FAKULTAS ILMU KOMPUTER | UNIVERSITAS SRIWIJAYA

PROCEEDING

ARS 2016

ANNUAL RESEARCH SEMINAR COMPUTER SCIENCE AND ICT

FAKULTAS ILMU KOMPUTER | UNIVERSITAS SRIWIJAYA

Palembang, Desember 06-07, 2016

ISBN 979-587-626-0

UNIVERSITAS SRIWIJAYA

JAIST JAPAN ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY

iaes Institute of Advanced Engineering and Science

Prosiding Seminar Nasional

Annual Research Seminar (ARS) 2016
Dalam Rangka Dies Natalis Fakultas Ilmu Komputer
Universitas Sriwijaya

Selasa 06 Desember 2016 Aula MM Universitas Sriwijaya Palembang

ISBN : 979-587-626-0

Diterbitkan oleh :
Program Studi Magister Teknik Informatika
Fakultas Ilmu Komputer
Universitas Sriwijaya
2016

KOMITE ANNUAL RESEARCH SEMINAR (ARS) 2016

Pengarah

Siti Nurmaini, Universitas Sriwijaya
Saparudin, Universitas Sriwijaya
Darmawijoyo, Universitas Sriwijaya
Jaidan Jauhari, Universitas Sriwijaya
Afriyan Firdaus, Universitas Sriwijaya
Fathoni, Universitas Sriwijaya

Komite Nasional

Rinaldi Munir, Institut Teknologi Bandung
Eko Kuswardono Budiardjo, Universitas Indonesia
Anto Satriyo Nugroho, PTIK-BPPT
Waskitho Wibisono, Institut Teknologi Sepuluh November
Ahmad Nizar Hidayanto, Universitas Indonesia
Teguh Bharata Adji, Universitas Gadjah Mada
Made Sudarma, Universitas Udayana
Reza Pulungan, Universitas Gadjah Mada
Indra Budi, Universitas Indonesia
Noor Akhmad Setiawan, Universitas Gadjah Mada
Sritrusta Sukaridhoto, Politek Elektronika Negeri
Tohari Ahmad, Institut Teknologi Sepuluh November
Suherman, Universitas Sumatera Utara
Ahmad Hoirul Basori, Telkom University
Eko Didik Widianto, Universitas Diponegoro
Gembong Edhi Setyawan, Universitas Brawijaya
Arda Yunianta, Universitas Mulawarman
Hargyo Tri Nugroho,Universitas Multimedia Nusantara

Ketua Pelaksana

Deris Stiawan, Universitas Sriwijaya

Wakil Ketua

Erwin, Universitas Sriwijaya

Komite Pelaksana

Reza Fersandaya Malik, Universitas Sriwijaya
Samsuryadi, Universitas Sriwijaya
Ermatita, Universitas Sriwijaya
Sukemi, Universitas Sriwijaya
Iwan Pahendra, Universitas Sriwijaya
Hadipurnawan Satria, Universitas Sriwijaya
Yudha Pratomo, Universitas Sriwijaya
Yusuf Hartono, Universitas Sriwijaya
Rifkie Primartha, Universitas Sriwijaya
Fachrurozi, Universitas Sriwijaya

DAFTAR ISI

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

REFERENSI

[1] V. P. Singh and P. Pal, "Survey of Different Types of CAPTCHA," *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 2, pp. 2242–2245, 2014.

[2] A. A. Chandavale, A. M. Sapkal, and R. M. Jalnekar, "Algorithm to break visual CAPTCHA," *2009 2nd Int. Conf. Emerg. Trends Eng. Technol. ICETET 2009*, pp. 258–262, 2009.

[3] M. T. Banday and N. Shah, "A Study of CAPTCHAs for Securing Web Services," *IJSDIA Int. J. Secur. Digit. Inf. Age*, vol. 1, no. 2, pp. 66–74, 2011.

[4] J. Yan and a. S. El Ahmad, "Breaking Visual CAPTCHAs with Naive Pattern Recognition Algorithms," *Twenty-Third Annu. Comput. Secur. Appl. Conf. (ACSAC 2007)*, pp. 279–291, 2007.

[5] A. Hindle, M. W. Godfrey, and R. C. Holt, "Reverse Engineering CAPTCHAs," in *2008 15th Working Conference on Reverse Engineering*, 2008, pp. 59–68.

Prosiding
ANNUAL RESEARCH SEMINAR 2016
6 Desember 2016, Vol 2 No. 1

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

Implementasi Prosedur Forensik untuk Analisis Artefak Whatsapp pada Ponsel Android

Yesi Novaria Kunang
Fakultas Ilmu Komputer
Universitas Bina Darma
Palembang, Indonesia
yesinovariakunang@binadarma.ac.id

Anggie Khristian
Fakultas Ilmu Komputer
Universitas Bina Darma
Palembang, Indonesia
anggie.khristian@gmail.com

Abstrak—Dengan maraknya penggunaan smartphone terutama yang berbasis Android yang menguasai hampir mencapai 85% pasar smartphone juga mendorong peningkatan jumlah penggunaan aplikasi pertukaran pesan seperti WhatsApp, facebook Messenger dan lainnya. Pengguna aplikasi WhatsApp messenger di seluruh dunia sejak April 2016 telah mencapai lebih dari 1 milyar mengungguli aplikasi sejenis. Di sisi lain pada beberapa kasus kejahatan dan kasus perdata yang sedang marak, mulai menggunakan barang bukti berupa percakapan, gambar, rekaman video dan lainnya yang berasal dari aplikasi WhatsApp.
Untuk itu pada penelitian ini menghasilkan prosedur yang bisa dijadikan rujukan dalam melakukan investigasi forensic aplikasi WhatsApp untuk mendapatkan barang bukti berupa sesi percakapan, data media seperti audio, no kontak, foto dan lainnya. Penelitian ini menggunakan teknik dekripsi file database aplikasi WhatsApp untuk membaca file database backup yang terenkripsi yang menyimpan sesi percakapan yang sudah dihapus.

Keywords— Android Forensik, WhatsApp messenger, crypt8, Prosedur Forensik

I. PENDAHULUAN

Aplikasi *WhatsApp Messenger* merupakan aplikasi *client* pertukaran pesan yang lintas platform untuk ponsel cerdas. Aplikasi ini menggunakan paket data internet untuk mengirim pesan, dokumen, gambar, video, user lokasi dan pesan *audio* ke pengguna lain menggunakan standar nomor ponsel seluler [1]. Aplikasi *WhatsApp* juga memilik fitur *auto sync* ke *phone address book* sehingga memungkinkan pengiriman pesan tak terbatas pada alamat kontak ponsel menggunakan aplikasi *WhatsApp*. Selain itu juga *WhatsApp* juga telah memiliki fitur untuk menelpon menggunakan aplikasi *WhatsApp calling* [2].

Berdasarkan data dari *The Statistics Portal*, Aplikasi *WhatsApp* merupakan aplikasi paling populer dibandingkan aplikasi sejenis seperti *Facebook, Messenger, WeChat, Skype, Viber, Line* dan lain-lain. Pada April 2016 jumlah pengguna aplikasi *WhatsApp* sudah mencapai lebih dari satu miliar. *The Statistics Portal* juga memberikan informasi jumlah volume pesan multimedia dari *WhatsApp* di seluruh dunia pada Februari 2016 pengguna dari aplikasi *mobile messaging* mengirimkan lebih dari 1,6 miliar pesan foto per hari. Aplikasi *WhatsApp* digunakan secara luas dan universal dengan versi yang tersedia untuk *Android, BlackBerry, iPhone* dan sistem operasi *Symbian. WhatsApp* sebagai aplikasi juga tidak tergantung pada perangkat *smartphone*, dan juga tidak tergantung pada operator [7].

Di sisi lain platform *open source Android* memberikan pengembang kebebasan untuk berkontribusi pada pertumbuhan yang cepat dari pasar *Android.* Hal ini bisa dilihat berdasarkan data dari *The Statiscs Portal* pada Kuarter I di tahun 2016 Sistem Operasi *Android* menguasai 84.1% pasar *smartphone* mengungguli *IOS*, *Microsoft*, *RIM* dan lainnya. Dengan teknologi *samrtphone Android* tersebut memberikan peluang bagi pengembang aplikasi untuk meluaskan penggunaan aplikasi, tapi di sisi lain pengguna *Android* mungkin tidak menyadari implikasi keamanan dan privasi saat mereka menginstal aplikasi di ponsel mereka. Pengguna ponsel hanya berasumsi bahwa dengan perangkat *smartphone* yang terkunci dengan sandi bisa melindungi informasi pribadi mereka, tanpa disadari aplikasi dapat menyimpan informasi pribadi pada perangkat termasuk juga aplikasi pertukaran pesan seperti *WhatsApp*.

Forensik *smartphone Android* telah berkembang dari waktu ke waktu menawarkan peluang yang signifikan dan tantangan menarik. Beberapa kejahatan yang diantaranya memanfaatkan kecanggihan *smartphone* Android tersebut untuk melakukan kejahatan seperti penipuan, perjudian, pornografi, korupsi, jaringan narkoba hingga kasus pembunuhan. Para pelaku kejahatan biasanya memanfaatkan aplikasi *chatting* sebagai sarana untuk berinteraksi dengan sesama rekan penjahat maupun korban. Pada beberapa kasus kejahatan yang marak baru-baru ini seperti pada kasus pembunuhan Mirna oleh

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

Jessica [11] dan pada kasus perdata kisruh internal partai PKS pemecatan Fahri Hamzah [10], menggunakan percakapan *WhatsApp* sebagai barang bukti di pengadilan. Hal tersebut memperlihatkan dari perspektif penyelidikan forensik, aplikasi *WhatsApp* dapat menyimpan data pembuktian yang dapat digunakan di pengadilan sebagai barang bukti. Oleh karena itu, sangat penting untuk memiliki sebuah metodologi dan *framework* untuk bisa mengurai data aplikasi *WhatsApp* di perangkat *Android* baik yang masih aktif maupun yang sudah dihapus menggunakan pendekatan Forensik. Hal lain yang akan dipelajari pada penelitian ini adalah mekanisme untuk membuka enkripsi file *database* maupun *file backup* dari aplikasi *WhatsApp* pada *Smartphone Android*. Untuk itu pada penelitian ini bisa memberikan kontribusi kerangka kerja yang bisa diterapkan untuk melakukan forensik data *backup* enkripsi *WhatsApp* yang tersimpan yang bisa saja berisi data percakapan yang sudah dihapus. Dengan pendekatan forensik yang digunakan tidak saja memungkinkan mengembalikan percakapan dan data yang ada tetapi juga data dan percakapan yang sudah dihapus.

II. TEKNOLOGI FORENSIK *WHATSAPP REVIEW*

Analisis forensik khususnya untuk aplikasi pertukaran pesan seperti *WhatsApp* pada smartphone telah banyak dibahas di beberapa jurnal yang telah diterbitkan dalam literatur. Dibandingkan dengan penelitian-penelitian sebelumnya penelitian ini memiliki perbedaan (a) memberikan kontribusi kerangka kerja /prosedur yang lebih detail untuk menganalisis barang bukti dari aplikasi *WhatsApp* pada *smartphone* berbasis *Android*, (b) Menyajikan analisis menyeluruh untuk pengambilan semua artefak yang dihasilkan oleh *WhatsApp Messenger* (yaitu *database* kontak, *file log*, gambar *avatar*, dan file preferensi), dan (c) menjelaskan proses alur proses deskripsi *file database WhatsApp* menggunakan versi enkripsi terakhir *crypt8*, yang dienkripsi menggunakan algoritma *AES* dengan panjang kunci 256 yang pendekatannya berbeda dengan yang sebelumnya masih menggunakan 192-bit enkripsi untuk *msgstore.db.crypt5* dan *msgstore.db.crypt7* yang pada [3] dan [7] menggunakan aplikasi *WhatsApp Xtract* yang berbasis *Python*. Untuk enkripsi menggunakan *crypt7* ke atas aplikasi ini tidak bisa mendekrip file *database*.

2.4. *Protokol WhatsApp*

WhatsApp menggunakan *open standard Messaging Extensible and Presence Protocol (XMPP)* yang telah disesuaikan. Protokol *XMPP* ini juga digunakan oleh aplikasi *Google talk, facebook messenger* . *XMPP* ini mirip seperti *HTTP,* saat *client* membuka *socket XMPP server* dan membiarkannya terbuka maka selama itu *client* tersebut *login*. Setelah *WhatsApp* terinstal di ponsel, aplikasi akan menciptakan akun pengguna menggunakan nomor telepon sebagai nama pengguna (ID: telepon number@s.whatsapp.net). *WhatsApp* otomatis mensinkronisasikan semua nomor telepon dari buku telepon pengguna dengan *database* terpusat dari pengguna *WhatsApp* untuk menambahkan kontak ke daftar kontak *WhatsApp* pengguna [3].

2.5. *Teknologi Enkripsi Database WhatsApp*

Mulai versi *WhatsApp* 2.9 pertukaran pesan disimpan di *'msgstore.db'* berupa *database* SQLite. Tapi dalam versi awal tersebut peneliti keamanan menemukan sesi *chat WhatsApp* bersifat rentan, karena file *database* yang menyimpan percakapan *chatting* tidak dienkripsi dan dapat dengan mudah diakses melalui banyak cara untuk mendapatkan rincian seluruh percakapan *chat*ting termasuk gambar, video, kontak dan sebagainya. Saat itu, peneliti keamanan mulai meneliti *database WhatsApp* (*msgstore.db*) untuk mengambil sesi percakapan bahkan yang sudah dihapus dari opsi *chat*. *WhatsApp* segera memperbaruinya dengan mekanisme enkripsi untuk melindungi *database*-nya [1].

Aplikasi *WhatsApp* otomatis mem-*backup* percakapan setiap hari pada pukul 04.00 pagi dan menyimpannya dalam *folder WhatsApp* pada ponsel Android. *Folder* tersebut terletak di memori internal atau kartu *SD* eksternal.

Aplikasi *WhatsApp* menggunakan ekstensi *crypt* dalam pengenskripsian *file database*-nya. *Crypt* menggunakan algoritma *AES*. Sebuah *file msgstore.db.crypt* menyimpan *database* pesan masuk dan pesan keluar dalam format *database* yang terenkripsi. Aplikasi *WhatsApp* menggunakan format ekstensi *crypt5, crypt6, crypt7, crypt8* untuk enkripsi *database*-nya [8].

Sekarang ini aplikasi *WhatsApp* menggunakan *crypt8* dalam pengenkripsiannya, dan mungkin saja nanti kedepannya akan menggunakan *crypt9*. Aplikasi *WhatsApp* menyimpan semua *database* yang terenkripsi di *folder WhatsApp* pada direktori */sdcard/WhatsApp/Databases/* dan *folder WhatsApp* tersebut bisa saja berada pada memori internal maupun eksternal atau *SD Card*. Untuk mendekripsi *database* aplikasi *WhatsApp*, maka diperlukan *file key* yang terletak pada direktori */data/data/com.whatsapp/files/* dan untuk masuk ke direktori tersebut membutuhkan hak akses *root*.

2.6. *Protokol Transfer Android*

Untuk mentransfer data pada smartphone android terdiri dari dua protokol yaitu:

- *USB Mass Storage* (*UMS*), *USB mass storage* adalah protokol standar yang digunakan oleh *flash drive, hard drive* eksternal, kartu *SD*, dan perangkat penyimpanan *USB* lainnya. Semua *file* atau aplikasi yang berada pada

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

media penyimpanan Android akan tidak bisa diakses oleh sistem Android ketika perangkat tersebut terkoneksi dengan komputer. Perangkat Android menggunakan *FAT File System* sebagai format *disk* nya, sehingga bisa langsung dibaca oleh sistem operasi Windows maupun Linux. Android bisa menggunakan *ext3/4* untuk format partisinya, dan format tersebut tidak bisa dibaca di sistem operasi Windows. Kelemahan dari protokol *UMS* ini adalah perangkat Android tidak bisa menggunakan atau membaca memori internal maupun eksternal selama perangkat tersebut terhubung ke komputer dan jika *smartphone* tersebut dilepaskan tanpa melakukan proses *ejecting* maka bisa terkena resiko terjadinya korup pada memori internal atau eksternal *smartphone* [9].

- *Media Transfer Protocol* (*MTP*), *MTP* adalah protokol yang umum digunakan untuk mentransfer file antara komputer dengan perangkat portabel. *MTP* sudah diperkenalkan sejak Android versi 3.0 (*Honeycomb*) dan dijadikan sebagai standar transfer protokol pada versi *Android* 4.0 (*Ice Cream Sandwich*). *MTP* tidak seperti standar USB, ini berarti hanya satu operasi / tugas yang dapat dilakukan pada satu waktu (seperti *read* dan *write*). Protokol ini sangat berbeda dengan *USB Mass Storage* yang mengekspos semua *disk* partisi Android ke komputer, sedangkan *MTP* beroperasi pada tingkat *file* saja. Jika menggunakan protokol *MTP*, fomat partisi *ext3/4* pada perangkat *Android* bisa dibaca pada Windows. Dengan kata lain, *MTP* membuat pengaksesan *storage Android* menjadi *cross-platform*. Kelebihan protokol *MTP* ini adalah perangkat *Android* tetap bisa digunakan dan *file* di memori internal maupun eksternal tetap bisa dibaca walaupun perangkat tersebut sedang terhubung dengan komputer dan memori *smartphone* tetap aman walaupun tanpa melakukan proses *ejecting* saat dilepas dari komputer, sehingga mengurangi resiko terjadinya korup pada memori internal atau eksternal [9].

III. IMPLEMENTASI PROSEDUR *WHATSAPP* FORENSIK DI ANDROID

Dalam penelitian ini menerapkan *Mobile* forensik yang dibuat oleh *National Institute of Standard and Technology* (NIST) [4] yang mempunyai beberapa tahap: *preservation, acquisition, examination & analysis,* dan *reporting* yang bisa dilihat pada gambar 1.

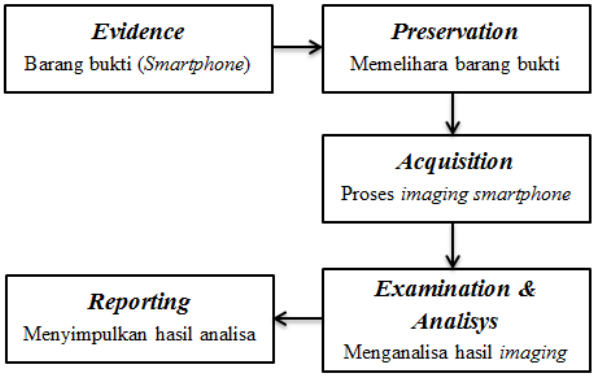


Fig. 7. *Tahapan Mobile Forensik yang Diterapkan*

2.7. *Preservation*

Pada tahapan *preservation* merupakan tahap awal dalam metode *mobile* forensik, hal yang dilakukan adalah melakukan pencarian, pengumpulan dan pendokumentasian barang bukti. Untuk pengujian pada penelitian yang menjadi sampel barang bukti yang dianalisis berupa dua buah *smartphone* yang diskenariokan sebagai barang bukti dalam kasus kejahatan. Kedua *smartphone* tersebut dalam kondisi tidak di *root* dengan kondisi fitur keamanan password aktif dan pengamanan layar aktif. Pada tahapan ini dilakukan pendokumentasian hal yang berkaitan dengan *smartphone* tersebut. Berikut merupakan hasil dokumentasi serta spesifikasi barang bukti:

TABLE V. TABEL SPESIFIKASI BARANG BUKTI (*EVIDENCE*)

	Merk	**Seri**	**Model**	**Versi OS**
Smartphone 1	Samsung	Galaxy	Ace 3	4.2.2 (*Jelly Bean*)
Smartphone 2	Smartfren	Andromax	AD683G	4.0 (*Ice Cream Sandwich*)

Selain melakukan pengumpulan dan pendokumentasian, pada tahap ini juga dilakukan persiapan dan perencanaan bagaimana cara *smartphone* tersebut nantinya akan dianalisis serta *tools* dan alat apa saja yang dibutuhkan untuk menunjang dalam melakukan proses tersebut.

Pada gambar 2 merupakan alur kerangka kerja yang dirancang untuk menganalisis *smartphone* untuk mendapatkan artefak *digital* yang berkaitan dengan aplikasi *WhatsApp* dalam kondisi kedua smartphone yang tidak di *root* dengan fitur pengamanan layar yang aktif. Alur kerja yang dirancang ini diusahakan memenuhi aturan forensik, dengan mengambil langkah-langkah yang seminimal mungkin dapat merubah barang bukti. Untuk pengujian digunakan *Smartphone* Android yang dalam kondisi tidak di *root*. Karena Seperti kebanyakan sistem operasi , pada *smartphone* Android yang tidak di *root* beberapa fiturnya telah dinonaktifkan untuk

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

mencegah pengguna bisa merusak sistem operasi . Kondisi "*rooting* sendiri menghilangkan keterbatasan tersebut sehingga akses penuh ke sistem diperbolehkan. Untuk kondisi ponsel Android yang sudah di-*rooting*, pengguna akan memiliki kontrol lebih besar untuk pengaturan, fitur dan performa ponsel sehingga proses mengakses file sistem untuk analisis forensik akan menjadi lebih mudah. Akan tetapi untuk prosedur forensik pada ponsel Android yang belum di *root*, sangat dihindari melakukan *rooting* permanen karena sangat beresiko merubah barang bukti dan bisa mengakibatkan data tertimpa [1].

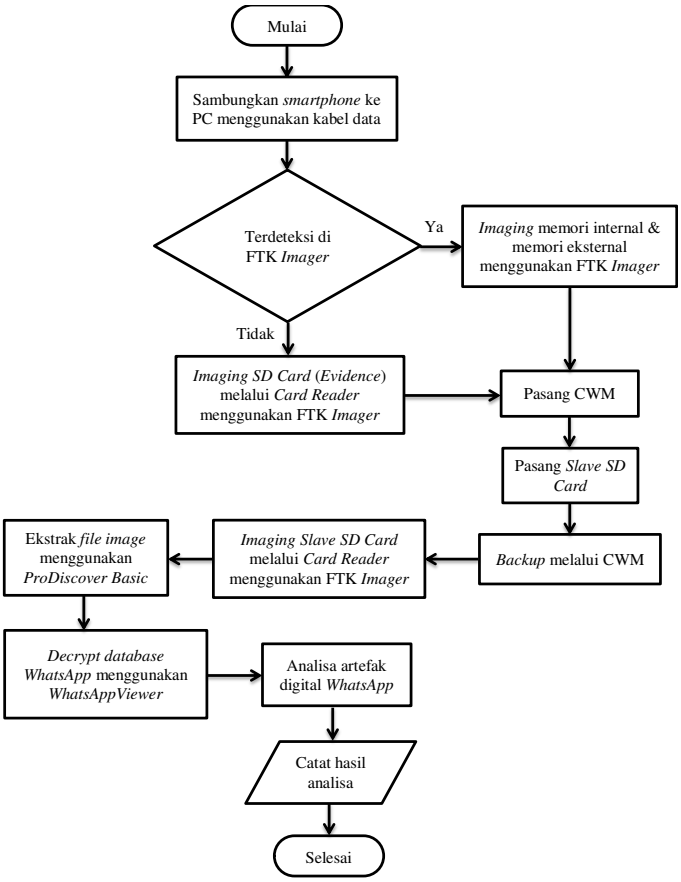


Fig. 8. Alur Kerja Prosedur Analisis Aplikasi *WhatsApp* pada Platform Android yang tidak di root

2.8. *Acquisition*

Pada tahapan *acquisition* dilakukan *imaging* baik memori internal maupun eksternal dari kedua ponsel dengan mengikuti prosedur atau alur kerja yang sudah dirancang pada gambar 2. Dalam melakukan proses pengambilan data-datanya, setiap perangkat *Android* bisa berbeda-beda caranya, dipengaruhi oleh jenis vendor dan hal yang lainnya seperti jenis protokol transfer, kondisi keamanan layar *smartphone* sedang aktif atau tidak, dan versi *Android*. Jenis perangkat mobile dan data yang akan diekstrak umumnya menentukan *tools* dan teknik yang harus digunakan dalam penyelidikan [4].

Ada beberapa cara dalam melakukan pengambilan data pada *smartphone* Android, seperti menggunakan *tools ADB* (*Android Debug Bridge*), *FTK Imager*, *ViaExtract*, *Magnet Forensic*, *AFLogical* dan lain sebagainya. Semua *tools* diatas mempunyai kelebihan dan kekurangan masing-masing, hal tersebut dipengaruhi oleh kondisi *smartphone*, seperti hak akses *root smartphone*, *USB Debugging*, keamanan layar, jenis vendor, versi Android dan protokol transfer yang didukung.

1) Pendeteksian Awal Smartphone dengan FTK Imager

Pada tabel 2 bisa dilihat hasil pendeteksian awal dengan FTK Imager, pada kedua *smartphone* fitur keamanan layarnya aktif, sehingga tidak bisa mengaktifkan *USB Debugging* dan hal ini menyebabkan *smartphone* tersebut tidak dapat terdeteksi pada *ADB*. Untuk itu proses imaging *SD card* (memori eksternal) kedua ponsel dilakukan dengan menggunakan *card reader*.

2) Backup Memori Internal Smartphone dengan Tool CWM

Untuk melakukan imaging memori internal pada kedua smartphone tersebut peneliti menggunakan *tool CWM* yang akan mengupdate *bootloader* Android sebagai pengganti *tool* komersial. Dengan *CWM* bisa mengambil data-data pada partisi sistem Android maupun memori internal tanpa harus melakukan *rooting*, mengaktifkan *USB Debugging*, dan juga tidak terpengaruh oleh keadaan keamanan layar *smartphone* sedang aktif atau tidak. Untuk memasang *CWM*, diperlukan cara yang berbeda pada setiap *smartphone*, tergantung vendornya, dan juga diperlukan sebuah *SD Card* untuk menampung hasil *backup*.

TABLE VI. PROSES AWAL PENDETEKSIAN *SMARTPHONE* DENGAN *FTK IMAGER* MENGGUNAKAN *USB*

	Proteksi password	**Keaman an layar**	**Protokol Transfer**	**Memori eksternal**	**Memori Internal**
Smartphone 1	aktif	Aktif	MTP	Tidak terdeteksi	Tidak terdeteksi

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

Smartphone 2	aktif	aktif	MTP	Tidak terdeteksi	Tidak terdeteksi

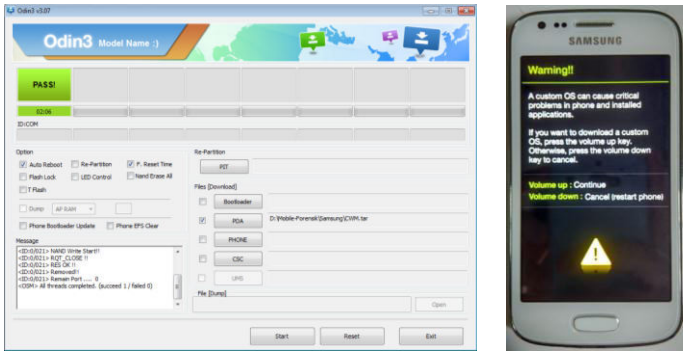


Fig. 9. Proses Instalasi CWM pada Smartphone 1 dengan tools Odin

Pada *smartphone 1* (*Android Samsung Galaxy Ace 3*) *tools CWM* diinstal dengan menggunakan *tools Odin* yang diinstal di komputer kemudian dihubungkan dengan *USB* ke ponsel. Sedangkan *Evidence* kedua yaitu perangkat android *Smartfren Andromax AD683G* kegiatan *flashing* dilakukan dengan *tools fastboot* yang berbasis *CMD*.

Untuk mengambil data-data pada memori internal dan partisi sistem *Android* akan menggunakan *CWM*. Sebelumnya masukkan *Slave SD Card* terlebih dahulu untuk menampung hasil *backup*. Untuk masuk ke mode *CWM Recovery* dilakukan saat *smartphone* dalam keadaan mati, lalu tekan tombol *power + home + volume up* secara bersamaan.

Fig. 10. Proses Instalasi CWM pada Smartphone 2 dengan tools fastboot

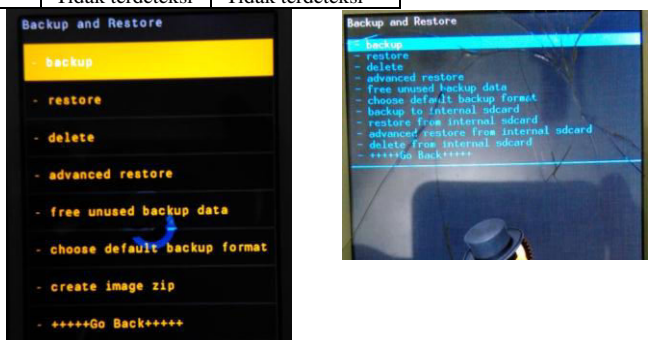


Fig. 11. Proses Backup pada Smartphone 1 & 2

3) Imaging Slave SD Card

Setelah proses *backup* melalui *CWM* telah dilakukan, maka selanjutnya adalah melakukan *imaging* terhadap *Slave SD Card* yang dimana pada *SD Card* tersebut terdapat hasil *backup* dari *evidence* 1 dan *evidence* 2. Untuk melakukan *imaging* pada *SD Card*, maka dibutuhkan sebuah *Card Reader* sebagai media untuk mengkoneksikan ke komputer. Proses *imaging* pada *Slave SD Card* menggunakan aplikasi *FTK Imager*.

2.9. *Examination and Analysis*

Tahap *examination and analysis* ini bertujuan untuk mengungkap dan melakukan analisis terhadap hasil dari tahap *acquisition* untuk memperoleh data yang berkaitan dengan aplikasi *WhatsApp*. Pada penelitian ini menggunakan beberapa *tools* yang digunakan untuk menganalisis hasil *imaging* yang telah dilakukan sebelumnya yaitu: *ProDiscover Basic, AccessData FTK Imager, WhatsApp Viewer,*dan *DB Browser for SQLite*.

1) Ekstraksi Data WhatsApp dari Data Image

Adapun langkah-langkah untuk mengekstrak data dari image adalah sebagai berikut:

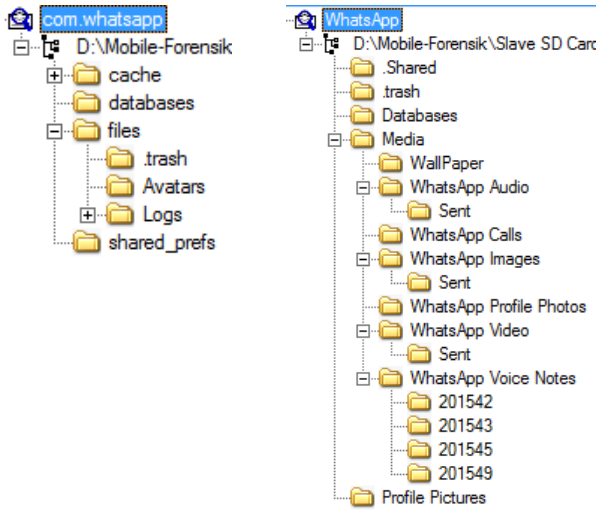
- Untuk mengambil data dari *backup image* memori eksternal dan internal untuk kedua *smartphone* digunakan *tools ProDiscover*. Data disimpan dalam folder yang berlabel sesuai tanggal backup. Data yang dicari adalah file *data.ext4.tar* yang kemudian diekstrak.
- Hasil ekstrak dianalisis dengan menggunakan *FTK Imager* untuk mengekspor folder WhatsApp dan folder com.whatsapp. Jika tidak bisa terbuka maka file tersebut berarti dalam kondisi dikompress sehingga sebelumnya diekstrak terlebih dahulu dengan 7zip.

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

TABLE VII. FOLDER HASIL EKSTRAKSI DAN EKSPOR DATA APLIKASI *WHATSAPP*

	Tempat Penyimpanan	Folder data yang diekspor
Smartphone 1	Memori Internal	Folder *WhatsApp*, com.whatsapp
Smartphone 2	Memori eksternal Memori Internal	Folder WhatsApp Folder com.whatsapp

Pada tabel 3 terlihat perbedaan tempat penyimpanan data pada kedua ponsel barang bukti.



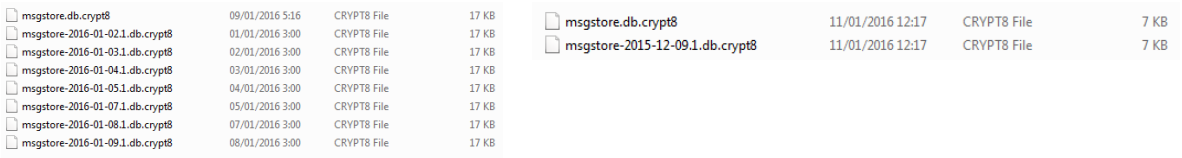


Fig. 13. Data di folder WhatsApp pada Smartphone 1 & 2 yang terenkripsi menggunakan crypt 8

Untuk mendekripsi *database* yang terenkripsi tersebut bisa menggunakan aplikasi *WhatsApp Viewer*, kemudian pilih menu *Decrypt .crypt8* pada aplikasi *WhatsApp Viewer*. Untuk mendekripsinya dibutuhkan sebuah *file key* yang terletak pada *folder com.whatsapp/files/*. Setelah didekripsi, maka akan muncul sebuah *file database* baru yang bernama *msgstore.decrypted.db* pada *folder* yang sama dengan *file database* yang terenkripsi.

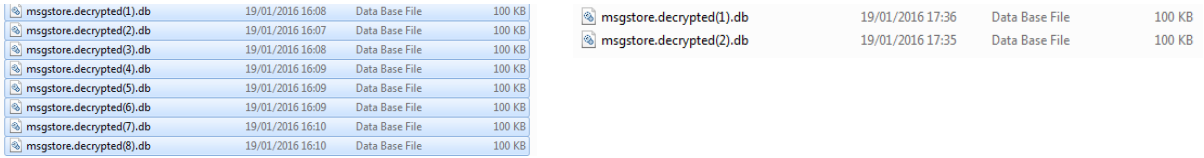


Fig. 14. File Database yang sudah didekripsi pada Smartphone 1 & 2

Fig. 12. Struktur Folder com.whatsapp dan folder WhatsApp

2) Decrypt Database WhatsApp

Setelah semua data-data yang berkaitan dengan aplikasi *WhatsApp* telah didapat, maka selanjutnya adalah mendekripsi *database* aplikasi *WhatsApp* yang terenkripsi *crypt8*. Pada gambar 6 terlihat file di folder WhatsApp dienkripsi menggunakan crypt8.

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

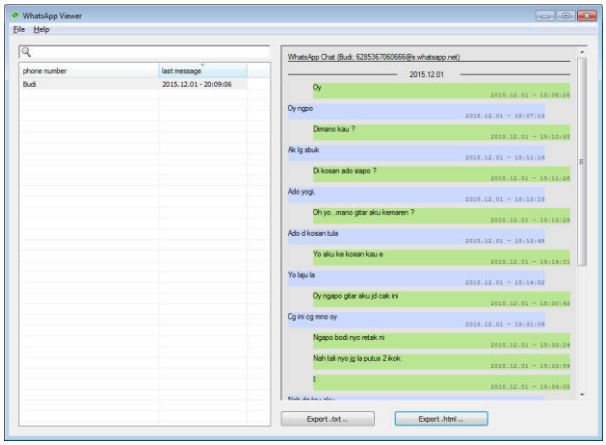


Fig. 15. Contoh WhatsApp Chat yang didapatkan

Pada aplikasi *WhatsApp Viewer* juga terdapat menu untuk meng-*convert* isi percakapan pada *database* yang sudah terdekripsi ke *format html*. Untuk *convert* ke *html*, pilih *chat* yang ingin di-*convert*, klik *Export .html*, pilih destinasi *folder* tempat menyimpan hasil *convert*, dan klik *Save*.

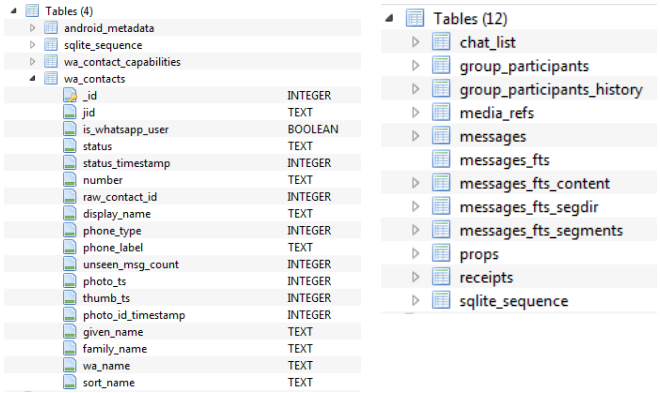


Fig. 16. Struktur tabel database wa.db dan msgstore.dcrypted.db

2.10. *Reporting*

Tahap *examination and analysis* ini bertujuan untuk mengungkap dan melakukan analisis terhadap hasil dari tahap *acquisition* untuk memperoleh data yang berkaitan dengan aplikasi *WhatsApp*. Pada penelitian ini menggunakan beberapa *tools* yang digunakan untuk menganalisis hasil *imaging* yang telah dilakukan sebelumnya yaitu: *ProDiscover Basic, AccessData FTK Imager, WhatsApp Viewer,*dan *DB Browser for SQLite*.

Pada tahapan ini akan membahas dan menyajikan secara detil semua artefak yang berkaitan dengan aplikasi *WhatsApp* yang telah didapatkan sebelumnya untuk mengungkap sebuah kasus kejahatan yang telah diskenariokan. Setelah melakukan analisa pada *evidence* 1 dan 2, dapat disimpulkan bahwa dengan menerapkan proses *mobile* forensik pada *platform* Android, artefak *digital* yang berkaitan dengan aplikasi *WhatsApp* bisa didapatkan. Selain percakapan dan foto *profile*, *file* media yang telah dikirim atau diterima bisa didapatkan seperti *file audio, video, voice note, images,* dan *call history* juga bisa didapatkan, tetapi disini peneliti hanya membuat percakapan dan *voice note* saja. Pada tabel dibawah merupakan informasi penting mengenai identitas pengguna aplikasi *WhatsApp*:

TABLE VIII. FOLDER HASIL EKSTRAKSI DAN EKSPOR DATA APLIKASI *WHATSAPP*

Informasi	**Evidence 1**	**Evidence2**
Nomor *Handphone* Pengguna	6285222743xxx	6285769730xxx
Versi Aplikasi	2.12.304	2.12.304
Nama Pengguna	Anggie Christian	Christian
Kontak	205	3
Percakapan	2	1
Encrypted Databases	8	2
Avatar	16	2
Profile Pictures	3	1
WhatsApp audio	-	-
WhatsApp calls	-	-
WhatsApp images	-	-
WhatsApp profile photo	-	-
WhatsApp video	-	-
WhatsApp voice notes	1	-

Pada direktori *com.whatsapp/databases/* terdapat beberapa *database* yang tidak terenkripsi dan pada direktori *com.whatsapp/avatar/files/* terdapat *thumbnails* foto profil pengguna dan kontak-kontak pada aplikasi *WhatsApp*. Untuk melihat *avatar* maupun file media lain seperti foto, video, dan lainnya bisa menggunakan aplikasi *FTK Imager*.

Untuk melihat kontak ponsel bisa dilihat disimpan pada *file wa.db* yang bisa dibuka dengan *DB browser for SQLite*, ditemukan semua kontak yang tersimpan pada *evidence*. Tidak hanya kontak yang terdaftar sebagai pengguna aplikasi *WhatsApp* saja yang bisa didapatkan, tetapi juga kontak pada *smartphone* yang tidak terdaftar sebagai pengguna aplikasi *WhatsApp*. Selain itu juga terdapat informasi mengenai identitas pengguna aplikasi *WhatsApp* yang terdapat pada direktori *com.whatsapp/shared_prefs* yang disimpan dalam format XML.

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

Aplikasi *WhatsApp* otomatis mem-*backup* percakapan setiap hari pada pukul 04.00 pagi ke dalam sebuah *SQLite3 database* dan menyimpannya dalam *folder WhatsApp* pada memori internal atau *SD Card*. *File database* tersebut dienkripsi dengan tipe enkripsi *crypt8*. Jadi saat ada perubahan, baik penambahan atau penghapusan percakapan pada aplikasi *WhatsApp*, maka percakapan-percakapan tersebut akan di-*backup* secara otomatis pada pukul 03.00 pagi. Data aplikasi *WhatsApp* terdapat pada dua *folder*, yang pertama adalah *folder com.whatsapp*, *folder* tersebut terdapat pada direktori */data/data/com.whatsapp* di partisi sistem Android, yang kedua yaitu *folder WhatsApp*, letak *folder* tersebut bisa berada pada memori internal maupun *SD Card*.

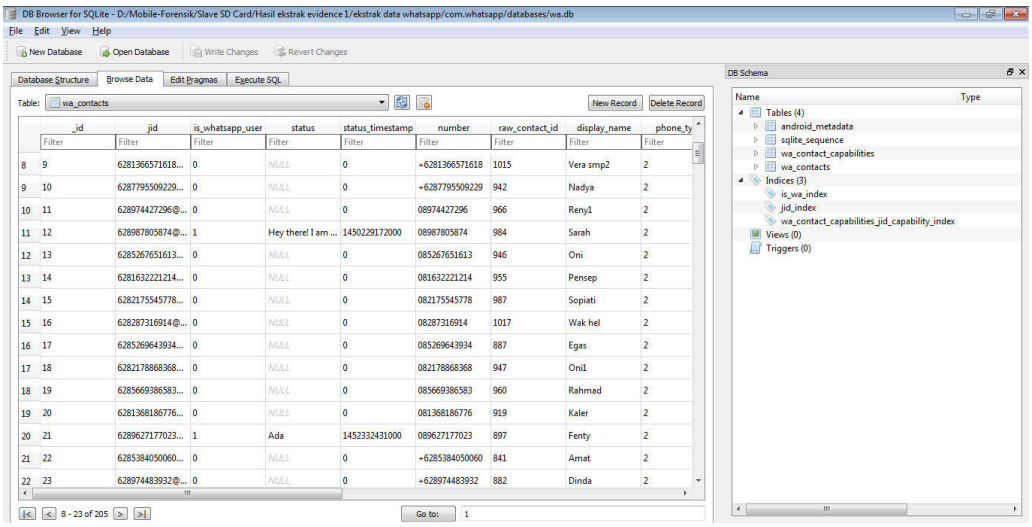


Fig. 17. Isi file wa.db pada evidence 1

Folder WhatsApp terletak pada memori internal atau bisa juga di *SD Card*, untuk mengaksesnya tidak butuh hak akses *root*, pengguna awam pun bisa membuka *folder* tersebut. Di dalam *folder WhatsApp* terdapat *file* media yang telah dikirim atau diterima pada aplikasi *WhatsApp*, serta terdapat juga *database* percakapan yang terenkripsi dan *database* tersebut tidak dapat dibuka tanpa disertai *file key* yang berada pada *folder com.whatsapp*. *Folder com.whatsapp* terdapat di direktori */data/data/com.whatsapp* pada partisi sistem Android, dimana untuk mengakses *folder* tersebut dibutuhkan hak akses *root*. Di dalam *folder com.whatsapp* terdapat *file key* dan *wa.db* yang penting untuk melakukan dekripsi. Metode enkripsi pada aplikasi *WhatsApp* menggunakan 256-bit AES, sehingga untuk melakukan dekripsi tanpa *file key* sangat sulit dilakukan.

Teknik dalam mendekripsi *database* aplikasi *WhatsApp* bisa berbeda-beda caranya, tergantung jenis enkripsi yang digunakan. Pada tipe enkripsi *crypt7* dan *crypt8* harus menggunakan *file key* untuk mendekripsi *file database*-nya, sedangkan pada jenis enkripsi *crypt5*, *database* tersebut bisa didekripsi tanpa memerlukan *file key*, tetapi hanya membutuhkan sebuah alamat *email (gmail)* yang digunakan pada *smartphone* tersebut untuk mendapatkan kode *hash* md5-nya. *Database* yang terenkripsi *crypt7* dan *crypt8* tidak bisa didekripsi menggunakan *file key* yang ada pada *smartphone* berbeda, jadi setiap *smartphone* yang ter-*install* aplikasi *WhatsApp* akan membuat sebuah *file key* yang unik yang hanya bisa digunakan oleh *smartphone* itu sendiri.

Sebagian besar *smartphone* Android tidak bisa dilakukan *imaging* terhadap partisi sistem dan memori internal, hal ini lah yang menjadi salah satu kendala dalam melakukan *mobile* forensik pada *platform* Android. Ada hal lain yang membuat proses *mobile* forensik semakin sulit dilakukan yaitu jika *SD Card smartphone* tersebut telah dienkripsi, sehingga prosesnya akan menjadi semakin rumit, selain itu jika memori internal atau eksternal sudah di-*format* berulang-ulang kali, maka hanya berkemungkinan kecil untuk mendapatkan data-data yang diinginkan kembali, karena keterbatasan ruang memori tersebut yang mengakibatkan tertimpanya data yang lama dengan yang baru.

IV. SIMPULAN DAN SARAN

Dengan menggunakan tahapan-tahapan prosedur forensik aplikasi *WhatsApp* pada platform yang digunakan pada penelitian ini menghasilkan beberapa kesimpulan dan saran

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

yang bisa dijadikan sebagai acuan prosedur standar untuk melakukan penyidikan forensik pada penggunaan *WhatsApp Messenger* di *smartphone Android* pada situasi real maupun sebagai referensi penelitian terkait.

2.11. *Simpulan*

1. Pendekatan prosedur yang digunakan untuk mendapatkan data-data artefak *WhatsApp* pada *smartphone* Android bisa berbeda-beda caranya tergantung pada beberapa hal seperti jenis *vendor*, fitur keamanan layar *smartphone*, protokol transfer yang digunakan, dan versi *Android*.
2. Dengan tahapan prosedur analisis forensic yang dilakukan pada penelitian ini berhasil mendapatkan artefak bukti berupa sesi *chat*, avatar, no kontak pada aplikasi *WhatsApp*, *voice notes*, foto profil, identitas pemilik akun *WhatsApp* dan juga bisa mendapatkan file media lainnya dan yang terpenting file *database backup* yang terenkripsi.
3. Pendekatan ekstraksi *database WhatsApp* yang diterapkan berhasil mengekstrak percakapan *chatting* yang disimpan di memori internal maupun external menggunakan *key WhatsApp extractor* dan *decryptor* untuk mengkonversi *database* backup ke dalam *database* teks yang dapat dilihat di *browser basis data SQLite*. Tahapan ini bisa membuka sesi *chat* yang sudah terhapus berdasarkan *backup data* yang tersimpan baik secara otomatis oleh aplikasi *WhatsApp* maupun *backup* manual.

2.12. *Saran*

1. Tantangan utama bagi setiap penyidik forensik adalah standar enkripsi *WhatsApp* yang selalu berkembang untuk melindungi *backup* dari akses yang tidak sah. Oleh karena itu, sangat penting bagi penyidik forensik untuk selalu meng*update* perkembangan teknologi yang berkaitan *database backup WhatsApp* agar dapat mengekstrak sesi chatting yang mungkin ada pada perangkat tersangka.
2. Tantangan lain adalah bahwa *WhatsApp* telah menambahkan fasilitas enkripsi *end-to-end* untuk semua pesan. Perlu dilakukan penelitian untuk melakukan forensik pada sesi percakapan yang memanfaatkan *enkripsi end to end.*
3. Fitur enkripsi yang dianalisis pada penelitian ini menggunakan crypt8 dengan teknologi *WhatsApp* yang terus *update* maka untuk ke depan perlu melakukan penelitian dan pengujian prosedur forensik untuk fitur enkripsi terbaru seperti *crypt9* dan *crypt10*.
4. Mengingat aplikasi *WhatsApp* merupakan aplikasi yang *cross platform*, penting juga untuk melakukan analisis forensik *WhatsApp* artefak pada *platform* yang lain.

REFERENSI

[1] Shuaibu, M. Z. & Bala A., 2016. WhatsApp Forensics and Its Challenges for Android Smartphone. *A Global Journal of Advance Engineering Technology and Sciences*, (5) May 2016, pp. 68-75.

[2] Lone, A.H., Badroo, F.A., Chudhary, K.R. & Khalique, A., 2015. Implementation of Forensic Analysis Procedures for WhatsApp and Viber Android Applications. *International Journal of Computer Applications (0975 – 8887)*, Volume 128 – No.12, pp. 26-32.

[3] Sahu, S., 2014. An Analysis of WhatsApp Forensics in Android Smartphones. *International Journal of Engineering Research,* ISSN:2319-6890, Volume No.3, Issue No.5, pp. 349-350.

[4] Ayers, R., Brothers. S., Jansen, W., 2014. Guidelines on Mobile Device Forensics, NIST Special Publication 800-101 Revision 1.

[5] The Statistics Portal, 2016. *Global mobile OS market share in sales to end users from 1st quarter 2009 to 1st quarter 2016*. [Online]. Available at: http://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/. [Accessed 15 Juli 2016].

[6] The Statistics Portal, 2016. *Most popular mobile messenger apps worldwide as of April 2016, based on number of monthly active users (in millions).* [Online]. Available at: http://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/. [Accessed 15 Juli 2016].

[7] Thakur, N. S., 2013. *Forensic Analysis of WhatsApp on Android Smartphones*. Master. University of New Orleans.

[8] File-Extensions.org. *Crypt File Extention*. [Online]. Available at: http://www.file-extensions.org/crypt-file-extension. [Accessed 5 Juli 2016].

[9] Hoffman, C., 2014. Android USB Connections Explained: MTP, PTP, and USB Mass Storage. [Online]. Available at : http://www.howtogeek.com/192732/android-usb-connections-explained-mtp-ptp-and-usb-mass-storage/. [Accessed 5 Juli 2016].

[10] Masharu, W., 2016. Sidang Lanjutan, Fahri Hamzah Serahkan Bukti Percakapan via Whatsapp. *Suara Pembaruan*, 25 Juli. [Online]. Available at: http://www.beritasatu.com/nasional/376383-sidang-lanjutan-fahri-hamzah-serahkan-bukti-percakapan-via-whatsapp.html. [Accessed 25 Juli 2016].

[11] Pratiwi, P.S., 2016. Suami Mirna Tunjukkan Bukti Percakapan Jessica pada Hakim. *CNN Indonesia*, 12 Juli. [Online]. Available at: http://www.cnnindonesia.com/nasional/20160712174700-12-144375/suami-mirna-tunjukkan-bukti-percakapan-jessica-pada-hakim/. [Accessed 25 Juli 2016].

2016 ARS
Annual Research Seminar
Computer Science & ICT
Fakultas Ilmu Komputer
Universitas Sriwijaya

SERTIFIKAT

Selasa | 06 Desember 2016

Diberikan Kepada :

YESI NOVARIA KUNANG

Sebagai

PEMAKALAH

SEMINAR NASIONAL
ANNUAL RESEARCH SEMINAR (ARS) 2016

yang diselenggarakan oleh Program Studi Magister Teknik Informatika Universitas Sriwijaya
dalam rangkaian Dies Natalis ke - 10 Fakultas Ilmu Komputer Universitas Sriwijaya

Ketua Program Studi Magister Informatika

Drs. Saparudin.MT., Ph.D

Ketua Pelaksana

ARS2016 Computer Science & ICT Annual Research Seminar

Deris Stiawan, Ph.D

UNIVERSITAS SRIWIJAYA

JAIST Japan Advanced Institute of Science and Technology

iaes Institute of Advanced Engineering and Science