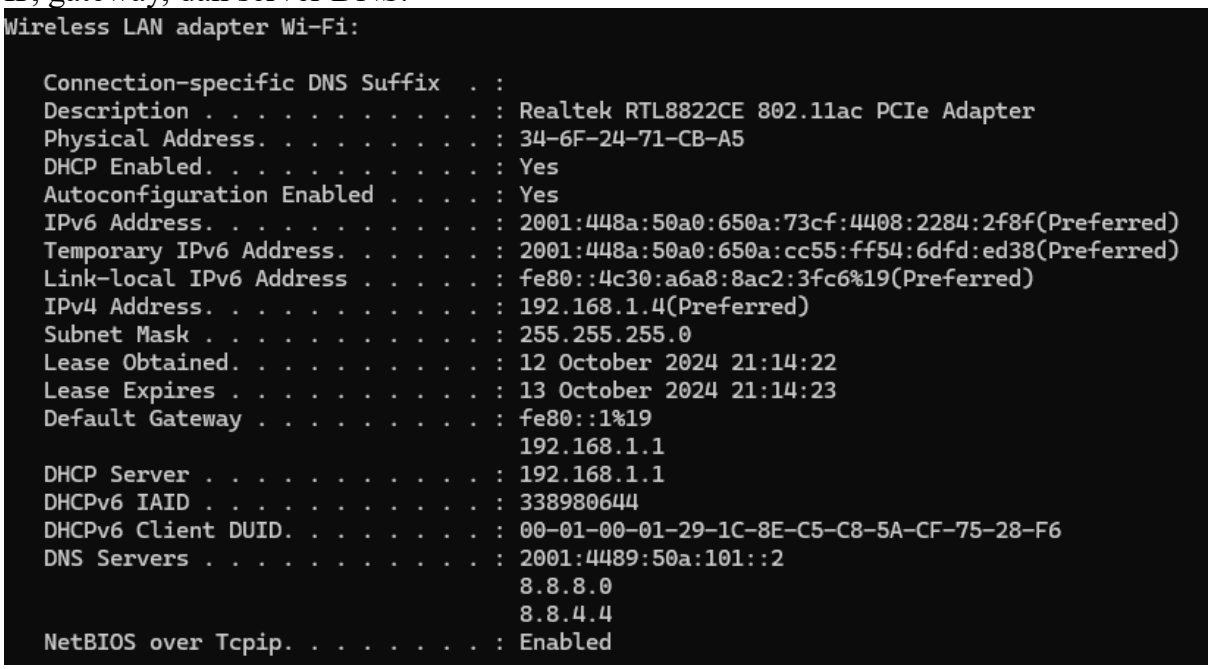
Laporan Tugas Komunikasi Data

Nama: Dino Alfian Zamri
Nim: 202310370311329
Mata Kuliah: Komunikasi Data

Tugas yang dilakukan yaitu mengerjakan Praktikum Komunikasi Data.
Bagian 1: Memeriksa konfigurasi jaringan pada PC

Menggunakan Command Prompt untuk menjalankan perintah ipconfig /all, yang akan menampilkan informasi penting tentang koneksi jaringan, termasuk alamat IP, gateway, dan server DNS.

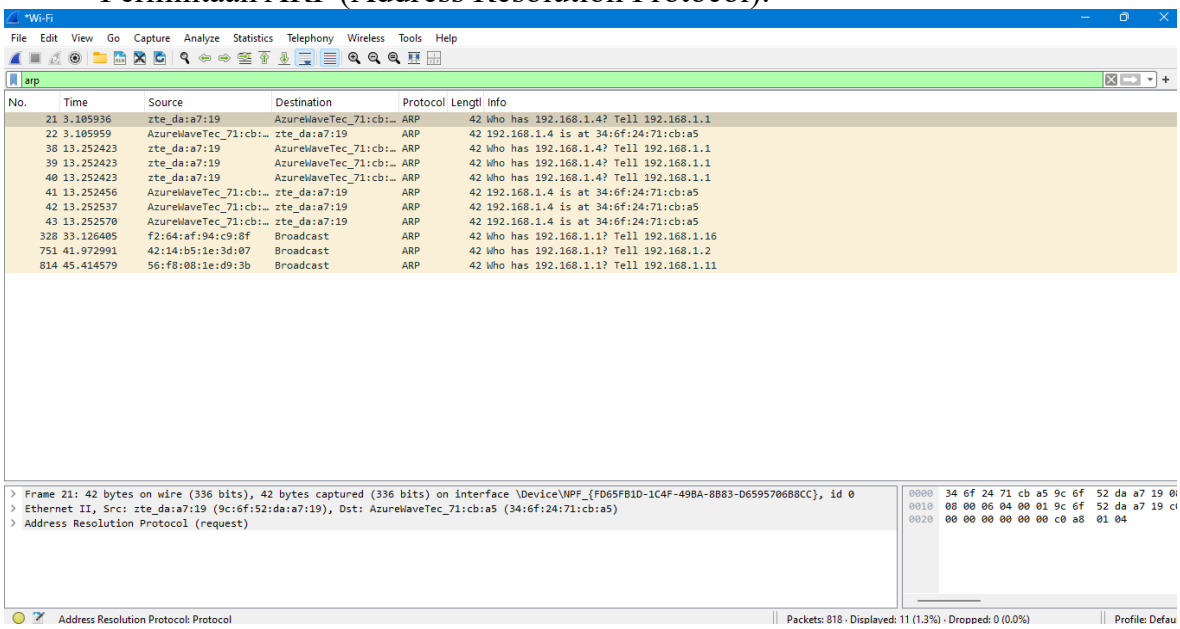


Alamat IP host PC saat ini adalah 192.168.1.4 yaitu alamat unik yang digunakan untuk mengidentifikasi perangkat di jaringan, sedangkan Default gateway yang digunakan adalah 192.168.1.1 yang berfungsi sebagai gerbang penghubung untuk perangkat ke jaringan lain.

Bagian 2: Memeriksa frame Ethernet dalam sebuah Wireshark.

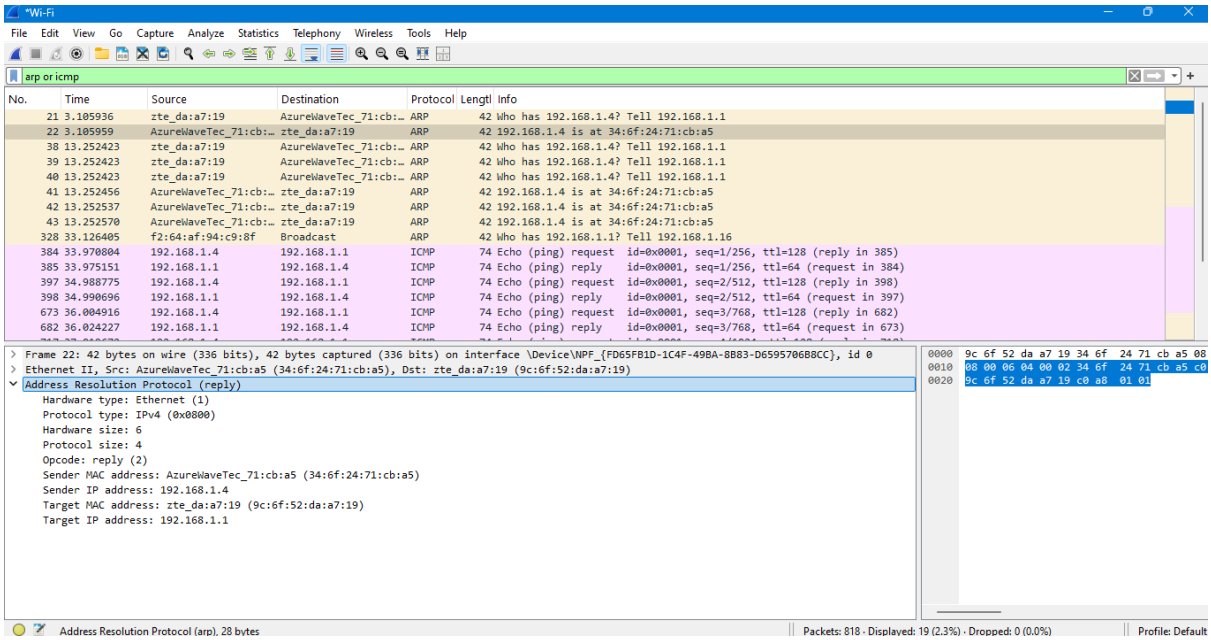
Menggunakan Wireshark untuk Memeriksa Paket: Membuka Wireshark, mulai penangkapan lalu lintas jaringan, lakukan ping dari host PC ke default gateway (misalnya ke alamat IP 192.168.1.1), dan hentikan penangkapan setelah ping selesai untuk menganalisis paket dalam Wireshark.

Permintaan ARP (Address Resolution Protocol):



Wireshark akan menampilkan permintaan ARP yang dibuat oleh host PC untuk mencari tahu alamat MAC dari default gateway dengan pertanyaan "Siapa yang memiliki alamat IP 192.168.18.1? Beritahu saya alamat MAC Anda."

Balasan ARP:



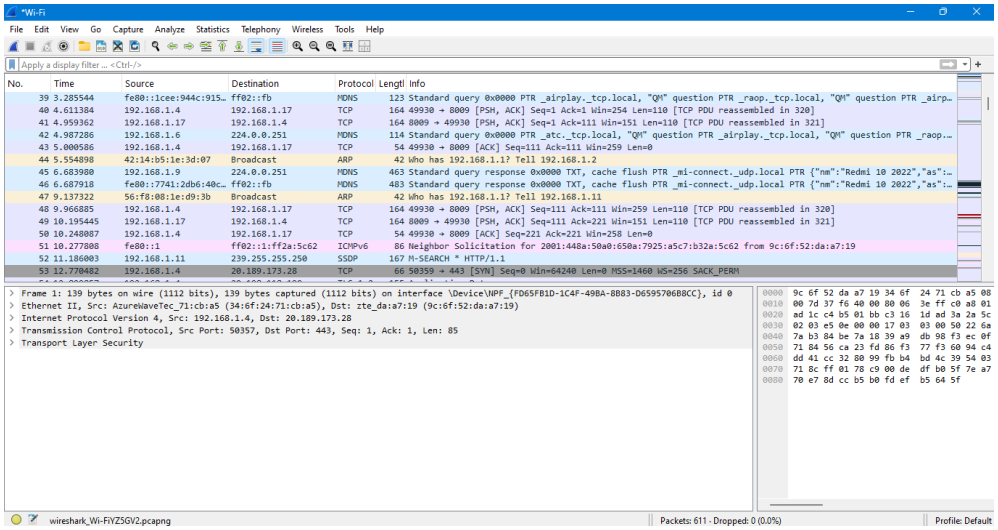
Sebagai respons, default gateway akan mengirim balasan ARP yang menyatakan alamat MAC-nya dengan informasi "Saya memiliki alamat IP 192.168.1.1, dan alamat MAC saya adalah zte_da:a7:19 (9c:6f:52:da:a7:19)"

Bagian 3: MenggunakanWiresharkuntukMengambildanMenganalisisFrameEthernet

1. Menentukan Alamat IP dari gateway default pada PC.
    a. Pastikan menggunakan model Realtime.
    b. Buka Command Prompt pada tab Desktop.
    c. Masukkan perintah ipconfig.

```
  Connection-specific DNS Suffix  . :

nknown adapter Local Area Connection:

  Media State . . . . . . . . . . . : Media disconnected
  Connection-specific DNS Suffix  . :

ireless LAN adapter Local Area Connection* 1:

  Media State . . . . . . . . . . . : Media disconnected
  Connection-specific DNS Suffix  . :

ireless LAN adapter Local Area Connection* 2:

  Media State . . . . . . . . . . . : Media disconnected
  Connection-specific DNS Suffix  . :

ireless LAN adapter Wi-Fi:

  Connection-specific DNS Suffix  . :
  IPv6 Address. . . . . . . . . . . : 2001:448a:50a0:650a:73cf:4408:2284:2f8f
  Temporary IPv6 Address. . . . . . : 2001:448a:50a0:650a:cc55:ff54:6dfd:ed38
  Link-local IPv6 Address . . . . . : fe80::4c30:a6a8:8ac2:3fc6%19
  IPv4 Address. . . . . . . . . . . : 192.168.1.4
  Subnet Mask . . . . . . . . . . . : 255.255.255.0
  Default Gateway . . . . . . . . . : fe80::1%19
                                      192.168.1.1
```

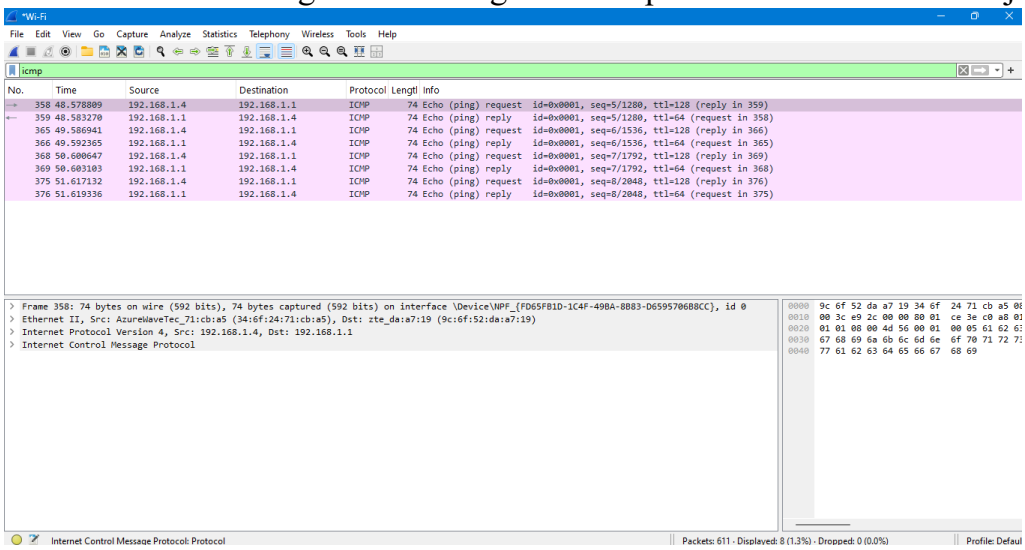
2. Melakukan pengambilan data lalu lintas di NIC PC.
    a. Buka Wireshark untuk melakukan pengambilan data.
    b. Klik "Start Capture" untuk memulai pengambilan data.
    c. Amati lalu lintas yang muncul pada daftar paket.



3. Melakukan ping ke gateway default PC pada Command Prompt.

```
C:\Users\HP>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=4ms TTL=64
Reply from 192.168.1.1: bytes=32 time=5ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 5ms, Average = 3ms

C:\Users\HP>
```

4. Melakukan pemberhentian pengambilan data lalu lintas di NIC.
5. Melakukan filtering Wireshark agar menampilkan lalu lintas ICMP saja.



6. Memeriksa permintaan Echo (ping) pertama di Wireshark

```
> Frame 358: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{FD65FB1D-1C4F-49BA-8B83-D6595706B8CC}, id 0
v Ethernet II, Src: AzureWaveTec_71:cb:a5 (34:6f:24:71:cb:a5), Dst: zte_da:a7:19 (9c:6f:52:da:a7:19)
    > Destination: zte_da:a7:19 (9c:6f:52:da:a7:19)
    > Source: AzureWaveTec_71:cb:a5 (34:6f:24:71:cb:a5)
      Type: IPv4 (0x0800)
      [Stream index: 0]
> Internet Protocol Version 4, Src: 192.168.1.4, Dst: 192.168.1.1
v Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0x4d56 [correct]
      [Checksum Status: Good]
      Identifier (BE): 1 (0x0001)
      Identifier (LE): 256 (0x0100)
      Sequence Number (BE): 5 (0x0005)
      Sequence Number (LE): 1280 (0x0500)
      [Response frame: 359]
    > Data (32 bytes)
```

7. Pengambilan paket untuk host jarak jauh.

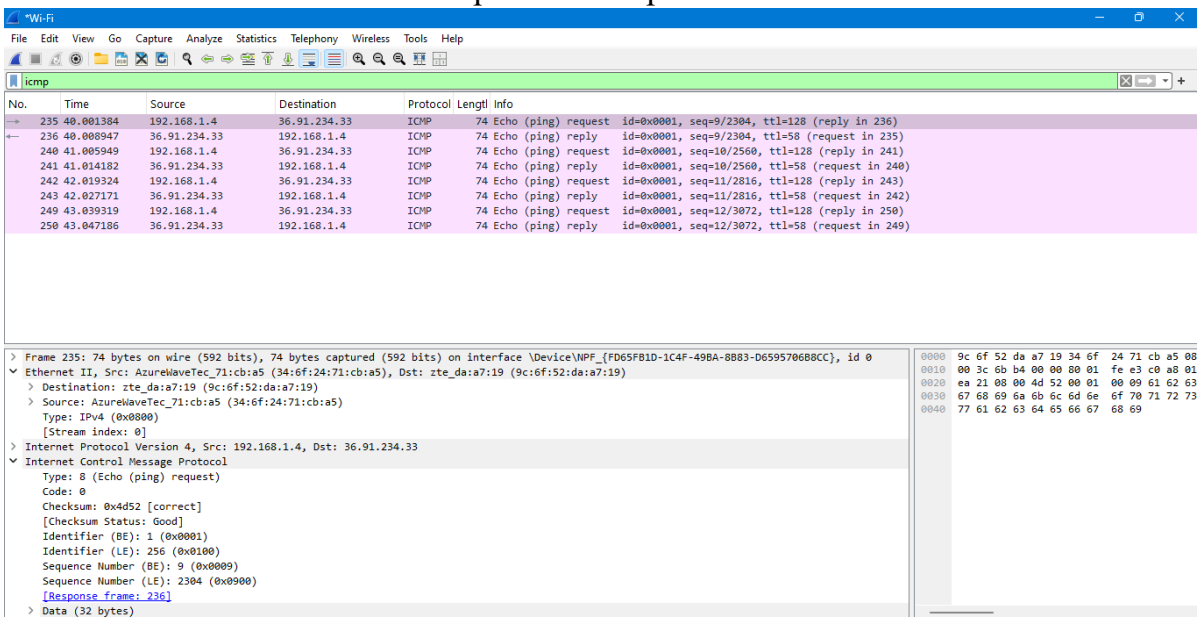
a. Melakukan “Start Capture” untuk memulai pengambilan Wireshark baru.

b. Pada Command Prompt, ping www.tokopedia.com.

```
C:\Users\HP>ping www.tokopedia.com

Pinging a1136.w7.akamai.net [36.91.234.33] with 32 bytes of data:
Reply from 36.91.234.33: bytes=32 time=7ms TTL=58
Reply from 36.91.234.33: bytes=32 time=8ms TTL=58
Reply from 36.91.234.33: bytes=32 time=8ms TTL=58
Reply from 36.91.234.33: bytes=32 time=8ms TTL=58

Ping statistics for 36.91.234.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 8ms, Average = 7ms

C:\Users\HP>
```

c. Menghentikan pengambilan paket.

d. Memeriksa data baru di panel daftar paket Wireshark.



PERTANYAANTUGAS

a. Apa tipe protokol yang digunakan dalam frame Ethernet saat melakukan ping dari host PC ke default gateway? Jelaskan bagaimana Anda menemukannya menggunakan Wireshark.

   Jawaban: Menggunakan Wireshark, melakukan ping dari host PC ke default gateway dan menghentikan penangkapan setelah ping selesai untuk menganalisis paket dalam Wireshark.

b. Deskripsikan informasi yang dapat ditemukan dalam frame pertama yang ditangkap oleh Wireshark ketika Anda melakukan ping ke default gateway.

   Jawaban: Mengandung alamat MAC sumber, alamat MAC tujuan, tipe frame, dan data ICMP.

c. Bandingkan alamat MAC dari frame permintaan ICMP pertama dengan alamat MAC yang diterima di frame balasan ICMP. Jelaskan perubahan yang terjadi.

   Jawaban: Pada frame permintaan ICMP pertama, alamat MAC sumber adalah MAC PC dan alamat MAC tujuan adalah MAC gateway. Di frame balasan ICMP, alamat MAC sumber menjadi MAC gateway dan alamat MAC tujuan menjadi MAC PC. Perubahan ini terjadi karena gateway membalas ping, sehingga MAC-nya menjadi sumber.

d. Bagaimana proses resolusi alamat bekerja ketika sebuah perangkat di jaringan ingin berkomunikasi dengan perangkat lain yang alamat IP-nya diketahui namun alamat MAC-nya tidak diketahui?

   Jawaban: Ketika perangkat ingin berkomunikasi, ia menggunakan ARP untuk menemukan alamat MAC berdasarkan alamat IP yang diketahui.

e. Apa alamat IP dari PC yang Anda gunakan dalam pengujian ini? Jelaskan langkah-langkah untuk menemukannya menggunakan Command Prompt.

   Jawaban: 191.168.1.4, Dengan cara melakukan ipconfig/all di CMD

f. Mengapa frame Ethernet yang dikirim dari PC Anda saat melakukan ping menggunakan alamat MAC broadcast? Jelaskan proses dan tujuannya.

   Jawaban: Frame Ethernet menggunakan alamat MAC broadcast untuk menemukan MAC address tujuan yang belum diketahui. Ini dilakukan melalui permintaan ARP, agar perangkat dengan IP yang cocok dapat merespons.