

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.

```
Microsoft Windows [version 10.0.19044.1889]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\User HP>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet :

    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :

Carte inconnue OpenVPN Wintun :

    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :

Carte Ethernet Ethernet 2 :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::1827:1eb5:a53d:7b42%8
    Adresse IPv4. . . . . : 192.168.56.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :

Carte réseau sans fil Подключение по локальной сети* 1 :

    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :
```

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

```

Carte réseau sans fil Подключение по локальной сети* 1 :

Statut du média. . . . . : Média déconnecté
Suffixe DNS propre à la connexion. . . :
Description. . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Adresse physique . . . . . : 34-F6-4B-6A-BB-C6
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui

Carte réseau sans fil Подключение по локальной сети* 10 :

Statut du média. . . . . : Média déconnecté
Suffixe DNS propre à la connexion. . . :
Description. . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Adresse physique . . . . . : 36-F6-4B-6A-BB-C5
DHCP activé. . . . . : Non
Configuration automatique activée. . . : Oui

Carte Ethernet VMware Network Adapter VMnet1 :

Suffixe DNS propre à la connexion. . . :
Description. . . . . : VMware Virtual Ethernet Adapter for VMnet1
Adresse physique . . . . . : 00-50-56-C0-00-01
DHCP activé. . . . . : Non
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::e990:a3cf:b896:7a4f%9(préféré)
Adresse IPv4. . . . . : 192.168.75.1(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0

```

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.

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 пропикуйте 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? Te11
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? Te11
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? Te11
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=6
25935	646.982227	172.16.38.1	172.16.38.201	ICMP	74	Echo (ping) reply id=6
25953	647.981032	172.16.38.201	172.16.38.1	ICMP	74	Echo (ping) request id=6
25954	647.987758	172.16.38.1	172.16.38.201	ICMP	74	Echo (ping) reply id=6
25992	648.991933	172.16.38.201	172.16.38.1	ICMP	74	Echo (ping) request id=6
25993	648.995156	172.16.38.1	172.16.38.201	ICMP	74	Echo (ping) reply id=6
26036	649.948891	da:1c:89:83:b9:87	Broadcast	ARP	60	Who has 172.16.38.1? Te11
26039	649.999368	172.16.38.201	172.16.38.1	ICMP	74	Echo (ping) request id=6
26040	650.003223	172.16.38.1	172.16.38.201	ICMP	74	Echo (ping) reply id=6
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? Te11

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.

22427	568.893261	IntelCor_e0:22:34	Broadcast	ARP	60	Who has 172.16.38.1? Tell
22434	569.122372	IntelCor_ae:f9:ed	Broadcast	ARP	60	Who has 169.254.169.254? Te
22462	570.335948	Cisco_60:9c:d3	Broadcast	ARP	60	Who has 172.16.39.138? Te
22486	571.672615	172.16.38.201	172.16.38.1	ICMP	74	Echo (ping) request id=0
22488	571.674292	172.16.38.1	172.16.38.201	ICMP	74	Echo (ping) reply id=0
22514	572.679916	172.16.38.201	172.16.38.1	ICMP	74	Echo (ping) request id=0
22515	572.680921	172.16.38.1	172.16.38.201	ICMP	74	Echo (ping) reply id=0
22530	573.685163	172.16.38.201	172.16.38.1	ICMP	74	Echo (ping) request id=0
22531	573.689695	172.16.38.1	172.16.38.201	ICMP	74	Echo (ping) reply id=0

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

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

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

> Internet Control Message Protocol

0000	70 18 a7 60 9c d3 34 f6 4b 6a bb c5 08 00 45 00	p 4 . Kj E .
0010	00 3c 71 b1 00 00 80 01 24 25 ac 10 26 c9 ac 10	- < q \$ % . . & . . .
0020	26 01 08 00 4d 5a 00 01 00 01 61 62 63 64 65 66	& . . . MZ abcdef

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.

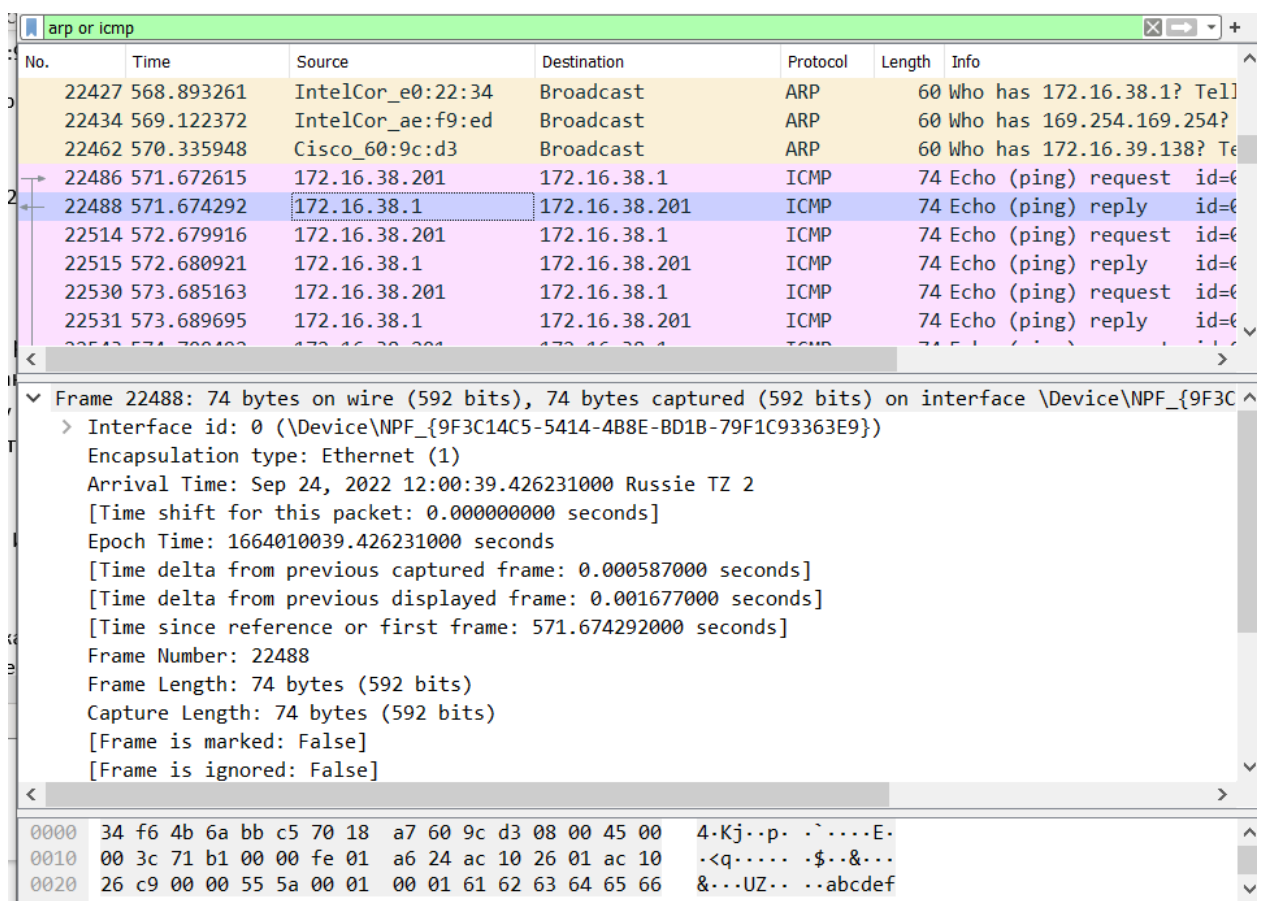


Рис 6.2

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.

No.	Time	Source	Destination	Protocol	Length	Info
10	0.205057	Cisco_60:9c:d3	Broadcast	ARP	60	Who has 172.16.39.177? Tel
23	0.873681	IntelCor_e0:22:34	Broadcast	ARP	60	Who has 172.16.38.1? Tel
85	3.995989	f6:1d:8a:c3:62:a5	Broadcast	ARP	60	Who has 172.16.38.84? Tel
89	4.101936	Apple_38:bb:53	Broadcast	ARP	60	Who has 172.16.38.84? Tel
159	6.963822	Lemobile_77:eb:e0	Broadcast	ARP	60	Who has 172.16.38.1? Tel
164	7.168382	Cisco_60:9c:d3	Broadcast	ARP	60	Who has 172.16.39.177? Tel
392	12.983781	Apple_8e:ab:46	Broadcast	ARP	60	Who has 172.16.38.208? Tel
440	16.177891	Apple_53:18:63	Broadcast	ARP	60	Who has 172.16.38.35? Tel
441	16.177891	f6:1d:8a:c3:62:a5	Broadcast	ARP	60	Who has 172.16.38.35? Tel
445	16.588340	Lemobile_77:eb:e0	Broadcast	ARP	60	Who has 172.16.38.1? Tel
449	16.588340	IntelCor_e0:22:34	Broadcast	ARP	60	Who has 172.16.38.1? Tel
453	16.794852	Apple_8e:ab:46	Broadcast	ARP	60	Who has 172.16.38.35? Tel
480	17.722247	Apple_53:18:63	Broadcast	ARP	60	Who has 172.16.38.68? Tel

< >

> Frame 10: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{9F3C14C5}

✓ 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)

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

Type: ARP (0x0806)

Padding: 00000000000000000000000000000000

> Address Resolution Protocol (request)

< >

0000	ff ff ff ff ff ff 70 18	a7 60 9c d3 08 06	00 01p.
0010	08 00 06 04 00 01 70 18	a7 60 9c d3 ac 10 26 01	p.&
0020	00 00 00 00 00 00 ac 10	27 b1 00 00 00 00 00 00	 '

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: 0000000000000000000000000000000000

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

```
C:\Users\User HP>ping rudn.ru

Envoi d'une requête 'ping' sur rudn.ru [185.178.208.57] avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 185.178.208.57:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),

C:\Users\User HP>ping rudn.ru
```

Рис8.1

```
C:\Users\User HP>ping esystem.rudn.ru

Envoi d'une requête 'ping' sur esystem.rudn.ru [188.72.108.189] avec 32 octets de données :
Réponse de 188.72.108.189 : octets=32 temps=4 ms TTL=48
Réponse de 188.72.108.189 : octets=32 temps=9 ms TTL=48
Réponse de 188.72.108.189 : octets=32 temps=4 ms TTL=48
Réponse de 188.72.108.189 : octets=32 temps=5 ms TTL=48

Statistiques Ping pour 188.72.108.189:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 4ms, Maximum = 9ms, Moyenne = 5ms

C:\Users\User HP>
```

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.

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.

Wireshark capture of HTTP traffic. The packet list shows a GET request for /cname.aspx. The packet details pane shows the source IP address 172.16.38.201, which is highlighted in blue. The packet bytes pane shows the raw data of the packet, with the source IP address 172.16.38.201 highlighted in blue.

No.	Time	Source	Destination	Protocol	Length	Info
807	31.782829	172.16.38.201	188.172.246.170	HTTP	182	GET /cname.aspx HTTP/
808	31.787731	188.172.246.170	172.16.38.201	HTTP	661	HTTP/1.1 403 Forbidde
821	31.852629	172.16.38.201	188.172.192.104	HTTP	183	GET /cname.aspx HTTP/
822	31.856353	188.172.192.104	172.16.38.201	HTTP	661	HTTP/1.1 403 Forbidde
1907	78.403221	172.16.38.201	178.255.155.173	HTTP	182	GET /cname.aspx HTTP/
1908	78.406197	178.255.155.173	172.16.38.201	HTTP	661	HTTP/1.1 403 Forbidde
1918	78.534967	172.16.38.201	158.176.86.3	HTTP	182	GET /cname.aspx HTTP/
1920	78.538935	158.176.86.3	172.16.38.201	HTTP	661	HTTP/1.1 403 Forbidde
3021	120.267218	172.16.38.201	188.172.246.170	HTTP	182	GET /cname.aspx HTTP/
3028	120.557118	188.172.246.170	172.16.38.201	HTTP	661	HTTP/1.1 403 Forbidde
3039	120.636929	172.16.38.201	188.172.192.104	HTTP	183	GET /cname.aspx HTTP/
3040	120.639915	188.172.192.104	172.16.38.201	HTTP	661	HTTP/1.1 403 Forbidde
5445	162.329969	172.16.38.201	213.227.186.144	HTTP	182	GET /cname.aspx HTTP/

Source: IntelCor_6a:bb:c5 (34:f6:4b:6a:bb:c5)
Address: IntelCor_6a:bb:c5 (34:f6:4b:6a:bb:c5)
Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.16.38.201, Dst: 188.172.246.170
> Transmission Control Protocol, Src Port: 56202, Dst Port: 80, Seq: 1, Ack: 1, Len: 128
> Hypertext Transfer Protocol

0000 70 18 a7 60 9c d3 34 f6 4b 6a bb c5 08 00 45 00 p...4. kj....E-
0010 00 a8 58 e6 40 00 80 06 1b 39 ac 10 26 c9 bc ac ..X.@...-9-&...
0020 f6 aa db 8a 00 50 b3 e0 ed e5 e5 ae b4 ec 50 18P.....P..

Specifies if this is an individual (unicast) address (eth.src.ig), 3 octets | Paquets : 233674 · Affichés : 252 (0.1%) · Perdus : 0 (0.0%) | Profil : Default

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.

The screenshot shows the Wireshark network protocol analyzer. The top pane displays a list of captured packets, filtered by 'dns'. The middle pane shows the details of the selected packet (No. 1331), and the bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
362	11.430095	172.16.38.201	37.18.92.5	DNS	82	Standard query 0x7c62
363	11.437795	37.18.92.5	172.16.38.201	DNS	517	Standard query response
811	31.808898	172.16.38.201	37.18.92.5	DNS	83	Standard query 0x2703
812	31.812611	37.18.92.5	172.16.38.201	DNS	519	Standard query response
849	32.882234	172.16.38.201	37.18.92.5	DNS	83	Standard query 0x4746
850	32.885715	37.18.92.5	172.16.38.201	DNS	519	Standard query response
1033	40.326416	172.16.38.201	37.18.92.5	DNS	87	Standard query 0xdf7d
1034	40.330514	37.18.92.5	172.16.38.201	DNS	553	Standard query response
1111	43.435443	172.16.38.201	37.18.92.5	DNS	85	Standard query 0x856e
1112	43.439589	37.18.92.5	172.16.38.201	DNS	462	Standard query response
1330	50.439879	172.16.38.201	37.18.92.5	DNS	86	Standard query 0x24ed
1331	50.465210	172.16.38.201	193.232.218.194	DNS	86	Standard query 0x24ed
1336	50.483144	37.18.92.5	172.16.38.201	DNS	552	Standard query response

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

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

Internet Protocol Version 4, Src: 172.16.38.201, Dst: 193.232.218.194

User Datagram Protocol, Src Port: 63209, Dst Port: 53

Domain Name System (query)

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.

The image shows a Wireshark interface with a packet capture list and a detailed view of a selected packet.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
1261	49.051722	173.194.220.139	172.16.38.201	QUIC	71	Protected Payload (KP)
1262	49.051979	173.194.220.139	172.16.38.201	QUIC	67	Protected Payload (KP)
1263	49.051979	173.194.220.139	172.16.38.201	QUIC	169	Protected Payload (KP)
1264	49.052190	172.16.38.201	173.194.220.139	QUIC	75	Protected Payload (KP)
1265	49.052567	172.16.38.201	173.194.220.139	QUIC	75	Protected Payload (KP)
1266	49.053881	173.194.220.139	172.16.38.201	QUIC	67	Protected Payload (KP)
1267	49.055645	172.16.38.201	173.194.220.139	QUIC	75	Protected Payload (KP)
1268	49.056512	173.194.220.139	172.16.38.201	QUIC	977	Protected Payload (KP)
1269	49.056512	173.194.220.139	172.16.38.201	QUIC	259	Protected Payload (KP)
1270	49.057326	172.16.38.201	173.194.220.139	QUIC	77	Protected Payload (KP)
1272	49.083505	172.16.38.201	173.194.220.139	QUIC	75	Protected Payload (KP)
1273	49.098259	173.194.220.139	172.16.38.201	QUIC	67	Protected Payload (KP)
1593	57.830015	172.16.38.201	64.233.161.94	QUIC	1292	Initial, DCID=8771a72

Packet Details (Packet 1273):

- 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)

Packet Bytes:

Offset	Hex	ASCII
0020	26 c9 01 bb f4 14 00 21 27 6d 58 3c 0f d3 29 36	&.....! 'mX<..)6
0030	91 d5 b1 e8 b0 49 1b 55 25 86 29 bd 81 a5 26 5aI·U %·)...&Z
0040	e7 61 06	·a·

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.

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

Appliquer un filtre d'affichage ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.38.201	217.146.13.137	SSL	1514	Continuation Data
2	0.055370	172.16.38.201	193.200.65.150	TLSv1.2	247	Application Data
3	0.139438	172.16.38.68	224.0.0.251	MDNS	262	Standard query response 6
4	0.139438	172.16.38.68	224.0.0.251	MDNS	220	Standard query 0x0000 AN
5	0.144788	193.200.65.150	172.16.38.201	TCP	60	443 → 49790 [ACK] Seq=1 /
6	0.193419	172.16.38.222	224.0.0.251	MDNS	136	Standard query 0x002d PTF
7	0.200268	172.16.38.151	224.0.0.251	MDNS	403	Standard query response 6
8	0.200268	193.200.65.150	172.16.38.201	TLSv1.2	781	Application Data
9	0.217275	172.16.39.47	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
10	0.242167	172.16.38.201	193.200.65.150	TCP	54	49790 → 443 [ACK] Seq=194
11	0.286736	172.16.38.68	224.0.0.251	MDNS	268	Standard query 0x0000 PTF
12	0.300685	172.16.38.201	217.146.13.137	TCP	1514	[TCP Retransmission] 4996
13	0.316252	172.16.38.114	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1

> Frame 1: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{...}

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

✓ Internet Protocol Version 4, Src: 172.16.38.201, Dst: 217.146.13.137

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 1500
- Identification: 0x354d (13645)
- > Flags: 0x40, Don't fragment
- ...0 0000 0000 0000 = Fragment Offset: 0

0000 70 18 a7 60 9c d3 34 f6 4b 6a bb c5 08 00 45 00 p...4- Kj...E-

0010 05 dc 35 4d 40 00 80 06 05 da ac 10 26 c9 d9 92 --5M@...-&...

0020 0d 89 c3 31 01 bb 6f 55 a7 8e 8b 46 85 0a 50 18 ...1..oU ...F..P-

Беспроводная сеть: <live capture in progress> | Paquets : 165 · Affichés : 165 (100.0%) | Profil : Default

6.1

Вывод

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