

**Министерство науки и высшего образования Российской Федерации  
федеральное государственное автономное образовательное учреждение высшего образования  
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»  
(Университет ИТМО)**

**Факультет программной инженерии и компьютерной техники**

**Отчет по лабораторной работе №3**

**по дисциплине «Компьютерная сеть»**

**Тема «Анализ трафика компьютерных сетей утилитой Wireshark»**

Выполнила:

студентка гр. № Р33212

Ян Цзяфэн

Санкт-Петербург

2021

## Оглавление

Цель работы.....	3
Вариант .....	3
Задачи.....	3
Анализ трафика утилиты ping.....	3
Анализ трафика утилиты tracert (traceroute) .....	5
Анализ HTTP-трафика .....	7
Анализ DNS-трафика .....	9
Анализ ARP-трафика .....	10
Анализ трафика утилиты nslookup.....	11
Анализ FTP-трафика .....	12
Анализ DHCP-трафика .....	12
Анализ Skype-трафика .....	15
Вывод .....	16
Список использованной литературы .....	16

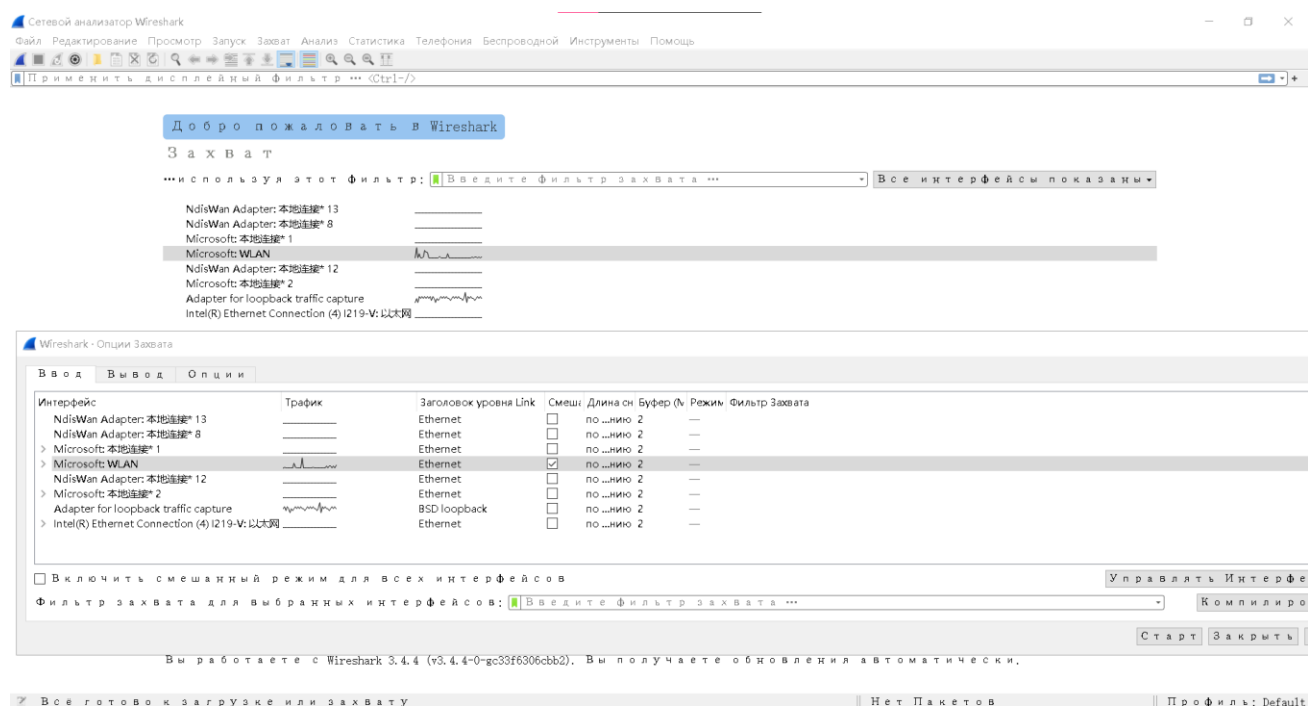
## Цель работы

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

## Вариант

www.yjf.ru

## Задачи



## Анализ трафика утилиты ping

Необходимо отследить и проанализировать трафик, создаваемый утилитой ping, запустив её следующим образом из командной строки:

ping -l размер\_пакета [www.yjf.ru](http://www.yjf.ru)

```
C:\Users\Yan Tszyafen>ping -l 100 www.yjf.ru

Pinging www.yjf.ru [5.188.131.10] with 100 bytes of data:
Reply from 5.188.131.10: bytes=100 time=29ms TTL=57
Reply from 5.188.131.10: bytes=100 time=55ms TTL=57
Reply from 5.188.131.10: bytes=100 time=36ms TTL=57
Reply from 5.188.131.10: bytes=100 time=35ms TTL=57

Ping statistics for 5.188.131.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 29ms, Maximum = 55ms, Average = 38ms
```

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\_100.pcap

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

ip.host == 5.188.131.10

No.	Time	Source	Destination	Protocol	Length	Info
287	87.516800	10.1.30.85	5.188.131.10	ICMP	142	Echo (ping) request id=0x0001, seq=51/13056, ttl=64 (reply in 288)
288	87.546392	5.188.131.10	10.1.30.85	ICMP	142	Echo (ping) reply id=0x0001, seq=51/13056, ttl=57 (request in 287)
289	88.526517	10.1.30.85	5.188.131.10	ICMP	142	Echo (ping) request id=0x0001, seq=52/13312, ttl=64 (reply in 290)
290	88.581670	5.188.131.10	10.1.30.85	ICMP	142	Echo (ping) reply id=0x0001, seq=52/13312, ttl=57 (request in 289)
291	89.531452	10.1.30.85	5.188.131.10	ICMP	142	Echo (ping) request id=0x0001, seq=53/13568, ttl=64 (reply in 292)
292	89.568201	5.188.131.10	10.1.30.85	ICMP	142	Echo (ping) reply id=0x0001, seq=53/13568, ttl=57 (request in 291)
293	90.546626	10.1.30.85	5.188.131.10	ICMP	142	Echo (ping) request id=0x0001, seq=54/13824, ttl=64 (reply in 294)
294	90.582335	5.188.131.10	10.1.30.85	ICMP	142	Echo (ping) reply id=0x0001, seq=54/13824, ttl=57 (request in 293)

> Frame 287: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits)

> Ethernet II, Src: IntelCor\_97:a9:14 (34:e1:2d:97:a9:14), Dst: Keenetic\_1e:dd:41 (50:ff:20:1e:dd:41)

> Internet Protocol Version 4, Src: 10.1.30.85, Dst: 5.188.131.10

> Internet Control Message Protocol

```

0000  50 ff 20 1e dd 41 34 e1 2d 97 a9 14 08 00 45 00  P...A4...E-
0010  00 80 7c 6e 00 00 40 01 4c f3 0a 01 1e 55 05 bc  ..|n-@L...U-
0020  83 0a 08 00 ea ba 00 01 00 33 61 62 63 64 65 66  ....3abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f  wabcdefg hijklmno
0050  70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68  pqrstuvwxyz abcdefgh
0060  69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61  ijklmnop qrstuvw
0070  62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71  bcdefghi jklmnopq
0080  72 73 74 75 76 77 61 62 63 64 65 66 67 68      rstuvwab cdefgh

```

ping\_100.pcap

Пакеты: 555 • Показаны: 8 (1.4%) • Профиль: Default

1. Имеет ли место фрагментация исходного пакета, какое поле на это указывает?  
Когда размер пакета больше чем 1472 байта, то имеет место фрагментация исходного пакета, и следующее поле на это указывает:

```

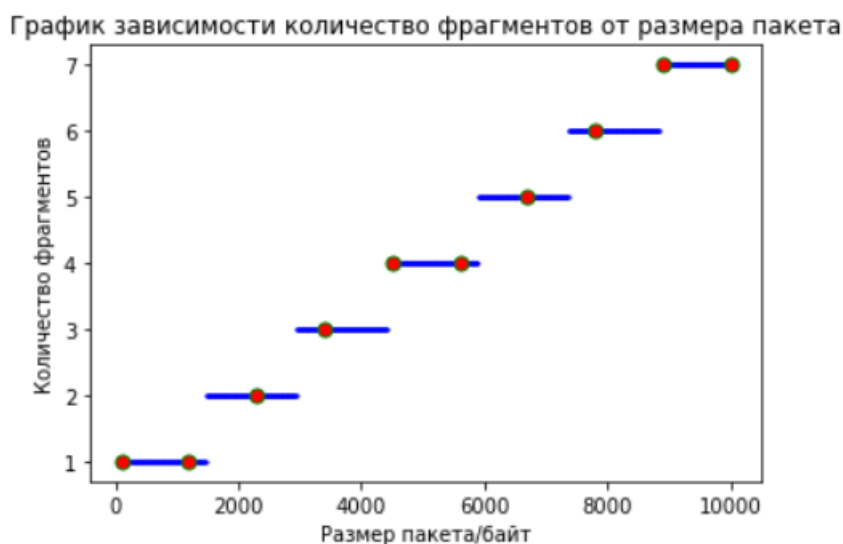
> Frame 7: 862 bytes on wire (6896 bits), 862 bytes captured (6896 bits)
> Ethernet II, Src: IntelCor_97:a9:14 (34:e1:2d:97:a9:14), Dst: 9e:e6:5e:33:58:64 (9e:e6:5e:33:58:64)
< Internet Protocol Version 4, Src: 172.20.10.3, Dst: 5.188.131.10
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 848
    Identification: 0xd6d9 (55001)
  > Flags: 0x00
    Fragment Offset: 1480
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x613d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.20.10.3
    Destination Address: 5.188.131.10
  > [2 IPv4 Fragments (2308 bytes): #6(1480), #7(828)]
  > Internet Control Message Protocol

```

2. Какая информация указывает, является ли фрагмент пакета последним или промежуточным?  
Последним.
3. Чему равно количество фрагментов при передаче ping-пакетов?  
Если размер пакета превышает 1472 байта, количество фрагментов равно размеру пакета, разделенному на 1472 байта и округленному в большую сторону.

Размер пакета	Количество фрагментов
100	1
1200	1
2300	2
3400	3
4500	4
5600	4
6700	5
7800	6
8900	7
10000	7

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?  
 Следующая команда может изменить значение параметра TTL исходного IP-пакета, но не может изменить значение параметра TTL IP-пакета, отправленного с сайта [www.yjf.ru](http://www.yjf.ru) :  
`ping -i [TTL] www.yjf.ru`
6. Что содержится в поле данных ping-пакета?  
 ASCII коды и 16-ричные коды для представления пакета, и ещё длина данных.

### Анализ трафика утилиты tracert (traceroute)

Необходимо отследить и проанализировать трафик, создаваемый утилитой tracert (или traceroute в Linux), запустив её следующим образом из командной строки:  
`tracert -d www.yjf.ru`

```

C:\Users\Yan Tszafafen>tracert -d www.yjf.ru

Tracing route to www.yjf.ru [5.188.131.10]
over a maximum of 30 hops:

  0  1 ms  <1 ms  <1 ms  192.168.1.1
  1  4 ms   8 ms   7 ms  93.100.24.1
  2  2 ms   1 ms   1 ms  93.100.0.105
  3  3 ms   2 ms   1 ms  93.100.0.42
  4  3 ms   1 ms   1 ms  194.226.100.162
  5 12 ms  14 ms  13 ms  92.53.94.95
  6 14 ms  17 ms  12 ms  92.53.94.57
  7 12 ms  10 ms  12 ms  5.188.131.10

Trace complete.

```

По результатам анализа собранной трассы, ответьте на следующие вопросы.

1. Сколько байт содержится в заголовке IP? Сколько байт содержится в поле данных?  
В заголовке IP содержится 20 байт. В поле данных содержится 64 байт.
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.  
Tracert сначала отправляет ответный пакет с TTL, равным 1, а затем увеличивает TTL на 1 в каждом последующем процессе отправки, пока целевой ответ или TTL не достигнет максимального значения.  
Система, выполняющая команду TRACERT, отправляет пакеты данных ICMP в отслеживаемую систему назначения. Поле TTL этих пакетов данных увеличивается с 1. Каждый раз, когда проходит через маршрутизатор, он будет уменьшать поле TTL на 1. Если TTL равно 0, поле TTL будет отброшено.
3. Чем отличаются ICMP-пакеты, генерируемые утилитой tracert, от ICMP-пакетов, генерируемых утилитой ping (см. предыдущее задание).  
Утилита ping генерирует пакеты «ICMP request» и «ICMP reply», а утилита tracert генерирует пакеты «ICMP error», «ICMP request» и «ICMP reply».
4. Чем отличаются полученные пакеты «ICMP reply» от «ICMP error» и зачем нужны оба этих типа ответов?  
«ICMP reply» - Echo (ping) reply, type:0, code:0. При достижении целевого адреса и ping не запрещен, и ответит на это сообщение.  
«ICMP error» - Time-to-live exceeded, type: 11, code:0. Tracert используется для определения пути, по которому осуществляется доступ к IP-данным. Когда tracert получает это сообщение, он знает, что маршрутизатор находится на этом пути.
5. Что изменится в работе tracert, если убрать ключ "-d"? Какой дополнительный трафик при этом будет генерироваться?

```
C:\Users\Yan Tsyafan>tracert www.yjf.ru

Tracing route to www.yjf.ru [5.188.131.10]
over a maximum of 30 hops:

  0  0 ms  0 ms  0 ms  router.asus.com [192.168.1.1]
  1  3 ms  2 ms  2 ms  93.100.24.1.pool.sknt.ru [93.100.24.1]
  2  3 ms  1 ms  1 ms  Router.sknt.ru [93.100.0.105]
  3  3 ms  1 ms  1 ms  Router.sknt.ru [93.100.0.42]
  4  3 ms  1 ms  3 ms  spbix.spb.net.selectel.ru [194.226.100.162]
  5  14 ms  12 ms  12 ms  92.53.94.95
  6  12 ms  12 ms  12 ms  92.53.94.57
  7  14 ms  13 ms  12 ms  5.188.131.10

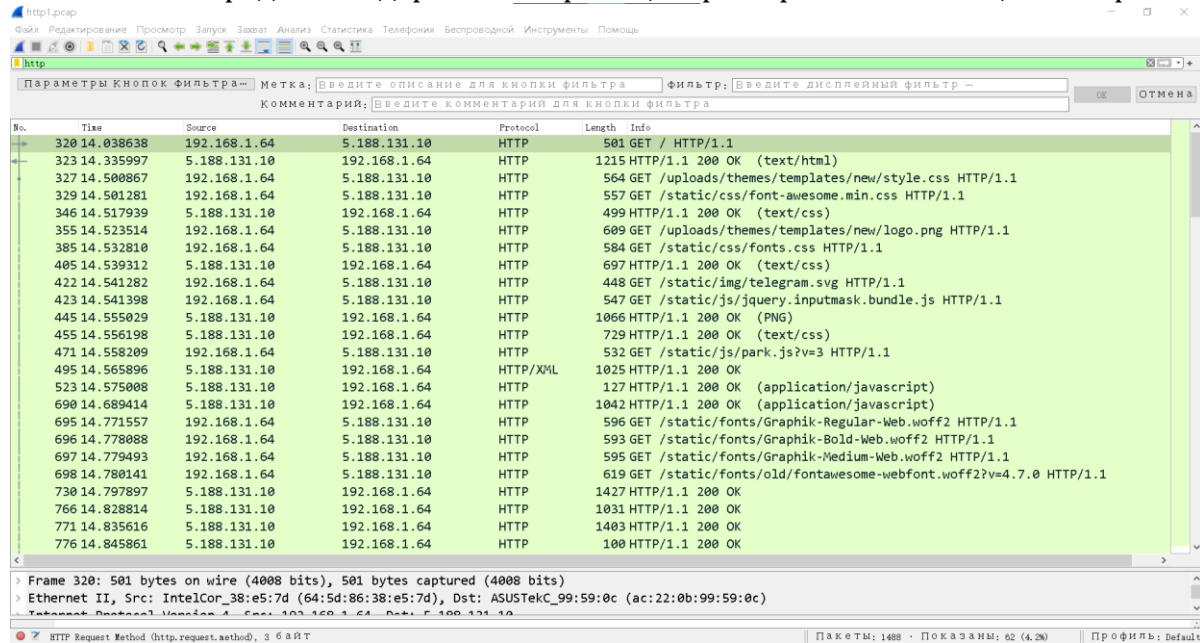
Trace complete.
```

## Анализ HTTP-трафика

- GET-сообщение от клиента (браузера);
- ответ сервера.

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).

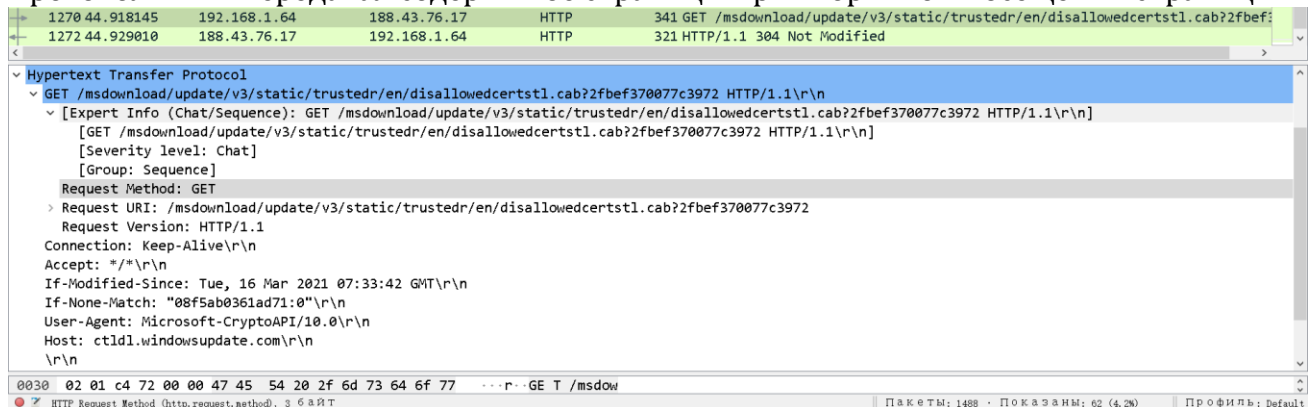
## Протокол HTTP передавал содержимое страницы при первичном посещении страницы:



The screenshot shows a Wireshark packet capture of an initial HTTP GET request and response. The packet list on the left shows a sequence of requests for various resources (HTML, CSS, JS, PNG, SVG) and a final 200 OK response. The selected packet (No. 320) is an HTTP GET request to 192.168.1.64 from 5.188.131.10. The packet details pane on the right shows the request structure, including the status bar at the bottom indicating 1488 packets and 62 shown.

No.	Time	Source	Destination	Protocol	Length	Info
320	14.038638	192.168.1.64	5.188.131.10	HTTP	501	GET / HTTP/1.1
323	14.335997	5.188.131.10	192.168.1.64	HTTP	1215	HTTP/1.1 200 OK (text/html)
327	14.500867	192.168.1.64	5.188.131.10	HTTP	564	GET /uploads/themes/templates/new/style.css HTTP/1.1
329	14.501281	192.168.1.64	5.188.131.10	HTTP	557	GET /static/css/font-awesome.min.css HTTP/1.1
346	14.517939	5.188.131.10	192.168.1.64	HTTP	499	HTTP/1.1 200 OK (text/css)
355	14.523514	192.168.1.64	5.188.131.10	HTTP	609	GET /uploads/themes/templates/new/logo.png HTTP/1.1
385	14.532810	192.168.1.64	5.188.131.10	HTTP	584	GET /static/css/fonts.css HTTP/1.1
405	14.539312	5.188.131.10	192.168.1.64	HTTP	697	HTTP/1.1 200 OK (text/css)
422	14.541282	192.168.1.64	5.188.131.10	HTTP	448	GET /static/img/telegram.svg HTTP/1.1
423	14.541398	192.168.1.64	5.188.131.10	HTTP	547	GET /static/js/jquery.inputmask.bundle.js HTTP/1.1
445	14.555029	5.188.131.10	192.168.1.64	HTTP	1066	HTTP/1.1 200 OK (PNG)
455	14.556198	5.188.131.10	192.168.1.64	HTTP	729	HTTP/1.1 200 OK (text/css)
471	14.558209	192.168.1.64	5.188.131.10	HTTP	532	GET /static/js/park.js?v=3 HTTP/1.1
495	14.565896	5.188.131.10	192.168.1.64	HTTP/XML	1025	HTTP/1.1 200 OK
523	14.575008	5.188.131.10	192.168.1.64	HTTP	127	HTTP/1.1 200 OK (application/javascript)
690	14.689414	5.188.131.10	192.168.1.64	HTTP	1042	HTTP/1.1 200 OK (application/javascript)
695	14.771557	192.168.1.64	5.188.131.10	HTTP	596	GET /static/fonts/Graphik-Regular-Web.woff2 HTTP/1.1
696	14.778088	192.168.1.64	5.188.131.10	HTTP	593	GET /static/fonts/Graphik-Bold-Web.woff2 HTTP/1.1
697	14.779493	192.168.1.64	5.188.131.10	HTTP	595	GET /static/fonts/Graphik-Medium-Web.woff2 HTTP/1.1
698	14.780141	192.168.1.64	5.188.131.10	HTTP	619	GET /static/fonts/old/fontawesome-webfont.woff2?v=4.7.0 HTTP/1.1
730	14.797897	5.188.131.10	192.168.1.64	HTTP	1427	HTTP/1.1 200 OK
766	14.828814	5.188.131.10	192.168.1.64	HTTP	1031	HTTP/1.1 200 OK
771	14.835616	5.188.131.10	192.168.1.64	HTTP	1403	HTTP/1.1 200 OK
776	14.845861	5.188.131.10	192.168.1.64	HTTP	100	HTTP/1.1 200 OK

## Протокол HTTP передавал содержимое страницы при вторичном посещении страницы:



The screenshot shows a Wireshark packet capture of a secondary HTTP GET request and response. The packet list on the left shows a GET request for a specific resource and a 304 Not Modified response. The selected packet (No. 1270) is an HTTP GET request to 192.168.1.64 from 127.0.44.918145. The packet details pane on the right shows the request structure, including the status bar at the bottom indicating 1488 packets and 62 shown.

No.	Time	Source	Destination	Protocol	Length	Info
1270	44.918145	192.168.1.64	188.43.76.17	HTTP	341	GET /msdownload/update/v3/static/trusted/en/disallowedcertstl.cab?2fbef370077c3972 HTTP/1.1
1272	44.929010	188.43.76.17	192.168.1.64	HTTP	321	HTTP/1.1 304 Not Modified



## 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.

The image shows a Windows command prompt window with the command `ipconfig /flushdns` executed, resulting in the message "Successfully flushed the DNS Resolver Cache." Below this, a Wireshark network traffic capture is displayed. The filter is set to `ip.addr == 192.168.1.122`. The packet list shows several DNS queries and responses. The packet details pane for packet 14087 (Frame 14087) shows a DNS query for `yjf.ru` from source `192.168.1.1` to destination `192.168.1.122`. The packet bytes pane shows the raw data of the DNS query.

No.	Time	Source	Destination	Protocol	Length	Info
13949	165.544276	192.168.1.122	192.168.1.1	DNS	83	Standard query 0x4b35 A maxcdn.bootstrapcdn.com
13950	165.544276	192.168.1.122	192.168.1.1	DNS	80	Standard query 0x6107 A cdnjs.cloudflare.com
13953	165.545521	192.168.1.1	192.168.1.122	DNS	179	Standard query response 0x5218 A code.jquery.com CNAME cds.s5x3j6q5.hwcd
13956	165.547102	192.168.1.1	192.168.1.122	DNS	530	Standard query response 0x6107 A cdnjs.cloudflare.com A 104.16.18.94 A 16
13957	165.547102	192.168.1.1	192.168.1.122	DNS	171	Standard query response 0x4b35 A maxcdn.bootstrapcdn.com A 104.18.10.207
13958	165.547411	192.168.1.122	192.168.1.1	DNS	65	Standard query 0x5ecc A rf.ru
13963	165.548984	192.168.1.122	192.168.1.1	DNS	76	Standard query 0x775c A api.whatsapp.com
13964	165.548999	192.168.1.122	192.168.1.1	DNS	69	Standard query 0xa374 A clubrf.ru
13983	165.552433	192.168.1.1	192.168.1.122	DNS	214	Standard query response 0x775c A api.whatsapp.com CNAME web.whatsapp.com
13989	165.554534	192.168.1.122	192.168.1.1	DNS	64	Standard query 0x9877 A t.me
13995	165.556921	192.168.1.1	192.168.1.122	DNS	186	Standard query response 0x5ecc A rf.ru A 5.188.131.10 NS anna.ns.cloudfla
13998	165.556921	192.168.1.1	192.168.1.122	DNS	261	Standard query response 0x9877 A t.me A 149.154.167.99 NS ns-cloud-b4.goc
14038	165.567012	192.168.1.1	192.168.1.122	DNS	124	Standard query response 0xa374 A clubrf.ru A 89.111.182.96 NS ns1.rf.ru
14087	165.575053	192.168.1.122	192.168.1.1	DNS	66	Standard query 0xff92 A yjf.ru
14152	165.598282	192.168.1.1	192.168.1.122	DNS	121	Standard query response 0xff92 A yjf.ru A 5.188.131.10 NS ns1.rf.ru NS ns
14338	165.874473	192.168.1.122	192.168.1.1	DNS	91	Standard query 0x397d A content-autofill.googleapis.com
14356	165.882337	192.168.1.1	192.168.1.122	DNS	218	Standard query response 0x397d A content-autofill.googleapis.com A 64.233

Frame 14087: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{A590680C-4D68-4EFF-880C-6C3532A11DED}, id 0  
Ethernet II, Src: IntelCor\_97:a9:14 (34:e1:2d:97:a9:14), Dst: ASUSTekC\_99:59:0c (ac:22:0b:99:59:0c)  
Internet Protocol Version 4, Src: 192.168.1.122, Dst: 192.168.1.1  
User Datagram Protocol, Src Port: 55167, Dst Port: 53  
Domain Name System (query)

0000 ac 22 0b 99 59 0c 34 e1 2d 97 a9 14 08 00 45 00 -.-Y.4. ....E-  
0010 00 34 af e1 00 00 40 11 47 0c c0 a8 01 7a c0 a8 -4....@. G.....Z-  
0020 01 01 d7 7f 00 35 00 20 be 45 ff 92 01 00 00 01 .....5. -E.....  
0030 00 00 00 00 00 00 03 79 6a 66 02 72 75 00 00 01 .....y jf.ru...  
0040 00 01 ..

По результатам анализа собранной трассы, ответьте на следующие вопросы.

1. Почему адрес, на который отправлен DNS-запрос, не совпадает с адресом посещаемого сайта?  
Балансировка нагрузки на основе DNS: на DNS-сервере одно и то же имя может быть настроено для нескольких разных адресов, и клиент, который наконец запрашивает имя, случайным образом получит один из адресов при разрешении имени.
2. Какие бывают типы DNS-запросов?  
В DNS имеются следующие типы запросов: итеративный (он же прямой), обратный и рекурсивный.  
A, NS, CNAME, SOA, WKS, PTR, HINFO, MX, AAAA, AXFR, ANY
3. В какой ситуации нужно выполнять независимые DNS-запросы для получения содержащихся на сайте изображений?  
При первом посещении сайта.

## 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” (проверить очистилась ли таблица можно с помощью команды команды “arp -a”, выводящей таблицу на экран);

```
C:\WINDOWS\system32>netsh interface ip delete arpcache
Ok.
```

```
C:\WINDOWS\system32>arp -a
```

```
Interface: 192.168.1.122 --- 0xe
    Internet Address      Physical Address      Type
    192.168.1.1           ac-22-0b-99-59-0c     dynamic
```

- очистить кэш браузера;
- зайти на Интернет-сайт, заданный по варианту.

```
C:\WINDOWS\system32>arp -a
```

```
Interface: 192.168.1.122 --- 0xe
    Internet Address      Physical Address      Type
    192.168.1.1           ac-22-0b-99-59-0c     dynamic
    192.168.1.255         ff-ff-ff-ff-ff-ff     static
    224.0.0.251           01-00-5e-00-00-fb     static
    239.255.255.250       01-00-5e-7f-ff-fa     static
```

Wireshark interface showing ARP traffic analysis. The packet list displays several ARP requests and replies. The packet details pane shows the structure of an ARP request packet (Frame 709). The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
676	17.276035	IntelCor_97:a9:14	Broadcast	ARP	42	Who has 169.254.169.254? Tell 192.168.1.122
700	18.090534	IntelCor_97:a9:14	Broadcast	ARP	42	Who has 169.254.169.254? Tell 192.168.1.122
702	19.088732	IntelCor_97:a9:14	Broadcast	ARP	42	Who has 169.254.169.254? Tell 192.168.1.122
708	26.172922	IntelCor_97:a9:14	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.122
709	26.175534	ASUSTekC_99:59:0c	IntelCor_97:a9:14	ARP	42	192.168.1.1 is at ac:22:0b:99:59:0c
3558	54.677615	ASUSTekC_99:59:0c	IntelCor_97:a9:14	ARP	42	Who has 192.168.1.122? Tell 192.168.1.1
3559	54.677628	IntelCor_97:a9:14	ASUSTekC_99:59:0c	ARP	42	192.168.1.122 is at 34:e1:2d:97:a9:14
6788	95.907162	ASUSTekC_99:59:0c	IntelCor_97:a9:14	ARP	42	Who has 192.168.1.122? Tell 192.168.1.1
6789	95.907174	IntelCor_97:a9:14	ASUSTekC_99:59:0c	ARP	42	192.168.1.122 is at 34:e1:2d:97:a9:14

> Frame 709: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0  
> Ethernet II, Src: ASUSTekC\_99:59:0c (ac:22:0b:99:59:0c), Dst: IntelCor\_97:a9:14 (34:e1:2d:97:a9:14)  
v Address Resolution Protocol (reply)  
 Hardware type: Ethernet (1)  
 Protocol type: IPv4 (0x0800)  
 Hardware size: 6  
 Protocol size: 4  
 Opcode: reply (2)  
 Sender MAC address: ASUSTekC\_99:59:0c (ac:22:0b:99:59:0c)  
 Sender IP address: 192.168.1.1  
 Target MAC address: IntelCor\_97:a9:14 (34:e1:2d:97:a9:14)  
 Target IP address: 192.168.1.122

0000 34 e1 2d 97 a9 14 ac 22 0b 99 59 0c 08 06 00 01 4 - - - - - " --Y-----  
0010 08 00 06 04 00 02 ac 22 0b 99 59 0c c0 a8 01 01 - - - - - " --Y-----  
0020 34 e1 2d 97 a9 14 c0 a8 01 7a 4 - - - - - z

По результатам анализа собранной трассы, ответьте на следующие вопросы.

1. Какие MAC-адреса присутствуют в захваченных пакетах ARP-протокола? Что означают эти адреса? Какие устройства они идентифицируют? (ipconfig /all)  
MAC-адрес - это адрес, используемый для подтверждения местоположения сетевого устройства.  
00:00:00:00:00:00 - Broadcast, чтобы получить MAC-адрес определенного IP-

адреса

34:e1:2d:97:a9:14 – Microsoft Wi-Fi Direct Virtual Adapter #3

ac:22:0b:99:59:0c – Физический адрес локального IP-адреса – DNS сервер

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

34:e1:2d:97:a9:14 – Microsoft Wi-Fi Direct Virtual Adapter #3

ac:22:0b:99:59:0c – Физический адрес локального IP-адреса – DNS сервер

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

Для того, чтобы получить ответ, т.е. MAC-адрес целевого адреса.

### 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".

```
C:\WINDOWS\system32>nslookup www.yjf.ru
Server: router.asus.com
Address: 192.168.1.1

Non-authoritative answer:
Name: www.yjf.ru
Address: 5.188.131.10

C:\WINDOWS\system32>nslookup -type=NS www.yjf.ru
Server: router.asus.com
Address: 192.168.1.1

yjf.ru
primary name server = ns1.rf.ru
responsible mail addr = hostmaster.yjf.ru
serial = 2021030502
refresh = 10800 (3 hours)
retry = 3600 (1 hour)
expire = 604800 (7 days)
default TTL = 3600 (1 hour)
```

По результатам анализа собранной трассы, ответьте на следующие вопросы.

1. Чем различается трасса трафика в п.2 и п.4, указанных выше?  
п.2: type – A(Address). Запись A относится к записи IP, используемой для указания имени хоста или имени домена.  
п.4: type – NS(Nameserver). Запись NS используется для указания того, какой DNS-сервер разрешает доменное имя.
2. Что содержится в поле «Answers» DNS-ответа?

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

```

  Authoritative nameservers
  yjf.ru: type SOA, class IN, mname ns1.rf.ru
    Name: yjf.ru
    Type: SOA (Start Of a zone of Authority) (6)
    Class: IN (0x0001)
    Time to live: 30 (30 seconds)
    Data length: 42
    Primary name server: ns1.rf.ru
    Responsible authority's mailbox: hostmaster.yjf.ru
    Serial Number: 2021030502
    Refresh Interval: 10800 (3 hours)
    Retry Interval: 3600 (1 hour)
    Expire limit: 604800 (7 days)
    Minimum TTL: 3600 (1 hour)

```

---

### 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.

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

По результатам анализа собранной трассы, ответьте на следующие вопросы.

1. Сколько байт данных содержится в пакете FTP-DATA?  
490 байт.
2. Как выбирается порт транспортного уровня, который используется для передачи FTP-пакетов?  
Port: 21.
3. Чем отличаются пакеты FTP от FTP-DATA?  
FTP: Source Port: 21, Содержит статус передачи FTP-пакета.  
FTP-DATA: Source Port: 49, Содержит размер данных в пакете FTP-DATA.

### Анализ DHCP-трафика

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

1. Убедиться, что для назначения IP-адреса на компьютере был использован DHCP и что компьютеру был назначен IP-адрес.

```
选择命令提示符
C:\Users\Yan Tszyafen>ipconfig/all

Windows IP Configuration

Host Name . . . . . : LAPTOP-7HMPD072
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter 以太网 :

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) Ethernet Connection (4) I219-V
Physical Address. . . . . : 8C-16-45-BF-9A-B6
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter 无线网络适配器 *1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
Physical Address. . . . . : 34-E1-2D-97-A9-15
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter 无线网络适配器 *2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
Physical Address. . . . . : 36-E1-2D-97-A9-14
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter WLAN:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) Dual Band Wireless-AC 8265
Physical Address. . . . . : 34-E1-2D-97-A9-14
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::6c69:47f5:35a4:7fab%14(Preferred)
IPv4 Address. . . . . : 192.168.1.122(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 15 апреля 2021 г. 23:43:23
Lease Expires . . . . . : 18 апреля 2021 г. 3:28:51
```

2. Настроить Wireshark-фильтр «bootp» (во время защиты УИР следует объяснить, почему именно такой фильтр используется для анализа DHCP-трафика).  
Поскольку dhcp улучшен на основе bootp. Но новая версия Wireshark использует DHCP вместо BOOTP.
3. Сбросить текущий IP-адрес, выданный накануне перед этим DHCP-сервером, с помощью команды: "ipconfig /release".

```

C:\Users\Yan Tszyafen>ipconfig /release

Windows IP Configuration

No operation can be performed on { } while it has its media disconnected.
No operation can be performed on { } * 1 while it has its media disconnected.
No operation can be performed on { } * 2 while it has its media disconnected.

Ethernet adapter { } :

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter { } * 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter { } * 2:

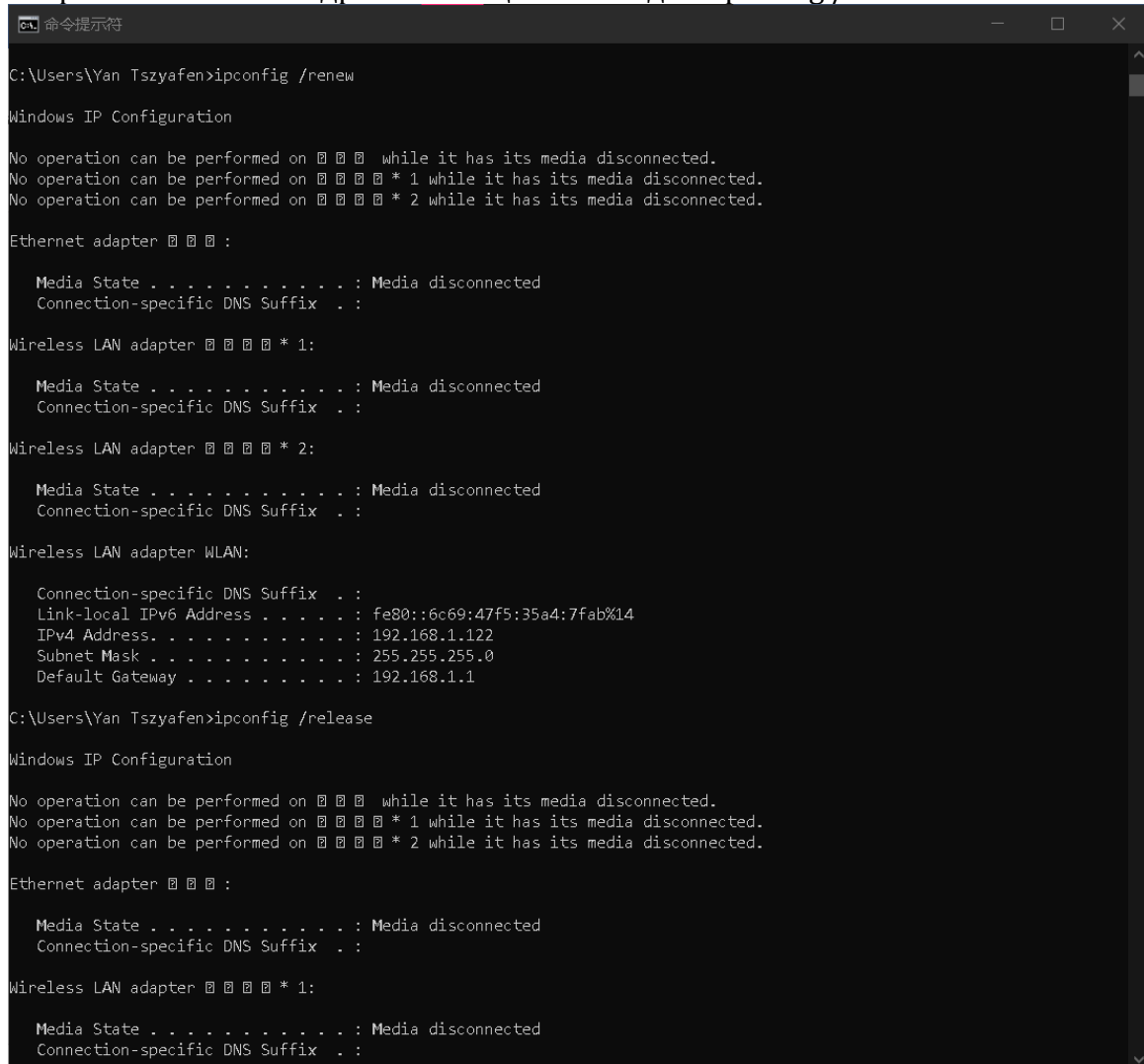
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter WLAN:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::6c69:47f5:35a4:7fab%14
    Default Gateway . . . . . :

```

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



```

C:\Users\Yan Tszyafen>ipconfig /renew

Windows IP Configuration

No operation can be performed on { } while it has its media disconnected.
No operation can be performed on { } * 1 while it has its media disconnected.
No operation can be performed on { } * 2 while it has its media disconnected.

Ethernet adapter { } :

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter { } * 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter { } * 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter WLAN:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::6c69:47f5:35a4:7fab%14
    IPv4 Address. . . . . : 192.168.1.122
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\Users\Yan Tszyafen>ipconfig /release

Windows IP Configuration

No operation can be performed on { } while it has its media disconnected.
No operation can be performed on { } * 1 while it has its media disconnected.
No operation can be performed on { } * 2 while it has its media disconnected.

Ethernet adapter { } :

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter { } * 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

```

5. Повторить п.3 и п.4.

Нарисуйте временную диаграмму, иллюстрирующую последовательность обмена первыми четырьмя DHCP-пакетами Discover/Offer/Request/ACK. Укажите для каждого пакета номера портов источника и назначения. По результатам анализа собранной трассы, ответьте на следующие вопросы.

6412	335.288107	192.168.1.122	192.168.1.1	DHCP	342 DHCP Release	- Transaction ID 0x31f7435
6584	343.514645	0.0.0.0	255.255.255.255	DHCP	344 DHCP Discover	- Transaction ID 0x58c29e0
6756	346.750401	192.168.1.1	192.168.1.122	DHCP	342 DHCP Offer	- Transaction ID 0x58c29e0
6757	346.751650	0.0.0.0	255.255.255.255	DHCP	370 DHCP Request	- Transaction ID 0x58c29e0
6758	347.057791	192.168.1.1	192.168.1.122	DHCP	357 DHCP ACK	- Transaction ID 0x58c29e0

1. Чем различаются пакеты «DHCP Discover» и «DHCP Request»?  
В пакете «DHCP Request» больше поле DHCP Server Identifier и Client Fully Qualified Domain Name, чем в пакете «DHCP Discover».
2. Как и почему менялись MAC- и IP-адреса источника и назначения в переданных DHCP-пакетах.  
Во время начального процесса запроса DHCP у клиента нет локального IP-адреса, а начальный адрес 0.0.0.0 для отправки широковещательного пакета. IP назначения в это время 255.255.255.255. Клиент хочет обнаружить DHCP-сервер, который может предоставлять ему услуги через этот пакет данных. Во время взаимодействия DHCP номер порта сервера - 67, а номер порта клиента - 68. Когда сервер DHCP получает пакет обнаружения DHCP, он отвечает клиенту пакетом предложения DHCP. DHCP-сервер по-прежнему использует широковещательный адрес в качестве адреса назначения, чтобы сообщить запрашивающим клиентам, что это DHCP-сервер, который можно использовать. Когда Клиент получает пакет предложения DHCP, он подтверждает, что существует сервер DHCP, который может с ним взаимодействовать, поэтому Клиент отправляет пакет запроса, чтобы запросить выделение IP. В настоящее время IP-адрес источника и IP-адрес назначения по-прежнему равны 0.0.0.0 и 255.255.255.255. Сервер отвечает на запрос DHCP пакетом DHCP ACK.
3. Каков IP-адрес DHCP-сервера?  
192.168.1.1
4. Что произойдёт, если очистить использованный фильтр "bootp"?  
Трудно найти пакеты DHCP.

## Анализ Skype-трафика

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

- отправить текстовое сообщение и получить ответ;
- осуществить короткий сеанс аудио-общения;
- осуществить короткий сеанс видео-общения.

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

1. Чем различаются пакета разных видов Skype-трафика (текст, аудио, видео)?  
Текст: protocol – tcp, src port – 443, пакет application data  
Аудио: protocol- udp, dis port – 53422, содержит поле data  
Видео: protocol- tcp, src port – 443, пакет application data

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

Текст: `ip.src == 192.168.1.122 && tcp.port == 443`

Аудио: `ip.src == 192.168.1.122 && udp.port == 53422`

Видео: `ip.src == 192.168.1.122 && tcp.port == 443`

Примечание. При выполнении п. 2.4.9 вместо Skype можно использовать любое другое аналогичное по функциональности программное обеспечение (Yahoo Messenger, MSN, Тох, «Mail.ru Агент» и любые другие)

## **Вывод**

Научилась использовать Wireshark для захвата и отслеживания пакетов и освоила анализ трафиков: утилиты ping, tracert, HTTP, DNS, ARP, nslookup, FTP, DHCP, Skype.

## **Список использованной литературы**

- 1 Алиев Т.И., Соснин В.В., Шинкарук Д.Н. Компьютерные сети и телекоммуникации: задания и тесты. – СПб: Университет ИТМО, 2018. – 112 с.
- 2 Т.И.Алиев СЕТИ ЭВМ И ТЕЛЕКОММУНИКАЦИИ - Санкт-Петербург: СПбГУ ИТМО, 2011. - 400 с. - экз.