



**ANALISA DIGITAL FORENSIK APLIKASI
FACEBOOK MESSENGER PADA ANDROID
DENGAN METODE LOGICAL ANALYSIS**

TESIS

UNIVERSITAS
Oleh
Mualim
MERCU BUANA
55415120012

**PROGRAM MAGISTER TEKNIK ELEKTRO
PROGRAM PASCASARJANA
UNIVERSITAS MERCU BUANA
2020**

ABSTRAK

Facebook messenger menjadi salah satu media social yang populer digunakan setelah Whatsapp. Dengan meningkatnya penggunaan aplikasi instant messaging tidak menutup kemungkinan aplikasi tersebut digunakan untuk mendukung aksi kejahatan sebagai media komunikasinya. Dalam kasus yang melibatkan perangkat smartphone, penyidik perlu melakukan mobile forensik. Mobile forensik merupakan salah satu cabang digital forensik yang mempelajari cara melakukan recovery bukti dari perangkat smartphone. Penelitian ini akan melakukan pengangkatan barang bukti digital dari facebook messenger pada smartphone android. Pada penelitian ini metode yang digunakan yaitu logical analysis, dengan tool yang digunakan ADB Pull. Hasil penelitian ini, tool ADB Pull dapat mendapatkan teks percakapan, akun, gambar, log voice call dan video, yang tidak didapatkan berupa pesan yang sudah dihapus.

Kata kunci: *Digital Forensik, Facebook Messenger, Logical Analysis.*



ABSTRACT

Facebook messenger is one of the popular social media used after Whatsapp. With the increasing use of instant messaging applications, it is possible for these applications to be used to support criminal acts as a medium of communication. In cases involving smartphone devices, investigators need to carry out mobile forensics. Mobile forensics is a branch of digital forensics that studies how to recover evidence from smartphone devices. This research will carry out the removal of digital evidence from Facebook Messenger on an Android smartphone. In this study, the method used was logical analysis, with the ADB Pull tool used. The results of this study, the ADB Pull tool can get conversation texts, accounts, voice call log images and videos, which are not obtained in the form of messages that have been deleted.

Keywords: *Digital Forensik, Facebook Messenger, Logical Analysis*



PERNYATAAN

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

Judul : Analisa Digital Forensik Aplikasi Facebook Messenger
Pada Android Dengan Metode Logical Analysis
Nama : Muallim
NIM : 55415120012
Program : Magister Teknik Elektro
Konsentrasi : Keamanan Jaringan ICT
Tanggal : 03 Desember 2020

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 diperguruan tinggi lain. Semua informasi, data, dan hasil pengolahannya yang digunakan, telah dinyatakan secara sumbernya dan dapat diperiksa kebenarannya.

UNIVERSITAS
MERCU BUANA

Jakarta, 03 Desember 2020



Muallim

PENGESAHAN TESIS

Judul : Analisa Digital Forensik Aplikasi Facebook Messenger
Pada Android Dengan Metode Logical Analysis
Nama : MUALIM
NIM : 55415120012
Program : Pascasarjana Program Magister Teknik Elektro
Konsentrasi : Keamanan Jaringan ICT
Tanggal : 03 Desember 2020

Mengesahkan,
Pembimbing



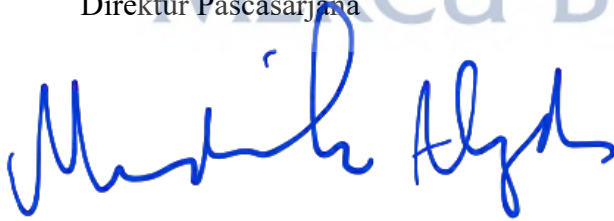
Prof. Dr. Ing. Mudrik Alaydrus

UNIVERSITAS

MERCU BUANA

Direktur Pascasarjana

Ketua Program Studi



Prof. Dr. Ing. Mudrik Alaydrus



Prof. Dr. Andi Adriansyah, M.Eng

PERNYATAAN *SIMILARITY CHECK*

Saya yang bertanda tangan di bawah ini menyatakan, bahwa karya ilmiah yang ditulis oleh

Nama : Muallim
NIM : 55415120012
Program Studi : Magister Teknik Elektro

dengan judul

“Analisa Digital Forensik Aplikasi Facebook Messenger Pada Android Dengan Metode Logical Analysis”,

telah dilakukan pengecekan *similarity* dengan sistem Turnitin pada tanggal 17/06/2021, didapatkan nilai persentase sebesar 27 %.

Jakarta, 17 Juni 2021

Administrator Turnitin

UNIVERSITAS
MERCU BUANA


Arie Pangudi, A.Md

KATA PENGANTAR

Dengan nama Allah SWT, yang Maha Pengasih lagi Maha Penyayang. Alhamdulillah, Puji syukur atas segala Rahmat dan Karunia-nya, disertai do'a restu keluarga, akhirnya dapat menyelesaikan tesis ini.

Dengan segala keterbatasan, penulis menyadari pula bahwa tesis ini tidak akan terwujud tanpa bantuan, bimbingan dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Bapak Prof. Dr. Ing, Mudrik Alaydrus selaku Dosen pembimbing dan Direktur Pascasarjana
2. Bapak Prof. Dr. Andi Adriansyah selaku Ketua Program Studi Magister Teknik Elektro.
3. Seluruh Dosen dan Staf Program Studi Magister Teknik Elektro Universitas Mercu Buana.
4. Bapak Miyono, atas segala bantuan dan dukungannya.
5. Kedua orang tua yang telah memberikan doa.
6. Istri dan anak-anakku yang telah mendukung dalam segala hal.
7. Rekan-rekan mahasiswa Magister Teknik Elektro angkatan 18.
8. Segenap pihak yang turut membantu menyelesaikan pembuatan dan penulisan tesis ini.

Penulis menyadari bahwa dalam penulisan tesis ini masih banyak kekurangan. Oleh karena itu saran dan kritik yang membangun akan penulis terima dengan senang hati. Akhir kata penulis berharap agar tesis ini bermanfaat khususnya bagi penulis maupun pihak-pihak yang berkepentingan.

Jakarta, 25 November 2020

Mualim

DAFTAR ISI

Halaman

ABSTRAK	i
ABSTRACT	ii
PERNYATAAN.....	iii
PENGESAHAN TESIS	iv
PERNYATAAN SIMILARITY CHECK	v
KATA PENGANTAR	vi
DAFTAR ISI.....	vii
DAFTAR TABEL.....	ix
DAFTAR GAMBAR	x
BAB I PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Tujuan Penelitian	3
1.4 Manfaat Penelitian	4
1.5 Batasan Masalah	4
BAB II KAJIAN PUSTAKA	
2.1 Penelitian Terkait	5
2.2 Digital Forensik.....	8
2.3 Komponen Digital Forensik.....	8
2.4 Tahapan Proses Mobile Forensics.....	9
2.5 Metode Dalam Forensics Analysis	10
2.6 Android	14
2.7 Facebook Messenger.....	17
2.8 Logical Tools	19
2.9 SQLite	20
BAB III METODE PENELITIAN	
3.1 Studi Pustaka.....	24
3.2 Simulasi Dan Skenario Pada Aplikasi Facebook Messenger..	25
3.3 Penyusunan Skenario	26
3.4 Akuisisi	26
3.5 Metode Analisis	28
3.6 Pelaporan.....	31
3.7 Hardware dan Software.....	32
BAB VI HASIL DAN ANALISA	
4.1 Pemeliharaan Barang Bukti (Preservation).....	33

4.2	Proses dan Teknik Akuisisi Data (Acquisition).....	35
4.3	Proses pengujian dan analisa (Examination dan Analysis).....	37
4.4.	Pembuatan laporan (Reporting)	48
4.5	Pembahasan.....	49
BAB V	KESIMPULAN DAN SARAN	
5.1	Kesimpulan	51
5.2	Saran.....	51
DAFTAR PUSTAKA	52
Lampiran		



DAFTAR TABEL

	Halaman
Tabel 2.1	Perbandingan Jurnal Referensi 7
Tabel 3.1	Hardware Dan Software Yang Digunakan 32
Tabel 4.1	Identifikasi Barang Bukti 34
Tabel 4.2	SQLite Database Facebook Messenger 38
Tabel 4.3	Struktur Kolom Pada Tabel Messages 41
Tabel 4.4	Informasi Yang Didapat Dari Teknik Akuisisi ADB Pull. 49



DAFTAR GAMBAR

	Halaman
Gambar 1.1	Global Mobile App Ranking..... 2
Gambar 2.1	Komponen Dalam Digital Forensik..... 8
Gambar 2.2	Proses Mobile Forensik..... 10
Gambar 2.3	Klasifikasi Tool System Mobile Device 11
Gambar 2.4	Fernico ZRT 12
Gambar 2.5	Arsitektur Android..... 14
Gambar 3.1	Langkah-langkah Penelitian..... 23
Gambar 3.2	Alur Studi Pustaka 24
Gambar 3.3	Langkah Simulasi..... 25
Gambar 3.4	Topologi Eksperimen..... 26
Gambar 3.5	Tahapan Proses Akuisisi Data..... 27
Gambar 3.6	Proses Akuisisi Data 28
Gambar 3.7	Flowchart Analisis Digital Forensik 29
Gambar 3.8	Flowchart pemeriksaan data yang sudah diakuisisi 31
Gambar 4.1	Foto Barang Bukti..... 34
Gambar 4.2	Proses Koneksi Smartphone Ke Host Komputer 35
Gambar 4.3	Proses Akusisi Direktori Facebook Messenger 36
Gambar 4.4	Proses Hashing..... 37
Gambar 4.5	Pengujian Ulang Nilai Hash Setelah Proses Copy..... 37
Gambar 4.6	Folder-folder Potensial FacebookMessenger..... 38
Gambar 4.7	Pertukaran Pesan Teks Yang Dilakukan..... 44
Gambar 4.8	ID Facebook Messenger 45
Gambar 4.9	Kolom Attachment Tabel Message..... 46
Gambar 4.10	Informasi URL Pada Kolom Attachment 46
Gambar 4.11	Hasil Akses URL Media 47
Gambar 4.12	Informasi URL Pada Kolom Share 47
Gambar 4.13	Hasil Akses URL Share Location..... 48
Gambar 4.14	Log Panggilan Suara Dan Video..... 48

Gambar 4.15 Jumlah informasi yang didapat dari proses forensik..... 51

