Университет ИТМО

Факультет ФПИ и КТ

P33131

**Отчет**

**по лабраторной работе №5**

# «Сети-компьютера»

Студент:

Ляо Ихун

Гр.P33131

Предподаватель:

Тропченко Андрей Александрович

**Цель работы**

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

В процессе выполнения домашнего задания выполняются наблюдения за передаваемым трафиком с компьютера пользователя в Интернет и в обратном направлении. Применение специализированной утилиты Wireshark позволяет наблюдать структуру передаваемых кадров, пакетов и сегментов данных различных сетевых протоколов. При выполнении УИР требуется анализировать последовательности команд и назначение служебных данных, используемых для организации обмена данными в следующих протоколах: ARP, DNS, FTP, HTTP, DHCP.

**Этап 1**

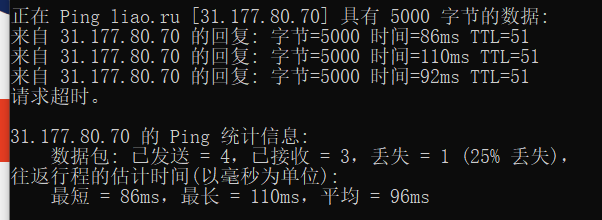
Необходимо отследить и проанализировать трафик, создаваемый

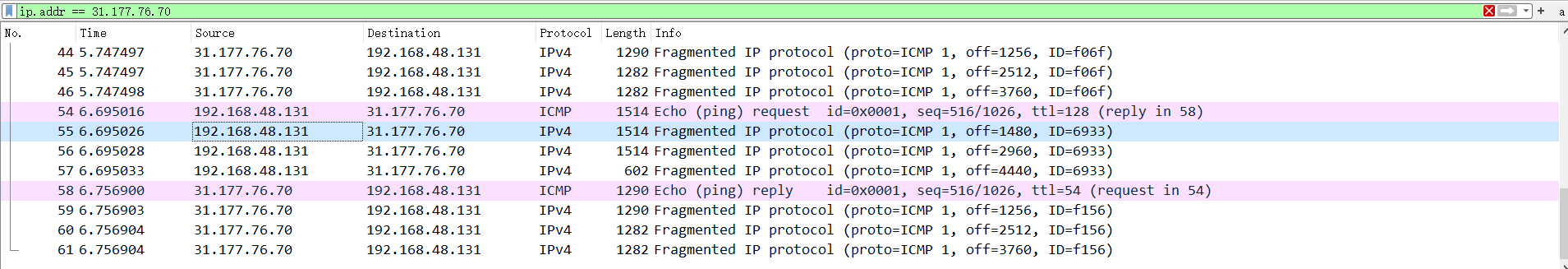
утилитой ping, запустив её следующим образом из командной строки:

“ping -l размер\_пакета адрес\_сайта\_по\_варианту”.

Например, “ping -l 2000 wireshark.org” (без кавычек). В качестве “размера\_пакета” необходимо поочерёдно использовать

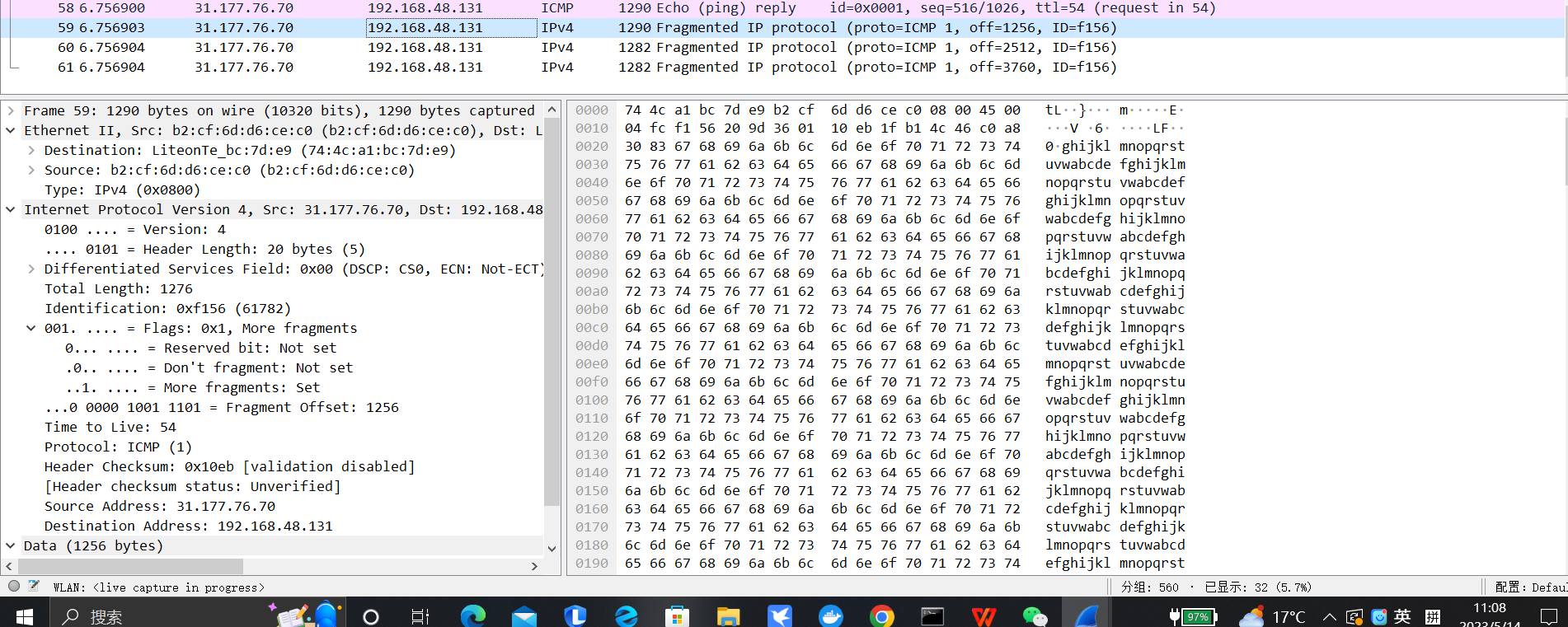
различные значения от 100 до 10000, самостоятельно выбрав шаг изменения. По результатам анализа собранной трассы, необходимо ответить на следующие вопросы и выполнить указанные задания.





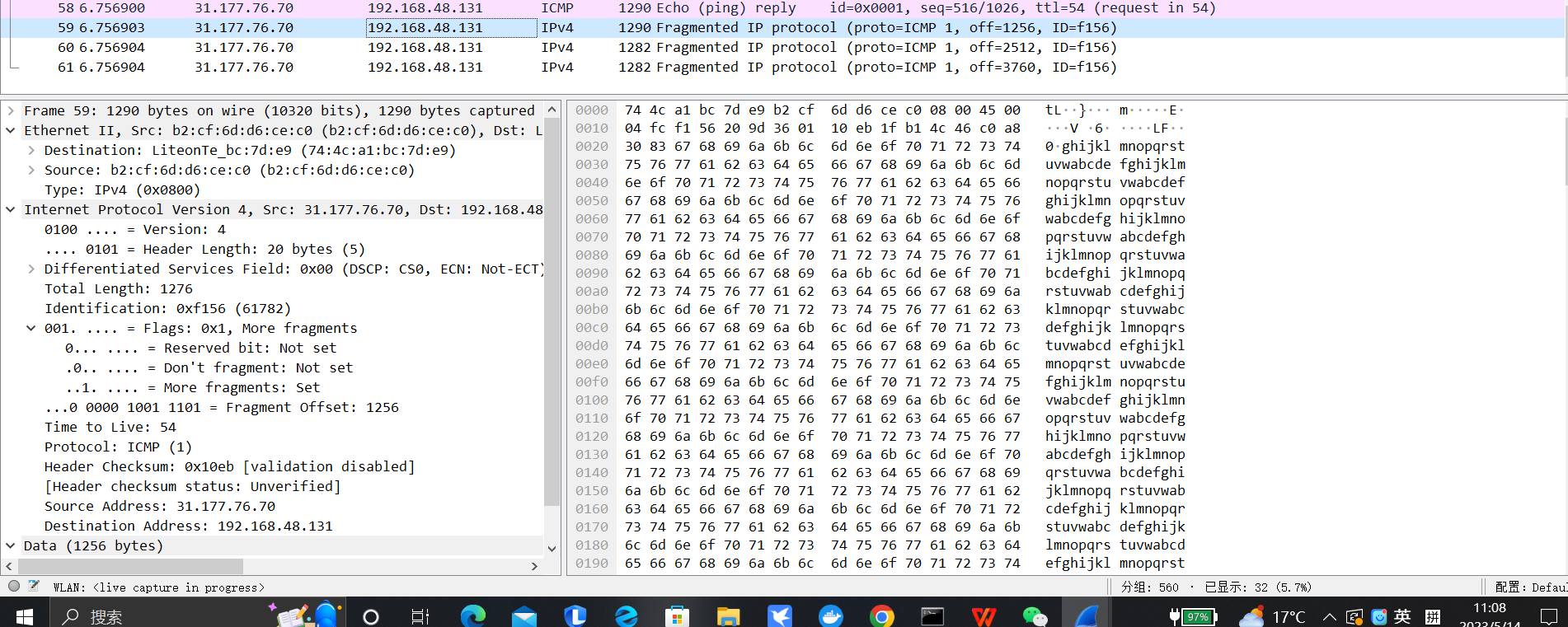
1. Имеет ли место фрагментация исходного пакета, какое поле на это указывает?

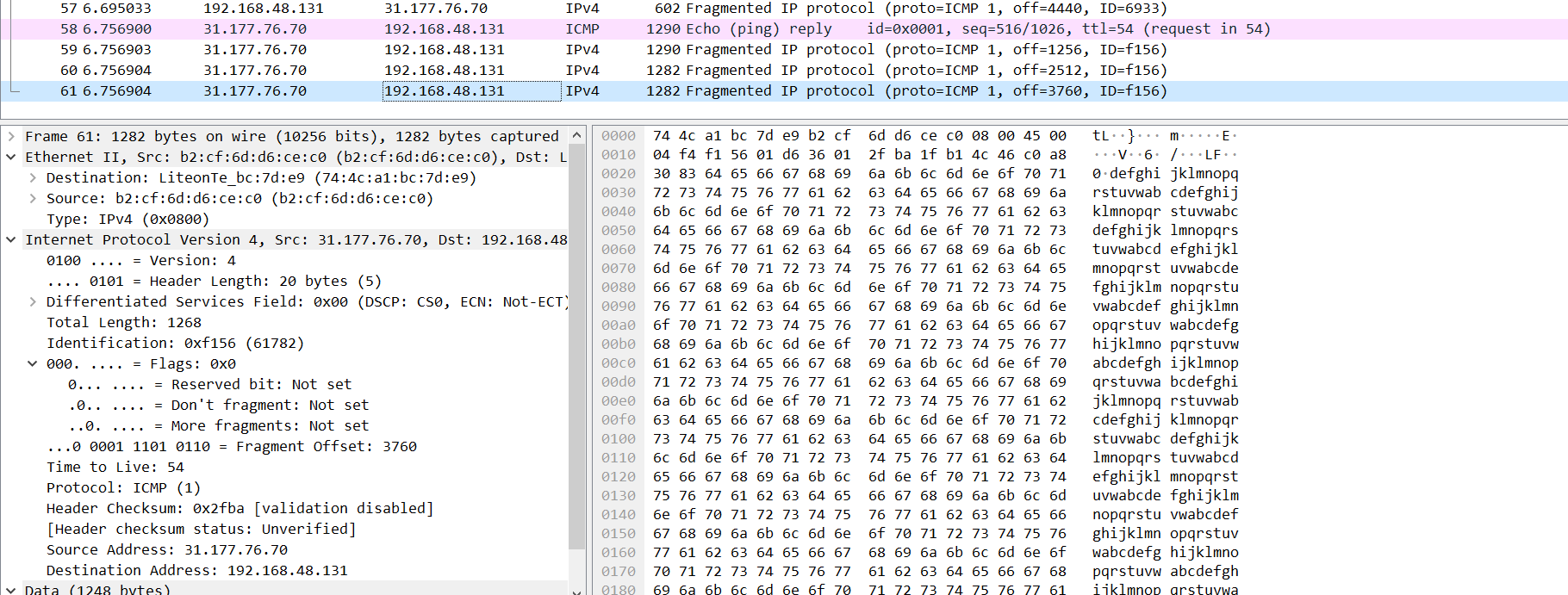
Да. Флаг More Fragments как раз указывает на наличие фрагментации исходного пакета.



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

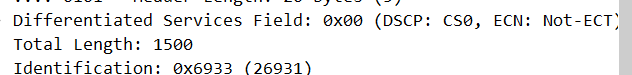
Флаг More Fragments



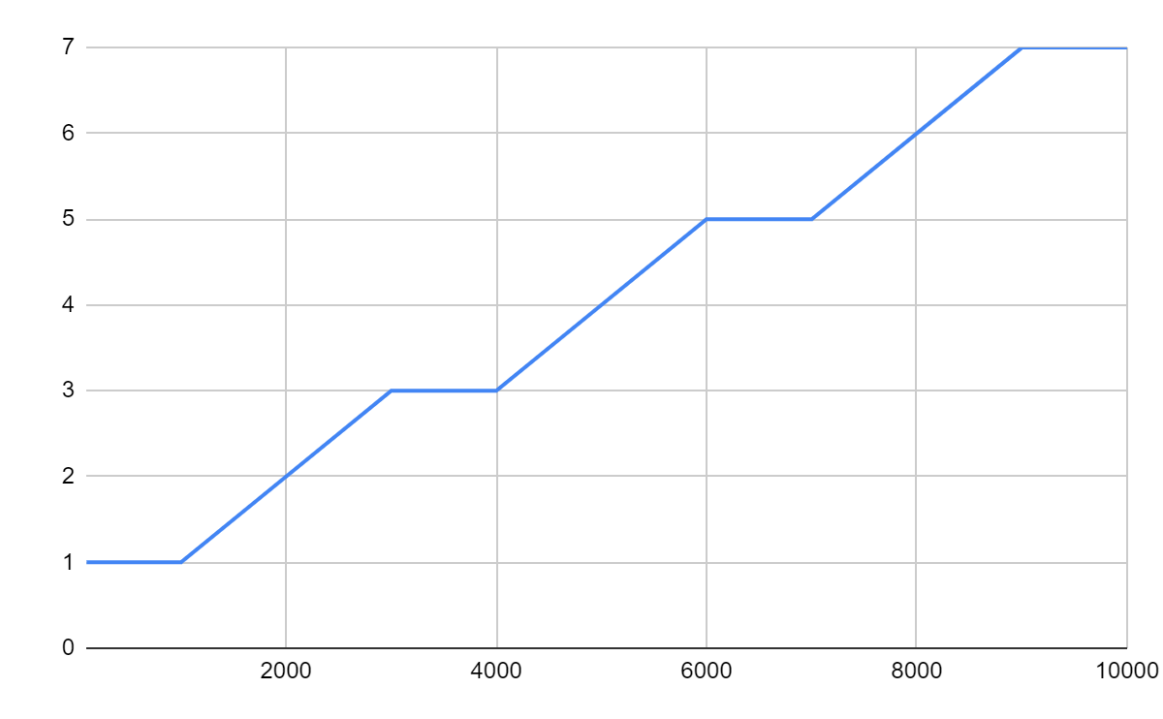


1. Чему равно количество фрагментов при передаче ping-пакетов?

Количество фрагментов = ceil(Длина сообщения (байт) / 1500 байт (фрагмент)

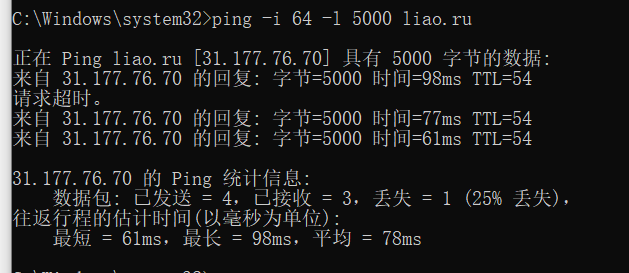


4.Построить график, в котором на оси абсцисс находится размер пакета, а по оси ординат – количество фрагментов, на которое был разделён каждый

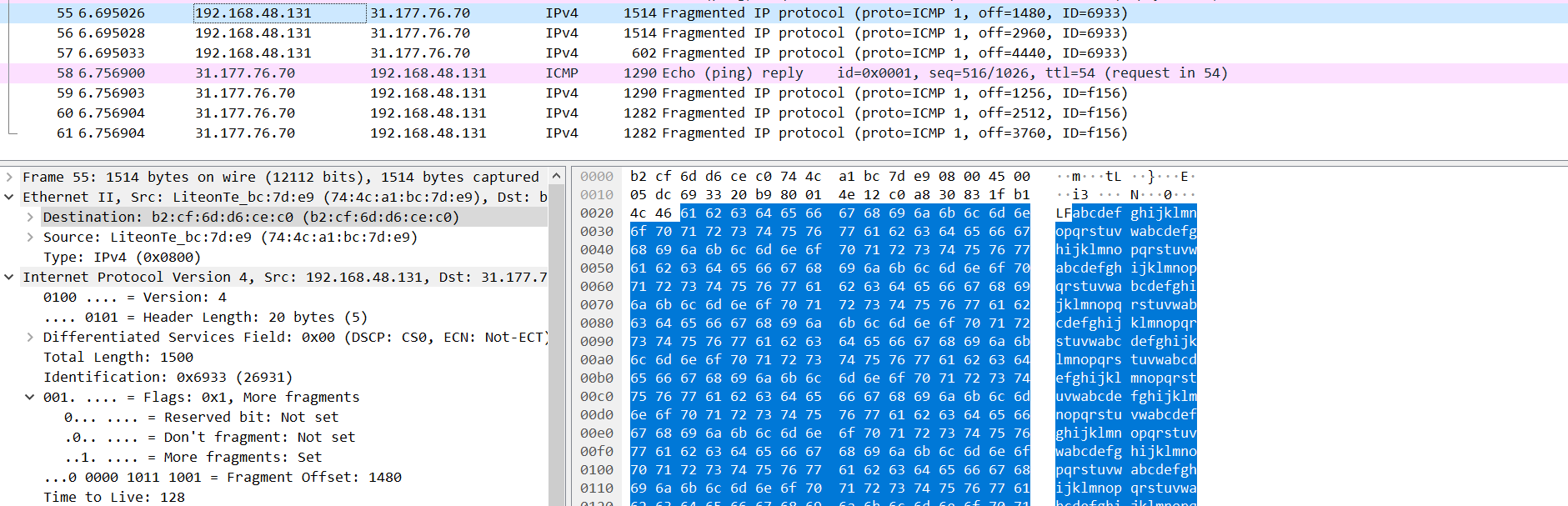


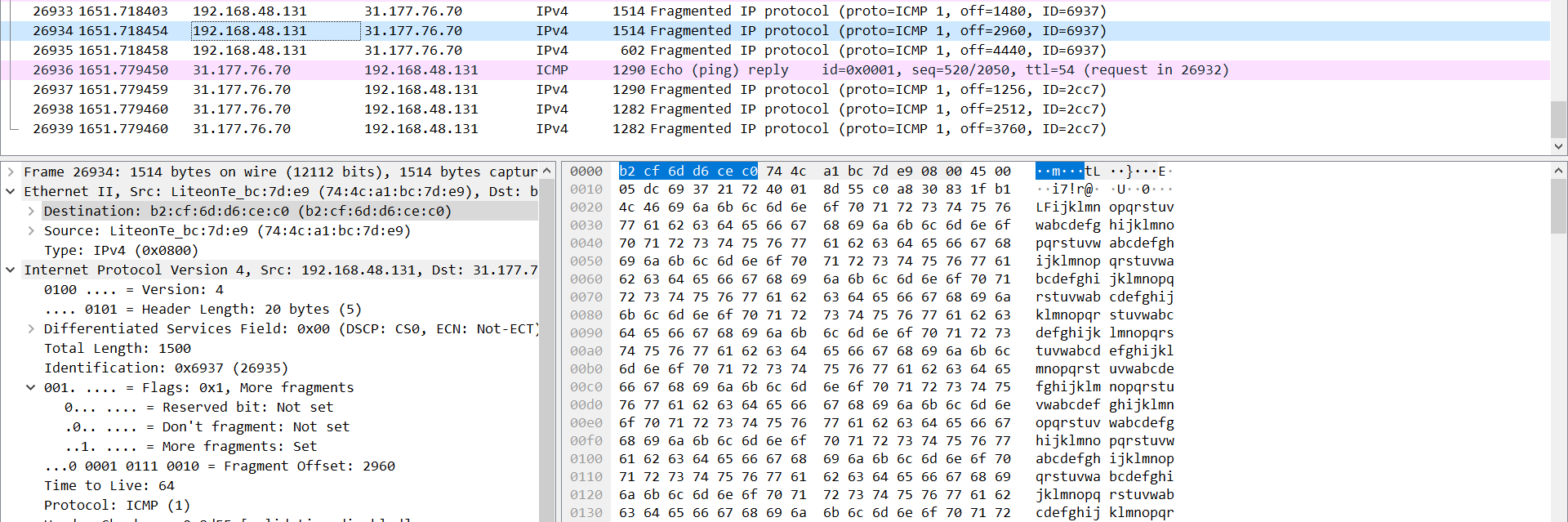
1. Как изменить поле TTL с помощью утилиты ping?

Ping -i <новая TTL>



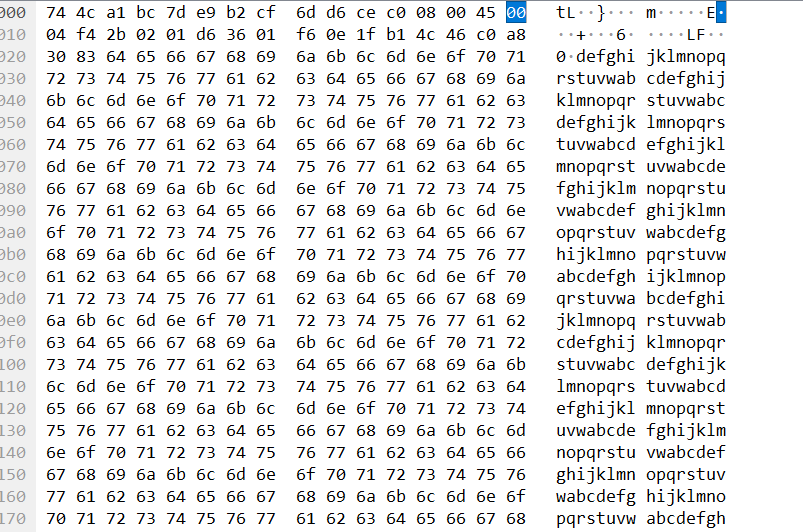
Before:



After:

1. Что содержится в поле данных ping-пакета?

ASCII английских букв и знаков

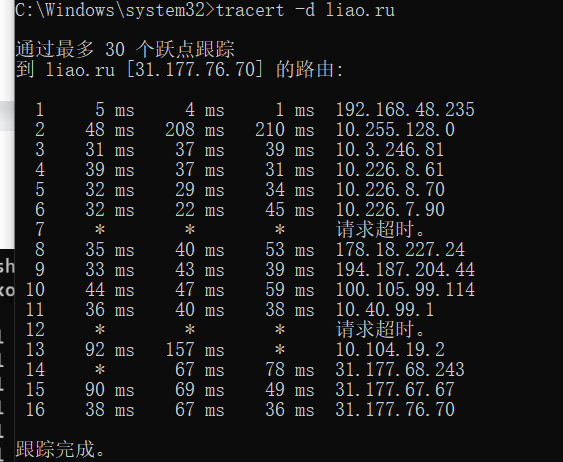


**Этап 2**

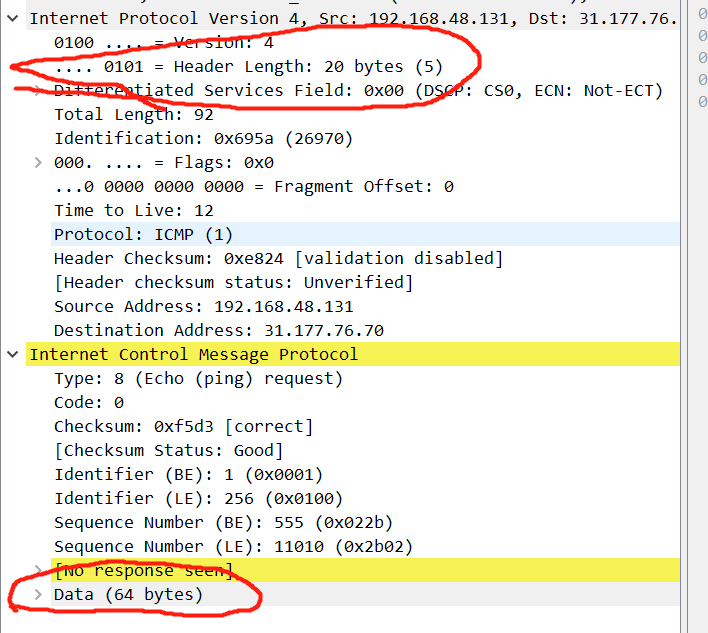
Необходимо отследить и проанализировать трафик, создаваемый утилитой tracert (или traceroute в Linux), запустив её следующим образом из командной строки:

“tracert -d адрес\_сайта\_по\_варианту”

Например, tracert wireshark.org.



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



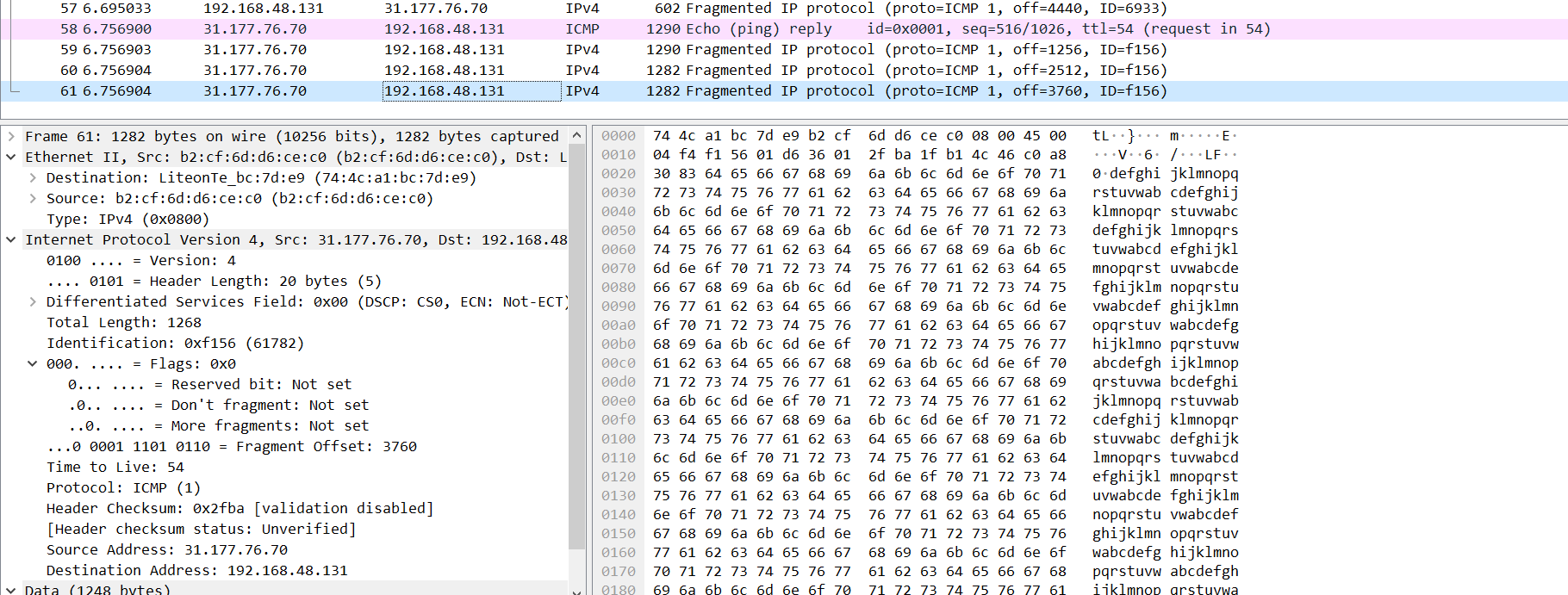
1. Как и почему изменяется поле TTL в следующих друг за другом ICMP-пакетах tracert? Для ответа на этот вопрос нужно проследить изменение TTL при передаче по маршруту, состоящему из более чем двух хопов.

Утилита tracert отправляет первый пакет с TTL, равным 1, и увеличивает значение TTL на 1 для каждого последующего пакета, отправляемого до тех пор, пока пункт назначения не ответит или пока не будет достигнуто максимальное значение поля TTL. И через каждый маршрутитатор TTL уменьшается на 1.

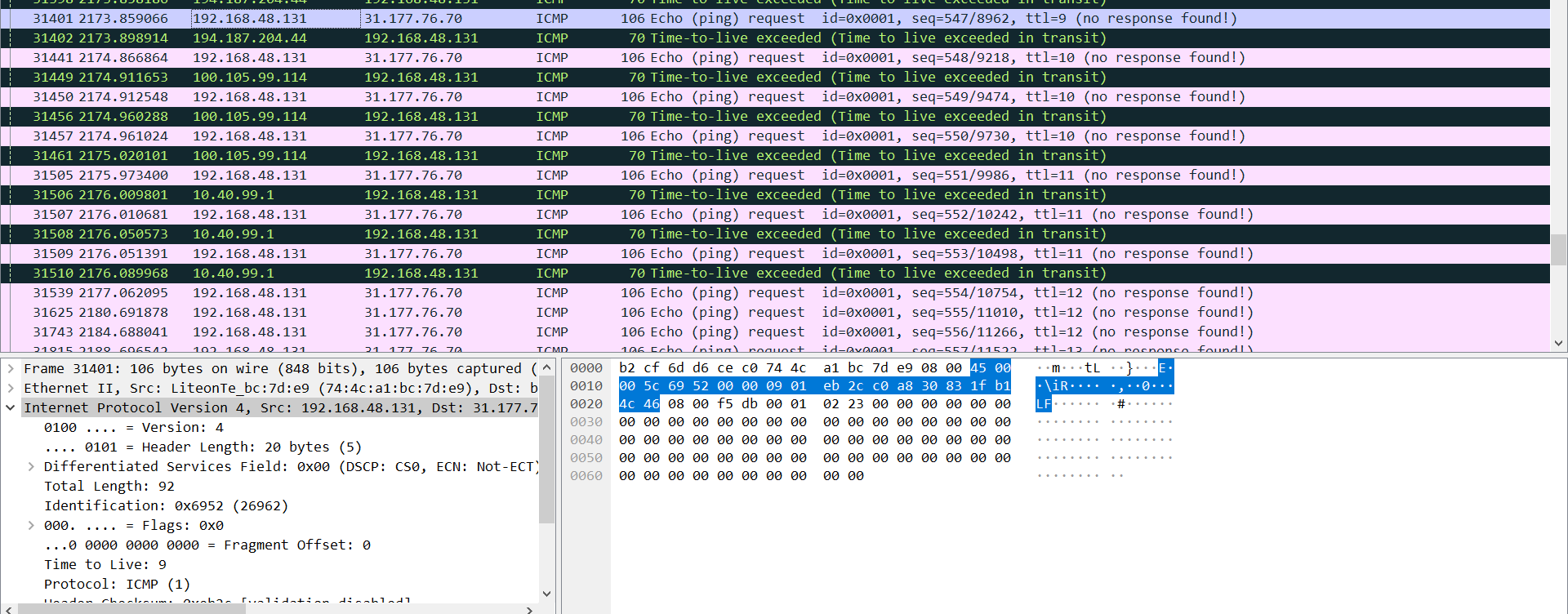
1. Чем отличаются ICMP-пакеты, генерируемые утилитой tracert, от ICMP-пакетов, генерируемых утилитой ping

В поле данных содержат нули.

ping



tracert:

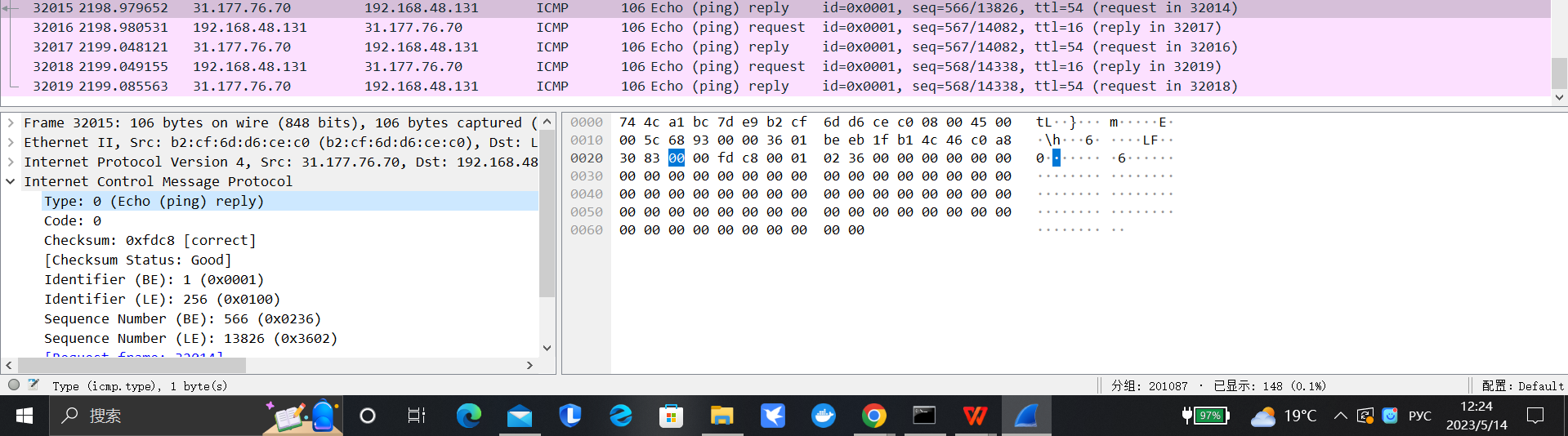
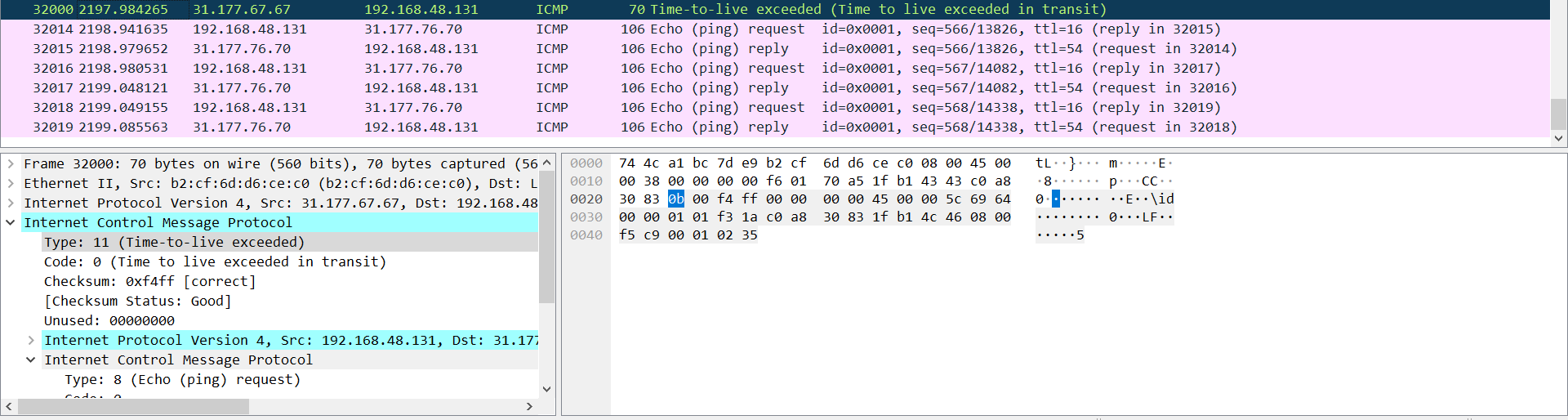
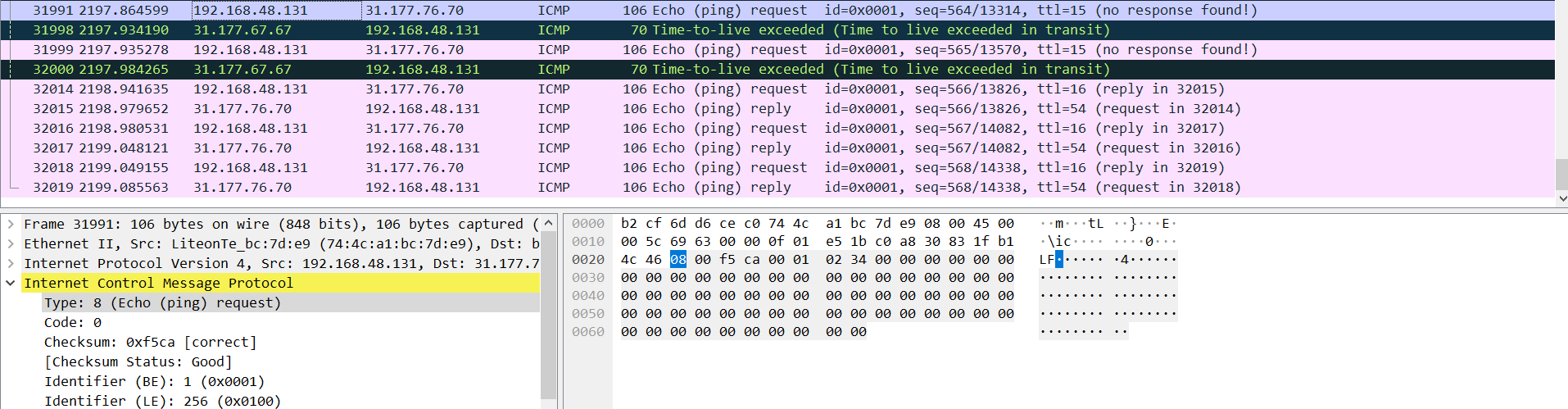


1. Чем отличаются полученные пакеты «ICMP reply» от «ICMP error» и зачем нужны оба этих типа ответов?

Пакеты «ICMP reply» указывают на получение ответного сообщения.

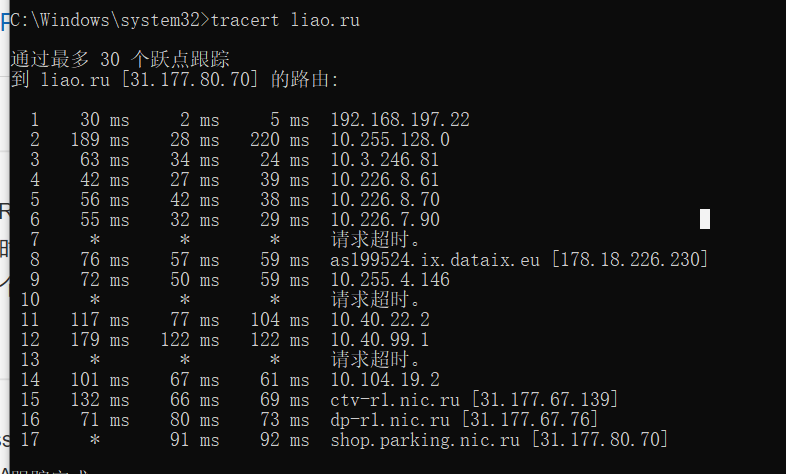
Пакеты «ICMP error» указывают на то, что произошла ошибка.

Они используются чтобы различать причину истечения TTL.



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

дополнительный трафик при этом будет генерироваться?



Без -d будет перевод ip на называние компьтера.

**Этап 3**

посещении Интернет-сайта, заданного по варианту. В списке захваченных пакетов

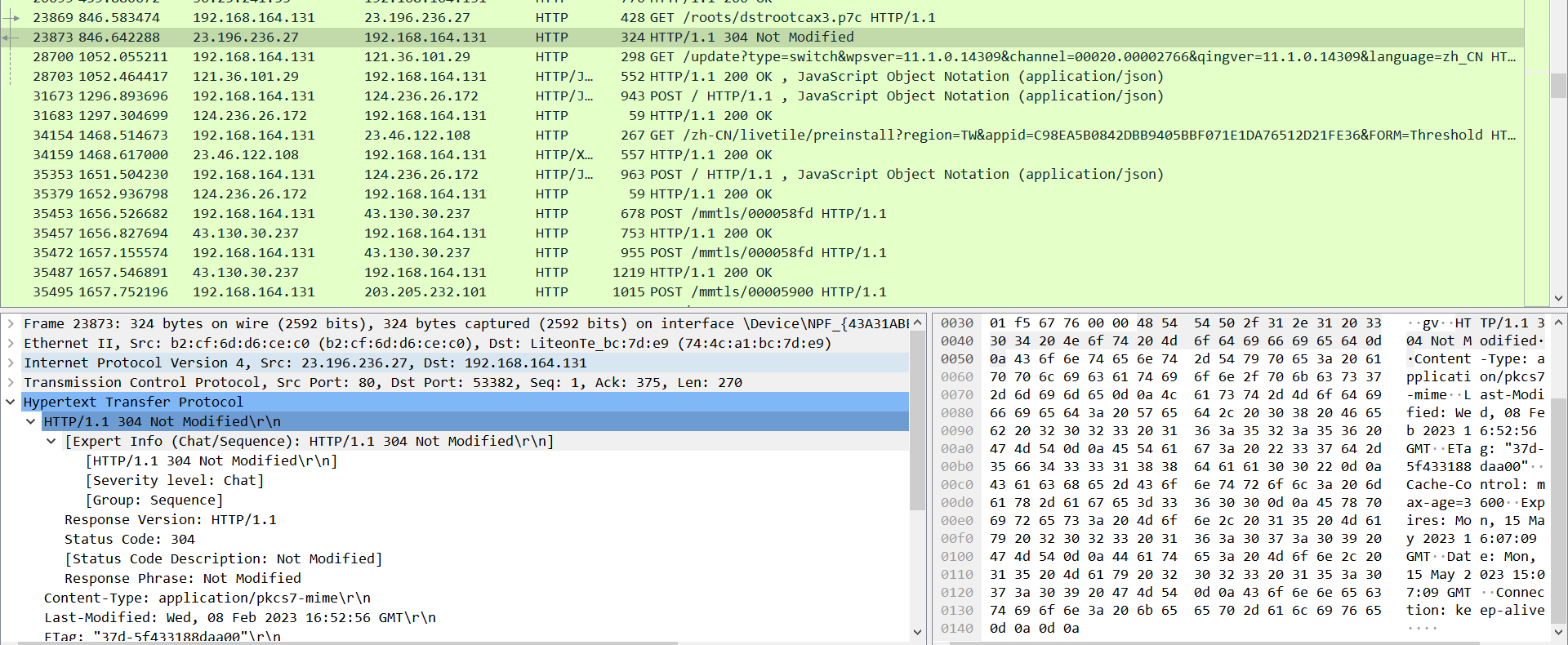
необходимо проанализировать следующую пару HTTP-сообщений (запрос-ответ):

● GET-сообщение от клиента (браузера);

● ответ сервера.

Для этого в поле с детальной информацией о пакете нужно развернуть строку “HTTP”. Затем необходимо обновить страницу в браузере так, чтобы вместо «HTTP GET» был сгенерирован «HTTP CONDITIONAL GET» (так называемый «условный GET»). Условные запросы GET содержат поля If-Modified-Since, If-Match, If-Range и подобные, которые позволяют при повторном запросе не передавать редко изменяемые данные. В ответ на условный GET тело запрашиваемого ресурса передается только в том случае, если этот

ресурс изменялся после даты «If-Modified- Since». Если ресурс не изменялся, сервер вернет код статуса «304 Not Modified».



**Этап 4**

Необходимо отследить и проанализировать трафик протокола DNS, сгенерированный в результате выполнения следующих действий:

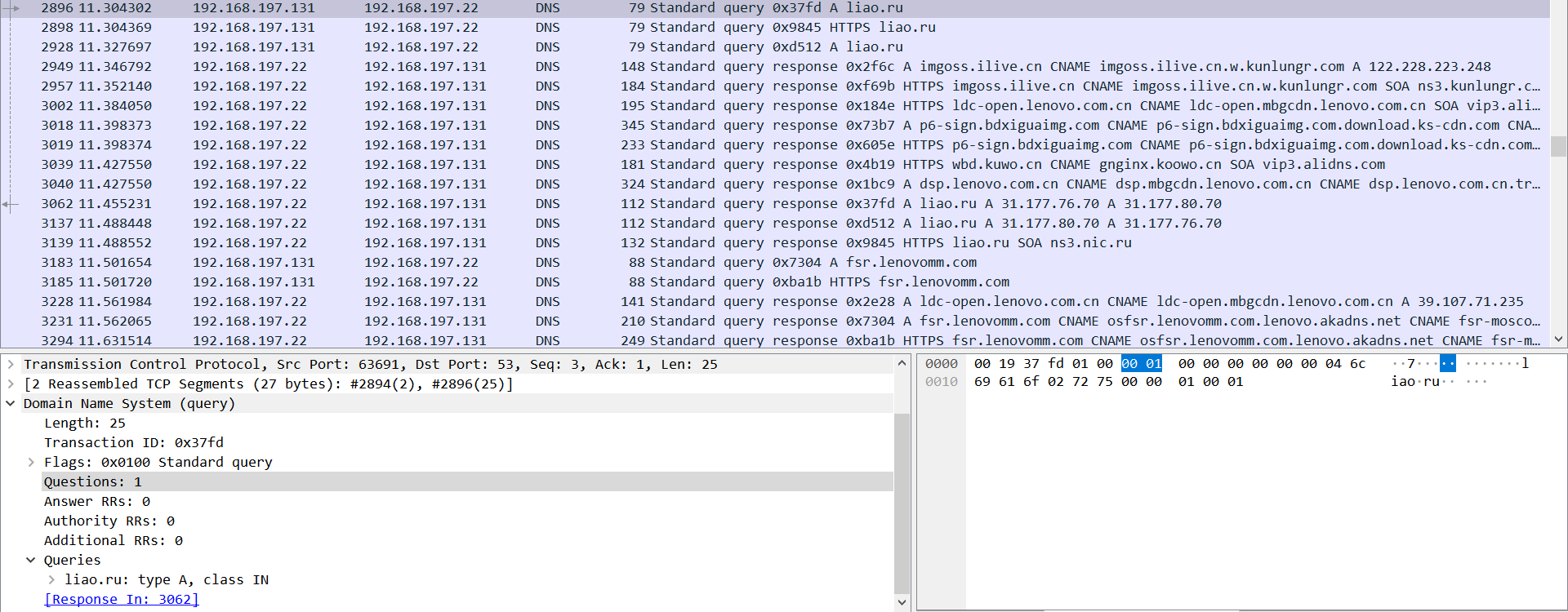
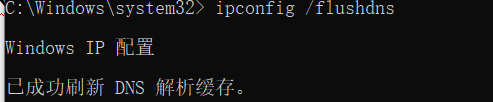
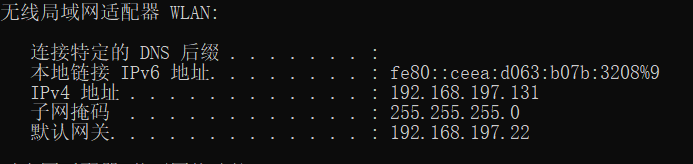
● настроить Wireshark-фильтр: “ip.addr == ваш\_IP\_адрес”;

● очистить кэш DNS с помощью команды ipconfig в командной

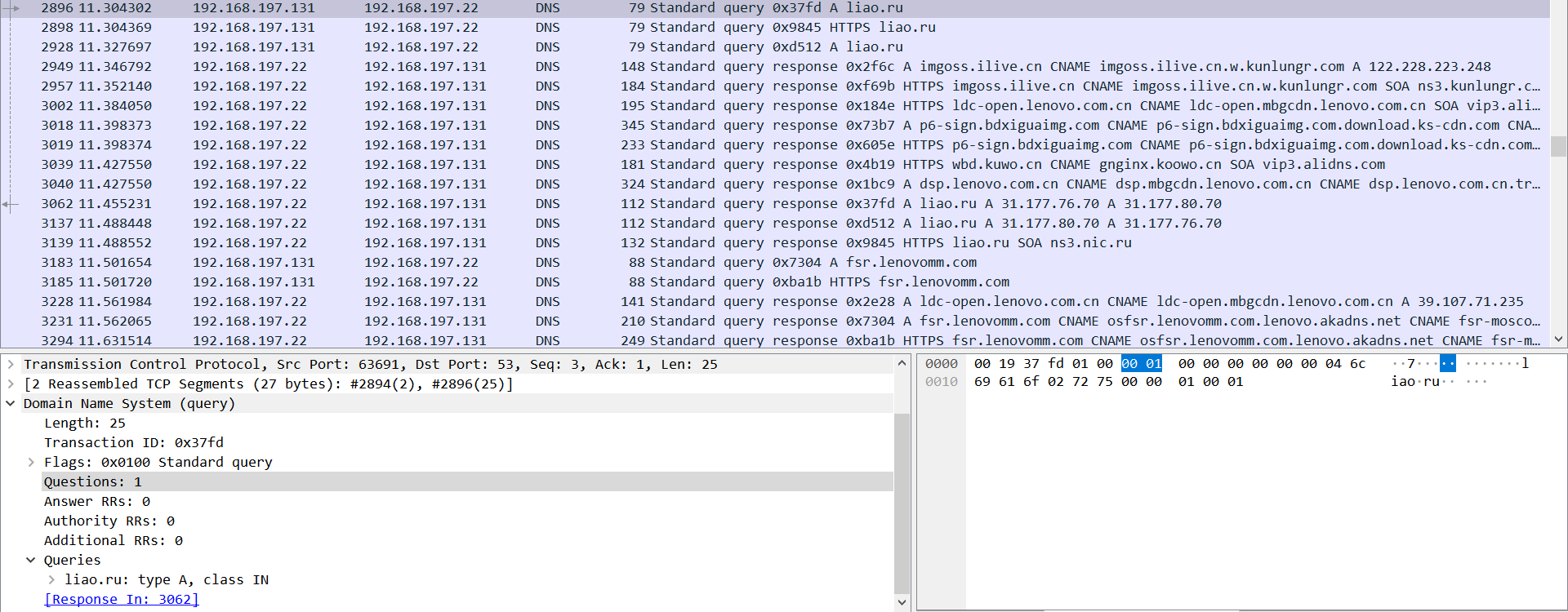
строке: ipconfig /flushdns

● очистить кэш браузера;

● зайти на Интернет-сайт, заданный по варианту



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



Необходимого получить с DNS-сервера адрес сайта.

1. Какие бывают типы DNS-запросов?

**Прямой:** преобразование домена в IP-адрес.

**Обратный:** преобразование IP-адреса в домен.

**Рекурсивный:** выполняется DNS-сервером, пока не будет найден домен или не будет получен ответ, что домен не существует. Рекурсия выполняется сервером.

**Итеративный:** то же самое, что рекурсивный, но также допускается выполнение поиска клиентом.

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

Если запрашиваемое изображение находится на другом сервере.

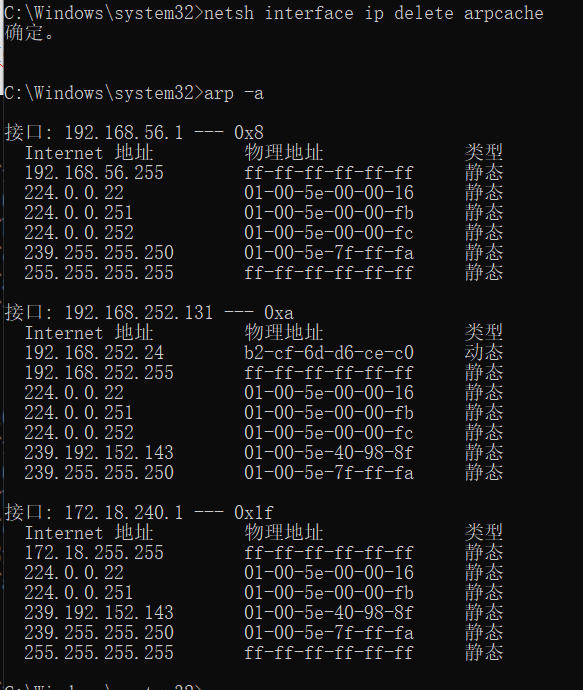
**Этап 5**

Необходимо отследить и проанализировать трафик протокола ARP, сгенерированный в результате выполнения следующих действий:

● очистить ARP-таблицу командой “netsh interface ip delete arpcache” (проверить очистилась ли таблица можно с помощью команды “arp -a”, выводящей таблицу на экран);

● очистить кэш браузера;

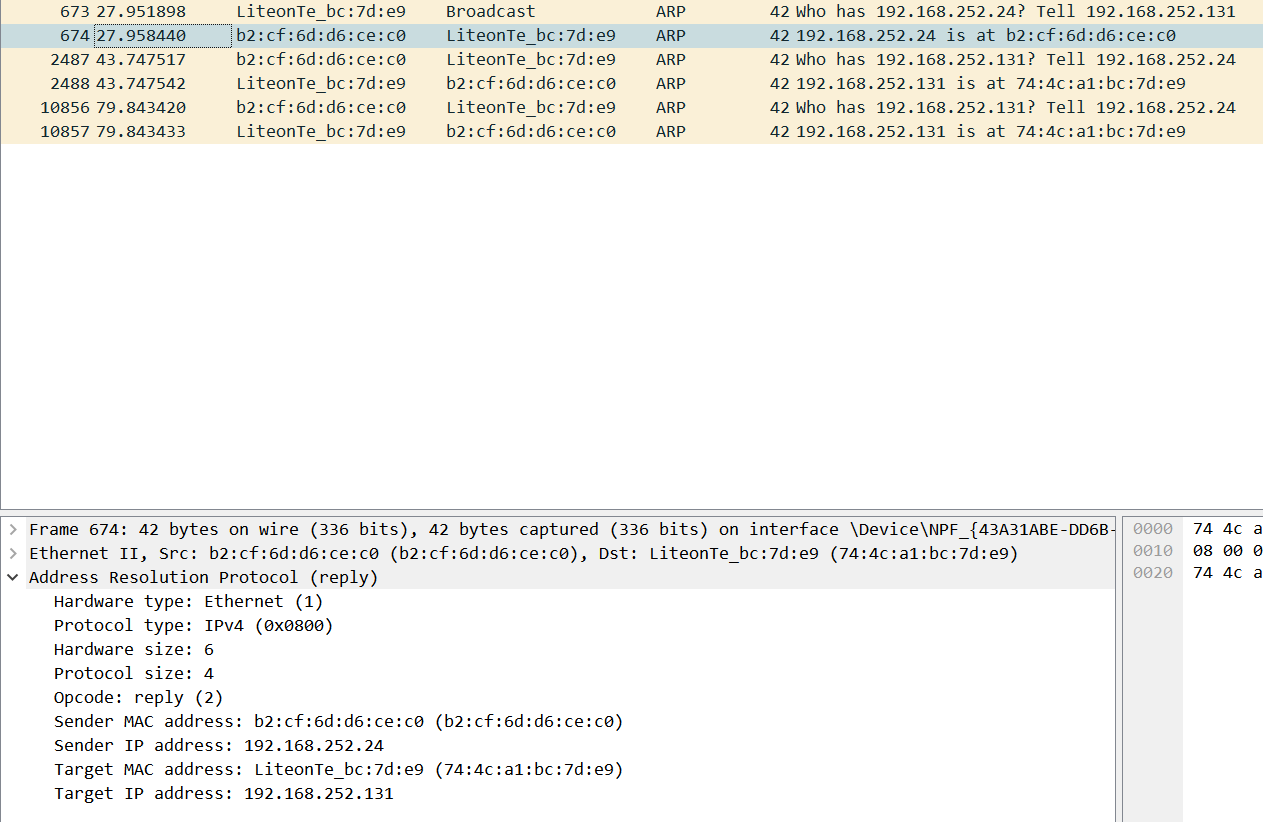
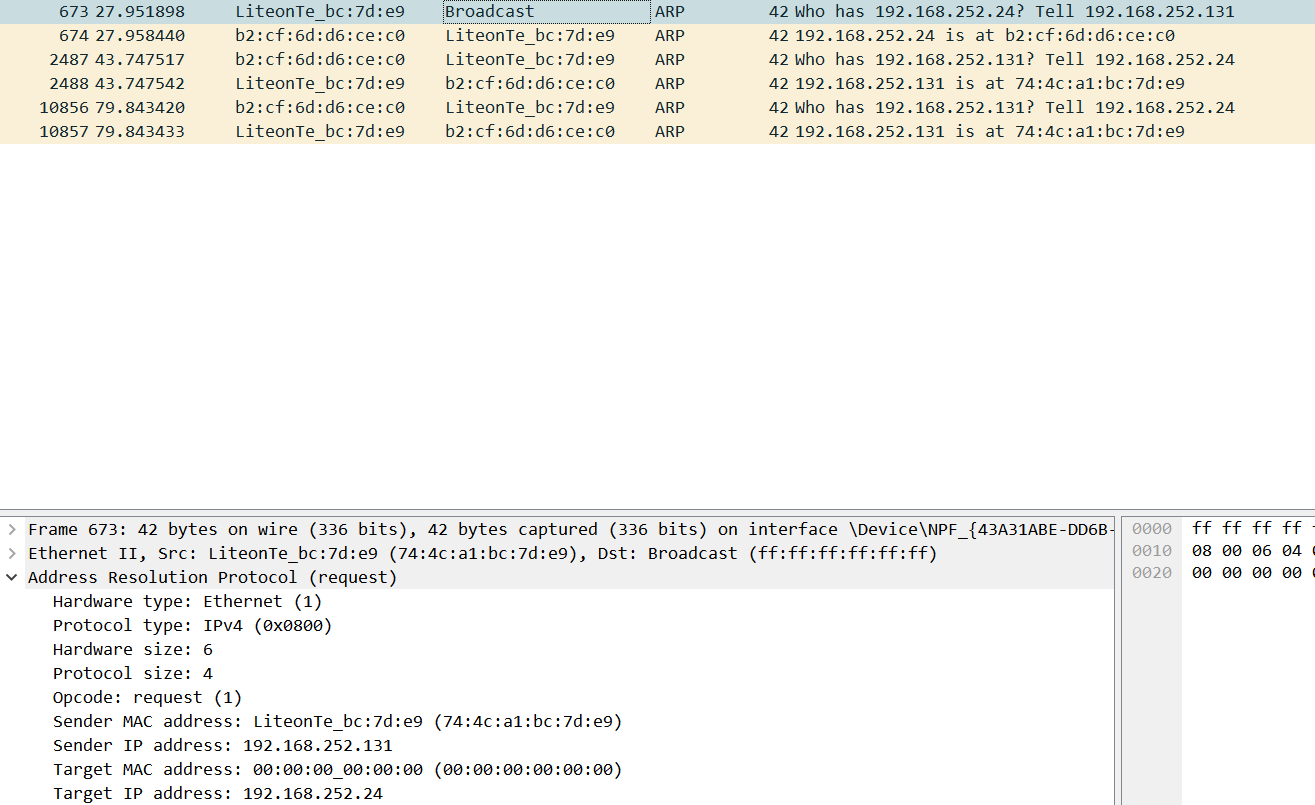
● зайти на Интернет-сайт, заданный по варианту



1. Какие МАС-адреса присутствуют в захваченных пакетах ARP-

протокола? Что означают эти адреса? Какие устройства они

идентифицируют?



74:4c:a1:bc:7d:e9 - адрес отправителя (ip =192.168.252.131 )

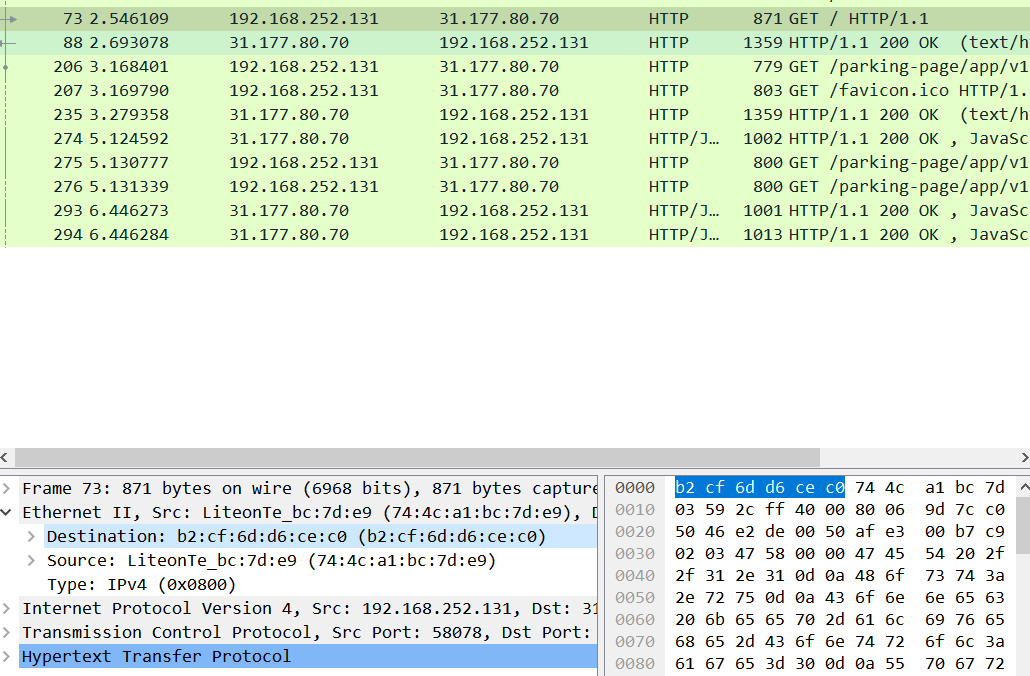
b2:cf:6d:d6:ce:c0 - адрес получаетеля (ip=192.168.252.24)

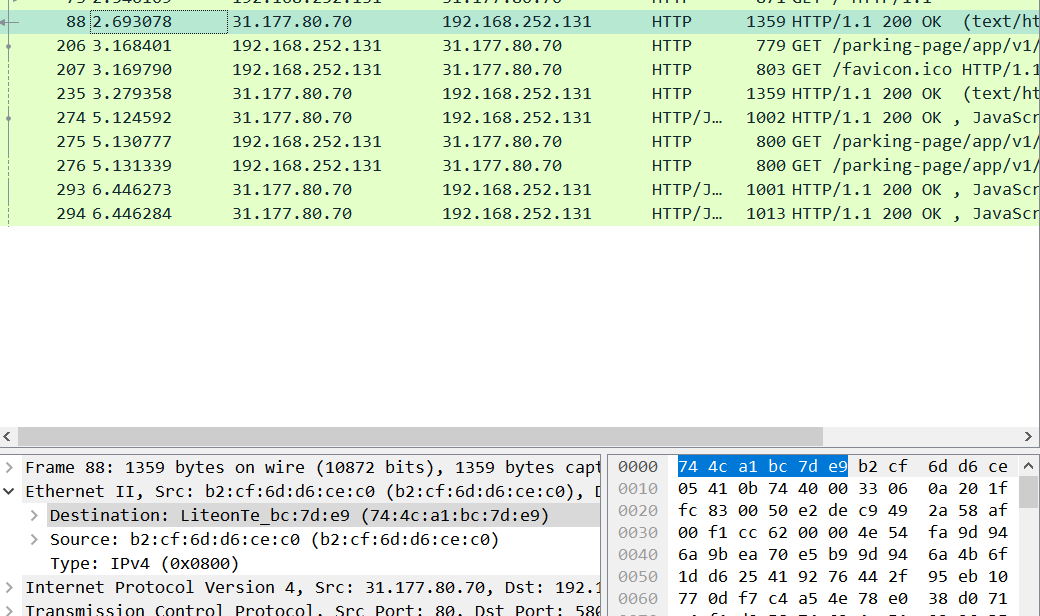
00:00:00:00:00:00 - boardcast

2. Какие МАС-адреса присутствуют в захваченных HTTP-пакетах и что означают эти адреса? Что означают эти адреса? Какие

устройства они идентифицируют?

Такие же адресы. Они служая для различения отправителя и получателя.





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

Чтобы получатель мог добавить информацию об отправителе в свою ARP-таблицу.

**Этап 6**

Необходимо отследить и проанализировать трафик протокола DNS, сгенерированный в результате выполнения следующих действий:

1. Настроить Wireshark-фильтр: “ip.addr == ваш\_IP\_адрес”.

2. Запустить в командной строке команду “nslookup

адрес\_сайта\_по\_варианту”.

3. Дождаться отправки трёх DNS-запросов и трёх DNS-ответов (в

работе нужно использовать только последние из них, т.к. первые два

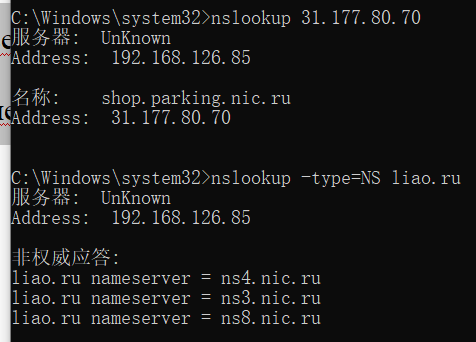
набора запросов/ответов специфичны для nslookup и не

генерируются другими сетевыми приложениями).

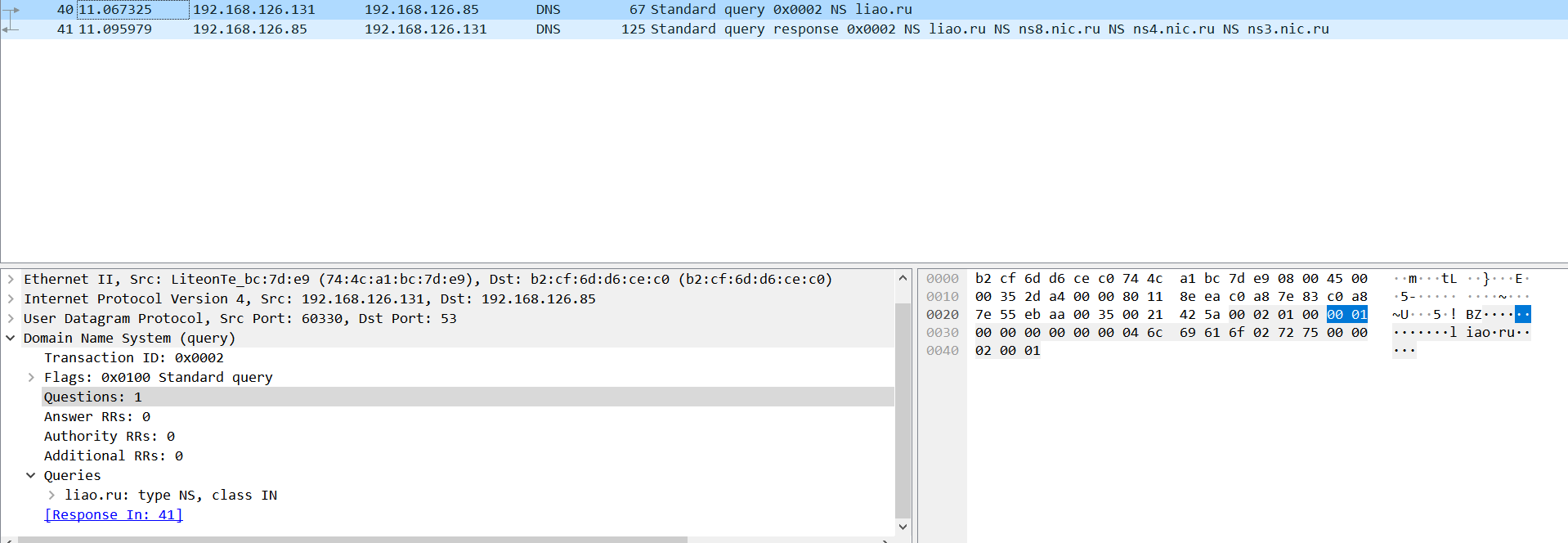
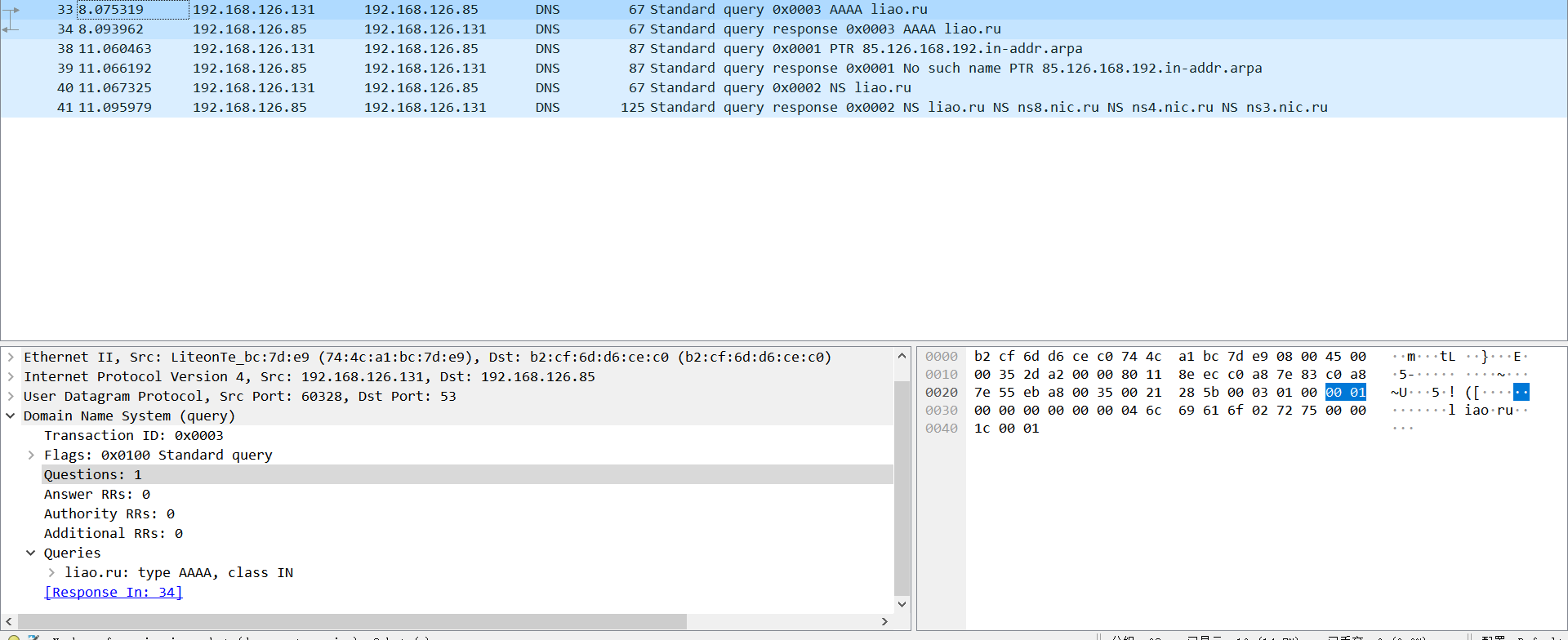
4. Повторить предыдущие два шага, используя команду:

“nslookup -type=NS имя\_сайта\_по\_варианту”.

По результатам анализа собранной трассы, ответьте на следующие



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

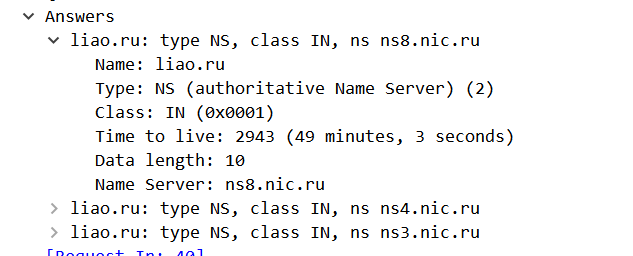
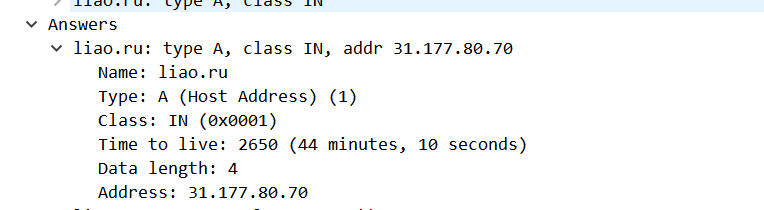


Типы dns записы разны.

Первый связан с IPv4-адресом хоста.

Вторый запрашивает имя домена севера.

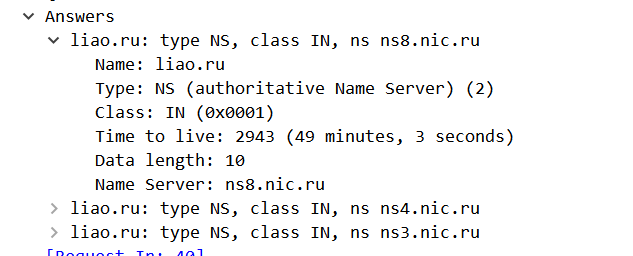
2. Что содержится в поле «Answers» DNS-ответа?



A -IPv4-адрес

NS -список authoritative Name Server.

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

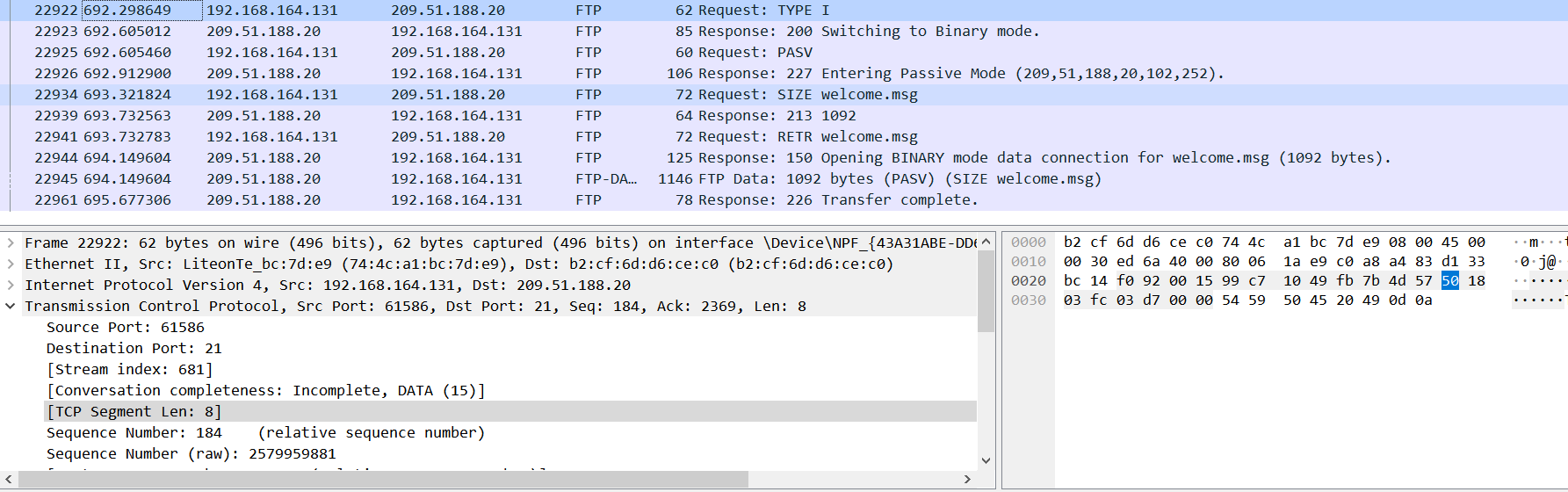
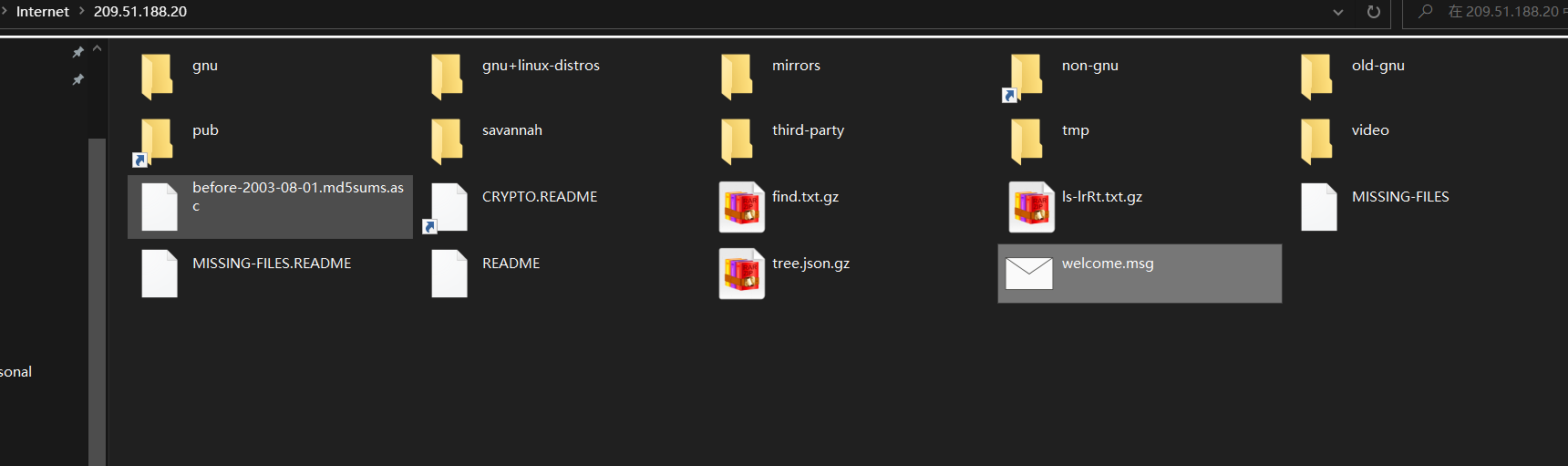


**Этап 7**

Необходимо отследить и проанализировать 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. В адресной строке путь к скачиваемому файлу должен начинаться с «ftp://». Адрес сайта нужно выбрать, руководствуясь правилами, указанными в п. 3.3 задания №3.



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

1092

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

61586->21

3. Чем отличаются пакеты FTP от FTP-DATA?

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

**Этап 8**

Необходимо отследить и проанализировать трафик протокола DHCP, сгенерированный в результате выполнения следующих действий:

1. Убедиться, что для назначения IP-адреса на компьютере был

использован DHCP и что компьютеру был назначен IP-адрес.

2. Настроить Wireshark-фильтр «bootp» (во время защиты УИР следует объяснить, почему именно такой фильтр используется для анализа DHCP-трафика).

3. Сбросить текущий IP-адрес, выданный накануне перед этим DHCP-сервером, с помощью команды: “ipconfig /release“.

4. Запросить новый IP-адрес с помощью команды: “ipconfig /renew“.

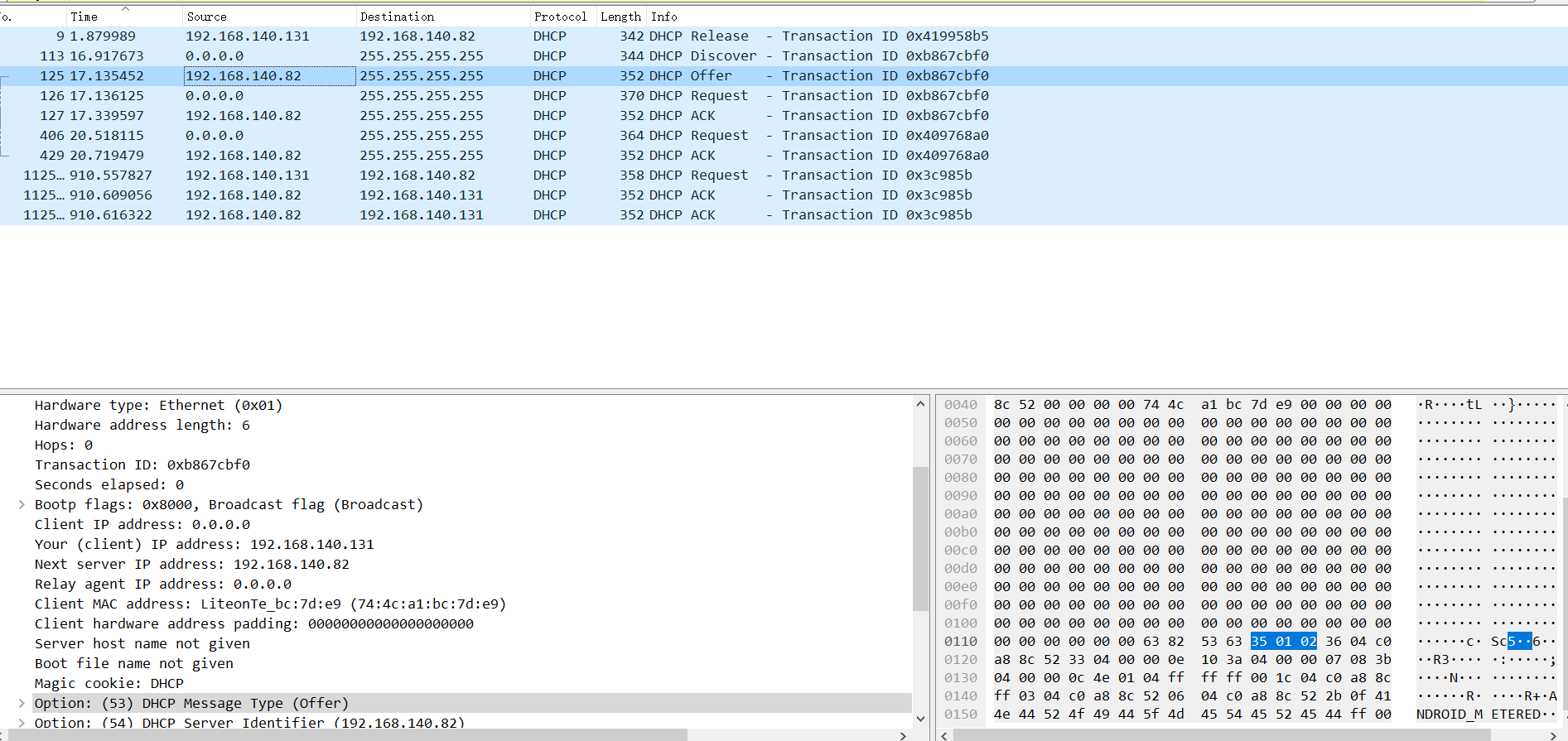
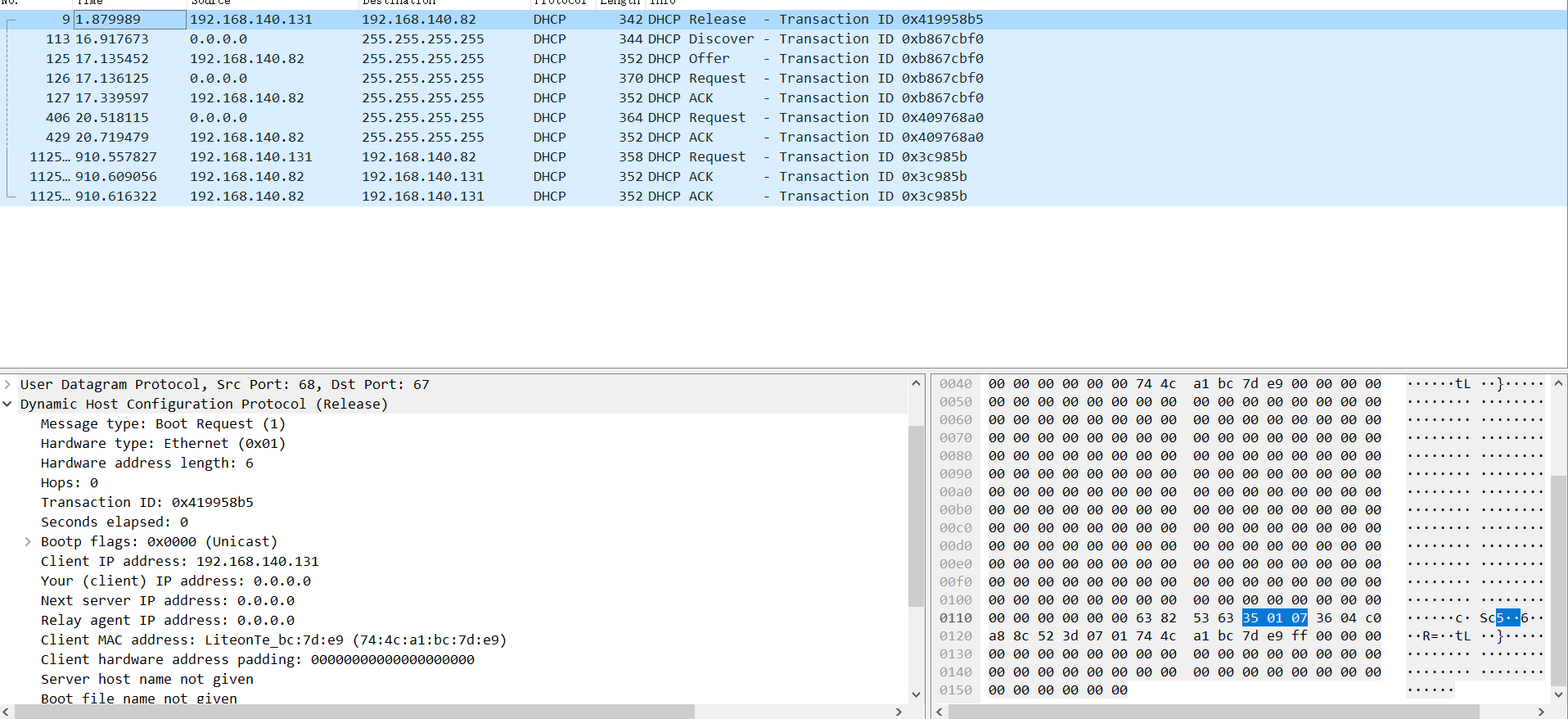
5. Повторить п.3 и п.4. Нарисуйте временн**у**ю диаграмму, иллюстрирующую последовательность обмена первыми четырьмя DHCP-пакетами Discover/Offer/Request/ACK. Укажите для каждого пакета номера портовисточника и назначения.

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

Discorver: Когда DHCP-клиент запрашивает адрес, он не знает местонахождение DHCP-сервера, поэтому DHCP-клиент отправляет сообщение в локальной сети.

Request: Клиент принимает предлагаемый адрес и сообщает северу об этом.

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



Когда Discover отправляется, клиент не знает где север поэтому он просто отправляет на широковещательные адреса и не поставит MAC ардес получателя. Но он знает свой MAC-адрес поэтому в запросе есть Client MAC address. Поскольку пока у клиента нет ip и он именно хочет запрашивать его, ip клиента является 0.0.0.0.

А при отправке Offer или ACK, адреса источника

соответствуют адресам DHCP-сервера, адреса назначения широковещательные.

1. Каков IP-адрес DHCP-сервера?

192.168.140.82

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

Будет показать все типы пакетов.

**Этап 9**

Необходимо отследить и проанализировать трафик Skype (или любой другой аналогичной по функциональности программы), сгенерированный в результате выполнения следующих действий:

● отправить текстовое сообщение и получить ответ;

● осуществить короткий сеанс аудио-общения;

● осуществить короткий сеанс видео-общения.

Для упрощения анализа передачи различных видов трафика Скайпом (тест, аудио, видео) можно независимо собрать трассы трафика для каждого из трёх перечисленных пунктов, останавливая и возобновляя захват трафика так, чтобы получить три отдельных файла.

1. Чем различаются пакета разных видов Skype-трафика (текст, аудио, видео)?

2. Какой Wireshark-фильтр следует использовать для независимой идентификации Skype-трафика разных видов (текст, аудио, видео)?

**Вывод**