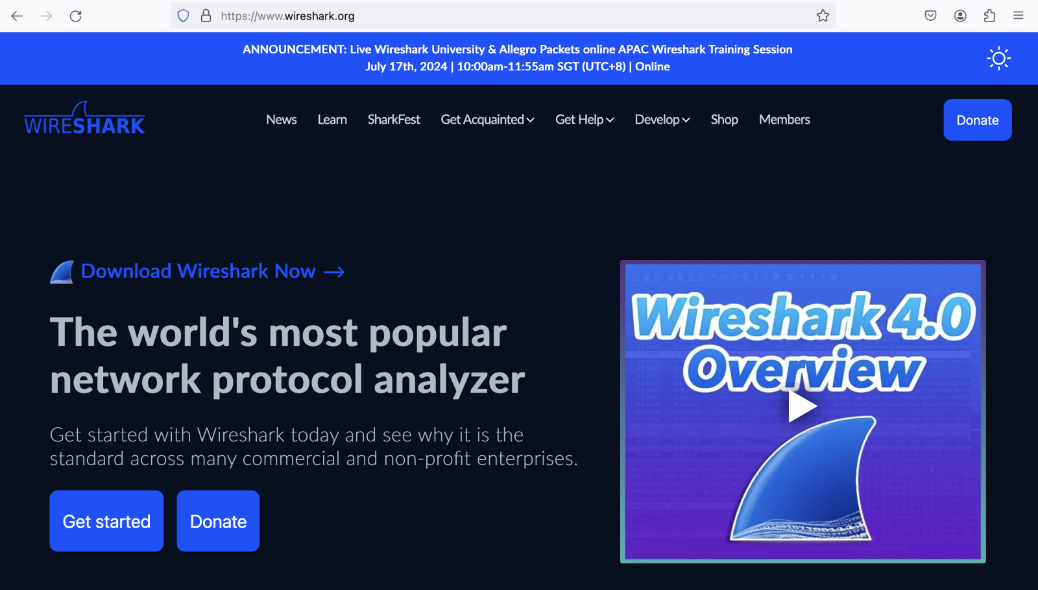
**Pengambilan Image Menggunakan Wireshark**

**6.5. Analisis MITM (Man in The Middle) Attack menggunakan wireshark**

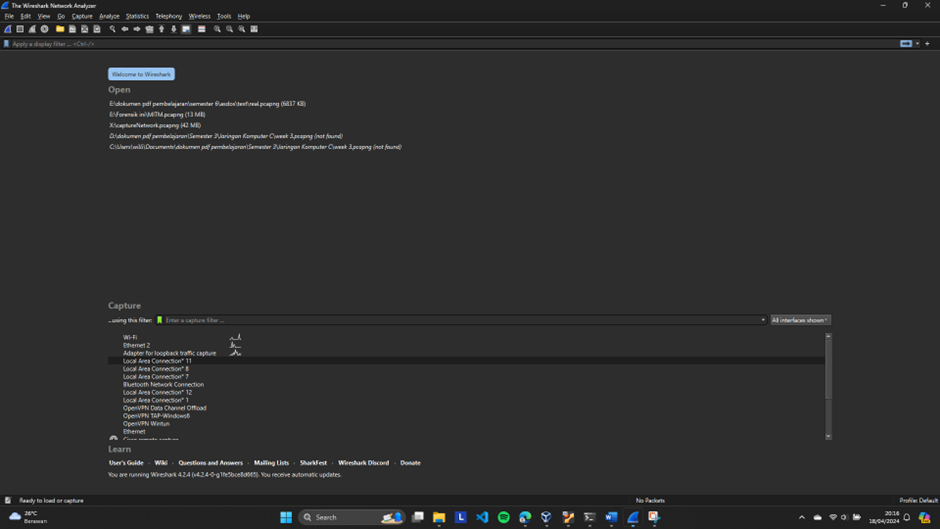
Man-in-the-Middle (MITM) attack merupakan suatu bentuk serangan dimana ketika penyerang melakukan penyusupan dan intersepsi di dalam suatu komunikasi jaringan tanpa diketahui oleh pengguna asli. Perangkat lunak Wireshark, sebagai alat analisis jaringan yang handal, menjadi pilihan dalam melakukan deteksi dan analisis bentuk serangan MITM.

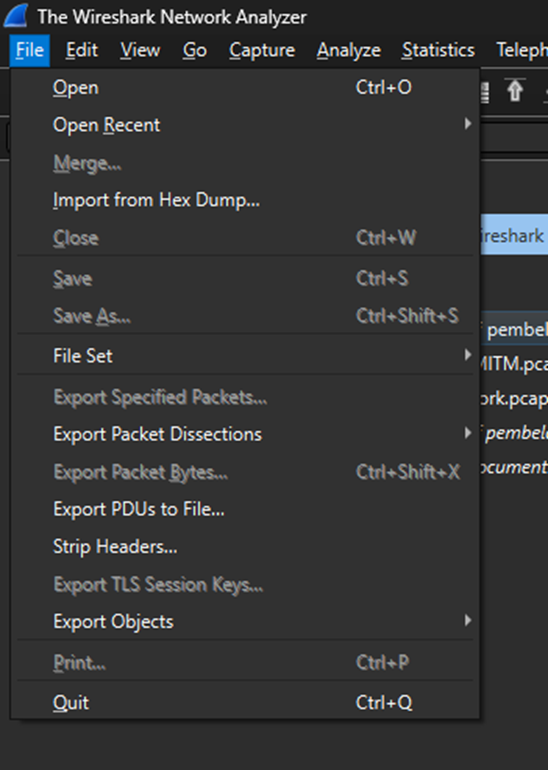
* Installer dari aplikasi Wireshark dapat diunduh di url: <https://2.na.dl.wireshark.org/win64/Wireshark-4.2.5-x64.exe>



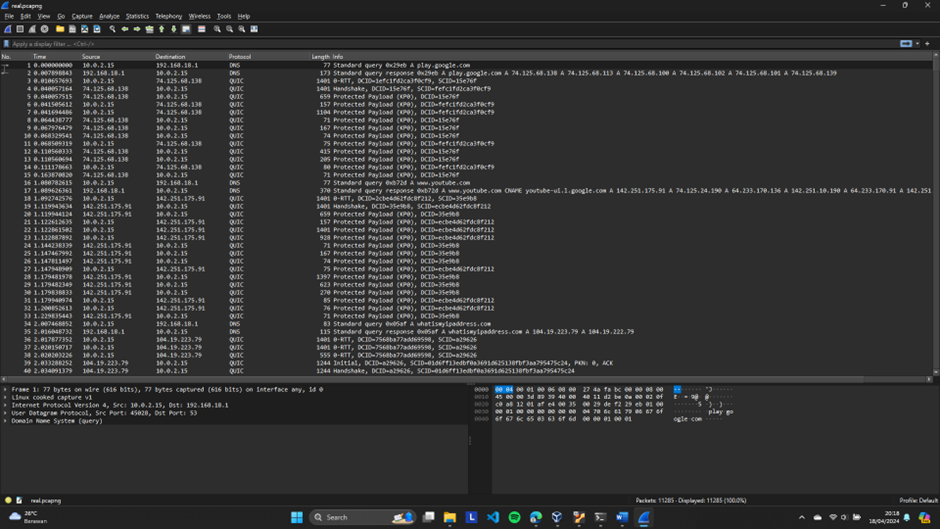
Gambar 6.11. Situs Wireshark

* Jalankan aplikasi wireshark yang sudah terinstal, lalu tekan menu file dan buka file image yang terletak di direktori: \labs\bab6\images\

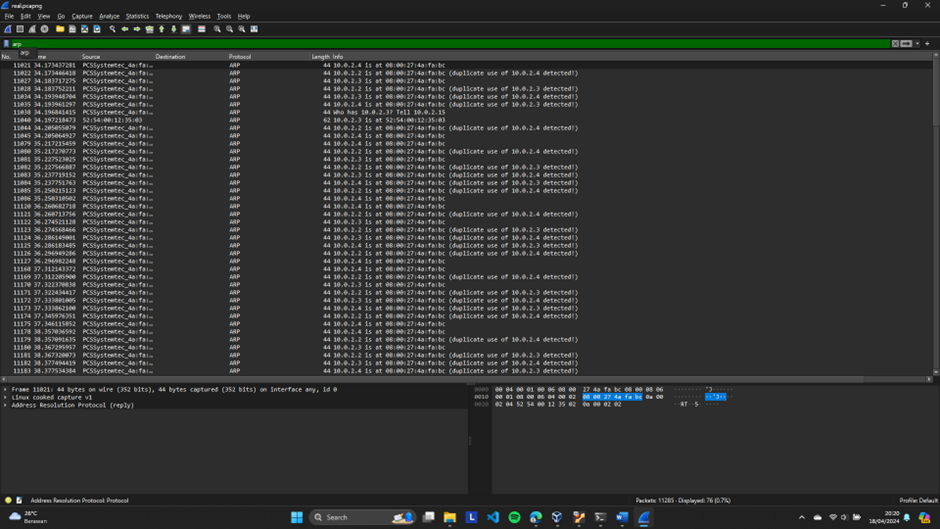
Gambar 6.12. Dashboard aplikasi wireshark



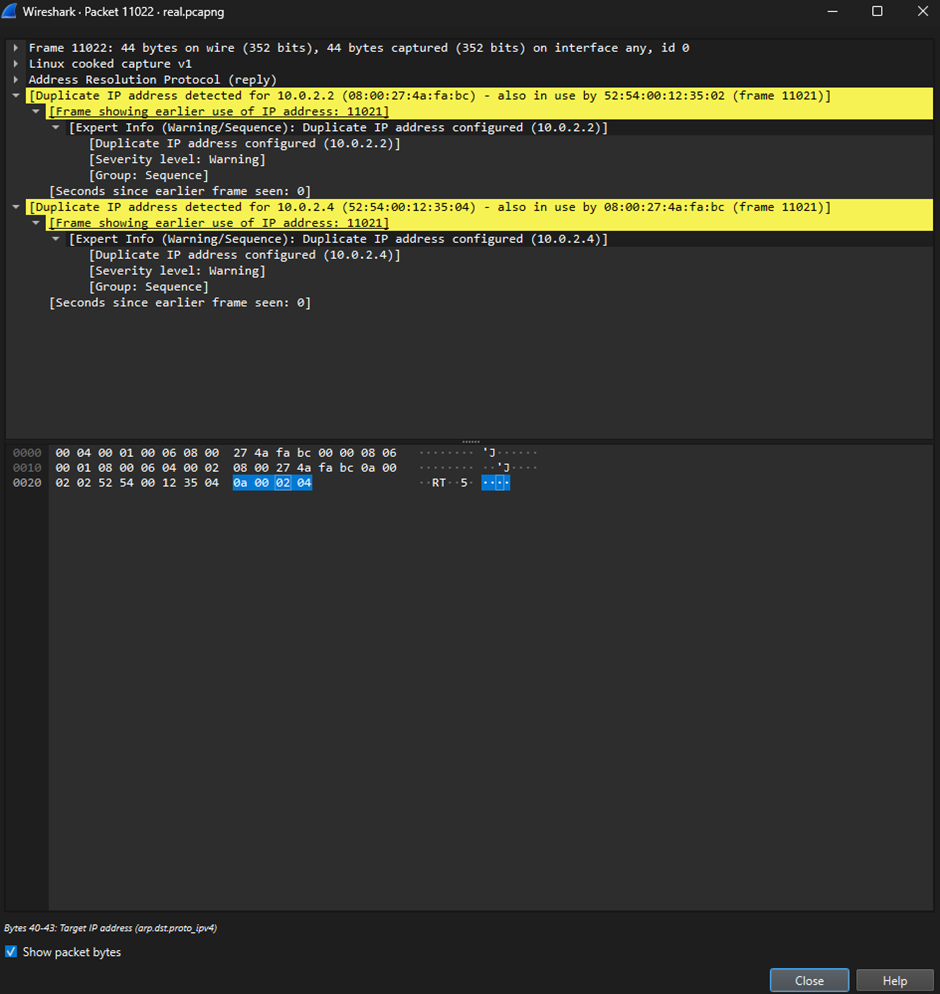
Gambar 6.13. Daftar Menu Aplikasi

Gambar 6.14. Tampilan ketika file image dibuka

* Selanjutnya, ahli dapat mengetikan filter ARP pada search bar.

Gambar 6.15. ARP pada kolom pencarian

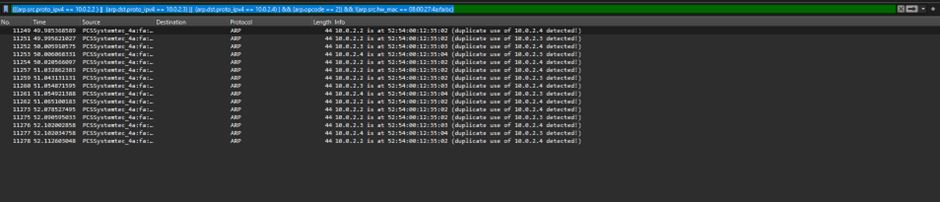
* Ahli memperoleh data bahwa terdapat beberapa duplikasi dengan ip 10.0.2.2-10.0.2.4. Klik dua kali pada salah satu baris yang terlihat mencurigakan (duplikasi)



Gambar 6.16 Duplikasi IP yang terjadi

* Selanjutnya, ahli akan melakukan filter terhadap ARP Poison Attack dengan mengetikan di search bar.

“(((arp.src.proto\_ipv4 == 10.0.2.2 ) || (arp.dst.proto\_ipv4 == 10.0.2.3) || (arp.dst.proto\_ipv4 == 10.0.2.4) ) && (arp.opcode == 2)) && !(arp.src.hw\_mac == 08:00:27:4a:fa:bc) “

Gambar 6.17. Filtering ARP poison attack

* + Filter tersebut akan memfilter alamat ip 10.0.2.2-10.0.2.4, opcode sebesar 2 dan mengecualikan paket ARP yang memiliki alamat MAC 08:00:27:4a:fa:bc.
* Lalu, ahli membuat label dengan menekan tombol “+” yang terletak pada kanan search bar

Gambar 6.18 Menambah label

* Pemberian nama label, disini ahli memberi nama “ARP Poisoning Attack (MITM)” sebagai label. Setelah itu tekan ok.

Gambar 6.19 Memberi nama label

* Filter ini bertujuan untuk menyaring dan mencegah serangan ARP Poisoning Attack jika terjadi di lain waktu.