Digibe: Digital Business and Entrepreneurship Journal
Vol. 2, No. 2, 2024, 88-96
E-ISSN : 3032-2480
https://journal.feb.uniku.ac.id/digibe

IMPLEMENTASI NETWORK TRAFFIC ANALISIS UNTUK MENDETEKSI ANOMALI JARINGAN PADA TWITTER/X DAN INSTAGRAM

Rakhmadi Rahman[1*], Egi Fahrezi Iswan[2]
[1,2] Information System Departement, Bacharuddin Jusuf Habibie, Sulawesi Selatan, Indonesia
*Coresponding Email: egifahrezi96@gmail.com

How to Cite: Rahman, Rahmadi,. Iswan, Egi Farezi (2024). Implementasi Network Traffic Analisis untuk Mendeteksi Anomali Jaringan pada Twitter/X Dan Instagram. *Digital Business and Entrepreneurship Journal (Digibe), Volume 2 (Nomor 2): 88-96*

Received: 25-06-2024 Accepted: 24-07-2024 Published: 3107-2024

Abstrak

Penelitian ini berfokus pada implementasi analisis lalu lintas jaringan menggunakan Wireshark untuk mendeteksi anomali pada aplikasi Twitter/X dan Instagram. Tujuan utamanya adalah mengidentifikasi tingkat lalu lintas pada port-port yang ditandai dengan warna hitam dan merah, yang dapat mengindikasikan potensi masalah atau aktivitas jaringan mencurigakan. Penelitian ini menggunakan pendekatan kuantitatif dengan mengumpulkan data lalu lintas jaringan, melakukan analisis statistik, dan menerapkan teknik deteksi anomali. Hasil penelitian diharapkan dapat membantu mengidentifikasi dan mengatasi tingkat lalu lintas tinggi, serta memberikan wawasan berharga tentang keamanan jaringan dan strategi yang lebih efektif untuk mendeteksi dan mengatasi ancaman keamanan. Dalam analisis jaringan menggunakan Wireshark, terdapat beberapa fitur dan indikator warna yang membantu dalam memeriksa dan menganalisis lalu lintas paket data. Port berwarna biru muda menunjukkan "*Sample inactive selected item*," yang memungkinkan pengguna untuk melihat contoh isi paket yang tidak aktif, berguna untuk penelusuran paket tidak aktif, analisis *payload data*, dan pemecahan masalah jaringan. Port berwarna abu-abu menunjukkan "*Sample active selected item*," yang menampilkan contoh isi paket yang sedang aktif, membantu dalam pemeriksaan konten paket aktif, analisis payload data, dan pemahaman konteks komunikasi. Port berwarna hitam dan merah menunjukkan tingkat lalu lintas yang tinggi, dengan port hitam mungkin mencurigakan dan port merah menunjukkan potensi masalah seperti serangan DDoS atau kemacetan jaringan. Port merah ditandai dengan status flag "Reset = Set" dalam header TCP, mengindikasikan kemungkinan gangguan konektivitas, kesalahan konfigurasi perangkat, aktivitas mencurigakan, atau masalah pada endpoint komunikasi.

Kata kunci: *Anomali Jaringan; Wireshark; Twitter/X; Instagram*

Abstract

This research focuses on implementing network traffic analysis using Wireshark to detect anomalies in the Twitter/X and Instagram applications. The main goal is to identify traffic levels on ports marked in black and red, which can indicate potential problems or suspicious network activity. This research uses a quantitative approach by collecting network traffic data, conducting statistical analysis, and applying anomaly detection techniques. The research results are expected to help identify and address high traffic levels, as well as provide valuable insights into network security and more effective strategies for detecting and addressing security threats. In network analysis using Wireshark, there are several features and color indicators that help in examining and analyzing data packet traffic. The light blue port indicates "Sample inactive selected item," which allows users to view a sample of inactive packet contents, useful for inactive packet tracing, data payload analysis, and network troubleshooting. The grayed port indicates "Sample active selected item," which displays a sample of currently active packet contents, assisting in active packet content inspection, data payload analysis, and understanding the communication context. Black and red ports indicate high levels of traffic, with black ports possibly suspicious and red ports indicating potential problems such as DDoS attacks or network congestion. Red ports are indicated by the status flag "Reset=Set" in the TCP header, indicating possible connectivity disruption, device misconfiguration, suspicious activity, or problems with the communications endpoint.

Keyword: *Network Anomalies; Wireshark; Twitter/X; Instagram*

E-ISSN : 3032-2480
https://journal.feb.uniku.ac.id/digibe

PENDAHULUAN

Analisis lalu lintas jaringan untuk mendeteksi anomali merupakan praktik penting dalam keamanan jaringan. Melalui analisis ini, kita dapat mengidentifikasi perilaku yang tidak biasa atau mencurigakan dalam lalu lintas jaringan, yang dapat menjadi tanda adanya serangan atau gangguan keamanan. Salah satu alat yang umum digunakan untuk menganalisis lalu lintas jaringan adalah Wireshark. Wireshark adalah perangkat lunak sumber terbuka yang memungkinkan pemantauan, analisis, dan pemfilteran paket data dalam jaringan. Dalam konteks ini, implementasi analisis lalu lintas jaringan untuk mendeteksi anomali pada aplikasi Twitter/X dan Instagram menggunakan Wireshark. dengan berkembangnya berbagai platform media sosial lainnya, ada kebutuhan untuk memperluas cakupan penelitian ini agar mencakup aplikasi lain yang populer. Hal ini akan membantu dalam menggeneralisasi temuan dan meningkatkan ketahanan teknik deteksi anomali. Banyak penelitian fokus pada analisis offline dari data lalu lintas jaringan yang dikumpulkan menggunakan Wireshark. Namun, ada kebutuhan untuk penelitian yang berfokus pada deteksi anomali secara real-time dan mekanisme respons otomatis untuk segera mengatasi ancaman keamanan saat terjadi.

Penelitian ini memberikan analisis komparatif anomali lalu lintas jaringan antara Twitter/X dan Instagram. Namun, diperlukan studi komparatif lebih lanjut untuk mengevaluasi efektivitas berbagai alat dan teknik deteksi anomali di berbagai lingkungan jaringan dan pola lalu lintas. Penelitian ini fokus pada data lalu lintas jaringan dengan menggabungkan analisis perilaku pengguna dapat memberikan wawasan tambahan tentang penyebab anomali jaringan dan membantu membedakan antara aktivitas yang tidak berbahaya dan yang berbahaya.

Penelitian ini berfokus pada implementasi analisis lalu lintas jaringan. Analisis lalu lintas jaringan adalah proses memantau, menangkap, dan menganalisis paket data yang bergerak melalui jaringan komputer. Tujuan utamanya adalah untuk memahami pola lalu lintas, mengidentifikasi masalah kinerja, dan mendeteksi aktivitas mencurigakan yang dapat mengindikasikan ancaman keamanan (Susanto, 2022).

Penelitian ini akan mendeteksi anomali. Deteksi anomali adalah proses mengidentifikasi pola yang tidak biasa atau mencurigakan dalam data yang dapat menunjukkan adanya masalah atau ancaman. Dalam konteks jaringan, anomali dapat berupa lonjakan lalu lintas yang tidak biasa, aktivitas pada port yang tidak biasa, atau pola komunikasi yang tidak sesuai dengan norma.Teknik deteksi anomali mencakup beberapa pendekatan. Pertama, threshold-based detection menggunakan batasan tertentu untuk mengidentifikasi anomali; misalnya, jika lalu lintas melebihi ambang batas yang telah ditentukan, itu dianggap sebagai anomali. Kedua, machine learning menggunakan algoritma pembelajaran mesin untuk mempelajari pola normal dalam data dan mendeteksi penyimpangan dari pola tersebut. Ketiga, behavioral analysis menganalisis perilaku pengguna atau sistem untuk mengidentifikasi aktivitas yang tidak biasa (Hadi & Nugroho, 2023).

Menurut Sari & Arifin (2022), wireshark adalah alat analisis lalu lintas jaringan sumber terbuka yang memungkinkan pengguna untuk menangkap dan memeriksa data yang bergerak melalui jaringan. Alat ini menyediakan antarmuka grafis yang memudahkan pengguna untuk memfilter, mengurutkan, dan menganalisis paket data. Wireshark memiliki berbagai fitur utama, termasuk kemampuan untuk menangkap paket data secara real-time atau dari file pcap yang telah disimpan, memfilter paket berdasarkan kriteria tertentu seperti alamat IP, protokol, atau port, menampilkan detail dari setiap paket, termasuk header dan payload, dalam format yang mudah dibaca, serta menyediakan berbagai statistik dan visualisasi untuk membantu analisis lalu lintas jaringan.

E-ISSN : 3032-2480
https://journal.feb.uniku.ac.id/digibe

Twitter/X merupakan platform media sosial yang memungkinkan pengguna untuk mengirim dan membaca pesan singkat, dengan lalu lintas jaringannya biasanya melibatkan permintaan HTTP/HTTPS untuk memuat konten, mengirim tweet, dan menerima notifikasi. Instagram, sebagai platform berbagi foto dan video, memungkinkan pengguna untuk mengunggah konten, memberikan like, dan mengirim pesan, dengan lalu lintas jaringannya mencakup permintaan HTTP/HTTPS untuk memuat gambar, video, dan interaksi pengguna. Potensi anomali yang dapat terdeteksi meliputi lonjakan tiba-tiba dalam lalu lintas yang mungkin mengindikasikan serangan DDoS atau aktivitas bot, aktivitas pada port yang tidak biasa yang dapat menunjukkan upaya eksploitasi atau komunikasi yang tidak sah, serta pola komunikasi yang tidak sesuai dengan norma yang bisa menandakan adanya malware atau aktivitas mencurigakan lainnya (Gunawan & Putra, 2023).

Menurut Pratama & Rachman (2024), keamanan jaringan melibatkan perlindungan terhadap berbagai ancaman yang dapat mengganggu integritas dan ketersediaan sistem. Salah satu ancaman utama adalah serangan DDoS, yang bertujuan membuat layanan tidak tersedia dengan membanjiri jaringan dengan lalu lintas yang berlebihan. Malware juga merupakan ancaman signifikan, karena perangkat lunak berbahaya ini dapat mencuri data, merusak sistem, atau mengambil alih kontrol jaringan. Eksploitasi kerentanan, yaitu memanfaatkan kelemahan dalam perangkat lunak atau protokol jaringan untuk mendapatkan akses tidak sah, juga menjadi perhatian penting. Untuk mengatasi ancaman ini, langkah-langkah keamanan yang dapat diterapkan termasuk enkripsi, yang mengamankan data dengan mengenkripsi komunikasi untuk mencegah penyadapan; firewall, yang mengontrol lalu lintas masuk dan keluar berdasarkan aturan keamanan yang ditentukan; serta intrusion detection systems (IDS), yang memantau jaringan untuk mendeteksi aktivitas mencurigakan atau tidak sah.

Rumusan Masalah

1. Bagaimana cara mengidentifikasi dan mengatasi tingkat lalu lintas yang tinggi pada port-port yang ditandai hitam dan merah dalam gambar tersebut?
2. Apakah lalu lintas yang tinggi tersebut merupakan hasil dari serangan atau aktivitas jaringan yang mencurigakan?
3. Bagaimana cara mengurangi risiko potensial yang mungkin terjadi akibat tingkat lalu lintas yang tinggi pada port-port tersebut?

Tujuan Penelitian

Tujuan dari penelitian ini ialah untuk mengidentifikasi pola, tren, dan potensi masalah dalam suatu sistem atau jaringan. Dengan mengamati visualisasi data, seperti penggunaan kode warna pada komponen tertentu, pengguna dapat mendeteksi area atau titik-titik kritis. Tujuan utama dari analisis ini adalah untuk mengidentifikasi tingkat lalu lintas pada port-port yang ditampilkan, khususnya yang ditandai dengan warna hitam dan merah. Hal ini dapat membantu dalam mendeteksi port-port yang mengalami tingkat lalu lintas yang tinggi, yang dapat mengindikasikan adanya potensi masalah atau aktivitas jaringan yang mencurigakan. Selain itu, tujuannya adalah untuk memberikan dasar bagi langkah-langkah selanjutnya dalam menganalisis dan mengatasi masalah yang terkait dengan tingkat lalu lintas yang tinggi pada port-port tersebut. Hal ini dapat melibatkan investigasi lebih lanjut, penyesuaian konfigurasi, atau pengambilan tindakan korektif untuk memperbaiki situasi yang tidak diinginkan.

E-ISSN : 3032-2480
https://journal.feb.uniku.ac.id/digibe

Kerangka Berpikir Penelitian

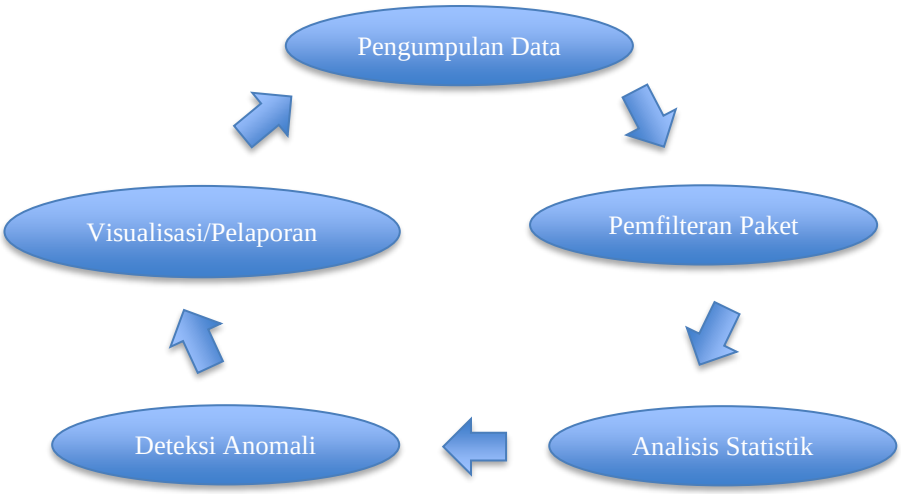
Pengumpulan data lalu lintas jaringan menggunakan Wireshark**,** Pemfilteran paket untuk memfokuskan pada lalu lintas yang relevan dengan aplikasi Twitter/X dan Instagram**,** Analisis statistik dasar untuk memahami pola lalu lintas jaringan normal**,** Penerapan teknik deteksi anomali untuk mengidentifikasi aktivitas mencurigakan**,** Visualisasi dan pelaporan hasil analisis untuk pemahaman yang lebih baik.

Hipotesis

1. Tingkat lalu lintas yang tinggi pada port-port tertentu merupakan indikasi adanya aktivitas jaringan yang mencurigakan, seperti serangan atau gangguan keamanan.
2. Penerapan teknik deteksi anomali yang tepat dapat membantu mengidentifikasi dan mengatasi tingkat lalu lintas yang tinggi pada port-port tersebut, sehingga mengurangi risiko potensial yang mungkin terjadi.

METODE

Metode penelitian ini menggunakan pendekatan kuantitatif, dengan fokus pada analisis data lalu lintas jaringan secara statistik dan penerapan teknik deteksi anomali. Alasan Pemilihan Metode Kuantitatif untuk mengidentifikasi Pengumpulan Data Kuantitatif dari Wireshark, Deteksi Anomali Berbasis Metrik, Analisis Deret Waktu dan Tren, Korelasi dan Identifikasi Penyebab, dan Pemodelan Prediksi.



Gambar 1. Metode Penelitian PPADV

Proses pengumpulan data diatas, merupakan gambaran untuk mendeteksi anomali jaringan menggunakan Wireshark, dan metode analisis data yang relevan seperti analisis statistik dasar, deteksi anomali menggunakan threshold-based detection, machine learning, dan behavioral analysis.

Teknik analisis yang digunakan dalam deteksi anomali ini adalah Machine learning, dimana Machine learning adalah teknik yang menggunakan algoritma pembelajaran mesin untuk mempelajari pola normal dalam data dan mendeteksi penyimpangan dari pola tersebut. Algoritma ini dapat dilatih menggunakan data historis untuk mengenali perilaku normal dan anomali.

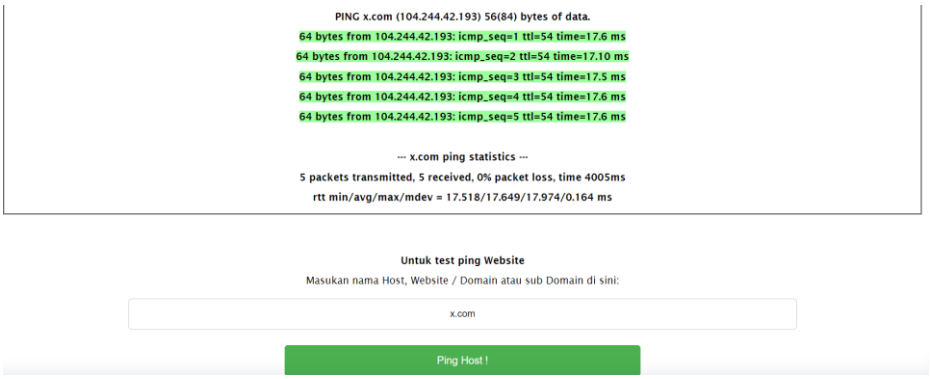
E-ISSN : 3032-2480
https://journal.feb.uniku.ac.id/digibe

HASIL DAN PEMBAHASAN

Analisis perbandingan aplikasi Twitter/X dan Instagram diperoleh bahwa hasil nilai akurasi probabilitas tertinggi dari data akses TCP dengan proses simulasi pengujian data yang di akses melalui traffic anomaly yang diakses melalui tools wireshark dan menghasilkan format data dalam bentuk csv.

1. Twitter/X

a. Pertama-tama kita harus ping nama host, website atau domainnya terlebih dahulu menggunakan https://ipsaya.com/



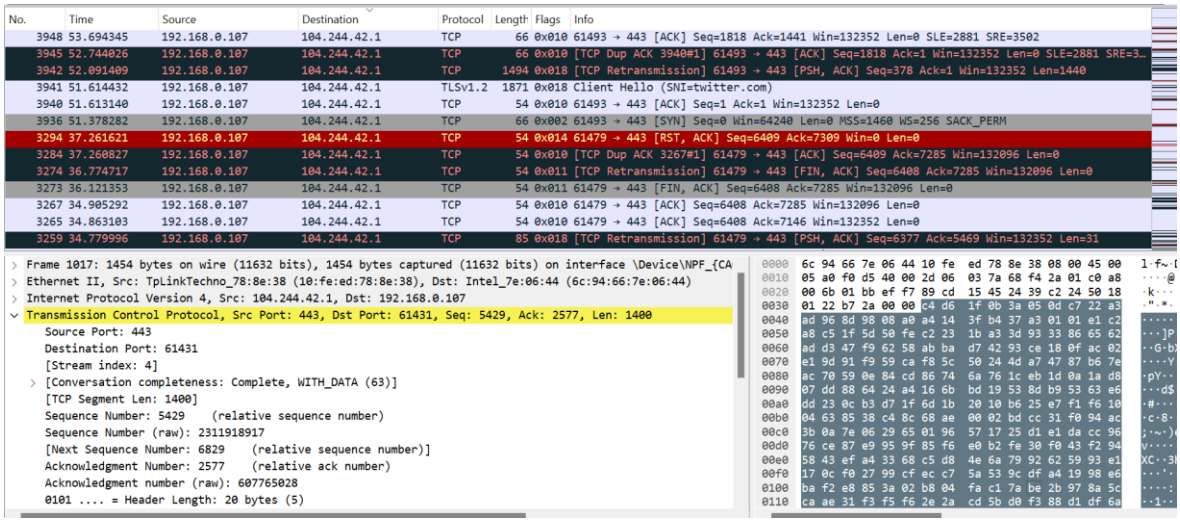
Gambar 2. Tampilan Cek Ping Host/Website Twitter/X

b. Kemudian masukkan ip adrress yang telah didapatkan sebelumnya, dengan memasukkan ip pada kolom **"lacak ip address"**

Gambar 3. Tampilan Lacak IP Address Twitter/X

c. Tampilan port-port Twitter/X pada aplikasi Wireshark

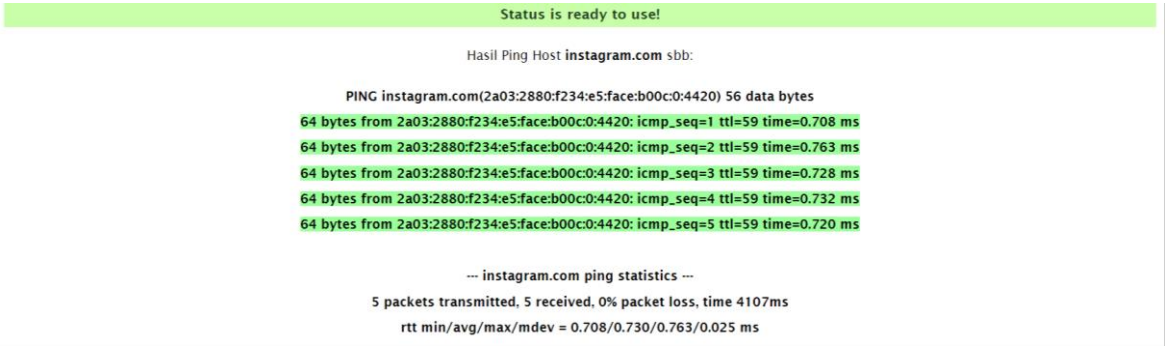
E-ISSN : 3032-2480
https://journal.feb.uniku.ac.id/digibe



Gambar 4. Tampilan port-port pada Twitter/X yang terdeteksi sebagai anomali

2. Instagram

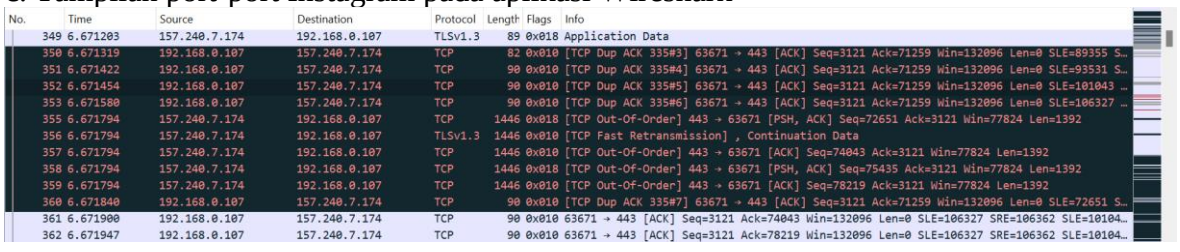
a. Ping nama host, website atau domainnya terlebih dahulu menggunakan https://ipsaya.com/



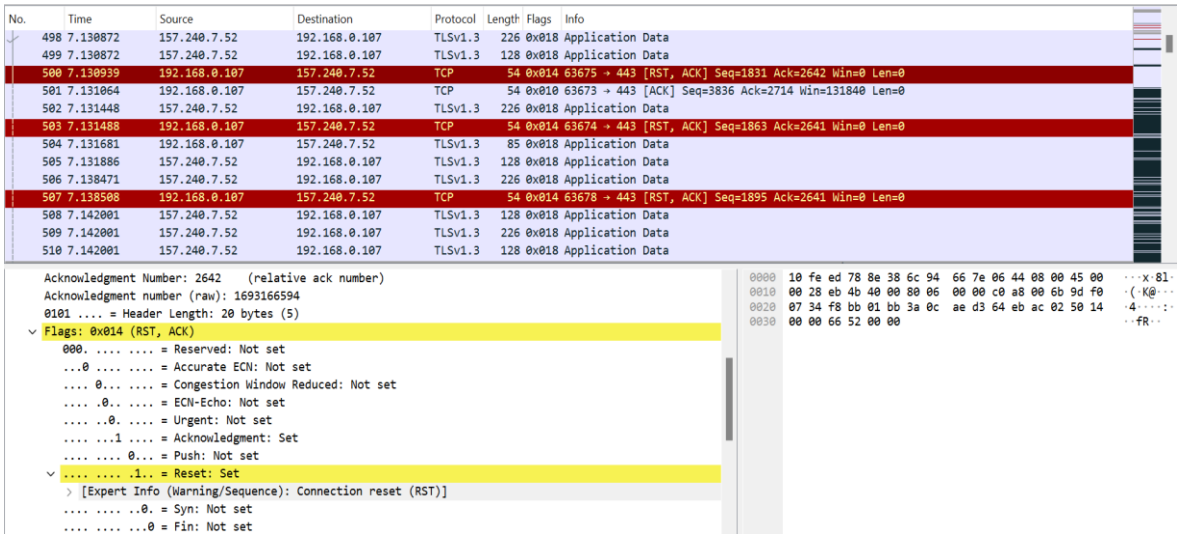
Gambar 5. Tampilan Cek Ping Host/Website Instagram

b. Pada Gambar 5. diatas menunjukkan bahwa ip adrress pada website instagram tidak terdeteksi ini dikarenakan proteksi/keamanan dari instagram/meta sudah kuat. Hal ini memungkinkan bahwa keamanan di Instagram lebih ketat dibandingkan Twitter/X.

c. Tampilan port-port Instagram pada aplikasi Wireshark



E-ISSN : 3032-2480
https://journal.feb.uniku.ac.id/digibe



Gambar 6. Tampilan Cek Ping Host/Website Instagram

Pada Gambar 4. Dan Gambar 6. Port yang berwarna biru muda merupakan "Sample inactive selected item" adalah salah satu opsi ketika ingin memeriksa konten atau isi paket data yang tidak aktif (inactive) atau paket yang telah dipilih. Ketika fitur ini diaktifkan, Wireshark akan menampilkan contoh atau sample dari isi paket yang tidak aktif (inactive) saat ini. Ini berguna dalam situasi seperti: Penelusuran Paket Tidak Aktif, Analisis Payload Data dan Pemecahan Masalah Jaringan.

Port yang berwarna abu-abu merupakan "*Sample active selected item*" adalah fitur pada Wireshark yang memungkinkan untuk melihat contoh atau sample dari isi paket yang sedang aktif (active) atau sedang dipilih. Dengan mengaktifkan fitur "Sample active selected item", Wireshark akan menampilkan contoh atau sample dari isi paket yang sedang aktif atau yang telah dipilih. Ini berguna dalam situasi-situasi seperti: Pemeriksaan Konten Paket Aktif, Analisis Payload Data dan Pemahaman Konteks Komunikasi.

Port yang berwarna hitam merupakan port yang mencurigakan dan port tersebut mengalami tingkat lalu lintas yang tinggi. Dalam konteks ini, port yang ditampilkan sebagai hitam mungkin menunjukkan bahwa lalu lintas pada port tersebut melebihi ambang batas tertentu atau telah melampaui tingkat normal yang diharapkan.

Port yang berwarna merah juga ditampilkan karena mengalami tingkat lalu lintas yang tinggi. Port-port yang ditandai merah menunjukkan bahwa lalu lintas pada port tersebut melampaui tingkat normal yang diharapkan. Hal ini dapat menunjukkan adanya masalah seperti serangan DDoS, aktivitas mencurigakan, atau bahkan kemacetan jaringan. Ditandai dengan status flag ”Reset = Set”. Yang dimana ketika flag RST dalam header TCP memiliki status "Set", ini dapat memberikan indikasi adanya masalah atau anomali dalam jaringan, seperti Gangguan konektivitas, Kesalahan konfigurasi perangkat, Aktivitas yang mencurigakan atau tidak normal dan Masalah pada salah satu *endpoint* dalam komunikasi.

Penelitian terdahulu yang dilaksanakan oleh (Riadi, 2019) dengan hasil penelitian menunjukkan analisis perbandingan menggunakan Naïve Bayes dan Support Vector Machine diperoleh bahwa hasil nilai akurasi probabilitas tertinggi dari data akses TCP dengan proses simulasi pengujian data yang di akses melalui traffic anomaly yang diakses melalui tools wireshark dan menghasilkan format data dalam bentuk cvs.

KESIMPULAN DAN SARAN

Implementasi analisis lalu lintas jaringan menggunakan Wireshark dapat menjadi alat yang efektif dalam mendeteksi anomali jaringan pada Twitter dan Instagram. Dengan menggunakan Wireshark, pengguna dapat memperoleh wawasan mendalam tentang lalu lintas jaringan yang terkait dengan Twitter dan Instagram. Dalam konteks ini, analisis lalu lintas jaringan dapat membantu mengidentifikasi serangan DDoS, serangan phishing, atau penyalahgunaan. Dengan memantau lalu lintas Twitter atau Instagram yang normal, pengguna dapat membuat profil perilaku lalu lintas yang digunakan sebagai dasar perbandingan untuk mendeteksi aktivitas yang mencurigakan atau tidak biasa. Wireshark juga dapat membantu mengidentifikasi lonjakan tiba-tiba dalam volume lalu lintas, jenis serangan yang digunakan, atau pola komunikasi yang tidak biasa, yang dapat mengindikasikan serangan atau anomali jaringan. Namun, penting untuk diingat bahwa Wireshark hanya merupakan alat pemantauan dan analisis, dan langkah-langkah tambahan seperti melaporkan masalah ke Twitter atau Instagram untuk mengambil tindakan keamanan yang sesuai akan diperlukan untuk menangani anomali yang terdeteksi. Dalam keseluruhan, implementasi analisis lalu lintas jaringan menggunakan Wireshark dapat membantu meningkatkan keamanan dan melindungi akun Twitter dan Instagram dari serangan atau penyalahgunaan.

DAFTAR PUSTAKA

Emir Risyad, Data, M., & Eko Sakti Pramukantoro. (2018). Perbandingan Performa Intrusion Detection System (IDS) Snort Dan Suricata Dalam Mendeteksi Serangan TCP SYN Flood. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *2*(9), 2615–2624. http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/2373

Gunawan, S., & Putra, M. (2023). *Analisis Lalu Lintas Jaringan pada Platform Media Sosial dan Potensi Anomali*. Jurnal Penelitian dan Pengembangan Teknologi, 20(2), 92-105.

Hadi, P., & Nugroho, Y. (2023). Pendekatan Deteksi Anomali dalam Lalu Lintas Jaringan Menggunakan Teknik Threshold dan Machine Learning. Jurnal Keamanan Informasi, 19(3), 77-92.

Muhammad, A. W. (2016). ANALISIS STATISTIK LOG JARINGAN UNTUK DETEKSI SERANGAN DDOS BERBASIS NEURAL NETWORK. *ILKOM Jurnal Ilmiah*, *8*(3), 220–225. https://doi.org/10.33096/ilkom.v8i3.76.220-225

Mukti, W. A. (2017). *Analisa dan perbandingan bukti forensik aplikasi media sosial facebook dan twitter pada smartphone android*. Repository.uinjkt.ac.id. https://repository.uinjkt.ac.id/dspace/handle/123456789/52787

Pratama, E., & Rachman, A. (2024). *Keamanan Jaringan: Ancaman dan Langkah-Langkah Perlindungan*. Jurnal Keamanan dan Sistem Informasi, 21(4), 110-123.

Putra, I. W. O. K., Purwanto, Y., & Suratman, F. Y. (2015). Perancangan Dan Analisis Deteksi Anomaly Berbasis Clustering Menggunakan Algoritma Modified K-means Dengan Timestamp Initialization Pada Sliding Window. *EProceedings of Engineering*, *2*(2). https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/1225

Riadi, I., Umar, R., & Aini, F. D. (2019). ANALISIS PERBANDINGAN DETECTION TRAFFIC ANOMALY DENGAN METODE NAIVE BAYES DAN SUPPORT VECTOR MACHINE (SVM). *ILKOM Jurnal Ilmiah*, *11*(1), 17. https://doi.org/10.33096/ilkom.v11i1.361.17-24

Sari, D., & Arifin, Z. (2022). Analisis Lalu Lintas Jaringan Menggunakan Wireshark: Fitur dan Aplikasi. Jurnal Sistem dan Teknologi Informasi, 16(1), 35-48.

Sri Winiarti, Desy Widayanti, Ulaya Ahdiani, & Ismail, T. (2022). Klasifikasi Jenis Buku Berdasarkan Cover dan Judul Buku Menggunakan Metode Support Vector Machine dan Cosine Similarity. *Sainteks/Saintek*, *19*(1), 53–53. https://doi.org/10.30595/sainteks.v19i1.13423

Sudiati, L. E. (2011). Analisa Representasi Queue pada Array vs Representasi Queue Pada Link List. *Majalah Ilmiah INFORMATIKA*, *2*(2). https://unaki.ac.id/ejournal/index.php/majalah-ilmiah-informatika/article/view/39

Susanto, R. (2022). *Implementasi Analisis Lalu Lintas Jaringan untuk Keamanan dan Kinerja Sistem*. Jurnal Teknologi Informasi dan Komunikasi, 11(2), 25-40.