РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятносте

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.

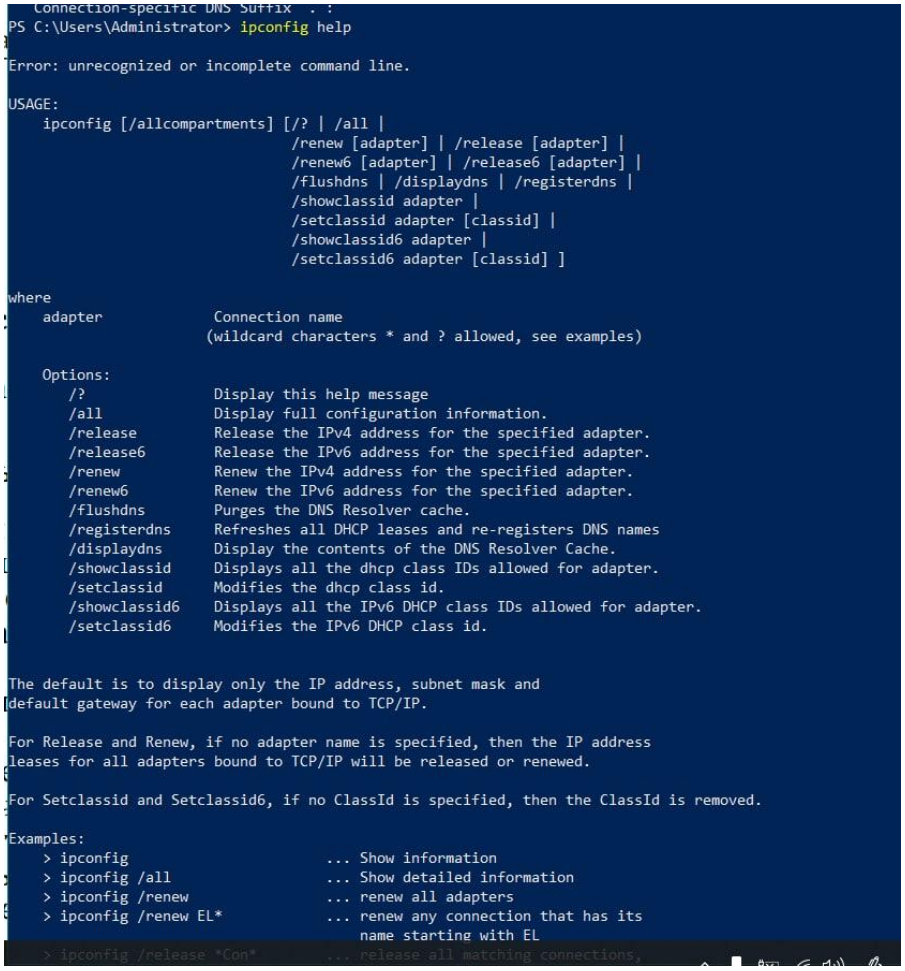
Задания для выполнения

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.



```
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

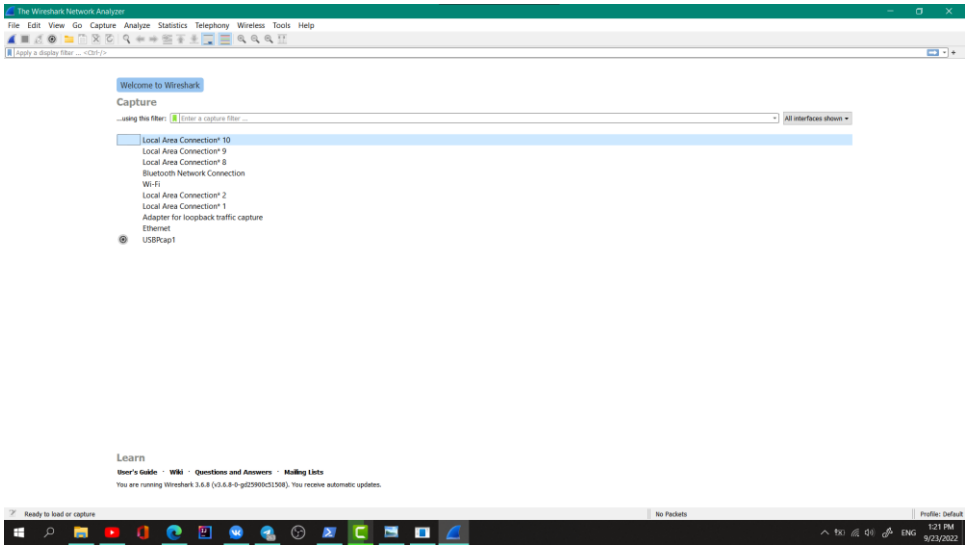
```
Wireless LAN adapter Local Area Connection* 1:

   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>
```

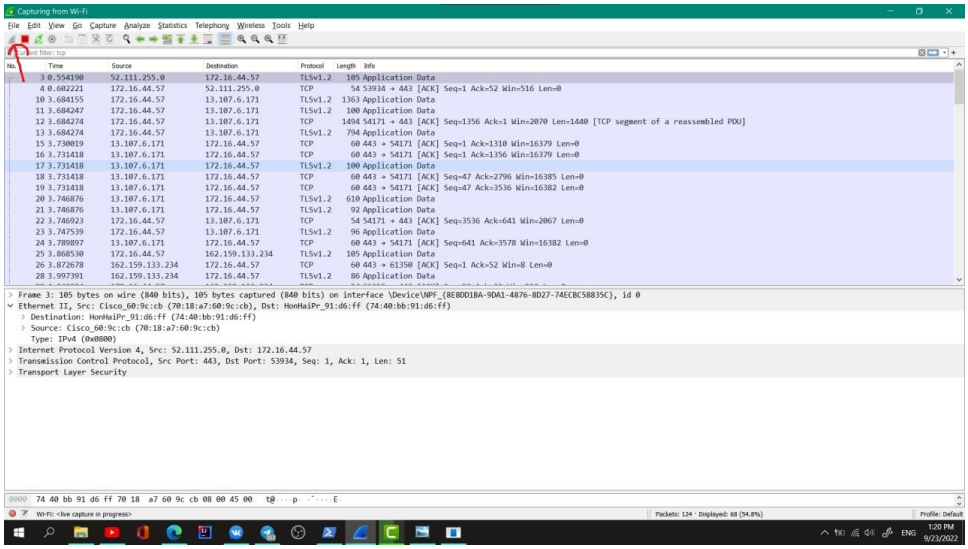
76	40	BB	91	D6	FF
1110100	1000000	10111011	10010001	10010001	11111111

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

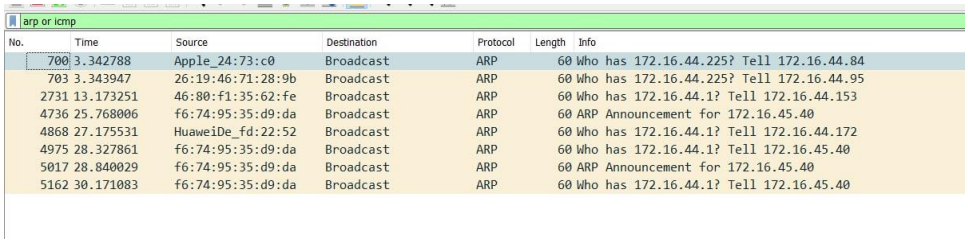
```
PS C:\Users\Administrator> ipconfig

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.

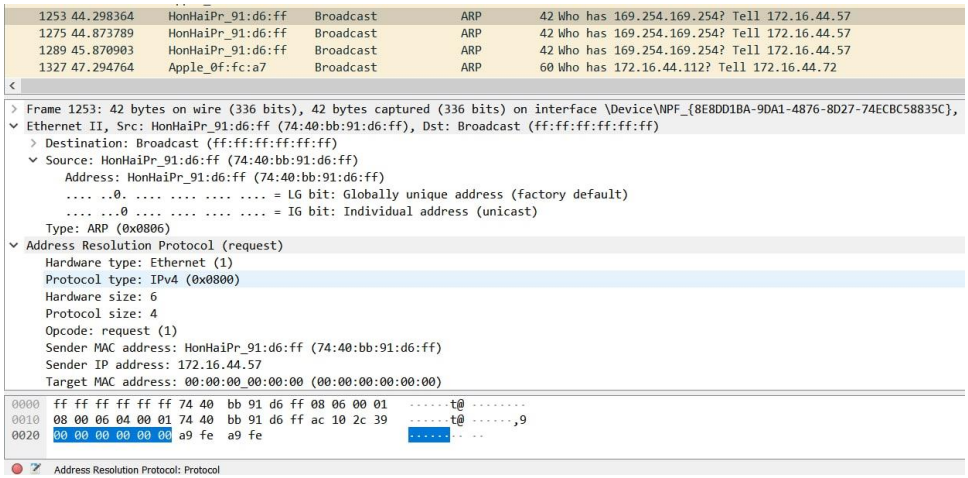
```
PS C:\Users\Administrator> ping 172.16.44.1

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.

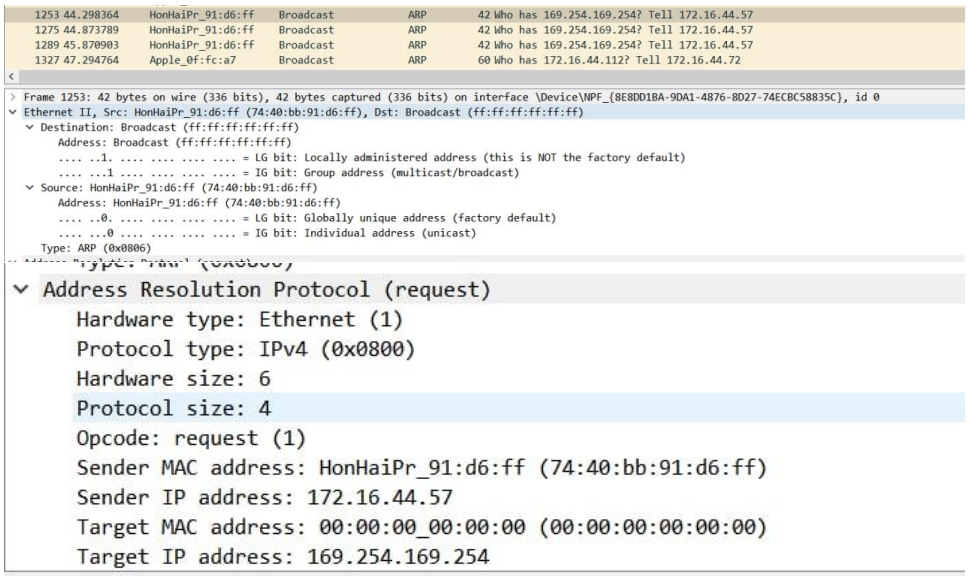


6. Остановите захват трафика в Wireshark.



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



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

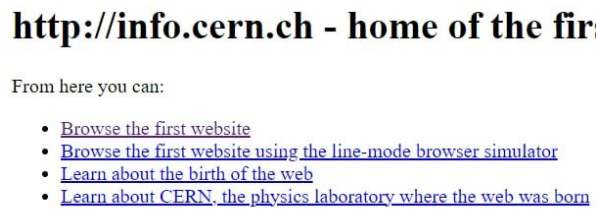
3.3.3.1. Постановка задачи

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.

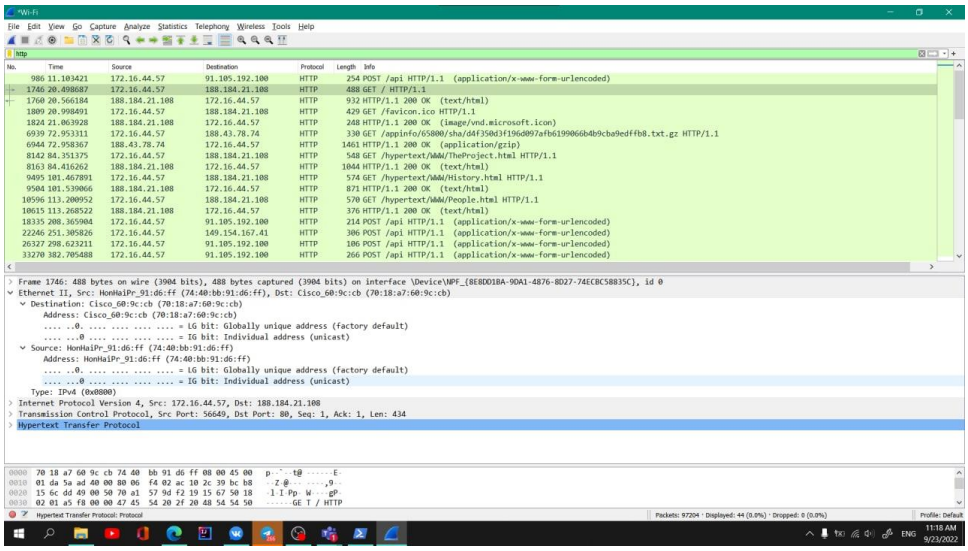


http://info.cern.ch - home of the first website

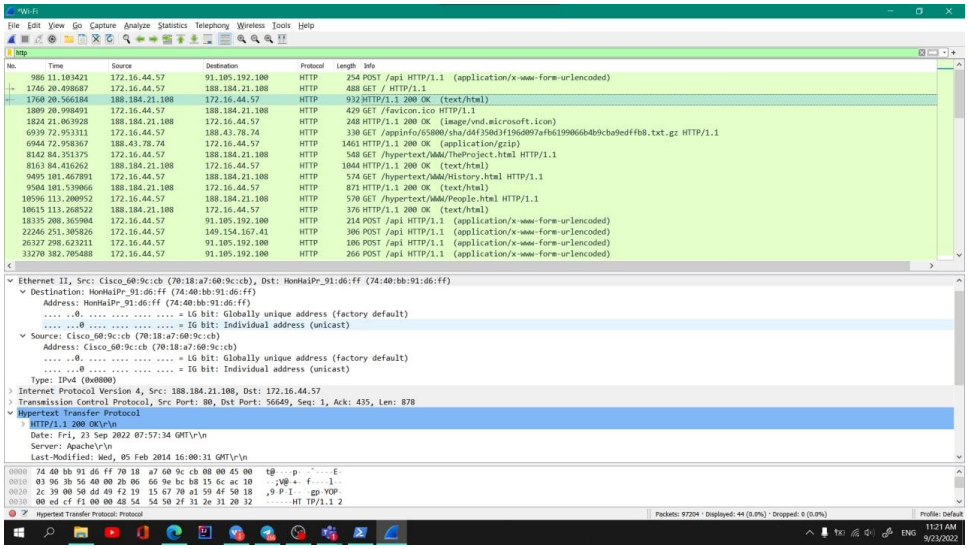
From here you can:

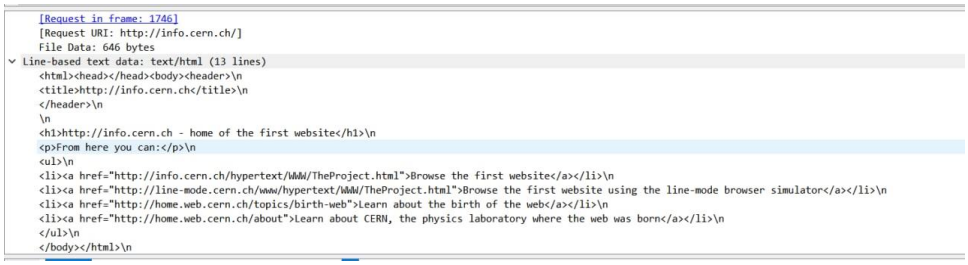
- Browse the first website
- Browse the first website using the line-mode browser simulator
- Learn about the birth of the web
- Learn about CERN, the physics laboratory where the web was born

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.

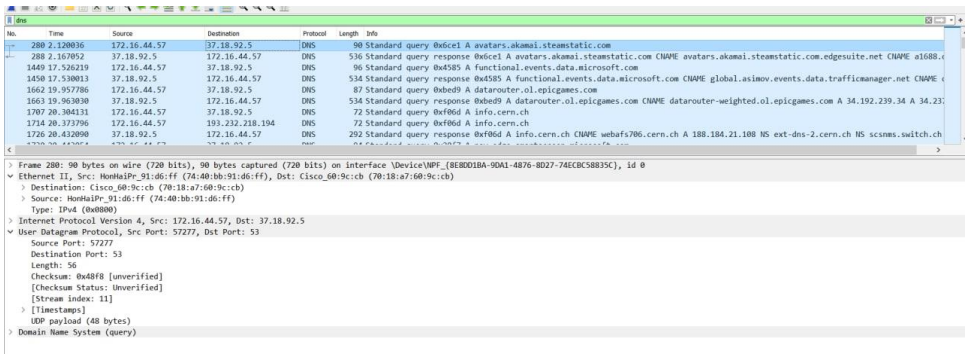


```
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 172.16.44.57, Dst: 188.184.21.108
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 474
    Identification: 0x5aad (23213)
  ▸ Flags: 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
```



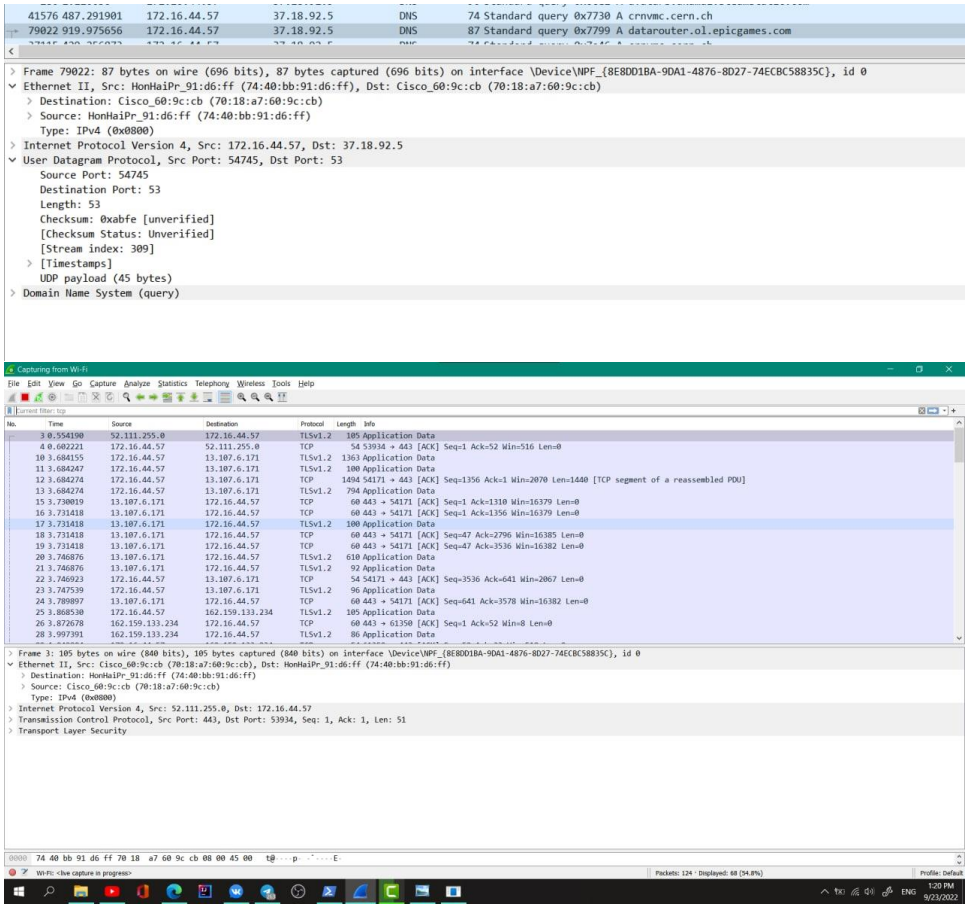


4. Wireshark в строке фильтра укажите dns и проанализируйте информацию по протоколу UDP в случае запросов и ответов. В отчёте приведите пояснение по информации, захваченной в Wireshark.



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