Лабораторная работа № 3. Анализ трафика в Wireshark

Студент: Яссин Оулед Салем

Группа: НПИбд02-20

. Цель работы

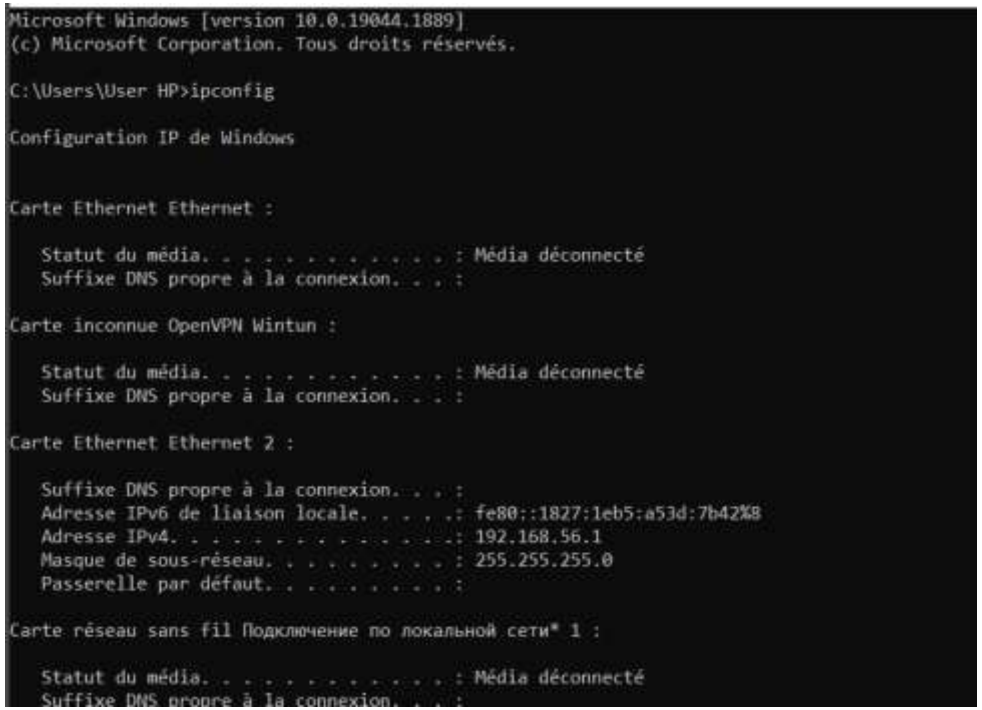
- Изучение посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.

. Задания для выполнения

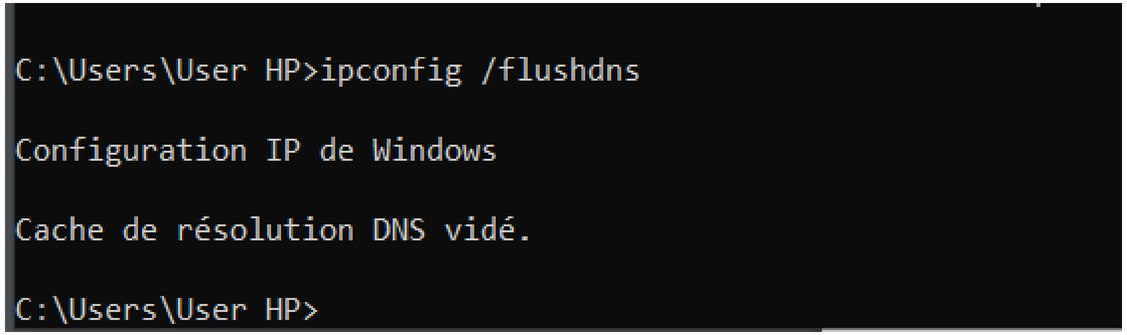
- MAC-адресация
- Анализ кадров канального уровня в Wireshark
- Анализ протоколов транспортного уровня в Wireshark

MAC-адресация

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

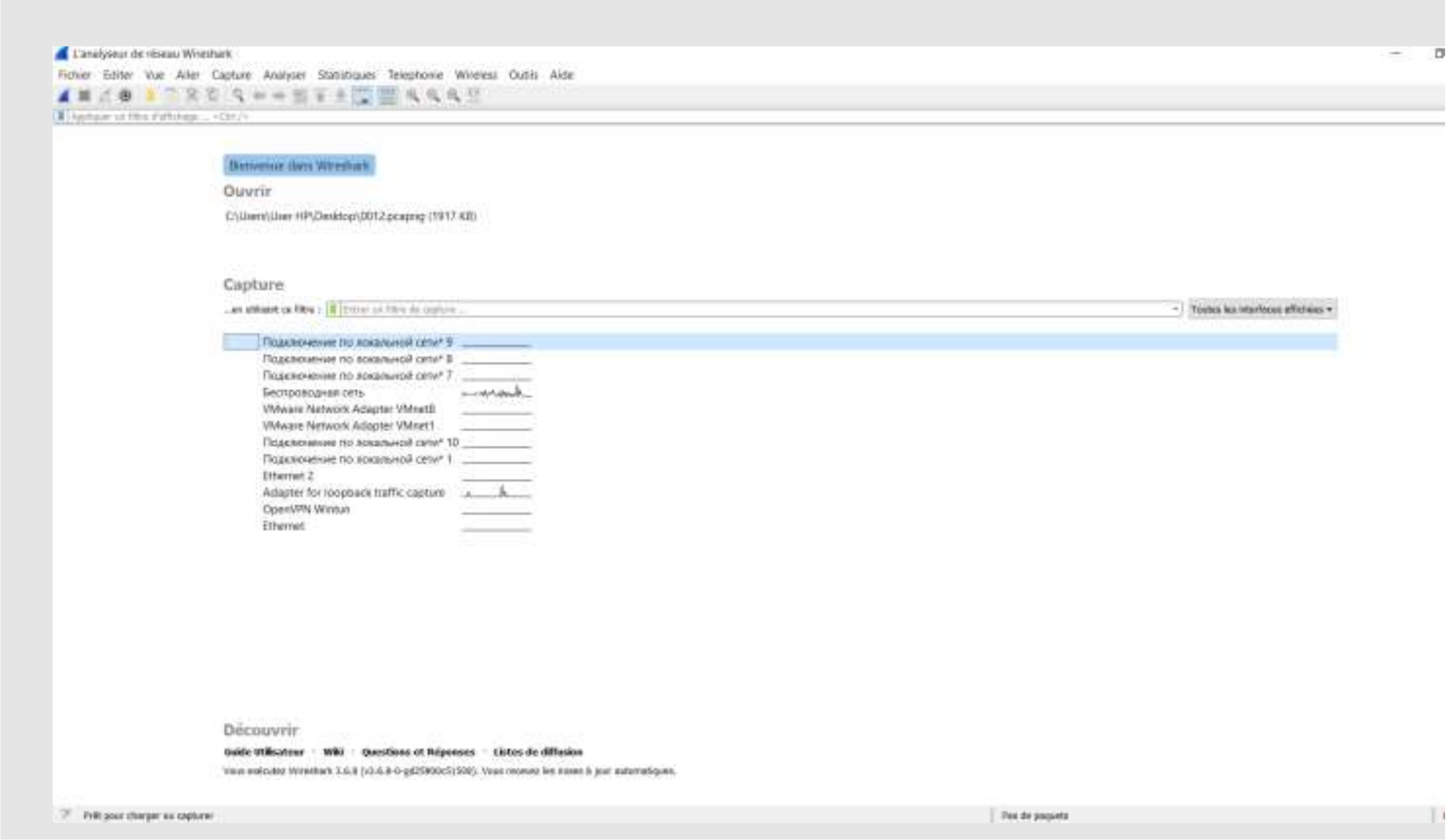


```
Microsoft Windows [version 10.0.19044.1889]
(c) Microsoft Corporation. Tous droits réservés.

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. . . :
```



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

Configuration IP de Windows

Cache de résolution DNS vidé.

C:\Users\User HP>
```

. Анализ кадров канального уровня в Wireshark

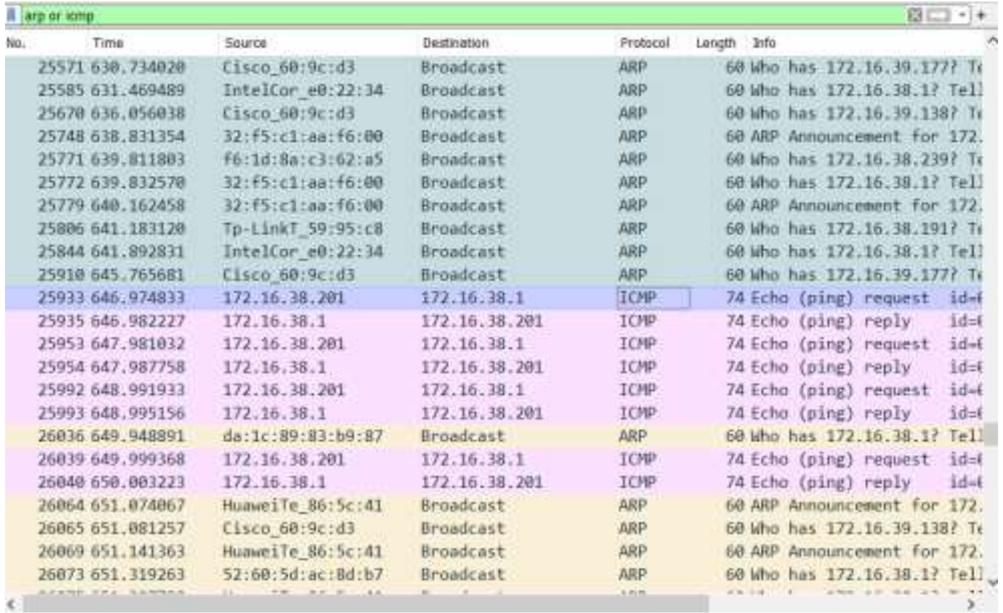

L'analyseur de réseau Wireshark
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide
Appliquer un filtre d'affichage ... <Ctrl-/>
Bienvenue dans Wireshark
Ouvrir
Capture
...en utilisant ce filtre :
Entrer un filtre de capture ...
Toutes les interfaces affichées
Découvrir
Guide Utilisateur · Wiki · Questions et Réponses · Listes de diffusion
Prêt pour charger ou capturer
Pas de paquets

C:\Users\User HP\Desktop\0012.pcapng (1917 KB)

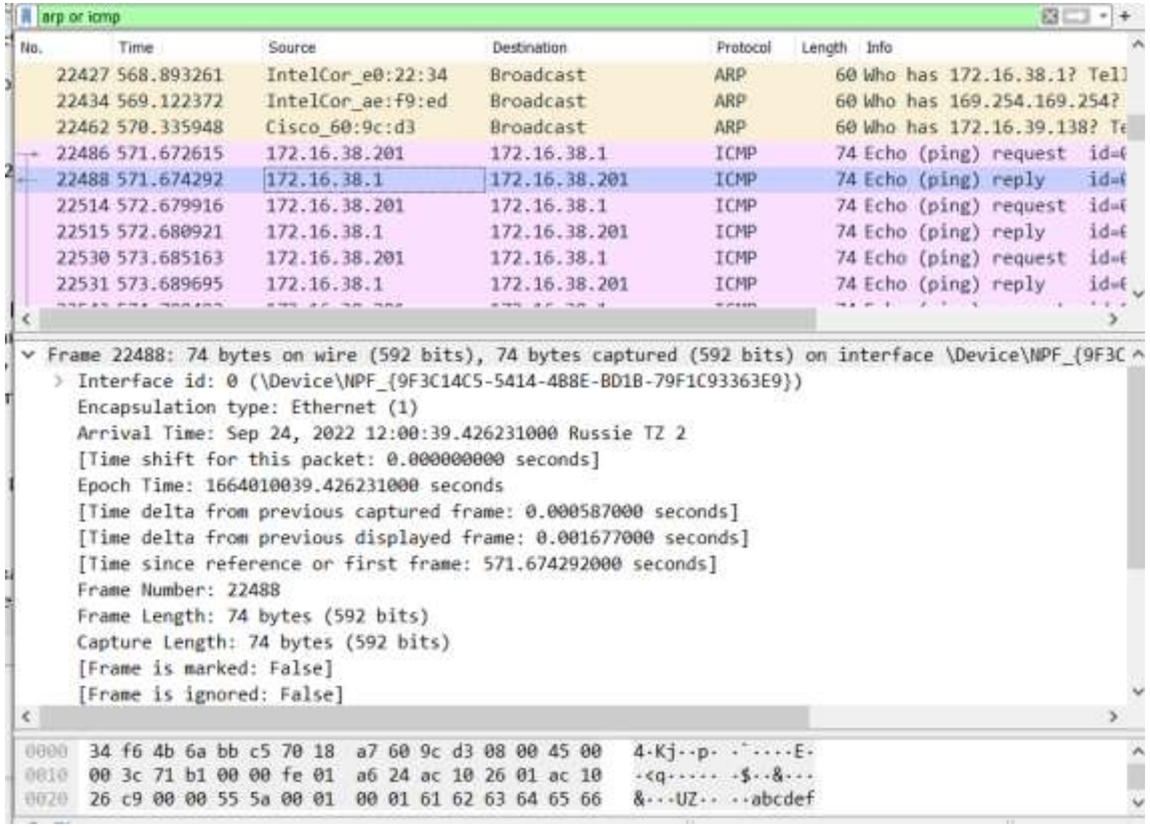
Подключение по локальной сети* 9
Подключение по локальной сети* 8
Подключение по локальной сети* 7
Беспроводная сеть
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Подключение по локальной сети* 10
Подключение по локальной сети* 1
Ethernet 2
Adapter for loopback traffic capture
OpenVPN Wintun
Ethernet

Vous exécutez Wireshark 3.6.8 (v3.6.8-0-gd25900c51508). Vous recevez les mises à jour automatiques.

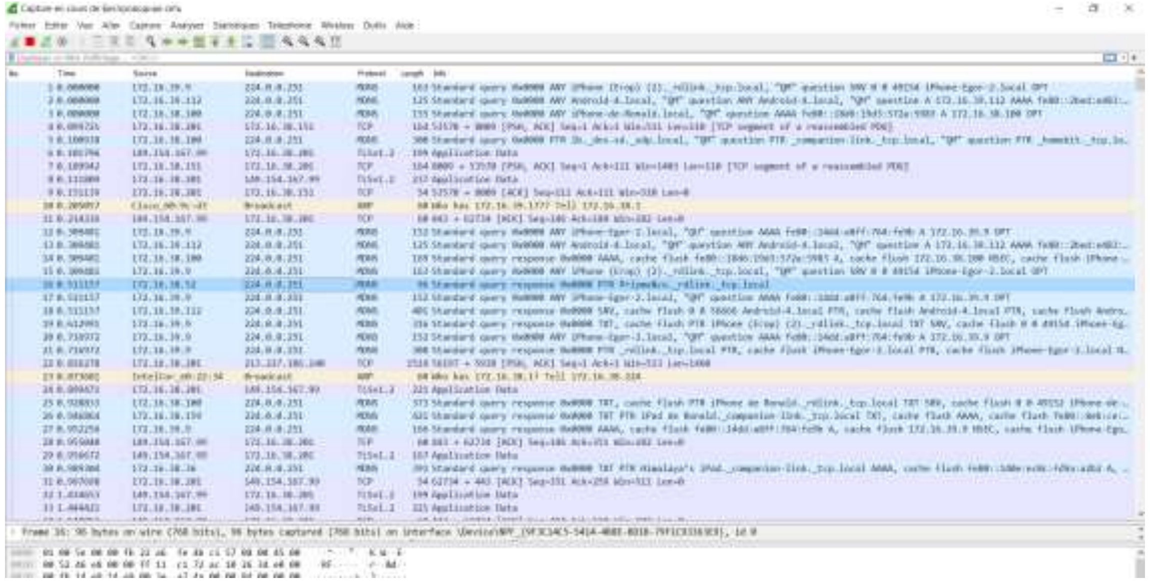
- 1. Установить на домашнем устройстве Wireshark.
- 2. С помощью Wireshark захватить и проанализировать пакеты ARP и ICMP в части кадров канального уровня.



```
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=(
25935 646.982227  172.16.38.1         172.16.38.201   ICMP       74 Echo (ping) reply    id=(
25953 647.981032  172.16.38.201       172.16.38.1     ICMP       74 Echo (ping) request  id=(
25954 647.987758  172.16.38.1         172.16.38.201   ICMP       74 Echo (ping) reply    id=(
25992 648.991933  172.16.38.201       172.16.38.1     ICMP       74 Echo (ping) request  id=(
25993 648.995156  172.16.38.1         172.16.38.201   ICMP       74 Echo (ping) reply    id=(
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=(
26040 650.003223  172.16.38.1         172.16.38.201   ICMP       74 Echo (ping) reply    id=(
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
```

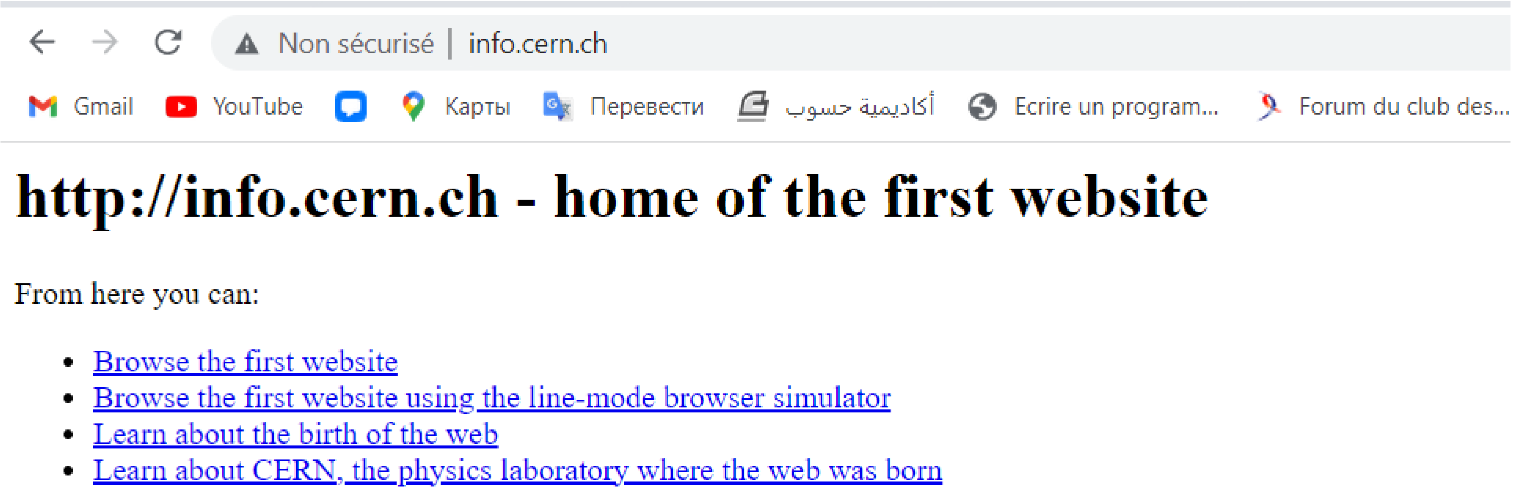


```
arp or icmp
No.    Time        Source              Destination     Protocol  Length  Info
22427 568.893261  IntelCor_e0:22:34   Broadcast       ARP        60 Who has 172.16.38.1? Tell
22434 569.122372  IntelCor_ae:f9:ed   Broadcast       ARP        60 Who has 169.254.169.254?
22462 570.335948  Cisco_60:9c:d3      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=(
22488 571.674292  172.16.38.1         172.16.38.201   ICMP       74 Echo (ping) reply    id=(
22514 572.679916  172.16.38.201       172.16.38.1     ICMP       74 Echo (ping) request  id=(
22515 572.680921  172.16.38.1         172.16.38.201   ICMP       74 Echo (ping) reply    id=(
22530 573.685163  172.16.38.201       172.16.38.1     ICMP       74 Echo (ping) request  id=(
22531 573.689695  172.16.38.1         172.16.38.201   ICMP       74 Echo (ping) reply    id=(

v Frame 22488: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{9F3C
  > Interface id: 0 (\Device\NPF_{9F3C14C5-5414-4B8E-BD1B-79F1C93363E9})
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 24, 2022 12:00:39.426231000 Russie TZ 2
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1664010039.426231000 seconds
    [Time delta from previous captured frame: 0.000587000 seconds]
    [Time delta from previous displayed frame: 0.001677000 seconds]
    [Time since reference or first frame: 571.674292000 seconds]
    Frame Number: 22488
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]

0000  34 f6 4b 6a bb c5 70 18  a7 60 9c d3 08 00 45 00   4·Kj··p· ·`····E·
0010  00 3c 71 b1 00 00 fe 01  a6 24 ac 10 26 01 ac 10   ·<q····· ·$··&···
0020  26 c9 00 00 55 5a 00 01  00 01 61 62 63 64 65 66   &···UZ·· ··abcdef
```



```
Capture en cours de [illegible]
Fichier  Editer  Vue  Aller  Capture  Analyser  Statistiques  Telephonie  Wireless  Outils  Aide
No.  Time        Source            Destination       Protocol  Length  Info
 1 0.000000   172.16.39.9       224.0.0.251       MDNS    163 Standard query 0x0000 ANY iPhone (Erop) (2)._rdlink._tcp.local, "QM" question SRV 0 0 49154 iPhone-Egor-2.local OPT
 2 0.000000   172.16.38.112     224.0.0.251       MDNS    125 Standard query 0x0000 ANY Android-4.local, "QM" question ANY Android-4.local, "QM" question A 172.16.38.112 AAAA fe80::2bed:e8b3:...
 3 0.000000   172.16.38.100     224.0.0.251       MDNS    133 Standard query 0x0000 ANY iPhone-de-Ronald.local, "QM" question AAAA fe80::[illegible] A 172.16.38.100 OPT
 4 0.099726   172.16.38.201     172.16.38.151     TCP     164 53570 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=531 Len=110 [TCP segment of a reassembled PDU]
 5 0.100318   172.16.38.100     224.0.0.251       MDNS    308 Standard query 0x0000 PTR [illegible]._dns-sd._udp.local, "QM" question PTR _companion-link._tcp.local, "QM" question PTR _homekit._tcp.lo...
 6 0.101796   149.154.167.99    172.16.38.201     TLSv1.2 109 Application Data
 7 0.109342   172.16.38.151     172.16.38.201     TCP     164 8009 → 53570 [PSH, ACK] Seq=1 Ack=111 Win=1403 Len=110 [TCP segment of a reassembled PDU]
 8 0.111000   172.16.38.201     149.154.167.99    TLSv1.2 237 Application Data
 9 0.151170   172.16.38.201     172.16.38.151     TCP      54 53570 → 8009 [ACK] Seq=111 Ack=111 Win=530 Len=0
10 0.205057   Cisco_60:9c:d3    Broadcast         ARP      60 Who has 172.16.39.177? Tell 172.16.38.1
11 0.214310   149.154.167.99    172.16.38.201     TCP      60 443 → 62734 [ACK] Seq=186 Ack=184 Win=282 Len=0
12 0.309401   172.16.39.9       224.0.0.251       MDNS    132 Standard query 0x0000 ANY iPhone-Egor-2.local, "QU" question AAAA fe80::[illegible] A 172.16.39.9 OPT
13 0.309401   172.16.38.112     224.0.0.251       MDNS    125 Standard query 0x0000 ANY Android-4.local, "QM" question ANY Android-4.local, "QM" question A 172.16.38.112 AAAA fe80::2bed:e8b3:...
14 0.309401   172.16.38.100     224.0.0.251       MDNS    169 Standard query response 0x0000 AAAA, cache flush fe80::[illegible] A, cache flush 172.16.38.100 NSEC, cache flush iPhone-...
15 0.309401   172.16.39.9       224.0.0.251       MDNS    163 Standard query 0x0000 ANY iPhone (Erop) (2)._rdlink._tcp.local, "QM" question SRV 0 0 49154 iPhone-Egor-2.local OPT
16 0.511157   172.16.38.52      224.0.0.251       MDNS     96 Standard query response 0x0000 PTR [illegible]._rdlink._tcp.local
17 0.511157   172.16.39.9       224.0.0.251       MDNS    132 Standard query 0x0000 ANY iPhone-Egor-2.local, "QM" question AAAA fe80::[illegible] A 172.16.39.9 OPT
18 0.511157   172.16.38.112     224.0.0.251       MDNS    405 Standard query response 0x0000 SRV, cache flush 0 0 [illegible] Android-4.local PTR, cache flush Android-4.local PTR, cache flush Andro...
19 0.612091   172.16.39.9       224.0.0.251       MDNS    316 Standard query response 0x0000 TXT, cache flush PTR iPhone (Erop) (2)._rdlink._tcp.local TXT SRV, cache flush 0 0 49154 iPhone-Eg...
20 0.710372   172.16.39.9       224.0.0.251       MDNS    132 Standard query 0x0000 ANY iPhone-Egor-2.local, "QM" question AAAA fe80::[illegible] A 172.16.39.9 OPT
21 0.710372   172.16.39.9       224.0.0.251       MDNS    308 Standard query response 0x0000 PTR _rdlink._tcp.local PTR, cache flush iPhone-Egor-2.local PTR, cache flush iPhone-Egor-2.local N...
22 0.811278   172.16.38.201     213.227.[illegible]  TCP    1514 [illegible] → 5938 [PSH, ACK] Seq=1 Ack=1 Win=513 Len=1460
23 0.873082   IntelCor_e0:22:34 Broadcast         ARP      60 Who has 172.16.38.1? Tell 172.16.38.[illegible]
24 0.899473   172.16.38.201     149.154.167.99    TLSv1.2 225 Application Data
25 0.928033   172.16.38.100     224.0.0.251       MDNS    373 Standard query response 0x0000 TXT, cache flush PTR iPhone de Ronald._rdlink._tcp.local TXT SRV, cache flush 0 0 49152 iPhone-de-...
26 0.946864   172.16.38.150     224.0.0.251       MDNS    421 Standard query response 0x0000 TXT PTR iPad de Ronald._companion-link._tcp.local TXT, cache flush AAAA, cache flush fe80::[illegible]...
27 0.952250   172.16.39.9       224.0.0.251       MDNS    156 Standard query response 0x0000 AAAA, cache flush fe80::[illegible] A, cache flush 172.16.39.9 NSEC, cache flush iPhone-Ego...
28 0.955088   149.154.167.99    172.16.38.201     TCP      60 443 → 62734 [ACK] Seq=186 Ack=355 Win=282 Len=0
29 0.956672   149.154.167.99    172.16.38.201     TLSv1.2 107 Application Data
30 0.989304   172.16.38.16      224.0.0.251       MDNS    393 Standard query response 0x0000 TXT PTR Himalaya's iPad._companion-link._tcp.local AAAA, cache flush fe80::[illegible] A, ...
31 0.997098   172.16.38.201     149.154.167.99    TCP      54 62734 → 443 [ACK] Seq=355 Ack=258 Win=511 Len=0
32 1.414653   149.154.167.99    172.16.38.201     TLSv1.2 199 Application Data
33 1.444421   172.16.38.201     149.154.167.99    TLSv1.2 325 Application Data

> Frame 16: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface \Device\NPF_{9F3C14C5-5414-4B8E-BD1B-79F1C93363E9}, id 0
```

Анализ протоколов транспортного уровня в Wireshark

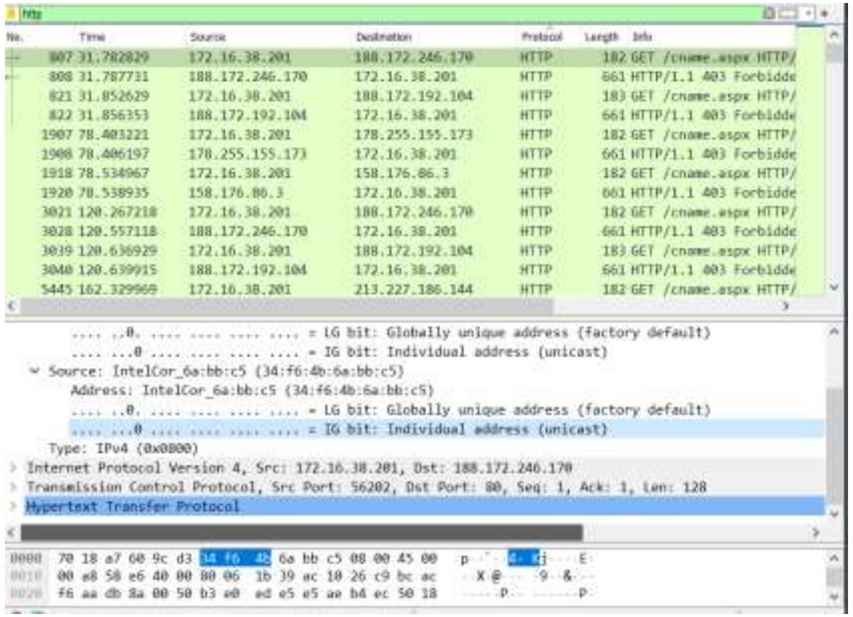


http://info.cern.ch - home of the first website

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

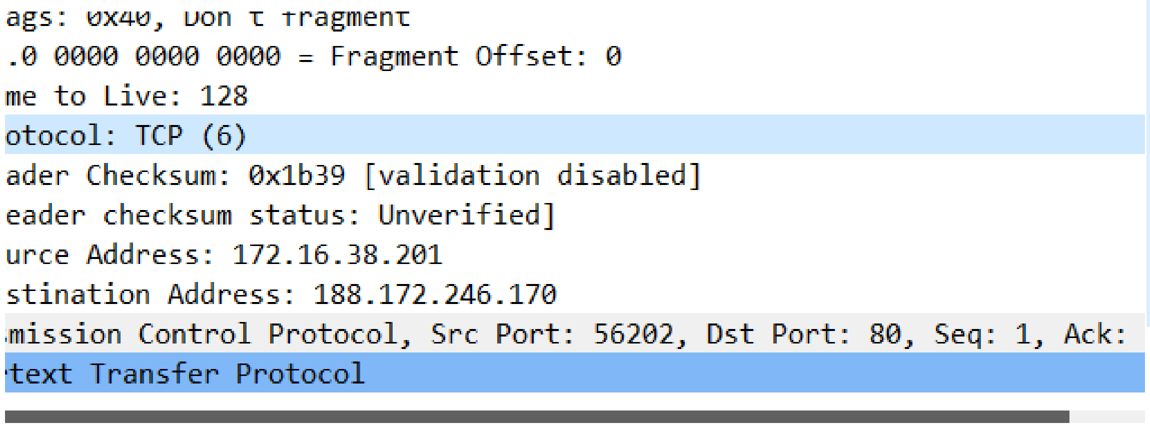
- С помощью Wireshark захватить и проанализировать пакеты HTTP, DNS в части заголовков и информации протоколов TCP, UDP, QUIC.



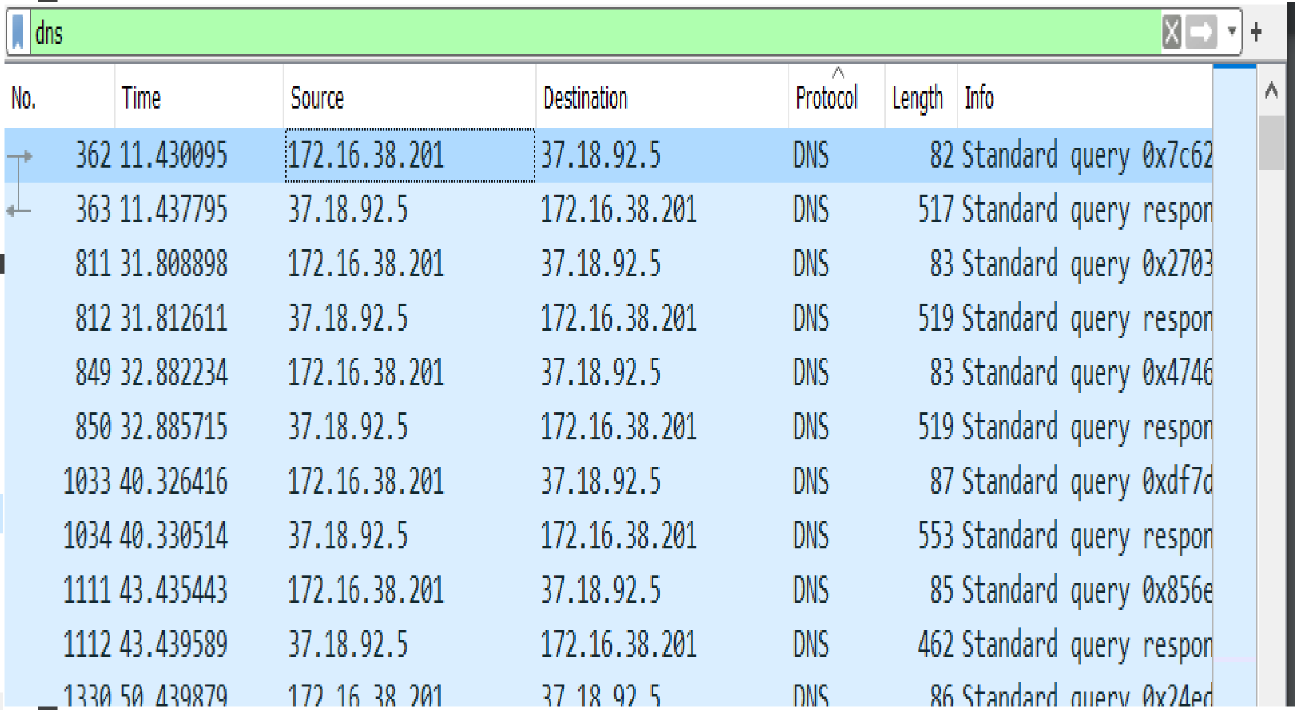
```
No.   Time        Source           Destination      Protocol  Length Info
 807 31.782829    172.16.38.201    188.172.246.170  HTTP      182 GET /cname.aspx HTTP/
 808 31.787731    188.172.246.170  172.16.38.201    HTTP      661 HTTP/1.1 403 Forbidde
 821 31.852629    172.16.38.201    188.172.192.104  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/
```

```
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: IntelCor_6a:bb:c5 (34:f6:4b:6a:bb:c5)
        Address: IntelCor_6a:bb:c5 (34:f6:4b:6a:bb:c5)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    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 e8 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 18   .....P........P.
```



```
ags: 0x40, Don't fragment
.0 0000 0000 0000 = Fragment Offset: 0
me to Live: 128
otocol: TCP (6)
ader Checksum: 0x1b39 [validation disabled]
eader checksum status: Unverified]
urce Address: 172.16.38.201
stination Address: 188.172.246.170
mission Control Protocol, Src Port: 56202, Dst Port: 80, Seq: 1, Ack:
text Transfer Protocol
```



```
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 respon
 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 respon
 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 respon
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 respon
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 respon
1330 50.439879    172.16.38.201    37.18.92.5       DNS        86 Standard query 0x24ed
```

Вывод

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