

# Лабораторная работа №3

Тема «Анализ трафика в Wireshark»  
по дисциплине «Сетевые технологии»

Выполнил: Щербак Маргарита Романовна

Студент группы: НПИбд-02-21

«22» сентября 2023г.

### **Цели работы:**

Изучить посредством Wireshark кадры Ethernet, проанализировать PDU протоколы транспортного и прикладного уровней стека TCP/IP.

## Выполнение работы

### MAC-адресация

С помощью команды ipconfig я получила информацию о сетевых соединениях, включая Адаптеры Ethernet 3, Ethernet 4 и беспроводную сеть.

```
Администратор: Windows Pc X + v
PS C:\Users\mrShcherbak_> ipconfig

Настройка протокола IP для Windows

Адаптер Ethernet Ethernet:

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

Адаптер беспроводной локальной сети Подключение по локальной сети* 1:

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

Адаптер беспроводной локальной сети Подключение по локальной сети* 3:

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

Адаптер Ethernet Ethernet 3:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . : fe80::10d9:3b9e:6725:b3ab%11
    Автонастройка IPv4-адреса . . . . : 169.254.181.151
    Маска подсети . . . . . : 255.255.0.0
    Основной шлюз. . . . . :

Адаптер Ethernet Ethernet 4:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . : fe80::f0cf:aad0:21b:e9b0%12
    Автонастройка IPv4-адреса . . . . : 169.254.56.53
    Маска подсети . . . . . : 255.255.0.0
    Основной шлюз. . . . . :

Адаптер беспроводной локальной сети Беспроводная сеть:

    DNS-суффикс подключения . . . . . : rudn.ru
    Локальный IPv6-адрес канала . . . : fe80::df8b:6ebd:c899:6b1f%6
    IPv4-адрес. . . . . : 192.168.209.83
    Маска подсети . . . . . : 255.255.224.0
    Основной шлюз. . . . . : 192.168.192.1

Адаптер Ethernet Сетевое подключение Bluetooth:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :
PS C:\Users\mrShcherbak_> |
```

```
Администратор: Windows Pc X + v

Адаптер Ethernet Ethernet 4:

DNS-суффикс подключения . . . . . :
Описание. . . . . : VirtualBox Host-Only Ethernet Adapter #2
Физический адрес. . . . . : 08-00-27-00-80-00
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::f0cf:aad0:21b:e9b0%12(Основной)
Автонастройка IPv4-адреса . . . . : 169.254.56.53(Основной)
Маска подсети . . . . . : 255.255.0.0
Основной шлюз. . . . . :
IAID DHCPv6 . . . . . : 453509159
DUID клиента DHCPv6 . . . . . : 00-01-00-01-2B-6A-8E-42-80-30-49-14-F6-C3
NetBios через TCP/IP. . . . . : Включен

Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения . . . . . : rudn.ru
Описание. . . . . : Qualcomm Atheros QCA9377 Wireless Network Adapter
Физический адрес. . . . . : 80-30-49-14-F6-C3
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::df8b:6ebd:c899:6b1f%6(Основной)
IPv4-адрес. . . . . : 192.168.209.83(Основной)
Маска подсети . . . . . : 255.255.224.0
Аренда получена. . . . . : 21 сентября 2023 г. 14:18:56
Срок аренды истекает. . . . . : 21 сентября 2023 г. 15:48:58
Основной шлюз. . . . . : 192.168.192.1
DHCP-сервер. . . . . : 192.168.192.3
IAID DHCPv6 . . . . . : 58732617
DUID клиента DHCPv6 . . . . . : 00-01-00-01-2B-6A-8E-42-80-30-49-14-F6-C3
DNS-серверы. . . . . : 193.232.218.195
NetBios через TCP/IP. . . . . : Включен

Адаптер Ethernet Сетевое подключение Bluetooth:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Bluetooth Device (Personal Area Network)
Физический адрес. . . . . : 80-30-49-14-F6-C4
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
PS C:\Users\mrShcherbak_> |
```

Вывод подробных сведений о конфигурации всех адаптеров

```
Администратор: Windows Pc
PS C:\Users\mrShcherbak_> ipconfig /displaydns

Настройка протокола IP для Windows

wpad
-----
Имя не существует.

wpad
-----
Имя не существует.

ocsp.digicert.com
-----
Имя записи. . . . . : ocsp.digicert.com
Тип записи. . . . . : 5
Срок жизни. . . . . : 1745
Длина данных. . . . : 8
Раздел. . . . . : Ответ
CNAME-запись. . . . : ocsp.edge.digicert.com

Имя записи. . . . . : ocsp.edge.digicert.com
Тип записи. . . . . : 5
Срок жизни. . . . . : 1745
Длина данных. . . . : 8
Раздел. . . . . : Ответ
CNAME-запись. . . . : fp2e7a.wpc.2be4.phicdn.net

Имя записи. . . . . : fp2e7a.wpc.2be4.phicdn.net
Тип записи. . . . . : 5
Срок жизни. . . . . : 1745
Длина данных. . . . : 8
Раздел. . . . . : Ответ
CNAME-запись. . . . : fp2e7a.wpc.phicdn.net

Имя записи. . . . . : fp2e7a.wpc.phicdn.net
Тип записи. . . . . : 1
Срок жизни. . . . . : 1745
Длина данных. . . . : 4
```

Выполнение команд ipconfig /displaydns и ipconfig /flushdns

```
PS C:\Users\mrShcherbak_> ipconfig /flushdns

Настройка протокола IP для Windows

Кэш сопоставителя DNS успешно очищен.
PS C:\Users\mrShcherbak_> ipconfig /displaydns

Настройка протокола IP для Windows

PS C:\Users\mrShcherbak_> |
```

Очистка кэша сопоставителя DNS с помощью команды ipconfig /flushdns и проверка наличия кэша командой ipconfig /displaydns

```
PS C:\Users\mrShcherbak_> ipconfig /displaydns > newff.txt
PS C:\Users\mrShcherbak_> ipconfig /all | more
```

#### Настройка протокола IP для Windows

```
Имя компьютера . . . . . : msk-mrshcherbak-gw-1
Основной DNS-суффикс . . . . . :
Тип узла. . . . . : Гибридный
IP-маршрутизация включена . . . . : Нет
WINS-прокси включен . . . . . : Нет
Порядок просмотра суффиксов DNS . : rudn.ru
```

#### Адаптер Ethernet Ethernet:

```
Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Realtek PCIe GbE Family Controller
Физический адрес. . . . . : B4-A9-FC-A2-F8-35
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. . . . . : 92-30-49-14-F6-C3
DHCP включен. . . . . : Нет
Автонастройка включена. . . . . : Да
```

#### Адаптер беспроводной локальной сети Подключение по локальной сети\* 3:

```
Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
Физический адрес. . . . . : 82-30-49-14-F6-C3
```

— Далее — |

```
newff
Файл Изменить Просмотр
Настройка протокола IP для Windows

browser-notifications.opera.com
-----
Имя записи. . . . . : browser-notifications.opera.com
Тип записи. . . . . : 5
Срок жизни. . . . . : 9
Длина данных. . . . . : 8
Раздел. . . . . : Ответ
CNAME-запись. . . . . : browser-notifications.geo.opera.com

Имя записи. . . . . : browser-notifications.geo.opera.com
Тип записи. . . . . : 5
Срок жизни. . . . . : 9
Длина данных. . . . . : 8
Раздел. . . . . : Ответ
CNAME-запись. . . . . : eu-browser-notifications.opera.com

Имя записи. . . . . : eu-browser-notifications.opera.com
Тип записи. . . . . : 1
Срок жизни. . . . . : 9
Длина данных. . . . . : 4
Раздел. . . . . : Ответ
A-запись (узла) . . . : 185.26.182.112

Имя записи. . . . . : eu-browser-notifications.opera.com
Тип записи. . . . . : 1
Срок жизни. . . . . : 9
Длина данных. . . . . : 4
Раздел. . . . . : Ответ
A-запись (узла) . . . : 185.26.182.111

api.dropboxapi.com
-----
Имя записи. . . . . : api.dropboxapi.com
Тип записи. . . . . : 5
Срок жизни. . . . . : 40
Длина данных. . . . . : 8
Раздел. . . . . : Ответ
CNAME-запись. . . . . : api.dropbox.com
```

Командой `ipconfig /displaydns > newff.txt` создается файл `newff.txt` в папке `C:\Users\mrShcherbak_`, содержащий вывод команды `ipconfig /displaydns`. Команда `ipconfig /all | more` разбивает подробные сведения о конфигурации всех адаптеров на страницы.



```
PS C:\Users\mrShcherbak_> ipconfig /all
```

#### Настройка протокола IP для Windows

```
Имя компьютера . . . . . : msk-mrshcherbak-gw-1
Основной DNS-суффикс . . . . . :
Тип узла. . . . . : Гибридный
IP-маршрутизация включена . . . . : Нет
WINS-прокси включен . . . . . : Нет
Порядок просмотра суффиксов DNS . : rudn.ru
```

#### Адаптер Ethernet Ethernet:

```
Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Realtek PCIe GbE Family Controller
Физический адрес. . . . . : B4-A9-FC-A2-F8-35
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. . . . . : 92-30-49-14-F6-C3
DHCP включен. . . . . : Нет
Автонастройка включена. . . . . : Да
```

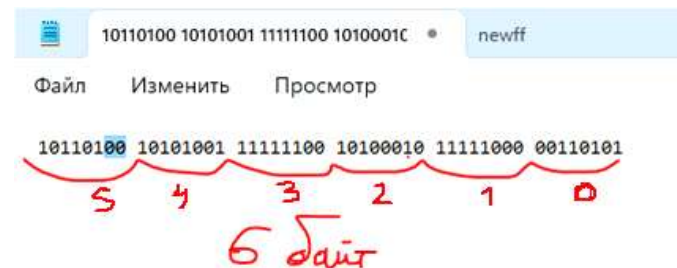
#### Адаптер беспроводной локальной сети Подключение по локальной сети\* 3:

```
Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
Физический адрес. . . . . : 82-30-49-14-F6-C3
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
```

#### Адаптер Ethernet Ethernet 3:

```
DNS-суффикс подключения . . . . . :
Описание. . . . . : VirtualBox Host-Only Ethernet Adapter #3
Физический адрес. . . . . : 08-00-27-00-88-D6
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::10d9:3b9e:6725:b3ab%11(Основной)
Автонастройка IPv4-адреса . . . . : 169.254.181.151(Основной)
Маска подсети . . . . . : 255.255.0.0
Основной шлюз. . . . . :
IAID DHCPv6 . . . . . : 1057488935
```

Определила MAC-адреса сетевых устройств, их тип и описала структуру MAC-адресов



MAC-адрес сетевого устройства Ethernet в двоичной системе счисления

# Анализ кадров канального уровня в Wireshark

```
Администратор: Windows Pc
Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

Установите последнюю версию PowerShell для новых функций и улучшения! https://aka.ms/PSWindows

PS C:\Users\mrShcherbak_> choco -y install wireshark
Chocolatey v2.2.2
PS C:\Users\mrShcherbak_> choco install wireshark
Chocolatey v2.2.2
Installing the following packages:
wireshark
By installing, you accept licenses for the packages.
Progress: Downloading chocolatey-windowsupdate.extension 1.0.5... 100%
```

Установила на своем устройстве  
Wireshark

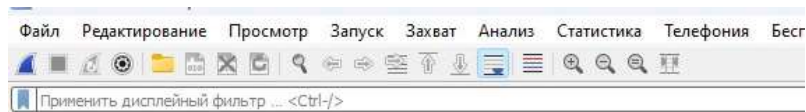
```
Администратор: Windows Pc
PS C:\Users\mrShcherbak_> choco install winpcap
Chocolatey v2.2.2
Installing the following packages:
winpcap
By installing, you accept licenses for the packages.
Progress: Downloading WinPcap 4.1.3.20161116... 100%

WinPcap v4.1.3.20161116 [Approved]
WinPcap package files install completed. Performing other installation steps.
The package WinPcap wants to run 'chocolateyInstall.ps1'.
Note: If you don't run this script, the installation will fail.
Note: To confirm automatically next time, use '-y' or consider:
choco feature enable -n allowGlobalConfirmation
Do you want to run the script?([Y]es/[A]ll - yes to all/[N]o/[P]rint): A

Downloading WinPcap
  from 'https://www.winpcap.org/install/bin/WinPcap_4_1_3.exe'
Progress: 100% - Completed download of C:\Users\mrShcherbak_\AppData\Local\Temp\chocolatey\WinPcap\WinPcapInstall.exe (893.68 KB) completed.
Hashes match.
C:\Users\mrShcherbak_\AppData\Local\Temp\chocolatey\WinPcap\4.1.3.20161116\WinPcapInstall.exe
Running Autohotkey installer
The install of WinPcap was successful.
Software install location not explicitly set, it could be in package or
default install location of installer.

Chocolatey installed 1/1 packages.
See the log for details (C:\ProgramData\chocolatey\logs\chocolatey.log).
PS C:\Users\mrShcherbak_> |
```





Welcome to Wireshark

## Захват

...используя этот фильтр:

- ☐ Беспроводная сеть
- ☐ Ethernet 4
- ☐ Ethernet 3
- ☐ Adapter for loopback traffic capture
- ☐ Подключение по локальной сети\* 11
- ☐ Подключение по локальной сети\* 10
- ☐ Подключение по локальной сети\* 9
- ☐ Сетевое подключение Bluetooth
- ☐ Подключение по локальной сети\* 3
- ☐ Подключение по локальной сети\* 1
- ☒ Ethernet
- ☐ USBPcap1



## Список сетевых устройств на моем компьютере

Пропинговала шлюз по умолчанию своего устройства

Адаптер беспроводной локальной сети Беспроводная сеть:

```
DNS-суффикс подключения . . . . . : rudn.ru
Локальный IPv6-адрес канала . . . . : fe80::df8b:6ebd:c899:6b1f%6
IPv4-адрес. . . . . : 192.168.209.83
Маска подсети . . . . . : 255.255.224.0
Основной шлюз. . . . . : 192.168.192.1
```

Адаптер Ethernet Сетевое подключение Bluetooth:

```
Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
PS C:\Users\mrShcherbak_> ping -n 4 192.168.192.1
```

```
Обмен пакетами с 192.168.192.1 по с 32 байтами данных:
Ответ от 192.168.192.1: число байт=32 время=1мс TTL=254
Ответ от 192.168.192.1: число байт=32 время=1мс TTL=254
Ответ от 192.168.192.1: число байт=32 время=1мс TTL=254
Ответ от 192.168.192.1: число байт=32 время=1мс TTL=254
```

Статистика Ping для 192.168.192.1:

```
Пакетов: отправлено = 4, получено = 4, потеряно = 0
(0% потеря)
```

Приблизительное время приема-передачи в мс:

```
Минимальное = 1мсек, Максимальное = 1 мсек, Среднее = 1 мсек
```

```
PS C:\Users\mrShcherbak_> |
```

Захват из Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

архив

No.	Time	Source	Destination	Protocol	Length	Info
168	15.162299	192.168.209.83	192.168.192.1	ICMP	74	Echo (ping) request id=0x0001, seq=33/8448, ttl=128 (reply in 169)
169	15.163904	192.168.192.1	192.168.209.83	ICMP	74	Echo (ping) reply id=0x0001, seq=33/8448, ttl=254 (request in 168)

> Frame 168: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{27FEDF1F-...}

Ethernet II, Src: LiteonTe\_14:f6:c3 (80:30:49:14:f6:c3), Dst: Cisco\_60:9c:eb (70:18:a7:60:9c:eb)

> Destination: Cisco\_60:9c:eb (70:18:a7:60:9c:eb)

> Source: LiteonTe\_14:f6:c3 (80:30:49:14:f6:c3)

Type: IPv4 (0x0008)

Internet Protocol Version 4, Src: 192.168.209.83, Dst: 192.168.192.1

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 60

Identification: 0x550b (21771)

0000 .... = Flags: 0x0

0... .... = Reserved bit: Not set

.0... .... = Don't fragment: Not set

.0... .... = More fragments: Not set

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 128

Protocol: ICMP (1)

Header Checksum: 8xd30f [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.209.83

Destination Address: 192.168.192.1

> Internet Control Message Protocol

Изучила эхо-запрос и  
эхо-ответ ICMP в  
программе Wireshark

Захват из Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

архив

No.	Time	Source	Destination	Protocol	Length	Info
168	15.162299	192.168.209.83	192.168.192.1	ICMP	74	Echo (ping) request id=0x0001, seq=33/8448, ttl=128 (reply in 169)
169	15.163904	192.168.192.1	192.168.209.83	ICMP	74	Echo (ping) reply id=0x0001, seq=33/8448, ttl=254 (request in 168)

> Frame 169: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{27FEDF1F-...}

Ethernet II, Src: Cisco\_60:9c:eb (70:18:a7:60:9c:eb), Dst: LiteonTe\_14:f6:c3 (80:30:49:14:f6:c3)

> Destination: LiteonTe\_14:f6:c3 (80:30:49:14:f6:c3)

> Source: Cisco\_60:9c:eb (70:18:a7:60:9c:eb)

Type: IPv4 (0x0008)

Internet Protocol Version 4, Src: 192.168.192.1, Dst: 192.168.209.83

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 60

Identification: 0x550b (21771)

0000 .... = Flags: 0x0

0... .... = Reserved bit: Not set

.0... .... = Don't fragment: Not set

.0... .... = More fragments: Not set

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 254

Protocol: ICMP (1)

Header Checksum: 8x550f [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.192.1

Destination Address: 192.168.209.83

> Internet Control Message Protocol

Захват из Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

arp or icmp

No.	Time	Source	Destination	Protocol	Length	Info
301	43.934622	LiteonTe_14:f6:c3	Broadcast	ARP	42	Who has 192.168.216.123? Tell 192.168.209.83
302	43.936337	IntelCor_af:d5:7a	LiteonTe_14:f6:c3	ARP	56	192.168.216.123 is at 90:78:41:af:d5:7a

> Frame 301: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF\_{27FEDF1F...}

▼ Ethernet II, Src: LiteonTe\_14:f6:c3 (80:30:49:14:f6:c3), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

▼ Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Address: Broadcast (ff:ff:ff:ff:ff:ff)

.... ..1. .... = LG bit: Locally administered address (this is NOT the factory def...

.... ..1 .... = IG bit: Group address (multicast/broadcast)

▼ Source: LiteonTe\_14:f6:c3 (80:30:49:14:f6:c3)

Address: LiteonTe\_14:f6:c3 (80:30:49:14:f6:c3)

.... ..0. .... = LG bit: Globally unique address (factory default)

.... ..0 .... = IG bit: Individual address (unicast)

Type: ARP (0x0806)

▼ Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

Sender MAC address: LiteonTe\_14:f6:c3 (80:30:49:14:f6:c3)

Sender IP address: 192.168.209.83

Target MAC address: 00:00:00\_00:00:00 (00:00:00:00:00:00)

Target IP address: 192.168.216.123

0000 ff ff ff ff ff ff  
0010 08 00 06 04 00 01  
0020 00 00 00 00 00 00

Изучила кадры  
данных протокола  
ARP

```
PS C:\Users\mrShcherbak_> ping rudn.ru
```

```
Обмен пакетами с rudn.ru [185.178.208.57] 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 185.178.208.57:
```

```
Пакетов: отправлено = 4, получено = 0, потеряно = 4
(100% потеря)
```

```
PS C:\Users\mrShcherbak_> |
```

Пропинговала по имени  
известный мне адрес — ping  
rudn.ru

Беспроводная сеть

Файл Редактирование Просмотр Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

arp or icmp

No.	Time	Source	Destination	Protocol	Length	Info
9	3.880134	Cisco_c6:af:00	Broadcast	ARP	42	Gratuitous ARP for 192.168.192.149 (Reply)
20	6.772610	192.168.209.83	185.178.208.57	ICMP	74	Echo (ping) request id=0x0001, seq=45/11520, ttl=128 (no response found!)
42	11.394615	192.168.209.83	185.178.208.57	ICMP	74	Echo (ping) request id=0x0001, seq=46/11776, ttl=128 (no response found!)
57	16.384259	192.168.209.83	185.178.208.57	ICMP	74	Echo (ping) request id=0x0001, seq=47/12032, ttl=128 (no response found!)
78	21.401209	192.168.209.83	185.178.208.57	ICMP	74	Echo (ping) request id=0x0001, seq=48/12288, ttl=128 (no response found!)
354	86.260245	192.168.209.83	193.232.210.195	ICMP	367	Destination unreachable (Port unreachable)
451	90.148875	Cisco_c6:af:00	Broadcast	ARP	42	Gratuitous ARP for 192.168.215.150 (Reply)

> Frame 20: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{27FE0F1} Ethernet II, Src: LiteonTe\_14:f6:c3 (80:30:49:14:f6:c3), Dst: Cisco\_60:9c:eb (70:18:a7:60:9c:eb)

- Destination: Cisco\_60:9c:eb (70:18:a7:60:9c:eb)  
Address: Cisco\_60:9c:eb (70:18:a7:60:9c:eb)  
.....0. .... = LG bit: Globally unique address (factory default)  
.....0. .... = IG bit: Individual address (unicast)
- Source: LiteonTe\_14:f6:c3 (80:30:49:14:f6:c3)  
Address: LiteonTe\_14:f6:c3 (80:30:49:14:f6:c3)  
.....0. .... = LG bit: Globally unique address (factory default)  
.....0. .... = IG bit: Individual address (unicast)

Type: IPv4 (0x0000)

Internet Protocol Version 4, Src: 192.168.209.83, Dst: 185.178.208.57

0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
0000 00.. = Differentiated Services Codepoint: Default (0)  
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 60  
Identification: 0xeffc (61436)

000. .... = Flags: 0x0  
0... .... = Reserved bit: Not set  
.0... .... = Don't fragment: Not set  
..0. .... = More fragments: Not set  
...0 0000 0000 0000 = Fragment Offset: 0  
Time to Live: 128  
Protocol: ICMP (1)

0000 70 18 a7 60 9c eb 80 30 49 14 f6 c3 00 00 45 00 p... 0 I... E-  
0010 00 3c ef fc 00 00 00 01 2e dc c0 a8 d1 53 b9 b2 .<.....S..  
0020 d0 39 00 00 4d 2e 00 01 00 2d 61 62 63 64 65 66 9 A...-abcdef  
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmopqrstuv  
0040 77 61 62 63 64 65 66 67 68 69 wabcdefgh

Сведения о запросах и ответах протоколов ARP и ICMP



# Анализ протоколов транспортного уровня в Wireshark

The image shows a Wireshark packet capture of an HTTP GET request. The packet list on the left shows a packet of length 334 bytes. The packet details pane on the right shows the following information:

- Source Port: 61031
- Destination Port: 80
- [Stream index: 55]
- [Conversation completeness: Complete, WITH\_DATA (31)]
- [TCP Segment Len: 524]
- Sequence Number: 1 (relative sequence number)
- Sequence Number (raw): 820873544
- [Next Sequence Number: 525 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 217209822
- 0101 .... = Header Length: 20 bytes (5)
- Flags: 0x018 (PSH, ACK)
- Window: 256
- [Calculated window size: 65536]
- [Window size scaling factor: 256]
- Checksum: 0x01db [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- [Timestamps]
- [SEQ/ACK analysis]
- TCP payload (524 bytes)
- Hypertext Transfer Protocol

## Сведения по протоколу TCP (GET)

The image shows a Wireshark packet capture of an HTTP GET request. The packet list on the left shows a packet of length 334 bytes. The packet details pane on the right shows the following information:

- Source Port: 80
- Destination Port: 61031
- [Stream index: 55]
- [Conversation completeness: Complete, WITH\_DATA (31)]
- [TCP Segment Len: 137]
- Sequence Number: 1 (relative sequence number)
- Sequence Number (raw): 217209822
- [Next Sequence Number: 138 (relative sequence number)]
- Acknowledgment Number: 525 (relative ack number)
- Acknowledgment number (raw): 820874868
- 0101 .... = Header Length: 20 bytes (5)
- Flags: 0x018 (PSH, ACK)
- Window: 501
- [Calculated window size: 64128]
- [Window size scaling factor: 128]
- Checksum: 0x74d3 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- [Timestamps]
- [SEQ/ACK analysis]
- TCP payload (137 bytes)
- Hypertext Transfer Protocol

## Сведения по протоколу TCP

Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

dns

No.	Time	Source	Destination	Protocol	Length	Info
186	17.439174	192.168.209.83	193.232.218.195	DNS	91	Standard query 0xe576 A teams.events.data.microsoft.com
187	17.441565	193.232.218.195	192.168.209.83	DNS	396	Standard query response 0xe576 A teams.events.data.microsoft.com
288	39.978479	192.168.209.83	193.232.218.195	DNS	72	Standard query 0x3a8f A info.cern.ch

Frame 186: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF... (27FED...)

Ethernet II, Src: LiteonTe\_14:f6:c3 (00:30:49:14:f6:c3), Dst: Cisco\_60:9c:eb (70:18:a7:60:9c:eb)

Destination: Cisco\_60:9c:eb (70:18:a7:60:9c:eb)

Address: Cisco\_60:9c:eb (70:18:a7:60:9c:eb)

.... 0. .... = 10 bit: Globally unique address (factory default)

.... 0. .... = 10 bit: Individual address (unicast)

Source: LiteonTe\_14:f6:c3 (00:30:49:14:f6:c3)

Address: LiteonTe\_14:f6:c3 (00:30:49:14:f6:c3)

.... 0. .... = 10 bit: Globally unique address (factory default)

.... 0. .... = 10 bit: Individual address (unicast)

Type: IPv4 (0x0000)

Internet Protocol Version 4, Src: 192.168.209.83, Dst: 193.232.218.195

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)

.....00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 77

Identification: 0x859b (34459)

000. .... = Flags: 0x0

0... .... = Reserved bit: Not set

0.. .... = Don't fragment: Not set

..0. .... = More fragments: Not set

...0 0000 0000 = Fragment Offset: 0

Time to Live: 128

Protocol: UDP (17)

Header Checksum: 0x855c [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.209.83

Destination Address: 193.232.218.195

Поиск по фильтру dns

Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

dns

No.	Time	Source	Destination	Protocol	Length	Info
186	17.439174	192.168.209.83	193.232.218.195	DNS	91	Standard query 0xe576 A teams.events.data.microsoft.com
187	17.441565	193.232.218.195	192.168.209.83	DNS	396	Standard query response 0xe576 A teams.events.data.microsoft.com
288	39.978479	192.168.209.83	193.232.218.195	DNS	72	Standard query 0x3a8f A info.cern.ch
281	39.978545	192.168.209.83	193.232.218.195	DNS	85	Standard query 0x27eb HTTPS_0001_https.info.cern.ch
282	40.061048	193.232.218.195	192.168.209.83	DNS	144	Standard query response 0x27eb No such name HTTPS_0001_https.inf
284	40.110030	193.232.218.195	192.168.209.83	DNS	188	Standard query response 0x3a8f A info.cern.ch CNAME webafs701.cern
287	40.419531	192.168.209.83	193.232.218.195	DNS	72	Standard query 0x32f1 A info.cern.ch
288	40.420654	192.168.209.83	193.232.218.195	DNS	72	Standard query 0xf220 A info.cern.ch
289	40.422087	192.168.209.83	193.232.218.195	DNS	72	Standard query 0x2b5f A info.cern.ch

Header Checksum: 0x855c [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.209.83

Destination Address: 193.232.218.195

User Datagram Protocol, Src Port: 54314, Dst Port: 53

Source Port: 54314

Destination Port: 53

Length: 38

Checksum: 0xa09a [unverified]

[Checksum status: Unverified]

[Stream index: 4]

[Timestamps]

UDP payload (38 bytes)

Domain Name System (query)

Transaction ID: 0x32f1

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

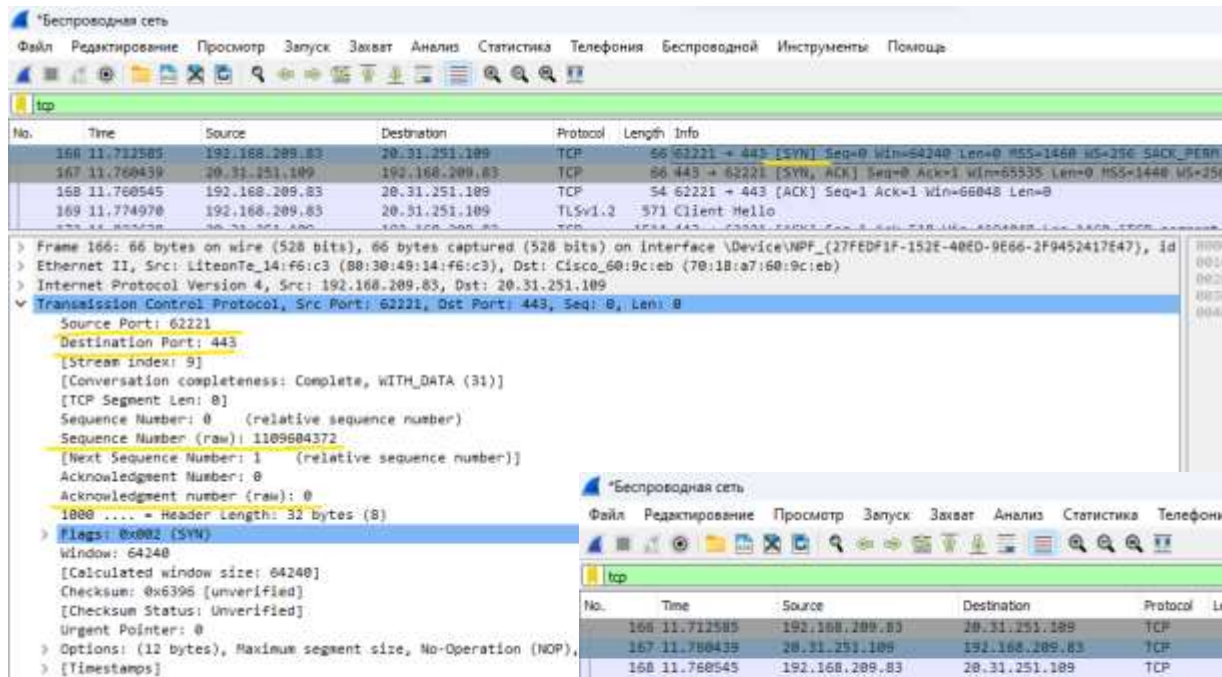
Info.cern.ch: type A, class IN

[Response Len: 792]

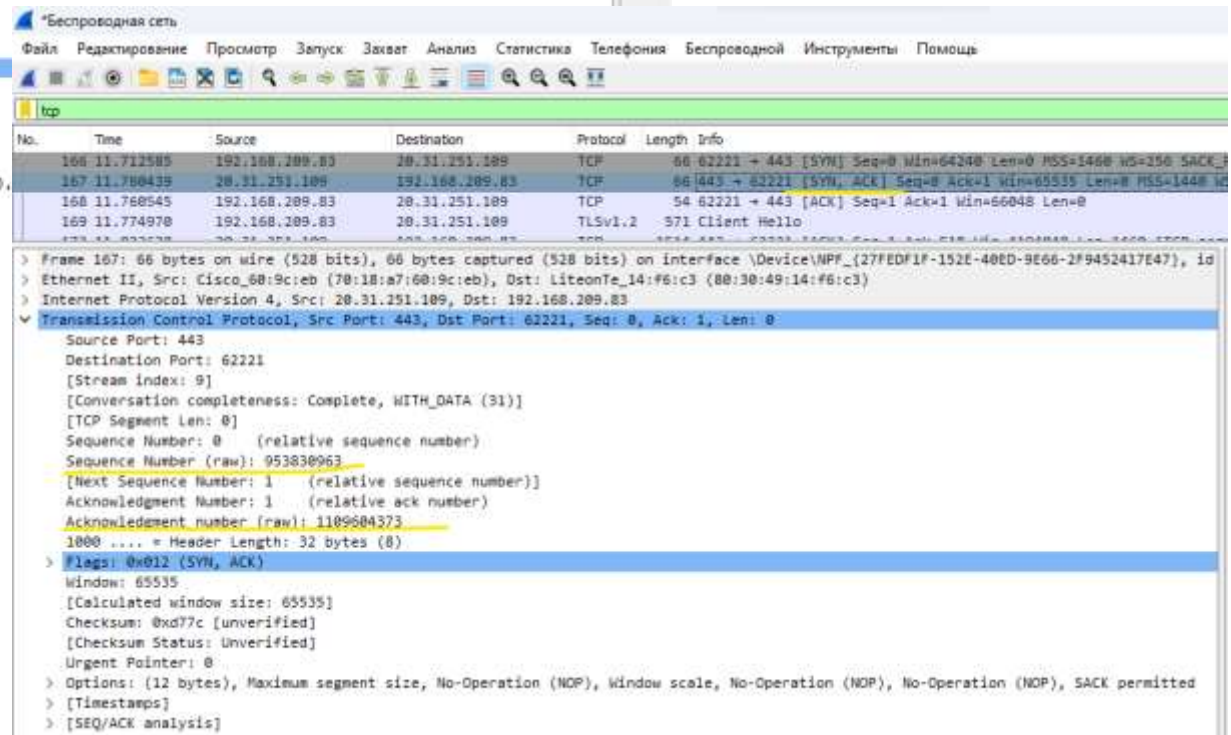
Сведения по протоколу UDP



# Анализ handshake протокола TCP в Wireshark



Первый этап  
«рукопожатия»



Второй этап  
«рукопожатия»

Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

tcp

No.	Time	Source	Destination	Protocol	Length	Info
166	11.713585	192.168.209.83	20.31.251.109	TCP	66	62221 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
167	11.768438	20.31.251.109	192.168.209.83	TCP	66	443 → 62221 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=
168	11.768545	192.168.209.83	20.31.251.109	TCP	54	62221 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
169	11.774970	192.168.209.83	20.31.251.109	TLSv1.2	571	Client Hello

> Frame 168: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{27FEDF1F-152E-40ED-9E66-2F9452417E47}, Id 0

> Ethernet II, Src: LiteonTe\_14:f6:c3 (80:30:49:14:f6:c3), Dst: Cisco\_60:9c:eb (70:18:a7:60:9c:eb)

> Internet Protocol Version 4, Src: 192.168.209.83, Dst: 20.31.251.109

Transmission Control Protocol, Src Port: 62221, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

Source Port: 62221

Destination Port: 443

[Stream index: 9]

[Conversation completeness: Complete, WITH\_DATA (31)]

[TCP Segment Len: 0]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 1189604373

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 953830964

0101 ... = Header Length: 20 bytes (5)

Flags: 0x010 (ACK)

Window: 256

[Calculated window size: 66048]

[Window size scaling factor: 256]

Checksum: 0x173a [unverified]

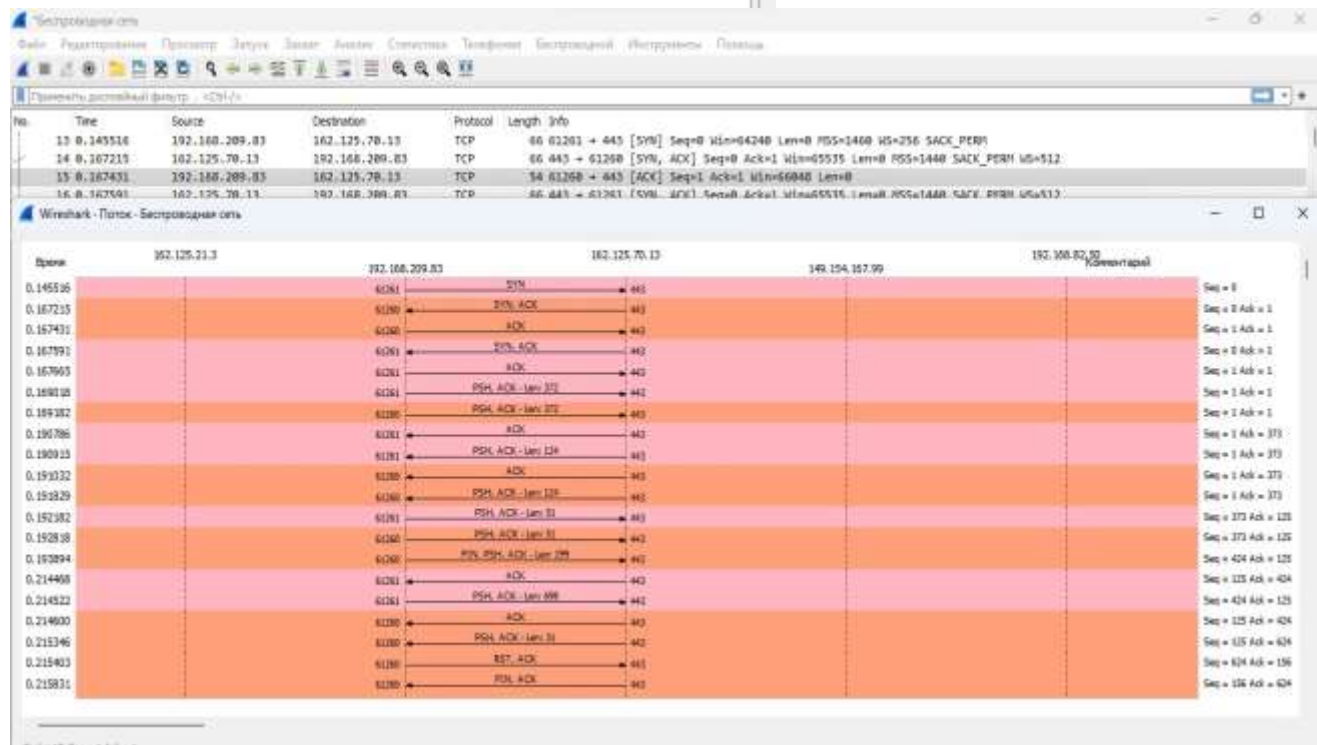
[Checksum Status: Unverified]

Urgent Pointer: 0

[Timestamps]

[SEQ/ACK analysis]

Третий этап  
«рукопожатия»



Просмотр графика  
потока

\*Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

tcp

No.	Time	Source	Destination	Protocol	Length	Info
3012	33.151197	192.168.209.83	52.182.143.210	TCP	54	62211 → 443 [ACK] Seq=10858 Ack=1227 Win=255 Len=0
3013	33.151669	192.168.209.83	52.182.143.210	TLSv1.2	96	Application Data
3014	33.349241	52.182.143.210	192.168.209.83	TCP	54	443 → 62211 [ACK] Seq=1227 Ack=10900 Win=2052 Len=0
3015	33.451918	192.168.209.29	192.168.209.83	TCP	66	49283 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P
3016	33.452027	192.168.209.83	192.168.209.29	TCP	66	7680 → 49283 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS
3017	33.456540	192.168.209.29	192.168.209.83	TCP	54	49283 → 7680 [ACK] Seq=1 Ack=1 Win=65536 Len=0
3018	33.456760	192.168.209.29	192.168.209.83	TCP	129	49283 → 7680 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=75
3019	33.456960	192.168.209.83	192.168.209.29	TCP	54	7680 → 49283 [FIN, ACK] Seq=1 Ack=76 Win=525312 Len=0
3020	33.459103	192.168.209.29	192.168.209.83	TCP	54	49283 → 7680 [ACK] Seq=76 Ack=2 Win=65536 Len=0
3021	33.459376	192.168.209.29	192.168.209.83	TCP	54	49283 → 7680 [FIN, ACK] Seq=76 Ack=2 Win=65536 Len=0
3022	33.459416	192.168.209.83	192.168.209.29	TCP	54	7680 → 49283 [ACK] Seq=2 Ack=77 Win=525312 Len=0

> Frame 3019: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{27FEDF1F-152E-40ED-9E66-2F9452417E47},  
 > Ethernet II, Src: LiteonTe\_14:f6:c3 (80:30:49:14:f6:c3), Dst: IntelCor\_69:5e:b0 (e0:2b:e9:69:5e:b0)  
 > Internet Protocol Version 4, Src: 192.168.209.83, Dst: 192.168.209.29  
 > Transmission Control Protocol, Src Port: 7680, Dst Port: 49283, Seq: 1, Ack: 76, Len: 0  
 Source Port: 7680  
 Destination Port: 49283  
 [Stream index: 43]  
 [Conversation completeness: Complete, WITH\_DATA (31)]  
 [TCP Segment Len: 0]  
 Sequence Number: 1 (relative sequence number)  
 Sequence Number (raw): 3469864546  
 [Next Sequence Number: 2 (relative sequence number)]  
 Acknowledgment Number: 76 (relative ack number)  
 Acknowledgment number (raw): 224321952  
 0101 .... = Header Length: 20 bytes (5)  
 > Flags: 0x011 (FIN, ACK)  
 Window: 2052  
 [Calculated window size: 525312]  
 [Window size scaling factor: 256]  
 Checksum: 0xf955 [unverified]  
 [Checksum Status: Unverified]  
 Urgent Pointer: 0  
 > [Timestamps]

## Заккрытие TCP-соединения

**Вывод:** таким образом, в ходе выполнения л/р №3, я изучила посредством Wireshark кадры Ethernet, проанализировала PDU протоколы транспортного и прикладного уровней стека TCP/IP.