АРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧЕРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

“НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО”

Факультет ПИиКТ

ОТЧЁТ

По лабораторной работе №4

По предмету: Компьютерные сети

Студент:

Андрейченко Леонид Вадимович

Группа P33301

Преподаватель:

Алиев Тауфик Измайлович

Санкт-Петербург

2023

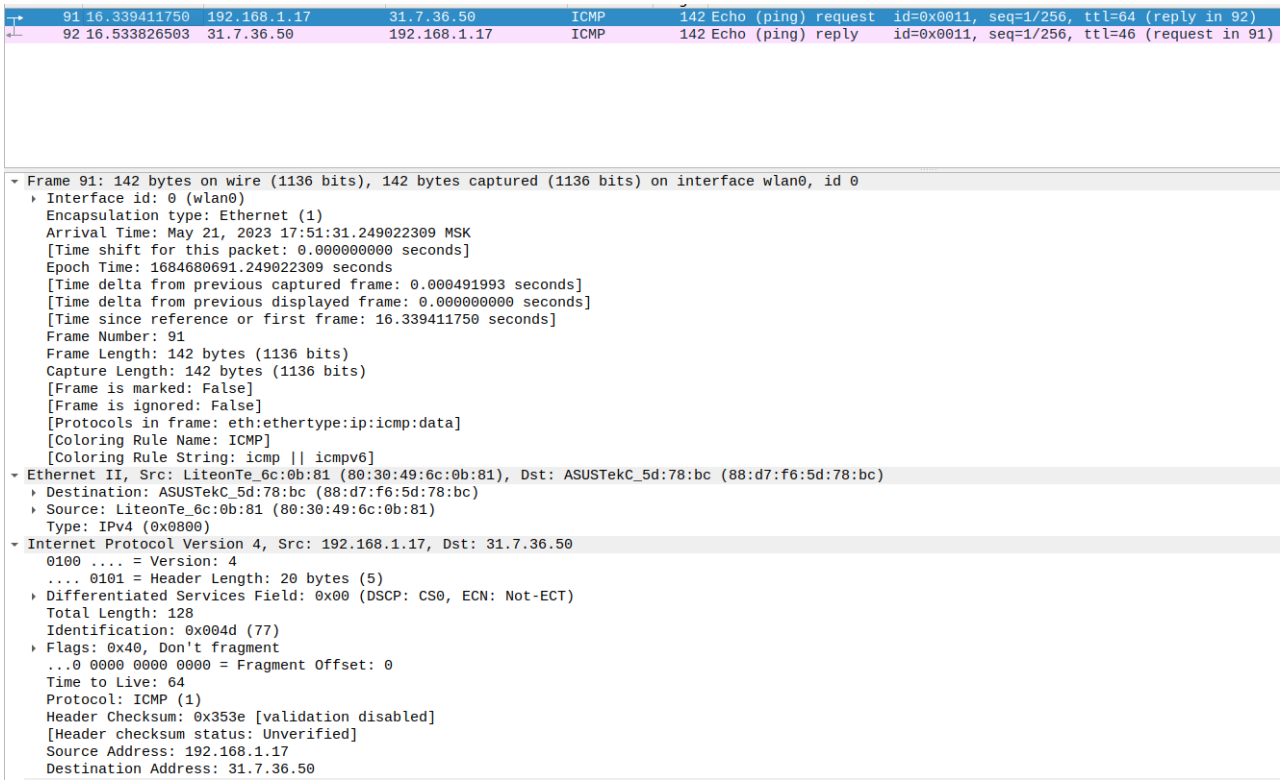
Вариант

http://www.alvadonna.com - Андрейченко Леонид Вадимович

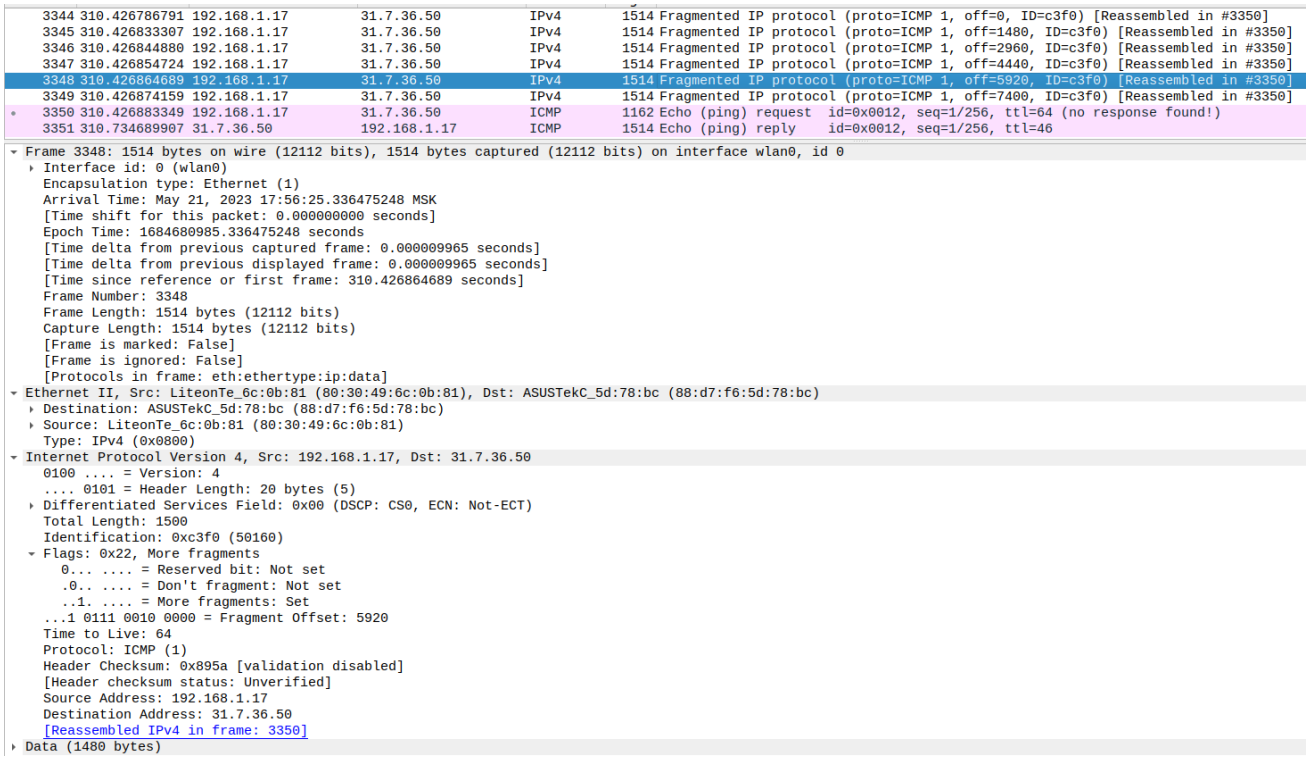
Анализ трафика утилиты ping

ping -s 100 -c 1 alvadonna.com

Пример отправки пакета размером в 100 байт



Пример отправки пакета размером в 10000 байт



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

Да, имеет место фрагментация пакета. Указано в поле MF IPv4 пакета. Пакет начинает фрагментироваться, когда его размер (с учетом заголовка) превышает 1500 байт, это 1480 байт данных.

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

Последний фрагмент можно идентифицировать по ненулевому смещению (это значит, что в пакеты были ещё фрагменты до него), но флаг MF отсутствует (значит, что больше фрагментов пакета не будет

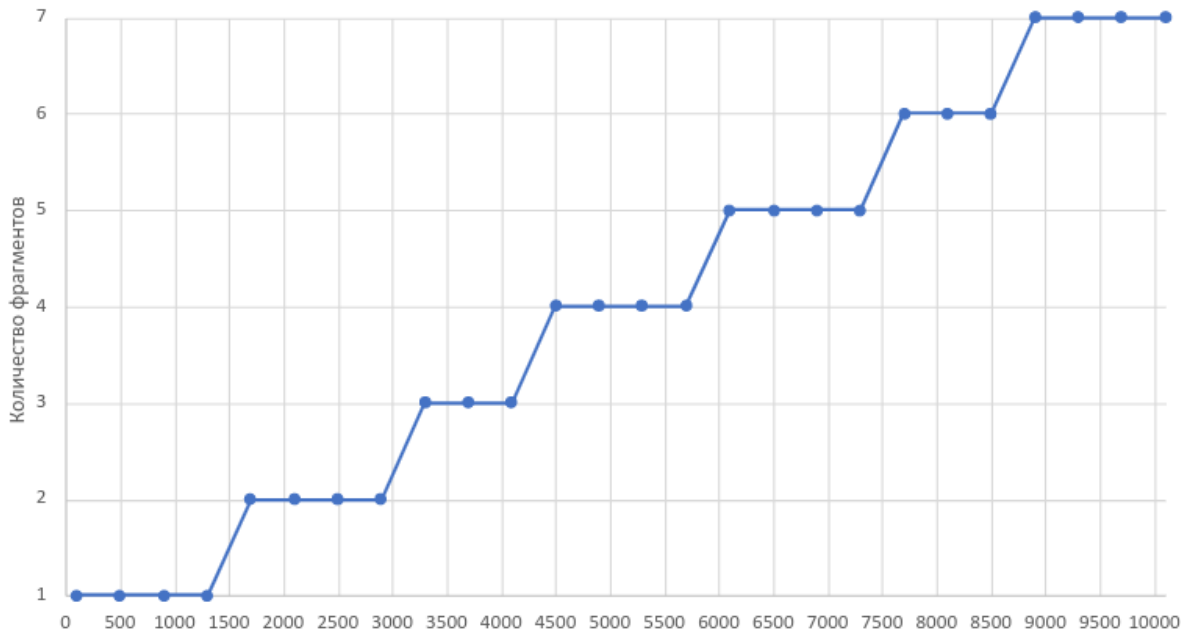
Промежуточный пакет иметь и ненулевое смещение, и установленный флаг MF.

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

Количество фрагментов зависит от соответствующего соединению MTU (Maximum Transmission Unit – максимальный размер передаваемого блока), а также от размера пакетов.

Можно вывести формулу if (size < mtu) -> size; else flour(size / mtu)

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



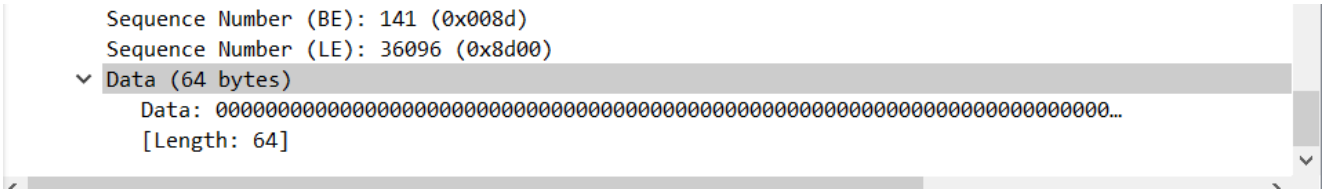
5. Использовать флаг -t <ttl> аргументом которого будет срок жизни пакета в миллисекундах.
6. Символы английского алфавита

Анализ утилиты traceroute

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

Заголовок: 20 байт, данные: 64.

```
> Ethernet II, Src: D-LinkIn_5f:46:2a (84:c9:b2:5f:46:2a), Dst: 9a:22:46:d6:45:a1 (9a:22:46:d6:45:a1)
v Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.103
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 120
```



2. Как и почему изменяется поле TTL в следующих друг за другом ICMP пакетах tracert?

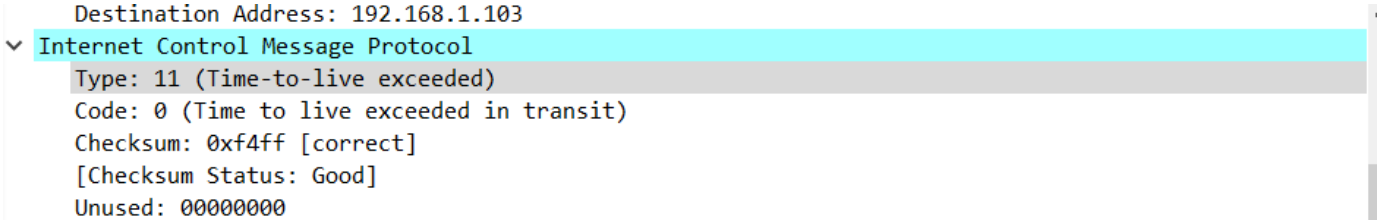
Увеличивается на 1. Это сделано для того, чтобы получать от каждого промежуточного узла IP-адрес, тем самым построив карту маршрута.

3. Чем отличаются ICMP-пакеты, генерируемые утилитой tracert, от ICMPпакетов, генерируемых утилитой ping

В ping-пакетах есть отметка времени, дефолтное значение TTL сильно выше, не меняется со следующим пакетом (в силу специфики утилиты). Содержимым поля data - здесь это нули, а в ping был алфавит.

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

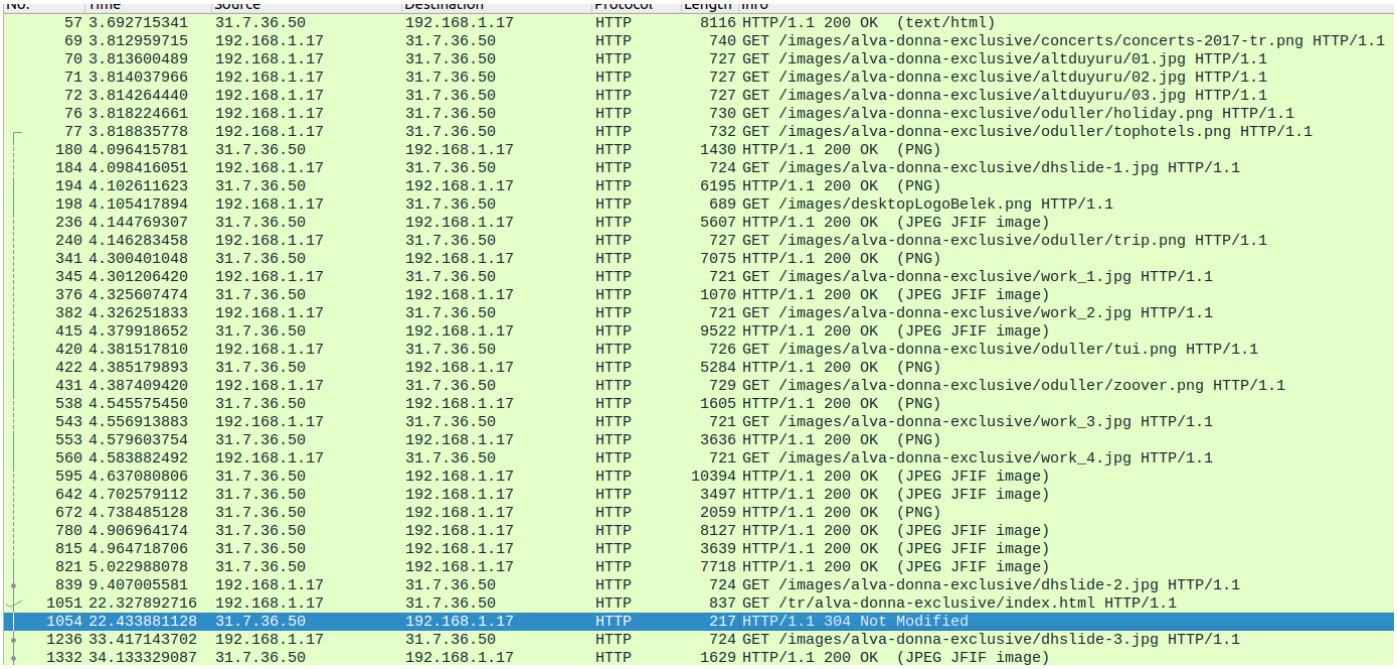
Различные значения в поле Type. Error возвращают ошибочные ответы, reply - обычный ответ на запрос от сервера. Оба типа нужны чтобы различать причину истечению TTL – в случае успешного достижения хоста приходит reply, а в случае ошибки error.



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

Ключ -d в версии linux, позволяет включить отладку на уровне сокета

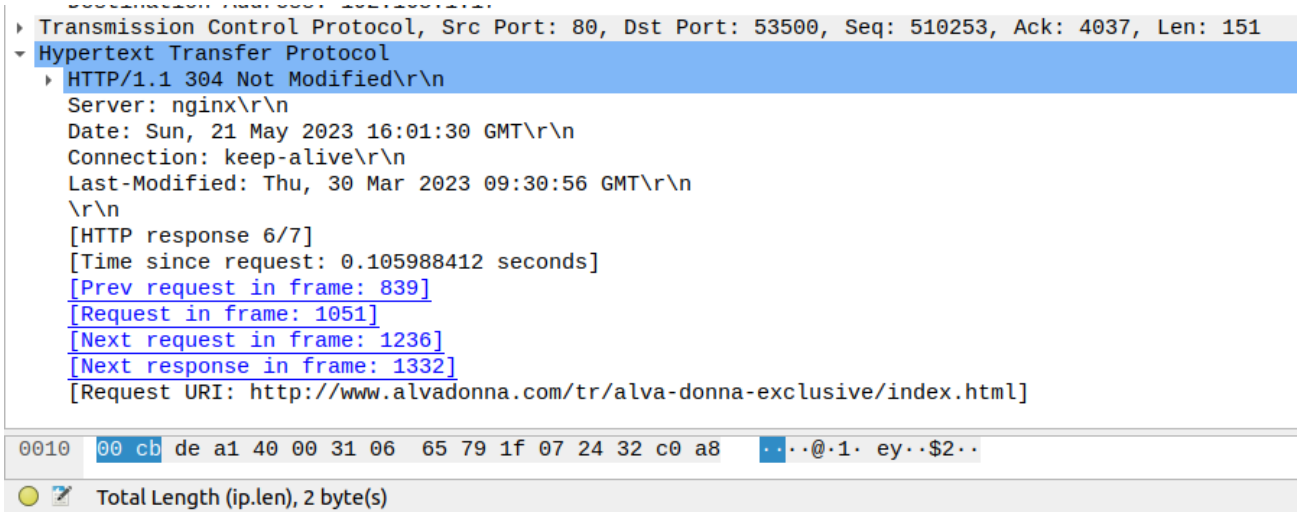
Анализ HTTP-трафика



No.	Time	Source	Destination	Protocol	Length	Info
57	3.692715341	31.7.36.50	192.168.1.17	HTTP	8116	HTTP/1.1 200 OK (text/html)
69	3.812959715	192.168.1.17	31.7.36.50	HTTP	740	GET /images/alva-donna-exclusive/concerts/concerts-2017-tr.png HTTP/1.1
70	3.813600489	192.168.1.17	31.7.36.50	HTTP	727	GET /images/alva-donna-exclusive/altduyuru/01.jpg HTTP/1.1
71	3.814037966	192.168.1.17	31.7.36.50	HTTP	727	GET /images/alva-donna-exclusive/altduyuru/02.jpg HTTP/1.1
72	3.814264440	192.168.1.17	31.7.36.50	HTTP	727	GET /images/alva-donna-exclusive/altduyuru/03.jpg HTTP/1.1
76	3.818224661	192.168.1.17	31.7.36.50	HTTP	730	GET /images/alva-donna-exclusive/oduller/holiday.png HTTP/1.1
77	3.818835778	192.168.1.17	31.7.36.50	HTTP	732	GET /images/alva-donna-exclusive/oduller/tophotels.png HTTP/1.1
180	4.096415781	31.7.36.50	192.168.1.17	HTTP	1430	HTTP/1.1 200 OK (PNG)
184	4.098416051	192.168.1.17	31.7.36.50	HTTP	724	GET /images/alva-donna-exclusive/dhslide-1.jpg HTTP/1.1
194	4.102611623	31.7.36.50	192.168.1.17	HTTP	6195	HTTP/1.1 200 OK (PNG)
198	4.105417894	192.168.1.17	31.7.36.50	HTTP	689	GET /images/desktopLogoBelek.png HTTP/1.1
236	4.144769307	31.7.36.50	192.168.1.17	HTTP	5607	HTTP/1.1 200 OK (JPEG JFIF image)
240	4.146283458	192.168.1.17	31.7.36.50	HTTP	727	GET /images/alva-donna-exclusive/oduller/trip.png HTTP/1.1
341	4.300401048	31.7.36.50	192.168.1.17	HTTP	7075	HTTP/1.1 200 OK (PNG)
345	4.301206420	192.168.1.17	31.7.36.50	HTTP	721	GET /images/alva-donna-exclusive/work_1.jpg HTTP/1.1
376	4.325607474	31.7.36.50	192.168.1.17	HTTP	1070	HTTP/1.1 200 OK (JPEG JFIF image)
382	4.326251833	192.168.1.17	31.7.36.50	HTTP	721	GET /images/alva-donna-exclusive/work_2.jpg HTTP/1.1
415	4.379918652	31.7.36.50	192.168.1.17	HTTP	9522	HTTP/1.1 200 OK (JPEG JFIF image)
420	4.381517810	192.168.1.17	31.7.36.50	HTTP	726	GET /images/alva-donna-exclusive/oduller/tui.png HTTP/1.1
422	4.385179893	31.7.36.50	192.168.1.17	HTTP	5284	HTTP/1.1 200 OK (PNG)
431	4.387409420	192.168.1.17	31.7.36.50	HTTP	729	GET /images/alva-donna-exclusive/oduller/zoover.png HTTP/1.1
538	4.545575450	31.7.36.50	192.168.1.17	HTTP	1605	HTTP/1.1 200 OK (PNG)
543	4.556913883	192.168.1.17	31.7.36.50	HTTP	721	GET /images/alva-donna-exclusive/work_3.jpg HTTP/1.1
553	4.579603754	31.7.36.50	192.168.1.17	HTTP	3636	HTTP/1.1 200 OK (PNG)
560	4.583882492	192.168.1.17	31.7.36.50	HTTP	721	GET /images/alva-donna-exclusive/work_4.jpg HTTP/1.1
595	4.637080806	31.7.36.50	192.168.1.17	HTTP	10394	HTTP/1.1 200 OK (JPEG JFIF image)
642	4.702579112	31.7.36.50	192.168.1.17	HTTP	3497	HTTP/1.1 200 OK (JPEG JFIF image)
672	4.738485128	31.7.36.50	192.168.1.17	HTTP	2059	HTTP/1.1 200 OK (PNG)
780	4.906964174	31.7.36.50	192.168.1.17	HTTP	8127	HTTP/1.1 200 OK (JPEG JFIF image)
815	4.964718706	31.7.36.50	192.168.1.17	HTTP	3639	HTTP/1.1 200 OK (JPEG JFIF image)
821	5.022988078	31.7.36.50	192.168.1.17	HTTP	7718	HTTP/1.1 200 OK (JPEG JFIF image)
839	9.407005581	192.168.1.17	31.7.36.50	HTTP	724	GET /images/alva-donna-exclusive/dhslide-2.jpg HTTP/1.1
1051	22.327892716	192.168.1.17	31.7.36.50	HTTP	837	GET /tr/alva-donna-exclusive/index.html HTTP/1.1
1054	22.433881128	31.7.36.50	192.168.1.17	HTTP	217	HTTP/1.1 304 Not Modified
1236	33.417143702	192.168.1.17	31.7.36.50	HTTP	724	GET /images/alva-donna-exclusive/dhslide-3.jpg HTTP/1.1
1332	34.133329087	31.7.36.50	192.168.1.17	HTTP	1629	HTTP/1.1 200 OK (JPEG JFIF image)

1. Сначала получаем гипертекст на запрошенном сайте
2. Поочередно получаем необходимые в html тексте скрипты js
3. Поочередно получаем необходимые картинки для отображения содержимого сайта
4. При вторичном запросе-обновлении получаем код ответа 304 “Not modified”, т. к. содержимое страницы не менялось. Данные о сайте остались в кэше браузера.

```
Hypertext Transfer Protocol
  GET /tr/alva-donna-exclusive/index.html HTTP/1.1\r\n
  Host: www.alvadonna.com\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 YaBrowser/23.3.3.706 Yowser/2.5 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
  Referer: http://www.alvadonna.com/\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: ru,en;q=0.9\r\n
  Cookie: _ga=GA1.2.556733594.1684678760; _gid=GA1.2.719053350.1684678760; _ym_uid=1684678760461057024; _ym_d=1684678760; _ym_isad=1; _gcl_au=1.1.898945602
  \r\n
  [Full request URI: http://www.alvadonna.com/tr/alva-donna-exclusive/index.html]
  [HTTP request 1/2]
  [Response in frame: 57]
  [Next request in frame: 69]

0010  03 02 d7 ef 40 00 40 06  5b 14 c0 a8 01 11 1f 07   ····@·@· [·····

Total Length (ip.len), 2 byte(s)                                  Пакеты: 6745 ·
```



```
Transmission Control Protocol, Src Port: 80, Dst Port: 53500, Seq: 510253, Ack: 4037, Len: 151
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
  Server: nginx\r\n
  Date: Sun, 21 May 2023 16:01:30 GMT\r\n
  Connection: keep-alive\r\n
  Last-Modified: Thu, 30 Mar 2023 09:30:56 GMT\r\n
  \r\n
  [HTTP response 6/7]
  [Time since request: 0.105988412 seconds]
  [Prev request in frame: 839]
  [Request in frame: 1051]
  [Next request in frame: 1236]
  [Next response in frame: 1332]
  [Request URI: http://www.alvadonna.com/tr/alva-donna-exclusive/index.html]

0010  00 cb de a1 40 00 31 06  65 79 1f 07 24 32 c0 a8   ····@·1· ey··$2··

Total Length (ip.len), 2 byte(s)
```

Анализ DNS-трафика

```
 99 7.010211847   192.168.1.17    192.168.1.1     DNS      88 Standard query 0x0a4a A www.alvadonna.com OPT
100 7.010423703   192.168.1.17    192.168.1.1     DNS      91 Standard query 0xb569 A cdnjs.cloudflare.com OPT
101 7.010511601   192.168.1.17    192.168.1.1     DNS      84 Standard query 0x889b A alvadonna.com OPT
102 7.012522617   192.168.1.1     192.168.1.17    DNS     131 Standard query response 0x0a4a A www.alvadonna.com CNAME alvadonna.com A 31.7.36.50 OPT
103 7.012941702   192.168.1.1     192.168.1.17    DNS     123 Standard query response 0xb569 A cdnjs.cloudflare.com A 104.17.24.14 A 104.17.25.14 OPT
104 7.013206379   192.168.1.1     192.168.1.17    DNS     100 Standard query response 0x889b A alvadonna.com A 31.7.36.50 OPT
```

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

После очистки кэша, адрес необходимого нам сайта отсутствует в локальной памяти и нужно сначала получить с DNS-сервера, где из таблиц сопоставления будет получен IP по домену. Адрес отправки соответствует шлюзу по умолчанию.

2. Какие бывают типы DNS-запросов?

- Прямой - преобразование домена в IP-адрес.
- Обратный – преобразование IP-адреса в домен.
- Рекурсивный – DNS-сервер опрашивает другие сервера, пока не найдёт ответ или не обнаружит, что домен не существует.
- Итеративный – тоже самое, что рекурсивный, но также допускается выполнение поиска клиентом.

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

Выполнять дополнительные DNS запросы необходимо, когда картинки лежат на другом доменном имени, а не на том же хосте.

Анализ ARP-трафика

```
 112 15.042535413  ASUSTekC_5d:78:bc  LiteonTe_6c:0b:81  ARP      42 Who has 192.168.1.17? Tell 192.168.1.1
 113 15.042547782  LiteonTe_6c:0b:81  ASUSTekC_5d:78:bc  ARP      42 192.168.1.17 is at 80:30:49:6c:0b:81
1348 65.526711443  ASUSTekC_5d:78:bc  LiteonTe_6c:0b:81  ARP      42 Who has 192.168.1.17? Tell 192.168.1.1
1349 65.526742143  LiteonTe_6c:0b:81  ASUSTekC_5d:78:bc  ARP      42 192.168.1.17 is at 80:30:49:6c:0b:81
1638 97.987514070  LiteonTe_6c:0b:81  Broadcast          ARP      42 Who has 192.168.1.1? Tell 192.168.1.17
1639 97.996198907  ASUSTekC_5d:78:bc  LiteonTe_6c:0b:81  ARP      42 192.168.1.1 is at 88:d7:f6:5d:78:bc
1844 115.006760099 ASUSTekC_5d:78:bc  LiteonTe_6c:0b:81  ARP      42 Who has 192.168.1.17? Tell 192.168.1.1
1845 115.006786928 LiteonTe_6c:0b:81  ASUSTekC_5d:78:bc  ARP      42 192.168.1.17 is at 80:30:49:6c:0b:81
```

```
▸ Frame 112: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlan0, id 0
▸ Ethernet II, Src: ASUSTekC_5d:78:bc (88:d7:f6:5d:78:bc), Dst: LiteonTe_6c:0b:81 (80:30:49:6c:0b:81)
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: ASUSTekC_5d:78:bc (88:d7:f6:5d:78:bc)
    Sender IP address: 192.168.1.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.17
```

```
 112 15.042535413  ASUSTekC_5d:78:bc  LiteonTe_6c:0b:81  ARP      42 Who has 192.168.1.17? Tell 192.168.1.1
 113 15.042547782  LiteonTe_6c:0b:81  ASUSTekC_5d:78:bc  ARP      42 192.168.1.17 is at 80:30:49:6c:0b:81
1348 65.526711443  ASUSTekC_5d:78:bc  LiteonTe_6c:0b:81  ARP      42 Who has 192.168.1.17? Tell 192.168.1.1
1349 65.526742143  LiteonTe_6c:0b:81  ASUSTekC_5d:78:bc  ARP      42 192.168.1.17 is at 80:30:49:6c:0b:81
1638 97.987514070  LiteonTe_6c:0b:81  Broadcast          ARP      42 Who has 192.168.1.1? Tell 192.168.1.17
1639 97.996198907  ASUSTekC_5d:78:bc  LiteonTe_6c:0b:81  ARP      42 192.168.1.1 is at 88:d7:f6:5d:78:bc
1844 115.006760099 ASUSTekC_5d:78:bc  LiteonTe_6c:0b:81  ARP      42 Who has 192.168.1.17? Tell 192.168.1.1
1845 115.006786928 LiteonTe_6c:0b:81  ASUSTekC_5d:78:bc  ARP      42 192.168.1.17 is at 80:30:49:6c:0b:81
```

```
▸ Frame 113: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlan0, id 0
▸ Ethernet II, Src: LiteonTe_6c:0b:81 (80:30:49:6c:0b:81), Dst: ASUSTekC_5d:78:bc (88:d7:f6:5d:78:bc)
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: LiteonTe_6c:0b:81 (80:30:49:6c:0b:81)
    Sender IP address: 192.168.1.17
    Target MAC address: ASUSTekC_5d:78:bc (88:d7:f6:5d:78:bc)
    Target IP address: 192.168.1.1
```

1. MAC-адреса

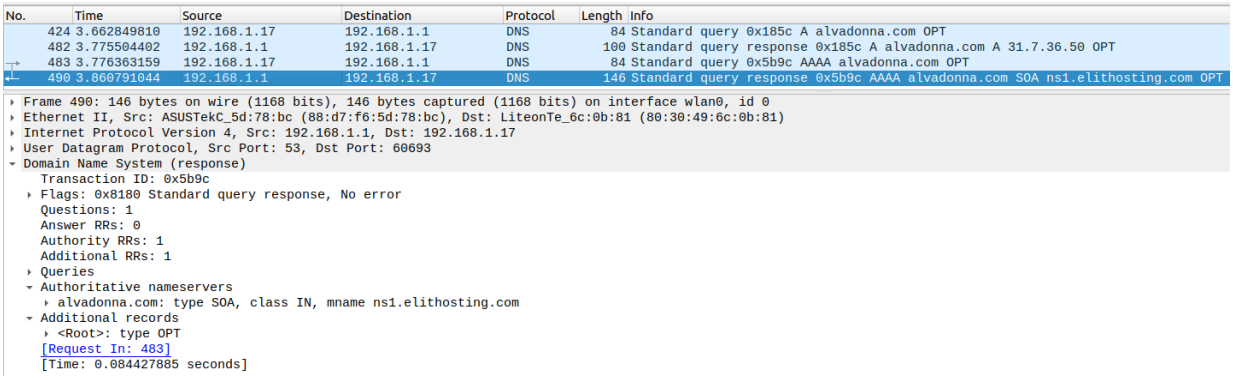
- 88:f7:d6:5d:78:bc- MAC-адрес нашего устройства
- 00:00:00:00:00:00 - MAC заполнитель, пока не будет получен реальный адрес
- 80:30:49:6c:0b:81 - MAC-адрес маршрутизатора

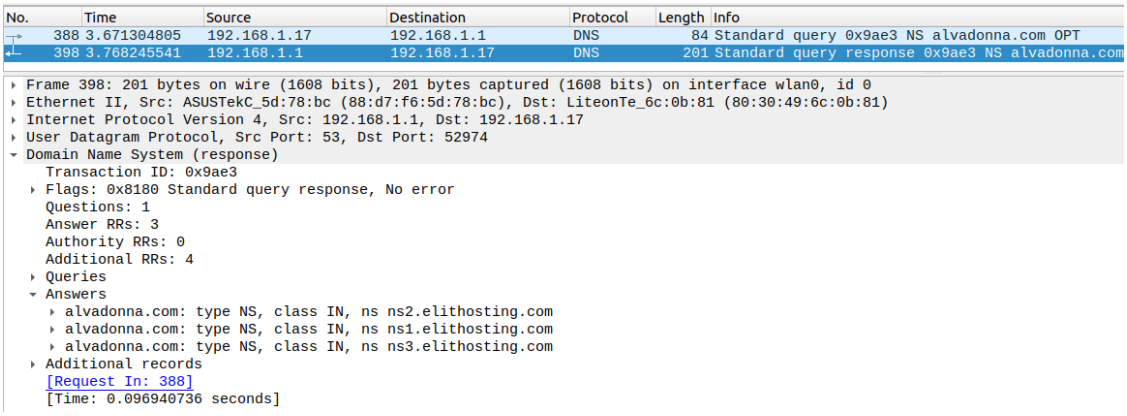
2. Те же самые, что и в первом пункте

3. IP адрес содержится в запросе по следующим причинам:

- Во-первых, этот адрес нужен для заполнения ARP-таблицы.
- Во-вторых, чтобы можно был сразу ответить на запрос, не отправляя ответный запрос

Анализ трафика утилиты nslookup



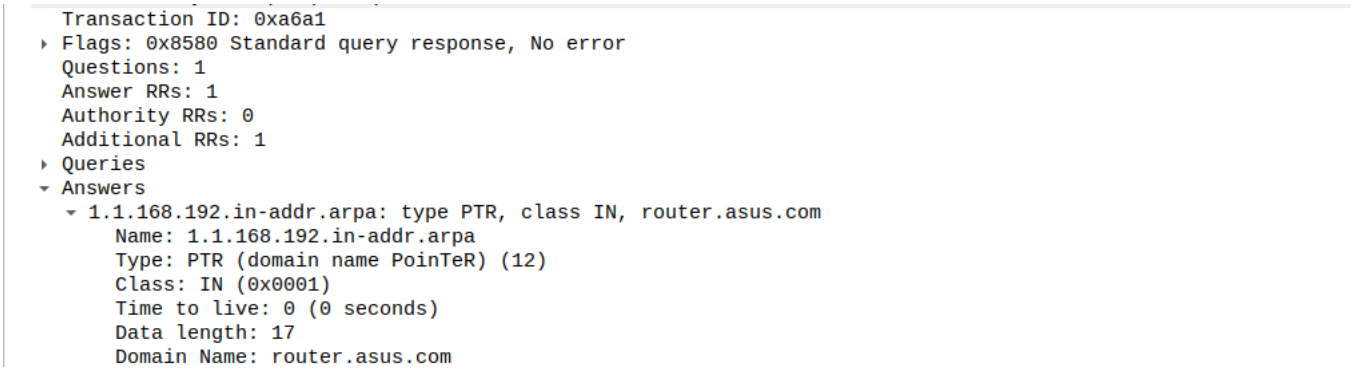


1. Чем различается трасса трафика в п.2 и п.4, указанных выше?

В п.2 DNS-ответе содержится IP сайта требуемого по имени сайта, в п.4 имена авторитативных серверов.

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

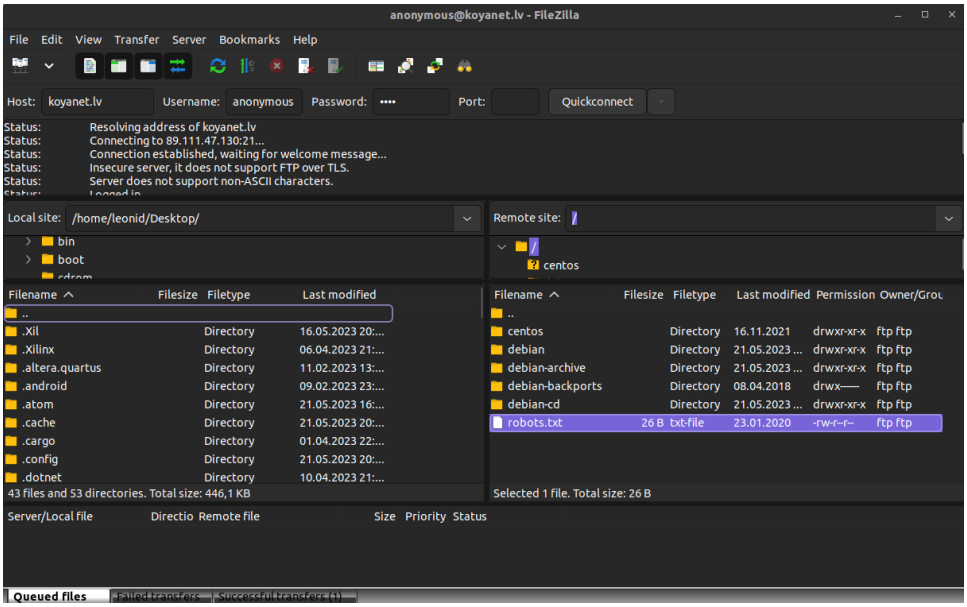
Имя хоста, тип и класс записи, TTL, длина поля данных, IP-адрес запрашиваемого хоста.



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

Авторитарной сервер лишь один – поставщик услуг ddns.

Анализ FTP-трафика



No.	Time	Source	Destination	Protocol	Length	Info
221	36.883089323	89.111.47.130	192.168.1.17	FTP	82	Response: 220 koyanet.lv
223	36.883218916	192.168.1.17	89.111.47.130	FTP	76	Request: AUTH TLS
225	36.900322423	89.111.47.130	192.168.1.17	FTP	104	Response: 530 Please login with USER and PASS.
226	36.900449580	192.168.1.17	89.111.47.130	FTP	76	Request: AUTH SSL
227	36.919370272	89.111.47.130	192.168.1.17	FTP	104	Response: 530 Please login with USER and PASS.
228	36.919733400	192.168.1.17	89.111.47.130	FTP	82	Request: USER anonymous
229	36.935948820	89.111.47.130	192.168.1.17	FTP	100	Response: 331 Please specify the password.
230	36.936089502	192.168.1.17	89.111.47.130	FTP	77	Request: PASS anon
231	36.957116176	89.111.47.130	192.168.1.17	FTP	89	Response: 230 Login successful.
232	36.957761193	192.168.1.17	89.111.47.130	FTP	73	Request: CWD /
234	36.972420244	89.111.47.130	192.168.1.17	FTP	103	Response: 250 Directory successfully changed.
235	36.972552016	192.168.1.17	89.111.47.130	FTP	71	Request: PWD
236	36.987476245	89.111.47.130	192.168.1.17	FTP	100	Response: 257 "/" is the current directory
237	36.987727703	192.168.1.17	89.111.47.130	FTP	74	Request: TYPE A
238	37.006602383	89.111.47.130	192.168.1.17	FTP	96	Response: 200 Switching to ASCII mode.
239	37.006721291	192.168.1.17	89.111.47.130	FTP	72	Request: PASV
240	37.021641711	89.111.47.130	192.168.1.17	FTP	118	Response: 227 Entering Passive Mode (89,111,47,130,204,241).
241	37.021850030	192.168.1.17	89.111.47.130	FTP	83	Request: RETR robots.txt
245	37.052333788	89.111.47.130	192.168.1.17	FTP	134	Response: 150 Opening BINARY mode data connection for robots.txt (26 bytes).
246	37.052333952	89.111.47.130	192.168.1.17	FTP-DATA	92	FTP Data: 26 bytes (PASV) (RETR robots.txt)
251	37.070027188	89.111.47.130	192.168.1.17	FTP	90	Response: 226 Transfer complete.

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

В моем случае 26 байт данных

```
    245 37.052333788  89.111.47.130  192.168.1.17  FTP       134 Response: 150 Opening BINARY mode data connec
    246 37.052333952  89.111.47.130  192.168.1.17  FTP-DATA   92 FTP Data: 26 bytes (PASV) (RETR robots.txt)
    251 37.070027188  89.111.47.130  192.168.1.17  FTP        90 Response: 226 Transfer complete.
```

```
▸ Frame 246: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface wlan0, id 0
▸ Ethernet II, Src: ASUSTekC_5d:78:bc (88:d7:f6:5d:78:bc), Dst: LiteonTe_6c:0b:81 (80:30:49:6c:0b:81)
▸ Internet Protocol Version 4, Src: 89.111.47.130, Dst: 192.168.1.17
▸ Transmission Control Protocol, Src Port: 52465, Dst Port: 60659, Seq: 1, Ack: 1, Len: 26
  FTP Data (26 bytes data)
  [Setup frame: 240]
  [Setup method: PASV]
  [Command: RETR robots.txt]
  Command frame: 241
  [Current working directory: /]
▸ Line-based text data (2 lines)
```

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

Для FTP используется порт 21, передающий управляющие сообщения. Для FTP-DATA может быть выбран любой порт, но по умолчанию используется 20. Для передачи файлов используется свободный порт.

```
    245 37.052333788  89.111.47.130  192.168.1.17  FTP       134 Response: 150 Opening BINARY mode data connection for robots.txt (26 bytes).
    246 37.052333952  89.111.47.130  192.168.1.17  FTP-DATA   92 FTP Data: 26 bytes (PASV) (RETR robots.txt)
    251 37.070027188  89.111.47.130  192.168.1.17  FTP        90 Response: 226 Transfer complete.
```

```
▸ Frame 245: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface wlan0, id 0
▸ Ethernet II, Src: ASUSTekC_5d:78:bc (88:d7:f6:5d:78:bc), Dst: LiteonTe_6c:0b:81 (80:30:49:6c:0b:81)
▸ Internet Protocol Version 4, Src: 89.111.47.130, Dst: 192.168.1.17
▾ Transmission Control Protocol, Src Port: 21, Dst Port: 52758, Seq: 303, Ack: 91, Len: 68
    Source Port: 21
    Destination Port: 52758
    [Stream index: 26]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 68]
    Sequence Number: 303    (relative sequence number)
    Sequence Number (raw): 3448149473
    [Next Sequence Number: 371    (relative sequence number)]
    Acknowledgment Number: 91    (relative ack number)
    Acknowledgment number (raw): 828832998
    1000 .... = Header Length: 32 bytes (8)
```

3. Чем отличаются пакеты FTP от FTP-DATA?

FTP передаёт команды серверу, а FTP-DATA работает с файлами.

Запрос на скачивание файла

```
  241 37.021850030  192.168.1.17   89.111.47.130   FTP        83 Request: RETR robots.txt
  245 37.052333788  89.111.47.130  192.168.1.17    FTP       134 Response: 150 Opening BINARY mode data connection for
  246 37.052333952  89.111.47.130  192.168.1.17    FTP-DATA   92 FTP Data: 26 bytes (PASV) (RETR robots.txt)
  251 37.070027188  89.111.47.130  192.168.1.17    FTP        90 Response: 226 Transfer complete.

▸ Frame 241: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface wlan0, id 0
▸ Ethernet II, Src: LiteonTe_6c:0b:81 (80:30:49:6c:0b:81), Dst: ASUSTekC_5d:78:bc (88:d7:f6:5d:78:bc)
▸ Internet Protocol Version 4, Src: 192.168.1.17, Dst: 89.111.47.130
▸ Transmission Control Protocol, Src Port: 52758, Dst Port: 21, Seq: 74, Ack: 303, Len: 17
▾ File Transfer Protocol (FTP)
  ▾ RETR robots.txt\r\n
      Request command: RETR
      Request arg: robots.txt
  [Current working directory: /]
  [Command response frames: 1]
  [Command response bytes: 26]
  [Command response first frame: 246]
  [Command response last frame: 246]
  [Setup frame: 240]
```

Непосредственно загрузка

```
  246 37.052333952  89.111.47.130  192.168.1.17    FTP-DATA   92 FTP Data: 26 bytes (PASV) (RETR robots.txt)
  251 37.070027188  89.111.47.130  192.168.1.17    FTP        90 Response: 226 Transfer complete.

▸ Frame 246: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface wlan0, id 0
▸ Ethernet II, Src: ASUSTekC_5d:78:bc (88:d7:f6:5d:78:bc), Dst: LiteonTe_6c:0b:81 (80:30:49:6c:0b:81)
▸ Internet Protocol Version 4, Src: 89.111.47.130, Dst: 192.168.1.17
▸ Transmission Control Protocol, Src Port: 52465, Dst Port: 60659, Seq: 1, Ack: 1, Len: 26
  FTP Data (26 bytes data)
  [Setup frame: 240]
  [Setup method: PASV]
  [Command: RETR robots.txt]
  Command frame: 241
  [Current working directory: /]
▾ Line-based text data (2 lines)
    User-agent: *\n
    Disallow: /\n
```

Анализ DHCP-трафика

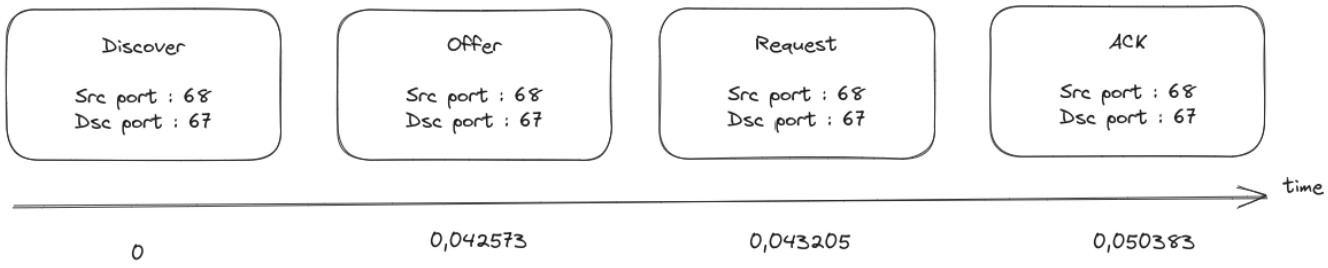
```
leonid-lenovo# dhclient -r
Killed old client process
leonid-lenovo# dhclient
```

```
  1899 69.732816433  0.0.0.0          255.255.255.255  DHCP  342 DHCP Discover - Transaction ID 0xe916016
  1901 69.783320994  192.168.1.1      192.168.1.17     DHCP  342 DHCP Offer    - Transaction ID 0xe916016
  1902 69.784017660  0.0.0.0          255.255.255.255  DHCP  342 DHCP Request  - Transaction ID 0xe916016
  1903 69.796524688  192.168.1.1      192.168.1.17     DHCP  349 DHCP ACK      - Transaction ID 0xe916016

▸ Frame 1899: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface wlan0, id 0
▸ Ethernet II, Src: LiteonTe_6c:0b:81 (80:30:49:6c:0b:81), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
▸ User Datagram Protocol, Src Port: 68, Dst Port: 67
▾ Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x0e916016
    Seconds elapsed: 0
  ▸ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: LiteonTe_6c:0b:81 (80:30:49:6c:0b:81)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▸ Option: (53) DHCP Message Type (Discover)
  ▸ Option: (50) Requested IP Address (192.168.1.17)
  ▸ Option: (12) Host Name
  ▸ Option: (55) Parameter Request List
  ▸ Option: (255) End
    Padding: 00000000000000000000000000000000000000000000
```

```
  1899 69.732816433  0.0.0.0          255.255.255.255  DHCP  342 DHCP Discover - Transaction ID 0xe916016
  1901 69.783320994  192.168.1.1      192.168.1.17     DHCP  342 DHCP Offer    - Transaction ID 0xe916016
  1902 69.784017660  0.0.0.0          255.255.255.255  DHCP  342 DHCP Request  - Transaction ID 0xe916016
  1903 69.796524688  192.168.1.1      192.168.1.17     DHCP  349 DHCP ACK      - Transaction ID 0xe916016

▸ Frame 1901: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface wlan0, id 0
▸ Ethernet II, Src: ASUSTekC_5d:78:bc (88:d7:f6:5d:78:bc), Dst: LiteonTe_6c:0b:81 (80:30:49:6c:0b:81)
▸ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.17
▸ 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: 0x0e916016
    Seconds elapsed: 0
  ▸ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.17
    Next server IP address: 192.168.1.1
    Relay agent IP address: 0.0.0.0
    Client MAC address: LiteonTe_6c:0b:81 (80:30:49:6c:0b:81)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▸ Option: (53) DHCP Message Type (Offer)
  ▸ Option: (54) DHCP Server Identifier (192.168.1.1)
  ▸ Option: (51) IP Address Lease Time
  ▸ Option: (58) Renewal Time Value
  ▸ Option: (59) Rebinding Time Value
  ▸ Option: (1) Subnet Mask (255.255.255.0)
  ▸ Option: (28) Broadcast Address (192.168.1.255)
  ▸ Option: (6) Domain Name Server
  ▸ Option: (3) Router
  ▸ Option: (255) End
    Padding: 0000000000000000
```

```
  1899 69.732816433  0.0.0.0          255.255.255.255  DHCP  342 DHCP Discover - Transaction ID 0xe916016
  1901 69.783320994  192.168.1.1      192.168.1.17     DHCP  342 DHCP Offer    - Transaction ID 0xe916016
  1902 69.784017660  0.0.0.0          255.255.255.255  DHCP  342 DHCP Request  - Transaction ID 0xe916016
  1903 69.796524688  192.168.1.1      192.168.1.17     DHCP  349 DHCP ACK      - Transaction ID 0xe916016

▸ Frame 1902: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface wlan0, id 0
▸ Ethernet II, Src: LiteonTe_6c:0b:81 (80:30:49:6c:0b:81), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
▸ User Datagram Protocol, Src Port: 68, Dst Port: 67
▾ Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x0e916016
    Seconds elapsed: 0
  ▸ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: LiteonTe_6c:0b:81 (80:30:49:6c:0b:81)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▸ Option: (53) DHCP Message Type (Request)
  ▸ Option: (54) DHCP Server Identifier (192.168.1.1)
  ▸ Option: (50) Requested IP Address (192.168.1.17)
  ▸ Option: (12) Host Name
  ▸ Option: (55) Parameter Request List
  ▸ Option: (255) End
    Padding: 00000000000000000000000000000000
```

```
  1899 69.732816433  0.0.0.0          255.255.255.255  DHCP  342 DHCP Discover - Transaction ID 0xe916016
  1901 69.783320994  192.168.1.1      192.168.1.17     DHCP  342 DHCP Offer    - Transaction ID 0xe916016
  1902 69.784017660  0.0.0.0          255.255.255.255  DHCP  342 DHCP Request  - Transaction ID 0xe916016
  1903 69.796524688  192.168.1.1      192.168.1.17     DHCP  349 DHCP ACK      - Transaction ID 0xe916016

▸ Frame 1903: 349 bytes on wire (2792 bits), 349 bytes captured (2792 bits) on interface wlan0, id 0
▸ Ethernet II, Src: ASUSTekC_5d:78:bc (88:d7:f6:5d:78:bc), Dst: LiteonTe_6c:0b:81 (80:30:49:6c:0b:81)
▸ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.17
▸ User Datagram Protocol, Src Port: 67, Dst Port: 68
▾ Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x0e916016
    Seconds elapsed: 0
  ▸ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.17
    Next server IP address: 192.168.1.1
    Relay agent IP address: 0.0.0.0
    Client MAC address: LiteonTe_6c:0b:81 (80:30:49:6c:0b:81)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▸ Option: (53) DHCP Message Type (ACK)
  ▸ Option: (54) DHCP Server Identifier (192.168.1.1)
  ▸ Option: (51) IP Address Lease Time
  ▸ Option: (58) Renewal Time Value
  ▸ Option: (59) Rebinding Time Value
  ▸ Option: (1) Subnet Mask (255.255.255.0)
  ▸ Option: (28) Broadcast Address (192.168.1.255)
  ▸ Option: (6) Domain Name Server
  ▸ Option: (12) Host Name
  ▸ Option: (3) Router
  ▸ Option: (255) End
```



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

Пакеты различаются назначением. Discover -запрос поиска, рассылается на все устройства локальной сети, для поиска DHCP-сервера. Если клиент удачно выберет предложенный «DHCP Offer», то отправит «DHCP Request» - этим сообщением он принимает предлагаемый адрес и уведомляет DHCP-сервер об этом.

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

Изначально у отправителя отсутствует IP (0.0.0.0), есть только MAC-адрес, по которому DHCP-сервер отправит ответ Адреса назначения являются широковещательными, чтобы уведомить все устройства, но ответить должен только DHCP-сервер. При отправке Offer или ACK пакетов, адреса источника соответствуют адресам DHCP-сервера, адреса назначения широковещательные.

3. Каков IP-адрес DHCP-сервера?

В качестве DHCP-сервера выступает роутер, чей адрес == 192.168.1.1

Выводы

В ходе выполнения лабораторной работы мною были получены навыки работы с анализатором трафика Wireshark, где были захвачены и изучены пакеты разных протоколов, их расположение по уровням TCP/IP модели, назначение и структура. Сложность работы заключается в объёме информации, в которой очень легко запутаться.