

**STUDI ANALISIS DIGITAL FORENSIK UNTUK APLIKASI WHATSAPP
PADA PLATFORM iOS DAN ANDROID**

TUGAS AKHIR

**Diajukan sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana
Jurusan Teknik Informatika**



OLEH :

**NAMA : Zeta Dwi Sukmana Panca Sedya
NO. MAHASISWA : 09523109**

**JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA**

2013

LEMBAR PENGESAHAN PEMBIMBING
STUDI ANALISIS DIGITAL FORENSIK UNTUK APLIKASI WHATSAPP
PADA PLATFORM IOS DAN ANDROID
TUGAS AKHIR



Oleh :

Nama : Zeta Dwi Sukmana

NIM : 09523109

Yogyakarta, April 2014

Pembimbing Tunggal,

Ahmad M. Rafie Pratama, ST., MIT.

LEMBAR PENGESAHAN PENGUJI
STUDI ANALISIS DIGITAL FORENSIK UNTUK APLIKASI WHATSAPP
PADA PLATFORM IOS DAN ANDROID
TUGAS AKHIR

Disusun oleh :

Nama : Zeta Dwi Sukmana

NIM : 09523109

Telah dipertahankan di depan Sidang Penguji sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Teknik Informatika
Fakultas Teknologi Industri Universitas Islam Indonesia.
Yogyakarta, Juli 2013

Tim Penguji:

Ahmad M. Rafie Pratama, ST., MIT _____

Anggota 1

Yudi Prayudi S.Si., M.Kom _____

Anggota 2

Ahmad Lutfi, S.Kom., M.Kom _____

Mengetahui,
Ketua Program Studi Teknik Informatika
Universitas Islam Indonesia

Yudi Prayudi S.Si., M.Kom

LEMBAR PERNYATAAN KEASLIAN
HASIL TUGAS AKHIR

Saya yang bertandatangan dibawah ini,

Nama : Zeta Dwi Sukmana Panca Sedy

NIM : 09523109

Menyatakan bahwa komponen dan seluruh isi dalam Laporan Tugas Akhir ini adalah hasil karya saya sendiri. Apabila dikemudian hari terbukti bahwa ada beberapa bagian dari karya ini adalah bukan hasil karya saya sendiri, maka saya akan siap menanggung resiko dan konsekuensi apapun.

Demikian pernyataan ini saya buat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, April 2014

Zeta Dwi Sukmana Panca Sedy

PERSEMBAHAN

Tugas Akhir yang telah dapat penulis selesaikan pada akhirnya dapat penulis persembahkan untuk :

1. Bapak dan Ibu tercinta yang telah memberikan dukungan dalam segala bentuk, baik itu secara moril maupun material.
2. Dosen pembimbing penulis yang telah sabar dan tekun dalam memberikan pengarahan terhadap penulis dalam segala bentuk sehingga penulis dapat menyelesaikan Tugas Akhir pada waktunya.
3. Teman-teman FTI UII khususnya angkatan 2009 jurusan Informatika yang telah memberikan kenangan manis kepada penulis selama mengikuti program studi di FTI UII.
4. Teman teman Konslay yang telah menemani perjalanan kehidupan selama menjadi mahasiswa dan membuahkan banyak kisah.
5. Galih Nistigyanti Amenika Putri yang telah memberikan waktu, semangat dan pengorbanan terhadap penulis dalam menyelesaikan Tugas Akhir
6. Dosen serta para staff FTI UII.

MOTTO

Senantiasalah berusaha dan berdoa dalam menjalani semuanya agar bisa mendapat hasil yang maksimal.

Selalu bersyukur dalam mendapatkan hasil meski tidak sempurna.

Kegagalan adalah 1% dari 99% keberhasilan

KATA PENGANTAR



Assalamu'alaikum Wr.Wb

Dengan mengucapkan Alhamdulillah, puji syukur ke hadirat Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya, sehingga penulis dapat menyelesaikan Tugas Akhir ini yang berjudul **“Studi Analisis Digital Forensik Aplikasi Whatsapp pada Platform iOS dan Android”** dengan baik.

Laporan tugas akhir ini disusun untuk melengkapi salah satu syarat guna memperoleh gelar sarjana Teknik Informatika pada Universitas Islam Indonesia dan atas apa yang telah diajarkan selama perkuliahan baik teori maupun praktek, disamping laporan itu sendiri yang merupakan rangkaian kegiatan yang harus dilakukan setelah tugas akhir ini selesai.

Penulisan dan penyelesaian tugas akhir ini tidak lepas dari saran, bimbingan, dukungan, serta bantuan dari berbagai pihak. Untuk itu pada kesempatan kali ini penulis menyampaikan ucapan terimakasih kepada :

1. Allah SWT atas segala hidayah, baroqah serta taufiq-Nya.
2. Bapak ku Giyarto SE. Yang selalu memberikan pengarahan dan dukungan yang tiada habisnya seperti seorang teman dan keluarga.
3. Ibu ku Lilis Indriyati yang selalu melimpahkan kasih sayang yang begitu besar, doa dan dukungan yang teramat besar baik secara moril maupun material.
4. Mas Avan dan Dek Rahma yang selalu ada untuk memberi bantuan.
5. Bapak Gumbolo selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia.
6. Bapak Yudi Prayudi, S.SI, M.KOM. selaku ketua jurusan Teknik Informatika.
7. Bapak Ahmad M.Rafie Pratama ST., MIT. Atas dedikasinya menjadi Dosen Jurusan Teknik Informatika dan Dosen Pembimbing.
8. Staff pengajar dan administrasi yang telah membantu hingga Tugas Akhir dapat disidangkan.
9. Galih Nistigyanti Amenika Putri untuk dukungan dan motivasi yang tiada batas, setia menemani baik dikala suka maupun duka.
10. Teman-teman Infinity semua.
11. Teman-teman kelas B informatika angkatan 2009.

12. Teman-teman konslay. Aii, Amrih, Bastian, Deny, Detry, Ezar, Fakhmi, Fafa, Girnanda, Rafky, Danar, Ryo, Upik, Guru, Ica, Rudi, Dimas dan Ganang. Terima kasih pada Reza dan Guruh yang telah membantu secara langsung dalam penyelesaian Tugas Akhir. Terima kasih atas kebersamaan yang kita bangun selama ini, semoga akan terus solid hingga masa yang akan datang.
13. Semua pihak yang telah membantu dalam pembuatan hingga terlaksananya tugas akhir ini, yang tidak bisa penulis sebutkan satu per satu.

Penulis menyadari dalam penulisan laporan Tugas Akhir ini masih jauh dari sempurna karena keterbatasan kemampuan dan pengalaman. Penulis mengharapkan saran dan kritik yang bersifat membangun untuk memperbaiki tugas akhir ini semoga dapat bermanfaat bagi penulis khususnya pembaca pada umumnya.

Wassalamu'alaikum Wr.Wb

Yogyakarta, April 2014

Zeta Dwi Sukmana PS

SARI

Kejahatan di dunia maya semakin marak terjadi sehingga perlu adanya penanggulangan. Penanggulangan diperlukan untuk menekan jumlah aktifitas *cyber crime* yaitu dengan adanya UU ITE (Undang-Undang Informasi dan Teknologi Elektronik). UU ITE mengatur perpindahan informasi elektronik secara umum dan melibatkan ilmu digital forensik dalam penegakannya. Digital forensik adalah suatu ilmu pengetahuan dan keahlian untuk mengidentifikasi, mengoleksi, menganalisa dan menguji bukti-bukti digital pada saat menangani sebuah kasus yang memerlukan penanganan dan identifikasi barang bukti digital.

Whatsapp sangat populer dan banyak digunakan sebagai aplikasi chat di ponsel. Aplikasi whatsapp tersedia di beberapa platform seperti, PC, Android, iOS dan BlackBerry. Banyaknya penipuan yang dilakukan dengan berkedok whatsapp. Website yang menawarkan produk dan penjual *online* juga sering mencantumkan nomer yang digunakan pada whatsapp sebagai contact personnya. Aplikasi *chat* juga sering digunakan untuk merencanakan suatu kejahatan. Dari kasus yang telah dipaparkan diatas, maka dirasa perlu dilakukan sebuah penelitian tentang analisis forensik terhadap aplikasi Whatsapp.

Kata kunci : Digital Forensik, Whatsapp

TAKARIR

Digital Forensik	Ilmu pengetahuan atau keahlian untuk mengidentifikasi, mengoleksi, serta menganalisa barang bukti digital.
<i>Forensic Imaging</i>	Proses menggandakan isi dari barang bukti agar barang bukti asli terjaga keasliannya.
<i>Backup</i>	Proses membuat atau mendapatkan data cadangan.
Investigator Forensik	perseorangan atau kelompok yang bertugas menyelidiki suatu kasus forensik.
<i>Tools</i>	Sebuah alat software yang berguna sebagai media pembantu proses investigasi forensik.
<i>Write Blocking</i>	Teknik Forensik untuk menghalangi penggandaan atau penulisan data.

DAFTAR ISI

HALAMAN JUDUL	I
LEMBAR PENGESAHAN	II
LEMBAR PENGUJI	III
LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR	IV
HALAMAN PERSEMBAHAN	V
HALAMAN MOTTO	VI
KATA PENGANTAR	VII
SARI	IX
TAKARIR	X
DAFTAR ISI	XI
DAFTAR GAMBAR	XIV
DAFTAR TABEL	XVI

BAB I PENDAHULUAN

1.1	Latar belakang	1
1.2	Rumusan Masalah	3
1.3	Batasan Masalah	3
1.4	Tujuan Penelitian	4
1.5	Manfaat Penelitian	4
1.6	Metodologi Penelitian	5
1.7	Sistematika Penulisan	6

BAB II LANDASAN TEORI

2.1	Forensik	8
2.1.1	Tujuan Komputer Forensik	8
2.1.2	Tahapan Digital Forensik	8
2.1.2.1	Pengumpulan Data (<i>Collecting</i>)	9
2.1.2.2	Pemeriksaan (<i>Examination</i>)	9

	2.1.2.3 Analisis	10
	2.1.2.4 Laporan	10
2.2	Forensik Mobile Device	10
2.3	Sitem Operasi Mobile	11
	2.3.1 Android	12
	2.3.2 Apple iOS	14
2.4	Aplikasi WhatsApp	15
	2.4.1 Fungsi Aplikasi Whatsapp	15
2.5	Struktur Berkas WhatsApp	16

BAB III METODOLOGI

3.1	Skenario Kasus	18
3.2	Proses Forensik iOS	19
	3.2.1 Pengumpulan Data (<i>Collecting</i>)	20
	3.2.2 Pemeriksaan (<i>Examination</i>)	21
	3.2.3 Analisis	22
	3.2.4 Laporan (<i>Reporting</i>)	23
	3.2.5 Presentasi	23
3.3	Proses Forensik Android	26
	3.3.1 Pengumpulan Data (<i>Collecting</i>)	27
	3.3.1.1 Backup Memori Internal	27
	3.3.1.2 Forensic Imaging Memori Internal	28
	3.3.1.3 Forensic Imaging Memori Eksternal	28
	3.3.2 Pemeriksaan (<i>Examination</i>)	29
	3.3.3 Analisis	30
	3.3.4` Laporan (<i>Reporting</i>)	31
	3.3.5 Presentasi	31
3.4	Metode Penyajian	34
3.4	Perbandingan Forensik Whatsapp pada iOS dan Android	34

BAB IV HASIL DAN PEMBAHASAN

4.1	Forensik Pada iOS	35
	4.1.1 Pengumpulan Data iOS	36
	4.1.2 Pemeriksaan Forensik iOS	41
	4.1.3 Analisis Forensik iOS	41
	4.1.4 Laporan Forensik iOS	48
	4.1.5 Pengumpulan Data iOS Dengan Oxygen	49
	4.1.6 Pemeriksaan Forensik iOS Dengan Oxygen	51
	4.1.7 Analisis Forensik iOS Dengan Oxygen	51
	4.1.8 Review Forensik iOS	59

4.2	Forensik Pada Android	60
4.2.1	Pengumpulan Data Forensik Android	62
4.2.1.1	Backup Android	62
4.2.2	Pemeriksaan Forensik Android	67
4.2.3	Analisis Forensik Android	68
4.2.3.1	Hasil Dan Pembahasan Android	68
4.2.4	Laporan Forensik Android	73
4.2.5	Review Forensik Android	74
4.3	Perbandingan Forensik Whatsapp pada Kedua Platform.....	76
 BAB V KESIMPULAN		
5.1	Kesimpulan	77
5.2	Saran	77

DAFTAR GAMBAR

Gambar 2.1	Tahapan Digital Forensik.....	9
Gambar 3.1	Bukti Transkrip Percakapan Dalam Bentuk Teks.....	19
Gambar 3.2	Alur Pengujian Pada iOS	24
Gambar 3.3	Alur Pengujian Pada iOS Menggunakan Oxygen	25
Gambar 3.4	Alur Pengujian Pada Android	33
Gambar 4.1	Folder Yang Dibuat iTunes Berisi Backup Daari iPhone..	37
Gambar 4.2	Isi Dari Folder Backup iTunes	38
Gambar 4.3	Tampilan Awal iPhone Backup Extractor	39
Gambar 4.4	Pemilihan File Backup Yang Akan Di Ekstrak	40
Gambar 4.5	Hasil Ekstrak File Backup iTunes	40
Gambar 4.6	Teknik Filtering Pada Hasil Forensic Imaging	41
Gambar 4.7	Isi Dari Folder Document	43
Gambar 4.8	Tabel Messages Pada File WhatsApp	43
Gambar 4.9	Tabel Messages Pada File WhatsApp	44
Gambar 4.10	Tabel Zwaphone Pada File WhatsApp	45
Gambar 4.11	Status ID Pelaku Pada File Net.Whatsapp.whatsapp	47
Gambar 4.12	Direktori Penyimpanan Gambar Yang Dikirimkan Korban	48
Gambar 4.13	Barang Bukti Yang Didapat Pada iOS	48
Gambar 4.14	Perangkat iOS Sudah Tersambung Dengan Oxygen	49
Gambar 4.15	Tampilan Pilihan Ekstrak Dalam Oxygen	50
Gambar 4.16	Struktur File Whatsapp Pada iOS	51
Gambar 4.17	Isi Dari Folder Document	52
Gambar 4.18	Tabel Messages Pada File Whatsapp	53
Gambar 4.19	Tabel Messages Pada File Whatsapp	54
Gambar 4.20	Tabel Zwaphone Pada File Whatsapp	55
Gambar 4.21	Nomor ID Pelaku Pada File Net.whatsapp.whatsapp	57
Gambar 4.22	Direktori Gambar Bukti Transfer	58
Gambar 4.23	Vesap Yang Ditemukan Pada Folder DCIM	59
Gambar 4.24	Perangkat Android Sudah Tersambung Oxygen	63
Gambar 4.25	Lembar Penelitian Pada Oxygen	64
Gambar 4.26	Alur Proses Backup Pada Oxygen	64
Gambar 4.27	Hasil Backup Menggunakan Oxygen	65
Gambar 4.28	Tipe File Backup Android	65
Gambar 4.29	Proses Ekstrak File Backup Menggunakan Oxygen	66
Gambar 4.30	Pemilihan File Yang Akan Diekstrak	67
Gambar 4.31	File Database Yang Ditemukan Menggunakan Oxygen ..	68
Gambar 4.32	Struktur File Yang Terdapat Pada Direktori Data	69
Gambar 4.33	Tabel Sqlite_Sequence Pada Msgstore.db	70

Gambar 4.34	Tabel Chat_list Pada Msgstore.db	70
Gambar 4.35	Tabel Messages Pada Msgstore.db	71
Gambar 4.36	Bukti Salah Satu Percakapan	72
Gambar 4.37	Vespa Yang Terdapat Pada Direktori DCIM	73
Gambar 4.38	Barang Bukti Yang Didapat Pada Android	74

DAFTAR TABEL

Tabel 4.1	Struktur File Barang Bukti Pada Backup iOS	42
Tabel 4.2	Hasil Analisis Terhadap File Net.whatsapp.whatsapp.....	45
Tabel 4.3	Hasil Analisis Mendalam Pada Tabel Messages.....	46
Tabel 4.4	Struktur File Whatsapp iOS Menggunakan Oxygen.....	51
Tabel 4.5	Hasil Analisis Terhadap File Net.whatsapp.whatsapp.....	55
Tabel 4.6	Hasil Analisis Mendalam Pada Tabel Messages.....	56
Tabel 4.7	Tool Yang Digunakan Dalam Forensik Pada iOS.....	59
Tabel 4.8	Struktur File Android Menggunakan Oxygen.....	69
Tabel 4.9	File Messages.db Pada Direktori Whatsapp.....	70
Tabel 4.10	Hasil Analisis Mendalam Pada Tabel Messages.....	71
Tabel 4.11	Tool Yang Akan Digunakan Dalam Forensik Android.....	74
Tabel 4.12	Perbandingan Tahapan Forensik Pada Kedua Platform	74

BAB I

PENDAHULUAN

1.1 Latar Belakang

Seiring perkembangan zaman, perkembangan di dunia teknologi dan informasi juga dituntut untuk terus berkembang dan salah satu buktinya adalah dengan mulai bermunculan berbagai macam piranti keras dan piranti lunak yang memiliki fungsi dan tujuan yang berbeda sesuai dengan kebutuhannya. Akan tetapi, perkembangan teknologi dan informasi yang ada tidak hanya menimbulkan dampak positif bagi penggunanya saja melainkan juga turut serta memicu dampak negative. Diantaranya adalah dengan adanya tindakan kriminal yang memanfaatkan perkembangan teknologi yang ada. Karena itu diperlukanlah ilmu yang lebih dalam menangani kejadian dan kemungkinan terburuk yang mungkin terjadi dengan memanfaatkan teknologi yang ada. Dan salah satu ilmu yang diperlukan adalah ilmu tentang digital forensik.

Digital forensik merupakan ilmu pengetahuan untuk mengidentifikasi, mengoleksi, serta menganalisa barang bukti digital sehingga dapat dipertanggungjawabkan di pengadilan. Namun penerapan ilmu digital forensik tidak sebanding dengan tingkat kemajuan Teknologi Informasi pada umumnya. Di Indonesia sendiri penerapan ilmu digital forensik barulah sebatas piranti-piranti perangkat keras secara umumnya, seperti *notebook, personal computer, handphone*, serta media penyimpanan lainnya seperti *hardisk* dan *flashdisk*. Padahal menurut hukum dan ilmu tentang forensik itu sendiri, segala bentuk jenis piranti perangkat keras maupun lunak yang ada, tidak akan luput dari kegiatan forensik digital serta proses investigasinya, salah satu bentuk piranti lunak yang juga tidak boleh luput dari kegiatan forensik adalah aplikasi chatting, dan salah satu pelopor media aplikasi chatting di dunia saat ini adalah WhatsApp Messenger.

WhatsApp Messenger adalah sebagai media aplikasi chatting sendiri masih sangat kurang diperhitungkan dalam kegiatan forensik digital karena masyarakat luas serta para investigator forensik beranggapan bahwa aplikasi WhatsApp

hanya sebuah aplikasi yang digunakan sebagai chatting, kirim foto, voice note serta mengirim letak keberadaan si pengguna sekarang. Namun dengan fitur yang ditawarkan oleh pengembang aplikasi WhatsApp tentu saja semakin membuat celah bagi para pelaku tindak kejahatan dalam beraksi.

Sebagai bukti bahwa WhatsApp Messenger mulai dapat menjadi suatu media tindak kejahatan adalah dengan banyaknya kasus kejahatan yang memanfaatkan aplikasi WhatsApp untuk merencanakan serta membicarakan aksi kejahatannya atau bisa digunakan para penjahat untuk membicarakan rencana mereka. Dan memungkinkan aplikasi WhatsApp ini menjadi alternatif para korupsi dan penjahat untuk saling membicarakan rencana tersebut.

Dari kasus yang telah dipaparkan diatas, maka dirasa perlu dilakukan sebuah penelitian tentang analisis forensik terhadap aplikasi WhatsApp pada platform Apple iOS dan Android. Penelitian ini dirasa penting dan perlu dilaksanakan dikarenakan minimnya informasi tentang analisis forensik terhadap aplikasi WhatsApp serta untuk dapat menguraikan apa yang harus diperhatikan dan dipertimbangkan seorang investigator forensik menemukan Smartphone yang berplatform Apple iOS dan Android terdapat aplikasi WhatsApp di TKP yang harus mampu mengidentifikasi perangkat, memahami kemampuan serta potensi perangkat smartphone yang berplatform Apple iOS dan Android mempunyai aplikasi WhatsApp ini sendiri sehingga dapat menemukan bukti dan menjamin bukti itu dapat berguna di persidangan.

1.2 Rumusan masalah

Setelah dijabarkan mengenai latar belakang permasalahan yang ada, maka dapat ditarik rumusan masalah sebagai berikut :

- a. Bagaimana cara menganalisis potensi *digital evidence* dari Aplikasi WhatsApp pada platform Apple iOS dan Google Android.
- b. Bagaimana proses *collecting digital evidence* dari Aplikasi WhatsApp pada platform Apple iOS dan Android.
- c. Bagaimana proses *examination* dilakukan terhadap *digital evidence* dari Aplikasi WhatsApp pada platform Apple iOS dan Android.
- d. Hasil apa saja yang bisa dipaparkan dari hasil analisa *digital evidence* Aplikasi WhatsApp pada platform Apple iOS dan Android.

1.3 Batasan Masalah

WhatsApp Messenger merupakan aplikasi chat yang tidak hanya memiliki fungsi utama mengirim pesan melalui jaringan internet, melainkan juga bisa mengirim gambar, audio note, share location dan juga group chat room. Aplikasi ini dapat berjalan di berbagai macam platform diantaranya adalah Apple iOS, Google Android, PC, dan BlackBerry. Berikut batasan-batasan masalah dalam penelitian ini :

- a. Aplikasi WhatsApp versi 2.9.2607 pada Google Android dipilih pada penelitian ini karena versi tersebut merupakan versi terbaru saat melakukan penelitian pada *smartphone* berplatform Android.
- b. Aplikasi WhatsApp versi 2.8.7 pada Apple iOS dipilih pada penelitian ini karena versi tersebut merupakan versi terbaru yang digunakan saat melakukan penelitian pada *smartphone* berplatform Apple iOS.

1.4 Tujuan Penelitian

Penelitian ini memiliki beberapa tujuan, diantaranya adalah :

- a. Mengetahui struktur *digital evidence* pada Aplikasi WhatsApp untuk IOS dan Android.
- b. Mengetahui tahapan *collecting* yang harus dilakukan terkait barang bukti *smartphone* yang berplatform IOS dan Android terdapat Aplikasi WhatsApp
- c. Mengetahui proses *examination* yang harus dilakukan terhadap *smartphone* berplatform IOS dan Android yang terdapat Aplikasi WhatsApp.
- d. Mengetahui hasil analisa yang didapatkan terhadap *digital evidence* dari Aplikasi WhatsApp pada *smartphone* berplatform IOS dan Andorid
- e. Mendapatkan hasil *reporting* yang bisa dipaparkan setelah melalui proses analisis investigasi forensik pada barang bukti *smartphone* yang berplatform IOS dan Android terdapat aplikasi WhatsApp

1.5 Manfaat Penelitian

Manfaat dilaksanakan penelitian ini adalah :

- a. Menambah pengetahuan tentang analisis yang dilakukan pada kasus forensik.
- b. Memberikan pemahaman akan pentingnya pengetahuan dan ilmu forensik terhadap berbagai macam aplikasi khususnya aplikasi WhatsApp Messenger
- c. Memberikan suatu kejelasan akan potensi tindak kejahatan yang dapat dilakukan oleh *smartphone* berplatform IOS dan Android terdapat aplikasi WhatsApp dan tools apa saja yang digunakan dalam proses analisis forensik

1.6 Metodologi penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah sebagai berikut:

1.6.1 Studi Literatur

Studi literatur adalah gambaran singkat dari apa yang telah dipelajari, argumentasi pada suatu topik. Studi ini mengelompokkan hasil-hasil pekerjaan secara bersama dan membahas arah perkembangannya lalu mengevaluasi penelitian sebelumnya dan saat ini dengan memperhatikan relevansi serta manfaatnya dengan penelitian yang dilakukan. Sumber studi didapatkan dari dokumentasi resmi, diskusi atau forum.

1.6.2 Simulasi

Simulasi kasus merupakan tahap pertama yang dibutuhkan pada proses Digital Forensik, dimana suatu kejadian baik secara sengaja atau tidak sengaja berdampak merugikan bagi salah satu kedua belah pihak dan melibatkan media digital sebagai alat tindak kejahatan sehingga perlu dilakukan suatu tahapan analisis forensik didalamnya untuk mendapatkan informasi secara kongkrit dan nyata demi menyelesaikan kasus yang terjadi. Simulasi dilakukan dengan beberapa skenario yang berbeda, dimana setiap skenario berpotensi kejahatan.

1.6.3 Analisis

Pada tahapan ini akan dilakukan analisis terhadap hasil *backup* dan *forensic text* dari *smartphone* yang terdapat aplikasi WhatsApp tersangka dengan menggunakan *tools* forensik. Sehingga dari proses analisis yang dilakukan ini dapat diketahui apa saja data-data terkait kasus tersebut serta menyelidiki sejauh mana penggunaan *smartphone* berplatform Apple iOS dan Google Android yang terdapat aplikasi WhatsApp dalam melakukan kejahatan

1.6.4 Kesimpulan

Kesimpulan merupakan tahap terakhir dari keseluruhan tahapan investigasi forensik, dimana kesimpulan yang didapatkan dari hasil investigasi forensik berupa laporan serta presentasi terkait hasil analisa yang didapatkan dari barang bukti digital yang ditemukan di TKP. Laporan serta presentasi yang

diperoleh oleh seorang investigator forensik pada akhirnya akan disampaikan didepan pengadilan secara jelas sehingga dapat dimengerti oleh semua pihak yang ada dan dapat dipertanggungjawabkan dimata hukum.

1.7 Sistematika Penulisan

Dalam penyusunan tugas akhir ini, sistematika penulisan dibagi menjadi beberapa bab yaitu sebagai berikut :

BAB I

PENDAHULUAN

Bab ini berisi pembahasan masalah secara umum yang meliputi bagian Latar Belakang, Rumusan Masalah, Batasan Masalah, Tujuan Penelitian, Manfaat penelitian, Metodologi Penelitian dan Sistematika penulisan.

BAB II

LANDASAN TEORI

Bab ini memuat landasan teori yang berfungsi sebagai sumber atau alat dalam memahami permasalahan terkait dengan smartphone berplatform IOS dan Android terdapat aplikasi WhatsApp.

BAB III

METODOLOGI

Bagian ini memuat studi literature mengenai permodelan uji coba serta langkah-langkah ujicoba proses investigasi forensik.

BAB IV

HASIL DAN PEMBAHASAN

Bagian ini berisi tentang proses pengujian, berupa print screen serta penjelasan data yang dapat didapat dari hasil forensik lalu menganalisa data tersebut sehingga bisa dijadikan sebagai barang bukti yang sah.

BAB V

KESIMPULAN DAN SARAN

Bab ini merupakan rangkuman serta kesimpulan kesimpulan dari hasil analisis dan saran yang dianggap perlu.

BAB II

LANDASAN TEORI

2.1 Forensik

Komputer forensik merupakan cabang ilmu forensik yang bertujuan mengungkapkan bukti legal dalam data digital. Dalam proses komputer forensik membutuhkan banyak pengetahuan mengenai hardware maupun software, hal ini ditujukan untuk mencegah adanya *accidental invalidation* ataupun kerusakan terhadap barang bukti yang ada serta untuk menjaga barang bukti tersebut agar bisa dimanfaatkan untuk keperluan analisis lebih lanjut. Secara umum, Komputer Forensik menggunakan aplikasi khusus untuk pelaksanaan inverstigasinya dan juga menggunakan teknik analisa untuk menjaga barang bukti yang legal (tidak mengalami kerusakan), oleh karena itu seorang profesional dalam bidang ini harus mempunyai pemahaman yang mendetail tentang hukum-hukum lokal, Regional, nasional atau bahkan internasional yang mempunyai pengaruh dalam proses pengumpulan dan penjagaan barng bukti tersebut.

2.1.1 Tujuan Komputer Forensik

Tujuan dari komputer forensik adalah untuk mengamankan dan menganalisa bukti digital. Selain itu juga bertujuan untuk mendapatkan fakta-fakta objektif dari sebuah insiden / pelanggaran keamanan sistem informasi. Fakta-fakta tersebut setelah diverifikasi akan menjadi bukti-bukti (evidence) yang akan digunakan di proses hukum.

2.1.2 Tahapan Digital Forensik

Untuk mendapatkan barang bukti yang sah atas suatu kasus kriminal yang terjadi, diperlukan berbagai macam teknik dan metode penanganan yang berbeda-beda namun secara keseluruhan tahapan-tahapan kegiatan dalam investigasi forensik pada barang bukti melewati 4 tahapan utama yaitu pengumpulan, pengujian, analisis, dan laporan.

Pada gambar 2.1 merupakan gambaran dimana dalam *computer forensic* ada 4 tahapan yang dilakukan untuk investigasi *forensic*.



Gambar 2.1 Tahapan Digital Forensik

2.1.2.1 Pengumpulan Data (*Collecting*)

Pengumpulan data merupakan tahap pertama yang harus dilakukan dalam proses forensik untuk mengidentifikasi sumber dan bagaimana data didapatkan. Tahapan pengumpulan data berikut meliputi beberapa kegiatan seperti:

1. Identifikasi
2. Pemberian nama (*labeling*)
3. Perekaman
4. Mendapatkan data

Dalam proses mendapatkan data, barang bukti yang ditemukan haruslah melewati serangkaian proses, proses yang dimaksud adalah *write protected*, *forensic imaging*, dan juga *backup* sehingga data yang didapatkan dapat dijamin keutuhan dan keasliannya.

2.1.2.2 Pemeriksaan (*Examination*)

Tahap selanjutnya yang harus dilakukan pada proses forensik setelah pengumpulan data adalah tahap pemeriksaan. Tahap ini merupakan proses dimana data dikumpulkan sehingga menghasilkan informasi terkait dengan kasus yang dihadapi.

Terdapat berbagai macam teknik yang dapat digunakan dalam tahapan ini. Teknik yang digunakan merupakan teknik yang dapat memastikan *image file* atau *backup file* dari alat bukti yang digunakan sesuai gambaran fakta kasus yang

lengkap, sehingga apa yang dicari dan akhirnya ditemukan oleh investigator forensik sama (*matching*) dengan gambaran fakta kasus yang sedang terjadi.

2.1.2.3 Analisis

Tahapan berikutnya setelah proses pemeriksaan adalah tahapan analisis terhadap data yang sudah diperoleh dari barang bukti. Begitu data diperoleh, penyidik sebagai pihak ketiga melakukan proses analisis terhadap data yang dicari sehingga mendapatkan informasi yang akurat sehingga penyidik yang telah berhasil mendapatkan informasi dapat melanjutkan ke tahap berikutnya yaitu laporan.

2.1.2.4 Laporan

Laporan merupakan tahap terakhir dari proses penyidikan forensik, dimana pada tahap ini penyidik melaporkan dan mempresentasikan hasil dari analisis dan kegiatan forensik yang dilakukan terhadap alat bukti yang ditemukan di TKP sehingga informasi yang didapatkan menjadi suatu informasi penting dan akurat terkait kasus yang sedang terjadi.

2.2 Forensik Mobile Device

Forensik mobile device merupakan cabang dari forensik digital yang berkaitan dengan pemulihan bukti digital. *Mobile device* biasanya merujuk ke ponsel, namun juga dapat berhubungan dengan perangkat digital yang memiliki memori dan alat komunikasi.

Banyaknya sistem operasi yang digunakan seperti Apple iOS, Google Android, RIM BlackBerry OS, Windows Mobile, Nokia Symbian OS, dan banyak lainnya. Keragaman sistem operasi mobile ini menciptakan tantangan untuk pengembangan digital forensik, dan untuk mobile forensik pada umumnya.

Perangkat mobile pada umumnya dapat menyimpan informasi di tiga lokasi. Salah satunya adalah memori internal. Memori internal pada perangkat mobile terdiri dari RAM (*Random Acces Memory*) dan ROM (*Read Only Memory*). Singkatnya RAM adalah ruang memori pada perangkat mobile yang dapat digunakan untuk menyimpan informasi sementara selama perangkat menjalankan tugas. Saat perangkat dimatikan, semua data dalam RAM biasanya

akan hilang. ROM umumnya merupakan memori internal pada ponsel, berfungsi sebagai media penyimpanan sistem dan data internal. Ada pula EEPROM (*Electrically Erasable and Programmable Read-Only Memory*) yang merupakan tempat penyimpanan data-data default seperti aplikasi bawaan dari sistem operasi itu sendiri. Selain pada memori internal, perangkat mobile juga menyimpan informasi dalam memori external.

Tahapan forensik pada Mobile Forensic secara umum hampir sama dengan tahapan forensik pada Computer Forensic, hanya saja terdapat perbedaan dalam cara melakukan tahapan tersebut karena ditentukan oleh karakteristik dari perangkat vendornya.

2.3 Sistem Operasi Mobile

Seperti sistem operasi pada komputer, sistem operasi mobile adalah software utama yang melakukan manajemen dan kontrol terhadap hardware secara langsung serta manajemen dan mengontrol software-software lain sehingga software lain tersebut dapat bekerja. Sehingga suatu sistem operasi mobile akan bertanggung jawab dalam mengoperasikan berbagai fungsi dan fitur yang tersedia dalam perangkat ponsel tersebut, task, keyboard, WAP, email, text message, sinkronisasi dengan aplikasi dan perangkat lain, memutar musik, camera, dan mengontrol fitur-fitur lainnya.

Banyak perusahaan ponsel yang membenamkan sistem operasi dalam produknya baik pada PDA, smartphone maupun handphone. Perkembangan aplikasi atau game selular sangat cepat sehingga menyebabkan perusahaan pembuat Mobile Operating System (OS) telah berlomba untuk memasarkan produk-produk mereka dengan menciptakan fungsi-fungsi dan teknologi yang kian hari kian memanjakan pengguna smartphone dari segi entertainment dan fungsionalitas pengguna selular untuk memudahkan tugas sehari-hari. Selain berfungsi untuk mengontrol sumber daya hardware dan software ponsel seperti keypad, layar, phonebook, baterai, dan koneksi ke jaringan, sistem operasi juga mengontrol agar semua aplikasi bisa berjalan stabil dan konsisten. Sistem operasi harus dirancang fleksibel sehingga para software developer lebih mudah menciptakan aplikasi-aplikasi baru yang canggih. Keunggulan lain dari ponsel

yang mempunyai operasi sistem adalah memiliki kekuasaan lebih untuk mendownload berbagai aplikasi tambahan yang tidak disediakan oleh vendor ponsel.

Sama halnya dengan komputer, jika tidak memiliki sistem operasi maka komputer itu tidak dapat digunakan. Begitupun dengan ponsel, dia juga tidak akan bisa digunakan jika tidak ada sistem yang tertanam didalam ponsel tersebut. Mulai dari ponsel generasi awal hingga generasi sekarang ini semuanya memiliki sistem operasi. Dahulu kala, sistem operasi untuk handphone masih cukup sederhana tanpa memiliki GUI (*Graphical User Interface*), alias masih berupa tampilan dot matrik. Namun sekarang sudah berkembang sistem operasi yang lebih modern dengan menungsu teknologi layar sentuh.

2.3.1 Android

Android merupakan salah satu sistem operasi mobile populer yang diciptakan oleh perusahaan Google. Pengertian sistem operasi Android secara singkat adalah sebuah sistem operasi berbasis linux yang diperuntukkan untuk telepon seluler (*smartphone*). Kelebihan Sistem operasi Android sendiri adalah menyediakan platform terbuka (*open source*) bagi para pengembang untuk menciptakan berbagai jutaan aplikasi mereka sendiri yang nantinya akan dipergunakan untuk berbagai piranti bergerak (*mobile devices*).

a. Android versi 1.1

Pada 9 maret 2009, Google merilis Android versi 1.1. Android versi ini dilengkapi dengan pembaruan estetis pada aplikasi, jam alarm, *voice search* (pencarian suara), pengiriman pesan dengan Gmail, dan pemberitahuan email.

b. Android versi 1.5 (Cupcake)

Pada pertengahan mei 2009, Google kembali merilis telepon seluler dengan menggunakan Android dan SDK (*Software Development Kit*) dengan versi 1.5 (Cupcake). Terdapat beberapa pembaruan termasuk juga penambahan beberapa fitur dalam versi ini yakni kemampuan merekam dan menonton video dengan modus kamera, mengunggah video ke Youtube dan gambar ke picasa

langsung dari telepon. Dukungan *Bluetooth* A2DP, kemampuan terhubung secara otomatis ke headset Bluetooth, animasi layar, dan keyboard pada layar yang dapat disesuaikan dengan sistem.

c. Android versi 1.6 (Donut)

Android versi 1.6 (Donut) dirilis pada september dengan menampilkan proses pencarian yang lebih baik dibanding sebelumnya, penggunaan baterai indikator dan kontrol applet VPN. Fitur lainnya adalah galeri yang memungkinkan pengguna memilih foto yang akan dihapus kamera, camcoder dan galeri yang dintegrasikan dan text to speech engine serta pengadaan resolusi VWGA.

d. Android versi 2.0/2.1 (Eclair)

Pada 3 Desember 2009 kembali diluncurkan ponsel Android dengan versi 2.0/2.1 (Eclair), perubahan yang dilakukan adalah pengoptimalan hardware, peningkatan Google Maps 3.1.2, perubahan UI dengan browser baru dan dukungan HTML5, daftar kontak yang baru, dukungan *flash* untuk kamera 3,2 MP, digital *Zoom*, dan *Bluetooth* 2.1.

e. Android versi 2.2 (Froyo)

Pada 20 Mei 2010, Android versi 2.2 (Froyo) diluncurkan. Perubahan-perubahan umumnya terhadap versi-versi sebelumnya antara lain dukungan Adobe Flash 10.1, kecepatan kinerja dan aplikasi 2 sampai 5 kali lebih cepat, intergrasi V8 JavaScript engine yang dipakai Google Chrome yang mempercepat kemampuan rendering pada browser, pemasangan aplikasi dalam SD Card, kemampuan WiFi Hotspot portable, dan kemampuan auto update dalam aplikasi Android Market.

f. Android versi 2.3 (Gingerbread)

Pada 6 Desember 2010, Android versi 2.3 (Gingerbread) diluncurkan. Perubahan-perubahan umum yang didapat dari Android versi ini antara lain peningkatan kemampuan permainan

(*gaming*), peningkatan fungsi copy paste, layar antar muka (User Interface) didesain ulang, dukungan format video VP8 dan WebM, efek audio baru, dukungan kemampuan Near Field Communication (NFC), dan dukungan jumlah kamera yang lebih dari satu.

g. Android versi 3.0/3.1 (Honeycomb)

Android Honeycomb dirancang khusus untuk tablet Android versi ini mendukung ukuran layar yang lebih besar. User interface pada Honeycomb juga berbeda karena sudah didesain untuk tablet. Honeycomb juga mendukung multi prosesor dan juga akselerasi perangkat keras (hardware) untuk grafis.

h. Android versi 4.0 (Ice Cream Sandwich)

Diumumkan pada tanggal 19 Oktober 2011, membawa fitur Honeycomb untuk *smartphone* dan menambahkan fitur baru termasuk membuka kunci dengan pengenalan wajah, jaringan data pemantauan penggunaan dan kontrol, terpacu kontak jejaring sosial, perangkat tambahan fotografi, mencari email secara offline, dan berbagi informasi dengan menggunakan NFC.

2.3.2 Apple iOS

Apple iOS adalah sebuah sistem operasi yang ditanamkan pada produk-produk yang diciptakan perusahaan terkenal Apple. Awalnya iOS hanya dikembangkan untuk iPhone. Namun seiring dengan berkembangnya teknologi maka iOS sendiri sekarang sudah diperluas untuk bisa dipergunakan pada berbagai jenis perangkat lainnya seperti iPod Touch, iPad dan Apple TV.

Versi terbaru dari sistem operasi iOS adalah iOS versi 6. Menurut beberapa sumber Apple akan meninggalkan Google Maps dan menggantinya dengan perangkat lunak lain dari sistem operasi *mobile* iOS 6 miliknya. Kelebihan dari sistem operasi iOS sendiri menurut desainer antarmuka iOS, Danilo Campos dari perusahaan Hipmunk adalah karena desain di mana tampilan iOS lebih elegan, dan mudah untuk dipergunakan dibandingkan dengan sistem operasi pada *smartphone* lainnya.

2.4 Aplikasi WhatsApp

Aplikasi WhatsApp adalah sebuah aplikasi pengirim pesan atau biasa disebut chatting yang dibuat dan dipasarkan oleh Brian Acton dan Jan Koum pada tahun 2009, kedua penemu WhatsApp ini berasal dari Santa Clara, California. WhatsApp Messenger pada awalnya merupakan aplikasi yang berjalan pada sistem operasi Apple iOS. Aplikasi ini memungkinkan pengguna untuk bertukar pesan melalui koneksi data (GPRS/EDGE/3G/HSDPA atau WiFi).

Aplikasi WhatsApp ini mempunyai sistem kerja yang sangat mirip dengan BlackBerry Messenger. Pada perkembangannya, pihak developer berhasil membuat aplikasi serupa untuk 3 platform terkenal lainnya seperti Symbian, Android, dan BlackBerry. Berbeda dengan BBM (BlackBerry Messenger) yang membutuhkan PIN berupa angka unik (berbeda untuk setiap device), pada WhatsApp ini hanya cukup menggunakan nomor telepon sebagai identifikasi. Setelah terpasang pada *smartphone*, WhatsApp akan mencari daftar kontak di buku telepon. Teman-teman yang telah menggunakan WhatsApp akan secara otomatis ditambahkan ke daftar favorite. Jadi tidak membutuhkan request dan approver seperti layaknya BBM (BlackBerry Messenger).

Fitur-fitur WhatsApp pada dasarnya tidak berbeda dengan BBM (BlackBerry Messenger), kecuali kelemahan pada fitur avatar (foto profil). WhatsApp akan menampilkan foto kontak di buku telepon sebagai avatar. WhatsApp juga tidak memberikan notifikasi ketika teman anda mengupdate status seperti pada BBM (BlackBerry Messenger). Status di WhatsApp lebih mirip Yahoo Messenger yang tertulis dibawah nama pengguna.

2.4.1 Fungsi Aplikasi WhatsApp

- a. WhatsApp memiliki fitur yang bisa dibilang komplit karena dengan WhatsApp selain kita bisa berkirim teks, kita juga bisa berkirim gambar, video, suara, dan bisa berkirim lokasi GPS via hardware GPS atau Gmaps.

- b. Aplikasi whatsapp terintegrasi ke dalam sistem layaknya sms kita dapat membuka pesan tanpa perlu membuka aplikasi terlebih dahulu.
- c. Aplikasi whatsapp memiliki status pesan yang berupa tanda, tanda tersebut adalah
 - Jam merah untuk proses loading di HP kita.
 - Tanda centang satu jika pesan terkirim tetapi penerima belum ada koneksi internet.
 - Tanda centang double jika pesan sudah terkirim ke penerima
 - Silang merah jika pesan gagal
- d. Aplikasi whatsapp memiliki fasilitas broadcast dan group chat. Dimana dengan fasilitas broadcast, kita dapat mengirim pesan ke banyak pengguna, sedangkan fasilitas group chat dapat kita gunakan untuk mengirim pesan ke anggota sesama komunitas.
- e. Aplikasi whatsapp tidak memerlukan login dan loading contact/avatar sehingga dapat menghemat penggunaan bandwidth.
- f. Aplikasi whatsapp dapat dimatikan dan hanya aktif jika ada pesan masuk sehingga bisa menghemat baterai.

2.5 Struktur Berkas WhatsApp

Berkas adalah kumpulan informasi yang diberi nama dan direkam pada media penyimpanan. Biasanya berkas mempresentasikan program dan data. Data dari berkas dapat bersifat numerik, alfabetik, alfanumerik, ataupun biner. Format berkas juga bisa bebas, misalnya berkas teks, atau dapat juga diformat pasti. Secara umum, berkas adalah urutan *bit*, *byte*, baris, atau catatan yang didefinisikan oleh pembuat berkas dan pengguna.

Sistem berkas merupakan mekanisme penyimpanan untuk akses, baik data maupun program yang berada dalam sistem operasi. Terdapat dua bagian penting dalam sistem berkas, yaitu :

- Kumpulan berkas sebagai tempat penyimpanan data, serta
- Struktur direktori, yang mengatur dan menyediakan informasi mengenai seluruh berkas dalam sistem.

Suatu berkas harus memiliki struktur yang dikenali oleh sistem operasi. Sebagai contoh, sistem operasi menginginkan suatu berkas yang dapat dieksekusi memiliki struktur tertentu agar dapat diketahui dimana berkas tersebut akan ditempatkan di memori dan di mana letak instruksi pertama berkas tersebut.

Tujuan mengetahui struktur dan sistem berkas dalam digital forensik adalah untuk menemukan *file* dan data yang akan dianalisis. Jenis sistem berkas dapat menentukan *tool* yang akan digunakan. Penemuan barang bukti dalam analisis forensik dapat dilakukan dengan menelusuri struktur berkas tersebut.

BAB III

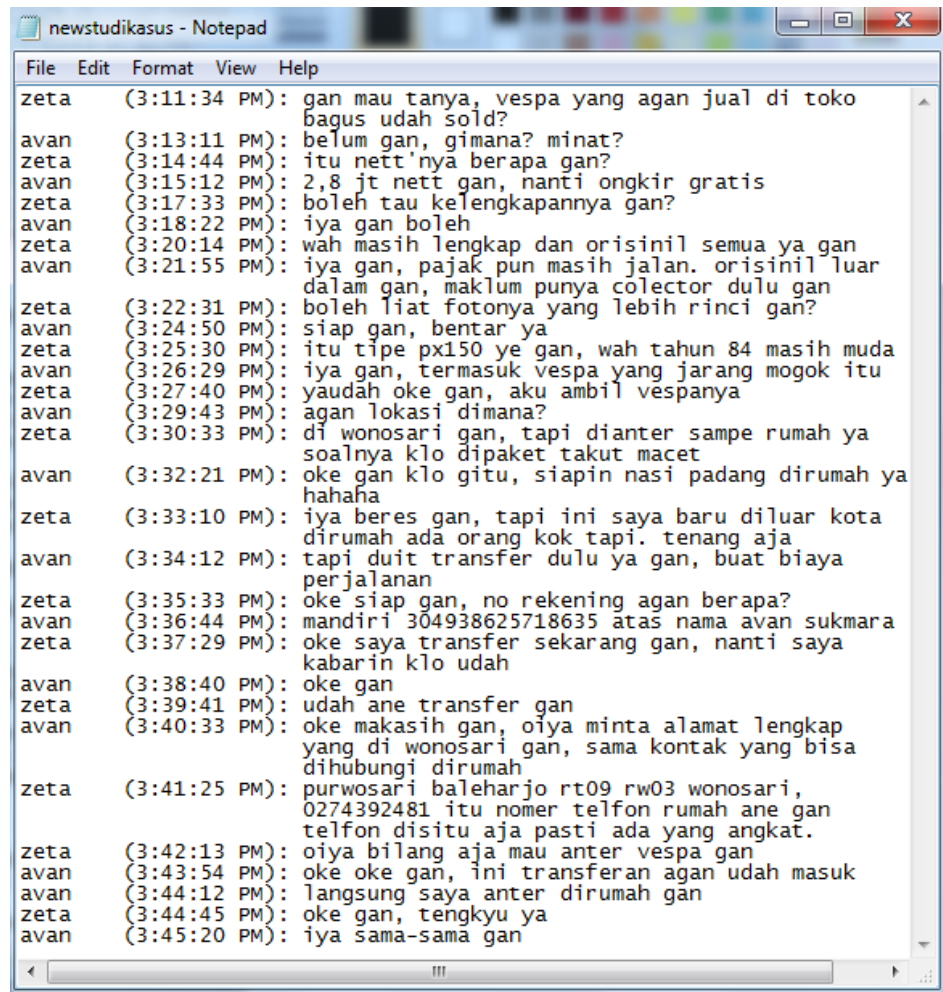
METODOLOGI

Metodologi yang dilakukan dalam melakukan Studi Analisis Digital Forensik aplikasi Whatsapp pada Android dan iOS diawali dengan melakukan simulasi skenario kasus. Setelah simulasi dilakukan, akan dilanjutkan dengan penanganan forensik dan melakukan tahapan forensik pada kedua platform. Pada akhirnya akan diambil perbandingan dari segi forensik yang menjadi perbedaan dari masing-masing platform.

3.1 Skenario Kasus

Diasumsikan pelaku kejahatan menjual sebuah vespa melalui situs jual beli online yang beralamatkan di <http://tokobagus.com> dan mencantumkan nomer telepon untuk ID whatsapp “+628135229911” dengan nama avan sebagai *contact person-nya*. Korban yang memiliki ID whatsapp “zeta” dengan nomer telepon “+6287738450051” mengontak pelaku melalui aplikasi whatsapp.

Aktifitas percakapan melalui whastapp dilakukan hingga mendapatkan kesepakatan transaksi. Percakapan dimulai dengan konfirmasi penjualan hingga diakhiri dengan kesepakatan transaksi. Pelaku mengirimkan *file* kelengkapan.txt yang berisikan kelengkapan dari vespa dan mengirimkan *file* gambar yang merupakan gambar dari vespa. Korban yang telah melakukan transaksi pembayaran mengirimkan *file* alamat.txt yang berisikan alamat korban dan file mandiri.JPG yang merupakan gambar barang bukti transaksi. Karena merasa tertipu barang yang sudah dibeli tidak kunjung datang dan pelaku memutuskan hubungan komunikasi, korban melakukan tindak kejahatan yang dilakukan pelaku dengan bukti percakapan whatsapp yang telah disimpan.



Gambar 3.1 bukti trasnkrip percakapan yang disimpan korban

3.2 Proses Forensik iOS

Sikap yang harus dilakukan jika menemukan barang bukti elektronik di TKP yaitu harus mengetahui apakah kondisi dalam keadaan *on* (hidup) atau dalam keadaan *off* (mati). Perbedaan itu sangat mempengaruhi berapa banyak informasi yang bisa diperiksa.

Dalam menemukan barang bukti berupa smartphone iPhone iOS yang masih hidup (*on*), analis forensik tidak boleh langsung mematikan perangkat tersebut. Langkah pertama yang harus dilakukan analis forensik adalah melakukan dokumentasi terhadap perangkat mulai dari dokumentasi fisik hingga non fisik seperti aplikasi apa saja yang masih dijalankan dan dapat dilihat dengan menekan

dua kali tombol home. Langkah kedua analisis forensik memasukkan barang bukti smartphone iPhone iOS kedalam kantong faraday, hal ini dimaksudkan agar perangkat tersebut tidak akan bisa mendapat sinyal. Langkah ketiga dapat dilakukan dengan mengubah mode perangkat menjadi airplane mode (mode *offline*). Langkah keempat adalah mengakses perangkat analysis workstation dengan menggunakan kabel data atau bluetooth. Langkah keempat yang membedakan dengan penanganan pada iPhone iOS mati (*off*), karena pada kondisi hidup (*on*) analisis forensik dapat melakukan akses ke seluruh data termasuk memori internal. Setelah langkah diatas selesai, analisis dapat mematikan perangkat dan mencabut baterai untuk mendapatkan dokumentasi IMEI, dan SIM card.

Barang bukti iPhone iOS dalam keadaan layar tidak aktif memerlukan penanganan khusus karena tidak mudah untuk membobol kombinasi password. Ketika password diaktifkan, perangkat iPhone iOS tidak dapat melakukan sinkronisasi dan tidak dapat diakses, kecuali terkoneksi dengan komputer yang sudah dihubungkan sebelumnya. Menurut para ahli terdapat prosedur untuk melakukan bypass passcode. Prosedur yang dimaksud adalah memunculkan raw command pada perangkat iPhone iOS untuk memuat RAM disk yang sudah dimodifikasi, dengan begitu prosedur tersebut dapat menghilangkan file konfigurasi dari passcode.

Barang bukti iPhone iOS dalam keadaan jailbreak mempunyai keuntungan lebih karena analisis mendapatkan hak akses penuh terhadap data yang ada dalam perangkat. Jika ditemukan barang bukti iPhone iOS dalam keadaan jailbreak maka analisis hanya mendapatkan beberapa data saja. Terdapat banyak tutorial untuk melakukan proses jailbreak terhadap perangkat, tetapi harus dilakukan hati-hati karena bila salah sedikit iPhone bisa mati.

3.2.1 Pengumpulan Data (collecting)

Proses pengumpulan data pada perangkat iPhone iOS dibedakan menjadi dua jenis yaitu pada perangkat yang sudah di *JailBreak* dan perangkat yang tidak di *JailBreak*.

Pada perangkat iPhone iOS yang sudah di jailbreak, pengumpulan data dapat dilakukan dengan forensic imaging yaitu melakukan command melalui SSH untuk mendapatkan RAW Image dari perangkat iPhone iOS. Dalam metode tersebut analis melakukan perintah DD menggandakan dari memori perangkat iPhone iOS lalu hasil DD tersebut ditersukan ke komputer analis melalui sambungan SSH.

Pada perangkat iPhone iOS yang tidak di JailBreak, pemeriksaan masih dapat dilakukan menggunakan tool *backup* iPhone iOS yang biasanya dipakai untuk transfer lagu, gambar dan video dari komputer ke iPhone iOS yaitu iTunes. iTunes digunakan untuk melakukan proses *backup* iPhone iOS ke komputer. Ketika iPhone iOS tersambung pada iTunes, secara otomatis iTunes membuat folder dengan nama Device UDID (Unique Device ID- panjang karakter 40 heksadesimal). Folder tersebut berisi konten-konten yang berada pada iPhone iOS. iPhone iOS dapat dihubungkan ke iTunes melalui jaringan *Wi-Fi* dan koneksi USB. Jika pilihan *automaticsync* pada iTunes dimatikan, maka pengguna dapat melakukan proses backup secara manual.

Pada proses backup iPhone iOS, pengguna dapat melakukan enkripsi pada backupnya sehingga file hasil backup memiliki keamanan lebih dan tidak mudah untuk diperiksa secara forensik. Ada beberapa tool yang dapat digunakan untuk bypass enkripsi dari backup iTunes diantaranya adalah iPhone Password Restore dan iTunes Backup Password Breaker. Kedua tool tersebut mempunyai cara kerja yang sama yaitu melakukan brute force untuk mendapatkan password iTunes.

Ekstraksi pada file backup dapat dilakukan dengan beberapa tool diantaranya iPhone Backup Extractor dan iPhone Backup Browser. iPhone Backup Extractor dapat digunakan untuk mengekstrak *file backup* sesuai dengan struktur file aslinya.

3.2.2 Pemeriksaan (*Examination*)

Pada tahapan ini, *image file* hasil dari proses *forensic imaging* yang telah dilakukan sebelumnya, diproses secara komprehensif dengan tujuan untuk

mendapatkan data-data digital yang diinginkan dan mendukung dalam proses penyelesaian kasus yang sedang terjadi.

Setelah mengetahui fakta kasus yang sedang terjadi, investigator forensik akan melakukan proses pencarian terhadap *image file* dan *backup file* pada aplikasi WhatsApp untuk menemukan barang bukti yang diinginkan. Terdapat berbagai macam teknik pemeriksaan dalam tahapan ini. Teknik yang dimaksud adalah :

- a. Teknik Filtering
- b. Teknik File Recovery

Teknik Filtering yang dimaksud adalah suatu teknik dimana investigator forensik akan menyaring hal-hal yang berkaitan langsung dengan barang bukti yang dicari. Salah satu bentuk teknik *filtering* adalah melakukan grouping terhadap isi *image file* yang didapatkan sehingga file-file yang terdapat pada *image file* akan dikelompokkan berdasarkan jenis tipe file yang secara langsung akan memudahkan dalam proses pencarian barang bukti.

Teknik selanjutnya adalah teknik *file recovery*, dimana proses pencarian akan dilakukan secara langsung terhadap hasil image file yang berstatus seperti *deleted file*, *lost file*, dan lain-lain.

3.2.3 Analisis

Tahapan berikutnya setelah proses pemeriksaan adalah tahapan analisis terhadap data yang sudah diperoleh dari tahapan-tahapan sebelumnya. Data-data tersebut akan dianalisis secara mendetail untuk dapat informasi serta pembuktian atas kejahatan apa yang terjadi dan kaitannya terhadap tindak pelaku kejahatan. Data-data digital yang melalui tahapan analisis harus dilengkapi dengan perlengkapan teknis dari data-data tersebut. Tahap analisis dapat dilakukan dengan *tool* Autopsy dan FTK(Forensic Tool Kit). Autopsy dan FTK secara umum dapat digunakan untuk memeriksa banyak tipe file, akan tetapi tool lain juga diperlukan untuk mendapatkan gambaran secara utuh dari isi beberapa file.

Beberapa data yang berkaitan dengan kasus dapat diakses dengan aplikasi default dengan catatan, file tersebut diekspor atau digandakan terlebih dahulu agar

menjaga keamanan dan keaslian file barang bukti yang asli. Untuk mengakses file secara langsung juga diperlukan kemampuan analisis yang berkompeten sehingga analis dapat menjelaskan relevansi dan implikasi dari tindakan-tindakan yang ia lakukan selama pemeriksaan.

Beberapa file database yang memiliki informasi yang berkaitan dengan kasus dapat dibuka dengan *tool* SQLite Database Browser. Tool ini tidak dapat membuka file dari sebuah image secara langsung sehingga dibutuhkan proses ekspor file database dari image dengan menggunakan tool yang lain.

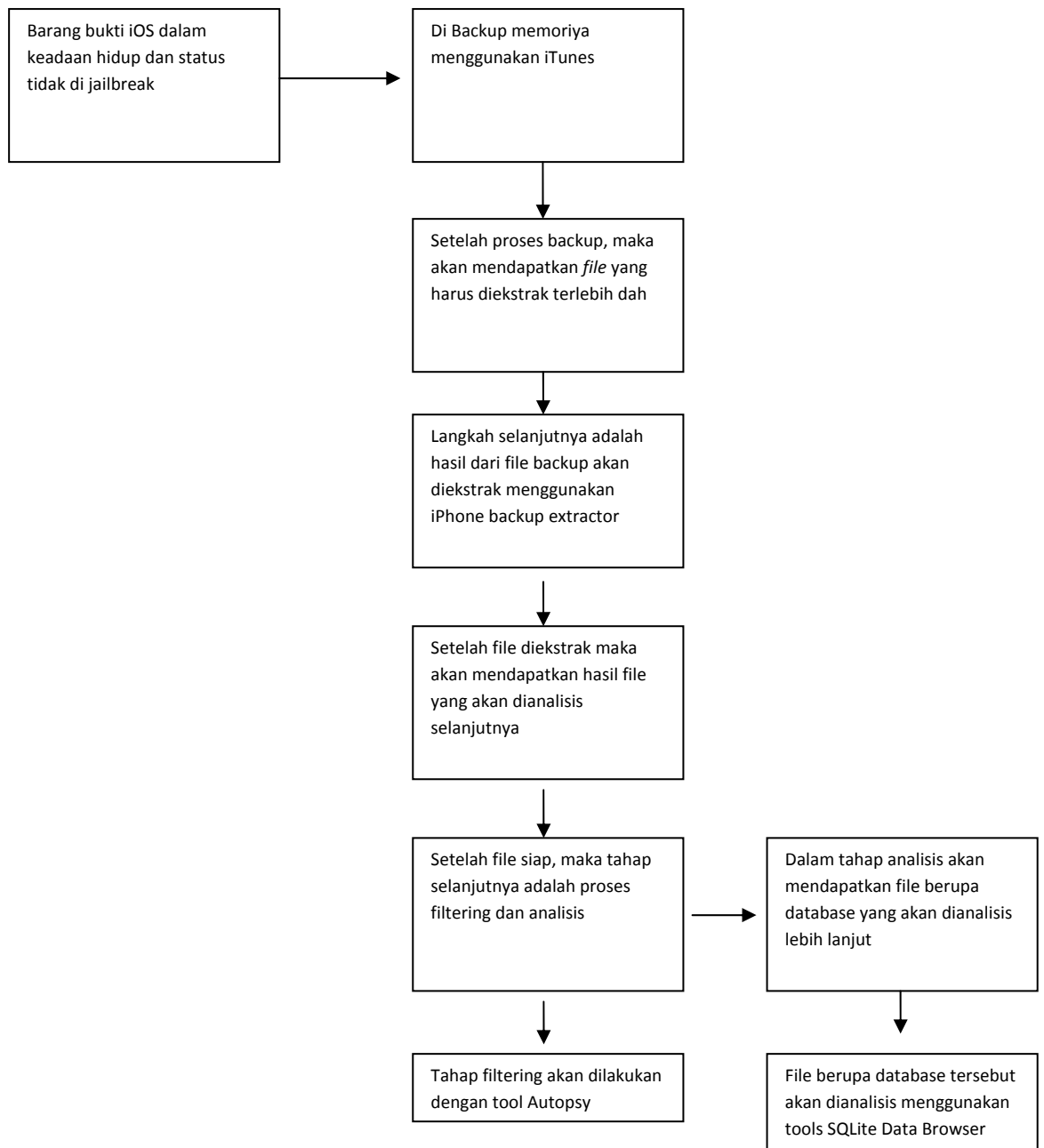
3.2.4 Laporan (*Reporting*)

Laporan merupakan tahap terakhir dari proses penyidikan forensik, dimana pada tahap ini penyidik melaporkan dan mempresentasikan hasil dari analisis dan kegiatan forensik yang dilakukan terhadap alat bukti yang ditemukan di TKP sehingga informasi yang didapatkan menjadi suatu informasi penting dan akurat terkait kasus yang sedang terjadi.

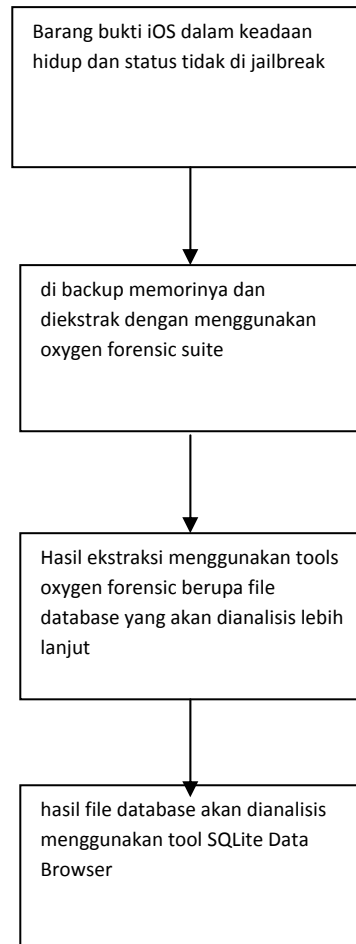
3.2.5 Presentasi

Presentasi merupakan tahapan akhir dari beberapa tahapan investigasi forensik sebelumnya, dimana pada tahapan ini penyidik berperan sebagai saksi ahli di mata pengadilan. Presentasi dari investigasi forensik pada barang bukti yang dilakukan berisi tentang penjelasan semua hasil penyelidikan terhadap barang bukti yang ditemukan di TKP secara tidak memihak dan mudah dimengerti.

Berikut adalah alur pengujian forensik pada iOS dan tool yang digunakan dalam melakukan forensik pada iOS.



Gambar 3.2 Alur pengujian pada iOS



Gambar 3.3 Alur pengujian pada iOS menggunakan Oxygen Forensic Suite

3.3 Proses Forensik Android

Sikap yang harus dilakukan jika menemukan barang bukti elektronik di TKP yaitu harus mengetahui apakah kondisi dalam keadaan *on* (hidup) atau dalam keadaan *off* (mati). Perbedaan itu sangat mempengaruhi berapa banyak informasi yang bisa diperiksa.

Dalam menemukan barang bukti berupa smartphone Android yang masih hidup (*on*), analis forensik tidak boleh langsung mematikan perangkat tersebut. Langkah pertama yang harus dilakukan analis forensik adalah melakukan dokumentasi terhadap perangkat mulai dari dokumentasi fisik hingga non fisik seperti aplikasi apa saja yang masih dijalankan dan dapat dilihat dengan menekan terus tombol home. Langkah kedua analis forensik memasukkan barang bukti smartphone kedalam kantong faraday, hal ini dimaksudkan agar perangkat tersebut tidak akan bisa mendapat sinyal. Langkah ketiga dapat dilakukan dengan mengubah mode perangkat menjadi airplane mode (mode *offline*). Langkah keempat adalah mengakses perangkat analysis workstation dengan menggunakan kabel data atau bluetooth. Langkah keempat yang membedakan dengan penanganan pada android mati (*off*), karena pada kondisi hidup (*on*) analis forensik dapat melakukan akses ke seluruh data termasuk memori internal. Setelah langkah diatas selesai, analis dapat mematikan perangkat dan mencabut baterai untuk mendapatkan dokumentasi IMEI, SIM card, dan memori external (jika ada)

Pada keadaan perangkat Android yang sudah mati (*off*), analis forensik tidak boleh langsung menyalakan perangkat tersebut. Hal tersebut menyebabkan analis forensik tidak dapat mengakses informasi secara keseluruhan.

Barang bukti Android yang ditemukan mempunyai kemungkinan diberi password oleh pemiliknya sehingga analis tidak dapat mengakses perangkat tersebut secara lebih dalam. Ada dua keadaan yang membedakan dalam kondisi

tersebut yaitu barang bukti Android dalam keadaan layar aktif (tidak dikunci) dan layar tidak aktif (dikunci).

Barang bukti Android dalam keadaan layar aktif mempunyai sedikit waktu antara 1 menit hingga 30 menit dimana memungkinkan analis mempunyai akses penuh terhadap perangkat tanpa memasukkan password terlebih dahulu. Cara yang dilakukan untuk menambah waktu agar android dalam keadaan menyala adalah dengan menambahkan waktu pada pengaturan waktu screen timeout untuk menunda perangkat agar kembali terkunci.

Barang bukti Android dalam keadaan layar tidak aktif memerlukan penanganan khusus karena tidaklah mudah untuk menjebol password yang sudah diatur oleh pemilik android. Tetapi menurut para ahli teknik yang dapat dilakukan dalam menjebol password dengan menggunakan Recovery Mode, Screen Lock BypassApp, menggunakan Gmail User/pass.

Pada saat barang bukti Android ditemukan dalam keadaan *Root* mempunyai keuntungan lebih karena analis mendapatkan hak akses (super user) penuh terhadap data yang ada dalam perangkat. Jika ditemukan barang bukti Android dalam keadaan tidak root (*unroot*) maka analis dapat melakukan proses *rooting* untuk pemeriksaan. Tutorial untuk melakukan proses root sudah banyak ditemukan di google, tutorial dapat berbeda untuk setiap perangkat dan jenis perangkat.

3.3.1 Pengumpulan Data (collecting)

Android mempunyai 4 sumber yang dapat di analisis secara forensik, yaitu memori *internal*, memori *eksternal*, *RAM* dan *SIM card*. Pada penelitian ini hanya difokuskan pada memori internal dan memori eksternal. Untuk melakukan analisis forensik pada Android dibutuhkan tiga sumber yaitu backup memori *internal*, *image memori internal* dan *image* dari *memori eksternal*.

3.3.1.1 Backup Memori Internal

Sistem berkas yang digunakan pada platform Android adalah “*Yet Another Flash File System*” (YAFFS), yang mana didesain untuk menjadi sistem berkas pada device yang menggunakan NAND Flash. Memori internal pada Android menggunakan jenis sistem berkas YAFFS dimana untuk saat ini tidak banyak *tool* forensik yang dapat mengekstraknya secara langsung.

Android dapat membuat backup dari memori internal dengan tool pihak ketiga antara lain Nandroid Backup, ADB Backup dan Oxygen. Nandroid backup merupakan *tools* yang dapat dijalankan pada komputer analis dengan menggunakan bantuan ADB (*Android Debug Bridge*) untuk menghubungkan komputer analis dengan perangkat Android. Nandroid Backup akan menghasilkan beberapa *file backup* yang mempunyai tipe file YAFFS dan tersimpan pada memori eksternal perangkat. ADB Backup adalah perintah ADB untuk melakukan backup melalui komputer analis, *file backup* yang dihasilkan hanya dapat di restore melalui ADB. Beberapa *file backup* yang dihasilkan ketiga tool tersebut dapat diekstraksi dengan menggunakan tool Unyaffs dan Yaffey. Oxygen juga merupakan tool pihak ketiga yang bisa digunakan dalam proses backup. Meskipun kekurangannya adalah berbayar, tetapi tool ini dapat menghasilkan hasil backup secara lengkap. Oxygen dapat membackup Android menyeluruh mulai dari memori internal sampai ke memori eksternal secara bersamaan. Dalam penelitian forensik, tool oxygen sangat bisa diandalkan karena dalam penggunaannya cukup mudah dan tinggal mengikuti perintah saja. Tetapi kekurangannya tool ini berbayar dan tidak bisa sembarangan untuk di download karena tool ini membutuhkan lisensi yang resmi untuk mengoperasikannya.

Android dapat membuat backup dari memori internal dengan memanfaatkan *tool* pihak ketiga antara lain

3.3.1.2 Forensic Imaging memori Internal

Imaging memori internal untuk Android saat ini masih sulit dilakukan karena keterbatasan tool forensik yang ada. Tool berbayar seperti oxygen forensic suite juga sulit untuk didapatkan meskipun dalam penelitian ini menggunakan tool

Oxygen forensic. Image file dari memori internal masih mungkin didapatkan dengan perintah DD. Perintah DD dapat digunakan karena merupakan cara sederhana untuk memperoleh raw data dari file, folder, volume atau drive fisik. ToolMobilEdit dapat digunakan untuk mengakses data-data internal dan mengekspornya ke komputer analis. Tool MobilEdit juga dapat mengakses data-data yang tersimpan di SIM Card dan memori eksternal. Aplikasi Root explorer juga bisa digunakan untuk mengambil data dari memori internal, dengan menggunakan akses super user kita dapat mengcopy semua data di memori internal kemudian di paste ke memori eksternal baru si copy lagi ke komputer analis.

3.3.1.3 Forensic Imaging Memori Eksternal

Terdapat dua macam memori eksternal pada android yaitu SD card (Secure Digital) dan Emmc (Embedded MultiMediaCard). Tidak ada perbedaan antara dua macam memori tersebut, hanya saja pada SD Card bersifat *portable*, mudah dilepaskan dan dilakukan pemeriksaan secara terpisah. eMMC merupakan SD Card yang tertanam pada perangkat dan merupakan memori eksternal yang tidak bisa dilepas dari perangkatnya.

Menurut ahli ada dua teknik yang dapat dilakukan untuk melakukan proses forensic imaging pada memori eksternal dengan jenis eMMC yaitu dengan :

1. Mengaktifkan UMS (USB Mass Storage) ketika Android dihubungkan dengan komputer dan melakukan proses forensic imaging dengan tool yang dipilih.
2. Melakukan perintah DD yang mana membutuhkan ADB Port Forwarding.

Memori eksternal SD card dapat bertipe file FAT dan EXT. Hal tersebut menjadikan memori ekstrenal SD Card mudah dilakukan proses *forensic imaging* karena beberapa tool *imager* mengenali dua tipe file tersebut. Para ahli menjelaskan bahwa analisis forensik memori internal dan memori eksternal pada Android harus dilakukan terpisah. Ekstraksi atau imaging untuk memori eksternal

dapat diselesaikan dengan *tool forensic imager* apapun, sama seperti membuat image dari hardisk komputer. Terdapat berbagai macam tools yang dapat digunakan dalam forensic imaging memori eksternal diantaranya FTK Imager, EnCase, DD dan Oxygen.

3.3.2 Pemeriksaan (*Examination*)

Pada tahapan ini, *image file* hasil dari proses *forensic imaging* yang telah dilakukan sebelumnya, diproses secara komprehensif dengan tujuan untuk mendapatkan data-data digital yang diinginkan dan mendukung dalam proses penyelesaian kasus yang sedang terjadi.

Setelah mengetahui fakta kasus yang sedang terjadi, investigator forensik akan melakukan proses pencarian terhadap *image file* dan *backup file* pada aplikasi WhatsApp untuk menemukan barang bukti yang diinginkan. Terdapat berbagai macam teknik pemeriksaan dalam tahapan ini. Teknik yang dimaksud adalah :

- c. Teknik Filtering
- d. Teknik File Recovery

Teknik Filtering yang dimaksud adalah suatu teknik dimana investigator forensik akan menyaring hal-hal yang berkaitan langsung dengan barang bukti yang dicari. Salah satu bentuk teknik *filtering* adalah melakukan grouping terhadap isi *image file* yang didapatkan sehingga file-file yang terdapat pada *image file* akan dikelompokkan berdasarkan jenis tipe file yang secara langsung akan memudahkan dalam proses pencarian barang bukti.

Teknik selanjutnya adalah teknik *file recovery*, dimana proses pencarian akan dilakukan secara langsung terhadap hasil image file yang berstatus seperti *deleted file*, *lost file*, dan lain-lain.

3.3.3 Analisis

Tahapan berikutnya setelah proses pemeriksaan adalah tahapan analisis terhadap data yang sudah diperoleh dari tahapan-tahapan sebelumnya. Data-data tersebut akan dianalisis secara mendetail untuk dapat informasi serta pembuktian

atas kejahatan apa yang terjadi dan kaitannya terhadap tindak pelaku kejahatan. Data-data digital yang melalui tahapan analisis harus dilengkapi dengan perlengkapan teknis dari data-data tersebut. Tahap analisis dapat dilakukan dengan *tool* Autopsy, FTK(Forensic Tool Kit) dan Oxygen Forensic . Autopsy, FTK dan Oxygen secara umum dapat digunakan untuk memeriksa banyak tipe file, akan tetapi tool lain juga diperlukan untuk mendapatkan gambaran secara utuh dari isi beberapa file.

Beberapa data yang berkaitan dengan kasus dapat diakses dengan aplikasi default dengan catatan, file tersebut diekspor atau digandakan terlebih dahulu agar menjaga keamanan dan keaslian file barang bukti yang asli. Untuk mengakses file secara langsung juga diperlukan kemampuan analisis yang berkompeten sehingga analis dapat menjelaskan relevansi dan implikasi dari tindakan-tindakan yang ia lakukan selama pemeriksaan.

Beberapa file database yang memiliki informasi yang berkaitan dengan kasus dapat dibuka dengan *tool* SQLite Database Browser. Tool ini tidak dapat membuka file dari sebuah image secara langsung sehingga dibutuhkan proses ekspor file database dari image dengan menggunakan tool yang lain.

3.3.4 Laporan (*Reporting*)

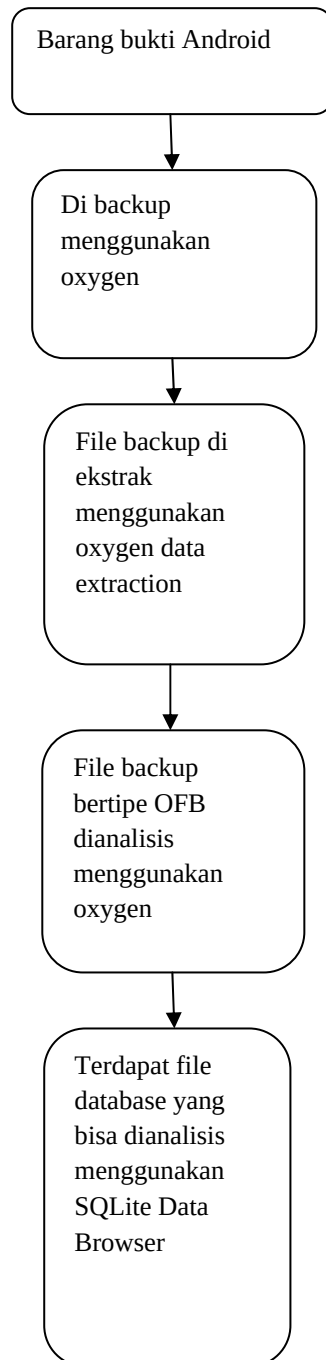
Laporan merupakan tahap terakhir dari proses penyidikan forensik, dimana pada tahap ini penyidik melaporkan dan mempresentasikan hasil dari analisis dan kegiatan forensik yang dilakukan terhadap alat bukti yang ditemukan di TKP sehingga informasi yang didapatkan menjadi suatu informasi penting dan akurat terkait kasus yang sedang terjadi. Hasil laporan yang dapat dipaparkan dari proses investigasi forensik dari barang bukti Smartphone berplatform Android terdapat aplikasi WhatsApp dapat dilihat secara lebih jelas pada halaman lampiran.

3.3.5 Presentasi

Presentasi merupakan tahapan akhir dari beberapa tahapan kegiatan investigasi forensik sebelumnya, dimana pada tahapan ini penyidik berperan sebagai ahli saksi di mata pengadilan. Presentasi dari investigasi forensik pada

barang bukti yang dilakukan berisi tentang penjelasan semua hasil penyelidikan terhadap barang bukti yang ditemukan di TKP secara lengkap, tidak memihak dan mudah dimengerti.

Berikut adalah alur pengujian forensik pada Android dan tool yang digunakan dalam melakukan forensik pada Android.



Gambar 3.4 Alur pengujian pada Android

3.4 Metode Penyajian

Laporan serta presentasi yang diperoleh oleh seorang investigator forensik didapat setelah tahapan forensik telah selesai dan menemukan cukup bukti. Laporan serta presentasi pada akhirnya akan disampaikan didepan pengadilan dengan tegas dan jelas.

3.5 Perbandingan Forensik Whatsapp pada iOS dan Android

Perbandingan yang dilakukan meliputi tahapan forensik, tool yang dipakai, dan letak barang bukti yang ditemukan. Perbandingan tersebut didapatkan peneliti dari hasil penelitian forensik yang telah dilakukan pada platform iOS dan Android.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Forensik Pada iOS

Peneliti memilih perangkat iOS yang diforensik adalah dalam keadaan hidup dan belum di *jailbreak* karena hanya dalam keadaan hidup iOS dapat di proses backup karena iOS sendiri tidak memiliki memori eksternal. Lalu perangkat iOS yang belum di *jailbreak* karena peneliti mengalami kesulitan untuk menemukan iOS yang sudah di *jailbreak* ketika simulasi dilakukan.

Ketika barang bukti iOS ditemukan dalam keadaan hidup, maka analis forensik dan investigator melakukan prosedur sebagai berikut :

1. Analis tidak mematikan perangkat dan membiarkan dalam keadaan menyala. Jika layar dalam keadaan aktif atau tidak terkunci maka analis melakukan proses perubahan setting agar layar tetap menyala. Hal tersebut dimaksudkan agar menambah waktu analis pada pemeriksaan sebelum perangkat mengunci layar (*screen locked*)
2. Mencatat spesifikasi teknis dari barang bukti. Ditemukan spesifikasi sebagai berikut :
 - iPhone 4
 - Firmware iOS 7.1
 - Jaringan GSM/HSDPA
 - Memori 16GB
 - RAM 512 MB
 - Waktu pada iPhone sama dengan waktu lokal
3. Membangun suatu area tanpa sinyal dengan kantong faraday atau cara yang paling sederhana adalah mengubah perangkat iOS menjadi *airplane mode*

4. Akses perangkat dengan menghubungkan ke komputer menggunakan kabel data, *bluetooth* tetapi disarankan pengaksesan perangkat tersebut menggunakan kabel data melalui USB port.
5. Setelah proses konektivitas dan sinkronisasi melalui instalasi driver perangkat selesai, proses selanjutnya adalah melakukan pengumpulan data dan pemeriksaan.
6. Matikan perangkat dengan menekan tombol *power* atau prosedur yang disediakan oleh perangkat. Setelah itu cabut baterai dan dilanjutkan dengan mencabut *SIM card* untuk pemeriksaan lebih lanjut. Tetapi pada perangkat iPhone4 baterai tidak bisa dicabut, jadi cukup menekan tombol *power* dan dilanjutkan dengan mencabut *SIM card* saja. Setelah semua pemeriksaan selesai, *SIM card* dikembalikan ke slot seperti semula.
7. Untuk perangkat yang baterainya hampir habis, sebaiknya dicarikan *charger* untuk menambah daya baterai. Jika *charger* tidak ditemukan, maka perangkat dapat dimatikan dan proses pemeriksaan selanjutnya dianggap sebagai perangkat dalam keadaan mati.

4.1.1 Pengumpulan data iOS

Perangkat iOS memiliki kemampuan untuk menyimpan data-data personal, sehingga dalam sisi forensik data personal ini perlu diselidiki. Data personal tersebut di backup melalui aplikasi iTunes. Berikut adalah langkah-langkah melakukan backup iPhone melalui iTunes

1. Install iTunes pada komputer.
2. Nonaktifkan fitur *auto synchronize* pada iTunes dengan cara klik edit pada menu bar, lalu pilih menu *preferences*. Check pilihan

3. Sumbungkan iPhone ke komputer dengan menggunakan kabel USB, setelah itu buka iTunes.
4. Pada iTunes, klik kanan pada iPhone lalu pilih *backup*.
5. Maka selanjutnya iTunes akan membuat backup dari iPhones di komputer. Lokasi hasil backup adalah C:\Users\zeta\AppData\Roaming\AppleComputer\MobileSync\Backup\
6. Secara otomatis iTunes membuat *folder* dengan nama Device UDID (Unique Device ID-panjang karakter 40 Heksadesimal). *Folder* tersebut berisi konten-konten yang berada pada iPhone.



Gambar 4.1 folder yang dibuat iTunes berisikan *backup* dari iPhone

Hasil dari backup iTunes adalah sebuah folder yang berisikan daftar *file backup* dan tidak memiliki ekstensi sehingga tidak dapat dibuka secara langsung. Setiap *file backup* tersebut mempunyai nama unik yang terdiri dari 40 karakter heksadesimal.

Name	Date modified	Type	Size
00cc245f0b63cf87b50a2b223e08e9648776...	21/03/2014 8:27	File	44 KB
00d8f864822fec05814a2d7a7a22f38b9d78...	21/03/2014 8:29	File	127 KB
00dc22c49d0c03d7932d982eb68843bc6c3...	21/03/2014 8:28	File	22 KB
00f08adc371ae3caac6c2bd30349			154 KB
0a0fe145cc0eeb1f5a0df31a00fb4			1 KB
0a6c7519d792dd131ff022e57064			2 KB
0a8e5fdeac8985c3e294c3cd453e23b2559c...	21/03/2014 8:27	File	1 KB
0a9b39ea20cd20280440fcd7fc94df91e470...	21/03/2014 8:28	File	2 KB
0a234e58cc15ce73bbced0429e84f935d50...	21/03/2014 8:29	File	1 KB
0a6742db13255420dd02a28732c37eb387d...	21/03/2014 8:29	File	1 KB
0a369263da844202abc83ac7d2edb8f589c...	21/03/2014 8:28	File	22 KB
0aa06f5a008e45ce3de003fb17644291738e...	21/03/2014 8:29	File	102 KB
0ac49e5b9a2832559b6d520c0ee533cdb18...	21/03/2014 8:29	File	14 KB
0acb3f77c0e2c82c9555458586ce9cb47f0d...	21/03/2014 8:28	File	1 KB
0ae90864361fc750fc21a3aa97d9b0852150...	21/03/2014 8:29	File	230 KB
0b5c36b1f8e4f7ab2f93dbe6ac7b0df33d3f...	21/03/2014 8:28	File	1 KB
0b5f589a3a24234cf455175dab7a05368e37...	21/03/2014 8:28	File	3 KB
0b8d4b34868246dfeae6b65c7b747d95658...	21/03/2014 8:27	File	4 KB
0b9b293f66308eab5591eb3e01620d9bf83f...	21/03/2014 8:28	File	38 KB
0b24c7b9e6f03f5efec1e9c129b6fd9c8286...	21/03/2014 8:28	File	31 KB

Gambar 4.2 Isi dari folder backup iTunes

Jika ketika ditemukan *file backup* dalam keadaan terenkripsi, maka langkah yang diambil adalah membobol enkripsi dari *file backup* tersebut sebelum dilakukan ekstraksi *file backup*. Untuk mendapatkan *password*, analis dapat memakai tool pihak ketiga yaitu iPhone Password Restore dan iTunes Backup Password Breaker dan melakukan metode *brute force*.

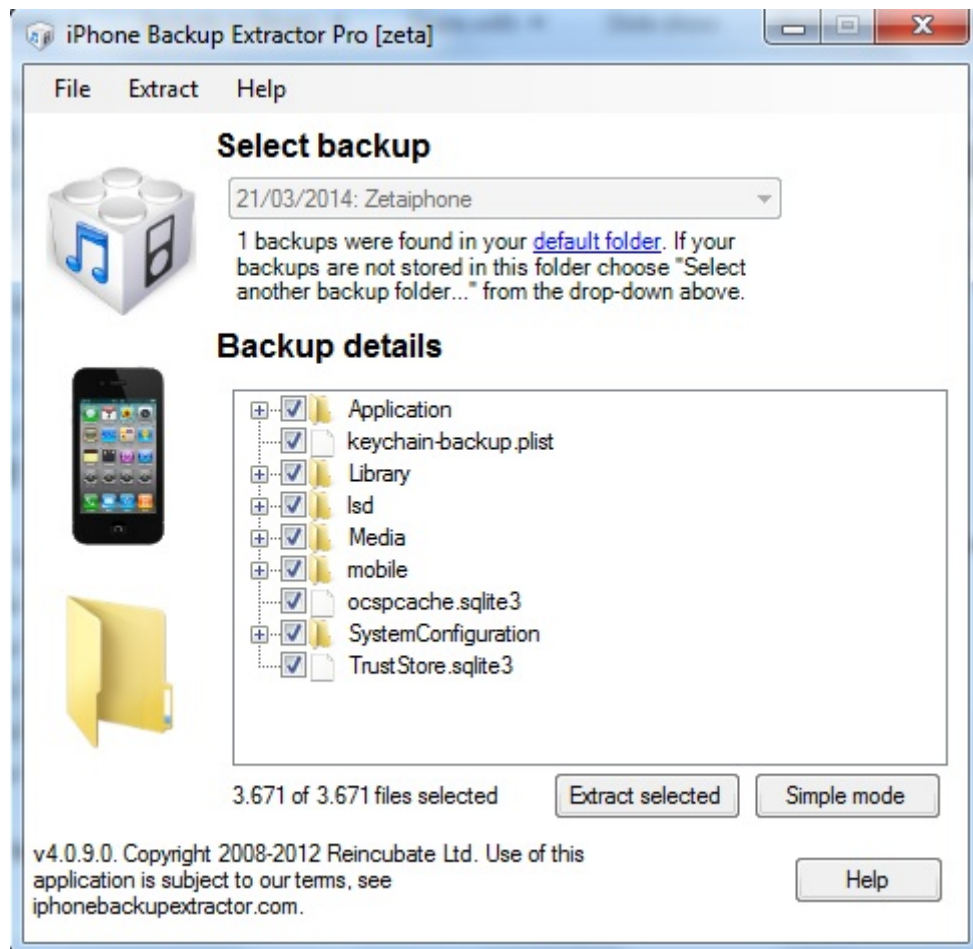
Peneliti memilih tool iPhone Backup Extractor untuk mengekstrak *file backup* dari iPhone karena mudah digunakan.berikut adalah langkah-langkah mengekstrak file backup dari iPhone.

1. Install tool iPhone Backup Extractor.
2. Buka tool iPhone Backup Extractor maka secara otomatis tool akan mendeteksi folder *backup* yang tadi telah dibuat.



Gambar 4.3 Tampilan awal iPhone Backup Extractor

3. Klik expert mode lalu centang *file* yang ingin diekstrak. Pilih *extract selected* lalu akan muncul *dialog window* yang menanyakan dimana file hasil ekstraksi akan disimpan.



Gambar 4.4 Pemilihan file Backup yang akan di ekstrak

Hasil ekstraksi *file backup* dapat diperlihatkan struktur file secara jelas dan nama *file* tersebut sehingga memudahkan dalam melakukan penyelidikan forensik. Hasil ekstraksi *file backup* merupakan *logical* sehingga teknik *recovery file* tidak dapat diterapkan.

library ▾ Share with ▾ Burn New folder ▾			
Name	Date modified	Type	Size
Application	21/03/2014 17:28	File folder	
Library	21/03/2014 17:28	File folder	
Isd	21/03/2014 17:28	File folder	
Media	21/03/2014 17:28	File folder	
mobile	21/03/2014 17:28	File folder	
SystemConfiguration	21/03/2014 17:28	File folder	
keychain-backup.plist	21/03/2014 8:28	PLIST File	203 KB
ocspcache.sqlite3	21/03/2014 8:28	SQLITE3 File	8.512 KB
TrustStore.sqlite3	21/03/2014 8:28	SQLITE3 File	16 KB

Gambar 4.5 Hasil ekstrak file backup iTunes

4.1.2 Pemeriksaan forensik iOS

Teknik yang digunakan pada tahapan pemeriksaan ini adalah teknik *filtering*. Teknik *file recovery* tidak dapat dilakukan karena hasil *forensic imaging* bersifat *logical*, tidak memiliki *deleted file* dan *lost file*. Teknik *filtering* dilakukan dengan tool autopsy untuk mencari file yang berkaitan dengan kasus.

Directory Listing		
/LogicalFileSet1/iphone/Application/net.whatsapp.WhatsApp/Documents		
Table Thumbnail		
Name	Location	Modified Time
ChatStorage.sqlite	/LogicalFileSet1/iphone/Application/net.whatsapp.WhatsApp/Docume...	0000-00-00 00:00:00
Colors.plist	/LogicalFileSet1/iphone/Application/net.whatsapp.WhatsApp/Docume...	0000-00-00 00:00:00
Contacts.sqlite	/LogicalFileSet1/iphone/Application/net.whatsapp.WhatsApp/Docume...	0000-00-00 00:00:00
ProfilePicReColors.plist	/LogicalFileSet1/iphone/Application/net.whatsapp.WhatsApp/Docume...	0000-00-00 00:00:00
StatusList.plist	/LogicalFileSet1/iphone/Application/net.whatsapp.WhatsApp/Docume...	0000-00-00 00:00:00
SyncHistory.plist	/LogicalFileSet1/iphone/Application/net.whatsapp.WhatsApp/Docume...	0000-00-00 00:00:00
wallpaper	/LogicalFileSet1/iphone/Application/net.whatsapp.WhatsApp/Docume...	0000-00-00 00:00:00

Gambar 4.6 Teknik *filtering* diterapkan pada hasil *forensic imaging*

4.1.3 Analisis Forensik iOS

Proses forensic imaging pada iPhone menghasilkan 1 folder utama yaitu folder hasil ekstraksi dari *file backup* iTunes. Hasil *forensic imaging* tersebut bersifat *logical file* yang berarti teknik *file recovery* tidak dapat dilakukan.

Peneliti memilih tool autopsy untuk melakukan analisis pada barang bukti. FTK (versi gratis) tidak memungkinkan untuk digunakan karena ada batasan 5000 file dalam pemeriksaannya.

Hasil analisis melalui autopsy ditemukan beberapa barang bukti terletak pada direktori /Application/com.whatsapp dan /Media/DCIM. Beberapa bukti tersebut akan dirangkum pada tabel berikut agar mudah dalam pembacaannya.

Tabel 4.1 Struktur File barang bukti pada hasil ekstrak file backup

Lokasi direktori	Barang bukti yang ditemukan	Deskripsi
/Application/	Folder net.whatsapp.whatsapp	folder tersebut berisikan file aplikasi whatsapp yang masih utuh. Hal tersebut membuktikan pelaku tidak menghapus aplikasi untuk penghilangan barang bukti.
/Media/DCIM/101 APPLE	IMG_1925.JPG IMG_1924.JPG IMG_1926.JPG	Terdapat 3 gambar IMG_1925.JPG dan IMG_1924.JPG Adalah dua gambar vespa yang dikirimkan oleh pelaku. Dan IMG_1926 Adalah bukti transfer yang dilakukan korban pada pelaku dengan bank BRI.
/Application/net.whatsapp.whatsapp/documents	Chat storage.sqlite,colors.plist,contact.sqlite,profilepicreq Data.plist,statuslist.plist,SyncHistory.plist,walpaper	Pada direktori tersebut terdapat percakapan,profile pengguna,status pengguna,dan walpaper pengguna.
/Application/net.whatsapp.whatsapp/Library/Preference	com.apple.mobileslideshow.plist net.whatsapp.WhatsApp.plist	Pada file tersebut ditemukan status dari ID pelaku

Pada gambar 4.7 diperlihatkan isi dari folder /Document yang berada pada direktori */Application/net.whatsapp.Whatsapp/*. Folder tersebut berisikan file yang berkaitan dengan aktifitas chat. Ada 2 jenis file yaitu berekstensi *sqlite* dan *plist*. File berekstensi *sqlite* adalah data percakapan yang dilakukan.

Name	Date modified	Type	Size
 ChatStorage.sqlite	21/03/2014 8:28	SQLITE File	4.764 KB
 Colors.plist	21/03/2014 8:28	PLIST File	2 KB
 Contacts.sqlite	21/03/2014 8:28	SQLITE File	204 KB
 ProfilePicRequestDates.plist	21/03/2014 8:28	PLIST File	1 KB
 StatusList.plist	21/03/2014 8:28	PLIST File	2 KB
 SyncHistory.plist	21/03/2014 8:28	PLIST File	1 KB
 wallpaper	21/03/2014 8:28	File	1.284 KB

Gambar 4.7 Isi dari *folder Document*

ZMESSAGEID	ZFROMJID	ZPUSHNAME	ZSTANZAID	ZTEXT	ZTOJID
417055821	6282135229911@s.	Zeta Zone	1395359962-4	Hehehe,iya silahkan	
417055842.935234			1395250828-326	Sebelum nawar, itu r	6282135229911@s.
417055904	6282135229911@s.	Zeta Zone	1395359962-5	Itu vespa taun 64 je	
417055929.004295			1395250828-350	Klo masalah repaint	6282135229911@s.
417055989	6282135229911@s.	Zeta Zone	1395359962-6	Sekali selah langsun	
417056002.141949			1395250828-370	Itu vespa udah perr	6282135229911@s.
417056073	6282135229911@s.	Zeta Zone	1395359962-7	Macet sih belum gan	
417056083.535403			1395250828-389	Saya minta fotonya	6282135229911@s.
417056234	6282135229911@s.	Zeta Zone	1395359962-8	Jadiin dulu nawarny	
417056247.737673			1395250828-414	Nawar 2jt pas ya ga	6282135229911@s.
417056281	6282135229911@s.	Zeta Zone	1395359962-9	Tambahin lagi gan, c	
417056313.386217			1395250828-438	Duh berapa ya gan,	6282135229911@s.
417056348	6282135229911@s.	Zeta Zone	1395359962-10	Gini aja gan,tambah	
417056382.281633			1395250828-456	Yaudah oke deh. Ng	6282135229911@s.
417056410	6282135229911@s.	Zeta Zone	1395359962-11	Saya lokasi bekasi g	
417056489.534075			1395250828-485	Saya lokasi di wonos	6282135229911@s.
417056554	6282135229911@s.	Zeta Zone	1395359962-12	Bisa bisa gan,saya k	
417056964	6282135229911@s.	Zeta Zone	1395363912-1		
417056984	6282135229911@s.	Zeta Zone	1395363912-3		
417056996	6282135229911@s.	Zeta Zone	1395363912-2		
417057023.841656			1395250828-533	Oiya gan, nomer rek	6282135229911@s.
417057073	6282135229911@s.	Zeta Zone	1395363912-4	Ini norek saya gan,	
417057085	6282135229911@s.	Zeta Zone	1395363912-5	Bca atas nama avan	
417057104	6282135229911@s.	Zeta Zone	1395363912-6	Nanti klo udah trans	

Gambar 4.8 Tabel *messages* pada *file whatsapp*

P	IE	ZFLAGS	ISFROMME	ZMESSAGESTATUS	ZMESSAGETYPE	ZSORT
10001	0	0	0	2	0	7
10002	0	0	1	2	0	8
10003	0	0	0	2	0	9
10004	0	0	1	2	0	10
10005	0	0	0	2	0	11
10006	0	0	1	2	0	12
10007	0	0	0	2	0	13
10008	0	0	1	2	0	14
10009	0	0	0	2	0	15
10010	0	0	1	2	0	16
10011	0	0	0	2	0	17
10012	0	0	1	2	0	18
10013	0	0	0	2	0	19
10014	0	0	1	2	0	20
10015	0	0	0	2	0	21
10016	0	0	1	2	0	22
10017	0	0	0	2	0	23
10018	0	0	0	2	1	24
10019	0	0	0	2	4	25

Gambar 4.9 Tabel *messages* pada file whatsapp

Barang bukti percakapan ditemukan analisis forensik pada *file* whatsapp. Dengan menggunakan SQLite Database Browser dapat terlihat secara jelas isi dari file tersebut. Analisis forensik melakukan penyelidikan untuk setiap tabel pada *database* tersebut dan menemukan tabel yang berkaitan dengan kasus.

n

SQLite Database Browser - F:/skripsi RAPI/iphone/Application/net.whatsapp.WhatsApp/Documents/Contacts.sqlite

File Edit View Help

Database Structure Browse Data Execute SQL

Table: ZWAPHONE

..	Z PK	Z ENT	Z OPT	ZCONTACT	ZFAVORITE	ZSTATUS	ZLABEL	ZPHONE	ZWHATSAPPID
70	160	4	2	12			_!<Other>!\$	+622743091267	622743091267
71	162	4	2	196			_!<Other>!\$	+6283865246319	6283865246319
72	163	4	2	187			_!<Other>!\$	02747822281	622747822281
73	166	4	7	3	252		8 _!<Mobile>!\$	083867211823	6283867211823
74	167	4	2	67			_!<Other>!\$	+6287738909061	6287738909061
75	171	4	7	231	264		40 _!<Other>!\$	085740934030	6285740934030
76	173	4	6	228			_!<Other>!\$	08562850525	628562850525
77	177	4	2	230			_!<Other>!\$	0811859124	62811859124
78	179	4	6	221	279		57 _!<Other>!\$	08976867654	628976867654
79	181	4	7	218	280		29 _!<Other>!\$	085656276686	6285656276686
80	182	4	7	233	263		2 _!<Other>!\$	085641462950	6285641462950
81	188	4	2	210			_!<Other>!\$	+6285642527460	6285642527460
82	190	4	7	226	258		5 _!<Mobile>!\$	08122691510	628122691510
83	191	4	2	219			_!<Other>!\$	085742152345	6285742152345
84	194	4	2	216			_!<Other>!\$	8280100	628280100
85	195	4	7	227	274		46 _!<Other>!\$	085640449442	6285640449442
86	196	4	2	68			_!<Mobile>!\$	+628995858438	628995858438
87	199	4	2	238			_!<Mobile>!\$	+6281226400048	6281226400048
88	200	4	5	241	276		62 _!<Mobile>!\$	+6282135229911	6282135229911

Gambar 4.10 Tabel *zwapphone* pada file whatsapp

Barang bukti *contact* nomor telfon yang disimpan oleh pelaku ditemukan analisis forensik pada *file* whatsapp di folder document contact. Dengan menggunakan SQLite Database Browser dapat terlihat secara jelas isi dari *file* tersebut. Analisis forensik melakukan penyelidikan untuk setiap tabel.

Tabel 4.2 Hasil analisis terhadap file *net.whatsapp.whatsapp*

Nama Tabel	Value	Deskripsi
ZPhone	ZPHONE ZWHATSAPPID	Pada tabel zphone ditemukan daftar <i>contact</i> yang terdapat pada aplikasi whatsapp. Zphone menandakan nomer telepon dari kontak. Dan zwhatsappid menandakan ID yang dipakai oleh nomer itu sendiri. Diawali dengan '628'
Messages	Pada tabel terdapat percakapan yang dilakukan oleh pelaku	Tabel tersebut berisikan percakapan yang dilakukan oleh pelaku. Analisis mendalam akan dilakukan pada

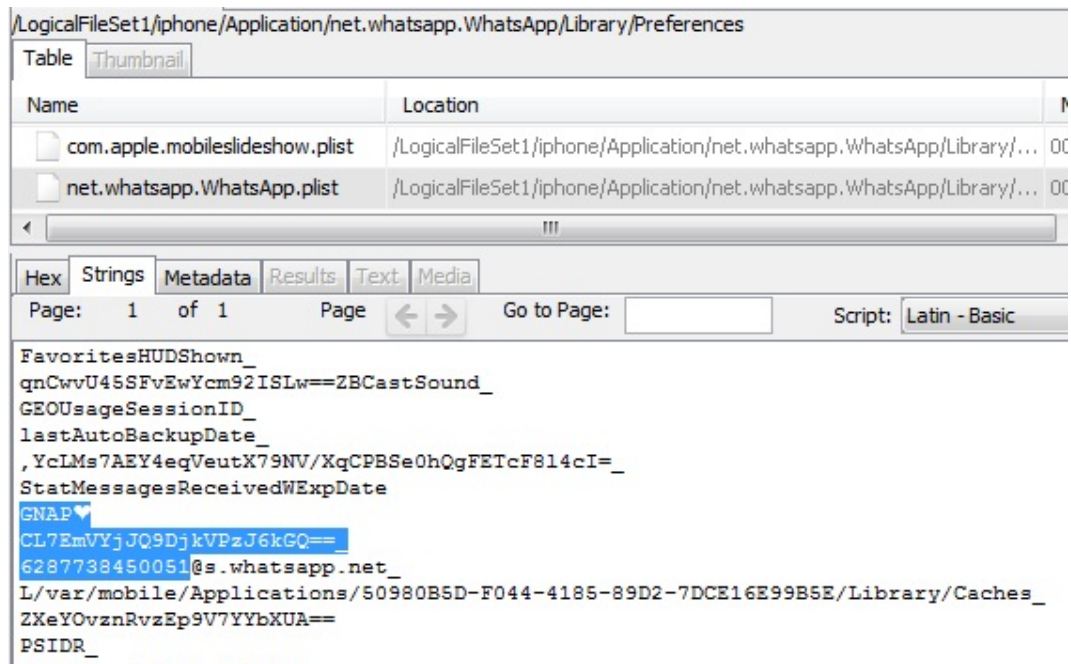
		pembahasan berikutnya.
--	--	------------------------

Pada tabel *messages* analis forensik melakukan analisis yang lebih mendalam untuk melengkapi barang bukti. Beberapa hasil analisis pada tabel *messages* akan dirangkum pada tabel berikut.

Tabel 4.3 Hasil analisis mendalam terhadap tabel *messages* pada file *whatsapp.db*

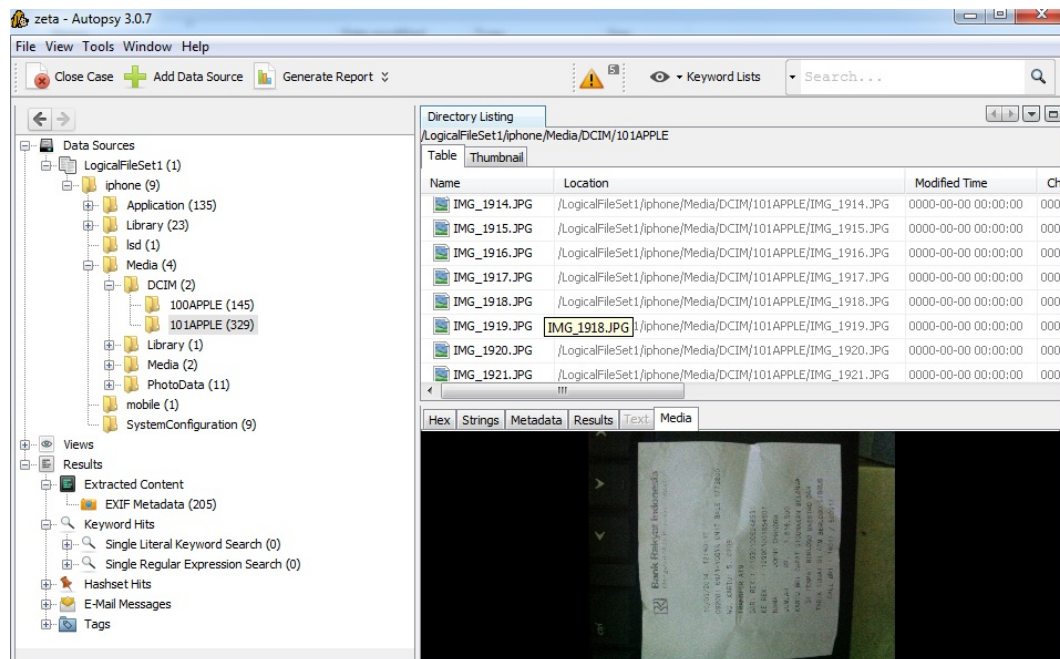
Nama Kolom	Value	Deskripsi
ZPK	15134,15135,15136 15137,..dst	Kolom tersebut berisikan urutan aktifitas chat yang dilakukan pelaku
ZFROMID	Nomor ID	Kolom tersebut berisikan ID nomor yang melakukan pengiriman pesan
ZTEXT	Percakapan/ <i>chat</i>	Kolom tersebut berisikan percakapan yang dilakukan oleh pelaku dan korban
ZISFROMME	1 dan 0	Kolom tersebut berisikan keterangan pengirim pesan. Value 1 menandakan korban mengirim pesan dan value 0 menandakan pelaku mengirim pesan.

Barang bukti status ID pelaku ditemukan analis forensik pada file *net.whatsapp.whatsapp* yang terletak pada direktori */Application/net.whatsapp.whatsapp/Library/Preference*. Barang bukti tersebut terlihat dengan Strings Viewer menggunakan tool Autopsy.



Gambar 4.11 Status ID pelaku ditemukan pada *file net.whatsapp.Whatsapp.plist*

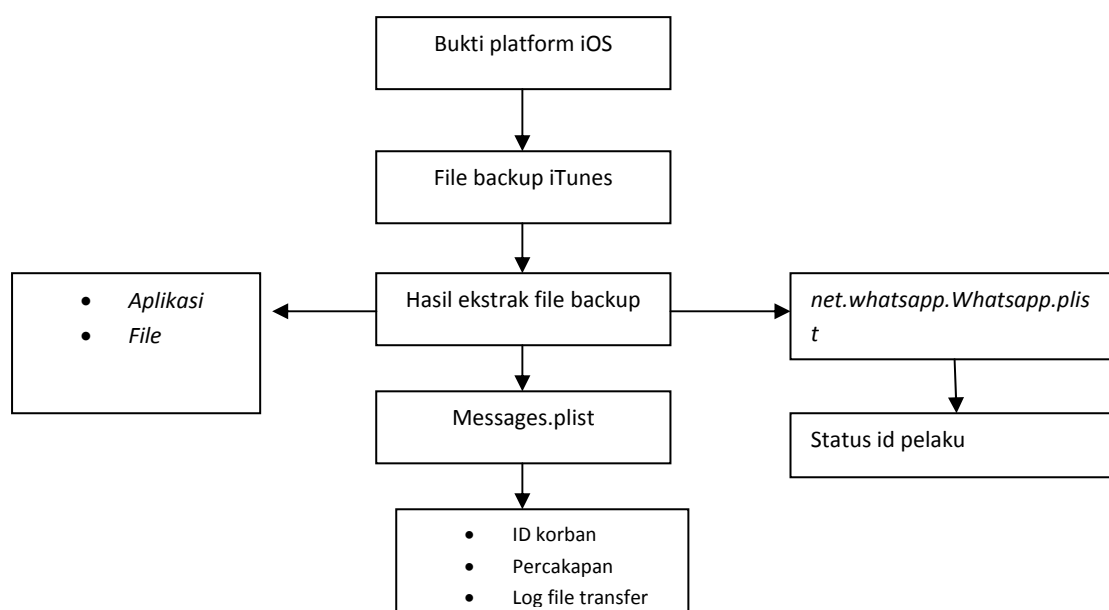
File gambar bernama IMG_1926.JPG yang dikirimkan korban kepada pelaku tersimpan pada direktori /media/DCIM/101 APPLE. File talamat.txt yang dikirim korban kepada pelaku tidak ditemukan. Terdapat 2 kemungkinan file alamat.txt tidak ditemukan yaitu dapat dikarenakan pelaku menghapus file tersebut sehingga tidak terdeteksi melalui hasil ekstrak backup. Kemungkinan kedua adalah pelaku tidak melakukan prosedur penyimpanan ketika mendapatkan kiriman *file* alamat.txt. Pada perangkat iOS, pengguna whatsapp dapat membuka kiriman *file* secara langsung tanpa harus menyimpannya.



Gambar 4.12 Direktori penyimpanan gambar yang dikirimkan korban kepada pelaku

4.1.4 Laporan Forensik iOS

Setelah melakukan 3 tahapan forensik, analis menemukan barang bukti yang didapatkan dari platform iOS yang digunakan oleh pelaku, pada gambar diperlihatkan barang bukti yang didapat.



Gambar 4.13 Barang bukti yang didapat pada platform iOS

4.1.5 Pengumpulan data iOS menggunakan Oxygen Forensic

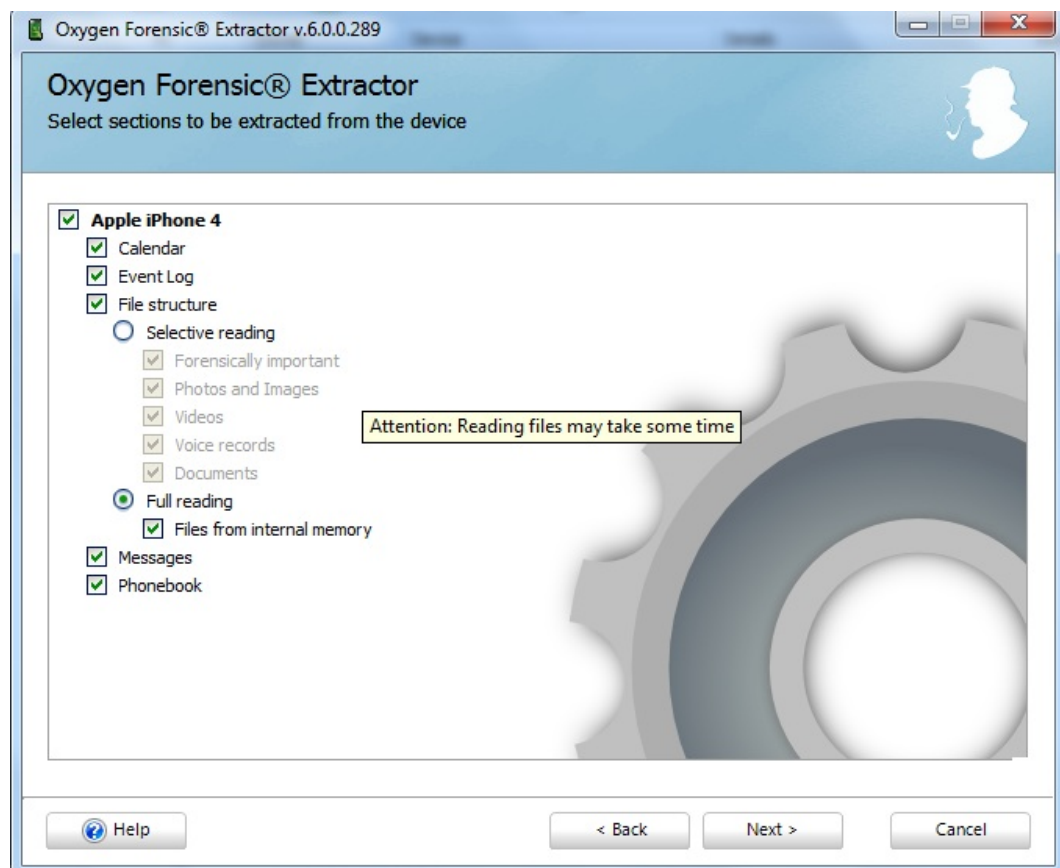
Perangkat iOS memiliki kemampuan untuk menyimpan data-data personal, sehingga dalam sisi forensik data personal ini perlu diselidiki. Oxygen Forensic adalah tools forensik mobile yang akan digunakan dalam melakukan analisis ini. Berikut adalah langkah-langkah melakukan pengambilan data menggunakan Oxygen Forensic.

1. Install Oxygen Forensic pada komputer.
2. Sambungkan perangkat iOS dengan komputer menggunakan kabel USB.
3. Jika iOS sudah tersambung maka akan muncul model iOS, IMEI, *Software Revision*, *Boot Loader* iOS pada Oxygen lalu klik next.



Gambar 4.14 perangkat iOS sudah tersambung dengan Oxygen

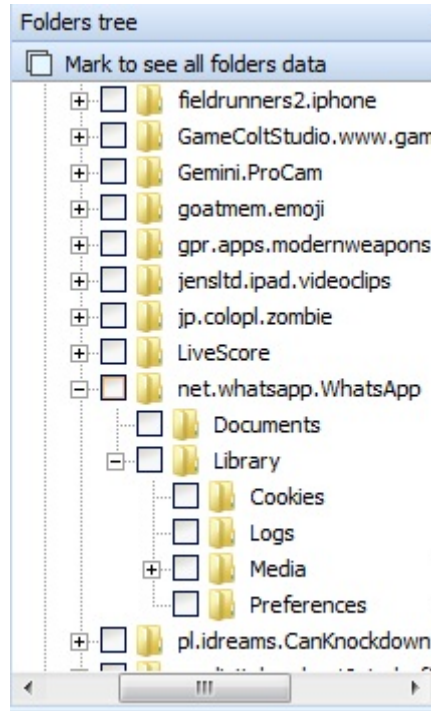
4. Langkah selanjutnya adalah mengisi daftar peneliti pada form oxygen. Langkah ini dilakukan untuk menjalankan proses investigasi secara jelas. Setelah semuanya selesai diisi lalu klik next.
5. Langkah selanjutnya adalah untuk memilih file apa saja yang akan di ekstrak. Karena analisis ini meneliti tentang aplikasi whatsapp, maka pilihan ekstraknya dipilih *full reading*. Pemilihan *full reading* dilakukan agar dapat melihat struktur file pada iOS secara lengkap. Jika sudah dicentang *full reading*, bisa langsung klik next.



Gambar 4.15 tampilan pilihan ekstrak yang ada dalam Oxygen Forensic

6. Jika langkah ekstrak file pada iOS berhasil, maka langsung klik finish dan perangkat iOS sudah bisa dianalisis.

Hasil ekstraksi *file* dapat diperlihatkan struktur *file* secara jelas dan nama *file* tersebut sehingga memudahkan dalam melakukan penyelidikan forensik. Hasil ekstraksi *file* tersebut merupakan struktur *file* dari perangkat iOS, sehingga teknik *recovery file* tidak perlu diterapkan.



Gambar 4.16 Struktur file whatsapp pada iOS

4.1.6 Pemeriksaan Forensik iOS dengan menggunakan Oxygen

Dalam tahapan pemeriksaan ini tidak perlu dilakukan menggunakan teknik filtering atau teknik file recovery karena saat membuka folder whatsapp maka akan langsung muncul file berbentuk database untuk memudahkan mencari file yang berkaitan dengan kasus.

4.1.7 Analisis Forensik iOS Dengan Oxygen

Proses backup pada iPhone menghasilkan file berbentuk OFB yang bisa dibuka menggunakan extraction wizzard.exe atau oxygen forensic. File tersebut berisi semua data pada iphone yang telah di backup dan disimpan untuk bisa diteliti lebih lanjut.

Peneliti memilih tool Oxygen Forensic untuk perbandingan dalam melakukan analisis pada barang bukti.

Hasil analisis melalui Oxygen Forensic ditemukan beberapa barang bukti terletak pada direktori */net.whatsapp.Whatsapp/document* dan */net.whatsapp.Whatsapp/library/document*.

Tabel 4.4 Struktur file whatsapp pada hasil ekstrak menggunakan oxygen

Lokasi Direktori	Barang bukti yang ditemukan	Deskripsi
<i>Private/var/mobile/Application</i>	Folder net.whatsapp.Whatsapp	Folder tersebut berisikan file aplikasi whatsapp yang masih utuh. Hal tersebut membuktikan pelaku tidak menghapus aplikasi untuk penghilangan barang bukti
<i>DCIM/101 APPLE</i>	IMG_1924 IMG_1925 IMG_1926	Terdapat dua gambar IMG_1924 dan IMG_1925 yang jika dibuka adalah foto vespa, sedangkan IMG_1926 adalah bukti transfer dengan kode bank BRI
<i>Private/var/mobile/Application/net.whatsapp.Whatsapp/document</i>	Chat storage.sqlite,colors.plist ,contact.sqlite,profilepicreq Data.plist,statuslist.plist, SyncHistory.plist,walpaper	Pada direktori tersebut terdapat percakapan, Profile pengguna,status Pengguna,dan walpaper pengguna.

Pada gambar 4.17 diperlihatkan isi dari folder */document* yang berada pada direktori *private/var/mobile/Application/net.whatsapp.Whatsapp*. folder tersebut berisikan file yang berkaitan dengan aktifitas chat. Ada 2 jenis file yaitu berekstensi *sqlite* dan *plist*.

Selected folder(s)					Images	Audio	Videos	Documents	Database files	Other files	PI
Name	Path	Size	Type								
☒ ChatStorage.sqlite	C:\private\var\mobile\Applicatio...	4,74 MB	SQLITE File								
☒ Colors.plist	C:\private\var\mobile\Applicatio...	1,11 KB	PLIST File								
☒ Contacts.sqlite	C:\private\var\mobile\Applicatio...	204,01 KB	SQLITE File								
☒ ProfilePicRequestDates.plist	C:\private\var\mobile\Applicatio...	496 B	PLIST File								
☒ StatusList.plist	C:\private\var\mobile\Applicatio...	1,44 KB	PLIST File								
☒ SyncHistory.plist	C:\private\var\mobile\Applicatio...	334 B	PLIST File								
☒ wallpaper	C:\private\var\mobile\Applicatio...	1,26 MB	File								

Gambar 4.17 isi dari *folder document*

ZMESSAGEDATE	ZFROMJID	ZPUSHNAME	ZSTANZAID	ZTEXT	ZTOJID
417055821	6282135229911@s.	Zeta Zone	1395359962-4	Hehehe,iya silahkan	
417055842.935234			1395250828-326	Sebelum nawar, itu r	6282135229911@s.
417055904	6282135229911@s.	Zeta Zone	1395359962-5	Itu vespa taun 64 je	
417055929.004295			1395250828-350	Klo masalah repaint	6282135229911@s.
417055989	6282135229911@s.	Zeta Zone	1395359962-6	Sekali selah langsun	
417056002.141949			1395250828-370	Itu vespa udah perr	6282135229911@s.
417056073	6282135229911@s.	Zeta Zone	1395359962-7	Macet sih belum gan	
417056083.535403			1395250828-389	Saya minta fotonya	6282135229911@s.
417056234	6282135229911@s.	Zeta Zone	1395359962-8	Jadiin dulu nawarny	
417056247.737673			1395250828-414	Nawar 2jt pas ya ga	6282135229911@s.
417056281	6282135229911@s.	Zeta Zone	1395359962-9	Tambahin lagi gan, c	
417056313.386217			1395250828-438	Duh berapa ya gan,	6282135229911@s.
417056348	6282135229911@s.	Zeta Zone	1395359962-10	Gini aja gan,tambah	
417056382.281633			1395250828-456	Yaudah oke deh. Ng	6282135229911@s.
417056410	6282135229911@s.	Zeta Zone	1395359962-11	Saya lokasi bekasi g	
417056489.534075			1395250828-485	Saya lokasi di wonos	6282135229911@s.
417056554	6282135229911@s.	Zeta Zone	1395359962-12	Bisa bisa gan,saya k	
417056964	6282135229911@s.	Zeta Zone	1395363912-1		
417056984	6282135229911@s.	Zeta Zone	1395363912-3		
417056996	6282135229911@s.	Zeta Zone	1395363912-2		
417057023.841656			1395250828-533	Oiya gan, nomer rek	6282135229911@s.
417057073	6282135229911@s.	Zeta Zone	1395363912-4	Ini norek saya gan,	
417057085	6282135229911@s.	Zeta Zone	1395363912-5	Bca atas nama avan	
417057104	6282135229911@s.	Zeta Zone	1395363912-6	Nanti klo udah trans	

Gambar 4.18 Tabel *messages* pada *file whatsapp*

SQLite Database browser - F:\skripsi\KAP\iphone\Application\net.whatsapp.whatsapp\Documents\chatstorage.sqlite

File Edit View Help

Database Structure Browse Data Execute SQL

Table: ZWAMESSAGE

ID	P1E	ZFLAGS	ISFROMME	ZMESSAGESTATUS	ZMESSAGETYPE	ZSORT
10001	0	0	0	2	0	7
10002	0	0	1	2	0	8
10003	0	0	0	2	0	9
10004	0	0	1	2	0	10
10005	0	0	0	2	0	11
10006	0	0	1	2	0	12
10007	0	0	0	2	0	13
10008	0	0	1	2	0	14
10009	0	0	0	2	0	15
10010	0	0	1	2	0	16
10011	0	0	0	2	0	17
10012	0	0	1	2	0	18
10013	0	0	0	2	0	19
10014	0	0	1	2	0	20
10015	0	0	0	2	0	21
10016	0	0	1	2	0	22
10017	0	0	0	2	0	23
10018	0	0	0	2	1	24
10019	0	0	0	2	4	25

Gambar 4.19 Tabel *messages* pada file whatsapp

Barang bukti percakapan ditemukan analisis forensik pada *file* whatsapp. Dengan menggunakan SQLite Database Browser dapat terlihat secara jelas isi dari file tersebut. Analisis forensik melakukan penyelidikan untuk setiap tabel pada *database* tersebut dan menemukan tabel yang berkaitan dengan kasus.

n

	Z_PK	Z_ENT	Z_OPT	ZCONTACT	ZFAVORITE	ZSTATUS	ZLABEL	ZPHONE	ZWHATSAPPID
70	160	4	2	12			_!<Other>!\$	+622743091267	622743091267
71	162	4	2	196			_!<Other>!\$	+6283865246319	6283865246319
72	163	4	2	187			_!<Other>!\$	02747822281	622747822281
73	166	4	7	3	252		8 _!<Mobile>!\$	083867211823	6283867211823
74	167	4	2	67			_!<Other>!\$	+6287738909061	6287738909061
75	171	4	7	231	264		40 _!<Other>!\$	085740934030	6285740934030
76	173	4	6	228			_!<Other>!\$	08562850525	628562850525
77	177	4	2	230			_!<Other>!\$	0811859124	62811859124
78	179	4	6	221	279		57 _!<Other>!\$	08976867654	628976867654
79	181	4	7	218	280		29 _!<Other>!\$	085656276686	6285656276686
80	182	4	7	233	263		2 _!<Other>!\$	085641462950	6285641462950
81	188	4	2	210			_!<Other>!\$	+6285642527460	6285642527460
82	190	4	7	226	258		5 _!<Mobile>!\$	08122691510	628122691510
83	191	4	2	219			_!<Other>!\$	085742152345	6285742152345
84	194	4	2	216			_!<Other>!\$	8280100	628280100
85	195	4	7	227	274		46 _!<Other>!\$	085640449442	6285640449442
86	196	4	2	68			_!<Mobile>!\$	+628995858438	628995858438
87	199	4	2	238			_!<Mobile>!\$	+6281226400048	6281226400048
88	200	4	5	241	276		62 _!<Mobile>!\$	+6282135229911	6282135229911

Gambar 4.20 Tabel *zwapphone* pada file whatsapp

Barang bukti *contact* nomor telfon yang disimpan oleh pelaku ditemukan analisis forensik pada *file* whatsapp di folder document contact. Dengan menggunakan SQLite Database Browser dapat terlihat secara jelas isi dari *file* tersebut. Analisis forensik melakukan penyelidikan untuk setiap tabel.

Tabel 4.5 Hasil analisis terhadap file *net.whatsapp.whatsapp*

Nama Tabel	Value	Deskripsi
Zphone	ZPHONE ZWHATSAPPID	Pada tabel zphone ditemukan daftar <i>contact</i> yang terdapat pada aplikasi whatsapp. Zphone menandakan nomer telepon dari kontak. Dan zwhatsappid menandakan ID yang dipakai oleh nomer itu sendiri. Diawali dengan '628'
Messages	Pada tabel terdapat percakapan yang dilakukan oleh pelaku	Tabel tersebut berisikan percakapan yang dilakukan oleh pelaku. Analisis mendalam akan dilakukan pada

		pembahasan berikutnya.
--	--	------------------------

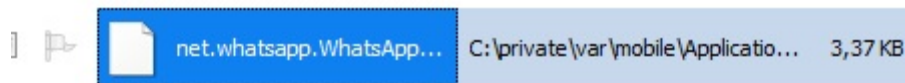
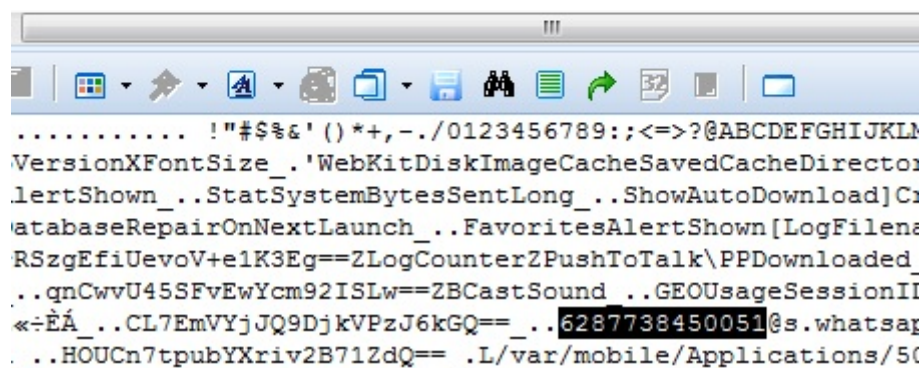
Pada tabel *messages* analis forensik melakukan analisis yang lebih mendalam untuk melengkapi barang bukti. Beberapa hasil analisis pada tabel *messages* akan dirangkum pada tabel berikut.

Tabel 4.6 Hasil analisis mendalam terhadap tabel *messages* pada file *whatsapp.db*

Nama Kolom	Value	Deskripsi
ZPK	15134,15135,15136 15137,..dst	Kolom tersebut berisikan urutan aktifitas chat yang dilakukan pelaku
ZFROMID	Nomor ID	Kolom tersebut berisikan ID nomor yang melakukan pengiriman pesan
ZTEXT	Percakapan/ <i>chat</i>	Kolom tersebut berisikan percakapan yang dilakukan oleh pelaku dan korban
ZISFROMME	1 dan 0	Kolom tersebut berisikan keterangan pengirim pesan. Value 1 menandakan korban mengirim pesan dan value 0 menandakan pelaku mengirim pesan.

Barang bukti status ID pelaku ditemukan analis forensik pada file *net.whatsapp.whatsapp* yang terletak pada direktori *private/var/mobile/Application/net.whatsapp.whatsapp/Library/Preference*.

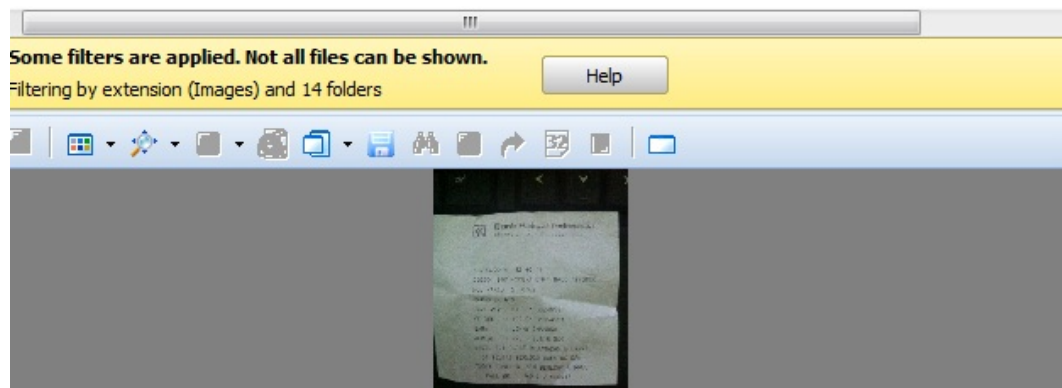
Barang bukti tersebut terlihat dengan menggunakan tool Oxygen.



Gambar 4.21 Nomor telepon ID pelaku ditemukan pada *file net.whatsapp.Whatsapp.plist*

File gambar bernama IMG_1926.JPG yang dikirimkan korban kepada pelaku tersimpan pada direktori /media/DCIM/101 APPLE. File alamat.txt yang dikirim korban kepada pelaku tidak ditemukan. Terdapat 2 kemungkinan file alamat.txt tidak ditemukan yaitu dapat dikarenakan pelaku menghapus file tersebut sehingga tidak terdeteksi melalui hasil ekstrak backup. Kemungkinan kedua adalah pelaku tidak melakukan prosedur penyimpanan ketika mendapatkan kiriman *file* alamat.txt.

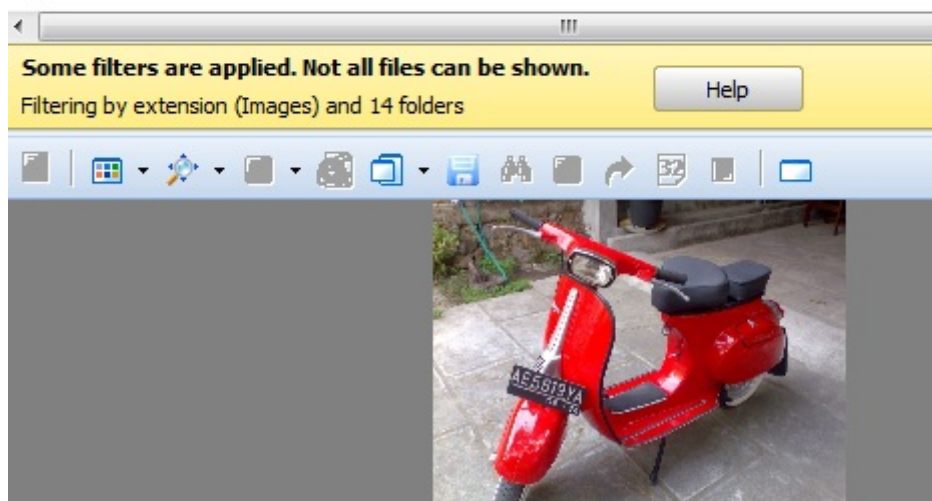
	Path	Name	Size	Type
	C:\private\var\mobile\Applicatio...	4e3fe37f91367d6428807...	68,24 KB	JPEG im
	C:\private\var\mobile\Applicatio...	5d92ec3474cafff3b6b14...	6,38 KB	PNG im
	C:\private\var\mobile\Applicatio...	915c3e999350cfe9e24f9...	5,40 KB	PNG im
	C:\private\var\mobile\Applicatio...	be5b66d2e560000e6ec...	78,20 KB	JPEG im
	C:\private\var\mobile\Applicatio...	f61f1bce88e33c20b1ff11...	70,65 KB	JPEG im



Gambar 4.22 Direktori gambar bukti transfer yang dikirimkan korban kepada pelaku

File gambar bernama IMG_1926.JPG yang dikirimkan korban kepada pelaku tersimpan pada direktori /media/DCIM/101 APPLE. File alamat.txt yang dikirim korban kepada pelaku tidak ditemukan. Terdapat 2 kemungkinan file alamat.txt tidak ditemukan yaitu dapat dikarenakan pelaku menghapus file tersebut sehingga tidak terdeteksi melalui hasil ekstrak backup. Kemungkinan kedua adalah pelaku tidak melakukan prosedur penyimpanan ketika mendapatkan kiriman *file* alamat.txt.

Selected folder(s)				Images	Audio	Videos	Documents
	Path	Name	Size				
☒	C:\private\var\mobile\Applicatio...	4e3fe37f91367d6428807...	68,24 KB				
☒	C:\private\var\mobile\Applicatio...	5d92ec3474cafff3b6b14...	6,38 KB				
☒	C:\private\var\mobile\Applicatio...	915c3e999350cfe9e24f9...	5,40 KB				
☒	C:\private\var\mobile\Applicatio...	be5b66d2e560000e6ec...	78,20 KB				
☒	C:\private\var\mobile\Applicatio...	f61f1bce88e33c20b1ff11...	70,65 KB				



Gambar 4.23 Foto vespa yang ditemukan pada direktori DCIM

4.1.8 Review Forensik iOS

Berikut adalah review tool yang digunakan dalam melakukan forensik pada iOS. Review tool dapat digunakan untuk bahan pembanding penelitian selanjutnya.

Tabel 4.7 Tool yang digunakan dalam forensik pada iOS

Tahapan	Tool yang dapat digunakan	Tool yang dipilih	Alasan
Backup memori	<ul style="list-style-type: none"> • iTunes • iCloud • oxygen forensic 	<ul style="list-style-type: none"> • iTunes • oxygen forensic 	Data langsung bisa didapat di komputer
Ekstrak file backup	<ul style="list-style-type: none"> • iPhone backup extractor • iPhone Backup Browser • Oxygen Forensic 	<ul style="list-style-type: none"> • iPhone Backup Extractor • oxygen forensic 	Lebih mudah untuk digunakan dan tidak berbayar. Memilih oxygen untuk perbandingan dengan tool lain
Filter dan analisis hasil ekstrak file backup	<ul style="list-style-type: none"> • Autopsy • FTK (<i>Forensic Tool Kit</i>) • Oxygen forensic 	<ul style="list-style-type: none"> • Autopsy • Oxygen forensic 	<p>Karena FTK tidak memungkinkan digunakan karena keterbatasan file.</p> <p>Memilih oxygen untuk perbandingan dengan tool lain</p>
Analisis file database	SQLite Data Browser	SQLite Data Browser	Mudah untuk digunakan dan aplikasi ini tidak berbayar

4.2 Forensik Pada Android

Peneliti memilih Android yang diforensik adalah dalam keadaan hidup karena dibutuhkan informasi dari memori *internal*. Ketika barang bukti Android ditemukan di TKP dalam keadaan hidup, maka analis forensik dan investigator melakukan prosedur sebagai berikut :

1. Analis tidak mematikan perangkat dan membiarkan dalam keadaan menyala. Jika layar dalam keadaan aktif maka analis melakukan perubahan *setting* yaitu merubah *timeout screen* menjadi paling lama untuk menyala dan meengaktifkan USB Debugging serta mengaktifkan Stay Awake. Hal ini dimaksudkan agar menambah waktu analis dalam melakukan pemeriksaan sebelum perangkat mengunci layar.
2. Mencatat spesifikasi dari barang bukti. Ditemukan spesifikasi barang bukti sebagai berikut :
 - ZTE N986
 - OS Android 4.2.1 (JellyBean)
 - Status Root
 - Jaringan CDMA
 - RAM 1 GB
 - Memori internal 4 GB
 - Memori eksternal 4 GB (bisa dicabut dari perangkat)
 - Waktu pada Android sama dengan waktu lokal
3. Membangun suatu area tanpa sinyal dengan kantong faraday atau jammer. Cara yang paling sederhana adalah mengubah Android menjadi *airplane mode*.
4. Akses perangkat dengan menghubungkan ke komputer menggunakan kabel data, bluetooth atau infrared. Disarankan pengaksesan perangkat menggunakan kabel data USB port yang sudah terproteksi akses penulisan (*write protect*)
5. Setelah proses konektivitas dan sinkronisasi melalui instalasi driver perangkat selesai, proses selanjutnya adalah melakukan pengumpulan data dan pemeriksaan.
6. Matikan perangkat dengan menekan tombol *power* atau melalui prosedur yang disediakan oleh perangkat. Setelah itu cabutt baterai dan dilanjutkan dengan melakukan mencabut *SIM Card* dan memori ekstrenal (jika ada) untuk pemeriksaan lebih lanjut.

Dalam penelitian ini, perangkat memiliki memori eksternal yang bisa dicabut dari perangkatnya.

7. Setelah semua proses pemeriksaan selesai, *SIM card* dan memori eksternal dikembalikan ke slot perangkat seperti semula.
8. Untuk perangkat yang baterainya hampir habis, sebaiknya dicarikan *charger* untuk memberikan daya. Jika *charger* tidak ditemukan, maka perangkat dapat dimatikan dan proses pemeriksaan selanjutnya dianggap sebagai perangkat dalam keadaan mati.

4.2.1 Pengumpulan data forensik Android

Forensic imaging pada Android dibagi menjadi 2 yaitu *backup* memori internal, dan *forensic imaging* memori internal. 2 sumber tersebut bisa didapat jika Android dalam keadaan *Root*. Android dalam keadaan tidak root hanya dapat diperiksa memori eksternalnya saja.

4.2.1.1 Backup Android

Untuk melakukan proses backup memori internal, peneliti memilih tool Oxygen forensic untuk membandingkan dengan tool yang lain. Berikut adalah langkah-langkah dalam melakukan proses backup memori internal Android.

1. Download tool Oxygen forensic.
2. Sambungkan perangkat Android pada komputer agar perangkat dapat terdeteksi oleh oxygen.

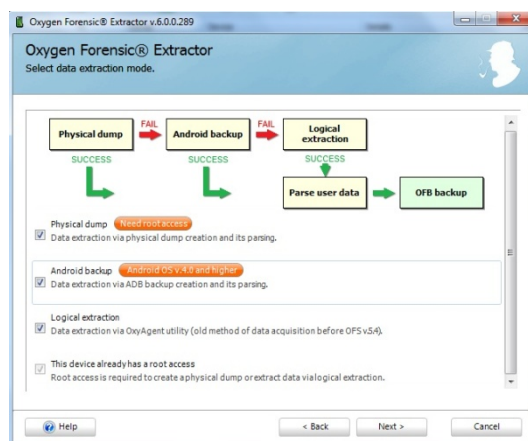


Gambar 4.24 Perangkat android sudah tersambung dengan oxygen

3. Setelah Android sudah tersambung dengan oxygen, maka langkah selanjutnya mengisi form peneliti pada tool oxygen.

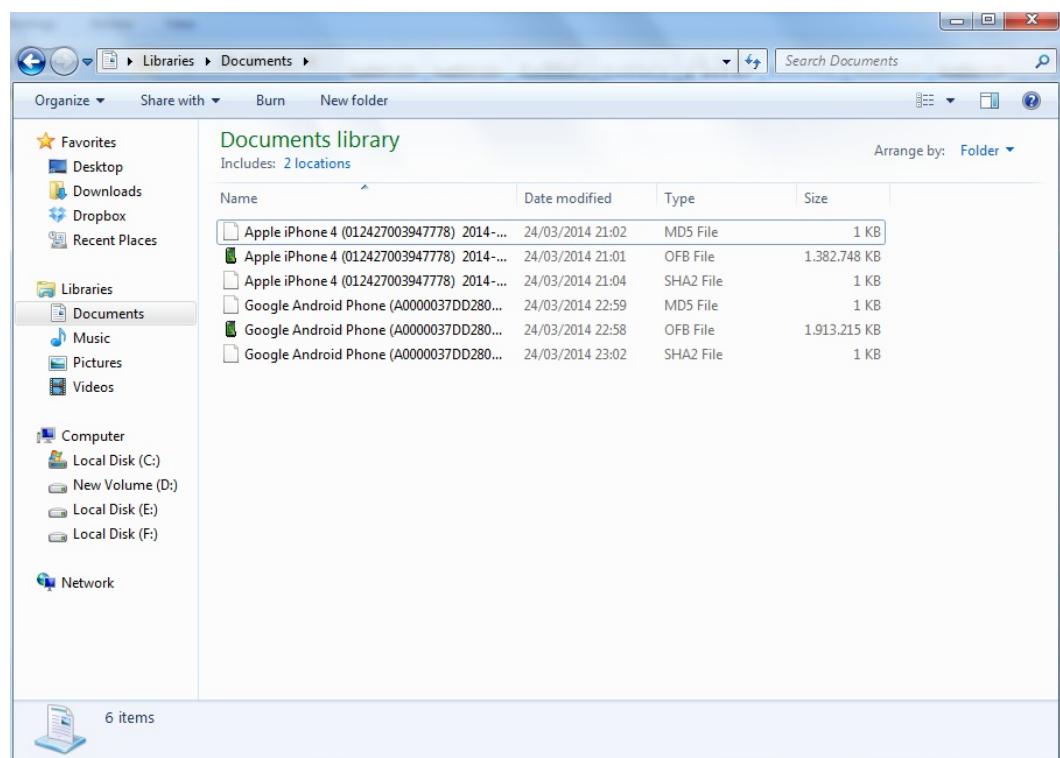
Gambar 4.25 lembar peneliti pada oxygen forensic

4. Langkah selanjutnya adalah memilih jenis data apa saja yang akan dibackup pada Android. Pemilihan jenis data mempengaruhi kecepatan backup pada oxygen.

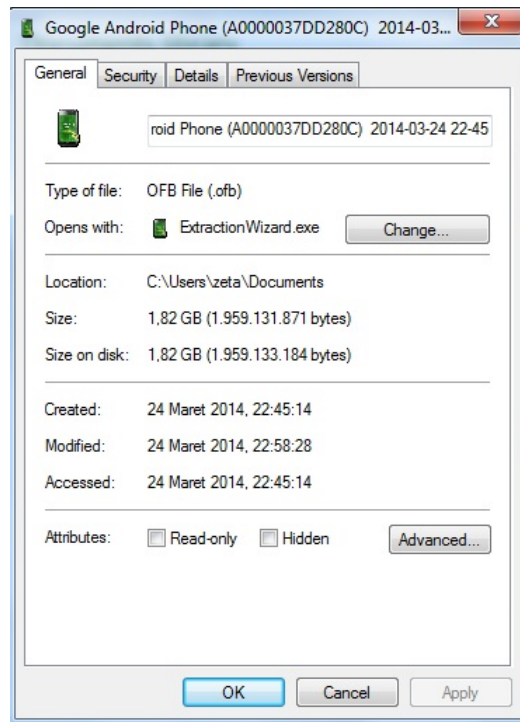


Gambar 4.26 alur proses backup pada tool oxygen

5. File hasil backup akan tersimpan pada komputer di *libraries/document*. Hasil file backup bertipe OFB dan hanya bisa diekstrak menggunakan oxygen forensik maupun extraction wizzard.

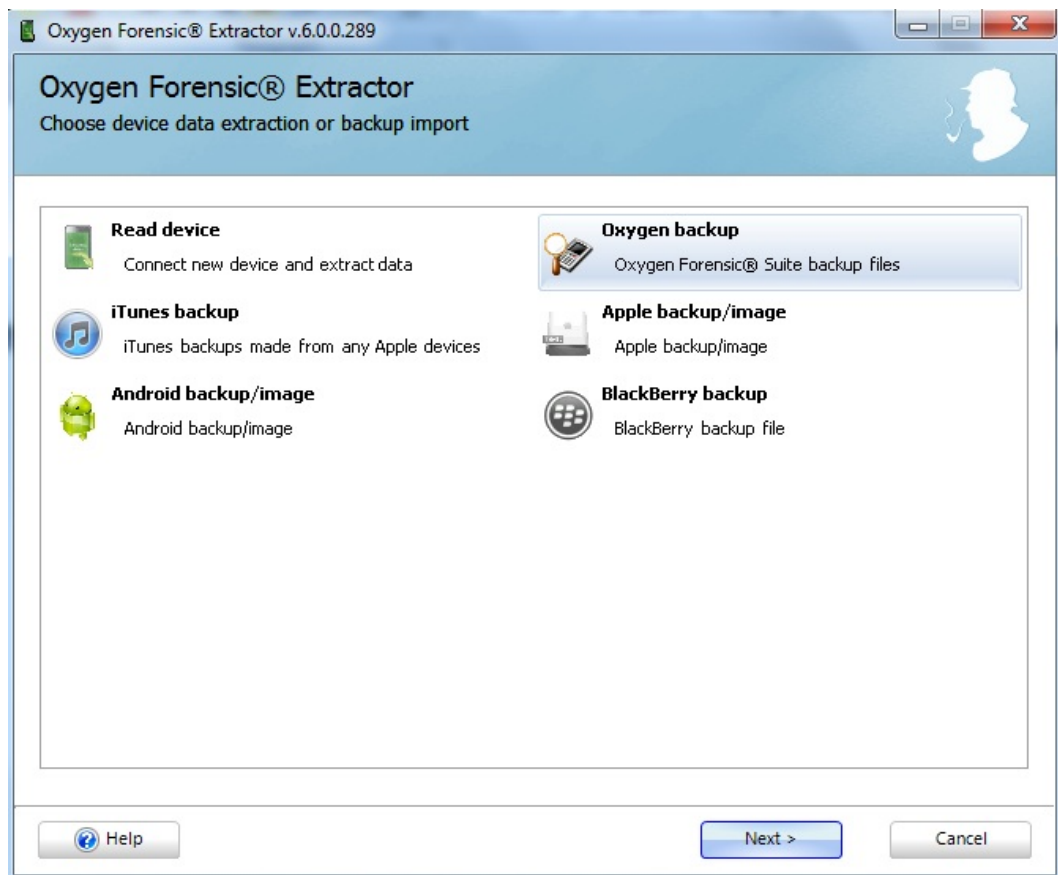


Gambar 4.27 hasil backup memori internal menggunakan oxygen



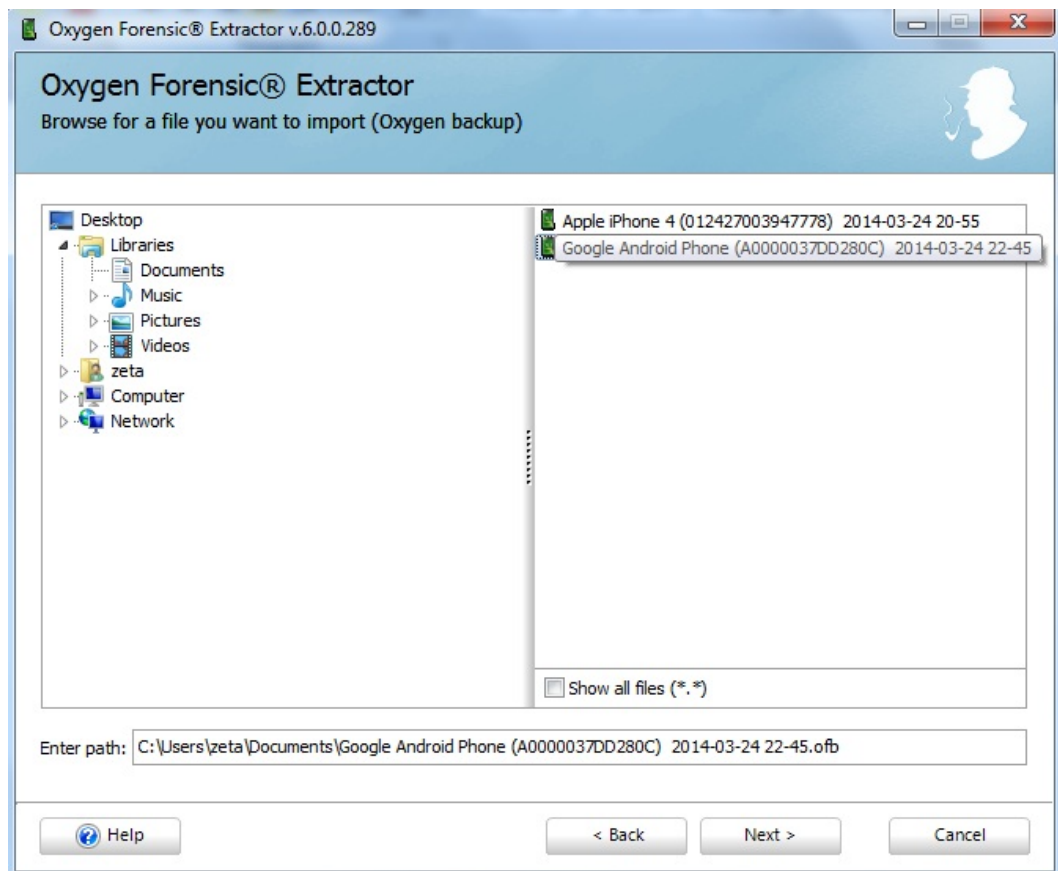
Gambar 4.28 Tipe file backup Android

6. File hasil backup diekstrak menggunakan tool oxygen data extraction yang sudah didapatkan satu paket saat instalasi oxygen forensic.
7. Buka tool oxygen data extraction, pilih oxygen backup lalu klik next. Tool ini hanya bisa mengekstrak jenis file yang di backup menggunakan oxygen forensic.



Gambar 4.29 Proses ekstrak file backup Android menggunakan oxygen data ekstraktor

8. Pilih file yang akan diekstrak pada folder libraries/document/Google Android Phone. File data akan mempengaruhi kecepatan saat ekstrak.



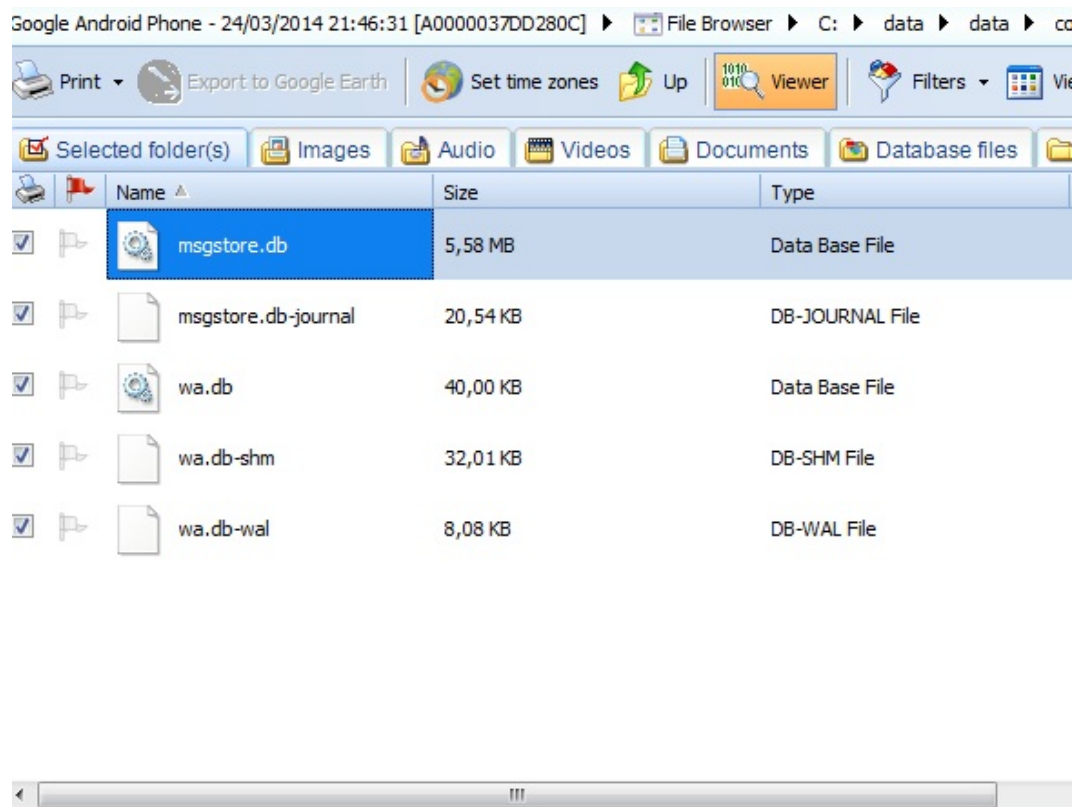
Gambar 4.30 Pemilihan file yang akan diekstrak menggunakan oxygen data extractor.

Hasil ekstraksi dari file backup memori internal merupakan ofb file sehingga teknik *recovery file* tidak dapat dilakukan pada file ini. Selanjutnya hasil ekstraksi akan dianalisis forensik lebih dalam menggunakan oxygen forensic.

4.2.2 Pemeriksaan forensik Android

Pada tahap ini, file yang berbentuk ofb file dilakukan pemeriksaa secara komperhensif untuk mendapatkan data-data digital yang sesuai dengan investigasi. Analisis forensik melakukan pencarian (*searching*) terhadap isi ofb file untuk mendapatkan file atau data yang diinginkan.

Peneliti memilih tool oxygen forensic untuk membandingkan dengan tool yang lain.



Gambar 4.31 file berbentuk database yang ditemukan pada whatsapp menggunakan tool oxygen forensic

4.2.3 Analisis forensik Android

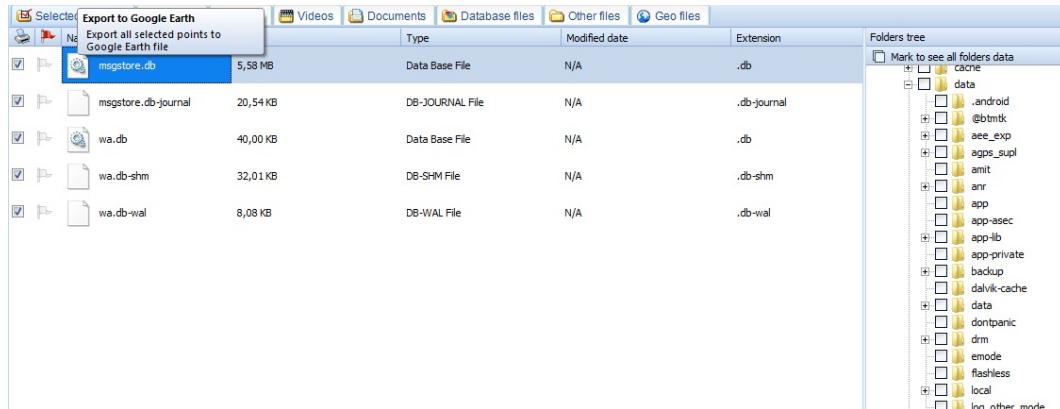
Proses forensik imaging pada android menggunakan tool oxygen menghasilkan satu file berbentuk ofb yang akan dianalisis lebih lanjut. File berbentuk ofb ini adalah image file yang hanya bisa dibuka menggunakan tool oxygen forensic saja.

4.2.3.1 Hasil dan pembahasan Android

Android pada umumnya terdiri dari 5 partisi untuk sistem berkasnya yaitu *1, cache, data, sdcard, system*. Pada penelitian ini difokuskan pada partisi system dan data saja.

Peneliti menggunakan tool oxygen untuk menganalisis barang bukti. Karena untuk membandingkan dengan autopsy dan tidak memungkinkan untuk menggunakan FTK (versi tidak berbayar) karena ada batasan 5000 file dalam pemeriksaannya.

Aplikasi whatsapp yang tersinstal pada Android secara default tersimpan pada memori internal. Strukur file Android yang terdapat pada oxygen mempunyai banyak struktur file tetapi hanya akan diteliti direktori data saja.



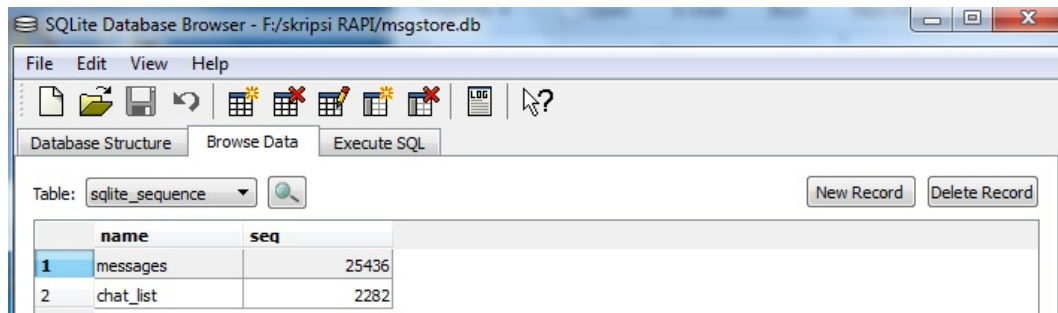
Gambar 4.32 struktur file yang terdapat pada direktori data

Pada direktori *data* banyak ditemukan barang bukti yang berkaitan dengan whatsapp. Yaitu terletak pada */data/data/com.whatsapp/database*. Beberapa bukti tersebut akan dirangkum pada tabel berikut agar mudah dalam pembacaannya.

Tabel 4.8 Struktur file barang bukti Android menggunakan oxygen

Lokasi direktori	Barang bukti yang ditemukan	Deskripsi
Data/data	Folder com.whatsapp	Folder tersebut berisikan file aplikasi whatsapp yang masih utuh. Hal tersebut membuktikan pelaku tidak menghapus aplikasi untuk penghilangan barang bukti
Data/data/com.whatsapp/database	File <i>msgstore.db</i>	Pada file tersebut ditemukan banyak barang bukti yang berkaitan dengan kasus diantaranya ID pelaku, daftar teman, percakapan dan status ID pelaku.

Analisis mendalam yang dilakukan pada file *msgstore.db* yang terdapat pada direktori */data/data/com.whatsapp/database*, ditemukan beberapa barang bukti. Pada gambar 4.33 diperlihatkan beberapa barang bukti yang ditemukan oleh analis forensik.



SQLite Database Browser - F:/skripsi RAPI/msgstore.db

File Edit View Help

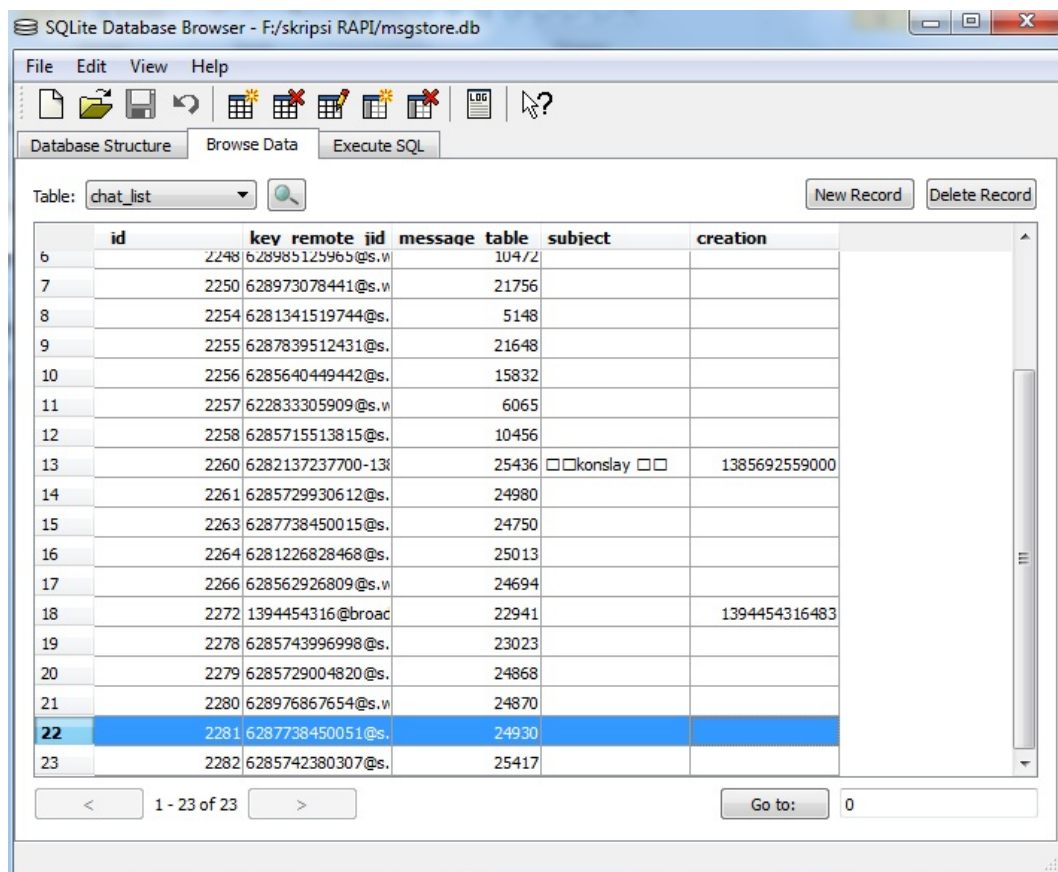
Database Structure Browse Data Execute SQL

Table: sqlite_sequence

	name	seq
1	messages	25436
2	chat_list	2282

New Record Delete Record

Gambar 4.33 tabel *sqlite_sequence* pada *msgstore.db*



SQLite Database Browser - F:/skripsi RAPI/msgstore.db

File Edit View Help

Database Structure Browse Data Execute SQL

Table: chat_list

	id	key	remote	jid	message	table	subject	creation
6	2248	628985125965	@s.w		10472			
7	2250	628973078441	@s.w		21756			
8	2254	6281341519744	@s.		5148			
9	2255	6287839512431	@s.		21648			
10	2256	6285640449442	@s.		15832			
11	2257	622833305909	@s.w		6065			
12	2258	6285715513815	@s.		10456			
13	2260	6282137237700-13			25436	☐ konslay ☐		1385692559000
14	2261	6285729930612	@s.		24980			
15	2263	6287738450015	@s.		24750			
16	2264	6281226828468	@s.		25013			
17	2266	628562926809	@s.w		24694			
18	2272	1394454316	@broac		22941			1394454316483
19	2278	6285743996998	@s.		23023			
20	2279	6285729004820	@s.		24868			
21	2280	628976867654	@s.w		24870			
22	2281	6287738450051	@s.		24930			
23	2282	6285742380307	@s.		25417			

1 - 23 of 23

Go to: 0

Gambar 4.34 tabel *chat list* pada *msgstore.db*

Dengan menggunakan SQLite Database Browser dapat terlihat secara jelas isi dari file tersebut. Analisis forensik melakukan penyidikan untuk setiap tabel pada database tersebut dan menemukan tabel yang berkaitan dengan kasus.

Tabel 4.9 file *message.db* pada direktori whatsapp

Nama tabel	Value	Deskripsi
Chat list	+6287738450051, +628135229911, dll	Tabel tersebut berisikan daftar teman dari ID pelaku. Terdapat nomer +6287738450051 yang merupakan ID korban.
Sqlite_sequence	Terdapat 2 kategori yaitu chat list dan messages	Tabel tersebut berisikan jumlah pesan yang sudah dikirim oleh pelaku
Messages	Pada tabel terdapat percakapan yang dilakukan oleh pelaku	Tabel tersebut berisikan percakapan yang dilakukan oleh pelaku. Analisis mendalam akan dilakukan pada pembahasan berikutnya.

Gambar 4.35 tabel *messages* pada *msgstore.db*

Seperti terlihat pada gambar, pada tabel *msgstore.db* ditemukan percakapan antara pelaku dan korban. Berikut adalah hasil dari analisis yang dilakukan pada tabel *messages*.

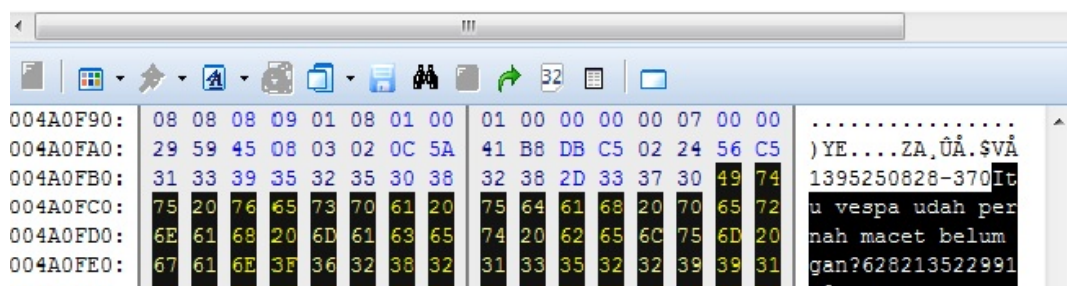
Tabel 4.10 hasil analisis mendalam terhadap tabel *messages* pada file *msgstore.db*

Nama kolom	Value	Deskripsi
Id	607,608,609,610,611,... dst	Berisikan urutan percakapan yang dilakukan oleh pelaku
Key remote_jid	+6287738450051, +628135229911, dst	Kontak yang sedang dihubungi oleh pelaku, termasuk id pelaku sendiri
Key from me	0 dan 1	Value 1 menandakan pelaku mengirim chat, dan value 0 menandakan

		pelaku menerima chat.
Key id	-1, -2, -3, -4, dst	Urutan id pelaku melakukan aktifitas chat dengan korban
Status	0, 4 dst	Value 0 menandakan pelaku menerima pesan dan value 4 pelaku mengirim pesan
Need push	0	Aktifitas chat pada tabel messages ditandai dengan angka 0
Data	Percakapan	Pada kolom tersebut berisikan percakapan yang dilakukan oleh pelaku

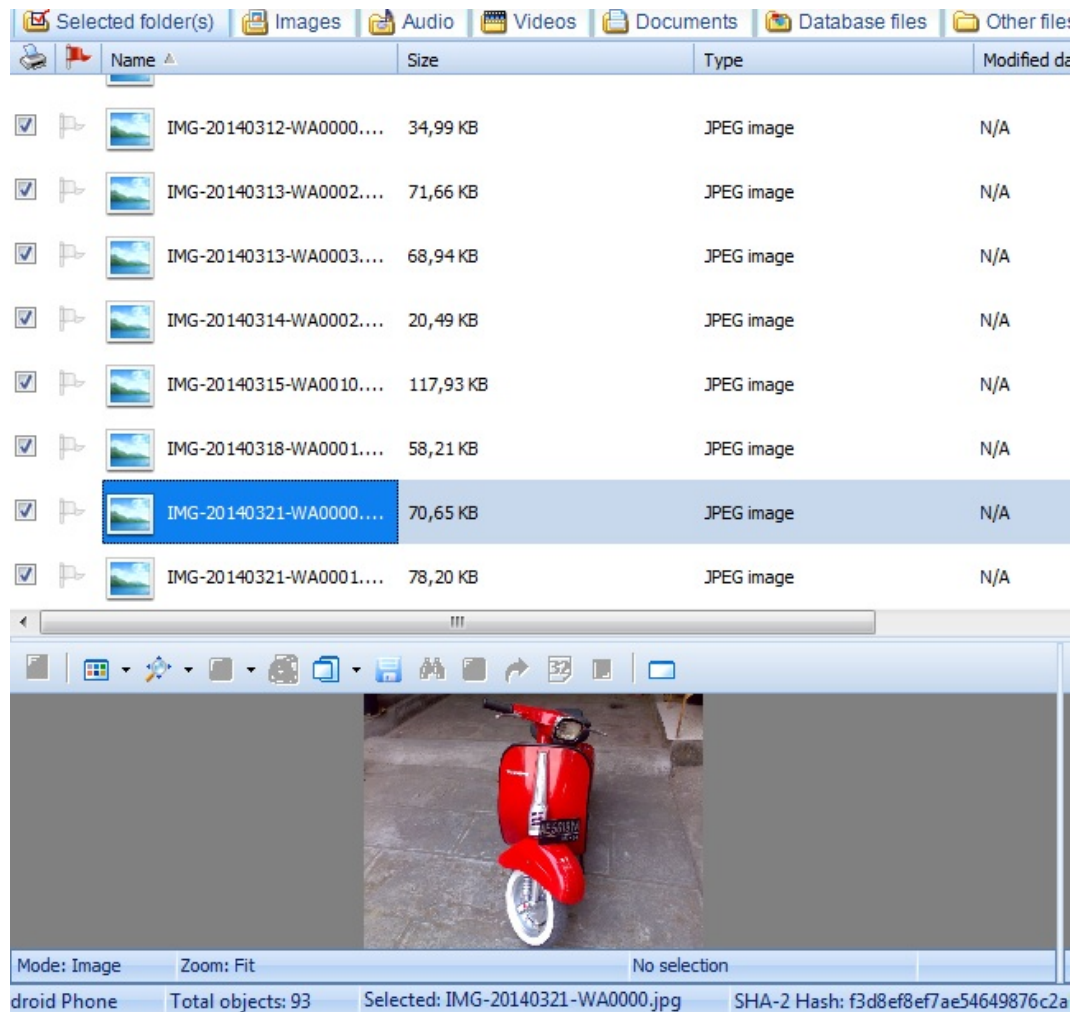
Selain menggunakan SQLite Data Browser, peneliti juga menemukan bukti percakapan pada chatstorage.sqlite yang bisa dibuka langsung menggunakan oxygen forensic. Bukti salah satu percakapan ini bisa dilihat secara jelas pada gambar 4.36

	Name	Size	Type	Path
☒	ChatStorage.sqlite	4,74 MB	SQLITE File	C:\private\va
☒	Colors.plist	1,11 KB	PLIST File	C:\private\va
☒	Contacts.sqlite	204,01 KB	SQLITE File	C:\private\va
☒	ProfilePicRequestDates.plist	496 B	PLIST File	C:\private\va
☒	StatusList.plist	1,44 KB	PLIST File	C:\private\va
☒	Synchistory.plist	334 B	PLIST File	C:\private\va
☒	wallpaper	1,26 MB	File	C:\private\va



Gambar 4.36 bukti salah satu percakapan korban ditemukan dengan tool oxygen

Barang bukti selain percakapan salah satu korban juga ditemukan bukti lain berupa file gambar yang dikirim oleh pelaku kepada korban. Bukti ini ditemukan pada folder DCIM pada direktori data.



Gambar 4.37 Barang bukti gambar vespa yang dikirim pelaku kepada korban terdapat pada direktori DCIM.

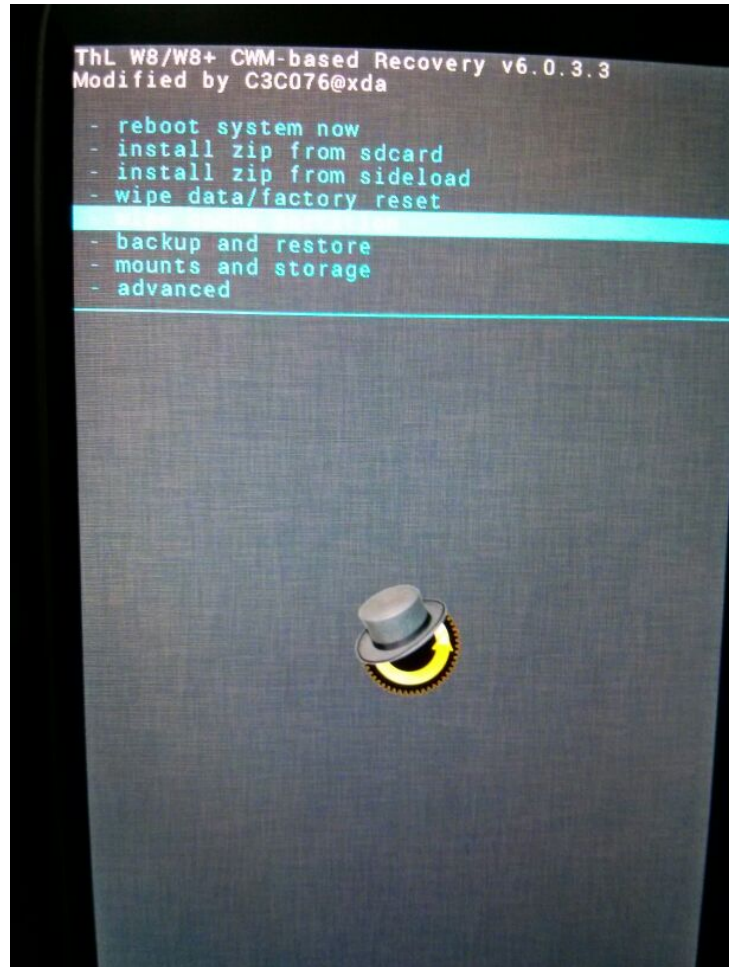
4.2.4 Pengumpulan Data Android Menggunakan CWM (*Clock Work Mod*)

Forensic imaging pada Android dibagi menjadi 2 yaitu *backup* memori internal, dan *forensic imaging* memori internal. 2 sumber tersebut bisa didapatkan jika Android dalam keadaan Root. Android dalam keadaan tidak Root hanya dapat diperiksa memori eksternalnya saja.

4.2.4.1 Backup Android

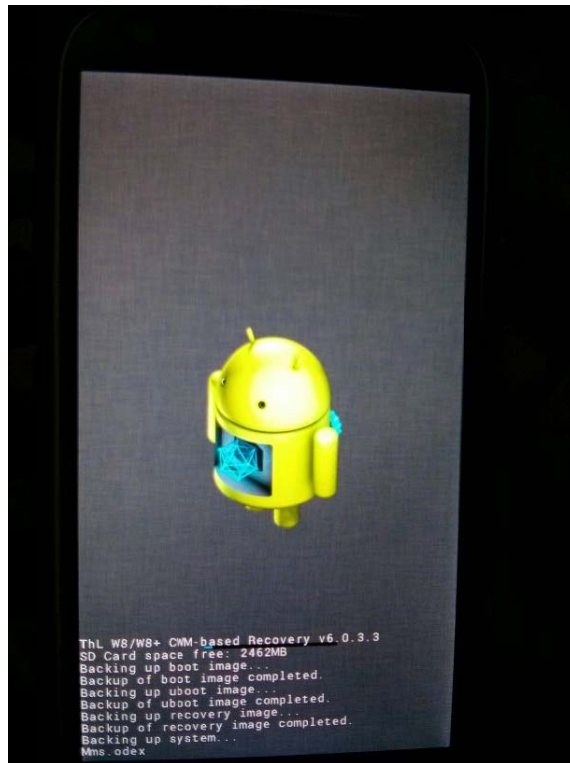
Untuk melakukan proses backup memori internal, peneliti memilih tool CWM (*Clock Work Mod*). Berikut adalah langkah-langkah dalam melakukan proses backup memori internal Android.

1. Download Mobile Uncle di Playstore
2. Matikan perangkat dan masuk ke CWM dengan cara tekan power dan tombol volume up secara bersamaan dalam waktu yang lumayan lama sampai masuk ke menu CWM.



Gambar 4.x Tampilan awal CWM pada perangkat Android

3. Setelah perangkat Android bisa masuk CWM, arahkan volume down ke backup and restore lalu tekan tombol power untuk melanjutkan proses.
4. Pada saat proses backup berlangsung, perangkat Android tidak boleh mati atau kehabisan baterai. Hal ini dikarenakan bila perangkat mati kemungkinan backup akan gagal.



Gambar 4.x Proses backup Android menggunakan CWM

5. Hasil backup akan tersimpan di memori eksternal Android. Saat proses backup berlangsung pastikan memori eksternal Android lebih besar daripada memori internal.
6. Setelah proses backup berhasil, maka langkah selanjutnya adalah reboot perangkat dan masuk ke file manager Android untuk melihat hasil backup.

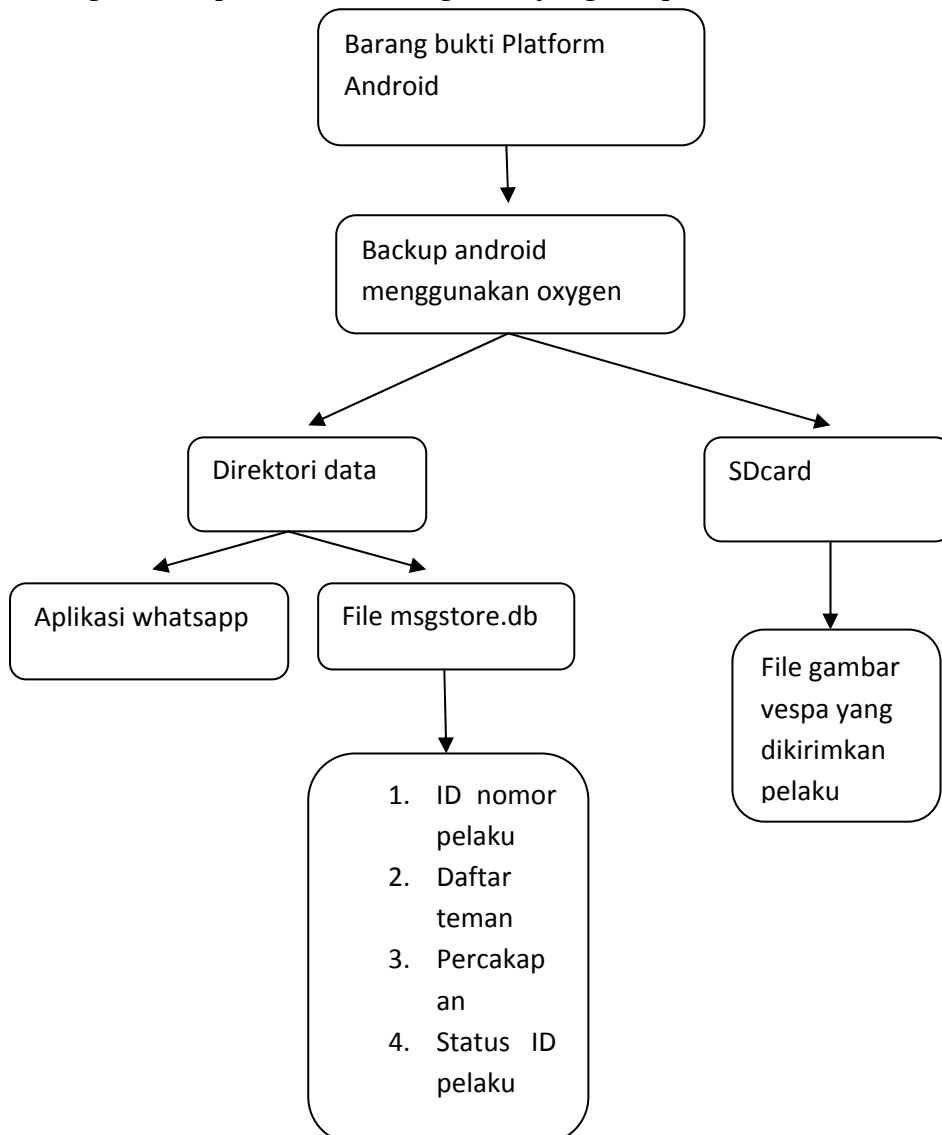


Gambar 4.x Hasil backup menggunakan CWM

File hasil backup menggunakan CWM berupa .tar dan belum bisa menemukan cara untuk mengekstrak file tersebut untuk melanjutkan ke langkah *image memori* internal. Jadi backup menggunakan tool CWM dikatakan gagal karena tidak dapat melanjutkan ke langkah *image memori* internal dan analisis lebih dalam untuk menemukan bukti pada perangkat Android.

4.2.5 Laporan Forensik Android

Setelah melakukan tahapan forensik, analis menemukan beberapa barang bukti yang didapatkan dari platform Android yang digunakan pelaku, pada gambar diperlihatkan barang bukti yang didapat.



Gambar 4.38 Barang bukti yang didapat pada platform Android

4.2.6 Review Forensik Android

Berikut adalah review tool yang digunakan dalam melakukan forensik pada Android. Review tool dapat digunakan untuk bahan pembandingan penelitian selanjutnya.

Tabel 4.11 Tool yang digunakan dalam forensik pada Android

Tahapan	Tool yang dapat digunakan	Tool yang dipilih	Alasan
Backup Android	1. Nandroid backup 2. Clock work mod 3. Oxygen forensic 4. ADB Backup	Oxygen dan CWM	Lebih mudah digunakan dan lebih lengkap.
Ekstraksi backup	1. Unyaffs 2. Yaffey 3. Oxygen data extraction	Oxygen Forensic	Karena mudah dalam penggunaannya
Forensic imaging Android	1. DD melalui ADB 2. MOBILedit 3. Oxygen forensic	Oxygen Forensic	Karena saat proses backup berlangsung, hasil backup akan langsung menjadi satu file bertipe OFB.
Recovery Android	1. Recovery My Files 2. Data Rescue	Recovery My Files	Dapat melakukan recovery pada suatu file image dan dapat berjalan pada OS windows
Analisis backup	1. FTK 2. Autopsy 3. Oxygen Forensic	Oxygen Forensic	Lebih mudah digunakan dan lebih lengkap
Analisis file database	SQLite Data Browser	SQLite Data Browser	Mudah digunakan dan dapat melihat struktur database
Analisis internal Android	1. FTK 2. Autopsy 3. Oxygen	Oxygen Forensic	Lebih mudah untuk digunakan dan lebih lengkap

	Forensic		
Analisis eksternal Android	1. FTK 2. Autopsy 3. Oxygen	Oxygen Forensic	Karena lebih lengkap dan lebih mudah saat digunakan

4.3 Perbandingan Forensik Pada Kedua Platform

Berikut adalah perbandingan forensik Whatsapp pada kedua platform yang meliputi tahapan forensik, tool yang dipakai, dan struktur file barang bukti yang ditemukan. Perbandingan tersebut didapatkan peneliti dari hasil penelitian forensik pada platform iOS dan Android.

Tabel 4.12 Perbandingan tahapan forensik pada platform iOS dan Android

Tahapan forensik		iOS	Android
Pengumpulan data	Hasil Imaging	Hasil ekstrak data perangkat	Hasil ekstrak data perangkat
	Jenis Image	Logical	Physical pada image memori perangkat
	Tool Yang Digunakan	1. Oxygen Forensic 2. iTunes dan iPhone Backup extractor	Oxygen Forensic
pemeriksaan	Teknik Yang Digunakan	Teknik filtering	Teknik recovery files pada image memori perangkat
	Tool yang digunakan	1. Recovery my files 2. Oxygen forensic	Oxygen Forensic
Analisis	Tool Yang Digunakan	Oxygen Forensic dan SQLite Data Browser.	SQLite Data Browser dan Oxygen

BAB V

KESIMPULAN

5.1 Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan dapat disimpulkan beberapa hal mengenai mobile forensik untuk aplikasi whatsapp pada platform iOS dan Android.

1. Struktur file aplikasi whatsapp pada iOS dan Android tidak jauh berbeda saat dilakukan proses penelitian.
2. Tahapan collecting yang dilakukan pada iOS dan Android berbeda saat pengumpulan data pada Android menggunakan CWM dan iOS menggunakan iTunes.
3. Tahapan examination yang dilakukan menggunakan tool oxygen pada platform iOS dan Android tidak jauh berbeda karena dalam tool oxygen sudah sangat lengkap untuk melakukan proses pemeriksaan.
4. Hasil analisa pada iOS dan Android terdapat persamaan karena dalam folder itu berisikan file-file database yang bertipe sama untuk dianalisis lebih lanjut.
5. Mendapatkan hasil laporan yang kurang lengkap karena keterbatasan tool yang bisa digunakan oleh penulis untuk melakukan studi analisis ini.
6. Perangkat iOS yang belum di jailbreak masih bisa dilakukan proses forensik meskipun tidak semua data bisa didapatkan terutama barang bukti yang sudah dihapus.

5.2 Saran

Mengingat keterbatasan yang dimiliki oleh penulis, maka penulis menyarankan dan mengharapkan untuk mengembangkan penelitian dimasa yang akan datang sebagai berikut.

1. Melakukan metode yang berbeda pada proses forensik agar bisa membandingkan mana yang lebih mudah digunakan dan mana yang lebih cepat mendapatkan hasil yang akurat.
2. Pembuatan tool forensik yang secara langsung dapat melakukan ekstrak terhadap perangkat Android pada proses *backup* menggunakan CWM.

DAFTAR PUSTAKA