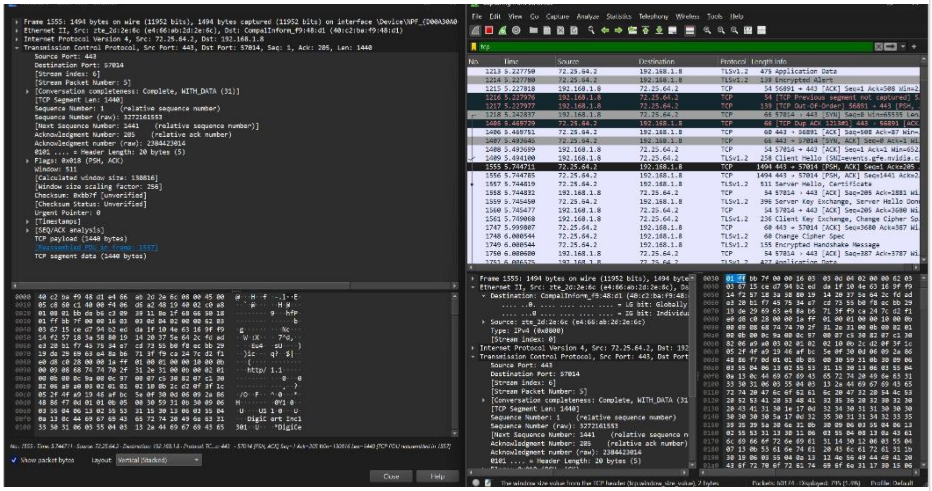
Experiment No: 12	
Name	Suyash Tambe
PRN	22070126117
Date of Performance	
Title	Implement and analyse TCP and ICMP protocols using Wireshark
Objective	The goal of this exercise is to use Wireshark to collect and analyze TCP and ICMP packets. The experiment tries to better understand the structure and behavior of various protocols during network communication.
Setup	• Wireshark was installed and configured to monitor the Ethernet interface. • The focus was on capturing **TCP** and **ICMP** traffic, applying respective filters in Wireshark.

Procedure	**Step 1: Capturing TCP Packets** 1. A packet capture session was initiated on the Ethernet interface. 2. **TCP** filters were applied to narrow the capture to TCP traffic. 3. A TCP connection to a web server (port 443) was established, capturing the packets exchanged during the session. **Step 2: Capturing ICMP Packets** 1. A new capture session was started, and the **ICMP** filter was applied. 2. **Ping** commands were issued to a remote server (www.google.com) to generate ICMP Echo Requests and Responses.

Analysis	TCP Packet Analysis • **Frame 1555** represents a **TCP segment** associated with encrypted application data over **TLSv1.2** • Source IP: 72.25.64.2 • Destination IP: 192.168.1.8 • Source Port: 443 (HTTPS) • Destination Port: 57014 (Client) • TCP Flags: PSH, ACK • Window Size: 130816 • Sequence Number: 3727216553 • Acknowledgment Number: 2348424014 • Payload Length: 1440 bytes ICMP Packet Analysis • **Frame 52** represents an **ICMP Echo Request** packet sent during a ping • Source IP: 2404:6800:4009:824::2004 (Google Server) • Destination IP: 2409:40e2:102d:c3d3:49e2:37cf:2c0b (Local Machine) • Protocol: ICMPv6 • Ping Request ID: 0x0001 • Sequence Number: 7 • ICMP Data: 32 bytes • The response (Frame 53) was received, confirming successful communication with a round-trip time of 39ms.

Screenshots

1. TCP



```
▸ Frame 1555: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface \Device\NPF_{D00A30A0
▸ Ethernet II, Src: zte_2d:2e:6c (e4:66:ab:2d:2e:6c), Dst: CompalInform_f9:48:d1 (40:c2:ba:f9:48:d1)
▸ Internet Protocol Version 4, Src: 72.25.64.2, Dst: 192.168.1.8
▾ Transmission Control Protocol, Src Port: 443, Dst Port: 57014, Seq: 1, Ack: 205, Len: 1440
    Source Port: 443
    Destination Port: 57014
    [Stream index: 6]
    [Stream Packet Number: 5]
  ▸ [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 1440]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3272161553
    [Next Sequence Number: 1441    (relative sequence number)]
    Acknowledgment Number: 205    (relative ack number)
    Acknowledgment number (raw): 2384423014
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x018 (PSH, ACK)
    Window: 511
    [Calculated window size: 130816]
    [Window size scaling factor: 256]
    Checksum: 0xbb7f [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
    TCP payload (1440 bytes)
    [Reassembled PDU in frame: 1557]
    TCP segment data (1440 bytes)

0000  40 c2 ba f9 48 d1 e4 66  ab 2d 2e 6c 08 00 45 00   @··H··f ·-.l··E·
0010  05 c8 60 c1 40 00 f4 06  d6 a2 48 19 40 02 c0 a8   ··`·@··· ··H·@···
0020  01 08 01 bb de b6 c3 09  39 11 8e 1f 68 66 50 18   ········ 9···hfP·
0030  01 ff bb 7f 00 00 16 03  03 0d 04 02 00 00 62 03   ········ ······b·
0040  03 67 15 ce d7 94 b2 ed  da 1f 10 4e 63 16 9f f9   ·g······ ···Nc···
0050  14 f2 57 18 3a 58 80 19  14 20 37 5e 64 2c fd ad   ··W·:X·· · 7^d,··
0060  e3 20 b1 f7 45 75 34 e7  cd 73 55 b0 f8 ec bb 29   · ··Eu4· ·sU····)
0070  19 de 29 69 63 e4 8a b6  71 3f f9 ca 24 7c d2 f1   ··)ic··· q?··$|··
0080  e0 d8 c0 28 00 00 1a ff  01 00 01 00 00 10 00 0b   ···(···· ········
0090  00 09 08 68 74 74 70 2f  31 2e 31 00 0b 00 02 01   ···http/ 1.1·····
00a0  00 0b 00 0c 9a 00 0c 97  00 07 c5 30 82 07 c1 30   ········ ···0···0
00b0  82 06 a9 a0 03 02 01 02  02 10 0b 2c d2 0f 3f 1c   ········ ···,··?·
00c0  05 2f 4f a9 19 46 af bc  5e 0f 30 0d 06 09 2a 86   ·/O··F·· ^·0···*·
00d0  48 86 f7 0d 01 01 0b 05  00 30 59 31 0b 30 09 06   H······· ·0Y1·0··
00e0  03 55 04 06 13 02 55 53  31 15 30 13 06 03 55 04   ·U····US 1·0···U·
00f0  0a 13 0c 44 69 67 69 43  65 72 74 20 49 6e 63 31   ···DigiC ert Inc1
0100  33 30 31 06 03 55 04 03  13 2a 44 69 67 69 43 65   301··U·· ·*DigiCe
```

No.: 1555 · Time: 5.744711 · Source: 72.25.64.2 · Destination: 192.168.1.8 · Protocol: TC... 443 → 57014 [PSH, ACK] Seq=1 Ack=205 Win=130816 Len=1440 [TCP PDU reassembled in 1557]

☑ Show packet bytes   Layout: Vertical (Stacked)

Close
Help
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

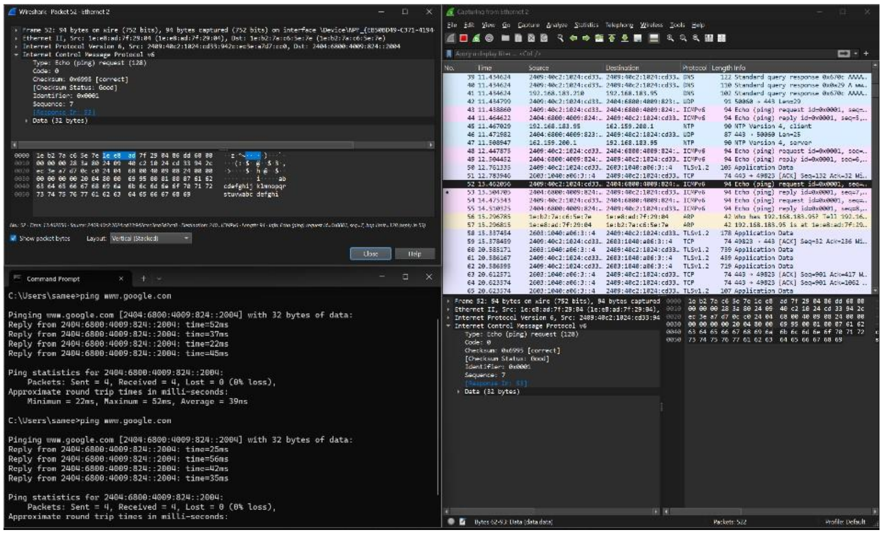
```
No.   Time      Source        Destination   Protocol Length Info
1213 5.227750  72.25.64.2    192.168.1.8   TLSv1.2   475 Application Data
1214 5.227780  72.25.64.2    192.168.1.8   TLSv1.2   139 Encrypted Alert
1215 5.227818  192.168.1.8   72.25.64.2    TCP        54 56891 → 443 [ACK] Seq=1 Ack=508 Win=2
1216 5.227976  192.168.1.8   72.25.64.2    TCP        54 [TCP Previous segment not captured] 5
1217 5.227977  192.168.1.8   72.25.64.2    TCP       139 [TCP Out-Of-Order] 56891 → 443 [PSH,
1218 5.242837  192.168.1.8   72.25.64.2    TCP        66 57014 → 443 [SYN] Seq=0 Win=65535 Len
1405 5.469729  72.25.64.2    192.168.1.8   TCP        66 [TCP Dup ACK 1213#1] 443 → 56891 [ACK
1406 5.469751  72.25.64.2    192.168.1.8   TCP        60 443 → 56891 [ACK] Seq=508 Ack=87 Win=
1407 5.493645  72.25.64.2    192.168.1.8   TCP        66 443 → 57014 [SYN, ACK] Seq=0 Ack=1 Wi
1408 5.493699  192.168.1.8   72.25.64.2    TCP        54 57014 → 443 [ACK] Seq=1 Ack=1 Win=652
1409 5.494100  192.168.1.8   72.25.64.2    TLSv1.2   258 Client Hello (SNI=events.gfe.nvidia.c
1555 5.744711  72.25.64.2    192.168.1.8   TCP      1494 443 → 57014 [PSH, ACK] Seq=1 Ack=205
1556 5.744785  72.25.64.2    192.168.1.8   TCP      1494 443 → 57014 [PSH, ACK] Seq=1441 Ack=2
1557 5.744819  72.25.64.2    192.168.1.8   TLSv1.2   511 Server Hello, Certificate
1558 5.744832  192.168.1.8   72.25.64.2    TCP        54 57014 → 443 [ACK] Seq=205 Ack=2881 Wi
1559 5.745450  72.25.64.2    192.168.1.8   TLSv1.2   396 Server Key Exchange, Server Hello Don
1560 5.745477  192.168.1.8   72.25.64.2    TCP        54 57014 → 443 [ACK] Seq=205 Ack=3680 Wi
1561 5.749068  192.168.1.8   72.25.64.2    TLSv1.2   236 Client Key Exchange, Change Cipher Sp
1747 5.999807  72.25.64.2    192.168.1.8   TCP        60 443 → 57014 [ACK] Seq=3680 Ack=387 Wi
1748 6.000544  72.25.64.2    192.168.1.8   TLSv1.2    60 Change Cipher Spec
1749 6.000544  72.25.64.2    192.168.1.8   TLSv1.2   155 Encrypted Handshake Message
1750 6.000600  192.168.1.8   72.25.64.2    TCP        54 57014 → 443 [ACK] Seq=387 Ack=3787 Wi
1751 6.006575  192.168.1.8   72.25.64.2    TLSv1.2   427 Application Data
```

```
▸ Frame 1555: 1494 bytes on wire (11952 bits), 1494 byte
▾ Ethernet II, Src: zte_2d:2e:6c (e4:66:ab:2d:2e:6c), Ds
  ▾ Destination: CompalInform_f9:48:d1 (40:c2:ba:f9:48:
      .... ..0. .... .... .... .... = LG bit: Globally
      .... ...0 .... .... .... .... = IG bit: Individu
  ▸ Source: zte_2d:2e:6c (e4:66:ab:2d:2e:6c)
    Type: IPv4 (0x0800)
    [Stream index: 0]
▸ Internet Protocol Version 4, Src: 72.25.64.2, Dst: 192
▾ Transmission Control Protocol, Src Port: 443, Dst Port
    Source Port: 443
    Destination Port: 57014
    [Stream index: 6]
    [Stream Packet Number: 5]
  ▸ [Conversation completeness: Complete, WITH_DATA (31
    [TCP Segment Len: 1440]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3272161553
    [Next Sequence Number: 1441    (relative sequence n
    Acknowledgment Number: 205    (relative ack number)
    Acknowledgment number (raw): 2384423014
    0101 .... = Header Length: 20 bytes (5)

0030  01 ff bb 7f 00 00 16 03  03 0d 04 02 00 00 62 03
0040  03 67 15 ce d7 94 b2 ed  da 1f 10 4e 63 16 9f f9
0050  14 f2 57 18 3a 58 80 19  14 20 37 5e 64 2c fd ad
0060  e3 20 b1 f7 45 75 34 e7  cd 73 55 b0 f8 ec bb 29
0070  19 de 29 69 63 e4 8a b6  71 3f f9 ca 24 7c d2 f1
0080  e0 d8 c0 28 00 00 1a ff  01 00 01 00 00 10 00 0b
0090  00 09 08 68 74 74 70 2f  31 2e 31 00 0b 00 02 01
00a0  00 0b 00 0c 9a 00 0c 97  00 07 c5 30 82 07 c1 30
00b0  82 06 a9 a0 03 02 01 02  02 10 0b 2c d2 0f 3f 1c
00c0  05 2f 4f a9 19 46 af bc  5e 0f 30 0d 06 09 2a 86
00d0  48 86 f7 0d 01 01 0b 05  00 30 59 31 0b 30 09 06
00e0  03 55 04 06 13 02 55 53  31 15 30 13 06 03 55 04
00f0  0a 13 0c 44 69 67 69 43  65 72 74 20 49 6e 63 31
0100  33 30 31 06 03 55 04 03  13 2a 44 69 67 69 43 65
0110  72 74 20 47 6c 6f 62 61  6c 20 47 32 20 54 4c 53
0120  20 52 53 41 20 53 48 41  32 35 36 20 32 30 32 30
0130  20 43 41 31 30 1e 17 0d  32 34 30 31 31 30 30 30
0140  30 30 30 30 5a 17 0d 32  35 30 31 31 34 32 33 35
0150  39 35 39 5a 30 6e 31 0b  30 09 06 03 55 04 06 13
0160  02 55 53 31 13 30 11 06  03 55 04 08 13 0a 43 61
0170  6c 69 66 6f 72 6e 69 61  31 14 30 12 06 03 55 04
0180  07 13 0b 53 61 6e 74 61  20 43 6c 61 72 61 31 1b
0190  30 19 06 03 55 04 0a 13  12 4e 56 49 44 49 41 20
01a0  43 6f 72 70 6f 72 61 74  69 6f 6e 31 17 30 15 06
```

The window size value from the TCP header (tcp.window_size_value), 2 bytes   Packets: 60174 · Displayed: 795 (1.3%)   Profile: Default

2. ICMP



Wireshark · Packet 52 · Ethernet 2

```
▸ Frame 52: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF_{CB500D49-C371-4194
▸ Ethernet II, Src: 1e:e8:ad:7f:29:04 (1e:e8:ad:7f:29:04), Dst: 1e:b2:7a:c6:5e:7e (1e:b2:7a:c6:5e:7e)
▸ Internet Protocol Version 6, Src: 2409:40c2:1024:cd33:942c:ec3e:a7d7:cc0, Dst: 2404:6800:4009:824::2004
▾ Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
    Code: 0
    Checksum: 0x6995 [correct]
    [Checksum Status: Good]
    Identifier: 0x0001
    Sequence: 7
    [Response In: 53]
  ▸ Data (32 bytes)

0000  1e b2 7a c6 5e 7e 1e e8  ad 7f 29 04 86 dd 60 00   ··z·^~·· ··)···`·
0010  00 00 00 28 3a 80 24 09  40 c2 10 24 cd 33 94 2c   ···(:·$· @··$·3·,
0020  ec 3e a7 d7 0c c0 24 04  68 00 40 09 08 24 00 00   ·>····$· h·@··$··
0030  00 00 00 00 20 04 80 00  69 95 00 01 00 07 61 62   ···· ··· i·····ab
0040  63 64 65 66 67 68 69 6a  6b 6c 6d 6e 6f 70 71 72   cdefghij klmnopqr
0050  73 74 75 76 77 61 62 63  64 65 66 67 68 69         stuvwabc defghi
```

☑ Show packet bytes   Layout: Vertical (Stacked)

```
C:\Users\samee>ping www.google.con

Pinging www.google.com [2404:6800:4009:824::2004] with 32 bytes of data:
Reply from 2404:6800:4009:824::2004: time=52ms
Reply from 2404:6800:4009:824::2004: time=37ms
Reply from 2404:6800:4009:824::2004: time=22ms
Reply from 2404:6800:4009:824::2004: time=45ms

Ping statistics for 2404:6800:4009:824::2004:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 22ms, Maximum = 52ms, Average = 39ms

C:\Users\samee>ping www.google.con

Pinging www.google.com [2404:6800:4009:824::2004] with 32 bytes of data:
Reply from 2404:6800:4009:824::2004: time=25ms
Reply from 2404:6800:4009:824::2004: time=56ms
Reply from 2404:6800:4009:824::2004: time=42ms
Reply from 2404:6800:4009:824::2004: time=35ms

Ping statistics for 2404:6800:4009:824::2004:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

Capturing from Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No. Time       Source                Destination           Protocol Length Info
39 11.434624  2409:40c2:1024:cd33…  2409:40c2:1024:cd33…  DNS       122 Standard query response 0x670c AAAA…
40 11.434624  2409:40c2:1024:cd33…  2409:40c2:1024:cd33…  DNS       130 Standard query response 0x0e29 A www…
41 11.434624  192.168.183.210       192.168.183.95        DNS       102 Standard query response 0x670c AAAA…
42 11.434799  2409:40c2:1024:cd33…  2404:6800:4009:823:…  UDP        91 50060 → 443 Len=29
43 11.438860  2409:40c2:1024:cd33…  2404:6800:4009:824:…  ICMPv6     94 Echo (ping) request id=0x0001, seq=…
44 11.464622  2404:6800:4009:824:…  2409:40c2:1024:cd33…  ICMPv6     94 Echo (ping) reply id=0x0001, seq=5,…
45 11.467029  192.168.183.95        162.159.200.1         NTP        90 NTP Version 4, client
46 11.471982  2404:6800:4009:823:…  2409:40c2:1024:cd33…  UDP        87 443 → 50060 Len=25
47 11.508947  162.159.200.1         192.168.183.95        NTP        90 NTP Version 4, server
48 12.447875  2409:40c2:1024:cd33…  2404:6800:4009:824:…  ICMPv6     94 Echo (ping) request id=0x0001, seq=…
49 12.504452  2404:6800:4009:824:…  2409:40c2:1024:cd33…  ICMPv6     94 Echo (ping) reply id=0x0001, seq=6,…
50 12.761335  2409:40c2:1024:cd33…  2603:1040:a06:3::4     TLSv1.2   105 Application Data
51 12.783946  2603:1040:a06:3::4     2409:40c2:1024:cd33…  TCP        74 443 → 49823 [ACK] Seq=132 Ack=32 Wi…
52 13.462056  2409:40c2:1024:cd33…  2404:6800:4009:824:…  ICMPv6     94 Echo (ping) request id=0x0001, seq=…
53 13.504705  2404:6800:4009:824:…  2409:40c2:1024:cd33…  ICMPv6     94 Echo (ping) reply id=0x0001, seq=7,…
54 14.475343  2409:40c2:1024:cd33…  2404:6800:4009:824:…  ICMPv6     94 Echo (ping) request id=0x0001, seq=…
55 14.510325  2404:6800:4009:824:…  2409:40c2:1024:cd33…  ICMPv6     94 Echo (ping) reply id=0x0001, seq=8,…
56 15.296785  1e:b2:7a:c6:5e:7e      1e:e8:ad:7f:29:04      ARP        42 Who has 192.168.183.95? Tell 192.16…
57 15.296815  1e:e8:ad:7f:29:04      1e:b2:7a:c6:5e:7e      ARP        42 192.168.183.95 is at 1e:e8:ad:7f:29…
58 15.337454  2603:1040:a06:3::4     2409:40c2:1024:cd33…  TLSv1.2   178 Application Data
59 15.378459  2409:40c2:1024:cd33…  2603:1040:a06:3::4     TCP        74 49823 → 443 [ACK] Seq=32 Ack=236 Wi…
60 20.585171  2603:1040:a06:3::4     2409:40c2:1024:cd33…  TLSv1.2   739 Application Data
61 20.586167  2409:40c2:1024:cd33…  2603:1040:a06:3::4     TLSv1.2   439 Application Data
62 20.586595  2409:40c2:1024:cd33…  2603:1040:a06:3::4     TLSv1.2   719 Application Data
63 20.612571  2603:1040:a06:3::4     2409:40c2:1024:cd33…  TCP        74 443 → 49823 [ACK] Seq=901 Ack=417 W…
64 20.623374  2603:1040:a06:3::4     2409:40c2:1024:cd33…  TCP        74 443 → 49823 [ACK] Seq=901 Ack=1062 …
65 20.623374  2603:1040:a06:3::4     2409:40c2:1024:cd33…  TLSv1.2   107 Application Data
```

```
▸ Frame 52: 94 bytes on wire (752 bits), 94 bytes captured
▸ Ethernet II, Src: 1e:e8:ad:7f:29:04 (1e:e8:ad:7f:29:04),
▸ Internet Protocol Version 6, Src: 2409:40c2:1024:cd33:94
▾ Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
    Code: 0
    Checksum: 0x6995 [correct]
    [Checksum Status: Good]
    Identifier: 0x0001
    Sequence: 7
    [Response In: 53]
  ▸ Data (32 bytes)

0000  1e b2 7a c6 5e 7e 1e e8  ad 7f 29 04 86 dd 60 00
0010  00 00 00 28 3a 80 24 09  40 c2 10 24 cd 33 94 2c
0020  ec 3e a7 d7 0c c0 24 04  68 00 40 09 08 24 00 00
0030  00 00 00 00 20 04 80 00  69 95 00 01 00 07 61 62
0040  63 64 65 66 67 68 69 6a  6b 6c 6d 6e 6f 70 71 72
0050  73 74 75 76 77 61 62 63  64 65 66 67 68 69
```

Bytes 62-93: Data (data.data)   Packets: 522   Profile: Default

Observation	The TCP packets were collected during an encrypted HTTPS session between a client and a server. The PSH and ACK flags were used to guarantee that data was transmitted and acknowledged properly. The ICMP packets were generated from ping requests, and responses confirmed connectivity and the average round-trip time (RTT) to the server was 39ms.
Self-assessment Q&A	NA
Conclusion	This experiment used Wireshark to explore both TCP and ICMP protocols. It explained how TCP manages reliable transmission and how ICMP may be used to diagnose network connection using ping. The capacity to collect and analyze packet structure, such as flags, sequence numbers, and headers, helped researchers better grasp these critical network protocols.