

**ANALISIS APLIKASI FACEBOOK MESSENGER
MENGUNAKAN METODE LIVE FORENSIK
PADA WINDOWS 10**

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



disusun oleh

SYIHABUDIN ABDUL WAHAB

18.83.0334

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

**ANALISIS APLIKASI FACEBOOK MESSENGER
MENGUNAKAN METODE LIVE FORENSIK
PADA WINDOWS 10**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



disusun oleh

SYIHABUDIN ABDUL WAHAB

18.83.0334

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

HALAMAN PERSETUJUAN

SKRIPSI

**ANALISIS APLIKASI FACEBOOK MESSENGER
MENGUNAKAN METODE LIVE FORENSIK
PADA WINDOWS 10**

yang disusun dan diajukan oleh

SYIHABUDIN ABDUL WAHAB

18.83.0334

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 22 Agustus 2023

Dosen Pembimbing,



Bapu Santoso, S.T., M.Eng

NIK. 190302327

HALAMAN PENGESAHAN
SKRIPSI
ANALISIS APLIKASI FACEBOOK MESSENGER
MENGGUNAKAN METODE LIVE FORENSIK
PADA WINDOWS 10

yang disusun dan diajukan oleh

Syihabudin Abdul Wahab

18.83.0334

Telah dipertahankan di depan Dewan Penguji
pada tanggal 22 Agustus 2023

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Banu Santoso, S.T., M.Eng
NIK. 190302327

Rizqi Sukma Kharisma, M.Kom
NIK. 190302215

Uyock Anggoro Saputro, M.Kom
NIK. 190302419

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 22 Agustus 2023

DEKAN FAKULTAS ILMU KOMPUTER



Hanif Al Fatta, S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Syihabudin Abdul Wahab
NIM : 18.83.0334

Menyatakan bahwa Skripsi dengan judul berikut:

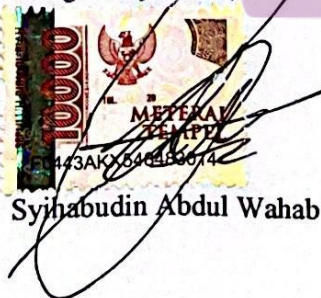

ANALISIS APLIKASI FACEBOOK MESSENGER MENGGUNAKAN METODE LIVE FORENSIK PADA WINDOWS 10

Dosen Pembimbing : Banu Santoso, 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, 22 Agustus 2023

Yang Menyatakan,



Syihabudin Abdul Wahab

HALAMAN PERSEMBAHAN

Dengan penuh rasa syukur dan bahagia telah menyelesaikan laporan tugas akhir ini yang tak luput dari doa-doa dan dukungan dari orang-orang tercinta yang selalu memberikan support. Dengan rasa bangga dan syukur saya haturkan rasa syukur dan terima kasih saya kepada:

1. Allah SWT karena hanya atas izin dan karunianya lah skripsi ini dapat dibuat dan selesai pada waktunya.
2. Kepada Ibu saya, yang telah memberikan dukungan moril maupun materil serta doa yang tiada henti untuk kesuksesan saya, karena tiada kata seindah lantunan doa dan tiada doa yang paling khusyuk selain doa yang terucap dari orang tua.
3. Bapak Banu Santoso.S.T, M.Eng selaku Pembimbing Tugas Akhir
4. Bapak serta Ibu dosen prodi Teknik Komputer
5. Kumara Shakhi, Kheiza Mahendra Akbar, M. Rafli Ramadhan, Fajriannor, Fadhli Dzil Ikram, selaku teman terbaik saya yang selalu memberidukungan terhadap saya
6. Teman-teman Teknik Komputer 03 yang telah berjuang bersama.
7. Diri saya sendiri yang telah berjuang dan semangat sampai di titik ini.

KATA PENGANTAR

Alhamdulillah puji syukur penulis panjatkan kepada Allah Subhanahu wa ta'ala atas rahmat dan karunianya yang telah senantiasa membimbing dan memudahkan jalan penulis dalam menyelesaikan penulisan tugas akhir ini. Tak lupa penulis ucapkan terimakasih kepada Dosen Pembimbing Bapak Banu Santoso, S.T., M.Eng, Penguji Bapak Rizqi Sukma Kharisma, M.Kom, Bapak Uyock Anggoro Saputro, M.Kom, kepada orang tua saya, serta semua pihak yang terkait dalam penyelesaian tugas akhir termasuk Keluarga, Sahabat dan Teman-teman.

Penulis berharap dengan adanya penulisan laporan tugas akhir ini dapat memberikan manfaat ataupun referensi bagi siapapun yang membutuhkan dan bisa dijadikan sebagai pengetahuan yang berguna dalam Analisis Forensik pada aplikasi *Facebook Messenger*.

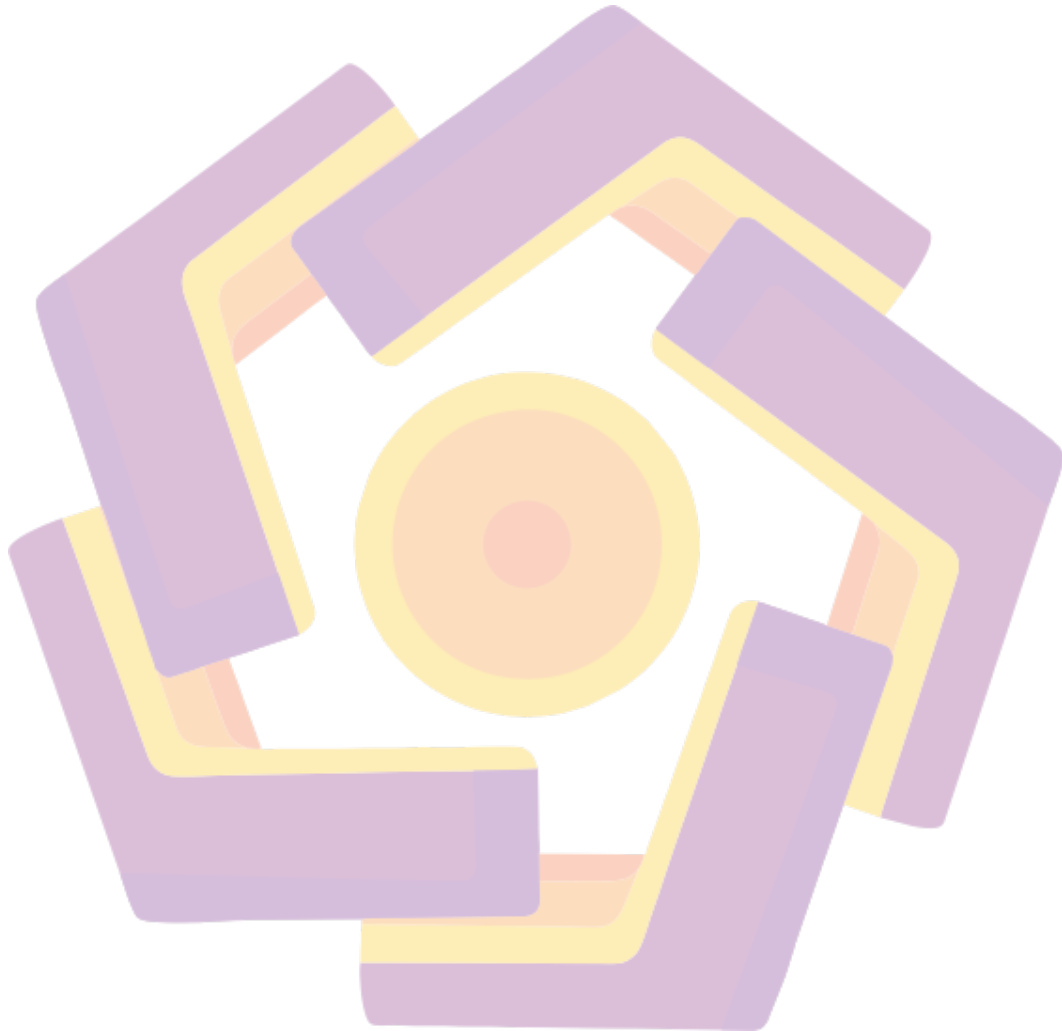
Yogyakarta, 22 Agustus 2023

Penulis

DAFTAR ISI

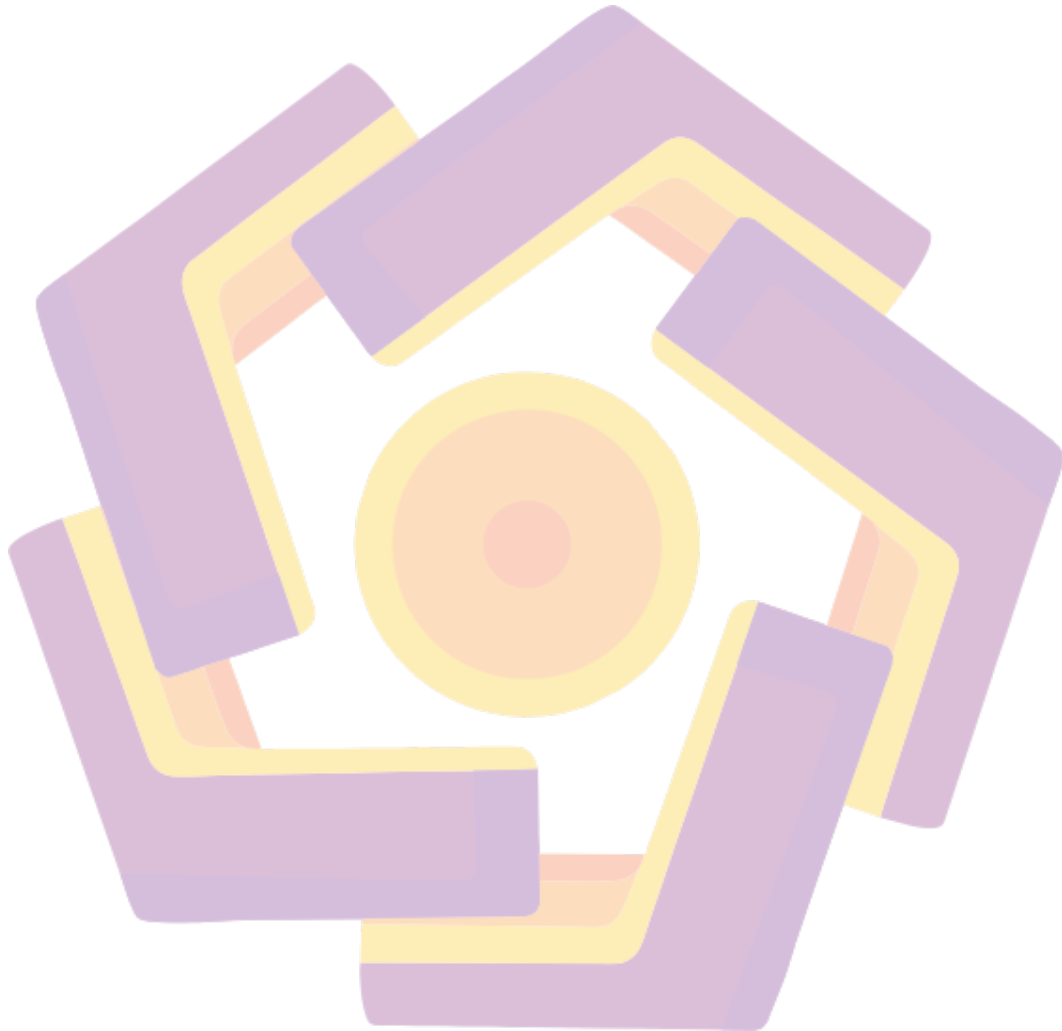
HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN.....	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	iv
HALAMAN PERSEMBAHAN	v
KATA PENGANTAR	vi
DAFTAR ISI.....	vii
DAFTAR TABEL.....	ix
DAFTAR GAMBAR	x
INTISARI.....	xi
ABSTRACT.....	xii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Sistematika Penulisan	3
BAB II TINJAUAN PUSTAKA.....	5
2.1 Studi Literatur	5
2.2 Dasar Teori.....	12
2.2.1 Digital Forensik	12
2.2.2 Live Forensics.....	13
2.2.3 Bukti Digital	13
2.2.4 Akuisisi	14
2.2.5 Facebook Messenger.....	15
2.2.6 Dumpit	16
2.2.7 Winhex.....	16
2.2.8 BelkaSoft Ram Capture	17
2.2.9 BelkaSoft Evidance Center.....	18
BAB III METODE PENELITIAN.....	20
3.1 Alur Penelitian	20
3.1.2 Studi Literatur	22
3.1.3 Alat dan Bahan.....	22
3.1.4 Penyusunan Skenario.....	23
3.1.5 Implementasi Skenario	24

BAB IV HASIL DAN PEMBAHASAN	27
4.1 Proses Digital Forensik Dengan live forensic.....	27
4.1.2 Collection.....	27
4.1.2 Examination.....	30
4.1.3 Analysis	35
4.1.4 Penyusunan Hasil Penelitian.....	42
BAB V PENUTUP	43
5.1 Kesimpulan	43
5.2 Saran	43
REFERENSI.....	44



DAFTAR TABEL

Tabel 2.1 Keaslian Penelitian.....	8
Tabel 3.1 Alat dan Bahan.....	20
Tabel 4.1 Data Pelaku dan Korban	34
Tabel 4.2 Pengelompokan data Percakapan.....	38
Tabel 4.3 Bukti Digital yang didapatkan	40



DAFTAR GAMBAR

Gambar 3.1 Alur Penelitian.....	19
Gambar 3.2 Percakapan Pelaku dan Korban.....	23
Gambar 3.3 Percakapan Pelaku dan Korban.....	23
Gambar 3.4 Percakapan Pelaku dan Korban.....	24
Gambar 3.5 Menghapus seluruh percakapan	24
Gambar 4.1 Pengambilan data RAM pada.....	24
Gambar 4.2 Proses awal DumpIt	25
Gambar 4.3 Proses akhir DumpIt.....	25
Gambar 4.4 Pemilihan folder pada RamCapturer	26
Gambar 4.5 Proses pengambilan data pada.....	26
Gambar 4.6 Proses akhir RamCapturer.....	27
Gambar 4.7 Tampilan Open File pada aplikasi Winhex	28
Gambar 4.8 Memilih file yang akan di analisa dengan Winhex	28
Gambar 4.9 Tampilan membuat New Case	29
Gambar 4.10 Menentukan file destinasi.....	30
Gambar 4.11 Pemilihan fitur Case	31
Gambar 4.12 Proses Analisa dan <i>Extracting Data</i>	31
Gambar 4.13 Proses akhir Analisa dan <i>Extracting Data</i>	32
Gambar 4.14 Tampilan profile facebook Pelaku	33
Gambar 4.15 Tampilan profile facebook Korban	33
Gambar 4.16 UserId Pelaku dan SenderId Korban.....	34
Gambar 4.17 Hasil pencarian percakapan pada aplikasi Winhex	34
Gambar 4.18 Hasil pencarian text pada aplikasi Winhex	35
Gambar 4.19 Hasil pencarian Sticker dan Foto Winhex.....	35
Gambar 4.20 Hasil pencarian text pada aplikasi Winhex	36
Gambar 4.21 Hasil pencarian lokasi file Video	36
Gambar 4.22 Folder lokasi file video.....	37
Gambar 4.23 File yang ditemukan pada folder penyimpanan mesenger.....	37

INTISARI

Facebook Messenger adalah aplikasi seluler yang dapat digunakan untuk mengirim pesan yang memfasilitasi pengguna Facebook dalam berinteraksi seperti obrolan, panggilan suara, dan panggilan video. Teknologi yang kian berkembang mengakibatkan muncul berbagai kasus *cybercrime* seperti penipuan, pelecehan seksual, pornografi, *cyber bullying*, dan *hacking*.

Metode live forensik dipilih karena kemampuannya untuk mengumpulkan dan menganalisis data secara real-time tanpa mengganggu integritas sistem. Penelitian ini mencakup langkah-langkah untuk mengakses data aplikasi Facebook Messenger yang tersimpan dalam *Random Access Memory*(RAM) sistem pada platform Windows 10. Langkah-langkah tersebut mencakup akuisisi memori, identifikasi struktur data yang relevan, dan ekstraksi informasi terkait aplikasi.

Hasil dari studi ini menunjukkan Winhex menemukan lebih banyak barang bukti digital dibandingkan *belkasoft Evidence Center*. Dalam hal akuisisi untuk waktu tercepat adalah DumpIt, dan untuk perangkat lunak yang memerlukan waktu lama adalah *Belkasoft RAM Capturer*.

Kata kunci: Live Forensik, Facebook Messenger, Windows, Analisis, Winhex, *Belkasoft Evidence Center*.

ABSTRACT

Facebook Messenger is a mobile application that can be used to send messages facilitating Facebook users in interacting such as chats, voice calls, and video calls. The advancing technology has led to various cybercrime cases such as fraud, sexual harassment, pornography, cyberbullying, and hacking.

The live forensics method is chosen due to its ability to collect and analyze data in real-time without disrupting the integrity of the system. This research encompasses steps to access Facebook Messenger application data stored in the Random Access Memory (RAM) of the system on the Windows 10 platform. These steps include memory acquisition, identification of relevant data structures, and extraction of application-related information.

The results of this study indicate that Winhex discovers more digital evidence compared to Belkasoft Evidence Center. In terms of acquisition, DumpIt is the fastest, and for software that requires more time, there is Belkasoft RAM Capturer.

Keyword: *Live Forensics, Facebook Messenger, Windows, Analysis, Winhex, Belkasoft Evidence Center.*