

# Назначение

1. Выберите первый сегмент UDP в вашей трассировке. Какой номер пакета этого сегмента в файле трассировки? Какой тип полезной нагрузки прикладного уровня или сообщения протокола передаются в этом сегменте UDP?

Посмотрите подробности этого пакета в Wireshark. Сколько полей в заголовке UDP? Как называются эти поля?

```
ptrvsrg@acer:~$ sudo wireshark
ptrvsrg@acer ~$ nslookup www.nyu.edu
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
www.nyu.edu canonical name = d1q5ku5vnwkd2k.cloudfront.net.
Name:   d1q5ku5vnwkd2k.cloudfront.net
Address: 13.33.243.62
Name:   d1q5ku5vnwkd2k.cloudfront.net
Address: 13.33.243.111
Name:   d1q5ku5vnwkd2k.cloudfront.net
Address: 13.33.243.38
Name:   d1q5ku5vnwkd2k.cloudfront.net
Address: 13.33.243.83
Name:   d1q5ku5vnwkd2k.cloudfront.net
Address: 2600:9000:2118:3200:1:f7e2:cb00:93a1
Name:   d1q5ku5vnwkd2k.cloudfront.net
Address: 2600:9000:2118:3c00:1:f7e2:cb00:93a1
Name:   d1q5ku5vnwkd2k.cloudfront.net
Address: 2600:9000:2118:4a00:1:f7e2:cb00:93a1
Name:   d1q5ku5vnwkd2k.cloudfront.net
Address: 2600:9000:2118:5400:1:f7e2:cb00:93a1
Name:   d1q5ku5vnwkd2k.cloudfront.net
Address: 2600:9000:2118:8200:1:f7e2:cb00:93a1
Name:   d1q5ku5vnwkd2k.cloudfront.net
Address: 2600:9000:2118:b000:1:f7e2:cb00:93a1
Name:   d1q5ku5vnwkd2k.cloudfront.net
Address: 2600:9000:2118:1600:1:f7e2:cb00:93a1
Name:   d1q5ku5vnwkd2k.cloudfront.net
Address: 2600:9000:2118:1c00:1:f7e2:cb00:93a1
```

Wireshark · Packet 31 · UDP\_wireshark\_file.pcapng

▶ Frame 31: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface wlp2s0, id 0  
▶ Ethernet II, Src: IntelCor\_9c:9f:e1 (f0:57:a6:9c:9f:e1), Dst: Tp-LinkT\_7e:93:dd (68:ff:7b:7e:93:dd)  
▶ Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.1

▼ User Datagram Protocol, Src Port: 35331, Dst Port: 53

Source Port: 35331  
Destination Port: 53  
Length: 48  
Checksum: 0x6d7f [unverified]  
[Checksum Status: Unverified]  
[Stream index: 3]  
▶ [Timestamps]  
UDP payload (40 bytes)

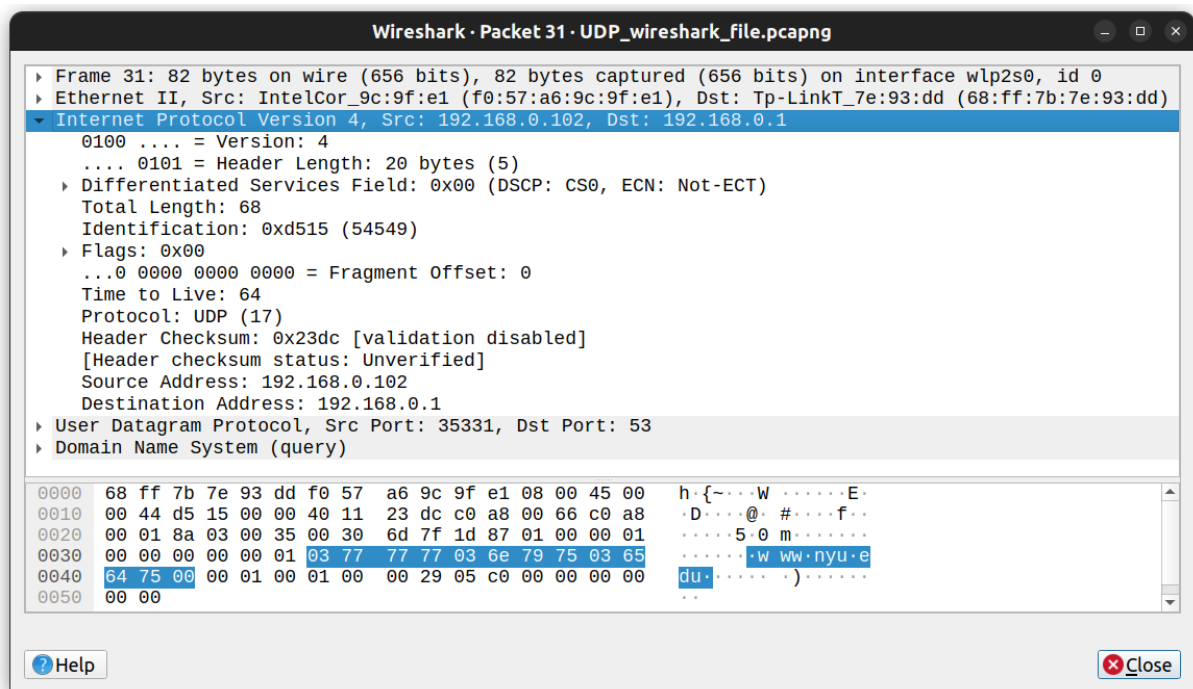
▼ Domain Name System (query)

Transaction ID: 0x1d87  
▶ Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 1  
▼ Queries  
▶ www.nyu.edu: type A, class IN  
▶ Additional records  
[\[Response In: 32\]](#)

0000	68 ff 7b 7e 93 dd f0 57 a6 9c 9f e1 08 00 45 00	h·{~·W ····E·
0010	00 44 d5 15 00 00 40 11 23 dc c0 a8 00 66 c0 a8	·D····@· #···f·
0020	00 01 8a 03 00 35 00 30 6d 7f 1d 87 01 00 00 01	···5·0 m·
0030	00 00 00 00 00 01 03 77 77 77 03 6e 79 75 03 65	·····w ww·nyu·e
0040	64 75 00 00 01 00 01 00 00 29 05 c0 00 00 00 00	du······)·
0050	00 00	··

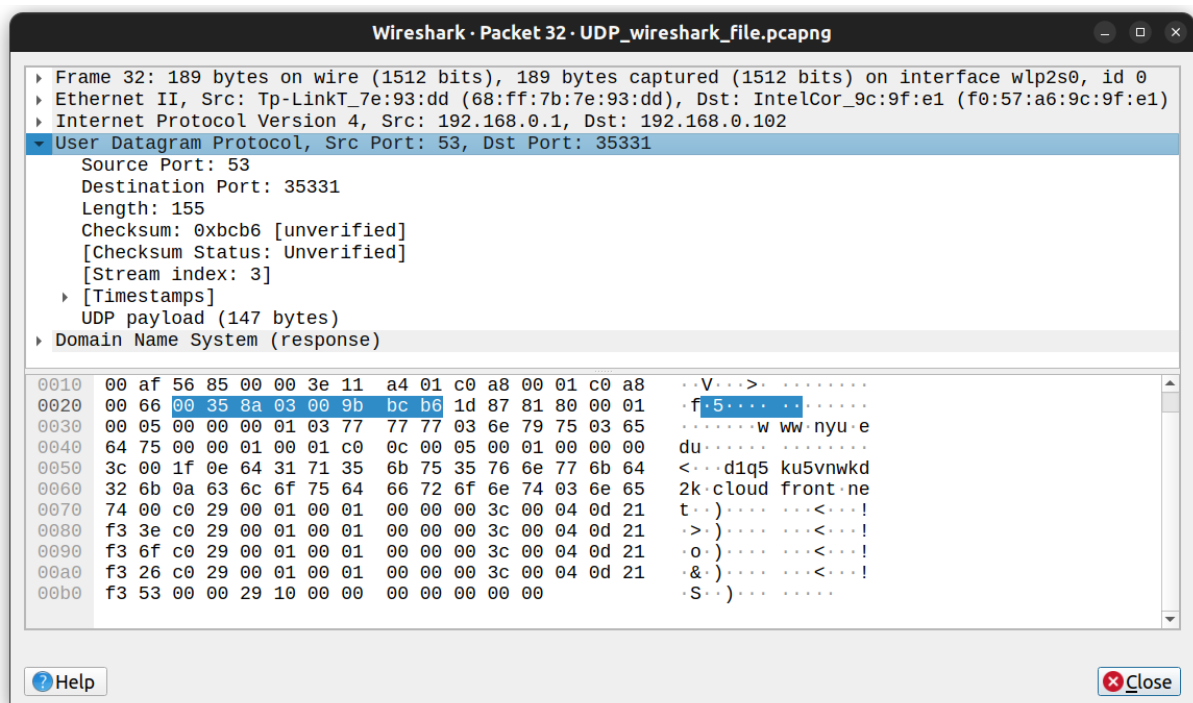
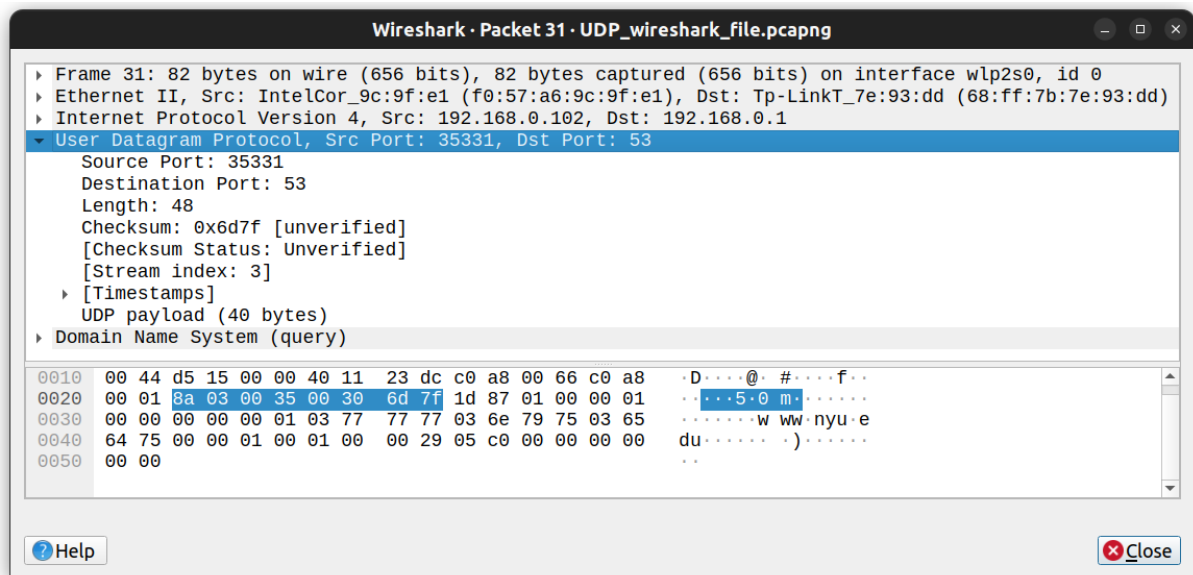
Help Close

- Номер пакета - 31
  - Тип полезной нагрузки сегмента UDP - DNS запись типа A
  - В заголовке UDP пакета 4 поля: порты источника и назначения, размер сегмента и контрольная сумма
2. Изучив отображаемую информацию в поле содержимого пакета Wireshark для этого пакета, какова длина (в байтах) каждого из полей заголовка UDP?
    - Длина каждого из полей заголовка UDP - 2 байта
  3. Значение в поле *Length* - это длина чего? Подтвердите свое утверждение с помощью захваченного UDP-пакета.
    - Значение в поле *Length* - это размер UDP сегмента (заголовок + размер полезной нагрузки). Подтверждается это тем, что сумма размера UDP заголовка (8 байтов) и размера записи DNS (40 байтов) равна значению в поле *Length* (48 байтов)
  4. Какое максимальное количество байтов может быть включено в полезную нагрузку UDP?
    - Размер поля *Length* - 2 байта. Значит, максимальный размер полезной нагрузки равен максимальному значению поля *Length* без учёта размера UDP заголовка, т.е.  $2^{16} - 1 - 8 = 65527$  байтов
  5. Каков максимально возможный номер исходного порта?
    - Размер поля *Source Port* - 2 байта. Значит, максимальный номер порта равен  $2^{16} - 1 = 65535$
  6. Какой номер протокола для UDP? Дайте ответ в десятичной системе счисления.



- Номер протокола для UDP - 17
7. Изучите пару пакетов UDP, в которых ваш хост отправляет первый пакет UDP, а второй пакет UDP является ответом на этот первый пакет UDP. Какой номер

пакета первого из этих двух сегментов UDP в файле трассировки? Какой номер пакета второго из этих двух сегментов UDP в файле трассировки? Опишите взаимосвязь между номерами портов в двух пакетах.



- Номер пакета первого из этих двух сегментов UDP - 31
- Номер пакета второго из этих двух сегментов UDP - 32
- Порт назначения первого сегмента является портом источника второго сегмента, и порт источника первого сегмента является портом назначения второго сегмента