SKRIPSI

ANALISIS BUKTI FORENSIK DIGITAL

PENIPUAN TRANSAKSI *ONLINE* PADA LINE MESSENGER

MENGGUNAKAN METODE FORENSIK LANGSUNG

SYAMSUL ARIFIN

NIM. 1910511055

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

TAHUN 2023

SKRIPSI

Diajukan sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana Komputer

ANALISIS BUKTI FORENSIK DIGITAL PENIPUAN TRANSAKSI *ONLINE* PADA LINE MESSENGER MENGGUNAKAN METODE FORENSIK LANGSUNG

SYAMSUL ARIFIN

NIM. 1910511055

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

TAHUN 2023

PERNYATAAN ORISINALITAS

SURAT PERNYATAAN ORISINALITAS

Yang bertanda tangan di bawah ini :

Nama Lengkap : Syamsul Arifin
Tempat/Tanggal Lahir : Jakarta, 21 Agustus 2001
Asal Sekolah/Universitas (Fakultas) : Universitas Pembangunan Nasional Veteran Jakarta

Dengan ini menyatakan bahwa karya dengan judul "Analisis Bukti Forensik Digital Penipuan Transaksi *Online* Pada Line Messenger Menggunakan Metode Forensik Langsung" belum pernah dipublikasikan dan belum pernah diikutsertakan dalam perlombaan apapun sebelumnya serta tidak mengandung unsur plagiat di dalamnya.

Apabila dikemudian hari pada naskah saya tersebut diketemukan unsur yang tidak sesuai dengan surat pernyataan ini, maka saya bersedia menerima konsekuensi hukum sesuai dengan peraturan perundang-undangan yang berlaku.

Jakarta, 10 Juli 2023

Yang menyatakan,

Syamsul Arifin
NIM 1910511055

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan di bawah ini:

Nama : Syamsul Arifin
NIM : 1910511055
Fakultas : Ilmu Komputer
Program Studi : S1 Informatika

Demi pembangunan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas royalty Non ekslusif (*Non-exlusive Royalty Free Right*) atas karya ilmiah saya berjudul:

ANALISIS BUKTI FORENSIK DIGITAL PENIPUAN TRANSAKSI ONLINE PADA LINE MESSENGER MENGGUNAKAN METODE FORENSIK LANGSUNG

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menympan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasi Skripsi saya selama tetap mencantumkan nama saya sebagai penulis Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta
Pada tanggal : 12 Juli 2023

Yang Menyatakan,

(Syamsul Arifin)

LEMBAR PENGESAHAN

Tugas Akhir ini diajukan oleh:

Nama	: Syamsul Arifin
NIM	: 1910511055
Program Studi	: S1 Informatika
Judul Tugas Akhir	: Analisis Bukti Forensik Digital Penipuan Transaksi Online Pada Line Messenger Menggunakan Metode Forensik Langsung

Telah berhasil dipertahankan dihadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana pada Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.

Dr. Tjahjanto, S.Kom., M.M.
Penguji I

Yuni Widiastiwi, S.Kom. ,M.Si
Penguji II

Henki Bayu Seta, S.Kom, MTI.
Pembimbing

Dr. Ermatita, M.Kom.
Dekan

Dr. Widya Cholil, M.I.T.
Kepala Program Studi

Ditetapkan di : Jakarta
Tanggal Ujian : 10 Juli 2023

ANALISIS BUKTI FORENSIK DIGITAL

PENIPUAN TRANSAKSI *ONLINE* PADA LINE MESSENGER

MENGGUNAKAN METODE FORENSIK LANGSUNG

SYAMSUL ARIFIN

ABSTRAK

Perkembangan teknologi komputer semakin pesat, hal ini berbanding lurus dengan peningkatan kejahatan di dunia maya. Salah satu contohnya adalah kasus penipuan dalam transaksi *online* yang kerap terjadi. Penipuan semacam ini dapat terjadi pada aplikasi populer bernama LINE Messenger, yang merupakan aplikasi pesan instan multiplatform berbasis *cloud*, gratis, dan non-profit. LINE tersedia untuk berbagai sistem operasi seperti Android, iOS, Windows Phone, Ubuntu Touch, serta dapat diakses melalui perangkat komputer seperti Windows, MacOS X, dan Linux. Melalui aplikasi LINE, pengguna dapat bertukar pesan teks, foto, video, audio, dokumen, stiker, dan berbagai jenis berkas lainnya.

Setiap aplikasi yang berjalan pada komputer meninggalkan jejak data dan informasi di dalam *volatile memory*, yang umumnya dikenal sebagai Random Access Memory (RAM). Data dan informasi yang tersimpan dalam RAM dapat diperoleh melalui teknik forensik digital yang dikenal sebagai "*live forensics*". *Live forensics* atau forensik langsung merupakan metode penyelidikan di mana proses pengumpulan bukti dilakukan saat komputer atau perangkat pelaku masih aktif digunakan. Dalam konteks penelitian ini, tujuannya adalah untuk mengidentifikasi bukti digital yang terkait dengan kasus penipuan transaksi online yang terdapat pada *volatile memory* (RAM) dan juga disk pada mesin.

Untuk mencapai tujuan tersebut, digunakan alat forensik yang disebut FTK Imager dan WinHex. Alat-alat ini mampu mengambil dan menganalisis data dan informasi yang tersimpan dalam RAM. Hasil penelitian ini berupa analisis dari bukti digital yang terkait dengan percakapan, yang dapat menjadi bukti yang signifikan dalam mengungkap kasus kejahatan transaksi online yang terjadi.

Kata kunci*:* *Forensik Digital, Forensik Langsung, LINE, Bukti Digital, Cybercrime, Volatile, Memory, Virtual Machine, Windows OS*

DIGITAL FORENSIC EVIDENCE ANALYSIS

ONLINE TRANSACTION FRAUD ON LINE MESSENGER

USING LIVE FORENSIC METHOD

SYAMSUL ARIFIN

ABSTRACT

The rapid development of computer technology is parallel to the increase in cybercrime. One example is the occurrence of fraud in online transactions. Such fraud can happen on the popular application called LINE Messenger, which is a multi-platform cloud-based instant messaging application that is free and non-profit. LINE is available for various operating systems such as Android, iOS, Windows Phone, Ubuntu Touch, and can also be accessed through computer devices like Windows, MacOS X, and Linux. Through the LINE application, users can exchange text messages, photos, videos, audios, documents, stickers, and various other file types.

Every application running on a computer leaves behind traces of data and information in volatile memory, commonly known as Random Access Memory (RAM). Data and information stored in RAM can be obtained through a digital forensic technique known as "live forensics." Live forensics is an investigation method where the evidence collection process takes place while the perpetrator's computer or device is still actively in use. In the context of this research, the aim is to identify digital evidence related to cases of online transaction fraud found in volatile memory (RAM) and also on the disk of the machine.

To achieve this goal, forensic tools called FTK Imager and WinHex are used. These tools are capable of retrieving and analyzing data and information stored in RAM. The results of this research consist of an analysis of digital evidence related to conversations, which can serve as significant evidence in uncovering cases of online transaction fraud.

***Keywords**: Digital Forensics, Live Forensics, LINE, Digital Evidence, Cybercrime, Volatile Memory, Virtual Machine, Windows OS*

KATA PENGANTAR

Puji dan syukur dipanjatkan atas kehadirat Allah SWT. karena atas karunia-Nya peneliti dapat menyelesaikan Tugas Akhir dengan baik.

Dalam penyelesaian Tugas Akhir ini tidak lepas dari bantuan banyak pihak yang telah memberikan bantuan dan dukungan. Untuk itu peneliti mengucapkan banyak terima kasih kepada:

1. Dr. Ermatita, M.Kom., selaku dekan Fakultas Ilmu Komputer.
2. Dr. Widya Cholil, M.I.T. selaku Ketua Program Studi Sarjana Jurusan Informatika.
3. Henki Bayu Seta, S.Kom, MTI. selaku Dosen Pembimbing.
4. Kedua orang tua yang telah memberikan dukungan baik secara moral maupun materil.
5. Semua teman-teman saya yang telah memberikan dukungan dan semangat dalam penyelesaian skripsi ini.
6. Dan semua pihak yang tidak dapat peneliti sebutkan satu persatu tanpa mengurangi rasa hormat.

Peneliti menyadari bahwa masih banyaknya kekurangan secara materi maupun teknik penulisan dari Tugas Akhir ini, mengingat kurangnya pengetahuan dan pengalaman peneliti. Oleh karena itu, kritik dan saran yang membangun akan sangat berarti bagi peneliti.

Jakarta, 6 Juni 2022

Peneliti,

Syamsul Arifin

DAFTAR ISI

DAFTAR GRAFIK

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

CPU	Central Processing Unit
ESI	Electronic Stored Information
FTK	Forensic ToolKit
GB	Gigabyte
GHz	Gigahertz
GPU	Graphics Processing Unit
HDD	Hard Disk Drive
ID	Identification/Identity
IM	Instant Messaging
IoT	Internet of Things
LNK	Link (shortcut) file
NIJ	National Institute of Justice
OS	Operating System
PDF	Portable Document Format
RAM	Random Access Memory
SMS	Short Message Service
TB	Terabyte
TM	Trademark
UWP	Universal Windows Platform
USB	Universal Serial Bus