**MODUL & PRAKTIKUM 6**

**JARINGAN KOMPUTER**



*Oleh :*

***NAMA : BILAL RAMADHAN AZZAH MULYADI***

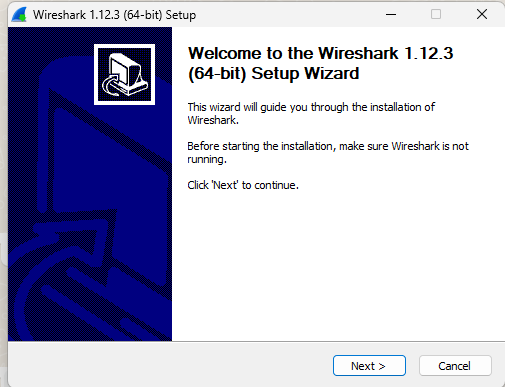
***NIM : 221031074***

***KELAS : SI-C***

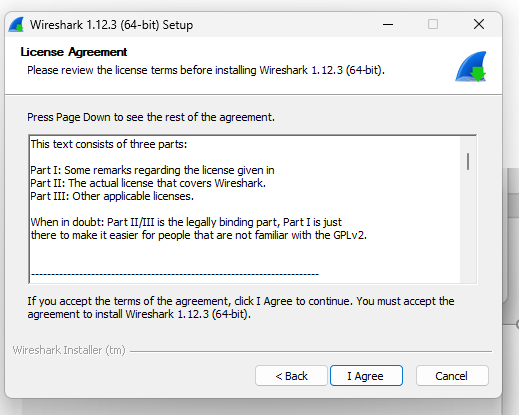
**INSTITUT TEKNOLOGI BACHARUDDIN JUSUF HABIBIE**

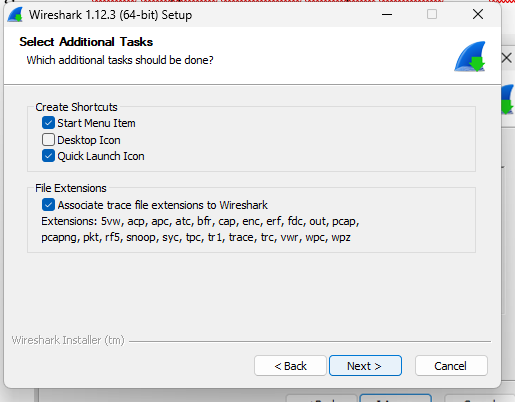
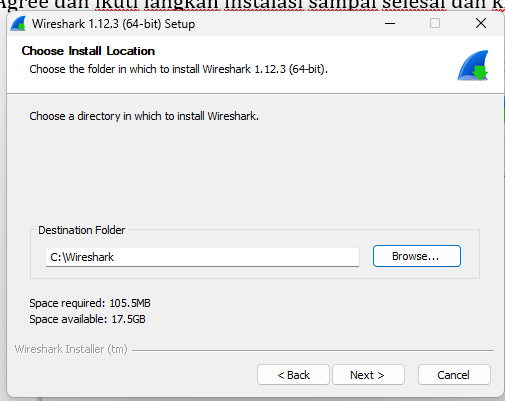
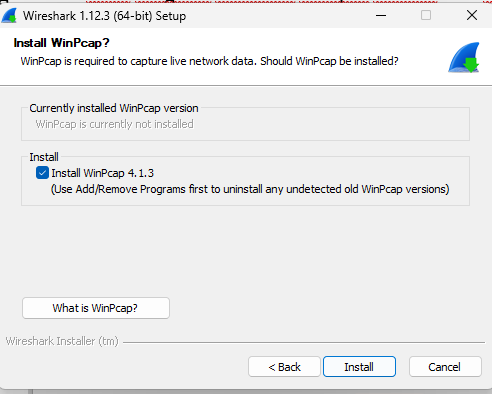
**2023**

1. Lakukan instalasi pada aplikasi dengan klik 2 kali pada aplikasi. Kemudian akan muncul seperti dibawah ini. Klik Next

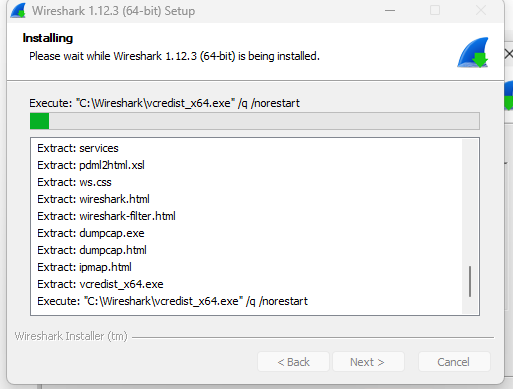


1. Klik I Agree dan ikuti langkah instalasi sampai selesai dan klik next sampai klik install

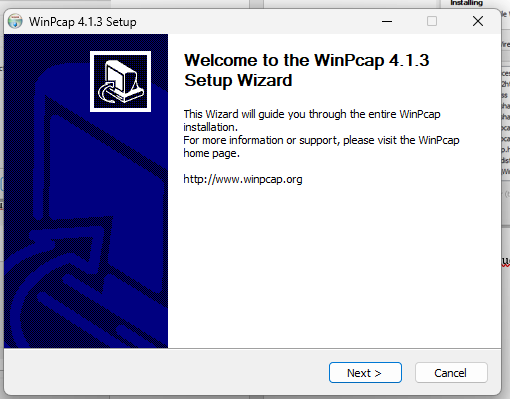




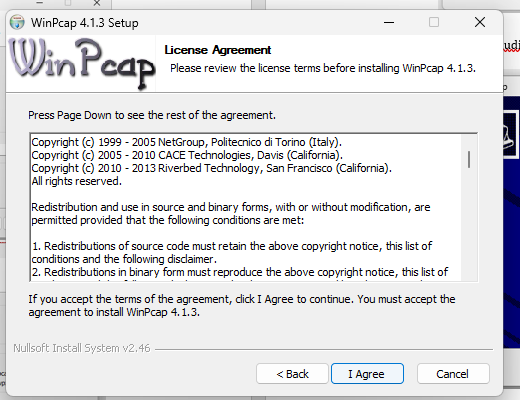
1. Menunggu proses instalasi dan kemudian klik next

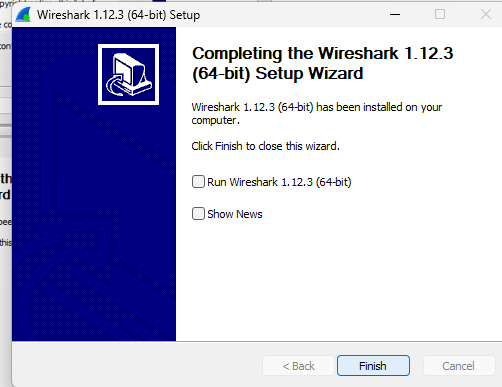


1. Kemudian muncul instalasi winPcap klik next

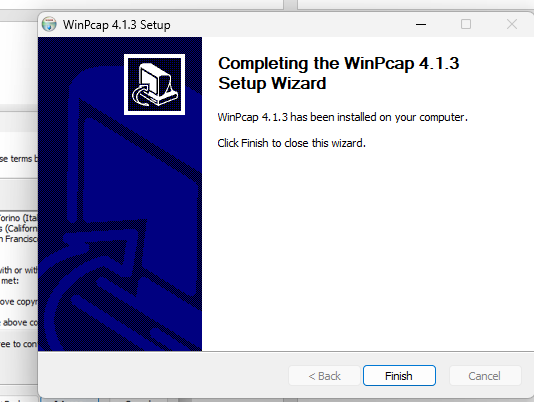


1. Klik I Agree dan klik next

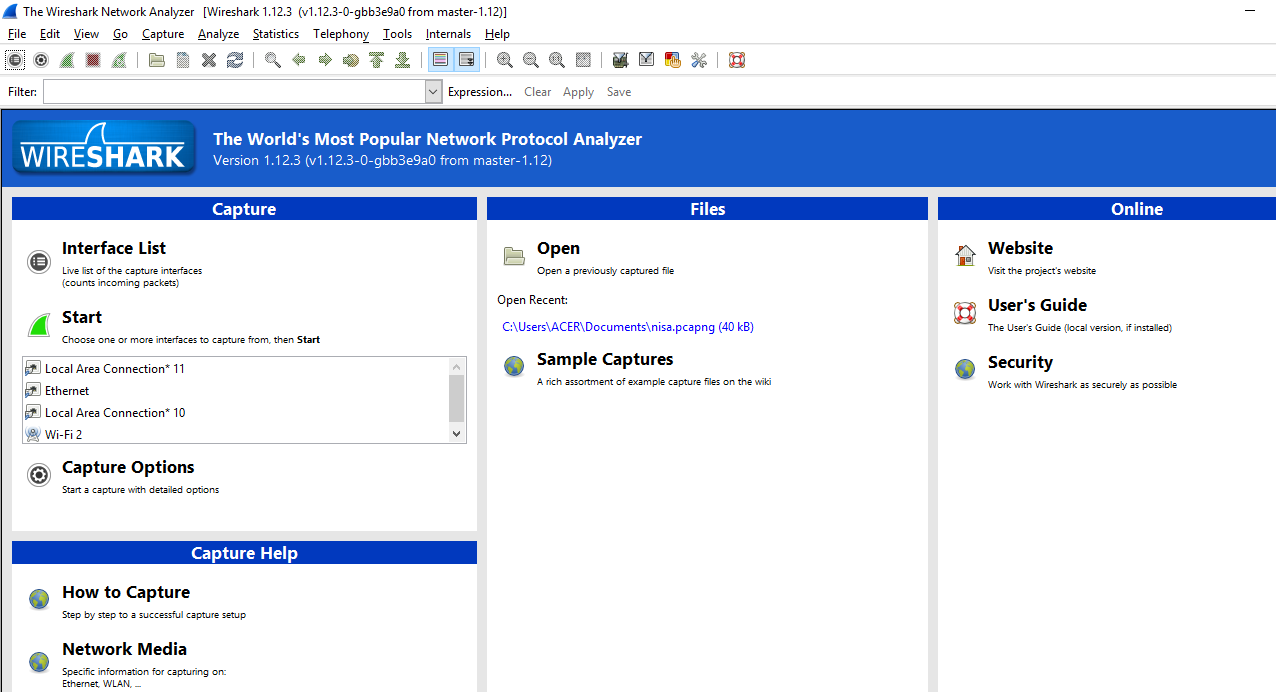




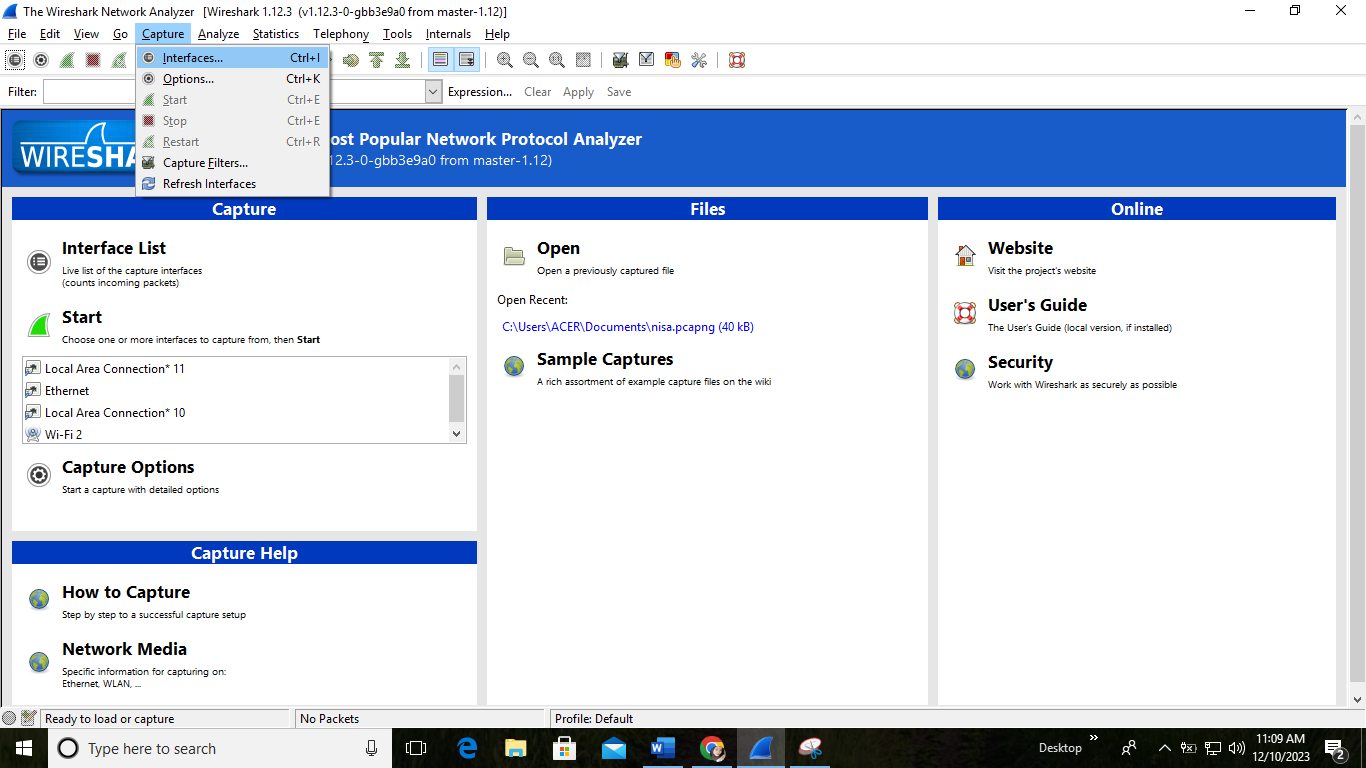
1. Menunggu Proses Instalasi



1. Setelah proses instalasi selesai klik finish, maka akan melanjutkan proses instalsi dariwireshark
2. Analisa Paket Data
3. jalankan aplikasi Wireshark yang sudah terinstall, maka muncul jendela seperti ini



1. Pada jendela Wireshark pilihlah menu Interface List

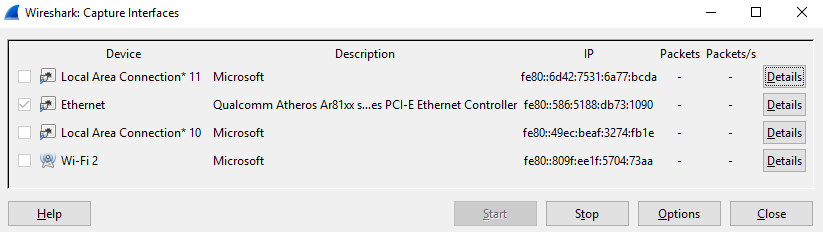


1. Selanjutnya biarkan jendela Wireshark tetap berjalan untuk melakukan capturing

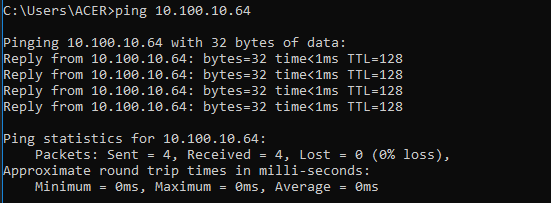
atau perekaman data.

1. Lanjutkan dengan memilih Interface yang ingin di-capture atau direkam, sebagai

contoh pilih Ethernet lalu tekan tombol Start untuk memulai capture paket data.



1. Kemudian untuk mendapatkan informasi dari paket data, lakukan perintah "ping" pada komputer 1 ke tujuan atau komputer 2 dengan cara menggunakan aplikasi Command Prompt



1. Jika pada jendela "cmd" atau Command Prompt muncul tampilan Reply from IP

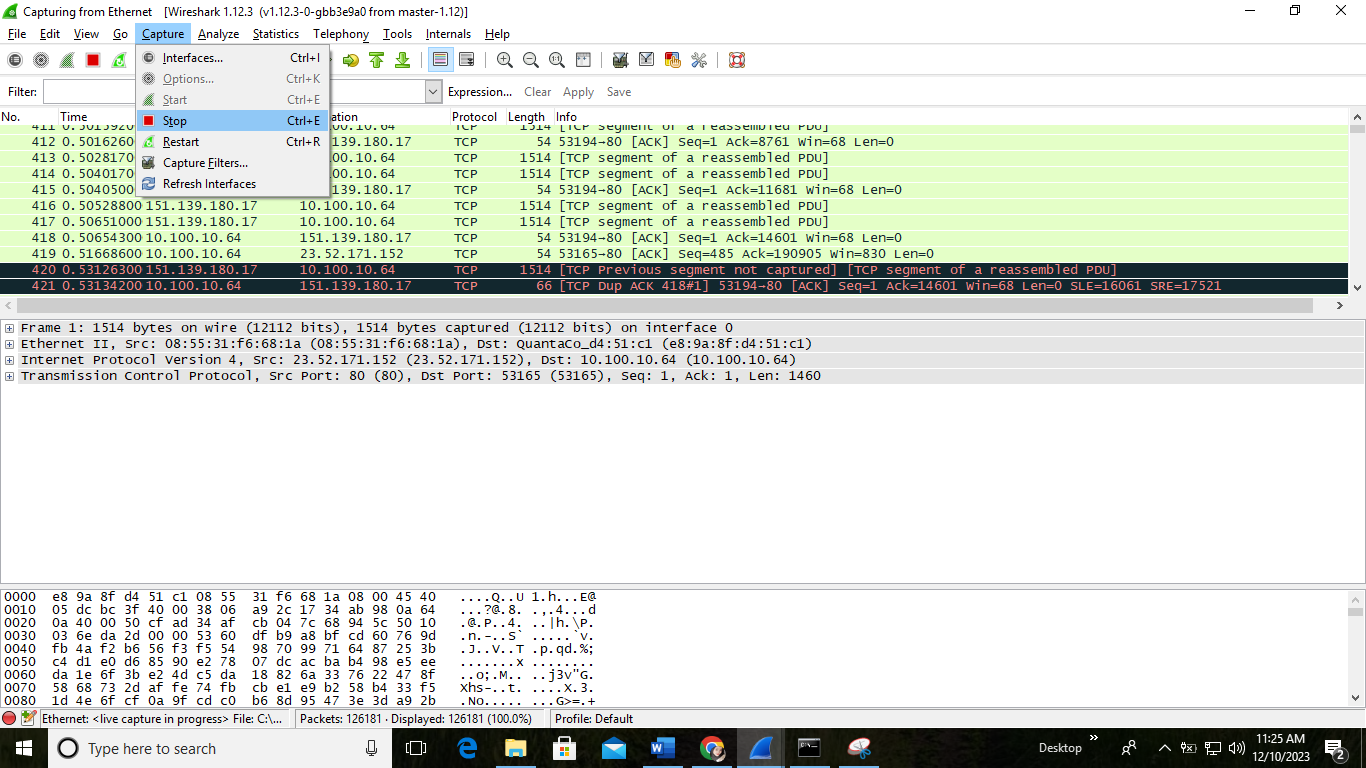
address atau Request Time Out, maka paket data sudah terkirim, jadi informasi

tersebut sudah dapat di analisa.

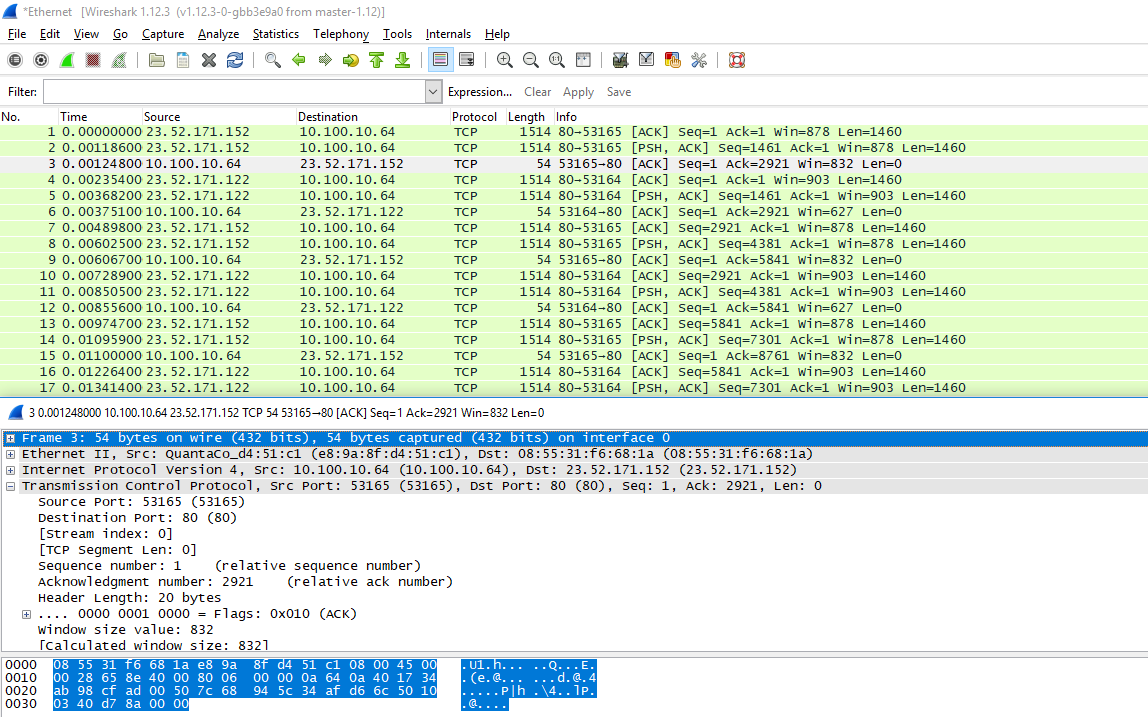
1. Kemudian kembali pada jendela Wireshark tekan tombol Stop pada Tab Capture,

maka muncul informasi-informasi dari paket data hasil dari perintah "ping" yang

dilakukan sebelumnya dari komputer I ke tujuan atau komputer 2.



1. Selanjutnya didapatkan hasil capture yang dilakukan dengan perintah "ping"



**Jumlah Frame** : Terdiri dari 17 Frume

**Time/Waktu** : Masing-masing frame memiliki rentang waktu yang berbeda-beda saat transmisi data

Source/ Sumber : Merupakan komputer sumber atau komputer yang melakukan perintah "ping" terhadap komputer yang dituju atau komputer 2. Sebagai contoh:

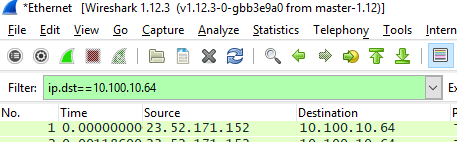
Frame 1 Melakukan broadcast atau menyebarkan informasi MAC Address computer "Wistron" melalui protocol ARP terhadap jaringan, lalu di jawablah

pada frame 2 bahwa MAC Address di terima oleh Komputer 2 "Pegatron", kemudian dibalas informasi tersebut ke komputer 1 pada kolom Destinasion.

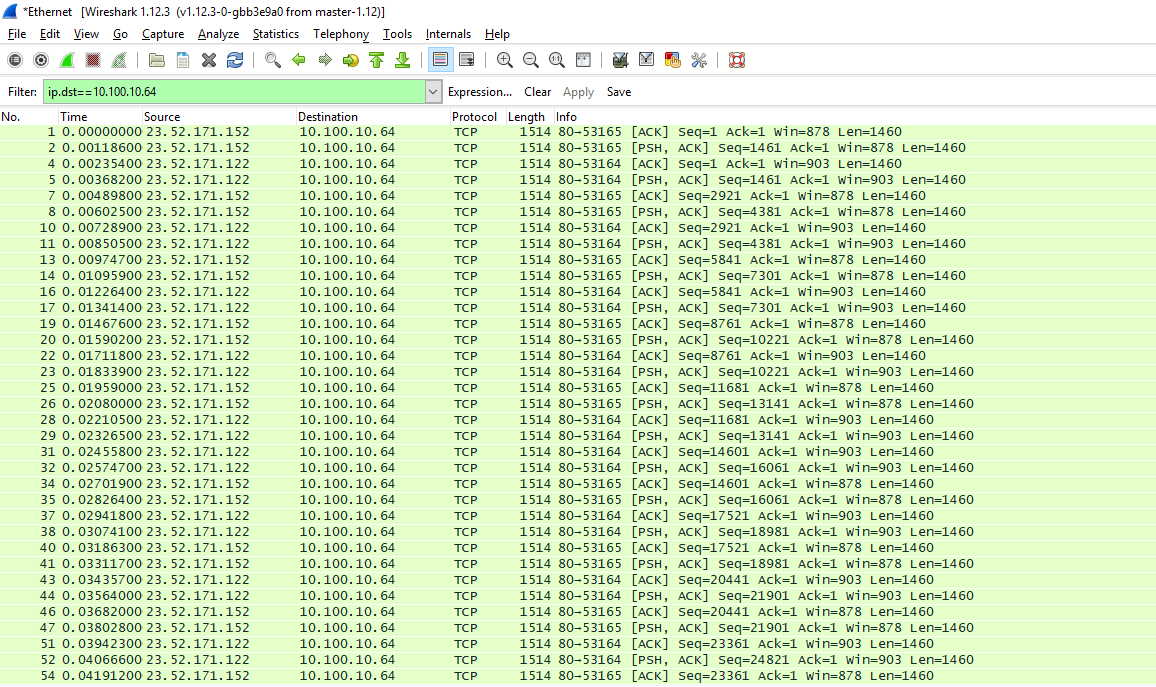
Pada frame 3 komputer 1 melakukan permintaan request dengan perintah "ping" dengan IP 10.100.10.64 melalui protocol ICMP, maka frame 4 dan frame 5 melakukan hal yang sama seperti komputer I pada frame 1 dan frame 2

Pada frame 6 komputer 2 melakukan balasan dengan dengan jawaban reply melalui protocol ICMP. Selanjutnya pada frame 7. komputer 1 melakukan permintaan / request kembali, kemudian di balas oleh komputer 2 pada frume 8. dst.

1. **Analisa Paket Data dengan Perintah Wireshark**
2. ketikan perintah "ip.dst-10.100.10.64 " pada kolom Display Filter yang bertujuan untuk memeriksa informasi yang dikirimkan dari komputer I ke komputer tujuan atau komputer 2.

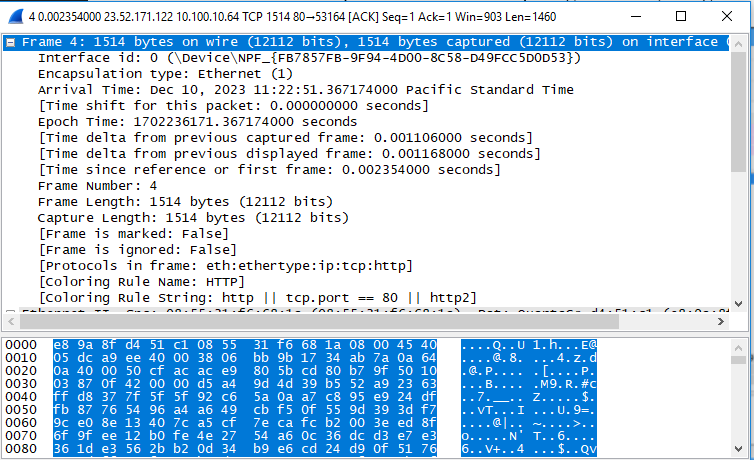


1. Maka didapatkan beberapa frame yang memiliki informasi pada kolom Info dengan keterangan bahwa IP Address 10.100.10.64 melakukan perintah "ping" atau permintaan/request.



1. Kemudian melakukan analisa pada paket data, sebagai contoh pada no.4 atau frame

ke 4 didapatkan informasi data pada gambar

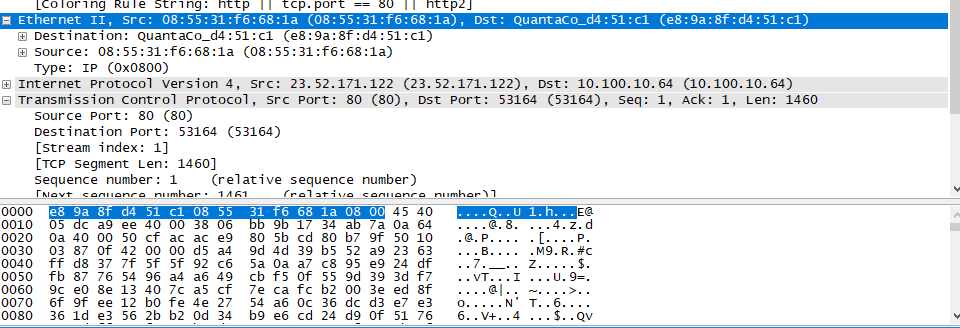


Pada detail paket data frame terdapat informasi sebagai berikut:

* Frame 4: 1514 bytes on wire (12112 bits), 74 bytes captured (12112 bits) on interface 0
* Arrival Time: Dec 10, 2023 11:22:51. 367174000 pacific standard time pada frame ke 4 mempunyai data berukuran 1514 Bytes melalui media kabel atau ethernet.
* Encapsulation type: Ethernet (1) Menunjukan enkapsulasi data melalui ethernet.
* Protocols in frame: eth.ethertype:ip:tcp:http

Kesimpulan frame 4 adalah transmisi data dilakukan pada ethernet, pada waktu 11.22

menggunakan protokol HTTP.



Pada detail paket data Ethernet II terdapat informasi sebagai berikut:

• Ethernet 11. Sre: F6:68:1A (08:55:31: (3e:97:0c:7f7e:fb), Dst: Pegatron b0:03:46

(e0:69:95:b0:e3:46)

• Destination: Pegatron\_b0c3:4b (et:69:95;b0:c3:4b)

• Address: Pegatron b0c3:4b (c0:69-95:60x3:46)

• Source: Wistronl 71:7c:f6 (3c:970e7f7c:f6)

• Address: Wistront 78.7c:f6 (3e:97:0e:717:16)

Menunjukkan sumber "Sre" interface pada ethernet memiliki MAC Address/

alamat fisik "3e:97:06:76-7c:16" atau komputer 1. Sedangkan tujuan "Dst"

memiliki MAC Address alamat fisik "e0:69:95:b0:c3:4b" atau komputer 2.

• Type: IPv4 (0x0800)

Menunjukkan protokol yang dilalui menggunakan IP Address versi 4.

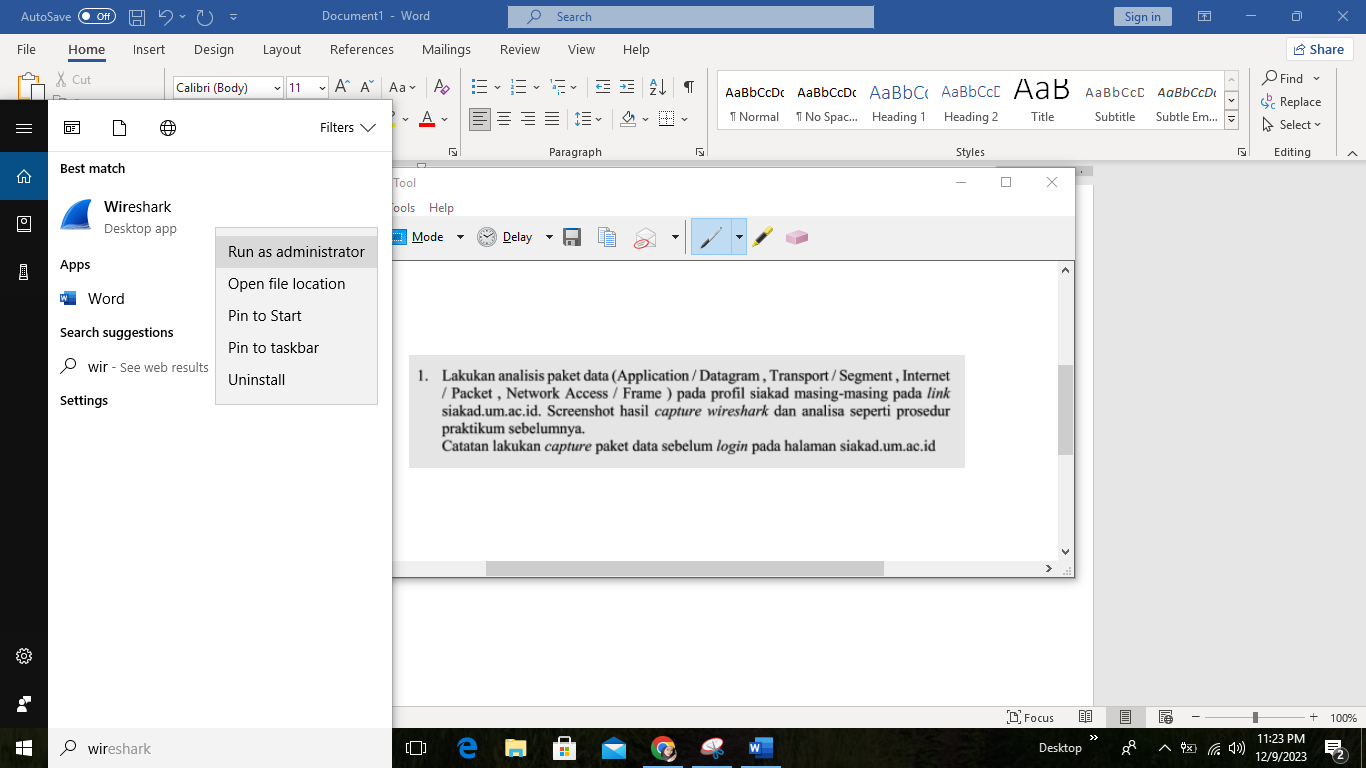
Kesimpulan Ethernet II adalah transmisi data yang dilakukan dikirim dari MAC

Address c0.69.95:60:23:4b atau komputer 1 ke MAC Address 30:97-0e:71;70:6 atau

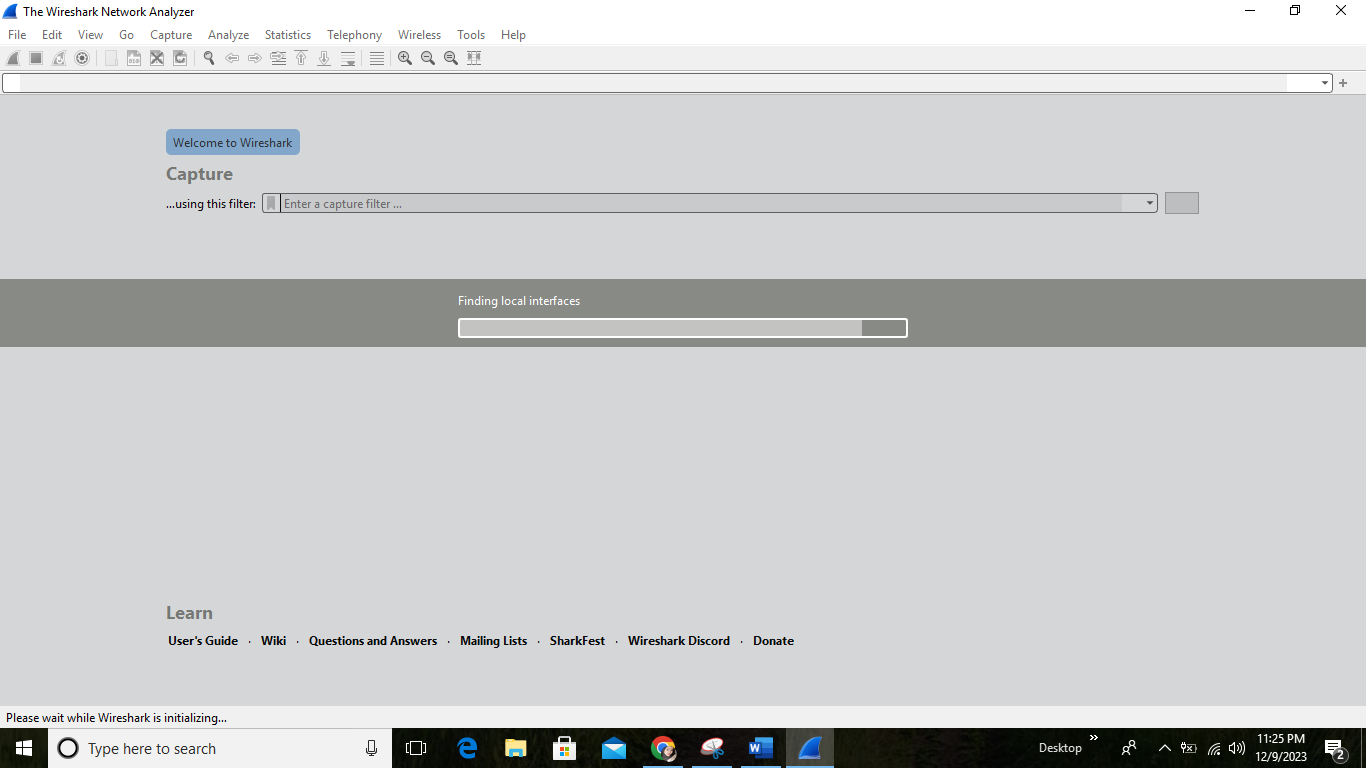
komputer 2 melalui IP Address versi 4.

LATIHAN

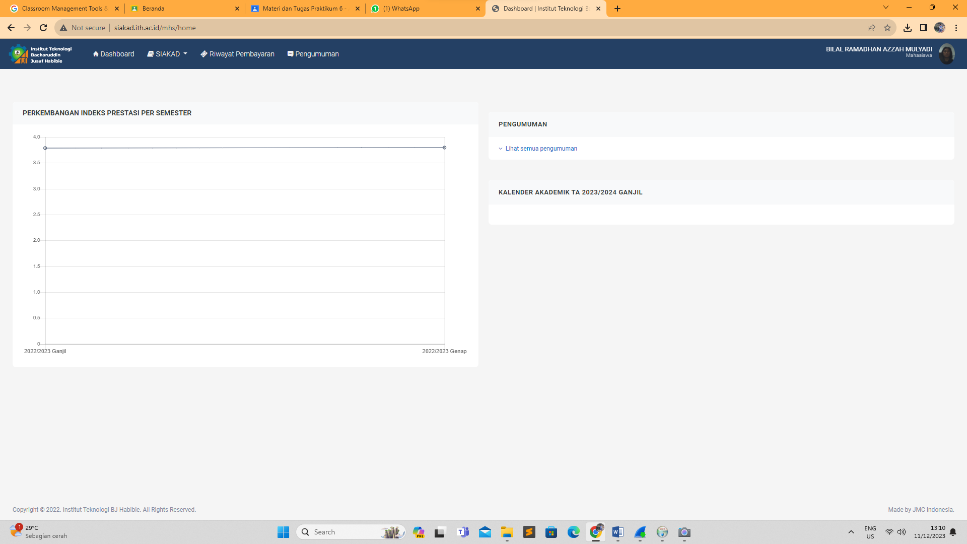
1. Buka/ jalankan aplikasi wireshark >> klik kanan>> run as administrator



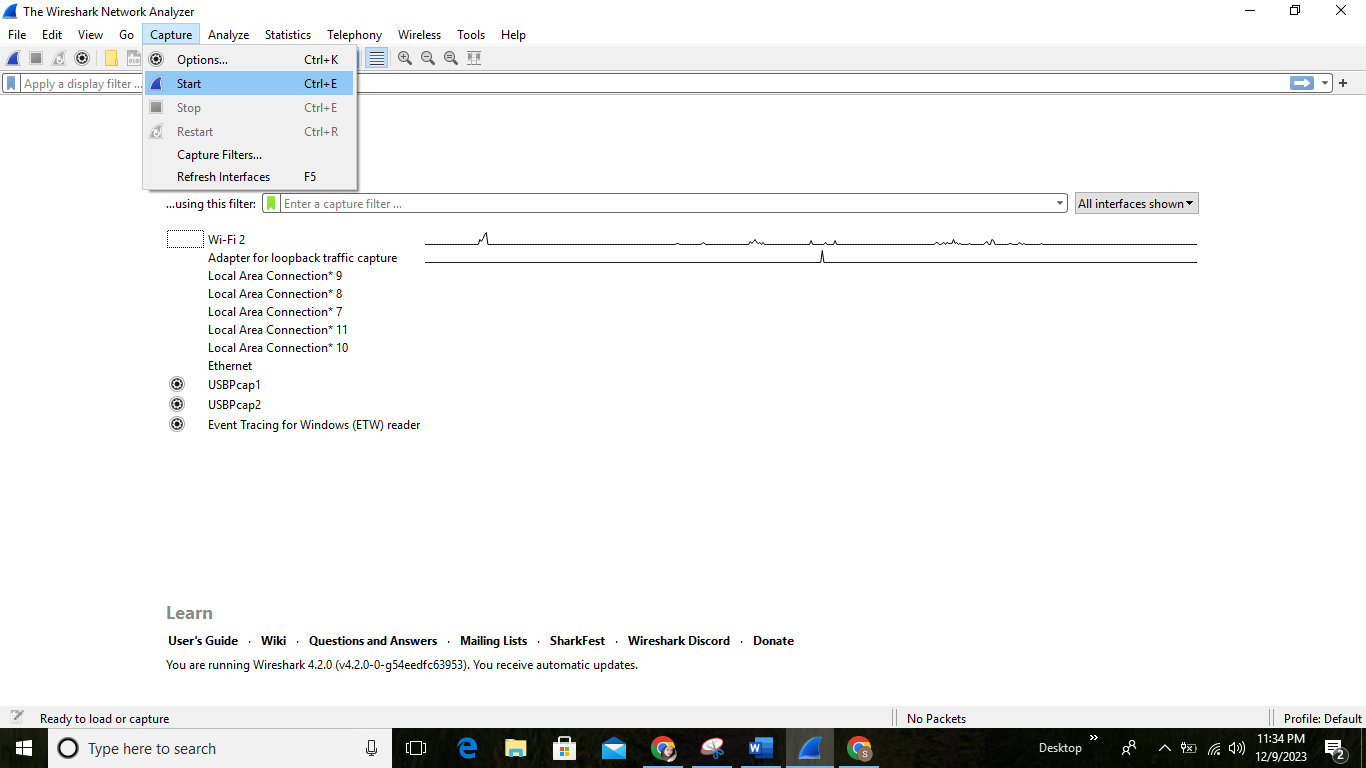
1. Proses Wireshark dibuka



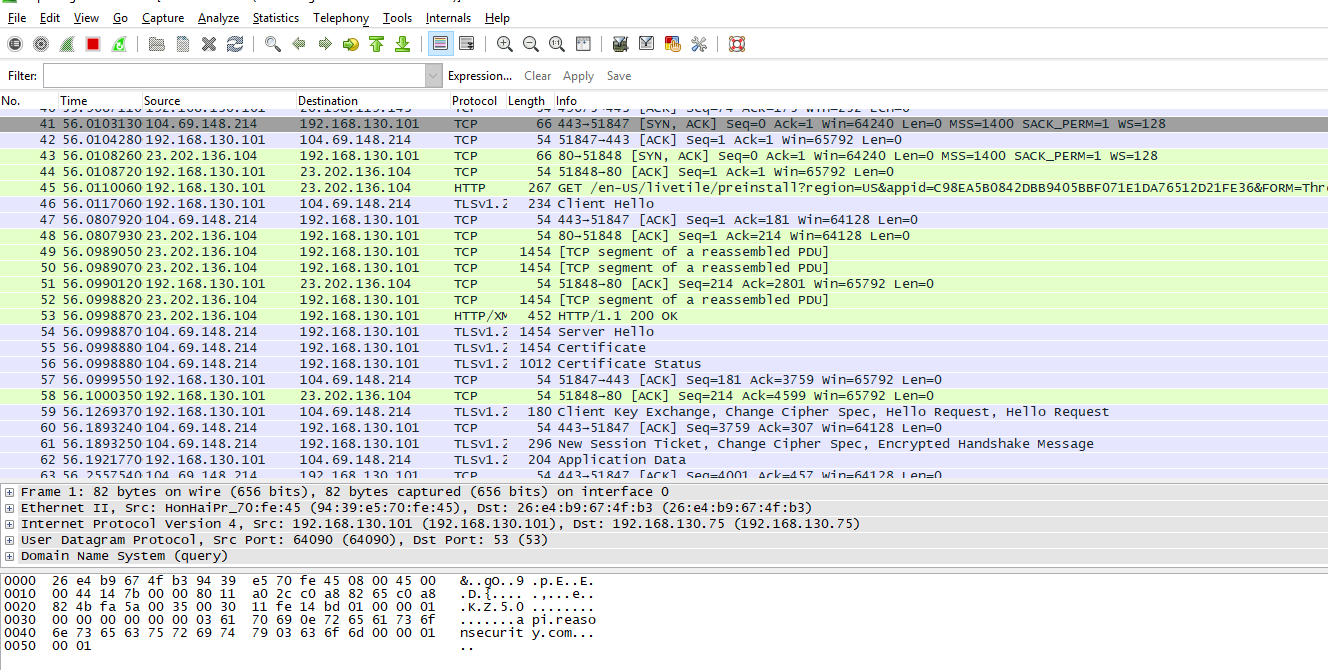
1. Sebelum melakukan analisa, pada web browser buka halaman siakad.ith.ac.id



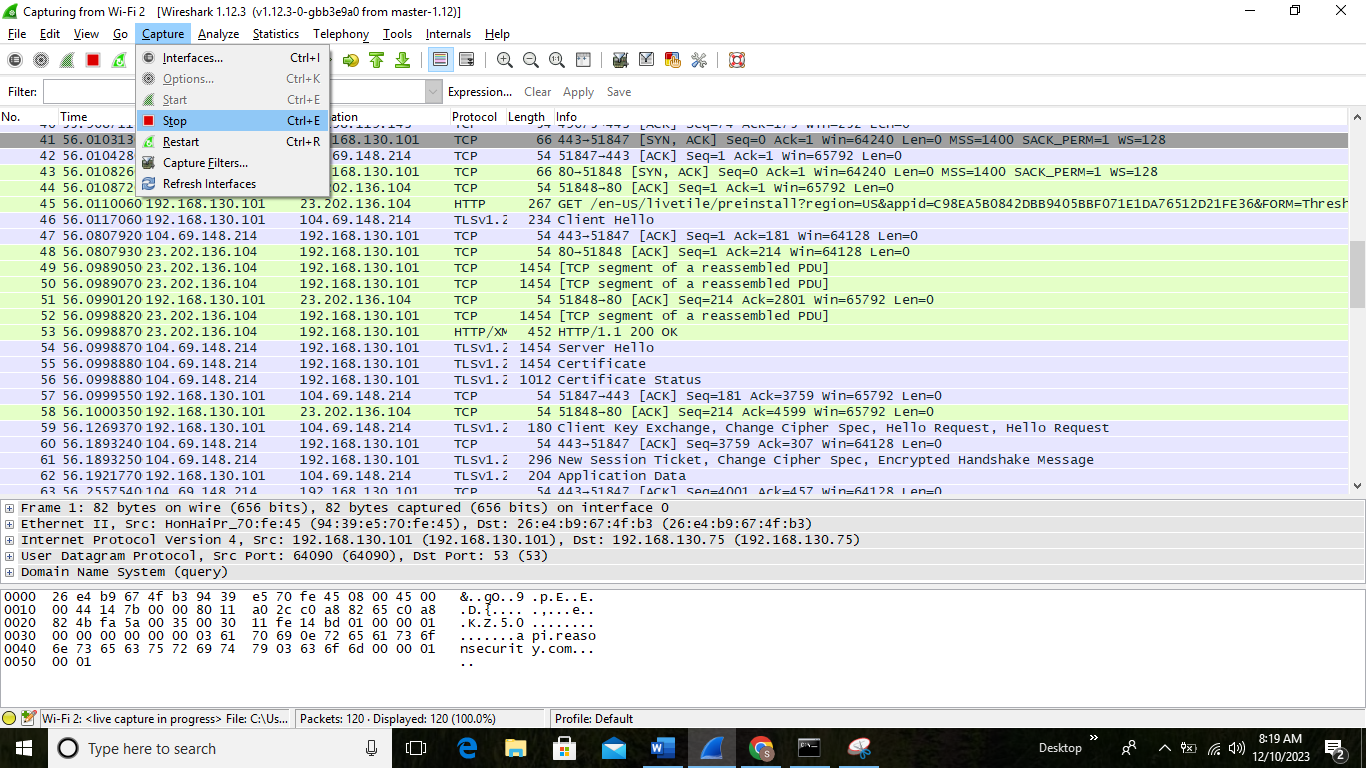
1. Selanjutnya untuk memulai menganilisa , pilih menu capture>>Start



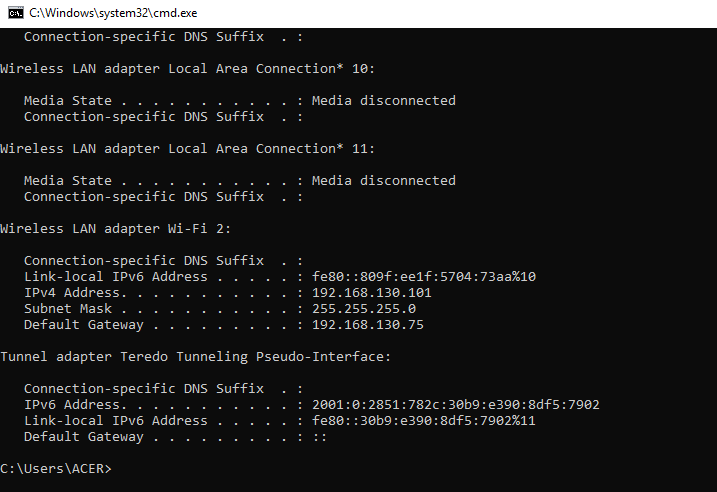
1. Kemudian akan muncul paket-paket data yang keluar masuk pada jaringan



6

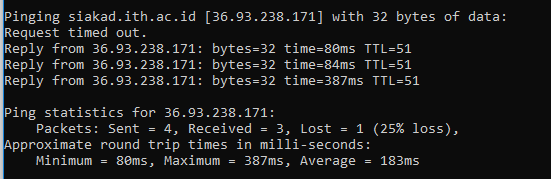


7



8. Dari rincian di atas dapat dilihat bahwa IP PC yang digunakan adalah 192.168.130.101

9. selanjutnya mengecek ip dari siakad.ith.ac.id pada command prompt lakukan ping terhadap alamat web maka hasilnya



10. Setelah dilakukan pengecekan maka diketahui bahwa ip address dari siakad.ith.ac.id adalah 36.93.238.171

11. Kemudian lakukan Analisa terhadap web

