

Register No:	99220040570
Name:	K.Hanumaan
Class/Section:	8501 A/S06
Ex.No:	13
Name of the Experiment	Capture and Analyse ICMP packet
Google Drive link of the packet tracer file (give view permission):	https://drive.google.com/file/d/1uWQcuBJXNYw2RQI4yHc0uvAcJpKBHDeq/view?usp=drive_link

1. Use command prompt and fill the following details using ipconfig /all command. (highlight and paste screenshot for each of the output).

Parameter	Value
Your Machine IP Address.	10.2.16.28
Your Machine MAC Address	14-D4-24-17-5E-9B
Default Gateway address	10.2.0.1
DNS Server IP Address	172.16.103.254

Wireless LAN adapter Wi-Fi:

```

Connection-specific DNS Suffix . : 
Description . . . . . : MediaTek MT7921 Wi-Fi 6 802.11ax PCIe Adapter
Physical Address. . . . . : 14-D4-24-17-5E-9B
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::81c6:cfc8:e5c5:292e%5(Preferred)
IPv4 Address. . . . . : 10.2.16.28(Preferred)
Subnet Mask . . . . . : 255.255.224.0
Lease Obtained. . . . . : 14 March 2025 13:40:12
Lease Expires . . . . . : 15 March 2025 01:40:12
Default Gateway . . . . . : 10.2.0.1
DHCP Server . . . . . : 10.2.0.2
DHCPv6 IAID . . . . . : 68473892
DHCPv6 Client DUID. . . . . : 00-01-00-01-2B-F6-99-AF-E0-73-E7-CE-7D-F6
DNS Servers . . . . . : 172.16.103.254
                        4.2.2.2
                        8.8.8.8
NetBIOS over Tcpi. . . . . : Enabled

```

2. Ping any website through command prompt and Fill the following details by applying the filter as **ICMP**:
(highlight and paste screenshot for each of the output).

ICMP Request message:

Field Name	Field Length (no of bits)	Field value
Type	8 bits	0 (Echo Request)
Code	8 bits	0 (No further details needed for Echo Reply)
Checksum	16 bits	0x4d56
Identifier	16 bits	1 (0x0001)
Sequence Number	16 bits	5 (0x0005)

The screenshot shows a Wireshark packet capture of an ICMP Echo (ping) request and reply. The packet list at the top shows frame 3421 as the request and frame 3436 as the reply. The packet details for frame 3421 show the ICMP Echo (ping) request with Type 8, Code 0, Checksum 0x4d56, Identifier 1, and Sequence Number 5. The packet bytes pane shows the raw data of the ICMP request.

No.	Time	Source	Destination	Protocol	Length	Info
→ 3421	15.130747	10.2.16.28	142.250.183.228	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 3436)
← 3436	15.144240	142.250.183.228	10.2.16.28	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=118 (request in 3421)
← 3681	16.143059	10.2.16.28	142.250.183.228	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 3684)
← 3684	16.156204	142.250.183.228	10.2.16.28	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=118 (request in 3681)
← 3958	17.146563	10.2.16.28	142.250.183.228	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (no response found!)
← 5389	21.719663	10.2.16.28	142.250.183.228	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (no response found!)

Frame 3421: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{149AA54B-F72F-4FA9-92FD-52EABE47000A}, id 0
 Ethernet II, Src: AzureWaveTec_17:5e:9b (14:d4:24:17:5e:9b), Dst: Sophos_fc:00:10 (c8:4f:86:fc:00:10)
 Internet Protocol Version 4, Src: 10.2.16.28, Dst: 142.250.183.228
 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: 3436]
 Data (32 bytes)

ICMP Reply message: (highlight and paste screenshot for each of the output).

Field Name	Field Length (no of bits)	Field value
Type	8 bits	0 (Echo Reply)
Code	8 bits	0 (No further details needed for Echo Reply)
Checksum	16 bits	0x5556
Identifier	16 bits	1 (0x0001)
Sequence Number	16 bits	5 (0x0005)

Wireshark packet capture showing ICMP Echo (ping) reply. The packet list shows a request from 10.2.16.28 to 142.250.183.228 and a reply from 142.250.183.228 to 10.2.16.28. The packet details pane shows the ICMP Echo (ping) reply with Type 0, Code 0, Checksum 0x5556, Identifier 1, and Sequence Number 5. The packet bytes pane shows the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
3421	15.130747	10.2.16.28	142.250.183.228	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 3436)
3436	15.144240	142.250.183.228	10.2.16.28	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=118 (request in 3421)
3681	16.143059	10.2.16.28	142.250.183.228	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 3684)
3684	16.156204	142.250.183.228	10.2.16.28	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=118 (request in 3681)
3958	17.146563	10.2.16.28	142.250.183.228	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (no response found!)
5389	21.719663	10.2.16.28	142.250.183.228	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (no response found!)

Frame 3436: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{149AA54B-F72F-4FA9-92FD-52EABE47000A}, id 0
 Ethernet II, Src: Sophos_fc:00:10 (c8:4f:86:fc:00:10), Dst: AzureWaveTec_17:5e:9b (14:d4:24:17:5e:9b)
 Internet Protocol Version 4, Src: 142.250.183.228, Dst: 10.2.16.28
 Internet Control Message Protocol
 Type: 0 (Echo (ping) reply)
 Code: 0
 Checksum: 0x5556 [correct]
 [Checksum Status: Good]
 Identifier (BE): 1 (0x0001)
 Identifier (LE): 256 (0x0100)
 Sequence Number (BE): 5 (0x0005)
 Sequence Number (LE): 1280 (0x0500)
 [Request frame: 3421]
 [Response time: 13.493 ms]
 Data (32 bytes)

Internet Control Message Protocol: Protocol | Packets: 8777 - Displayed: 6 (0.1%) - Dropped: 0 (0.0%) | Profile: Default

Paste the Wireshark File with view permission:

Google Drive Link:

https://drive.google.com/file/d/1uWQcuBJXNYw2RQl4yHc0uvAcJpKBHDeq/view?usp=drive_link

Rubrics for Wireshark labs: (To be Filled by the Class Teacher)

Rubrics	Excellent	Fair	Poor	Marks
Understanding (2)	Understand the Concept very well. (2)	Understand the Concept (1)	Poor Understand the Concept (0)	
Usage of filters (3)	Identified and applied the filter correctly (3)	Identified the filter, but not applied correctly (2-1)	Couldn't identify and apply the filter. Just captured the packets (1)	
Attach relevant Screenshots (3)	clearly Highlighted the answers and attached the screenshots (3)	attached the screenshots, but not highlighted. (2-1)	Did not attach the screenshots (0)	
On time Submission (2)	Early or on time submission (2)	Submitted after deadline (1)	Did not Submit (0)	
Total				