

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.

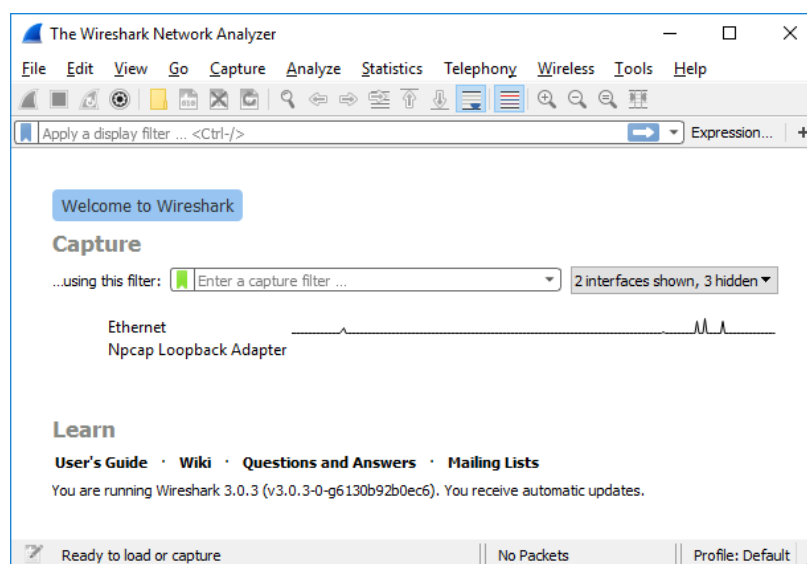
Необходимые ресурсы

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

Инструкции

Шаг 1. Перехват трафика DNS

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



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

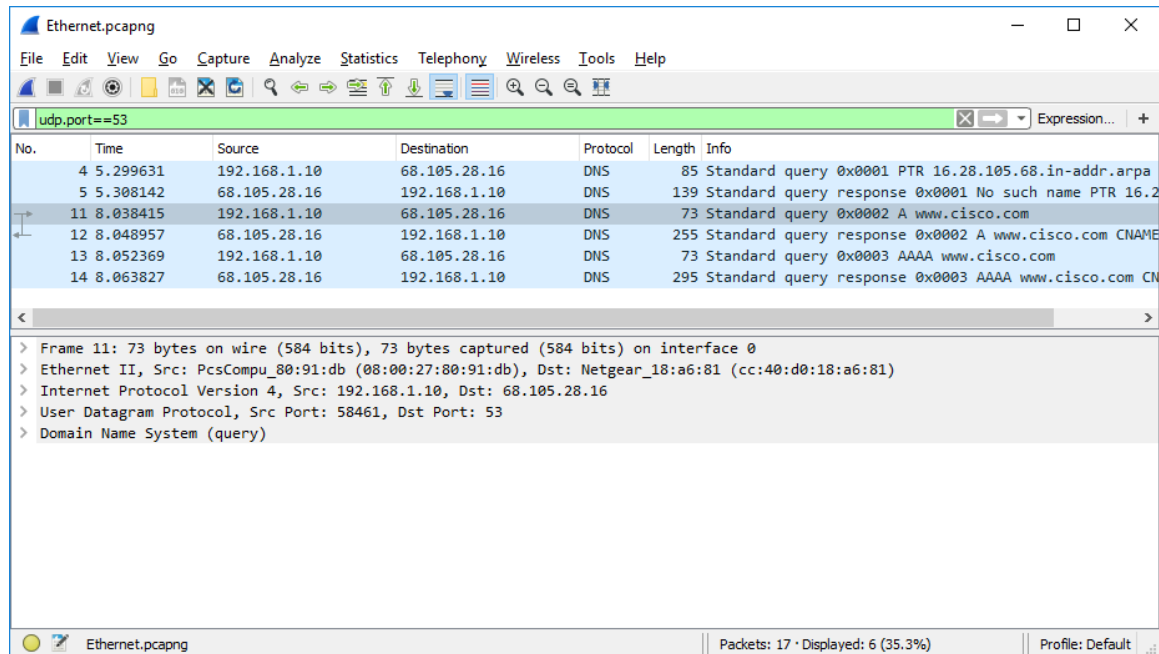
- e. После завершения введите **exit**, чтобы выйти из интерактивного режима nslookup. Закройте командную строку.
- f. Щелкните **Stop capturing packets** (Остановить перехват пакетов), чтобы остановить захват данных программой Wireshark.

Шаг 2. Изучение трафика DNS-запроса

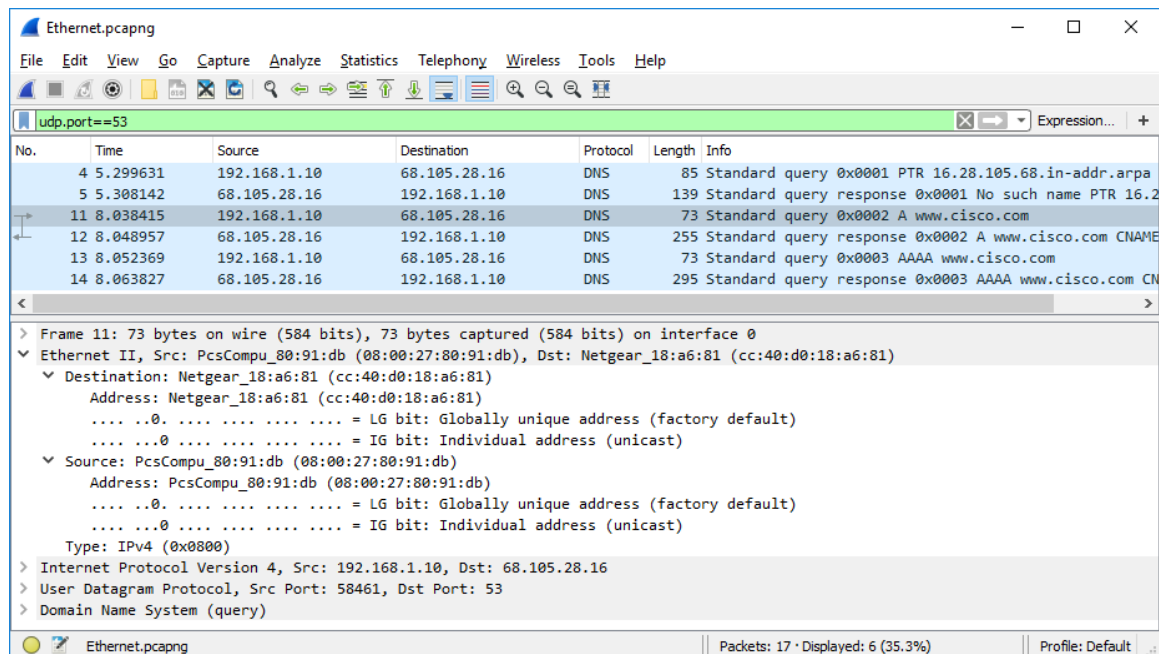
- a. Наблюдайте за трафиком, захваченным в области списка пакетов Wireshark. Введите **udp.port == 53** в поле фильтра и нажмите стрелку (или кнопку Enter) для показа только пакетов DNS.
- b. Выберите пакет DNS с маркировкой **Standard query 0x0002 A www.cisco.co** (Стандартный запрос 0x0002 A www.cisco.com).

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).

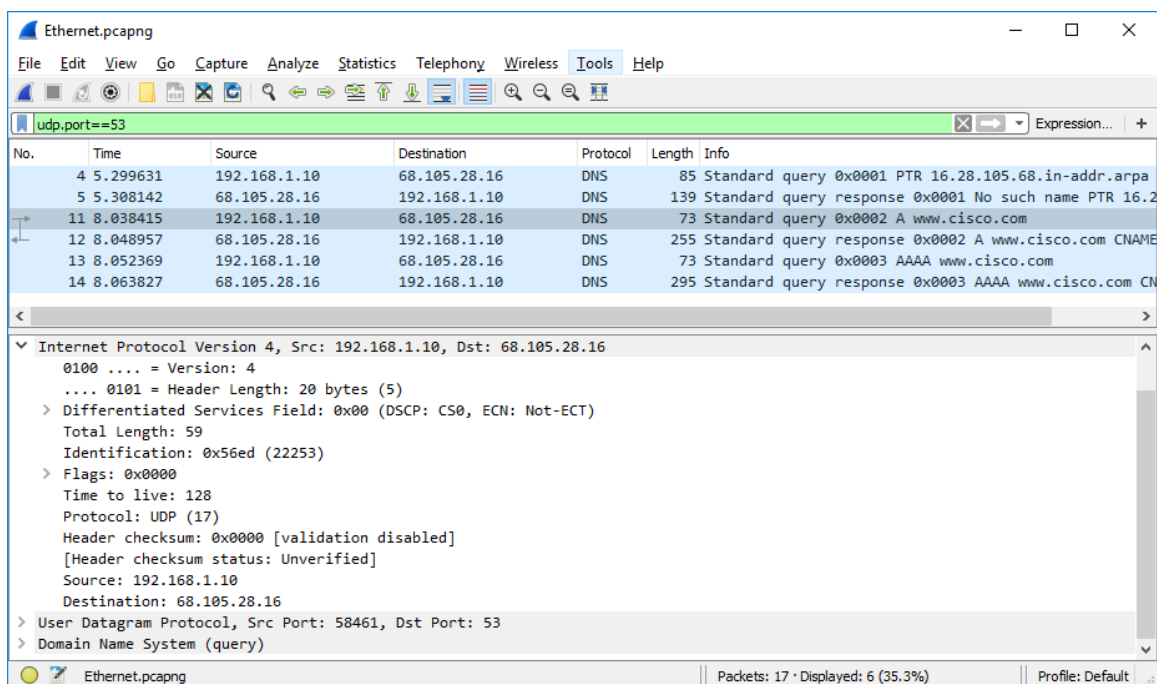


с. Разверните **Ethernet II** для просмотра сведений. Наблюдайте за полями источника и назначения.



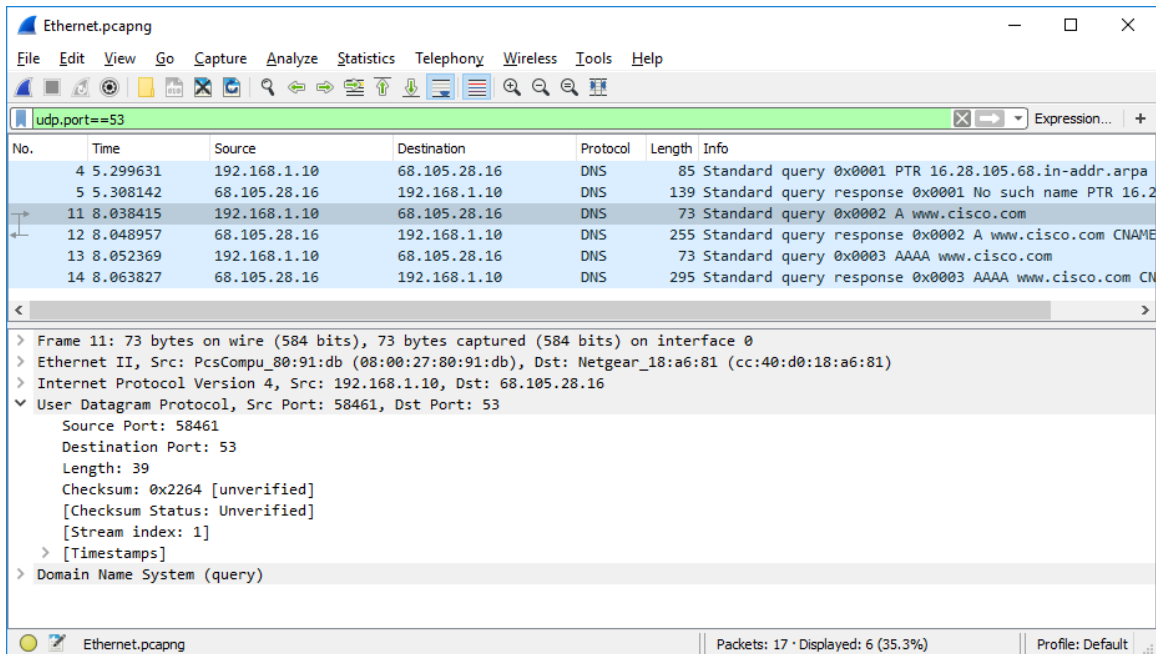
Назовите MAC-адреса источника и назначения. С какими сетевыми интерфейсами связаны эти MAC-адреса?

- а. 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?

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



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

- c. 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

```
Host Name . . . . . : DESKTOP
Основной DNS-суффикс. . . . . :
```

```
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?

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

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

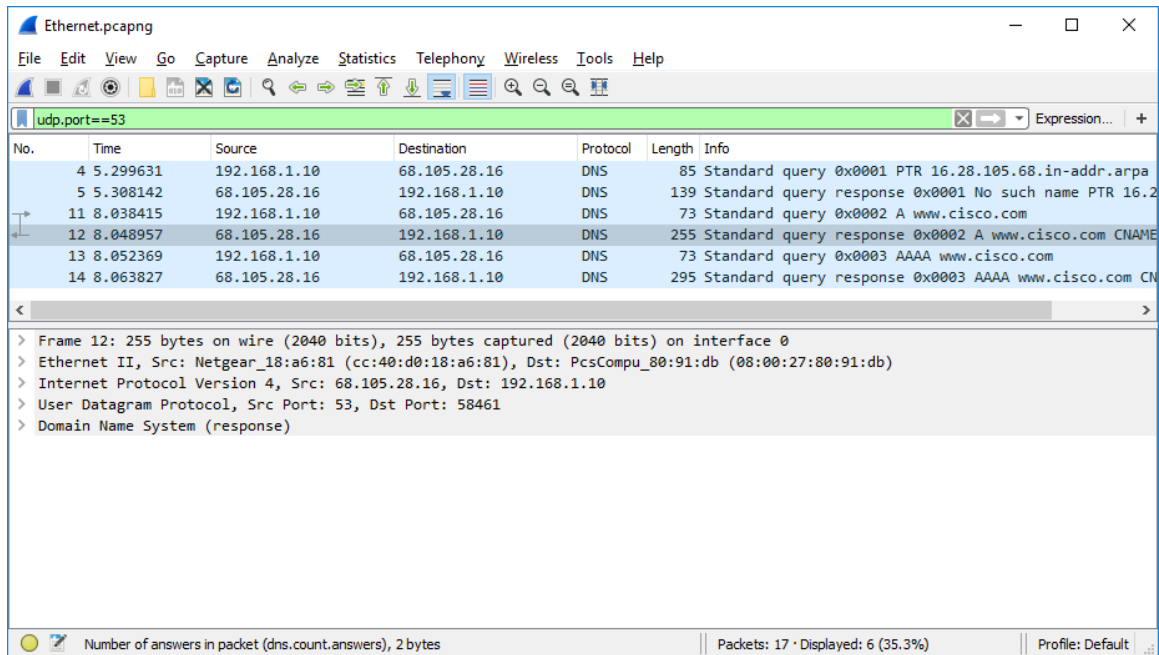
The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The filter bar at the top displays 'udp.port==53'. The packet list pane shows several DNS packets, with packet 11 selected. The packet details pane for packet 11 shows the following structure:

- Frame 11: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
- Ethernet II, Src: PcsCompu_08:91:db (08:00:27:80:91:db), Dst: Netgear_18:a6:81 (cc:40:d0:18:a6:81)
- Internet Protocol Version 4, Src: 192.168.1.10, Dst: 68.105.28.16
- User Datagram Protocol, Src Port: 58461, Dst Port: 53
- Domain Name System (query)
 - Transaction ID: 0x0002
 - Flags: 0x0100 Standard query
 - 0... .. = Response: Message is a query
 - .000 0... .. = Opcode: Standard query (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)

The status bar at the bottom indicates: 'Do query recursively? (dns.flags.recdesired), 2 bytes | Packets: 17 · Displayed: 6 (35.3%) | Profile: Default'.

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.

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

The screenshot shows the Wireshark interface with a packet capture of DNS traffic. The packet list at the top shows a query from 192.168.1.10 to 68.105.28.16 for www.cisco.com. The packet details pane shows the response with flags, queries, and answers.

No.	Time	Source	Destination	Protocol	Length	Info
4	5.299631	192.168.1.10	68.105.28.16	DNS	85	Standard query 0x0001 PTR 16.28.105.68.in-addr.arpa
5	5.308142	68.105.28.16	192.168.1.10	DNS	139	Standard query response 0x0001 No such name PTR 16.2
11	8.038415	192.168.1.10	68.105.28.16	DNS	73	Standard query 0x0002 A www.cisco.com
12	8.048957	68.105.28.16	192.168.1.10	DNS	255	Standard query response 0x0002 A www.cisco.com CNAME
13	8.052369	192.168.1.10	68.105.28.16	DNS	73	Standard query 0x0003 AAAA www.cisco.com
14	8.063827	68.105.28.16	192.168.1.10	DNS	295	Standard query response 0x0003 AAAA www.cisco.com CN

Domain Name System (response)
Transaction ID: 0x0002

- Flags: 0x8180 Standard query response, No error
 - 1... .. = 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
 -00 .. = 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 wwds.cisco.com.edgekey.net
 - wwds.cisco.com.edgekey.net: type CNAME, class IN, cname wwds.cisco.com.edgekey.net.globalredir.akadns.net
 - wwds.cisco.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e2867.dsca.akamaiedge.net
 - e2867.dsca.akamaiedge.net: type A, class IN, addr 96.7.79.147

[Request In: 11]
[Time: 0.010542000 seconds]

Может ли DNS-сервер выполнять рекурсивные запросы?

- c. Наблюдайте за записями CNAME и A в сведениях об ответах.
Сравните эти результаты с результатами команды nslookup.

Вопрос для повторения

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

Конец документа