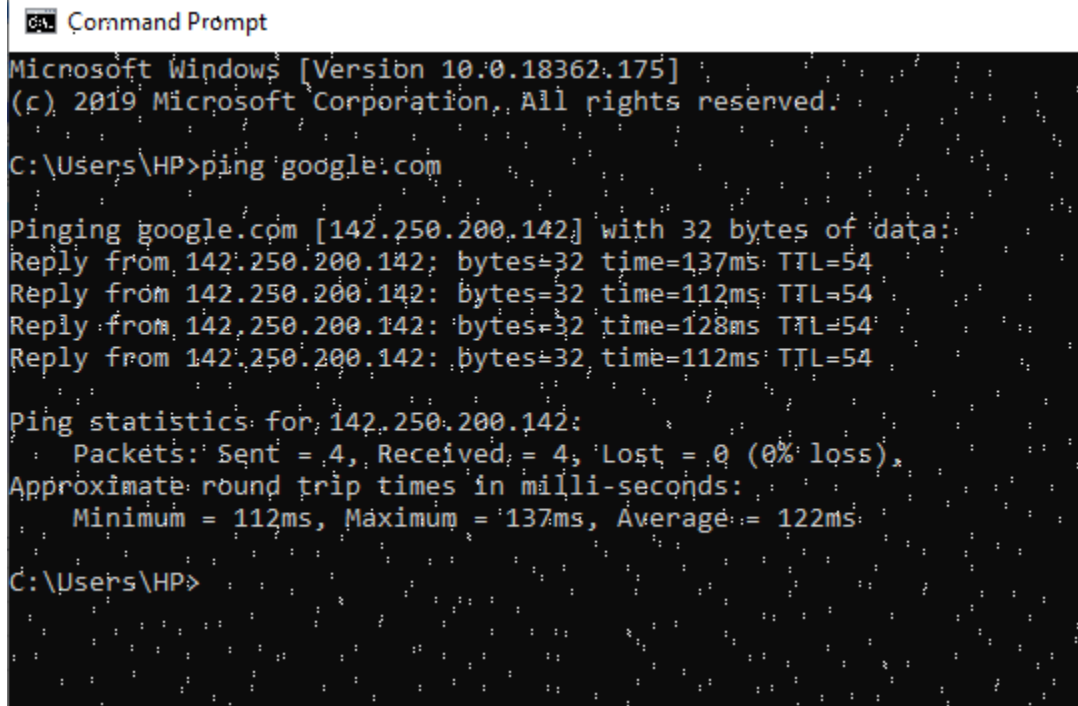


Performed ping google.com screenshot:



```
Command Prompt
Microsoft Windows [Version 10.0.18362.175]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\HP>ping google.com

Pinging google.com [142.250.200.142] with 32 bytes of data:
Reply from 142.250.200.142: bytes=32 time=137ms TTL=54
Reply from 142.250.200.142: bytes=32 time=112ms TTL=54
Reply from 142.250.200.142: bytes=32 time=128ms TTL=54
Reply from 142.250.200.142: bytes=32 time=112ms TTL=54

Ping statistics for 142.250.200.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 112ms, Maximum = 137ms, Average = 122ms

C:\Users\HP>
```

1. Choose the first ICMP request packet that you come across and answer the following questions:

a. What is the packet protocol and protocol number?

ICMP (1)

Wireshark · Packet 2890 · Wi-Fi

.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 60
Identification: 0xdeda (57050)
> 000. = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: ICMP (1)
Header Checksum: 0x1827 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.43.142
Destination Address: 142.250.200.142
> Internet Control Message Protocol

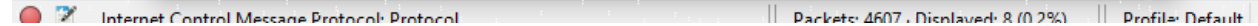
0000	f6 67 28 8f 3d 29 08 11 96 47 d7 c0 08 00 45 00	·g(·=)· ·G····E·
0010	00 3c de da 00 00 80 01 18 27 c0 a8 2b 8e 8e fa	·<······ ·'·+··
0020	c8 8e 08 00 4c ce 00 01 00 8d 61 62 63 64 65 66	····L···· ··abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69	wabdefg hi

No.: 2890 · Time: 24.003541 · Source: 192.168.43.142 · Destination: 142.2...a: Echo (ping) request id=0x0001, seq=141/36096, ttl=128 (reply in 2912)

☒ Show packet bytes

Close Help

8 (Echo (ping) request) code: 0



c. What is the checksum number and status?

0x4cce status: Good

The image shows a Wireshark packet capture window titled "Wireshark · Packet 2890 · unit 5.pcapng". The packet list on the left shows packet 2890 selected. The packet details pane shows the following information:

- Destination Address: 142.250.200.142
- Internet Control Message Protocol
 - Type: 8 (Echo (ping) request)
 - Code: 0
 - Checksum: 0x4cce [correct] **0x4cce**
 - [Checksum Status: Good] **Good**
 - Identifier (BE): 1 (0x0001)
 - Identifier (LE): 256 (0x0100)
 - Sequence Number (BE): 141 (0x008d)
 - Sequence Number (LE): 36096 (0x8d00)
 - [Response frame: 2912]
- Data (32 bytes)

The packet bytes pane shows the following data:

Offset	Hex	ASCII
0000	f6 67 28 8f 3d 29 08 11 96 47 d7 c0 08 00 45 00	g(=)G...E.
0010	00 3c de da 00 00 80 01 18 27 c0 a8 2b 8e 8e fa	<.....+...
0020	c8 8e 08 00 4c ce 00 01 00 8d 61 62 63 64 65 66	...L...abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69	wabcdefg hi

At the bottom of the packet details pane, the following information is displayed:

No.: 2890 · Time: 24.003541 · Source: 132.168.43.142 · Destination: 142.250.200.142 · Echo (ping) request id=0x0001, seq=141/36096, ttl=128 (reply in 2912)

The "Show packet bytes" checkbox is checked. The "Close" and "Help" buttons are visible at the bottom right of the packet details pane.

2. Examine the corresponding ICMP reply packet and answer the following questions:

d. What type and code number values do the ICMP packets have?

0 (Echo (ping) reply) code: 0

Wireshark · Packet 2912 · unit 5.pcapng

Internet Control Message Protocol

- Type: 0 (Echo (ping) reply)
- Code: 0
- Checksum: 0x54ce [correct]
[Checksum Status: Good]
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence Number (BE): 141 (0x008d)
- Sequence Number (LE): 36096 (0x8d00)

0000	08 11 96 47 d7 c0 f6 67 28 8f 3d 29 08 00 45 00	...G...g (=)...E...
0010	00 3c 00 00 00 00 36 01 41 02 8e fa c8 8e c0 a8	<...6...A.....
0020	2b 8e 00 00 54 ce 00 01 00 8d 61 62 63 64 65 66	+...T... ..abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn'opqrstuv
0040	77 61 62 63 64 65 66 67 68 69	wabcdefg hi

No.: 2912 · Time: 24.140685 · Source: 142.250.200.142 · Destination: 192.1...a: Echo (ping) reply id=0x0001, seq=141/36096, ttl=54 (request in 2890)

☒ Show packet bytes

Close Help

e. How many bytes are the checksum and identifier fields?

They are 6 bytes each

Wireshark · Packet 2912 · unit 5.pcapng

Internet Control Message Protocol

- Type: 0 (Echo (ping) reply)
- Code: 0
- Checksum: 0x54ce [correct]
- [Checksum Status: Good]
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence Number (BE): 141 (0x008d)
- Sequence Number (LE): 36096 (0x8d00)
- [\[Request frame: 2890\]](#)
- [Response time: 137.144 ms]
- > Data (32 bytes)

0000	08 11 96 47 d7 c0 f6 67 28 8f 3d 29 08 00 45 00	...G...g (=) ..E.
0010	00 3c 00 00 00 00 36 01 41 02 8e fa c8 8e c0 a8	...<...6..A.....
0020	2b 8e 00 00 54 ce 00 01 00 8d 61 62 63 64 65 66	+...T... ..abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69	wabcdefgh.hi

No.: 2912 · Time: 24.140685 · Source: 142.250.200.142 · Destination: 192.1...a: Echo (ping) reply id=0x0001, seq=141/36096, ttl=54 (request in 2890)

☒ Show packet bytes

Close Help

3. Another aspect of this investigation will involve looking at ICMP messages generated by Traceroute programs. In particular, you will be tasked with answering the following questions:

Performed traceroute google.com screenshot:

```
Command Prompt

Microsoft Windows [Version 10.0.18362.175]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\HP>tracert google.com

Tracing route to google.com [142.250.185.14]
over a maximum of 30 hops:

  0  4 ms    6 ms    2 ms   192.168.43.1
  1 305 ms   97 ms   55 ms   10.100.0.254
  2 199 ms   28 ms   49 ms   10.170.131.225
  3  50 ms    *      *      10.202.1.38
  4  37 ms   42 ms   27 ms   10.202.1.49
  5  *        *      *      Request timed out.
  6  *        *      *      Request timed out.
  7  25 ms   38 ms  302 ms  197.210.68.73
  8  76 ms   45 ms   51 ms  102.89.59.10
  9  47 ms  142 ms   53 ms  142.250.167.254
 10 333 ms   36 ms   40 ms  172.253.64.7
 11  49 ms   49 ms   52 ms  192.178.106.250
 12 408 ms  429 ms   *      66.249.94.86
 13 118 ms  110 ms  395 ms  142.251.48.124
 14 130 ms  112 ms  138 ms  142.251.76.117
 15 125 ms  114 ms  111 ms  142.251.49.55
 16 134 ms  111 ms  421 ms  mad4is11-in-f14.1e100.net [142.250.185.14]

Trace complete.

C:\Users\HP>
```

f. What is the IP address of your host PC (from the traceroute result)?

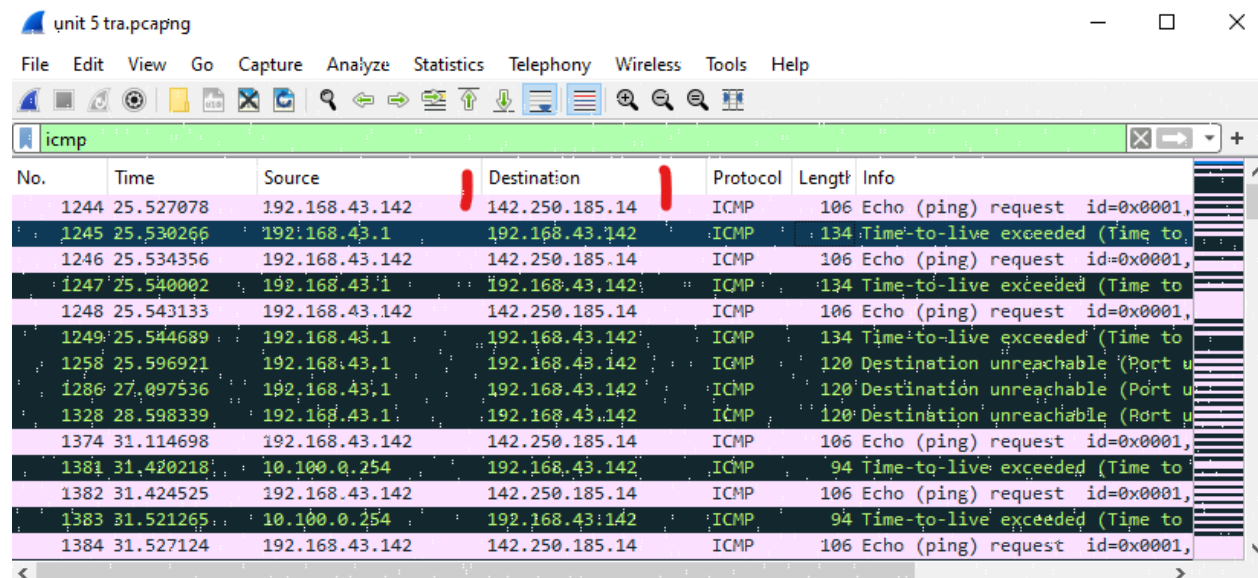
192.168.43.142

unit 5 tra.pcapng

No.	Time	Source	Destination	Protocol	Length	Info
1244	25.527078	192.168.43.142	142.250.185.14	ICMP	106	Echo (ping) request id=0x0001,
1245	25.530266	192.168.43.1	192.168.43.142	ICMP	134	Time-to-live exceeded (Time to
1246	25.534356	192.168.43.142	142.250.185.14	ICMP	106	Echo (ping) request id=0x0001,
1247	25.540002	192.168.43.1	192.168.43.142	ICMP	134	Time-to-live exceeded (Time to
1248	25.543133	192.168.43.142	142.250.185.14	ICMP	106	Echo (ping) request id=0x0001,
1249	25.544689	192.168.43.1	192.168.43.142	ICMP	134	Time-to-live exceeded (Time to
1258	25.596921	192.168.43.1	192.168.43.142	ICMP	120	Destination unreachable (Port u
1286	27.097536	192.168.43.1	192.168.43.142	ICMP	120	Destination unreachable (Port u
1328	28.598339	192.168.43.1	192.168.43.142	ICMP	120	Destination unreachable (Port u
1374	31.114698	192.168.43.142	142.250.185.14	ICMP	106	Echo (ping) request id=0x0001,
1381	31.420218	10.100.0.254	192.168.43.142	ICMP	94	Time-to-live exceeded (Time to
1382	31.424525	192.168.43.142	142.250.185.14	ICMP	106	Echo (ping) request id=0x0001,
1383	31.521265	10.100.0.254	192.168.43.142	ICMP	94	Time-to-live exceeded (Time to
1384	31.527124	192.168.43.142	142.250.185.14	ICMP	106	Echo (ping) request id=0x0001,

g. What is the IP address of the target destination host (from the traceroute result)?

142.250.185.14



The image shows a Wireshark packet capture window titled 'unit 5 tra.pcapng'. The packet list pane shows a series of ICMP packets. The first packet (No. 1244) is an Echo (ping) request from 192.168.43.142 to 142.250.185.14. The second packet (No. 1245) is a Time-to-live exceeded message from 192.168.43.1 to 192.168.43.142. The third packet (No. 1246) is an Echo (ping) request from 192.168.43.142 to 142.250.185.14. The fourth packet (No. 1247) is a Time-to-live exceeded message from 192.168.43.1 to 192.168.43.142. The fifth packet (No. 1248) is an Echo (ping) request from 192.168.43.142 to 142.250.185.14. The sixth packet (No. 1249) is a Time-to-live exceeded message from 192.168.43.1 to 192.168.43.142. The seventh packet (No. 1258) is a Destination unreachable (Port unreachable) message from 192.168.43.1 to 192.168.43.142. The eighth packet (No. 1286) is a Destination unreachable (Port unreachable) message from 192.168.43.1 to 192.168.43.142. The ninth packet (No. 1328) is a Destination unreachable (Port unreachable) message from 192.168.43.1 to 192.168.43.142. The tenth packet (No. 1374) is an Echo (ping) request from 192.168.43.142 to 142.250.185.14. The eleventh packet (No. 1381) is a Time-to-live exceeded message from 10.100.0.254 to 192.168.43.142. The twelfth packet (No. 1382) is an Echo (ping) request from 192.168.43.142 to 142.250.185.14. The thirteenth packet (No. 1383) is a Time-to-live exceeded message from 10.100.0.254 to 192.168.43.142. The fourteenth packet (No. 1384) is an Echo (ping) request from 192.168.43.142 to 142.250.185.14.

No.	Time	Source	Destination	Protocol	Length	Info
1244	25.527078	192.168.43.142	142.250.185.14	ICMP	106	Echo (ping) request id=0x0001,
1245	25.530266	192.168.43.1	192.168.43.142	ICMP	134	Time-to-live exceeded (Time to
1246	25.534356	192.168.43.142	142.250.185.14	ICMP	106	Echo (ping) request id=0x0001,
1247	25.540002	192.168.43.1	192.168.43.142	ICMP	134	Time-to-live exceeded (Time to
1248	25.543133	192.168.43.142	142.250.185.14	ICMP	106	Echo (ping) request id=0x0001,
1249	25.544689	192.168.43.1	192.168.43.142	ICMP	134	Time-to-live exceeded (Time to
1258	25.596921	192.168.43.1	192.168.43.142	ICMP	120	Destination unreachable (Port u
1286	27.097536	192.168.43.1	192.168.43.142	ICMP	120	Destination unreachable (Port u
1328	28.598339	192.168.43.1	192.168.43.142	ICMP	120	Destination unreachable (Port u
1374	31.114698	192.168.43.142	142.250.185.14	ICMP	106	Echo (ping) request id=0x0001,
1381	31.420218	10.100.0.254	192.168.43.142	ICMP	94	Time-to-live exceeded (Time to
1382	31.424525	192.168.43.142	142.250.185.14	ICMP	106	Echo (ping) request id=0x0001,
1383	31.521265	10.100.0.254	192.168.43.142	ICMP	94	Time-to-live exceeded (Time to
1384	31.527124	192.168.43.142	142.250.185.14	ICMP	106	Echo (ping) request id=0x0001,

4. Additionally, as part of your investigation, you will need to save and submit two Wireshark capture files (one for the ping command capture and one for the traceroute command capture).

(The two captures have been uploaded to the assignment section)

5. Finally, you will need to take screenshots of the relevant information for all of the questions outlined above (a-g), along with their answers, and include them in an MS Word or PDF file. This file should then be submitted as your assignment.

(All instructions duly adhered to)