https://journaledutech.com/index.php/great
Global Research and Innovation Journal (GREAT)
Volume 1, Nomor 3, 2025, Hal. 2207-2219
ISSN : 3090-3289

IMPLEMENTASI PACKET SNIFFING DENGAN WIRESHARK UNTUK ANALISIS TRAFIK JARINGAN DAN IDENTIFIKASI ANCAMAN DI SMKN 4 MATARAM

Uswatun Hasanah[1], Maspaeni[2], Emi Suryadi[3]
Rekayasa Sistem Komputer, Universitas Teknologi Mataram, Kota Mataram
E-mail: uswatunhasanahdompu7@gmail.com[1]

ABSTRAK

Penelitian ini bertujuan untuk menganalisis lalu lintas jaringan dan mengidentifikasi ancaman keamanan pada jaringan WiFi sekolah menggunakan teknik packet sniffing dengan Wireshark. Metode penelitian yang digunakan adalah action research melalui tahapan perencanaan, tindakan, observasi, dan refleksi. Pengujian dilakukan dengan passive sniffing pada jaringan WiFi sekolah untuk memantau jumlah pengguna, protokol yang digunakan, dan kualitas layanan (QoS) pada jam sibuk dan di luar jam sibuk. Selain itu, simulasi serangan Denial of Service (DoS) atau (DDoS) dilakukan dengan menggunakan teknik deauthentication flood, serangan Rogue Access Point, dan ICMP Floods untuk menguji kerentanan jaringan. Hasil penelitian menunjukkan bahwa pada jam sibuk terjadi peningkatan delay dan jitter serta penurunan throughput, sedangkan pada jam di luar jam sibuk kinerja jaringan lebih stabil. Serangan deauthentication berhasil memutus klien dari access point, Rogue Access Point berhasil menangkap paket data dari klien yang terhubung, dan ICMP Floods berpotensi mengganggu ketersediaan layanan.

Kata kunci **Wireshark, Packet Sniffing, Analisis Trafik, DoS, Rogue Access Point**

ABSTRACT

This study aims to analyze network traffic and identify security threats on school WiFi networks using packet sniffing techniques with Wireshark. The research method applied is action research through the stages of planning, action, observation, and reflection. Testing was conducted through passive sniffing on the school WiFi network to monitor the number of users, protocols used, and Quality of Service (QoS) during peak and off-peak hours. In addition, Denial of Service (DoS) attack simulations using deauthentication flood, Rogue Access Point, and ICMP Flood techniques were conducted to examine network vulnerabilities. The results showed that during peak hours, delay and jitter increased while throughput decreased, while during off-peak hours, network performance was more stable. Deauthentication attacks successfully disconnected clients from the access point, Rogue Access Point successfully captured data packets from connected clients, and ICMP Flood had the potential to disrupt service availability.

Keywords ***Wireshark, Packet Sniffing, Traffic Analysis, DoS, Rogue Access Point***

1. PENDAHULUAN

Packet sniffing adalah metode serangan yang melibatkan intersepsi semua paket yang melewati media komunikasi, baik kabel maupun nirkabel. Setelah paket ditangkap, paket-paket tersebut disusun kembali sehingga data yang dikirim oleh satu pihak dapat dicuri oleh pihak yang tidak berwenang. Hal ini dimungkinkan karena semua koneksi Ethernet pada dasarnya merupakan koneksi siaran, di mana semua host dalam grup jaringan menerima paket yang dikirim oleh satu host. Melindungi diri dari interferensi ini cukup sulit karena sifat pasif packet sniffing (penyerang tidak perlu melakukan apa pun, cukup mendengarkan) (Nasution et al., 2021).

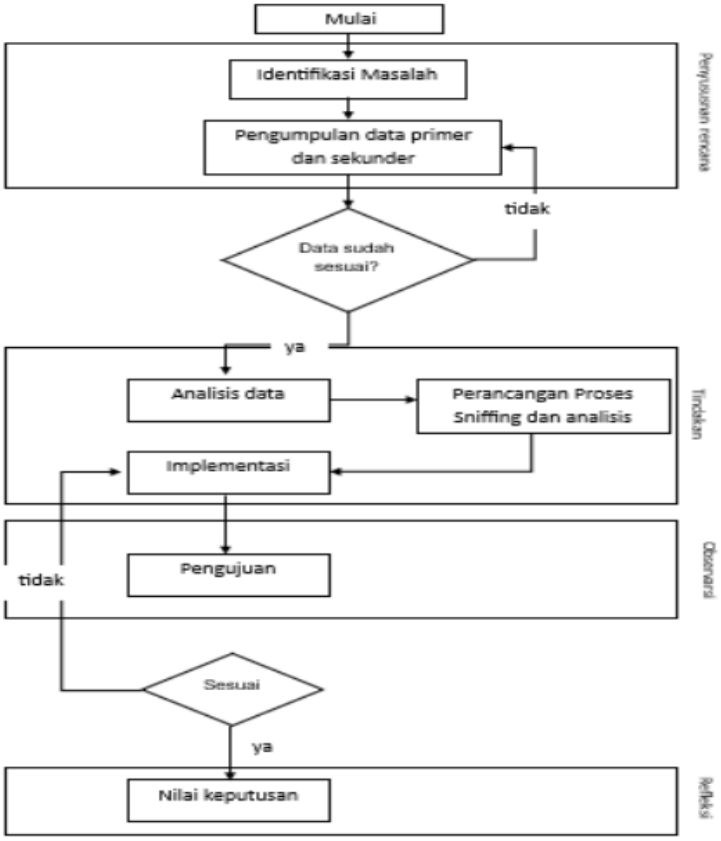
Wireshark adalah perangkat lunak yang digunakan untuk menganalisis paket data di jaringan, juga dikenal sebagai Network Packet Analyzer. Perangkat lunak ini menangkap setiap paket yang melewati jaringan dan menampilkan semua informasi paket data secara

detail. Semua jenis paket informasi dalam berbagai format protokol dapat dengan mudah ditangkap dan dianalisis. Wireshark memfasilitasi analisis kinerja jaringan (Hasbi & Saputra, 2021). Wireshark dipilih karena bersifat sumber terbuka, memiliki fitur analitis, dan banyak digunakan dalam penelitian keamanan jaringan sebelumnya.

Packet sniffing adalah teknik untuk memantau dan menangkap paket data yang melintasi jaringan komputer, baik kabel maupun nirkabel. Data yang ditangkap dapat direplikasi, sehingga informasi sensitif seperti kata sandi dapat terekspos ke pihak yang tidak berwenang (Arini et al., 2024).

2. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian tindakan, yang menggabungkan kegiatan penelitian dan tindakan nyata untuk secara langsung mengatasi permasalahan yang dihadapi di lapangan. Pendekatan ini dipilih karena sejalan dengan tujuan penelitian, yang tidak hanya mencakup analisis kondisi jaringan tetapi juga penyediaan langkah-langkah perbaikan yang dapat diterapkan di lingkungan sekolah. Metode penelitian tindakan memungkinkan peneliti untuk berpartisipasi aktif dalam setiap langkah proses penelitian, mulai dari observasi dan tindakan hingga refleksi atas hasil penelitian.



Gambar 1 Action Research

Penelitian ini menggunakan pendekatan penelitian tindakan yang terdiri dari empat tahap utama: perencanaan, tindakan, observasi, dan refleksi. Setiap tahap dilakukan secara sistematis dan berurutan untuk memecahkan masalah jaringan di dunia nyata dan menghasilkan solusi yang aplikatif.

a. Perencanaan (Planning)

Tahap ini dimulai dengan mengidentifikasi permasalahan jaringan WiFi di SMKN 4 Mataram, seperti koneksi yang lambat, gangguan akses, dan kurangnya sistem pemantauan lalu lintas. Tahap ini dilanjutkan dengan pengumpulan data primer melalui observasi dan tangkapan data Wireshark, serta data sekunder dari literatur akademis. Data yang terkumpul digunakan untuk merancang strategi analisis jaringan menggunakan Wireshark, termasuk menentukan parameter yang akan diuji, seperti delay, jitter, throughput, dan packet loss.

b. Tindakan (Action)

Pada tahap ini, para peneliti melakukan proses sniffing pasif pada jaringan sekolah menggunakan Wireshark untuk menangkap dan menganalisis paket data yang lewat. Proses ini meliputi analisis data awal, perancangan skenario pengujian, dan penerapan tindakan langsung di lapangan. Langkah ini menghasilkan data real-time tentang lalu lintas jaringan, protokol yang digunakan, dan indikasi potensi ancaman, seperti DoS atau Rogue Access Point.

c. Observasi (Observation)

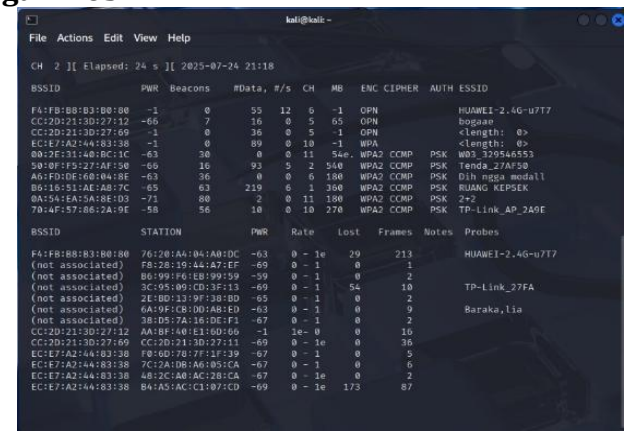
Tahap observasi dilakukan untuk memantau dan mengevaluasi hasil dari proses tindakan. Peneliti menguji paket-paket yang ditangkap dan membandingkannya dengan parameter kinerja jaringan yang telah ditentukan. Jika hasil pengujian tidak memenuhi target yang diharapkan, perbaikan akan dilakukan pada tahap tindakan sebelumnya. Proses ini memastikan bahwa setiap hasil observasi dapat dipertanggungjawabkan secara ilmiah dan akurat.

d. Refleksi (Reflection)

Tahap refleksi bertujuan untuk menilai efektivitas keseluruhan proses penelitian. Peneliti meninjau hasil pengujian dan menarik kesimpulan mengenai tingkat keberhasilan analisis jaringan menggunakan Wireshark. Selanjutnya, tahap ini digunakan untuk mengembangkan rekomendasi teknis, seperti peningkatan konfigurasi keamanan jaringan dan penerapan sistem deteksi ancaman (IDS/WIPS). Hasil refleksi menjadi dasar untuk menentukan tindakan korektif guna meningkatkan keamanan dan kinerja jaringan di masa mendatang.

3. HASIL DAN PEMBAHASAN

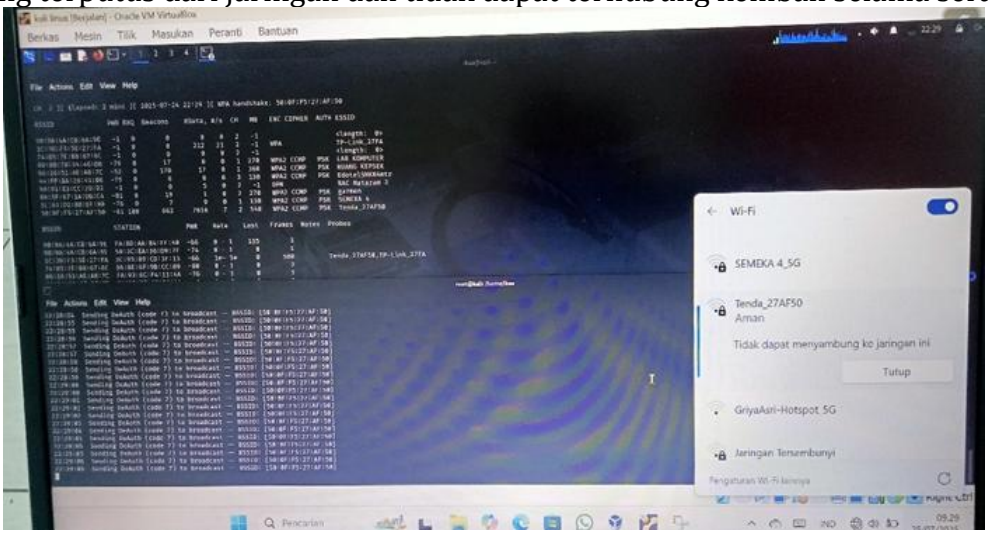
a. Simulasi serangan DoS



Gambar 2 Jaringan Wifi Target

Gambar 2 menunjukkan tampilan alat pemantauan jaringan nirkabel menggunakan mode monitor di Kali Linux, yang menampilkan daftar titik akses (AP) dan perangkat yang

terhubung ke kanal 2 pada jaringan WiFi terdekat. Salah satu target yang dipilih untuk simulasi serangan DoS (Denial of Service) adalah jaringan WiFi bernama Tenda_27AF50. Serangan DoS yang menargetkan AP ini bertujuan untuk membanjiri jaringan dengan paket-paket palsu (seperti frame deauthentication), sehingga menyebabkan klien yang terhubung terputus dari jaringan dan tidak dapat terhubung kembali selama serangan.

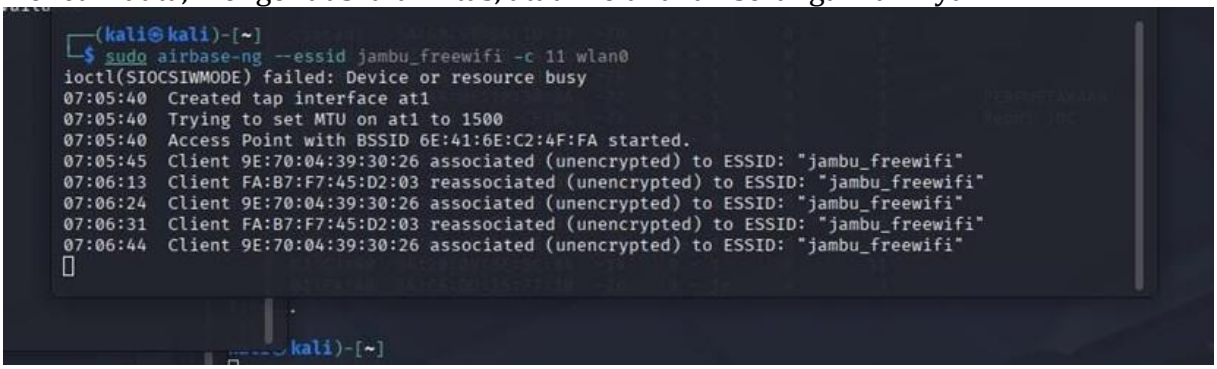


Gambar 3 koneksi terputus

Gambar 3 Menunjukkan hasil tindak lanjut dari upaya serangan DoS (Denial of Service) yang berhasil terhadap jaringan WiFi target bernama Tenda_27AF50. Desktop korban menampilkan status koneksi WiFi "Tidak dapat terhubung ke jaringan ini", meskipun jaringan tersebut masih terdeteksi dan muncul sebagai "Aman". Eksperimen ini membuktikan bahwa jaringan dengan enkripsi WPA2-PSK masih rentan terhadap serangan pemutusan koneksi jika tidak dilindungi dengan fitur keamanan canggih seperti (Bingkai Manajemen Terlindungi).

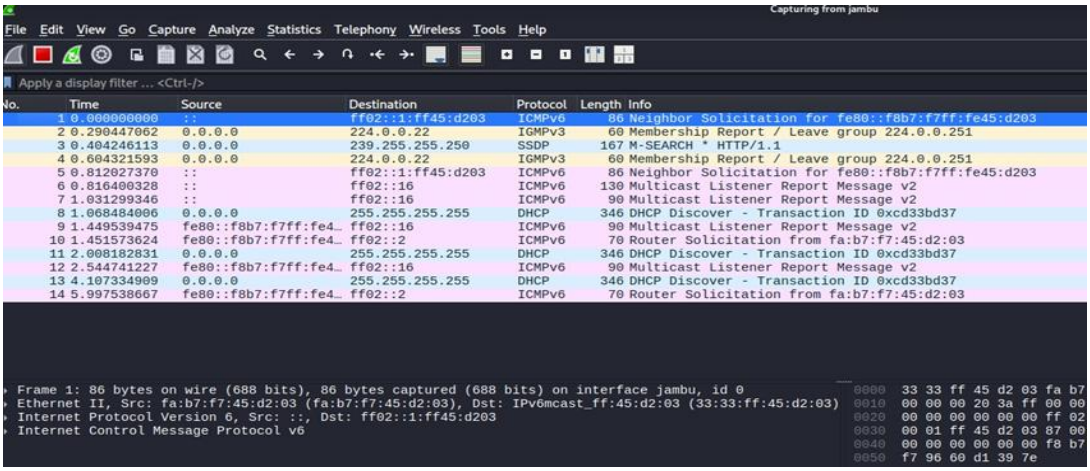
b. Simulasi Serangan Rogue Accsess Point

Rogue Access Point (Rogue AP) adalah titik akses WiFi palsu yang dibuat oleh penyerang untuk mengelabui pengguna agar terhubung ke jaringan mereka — dengan tujuan mencuri data, mengendus lalu lintas, atau melakukan serangan lainnya.



Gambar 4 Jaringan Wifi palsu

Gambar 4 Menunjukkan hasil simulasi serangan titik akses (AP) palsu yang mencoba membuat jaringan WiFi palsu bernama "jambu_freewifi". Beberapa perangkat klien dengan alamat MAC berbeda terlihat berulang kali terhubung dan terhubung kembali dengan titik akses palsu tersebut, ditandai dengan status "terhubung (tidak terenkripsi)", yang menunjukkan bahwa koneksi terjadi tanpa enkripsi atau perlindungan data.

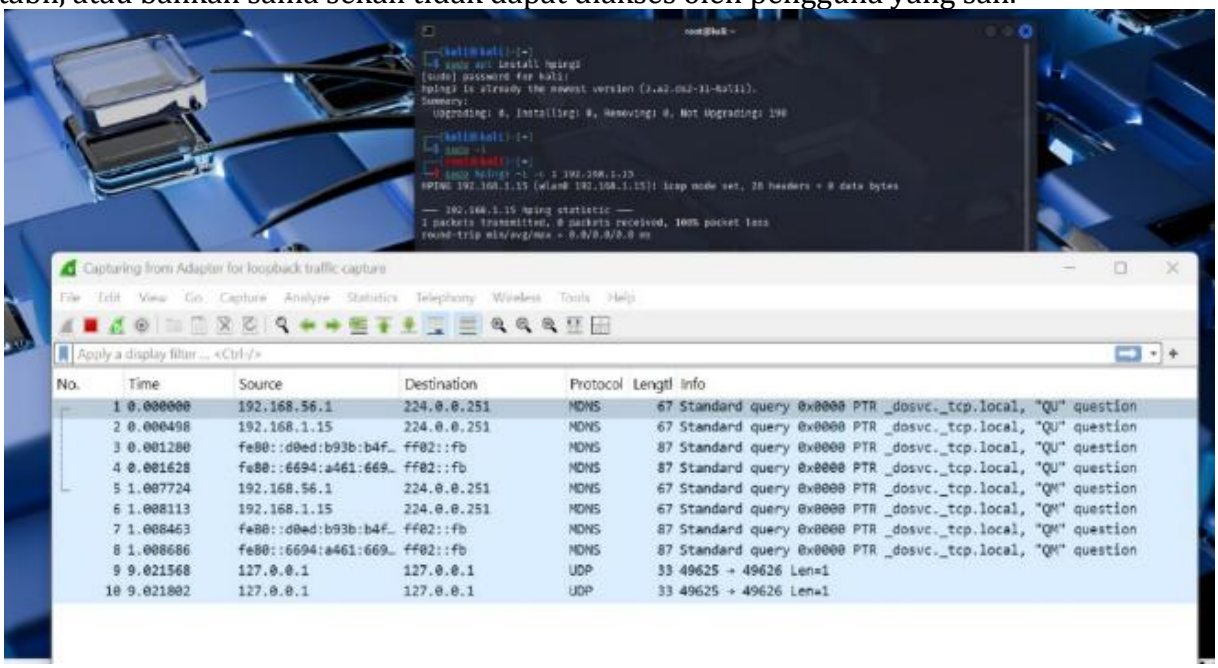


Gambar 5 trafik jaringan client

Gambar 5 Ini menunjukkan penangkapan paket menggunakan Wireshark pada antarmuka virtual yang terhubung ke jaringan WiFi palsu "jambu_freewifi". Tampilan ini menunjukkan bahwa perangkat klien telah berhasil terhubung ke titik akses palsu dan mulai mengirim serta menerima data.

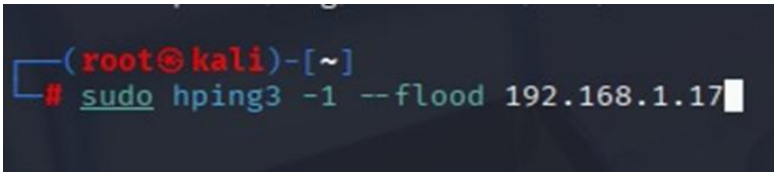
c. Simulasi Serangan DDOS

Ini adalah jenis serangan siber yang bertujuan membanjiri server, layanan, atau jaringan dengan lalu lintas dalam jumlah sangat besar sehingga sistem menjadi lambat, tidak stabil, atau bahkan sama sekali tidak dapat diakses oleh pengguna yang sah.



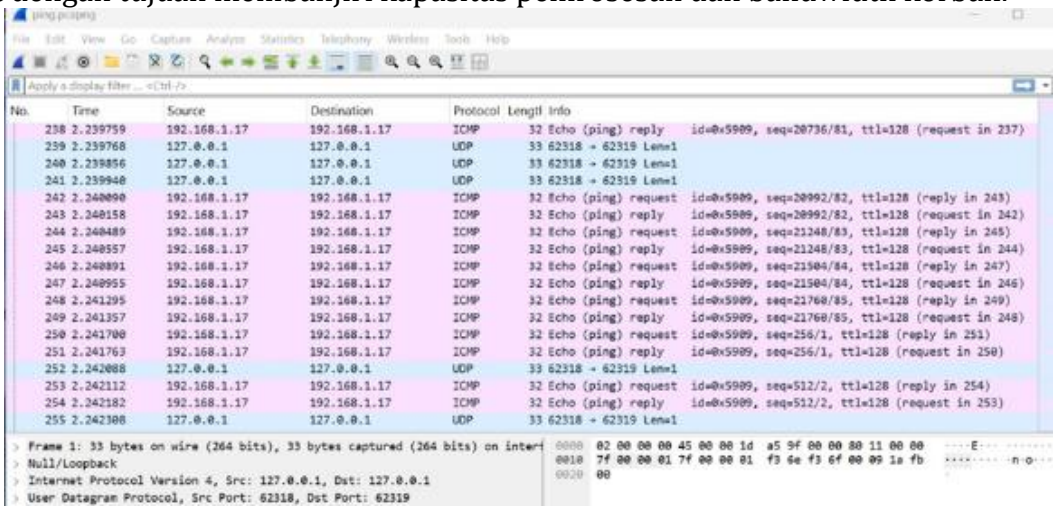
Gambar 6 Percobaan Serangan

Berdasarkan gambar di atas, saat menguji serangan menggunakan hping3, serangan tersebut ditargetkan pada IP 192.168.1.15, yang merupakan salah satu alamat di jaringan LAN sekolah.



Gambar 7 Melakukan Flood Pada IP Target

Perintah ini pada dasarnya adalah simulasi atau eksekusi Serangan Banjir ICMP, jenis serangan Denial of Service (DoS), yang mengirimkan sejumlah besar paket ICMP ke target dengan tujuan membanjiri kapasitas pemrosesan dan bandwidth korban.



Gambar 8 Hasil Ping Flood jaringan Target

Gambar di atas adalah tangkapan paket menggunakan Wireshark, yang merekam aktivitas jaringan selama serangan Banjir ICMP yang dilakukan menggunakan perintah hping3 yang telah dijelaskan sebelumnya. Banyaknya paket permintaan dan balasan yang tiba dalam waktu yang sangat singkat (hanya berselang beberapa milidetik) merupakan indikasi jelas adanya banjir paket yang menargetkan target.

d. Perhitungan Kualitas Layanan Jaringan (QoS) Saat Sibuk

1) Delay

Perhitungan ini dilakukan selama jam sibuk sekolah untuk memastikan kinerja jaringan stabil. Sebanyak 148 pengguna terhubung.

o.	Time		time 2	time 1	delay
1	0		0,000058	0	0,000058
2	0,000058		0,000065	0,000058	7,00E-06
3	0,000065		0,00007	0,000065	0,000005
4	0,00007		0,002255	0,00007	0,002185
5	0,002255		0,002301	0,002255	0,000046
6	0,002301		0,002319	0,002301	1,80E-05
7	0,002319		0,002335	0,002319	0,000016
8	0,002335		0,00235	0,002335	1,50E-05
9	0,00235		0,002368	0,00235	1,80E-05
10	0,002368		0,002383	0,002368	1,50E-05
11	0,002383		0,002403	0,002383	2,00E-05
12	0,002403		0,002421	0,002403	1,80E-05
13	0,002421		0,002435	0,002421	1,40E-05
14	0,002435		0,002552	0,002435	0,000117
15	0,002552		0,002572	0,002552	2,00E-05
16	0,002572		0,002588	0,002572	0,000016
17	0,002588		0,002605	0,002588	1,70E-05

Gambar 9 perhitungan delay

Pada hasil yang ditampilkan, penundaan menunjukkan seberapa cepat paket berikutnya diterima setelah paket sebelumnya. Nilai penundaan yang kecil menunjukkan kinerja jaringan yang baik, sementara nilai penundaan yang besar dapat menunjukkan kemacetan atau gangguan jaringan.

127998	170,6686		170,6698	170,6686	0,001186
127999	170,6698		170,6698	170,6698	3,10E-05
128000	170,6698		170,6719	170,6698	0,002057
128001	170,6719		170,6734	170,6719	0,00151
128002	170,6734		170,6734	170,6734	5,90E-05
128003	170,6734		170,6734	170,6734	5,00E-06
128004	170,6734		170,6736	170,6734	0,000128
128005	170,6736		170,6737	170,6736	0,000135
128006	170,6737		170,7016	170,6737	0,02789
128007	170,7016		170,7467	170,7016	0,045121
128008	170,7467		170,8761	170,7467	0,129384
128009	170,8761		170,8827	170,8761	0,006632
128010	170,8827		170,8908	170,8827	0,008131
128011	170,8908		170,8915	170,8908	0,00068
128012	170,8915				
				Total dela	170,8915
				Rata - Rat	0,001335
				rumus = total delay / jumlah data	

Gambar 10 Total Delay

Total penundaan mencapai 170,8915 detik dengan rata-rata penundaan sekitar 0,001335 detik (1,335 milidetik), yang menunjukkan bahwa waktu penundaan antar paket pada jaringan masih dalam batas normal untuk komunikasi jaringan nirkabel.

2) Jitter

	Jitter	
delay 1	delay 2	jitter
0,000051	7,00E-06	-4,4E-05
2,00E-06	0,000005	3,00E-06
-0,00218	0,002185	0,004365
0,002139	0,000046	-0,00209
2,80E-05	1,80E-05	-1,00E-05
2,00E-06	0,000016	1,40E-05
1,00E-06	1,50E-05	1,40E-05
-3,00E-06	1,80E-05	2,10E-05
3,00E-06	1,50E-05	1,20E-05
-5,00E-06	2,00E-05	2,50E-05
2,00E-06	1,80E-05	1,60E-05
4,00E-06	1,40E-05	1,00E-05
-0,0001	0,000117	0,00022
9,70E-05	2,00E-05	-7,70E-05
4,00E-06	0,000016	1,20E-05
-1,00E-06	1,70E-05	1,80E-05

Gambar 11 Perhitungan Jitter

0,012206	0,001186	-0,01102
0,001155	3,10E-05	-0,00112
-0,00203	0,002057	0,004083
0,000547	0,00151	0,000963
0,001451	5,90E-05	-0,00139
5,40E-05	5,00E-06	-4,90E-05
-0,00012	0,000128	0,000251
-7,00E-06	0,000135	0,000142
-0,02776	0,02789	0,055645
-0,01723	0,045121	0,062352
-0,08426	0,129384	0,213647
0,122752	0,006632	-0,11612
-0,0015	0,008131	0,00963
0,007451	0,00068	-0,00677
total jitter		170,8921
rata" jitter		0,001335
rumus = delay2-delay1		

Gambar 12 Total Jitter

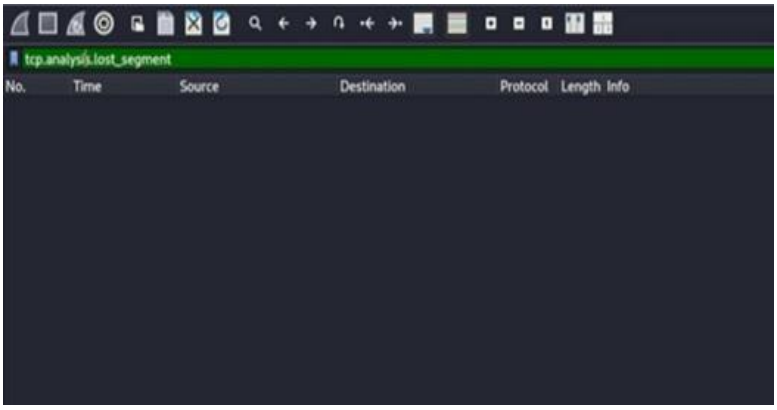
Berdasarkan data pada gambar, total jitter yang dihitung adalah 170,8921 detik, dan rata-rata jitter sekitar 0,001335 detik (1,335 milidetik). Nilai ini menunjukkan bahwa meskipun terdapat variasi waktu tunda, jaringan secara keseluruhan masih memiliki stabilitas waktu antar-paket yang cukup baik.

3) Throughput

Gambar 13 Perhitungan Throughput

Perhitungan throughput pada gambar di atas menggunakan rumus jumlah byte dibagi rentang waktu untuk menentukan jumlah data yang berhasil dikirim per detik. Dari data yang tersedia, total data yang ditransfer adalah 5.811.098 byte dalam 170,892 detik, menghasilkan kecepatan sekitar 34.004.505 byte per detik. Nilai ini menunjukkan seberapa cepat jaringan secara efektif mentransfer data selama proses pemantauan.

4) Packet Loss



Gambar 14 Paket Loss

Gambar di atas menunjukkan hasil filter tcp.analysis.lost_segment di Wireshark, yang tidak menampilkan data atau baris. Ini berarti tidak ada kehilangan paket atau segmen TCP yang terdeteksi selama proses perekaman lalu lintas jaringan. Ini merupakan indikator positif bahwa kualitas koneksi jaringan selama sesi pemantauan cukup andal.

e. Perhitungan Kualitas Layanan Jaringan (QoS) Saat tidak sibuk

1) Delay

Pada jam tidak sibuk jumlah dari pengguna yang terkoneksi sebanyak 20 pengguna.

	Time		perhitungan delay	
1	0	time 2	time1	delay
2	0,004019	0,004019	0	-0,004019
3	0,004051	0,004051	0,004019	-3,2E-05
4	0,004065	0,004065	0,004051	-1,4E-05
5	0,006508	0,006508	0,004065	-0,002443
6	0,006586	0,006586	0,006508	-7,8E-05
7	0,006612	0,006612	0,006586	-0,000026
8	0,006635	0,006635	0,006612	-2,3E-05
9	0,006662	0,006662	0,006635	-2,7E-05
10	0,006685	0,006685	0,006662	-2,3E-05
11	0,008187	0,008187	0,006685	-0,001502
12	0,00825	0,00825	0,008187	-6,3E-05
13	0,008913	0,008913	0,00825	-0,000663
14	0,008937	0,008937	0,008913	-2,4E-05
15	0,008948	0,008948	0,008937	-1,1E-05
16	0,008997	0,008997	0,008948	-4,9E-05
17	0,009008	0,009008	0,008997	-1,1E-05

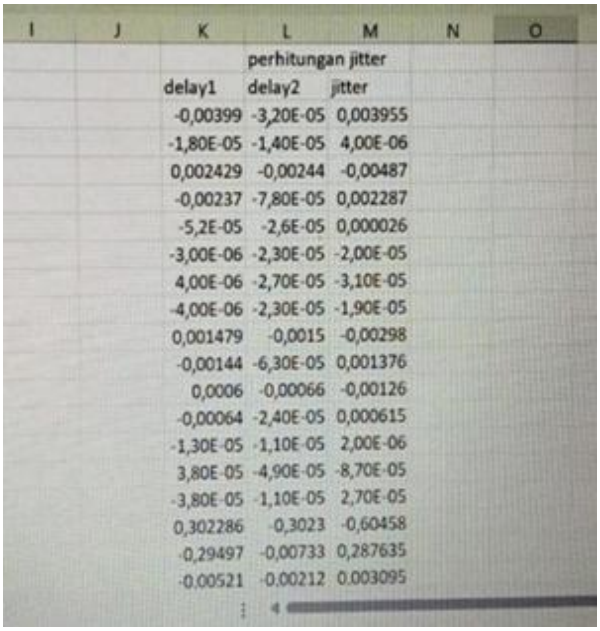
Gambar 15 Perhitungan Delay waktu siang

54218	242,190084	242,190084	242,187266	-0,002818
54219	242,19106	242,19106	242,190084	-0,000976
54220	242,192553	242,192553	242,19106	-0,001493
54221	242,221077	242,221077	242,192553	-0,028524
54222	242,22764	242,22764	242,221077	-0,006563
54223	242,254088	242,254088	242,22764	-0,026448
54224	242,269789	242,269789	242,254088	-0,015701
54225	242,269801	242,269801	242,269789	-1,2E-05
54226	242,323048	242,323048	242,269801	-0,053247
			total delay	-242,323048
			rata" delay	-0,004468844

Gambar 16 Rata Rata Delay

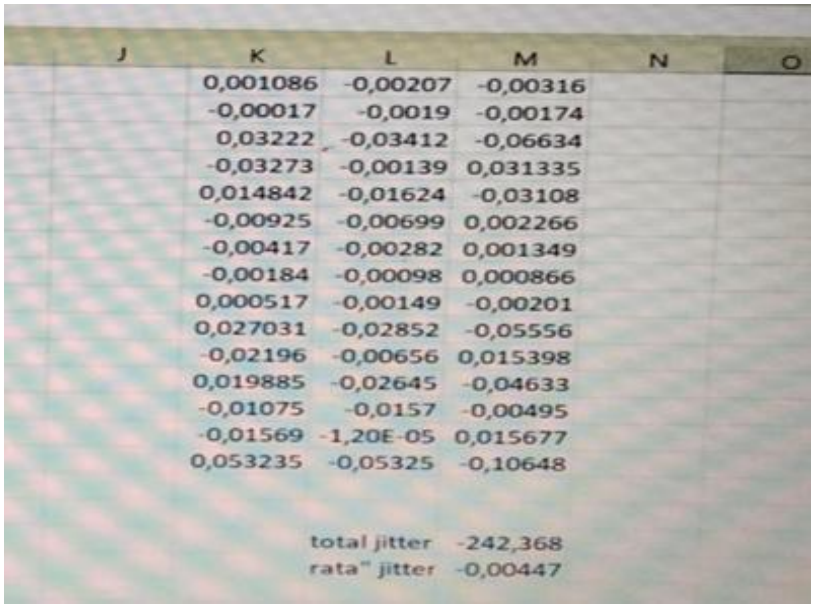
Gambar di atas menunjukkan hasil perhitungan penundaan jaringan yang dilakukan pada siang hari. Penundaan dihitung berdasarkan selisih waktu antar paket yang diterima (waktu2 - waktu1). Nilai penundaan yang relatif kecil ini menunjukkan bahwa jaringan masih mampu mengirimkan paket data dengan penundaan minimal, bahkan pada siang hari.

2) Jitter



I	J	K	L	M	N	O
		perhitungan jitter				
		delay1	delay2	jitter		
		-0,00399	-3,20E-05	0,003955		
		-1,80E-05	-1,40E-05	4,00E-06		
		0,002429	-0,00244	-0,00487		
		-0,00237	-7,80E-05	0,002287		
		-5,2E-05	-2,6E-05	0,000026		
		-3,00E-06	-2,30E-05	-2,00E-05		
		4,00E-06	-2,70E-05	-3,10E-05		
		-4,00E-06	-2,30E-05	-1,90E-05		
		0,001479	-0,0015	-0,00298		
		-0,00144	-6,30E-05	0,001376		
		0,0006	-0,00066	-0,00126		
		-0,00064	-2,40E-05	0,000615		
		-1,30E-05	-1,10E-05	2,00E-06		
		3,80E-05	-4,90E-05	-8,70E-05		
		-3,80E-05	-1,10E-05	2,70E-05		
		0,302286	-0,3023	-0,60458		
		-0,29497	-0,00733	0,287635		
		-0,00521	-0,00212	0,003095		

Gambar 17 Perhitungan Jitter Waktu Siang



J	K	L	M	N	O
	0,001086	-0,00207	-0,00316		
	-0,00017	-0,0019	-0,00174		
	0,03222	-0,03412	-0,06634		
	-0,03273	-0,00139	0,031335		
	0,014842	-0,01624	-0,03108		
	-0,00925	-0,00699	0,002266		
	-0,00417	-0,00282	0,001349		
	-0,00184	-0,00098	0,000866		
	0,000517	-0,00149	-0,00201		
	0,027031	-0,02852	-0,05556		
	-0,02196	-0,00656	0,015398		
	0,019885	-0,02645	-0,04633		
	-0,01075	-0,0157	-0,00495		
	-0,01569	-1,20E-05	0,015677		
	0,053235	-0,05325	-0,10648		
		total jitter	-242,368		
		rata" jitter	-0,00447		

Gambar 18 Rata Rata Jitter

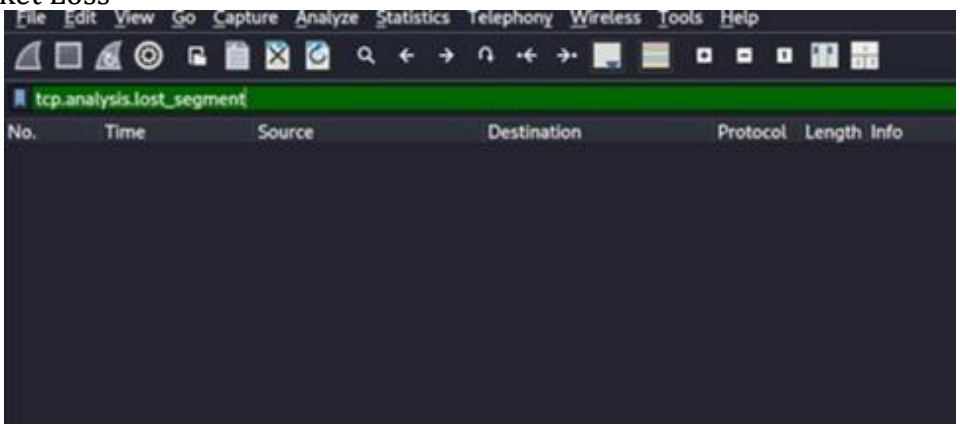
Rata-rata, jitter masih dalam batas wajar, tetapi keberadaan beberapa nilai ekstrem menunjukkan ketidakstabilan yang memerlukan investigasi lebih lanjut, terutama jika sistem ini digunakan untuk aplikasi yang membutuhkan latensi rendah. Jadi, ini bukan berarti kualitas jaringan yang buruk, melainkan hanya anomali akibat metode perhitungan atau pengaturan waktu di Wireshark/perangkat yang digunakan.

3) Throughput

Gambar 19 Perhitungan Throughput Waktu Siang

Perhitungan throughput di atas mengukur laju transfer data dengan membagi jumlah total byte yang ditransfer (1.665.850 byte) dengan total waktu yang dibutuhkan (242,323 detik), menghasilkan nilai 6.874.502 byte per detik (B/s). Hasil ini menunjukkan laju transfer data yang relatif rendah, konsisten dengan standar koneksi broadband dasar, dan dapat digunakan untuk mengevaluasi kinerja jaringan atau aplikasi, seperti streaming atau pengunduhan, yang umumnya membutuhkan throughput yang lebih tinggi untuk pengalaman yang lebih lancar.

4) Packet Loss



Gambar 20 Perhitungan Paket Loss

Ini menunjukkan bahwa semua paket berhasil dikirim dan diterima tanpa kehilangan data. Namun, perbedaan yang mencolok adalah pada siang hari, lalu lintas jaringan biasanya lebih padat karena lebih banyak perangkat yang terhubung secara bersamaan. Jadi, meskipun tidak ada kehilangan paket, kemungkinan penundaan dan jitter lebih tinggi dibandingkan di pagi hari.

f. Simulasi Serangan Jaringan

Studi ini mensimulasikan tiga jenis serangan umum pada jaringan WiFi: Serangan Deauthentication (DoS), Rogue Access Point, dan ICMP Flood (DDoS). Tujuan simulasi ini adalah untuk menentukan kerentanan jaringan WiFi sekolah terhadap ancaman yang sering muncul di lingkungan publik.

1) Serangan DoS (Deauthentication Attack)

Serangan ini mengirimkan paket deautentikasi berulang kali kepada klien, memutus koneksi mereka dari jaringan dan mencegah mereka terhubung kembali selama serangan. Hal ini disebabkan oleh frame manajemen dalam protokol 802.11 yang tidak terenkripsi (Fitri Nova dkk., 2022). Hasil pengujian menunjukkan bahwa serangan ini dapat mengurangi throughput jaringan secara signifikan dan mengganggu stabilitas koneksi WiFi.

2) Serangan Rogue Access Point

Dalam serangan ini, titik akses palsu dibuat dengan SSID yang sama dengan jaringan sekolah yang sebenarnya. Pengguna yang terhubung ke jaringan palsu tersebut tanpa sadar mengirimkan data sensitif seperti alamat IP atau paket autentikasi yang dapat dicegat oleh penyerang (Syahrulah dkk., 2018). Pengujian menunjukkan bahwa beberapa perangkat pengguna secara otomatis beralih ke jaringan palsu karena sinyalnya yang lebih kuat.

3) Serangan ICMP Flood (DDoS)

Serangan ini dilakukan dengan mengirimkan permintaan ICMP (ping) secara terus-menerus menggunakan hping3, yang menyebabkan lalu lintas jaringan yang padat dan mengurangi ketersediaan layanan (Ridho & Arman, 2020). Dampaknya terlihat pada peningkatan latensi dan penurunan kecepatan akses jaringan.

4. KESIMPULAN

Kesimpulan dari studi ini adalah jaringan WiFi di SMKN 4 Mataram menunjukkan kinerja yang bervariasi tergantung jumlah pengguna, sementara penggunaan Wireshark terbukti efektif dalam menganalisis paket dan mendeteksi potensi ancaman. Namun, serangan seperti Deauthentication, Rogue Access Point, dan ICMP Flood menunjukkan bahwa jaringan masih rentan, sehingga diperlukan langkah-langkah keamanan tambahan, termasuk Protected Management Frames (802.11w), sistem IDS/WIPS, dan kebijakan keamanan pengguna yang lebih ketat.

5. DAFTAR PUSTAKA

Arini, A., Luthfi Arsalan, M., & Teja Sukmana, H. (2024). Keamanan Jaringan Wi-Fi Terhadap Serangan Packet Sniffing Menggunakan Firewall Rule (Studi Kasus : Pt. Akurat.Co). Cyber Security Dan Forensik Digital, 6(2), 30–38. https://doi.org/10.14421/csecurity.2023.6.2.4075

Fitri Nova, Pratama, M. D., & Prayama, D. (2022). Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos. JITSI : Jurnal Ilmiah Teknologi Sistem Informasi, 3(1), 1–7. https://doi.org/10.62527/jitsi.3.1.59

Hasbi, M., & Saputra, N. R. (2021). ANALISIS QUALITY OF SERVICE (QOS) JARINGAN INTERNET KANTOR PUSAT KING BUKOPIN DENGAN MENGGUNAKAN WIRESHARK. 12(1), 17–23.

Milan, R. M. S., & Tri Rochmadi, T. R. (2024). Analisis Dan Monitor Sniffing Paket Data Jaringan Lokal Dengan Network Analyzer Wireshark. Cyber Security Dan Forensik Digital, 6(2), 62–68. https://doi.org/10.14421/csecurity.2023.6.2.4279

Nasution, M. H., Nasution, K., & Sulaiman, O. K. (2021). Implementasi Aplikasi Cain and Abel Dalam Penyadapan Paket Data Pada Jaringan Wifi. Seminar Nasional Teknik (SEMNASTEK) UISU, 4(1), 108–112.

Pandari, J. L. J., & Sulistyo, W. (2023). Implementasi Intrusion Detection System (IDS) untuk Mendeteksi serangan Metasploit Exploit Menggunakan Snort dan Wireshark. Jurnal Pendidikan Teknologi Informasi (JUKANTI), 6(1 SE-Artikel), 41–50.

Ridho, M. A., & Arman, M. (2020). Analisis Serangan DDoS Menggunakan Metode Jaringan Saraf Tiruan. Jurnal Sisfokom (Sistem Informasi Dan Komputer), 9(3), 373–379. https://doi.org/10.32736/sisfokom.v9i3.945

Syahrulah, F., Bhawiyuga, A., & Data, M. (2018). Implementasi Sistem Pendeteksi Rogue Access Point Dengan Metode Perhitungan Nilai Round Trip Time. Jurnal

Pengembangan Teknologi Informasi Dan Ilmu Komputer (J-PTIIK) Universitas Brawijaya, 2(12), 7367–7373.

TAMSIR ARIYADI, Irwansyah, I., & Huda Mubarok, M. S. (2024). Analisis Keamanan Jaringan Wifi Mahasiswa Ubd Dari Serangan Packet Sniffing. Jurnal Ilmiah Informatika, 12(01), 53–58. https://doi.org/10.33884/jif.v12i01.8739

Umasugi, A. (2022). Analisis keamanan jaringan wifi terhadap packet sniffing di Kampus A Universitas Muhammadiyah Maluku Utara. PRODUKTIF : Jurnal Ilmiah Pendidikan Teknologi Informasi, 6(2), 597–602.