VERSION 1.0 JULY 12, 2022

[PRAKTIKUM KOMUNIKASI DATA]

MODUL 1 TUGAS – BASIC NETWORK CONNECTIVITY AND COMMUNICATIONS

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 1-3 : Basic Network Connectivity and Comunications Exam yang terdiri dari beberapa chapter berikut :

1. Networking Today (Chapter 1)
2. Basic Switch and End Device Configuration (Chapter 2)
3. Protocols and Models (Chapter 3)

TUJUAN PRAKTIKUM

1. Bagian 1: Capture and Analyze Local ICMP Data in Wireshark
2. Bagian 2: Capture and Analyze Remote ICMP Data in Wireshark

PERSIAPAN SOFTWARE/APLIKASI

- Komputer/Laptop
- Sistem operasi Windows/Linux/Max OS
- Packet Tracer v8.1.1 https://www.packettracernetwork.com/download/download-packet-tracer.html
- Wireshark 3.6.6 https://www.wireshark.org/download.html

MATERI TUGAS

Bagian 1: Capture and Analyze Local ICMP Data in Wireshark

Di bagian ini, akan melalukan ping ke perangkat lain dalam satu jaringan LAN dan menangkap serta membalas ICMP request dengan menggunakan Wireshark. Analisis ini akan membantu memperjelas bagaimana packet headers melakukan transport data ke destinationnya.

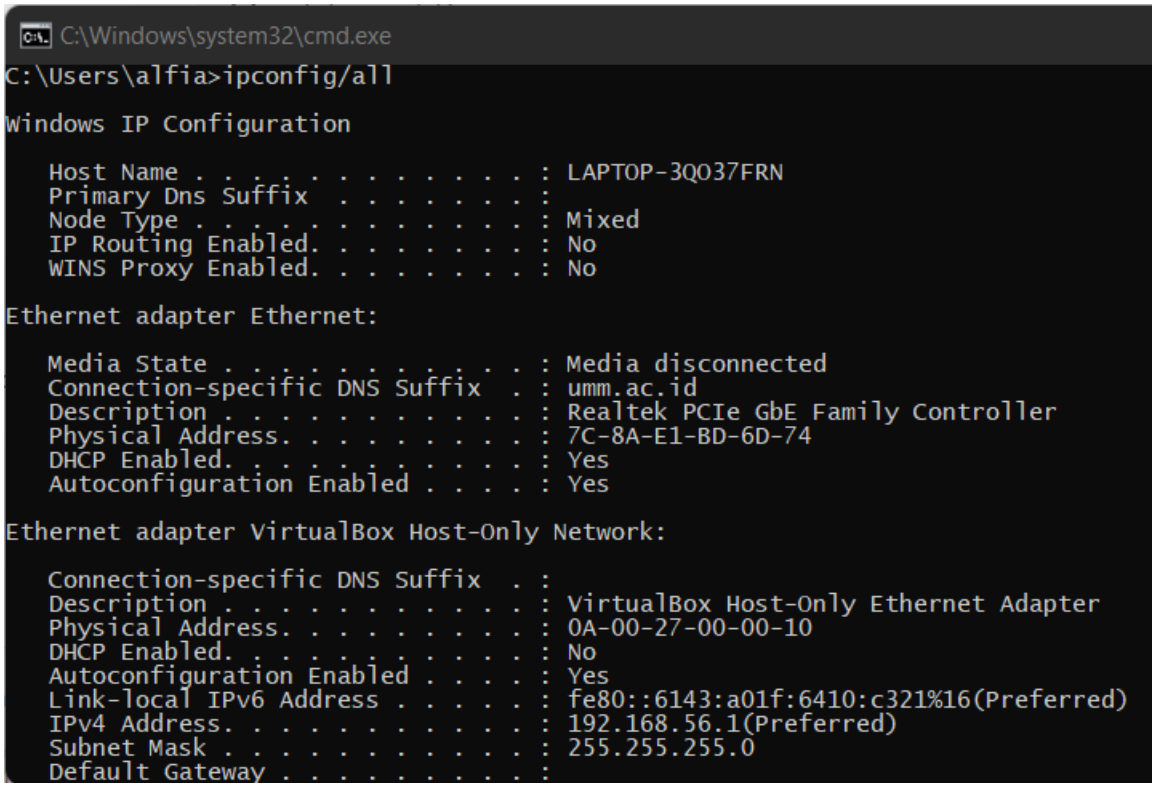
Sebagai catatan karena praktikum kali ini menggunakan setidaknya minimal 2 IP Address, maka bisa menggunakan metode dual Perangkat PC/laptop. Jika memang tidak bisa, alternatifnya adalah dengan menggunakan smartphone. Dan pastikan terhubungan dalam satu jaringan lokal.

1. Mendapatkan Informasi Interface Address Dari PC.

   Catat terlebih dahulu IP Address dan Network Interface Card (NIC) atau MAC pada Perangkat melalui command pada Command Prompt.

   - Buka Command Prompt dari PC/laptop dan masukkan command **ipconfig /all**

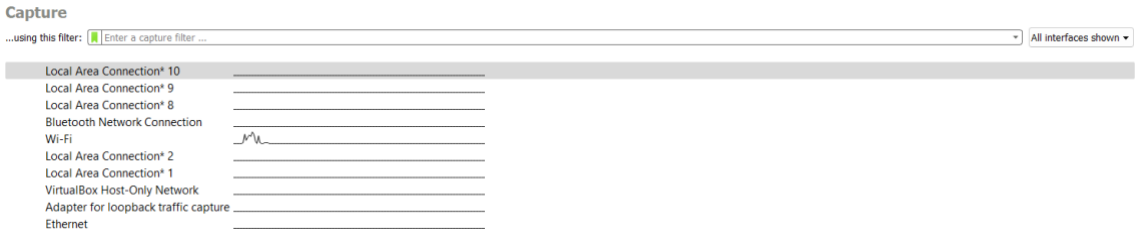
- Fokus pada jenis jaringan yang terhubung dengan Perangkat. Sebagai contoh seperti berikut:



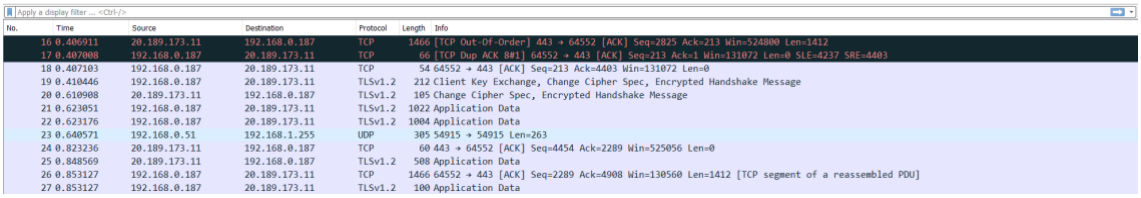
- Lakukan juga untuk Perangkat yang satunya dan catat nilai IP Addressnya. Jika menggunakan smartphone, silahkan cari IP Address dari smartphone di setting.

2. Menjalankan Wireshark dan Memulai Capture Data

- Buka wireshark, pada halaman awal akan muncul beberapa jaringan pada menu **Capture.** Pilih jaringan yang digunakan dengan cara double click. Pada dasarnya jaringan yang memiliki traffic akan terlihat ada grafik seperti berikut. Disini dicontohkan menggunakan Wi-Fi 2.

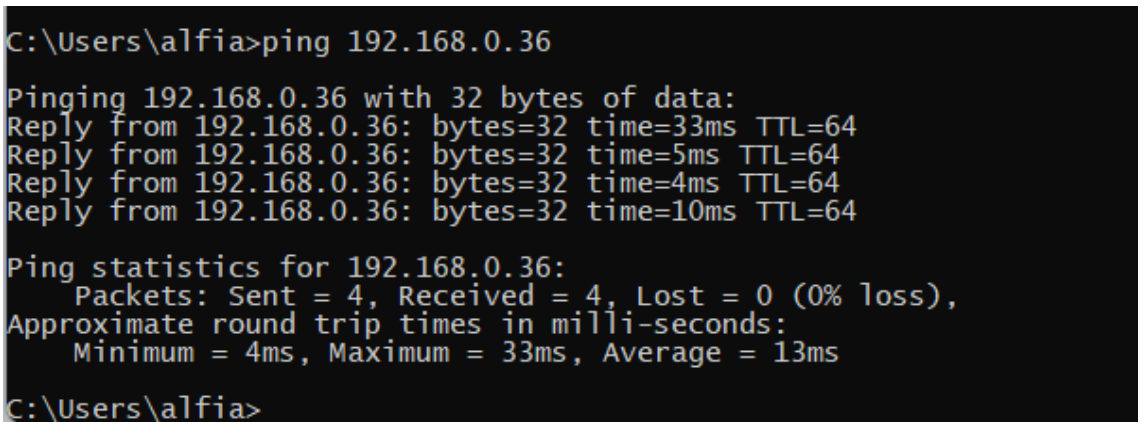


- Setelah double click jaringan yang dipilih, akan muncul semua proses yang terjadi dalam jaringan local tersebut pada wireshark dengan sangat cepat, contohnya seperti berikut :

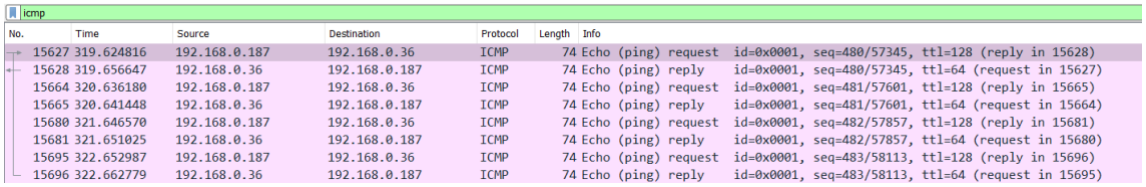


- Selain itu juga bisa memfilter berdasarkan Protocolnnya. Pada praktikum kali ini, hanya memfilter protocol **ICMP** saja. Pada field filter diatas, masukkan **ICMP** dan tekan ENTER pada keyboard.
- Pada list event seharusnya kosong karena belum melakukan kegiatan yang melibatkan protocol **ICMP.**

- Berikutnya, buka lagi command prompt untuk melakukan ping namun dengan IP Address dari Perangkat yang berbeda.

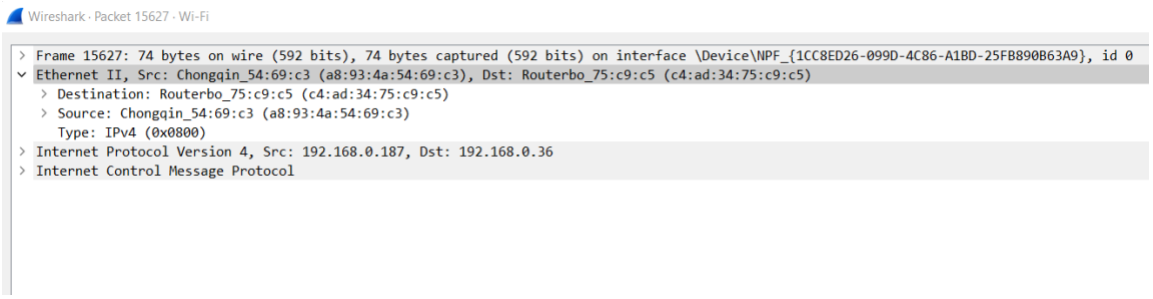


- Seperti pada gambar diatas, IP Address dari Perangkat kedua adalah 192.168.0.36. Pastikan menulis IP Address dengan benar. Apabila terjadi kendala error alternatifnya adalah matikan firewall pada pc/laptop.
- Setelah melakukan ping dari Perangkat yang berbeda, cek kembali ke wireshark. Maka akan muncul beberapa event baru dari protocol ICMP



- Klik stop capture apabila sudah berhasil.

3. Menganalisis data yang telah di-capture
   - Perhatikan bahwa kolom source adalah IP Addres. Sedangkan pada kolom destination adalah IP tujuan yang didapat dari IP Address Perangkat kedua.
   - Klik salah satu ICMP Request PDU yang ada pada di section atas wireshark.
   - Akan muncul tab baru, double klik Ethernet II untuk melihat destination dan source MAC



Catatan: Pada contoh sebelumnya dari permintaan ICMP yang telah ditangkap, data ICMP dienkapsulasi di dalam IPv4 packet PDU (header IPv4) yang kemudian dienkapsulasi dalam tab PDU Ethernet II (header Ethernet II) untuk ditransmisikan ke LAN.

Bagian 2: Melakukan Capture dan Analisis Pada Remote ICMP Data di dalam Wireshark

Pada Bagian ini, akan melakukan ping ke host jarak jauh dan memeriksa data yang dihasilkan dari ping tersebut. Kemudian akan menentukan data apa yang berbeda dari data pada Bagian 1.

1. Memulai capture data pada interface
   a. Tekan CTRL + W pada wireshark untuk menutup data sebelumnya.
   b. Lakukan capture data lagi, pada halaman awal akan muncul beberapa jaringan pada menu **Capture.** Pilih jaringan yang digunakan dengan cara double click
   c. Lakukan ping ketiga URL situs web berikut ke command prompt
      - www.tokopedia.com

- www.cisco.comhttp://www.cisco.com/
- www.instagram.com

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

Pinging www.tokopedia.com [23.54.58.69] with 32 bytes of data:
Reply from 23.54.58.69: bytes=32 time=33ms TTL=54
Reply from 23.54.58.69: bytes=32 time=32ms TTL=54
Reply from 23.54.58.69: bytes=32 time=32ms TTL=54
Reply from 23.54.58.69: bytes=32 time=34ms TTL=54

Ping statistics for 23.54.58.69:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 32ms, Maximum = 34ms, Average = 32ms

C:\Users\alfia>
```

```
C:\Users\alfia>ping www.cisco.com

Pinging www.cisco.com [23.15.104.32] with 32 bytes of data:
Reply from 23.15.104.32: bytes=32 time=29ms TTL=54
Reply from 23.15.104.32: bytes=32 time=32ms TTL=54
Reply from 23.15.104.32: bytes=32 time=30ms TTL=54
Reply from 23.15.104.32: bytes=32 time=30ms TTL=54

Ping statistics for 23.15.104.32:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 29ms, Maximum = 32ms, Average = 30ms

C:\Users\alfia>
```

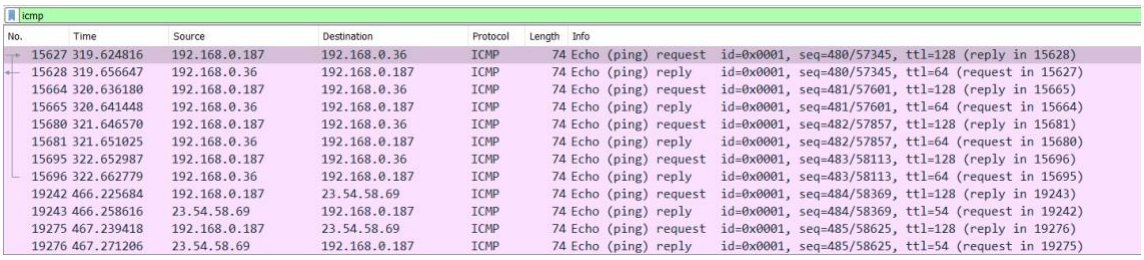
```
C:\Users\alfia>ping www.instagram.com

Pinging www.instagram.com [157.240.218.174] with 32 bytes of data:
Reply from 157.240.218.174: bytes=32 time=33ms TTL=54
Reply from 157.240.218.174: bytes=32 time=32ms TTL=54
Reply from 157.240.218.174: bytes=32 time=32ms TTL=54
Reply from 157.240.218.174: bytes=32 time=32ms TTL=54

Ping statistics for 157.240.218.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 32ms, Maximum = 33ms, Average = 32ms

C:\Users\alfia>
```

d. Saat melakukan ping ke URL tersebut, lihat pada wireshark untuk melihat proses capturing.



icmp

No.	Time	Source	Destination	Protocol	Length	Info
15627	319.624816	192.168.0.187	192.168.0.36	ICMP	74	Echo (ping) request id=0x0001, seq=480/57345, ttl=128 (reply in 15628)
15628	319.656647	192.168.0.36	192.168.0.187	ICMP	74	Echo (ping) reply id=0x0001, seq=480/57345, ttl=64 (request in 15627)
15664	320.636180	192.168.0.187	192.168.0.36	ICMP	74	Echo (ping) request id=0x0001, seq=481/57601, ttl=128 (reply in 15665)
15665	320.641448	192.168.0.36	192.168.0.187	ICMP	74	Echo (ping) reply id=0x0001, seq=481/57601, ttl=64 (request in 15664)
15680	321.646570	192.168.0.187	192.168.0.36	ICMP	74	Echo (ping) request id=0x0001, seq=482/57857, ttl=128 (reply in 15681)
15681	321.651025	192.168.0.36	192.168.0.187	ICMP	74	Echo (ping) reply id=0x0001, seq=482/57857, ttl=64 (request in 15680)
15695	322.652987	192.168.0.187	192.168.0.36	ICMP	74	Echo (ping) request id=0x0001, seq=483/58113, ttl=128 (reply in 15696)
15696	322.662779	192.168.0.36	192.168.0.187	ICMP	74	Echo (ping) reply id=0x0001, seq=483/58113, ttl=64 (request in 15695)
19242	466.225684	192.168.0.187	23.54.58.69	ICMP	74	Echo (ping) request id=0x0001, seq=484/58369, ttl=128 (reply in 19243)
19243	466.258616	23.54.58.69	192.168.0.187	ICMP	74	Echo (ping) reply id=0x0001, seq=484/58369, ttl=54 (request in 19242)
19275	467.239418	192.168.0.187	23.54.58.69	ICMP	74	Echo (ping) request id=0x0001, seq=485/58625, ttl=128 (reply in 19276)
19276	467.271206	23.54.58.69	192.168.0.187	ICMP	74	Echo (ping) reply id=0x0001, seq=485/58625, ttl=54 (request in 19275)

Catatan: Saat melakukan ping ke URL diatas, perhatikan bahwa Domain Name Server (DNS) menerjemahkan URL ke IP Address. Perhatikan IP Address yang diterima untuk setiap URL. Sstop capturing data dengan mengklik ikon Stop Capture.

PERTANYAAN TUGAS

1. Lakukan analisa data dari remote host. Lalu tentukan IP Address dan MAC dari ketiga URL diatas!
2. Bagaimana informasinya bisa berbeda dari informasi ping lokal yang diterima di Bagian 1? Jelaskan dengan bahasa sendiri!
3. Mengapa Wireshark menunjukkan alamat MAC sebenarnya dari local host, namun bukan alamat MAC sebenarnya untuk remote host?
4. Simpan hasil kerja wireshark untuk yang local host dan remote host dalam 1 folder!

CATATAN TUGAS

1. Batas maksimal dikerjakan H-1 praktikum dan dikumpulkan di i-Lab dengan format : **[Nama_Nim_Modul1].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