 Университет ИТМО

Мегафакультет компьютерных технологий и управления

Факультет программной инженерии и компьютерной техники

Лаюораторная работа №5

Анализ трафика компьютерных сетей утилитой Wireshark

Группа:

Р33101

Студент:

Хуан Сыюань

Преподаватель:

Тропченко Андрей Александрович

### Цель работы

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

### Задание

1. Запустить Wireshark. В появившемся окне выбрать интерфейс для которого необходимо осуществлять анализ проходящих через него пакетов. После выбора адаптера, нужно запустить процесс захвата трафика (кнопка Start).
2. Инициировать процесс передачи трафика по сети
3. Установить значение “Фильтра”, чтобы из всего множества перехватываемых пакетов Wireshark отобразил только те, которые имеют отношение к выполняемому заданию.
4. Дождаться появления данных в списке захваченных пакетов и убедиться, что количество пакетов достаточно для выполнения задания.
5. Сохранить захваченный трафик в файл-трассу (pcap).
6. Описать в отчёте структуру наблюдаемых PDU (т.е. протокольных блоков данных: кадров, пакетов, сегментов) как для запросов, так и ответов.
7. Написать в отчёте ответы на вопросы задания
8. Поместить в отчёт скриншоты окна Wireshark, иллюстрирующие ответы из вышеуказанных п.6 и п.7.

URL - Адрес сайта, в название которого лексически входит фамилия студента: <http://huang.ru/>

Ip = 92.53.96.250

### Выполнение работы

#### 1. Анализ трафика утилиты ping

Необходимо отследить и проанализировать трафик, создаваемый утилитой ping, запустив её следующим образом из командной строки: “ping -l размер\_пакета адрес\_сайта\_по\_варианту”. 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.

Ping -s 2000 92.53.96.250

Wireshark:

ip

ip.addr == 92.53.96.250

IP/ICMP packet structure:Изображение выглядит как стол

Автоматически созданное описание

1. Имеет ли место фрагментация исходного пакета, какое поле на это указывает? Is fragmentation of the original packet taking place, which field indicates this?

Yes, there is fragmentation for packets larger than 1480 bytes. You can see the number of fragments in the more fragments field, if it is set to 1, then this is an intermediate fragment; fragments are also marked in black, and the final one with the flag more fragments = 0 is the last one.

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, электроника, компьютер

Автоматически созданное описание

1. Какая информация указывает, является ли фрагмент пакета последним или промежуточным? What information indicates whether a packet fragment is the last or intermediate?

More fragments field: 1 - intermediate, 0 - last

Изображение выглядит как текст, электроника, компьютер, снимок экрана

Автоматически созданное описание

1. Чему равно количество фрагментов при передаче ping-пакетов? What is the number of fragments when transmitting ping packets?

Number of fragments = ceil( Message length (bytes) / 1480 bytes (fragment) )

1. Построить график, в котором на оси абсцисс находится размер\_пакета, а по оси ординат – количество фрагментов, на которое был разделён каждый ping-пакет. Construct a graph in which the abscissa axis is the packet\_size, and the ordinate axis is the number of fragments into which each ping packet was divided.



1. Как изменить поле TTL с помощью утилиты ping? How can I change the TTL field using the ping utility?

Use key -i <TTL> (time to live)

1. Что содержится в поле данных ping-пакета? What is in the data field of a ping packet?

ASCII characters, the field can also contain a timestamp or batch number.

**2. Анализ трафика утилиты tracert (traceroute)**

You need to trace and analyze the traffic generated by the tracert utility (or traceroute on Linux) by running it like this from the command line:

“tracert -d site\_url\_of\_variant”

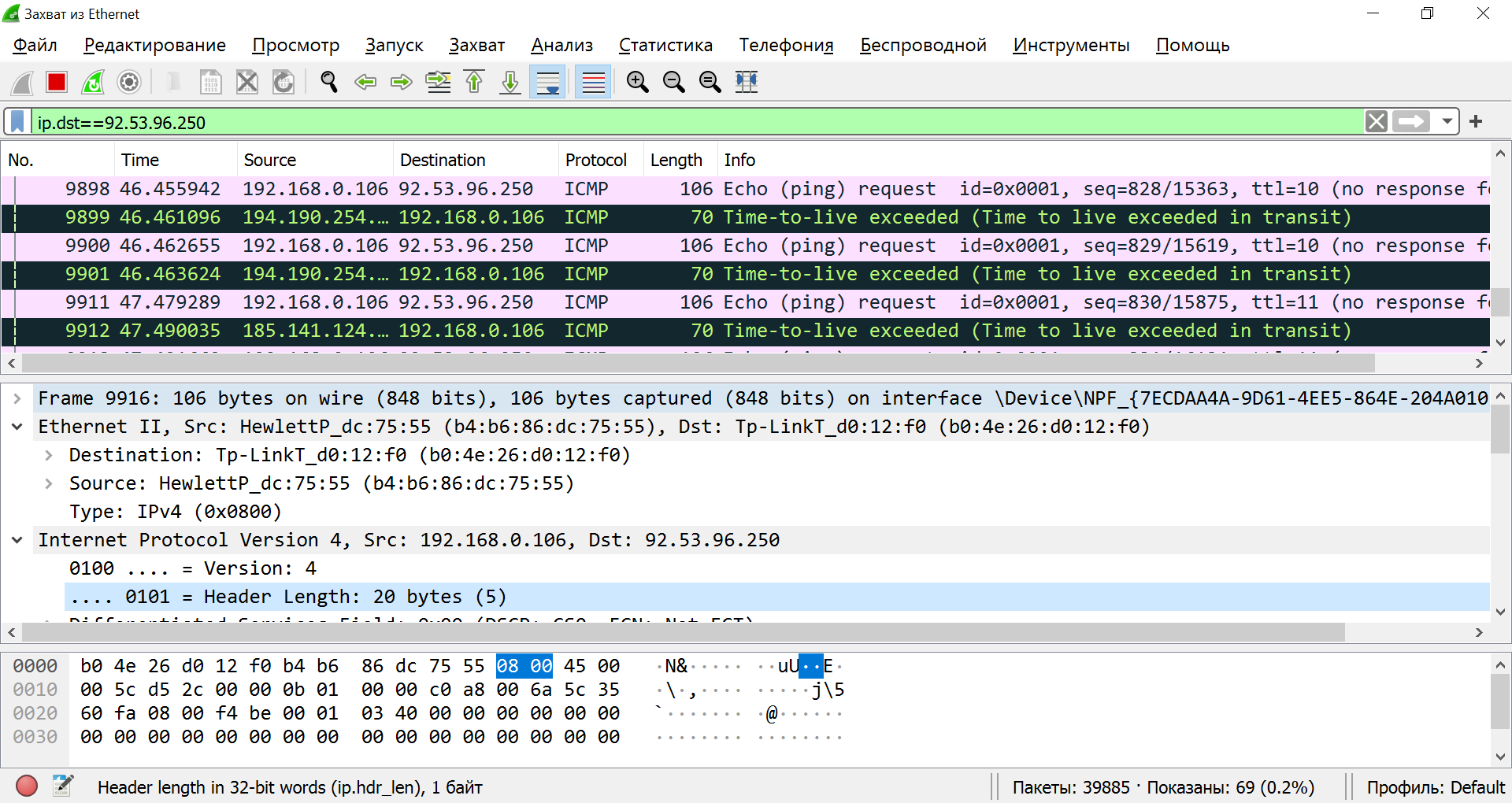
Based on the results of the analysis of the collected trace, answer the following questions.

Изображение выглядит как текст

Автоматически созданное описание

1. Сколько байт содержится в заголовке IP? Сколько байт содержится в поле данных? How many bytes are in the IP header? How many bytes are in the data field?

IP header - 20 bytes

Data field - 64 bytes

Изображение выглядит как стол

Автоматически созданное описание

1. Как и почему изменяется поле TTL в следующих друг за другом ICMP-пакетах tracert? How and why does the TTL field change in successive ICMP tracert packets?

At each verification step, the TTL is incremented by one so that the IP addresses of each host in the transmission chain can be retrieved sequentially.

Each intermediate node subtracts one from the value of the TTL field so that the number of nodes passed can be tracked.

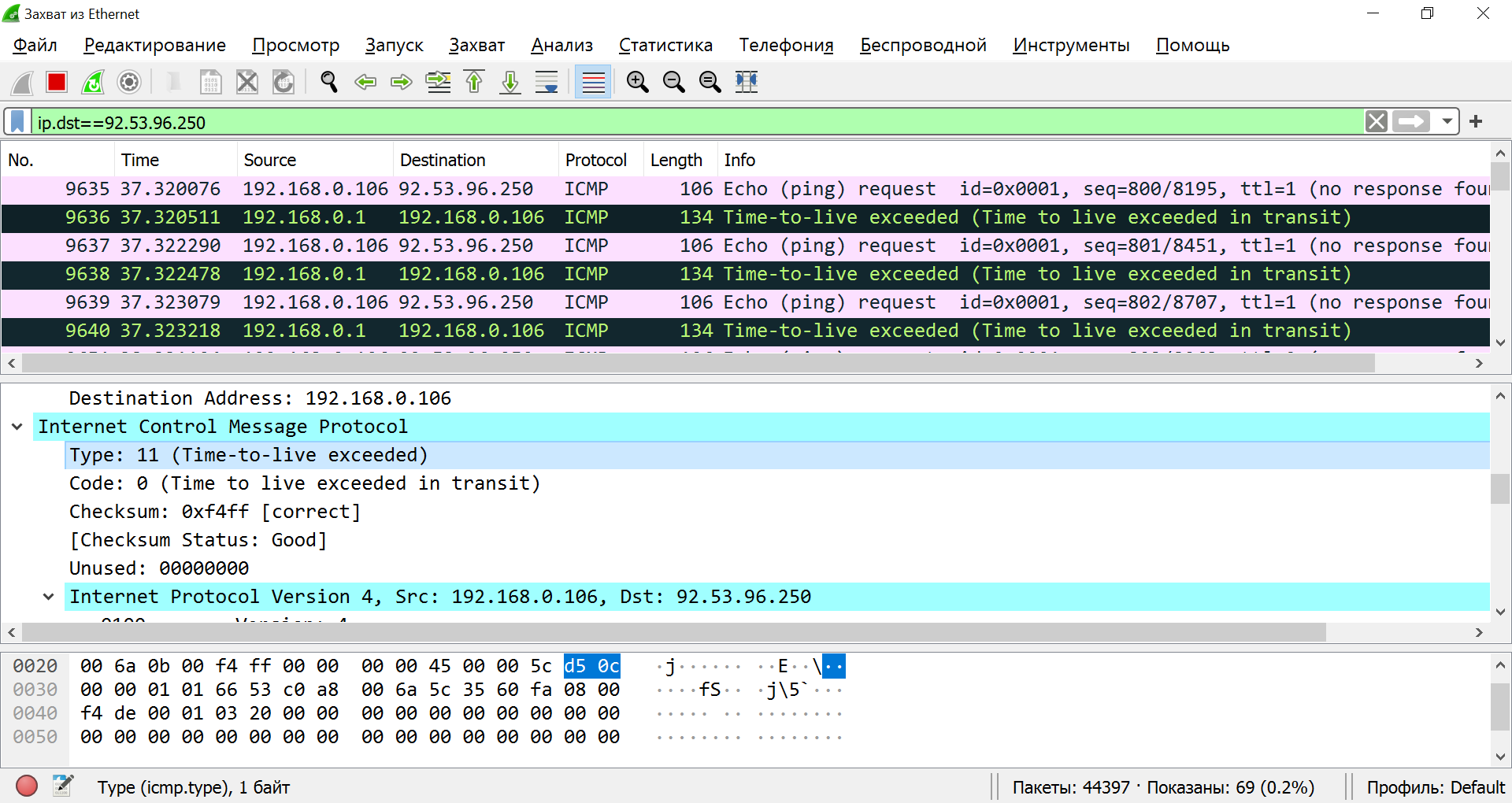
When TTL = 0 (or the packet has reached the destination), the transmission of the packet is terminated.

1. Чем отличаются ICMP-пакеты, генерируемые утилитой tracert, от ICMP-пакетов, генерируемых утилитой ping? What is the difference between ICMP packets generated by the tracert utility and ICMP packets generated by the ping utility?

Different type of messages: ping has 8, tracert has 11. Tracert also sets a different TTL for each verification step.

Изображение выглядит как стол

Автоматически созданное описание



1. Чем отличаются полученные пакеты «ICMP reply» от «ICMP error» и зачем нужны оба этих типа ответов? What is the difference between received “ICMP reply” packets and “ICMP error” packets and why are both of these types of responses needed?

Error is sent by an intermediate host when the TTL becomes 0.

Reply is sent by an end node when a packet successfully reaches it.

Изображение выглядит как текст

Автоматически созданное описание

1. Что изменится в работе tracert, если убрать ключ “-d”? Какой дополнительный трафик при этом будет генерироваться? What will change in the work of tracert if you remove the “-d” switch? What additional traffic will be generated?

An attempt will be made to determine the hostname from its IP address, i.e. additional queries to the DNS server will be made.

**3. Анализ HTTP-трафика**

Необходимо отследить и проанализировать HTTP-трафик, создаваемый браузером при 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».

По результатам анализа собранной трассы покажите, каким образом протокол HTTP передавал содержимое страницы при первичном посещении страницы и при вторичном запросе-обновлении от браузера (т.е. при различных видах GET-запросов).

TCP datagram structure:Изображение выглядит как стол

Автоматически созданное описание

HTTP message structure:

1. Start string - <Method> <URI> HTTP/<Version>

2. Headers - a set of parameters and their values

3. Message body - optional data

First GET request - new data - get site html

Изображение выглядит как текст, электроника, снимок экрана, компьютер

Автоматически созданное описание

Second GET request - asking if the data has changedИзображение выглядит как текст

Автоматически созданное описание

When re-requesting resources (mainly js files), the returned response code is 304. Since the state of the resources has not changed, no download occurs and the data is taken from the browser cache.

**4. Анализ DNS-трафика**

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.

По результатам анализа собранной трассы, ответьте на следующие вопросы.

DNS packet structure:Изображение выглядит как стол

Автоматически созданное описание

1. Почему адрес, на который отправлен DNS-запрос, не совпадает с адресом посещаемого сайта? 1. Why doesn't the address to which the DNS query was sent to match the address of the visited site?

The request is not sent to the site, but to a special DNS server.

Изображение выглядит как текст

Автоматически созданное описание

1. Какие бывают типы DNS-запросов?

Рекурсивный - DNS-серверу посылается доменное имя, для которого он должен вернуть IP-адрес. DNS-сервер может обратиться к другим серверам для выполнения запроса

Итеративный - при получении такого запроса DNS-сервер не опрашивает другие сервера, а возвращает либо IP-адрес, либо имя другого DNS-сервера, который может знать ответ

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

Если адрес, на котором хранится изображение отличается от адреса сайта.

**5. Анализ ARP-трафика**

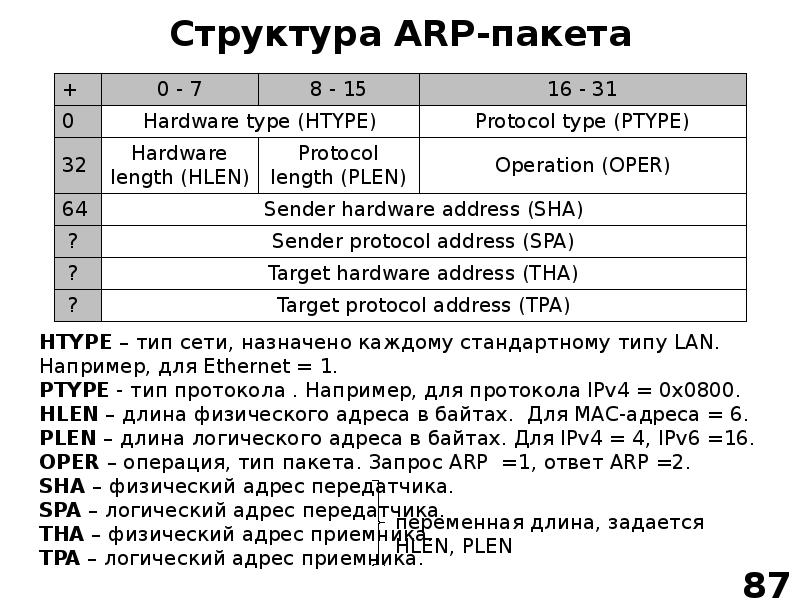
Необходимо отследить и проанализировать трафик протокола ARP, сгенерированный в результате выполнения следующих действий:

* очистить ARP-таблицу командой “netsh interface ip delete arpcache”;
* очистить кэш браузера;
* зайти на Интернет-сайт, заданный по варианту.

По результатам анализа собранной трассы, ответьте на следующие

вопросы.

ARP packet structure:



1. Какие МАС-адреса присутствуют в захваченных пакетах ARP-протокола? Что означают эти адреса? Какие устройства они идентифицируют? What MAC addresses are present in the captured ARP packets? What do these addresses mean? What devices do they identify?

B0:4e:26:d0:12:f0 - sender address (router) (ip = 192.168.0.1)

B4:b6:86:dc:75:55 - address of the recipient's device (the computer from which the request to the site is made) (ip = 192.168.0.106)

00:00:00:00:00:00 - broadcast address

Изображение выглядит как текст

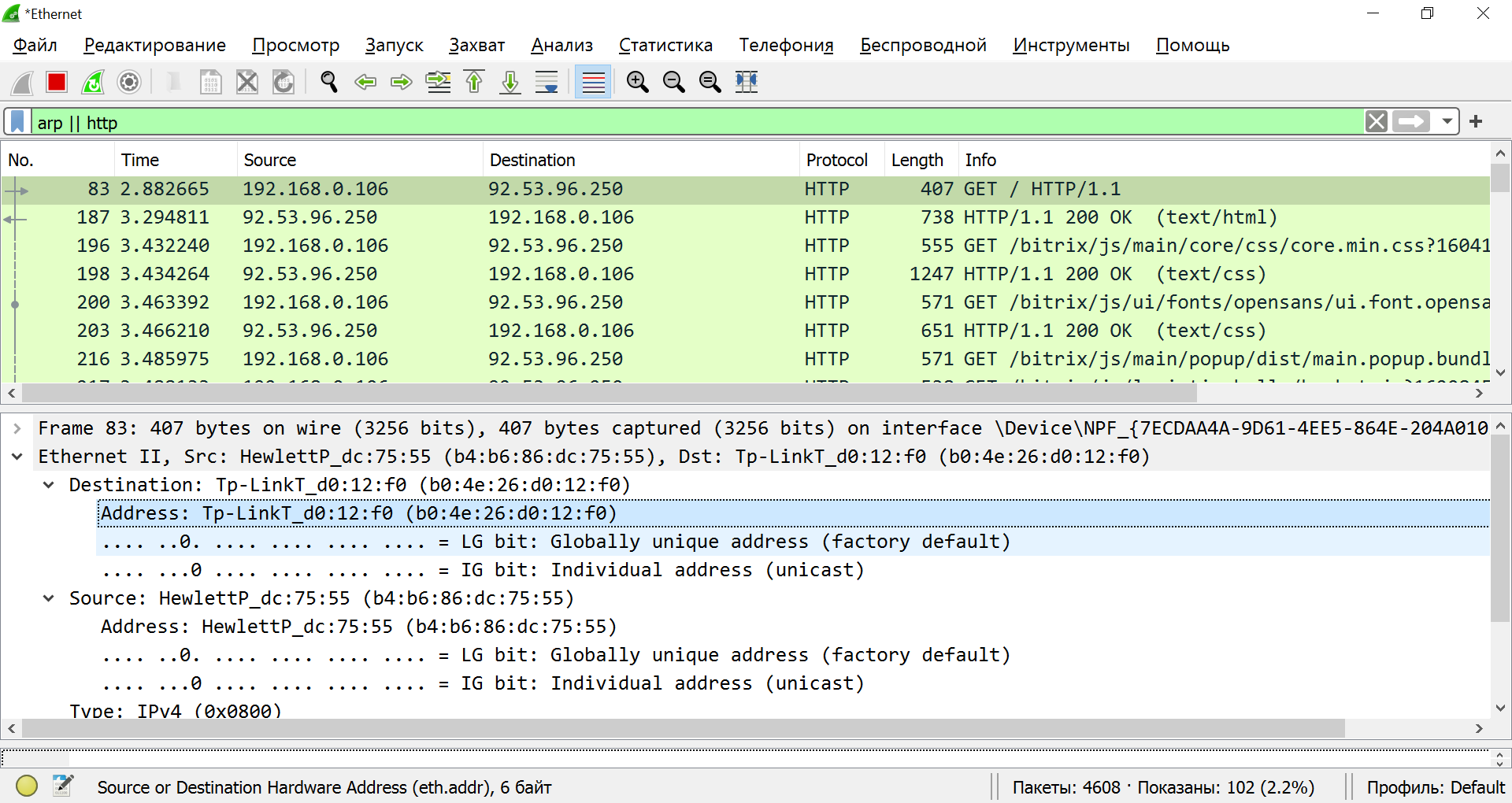
Автоматически созданное описание

Изображение выглядит как стол

Автоматически созданное описание

1. Какие МАС-адреса присутствуют в захваченных HTTP-пакетах и что означают эти адреса? Какие устройства они идентифицируют? What MAC addresses are present in the captured HTTP packets and what do these addresses mean? What devices do they identify?

There is the MAC address of the device from which the http request is made and the MAC address of the router



1. Для чего ARP-запрос содержит IP-адрес источника? Why does an ARP request contain the source IP address?

So that the receiving host can add information about the sending host to its ARP table.

**6. Анализ трафика утилиты nslookup**

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”.

nslookup 92.53.96.250

Изображение выглядит как текст

Автоматически созданное описание

nslookup -type-NS 92.53.96.250

Изображение выглядит как текст

Автоматически созданное описание

По результатам анализа собранной трассы, ответьте на следующие

вопросы.

1. Чем различается трасса трафика в п.2 и п.4, указанных выше? What is the difference between the traffic route in paragraph 2 and paragraph 4 above?

When launched in step 2, the utility looks for the IP address of the host (record type A (IPv4) or AAAA (IPv6)).

When launched in step 4, the utility searches for the Name Server for the requested host.

Изображение выглядит как стол

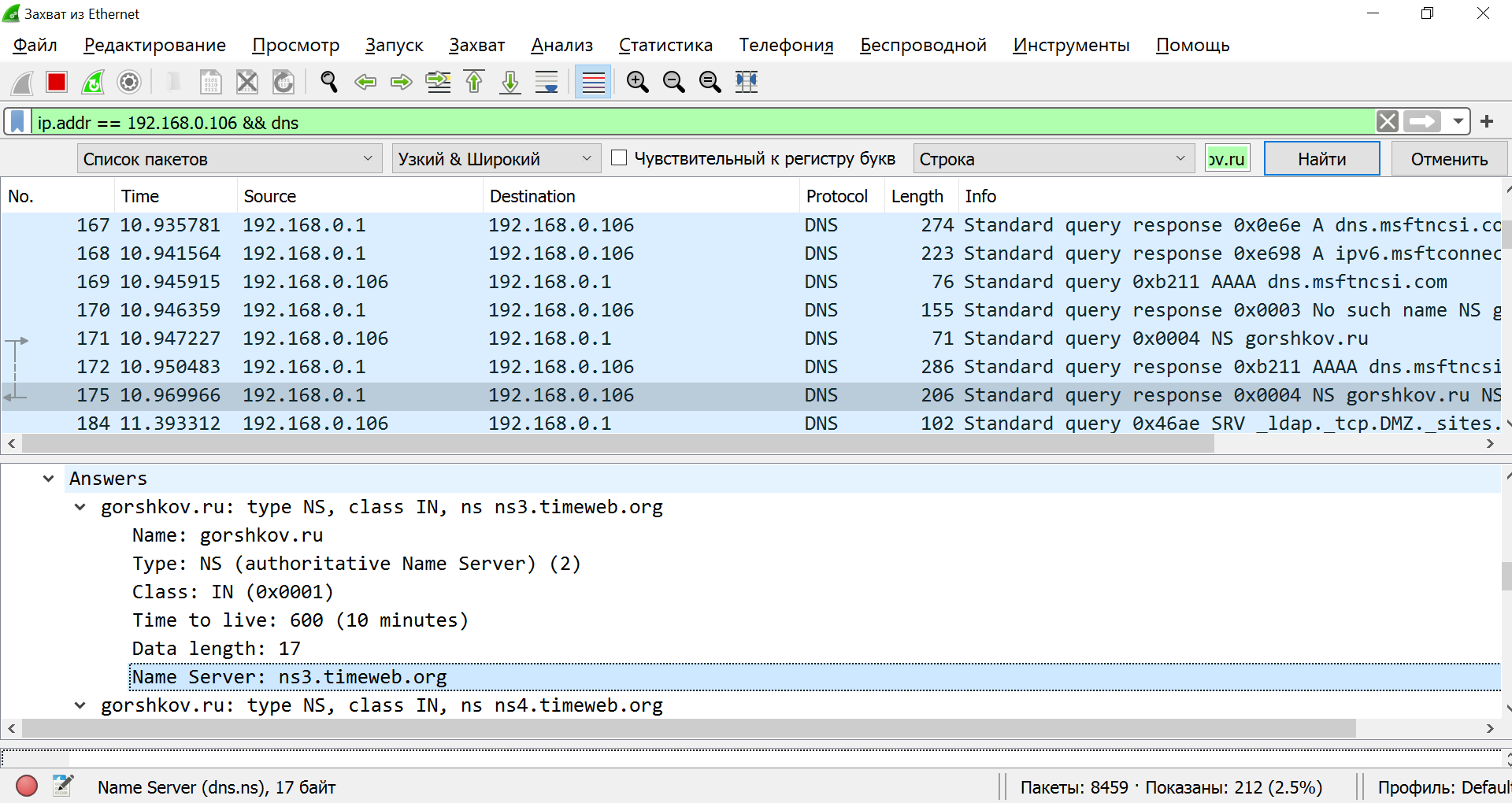
Автоматически созданное описание

1. Что содержится в поле «Answers» DNS-ответа? What is contained in the "Answers" field of the DNS response?

Data of requested DNS record type: for A - IPv4 address, for NS - authoritative Name Server list.

Изображение выглядит как стол

Автоматически созданное описание



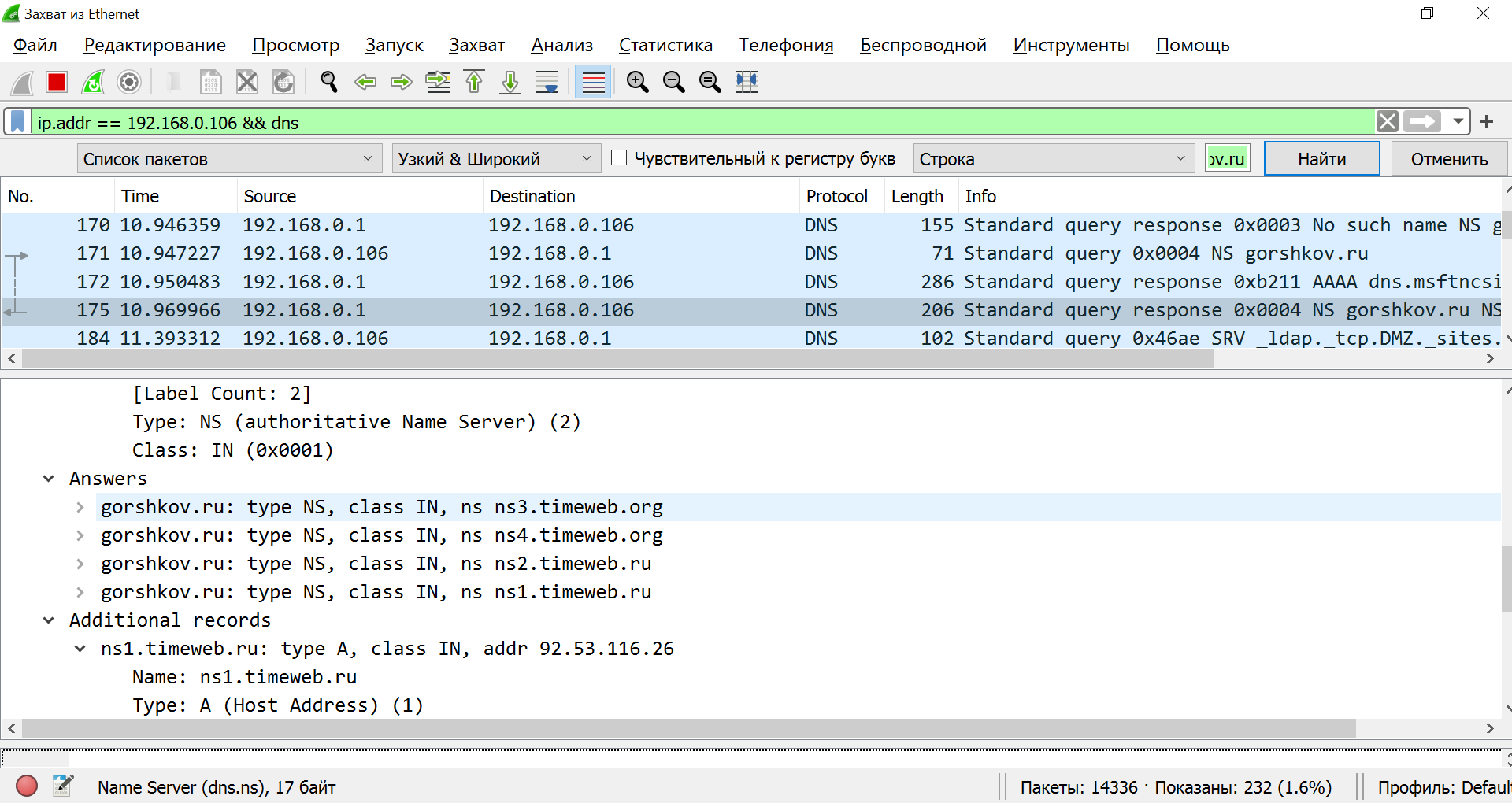
1. Каковы имена серверов, возвращающих авторитативный (authoritative) отклик? 3. What are the names of servers returning an authoritative response?

gorshkov.ru nameserver = ns3.timeweb.org

gorshkov.ru nameserver = ns4.timeweb.org

gorshkov.ru nameserver = ns2.timeweb.ru

gorshkov.ru nameserver = ns1.timeweb.ru



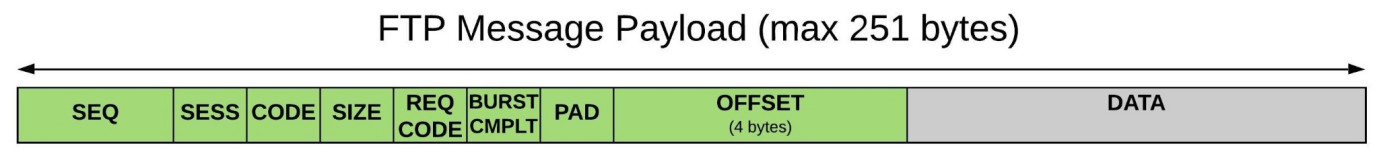
**7. Анализ FTP-трафика**

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.

По результатам анализа собранной трассы, ответьте на следующие вопросы.

Структура FTP-сообщения:



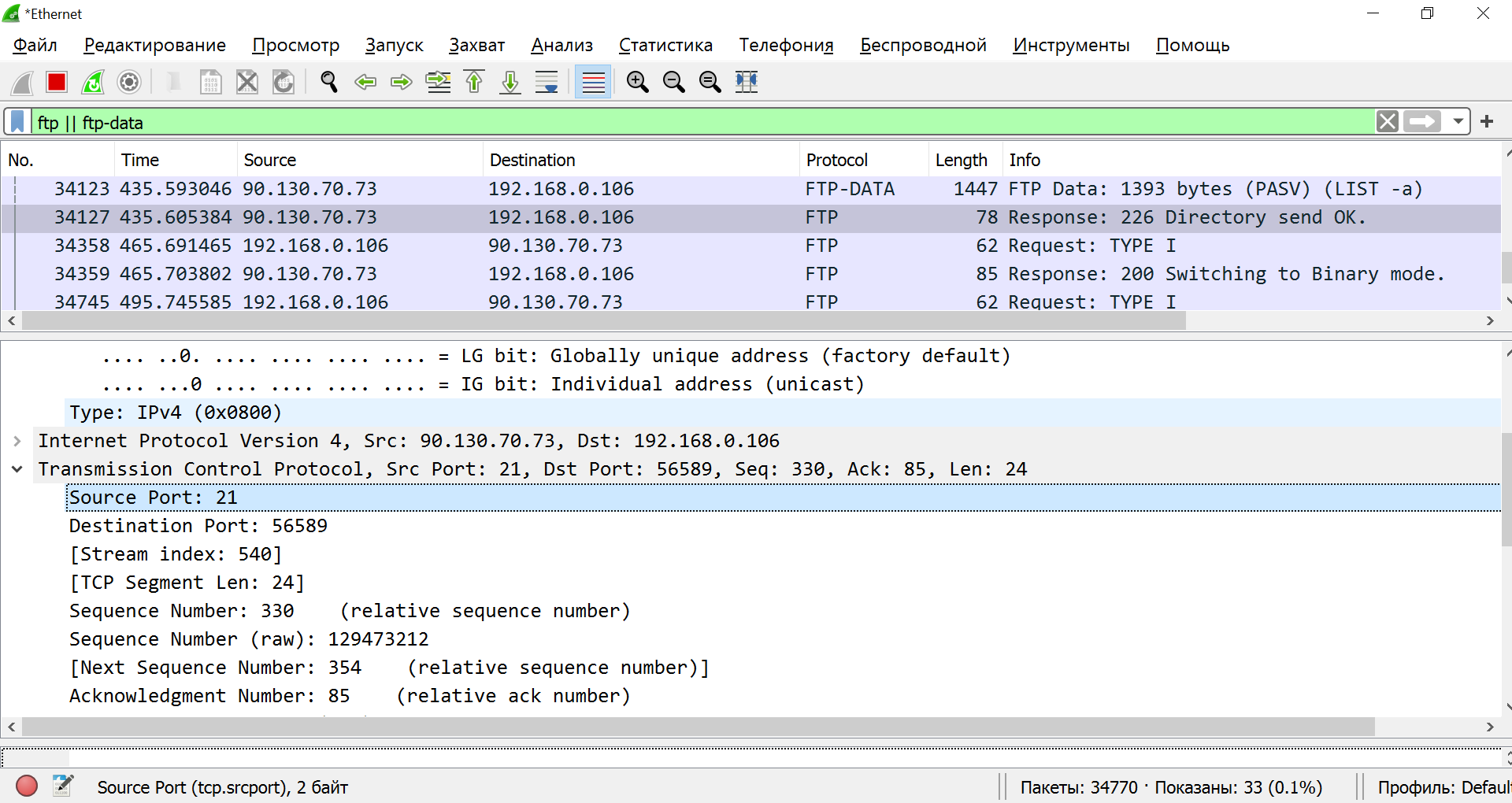
1. Сколько байт данных содержится в пакете FTP-DATA? How many bytes of data are in an FTP-DATA packet?

1460 byte

Изображение выглядит как стол

Автоматически созданное описание

1. Как выбирается порт транспортного уровня, который используется для передачи FTP-пакетов? How is the transport layer port selected, which is used to transfer FTP packets?

Port 21 is used for control flow on the server. Port 20 is used for data transfer if the transfer is in active mode, or from any client port to any server port in passive mode. Изображение выглядит как стол

Автоматически созданное описание

1. Чем отличаются пакеты FTP от FTP-DATA? 3. What is the difference between FTP packets and FTP-DATA?

FTP packets transmit commands and server responses to them. These packets are small and contain no data. FTP-DATA-packets contain the transferred data, they are much larger.

**Вывод**

I got acquainted with the Wireshark application, created for traffic analysis, learned how to write filters for requests, figured out what packets consist of, studied their structure, and analyzed it by answering questions.