# Лабораторная работа: изучение захваченных данных DNS UDP с помощью программы Wireshark

Топология



## Задачи

Часть 1. Запись данных ІР-конфигурации ПК

Часть 2. Захват запросов и ответов DNS с помощью программы Wireshark

Часть 3. Анализ захваченных пакетов DNS или UDP

## Исходные данные/сценарий

Если вы хоть раз выходили в Интернет, то пользовались службой доменных имён (DNS). DNS — это распределённая сеть серверов, которая преобразует понятные имена доменов, например www.google.com, в IP-адрес. При вводе в браузер URL-адреса какого-либо сайта ПК отправляет в DNS запрос об IP-адресе DNS-сервера. Запрос DNS-сервера вашего ПК и ответ DNS-сервера используют в качестве протокола транспортного уровня протокол пользовательских датаграмм (UDP). UDP не требует соединения и настройки сеанса, как TCP. Запросы и ответы DNS чрезвычайно малы и не требуют служебных сигналов TCP.

В ходе лабораторной работы вы будете обмениваться данными с DNS-сервером, отправляя в DNS запросы по транспортному протоколу UDP. Для анализа обмена данными с сервером доменных имен будет использоваться программа Wireshark.

Примечание. Эту лабораторную работу нельзя выполнять при помощи Netlab. Она предполагает наличие доступа к Интернету.

## Необходимые ресурсы

1 ПК (Windows 7, Vista или XP с доступом к командной строке, доступу к Интернету и установленному анализатору пакетов Wireshark)

# Часть 1: Запись данных ІР-конфигурации ПК

В части 1 с помощью команды**ipconfig /all**на локальном ПК вам нужно будет найти и записать MACи IP-адреса сетевого адаптера вашего ПК, IP-адрес указанного шлюза по умолчанию и IP-адрес DNSсервера, указанного для ПК. Запишите эти данные в приведённую ниже таблицу. Они вам потребуются для анализа пакетов в следующих частях лабораторной работы.

| ІР-адрес                    |  |
|-----------------------------|--|
| МАС-адрес                   |  |
| IP-адрес шлюза по умолчанию |  |
| IP-адрес DNS-сервера        |  |

## Часть 2: Захват запросов и ответов DNS с помощью программы Wireshark

В части 2 вам нужно настроить программу Wireshark для захвата пакетов запросов и ответов DNS и продемонстрировать использование транспортного протокола UDP при обмене данными с DNS-сервером.

a. Нажмите кнопку Пуск и откройте программу Wireshark.

**Примечание**. Если программа Wireshark не установлена, её можно загрузить по адресу <u>http://www.wireshark.org/download.html</u>.

- b. Выберите интерфейс Wireshark для захвата пакетов. Используйте Interface List (Список интерфейсов), чтобы выбрать интерфейс, который связан IP- и МАС-адресами ПК, записанными в части 1.
- с. Выбрав нужный интерфейс, нажмите Start (Начать), чтобы начать захват пакетов.
- d. Откройте веб-браузер и введите www.google.com. Нажмите клавишу ВВОД, чтобы продолжить.
- e. Как только откроется главная страница Google, нажмите кнопку **Stop** (Остановить), чтобы остановить захват данных программой Wireshark.

## Часть 3: Анализ захваченных пакетов DNS или UDP

В части 3 вам необходимо изучить пакеты UDP, созданные при обмене данными с DNS-сервером для IP-адресов www.google.com.

### Шаг 1: Отфильтруйте DNS-пакеты.

a. В главном окне программы Wireshark введите **dns в** строке **Filter** (Фильтр). Нажмите **Apply** (Применить) или клавишу ВВОД.

**Примечание**. Если после применения фильтра DNS никакие результаты не отображаются, закройте веб-браузер и введите в окне командной строки команду **ipconfig /flushdns**, чтобы удалить все предыдущие результаты DNS. Перезапустите захват данных программой Wireshark и повторите шаги 2b–2e. Если решить проблему не удалось, в окне командной строки введите команду **nslookup www.google.com** в качестве альтернативы браузеру.

| Capturing from Microsoft: \Device\NPF_{853821E3-ACB7-400B-8CCB-9B26B91F82AB} [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]   |  |  |  |  |  |  |
|--|--|--|--|--|--|--|
| ● ● ∡ ■ ∡ ⊨ ≞ % ≈   ♀ ⇔ ⇔ 주 ⊻   ⊟ ⊑   ♀ ♀ ℚ ⊡   ¥ ⊠ ≅ %   ¤  |  |  |  |  |  |  |
| Filter: dns Expression Clear Apply Save  |  |  |  |  |  |  |
| No.         Time         Source         Destination         Protocol         Length         Info           4 1.613556000 192.168.1.11         192.168.1.11         DNS         74 Standard query 0x3f76 A www.google.com           5 1.624376000 192.168.1.11         192.168.1.11         DNS         290 Standard query response 0x3f76 A 74.125.           47 2.180985000 192.168.1.11         192.168.1.11         DNS         75 Standard query 0x6dc A plus.google.com           48 2.181866000 192.168.1.11         192.168.1.11         DNS         75 Standard query 0x318f A maps.google.com   |  |  |  |  |  |  |
| 49 2.182440000 192.168.1.11 192.168.1.1 DNS 75 Standard query 0x5d4f A play.google.com -   |  |  |  |  |  |  |
| <pre>Image: Image: Imag</pre> |  |  |  |  |  |  |
| 0000       30       46       9a       99       c5       72       90       4c       e5       be       15       63       08       00       45       00       0Fr.L      c.E.         0010       00       3c       40       9f       00       08       11       76       b5       c0       a8       01       0b       c0       a8      v       v       v         0020       01       01       cb       8e       03       50       28       e2       5f       3f       76       01       00       00       1        v  |  |  |  |  |  |  |
| O Microsoft: \Device\NPF_{853821E3-ACB7-40 Packets: 630 Displayed: 40 Profile: Default   |  |  |  |  |  |  |

b. На панели списка захваченных пакетов (верхний раздел) в главном окне программы найдите пакет со словами Standard query (стандартный запрос) и A www.google.com (запрос сайта google.com). См. пример в кадре 4.

#### Шаг 2: Изучите сегмент UDP с помощью DNS-запроса.

Изучите UDP с помощью DNS-запроса о сайте www.google.com, захваченного программой Wireshark. В данном примере для анализа выбран захваченный кадр 4 на панели списка захваченных пакетов. Протоколы в этом запросе отображаются на панели сведений о пакетах (Details, средний раздел) в главном окне. Записи протокола выделены серым цветом.

```
    B Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
    B Ethernet II, Src: HonHaiPr_be:15:63 (90:4c:e5:be:15:63), Dst: Netgear_99:c5:72 (30:46:9a:99:c5:72)
    B Internet Protocol Version 4, Src: 192.168.1.11 (192.168.1.11), Dst: 192.168.1.1 (192.168.1.1)
    □ User Datagram Protocol, Src Port: 52110 (52110), Dst Port: domain (53)
Source port: 52110 (52110)
Destination port: domain (53)
Length: 40
    B Checksum: Oxe25f [validation disabled]
    B Domain Name System (query)
```

- а. На панели сведений о пакетах кадр 4 имеет 74 байта данных, как показано в первой строке. Это количество байтов нужно отправить в качестве DNS-запроса на сервер, который запрашивает IPадреса сайта www.google.com.
- b. Строка Ethernet II содержит MAC-адреса источника и назначения. MAC-адрес источника принадлежит вашему локальному ПК как источнику DNS-запроса. MAC-адрес назначения — это шлюз по умолчанию, поскольку это последняя остановка запроса перед выходом из локальной сети.

Совпадает ли МАС-адрес источника с адресом, записанным в части 1 для локального ПК?

с. В строке интернет-протокола версии 4 захваченные данные IP-пакета показывают, что IP-адрес источника данного DNS-запроса — 192.168.1.11, а IP-адрес назначения — 192.168.1.1. В данном примере адрес назначения — это шлюз по умолчанию. В данной сети шлюзом по умолчанию является маршрутизатор.

Можете ли вы сопоставить IP- и МАС-адреса для устройств источника и назначения?

| Устройство           | IP-адрес | МАС-адрес |
|----------------------|----------|-----------|
| Локальный ПК         |          |           |
| Шлюз по<br>умолчанию |          |           |

IP-пакет и заголовок инкапсулируют сегмент UDP. Сегмент UDP содержит DNS-запрос в виде данных.

d. Заголовок UDP имеет только четыре поля: порт источника, порт адресата, длина и контрольная сумма. Как показано ниже, длина каждого поля в заголовке UDP составляет всего 16 бит.

#### CELMEHT UDP

| 0                   | 16 31                 |  |  |  |  |
|---------------------|-----------------------|--|--|--|--|
| ПОРТ ИСТОЧНИКА UDP  | ПОРТ НАЗНАЧЕНИЯ UDP   |  |  |  |  |
| ДЛИНА СООБЩЕНИЯ UDP | КОНТРОЛЬНАЯ СУММА UDP |  |  |  |  |
| ДАННЫЕ              |                       |  |  |  |  |
| ДАННЫЕ              |                       |  |  |  |  |

Разверните протокол UDP на панели сведений о пакетах, нажав на значок плюса (+). Обратите внимание на то, что в открывшемся окне будут только четыре поля. Номер порта источника в данном примере — 52110. Порт источника был случайно сгенерирован локальным ПК с использованием зарезервированных номеров портов. Порт назначения — 53. Порт 53 — это общеизвестный порт, зарезервированный для использования с DNS. DNS-серверы получают DNS-запросы от клиентов через порт 53.

```
    User Datagram Protocol, Src Port: 52110 (52110), Dst Port: domain (53)
Source port: 52110 (52110)
Destination port: domain (53)
Length: 40
    Checksum: 0xe25f [validation disabled]
[Good Checksum: False]
[Bad Checksum: False]
```

В данном примере длина этого сегмента UDP составляет 40 байт. Из 40 байтов восемь составляют заголовок. Остальные 32 байта используются данными DNS-запроса. На приведённом ниже снимке экрана выделены 32 байта данных DNS-запроса на панели отображения пакета в виде последовательности байтов (нижний раздел главного окне Wireshark).

| <pre>□ Domain Name System (query)     [Response In: 5]     Transaction ID: 0x3f76     Flags: 0x0100 Standard query     Questions: 1     Answer RRs: 0     Authority RRs: 0     Additional RRs: 0     Queries     www.google.com: type A, class IN         Name: www.google.com         Type: A (Host address)         Class: IN (0x0001)</pre> | H |
|--|---|
| 4  |   |
| 0000       30       46       9a       99       c5       72       90       4c       e5       be       15       63       08       004       50       0FF.L      c.E.         0010       00       32       40       9f       00       08       01       0F       cost   |   |

Контрольная сумма используется для определения целостности пакета после передачи через Интернет.

Заголовок UDP отличается низкими потерями, поскольку протокол UDP не имеет полей, связанных с трёхсторонним рукопожатием в протоколе TCP. Любые проблемы с надёжностью передачи данных должны решаться на уровне приложений.

Запишите результаты захвата данных программой Wireshark в приведённую ниже таблицу.

| Размер кадра         |  |
|----------------------|--|
| МАС-адрес источника  |  |
| МАС-адрес назначения |  |
| IP-адрес источника   |  |
| IP-адрес назначения  |  |
| Порт источника       |  |
| Порт назначения      |  |

Совпадает ли IP-адрес источника с IP-адресом локального ПК, записанным в части 1?

Совпадает ли IP-адрес назначения со шлюзом по умолчанию, записанным в части 1?

#### Шаг 3: Изучите UDP с помощью DNS-ответа.

В этом шаге вам нужно изучить пакет DNS-ответа и убедиться в том, что он также использует протокол UDP.

а. В данном примере соответствующим пакетом DNS-ответа является кадр 5. Обратите внимание на то, что количество байт на линии составляет 290. Этот пакет превышает по объёму пакет DNSзапроса.

| Filter:                         | dns  |                 |                 | -        | Expression. | Clear Aş | oply Sav | re       |                     |
|---------------------------------|--|-----------------|-----------------|----------|-------------|----------|----------|----------|---------------------|
| No.                             | Time   | Source          | Destination     | Protocol | Length      | Info     |          |          |                     |
|                                 | 4 1.61355600   | 0 192.168.1.11  | 192.168.1.1     | DNS      | 74          | Standard | query    | 0x3f76   | A www.google.com 🦳  |
|                                 | 5 1.62437600   | 0 192.168.1.1   | 192.168.1.11    | DNS      | 290         | Standard | query    | respons  | e 0x3f76 A 74.125   |
|                                 | 47 2.18098500  | 0 192.168.1.11  | 192.168.1.1     | DNS      | 75          | standard | query    | 0x6bdc   | A plus.google.com   |
|                                 | 48 2.18186600  | 0 192.168.1.11  | 192.168.1.1     | DNS      | 75          | Standard | query    | 0x318f   | A maps.google.com   |
|                                 | 49 2.18244000  | 0 192.168.1.11  | 192.168.1.1     | DNS      | 75          | Standard | query    | 0x5d4f   | A play.google.com 👻 |
| •                               |  |                 |                 |          |             |          |          |          | 4                   |
| 🕀 Fra                           | ame 5: 290 byt   | es on wire (23  | 20 bits), 290 b | ytes cap | otured (2   | 320 bits | ) on i   | nterface | 2 0                 |
| 🗄 Et                            | hernet II, Sro   | : Netgear_99:c  | 5:72 (30:46:9a: | 99:c5:72 | 2), Dst:    | HonHaiPr | _be:15   | :63 (90: | :4c:e5:be:15:63)    |
| 🗄 In                            | ternet Protoco   | ol Version 4, S | rc: 192.168.1.1 | (192.16  | 58.1.1),    | Dst: 192 | .168.1   | .11 (192 | 2.168.1.11)         |
| 🖃 Us                            | 🗆 User Datagram Protocol, Src Port: domain (53), Dst Port: 52110 (52110) |                 |                 |          |             |          |          |          |                     |
| Source port: domain (53)        |  |                 |                 |          |             |          |          |          |                     |
| Destination port: 52110 (52110) |  |                 |                 |          |             |          |          |          |                     |
| Length: 256                     |  |                 |                 |          |             |          |          |          |                     |
| - (                             | Checksum: 0xc4   | ca [validation  | disabled]       |          |             |          |          |          |                     |
|                                 | [Good Checks   | um: False]      |                 |          |             |          |          |          |                     |
|                                 | [Bad Checksı   | ım: False]      |                 |          |             |          |          |          |                     |
| ± Dor                           | main Name Syst   | em (response)   |                 |          |             |          |          |          |                     |

- b. Судя по кадру Ethernet II для DNS-ответа, с какого устройства получен MAC-адрес источника и какое устройство является MAC-адресом назначения?
- с. Обратите внимание на IP-адреса источника и назначения в IP-пакете. Назовите IP-адрес назначения. Назовите IP-адрес источника.

IP-адрес назначения: \_\_\_\_\_ IP-адрес источника: \_\_\_\_\_

Что произошло с ролями источника и назначения локального узла и шлюза по умолчанию?

d. В сегменте UDP роли номеров портов также изменились на противоположные. Номер порта назначения — 52110. Номер порта 52110 — это тот же порт, который был сгенерирован локальным ПК при отправке DNS-запроса на DNS-сервер. Ваш локальный ПК ожидает DNS-ответа от этого порта.

Номер порта назначения — 53. DNS-сервер ожидает DNS-запроса от порта 53, а затем отправляет DNS-ответ с номером порта источника 53 создателю DNS-запроса.

При расширении DNS-запроса обратите внимание на преобразованные IP-адреса сайта www.google.com в разделе **Ответы**.

```
User Datagram Protocol, Src Port: domain (53), Dst Port: 52110 (52110)
   Source port: domain (53)
   Destination port: 52110 (52110)
   Length: 256
  Checksum: Oxc4ca [validation disabled]
     [Good Checksum: False]
     [Bad Checksum: False]
😑 Domain Name System (respon
   [Request In: 4]
   [Time: 0.010820000 seconds]
   Transaction ID: 0x3f76
 Ouestions: 1
   Answer RRs: 5
Authority RRs: 4
   Additional RRs: 4

    Oueries

  Answers

    www.google.com: type A, class IN, addr 74.125.227.84

    www.google.com: type A, class IN, addr 74.125.227.80

    www.google.com: type A, class IN, addr 74.125.227.81

    www.google.com: type A, class IN, addr 74.125.227.82

    www.google.com: type A, class IN, addr 74.125.227.83

  ⊟ Authoritative nameservers

    google.com: type NS, class IN, ns ns1.google.com

    google.com: type N5, class IN, ns ns2.google.com

   ∃ google.com: type NS, class IN, ns ns3.google.com
   google.com: type NS, class IN, ns ns4.google.com
  ⊟ Additional records

    Ins1.google.com: type A, class IN, addr 216.239.32.10

   ⊞ ns2.google.com: type A, class IN, addr 216.239.34.10
```

#### Вопросы на закрепление

В чём состоят преимущества использования протокола UDP вместо протокола TCP в качестве транспортного протокола для DNS?