VERSION 1.0 JULY 14, 2022

[PRAKTIKUM KOMUNIKASI DATA]

MODUL 5 TUGAS – ETHERNET CONCEPTS

DISUSUN OLEH :

NUR EVINA MAKNUN
CHINTYA TRIA DIANA OKTAVIANI

DIAUDIT OLEH :

LUQMAN HAKIM, S.KOM., M.KOM.

PRESENTED BY: TIM LAB-IT
UNIVERSITAS MUHAMMADIYAH MALANG

[PRAKTIKUM KOMUNIKASI DATA]

PERSIAPAN MATERI

Praktikan diharapkan mempelajari Group Exam Modules 4 - 7: Ethernet Concepts Exam yang terdiri dari beberapa chapter berikut :

1. Physical Layer (Chapter 4)
2. Number Systems (Chapter 5)
3. Data Link Layer (Chapter 6)
4. Ethernet Switching (Chapter 7)

TUJUAN PRAKTIKUM

1. Bagian 1: Memeriksa Header dalam Frame Ethernet 2
2. Bagian 2: Menggunakan Wireshark untuk mengambil dan menganalisis Frame Ethernet

PERSIAPAN SOFTWARE/APLIKASI

- Komputer/Laptop
- Sistem operasi Windows/Linux/Max OS
- Wireshark 3.6.6 https://www.wireshark.org/download.html

MATERI POKOK

Bagian 1: Memeriksa Header dalam Frame Ethernet 2

1. Meninjau deskripsi dan panjang pada Header Ethernet 2

Preamble	Destination Address	Source Address	Frame Type	Data	FCS
8 Bytes	6 Bytes	6 Bytes	2 Bytes	46 – 1500 Bytes	4 Bytes

2. Memeriksa konfigurasi jaringan pada PC

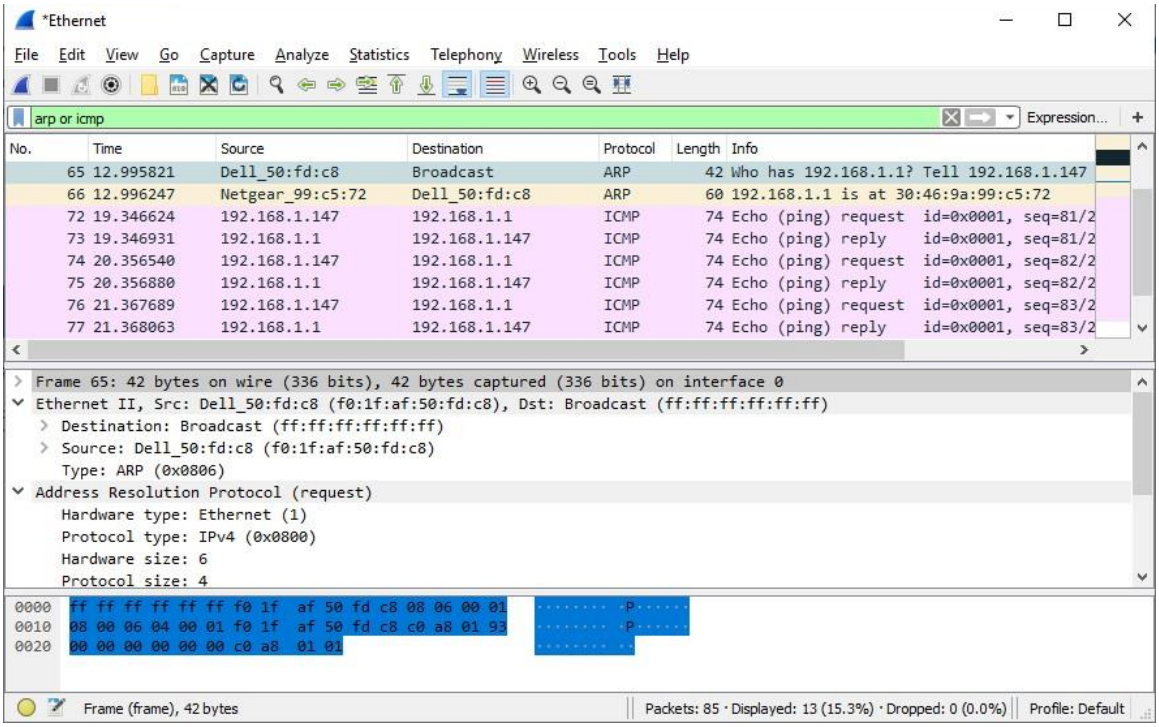
   Alamat IP host PC adalah 192.168.1.147 dan default gateway memiliki alamat IP 192.168.1.1

```
C:\> ipconfig /all

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82579LM Gigabit Network
```

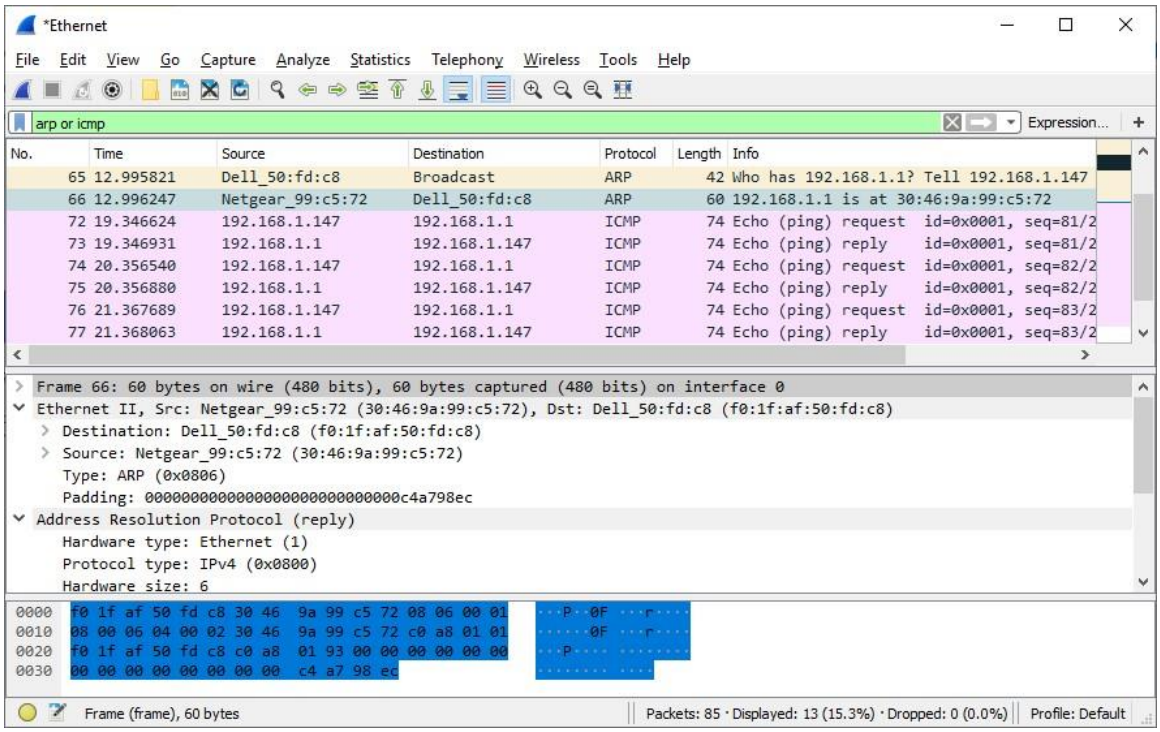
```
Connection
   Physical Address. . . . . . . . . : F0-1F-AF-50-FD-C8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::58c5:45f2:7e5e:29c2%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.147(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, September 6, 2019 11:08:36 AM
   Lease Expires . . . . . . . . . . : Saturday, September 7, 2019 11:08:36 AM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
<output omitted>
```

3. Memeriksa frame Ethernet dalam sebuah Wireshark.
   Hasil screenshoot di bawah ini menunjukkan paket yang dihasilkan oleh ping yang dikeluarkan dari host PC ke default gateway-nya.

Permintaan ARP



Balasan ARP



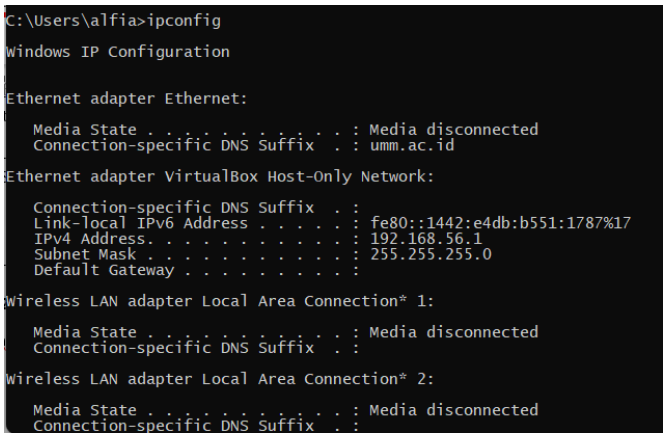
4. Memeriksa konten header Ethernet 2 dari permintaan ARP.

Field	Value	Description
Preamble	Not shown in capture	This field contains synchronizing bits, processed by the NIC hardware.
Destination Address Source Address	Broadcast (ff:ff:ff:ff:ff:ff) Netgear_99:c5:72 (30:46:9a:99:c5:72)	Layer 2 addresses for the frame. Each address is 48 bits long, or 6 octets, expressed as 12 hexadecimal digits, 0-9,A-F. A common format is 12:34:56:78:9A:BC. The first six hex numbers indicate the manufacturer of the network interface card (NIC), the last six hex numbers are the serial number of the NIC. The destination address may be a broadcast, which contains all ones, or a unicast. The source address is always unicast.
Frame Type	0x0806	For Ethernet II frames, this field contains a hexadecimal value that is used to indicate the type of upper-layer protocol in the data field. There are numerous upper-layer protocols supported by Ethernet II. Two common frame types are these: Value Description 0x0800 IPv4 Protocol

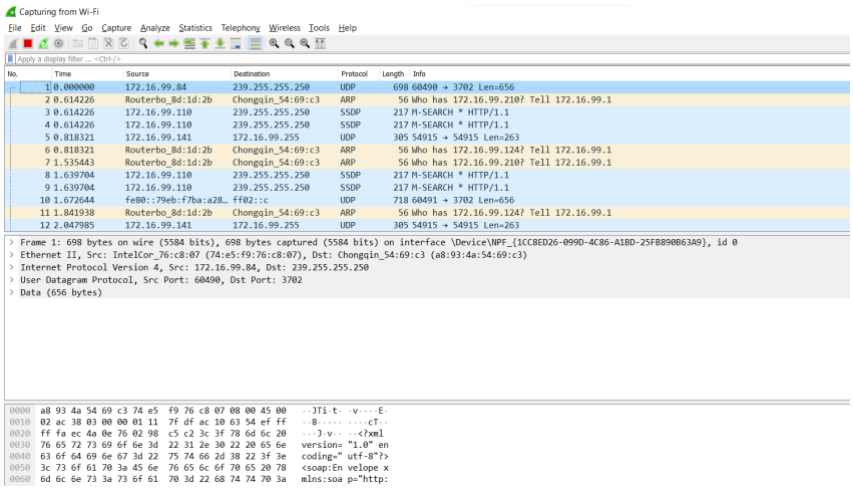
		0x0806 Address Resolution Protocol (ARP)
Data	ARP	Contains the encapsulated upper-level protocol. The data field is between 46 – 1,500 bytes.
FCS	Not shown in capture	Frame Check Sequence, used by the NIC to identify errors during transmission. The value is computed by the sending device, encompassing frame addresses, type, and data field. It is verified by the receiver.

Bagian 2: Menggunakan Wireshark untuk mengambil dan menganalisis Frame Ethernet

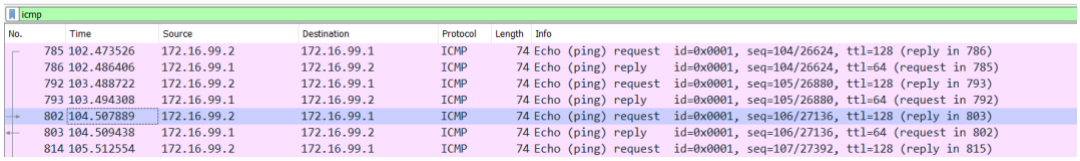
1. Tentukan alamat IP dari gateway default pada PC.
   a. Pastikan menggunakan model Realtime
   b. Buka Command Prompt pada tab Desktop
   c. Masukkan command **ipconfig**



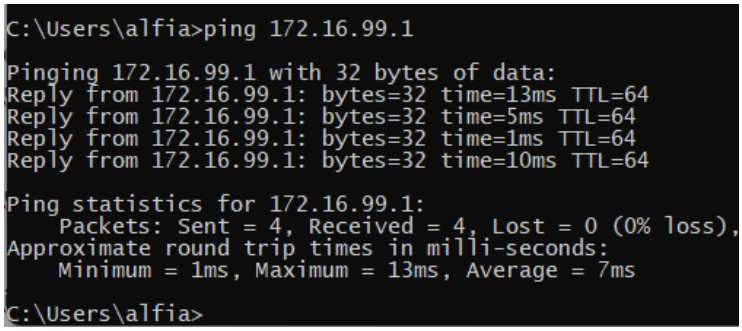
2. Lakukan pengambilan data lalu lintas di NIC PIC.
   a. Buka Wireshark untuk melakukan pengambilan data
   b. Amatilah lalu lintas yang muncul pada daftar paket.



3. Lakukan filtering wireshark agar menampilkan lalu lintas ICMP saja
   a. Gunakan filter di wireshark untuk memblokir visibilitas lalu lintas yang tidak diinginkan.
   b. Agar hanya lalu lintas ICMP saja yang akan muncul. Pada kotak filter wireshark silahkan ketik ICMP
   c. Kotak akan berubah menjadi warna hijau, jika sudah difilter dengan benar.
   d. Klik “Terapkan” (panah kanan) untuk menerapkan filter.

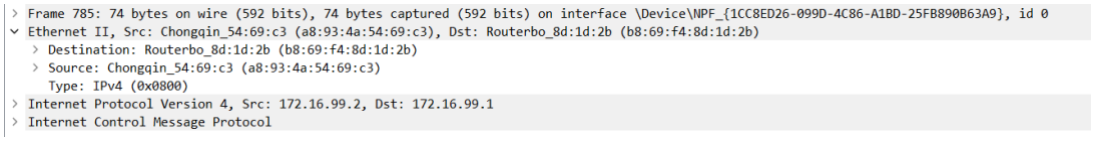


4. Lakukan ping gateway default PC pada command prompt
   a. Lakukan ping gateway default menggunakan alamat IP pada langkah 1



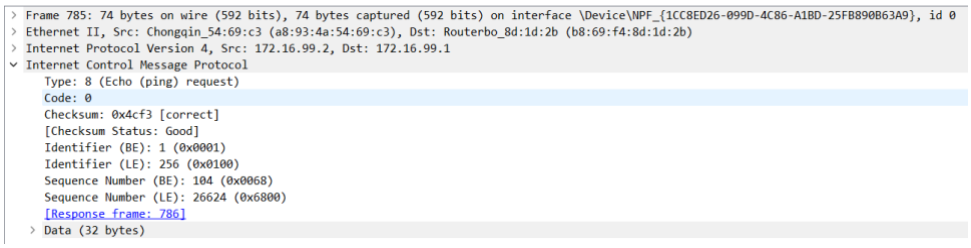
5. Lakukan pemberhentian pengambilan data lalu lintas di NIC
   a. Klik ikon **Stop Capturing Packets** untuk berhenti

6. Periksalah permintaan Echo (ping) pertama di Wireshark.
   a. Pada panel bagian atas, klik frame pertama yang terdaftar. Akan muncul permintaan Echo (ping) dibawah judul Info
   b. Periksa baris pertama di bagian tengah. Baris ini menampilkan panjang dari frame.
   c. Baris kedua di panel detail paket menunjukkan Frame Ethernet 2. Alamat MAC sumber dan tujuan juga ikut ditampilkan.
   d. Klik tanda (>) diawal baris kedua untuk informasi tentang Frame Ethernet 2

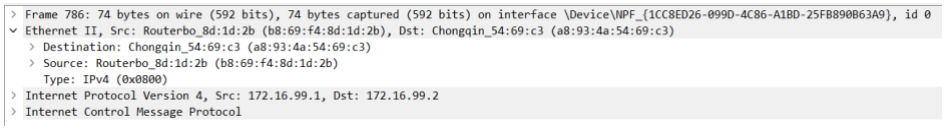


e. Dua baris terakhir yang ditampilkan di bagian tengah memberikan informasi tentang bidang data. Perhatikan bahwa data berisi informasi alamat IPv4 sumber dan tujuan.

f. Pilih garis mana saja di bagian tengah untuk menyorot bagian frame tersebut (hex dan ASCII) di panel Packet Bytes (bagian bawah). Klik baris Internet Control Message Protocol di bagian tengah dan periksa apa yang disorot di panel Packet Bytes.



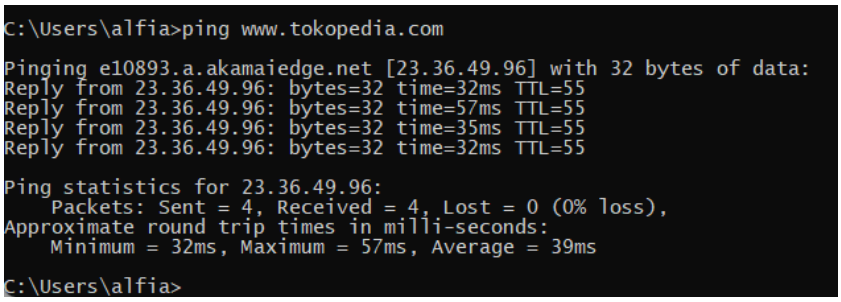
g. Klik next frame dibagian atas dan periksa balasan Echo. Perhatikan bahwa alamat MAC sumber dan tujuan telah dibalik, karena frame ini dikirim dari router gateway default sebagai balasan untuk ping pertama



7. Pengambilan paket untuk host jarak jauh

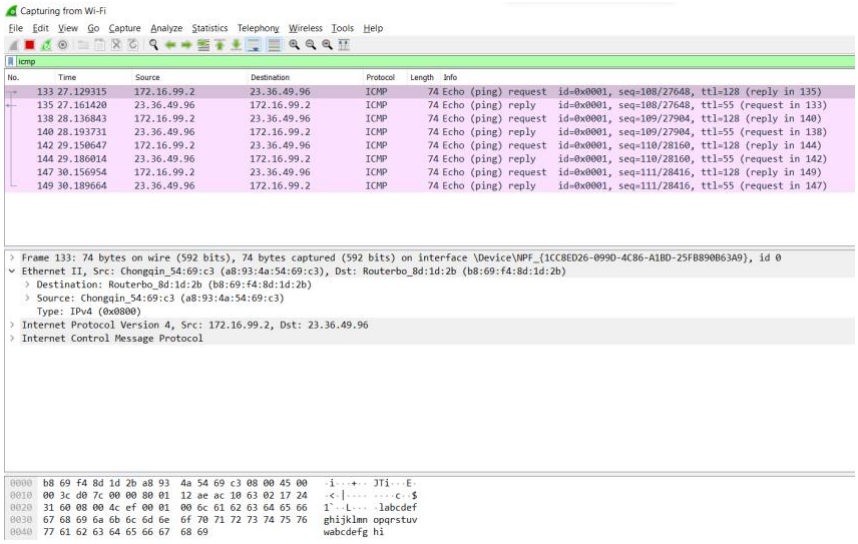
a. Klik **Start Capture** untuk memulai pengambilan wireshark baru. Lalu akan menerima sebuah pop-up yang menanyakan apakah ingin menyimpan paket yang diambil sebelumnya ke file sebelum memulai pengambilan baru. Klik **Continue without Saving.**

b. Pada command prompt, ping www.tokopedia.com



c. Hentikan pengambilan paket.

d. Periksalah data baru di panel daftar paket wireshark



PERTANYAAN TUGAS

1. Apa alamat IP sumber dan IP tujuan yang terdapat dalam Data Field of the Frame?
2. Bandingkan alamat yang ada di jawaban nomor 1 dengan alamat yang diterima di step 6!
3. Dari jawaban soal nomor 2, mengapa destination IP address berubah, sedangkan destination MAC address masih sama?

CATATAN

1. Batas maksimal dikerjakan H-1 praktikum dan dikumpulkan di i-Lab dengan format **[Nama_Nim_Modul5].rar**
2. Batas maksimal pengerjaan netacad adalah 1 minggu setelah jadwal praktikum

KRITERIA PENILAIAN TUGAS

>81 : Praktikan mampu mengerjakan serta menjelaskan tugas yang ada di materi tugas dengan benar

70 – 40 : Praktikan mampu mengerjakan serta menjelaskan tugas yang ada di materi tugas namun kurang maksimal.

KRITERIA PENILAIAN PRAKTEK

>81 : Praktikan mampu memahami, menjawab dan menjelaskan materi praktek kepada asisten.

70 – 80 : Praktikan mampu memahami, menjawab dan menjelaskan materi praktek kepada asisten namun kurang maksimal.

55 – 69 : Praktikan mampu menjawab soal yang ada di materi praktek kepada asisten namun tidak bisa menjelaskan proses yang terjadi.

<55 : Praktikan tidak memahami, menjawab dan menjelaskan materi praktek kepada asisten.

DETAIL PENILAIAN PRAKTIKUM

ASPEK PENILAIAN	POIN
TUGAS	30
PRAKTEK	70