

ANALISIS FORENSIK WHATSAPP MESSENGER DI PONSEL

CERDAS ANDROID

SKRIPSI



Disusun oleh:

Ilhami Algi Plianda

17.83.0008

**PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021**

ANALISIS FORENSIK WHATSAPP MESSENGER DI PONSEL

CERDAS ANDROID

SKRIPSI

Diajukan kepada Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
untuk memenuhi salah satu syarat memperoleh gelar Sarjana Komputer
Pada Jenjang Program Sarjana – Program Studi Teknik Komputer



Disusun oleh:

Ilhami Algi Plianda
17.83.0008

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS FORENSIK WHATSAPP MESSENGER DI PONSEL

CERDAS ANDROID

yang dipersiapkan dan disusun oleh

Ilhami Algi Plianda

17.83.0008

Telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 3 Mei 2021

Dosen Pembimbing,

Rini Indrayani, S.T., M.Eng

NIK. 190302417

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS FORENSIK WHATSAPP MESSENGER DI PONSEL

CERDAS ANDROID

yang dipersiapkan dan disusun oleh

Ilhami Algi Plianda

17.83.0008

Telah dipertahankan di depan Dewan Penguji
pada tanggal 26 April 2021

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Dony Ariyus, M.Kom

NIK. 190302128

Majid Rahardi, S.Kom., M.Eng

NIK. 190302393

Rini Indrayani, ST., M.Eng

NIK. 190302412

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 26 April 2021

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, M.Kom

NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Ilhami Algi Plianda

NIM : 17.83.0008

Menyatakan bahwa Skripsidengan judul berikut:

Analisis Forensik WhatsApp Messenger Di Ponsel Cerdas Android

Dosen Pembimbing : Rini Indrayani, S.T., M.Eng

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi

Yogyakarta, 3 Mei 2021

Yang Menyatakan,



Ilhami Algi Plianda

HALAMAN MOTTO

If something stands between you and your success move it never be denied

“Jika sesuatu berdiri antara anda dan kesuksesan anda memindahkannya tidak pernah ditolak

(The Rock Dwayne Johnson)

"It's okay to start with success, but it's more important to pay attention to lessons about failure."

"Tidak apa-apa untuk memulai dengan sukses, tetapi lebih penting untuk memperhatikan pelajaran tentang kegagalan."

(Bill Gates)

"Nothing will work unless you do."

"Tidak ada yang akan berhasil kecuali Anda melakukannya."

(Maya Angelou)

"As long as there are hands to respond to and feet to step on, nothing is impossible, right?"

“Selama ada tangan yang bisa menanggapi dan kaki untuk melangkah, tak ada yang tak mungkin, bukan?”

(Ilhami Algi Plianda)



HALAMAN PERSEMBAHAN

Dengan segala kerendahan hati dan penuh rasa syukur kepada Allah SWT, karya kecil ini dan sederhana ini, kupersembahkan sebagai wujud rasa hormat dan terima kasih yang tak terhingga kepada orang-orang terdekat dan kucintai. Skripsi ini penyusun mempersembahkan untuk:

1. Terima Kasih kepada Ibu Rini Indrayani, ST, M.Eng. selaku dosen pembimbing saya sangat banyak membantu dalam penyusunan skripsi
2. Terima kasih kepada dosen-dosen prodi Teknik Komputer untuk ilmu yang berikan sampai saat ini semoga menjadi berkah sampai kekal.
3. Kepada orang tua saya Bapak Bastami dan Ibu Ernawati yang senantiasa memberikan dukungan, uang, semangat dan doa sehingga penyusunan skripsi dapat berjalan dengan lancar dan Kakak saya Ilhami Rizqi dan adik Coni Fadela tidak pernah berhenti memberikan semangat.
4. Teman-teman Teknik Komputer 01 Terkhusus Hafiz Nur Setyo, Aljo Renaldo, Hardiansyah, Dila yang telah banyak membantu penyusunan skripsi.
5. Teman-teman kontrakan hardiansyah, Aljo Renaldo, Tirta Maulana, Randika Ramdan Pamilio, Hafiz Nur Setyo, Lisa Naomi, Umi muslifah, Nunda, Ansuri Padila, Setiawan, Dhafid, Albar, Deris yang telah memberikan semangat serta dukungan selama menyelesaikan skripsi ini.
6. Teman-teman Teknik Komputer 2017 yang tercinta.

KATA PENGANTAR

Puji syukur saya ucapkan kepada Tuhan Yang Maha Esa, atas rahmat dan karunia-Nya yang telah diberikan sehingga dapat menyelesaikan penulisan skripsi dengan judul “Analisis Forensik Whatsapp Messenger Di Ponsel Cerdas Android”. Penulisan skripsi ini diharapkan dapat memberikan sumbangan bagi dunia pendidikan khususnya di bidang Jaringan Internet.

Skripsi ini juga sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer pada Program Studi S1 Teknik Komputer Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.

Penulisan skripsi ini dapat berjalan dengan lancar hingga selesai dikarenakan banyak bantuan dan bimbingan dari berbagai pihak. Oleh karena itu, penulisan mengucapkan terima kasih kepada:

1. Allah SWT karena atas karunia-Nya, penulis dapat menyelesaikan skripsi ini dengan baik dan lancar semoga dapat memberikan manfaat di kemudian hari.
2. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas AMIKOM.
3. Bapak Dony Ariyus, M.Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta.
4. Ibu Rini Indrayani, ST, M.Eng. selaku Dosen Pembimbing yang telah bersedia memberikan pengarahan dan bimbingan dalam penyusunan Skripsi ini.
5. Segenap Dosen, Staff, dan Karyawan Universitas AMIKOM Yogyakarta telah memberikan ilmu kepada penulis dibangku kuliah dan membantu penulis dalam kelancaran administrasi sampai Skripsi terselesaikan.
6. Kedua Orang tua, saudara-saudara beserta keluarga yang selalu mendoakan dan memberikan dukungan kepada penulis.
7. Serta semua pihak teman-teman S1 Teknik Komputer dalam penyusunan Skripsi yang tidak dapat disebut satu per satu.

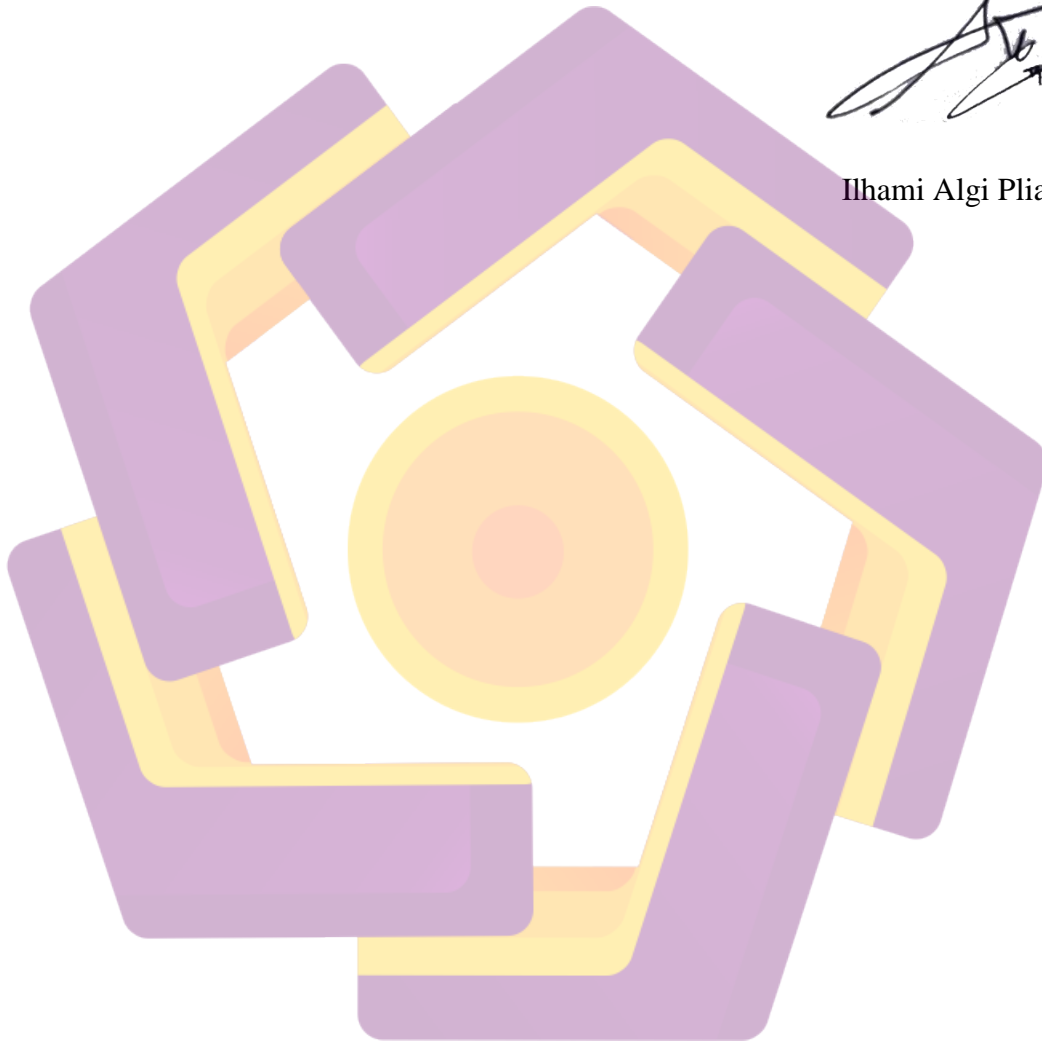
Penulis semoga skripsi ini bermanfaat bagi semua pihak yang terkait dalam penulisan ini. Skripsi ini didalam penulisan ada kekurnagan karena terbatasnya

pengetahuan dan pengalaman penulis. Karena itu, dengan terbuka lapang hati penulis mengharapkan kritik dan saran yang guna menyempurnakan skripsi ini.

Yogyakarta,



Ilhami Algi Plianda



DAFTAR ISI

HALAMAN JUDUL.....	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN KEASLIAN SKRIPSI.....	v
HALAMAN MOTTO.....	vi
HALAMAN PERSEMBAHAN.....	viii
KATA PENGANTAR.....	ix
DAFTAR ISI.....	xi
DAFTAR TABEL.....	xv
DAFTAR GAMBAR.....	xvii
DAFTAR ISTILAH.....	xxi
INTISARI.....	xxii
<i>ABSTRACT</i>	xxiii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah dan Hipotesis (hipotesis opsional).....	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	4
1.6 Sistematika Penulisan.....	4
BAB II LANDASAN TEORI.....	6
2.1 Tinjauan Pustaka.....	6
2.2 Bukti Digital.....	10
2.3 Digital Forensik.....	11
2.4 Aplikasi WhatsApp.....	11

2.5 <i>Mobile Forensic</i>	12
2.6 <i>Cybercrime</i>	12
2.7 <i>Instan Messenger</i>	13
2.8 <i>Data Recovery</i>	13
2.9 <i>MOBILedit Forensik</i>	14
2.10 <i>FTK Imager</i>	14
2.11 <i>DB SQLite Browser</i>	14
2.12 <i>WhatsApp Viwers</i>	15
2.13 <i>NIST (National Institute of Standars and Technology)</i>	15
2.14 <i>SOP (Standars Opersional Prosedur)</i>	16
2.15 <i>Penegakan Hukum Pidana</i>	16
BAB III METODOLOGI PENELITIAN	18
3.1 <i>Deskripsi Singkat Obyek</i>	18
3.2 <i>Analisis Permasalahan</i>	19
3.3 <i>Solusi Yang Diusulkan</i>	20
3.4 <i>Alat dan Bahan Penelitian</i>	21
3.5 <i>Metode Penelitian</i>	22
3.5.1 <i>Metode Pengumpulan Data</i>	25
3.5.2 <i>Prosedur Penelitian</i>	25
3.5.3 <i>Metode Ekstraksi Data di Smartphone</i>	26
3.5.4 <i>Metode Akusisi Live Forensik</i>	28
3.5.5 <i>Analisi</i>	29
3.5.6 <i>Metode Perancangan Simulasi Kasus</i>	30
3.5.6.1 <i>Alur Perancangan Analisis Investigasi Formal & Informal</i>	31

BAB IV PEMBAHASAN.....	34
4.1 Collection (Pengumpulan)	34
4.1.1 Perancangan Skenario.....	34
4.1.2 Persiapan	34
4.1.3 Proses Uji Coba MOBILedit.....	35
4.1.4 Proses Uji Coba Oxygen Forensik.....	39
4.1.3 Proses Opsi Informal.....	41
4.2 Imaging	45
4.2.1 Imaging Data Formal	45
4.2.1 Imaging Data Informal.....	48
4.3 Examination dan Analisis	53
4.3.1 Ekstraksi Data WhatsApp Logical dari MOBILedit	53
4.3.2 Analisis data WhatsApp Pada MOBILedit.....	57
4.3.3 Ekstraksi data WhatsApp Logical dari Oxygen Forensik.....	59
4.3.4 Analisis hasil data WhatsApp di Oxygen Forensik	60
4.3.5 Ekstraksi Data Informal Dengan Teknik Physical Memori.....	65
4.3.6 Decrypt Database WhatsApp.....	68
4.3.7 Analisis	69
4.3.8 Analisis Pesan Teks	72
4.3.9 Informasi Kontak	74
4.4 Reporting(Laporan).....	76
4.5 Analisis Hukum yang Berlaku	78
4.5.1 Kasus Penipuan	78
4.5.2 Kasus Penghilangan Barang Bukti.....	79

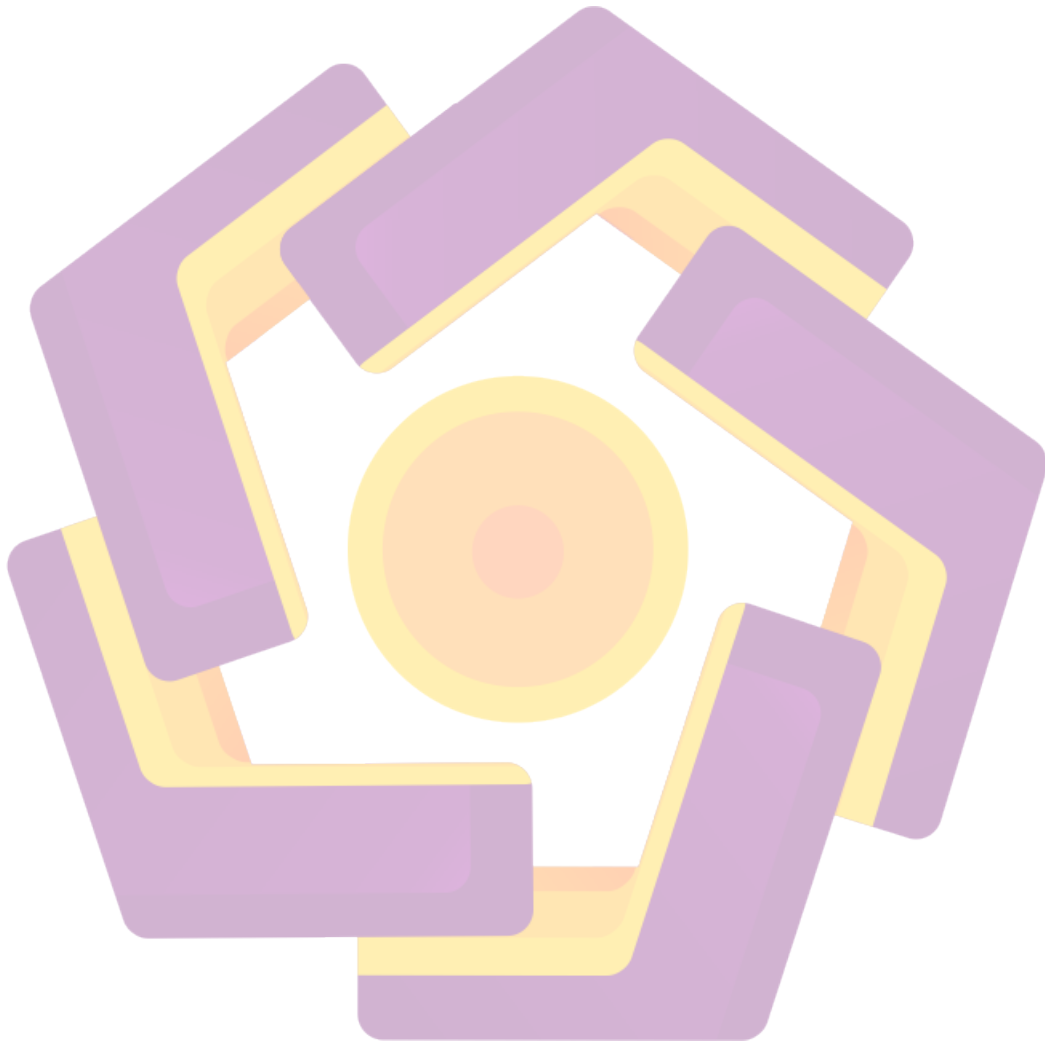
BAB V PENUTUP..... 81

 5.1 Kesimpulan 81

 5.2 Saran 81

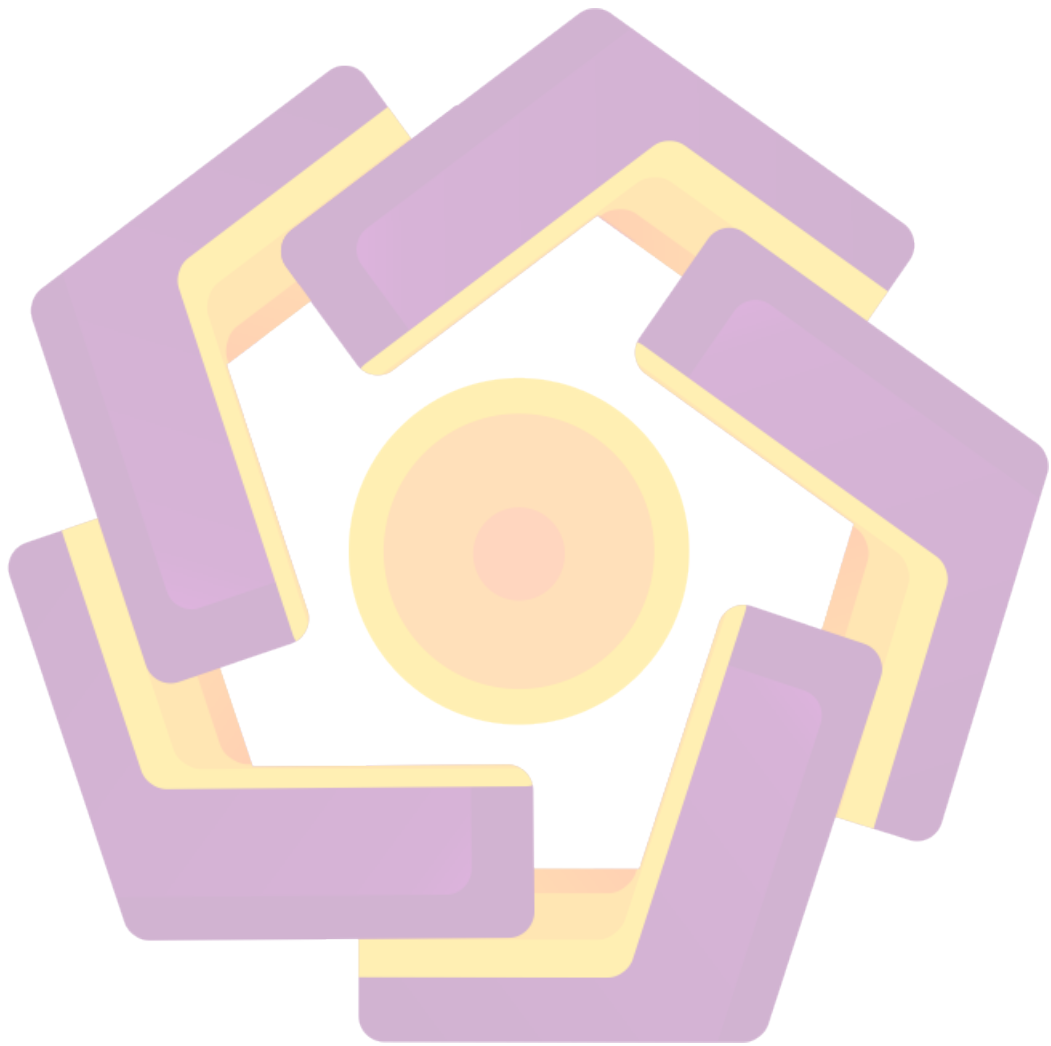
DAFTAR PUSTAKA 83

LAMPIRAN..... 86



DAFTAR TABEL

Tabel 2.1 Literatur dan Penelitian Sebelumnya	9
Tabel 3.1 Masalah Pada Objek Penelitian.....	19
Tabel 3.2. Daftar Solusi	20
Tabel 3.3 Alat dan Bahan Penelitian.....	21
Tabel 4.2.1.1 Vrefikasi Hasil Imaging.....	47
Tabel 4.2.1.2 Detail Akuisisi Data Backup MOBILedit (Smartphone).....	47
Tabel 4.2.1.3 Vrefikasi Hasil Imaging.....	48
Tabel 4.2.1.4 Detail Akuisisi Data Backup Oxygen Forensik.....	49
Tabel 4.2.3.1 Vrefikasi Hasil Imaging Memori Card	52
Tabel 4.2.3.2 Hasil Akuisisi Memori Card Pada Smratphone.....	52
Tabel 4.3.1.1 Folder Hasil Ekstraksi dan Ekspor data Aplikasi WhatsApp	54
Tabel 4.3.2.1 Laporan ditemukan pada MOBILedit Forensik	58
Tabel 4.3.4.1 Hasil Laporan ditemukan Pada Oxygen Forensik.....	66
Tabel 4.3.7.1 Hasil Artefak WhatsApp.....	71
Tabel 4.4.1 Hasil Informasi Laporan	76
Tabel 4.4.2 Perbandingan Hasil Laporan Kemampuan Tools	78

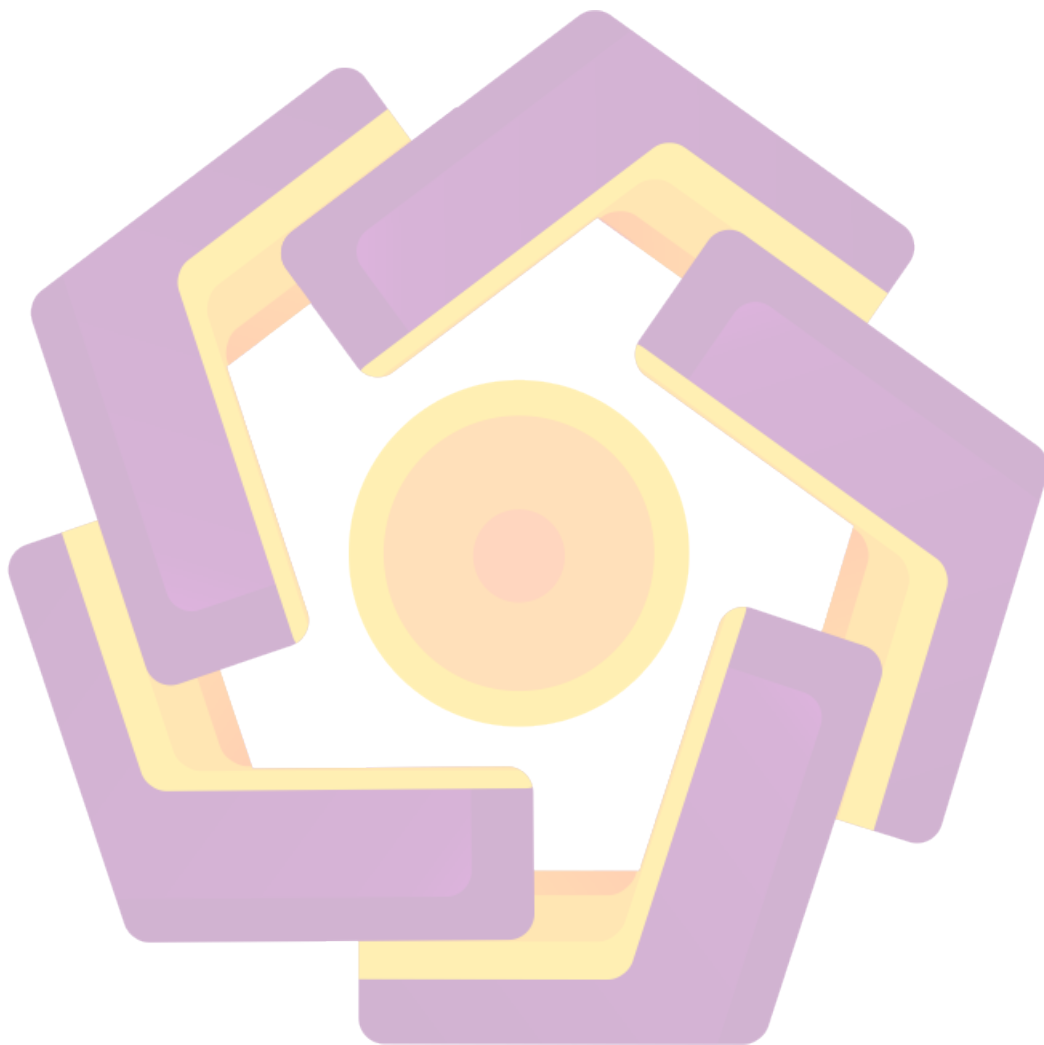


DAFTAR GAMBAR

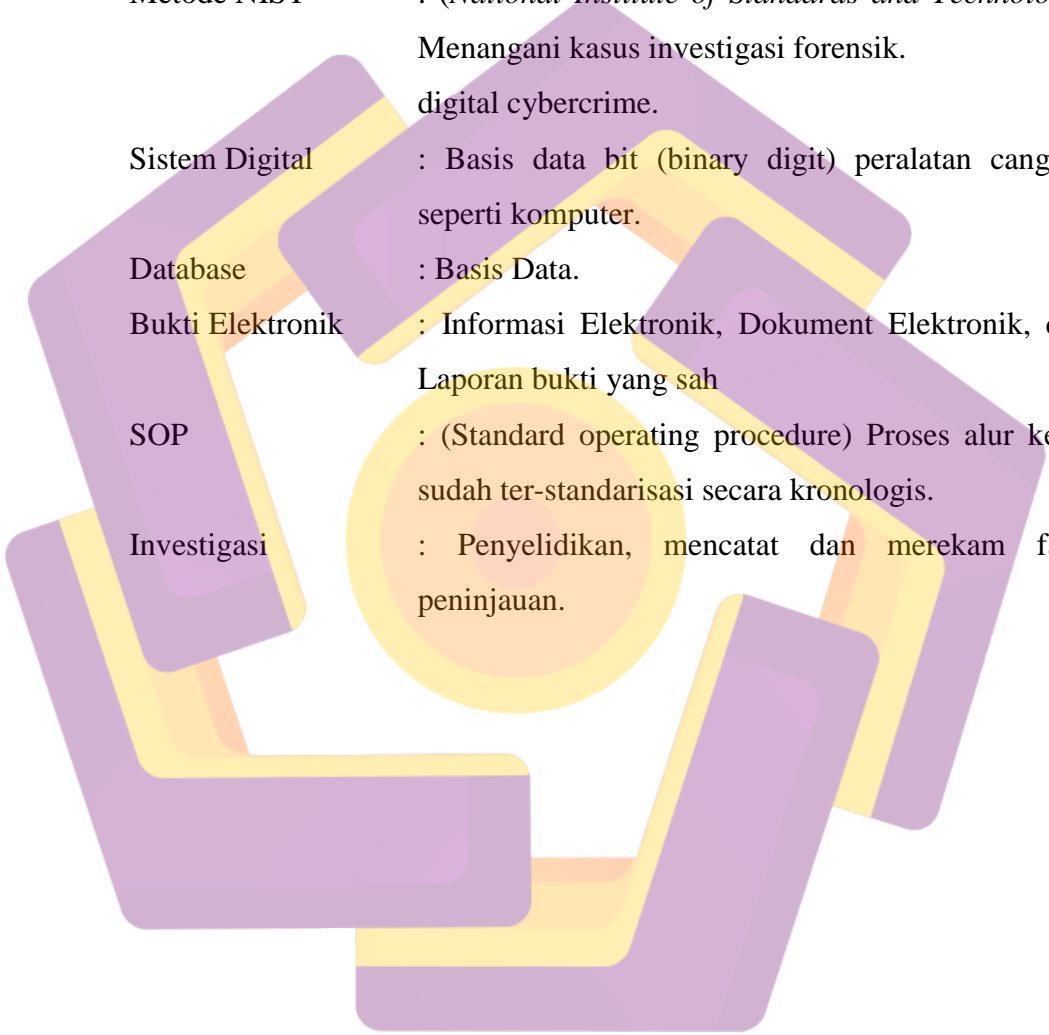
Gambar 3.2. Tahapan Metode Forensik	22
Gambar 3.2. Prosedur Penelitian.....	25
Gambar 3.5.3.1 Pramida Fase Forensik	27
Gambar 3.5.4.1 Teknik Akuisisi Live Forensik.....	29
Gambar 3.5.4.1. Flowchart Analisis Investigasi Data Formal	31
Gambar 3.5.4.1. Flowchart Analisis Investigasi Data Informal.....	32
Gambar 4.1.1.1 Simulasi Kasus Penipuan Pada Aplikasi WhatsApp.....	34
Gambar 4.1.2.1 Evidence ditemukan dan Spesifikasi Smartphone	35
Gambar 4.1.2.2 MOBILedit Berhasil diinstall dan Terhubung Perangkat	36
Gambar 4.1.2.3 Telpon Tidak di Root	36
Gambar 4.1.2.4 Aplikasi WhatsApp yang di Ekstraksi	37
Gambar 4.1.2.5 Informasi Case Detail Smartphone dan Investigator.....	37
Gambar 4.1.2.6 Format Pemilihan Laporan dan Penyimpanan	38
Gambar 4.1.2.7 Password Perangkat dan MOBILedit Forensik.....	38
Gambar 4.1.2.8 Hasil Data yang Berhasil dibakup	39
Gambar 4.1.4.1 Tampilan Oxygen Forensik.....	40
Gambar 4.1.4.2 Informasi Yang didapatkan di Smartphone	40
Gambar 4.1.4.3 Proses Ekspor Data Smartphone penyimpanan.....	41
Gambar 4.1.4.4 Data Berhasil di Backup.....	42
Gambar 4.1.5.1 Rooting Smartphone.....	43
Gambar 4.1.5.2 Tools Backup yang dibutuhkan.....	44
Gambar 4.1.5.3 Proses Install CWM Recovery	44

Gambar 4.1.5.4 Tampilan Proses CWM Recovery Backup & Restore	45
Gambar 4.2.1.1 Data yang akan di Akuisisi.....	46
Gambar 4.2.1.2 Pproses Akuisisi Data Penyimpanan Aplikasi WhatsApp	46
Gambar 4.2.1.3 Informasi Nilai Hash File Image	47
Gambar 4.2.1.4 Informasi Folder Data WhatsApp Aplikasi Oxygen Forensik....	48
Gambar 4.2.3.1 Imaging Memori Dengan Card Reader di FTK Imager	50
Gambar 4.2.3.2 Imaging File Memori dan Penyimpanan Hasil Imaging	50
Gambar 4.2.3.3 Informasi Nilai Hash dan Proses Akuisisi.....	51
Gambar 4.2.3.4 Proses Akuisisi Hasil Imaging Memori	51
Gambar 4.2.3.5 Hasil Imaging Backup Memori	52
Gambar 4.3.1.1 Struktur Direktori com.whatsapp	53
Gambar 4.3.1.2 Informasi Database WhatsApp.....	54
Gambar 4.3.1.3 Informasi Evidence, devices, dan investigator.....	55
Gambar 4.3.1.4 Hasil Media Gambar dan Video ditemukan.....	56
Gambar 4.3.1.5 Permission pada Perangkat	57
Gambar 4.3.2.1 Hasil Analisis Manual	57
Gambar 4.3.2.2 Laporan Informasi	58
Gambar 4.3.3.1 Hasil File Ekstraksi dari Oxygen Forensik	59
Gambar 4.3.3.2 Hasil Informasi File Devices.....	60
Gambar 4.3.4.1 Data Even Log didapatkan	60
Gambar 4.3.4.2 Hasil Data Call	61
Gambar 4.3.4.3 Hasil Kontak ditemukan ekstkasi logical dan manual	61
Gambar 4.3.4.4 Hasil Messages ditemukan pada perangkat.....	62

Gambar 4.3.4.5 Hasil Media Video ditemukan	62
Gambar 4.3.4.6 Data File ditemukan	63
Gambar 4.3.4.7 Hasil Permission Pada Smartphone	64
Gambar 4.3.4.8 Hasil Data Recovery Kontak.....	64
Gambar 4.3.5.1 Data Ekstak dan di Analisis	65
Gambar 4.3.5.2 Database WhatsApp	66
Gambar 4.3.5.3 Folder File terdapat Kunci, Logs, dan Avatars	66
Gambar 4.3.5.4 Temuan Hasil Ekstraksi Gambar & Video.....	67
Gambar 4.3.5.5 Hasil Data Ekstraksi dan Recovery	68
Gambar 4.3.6.1 Mendeskripsi Database crypt12 diWhatsApp Viwers	68
Gambar 4.3.6.2 Hasil Deskripsi Database	69
Gambar 4.3.6.3 Hasil Percakapan Berhasil dipulihkan.....	69
Gambar 4.3.6.4 Hasil Percakapan di Convert Html.....	70
Gambar 4.3.8.1 Database WhatsApp	72
Gambar 4.3.8.2 Hasil Pesan didatabase msgstore.db.....	73
Gambar 4.3.8.3 Informasi Waktu pesan ditambahkan dan dihapuskan.....	74
Gambar 4.3.9.1 Hasil Kontak di Database wa.db	75
Gambar 4.3.9.2 Kontak di Blokir	75
Gambar 4.3.9.3 Hasil Kontak ditambahkan	75
Gambar 4.3.9.4 Hasil Logs Database.....	75



DAFTAR ISTILAH



Cybercrime	: Kejahatan dunia maya.
Penipuan	: Tindakan kriminal tipu kebohongan.
Forensik Digital	: mengidentifikasi, menganalisa, kasus digital.
Metode NIST	: (<i>National Institute of Standards and Technology</i>) Menangani kasus investigasi forensik. digital cybercrime.
Sistem Digital	: Basis data bit (binary digit) peralatan canggih seperti komputer.
Database	: Basis Data.
Bukti Elektronik	: Informasi Elektronik, Dokument Elektronik, dan Laporan bukti yang sah
SOP	: (Standard operating procedure) Proses alur kerja sudah ter-standarisasi secara kronologis.
Investigasi	: Penyelidikan, mencatat dan merekam faka peninjauan.

INTISARI

Kejahatan digital atau yang dikenal dengan *cybercrime* saat ini sangat rentan dengan menggunakan aplikasi *instant messenger* (IM) yaitu WhatsApp. WhatsApp menjadi sasaran para penjahat *cybercrime* (*penipuan*). Perkembangan aplikasi WhatsApp sangat pesat karena berbagi fitur dalam mendukung pengguna untuk berkomunikasi dan bertukar informasi sehingga banyak oknum yang melakukan kejahatan *cybercrime* dengan penipuan pada aplikasi WhatsApp di smartphone Android.

Analisis dilakukan untuk implementasi bukti dan jejak digital yang dilakukan secara *live forensik* menggunakan metode NIST (*National Institute of Standards and Technology*) yaitu *Collection, Examination, Analysis, dan Reporting*. Proses investigasi menggunakan alat seperti MOBILedit Forensics, Oxygen Forensics, dan FTK Imager. Persentase bukti yang ditemukan adalah 40%, oleh karena itu peneliti menawarkan proses Informal menggunakan metode *rooting* untuk pemulihan akses data.

Hasil dari implementasi ekstraksi data adalah file media, 2 gambar, 1 video, 3 percakapan, 11 kontak, 2 database, artefak, 3 avatar, 4 file data, dan hampir 80% data berhasil direcovery menggunakan *metode rooting*. Sehingga kasus yang ditemukan seperti percakapan dalam modus penipuan, gambar dan video. Informasi hasil perkara digunakan sebagai bukti laporan dalam penanganan kasus *cybercrime* di aplikasi WhatsApp. Barang bukti akan digunakan sebagai tindak pidana penipuan yang terjadi pada aplikasi WhatsApp berbasis smartphone android dan sistem pembuktian dalam kasus *cybercrime* (*penipuan*) ditentukan berdasarkan Pasal 378 KUHP. Barang bukti dan keterangan saksi mengacu pada dokumen elektronik dan bukti hukum hasil cetak yang sah sebagai pelaku *cybercrime* (*penipuan*). Undang-Undang Nomor 19 Tahun 2016 Pasal 28 ayat (1) dan Pasal 45 A ayat (1) UU 19/2016.

Kata kunci: *Forensik Digital, Forensik Seluler, Kejahatan Dunia Maya, Messenger Whatsapp, Live Forensik, Prosedur Forensik*

ABSTRACT

Digital crime or what is known as cybercrime is currently very vulnerable by using instant messenger (IM) applications, namely WhatsApp. WhatsApp is the target of cybercrime (fraud) criminals. The development of the WhatsApp application is very rapid because it shares features in supporting users to communicate and exchange information so that many individuals commit cybercrime crimes with fraud on the WhatsApp application on an Android smartphone.

The analysis was carried out for the implementation of digital evidence and traces carried out by live forensics using the NIST (National Institute of Standards and Technology) method, namely Collection, Examination, Analysis, and Reporting. The investigation process uses tools such as MOBILedit Forensics, Oxygen Forensics, and FTK Imager. The percentage of evidence found was 40%, therefore the researcher offers an informal process using the rooting method for data access recovery.

The results of the data extraction implementation were media files, 2 images, 1 video, 3 conversations, 11 contacts, 2 databases, artifacts, 3 avatars, 4 data files, and almost 80% of the data were successfully recovered using the rooting method. So that cases that are found such as conversations in fraud mode, pictures, and videos. Information on the results of the case is used as evidence for reports in the handling of cybercrime cases on the WhatsApp application. Evidence will be used as a criminal act of fraud that occurs on the WhatsApp application based on an android smartphone and the evidence system in cybercrime (fraud) cases is determined based on Article 378 of the Criminal Code. Evidence and witness testimony refer to electronic documents and printed results of Formal evidence that are valid as perpetrators of cybercrime (fraud). Law Number 19 the Year 2016 Article 28 paragraph (1) and Article 45 A paragraph (1) Law 19/2016.

Keyword: *Digital Forensic, Mobile Forensic, Cybercrime, Whatsapp Messaging, Live Forensic, Prosedur Forensic*