ANALISIS APLIKASI FACEBOOK MESSENGER MENGGUNAKAN 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

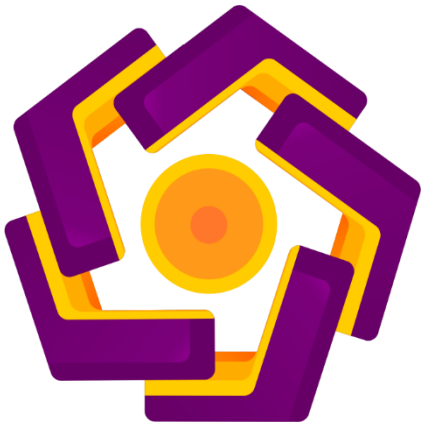
2023

ANALISIS APLIKASI FACEBOOK MESSENGER MENGGUNAKAN 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 MENGGUNAKAN METODE LIVE FORENSIK PADA WINDOWS 10

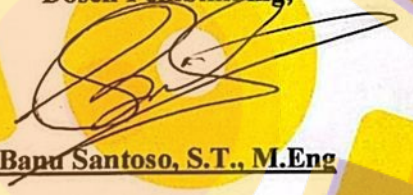
yang disusun dan diajukan oleh

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

DAFTAR TABEL

DAFTAR GAMBAR

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.*