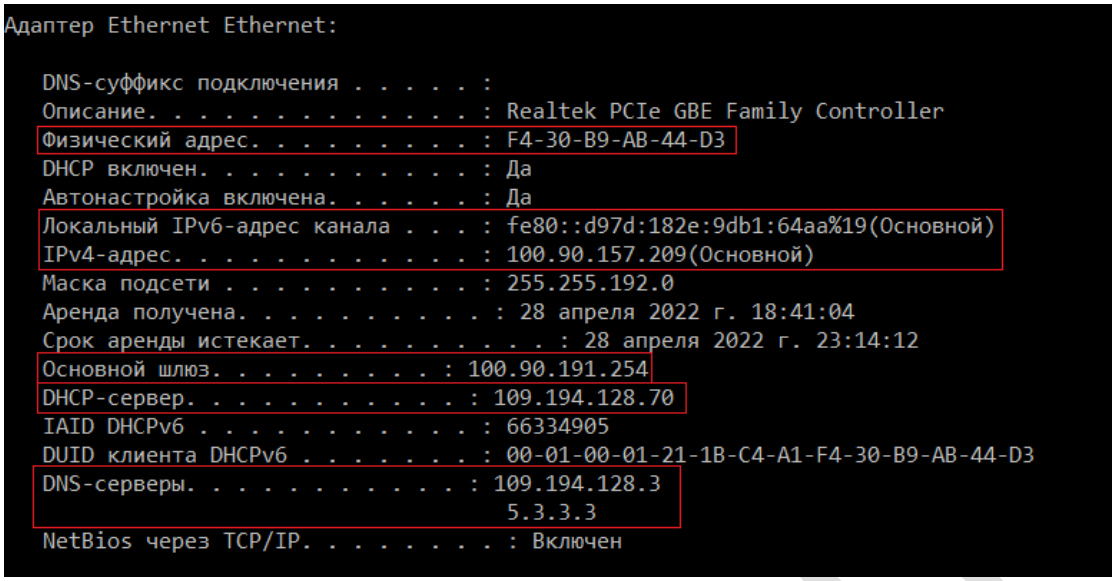
Лабораторная работа № 1

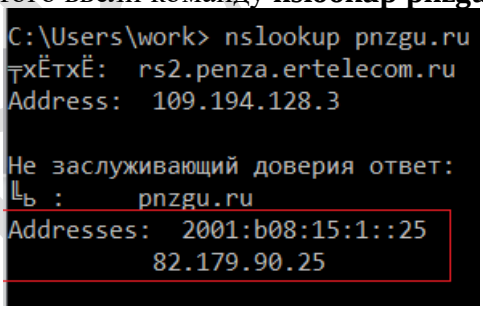
1. Запустили утилиту ipconfig в командной строке с помощью команды **ipconfig /all**, полученные данные оформили в таблице.

```
C:\Users\work>ipconfig /all

Настройка протокола IP для Windows

   Имя компьютера  . . . . . . . . . : DESKTOP-7675C4N
   Основной DNS-суффикс  . . . . . . :
   Тип узла. . . . . . . . . . . . . : Гибридный
   IP-маршрутизация включена . . . . : Нет
   WINS-прокси включен . . . . . . . : Нет

Неизвестный адаптер Подключение по локальной сети 2:

   Состояние среды. . . . . . . . : Среда передачи недоступна.
   DNS-суффикс подключения . . . . . :
   Описание. . . . . . . . . . . . . : Windscribe Windtun420
   Физический адрес. . . . . . . . . :
   DHCP включен. . . . . . . . . . . : Нет
   Автонастройка включена. . . . . . : Да

Неизвестный адаптер Подключение по локальной сети:

   Состояние среды. . . . . . . . : Среда передачи недоступна.
   DNS-суффикс подключения . . . . . :
   Описание. . . . . . . . . . . . . : Windscribe VPN
   Физический адрес. . . . . . . . . : 00-FF-B9-1A-32-0A
   DHCP включен. . . . . . . . . . . : Да
   Автонастройка включена. . . . . . : Да

Адаптер беспроводной локальной сети Беспроводная сеть:

   Состояние среды. . . . . . . . : Среда передачи недоступна.
   DNS-суффикс подключения . . . . . :
   Описание. . . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 7265
   Физический адрес. . . . . . . . . : A0-AF-BD-E7-43-ED
   DHCP включен. . . . . . . . . . . : Да
   Автонастройка включена. . . . . . : Да

Адаптер беспроводной локальной сети Подключение по локальной сети* 1:

   Состояние среды. . . . . . . . : Среда передачи недоступна.
   DNS-суффикс подключения . . . . . :
   Описание. . . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Физический адрес. . . . . . . . . : A2-AF-BD-E7-43-ED
   DHCP включен. . . . . . . . . . . : Да
   Автонастройка включена. . . . . . : Да

Адаптер беспроводной локальной сети Подключение по локальной сети* 2:

   Состояние среды. . . . . . . . : Среда передачи недоступна.
   DNS-суффикс подключения . . . . . :
```



Имя ПК	DESKTOP-7675C4N
IP-адрес основного сетевого интерфейса компьютера	100.90.157.209 (IPv4) fe80::d97d:182e:9db1:64aa%19 (IPv6)
Физический адрес основного сетевого интерфейса компьютера	F4-30-B9-AB-44-D3
IP-адрес шлюза	100.90.191.254
IP-адреса DNS-серверов	109.194.128.3 5.3.3.3
Использование DHCP (DHCP сервер)	109.194.128.70

2. С помощью утилиты nslookup определили IP-адрес сервера с доменным именем pnzgu.ru, для этого ввели команду **nslookup pnzgu.ru**.



3. Проверили связь с удалённым сервером pnzgu.ru. Для этого отправили на него 10 эхо-пакетов с помощью утилиты ping, в командную строку ввели **ping -n 20 pnzgu.ru**. Состояние связи стабильное, так как ни один из пакетов не был потерян, а TTL не был превышен. Результаты работы отобразили в таблице.

```
C:\Users\work>ping -n 10 pnzgu.ru

Обмен пакетами с pnzgu.ru [82.179.90.25] с 32 байтами данных:
Ответ от 82.179.90.25: число байт=32 время=30мс TTL=57
Ответ от 82.179.90.25: число байт=32 время=30мс TTL=57
Ответ от 82.179.90.25: число байт=32 время=30мс TTL=57
Ответ от 82.179.90.25: число байт=32 время=30мс TTL=57
Ответ от 82.179.90.25: число байт=32 время=30мс TTL=57
Ответ от 82.179.90.25: число байт=32 время=30мс TTL=57
Ответ от 82.179.90.25: число байт=32 время=30мс TTL=57
Ответ от 82.179.90.25: число байт=32 время=31мс TTL=57
Ответ от 82.179.90.25: число байт=32 время=32мс TTL=57
Ответ от 82.179.90.25: число байт=32 время=32мс TTL=57

Статистика Ping для 82.179.90.25:
    Пакетов: отправлено = 10, получено = 10, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 30мсек, Максимальное = 32 мсек, Среднее = 30 мсек
```

IP-адрес хоста назначения	82.179.90.25
Среднее время приема-передачи	30 мс
Процент потерянных пакетов	0% потерь

4. В командную строку ввели **arp -a**, затем пропинговали и сохранили в кеше и повторно ввели эту команду. В arp-кэше после пингования добавился новый адрес.

```
Интерфейс: 192.168.1.108 --- 0x10
  адрес в Интернете      Физический адрес      Тип
  192.168.1.1           50-ff-20-3f-bc-1d     динамический
  192.168.1.112         b4-c9-b9-a4-1b-07     динамический
  192.168.1.255         ff-ff-ff-ff-ff-ff     статический
  224.0.0.2             01-00-5e-00-00-02     статический
  224.0.0.22            01-00-5e-00-00-16     статический
  224.0.0.187           01-00-5e-00-00-bb     статический
  224.0.0.250           01-00-5e-00-00-fa     статический
  224.0.0.251           01-00-5e-00-00-fb     статический
  224.0.0.252           01-00-5e-00-00-fc     статический
  239.192.152.143       01-00-5e-40-98-8f     статический
  239.255.3.22          01-00-5e-7f-03-16     статический
  239.255.255.250       01-00-5e-7f-ff-fa     статический
  239.255.255.251       01-00-5e-7f-ff-fb     статический
  255.255.255.255       ff-ff-ff-ff-ff-ff     статический

C:\Users\ArtK0>ping 192.168.1.56

Обмен пакетами с 192.168.1.56 по с 32 байтами данных:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.

Статистика Ping для 192.168.1.56:
    Пакетов: отправлено = 4, получено = 0, потеряно = 4
    (100% потерь)

C:\Users\ArtK0>ping 192.168.1.45

Обмен пакетами с 192.168.1.45 по с 32 байтами данных:
Ответ от 192.168.1.45: число байт=32 время=39мс TTL=128
Ответ от 192.168.1.45: число байт=32 время=53мс TTL=128
Ответ от 192.168.1.45: число байт=32 время=61мс TTL=128
Ответ от 192.168.1.45: число байт=32 время=73мс TTL=128

Статистика Ping для 192.168.1.45:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 39мсек, Максимальное = 73 мсек, Среднее = 56 мсек

C:\Users\ArtK0>arp -a

Интерфейс: 192.168.1.108 --- 0x10
  адрес в Интернете      Физический адрес      Тип
  192.168.1.1           50-ff-20-3f-bc-1d     динамический
  192.168.1.45          c4-4f-33-e2-69-0c     динамический
  192.168.1.56          98-48-27-81-62-77     динамический
  192.168.1.112         b4-c9-b9-a4-1b-07     динамический
  192.168.1.255         ff-ff-ff-ff-ff-ff     статический
  224.0.0.2             01-00-5e-00-00-02     статический
  224.0.0.22            01-00-5e-00-00-16     статический
  224.0.0.187           01-00-5e-00-00-bb     статический
  224.0.0.250           01-00-5e-00-00-fa     статический
  224.0.0.251           01-00-5e-00-00-fb     статический
  224.0.0.252           01-00-5e-00-00-fc     статический
  239.192.152.143       01-00-5e-40-98-8f     статический
  239.255.3.22          01-00-5e-7f-03-16     статический
  239.255.255.250       01-00-5e-7f-ff-fa     статический
  239.255.255.251       01-00-5e-7f-ff-fb     статический
  255.255.255.255       ff-ff-ff-ff-ff-ff     статический

C:\Users\ArtK0>
```

5. Провели трассировку удалённого хоста pnzgu.ru, для этого ввели в командную строку **tracert pnzgu.ru**. Трассировка прошла успешно, без потери пакетов.

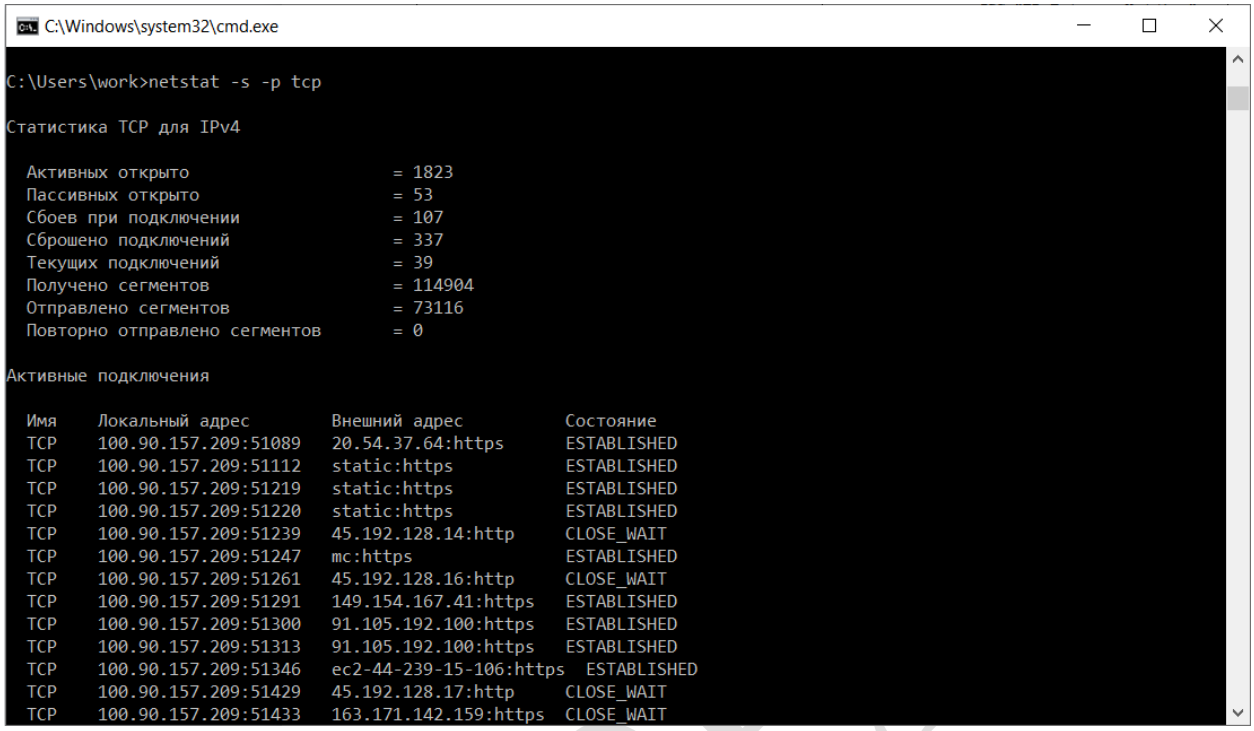
```
C:\Users\work>tracert pnzgu.ru

Трассировка маршрута к pnzgu.ru [82.179.90.25]
с максимальным числом прыжков 30:

  1     1 ms     1 ms     1 ms  100.90.255.252
  2     1 ms     1 ms     1 ms  109.194.136.18
  3    14 ms    24 ms    11 ms  ertelecom.msk.ru [194.190.254.142]
  4    21 ms    17 ms    23 ms  m9-3-gw.msk.runnet.ru [194.190.254.141]
  5    35 ms    35 ms    35 ms  pnzgu.penza.runnet.ru [194.190.254.10]
  6    30 ms    30 ms    29 ms  gamma-ng.pnzgu.ru [82.179.90.244]
  7    30 ms    30 ms    30 ms  sigma.pnzgu.ru [82.179.90.225]
  8    30 ms    30 ms    30 ms  apollo-ng.pnzgu.ru [82.179.90.25]

Трассировка завершена.
```

С помощью сервиса WHOIS получили информацию о некоторых маршрутизаторах.

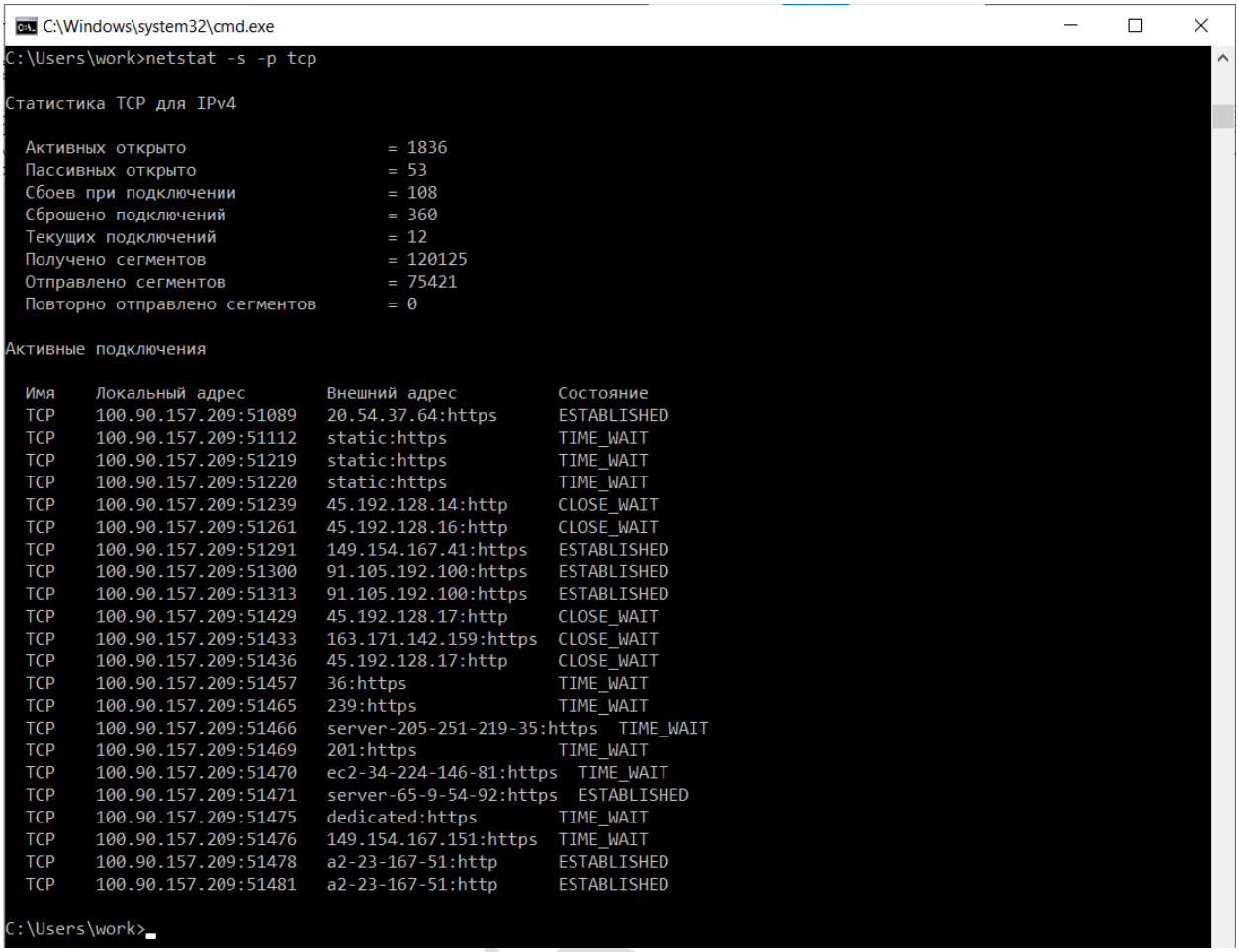
Маршрутизатор	**pnzgu.penza.runnet.ru [194.190.254.10]**
Название организации	RUNNET Federal University Computer Network
Физический адрес	Brusov per., 21-2, 125009, Moscow, RUSSIAN FEDERATION
Контактные данные администратора	+74959692617 incident@runnet.ru

Маршрутизатор	**sigma.pnzgu.ru [82.179.90.225]**
Название организации	PNZGU-NET Penza State University
Физический адрес	40, Krasnaya st., 440026, Penza, Russia
Контактные данные администратора	Konstantin V Popov +7 8412 563926 cnit@pnzgu.ru

6. Открыли Google Chrom (3 вкладки) и Mozilla Firefox (1 вкладка) и посмотрели все сетевые подключения **netstat -s -p tcp**

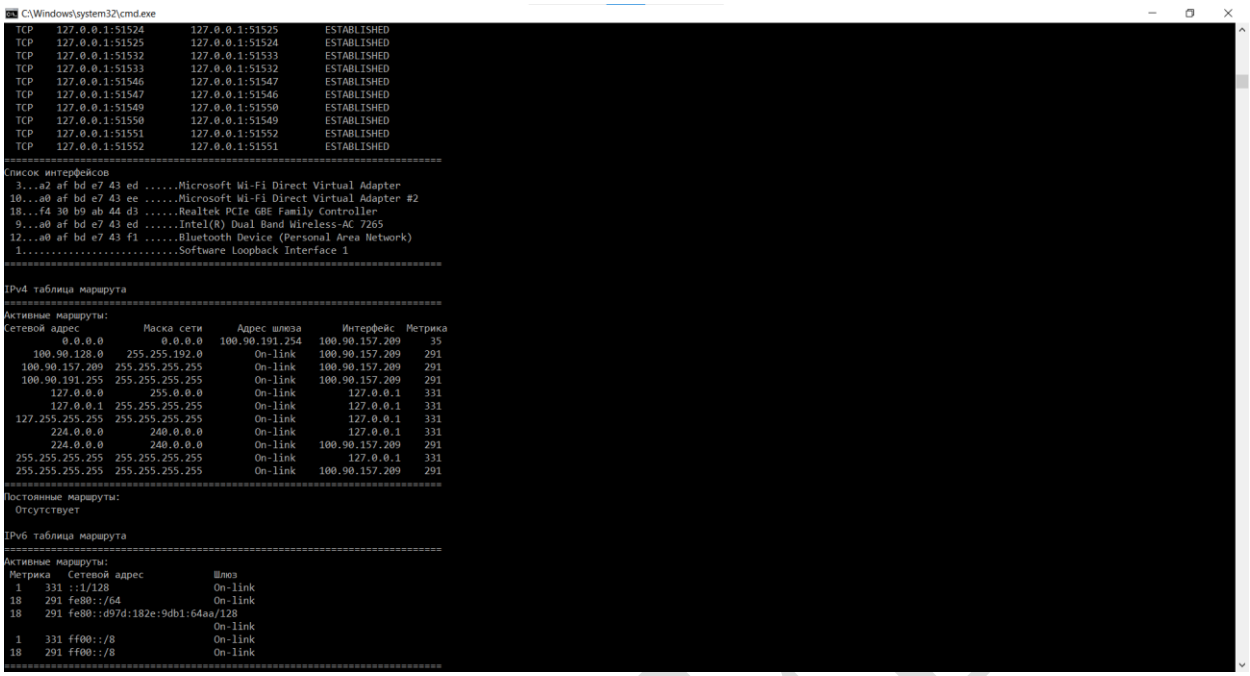


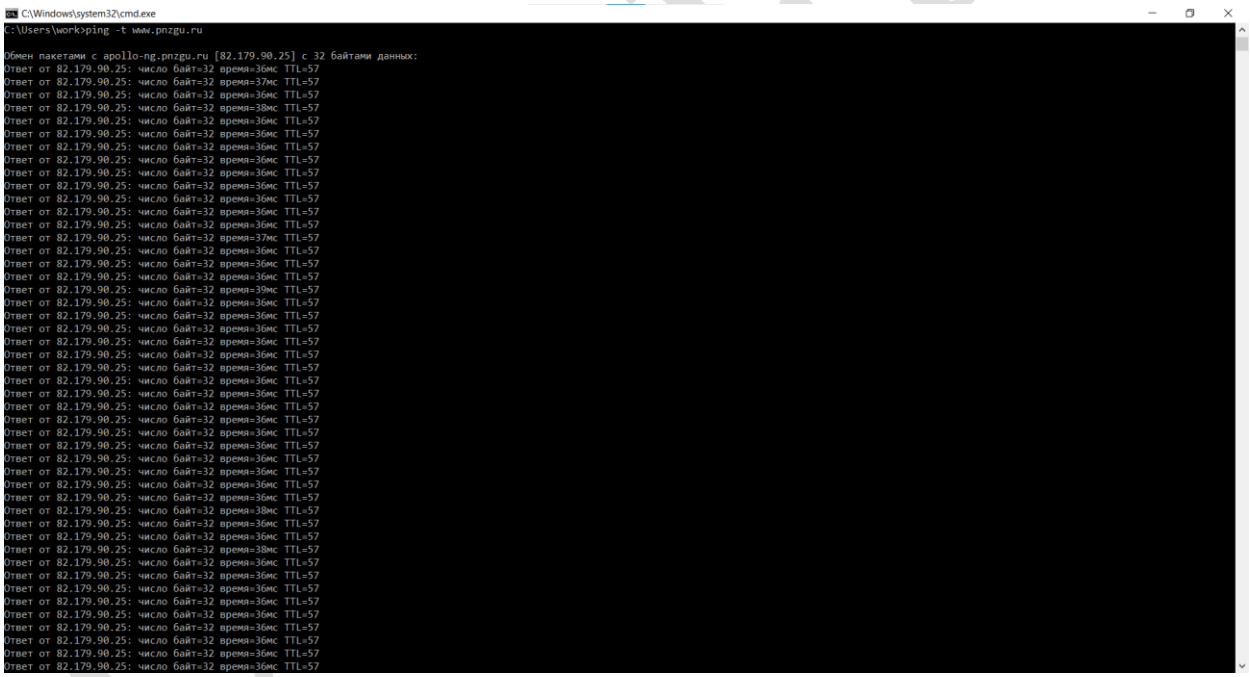
Закрыли браузеры и повторно ввели команду - активных подключений стало меньше



Контроль в реальном времени:

Открыли ранее закрытые сетевые приложения, запустили команду **netstat -s -p tcp -n -r 30** и в новом окне - **ping -t .** Результаты работы представлены ниже.





Остановили работу утилиты с помощью сочетания клавиш Ctrl+C.

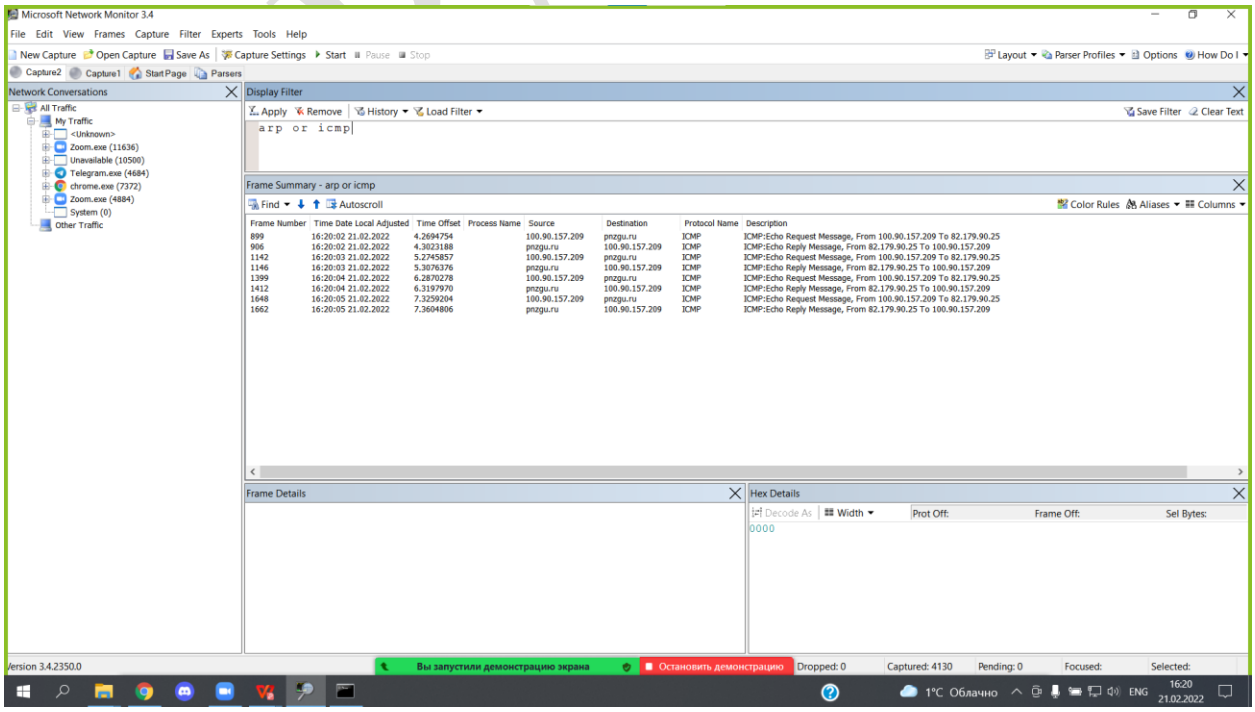
Лабораторная работа № 2

1. Запустили командную строку от имени администратора и посмотрели arp-кэш

```
C:\Windows\system32>arp -d

C:\Windows\system32>arp -a

Интерфейс: 100.90.157.209 --- 0x12
  адрес в Интернете      Физический адрес      Тип
  100.90.191.254         00-00-5e-00-01-8a     динамический
  224.0.0.22             01-00-5e-00-00-16     статический
  255.255.255.255        ff-ff-ff-ff-ff-ff     статический
```

2. Создали новую Capture и пропинговали сайт университета.

```
C:\Windows\system32>ping pnzgu.ru

Обмен пакетами с pnzgu.ru [82.179.90.25] с 32 байтами данных:
Ответ от 82.179.90.25: число байт=32 время=32мс TTL=57
Ответ от 82.179.90.25: число байт=32 время=33мс TTL=57
Ответ от 82.179.90.25: число байт=32 время=32мс TTL=57
Ответ от 82.179.90.25: число байт=32 время=34мс TTL=57

Статистика Ping для 82.179.90.25:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 32мсек, Максимальное = 34 мсек, Среднее = 32 мсек
```



Так как данный компьютер подключен к сети через ethernet, arp протоколы отсутствуют.

3. Разобрали протокол IP, зашли на сайт и совершили несколько внутренних переходов. Отфильтровали кадры по протоколу TCP и рассмотрели IP-протокол.

Адрес получателя: F430B9 AB44D3 [F4-30-B9-AB-44-D3]

Адрес отправителя: USC INFORMATION SCIENCES INST 00018A [00-00-5E-00-01-8A]

```
Frame: Number = 5689, Captured Frame Length = 60, MediaType = ETHERNET
Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[F4-30-B9-AB-44-D3],SourceAddress:[00-00-5E-00-01-8A]
  DestinationAddress: F430B9 AB44D3 [F4-30-B9-AB-44-D3]
  SourceAddress: USC INFORMATION SCIENCES INST 00018A [00-00-5E-00-01-8A]
  EthernetType: Internet IP (IPv4), 2048(0x800)
  UnknownData: Binary Large Object (6 Bytes)
Ipv4: Src = 74.125.131.198, Dest = 100.90.11.238, Next Protocol = TCP, Packet ID = 59057, Total IP Length = 40
  Versions: IPv4, Internet Protocol; Header Length = 20
  DifferentiatedServicesField: DSCP: 28, ECN: 0
  TotalLength: 40 (0x28)
  Identification: 59057 (0xE6B1)
  FragmentFlags: 0 (0x0)
  TimeToLive: 124 (0x7C)
  NextProtocol: TCP, 6(0x6)
  Checksum: 6435 (0x1923)
  SourceAddress: 74.125.131.198
  DestinationAddress: 100.90.11.238
Tcp: Flags=...A...., SrcPort=HTTPS(443), DstPort=65338, PayloadLen=0, Seq=846027111, Ack=397408227, Win=574
```

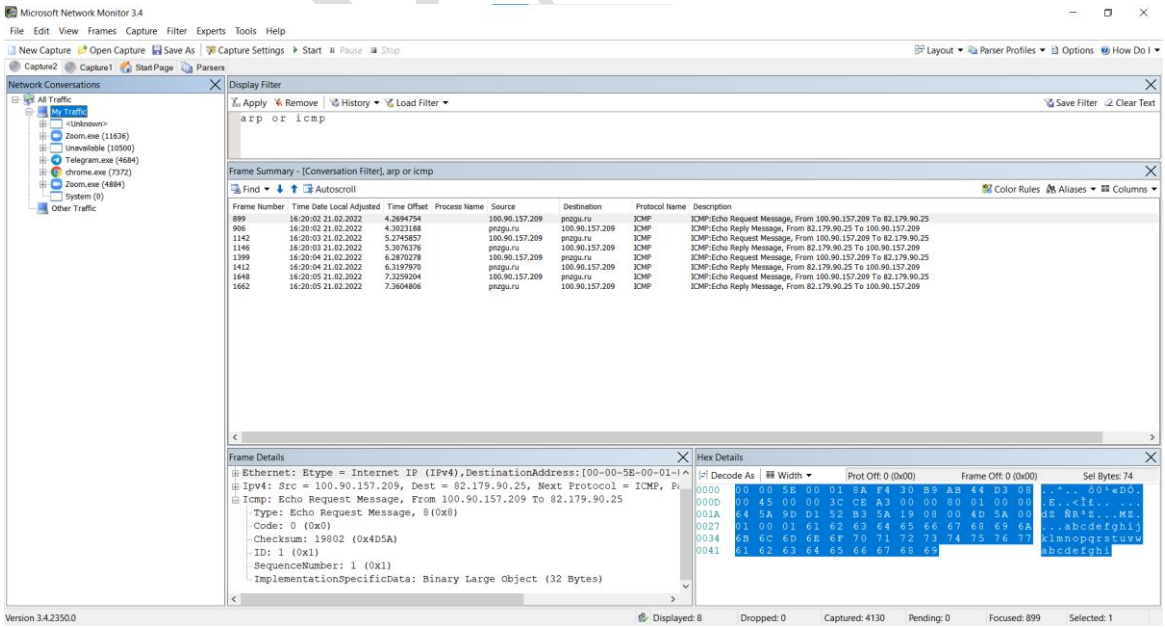
4. Разобрали протокол ICMP. С помощью утилиты traceroute отправили эхо-сообщение на удалённый сервер. Отфильтровали и разобрали полученные кадры.

Данный протокол рассылает эхо-сообщения и содержит следующие поля:

Тип - эхо-сообщения

Код функции соответствующего типа сообщения - 0, т. к. тип имеет 1 функцию

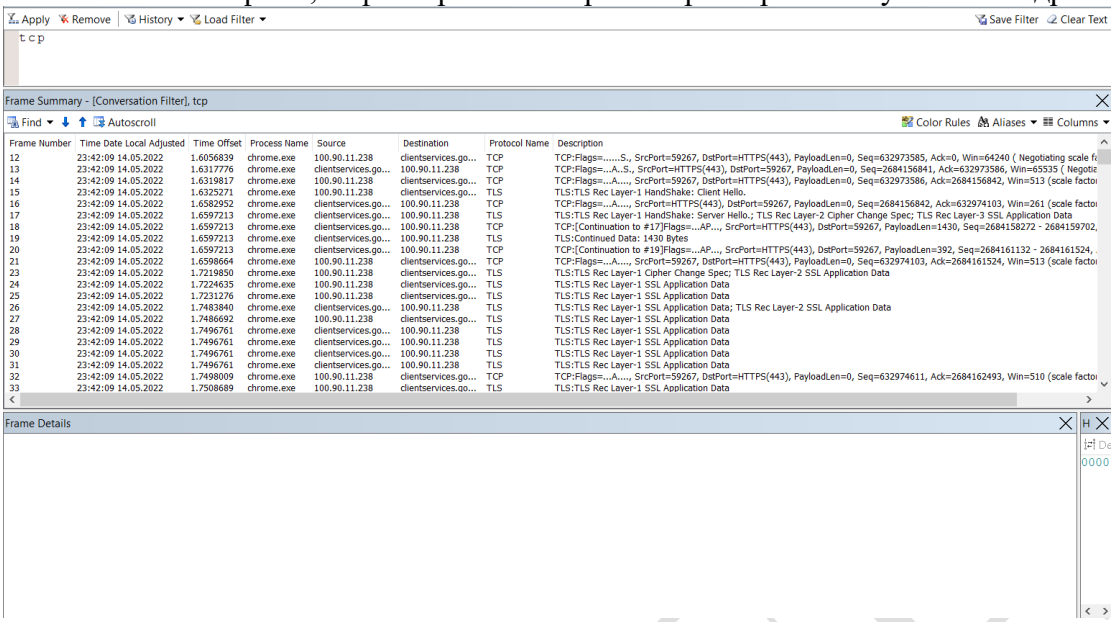
Контрольная сумма, ID и номер пакета, тип объекта.



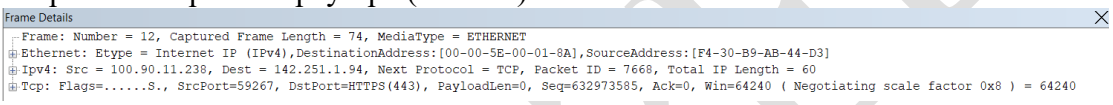
Лабораторная работа № 3

1. Настроили сетевой монитор и запустили Capture. Открыли браузер, зашли на главную страницу сайта и совершили несколько внутренних переходов.

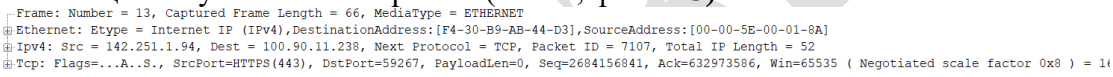
2. Остановили Capture, отфильтровали запросы и разобрали полученные кадры.



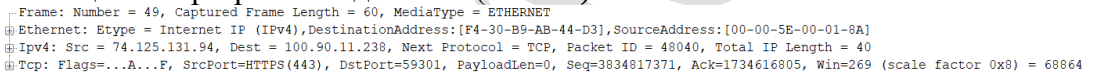
Запрос на открытие браузера (Флаг A)



Квитанция об успешном открытии (Ответ, флаг AS)



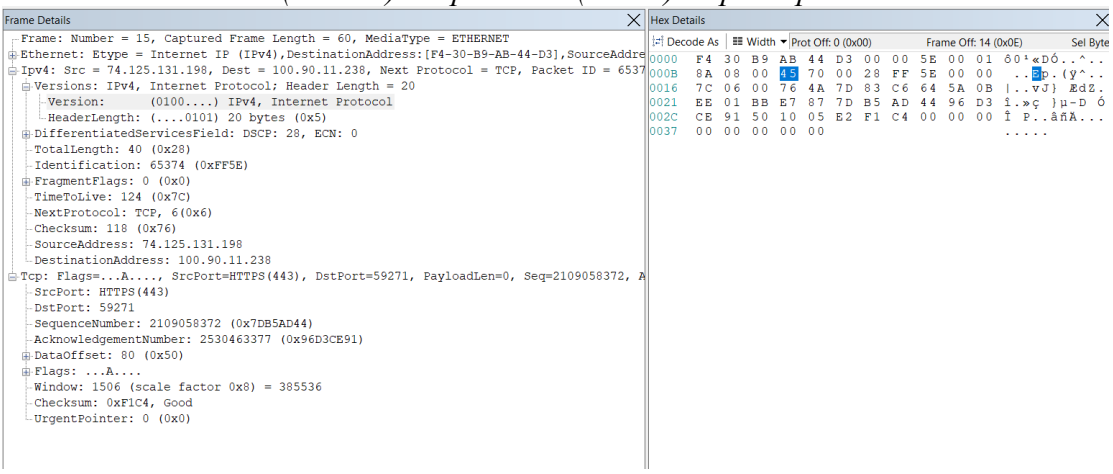
Сообщение о разрыве соединения (Флаг F)



3. Посчитали контрольную суму заголовка.

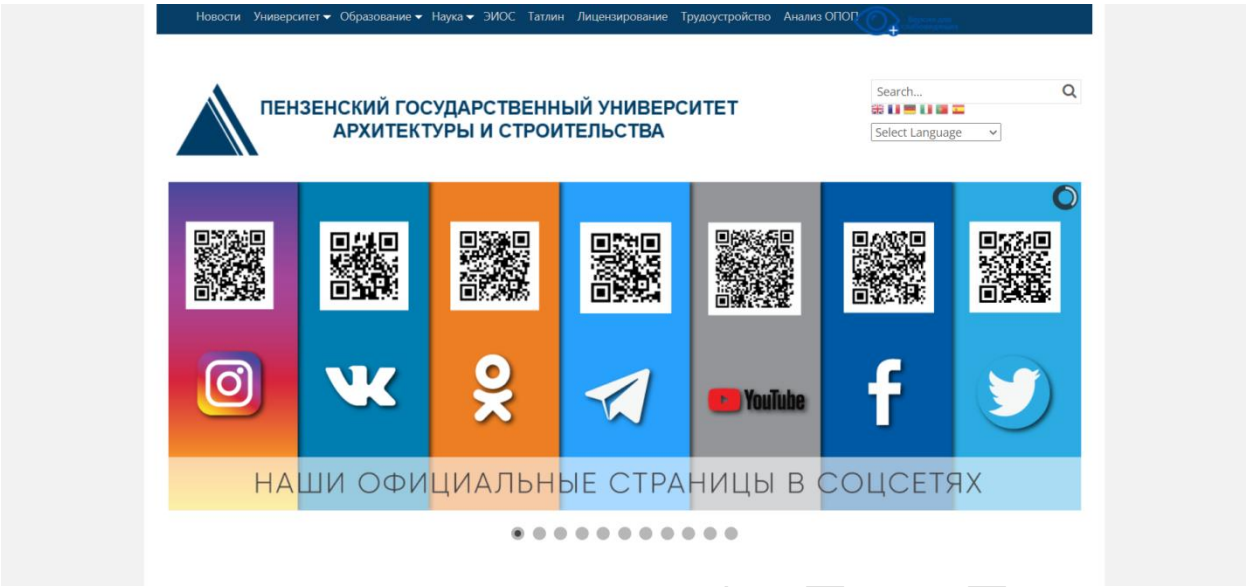
Контрольная сумма пакета TCP = Псевдо-заголовок (IP) + TCP-заголовок + TCP-сообщение = 76_{16}

Псевдозаголовок = IP-адрес источника + IP-адрес получателя + длина сегмента TCP/UDP (16 бит) + протокол (8 бит) + фиксированные 8 биты

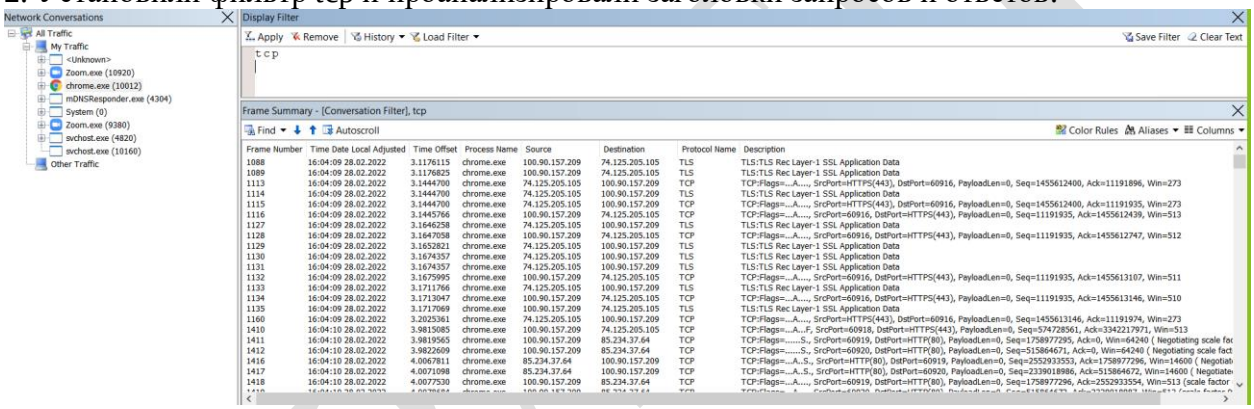


Лабораторная работа № 4

1. Настроили сетевой монитор и запустили Capture. Зашли на главную страницу http://pguas.ru/ и закрыли браузер.

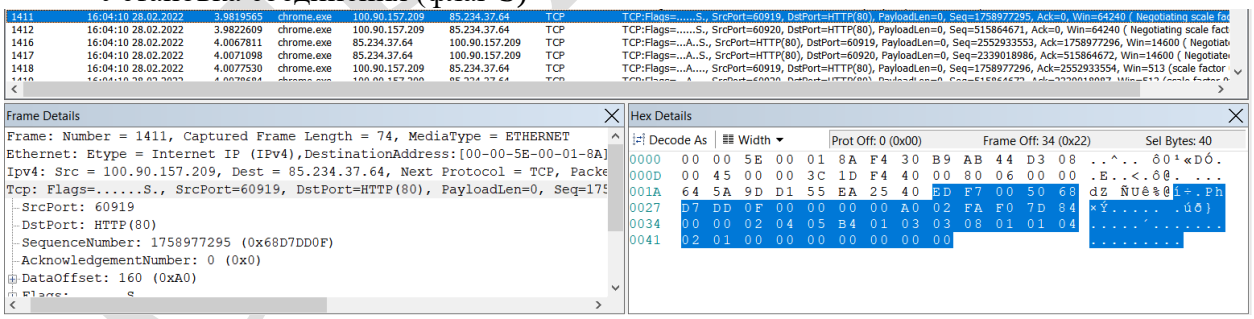


2. Установили фильтр tcp и проанализировали заголовки запросов и ответов.

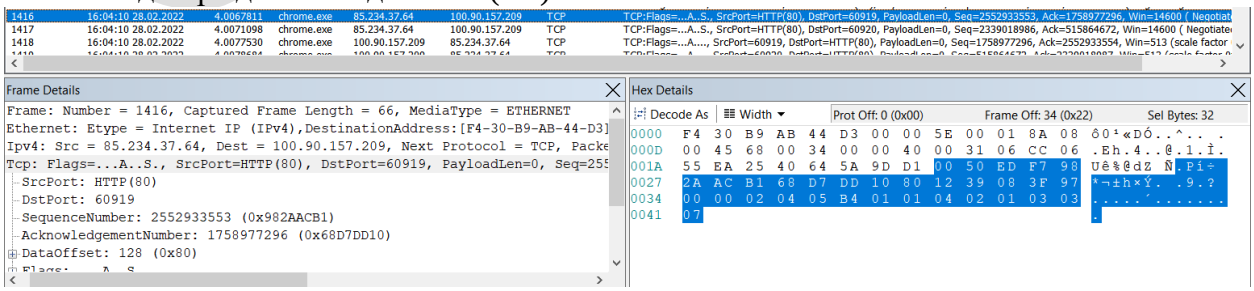


3. Разобрали полученные кадры.

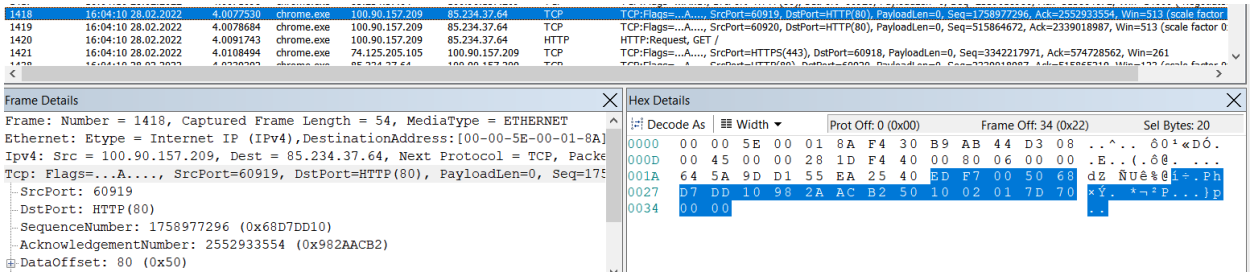
Установка соединения (флаг S)



Подтверждение соединения (AS)

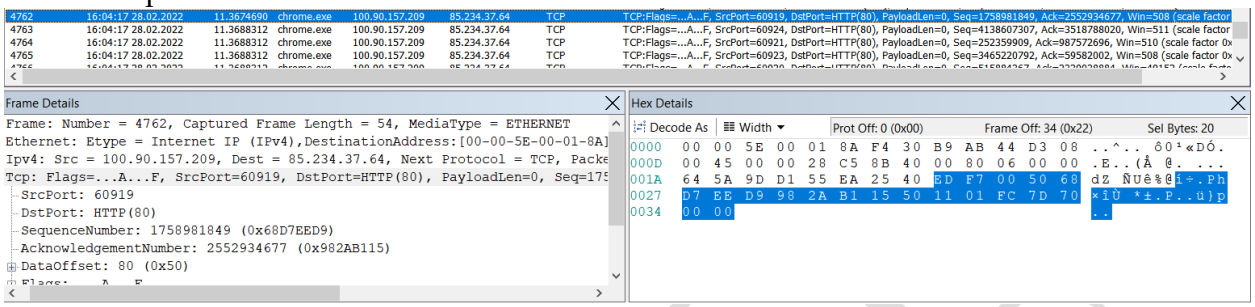


Квитанция об окончательном подтверждении (флаг A)

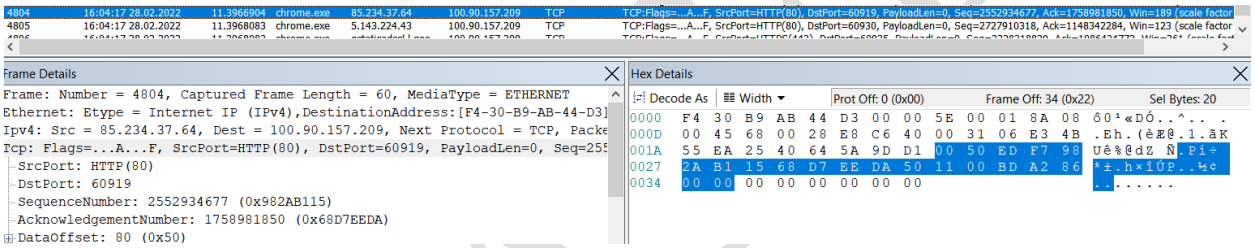


Квитанция о разрыве соединения (флаг AF) Запрос и ответ

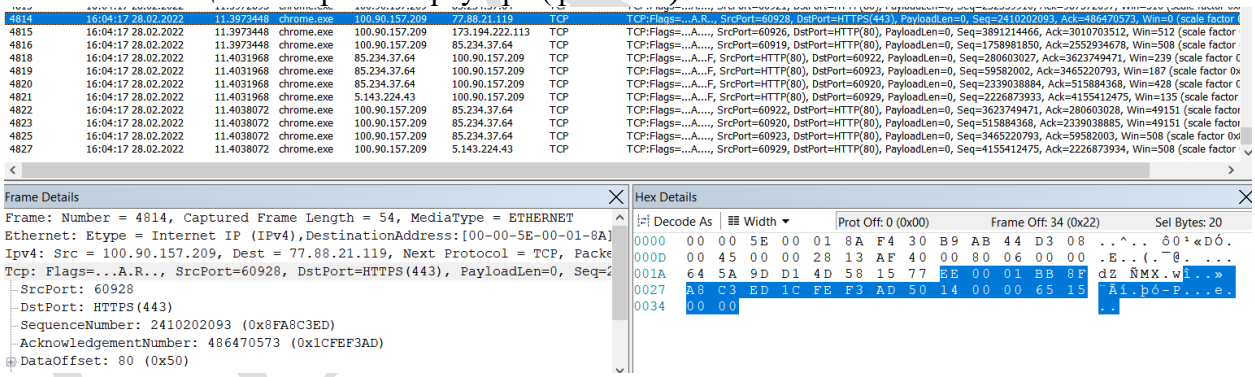
Запрос



Ответ

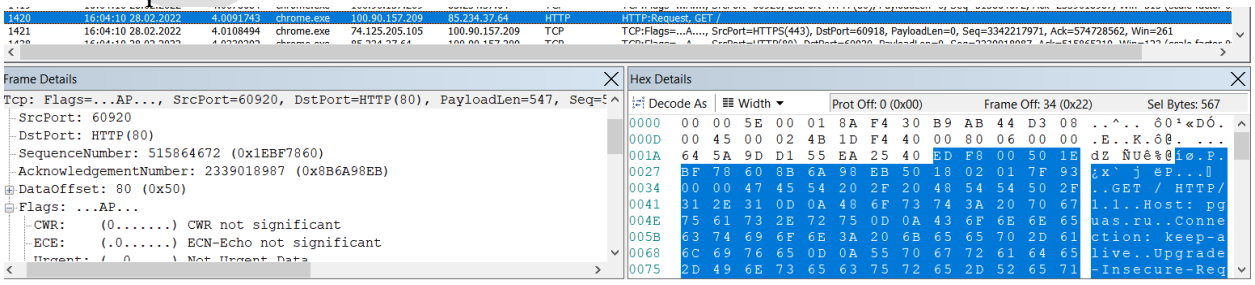


Квитанция о закрытии браузера (флаг AR)

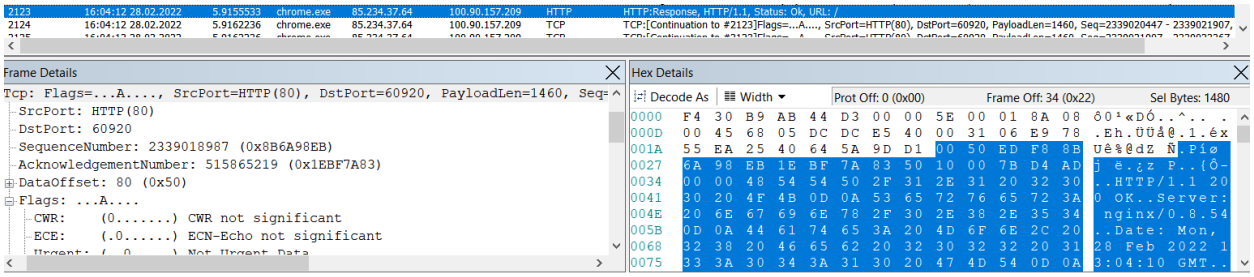


4. Посмотрели get запрос полученный при загрузке страницы. Запрос вернулся с кодом 200, значит, ошибок не возникло.

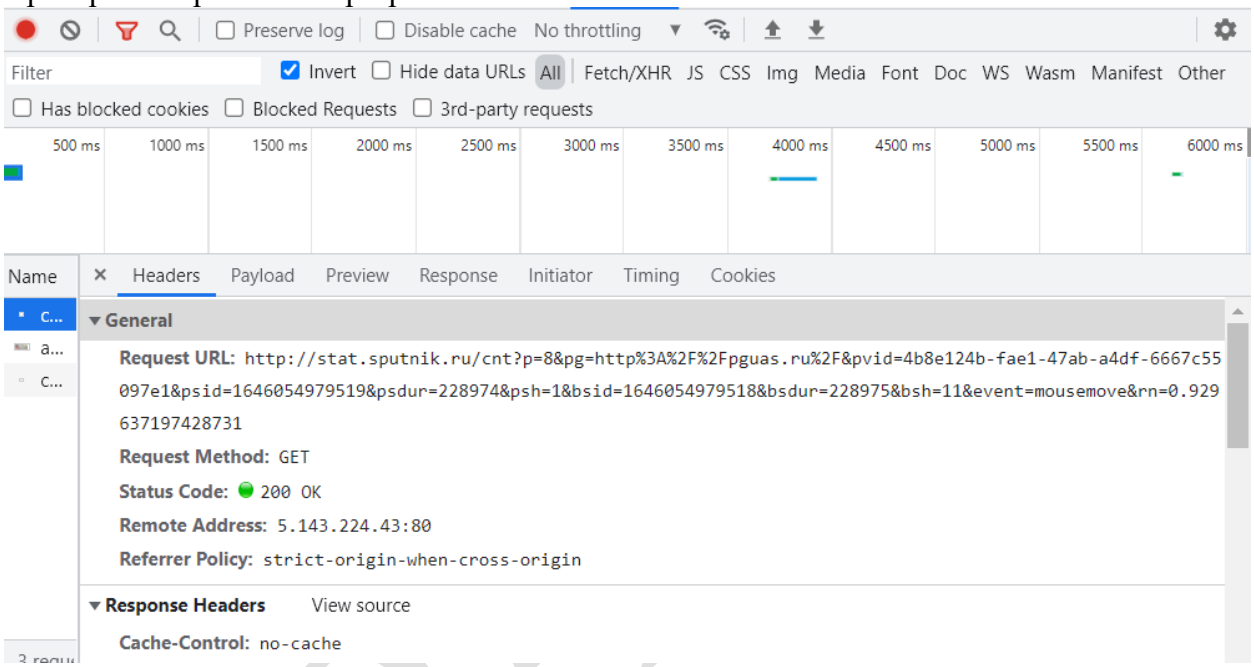
Запрос



Ответ

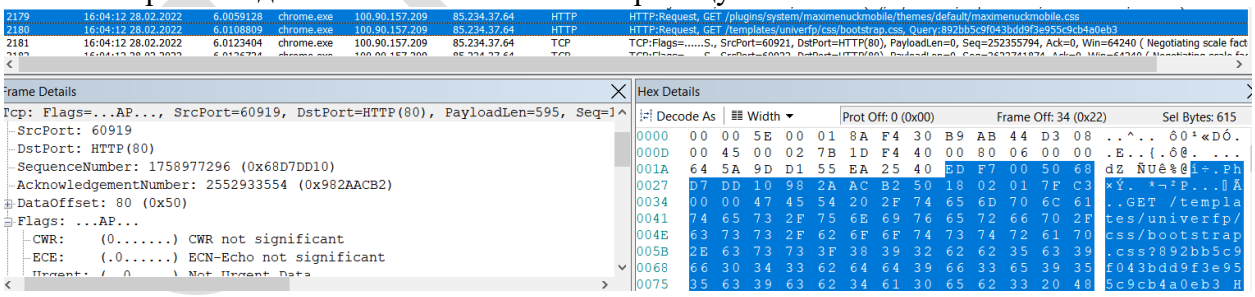


Проверили через панель разработчика



5. Посмотрели код страницы и представили в отчёте теги, которые вызвали запрос к веб-серверу и ответ сервера

Запрос о подключении css стилей на страницу



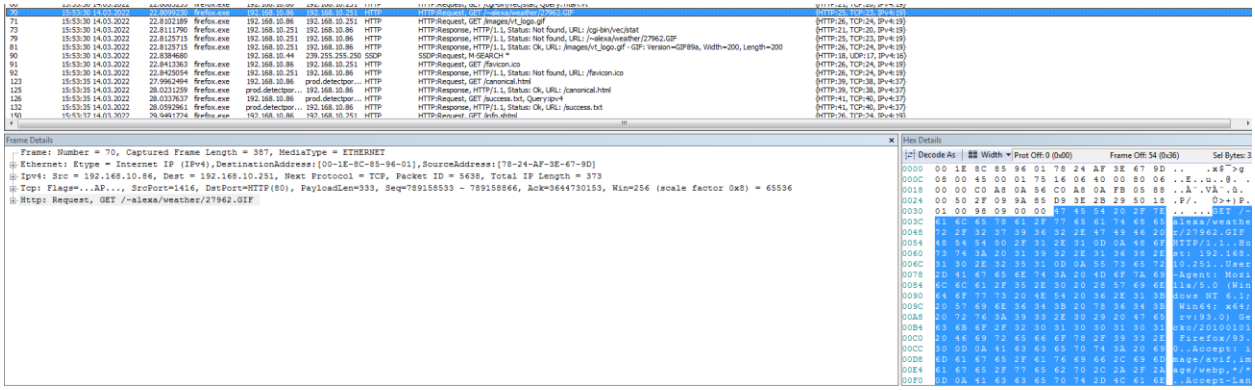
Вызван следующими тегами

```
<link href="/plugins/system/maximenuckmobile/themes/default/maximenuckmobile.css" rel="stylesheet" />
<link href="/templates/univerfp/css/bootstrap.css?892bb5c9f043bdd9f3e955c9cb4a0eb3" rel="stylesheet" />
```

Настроили http соединение и разобрали некоторые запросы.

Запрос о подключении изображения на страницу вызван следующим тегом

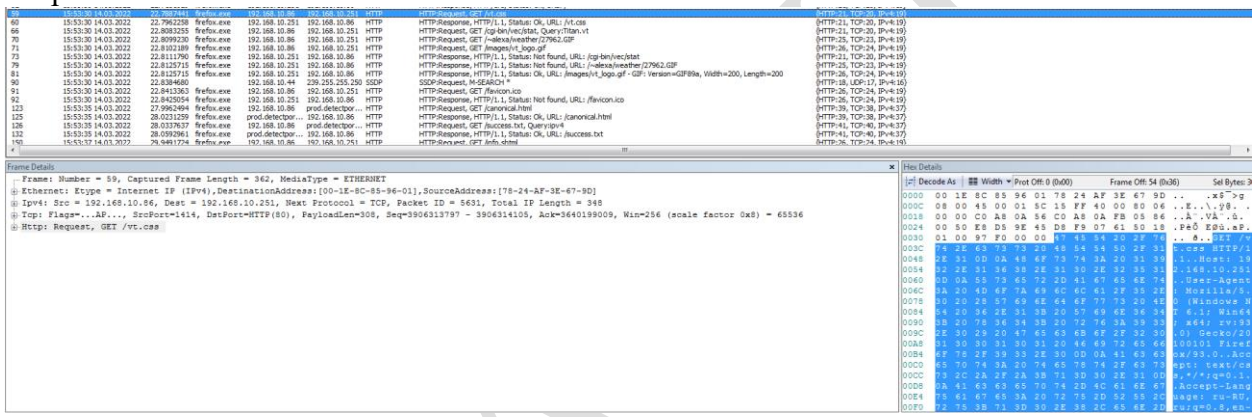
<td align="center"> <img src="/~alexa/weather/27962.GIF" border="0">



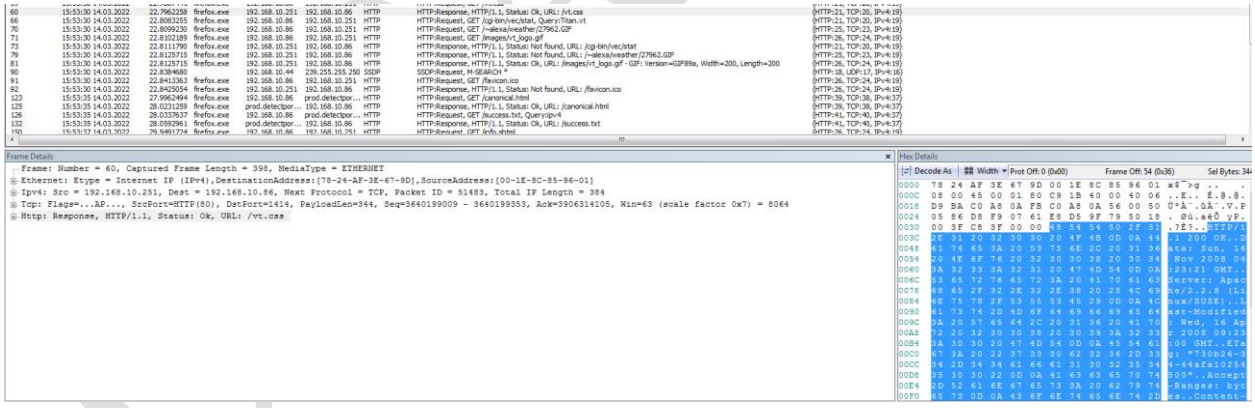
Подключение стилей на страницу

<link rel="stylesheet" href="vt.css" type="text/css">

Запрос

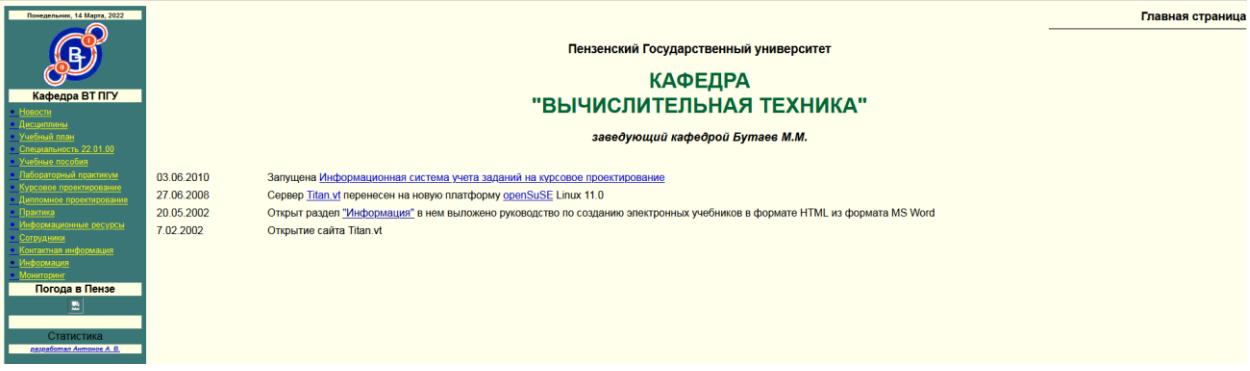


Ответ

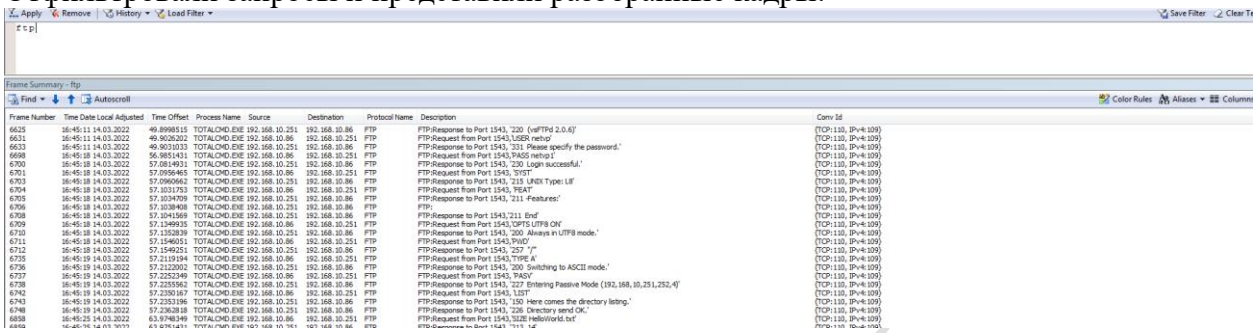


Лабораторная работа № 5

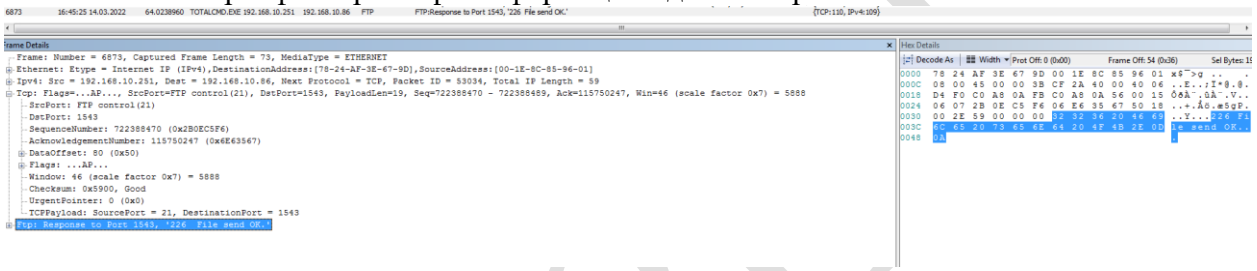
1. Настроили сетевой монитор и зашли на ftp сервер по адресу 192.168.10.251



2. Запустили Total Commander и настроили фильтрацию по протоколу ftp . Зашли на ftp сервер, изменили файл и сохранили его на сетевой диск. Отфильтровали запросы и представили разобранные кадры.



Сетевой монитор с фильтром ftp. Информация идёт на порт 21.



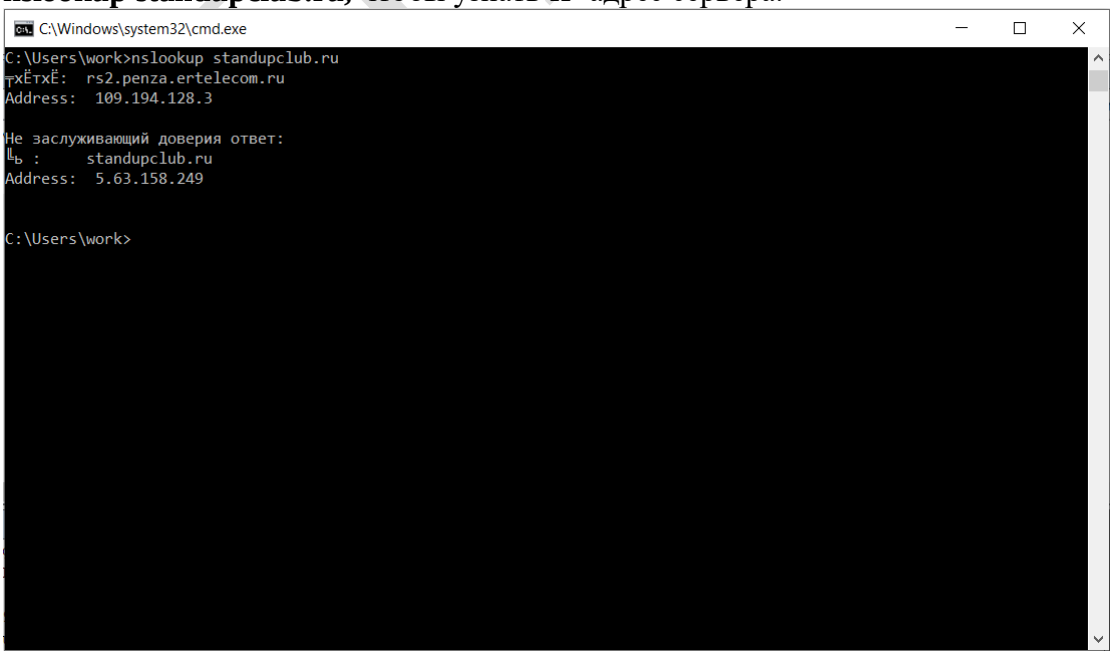
3. Сравнили кадры сетевого монитора и Commander, они соответствуют сетевому монитору. В сетевом мониторе кадры представлены более подробно, но ответ называется «запросом».

Сохранение файла.

```
Download
Waiting for server...
226 File send OK.
Copied (14.03.2022 16:45:25): ftp://192.168.10.251//HelloWorld.txt -> C:\Users\student\AppData\Local\Temp\_tc\HelloWorld.txt 14 bytes, 0 kbytes/s
```

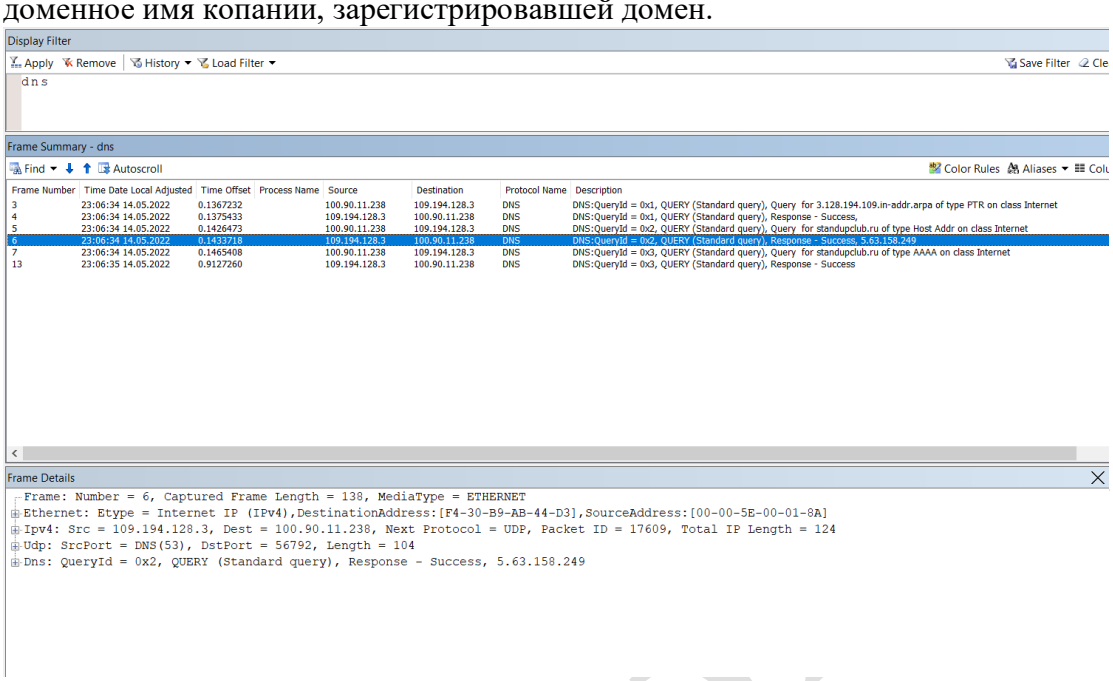
Лабораторная работа № 6

1. Создали и настроили новую Capture, запустили её. Ввели в командную строку **nslookup standupclub.ru,** чтобы узнать IP-адрес сервера.

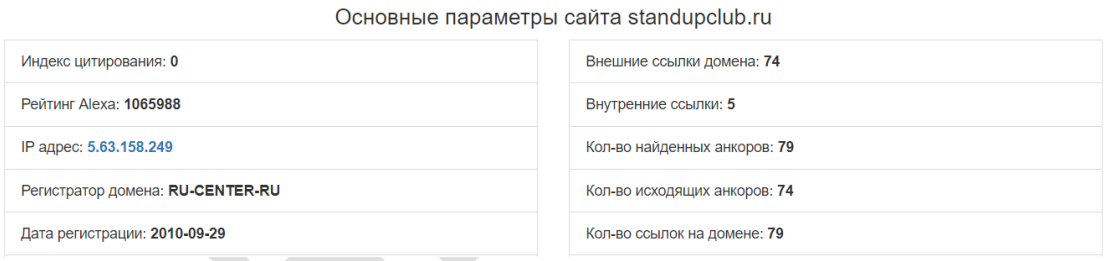


2. Отфильтровали запросы и разобрали DNS-кадры. Пинг успешно дошёл до сервера, на рисунке ниже представлен ответ.

Flags: Response, Opcode - QUERY (Standard query), RD, RA, Rcode - Success - успешный ответ
ARecord: standupclub.ru of type Host Addr on class Internet: 5.63.158.249 - IP-адрес
AuthorityRecord: standupclub.ru of type NS on class Internet: dns1.yandex.net - доменное имя копании, зарегистрировавшей домен.

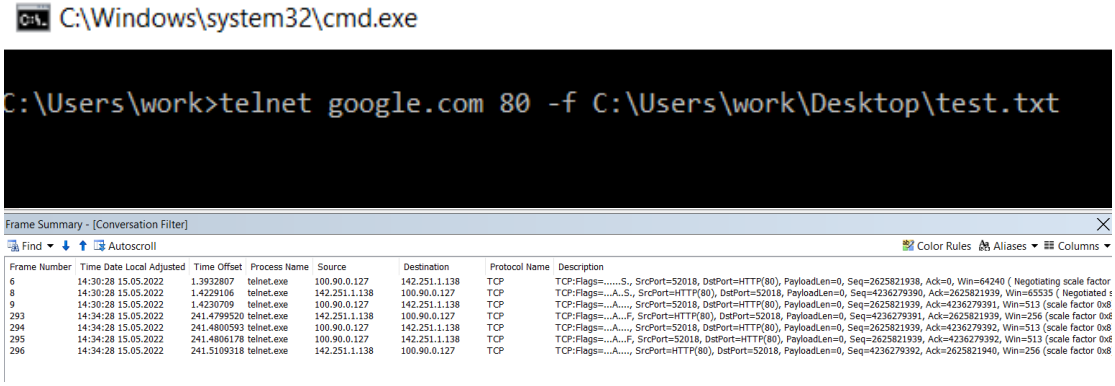


3. С помощью сервиса WHOIS проверили правильность работы утилиты. Утилита работает верно.



Лабораторная работа № 7

1. Создали и настроили новую Capture, настроили telnet-клиент (Как это сделать, показано в руководстве по cmd). Запустили окно захвата и подключились к telnet-серверу.
2. Добавили файл с ПК на сервер с помощью команды telnet google.com 80 -f C:\Users\work\Desktop\test.txt.



3. Остановили окно захвата и разобрали полученные кадры.

Квитанция об успешном подключении к серверу

```
⊞ Ipv4: Src = 142.251.1.138, Dest = 100.90.0.127, Next Protocol = TCP, Packet ID = 5061, Total IP Length = 52
⊟ Tcp: Flags=...A..S., SrcPort=HTTP(80), DstPort=52018, PayloadLen=0, Seq=4236279390, Ack=2625821939, Win=65535 ( Negotiated scale factor 0x8 ) = 1
    SrcPort: HTTP(80)
    DstPort: 52018
    SequenceNumber: 4236279390 (0xFC807E5E)
    AcknowledgementNumber: 2625821939 (0x9C82DCF3)
  ⊞ DataOffset: 128 (0x80)
  ⊞ Flags: ...A..S.
    Window: 65535 ( Negotiated scale factor 0x8 ) = 16776960
    Checksum: 0xB9E7, Good
    UrgentPointer: 0 (0x0)
  ⊞ TCPOptions:
```

Квитанция о разрыве соединения

```
  Frame: Number = 295, Captured Frame Length = 54, MediaType = ETHERNET
⊞ Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[00-00-5E-00-01-8A],SourceAddress:[F4-30-B9-AB-44-D3]
⊞ Ipv4: Src = 100.90.0.127, Dest = 142.251.1.138, Next Protocol = TCP, Packet ID = 19884, Total IP Length = 40
⊟ Tcp: Flags=...A...F, SrcPort=52018, DstPort=HTTP(80), PayloadLen=0, Seq=2625821939, Ack=4236279392, Win=513 (scale factor 0x8) = 131328
    SrcPort: 52018
    DstPort: HTTP(80)
    SequenceNumber: 2625821939 (0x9C82DCF3)
    AcknowledgementNumber: 4236279392 (0xFC807E60)
  ⊞ DataOffset: 80 (0x50)
  ⊞ Flags: ...A...F
    Window: 513 (scale factor 0x8) = 131328
    Checksum: 0xF578, Disregarded
    UrgentPointer: 0 (0x0)
```