Progress Report 1

Kelompok 2
Dave Travis - 2201020008
Muhammad Noval - 2201020014
Rizsky Parsadanta R. - 2201020117
Arya Winata - 2201020001

Judul proyek	:	Analisis Serangan Sniffing & Mitigasinya di Wireshark
Tujuan proyek	:	Memahami cara kerja penyerangan *packet sniffing* dan metode pencegahannya.
Target proyek (Minggu 1)	:	Studi konsep & instalasi Wireshark

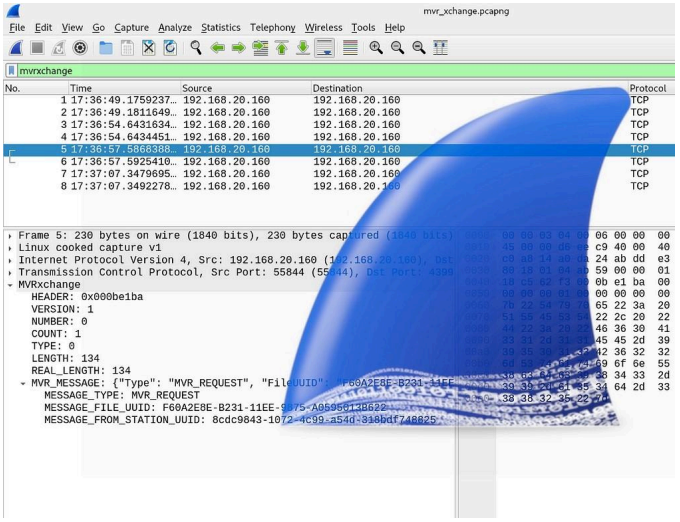
1. Studi Konsep

Proyek kami akan membahas mengenai serangan pada sebuah lalu lintas jaringan, yang terfokuskan pada serangan sniffing, dan sebelum terjun ke pembahasan tahapan analisis dan penggunaan Wireshark dalam penanganan serangan tersebut, kami akan memberikan landasan teori yang berperan sebagai dasar aktivitas yang akan kami lakukan.

Meskipun bersifat umum, studi konsep ini berperan langsung dalam memberikan gambaran menyeluruh mengenai prinsip kerja sebuah jaringan. Pembaca dapat mendapatkan gambaran bagaimana dilakukannya dalam menganalisa paket jaringan, cara kerja dan peran software Wireshark sebagai *network protocol analyzer*, serta pentingnya enkripsi dalam melindungi data yang dikirim dalam sebuah jaringan, sebab target utama dari proyek ini ialah serangan *sniffing* yang mengincar data transfer yang terjadi pada sebuah jaringan.

- Wireshark

Wireshark adalah aplikasi *network protocol analyzer* (analisis protokol jaringan) yang memungkinkan pengguna untuk menangkap (seperti screenshot dan disimpan hasil tangkapannya) dan menganalisis paket data yang melewati sebuah jaringan yang dipantau pada sesi tersebut. Secara umum, Wireshark memiliki kegunaan yang sangat bervariasi, tergantung pada siapa yang menggunakan software ini; pekerja di bidang jaringan biasanya menggunakannya untuk troubleshooting dan analisis keamanan.

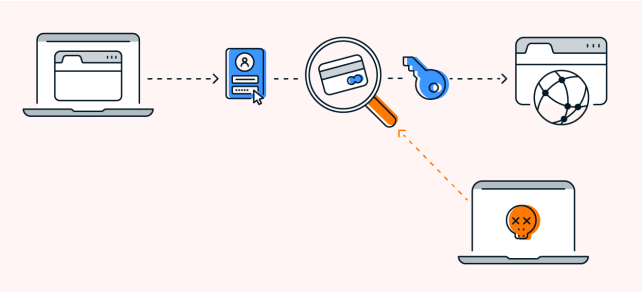


Gambar UI Wireshark

Pada proyek kami kali ini, akan difokuskan pada pembelajaran sebuah jaringan, guna menganalisis sebuah serangan packet sniffing dan metode pencegahan yang paling optimal untuk permasalahan yang ditemui.

- Packet Sniffing

Packet Sniffing adalah teknik yang dilakukan oleh pihak ketiga dalam transfer data untuk mengintersepsi dan merekam paket data yang dikirim, baik dalam lingkungan *wired* maupun *wireless*. Pihak yang melakukan tindakan ini bisa melaksanakannya secara pasif (sekadar mendengarkan lalu lintas data) atau aktif (mengganggu alur komunikasi).



Ilustrasi *Packet Sniffing*

Pada proyek kami, akan diilustrasikan ke depannya bagaimana dampak dari tindakan sniffing ini terhadap sebuah proses transfer data pada lingkungan jaringan tertutup, sampai bagaimana solusi terbaik yang dapat diaplikasikan untuk menghindari terjadinya *sniffing* dalam jaringan terkait.

- HTTP vs HTTPS

HTTP (*HyperText Transfer Protocol*) adalah protokol komunikasi untuk transfer data web yang mengirimkan informasi dalam bentuk teks biasa, sehingga data yang terkirim rentan terhadap penyadapan. Dan sebaliknya, HTTPS (HTTP *Secure*) seperti namanya, merupakan versi aman dari HTTP yang menggunakan enkripsi berbasis TLS/SSL untuk melindungi integritas dan kerahasiaan data selama transmisi data.

Ilustrasi HTTP dan HTTPS

Proyek kami ini, akan kami berikan perbedaan *sniffing* data terhadap kedua pihak protokol, sehingga terlihat secara langsung seberapa beda protokol yang ada.

- Enkripsi Data 101

Enkripsi adalah proses mengubah data yang dapat dibaca (*plaintext*) menjadi bentuk tidak terbaca (*ciphertext*) menggunakan algoritma dan kunci kriptografi, sehingga hanya pihak yang memiliki kunci dekripsi yang dapat mengakses informasi aslinya. Dalam konteks keamanan jaringan, enkripsi berperan krusial dalam mencegah pencurian data saat terjadi penyadapan, terutama pada layanan yang melibatkan autentikasi atau transaksi. Tanpa enkripsi, informasi sensitif seperti kata sandi atau riwayat aktivitas pengguna dapat dengan mudah dieksploitasi oleh pihak tidak sah.

Dalam cakupan proyek kami kali ini, enkripsi data menjadi salah satu target akhir yang akan dilakukan guna merancang sebuah protokol yang aman dalam kegiatan transfer data dari satu pihak ke pihak yang lainnya, walaupun tetap dalam satu jaringan.

- Mitigasi Keamanan

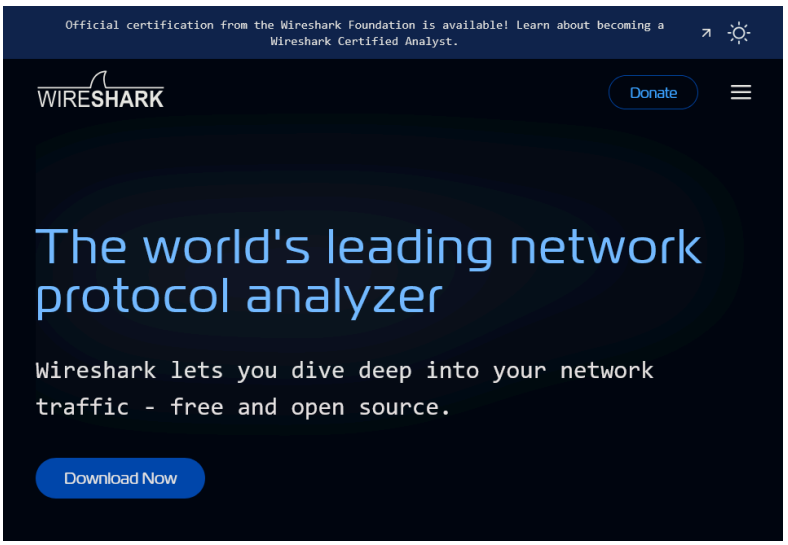
Mitigasi keamanan dalam proyek kami kali ini mengacu pada serangkaian langkah pencegahan dan respons yang dirancang untuk mengurangi resiko atau dampak dari ancaman jaringan, termasuk serangan *packet sniffing*. Strategi mitigasi yang efektif meliputi penggunaan protokol berbasis enkripsi seperti HTTPS,

penerapan *HTTP Strict Transport Security* (HSTS), penggunaan jaringan pribadi virtual (VPN), serta edukasi pengguna untuk menghindari login di jaringan publik tanpa perlindungan.

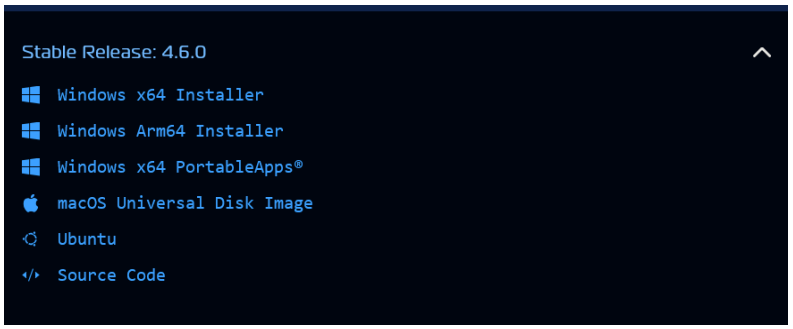
2. Instalasi Wireshark

Pada bagian ini akan kami jelaskan proses instalasi sederhana terhadap software Wireshark pada PC anggota kelompok. Langkah-langkah berikut merupakan tahapan yang dilakukan guna memakai Wireshark untuk keperluan proyek ini ke depannya.

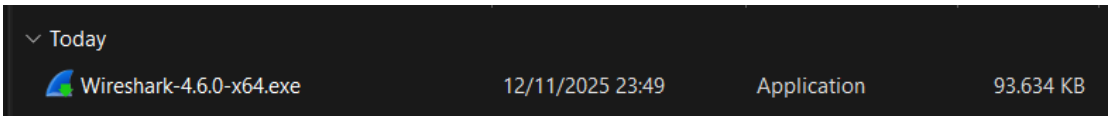
1. Kunjungi situs resmi Wireshark: https://wireshark.org



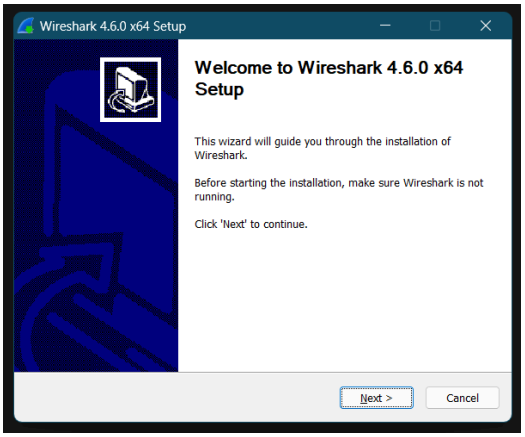
2. Download installer untuk Windows (Opsi 1: Windows x64 Installer)

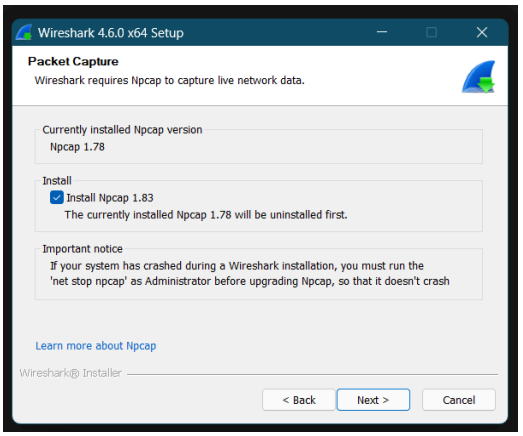


3. Jalankan file .exe setelah file installer siap didownload

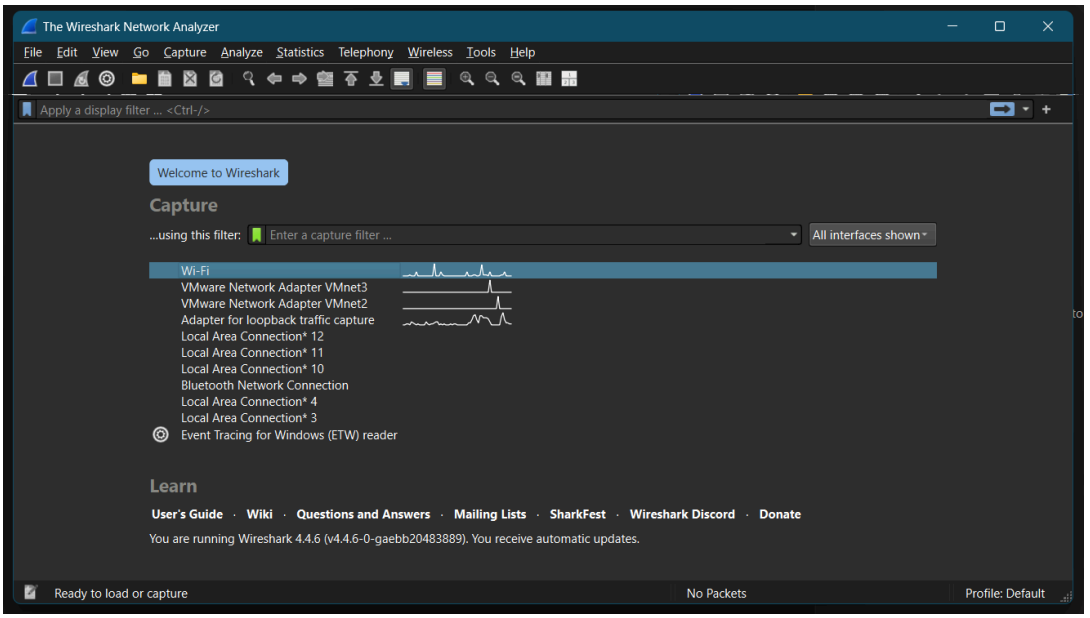


4. Ikuti program wizard instalasi hingga selesai (dan jangan lupa centang Install N pcap, karena akan digunakan nantinya untuk *capture* paket)

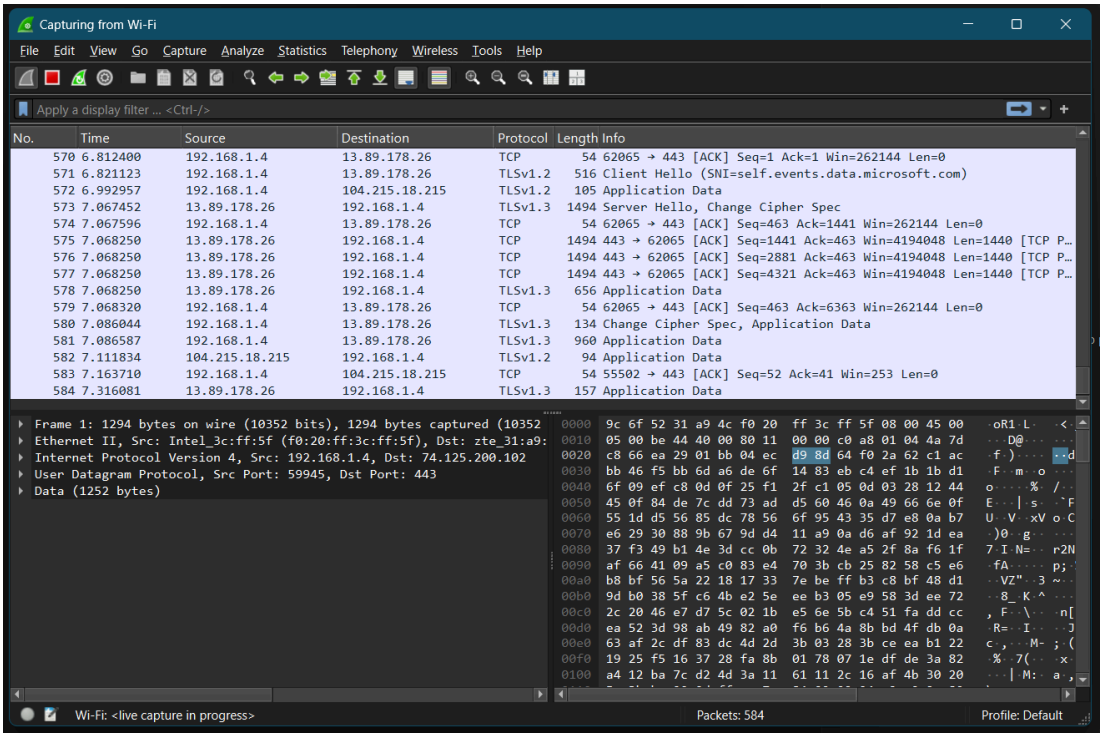




5. Selesai, buka WireShark



Berikut merupakan tampilan capture dari Wireshark, yang terdaftar jaringan yang dapat dipantau secara langsung dan siap untuk di *capture*. Salah satunya ialah jaringan Wi-Fi yang sedang terhubung dengan perangkat anggota kelompok. Jika jaringan tersebut dipilih, maka akan muncul data seperti ini:



Data-data pada gambar di atas mungkin terlihat asing, namun dengan teknik dan filter yang benar, angka-angka tersebut dapat menjadi sangat berguna dalam menganalisis arus data pada sebuah jaringan, terutama pada proyek kami kali ini.

Mungkin itu saja yang dapat kami sampaikan, kita ketemu lagi pada minggu depan saat kami membahas progress minggu ke dua: **Setup jaringan sederhana (LAN/VirtualBox/Packet Tracer)**. *See ya there, amigos, peace!*

- Kelompok 2