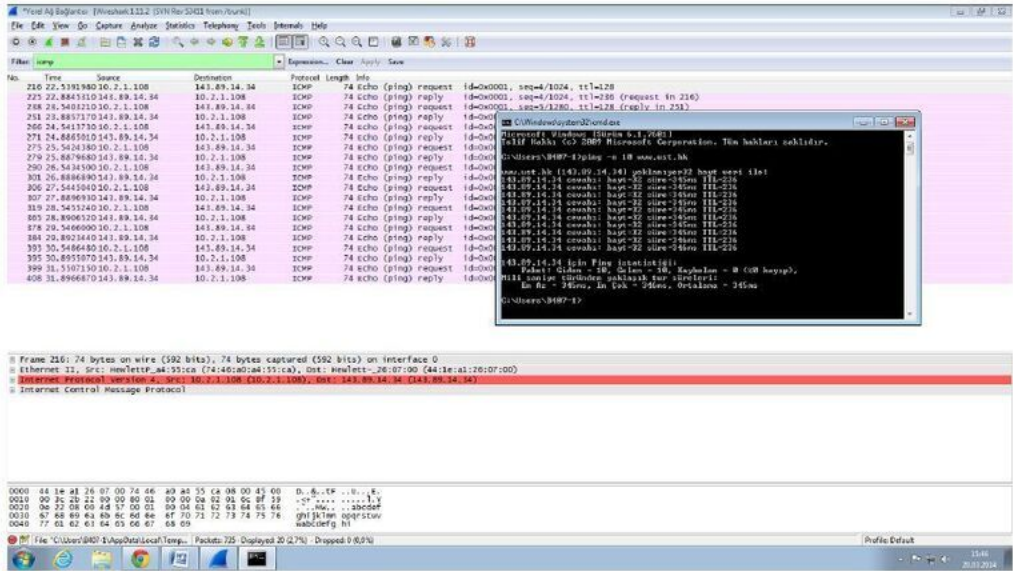




Başkent Üniversitesi
Elektrik - Elektronik Mühendisliği Bölümü

EEM 438

Deney No: 3



Gerekli komutlar yazıldı. 10 ping atıldı, 10x2 den 20 tane mesaj yakaladık.

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

Benim ip adresim: source: 10.2.1.108

Varış ip adresi (Honkong): destination: 143.89.14.34

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

Network layer üzerinden çalışan bir sistem için type ve code üzerinden çalışması yeterlidir. Çünkü fazla karmaşık bir katmana ihtiyaç yoktur.

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 screenshot shows a Wireshark packet capture of ICMP Echo (ping) requests and replies. The packet list pane displays a series of requests and replies between the source IP 10.2.1.108 and the destination IP 143.89.14.34. The packet details pane for the selected packet (Frame 216) shows the following fields:

- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0x457 [correct]
- Identifier (id): 1 (0x0001)
- Identifier (id): 256 (0x0100)
- Sequence number (seq): 4 (0x0004)
- Sequence number (seq): 1624 (0x0600)
- Resource frame: 2241
- Data (22 bytes)

The packet bytes pane shows the raw data in hexadecimal and ASCII. The first few bytes are 0000 44 1e 26 07 00 74 46, which correspond to the ICMP Echo request structure.

Type: 8 (Echo (ping) request)

Code: 0

Bunun yanında "Internet Control Message Protocol" içinde Checksum, Identifier, Sequence number bulunmaktadır. Her biri 2 şer bytedir.

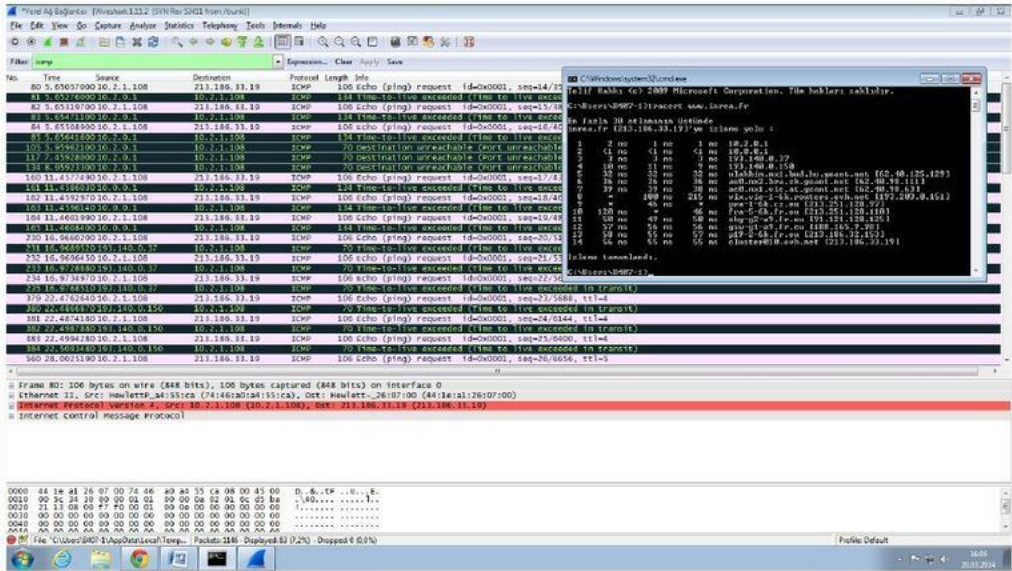
4. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

[illegible]

Type: 0 (Echo (ping) request)

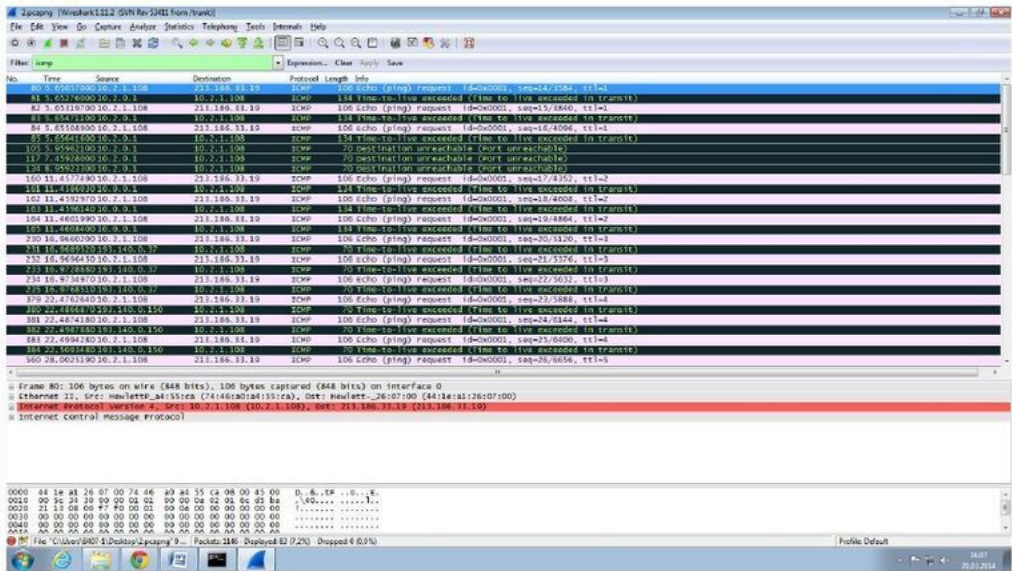
Code: 0

Bunun yanında "Internet Control Message Protocol" içinde Checksum, Identifier, Sequence number bulunmaktadır. Her biri 2 şer byte dır.



Gerekli komutlar tekrardan yazıldı bu sefer Fransa'daki bir ip ye bağlanılmaya çalışıldı.

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



Benim ip adresim: source: 10.2.1.108

Varış ip adresi (destination) (Fransa): destination: 213.186.33.19

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 screenshot shows a Wireshark capture of ICMP echo packets. The packet list displays a series of 'Echo (ping) request' and 'Echo (ping) reply' packets. The packet details pane for the selected packet shows the following fields:

- Type: 8 (Echo (ping) Request)
- Code: 0
- Checksum: 0x7f70 [correct]
- Identifier (id): 1 (0x0001)
- Identifier (li): 256 (0x0100)
- Sequence number (seq): 14 (0x000e)
- Sequence number (li): 256 (0x0100)
- Data (64 bytes):

The screenshot shows a Wireshark capture of ICMP echo packets. The packet list displays a series of 'Echo (ping) request' and 'Echo (ping) reply' packets. The packet details pane for the selected packet shows the following fields:

- Type: 8 (Echo (ping) Request)
- Code: 0
- Checksum: 0x4557 [correct]
- Identifier (id): 1 (0x0001)
- Identifier (li): 256 (0x0100)
- Sequence number (seq): 1 (0x0001)
- Sequence number (li): 1024 (0x0400)
- Data (32 bytes):

Ping request mesajı ile ICMP echo packet arasındaki tüm bilgiler aynıdır. İçerik olarak Type, Code, Checksum, Identifier, Sequence number bulunmaktadır.

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 screenshot shows a Wireshark packet capture of ICMP Echo (ping) requests. The selected packet is an ICMP Echo (ping) request from 10.0.2.15 to 211.186.33.19. The packet details pane shows the following fields:

- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 211.186.33.19
- Internet Control Message Protocol
 - Type: 8 (Echo (ping) request)
 - Checksum: 0x7f70 [correct]
 - Identifier (id): 1 (0x000001)
 - Identifier (id): 256 (0x0100)
 - Sequence number (seq): 14 (0x00000e)
 - Sequence number (seq): 256 (0x0100)
 - Data (64 bytes)

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

The screenshot shows a Wireshark packet capture of ICMP Echo (ping) requests. The selected packet is an ICMP Echo (ping) request from 10.0.2.15 to 211.186.33.19. The packet details pane shows the following fields:

- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 211.186.33.19
- Internet Control Message Protocol
 - Type: 8 (Echo (ping) request)
 - Checksum: 0x7f70 [correct]
 - Identifier (id): 1 (0x000001)
 - Identifier (id): 256 (0x0100)
 - Sequence number (seq): 14 (0x00000e)
 - Sequence number (seq): 256 (0x0100)
 - Data (64 bytes)

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

ICMP error packet ve ICMP echo packet arasında fazladan ip header bölümü ve identifier bölümü bulunmaktadır.

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 screenshot shows a Wireshark packet capture of ICMP Echo (ping) requests and replies. The third packet is highlighted, showing a successful ping reply. The packet details pane shows the following information:

- Frame 842: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
- Ethernet II, Src: Hewlett-Packard (44:15:16:07:00:00), Dst: Hewlett-Packard (44:15:16:07:00:00)
- Internet Protocol Version 4, Src: 10.2.1.108, Dst: 213.186.33.19
- Internet Control Message Protocol
 - Type: 8 (Echo (ping) request)
 - Code: 0 (Time to live exceeded (time to live exceeded in transit))
 - Checksum: 0x4f7f (correct)

The packet bytes pane shows the raw data of the ICMP Echo (ping) request, including the identifier (0x0001), sequence number (seq=47/12042), and ttl (12).

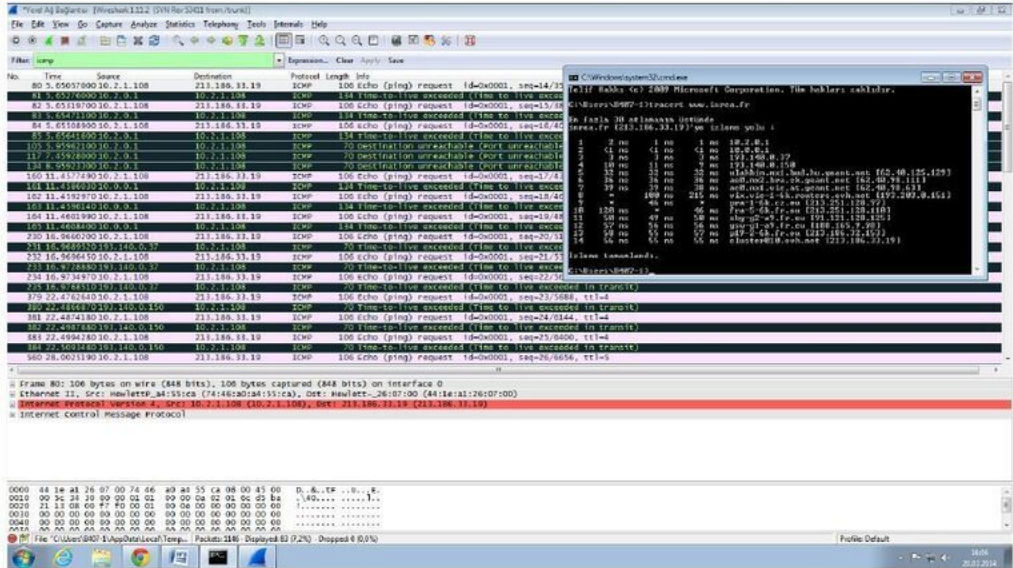
The screenshot shows a Wireshark packet capture of ICMP Echo (ping) requests and replies. The third packet is highlighted, showing a successful ping reply. The packet details pane shows the following information:

- Frame 863: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
- Ethernet II, Src: Hewlett-Packard (44:15:16:07:00:00), Dst: Hewlett-Packard (44:15:16:07:00:00)
- Internet Protocol Version 4, Src: 213.186.33.19, Dst: 10.2.1.108
- Internet Control Message Protocol
 - Type: 0 (Echo (ping) reply)
 - Code: 0
 - Checksum: 0xffff (correct)
 - Identifier (id): 1 (0x0001)
 - Identifier (id): 230 (0x0000)
 - Sequence number (seq): 55 (0x0037)
 - Sequence number (seq): 14080 (0x3700)
 - Request frame: 861

The packet bytes pane shows the raw data of the ICMP Echo (ping) reply, including the identifier (0x0001), sequence number (seq=55/14080), and ttl (12).

Son 3 paket arasındaki time to live değerlerinde küçük fark 11 den 0 a değişmesi olarak gözükmemektedir.

10. Within the tracer 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?



Daha fazla süre harcayan veri 8. Adımda bulunmaktadır. Sebebi sanırım pink kontrol servisi üzerinden ulaşmaya çalışmış olması buda private server olamasından kaynaklanıyor olabilir. (<http://ovh.net/>)

Ülke olarak Fransa ve Çek Cumhuriyeti üzerinden ping işlemleri yapılmıştır.