РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ
ПО ЛАБОРАТОРНОЙ РАБОТЕ № 3

дисциплина: Сетевые технологии

Студент: Яссин Оулед Салем

С/б: 10304121

Группа: НПИбд-02-20

МОСКВА

2022 г.

Лабораторная работа № 3. Анализ трафика в Wireshark 3.1.

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.

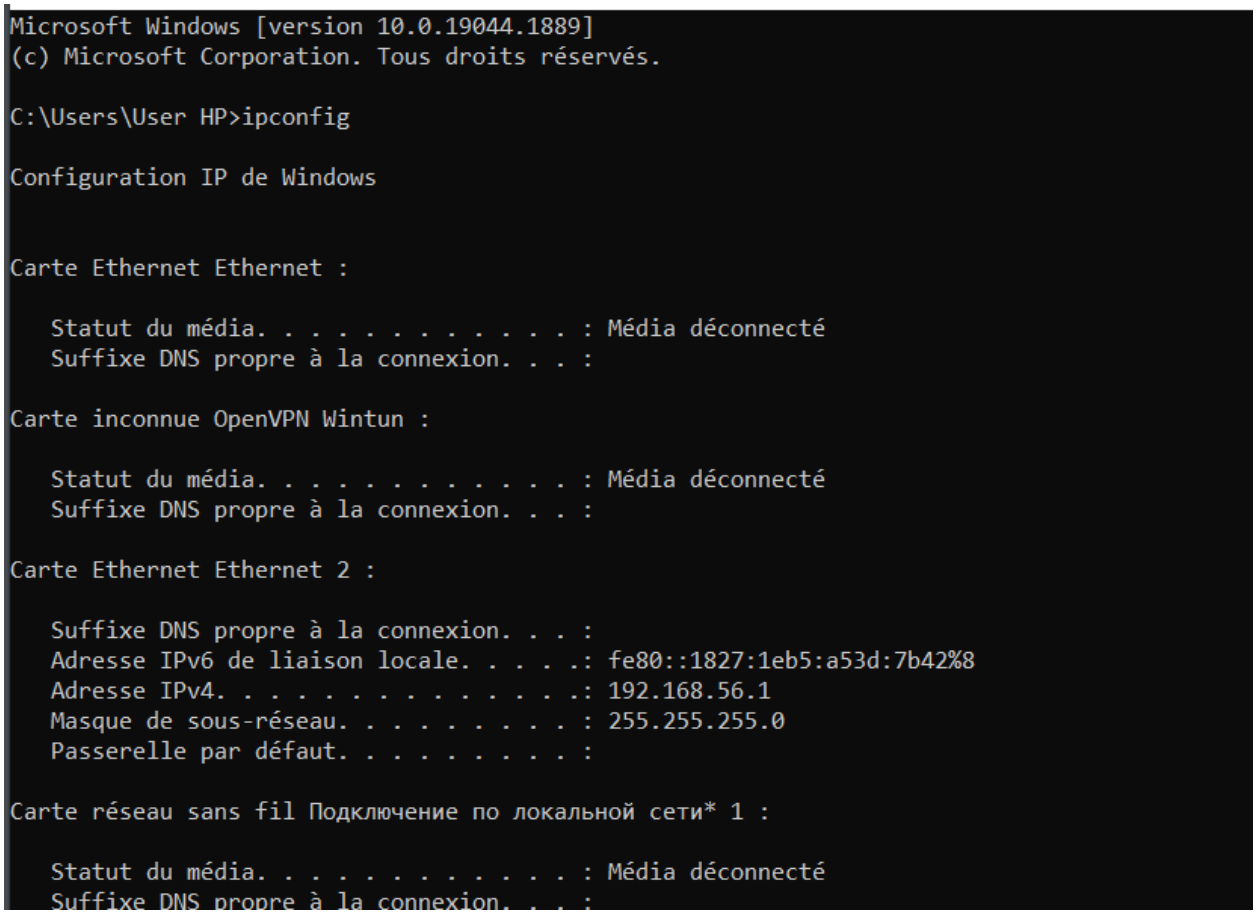


Рис 1.1

```
où
    carte             Nom de connexion
                       (caractères génériques * et ? autorisés, voir les
                        exemples)

    Options :
       /?              Affiche ce message d'aide
       /all            Affiche toutes les informations de configuration.
       /release        Libère l'adresse IPv4 pour la carte spécifiée.
       /release6       Libère l'adresse IPv6 pour la carte spécifiée.
       /renew          Renouvelle l'adresse IPv4 pour la carte spécifiée.
       /renew6         Renouvelle l'adresse IPv6 pour la carte spécifiée.
       /flushdns       Purge le cache de résolution DNS.
       /registerdns    Actualise tous les baux DHCP et réenregistre les noms
                       DNS
       /displaydns     Affiche le contenu du cache de résolution DNS.
       /showclassid    Affiche tous les ID de classe DHCP autorisés pour la
                       carte.
       /setclassid     Modifie l'ID de classe DHCP.
       /showclassid6   Affiche tous les ID de classe DHCP IPv6 autorisés pour
                       la carte.
       /setclassid6    Modifie l'ID de classe DHCP IPv6.


La valeur par défaut affiche uniquement l'adresse IP, le masque de sous-réseau
et la passerelle par défaut de chaque carte liée à TCP/IP.

Pour Release et Renew, si aucun nom de carte n'est spécifié, les baux d'adresse
IP pour toutes les cartes liées à TCP/IP sont libérés ou renouvelés.
```

Рис 1.2

На рисунке 1.3 мы использовали опцию /flushdns, которая очищает кэш сопоставителя DNS.

```
C:\Users\User HP>ipconfig /flushdns

Configuration IP de Windows

Cache de résolution DNS vidé.

C:\Users\User HP>
```

Рис1.3

2. MAC-адреса

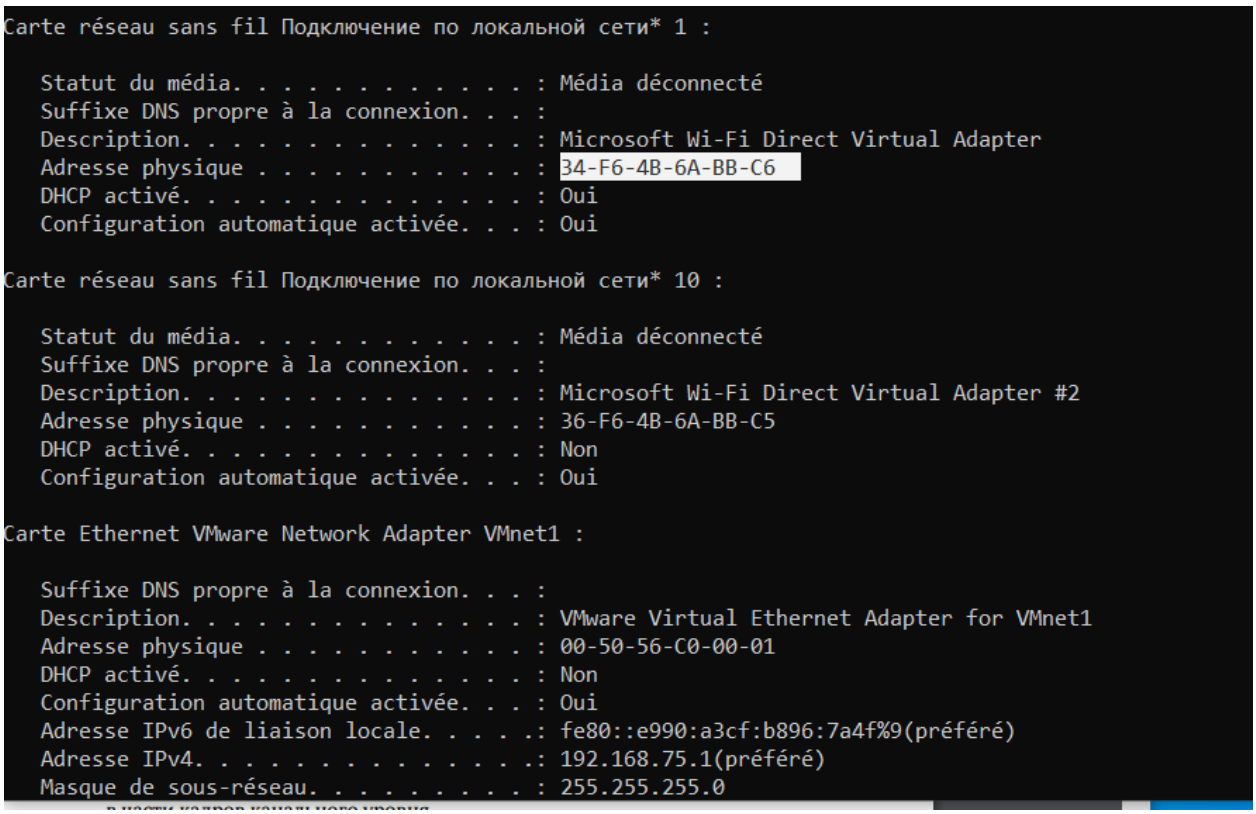


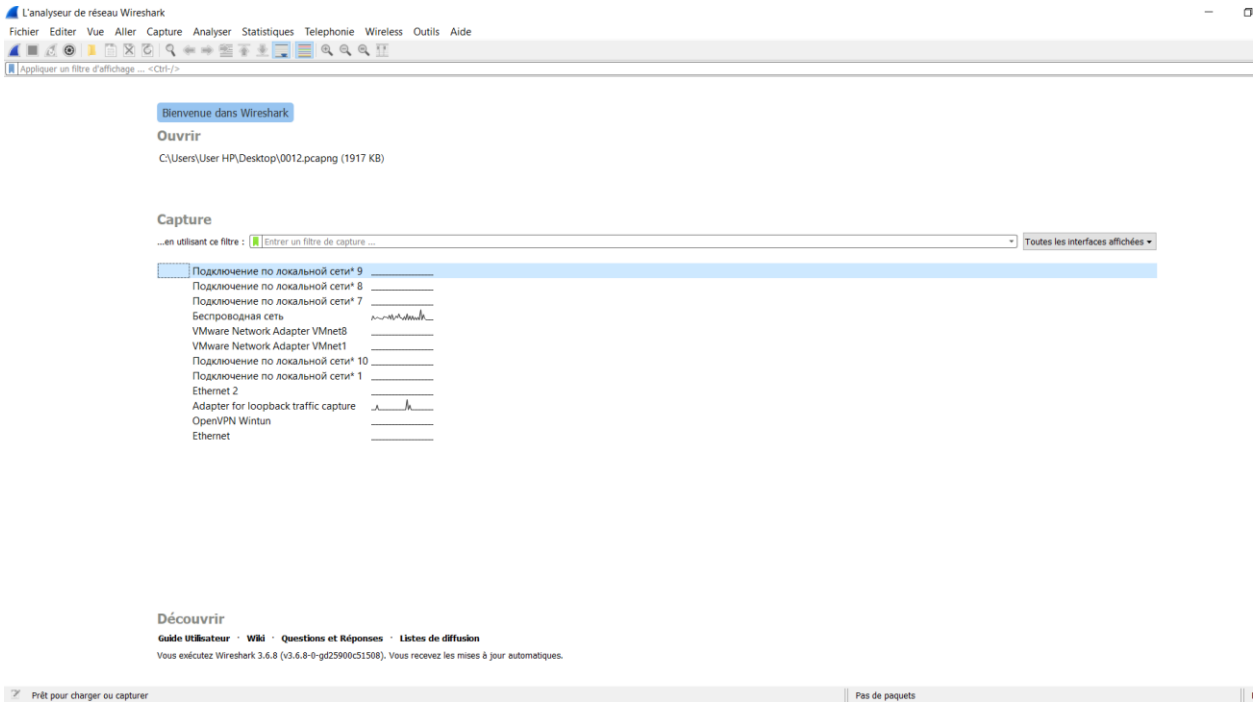
Рис 2.1

3.3.2. Анализ кадров канального уровня в Wireshark

3.3.2.1. Постановка задачи

1. Установить на домашнем устройстве Wireshark.

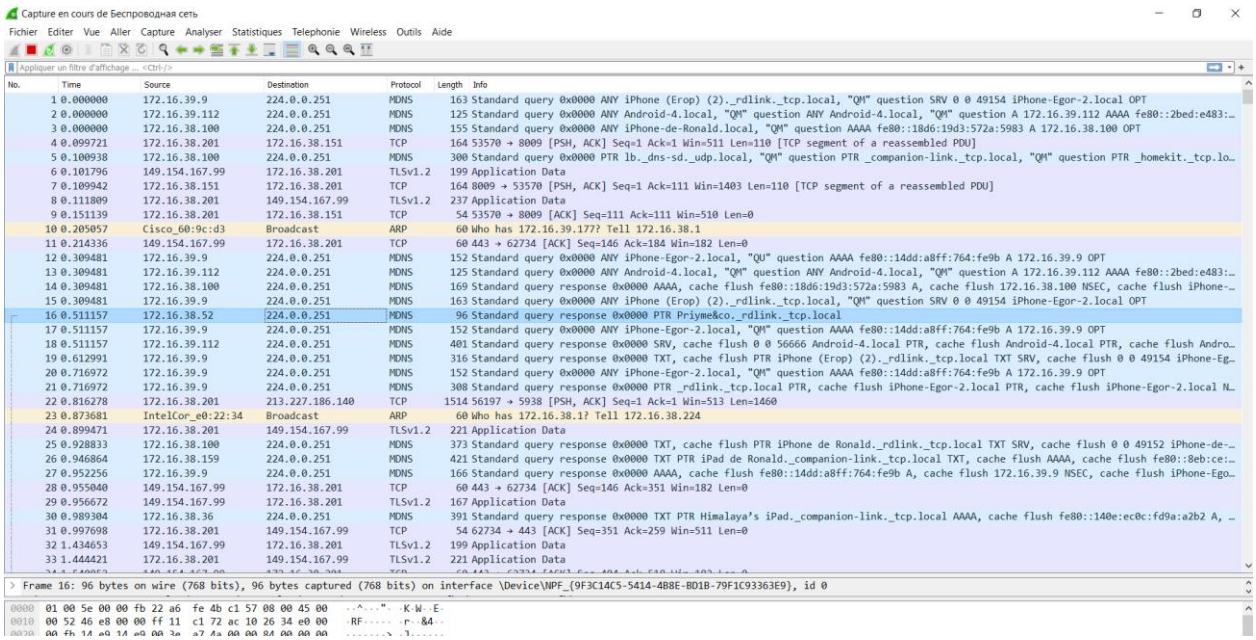
2. С помощью Wireshark захватить и проанализировать пакеты ARP и ICMP в части кадров канального уровня.



Порядок выполнения работы

1. Установите на вашем устройстве Wireshark.

2. Запустите Wireshark. Выберите активный на вашем устройстве сетевой интерфейс. Убедитесь, что начался процесс захвата трафика.



3. На вашем устройстве в консоли определите с помощью команды ipconfig для ОС типа Windows или ifconfig для систем типа Linux IP-адрес вашего устройства и шлюз по умолчанию (default gateway).

```
Carte réseau sans fil Беспроводная сеть :

   Suffixe DNS propre à la connexion. . . : rudn.ru
   Adresse IPv6 de liaison locale. . . . .: fe80::1056:32b4:1010:87d6%16
   Adresse IPv4. . . . . . . . . . . . . .: 172.16.38.201
   Masque de sous-réseau. . . . . . . . . : 255.255.254.0
   Passerelle par défaut. . . . . . . . . : 172.16.38.1

C:\Users\User HP>
```

4. На вашем устройстве в консоли с помощью команды ping адрес_шлюза пропингуйте шлюз по умолчанию. Для остановки процесса используйте комбинацию клавиш Ctrl + c или изначально при помощи параметров команды ping задайте число сообщений эхо-запроса.

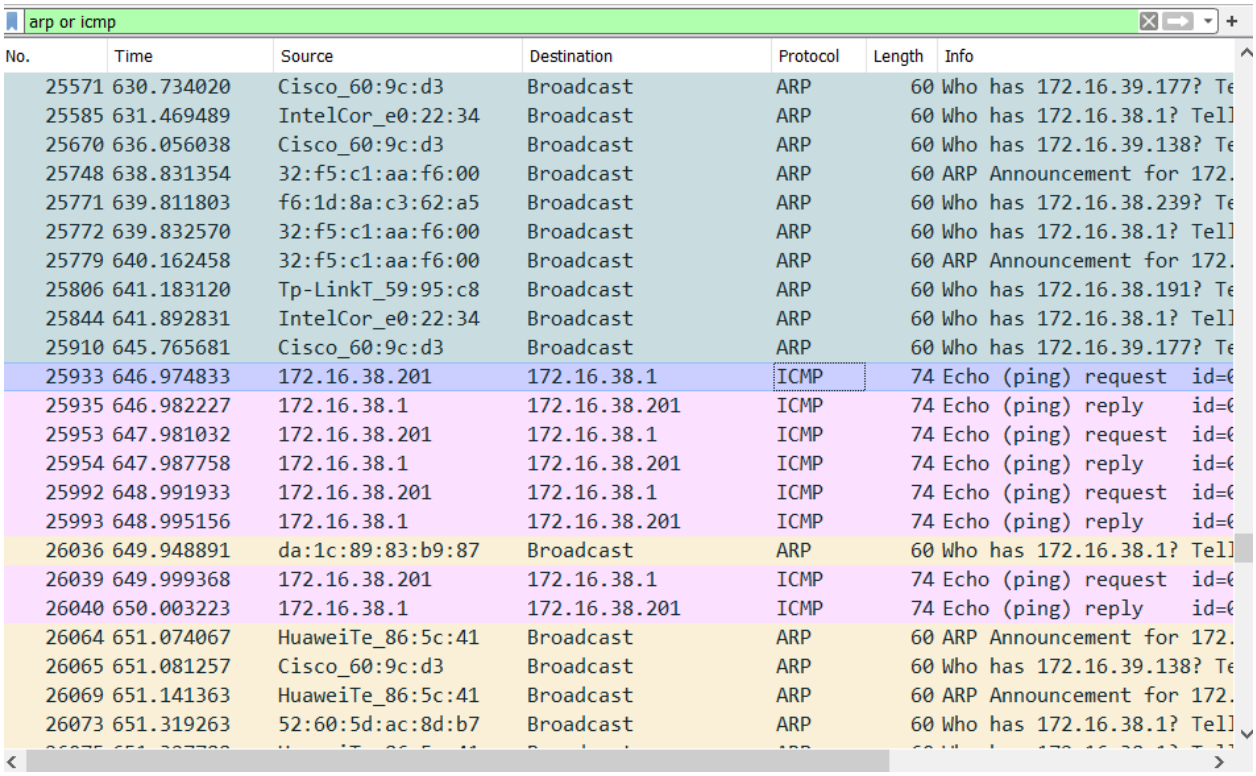
```
C:\Users\User HP>ping 172.16.38.1

Envoi d'une requête 'Ping'  172.16.38.1 avec 32 octets de données :
Réponse de 172.16.38.1 : octets=32 temps=1 ms TTL=254
Réponse de 172.16.38.1 : octets=32 temps=1 ms TTL=254
Réponse de 172.16.38.1 : octets=32 temps=4 ms TTL=254
Réponse de 172.16.38.1 : octets=32 temps=1 ms TTL=254

Statistiques Ping pour 172.16.38.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 4ms, Moyenne = 1ms

C:\Users\User HP>

C:\Users\User HP>
```

4.1

```
C:\Users\User HP>ping 172.16.38.1

Envoi d'une requête 'Ping'  172.16.38.1 avec 32 octets de données :
Réponse de 172.16.38.1 : octets=32 temps=7 ms TTL=254
Réponse de 172.16.38.1 : octets=32 temps=6 ms TTL=254
Réponse de 172.16.38.1 : octets=32 temps=3 ms TTL=254
Réponse de 172.16.38.1 : octets=32 temps=3 ms TTL=254

Statistiques Ping pour 172.16.38.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 3ms, Maximum = 7ms, Moyenne = 4ms

C:\Users\User HP>
```

4.1.1

5. В Wireshark остановите захват трафика. В строке фильтра пропишите фильтр arp or icmp. Убедитесь, что в списке пакетов отобразятся только пакеты ARP или ICMP, в частности пакеты, которые были сгенерированы с помощью команды ping, отправленной с вашего устройства на шлюз по умолчанию.



arp or icmp

No.	Time	Source	Destination	Protocol	Length	Info
25571	630.734020	Cisco_60:9c:d3	Broadcast	ARP	60	Who has 172.16.39.177? Te
25585	631.469489	IntelCor_e0:22:34	Broadcast	ARP	60	Who has 172.16.38.1? Tell
25670	636.056038	Cisco_60:9c:d3	Broadcast	ARP	60	Who has 172.16.39.138? Te
25748	638.831354	32:f5:c1:aa:f6:00	Broadcast	ARP	60	ARP Announcement for 172.
25771	639.811803	f6:1d:8a:c3:62:a5	Broadcast	ARP	60	Who has 172.16.38.239? Te
25772	639.832570	32:f5:c1:aa:f6:00	Broadcast	ARP	60	Who has 172.16.38.1? Tell
25779	640.162458	32:f5:c1:aa:f6:00	Broadcast	ARP	60	ARP Announcement for 172.
25806	641.183120	Tp-LinkT_59:95:c8	Broadcast	ARP	60	Who has 172.16.38.191? Te
25844	641.892831	IntelCor_e0:22:34	Broadcast	ARP	60	Who has 172.16.38.1? Tell
25910	645.765681	Cisco_60:9c:d3	Broadcast	ARP	60	Who has 172.16.39.177? Te
25933	646.974833	172.16.38.201	172.16.38.1	ICMP	74	Echo (ping) request id=0
25935	646.982227	172.16.38.1	172.16.38.201	ICMP	74	Echo (ping) reply id=0
25953	647.981032	172.16.38.201	172.16.38.1	ICMP	74	Echo (ping) request id=0
25954	647.987758	172.16.38.1	172.16.38.201	ICMP	74	Echo (ping) reply id=0
25992	648.991933	172.16.38.201	172.16.38.1	ICMP	74	Echo (ping) request id=0
25993	648.995156	172.16.38.1	172.16.38.201	ICMP	74	Echo (ping) reply id=0
26036	649.948891	da:1c:89:83:b9:87	Broadcast	ARP	60	Who has 172.16.38.1? Tell
26039	649.999368	172.16.38.201	172.16.38.1	ICMP	74	Echo (ping) request id=0
26040	650.003223	172.16.38.1	172.16.38.201	ICMP	74	Echo (ping) reply id=0
26064	651.074067	HuaweiTe_86:5c:41	Broadcast	ARP	60	ARP Announcement for 172.
26065	651.081257	Cisco_60:9c:d3	Broadcast	ARP	60	Who has 172.16.39.138? Te
26069	651.141363	HuaweiTe_86:5c:41	Broadcast	ARP	60	ARP Announcement for 172.
26073	651.319263	52:60:5d:ac:8d:b7	Broadcast	ARP	60	Who has 172.16.38.1? Tell

6. Изучите эхо-запрос и эхо-ответ ICMP в программе Wireshark:

– На панели списка пакетов (верхний раздел) выберите первый указанный кадр ICMP — эхо-запрос. Изучите информацию на панели сведений о пакете в средней части экрана. В отчёте укажите длину кадра, к какому типу Ethernet относится кадр, определите MAC-адреса источника и шлюза, определите тип MAC-адресов.

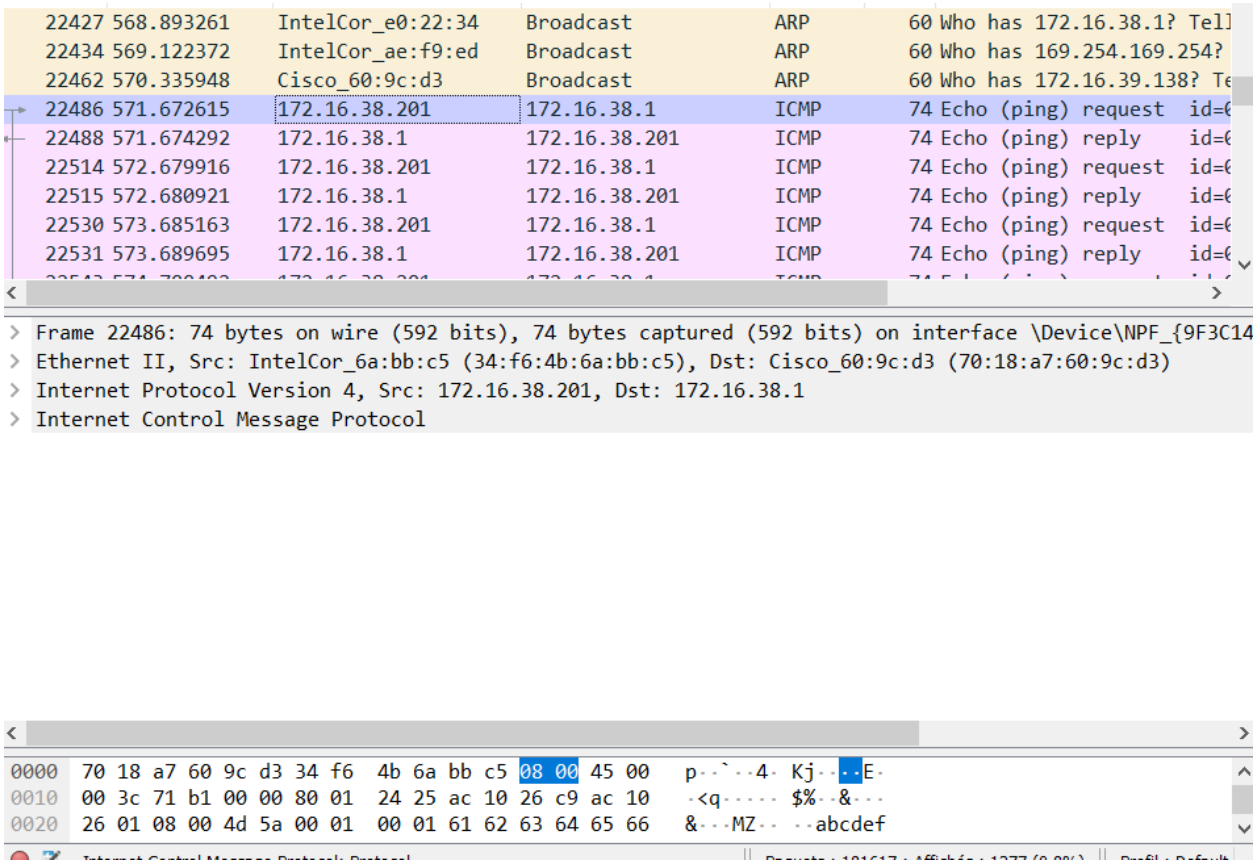


Рис.6.1

Frame 22486: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{9F3C14C5-5414-4B8E-BD1B-79F1C93363E9}, id 0

Interface id: 0 (\Device\NPF_{9F3C14C5-5414-4B8E-BD1B-79F1C93363E9})

Encapsulation type: Ethernet (1)

Arrival Time: Sep 24, 2022 12:00:39.424554000 Russie TZ 2

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1664010039.424554000 seconds

[Time delta from previous captured frame: 0.038635000 seconds]

[Time delta from previous displayed frame: 1.336667000 seconds]

[Time since reference or first frame: 571.672615000 seconds]

Frame Number: 22486

Frame Length: 74 bytes (592 bits)

Capture Length: 74 bytes (592 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:icmp:data]

[Coloring Rule Name: ICMP]

[Coloring Rule String: icmp || icmpv6]

Ethernet II, Src: IntelCor_6a:bb:c5 (34:f6:4b:6a:bb:c5), Dst: Cisco_60:9c:d3 (70:18:a7:60:9c:d3)

Destination: Cisco_60:9c:d3 (70:18:a7:60:9c:d3)

Source: IntelCor_6a:bb:c5 (34:f6:4b:6a:bb:c5)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 172.16.38.201, Dst: 172.16.38.1

Internet Control Message Protocol

– На панели списка пакетов (верхний раздел) выберите второй указанный кадр ICMP — эхо-ответ. Изучите информацию на панели сведений о пакете в средней части экрана. В отчёте укажите длину кадра, к какому типу Ethernet относится кадр, определите MAC-адреса источника и шлюза, определите тип MAC-адресов.

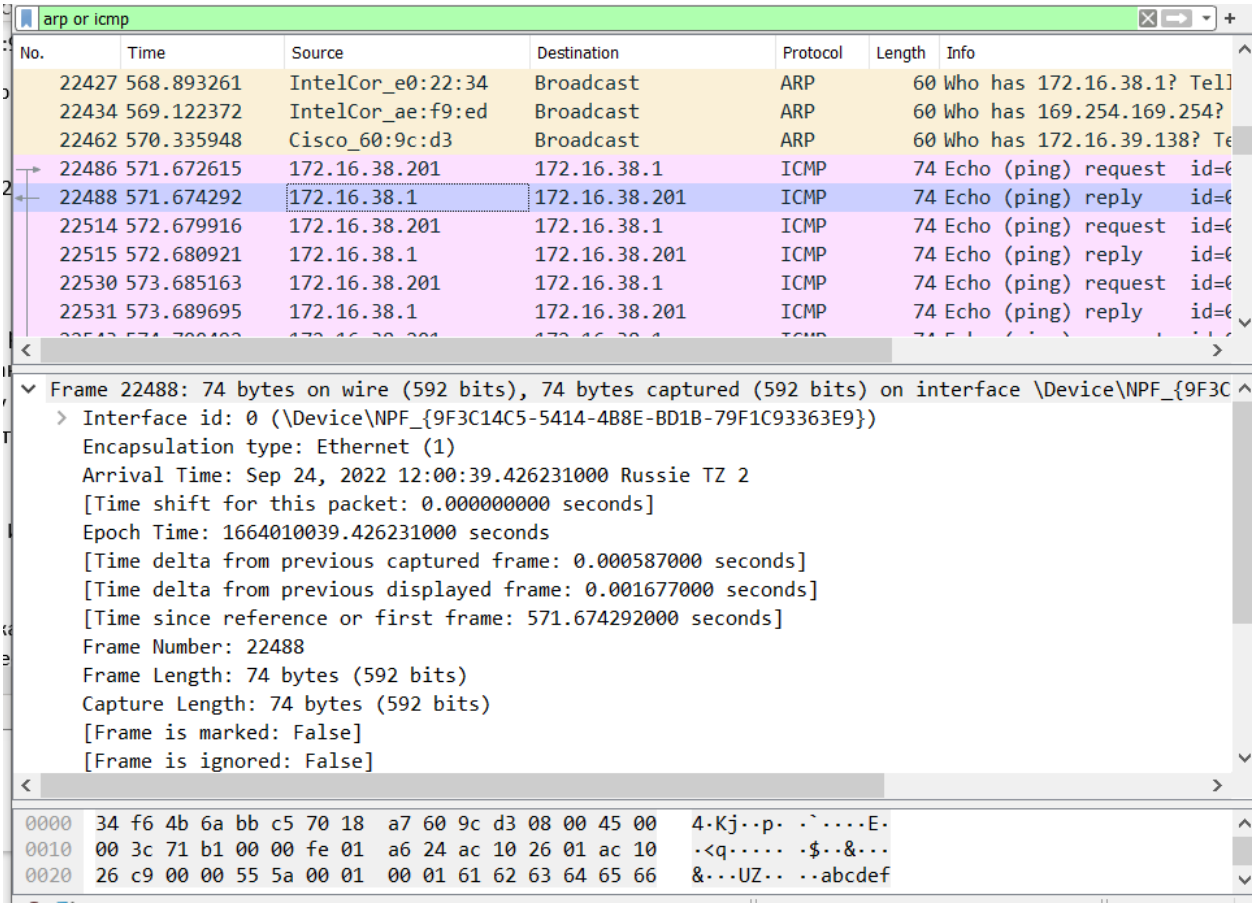


Рис 6.2

Ethernet II, Src: Cisco_60:9c:d3 (70:18:a7:60:9c:d3), Dst: IntelCor_6a:bb:c5 (34:f6:4b:6a:bb:c5)

Destination: IntelCor_6a:bb:c5 (34:f6:4b:6a:bb:c5)

Source: Cisco_60:9c:d3 (70:18:a7:60:9c:d3)

Type: IPv4 (0x0800)

7. Изучите кадры данных протокола ARP. Изучите данные в полях заголовка Ethernet II.

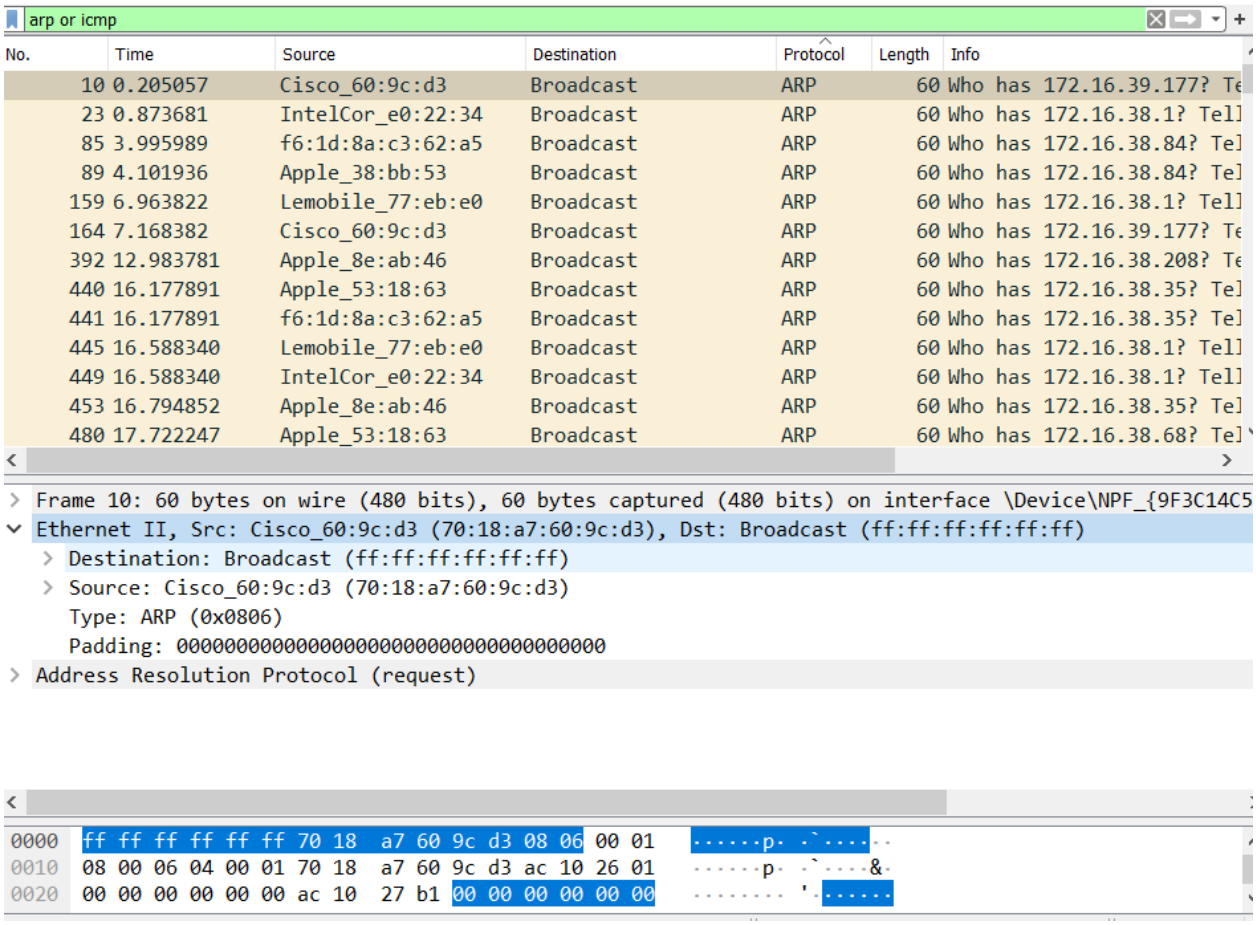


Рис 7.1

Ethernet II, Src: Cisco_60:9c:d3 (70:18:a7:60:9c:d3), 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: Cisco_60:9c:d3 (70:18:a7:60:9c:d3)

Address: Cisco_60:9c:d3 (70:18:a7:60:9c:d3)

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

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

Type: ARP (0x0806)

Padding: 000000000000000000000000000000000000

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.

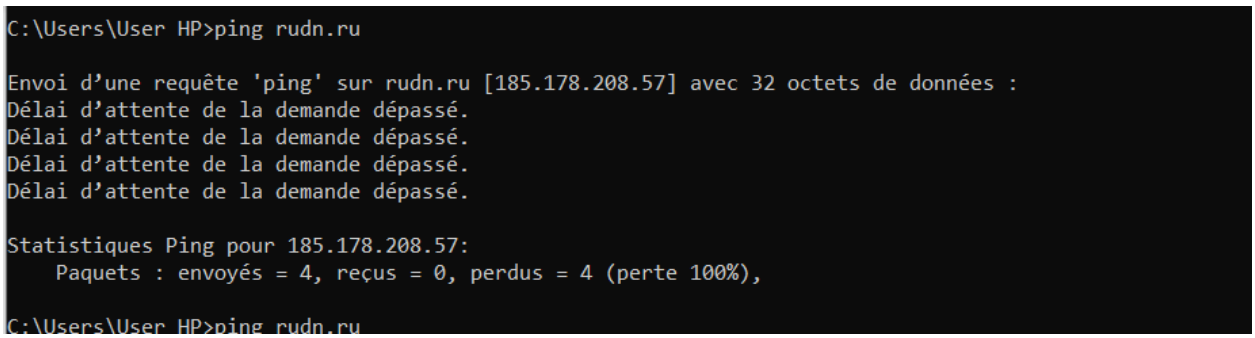


Рис8.1

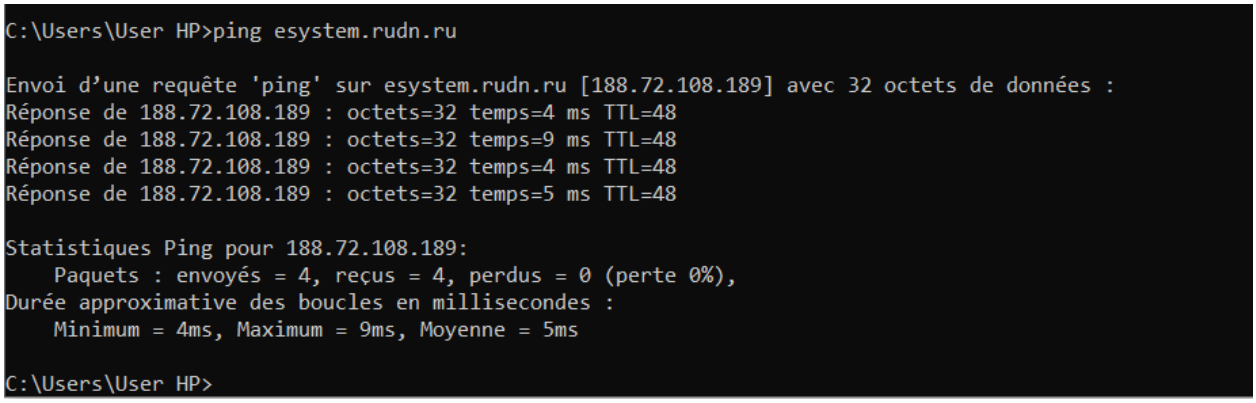


Рис 8.2

Анализ протоколов транспортного уровня в Wireshark

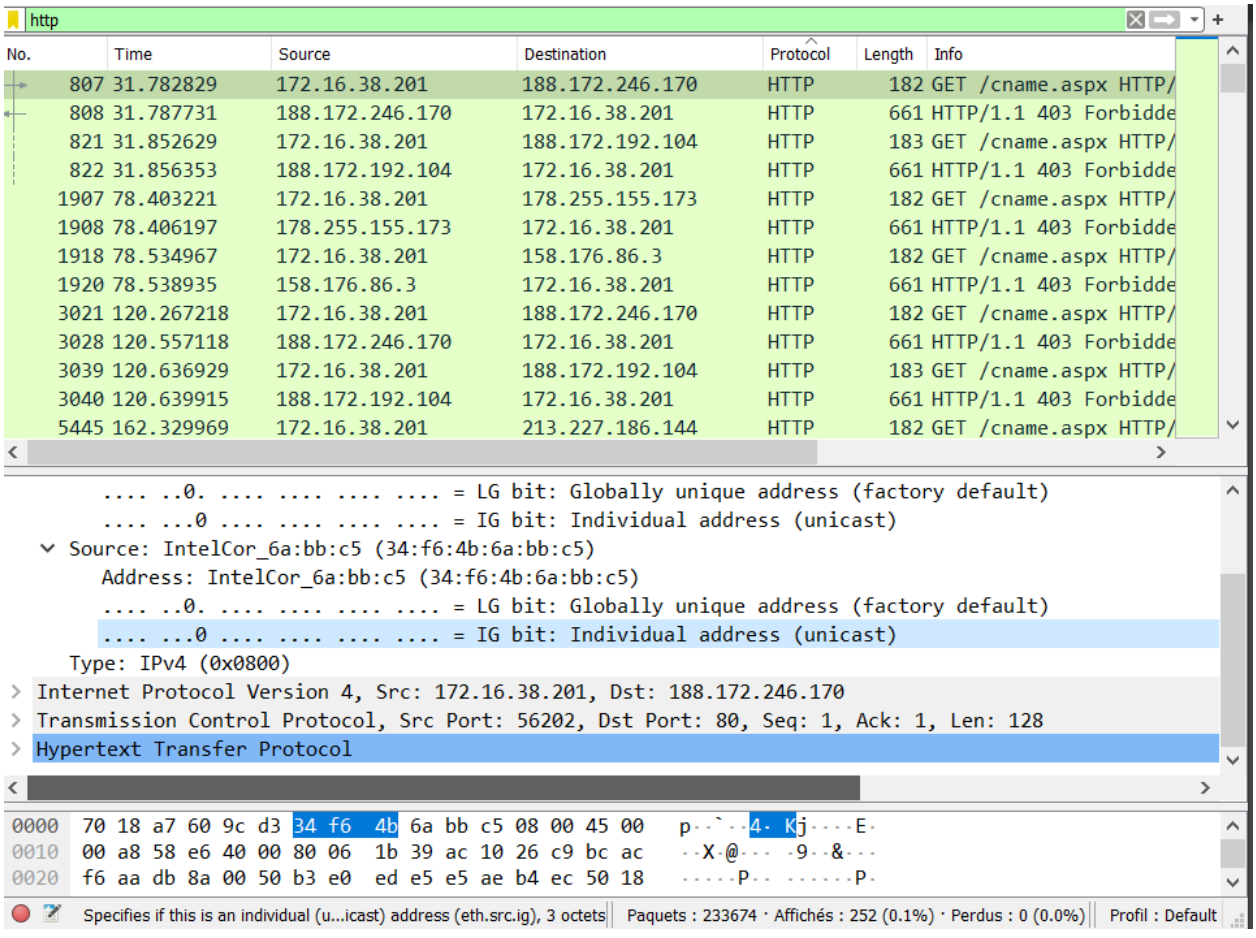
Постановка задачи С помощью Wireshark захватить и проанализировать пакеты HTTP, DNS в части заголовков и информации протоколов TCP, UDP, QUIC.

Порядок выполнения работы

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.

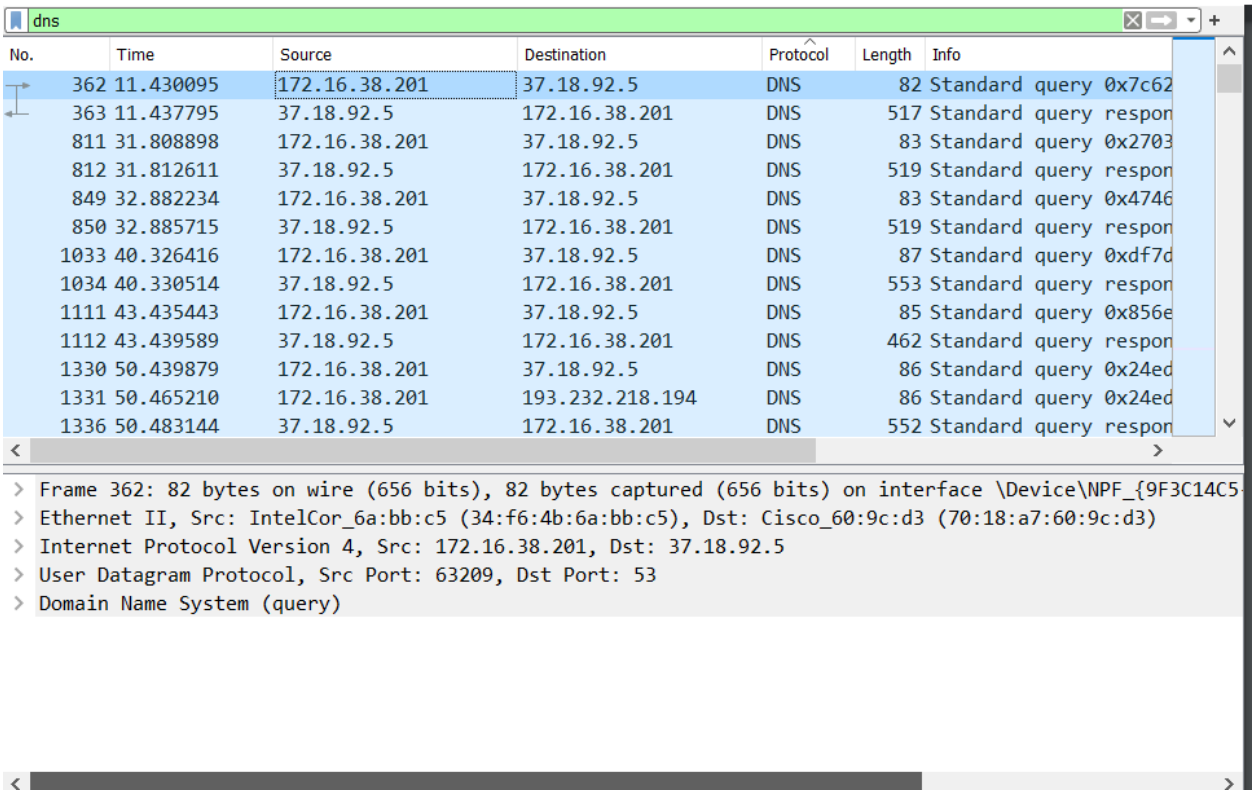
3. В Wireshark в строке фильтра укажите http и проанализируйте информацию по протоколу TCP в случае запросов и ответов. В отчёте приведите пояснение по информации, захваченной в Wireshark.



TCP payload (128 bytes)

```
> Flags: 0x40, Don't Fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0x1b39 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 172.16.38.201
  Destination Address: 188.172.246.170
Transmission Control Protocol, Src Port: 56202, Dst Port: 80, Seq: 1, Ack: 1, Len: 128
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.



4.1

Frame 1331: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{9F3C14C5-5414-4B8E-BD1B-79F1C93363E9}, id 0

Interface id: 0 (\Device\NPF_{9F3C14C5-5414-4B8E-BD1B-79F1C93363E9})

Encapsulation type: Ethernet (1)

Arrival Time: Sep 24, 2022 11:51:58.217149000 Russie TZ 2

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1664009518.217149000 seconds

[Time delta from previous captured frame: 0.025331000 seconds]

[Time delta from previous displayed frame: 0.025331000 seconds]

[Time since reference or first frame: 50.465210000 seconds]

Frame Number: 1331

Frame Length: 86 bytes (688 bits)

Capture Length: 86 bytes (688 bits)

[Frame is marked: False]

[Frame is ignored: False]

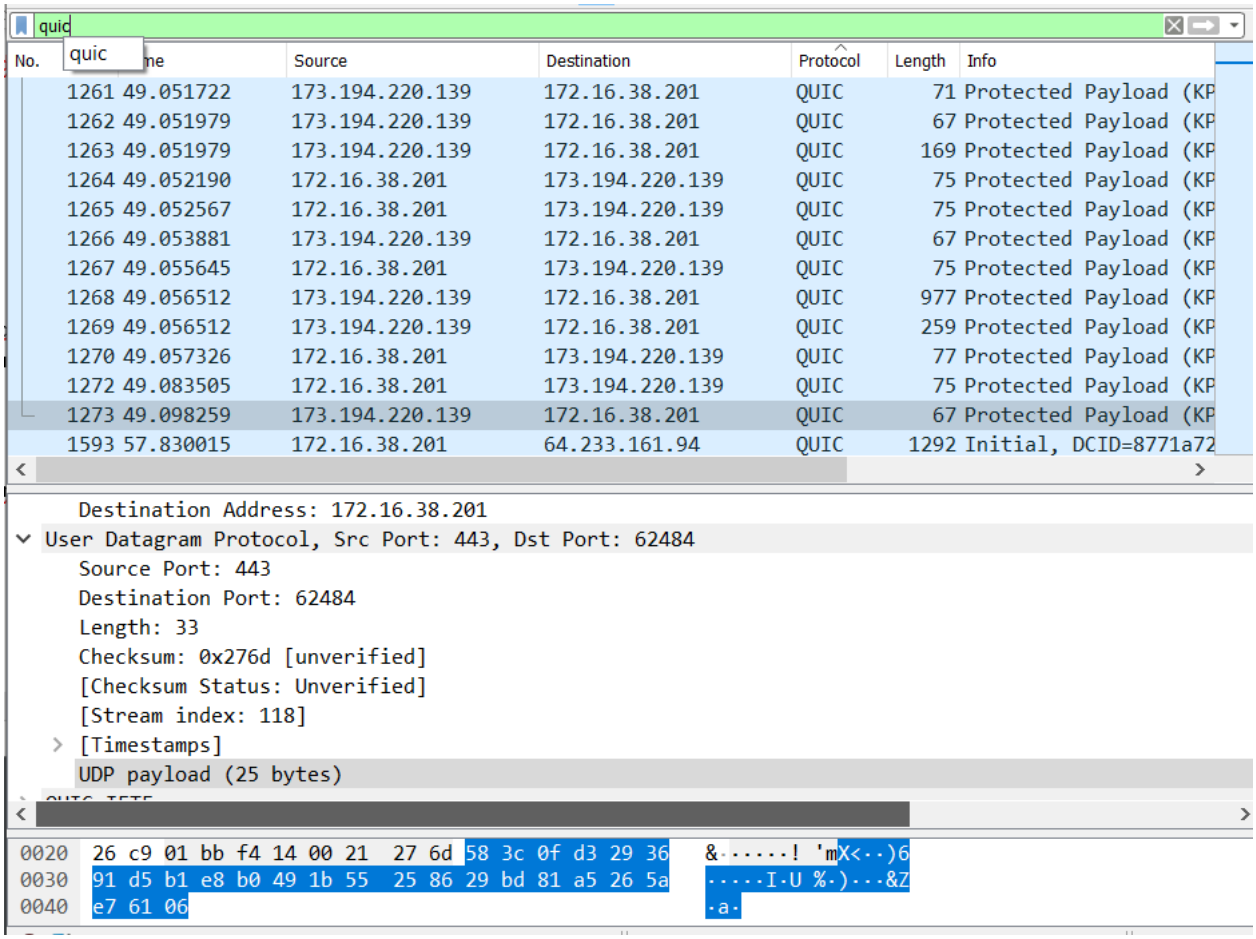
[Protocols in frame: eth:ethertype:ip:udp:dns]

[Coloring Rule Name: UDP]

[Coloring Rule String: udp]

UDP payload (44 bytes)

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.



Frame 1273: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{9F3C14C5-5414-4B8E-BD1B-79F1C93363E9}, id 0

Ethernet II, Src: Cisco_60:9c:d3 (70:18:a7:60:9c:d3), Dst: IntelCor_6a:bb:c5 (34:f6:4b:6a:bb:c5)

Internet Protocol Version 4, Src: 173.194.220.139, Dst: 172.16.38.201

0100 .... = Version: 4

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

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

Total Length: 53

Identification: 0x0000 (0)

Flags: 0x40, Don't fragment

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

Time to Live: 60

Protocol: UDP (17)

Header Checksum: 0xe190 [validation disabled]

[Header checksum status: Unverified]

Source Address: 173.194.220.139

Destination Address: 172.16.38.201

User Datagram Protocol, Src Port: 443, Dst Port: 62484

Source Port: 443

Destination Port: 62484

Length: 33

Checksum: 0x276d [unverified]

[Checksum Status: Unverified]

[Stream index: 118]

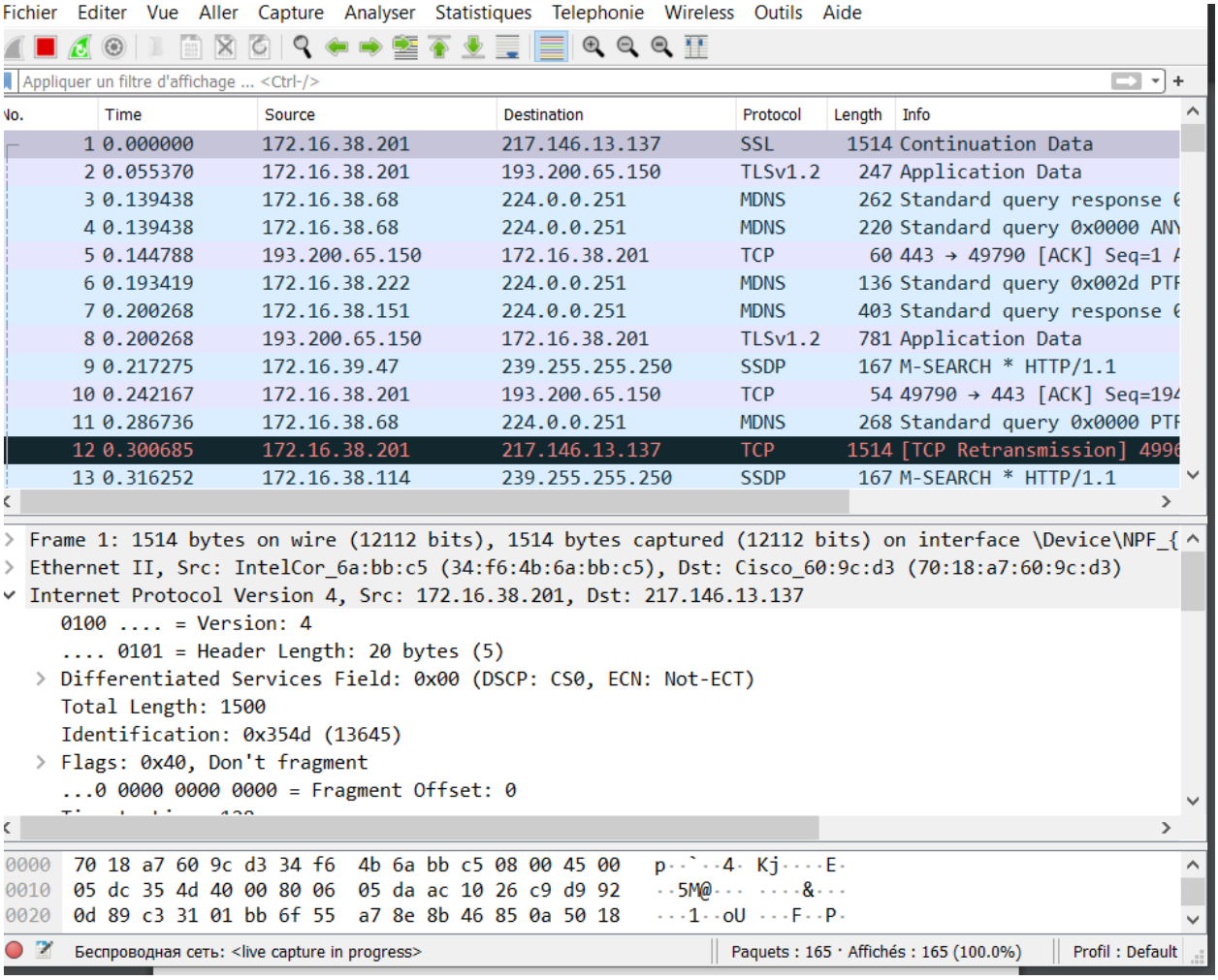
[Timestamps]

UDP payload (25 bytes)

QUIC IETF

6. Остановите захват трафика в Wireshark.

6.



6.1

Вывод

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