Университет ИТМО

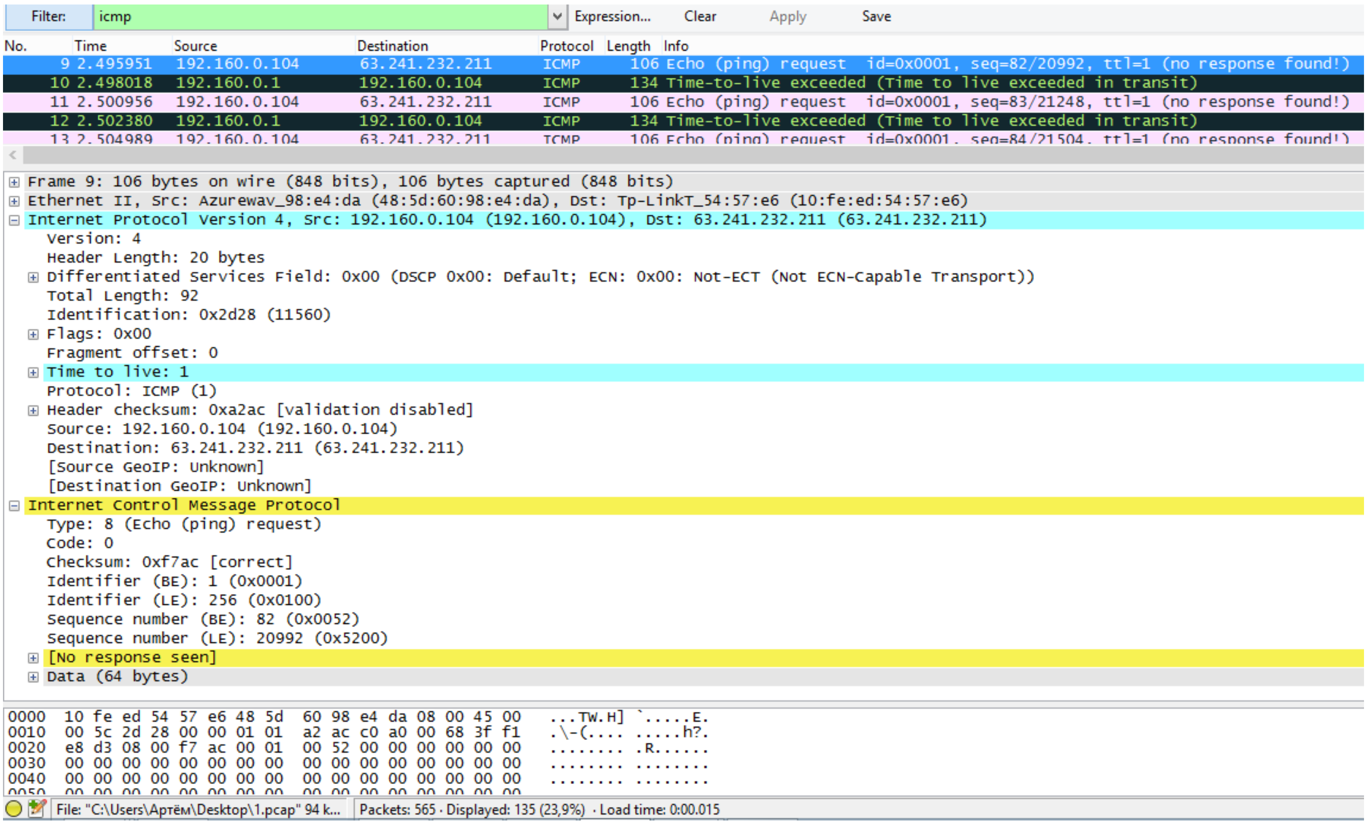
Лабораторная работа №3 по дисциплине «Сети ЭВМ и телекоммуникации»

Выполнил:
студент 3-го курса
группы 3125
Припадчев Артём

Санкт-Петербург
2015

Часть 1. Исследование структуры сетевых пакетов с помощью анализатора трафика Wireshark

Протокол IP



Filter: icmp

```
No.  Time      Source          Destination      Protocol Length Info
   9 2.495951  192.160.0.104   63.241.232.211   ICMP     106 Echo (ping) request  id=0x0001, seq=82/20992, ttl=1 (no response found!)
  10 2.498018  192.160.0.1     192.160.0.104    ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
  11 2.500956  192.160.0.104   63.241.232.211   ICMP     106 Echo (ping) request  id=0x0001, seq=83/21248, ttl=1 (no response found!)
  12 2.502380  192.160.0.1     192.160.0.104    ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
  13 2.504989  192.160.0.104   63.241.232.211   ICMP     106 Echo (ping) request  id=0x0001, seq=84/21504, ttl=1 (no response found!)
```

```
⊞ Frame 9: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
⊞ Ethernet II, Src: Azurewav_98:e4:da (48:5d:60:98:e4:da), Dst: Tp-LinkT_54:57:e6 (10:fe:ed:54:57:e6)
⊟ Internet Protocol Version 4, Src: 192.160.0.104 (192.160.0.104), Dst: 63.241.232.211 (63.241.232.211)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 92
    Identification: 0x2d28 (11560)
  ⊞ Flags: 0x00
    Fragment offset: 0
  ⊞ Time to live: 1
    Protocol: ICMP (1)
  ⊞ Header checksum: 0xa2ac [validation disabled]
    Source: 192.160.0.104 (192.160.0.104)
    Destination: 63.241.232.211 (63.241.232.211)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7ac [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 82 (0x0052)
    Sequence number (LE): 20992 (0x5200)
  ⊞ [No response seen]
  ⊞ Data (64 bytes)
```

```
0000  10 fe ed 54 57 e6 48 5d  60 98 e4 da 08 00 45 00   ...TW.H] `.....E.
0010  00 5c 2d 28 00 00 01 01  a2 ac c0 a0 00 68 3f f1   .\-(.... .....h?.
0020  e8 d3 08 00 f7 ac 00 01  00 52 00 00 00 00 00 00   ........ .R......
0030  00 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 00   ........ ........
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

File: "C:\Users\Артём\Desktop\1.pcap" 94 k... | Packets: 565 · Displayed: 135 (23,9%) · Load time: 0:00.015

```
tracert www.pa.gov
```

1) Мой IP-адрес: 192.160.0.104

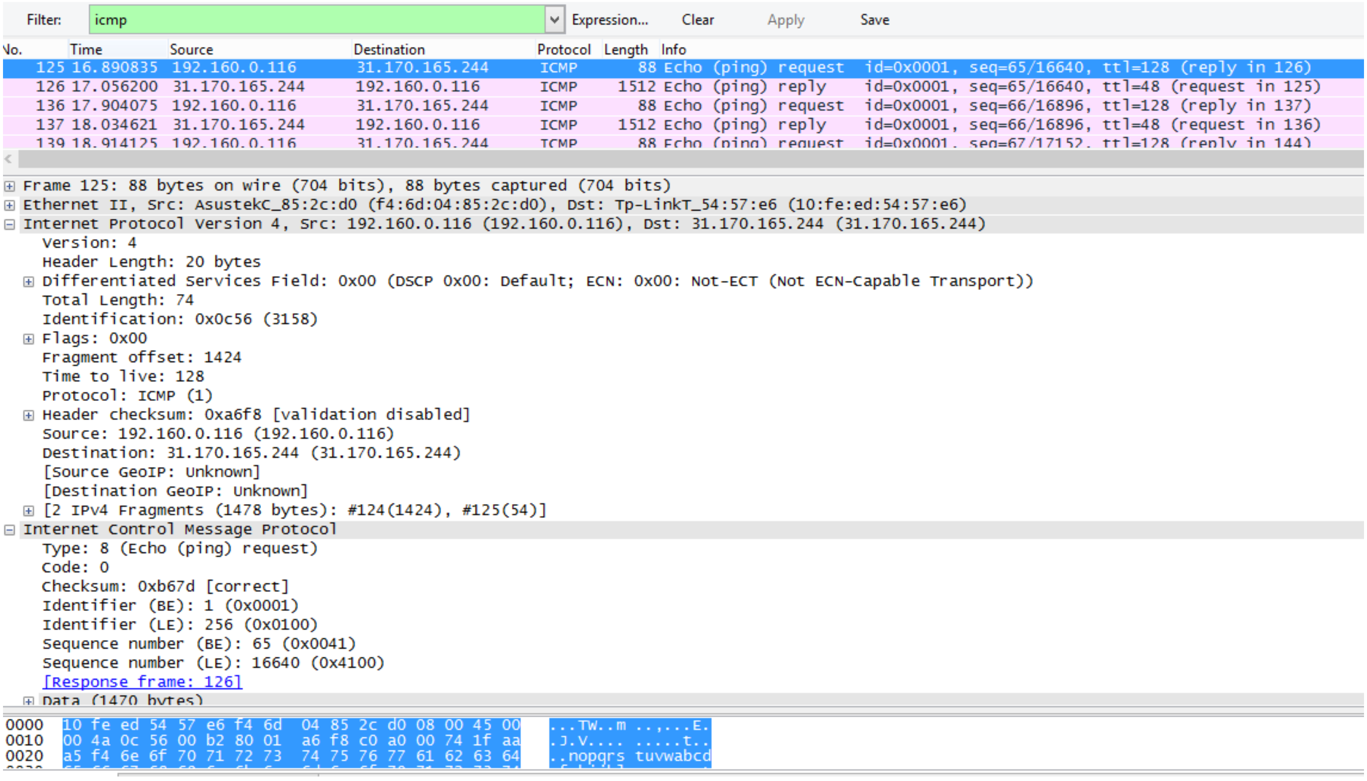
2) Protocol: ICMP

3) Header length: 20 bytes
Total length - header length = 92 - 20 = 72 bytes

4) Time to live: 1 данное поле инкрементируется на следующих ICMP Echo request (с повторением одного значения несколько раз)

5) Identification: 0x2d28 (11560)
Идентификатор - значение, назначаемое отправителем пакета и предназначенное для определения корректной последовательности фрагментов при сборке пакета.

Фрагментация пакетов



```
No.  Time       Source          Destination     Protocol Length Info
 125 16.890835  192.160.0.116   31.170.165.244  ICMP       88 Echo (ping) request  id=0x0001, seq=65/16640, ttl=128 (reply in 126)
 126 17.056200  31.170.165.244  192.160.0.116   ICMP     1512 Echo (ping) reply    id=0x0001, seq=65/16640, ttl=48 (request in 125)
 136 17.904075  192.160.0.116   31.170.165.244  ICMP       88 Echo (ping) request  id=0x0001, seq=66/16896, ttl=128 (reply in 137)
 137 18.034621  31.170.165.244  192.160.0.116   ICMP     1512 Echo (ping) reply    id=0x0001, seq=66/16896, ttl=48 (request in 136)
 139 18.914125  192.160.0.116   31.170.165.244  ICMP       88 Echo (ping) request  id=0x0001, seq=67/17152, ttl=128 (reply in 144)
```

```
⊞ Frame 125: 88 bytes on wire (704 bits), 88 bytes captured (704 bits)
⊞ Ethernet II, Src: AsustekC_85:2c:d0 (f4:6d:04:85:2c:d0), Dst: Tp-LinkT_54:57:e6 (10:fe:ed:54:57:e6)
⊟ Internet Protocol Version 4, Src: 192.160.0.116 (192.160.0.116), Dst: 31.170.165.244 (31.170.165.244)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 74
    Identification: 0x0c56 (3158)
  ⊞ Flags: 0x00
    Fragment offset: 1424
    Time to live: 128
    Protocol: ICMP (1)
  ⊞ Header checksum: 0xa6f8 [validation disabled]
    Source: 192.160.0.116 (192.160.0.116)
    Destination: 31.170.165.244 (31.170.165.244)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ⊞ [2 IPv4 Fragments (1478 bytes): #124(1424), #125(54)]
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xb67d [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 65 (0x0041)
    Sequence number (LE): 16640 (0x4100)
    [Response frame: 126]
  ⊞ Data (1470 bytes)
```

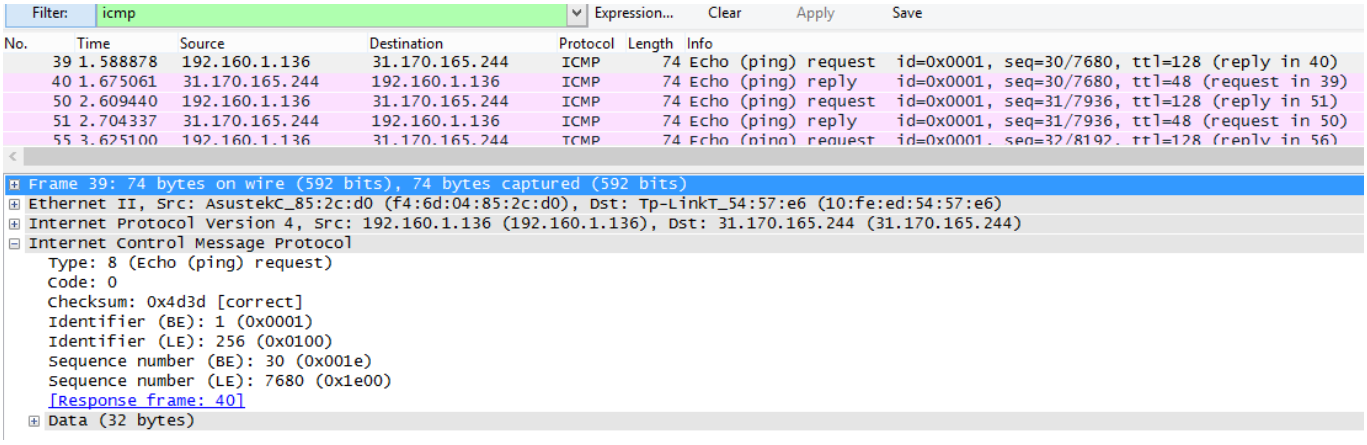
```
0000  10 fe ed 54 57 e6 f4 6d  04 85 2c d0 08 00 45 00   ...TW..m ..,...E.
0010  00 4a 0c 56 00 b2 80 01  a6 f8 c0 a0 00 74 1f aa   .J.V.... .....t..
0020  a5 f4 6e 6f 70 71 72 73  74 75 76 77 61 62 63 64   ..nopqrs tuvwabcd
```

ping -l 1470 4tochka.esy.es

1, 3) Фрагментация имеет место, на это указывает поле 2 IPv4 Fragments

2) В заголовке 3 бита флагов. Первый бит должен быть всегда равен нулю, второй бит DF (don't fragment) определяет возможность фрагментации пакета и трений бит MF (more fragments) показывает, не является ли этот пакет последним в цепочке пакетов.

Вариант 5. ICMP



```
No.   Time      Source          Destination     Protocol Length Info
   39 1.588878  192.160.1.136   31.170.165.244  ICMP     74 Echo (ping) request  id=0x0001, seq=30/7680, ttl=128 (reply in 40)
   40 1.675061  31.170.165.244  192.160.1.136   ICMP     74 Echo (ping) reply    id=0x0001, seq=30/7680, ttl=48 (request in 39)
   50 2.609440  192.160.1.136   31.170.165.244  ICMP     74 Echo (ping) request  id=0x0001, seq=31/7936, ttl=128 (reply in 51)
   51 2.704337  31.170.165.244  192.160.1.136   ICMP     74 Echo (ping) reply    id=0x0001, seq=31/7936, ttl=48 (request in 50)
   55 3.625100  192.160.1.136   31.170.165.244  ICMP     74 Echo (ping) request  id=0x0001, seq=32/8192, ttl=128 (reply in 56)

⊞ Frame 39: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
⊞ Ethernet II, Src: AsustekC_85:2c:d0 (f4:6d:04:85:2c:d0), Dst: Tp-LinkT_54:57:e6 (10:fe:ed:54:57:e6)
⊞ Internet Protocol Version 4, Src: 192.160.1.136 (192.160.1.136), Dst: 31.170.165.244 (31.170.165.244)
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d3d [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 30 (0x001e)
    Sequence number (LE): 7680 (0x1e00)
    [Response frame: 40]
  ⊞ Data (32 bytes)
```

`ping -n 10 4tochka.esy.es`

1) 20 пакетов, 10 запросов и 10 ответов

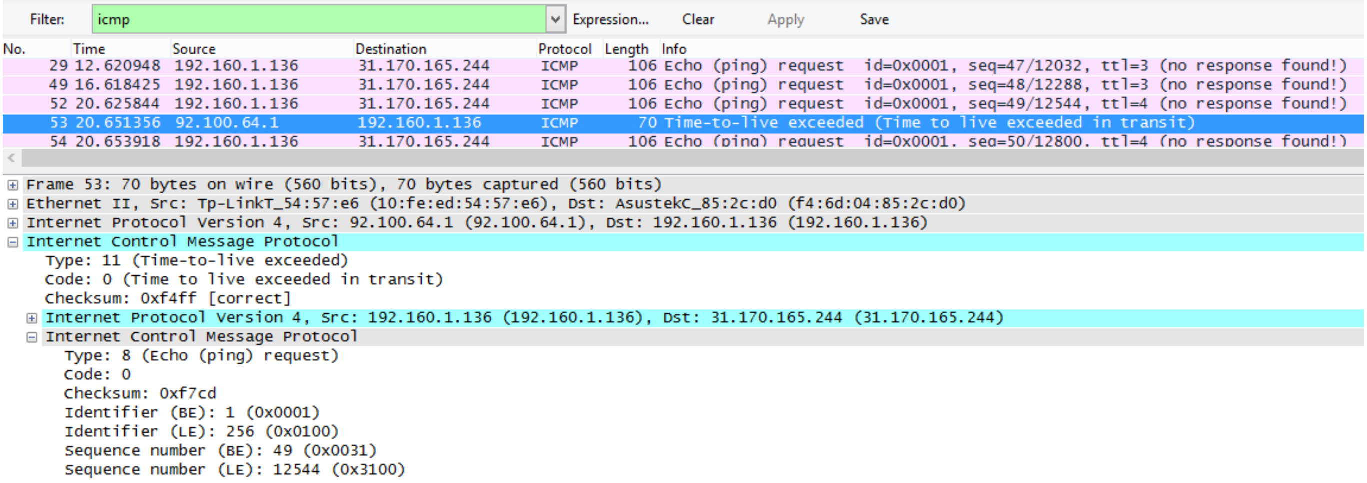
2) Мой ip 192.160.1.136. IP-адрес назначения: 31.170.165.244

3) Type: 8 Echo (ping) request Code: 0

Также содержит поля Checksum 2 байта, Identifier 2 байта, Sequence number 2 байта и поле Data 32 байта

4) Type: 0 Echo (ping) reply Code: 0

Также содержит поля Checksum 2 байта, Identifier 2 байта, Sequence number 2 байта и поле Data 32 байта



```
No.   Time       Source          Destination     Protocol Length Info
   29 12.620948  192.160.1.136   31.170.165.244  ICMP     106 Echo (ping) request  id=0x0001, seq=47/12032, ttl=3 (no response found!)
   49 16.618425  192.160.1.136   31.170.165.244  ICMP     106 Echo (ping) request  id=0x0001, seq=48/12288, ttl=3 (no response found!)
   52 20.625844  192.160.1.136   31.170.165.244  ICMP     106 Echo (ping) request  id=0x0001, seq=49/12544, ttl=4 (no response found!)
   53 20.651356  92.100.64.1     192.160.1.136   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   54 20.653918  192.160.1.136   31.170.165.244  ICMP     106 Echo (ping) request  id=0x0001, seq=50/12800, ttl=4 (no response found!)

⊞ Frame 53: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
⊞ Ethernet II, Src: Tp-LinkT_54:57:e6 (10:fe:ed:54:57:e6), Dst: AsustekC_85:2c:d0 (f4:6d:04:85:2c:d0)
⊞ Internet Protocol Version 4, Src: 92.100.64.1 (92.100.64.1), Dst: 192.160.1.136 (192.160.1.136)
⊟ Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
  ⊞ Internet Protocol Version 4, Src: 192.160.1.136 (192.160.1.136), Dst: 31.170.165.244 (31.170.165.244)
  ⊟ Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0xf7cd
      Identifier (BE): 1 (0x0001)
      Identifier (LE): 256 (0x0100)
      Sequence number (BE): 49 (0x0031)
      Sequence number (LE): 12544 (0x3100)
```

`tracert 4tochka.esy.es`

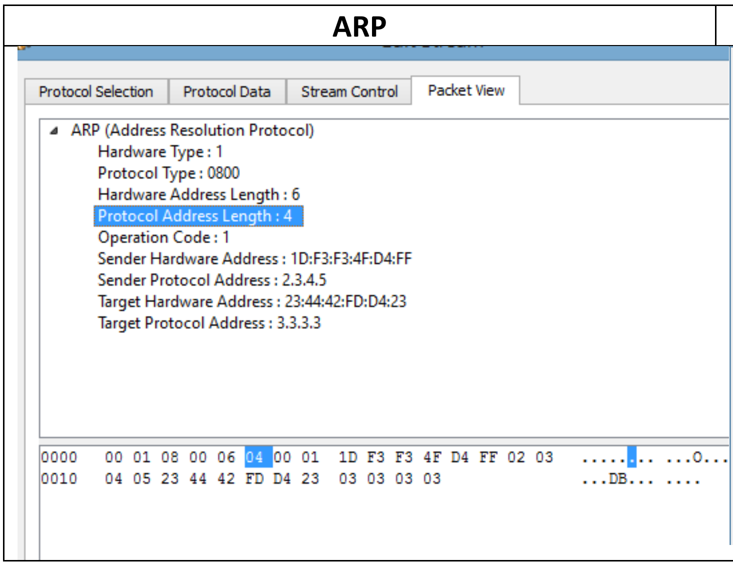
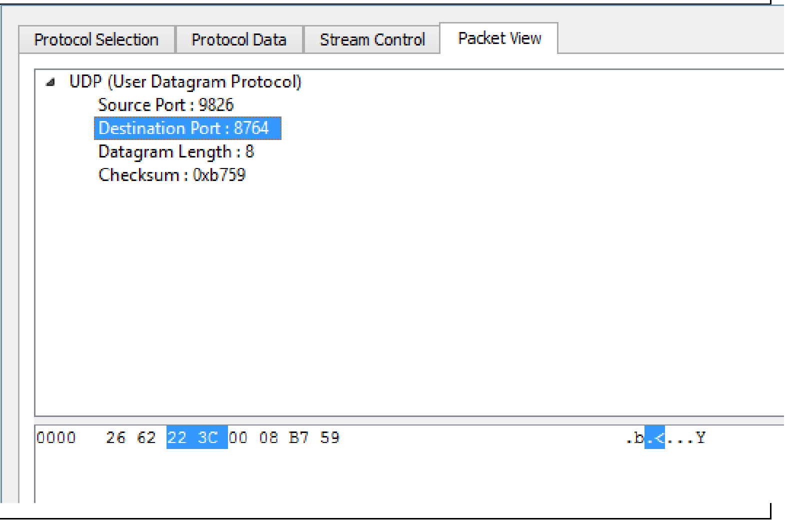
1) Мой IP 192.160.1.136 IP назначения: 31.170.165.244

2) Отличаются размером данных. Здесь Data занимает 64 байта.

3) Например, Time exceeded. Type - 11 (TTL exceeded). Code: 0 (в процессе передачи дейтаграммы поле TTL приняло значение 0).

ICMP Error содержит в общем случае Type, Code, Checksum, а дальше уже в зависимости от ошибки

Часть 2. Исследование структуры сетевых пакетов с помощью генератора пакетов Ostinato

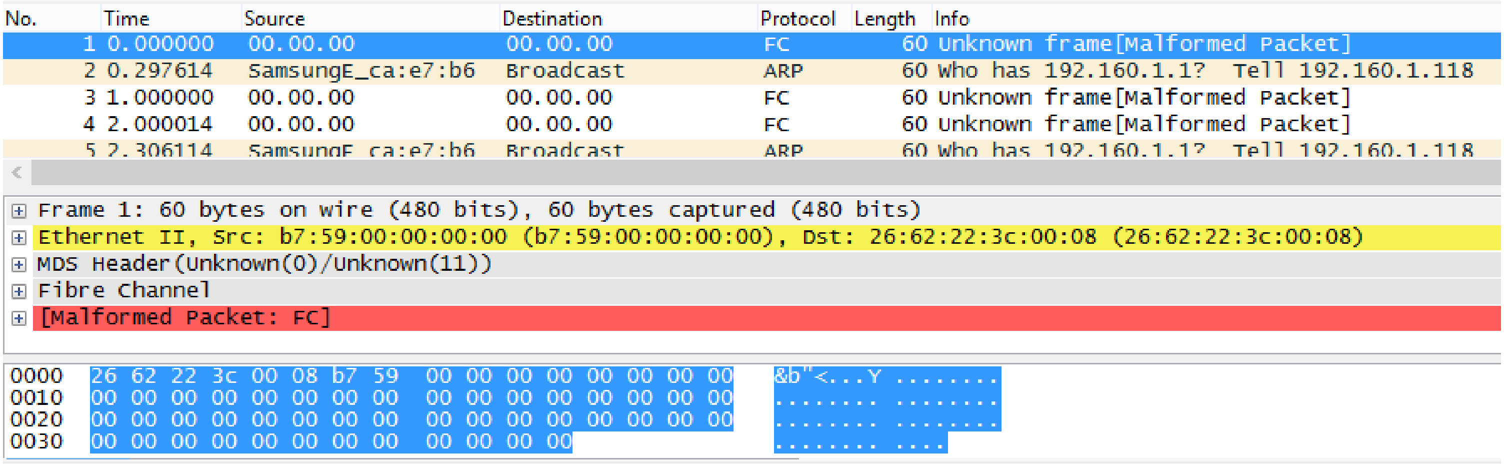
ARP	UDP
	

Protocol Selection | Protocol Data | Stream Control | Packet View

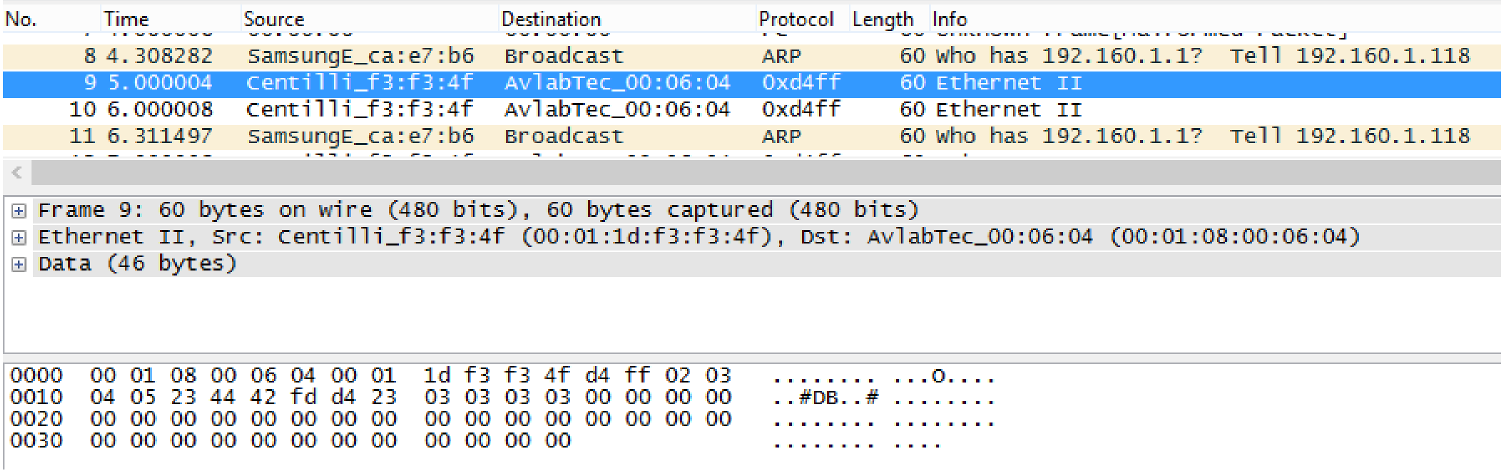
```
◢ ARP (Address Resolution Protocol)
      Hardware Type : 1
      Protocol Type : 0800
      Hardware Address Length : 6
      Protocol Address Length : 4
      Operation Code : 1
      Sender Hardware Address : 1D:F3:F3:4F:D4:FF
      Sender Protocol Address : 2.3.4.5
      Target Hardware Address : 23:44:42:FD:D4:23
      Target Protocol Address : 3.3.3.3

0000   00 01 08 00 06 04 00 01  1D F3 F3 4F D4 FF 02 03   ........ ...O...
0010   04 05 23 44 42 FD D4 23  03 03 03 03               ...DB... ....
```

Protocol Selection | Protocol Data | Stream Control | Packet View

```
◢ UDP (User Datagram Protocol)
      Source Port : 9826
      Destination Port : 8764
      Datagram Length : 8
      Checksum : 0xb759

0000   26 62 22 3C 00 08 B7 59                            .b.<...Y
```



```
No.  Time      Source             Destination  Protocol Length Info
   1 0.000000  00.00.00           00.00.00     FC          60 Unknown frame[Malformed Packet]
   2 0.297614  SamsungE_ca:e7:b6  Broadcast    ARP         60 Who has 192.160.1.1?  Tell 192.160.1.118
   3 1.000000  00.00.00           00.00.00     FC          60 Unknown frame[Malformed Packet]
   4 2.000014  00.00.00           00.00.00     FC          60 Unknown frame[Malformed Packet]
   5 2.306114  SamsungE_ca:e7:b6  Broadcast    ARP         60 Who has 192.160.1.1?  Tell 192.160.1.118

⊞ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊞ Ethernet II, Src: b7:59:00:00:00:00 (b7:59:00:00:00:00), Dst: 26:62:22:3c:00:08 (26:62:22:3c:00:08)
⊞ MDS Header(Unknown(0)/Unknown(11))
⊞ Fibre Channel
⊞ [Malformed Packet: FC]

0000  26 62 22 3c 00 08 b7 59  00 00 00 00 00 00 00 00   &b"<...Y ........
0010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```



```
No.  Time      Source              Destination         Protocol Length Info
   8 4.308282  SamsungE_ca:e7:b6   Broadcast           ARP         60 Who has 192.160.1.1?  Tell 192.160.1.118
   9 5.000004  Centilli_f3:f3:4f   AvlabTec_00:06:04   0xd4ff      60 Ethernet II
  10 6.000008  Centilli_f3:f3:4f   AvlabTec_00:06:04   0xd4ff      60 Ethernet II
  11 6.311497  SamsungE_ca:e7:b6   Broadcast           ARP         60 Who has 192.160.1.1?  Tell 192.160.1.118

⊞ Frame 9: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊞ Ethernet II, Src: Centilli_f3:f3:4f (00:01:1d:f3:f3:4f), Dst: AvlabTec_00:06:04 (00:01:08:00:06:04)
⊞ Data (46 bytes)

0000  00 01 08 00 06 04 00 01  1d f3 f3 4f d4 ff 02 03   ........ ...O....
0010  04 05 23 44 42 fd d4 23  03 03 03 03 00 00 00 00   ..#DB..# ........
0020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

Sequential Streams отличается от **Interleaved Streams** тем, что в первом случае сначала будут отправлены все пакеты первого протокола, а затем пакеты второго протокола. Во втором случае пакеты чередуются при передаче.

В Wireshark протокол посылаемых пакетов определяется неправильно, т.к. пропущены некоторые уровни сетевой модели. UDP – это протокол 4 (транспортного) уровня, а ARP – 2 (канального).