# Teknik Sniffing Jaringan Menggunakan Wireshark

**Richo Muhhamad Farhan[1], Gregorius Hendita Artha Kusuma[2]**
Program Studi Teknik Informatika[1,2]
Fakultas Teknik Universitas Pancasila, Jakarta, Indonesia[1,2]
richo.muhhamad@gmail.com[1] gregorius@univpancasila.ac.id [2]

***Abstract*—Computer network security factor is an absolute thing in building a network. Basically, the security system owned by the operating system is not enough to secure computer networks. Therefore, to get a computer network security, we need a tool that can detect the existence of an attack mechanism from the network. Where the purpose of this attack is to make the computer that accesses it unable to run normally on a computer network. Wireshark is software that can analyze computer network activity so that it can help detect imminent attacks so users don't have to worry about these attacks.**

***Kata kunci*—*sniffing,jaringan,wireshark***

## I. PENDAHULUAN

Jaringan komputer ini mencakup ke beberapa jaringan komputer, baik swasta maupun negeri, untuk dilakukan pada pekerjaan sehari-hari dalam transaksi dan komunikasi di kalangan bisnis, instansi pemerintahan dana individu. Dari pengamatan pada keamanan maka keamanan jaringan komputer dapat dilihat dari segi bentuknya, yaitu keamanan hardware berhubungan pada perangkat keras yang digunakan dalam jaringan komputer. Keamanan hardware kadang diabaikan padahal hal utama untuk menjaga jaringan supaya tetap stabil. Dalam keamanan hardware, server, dan tempat penyimpanan data wajib menjadi perhatian utama. Akses melalui fisik terhadap server dan data - data penting dibatasi semaksimal mungkin. Keamanan software, sesuai dengan namanya, maka yang perangkat lunak yang harus diamankan. Perangkat lunak yang dimaksud disini bisa berupa system operasi, sistem aplikasi, data dan informasi yang tersimpan dalam komputer jaringan terutama pada server. Contohnya, jika server hanya bertugas menjadi router, tidak perlu software web server dan FTP server diinstal, Membatasi software yang dipasang akan mengurangi konflik antar software yang membatasi akses, contohnya jika router dipasangi juga dengan FTP server, maka orang dari luar dengan login anonymous mungkin akan dapat mengakses router tersebut. Wireshark dalam memonitor suatu jaringan komputer dapat membantu memudahkan seorang administrator jaringan untuk melakukan pengawasan terhadap suatu jaringan komputer. Dengan aplikasi wireshark ini dapat melakukan monitoring, meninjau serta melakukan penyimpanan informasi sebuah paket baik paket yang keluar maupun paket yang masuk di dalam suatu jaringan secara detail. Selain itu tampilan grafis (GUI) pada wireshark cukup baik sehingga lebih memudahkan dalam memonitoring semua aktifitas serta kegiatan yang dilakukan pada suatu jaringan atau pada jaringan yang dimiliki.

## II. METODOLOGI PENELITIAN

Untuk menghindari berbagai macam serangan baik itu oleh para hacker maupun cracker keamanan jaringan sangatlah diperlukan. Ternyata serangan tersebut bukan Cuma berasal dari serangan para hacker dan cracker, tetapi juga berasal dari lingkungan sekitar. Oleh karena itu administrator diharuskan lebih teliti dalam memilih atau menganalisa sistem jaringan yang digunakan. Pada dasarnya komputer yang terhubung ke dalam jaringan memiliki ancaman(Sutarti et al., 2018) serangan yang lebih besar dibandingkan dengan komputer yang tidak terhubung ke jaringan. Resiko ini dapat dikurangi oleh network security, namun network security ini akan bertentangan dengan software network acces. Dikarenakan adanya network access, network security(Ning et al., 2013) memiliki tingkat kerawanan yang tinggi. Berikut ini merupakan jenis – jenis keamanan jaringan komputer : Didalam komputer harusnya mempunyai beberapa sistem keamanan yang baik. Hal ini dimaksudkan untuk menghindari terjadinya serangan – serangan oleh para hacker atau pelaku lain yang dapat mengganggu kinerja komputer anda seperti yang telah dijelaskan tadi. Pada dasarnya sistem keamanan komputer memiliki 5 jenis keamanan yang dapat memperkuat sistem keamanan komputer.

Keamanan fisik Klasifikasi keamanan didukung melalui hardware ataupun perangkat keras. Tujuan dari keamanan fisik yakni mampu melindungi hardware agar selalu dalam kondisi terbaik sehingga dapat digunakan dalam melaksanakan operasi jaringan. b. Keamanan Jaringan Keamanan jaringan merupakan hal yang abstrak. Hal tersebut dikarenakan jenis keamanan dilakukan oleh benda tidak kelihatan atau tidak kasat mata, baik itu menggunakan software maupun perintah tertentu. Contoh keamanan jaringan yaitu, dengan menggunakan proxy maupun firewall untuk melakukan filter pada user yang ingin menggunakan

akses dalam jaringan. c. Otorisasi Akses Jenis keamanan jaringan atau otorisasi akses merupakan suatu keamanan jaringan dengan menggunakan password atau kata sandi, ketika akan menghubungkan perangkat dalam jaringan. Hal tersebut dilakukan agar administrator dapat membatasi akses user yang sudah terpilih saja yang bisa terhubung pada sebuah jaringan. Proteksi Virus Virus mampu melakukan metode penyerangan pada system komputer dengan menggunakan program, dan menjadikan sistem yang ada di komputer menjadi berantakan dan mengakibatkan kerusakan. Untuk menangani serangan virus, dapat menggunakan atau menginstal software anti virus pada komputer selalu update dengan database baru. e. Penganan Rencana Penganan Rencana ini merupakan langkah – langkah yang harus diambil apabila terjadi bencana alam yang mengakibatkan kerusakan dan kehilangan data – data penting pada semua sistem jaringan komputer. Perencanaan bencana ini bertujuan untuk terjadinya kerusakan pada system dapat cepat teratasi.

Untuk memahami mengenai pengertian dari jaringan komputer serta hal – hal penting yang terdapat pada jaringan komputer, berikut ini adalah pengertian jaringan komputer menurut para ahli serta hal – hal penting yang terdapat dalam jaringan komputer. Jaringan komputer adalah sebuah sistem yang terdiri atas komputer - komputer yang dihubungkan satu sama lain untuk dapat berbagi sumber daya satu sama lain seperti printer dan cpu, dan dapat saling berkomunikasi baik dalam surel atau pesan instan, serta agar dapat melakukan akses pada suatu informasi atau peramban web. Tujuan dari suatu jaringan komputer yaitu bertujuan agar setiap komputer dapat dalam jaringan komputer bisa meminta serta memberikan pelayanan atau memberikan sebuah service. Pada suatu jaringan perangkat yang mengakses baik menerima atau menggunakan layan biasa disebut perangkat klien (client) dan perangkat yang menyediakan atau mengirim layanan biasa disebut peladen (server). Desain ini biasa disebut dengan metode sistem client server, metode ini biasa digunakan hampir seluruh penerapan atau pembuatan suatu jaringan komputer. Jaringan komputer merupakan kumpulan beberapa komputer yang berjumlah banyak serta terletak secara terpisah-pisah tetapi terhubung dengan lainnya. Sebuah komputer dapat dikatakan saling terhubung apabila komputer terhubung dengan satu komputer lain, atau terhubung dengan banyak komputer dengan kondisi dapat saling mengirimkan informasi ataupun data dengan komputer lainnya . Bentuk koneksi dalam jaringan komputer dapat melalui media kawat tembaga atau melalui kabel serat optik, delombang mikro, maupun satelit komunikasi. Dari beberapa pendapat diatas maka dapat disimpulkan bahwa jaringan komputer merupakan suatu jaringan pada telekomunikasi yang menghubungkan satu komputer dengan komputer yang lain dengan tujuan agar dapat untuk saling berkomunikasi serta dapat bertukar data satu sama lain.

## III. HASIL DAN PEMBAHASAN

*A.Penjelasan Wireshark*

Wireshark adalah salah satu dari alat analisa jaringan yang biasa dipakai oleh seorang Network Administrator untuk melakukan pemecahan masalah yang ada dalam jaringan, menganalisa, perangkat lunak atau untuk pengembangan sebuah protokol dalam komunikasi, dan atau dalam pendidikan. Pertama kali wireshark muncul dengan nama Ethereal, lalu pada bulan Mei tahun 2006 proyek ini mengganti namanya menjadi Wireshark karena ada permasalahan mengenai merek dagang. Bahasa Pemrograman yang dipakai dalam wireshark adalah bahasa C dengan public license GNU. Wireshark banyak digemari karena interface wireshark yang telah menggunakan tampilan grafis atau GUI. Seperti namanya, aplikasi Wireshark dapat menangkap beberapa paket data yang berkeliaran dalam lalu lintas jaringan yang dilihat. Seluruh jenis informasi paket dalam bermacam-macam format protokol pun bisa dengan mudah ditangkap dan dianalisis. Oleh karena itu, tool ini sering digunakan untuk sniffing (mendapatkan informasi penting seperti username dan password) dengan menangkap paket yang berkeliaran dalam lalu lintas jaringan dan menganalisanya. Untuk dapat menjalankan tool ini caranya cukup mudah, hanya perlu memberikan perintah untuk Perancangan Sistem Menggunakan Wireshark. Berbeda dengan perancangan dalam jurnal sebelumnya, dalam perancangan sistem menggunakan wireshark lebih menunjuk pada aktivitas illegal. Seperti yang telah dijelaskan dalam jurnal, uses diberikan hak akses berupa proses upload maka pada system yang akan dibangun menggunakan pembatas harddisk dengan menggunakan disk quota, jadi user tidak bisa melakukan upload secara sembarang karena telah dibatasi kuota untuk melakukan proses upload. Proses yang dilakukan tersebut diawasi oleh wireshark agar uses dapat dengan aman meng-upload data tanpa perlu mengkhawatirkan ada yang menyusupi pada saat melakukan upload data.

Tujuan dan Manfaat Wireshark Manfaat dari penggunaan aplikasi wireshark ini yaitu sebagai berikut :

a) Menangkap informasi atau data paket yang dikirim dan diterima dalam jaringan komputer
b) Mengetahui aktifitas yang terjadi dalam jaringan komputer
c) Mengetahui dan menganalisa kinerja jaringan komputer yang dimiliki seperti kecepatan akses/share data dan koneksi jaringan ke internet
d) Mengamati keamanan dari jaringan komputer. Kegunaan Wireshark, beberapa kegunaan wireshark diantaranya, wireshark digunakan oleh seorang network administrator untuk menganalisis lalu lintas dalam jaringannya. Wireshark dapat mengambil paket data ataupun informasi yang sedang terjadi di dalam sebuah jaringan dan semua jenis informasi yang diperoleh ini bisa dengan mudah untuk dianalisis, salah satu caranya menggunakan sniffing, dengan menggunakan sniffing

maka memungkinkan untuk memperoleh informasi penting seperti username dan password yang ada di dalam jaringan. Wireshark merupakan aplikasi yang digunakan untuk menganalisis lalu – lintas yang terjadi dalam jaringan komputer, dimana software ini memiliki beberapa fungsi yang cukup bermanfaat bagi seorang profesional jaringan, peneliti, administrator jaringan, ataupun pengembang perangkat lunak jaringan. Wireshark bisa meng-tracking data secara realtime melalui Ethernet, FDDI, Token Ring, serial (PPP dan SLIP), wireless LAN 802.11, ataupun konektivitas ATM. Program ini pun marak dipakai oleh seorang chatters untuk mendapatkan alamat ip korban ataupun alamat IP para chatter lain melalui typing room. Alat dalam wireshark bisa menganalisis perpindahan paket data pada sebuah jaringan, yakni proses koneksi dan transmisi data antar beberapa komputer. Selama dapat memperoleh paket langsung melalui jaringan, dalam tool seperti pada wireshark, maka dapat menggunakan wireshark untuk menyadap percakapan melalui Voice over IP.

*B.Instalasi Wireshark*

Download wireshark lalu melakukan Instalasi, Wireshark bisa didapat dengan cara mendownload dengan Gratis melalui situs Official Wireshark. Di situs officialnya wireshark tersedia untuk sistem operasi mac OS dan juga Windows. Selama proses instalasi berlangsung pada windows, terkadang akan diminta untuk menginstal WinPcap, karena WinPcap merupakan library atau software pendukung yang nantinya akan digunakan untuk pengambilan data secara realtime. Untuk penginstalan wireshark di komputer atau laptop caranya seperti menginstal software-software additional tasks yang berukuran kecil dan tidak perlu kapasitas yang besar pada hardisk, yang pasti harus memiliki software installer-nya atau jika belum memiliki bisa di download pada situs resminya bisa searching di google atau bisa juga minta kepada rekan anda yang memiliki, agar lebih jelasnya cara instalasi wireshark yaitu sebagai berikut:

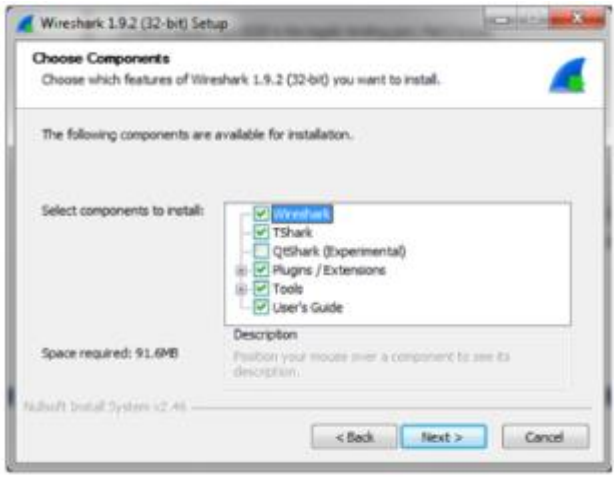
1. Setelah mendownload software nya, klik pada software instalasinya lalu akan muncul dialog box seperti berikut dan klik“next”.


Gambar 1 Instalasi WireShark

2. Akan muncul dialog box tentang “License Agreement”, lalu klik I Agree untuk melanjutkan.

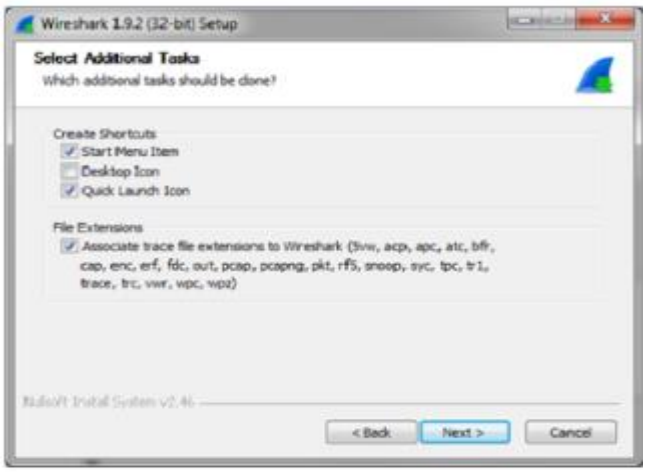

Gambar 2 Instalasi WireShark

3. Pilih Component pada Wireshark yang akan kamu install lalu klik next.



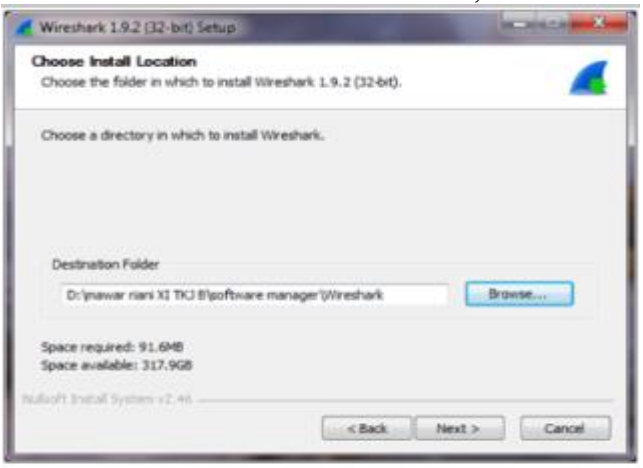

Gambar 3 Instalasi WireShark

4. Centang pada kolom File Extention, lalu klik next.



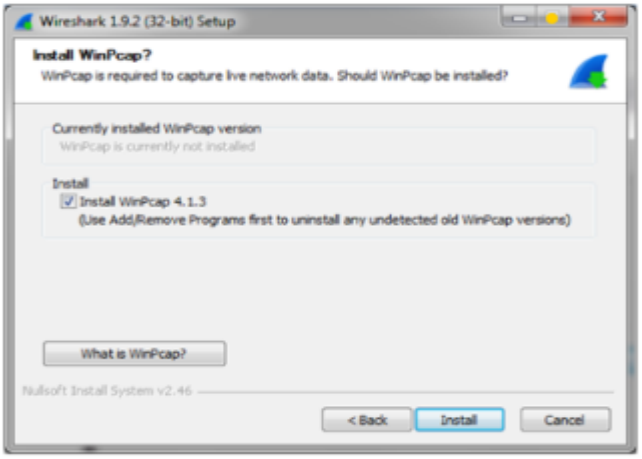

Gambar 4 Instalasi WireShark

5. Pilih letak dimana Wireshark akan diinstal, lalu klik next.



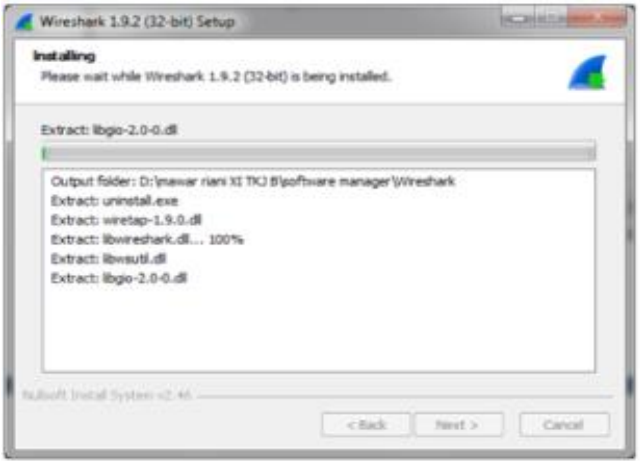

Gambar 5 Instalasi WireShark

6. centang pada kolom Install "WinCap", agar kita bisa mengcapture paket-paket data yang lewat ke jaringan.




Gambar 6 Instalasi WireShark

7. tunggu proses Installing, setelah selesai klik next.




Gambar 7 Instalasi WireShark

8. akan muncul dialog box seperti berikut untuk menginstall WinCap, lalu klik next


Gambar 8 Instalasi WireShark

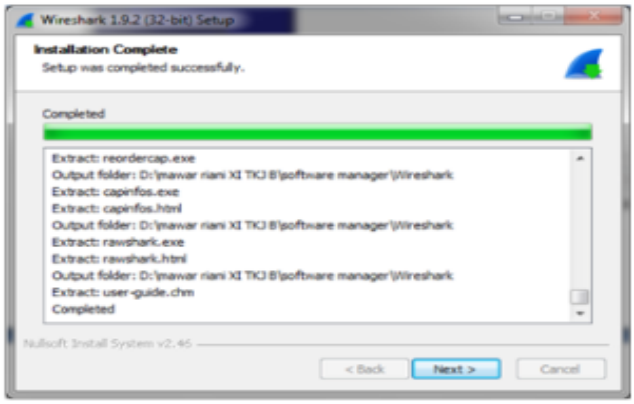
9. klik "I Agree" setelah membaca License Agreement.


Gambar 9 Instalasi WireShark

10. instalan sudah selsai. klik finish.


Gambar 10 Instalasi WireShark

11. klik next untuk melanjutkan.

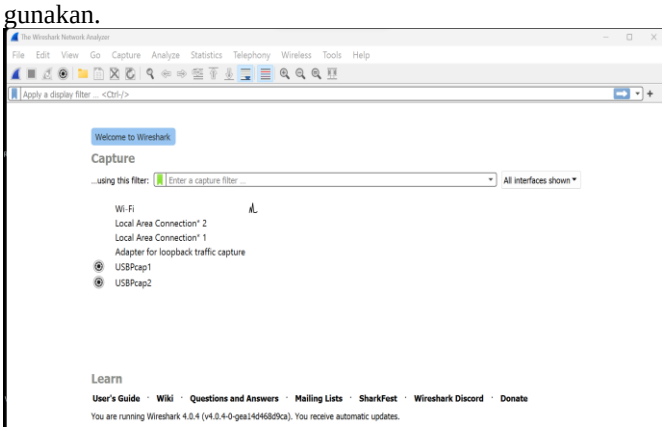



Gambar 11 Instalasi WireShark

12. pada tampilan ini kita diharuskan untuk memilih apakah langsung di tutup aplikasi dari wireshark ini ataupun langsung dijalankan, lalu klik finish.


Gambar 12 Instalasi WireShark

13. ini adalah tampilan wireshark yang langsung dapat kita gunakan.




Gambar 13 Instalasi WireShark

*C.Kegunaan Wireshark*

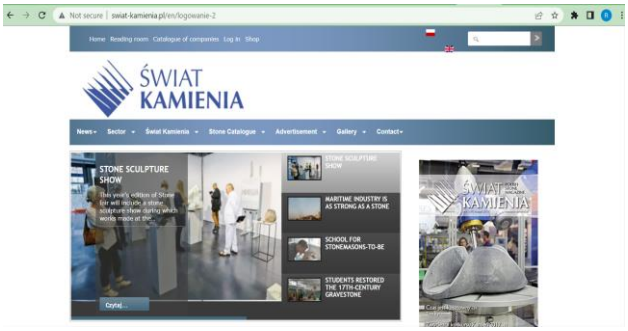
Banyak digunakan dalam memecahkan troubleshooting jaringan untuk memeriksa keamanan jaringan, mendebug implementasi protokol jaringan dalam software mereka, melakukan debugging implementasi paket, protocol, serta belajar. protocol dan banyak juga digunakan untuk sniffer atau mengendus data-data privasi di jaringan. Wireshark ini diibaratkan sebagai media atau tool yang dapat dipakai oleh user untuk penggunaan, apakah untuk kebaikan atau kejahatan. Hal ini karena wireshark dapat digunakan untuk mencari informasi yang sensitif yang berkeliaran pada jaringan, contohnya kata sandi, cookie dan lain sebagainnya. Wireshark dapat menganalisa paket data secara real time. Artinya aplikasi wireshark ini akan mengawasi semua paket data yang keluar masuk melalui antarmuka yang telah ditentukan oleh user sebelumnya. Wireshark dapat menganalisa paket data secara real time artinya, aplikasi wireshark akan mengawasi semua paket data yang keluar masuk melalui antarmuka yang telah ditentukan dan selanjutnya menampilkannya. Jika Komputer terhubung dengan jaringan kecepatan tinggi dan pada komputer sedang digunakan aplikasi berbasis jaringan, aplikasi wireshark akan menampilkan banyak sekali paket data dan menimbulkan kebingungan karena ada begitu banyak paket data jaringan yang muncul. Aplikasi wireshark dapat memfilter jenis protokol tertentu yang ingin ditampilkan.

*D.Sniffing Jaringan Menggunakan Wireshark*

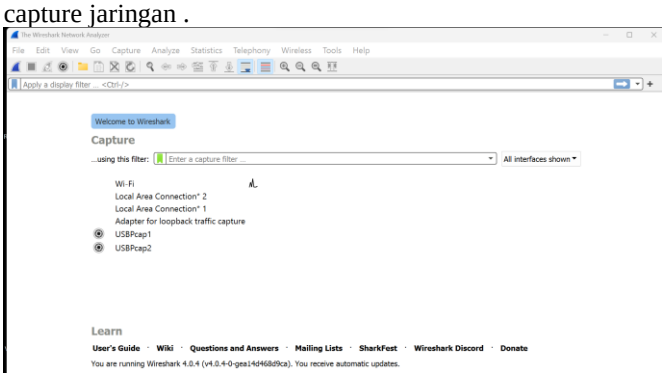
Sniffing merupakan proses yang dilakukan untuk mendapatkan paket data yang dikirimkan melalui jaringan komputer. Sniffing bisa digunakan untuk memantau dan menangkap semua lalu lintas yang terjadi di dalamnya tanpa pengecualian darimana dan untuk siapa paket-paket tersebut dikirimkan. Dampak negatif dari sniffing adalah seseorang bisa melihat informasi rahasia milik orang lain yang terhubung ke jaringan contohnya adalah username dan password . Dampak baik dari sniffing jaringan adalah untuk menganalisa paket data yang melewati jaringan sehingga jaringan dapat lebih optimal, menganalisa data apakah mempengaruhi performa jaringan atau tidak, dan dapat mengetahui bila ada pihak asing yang menyusup kedalam jaringan.Pada kesempatan kali ini peneliti ingin memberikan sebuah contoh kasus pada salah satu website http : http://swiat-kamienia.pl/en/logowanie-2 pada website ini peneliti ingin melakukan snifiing jaringan pada sebuah user dengan mencari password dan username.

Berikut ini adalah cara cara Sniffing jaringan menggunakan Wireshark :

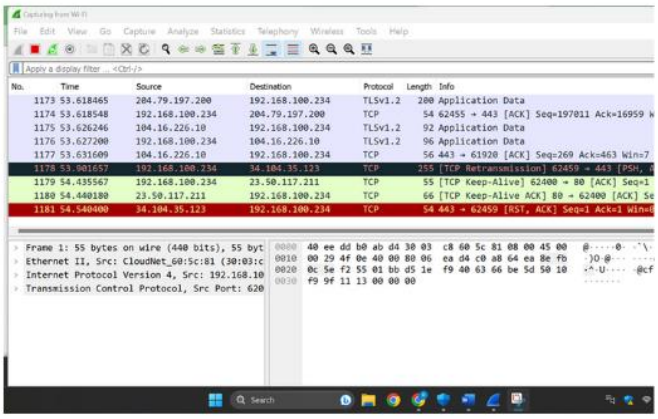
1. Pertama,kita harus mencari website http yang ingin kita sniffing jaringan nya,saya sudah mempunyai contoh salah satu website http



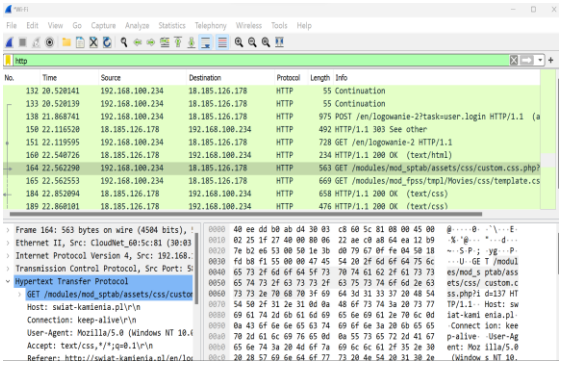

2. Selanjutnya kita membuka wireshark untuk melakukan capture jaringan .



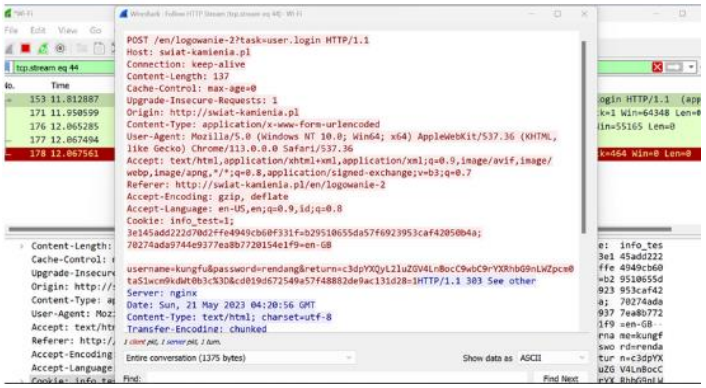

3. Setelah itu,kita mulai melakukan capturing di dalam wireshark.



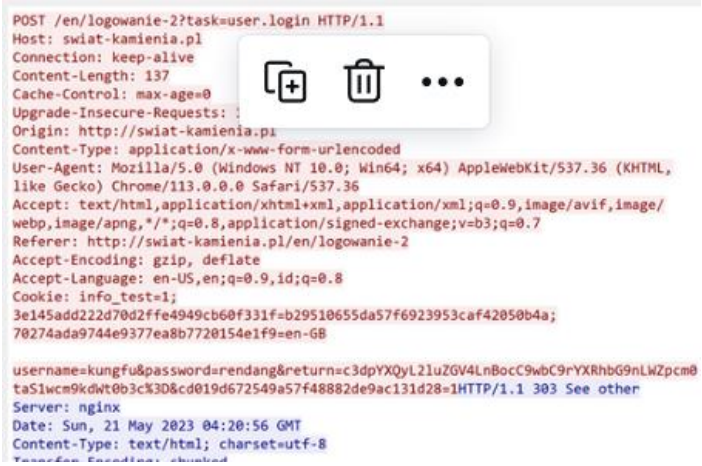
4.Setelah itu mencari http.request.method=="post pada kolom pencarian wireshark



5. Pada bagian post didalam http tersebut kita klik kanan dan follow http stream




6.Pada bagian ini kita bisa melakukan sniffing jaringan dengan melihat id dan password pengguna karena semua data pengguna akan muncul pada bagian ini




| Progres Mingguan | Hasil Progres |
|---|---|
| Minggu KE 1 | PENGENALAN TOOLS |
| Minggu KE 2 | PENETAPAN TOOLS PADA SETIAP ORANG |
| Minggu KE 3 | INSTALASI TOOLS |
| Minggu KE 4 | PRESENTASI TOOLS YANG DIMILIKI |
| Minggu KE 5 | IDLE (Mencari Referensi Referensi Penjelasan Dan Contoh Sniffing Pada Tools) |
| Minggu KE 6 | MENCOBA SNIFFING MENGGUNAKAN TOOLS Wireshark |
| Minggu KE 7 | MENJELASKAN FUNGSI TOOLS |
| Minggu KE 8 | IDLE (Mencari Website Http Pada Internet) |
| Minggu KE 9 | IDLE (Mencoba Sniffing Ke Beberapa Website Http) |

| | |
|---|---|
| Minggu KE 10 | IDLE (Mencari Website Http Yang Sesuai Untuk Disniffing) |
| Minggu KE 11 | MENCOBA MONITORING JARINGAN MENGGUNAKAN WIRESHARK |
| Minggu KE 12 | IDLE (Menuggu Hasil Monitoring Jaringan Apakah Sudah Sesuai) |
| Minggu KE 13 | IDLE (Pembuatan Laporan Akhir Untuk Tools Wireshark) |
| Minggu KE 14 | Pengumpulan Laporan Akhir |

## IV. KESIMPULAN

Dari penelitian tentang analisis keamanan data pada website dengan wireshark dapat ditarik kesimpulan bahwa protokol HTTP tidak terlalu aman untuk digunakan untuk menulis informasi pribadi yang bersifat rahasia khususnya username dan password. Pada gambar (berapa) sudah terlihat halisnya pada metode post yang tertangkap wireshark apa yang dimasukan oleh user dapat terbaca jelas tanpa enkripsi. Sedangkan protocol HTTPS lebih aman karena saat kita mengakses situs dengan protocol HTTPS tidak ada protocol HTTPS yang dapat tertangkap oleh aplikasi ini. Informasi yang disajikan lewat pelacakan IP halaman yang dikunjungi hanya berupa IP asal dan tujuan atau server dan port yang digunakan untuk melakukan komunikasi, paket data yang melewati hanya bisa diketahui jumlahnya saja dan ketika dilihat paket tersebut tidak bisa terbaca atau telah terenkripsi yang digunakan oleh masing-masing situs web.

## DAFTAR PUSTAKA

[1] Hanipah, R. and Dhika, H., 2020. Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Dengan Wireshark. *DoubleClick: Journal of Computer*

[2] Susianto, Didi, and Anisa Rachmawati. "Implementasi dan Analisis Jaringan Menggunakan Wireshark, Cain and Abels, Network Minner." *Jurnal Cendikia* 16.2 Oktober (2018): 120-125.

[3] Prasetyo, Inung Bagus. "Analisa Sniffing Paket ICMP Menggunakan Wireshark." *Jurnal SISTEMASI* 8.1 (2019): 221.

[4] Dimas Prasetya Wijayag - ( Teknologi Informasi * )

[5] Gunawan, Indra. "Analisis Keamanan Data Pada Website Dengan Wireshark." *JES (Jurnal Elektro Smart)* 1.1 (2021): 16-19

[6] Saxena, Praful, and Sandeep Kumar Sharma. "Analysis of network traffic by using packet sniffing tool: Wireshark." *International Journal of Advance Research, Ideas and Innovations in Technology* 3.6 (2017): 804-808.

[7] Asrodia, Pallavi, and Hemlata Patel. "Analysis of various packet sniffing tools for network monitoring and analysis." *International Journal of Electrical, Electronics and Computer Engineering* 1.1 (2012): 55-58.

[8] Luthfansa, UDR Zaky Maula, and Ulla Delfana Unknown Rosiani. "Pemanfaatan Wireshark untuk Sniffing Komunikasi Data Berprotokol HTTP pada Jaringan Internet." *Journal Information Engineering and Educational Technology) ISSN* 2549 (2021): 869X.

[9] Abdillah, Muhamad Aznar, Anton Yudhana, and Abdul Fadil. "Sniffing Pada Jaringan WiFi Berbasis Protokol 802.1 x Menggunakan Aplikasi Wireshark." *J-SAKTI (Jurnal Sains Komputer dan Informatika)* 4.1 (2020): 1-8.

[10] Pavithirakini, S., et al. "Improve the Capabilities of Wireshark as a tool for Intrusion Detection in DOS Attacks." *International Journal of Scientific and Research Publications* 6.4 (2016): 378-384