Лабораторная работа: изучение захваченных данных DNS 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

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 IP-конфигурации ПК

В части 1 с помощью команды **ipconfig /all** на локальном ПК вам нужно будет найти и записать MAC- и IP-адреса сетевого адаптера вашего ПК, IP-адрес указанного шлюза по умолчанию и IP-адрес DNS-сервера, указанного для ПК. Запишите эти данные в приведённую ниже таблицу. Они вам потребуются 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 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 http://www.wireshark.org/download.html.

b. Выберите интерфейс Wireshark для захвата пакетов. Используйте **Interface List** (Список интерфейсов), чтобы выбрать интерфейс, который связан IP- и MAC-адресами ПК, записанными в части 1.

c. 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.

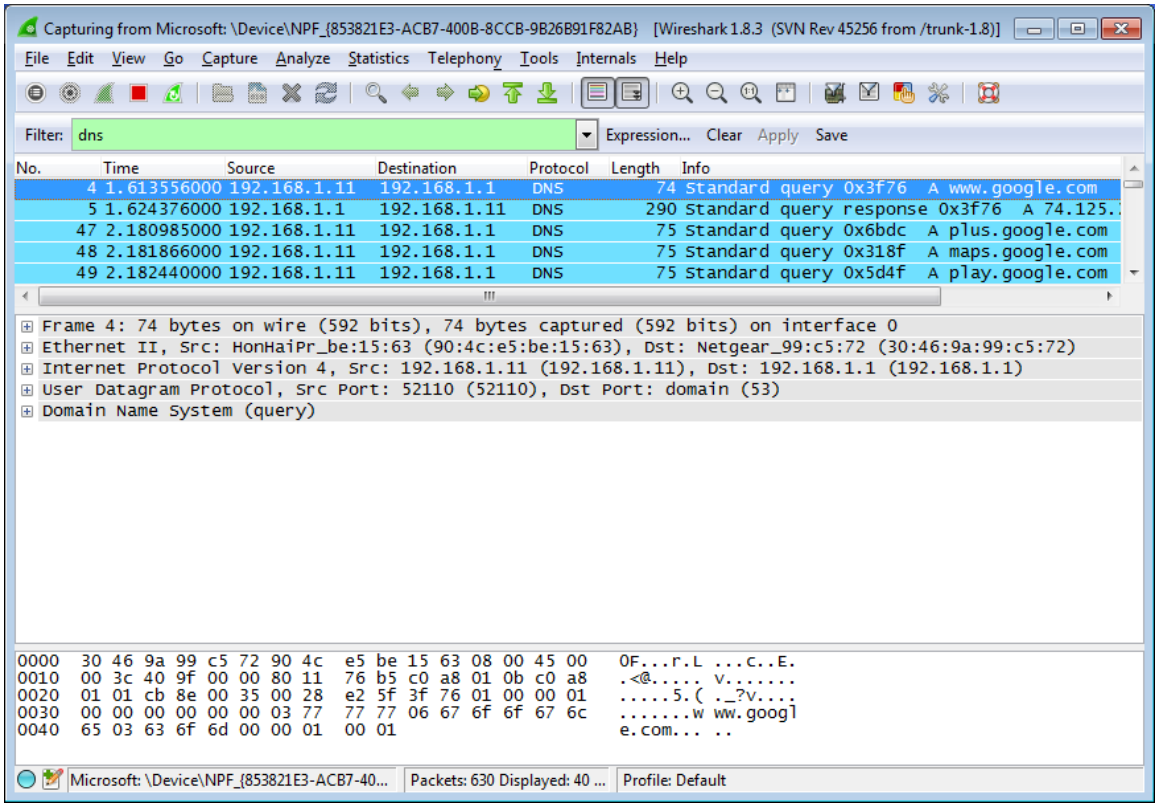
Часть 3: Анализ захваченных пакетов DNS или UDP

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.

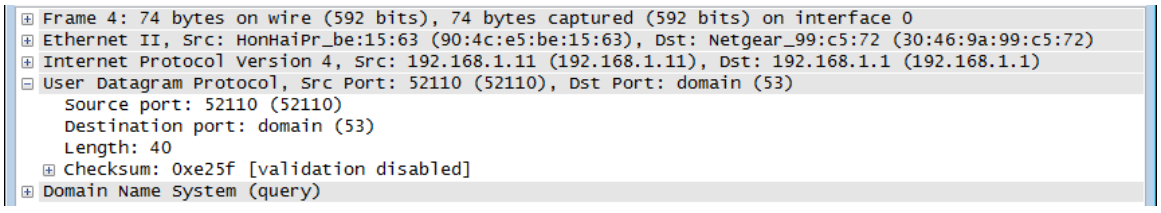
   Примечание. Если после применения фильтра DNS никакие результаты не отображаются, закройте веб-браузер и введите в окне командной строки команду **ipconfig /flushdns**, чтобы удалить все предыдущие результаты DNS. Перезапустите захват данных программой Wireshark и повторите шаги 2b–2e. Если решить проблему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



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.



a. 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 IP-адреса 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 MAC-адрес источника с адресом, записанным в части 1 для локального ПК?

c. 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 MAC-адреса для устройств источника и назначения?

Устройство	IP-адрес	MAC-адрес
Локальный ПК		
Шлюз по умолчанию		

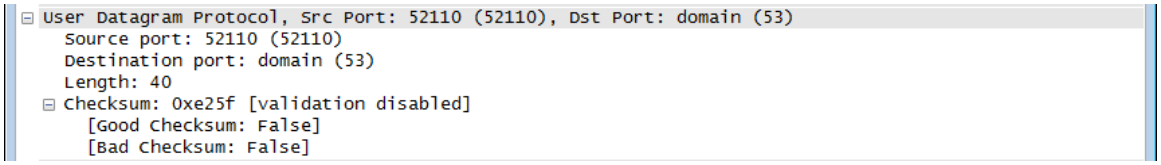
IP-пакет и заголовок инкапсулируют сегмент UDP. Сегмент UDP содержит DNS-запрос в виде данных.

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

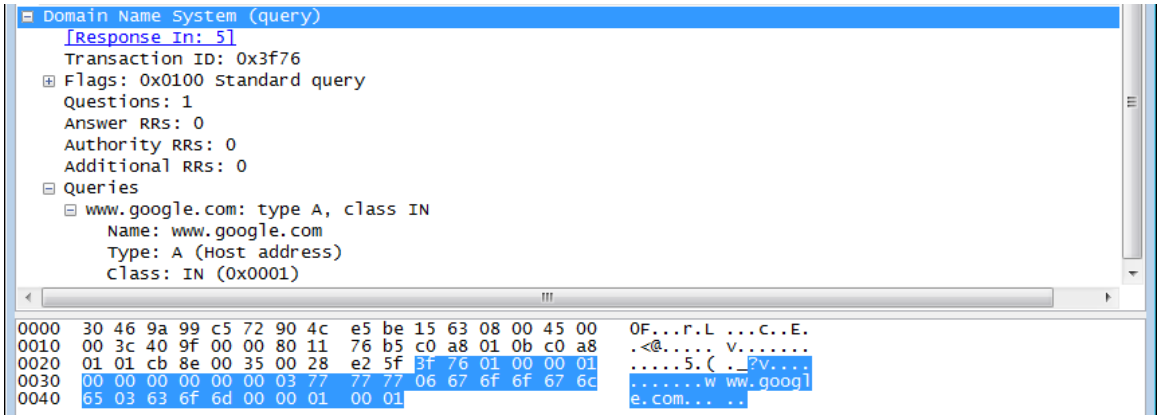
СЕГМЕНТ UDP

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

Разверните 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.



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).



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

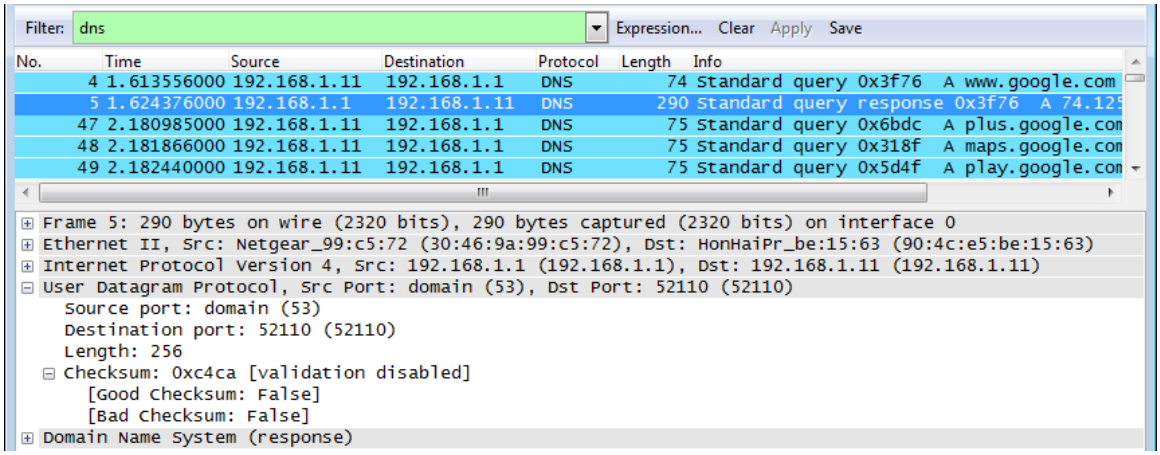
Совпадает ли IP-адрес источника с IP-адресом локального ПК, записанным в части 1?

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

Шаг 3: Изучите 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 5. Обратите внимание на то, что количество байт на линии составляет 290. Этот пакет превышает по объёму пакет DNS-запроса.



b. Судя по кадру Ethernet II для DNS-ответа, с какого устройства получен MAC-адрес источника и какое устройство является MAC-адресом назначения?

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

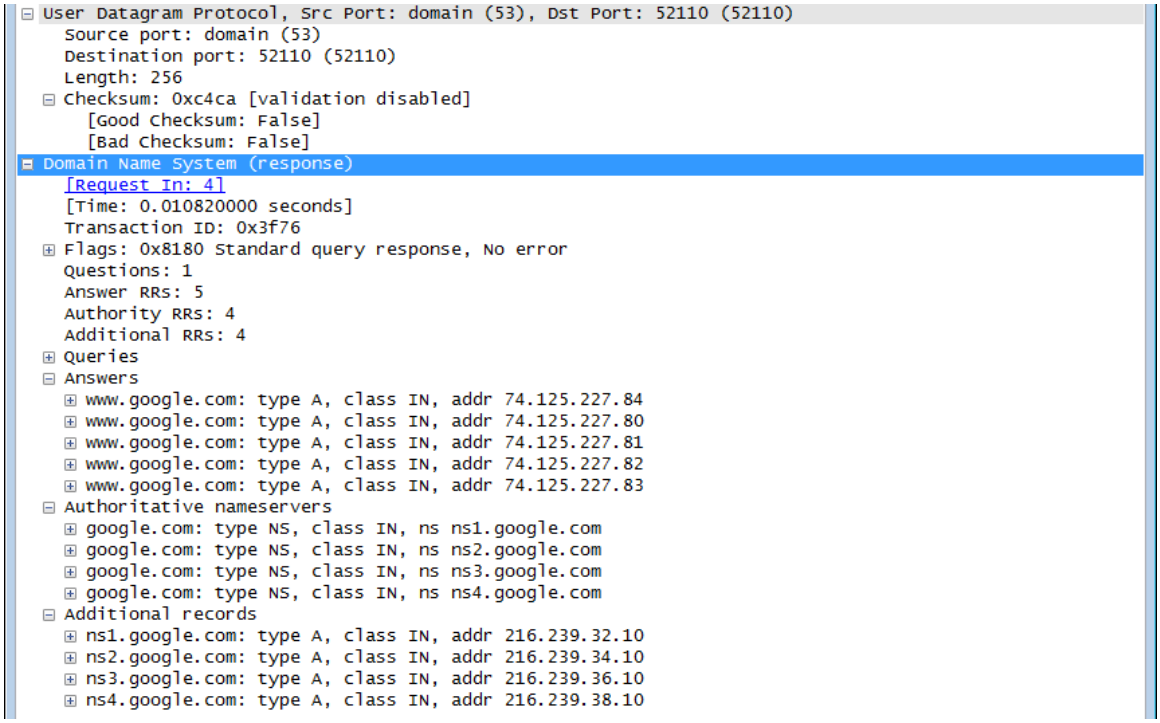
IP-адрес назначения: IP-адрес источника:

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 — 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**.



Вопросы на закрепление

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