Санкт-Петербургский национальный исследовательский УНИВЕРСИТЕТ информационных технологий, механики и оптики

**Факультет программной инженерии и компьютерной техники**

**ЛАБОРАТОРНАЯ РАБОТА № 3**

**ПО ДИСЦИПЛИНЕ «СЕТИ ЭВМ И ТЕЛЕКОММУНИКАЦИИ»**

Выполнили: Нгу Фыонг Ань

Группа: P3310

Преподаватель: Шинкарук Д.Н.

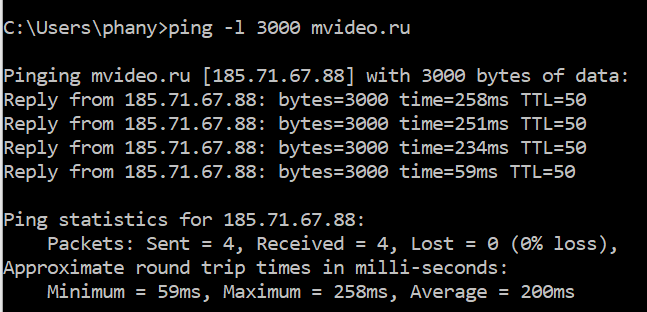
Санкт-Петербург

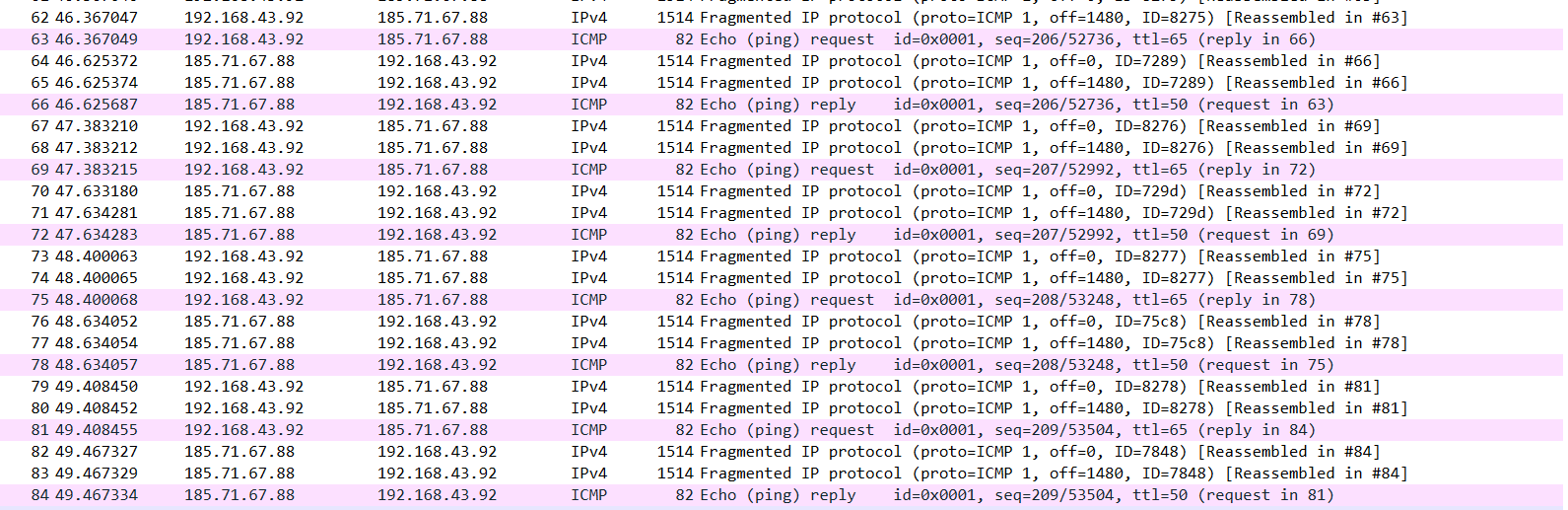
2020

**Цель:**

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

1. **Анализ трафика утилиты ping**

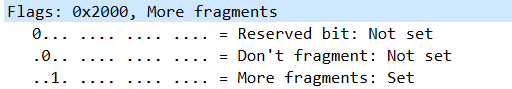




|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Размер пакета | 100 | 500 | 1000 | 3000 | 5000 | 7000 |
| Фрагмент ация | Нет | Нет | Нет | Да | Да | Да |
| Кол-во фрагментов | 1 | 1 | 1 | 3 | 4 | 5 |

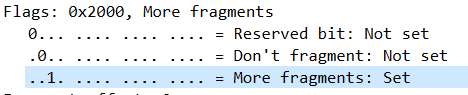
1. **Имеет ли место фрагментация исходного пакета, какое поле на это указывает?**

Имеет место фрагментация исходного пакета. Поле флага указывает на это.

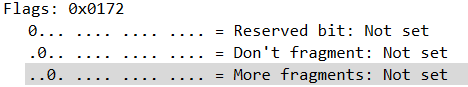


1. **Какая информация указывает, является ли фрагмент пакета последним или промежуточным?**

Промежуточный пакет:



Последний пакет:

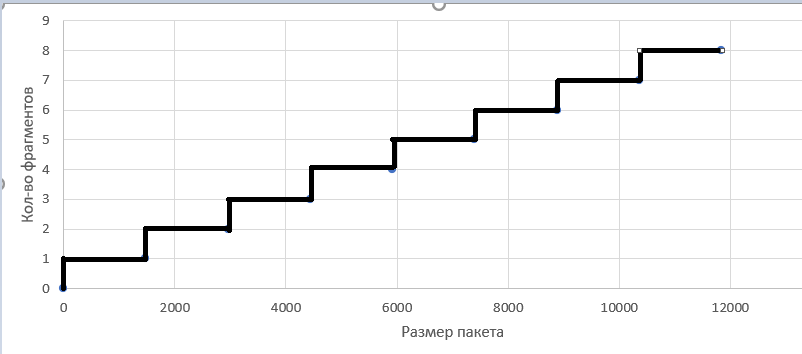


1. **Чему равно количество фрагментов при передаче ping-пакетов?**

Максимальный размер фрагмента в нашем случае равен 1500 байт, куда входит

* IPv4 заголовок (20 байт).
* Остальной объем занимает ICMP пакет. Который включает в себя заголовок (8 байт (Header + Header data) и payload.
* количество фрагментов ping пакета: N= (packet-size + 8) / 1480.

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



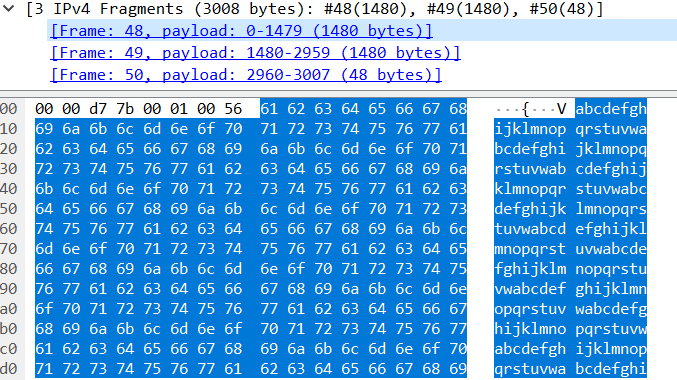
1. **Как изменить поле TTL с помощью утилиты ping?**

При проходе через каждый узел значение TTL уменьшается на единицу. Если поле TTL пакета достигло нуля марштрутизатор обнаруживающий его отбрасывает пакет и отправляет сообщение ICMP обратно на исходный узел.

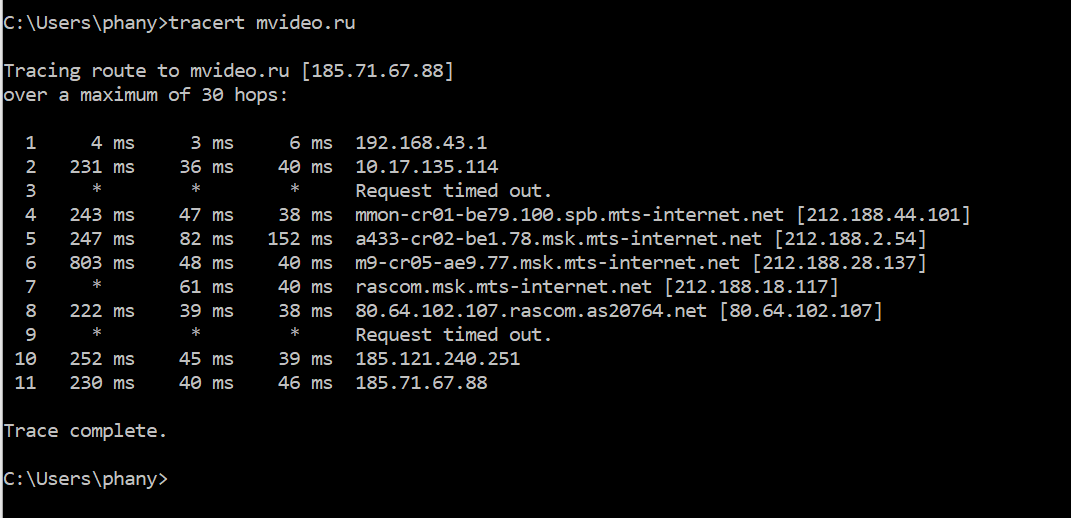
1. **Что содержится в поле данных ping-пакета?**

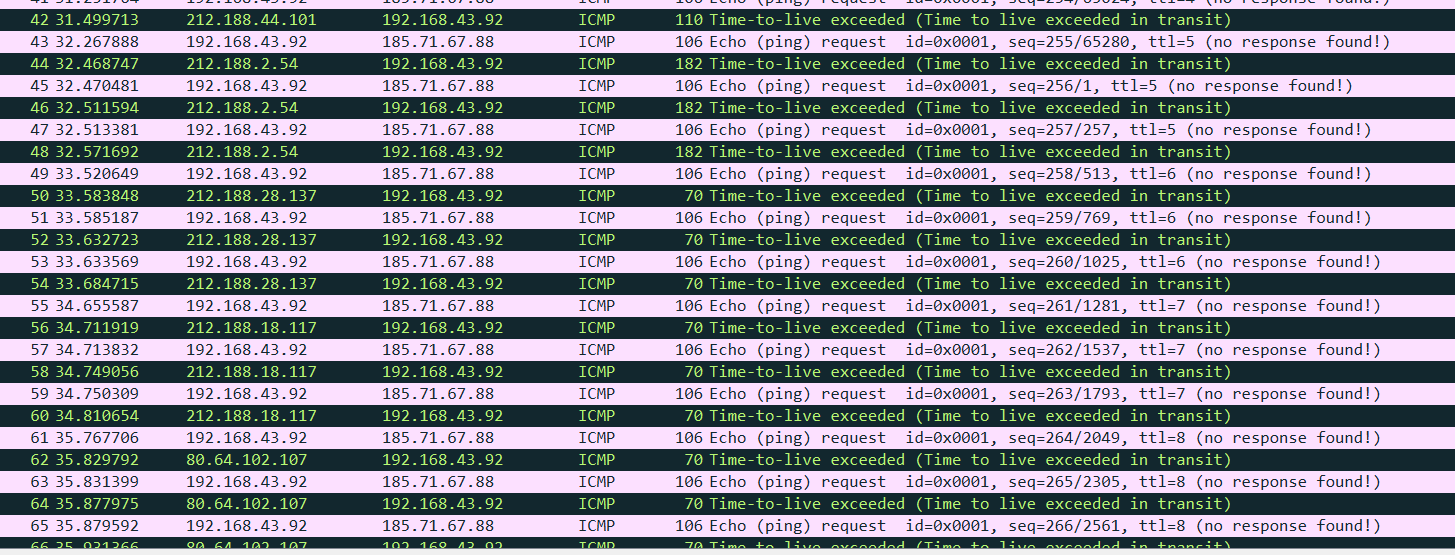
В поле данных ping-пакета содержится Header Data и Payload

* В Header Data, при ping запросах, содержится идентификатор запроса и порядковый номер.
* В Payload Data ping пакета содержится время отправки пакета и порядковый номер.



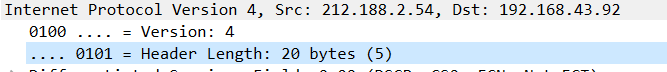
1. **Анализ трафика утилиты Tracert(Traceroute)**



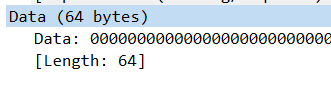


1. **Сколько байт содержится в заголовке IP? Сколько байт содержится в поле данных?**

Заголовок IP: 20 байт

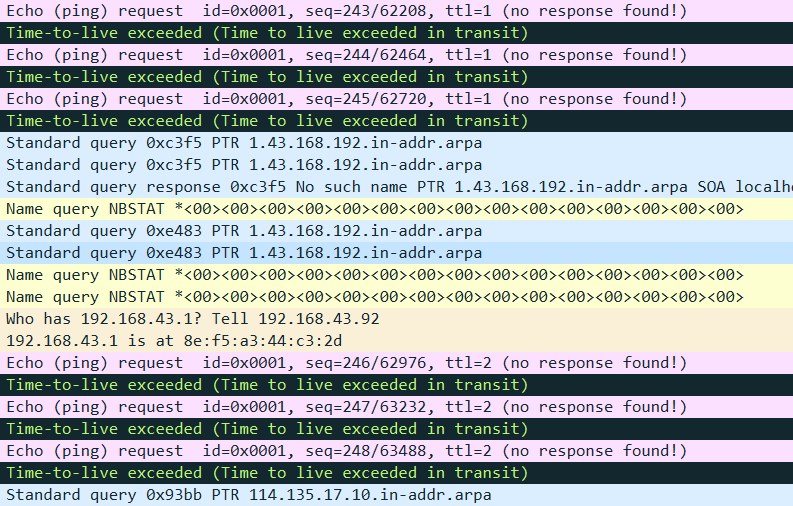


Поле данных: 64 байт



1. **Как изменяется поле TTL в следующий друг за другом ICMP-пакет tracert?**

Отправитель генерирует первый ICMP-пакет с значением TTL = 1, когда этот пакет поступает на маршрутизатор, тот маршрутизатор уменьшит значение TTL на единицу. Пакет с значением TTL = 0 не может быть переслан в Интернет, маршрутизатор отправляет ответ обратно отправителю с сообщением Time-to-live exceeded, так что отправитель знает первый хоп. Отправитель продолжает генерировать второй ICMP-пакет с TTL = 2, чтобы узнать второй хоп. Все так продолжается до назначения.



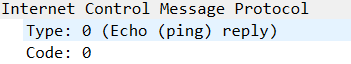
1. **Чем отличается ICMP-пакеты генерируемые утилитой tracert от ICMP пакетов генерируемых утилитой ping?**

Для ping пакет генерируется с значением TTL = максимальное значение, при проходе через каждый хоп значение TTL уменьшается на единицу.

Для tracert первый пакет генерируется с TTL = 1, второй с TTL = 2, третьий с TTl = 3, ….. TTL на-растает

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

ICMP reply: Пакет ICMP указывает, что хост назначения существует и сам отправил ответ ICMP

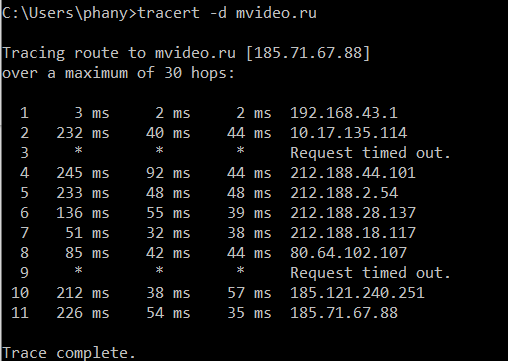


ICMP error предназначенный для определения маршрута(промежуточного узла),проходит пакет до заданного узла.

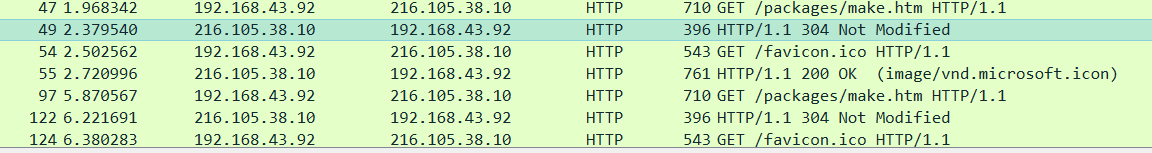


1. **Что изменится в работе tracert ,если убрать ключ “-d”? Какой дополнительный трафик при этом будет генерироваться**?

Эта опция не позволяет tracert преобразовывать IP-адреса в имена хостов, что часто приводит к гораздо более быстрым результатам.



1. **Анализ HTTP-трафик**



**HTTP GET**:

Когда кеш клиента пуст, запрос НЕ является условным (normal GET). С пустым кешем или без кеша ресурс отправляется обратно со статусом 200 OK.

Шаг 1: [**HTTP client**] ------------------request with empty cache-------------------> [**HTTP server**]

Шаг 2: [**HTTP client**] <---------------response with status code 200 OK------------ [**HTTP server**]

**HTTP CONDITIONAL GET:**

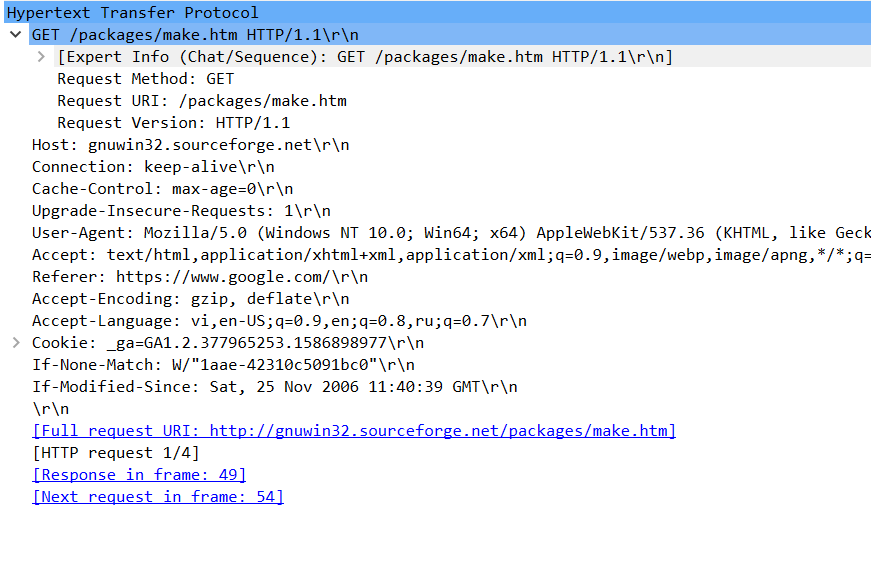
При отправке запроса с устаревшим кешем запрос является условным (CONDITIONAL GET). Если ресурс не изменялся, сервер вернет код статуса 304 Not Modified.

Шаг 1**: [HTTP client]** ---------------------request with stale cache--------------------> **[HTTP server]**

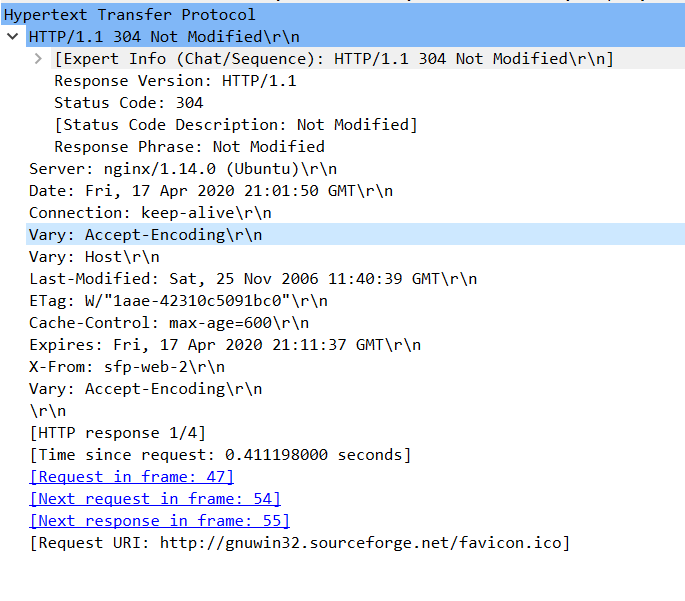
Шаг 2: **[HTTP client]** <-------response with status code 304 Not Modified------- **[HTTP server]**

GET-сообщение от клиента(браузера):



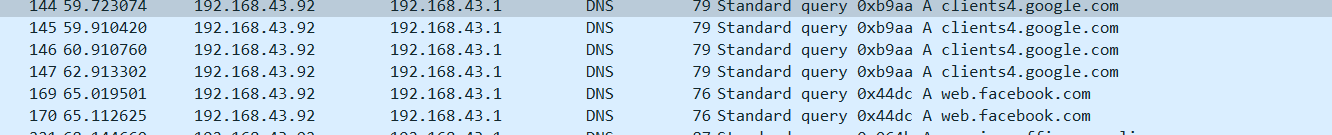


Ответ сервера:



Ресурс не изменялся, сервер вернет код статуса «304 Not Modified»

1. **Анализ DNS-трафика**



**Принцип работы DNS:**

DNS (Domain Name System) - это служба в сети TCP/IP, которая позволяет клиентам преобразовывать имена в IP-адреса.

Шаг 1: [DNS client] -------------Where is web.facebook.com---------> [DNS server]

Шаг 2: [DNS client] <---------It is at 157.240.203.16 --------- [DNS server]

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

Потому, что DNS запрос отправляется на адрес DNS сервера, чтобы по строковому адресу сайта узнать его IP

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

* **Recursive** – Такие запросы можно представить так: “Какой IP-адрес у a.merionet.ru?”
* **Iterative** запросы. Данные запросы передаются между DNS-серверами, когда один из них не имеет соответствующих записей. Таким образом, инициатор запроса будет контактировать с сервером, который имеет нужную запись
* **Inverse**. Собственно из названия данного запроса понятно, что они работают по инверсному принципу, то есть при известном IP-адресе запрашивается информация о доменном имени.

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

В случае, когда изображения представлены ссылкой на другое доменное имя. В этом случае необходимо делать DNS запросы для определения IP адресов этих доменов, чтобы получить изображения

**Анализ ARP-трафика**



**Принцип работы ARP:**

ARP (Address Resolution Protocol) - это служба в сети TCP/IP, которая позволяет клиентам найти MAC-адрес по заданому IP-адресу.

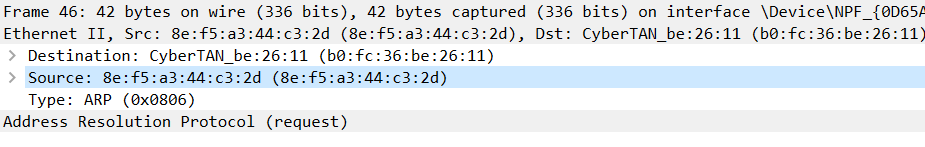
В этом случае хост ищет MAC-адрес маршрутизатора для отправки HTTP GET запрос, затем маршрутизатор ищет MAC-адрес хоста для отправки HTTP ответ.

Шаг 1: [Host] ---------ARP request: Who has 192.168.43.92? Tell 192.168.43.1--------> [Router]

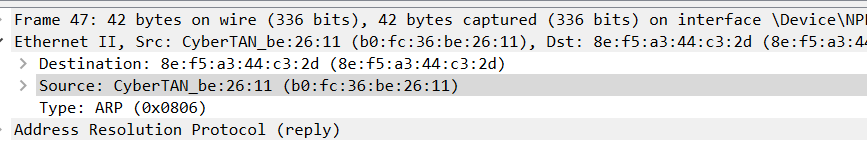
Шаг 2: [Host] <-------------ARP reply: 192.168.43.92 is at b0:fc:36:be:26:11 ------------- [Router]

1. **Какие MAC-адресса присуствуют в захваченных пакетах ARP-протокола?Что означают эти адресса? Какие устройства они идентифицируют?**

В пакете ARP запроса:



В пакете ARP ответа:



Broadcast MAC широковещательный адрес. Используется для передачи пакетов всем устройствам локальной сети - ff:ff:ff:ff:ff:ff

MAС- идентифицирующий wifi роутер - адресс маршрутизатора: b0:fc:36:be:26:11

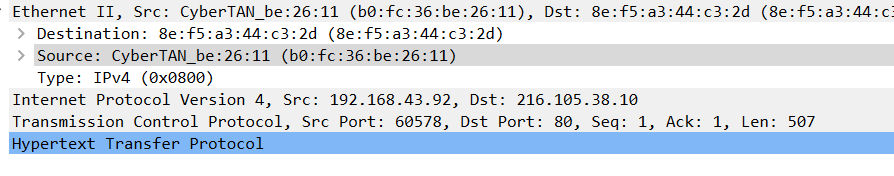
MAC- идентифицирующий компьютер - адресс хоста: 8e:f5:a3:44:c3:2d

MAC адресс является уникальным.

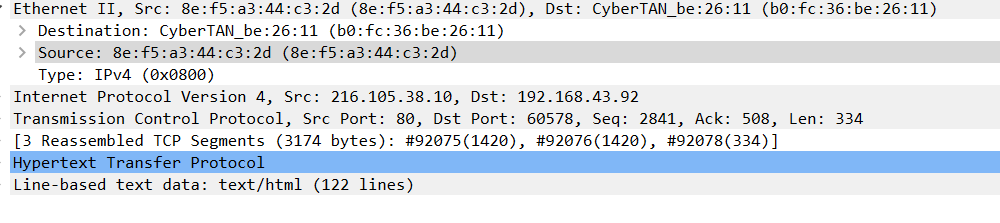
Кадры (Frames) передаются в локальной сети с использованием MAC-адреса.

1. **Какие MAC-адресса присутствуют в захваченных пакетах HTTP и что означают эти адресса ? Какие устройства они идентифицируют**?

В пакете HTTP запрос:



В пакете HTTP ответа:



В захваченных HTTP пакетах присутствует 2 MAC адреса

MAС- идентифицирующий wifi роутер - адресс маршрутизатора: c2-86-cf-fe-ea-84

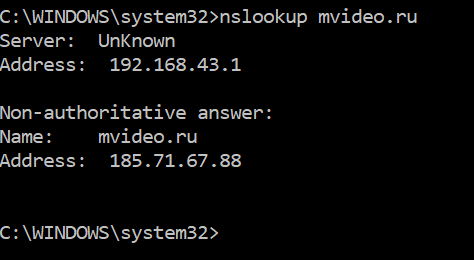
MAC- идентифицирующий компьютер - адресс хоста:52:a5:38:10:c3:0a

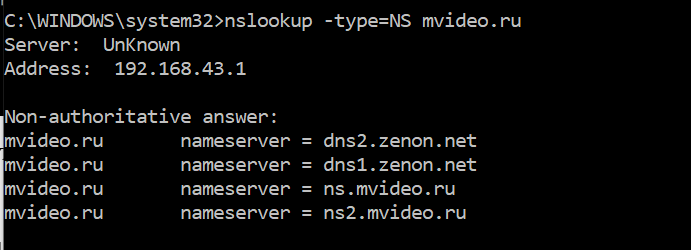
В HTTP-пакетах также можно увидеть, что присутствующие MAC-адреса - адреса отправителя и получателя в сети Ethernet. Отправитель – устройство в сети; получатель – хост (роутер), использующийся для перенаправления фрейма на требуемый адрес в иной сети, а также для получения ответа и его пересылки изначальному отправителю. В отличие от ARP, у HTTP не наблюдается использования MAC-адреса ff:ff:ff:ff:ff:ff

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

Чтобы хост (которого надо найти Мас-адресс) отправит пакет ARP-ответа источнику

**Анализ трафика утилиты nslookup**





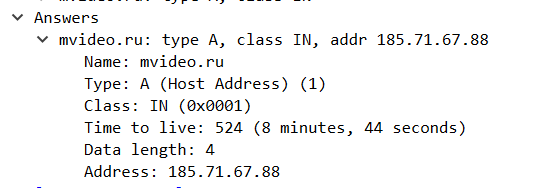
1. **Чем различается трасса трафика п.2 и п.4 ,указанных выше?**

Nslookup mvideo.ru выпольнить к DNS-серверу, заданному по умолчанию, на ответе содержался IP адрес указанного сайта.

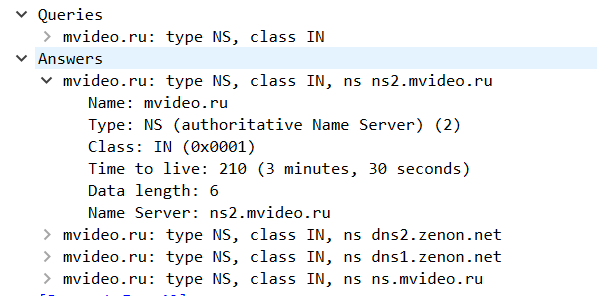
Nslookup -type=NS Команда выведет список используемых серверов имен. Обычно от двух до четырех серверов.

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

Nslookup:

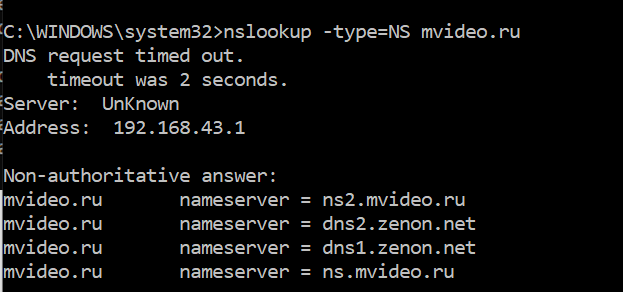


Nslookup -type=NS



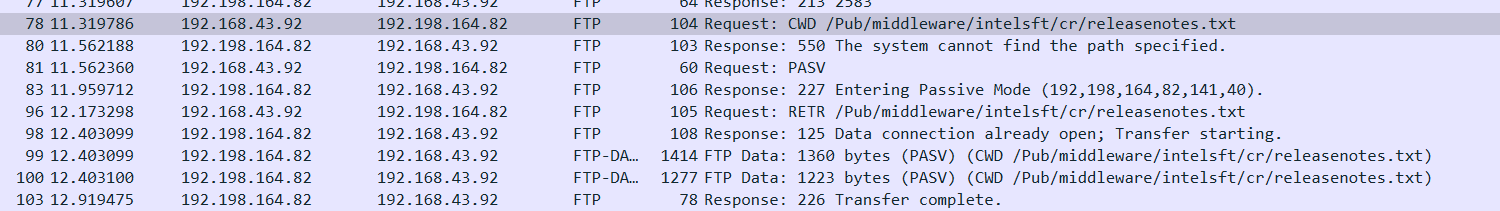
1. **Каковы имена серверов, возвращающих авторитативный (authoritative) отклик?**

Нет серверов, возвращающих авторитативный (authoritative) отклик.



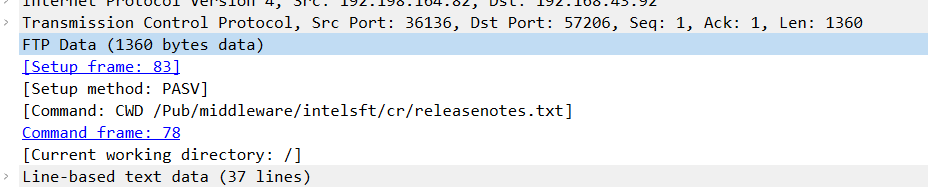
**Анализ FTP- трафика**

Захваченные данные:



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

1360 байтов данных содержится в пакете FTP-DATA



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

Для передачи FTP - пакетов, клиент открывает случайный порт в диапазоне от 1025. На сервере используется порт 21.

**Вопрос 3. Чем отличаются пакеты FTP от FTP-DATA**?

Пакеты FTP используются для передачи команд.

FTP-DATA используется для передачи данных.

**ВЫВОД**

Я познакомился с структурой протокольных блоков данных. Я понимаю процесс работы Интернета.Я выполнял 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(Ping ,Tracert,HTTP,ARP,nslookup,…)