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

Топология

Задачи

Часть 1. Запись данных IP-конфигурации ПК

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

Часть 3. Анализ захваченных пакетов DNS или UDP

Общие сведения/сценарий

Если вы хотя бы однажды выходили в Интернет, то пользовались службой 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 сайта компьютер отправляет DNS-запрос об IP-адресе на DNS-сервер. При запросе компьютером DNS-сервера и ответе DNS-сервера в качестве протокола транспортного уровня используется протокол передачи датаграмм пользователя (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 работы необходим доступ в Интернет.

Необходимые ресурсы

Один ПК (Windows 7 или 8 с доступом к командной строке, выходом в Интернет и установленной программой Wireshark)

Часть 1: Запись данных IP-конфигурации ПК

В части 1 с помощью команды **ipconfig /all** на локальном ПК вам нужно будет найти и записать MAC-адрес и IP-адрес сетевой платы вашего 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	
MAC-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 будет настроить программу Wireshark для захвата пакетов запросов и ответов DNS, чтобы продемонстрировать использование транспортного протокола UDP при обмене данными с DNS-сервером.

a. Нажмите кнопку **Пуск** и откройте программу Wireshark.

b. Выберите интерфейс для захвата пакетов с помощью Wireshark. Используйте **Interface List** (Список интерфейсов) для выбора интерфейса, связанного с записанными в части 1 IP-адресом и MAC-адресом ПК.

c. Выбрав нужный интерфейс, нажмите **Start** (Пуск), чтобы начать захват пакетов.

d. Откройте веб-браузер и введите адрес **www.google.com**. Для продолжения нажмите клавишу **Enter**.

e. Как только откроется домашняя страница Google, нажмите кнопку **Stop** (Остановить), чтобы остановить захват данных программой Wireshark.

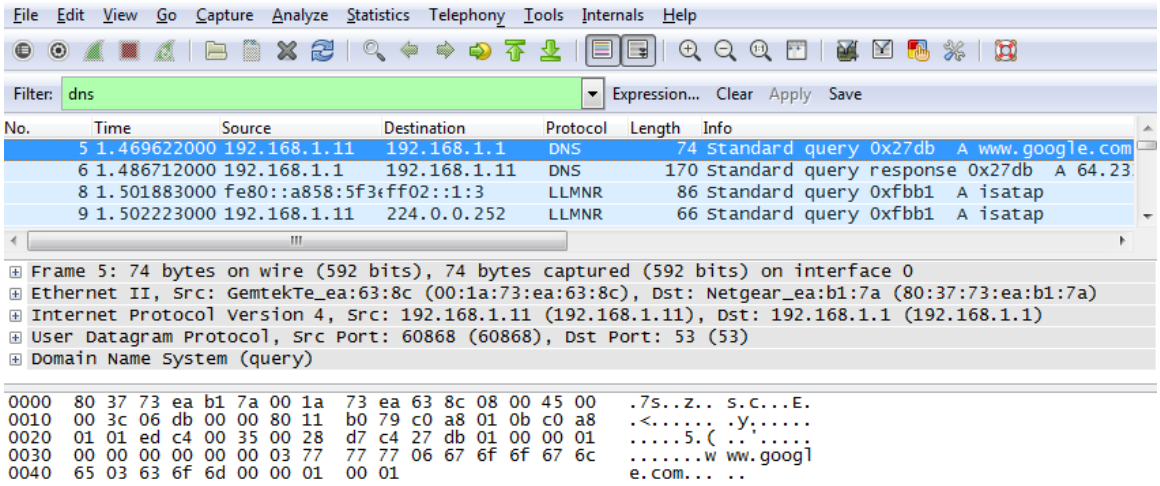
Часть 3: Анализ захваченных пакетов DNS или UDP

В части 3 вам необходимо будет 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 поле **Filter** (Фильтр). Нажмите **Apply** (Применить) или клавишу **Enter**.

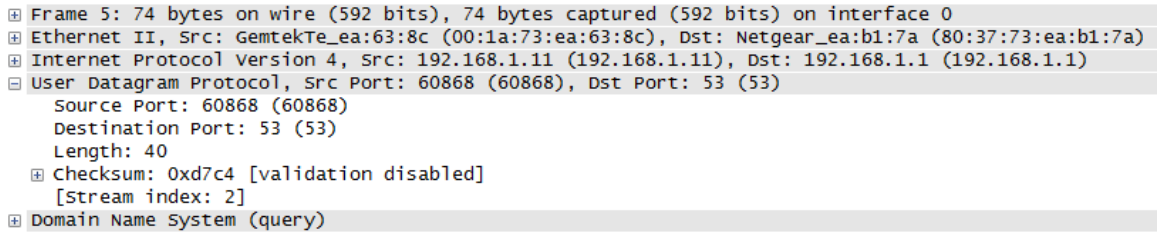
Примечание. Если после применения фильтра DNS вы не видите никаких результатов, закройте браузер. В окне командной строки введите **ipconfig /flushdns** для удаления всех предыдущих результатов DNS. Перезапустите захват данных программой Wireshark и повторите шаги 2Б — 2Д. Если таким образом решить проблему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



b. На панели списка захваченных пакетов (верхний раздел) в главном окне программы найдите пакет с информацией **Standard query** (Стандартный запрос) и **A www.google.com**. В качестве примера можно взять кадр 5.

Шаг 2: 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 5 на панели списка захваченных пакетов. Протоколы в этом запросе отображаются на панели сведений о пакетах (средний раздел) в главном окне. Сведения о протоколе выделены серым цветом.



a. Как показано в первой строке на панели сведений о пакетах, кадр 5 содержал 74 байта данных во время передачи. Это количество байтов для отправки DNS-запроса на сервер доменных имен с запросом IP-адресов сайта www.google.com.

b. Строка Ethernet II содержит MAC-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?

c. В строке Internet Protocol Version 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 указать IP-адрес и MAC-адрес для устройств источника и назначения?

Устройство	IP-адрес	MAC-адрес
Локальный ПК		
Шлюз по 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 назначения, длина и контрольная сумма. Как показано ниже, длина каждого поля в заголовке UDP составляет всего 16 бит.

СЕГМЕНТ UDP

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

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.

```
⊟ User Datagram Protocol, Src Port: 60868 (60868), Dst Port: 53 (53)
    Source Port: 60868 (60868)
    Destination Port: 53 (53)
    Length: 40
  ⊟ Checksum: 0xd7c4 [validation disabled]
      [Good Checksum: False]
      [Bad Checksum: False]
    [Stream index: 2]
```

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).

```
⊟ Domain Name System (query)
    [Response In: 6]
    Transaction ID: 0x27db
  ⊞ 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
        [Name Length: 14]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

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	
MAC-адрес источника	
MAC-адрес назначения	
IP-адрес источника	
IP-адрес назначения	
Порт источника	
Порт назначения	

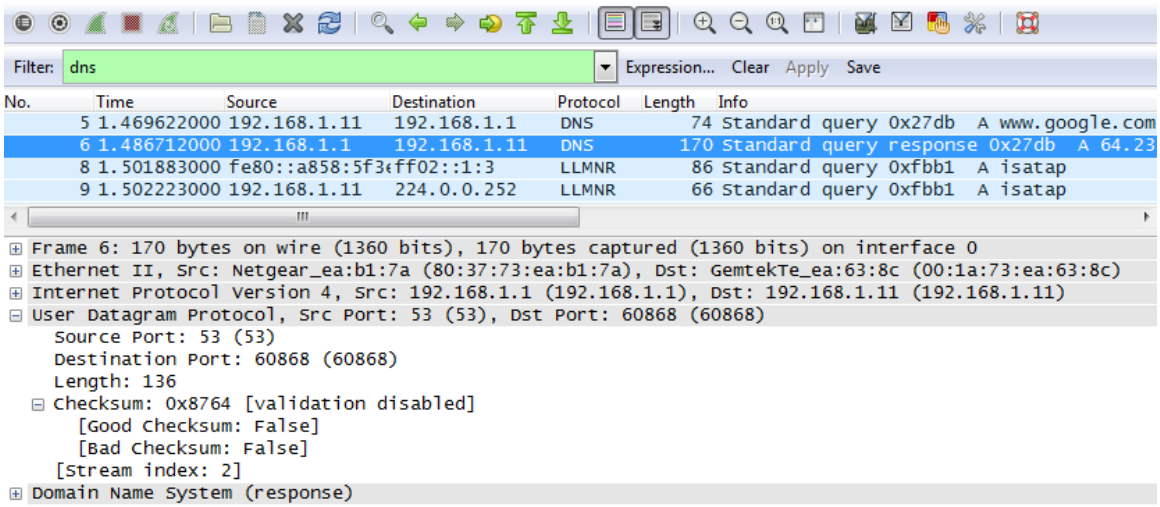
Совпадает ли IP-адрес источника с IP-адресом локального ПК, записанным в части 1?

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

Шаг 3: Изучите 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.

a. В данном примере соответствующим пакетом DNS-ответа является кадр 6. Обратите внимание на то, что количество байтов во время передачи составляет 170. Этот пакет превышает по объему пакет DNS-запроса.



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

c. Обратите внимание на IP-адреса источника и назначения в IP-пакете. Назовите IP-адрес назначения. Назовите IP-адрес источника.

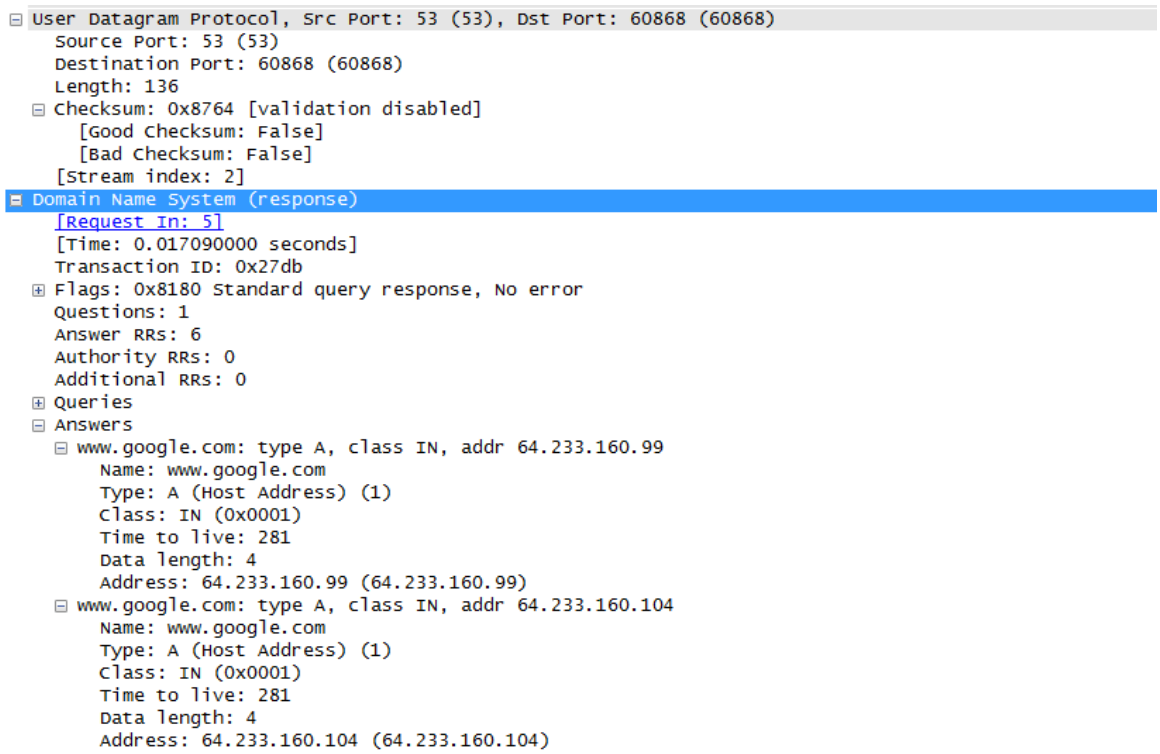
IP-адрес назначения: IP-адрес источника:

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 — 60868. Номер порта 60868 — 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).



Вопросы для повторения

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

