LAPORAN

KOMUNIKASI DATA

“ Analisis Traffic Jaringan Menggunakan Tools Wireshark ”

Disusun Oleh

Nama : Muhamad Rahardi Nur

NIM : 09011282025079

Kelas : SK4A

Dosen Pengampu : Adi Hermansyah, M.T.

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2022

I. Dasar Teori

Wireshark adalah sebuah aplikasi *capture paket data* berbasis *open-source* yang berguna untuk memindai dan menangkap trafik data pada jaringan internet. Aplikasi ini umum digunakan sebagai alat *troubleshoot* pada jaringan yang bermasalah, selain itu juga biasa digunakan untuk pengujian *software* karena kemampuannya untuk membaca konten dari tiap paket trafik data. Aplikasi ini sebelumnya dikenal dengan nama **Ethereal**, namun karena permasalahan merek dagang lalu namanya diubah menjadi **Wireshark**.

Wireshark mendukung banyak format file paket capture/trace termasuk **.cap** dan **.erf**. Selain itu, alat dekripsi yang terintegrasi di dalamnya mampu menampilkan paket-paket terekripsi dari sejumlah protokol yang umum digunakan pada jaringan internet saat ini, termasuk WEP dan WPA/WPA2. Salah satu kemudahan Wireshark adalah distribusi pengembangannya yang bersifat *cross-platform*, sehingga pengguna Linux dan Macintosh juga dapat menginstal dan menggunakan aplikasi ini.

Dalam persepsi yang positif, Wireshark berguna untuk pekerjaan analisis jaringan. Cara kerjanya yaitu dengan ‘menangkap’ paket-paket data dari protokol-protokol yang berbeda dari berbagai tipe jaringan yang umum ditemukan di dalam trafik jaringan internet. Paket-paket data tersebut ‘ditangkap’ lalu ditampilkan di jendela hasil capture secara real-time. Pada awal proses analisis jaringan menggunakan Wireshark, semua paket data yang berhasil ditangkap tadi ditampilkan semua tanpa pilih-pilih (promiscuous mode). Semua paket data tersebut bisa diolah lagi menggunakan perintah sorting dan filter.

Dalam persepsi yang negatif, Wireshark biasa digunakan oleh sebagian hacker untuk melakukan sniffing. Terminologi sniffing sebenarnya tidak jauh berbeda dengan capture paket data, namun dalam konotasi yang negatif, karena bisa jadi menimbulkan dampak yang merugikan untuk orang lain terutama dari sisi privasi.

Wireshark sendiri juga memiliki fitur yang cukup lengkap, diantaranya yaitu:

- Multiplatform, bisa dipakai untuk beberapa basis sistem operasi (Unix, Mac, Windows, serta Linux)
- Bisa lakukan capture paket data jaringan secara real time
- Bisa menampilkan informasi protokol jaringan dari paket data secara komplit
- Paket data bisa disimpan jadi file serta nantinya bisa di buka kembali untuk analisa lebih lanjut
- Filtering paket data jaringan
- Pencarian paket data dengan persyaratan spesifik
- Pewarnaan penampilan paket data untuk memudahkan analisis paket data
- Menampilkan data statistik
- Untuk lakukan capture paket data yang keluar maupun masuk pada jaringan, wireshark membutuhkan piranti fisik NIC (Network Interface Card).

Quality of service (QoS) (Bahasa Indonesia : kualitas layanan) mengacu pada teknologi apa pun yang mengelola lalu lintas data untuk mengurangi packet loss (kehilangan paket), latency, dan jitter pada jaringan. QoS mengontrol dan mengelola sumber daya jaringan dengan menetapkan prioritas untuk tipe data tertentu pada jaringan.

Parameter Quality of Service terdiri dari :

- Throughput, Throughput yaitu kecepatan (rate) transfer data efektif, yang diukur dalam bps (bit per second). Throughput adalah jumlah total kedatangan paket yang sukses yang diamati pada tujuan selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut.

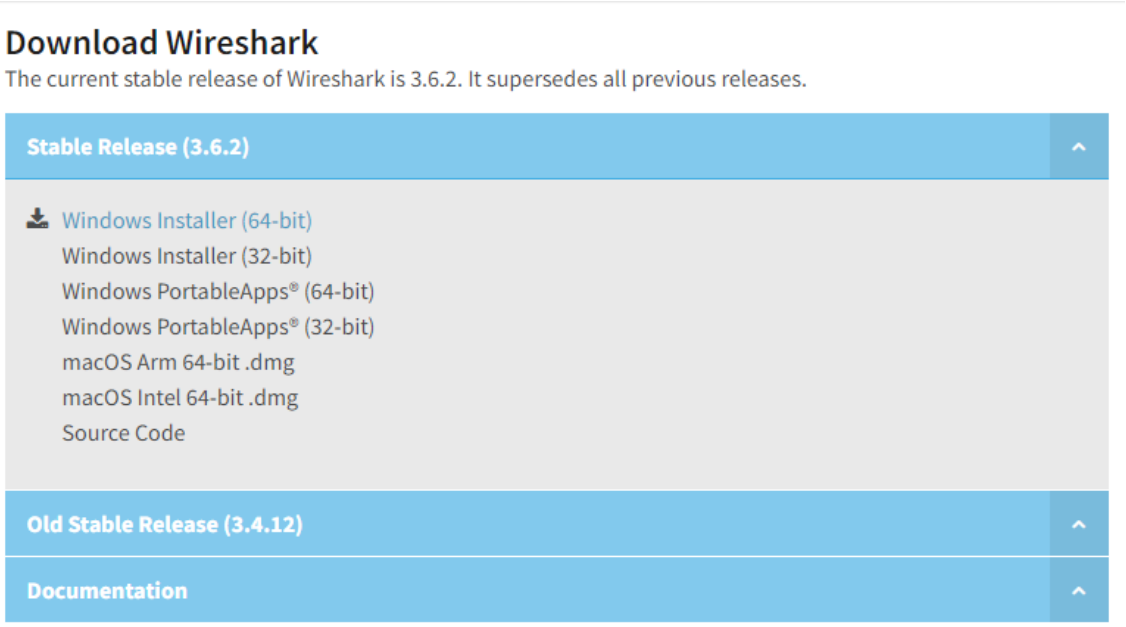
- Packet Loss, Packet Loss merupakan suatu parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang dapat terjadi karena collision dan congestion pada jaringan

- Delay (Latency), Delay (Latency) merupakan waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan. Delay dapat dipengaruhi oleh jarak, media fisik, congesti atau juga waktu proses yang lama.

- Jitter atau Variasi Kedatangan Paket, Jitter diakibatkan oleh variasi-variasi dalam panjang antrian, dalam waktu pengolahan data, dan juga dalam waktu penghimpunan ulang paket-paket diakhir perjalanan jitter.

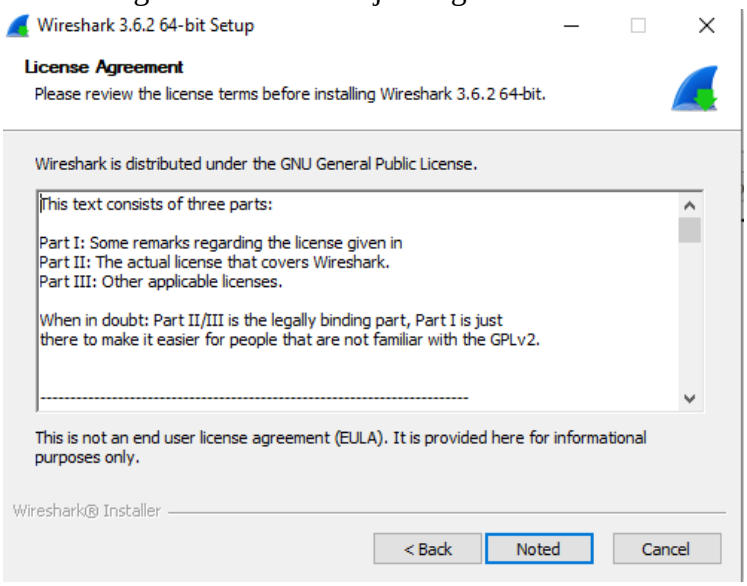
II. Instalasi Wireshark

- Buka situs wireshark.org
- Download dan pilih sesuai dengan os yang digunakan

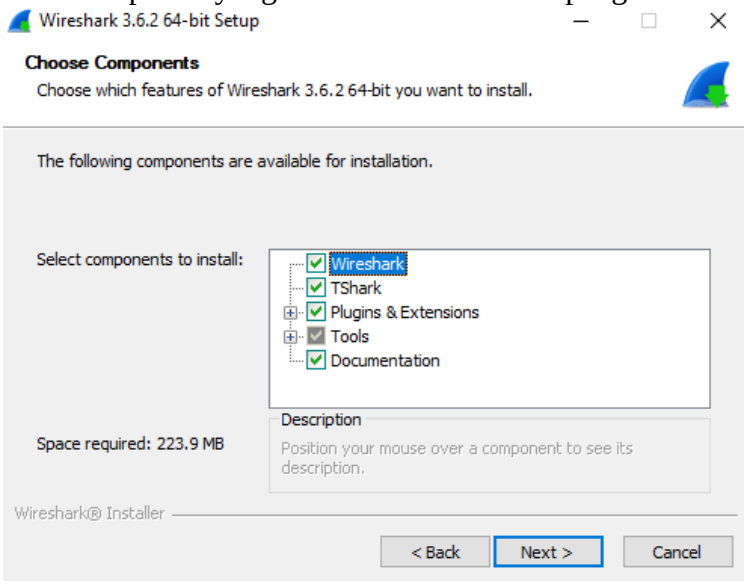


- Lakukan penginstalan seperti biasa

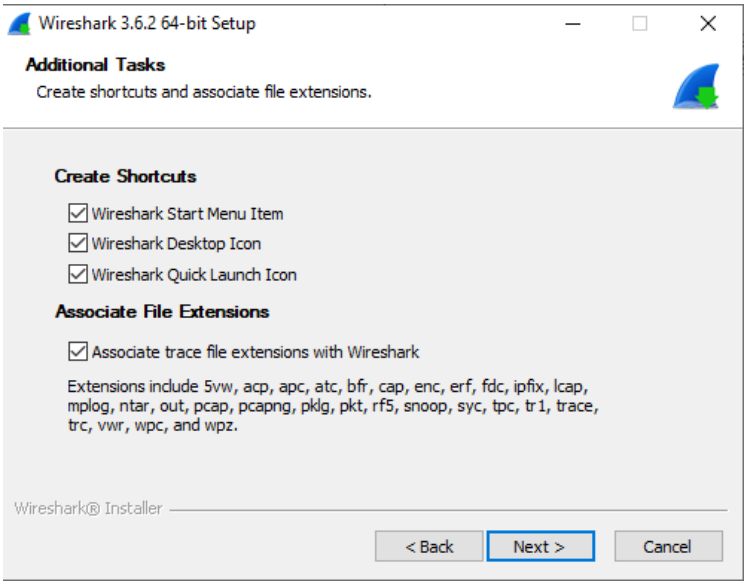
- License Agreement lewati saja dengan cara klik noted



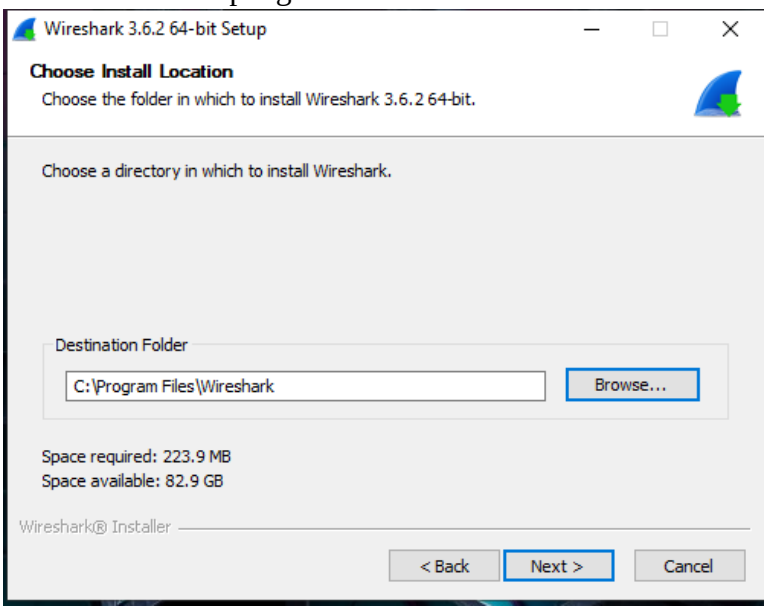
- Pilih komponen yang akan ikut serta dalam penginstallan



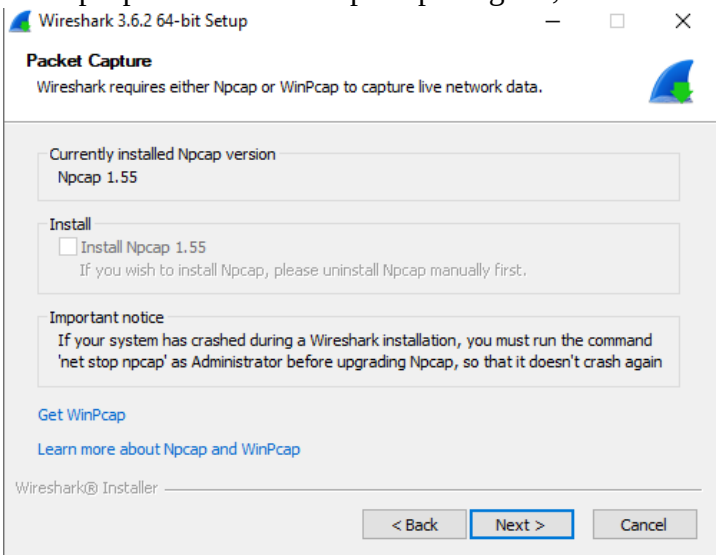
- Buat shortcut dan extensi file



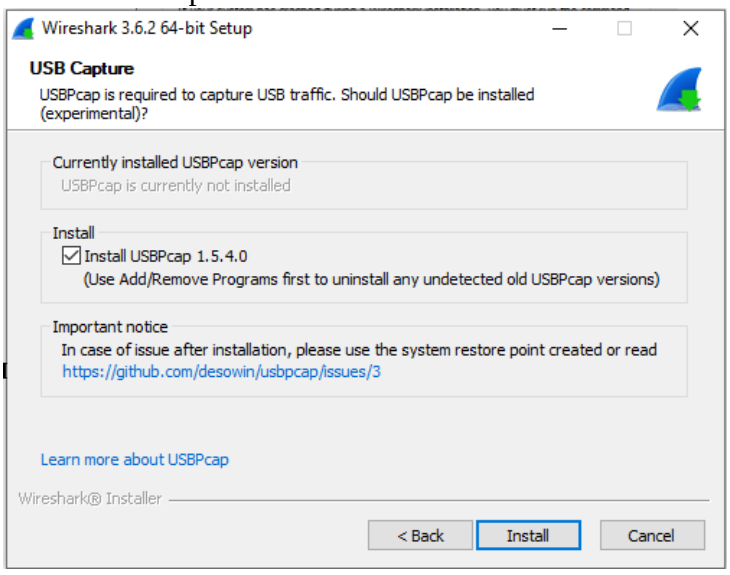
- Atur lokasi foder penginstallan



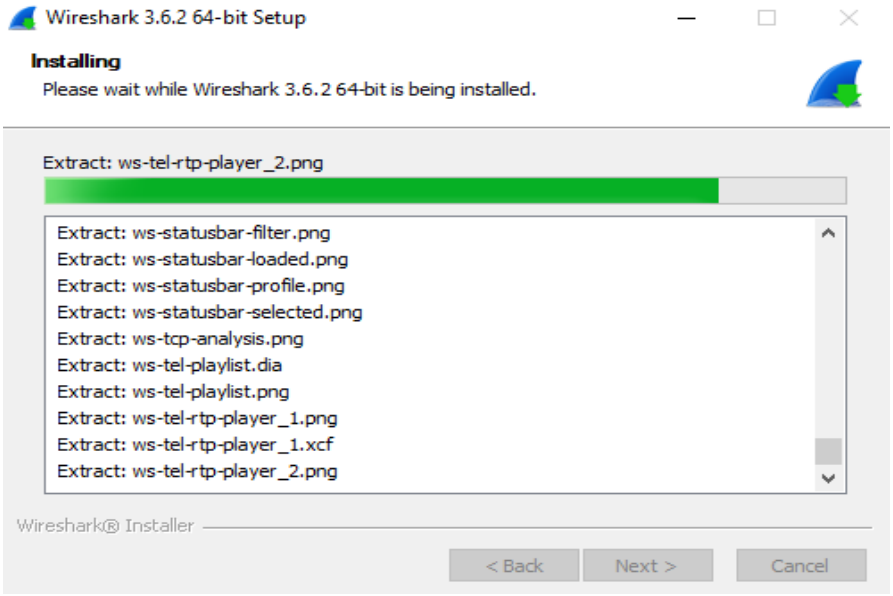
- Jika npcap sudah terinstall pada perangkat ,klik next



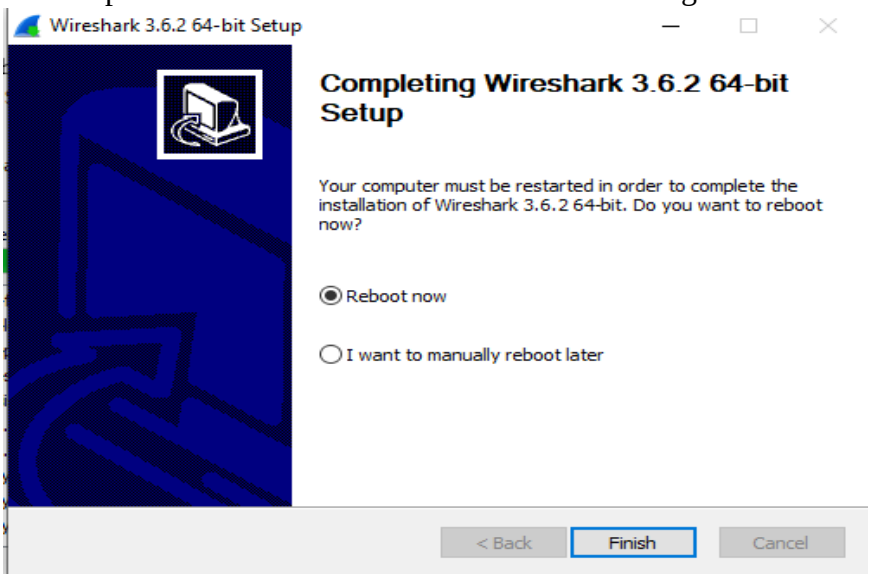
- Install USBCap



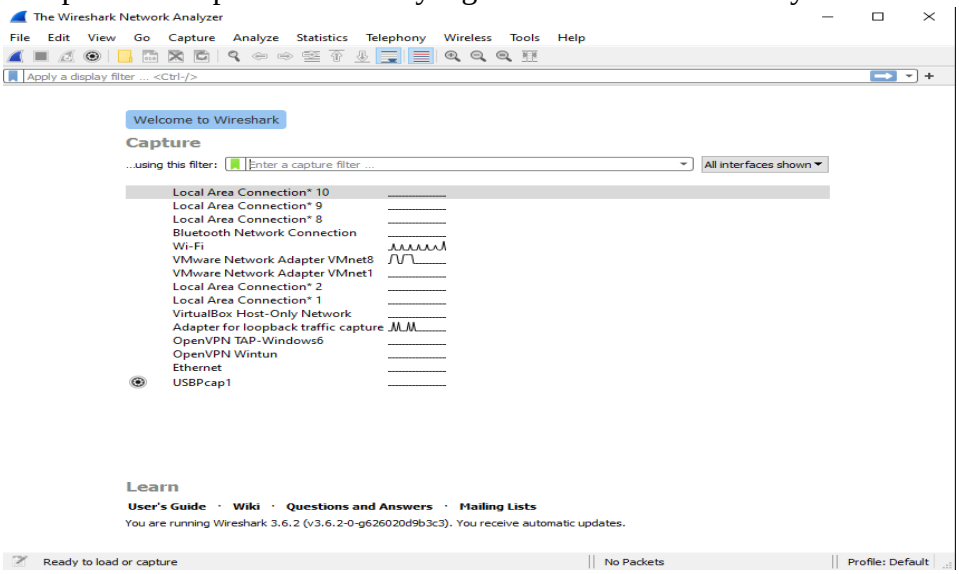
- Proses instalasi wireshark sedang berjalan



- Setelah proses instalasi selesai bisa di reboot sekarang atau nanti

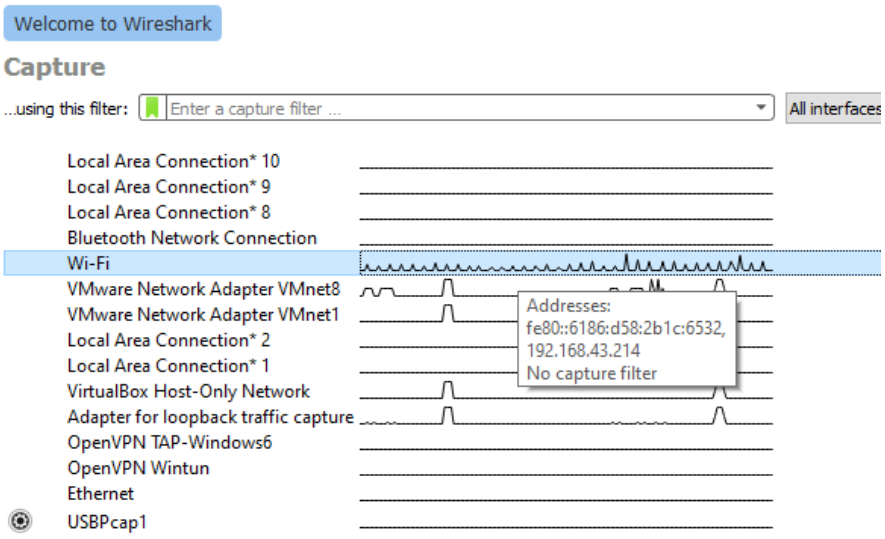


- Tampilan menu pada wireshark yang telah diinstall sebelumnya

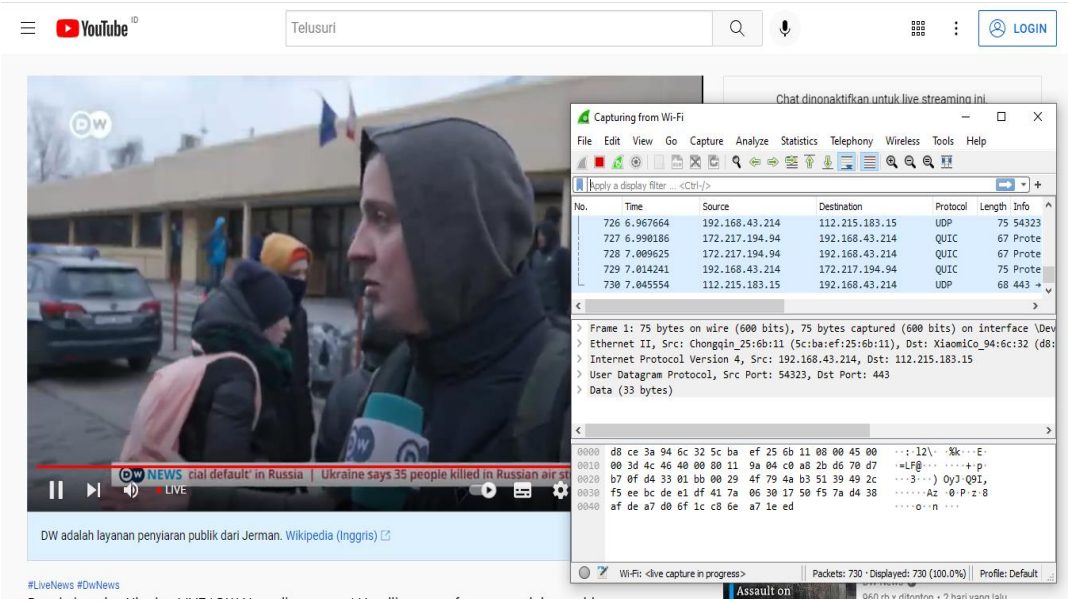


III. Analisa QoS

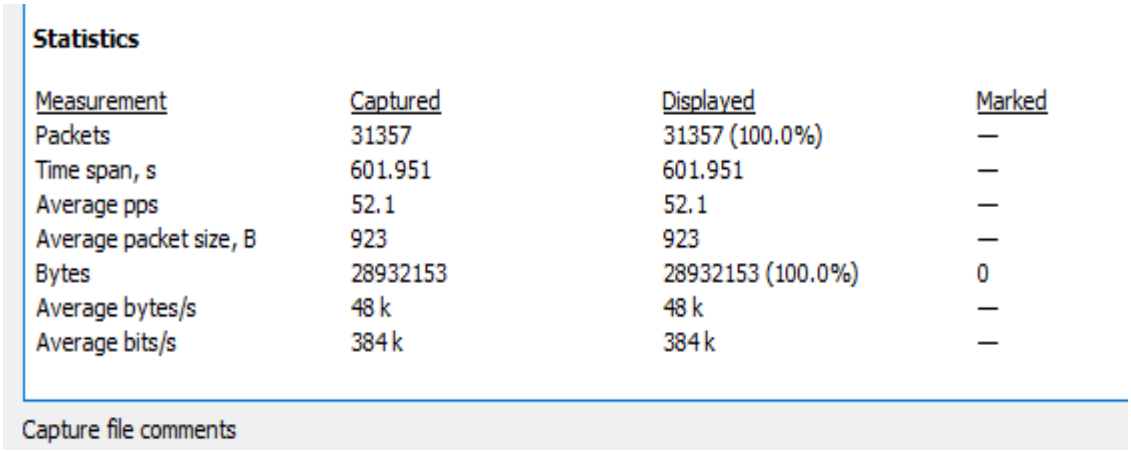
Pilih WiFi untuk analisis trafik jaringan



Kemudian, buka youtube dan capture selama beberapa menit



Statistic Captures



Statistics

Measurement	Captured	Displayed	Marked
Packets	31357	31357 (100.0%)	—
Time span, s	601.951	601.951	—
Average pps	52.1	52.1	—
Average packet size, B	923	923	—
Bytes	28932153	28932153 (100.0%)	0
Average bytes/s	48 k	48 k	—
Average bits/s	384 k	384 k	—

Capture file comments

- **Throughput**
  Persamaan perhitungannya yaitu :
  Jumlah Bytes / time span
  = 28932153 / 601.951
  = 48.063,967 b x 8
  = 384.511,576
  = 384 k
- **Packet Loss**
  Persamaan perhitungannya yaitu :
  [((Paket Dikirim – Paket Diterima) / Paket Dikirim) x 100]
  = [((31357 – 31357) / 31357) x 100]
  = (0 / 31357) x 100
  = 0.0 %

- **Delay**
  Persamaan perhitungannya yaitu:
  Total Delay / Total Paket yang diterima
  = 601,951 / 31357
  = 0,0191967 sec

- **Jitter**
  Persamaan perhitungannya yaitu:
  Total Variasi Delay = Delay – rata rata delay
  = 601,951 – 0,0191967
  = 601,9318033

  Jitter = Total Variasi Delay / Total Paket yang diterima
  = 601,9318033 / 31357
  = 0,0191960 sec