1. Data Primer

Dalam Penelitian melakukan pengumpulan data-data dan informasi yang diperoleh dengan mencari data-data survey dan melakukan analisis untuk mendapatkan data primer melalui kegiatan simulasi. Dalam penelitian mengumpulkan data-data simulasi dengan melakukan simulasi mencari dan menganalisa data forensik menggunakan *smartphone* berbasis *Android* dengan versi 8.5.1.0 yang telah terpasang aplikasi WhatsApp messenger dan menggunakan akun palsu, yang kemudian data hasil simulasi ini akan dijadikan dalam penelitian sebagai hasil penelitian

2. Data Sekunder

Dalam penelitian mendapatkan data-data sekunder dengan melakukan studi pustaka dan studi literatur. Berikut studi literatur yang dilakukan peneliti dengan membandingkan penelitian ini dengan penelitian sejenis:



Gambar 1. Perbandingan penelitian dengan penelitian sebelumnya

3.2 Metodologi Penelitian

Dalam penelitian menggunakan metode simulasi sebagai metode untuk mencari dan menganalisa bukti forensik dengan cara melakukan uji coba simulasi terhadap aplikasi *WhatsApp messenger* yang terpasang pada *smartphone* berbasis *Android* versi 8.5.1.0 dalam penelitian ini.

1. Problem Formulation

Setelah melakukan pengumpulan data-data yang diperlukan, maka didapatkan permasalahan utama dalam pencarian bukti forensik yaitu dapatkah bukti forensik ditemukan pada aplikasi *instant messaging WhatsApp messenger* versi 2.18.46 yang diakses pada *smartphone Android* versi 8.5.1.0.

2. Conceptual Model

Setelah melakukan formulasi permasalahan, dilakukan perancangan dan penggambaran konsep model untuk simulasi yang akan dilakukan dalam penelitian ini.

3. Input and Output Data

Pada tahap ini membuat *input* dan *output* apa yang akan diproses pada simulasi. *Input* merupakan berupa atribut yang diperlukan dalam simulasi, yaitu data dari akun palsu yang telah dibuat ketika mengakses *WhatsApp messenger* pada *smartphone Android*. Sementara *output* berdasarkan permasalahan yang diformulasikan, yaitu ditemukan atau tidaknya bukti forensik yang didapatkan dari aplikasi *WhatsApp messenger* tersebut.

4. Modeling

Langkah awal yang dilakukan pada tahapan ini adalah menentukan parameter yang digunakan selama simulasi, pada tahapan ini dilakukan pembuatan skenario-skenario yang akan digunakan untuk simulasi.

5. Simulation

Pada tahapan ini melakukan implementasi model yang dihasilkan dalam tahapan sebelumnya. Selain itu dilakukan pula proses *root* pada *smartphone Android*, pemasangan aplikasi *database browser (DB Browser for SQLite)* dan aplikasi *recovery (Wondershare Dr. Fone for Android)* dan pembuatan akun palsu yang akan digunakan pada penelitian ini.

6. Verification and Validation

Pada tahapan ini dilakukan verifikasi dan validasi untuk mengecek dan memastikan keberhasilan dan kebenaran dari tahap sebelumnya, sehingga simulasi siap untuk dilaksanakan. Verifikasi dan validasi akan dilakukan terhadap tahap *conceptual model*, *modeling* dan *simulation*.

7. Experimentation

Tahap *experimentation* ini merupakan tahap paling penting dalam penelitian. Proses simulasi dari skenario yang telah ditentukan sebelumnya akan dijalankan pada tahap ini. Hasil yang didapat kemudian dianalisa data yang dibutuhkan.

8. *Output Analysis*

Pada tahap ini dilakukan analisis *output* dari simulasi yang dilakukan pada tahap sebelumnya. Hasil penelitian dianalisa untuk mengetahui apakah berhasil ditemukan atau tidaknya bukti forensik yang ditentukan untuk dicari.

IV. Hasil dan Pembahasan

4.1 Conceptual Model

Dalam penelitian ini, tahap membuat konsep model merupakan tahap dilakukannya penggambaran diri *input*, proses dan *output* yang dihasilkan. Gambaran arsitektur proses pencarian bukti forensik pada aplikasi *WhatsApp Messenger*.



Gambar 2. Arsitektur Simulasi Pencarian dan Analisa Bukti Forensik



Gambar 3. Arsitektur Komunikasi Data pada *WhatsApp Messenger*



Gambar 4. Proses *Recovery Data*

4.2 Skenario

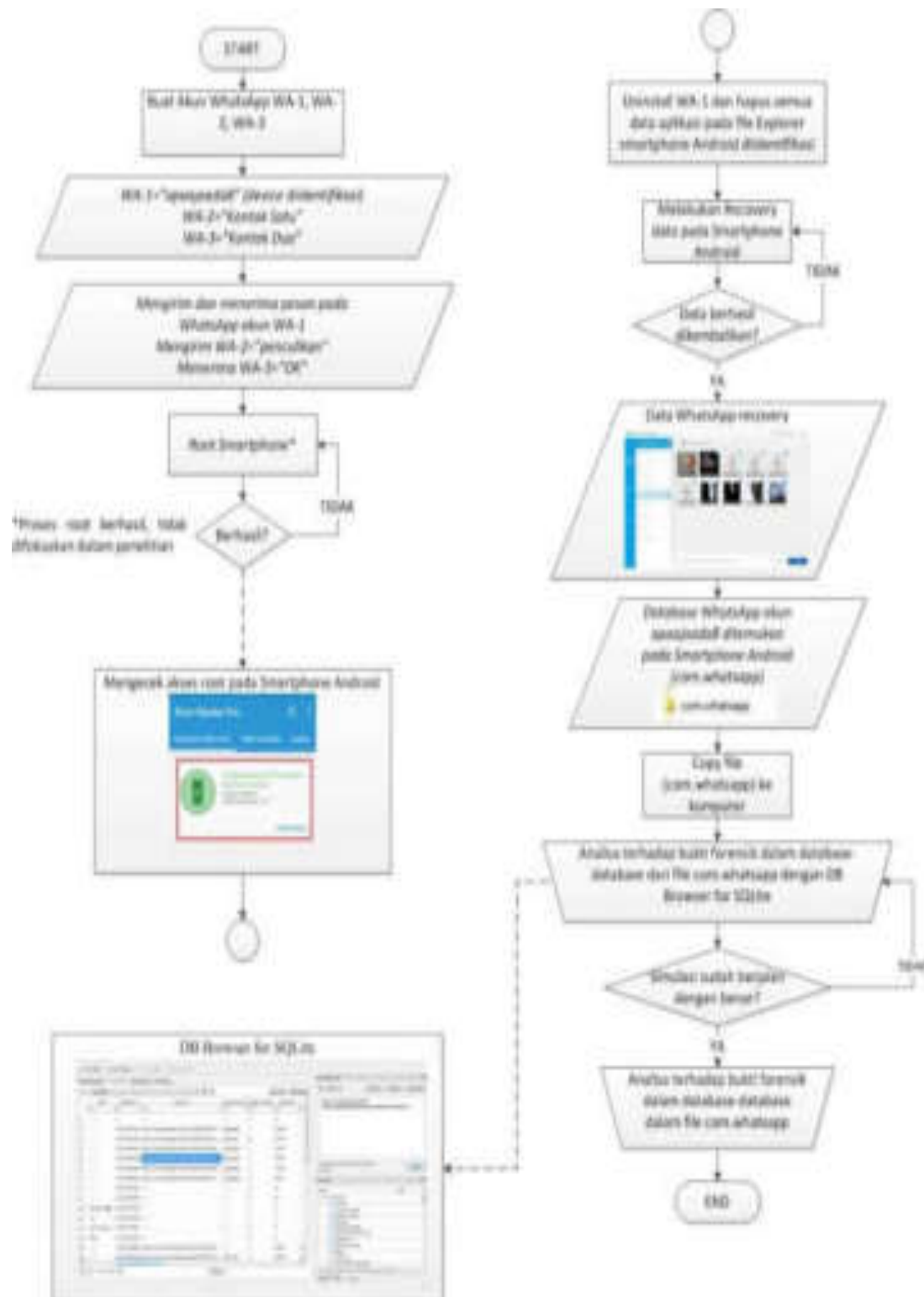
Adapun skenario simulasi yang dijalankan dalam penelitian ini adalah sebagai berikut:

Tabel 2. Skenario Data Simulasi *WhatsApp* Forensik

Skenario	Data Input/Output	Bentuk Data
Skenario 1	Aplikasi dan seluruh data pada aplikasi tersebut	<i>File database (com.whatsapp)</i>
Skenario 2	Nama Akun WA (apaajaada8) dan Nomor akun WA (+62895412230291)	Teks
Skenario 3	Daftar nama kontak WA (Kontak Satu, Kontak Dua) dan Daftar nomor kontak WA (+6281298220138, 089628377685)	Teks
Skenario 4	Nama <i>WhatsApp group chat</i> (Misi Bersatu)	Teks
Skenario 5	Kontak anggota <i>group chat</i> (Kontak Satu: +6281298220138, Kontak Dua: 089628377685)	Teks

Skenario	Data Input/Output	Bentuk Data
	Pesan teks <i>personal chat</i> : -Tes (sending ke Kontak Satu) -Yes one two three (receive dari Kontak Satu)	
Skenario 6	-Culik kity jam 3 sore (sending ke Kontak Satu) -Siap, bambu apus (receive dari Kontak Satu) -Good (sending ke Kontak Satu) -On tkp (receive dari Kontak Satu) -Siap (sending ke Kontak Satu)	Teks
Skenario 7	Pesan gambar <i>personal chat</i> (IMG-20180216-WA0005).jpg	Gambar
Skenario 8	Pesan video <i>personal chat</i> (VID-20180216-WA0006.mp4)	Video
Skenario 9	Pesan file dokumen zip <i>personal chat</i> (SuperSU-v2.82-201705271822.zip)	File Zip
	Pesan teks <i>group chat</i> : -Tes (sending) -Satu dua tiga (sending) -Stand by (sending)	
Skenario 10	-Oke (receive Kontak Dua) -Standar by malam (Receive Kontak Dua) -Siap (receive Kontak Satu) -Penculikan kity sukses (receive Kontak Satu) -Good joob, lokasi diterima (sending)	Teks
Skenario 11	Pesan gambar <i>group chat</i> (IMG-20180216-WA0008.jpg, IMG-20180216-WA0009.jpg)	Gambar
Skenario 12	Pesan video <i>group chat</i> (VID-20180216-WA0007.mp4, VID-20180216-WA0010.mp4)	Video
Skenario 13	Pesan file dokumen zip <i>group chat</i> (SuperSU-v2.82-201705271822.zip)	File Zip
Skenario 14	Pesan voice note <i>group chat</i> (PTT-20180216-WA0011.mp4, PTT-20180216-WA0012.mp4)	Audio
Skenario 15	Pesan location <i>group chat</i> (Gerbang Tol Bambu Apus (Jalan Tol Lingkar Luar Selatan, Jakarta, Jakarta))	Maps

4.3 Flowchart Simulasi



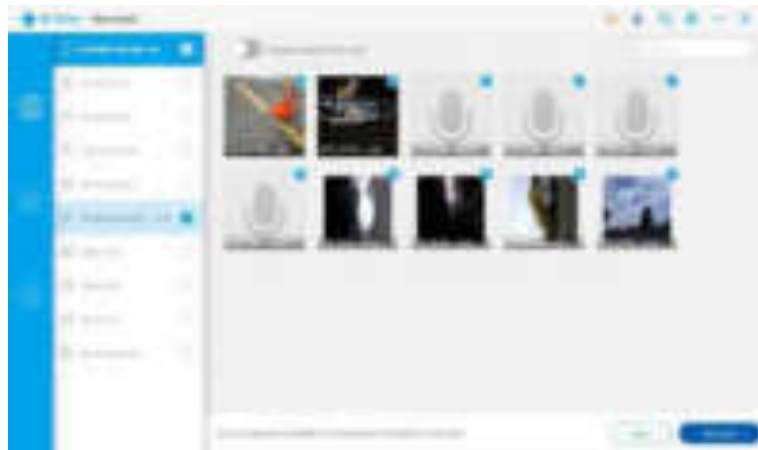
Gambar 5. Flowchart Simulasi

4.4 Output Analysis

Tabel 3. Output

	Skenario	WhatsApp Messenger	Bukti Forensik
1	Mengembalikan file dan data-data yang dihapus Data dan file yang dikembalikan	File dan data-data berhasil dikembalikan com.whatsapp (file dan data-data WhatsApp Messenger)	
2	Menemukan bukti forensik berupa nama akun Menemukan bukti forensik berupa nomor telepon akun WA	Nama akun tidak berhasil ditemukan pada penelitian ini, karena data tersimpan pada server, bukan pada database Nomor akun WA berhasil ditemukan	tidak ada 62895412230291 @s.whatsapp.net
3	Menemukan bukti forensik berupa daftar nama kontak Menemukan bukti forensik berupa daftar nama kontak	Daftar nama berhasil ditemukan Daftar nomor kontak berhasil ditemukan	kontak satu dan Kontak Dua 6281298220138 dan 89628377685
4	Menemukan bukti forensik berupa nama <i>group</i>	Nama <i>group</i> berhasil ditemukan	Misi Bersatu
5	Menemukan bukti forensik berupa kontak anggota <i>group chat</i>	Kontak anggota <i>group chat</i> berhasil ditemukan	6289628377685@ s.whatsapp.net dan 6281298220138@ s.whatsapp.net
6	Menemukan bukti forensik berupa isi pesan teks	Pesan teks berhasil ditemukan	Ada
7	Menemukan bukti forensik berupa <i>file</i> pesan gambar	<i>File</i> pesan gambar beserta media <i>URL</i> berhasil ditemukan	IMG-20180216- WA0005.jpg dengan media URL https://mmg-fna.whatsapp.net/d/f/ArvMuGJ5nUhF7IMU0sMY4QY-UMWkQpwb_hFek3N0HJY1.enc
8	Menemukan bukti forensik berupa <i>file</i> pesan video	pesan video beserta media <i>URL</i> berhasil ditemukan	IMG-20180216- WA0006.jpg dengan URL https://mmg-fna.whatsapp.net/d/f/AtFwCMcPcYA CrE8VlCJGJuUJcZAv0U9- ta_3_XFUrmvq.enc
9	Menemukan bukti forensik berupa <i>file</i> dokumen <i>zip</i>	Nama <i>file</i> dokumen <i>zip</i> beserta media <i>URL</i> berhasil ditemukan	SuperSU-v2.82- 201705271822 dengan media URL https://mmg-fna.whatsapp.net/d/f/Atqgw5Zn_bi6jrXnvED3XrUvIv8BZsZOwB95BB- n9cds.enc
10	Menemukan bukti forensik berupa pesan teks <i>group chat</i>	Pesan teks <i>group chat</i> berhasil ditemukan	Ada
11	Menemukan bukti forensik berupa <i>file</i> pesan gambar	Nama file pesan gambar beserta media URL berhasil ditemukan.	IMG-20180216- WA0008.jpg, IMG-20180216- WA0009.jpg https://mmg-fna.whatsapp.net/d/f/AkrWfSN0E- iKiDqw8oX2eRiQa3vfNglX4gz93U K8iYRY.enc
12	Menemukan bukti forensik berupa <i>file</i> pesan video	Nama <i>file</i> pesan video beserta media <i>URL</i> berhasil ditemukan	VID-20180216- WA0007.mp4,
13	Menemukan bukti forensik berupa <i>file</i> dokumen <i>zip</i>	Nama <i>file</i> dokumen <i>zip</i> beserta media <i>URL</i> berhasil ditemukan	VID-20180216- WA0007.mp4, VID-20180216- WA0010.mp4
14	Menemukan bukti forensik berupa <i>file voice note</i>	Nama jenis <i>file voice note</i> beserta media <i>URL</i> berhasil ditemukan	audio/ogg; https://mmg.whatsapp.net/d/f/ApZdQ5luPRG- YxOmd8yGT0QzNI_K5-opEeVXN- 9XwQyB.enc
15	Menemukan bukti forensik berupa pesan <i>location</i>	Nama <i>file</i> pesan <i>location</i> beserta media <i>URL</i> berhasil ditemukan	Gerbang Tol Bambu Apus Jalan Tol Lingkar Luar Selatan, Jakarta, Jakarta https://foursquare.com/v/4bf9bc858d30d13a87be0218

1. Hasil Simulasi Skenario 1



Gambar 6. Proses *Recovery Data WA*

cache	2/18/2018 5:13 AM	File folder
cache_image	2/18/2018 5:13 AM	File folder
database	2/18/2018 5:13 PM	File folder
files	2/18/2018 5:13 AM	File folder
img	2/18/2018 5:13 AM	File folder
msg_backup	2/18/2018 5:13 AM	File folder
shared_prefs	2/18/2018 5:13 AM	File folder

Gambar 7. Data Aplikasi WA yang berhasil dikembalikan

2. Hasil Simulasi Skenario 2

number	raw_contact_id	display_name
Filter	Filter	Filter
+6281298220138	1374	Kontak Satu
089628377685	1376	Kontak Dua
012095412238291@u.watutamu.net	1377	Mel Bernifu
Filter	Filter	Filter

Gambar 8. Nomor Kontak WA pada *Device* Diidentifikasi

4. Hasil Simulasi Skenario 3

number	raw_contact_id	display_name
Filter	Filter	Filter
+6281298220138	1374	Kontak Satu
089628377685	1376	Kontak Dua

Gambar 9. Daftar nomor dan nama kontak pada WA

5. Hasil Simulasi Skenario 4

number	fbw_contact_id	Display_name
Filter	Filter	Filter
0000	0000	0000
+6281298220138	1374	Kontak Satu
888428377685	1374	Kontak Dua
628954123302910@s.whatsapp.net	0000	Min Berada

Gambar 10. Nama *Group* WA pada akun *WA device* diidentifikasi

6. Hasil Simulasi Skenario 5

number	fbw_contact_id	Display_name
Filter	Filter	Filter
0000	0000	0000
+6281298220138	1374	Kontak Satu
888428377685	1374	Kontak Dua
628954123302910@s.whatsapp.net	0000	Min Berada

Gambar 11. Nomor daftar kontak *group* WA dalam *WA device* diidentifikasi

7. Hasil Simulasi Skenario 6

number	fbw_contact_id	Display_name
Filter	Filter	Filter
0000	0000	0000
+6281298220138	1374	Kontak Satu
888428377685	1374	Kontak Dua
628954123302910@s.whatsapp.net	0000	Min Berada

Gambar 12. Isi pesan *teks personal chat* WA dalam *device* diidentifikasi

8. Hasil Simulasi Skenario 7

media_size	media_name	media_caption
Filter	Filter	Filter
0000	0000	0000
110212	34C-20180218-WA0005.jpg	0000

Gambar 13. Nama *file* gambar *personal chat* *WA device* diidentifikasi

media_url	media_t
Filter	Filter
https://mmg-fba.whatsapp.net/d/t/ArvMgC5vUeF77M00dM4QY-UMWbQjwb_hFv3M0H0Y1.enc	img

Gambar 14. Media URL file gambar personal Chat WA Device diidentifikasi (terenkripsi)

9. Hasil Simulasi Skenario 8

media_size	media_name	media_caption
Filter	Filter	Filter
19023	VID-20180216-WA0006.mp4	

Gambar 15. Nama file video personal chat WA device diidentifikasi

media_url	media_mime_type
Filter	Filter
https://mmg-fba.whatsapp.net/d/t/AFwCAdPvK0S8V3JCw3zJAu8U8a_3_8fimg.enc	video/mp4

Gambar 16. Media URL file video personal chat WA device diidentifikasi (terenkripsi)

10. Hasil Simulasi Skenario 9

SuperSU-v2.82-201705271822	pB3ztW56uq
SuperSU-v2.82-201705271822	swA54obOL

Gambar 17. File Zip personal chat WA device diidentifikasi

https://mmg.whatsapp.net/d/t/Ag2bQ3uF8G-Yd0ndlyGTaQnU_X3-qf8vY0i-W0wQyB.enc	audio/ogg; codecs=
https://mmg.whatsapp.net/d/t/AgjYSp20NvondpMAJ0Wbude6_Z5umZze-TN1kz86.enc	audio/ogg; codecs=
https://mmg-fba.whatsapp.net/d/t/Atggv52h_b4jyxw4C3u3u3h8Lz20w4918B-ekobh.enc	application/zip

Gambar 18. Media URL file Zip personal chat WA device diidentifikasi (terenkripsi)

11. Hasil Simulasi Skenario 10

Year	Year	Year	Year	
02000012200000	1	1900000000	10 0	True
02000012200000	1	00000000	0 0	False (no logs)
02000012200000	1	00000000	0 0	Handled by
02000012200000	1	00000000	0 0	True
02000012200000	1	00000000	0 0	True
02000012200000	0	00000000	0 0	True
02000012200000	0	00000000	0 0	Handled by router
02000012200000	0	00000000	0 0	True
02000012200000	0	00000000	0 0	True
02000012200000	0	00000000	0 0	True
02000012200000	0	00000000	0 0	Exception (no action)
02000012200000	1	00000000	0 0	True
02000012200000	0	00000000	0 0	True
02000012200000	0	00000000	0 0	True
02000012200000	0	00000000	0 0	True
02000012200000	1	00000000	0 0	Good path, does not return

Gambar 19. Isi pesan teks *group chat* WA device diidentifikasi

12. Hasil Simulasi Skenario 11

media_name_type	media_vsa_type	media_vsa	media_name
video	0	0	video
video/mp4	3	3020004	VID-20180216-WA00007.mp4
image	1	51940	IMG-20180216-WA00008.jpg
image	0	0	image
image	0	0	image
image	0	0	image
image/jpg	1	178312	image

Gambar 20. Nama file gambar *group chat* WA device diidentifikasi

[illegible]

Gambar 21. Media *URL file* gambar *group chat* WA device diidentifikasi (terenkripsi)

16. Hasil Simulasi Skenario 15



Gambar 27. Pesan *locatin group chat* WA device diidentifikasi



Gambar 28. Media *URL* pesan *location group chat* WA device diidentifikasi (tidak terenkripsi)

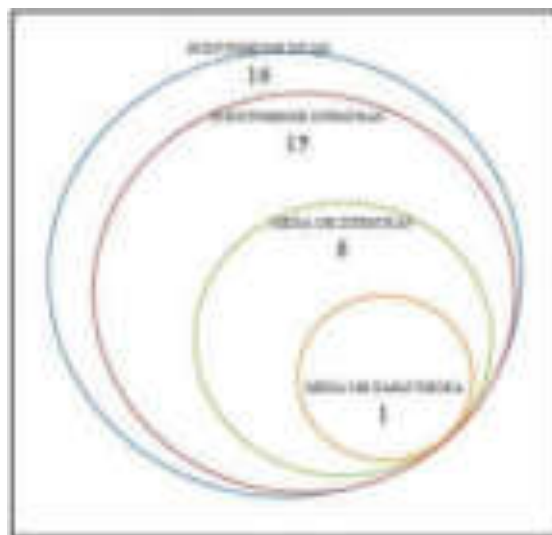
Media *URL* pesan *location* merupakan satu-satunya media *URL* yang dapat dibuka. Karena merupakan media ekstension sehingga tidak terenkripsi oleh *WhatsApp Messenger*.

4.5 Hasil Keseluruhan Analisis

Berikut ini merupakan rekapitulasi hasil keseluruhan analisis dari skenario yang telah dijalankan dengan menggunakan DB Browser for SQLite:

Tabel 4. Hasil analisis data WA menggunakan DB Browser for SQLite

No	Data Yang Dicari	Bukti Forensik		Media <i>URL</i>	
		Ada	Tidak	Ada	Tidak
1	Nama akun <i>WhatsApp messenger</i>		√	-	-
2	Nomor akun <i>WhatsApp messenger</i>	√		-	-
3	Daftar nama kontak pada <i>WhatsApp Messenger</i>	√		-	-
4	Daftar nomor kontak pada <i>WhatsApp Messenger</i>	√		-	-
5	<i>Group chat WhatsApp Messenger</i>	√		-	-
6	Anggota <i>group WhatsApp Messenger</i>	√		-	-
7	Pesan teks pada <i>chat personal</i>	√		-	-
8	Pesan <i>file</i> gambar pada <i>personal chat</i>	√			√
9	Pesan <i>file</i> video pada <i>personal chat</i>	√			√
10	Pesan <i>file</i> dokumen pada <i>personal chat</i>	√			√
11	Pesan teks pada <i>group chat</i>	√		-	-
12	Pesan <i>file</i> gambar pada <i>group chat</i>	√			√
13	Pesan <i>file</i> video pada <i>group chat</i>	√			√
14	Pesan <i>file</i> dokumen pada <i>group chat</i>	√			√
15	Pesan <i>voice note</i> pada <i>group chat</i>	√			√
16	Pesan <i>location</i> pada <i>group chat</i>	√		√	



Gambar 29. Diagram rumusan keseluruhan bukti forensik WA messenger

V. Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan hasil dari tahapan-tahapan metode simulasi yang telah dilakukan, proses pencarian dan analisa bukti forensik pada aplikasi *WhatsApp messenger* yang diakses pada *smartphone Android* dapat disimpulkan bahwa jenis-jenis data pada aplikasi *WhatsApp messenger* sebagian besar disimpan oleh server dengan diisolasi dengan prosedur enkripsi. Namun terdapat pula yang tersimpan pada memori internal perangkat *Android* yang hanya dapat diakses setelah perangkat *Android* melalui proses *root*.

Berdasarkan tabel hasil semua skenario pencarian bukti forensik yang telah ditemukan sebelumnya, pada aplikasi *WhatsApp messenger* hampir semua bukti forensik dapat ditemukan. Bukti forensik jejak yang ditemukan dalam database *WhatsApp messenger* adalah nomor akun *WhatsApp messenger*, daftar nama dan nomor kontak WA, *group chat* WA, data pesan teks, pesan gambar, pesan video, pesan file dokumen *zip*, pesan *voice note*, pesan *location maps*. Namun media URL pesan gambar, video, file dokumen *zip*, dan *voice note* tidak dapat dibuka karena terenkripsi oleh *WhatsApp messenger*. Hanya pesan *location maps* saja yang bisa dibuka media URL nya dengan *browser*.

5.2 Saran

Dalam pengembangan penelitian selanjutnya agar menjadi lebih baik karena penelitian ini masih memiliki banyak kekurangan dan keterbatasan. Berikut saran untuk penelitian selanjutnya, diantaranya:

1. Melakukan pencarian bukti forensik lebih lanjut pada aplikasi *WhatsApp messenger* untuk menemukan bukti forensik yang tidak berhasil ditemukan, seperti nama akun *WhatsApp messenger*.
2. Melakukan dekripsi bukti forensik berupa media URL yang terenkripsi oleh *WhatsApp messenger*, sehingga media URL dapat terbuka untuk menjadikan bukti yang lebih akurat.
3. Menggunakan aplikasi *instant messaging* atau media sosial lainnya serta perangkat *smartphone android* dengan sistem operasi lainnya untuk melakukan analisa dan pencarian bukti forensik.

VI. Daftar Pustaka

- [1] Anglano, C. (2014). *Forensic Analysis of WhatsApp Messenger on Android Smartphones*. Elsevier. Computer Science Institute, Universita del Piemonte Orientale, Italy.
- [2] Mukti, W.A. (2017). *Analisa Dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook Dan Twitter Pada Smartphone Android*. Skripsi Teknik Informatika Universitas Islam Negeri Syarif Hidayatullah. Jakarta.
- [3] Indrajit, R. E. (2012). *Forensik Komputer*. Forensik Komputer.
- [4] Kemp, S. (2017, April 26). *Digital in 2016*. Retrieved from We Are Social. Website <https://wearesocial.com/uk/special-reports/state-internet-q2-2017>

- [5] Mahajan, A., Dahiya, M.S., & Sanghvi, H.P. (2015, April). Forensic Analysis of Instant Messenger Application on Android Devices. *International Journal of Computer Applications* (0975-8887). Gujarat Forensic Sciences University. India.
- [6] Madani, S. A., J. K., & Mahlknecht, S. (2010). Wireless sensor networks : modeling and simulation.
- [7] Mutawa, N. A., Baggili, & Marrington. (2012). Forensic analysis of social networking applications on mobile devices. *Digital Investigation*.
- [8] Nugroho, D. R., Suadi, W., & Pratomo, B. A. (2010). Implementasi Sistem Manajemen Database untuk SQLite di Sistem Android. *Android Database SQLite*.
- [9] Raharjo, B. (2013). Sekilas Mengenai Forensik Digital.
- [10] Sfaat, N. (2012). *Pemrograman Aplikasi Mobile Smartphone*. Bandung: Informatika.
- [11] Staff, A. (2012, Juli 18). *Social Media's Role In Law Enforcement Growing*. Retrieved from Breaking Gov Website: <http://breakinggov.com/2012/07/18/social-medias-role-in-law-enforcement-growing/>.
- [12] Thakur, N.S. (2013). Forensic Analysis of WhatsApp on Android Smartphones. University of New Orleans Theses and Dissertation.
- [13] Webster. R (2014, Desember 19). The Growing Problem of Cybercrime. Retrieved from Instant Checkmate. Website: <http://www.russellwebster.com/the-growing-problem-of-cybercrime/>
- [14] Wilson, C. (2015, September 15). *Android Phone Forensic Analysis*. Retrieved from Data Forensic: <http://www.dataforensics.org/android-phone-forensics-analysis/>
- [15] Yadi, I. Z., & Kunang, Y. N. (2014). Analisis Forensik pada Platform Android. *Konferensi Nasional Ilmu Komputer (KONIK) 2014*.