

LAPORAN INSTALLASI DAN PROBLEM SOLVING "WIRESHARK"



DI BUAT OLEH:

NAMA: TITIN AGISTINA

NIM: 09011182025012

KELAS: SK4 B INDRALAYA

MATA KULIAH: KOMUNIKASI DATA

**JURUSAN SISTEM KOMPUTER,
FAKULTAS ILMU KOMPUTER,
UNIVERSITS SRIWIJAYA TA: 2021/2022**

I. PENGERTIAN WIRESHARK

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.

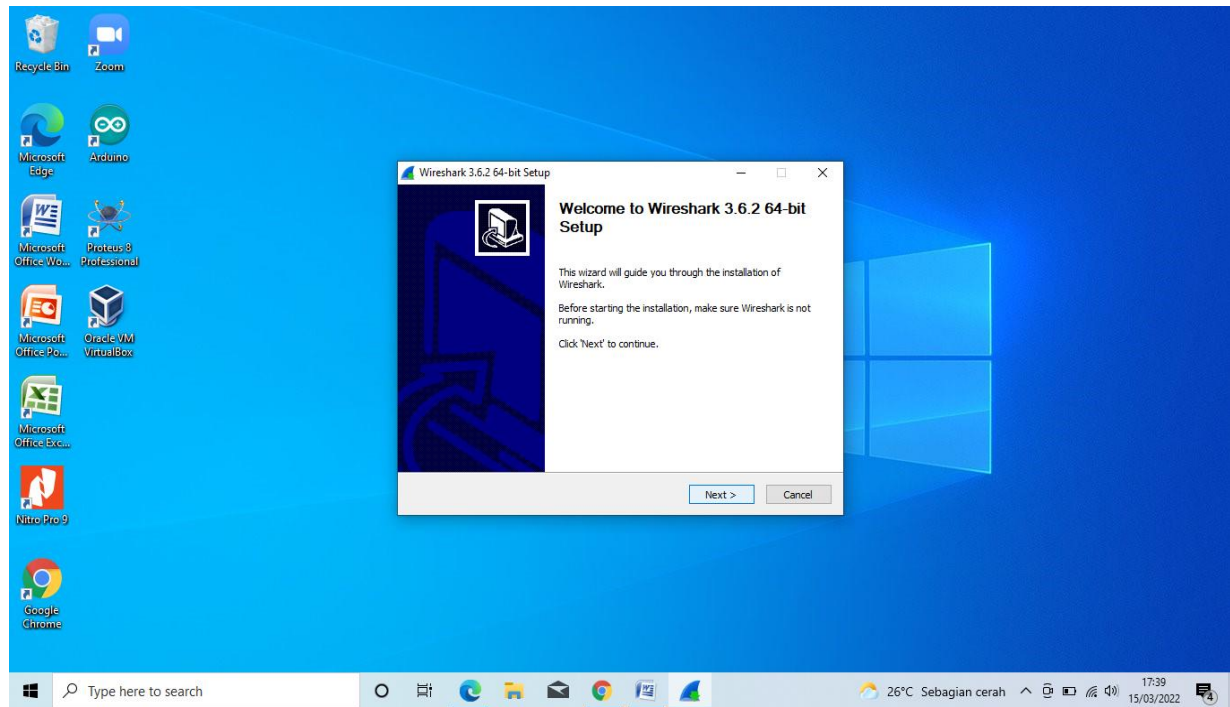
Wireshark mendukung banyak format file paket capture/trace termasuk .cap dan .erf. Selain itu, alat dekripsi yang terintegrasi di dalamnya mampu menampilkan paket-paket terekripsi dari sejumlah protokol-protokol yang umum digunakan pada jaringan internet saat ini, termasuk WEP dan WPA/WPA2. Salah satu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

II. FUNGSI WIRESHARK

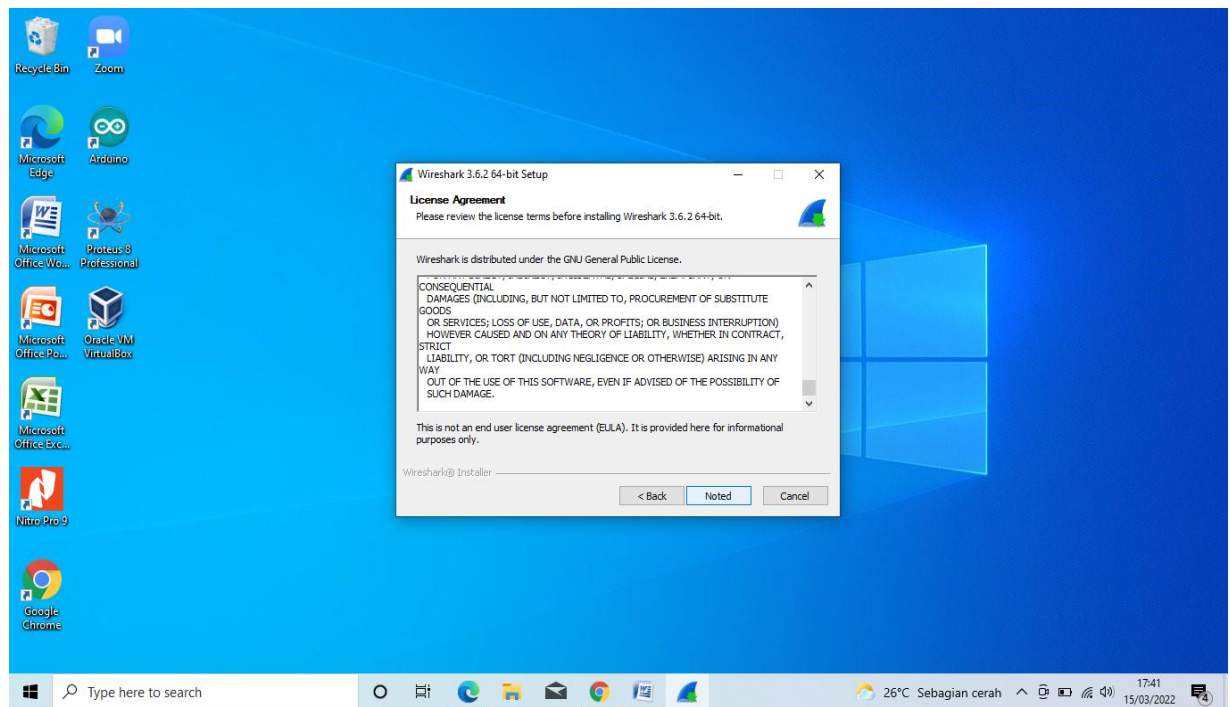
Dalam persepsi yang positif, Wireshark berguna untuk pekerjaan analisis jaringan. Cara kerjanya yaitu dengan ‘menangkap’ paket-paket data dari protokol-protokol yang berbeda dari berbagai tipe jaringan yang umum ditemukan di dalam trafik jaringan internet. Paket-paket data tersebut ‘ditangkap’ lalu ditampilkan 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.

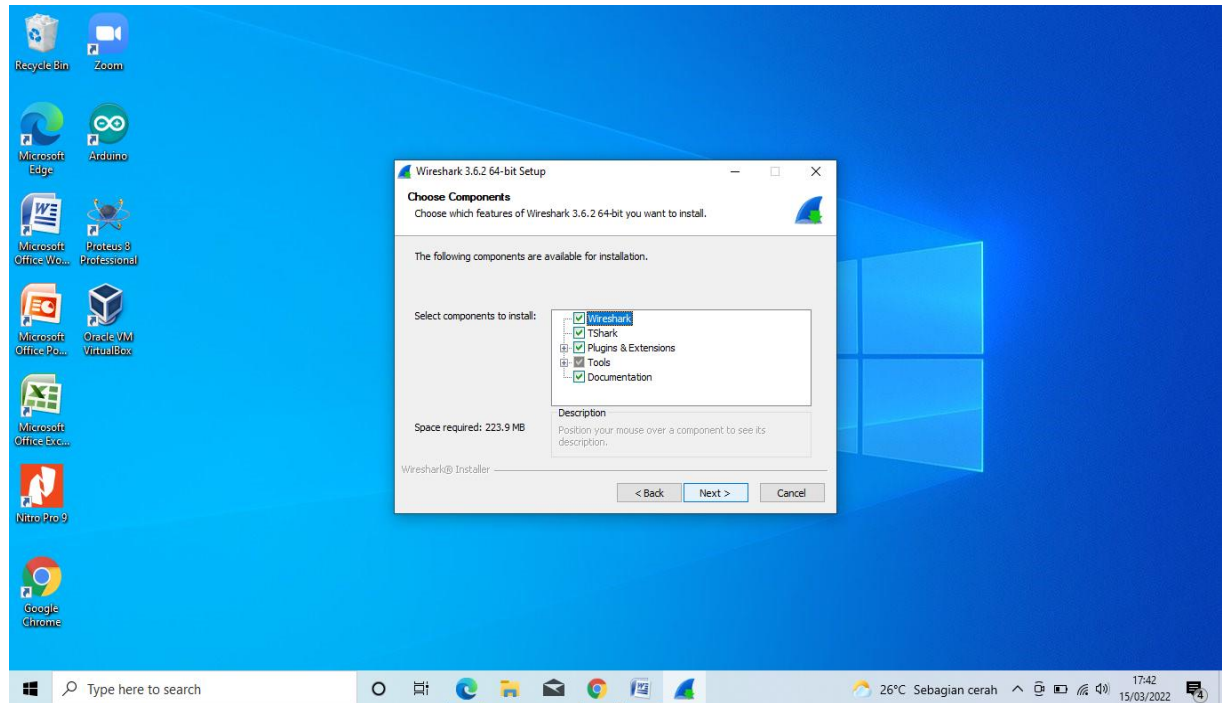
III. CARA KERJA WIRESHARK

1. Pertama-tama kita download terlebih dulu wireshark nya melalui link berikut ini :
<https://bit.ly/3cHSe9H>
2. langkah selanjutnya yaitu buka file yang telah di download lalu klik next.

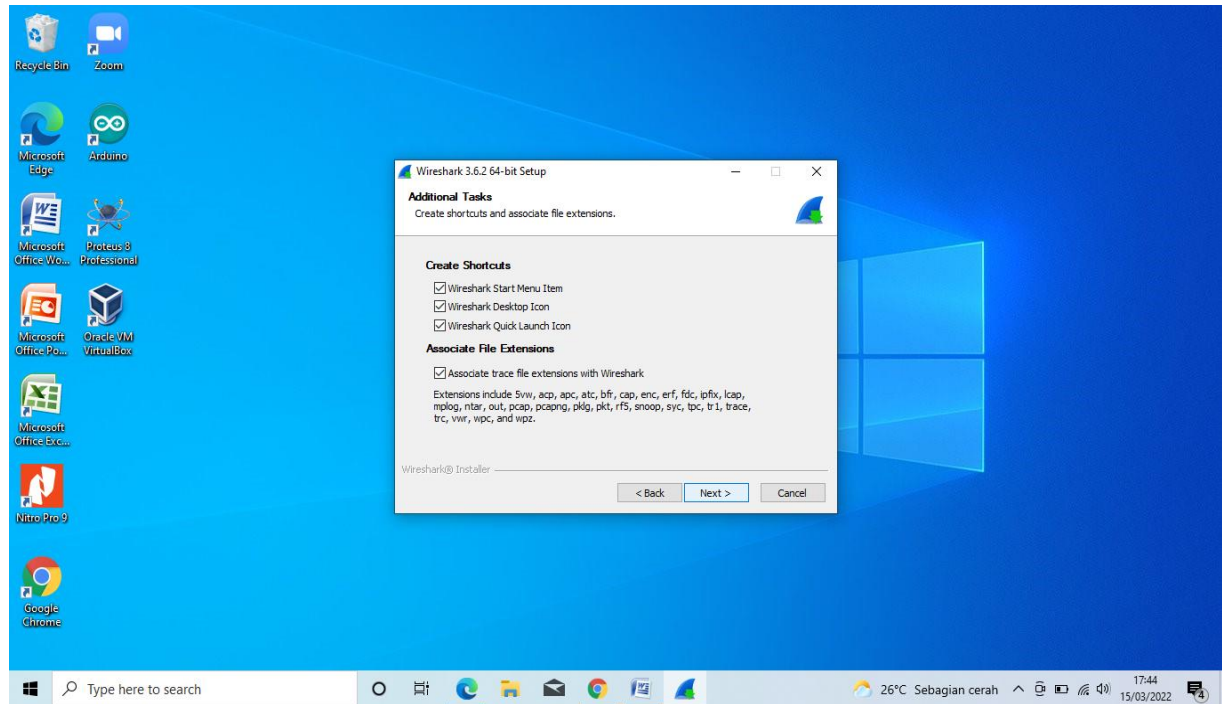


3. kemudian setelah itu akan muncul seperti gambar, dan klik noted dan pilih wireshark lalu next.

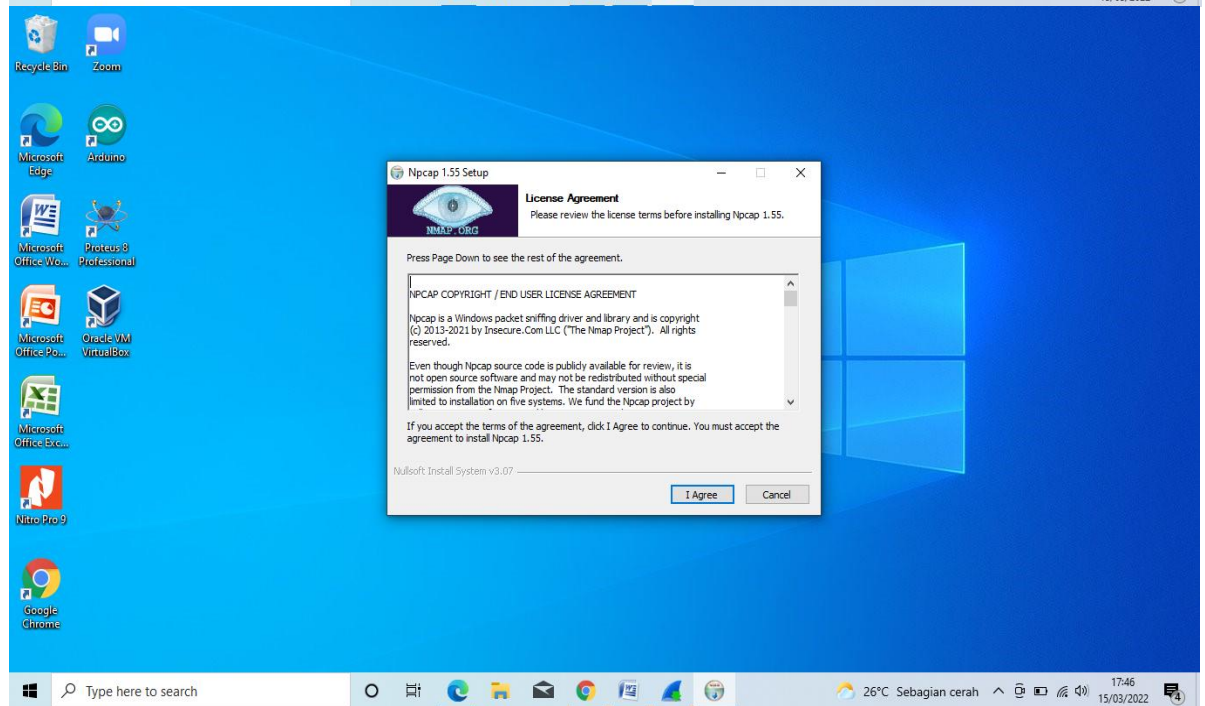
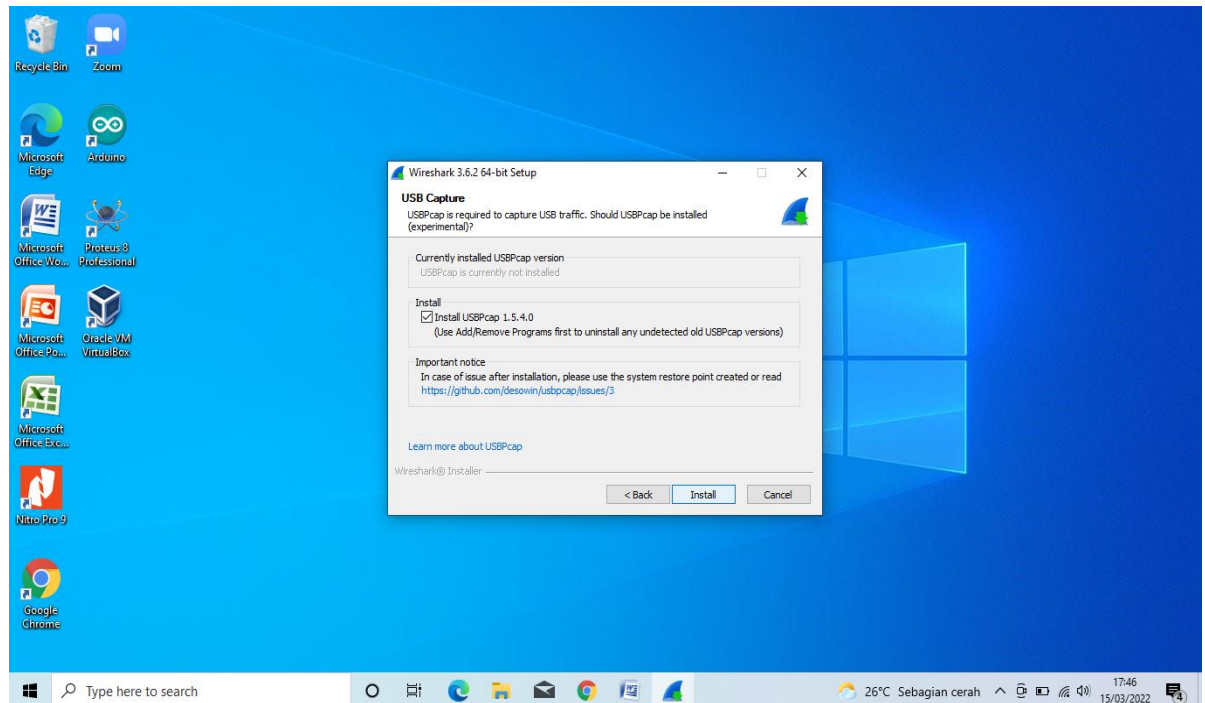


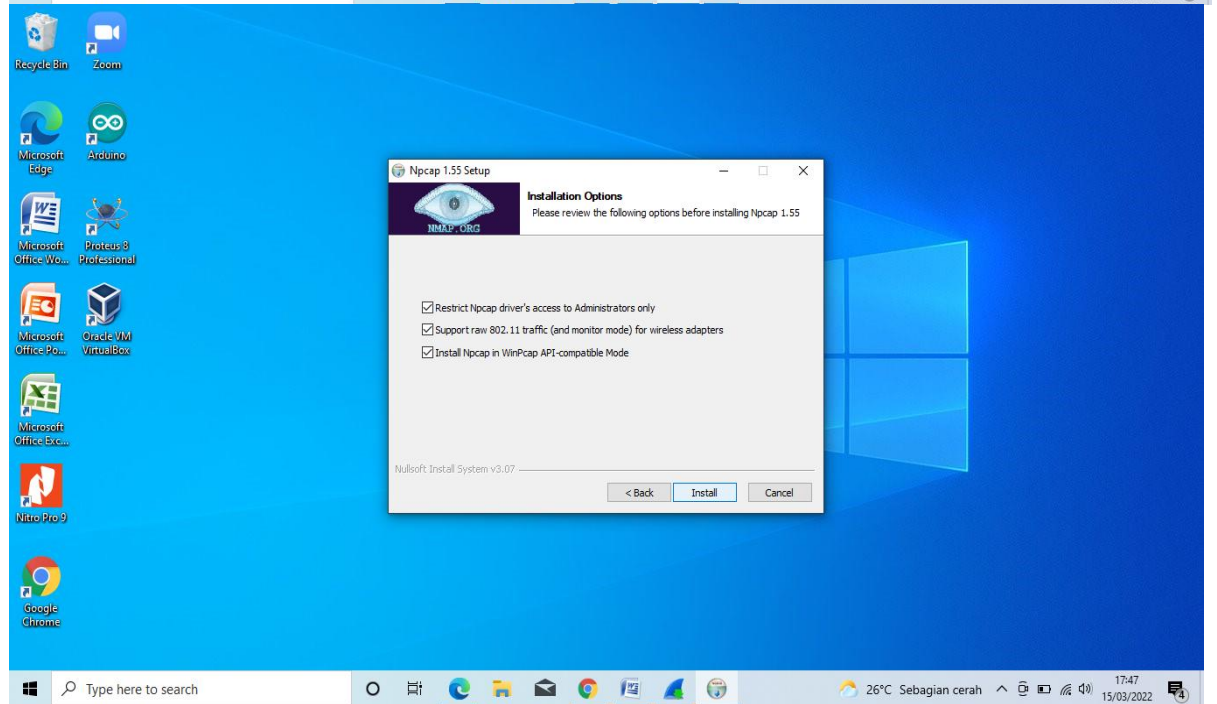
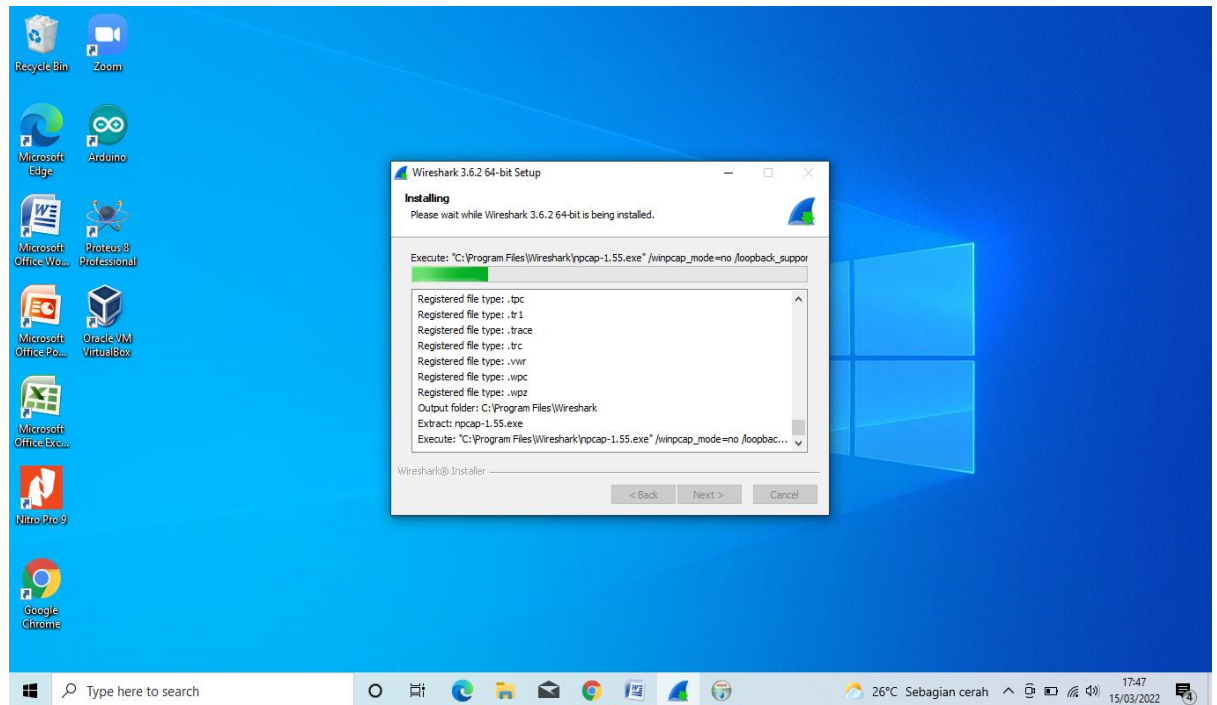


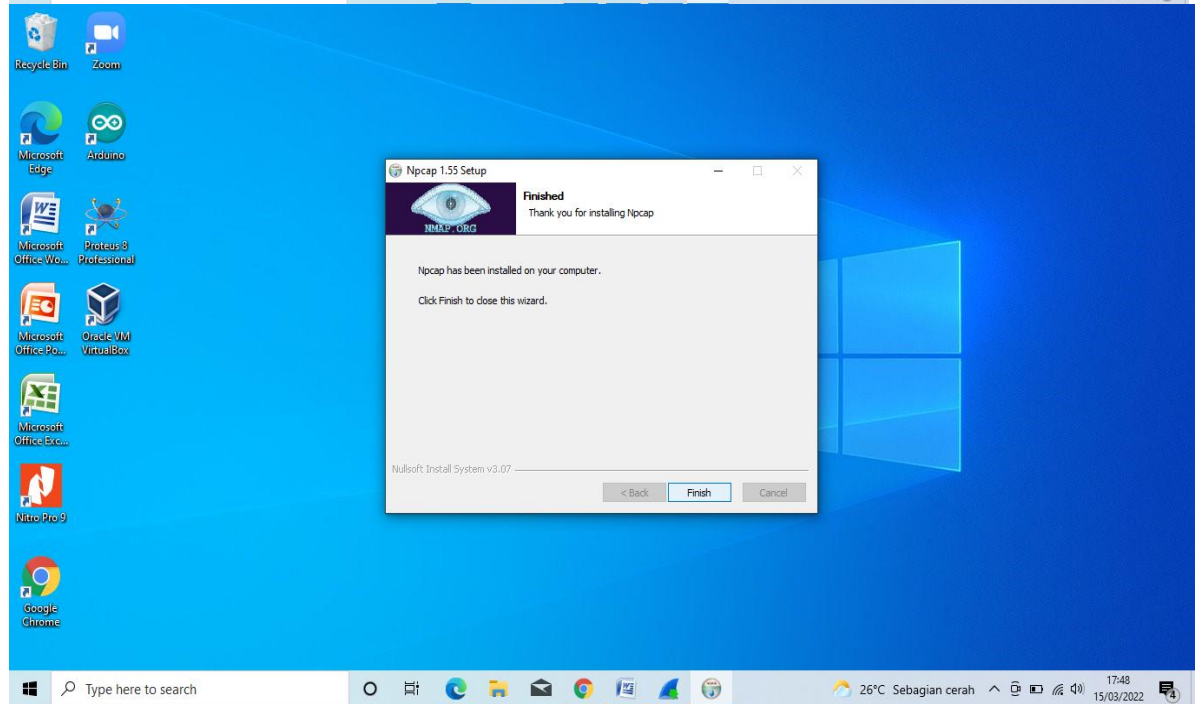
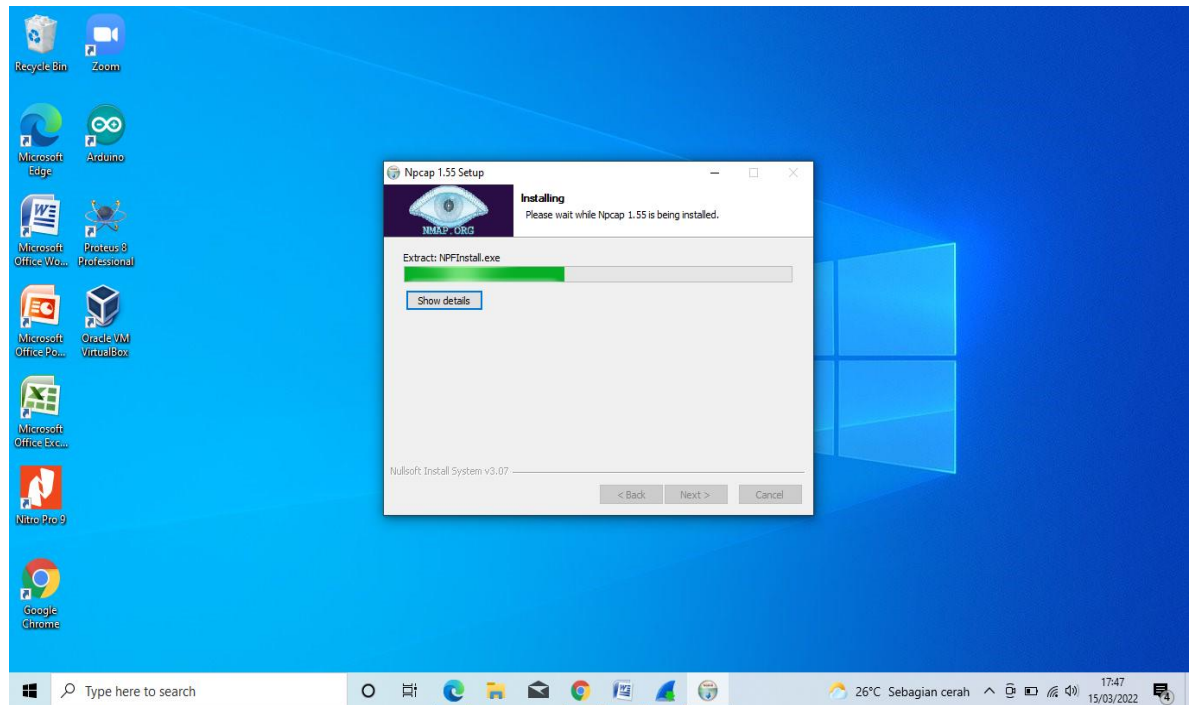
4. kemudian akan di bawa kepada tampilan dimana kita harus mencentang semua.lalu pilih next.

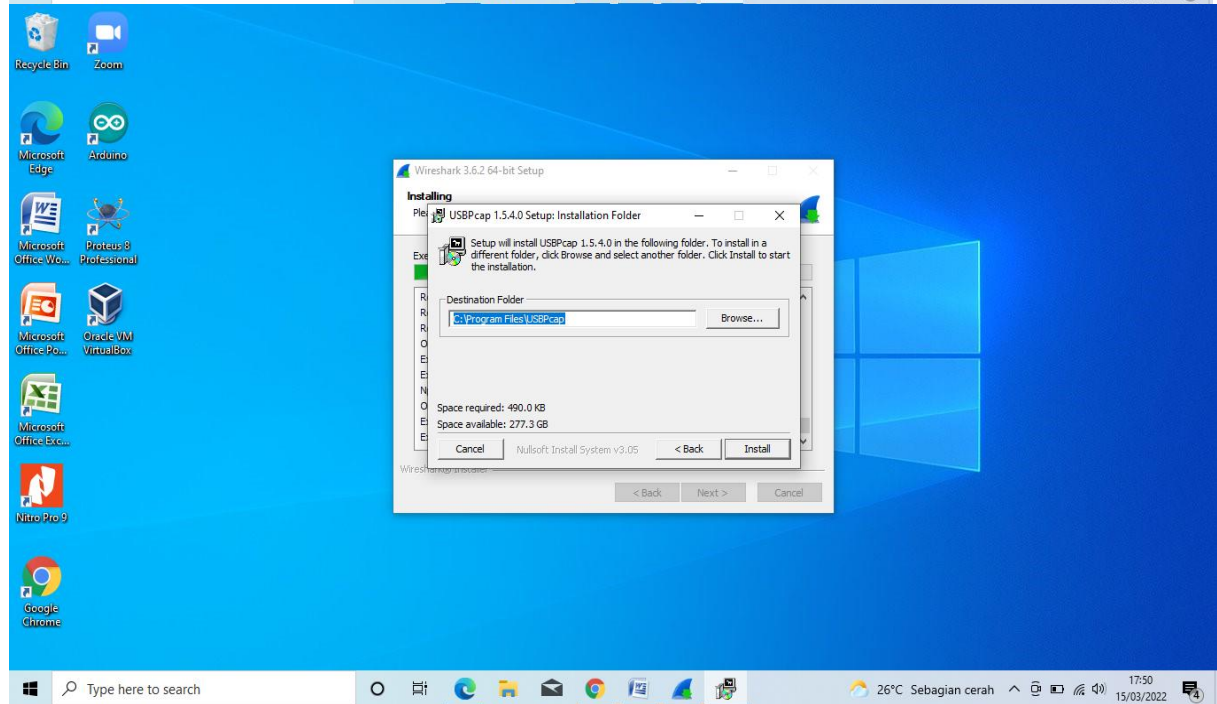
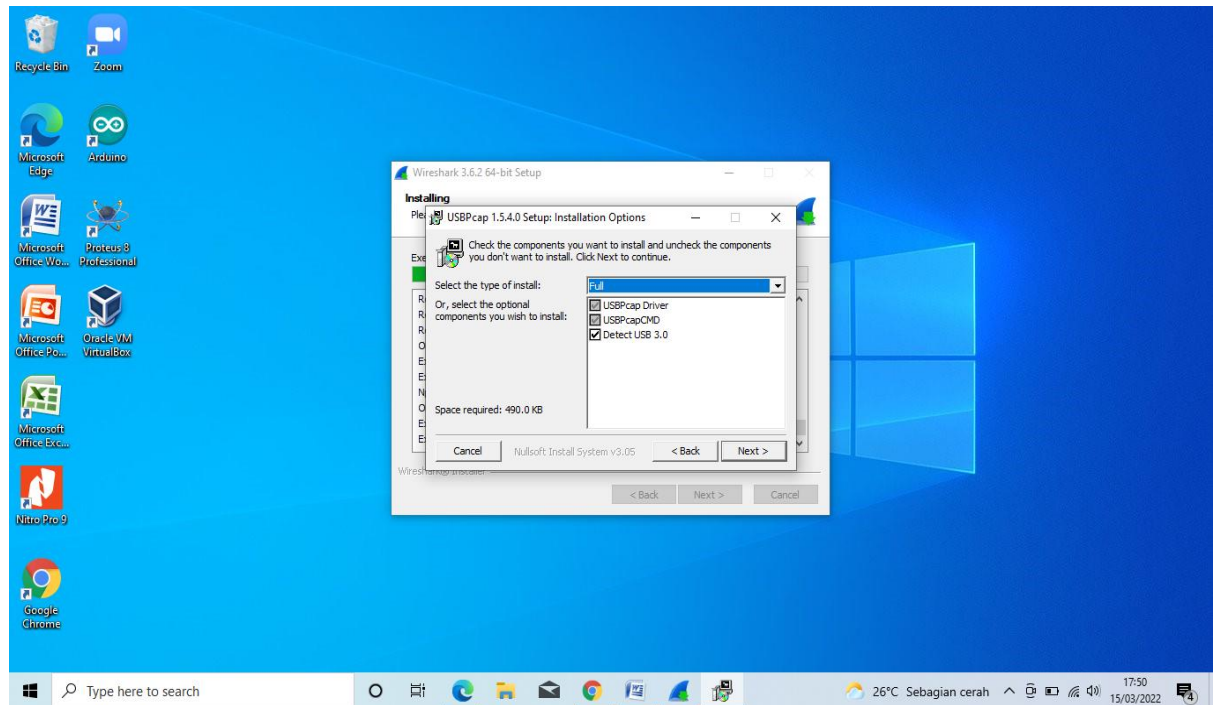


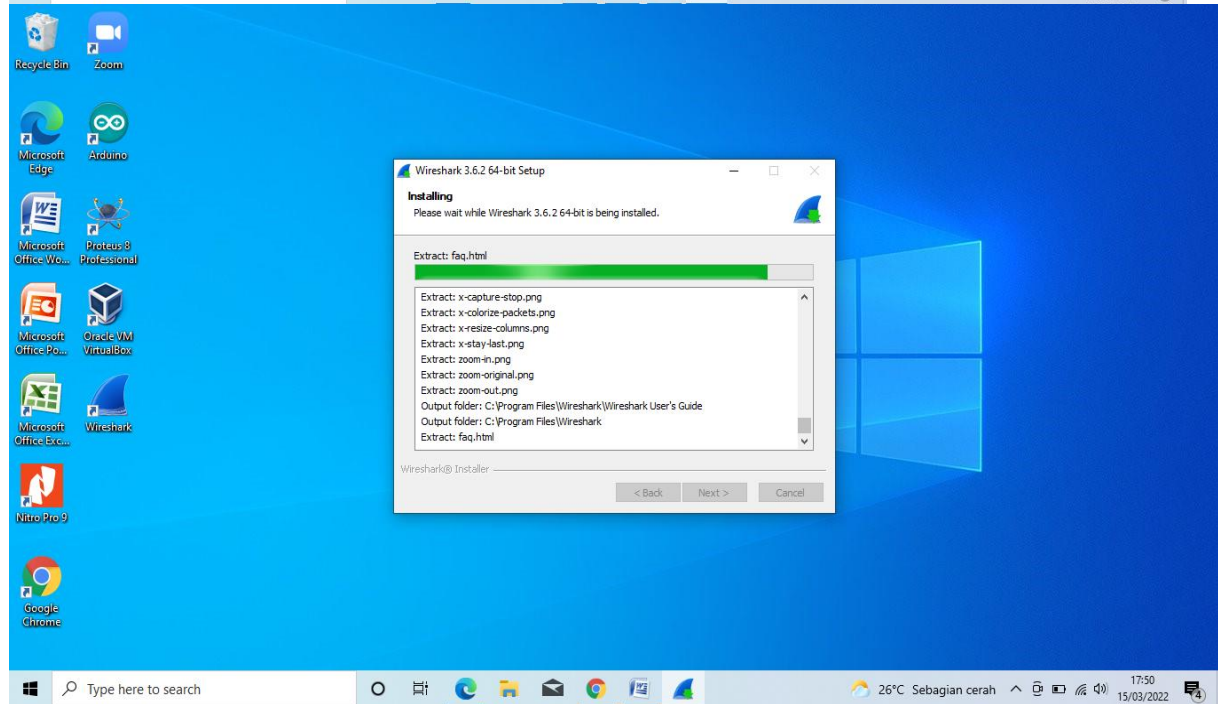
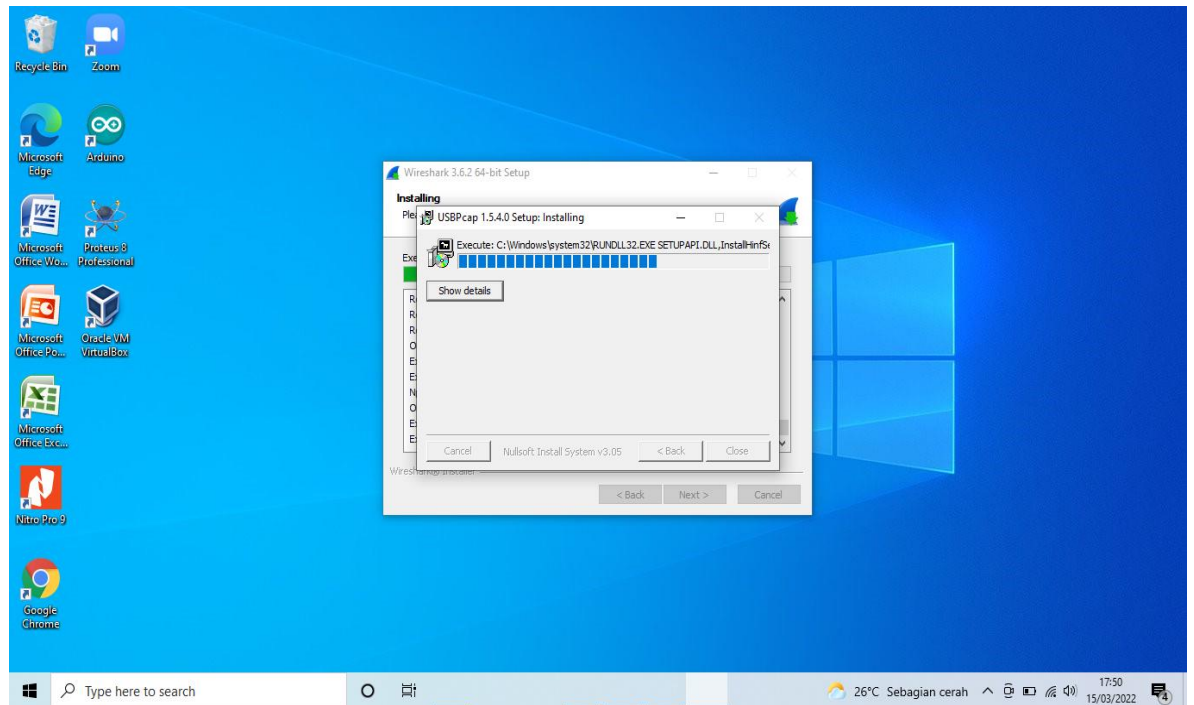
5. kemudian kita mulai install. Dan ikuti langkah-langkah pada gambar.



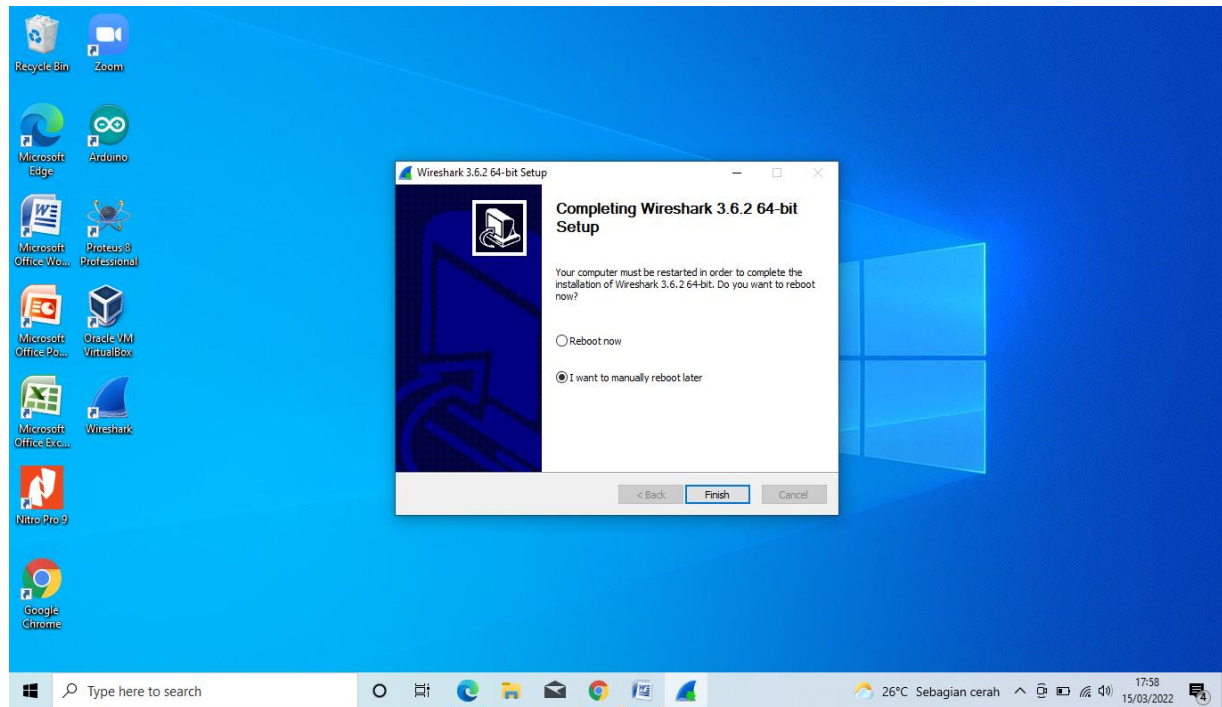




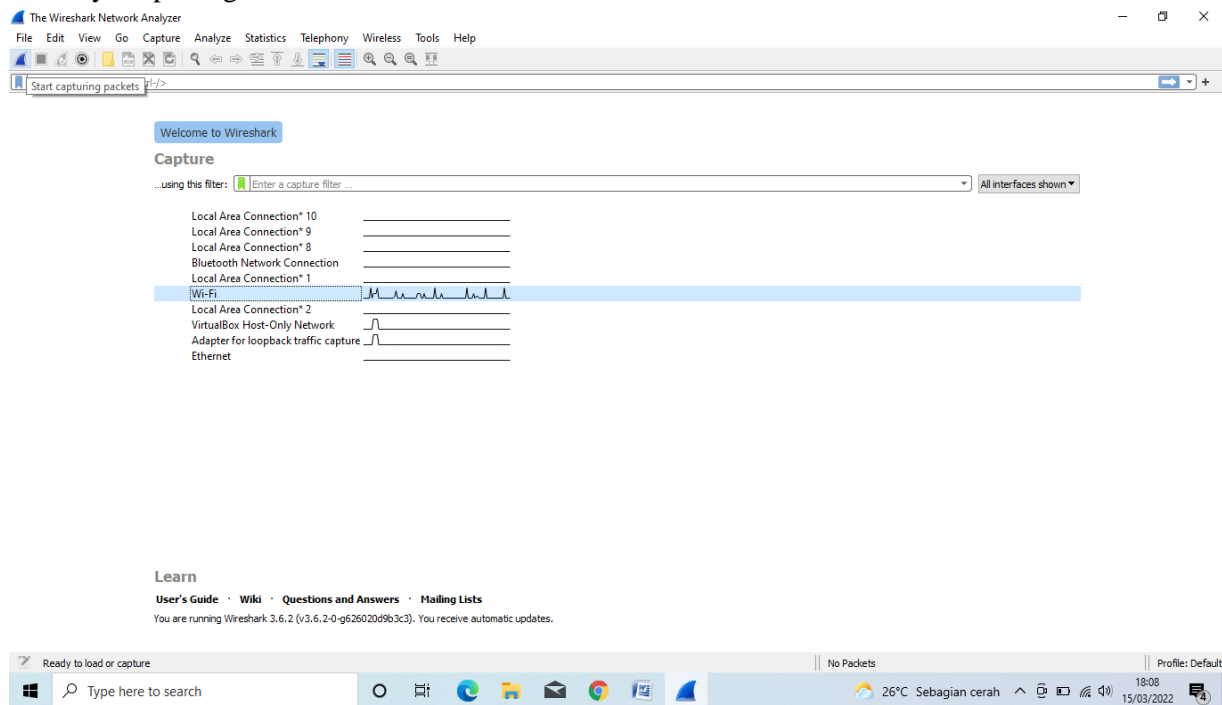




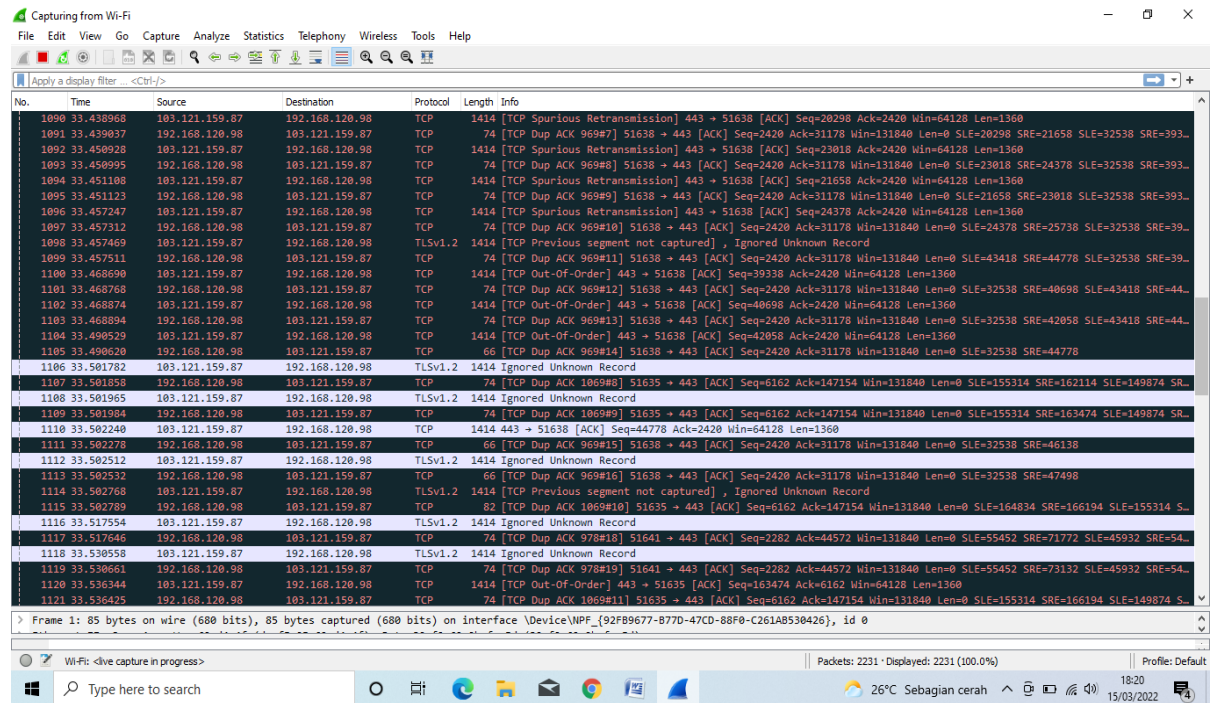
6. instalasi finish



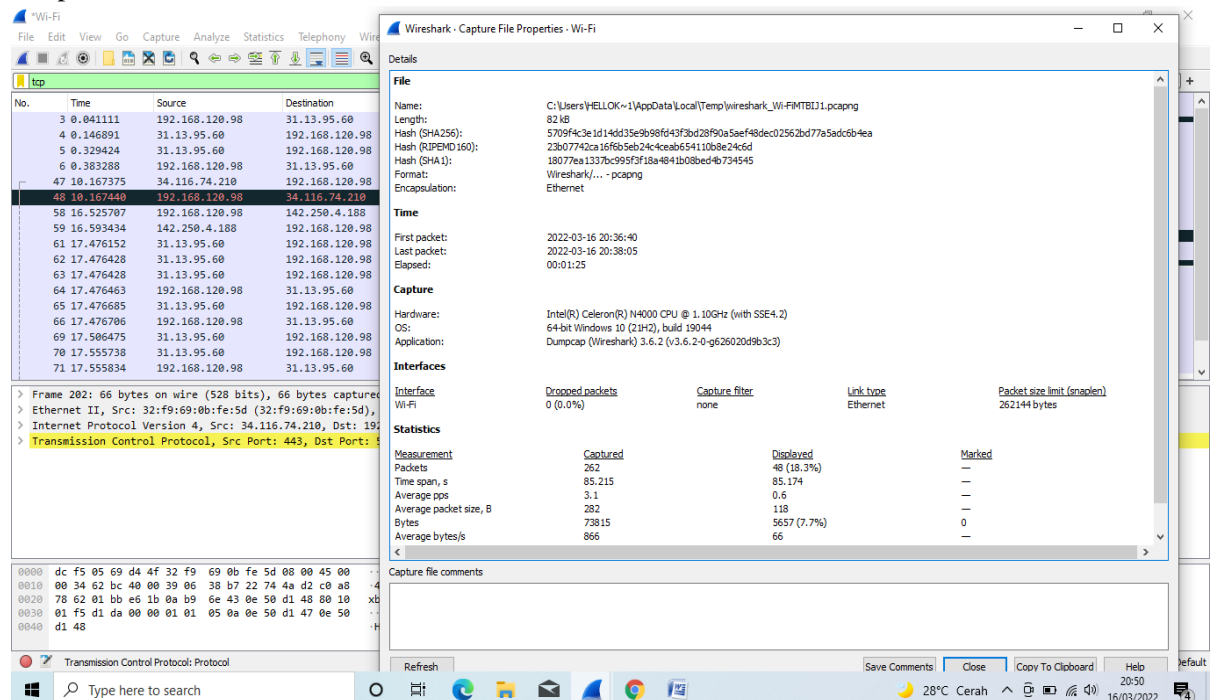
7. kita open wireshark nya dengan cara klik kanan lalu pilih run administrator, lalu akan menampilkan berbagai macam option. Disini saya menggunakan paket wifi maka yang akan saya capturing adalah wifi



8. ini adalah tampilan dimana jaringan paket data wifi saya



9. untuk menganalisa lalu lintas jaringan sebelumnya saya sudah menonton youtube terlebih dulu di situs web selama 1 menit. Dan kembali lagi pada wireshark nya menunggu selama 1 menit, kemudian memfilter nya menggunakan “tcp.analysis.lost_segment” karena hanya untuk melihat paket data lost nya. Kemudian kembali memfilter kembali dengan”tcp” lalu enter kemudian capture file properties. Sehingga perhitungannya bisa didapatkan



IV. ANALISIS PAKET DATA Q OS

1) Throughput:

Jumlah bytes : time span = hasil bytes

$$73815 : 85,215 = 866,2207357859532 \text{ b x } 8$$

$$= 6929 \text{ k}$$

Wireshark - Capture File Properties - Wi-Fi

Details

Name: C:\Users\HELLOK\1\AppData\Local\Temp\wireshark_Wi-FiMTBJ1.pcapng
 Length: 82 kB
 Hash (SHA256): 5709f4c3e1d14dd35e9b98f43f3bd28f90a5aef48dec02562bd77a5adc6b4ea
 Hash (RIPEMD 160): 23b07742ca16f6b5eb24c4ceab54110b8e24c5d
 Hash (SHA1): 18077ea1337bc995f3f18a4b41b08bed4b734545
 Format: Wireshark/... - pcapng
 Encapsulation: Ethernet

Time

First packet: 2022-03-16 20:36:40
 Last packet: 2022-03-16 20:38:05
 Elapsed: 00:01:25

Capture

Hardware: Intel(R) Celeron(R) N4000 CPU @ 1.10GHz (with SSE4.2)
 OS: 64-bit Windows 10 (21H2), build 19044
 Application: Dumpcap (Wireshark) 3.6.2 (v3.6.2-0-g526020d9b3c3)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Wi-Fi	0 (0.0%)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	262	48 (18.3%)	—
Time span, s	85.215	85.174	—
Average pps	3.1	0.6	—
Average packet size, B	282	118	—
Bytes	73815	5657 (7.7%)	0
Average bytes/s	866	66	—
Average bits/s	6929	531	—

2) Packet loss:

$[(\text{paket dikirim} - \text{paket diterima}) : \text{paket dikirim}] \times 100]$

$[(262 - 261) : 262] \times 100]$

$[(1) : 262] \times 100]$

= 0,3816793893129771 di bulatkan menjadi 0,4

Wireshark - Capture File Properties - Wi-Fi

Details

Name: C:\Users\HELLOK\1\AppData\Local\Temp\wireshark_Wi-FiMTBJ1.pcapng
 Length: 82 kB
 Hash (SHA256): 5709f4c3e1d14dd35e9b98f43f3bd28f90a5aef48dec02562bd77a5adc6b4ea
 Hash (RIPEMD 160): 23b07742ca16f6b5eb24c4ceab54110b8e24c5d
 Hash (SHA1): 18077ea1337bc995f3f18a4b41b08bed4b734545
 Format: Wireshark/... - pcapng
 Encapsulation: Ethernet

Time

First packet: 2022-03-16 20:36:40
 Last packet: 2022-03-16 20:38:05
 Elapsed: 00:01:25

Capture

Hardware: Intel(R) Celeron(R) N4000 CPU @ 1.10GHz (with SSE4.2)
 OS: 64-bit Windows 10 (21H2), build 19044
 Application: Dumpcap (Wireshark) 3.6.2 (v3.6.2-0-g526020d9b3c3)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Wi-Fi	0 (0.0%)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	262	1 (0.4%)	—
Time span, s	85.215	—	—
Average pps	3.1	—	—
Average packet size, B	282	66	—
Bytes	73815	66 (0.1%)	0
Average bytes/s	866	—	—
Average bits/s	6929	—	—

Capture file comments

3) Delay :

Total delay = 85,174305 s

Rata-rata delay = $0,325092767 \text{ s} \times 1000 = 325,092767 \text{ ms}$

keseluruhan menyatakan bahwa pelayanan wifi dalam kondisi “Baik” atau dengan kata lain “Memuaskan”.