

## 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
тхѐтхѐ: rs2.penza.ertelecom.ru
Address: 109.194.128.3

Не заслуживающий доверия ответ:
ль : 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=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-кеше 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.

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

Маршрутизатор	<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>arp -d

C:\Windows\system32>arp -a

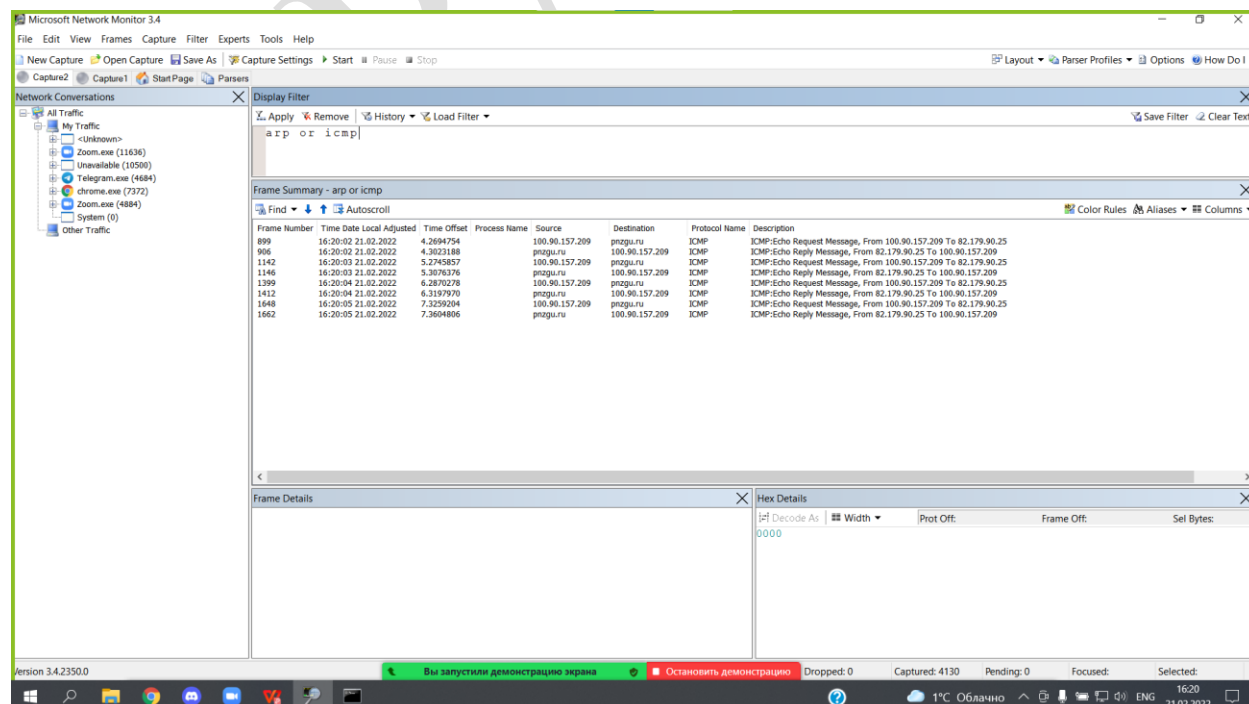
Интерфейс: 100.90.157.209 --- 0x12
    адрес в Интернете          Физический адрес      Тип
100.90.191.254                00-00-5e-00-01-8a     динамический
224.0.0.22                    01-00-5e-00-00-16     статический
255.255.255.255              ff-ff-ff-ff-ff-ff     статический
```

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.

Microsoft Network Monitor 3.4

File Edit View Frames Capture Filter Experts Tools Help

New Capture Open Capture Save As Capture Settings Start Pause Stop

Capture2 Capture1 Start Page Parsers

Network Conversations

My Traffic

Unknown (11636)

Zoom.exe (16500)

Telegram.exe (4684)

Zoom.exe (4684)

chrome.exe (7372)

System (8)

Other Traffic

Display Filter

arp or icmp

Frame Summary (Conversation Filter, arp or icmp)

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
899	16:20:02 21.02.2022	4.3894704	proguru	100.90.157.209	82.179.90.25	ICMP	ICMP-Echo Request Message, From 100.90.157.209 To 82.179.90.25
906	16:20:02 21.02.2022	4.3923188	proguru	100.90.157.209	82.179.90.25	ICMP	ICMP-Echo Reply Message, From 82.179.90.25 To 100.90.157.209
1142	16:20:03 21.02.2022	5.2745857	proguru	100.90.157.209	82.179.90.25	ICMP	ICMP-Echo Request Message, From 100.90.157.209 To 82.179.90.25
1146	16:20:03 21.02.2022	5.3079376	proguru	100.90.157.209	82.179.90.25	ICMP	ICMP-Echo Reply Message, From 82.179.90.25 To 100.90.157.209
1399	16:20:04 21.02.2022	6.2870278	proguru	100.90.157.209	82.179.90.25	ICMP	ICMP-Echo Request Message, From 100.90.157.209 To 82.179.90.25
1412	16:20:04 21.02.2022	6.3187970	proguru	100.90.157.209	82.179.90.25	ICMP	ICMP-Echo Reply Message, From 82.179.90.25 To 100.90.157.209
1648	16:20:05 21.02.2022	7.2259204	proguru	100.90.157.209	82.179.90.25	ICMP	ICMP-Echo Request Message, From 100.90.157.209 To 82.179.90.25
1662	16:20:05 21.02.2022	7.3604806	proguru	100.90.157.209	82.179.90.25	ICMP	ICMP-Echo Reply Message, From 82.179.90.25 To 100.90.157.209

Frame Details

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

IPv4: Src = 100.90.157.209, Dest = 82.179.90.25, Next Protocol = ICMP, P...

ICMP: Echo Request Message, From 100.90.157.209 To 82.179.90.25

Type: Echo Request Message, 8(0x8)

Code: 0 (0x0)

Checksum: 19802 (0x4D5A)

ID: 1 (0x1)

SequenceNumber: 1 (0x1)

ImplementationSpecificData: Binary Large Object (32 Bytes)

Hex Details

Decode As Width Prot Off: 0 (0x00) Frame Off: 0 (0x00) Set Bytes: 74

Offset	Hex	ASCII
0000	00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00	.....
0001	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0002	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0003	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0004	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0005	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0006	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0007	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0008	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0009	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
000A	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
000B	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
000C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
000D	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
000E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
000F	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0010	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0011	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0012	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0013	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0014	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0015	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0016	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0017	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0018	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0019	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
001A	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
001B	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
001C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
001D	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
001E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
001F	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....


### Лабораторная работа № 3

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

Apply Remove History Load Filter Save Filter Clear Text

tcp

### Запрос на открытие браузера (Флаг A)



Frame Details

- 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=HTTPS(443), PayloadLen=0, Seq=632973585, Ack=0, Win=64240 ( Negotiating scale factor 0x8 ) = 64240

```
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 = 100.0.0.1, 1.238, Next Protocol = TCP, Packet ID = 7107, Total Frame Length = 66
TCP: Seq = ...A.S., SrcPort=HTTFS(443), DstPort=59267, PayloadLen=0, Seq=2684156841, Ack=632973586, Win=65535 ( Negotiated scale factor 0x8 ) = 1
```

```

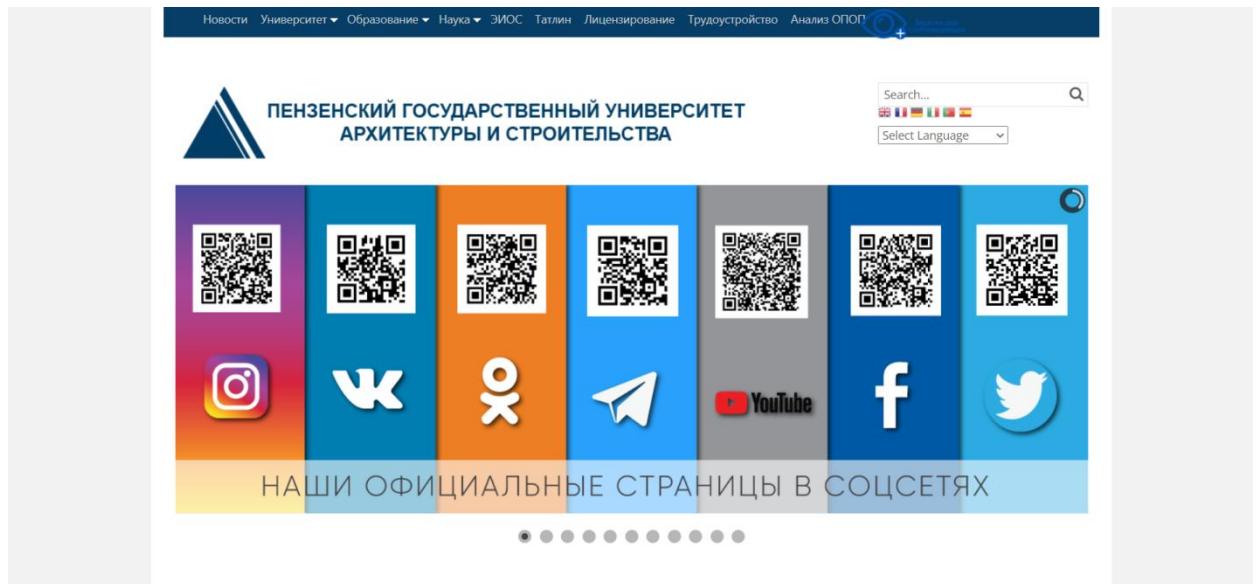
Frame: Number = 49, Captured Frame Length = 60, MediaType = ETHERNET
Ethernet: Etype = Internet IP (IPv4), DestinationAddress: [F4-30-B9-AB-44-D3], SourceAddress: [00-00-5E-00-01-8A]
IPv4: Src = 74.125.131.94, Dest = 100.90.11.238, Net Protocol = TCP, Packet ID = 48040, Total IP Length = 40
TCP: Flags = ...A..F., SrcPort=HTTFS(443), DstPort=59301, PayloadLen=0, Seq=3834817371, Ack=1734616805, Win=269
(scale factor 0x8) = 68864

```

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

Frame Details	Hex Details																																										
<ul style="list-style-type: none"> <li>Frame: Number = 15, Captured Frame Length = 60, MediaType = ETHERNET</li> <li>Ethernet: Etype = Internet IP (IPv4), DestinationAddress: [F4-30-B9-AB-44-D3], SourceAddress: [08-00-2B-01-01-01], SrcPort: 59271, DstPort: 443</li> <li>IPv4: Src = 74.125.131.198, Dest = 100.90.11.238, Next Protocol = TCP, Packet ID = 6537</li> <li>Versions: IPv4, Internet Protocol: Header Length = 20 <ul style="list-style-type: none"> <li>Version: 01000... IPv4, Internet Protocol</li> <li>HeaderLength: (...0101) 20 bytes (0x5)</li> </ul> </li> <li>DifferentiatedServicesField: DSCP: 28, ECN: 0</li> <li>TotalLength: 40 (0x28)</li> <li>Identification: 65374 (0xF5FE)</li> <li>FragmentFlags: 0 (0x0)</li> <li>TimeToLive: 124 (0x7C)</li> <li>NextProtocol: TCP, 6(0x6)</li> <li>Checksum: 118 (0x76)</li> <li>SourceAddress: 74.125.131.198</li> <li>DestinationAddress: 100.90.11.238</li> <li>Tcp: Flags=...A..., SrcPort=HTTPS(443), DstPort=59271, PayloadLen=0, Seq=2109058372, A <ul style="list-style-type: none"> <li>SrcPort: HTTPS(443)</li> <li>DstPort: 59271</li> <li>SequenceNumber: 2109058372 (0x7DB5AD44)</li> <li>AcknowledgementNumber: 2530463377 (0x96D3CE91)</li> </ul> </li> <li>DataOffset: 80 (0x50)</li> <li>Flags: ...A.... <ul style="list-style-type: none"> <li>Window: 1506 (scale factor 0x8) = 385536</li> <li>Checksum: 0xF1C4, Good</li> <li>UrgentPointer: 0 (0x0)</li> </ul> </li> </ul>	<table> <thead> <tr> <th>Offset</th><th>Decode As</th><th>Width</th><th>Prot Off: 0 (0x00)</th><th>Frame Off: 14 (0x0E)</th><th>Sel Byte</th></tr> </thead> <tbody> <tr> <td>0000</td><td>F4 30 B9 AB 44 D3 00 00</td><td>8</td><td>5E 00 01 60</td><td>0</td><td>00 00 00 00</td></tr> <tr> <td>000B</td><td>08 00 00 45 70 00 28 FF</td><td>8</td><td>5E 00 00 00</td><td>0</td><td>00 00 00 00</td></tr> <tr> <td>0016</td><td>7C 06 00 76 4A 7D 83 C6</td><td>8</td><td>64 5A 0B 10</td><td>0</td><td>00 00 00 00</td></tr> <tr> <td>0021</td><td>EE 01 BB E7 7D B5 AD 44</td><td>8</td><td>96 D3 10 00</td><td>0</td><td>00 00 00 00</td></tr> <tr> <td>002C</td><td>CE 91 50 10 05 E2 F1 C4</td><td>8</td><td>00 00 00 00</td><td>0</td><td>00 00 00 00</td></tr> <tr> <td>0037</td><td>00 00 00 00 00 00</td><td>8</td><td></td><td></td><td></td></tr> </tbody> </table>	Offset	Decode As	Width	Prot Off: 0 (0x00)	Frame Off: 14 (0x0E)	Sel Byte	0000	F4 30 B9 AB 44 D3 00 00	8	5E 00 01 60	0	00 00 00 00	000B	08 00 00 45 70 00 28 FF	8	5E 00 00 00	0	00 00 00 00	0016	7C 06 00 76 4A 7D 83 C6	8	64 5A 0B 10	0	00 00 00 00	0021	EE 01 BB E7 7D B5 AD 44	8	96 D3 10 00	0	00 00 00 00	002C	CE 91 50 10 05 E2 F1 C4	8	00 00 00 00	0	00 00 00 00	0037	00 00 00 00 00 00	8			
Offset	Decode As	Width	Prot Off: 0 (0x00)	Frame Off: 14 (0x0E)	Sel Byte																																						
0000	F4 30 B9 AB 44 D3 00 00	8	5E 00 01 60	0	00 00 00 00																																						
000B	08 00 00 45 70 00 28 FF	8	5E 00 00 00	0	00 00 00 00																																						
0016	7C 06 00 76 4A 7D 83 C6	8	64 5A 0B 10	0	00 00 00 00																																						
0021	EE 01 BB E7 7D B5 AD 44	8	96 D3 10 00	0	00 00 00 00																																						
002C	CE 91 50 10 05 E2 F1 C4	8	00 00 00 00	0	00 00 00 00																																						
0037	00 00 00 00 00 00	8																																									

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)



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
1422	16:04:10.28.02.2022	4.0323203	chrome.exe	85.234.37.64	100.90.157.209	TCP	TCP:Flags=...A..., SrcPort=HTTPS(443), DstPort=60920, PayloadLen=0, Seq=2339018987, Ack=515864672, Win=513 (scale factor 0)

Frame Details	Hex 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 (0x68D7DD10) AcknowledgeNumber: 2552933554 (0x982AACB2) DataOffset: 80 (0x50)	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 ... ^.. 60 ^ dO. 000D 00 45 00 00 28 1D F4 40 00 80 06 00 00 ... E.. (. 60. ... 001A 64 5A 9D D1 55 EA 25 40 BD F7 00 50 68 dZ NUe%0P... Ph 0027 D7 DD 10 98 2A AC B2 50 10 02 01 7D 70 *Y. * ^ 2 P... P 0034 00 00

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

4762	16:04:17.28.02.2022	11.3674690	chrome.exe	100.90.157.209	85.234.37.64	TCP	TCP:Flags=...A..F, 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..F, SrcPort=60924, DstPort=HTTP(80), PayloadLen=0, Seq=4138607307, Ack=2518788020, 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..F, SrcPort=60921, DstPort=HTTP(80), PayloadLen=0, Seq=252359909, Ack=987572696, Win=510 (scale factor 0)
4765	16:04:17.28.02.2022	11.3688312	chrome.exe	100.90.157.209	85.234.37.64	TCP	TCP:Flags=...A..F, SrcPort=60923, DstPort=HTTP(80), PayloadLen=0, Seq=3465220792, Ack=59582002, Win=508 (scale factor 0)

Frame Details	Hex 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..F, SrcPort=60919, DstPort=HTTP(80), PayloadLen=0, Seq=1758981849 (0x68D7EED9) AcknowledgeNumber: 2552934677 (0x982AB115) DataOffset: 80 (0x50)	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 ... ^.. 60 ^ dO. 000D 00 45 00 00 28 C5 B8 40 00 80 06 00 00 ... E.. (. 60. ... 001A 64 5A 9D D1 55 EA 25 40 BD F7 00 50 68 dZ NUe%0P... Ph 0027 D7 DD 10 98 2A B1 15 50 11 01 FC 7D 70 *iD * ^ 2 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..F, 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..F, SrcPort=HTTP(80), DstPort=60920, 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..F, SrcPort=HTTP(443), DstPort=60920, PayloadLen=0, Seq=2339018987, Ack=515864672, Win=513 (scale factor 0)

Frame Details	Hex Details
Frame: Number = 4804, Captured Frame Length = 60, 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..F, SrcPort=HTTP(80), DstPort=60919, PayloadLen=0, Seq=2552934677 (0x982AB115) AcknowledgeNumber: 1758981850 (0x68D7EEDA) DataOffset: 80 (0x50)	Decode As Width Prot Off: 0 (0x00) Frame Off: 34 (0x22) Sel Bytes: 20 0000 F4 30 B9 AB 44 D3 00 00 5E 00 01 8A 08 60 ^ ^ dO.. ^ ^ .. 000D 00 45 68 00 28 E8 C6 40 00 31 06 E3 4B .. E.. (. 60. ... 001A 55 EA 25 40 64 5A 9D D1 00 50 BD F7 98 Ue%0dZ N P1= 0027 2A B1 15 68 D7 EE DA 50 11 00 BD A2 86 * ^ h x i P... ^ e 0034 00 00 00 00 00 00 00 00 00 00 00 00 ..

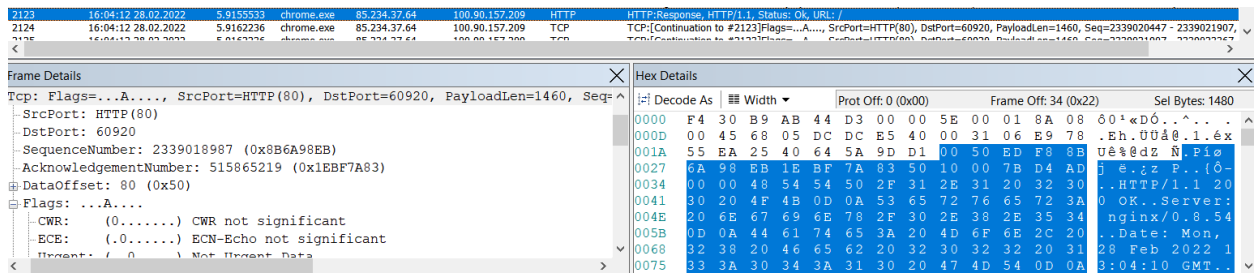
## Квитанция о закрытии браузера (флаг AR)

4814	16:04:17.28.02.2022	11.3972443	chrome.exe	100.90.157.209	77.88.21.119	TCP	TCP:Flags=...A..R, SrcPort=60920, DstPort=HTTP(80), PayloadLen=0, Seq=414202093, Ack=574728562, Win=512 (scale factor 0)
4815	16:04:17.28.02.2022	11.3973448	chrome.exe	100.90.157.209	173.194.222.113	TCP	TCP:Flags=...A..R, SrcPort=60926, DstPort=HTTP(80), PayloadLen=0, Seq=3891214466, Ack=3010703312, 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..R, SrcPort=60919, DstPort=HTTP(80), PayloadLen=0, Seq=1758981850, Ack=2552934676, Win=508 (scale factor 0)
4818	16:04:17.28.02.2022	11.4031968	chrome.exe	85.234.37.64	100.90.157.209	TCP	TCP:Flags=...A..R, SrcPort=HTTP(80), DstPort=60922, PayloadLen=0, Seq=280630027, Ack=3623749471, Win=239 (scale factor 0)
4819	16:04:17.28.02.2022	11.4031968	chrome.exe	85.234.37.64	100.90.157.209	TCP	TCP:Flags=...A..R, SrcPort=HTTP(80), DstPort=60923, PayloadLen=0, Seq=59582002, Ack=3465220793, Win=187 (scale factor 0)
4820	16:04:17.28.02.2022	11.4031968	chrome.exe	85.234.37.64	100.90.157.209	TCP	TCP:Flags=...A..R, SrcPort=HTTP(80), DstPort=60920, PayloadLen=0, Seq=2339038884, Ack=515884368, Win=428 (scale factor 0)
4821	16:04:17.28.02.2022	11.4031968	chrome.exe	5.143.224.43	100.90.157.209	TCP	TCP:Flags=...A..R, SrcPort=HTTP(80), DstPort=60929, PayloadLen=0, Seq=2226873933, Ack=4155412475, Win=135 (scale factor 0)
4822	16:04:17.28.02.2022	11.4038072	chrome.exe	100.90.157.209	85.234.37.64	TCP	TCP:Flags=...A..R, SrcPort=60922, DstPort=HTTP(80), PayloadLen=0, Seq=3623749471, Ack=280630028, Win=49151 (scale factor 0)
4823	16:04:17.28.02.2022	11.4038072	chrome.exe	100.90.157.209	85.234.37.64	TCP	TCP:Flags=...A..R, SrcPort=60920, DstPort=HTTP(80), PayloadLen=0, Seq=515884368, Ack=2339038885, Win=49151 (scale factor 0)
4825	16:04:17.28.02.2022	11.4038072	chrome.exe	100.90.157.209	85.234.37.64	TCP	TCP:Flags=...A..R, SrcPort=60923, DstPort=HTTP(80), PayloadLen=0, Seq=3465220793, Ack=59582003, Win=508 (scale factor 0)
4827	16:04:17.28.02.2022	11.4038072	chrome.exe	100.90.157.209	5.143.224.43	TCP	TCP:Flags=...A..R, SrcPort=60929, DstPort=HTTP(80), PayloadLen=0, Seq=4155412475, Ack=2226873934, Win=508 (scale factor 0)

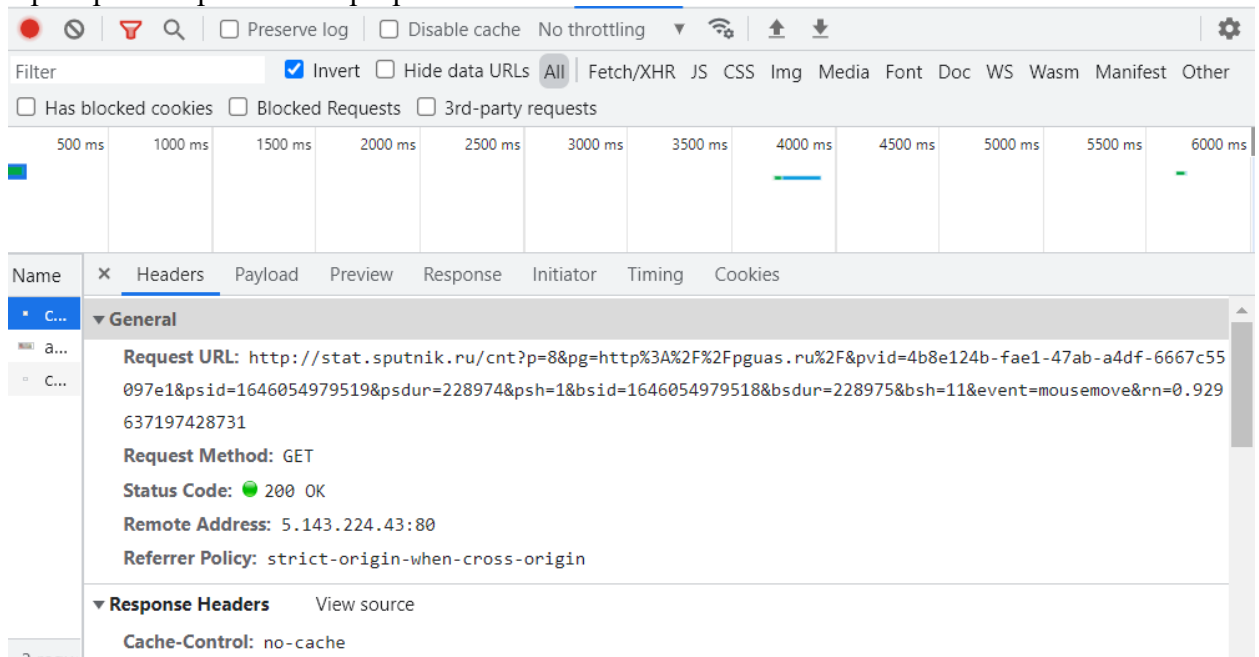
Frame Details	Hex Details
Frame: Number = 4814, Captured Frame Length = 54, MediaType = ETHERNET Ethernet: Etype = Internet IP (IPv4), DestinationAddress: [00-00-5E-00-01-8A] IPv4: Src = 100.90.157.209, Dest = 77.88.21.119, Next Protocol = TCP, Packe Tcp: Flags=...A..R, SrcPort=60928, DstPort=HTTPS(443), PayloadLen=0, Seq=2410202093 (0x8FA8C3ED) AcknowledgeNumber: 486470573 (0x1CFEF3AD) DataOffset: 80 (0x50)	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 ... ^.. 60 ^ dO. 000D 00 45 00 00 28 13 AF 40 00 80 06 00 00 ... E.. (. ^ 60. ... 001A 64 5A 9D D1 4D 58 15 77 EE 00 01 B8 8F dZ NMx.w l... 0027 A8 C3 ED 1C FE F3 AD 50 14 00 00 65 15 A l.p0-P...e 0034 00 00

Frame Details	Hex Details
Tcp: Flags=...AP..., SrcPort=60920, DstPort=HTTP(80), PayloadLen=547, Seq=515864672 (0x1EBF7860) SrcPort: 60920 DstPort: HTTP(80) SequenceNumber: 515864672 (0x1EBF7860) AcknowledgeNumber: 2339018987 (0x8B6A98EB) DataOffset: 80 (0x50) Flags: ...AP... CWR: (0.....) CWR not significant ECE: (.0.....) ECN-Echo not significant URG: (0.....) Not Urgent Data	Decode As Width Prot Off: 0 (0x00) Frame Off: 34 (0x22) Sel Bytes: 567 0000 00 00 5E 00 01 8A F4 30 B9 AB 44 D3 08 ... ^.. 60 ^ dO. 000D 00 45 00 02 4B 1D F4 40 00 80 06 00 00 ... E.. K. 60. ... 001A 64 5A 9D D1 55 EA 25 40 BD F8 00 50 1E dZ NUe%0P... Ph 0027 A8 C3 ED 1C FE F3 AD 50 14 00 00 65 15 A l.p0-P...e 0034 00 00 47 45 54 20 2F 20 48 54 54 50 2F .. GET / HTTP/ 0041 31 2E 31 0D 0A 48 6F 73 74 3A 20 70 67 l.l..Host: pg 004E 75 61 73 2E 72 75 0D 0A 43 6F 6E 6E 65 uas.ru..Conne 005B 63 74 69 6F 6E 3A 20 6B 65 70 70 2D 61 ction: keep-a 0068 6C 69 76 65 0D 0A 55 70 67 72 61 64 65 live..Upgrade 0075 2D 49 6E 73 65 63 75 72 65 2D 52 65 71 -Insecure-Req

## Ответ

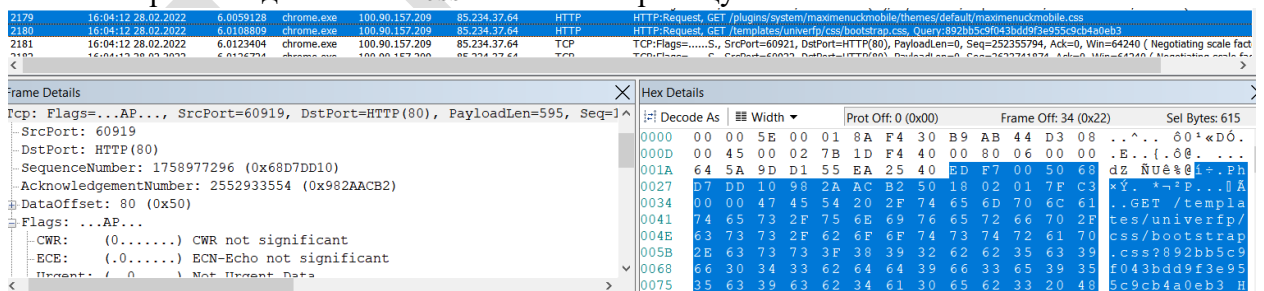


## Проверили через панель разработчика



## 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"> 
```

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

 <p><b>Кафедра ВТ ПГУ</b></p> <ul style="list-style-type: none"> <li>Цели</li> <li>Достижения</li> <li>Учебный план</li> <li>Специальность 22.01.06</li> <li>Учебная программа</li> <li>Дифференциальные задания</li> <li>Курсовое проектирование</li> <li>Дипломное проектирование</li> <li>Публикации</li> <li>Информационные ресурсы</li> <li>Сертификаты</li> <li>Контактная информация</li> <li>Информация</li> <li>Материалы</li> </ul> <p><b>Погода в Пензе</b></p>  <p><b>Статистика</b></p> <p>кабинет Антона А. В.</p>	<p>Пензенский Государственный университет</p> <h1>КАФЕДРА "ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА"</h1> <p>заведующий кафедрой Бутеев М.М.</p> <hr/> <div> <div> <p>03.06.2010</p> <p>27.06.2008</p> <p>20.05.2002</p> <p>7.02.2002</p> </div> <div> <p>Запущена <a href="#">Информационная система учета заданий на курсовое проектирование</a></p> <p>Сервер Titan v1 перенесен на новую платформу openSuSE Linux 11.0</p> <p>Открыт раздел "<a href="#">Информации</a>" в нем выложено руководство по созданию электронных учебников в формате HTML из формата MS Word</p> <p>Открытие сайта Titan.vt</p> </div> </div>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



Frame Number	Time	Date	Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description	Conn Id
6625	36:45:11.14	03/03/2022		49.898915	TOTALCME	DE 192.168.10.251	192.168.10.86	FTP	FTP-Response to Port 1543, 720. (vrfid 2.0.6)	(TCP:150, P=4=100)
6626	36:45:11.14	03/03/2022		49.900202	TOTALCME	DE 192.168.10.251	192.168.10.251	FTP	FTP-Request from Port 1543, 1628. vrfid=1	(TCP:150, P=4=100)
6633	36:45:11.14	03/03/2022		49.901033	TOTALCME	DE 192.168.10.251	192.168.10.86	FTP	FTP-Response to Port 1543, 331. Please specify the password.	(TCP:150, P=4=100)
6634	36:45:11.14	03/03/2022		49.901493	TOTALCME	DE 192.168.10.251	192.168.10.86	FTP	FTP-Response to Port 1543, 331. Please specify the password.	(TCP:150, P=4=100)
6700	36:45:18.14	03/03/2022		57.9814931	TOTALCME	DE 192.168.10.251	192.168.10.86	FTP	FTP-Response to Port 1543, 320. Login successful.	(TCP:150, P=4=100)
6701	36:45:18.14	03/03/2022		57.9814931	TOTALCME	DE 192.168.10.251	192.168.10.86	FTP	FTP-Request from Port 1543, 320ST	(TCP:150, P=4=100)
6703	36:45:18.14	03/03/2022		57.9906661	TOTALCME	DE 192.168.10.251	192.168.10.86	FTP	FTP-Response to Port 1543, 321. UNIX Type: LiF	(TCP:150, P=4=100)
6704	36:45:18.14	03/03/2022		57.1031751	TOTALCME	DE 192.168.10.86	192.168.10.251	FTP	FTP-Request from Port 1543, 324T	(TCP:150, P=4=100)
6706	36:45:18.14	03/03/2022		57.1034901	TOTALCME	DE 192.168.10.251	192.168.10.86	FTP	FTP-Response to Port 1543, 321. Features:	(TCP:150, P=4=100)
6708	36:45:18.14	03/03/2022		57.1038946	TOTALCME	DE 192.168.10.251	192.168.10.86	FTP	FTP-	(TCP:150, P=4=100)
6709	36:45:18.14	03/03/2022		57.1031466	TOTALCME	DE 192.168.10.251	192.168.10.86	FTP	FTP-Response to Port 1543, 721. End	(TCP:150, P=4=100)
6709	36:45:18.14	03/03/2022		57.1349933	TOTALCME	DE 192.168.10.86	192.168.10.251	FTP	FTP-Request from Port 1543, CPTS LFTR ON	(TCP:150, P=4=100)
6710	36:45:18.14	03/03/2022		57.1352803	TOTALCME	DE 192.168.10.251	192.168.10.86	FTP	FTP-Response to Port 1543, 720. vrfid=1	(TCP:150, P=4=100)
6711	36:45:18.14	03/03/2022		57.140051	TOTALCME	DE 192.168.10.86	192.168.10.251	FTP	FTP-Request from Port 1543, PWD	(TCP:150, P=4=100)
6712	36:45:18.14	03/03/2022		57.140251	TOTALCME	DE 192.168.10.251	192.168.10.86	FTP	FTP-Response to Port 1543, 727. Y	(TCP:150, P=4=100)
6738	36:45:18.14	03/03/2022		57.2119194	TOTALCME	DE 192.168.10.86	192.168.10.251	FTP	FTP-Request from Port 1543, TTYPE	(TCP:150, P=4=100)
6739	36:45:18.14	03/03/2022		57.2220021	TOTALCME	DE 192.168.10.251	192.168.10.86	FTP	FTP-Response to Port 1543, 720. vrfid=1	(TCP:150, P=4=100)
6737	36:45:18.14	03/03/2022		57.2225324	TOTALCME	DE 192.168.10.86	192.168.10.251	FTP	FTP-Request from Port 1543, TASY	(TCP:150, P=4=100)
6738	36:45:18.14	03/03/2022		57.2235561	TOTALCME	DE 192.168.10.251	192.168.10.86	FTP	FTP-Response to Port 1543, 720. vrfid=1	(TCP:150, P=4=100)
6742	36:45:18.14	03/03/2022		57.2350167	TOTALCME	DE 192.168.10.86	192.168.10.251	FTP	FTP-Request from Port 1543, LIST	(TCP:150, P=4=100)
6743	36:45:18.14	03/03/2022		57.2351916	TOTALCME	DE 192.168.10.251	192.168.10.86	FTP	FTP-Response to Port 1543, 720. vrfid=1	(TCP:150, P=4=100)
6748	36:45:18.14	03/03/2022		57.2362818	TOTALCME	DE 192.168.10.251	192.168.10.86	FTP	FTP-Response to Port 1543, 728. Directory send OK.	(TCP:150, P=4=100)
6749	36:45:18.14	03/03/2022		57.2364396	TOTALCME	DE 192.168.10.251	192.168.10.86	FTP	FTP-Request from Port 1543, 728B. vrfid=1	(TCP:150, P=4=100)
6800	36:46:05.74	03/03/2022		63.6761411	TPPFW:FW					

The image shows a Wireshark packet capture of an HTTP GET request. The packet is captured on the 'eth0' interface. The frame details show the Ethernet II header, Internet Protocol Version 4 header, and Hypertext Transfer Protocol header. The packet bytes pane shows the raw data of the request.

**Frame Details:**

- Frame Number: 6073, Captured Frame Length: 73, MediaType: ETHERNET
- Ethernet II Type: Internet, IP (IPv4), Destination Address: [70:2a:4f:3e:47:9d], Source Address: [00:1e:6c:85:94-01]
- IPv4 Src: 192.168.10.251, Dest: 192.168.10.86, Next Protocol: TCP, Packet ID: 53034, Total IP Length: 59
- TCP: Flags...:AP..., SrcPort=FTP control (21), DestPort=1543, Seq=722386470 - 722386489, Ack=115750247, Win=46 (scale factor 0x7) = 5888
- SeqPort: FTP control (21)
- DestPort: 1543
- SequenceNumber: 722386470 (0x2B0C5F6)
- AcknowledgmentNumber: 115750247 (0x6E63567)
- DataOffset: 80 (0x50)
- Flags: ...AP...
- Window: 46 (scale factor 0x7) = 5888
- Checksum: 0x5900, Good
- EndPoint: 0 (0x0)
- TCPPayload: SourcePort = 21, DestinationPort = 1543

**Packet Bytes:**

0000 78 24 AF 3E 67 9D 00 1E 8C 85 94 01 x8"~q...  
 0008 00 00 45 00 10 38 CF 2A 40 00 4D 06 ...P"8.  
 0018 D4 F0 C0 A8 0B FB C0 A8 56 00 15 0A...A.V..  
 0024 06 07 28 0E C5 F6 0E E6 35 67 80 18 ...A.msp  
 0030 00 2E 59 00 00 00 00 00 00 00 00 ...P...  
 003C 6C 65 20 73 65 65 64 20 4F 4B 2E 00 ...s.sand.OF..  
 0048 0A

```
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
```

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 компании, зарегистрировавшей домен.

Display Filter

Apply Remove History Load Filter Save Filter Clear

dns

Frame Summary - dns

Find Autoscroll Color Rules Aliases Columns

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
3	23:06:34 14.05.2022	0.1367232		100.90.11.238	109.194.128.3	DNS	DNS:QueryId = 0x1, QUERY (Standard query), Query for 3.128.194.109.in-addr.arpa of type PTR on class Internet
4	23:06:34 14.05.2022	0.1375433		109.194.128.3	100.90.11.238	DNS	DNS:QueryId = 0x1, QUERY (Standard query), Response - Success
5	23:06:34 14.05.2022	0.1426472		100.90.11.238	109.194.128.3	DNS	DNS:QueryId = 0x2, QUERY (Standard query), Query for standupclub.ru of type Host Addr on class Internet
6	23:06:34 14.05.2022	0.1433718		109.194.128.3	100.90.11.238	DNS	DNS:QueryId = 0x2, QUERY (Standard query), Response - Success, 5.63.158.249
7	23:06:34 14.05.2022	0.1465408		100.90.11.238	109.194.128.3	DNS	DNS:QueryId = 0x3, QUERY (Standard query), Query for standupclub.ru of type AAAA on class Internet
13	23:06:35 14.05.2022	0.9127260		109.194.128.3	100.90.11.238	DNS	DNS:QueryId = 0x3, QUERY (Standard query), Response - Success

Frame Details

Frame: Number = 6, Captured Frame Length = 138, MediaType = ETHERNET

Ethernet: Etype = Internet IP (IPv4), DestinationAddress: [F4-30-B9-AB-44-D3], SourceAddress: [00-00-5B-00-01-8A]

IPv4: Src = 109.194.128.3, Dest = 100.90.11.238, Next Protocol = UDP, Packet ID = 17609, Total IP Length = 124

Udp: SrcPort = DNS (53), DstPort = 56792, Length = 104

Dns: QueryId = 0x2, QUERY (Standard query), Response - Success, 5.63.158.249

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: 5.63.158.249	Кол-во найденных анкорев: 79
Регистратор домена: RU-CENTER-RU	Кол-во исходящих анкорев: 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.

C:\Windows\system32\cmd.exe

C:\Users\work>telnet google.com 80 -f C:\Users\work\Desktop\test.txt

Frame Summary - [Conversation Filter]

Find Autoscroll Color Rules Aliases Columns

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
6	14:30:28 15.05.2022	1.3932807	telnet.exe	100.90.0.127	142.251.1.138	TCP	TCP:Flags=...S., SrcPort=52018, DstPort=HTTP(80), PayloadLen=0, Seq=2625821938, Ack=0, Win=64240 ( Negotiating scale factor
8	14:30:28 15.05.2022	1.4229106	telnet.exe	142.251.1.138	100.90.0.127	TCP	TCP:Flags=...A..S., SrcPort=HTTP(80), DstPort=52018, PayloadLen=0, Seq=4236279390, Ack=2625821939, Win=65535 ( Negotiated s
9	14:30:28 15.05.2022	1.4230709	telnet.exe	100.90.0.127	142.251.1.138	TCP	TCP:Flags=...A...., SrcPort=52018, DstPort=HTTP(80), PayloadLen=0, Seq=2625821939, Ack=4236279391, Win=513 (scale factor 0x8
293	14:34:28 15.05.2022	241.4795520	telnet.exe	142.251.1.138	100.90.0.127	TCP	TCP:Flags=...A..F., SrcPort=HTTP(80), DstPort=52018, PayloadLen=0, Seq=4236279391, Ack=2625821939, Win=256 (scale factor 0x8
294	14:34:28 15.05.2022	241.4800593	telnet.exe	100.90.0.127	142.251.1.138	TCP	TCP:Flags=...A...., SrcPort=52018, DstPort=HTTP(80), PayloadLen=0, Seq=2625821939, Ack=4236279392, Win=513 (scale factor 0x8
295	14:34:28 15.05.2022	241.4806178	telnet.exe	100.90.0.127	142.251.1.138	TCP	TCP:Flags=...A..F., SrcPort=52018, DstPort=HTTP(80), PayloadLen=0, Seq=2625821939, Ack=4236279392, Win=513 (scale factor 0x8
296	14:34:28 15.05.2022	241.5109318	telnet.exe	142.251.1.138	100.90.0.127	TCP	TCP:Flags=...A...., SrcPort=HTTP(80), DstPort=52018, PayloadLen=0, Seq=4236279392, Ack=2625821940, Win=256 (scale factor 0x8

### 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 (0xFC807B5E) |
| 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 (0xFC807B60) |
+-----+
| DataOffset: 80 (0x50) |
+-----+
| Flags: ...A...F |
| Window: 513 (scale factor 0x8) = 131328 |
| Checksum: 0xF578, Disregarded |
| UrgentPointer: 0 (0x0) |
+-----+
```