

## 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 . . . . . :
```

Адаптер Ethernet Ethernet:

DNS-суффикс подключения . . . . . :  
Описание. . . . . : Realtek PCIe GBE Family Controller  
Физический адрес. . . . . : F4-30-B9-AB-44-D3  
DHCP включен. . . . . : Да  
Автонастройка включена. . . . . : Да  
Локальный IPv6-адрес канала . . . . . : fe80::d97d:182e:9db1:64aa%19(Основной)  
IPv4-адрес. . . . . : 100.90.157.209(Основной)  
Маска подсети . . . . . : 255.255.192.0  
Аренда получена. . . . . : 28 апреля 2022 г. 18:41:04  
Срок аренды истекает. . . . . : 28 апреля 2022 г. 23:14:12  
Основной шлюз. . . . . : 100.90.191.254  
DHCP-сервер. . . . . : 109.194.128.70  
IAID DHCPv6 . . . . . : 66334905  
DUID клиента DHCPv6 . . . . . : 00-01-00-01-21-1B-C4-A1-F4-30-B9-AB-44-D3  
DNS-серверы. . . . . : 109.194.128.3  
                          5.3.3.3  
NetBios через TCP/IP. . . . . : Включен

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**.

```
C:\Users\work> nslookup pnzgu.ru
Trx ётхё: rs2.penza.ertelecom.ru
Address: 109.194.128.3

Не заслуживающий доверия ответ:
Лъ : pnzgu.ru
Addresses: 2001:b08:15:1::25
              82.179.90.25
```

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=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% потеря)

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% потеря

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% потеря)

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% потеря)

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.

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

<b>Маршрутизатор</b>	<b>sigma.pnzgu.ru [82.179.90.225]</b>
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**

```
C:\Windows\system32\cmd.exe
C:\Users\work>netstat -s -p tcp
Статистика TCP для IPv4

Активных открыто          = 1823
Пассивных открыто         = 53
Сбоев при подключении     = 107
Сброшено подключений      = 337
Текущих подключений       = 39
Получено сегментов        = 114904
Отправлено сегментов      = 73116
Повторно отправлено сегментов = 0

Активные подключения

Имя    Локальный адрес   Внешний адрес   Состояние
TCP    100.90.157.209:51089 20.54.37.64:https ESTABLISHED
TCP    100.90.157.209:51112 static:https      ESTABLISHED
TCP    100.90.157.209:51219 static:https      ESTABLISHED
TCP    100.90.157.209:51220 static:https      ESTABLISHED
TCP    100.90.157.209:51239 45.192.128.14:http CLOSE_WAIT
TCP    100.90.157.209:51247 mc:https        ESTABLISHED
TCP    100.90.157.209:51261 45.192.128.16:http CLOSE_WAIT
TCP    100.90.157.209:51291 149.154.167.41:https ESTABLISHED
TCP    100.90.157.209:51300 91.105.192.100:https ESTABLISHED
TCP    100.90.157.209:51313 91.105.192.100:https ESTABLISHED
TCP    100.90.157.209:51346 ec2-44-239-15-106:https ESTABLISHED
TCP    100.90.157.209:51429 45.192.128.17:http CLOSE_WAIT
TCP    100.90.157.209:51433 163.171.142.159:https CLOSE_WAIT
```

Закрыли браузеры и повторно ввели команду - активных подключений стало меньше

```
C:\Windows\system32\cmd.exe
C:\Users\work>netstat -s -p tcp

Статистика TCP для IPv4

Активных открыто          = 1836
Пассивных открыто         = 53
Сбоев при подключении      = 108
Сброшено подключений      = 360
Текущих подключений       = 12
Получено сегментов        = 120125
Отправлено сегментов      = 75421
Повторно отправлено сегментов = 0

Активные подключения

Имя      Локальный адрес   Внешний адрес   Состояние
TCP      100.90.157.209:51089 20.54.37.64:https ESTABLISHED
TCP      100.90.157.209:51112 static:https      TIME_WAIT
TCP      100.90.157.209:51219 static:https      TIME_WAIT
TCP      100.90.157.209:51220 static:https      TIME_WAIT
TCP      100.90.157.209:51239 45.192.128.14:http CLOSE_WAIT
TCP      100.90.157.209:51261 45.192.128.16:http CLOSE_WAIT
TCP      100.90.157.209:51291 149.154.167.41:https ESTABLISHED
TCP      100.90.157.209:51300 91.105.192.100:https ESTABLISHED
TCP      100.90.157.209:51313 91.105.192.100:https ESTABLISHED
TCP      100.90.157.209:51429 45.192.128.17:http CLOSE_WAIT
TCP      100.90.157.209:51433 163.171.142.159:https CLOSE_WAIT
TCP      100.90.157.209:51436 45.192.128.17:http CLOSE_WAIT
TCP      100.90.157.209:51457 36:https        TIME_WAIT
TCP      100.90.157.209:51465 239:https       TIME_WAIT
TCP      100.90.157.209:51466 server-205-251-219-35:https TIME_WAIT
TCP      100.90.157.209:51469 201:https        TIME_WAIT
TCP      100.90.157.209:51470 ec2-34-224-146-81:https TIME_WAIT
TCP      100.90.157.209:51471 server-65-9-54-92:https ESTABLISHED
TCP      100.90.157.209:51475 dedicated:https    TIME_WAIT
TCP      100.90.157.209:51476 149.154.167.151:https TIME_WAIT
TCP      100.90.157.209:51478 a2-23-167-51:http  ESTABLISHED
TCP      100.90.157.209:51481 a2-23-167-51:http  ESTABLISHED

C:\Users\work>
```

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.

```
C:\Windows\system32\cmd.exe
TCP 127.0.0.1:51524 127.0.0.1:51525 ESTABLISHED
TCP 127.0.0.1:51525 127.0.0.1:51524 ESTABLISHED
TCP 127.0.0.1:51527 127.0.0.1:51533 ESTABLISHED
TCP 127.0.0.1:51533 127.0.0.1:51532 ESTABLISHED
TCP 127.0.0.1:51546 127.0.0.1:51547 ESTABLISHED
TCP 127.0.0.1:51547 127.0.0.1:51546 ESTABLISHED
TCP 127.0.0.1:51549 127.0.0.1:51550 ESTABLISHED
TCP 127.0.0.1:51550 127.0.0.1:51549 ESTABLISHED
TCP 127.0.0.1:51551 127.0.0.1:51552 ESTABLISHED
TCP 127.0.0.1:51552 127.0.0.1:51551 ESTABLISHED
=====
Список интерфейсов
3...a2 af bd e7 43 ....Microsoft Wi-Fi Direct Virtual Adapter
10...a9 af bd e7 43 ee ....Microsoft Wi-Fi Direct Virtual Adapter #2
18...f4 30 b9 ab 4d d3 ....Realtek PCIe GBE Family Controller
9...98 af bd e7 43 ed ....intel(R) Dual Band Wireless-AC 7265
12...a9 af bd e7 43 f1 ....Bluetooth Device (Personal Area Network)
1....Software Loopback Interface 1

IPv4 таблица маршрута
=====
Активные маршруты:
Сетевой адрес      Маска сети     Адрес шлюза   Интерфейс   Метрика
0.0.0.0          0.0.0.0       108.90.191.254 108.90.157.209  35
108.90.128.0    255.255.192.0        On-link      108.90.157.209  291
108.90.157.209  255.255.255.255        On-link      108.90.157.209  291
108.90.191.255  255.255.255.255        On-link      108.90.157.209  291
127.0.0.0        255.0.0.0       127.0.0.1      127.0.0.1   331
130.0.0.0        255.255.255.255        On-link      127.0.0.1   331
127.253.255.255 255.255.255.255        On-link      127.0.0.1   331
224.0.0.0        240.0.0.0       127.0.0.1      127.0.0.1   331
224.0.0.0        240.0.0.0       108.90.157.209 108.90.157.209  291
255.255.255.255 255.255.255.255        On-link      127.0.0.1   331
255.255.255.255 255.255.255.255        On-link      108.90.157.209  291

Постоянные маршруты:
Отсутствует

IPv6 таблица маршрута
=====
Активные маршруты:
Метрика Сетевой адрес      Шлюз
1      331 ::1/128        On-link
18     291 fe80::/64       On-link
18     291 fe80::97d1:182e:16aa:/128
1      331 ff00::/8        On-link
18     291 ff00::/8        On-link
```

Остановили работу утилиты с помощью сочетания клавиш Ctrl+C.

## Лабораторная работа № 2

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

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

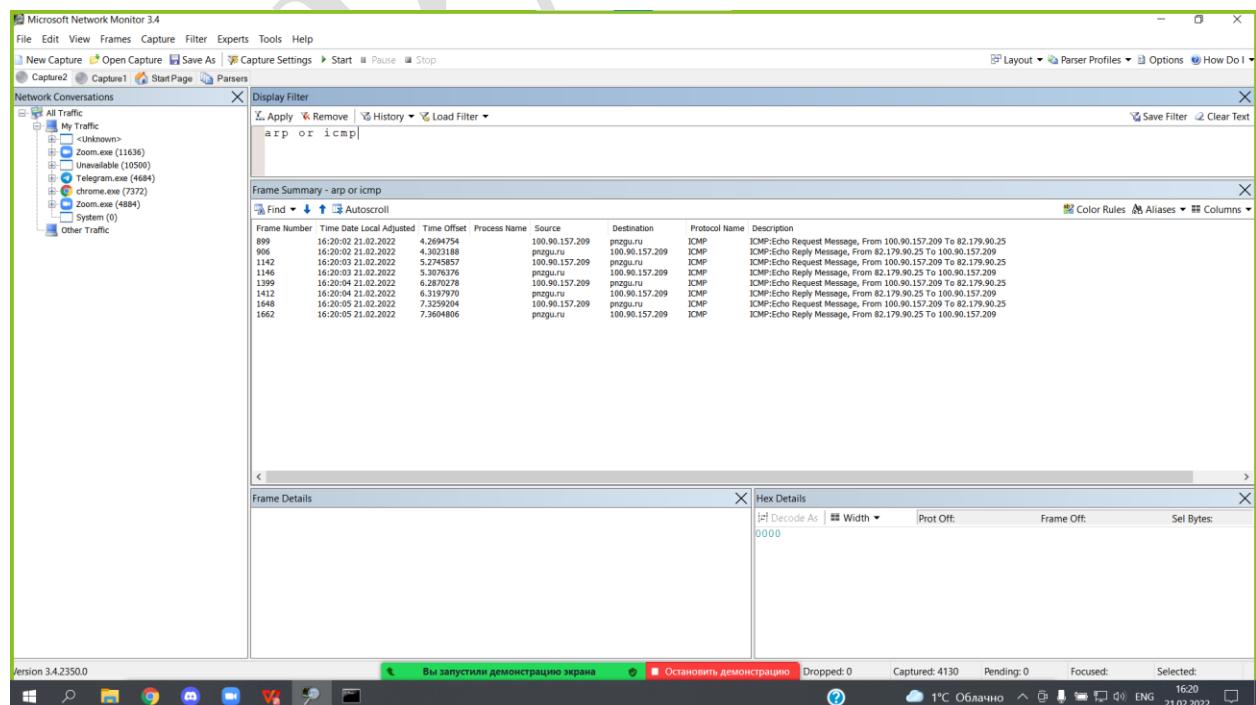
Интерфейс: 100.90.157.209 --- 0x12
    адрес в Интернете      Физический адрес      Тип
    100.90.191.254        00-00-5e-00-01-8a      динамический
    224.0.0.22            01-00-5e-00-00-16      статический
    255.255.255.255      ff-ff-ff-ff-ff-ff      статический
```

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% потеря)
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
```

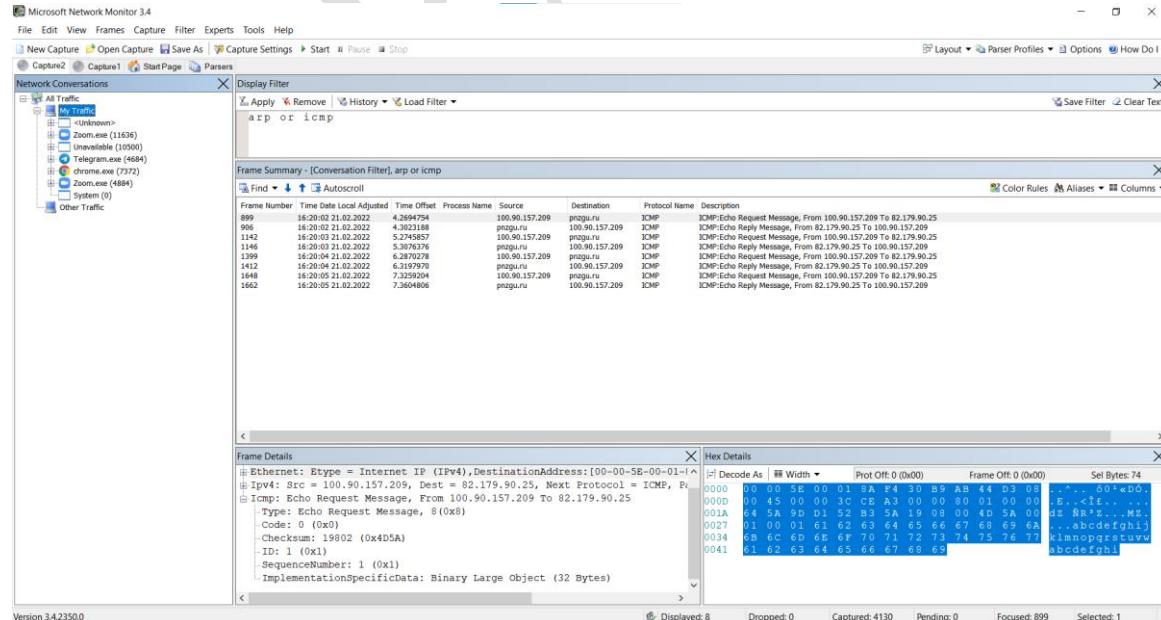
4. Разобрали протокол ICMP. С помощью утилиты traceroute отправили эхо-сообщение на удалённый сервер. Отфильтровали и разобрали полученные кадры.

Данный протокол рассыпает 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.

Frame Summary - [Conversation Filter], tcp

Frame Number	Time	Date	Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
12	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=.....S., SrcPort=59267, DstPort=HTTP(443), PayloadLen=0, Seq=632973585, Ack=0, Win=64240 ( Negotiating scale factor )
13	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=...A..S., SrcPort=HTTP(443), DstPort=59267, PayloadLen=0, Seq=632973584, Ack=632973586, Win=65535 ( scale factor )
14	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=...A..S., SrcPort=HTTP(443), DstPort=59267, PayloadLen=0, Seq=632973586, Ack=2684156842, Win=513 ( scale factor )
15	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TLS	TLS:TLS Rec Layer-1 Handshake: Client Hello.
16	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=...A..S., SrcPort=HTTP(443), DstPort=59267, PayloadLen=0, Seq=632974103, Ack=632974103, Win=261 ( scale factor )
17	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TLS	TLS:TLS Rec Layer-1 Handshake: Server Hello, TLS Rec Layer-2 Cipher Change Spec; TLS Rec Layer-2 SSL Application Data
18	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:[Continuation to #17]Flags=...A..P., SrcPort=HTTP(443), DstPort=59267, PayloadLen=1430, Seq=2684158272, Ack=2684159702, Win=510 ( scale factor )
19	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TLS	TCP:[Continuation to #19]Flags=...A..P., SrcPort=HTTP(443), DstPort=59267, PayloadLen=392, Seq=632974103, Ack=2684161132 - 2684161524, Win=513 ( scale factor )
20	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:[Continuation to #19]Flags=...A..P., SrcPort=HTTP(443), DstPort=59267, PayloadLen=392, Seq=632974103, Ack=2684161132 - 2684161524, Win=513 ( scale factor )
21	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=...A..S., SrcPort=59267, DstPort=HTTP(443), PayloadLen=0, Seq=632974103, Ack=64240 ( Negotiating scale factor 0x8 ) = 64240
23	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TLS	TLS:TLS Rec Layer-1 Cipher Change Spec; TLS Rec Layer-2 SSL Application Data
24	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TLS	TLS:TLS Rec Layer-1 Application Data
25	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TLS	TLS:TLS Rec Layer-1 SSL Application Data
26	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TLS	TLS:TLS Rec Layer-1 SSL Application Data; TLS Rec Layer-2 SSL Application Data
27	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TLS	TLS:TLS Rec Layer-1 SSL Application Data
28	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TLS	TLS:TLS Rec Layer-1 SSL Application Data
29	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TLS	TLS:TLS Rec Layer-1 SSL Application Data
30	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TLS	TLS:TLS Rec Layer-1 SSL Application Data
31	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TLS	TLS:TLS Rec Layer-1 SSL Application Data
32	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=...A..S., SrcPort=59267, DstPort=HTTP(443), PayloadLen=0, Seq=632974611, Ack=2684162493, Win=510 ( scale factor )
33	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TLS	TLS:TLS Rec Layer-1 SSL Application Data

Frame Details

```
[H] D6 0000
```

### Запрос на открытие браузера (Флаг A)

Frame Details

```
[H] D6 0000
```

Frame: Number = 12, Captured Frame Length = 74, MediaType = ETHERNET  
 Ethernet: Etype = Internet IP (IPv4), DestinationAddress:[00-00-5E-00-01-8A], SourceAddress:[F4-30-B9-AB-44-D3]  
 Ipv4: Src = 100.90.11.238, Dest = 142.251.1.94, Next Protocol = TCP, Packet ID = 7668, Total IP Length = 60  
 Tcp: Flags=.....S., SrcPort=59267, DstPort=HTTP(443), PayloadLen=0, Seq=632973585, Ack=0, Win=64240 ( Negotiating scale factor 0x8 ) = 64240

### Квитанция об успешном открытии (Ответ, флаг AS)

Frame: Number = 13, Captured Frame Length = 66, MediaType = ETHERNET  
 Ethernet: Etype = Internet IP (IPv4), DestinationAddress:[F4-30-B9-AB-44-D3], SourceAddress:[00-00-5E-00-01-8A]  
 Ipv4: Src = 142.251.1.94, Dest = 100.90.11.238, Next Protocol = TCP, Packet ID = 7107, Total IP Length = 52  
 Tcp: Flags=...A..S., SrcPort=HTTP(443), DstPort=59267, PayloadLen=0, Seq=632973586, Win=5535 ( Negotiated scale factor 0x8 ) = 14

### Сообщение о разрыве соединения (Флаг F)

Frame: Number = 49, 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]  
 Ipv4: Src = 74.125.131.94, Dest = 100.90.11.238, Next Protocol = TCP, Packet ID = 48040, Total IP Length = 40  
 Tcp: Flags=...A..F., SrcPort=HTTP(443), DstPort=59301, PayloadLen=0, Seq=3834817371, Ack=1734616805, Win=269 ( scale factor 0x8 ) = 68864

### 3. Посчитали контрольную сумму заголовка.

Контрольная сумма пакета TCP = Псевдо-заголовок (IP) + TCP-заголовок + TCP-сообщение = 7616

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

Frame Details

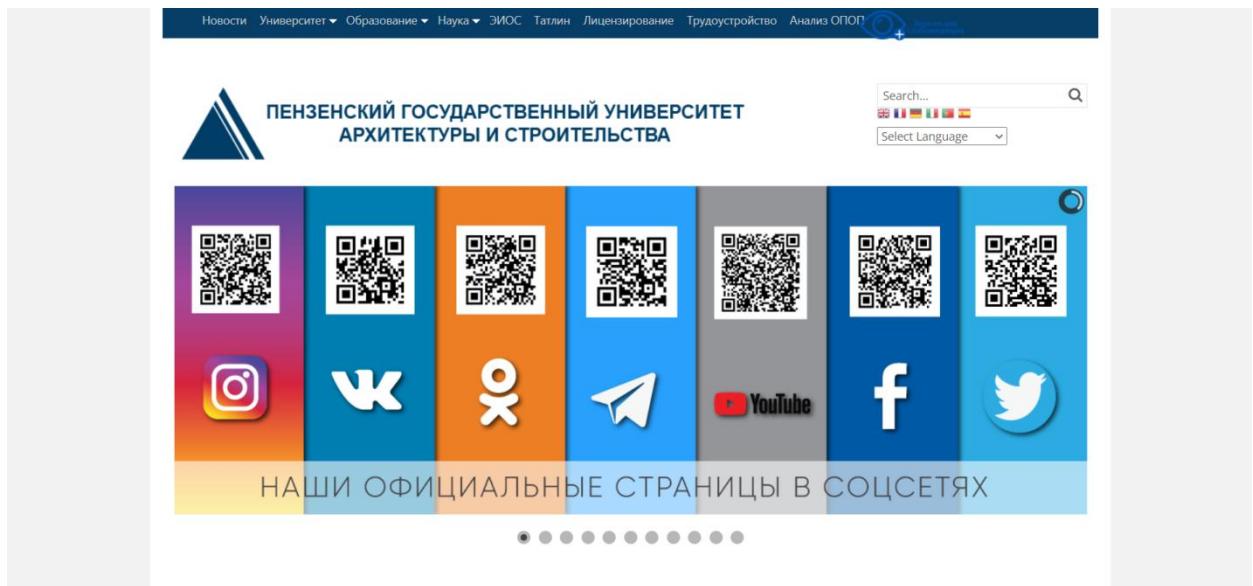
Frame Number	Time	Date	Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
15	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=.....S., SrcPort=59267, DstPort=HTTP(443), PayloadLen=0, Seq=2109058372, Ack=0, Win=64240 ( Negotiating scale factor 0x8 )
16	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=...A..S., SrcPort=59267, DstPort=HTTP(443), PayloadLen=0, Seq=2109058372, Ack=0, Win=64240 ( Negotiating scale factor 0x8 )
17	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=...A..S., SrcPort=59267, DstPort=HTTP(443), PayloadLen=0, Seq=2109058372, Ack=0, Win=64240 ( Negotiating scale factor 0x8 )
18	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=...A..S., SrcPort=59267, DstPort=HTTP(443), PayloadLen=0, Seq=2109058372, Ack=0, Win=64240 ( Negotiating scale factor 0x8 )
19	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=...A..S., SrcPort=59267, DstPort=HTTP(443), PayloadLen=0, Seq=2109058372, Ack=0, Win=64240 ( Negotiating scale factor 0x8 )
20	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=...A..S., SrcPort=59267, DstPort=HTTP(443), PayloadLen=0, Seq=2109058372, Ack=0, Win=64240 ( Negotiating scale factor 0x8 )
21	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=...A..S., SrcPort=59267, DstPort=HTTP(443), PayloadLen=0, Seq=2109058372, Ack=0, Win=64240 ( Negotiating scale factor 0x8 )
22	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=...A..S., SrcPort=59267, DstPort=HTTP(443), PayloadLen=0, Seq=2109058372, Ack=0, Win=64240 ( Negotiating scale factor 0x8 )
23	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=...A..S., SrcPort=59267, DstPort=HTTP(443), PayloadLen=0, Seq=2109058372, Ack=0, Win=64240 ( Negotiating scale factor 0x8 )
24	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=...A..S., SrcPort=59267, DstPort=HTTP(443), PayloadLen=0, Seq=2109058372, Ack=0, Win=64240 ( Negotiating scale factor 0x8 )
25	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=...A..S., SrcPort=59267, DstPort=HTTP(443), PayloadLen=0, Seq=2109058372, Ack=0, Win=64240 ( Negotiating scale factor 0x8 )
26	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=...A..S., SrcPort=59267, DstPort=HTTP(443), PayloadLen=0, Seq=2109058372, Ack=0, Win=64240 ( Negotiating scale factor 0x8 )
27	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=...A..S., SrcPort=59267, DstPort=HTTP(443), PayloadLen=0, Seq=2109058372, Ack=0, Win=64240 ( Negotiating scale factor 0x8 )
28	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=...A..S., SrcPort=59267, DstPort=HTTP(443), PayloadLen=0, Seq=2109058372, Ack=0, Win=64240 ( Negotiating scale factor 0x8 )
29	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=...A..S., SrcPort=59267, DstPort=HTTP(443), PayloadLen=0, Seq=2109058372, Ack=0, Win=64240 ( Negotiating scale factor 0x8 )
30	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=...A..S., SrcPort=59267, DstPort=HTTP(443), PayloadLen=0, Seq=2109058372, Ack=0, Win=64240 ( Negotiating scale factor 0x8 )
31	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=...A..S., SrcPort=59267, DstPort=HTTP(443), PayloadLen=0, Seq=2109058372, Ack=0, Win=64240 ( Negotiating scale factor 0x8 )
32	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=...A..S., SrcPort=59267, DstPort=HTTP(443), PayloadLen=0, Seq=2109058372, Ack=0, Win=64240 ( Negotiating scale factor 0x8 )
33	23:42:09	14.05.2022			chrome.exe	100.90.11.238	clientservices.go...	TCP	TCP:Flags=...A..S., SrcPort=59267, DstPort=HTTP(443), PayloadLen=0, Seq=2109058372, Ack=0, Win=64240 ( Negotiating scale factor 0x8 )

Hex Details

[H]	Decode As	Width	Prot Off: 0x00	Frame Off: 14 (0x0E)	Sel Byte
0000	F4 30 B9 AB 44 D3 00 00 00 5B 00 01 00 00	0x00	0x00	0x00	0x00
0001	8A 08 00 43 70 00 28 FF 5E 00 00 00 00 00 00	0x00	0x00	0x00	0x00
0002	7C 06 00 76 4A 7D 83 C6 64 5A 0B 00 00 00 00 00	0x00	0x00	0x00	0x00
0003	EE 01 BB E7 87 7D B5 AD 44 96 D3 00 00 00 00 00	0x00	0x00	0x00	0x00
0004	CE 91 50 10 05 E2 F1 C4 00 00 00 00 00 00 00 00	0x00	0x00	0x00	0x00
0005	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0x00	0x00	0x00	0x00

### 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.

Network Conversations

Display Filter: `tcp`

Frame Summary - [Conversation Filter], `tcp`

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
1088	16:04:09 28.02.2022	3.1176115	chrome.exe	100.90.157.209	74.125.205.105	TLS	TLS:TLS Rec Layer-1 SSL Application Data
1089	16:04:09 28.02.2022	3.1176825	chrome.exe	100.90.157.209	74.125.205.105	TLS	TLS:TLS Rec Layer-1 SSL Application Data
1112	16:04:09 28.02.2022	3.1444769	chrome.exe	100.90.157.209	74.125.205.105	TCP	TCP Flags=...A..., SrcPort=HTTP(80), DstPort=60916, PayloadLen=0, Seq=1455612400, Ack=11191896, Win=273
1114	16:04:09 28.02.2022	3.1444790	chrome.exe	74.125.205.105	100.90.157.209	TLS	TLS:TLS Rec Layer-1 SSL Application Data
1115	16:04:09 28.02.2022	3.1444790	chrome.exe	74.125.205.105	100.90.157.209	TCP	TCP Flags=...A..., SrcPort=HTTP(443), DstPort=60916, PayloadLen=0, Seq=1455612400, Ack=11191935, Win=273
1116	16:04:09 28.02.2022	3.1444795	chrome.exe	100.90.157.209	74.125.205.105	TCP	TCP Flags=...A..., SrcPort=60916, DstPort=HTTP(443), PayloadLen=0, Seq=11191935, Ack=1455612409, Win=513
1117	16:04:09 28.02.2022	3.1444795	chrome.exe	100.90.157.209	74.125.205.105	TLS	TLS:TLS Rec Layer-1 SSL Application Data
1128	16:04:09 28.02.2022	3.1647058	chrome.exe	100.90.157.209	74.125.205.105	TLS	TLS:TLS Rec Layer-1 SSL Application Data
1129	16:04:09 28.02.2022	3.1652821	chrome.exe	74.125.205.105	100.90.157.209	TLS	TLS:TLS Rec Layer-1 SSL Application Data
1130	16:04:09 28.02.2022	3.1674357	chrome.exe	74.125.205.105	100.90.157.209	TLS	TLS:TLS Rec Layer-1 SSL Application Data
1131	16:04:09 28.02.2022	3.1674379	chrome.exe	100.90.157.209	74.125.205.105	TCP	TCP Flags=...A..., SrcPort=60916, DstPort=HTTP(443), PayloadLen=0, Seq=11191935, Ack=1455613107, Win=511
1132	16:04:09 28.02.2022	3.1675995	chrome.exe	100.90.157.209	74.125.205.105	TLS	TLS:TLS Rec Layer-1 SSL Application Data
1133	16:04:09 28.02.2022	3.1711769	chrome.exe	74.125.205.105	100.90.157.209	TLS	TLS:TLS Rec Layer-1 SSL Application Data
1134	16:04:09 28.02.2022	3.1711794	chrome.exe	100.90.157.209	74.125.205.105	TCP	TCP Flags=...A..., SrcPort=60916, DstPort=HTTP(443), PayloadLen=0, Seq=11191935, Ack=1455613106, Win=510
1135	16:04:09 28.02.2022	3.1711794	chrome.exe	100.90.157.209	74.125.205.105	TLS	TLS:TLS Rec Layer-1 SSL Application Data
1160	16:04:09 28.02.2022	3.2025361	chrome.exe	74.125.205.105	100.90.157.209	TCP	TCP Flags=...A..., SrcPort=HTTP(443), DstPort=60916, PayloadLen=0, Seq=1455613146, Ack=11191974, Win=273
1410	16:04:10 28.02.2022	3.9815965	chrome.exe	100.90.157.209	85.234.37.64	TCP	TCP Flags=...A..., SrcPort=60918, DstPort=HTTP(443), PayloadLen=0, Seq=574278561, Ack=3342217971, Win=513
1411	16:04:10 28.02.2022	3.9822609	chrome.exe	100.90.157.209	85.234.37.64	TCP	TCP Flags=...A..., SrcPort=60920, DstPort=HTTP(80), PayloadLen=0, Seq=515864671, Ack=0, Win=6240 ( Negotiate scale fact )
1412	16:04:10 28.02.2022	4.0067811	chrome.exe	85.234.37.64	100.90.157.209	TCP	TCP Flags=...A..., SrcPort=HTTP(80), DstPort=60919, PayloadLen=0, Seq=2552933535, Ack=1758977295, Win=14600 ( Negotiate scale fact )
1416	16:04:10 28.02.2022	4.0071098	chrome.exe	85.234.37.64	100.90.157.209	TCP	TCP Flags=...A..., SrcPort=HTTP(80), DstPort=60920, PayloadLen=0, Seq=2339018986, Ack=515864672, Win=14600 ( Negotiate scale fact )
1417	16:04:10 28.02.2022	4.0077530	chrome.exe	100.90.157.209	85.234.37.64	TCP	TCP Flags=...A..., SrcPort=60919, DstPort=HTTP(80), PayloadLen=0, Seq=2339018986, Ack=515864672, Win=14600 ( Negotiate scale fact )
1418	16:04:10 28.02.2022	4.0077530	chrome.exe	100.90.157.209	85.234.37.64	TCP	TCP Flags=...A..., SrcPort=60919, DstPort=HTTP(80), PayloadLen=0, Seq=1758977296, Ack=2552933544, Win=513 ( scale factor )

### 3. Разобрали полученные кадры.

#### Установка соединения (флаг S)

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
1411	16:04:10 28.02.2022	3.9815965	chrome.exe	100.90.157.209	85.234.37.64	TCP	TCP Flags=...S, SrcPort=60919, DstPort=HTTP(80), PayloadLen=0, Seq=1758977295, Ack=0, Win=6240 ( Negotiate scale fact )
1412	16:04:10 28.02.2022	3.9822609	chrome.exe	100.90.157.209	85.234.37.64	TCP	TCP Flags=...S, SrcPort=60920, DstPort=HTTP(80), PayloadLen=0, Seq=515864671, Ack=0, Win=6240 ( Negotiate scale fact )
1416	16:04:10 28.02.2022	4.0067811	chrome.exe	85.234.37.64	100.90.157.209	TCP	TCP Flags=...A..., SrcPort=HTTP(80), DstPort=60919, PayloadLen=0, Seq=2552933535, Ack=1758977295, Win=14600 ( Negotiate scale fact )
1417	16:04:10 28.02.2022	4.0071098	chrome.exe	85.234.37.64	100.90.157.209	TCP	TCP Flags=...A..., SrcPort=HTTP(80), DstPort=60920, PayloadLen=0, Seq=2339018986, Ack=515864672, Win=14600 ( Negotiate scale fact )
1418	16:04:10 28.02.2022	4.0077530	chrome.exe	100.90.157.209	85.234.37.64	TCP	TCP Flags=...A..., SrcPort=60919, DstPort=HTTP(80), PayloadLen=0, Seq=1758977296, Ack=2552933544, Win=513 ( scale factor )

Frame Details

Hex Details

Frame: Number = 1411, Captured Frame Length = 74, MediaType = ETHERNET

Ethernet: Etype = Internet IP (IPv4), DestinationAddress:[00-00-5E-00-01-8A]

Ipv4: Src = 100.90.157.209, Dest = 85.234.37.64, Next Protocol = TCP, Packe

Tcp: Flags=...S..., SrcPort=60919, DstPort=HTTP(80), PayloadLen=0, Seq=1758977295, Ack=0, Win=6240 ( Negotiate scale fact )

SrcPort: 60919

DstPort: HTTP(80)

SequenceNumber: 1758977295 (0x68D7DD0F)

AcknowledgementNumber: 0 (0x0)

DataOffset: 160 (0xA0)

Flags: S

Frame Details

Hex Details

Frame: Number = 1411, Captured Frame Length = 74, MediaType = ETHERNET

Ethernet: Etype = Internet IP (IPv4), DestinationAddress:[00-00-5E-00-01-8A]

Ipv4: Src = 100.90.157.209, Dest = 85.234.37.64, Next Protocol = TCP, Packe

Tcp: Flags=...S..., SrcPort=60919, DstPort=HTTP(80), PayloadLen=0, Seq=1758977295, Ack=0, Win=6240 ( Negotiate scale fact )

SrcPort: 60919

DstPort: HTTP(80)

SequenceNumber: 1758977295 (0x68D7DD0F)

AcknowledgementNumber: 0 (0x0)

DataOffset: 160 (0xA0)

Flags: S

#### Подтверждение соединения (AS)

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
1416	16:04:10 28.02.2022	4.0067811	chrome.exe	85.234.37.64	100.90.157.209	TCP	TCP Flags=...A..., SrcPort=HTTP(80), DstPort=60919, PayloadLen=0, Seq=2552933535, Ack=1758977296, Win=14600 ( Negotiate scale fact )
1417	16:04:10 28.02.2022	4.0071098	chrome.exe	85.234.37.64	100.90.157.209	TCP	TCP Flags=...A..., SrcPort=HTTP(80), DstPort=60920, PayloadLen=0, Seq=2339018986, Ack=515864672, Win=14600 ( Negotiate scale fact )
1418	16:04:10 28.02.2022	4.0077530	chrome.exe	100.90.157.209	85.234.37.64	TCP	TCP Flags=...A..., SrcPort=60919, DstPort=HTTP(80), PayloadLen=0, Seq=1758977296, Ack=2552933544, Win=513 ( scale factor )

Frame Details

Hex Details

Frame: Number = 1416, Captured Frame Length = 66, MediaType = ETHERNET

Ethernet: Etype = Internet IP (IPv4), DestinationAddress:[F4-30-B9-AB-44-D3]

Ipv4: Src = 85.234.37.64, Dest = 100.90.157.209, Next Protocol = TCP, Packe

Tcp: Flags=...A..., SrcPort=HTTP(80), DstPort=60919, PayloadLen=0, Seq=2552933535, Ack=1758977296, Win=14600 ( Negotiate scale fact )

SrcPort: HTTP(80)

DstPort: 60919

SequenceNumber: 2552933535 (0x982AACB1)

AcknowledgementNumber: 1758977296 (0x68D7DD10)

DataOffset: 128 (0x80)

Flags: A S

Frame Details

Hex Details

Frame: Number = 1416, Captured Frame Length = 66, MediaType = ETHERNET

Ethernet: Etype = Internet IP (IPv4), DestinationAddress:[F4-30-B9-AB-44-D3]

Ipv4: Src = 85.234.37.64, Dest = 100.90.157.209, Next Protocol = TCP, Packe

Tcp: Flags=...A..., SrcPort=HTTP(80), DstPort=60919, PayloadLen=0, Seq=2552933535, Ack=1758977296, Win=14600 ( Negotiate scale fact )

SrcPort: HTTP(80)

DstPort: 60919

SequenceNumber: 2552933535 (0x982AACB1)

AcknowledgementNumber: 1758977296 (0x68D7DD10)

DataOffset: 128 (0x80)

Flags: A S

#### Квитанция об окончательном подтверждении (флаг A)

1418	16:04:10 28.02.2022	4.0077530	chrome.exe	100.90.157.209	85.234.37.64	TCP	TCP:Flags=...A..., SrcPort=60919, DstPort=HTTP(80), PayloadLen=0, Seq=1758977296, Ack=2552933554, Win=513 (scale factor 0)
1419	16:04:10 28.02.2022	4.0078684	chrome.exe	100.90.157.209	85.234.37.64	TCP	TCP:Flags=...A..., SrcPort=60920, DstPort=HTTP(80), PayloadLen=0, Seq=515864672, Ack=2339018987, Win=513 (scale factor 0)
1420	16:04:10 28.02.2022	4.0091743	chrome.exe	100.90.157.209	85.234.37.64	HTTP	HTTP:Request, GET /
1421	16:04:10 28.02.2022	4.0108494	chrome.exe	74.125.205.105	100.90.157.209	TCP	TCP:Flags=...A..., SrcPort=HTTPS(443), DstPort=60918, PayloadLen=0, Seq=3342217971, Ack=574728562, Win=261

Frame Details							
Frame: Number = 1418, Captured Frame Length = 54, MediaType = ETHERNET							
Ethernet: Etype = Internet IP (IPv4), DestinationAddress:[00-00-5E-00-01-8A]							
Ipv4: Src = 100.90.157.209, Dest = 85.234.37.64, Next Protocol = TCP, Packe							
Tcp: Flags=...A..., SrcPort=60919, DstPort=HTTP(80), PayloadLen=0, Seq=1758977296, Ack=2552933554, Win=513 (scale factor 0)							
SrcPort: 60919							
DstPort: HTTP(80)							
SequenceNumber: 1758977296 (0x68D7DD10)							
AcknowledgementNumber: 2552933554 (0x982AACB2)							
DataOffset: 80 (0x50)							
Hex Details							
[!]: Decode As   # Width ▾   Prot Off: 0 (0x00)   Frame Off: 34 (0x22)   Sel Bytes: 20							
0000 00 00 5E 00 01 8A F4 30 B9 AB 44 D3 08 ..^.. 0^1 «DÓ.							
0000D 00 45 00 00 28 1D F4 40 00 80 06 00 00 .E..(.6@. .							
001A 64 5A 9D D1 55 EA 25 40 ED F7 00 50 68 dz ÑUë%@i..Ph							
0027 D7 DD 10 98 2A AC B2 50 10 02 01 7D 70 xÍ. *~*P...}p							
0034 00 00 ..							

## Квитанция о разрыве соединения (флаг AF) Запрос и ответ

### Запрос

4762	16:04:17 28.02.2022	11.3674690	chrome.exe	100.90.157.209	85.234.37.64	TCP	TCP:Flags=...A..., SrcPort=60919, DstPort=HTTP(80), PayloadLen=0, Seq=1758981849, Ack=2552934677, Win=508 (scale factor 0)
4763	16:04:17 28.02.2022	11.3688312	chrome.exe	100.90.157.209	85.234.37.64	TCP	TCP:Flags=...A..., SrcPort=60924, DstPort=HTTP(80), PayloadLen=0, Seq=4138607307, Ack=3518788020, Win=511 (scale factor 0)
4764	16:04:17 28.02.2022	11.3688312	chrome.exe	100.90.157.209	85.234.37.64	TCP	TCP:Flags=...A..., SrcPort=60921, DstPort=HTTP(80), PayloadLen=0, Seq=25239909, Ack=987572696, Win=510 (scale factor 0x
4765	16:04:17 28.02.2022	11.3688312	chrome.exe	100.90.157.209	85.234.37.64	TCP	TCP:Flags=...A..., SrcPort=60923, DstPort=HTTP(80), PayloadLen=0, Seq=3465220792, Ack=59582002, Win=508 (scale factor 0x

Frame Details							
Frame: Number = 4762, Captured Frame Length = 54, MediaType = ETHERNET							
Ethernet: Etype = Internet IP (IPv4), DestinationAddress:[00-00-5E-00-01-8A]							
Ipv4: Src = 100.90.157.209, Dest = 85.234.37.64, Next Protocol = TCP, Packe							
Tcp: Flags=...A..., SrcPort=60919, DstPort=HTTP(80), PayloadLen=0, Seq=1758981849, Ack=2552934677, Win=508 (scale factor 0)							
SrcPort: 60919							
DstPort: HTTP(80)							
SequenceNumber: 1758981849 (0x68D7EED9)							
AcknowledgementNumber: 2552934677 (0x982AB115)							
DataOffset: 80 (0x50)							
Hex Details							
[!]: Decode As   # Width ▾   Prot Off: 0 (0x00)   Frame Off: 34 (0x22)   Sel Bytes: 20							
0000 00 00 5E 00 01 8A F4 30 B9 AB 44 D3 08 ..^.. 0^1 «DÓ.							
0000D 00 45 00 00 28 1D F4 40 00 80 06 00 00 .E..(.6@. .							
001A 64 5A 9D D1 55 EA 25 40 ED F7 00 50 68 dz ÑUë%@i..Ph							
0027 D7 EE D9 98 2A B1 15 50 11 01 FC 7D 70 xÍ0 *~*P..}p							
0034 00 00 ..							

### Ответ

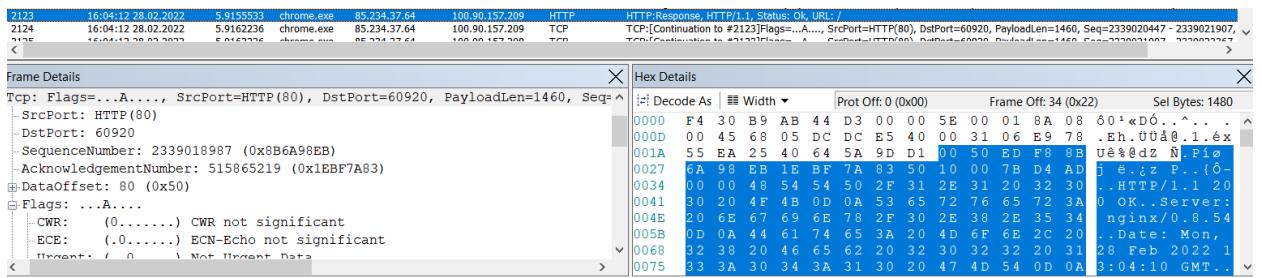
4804	16:04:17 28.02.2022	11.3966904	chrome.exe	85.234.37.64	100.90.157.209	TCP	TCP:Flags=...A..., SrcPort=HTTP(80), DstPort=60919, PayloadLen=0, Seq=2552934677, Ack=1758981850, Win=189 (scale factor 0)
4805	16:04:17 28.02.2022	11.3968083	chrome.exe	5.143.224.43	100.90.157.209	TCP	TCP:Flags=...A..., SrcPort=HTTP(80), DstPort=60930, PayloadLen=0, Seq=2727910318, Ack=1148342284, Win=123 (scale factor 0)
4806	16:04:17 28.02.2022	11.3968083	chrome.exe	5.143.224.43	100.90.157.209	TCP	TCP:Flags=...A..., SrcPort=HTTP(80), DstPort=60930, PayloadLen=0, Seq=2727910318, Ack=1148342284, Win=123 (scale factor 0)

Frame Details							
Frame: Number = 4804, Captured Frame Length = 60, MediaType = ETHERNET							
Ethernet: Etype = Internet IP (IPv4), DestinationAddress:[F4-30-8B-AB-44-D3]							
Ipv4: Src = 85.234.37.64, Dest = 100.90.157.209, Next Protocol = TCP, Packe							
Tcp: Flags=...A..., SrcPort=HTTP(80), DstPort=60919, PayloadLen=0, Seq=2552934677, Ack=1758981850, Win=189 (scale factor 0)							
SrcPort: 60919							
DstPort: HTTP(80)							
SequenceNumber: 2552934677 (0x68D7EED9)							
AcknowledgementNumber: 1758981850 (0x982AB115)							
DataOffset: 80 (0x50)							
Hex Details							
[!]: Decode As   # Width ▾   Prot Off: 0 (0x00)   Frame Off: 34 (0x22)   Sel Bytes: 20							
0000 F4 30 B9 AB 44 D3 00 00 00 5E 00 01 8A 08 0^1 «DÓ.							
0000D 00 45 68 00 28 E8 C6 40 00 31 06 E3 4B .Eh.(é@. 1. ÁK							
001A 55 EA 25 40 64 5A 9D D1 00 50 ED F7 98 Úé@dz N.Pi=							
0027 2A B1 15 68 D7 EE DA 50 11 00 BD A2 86 x~.hÍÜ.P..49							
0034 00 00 00 00 00 00 00 00 ..							

## Квитанция о закрытии браузера (флаг AR)

### Запрос

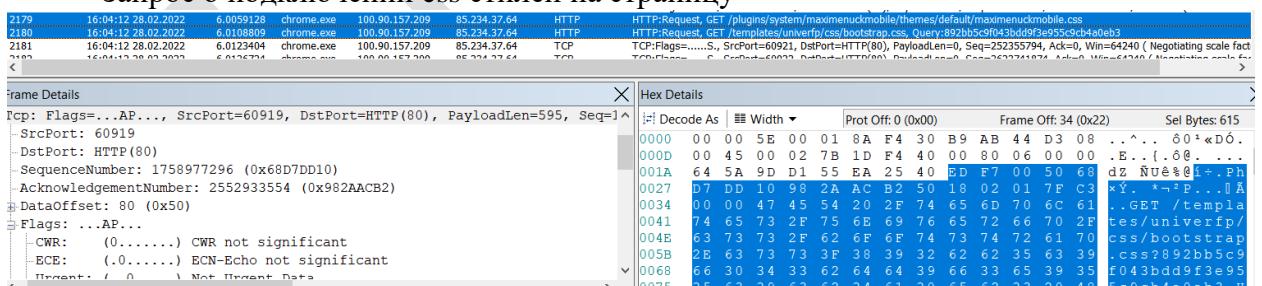
4814	16:04:17 28.02.2022	11.3973448	chrome.exe	100.90.157.209	77.88.21.119	TCP	TCP:Flags=...A..., SrcPort=60928, DstPort=HTTPS(443), PayloadLen=0, Seq=41202093, Ack=8647573, Win=0 (scale factor 0)
4815	16:04:17 28.02.2022	11.3973448	chrome.exe	100.90.157.209	77.88.21.119	TCP	TCP:Flags=...A..., SrcPort=60926, DstPort=HTTP(80), PayloadLen=0, Seq=389121466, Ack=3010703512, Win=512 (scale factor 0)
4816	16:04:17 28.02.2022	11.3973448	chrome.exe	100.90.157.209	85.234.37.64	TCP	TCP:Flags=...A..., SrcPort=60919, DstPort=HTTP(80), PayloadLen=0, Seq=1758981850, Ack=2552934678, Win=508 (scale factor 0)
4818	16:04:17 28.02.2022	11.4031836	chrome.exe	85.234.37.64	100.90.157.209	TCP	TCP:Flags=...A..., SrcPort=HTTP(80), DstPort=60922, PayloadLen=0, Seq=2339018987, Ack=362399471, Win=239 (scale factor 0)
4819	16:04:17 28.02.2022	11.4031836	chrome.exe	85.234.37.64	100.90.157.209	TCP	TCP:Flags=...A..., SrcPort=HTTP(80), DstPort=60923, PayloadLen=0, Seq=3342217971, Ack=362399471, Win=239 (scale factor 0)
4820	16:04:17 28.02.2022	11.4031868	chrome.exe	85.234.37.64	100.90.157.209	TCP	TCP:Flags=...A..., SrcPort=HTTP(80), DstPort=60923, PayloadLen=0, Seq=3342217971, Ack=362399471, Win=239 (scale factor 0)
4821	16:04:17 28.02.2022	11.4031868	chrome.exe	5.143.224.43	100.90.157.209	TCP	TCP:Flags=...A..., SrcPort=HTTP(80), DstPort=60923, PayloadLen=0, Seq=236872933, Ack=115512375, Win=128 (scale factor 0)
4822	16:04:17 28.02.2022	11.4030872	chrome.exe	100.90.157.209	85.234.37.64	TCP	TCP:Flags=...A..., SrcPort=60922, DstPort=HTTP(80), PayloadLen=0, Seq=3623947491, Ack=280630208, Win=9151 (scale factor 0)
4823	16:04:17 28.02.2022	11.4030872	chrome.exe	100.90.157.209	85.234.37.64	TCP	TCP:Flags=...A..., SrcPort=60920, DstPort=HTTP(80), PayloadLen=0, Seq=515884368, Win=9151 (scale factor 0)
4825	16:04:17 28.02.2022	11.4030872	chrome.exe	100.90.157.209	85.234.37.64	TCP	TCP:Flags=...A..., SrcPort=60923, DstPort=HTTP(80), PayloadLen=0, Seq=3465220793, Ack=9582003, Win=508 (scale factor 0x



## 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"> 
```

Frame Details

- Frame Number: 71, Captured Frame Length = 360, MediaType = ETHERNET
- Ethernet: Etype = Internet IP (IPv4), DestinationAddress:[00-1E-8C-85-96-01], SourceAddress:[7B-24-AF-3E-67-9D]
- Ipv4: Src = 192.168.10.86, Dest = 192.168.10.251, Next Protocol = TCP, Packet ID = 5638, Total IP Length = 373
- Top: Flags=..A.P., SrcPort=1416, DstPort=HTTP(80), PayloadLen=333, Seq=789158593 - 78915866, Ack=5644730155, Win=256 (scale factor 0x8) = 65536
- Http: Request, GET /alex/weather/27962.GIF

Hex Details

[x] Decode As	Width	Prot Off: 0 (0x0)	Frame Off: 54 (0x36)	Set Bytes: 3
0000 00 1E 8C 85 96 01 7B 24 AF 3E 67 9D .. .x->.g	16			
0001 00 00 C0 A0 0A 56 C0 A8 0A 50 00 50 .. .E..V..A..	16			
0018 00 00 50 2F 09 9A 85 D9 3E 2B 29 50 18 .. .P./.O+P.	16			
0030 01 00 98 09 00 00 17 45 51 20 2F 7E .. . .GET /~	16			
0031 00 00 00 00 00 00 00 00 00 00 00 .. .	16			
0048 00 00 00 00 00 00 00 00 00 00 00 .. .	16			
0054 00 00 00 00 00 00 00 00 00 00 00 .. .	16			
0060 7B 7B 9A 20 31 39 3B 2E 31 16 3B 2B .. .ttx 192.169.	16			
0078 31 39 2E 00 00 00 00 00 00 00 00 .. .	16			
0084 00 00 00 00 00 00 00 00 00 00 00 .. .	16			
0090 64 67 17 77 7B 20 4E 50 20 3B 2E 31 3B .. .down HT ..	16			
0096 20 57 99 82 00 34 31 20 16 24 3B 3A .. .Win64 HT ..	16			
00A2 00 00 00 00 00 00 00 00 00 00 00 .. .	16			
00A8 63 63 49 50 2F 31 23 31 30 31 30 31 .. .	16			
00B4 00 00 00 00 00 00 00 00 00 00 00 .. .	16			
00C0 20 40 69 72 45 66 4F 78 27 39 33 2B .. .Firefox 99.	16			
00CC 00 00 00 00 00 00 00 00 00 00 00 .. .	16			
00E4 63 67 65 27 77 65 62 70 2C 2A 2B 2A .. .age/webp ..	16			
00F0 00 00 43 63 63 65 70 2D 1C 61 6B .. .Accept-Lan	16			

Подключение стилей на страницу  
<link rel="stylesheet" href="vt.css" type="text/css">

Запрос

Frame Details

- Frame Number: 60, Captured Frame Length = 360, MediaType = ETHERNET
- Ethernet: Etype = Internet IP (IPv4), DestinationAddress:[00-1E-8C-85-96-01], SourceAddress:[7B-24-AF-3E-67-9D]
- Ipv4: Src = 192.168.10.86, Dest = 192.168.10.251, Next Protocol = TCP, Packet ID = 5631, Total IP Length = 348
- Top: Flags=..A.P., SrcPort=1416, DstPort=HTTP(80), PayloadLen=308, Seq=3906313797 - 3906314105, Ack=3640199009, Win=256 (scale factor 0x8) = 65536
- Http: Request, GET /vt.css

Hex Details

[x] Decode As	Width	Prot Off: 0 (0x0)	Frame Off: 54 (0x36)	Set Bytes: 3
0000 00 1E 8C 85 96 01 7B 24 AF 3E 67 9D .. .x->.g	16			
0001 00 00 C0 A0 0A 56 C0 A8 0A 50 00 50 .. .E..V..A..	16			
0018 00 00 50 2F 09 9A 85 D9 3E 2B 29 50 18 .. .P./.O+P.	16			
0030 01 00 98 09 00 00 17 45 51 20 2F 7E .. . .GET /~	16			
0031 00 00 00 00 00 00 00 00 00 00 00 .. .	16			
0048 00 00 00 00 00 00 00 00 00 00 00 .. .	16			
0054 00 00 00 00 00 00 00 00 00 00 00 .. .	16			
0060 7B 7B 9A 20 31 39 3B 2E 31 16 3B 2B .. .ttx 192.169.	16			
0078 31 39 2E 00 00 00 00 00 00 00 00 .. .	16			
0084 00 00 00 00 00 00 00 00 00 00 00 .. .	16			
0090 64 67 17 77 7B 20 4E 50 20 3B 2E 31 3B .. .down HT ..	16			
0096 20 57 99 82 00 34 31 20 16 24 3B 3A .. .Win64 HT ..	16			
00A2 00 00 00 00 00 00 00 00 00 00 00 .. .	16			
00A8 63 63 49 50 2F 31 23 31 30 31 30 31 .. .	16			
00B4 00 00 00 00 00 00 00 00 00 00 00 .. .	16			
00C0 20 40 69 72 45 66 4F 78 27 39 33 2B .. .Firefox 99.	16			
00CC 00 00 00 00 00 00 00 00 00 00 00 .. .	16			
00E4 63 67 65 27 77 65 62 70 2C 2A 2B 2A .. .age/webp ..	16			
00F0 00 00 43 63 63 65 70 2D 1C 61 6B .. .Accept-Lan	16			

Ответ

Frame Details

- Frame Number: 60, Captured Frame Length = 360, MediaType = ETHERNET
- Ethernet: Etype = Internet IP (IPv4), DestinationAddress:[00-1E-8C-85-96-01], SourceAddress:[7B-24-AF-3E-67-9D]
- Ipv4: Src = 192.168.10.86, Dest = 192.168.10.251, Next Protocol = TCP, Packet ID = 5631, Total IP Length = 348
- Top: Flags=..A.P., SrcPort=1416, DstPort=HTTP(80), PayloadLen=308, Seq=3906313797 - 3906314105, Ack=3640199009, Win=256 (scale factor 0x8) = 65536
- Http: Request, GET /vt.css

Hex Details

[x] Decode As	Width	Prot Off: 0 (0x0)	Frame Off: 54 (0x36)	Set Bytes: 3
0000 00 1E 8C 85 96 01 7B 24 AF 3E 67 9D .. .x->.g	16			
0001 00 00 C0 A0 0A 56 C0 A8 0A 50 00 50 .. .E..V..A..	16			
0018 00 00 50 2F 09 9A 85 D9 3E 2B 29 50 18 .. .P./.O+P.	16			
0030 01 00 97 09 00 00 17 45 51 20 2F 7E .. . .GET /~	16			
0031 00 00 00 00 00 00 00 00 00 00 00 .. .	16			
0048 00 00 00 00 00 00 00 00 00 00 00 .. .	16			
0054 00 00 00 00 00 00 00 00 00 00 00 .. .	16			
0060 7B 7B 9A 20 31 39 3B 2E 31 16 3B 2B .. .ttx 192.169.	16			
0078 31 39 2E 00 00 00 00 00 00 00 00 .. .	16			
0084 00 00 00 00 00 00 00 00 00 00 00 .. .	16			
0090 64 67 17 77 7B 20 4E 50 20 3B 2E 31 3B .. .down HT ..	16			
0096 20 57 99 82 00 34 31 20 16 24 3B 3A .. .Win64 HT ..	16			
00A2 00 00 00 00 00 00 00 00 00 00 00 .. .	16			
00A8 63 63 49 50 2F 31 23 31 30 31 30 31 .. .	16			
00B4 00 00 00 00 00 00 00 00 00 00 00 .. .	16			
00C0 20 40 69 72 45 66 4F 78 27 39 33 2B .. .Firefox 99.	16			
00CC 00 00 00 00 00 00 00 00 00 00 00 .. .	16			
00E4 63 67 65 27 77 65 62 70 2C 2A 2B 2A .. .age/webp ..	16			
00F0 00 00 43 63 63 65 70 2D 1C 61 6B .. .Accept-Lan	16			

## Лабораторная работа № 5

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

Понедельник, 14 марта, 2022

Кафедра ВТ ПГУ

- Новости
- Документы
- Учебный план
- Стандартность 22.01.00
- Членские посты
- Бакалавриат
- Магистратура
- Дипломное проектирование
- Практика
- Информационные ресурсы
- Сотрудники
- Контактная информация
- Информация
- Мониторинг

Погода в Пензе

Статистика

Сайт кафедры А. В.

Пензенский Государственный университет

КАФЕДРА  
"ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА"

заведующий кафедрой Бутаев М.М.

03.06.2010 Запущена Информационная система учета заданий на курсовое проектирование

27.06.2008 Сервер [Titan vt](#) перенесен на новую платформу [openSUSE](#) Linux 11.0

20.05.2002 Открыт раздел "Информация" в нем выложен руководство по созданию электронных учебников в формате MS Word

7.02.2002 Открытие сайта [Titan vt](#)

Главная страница

0000 7B 7B 9A 20 31 39 3B 2E 31 16 3B 2B .. .ttx 192.169.

0001 00 00 00 00 00 00 00 00 00 00 00 .. .

0018 00 00 50 2F 09 9A 85 D9 3E 2B 29 50 18 .. .P./.O+P.

0030 01 00 97 09 00 00 17 45 51 20 2F 7E .. . .GET /~

0031 00 00 00 00 00 00 00 00 00 00 00 .. .

0048 00 00 00 00 00 00 00 00 00 00 00 .. .

0054 00 00 00 00 00 00 00 00 00 00 00 .. .

0060 7B 7B 9A 20 31 39 3B 2E 31 16 3B 2B .. .ttx 192.169.

0078 31 39 2E 00 00 00 00 00 00 00 00 .. .

0084 00 00 00 00 00 00 00 00 00 00 00 .. .

0090 64 67 17 77 7B 20 4E 50 20 3B 2E 31 3B .. .down HT ..

0096 20 57 99 82 00 34 31 20 16 24 3B 3A .. .Win64 HT ..

00A2 00 00 00 00 00 00 00 00 00 00 00 .. .

00A8 63 63 49 50 2F 31 23 31 30 31 30 31 .. .

00B4 00 00 00 00 00 00 00 00 00 00 00 .. .

00C0 00 00 00 00 00 00 00 00 00 00 00 .. .

00CC 00 00 00 00 00 00 00 00 00 00 00 .. .

00DC 00 00 00 00 00 00 00 00 00 00 00 .. .

00E4 00 00 00 00 00 00 00 00 00 00 00 .. .

00E9 00 00 00 00 00 00 00 00 00 00 00 .. .

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.

Frame Summary - ftp

Frame Number	Time Offset	Process Name	Source	Destination	Protocol Name	Description	Conn Id	
6630	16:45:11 14.03.2022	-49.09815	TOTALCMD.EVE	192.168.10.251	192.168.10.86	FTP	FTP-Request to Port 1543, "220 [null]Pd 2.6.0"	(TCP)110, Pv=4,109
6631	16:45:11 14.03.2022	-49.90362	TOTALCMD.EVE	192.168.10.251	192.168.10.86	FTP	FTP-Request from Port 1543, "LSNR retch"	(TCP)110, Pv=4,109
6633	16:45:11 14.03.2022	-49.90310	TOTALCMD.EVE	192.168.10.251	192.168.10.86	FTP	FTP-Response to Port 1543, "331 Please specify the password."	(TCP)110, Pv=4,109
6634	16:45:11 14.03.2022	-49.90310	TOTALCMD.EVE	192.168.10.251	192.168.10.86	FTP	FTP-Request to Port 1543, "230 Login successful."	(TCP)110, Pv=4,109
6700	16:45:18 14.03.2022	-57.08149	TOTALCMD.EVE	192.168.10.251	192.168.10.86	FTP	FTP-Response to Port 1543, "230 Login successful."	(TCP)110, Pv=4,109
6701	16:45:18 14.03.2022	-57.09564	TOTALCMD.EVE	192.168.10.251	192.168.10.86	FTP	FTP-Request from Port 1543, "SYST"	(TCP)110, Pv=4,109
6703	16:45:18 14.03.2022	-57.10117	TOTALCMD.EVE	192.168.10.251	192.168.10.86	FTP	FTP-Response to Port 1543, "213 System type: LUF"	(TCP)110, Pv=4,109
6704	16:45:18 14.03.2022	-57.10317	TOTALCMD.EVE	192.168.10.251	192.168.10.86	FTP	FTP-Request from Port 1543, "FEAT"	(TCP)110, Pv=4,109
6705	16:45:18 14.03.2022	-57.10384	TOTALCMD.EVE	192.168.10.251	192.168.10.86	FTP	FTP-Response to Port 1543, "214 FEATs supported"	(TCP)110, Pv=4,109
6706	16:45:18 14.03.2022	-57.1038409	TOTALCMD.EVE	192.168.10.251	192.168.10.86	FTP	FTP-Request from Port 1543, "1543,211 Leaf"	(TCP)110, Pv=4,109
6708	16:45:18 14.03.2022	-57.10414	TOTALCMD.EVE	192.168.10.251	192.168.10.86	FTP	FTP-Response to Port 1543, "200 Aliveness in UTF8 mode."	(TCP)110, Pv=4,109
6709	16:45:18 14.03.2022	-57.1041409	TOTALCMD.EVE	192.168.10.251	192.168.10.86	FTP	FTP-Request from Port 1543, "OPTS UTF8 ON"	(TCP)110, Pv=4,109
6710	16:45:18 14.03.2022	-57.11528	TOTALCMD.EVE	192.168.10.251	192.168.10.86	FTP	FTP-Response to Port 1543, "200 Aliveness in UTF8 mode."	(TCP)110, Pv=4,109
6711	16:45:18 14.03.2022	-57.1152809	TOTALCMD.EVE	192.168.10.251	192.168.10.86	FTP	FTP-Request to Port 1543, "PWD"	(TCP)110, Pv=4,109
6712	16:45:18 14.03.2022	-57.15492	TOTALCMD.EVE	192.168.10.251	192.168.10.86	FTP	FTP-Response to Port 1543, "557 "/"	(TCP)110, Pv=4,109
6725	16:45:19 14.03.2022	-57.21191	TOTALCMD.EVE	192.168.10.251	192.168.10.86	FTP	FTP-Request to Port 1543, "TYPE A"	(TCP)110, Pv=4,109
6726	16:45:19 14.03.2022	-57.2119109	TOTALCMD.EVE	192.168.10.251	192.168.10.86	FTP	FTP-Response to Port 1543, "500 Command not supported in ASCII mode."	(TCP)110, Pv=4,109
6737	16:45:19 14.03.2022	-57.22532	TOTALCMD.EVE	192.168.10.86	192.168.10.251	FTP	FTP-Request from Port 1543, "PASV"	(TCP)110, Pv=4,109
6738	16:45:19 14.03.2022	-57.2253209	TOTALCMD.EVE	192.168.10.86	192.168.10.251	FTP	FTP-Response to Port 1543, "229 Entering Passive Mode (192,168,10,251,1252,4)"	(TCP)110, Pv=4,109
6740	16:45:19 14.03.2022	-57.22536	TOTALCMD.EVE	192.168.10.86	192.168.10.251	FTP	FTP-Request to Port 1543, "CD .."	(TCP)110, Pv=4,109
6743	16:45:19 14.03.2022	-57.2253196	TOTALCMD.EVE	192.168.10.86	192.168.10.251	FTP	FTP-Response to Port 1543, "150 Here comes the directory listing."	(TCP)110, Pv=4,109
6746	16:45:19 14.03.2022	-57.225319609	TOTALCMD.EVE	192.168.10.86	192.168.10.251	FTP	FTP-Request to Port 1543, "RETR HelloWorld.txt"	(TCP)110, Pv=4,109
6748	16:45:20 14.03.2022	-63.9748349	TOTALCMD.EVE	192.168.10.86	192.168.10.251	FTP	FTP-Request from Port 1543, "226 File closed."	(TCP)110, Pv=4,109
6840	16:45:23 14.03.2022	-63.974834909	TOTALCMD.EVE	192.168.10.86	192.168.10.251	FTP	FTP-Response to Port 1543, "226 File send OK."	(TCP)110, Pv=4,109

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

6873 16:45:25 14.03.2022 64.0288960 TOTALCMD.EVE 192.168.10.251 192.168.10.86 FTP FTP-Response to Port 1543, "226 File send OK."

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.

```
C:\Windows\system32\cmd.exe
C:\Users\work>nslookup standupclub.ru
Server:  rs2.penza.ertelcom.ru
Address: 109.194.128.3

Name: standupclub.ru
Address: 5.63.158.249

C:\Users\work>
```

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.

#### Основные параметры сайта standupclub.ru

Индекс цитирования: 0	Внешние ссылки домена: 74
Рейтинг Alexa: 1065988	Внутренние ссылки: 5
IP адрес: <a href="http://5.63.158.249">5.63.158.249</a>	Кол-во найденных анкоров: 79
Регистратор домена: RU-CENTER-RU	Кол-во исходящих анкоров: 74
Дата регистрации: 2010-09-29	Кол-во ссылок на домене: 79

### 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 (0xFC807E5B)
    | 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)
```

ОБРАЗЕЦ