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*