федеральное государственное автономное образовательное учреждение
высшего образования

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

ОТЧЕТ

по лабораторной работе №3

«Анализ трафика компьютерных сетей с помощью утилиты Wireshark»

по дисциплине «**Компьютерные сети**»

Вариант ЛР4

Автор: Кулаков Н. В.

Факультет: ПИиКТ

Группа: Р33312

Преподаватель: Алиев Т. И.

Санкт-Петербург 2023

1. Постановка задачи и исходные данные

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

В процессе произвести наблюдения за передаваемым трафиком с компьютера пользователя в Интернет и в обратном направлении с использованием специализированной утилиты Wireshark, которая позволяет наблюдать структуру передаваемых кадров, пакетов и сегментов данных различных сетевых протоколов. При выполнении УИР требуется проанализировать последовательности команд и назначение служебных данных, используемых для организации обмена данными в различных протоколах.

2. Выполнение

2.1. Анализ трафика утилиты ping

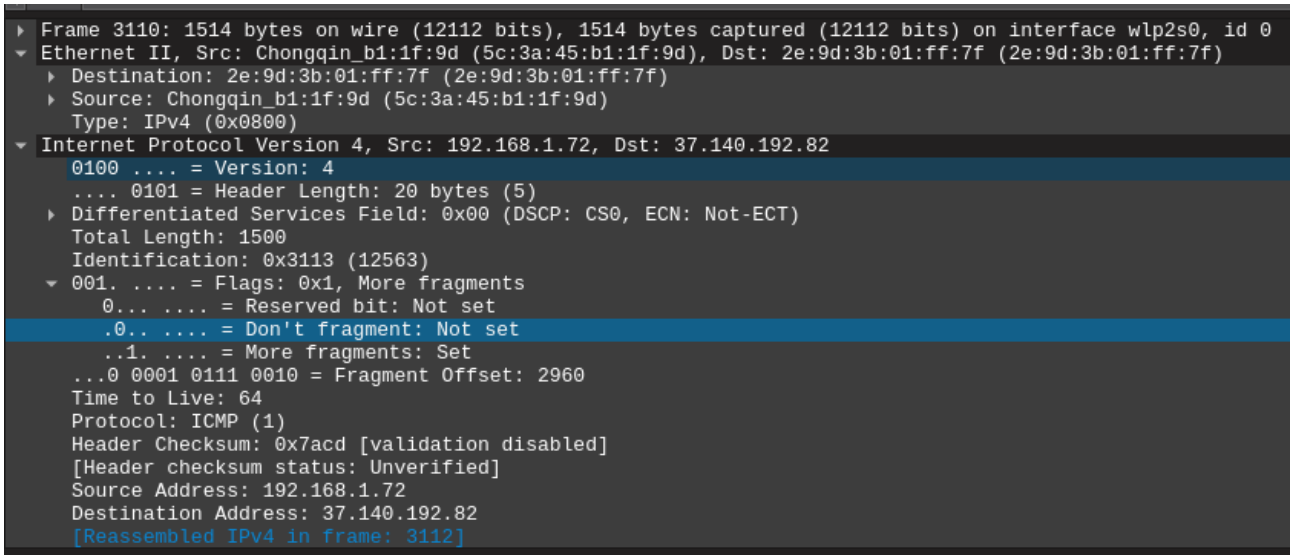
```
nikit@host lab-4 % ping -s 200 kulakov-pro.ru
PING kulakov-pro.ru (37.140.192.82) 200(228) bytes of data.
208 bytes from server51.hosting.reg.ru (37.140.192.82): icmp_seq=1 ttl=45 time=62.8 ms
208 bytes from server51.hosting.reg.ru (37.140.192.82): icmp_seq=2 ttl=45 time=53.9 ms
208 bytes from server51.hosting.reg.ru (37.140.192.82): icmp_seq=3 ttl=45 time=53.6 ms
208 bytes from server51.hosting.reg.ru (37.140.192.82): icmp_seq=4 ttl=45 time=50.2 ms
208 bytes from server51.hosting.reg.ru (37.140.192.82): icmp_seq=5 ttl=45 time=48.0 ms
```

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

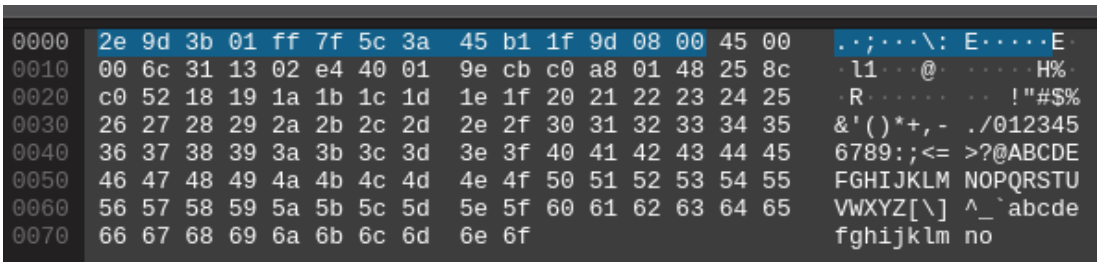
ICMP пакет передается внутри пакета IP, который передается по Ethernet, максимальный размер кадра которого равен 1518 байт. Соответственно, при передаче пакет ICMP фрагментируется. Ниже представлен результат при передаче 6000 байт.

```
3107 514.391415538 192.168.1.197 192.168.1.72     DNS      102 Standard query response 0x5f77 AAAA kulakov-pro.ru AAAA 2a00:f940:2:2:1:1:0:51
3108 514.391815733 192.168.1.72  37.140.192.82    IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3113) [Reassembled in #3112]
3109 514.391829632 192.168.1.72  37.140.192.82    IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3113) [Reassembled in #3112]
3110 514.391834940 192.168.1.72  37.140.192.82    IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=2960, ID=3113) [Reassembled in #3112]
3111 514.391856731 192.168.1.72  37.140.192.82    IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=4440, ID=3113) [Reassembled in #3112]
3112 514.391861620 192.168.1.72  37.140.192.82    ICMP     122 Echo (ping) request  id=0x1c72, seq=1/256, ttl=64 (no response found!)
3113 515.415518899 192.168.1.72  37.140.192.82    IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=334c) [Reassembled in #3117]
3114 515.415539223 192.168.1.72  37.140.192.82    IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=334c) [Reassembled in #3117]
3115 515.415545369 192.168.1.72  37.140.192.82    IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=2960, ID=334c) [Reassembled in #3117]
3116 515.415552563 192.168.1.72  37.140.192.82    IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=4440, ID=334c) [Reassembled in #3117]
```

Ниже представлено содержимое кадра 3110. Мы видим, что пакет IPv4, который в нем лежит, имеет размер 1500 байт (с учетом заголовка), а размер кадра Ethernet равен 1514 байтам.



Сам заголовок Ethernet II содержит MAC адреса — 12 байт и 2 байта, отвечающие за тип протокола выше (IPv4).



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

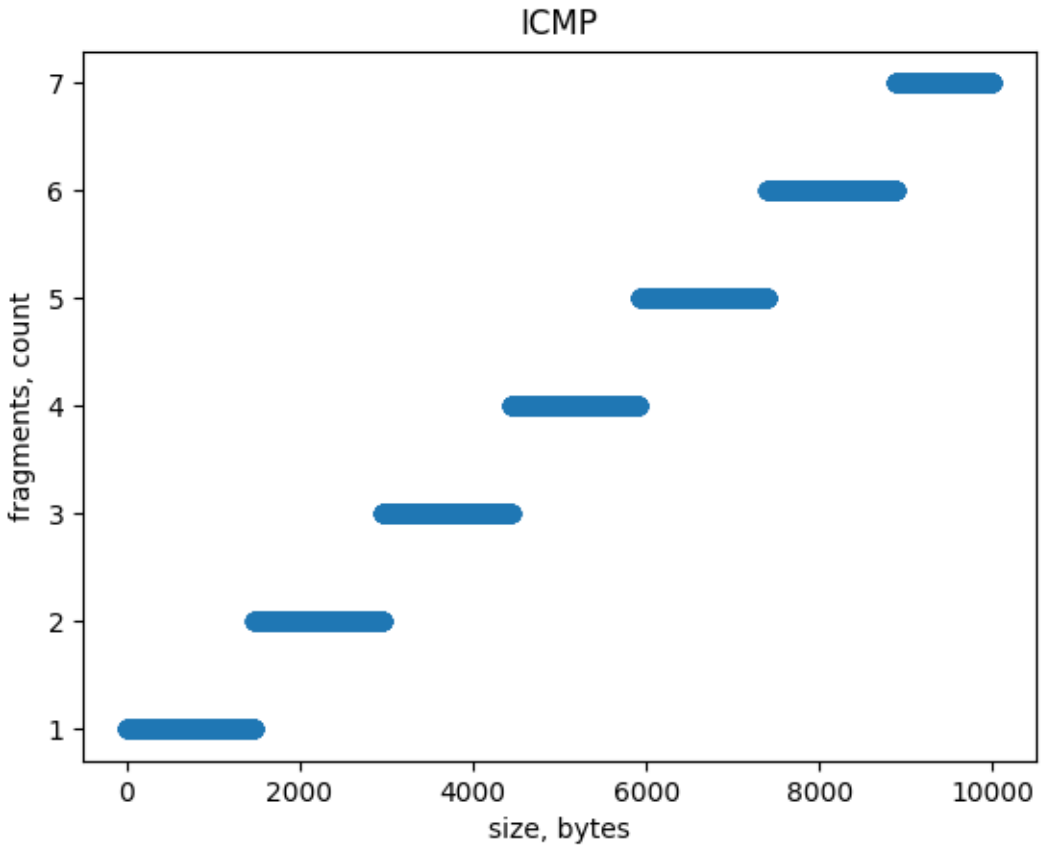
Флаг «More fragments» в пакете IPv4 отвечает за то, является ли фрагмент не последним.

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

Количество фрагментов прямопропорционально размеру передаваемого пакета. Так если передается пакет размера 6000 (6028) байт, то для его полной передачи с учетом потребуется 5 фрагментов, в связи с ограничением размера кадра

Ethernet (описано выше). Так в каждый пакет будет умещаться IPv4 максимум 1480 байт данных, потому что пакет IPv4 вкладывается в кадр Ethernet.

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

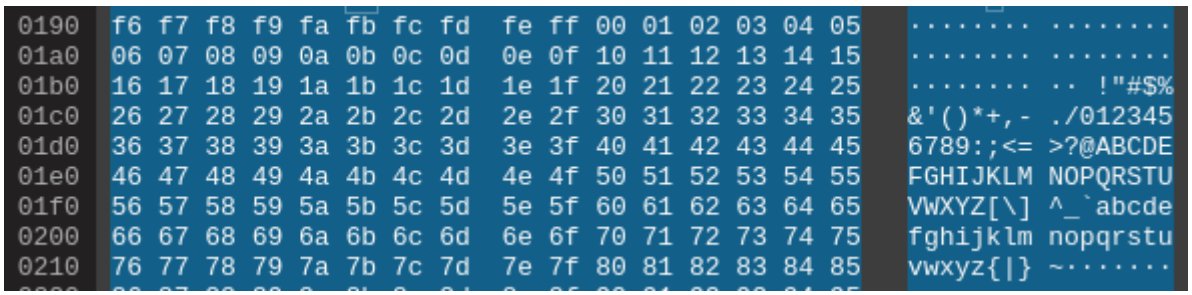


5. Как изменить поле TTL с помощью утилиты ping?

```
-t ttl
    ping only. Set the IP Time to Live.
```

6. Что содержится в поле данных ping-пакета?

Мусор в виде ASCII символов, если это так можно трактовать. Другими словами, однобайтовые слова, последовательно идущие друг за другом и увеличивающиеся на единицу.



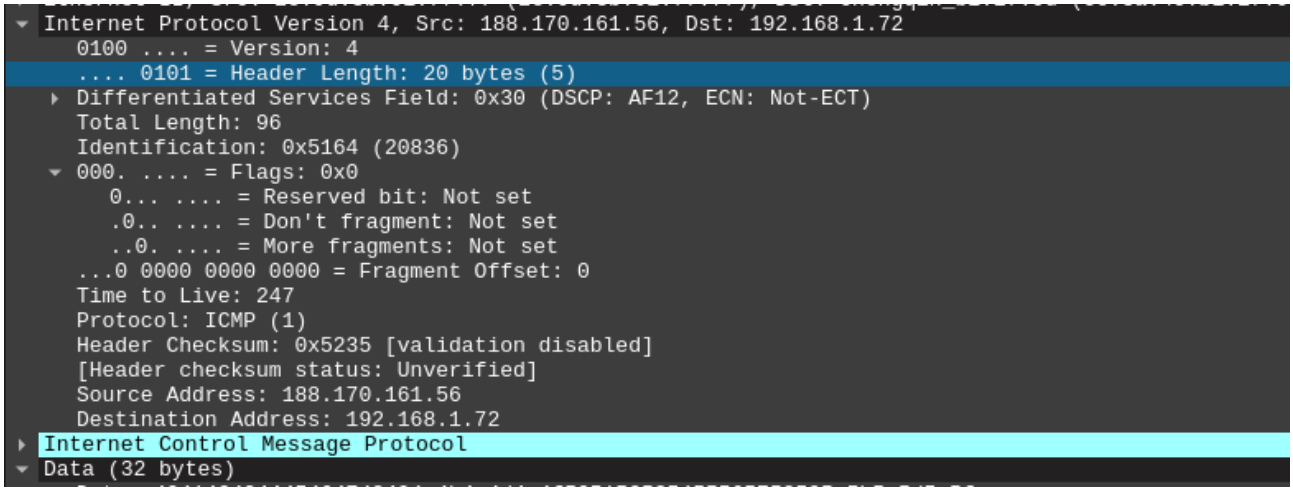
2.2. Анализ трафика утилиты tracert (traceroute)

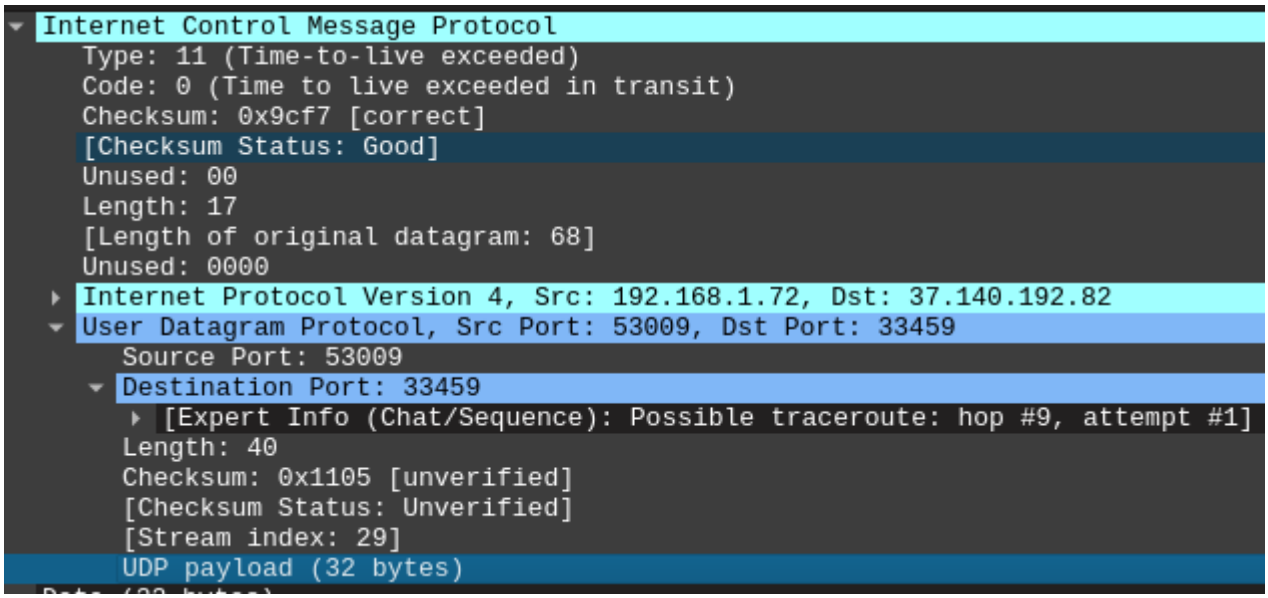
```
(machine-learning) nikit@host lab-4 % traceroute kulakov-pro.ru
traceroute to kulakov-pro.ru (37.140.192.82), 30 hops max, 60 byte packets
 1  192.168.1.197 (192.168.1.197)  6.090 ms  6.041 ms  6.014 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  188.170.161.57 (188.170.161.57)  56.102 ms  52.769 ms  55.991 ms
 9  188.170.161.56 (188.170.161.56)  52.693 ms  67.227 ms  63.935 ms
10  * * *
11  37.29.3.22 (37.29.3.22)  70.367 ms  70.339 ms  66.187 ms
12  185.140.148.19 (185.140.148.19)  66.153 ms  69.381 ms 185.140.148.31 (185.140.148.31)  44.77
3 ms
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  server51.hosting.reg.ru (37.140.192.82)  53.716 ms  58.197 ms  58.239 ms
```

В соответствии с документацией, звездочки означают, что либо маршрутизатор в течение какого-то времени не отвечает, либо временно перегружен, либо некоторые маршрутизаторы специально не реагируют на данные сообщения, так как им запретили. Таким образом, в некоторых случаях даже когда выставим огромное значение TTL, то все равно не достигнем конечного узла.

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

Ниже представлен ответ от маршрутизатора с типом time-limit-esceeds. В заголовке IP содержится 20 байт. В поле данных 32 байта

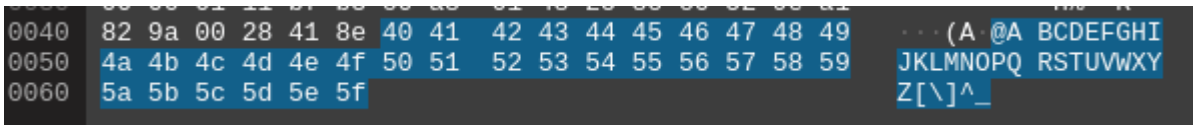




2. Как и почему изменяется поле TTL в следующих друг за другом ICMP-пакетах tracert? Для ответа на этот вопрос нужно проследить изменение TTL при передаче по маршруту, состоящему из более чем двух хопов.

Для определения пути tracert отправляет пакеты с TTL, который увеличивается. Таким образом, когда TTL сравнится в маршрутизаторе равным 0, то тот посылает ICMP сообщение с информацией о том, что TTL exceeds. Таким образом, по умолчанию сначала посылается пакет с TTL равным 1 (n-ое кол-во штук), затем с TTL равным 2 и т. д. до тех пор пока не достигнем конечного узла.

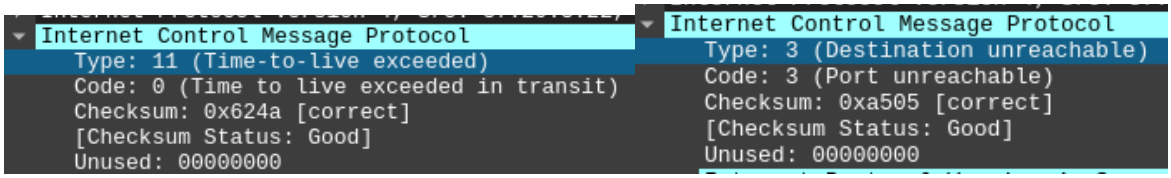
3. Чем отличаются ICMP-пакеты, генерируемые утилитой tracert, от ICMP-пакетов, генерируемых утилитой ping (см. предыдущее задание).



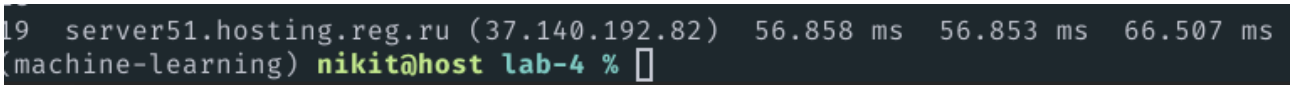
В данном случае тоже возвращаются инкрементирующиеся слова, однако начиная с другого числа.

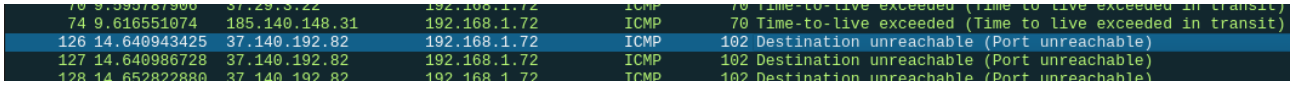
4. Чем отличаются полученные пакеты «ICMP reply» от «ICMP error» и зачем нужны оба этих типа ответов?

При отправке получал только 2 варианта ответов от ICMP: TTL exceeded — пакет достиг маршрутизатора, второй — порт недоступен. Как правило второе указывает на состояние перегрузки или проблему с конфигурацией процесса на хосте, создающем отчеты, значит, вероятно, маршрутизатор не ожидает таких запросов.



Второй ответ получаем уже только на конечном узле:





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

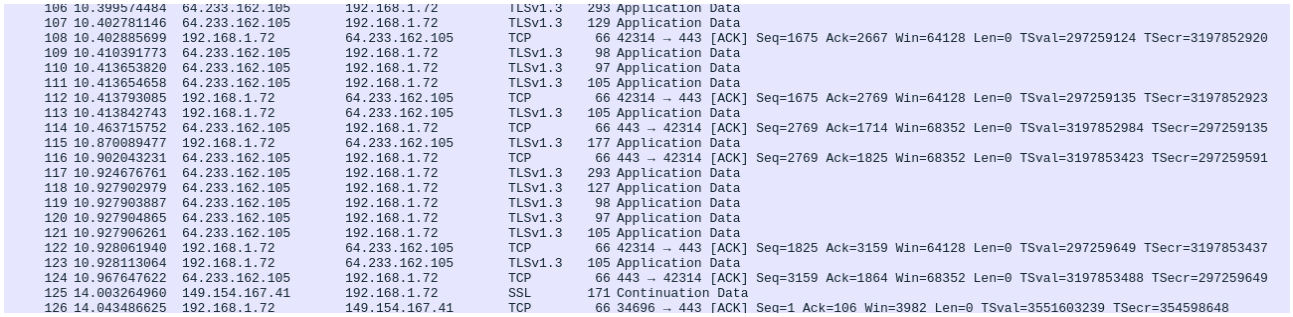
Из документации WINDOWS:

Параметр -d с помощью команды tracert программа TRACERT не требуется выполнять поиск в DNS для каждого IP-адреса, так, что команда TRACERT отображает IP-адрес ближних интерфейсов маршрутизаторов.

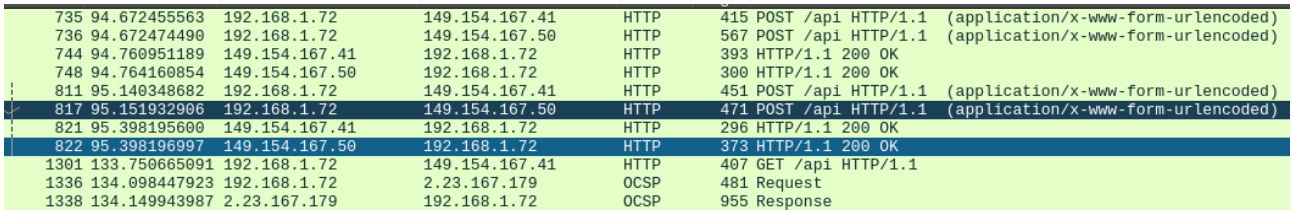
В Linux этот флаг связан с дополнительной отладочной информацией от сокетов.

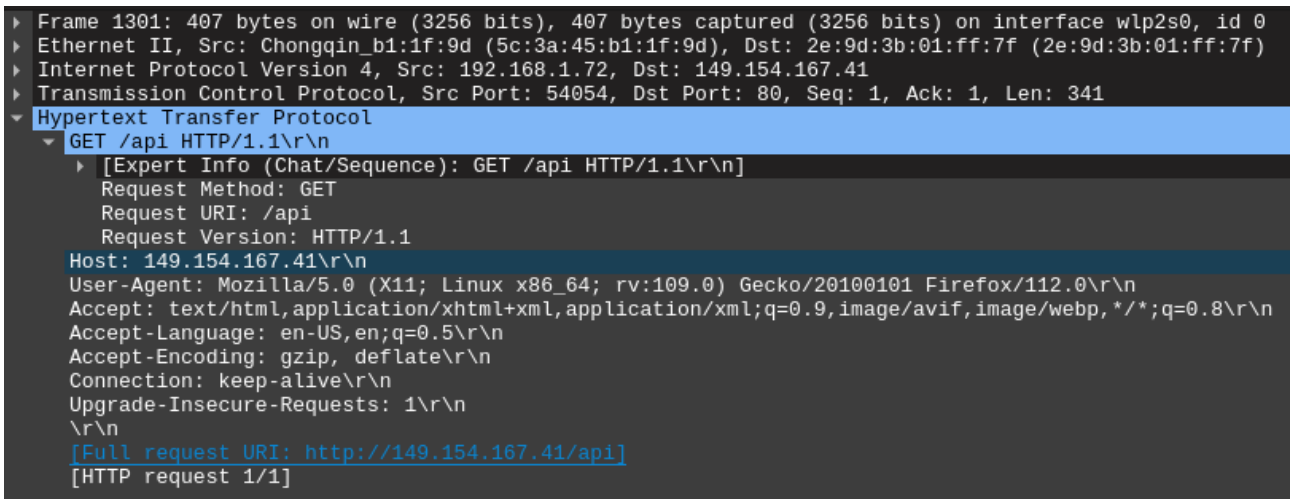
2.3. Анализ HTTP-трафика

В данном пункте описано только то, что удалось получить. Запросы от браузера видны только TLS и TCP.



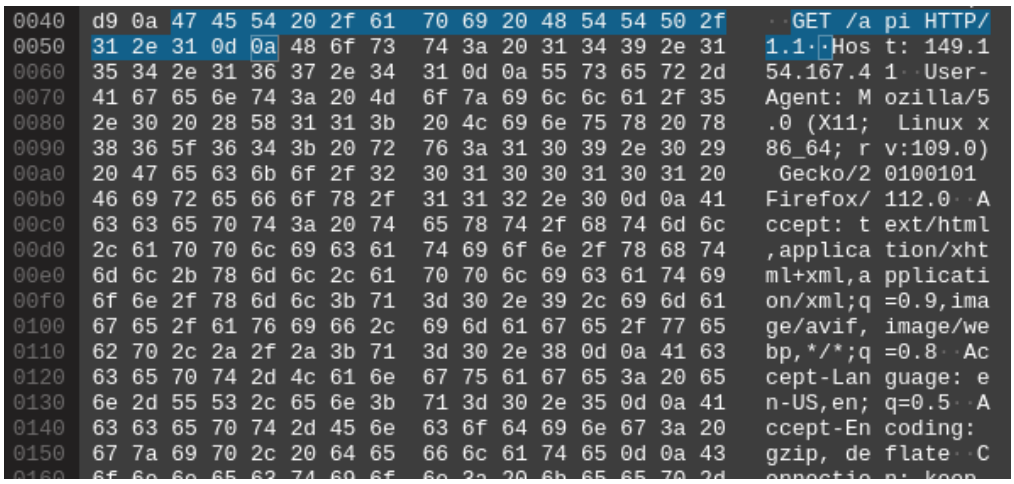
Рассмотрим какой-то из пакетов HTTP. Как можем увидеть, протокол HTTP является прикладным протоколом, и поэтому работает поверх протокола TCP.





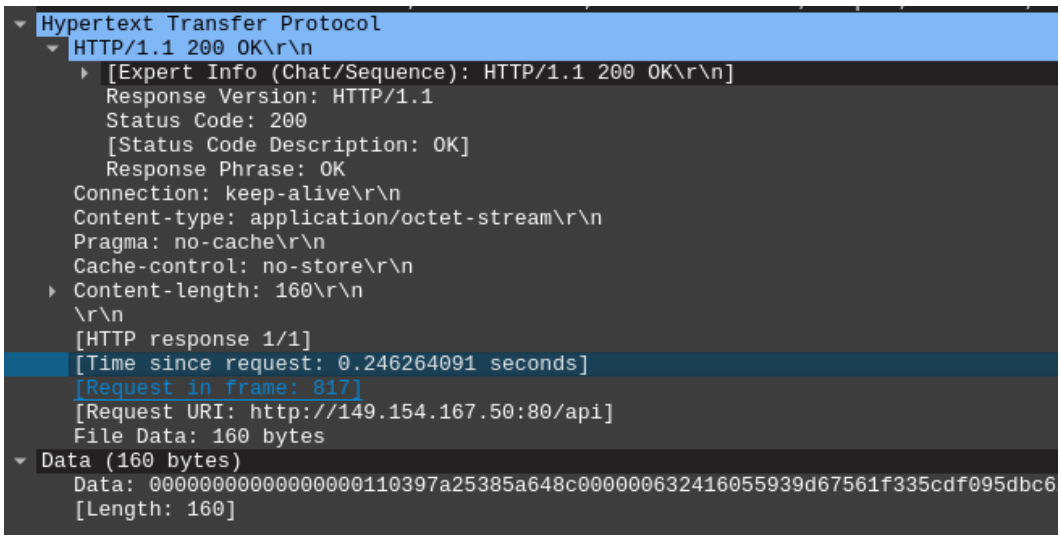
Сообщение прокола представляется в виде:

- <Тип запроса (GET/POST)> <путь относительно корня> <Протокол/версия>
- Затем с новой строки (переноса) идут значения вида ключ:значение
- После идет тело запроса, может отсутвовать

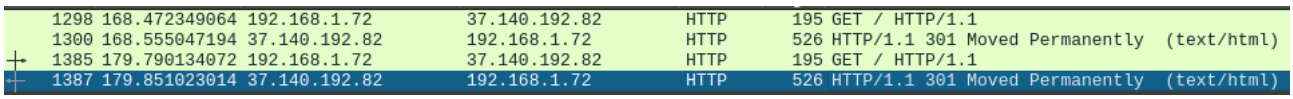


Ответ выглядит в виде:

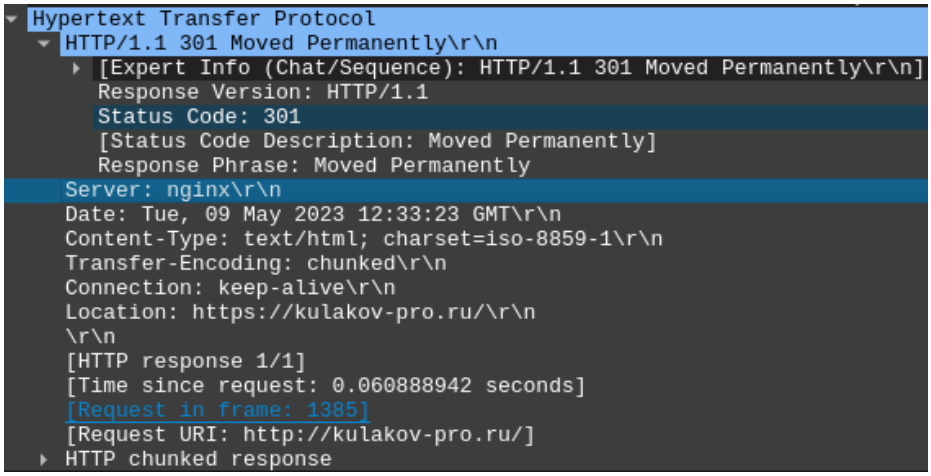
- <Протокол/версия> <Статус> <перенос>
- Заголовок вида ключ-значение
- Тело запроса



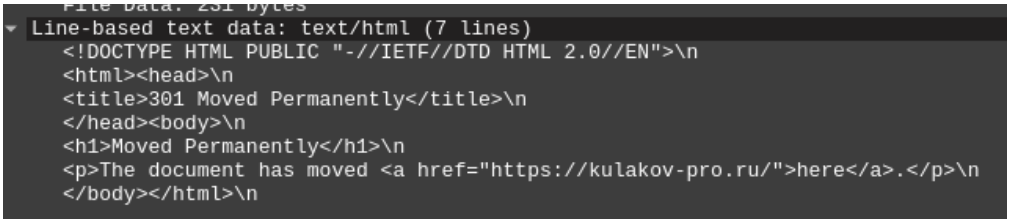
С помощью утилиты wget удалось послать запрос на http://kulakov-pro.ru и получить следующий ответ:



Нас перенаправляет на https версию страницы.



Тело запроса:

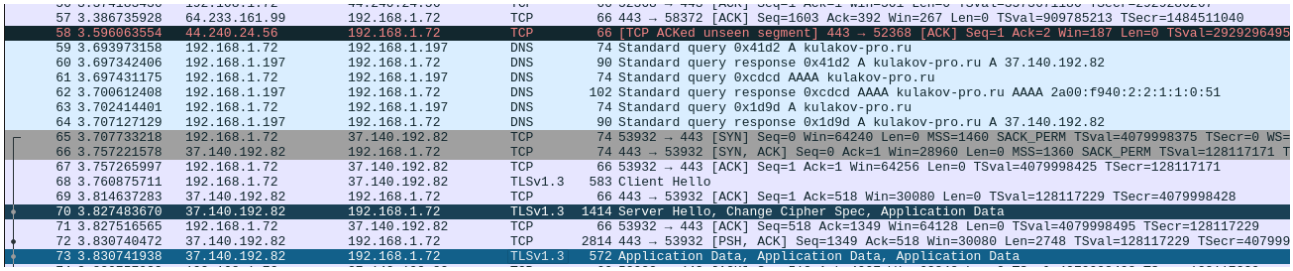


Подытожив, понимаем, что wireshark не отображает https запросы и ответы.

2.4. Анализ DNS-трафика

Отчищаем dns, перезапуская сервис:

```
sudo /etc/init.d/dnsmasq restart
```



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

Для того, чтобы получить IP адрес сайта отправляется запрос на DNS сервер, который возвращает IP адрес уже сайта. На рисунке ниже мы можем видеть, что получается как IPv4, так и IPv6 адреса необходимой страницы. Адресом назначения указан адрес маршрутизатора (модема телефона).

2. Какие бывают типы DNS-запросов?

- Прямой — запрос на преобразование имени (символьного адреса) хоста в его IP-адрес.
- Обратный — запрос на преобразование адреса хоста в его имя.
- Рекурсивный - DNS-сервер опрашивает серверы (в порядке убывания уровня зон в имени), пока не найдёт ответ или не обнаружит, что домен не существует.
- Нерекурсивный (итеративный) - DNS-сервер либо возвращает данные о зоне, за которую он ответственен, либо возвращает ошибку.

Также выделяют запросы типа:

- A — получение IPv4
- AAAA — получение IPv6
- CNAME — получение канонического имени
- MX — получение информации о почтовых серверах, ответственных за обработку почту для данного домена
- NS (Name Server) — вернуть список DNS серверов, ответственных за данный домен
- PTR - обратная DNS-запись или запись указателя связывает IP-адрес хоста с его каноническим именем.

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

- Если изображения хранятся на отдельном сервере или поддомене
- Используется CDN (Content Derivery Network), где ресурсы могут храниться на разных серверах

2.5. Анализ ARP-трафика

Очищаем таблицу MAC адресов:

```
nikit@host lab-4 % arp -a
? (192.168.1.197) at 2e:9d:3b:01:ff:7f [ether] on wlp2s0
nikit@host lab-4 % arp --delete 192.168.1.197
```

Как можно заметить ниже ARP запросы посылаются как от маршрутизатора (192.168.1.197), так и от компьютера (192.168.1.72). Broadcast означает, что данный запрос предназначен всем узлам в данной локальной сети.

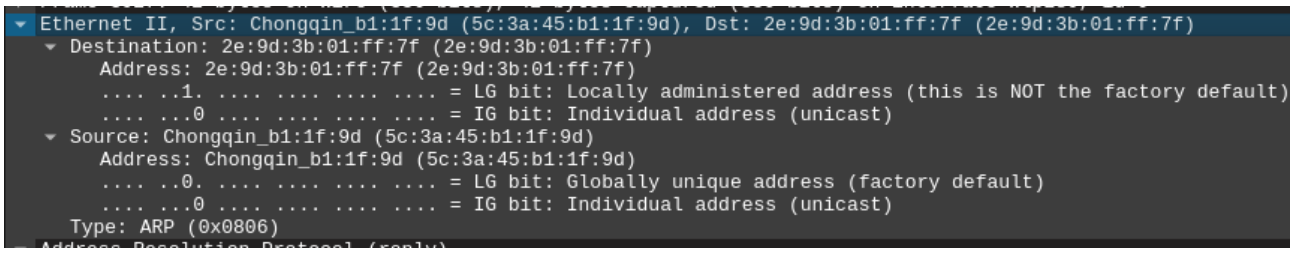
```
3491 396.604475809 2e:9d:3b:01:ff:7f  Chongqin_b1:1f:9d  ARP  42 Who has 192.168.1.72? Tell 192.168.1.197
3492 396.604503397 Chongqin_b1:1f:9d  2e:9d:3b:01:ff:7f  ARP  42 192.168.1.72 is at 5c:3a:45:b1:1f:9d
3506 407.484092450 Chongqin_b1:1f:9d  Broadcast           ARP  42 Who has 192.168.1.197? Tell 192.168.1.72
3507 407.488023304 2e:9d:3b:01:ff:7f  Chongqin_b1:1f:9d  ARP  42 192.168.1.197 is at 2e:9d:3b:01:ff:7f
```

```
▸ Frame 3926: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlp2s0, id 0
▸ Ethernet II, Src: 2e:9d:3b:01:ff:7f (2e:9d:3b:01:ff:7f), Dst: Chongqin_b1:1f:9d (5c:3a:45:b1:1f:9d)
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 2e:9d:3b:01:ff:7f (2e:9d:3b:01:ff:7f)
    Sender IP address: 192.168.1.197
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.72
```

```
▸ Frame 3927: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlp2s0, id 0
▸ Ethernet II, Src: Chongqin_b1:1f:9d (5c:3a:45:b1:1f:9d), Dst: 2e:9d:3b:01:ff:7f (2e:9d:3b:01:ff:7f)
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Chongqin_b1:1f:9d (5c:3a:45:b1:1f:9d)
    Sender IP address: 192.168.1.72
    Target MAC address: 2e:9d:3b:01:ff:7f (2e:9d:3b:01:ff:7f)
    Target IP address: 192.168.1.197
```

1. Какие MAC-адреса присутствуют в захваченных пакетах ARP-протокола? Что означают эти адреса? Какие устройства они идентифицируют?

При запросе присутствуют MAC адрес отправителя, при ответе MAC адрес отправителя и получателя. MAC адрес — физический адрес устройства. Ниже показано, что он является глобальным индивидуальным для отправителя — компьютера и локальным индивиальным для модема (телефона, раздающего интернет) (заданы соответствующие биты MAC адреса):



2. Какие MAC-адреса присутствуют в захваченных HTTP-пакетах и что означают эти адреса? Что означают эти адреса? Какие устройства они идентифицируют?

Те же самые, что и в ARP запросе. Теперь по ним определяется с какого компьютера на какой маршрутизатор (модем) отправить/получить сообщение.

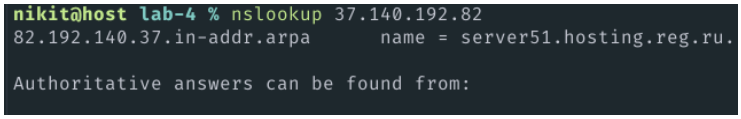
3. Для чего ARP-запрос содержит IP-адрес источника?

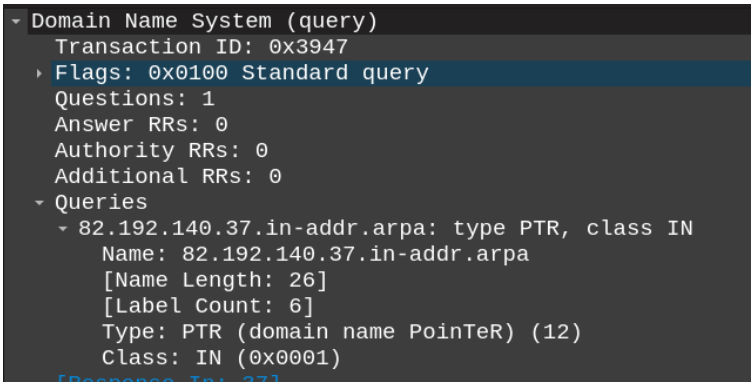
Скорее всего для определения коллизий со стороны получателя запроса, который по своей таблице ARP сможет это определить, однако конкретной информации по этому найти не удалось. ARP же протокол канального уровня, поэтому для понимания куда послать ответ ему IP адреса не нужны, так как с запросом был послан MAC адрес источника.

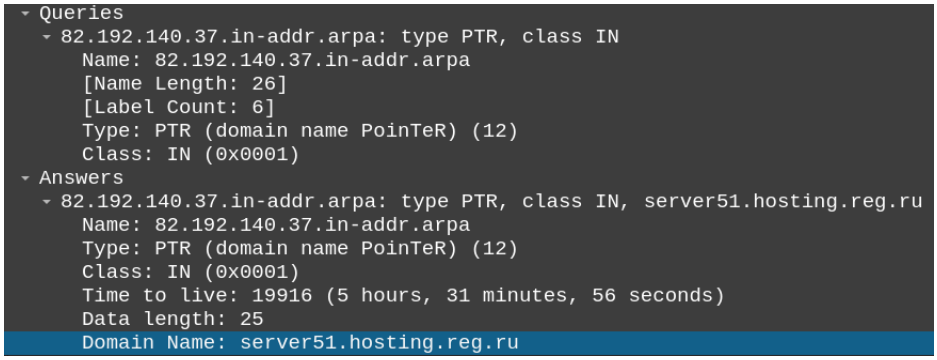
2.6. Анализ трафика утилиты nslookup

Утилита nslookup предназначена для получения различной информации с DNS серверов.

Первая команда, которая была послана для получения dns имени по ip адресу. Тип запроса — PTR, то есть получаем по известному ip адресу dns имя. Ниже представлено содержимое dns сообщения отправителя и получателя.







Данный запрос — запрос типа NS, то есть для получения DNS-серверов, которые отвечают за разрешение ip адреса и dns имени для данного доменного имени. Таким образом, определели, что авторитативный ответ может быть получен от DNS-серверов ns1.hosting.reg.ru и ns2.hosting.reg.ru.

```
nikit@host lab-4 % nslookup -type=ns kulakov-pro.ru
Server:         192.168.1.197
Address:        192.168.1.197#53

Non-authoritative answer:
KULAKOV-PRO.ru  nameserver = ns1.hosting.reg.ru.
KULAKOV-PRO.ru  nameserver = ns2.hosting.reg.ru.

Authoritative answers can be found from:
ns1.hosting.reg.ru      internet address = 31.31.194.245
ns1.hosting.reg.ru      internet address = 31.31.194.251
ns1.hosting.reg.ru      internet address = 31.31.196.37
ns1.hosting.reg.ru      internet address = 31.31.196.52
ns1.hosting.reg.ru      internet address = 31.31.196.61
ns1.hosting.reg.ru      internet address = 31.31.196.180
ns1.hosting.reg.ru      internet address = 31.31.198.177
ns1.hosting.reg.ru      internet address = 37.140.192.20
ns1.hosting.reg.ru      internet address = 37.140.192.93
ns1.hosting.reg.ru      internet address = 37.140.193.121
ns1.hosting.reg.ru      internet address = 37.140.196.144
ns1.hosting.reg.ru      internet address = 194.58.91.38
ns1.hosting.reg.ru      internet address = 194.67.73.6
ns1.hosting.reg.ru      internet address = 194.67.73.9
```

```
Domain Name System (query)
    Transaction ID: 0x6c40
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ kulakov-pro.ru: type NS, class IN
        Name: kulakov-pro.ru
        [Name Length: 14]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
      [Response In: 61]
```

```
Domain Name System (response)
    Transaction ID: 0x6c40
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 14
  ▾ Queries
    ▾ kulakov-pro.ru: type NS, class IN
        Name: kulakov-pro.ru
        [Name Length: 14]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
  ▾ Answers
    ▾ KULAKOV-PRO.ru: type NS, class IN, ns ns1.hosting.reg.ru
        Name: KULAKOV-PRO.ru
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 1591 (26 minutes, 31 seconds)
        Data length: 20
        Name Server: ns1.hosting.reg.ru
    ▾ KULAKOV-PRO.ru: type NS, class IN, ns ns2.hosting.reg.ru
        Name: KULAKOV-PRO.ru
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 1591 (26 minutes, 31 seconds)
        Data length: 6
        Name Server: ns2.hosting.reg.ru
  ▾ Additional records
    ▾ ns1.hosting.reg.ru: type A, class IN, addr 31.31.194.245
        Name: ns1.hosting.reg.ru
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

```
    36 3.383502… 192.168.1.72   192.168.1.197  DNS     86 Standard query 0x3947 PTR 82.192.140.37.in-addr.arpa
    37 3.456506… 192.168.1.197  192.168.1.72   DNS    123 Standard query response 0x3947 PTR 82.192.140.37.in-addr.arpa PTR server51.hosting.reg.ru
    60 11.33486… 192.168.1.72   192.168.1.197  DNS     74 Standard query 0x6c40 NS kulakov-pro.ru
    61 11.37140… 192.168.1.197  192.168.1.72   DNS    360 Standard query response 0x6c40 NS kulakov-pro.ru NS ns1.hosting.reg.ru NS ns2.hosting.reg.ru A 31.31.194.24
```

Неавторитетная запись означает, что соотношение было получено нет от dns-сервера, который отвечает за данный сектор доменных имен. Так, например, если мы попросим авторитетный dns-сервер предоставить эту информацию, то этого предупреждения не будет.

```
nikit@host lab-4 % nslookup kulakov-pro.ru ns1.hosting.reg.ru
Server:         ns1.hosting.reg.ru
Address:        31.31.194.245#53

Name:   kulakov-pro.ru
Address: 37.140.192.82
Name:   kulakov-pro.ru
Address: 2a00:f940:2:2:1:1:0:51
```

В поле ANSWERS содержатся соответствующие записи на запрос. Одному запросу может соответствовать несколько записей ответа, как во втором примере. Поля соответствуют типу запроса.

2.7. Анализ FTP-трафика

Для получения чего-либо по протоколу ftp был осуществлен запрос на gitlab.se.ifmo.ru.

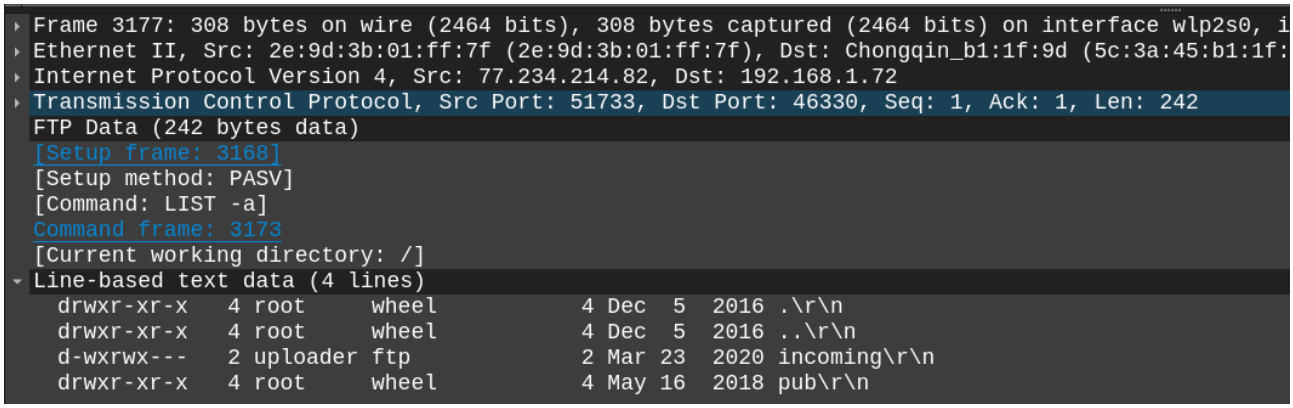
```
nikit@host lab-4 % wget ftp://gitlab.se.ifmo.ru
--2023-05-09 18:50:28--  ftp://gitlab.se.ifmo.ru/
           => '.listing'
Resolving gitlab.se.ifmo.ru... 77.234.214.82
Connecting to gitlab.se.ifmo.ru|77.234.214.82|:21... connected.
Logging in as anonymous ... Logged in!
==> SYST ... done.    ==> PWD ... done.
==> TYPE I ... done.  ==> CWD not needed.
==> PASV ... done.    ==> LIST ... done.

.listing                    [ <=>                                ]     242  --.-KB/s    in 0.01s

2023-05-09 18:50:29 (18.8 KB/s) - '.listing' saved [242]

Removed '.listing'.
Wrote HTML-ized index to 'index.html' [388].
```

Соответствующие ему сообщения в wireshark:

31…	69.68436…	77.234.214.82	192.168.1.72	FTP	110	Response: 220 ProFTPD 1.3.5a Server (FTP Server) [77.234.214.82]
31…	69.68453…	192.168.1.72	77.234.214.82	FTP	70	Request: USER anonymous
31…	69.72298…	77.234.214.82	192.168.1.72	FTP	129	Response: 331 Anonymous login ok, send your complete email address as your password
31…	69.72331…	192.168.1.72	77.234.214.82	FTP	67	Request: PASS -wget@
31…	69.76466…	77.234.214.82	192.168.1.72	FTP	104	Response: 230 Anonymous access granted, restrictions apply
31…	69.76487…	192.168.1.72	77.234.214.82	FTP	60	Request: SYST
31…	69.80437…	77.234.214.82	192.168.1.72	FTP	73	Response: 215 UNIX Type: L8
31…	69.80462…	192.168.1.72	77.234.214.82	FTP	59	Request: PWD
31…	69.85152…	77.234.214.82	192.168.1.72	FTP	88	Response: 257 "/" is the current directory
31…	69.85174…	192.168.1.72	77.234.214.82	FTP	62	Request: TYPE I
31…	69.88320…	77.234.214.82	192.168.1.72	FTP	73	Response: 200 Type set to I
31…	69.88339…	192.168.1.72	77.234.214.82	FTP	60	Request: PASV
31…	69.92342…	77.234.214.82	192.168.1.72	FTP	105	Response: 227 Entering Passive Mode (77,234,214,82,202,21).
31…	69.96749…	192.168.1.72	77.234.214.82	FTP	63	Request: LIST -a
31…	70.01302…	77.234.214.82	192.168.1.72	FTP	109	Response: 150 Opening BINARY mode data connection for file list
31…	70.02573…	77.234.214.82	192.168.1.72	FTP-…	308	FTP Data: 242 bytes (PASV) (LIST -a)
31…	70.07554…	77.234.214.82	192.168.1.72	FTP	77	Response: 226 Transfer complete

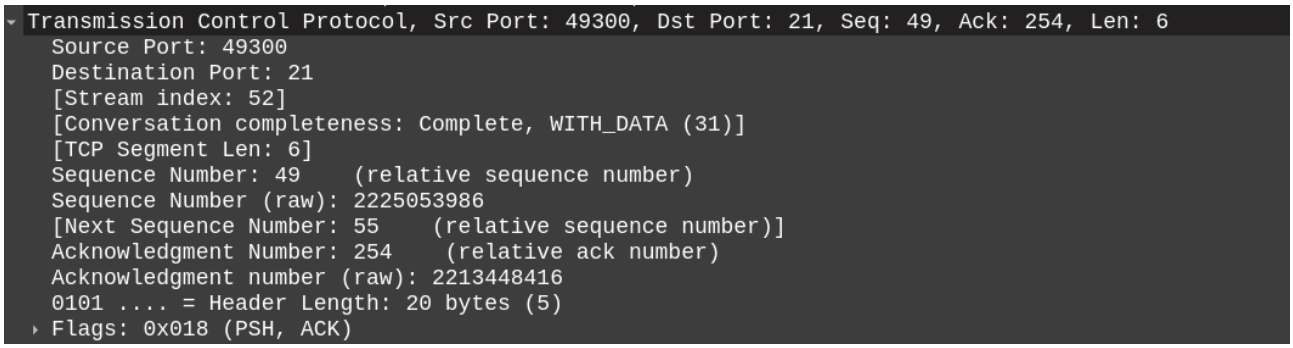
1. Сколько байт данных содержится в пакете FTP-DATA?

Для данного запроса количество байт данных соответствует 242. Ниже представлено подтверждение:

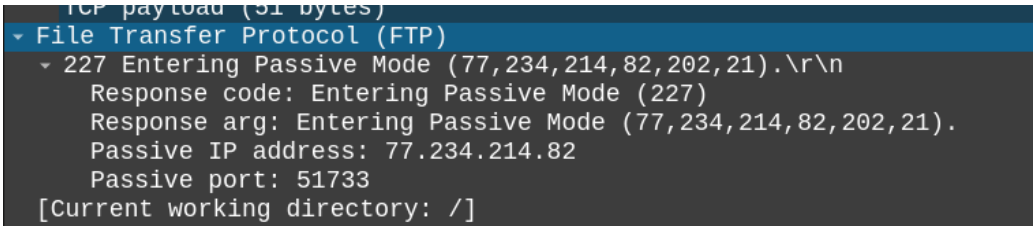


2. Как выбирается порт транспортного уровня, который используется для передачи FTP-пакетов?

Для протокола FTP стандартный порт для управления — 21. На моем компьютере он был выставлен в 49300.



FTP-data использует как правило случайный порт. В сообщении N31 пассивным портом был выставлен 51733, этот порт затем использовался сервером для отправки данных компьютеру. На стороне компьютера был выставлен порт 46330.



3. Чем отличаются пакеты FTP от FTP-DATA?

FTP используется для управления каналом: аутентификации, навигации и общего управления передачей файлов.

FTP-DATA - отвечает за передачу фактических данных файла между клиентом и сервером.

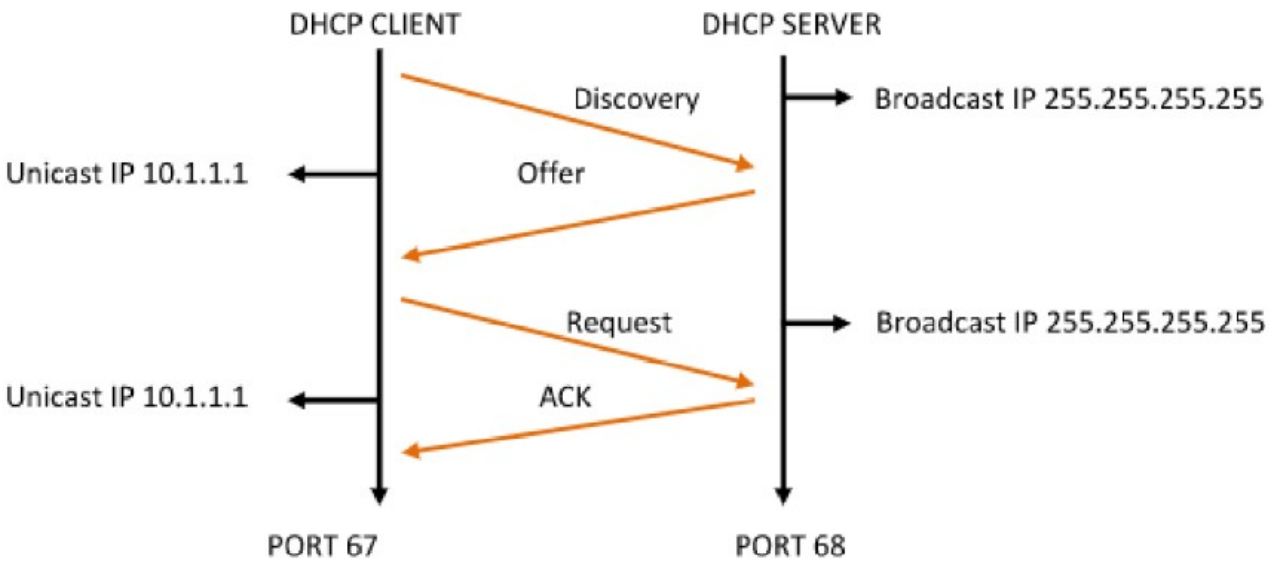
Это можно увидеть по описанию сообщений в Wireshark.

2.8. Анализ DHCP-трафика

Для того, чтобы стриггерить посылку DHCP запросов воспользуемся командами ниже:

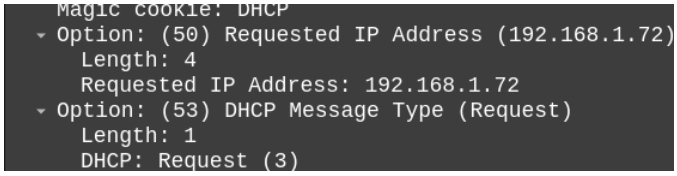
```
nikit@host lab-4 % sudo nmap --script broadcast-dhcp-discover
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-09 19:11 MSK
Pre-scan script results:
| broadcast-dhcp-discover:
|   Response 1 of 1:
|     Interface: wlp2s0
|     IP Offered: 192.168.1.241
|     DHCP Message Type: DHCPOFFER
|     Server Identifier: 192.168.1.197
|     IP Address Lease Time: 59m59s
|     Renewal Time Value: 29m59s
|     Rebinding Time Value: 52m29s
|     Subnet Mask: 255.255.255.0
|     Broadcast Address: 192.168.1.255
|     Router: 192.168.1.197
|     Domain Name Server: 192.168.1.197
|_    Vendor Specific Information: ANDROID_METERED
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 10.23 seconds
nikit@host lab-4 % sudo dhcpcd -T wlp2s0
dhcpcd-9.4.1 starting
```

Благодаря первой команде инициируется discover + offer, благодаря второй — request + ack. То есть компьютер посылает первый запрос, ему от модема (телефона) посылается ответ.



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

DHCP-discover — запрос поиска DHCP-сервера. DHCP-request — запрос на присвоение запрошенного IP адреса (в поле данных указывается).



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

1) DHCP-discover — инициируется клиентом. MAC адрес отправителя — компьютер, IP адрес — 0.0.0.0 (не задан); MAC адрес получателя — broadcast, IP адрес — 255.255.255.255 (limited broadcast — все устройства в локальной сети).

2) DHCP-offer — инициируется сервером. MAC адрес и IP адрес отправителя — сервера; MAC адрес получателя — broadcast, IP адрес получателя — 255.255.255.255.

3) DHCP-request — инициируется клиентом. MAC адрес отправителя — компьютер, IP адрес — 0.0.0.0 (не задан); MAC адрес получателя — broadcast, IP адрес — 255.255.255.255 (limited broadcast)

4) DHCP-ack — инициируется сервером. MAC адрес и IP адрес отправителя — сервера; MAC адрес получателя — компьютер, IP адрес — запрошенный в DHCP-request.

3. Каков IP-адрес DHCP-сервера?

192.168.1.197

```
▸ User Datagram Protocol, Src Port: 67, Dst Port: 68
▾ Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x5cfcdd90
    Seconds elapsed: 0
  ▸ Bootp flags: 0x8000, Broadcast flag (Broadcast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.241
    Next server IP address: 192.168.1.197
```

4. Что произойдёт, если очистить использованный фильтр «bootp» (dhcp)?

Поскольку это был единственный фильтр, то будут просто отображаться все запросы-ответы.

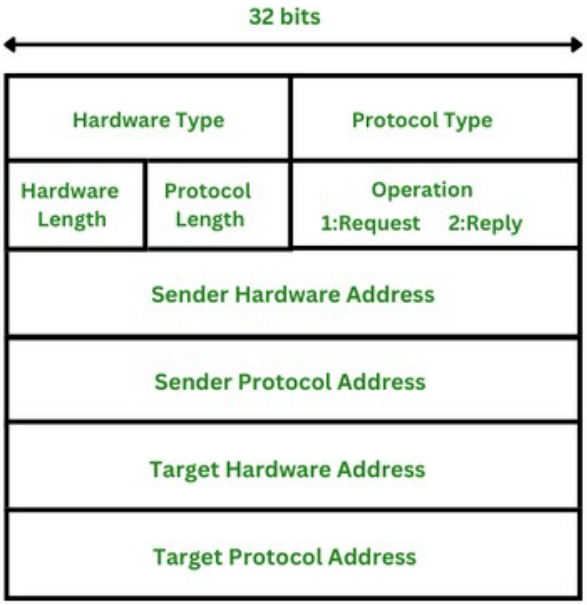
2.9. Структуры наблюдаемых пакетов заголовков

2.9.1. Ethernet II

Адрес получателя	Адрес отправителя	Тип	Данные	CRC
6	6	2	46 ... 1500	4

Источник : intuit

2.9.2. ARP



Источник: [geeksforgeeks]

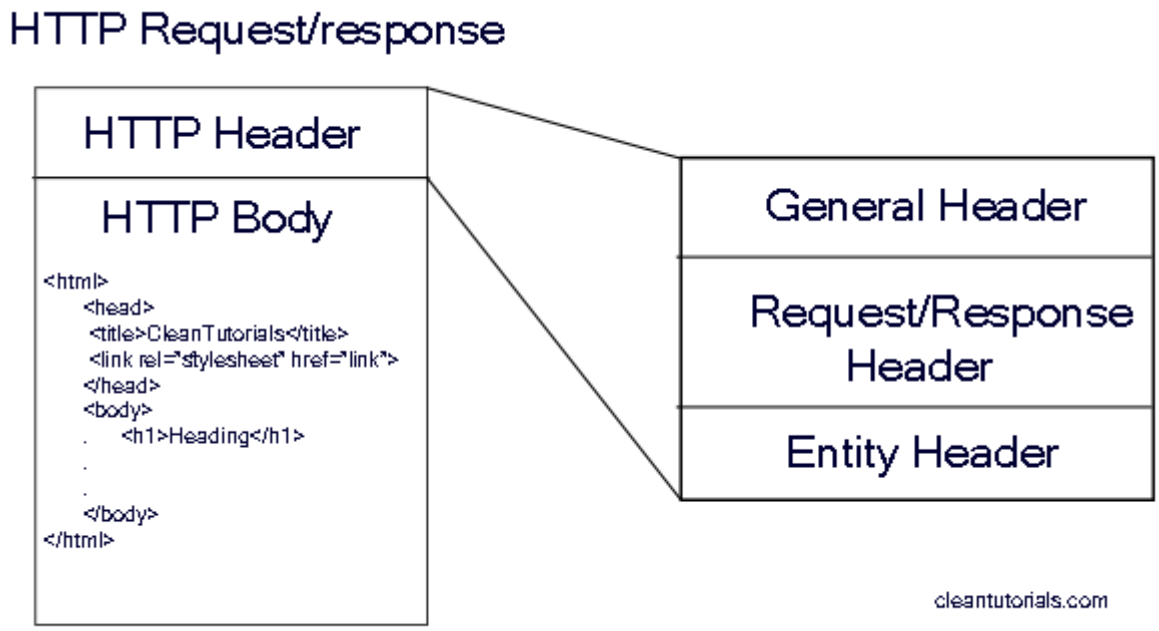
2.9.3. IPv4

Источник: Презентация №2 лекции по Компьютерным сетям, Алиев Тауфик Измайлович, 2023.

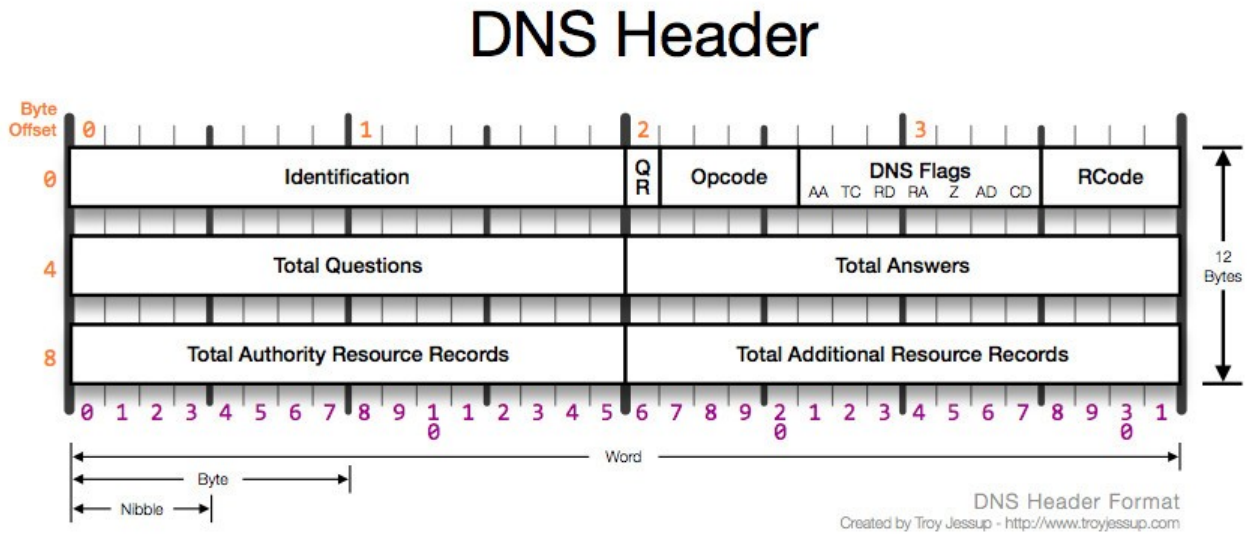
2.9.4. ICMP

Источник: Презентация №2 лекции по Компьютерным сетям, Алиев Тауфик Измайлович, 2023.

2.9.5. HTTP

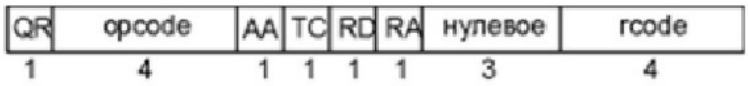


2.9.6. DNS



Identification — позволяет клиенту определить, на какой запрос пришел отклик.

Флаги:



где,
QR - тип сообщения
opcode - код операции
AA - авторитетный ответ
TC - "обрезано"
RD - "требуется рекурсия"
RA - "рекурсия возможна"
rcode - код возврата

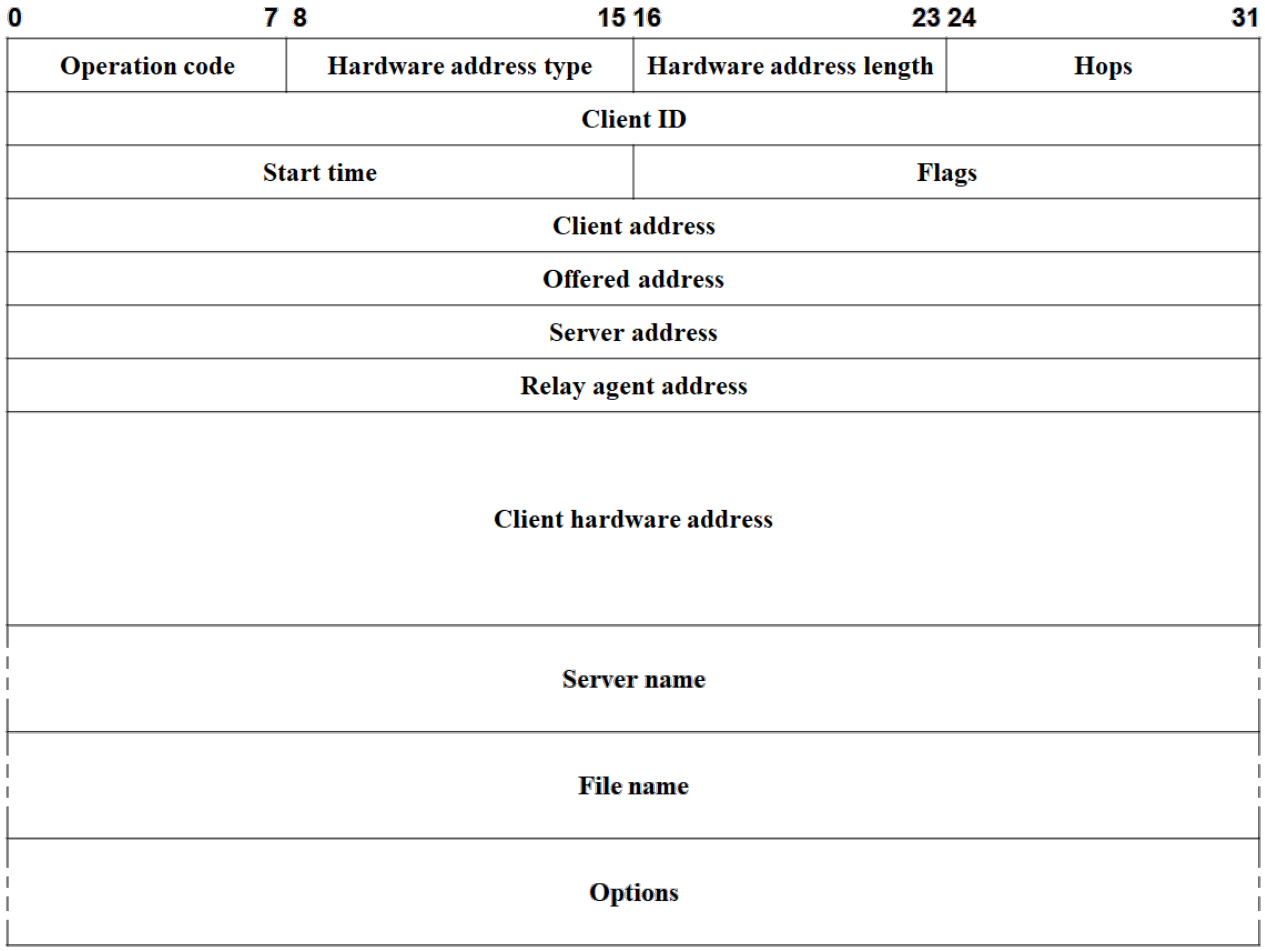
Следующие четыре 16-битных поля указывают на количество пунктов в четырех полях переменной длины, которые завершают запись. В запросе number of questions обычно равно 1, а остальные три счетчика равны 0. В отклике number of answers по меньшей мере равно 1, а оставшиеся два счетчика могут быть как нулевыми, так и ненулевыми.

2.9.7. FTP

Зависит от текущего режима работы (активный, пассивный). Подробнее здесь:

https://www.rhyshaden.com/ftp.htm

2.9.8. DHCP



Источник: [wikimedia commons]

- Operation code - тип DHCP-сообщения. Если значение 0×01 – запрос к серверу, иначе — оно являет ответом DHCP-сервера.
- Hardware Type - тип адреса на канальном уровне. DHCP может работать поверх различных протоколов на канальном уровне, поэтому нужно указывать на каком именно.
- Hardware Length - длина аппаратного адреса в байтах.
- Hops - количество промежуточных маршрутизаторов, которые находятся на пути между клиентом и сервером.
- Transaction ID – идентификатор процесса получения IP-адреса.

- Seconds Elapsed - время в секундах с момента начала процесса получения IP.
- Flags - поле для флагов и параметров протокола.
- Client IP Address - IP-адрес клиента. Не пусто, если у клиента уже есть IP и он хочет продлить время аренды IP-адреса.
- Your ID Address – предложенный DHCP-серверов IP клиенту.
- Server IP Address - IP-адрес сервера.
- Client Hardware Address – MAC клиента.
- Server Hostname – доменное имя сервера (если присуттвует).
- Boot File - служит указателем для бездисковых рабочих станций о имени файла инициализации на сервере.
- Options – информация для динамической конфигурации хоста.

3. Выводы

В ходе выполнения лабораторной работы с помощью программы Wireshark убедился в том, каким образом представляются пакеты, как они оборачивают при проходе от соседних уровней или одного и того же уровня, как в пакете IPv4 лежит ICMP пакет, который принадлежит как и IP сетевому уровню. В целом, подтвердились те знания, которые были получены на лекции.