Computer Networks Advanced Course

Network Layer – ICMP

Barak Gonen

Topics

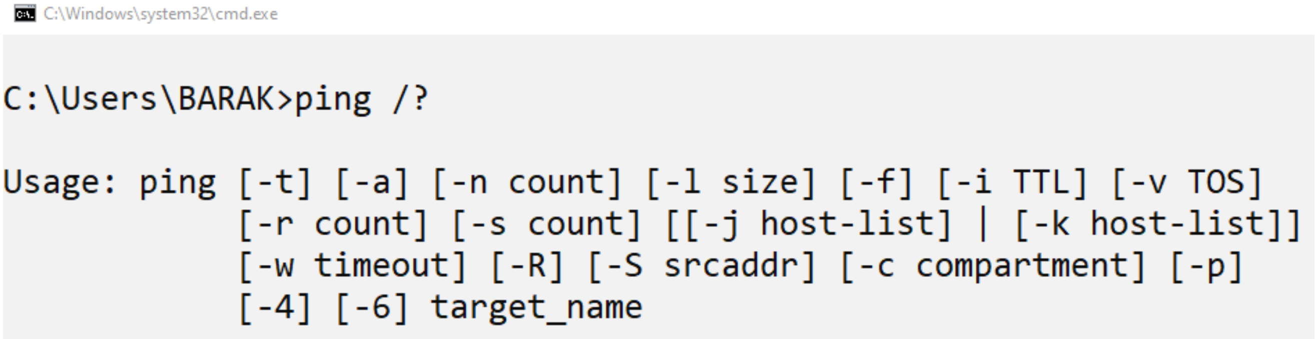
- ICMP
- Create and send Ping using Scapy

ICMP

- Internet Control Message Protocol
- Used by technicians to check connectivity
- Most known usage – Ping
- Note: ICMP is above IP but it is not a transport layer protocol
  - There are no ports

Ping

- In CMD, write: ping /?
- Send 2 packets
- Send IPv6 ping to dns.google.com

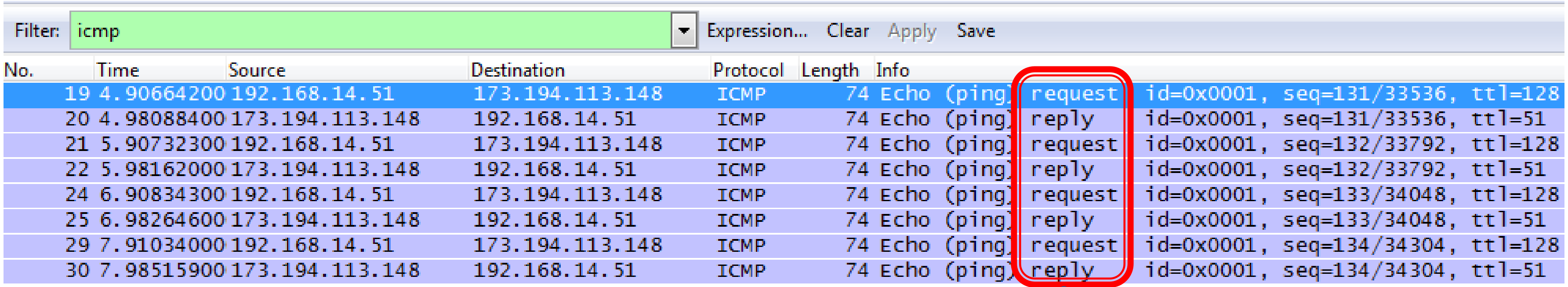


```
C:\Users\BARAK>ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name
```

Hands On

- Fire up Wireshark
- Ping anywhere
- Use "ICMP" as filter



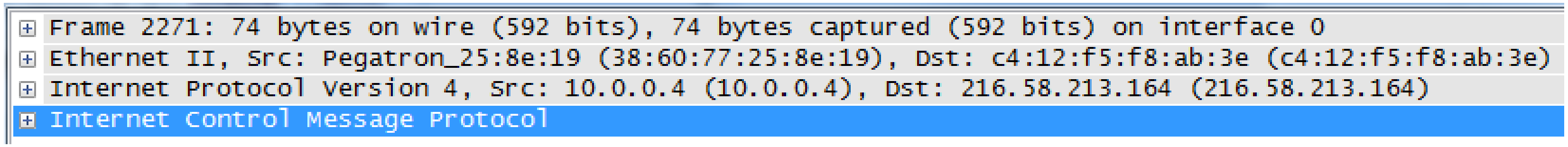
Filter: icmp

No.	Time	Source	Destination	Protocol	Length	Info
19	4.90664200	192.168.14.51	173.194.113.148	ICMP	74	Echo (ping) request id=0x0001, seq=131/33536, ttl=128
20	4.98088400	173.194.113.148	192.168.14.51	ICMP	74	Echo (ping) reply id=0x0001, seq=131/33536, ttl=51
21	5.90732300	192.168.14.51	173.194.113.148	ICMP	74	Echo (ping) request id=0x0001, seq=132/33792, ttl=128
22	5.98162000	173.194.113.148	192.168.14.51	ICMP	74	Echo (ping) reply id=0x0001, seq=132/33792, ttl=51
24	6.90834300	192.168.14.51	173.194.113.148	ICMP	74	Echo (ping) request id=0x0001, seq=133/34048, ttl=128
25	6.98264600	173.194.113.148	192.168.14.51	ICMP	74	Echo (ping) reply id=0x0001, seq=133/34048, ttl=51
29	7.91034000	192.168.14.51	173.194.113.148	ICMP	74	Echo (ping) request id=0x0001, seq=134/34304, ttl=128
30	7.98515900	173.194.113.148	192.168.14.51	ICMP	74	Echo (ping) reply id=0x0001, seq=134/34304, ttl=51

Note Ping request and reply

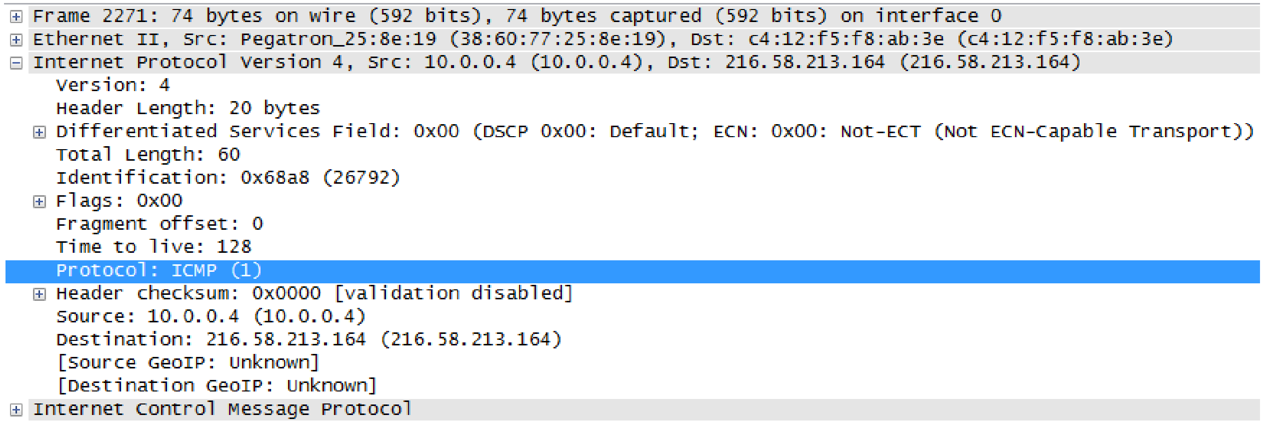
Ping

- ICMP is above IP



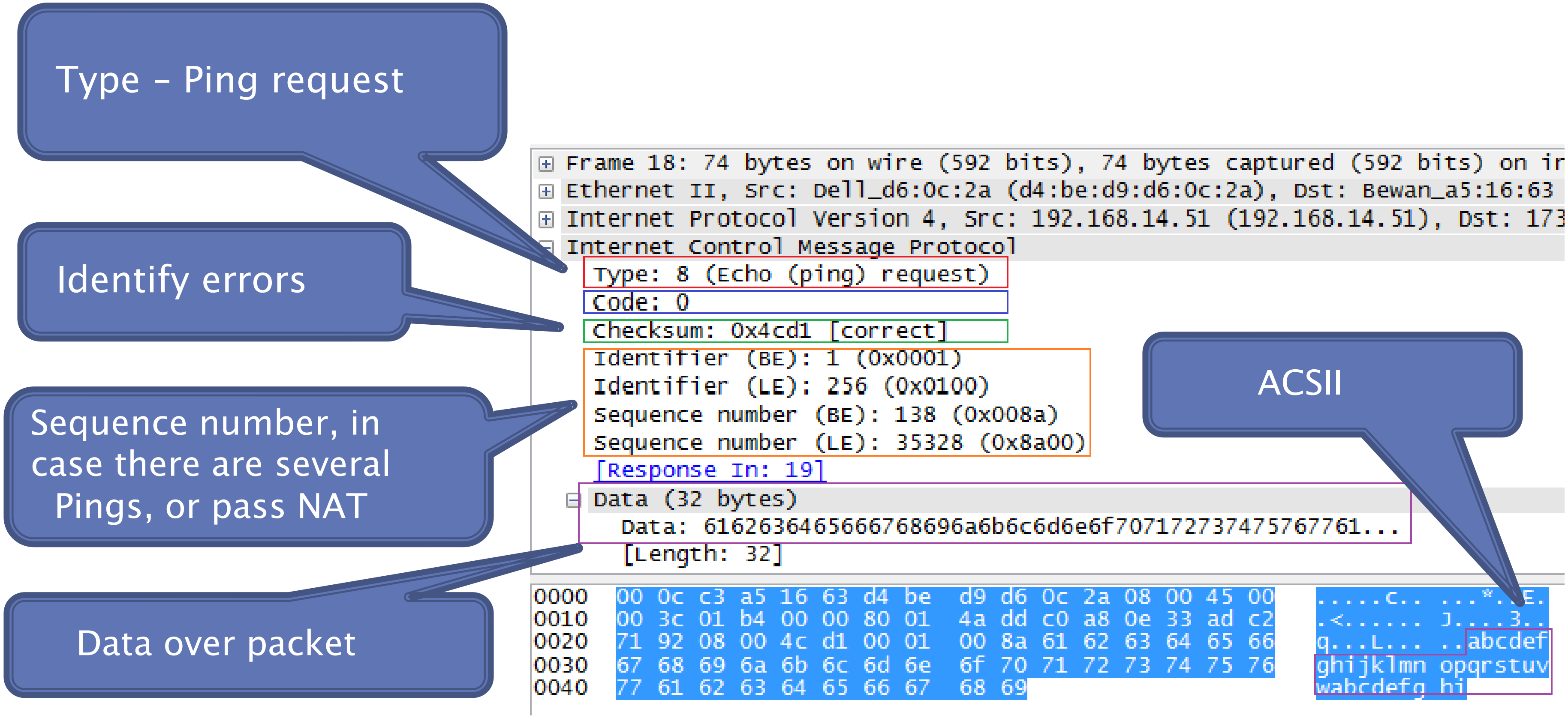
```
⊞ Frame 2271: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
⊞ Ethernet II, Src: Pegatron_25:8e:19 (38:60:77:25:8e:19), Dst: c4:12:f5:f8:ab:3e (c4:12:f5:f8:ab:3e)
⊞ Internet Protocol Version 4, Src: 10.0.0.4 (10.0.0.4), Dst: 216.58.213.164 (216.58.213.164)
⊞ Internet Control Message Protocol
```

- How can the receiver tell that it's ICMP?
  - Look for the protocol field in IP



```
⊞ Frame 2271: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
⊞ Ethernet II, Src: Pegatron_25:8e:19 (38:60:77:25:8e:19), Dst: c4:12:f5:f8:ab:3e (c4:12:f5:f8:ab:3e)
⊟ Internet Protocol Version 4, Src: 10.0.0.4 (10.0.0.4), Dst: 216.58.213.164 (216.58.213.164)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 60
    Identification: 0x68a8 (26792)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
  ⊞ Header checksum: 0x0000 [validation disabled]
    Source: 10.0.0.4 (10.0.0.4)
    Destination: 216.58.213.164 (216.58.213.164)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊞ Internet Control Message Protocol
```

Ping Request



Type – Ping request

Identify errors

Sequence number, in case there are several Pings, or pass NAT

Data over packet

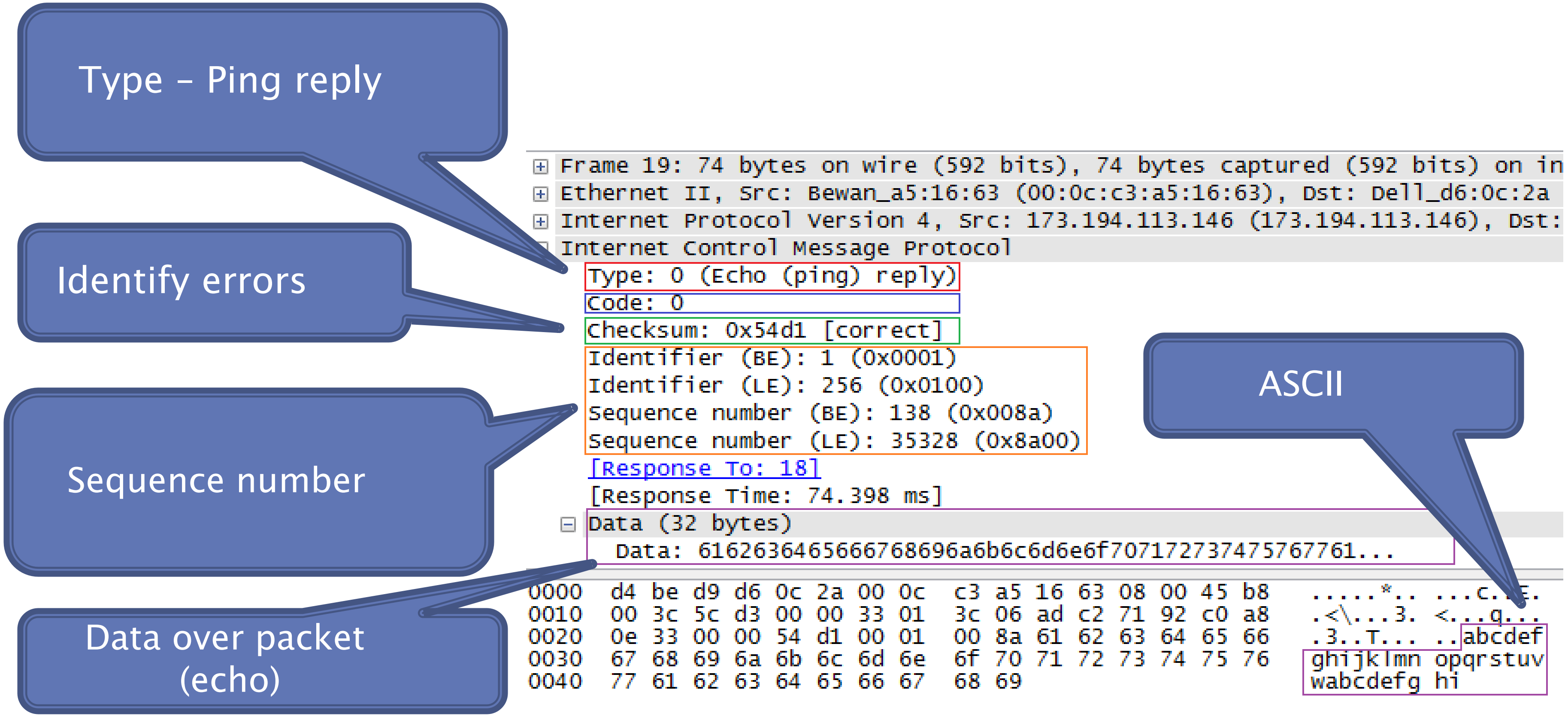
ACSII

```
⊞ Frame 18: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on ir
⊞ Ethernet II, Src: Dell_d6:0c:2a (d4:be:d9:d6:0c:2a), Dst: Bewan_a5:16:63
⊞ Internet Protocol Version 4, Src: 192.168.14.51 (192.168.14.51), Dst: 173
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4cd1 [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 138 (0x008a)
    Sequence number (LE): 35328 (0x8a00)
    [Response In: 19]
  ⊟ Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
      [Length: 32]

0000  00 0c c3 a5 16 63 d4 be  d9 d6 0c 2a 08 00 45 00   .....c.. ...*..E.
0010  00 3c 01 b4 00 00 80 01  4a dd c0 a8 0e 33 ad c2   .<...... J....3..
0020  71 92 08 00 4c d1 00 01  00 8a 61 62 63 64 65 66   q...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
```

- In the reply, which values will be identical?

Ping Reply



Type – Ping reply

Identify errors

Sequence number

Data over packet (echo)

ASCII

```
⊞ Frame 19: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on in
⊞ Ethernet II, Src: Bewan_a5:16:63 (00:0c:c3:a5:16:63), Dst: Dell_d6:0c:2a
⊞ Internet Protocol Version 4, Src: 173.194.113.146 (173.194.113.146), Dst:
⊟ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x54d1 [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 138 (0x008a)
    Sequence number (LE): 35328 (0x8a00)
    [Response To: 18]
    [Response Time: 74.398 ms]
  ⊟ Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677761...

0000  d4 be d9 d6 0c 2a 00 0c  c3 a5 16 63 08 00 45 b8   ......*. ...c..E.
0010  00 3c 5c d3 00 00 33 01  3c 06 ad c2 71 92 c0 a8   .<\...3. <...q...
0020  0e 33 00 00 54 d1 00 01  00 8a 61 62 63 64 65 66   .3..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
```

Fun with Ping

- Ex. 7.5
- Cause Google to send you a ping reply with data "You are the best!"