Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

Кафедра компьютерных систем в управлении и проектировании (КСУП)

«СИСТЕМА ДОМЕННЫХ ИМЁН»

Отчет к лабораторной работе №7 по дисциплине  
«Сети и телекоммуникации (СиТ)»

Выполнили:

Студенты гр. 589-2

Сухарев М.А.

Карабатов П.В.

Батухтин И.С.

Зайнулин В.C

Принял:

К.т.н, доцент кафедры КСУП

Коколов А.А.

Содержание

[1 Введение 3](#_Toc122551426)

[1.1 Цель работы 3](#_Toc122551427)

[1.2 Задание на лабораторную работу 3](#_Toc122551428)

[2 Ход выполнения работы 5](#_Toc122551429)

[3 Заключение 12](#_Toc122551430)

# Введение

## Цель работы

Целью данной лабораторной работы является изучение принципов работы протокола DNS.

## Задание на лабораторную работу

В данной лабораторной работе требуется сделать следующее:

Первая часть лабораторной работы выполняется с локальной машины, не с терминального сервера! Отчёт должен содержать несколько разобранных DNS пакетов, с полями сопоставленными с сырыми данными (в hex-виде).

1. Запустить WireShark и настроить для захвата DNS пакетов
2. Открыть в браузере yaplakal.com
3. Дождаться загрузки
4. Переписать сколько и каких DNS запросов было сделано локальным DNS-сервером.
5. Очистить лог WireShark
6. Выполнить запрос разыменования доменного имени gmail.com.
7. Расшифровать содержимое ответного пакета.
8. Подключиться к учебному unix серверу, выполнить пункт 6 с помощью утилиты dig.
9. Сравнить результаты, полученные в пунктах 6 и 8.
10. Выполнить запрос разыменования доменного имени google.com и vk.com к следующим DNS серверам:
    * DNS сервер по умолчанию;
    * ns.runnet.ru
    * 8.8.8.8
    * 8.8.4.4
    * 4.2.2.2
    * 198.153.192.1
11. Сравните результаты. Сделать выводы
12. Выполнить пункт 10 после истечения времени жизни локальной копии квитанции. Сравнить результаты. Сделать выводы
13. Сравнить результаты пунктов 10 и 11. Сделать выводы.

# Ход выполнения работы

Для начала воспользуемся Wireshark для анализа запросов/ответов DNS для сайта yaplakal.com

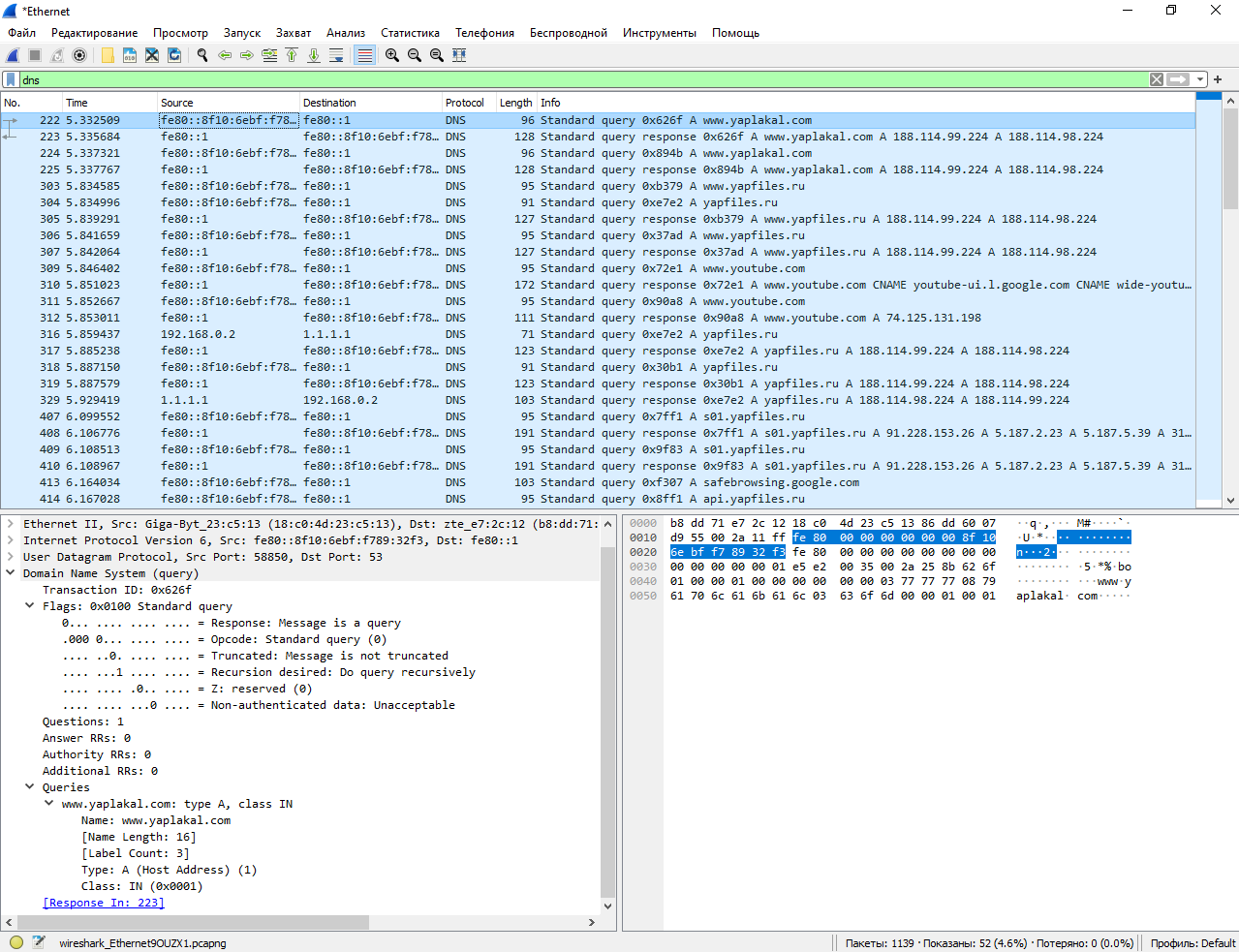


Рисунок .. Интерфейс Wireshark

При посещении данного сайта было отправлено 23 запроса. Локальный DNS сервер разыменовал следующие доменные имена:

Таблица 2.1. Результат разыменовывания

|  |  |
| --- | --- |
| Запрос | Ответ |
| www.yaplakal.com | 188.114.99.224  188.114.98.224 |
| www.yapfiles.ru | 188.114.99.224  188.114.98.224 |
| www.youtube.com | 74.125.131.198 |
| s01.yapfiles.ru | 91.228.153.26  5.187.2.23  5.187.5.39  31.172.70.84  5.187.1.44  91.228.153.11 |
| safebrowsing.google.com | 216.58.207.206 |
| api.yapfiles.ru | 188.114.99.224  188.114.98.224 |
| s02.yapfiles.ru | 5.187.5.39  5.187.2.23  5.187.1.44  91.228.153.11  31.172.70.84  91.228.153.26 |
| jnn-pa.googleapis.com | 142.250.74.74  172.217.21.170  142.250.74.106 |
| i.ytimg.com | 216.58.207.246  216.58.211.22  142.250.74.22  142.250.74.54  142.250.74.86  216.58.207.214  142.250.74.118  142.250.74.150  142.250.74.182 |
| sponsor.ajay.app | 172.64.102.23  172.64.103.23 |
| vk.com | 93.186.225.194  87.240.132.78  87.240.129.133  87.240.132.72  87.240.132.67  87.240.137.164 |

В таблице представлены только уникальные запросы.

Расшифровка основного запроса выглядит так:

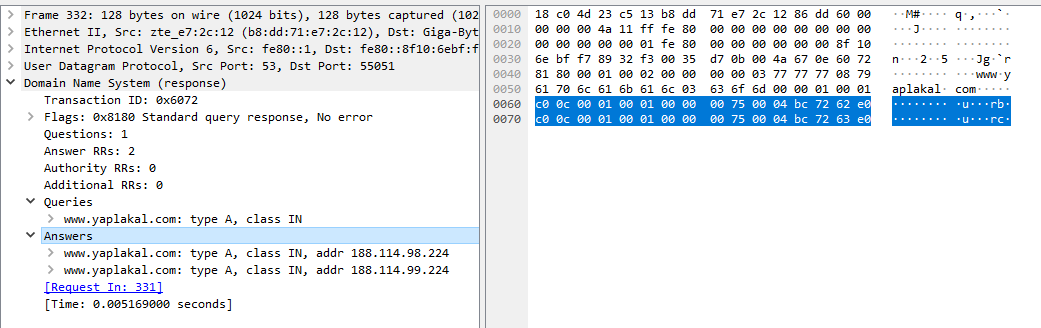


Рисунок 2.2. Расшифровка запроса разыменовывания домена yaplakal.com

Далее произведем операцию разыменовывания домена gmail.com уже вручную с помощью утилиты nslookup. Для этого откроем терминал и запустим утилиту в интерактивном режиме.

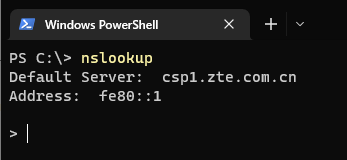


Рисунок 2.3. Запуск nslookup

Стандартный сервер – это сервер роутера ZTE. Теперь отправим запрос на разыменовывание домена gmail.com.

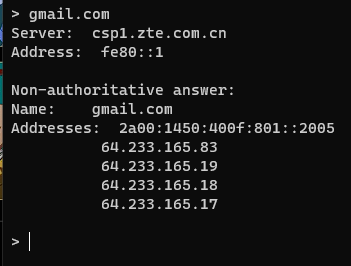


Рисунок 2.4. Разыменовывание gmail.com

Далее повторим пункт 6 из задания, но уже на удаленном учебном сервере с помощью утилиты dig. Для этого через PuTTY подключаемся к kcup.tusur.ru:22.

Вводим в консоль “dig yaplakal.com” и получаем следующий результат:

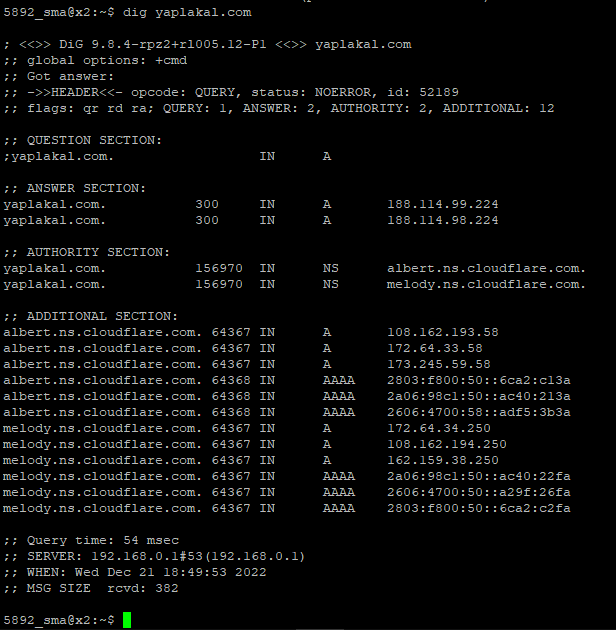


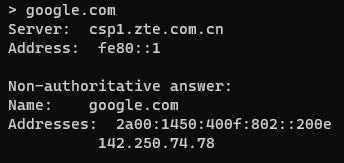
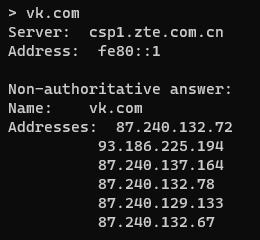
Рисунок 2.5. Разыменовывание домена yaplakal.com с помощю утилиты dig

В результате получаем похожий результат что и в Wireshark, с единственным отличием что после разыменовывания домена не происходило разыменовывание других источников, находившихся на главном домене, так-как они не были обработаны и их адрес не требуется.

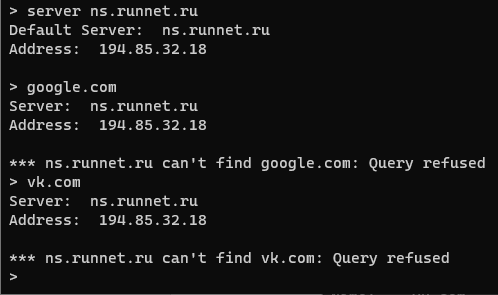
В ответе dig есть как и обычные адреса хостов, так и домены DNS-серверов самого сайта, в данном случае используются DNS Cloudflare.

Теперь перейдем к пункту 10. Для этого вернемся к локальной машине и утилите nslookup. Нужно выполнить запрос для google.com и vk.com на определенные сервера:

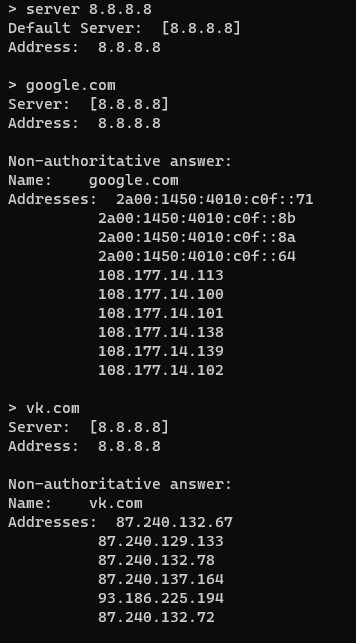
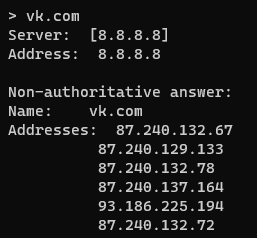
DNS сервер по умолчанию:

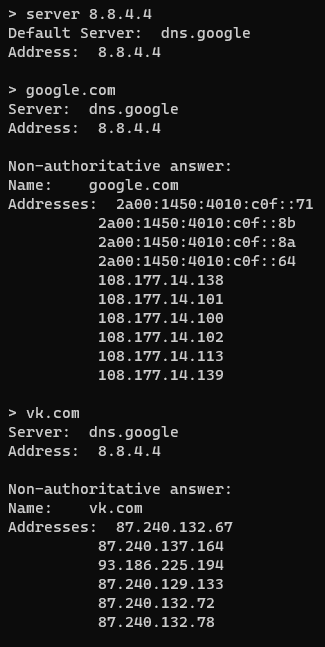
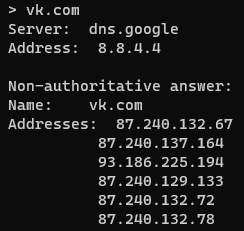
ns.runnet.ru:



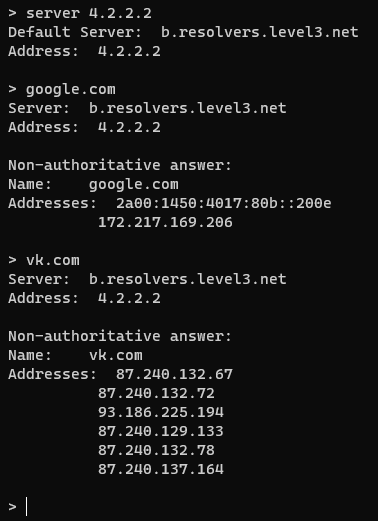
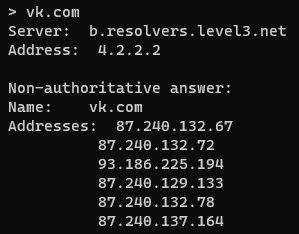
8.8.8.8:

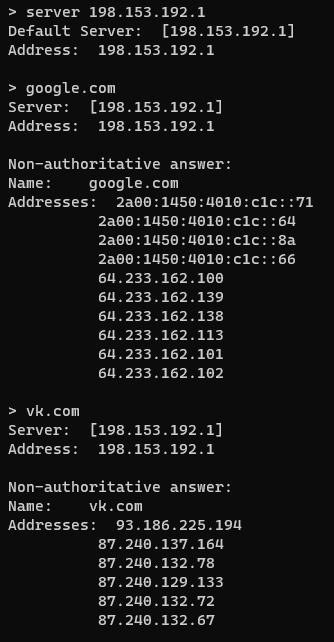
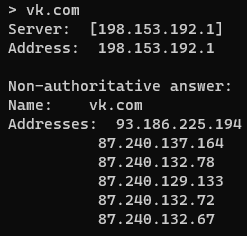
8.8.4.4:

4.2.2.2:

198.153.192.1:

По этим наблюдениям можно сделать вывод, что самые развернутые ответы у серверов 8.8.8.8, 8.8.4.4 и 198.153.192.1. Также сервер ns.runnet.ru не имеет информации о искомых доменах.

Если повторить запросы после окончания времени жизни, то ответ слегка изменится в виде изменения порядка выдачи адресов, но сами адреса остаются неизменными.

# Заключение

В ходе выполнения данной лабораторной работы были получены навыки и знания работы с DNS.