УНИВЕРСИТЕТ ИТМО

Факультет программной инженерии и компьютерной техники

Направление подготовки 09.03.04 Программная инженерия

Дисциплина «Компьютерные сети»

**Лабораторная работа №5**

Студенты

*Кузнецов М. А.*

*P33131*

Преподаватель

*Тропченко А. А.*

Санкт-Петербург, 2023 г.

Оглавление

[Цель работы 2](#_Toc103095153)

[Этап 1. Анализ трафика утилиты ping 2](#_Toc103095154)

[Анализ полученных пакетов 2](#_Toc103095155)

[График 3](#_Toc103095156)

[Этап 2. Анализ трафика утилиты tracert 4](#_Toc103095157)

[Этап 3. Анализ HTTP-трафика 5](#_Toc103095158)

[Этап 4. Анализ DNS трафика 6](#_Toc103095159)

[Этап 4. Анализ ARP трафика 7](#_Toc103095160)

[Этап 6. Анализ утилиты nslookup 8](#_Toc103095161)

[Вывод по лабораторной работе 10](#_Toc103095162)

# Цель работы

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

*Используемый веб-сайт: https://maxkuznetsov.space*

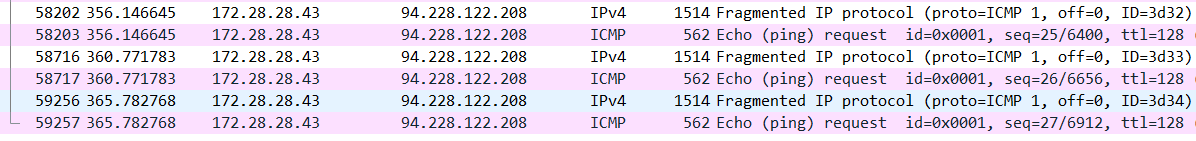
# Этап 1. Анализ трафика утилиты ping

ping -l 2000 maxkuznetsov.space

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

## Анализ полученных пакетов



Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

1. ***Имеет ли место фрагментация исходного пакета? Какое поле на это указывает?*** *Да, имеет. Флаг More Fragments как раз указывает на наличие фрагментации исходного пакета.*
2. ***Какая информация указывает, является ли фрагмент пакета последним или промежуточным?*** *Для промежуточных пакетов поле MF=1, для последнего MF=0*
3. ***Чему равно количество фрагментов при передаче ping-пакетов?*** *Ping передает данные по 32 байта, так что фрагментации для них нет, т.е. 0 фрагментов*

## График

Изображение выглядит как линия, диаграмма, График, Параллельный

Автоматически созданное описание

1. ***Как изменить поле TTL с помощью утилиты ping?*** *Для изменения TTL нужно добавить ключ -i, его аргументом является срок жизни пакета в миллисекундах*
2. ***Что содержится в поле данных пакета ping?*** *Символы английского алфавита.*

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

# Этап 2. Анализ трафика утилиты tracert

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

1. ***Сколько байт содержится в заголовке IP? Сколько байта содержится в поле данных?*** *Заголовок: 20 байт, данные: 64.*
2. ***Как и почему изменяется поле TTL в следующих друг за другом ICMP пакетах tracert?*** *Утилита отправляет первый пакет с TTL равным 1, и увеличивает значение на 1 для каждого последующего отправляемого пока назначение не ответит или пока не будет достигнуто максимальное значение.*
3. ***Чем отличаются ICMP пакеты, генерируемые утилитой tracert, от ICMP пакетов, генерируемых утилитой ping?*** *В поле данных у tracert содержатся нули.*

Изображение выглядит как текст, снимок экрана, Шрифт, дизайн

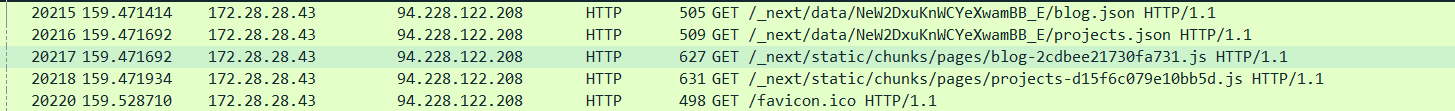
Автоматически созданное описание

1. ***Чем отличаются полученные пакеты ICMP reply от ICMPP error и зачем нужны оба этих типа ответов?*** *Пакеты ICMP reply указывают на получение нового ответного сообщения. Пакеты ICMP error указывают на то, что произошла ошибка. Они используются, чтобы различать причину истечения TTL.*
2. ***Что изменится в работе tracert, если убрать ключ -d? Какой дополнительный трафик при этом будет генерироваться?*** *Будут также слаться DNS запросы, чтобы разрешить IP-адреса в доменные имена*

# Этап 3. Анализ HTTP-трафика

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание



Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

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*

# Этап 4. Анализ DNS трафика

Изображение выглядит как стол

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описание

1. ***Почему адрес, на который отправлен DNS-запрос, не совпадает с***

***адресом посещаемого сайта?*** *Адрес отправки соответствует шлюзу по умолчанию.*

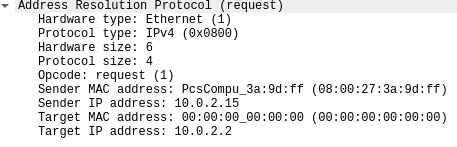
1. ***Какие бывают типы DNS-запросов****? Типы DNS-запросов:*

* ***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. ***В какой ситуации нужно выполнять независимые DNS-запросы для получения содержащихся на сайте изображений?****Выполнять дополнительные DNS запросы необходимо, когда картинки лежат на другом доменном имени, а не на том же хосте*

# Этап 4. Анализ ARP трафика





1. ***Какие МАС-адреса присутствуют в захваченных пакетах ARP протокола? Что означают эти адреса? Какие устройства они***

***идентифицируют?***

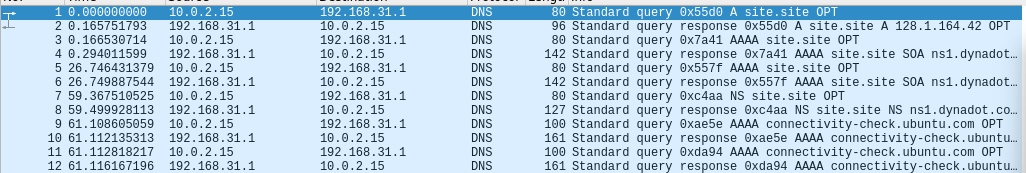
* *08:00:27:3a:9d:ff- MAC-адрес нашего устройства*
* *00:00:00:00:00:00 - MAC заполнитель, пока не будет получен реальный адрес*
* *52:54:00:12:35:02 - MAC-адрес маршрутизатора*

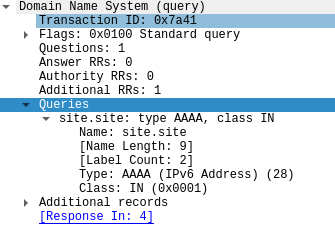
1. ***Какие МАС-адреса присутствуют в захваченных HTTP-пакетах и что означают эти адреса? Что означают эти адреса? Какие устройства они идентифицируют?*** *Те же самые, что и в первом пункте*
2. ***Для чего ARP-запрос содержит IP-адрес источника?*** *IP адрес содержится в запросе по следующим причинам:*

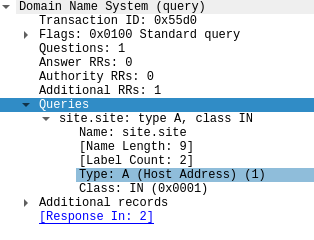
*Во-первых, этот адрес нужен для заполнения ARP-таблицы.*

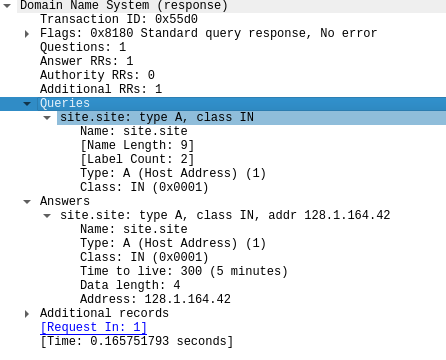
*Во-вторых, чтобы можно был сразу ответить на запрос, не отправляя ответный запрос*

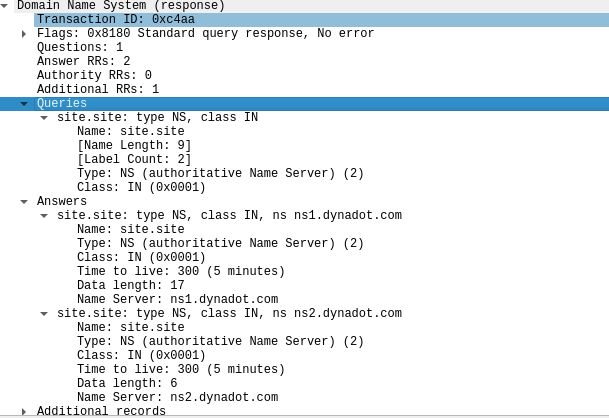
# Этап 6. Анализ утилиты nslookup



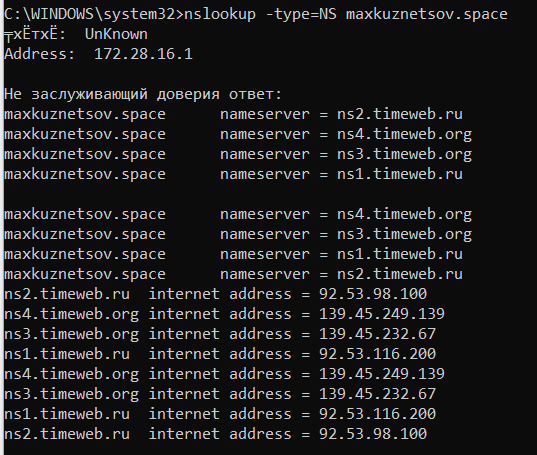








1. ***Чем различается трасса трафика в п.2 и п.4, указанных выше?*** *Различия:* 
   * *Queries: type (IPv6 Address и Host Address)*
   * *Answers: type (A и NS)*
2. ***Что содержится в поле «Answers» DNS-ответа?*** *В зависимости от типа запроса, поле может содержать:*
   * *IPv4 адрес (для типа A)*
   * *IPv6 адрес (для типа AAAA)*
   * *Доменное имя сервера (для типа NS)*
   * *MX (для почты)*
3. ***Каковы имена серверов, возвращающих авторитативный (authoritative) отклик?*** *Серверов, возвращающих авторитативный отклик, нет*



# Этап 7. Анализ FTP трафика

1. **Сколько байт данных содержится в пакете FTP-DATA?**

Размер может быть любым, но не больше MTU. В данном случае 409 байт.

Изображение выглядит как текст, Шрифт, число, снимок экрана

Автоматически созданное описание

1. **Как выбирается порт транспортного уровня, который используется для передачи FTP-пакетов?**

Для потока управления на сервере используется порт 21. Для передачи данных используется порт 20, если передача идет в активном режиме, либо с любого порта клиента к любому порту сервера в пассивном режиме.

Изображение выглядит как текст, снимок экрана, число, Шрифт

Автоматически созданное описание

1. **Чем отличаются пакеты FTP от FTP-DATA?**

FTP используется для выполнения команд (request/response), а FTP-DATA работает с файлами.

# 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.*