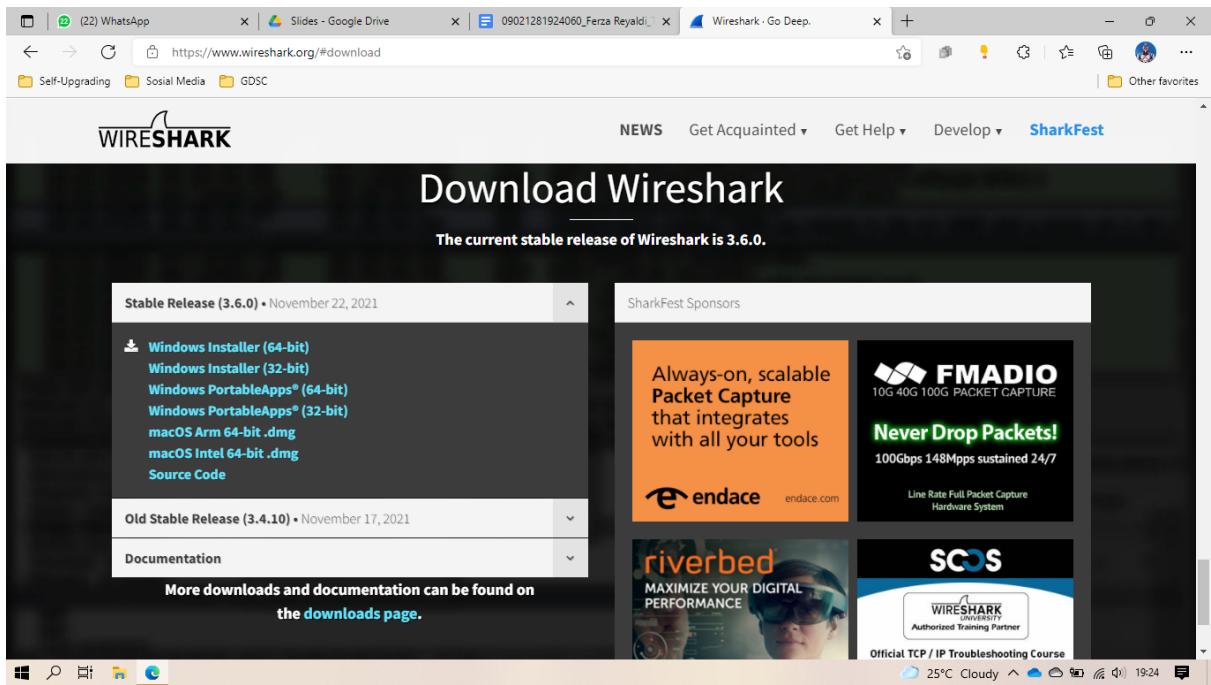


Nama : Ferza Reyaldi  
NIM : 09021281924060  
Mata Kuliah : Keamanan Jaringan Komputer

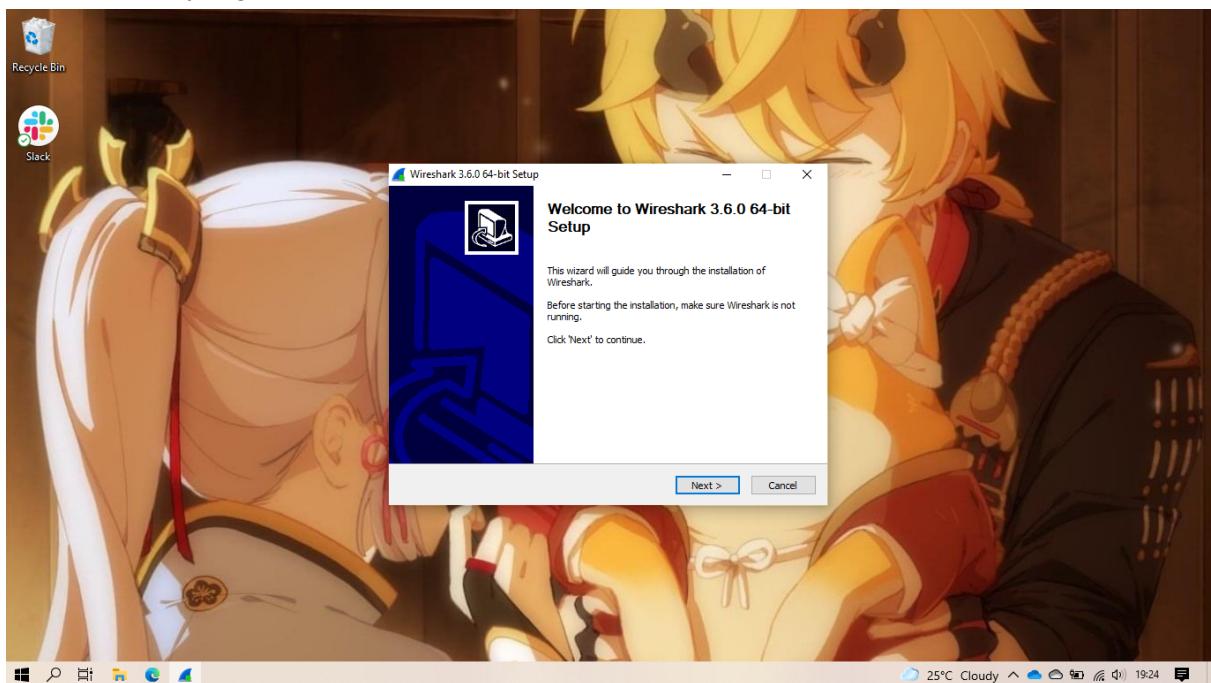
### Tugas Pertemuan 3 (Pertemuan 13)

#### Instal Wireshark Pada Komputer

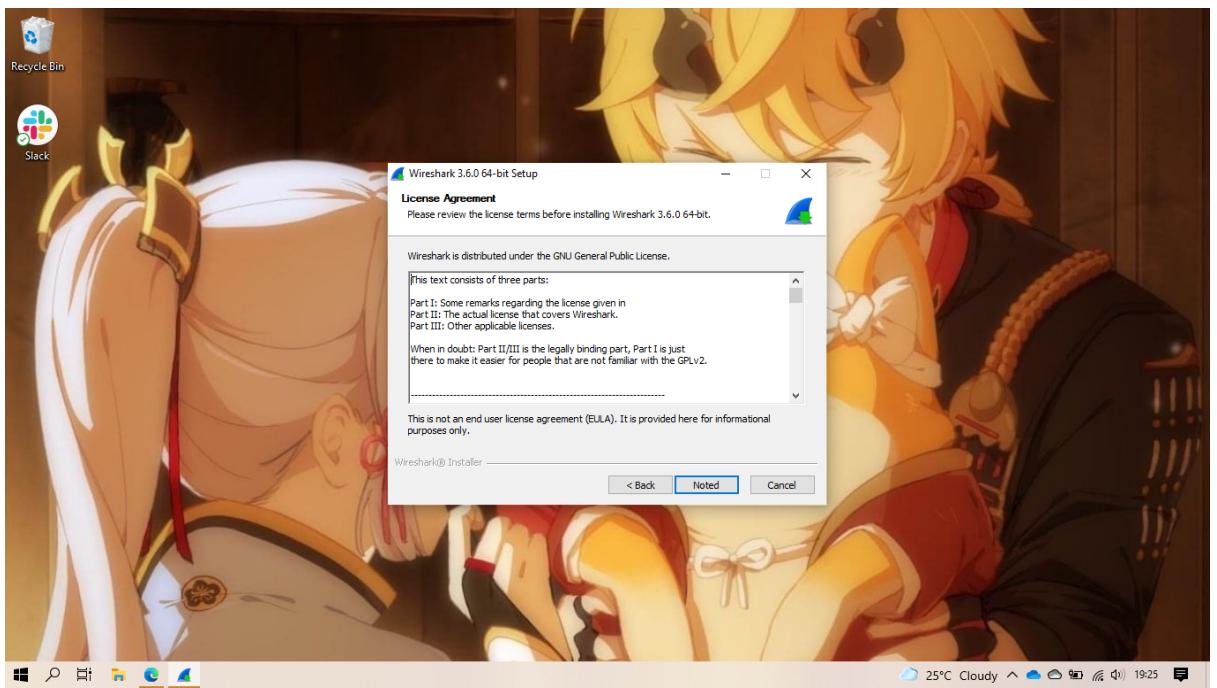
- 1) Buka website <https://www.wireshark.org/>



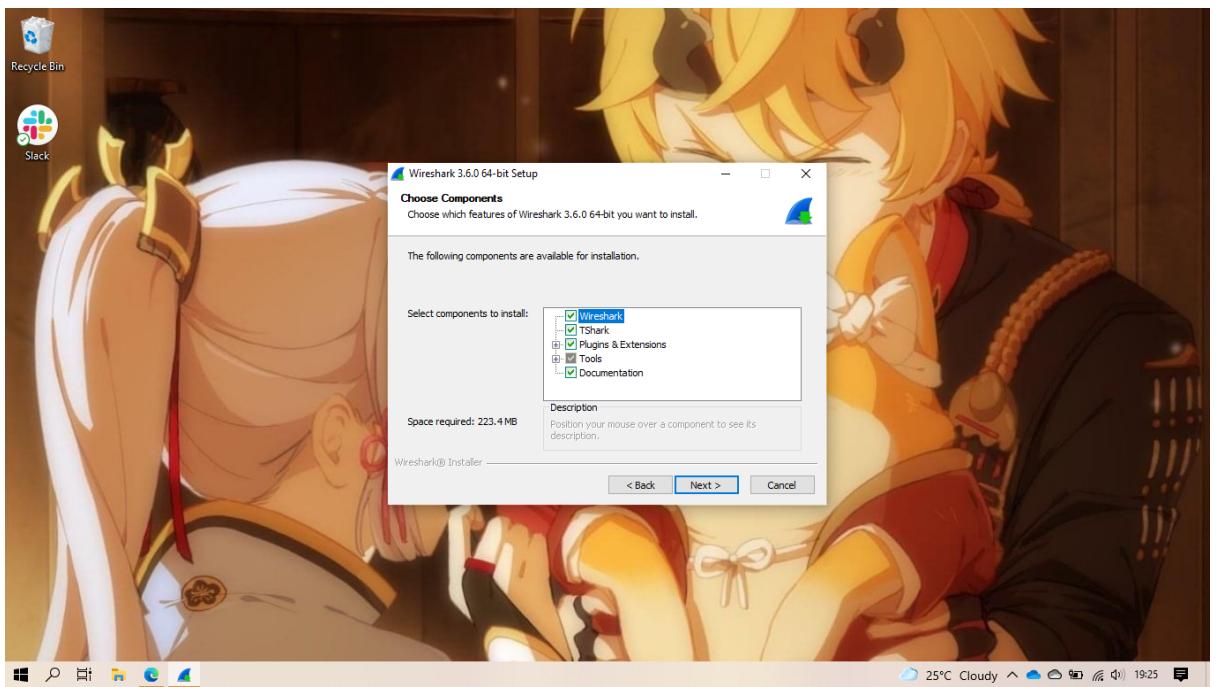
- 2) Tekan tombol download, pilih operasi sistem yang sesuai dengan komputer anda.
- 3) Buka installer yang telah diunduh, tekan next.



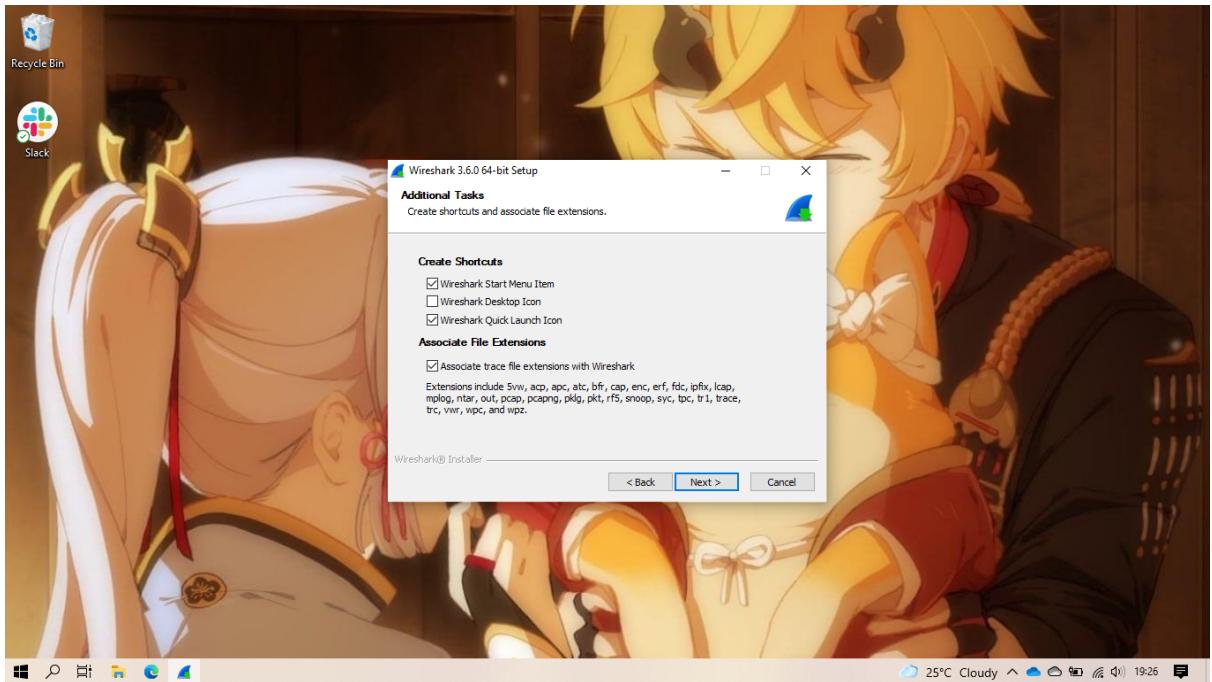
4) Tekan noted.



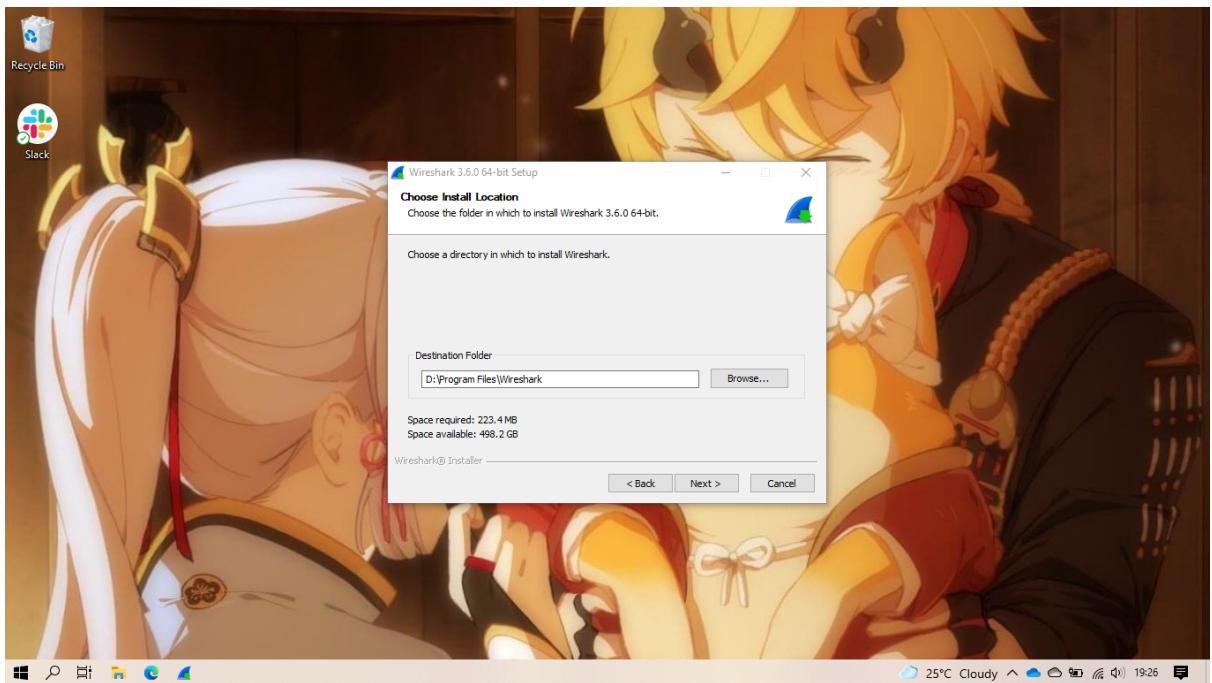
5) Pilih semua checkbox, kemudian tekan next.



6) Tekan next.

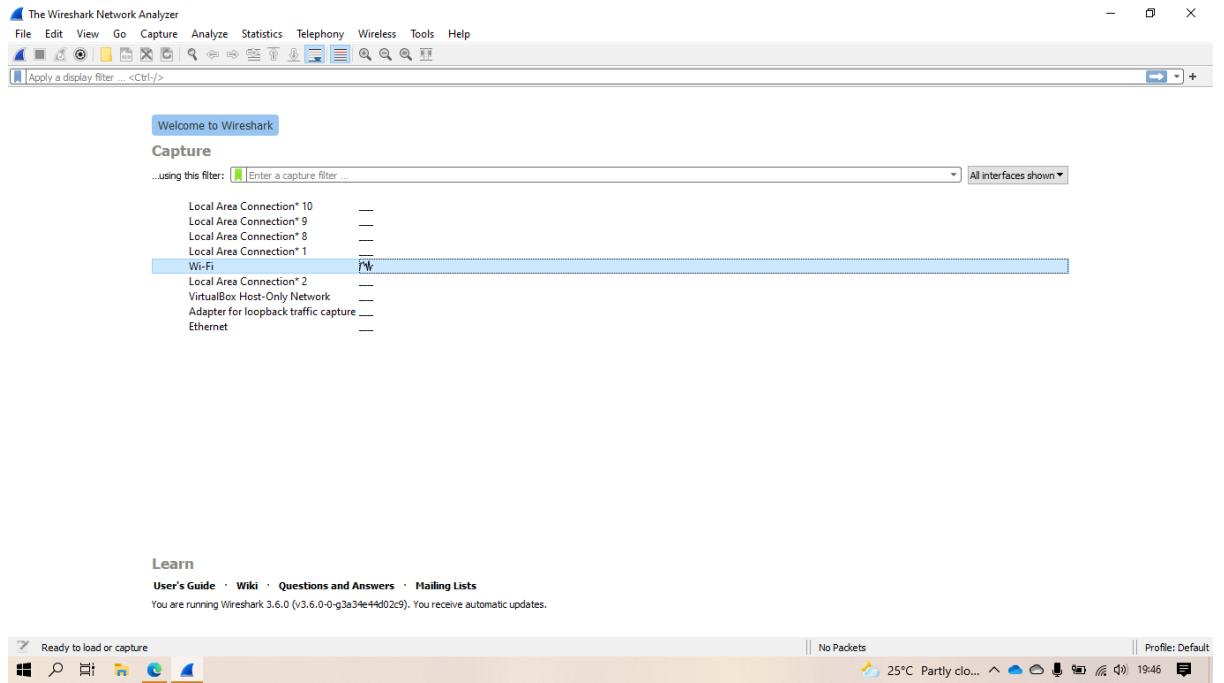


7) Pilih direktori menginstal wireshark dan tekan next 4 kali. Tunggu sampai proses instalasi selesai.

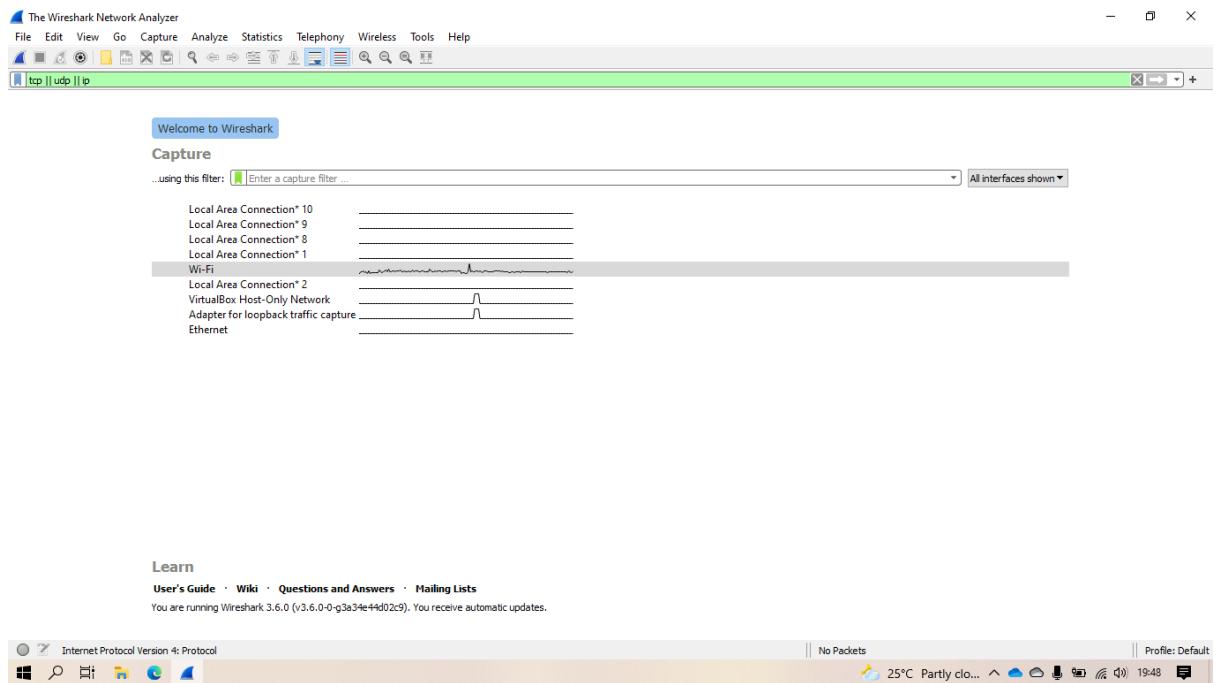


## Dasar-dasar Penggunaan Wireshark

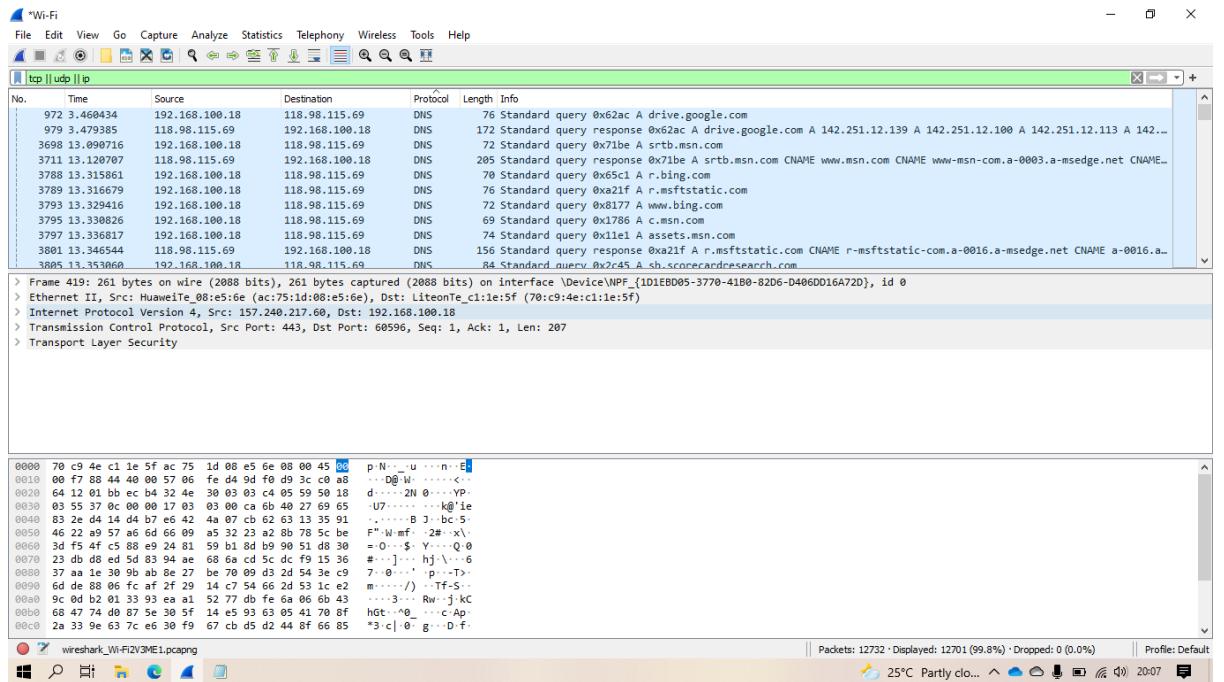
- 1) Pilih network interface, sebagai contoh dipilih wifi.



- 2) Masukkan filter TCP, UDP, dan IP dengan menuliskan **tcp || udp || ip**.



3) Klik start capturing packets untuk mulai menangkap traffic.



4) Kemudian tekan stop capturing packets.

### Analisa Hasil Capture (TCP, UDP, IP)

IP:

IP komputer saya adalah 192.168.100.18.

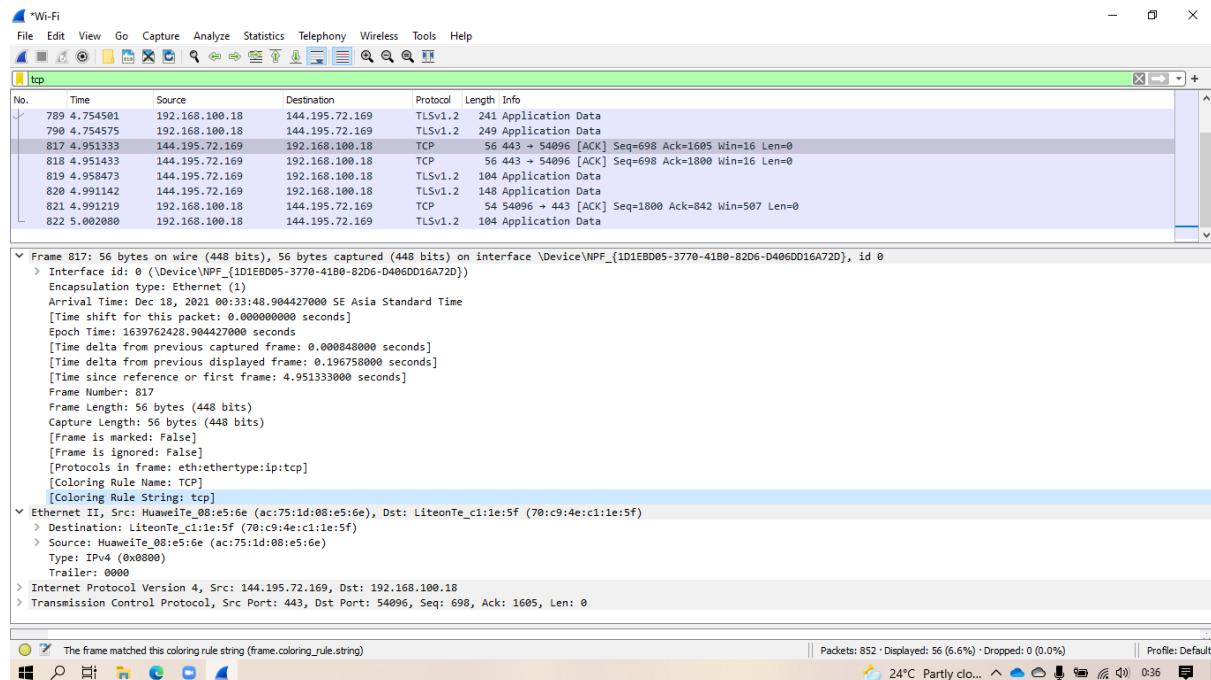
IP website yang dibuka adalah 144.195.72.169.

## TCP:

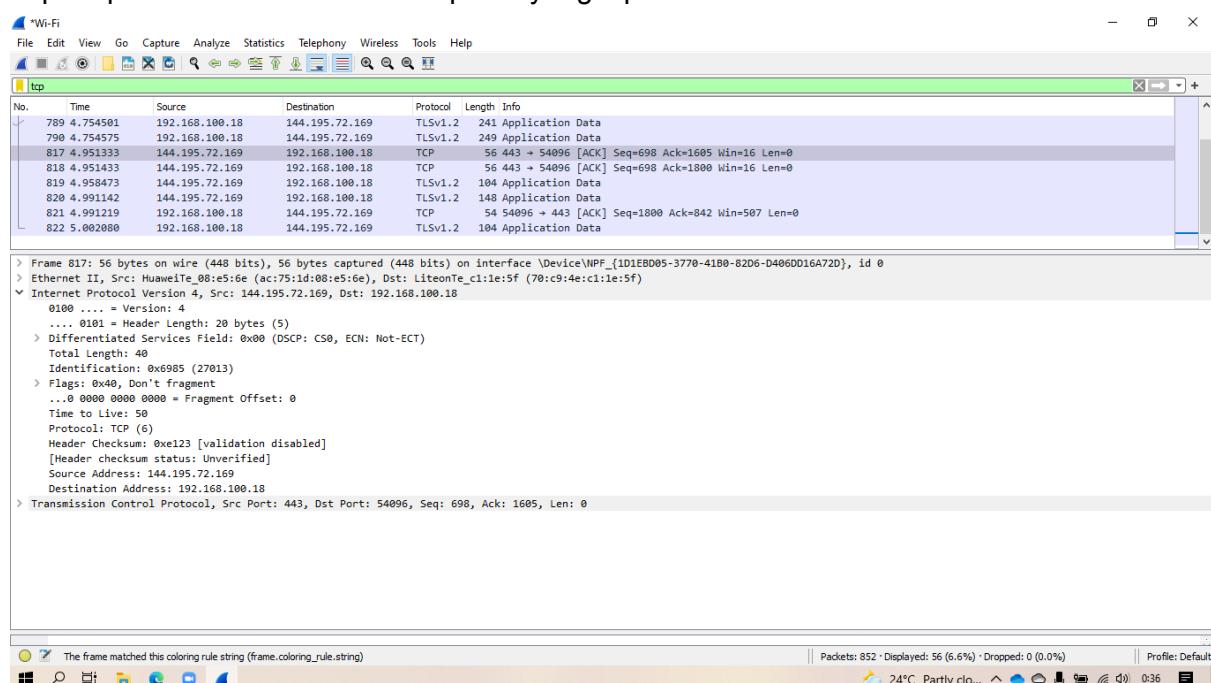
TCP digunakan sebagai protokol untuk koneksi yang bersifat reliable.

TCP bersifat connection oriented, artinya sebelum proses transmisi data terjadi, dua aplikasi TCP harus melakukan pertukaran kontrol informasi (dikenal sebagai 3 way handshaking): SYN, SYN-ACK, dan ACK.

Seperi tercantum pada screenshot di bawah ini: client mengirim paket ACK ke server.



Data yang dipertukarkan antara TCP module disebut Segment atau Data Segment. Setiap segment berisi sebuah checksum untuk memverifikasi apakah data dalam kondisi OK. Seperti pada screenshot dibawah paket yang dipilih memiliki checksum: unverified.



## UDP:

Protokol UDP memiliki karakteristik : Connectionless oriented, Unreliable, dan Non sequencing datagram service.

UDP merupakan protokol yang bersifat connectionless oriented, artinya saat melakukan pengiriman data tidak dilakukan proses handshaking. Seperti di screenshot di bawah tidak ada SYN, SYN-ACK, dan ACK seperti pada protokol TCP.

The screenshots show two instances of the Wireshark network traffic analyzer. Both instances are capturing traffic on a Wi-Fi interface, with the top one showing the raw capture and the bottom one showing the same capture with specific UDP header fields highlighted in blue.

**Top Screenshot (Raw Capture):**

- Packets:** 852
- Displayed:** 852 (100.0%)
- Dropped:** 0 (0.0%)
- Profile:** Default
- System Status:** 24°C Partly cloudy
- Time:** 0:34

**Bottom Screenshot (Colored Headers):**

- Packets:** 852
- Displayed:** 852 (100.0%)
- Dropped:** 0 (0.0%)
- Profile:** Default
- System Status:** 24°C Partly cloudy
- Time:** 0:34

**Table: Captured Packets (Top Screenshot)**

No.	Time	Source	Destination	Protocol	Length	Info
825	5.002340	192.168.100.18	144.195.72.169	UDP	1158	49905 → 8801 Len=1116
826	5.002401	192.168.100.18	144.195.72.169	UDP	1157	49905 → 8801 Len=1115
827	5.002464	192.168.100.18	144.195.72.169	UDP	1157	49905 → 8801 Len=1115
828	5.002529	192.168.100.18	144.195.72.169	UDP	130	49906 → 8801 Len=88
829	5.012199	192.168.100.18	144.195.72.169	UDP	1243	49905 → 8801 Len=1201
830	5.012294	192.168.100.18	144.195.72.169	UDP	1243	49905 → 8801 Len=1201
831	5.012353	192.168.100.18	144.195.72.169	UDP	1243	49905 → 8801 Len=1201
832	5.012414	192.168.100.18	144.195.72.169	UDP	1243	49905 → 8801 Len=1201
833	5.012448	192.168.100.18	144.195.72.169	UDP	106	49906 → 8801 Len=64

**Table: Captured Packets (Bottom Screenshot)**

No.	Time	Source	Destination	Protocol	Length	Info
825	5.002340	192.168.100.18	144.195.72.169	UDP	1158	49905 → 8801 Len=1116
826	5.002401	192.168.100.18	144.195.72.169	UDP	1157	49905 → 8801 Len=1115
827	5.002464	192.168.100.18	144.195.72.169	UDP	1157	49905 → 8801 Len=1115
828	5.002529	192.168.100.18	144.195.72.169	UDP	130	49906 → 8801 Len=88
829	5.012199	192.168.100.18	144.195.72.169	UDP	1243	49905 → 8801 Len=1201
830	5.012294	192.168.100.18	144.195.72.169	UDP	1243	49905 → 8801 Len=1201
831	5.012353	192.168.100.18	144.195.72.169	UDP	1243	49905 → 8801 Len=1201
832	5.012414	192.168.100.18	144.195.72.169	UDP	1243	49905 → 8801 Len=1201
833	5.012448	192.168.100.18	144.195.72.169	UDP	106	49906 → 8801 Len=64

**Analysis (Top Screenshot):**

- Interface id: 0 (\Device\NPF\_{1D1EB0D5-3770-41B0-82D6-D406DD16A72D})
- Encapsulation type: Ethernet (1)
- Arrival Time: Dec 18, 2021 00:33:48.955434000 SE Asia Standard Time
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1639762428.955434000 seconds
- [Time delta from previous captured frame: 0.000056000 seconds]
- [Time delta from previous displayed frame: 0.000056000 seconds]
- [Time since reference or first frame: 5.002340000 seconds]
- Frame Number: 825
- Frame Length: 1158 bytes (9264 bits)
- Capture Length: 1158 bytes (9264 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:etherType:ip:udp:data]
- [Coloring Rule String: udp]

**Analysis (Bottom Screenshot):**

- Ethernet II, Src: LiteonTe\_c1:e1:5f (70:c9:4e:c1:1e:5f), Dst: HuaweiTe\_08:e5:6e (ac:75:1d:08:e5:6e)
- Destination: HuaweiTe\_08:e5:6e (ac:75:1d:08:e5:6e)
- Source: LiteonTe\_c1:e1:5f (70:c9:4e:c1:1e:5f)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.100.18, Dst: 144.195.72.169
- User Datagram Protocol, Src Port: 49905, Dst Port: 8801
- Data (1116 bytes)