Available online at JKTE Website : http://journal.uta45jakarta.ac.id/index.php/JKTE

JURNAL KAJIAN TEKNIK ELEKTRO
EISSN : 2502-8464

Identifikasi Malware Pada Wireshark

Palindungan Tampubolon [1], EE Lailatul Putri[2], Nabila Reva Zalianti[3] , Muhammad Reza Raditya [4]

[1,2,3,4] *Universitas 17 Agustus 1945 Jakarta, 14350, Indonesia*

INFORMASI ARTIKEL

Received: February 30, 2024
Revised: May 31, 2024
Available online: June 08, 2024

CORRESPONDENCE

E-mail:
parlindungan.tampubolon@uta45jakarta.ac.id

A B S T R A K

Penelitian ini bertujuan untuk menganalisis penggunaan Wireshark dalam mengidentifikasi keberadaan malware. Tujuan utamanya adalah mengidentifikasi komunikasi mencurigakan yang dilakukan oleh malware, seperti pengiriman data ke server Command and Control (C&C), penggunaan protokol yang tidak biasa, atau pola komunikasi yang abnormal lainnya. Wireshark digunakan untuk menangkap dan menganalisis lalu lintas jaringan, dengan fokus pada pola komunikasi yang mencurigakan dan protokol yang sering digunakan oleh malware, seperti HTTP dan DNS. Data yang dianalisis berasal dari lingkungan jaringan berisiko tinggi, dan hasil tangkapan disimpan dalam format .pcap untuk analisis lebih lanjut. Dalam penelitian ini menunjukkan bahwa malware sering menggunakan protokol HTTP dan DNS untuk berkomunikasi dengan server jarak jauh, serta memanfaatkan pola lalu lintas yang sulit terdeteksi secara manual. Penelitian ini berhasil mengidentifikasi berbagai pola lalu lintas yang mengindikasikan keberadaan malware, yang kemudian divalidasi menggunakan layanan seperti VirusTotal. Temuan ini memberikan kontribusi penting dalam memahami cara kerja malware dan bagaimana upaya pencegahan dapat dilakukan untuk meningkatkan keamanan jaringan.

Kata kunci— Malware, Wireshark, lalu lintas jaringan, analisis protokol, keamanan informasi

A B S T R A C T

This study aims to analyze the use of Wireshark in identifying the presence of malware. The primary objective is to identify suspicious communications conducted by malware, such as data transmission to Command and Control (C&C) servers, the use of unusual protocols, or other abnormal communication patterns. Wireshark is used to capture and analyze network traffic, focusing on suspicious communication patterns and protocols frequently used by malware, such as HTTP and DNS. The analyzed data is sourced from high-risk network environments, and the captured traffic is saved in .pcap format for further analysis. The findings of this study reveal that malware often uses HTTP and DNS protocols to communicate with remote servers and employs traffic patterns that are difficult to detect manually. The research successfully identified various traffic patterns indicating the presence of malware, which were subsequently validated using services such as VirusTotal. These findings provide significant contributions to understanding malware behavior and identifying preventive measures to enhance network security.

Keywords— Malware, Wireshark, network traffic, protocol analysis, information security

I. PENDAHULUAN

Keamanan informasi merupakan suatu hal penting dalam era digital yang mengintegrasikan semua aspek ke dalam internet (Ramdan et al., 2022). Meningkatnya pemanfaatan teknologi internet justru juga menjadi tantangan baru dalam perlindungan data pribadi, terutama pada pengumpulan, pemanfaatan, dan penyebaran data pribadi seseorang. Ancaman yang sering terjadi adalah penipuan yang memanfaatkan celah penggunaan teknologi digital (Parulian et al., 2021). Serangan siber merupakan ancaman serius bagi organisasi dan instansi yang mengandalkan jaringan komputer dalam operasionalnya

(Ikhwanul Uzlah & Adi Saputra, 2024) (Rabbani & Diana, 2023).

Peningkatan ketergantungan terhadap teknologi digital memberikan ancaman terhadap rentannya keamanan informasi yang menjadi salah satu tantangan utama dalam era modern (Sandriana & Maulana, 2022). Keamanan siber merupakan cara dalam melindungi penggunaan ruang siber dari berbagai ancaman dan serangan (Afifah Rodhiyatun Nisa et al., 2024) (Sutra & Haryanto, 2023). Berbagai jenis malware terus berkembang dengan kemampuan yang kompleks (Pajar Setia et al., 2018) dalam menyusup pada sistem yang ada, mencuri data, bahkan mengganggu operasional suatu sistem dan jaringan. Untuk itu dibutuhkan suatu tools dan metode yang digunakan untuk mendeteksi ancaman tersebut (Nugroho & Prayudi, 2015).

Wireshark merupakan salah satu tools dalam menganalisis jaringan yang dapat digunakan untuk menangkap dan menganalisis lalu lintas data. Wireshark mempunyai kemampuan dalam memonitor protokol jaringan, memfilter komunikasi, dan mengidentifikasi anomali yang terindikasi adanya aktivitas malware. Melalui analisis terhadap pola lalu lintas yang tidak wajar, user dapat mengidentifikasi keberadaan malware serta memahami teknik pengoperasiannya.

Penelitian ini bertujuan untuk menguji pemanfaatan Wireshark dalam mendeteksi malware melalui analisis pola komunikasi jaringan yang diduga mencurigakan.

II. LANDASAN TEORI

Pada bab ini akan dijelaskan beberapa teori yang mendukung penelitian.

2.1 Malware

Malware atau malicious software merupakan semua perangkat lunak yang digunakan dengan tujuan untuk melanggar sistem komputer dan kebijakan keamanan yang berhubungan dengan aspek kerahasiaan, keutuhan, dan ketersediaan. Malware juga dapat diartikan sebagai kode yang melakukan aksi berbahaya. Malware dapat berupa script, kode, executable file, maupun bentuk lainnya, yang dapat tersebar melalui banyak media, seperti situs internet, e-mail, ataupun USB (Mariyah Fairuz et al., 2021).

2.2 Wireshark

Sebelumnya dikenal dengan nama Ethereal. Itu dikembangkan oleh Gerald Combs pada tahun 1988. Ini terutama digunakan untuk memecahkan masalah dan menganalisis jaringan komputer. Ini dapat dijalankan pada mesin windows dan UNIX. Sudah terinstal sebelumnya dengan beberapa distribusi Linux seperti Kali Linux. Ini mendukung berbagai macam protokol yang berbeda. Ini mendukung keduanya baris perintah dan antarmuka pengguna grafis. Ini memberikan detail mikroskopis tentang apa yang terjadi di jaringan dan juga merupakan standar di banyak institusi pendidikan, organisasi komersial dan nirlaba (Iqbal & Naaz, 2019)

III. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus untuk menganalisis bagaimana Wireshark dapat digunakan dalam mengidentifikasi malware, dan subjek penelitian terdiri dari data lalu lintas jaringan yang ditangkap dari lingkungan jaringan yang berisiko tinggi. Data ini mencakup berbagai jenis lalu lintas jaringan, baik yang normal maupun yang mencurigakan.

Wireshark juga digunakan sebagai instrumen utama untuk menangkap dan menganalisis paket data jaringan. Fitur-fitur Wireshark, seperti filter tampilan dan analisis protokol, dimanfaatkan untuk mengidentifikasi pola-pola yang mencurigakan. Prosedur Penelitian Menginstal dan mengonfigurasi Wireshark pada perangkat yang digunakan untuk menangkap lalu lintas jaringan (Orebaugh, A., Ramirez, G., & Beale, J. 2006).

Dengan menangkap lalu lintas jaringan selama periode waktu tertentu dan menyimpan hasil tangkapan paket dalam format .pcap untuk analisis lebih lanjut (Sutarti et al., 2023). Dengan menyimpan hasil tangkapan paket dalam format .pcap untuk analisis lebih lanjut dan menggunakan filter tampilan untuk memfokuskan analisis pada paket yang mencurigakan, seperti paket dengan tujuan alamat IP yang tidak dikenal atau pola komunikasi yang tidak biasa untuk mengidentifikasi protokol yang sering digunakan oleh malware, seperti HTTP, HTTPS, DNS, dan lain-lain.

Menganalisis pola lalu lintas yang mencurigakan, termasuk frekuensi tinggi dari permintaan tertentu, pengiriman data ke server C&C, dan komunikasi dengan alamat IP yang tidak dikenal dan membandingkan temuan dari analisis Wireshark dengan database signature malware untuk memvalidasi keberadaan malware

Menyusun laporan hasil analisis, termasuk deskripsi pola mencurigakan yang teridentifikasi dan interpretasi temuan dan menyajikan hasil dalam bentuk tabel, grafik, atau visualisasi lain yang relevan untuk mempermudah pemahaman

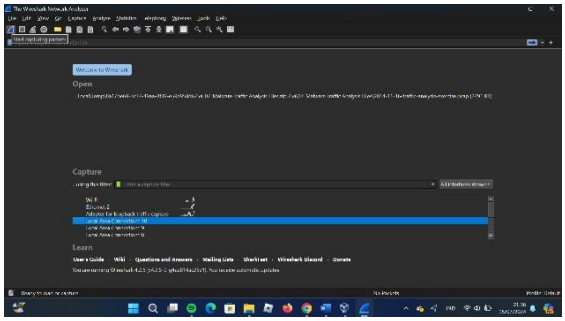
Penelitian ini dilakukan dengan memperhatikan aspek keamanan dan etika. Data yang digunakan dalam penelitian diambil dari lingkungan jaringan yang telah mendapatkan izin dari pemiliknya. Selain itu, data yang dianalisis dijaga kerahasiaannya dan hanya digunakan untuk tujuan penelitian ini

IV. HASIL DAN PEMBAHASAN

Pada hasil dan pembahasan ini akan di jelaskan mengenai hasil Identifikasi Malware pada Wireshark. Berikut penjelasannya.

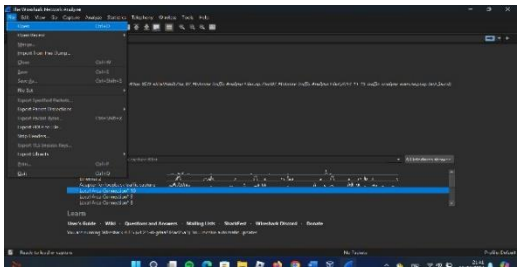
A. Identifikasi Malware pada Wireshark

Berikut dijelaskan detail cara kerja Wireshark sebagai berikut.



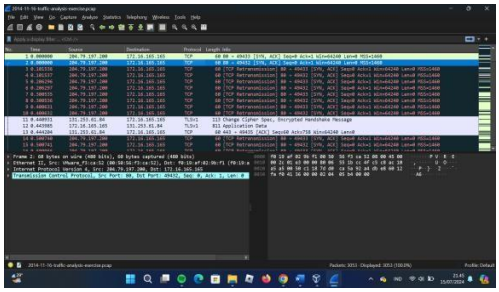
Gambar 1 Tampilan Awal Wireshark

Wireshark adalah alat analisis jaringan yang sering digunakan untuk memantau dan menganalisis lalu lintas jaringan dalam waktu nyata. Setelah membuka Wireshark, tampilan awal akan menunjukkan daftar antarmuka jaringan yang tersedia untuk dipilih. Pengguna dapat memilih salah satu antarmuka jaringan untuk mulai menangkap paket data. Tampilan ini juga mencakup berbagai filter dan opsi konfigurasi yang memungkinkan pengguna untuk memfokuskan analisis pada jenis lalu lintas tertentu. Di bagian atas, terdapat menu utama yang menyediakan berbagai opsi untuk menangkap, menganalisis, dan mengekspor data.



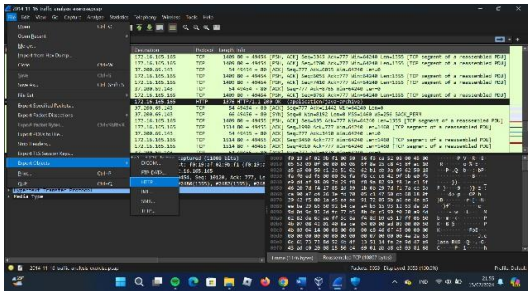
Gambar 2 Masuk open dari downloadan malware

Pada tahap ini, pengguna membuka file yang telah diunduh yang diduga berisi malware. File ini biasanya berupa executable (misalnya .exe atau .zip) yang mengandung perangkat lunak berbahaya. Proses ini bertujuan untuk melihat apakah malware tersebut memengaruhi lalu lintas jaringan yang ditangkap oleh Wireshark. Ketika malware dijalankan, ia akan mencoba untuk berkomunikasi dengan server atau perangkat lain di jaringan, dan aktivitas ini akan terlihat dalam bentuk paket data di Wireshark, memberikan petunjuk tentang jenis malware dan tindakannya.



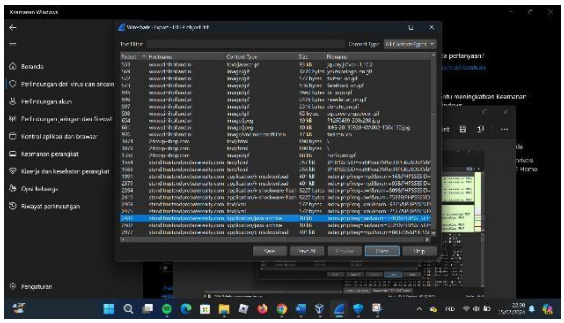
Gambar 3 Tampilan Traffic Analysis

Setelah malware dijalankan, Wireshark akan mulai menangkap lalu lintas jaringan yang terjadi. Tampilan analisis lalu lintas akan menunjukkan berbagai paket data yang dikirim dan diterima melalui jaringan, termasuk komunikasi antara malware dan server jarak jauh. Paket-paket ini bisa mencakup permintaan HTTP, pengiriman data, atau komunikasi lain yang terkait dengan kegiatan berbahaya. Wireshark menyediakan berbagai filter untuk mempermudah pencarian paket terkait malware, seperti mencari paket dengan protokol tertentu atau mengidentifikasi sumber dan tujuan paket yang mencurigakan.



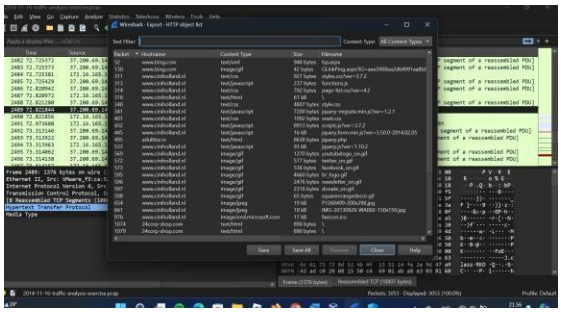
Gambar 4 Export ke HTTP dalam File

Langkah ini melibatkan ekspor data yang relevan dari Wireshark, khususnya yang terkait dengan lalu lintas HTTP. Wireshark memungkinkan pengguna untuk memfilter paket berdasarkan protokol, dan dalam hal ini, paket HTTP yang mungkin digunakan oleh malware untuk berkomunikasi dengan server jarak jauh dapat diekspor. Data yang diekspor dapat disimpan dalam format file (misalnya, .pcap) dan digunakan untuk analisis lebih lanjut. Proses ekspor ini membantu memisahkan lalu lintas yang relevan dari data lainnya yang tidak diperlukan.



Gambar 5 Mencari File dengan Hypertext/program aneh dan save

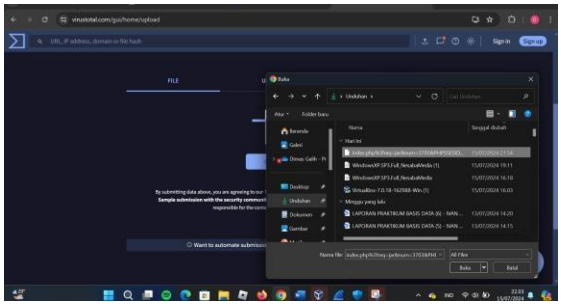
Pada tahap ini, pengguna akan mencari file atau program yang tampaknya mencurigakan atau tidak biasa dalam lalu lintas HTTP yang diekspor. File ini mungkin berupa skrip atau program yang dikirimkan oleh server kepada sistem yang terinfeksi. Wireshark memungkinkan pengguna untuk melihat data yang terkandung dalam setiap paket, termasuk file atau skrip yang diunduh atau dikirim melalui HTTP. Jika ditemukan file yang mencurigakan, file tersebut dapat disalin dan disimpan untuk dianalisis lebih lanjut.



Gambar 6 Save File Yang Akan Di Analisis

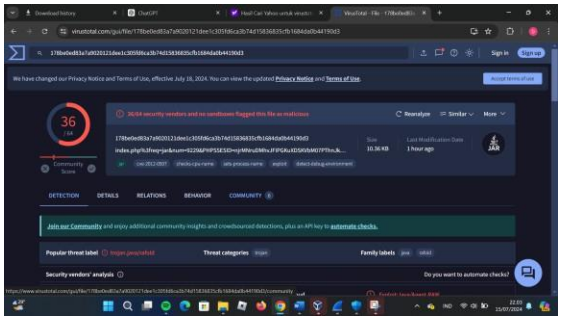
Setelah file mencurigakan ditemukan, langkah selanjutnya adalah menyimpannya ke dalam sistem untuk dianalisis secara mendalam. Proses penyimpanan ini

memastikan bahwa file berbahaya tidak langsung dijalankan atau dieksekusi, yang dapat menyebabkan infeksi lebih lanjut. File yang disimpan ini bisa berupa file berjenis .exe, .dll, atau bahkan skrip yang digunakan oleh malware untuk melakukan aksinya. Penyimpanan file ini juga memudahkan untuk melakukan analisis lebih lanjut dengan alat lain seperti sandboxing atau analisis virus.



Gambar 7 Identifikasi Malware di Virus total

Setelah file yang mencurigakan berhasil disalin dan disimpan, langkah berikutnya adalah mengunggahnya ke VirusTotal, sebuah layanan online yang memungkinkan pengguna untuk memeriksa apakah file tersebut terdeteksi sebagai malware oleh berbagai mesin antivirus. VirusTotal akan memberikan analisis yang komprehensif mengenai potensi ancaman yang terkandung dalam file tersebut. Ini dapat membantu pengguna dalam mengidentifikasi apakah file tersebut benar-benar berbahaya dan memberi petunjuk lebih lanjut mengenai jenis malware yang dihadapi.



Gambar 8 Malware Teridentifikasi

Jika file yang diunggah ke VirusTotal teridentifikasi sebagai malware, maka hasilnya akan menunjukkan jenis dan perilaku dari malware tersebut. Laporan ini mencakup informasi mengenai kategori malware, seperti trojan, worm, atau ransomware, serta nama-nama antivirus yang mendeteksi ancaman tersebut. Identifikasi ini penting untuk pemahaman lebih lanjut mengenai cara malware bekerja, cara penyebarannya, dan langkah-langkah pencegahan yang dapat diambil untuk melindungi sistem dari infeksi lebih lanjut.

V. PENUTUP

Penelitian ini menunjukkan bahwa Wireshark merupakan alat yang efektif untuk mendeteksi dan menganalisis keberadaan malware dalam lalu lintas jaringan. Dengan fitur seperti filter tampilan dan analisis protokol, Wireshark dapat mengidentifikasi pola mencurigakan yang sering dikaitkan dengan aktivitas malware. Langkah-langkah yang diambil, mulai dari menangkap lalu lintas jaringan hingga memvalidasi hasil menggunakan layanan seperti VirusTotal, memberikan pendekatan sistematis untuk mengamankan jaringan dari ancaman malware. Ke depan, penelitian ini dapat diperluas dengan mengintegrasikan teknik pembelajaran mesin untuk meningkatkan akurasi deteksi dan analisis. Selain itu, penting untuk terus memperbarui database signature malware agar analisis tetap relevan dengan ancaman terkini.

REFERENSI

Afifah Rodhiyatun Nisa, A., Ananditto Daffa Wijayanto, Arya Prabudi Jaya Priana, & Setiawan, A. (2024). Analisis Log Server untuk mendeteksi Serang DDoS pada Keamaan Jaringan di Website. *Journal of Internet and Software Engineering*, *1*(3), 17. https://doi.org/10.47134/pjise.v1i3.2612

Ikhwanul Uzlah, L., & Adi Saputra, R. (2024). DETEKSI SERANGAN SIBER PADA JARINGAN KOMPUTER MENGGUNAKAN METODE RANDOM FOREST. In *Jurnal Mahasiswa Teknik Informatika* (Vol. 8, Issue 3). https://bit.ly/CyberSecurityAttacks.

Iqbal, H., & Naaz, S. (2019). Wireshark as a Tool for Detection of Various LAN Attacks. *International Journal of Computer Sciences and Engineering*, *7*(5), 833–837. https://doi.org/10.26438/ijcse/v7i5.833837

Mariyah Fairuz, G., Yusuf, M., & Setiadji, B. (2021). Pembuatan Bahan Cyber Exercise sebagai Sarana Latihan Penanganan Insiden Malware (Studi Kasus: Instansi XYZ). *Jurnal Info Kripto, 15 (3)*, 123–131.

Nugroho, H. A., & Prayudi, Y. (2015). PENGGUNAAN TEKNIK REVERSE ENGINEERING PADA MALWARE ANALYSIS UNTUK IDENTIFIKASI SERANGAN MALWARE. *KNSI 2014*. www.thehackernews.com

Pajar Setia, T., Widiyasono, N., & Putra Aldya, A. (2018). Analysis Malware Flawed Ammyy RAT Dengan Metode Reverse Engineering. *Jurnal Informatika: Jurnal Pengembangan IT*, *3*(3), 371–379. https://doi.org/10.30591/jpit.v3i3.1019

Parulian, S., Pratiwi, D. A., & Cahya Yustina, M. (2021). *Ancaman dan Solusi Serangan Siber di Indonesia*. http://ejournal.upi.edu/index.php/TELNECT/

Rabbani, S., & Diana, D. (2023). Prediksi Kategori Serangan Siber dengan Algoritma Klasifikasi Random Forest Menggunakan Rapidminer. *SMATIKA JURNAL*, *13*(02), 284–293. https://doi.org/10.32664/smatika.v13i02.934

Ramdan, A., Widyasono, N., & Mubarok, H. (2022). Prediksi Jaringan TOR dan VPN menggunakan Algoritma K-Nearest Neighbour pada Trafik Darknet. In *Jurnal Sistem Cerdas*.

Sandriana, A., & Maulana, F. (2022). E-JOINT (Electronica and Electrical Journal of Innovation Technology) Klasifikasi serangan Malware terhadap Lalu Lintas Jaringan Internet of Things menggunakan Algoritma K-Nearest Neighbour (K-NN). *E- JOINT (Electronica*

and Electrical Journal of Innovation Technology), 3 (1)(1), 12.

Sutarti, Siswanto, & Bachtiar, A. (2023). ANALISIS WEB PHISHING MENGGUNAKAN METODE NETWORK FORENSIC DAN BLOCK ACCESS SITUS DENGAN ROUTER MIKROTIK. *Jurnal PROSISKO*, *10 (1)*, 71–83.

Sutra, S. M. S., & Haryanto, A. (2023). Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020. *56Global Political Studies Journal*, *7 (1)*, 56–59.

Beale, J., Orebaugh, A., & Ramirez, G. (2006). *Wireshark & Ethereal network protocol analyzer toolkit*. Elsevier.