



**ANALISA PERBANDINGAN TOOLS EKSTAKTOR
WHATSAPP DATABASE *CRYPT12* MENGGUNAKAN
METODA *LOGICAL EXTRACTION***

TESIS

**Diajukan Sebagai Salah Satu Syarat Untuk Menyelesaikan
Program Pascasarjana Program Magister Teknik Elektro**

**UNIVERSITAS
MERCU BUANA**

**Oleh :
Zulkarnaen Akbar**

55414120030

**PROGRAM MAGISTER TEKNIK ELEKTRO
PROGRAM PASCASARJANA
UNIVERSITAS MERCU BUANA
2017**



**ANALISA PERBANDINGAN TOOLS EKSTAKTOR
WHATSAPP DATABASE *CRYPT12* MENGGUNAKAN
METODA *LOGICAL EXTRACTION***

TESIS

**Diajukan Sebagai Salah Satu Syarat Untuk Menyelesaikan
Program Pascasarjana Program Magister Teknik Elektro**

**UNIVERSITAS
MERCU BUANA**

**Oleh :
Zulkarnaen Akbar**

55414120030

**UNIVERSITAS MERCU BUANA
PROGRAM PASCASARJANA**

PENGESAHAN TESIS

Judul : Analisa Perbandingan Tools Ekstraktor WhatsApp Database
Crypt12 Menggunakan Metoda Logical Extraction

Nama : Zulkarnaen Akbar

NIM : 55414120030

Program : Pascasarjana Program Magister Teknik Elektro

Konsentrasi : Keamanan Jaringan ICT

Tanggal : 22 Mei 2017

Pembimbing



(Dr. Ir. Iwan Krisnadi, MBA)

UNIVERSITAS

Mengesahkan :

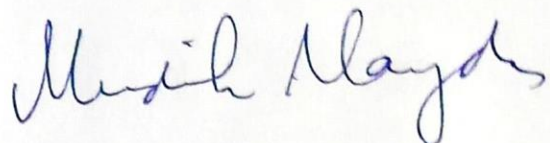
Direktur Pascasarjana

Ketua Program Studi

Magister Teknik Elektro



(Prof. Dr. Didik J. Rachbini)



(Prof. Dr. -Ing. Mudrik Alaydrus)

PERNYATAAN

Saya yang bertandatangan di bawah ini menyatakan dengan sebenar-benarnya bahwa seluruh tulisan dan pernyataan dalam Tesis ini:

Judul : Analisa Perbandingan Tools Ekstraktor WhatsApp Database
Crypt12 Menggunakan Metoda *Logical Extraction*
Nama : Zulkarnaen Akbar
N I M : 55414120030
Program : Pascasarjana Program Magister Teknik Elektro
Kosentrasi : Keamanan Jaringan ICT

Merupakan hasil studi pustaka, penelitian lapangan, dan karya saya sendiri dengan bimbingan Pembimbing yang ditetapkan dengan Surat Keputusan Ketua Program Studi Magister Teknik Elektro Universitas Mercu Buana.

Tesis ini belum pernah diajukan untuk memperoleh gelar magister pada program sejenis di perguruan tinggi lain. Semua informasi, data, dan hasil pengolahannya yang digunakan, telah dinyatakan secara jelas sumbernya dan dapat diperiksa kebenarannya.

Jakarta, 22 Mei 2017



Zulkarnaen Akbar

KATA PENGANTAR

Bismillahi Rahmaanir Rahiim

Alhamdulillah, segala puja dan puji kami haturkan kehadirat *Ilahi Rabbi*, yang telah menganugerahkan segala nikmat-Nya terutama nikmat sehat dan keimanan. *Shalawat* dan *Salam* kami haturkan kepada junjungan alam semesta Muhammad SAW beserta keluarga, sahabat, *tabi'in*, *tabiu't at tabi'in* dan sampai kepada kita pengikutnya hingga akhir zaman, Aamiin. Tugas Akhir ini yang yang berjudul **“Analisa Perbandingan Tools Ekstraktor WhatsApp Database Crypt12 Menggunakan Metoda Logical Extraction”** ini disusun sebagai salah satu syarat untuk memperoleh gelar Starta Dua (S2) atau Magister pada Program Studi Magister Teknik Elektro Universitas Mercubuana Jakarta.

Pada kesempatan ini penulis mengucapkan terimakasih yang sebesar besarnya kepada yang terhormat.

1. Prof. Dr –ing. Mudrik Alaydrus selaku ketua Program Studi Magister Teknik Elektro Universitas Mercubuana
2. Dr. Ir. Iwan Krisnadi, MBA selaku dosen pembimbing yang dengan sabar membimbing dan mengarahkan penulis hingga selesai Tugas Akhir ini.
3. Ibu (Istiqomah) dan (Bapak Marzuki) yang tercinta atas pengorbanan kasih sayang, dukungan yang baik dan do'anya kepada penulis dalam menyelesaikan Tugas Akhir ini.
4. Kedua Adik yang tersayang (Zulfatun Nisa dan Zulfikri Hidayatullah) yang telah memberikan do'a, dukungan serta bantuan kepada penulis dalam menyelesaikan Tugas Akhir ini.
5. Paman (Mansyur Syah) dan Bibi (Mardilah) yang memberikan do'a dan suport kepada penulis dalam menyelesaikan Tugas Akhir ini.
6. Keluarga Besar M.TEL 16 serta teman teman seperjuangan M.TEL di Konsentrasi Sekuriti Sistim ICT dalam mengerjakan Tesis yang telah

memberikan dukungan serta bantuan kepada penulis dalam menyelesaikan Tugas Akhir ini.

7. Teman-teman alumni Universitas Diponegoro yang berada di Jakarta Agus, Madchan, Handi, Tyok, Mbah Tom, Mujib, Faqih, Sahid dan masih banyak lagi yang tidak bisa disebutkan satu persatu yang telah memberikan dukungan serta bantuan kepada penulis dalam menyelesaikan Tugas Akhir ini.
8. Keluarga Besar PT. Treemas Solusi Utama dan teman-teman di client (HSBC dan SIGMA) yang memberikan suport dan memerikan waktu disela-sela kesibukan pekerjaan untuk menyelesaikan Tugas Akhir ini.
9. Dewan Guru dan teman-teman Jama'ah Majelis Rasulullah SAW yang telah memberikan do'a dan suport kepada penulis dalam menyelesaikan Tugas Akhir ini.
10. Semua sahabat dan semua pihak yang telah memberikan dukungan serta do'a kepada penulis dalam menyelesaikan Tugas Akhir ini.

Penulis menyadari bahwa Tugas Akhir ini jauh dari kata sempurna, tetapi Penulis berharap Tugas Akhir ini dapat memberikan manfaat, meski apa yang kami lakukan merupakan hanya setitik ilmu dari lautan ilmu yang tak terbatas. Semoga Allah memberi kerberkahan setiap ilmu yang kita pelajari dan amalkan.

Jakarta, 22 Mei 2017

Penulis

DAFTAR ISI

JUDUL TESIS	i
PENGESAHAN TESIS	ii
PERNYATAAN TESIS	iii
ABSTRACT	iv
ABSTRAK	v
KATA PENGANTAR	vi
DAFTAR ISI.....	viii
DAFTAR GAMBAR	x
DAFTAR TABEL.....	xiii
DAFTAR SINGKATAN	xiv
Bab I PENDAHULUAN	1
A. Latar Belakang	1
B. Rumusan Masalah.....	2
C. Tujuan Penelitian	3
D. Batasan Penelitian.....	3
E. Metodologi Penelitian.....	4
Bab II LANDASAN TEORI.....	6
A. Penelitian Terkait	6
B. Digital Forensic	10
C. Perkembangan Digital Forensics	11
D. Penerapan Metode Ilmiah untuk Digital Forensics.....	11
E. Mobile Forensics.....	13
F. Teory Enkripsi	23
G. Metode Enkripsi.....	23
H. Teknik-teknik Forensics Whatsapp.....	28

Bab III METODE PENELITIAN.....	34
A. Obyek Penelitian.....	34
B. Alur Proses Penelitian.....	35
 Bab IV PEMBAHASAN	 37
A. Uji Penelitian Forensics Pada Android	37
B. Database <i>Cryp12</i> dan tools Ekstraktor Database <i>Cryp12</i>	43
C. Analisa Database Dekripsi <i>Cryp12</i> Whatsapp Massanger	56
 Bab V KESIMPULAN dan SARAN	 69
A. Kesimpulan	69
B. Saran dan Usulan Penelitian Selanjutnya	69
 Daftar Pustaka	 70



DAFTAR GAMBAR

Gambar 2.1. Relasi Antara Jurnal Pendukung	7
Gambar 2.2. Konfigurasi Memori.....	17
Gambar 2.3. Format Ukuran SIM Card	18
Gambar 2.4. Struktur Jaringan Selular.....	19
Gambar 2.5. Sistem Clasifikasi Tools Perangkat Mobile	20
Gambar 2.6. Symmetrc-Key Encryption.....	23
Gambar 2.7. Mesin Untuk menentukan algoritma DES	27
Gambar 2.8. Asymmetric Encryption	25
Gambar 2.9. Visualisasi Algoritma Diffie-Hellman	26
Gambar 2.10. Rumuasn untuk Algoritma RSA	27
Gambar 2.11. Metodologi WhatsApp forensic dengan Internet Protocol.....	28
Gambar 2.12. Hasil dari WhatsApp forensics dengan menggunakn tools wireshark.....	29
Gambar 2.13. Metodologi WhatsApp forensics menggunakan Logical Extraction.....	30
Gambar 2.14. Log / hostory database, nomor telepon yang berwarna abu-abu untuk memastikan privasi pemilik.....	30
Gambar 2.15. Multimedia file exchange: sender side.....	31
Gambar 2.16. Multimedia file exchange: recipient side	31
Gambar 2.17. Metodologi Network analysis experimental setup.....	32

Gambar 3.1. Bagan alur Proses Penelitian	35
Gambar 4.1. List database kontak WhatsApp	39
Gambar 4.2. Detail list kontak WhatsApp massanger	40
Gambar 4.3. Record penerima multimedia file jpg	42
Gambar 4.4. Record pengiriman multimedia file jpg	42
Gambar 4.5. Log informasi WhatsApp	43
Gambar 4.6. Konsep Secara Umum Tools WhatsApp Forensics	44
Gambar 4.7. Versi <i>Andriller</i> 2.6.4.0.....	45
Gambar 4.8. Proses awal enkripsi crypt12 menggunakan tools <i>Andriller</i>	45
Gambar 4.9. Decrypting file crypt12 dengan menggunakan <i>Key</i>	46
Gambar 4.10. Hasil dari dekripsi File database crypt12 dengan <i>Andriller</i>	46
Gambar 4.11. Forensics WhatsApp call.....	47
Gambar 4.12. Forensics WhatsApp Messages	47
Gambar 4.13. Versi dari WhatsApp Viewer v1.9	48
Gambar 4.14. Proses dari pengujian dengan menggunakan tools WhatsApp Massanger	49
Gambar 4.15. Hasil dari description file database menggunakan tools <i>WhatsApp Viewer</i>	49
Gambar 4.16. Hasil dari uji forenics menggunakan tools <i>WhatsApp viewer</i> ...	49
Gambar 4.17. Tapilan web <i>Whacrypt</i>	50
Gambar 4.18. Proses upload key, upload file <i>.crypt12</i> dan hasil deskripsi.....	51
Gambar 4.19. Hasil dari uji forenics menggunakan tools <i>Whacrypt</i>	52
Gambar 4.20. History percakapan chating.....	55

Gambar 4.21. History log panggilan	55
Gambar 4.22. Timeline backup WhatsApp.....	63
Gambar 4.23. Konektifitas antar table WhatsApp massaging	64



DAFTAR TABLE

Tabel 2.1. Tabel perbandingan Penelitian.....	9
Tabel 2.1. Karakteristik Hardware	15
Tabel 2.2. Karakteristik Software	15
Tabel 4.1. WhatsApp massanger database.....	38
Tabel 4.2. Lokasi file <i>Crypt12</i> dan key.....	44
Tabel 4.3. Fitur Andriller	48
Tabel 4.4. Fitur WhatsApp Viewer.....	50
Tabel 4.5. Fitur Whatcrypt.....	52
Table 4.6. Informasi Tools WhatsApp Forenics	53
Table 4.7. Tabel Hasil Riset perbandingan data sistem dengan data Backup..	62

UNIVERSITAS
MERCU BUANA

DAFTAR SINGKATAN

2FF	2 Form Factor
3FF	3 Form Factor
4FF	4 Form Factor
4G LTE.....	4 Generation Long Term Evolution
AES	Advanced Encryption Standard
BWA	Broadband Wireless Acces
CD ROM.....	Compact Disc - Read Only Memory
CDMA.....	Code Division Multiple Access
DES	Data Encryption Standard
DRAM.....	Dynamic Random Access Memory
DVB	Digital Video Broadcasting
DVD	Digital Versatile Disc
EFF.....	Electronic Frontier Foundation
FBI	Federal Bureau Investigation
GGSN.....	Gateway GPRS Support Node
GMSC	Gateway Mobile Switching Center
GSM	Global System For Mobile Communication
HLR.....	Home Location Register
iDEN	Integrated Digital Enhanced Network

IETF	<i>Internet Engineering Task Force protocol</i>
IP	<i>Internet Protocol</i>
IrDA	<i>Infrared Data Association</i>
JTAG.....	<i>Joint Test Action Group</i>
ME.....	<i>Mobile Equipment</i>
Micro SD.....	<i>Micro Secure Digital</i>
Micro SDXC	<i>Secure Digital eXtended Capacity</i>
MSC	<i>Mobile Switching Center</i>
NAND flash	<i>NOT AND</i>
NFC.....	<i>Near Field Communication</i>
NOR flash	<i>NOT OR</i>
PSTN.....	<i>Public Swich Telephone Network</i>
Quad HD 4K	<i>Quad High Dimension 4K</i>
RAM.....	<i>Random Access Memory</i>
RNC	<i>Radio Network Controler</i>
RSA.....	<i>Rivest, Shamir, and Adleman</i>
SDM	<i>Sumbar Daya Manusia</i>
SGSN	<i>Serving GPRS Suport</i>
SIM card.....	<i>Subscriber Identity Module</i>
SRAM	<i>Static Random Access Memory</i>
TDMA	<i>Time Division Multiple Access</i>
UICC.....	<i>Universal Integradet Circuit Card</i>

VLR..... *Visitor Location Register*
WiFi *Wireless Fidelity*
WiMAX *Worldwide Interporability for Microwave Access*
WLAN..... *Wireless Local Area Network*



UNIVERSITAS
MERCU BUANA