УНИВЕРСИТЕТ ИТМО

Факультет программной инженерии и компьютерной техники

Направление подготовки 09.03.04 Программная инженерия

Дисциплина «Компьютерные сети»

**Лабораторная работа №5**

Студенты

*Кустарев И.П.*

*P33121*

Преподаватель

*Тропченко А.*

Санкт-Петербург, 2023 г.

# Цель работы

*Изучить структуру протокольных блоков данных, анализируя реальный трафик на компьютере студента с помощью бесплатно распространяемой утилиты Wireshark*

*Используемый веб-сайт: https://kip.su/*

# Этап 1. Анализ трафика утилиты ping

ping -l 2000 kip.su

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

## Анализ полученных пакетов

Изображение выглядит как текст, снимок экрана, Шрифт, число

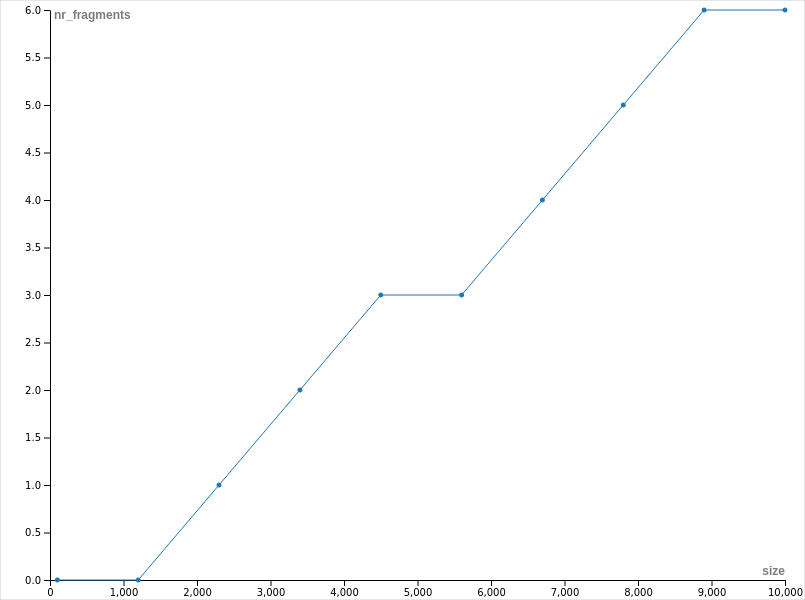
Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

1. *Да, имеет место фрагментация пакета. Указано в поле MF IPv4 пакета.*
2. *Для промежуточных пакетов поле MF=1, для последнего MF=0*
3. *Ping передает данные по 32 байта, так что фрагментации для них нет, т.е. 0 фрагментов*

## График



1. *Использовать флаг -t <ttl>*
2. *Символы английского алфавита, иногда может быть отметка времени и Sequence Number ICMP-пакета.*

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

# Этап 2. Анализ трафика утилиты tracert

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

1. *Заголовок: 20 байт, данные: 92.*
2. *Увеличивается на 1 каждые 3 пакета, чтобы выявить расстояние в хопах до хоста*
3. *В ping-пакетах есть отметка времени, дефолтное значение TTL сильно выше, не меняется со следующим пакетом (в силу специфики утилиты)*
4. *Различные значения в поле Type*
5. *Будут также слаться DNS запросы, чтобы разрешить IP-адреса в доменные имена*

# Этап 3. Анализ HTTP-трафика (для анализа взял сайт <http://www.kip-guide.ru/>, тк у <https://kip.su/> - используется TLS)

Изображение выглядит как текст, меню, документ, Шрифт

Автоматически созданное описание

1. *Сначала получаем гипертекст на запрошенном сайте*
2. *Поочередно получаем необходимые в html тексте скрипты js*
3. *Поочередно получаем необходимые картинки для отображения содержимого сайта*
4. *При вторичном запросе-обновлении получаем код ответа 304 “Not modified”, т. к. содержимое страницы не менялось*

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

# Этап 4. Анализ DNS трафика

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, Шрифт, число

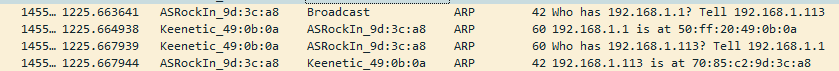
Автоматически созданное описание

1. *Адрес отправки соответствует шлюзу по умолчанию.*
2. *Типы DNS-запросов:*

* ***Итеративный (прямой).*** *Ожидает либо IP-адрес доменного имени, либо имя DNS-сервера ответственного за данный домен. Так работают корневые или TLD серверы. Сервер, к которому обратились, не обращается к другим серверам*
* ***Рекурсивный.*** *Получает доменное имя и принимает IP-адрес, dns-сервер может обращаться к другим серверам*
* ***Обратный.*** *Сервер получает IP, должен вернуть доменное имя.*

1. *Выполнять дополнительные DNS запросы необходимо, когда картинки лежат на другом доменном имени, а не на том же хосте*

# Этап 5. Анализ ARP трафика



Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

1. *MAC-адреса*

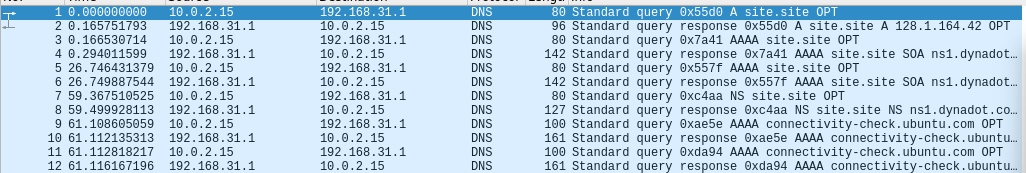
* *70:85:c2:9d:3c:a8 - MAC-адрес нашего устройства*
* *00:00:00:00:00:00 - MAC заполнитель, пока не будет получен реальный адрес*
* *50:ff:20:49:0b:0a - MAC-адрес маршрутизатора*

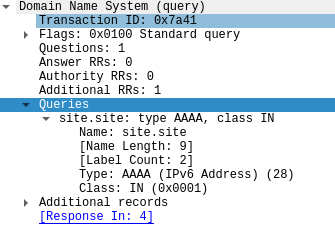
1. *Те же самые, что и в первом пункте*
2. *IP адрес содержится в запросе по следующим причинам:*

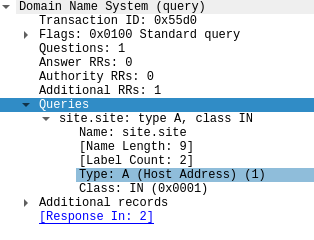
*Во-первых, этот адрес нужен для заполнения ARP-таблицы.*

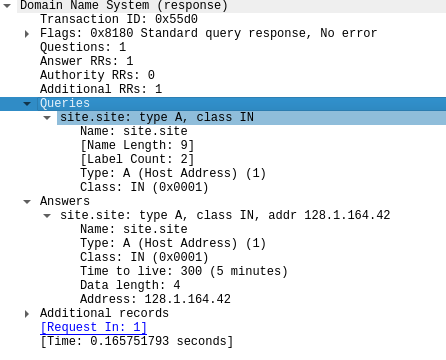
*Во-вторых, чтобы можно был сразу ответить на запрос, не отправляя ответный запрос*

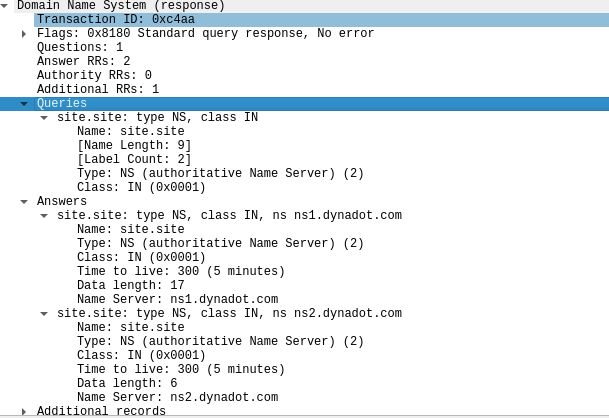
# Этап 6. Анализ утилиты nslookup



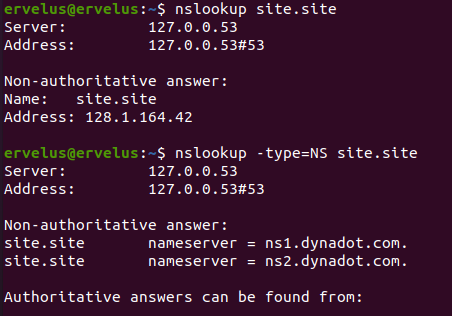








1. *Различия:* 
   * *Queries: type (IPv6 Address и Host Address)*
   * *Answers: type (A и NS)*
2. *В зависимости от типа запроса, поле может содержать:*
   * *IPv4 адрес (для типа A)*
   * *IPv6 адрес (для типа AAAA)*
   * *Доменное имя сервера (для типа NS)*
   * *MX (для почты)*
3. *Серверов, возвращающих авторитативный отклик, нет*



# Вывод по лабораторной работе

*Во время выполнения лабораторной работы мы познакомились с работой различных протоколов передачи данных, проанализировали переданные пакеты с помощью программы Wireshark и протестировали соединения через разные утилиты.*