

CSE Lab 4

WireShark TCP Lab

Aditya Balwani, SBUID : 109353920

Part 1

1. What is the IP address of your host? What is the IP address of the destination host?

My IP Address is 130.245.23.108. The IP address of the destination host is 143.89.14.2

2. Why is it that an ICMP packet does not have source and destination port numbers?

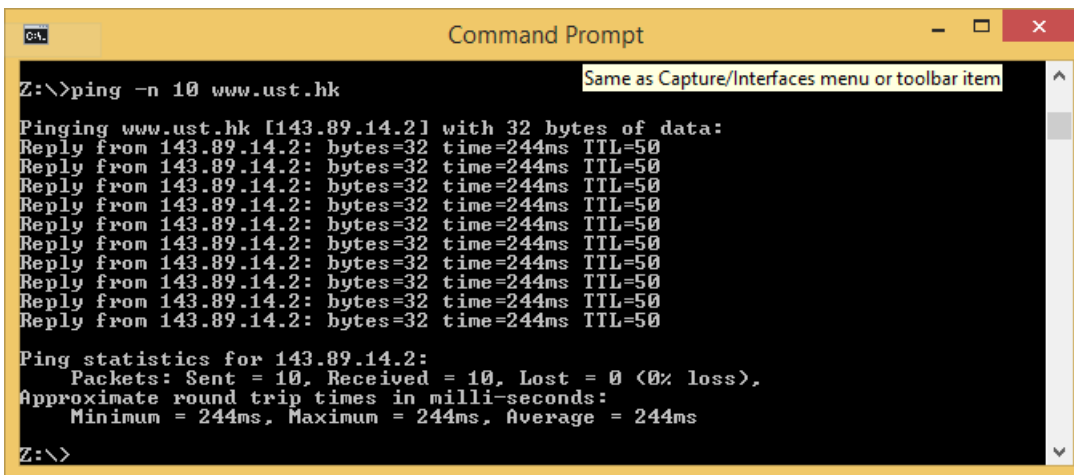
The ICMP Packet doesn't have a source and destination port number because it is designed to communicate between the network layer and not the application layer.

3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

- The ICMP Type is 8
- THE ICMP Code number is 0
- The checksum is 16 bytes
- Sequence numbers:
 - BE is 16 bytes
 - LE is 16 bytes
- Identifiers
 - BE is 16 bytes
 - LE is 16 bytes

4. **Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?**

- The ICMP Type is 0
- THE ICMP Code number is 0
- The checksum is 16 bytes
- Sequence numbers:
 - BE is 16 bytes
 - LE is 16 bytes
- Identifiers
 - BE is 16 bytes
 - LE is 16 bytes



```
Command Prompt
Z:\>ping -n 10 www.ust.hk

Pinging www.ust.hk [143.89.14.2] with 32 bytes of data:
Reply from 143.89.14.2: bytes=32 time=244ms TTL=50
Reply from 143.89.14.2: bytes=32 time=244ms TTL=50
Reply from 143.89.14.2: bytes=32 time=244ms TTL=50
Reply from 143.89.14.2: bytes=32 time=244ms TTL=50
Reply from 143.89.14.2: bytes=32 time=244ms TTL=50
Reply from 143.89.14.2: bytes=32 time=244ms TTL=50
Reply from 143.89.14.2: bytes=32 time=244ms TTL=50
Reply from 143.89.14.2: bytes=32 time=244ms TTL=50
Reply from 143.89.14.2: bytes=32 time=244ms TTL=50
Reply from 143.89.14.2: bytes=32 time=244ms TTL=50

Ping statistics for 143.89.14.2:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 244ms, Maximum = 244ms, Average = 244ms
Z:\>
```

lab5cap1.pcap [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: icmp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
20	1.851877	130.245.23.108	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=64/16384, ttl=128 (reply in 23)
23	2.096517	143.89.14.2	130.245.23.108	ICMP	74	Echo (ping) reply id=0x0001, seq=64/16384, ttl=50 (request in 20)
24	2.856181	130.245.23.108	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=65/16640, ttl=128 (reply in 27)

Frame 20: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

Ethernet II, Src: Universa_1c:c4:41 (00:21:86:1c:c4:41), Dst: Netscreen_ff:10:02 (00:10:db:ff:10:02)

Internet Protocol Version 4, Src: 130.245.23.108 (130.245.23.108), Dst: 143.89.14.2 (143.89.14.2)

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x4d1b [correct]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 64 (0x0040)

Sequence number (LE): 16384 (0x4000)

[Response frame: 23]

Data (32 bytes)

0000 00 10 db ff 10 02 00 21 86 1c c4 41 08 00 45 00!...A..E.
0010 00 3c 04 69 00 00 80 01 00 00 82 f5 17 6c 8f 59 <..i.....Y.
0020 0e 02 08 00 4d 1b 00 01 00 40 61 62 63 64 65 66 ..M...@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 wabcedfg hi

Frame (frame), 74 bytes Packets: 82 · Displayed: 20 (24.4%) · Load time: 0:00.000 Profile: Default

lab5cap1.pcap [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: icmp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
20	1.851877	130.245.23.108	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=64/16384, ttl=128 (reply in 23)
23	2.096517	143.89.14.2	130.245.23.108	ICMP	74	Echo (ping) reply id=0x0001, seq=64/16384, ttl=50 (request in 20)
24	2.856181	130.245.23.108	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=65/16640, ttl=128 (reply in 27)

Frame 23: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

Ethernet II, Src: Netscreen_ff:10:02 (00:10:db:ff:10:02), Dst: Universa_1c:c4:41 (00:21:86:1c:c4:41)

Internet Protocol Version 4, Src: 143.89.14.2 (143.89.14.2), Dst: 130.245.23.108 (130.245.23.108)

Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

Checksum: 0x551b [correct]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 64 (0x0040)

Sequence number (LE): 16384 (0x4000)

[Request frame: 20]

[Response time: 244.640 ms]

Data (32 bytes)

0000 00 21 86 1c c4 41 00 10 db ff 10 02 08 00 45 00 .!...A..E.
0010 00 3c bd 2f 00 00 32 01 93 d5 8f 59 0e 02 82 f5 <./..2. ...Y...
0020 17 6c 00 00 55 1b 00 01 00 40 61 62 63 64 65 66 ..l..U...@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 wabcedfg hi

File: "C:\Users\Aditya\Dropbox\Notes\CSE3... Packets: 82 · Displayed: 20 (24.4%) · Load time: 0:00.000 Profile: Default

Part 2

5. What is the IP address of your host? What is the IP address of the target destination host?

My IP Address is 130.245.23.108. The IP address of the destination host is 128.93.162.84

6. If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?

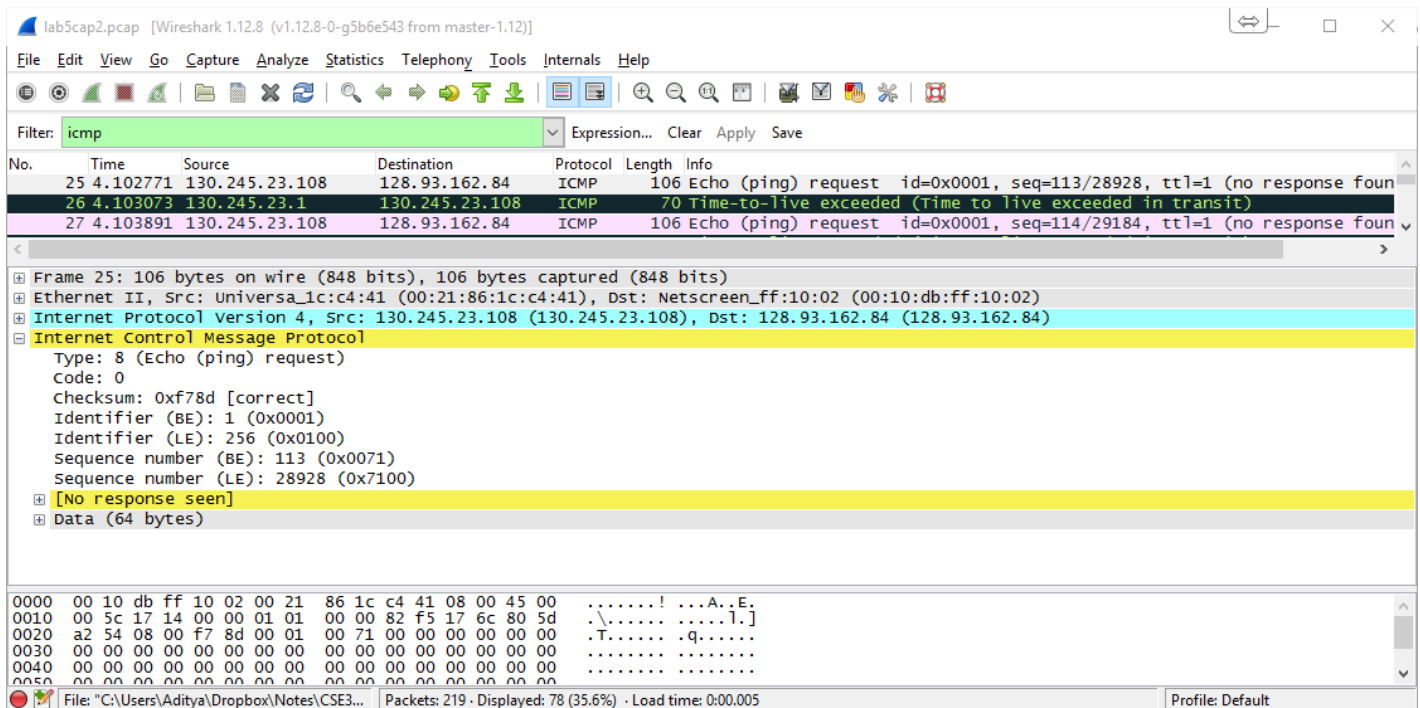
No if ICMP sent UDP packets, the IP protocol number would then be 11

7. Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?

The echo packet has the same fields as the query packet

8. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?

The error packet contains the IP header of the original packet and the original ICMP packet



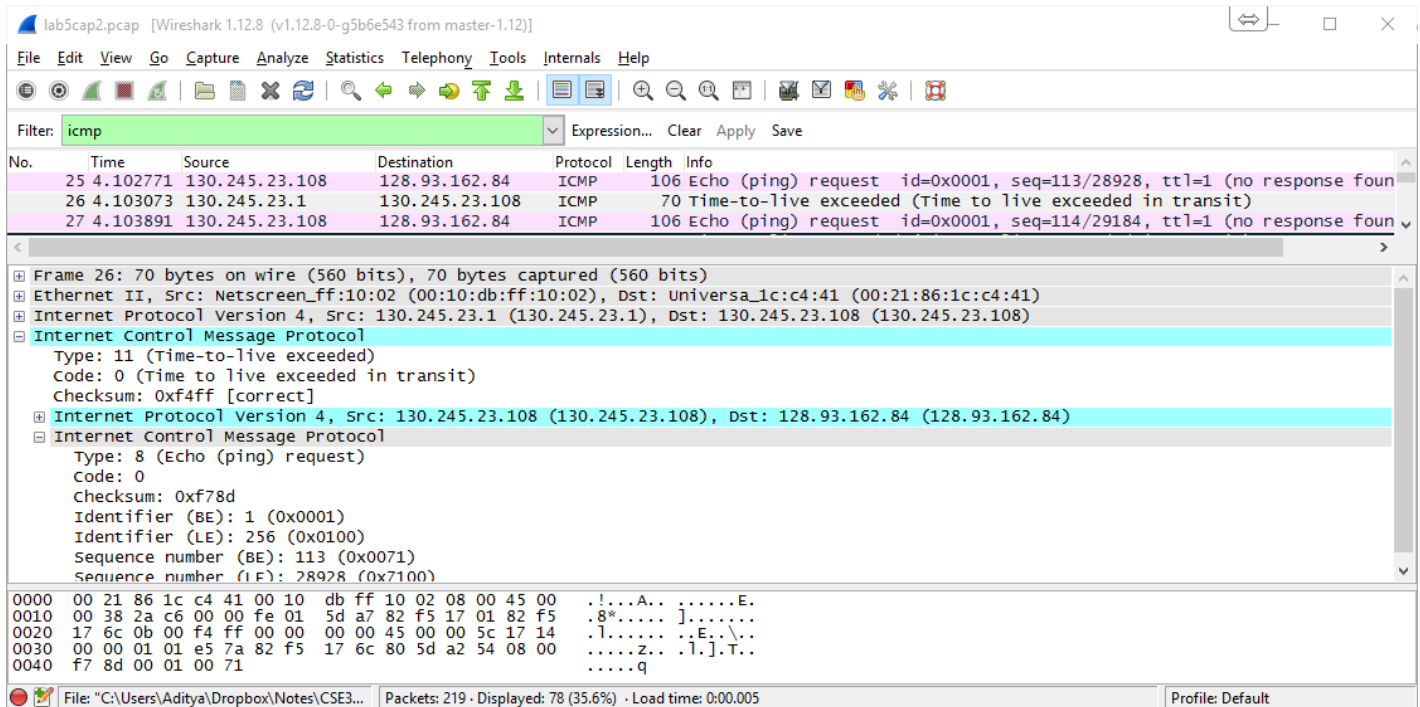
The screenshot shows the Wireshark interface with the filter 'icmp' applied. The packet list shows three ICMP packets:

No.	Time	Source	Destination	Protocol	Length	Info
25	4.102771	130.245.23.108	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=113/28928, ttl=1 (no response found)
26	4.103073	130.245.23.1	130.245.23.108	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
27	4.103891	130.245.23.108	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=114/29184, ttl=1 (no response found)

The packet details for packet 26 (ICMP error) are expanded, showing:

- Frame 25: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
- Ethernet II, Src: Universa1c:c4:41 (00:21:86:1c:c4:41), Dst: Netscreen_ff:10:02 (00:10:db:ff:10:02)
- Internet Protocol Version 4, Src: 130.245.23.108 (130.245.23.108), Dst: 128.93.162.84 (128.93.162.84)
- Internet Control Message Protocol
 - Type: 8 (Echo (ping) request)
 - Code: 0
 - Checksum: 0xf78d [correct]
 - Identifier (BE): 1 (0x0001)
 - Identifier (LE): 256 (0x0100)
 - Sequence number (BE): 113 (0x0071)
 - Sequence number (LE): 28928 (0x7100)
 - [No response seen]
 - Data (64 bytes)

The packet bytes pane shows the raw data of the ICMP error packet, including the original IP header and ICMP data.



9. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?

The last 3 ICMP packets received are Ping replies (type 0) instead of TTL Expired (type 11) because the packets have made their way to the destination

10. Within the traceroute measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in Figure 4, is there a link whose delay is significantly longer than others? On the basis of the router names, can you guess the location of the two routers on the end of this link?

Within the traceroute measurements, the link between step 5 to 6 has a significantly longer delay than others.

In figure 4, the link from step 9 to 10 has a delay significantly longer than others. This is the link from NYC to Pastourelle, France

```
Command Prompt

Z:\>tracert www.inria.fr

Tracing route to ezp3.inria.fr [128.93.162.84]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    130.245.23.1
  1  2 ms     1 ms     1 ms     perimeter.cs.stonybrook.edu [130.245.5.1]
  2  <1 ms    <1 ms    <1 ms    130.245.5.253
  3  3 ms     3 ms     3 ms     nyc-7600-stonybrook.nysernet.net [199.109.4.73]

  4  30 ms    30 ms    30 ms    199.109.5.26
  5  104 ms   104 ms   104 ms   internet2.mx1.lon.uk.geant.net [62.40.124.44]
  6  92 ms    92 ms    92 ms    ae0.mx1.par.fr.geant.net [62.40.98.77]
  7  94 ms    95 ms    94 ms    renater-lb1-gw.mx1.par.fr.geant.net [62.40.124.7]
  8  92 ms    92 ms    92 ms    te1-1-paris1-rtr-021.noc.renater.fr [193.51.177.251]
  9  92 ms    92 ms    92 ms    te1-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
 10  92 ms    93 ms    93 ms    inria-rocquencourt-gi3-2-inria-rtr-021.noc.renater.fr [193.51.184.177]
 11  *        *        *        Request timed out.
 12  *        *        *        Request timed out.
 13  93 ms    93 ms    93 ms    ezp3.inria.fr [128.93.162.84]

Trace complete.

Z:\>
```

lab5cap2.pcap [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: icmp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
169	33.467441	130.245.23.108	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=147/37632, ttl=12 (no response fou
180	37.468379	130.245.23.108	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=148/37888, ttl=12 (no response fou
193	41.469291	130.245.23.108	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=149/38144, ttl=13 (reply in 194)
194	41.563055	128.93.162.84	130.245.23.108	ICMP	106	Echo (ping) reply id=0x0001, seq=149/38144, ttl=53 (request in 193)
195	41.563863	130.245.23.108	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=150/38400, ttl=13 (reply in 196)
196	41.657132	128.93.162.84	130.245.23.108	ICMP	106	Echo (ping) reply id=0x0001, seq=150/38400, ttl=53 (request in 195)
197	41.657847	130.245.23.108	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=151/38656, ttl=13 (reply in 198)
198	41.751048	128.93.162.84	130.245.23.108	ICMP	106	Echo (ping) reply id=0x0001, seq=151/38656, ttl=53 (request in 197)

Frame 194: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)

Ethernet II, Src: Netscreen_ff:10:02 (00:10:db:ff:10:02), Dst: Universa_1c:c4:41 (00:21:86:1c:c4:41)

Internet Protocol Version 4, Src: 128.93.162.84 (128.93.162.84), Dst: 130.245.23.108 (130.245.23.108)

Internet Control Message Protocol

- Type: 0 (Echo (ping) reply)
- code: 0
- checksum: 0xff69 [correct]
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence number (BE): 149 (0x0095)
- Sequence number (LE): 38144 (0x9500)
- [Request frame: 193]
- [Response time: 93.764 ms]

Data (64 bytes)

0000 00 21 86 1c c4 41 00 10 db ff 10 02 08 00 45 00 .!...A..E.
0010 00 5c 5b cf 00 00 35 01 6c bf 80 5d a2 54 82 f5 .\...5. l...].T..
0020 17 6c 00 00 ff 69 00 01 00 95 00 00 00 00 00 00 .[...5.
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File: "C:\Users\Aditya\Dropbox\Notes\CSE3..." Packets: 219 · Displayed: 78 (35.6%) · Load time: 0:00.005 Profile: Default