**Министерство науки и высшего образования Российской Федерации**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

**Факультет безопасности информационных технологий**

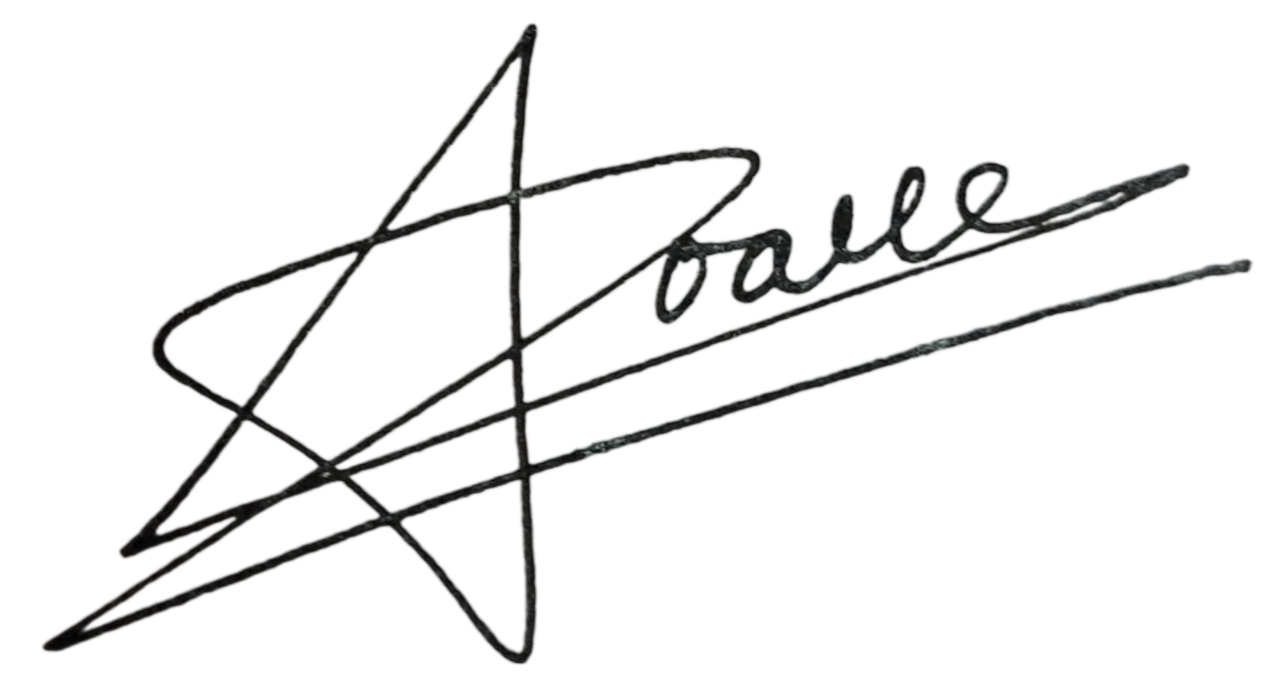
**Дисциплина:**

«Компьютерные сети»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №2**

«Анализ трафика компьютерных сетей утилитой Wireshark»

**Выполнили:**

Чу Ван Доан, студент группы N3347

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

**Проверил:**

Есипов Дмитрий Андреевич

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(отметка о выполнении)

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

# Содержание

[Введение 3](#_heading=h.gjdgxs)

[1 ХОД РАБОТЫ 4](#_heading=h.30j0zll)

[1.1 Анализ трафика утилиты ping 4](#_heading=h.7n6fsycnmhke)

[1.2 Анализ трафика утилиты tracert 7](#_heading=h.1r56rmsdgsri)

[1.3 Анализ HTTP-трафика 10](#_heading=h.df3nizyg7vph)

[1.4 Анализ DNS-трафика 12](#_heading=h.sqyt378uo5p0)

[1.5 Анализ ARP-трафика 14](#_heading=h.jiy06j3kew7s)

[1.6 Анализ трафика утилиты nslookup 16](#_heading=h.5gg0c6q6hcu)

[1.7 Анализ FTP-трафика 18](#_heading=h.9kwzlcamop43)

[1.8 Анализ DHCP-трафика 20](#_heading=h.dprc4kkws19a)

[Заключение 23](#_heading=h.tyjcwt)

## Введение

Цель работы – изучить структуру протокольных блоков данных, анализируя реальный трафик на компьютере студента с помощью бесплатно распространяемой утилиты Wireshark.

Для достижения поставленной цели необходимо решить следующие задачи:

* установить Wireshark;
* ознакомиться с теорией;
* выполнить анализ трафика;
* составить отчёт.

## ХОД РАБОТЫ

Чтобы выполнить эту лабораторную работу, я использую веб-сайт с доменом второго уровня "chu", что является моей фамилией: <https://chu292.github.io>

### 1.1 Анализ трафика утилиты ping

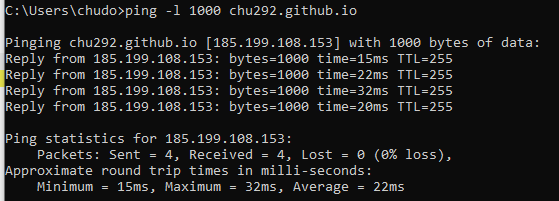


Рисунок 1 – Пример использования утилиты ping

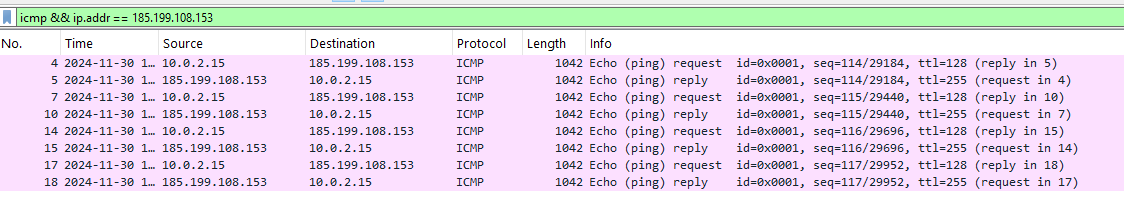


Рисунок 2 – Пример трафика утилиты ping

Ответы на вопросы:

1. Имеет ли место фрагментация исходного пакета, какое поле на это указывает?

* Нет, фрагментация отсутствует.
* Поля, которые указывают на это: "Flags" (значение 0x0) и "Fragment Offset" (значение 0).

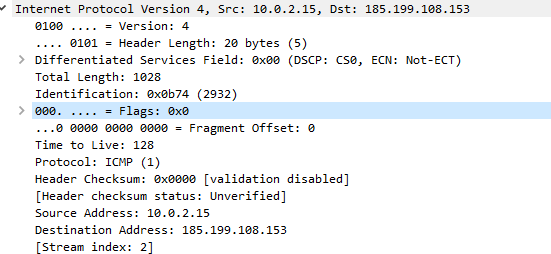


Рисунок 3 – Пакет со флагом 0x0

2. Какая информация указывает, является ли фрагмент пакета последним или промежуточным?

Установка флага MF (More fragments) в заголовке IPv4 указывает, что фрагмент пакета является промежуточным. Сброс флага MF (More fragments) в заголовке IPv4 указывает, что фрагмент пакета является послежним (рисунок 4).

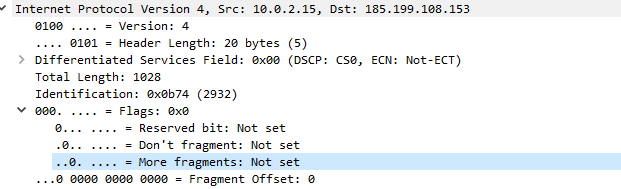


Рисунок 4 - Последний пакет

3. Чему равно количество фрагментов при передаче ping-пакетов?

Количество фрагментов при передаче ping-пакетов при разных размерах пакета показано в таблице 1.

Таблица 1. Зависимость количества фрагментов от размера пакета.

| Размер Пакета | Количество Фрагментов | Размер Пакета | Количество Фрагментов | Размер Пакета | Количество Фрагментов |
| --- | --- | --- | --- | --- | --- |
| 100 | 1 | 3600 | 3 | 7100 | 5 |
| 600 | 1 | 4100 | 3 | 7600 | 6 |
| 1100 | 1 | 4600 | 4 | 8100 | 6 |
| 1600 | 2 | 5100 | 4 | 8600 | 6 |
| 2100 | 2 | 5600 | 4 | 9100 | 7 |
| 2600 | 2 | 6100 | 5 | 9600 | 7 |
| 3100 | 3 | 6600 | 5 | 10000 | 7 |

Рисунок 5 - Количество фрагментов

4. Построить график, в котором на оси абсцисс находится размер\_пакета, а по оси ординат – количество фрагментов, на которое был разделён каждый ping-пакет.

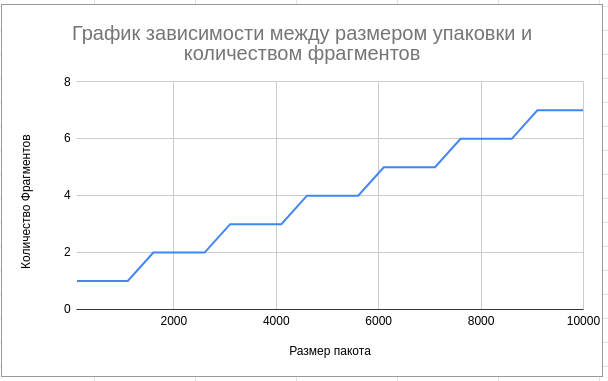


Рисунок 5 - Зависимость количества фрагментов от размера пакета

5. Как изменить поле TTL с помощью утилиты ping?

ping -i <срок жизни в миллисекундах> <адрес>

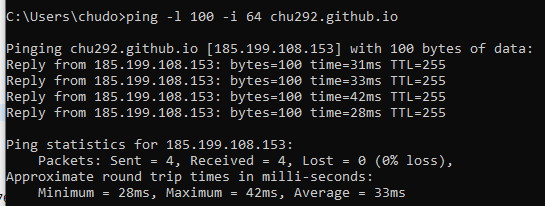


Рисунок 6 - Изменение TTL

6. Что содержится в поле данных ping-пакета?

Поле данных пакета ping содержит часть "payload", которая может быть настроена пользователем или заполнена по умолчанию операционной системой.

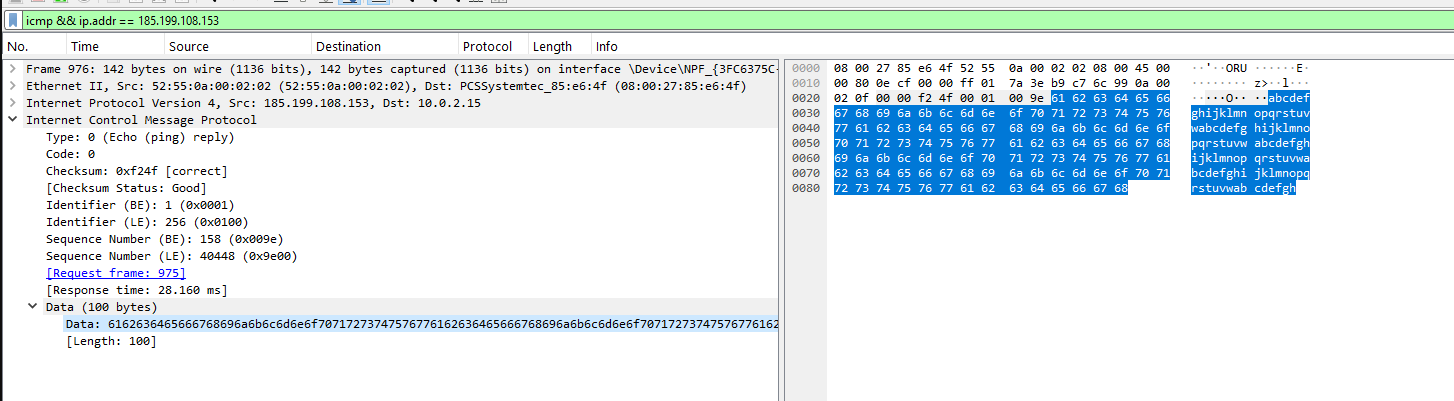


Рисунок 7 - Фрагмент данных ping-пакета

### 1.2 Анализ трафика утилиты tracert

Traceroute (tracert) — это утилита, предназначенная для определения маршрута прохождения данных в сети. Она отправляет пакеты на промежуточные узлы и отслеживает их путь обратно. Tracert постепенно увеличивает значение TTL в отправляемых пакетах, пока не достигнет целевого узла. Когда маршрутизатор получает пакет с TTL, равным 1, он возвращает его обратно, что позволяет tracert определить путь до этого маршрутизатора.

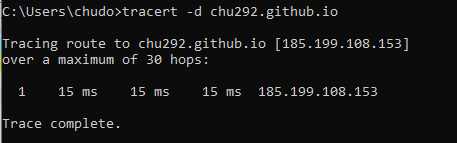
****

Рисунок 8 - Пример использования утилиты tracert

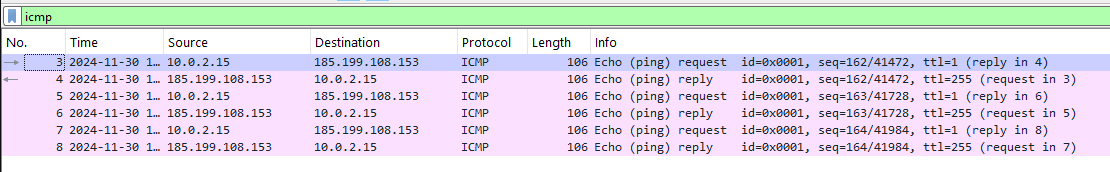


Рисунок 9 - Пример трафика утилиты tracert

Ответы на вопросы:

1. Сколько байт содержится в заголовке IP? Сколько байт содержится в поле данных?

20 байт в заголовке, 64 байта – в поле данных.



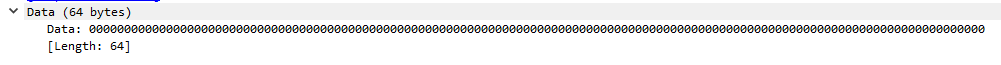


Рисунок 10 - 20 байт в заголовке, 64 байта – в поле данных

2. Как и почему изменяется поле TTL в следующих друг за другом ICMP- пакетах tracert?

Чтобы ответить на этот вопрос, необходимо отследить изменение TTL при прохождении маршрута, содержащего более двух узлов. Tracert работает, увеличивая TTL (время жизни пакета) в IPv4, начиная с 1. Каждый раз, когда пакет достигает очередного узла, значение TTL возрастает на 1, пока не достигнет цели. Когда tracert отправляет пакет с TTL, равным 1, маршрутизатор по пути уменьшает TTL на 1 и пересылает его дальше.

Если маршрутизатор получает пакет с TTL, равным нулю, он воспринимает это как ошибку и отправляет обратно сообщение ICMP (Internet Control Message Protocol) с кодом "Time-to-Live exceeded". Таким образом, tracert может отследить путь, который пакет проделал через сеть, до самого конечного узла.

3. Чем отличаются ICMP-пакеты, генерируемые утилитой tracert, от ICMP- пакетов, генерируемых утилитой ping (см. предыдущее задание).

ICMP-пакеты, генерируемые утилитой tracert, отличаются от ICMP-пакетов, генерируемых утилитой ping, использованием поля TTL. Tracert модифицирует TTL, чтобы получать ICMP Time Exceeded (тип 11) от промежуточных маршрутизаторов, тогда как ping просто отправляет ICMP Echo Request (тип 8) и ожидает Echo Reply (тип 0) от конечного узла.

4. Чем отличаются полученные пакеты «ICMP reply» от «ICMP error» и зачем нужны оба этих типа ответов?

ICMP Reply нужен для подтверждения успешной доставки пакета. ICMP Error нужен для диагностики и обработки ошибок в сети. Оба типа пакетов критически важны для управления и отладки сетевых подключений.

5. Что изменится в работе tracert, если убрать ключ “-d”? Какой дополнительный трафик при этом будет генерироваться?

Если убрать ключ -d, tracert начнет выполнять обратное разрешение DNS для IP-адресов промежуточных узлов, что замедлит выполнение команды и создаст дополнительный трафик в виде DNS-запросов.

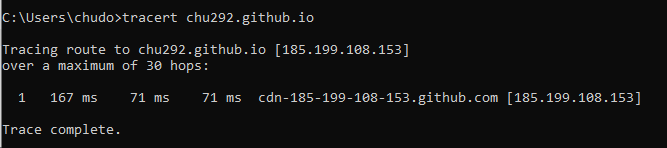


Рисунок 11 - Пример использования утилиты tracert без “-d”

### 1.3 Анализ HTTP-трафика

Отследим и проанализируем HTTP-трафик, создаваемый браузером при посещении Интернет-сайта, заданного по варианту. Список захваченных пакетов показан на рисунке 12.

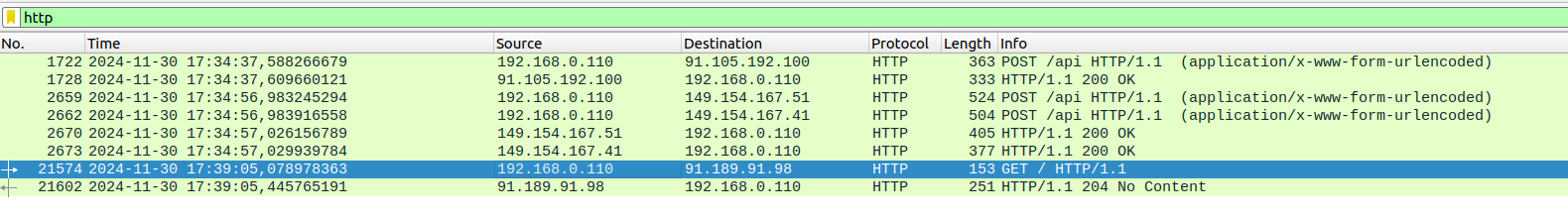


Рисунок 12 - Захваченные пакеты

HTTP (протокол передачи гипертекста) — протокол прикладного уровня передачи данных, изначально — в виде гипертекстовых документов в формате HTML, в настоящее время используется для передачи произвольных данных. GET-сообщение от клиента показано на рисунке 12. Он применяется, когда браузер запрашивает объект, идентифицирующий полем URL.

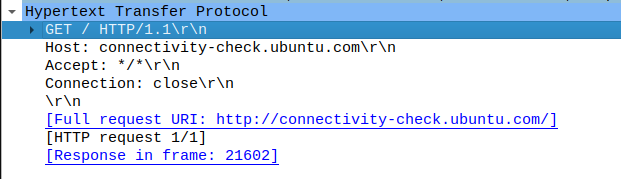


Рисунок 13 - GET-сообщение

Ответ сервера показан на рисунок 13. В ответе сервер отвечает OK (код ответа 200) и присылает нужные данные.

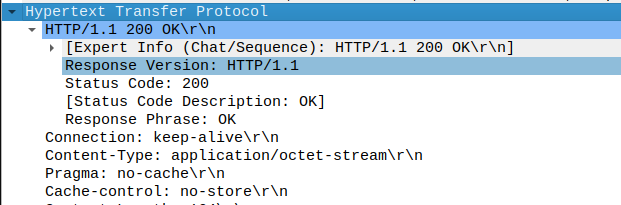


Рисунок 14 - Ответ сервера с кодом 200

HTTP-протокол имеет механизм, позволяющий прокси-серверу проверять актуальность объектов. Для этого применяется так называемый метод GET с условием. После того, что мы обновили страницу в браузере, условный GET был сгенерирован (рисунок 14).

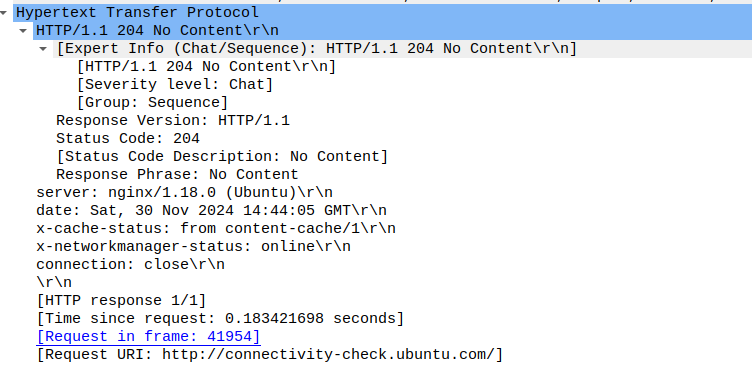


Рисунок 15 - Ответ сервера с кодом 204

Ответ с кодом 204 No Content в данном случае используется для проверки того, что сетевое подключение клиента к http://connectivity-check.ubuntu.com/ работает нормально. Сервер не отправляет никакого содержимого, так как цель запроса заключается только в подтверждении состояния подключения, а не в получении данных (рисунок 15).

### 1.4 Анализ DNS-трафика

DNS (Domain Name System) — это система, которая переводит доменные имена в IP- адреса. Когда вы вводите доменное имя в адресной строке браузера, DNS-сервер ищет соответствующий IP-адрес, а затем направляет ваш запрос на нужный сервер. Протоколы DNS обеспечивают коммуникацию между DNS-клиентами (например, браузерами) и DNS- серверами. Они определяют, как запросы отправляются между клиентами и серверами, как ответы обрабатываются и как данные хранятся и обновляются. Рисунок 16 – Фрагмент DNS-трафика

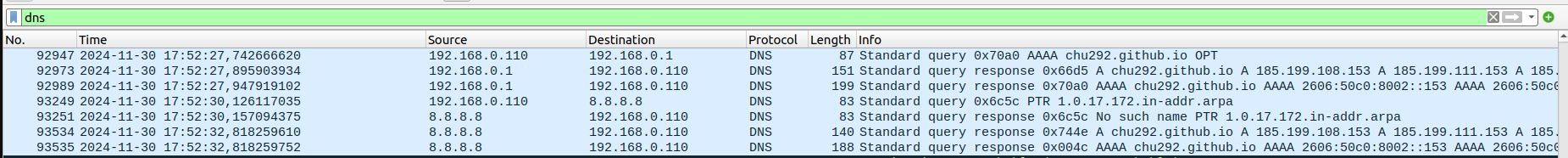


Рисунок 16 - Фрагмент DNS-трафика

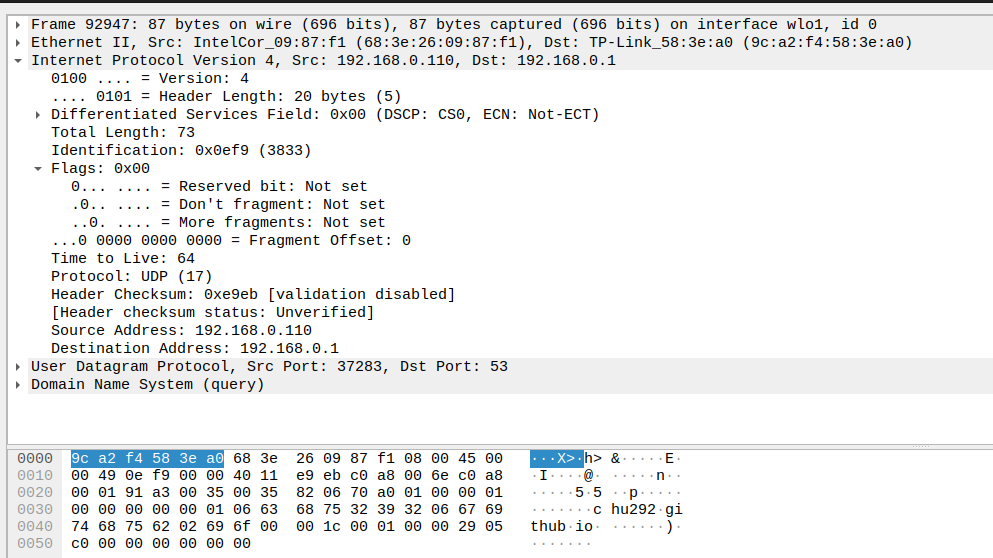


Рисунок 17 – Структура DNS

Ответы на вопросы:

1. Почему адрес, на который отправлен DNS-запрос, не совпадает с адресом посещаемого сайта?

Адрес, на который отправлен DNS-запрос, не совпадает с адресом посещаемого сайта, потому что DNS-запрос отправляется к DNS-серверу, который отвечает за преобразование доменного имени в IP-адрес. DNS-сервер — это отдельный узел в сети, и его адрес обычно задается провайдером интернет-услуг (ISP) или настроен вручную. После получения IP-адреса сайт запрашивается уже напрямую.

2. Какие бывают типы DNS-запросов?

Типы DNS-запросов:

* A (Address Record) – Преобразует доменное имя в IPv4-адрес.
* AAAA (IPv6 Address Record) – Преобразует доменное имя в IPv6-адрес.
* CNAME (Canonical Name) – Используется для указания псевдонима доменного имени.
* MX (Mail Exchange) – Определяет почтовые серверы для домена.
* NS (Name Server) – Указывает DNS-серверы для домена.
* PTR (Pointer Record) – Обратное разрешение (из IP-адреса в доменное имя).
* TXT (Text Record) – Содержит текстовую информацию, часто используется для проверки доменов.
* SOA (Start of Authority) – Информация о зоне DNS.

3. В какой ситуации нужно выполнять независимые DNS-запросы для получения содержащихся на сайте изображений?

Независимые DNS-запросы для получения изображений на сайте нужно выполнять в следующей ситуации:

Когда изображения на сайте загружаются с других доменов (например, через внешние ресурсы или CDN). В таких случаях для каждого домена, с которого загружаются изображения, выполняется отдельный DNS-запрос, чтобы преобразовать доменное имя в IP-адрес.

Пример:

Сайт может находиться на example.com, но изображения могут загружаться с cdn.example.com или другого внешнего сервера. В таком случае нужно сначала выполнить DNS-запрос для домена cdn.example.com, чтобы получить его IP-адрес и загрузить изображения.

### 1.5 Анализ ARP-трафика

ARP (Address Resolution Protocol) – протокол, который используется для определения MAC-адреса устройства по его IP-адресу в локальной сети. Он работает, отправляя широковещательные запросы на все устройства в сети, которые содержат IP- адрес устройства, ищущего MAC-адрес. Устройства, имеющие указанный IP-адрес, отвечают со своим MAC-адресом, и таким образом ARP определяет соответствие между IP- и MAC-адресами.

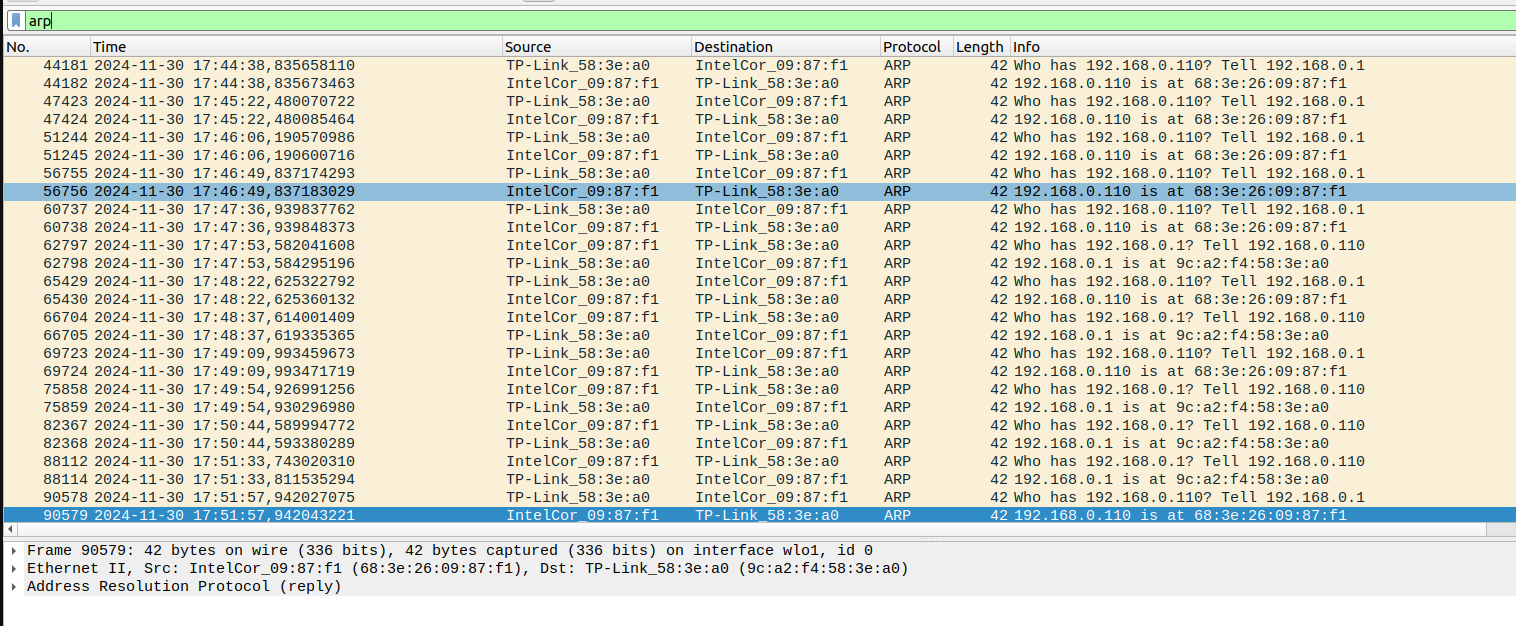
****

Рисунок 17 – Фрагмент ARP-трафика

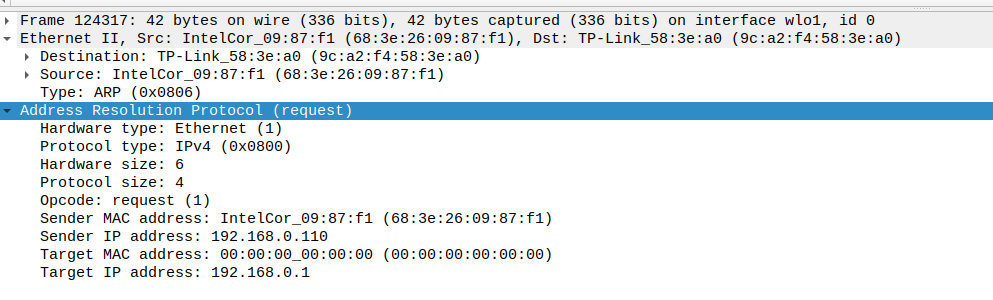


Рисунок 18 – Пример ARP-запроса

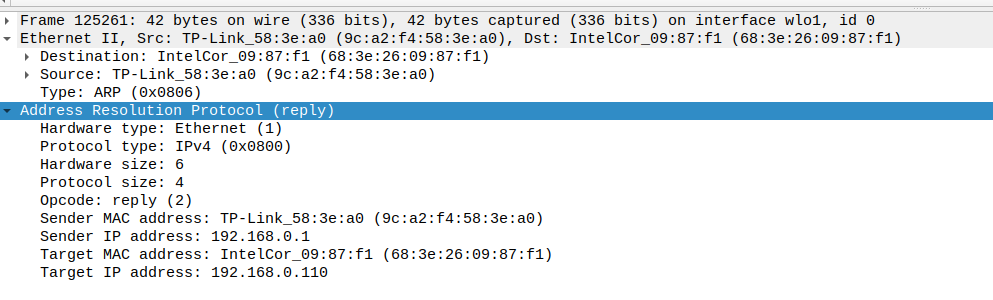


Рисунок 19 – Пример ARP-ответа

Ответы на вопросы:

1. Какие МАС-адреса присутствуют в захваченных пакетах ARP-протокола? Что означают эти адреса? Какие устройства они идентифицируют? В ARP-протоколе обычно встречаются два типа МАС-адресов: МАС-адрес отправителя (Source MAC Address) и МАС-адрес получателя (Destination MAC Address).

МАС-адрес отправителя (Source MAC Address):

* Что означает: MAC-адрес устройства, которое отправляет ARP-запрос или ARP-ответ.
* Что идентифицирует: Идентифицирует устройство, инициировавшее запрос или отправившее ответ.

МАС-адрес получателя (Destination MAC Address):

* Что означает: В ARP-запросе это широковещательный адрес FF:FF:FF:FF:FF:FF. В ARP-ответе это MAC-адрес устройства, которое ответило на запрос.
* Что идентифицирует: В запросе — все устройства в сети, в ответе — конкретное устройство, отвечающее на запрос.

2. Какие МАС-адреса присутствуют в захваченных HTTP-пакетах и что означают эти адреса? Какие устройства они идентифицируют? В захваченных HTTP-пакетах также содержатся МАС-адреса отправителя и получателя.

МАС-адрес отправителя (Source MAC Address):

* Что означает: MAC-адрес устройства, которое отправляет HTTP-запрос или ответ.
* Что идентифицирует: Идентифицирует устройство, которое отправляет пакет, например, клиент (компьютер или телефон), который отправляет запрос на сервер.

МАС-адрес получателя (Destination MAC Address):

* Что означает: MAC-адрес устройства, которому адресован HTTP-пакет.
* Что идентифицирует: Идентифицирует устройство, принимающее пакет, например, маршрутизатор или сервер, принимающий запрос.

3. Для чего ARP-запрос содержит IP-адрес источника?

ARP-запрос содержит IP-адрес источника для того, чтобы устройство, получающее запрос, знало, от какого IP-адреса пришел запрос и могло отправить ARP-ответ обратно на правильный IP-адрес.

### 1.6 Анализ трафика утилиты nslookup

nslookup — утилита, предоставляющая пользователю интерфейс командной строки

для обращения к системе DNS (проще говоря, DNS-клиент).

Отследим и проанализируем трафик протокола DNS, сгенерированный в результате

выполнения следующих действий:

− настроить Wireshark-фильтр: “ip.addr == 10.0.2.3”.

− запустить команду “nslookup chu292.github.io” (рис.20);

− дождаться отправки трёх DNS-запросов и трёх DNS-ответов;

− повторить предыдущие два шага, используя команду: “nslookup -type=NS имя\_сайта\_по\_варианту”.

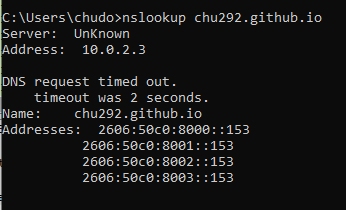


Рисунок 20 – Выполнение команды nslookup без опции -type=NS

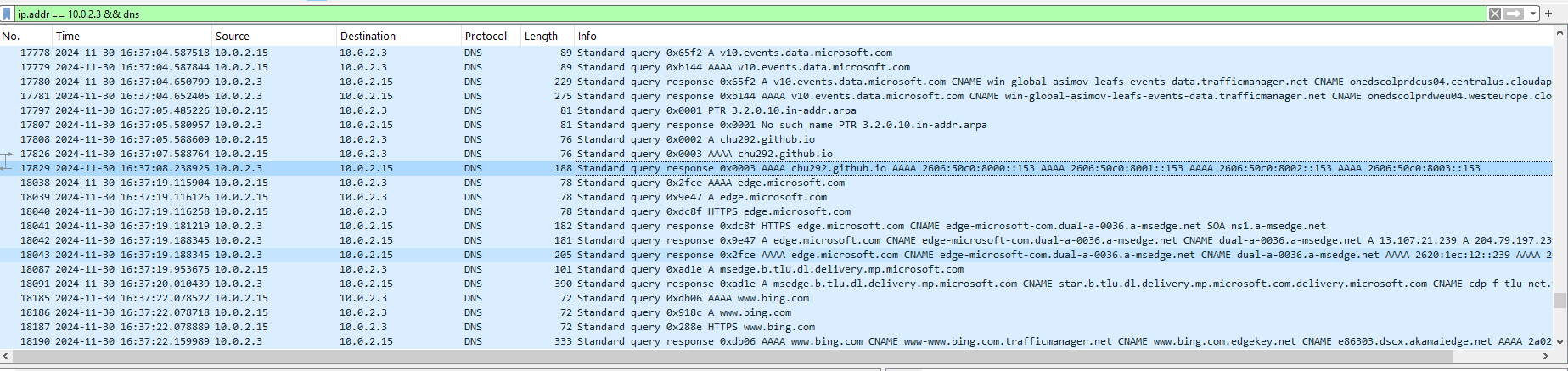


Рисунок 21 - Результат анализа трафика утилиты nslookup без опции -type=NS

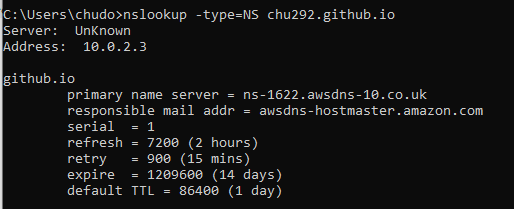


Рисунок 22 - Выполнение команды nslookup с опцией -type=NS

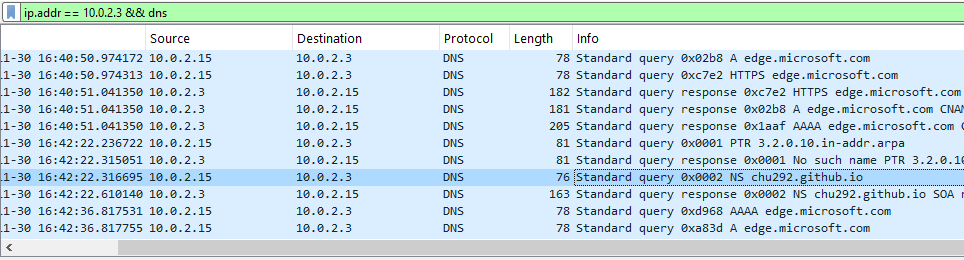
****

Рисунок 24 - Результат анализа трафика утилиты nslookup с опцией -type=NS

Ответы на вопросы

1. Чем различается трасса трафика в п.2 и п.4?

В пунктах 2 и 4 трасса трафика различается по следующему:

В пункте 2, при использовании обычного запроса DNS, происходит разрешение доменного имени в IP-адрес.

В пункте 4, при использовании -type=NS, запрос выполняется для поиска серверов имен (NS-записи), и результатом является IP-адреса DNS-серверов, которые управляют доменом.

Таким образом, в пункте 2 трафик направлен к основному серверу, который предоставляет IP-адрес, а в пункте 4 — к DNS-серверам для получения информации о зоне домена.

2. Что содержится в поле «Answers» DNS-ответа?

В поле «Answers» DNS-ответа содержатся записи, соответствующие запросу. Это могут быть:

* A (IP-адрес для доменного имени),
* AAAA (IPv6-адрес),
* MX (почтовые серверы),
* NS (серверы имен) и другие типы записей, в зависимости от типа запроса.

3. Каковы имена серверов, возвращающих авторитативный (authoritative)

отклик?

Имена серверов, возвращающих авторитативный отклик, указаны в NS-записях DNS-ответа. Эти серверы являются авторитативными DNS-серверами для домена и отвечают на запросы с точной информацией о домене.

### 1.7 Анализ FTP-трафика

Отследим и проанализируем трафик протокола FTP, сгенерированный в результате

выполнения следующих действий:

− настроить Wireshark-фильтр «ftp || ftp-data»;

− скачать в браузере небольшой файл с соответствующего варианту FTP сервера в Интернете.

Подключение к FTP-серверу

* + ftp ftp.dlptest.com
  + Name: dlpuser
  + Password: rNrKYTX9g7z3RgJRmxWuGHbeu

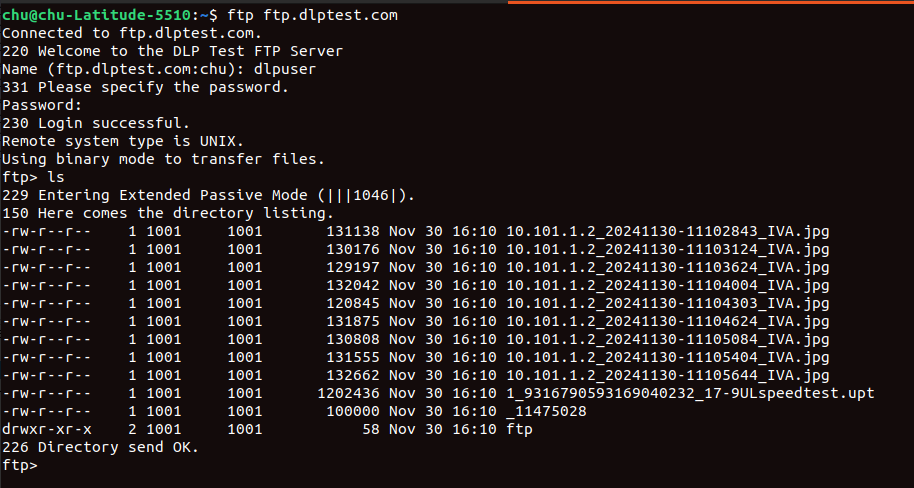


Рисунок 25 - Подключение к FTP-серверу

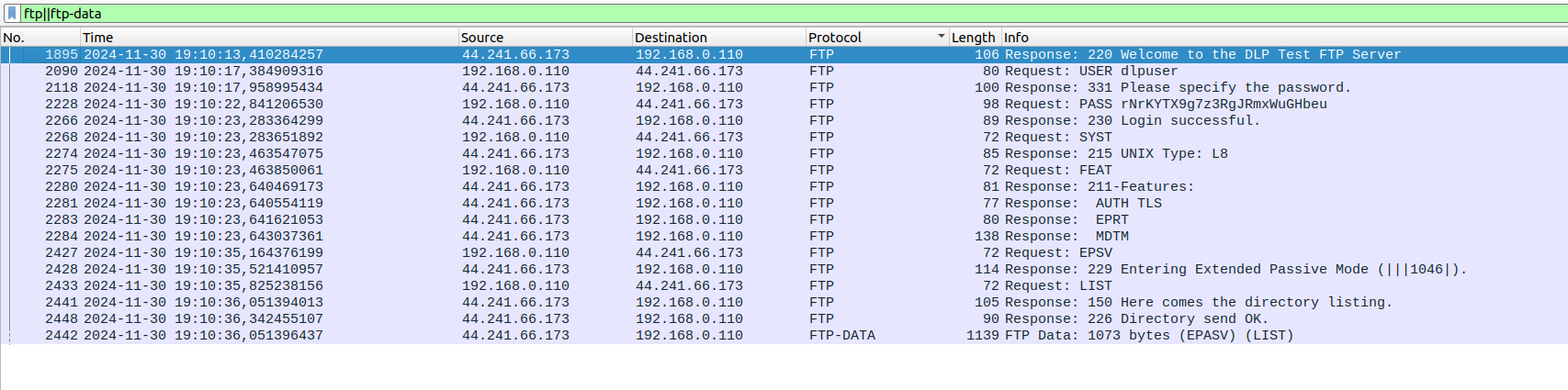


Рисунок 26 - Анализ трассы FTP

Ответы на вопросы:

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

В пакете FTP-DATA содержится 1073 байт.

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

Порт транспортного уровня, который используется для передачи FTP-пакетов является 21.

3. Чем отличаются пакеты FTP от FTP-DATA?

Пакеты FTP используются для передачи управляющей информации (например, команды, ответы сервера), в то время как пакеты FTP-DATA предназначены для передачи файловых данных. Главные различия:

* FTP: управляет сессией, передает команды и ответы.
* FTP-DATA: передает сам файл или его части в рамках сессии FTP.

FTP использует управляющий канал (обычно порт 21), а FTP-DATA — канал данных (порт 20 для активного режима или случайный порт в пассивном режиме).

### 1.8 Анализ DHCP-трафика

DHCP (протокол динамической настройки узла) — прикладной протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент- сервер».

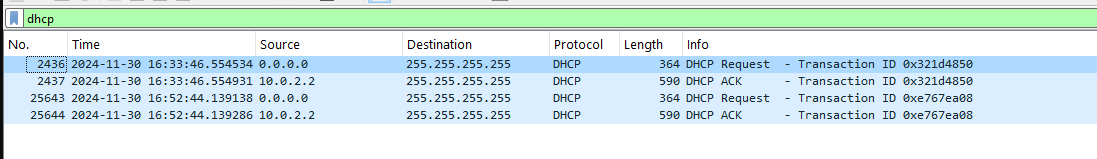


Рисунок 27 - Анализ DHCP трассы

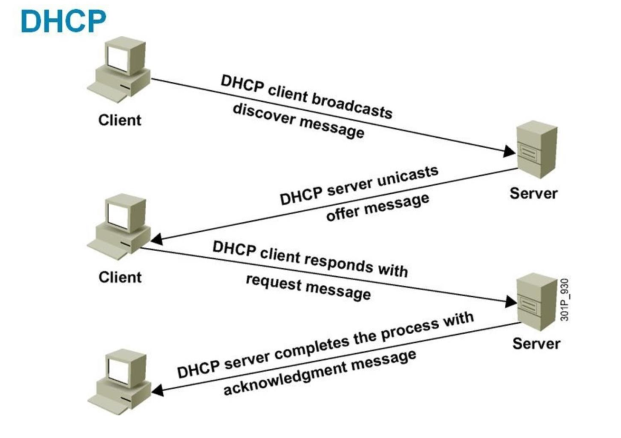


Рисунок 28 - Работа протокола DHCP

Ответы на вопросы

1. Чем различаются пакеты «DHCP Discover» и «DHCP Request»?

Пакеты DHCP Discover и DHCP Request имеют следующие различия:

DHCP Discover:

* Используется клиентом для поиска DHCP-сервера.
* Отправляется с широковещательным адресом (255.255.255.255).
* Содержит запрос на получение IP-адреса и другую информацию.

DHCP Request:

* Отправляется клиентом после того, как он получил предложение от DHCP-сервера.
* Содержит запрос на подтверждение выбранного IP-адреса.
* Может быть использован для продления аренды IP-адреса, если клиент уже имеет активную аренду.

1. Как и почему менялись MAC- и IP-адреса источника и назначения в переданных DHCP-пакетах?

MAC-адреса:

* В DHCP Discover и DHCP Request исходный MAC-адрес принадлежит клиенту, а MAC-адрес назначения — это широковещательный адрес (255.255.255.255), поскольку клиент еще не знает адреса сервера.
* В ответах сервера, например в DHCP Offer и DHCP Ack, исходный MAC-адрес будет указывать на сервер DHCP, а MAC-адрес назначения — это MAC-адрес клиента.
* MAC-адреса меняются, потому что на этапе обнаружения сервер и клиент взаимодействуют по каналу Ethernet, и адреса используются для точной передачи пакетов между ними.

IP-адреса:

* В DHCP Discover IP-адрес источника клиента обычно равен 0.0.0.0, потому что клиент еще не имеет IP-адреса и пытается получить его через DHCP.
* В DHCP Offer и DHCP Ack сервер присваивает клиенту IP-адрес, который он предлагает или подтверждает.
* Адреса источника и назначения изменяются, потому что сервер на момент отправки DHCP Offer или DHCP Ack знает, какой IP-адрес можно присвоить клиенту.

1. Каков IP-адрес DHCP-сервера?

До назначения IP-адреса клиенту:

В пакете DHCP Discover IP-адрес источника будет 0.0.0.0, так как клиент еще не имеет IP-адреса. IP-адрес назначения будет 255.255.255.255, это широковещательный адрес, на который отправляется запрос.

Ответ сервера:

Когда сервер DHCP отправляет DHCP Offer или DHCP Ack, его IP-адрес будет отображен в поле siaddr (серверный IP-адрес) в пакете. Это IP-адрес самого DHCP-сервера, который клиент может использовать для получения конфигурации.

siaddr: Это поле в пакете DHCP может содержать IP-адрес сервера, который клиенту необходимо использовать для получения конфигурации или для дальнейшей работы. Этот адрес может быть статический (например, заданный в настройках сети) или выделенный сервером в зависимости от конфигурации сети.

1. Что произойдёт, если очистить использованный фильтр “bootp”?

* Wireshark перестанет фильтровать пакеты DHCP: Будут отображаться все пакеты, а не только те, которые связаны с DHCP (BootP).
* Пакеты других протоколов будут видны: Например, пакеты ARP, TCP, UDP и другие, которые были до этого скрыты фильтром "bootp".

## Заключение

Выполнены задачи:

− выполнены наблюдения за передаваемым трафиком с компьютера

пользователя в Интернет и в обратном направлении;

− анализированы последовательности команд и назначение служебных данных,

используемых для организации обмена данными в следующих протоколах: ARP, DNS, FTP, HTTP, DHCP.

После выполнения работы узнала, как читать захваченный пакет, как использовать

фильтр для того, чтобы получить только пакеты, которые нам нужны, а также понятнее природу протоколов.