МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,

СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»

(СПбГУТ)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Факультет инфокоммуникационных сетей и систем

Кафедра защищенных систем связи

Дисциплина Безопасность компьютерных сетей

ЛАБОРАТОРНАЯ РАБОТА №1

Изучение перехваченных пакетов DNS и UDP с помощью программы Wireshark

Направление/специальность подготовки

11.03.02 Инфокоммуникационные технологии и системы связи

Студент:

Громов А. А., ИКТЗ-83 \_\_\_\_\_\_\_\_\_

*(Ф.И.О., № группы) (подпись)*

Проверил:

Ушаков И. А.

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

1. Топология



1. Задачи

Часть 1. Запись данных IP-конфигурации ПК

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

Часть 3. Анализ перехваченных пакетов DNS или UDP

1. Общие сведения и сценарий

Когда вы пользуетесь Интернетом, то используете систему 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.

1. Необходимые ресурсы

* Виртуальная машина рабочей станции CyberOps
* Доступ к Интернету

1. Запись данных IP-конфигурации ВМ

В части 1 вы воспользуетесь командами на ВМ рабочей станции CyberOps, чтобы найти и записать МАС-адрес и IP-адрес сетевой интерфейсной платы своей ВМ, 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 | ﻿192.168.0.10 |
| MAC-адрес | ﻿08:00:27:2d:4d:c7 |
| IP-адрес шлюза по умолчанию | ﻿192.168.0.1 |
| IP-адрес DNS-сервера | 8.8.4.4 |

* + 1. Откройте терминал на ВМ. Введите **ifconfig** в командную строку, чтобы отобразить сведения об интерфейсе.

[analyst@secOps ~]$ **ifconfig**

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 192.168.1.19 netmask 255.255.255.0 broadcast 192.168.1.255

inet6 fe80::997f:9b16:5aae:1868 prefixlen 64 scopeid 0x20<link>

ether 08:00:27:c9:fa:a1 txqueuelen 1000 (Ethernet)

RX packets 1381 bytes 87320 (85.2 KiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 24 bytes 1857 (1.8 KiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

device interrupt 19 base 0xd000

<некоторые выходные данные пропущены>

* + 1. В командной строке терминала введите **cat /etc/resolv.conf** для определения DNS-сервера.

[analyst@secOps ~]$ **cat /etc/resolv.conf**

# Generated by resolvconf

nameserver 192.168.1.1

* + 1. В командной строке терминала введите **netstat -r** для отображения таблицы IP-маршрутизации на IP-адрес шлюза по умолчанию.

[analyst@secOps ~]$ **netstat -r**

Таблица IP-маршрутизации

Destination Gateway Genmask Flags MSS Window irtt Iface

default 192.168.1.1 0.0.0.0 UG 0 0 0 enp0s3

192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 enp0s3

**Примечание**. IP-адрес DNS и IP-адрес шлюза по умолчанию часто совпадают, особенно в небольших сетях. Однако в школьной сети или сети компании адреса, скорее всего, будут различаться.

1. Перехват запросов и ответов DNS с помощью программы Wireshark

В части 2 вы настроите программу Wireshark для перехвата пакетов запросов и ответов DNS. Таким образом демонстрируется использование транспортного протокола UDP при обмене данными с DNS-сервером.

* + 1. В окне терминала запустите программу Wireshark и нажмите кнопку **ОК**  в ответ на приглашение.

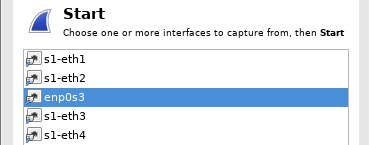
[analyst@secOps ~]$ **sudo wireshark-gtk**

[sudo] пароль для analyst:

\*\* (wireshark-gtk:950): WARNING \*\*: Couldn't connect to accessibility bus: Failed to connect to socket /tmp/dbus-REDRWOHelr: Connection refused (ПРЕДУПРЕЖДЕНИЕ \*\*. Не удается подключиться к шине доступности. Не удалось подключиться к сокету /tmp/dbus-REDRWOHelr. В подключении отказано.)

Gtk-Message: GtkDialog mapped without a transient parent (GtkDialog сопоставлен без промежуточного родителя) Это не рекомендуется.

* + 1. В окне Wireshark выберите **enp0s3** из списка интерфейсов и нажмите кнопку **Start** (Пуск).



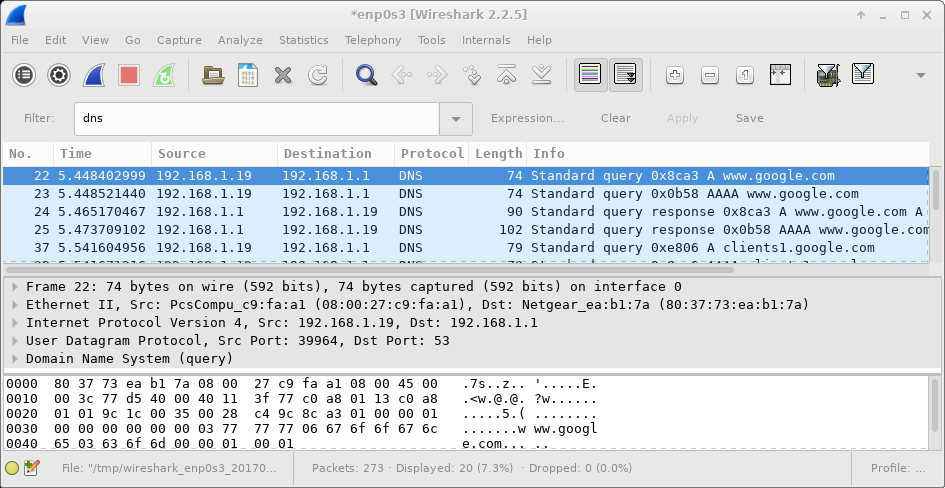
* + 1. Выбрав нужный интерфейс, нажмите Start (Пуск), чтобы начать захват пакетов.
    2. Откройте веб-обозреватель и введите адрес **www.google.com**. Нажмите клавишу Enter (Ввод), чтобы продолжить.
    3. Как только откроется главная страница Google, нажмите кнопку **Stop** (Остановить), чтобы остановить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

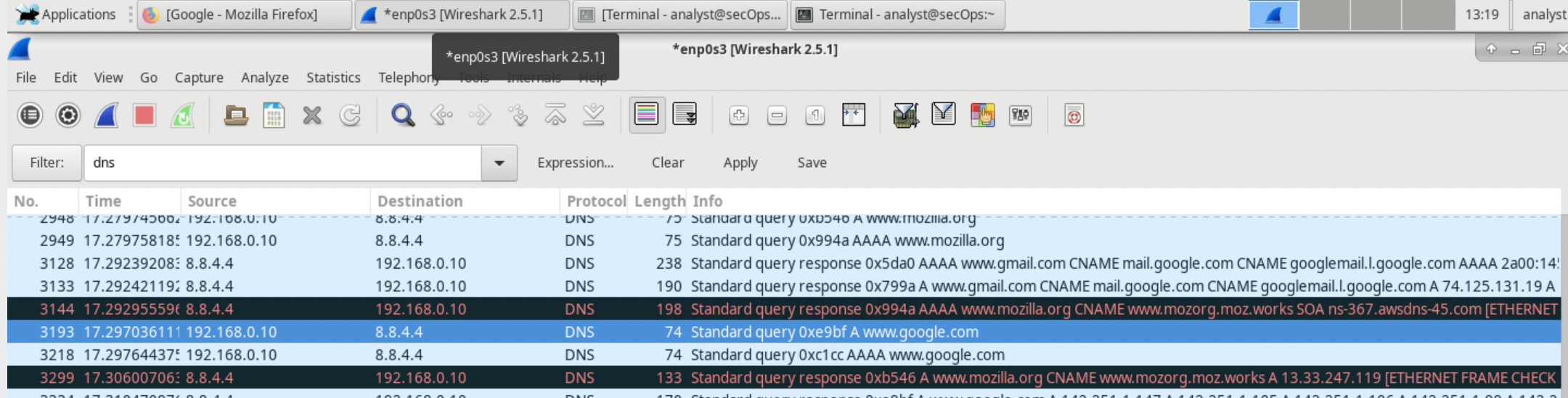
1. Анализ перехваченных пакетов DNS или UDP

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). Нажмите **Apply** (Применить).

**Примечание**. Если после применения фильтра DNS вы не видите никаких результатов, закройте веб-обозреватель. В окне терминала введите ping [**www.google.com**](http://www.google.com) в качестве альтернативы браузеру.





* + 1. 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 посмотрите кадр 22 выше.
  1. Изучение полей в пакете запроса DNS.

Поля протокола, выделенные серым, отображаются на панели сведений о пакетах (средний раздел) главного окна.

* + 1. Как показано в первой строке на панели сведений о пакетах, кадр 22 содержал 74 байта данных во время передачи. Это число байтов, потребовавшееся для отправки DNS-запроса на именованный сервер, запросивший IP-адреса сайта www.google.com. Если используется другой веб-адрес, например www.cisco.com, количество байтов может быть иным.
    2. Строка Ethernet II содержит МАС-адреса источника и места назначения. MAC-адрес источника принадлежит вашей ВМ 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 ВМ?

да

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

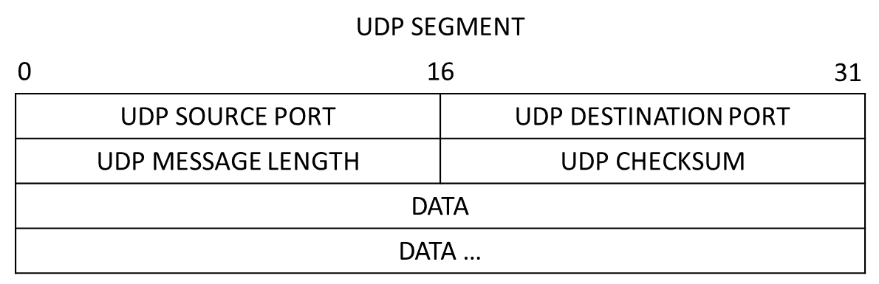
* + 1. В строке Internet Protocol Version 4 перехваченные программой Wireshark данные IP-пакета показывают, что IP-адрес источника данного DNS-запроса — 192.168.1.19, а IP-адрес назначения — 192.168.1.1. В данном примере адрес назначения — это шлюз по умолчанию. В данной сети шлюзом по умолчанию является маршрутизатор.

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

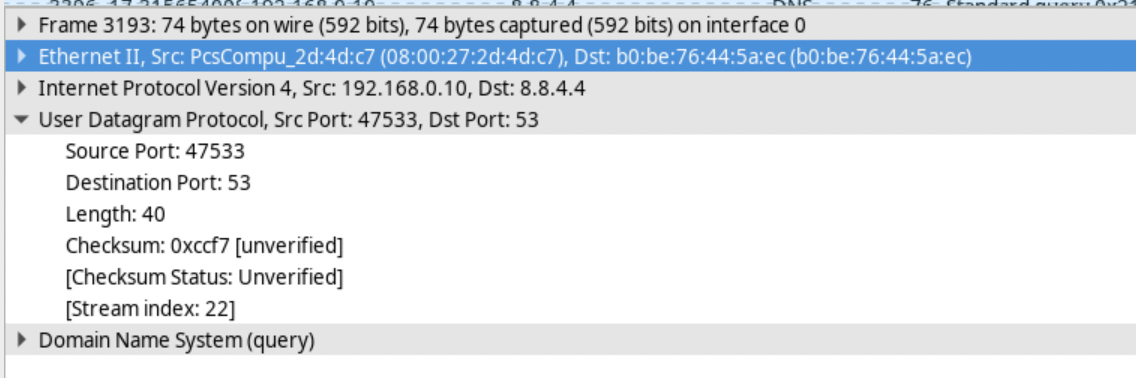
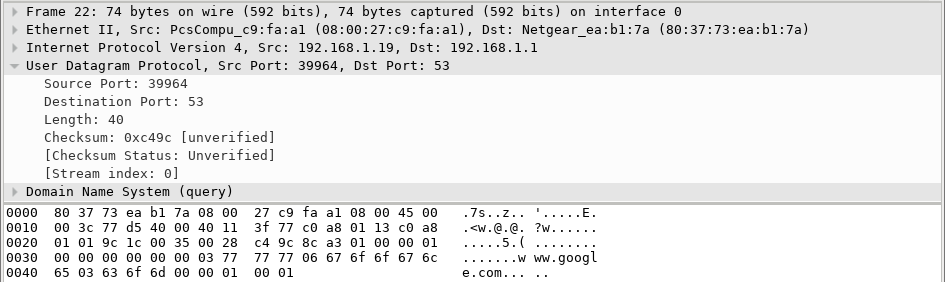
|  |  |  |
| --- | --- | --- |
| Устройство | IP-адрес | MAC-адрес |
| ВМ | 192.168.0.10 | ﻿08:00:27:2d:4d:c7 |
| Шлюз по умолчанию | 8.8.4.4(ip dns) | ﻿b0:be:76:44:5a:ec(MAC роутера) |

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

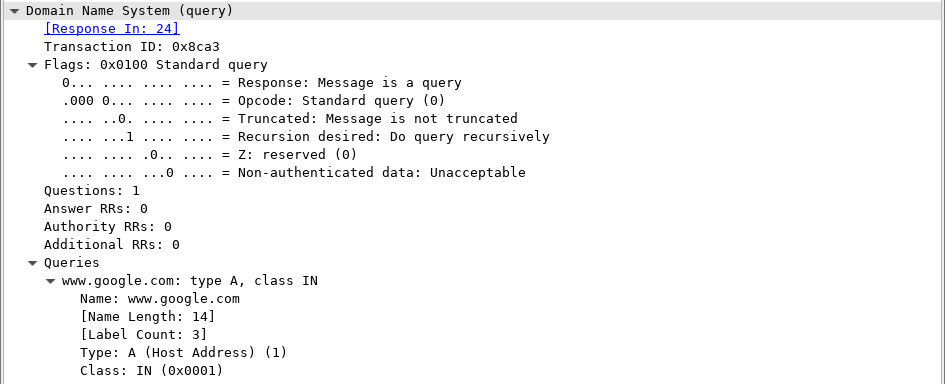
* + 1. Щелкните стрелку рядом с протоколом пользовательских датаграмм, чтобы просмотреть сведения. Заголовок UDP имеет только четыре поля: порт источника, порт назначения, длина и контрольная сумма. Как показано ниже, длина каждого поля в заголовке UDP составляет всего 16 бит.

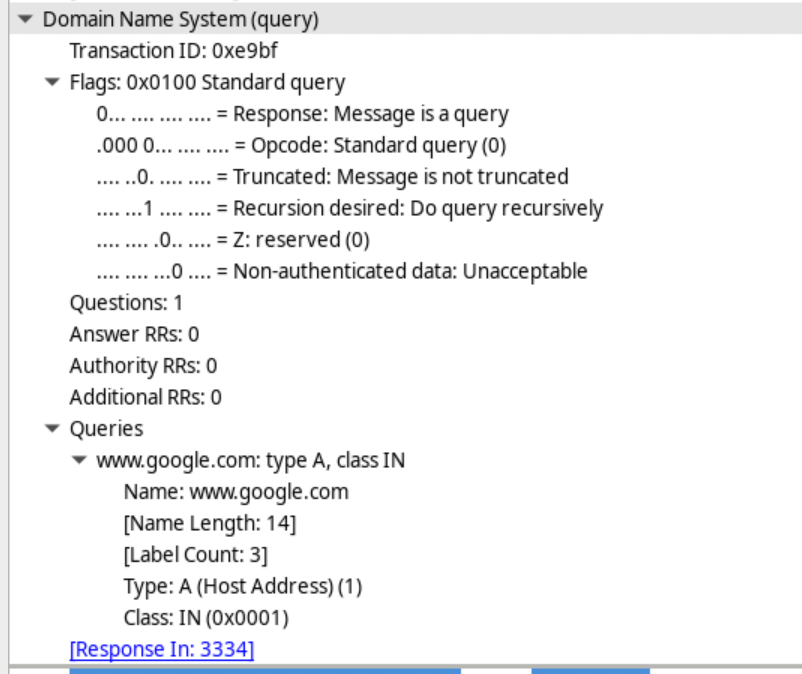


* + 1. Щелкните стрелку рядом с протоколом пользовательских датаграмм, чтобы просмотреть сведения. Обратите внимание на то, что отображаются всего четыре поля. Номер порта источника в данном примере — 39964. Порт источника был случайным образом сформирован ВМ с использованием незарезервированных номеров 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. Длина сегмента UDP в данном примере может быть иной. 8 из 40 байт используются в качестве заголовка. Остальные 32 байта используются данными DNS-запроса. На следующем рисунке показаны 32 байта данных DNS-запроса на панели отображения байтов пакета (нижний раздел) главного окна Wireshark.





Контрольная сумма используется для определения целостности заголовка UDP 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 уровне приложений.

Запишите результаты захвата данных программой Wireshark в приведенную ниже таблицу.

|  |  |
| --- | --- |
| Размер кадра | 74 byte |
| MAC-адрес источника | ﻿08:00:27:2d:4d:c7 |
| MAC-адрес назначения | ﻿b0:be:76:44:5a:ec |
| IP-адрес источника | 192.168.0.10 |
| IP-адрес назначения | 8.8.4.4 |
| Порт источника | ﻿47533 |
| Порт назначения | 53 |

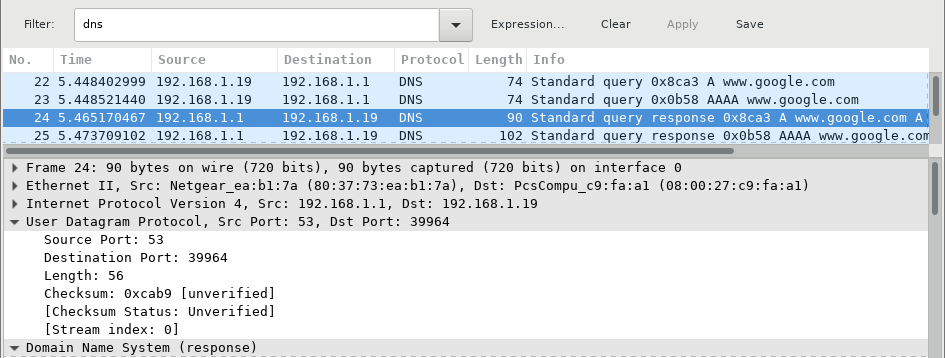
Совпадает ли IP-адрес источника с IP-адресом локального ПК, записанным в части 1? да

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

* 1. Изучение полей в пакете 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 24. Обратите внимание на то, что количество байтов во время передачи составляет 90. Этот пакет превышает по объему пакет DNS-запроса. Это связано с тем, что пакет DNS-ответа будет содержать разнообразные сведения о домене.



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

MAC-адрес источника – шлюз по умолчанию, MAC-адрес назначения - ВМ

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

IP-адрес назначения: ВМ, IP-адрес источника: dns сервер

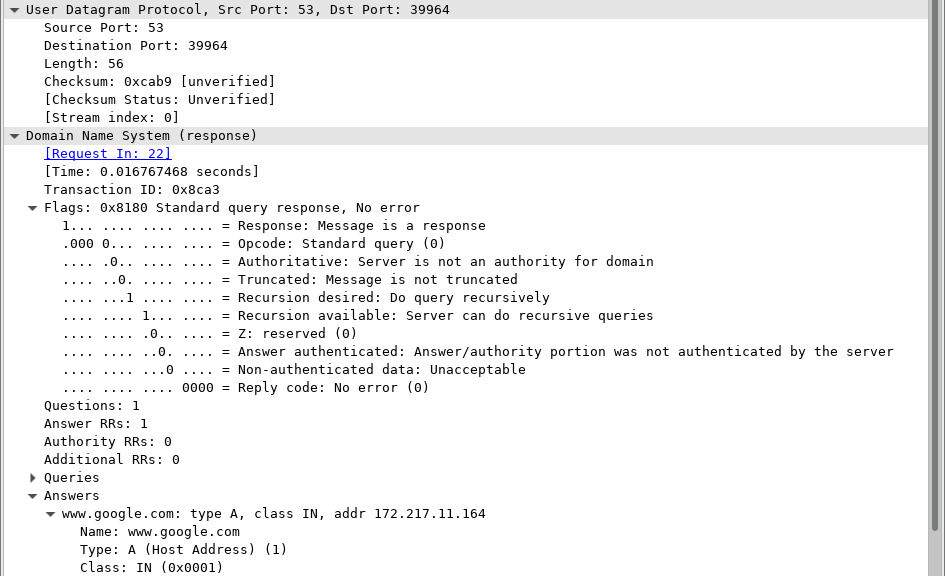
Что произошло с ролями источника и назначения для ВМ и шлюза по умолчанию?

Поменялись местами

* + 1. В сегменте UDP роли номеров портов также изменились на противоположные. Номер порта назначения — 39964. Номер порта 39964 — это тот же номер порта, который был сформирован ВМ при отправке DNS-запроса на DNS-сервер. ВМ 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?

Скорость передачи(за счет отсутствия установления сессии) , объем пакета