**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:**

Ахраров Али, студент группы N3250



(подпись)

**Проверил:**

Есипов Д.А.

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

(отметка о выполнении)

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

(подпись)

Содержание

[Введение 4](#_Toc182059805)

[1 АНАЛИЗ ТРАФИКА УТИЛИТЫ PING 5](#_Toc182059806)

[2 АНАЛИЗ ТРАФИКА УТИЛИТЫ TRACERT (TRACEROUTE) 10](#_Toc182059807)

[3 АНАЛИЗ HTTP-ТРАФИКА 13](#_Toc182059808)

[4 АНАЛИЗ DNS-ТРАФИКА 15](#_Toc182059809)

[5 АНАЛИЗ ARP-ТРАФИКА 18](#_Toc182059810)

[6 АНАЛИЗ ТРАФИКА УТИЛИТЫ NSLOOKUP 20](#_Toc182059811)

[7 АНАЛИЗ FTP-ТРАФИКА 22](#_Toc182059812)

[8 АНАЛИЗ DHCP-ТРАФИКА 24](#_Toc182059813)

[Заключение 27](#_Toc182059814)

Введение

Цель работы - исследование структуры протокольных блоков данных путем анализа реального сетевого трафика на компьютере студента с использованием свободно распространяемой утилиты Wireshark.

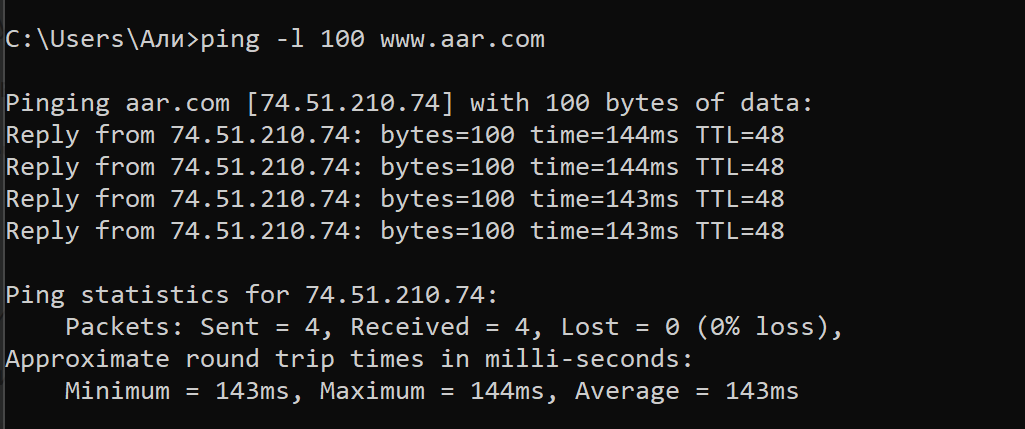
Для достижения этой цели необходимо выполнить следующие задачи:

* Установить программное обеспечение Wireshark;
* Проанализировать последовательности команд и назначение служебных данных;
* Освоить работу с фильтрами в Wireshark;
* Захватить и сохранить достаточное количество дампов пакетов;
* Ответить на поставленные вопросы.

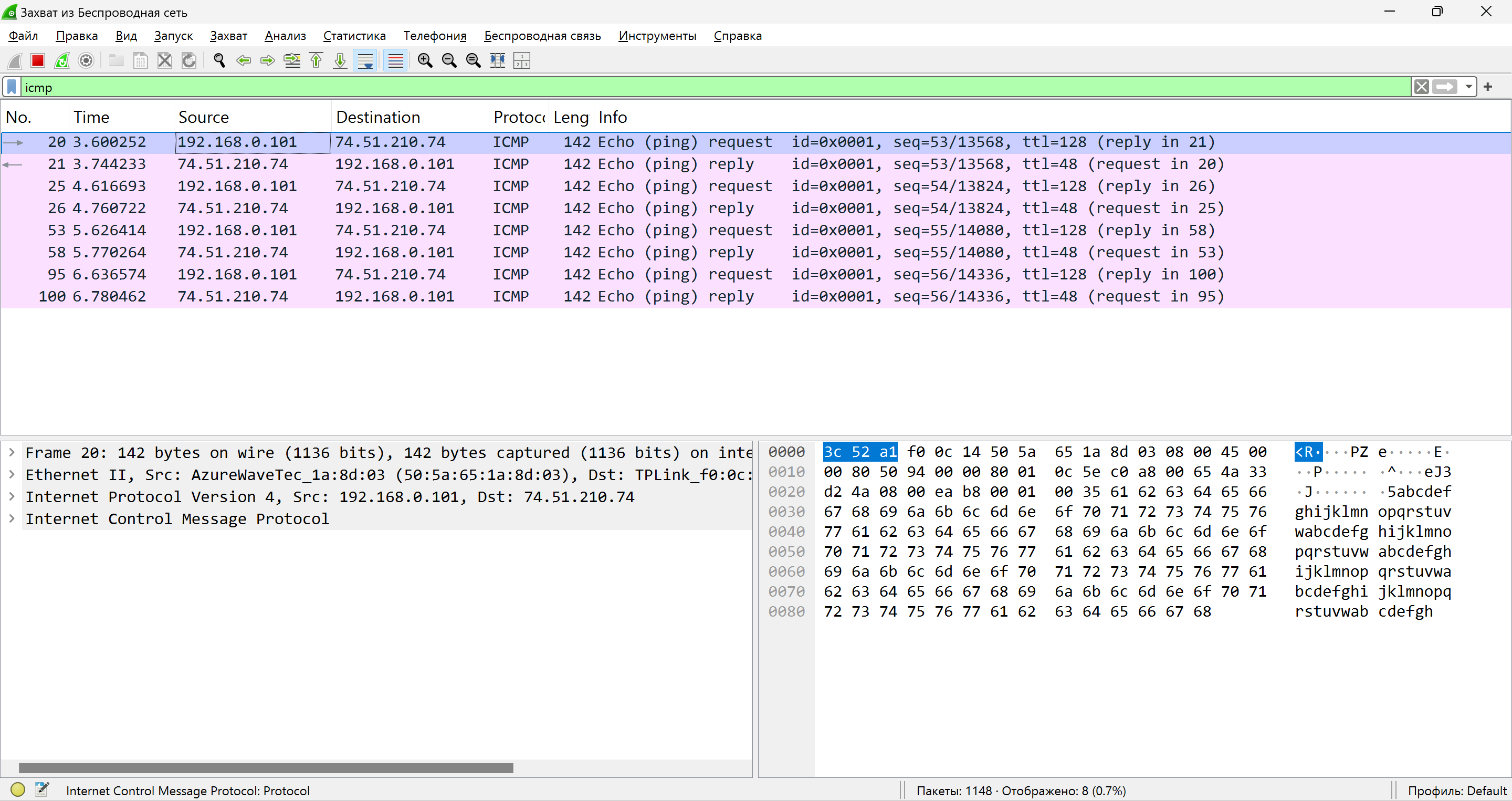
# АНАЛИЗ ТРАФИКА УТИЛИТЫ PING

Ping (Packet Internet Groper) — это утилита для измерения задержки и проверки доступности узлов в сети. Она работает, отправляя ICMP Echo Request сообщения на целевой узел и ожидая получения ICMP Echo Reply сообщений. Ping вычисляет задержку на основе времени отправки и получения ICMP сообщений.

Используемый сайт: <https://www.aar.com/>.



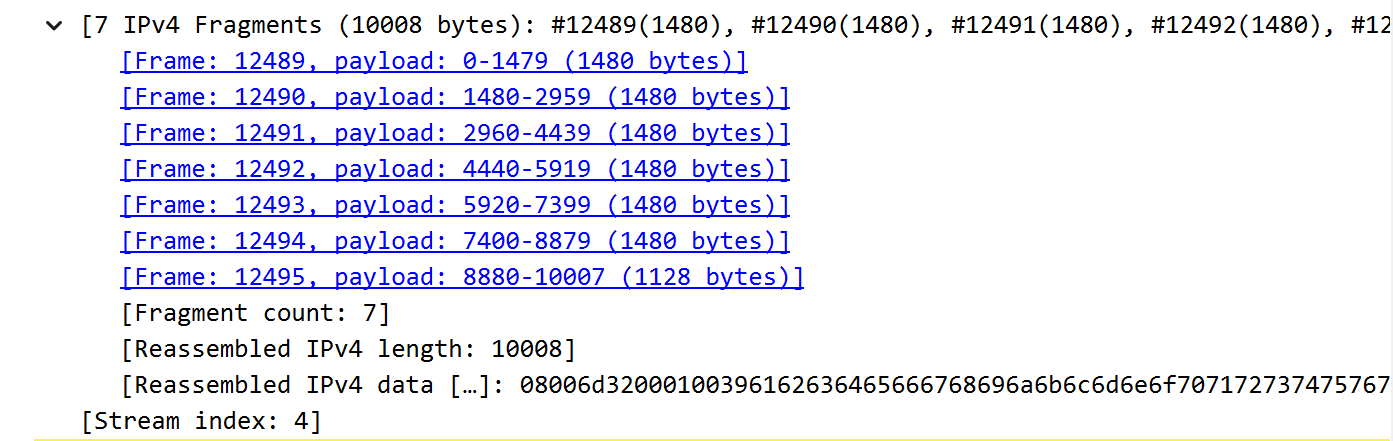
*Рисунок 1* – Пример использования утилиты ping



*Рисунок 2* – Пример трафика утилиты ping

**Ответы на вопросы:**

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



Фрагментация исходного пакета имеет место, что видно по разделу IPv4 Fragments. В новейшей версии Wireshark фрагментированные пакеты отображаются как единый пакет.

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

Установленный more fragments flag показывает, что пакет является промежуточным.

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

Количество фрагментов зависит от размера пакета и MTU сети (обычно 1500 байт

для Ethernet). Количество фрагментов можно вычислить как:

В нашем случае MTU равно 1480 байт.

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

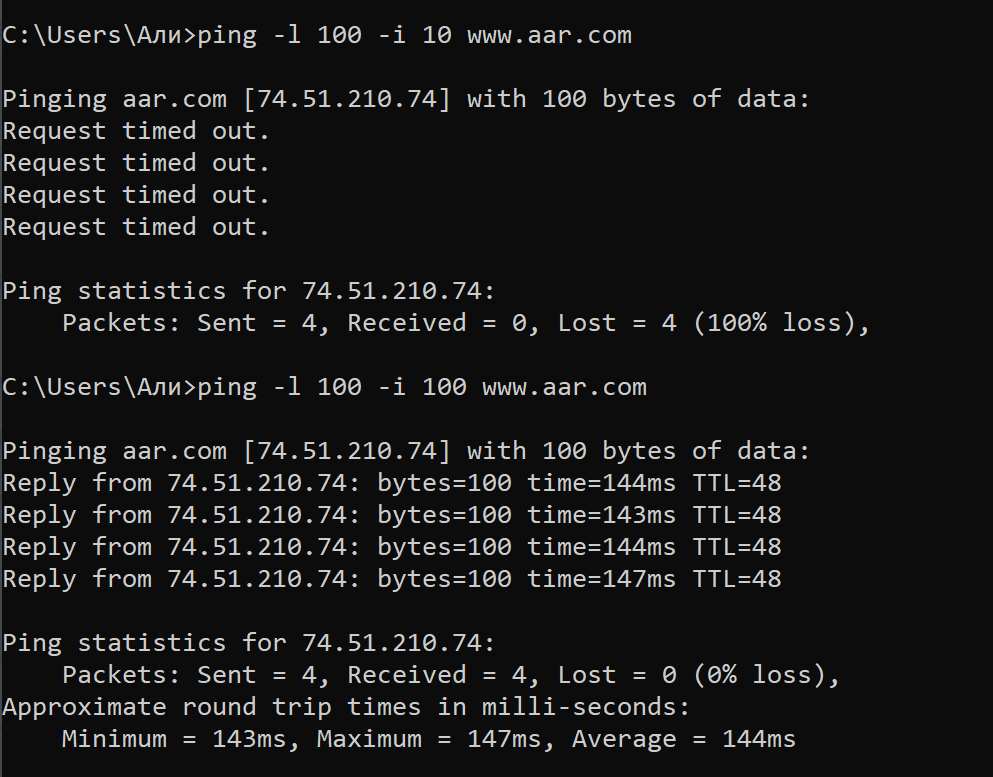
**

*Рисунок 4* – График фрагментации

1. *Как изменить поле TTL с помощью утилиты ping?*

Листинг 1 – Изменение команды ping

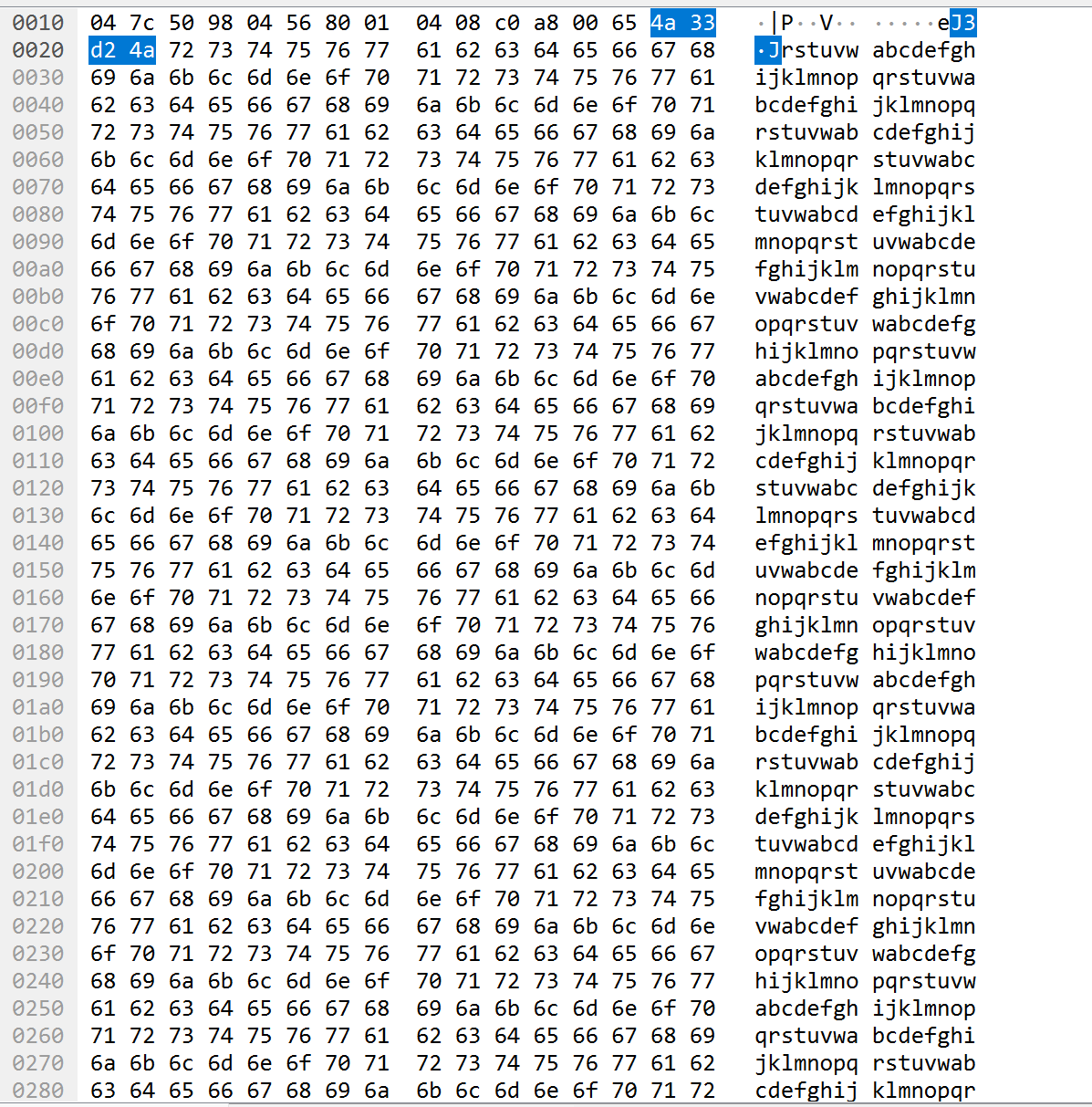
ping -i <срок жизни в миллисекундах> <адрес>



*Рисунок 5* – Изменение TTL

1. *Что содержится в поле данных ping-пакета?*

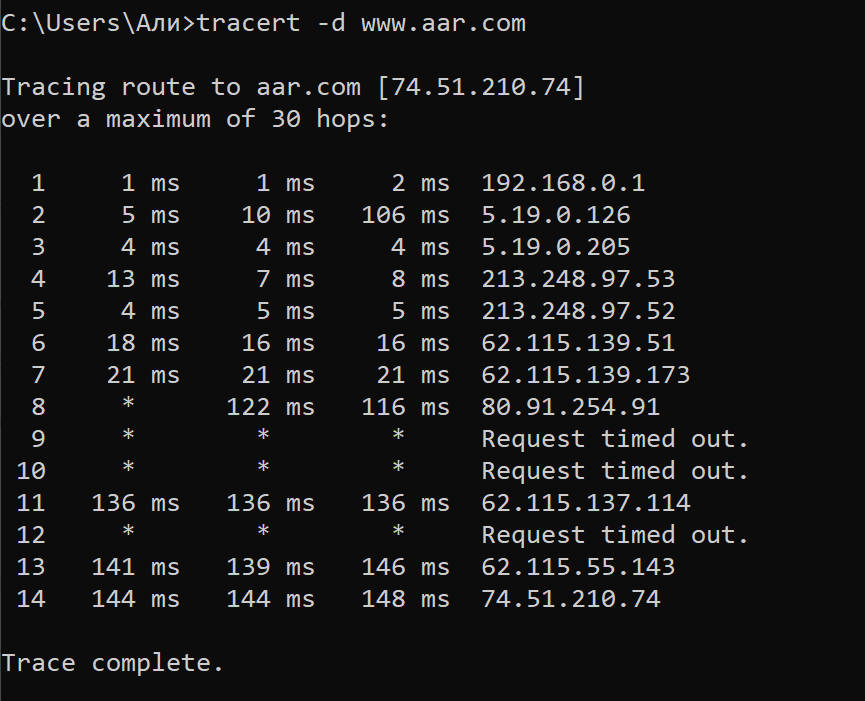
Поле данных ping обычно включает тестовую информацию — это может быть строка, состоящая из цифр, либо пустое поле, которое заполняется случайными байтами для измерения задержек в сети.

**

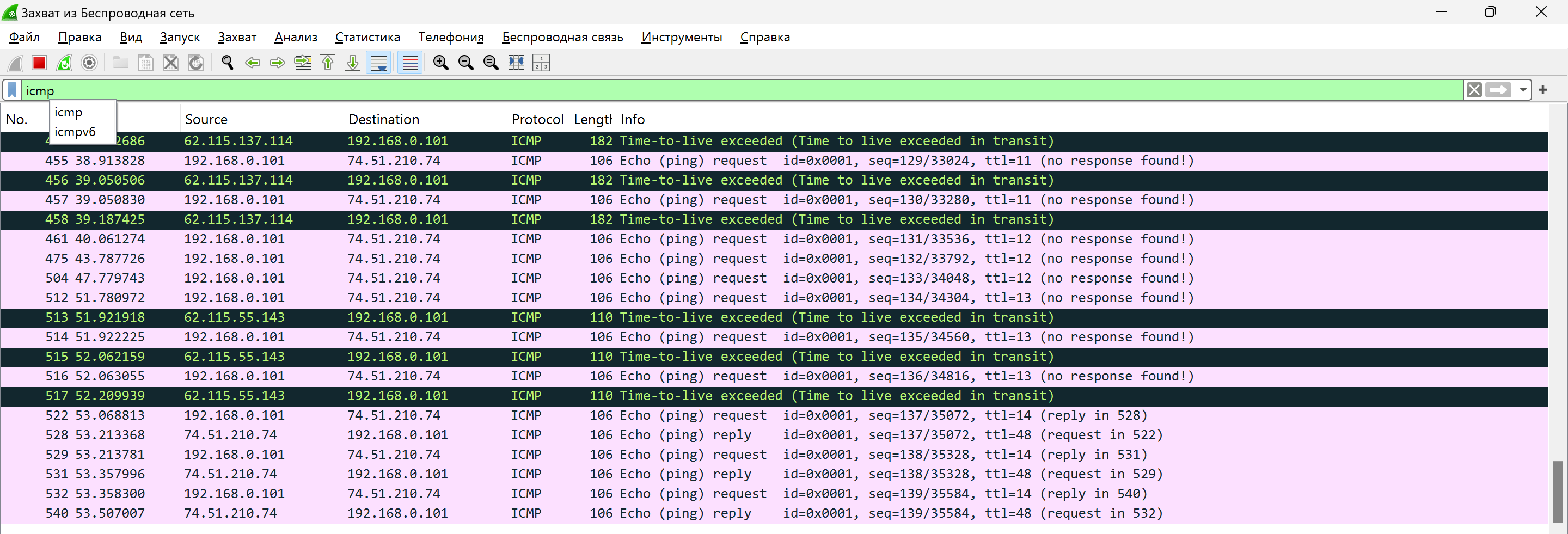
*Рисунок 6 –* Фрагмент данных ping-пакета

# АНАЛИЗ ТРАФИКА УТИЛИТЫ TRACERT (TRACEROUTE)

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 7* – Пример использования утилиты tracert

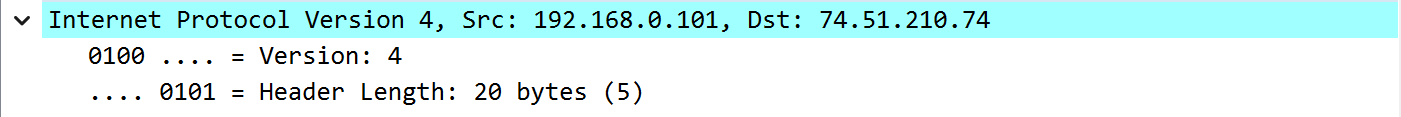
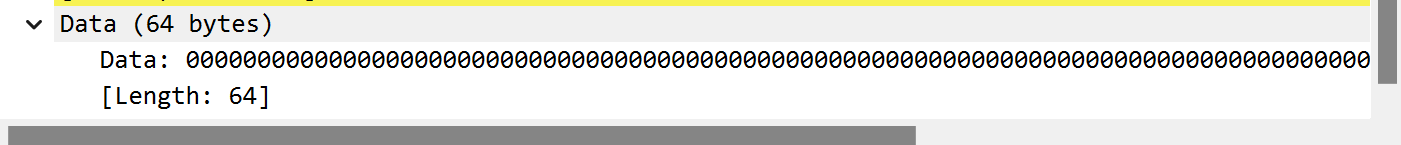


*Рисунок 8* - Пример трафика утилиты tracert

**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.

1. *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.

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

Tracert использует протокол ICMP для определения маршрута к целевому узлу. Для этого он постепенно увеличивает значение TTL в отправляемых пакетах. Когда пакет с превышенным TTL достигает маршрутизатора, тот отправляет ответное сообщение с кодом "TTL expired", что позволяет tracert определить пройденный путь. Ping же используется для измерения времени отклика целевого узла. Он отправляет ICMP echo-request и ждет ICMP echo-reply, вычисляя время прохождения сигнала и задержку на основе времени отправки и получения. Содержимое поля данных утилиты tracert обычно состоит из нулей, тогда как утилита ping использует алфавит.

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

Пакеты «ICMP error» отправляются, когда маршрутизатор обнаруживает, что время

жизни пакета (TTL) истекло

«ICMP reply» используется для проверки доступности удаленного узла. Если пакеты

«ICMP reply» получены, то узел считается доступным.

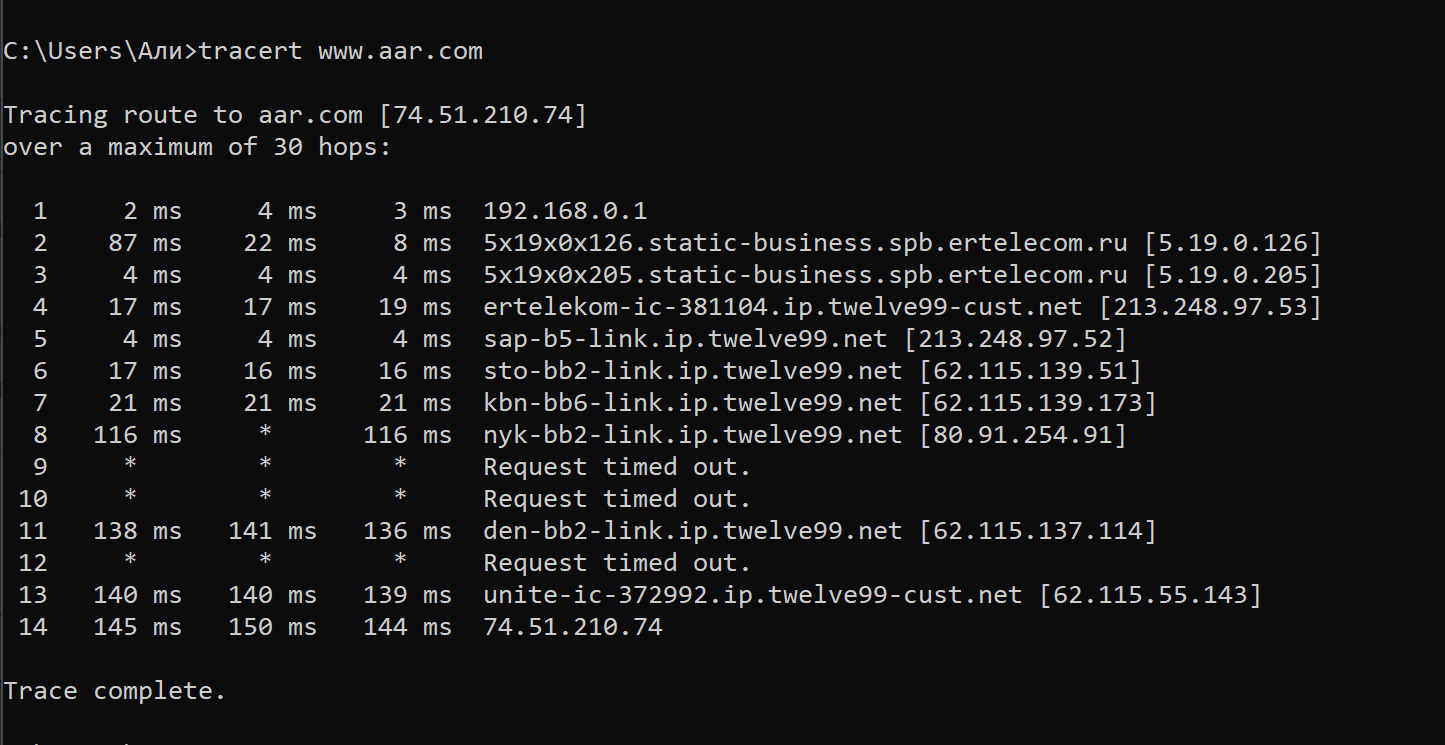
1. *Что изменится в работе tracert, если убрать ключ “-d”? Какой дополнительный*

*трафик при этом будет генерироваться?*

Ключ “-d” предотвращает попытки команды tracert разрешения IP-адресов

промежуточных маршрутизаторов в имена. Увеличивает скорость вывода результатов

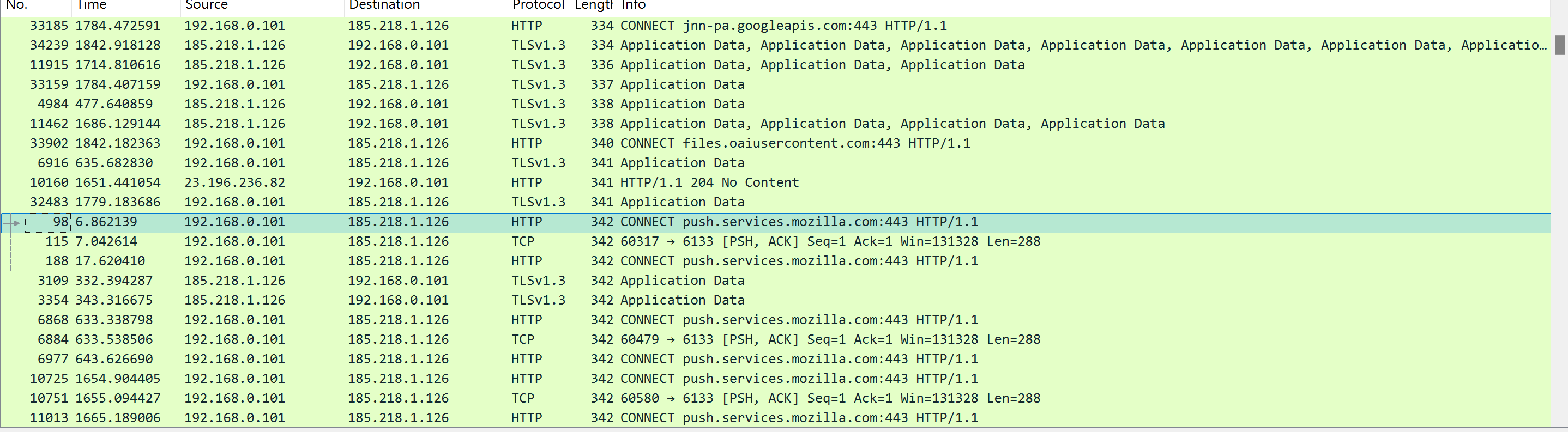
команды tracert.



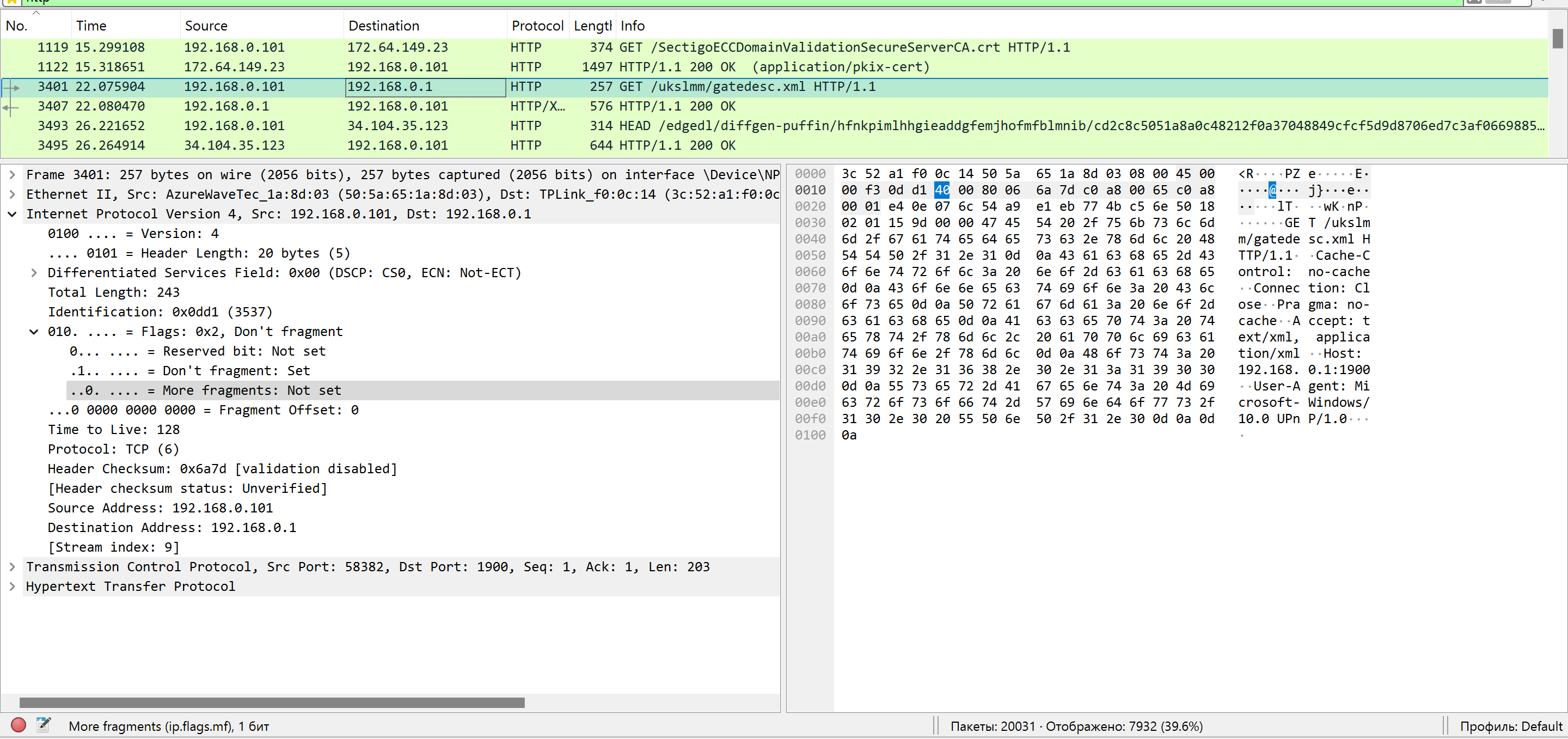
*Рисунок 11* – Пример использования утилиты tracert без “-d”

# АНАЛИЗ HTTP-ТРАФИКА

HTTP (Hypertext Transfer Protocol) — это протокол, используемый для передачи данных между веб-серверами и браузерами. Он работает на верхнем уровне модели OSI и используется для передачи HTML, CSS, JavaScript и других веб-ресурсов. HTTP поддерживает такие функции, как GET и POST запросы, cookies, сессии и т.д.



*Рисунок 12* – Фрагмент HTTP-трафика



*Рисунок 13* – Пример GET-запроса

**Первичный GET-запрос:**

− при первом посещении сайта браузер отправляет обычный GET-запрос

на сервер, и сервер возвращает полный HTTP-ответ, включая тело сообщения, которое

содержит все данные страницы (HTML, CSS, изображения и т.д.);

− заголовки запроса включают информацию о браузере, версии протокола

HTTP, целевом ресурсе, языке и других настройках;

− в ответе сервера обычно содержится код состояния 200 OK, а также тело

сообщения, содержащее данные страницы.

**Условный GET-запрос (Conditional GET):**

− при повторной загрузке страницы, браузер отправляет условный GET-запрос,

используя заголовки If-Modified-Since или If-None-Match для проверки, изменялся

ли ресурс с момента последнего запроса;

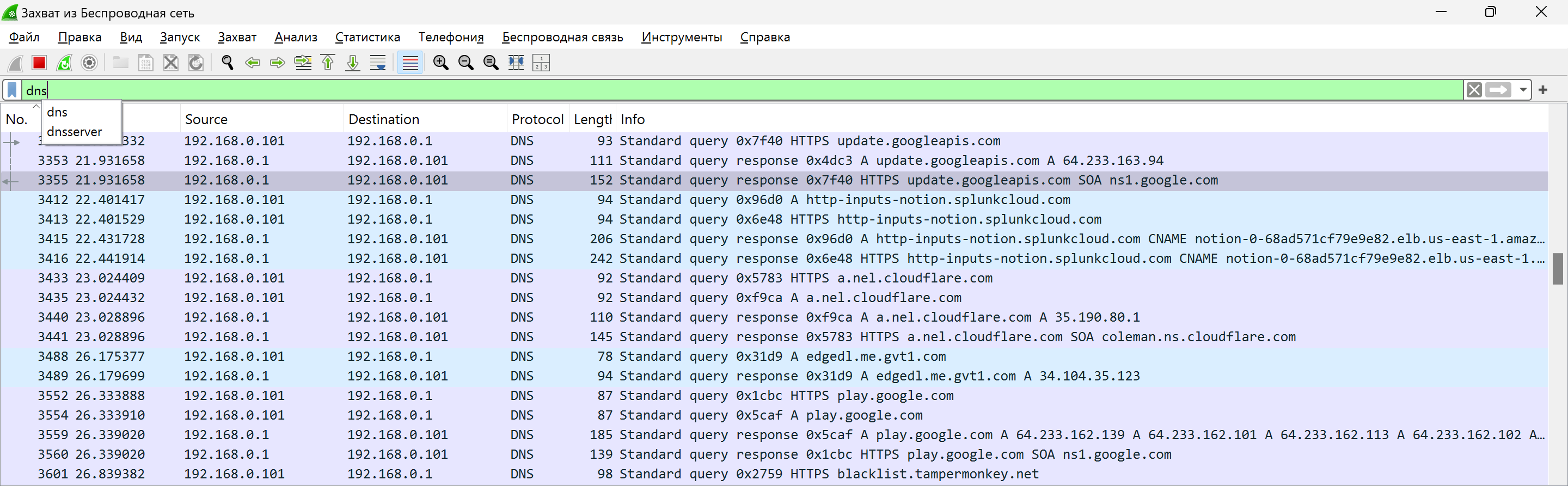
− если ресурс не изменялся (содержимое страницы осталось прежним), сервер

отвечает с кодом 304 Not Modified и не отправляет тело сообщения, что экономит трафик;

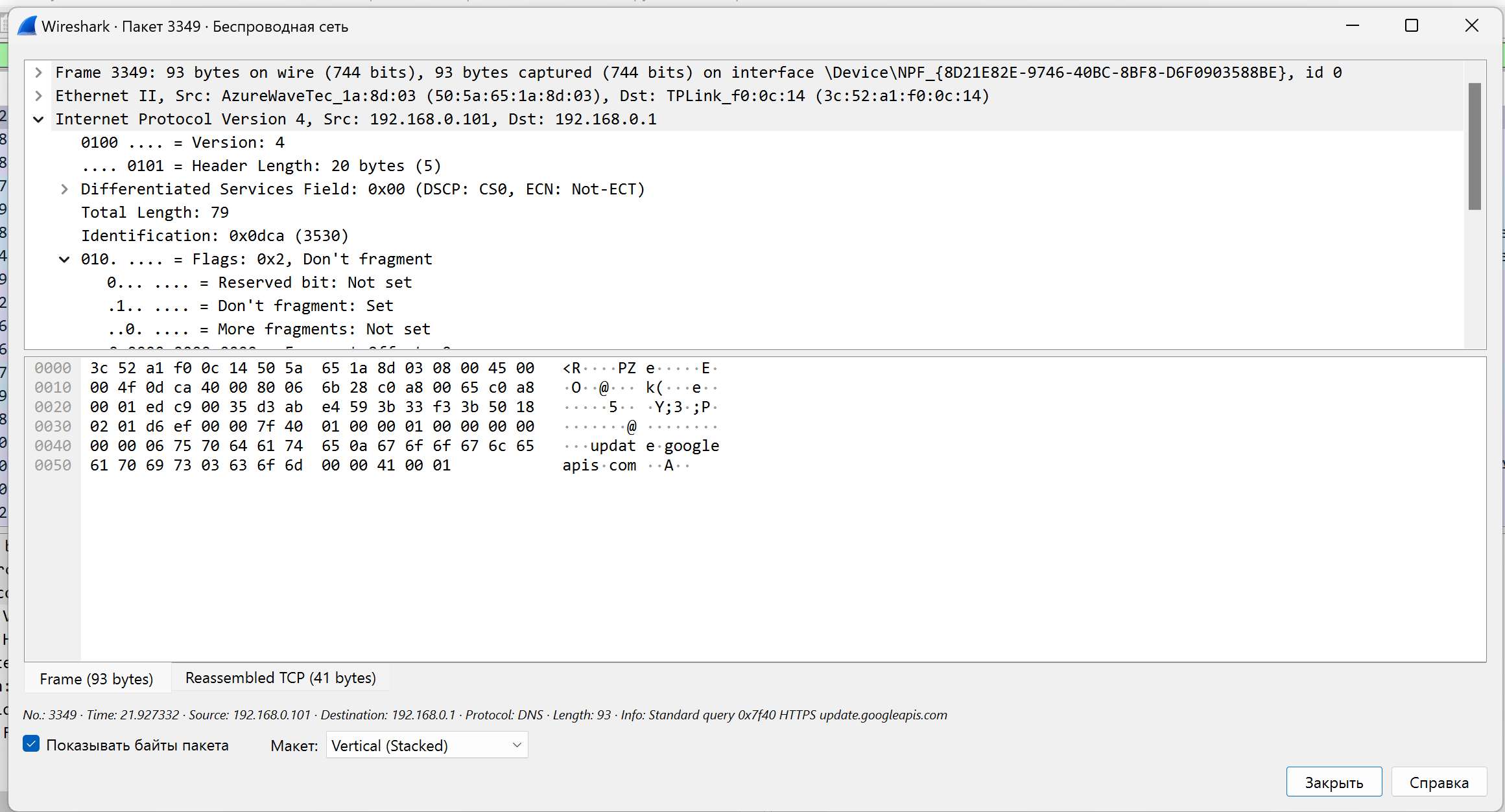
− если ресурс изменился, сервер вернет обновленную версию страницы

с полным телом сообщения и кодом состояния 200 OK.

# 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 14 – Фрагмент DNS-трафика 

*Рисунок 14* – Фрагмент DNS-трафика

****

*Рисунок 15* – Структура DNS

**Ответы на вопросы:**

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

DNS-запрос отправляется не на адрес сайта, который вы пытаетесь посетить а на DNS-сервер, который отвечает за преобразование доменного имени (например, example.com) в IP-адрес. Ваш компьютер не знает IP-адреса сайта до получения ответа от DNS-сервера, поэтому изначально отправляет запрос на IP-адрес DNS-сервера (например, на сервер вашего интернет-провайдера или общедоступные DNS-сервера, такие как Google DNS с адресом 8.8.8.8).

1. *Какие бывают типы DNS-запросов?*

Основные типы DNS-запросов включают:

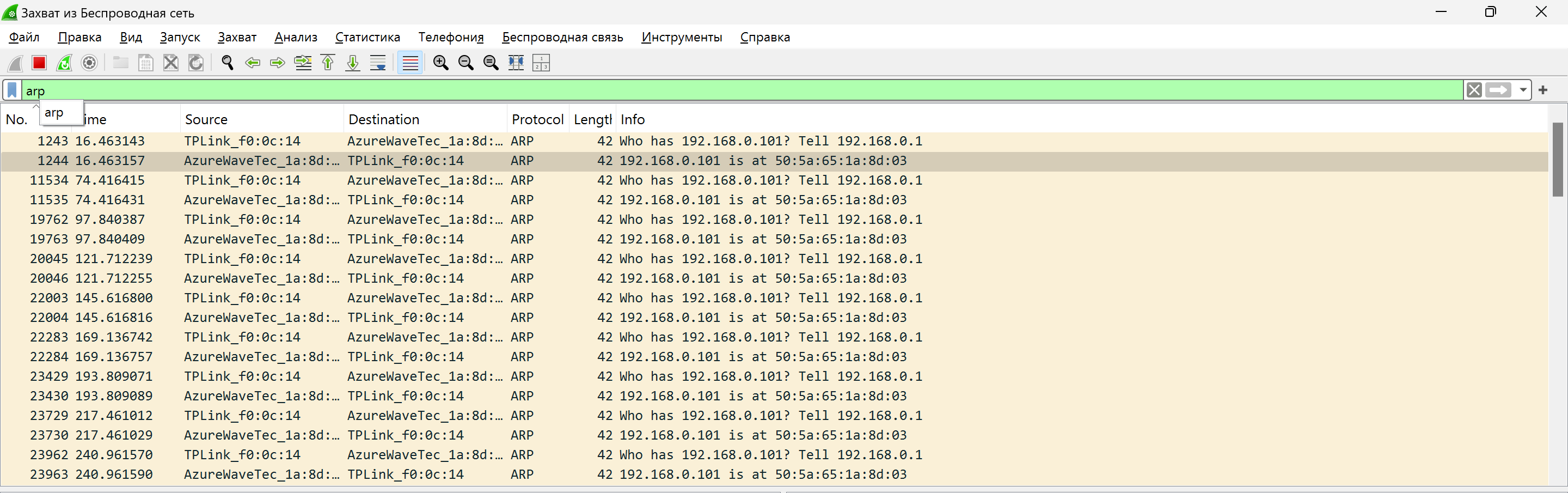
* A-запрос (Address Record): возвращает IPv4-адрес для указанного домена;
* AAAA-запрос: возвращает IPv6-адрес для указанного домена;
* CNAME-запрос (Canonical Name Record): возвращает каноническое
* (основное) доменное имя для указанного псевдонима;
* MX-запрос (Mail Exchange Record): возвращает адрес почтового сервера
* для указанного домена;
* NS-запрос (Name Server Record): возвращает список DNS-серверов,
* отвечающих за домен;
* PTR-запрос (Pointer Record): используется для обратного DNS, возвращая
* доменное имя для указанного IP-адреса;
* SOA-запрос (Start of Authority): возвращает информацию о DNS-зоне,
* включая основные данные о DNS-сервере.

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

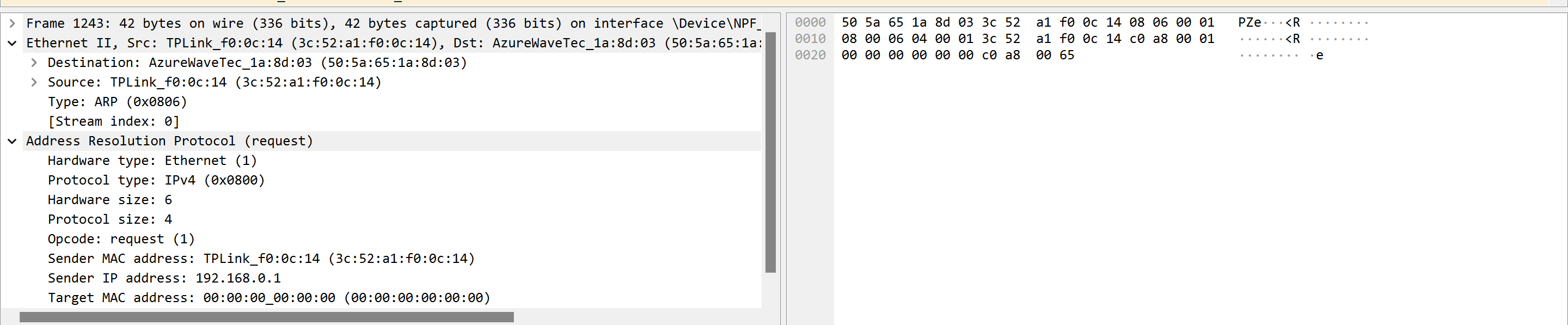
Независимые DNS-запросы требуются в том случае, если изображения на сайте загружаются с других доменов, отличных от основного домена страницы. Например, если основной сайт запрашивается по адресу example.com, но изображения загружаются с домена images.example.com или другого ресурса, тогда для каждого отдельного домена выполняется свой DNS-запрос. Это также происходит, если ресурсы, такие как изображения, загружаются с внешних источников (например, CDN или рекламных серверов).

# АНАЛИЗ ARP-ТРАФИКА

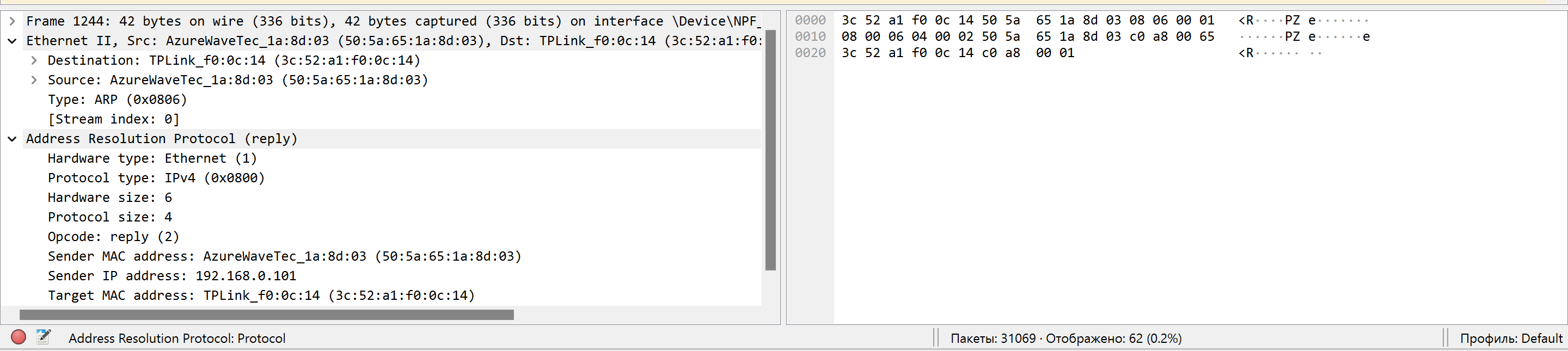
ARP (Address Resolution Protocol) – протокол, который используется для определения MAC-адреса устройства по его IP-адресу в локальной сети. Он работает, отправляя широковещательные запросы на все устройства в сети, которые содержат IP-адрес устройства, ищущего MAC-адрес. Устройства, имеющие указанный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



*Рисунок 16* – Фрагмент ARP-трафика



*Рисунок 17* – Пример ARP-запроса



*Рисунок 18* – 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).*

Source MAC Address — это МАС-адрес устройства, инициировавшего ARP-запрос (обычно это ваш компьютер или маршрутизатор). Destination MAC Address — это МАС-адрес устройства, к которому запрашивается связь (устройства, которое имеет указанный IP-адрес). Эти адреса идентифицируют физические устройства (сетевые интерфейсы) в локальной сети, такие как ваш компьютер, маршрутизатор или другой узел.

1. 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.

Source MAC Address в HTTP-пакете — это адрес сетевого интерфейса вашего устройства, которое отправляет запрос к серверу.Destination MAC Address — это адрес маршрутизатора (или другого сетевого устройства), через которое передается запрос на сервер. Эти адреса идентифицируют устройства в локальной сети или ближайшем сегменте сети, через который проходит HTTP-запрос.

1. *Для чего ARP-запрос содержит IP-адрес источника?*

ARP-запрос содержит IP-адрес источника для того, чтобы узел, который отправляет ARP-ответ, знал, кому именно отправлять ответное сообщение. Это позволяет получателю ARP-запроса узнать как МАС-адрес устройства, отправляющего запрос, так и его IP-адрес, чтобы затем связать их для дальнейшего общения в локальной сети.

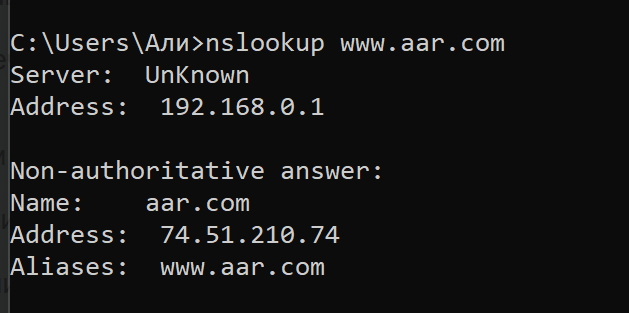
# АНАЛИЗ ТРАФИКА УТИЛИТЫ NSLOOKUP

NSLOOKUP — это утилита, которая позволяет через командную строку узнать

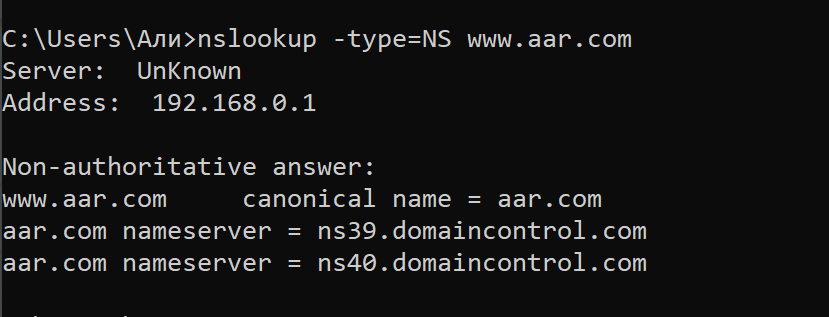
содержимое DNS.

Она может помочь:

* узнать IP-адрес;
* узнать A, NS, SOA, MX-записи для домена.



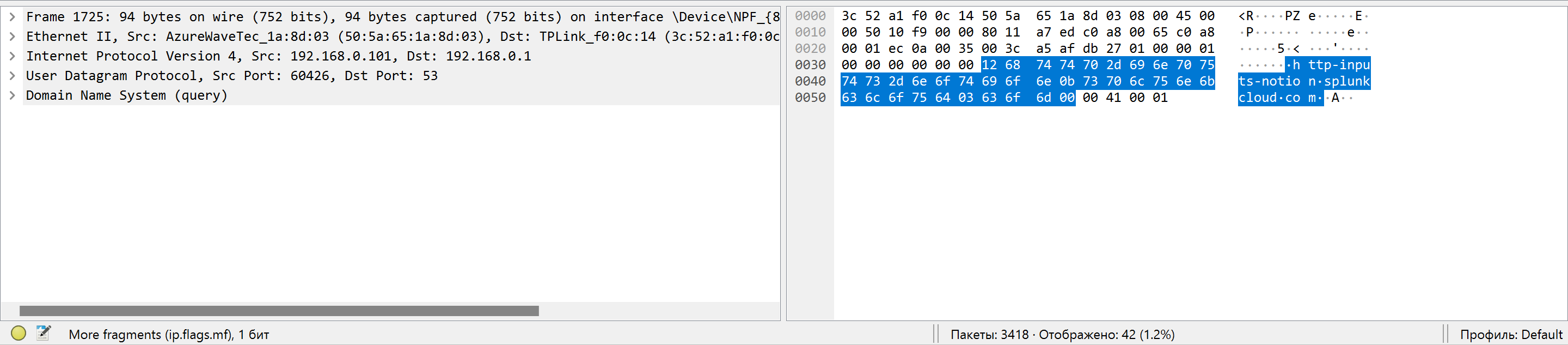
*Рисунок 19* – Использование nslookup



*Рисунок 20* – Использование nslookup с дополнительным параметром



*Рисунок 21* – Трафик от nslookup



*Рисунок 22* – Пример запроса DNS при действии nslookup

Ответы на вопросы

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

В п.2 утилита nslookup отправляет стандартный DNS-запрос, чтобы получить A-запись (адрес хоста) для указанного домена. В п.4 команда nslookup -type=NS запрашивает NS-записи, которые содержат имена DNS-серверов, ответственных за домен. Эти записи не содержат IP-адресов самого сайта, а указывают на серверы, отвечающие за его зону.

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

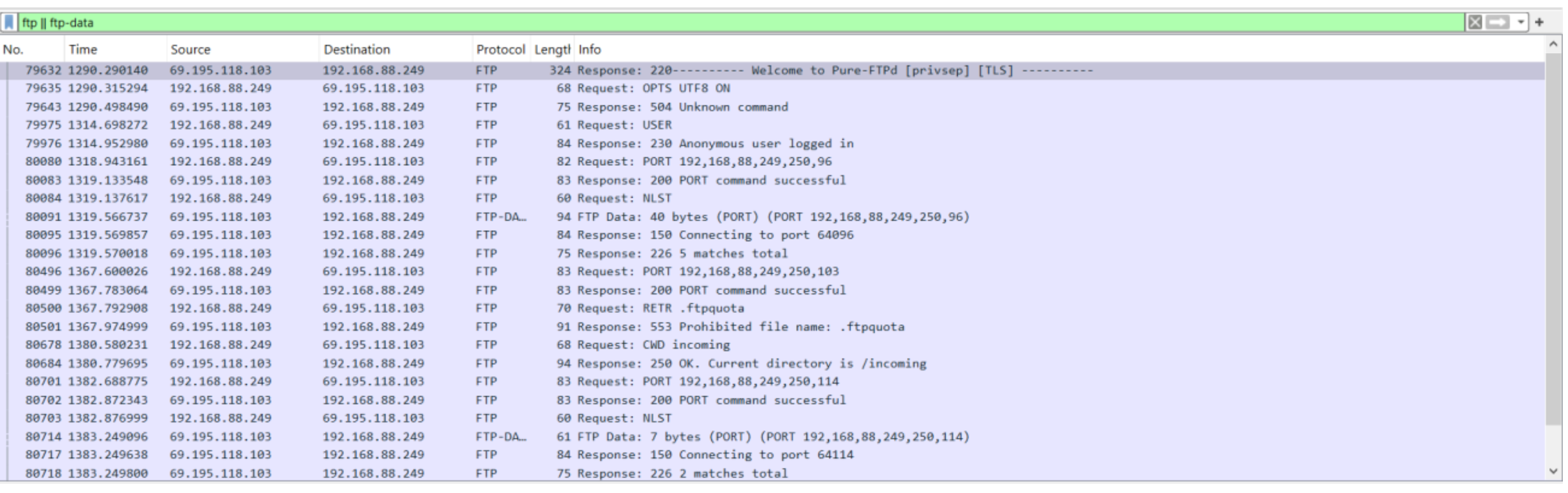
Поле Answers в DNS-ответе содержит информацию о запрашиваемом ресурсе. В случае стандартного запроса (п.2), это IP-адрес сайта (A-запись). В случае запроса на NS-записи (п.4), в поле Answers содержатся имена серверов, которые ответственны за зону указанного домена.

1. *Каковы имена серверов, возвращающих авторитативный (authoritative) отклик?*

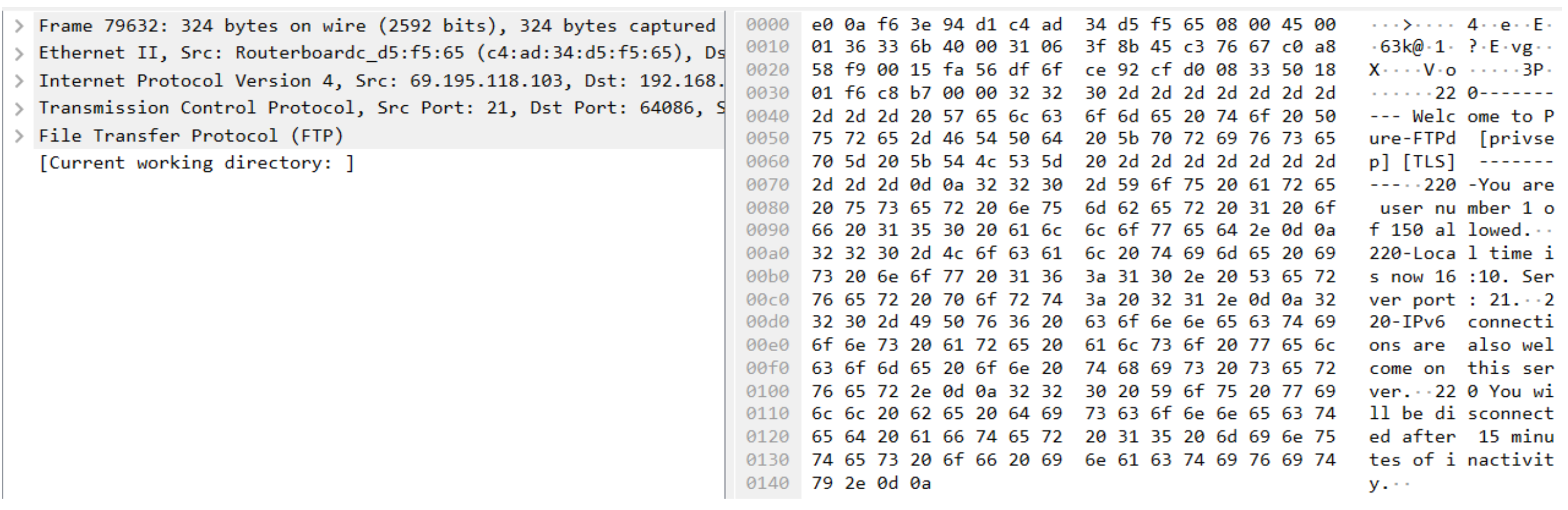
Имена серверов, дающих авторитативные ответы, находятся в поле Authority. Это серверы, которые ответственны за домен, к которому принадлежит запрашиваемый ресурс. Их можно найти в ответах на NS-запросы и в случае с A-запросами, если они обрабатываются авторитативным сервером.

# АНАЛИЗ FTP-ТРАФИКА

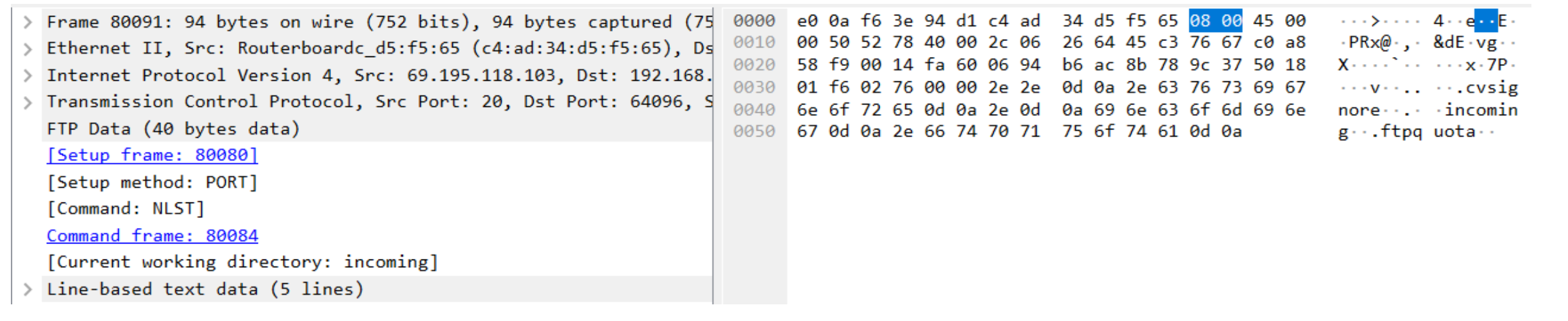
FTP (File Transfer Protocol) — это протокол, который предназначен для передачи файлов через Интернет или локальную компьютерную сеть. Основное назначение FTP — пересылать, копировать или передавать файл с удаленного компьютера на локальный и наоборот. Кроме того, при помощи FTP можно работать со своими файлами прямо на удаленном компьютере. Например, можно передать доступ к файлам или к части файлов своему разработчику, а он сможет переименовывать их, удалять или создавать каталоги.



*Рисунок 24* – Взаимодействие с публичным ftp-сервером



*Рисунок 25* – Ответ о подключении к серверу (ftp)



*Рисунок 26* – Получение данных с ftp-сервера (ftp-data)

**Ответы на вопросы:**

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

FTP-DATA — это пакеты, содержащие полезные данные, которые передаются в процессе передачи файлов через FTP. Размер данных в пакете может варьироваться, но обычно составляет 1460 байт, что связано с ограничением на максимальный размер сегмента (MSS) TCP для большинства сетей. Чтобы узнать точный размер данных в пакете, в Wireshark можно посмотреть поле "Length" в деталях пакета FTP-DATA. Оно указывает количество байт данных, переданных в данном пакете.

* 1. *Как выбирается порт транспортного уровня, который используется*

*для передачи FTP-пакетов?*

FTP использует два порта:

* порт 21 для команд управления (FTP control), используется для передачи управляющих команд между клиентом и сервером;
* порт 20 (или случайно выбранный порт в активном или пассивном режиме) для передачи данных (FTP-DATA). В активном режиме клиент сообщает серверу о порте, который нужно использовать для передачи данных, а в пассивном режиме сервер сообщает клиенту порт, который будет использоваться для передачи данных. В активном режиме клиент сообщает серверу, какой порт он должен использовать для передачи данных, а в пассивном режиме сервер выбирает случайный порт для передачи данных.
  1. *Чем отличаются пакеты FTP от FTP-DATA?*

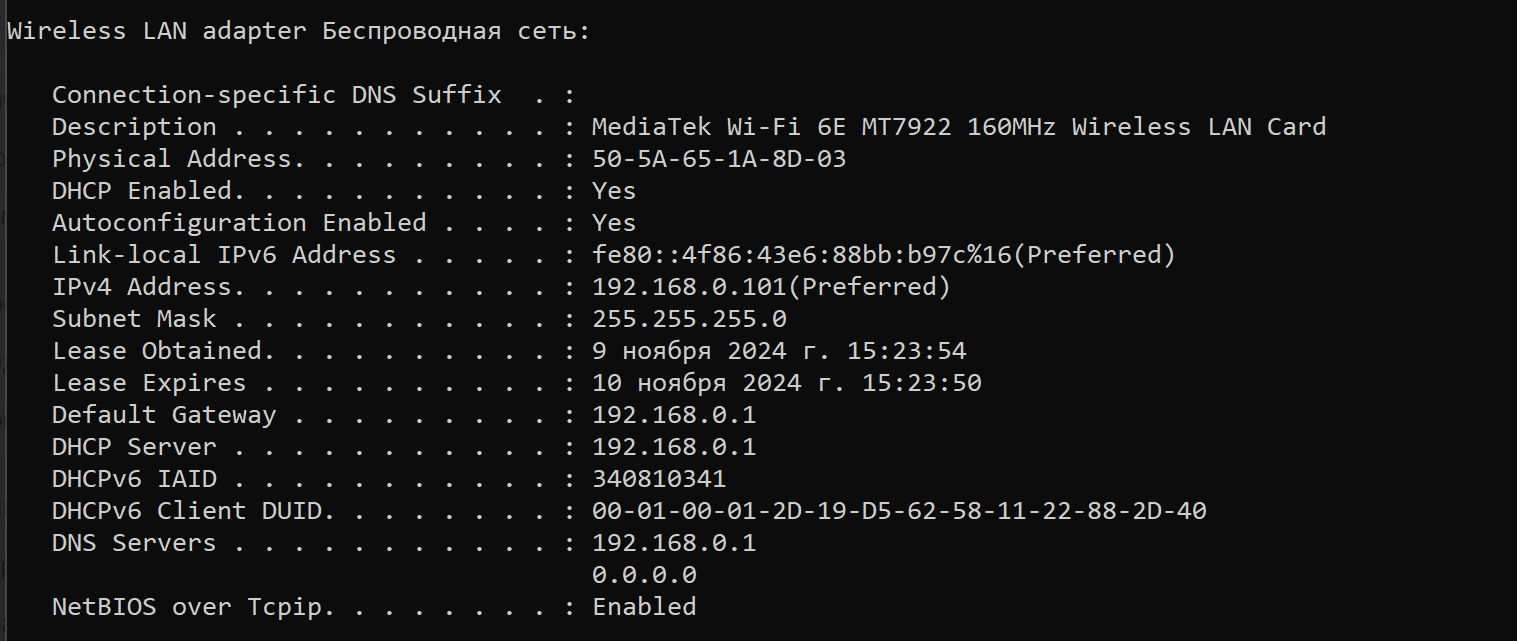
FTP-пакеты — это управляющие пакеты, которые используются для отправки команд между клиентом и сервером. Например, команды авторизации, навигации по директориям или запроса на скачивание файла. Эти пакеты передаются по порту

FTP-DATA — это пакеты, которые содержат полезные данные (например, части файлов), передаваемые между клиентом и сервером. Эти пакеты передаются по порту 20 или случайному порту в пассивном режиме. Основное различие заключается в том, что FTP-пакеты используются для управления сессией и отправки команд, а FTP-DATA содержат фактические данные, передаваемые между клиентом и сервером.

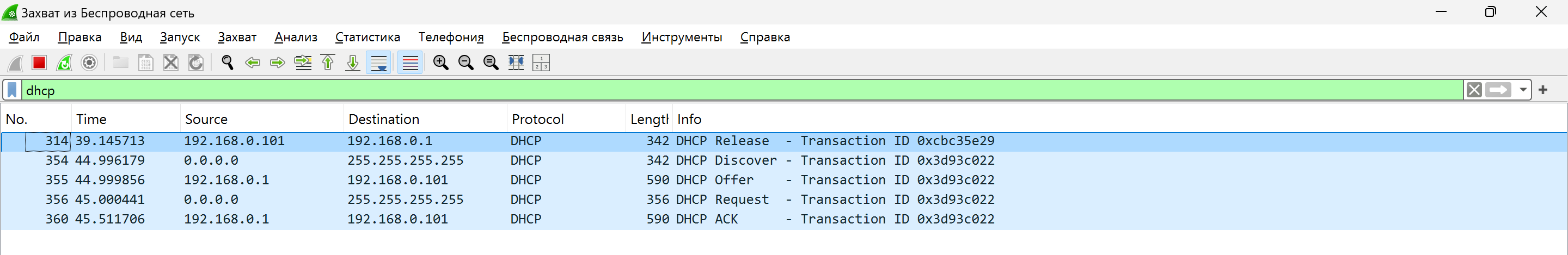
# АНАЛИЗ DHCP-ТРАФИКА

DHCP (Dynamic Host Configuration Protocol) — это сетевой протокол, используемый для автоматического назначения IP-адресов и других сетевых параметров (например, шлюза, маски подсети и DNS-серверов) устройствам в сети.

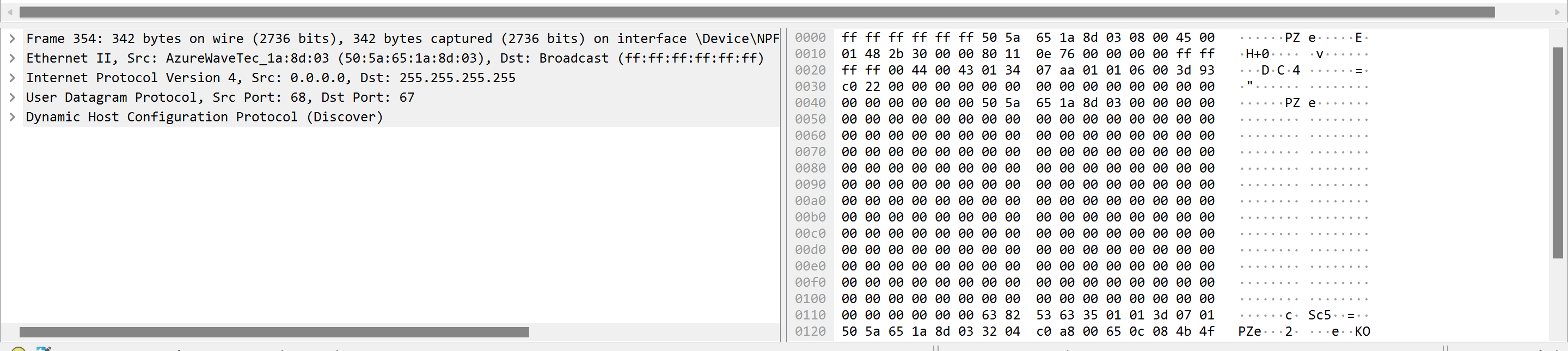
Этот процесс позволяет упростить управление IP-адресами и уменьшить вероятность конфликта IP-адресов, когда два устройства случайно получают один и тот же IP-адрес.



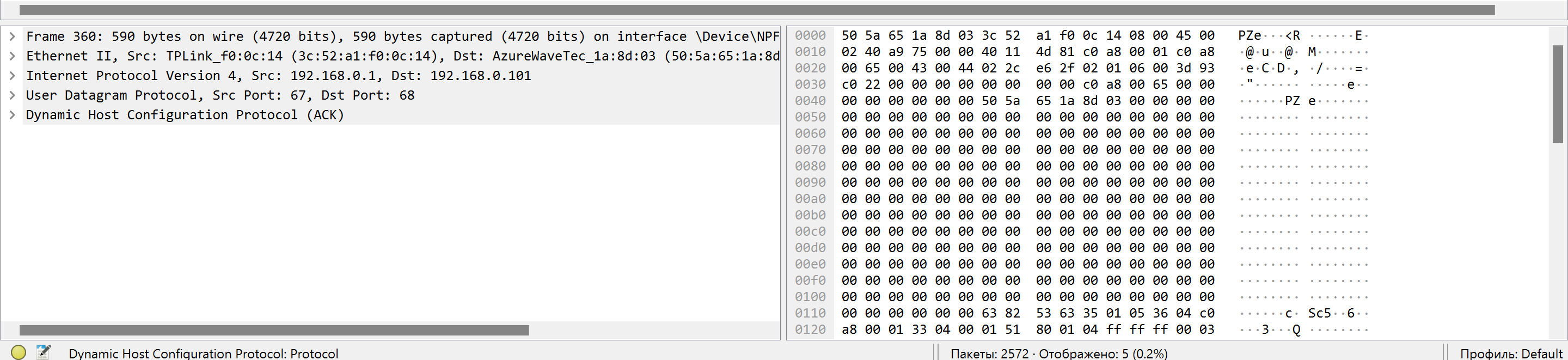
*Рисунок 27* – IP-адрес компьютеру выдан DHCP-сервером

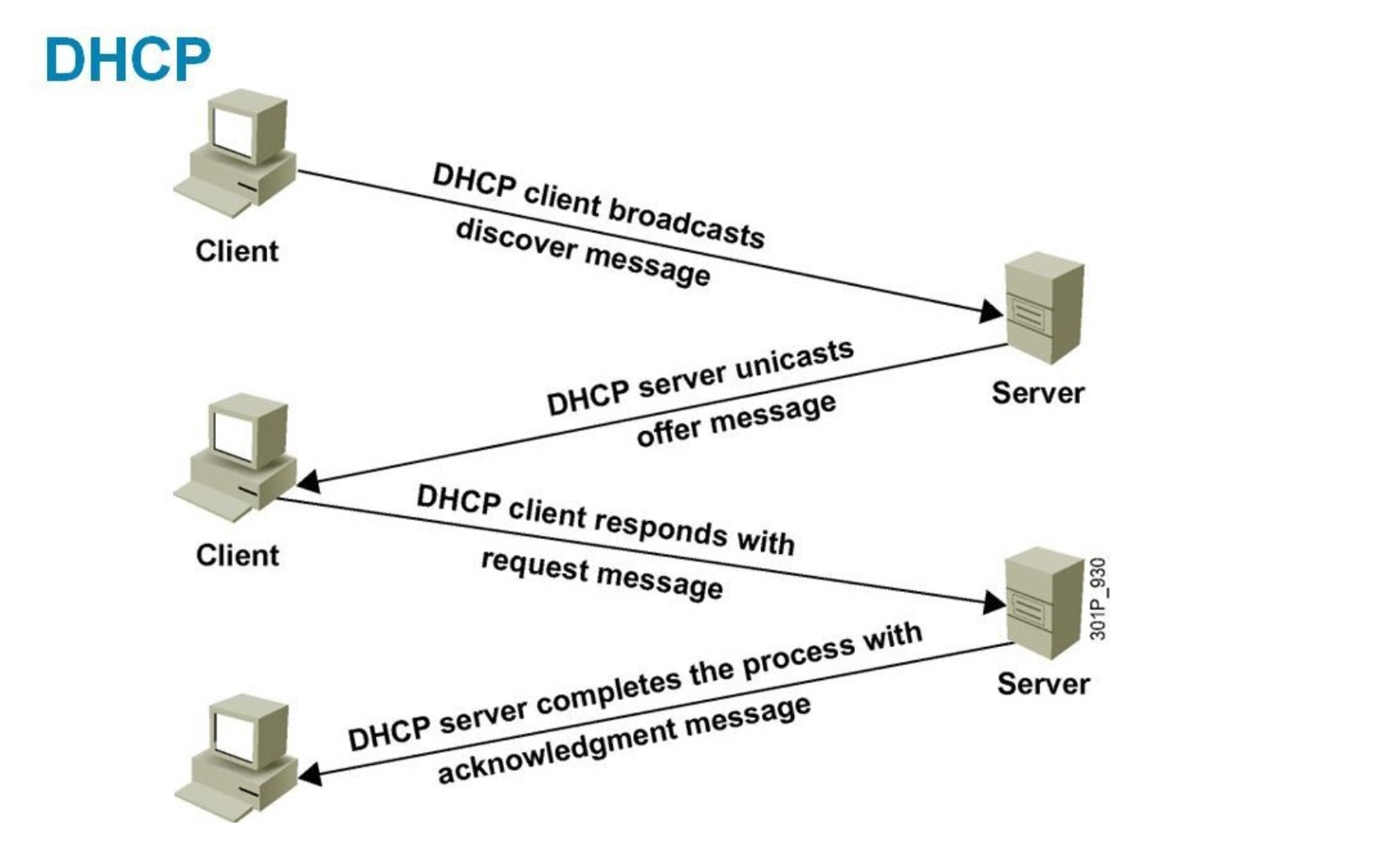
****

*Рисунок 28* – Работа DHCP (было выполнено 2 команды: ipconfig /release и ipconfig /renew)



*Рисунок 29* – Строение Discover

*Рисунок 30* – Строение ACK



*Рисунок 31* – Работа протокола DHCP

**Ответы на вопросы**

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

* DHCP Discover — это первый пакет, отправленный клиентом в широковещательном режиме (broadcast), чтобы найти DHCP-сервер и начать процесс получения IP-адреса.
* DHCP Request — это пакет, отправляемый клиентом после получения предложения от DHCP-сервера (DHCP Offer), чтобы официально запросить предложенный IP-адрес.

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

В начале обмена (пакет Discover) клиент ещё не знает свой IP-адрес, поэтому он использует широковещательный IP-адрес (0.0.0.0) и MAC-адрес своего сетевого интерфейса. В пакете DHCP Offer сервер сообщает клиенту, какой IP-адрес может бытьназначен. MAC-адрес источника — это всегда MAC-адрес клиента, а MAC-адрес назначения зависит от того, кому отправляется пакет: серверу или всем устройствам в сети (в случае broadcast).

1. *Каков IP-адрес DHCP-сервера?*

Адрес DHCP-сервера можно найти в поле "Server Identifier" в пакете DHCP Offer или DHCP ACK. Он указывает, какой сервер отвечает на запросы.

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

Очистка фильтра в Wireshark приведет к тому, что вы снова будете видеть весь сетевой трафик, а не только DHCP-пакеты. Это может усложнить анализ, так как в захваченном трафике будет больше данных.

# Заключение

В результате проделанной работы была исследована структура протокольных блоков данных, а также проведен анализ реального сетевого трафика на компьютере студента с использованием бесплатной утилиты Wireshark.

Изучены возможности программы Wireshark, выполнен сбор дампов пакетов и произведено детальное исследование необходимых сетевых пакетов.