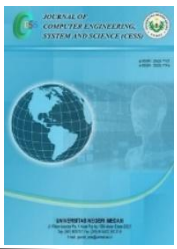
*CESS (Journal of Computer Engineering, System and Science)*
*Vol. 10, No. 2, Juli 2025, pp.448-456*

1

**CESS**
**(Journal of Computer Engineering, System and Science)**
Available online: https://jurnal.unimed.ac.id/2012/index.php/cess
ISSN: 2502-714x (Print) | ISSN: 2502-7131 (Online)



# Analisis Keamanan Enkripsi End-To-End Pada Aplikasi WhatsApp Untuk Menanggulangi Ancaman Kriminalitas *Siber* Menggunakan *Burp Suite*

## *Analysis of End-to-End Encryption Security on WhatsApp Application to Counter Cybercrime Threats Using Burp Suite*

**Hana Meylia Nurohmah[1*], Fahmi Fachri[2]**

*[1,2]Program Studi Teknik Informatika, Universitas Ma'arif Nahdlatul Ulama, Kebumen*
*Jalan Kutorjo Km.05 Jatisari Kebumen*
*Email: [1]hanakebumen21@gmail.com, [2]fahmifachriumnu@gmail.com*
**Corresponding Author*

**A B S T R A K**

Penelitian ini bertujuan untuk mengevaluasi efektivitas sistem enkripsi end-to-end (E2EE) pada aplikasi WhatsApp dalam melindungi komunikasi pengguna dari potensi intersepsi data. Pengujian dilakukan melalui metode penetration testing dengan menggunakan *Burp Suite Community Edition*, difokuskan pada lalu lintas jaringan dalam tiga skenario pengujian: komunikasi teks satu arah, komunikasi dua arah, dan pengiriman file media. Setiap skenario diuji sebanyak satu kali pada dua perangkat Android serta laptop sebagai perantara analisis jaringan yang terhubung melalui jaringan lokal dengan konfigurasi proxy aktif. Hasil pengujian menunjukkan bahwa metadata komunikasi seperti alamat IP, host server, dan jenis permintaan protokol berhasil ditangkap oleh alat, tetapi isi pesan tetap tidak dapat diakses dalam bentuk plaintext. Hal ini menunjukkan bahwa WhatsApp telah mengimplementasikan sistem E2EE secara efektif, sehingga mampu mencegah intersepsi isi komunikasi meskipun lalu lintas data terpantau. Keterbatasan penelitian ini terletak pada cakupan alat dan jaringan yang digunakan, tanpa *bypass certificate pinning* atau analisis mendalam terhadap sisi klien. Oleh karena itu, disarankan agar penelitian lanjutan menggunakan tools lanjutan seperti *Frida* atau *Wireshark* dan mencakup analisis terhadap potensi kebocoran metadata dan keamanan *endpoint*. Temuan ini diharapkan dapat menjadi referensi dalam evaluasi keamanan aplikasi pesan instan serta meningkatkan kesadaran pengguna terhadap pentingnya perlindungan privasi digital.

**Kata kunci:** *WhatsApp; end-to-end encryption; Burp Suite; penetration testing; metadata; keamanan aplikasi; privasi digital.*

**A B S T R A C T**
This study aims to evaluate the effectiveness of the end-to-end encryption (E2EE) system in the WhatsApp application in protecting user communications from potential data interception. Testing was conducted using penetration testing using Burp Suite Community Edition, focusing on network traffic in three test scenarios: one-way text communication, two-way communication, and media file delivery. Each scenario was tested once on two Android and laptop as an intermediary for connected over a local network with an active proxy configuration. The test results showed that communication metadata such as IP addresses, server hosts, and protocol request types were successfully captured by the tool, but the message content remained inaccessible in plaintext. This indicates that WhatsApp has implemented an effective E2EE system, thus preventing interception of communication content even though data traffic was monitored. The limitations of this study lie in the scope of the tool and network used, without bypassing certificate pinning or in-depth client-side analysis. Therefore, further research using advanced tools such as Frida or Wireshark is recommended, including analysis of potential metadata leaks and endpoint security. These findings are expected to serve as a reference in evaluating the security of instant messaging applications and raise user awareness of the importance of digital privacy protection.

**Keywords***: WhatsApp; end-to-end encryption; Burp Suite; penetration testing; metadata; application security; digital privacy.*

## 1. PENDAHULUAN

Dalam era komunikasi digital yang serba cepat, keamanan informasi pribadi menjadi isu yang semakin krusial. Aplikasi pesan instan seperti WhatsApp telah mengadopsi teknologi *end-to-end encryption* (E2EE) untuk menjamin bahwa hanya pengirim dan penerima yang dapat membaca isi pesan. Namun, berbagai insiden keamanan menunjukkan bahwa proteksi enkripsi saja tidak selalu cukup untuk menjamin kerahasiaan data. Salah satu kasus paling kontroversial adalah penyalahgunaan spyware Pegasus oleh NSO Group, yang mengeksploitasi celah zero-click pada WhatsApp untuk memantau perangkat tanpa sepengetahuan pengguna [12]. Studi lain juga mencatat aktivitas serupa oleh kelompok bernama Paragon, yang memanfaatkan kerentanan sisi klien untuk mengakses komunikasi terenkripsi. Kedua kasus tersebut menyoroti fakta bahwa sekalipun E2EE diterapkan, sistem tetap rentan terhadap intersepsi atau manipulasi di titik akhir (*endpoint*) [5]. Meskipun WhatsApp telah mengklaim kepatuhan terhadap protokol keamanan modern, pertanyaan tetap muncul: sejauh mana komunikasi dalam aplikasi ini benar-benar aman dari intersepsi jaringan, terutama pada level permukaan seperti metadata? Sejumlah studi sebelumnya [7][2] telah membahas konsep E2EE pada WhatsApp, namun sebagian besar hanya bersifat deskriptif tanpa melakukan simulasi teknis yang mendalam terhadap lalu lintas data menggunakan alat penetration testing. Selain itu, studi yang ada jarang mengungkap secara eksplisit apakah metadata komunikasi masih dapat diakses, atau bagaimana tools analisis jaringan seperti *Burp Suite* dapat mengungkap potensi celah privasi non-konten.

Penelitian ini hadir untuk mengisi celah tersebut dengan pendekatan eksperimental menggunakan *Burp Suite Community Edition* sebagai alat utama untuk mengintersepsi dan menganalisis lalu lintas komunikasi WhatsApp dalam berbagai skenario pengujian. Tidak seperti studi sebelumnya yang hanya membahas prinsip kriptografi, studi ini menyelidiki

secara langsung seberapa jauh komunikasi terenkripsi dapat diamati melalui teknik pengujian penetrasi sederhana. Dengan demikian, penelitian ini tidak hanya mengonfirmasi efektivitas E2EE, tetapi juga menyoroti risiko potensial dari metadata yang masih terbuka di lapisan permukaan jaringan [7]. Secara khusus, tujuan dari penelitian ini adalah untuk:

1. Menguji apakah lalu lintas WhatsApp dapat diintersepsi menggunakan Burp Suite,
2. Menentukan sejauh mana informasi sensitif (konten atau metadata) dapat terungkap dalam skenario jaringan terkendali,
3. Menilai efektivitas enkripsi end-to-end dari sudut pandang teknis, bukan hanya deklaratif.

Dengan pendekatan eksperimental dan pengamatan langsung terhadap lalu lintas data, penelitian ini diharapkan memberikan kontribusi nyata dalam mengevaluasi tingkat keamanan praktis dari sistem E2EE WhatsApp dan memperkaya diskusi akademik tentang privasi digital dalam konteks teknis dan aktual.

## 2. METODE PENELITIAN

### 2.1. Pendekatan dan Jenis Penelitian

Penelitian ini menggunakan pendekatan kualitatif eksperimental yang bertujuan untuk mengevaluasi sejauh mana sistem *end-to-end encryption* (E2EE) pada WhatsApp mampu melindungi komunikasi pengguna dari intersepsi jaringan. Fokus utama ditujukan pada pengamatan langsung lalu lintas komunikasi dengan bantuan alat Burp Suite melalui konfigurasi jaringan lokal yang terkendali.

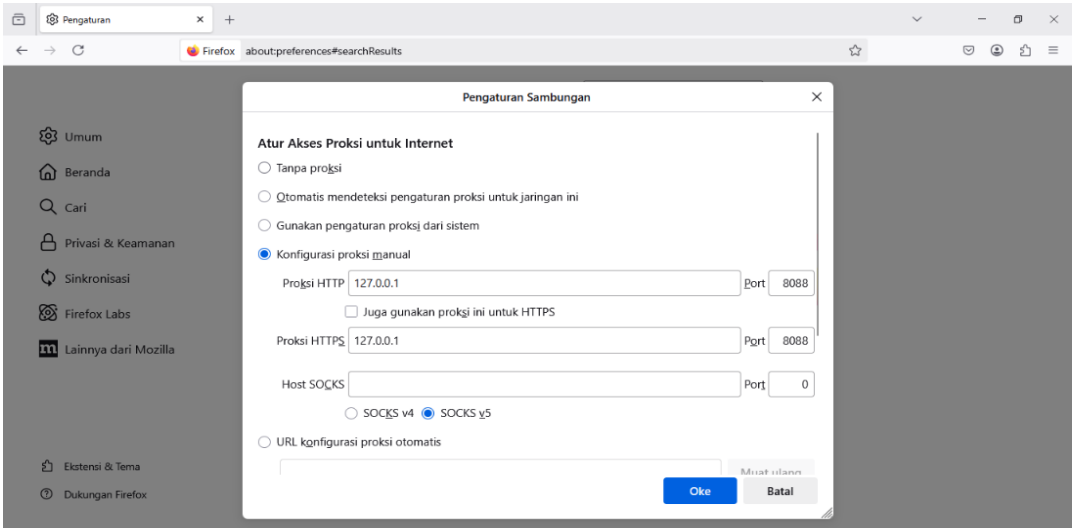
### 2.2. Lingkungan dan Alat Penelitian

Tabel 1. Lingkungan dan Alat Penelitian

| Komponen | Spesifikasi |
|---|---|
| Laptop Proxy | Windows 11, Intel Core i5 Gen-10, RAM 8 GB |
| Perangkat | Android & laptop acer windows 11 (dua perangkat) |
| Aplikasi WhatsApp | Melalui whatsapp web |
| Burp Suite | Burp Suite Community Edition v2023.9.2 |
| Jaringan | Wi-Fi lokal (closed network), proxy aktif port 8088 |
| Sertifikat Burp CA | Diinstal manual ke perangkat Android via pengaturan keamanan & VPN |

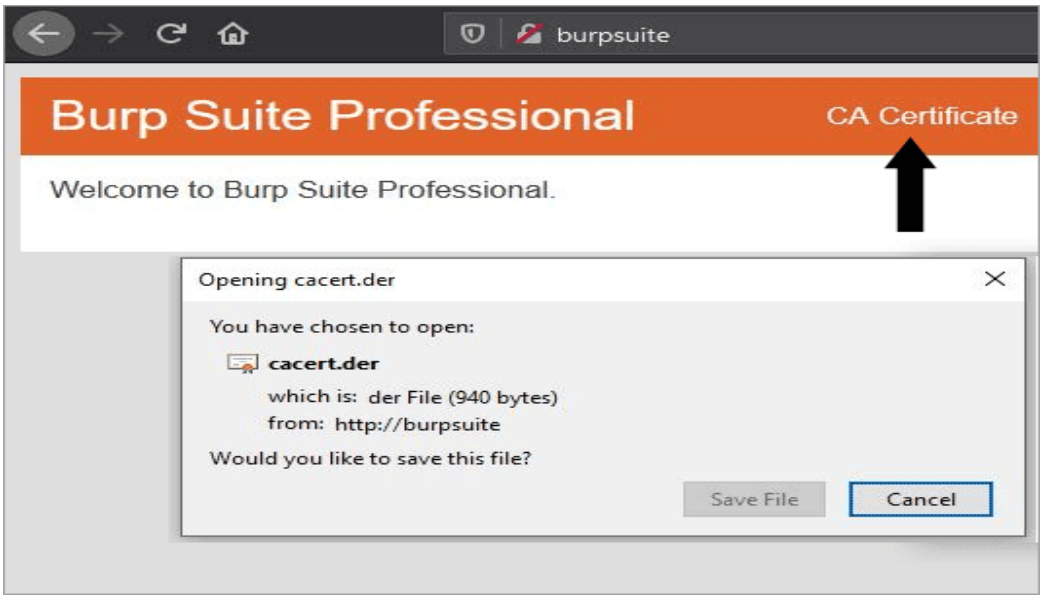
### 2.3. Langkah dan Prosedur Eksperimen

1. Instalasi & Konfigurasi Burp Suite
   - Unduh dan pasang Burp Suite v2023.9.2 Community Edition di laptop Windows.
   - Atur intercept proxy listener di port 8088.




Gambar 1. Instalasi dan Konfigurasi Burp Suite

2. Konfigurasi Perangkat Android
   - Atur proxy Wi-Fi agar diarahkan ke 450cenar IP laptop (192.168.1.100:8088).
   - Unduh dan pasang sertifikat CA dari Burp Suite melalui browser perangkat.
   - Tambahkan sertifikat melalui menu *Pengaturan > Keamanan > Instal Sertifikat* (format .cer).



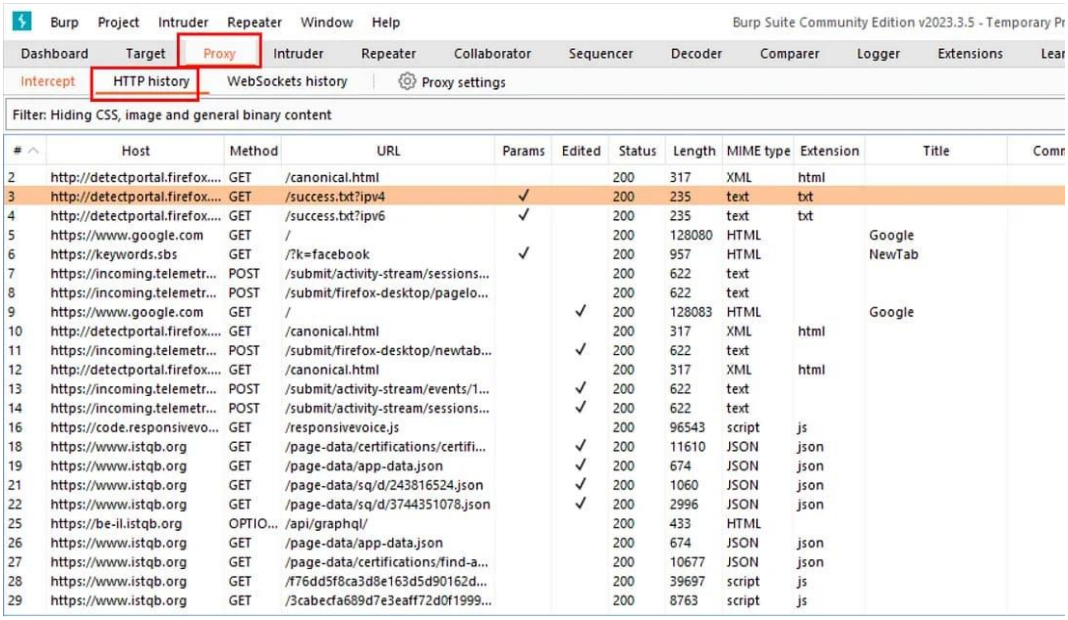

Gambar 2. Sertifikat Burp Suite

3. Simulasi Skenario Pengujian WhatsApp
   Tiga skenario dilakukan sebagai berikut:

Tabel 2. Scenario Pengujian WhatsApp

| No | Skenario | Deskripsi Aktivitas |
|---|---|---|
| 1 | Pesan Teks Satu Arah | Pengguna A mengirim pesan ke pengguna B |
| 2 | Komunikasi Dua Arah | A dan B saling bertukar pesan secara interaktif |
| 3 | Pengiriman File Media | A mengirim gambar dan PDF ke B melalui WhatsApp |

4. Pengamatan dan Dokumentasi
   - Aktifkan *Intercept is off* di Burp untuk mode *pass-through.*
   - Amati semua *log* komunikasi di tab *HTTP history*.
   - Simpan *log* tangkapan data dan tanggapan server.




Gambar 3. Riwayat HTTP(S) Burp Suite

5. Parameter Uji dan Kriteria Keberhasilan

Tabel 3. Skenario dan Parameter Uji Keberhasilan

| No | Skenario Pengujian | Teknik yang Digunakan | Parameter Uji | Kriteria Keberhasilan |
|---|---|---|---|---|
| 1 | Intersepsi Data (MitM) | Intercept Proxy (HTTPs capture) | Dapatkah traffic komunikasi dibaca? | Tidak ada isi pesan terbaca/terdekripsi |
| 2 | Manipulasi Permintaan | Request Modifying Tool | Respons server terhadap permintaan modifikasi | Permintaan ditolak atau tidak berhasil |
| 3 | Observasi Proses Enkripsi | Packet Sniffing & TLS Analysis | Apakah proses handshake atau key exchange terlihat? | Tidak ditemukan kunci enkripsi yang terekspos |

6. Jenis Data yang Dihasilkan
   - Log metadata komunikasi: IP server, waktu, ukuran payload, jenis permintaan (GET, POST)
   - Header TLS/HTTPS: Informasi cipher suite, port, handshake
   - Catatan kegagalan decoding konten: Konten tetap terenkripsi dan tidak terbaca oleh Burp Suite
   - Screenshots dan export log file dari Burp sebagai dokumentasi hasil
7. Batasan Eksperimen
   - *Certificate pinning* WhatsApp tidak dapat dilewati dengan Burp Suite.
   - Tidak dilakukan *rooting* pada perangkat Android, sehingga akses terhadap sistem file atau *reverse engineering* tidak dilakukan.
   - Hanya dilakukan di jaringan lokal yang terkendali, belum menguji serangan pada jaringan publik.

## 3. HASIL DAN PEMBAHASAN

### 3.1. Hasil Pengujian

Pengujian dilakukan pada tiga skenario komunikasi WhatsApp: pengiriman pesan teks satu arah, komunikasi dua arah, dan pengiriman file media (gambar dan dokumen). Berikut adalah ringkasan hasil pengamatan dari setiap skenario.

Tabel 4. Ringkasan Hasil Pengamatan Intersepsi Komunikasi WhatsApp

| Skenario | Metadata Terbaca | Konten Terenkripsi | Header HTTPS Terbaca | Isi Pesan Terlihat |
|---|---|---|---|---|
| Pesan teks satu arah | Ya | Ya | Ya | Tidak |
| Komunikasi dua arah | Ya | Ya | Ya | Tidak |
| Pengiriman file media | Ya | Ya | Ya | Tidak |

Tabel 5. Indikator Pengujian Teknis

| Parameter | Nilai |
|---|---|
| Total skenario diuji | 3 |
| Jumlah intersepsi konten berhasil | 0/3 (0%) |
| Jumlah metadata berhasil dibaca | 3/3 (100%) |
| Rata-rata ukuran payload | Teks: ±0.5–2 KB; File media: ±100–300 KB |
| Keberhasilan bypass TLS pinning | Tidak berhasil (0%) |
| Status sertifikat Burp | Ditanam secara manual, tetap ditolak WhatsApp |

Pada ketiga skenario, Burp Suite berhasil menangkap metadata komunikasi seperti alamat IP server WhatsApp, timestamp, jenis request (GET/POST), ukuran payload, serta domain tujuan. Namun, isi pesan atau file yang dikirim tetap tidak dapat ditampilkan dalam bentuk plaintext. Burp Suite tidak mampu mendekripsi isi komunikasi karena lalu lintas dilindungi *oleh Transport Layer Security* (TLS) dan *end-to-end encryption* (E2EE) WhatsApp.

Log komunikasi yang ditampilkan pada tab "HTTP History" Burp Suite menunjukkan banyak permintaan HTTPS yang dienkripsi sepenuhnya. Selain itu, setiap payload dan respons server berada dalam format binari atau kode hexadecimal yang tidak terbaca, mempertegas keberadaan sistem enkripsi yang aktif.

### 3.2. Analisis Hasil

Hasil tersebut menunjukkan bahwa sistem E2EE yang diterapkan WhatsApp berjalan dengan baik dalam mencegah intersepsi isi komunikasi melalui teknik *man-in-the-middle* dasar. Meskipun Burp Suite mampu bertindak sebagai proxy dan menangkap lalu lintas data, semua konten utama seperti pesan teks dan file tetap terenkripsi. Hal ini konsisten dengan arsitektur WhatsApp yang menggunakan protokol *Signal Protocol*, di mana kunci enkripsi hanya disimpan pada perangkat pengguna.

Namun, metadata seperti alamat server, waktu komunikasi, dan besar data tetap dapat diakses. Ini menunjukkan adanya potensi eksploitasi privasi melalui analisis lalu lintas. Pihak ketiga masih bisa membangun profil perilaku pengguna tanpa harus membaca isi pesan. Misalnya, dari waktu komunikasi dan ukuran payload, seseorang dapat memperkirakan kapan pengguna aktif dan jenis komunikasi apa yang sedang terjadi (teks pendek atau file besar).

### 3.3. Diskusi terhadap Efektivitas E2EE

*Burp Suite Community Edition* adalah alat penetration testing berbasis proxy yang handal untuk intersepsi HTTP/HTTPS. Namun, keterbatasan fungsionalnya membuatnya tidak optimal untuk pengujian terhadap aplikasi dengan keamanan tingkat lanjut seperti WhatsApp. Fitur seperti *certificate pinning dan obfuscation library* pada WhatsApp membuat Burp gagal melakukan intersepsi isi pesan.

Studi oleh [16] menyarankan penggunaan *Frida atau objection* untuk *bypass certificate pinning* serta akses ke log sisi klien. Selain itu, *Wireshark* lebih cocok untuk analisis granular terhadap lalu lintas real-time pada layer transport, meskipun tetap tidak mampu membaca konten terenkripsi E2EE.

Dengan demikian Burp Suite cocok untuk simulasi *man-in-the-middle* (MITM) di layer permukaan, namun tidak cukup untuk *bypass proteksi* tingkat klien, sehingga membatasi kedalaman analisis yang bisa dicapai dalam studi ini.

### 3.4. Keterbatasan Teknik Pengujian

Beberapa batasan dalam eksperimen ini perlu dicatat:

- *Burp Suite Community Edition* tidak memiliki fitur advanced seperti bypass TLS pinning, sehingga tidak memungkinkan intersepsi lalu lintas pada aplikasi dengan proteksi tambahan.
- Perangkat Android tidak di-root, sehingga tidak memungkinkan eksplorasi keamanan di sisi klien, seperti penyimpanan lokal atau *reverse engineering* aplikasi.
- Uji dilakukan di jaringan lokal, sehingga tidak merepresentasikan skenario ancaman pada jaringan publik atau jaringan tidak aman.

### 3.5. Implikasi Temuan

Meskipun konten pesan aman, metadata tetap terbuka dan dapat menjadi celah dalam privasi pengguna. Oleh karena itu, perlindungan keamanan tidak cukup hanya mengandalkan E2EE. Pengguna perlu:

- Menghindari penggunaan jaringan Wi-Fi publik tanpa perlindungan VPN.
- Mengaktifkan autentikasi dua faktor.

- Tidak menggunakan aplikasi WhatsApp modifikasi atau tidak resmi.
- Meningkatkan literasi keamanan digital.

### 3.6. Perbandingan dengan Studi Serupa

Penelitian ini memperkuat temuan dari Alamsyah dkk yang juga menyimpulkan bahwa isi pesan WhatsApp tidak dapat diakses menggunakan Burp Suite meskipun metadata berhasil ditangkap [2]. Namun, studi ini memperluas skenario uji hingga mencakup pengiriman file media, yang belum dikaji secara teknis dalam penelitian mereka.

Sementara itu**,** Fajri (2021) hanya menyajikan kajian teoretis mengenai E2EE pada WhatsApp, tanpa eksperimen langsung [7]. Dengan demikian, penelitian ini memberikan kontribusi baru berupa simulasi teknis nyata pada jaringan terkendali, serta dokumentasi struktur data terenkripsi yang ditangkap selama uji.

Sistem enkripsi end-to-end (E2EE) pada WhatsApp terbukti sangat efektif dalam mencegah intersepsi isi pesan, baik teks maupun file, dalam skenario pengujian berbasis jaringan lokal. Seluruh konten komunikasi dienkripsi sepenuhnya, dan tidak ada payload yang dapat dibaca dalam bentuk plaintext.

Metadata komunikasi tetap dapat diakses, termasuk alamat IP, domain server, ukuran payload, serta waktu komunikasi, yang dapat dimanfaatkan untuk profiling pengguna.
Burp Suite CE terbukti memiliki keterbatasan dalam menembus proteksi TLS dan certificate pinning WhatsApp. Diperlukan tools lanjutan seperti Frida atau Wireshark untuk eksplorasi sisi klien secara lebih dalam.

Studi ini memperluas cakupan pengujian yang sebelumnya hanya bersifat teoretis, dengan menambahkan pendekatan praktis dan analisis kualitatif atas hasil uji komunikasi real.

## 4. KESIMPULAN

Sistem enkripsi end-to-end (E2EE) yang diterapkan WhatsApp terbukti efektif dalam mencegah intersepsi isi pesan. Selama proses pengujian, tidak ditemukan konten pesan dalam bentuk plaintext, baik pada komunikasi satu arah, dua arah, maupun pengiriman file media. Burp Suite hanya mampu menangkap metadata komunikasi, seperti alamat IP server, domain tujuan, *timestamp*, dan ukuran *payload*. Hal ini menunjukkan bahwa meskipun konten pesan dilindungi, data pendukung di sekitar komunikasi masih dapat diamati dan berpotensi dimanfaatkan untuk profiling pengguna. Pengujian menggunakan *Burp Suite Community Edition* tidak berhasil menembus certificate pinning atau enkripsi TLS, sehingga lalu lintas data tetap tidak dapat didekripsi. Ini mengindikasikan bahwa WhatsApp memiliki lapisan perlindungan berlapis yang tangguh, baik pada tingkat protokol aplikasi maupun transport. Penggunaan metode penetration testing berbasis observasi jaringan berhasil memberikan gambaran teknis praktis tentang keamanan komunikasi, khususnya pada lapisan *surface-level*. Namun, karena keterbatasan alat dan pengujian tidak dilakukan pada tingkat endpoint (perangkat pengguna), maka penelitian ini belum menyentuh aspek kerentanan dari sisi dalam aplikasi atau sistem operasi. Keamanan komunikasi digital tidak hanya ditentukan oleh teknologi enkripsi, tetapi juga oleh perilaku dan kewaspadaan pengguna. Oleh karena itu, penggunaan jaringan aman, pemahaman terhadap ancaman digital, dan pemanfaatan fitur keamanan tambahan sangat penting untuk menjaga privasi data secara menyeluruh.

Penelitian ini memiliki beberapa keterbatasan teknis dan metodologis yang perlu dicatat sebagai bahan evaluasi yaitu versi dari Burp Suite tidak menyediakan fitur untuk *bypass certificate pinning* yang diterapkan oleh WhatsApp. Hal ini membatasi kemampuan pengujian

terhadap komunikasi terenkripsi secara lebih dalam, penelitian ini tidak mencakup eksplorasi sisi klien (perangkat Android), seperti *reverse engineering* aplikasi atau analisis memori perangkat, yang berpotensi membuka titik lemah sistem di luar protokol komunikasi; Eksperimen hanya dilakukan dalam jaringan Wi-Fi tertutup dan terkendali. Oleh karena itu, hasilnya belum mewakili risiko komunikasi dalam lingkungan jaringan publik atau tidak aman, seperti hotspot umum. Penelitian hanya mencakup tiga jenis skenario komunikasi sederhana dan belum menyertakan skenario komunikasi grup, panggilan suara/video, atau integrasi dengan layanan pihak ketiga.

Untuk meningkatkan kontribusi ilmiah dan pemahaman teknis terhadap sistem keamanan E2EE pada aplikasi perpesanan, disarankan menggunakan tools lanjutan seperti Frida atau Magisk untuk bypass certificate pinning, serta melakukan analisis endpoint pada perangkat yang di-root guna mengidentifikasi kelemahan sisi klien. Pengujian juga perlu diperluas mencakup fitur kompleks seperti grup, pesan suara, video call, dan lainnya. Pendekatan penetration testing dapat dikombinasikan dengan analisis forensik untuk menilai potensi kebocoran data. Selain itu, studi komparatif antar aplikasi dan pengembangan threat modelling khusus E2EE disarankan untuk evaluasi keamanan yang lebih sistematis.

## DAFTAR PUSTAKA

[1] Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., ... & Schneier, B. (2015). Keys under doormats: Mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity, 1*(1), 69–79.

[2] Alamsyah, M., & Rahman, F. (2021). Analisis keamanan enkripsi end-to-end pada aplikasi WhatsApp menggunakan metode penetration testing. *Jurnal Teknologi Informasi dan Komunikasi*, 8(2), 120–130.

[3] Andriansyah, R. (2021). Keamanan Siber dan Perlindungan Data di Era Digital. Jakarta: Pustaka Media.

[4] Andriyanto, M. R., & Sukmasetya, P. (2022). *Penerapan Algoritma Advanced Encryption Standard (AES) untuk Keamanan Data Transaksi pada Sistem E-Marketplace*. Journal of Computer System and Informatics (JoSYC), 4(1), 179–187.

[5] Deibert, R., & Scott-Railton, J. (2021). *The global threat of commercial spyware: Citizen Lab's analysis of Pegasus*. Citizen Lab Reports.

[6] Dewi, L. P., & Santoso, B. (2020). Studi pengujian keamanan aplikasi pesan instan dengan Burp Suite pada platform Android. *Jurnal Sistem Informasi*, 16(1), 45–52.

[7] Fajri, R. (2021). Keamanan Data pada Aplikasi Pesan Instan dengan Teknologi Enkripsi End-to-End. Jurnal Teknologi Informasi dan Komunikasi, 10(2), 45-55.

[8] Firmansyah, D. (2020). Keamanan Informasi dan Kriptografi: Konsep dan Implementasi. Bandung: Informatika.

[9] Hakim, R. (2022). Forensik Digital dan Keamanan Data dalam Aplikasi Perpesanan. Yogyakarta: Deepublish.

[10] Hassan, M., & Khan, I. (2020). *Mobile application penetration testing using Burp Suite: An empirical study*. *International Journal of Cyber Security and Digital Forensics (IJCSDF)*, 9(3), 205–215.

[11] Hidayat, R., & Setiawan, M. (2022). Pengujian keamanan aplikasi berbasis Android menggunakan Burp Suite. *Jurnal Rekayasa Perangkat Lunak*, 9(1), 65–73.

[12] Jones, M. (2024). *Pegasus spyware exploits zero-click vulnerability on WhatsApp to infect thousands*. *The Hacker News*.
[13] Laksamana, B. (2019). Ancaman Kejahatan Siber di Indonesia dan Cara Mengatasinya. Surabaya: CV. Teknologi Cerdas.
[14] Munir, R. (2022). Analisis Keamanan Enkripsi End-to-End Aplikasi WhatsApp. *Makalah Kriptografi dan Koding*, II4031.
[15] Munir, R. (2024). *Pemodelan dan Analisis End-to-End Encryption pada Aplikasi WhatsApp*. Institut Teknologi Bandung.
[16] OWASP Foundation. (2020). *Mobile Security Testing Guide (MSTG)*.
[17] Prasetyo, A. (2022). Peran Enkripsi dalam Keamanan Jaringan dan Aplikasi Mobile. Jakarta: PT. Cyber Nusantara.
[18] Permana, A. (2020). Analisis Risiko Keamanan Siber pada Aplikasi Pesan Instan. *Jurnal Keamanan Siber Indonesia*, 5(1), 12-20.
[19] Pratama, Y., & Hartono, S. (2019). Penilaian keamanan sistem komunikasi WhatsApp menggunakan metode penetration testing. *Jurnal Informatika*, 13(2), 98–106.
[20] Rahmawati, S., & Santoso, H. (2021). Persepsi Pengguna terhadap Keamanan Data pada Aplikasi WhatsApp. *Jurnal Sistem Informasi Indonesia*, 14(1), 67-75.
[21] Ramadhani, S. (2020). "Analisis Keamanan WhatsApp dalam Menghadapi Ancaman Kejahatan Siber." *Jurnal Teknologi dan Keamanan Siber*, 5(2), 112–125.
[22] Rohman, A. (2022). Analisis eksploitasi API dalam aplikasi WhatsApp. Surabaya: Cybersecurity Institute.
[23] Santoso, A. (2025). Analisis Keamanan Enkripsi End-to-End pada Aplikasi WhatsApp untuk Menanggulangi Ancaman Kriminalitas Siber. UI Digital Library.
[24] Santoso, J. (2021). Penggunaan Burp Suite untuk Pengujian Penetrasi Aplikasi Web dan Mobile. Yogyakarta: Andi Publisher.
[25] Sari, R., & Putra, G. (2022). Analisis keamanan enkripsi end-to-end pada aplikasi WhatsApp berbasis Android. *Jurnal Teknologi Informasi*, 10(1), 57–65.
[26] Setiawan, M. (2022). "Implementasi End-to-End Encryption pada Aplikasi Perpesanan dan Tantangannya." *Jurnal Keamanan Teknologi Informasi*, 8(1), 75–90.
[27] Siregar, D. (2021). Pengujian keamanan aplikasi mobile menggunakan Burp Suite: Studi kasus WhatsApp. Medan: Digital Security Press. Syahputra, J. (2023). "Tinjauan Terhadap Implementasi Advanced Encryption Standard (AES) 256 pada Aplikasi WhatsApp."
[28] Wahyudi, T. (2019). Keamanan Data dalam Aplikasi Berbasis Cloud dan Mobile. Malang: Universitas Teknologi Indonesia Press.
[29] Wicaksono, A., & Haryanto, L. (2020). Pemanfaatan Burp Suite dalam pengujian keamanan aplikasi mobile. *Jurnal Sistem dan Teknologi Informasi*, 8(3), 130–138.