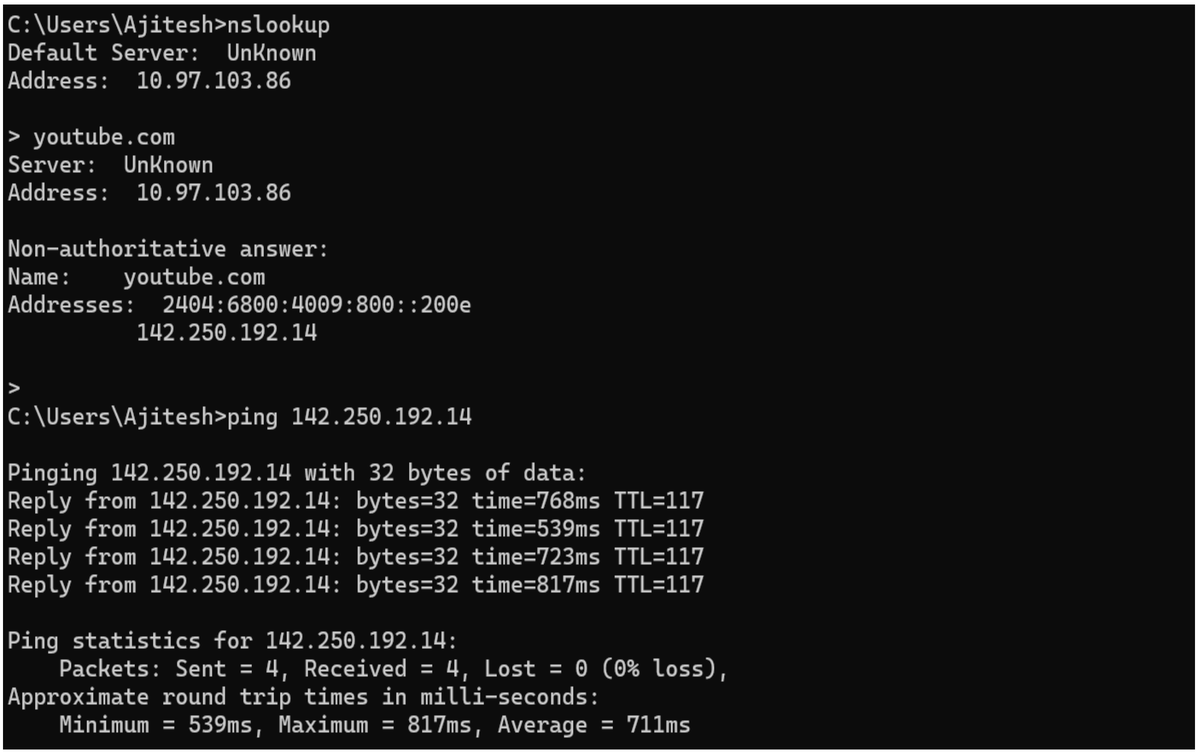
Practical – 7

Aim of the Practical: To analyze network traffic using Wireshark – capture ICMP packets and study their header fields.

Observation and Analysis:

Ping – Part I

Figure 1: This image captures a Command Prompt session where the ping utility is used to test network connectivity to IP address 142.250.192.14. The output shows four successful replies from the IP address, along with the round-trip time for each packet.



```
C:\Users\Ajitesh>nslookup
Default Server:  UnKnown
Address:  10.97.103.86

> youtube.com
Server:  UnKnown
Address:  10.97.103.86

Non-authoritative answer:
Name:    youtube.com
Addresses:  2404:6800:4009:800::200e
          142.250.192.14

>
C:\Users\Ajitesh>ping 142.250.192.14

Pinging 142.250.192.14 with 32 bytes of data:
Reply from 142.250.192.14: bytes=32 time=768ms TTL=117
Reply from 142.250.192.14: bytes=32 time=539ms TTL=117
Reply from 142.250.192.14: bytes=32 time=723ms TTL=117
Reply from 142.250.192.14: bytes=32 time=817ms TTL=117

Ping statistics for 142.250.192.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 539ms, Maximum = 817ms, Average = 711ms
```

1.	Destination IP address:	142.250.192.14
2.	Number of ping messages sent:	4
3.	Number of bytes of data sent with each ping message:	32 bytes

<table>
<tr><td>4.</td><td>Round-trip time for each packet:</td><td><table><tr><td>Packet 1</td><td>768ms</td></tr><tr><td>Packet 2</td><td>539ms</td></tr><tr><td>Packet 3</td><td>723ms</td></tr><tr><td>Packet 4</td><td>817ms</td></tr></table></td></tr>
<tr><td>5</td><td>Minimum round-trip:
Average round-trip:
Maximum round-trip:</td><td>Minimum = 539ms,
Average = 711ms,
Maximum = 817ms</td></tr>
</table>

The ping command was executed to test network connectivity and measure latency to the destination IP address 142.250.192.14. The results from this test indicate a successful connection, as all four ICMP Echo Request packets that were sent received a corresponding reply, resulting in **0% packet loss**. This outcome demonstrates a reliable and stable network path to the host. However, the analysis of the Round-Trip Time (RTT) statistics points to significant network delay. The average RTT was recorded at **711ms**, with individual packet times fluctuating between a minimum of **539ms** and a maximum of **817ms**. This high average latency, coupled with the variance between the RTT values, suggests that while the connection is stable, it is affected by factors such as network congestion or considerable physical distance to the destination server.

Ping – Part II

1.	Destination IP address of Echo Request ICMP messages: Does the result agree with Part I?	142.250.192.14 Yes, this matches the IP address used in the ping command.
2.	Number of Echo Request ICMP packets: Number of Echo Reply ICMP packets: Does the result agree with Part I?	4 Echo Request 4 Echo Reply Yes
3.	Number of bytes of data carried by each ICMP packet: Does the result agree with Part I?	32 bytes Yes
4.	Difference between the time the first Echo message was sent and the first reply message was received:	Request Time = 25.962984 Response Time = 26.731600 Difference = 0.768616
5.	Fields that are same in Echo Request and Echo Reply: Reason:	Identifier, Sequence Number, and Data These fields are kept identical so the source host can match a specific incoming reply to the original request it sent. The Identifier and Sequence Number act as a unique session tracker, and the Data is echoed back to confirm integrity.
6.	Fields that are different in Echo Request and Echo Reply: Reason:	Type and Checksum The Type field must change from 8 (Echo Request) to 0 (Echo Reply) to distinguish the query from the response. The Checksum is recalculated by the replying host because the ICMP header content (specifically the Type field) has changed.

Explanations:

1. Destination IP address of Echo Request ICMP messages:

Does the result agree with Part I?

Ans: The destination IP address for the ICMP Echo Request messages was identified as 142.250.192.14 in the Wireshark capture.

This address matches the one used in the executed ping command, confirming that the captured traffic corresponds directly to the network test that was performed.

2. Number of Echo Request ICMP packets:

Number of Echo Reply ICMP packets:

Does the result agree with Part I?

Ans: The Wireshark capture log shows a total of **four ICMP Echo Request packets** being sent from the source and **four ICMP Echo Reply packets** being returned from the destination.

This one-to-one correspondence perfectly matches the “Ping statistics” from the command prompt, which reported **Sent = 4, Received = 4**. This indicates a successful and reliable connection during the test, with **0% packet loss**. The observation of four packets is consistent with the default behaviour of the ping command on the Windows operating system.

3. Number of bytes of data carried by each ICMP packet:

Does the result agree with Part I?

The ping command was initiated with a data payload of 32 bytes. Analysis of the ICMP packet details in Wireshark confirms that both the Echo Request and Echo Reply messages contained a data section with a length of 32 bytes. This payload is echoed by the destination host to verify the integrity of the data path.

4. Difference between the time the first Echo message was sent and the first reply message was received:

Ans: Time of first Echo Request packet sent: 25.962984 s

Time of first Echo Reply packet received: 26.731600 s

The calculation is as follows: 26.731600 s - 25.962984 s = 0.768616 s

5. Fields that are same in Echo Request and Echo Reply:

Reason:

Ans: The fields that remain unchanged between the Echo Request and its corresponding Echo Reply are the **Identifier**, the **Sequence Number**, and the **Data** payload.

Reason: These fields are kept consistent for tracking and validation.

- **Identifier:** This field acts like a conversation ID. The value (0x0001 in this case) remains constant for all packets within a single ping session, allowing the operating system to associate incoming replies with the correct originating process.
- **Sequence Number:** This number is incremented for each new request sent. The destination server copies this number directly into its reply. This allows the source to match each reply to its specific request, which is essential for calculating individual RTTs and detecting out-of-order or lost packets.
- **Data:** The 32-byte payload is mirrored exactly to fulfil the echo function of the protocol, verifying that data can be transmitted and returned without being altered.

6. Fields that are different in Echo Request and Echo Reply:

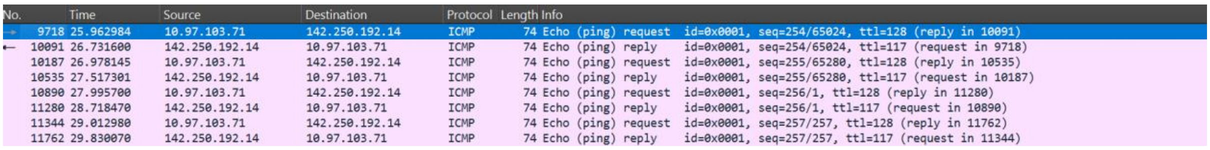
Reason:

Ans: The fields that are necessarily different are the **Type** and the **Checksum**.

Reason:

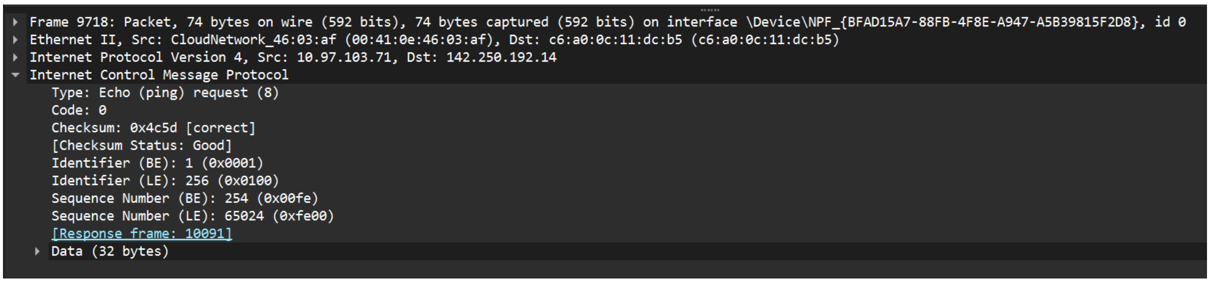
- **Type:** This is the most fundamental change. The request packet uses **Type 8** to signal an "Echo Request". The replying host must change this value to **Type 0** to signify an "Echo Reply". This code change is what defines the packet as a response rather than another query.
- **Checksum:** This is an error-detection field calculated based on the contents of the ICMP message. Because a key value in the header (the Type field) was changed from 8 to 0, the original checksum is no longer valid. Therefore, the replying host must recalculate a new checksum for the reply packet. The captured packets show two different checksums: 0x4c5a for the request and 0x545d for the reply.

Figure 2: This screenshot shows the Wireshark packet list pane, displaying a filtered view of ICMP traffic. It illustrates the conversation between two hosts, showing a sequence of four Echo Request packets and their corresponding Echo Reply packets.



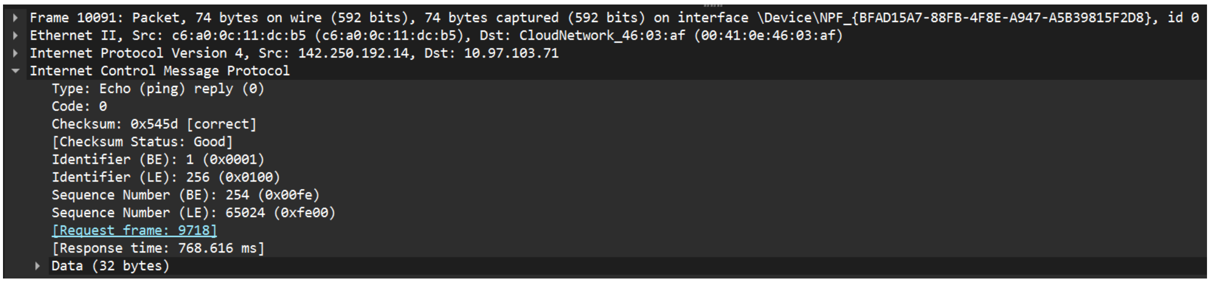
```
No.     Time        Source          Destination     Protocol Length Info
→  9718 25.962984   10.97.103.71    142.250.192.14  ICMP      74 Echo (ping) request  id=0x0001, seq=254/65024, ttl=128 (reply in 10091)
← 10091 26.731600   142.250.192.14  10.97.103.71    ICMP      74 Echo (ping) reply    id=0x0001, seq=254/65024, ttl=117 (request in 9718)
  10187 26.978145   10.97.103.71    142.250.192.14  ICMP      74 Echo (ping) request  id=0x0001, seq=255/65280, ttl=128 (reply in 10535)
  10535 27.517301   142.250.192.14  10.97.103.71    ICMP      74 Echo (ping) reply    id=0x0001, seq=255/65280, ttl=117 (request in 10187)
  10890 27.995700   10.97.103.71    142.250.192.14  ICMP      74 Echo (ping) request  id=0x0001, seq=256/1, ttl=128 (reply in 11280)
  11280 28.718470   142.250.192.14  10.97.103.71    ICMP      74 Echo (ping) reply    id=0x0001, seq=256/1, ttl=117 (request in 10890)
  11344 29.012980   10.97.103.71    142.250.192.14  ICMP      74 Echo (ping) request  id=0x0001, seq=257/257, ttl=128 (reply in 11762)
  11762 29.830070   142.250.192.14  10.97.103.71    ICMP      74 Echo (ping) reply    id=0x0001, seq=257/257, ttl=117 (request in 11344)
```

Figure 3: This image displays the detailed breakdown of an ICMP Echo Request packet (Frame 9718) as captured in Wireshark.



```
▸ Frame 9718: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{BFAD15A7-88FB-4F8E-A947-A5B39815F2D8}, id 0
▸ Ethernet II, Src: CloudNetwork_46:03:af (00:41:0e:46:03:af), Dst: c6:a0:0c:11:dc:b5 (c6:a0:0c:11:dc:b5)
▸ Internet Protocol Version 4, Src: 10.97.103.71, Dst: 142.250.192.14
▾ Internet Control Message Protocol
    Type: Echo (ping) request (8)
    Code: 0
    Checksum: 0x4c5d [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 254 (0x00fe)
    Sequence Number (LE): 65024 (0xfe00)
    [Response frame: 10091]
  ▸ Data (32 bytes)
```

Figure 4: This figure provides a detailed view of an ICMP Echo Reply packet from the Wireshark capture.



```
▸ Frame 10091: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{BFAD15A7-88FB-4F8E-A947-A5B39815F2D8}, id 0
▸ Ethernet II, Src: c6:a0:0c:11:dc:b5 (c6:a0:0c:11:dc:b5), Dst: CloudNetwork_46:03:af (00:41:0e:46:03:af)
▸ Internet Protocol Version 4, Src: 142.250.192.14, Dst: 10.97.103.71
▾ Internet Control Message Protocol
    Type: Echo (ping) reply (0)
    Code: 0
    Checksum: 0x545d [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 254 (0x00fe)
    Sequence Number (LE): 65024 (0xfe00)
    [Request frame: 9718]
    [Response time: 768.616 ms]
  ▸ Data (32 bytes)
```

Conclusion

This lab successfully demonstrated the relationship between the ping command and the ICMP protocol by capturing and analyzing network traffic with Wireshark. The experiment confirmed that ping functions by exchanging ICMP Echo Request (Type 8) and Echo Reply (Type 0) packets, resulting in a successful test with 0% packet loss but a high average latency of 711ms to the host 142.250.192.14. Detailed packet inspection revealed the core mechanics of ICMP: the Identifier and Sequence Number were mirrored to correlate the request and reply, while the Type field was changed from 8 to 0 and the Checksum was recalculated to form a valid response. Ultimately, the lab fulfilled all its objectives by providing a practical understanding of how ICMP header fields are used for network diagnostics, effectively bridging the gap between theory and real-world application.