**TECHNICAL REPORT**

**PRAKTIKUM JARINGAN KOMPUTER**

**MODUL 4**



**Disusun Oleh :**

|  |
| --- |
| TGL. PRAKTIKUM : 8 April 2021  NAMA : Achmad Farid Alfa Waid  NIM : 190411100073  KELOMPOK : 1  DOSEN : Yoga Dwitya Pramudita, S.Kom  ASPRAK : Rizal Abdul Fata |



**LABORATORIUM COMMON COMPUTING**

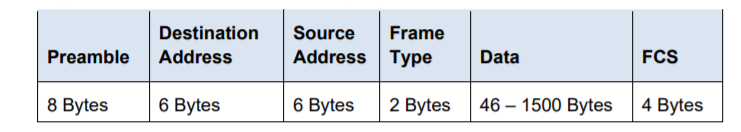
**JURUSAN TEKNIK INFORMATIKA**

**FAKULTAS TEKNIK**

**UNIVERSITAS TRUNOJOYO MADURA**

**2020**

1. **Latihan 1**
2. **Langkah 1: Review Deskripsi dan Panjang Header Ethernet II**



**Preamble:**

8 bit ini mengandung bit-bit sinkronisasi, diproses oleh hardware NIC.

**Destination Address:**

6 byte adalah Destination Mac Address dari tujuan data. Disinilah Mac Address digunakan kompter untuk berkomunikasi. jadi, sebelum sampai ke target yang dituju, sebaiknya adalah untuk mengetahui Mac Addresnya terlebih dahulu, agar mempermudah ketika berkomunikasi menggunakan ethernet. Mac Address tujuan data juga dapat di isi dengan (ff:ff:ff:ff:ff:ff). ini berfungsi untuk membroadcast data. jadi seluruh pc akan membaca dari pesan dengan mac address tujuan seperti tersebut.

**Source Address:**

6 byte adalah Mac Address dari pengirim. perangkat jaringannya pasti telah terdapat Mac Addressnya. Contoh value: Netgear\_99:c5:72 (30:46:9a:99:c5:72). 6 angka heksa pertama menunjukkan kode network interface card (NIC), 6 angka heksa terakhir merupakan nomor seri dari NIC tersebut.

**Frame Type:**

2 byte digunakan untuk type komunikasi. 2 byte ini maka di isi dengan 08 06 kalau untuk valuenya sendiri maka akan terlihat seperti ini (0x0806). Untuk frame Ethernet II, field ini mengandung suatu nilai hexadecimal yang digunakan untuk menunjukkan jenis protokol upperlayer dalam data field.

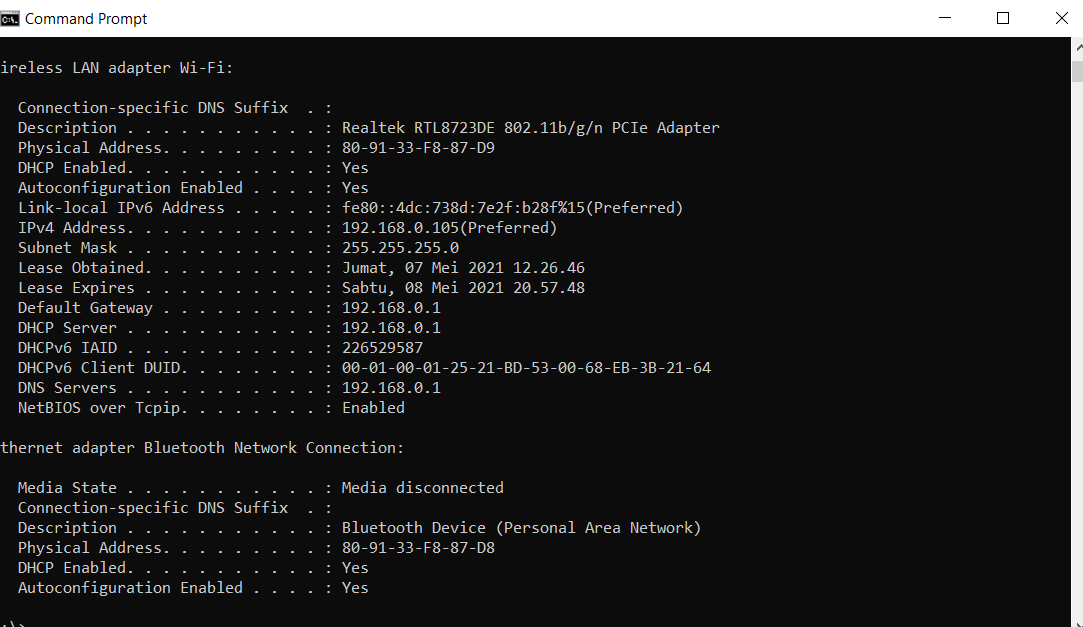
**Data:**

Data 46 – 1500 byte ini merupakan protokol upper-level yang terenkapsulasi dan memiliki panjang tampungan dari interval 46 byte hingga 1500 byte.

**FCS(Frame Check Sequence):**

Dilihat dari banyaknya byte(4 byte) kemungkinan frame ini merupakan CRC32.

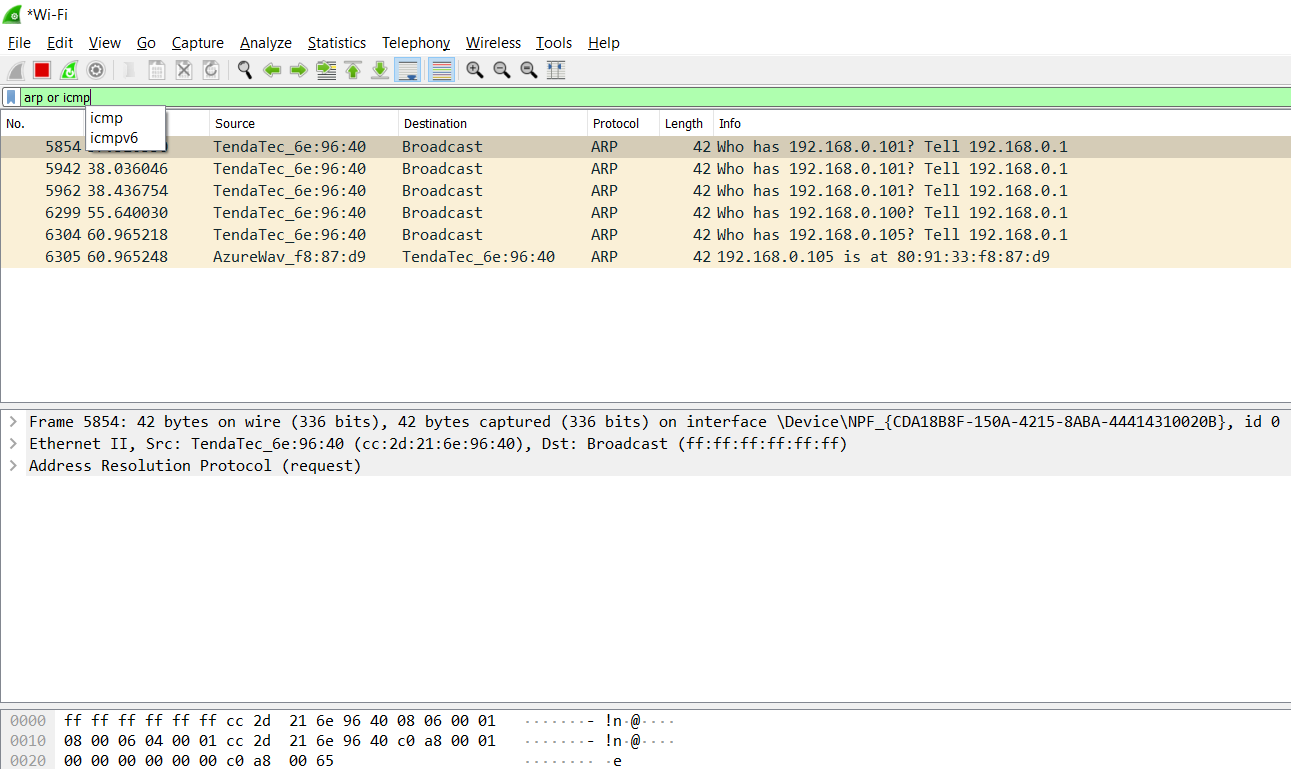
1. **Langkah 2: Memeriksa konfigurasi jaringan dari PC**



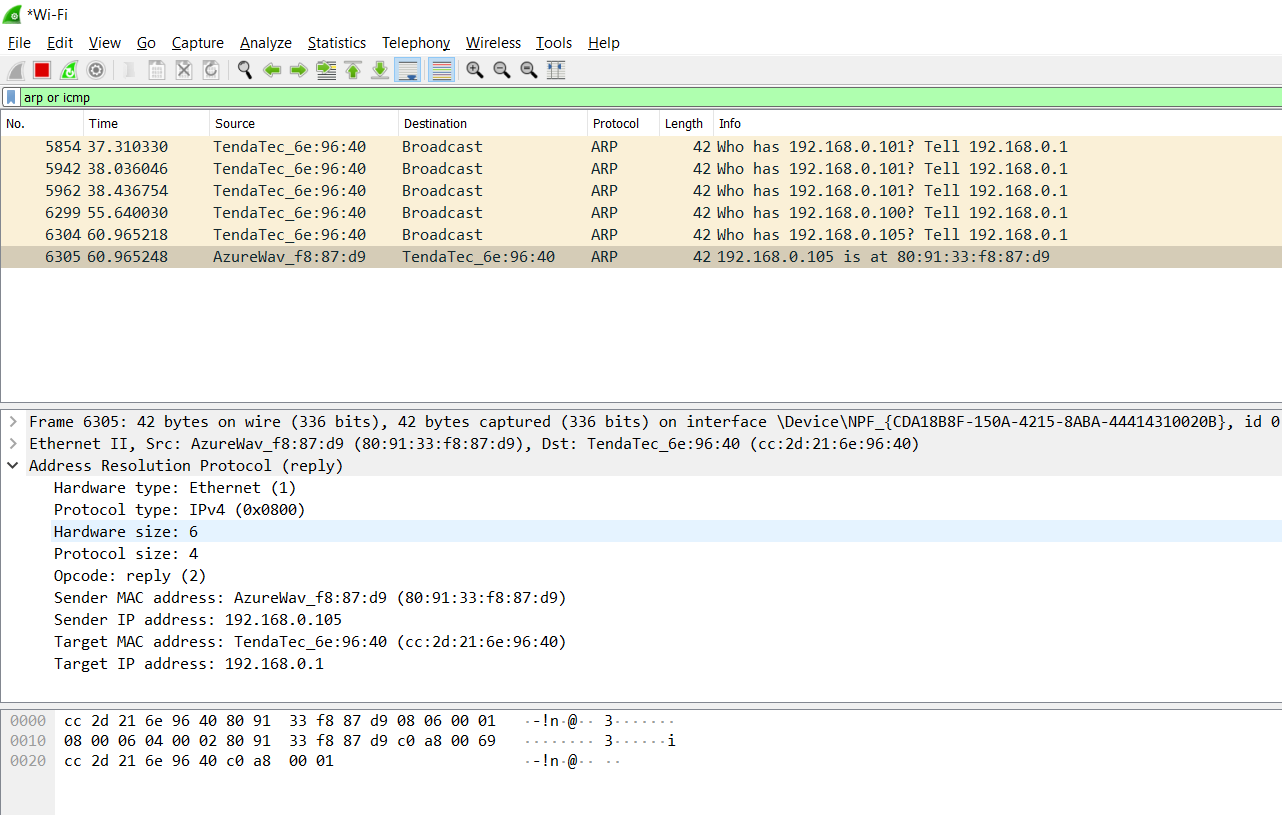
Pada PC saya memiliki **IP Addres 192.168.0.105** dan **default gateaway 192.168.0.1**

1. **Langkag 3: Memeriksa frame Ethernet dalam tangkapan Wireshark**

Dikarenakan saya menggunakan jaringan wifi maka untuk capture jaringanya saya memilih wifi. berikut merupakan rincian frame untuk suatu request ARP or ICMP.



berikut merupakan rincian frame untuk balsan ARP (ARP reply)



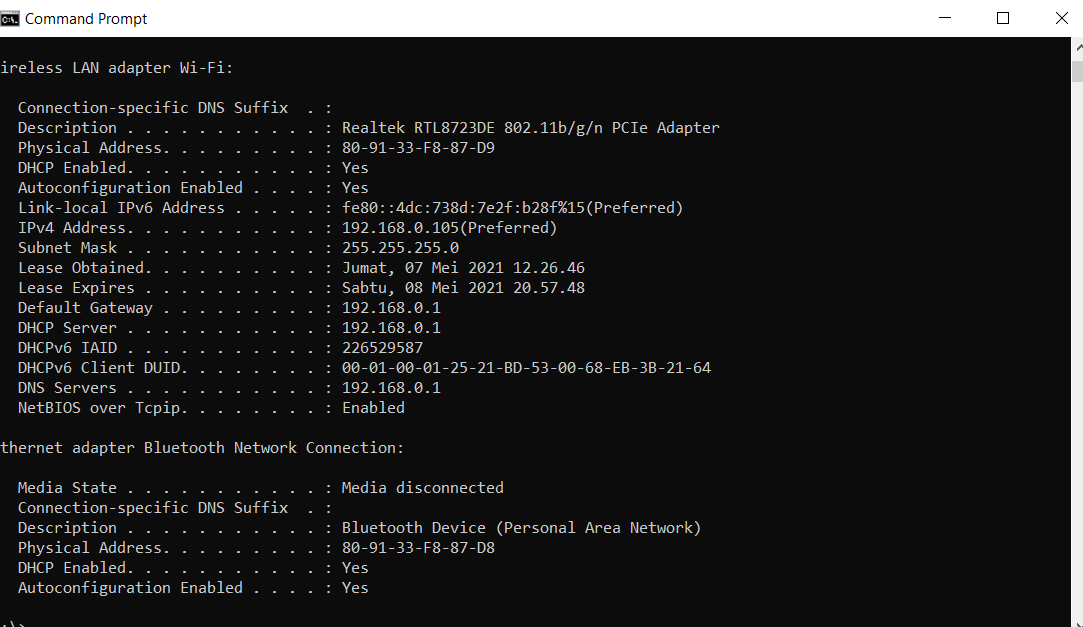
1. **Langkah 4: Memeriksa isi header Ethernet II dari Request ARP**

|  |  |  |
| --- | --- | --- |
| **Field** | **Value** | **Description** |
| Preamble | Tidak terlihat dalam tangkapan | Field ini mengandung bit-bit sinkronisasi, diproses oleh hardware NIC |
| Destination Address  Source Address | Broadcast (ff:ff:ff:ff:ff:ff)  AzureWav\_f8:87:d9 (80:91:33:f8:87:d9) | Alamat Layer 2 untuk frame tersebut. Setiap address panjangnya 48 bit atau 6 octet, diekspresikan sebagai 12 digit hexadecimal, 0- 9,A-F. Format umumnya 12:34:56:78:9A:BC.  6 angka heksa pertama menunjukkan kode pabrik network interface card (NIC), 6 angka heksa terakhir merupakan nomor seri dari NIC tersebut. Destination Address dapat berupa alamat broadcast yang berisi semua alamat atau unicast. Source address selalu unicast. |
| Frame Type | 0x0806 | Untuk frame Ethernet II, field ini mengandung suatu nilai hexadecimal yang digunakan untuk menunjukkan jenis protokol upperlayer dalam data field. Ada banyak protokol upper-layer yang didukung oleh Ethernet II. Dua jenis frame yang umum adalah Nilai Deskripsi 0x0800 IPv4 Protocol 0x0806 Address Resolution Protocol (ARP) |
| Data | ARP | Mengandung protokol upper-level yang terenkapsulasi. Data field antara 46 – 1,500 byte. |
| FCS | Tidak terlihat dalam tangkapan | Frame Check Sequence, digunakan oleh NIC untuk mengidentifikasi error selama transmisi. Nilai ini dihitung oleh perangkat yang mengirimkan, mencakup jenis, field data dan alamat frame. Ini diverifikasi oleh penerima (receiver). |

1. **Soal dalam modul**
2. Apa yang penting mengenai isi dari field destination address?
3. Mengapa PC mengirimkan suatu broadcast ARP sebelum mengirimkan request ping yang pertama?
4. Sebutkan MAC address dari source dalam frame pertama?
5. Sebutkan Vendor ID (OUI) dari Source NIC dalam balasan ARP?
6. Bagian mana dari MAC address yang merupakan OUI?
7. Sebutkan nomor seri NIC dari source!

**Jawaban :**

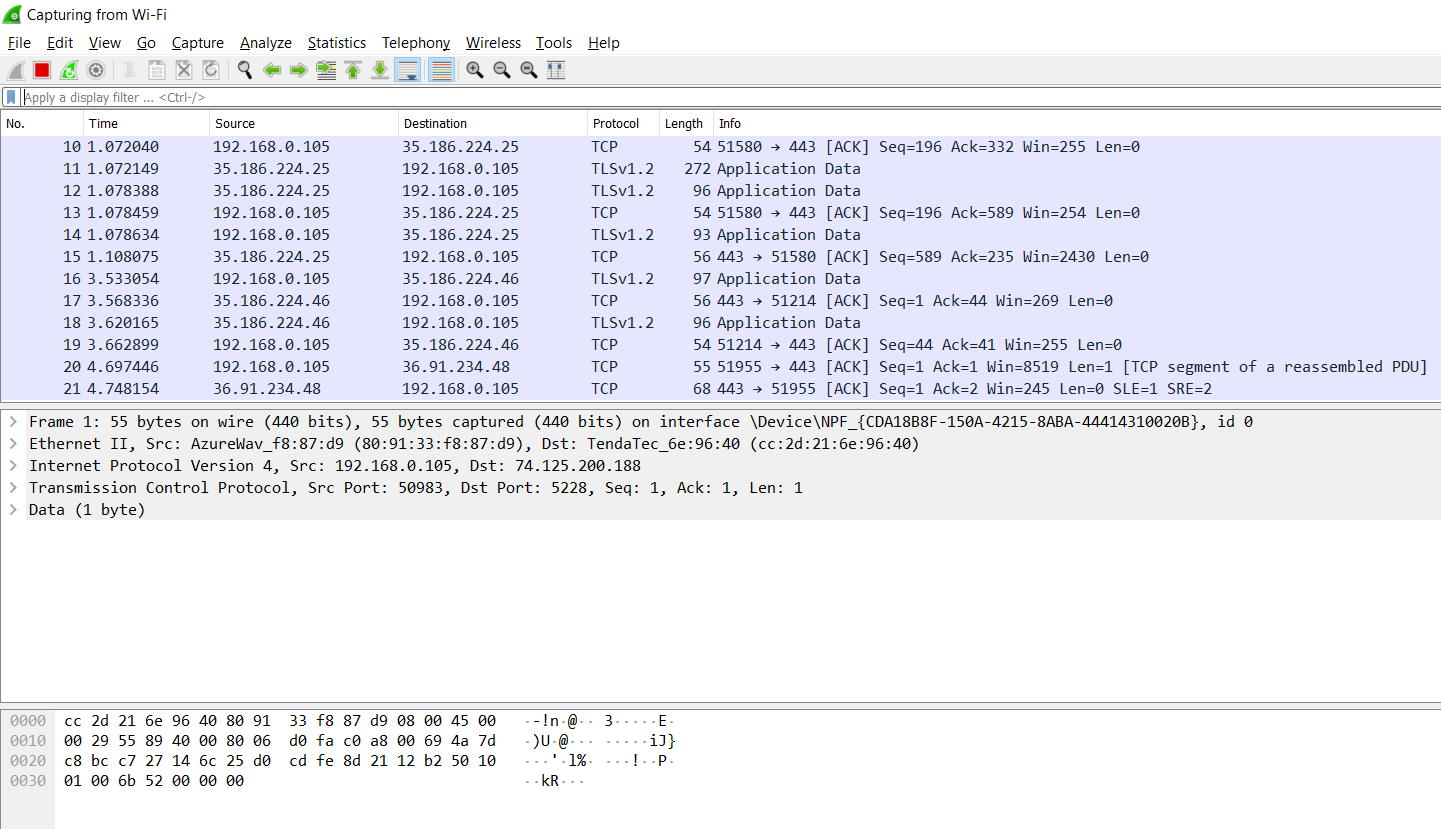
1. Field Destination Address adalah sebuah field yang memiliki panjang 6 byte yang menandakan alamat tujuan ke mana frame yang bersangkutan akan dikirimkan. Alamat tujuan ini bisa berupa alamat unicast Ethernet, alamat multicast Ethernet, atau alamat broadcast Ethernet. Jika tidak ada alamat pada field destination addres, maka tidak aka nada yang dituju.
2. untuk meminta Mac Address dari host dengan alamat IP yang terdapat dalam ARP. MAC Address tersebut nantinya akan digunakan untuk alamat yang akan dituju.
3. 80:91:33:f8:87:d9
4. Azure Wave
5. 3 octet pertama dari alamat Mac menunjukkan OUI.
6. f8:87:d9
7. **Latihan 2**
8. **Langkah 1: Mengetahui IP address dari default gateway pada PC anda**



Pada PC saya memiliki **IP Addres 192.168.0.105** dan **default gateaway 192.168.0.1**

1. **Langkah 2: Mulai menangkap trafik pada NIC PC**

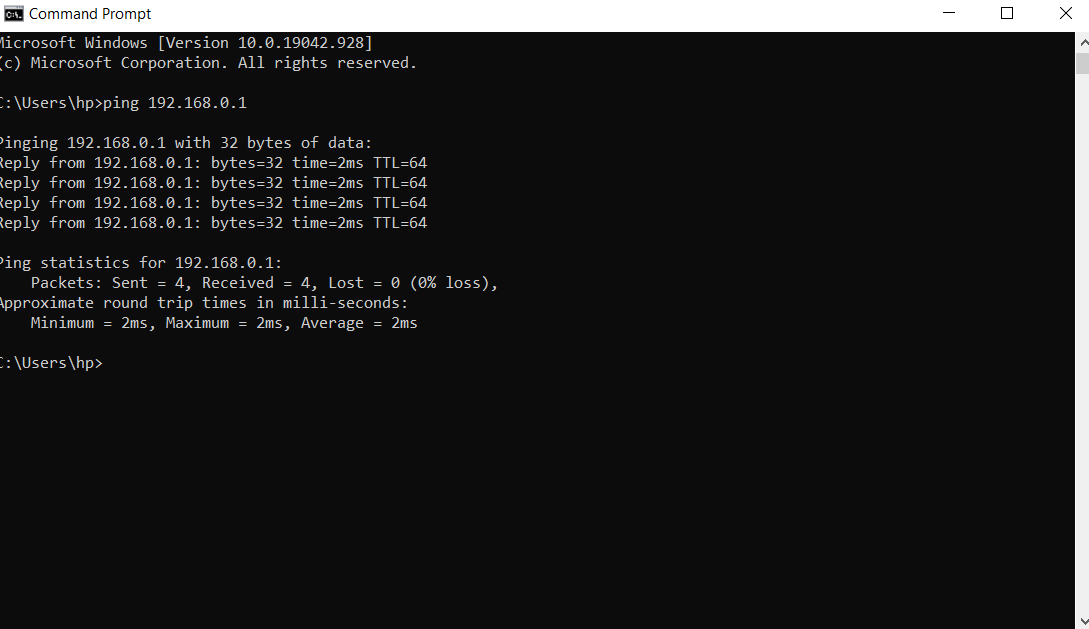
Saya menggunakan wifi untuk capture jaringan.



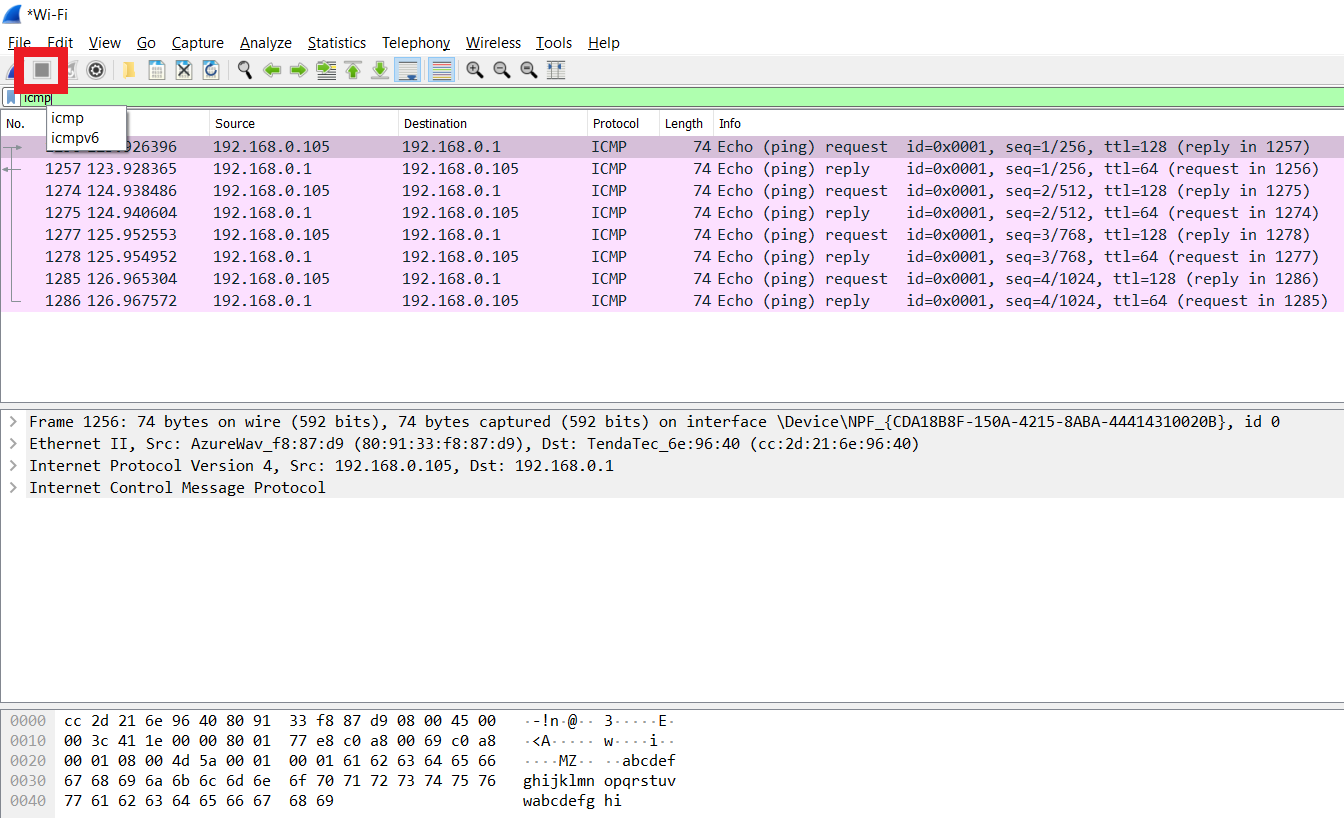
1. **Langkah 3: Menfilter Wireshark untuk menampilkan hanya trafik ICMP**



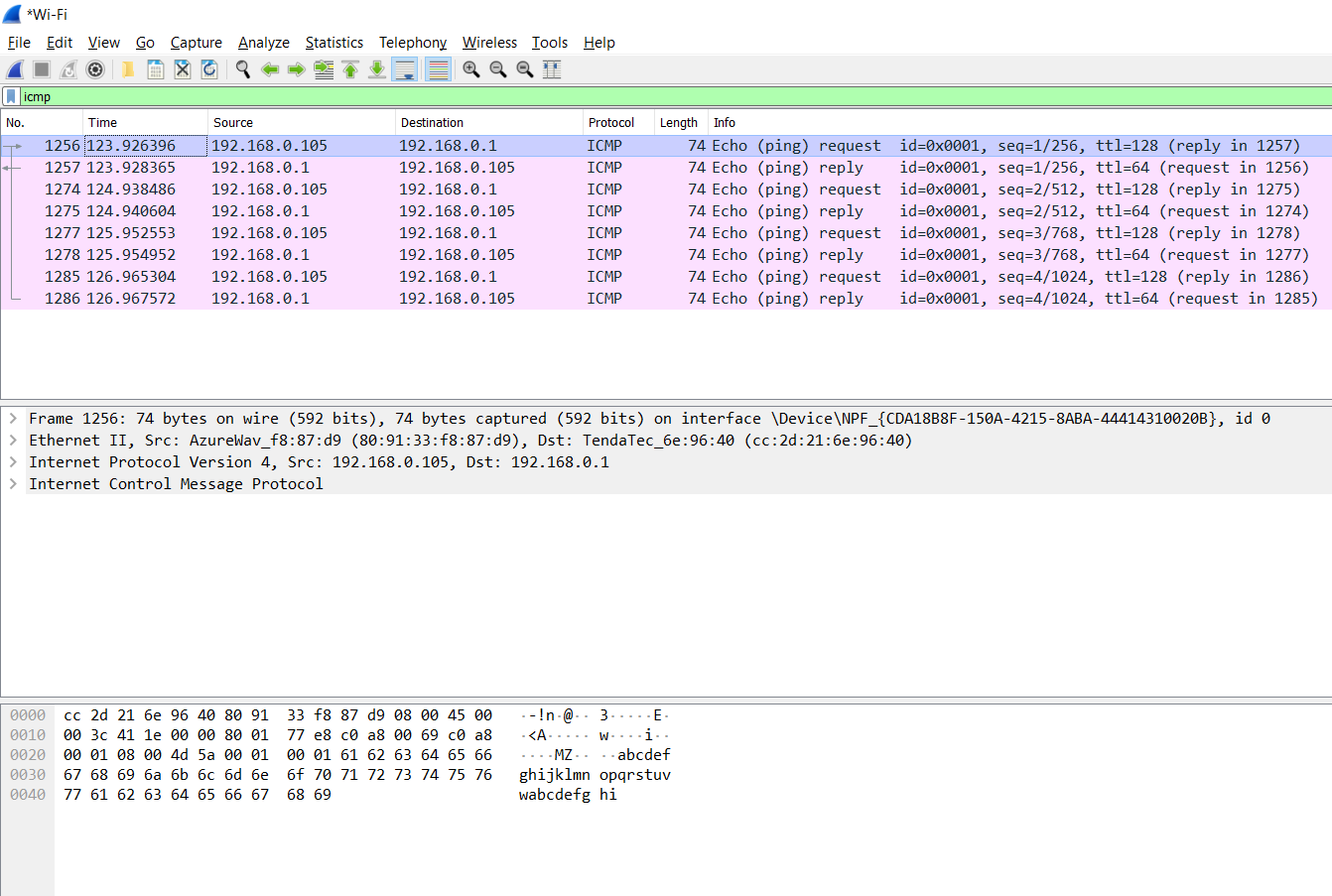
1. **Langkah 4: Dari jendela command prompt, ping default gateway dari PC**



1. **Langkah 5: Hentikan penangkapan trafik pada NIC**



1. **Langkah 6: Periksa request Echo (ping) pertama dalam Wireshark**



1. **Soal dalam modul**
2. Apa MAC address dari NIC PC?
3. Apa MAC address dari default gateway?
4. Anda dapat klik tanda lebih dari (>) pada awal baris kedua untuk memperoleh informasi lanjutan dari frame Ethernet II.

Jenis frame apa yang ditampilkan?

1. Dua baris terakhir ditampilkan dalam bagian tengah menyediakan informasi mengenai field data dari frame. Ingatlah bahwa data mengandung informasi IPv4 address source dan destination.

Mana IP address dari source?

Mana IP address dari destination?

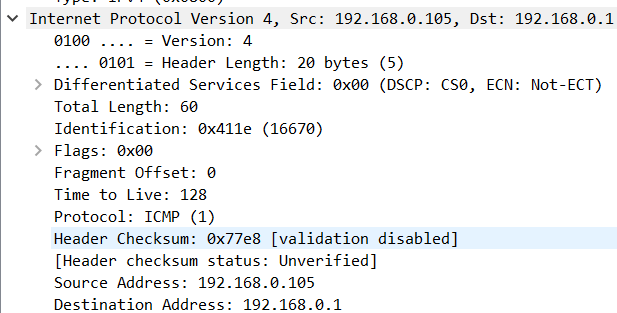
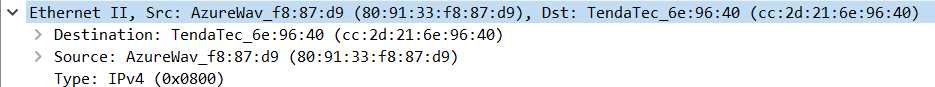
1. Anda dapat klik baris manapun dalam bagian tengah untuk menyorot bagian itu dari frame (hex dan ASCII) dalam panel Packet Bytes (bagian bawah). Klik baris Internet Control Message Protocol dalam bagian tengah dan periksa apa yang disorot dalam panel Packet Bytes.

Bagaimana mengeja dua oktet terakhir yang disorot?

1. Klik frame selanjutnya di dalam bagian atas dan periksalah frame Echo reply. Ingatlah bahwa MAC address dari source dan destination sudah terbalik, karena frame ini dikirimkan dari router default gateway sebagai balasan terhadap ping yang pertama.
2. Sebutkan device dan MAC address yang ditampilkan sebagai destination address!

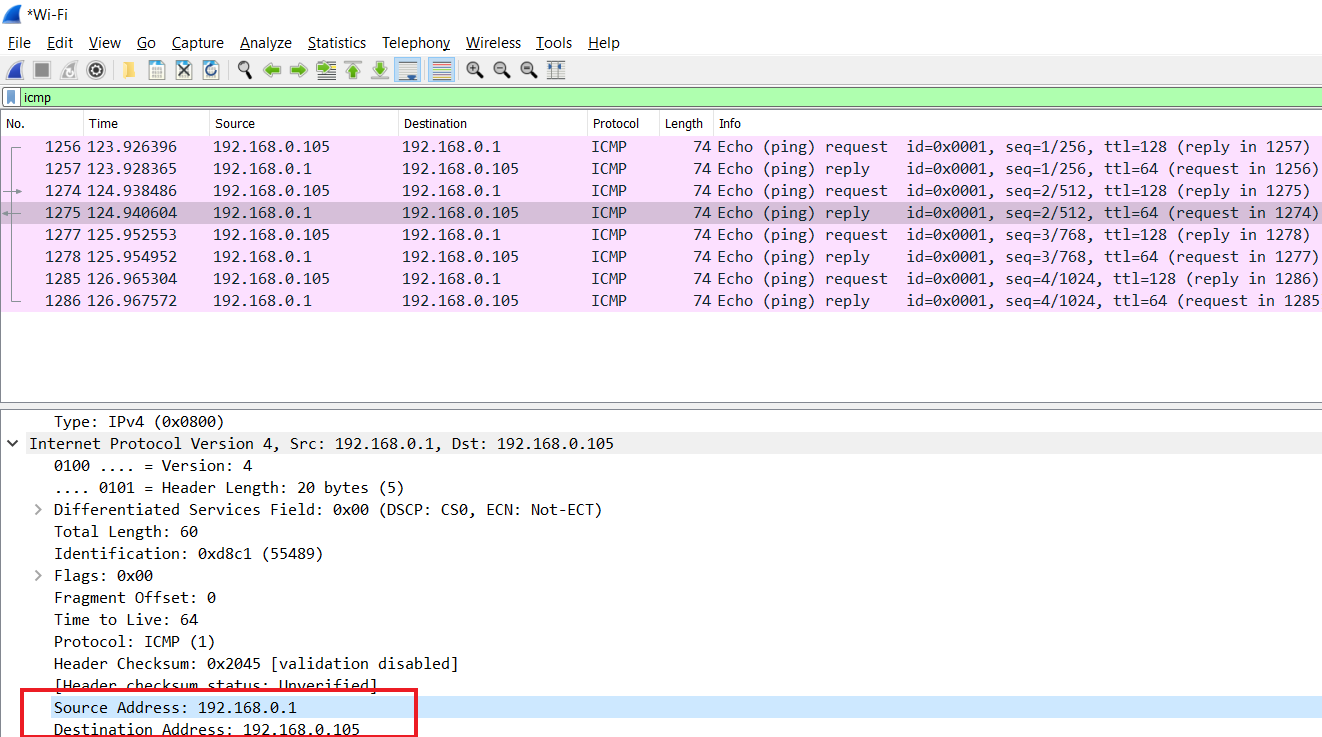
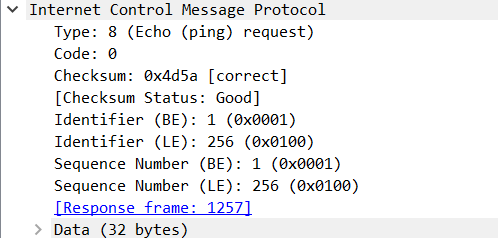
**Jawaban :**

1. 80:91:33:f8:87:d9
2. cc:2d:21:6e:96:40

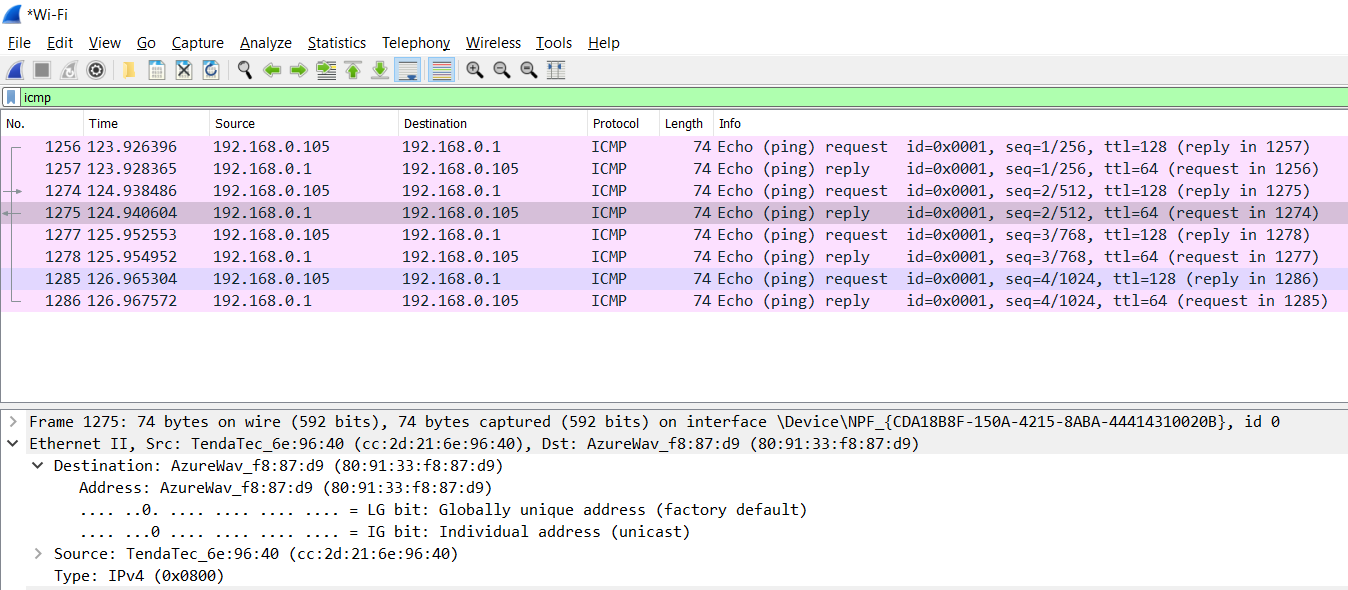


Ip Address : 192.168.0.105

Destination Address: 192.168.0.1



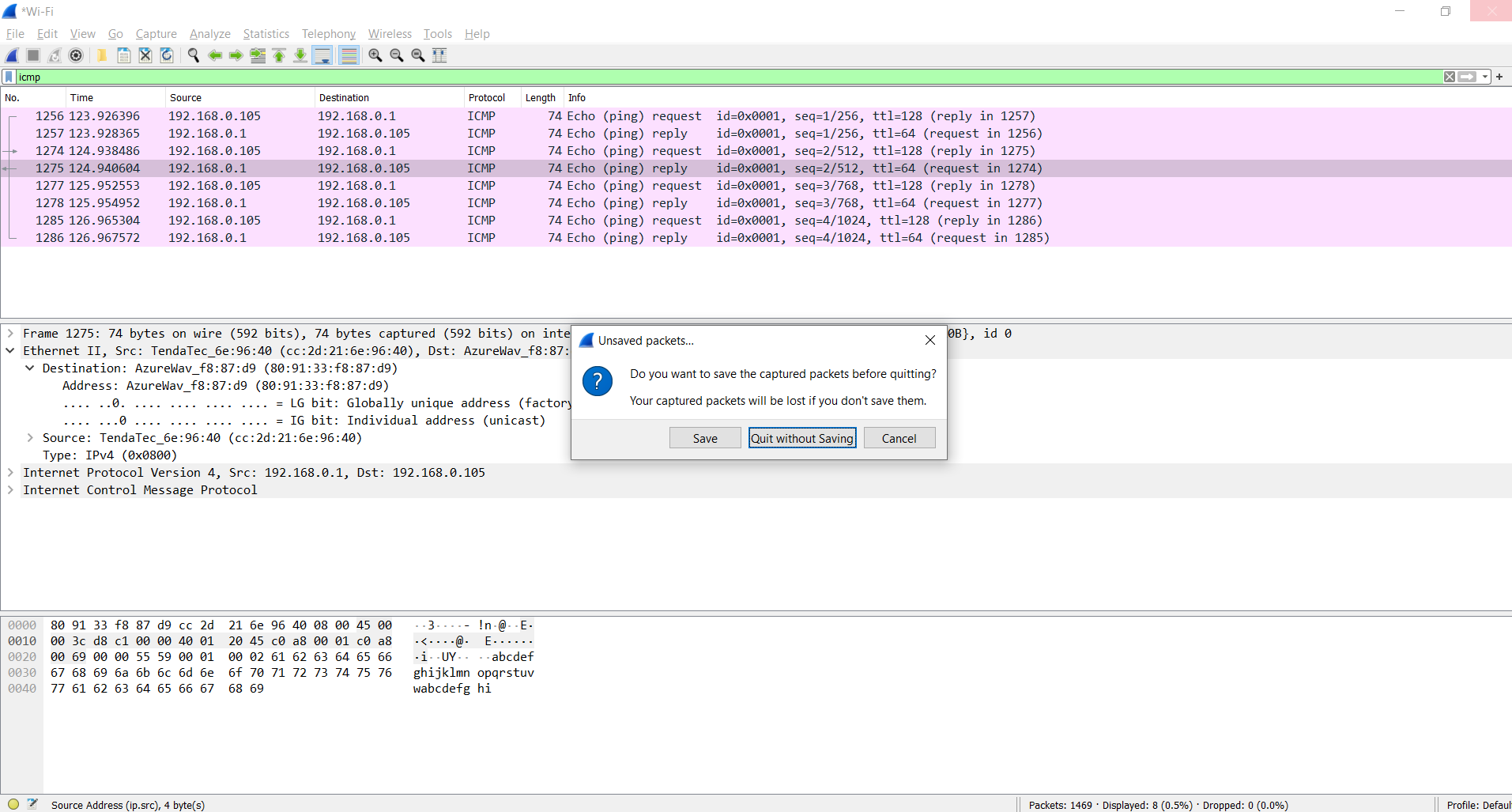
Terbalik



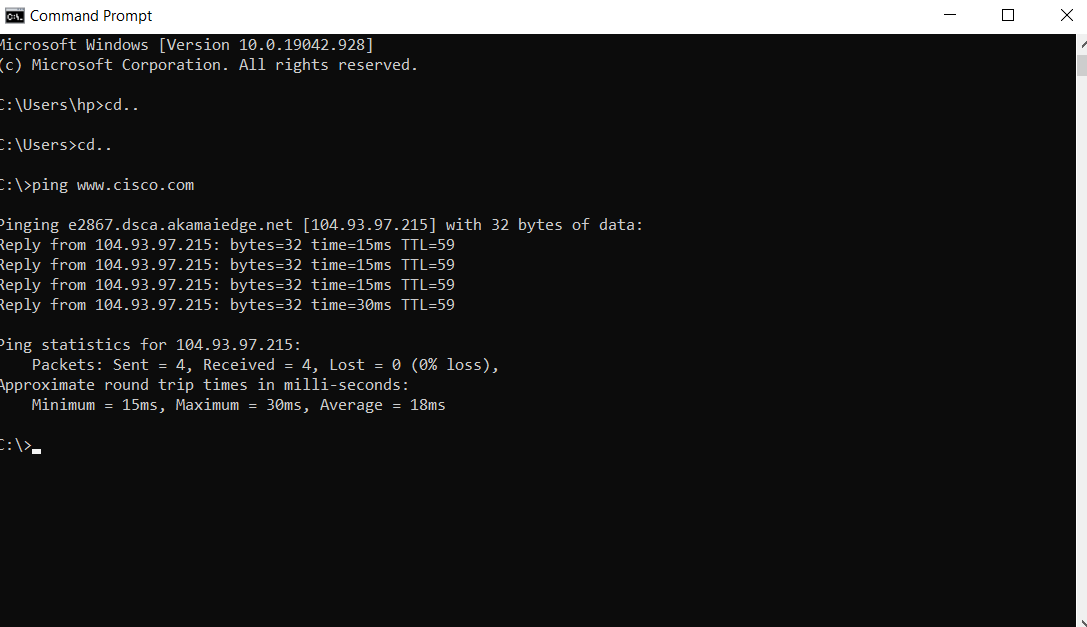
Azure Wave

1. **Langkah 7: Menangkap paket host jauh**

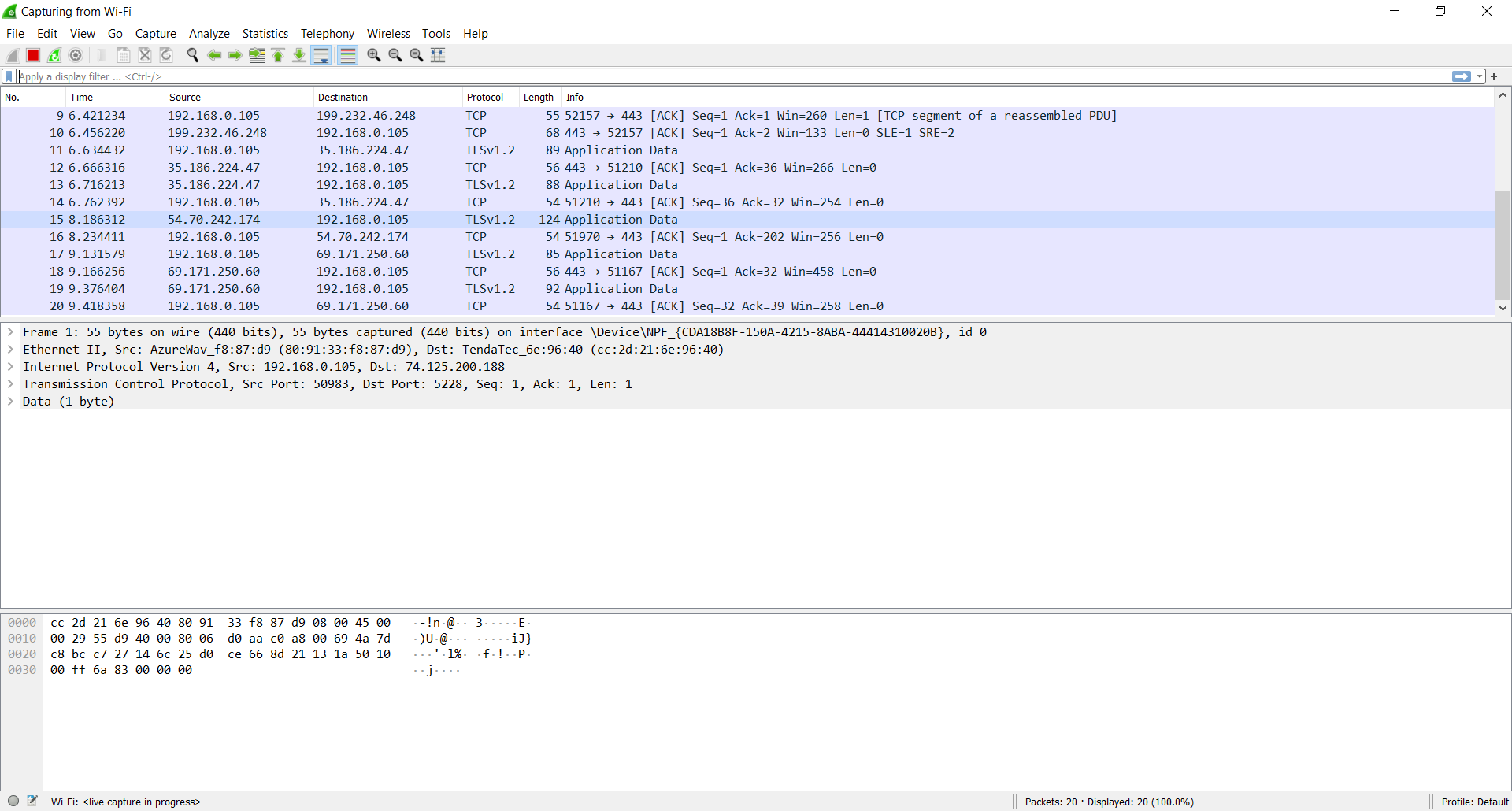
Quit without saving



Ping ke [www.cisco.com](http://www.cisco.com)



Capture whireshark baru



1. **Soal dalam modul**
2. Dalam frame request echo (ping) pertama, mana yang merupakan MAC address source dan destination?

**Source:**

**Destination:**

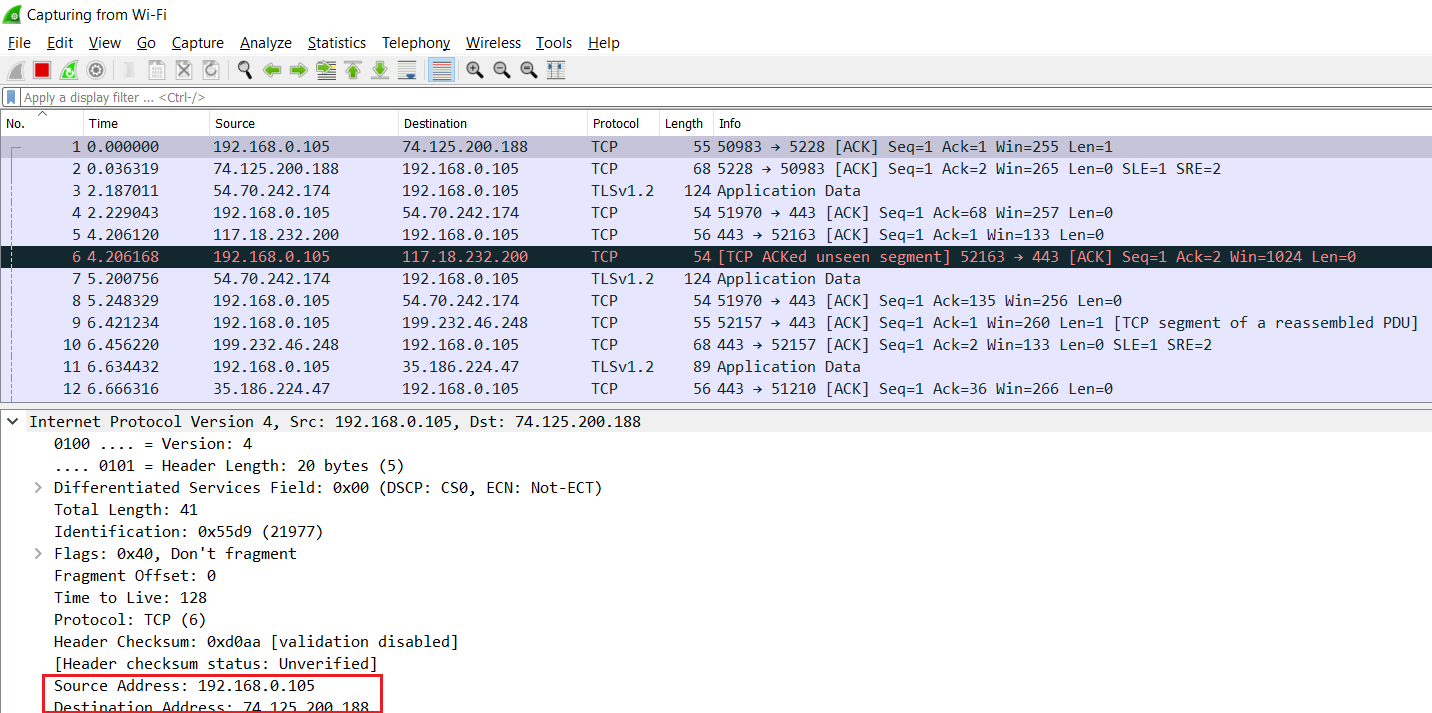
1. Sebtukan IP address source dan destination yang terkandung di dalam field data dari frame!

**Source:**

**Destination:**

1. Bandingkan address ini dengan address yang diterima pada Langkah 6. Address yang berubah hanyalah IP address destination. Mengapa IP address destination berubah, sedangkan MAC address destination tersebut masih tetap sama?
2. Wireshark tidak menampilkan field preamble dari suatu header frame. Apa yang terkandung dalam preamble?

**Jawaban :**



**Source: 192.168.0.105**

**Destination: 74.125.200.188**

1. **Source: 192.168.0.105**

**Destination: 74.125.200.188**

1. Langkah 6:

**Source: 192.168.0.105**

**Destination: 192.168.0.1**

Langkah 7:

**Source: 192.168.0.105**

**Destination: 74.125.200.188**

Karena frame layer 2 tidak pernah meninggalkan LAN. Ketika ping dikeluarkan ke host jarak jauh, sumber akan menggunakan alamat MAC Gateway Default untuk tujuan bingkai. Default Gateway menerima paket, menghapus informasi frame Layer 2 dari paket dan kemudian membuat header frame baru dengan alamat MAC hop berikutnya. Proses ini berlanjut dari router ke router hingga paket mencapai alamat IP tujuannya.

1. Field Preamble berisi tujuh oktet dari urutan 1010 bergantian, dan satu oktet yang menandakan awal frame, 10101011.