

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятности

ОТЧЕТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ №3

дисциплина: Сетевые технологии

Студент: Алхатиб Осама

Группа: НПИбд-02-20

МОСКВА

2022 г.

Цель работы

Изучение посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.

Задания для выполнения

MAC-адресация

3.3.1.1. Постановка задачи

1. Изучение возможностей команды `ipconfig` для ОС типа Windows (`ifconfig` для систем типа Linux).
2. Определение MAC-адреса устройства и его типа.

```
Connection-specific DNS Suffix . : 
PS C:\Users\Administrator> ipconfig help
Error: unrecognized or incomplete command line.

USAGE:
    ipconfig [/allcompartments] [/? | /all |
        /renew [adapter] | /release [adapter] |
        /renew6 [adapter] | /release6 [adapter] |
        /flushdns | /displaydns | /registerdns |
        /showclassid adapter |
        /setclassid adapter [classid] |
        /showclassid6 adapter |
        /setclassid6 adapter [classid] ]

where
    adapter          Connection name
                     (wildcard characters * and ? allowed, see examples)

Options:
    /?              Display this help message
    /all            Display full configuration information.
    /release        Release the IPv4 address for the specified adapter.
    /release6       Release the IPv6 address for the specified adapter.
    /renew          Renew the IPv4 address for the specified adapter.
    /renew6         Renew the IPv6 address for the specified adapter.
    /flushdns       Purges the DNS Resolver cache.
    /registerdns     Refreshes all DHCP leases and re-registers DNS names
    /displaydns     Display the contents of the DNS Resolver Cache.
    /showclassid    Displays all the dhcp class IDs allowed for adapter.
    /setclassid     Modifies the dhcp class id.
    /showclassid6   Displays all the IPv6 DHCP class IDs allowed for adapter.
    /setclassid6    Modifies the IPv6 DHCP class id.

The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is removed.

Examples:
> ipconfig          ... Show information
> ipconfig /all     ... Show detailed information
> ipconfig /renew    ... renew all adapters
> ipconfig /renew EL* ... renew any connection that has its
                        name starting with EL
> ipconfig /release *Con* ... release all matching connections.
```

```

PS C:\Users\Administrator> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

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

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::501b:d1c7:c59f:b26d%11
    IPv4 Address. . . . . : 192.168.5.166
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.5.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
PS C:\Users\Administrator>

```

На рисунке 4 мы использовали опцию /flushdns, которая очищает кэш сопоставителя DNS.

```

PS C:\Users\Administrator> ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
PS C:\Users\Administrator>

```

2. MAC-адреса

```

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 
    Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
    Physical Address. . . . . : 76-40-BB-91-D6-FF
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 
    Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
    Physical Address. . . . . : F6-40-BB-91-D6-FF
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . : 
    Description . . . . . : Realtek RTL8822BE 802.11ac PCIe Adapter
    Physical Address. . . . . : 74-40-BB-91-D6-FF
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . : fe80::501b:d1c7:c59f:b26d%11(Preferred)
    IPv4 Address. . . . . : 192.168.5.166(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Wednesday, September 21, 2022 11:49:37 PM
    Lease Expires . . . . . : Friday, September 23, 2022 4:07:13 AM
    Default Gateway . . . . . : 192.168.5.1
    DHCP Server . . . . . : 192.168.5.1
    DHCPv6 IAID . . . . . : 108282043
    DHCPv6 Client DUID . . . . . : 00-01-00-01-29-AA-1D-16-10-62-E5-DF-DE-22
    DNS Servers . . . . . : 192.168.5.1
    NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 
    Description . . . . . : Bluetooth Device (Personal Area Network)
    Physical Address. . . . . : 74-40-BB-91-D7-00
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes

PS C:\Users\Administrator> ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
PS C:\Users\Administrator>

```

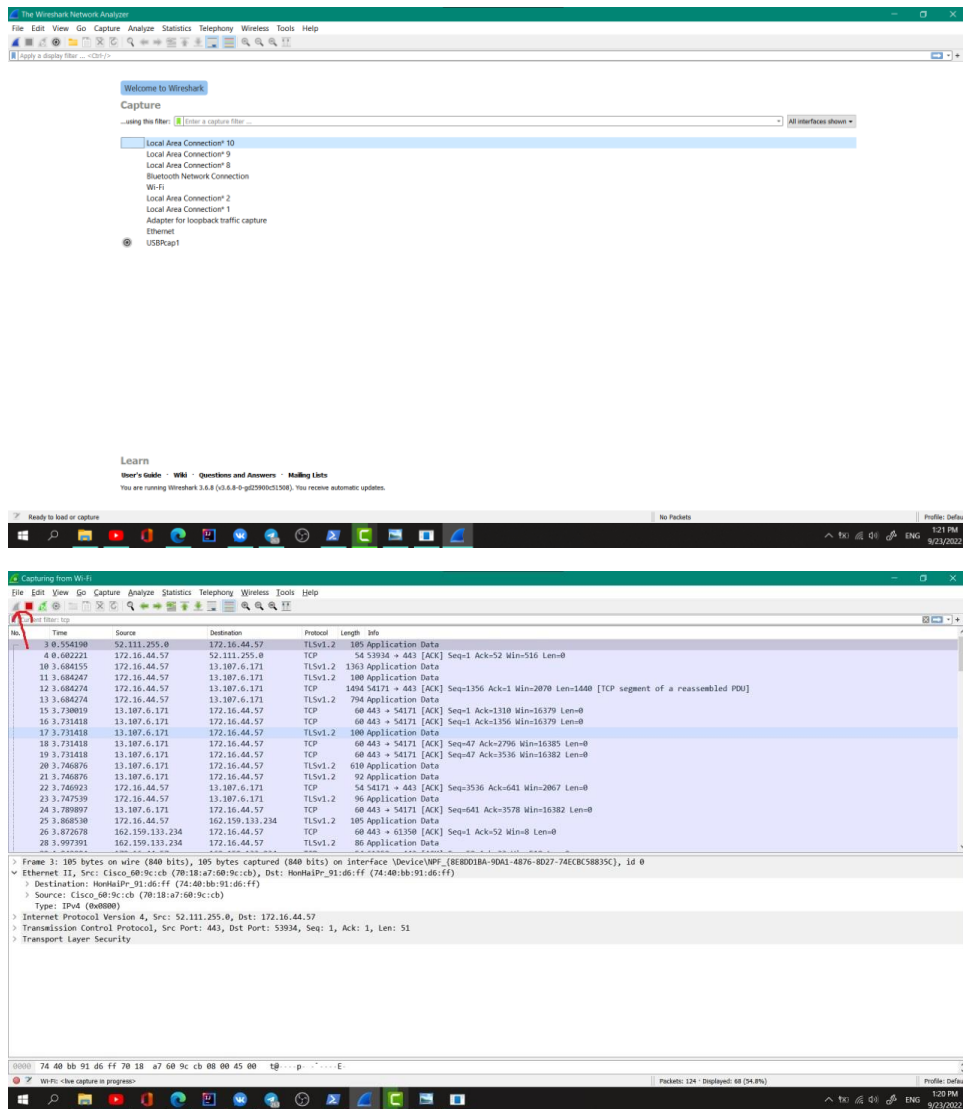
| | | | | | |
|---------|---------|----------|----------|----------|----------|
| 76 | 40 | BB | 91 | D6 | FF |
| 1110100 | 1000000 | 10111011 | 10010001 | 10010001 | 11111111 |

Анализ протоколов транспортного уровня в Wireshark

Постановка задачи С помощью Wireshark захватить и проанализировать пакеты HTTP, DNS в части заголовков и информации протоколов TCP, UDP, QUIC.



2. На вашем устройстве в браузере перейдите на сайт, работающий по протоколу HTTP (например, на сайт CERN <http://info.cern.ch/>). При необходимости получения большей информации для Wireshark поперемещайтесь по ссылкам или разделам сайта в браузере.



3.команды ipconfig IP-адрес 172.16.44.57 шлюз по умолчанию 172.16.44.1


```

PS C:\Users\Administrator> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

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

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::501b:d1c7:c59f:b26d%11
    IPv4 Address. . . . . : 172.16.44.57
    Subnet Mask . . . . . : 255.255.254.0
    Default Gateway . . . . . : 172.16.44.1

Ethernet adapter Bluetooth Network Connection:

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

```

4. Wireshark в строке фильтра укажите dns и проанализируйте информацию по протоколу UDP в случае запросов и ответов. В отчёте приведите пояснение по информации, захваченной в Wireshark.

```

PS C:\Users\Administrator> ping 172.16.44.1

Pinging 172.16.44.1 with 32 bytes of data:
Reply from 172.16.44.1: bytes=32 time=1ms TTL=254
Reply from 172.16.44.1: bytes=32 time=19ms TTL=254
Reply from 172.16.44.1: bytes=32 time=2ms TTL=254
Reply from 172.16.44.1: bytes=32 time=6ms TTL=254

Ping statistics for 172.16.44.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 19ms, Average = 7ms
PS C:\Users\Administrator>

PS C:\Users\Administrator> ping 172.16.44.1

Pinging 172.16.44.1 with 32 bytes of data:
Reply from 172.16.44.1: bytes=32 time=3ms TTL=254
Reply from 172.16.44.1: bytes=32 time=2ms TTL=254
Reply from 172.16.44.1: bytes=32 time=12ms TTL=254
Reply from 172.16.44.1: bytes=32 time=2ms TTL=254

Ping statistics for 172.16.44.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 12ms, Average = 4ms

```

5. Wireshark в строке фильтра укажите quic и проанализируйте информацию по протоколу quic в случае запросов и ответов. В отчёте приведите пояснение по информации, захваченной в Wireshark.

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|-------------------|-------------|----------|--------|--|
| 700 | 3.342788 | Apple_24:73:c0 | Broadcast | ARP | 60 | Who has 172.16.44.225? Tell 172.16.44.84 |
| 703 | 3.343947 | 26:19:46:71:28:9b | Broadcast | ARP | 60 | Who has 172.16.44.225? Tell 172.16.44.95 |
| 2731 | 13.173251 | 46:80:f1:35:62:fe | Broadcast | ARP | 60 | Who has 172.16.44.1? Tell 172.16.44.153 |
| 4736 | 25.768006 | f6:74:95:35:d9:da | Broadcast | ARP | 60 | ARP Announcement for 172.16.45.40 |
| 4868 | 27.175531 | HuaweiDe_fd:22:52 | Broadcast | ARP | 60 | Who has 172.16.44.1? Tell 172.16.44.172 |
| 4975 | 28.327861 | f6:74:95:35:d9:da | Broadcast | ARP | 60 | Who has 172.16.44.1? Tell 172.16.45.40 |
| 5017 | 28.840029 | f6:74:95:35:d9:da | Broadcast | ARP | 60 | ARP Announcement for 172.16.45.40 |
| 5162 | 30.171083 | f6:74:95:35:d9:da | Broadcast | ARP | 60 | Who has 172.16.44.1? Tell 172.16.45.40 |

6. Остановите захват трафика в Wireshark.

| | | | | | | |
|------|-----------|-------------------|-----------|-----|----|--|
| 1253 | 44.298364 | HonHaiPr_91:d6:ff | Broadcast | ARP | 42 | Who has 169.254.169.254? Tell 172.16.44.57 |
| 1275 | 44.873789 | HonHaiPr_91:d6:ff | Broadcast | ARP | 42 | Who has 169.254.169.254? Tell 172.16.44.57 |
| 1289 | 45.870903 | HonHaiPr_91:d6:ff | Broadcast | ARP | 42 | Who has 169.254.169.254? Tell 172.16.44.57 |
| 1327 | 47.294764 | Apple_0f:fc:a7 | Broadcast | ARP | 60 | Who has 172.16.44.112? Tell 172.16.44.72 |

> Frame 1253: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{8E8DD1BA-9DA1-4876-8D27-74ECBC58835C}, Ethernet II, Src: HonHaiPr_91:d6:ff (74:40:bb:91:d6:ff), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Destination: Broadcast (ff:ff:ff:ff:ff:ff)

> Source: HonHaiPr_91:d6:ff (74:40:bb:91:d6:ff)

Address: HonHaiPr_91:d6:ff (74:40:bb:91:d6:ff)

....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: HonHaiPr_91:d6:ff (74:40:bb:91:d6:ff)

Sender IP address: 172.16.44.57

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

| | | |
|------|---|----------------|
| 0000 | ff ff ff ff ff 74 40 bb 91 d6 ff 08 06 00 01 |t@..... |
| 0010 | 08 00 06 04 00 01 74 40 bb 91 d6 ff ac 10 2c 39 |t@.....,9 |
| 0020 | 00 00 00 00 00 00 a9 fe a9 fe | |

Address Resolution Protocol: Protocol

MAC-адрес источника:74:40:bb:91:d6:ff или 172.16.44.57

MAC-адрес шлюза:ff:ff:ff:ff:ff:ff или 172.16.44.1

| | | | | | | |
|------|-----------|-------------------|-----------|-----|----|--|
| 1253 | 44.298364 | HonHaiPr_91:d6:ff | Broadcast | ARP | 42 | Who has 169.254.169.254? Tell 172.16.44.57 |
| 1275 | 44.873789 | HonHaiPr_91:d6:ff | Broadcast | ARP | 42 | Who has 169.254.169.254? Tell 172.16.44.57 |
| 1289 | 45.870903 | HonHaiPr_91:d6:ff | Broadcast | ARP | 42 | Who has 169.254.169.254? Tell 172.16.44.57 |
| 1327 | 47.294764 | Apple_0f:fc:a7 | Broadcast | ARP | 60 | Who has 172.16.44.112? Tell 172.16.44.72 |

> Frame 1253: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{8E8DD1BA-9DA1-4876-8D27-74ECBC58835C}, id 0

> Ethernet II, Src: HonHaiPr_91:d6:ff (74:40:bb:91:d6:ff), 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 default)

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

> Source: HonHaiPr_91:d6:ff (74:40:bb:91:d6:ff)

Address: HonHaiPr_91:d6:ff (74:40:bb:91:d6:ff)

....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: HonHaiPr_91:d6:ff (74:40:bb:91:d6:ff)

Sender IP address: 172.16.44.57

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

Target IP address: 169.254.169.254

MAC-адрес: ff:ff:ff:ff:ff:ff или 172.16.44.57

MAC-адрес источника: ff:ff:ff:ff:ff:ff или 172.16.44.1

8. Начните новый процесс захвата трафика в Wireshark. На вашем устройстве в консоли пропингуйте по имени какой-нибудь известный вам адрес, например ping rudn.ru.

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

Pinging rudn.ru [185.178.208.57] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 185.178.208.57:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\Administrator> ping rudn.ru

Pinging rudn.ru [185.178.208.57] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 185.178.208.57:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Пропинговали Туис РУДН.

```
PS C:\Users\Administrator> ping esystem.rudn.ru

Pinging esystem.rudn.ru [188.72.108.189] with 32 bytes of data:
Reply from 188.72.108.189: bytes=32 time=4ms TTL=48
Reply from 188.72.108.189: bytes=32 time=4ms TTL=48
Reply from 188.72.108.189: bytes=32 time=3ms TTL=48
Reply from 188.72.108.189: bytes=32 time=4ms TTL=48

Ping statistics for 188.72.108.189:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 4ms, Average = 3ms
PS C:\Users\Administrator>
```

3.3.3. Анализ протоколов транспортного уровня в Wireshark

3.3.3.1. Постановка задачи

С помощью Wireshark захватить и проанализировать пакеты HTTP, DNS в части заголовков и информации протоколов TCP, UDP, QUIC

1. Запустите Wireshark. Выберите активный на вашем устройстве сетевой интерфейс. Убедитесь, что начался процесс захвата трафика.
2. На вашем устройстве в браузере перейдите на сайт, работающий по протоколу HTTP (например, на сайт CERN <http://info.cern.ch/>). При необходимости получения большей

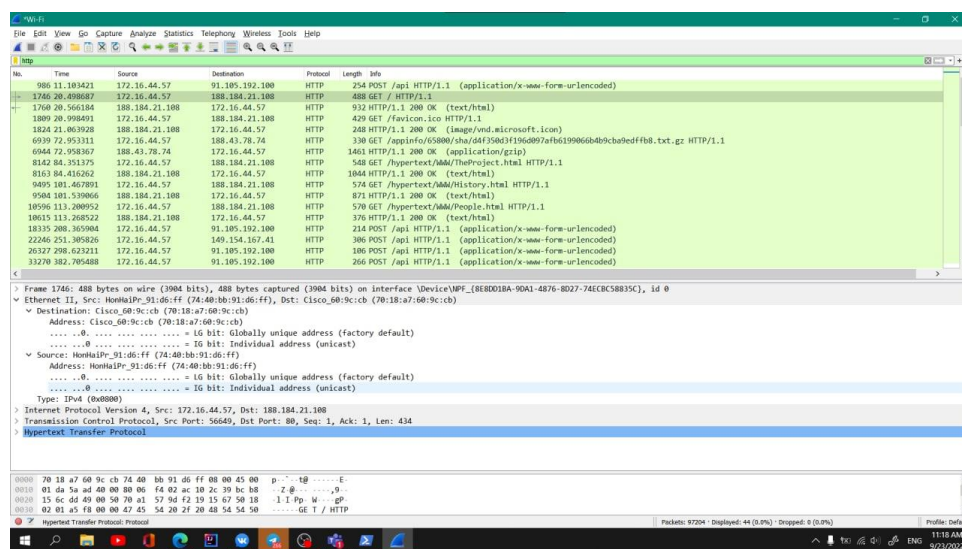
информации для Wireshark поперемещайтесь по ссылкам или разделам сайта в браузере.

http://info.cern.ch - home of the first website

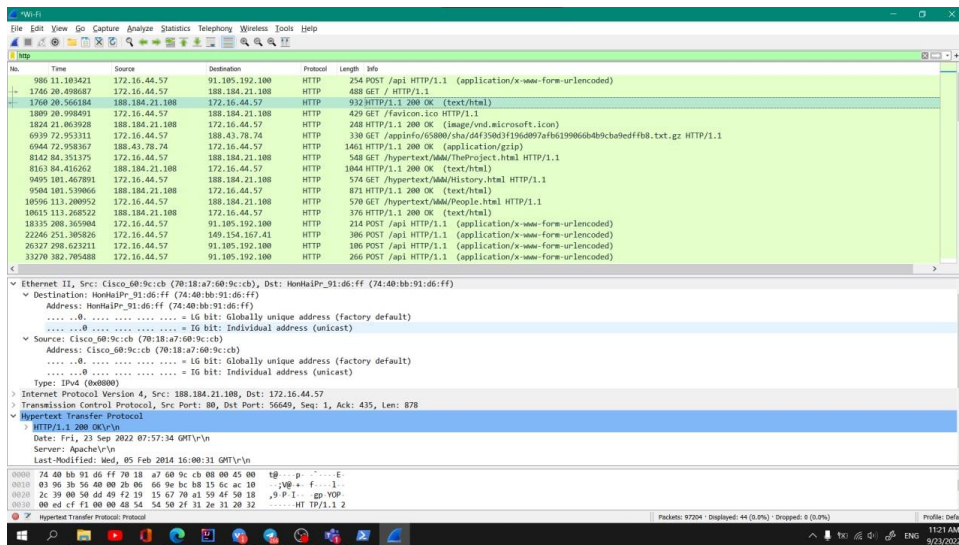
From here you can:

- [Browse the first website](#)
- [Browse the first website using the line-mode browser simulator](#)
- [Learn about the birth of the web](#)
- [Learn about CERN, the physics laboratory where the web was born](#)

3. В Wireshark в строке фильтра укажите http и проанализируйте информацию по протоколу TCP в случае запросов и ответов. В отчёте приведите пояснение по информации, захваченной в Wireshark.

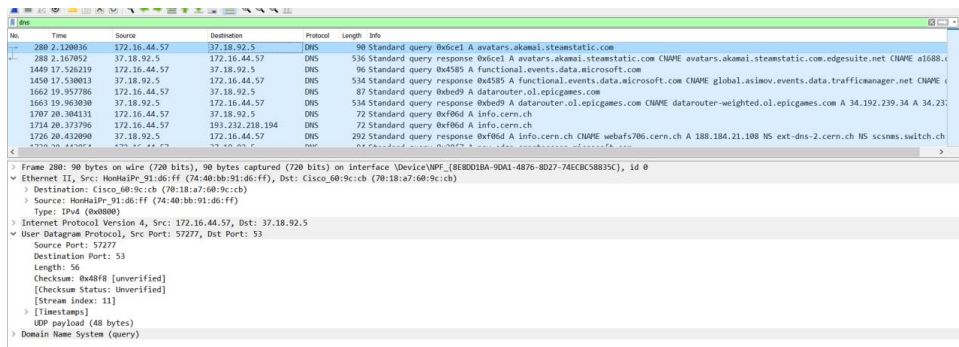


| |
|--|
| Type: IPv4 (0x0800) |
| Internet Protocol Version 4, Src: 172.16.44.57, Dst: 188.184.21.108 |
| 0100 = Version: 4 |
| 0101 = Header Length: 20 bytes (5) |
| > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) |
| Total Length: 474 |
| Identification: 0x5aad (23213) |
| > Flags: 0x40, Don't fragment |
| ...0 0000 0000 0000 = Fragment Offset: 0 |
| Time to Live: 128 |
| Protocol: TCP (6) |
| Header Checksum: 0xf402 [validation disabled] |
| [Header checksum status: Unverified] |
| Source Address: 172.16.44.57 |
| Destination Address: 188.184.21.108 |
| > Transmission Control Protocol, Src Port: 56649, Dst Port: 80, Seq: 1, Ack: 1, Len: 434 |
| > Hypertext Transfer Protocol |



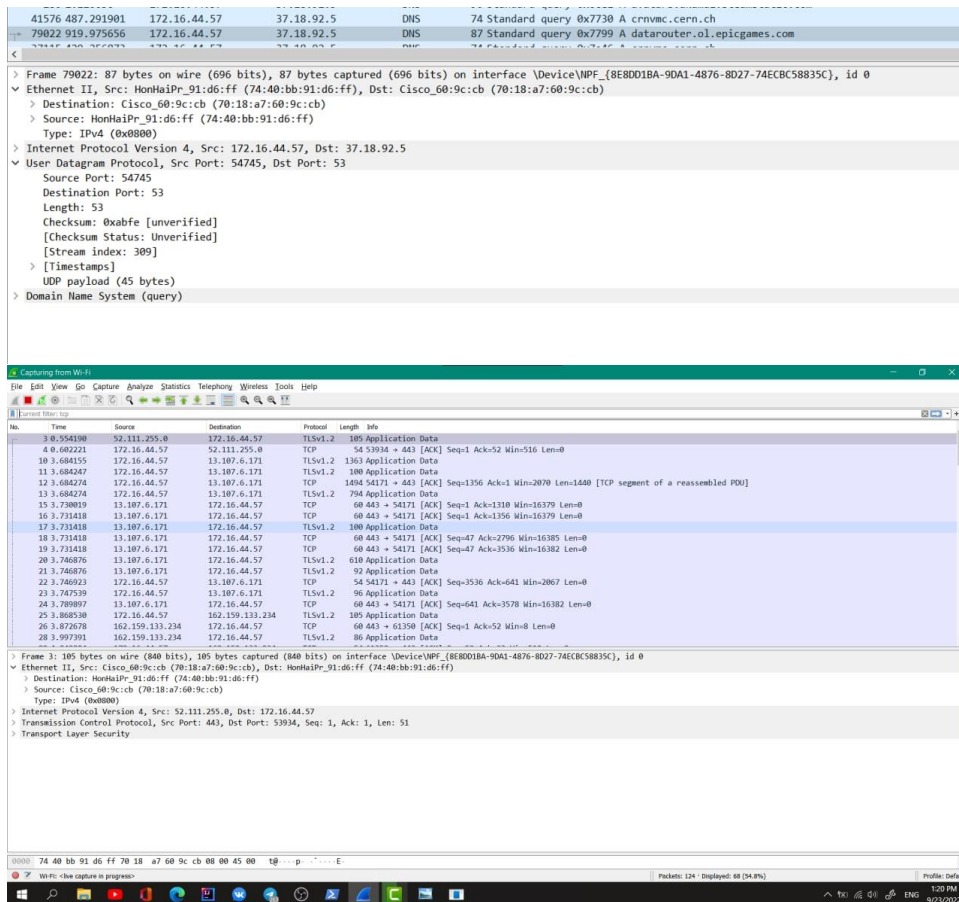
```
[Request in frame: 1746]
[Request URI: http://info.cern.ch/]
File Data: 646 bytes
Line-based text data: text/html (13 lines)
<html><head></head><body><header>\n
<title>http://info.cern.ch</title>\n
</header>\n
<h1>http://info.cern.ch - home of the first website</h1>\n
<p>From here you can:</p>\n
<ul>\n
<li>a href="http://info.cern.ch/hypertext/MMD/TheProject.html">Browse the first website</li>\n
<li>a href="http://line-mode.cern.ch/www/hypertext/MMD/TheProject.html">Browse the first website using the line-mode browser simulator</li>\n
<li>a href="http://home.web.cern.ch/topics/birth-web">Learn about the birth of the web</li>\n
<li>a href="http://home.web.cern.ch/about">Learn about CERN, the physics laboratory where the web was born</li>\n
</ul>\n
</body></html>\n
```

4. Wireshark в строке фильтра укажите dns и проанализируйте информацию по протоколу UDP в случае запросов и ответов. В отчёте приведите пояснение по информации, захваченной в Wireshark.



5. Wireshark в строке фильтра укажите quic и проанализируйте информацию по протоколу quic в случае запросов и ответов. В отчёте приведите пояснение по информации, захваченной в Wireshark.

6. Остановите захват трафика в Wireshark.



Вывод

Посредством Wireshark кадров Ethernet, анализировала PDU протоколы транспортного и прикладного уровней стека TCP/IP