

## Analisis Keamanan Data pada Aplikasi Chatting Menggunakan Metode Network Forensics

Reben Yulandra Agustian<sup>1\*</sup>, Tata Sutabri<sup>2</sup>  
<sup>1,2</sup> Universitas Binadarma, Indonesia

Alamat: Jl. Jenderal Ahmad Yani No.3, 9/10 Ulu, Kecamatan Seberang Ulu 1, Kota Palembang,  
Sumatera Selatan 30111

Korespondensi penulis : [rebenn02@gmail.com](mailto:rebenn02@gmail.com) \*

**Abstract,** *This study aims to analyze data security in popular chat applications using network forensics methods. This method enables the collection and analysis of data from networks to detect and understand potential threats or security breaches. In this research, several chat applications are analyzed to identify vulnerabilities that unauthorized parties could exploit. The results of this study are expected to provide a better understanding of the steps that can be taken to enhance data security in chat applications.*

**Keywords;** *Data Security, Chat Applications, Network Forensics, Network Analysis, Security Threats*

**Abstrak,** Penelitian ini bertujuan untuk menganalisis keamanan data pada aplikasi chatting populer menggunakan metode network forensics. Metode ini memungkinkan pengumpulan dan analisis data dari jaringan untuk mendeteksi dan memahami potensi ancaman atau pelanggaran keamanan. Dalam penelitian ini, beberapa aplikasi chatting dianalisis untuk mengidentifikasi kelemahan yang dapat dimanfaatkan oleh pihak tak berwenang. Hasil penelitian ini diharapkan memberikan pemahaman yang lebih baik tentang langkah- langkah yang dapat diambil untuk meningkatkan keamanan data pada aplikasi chatting.

**Kata Kunci;** Keamanan Data, Aplikasi Chatting, Network Forensics, Forensik Jaringan, Ancaman Keamanan

### 1. PENDAHULUAN

Kemajuan teknologi informasi telah mengubah cara komunikasi masyarakat dengan cepat. Salah satu alat komunikasi paling populer adalah aplikasi chatting yang digunakan untuk komunikasi pribadi maupun profesional. Namun, data yang dikirimkan melalui aplikasi ini rentan terhadap serangan siber seperti man-in-the-middle attacks, data interception, dan peretasan. (Sumber: Daulay C Indrayani, 2022).

Menurut data Badan Siber dan Sandi Negara (BSSN), insiden kejahatan siber di Indonesia terus meningkat, terutama pada aplikasi komunikasi digital. Studi ini bertujuan untuk menganalisis keamanan data pada aplikasi chatting menggunakan metode network forensics dan mengidentifikasi langkah-langkah yang diperlukan untuk meningkatkan keamanan data.

### 2. METODE

Penelitian ini menggunakan metode network forensics , yang mencakup beberapa langkah sebagai berikut:

1. Identifikasi : Menentukan jenis data yang akan dijelaskan dan alat yang diperlukan.

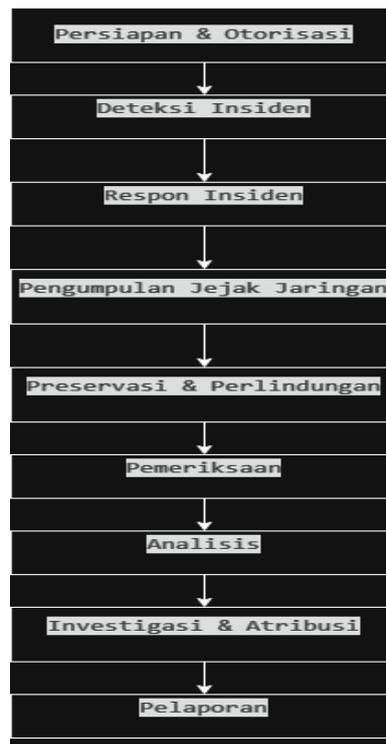
2. Pengumpulan Data : Mengumpulkan data dari lalu lintas jaringan aplikasi chatting menggunakan alat seperti Wireshark.
3. Pemeriksaan : Menganalisis data yang dikumpulkan untuk menemukan pola atau anomali.
4. Analisis : Mengevaluasi hasil pemeriksaan untuk mengidentifikasi potensi ancaman.
5. Pelaporan : Menyusun laporan yang menjelaskan temuan dan rekomendasi.

### 3. HASIL DAN PEMBAHASAN

Hasil analisis menunjukkan bahwa beberapa aplikasi chatting menggunakan enkripsi untuk melindungi data pengguna, namun celah keamanan tetap ada. Misalnya, pengujian terhadap aplikasi WhatsApp menunjukkan bahwa meskipun pesan terenkripsi, metadata masih dapat diakses oleh penyusup.

**Tabel 1 di bawah ini menunjukkan ringkasan hasil pengujian keamanan pada beberapa aplikasi chatting:**

Aplikasi	Enkripsi	Kerentanan
Ada apa	Ya	Metadata dapat diakses
Telegram	Ya	Serangan Man-in-the-Middle (MitM)
Sinyal	Ya	Potensi serangan phishing



**Gambar 1 Diagram Alur Proses Forensik Jaringan**

#### **4. KESIMPULAN**

Analisis keamanan data pada aplikasi chatting dengan metode network forensics memberikan wawasan penting tentang kerentanan yang ada. Meskipun enkripsi digunakan untuk melindungi komunikasi, pengguna tetap harus waspada terhadap potensi ancaman lain seperti metadata pencurian dan serangan MitM. Rekomendasi untuk meningkatkan keamanan termasuk penggunaan VPN dan kesadaran akan melakukan praktik keamanan siber.

#### **DAFTAR PUSTAKA**

Tata, Sutabri. (2013). Pengantar Teknologi Informasi. Yogyakarta: ANDI.

Tata, Sutabri. (201G). Sistem Informasi Bisnis. Yogyakarta:ANDI.

Tata, sutabri. (2012). Konsep Sistem Informasi. Yogyakarta:ANDI.

Purnama, A., & Putri, ND (2023). "Keamanan Data dalam Aplikasi Digital." Jurnal Teknologi Informasi.

BSSN (Badan Siber dan Sandi Negara). (2023). "Laporan Keamanan Siber Indonesia."

Dokumentasi Wireshark. (2023). "Forensik Jaringan dengan Wireshark."

- Ahmadi, A.-. (2018). "Akuisisi Data Forensik Google Drive pada Android dengan Metode National Institute of Justice (NIJ)." *Jurnal CoreIT: Jurnal Hasil Penelitian Ilmu Komputer Dan Teknologi Informasi*, 4(1), 8.
- Daulay, Z. S., s Indrayani, R. (2022). "Analisis Keamanan Browser dalam Bersosial Media Menggunakan Metode NIJ." *Djtechno: Jurnal Teknologi Informasi*, 3(2), 167– 175.
- Hafizh, M. N., Riadi, I., s Fadlil, A. (2020). "Forensik Jaringan Terhadap Serangan ARP Spoofing Menggunakan Metode Live Forensic." *Jurnal Telekomunikasi Dan Komputer*, 10(2), 111.
- Putri, A. S., s Zakaria, R. (2020). "Analisis Pemetaan e-commerce Terbesar di Indonesia Berdasarkan Model Kekuatan Ekonomi Digital." *Seminar Dan Konferensi Nasional IDEC*, 1(November), 1–14