

**ANALISIS DAMPAK TROJAN EMOTET PADA OS WINDOWS 10
MENGUNAKAN PACKET ANALYSIS DAN TOOL
WIRESHARK
SKRIPSI**

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



disusun oleh
RISWAN I LATIF
21.83.0589

Kepada
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2026

**ANALISIS DAMPAK TROJAN EMOTET PADA OS WINDOWS 10
MENGUNAKAN PACKET ANALYSIS DAN TOOL
WIRESHARK**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



disusun oleh

RISWAN I LATIF

21.83.0589

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2026**

HALAMAN PERSETUJUAN

SKRIPSI

**ANALISIS DAMPAK TROJAN EMOTET PADA OS WINDOWS 10
MENGUNAKAN PACKET ANALYSIS DAN TOOL
WIRESHARK**

yang disusun dan diajukan oleh

RISWAN I LATIF

21.83.0589

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 22 Juni 2026

Dosen Pembimbing,



Melwin Syafrizal, S.Kom., M.Eng., Ph.D.

NIK. 190302105

HALAMAN PENGESAHAN

SKRIPSI

**ANALISIS DAMPAK TROJAN EMOTET PADA OS WINDOWS 10
MENGUNAKAN PACKET ANALYSIS DAN TOOL
WIRESHARK**

yang disusun dan diajukan oleh

RISWAN I LATIF

21.83.0589

Telah dipertahankan di depan Dewan Penguji
pada tanggal 22 Juni 2026

Susunan Dewan Penguji

Nama Penguji

Jeki Kuswanto, S.Kom., M.Kom
NIK. 190302456

Muhammad Kopravi, S.Kom., M.Eng.
NIK. 190302454

Dr. Dony Ariyus, S.S., M.Kom.
NIK. 190302128

Tanda Tangan

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 22 Juni 2026

DEKAN FAKULTAS ILMU KOMPUTER



Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : RISWAN I LATIF
NIM : 21.83.0589

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISIS DAMPAK TROJAN EMOTET PADA OS WINDOWS 10 MENGUNAKAN PACKET ANALYSIS DAN TOOL WIRESHARK

Dosen Pembimbing : Melwin Syafrizal, S.Kom., M.Eng., Ph.D.

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 Juni 2026

Yang Menyatakan,



RISWAN I LATIF

HALAMAN PERSEMBAHAN

Dengan rasa syukur yang mendalam, dengan telah diselesaikannya Skripsi ini Penulis mempersembahkannya kepada:

1. Allah SWT, yang senantiasa melimpahkan rahmat, karunia, kesehatan, dan kemudahan sehingga penulis dapat menyelesaikan skripsi ini dengan baik.
2. Kedua orang tua tercinta, atas segala doa, kasih sayang, pengorbanan, serta dukungan yang tidak pernah putus dalam setiap langkah kehidupan dan pendidikan penulis.
3. Dosen pembimbing dan seluruh dosen Program Studi Teknik Komputer Universitas Amikom Yogyakarta, yang telah memberikan ilmu, arahan, bimbingan, serta pengalaman berharga selama masa perkuliahan dan proses penyusunan skripsi ini.
4. Keluarga tercinta, yang selalu memberikan semangat, perhatian, dan motivasi selama proses penyusunan skripsi ini.
5. Pacar tercinta, yang selalu hadir memberikan dukungan, doa, semangat, serta menjadi tempat berbagi cerita dan motivasi selama perjalanan penyelesaian skripsi.
6. Universitas Amikom Yogyakarta, yang telah menjadi tempat penulis menuntut ilmu, mengembangkan wawasan, serta membentuk kemampuan akademik dan profesional.
7. Sahabat, teman, dan seluruh pihak yang telah membantu, baik secara langsung maupun tidak langsung, sehingga skripsi ini dapat diselesaikan dengan baik.

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat, karunia, dan hidayah-Nya sehingga skripsi yang berjudul "**Analisis Dampak Trojan Emotet pada OS Windows 10 Menggunakan Packet Analysis dan Tool Wireshark**" dapat diselesaikan dengan baik sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer pada Program Studi Teknik Komputer, Fakul Ilmu Komputer, Universitas Amikom Yogyakarta.

Penyusunan skripsi tidak terlepas dari bantuan, dukungan, serta bimbingan dari kedua orang tua dan keluarga yang selalu memberikan doa dan motivasi, kepada Bapak **Melwin Syafrizal, S.Kom., M.Eng., Ph.D.** selaku dosen pembimbing yang telah memberikan arahan dan masukan selama proses penelitian, serta kepada seluruh dosen dan civitas akademika Universitas Amikom Yogyakarta yang telah memberikan ilmu dan pengalaman selama masa perkuliahan.

Penelitian ini dilakukan untuk menganalisis dampak aktivitas Trojan Emotet terhadap sistem operasi Windows melalui pendekatan *packet analysis* menggunakan Wireshark. Penulis berharap hasil penelitian ini dapat memberikan kontribusi bagi pengembangan pengetahuan dibidang keamanan siber serta menjadi referensi bagi peneliti selanjutnya.

Yogyakarta, 20 Mei 2026

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	iv
HALAMAN PERSEMBAHAN	v
KATA PENGANTAR	vi
DAFTAR ISI.....	vii
DAFTAR TABEL.....	x
DAFTAR GAMBAR.....	xi
DAFTAR SINGKATAN	xii
DAFTAR ISTILAH	xiv
INTISARI	xv
<i>ABSTRACT</i>	xvi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Sistematika Penulisan	4
BAB II TINJAUAN PUSTAKA	5
2.1 Studi Literatur	5
2.2 Dasar Teori.....	11
2.2.1 Malware	11
2.2.2 Trojan Horse	11

2.2.3	Trojan Emotet	12
2.2.4	Sistem Operasi Windows	12
2.2.5	Keamanan Jaringan	13
2.2.6	Lalu lintas Jaringan (<i>Network Traffic</i>)	13
2.2.7	<i>Packet Analysis</i>	13
2.2.8	Wireshark	14
2.2.9	<i>CIA Triad (Confidentiality, Integrity, Availability)</i>	14
2.2.10	<i>Indicator of Compromise (IoC)</i>	15
2.2.11	<i>Command and Control (C2) Architecture</i>	16
2.2.12	<i>Remote Access Trojan (RAT)</i>	17
2.3	Kerangka Konseptual Penelitian	18
BAB III METODE PENELITIAN		20
3.1	Objek Penelitian	20
3.2	Alur Penelitian	20
3.2.1	Studi Literatur	21
3.2.2	Perumusan Parameter Analisis	22
3.2.3	Persiapan Lingkungan Uji	22
3.2.4	Instalasi Sistem Operasi Windows	23
3.2.5	Eksekusi Sampel Emotet	23
3.2.6	Skenario Pengujian	23
3.2.7	Proses Packet Capture Menggunakan Wireshark	25
3.2.8	Analisis Parameter Jaringan	25
3.2.9	Identifikasi <i>Indicator of Compromise (IoC)</i>	26

3.2.10	Evaluasi Dampak Berdasarkan <i>CIA</i>	26
3.2.11	Kesimpulan	27
3.3	Alat dan Bahan.....	27
3.3.1	Perangkat Lunak	27
3.3.2	Perangkat Keras	27
BAB IV HASIL & PEMBAHASAN.....		28
4.1	Gambaran Umum Lingkungan Pengujian.....	28
4.2	Hasil dan Analisis Lalu Lintas Jaringan	30
BAB V PENUTUP		56
REFERENSI		58
LAMPIRAN.....		61

DAFTAR TABEL

Tabel 2. 1 Keaslian Penelitian	8
Tabel 4. 1 Spesifikasi Perangkat Keras.....	28
Tabel 4. 2 Analisis Port Komunikasi	33
Tabel 4. 3 Analisis Protokol Jaringan	36
Tabel 4. 4 Analisis Session dan Frekuensi Koneksi	38
Tabel 4. 5 Analisis <i>Payload</i>	40
Tabel 4. 6 Analisis Beaconing Pattern	42
Tabel 4. 7 Analisis Kuantitatif Komunikasi Jaringan.....	46
Tabel 4. 8 Korelasi Trafik, IoC dan Dampak Keamanan.....	48

DAFTAR GAMBAR

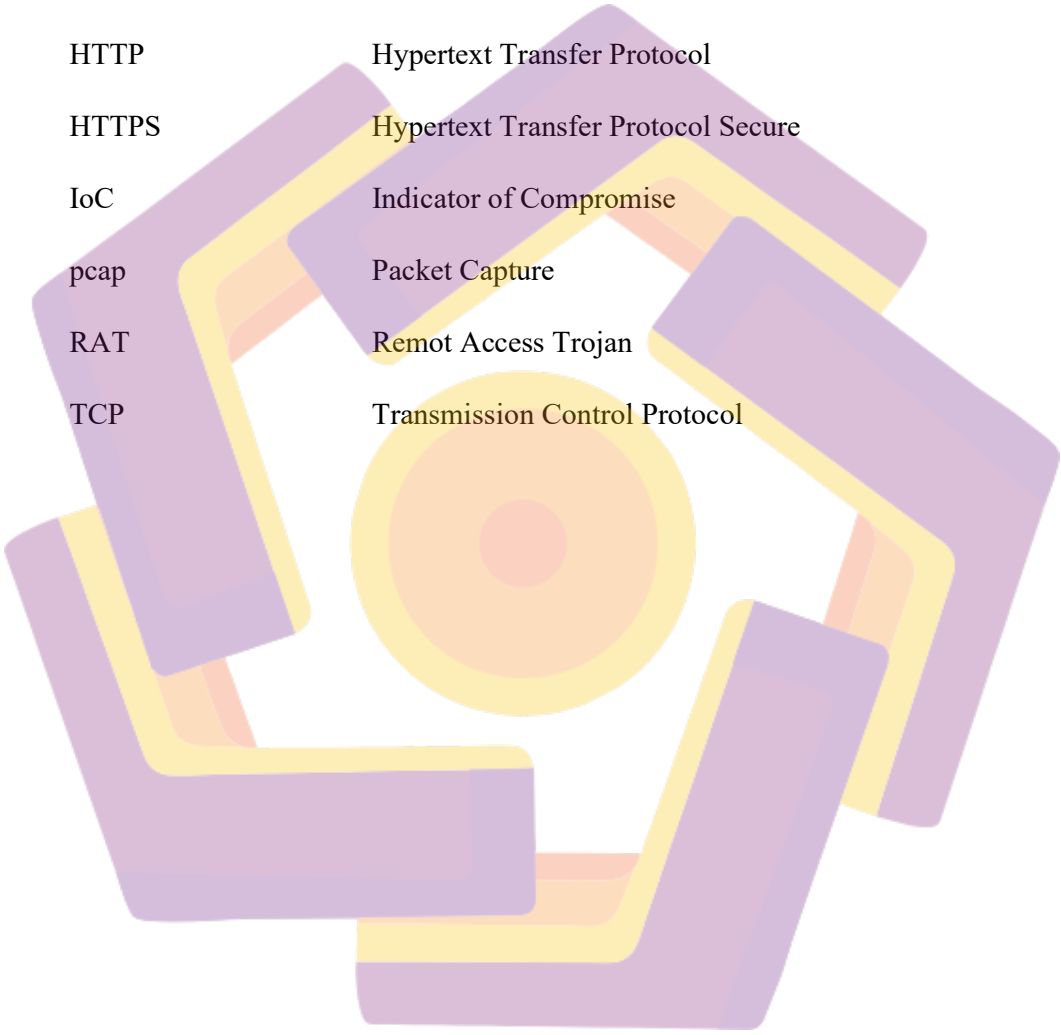
Gambar 2. 1 CIA Triad	15
Gambar 2. 2 Indicator of Compromise (IoC).....	15
Gambar 2. 3 <i>Command and Control (C2) Architecture</i>	16
Gambar 2. 4 Kerangka Konseptual Penelitian.....	19
Gambar 3. 1 Diagram Alur Penelitian	21
Gambar 4. 1 Topologi Lingkungan Pengujian.....	30
Gambar 4. 2 Tampilan utama hasil packet capture pada Wireshark.....	31
Gambar 4. 3 Detail Protokol IPv4 dan TCP pada Wireshark	35
Gambar 4. 4 Hasil analisis Conversation pada Wireshark.....	44
Gambar 4. 5 Hasil analisis Endpoints (IPv4) pada Wireshark.....	44
Gambar 4. 6 Hasil pengecekan IP pada VirusTotal	51
Gambar 4. 7 Tampilan Follow TCP Stream pada Wireshark	53

DAFTAR SINGKATAN

Lampiran 1. Hasil Analisis <i>Conversation</i> (TCP) pada Wireshark.....	61
Lampiran 2. Hasil Analisis Endpoints (IPv4) pada Wireshark.....	61
Lampiran 3. Hasil Pengecekan Alamat IP Menggunakan VirusTotal.....	62
Lampiran 4. Hasil Analisis Follow TCP Stream pada Wireshark	62

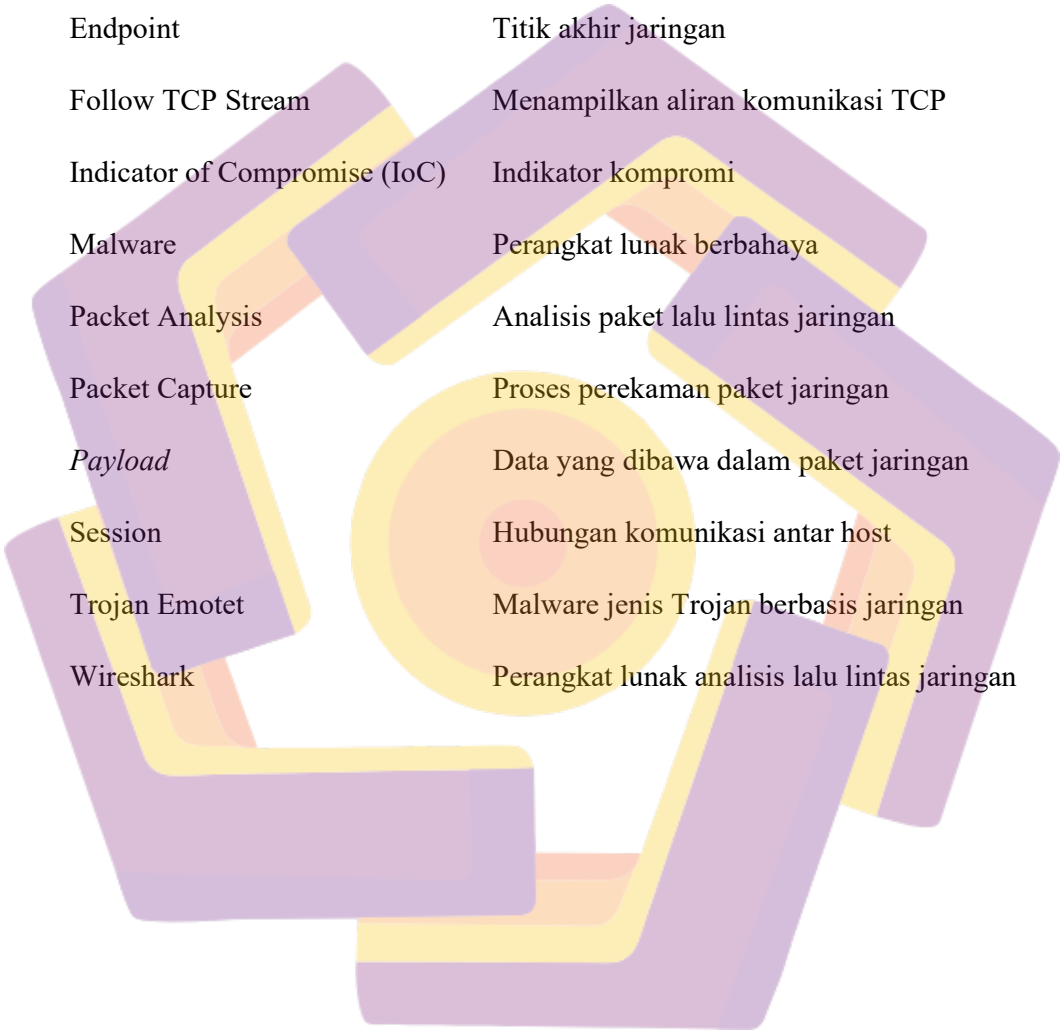


DAFTAR SINGKATAN



C2	Command and Control
CIA	Confidentiality, Integrity, Availability
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IoC	Indicator of Compromise
pcap	Packet Capture
RAT	Remot Access Trojan
TCP	Transmission Control Protocol

DAFTAR ISTILAH



Beaconing	Komunikasi Berulang
Command and Control (C2)	Kendali dan pengendalian
Endpoint	Titik akhir jaringan
Follow TCP Stream	Menampilkan aliran komunikasi TCP
Indicator of Compromise (IoC)	Indikator kompromi
Malware	Perangkat lunak berbahaya
Packet Analysis	Analisis paket lalu lintas jaringan
Packet Capture	Proses perekaman paket jaringan
<i>Payload</i>	Data yang dibawa dalam paket jaringan
Session	Hubungan komunikasi antar host
Trojan Emotet	Malware jenis Trojan berbasis jaringan
Wireshark	Perangkat lunak analisis lalu lintas jaringan

INTISARI

Penelitian ini menganalisis aktivitas lalu lintas jaringan malware Emotet pada sistem operasi Windows menggunakan Wireshark melalui metode *packet analysis* dalam lingkungan terisolasi. Hasil analisis menunjukkan bahwa sistem melakukan komunikasi dengan beberapa alamat IP eksternal melalui protokol TCP, HTTP, dan HTTPS menggunakan port 80 dan 443 dengan pola komunikasi berulang (*beaconing*), *session* komunikasi aktif, *payload* terenkripsi, serta komunikasi *multi-destination* yang mengindikasikan mekanisme *Command and Control (C2)*. Aktivitas komunikasi tersebut menunjukkan indikasi kompromi sistem berupa komunikasi otomatis, potensi data *exfiltration* serta pengendalian sistem dari jarak jauh yang berdampak pada aspek *Confidentiality, Integrity, dan Availability (CIA)*. Hasil penelitian menunjukkan bahwa analisis *packet capture* menggunakan Wireshark mampu mengidentifikasi karakteristik komunikasi malware Emotet serta indikator kompromi jaringan secara sistematis berdasarkan pola lalu lintas jaringan yang terdeteksi.

Kata kunci: *Network Traffic Analysis, Indicator of Compromise (IoC), Command and Control (C2), Wireshark, CIA Triad*

ABSTRACT

This study analyzed the traffic activity of the Emotet malware network on the Windows operating system using Wireshark through the packet analysis method in an isolated environment. The results of the analysis showed that the system communicated with several external IP addresses through TCP, HTTP, and HTTPS protocols using ports 80 and 443 with a pattern of repeated communication (beaconing), active communication sessions, encrypted payloads, and multi-destination communication indicating the Command and Control (C2) mechanism. These communication activities show indications of system compromise in the form of automatic communication, potential data exfiltration and remote system control which has an impact on the aspects of Confidentiality, Integrity, and Availability (CIA). The results showed that packet capture analysis using Wireshark was able to identify the communication characteristics of the Emotet malware as well as network compromise indicators systematically based on the detected network traffic patterns.

Keyword: