



Analisa Forensics Terhadap Database Sqlite pada Aplikasi IMO Berbasis Android

Muhammad Kukuh Tri Haryanto

12917209

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Digital Forensk

Program Studi Magister Teknik Informatika

Program Pascasarjana Fakultas Teknologi Industri

Universitas Islam Indonesia

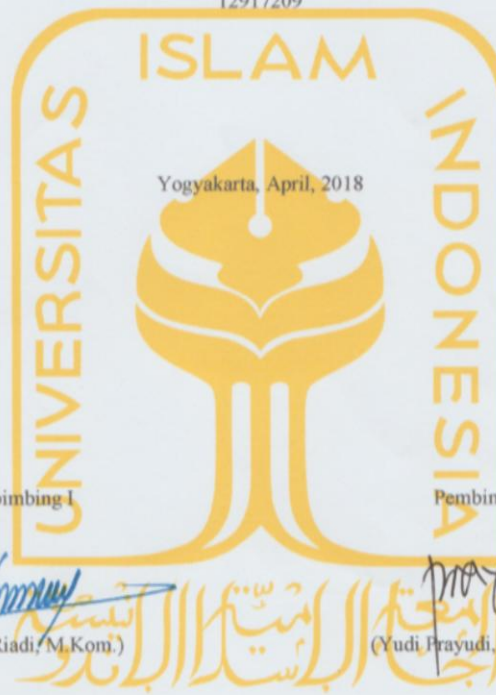
2018

Lembar Pengesahan Pembimbing

Analisa Forensics terhadap Database Sqlite pada Aplikasi IMO Berbasis Android

Muhammad Kukuh Tri Haryanto

12917209



Yogyakarta, April, 2018

Pembimbing I

(Dr. Imam Riadi, M.Kom.)

Pembimbing II

(Yudi Prayudi, S.Si, M.Kom.)

Lembar Pengesahan Penguji

Analisa Forensics terhadap Database Sqlite pada Aplikasi IMO Berbasis Android

Muhammad Kukuh Tri Haryanto

12917209



Yogyakarta, April, 2018

Tim Penguji,

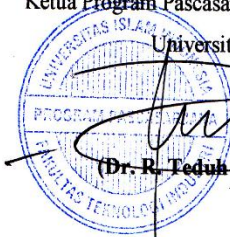
Dr. Imam Riadi, M. Kom
Ketua

Yudi Prayudi, S. Si., M. Kom
Anggota I

Dr. Bambang Sugiantoro, S. Si., M. T
Anggota II

Mengetahui,

Ketua Program Pascasarjana Fakultas Teknologi Industri
Universitas Islam Indonesia



(Dr. R. Teduh Dirgahayu, ST., M. Sc)

Abstrak

Analisis Forensics Terhadap Database Sqlite pada Aplikasi IMO Berbasis Android

Internet merupakan hasil inovasi teknologi yang bersifat praktis, sedangkan sosial media sebuah media untuk bersosialisasi satu sama lain dan dilakukan secara online hingga memungkinkan manusia untuk saling berinteraksi tanpa dibatasi oleh ruang dan waktu. Instan Messenger adalah proses pengiriman pesan secara cepat melalui perantara jaringan internet. Sedangkan aplikasi Instan Messenger digunakan oleh sebagian besar orang di dunia karena layanan pesan berpusat pada operator yang rendah pembiayaannya. Pengujian forensik digital sering melakukan analisis terhadap aplikasi Instan Messenger pada perangkat android.

Untuk saat ini aplikasi Instan Messenger selalu menjadi area penelitian utama bagi pemeriksaan forensik. Mempertimbangkan karya penelitian yang ada di bidang ini, maka akan difokuskan untuk melakukan analisa forensik Instan Messenger untuk aplikasi IMO berbasis android. Pengujian akan dilakukan pada dua perangkat smartphone yakni Samsung Tab 3.8 dan Samsung GT-S5312. Skenario yang dilakukan dengan pemasangan aplikasi IMO pada setiap android, selanjutnya dilakukan komunikasi chat dalam bentuk teks, video dan gambar. Dari aktivitas tersebut dilakukan akuisisi sehingga didapatkan isi struktur folder IMO yang selanjutnya dianalisa untuk mendapatkan bukti digital.

Hasil pengujian menunjukkan bahwa struktur folder dalam aplikasi IMO dapat dianalisis dengan proses akuisisi dan disimpan pada internal perangkat android terdiri dari 6 folder, dimana 2 foldernya memiliki sub folder yang terdiri dari gambar, teks dan video dari kegiatan pengguna dan dapat dipelajari oleh pemeriksa forensik.

Kata Kunci

Aplikasi instant messenger, perangkat android, IMO, struktur folder dan isinya, pemeriksa forensik.

Abstract

The Forensic Analisis of SQLite Data in IMO Application on Android Devices

Internet in the result of technological innovations the are practical eventhough social media is medium for socializing each others and it is done online to enable humans interacting without bieng limited by space and time. Instant messenger is the process of sending messages quickly through internet network intermediaries.while instant messenger applications are used by most people in the world because the message service centered on the operator of low-financing.Digital forensics testing often performs an analysis of Instant Messenger application on android devices.

Nowadays Instant messenger applications have always been became the main research for forensic investigators. Considering the existing research work in this field, this study will be focused on performing Instant Messenger forensic analysis for android based IMO applications. Testing will be done on two smartphone devices namely Samsung Tab 3.8 and Samsung GT-S312. The scenarios are done by installing IMO application on every android,mchatting communication in the form of text, video and picture become the next step. Because of these activities, aquisition process are carried out to get the contents of IMO folders structure which is then analyzed to obtain digital evidences.

The results indicated that the structure folder in the IMO application can be analyzed by the acquisition process and stored it on the internal android device which are consisted of 6 folders, 2 folders of them have subfolders that are consisted of images, text, and video from users and it can be studied by forensic examiner.

Keywords

Instant messenger application, android devices, IMO, structure of folders and contents, forensic examiners.

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, April 2018



Muhammad Kukuh Tri Haryanto

Halaman Kontribusi

Kontribusi dari pihak terkait dalam penyelesaian penulisan tesis ini:

1. Bapak Dr. Imam Riadi selaku Pembimbing I, Bapak Yudi Prayudi, S. Si., M. Kom selaku pembimbing II dan Bapak Dr. Bambang Sugiantoro, MT selaku dosen penguji yang telah memberikan arahan – arahnya kepada penulis, sehingga penulisan tesis ini selesai dengan baik.
2. Ibuku tercinta yang telah mendanai biaya perkuliahan sehingga bisa selesai masa studinya sampai dengan tahap pembuatan tesis ini.
3. Kakakku Siti Rojiah dan Adik ku Hexa, terima kasih atas bantuan biaya kuliah selama ini.
4. Mas Windi dan Mas Andik yang telah memberikan masukan saran dan motivasi sehingga terselesaikan revisi thesis ini

Halaman Persembahan

Allah akan meninggikan orang-orang yang beriman diantaramu dan orang-orang yang diberi ilmu pengetahuan beberapa derajat (QS Al-Mujadilah : 11)

Alhamdulillah..Alhamdulillah..Alhamdulillahirobbil'alamin..

Karya ini saya persembahkan kepada: Ayahanda Drs. Sugito Harun (alm), Nenek Rono Rejo (alm) dan Ibunda Suharmini, yang senantiasa menjadi orang tua yang luar biasa karena tidak pernah putus asa dalam usaha membesarkan dan mendidik anak-anaknya. Keluarga besar, yang selalu memberikan semangatnya dalam usahaku menuntut ilmu selama ini.

Hanya sebuah karya kecil dan untaian kata-kata ini yang dapat saya persembahkan kepada pembaca semua. Saya mohon maaf sebesar-besarnya atas segala kekhilafan salah dan kekuranganku. Semoga karya kecil ini bermanfaat untuk semua pembaca dan dapat di ambil hikmahnya.

Kata Pengantar

Penulis ucapkan rasa syukur kepada ALLAH SWT yang selalu memberikan kesehatan dan keselamatan pada diri penulis sehingga dapat menyelesaikan tesis dengan judul: **“ANALISIS FORENSIK DATA SQLITE DALAM APLIKASI IMO PADA PERANGKAT ANDROID”** sebagai persyaratan untuk mencapai gelar Magister Teknik Informatika pada program Pasca Sarjana Universitas Islam Indonesia.

Pada kesempatan ini dengan penuh kerendahan hati penulis haturkan ucapan terima kasih yang tak terhingga dan penghargaan yang setinggi-tingginya kepada Ayahanda DRS. Sugito Harun (alm) dan Ibunda Suharmini, dan Keluarga besar saya yang selalu memberikan motivasi, doa dan kasih sayangnya kepada penulis.

Di samping itu, secara khusus penulis ucapkan terima kasih yang sebesar- besarnya kepada:

1. Bapak Nandang Sutrisno, S.H., LL.M., M. Hum., Ph.D sebagai Rektor Universitas Islam Indonesia Yogyakarta
2. Bapak Direktur Program Pascasarjana, R. Teduh Dirgahayu, ST., M.Sc., dan para Asisten direktur atas segala fasilitas yang telah diberikan selama penulis menempuh studi.
3. Bapak Dr. Imam Riadi, M. Kom selaku dosen pembimbing I, terima kasih atas segala bantuan dan dukungan, semangat dan pengetahuannya serta kemudahan yang diberikan.
4. Bapak Yudi Prayudi, S.Si., M.Kom, selaku Ketua PUSFID Fakultas Teknologi Industri Universitas Islam Indonesia Yogyakarta sekaligus Pembimbing II yang telah memberikan motivasi dan semangat serta bimbingan yang sangat berarti bagi penulis dalam menyelesaikan tesis ini.
5. Seluruh Dosen dan Staff Universitas Islam Indonesia Yogyakarta khususnya Fakultas Teknologi Industri, yang baik secara langsung maupun tidak langsung telah membantu penulis selama masa-masa studi penulis.

6. Rekan-rekan mahasiswa Forensik Digital khususnya angkatan VII dan VIII yang selama ini berjuang bersama dan selalu memberikan semangat satu sama lain dalam penyelesaian tesis ini.
7. Semua pihak yang telah membantu penulis selama penyusunan karya ini yang tidak dapat penulis sebutkan satu persatu.

Semoga Allah SWT senantiasa memberikan rahmat dan anugerah-Nya yang berlimpah kepada beliau-beliau yang tersebut di atas, penulis menyadari sepenuhnya bahwa dalam karya ini terdapat banyak kekurangan, oleh karena itu semua saran dan kritik dari pembaca selanjutnya diharapkan, Akhirnya harapan penulis semoga tesis ini dapat bermanfaat dalam bidang ilmu pengetahuan kedepannya..

Yogyakarta, April 2018



Muhammad Kukuh Tri Haryanto, S. Kom

Daftar Isi

Lembar Pengesahan Pembimbing	i
Lembar Pengesahan Penguji.....	ii
Abstract	iv
Pernyataan Keaslian Tulisan	v
Halaman Kontribusi.....	vi
Halaman Persembahan	vii
Kata Pengantar.....	viii
Daftar Isi	x
Daftar Tabel.....	xii
Daftar Gambar	xiii
BAB 1 Pendahuluan	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Penelitian Terkait	4
1.7 Metode Penelitian	4
1.8 Review Penelitian	5
1.9 Sistematika Penulisan	10
BAB 2 Tinjauan Pustaka	11
2.1 Perkembangan Sosial Media.....	11
2.2 Forensik Digital	13

2.3	Mobile Forensik	15
2.3.1	Bukti Digital Terkait Mobile Forensik	17
2.3.2	Tantangan Dalam Mobile Forensik	17
2.4	Android	19
2.4.1	Aquisisi Handphone Android	22
2.5	Aplikasi Instant Messenger IMO	22
2.6	Sqlite	23
BAB 3 Metode Penelitian.....		26
3.1	Studi Pustaka.....	26
3.2	Simulasi dan Skenario pada Aplikasi IMO di Android	27
3.3	Penyusunan Skenario	28
3.4	Akuisisi	29
3.5	Analisis	30
BAB 4 Hasil dan Pembahasan.....		31
4.1	Simulasi.....	31
4.2	Cara memperoleh Data	31
BAB 5 Kesimpulan dan Saran.....		43
5.1	Kesimpulan	43
5.2	Saran	43
Daftar Pustaka		44

Daftar Tabel

Tabel 1-1 Tabel Literatur Review	6
Tabel 1-2 Tabel Literatur Review yang mendekati	9
Tabel 3-1 Kebutuhan Perangkat Lunak	28
Tabel 4-1 Nilai hash Smartphone Samsung Tab. 3.8	33
Tabel 4-2 Nilai hash Samsung GT – S 5312	33
Tabel 4-3 Direktori pada Aplikasi IMO	35
Tabel 4-4 Tabel Image (Gambar) pada folder cache	36
Tabel 4-5 Tabel Video pada folder Exocache	37

Daftar Gambar

Gambar 1-1 Data Pengguna Media Internet di Dunia	1
Gambar 1-2 Grafik Prosentase Pengguna Aplikasi Instant Messenger	2
Gambar 1-3 Langkah-langkah Penelitian	4
Gambar 2-1 Hasil Survey Media Sosial 2017	11
Gambar 2-2 Hasil Survey Media Sosial Tahun 2016	11
Gambar 2-3 Hasil Survey Pengguna Mobile pada Tahun 2017	12
Gambar 2-4 Hasil Survey Pengguna Mobile dengan Berbagai Platform	12
Gambar 2-5 Grafik Pengguna	13
Gambar 2-6 Android Arsitektur	20
Gambar 3-1 Langkah-langkah penelitian	26
Gambar 3-2 Alur Studi Pustaka	27
Gambar 3-3 Langkah Simulasi	28
Gambar 3-4 Proses Akuisisi Data	29
Gambar 4-1 Proses Akuisisi Data	32
Gambar 4-2 Proses Hash	33
Gambar 4-3 Proses dan Hasil Imaging	34
Gambar 4-4 Stuktur Folder dalam IMO	34
Gambar 4-5 File database di IMO	38
Gambar 4-6 File database account_db	38
Gambar 4-7 File tabel <i>calls_only</i> pada database <i>immofriends</i>	39
Gambar 4-8 File tabel <i>friends</i> pada database <i>immofr iends</i>	39
Gambar 4-9 File tabel <i>imo_phonebook</i> pada database <i>immofriends</i>	40
Gambar 4-10 File tabel <i>messages</i> pada database <i>immofriends</i>	40
Gambar 4-11 Tabel <i>phone_numbers</i> pada database <i>immofriends</i>	41
Gambar 4-12 Tabel <i>phone_entries</i> pada database <i>immofriends</i>	41
Gambar 4-13 video_message pada database <i>immofriends</i>	42

BAB 1

Pendahuluan

1.1 Latar Belakang

Internet dan Sosial Media merupakan hasil inovasi teknologi yang bersifat praktis, instant dan global sebagai sarana untuk berbagi Informasi dan Teknologi. Menurut analisa We Are Social's yakni sebagai sebuah agensi marketing melaporkan bahwa banyaknya data pengguna mobile sosial user dan media sosial di seluruh Dunia mencapai jumlah 3.773 untuk pengguna Internet dengan 4.917 jutanya adalah mobile user. (<https://wearesocial.com/special-reports/digital-in-2017-global>.)

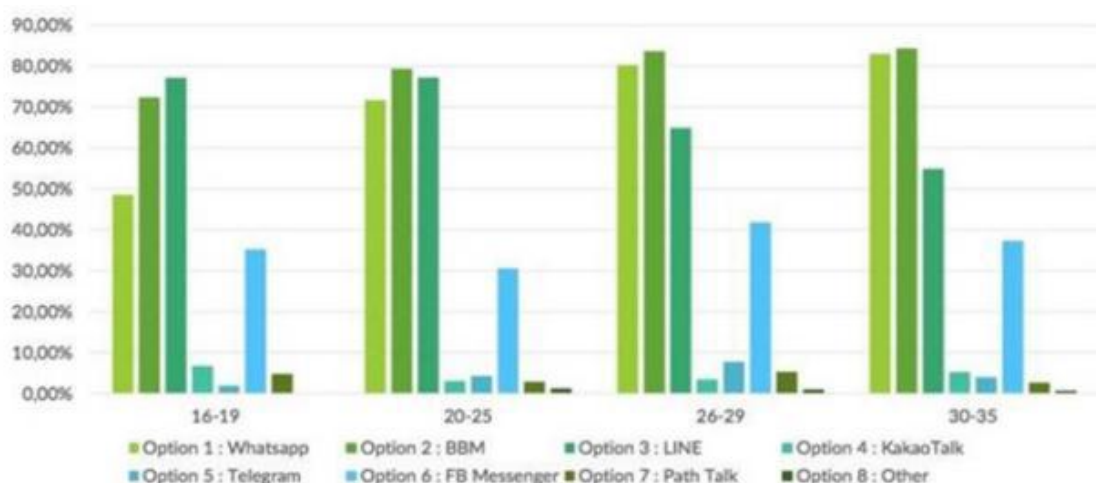


Gambar 1-1 Data Pengguna Media Internet di Dunia

Data survei pengguna Instant Messenger di Indonesia yang dilakukan oleh lembaga survei *online* JakPat (data awal tahun 2016), bahwa pengguna Blackberry Messenger merilis hasil surveynya sebagai berikut pengguna Blackberry Messenger menempati peringkat pertama dengan prosentase 80,31 % pengguna disusul WhatsApp dengan prosentase 72,78 % pengguna, dan di posisi ketiga adalah LINE dengan prosentase 71,33 persen (lihat

—Gambar 1-1). beberapa Instant Messenger yang telah di survey oleh Jacpat terdapat Instant Messenger yang lain di antaranya Telegram, WeChat, KakaoTalk, IMO. Selama ini beberapa Instant Messenger digunakan juga untuk sarana transaksi, hal ini terlihat pada iklan baik yang online maupun offline yang menyertakan nomor-nomor Instant Messenger sebagai contact personnya. Publik selama ini belum punya kemampuan untuk membedakan kontak person tersebut digunakan untuk sarana kejahatan atau bukan.

Laporan yang dikeluarkan oleh RSA Anti Fraud Command Center (AFCC), menyebutkan bahwa dari tahun 2013 hingga 2015 terjadi peningkatan aktivitas cybercrime mencapai 173% di seluruh dunia dengan total kerugian mencapai angka US\$ 325 Milyar. Laporan tersebut juga melaporkan bahwa pada tahun 2015 sebesar 45% transaksi dilakukan melalui saluran mobile sedangkan sebesar 61% penipuan terjadi melalui perangkat mobile (Fauzan, Riadi, & Fadlil, 2017)



Gambar 1-2 Grafik Prosentase Pengguna Aplikasi Instant Messenger

Penggunaan social media dan Instant Messenger dalam beberapa tahun terakhir ini terbukti menjadi alternatif sebagai media berkomunikasi yang berbiaya murah. salah satunya IMO Messenger. Aplikasi IMO menawarkan transmisi data secara real time melalui internet yang memungkinkan penggunaanya dapat mengirimkan pesan teks obrolan grup, pembagian foto, video, video dan panggilan audio.

Pelaku kejahatan juga memanfaatkan aplikasi Instant Messenger untuk aktivitas ilegal mereka di seperti Phishing atau aktifitas hacker, penipuan, trafficking, dan kejahatan cyber

lainnya. IMO sebagai salah satu Instant Messenger juga berpotensi untuk digunakan sebagai sarana tindak kejahatan seperti cyber stalking (penggunaan internet/ alat elektronik untuk melecehkan seseorang, sekelompok orang atau organisasi tertentu), sextortion (pemerasan seksual di dunia maya), drug trafficking (kejahatan perdagangan narkoba).

Instant Messenger IMO pernah diteliti oleh (Deb, 2012) yang hanya menerangkan letak direktori data, tetapi dalam penelitian tersebut belum meneliti secara detail isi direktori database yang ada pada Instant Messenger IMO, di dalam penelitian ini akan lebih menjabarkan Isi dari Direktori Instant Messenger yang terletak di *com.imo.android.imoim* yang didalamnya terdapat file berupa pesan teks, image, dan video.

1.2 Rumusan Masalah

Agar penelitian ini lebih fokus dan terarah sesuai dengan latar belakang, maka dalam penelitian ini rumusan masalah adalah sebagai berikut

- a) Bagaimana cara mengambil struktur folder pada instant messenger imo berbasis android ?
- b) File apa saja yang tersimpan dalam Instant Messenger IMO ?

1.3 Batasan Masalah

Agar lebih fokus dalam pembahasan tentang kejahatan melalui *instant massanger* maka dalam penelitian ini hanya membahas tentang aplikasi Instant messenger IMO.

1.4 Tujuan Penelitian

Ada tujuan yang ingin dicapai dalam penelitian ini adalah

- a. Mendapatkan data melalui proses forensik dan akusisi dari smartphone melalui proses Forensik di Linux dan SQLite.
- b. Mengenali / menemukan data di direktory Instant Messenger khusus nya IMO.

1.5 Manfaat Penelitian

Dari uraian yang telah dipaparkan pada latar belakang dan rumusan masalah, adapun manfaat yang ingin di capai dalam penelitian ini adalah

- a. Menemukan barang bukti digital
- b. Diharapkan proses ini bisa menambah kepustakaan dibidang ilmu digital forensik khususnya mobile forensik.

1.6 Penelitian Terkait

Pada bagian ini akan dibahas ulasan tentang penelitian yang telah dilakukan sebelumnya berkaitan dengan penelitian yang akan dilakukan mengenai Instant Messenger. Pada penelitian ini dilakukan oleh (Iqbal, Marrington, & Baggili, 2014) menyatakan bahwa mereka melakukan penelitian untuk memperoleh dan menganalisa bukti digital yang ada pada smartphone yang terinstal sebuah Aplikasi Instant Messenger. Dalam kasus ini dapat merekonstruksi data berupa teks dengan menggunakan Plutil dan Sqlite Database Browser (Iqbal, Marrington & Baggili, 2014)

Yudi Prayudi dalam penelitiannya yang membahas tentang Analisa Forensik pada smartphone membahas penerapan forensika digital pada Blackberry sama prosedurnya dengan smartphone lainnya sebagaimana prosedur yang dikemukakan oleh ACPO. Di mana hasil penelitiannya berupa data yang diekstrak dari storage, daftar contact dan memory card device barang bukti antara lain adalah : foto, memo, voicenotes, history call, sms dan messenger dari pelaku. (Prayudi & Iqbal, 2013). Swasti Bhushan Deb dan Sudhir Misr dalam penelitiannya tentang Instant Massanger, membahas Aplikasi Instant Messenger Hike dimana dalam penelitiannya memperoleh data yang ada pada direktory Aplikasi Hike yang secara detail dapat di kenali, sedangkan untuk Instant Messenger IMO peneliti sebelumnya hanya dapat mengenali root direktorinya saja (Deb, 2012)

1.7 Metode Penelitian

NIST (*National Institute of Standards and Technology*) atau The National Bureau of Standards adalah sebuah badan non-regulator dari bagian Administrasi Teknologi dari Departemen Perdagangan Amerika Serikat menyatakan bahwa untuk melakukan pengujian semua tools dan device dalam melakukan lingkungan pengujian untuk dicantumkan. Berikut langkah-langkah yang akan di lakukan :



Gambar 1-3 Langkah-langkah Penelitian

A. Perangkat Simulasi

- a. Samsung Tab 3.8
- b. Samsung Galaxy Young
- c. Micro Usb Cable
- d. Card Reader
- e. Windows 7 dan Linux Santoku 16.10 platforms untuk Akusisi
- f. DB Browser for SQLite dan SQLiteman

B. Skenario

Dalam melakukan analisis forensik untuk mendapatkan artefak sehingga kegiatan ini perlu dilakukan pembuatan skenario secara rinci terhadap aplikasi IMO sebagai berikut :

- a. Installasi aplikasi IMO dan menambahkan teman
- b. Menggunakan fitur chat text dan memberikan pesan
- c. Mengirimkan foto dan menerima foto
- d. Mengirim dan menerima emoji
- e. Melakukan video chat dan berbagi video

1.8 Review Penelitian

Pada bagian ini akan dibahas ulasan tentang penelitian yang telah dilakukan secara relevan dan berkaitan dengan penelitian yang akan dilakukan Instant Messenger. Penelitian diawali oleh (Choi, Park, & Kim, 2017) dimana penelitian yang dilakukan membahas tentang enkripsi data pada database di (Choi et al., 2017), KakaoTalk dimana file database belum terenkripsi. Tujuan dari penelitian ini adalah bagaimana memberikan Enkripsi pada KakaoTalk messenger.

(Ming & Xie, 2017) meneliti tentang live forensik (Remote Live Forensics for Android Devices) tersebut menggunakan Framework Droid GRR. Tujuan penelitian ini adalah untuk mengintegrasikan GRR Rapid Response forensic framework pada android. (Anwar & Riadi, 2017) membahas tentang Analisis Forensik WhatsApp Messenger smartphone pada Web, dimana tujuan dari penelitian ini adalah tentang Mobile Forensic Analysis dan Investigation pada smartphone Android dan aplikasi ganda berbasis web browser. (Zamroni, Umar, & Riadi, 2016) Penelitian ini memaparkan langkah-langkah forensik yang dilakukan seperti ekstraksi artefak, dekripsi, dan analisis data dari aplikasi WhatsApp pada perangkat seluler berbasis Android dan tujuan penelitian ini adalah untuk dapat melakukan ekstraksi artefak komunikasi dari aplikasi WhatsApp.

Tabel 1-1 Tabel Literatur Review

Paper Utama	Judul	Isi Penelitian	Tujuan
(Racioppo & Murthy, 2012)	Android Forensics: A Case Study of the "HTC Incredible" Phone	Dalam penelitian yang dilakukan akusisi pada phone HTC menggunakan Kernel Linux dan AccessData FTK Imager	Mengetahui directory data pada HTC phone
(Yadi & Kunang, 2014)	Analisis Forensik Pada Platform Android	Penelitian adalah untuk mengevaluasi kinerja tool ekstraksi yang mendukung ponsel Android. Dengan menggunakan berbagai literatur di bidang forensik digital dan metode ekstraksi data serta kriteria dan metodologi yang bisa digunakan untuk bisa melakukan evaluasi. Tiga perangkat lunak yang berbeda dievaluasi serta dibandingkan dengan proses ekstraksi manual pada dua perangkat ponsel Android. Data forensik aktual dalam perangkat mobile kemudian diidentifikasi dan dihitung. Kemudian dibandingkan dengan hasil ekstraksi data dari tiga tools forensik android yang diuji serta dievaluasi berdasarkan kelengkapan data yang bisa dikumpulkan serta fitur masing-masing tool	Penelitian ini memberikan gambaran tahapan yang bisa diterapkan di bidang analisis forensik android serta kriteria evaluasi tool yang bisa digunakan sebagai referensi pemilihan tool forensik android.

Tabel 1 1 Tabel Literatur Review (Lanjutan)

(Iqbal et al., 2014)	Forensic artifacts of the ChatON Instant Messaging application	Dalam Penelitian yang di lakukannya forensik artifact ChatOn berhasil menemukan data berupa teks dengan menggunakan Plutil dan Sqlite Database Browser	Mengetahui directory data teks pada device iPhone yang berjalan pada iOS 6 dan Samsung Galaxy Android 4.1
(Zamroni et al., 2016)	Analisis Forensik Aplikasi Instant Messaging Berbasis Android	Penelitian ini memaparkan langkah-langkah forensik yang dilakukan seperti ekstraksi artifak, dekripsi, dan analisis data dari aplikasi WA pada perangkat seluler berbasis Android	Penelitian berhasil melakukan ekstraksi artifak komunikasi dari aplikasi WhatsApp
(Kunang & Khristian, 2016)	Implementasi Prosedur Forensik untuk Analisis Artefak Whatsapp pada Ponsel Android	Analisis forensik khususnya untuk aplikasi pertukaran pesan seperti WhatsApp pada smartphone	Analisis forensic yang dilakukan pada penelitian ini berhasil mendapatkan artefak bukti berupa sesi chat, avatar, no kontak pada aplikasi WhatsApp, voice notes, foto profil, identitas pemilik akun WhatsApp dan juga bisa mendapatkan file media lainnya dan yang terpenting file database backup yang terenkripsi

Tabel 1 1 Tabel Literatur Review (Lanjutan)

Paper Utama	Judul	Isi Penelitian	Tujuan
(Choi et al., 2017)	Forensic analysis of the backup database file in KakaoTalk messenger	Dalam Penelitian yang dilakukan back up database file di KakaoTalk mendapatkan File yang belum terenkripsi	Peneliti berusaha emberikan Enkripsi pada KakaoTalk messenger
(Ming & Xie, 2017)	Remote Live Forensics for Android Devices	Dalam Penelitian (Remote Live Forensics for Android Devices) tersebut menggunakan Framework DroidGRR	Mengintegrasikan GRR Rapid Response forensic framework pada android
(anwar & Riadi, 2017)	Analisis Investigasi Forensik WhatsApp MessengerSmartphone Terhadap WhatsApp Berbasis Web	Analisis Forensik WhatsApp Messenger smartphone pada Web	Penelitian ini dapat bermanfaat untuk Mobile Forensic Analysis dan Investigation pada smartphone Android dan aplikasi ganda berbasis web browser

Tabel 1-2 Tabel Literatur Review yang mendekati

Paper Utama	Judul	Isi Penelitian	Tujuan
(Deb, 2012)	The Forensic Investigation of Hike Messenger and Imo Application on Android Devices	Dalam penelitian ini forensik data lebih membahas aplikasi Hike	Mengetahui Log chat yang ada di Hike Messenger
Usulan Penelitian			
	Analisa Forensics Terhadap Database Sqlite pada Aplikasi IMO berbasis Android	Melakukan Analisa barang bukti Digital yang terdapat pada aplikasi IMO dengan sistem operasi android	Mendapatkan Database SQLite dan File lainnya pada Folder com.imo.android.imoim/cache yang bisa dijadikan barangbukti digital pada aplikasi IMO

1.9 Sistematika Penulisan

Tahapan ini merupakan gambaran secara umum terkait sistematika penulisan, dengan tujuan memberikan gambaran secara ringkas terkait kerangka penulisan.

BAB I Pendahuluan

Tahapan ini merupakan tahapan awal yang dilakukan dalam penelitian. Pada tahapan ini berisikan penjelasan terkait latar belakang masalah penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB II Landasan Teori

Pada tahapan ini berisikan penjelasan mengenai beberapa teori yang mendukung penelitian yang sedang dilakukan. Teori tersebut terkait *Analisa Forensics terhadap Database Sqlite pada Aplikasi IMO Berbasis Android*

BAB III Metodologi Penelitian

Bab ini berisikan gambaran secara umum tentang analisa yang dilakukan terhadap proses dan mekanisme akusisi database pada Aplikasi IMO berbasis Android

BAB IV Hasil dan Pembahasan

Pada tahapan ini membahas tentang hasil implementasi dari proses akuisisi data pada Aplikasi IMO berbasis Android

BAB V Kesimpulan dan Saran

Tahapan ini merupakan tahapan akhir yang dilakukan peneliti dengan memaparkan kesimpulan dari keseluruhan uraian pada setiap Bab sebelumnya, serta saran untuk pengembangan penelitian berikutnya.

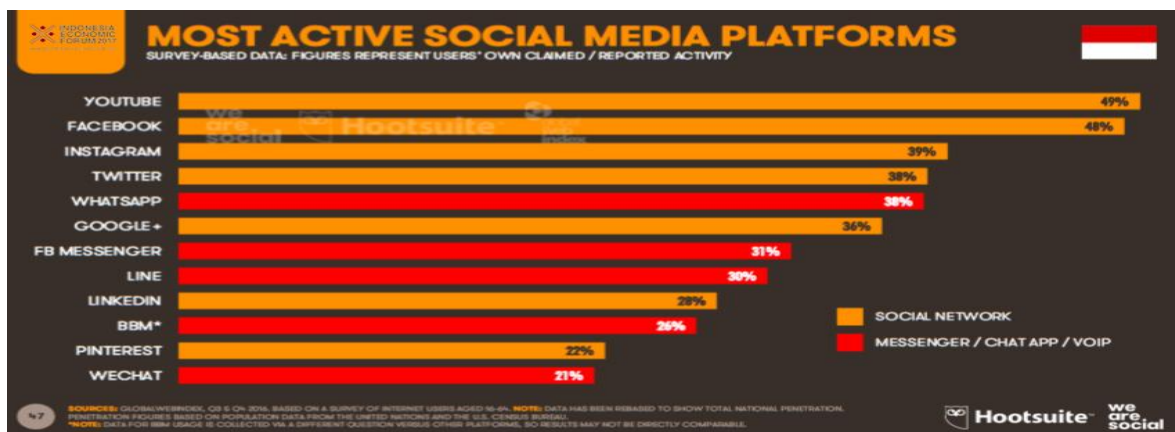
BAB 2

Tinjauan Pustaka

2.1 Perkembangan Sosial Media

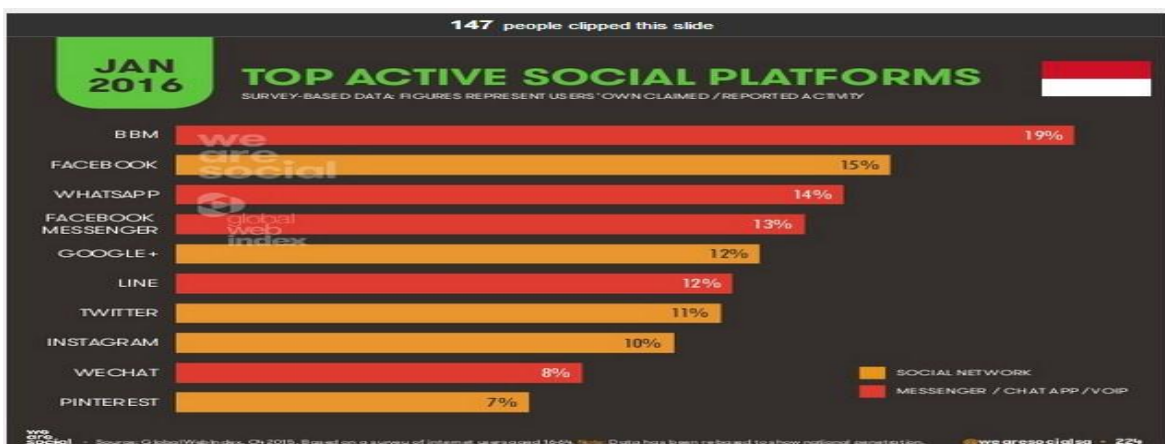
Sebagian besar masyarakat Indonesia mengakses internet menggunakan perangkat mobile mereka dengan jumlah 377 juta lebih, ini berarti melebihi populasi penduduk Indonesia. Bisa diartikan juga sebagian masyarakat memiliki 2 kartu SIM atau memiliki lebih dari satu handphone untuk mengakses internet.

Hasil survei Januari 2017 pada gambar 2.1 tentang media sosial dan aplikasi youtube menempati urutan pertama berbeda dengan survey tahun 2016 pada Gambar 2.2 yang menempatkan BBM di urutan pertama.



Gambar 2-1 Hasil Survey Media Sosial 2017

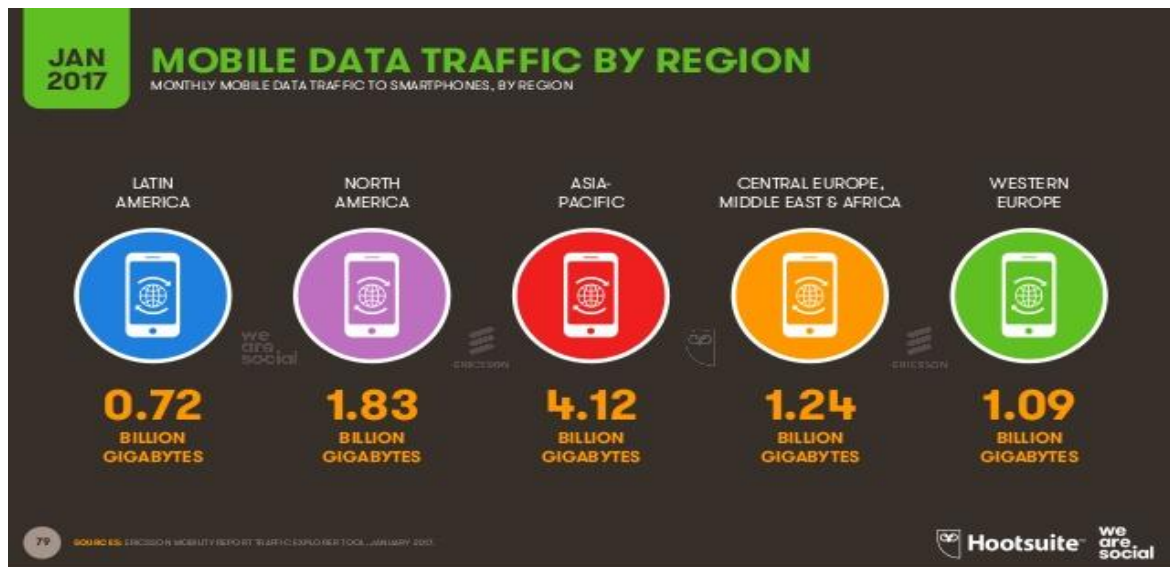
(<https://Wearesocial.Com/Special-Reports/Digital-in-2017-Global-Overview.>)



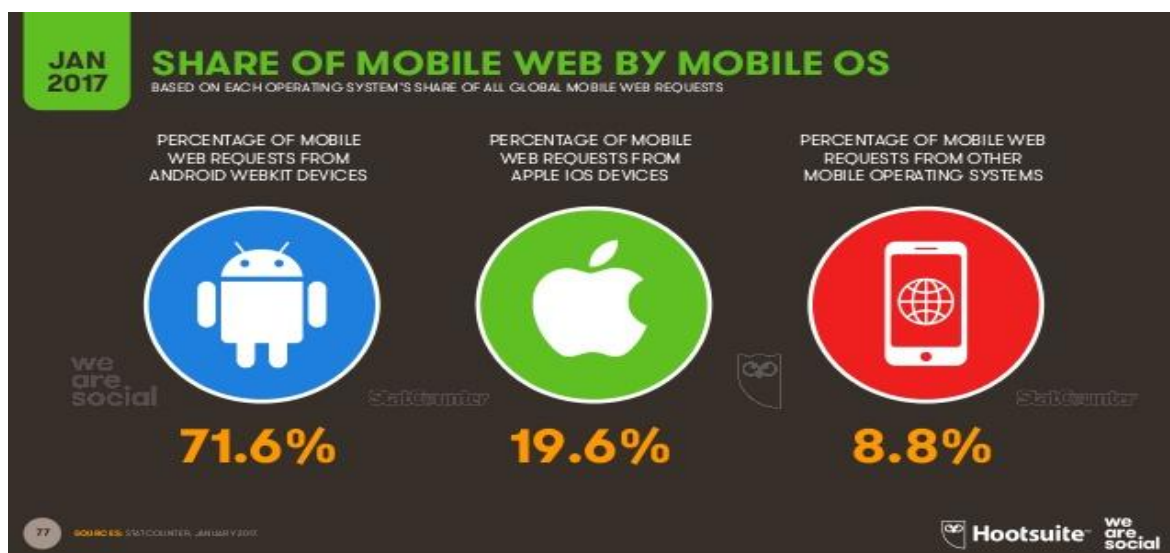
Gambar 2-2 Hasil Survey Media Sosial Tahun 2016

(<https://wearesocial.com/uk/special-reports/digital-in-2016.>)

Dalam perkembangannya Asia termasuk Indonesia menempati urutan ketiga dalam penggunaan perangkat mobile dengan jumlah pengguna 4.12 juta pada gambar 2.3 dan sebagian besar menggunakan Android sebagai Platformnya pada gambar 2.4 yang Android di urutan pertama

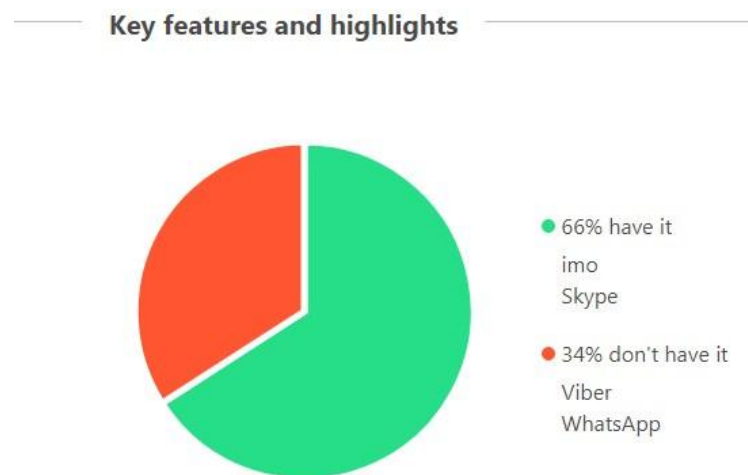


Gambar 2-3 Hasil Survey Pengguna Mobile pada Tahun 2017
(<https://wearesocial.com/special-reports/digital-in-2017-global>.)



Gambar 2-4 Hasil Survey Pengguna Mobile dengan Berbagai Platform
(<https://wearesocial.com/special-reports/digital-in-2017-global>)

Sejak dirilis tahun 2011 yang lalu, Instant massanger IMO yang dikembangkan oleh imo.im sebagai perangkat Aplikasi yang mendukung sistem operasi android secara bertahap melakukan perbaikan featurenya walaupun kalah dengan whatsapp, viber dan skype. berikut prosentase pengguna Instant Massanger IMO



Gambar 2-5 Grafik Pengguna
(<https://versus.com/en/imo-vs-viber-vs-whatsapp>)

2.2 Forensik Digital

Menurut (Miller, Grand, Fondell, & Anthony, 2006) definisi forensik digital : *“The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.”* Dimana penggunaan metode secara ilmiah terhadap preservation, collection, validation, identification, analysis, interpretation, documentation and presentation yang berasal dari bukti digital untuk tujuan memfasilitas dan merekontruksi terhadap tindak kejahatan dan terhadap tindakan tidak sah terhadap suatu operasi yang telah direncanakan. (Miller et al., 2006). Menurut Muh. Azhar seorang ahli digital forensik, forensik digital adalah aplikasi ilmu pengetahuan dan teknologi komputer untuk memeriksa dan menganalisa setiap barang bukti elektronik dan barang bukti digital dalam rangka melihat keterkaitan antara bukti digital yang satu dengan yang lain, sehingga kejahatan

tersebut menjadi terang dan keberadaan pelaku dapat di lacak kemudian di tangkap demi mempertanggungjawabkan kejahatannya (Al-Azhar, 2012).

Hal yang perlu di pahami seorang ahli forensik digital adalah prinsip dasarnya dalam hal ini ACPO (*Association Of Chief Police Officers*) England Wales & Nireland adalah salah satu lembaga hukum di United Kingdom (UK) bidang penegakan hukum menyatakan bahwa prinsip-prinsip dasar sebagai berikut (Williams, 2012):

- a. Tidak ada tindakan dari lembaga penegak hukum atau agen untuk mengubah data yang telah disimpan di komputer atau media penyimpanan yang selanjutnya dapat diandalkan di pengadilan;
- b. Dalam keadaan apapun seseorang merasa perlu untuk mengakses data asli yang disimpan di komputer atau media penyimpanan, orang tersebut harus kompeten untuk melakukannya dan dapat memberikan bukti yang bisa menjelaskan relevansi dan implikasi dari tindakan mereka;
- c. Jejak audit atau catatan semua proses yang diterapkan pada bukti elektronik berbasis komputer harus dibuat dan dipelihara/dirawat. Pihak ketiga yang independen harus dapat memeriksa proses-proses tersebut dan mencapai hasil yang sama;
- d. Orang yang bertanggung jawab atas penyelidikan (petugas kasus) memiliki tanggung jawab sepenuhnya untuk memastikan bahwa hukum dan prinsip-prinsip penyelidikan ditaati.

Dari keempat prinsip diatas dapat di simpulkan bahwa lembaga atau penegak hukum dilarang merubah data digital yang nantinya akan dipertanggungjawabkan di pengadilan, bahwa seseorang yang mempunyai kewenangan terhadap barang bukti digital dipastikan kompetensinya dan dapat menjelaskan tindakan serta analisis terhadap barang bukti digital. Beberapa catatan teknis terhadap langkah-langkah yang telah di lakukan ini untuk menjaga bila pihak ketiga mengakses barang bukti digital akan memperoleh hasil yang sama dan yang terakhir adalah seseorang yang telah melakukan pemeriksaan barang bukti harus dapat memastikan bahwa proses yang dilakukan berdasarkan hukum yang berlaku sesuai prinsip-prinsip dasar dan dapat di presentasikan dengan baik.

2.3 Mobile Forensik

Mobile forensik adalah salah satu cabang keilmuan dari forensik digital yang memulihkan bukti digital atau data dari mobile phone dibawah kondisi forensik suara dengan metode yang dapat di pertanggungjawabkan (Harrill & Mislan, 2007). Forensik digital sangat berkembang pesat dengan peningkatan pada perangkat mobile.

Penyelidikan forensik perangkat mobile pada umumnya di mulai dengan nomor telepon yang dihubungi, menjawab telepon di terima atau tidak, nomor telepon yang di simpan dan pesan text yang dikirim diterima maupun yang dihapus. Kemampuan handphone atau smartphone meningkatkan kinerja, kapasitas penyimpanan dan kemampuan multimedia mengubah handphone atau smartphone menjadi penampung data yang dapat menyimpan berbagai informasi (Punja & Mislan, 2008).

Dari sudut pandang forensik digital dalam hal ini melakukan investigasi pada perangkat mobile dapat memberikan banyak barang bukti tentang pengguna dan kemampuan lain terkait pemulihan informasi tambahan sebagai barang bukti (Ayers, Jansen, & Brothers, 2014). Menurut pendapat dari (Ayers et al., 2014) Mobile Forensik merupakan ilmu atau keahlian dalam proses dan mengelola barang bukti digital yang berasal dari mobile devices, handphone/cell-phone, tablets dan berbagai istilah serta varian sejenis lainnya dengan metode yang dapat dipertanggung jawabkan. Pada prinsipnya mobile forensik memiliki kesamaan metode dengan digital forensik yang sudah ada, hanya saja kita mengubah *point of view* dari target bukti digital yang biasanya terdapat pada perangkat *computer desktop* atau *notebook* kemudian beralih pada perangkat telepon bergerak atau *mobile devices* perbedaan yang sangat besar terdapat pada sisi teknis pelaksanaannya. Mobile forensik merupakan respon digital forensik terhadap perkembangan teknologi informasi yang telah mengevolusi perangkat komputer tradisional menjadi komputer tablet dan dunia telekomunikasi yang telah mengaplikasikan komputer dengan sangat baik sehingga menjadi smartphone.

Sehingga ketergantungan manusia terhadap perangkat telekomunikasi saat ini sangatlah besar hampir semua tugas sederhana dari prinsip kerja komputer telah dapat diaplikasikan. Kemajuan teknologi ini juga mempengaruhi perubahan gaya hidup dan cara bersosialisasi masyarakat modern saat ini yang mau tidak mau juga banyak melibatkan teknologi ini dalam setiap aktivitas manusia baik itu positif dan negatif termasuk diantaranya

aktivitas yang berhubungan dengan kejahatan. Banyak modus operandi yang terjadi dengan melibatkan perangkat telekomunikasi bergerak bahkan popularitas *smartphone* juga menjadi ladang baru yang sangat menarik bagi hacker dalam kejahatan dunia maya.

Sejak pertama mobile devices mulai dihadirkan dalam persidangan dan menjadi barang bukti hukum yang sah dengan teknologi yang sangat jauh tertinggal dari *smartphone* saat ini, tantangan yang dihadapi oleh investigator digital forensics semakin hari semakin kompleks dikarenakan teknologi yang mengikutinya juga semakin lama semakin berkembang. Perbedaan mobile device tentu berbeda juga karakteristik dari hardwarenya, berbeda juga arsitektur dari sistem operasinya dan berbeda *teknologi celullarnya*. Butuh keahlian yang khusus dan proses belajar yang cukup mendalam untuk dapat menjadi ahli di bidang ini.

Seorang ahli mobile forensik harus mengerti dan paham mengenai apa itu mobile phone dan berbagai jenisnya, apa saja sistem operasi yang terdapat dalam mobile phone tersebut, mengerti bagaimana mobile forensik itu dilakukan serta prosesnya, tahu apa saja tools software, hardware yang harus digunakan pada masing-masing jenis dari mobile phone dan sistem operasinya. Untuk mencakup semua ilmu pengetahuan yang diperlukan ini, seorang ahli mobile forensik harus peka terhadap perkembangan teknologi dari mobile phone. Banyak hal yang dapat dilakukan dengan menggunakan mobile devices saat ini, kemajuan teknologi seakan membuat komputer dalam genggaman kita. Berbagai potensi manfaat dari mobile devices baik itu buruk maupun positif seiring mengikuti para penggunanya. Menurut (Al-Azhar, 2012) Terkait dengan bahasan mobile forensik, maka potensi kejahatan yang bisa dilakukan dengan menggunakan sebuah mobile devices, beberapa diantaranya adalah sebagai berikut:

1. Penyebaran pornografi (gambar dan video)
2. Transaksi data rahasia dari perusahaan
3. Sms dan mms berbau ancaman
4. Kloning SIM data untuk penipuan
5. *Spamming*
6. Penyebaran *virus* dan *trojan* yang bertujuan untuk aktivitas ilegal

2.3.1 Bukti Digital Terkait Mobile Forensik

Tujuan utama dari mobile forensik adalah mencari dan menggali berbagai informasi yang terkandung dalam mobile devices yang berpotensi sebagai alat bukti digital untuk kemudian dianalisa dan diolah agar dapat dihadirkan ke tengah persidangan sebagai alat bukti yang sah tanpa mengurangi kaedah dari aturan dan metode digital forensik sehingga hasilnya dapat dipertanggung jawabkan. Berikut adalah beberapa hal penting yang dapat berpotensi menjadi bukti digital dalam digital forensik secara umum (belum termasuk berbagai aplikasi *smartphone* teknologi terbaru):

1. Call history, phonebook, informasi data dari SIM card.
2. SMS dan MMS.
3. Internet Setting (GPRS & WAP).
4. Network informasi (GPS location).
5. Email, memo, calender events.
6. Aktivitas browsing.
7. Photo, audio files dan video, audio recording.

Banyaknya informasi yang bisa didapat dan besarnya potensi yang dimiliki oleh informasi tersebut untuk membuka tabir sebuah investigasi menjadikan mobile forensik salah satu elemen yang penting didalam digital forensik saat ini. Pesatnya kemajuan teknologi mobile devices dan semakin bertambahnya pengguna dari mobile devices itu sendiri membuat mobile forensik sangat menantang dan menjadi lahan yang menjanjikan sebagai sebuah profesi dimasa yang akan datang. Sehingga pengetahuan ini sangatlah layak jadi pilihan bagi kita yang bergelut didunia digital forensik khususnya dan dunia IT pada umumnya. Pada tahun 2013 sebuah analisa tentang design dan implementasi dalam android aplikasi secara otomatis mampu mengumpulkan data yang berguna untuk penyelidikan yang berkaitan dengan kriminal dengan menggunakan mobile device (Grover, 2013).

2.3.2 Tantangan Dalam Mobile Forensik

Forensik Digital adalah cabang ilmu forensik berfokus pada pemulihan dan investigasi data mentah yang berada di perangkat elektronik atau digital. Ponsel forensik merupakan cabang dari forensik digital yang berkaitan dengan pemulihan bukti digital dari perangkat mobile. Prinsip utama untuk pemeriksaan atau data akuisisi tidak mungkin tanpa mengubah

konfigurasi perangkat, prosedur dan perubahan harus diuji, divalidasi, dan didokumentasikan. Metodologi yang tepat dan pedoman pemeriksaan yang benar akan menghasilkan keakuratan data. Proses pemeriksaan ponsel terbagi dalam tiga kategori *seizure, acquisition dan analysis*.

Smartphone merupakan perangkat yang dapat mengirim atau menerima data dari sumber-sumber yang berbeda seperti akses wi-fi, sistem telekomunikasi dan bluetooth. Smartphone adalah sistem dinamis yang menyediakan banyak tantangan untuk pemeriksaan dalam menggali dan menganalisis bukti digital. Peningkatan pesat dalam jumlah berbagai jenis smartphone dari berbagai produsen membuat kesulitan dalam mengembangkan proses tunggal atau alat untuk memeriksa jenis perangkat. Oleh karena itu, pengetahuan dan keterampilan khusus dibutuhkan untuk memperoleh dan menganalisis perangkat.

Tantangan terbesar dalam mobile forensik ketika datang ke platform mobile adalah fakta bahwa data dapat diakses, disimpan dan disinkronisasi di beberapa perangkat. Seperti data yang stabil dan dapat cepat berubah atau dihapus untuk upaya pelestarian data. Berikut ini beberapa alasan dalam tantangan mobile forensik: (Lutes & Mislan, 2008)

1. Hardware differences: pasar didominasi dengan model yang berbeda dari ponsel dari berbagai model produsen. Pemeriksaan forensik dapat menemukan berbagai jenis model smartphone yang berbeda dalam ukuran hardware, fitur dan sistem operasi.
2. Mobile operating systems: seperti komputer dimana windows telah mendominasi pasar, perangkat mobile secara luas menggunakan sistem operasi seperti Android, Apple iOS, RIM Blackberry dan masih banyak lagi.
3. Mobile Platform security features: platform mobile modern yang berisi built in fitur keamanan untuk melindungi data pengguna dan privasi. Fitur ini sebagai rintangan dalam akuisisi dan pemeriksaan forensik.
4. Lack of resources: dengan meningkatnya jumlah smartphone peralatan yang diperlukan dalam pemeriksaan forensik dengan perangkat mobile yang lebih modern.
5. Generic state of the device: bahkan jika perangkat tampak berada dalam keadaan off, proses latar belakang mungkin masih berjalan semisal jam alarm, agenda kegiatan dan lain-lain.

6. Anti-forensic techniques: seperti data yang disembunyikan, data yang kebingungan, data pemalsuan dan penyekaan, melakukan penyelidikan atas media digital lebih sulit.
7. Dynamic nature of evidence bukti digital dapat dengan mudah diubah baik sengaja maupun dengan tidak sengaja.
8. Accidental reset: smartphone menyediakan fitur untuk mengatur ulang semuanya. Reset perangkat sengaja sambil memeriksa dapat mengakibatkan hilangnya data.
9. Device alteration: cara yang mungkin untuk mengubah perangkat dapat berkisar dari memindahkan data aplikasi, mengubah nama file, dan memodifikasi sistem operasi dalam keahlian tersangka harus diperhitungkan.
10. Passcode recovery: perangkat dilindungi dengan kode sandi, pemeriksaan forensik perlu untuk mendapat akses ke perangkat tanpa merusak data pada perangkat.
11. Communication shielding: perangkat smartphone berkomunikasi melalui jaringan selular, jaringan wifi, bluetooth, dan inframerah.
12. Lack of availability of tools: ada berbagai macam perangkat yang mungkin tidak mendukung perangkat atau melakukan fungsi yang diperlukan, sehingga kombinasi alat harus dilakukan.
13. Malicious program: perangkat mungkin berisi perangkat lunak berbahaya atau *malware* seperti virus atau *trojan*.
14. Legal issues: perangkat smartphone mungkin terlibat dalam kejahatan yang dapat menyeberangi batas geografis, untuk mengatasi masalah multi-yurisdiksi pemeriksaan.

2.4 Android

Android adalah system operasi (OS) yang di kembangkan oleh Open Handset Alliance (OHA). Aliansi ini adalah kumpulan lebih dari perusahaan yang bergerak di bidang teknologi mobile mulai dari handset manufaktur dan penyedia semikonduktor dan juga pengembang perangkat lunak termasuk Acer, ARM, Google, eBay, HTC, Intel, LG Electronics, Qualcomm, Sprint dan T-Mobile. Tujuannya adalah untuk mempercepat inovasi pengembangan perangkat mobile dan menawarkan ke pengguna lebih banyak fitur dan pengalaman menggunakan perangkat mobile serta lebih murah.



Gambar 2-6 Android Arsitektur

Didalam Android ada 4 hal penting yaitu linux kernel, libraries, android runtime dan applications seperti ditunjukkan pada gambar 2.5. Berikut penjeleasannya bahwa android menggunakan kernel linux 2.6. Ketika berjalan pada hard drive pada system device terletak pada physical hard drive atau di /dev/hd0. Selain hal itu linux hanya mengerti karakter dan perangkat block seperti keyboard dan disk drive masing-masing. Memory Technology Device (MTD) di perlukan untuk menyediakan sebuah antarmuka linux OS dan physical flash karena perangkat flash memory tidak dilihat sebagai karakter atau block device (Dedekind, 2009).

Secara umum arsitektur android di bagi 4 layer elemen, antara lain :

1. Layer Applications dan Widget

Inilah layer pertama pada OS Android, biasa dinamakan layer applications dan widget. Layer ini merupakan layer yang berhubungan dengan aplikasi-aplikasi inti yang berjalan pada Android OS. Seperti klien email, program SMS, kalender, browser, peta, kontak, dan lain-lain. Semua aplikasi ini dibuat dengan menggunakan bahasa Java. Apabila membuat aplikasi, maka aplikasi itu ada di layer ini.

2. Layer Applications Framework

Applications framework merupakan layer dimana para pembuat aplikasi menggunakan komponen-komponen yang ada di sini untuk membuat aplikasi mereka. Beberapa contoh komponen yang termasuk di dalam Applications framework adalah sebagai berikut :

- a. Views
- b. Content Provider.
- c. Resource Manager
- d. Notification Manager
- e. Activity Manager

3. Layer Libraries

Pada layer libraries inilah kita bisa temukan fitur-fitur dari Android. Untuk mengimplentasikan aplikasi biasanya mengakses libraries ini. Libraries ada dua, yaitu libraries media dimana ini memutar video dan audio, dan libraries untuk menjalankan tampilan, seperti libraries graphic, libraries SQLite untuk support data base dan masih banyak library lainnya.

4. Android RunTime

Dilayer inilah aplikasi android dapat berjalan. Android runtime dibagi jadi 2 bagian yaitu:

- a. Core Libraries : fungsinya untuk menterjemahkan bahasa Java dan C.
- b. Dalvik Virtual Machine : berfungsi sebagai virtual mesin berbasis register yang bertugas mengoptimalkan jalannya fungsi-fungsi di Android agar lebih efisien.

Android runtime sistem menggunakan mesin Dalvik virtual (VM), yang memungkinkan multipleapplications dapat dijalankan secara bersamaan karena setiap aplikasi mempunyai VM Android yang terpisah kemudian dikompilasi ke Dalvik executable (Dex) file (DalvikVM, 2008).

5. Linux Kernel

Linux Kernel inilah ini dari sistem operasi Android berada. Isinya adalah file-file sistem yang tugasnya mengelola system processing, memory, resource, drivers dan fungsi-fungsi sistem Android lain. Disini kita dapat melihat adanya kemiripan file sistem pada Android dan sistem operasi berbasis linux. Kernel disini berbasis monolithic. Pada versi linux yang digunakan versi 2.6, versi 3.x dan pada Android versi 4.0 keatas.

2.4.1 Aquisisi Handphone Android

Dalam bidang digital forensics, akuisisi dan imaging adalah tahap yang sangat crucial. Tahap ini adalah tahap awal untuk mendapatkan data yang kemudian nantinya akan dianalisis sesuai dengan kebutuhan proses investigasi. Kesalahan atau ketidakakuratan dalam proses akuisisi ini akan berakibat kualitas dan integritas data yang dianalisispun menjadi berkurang. Bahkan lebih lanjut dalam aspek hukum, kesalahan proses akuisisi data ini akan berdampak pada tidak diterimanya bukti digital yang diajukan dalam proses persidangan.

Salah satu tantangan dalam proses akuisisi data ini adalah pada bukti elektronik berupa handphone. Beragamnya jenis, sistem operasi serta type dan merek handphone adalah merupakan tantangan yang tiada henti untuk aktivitas mobile forensics. Tidak jarang aplikasi mobile forensics versi terbaru pun tidak bisa mengenali dan membaca data pada jenis handphone tertentu. Handphone dengan tingkat keamanan yang baik seperti halnya iPhone dan blackberry umumnya masih dipandang sebagai handphone yang tidak mudah dideteksi oleh aplikasi mobile forensik apapun. walaupun akhirnya dapat diakuisisi datanya, biasanya memerlukan waktu update version tertentu sehingga si vendor mengumumkan bahwa aplikasinya bisa melakukan akuisisi terhadap iPhone dan Blackberry. (Prayogo, Riadi, & Luthfi, 2017)

Sebaliknya dengan handphone produk China, kreativitas vendor-vendor handphone China juga kadang menjadi tantangan sendiri bagi aplikasi mobile forensics. Ini tidak lepas dari karakteristik sistem operasi handphone (Android) yang memberikan fleksibilitas kepada pabrikan untuk melakukan kustomisasi model dan kemampuan handphonenya. Karena itu framework analisis mobile forensics kadang sangat dipengaruhi oleh type dan merek handphonenya, sehingga sangat menyulitkan dibuatkan sebuah standard untuk analisisnya. Demikian juga untuk tahap akuisisinya. Berikut ini adalah salah satu artikel bagus untuk memberikan gambaran tentang beberapa langkah dasar untuk melakukan akuisisi sebuah handphone. (Riadi, Sunardi, & Firdonsyah, 2017)

2.5 Aplikasi Instant Messenger IMO

IMO messenger adalah aplikasi pesan mobile yang unik dimana pengguna dapat saling berkiriman video, foto, teks dan bervideo call. bisa jadi aplikasi yang menyenangkan untuk berbagi momen dalam rupa video dan foto. Pengguna juga dapat membuat video/foto

menjadi lebih ramai dengan menambahkan teks. Saat ini Imo messenger menjadi pilihan bagi remaja untuk berkomunikasi dengan orang lain karena fitur Imo lebih ringan dibandingkan WhatsApp maupun Skype, imo messenger juga memiliki fitur yang bisa dibilang sudah cukup jika dibandingkan dengan aplikasi messenger saat ini seperti grup chatting, share photo dan video, voice call, dan juga penyimpanan chat history.

Imo messenger dibuat karena melihat banyaknya pesan dalam satu hari yang dikirim ataupun diterima melalui sistem operasi iOS, Android, dan Blackberry melalui banyak sekali aplikasi messenger. Dengan banyaknya aplikasi messenger yang bisa ditampung oleh imo messenger seperti halnya tersebut sangat membantu.

Fitur imo messenger yang paling menarik adalah kemampuan untuk menghubungkan banyak akun. saat pengguna register imo, secara otomatis bisa melakukan login terhadap layanan messaging lainnya, dan imo messenger akan menghubungkan semuanya. saat pengguna login, notifikasi yang kita terima akan seperti notifikasi pada normalnya. Memang imo messenger belum dapat mengatur akun WhatsApp, LINE, WeChat, Snapchat atau KakaoTalk, tetapi seperti sejauh ini sudah cukup sekali sebagai alternatif dari aplikasi messenger. (Aji, Riadi, & Lutfhi, 2017).

Adapun berikut fitur-fitur yang dimilikinya antara lain:

- a. Web messenger
- b. Photo sharing
- c. Photo dan photo management
- d. Video chat
- e. Voice chat

Seperti halnya messenger yang lain Imo messenger bisa diakses menggunakan Internet, jaringan IMO Messenger juga Add user Google Talk, Facebook, AIM, MSN Messenger, ICQ, Skype, Jabber, MySpace, MSN Messenger, Hyves, Yahoo Messenger.

2.6 Sqlite

SQLite itu merupakan sebuah Database yang bersifat ACID-compliant dan memiliki ukuran pustaka kode yang relatif kecil, ditulis dalam bahasa C. SQLite merupakan proyek yang bersifat public domain. SQLite adalah sebuah open source database yang telah ada cukup lama, cukup stabil, dan sangat terkenal pada perangkat kecil, termasuk Android (Jeon, Bang,

& Lee, 2012). Android menyediakan database relasional yang ringan untuk setiap aplikasi menggunakan SQLite. Aplikasi dapat mengambil keuntungan dari itu untuk mengatur relational database engine untuk menyimpan data secara aman dan efisien. Untuk Android, SQLite dijadikan satu di dalam Android runtime, sehingga setiap aplikasi Android dapat membuat basis data SQLite (Meier, 2012).

SQLite merupakan suatu perpustakaan yang menerapkan mesin database self-contained, serverless, zero configuration, dan transaction. Aplikasi pengaturan waktu yang menggunakan SQLite memungkinkan SQLite digunakan pada saat ujian ataupun presentasi (Setiyadi & Harihayati, 2015).

Karena SQLite menggunakan antarmuka SQL, cukup mudah untuk digunakan orang-orang dengan pengalaman lain yang berbasis databases. Terdapat beberapa alasan mengapa SQLite sangat cocok untuk pengembangan aplikasi Android, yaitu: Database dengan konfigurasi nol. Artinya tidak ada konfigurasi database untuk para developer. Ini membuatnya relatif mudah digunakan. Tidak memiliki server. Tidak ada proses database SQLite yang berjalan (Mulyadi, 2010). Pada dasarnya satu set libraries menyediakan fungsionalitas database. Single-file database. Ini membuat keamanan database secara langsung. Open source. Hal ini membuat developer mudah dalam pengembangan aplikasi diantaranya PHP, Firefox, Chrome, iPhone dan Android adalah contoh produk yang menggunakan SQLite. Di Browser Firefox, SQLite dipakai untuk menyimpan konfigurasi, bookmark dan history website sedangkan di smartphone Android, SQLite dipakai untuk menyimpan contact. SQLite mendukung semua platform (Nugroho, 2010).

SQLite adalah embedded database yang paling terkenal, SQLite memiliki fitur-fitur sebagai berikut (Bhosale, Patil, & Patil, 2015).

- **no-dependency**, SQLite library didesain untuk mandiri dan memerlukan bantuan yang minimal dari library lain sehingga bisa mudah diaplikasikan pada aneka platform
- **serverless dan zero-configuration**, SQLite tidak memerlukan proses server yang tersendiri untuk mengakses data. Keseluruhan operasi di SQLite adalah berdasarkan konsep baca dan tulis langsung ke file di storage atau memory.

- **SQL compliance**, SQLite mendukung 90% standard SQL syntax. Hal ini akan mempermudah kurva belajar para pengembang aplikasi yang sudah terbiasa dengan SQL Programming
- **dukungan banyak platform**, SQLite memiliki kompatibilitas yang tinggi untuk diaplikasikan pada banyak platform dan beraneka jenis bahasa pemrograman.

Kelebihan Sqlite :

Database SQLite memiliki kelebihan sebagai berikut :

1. SQLite hanya menggunakan operasi read/write tanpa adanya perantara proses server tersendiri, tentunya akan membuat performance yang ditawarkan oleh SQLite menjadi jauh lebih baik apabila dibandingkan dengan database yang lain.
2. SQLite bersifat serverless dan zero configuration, akan lebih memudahkan pengembang untuk melakukan migrasi dari satu environment ke environment yang lain. Cukup dengan copy paste file-file yang diperlukan maka aplikasi dan database kita akan termigrasi dengan mudah (Prasetyo, 2006).

Kekurangan SQLite :

1. Beberapa syntax SQL standard yang tidak disupport oleh SQLite adalah perintah *right* dan *outer join*. Keamanan yang dimiliki SQLite sangat rapuh, karena cara kerja SQLite berdasarkan pada operasi baca/tulis, maka keamanan yang dimiliki oleh SQLite hanya *read* dan *write* saja, yang didasarkan pada security file system environment yang digunakan.. Semua security harus dimanage oleh business logic layer aplikasi aplikasi sehingga dibutuhkan suatu algoritma kriptografi yang dapat mengenkripsi data administrator pada database SQLite (Ariyus, 2008).
2. Reliability, untuk ukuran data yang kecil, reliability/ketahanan database SQLite mungkin lebih baik daripada database konvensional. Tapi untuk data besar hal ini akan sulit. Karena SQLite menggunakan operasi read/write secara langsung ke file. Sehingga ketika operasi write terjadi, seluruh file akan *di-lock* dan menyebabkan operasi yang lain tidak bisa berjalan. Meskipun proses locking ini terjadi hanya dalam hitungan mili bahkan mungkin micro second. Tapi jika frekuensi pengaksesan data cukup tinggi bisa jadi akan menyebabkan turunya performansi aplikasi. Dalam beberapa kasus hal ini bisa diakali dengan memecah data menjadi beberapa file yang lebih kecil.

BAB 3

Metode Penelitian

Metode adalah kegiatan ilmiah yang berkaitan dengan suatu cara kerja (sistematis) untuk memahami suatu subjek atau objek penelitian, sebagai upaya untuk menemukan jawaban yang dapat dipertanggungjawabkan secara ilmiah dan termasuk keabsahannya. (Ruslan, 2008). Untuk itu dalam tahap penelitian ini dilakukan langkah-langkah untuk menemukan jawaban terkait permasalahan terhadap aplikasi IMO yang diilustrasikan dalam Gambar 3.1 di bawah ini :



Gambar 3-1 Langkah-langkah penelitian

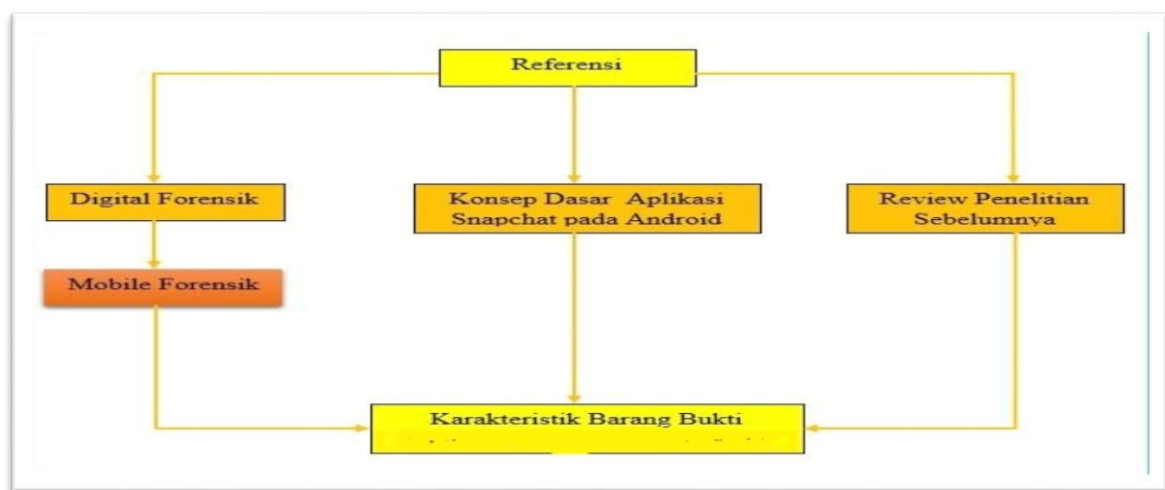
Pada langkah penelitian ini hal yang akan dilakukan yang pertama adalah melakukan studi pustaka hal ini terkait literatur-literatur terkait objek penelitian. Selanjutnya setelah menemukan objek untuk dilakukan penelitian hal kedua yang akan dilakukan yaitu melakukan simulasi kasus dan melakukan perancangan scenario untuk melakukan tahap investigasi digital forensic. Kemudian pada tahap analisis IMO hal yang akan dilakukan adalah melakukan pencarian barang bukti digital terhadap objek penelitian yang nantinya akan dilakukan analisa. Hal terakhir yang dilakukan adalah membuat pelaporan yang menjadi salah satu hal penting dalam tahapan-tahapan digital forensik.

3.1 Studi Pustaka

Studi Kepustakaan yaitu mengadakan penelitian dengan cara mempelajari dan membaca literatur-literatur yang ada hubungannya dengan permasalahan yang menjadi obyek penelitian. Sedangkan menurut Moh. Nazir dalam bukunya yang berjudul 'Metode Penelitian' mengemukakan bahwa yang dimaksud dengan: "Studi kepustakaan adalah teknik pengumpulan data dengan mengadakan studi penelaahan terhadap buku-buku, literatur-

literatur, catatan-catatan, dan laporan-laporan yang ada hubungannya dengan masalah yang dipecahkan (Nazir, 1988).

Studi kepustakaan yang dilakukan sebelum melakukan penelitian bertujuan untuk menemukan suatu masalah untuk diteliti. Dalam arti bukti-bukti atau pernyataan bahwa masalah yang akan diteliti itu belum terjawab atau belum terpecahkan secara memuaskan atau belum pernah diteliti orang mengenai tujuan, data dan metode, analisa dan hasil untuk waktu dan tempat yang sama. Untuk itu secara garis besar proses studi pustaka dapat dilihat pada Gambar 3.2 di bawah ini:



Gambar 3-2 Alur Studi Pustaka

Dalam melakukan teknik melakukan pengumpulan data terkait dengan objek penelitian, dengan mengumpulkan bahan-bahan referensi yang terkait dengan penelitian melalui buku, artikel, paper, jurnal, makalah, dan mengunjungi beberapa website yang terkait dengan mobile forensic dan arsitektur android.

3.2 Simulasi dan Skenario pada Aplikasi IMO di Android

NIST (National Institute of Standards and Technology) atau The National Bureau of Standards, adalah sebuah badan non-regulator dari bagian Administrasi Teknologi dari Departemen Perdagangan Amerika Serikat menyatakan bahwa untuk melakukan pengujian semua tools dan device dalam melakukan lingkungan pengujian untuk dicantumkan. Simulasi adalah proses yang diperlukan untuk operasionalisasi suatu model untuk meniru tingkah laku sistem yang sesungguhnya. Tujuannya untuk melakukan pembuktian terhadap rumusan masalah dalam penelitian ini. Simulasi dilakukan karena tidak memungkinkan

untuk melakukan investigasi pada kasus nyata. Simulasi dilakukan dengan melakukan penyusunan skenario seperti terlihat pada Gambar 3. 3:



Gambar 3-3 Langkah Simulasi

Simulasi akan dilakukan di Pusat Studi Digital Forensik (Pusfid) UII. Dalam melakukan simulasi dibutuhkan dua perangkat smartphone Samsung Tab 3.8 dan Samsung GT-S5312 kemudian kedua perangkat tersebut melakukan komunikasi dan saling mengirimkan chatting,kirim gambar dan video call. Tahap selanjutnya adalah melakukan akuisisi atau imaging terhadap kedua smartphone tersebut menggunakan Linux Santoku.

Adapun spesifikasi perangkat lunak / software yang digunakan untuk analisa bukti digital pada kasus ini adalah sebagai berikut:

Tabel 3-1 Kebutuhan Perangkat Lunak

No	Software	Fungsionalitas
1	Linux Santoku	Sistem operasi laptop Investigator untuk akusisi
2	SQLiteman	Perangkat Lunak untuk melihat hasil akusisi data di Linux
3	DB browser for SQLite	Perangkat lunak untuk analisa hasil akuisisi data

3.3 Penyusunan Skenario

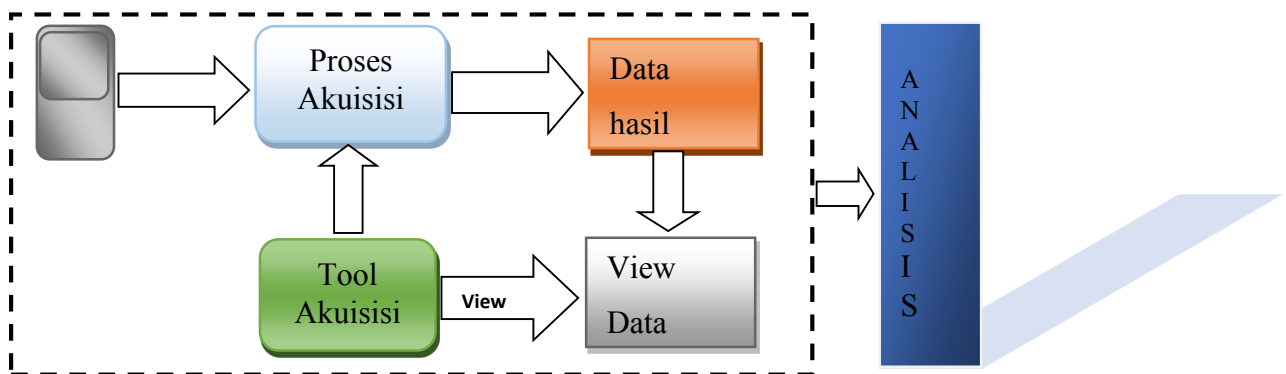
Pada langkah ini skenario yang akan dilakukan adalah sebagai berikut :

- Smartphone yang berbasis Android saling melakukan koneksi ke internet untuk melakukan komunikasi menggunakan aplikasi Instant messenger IMO

- b. Komunikasi menggunakan aplikasi IMO dengan melakukan chatting, kirim gambar dan video call sesuai dengan simulasi koneksi yang dilakukan.
- c. Pada langkah selanjutnya dilakukan akuisisi/imaging kedua smartphone tersebut menggunakan Linux untuk mendapatkan imaging yang nantinya akan dilakukan analisis.
- d. Pada langkah ini dilakukan analisis dari IMO Evidence kedua perangkat smartphone untuk mendapatkan bukti digital yang diperlukan.
- e. Tahap terakhir adalah melakukan analisa SQLite Record terhadap bukti yang di temukan untuk mendapatkan informasi-informasi penting terkait aplikasi Instant messenger IMO.

3.4 Akuisisi

Akuisisi merupakan proses imaging ataupun proses untuk mendapatkan data khususnya perangkat mobile phone yang di gunakan untuk melakukan tindakan kejahatan. Pada proses pengumpulan bukti digital ada 3 extraction techniques yang di gunakan pada perangkat mobile phone antara lain Physical Collection, Logical Collection, dan File System Extraction. (Silla, 2015)



Gambar 3-4 Proses Akuisisi Data

Dalam proses akuisisi ini memiliki beberapa tahapan umum antara lain:

1. Duplikasi forensik digital merupakan teknik menggandakan barang bukti secara identik untuk memastikan integritas hasil dan sumber.
2. Hashing dilakukan guna mengetahui derajat kesamaan pada sumber asli dari hasil duplikasi. Setelah proses forensik imaging selesai dan menghasilkan image file, maka hasil image file tersebut diperiksa untuk kecocokan nilai hash MD5.

3. Forensik ekstraksi merupakan proses di mana data diambil atau diekstrak dari file hasil forensik imaging baik menggunakan query atau tool forensik analisis.
4. Setelah mendapatkan file-file atau artifak digital yang diinginkan dari proses penyelidikan untuk mengetahui metadata, waktu, log pengguna, serta bagaimana data tersebut dapat di proses, dibaca dan dimengerti.

3.5 Analisis

Di-era yang semakin modern dan maju ini perkembangan smartphone semakin lama semakin maju. Perkembangan instan messenger juga mengalami perubahan yang semakin signifikan dengan penambahan berbagai fitur-fitur baru pada aplikasi yang berguna untuk memudahkan pengguna atau *user*. Dengan semakin berkembangnya keamanan pada smartphone yang semakin rumit dan komplek, maka dari itu perlu dilakukan proses analisa yang semakin mendalam.

Analisis adalah sekumpulan kegiatan, aktivitas dan proses yang saling berkaitan untuk memecahkan masalah atau memecahkan komponen menjadi lebih detail dan digabungkan kembali lalu ditarik kesimpulan. Melakukan analisis pada hasil pemeriksaan dengan menggunakan metode dibenarkan secara teknik dan hukum untuk mendapatkan informasi yang berguna dan dapat menjawab pertanyaan-pertanyaan yang menjadi pendorong untuk melakukan pengumpulan dan pemeriksaan. Analisa barang bukti elektronik bertujuan untuk mengambil barang bukti digital mengenai data-data yang diduga menjadi bukti tindak kejahatan dengan menggunakan SQLiteMan. SQLiteMan adalah manajemen database dapat melakukan pernyataan SQL tuning, mengelola tabel, pandangan atau pemicu, administrasi ruang database dan statistik indeks.

BAB 4

Hasil dan Pembahasan

4.1 Simulasi

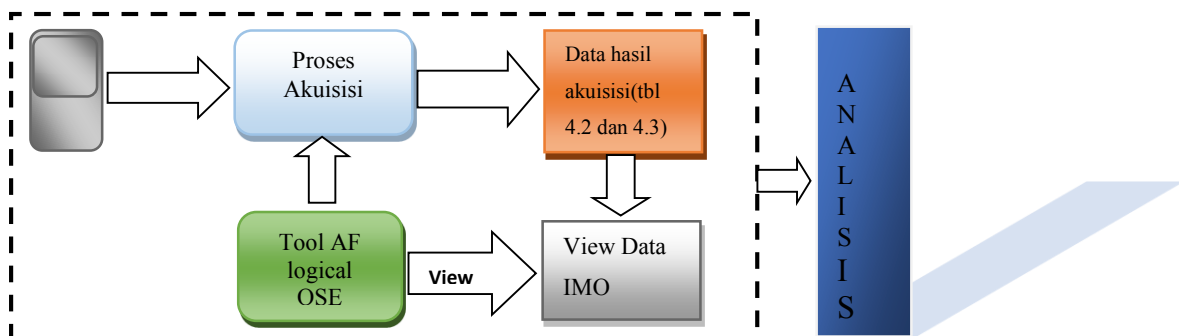
Simulasi dilakukan di Pusat Studi Digital Forensik (PUSFID) Universitas Islam Indonesia. Dalam melakukan simulasi dibutuhkan dua perangkat smartphone Samsung Tab 3.8 dan Samsung Galaxy Young berbasis Android dan terinstall aplikasi IMO kemudian kedua perangkat tersebut melakukan komunikasi dan saling mengirimkan chatting, kirim gambar dan video call. Tahap selanjutnya adalah melakukan akuisisi atau imaging terhadap kedua perangkat smartphone tersebut menggunakan PC atau Laptop yang sebelumnya terinstall Linux Santoku setelah dilakukan imaging maka dilakukan proses analisis dan kemudian dibuat laporan terhadap barang bukti tersebut.

4.2 Cara memperoleh Data

Proses imaging atau lebih terkenal dengan istilah akuisisi merupakan proses untuk mendapatkan data, khususnya pada perangkat smartphone yang digunakan untuk tindakan kejahatan. Terdapat 3 teknik ectraction yang biasa dipergunakan dalam proses pengumpulan bukti digital smartphone. Teknik – teknik tersebut adalah physical extraction, logical extraction, dan file system extraction. Physical extraction merupakan salinan bit by bit dari seluruh flash memori dari perangkat mobile dimana dengan teknik ini memungkinkan akuisisi secara utuh terhadap file yang disembunyikan atau terhapus. Logical extraction merupakan akuisisi dalam perangkat moile dengan bit for bit pada logical storage yang mencakup file dan direktori yang berada pada logical storage (file system). Akuisisi ini memungkinkan struktur data system lebih mudah untuk diextract dan diatur. File System Extraction, selanjutnya, merupakan akuisisi terhadap file yang terdapat dalam memori perangkat mobile dimana dengan teknik ini memungkinkan kita untuk mendapatkan akses semua file yang ada didalam memori perangkat mobile (allocated space), termasuk gambar, video, database file, sistem file dan log.

Penelitian studi kasus analisa forensik terhadap database pada aplikasi IMO diperoleh dari memori internal yang terinstal aplikasi IMO . Handphone yang dipergunakan

dalam studi ini ada 2 yaitu Smartphone Samsung Tab 3.8 dan Samsung GT – S 5312, yang dijadikan sebagai barang bukti dengan melakukan akuisisi yaitu suatu proses imaging untuk mendapatkan data cloning atau duplikat dengan tujuan tidak merusak barang bukti digital. Tools atau Aplikasi AF logical OSE menggunakan Aplikasi yang berjalan di system Operasi Linux Santoku. Proses Akusisi data dapat digambarkan pada gambar 4.1 sebagai berikut:



Gambar 4-1 Proses Akuisisi Data

Proses Akusisi dimulai dari melakukan kloning dari memori internal Smartphone kedalam sdcard, kemudian dilakukan proses pembuatan file ‘dd’

Untuk memastikan bahwa proses akuisisi atau imaging yang dilakukan dapat dipertanggung jawabkan atau otentik dari file back up didapatkan nilai hash sebagai berikut:

- a. Nilai hash Smartphone Samsung Tab. 3.8 ditunjukkan pada Tabel 4-1.
- b. Nilai hash Samsung GT – S 5312 ditunjukkan pada Tabel 4-2.

Dalam melakukan proses pengambilan Serial Hash pada file akusisi maka langkah – langkah yang dilakukan bisa ditunjukkan dengan gambar dibawah ini:

Md5sum /home/Santoku/forensik/gts5312.dd

Md5sum /home/Santoku/forensik/st311v2.dd

```

santoku@santoku-desktop: /
File Edit Tabs Help

santoku@santoku-desktop:/$ md5sum /home/santoku/forensik/gts5312.dd
6e20748f6f1ce77594369ddf71fd4ae20/home/santoku/forensik/gts5312.dd
santoku@santoku-desktop:/$ md5sum /home/santoku/forensik/st31lv2.dd
5903582295683c9456141aa68c20023b5/home/santoku/forensik/st31lv2.dd
santoku@santoku-desktop :/$

```

Gambar 4-2 Proses Hash

Adapun Tabel tersebut dapat dilihat dibawah ini:

Tabel 4-1 Nilai hash Smartphone Samsung Tab. 3.8

No	Name	Info
1	File Dump	Path Smartphone Samsung Tab. 3.8 Size(bytes)31.972.130.81 MD5903582295683c9456141aa68c20023b5

Tabel 4-2 Nilai hash Samsung GT – S 5312

No	Name	Info
1	File Dump	Path Samsung GT – S 5312 Size(bytes) 1.975.448.064 MD5 6e20748f6f1ce77594369ddf71fd4ae20

Dari hasil proses akusisi barang bukti Smartphone Samsung Tab 3.8 dan Samsung GT – S 5312 dengan menggunakan “AF Logical OSE” menunjukkan tidak ada kendala atau masalah, karena Sistem Operasi Linux Santoku membaca penuh driver USB. Hasil Ekstrak yang di dapat pada aplikasi *chat imo* terdiri dari beberapa folder seperti terlihat pada gambar 4.3

```
compiled options:
command line: dc3dd if=/dev/sdb1 of=/home/blacktridi/uji_forensik/data.dd has
device size: 3858297 sectors (probed)
sector size: 512 bytes (probed)
1975448064 bytes (1,8 G) copied (100%), 238,31 s, 7,9 M/s

input results for device `/dev/sdb1':
3858297 sectors in
0 bad sectors replaced by zeros
4c9a1dfb9bd7e71627016e7a28b83533 (md5)

output results for file `/home/blacktridi/uji_forensik/data.dd':
3858297 sectors out
```

Proses *running* akuisisi

Hasil Akuisisi

Activate Windows

Gambar 4-3 Proses dan Hasil Imaging yang berisi folder lib, cache, databases, files, no_backup dan shared_pref.

Racioppo & Murthy (2012) dalam studinya bertujuan untuk mengetahui isi direktori pada HTC phone. Demikian juga Iqbal et al (2014) juga bertujuan untuk mengetahui isi direktory data teks pada devise iPhone yang berjalan pada iO56 dan Samsung Galaxy Android 4.1. Namun Swati Bushan Deb & Sudir Misra (2017) yang melakukan studi kasus pada aplikasi IMO dan Hike Messenger tidak menjelaskan atau mengetahui isi dalam direktory data. Mereka hanya menjelaskan letak atau posisi direktori data pada aplikasi IMO dan Hike Messenger. Sedangkan disini penulis, menganalisa barang bukti untuk mengetahui letak dan isi data yang terdapat dalam instant messenger IMO pada 2 Smartphone Samsung Tab 3.8 dan Samsung GT – S 5312

Setelah dilakukan proses akuisisi, hasil ekstraksi dalam aplikasi chat Imo menunjukkan bahwa terdapat enam folder: folder lib, folder cache, folder database, folder files, folder no-back up, dan folder shared-pref. Hasil penemuan keenam folder dari barang bukti tersebut ditunjukkan dengan rinci dalam Gambar 4.4 dibawah ini:



Gambar 4-4 Struktur Folder dalam IMO

Dari keenam folder tersebut, terdapat beberapa folder yang terisi sub folder dan tidak ada sub folder. 4 folder tidak memiliki (lab, files, no back-up, dan shared-pref). Sedangkan 2

folder lainnya (cache dan database) memiliki sub folder. Direktori pada masing – masing folder ditunjukkan pada Tabel 4.3 dibawah ini:

Tabel 4-3 Direktori pada Aplikasi IMO

No	Nama folder	Isi folder
1	Lib	-
2	Cache	5 sub folder : - Exocache - Com.android.renderscript.cache - Image_manager_disk_cache - webviewcacheChromium - webviewcacheChromiumStaging 10 file Image
3	Database	1 sub Folder : - com.google.android.gms.ads.db 4 file database
4	Files	-
5	No_backup	-
6	Shared_prefs	-

Setelah di buka satu per satu dari folder tersebut, yang terdapat data atau barang bukti yang bisa dianalisa adalah, folder *cache* dan *folder database*. dalam kedua folder tesebut berisi kumpulan file dari aktifitas pengguna imo yang berupa file gambar dan video. Pada folder cache terdapat 10 file image dan subfolder exocache yang berisi 1 file video.

Dari data yang diperoleh menunjukkan rincian nama file, lokasi file, ukuran file, serta keterangan time stamp kapan file image tersebut dibuat. Lokasi dari semua file image terebut ada di com.imo.adroid.imoim/cache. Sedangkan tipe/jenis dari file image adalah RIFF audio. Ukuran file image bervariasi dari ukuran terbesarnya adalah 74.0 KiB, dan ukuran terkecil adalah 20.1 KiB. Rincian file image ditunjukkan pada Tabel 4.4 di bawah ini:

Tabel 4-4 Tabel Image (Gambar) pada folder cache

No	Name	Location	File Type	Total size	Size on disk	Last modification	Last access	Last permission change
1	IMG_R_200180122_103802_2.webp	com.imo.android.imoim/cache	RIFF audio	74.0 KiB	76.0 KiB	22/01/18 11:36	06/02/18 01:42	22/01/18 04:14
2	IMG_R_20180122_104014_3.webp	com.imo.android.imoim/cache	RIFF audio	44.7 KiB	48.0 KiB	22/01/18 11:39	06/02/18 01:42	22/01/18 04:14
3	IMG_R_20180121_153838_0.webp	com.imo.android.imoim/cache	RIFF audio	67,5 KiB	68,0 KiB	22/01/18 11:45	06/02/18 01:42	21/01/18 20:16
4	IMG_R_20180121_154130_1.webp	com.imo.android.imoim/cache	RIFF audio	69,2 KiB	72,0 KiB	22/01/18 11:50	06/02/18 01:42	21/01/18 20:17
5	IMG_R_20180122_081256_0.webp	com.imo.android.imoim/cache	RIFF audio	33,5 KiB	36,0 KiB	22/01/18 11:52	06/02/18 01:42	22/01/18 04:14
6	IMG_R_20180122_083137_1.webp	com.imo.android.imoim/cache	RIFF audio	33,5 KiB	36,0 KiB	22/01/18 11:55	06/02/18 01:42	22/01/18 04:14
7	IMG_R_20180122_104017_4.webp	com.imo.android.imoim/cache	RIFF audio	28,3 KiB	32,0 KiB	22/01/18 11:58	06/02/18 01:42	22/01/18 04:14

Tabel 4 4 Tabel Image (lanjutan)

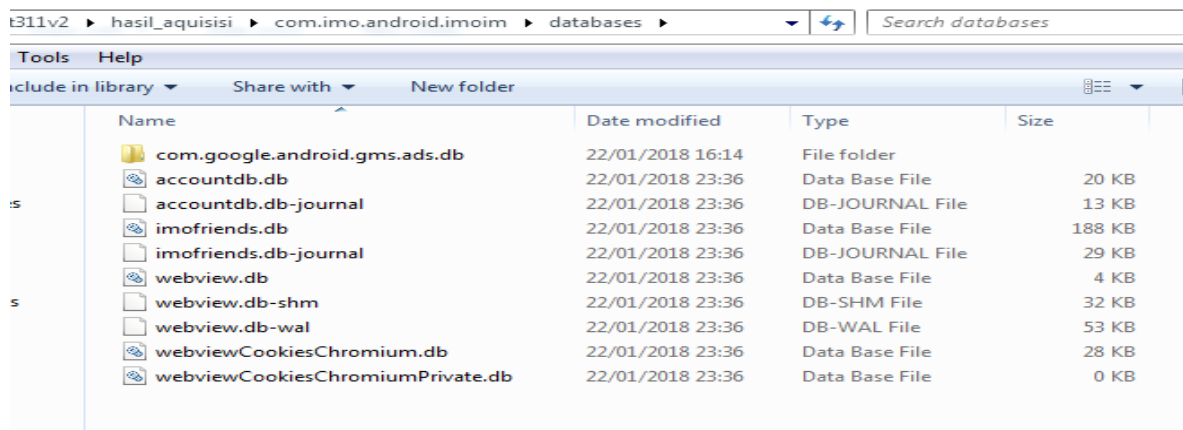
8	IMG_R_20180122_104019_5.webp	com.imo.android.imoim/cache	RIFF audio	63,9 KiB	64,0 KiB	22/01/18 11:59	06/02/18 01:42	22/01/18 04:14
9	IMG_R_20180122_104021_6.webp	com.imo.android.imoim/cache	RIFF audio	73,1 KiB	76,0 KiB	22/01/18 11:23	06/02/18 01:42	22/01/18 04:14
10	IMG_R_20180122_104023_7.webp	com.imo.android.imoim/cache	RIFF audio	24,0 KiB	22/01/18 11:26	22/01/18 11:26	06/02/18 01:42	22/01/18 04:14

Disamping 10 file image tersebut terdapat juga 1 file video yang ada dalam folder cache tersebut. Tipe dari file video tersebut adalah MPEG-4 dengan ukuran 1.1 MiB. Adapun rincian file video tersebut digambarkan pada Tabel 4.3 dibawah ini:

Tabel 4-5 Tabel Video pada folder Exocache

No	Name	Location	File Type	Total size	Size on disk	Last modification	Last access	Last permission change
1	0.0.1516591336917.v3.exo	com.imo.android.imoim/cache/exocache	MPEG-4 Video	1,1 MiB	1,1 MiB	22/01/18 11:31	06/02/18 01:48	22/01/18 04:14

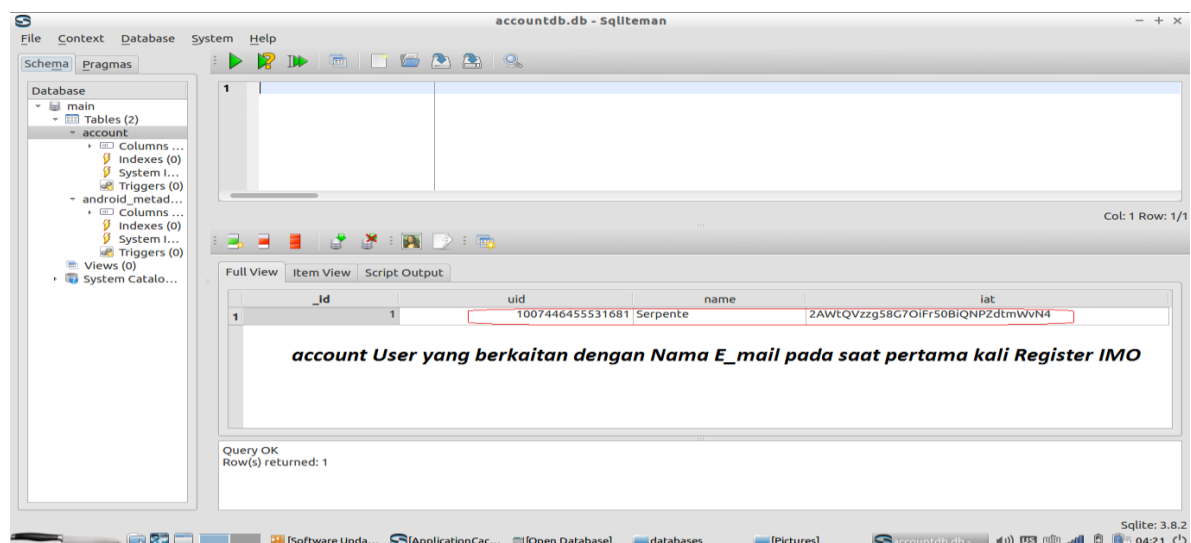
Analisa selanjutnya pada folder databases didapatkan 1 subfolder dan beberapa file yang bereksistensi SQLite (*.db) yang dapat dibuka dengan menggunakan Aplikasi SQLiteman pada Linux Santoku atau DB Browser for SQLite pada windows. File - file db tersebut bisa dilihat pada Gambar 4.5.



Name	Date modified	Type	Size
com.google.android.gms.ads.db	22/01/2018 16:14	File folder	
accountdb.db	22/01/2018 23:36	Data Base File	20 KB
accountdb.db-journal	22/01/2018 23:36	DB-JOURNAL File	13 KB
imofriends.db	22/01/2018 23:36	Data Base File	188 KB
imofriends.db-journal	22/01/2018 23:36	DB-JOURNAL File	29 KB
webview.db	22/01/2018 23:36	Data Base File	4 KB
webview.db-shm	22/01/2018 23:36	DB-SHM File	32 KB
webview.db-wal	22/01/2018 23:36	DB-WAL File	53 KB
webviewCookiesChromium.db	22/01/2018 23:36	Data Base File	28 KB
webviewCookiesChromiumPrivate.db	22/01/2018 23:36	Data Base File	0 KB

Gambar 4-5 File database di IMO

Pada Gambar 4.6 adalah file database *account_db*, terdapat dua (2) tabel yang terisi data, yaitu : tabel *account* dan *android_metadata*. Pada tabel *account* terdapat 1 user dengan nama pengguna Seperti yang mengacu pada nama email yang didaftarkan di *account* smartphone. Sedangkan di tabel *android_metadata* tidak ada isi datanya, sehingga tidak ditemukan barang bukti.



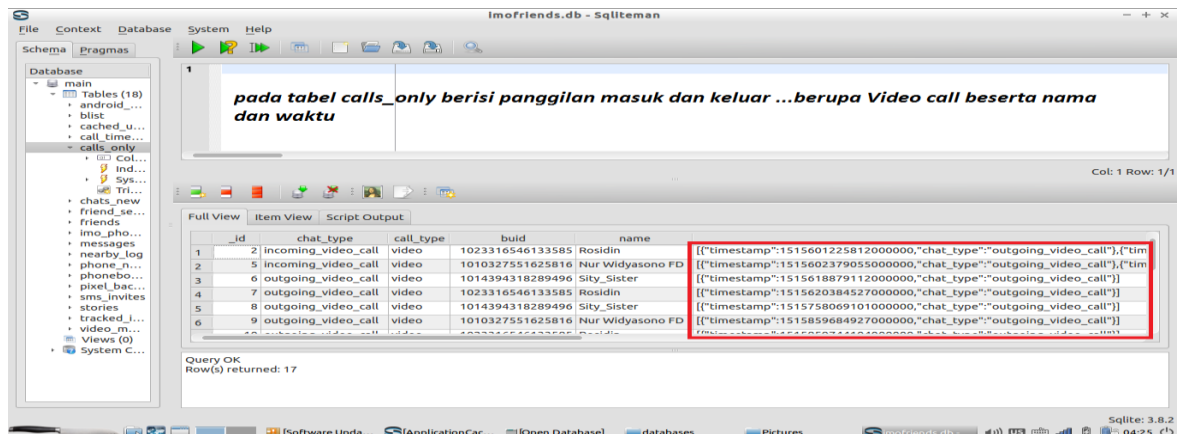
_id	uid	name	iat
1	1007446455531681	Serpente	2AWtQVzzg58G7OIFr50BIQNPZdtmWvN4

account User yang berkaitan dengan Nama E_mail pada saat pertama kali Register IMO

Query OK
Row(s) returned: 1

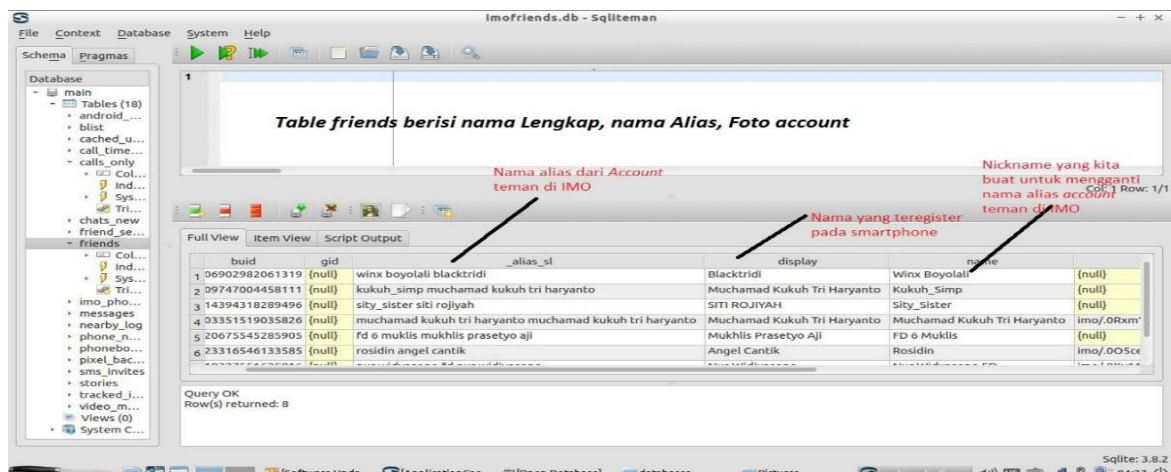
Gambar 4-6 File database *account_db*

Pada Gambar 4.7 adalah file tabel *calls_only* yang terdapat pada database *imofriends*. Tabel *calls_only* berisi log data panggilan masuk dan panggilan keluar beserta waktunya yang menggunakan tipe data time stamp, hanya saja untuk timestamp masih belum bisa diuraikan sehingga belum bisa diketahui waktu dan tanggal dari aktifitas tersebut dilakukan.



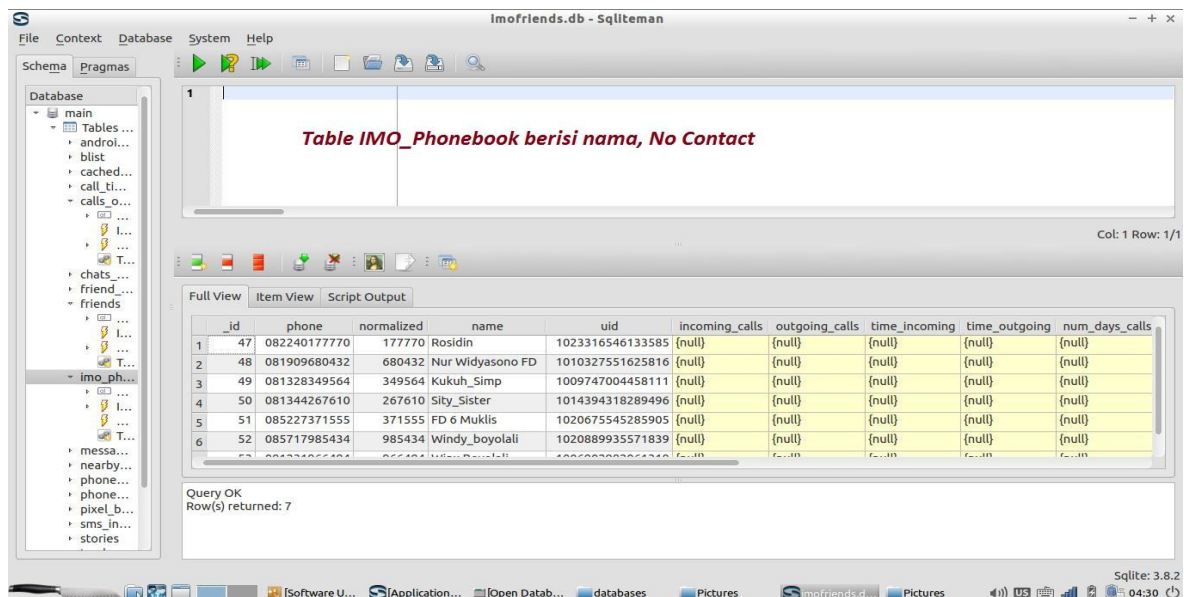
Gambar 4-7 File tabel *calls_only* pada database *immofriends*

Pada Gambar 4.8 adalah file tabel *friends* yang terdapat pada database *imofriends*. Tabel *friends* menunjukkan informasi tentang nama *user* sebagai register awal dari pemilik smartphone, nama alias yang dibuat oleh *user* pemilik smartphone yang dijadikan sebagai *nickname* pada *account* IMO tersebut dan pemberian nama *nickname* yang kita lakukan.



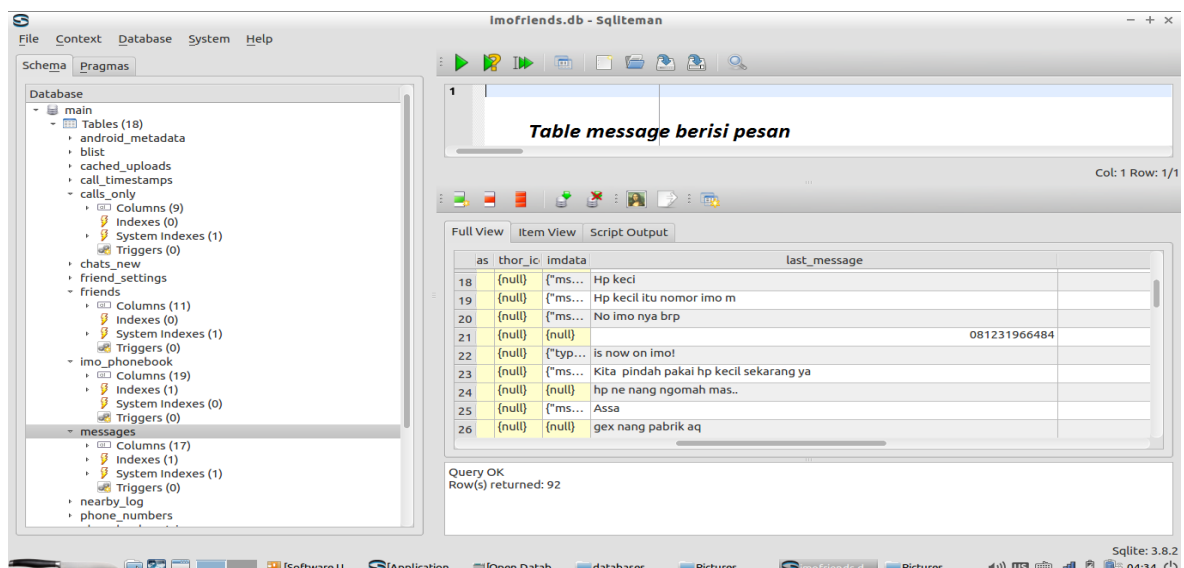
Gambar 4-8 File tabel *friends* pada database *immo friends*

Pada Gambar 4.9 adalah file tabel *imo_phonebook* yang terdapat pada database *imofriends*. Tabel *phone_book* berisi nomor kontak beserta nama pengguna.



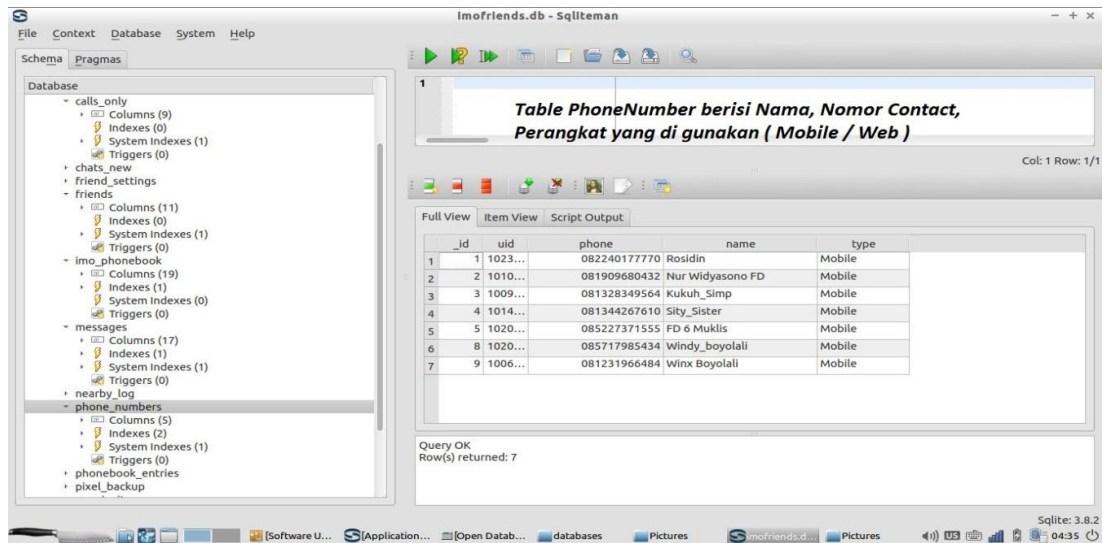
Gambar 4-9 File tabel *imo_phonebook* pada database *immofriends*

Pada Gambar 4.10 adalah file tabel *messages* yang terdapat pada database *imofriends*. Dalam tabel *messages* didapatkan history chat sebanyak 812 pesan, yang dapat diuraikan informasi pesan teks dan timestamp pesan tersebut.



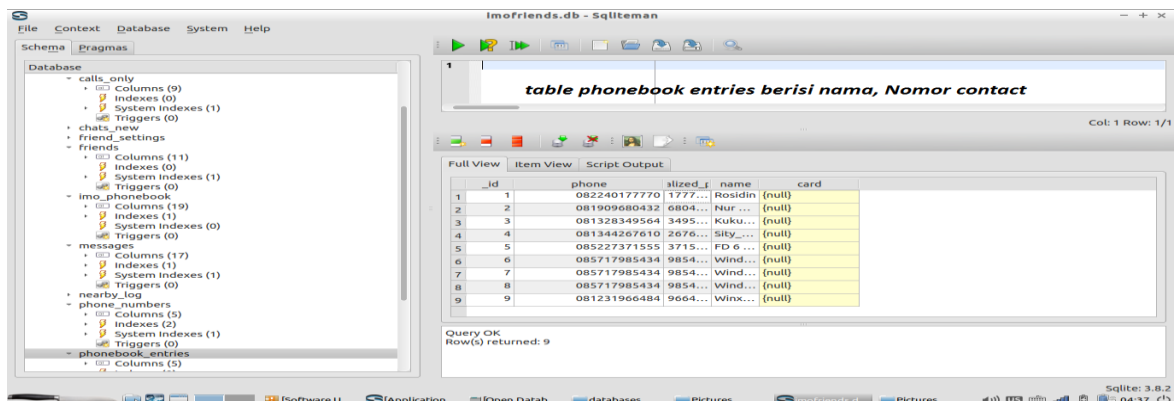
Gambar 4-10 File tabel *messages* pada database *immofriends*

Pada Gambar 4.11 adalah file tabel *phone_numbers* yang terdapat pada database *imofriends*. Tabel tersebut menunjukkan perangkat yang digunakan oleh masing-masing user (*mobile/web*).



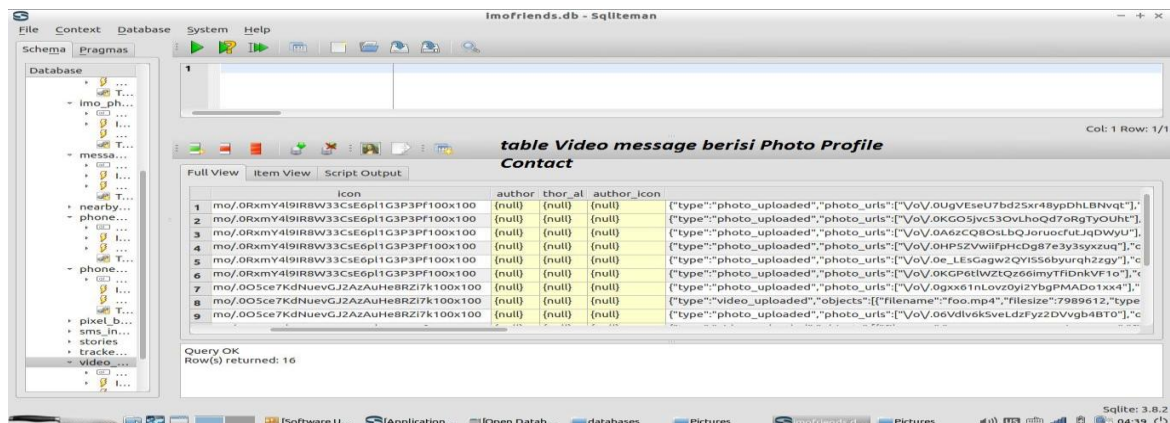
Gambar 4-11 Tabel *phone_numbers* pada database *imofriends*

Pada Gambar 4.12 adalah file tabel *phone_entries* yang terdapat pada database *imofriends*. Tabel ini berisi daftar nomor kontak beserta nama kontak.



Gambar 4-12 Tabel *phone_entries* pada database *imofriends*

Pada Gambar 4.13 adalah file tabel *phone_video message* yang terdapat pada database *imofriends*. Dari tabel *phone_video message* didapatkan informasi riwayat video call yang pernah dilakukan beserta timestamp.



Gambar 4-13 video_message pada database *immofriends*

Berdasarkan latar belakang masalah yang terjadi mengenai analisa forensik terhadap data Sqlite pada aplikasi IMO berbasis android dapat dirumuskan bahwa dalam pengambilan data tidak mengalami kendala atau masalah. Dalam hal ini sistem operasi Linux Santoku mampu membaca penuh driver USB. Dalam prosesnya menghasilkan ekstrak yang berisi beberapa folder antara lain: folderlib, cache, database, files, no_backup dan shared_pref.

Penelitian ini memberikan gambaran bagaimana melakukan akuisisi dan analisa forensik terhadap Sqlite pada aplikasi IMO berbasis android untuk mendapatkan informasi bukti forensik terkait data yang menunjukkan rincian nama file, lokasi file, ukuran file serta ketengan kapan file tersebut dibuat.

BAB 5

Kesimpulan dan Saran

5.1 Kesimpulan

Setelah dilakukan serangkaian penelitian dan analisa terhadap perangkat smartphone Samsung Tab 3.8 dan Samsung GT-S5312 terkait penelitian aplikasi IMO dapat disimpulkan sebagai berikut:

- a. Dalam penelitian ini proses akusisi menggunakan metode NIST dengan menggunakan aplikasi AF logical OSE yang berjalan di sistem linux Santoku dapat menemukan struktur folder dan isinya di aplikasi IMO.
- b. Aplikasi AF logical OSE yang berjalan di sistem linux Santoku dapat membaca dan menunjukkan bahwa terdapat 6 folder didalam aplikasi IMO yaitu lib, cache, database, files, no back_up, dan shared_pref dari keenam folder tersebut hanya folder cache dan database yang memiliki subfolder. Subfolder tersebut berisi kumpulan file gambar dan video dari aktifitas pengguna aplikasi IMO.

5.2 Saran

Pada Penelitian database SQLite pada aplikasi IMO berbasis Android ini dengan menggunakan Linux Santoku untuk akusisinya sementara ini hanya mampu menemukan Log_video call. Oleh karena itu sangat diharapkan sekali pada penelian selanjutnya mampu melakukan penelusuran file video call pada Aplikasi IMO berbasis Android

Daftar Pustaka

- Aji, M. P., Riadi, I., & Lutfhi, A. (2017). The digital forensic analysis of snapchat application using XML records. *Journal of Theoretical and Applied Information Technology*, 95(19), 4992–5002.
- Al-Azhar, M. . (2012). *Digital Forensik Panduan Praktis Investigasi Komputer*.
- anwar, nuril, & Riadi, I. (2017). Analisis Investigasi Forensik WhatsApp Messenger Smartphone Terhadap WhatsApp Berbasis Web. *Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika*, 3(1), 1–10. Retrieved from <http://journal.uad.ac.id/index.php/JITEKI/article/view/6643/3530>
- Ariyus, D. (2008). *Pengantar Ilmu Kriptografi: Teori Analisa dan Implementasi*. Yogyakarta: CV. Andi Offset.
- 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>
- Bhosale, S. T., Patil, T., & Patil, P. (2015). SQLite : Light Database System. *International Journal of Computer Science And Mobile Computing*, 4(4), 882–885.
- Choi, J., Park, J., & Kim, H. (2017). Forensic analysis of the backup database file in KakaoTalk messenger. *2017 IEEE International Conference on Big Data and Smart Computing, BigComp 2017*, 156–161. <https://doi.org/10.1109/BIGCOMP.2017.7881732>
- DalvikVM. (2008). Dalvik Virtual Machine. Retrieved from <https://www.javatpoint.com/dalvik-virtual-machine>
- Deb, S. B. (2012). The Forensic Investigation of Hike Messenger and Imo Application on Android Devices .
- Dedekind. (2009). Memory Technology Devices. Retrieved January 5, 2018, from <http://www.linux-mtd.infradead.org/faq/general.html>
- Fauzan, A., Riadi, I., & Fadlil, A. (2017). Analisis Forensik Digital Pada Line Messenger Untuk Penanganan Cybercrime. *Annual Research Seminar (ARS)*, 2(1), 159–163. Retrieved from <http://seminar.ilkom.unsri.ac.id/index.php/ars/article/view/832/752>
- Grover, J. (2013). Android forensics: Automated data collection and reporting from a mobile device. *Digital Investigation*, 10(SUPPL.). <https://doi.org/10.1016/j.diin.2013.06.002>
- Harrill, D. C., & Mislán, R. P. (2007). A Small Scale Digital Device Forensics ontology. *Small Scale Digital Device Forensics Journal*, 1(1), 1–7. <https://versus.com/en/imo-vs-viber-vs-whatsapp>. (n.d.). Retrieved from <https://wearesocial.com/special-reports/digital-in-2017-global>. (n.d.). <https://wearesocial.com/uk/special-reports/digital-in-2016>. (n.d.). Retrieved from <https://wearesocial.com/uk/special-reports/digital-in-2016>
- Iqbal, A., Marrington, A., & Baggili, I. (2014). Forensic artifacts of the ChatON Instant Messaging application. *Int. Workshop Syst. Approaches Digit. Forensics Eng., SADFE*. <https://doi.org/10.1109/SADFE.2013.6911538>
- Jeon, S., Bang, J., & Lee, S. (2012). A recovery method of deleted record for SQLite database, (August). <https://doi.org/10.1007/s00779-011-0428-7>

- Kunang, Y. N., & Khristian, A. (2016). Implementasi prosedur forensik untuk analisis artefak Whatsapp pada ponsel android. *Annual Research Seminar*, 2(1), 59–68. Retrieved from <http://ars.ilkom.unsri.ac.id>
- Lutes, K. D., & Mislán, R. P. (2008). Challenges in Mobile Phone Forensics. *Imeti 2008: International Multi-Conference on Engineering and Technological Innovation, Vol I, Proceedings*, 348–352.
- Meier, R. (2012). Professional Android 4 Application Development. *Development*, 576. <https://doi.org/9781118102275>
- Miller, D. A., Grand, J. B., Fondell, T. F., & Anthony, M. (2006). A Road Map for Digital Forensic Research. *Journal of Animal Ecology*, 75(1), 101–110. <https://doi.org/10.1111/j.1365-2656.2005.01025.x>
- Ming, J., & Xie, M. (2017). Remote live forensics for Android devices. *2016 IEEE Conference on Communications and Network Security, CNS 2016*, 374–375. <https://doi.org/10.1109/CNS.2016.7860518>
- Mulyadi. (2010). *Membuat Aplikasi untuk Android*. Yogyakarta: Multimedia Center Publishing.
- Nugroho, A. (2010). *Mengembangkan Aplikasi Basis Data Menggunakan C# dan SQLite Server*. Yogyakarta: CV. Andi Offset.
- Prasetyo, D. (2006). *Keamanan SQLite Database pada RDBMS*. Jakarta: PT Elex Media Komputindo.
- Prayogo, A., Riadi, I., & Luthfi, A. (2017). Mobile Forensics Development of Mobile Banking Application using Static Forensic. *International Journal of Computer Applications*, 160(1), 5–10. <https://doi.org/10.5120/ijca2017912925>
- Prayudi, Y., & Iqbal, M. (2013). Analisis Forensika Digital Pada Blackberry Untuk Mendukung Penanganan Kasus Cybercrime Menggunakan Smartphone. *Seminar Nasional Sistem Informasi Indonesia*, (June 2014).
- Punja, S. S. G., & Mislán, R. R. P. (2008). Mobile Device Analysis. *Small Scale Digital Device Forensics ...*, 2(1), 1–16. <https://doi.org/10.1145/2046614.2046618>
- Racioppo, C., & Murthy, N. (2012). Android Forensics: A Case Study of the “ HTC Incredible ” Phone. *Proceedings of Student-Faculty Research Day*, 1–8. Retrieved from <http://csis.pace.edu/~ctappert/srd2012/b6.pdf>
- Riadi, I., Sunardi, & Firdonsyah, A. (2017). Forensic Investigation Technique on Android's Blackberry Messenger using NIST Framework. *International Journal of Cyber-Security and Digital Forensics*, 16(4), 198–205.
- Ruslan, R. (2008). *Manajemen Public Relations & Media Komunikasi*. Jakarta: PT Raja Garfindo Persada.
- Setiyadi, A., & Harihayati, T. (2015). Penerapan SQLite Pada Aplikasi Pengaturan Waktu Ujian dan Presentasi. *Majalah Ilmiah UNIKOM*, 13(2), 221–225.
- Silla, C. (2015). WeChat forensic artifacts : Android phone extraction and analysis.
- Williams, J. (2012). ACPO Good Practice Guide for Digital Evidence, (March), 41. Retrieved from [http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf%0Ahttp://www.acpo.police.uk/documents/crime/2014/Revised Good Practice Guide for Digital Evidence_Vers 5_Oct 2011_Website.pdf](http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf%0Ahttp://www.acpo.police.uk/documents/crime/2014/Revised_Good_Practice_Guide_for_Digital_Evidence_Vers_5_Oct_2011_Website.pdf)
- Yadi, I. Z., & Kunang, Y. N. (2014). Analisis Forensik Pada Platform Android. *Konferensi Nasional Ilmu Komputer (KONIK)*, 141–148.

<https://doi.org/10.13140/RG.2.1.2967.0003>

Zamroni, G. M., Umar, R., & Riadi, I. (2016). Analisis Forensik Aplikasi Instant Messaging Berbasis Android. *Annual Research Seminar (ARS)*, 2(1), 102–105.