

HALAMAN PENGESAHAN .....	i
PERNYATAAN BEBAS PLAGIASI .....	iii
HALAMAN PERSEMBAHAN .....	iv
KATA PENGANTAR .....	vi
DAFTAR ISI .....	vii
DAFTAR TABEL .....	x
DAFTAR GAMBAR .....	xi
DAFTAR SINGKATAN .....	xiii
INTISARI .....	xiv
ABSTRACT .....	xv
BAB I Pendahuluan .....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	3
1.3 Tujuan Penelitian .....	3
1.4 Batasan Penelitian .....	4
1.5 Manfaat Penelitian .....	4
1.6 Sistematika Penulisan .....	4
1.6.1 BAB I: Pendahuluan .....	4
1.6.2 BAB II: Tinjauan Pustaka dan Dasar Teori .....	4
1.6.3 BAB III: Metode Penelitian .....	4
1.6.4 BAB IV: Hasil dan Pembahasan .....	5
1.6.5 BAB V: Kesimpulan dan Saran .....	5
BAB II Tinjauan Pustaka dan Dasar Teori .....	6
2.1 Tinjauan Pustaka .....	6
2.2 Dasar Teori .....	10
2.2.1 WhatsApp .....	10
2.2.1.1 <i>Delete messages</i> .....	11
2.2.1.2 <i>Disappearing message</i> .....	11
2.2.1.3 <i>View once</i> .....	11
2.2.2 SQLite .....	12
2.2.2.1 <i>Write-Ahead Logging</i> .....	13
2.2.2.2 FQLite - SQLite Forensic Toolkit .....	15
2.2.3 Android .....	15
2.2.4 <i>Android Debug Bridge (adb)</i> .....	16
2.2.5 <i>Rooting</i> .....	16
2.2.5.1 TWRP .....	18

2.2.5.2	Magisk .....	18
2.2.6	Forensik Digital .....	18
2.2.7	Kerangka Kerja Forensik Digital NIST SP 800-86.....	19
2.2.8	Petunjuk Forensik Perangkat <i>Mobile</i> NIST SP 800-101r1 .....	21
2.2.9	Magnet ACQUIRE.....	24
2.2.10	Autopsy .....	24
2.2.11	Sistem Bilangan Heksadesimal.....	25
2.2.11.1	HxD - Freeware Hex Editor and Disk Editor .....	26
2.2.12	<i>Regular Expression</i> .....	26
2.2.13	Python .....	31
2.2.14	Visual Studio Code.....	32
2.3	Analisis Perbandingan Metode .....	32
2.4	Metode yang Dipilih .....	40
BAB III Metode Penelitian.....		42
3.1	Alat dan Bahan Tugas akhir .....	42
3.1.1	Alat Tugas akhir.....	42
3.1.1.1	Perangkat Keras.....	42
3.1.1.2	Perangkat Lunak .....	42
3.1.2	Bahan Tugas akhir .....	43
3.2	Alur Tugas Akhir.....	44
3.2.1	Membuka kunci <i>bootloader</i> perangkat .....	44
3.2.2	Simulasi percakapan dengan penghapusan pesan dan media .....	45
3.2.3	Preservasi: Mengamankan Perangkat.....	48
3.2.4	Akuisisi .....	50
3.2.4.1	Membuka Akses <i>Root</i> Perangkat .....	50
3.2.4.2	Akuisisi Data WhatsApp .....	53
3.2.5	Eksaminasi .....	53
3.2.5.1	Penguraian Struktur Basis Data .....	53
3.2.5.2	Pemeriksaan Heksadesimal Berkas WAL .....	54
3.2.5.3	Pembuatan Program Penemuan Pola Heksadesimal .....	54
3.2.6	Analisis: Rekonstruksi Percakapan .....	54
3.2.7	Pelaporan: Pembuatan Laporan Hasil Forensik Digital Perangkat <i>Mobile</i> .....	54
BAB IV Hasil dan Pembahasan.....		55
4.1	Eksaminasi Data .....	55
4.1.1	Penguraian Struktur Basis Data .....	56
4.1.2	Pemeriksaan Heksadesimal Berkas WAL.....	59
4.1.3	Pembuatan Program Penemuan Pola Heksadesimal.....	66
4.2	Analisis: Rekonstruksi Percakapan .....	70



4.2.1	Skenario 1 .....	70
4.2.2	Skenario 2 .....	72
4.2.3	Skenario 3 .....	77
4.3	Perbandingan Hasil Akhir .....	80
BAB V	Kesimpulan dan Saran .....	82
5.1	Kesimpulan .....	82
5.2	Saran .....	83
DAFTAR PUSTAKA	.....	84
LAMPIRAN	.....	L-1
L.1	Gambar .....	L-1
L.1.1	Tangkapan layar respon <i>fetch</i> URL media menggunakan Postman .	L-1
L.1.2	Tangkapan layar dekripsi media menggunakan whatsapp-media-decrypt .....	L-3
L.2	<i>Source Code</i> .....	L-4
L.2.1	Kode Python untuk dekode heksadesimal .....	L-4
L.2.2	Kode Python untuk ekstraksi pesan .....	L-5
L.2.3	Kode Python untuk ekstraksi media .....	L-11
L.3	Laporan Forensik Digital .....	L-16

## DAFTAR TABEL

Tabel 2.1	Contoh penggunaan sintaksis karakter <i>regular expression</i> .....	27
Tabel 2.2	Contoh penggunaan sintaksis <i>quantifier regular expression</i> .....	28
Tabel 2.3	Contoh penggunaan sintaksis logika <i>regular expression</i> .....	28
Tabel 2.4	Contoh penggunaan sintaksis kelas karakter <i>regular expression</i> .....	29
Tabel 2.5	Contoh penggunaan sintaksis <i>anchors</i> dan <i>boundaries regular expression</i> .....	30
Tabel 2.6	Contoh penggunaan sintaksis <i>inline modifiers regular expression</i> .....	30
Tabel 2.7	Contoh penggunaan sintaksis <i>lookarounds regular expression</i> .....	31
Tabel 2.8	Perbandingan metode pemulihan pesan untuk fitur <i>delete message</i> ..	34
Tabel 2.9	Perbandingan metode pemulihan pesan untuk fitur <i>disappearing message</i> .....	37
Tabel 2.10	Perbandingan metode pemulihan pesan untuk fitur <i>view once</i> .....	39
Tabel 3.1	Percakapan skenario 1 .....	46
Tabel 3.2	Percakapan skenario 2 .....	47
Tabel 3.3	Percakapan skenario 3 .....	49
Tabel 4.1	Hubungan basis data dengan isi pesan .....	60
Tabel 4.2	Pembacaan representasi bita pada <i>header baris SQLite</i> .....	63
Tabel 4.3	Rekonstruksi percakapan skenario 1 .....	73
Tabel 4.4	Rekonstruksi percakapan skenario 2 .....	78
Tabel 4.5	Rekonstruksi percakapan skenario 3 .....	80

Gambar 2.1	Transaksi SQLite mode <i>journal rollback</i> .....	14
Gambar 2.2	Transaksi SQLite mode <i>journal WAL</i> .....	14
Gambar 2.3	<i>Header</i> berkas basis data SQLite.....	15
Gambar 2.4	Alur verifikasi <i>boot</i> .....	17
Gambar 2.5	Cabang forensik digital .....	19
Gambar 2.6	Kerangka kerja forensik digital NIST SP 800-86 .....	20
Gambar 2.7	Pohon keputusan preservasi perangkat <i>mobile</i> .....	23
Gambar 2.8	Tampilan perangkat lunak Autopsy .....	25
Gambar 3.1	Diagram alir penelitian .....	44
Gambar 3.2	(a) Mengaktifkan opsi pengembang, (b) Mengizinkan <i>debugging</i> USB, dan (c) Peringatan <i>bootloader</i> terbuka .....	45
Gambar 3.3	Preservasi perangkat dengan mematikan koneksi nirkabel .....	48
Gambar 3.4	Diagram alir untuk membuka akses <i>root</i> pada perangkat.....	51
Gambar 3.5	(a) Perangkat dalam mode <i>fastboot</i> dan (b) TWRP yang telah terpasang .....	52
Gambar 3.6	(a) Memasang Magisk menggunakan TWRP dan (b) Mengaktifkan akses <i>root</i> melalui Magisk .....	52
Gambar 3.7	Akuisisi fisik menggunakan Magnet ACQUIRE .....	53
Gambar 4.1	Kode Python untuk Membuat Salinan Direktori .....	55
Gambar 4.2	Potongan heksadesimal berkas <i>msgstore.db</i> yang mengandung id pesan.....	61
Gambar 4.3	Analisis struktur heksadesimal sebuah (a) pesan biasa diterima, (b) pesan biasa dikirim, (c) pesan dengan fitur <i>disappearing message</i> dikirim.....	62
Gambar 4.4	Potongan heksadesimal berkas <i>msgstore.db</i> yang mengandung UUID media.....	64
Gambar 4.5	Analisis struktur heksadesimal media pada pesan.....	65
Gambar 4.6	Tabel message basis data <i>msgstore.db</i> pada skenario 1 .....	71
Gambar 4.7	Tabel <i>message_media</i> basis data <i>msgstore.db</i> pada skenario 1 ....	71
Gambar 4.8	Hasil ekstraksi pesan dari basis data <i>msgstore</i> skenario 1 .....	72
Gambar 4.9	Tabel message basis data <i>msgstore.db</i> pada skenario 2 .....	74
Gambar 4.10	Tabel <i>message_media</i> basis data <i>msgstore.db</i> pada skenario 2 ....	75
Gambar 4.11	Hasil pemeriksaan direktori dari kolom <i>file_path</i> (a) <code>/data/user/0/com.whatsapp/files/ViewOnce/</code> (b) <code>Media/WhatsApp Images/Sent/</code> .....	75
Gambar 4.12	Hasil ekstraksi pesan dari basis data <i>msgstore</i> skenario 2 .....	76
Gambar 4.13	Hasil ekstraksi media dari basis data <i>msgstore</i> skenario 2 .....	77
Gambar 4.14	Tabel message basis data <i>msgstore.db</i> pada skenario 3 .....	79
Gambar 4.15	Hasil ekstraksi pesan dari basis data <i>msgstore</i> skenario 3 .....	79
Gambar 4.16	Grafik perbandingan pesan dan media pada percakapan, basis data, dan berkas WAL .....	81
Gambar 4.17	Persentase pemulihan pesan dan media terhapus .....	81
Gambar 1	Respon (heksadesimal) URL media dari pesan baris ketiga .....	L-1



UNIVERSITAS  
GADJAH MADA

**Pemulihan Data Aplikasi Media Sosial WhatsApp dengan Analisis Heksadesimal Berkas Write-Ahead Logging SQLite untuk Forensik Digital**

Perwira Akhdan Zumarsyah, Ir. Sujoko Sumaryono, M.T.; Dani Adhipta, S.Si., M.T.

Universitas Gadjah Mada, 2025 | Diunduh dari <http://etd.repository.ugm.ac.id/>

Gambar 2	Respon (heksadesimal) URL media dari pesan baris kesembilan .	L-2
Gambar 3	Dekripsi media dari pesan baris ketiga .....	L-3
Gambar 4	Dekripsi media dari pesan baris kesembilan .....	L-3

## DAFTAR SINGKATAN

ADB	= Android Debug Bridge
BLOB	= Binary Large Object
IMEI	= International Mobile Equipment Identity
IoT	= Internet of Things
JID	= Jabber ID
NIJ	= National Institute of Justice
NIST	= National Institute of Standards and Technology
OEM	= Original Equipment Manufacturer
RAM	= Random Access Memory
Regex	= Regular Expression
SWGDE	= The Scientific Working Group on Digital Evidence
TWRP	= Team Win Recovery Project
URL	= Uniform Resource Locator
USB	= Universal Serial Bus
UUID	= Universal Unique ID
WAL	= Write-Ahead Logging