



# [PRAKTIKUM KOMUNIKASI DATA]

## MODUL 1 TUGAS – BASIC NETWORK CONNECTIVITY AND COMMUNICATIONS

**DISUSUN OLEH :**

FAIZAL QADRI TRIANTO

RIFKI RAMADANY MAJID

**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 Communications 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

1. Perangkat : Komputer/Laptop
  2. Sistem Operasi: Windows/Linux/Mac OS
  3. Aplikasi :
    - Packet Tracer 8.2.2 <https://skillsforall.com/resources/lab-downloads?courseLang=en-US>
    - Wireshark 4.2.6 <https://www.wireshark.org/download.html>
- 

### MATERI TUGAS

#### **Bagian 1: Capture and Analyze Local ICMP Data in Wireshark**

Di bagian ini, Anda akan melakukan ping ke perangkat lain dalam jaringan LAN yang sama dan menangkap serta menganalisis permintaan ICMP menggunakan Wireshark. Analisis ini akan membantu memperjelas bagaimana header paket membawa data ke tujuannya.

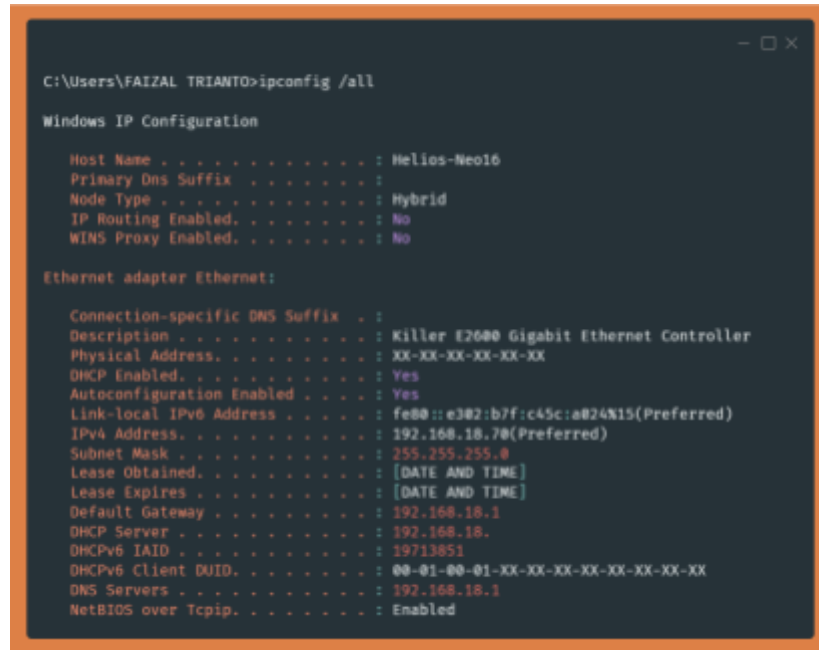
Praktikum ini memerlukan setidaknya dua alamat IP, sehingga Anda dapat menggunakan dua perangkat PC/laptop. Jika tidak memungkinkan, Anda bisa menggunakan smartphone sebagai alternatif. Pastikan kedua perangkat terhubung ke jaringan lokal yang sama.

1. Mendapatkan Informasi Alamat Jaringan dari PC:

Catat terlebih dahulu IP Address dan Network Interface Card (NIC) atau MAC Address

pada perangkat melalui Command Prompt.

- Buka Command Prompt dari PC/laptop dan masukkan perintah **ipconfig /all**.
- Fokus pada jenis jaringan yang terhubung dengan perangkat, seperti Wi-Fi atau Ethernet, dan catat alamat IP serta MAC Address yang tertera.



```

C:\Users\FAIZAL TRIANTO>ipconfig /all

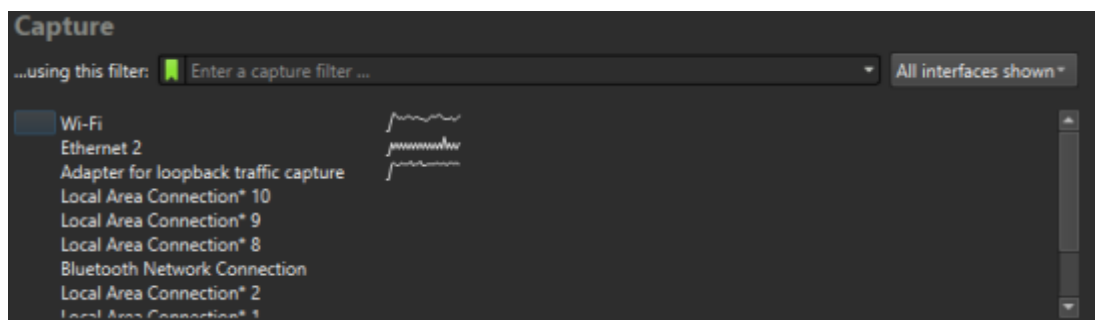
Windows IP Configuration

Host Name . . . . . : Helios-Neo16
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Description . . . . . : Killer E2000 Gigabit Ethernet Controller
Physical Address. . . . . : XX-XX-XX-XX-XX-XX
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::e302:b7f:c45c:a024%15(Preferred)
IPv4 Address. . . . . : 192.168.18.70(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : [DATE AND TIME]
Lease Expires . . . . . : [DATE AND TIME]
Default Gateway . . . . . : 192.168.18.1
DHCP Server . . . . . : 192.168.18.1
DHCPv6 IAID . . . . . : 19713851
DHCPv6 Client DUID. . . . . : 00-01-00-01-XX-XX-XX-XX-XX-XX-XX-XX-XX
DNS Servers . . . . . : 192.168.18.1
NetBIOS over Tcpip. . . . . : Enabled
  
```

- Lakukan langkah yang sama untuk perangkat lain dan catat alamat IP-nya. Jika menggunakan smartphone, cari alamat IP di pengaturan jaringan.
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. Jaringan yang memiliki traffic akan terlihat dalam bentuk grafik. Sebagai contoh, gunakan Wi-Fi.



- Setelah double-click jaringan yang dipilih, Wireshark akan menampilkan semua proses

yang terjadi dalam jaringan lokal tersebut dengan cepat.

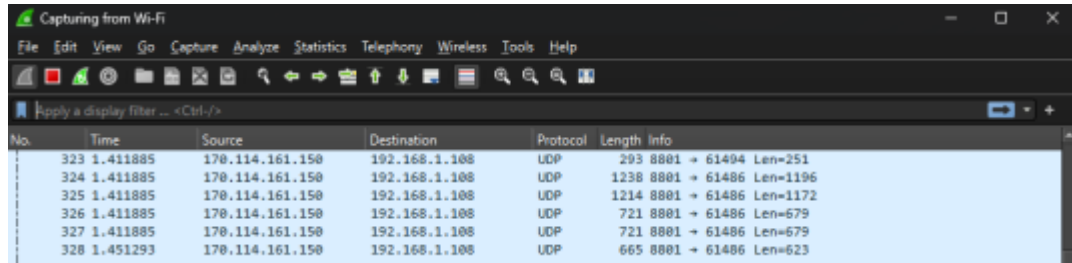
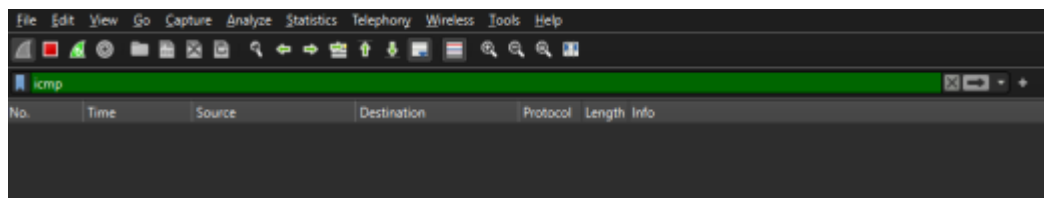


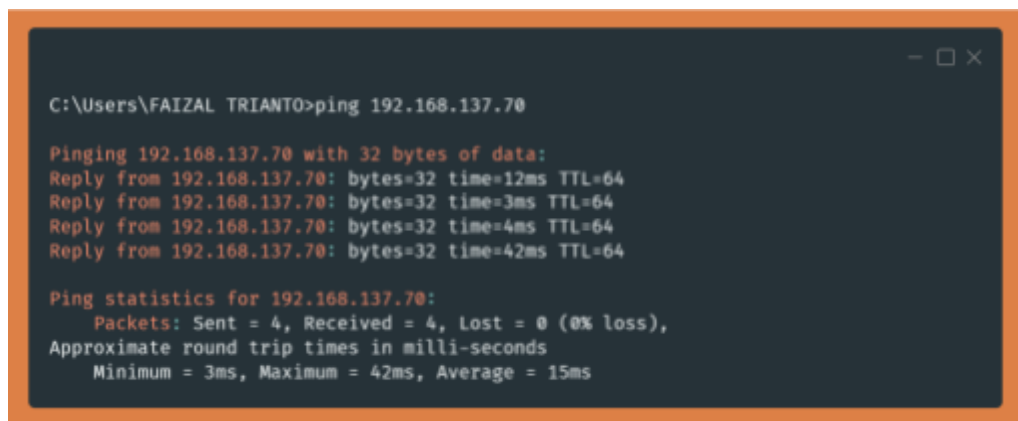
Figure 1: Wireshark packet capture showing ICMP traffic. The display filter is set to 'icmp'. The packet list shows several ICMP Echo (ping) requests from 170.114.161.150 to 192.168.1.108.

No.	Time	Source	Destination	Protocol	Length	Info
323	1.411885	170.114.161.150	192.168.1.108	UDP	293	8801 → 61404 Len=251
324	1.411885	170.114.161.150	192.168.1.108	UDP	1238	8801 → 61486 Len=1196
325	1.411885	170.114.161.150	192.168.1.108	UDP	1214	8801 → 61486 Len=1172
326	1.411885	170.114.161.150	192.168.1.108	UDP	721	8801 → 61486 Len=679
327	1.411885	170.114.161.150	192.168.1.108	UDP	721	8801 → 61486 Len=679
328	1.451293	170.114.161.150	192.168.1.108	UDP	665	8801 → 61486 Len=623

- Anda dapat memfilter data berdasarkan protokol. Pada praktikum kali ini, hanya memfilter protokol **ICMP** saja. Pada field filter di bagian atas, masukkan **icmp** dan tekan ENTER pada keyboard.
- Pada daftar event, seharusnya kosong karena belum ada aktivitas yang melibatkan protokol **ICMP**.



- Buka kembali Command Prompt untuk melakukan ping dengan menggunakan IP Address dari perangkat lain.



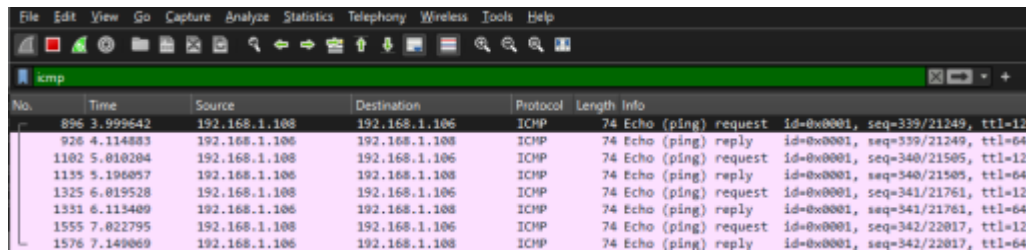
```
C:\Users\FAIZAL TRIANTO>ping 192.168.137.70

Pinging 192.168.137.70 with 32 bytes of data:
Reply from 192.168.137.70: bytes=32 time=12ms TTL=64
Reply from 192.168.137.70: bytes=32 time=3ms TTL=64
Reply from 192.168.137.70: bytes=32 time=4ms TTL=64
Reply from 192.168.137.70: bytes=32 time=42ms TTL=64

Ping statistics for 192.168.137.70:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 42ms, Average = 15ms
```

- Misalnya, IP Address dari perangkat kedua adalah 192.168.1.106. Pastikan menulis IP Address dengan benar. Jika terjadi error, coba matikan firewall pada PC/laptop.
- Setelah melakukan ping dari perangkat lain, periksa kembali Wireshark. Akan muncul

beberapa event baru dari protokol ICMP.



No.	Time	Source	Destination	Protocol	Length	Info
896	3.999642	192.168.1.108	192.168.1.106	ICMP	74	Echo (ping) request id=0x0001, seq=339/21249, ttl=128
926	4.114883	192.168.1.106	192.168.1.108	ICMP	74	Echo (ping) reply id=0x0001, seq=339/21249, ttl=64
1102	5.010204	192.168.1.108	192.168.1.106	ICMP	74	Echo (ping) request id=0x0001, seq=340/21505, ttl=128
1135	5.196057	192.168.1.106	192.168.1.108	ICMP	74	Echo (ping) reply id=0x0001, seq=340/21505, ttl=64
1325	6.019528	192.168.1.108	192.168.1.106	ICMP	74	Echo (ping) request id=0x0001, seq=341/21761, ttl=128
1351	6.113409	192.168.1.106	192.168.1.108	ICMP	74	Echo (ping) reply id=0x0001, seq=341/21761, ttl=64
1555	7.022795	192.168.1.108	192.168.1.106	ICMP	74	Echo (ping) request id=0x0001, seq=342/22017, ttl=128
1576	7.149069	192.168.1.106	192.168.1.108	ICMP	74	Echo (ping) reply id=0x0001, seq=342/22017, ttl=64

- Klik Stop Capture jika sudah berhasil.
3. Menganalisis Data yang Telah Di-capture:
- Perhatikan bahwa kolom Source menunjukkan IP Address pengirim, sedangkan kolom Destination menunjukkan IP tujuan yang didapat dari IP Address perangkat kedua.
  - Klik salah satu ICMP Request PDU yang ada di bagian atas Wireshark.
  - Akan muncul tab baru, double-click pada Ethernet II untuk melihat destination dan source MAC Address.

```

> Frame 1555: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF...
> Ethernet II, Src: Intel_21:3f:db (f0:d4:15:21:3f:db), Dst: 8e:7c:ac:33:cb:ab (8e:7c:ac:33:cb:ab)
  > Destination: 8e:7c:ac:33:cb:ab (8e:7c:ac:33:cb:ab)
  > Source: Intel_21:3f:db (f0:d4:15:21:3f:db)
    Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 192.168.1.108, Dst: 192.168.1.106
  > Internet Control Message Protocol

```

**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.

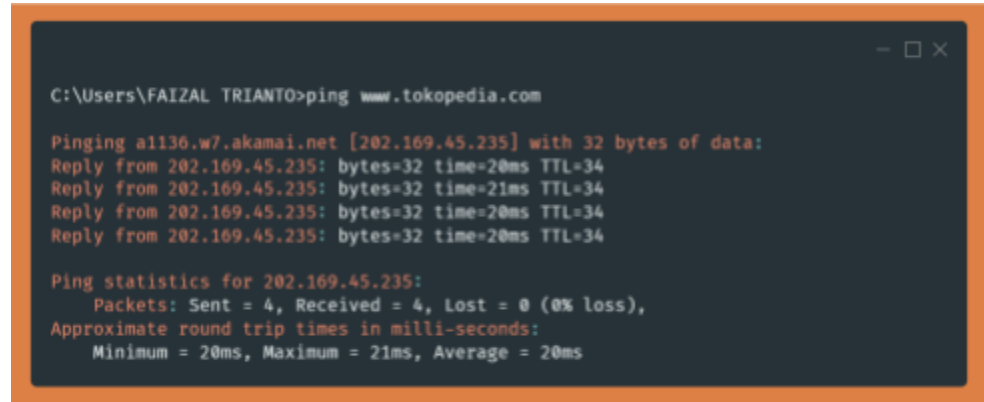
## Bagian 2: Capture and Analyze Remote ICMP Data in Wireshark

Di bagian ini, Anda akan melakukan ping ke host jarak jauh dan memeriksa data yang dihasilkan dari ping tersebut. Anda kemudian akan menentukan perbedaan data ini dibandingkan dengan data dari Bagian 1.

1. Menganalisis Data yang Telah Di-capture:
  - Tekan CTRL + W pada Wireshark untuk menutup data capture sebelumnya.
  - Lakukan capture data lagi. Pada halaman awal, pilih jaringan yang digunakan dengan

cara double-click.

- Lakukan ping ke tiga URL situs web berikut melalui Command Prompt:
  - ping [www.tokopedia.com](http://www.tokopedia.com)

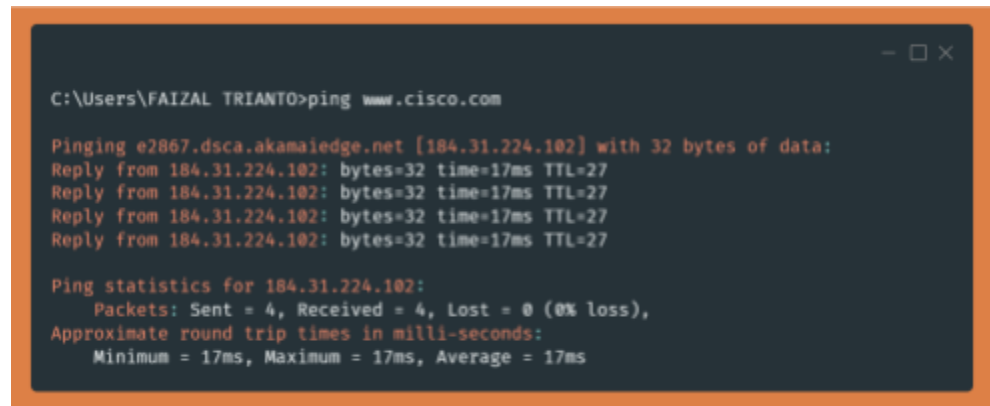


```
C:\Users\FAIZAL TRIANTO>ping www.tokopedia.com

Pinging a1136.w7.akamai.net [202.169.45.235] with 32 bytes of data:
Reply from 202.169.45.235: bytes=32 time=20ms TTL=34
Reply from 202.169.45.235: bytes=32 time=21ms TTL=34
Reply from 202.169.45.235: bytes=32 time=20ms TTL=34
Reply from 202.169.45.235: bytes=32 time=20ms TTL=34

Ping statistics for 202.169.45.235:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 21ms, Average = 20ms
```

- ping [www.cisco.com](http://www.cisco.com)

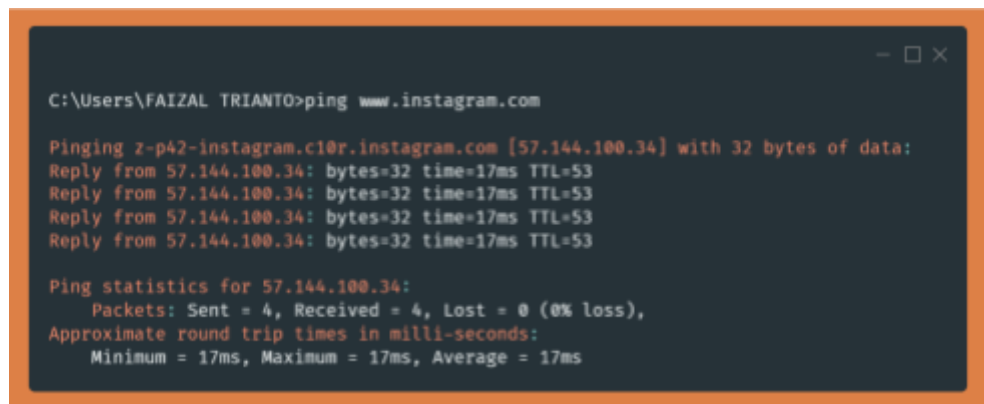


```
C:\Users\FAIZAL TRIANTO>ping www.cisco.com

Pinging e2867.dsca.akamaiedge.net [184.31.224.102] with 32 bytes of data:
Reply from 184.31.224.102: bytes=32 time=17ms TTL=27
Reply from 184.31.224.102: bytes=32 time=17ms TTL=27
Reply from 184.31.224.102: bytes=32 time=17ms TTL=27
Reply from 184.31.224.102: bytes=32 time=17ms TTL=27

Ping statistics for 184.31.224.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 17ms, Maximum = 17ms, Average = 17ms
```

- ping [www.instagram.com](http://www.instagram.com)

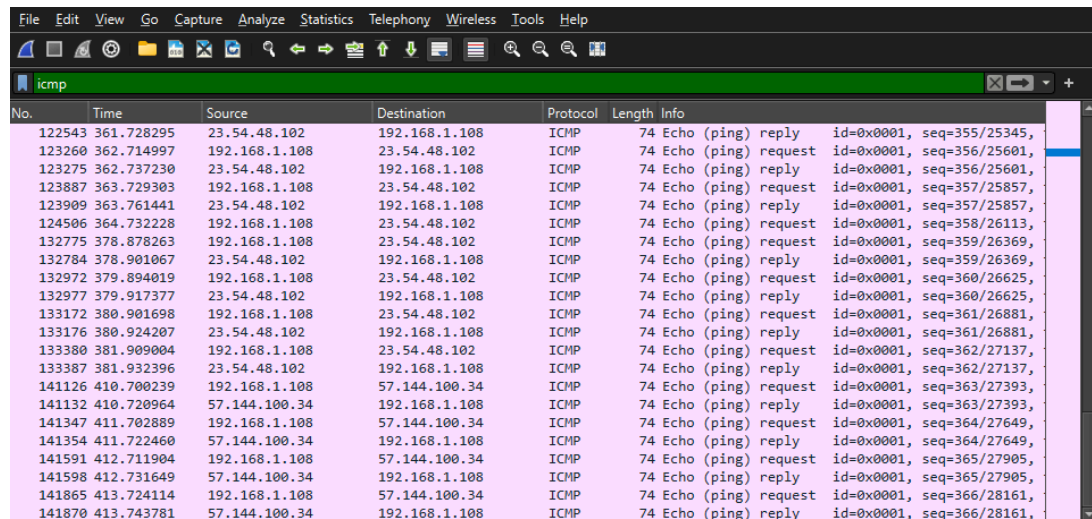


```
C:\Users\FAIZAL TRIANTO>ping www.instagram.com

Pinging z-p42-instagram.c10r.instagram.com [57.144.100.34] with 32 bytes of data:
Reply from 57.144.100.34: bytes=32 time=17ms TTL=53
Reply from 57.144.100.34: bytes=32 time=17ms TTL=53
Reply from 57.144.100.34: bytes=32 time=17ms TTL=53
Reply from 57.144.100.34: bytes=32 time=17ms TTL=53

Ping statistics for 57.144.100.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 17ms, Maximum = 17ms, Average = 17ms
```

- Saat melakukan ping ke URL tersebut, perhatikan Wireshark untuk melihat proses capturing.



No.	Time	Source	Destination	Protocol	Length	Info
122543	361.728295	23.54.48.102	192.168.1.108	ICMP	74	Echo (ping) reply id=0x0001, seq=355/25345,
123260	362.714997	192.168.1.108	23.54.48.102	ICMP	74	Echo (ping) request id=0x0001, seq=356/25601,
123275	362.737230	23.54.48.102	192.168.1.108	ICMP	74	Echo (ping) reply id=0x0001, seq=356/25601,
123887	363.729303	192.168.1.108	23.54.48.102	ICMP	74	Echo (ping) request id=0x0001, seq=357/25857,
123909	363.761441	23.54.48.102	192.168.1.108	ICMP	74	Echo (ping) reply id=0x0001, seq=357/25857,
124506	364.732228	192.168.1.108	23.54.48.102	ICMP	74	Echo (ping) request id=0x0001, seq=358/26113,
132775	378.878263	192.168.1.108	23.54.48.102	ICMP	74	Echo (ping) request id=0x0001, seq=359/26369,
132784	378.901067	23.54.48.102	192.168.1.108	ICMP	74	Echo (ping) reply id=0x0001, seq=359/26369,
132972	379.894019	192.168.1.108	23.54.48.102	ICMP	74	Echo (ping) request id=0x0001, seq=360/26625,
132977	379.917377	23.54.48.102	192.168.1.108	ICMP	74	Echo (ping) reply id=0x0001, seq=360/26625,
133172	380.901698	192.168.1.108	23.54.48.102	ICMP	74	Echo (ping) request id=0x0001, seq=361/26881,
133176	380.924207	23.54.48.102	192.168.1.108	ICMP	74	Echo (ping) reply id=0x0001, seq=361/26881,
133380	381.909004	192.168.1.108	23.54.48.102	ICMP	74	Echo (ping) request id=0x0001, seq=362/27137,
133387	381.932396	23.54.48.102	192.168.1.108	ICMP	74	Echo (ping) reply id=0x0001, seq=362/27137,
141126	410.700239	192.168.1.108	57.144.100.34	ICMP	74	Echo (ping) request id=0x0001, seq=363/27393,
141132	410.720964	57.144.100.34	192.168.1.108	ICMP	74	Echo (ping) reply id=0x0001, seq=363/27393,
141347	411.702889	192.168.1.108	57.144.100.34	ICMP	74	Echo (ping) request id=0x0001, seq=364/27649,
141354	411.722460	57.144.100.34	192.168.1.108	ICMP	74	Echo (ping) reply id=0x0001, seq=364/27649,
141591	412.711904	192.168.1.108	57.144.100.34	ICMP	74	Echo (ping) request id=0x0001, seq=365/27905,
141598	412.731649	57.144.100.34	192.168.1.108	ICMP	74	Echo (ping) reply id=0x0001, seq=365/27905,
141865	413.724114	192.168.1.108	57.144.100.34	ICMP	74	Echo (ping) request id=0x0001, seq=366/28161,
141870	413.743781	57.144.100.34	192.168.1.108	ICMP	74	Echo (ping) reply id=0x0001, seq=366/28161,

**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.

---

## PERTANYAAN TUGAS

Berdasarkan informasi yang diperiksa selama penangkapan Packet Tracer tentukan:

- a. Apakah MAC Address dari perangkat Anda berubah ketika Anda terhubung ke jaringan yang berbeda? Berikan penjelasan rinci dan contoh tentang bagaimana MAC Address berperilaku di jaringan yang berbeda.
- b. Mengapa MAC Address penting dalam jaringan komputer? Diskusikan bagaimana MAC Address digunakan dalam proses pengiriman data dan identifikasi perangkat.
- c. Setelah melakukan ping ke ketiga URL, gunakan Wireshark untuk mengidentifikasi IP Address dari setiap host tersebut. Bagaimana proses pengambilan data ini berbeda dari pengambilan data lokal yang dilakukan sebelumnya?
- d. Jelaskan bagaimana Anda dapat memastikan bahwa PC/Laptop Anda dapat terhubung ke ketiga URL tersebut. Langkah apa yang diambil untuk mengatasi masalah koneksi yang mungkin terjadi?
- e. Apa perbedaan utama yang Anda temukan antara hasil ping lokal dan ping remote? Gunakan pemahaman Anda tentang jaringan untuk menjelaskan mengapa perbedaan ini terjadi.



---

## CATATAN PRAKTEK

1. Batas maksimal dikerjakan H-1 praktikum dan dikumpulkan di i-Lab dengan format:  
**[Nama\_Nim\_Modul1].rar**
  2. Batas maksimal pengerjaan di NetAcad adalah 1 minggu setelah jadwal praktikum.
  3. Semoga Beruntung ! 😊
- 

## KRITERIA PENILAIAN TUGAS

- > 81 : Praktikan mampu mengerjakan serta menjelaskan tugas yang ada di materi tugas dengan benar.
  - 70 – 80 : Praktikan mampu mengerjakan serta menjelaskan tugas yang ada di materi tugas namun kurang maksimal.
  - 55 - 69 : Praktikan memiliki pemahaman yang terbatas tentang materi tugas dan perlu meningkatkan kemampuan dalam mengerjakan serta menjelaskan tugas.
  - < 55 : Praktikan tidak memahami, menjawab, dan memahami materi modul tugas.
- 

## 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