

Лабораторная работа. Исследование трафика DNS

Задачи

- Часть 1. Перехват трафика DNS
- Часть 2. Изучение трафика DNS-запроса
- Часть 3. Изучение трафика DNS-ответа

Общие сведения и сценарий

Wireshark — средство перехвата и анализа пакетов с открытым исходным кодом. Wireshark дает подробную информацию о стеке сетевых протоколов. Wireshark позволяет фильтровать трафик для поиска и устранения неполадок сети, изучения проблем безопасности и анализа сетевых протоколов. Wireshark позволяет просматривать сведения о пакетах, поэтому злоумышленник может использовать программу как разведывательное средство.

В этой лабораторной работе вы установите программу Wireshark в системе Windows для фильтрации пакетов DNS и просмотра информации как о пакетах запросов, так и ответов DNS.

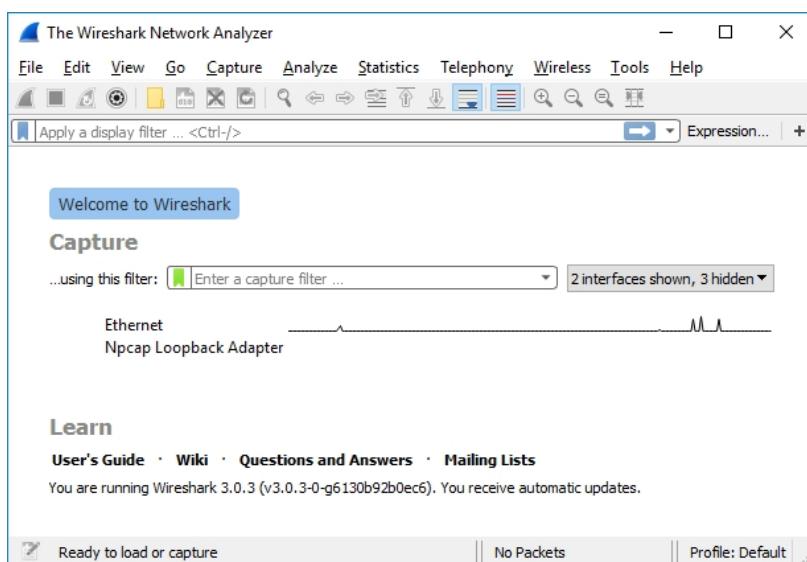
Необходимые ресурсы

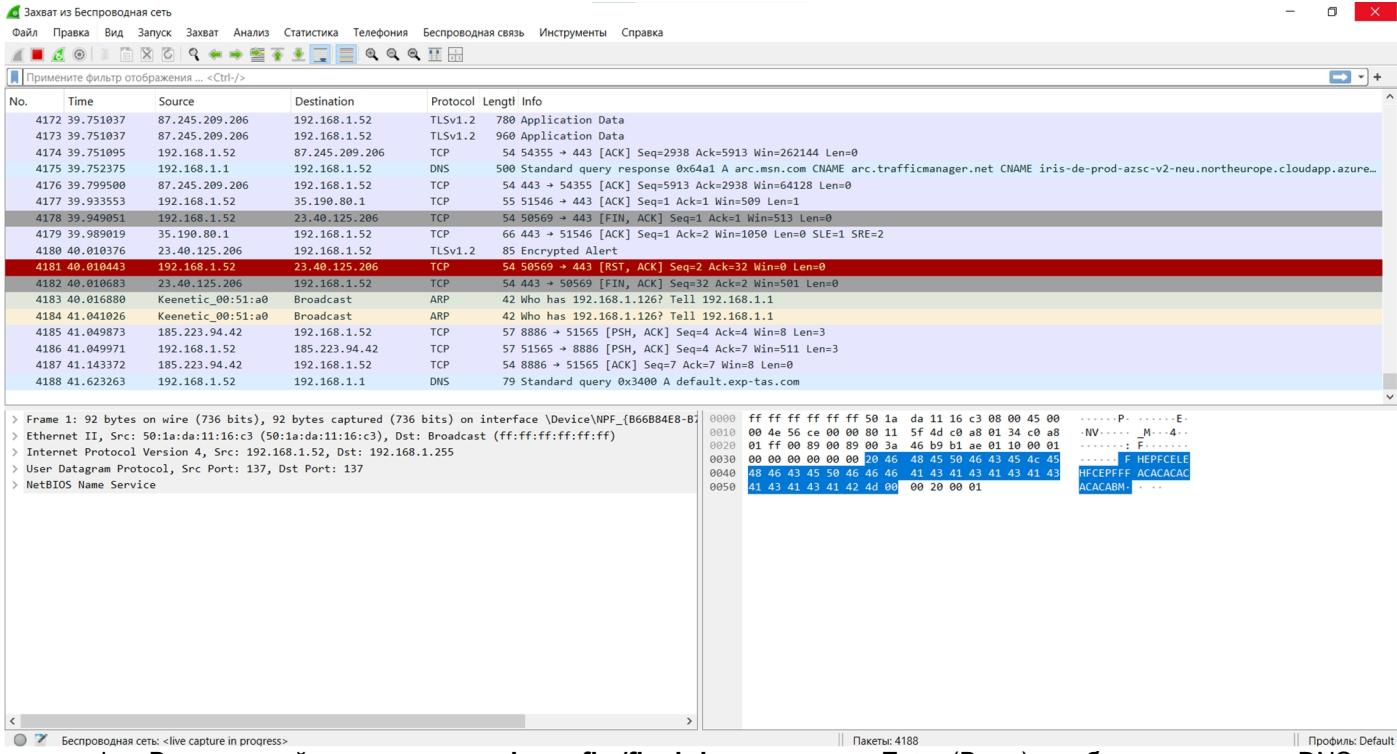
- 1 ПК с Windows, доступом в Интернет и установленной программой Wireshark

Инструкции

Шаг 1. Перехват трафика DNS

- a. Откройте **Wireshark** и начните захват данных программой Wireshark, дважды щелкнув по сетевому интерфейсу с трафиком.





b. В командной строке введите **ipconfig /flushdns** и нажмите Enter (Ввод), чтобы очистить кеш DNS.

Microsoft Windows [Version 10.0.19045.5555]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\Jake>ipconfig /flushdns

Настройка протокола IP для Windows

Кэш сопоставителя DNS успешно очищен.

C:\Users\Jake>

Лабораторная работа. Исследование трафика DNS

```
C:\Users\Student> ipconfig /flushdns
```

Настройка IP для Windows

Успешно сброшен кэш DNS клиента.

- c. Введите **nslookup** в ответ на приглашение войти в интерактивный режим.
- d. Введите доменное имя веб-сайта. В данном примере используется доменное имя www.cisco.com. В командной строке введите **www.cisco.com**.

```
C:\Users\Student> nslookup
```

Сервер по умолчанию: неизвестно

Address: 68.105.28.16

```
>www.cisco.com
```

Сервер: неизвестно

Address: 68.105.28.16

Не заслуживающий доверия ответ:

Name: e2867.dsca.akamaiedge.net

Addresses: 2001:578:28:68d::b33

 2001:578:28:685::b33

 96.7.79.147

Псевдонимы: www.cisco.com

 www.cisco.com.akadns.net

 wwwds.cisco.com.edgekey.net

 wwwds.cisco.com.edgekey.net.globalredir.akadns.net

- e. После завершения введите **exit**, чтобы выйти из интерактивного режима nslookup. Закройте командную строку.
- f. Щелкните **Stop capturing packets** (Остановить перехват пакетов), чтобы остановить захват данных программой Wireshark.

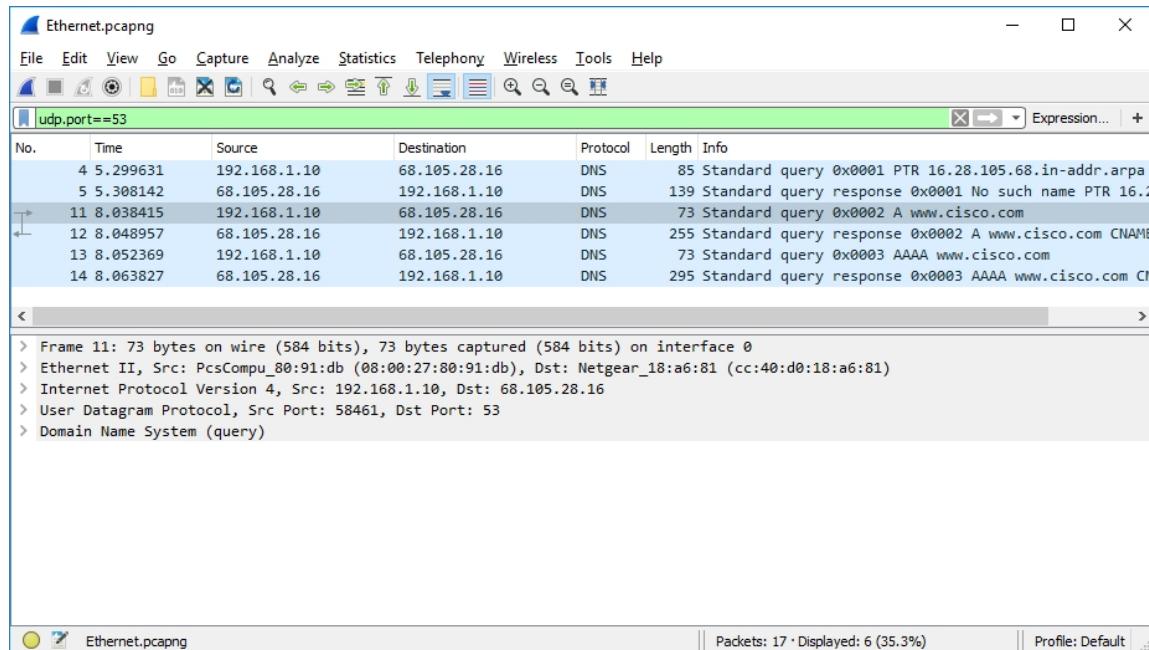
```
its> www.cisco.com
TrXЕтХЕ: UnKnown
Address: 192.168.1.1
S
Не заслуживающий доверия ответ:
Name : e2867.dsca.akamaiedge.net
Addresses: 2001:2030:21:1ae::b33
              2001:2030:21:187::b33
              2001:2030:21:1b1::b33
              2.23.145.12
Aliases: www.cisco.com
              www.cisco.com.akadns.net
              wwwds.cisco.com.edgekey.net
              wwwds.cisco.com.edgekey.net.globalredir.akadns.net
>
```

Шаг 2. Изучение трафика DNS-запроса

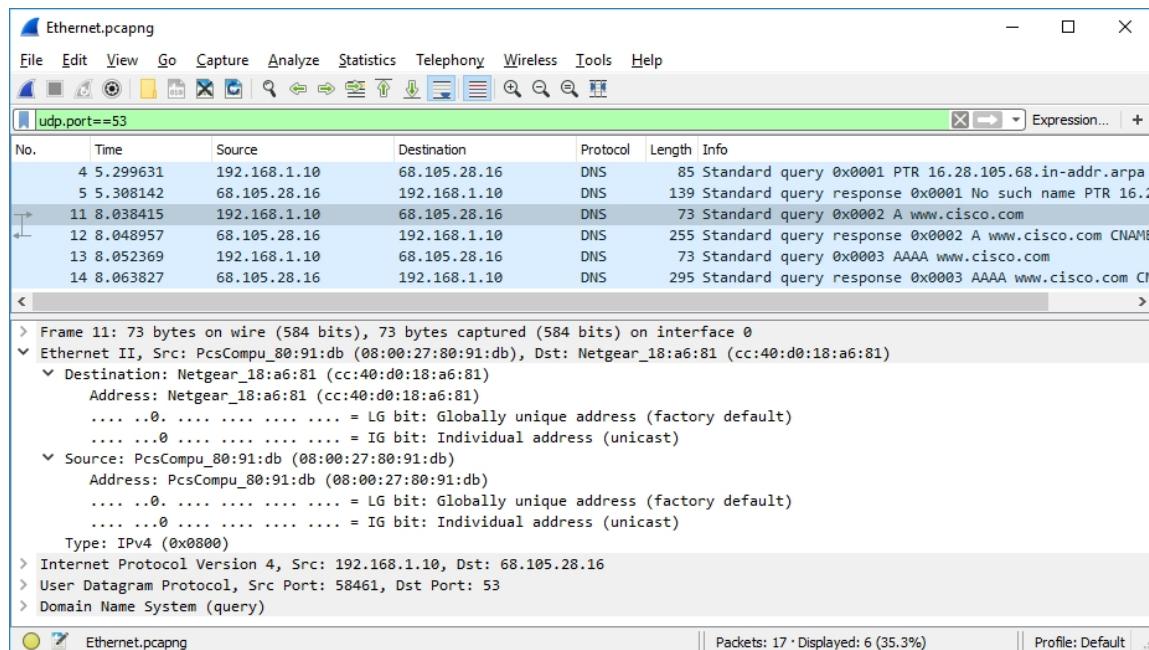
- a. Наблюдайте за трафиком, захваченным в области списка пакетов Wireshark. Введите **udp.port == 53** в поле фильтра и нажмите стрелку (или кнопку Enter) для показа только пакетов DNS.
- b. Выберите пакет DNS с маркировкой **Standard query 0x0002 A www.cisco.co** (Стандартный запрос 0x0002 A www.cisco.com).

Лабораторная работа. Исследование трафика DNS

В области сведений о пакетах обратите внимание, что этот пакет имеет следующие сведения: Ethernet II, протокол IPv4, протокол UDP и систему доменных имен (запрос).



c. Разверните Ethernet II для просмотра сведений. Наблюдайте за полями источника и назначения.



Назовите MAC-адреса источника и назначения. С какими сетевыми интерфейсами связаны эти MAC-адреса?

Лабораторная работа. Исследование трафика DNS

Ethernet II, Src: 50:1a:da:11:16:c3 (50:1a:da:11:16:c3), Dst: Keenetic_00:51:a0 (50:ff:20:00:51:a0)
 > Destination: Keenetic_00:51:a0 (50:ff:20:00:51:a0)
 > Source: 50:1a:da:11:16:c3 (50:1a:da:11:16:c3)
 Type: IPv4 (0x0800)
 [Stream index: 0]

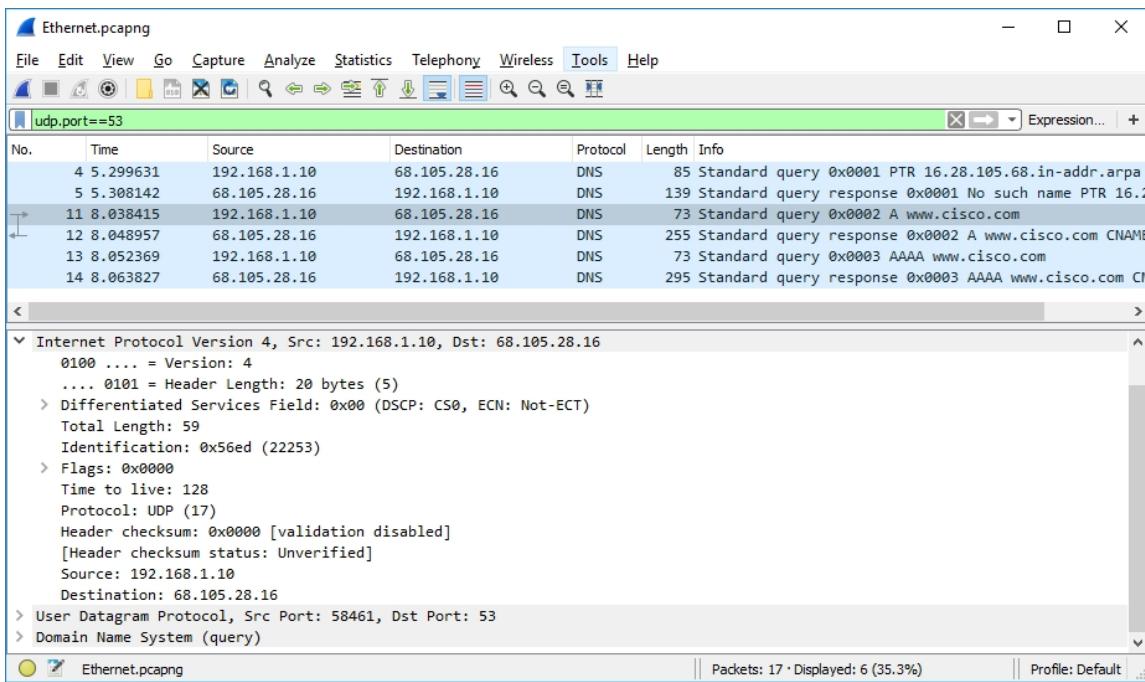
Interface id: 0 (\Device\NPF_{B66B84E8-B701-4D10-B44A-0EDEBA5EAABA})

Interface name: \Device\NPF_{B66B84E8-B701-4D10-B44A-0EDEBA5EAABA}

Interface description: Беспроводная сеть

Лабораторная работа. Исследование трафика DNS

Раскройте Internet Protocol Version 4 (Протокол IPv4). Наблюдайте за IPv4-адресами источника и назначения.

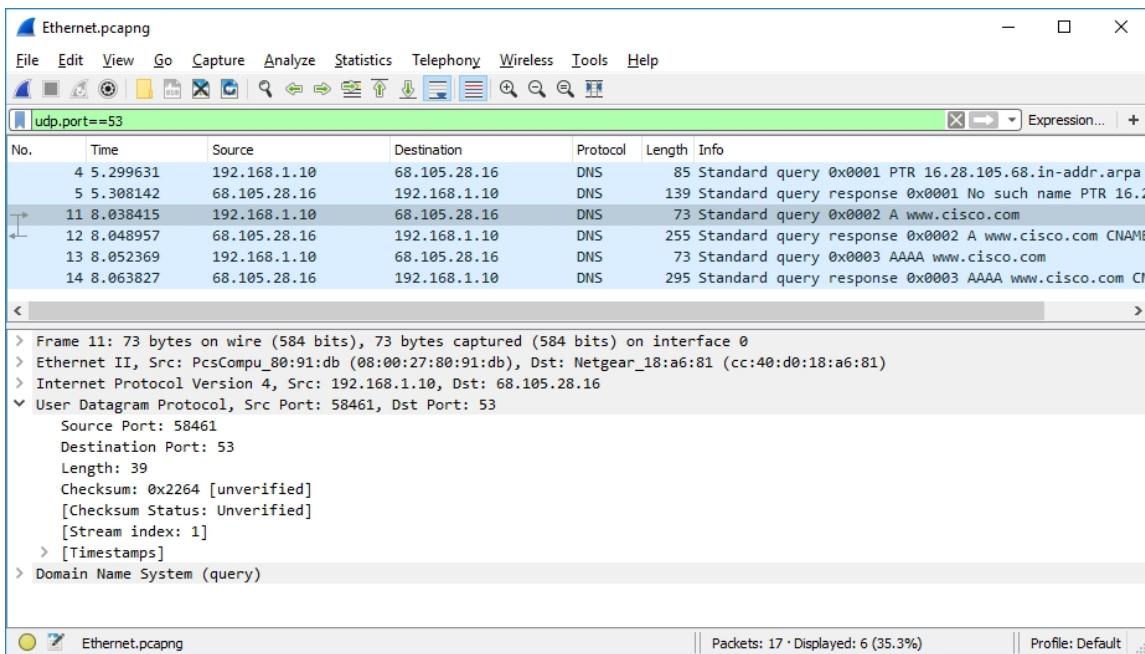


Назовите IP-адреса источника и назначения. С какими сетевыми интерфейсами связаны эти IP-адреса?

Source Address: 192.168.1.52
Destination Address: 192.168.1.1

Лабораторная работа. Исследование трафика DNS

- a. Раскройте **User Datagram Protocol** (Протокол UDP). Наблюдайте за портами источника и назначения.



Назовите порты источника и назначения. Назовите номер порта DNS по умолчанию.

Source Port: 53116

Destination Port: 53

Номер dns - 53

- b. Откройте командную строку и введите **arp -a** и **ipconfig /all** для записи MAC- и IP-адресов компьютера.

C:\Users\Student> **arp -a**

```
Interface: 192.168.1.10 --- 0x4
  Internet Address Physical Address Type
    192.168.1.1 cc-40-d0-18-a6-81 dynamic
    192.168.1.122 b0-a7-37-46-70-bb dynamic
    192.168.1.255 ff-ff-ff-ff-ff-ff static
    224.0.0.22 01-00-5e-00-00-16 static
    224.0.0.252 01-00-5e-00-00-fc static
    239.255.255.250 01-00-5e-7f-ff-fa static
    255.255.255.255 ff-ff-ff-ff-ff-ff static
```

C:\Users\Student> **ipconfig /all**

Настройка IP для Windows

Лабораторная работа. Исследование трафика DNS

Host Name : DESKTOP

Основной DNS-суффикс. :

Лабораторная работа. Исследование трафика DNS

```
Node Type . . . . . : Гибрид
Включена IP-маршрутизация. . . . . : Нет
Включен WINS-прокси. . . . . : Нет
```

Ethernet adapter Ethernet:

```
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-80-91-DB
DHCP Enabled. . . . . : Да
Автонастройка включена . . . . . : Да
Link-local IPv6-адрес. . . . . : fe80::d829:6d18:e229:a705%4 (Preferred)
IPv4 Address. . . . . : 192.168.1.10 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
Аренда получена. . . . . : Tuesday, August 20, 2019 5:39:51 PM
Аренда истекает . . . . . : Wednesday, August 21, 2019 5:39:50 PM
Default Gateway . . . . . : 192.168.1.1
DHCP-сервер . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 50855975
DHCPv6 Client DUID. . . . . : 00-01-00-01-24-21-BA-64-08-00-27-80-91-DB
DNS-серверы . . . . . : 68.105.28.16
                                         68.105.29.16
NetBios через TCP/IP. . . . . : Включен
```

Сравните MAC- и IP-адреса в результатах программы Wireshark с результатами из ipconfig/all.
Каковы ваши наблюдения?

Адаптер беспроводной локальной сети Беспроводная сеть:

```
DNS-суффикс подключения . . . . . :
Описание. . . . . : MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
Физический адрес. . . . . : 50-1A-DA-11-16-C3
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . . . : fe80::2d20:8a4f:aa04:cb59%20 (Основной)
IPv4-адрес. . . . . : 192.168.1.52 (Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена. . . . . : 11 марта 2025 г. 4:48:02
Срок аренды истекает. . . . . : 11 марта 2025 г. 11:48:00
Основной шлюз. . . . . : 192.168.1.1
DHCP-сервер. . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 496035944
DUID клиента DHCPv6 . . . . . : 00-01-00-01-2C-E9-91-27-04-42-1A-A2-4D-5A
DNS-серверы. . . . . : 192.168.1.1
NetBios через TCP/IP. . . . . : Включен
```

Лабораторная работа. Исследование трафика DNS

Интерфейс: 192.168.40.1 --- 0xс

адрес в Интернете	Физический адрес	Тип
192.168.40.255	ff-ff-ff-ff-ff-ff	статический
224.0.0.2	01-00-5e-00-00-02	статический
224.0.0.22	01-00-5e-00-00-16	статический
224.0.0.251	01-00-5e-00-00-fb	статический
224.0.0.252	01-00-5e-00-00-fc	статический
230.0.0.1	01-00-5e-00-00-01	статический
239.255.255.250	01-00-5e-7f-ff-fa	статический
255.255.255.255	ff-ff-ff-ff-ff-ff	статический

Интерфейс: 26.201.96.157 --- 0xe

адрес в Интернете	Физический адрес	Тип
26.0.0.1	02-00-00-00-51-00	динамический
26.255.255.255	ff-ff-ff-ff-ff-ff	статический
224.0.0.2	01-00-5e-00-00-02	статический
224.0.0.22	01-00-5e-00-00-16	статический
224.0.0.251	01-00-5e-00-00-fb	статический
224.0.0.252	01-00-5e-00-00-fc	статический
230.0.0.1	01-00-5e-00-00-01	статический
239.255.255.250	01-00-5e-7f-ff-fa	статический

Интерфейс: 192.168.193.1 --- 0x10

адрес в Интернете	Физический адрес	Тип
192.168.193.255	ff-ff-ff-ff-ff-ff	статический
224.0.0.2	01-00-5e-00-00-02	статический
224.0.0.22	01-00-5e-00-00-16	статический
224.0.0.251	01-00-5e-00-00-fb	статический
224.0.0.252	01-00-5e-00-00-fc	статический
230.0.0.1	01-00-5e-00-00-01	статический
239.255.255.250	01-00-5e-7f-ff-fa	статический
255.255.255.255	ff-ff-ff-ff-ff-ff	статический

Интерфейс: 192.168.1.52 --- 0x14

адрес в Интернете	Физический адрес	Тип
192.168.1.1	50-ff-20-00-51-a0	динамический
192.168.1.255	ff-ff-ff-ff-ff-ff	статический
224.0.0.2	01-00-5e-00-00-02	статический
224.0.0.22	01-00-5e-00-00-16	статический
224.0.0.251	01-00-5e-00-00-fb	статический
224.0.0.252	01-00-5e-00-00-fc	статический
224.0.0.253	01-00-5e-00-00-fd	статический
230.0.0.1	01-00-5e-00-00-01	статический
239.255.255.250	01-00-5e-7f-ff-fa	статический
255.255.255.255	ff-ff-ff-ff-ff-ff	статический

Интерфейс: 192.168.56.1 --- 0x16

адрес в Интернете	Физический адрес	Тип
192.168.56.255	ff-ff-ff-ff-ff-ff	статический
224.0.0.2	01-00-5e-00-00-02	статический
224.0.0.22	01-00-5e-00-00-16	статический
224.0.0.251	01-00-5e-00-00-fb	статический
224.0.0.252	01-00-5e-00-00-fc	статический
230.0.0.1	01-00-5e-00-00-01	статический
239.255.255.250	01-00-5e-7f-ff-fa	статический

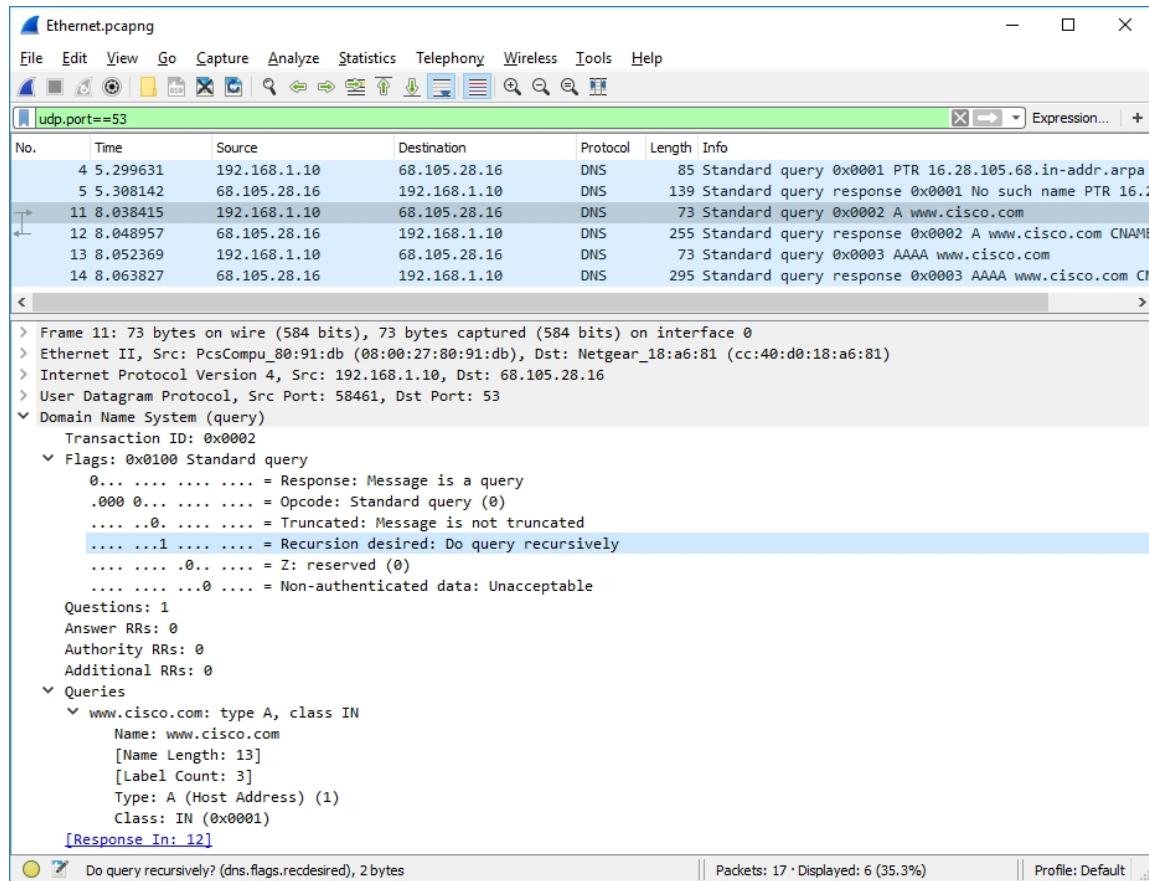
Интерфейс: 172.20.176.1 --- 0x1f

адрес в Интернете	Физический адрес	Тип
172.20.191.255	ff-ff-ff-ff-ff-ff	статический
224.0.0.2	01-00-5e-00-00-02	статический
224.0.0.22	01-00-5e-00-00-16	статический
224.0.0.251	01-00-5e-00-00-fb	статический
239.255.255.250	01-00-5e-7f-ff-fa	статический
255.255.255.255	ff-ff-ff-ff-ff-ff	статический

- c. Разверните **Domain Name System (query)** (Система доменных имен (запрос)) в области сведений о пакетах. Затем разверните **Flags** (Флаги) и **Queries** (Запросы).

Лабораторная работа. Исследование трафика DNS

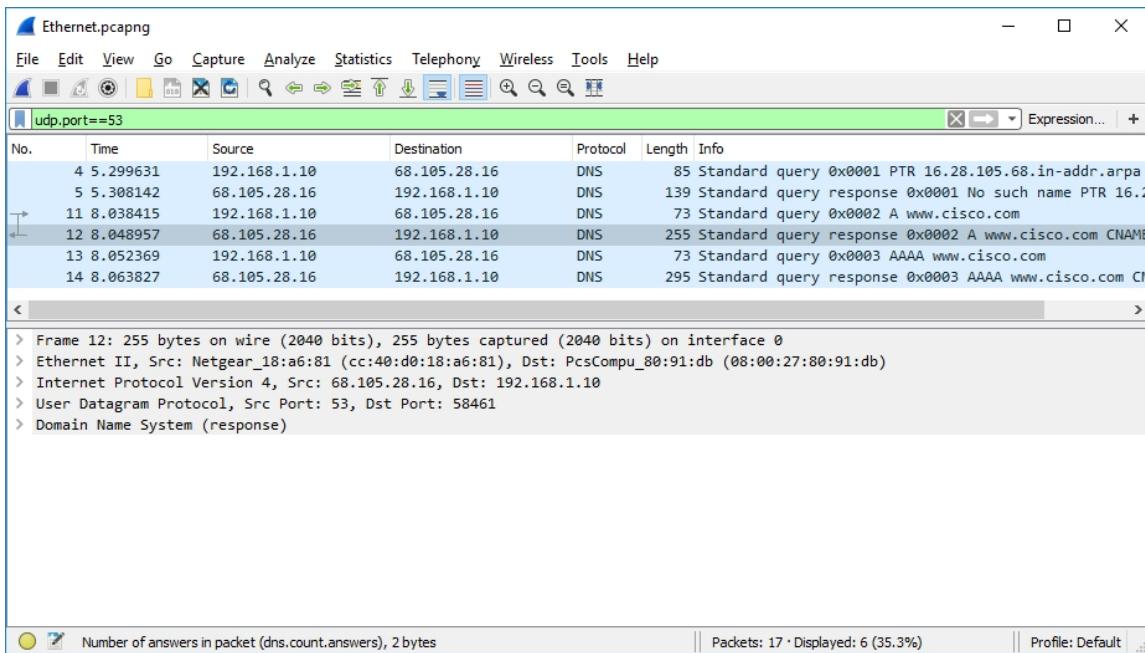
Изучите результаты. Флаг настроен для рекурсивного формирования запросов для IP-адреса на сайте www.cisco.com.



```
Domain Name System (query)
  Transaction ID: 0x0004
  Flags: 0x0100 Standard query
    0... .... .... = Response: Message is a query
    .000 0... .... .... = Opcode: Standard query (0)
    .... ..0. .... .... = Truncated: Message is not truncated
    .... ....1 .... .... = Recursion desired: Do query recursively
    .... .... .0.. .... = Z: reserved (0)
    .... .... ....0 .... = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    > www.cisco.com: type A, class IN
      Name: www.cisco.com
      [Name Length: 13]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      [Response In: 15]
```

Шаг 3. Изучение трафика DNS-ответа

- а. Выберите соответствующий пакет DNS-ответа с маркировкой **Standard query 0x000# A www.cisco.co** (Стандартный запрос 0x0002 A www.cisco.com).



Назовите MAC- и IP-адреса источника и назначения и номера портов. Проведите их сравнение с адресами в пакетах DNS-запроса.

Source Port: 53

Destination Port: 53116

Header checksum status. unanswered

Source Address: 192.168.1.1

Destination Address: 192.168.1.52

> Destination: 50:1a:da:11:16:c3 (50:1a:da:11:16:c3)

> Source: Keenetic_00:51:a0 (50:ff:20:00:51:a0)

Порты и адреса поменялись местами

Лабораторная работа. Исследование трафика DNS

- b. Разверните Domain Name System (response) (Система доменных имен (ответ)). Затем разверните Flags (Флаги), Queries (Запросы) и Answers (Ответы). Изучите результаты.

The screenshot shows a Wireshark capture of DNS traffic on port 53. The main pane displays several DNS messages, with the 12th message selected. The details pane shows the following breakdown:

- Domain Name System (response)**: Transaction ID: 0x0002
- Flags**: 0x8180 Standard query response, No error
 - .000 0... = Response: Message is a response
 - .000 0... = Opcode: Standard query (0)
 -0... = Authoritative: Server is not an authority for domain
 -0... = Truncated: Message is not truncated
 -1... = Recursion desired: Do query recursively
 -1... = Recursion available: Server can do recursive queries
 -0... = Z: reserved (0)
 -0... = Answer authenticated: Answer/authority portion was not authenticated by the server
 -0... = Non-authenticated data: Unacceptable
 -0000 = Reply code: No error (0)
- Questions**: 1
- Answer RRs**: 5
- Authority RRs**: 0
- Additional RRs**: 0
- Queries**:
 - www.cisco.com: type A, class IN
 - Name: www.cisco.com
 - [Name Length: 13]
 - [Label Count: 3]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
- Answers**:
 - www.cisco.com: type CNAME, class IN, cname www.cisco.com.akadns.net
 - www.cisco.com.akadns.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net
 - wwwds.cisco.com.edgekey.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net.globalredirect.akadns.net
 - wwwds.cisco.com.edgekey.net.globalredirect.akadns.net: type CNAME, class IN, cname e2867.dsca.akamaiedge.net
 - e2867.dsca.akamaiedge.net: type A, class IN, addr 96.7.79.147

Below the main pane, the status bar indicates: Ethernet (eth), 14 bytes | Packets: 17 • Displayed: 6 (35.3%) | Profile: Default

At the bottom, the expanded 'Answers' section shows:

- www.cisco.com: type CNAME, class IN, cname www.cisco.com.akadns.net
- www.cisco.com.akadns.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net
- wwwds.cisco.com.edgekey.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net.globalredirect.akadns.net
- wwwds.cisco.com.edgekey.net.globalredirect.akadns.net: type CNAME, class IN, cname e2867.dsca.akamaiedge.net
- e2867.dsca.akamaiedge.net: type A, class IN, addr 23.40.109.13

Может ли DNS-сервер выполнять рекурсивные запросы?
Да

Лабораторная работа. Исследование трафика DNS

с. Наблюдайте за записями CNAME и A в сведениях об ответах.

Сравните эти результаты с результатами команды nslookup.

```
▼ www.cisco.com: type CNAME, class IN, cname www.cisco.com.akadns.net
  Name: www.cisco.com
  Type: CNAME (5) (Canonical NAME for an alias)
  Class: IN (0x0001)
  Time to live: 3382 (56 minutes, 22 seconds)
  Data length: 26
  CNAME: www.cisco.com.akadns.net
  > www.cisco.com.akadns.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net
  > wwwds.cisco.com.edgekey.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net.globalredir
  > wwwds.cisco.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e2867.dsca.akama
  ▼ e2867.dsca.akamaiedge.net: type A, class IN, addr 23.40.109.13
    Name: e2867.dsca.akamaiedge.net
    Type: A (1) (Host Address)
    Class: IN (0x0001)
    Time to live: 20 (20 seconds)
    Data length: 4
    Address: 23.40.109.13
  . . . . .
```

Данные совпадают

Вопрос для повторения

- На основании результатов Wireshark какие еще сведения можно почерпнуть о сети, когда удаляется фильтр?
 - Как хакер может использовать программу Wireshark в целях нарушения безопасности сети?

Конец документа