

HW7

1

The image shows a Wireshark packet capture window titled "*Ethernet". The filter bar at the top is set to "udp". The packet list shows several DNS packets. Packet 11 is selected, showing details for a DNS Standard query from 192.168.1.63 to 192.168.1.1. The details pane shows the User Datagram Protocol (UDP) section with Source Port: 64460, Destination Port: 53, Length: 50, and Checksum: 0x83d4 [unverified]. The UDP payload is a Domain Name System (query) packet. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
11	0.777796	192.168.1.63	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.
12	0.789403	192.168.1.1	192.168.1.63	DNS	84	Standard query response 0x0001 No such name PT
13	0.791465	192.168.1.63	192.168.1.1	DNS	74	Standard query 0x0002 A www.google.com
14	0.792892	192.168.1.1	192.168.1.63	DNS	170	Standard query response 0x0002 A www.google.co
15	0.796153	192.168.1.63	192.168.1.1	DNS	74	Standard query 0x0003 AAAA www.google.com
16	0.804467	192.168.1.1	192.168.1.63	DNS	186	Standard query response 0x0003 AAAA www.google

Frame 11: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{45939136-950B-4A86-B5D2-5B48}

Ethernet II, Src: HewlettP_0e:f2:25 (84:a9:3e:0e:f2:25), Dst: Keenetic_1e:95:c8 (50:ff:20:1e:95:c8)

Internet Protocol Version 4, Src: 192.168.1.63, Dst: 192.168.1.1

User Datagram Protocol, Src Port: 64460, Dst Port: 53

Source Port: 64460

Destination Port: 53

Length: 50

Checksum: 0x83d4 [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

[Timestamps]

UDP payload (42 bytes)

Domain Name System (query)

0010 00 46 65 91 00 00 40 11 00 00 c0 a8 01 3f c0 a8 .Fe...@.?..

0020 01 01 fb cc 00 35 00 32 83 d4 00 01 01 00 00 015.2

0030 00 00 00 00 00 00 01 31 01 31 03 31 36 38 03 311 .1.168.1

0040 39 32 07 69 6e 2d 61 64 64 72 04 61 72 70 61 00 92.in-ad dr.arpa.

0050 00 0c 00 01

wireshark_Ethernet500ML1.pcapng || Пакеты: 33 · Показаны: 6 (18.2%) || Профиль: Default

4 поля:

Source Port: 64460

Destination Port: 53

Length: 50

Checksum: 0x83d4 [unverified]

Длина каждого поля 2 байта

Length = 8 (заголовок) + 42 (данные)

Length - 16-битное число, значит не больше $2^{16} - 1 - 8 = 65527$ (так как заголовок тоже учитывается)

Port тоже 16-битное число, то есть до $2^{16} - 1$

```

0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 70
  Identification: 0x6591 (26001)
> Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.63
  Destination Address: 192.168.1.1
▼ User Datagram Protocol, Src Port: 64460, Dst Port: 53
  Source Port: 64460
  Destination Port: 53

```

0010	00 46 65 91 00 00 40 11	00 00 c0 a8 01 3f c0 a8	Fe...@... ..?
0020	01 01 fb cc 00 35 00 32	83 d4 00 01 01 00 00 01	...5.2
0030	00 00 00 00 00 00 01 31	01 31 03 31 36 38 03 311 .1.168.1
0040	39 32 07 69 6e 2d 61 64	64 72 04 61 72 70 61 00	92.in-ad dr.arpa
0050	00 0c 00 01	

Protocol (ip.proto), 1 byte(s) | Пакеты: 33 · Показаны: 6 (18.2%) | Профиль: Default

Номер протокола 17 в десятичной или 11 в шестнадцатеричной

*Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

udp

No.	Time	Source	Destination	Protocol	Length	Info
11	0.777796	192.168.1.63	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.
12	0.789403	192.168.1.1	192.168.1.63	DNS	84	Standard query response 0x0001 No such name PT
13	0.791465	192.168.1.63	192.168.1.1	DNS	74	Standard query 0x0002 A www.google.com
14	0.792892	192.168.1.1	192.168.1.63	DNS	170	Standard query response 0x0002 A www.google.co
15	0.796153	192.168.1.63	192.168.1.1	DNS	74	Standard query 0x0003 AAAA www.google.com
16	0.804467	192.168.1.1	192.168.1.63	DNS	186	Standard query response 0x0003 AAAA www.google

```

Total Length: 70
Identification: 0x58d3 (22739)
> Flags: 0x40, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
  Header Checksum: 0x5e43 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.1
  Destination Address: 192.168.1.63
▼ User Datagram Protocol, Src Port: 53, Dst Port: 64460
  Source Port: 53
  Destination Port: 64460
  Length: 50
  Checksum: 0x73f7 [unverified]
  [Checksum Status: Unverified]

```

0010	00 46 58 d3 40 00 40 11	5e 43 c0 a8 01 01 c0 a8	FX...@... ^C.....
0020	01 3f 00 35 fb cc 00 32	73 f7 00 01 80 83 00 01	...5...2 s.....
0030	00 00 00 00 00 00 01 31	01 31 03 31 36 38 03 311 .1.168.1
0040	39 32 07 69 6e 2d 61 64	64 72 04 61 72 70 61 00	92.in-ad dr.arpa
0050	00 0c 00 01	

Source Port (udp.srcport), 2 byte(s) | Пакеты: 33 · Показаны: 6 (18.2%) · Потеряно: 0 (0.0%) | Профиль: Default

В ответном пакете
Source Port: 53

Destination Port: 64460

То есть порты поменялись местами