PERIPHERAL
JURNAL ILMU KOMPUTER
Penerbit: Universitas Cokroaminoto Palopo

Peripheral: Jurnal Ilmu Komputer **Vol. 1, No. 2, Tahun 2025**

Analisis Keamanan Jaringan Nirkabel dari *Packet Sniffing* pada Kantor Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kota Palopo

Muh. Syaiful Haq[1], Siaulhak[2]
[12]Universitas Cokroaminoto Palopo
haq@gmail.com[1], siaulhak@uncp.ac.id[2]

Article Info
Kata Kunci:
Analisis Keamanan Jaringan Nirkabel dari *Packet Sniffing*

Abstrak
Hasil dalam penelitian analisis keamanan jaringan nirkabel dari *packet sniffing* menggunakan *aplikasi wireshark* pada Kantor Dinas Penanaman Modal Dan Pelayana Terpadu Satu Pintu Kota Palopo adalah sebagai berikut: Jaringan nirkabel pada Kantor Dinas Penanaman Modal Dan Pelayana Terpadu Satu Pintu Kota Palopo masih cukup lemah keamananya karena masih rentan terhadap *packet sniffing* yang dapat membahayakan data-data pada user. Analisis jaringan nirkabel berhasil dilakukan dengan fokus analisis hasil pada protocol jaringan yang tidak aman yaitu *Hypertext Transfer Protocol* (HTTP).

PENDAHULUAN

Keamanan jaringan menjadi sangat penting dan harus diperhatikan, jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat dicuri datanya oleh para *cracker*, baik jaringan LAN maupun *wireless*. Pada saat data dikirim melewati beberapa terminal untuk sampai tujuan berarti akan memberikan kesempatan kepada *user* lain yang tidak bertanggung jawab untuk menyadap atau mengubah data, bahkan sampai mencuri data tersebut. Dalam pembangunan perancangannya, sistem keamanan jaringan yang terhubung ke internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang

berada dalam jaringan tersebut secara efektif dan meminimalisir terjadinya serangan oleh para *hacker* maupun *cracker.* (Husaifah, dkk., 2021).

Setiap jaringan internal perusahaan atau kantor mempunyai satu atau lebih *server,* contohnya *web server*, *mail server*, DNS server, dan lain-lain. *Server-server* itu merupakan tujuan akses penjahat *cyber* melalui internet. Setiap perusahaan yang mempunyai *server farm* tentu juga ingin *server* mereka aman dari jaringan luar, dan tidak ingin jaringan internal diakses oleh pihak-pihak yang tidak berwenang. Oleh karena itu, sistem keamanan jaringan dibutuhkan untuk membatasi *privilage level* jaringan luar mengakses *server,* dan melakukan *blocking* terhadap *traffic network* yang dianggap berbahaya terhadap jaringan internal. Penggunaan jaringan *wireless* di kantor penanaman modal kota Palopo dapat digunakan pada karyawan maupun masyarakat mempunyai keperluan dikantor penanaman modal. Untuk meningkatkan pelayanan karyawan serta masyarakat, hal-hal yang perlu di antisipasi yaitu serangan terhadap fasilitas internet pada setiap ruangan.

Salah satu potensi penyerangan keamanan jaringan yaitu *packet sniffing*. *Packet sniffing* merupakan proses penyadapan atau *memonitoring* terhadap paket data di jaringan komputer, yang diantaranya dapat mencuri serta mengambil seluruh lalu lintas jaringan yang lewat tanpa peduli kepada siapa pemilik paket itu yang pada curi. Beberapa aksi *sniffin*g lebih menakutkan lagi, biasanya *cracker* melakukan *sniffing* ditempat rawan, misalnya seorang user melakukan *sniffing* di universitas tempat belajar, atau seorang *cracker* melakukan sniffing untuk mencuri *password email*, bahkan mencuri data transaksi melalui kartu kredit maupun hal lainnya. Pada kenyataanya, masih sedikit solusi yang tepat untuk mendeteksi maupun untuk mencegah aktivitas *sniffing* ini. Sistem deteksi penyusup jaringan yang ada saat ini umumnya mampu mendeteksi berbagai serangan tetapi tidak mengambil tindakan lebih lanjut

Wireshark merupakan perangkat lunak open-source yang andal untuk menganalisis jaringan. Alat ini memungkinkan pengguna untuk langsung menangkap paket-paket data yang bergerak dalam jaringan (Team, 2024). *Wireshark* dapat menangkap semua paket data yang lewat pada jaringan kepada siapa paket itu dikirimkan. Disaat inilah biasanya terjadi pencurian data pribadi atau identitas oleh *hacker* jika tidak berhati-hati dalam beraktivitas di dunia maya. Data yang biasanya di incar adalah data yang cukup penting misalnya data akun, *email, username* dan *password*, dan lain-lain sehingga dapat merugikan orang- orang yang beraktivitas di dunia maya.

Wireshark merupakan salah satu *software* yang digunakan untuk menganalisa terhadap protokol jaringan dan mengaudit keamanan jaringan. *Wireshark* juga mempunyai kemampuan untuk mem*block* lalu lintas yang lewat pada jaringan LAN, mencuri *password,* dan menyadap protokol-protokol umum yang aktif, dengan adanya *wireshark* maka dipastikan di selesaikan terhadap masalah yang timbul agar tidak terjadi, bisa diartikan bahwa *wireshark* merupakan aplikasi atau *software* untuk menganalisa gerak-gerik yang mencurigakan.

Menurut setiawan & prasetyaningsih (2019), *packet sniffing* merupakan proses pengendusan paket data pada sistem jaringan komputer, yang diantaranya dapat memonitor dan menangkap semua lalu lintas jaringan yang lewat tanpa peduli kepada siapa paket itu di kirimkan. Contoh dampak *negatif sniffing*, seseorang dapat melihat

paket data informasi seperti *username* dan *password* yang lewat pada jaringan komputer.

Menurut Agustiara, dkk., (2022), *sniffing* dalam pengertian berarti mengendus, sedangkan dalam ilmu keamanan jaringan *sniffing* merupakan aktifitas menangkap paket-paket data yang lewat dalam sebuah jaringan. *Sniffing* sendiri biasanya digunakan untuk menangkap informasi-informasi vital dari sebuah jaringan seperti *password*, *email text*, dan *file transfer*. *Sniffing* biasanya menyerang protokol-protokol seperti *Telnet*, HTTP, POP, IMAP, SBM, FTP, dan lain-lain. Dalam metode *hacking, sniffing* dibagi menjadi dua bagian *passive sniffing* dan *active sniffing:*

Passive sniffing tindak kejahatan berupa penyadapan yang pelaku lakukan tanpa mengubah isi paket data yang *server* kirimkan kepada klien. Hal tersebut seringkali membuat korban tidak menyadari adanya serangan pada data mereka. *Sniffing* jenis ini sering terjadi di perangkat *hub*. Perangkat tersebut bertugas untuk mengirimkan paket data untuk klien. Meski demikian, hal tersebut tidak terjadi pada *switch* karena mereka bertugas untuk mengatur *traffic* jaringan dengan membaca *MAC address*.
Active sniffing adalah kebalikan dari *passive sniffing*. Pelaku mengubah isi paket data yang ada pada jaringan yang *server* kirim kepada klien. Jenis *sniffing* satu ini banyak terjadi pada *ARP poisoning* dan m*an in the middle attack* (MITM). Mengapa serangan ini tidak terjadi pada perangkat *hub*, Apabila hal tersebut dilakukan, maka serangan bisa ditemukan pada *switch* jaringan. Oleh sebab itu, pelaku kejahatan memilih target lain, bukan perangkat *hub*, melainkan MITM dan ARP *poisoning*.

Seperti yang sudah dipaparkan, *sniffing* adalah salah satu kejahatan *siber* yang bekerja melalui jaringan *wifi* publik yang tidak memiliki keamanan yang terjamin. Pertama-tama pelaku akan menargetkan korban terlebih dahulu, kemudian melancarkan aksinya dengan memindahkan data melalui jaringan dari satu perangkat ke perangkat lain tanpa dapat diketahui oleh korban. Pada proses transfer data, terjadi aliran data secara bolak-balik dari client dan pengguna. Di situlah *sniffer* bekerja, mereka menangkap paket-paket data yang dikirimkan menggunakan sebuah *tools*. Setelah itu, *sniffer* akan menangkap salah satu data dan kemudian tersangkut pada komputer korban dengan memanfaatkan alamat IP perangkat, dan kemudian sniffer akan mengirimkan sebuah program berbahaya dan tersembunyi yang dapat mengambil seluruh data korban. Lebih lengkapnya, simak penjelasan di bawah ini untuk mengetahui bagaimana pelaku *sniffing* dapat dengan mudah mendapatkan akses pada data-data kamu.

Cara kerja *sniffing* adalah seorang *sniffer* akan mengumpulkan paket data yang melintas pada jaringan, karena jaringan yang digunakan merupakan jaringan publik, membuat orang lain dengan mudah mengetahui siapa saja yang terkoneksi dengan jaringan tersebut.

Cara kerja *sniffing* adalah mengubah bentuk data dari paket-paket yang sudah dikumpulkan. Jadi, data awal yang dikirimkan masih berbentuk binary karena merupakan data yang terenkripsi. Kemudian, yang awalnya berbentuk binary tersebut selanjutnya dikonversikan menjadi bentuk yang lebih mudah dimengerti oleh manusia.

Cara kerja *sniffing* adalah dengan menganalisis data yang sudah dikonversikan kedalam bentuk *blok protocol* berdasarkan sumber transmisi data yang digunakan oleh korban. Saat data sudah dapat dibaca dengan mudah, selanjutnya *sniffer* akan

menganalisis data yang diperlukan dan yang tidak diperlukan, serta mereka juga menilai seberapa berharganya data tersebut.

Cara kerja *sniffing* adalah *sniffer* akan mulai memproses pengambilan data dengan memindahkannya ke perangkat pribadi mereka menggunakan tools tertentu dan membuat data kamu akan dimanfaatkan dan disebarluaskan kepada pihak-pihak yang tidak bertanggung jawab.

Server merupakan pusat kontrol dari jaringan komputer. *Server* berfungsi untuk menyimpan informasi dan untuk mengelola suatu jaringan komputer. *Server* akan melayani seluruh *client* atau *workstation* yang terhubung ke jaringan. Sistem operasi yang digunakan pada *server* adalah sistem operasi yang khusus yang dapat memberikan layanan bagi *workstation.*

Gambar 1. *Server*
(Sumber: https://www.networkworld.com/2024)

Workstation adalah komputer yang terhubung dengan sebuah LAN. Semua komputer yang terhubung dengan jaringan dapat dikatakan sebagai *workstation*. Komputer ini yang melakukan akses ke *server* guna mendapat layanan yang telah disediakan oleh *server*.

Gambar 2 *Workstation*
(Sumber: https://www.indiamart.com/2024)

Network Interface Card (NIC) adalah *expansionboard* yang digunakan supaya komputer dapat dihubungkan dengan jaringan. Sebagian besar NIC dirancang untuk jaringan, protokol, dan media tertentu. NIC biasa disebut dengan LAN card.

Gambar 3 *Network Interface Card*
(Sumber: https://www.indiamart.com/2024)

Kabel adalah saluran yang menghubungkan antara 2 *workstation* atau lebih. Jenis- jenis kabel yang digunakan dalam jaringan antara lain kabel *coaxial*, *fiber optic*, dan *Twised Pair*.

Gambar 4 Kabel
(Sumber: https://www.shopee.co.id/2024)

Switch adalah perangkat yang juga berfungsi untuk menghubungkan *multiple* komputer. *Switch* secara fisik sama dengan *hub* tetapi logikalnya sama dengan barisan *brigde*. Peningkatan kecerdasan dibandingkan *hub*, yaitu memiliki pengertian terhadap alamat MAC (*Medium* Access Control) atau pada *link layer* model OSI sehingga hanya mengirimkan data pada *port* yang dituju (*unicast*). Hal ini berbeda dengan *hub* yang mengirimkan data ke semua *port* (*broadcast*). Proses kerjanya adalah apabila paket data datang, *header* dicek untuk menentukan di segmen mana tujuan paket datanya. Kemudian data akan dikirim kembali (*forwaded*) ke segmen tujuan tersebut.

Gambar 5 *Switch*
(Sumber: https://www.indoworx.com/2024)

Router adalah perangkat yang berfungsi menghubungkan suatu LAN ke suatu *internetworking*/WAN dan mengelola penyaluran lalu-lintas data di dalamnya. *Router* akan menentukan jalur terbaik untuk komunikasi data. *Router* bekerja pada *layer network* dari model OSI untuk memindahkan paket-paket antar jaringan menggunakan alamat logikanya. *Router* memliki tabel *routing* yang melakukan pencatatan terhadap semua alamat jaringan yang diketahui dan lintasan yang mungkin dilalui serta waktu tempuhnya. *Route*r bekerja hanya jika protokol jaringan yang dikonfigurasi adalah protokol yang *routable* seperti TCP/IP atau IPX/SPX. Ini berbeda dengan *bridge* yang bersifat *protocolin dependent*. (Eryadi 2020).

Gambar 6 *Router*
(Sumber: https://www.indoworx.com/2024)

Wireshark adalah program penganalisa jaringan yang sangat populer saat ini, tapi anehnya program ini kebanyakan dikenal bukan karena fungsi utamanya melainkan karena sering digunakan untuk keperluan *hacking* pemula. Karena terjadi pembelokan fungsi inilah meretas DC merasa sangat menarik untuk membahas fungsi dan pengertian *Wireshark* serta bagaimana cara menggunakan *wireshark*. *Wireshark* juga

merupakan program *Network Protocol Analyzer* alias penganalisa protokol jaringan yang lengkap. Program ini dapat merakam semua paket yang lewat serta menyeleksi dan menampilkan data tersebut sedetail mungkin, misalnya postingan komentar kamu di blog atau bahkan *username* dan *password*. Sebenarnya *wireshark* tidak di desain untuk *hacker*. Fungsi utamanya tidak diperuntukkan untuk *hacking*. *Wireshark* utamanya dibuat untuk administrator jaringan untuk dapat melacak apa yang terjadi didalam jaringan miliknya atau untuk memastikan jaringannya bekerja dengan baik, serta tidak ada yang melakukan hal-hal buruk pada jaringan itu. Menurut Jamaluddin, Hasbullah, Suaeb, (2018) *Wireshark* adalah alat penganalis paket jaringan *ope source* yang menangkap paket data yang melewati jaringan dan menyajikan dalam bentuk yang dapat dimengerti. *Wireshark* dapat dianggap sebagai pisau tentara *Swiss* karena dapat digunakan dalam situasi yang berbeda seperti masalah jaringan, operasi keamanan, dan protokol pembelajaran internal. *Wireshark* mendukung berbagai protokol mulai dari TCP, UDP, dan HTTP ke protokol canggih seperti *AppleTalk*.

METODE

Jenis Penelitian

Jenis penelitian yang akan digunakan dalam penelitian ini adalah penelitian kualitatif dengan model penelitian Simulasi, berasal dari kata simulate yang artinya berbuat seakan-akan ada kejadian. Sebagai metode mengajar, simulasi dapat diartikan cara penyajian pengalaman belajar dengan mengguakan situasi tiruan untuk memahami tentang konsep, prinsip, atau keterampilan tertentu. Pada penelitian ini dilakukan penyerangan jaringan pada kantor dinas penanaman modal kota palopo menggunakan komputer yang telah di hubungkan ke jaringan internet kantor dinas penanaman modal kota palopo dan di gunakan untuk login ke suatu *website* menggunakan *username* dan *password*. Metode simulasi ini dapat digunakan untuk pembelajaran maupun proses penelitian (Hasbullah, dkk., 2019).

Adapun tahap-tahap dari model simulasi yang *identification, Analysis, Design, Implement, Enforcement* dan *Enhancemen* maka dari itu umpan balik dari evaluasi in bisa berdampak pada perubahan dalam arsitektur dan teknologi yang digunakan saat ini.

Adapun penjelasan tahap-tahap sebagai berikut:

1. *Identification*

Pada tahapan ini dilakukan proses identidikasi masalah yang dijadikan dasar dari jurnal-jurnal, dan buku untuk menjuang penelitian.

2. *Analysis*

Analisa Kebutuhan, tahap analisis dilakukan untuk mengumpulkan data yang dibutuhkan dalam penelitian. Pada tahap ini bertujuan untuk memperoleh informasi mengenai harapan dari pengguna sistem atau aplikasi yang akan dikembangkan.

3. *Design*

Desain sistem, tahap desain dilakukan untuk membuat simulasi rancangan yang siap untuk diimplementasikan. Pada tahap ini akan dibuat rancangan sistem seperti arsitektur sistem.

4. *Implement*

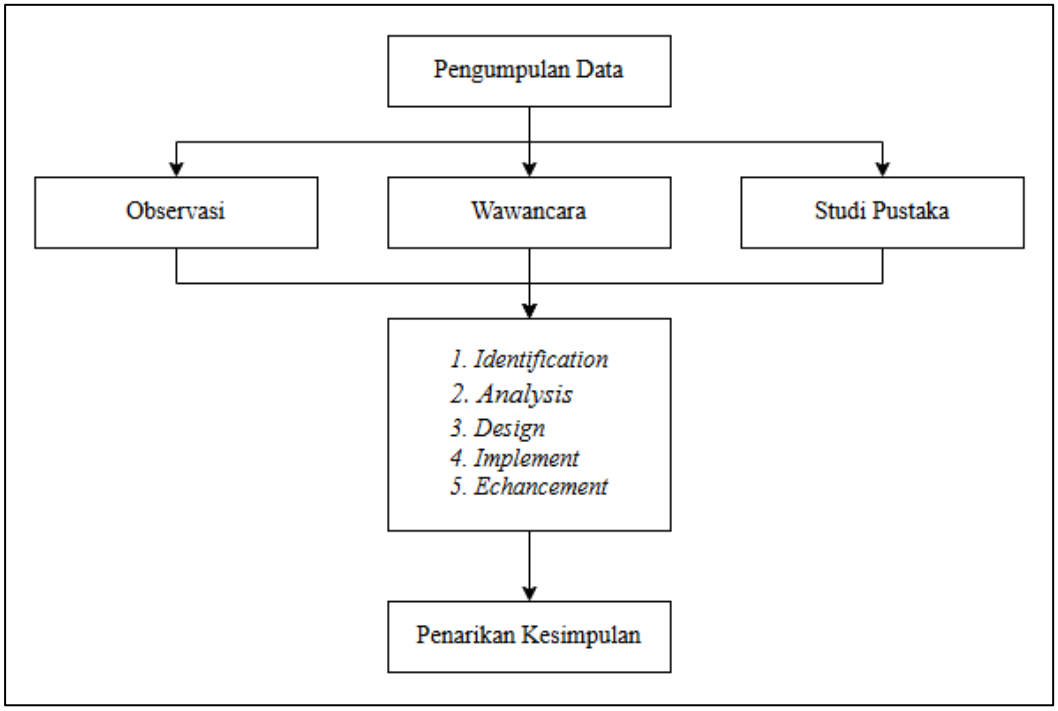
Unit-unit individu program atau program digabung dan diuji sebagai sebuah sistem lengkap untuk memastikan apakah sesuai dengan kebutuhan perangkat lunak atau tidak.

5. *Enhancement*

Hasil analisis untuk memahami perilaku sistem memberikan pemahaman yang lebih dalam menganalisis sistem yang sedang diteliti serta membatu dalam mengekplorasi data numerik yang dihasilkan oleh simulasi.

Tahapan Penelitian

Adapun tahapan penelitian dalam penelitian ini dapat dilihat pada gambar dibawah.



Gambar 8. Tahapan Penelitian

1. Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan penulis untuk memperoleh data dan informasi dalam penelitian ini yaitu:

a. Studi Pustaka

Tahapan selanjutnya yaitu studi pustaka dimana peneliti mengumpulkan data yang dilakukan dengan cara mencari referensi yang relevan menyangkut dengan penelitian yang akan dilakukan. Referensi bisa diperoleh dari skripsi, buku-buku ilmiah, jurnal *online*, artikel serta buku yang ada di perpustakaan Universitas Cokroaminoto Palopo.

b. Observasi

Teknik observasi merupakan salah satu teknik pengumpulan data yang dilakukan melalui suatu pengamatan yang disertai dengan pencatatan terhadap situasi atau perilaku dari objek atau subjek yang menjadi sasaran. Hal ini dilakukan berdasarkan pengetahuan dan gagasan yang sudah diketahui, sehingga didapatkan berbagai informasi yang dibutuhkan untuk melanjutkan penelitian di Kantor Dinas Penanaman Modal Kota Palopo.

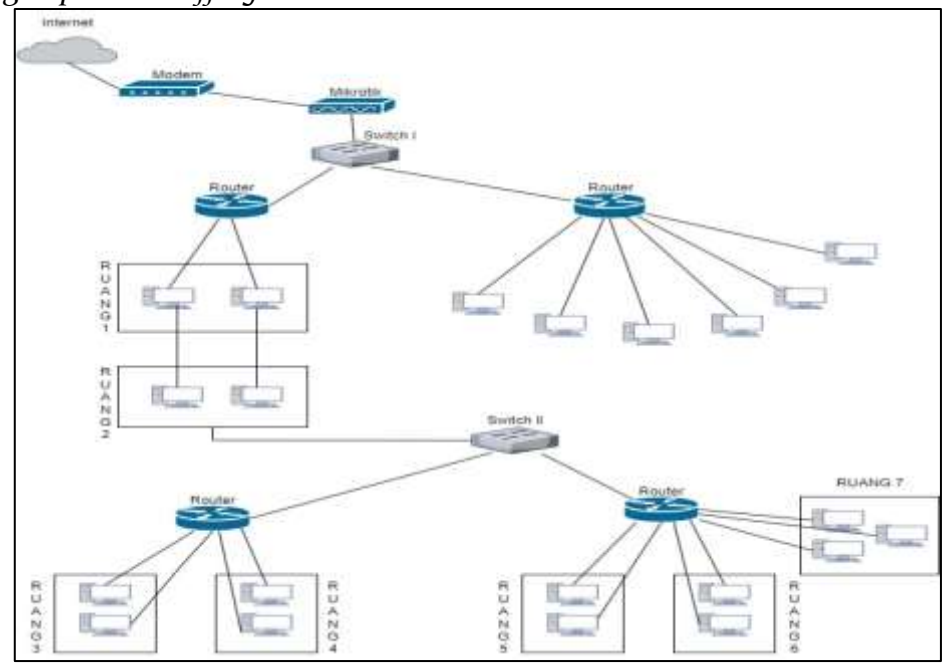
c. Wawancara

Wawancara menurut Sugiyono (2016:194), menyatakan bahwa wawancara digunakan sebagai teknik pengumpulan data jika peneliti ingin melakukan studi pendahuluan untuk menemukan permasalahan yang harus diteliti, serta juga apabila peneliti ingin mengetahui hal-hal dari responden yang lebih mendalam.

2. Analisis Sistem

a. Sistem yang berjalan

Sistem jaringan yang berjalan kantor dinas Penamaman Modal Kota palopo menggunakan topologi *Tree* terdiri dari satu modem serta memiliki 22 komputer *client* yang terhubung pada 2 *switch* dan 4 *router* yang dimana jalur distribusi utama ke server menggunakan sebuah mikrotik. Pada Kantor dinas Penanaman Modal Kota Palopo di perlukan menguji sistem keamanan jaringan dari serangan *packet sniffing* maka dari itu penelitian ini akan dilakukan penyerangan menggunakan simulasi penyerangan *packet sniffing wireshark.*



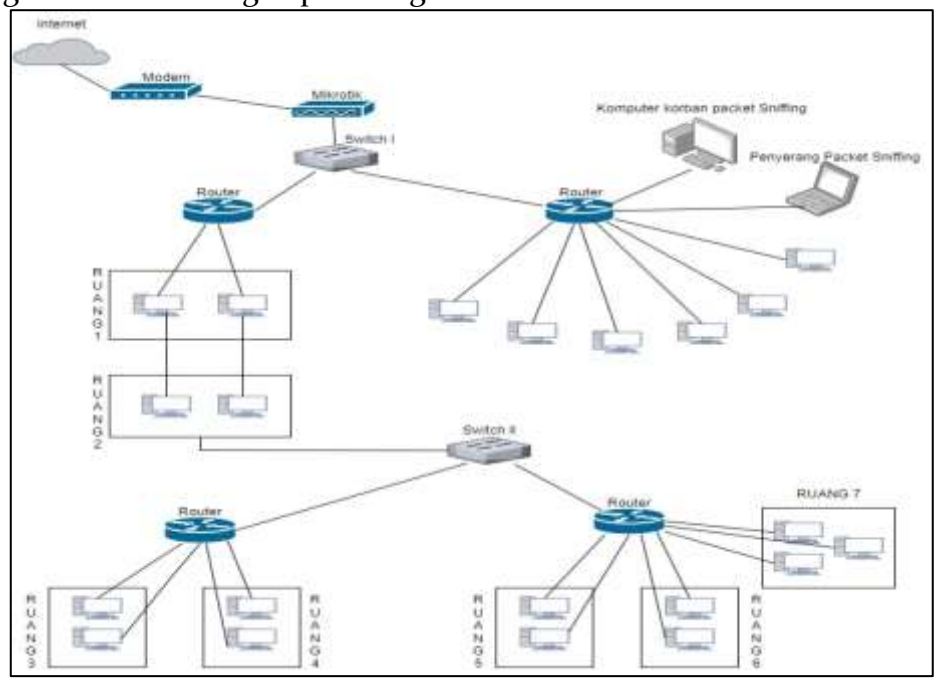
Gambar 9. Sistem yang berjalan

b. Sistem yang diusulkan

Sistem yang akan diusulkan yaitu peneliti akan menambahkan sebuah PC/laptop untuk software wireshark untuk mengetahui apakah jaringan Kantor Dinas Penanaman Modal Kota Palopo aman terhadap serangan packet sniffing dengan wireshark ini dapat merakam semua paket yang lewat serta menyeleksi dan menampilkan data tersebut sedetail mungkin. Sebenarnya wireshark tidak di desain untuk hacker. Fungsi utamanya tidak diperuntukkan untuk hacking. Wireshark utamanya dibuat untuk administrator jaringan untuk dapat melacak apa yang terjadi didalam jaringan miliknya atau untuk memastikan jaringannya bekerja dengan baik, serta tidak ada yang melakukan hal-hal buruk pada jaringan itu.

Pada penelitian ini penulis ingin memberikan gambaran bagaimana simulasi dari penyerangan *packet sniffing* yang menggunakan keamanan maupun tidak. Penulis juga menyarankan untuk menerapkan keamanan enkripsi *WPA2-PSK* pada *wi-fi* untuk meningkatkan keamanan, dengan menerapkan keamanan tersebut, hanya pengguna

yang memiliki akses yang dapat mengakses jaringan, sehinggan serangan *sniffing* oleh pihak yang tidak berwenang dapat dicegah.



Gambar 10. Sistem yang diusulkan

2. **Penarikan Kesimpulan**

Tahapan terakhir ini bertujuan untuk menarik kesimpulan dari hasil analisis jaringan kantor dinas penanaman modal kota palopo Hasil dengan dilakukannya analisis uji coba dalam penelitian ini menunjukkan bahwa apakah penyerangan *packet sniffing* pada kantor dinas penanaman modal kota Palopo dapat di cegah atau tidak, agar jaringan tersebut terhindar dari pencurian data dengan menggunakan metode serangan *sniffing* pada jaringan nirkabel. Pada saat target mengakses *website* menggunakan jaringan kantor dinas penanaman modal kota palopo menggunakan *browser*, kemudian *browser* meminta data pada server, server langsung mengirim data yang di minta dalam bentuk teks biasa melalui TCP tanpa adanya perlindungan lebih. Sehingga pada saat melakukan proses *sniffing,* seluruh data yang melewati komputer penyerang akan ter-*capture* pada aplikasi *wireshark* dan data tersebut dapat dibaca langsung oleh penyerangan.

HASIL DAN PEMBAHASAN

Hasil pengumpulan data dengan jenis penelitian adalah penelitian kualitatif dengan model penelitian simulasi yang telah peneliti terapkan dalam penelitian ini, dimulai dengan melakukan observasi dan wawancara pada lokasi penelitian yaitu pada Kantor Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kota Palopo. Hasil penelitian adalah analisis keamanan jaringan nirkabel dari serangan packet menggunakan *Wireshark.* Adapun tahapan dalam penelitian ini yaitu: *identification, Analysis, Design, Implement,* dan *Enhancemen.*

1. *Identification*

Tahap pertama yaitu identifikasi masalah pada tahap ini peneliti melakukan pengumpulan data dari jaringan nirkabel Kantor Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kota Palopo. Data-data dari kebutuhan dari user (pengguna) dan menganalisisnya. Seperti pada lokasi Penelitian ini, jaringan *wireless*

atau WI-FI pada Kantor Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kota Palopo ini masih rentan terhadap serangan.

Berdasarkan hasil identifikasi di Kantor Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kota Palopo yaitu rentannya jaringan nirkabel terhadap serangan karena kurangnya perhatian terhadap keamanan jaringan tersebut sehingga data-data tidak terjamin kerahasiaanya. Oleh karena itu penulis memberikan sebuah solusi yaitu dengan melakukan packet sniffing untuk mengetahui tingkat kerentanan dari jaringan nirkabel tersebut.

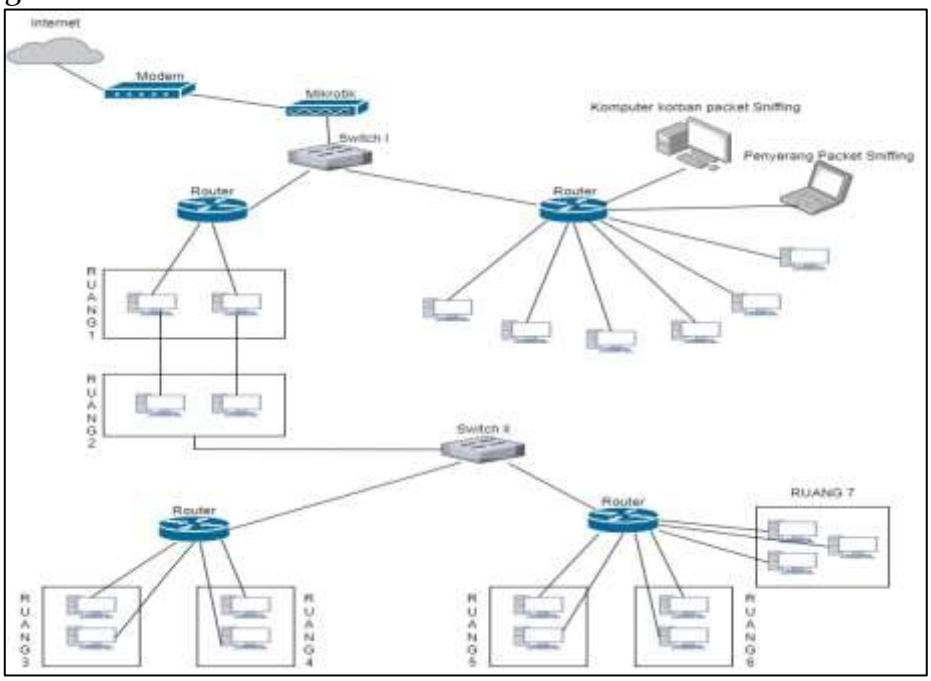
2. *Analysis*

a. Analisis Permasalahan

Berdasarkan hasil analisis dari sebuah keadaan yang ada di Kantor Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kota Palopo ini, maka unruk mengatasinya dilakukan analisis keamanan jaringan nirkabel dari *packet sniffing*, dimana peneliti memanfaatkan aplikasi *Wireshark* untuk melakukan analisis tersebut.

b. Analisis Sistem yang Diusulkan

Gambaran bagaimana simulasi dari penyerangan *packet sniffing* yang menggunakan keamanan maupun tidak. Penulis juga menyarankan untuk menerapkan keamanan enkripsi WPA2-PSK pada wi-fi untuk meningkatkan keamanan, dengan menerapkan keamanan tersebut, hanya pengguna yang memiliki akses yang dapat mengakses jaringan, sehinggan serangan sniffing oleh pihak yang tidak berwenang dapat dicegah.



Gambar 11. Sistem yang Diusulkan

c. Analisis Kebutuan

a) Kebutuhan Perangkat Lunak

Hasil analisis kebutuhan sistem dalam penelitian ini akan menggunakan perangkat lunak (*software*) dalam penerapannya, dapat dilihat pada tabel.

Tabel 2. Kebutuhan Perangkat Lunak

Perangkat Lunak	Keterangan
Windows 10	Sistem operasi yang digunakan dalam penelitian
Wireshark	*Software* yang digunakan menganalisis
Drow.io	*Software* yang digunakan untuk membuat topologi sistem

b) Kebutuhan Perangkat Keras

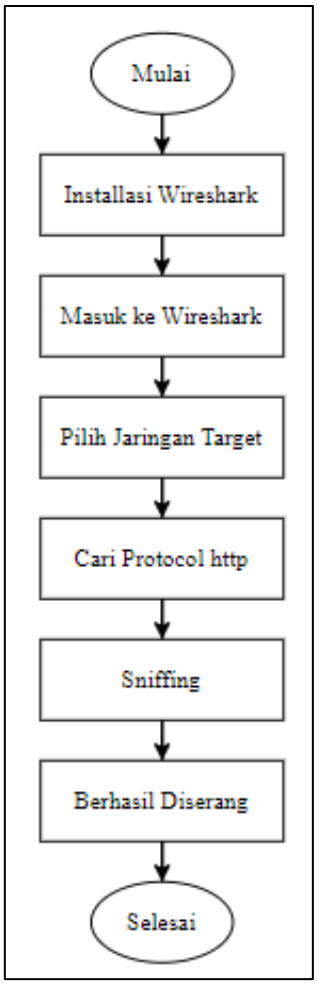
Hasil analisis kebutuhan perangkat keras dalam penelitian ini adalah akan menggunakan beberapa perangkat keras (*hardware*), dapat dilihat pada tabel.

Tabel 3. Kebutuhan Perangkat Keras

Perangkat Keras	Keterangan
Laptop	Digunakan untuk menganalisis
Mikrotik	Perangkat jaringan yang dianalisis

3. *Design*

Design skema penyerangan yang dilakukan pada penyerangan packet sniffing pada jaringan nirkabel Kantor Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kota Palopo menggunakan *Wireshark* yaitu dengan cara melakukan penyerangan terhadap router dengan memanfaatkan *protocol* http. Adapun bentuk penyerangan tersebut akan penulis gambarkan pada sebuah *flowchart*, yang dapat dilihat pada gambar di bawah ini.



Gambar 12. *Design* Skema Penyerangan

Pada skema penyerangan di atas, langkah-langkah yang dilakukan adalah sebagai berikut:

a. *Installasi Wireshark*

Tahap pertama yang dilakukan untuk melakukan penyerangan menginstal *wireshark* sebagai *software* analisis.

b. Masuk ke *Wireshark*

Tahap ini adalah langkah kedua, dimana penulis masuk dalam *software* untuk mulai melakukan penyerangan.

c. Jaringan Target

Jaringan target ini adalah jaringan yang dianalisis dalam hal ini adalah jaringan nirkabel dari Kantor Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kota Palopo.

d. *Protocol HTTP*

Protocol http ini adalah salah satu *protocol transfe*r data atau komunikasi antar komputer melalui *browser web* untuk meminta halaman *web* dari server *web*. *Protocol* ini menjadi jalur penyerangan dengan memanfaat ketidak amanan dari protocol tersebut.

e. *Sniffing*

Sniffing ini adalah serangan yang dilakukan untuk medapatkan informasi atau data dari pengguna seperti *username* dan *password*.

f. Berhasil Diserang (Hasil Penyerangan)

Tahap terakhir dalam skema penyerangan adalah merangkum infomasi-informasi penting yang berhasil diperoleh dari pengguna.

4. *Implement*

Pada tahap ini peneliti melakukan implementasi penyerangan untuk menguji keamanan jaringan nirkabel pada Kantor Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kota Palopo. Tahap *Implement* ini terbagi menjadi dua tahap yaitu *installasi Wireshark* dan melakukan serangan paket sniffing menggunakan *Wireshark*.

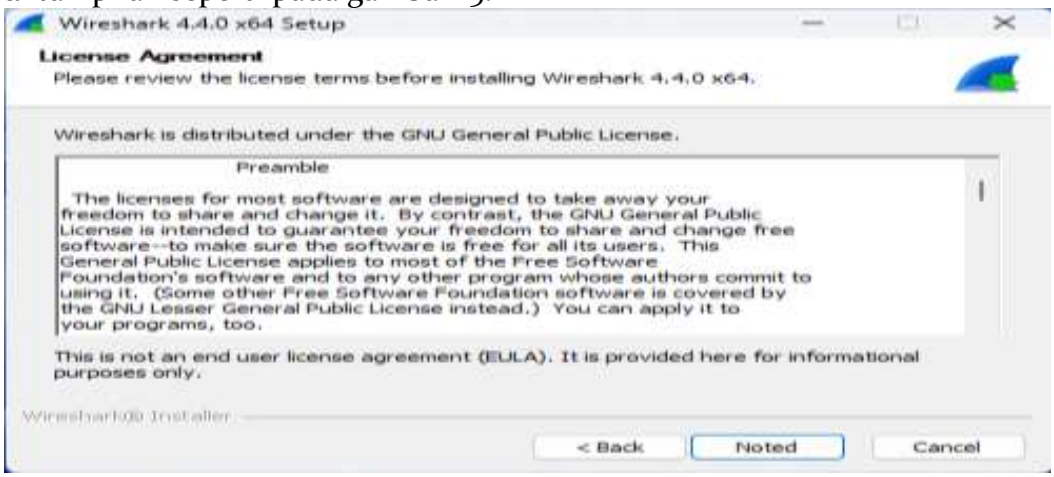
a. *Installasi Wireshark*

Download wireshark pada browser lalu melakukan *Installasi*, klik kanan pada file yang telah di *download* kemudian pilih "*run administrator*". Dapat dilihat pada gambar 13 dan 14.

Gambar 13. *Download Wireshark*

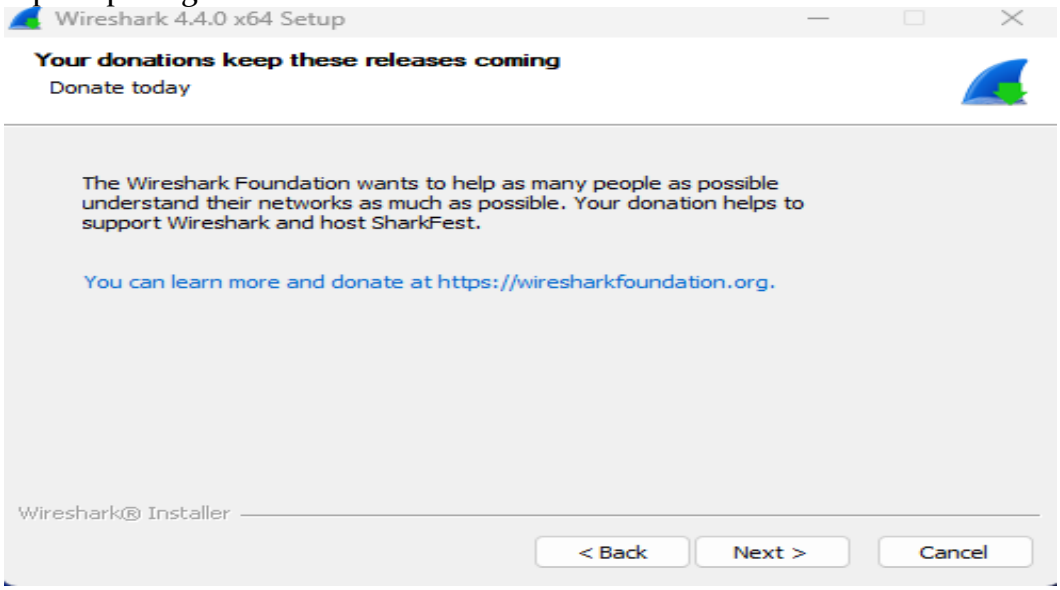
Gambar 14. *Installasi Wireshark* 1

Selanjutnya setelah melewati dua tahapan pada gambar 13 dan 14, maka akan muncul tampilan seperti pada gambar 15.



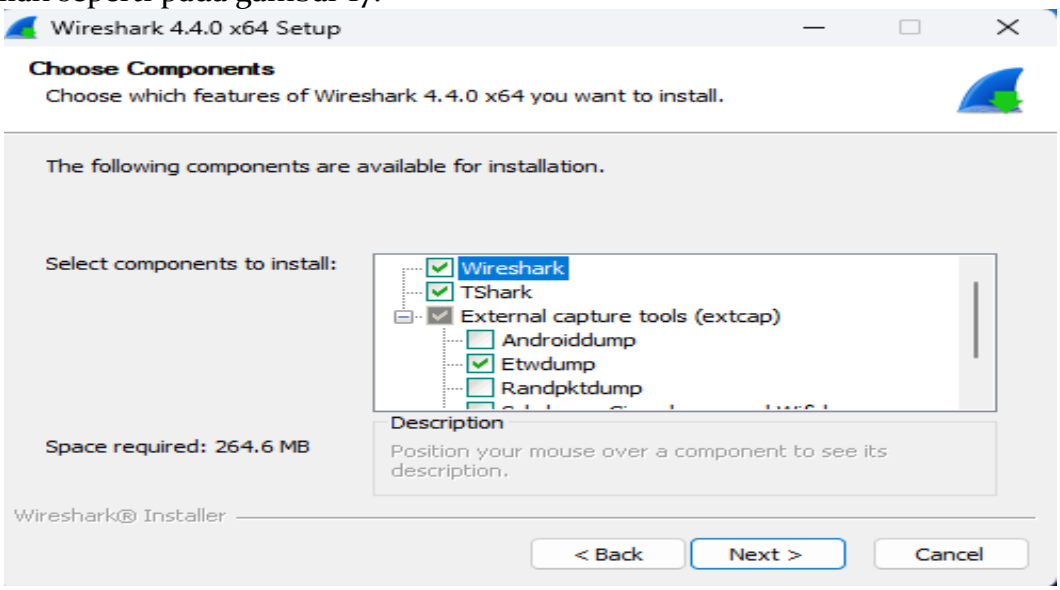
Gambar 15. *Installasi Wireshark* 2

Selanjutnya setelah diklik "*noted*" pada gambar 15, kemudian muncul tampilan seperti pada gambar 16.



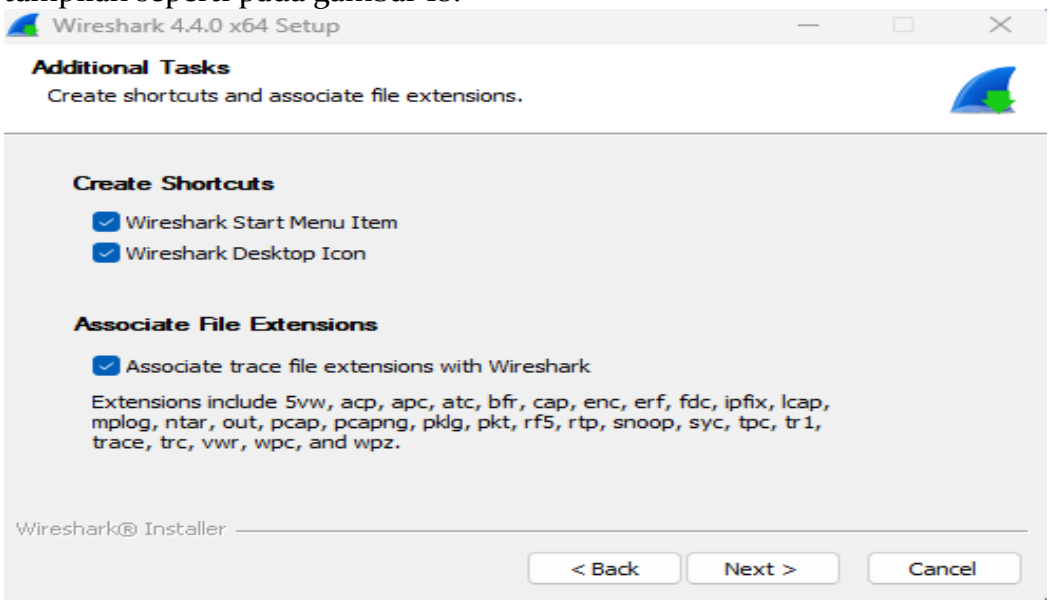
Gambar 16. *Installasi Wireshark* 3

Setelah memilih "*next*" pada gambar 16 diatas, maka selanjutnya muncul tampilan seperti pada gambar 17.



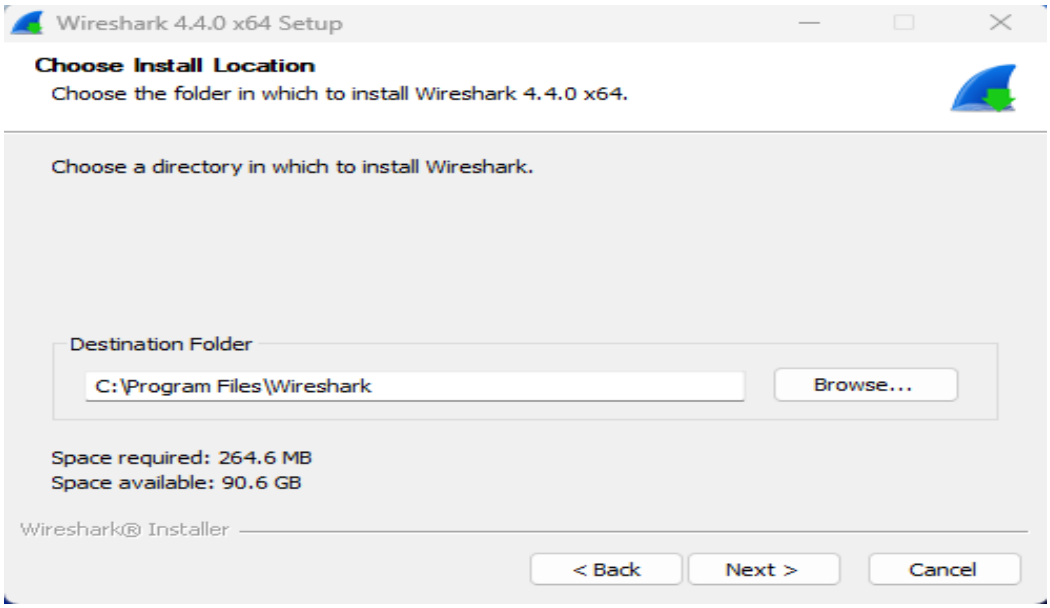
Gambar 17. *Installasi Wireshark* 4

Setelah mencentang "*wireshark, tshark,* dan *etwdump"* pada bagian *select components to iinstall* kemudian klik "*next"* pada gambar 17, maka selanjutnya muncul tampilan seperti pada gambar 18.



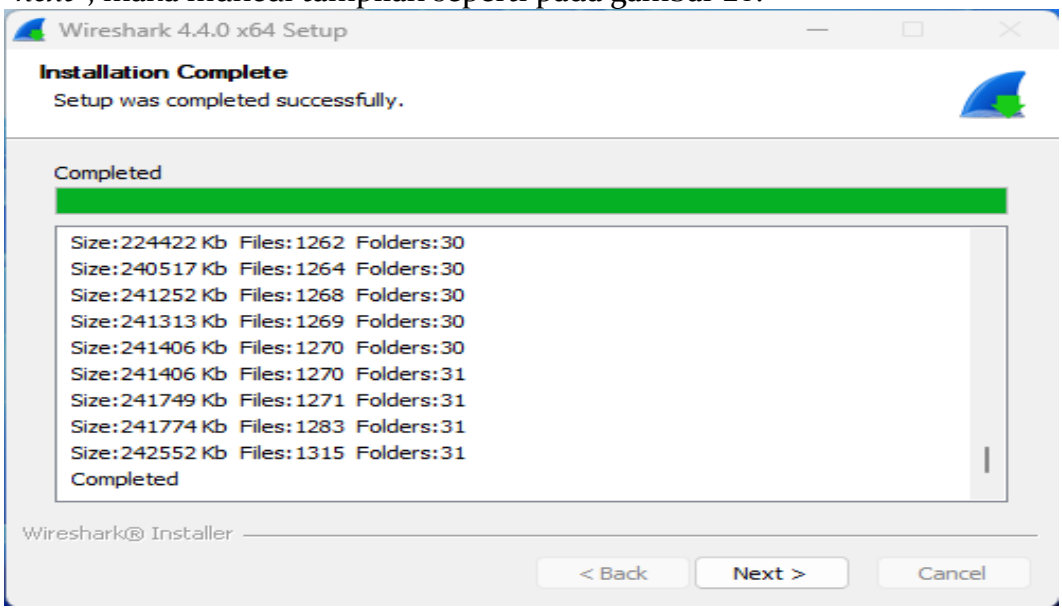
Gambar 18. Installasi Wireshark 5

Selanjutnya pada gambar 18 centang bagian "*create shortcute* dan *associate file extensions*" dan klik "*next*", maka muncul tampilan selanjutnya seperti pada gambar 19.



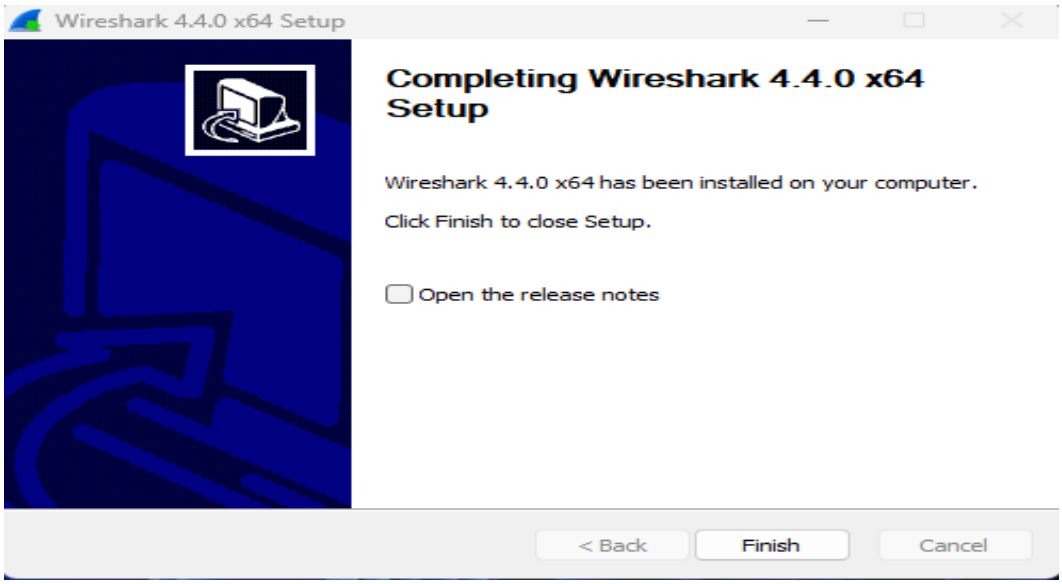
Gambar 19. *Installasi Wireshark* 6

Kemudian pada gamber 19 adalah memilih lokasi penyimpanan file *wireshark* lalu setelah dipilih C:\program files*wirwshark* sebagai lokasi penyimpanan kemudian klik "*next*", maka muncul tampilan seperti pada gambar 20.



Gambar 20. *Installasi Wireshark* 7

Pada gambar 20 adalah proses installasi dari semua proses yang telah dilakukan, jika proses installasi telah selesai lalu klik "*next*", maka muncul tampilan seperti pada gambar 21.



Gambar 21. *Installasi Wireshark* 8

Pada gambar 21 adalah tahapan terakhir dari proses installasi wireshark, selanjutnya adalah klik "*finish"* dan penginstallan wireshark berhasil dilakukan.

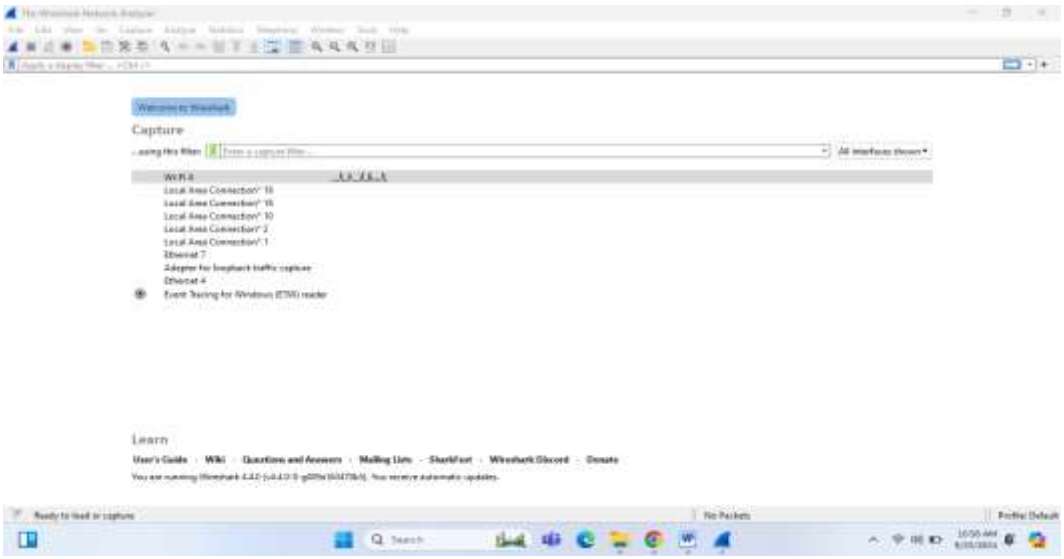
Tabel 4. *Installasi Wireshark*

Installasi Wireshark
1. *Download wireshark* pada *browser*. 2. Klik kanan pada file *wireshark* kemudian pilih *run administrator*. 3. Selanjutnya klik *next* 4. Klik *noted* 5. Klik *next* 6. Kemudian centang pada *wireshark, tshark,* dan *etwdump"* dibagian *select components to iinstall* kemudian klik "*next"* 7. Kemudian centang lagi bagian "*create shortcute* dan *associate file extensions*" dan klik "*next*". 8. Selanjutnya pilih lokasi penyimpanan dan klik *next*. 9. Kemudian tunggu proses penginstallan selesai lalu klik *next*. 10. Kemudian yang terakhir klik *finish*

b. Pengujian *Packet Sniffing*

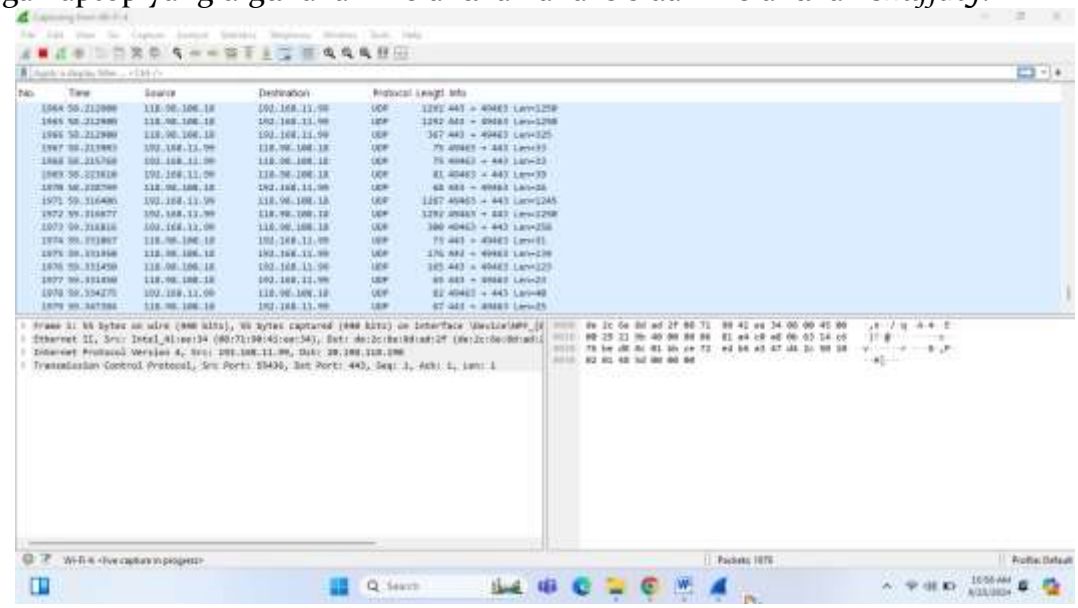
Pengujian *packet sniffing* ini untuk menganalisis dan melihat *packet* data yang dikirim melalui jaringan dalam hal ini adalah sistem jaringan nirkabel yang digunakan pada Kantor Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kota Palopo. Pada tahap ini peneliti melakukan pengujian *packet sniffing* dengan cara berada dalam jaringan atau terhubung dalam jaringan yang diuji.

Langkah pertama dilakukan dalam melakukan pengujian packet sniffing ini adalah dengan masuk ke aplikasi *wireshark* kemudian pilih jaringan yang dianalisis, seperti yang ditunjukkan pada gambar 22, peneliti memilih Wi-Fi 4 karena jaringan tersebut adalah jaringan pada Kantor Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kota Palopo yang telah peneliti coneksikan dengan laptop peneliti yang dijadikan sebagai penyerang atau attcker untuk melakukan *packet sniffing*.



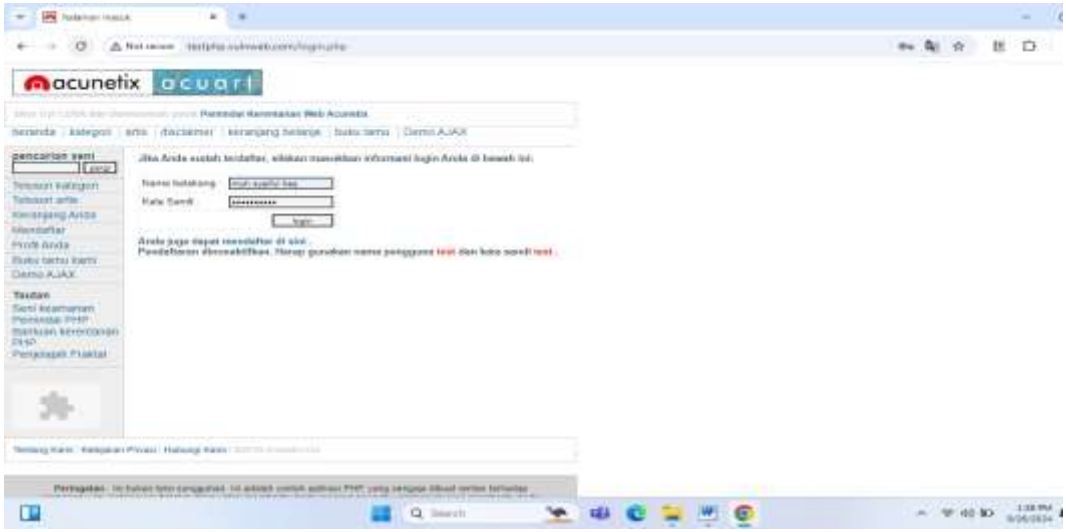
Gambar 22. Tampilan Awal *Wireshark*

Selanjutnya adalah tampilan *packet* yang tercapture di dalam *wireshark* dengan memilih jaringan yang ingin di analisis, disini penulis memilih Wi-Fi 4 karena ini adalah *interface* dari jaringan Kantor Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kota Palopo yang terhubung dengan laptop peneliti dimana laptop peneliti sebagai laptop yang digunakan melakukan analisis dan melakukan *smiffing*.



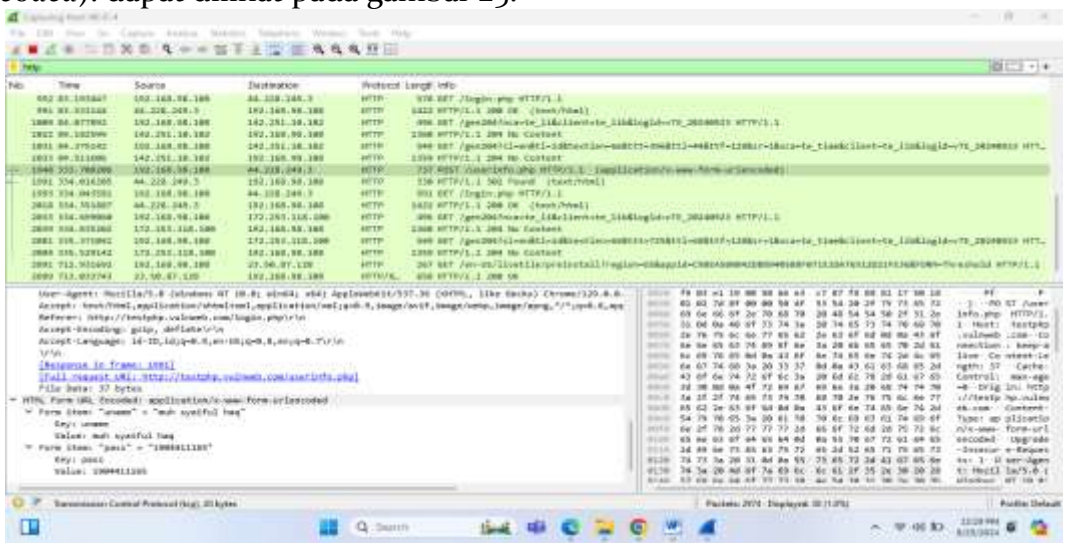
Gambar 23. *Traffic* Jaringan DPMPTSP

Selanjutnya adalah melakukan pengunjungan ke sebuah *website* yang masih menggunakan *protocol Hypertext Transfer Protocol* (HTTP) dan mecoba untuk login pada situs tersebut. Dapat dilihat seperti pada gambar 24.



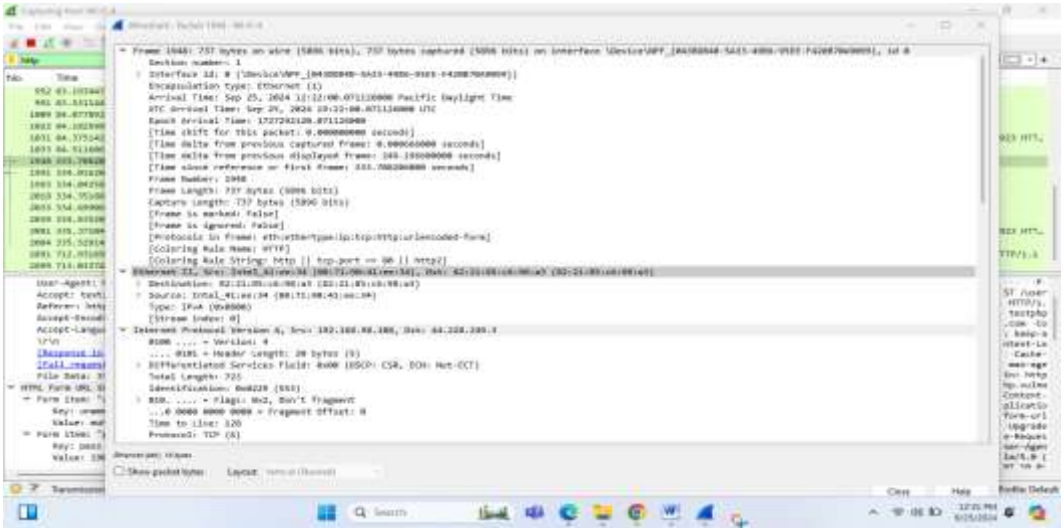
Gambar 24. *Login Website*

Selanjutnya adalah melakukan konfigurasi untuk melakukan *packet sniffing* dengan mencari "*http.request.method="post* pada kolom pencarian *wireshark*, pada kolom tersebut peneliti mengetikkan "*http*" dan hasil yang diperoleh dari pencarian tersebut adalah nomor "1948", time "333.7082206", *source* (sumber) "192.168.98.108", dengan *destination* (tujuan) "44.228.249.3", kemudian *protocol* "*Hypertext Transfer Protocol* (HTTP)", info "*POST /userinfo.php HTTP/1.1* (*application/x-www-form-urlencoded*). dapat dilihat pada gambar 25.



Gambar 25. Konfigurasi *Packet Sniffing*

Selanjutnya adalah melihat detail informasi yang didapatkan setelah melakukan *packet sniffing* dengan cara klik dua kali pada POST yang telah diperoleh, hasilnya dpat dilihat pada gambar 26.



Gambar 26. Hasil *Capturing Packet Sniffing* 1

Gambar 27. Hasil *Capturing Packet Sniffing* 2

Hasil yang didapatkan dari *packet sniffing* yang telah dilakukan dan diperolehlah sebuah data *login website user* pada jaringan nirkabel Kantor Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kota Palopo adalah *username* "muh syaiful haq" dan *password* "1904411165".

5. *Enhancemen*

Berdasarkan hasil pengujian dengan melakukan *packet sniffing* menggunakan aplikasi *wireshark* didapatkan hasil analisis jaringan nirkabel pada Kantor Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kota Palopo adalah tidak adanya *filter* terhadap *website* yang berbahaya untuk dikunjungi oleh *user* pada jaringan nirkabel tersebut, dengan didapatkannya data *login* dari sebuah *website* dengan *username* "muh syaiful haq" dan *password* "194411165" yang dilakukan oleh salah satu *user* yang terhubung dalam jaringan nirkabel pada Kantor Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kota Palopo.

Tabel 5. Hasil Analisis

Serangan	Informasi yang diperoleh	Status
Packet Sniffing	1. Sumber IP 192.168.98.108	Berhasil
	2. Tujuan 44.228.249.3	Berhasil
	3. *Port* 80	Berhasil
	4. *Website "POST/userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)."*	Berhasil
	5. *Host test.php.vulnweb.com*	Berhasil
	6. *Username* "muh syaiful haq"	Berhasil
	7. *Password* "1944111165"	Berhasil

SIMPULAN

Adapun kesimpulan dalam penelitian analisis keamanan jaringan nirkabel dari *packet sniffing* menggunakan *aplikasi wireshark* pada Kantor Dinas Penanaman Modal Dan Pelayana Terpadu Satu Pintu Kota Palopo adalah sebagai berikut:

1. Jaringan nirkabel pada Kantor Dinas Penanaman Modal Dan Pelayana Terpadu Satu Pintu Kota Palopo masih cukup lemah keamananya karena masih rentan terhadap *packet sniffing* yang dapat membahayakan data-data pada user.
2. Analisis jaringan nirkabel berhasil dilakukan dengan fokus analisis hasil pada protocol jaringan yang tidak aman yaitu *Hypertext Transfer Protocol* (HTTP).

DAFTAR PUSTAKA

Fatwa, Muhamad, Ristu Rizki, Pandiangan Sriwinarty, and Edi Supriyadi. 2022. "Pengaplikasian Matlab pada Perhitungan Matriks." Papanda Journal of Mathematics and Science Research 1(2): 81–93. doi:10.56916/pjmsr.v1i2.260.

Sallata, M Kudeng. "Konservasi Dan Pengelolaan Sumber Daya Air Berdasarkan Keberadaannya Sebagai Sumber Daya Alam." 12.

Teguh, H. A. P. (2021). Kajian Optimasi Penggunaan Lahan Dalam Mendukung Konservasi Tanah Dan Air Pada Das Kuranji (Doctoral dissertation, Universitas Andalas).

King, A. P., & Aljabar, P. (2022). MATLAB programming for biomedical engineers and scientists. Academic Press.

Koroche, K. A. (2021). Weighted average based differential quadrature method for one-dimensional homogeneous first order nonlinear parabolic partial differential equation. Indian Journal of Advanced Mathematics, 1(1), 15-28.

Singh, V. P., & Fiorentino, M. (Eds.). (2013). Geographical information systems in hydrology (Vol. 26). Springer Science & Business Media.

Sabale, R., Venkatesh, B., & Jose, M. (2023). Sustainable water resource management through conjunctive use of groundwater and surface water: A review. Innovative Infrastructure Solutions, 8(1), 17.

Singh, R. M., Datta, B., & Jain, A. (2004). Identification of unknown groundwater pollution sources using artificial neural networks. Journal of water resources planning and management, 130(6), 506-514.

Sinha, K. K., Gupta, M. K., Banerjee, M. K., Meraj, G., Singh, S. K., Kanga, S., ... & Sahu, N. (2022). Neural network-based modeling of water quality in Jodhpur, India. Hydrology, 9(5), 92.

Awasthi, D. (2020). Low Cost Smart Water Meter for Residential Communities (Doctoral dissertation, International Institute of Information Technology Hyderabad).

Simonovic, S. P. (2012). Managing water resources: methods and tools for a systems approach. Routledge.