Лабораторная работа. Изучение захваченных пакетов DNS и UDP с помощью программы Wireshark

1. Топология



1. Цели

Часть 1. Запись данных о конфигурации IP на ПК

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

Часть 3. Анализ захваченных пакетов DNS или UDP

1. Общие сведения/сценарий

Если вы хотя бы однажды выходили в Интернет, то пользовались системой доменных имен (DNS). DNS — это распределенная сеть серверов, которая преобразует понятные человеку имена доменов, например www.google.com, в IP-адреса. При вводе в браузере URL-адреса какого-либо веб-сайта компьютер отправляет DNS-запрос на IP-адрес DNS-сервера. При запросе компьютером DNS-сервера и ответе DNS-сервера в качестве протокола транспортного уровня используется протокол пользовательских датаграмм (UDP). В отличие от TCP, UDP является протоколом без установления соединения и не требует установления сеанса. Запросы и ответы DNS имеют чрезвычайно малый объем и не требуют использования служебной информации TCP.

В ходе лабораторной работы вы будете обмениваться данными с DNS-сервером, отправляя DNS-запросы с помощью транспортного протокола UDP. Для анализа обмена данными с сервером доменных имен будет использоваться программа Wireshark.

**Примечание.** Эту лабораторную работу нельзя выполнять при помощи Netlab. Для выполнения лабораторной работы необходим доступ к Интернету.

1. Необходимые ресурсы

Один ПК (под управлением Windows 7, 8 или 10 с доступом к командной строке, доступом к Интернету и установленной программой Wireshark)

1. Запись данных IP-конфигурации ПК

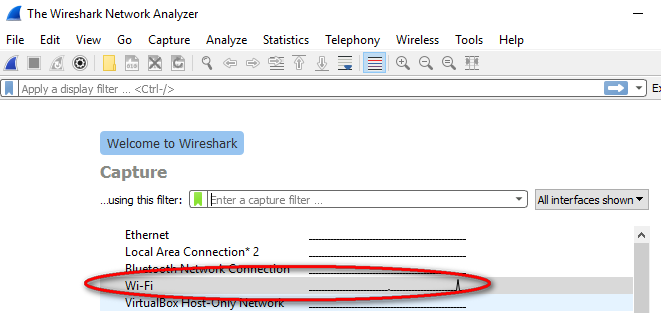
В части 1 с помощью команды **ipconfig /all** на локальном ПК вам нужно будет найти и записать МАС-адрес и IP-адрес сетевой интерфейсной платы своего ПК, IP-адрес указанного шлюза по умолчанию и IP-адрес DNS-сервера, указанного для ПК. Запишите эти данные в приведенную ниже таблицу. Они потребуются вам для анализа пакетов в следующих частях лабораторной работы.

|  |  |
| --- | --- |
| IP-адрес | 192.168.0.171 |
| MAC-адрес | 04-7C-16-B4-1C-0D |
| IP-адрес шлюза по умолчанию | fe80::394:ce4e:b278:3a3%17 |
| IP-адрес DNS-сервера | 192.168.0.1 |

1. Захват запросов и ответов DNS с помощью программы Wireshark

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

* + 1. Нажмите кнопку **Пуск** и откройте программу Wireshark.
    2. Выберите интерфейс для захвата пакетов с помощью Wireshark. Выберите (выделите) активный интерфейс захвата.



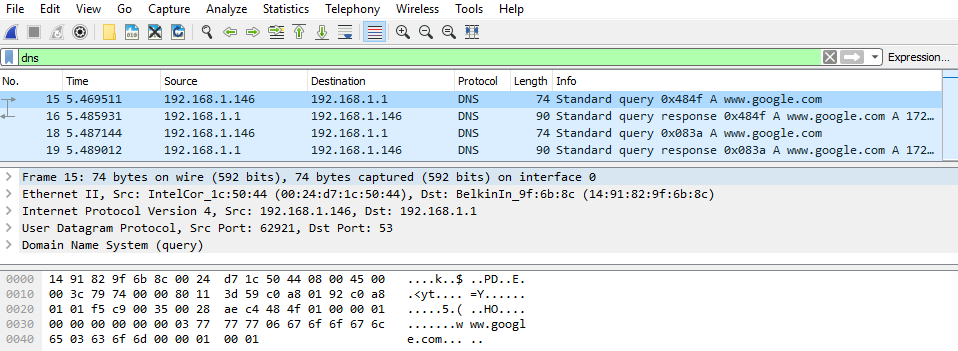
* + 1. Выбрав нужный интерфейс, нажмите **Start** (Пуск), чтобы начать захват пакетов.
    2. Откройте веб-браузер и введите адрес **www.google.com**. Для продолжения нажмите клавишу **Enter**.
    3. Как только откроется главная страница Google, нажмите кнопку **Stop** (Остановить), чтобы остановить захват данных программой Wireshark.

1. Анализ захваченных пакетов DNS или UDP

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

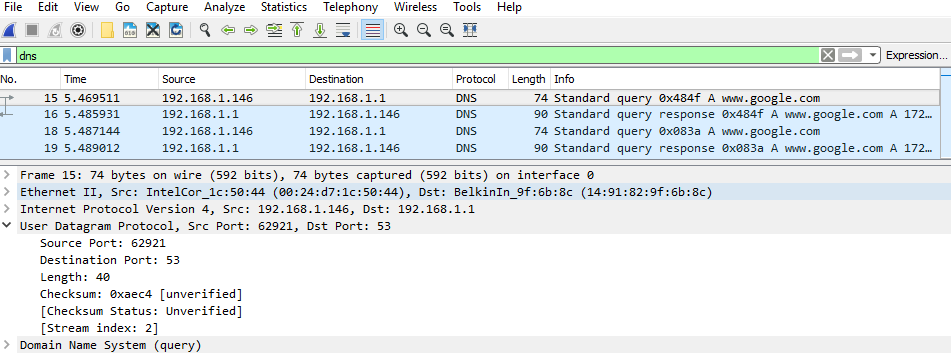
* 1. Отфильтруйте DNS-пакеты.
     1. В главном окне программы Wireshark введите **dns** в поле **Filter** (Фильтр) инструментальной панели и нажмите **Enter** (Ввод).

**Примечание**. Если после применения фильтра DNS вы не видите никаких результатов, закройте браузер. В окне командной строки введите **ipconfig /flushdns** для удаления всех предыдущих результатов DNS. Перезапустите захват данных программой Wireshark и повторите шаги 2Б — 2Д. Если таким образом решить проблему не удалось, то вместо использования браузера введите в окне командной строки команду**nslookup** [**www.google.com**](http://www.google.com).



* + 1. На панели списка пакетов (верхний раздел) в главном окне программы найдите пакет с информацией **Standard query** (Стандартный запрос) и **A www.google.com** (Запрос сайта google.com). В качестве примера можно взять кадр 15.
  1. Изучите сегмент UDP с помощью DNS-запроса.

Изучите данные UDP, используя DNS-запрос для адреса www.google.com, захваченный программой Wireshark. В данном примере для анализа выбран захваченный программой Wireshark кадр 15 на панели списка пакетов. Протоколы в этом запросе отображаются на панели сведений о пакетах (средний раздел) в главном окне. Сведения о протоколе выделены серым цветом.



* + 1. Как показано в первой строке на панели сведений о пакетах, кадр 15 содержал 74 байта данных во время передачи. Это количество байтов нужно отправить в качестве DNS-запроса на сервер, который запрашивает IP-адреса сайта www.google.com.
    2. Строка Ethernet II содержит МАС-адреса источника и места назначения. MAC-адрес источника принадлежит вашему локальному ПК как источнику DNS-запроса. MAC-адрес назначения — это шлюз по умолчанию, поскольку это последняя остановка перед выходом запроса из локальной сети.

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

**Да**

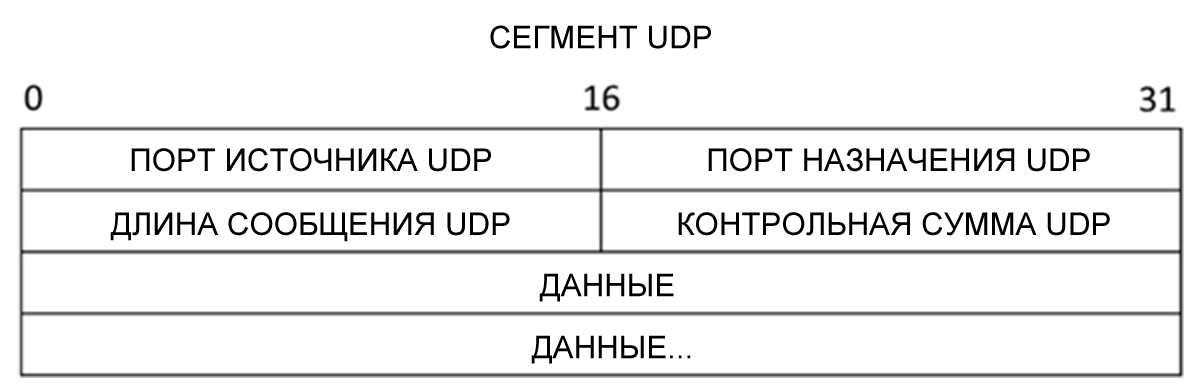
* + 1. В строке Internet Protocol Version 4 захваченные данные IP-пакета показывают, что IP-адрес источника данного DNS-запроса — 192.168.1.146, а IP-адрес назначения — 192.168.1.1. В данном примере адрес назначения — это шлюз по умолчанию. В данной сети шлюзом по умолчанию является маршрутизатор.

Можете ли вы указать IP-адрес и МАС-адрес для устройств источника и назначения?

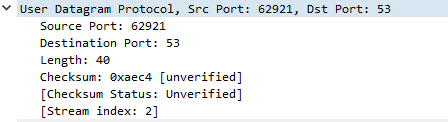
|  |  |  |
| --- | --- | --- |
| Устройство | IP-адрес | MAC-адрес |
| Локальный ПК | Internet Protocol Version 4, Src: 192.168.0.171 | 04-7C-16-B4-1C-0D |
| Шлюз по умолчанию | 192.168.0.1 | TpLinkTechno\_20:89:53 (98:da:c4:20:89:53) |

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

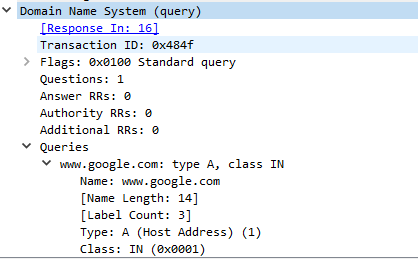
* + 1. Заголовок UDP имеет только четыре поля: порт источника, порт назначения, длина и контрольная сумма. Как показано ниже, длина каждого поля в заголовке UDP составляет всего 16 бит.



Разверните узел User Datagram Protocol на панели сведений о пакетах, нажав на значок «плюс» (+). Обратите внимание на то, что отображаются всего четыре поля. Номер порта источника в данном примере — 60868. Порт источника был случайно сгенерирован локальным ПК с использованием незарезервированных номеров портов. Порт назначения — 53. Порт 53 — это «хорошо известный порт», зарезервированный для использования с DNS. DNS-серверы прослушивают порт 53 для получения DNS-запросов от клиентов.



В данном примере длина сегмента UDP составляет 40 байт. 8 из 40 байт используются в качестве заголовка. Остальные 32 байта используются данными DNS-запроса. На следующем рисунке выделены 32 байта данных DNS-запроса на панели отображения байтов пакета (нижний раздел главного окна Wireshark).



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

Заголовок UDP несет мало служебной информации, поскольку протокол UDP не имеет полей, связанных с трехсторонним квитированием в протоколе TCP. Любые проблемы с надежностью передачи данных должны решаться на прикладном уровне.

Запишите результаты захвата данных программой Wireshark в приведенную ниже таблицу.

|  |  |
| --- | --- |
| Размер кадра | 74 байта |
| MAC-адрес источника | 04-7C-16-B4-1C-0D |
| MAC-адрес назначения | (98:da:c4:20:89:53) |
| IP-адрес источника | 192.168.0.171 |
| IP-адрес назначения | 192.168.0.1 |
| Порт источника | 59614 |
| Порт назначения | 53 |

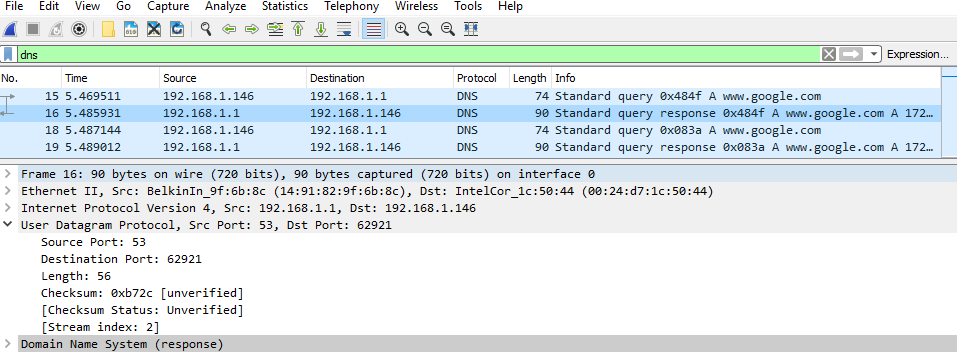
Совпадает ли IP-адрес источника с IP-адресом локального ПК, записанным в части 1? **ДА**

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

* 1. Изучите сегмент UDP с помощью DNS-ответа.

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

* + 1. В данном примере соответствующим пакетом DNS-ответа является кадр 16. Обратите внимание на то, что количество байтов во время передачи составляет 90. Этот пакет превышает по объему пакет DNS-запроса.



* + 1. Если судить по кадру Ethernet II для DNS-ответа, какому устройству соответствует MAC-адрес источника и какое устройство соответствует MAC-адресу назначения?

**Источник – шлюз по умолчанию, а назначение - ПК**

* + 1. Обратите внимание на IP-адреса источника и назначения в IP-пакете. Назовите IP-адрес назначения. Назовите IP-адрес источника.

IP-адрес назначения: 192.168.0.1 IP-адрес источника: 192.168.0.171

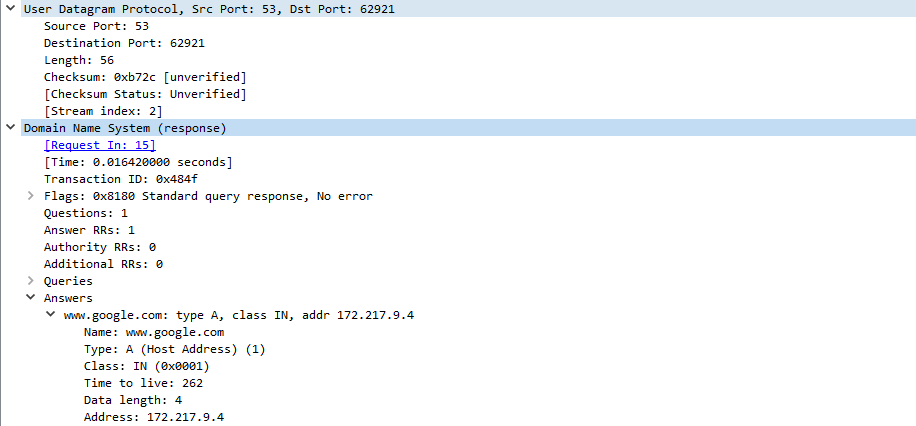
Что произошло с ролями источника и назначения локального узла и шлюза по умолчанию?

**Поменялись ролями**

* + 1. В сегменте UDP роли номеров портов также изменились на противоположные. Номер порта назначения — 62921. Номер порта 62921 — это тот же номер порта, который был сгенерирован локальным ПК при отправке DNS-запроса на DNS-сервер. Ваш локальный ПК прослушивает этот порт для получения DNS-ответа.

Номер порта источника — 53. DNS-сервер прослушивает порт 53 для получения DNS-запроса, а затем отправляет DNS-ответ с номером порта источника 53 обратно инициатору DNS-запроса.

После того как будет развернута строка DNS-запроса, обратите внимание на преобразованные IP-адреса сайта www.google.com в разделе **Answers** (Ответы).



1. Вопросы для повторения

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

**В отличие от TCP, UDP является протоколом без установления соединения и не требует установления сеанса. Запросы и ответы DNS имеют чрезвычайно малый объем и не требуют использования служебной информации TCP.**