HỌ TÊN : NGUYỄN XUÂN TRỰC

MSSV : 1513804

==========o0o==========

Windows Command Prompt: "ping –n 10 www.yahoo.com"

```
C:\Windows\System32>ping -n 10 www.yahoo.com

Pinging new-fp-shed.wg1.b.yahoo.com [202.165.107.49] with 32 bytes of data:
Reply from 202.165.107.49: bytes=32 time=67ms TTL=52
Reply from 202.165.107.49: bytes=32 time=84ms TTL=52
Reply from 202.165.107.49: bytes=32 time=95ms TTL=52
Reply from 202.165.107.49: bytes=32 time=108ms TTL=52
Reply from 202.165.107.49: bytes=32 time=113ms TTL=52
Reply from 202.165.107.49: bytes=32 time=127ms TTL=52
Reply from 202.165.107.49: bytes=32 time=142ms TTL=52
Reply from 202.165.107.49: bytes=32 time=156ms TTL=52
Reply from 202.165.107.49: bytes=32 time=65ms TTL=52
Reply from 202.165.107.49: bytes=32 time=81ms TTL=52

Ping statistics for 202.165.107.49:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 65ms, Maximum = 156ms, Average = 103ms
```

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

ANSWER

icmp

No.	Time	Source	Destination	Protocol	Length	Info
178	07:33:04.931131	172.17.0.229	202.165.107.49	ICMP	74	Echo (ping) request id=0x0100, seq=21/5376, ttl=128 (reply in 180)
180	07:33:04.998656	202.165.107.49	172.17.0.229	ICMP	74	Echo (ping) reply id=0x0100, seq=21/5376, ttl=52 (request in 178)
191	07:33:05.938203	172.17.0.229	202.165.107.49	ICMP	74	Echo (ping) request id=0x0100, seq=22/5632, ttl=128 (reply in 193)
193	07:33:06.022609	202.165.107.49	172.17.0.229	ICMP	74	Echo (ping) reply id=0x0100, seq=22/5632, ttl=52 (request in 191)
224	07:33:06.951289	172.17.0.229	202.165.107.49	ICMP	74	Echo (ping) request id=0x0100, seq=23/5888, ttl=128 (reply in 228)
228	07:33:07.046877	202.165.107.49	172.17.0.229	ICMP	74	Echo (ping) reply id=0x0100, seq=23/5888, ttl=52 (request in 224)
244	07:33:07.962296	172.17.0.229	202.165.107.49	ICMP	74	Echo (ping) request id=0x0100, seq=24/6144, ttl=128 (reply in 247)
247	07:33:08.070566	202.165.107.49	172.17.0.229	ICMP	74	Echo (ping) reply id=0x0100, seq=24/6144, ttl=52 (request in 244)
270	07:33:08.981461	172.17.0.229	202.165.107.49	ICMP	74	Echo (ping) request id=0x0100, seq=25/6400, ttl=128 (reply in 273)
273	07:33:09.094775	202.165.107.49	172.17.0.229	ICMP	74	Echo (ping) reply id=0x0100, seq=25/6400, ttl=52 (request in 270)
278	07:33:09.991466	172.17.0.229	202.165.107.49	ICMP	74	Echo (ping) request id=0x0100, seq=26/6656, ttl=128 (reply in 282)
282	07:33:10.118612	202.165.107.49	172.17.0.229	ICMP	74	Echo (ping) reply id=0x0100, seq=26/6656, ttl=52 (request in 278)
301	07:33:11.001100	172.17.0.229	202.165.107.49	ICMP	74	Echo (ping) request id=0x0100, seq=27/6912, ttl=128 (reply in 308)
308	07:33:11.143446	202.165.107.49	172.17.0.229	ICMP	74	Echo (ping) reply id=0x0100, seq=27/6912, ttl=52 (request in 301)
387	07:33:12.011434	172.17.0.229	202.165.107.49	ICMP	74	Echo (ping) request id=0x0100, seq=28/7168, ttl=128 (reply in 391)
391	07:33:12.167600	202.165.107.49	172.17.0.229	ICMP	74	Echo (ping) reply id=0x0100, seq=28/7168, ttl=52 (request in 387)
405	07:33:13.022916	172.17.0.229	202.165.107.49	ICMP	74	Echo (ping) request id=0x0100, seq=29/7424, ttl=128 (reply in 406)
406	07:33:13.088480	202.165.107.49	172.17.0.229	ICMP	74	Echo (ping) reply id=0x0100, seq=29/7424, ttl=52 (request in 405)
418	07:33:14.031412	172.17.0.229	202.165.107.49	ICMP	74	Echo (ping) request id=0x0100, seq=30/7680, ttl=128 (reply in 425)
425	07:33:14.112260	202.165.107.49	172.17.0.229	ICMP	74	Echo (ping) reply id=0x0100, seq=30/7680, ttl=52 (request in 418)

Host: 172.17.0.229

Destination: 202.165.107.49 (www.yahoo.com)

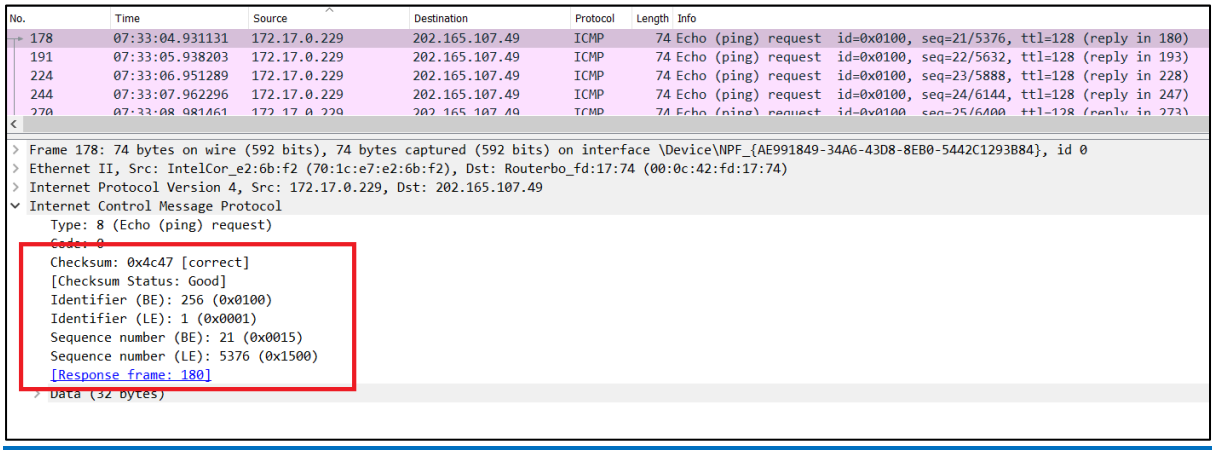
2) Why is it that an ICMP packet does not have source and destination port numbers?

ANSWER

The ICMP packet does not have source and destination port numbers because it was designed to communicate network-layer information between hosts and routers, not between application layer processes.

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?

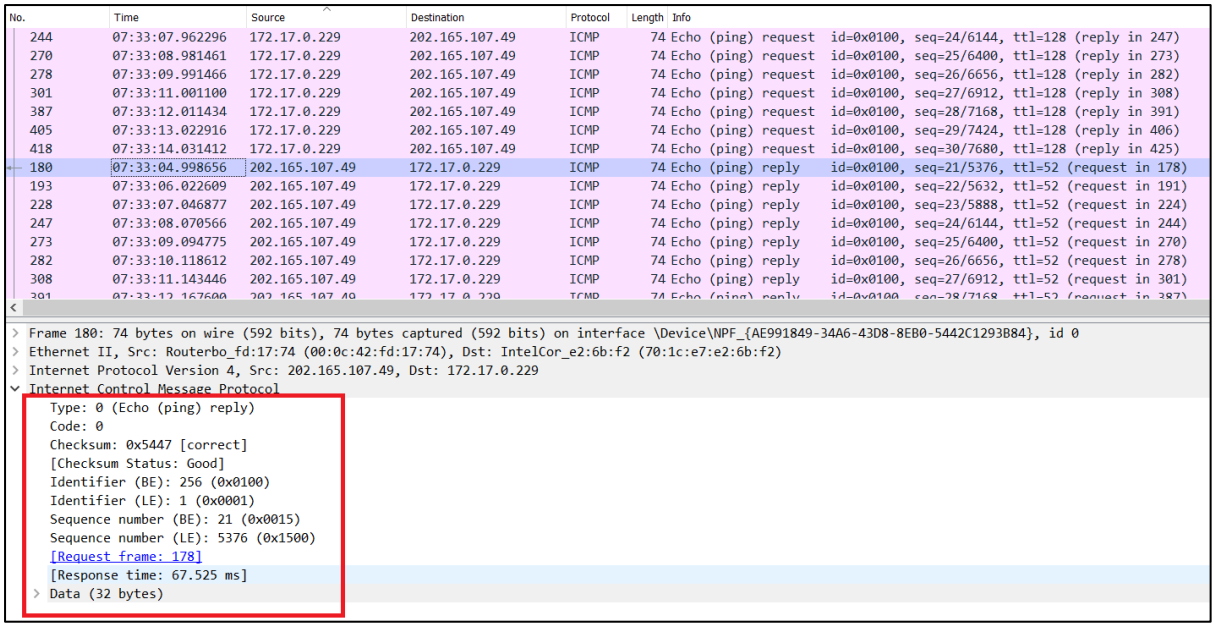
ANSWER



- ICMP type – 8, ICMP code 0.
- Checksum, identifier, sequence number and data fields.
- Checksum: 0x4c47
- Identifier (BE): 256
- Identifier (LE): 1
- Sequence number (BE): 21
- Sequence number (LE): 5376

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?

ANSWER



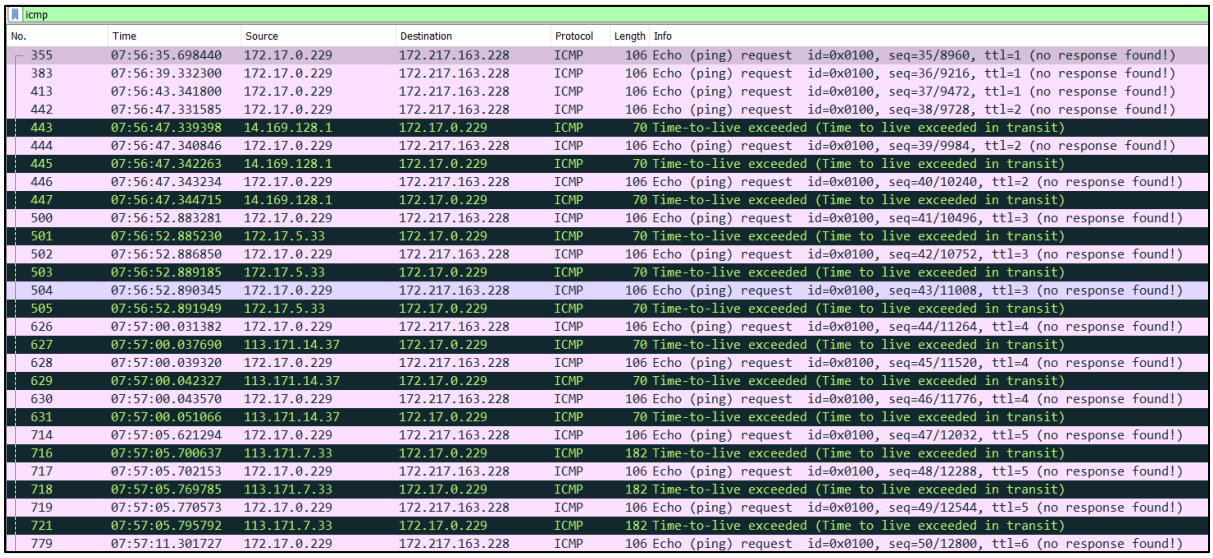
- ICMP type – 0, ICMP code – 0.
- Checksum, identifier, sequence number, and data fields.
- Checksum: 0x5447
- Identifier (BE): 256
- Identifier (LE): 1
- Sequence number (BE): 21
- Sequence number (LE): 5376

Windows Command Prompt: “tracert www.google.com”

```
C:\Windows\System32>tracert www.google.com

Tracing route to www.google.com [172.217.163.228]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2     7 ms     1 ms     1 ms  static.vnpt.vn [14.169.128.1]
  3     2 ms     2 ms     1 ms  172.17.5.33
  4     6 ms     3 ms     7 ms  static.vnpt.vn [113.171.14.37]
  5    79 ms    67 ms    25 ms  static.vnpt.vn [113.171.7.33]
  6     5 ms     2 ms     2 ms  static.vnpt.vn [113.171.50.218]
  7    60 ms    25 ms    75 ms  static.vnpt.vn [113.171.37.108]
  8    74 ms    27 ms    72 ms  72.14.213.88
  9    78 ms    25 ms    74 ms  66.249.94.253
 10    92 ms    63 ms    37 ms  172.253.64.111
 11    25 ms    72 ms    25 ms  hkg12s18-in-f4.1e100.net [172.217.163.228]

Trace complete.

C:\Windows\System32>
```

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

ANSWER



icmp

No.	Time	Source	Destination	Protocol	Length	Info
355	07:56:35.698440	172.17.0.229	172.217.163.228	ICMP	106	Echo (ping) request id=0x0100, seq=35/8960, ttl=1 (no response found!)
383	07:56:39.332300	172.17.0.229	172.217.163.228	ICMP	106	Echo (ping) request id=0x0100, seq=36/9216, ttl=1 (no response found!)
413	07:56:43.341800	172.17.0.229	172.217.163.228	ICMP	106	Echo (ping) request id=0x0100, seq=37/9472, ttl=1 (no response found!)
442	07:56:47.331585	172.17.0.229	172.217.163.228	ICMP	106	Echo (ping) request id=0x0100, seq=38/9728, ttl=2 (no response found!)
443	07:56:47.339398	14.169.128.1	172.17.0.229	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
444	07:56:47.340846	172.17.0.229	172.217.163.228	ICMP	106	Echo (ping) request id=0x0100, seq=39/9984, ttl=2 (no response found!)
445	07:56:47.342263	14.169.128.1	172.17.0.229	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
446	07:56:47.343234	172.17.0.229	172.217.163.228	ICMP	106	Echo (ping) request id=0x0100, seq=40/10240, ttl=2 (no response found!)
447	07:56:47.344715	14.169.128.1	172.17.0.229	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
500	07:56:52.883281	172.17.0.229	172.217.163.228	ICMP	106	Echo (ping) request id=0x0100, seq=41/10496, ttl=3 (no response found!)
501	07:56:52.885230	172.17.5.33	172.17.0.229	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
502	07:56:52.886850	172.17.0.229	172.217.163.228	ICMP	106	Echo (ping) request id=0x0100, seq=42/10752, ttl=3 (no response found!)
503	07:56:52.889185	172.17.5.33	172.17.0.229	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
504	07:56:52.890345	172.17.0.229	172.217.163.228	ICMP	106	Echo (ping) request id=0x0100, seq=43/11008, ttl=3 (no response found!)
505	07:56:52.891949	172.17.5.33	172.17.0.229	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
626	07:57:00.031382	172.17.0.229	172.217.163.228	ICMP	106	Echo (ping) request id=0x0100, seq=44/11264, ttl=4 (no response found!)
627	07:57:00.037690	113.171.14.37	172.17.0.229	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
628	07:57:00.039320	172.17.0.229	172.217.163.228	ICMP	106	Echo (ping) request id=0x0100, seq=45/11520, ttl=4 (no response found!)
629	07:57:00.042327	113.171.14.37	172.17.0.229	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
630	07:57:00.043570	172.17.0.229	172.217.163.228	ICMP	106	Echo (ping) request id=0x0100, seq=46/11776, ttl=4 (no response found!)
631	07:57:00.051066	113.171.14.37	172.17.0.229	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
714	07:57:05.621294	172.17.0.229	172.217.163.228	ICMP	106	Echo (ping) request id=0x0100, seq=47/12032, ttl=5 (no response found!)
716	07:57:05.700637	113.171.7.33	172.17.0.229	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
717	07:57:05.702153	172.17.0.229	172.217.163.228	ICMP	106	Echo (ping) request id=0x0100, seq=48/12288, ttl=5 (no response found!)
718	07:57:05.769785	113.171.7.33	172.17.0.229	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
719	07:57:05.770573	172.17.0.229	172.217.163.228	ICMP	106	Echo (ping) request id=0x0100, seq=49/12544, ttl=5 (no response found!)
721	07:57:05.795792	113.171.7.33	172.17.0.229	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
779	07:57:11.301727	172.17.0.229	172.217.163.228	ICMP	106	Echo (ping) request id=0x0100, seq=50/12800, ttl=6 (no response found!)

Host: 172.17.0.229

Destination: 172.217.163.228 (www.google.com)

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?

ANSWER

No, it would be 08 instead of 01.

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?

ANSWER

No

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

ANSWER

The IP header and the first 8 bytes of the original ICMP packet.

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?

ANSWER

- The last 3 packets are type 0.
- They are different because all the datagrams made it to the hose before the TTL expired.

10) Within the tracert 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?

ANSWER

- Yes, from 6 to 7 there was a long delay.
- Yes, from 9 to 10 in figure 4.
- In figure 4 the first location is NYC and the second is Pastourelle.