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: Саинт-Амур Измаэль
Группа: НПИбд-02-20

МОСКВА

2022 г.

Цель:

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

Ход работы:

3.3.1. MAC-адресация

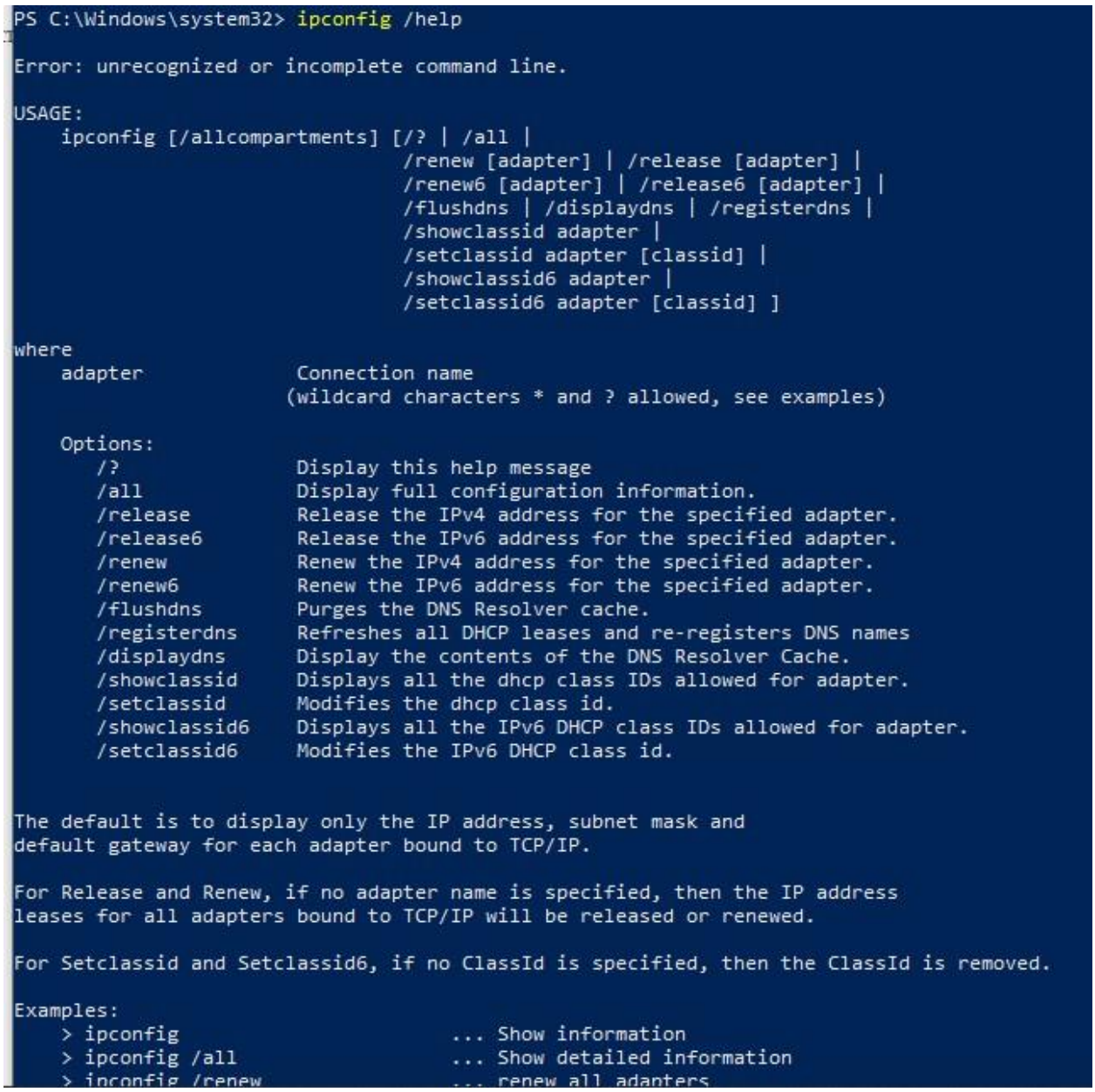
3.3.1.1. Постановка задачи

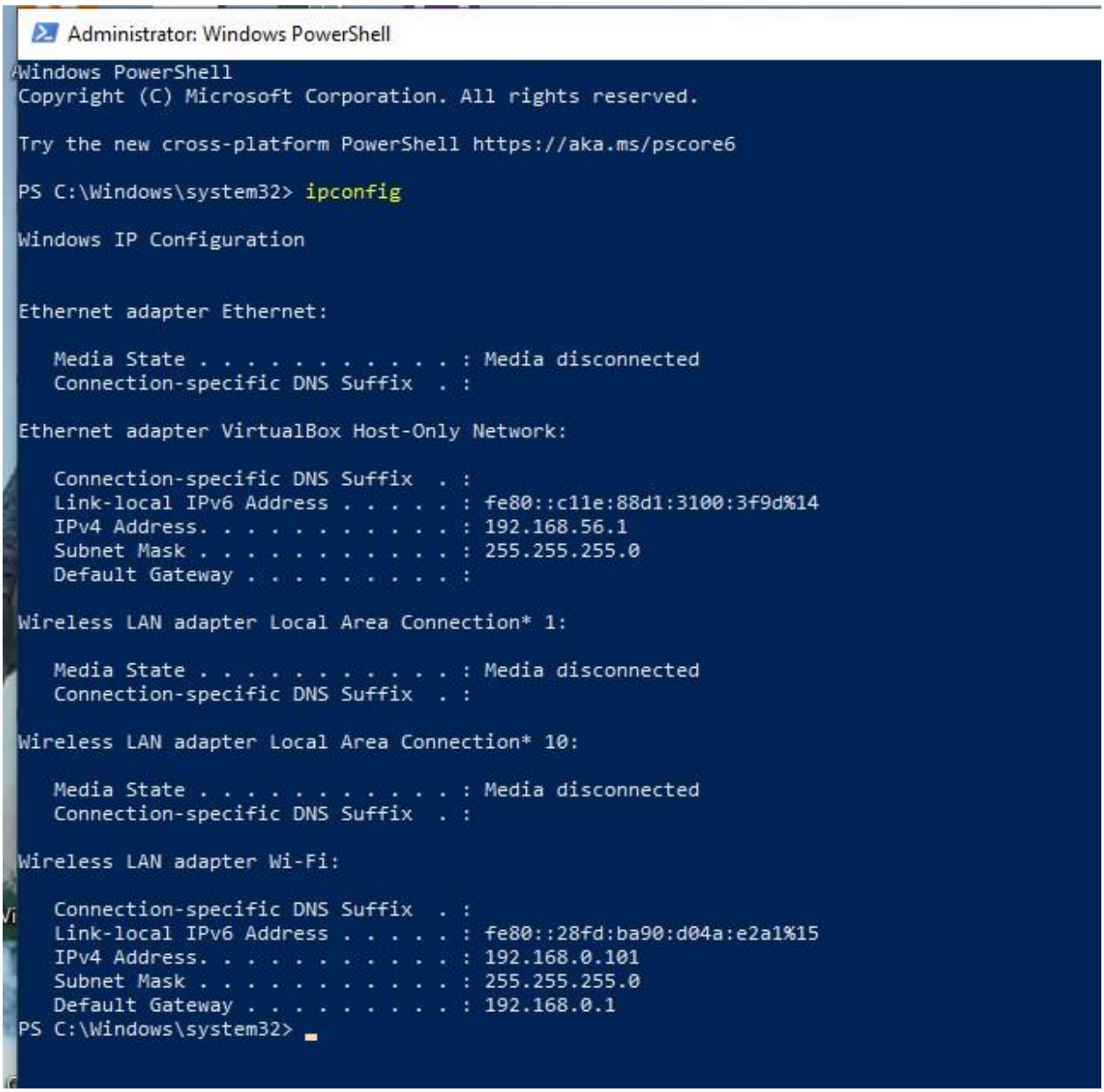
1. Изучение возможностей команды ipconfig для ОС типа Windows (ifconfig для систем типа Linux).

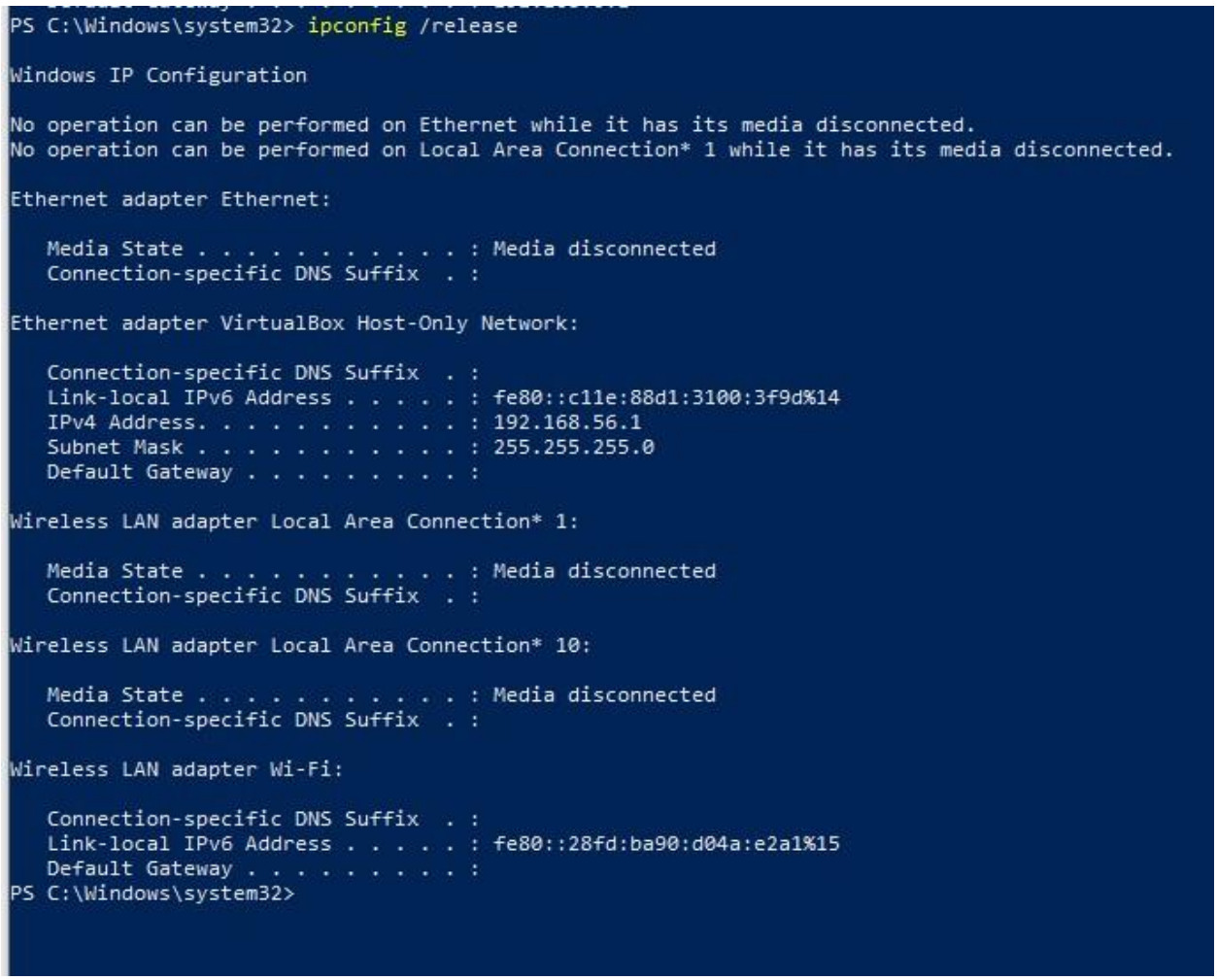
2. Определение MAC-адреса устройства и его типа.

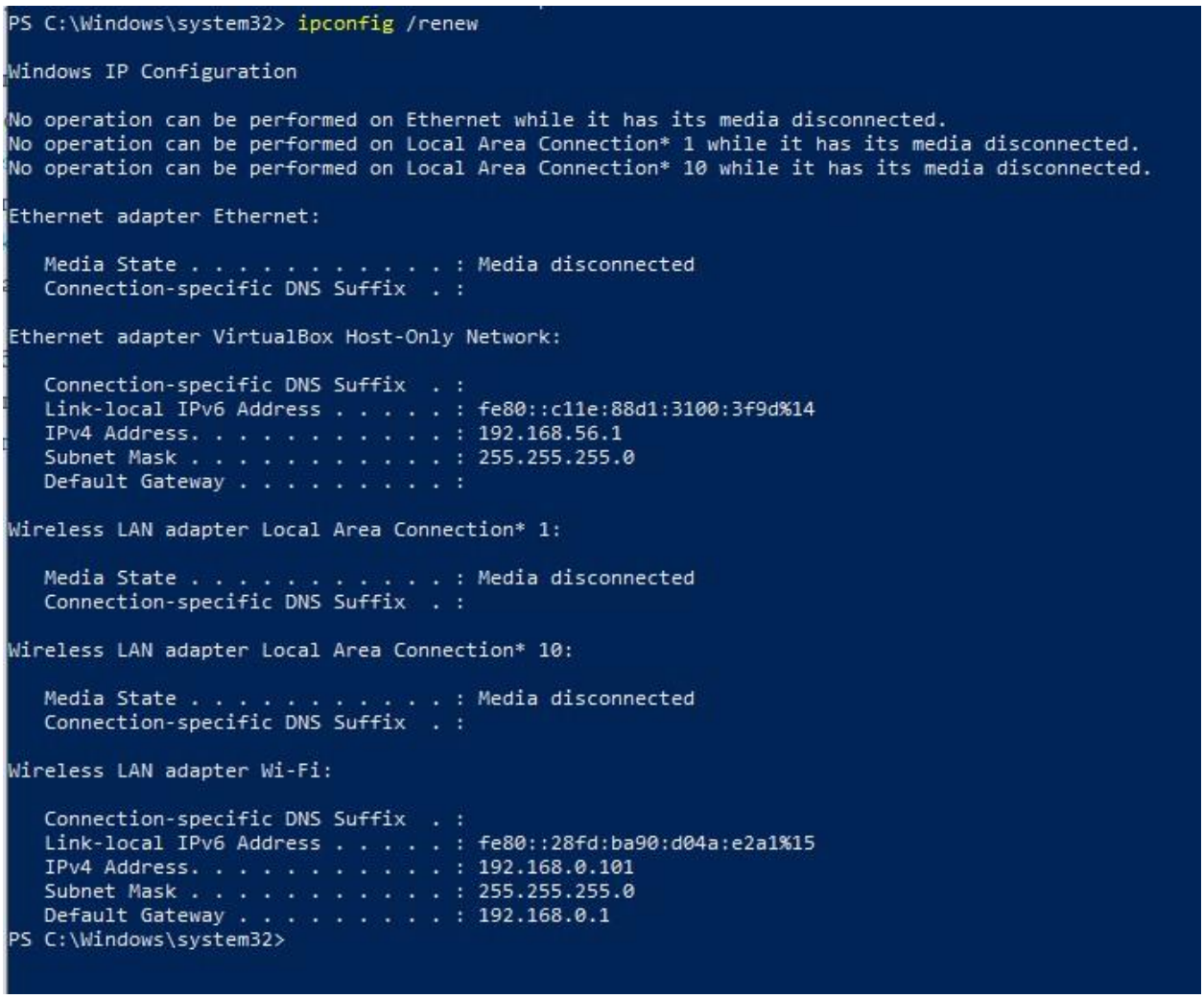
3.3.1.2. Порядок выполнения работы

1. С помощью команды ipconfig для ОС типа Windows или ifconfig для систем типа Linux выведите информацию о текущем сетевом соединении. Используйте разные опции команды. В отчёте поясните детально полученную в каждом случае при выводе информацию. Подтвердите свой ответ скриншотами.


PS C:\Windows\system32> 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


Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Windows\system32> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Ethernet adapter VirtualBox Host-Only Network:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::c11e:88d1:3100:3f9d%14
IPv4 Address. . . . . : 192.168.56.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Wireless LAN adapter Local Area Connection* 1:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 10:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::28fd:ba90:d04a:e2a1%15
IPv4 Address. . . . . : 192.168.0.101
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
PS C:\Windows\system32>

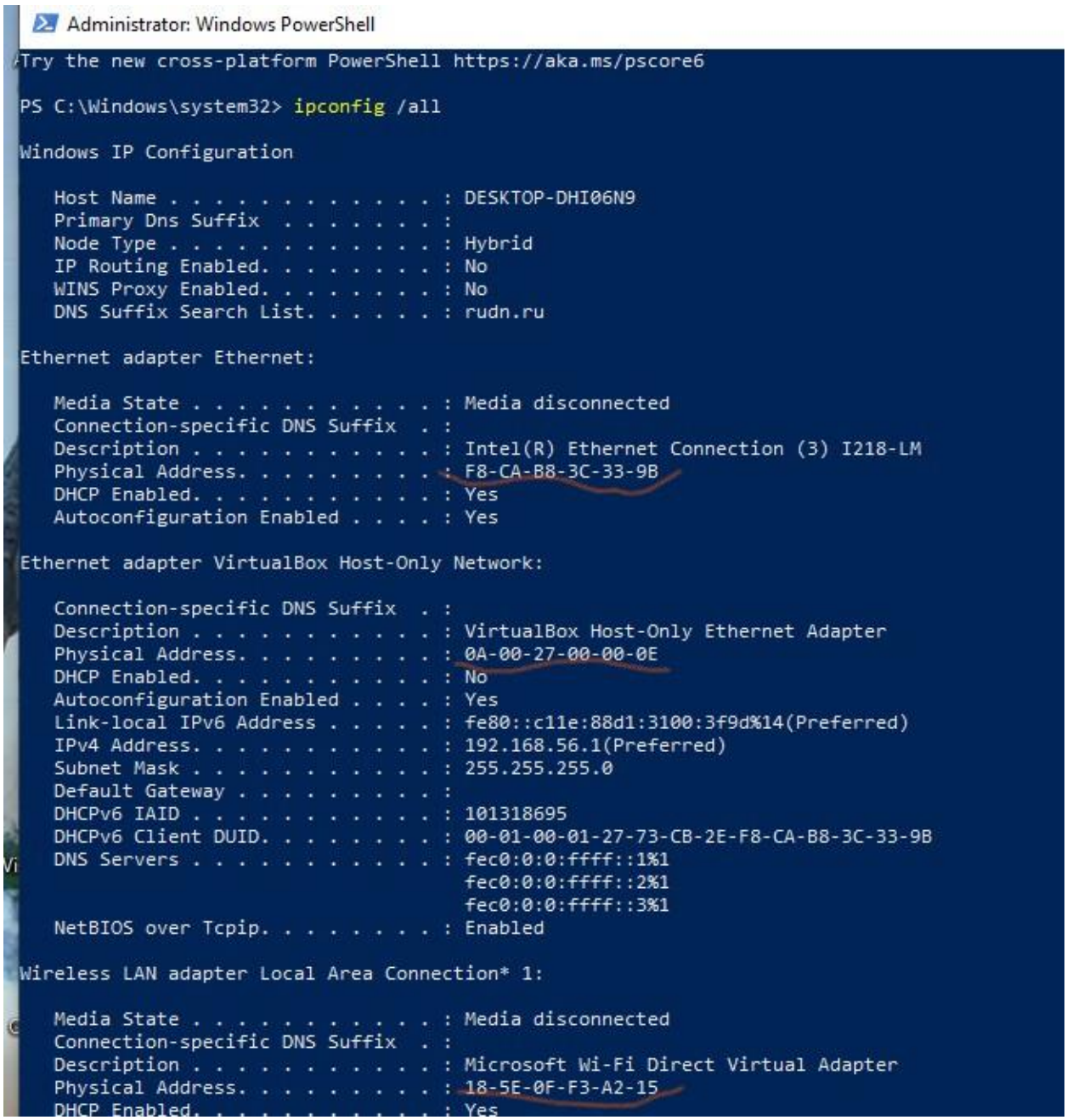

PS C:\Windows\system32> ipconfig /release
Windows IP Configuration
No operation can be performed on Ethernet while it has its media disconnected.
No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
Ethernet adapter Ethernet:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Ethernet adapter VirtualBox Host-Only Network:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::c11e:88d1:3100:3f9d%14
IPv4 Address. . . . . : 192.168.56.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Wireless LAN adapter Local Area Connection* 1:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 10:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::28fd:ba90:d04a:e2a1%15
Default Gateway . . . . . :
PS C:\Windows\system32>

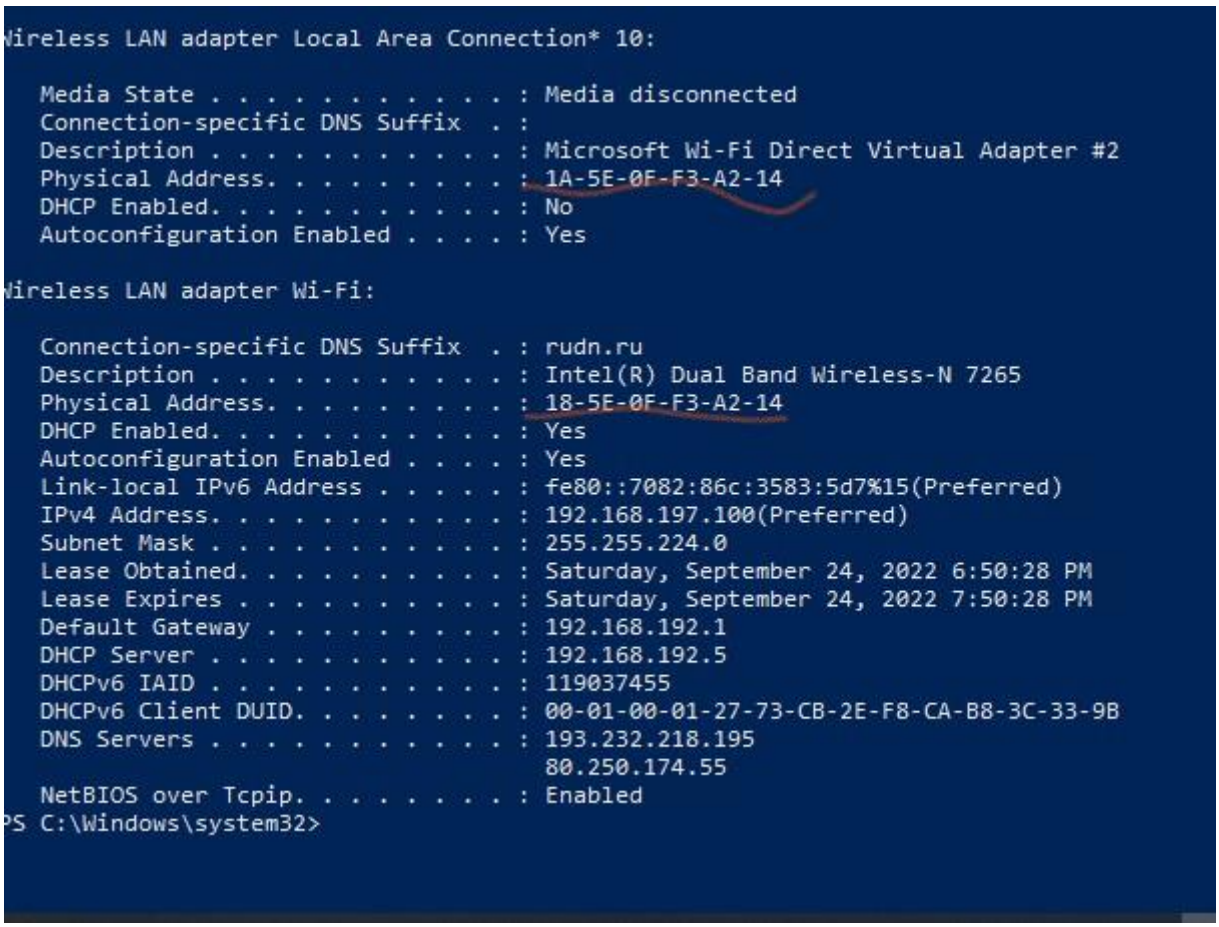


2. Определите MAC-адреса сетевых интерфейсов на вашем компьютере. Подтвердите свой ответ скриншотом.

3. Опишите структуру MAC-адресов вашего устройства. Какая часть адреса идентифицирует производителя? Какая часть адреса идентифицирует сетевой

интерфейс? Определите, каким является адрес — индивидуальным или групповым, глобально администрируемым или локально администрируемым.Поясните свой ответ. Используйте шестнадцатеричную запись MAC-адреса для пояснения.


Administrator: Windows PowerShell
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Windows\system32> ipconfig /all
Windows IP Configuration
Host Name . . . . . : DESKTOP-DHI06N9
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : rudn.ru
Ethernet adapter Ethernet:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) Ethernet Connection (3) I218-LM
Physical Address. . . . . : F8-CA-B8-3C-33-9B
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Ethernet adapter VirtualBox Host-Only Network:
Connection-specific DNS Suffix . :
Description . . . . . : VirtualBox Host-Only Ethernet Adapter
Physical Address. . . . . : 0A-00-27-00-00-0E
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::c11e:88d1:3100:3f9d%14(Preferred)
IPv4 Address. . . . . : 192.168.56.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 101318695
DHCPv6 Client DUID. . . . . : 00-01-00-01-27-73-CB-2E-F8-CA-B8-3C-33-9B
DNS Servers . . . . . : fec0:0:0:ffff::1%1
fec0:0:0:ffff::2%1
fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled
Wireless LAN adapter Local Area Connection* 1:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : 18-5E-0F-F3-A2-15
DHCP Enabled. . . . . : Yes



3.3.2. Анализ кадров канального уровня в Wireshark

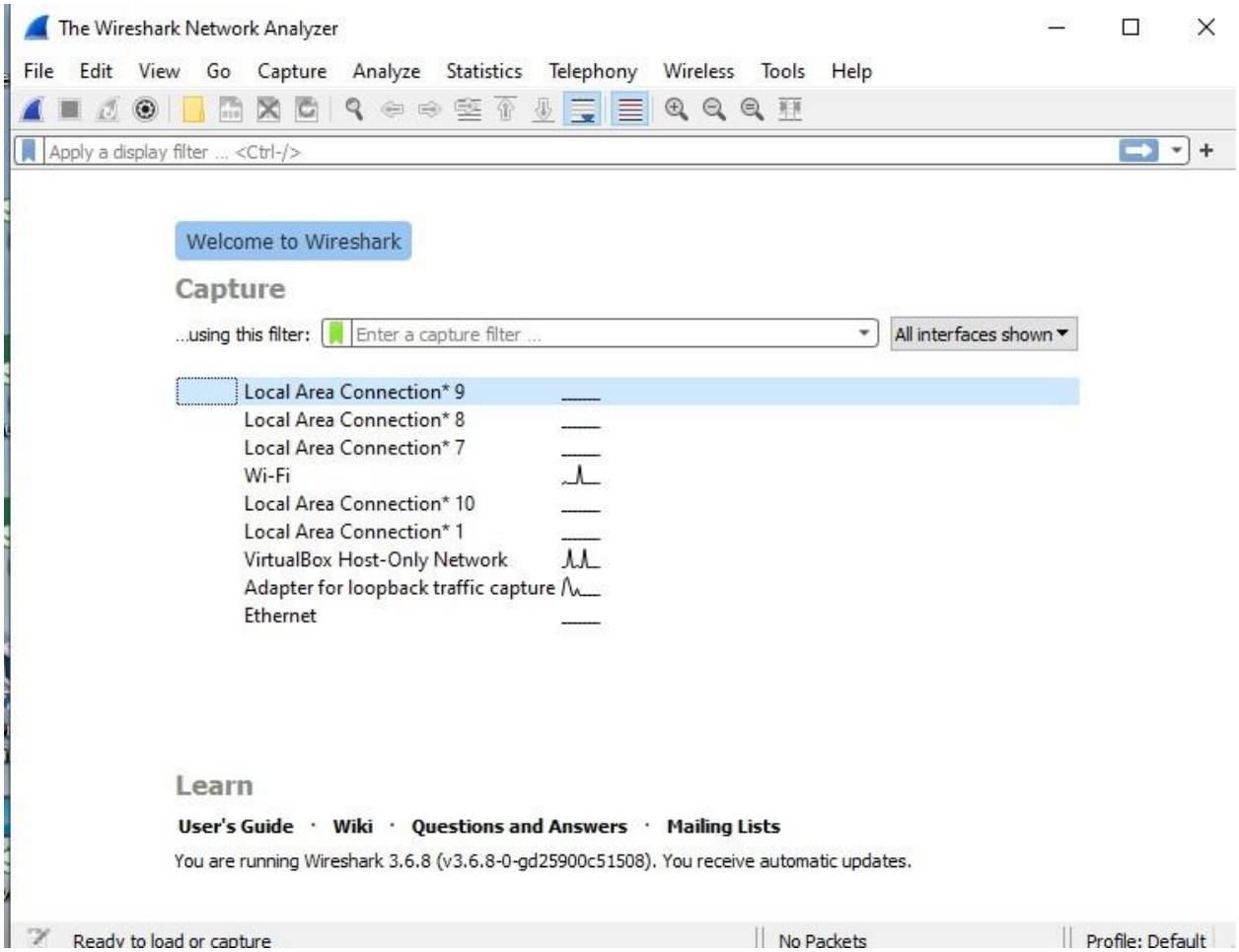
3.3.2.1. Постановка задачи

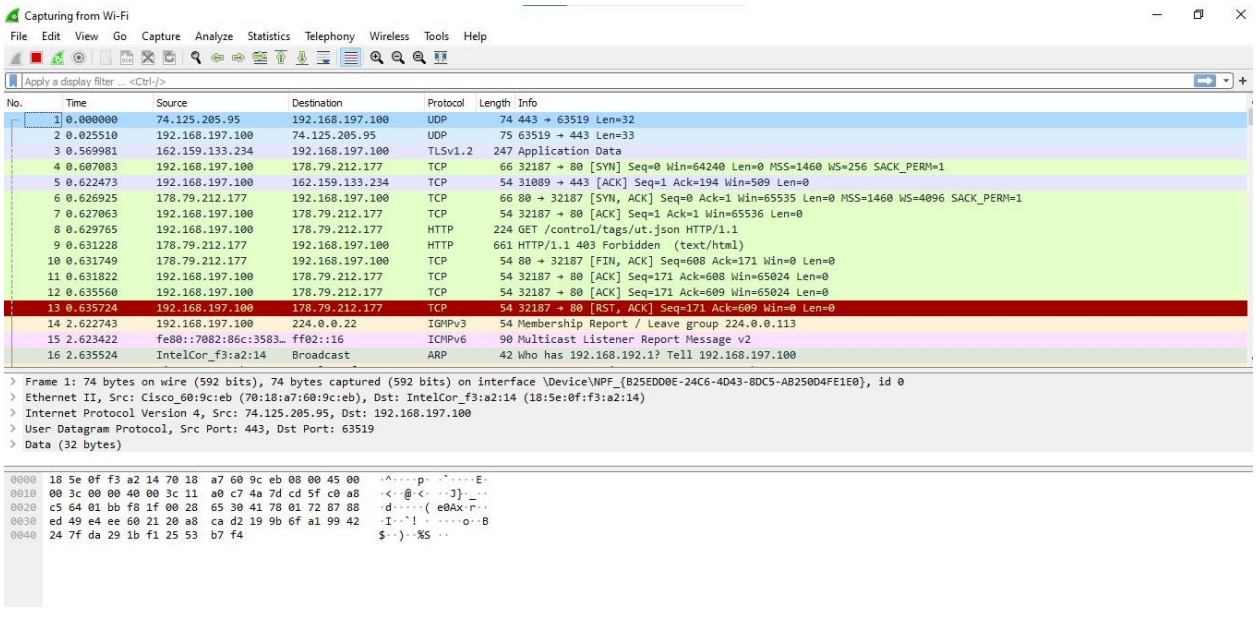
1. Установить на домашнем устройстве Wireshark.

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

1. Установите на вашем устройстве Wireshark.

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





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).

```
PS C:\Windows\system32> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

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

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c11e:88d1:3100:3f9d%14
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 10:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : rudn.ru
   Link-local IPv6 Address . . . . . : fe80::7082:86c:3583:5d7%15
   IPv4 Address. . . . . . . . . . . : 192.168.197.100
   Subnet Mask . . . . . . . . . . . : 255.255.224.0
   Default Gateway . . . . . . . . . : 192.168.192.1
PS C:\Windows\system32>
```

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.

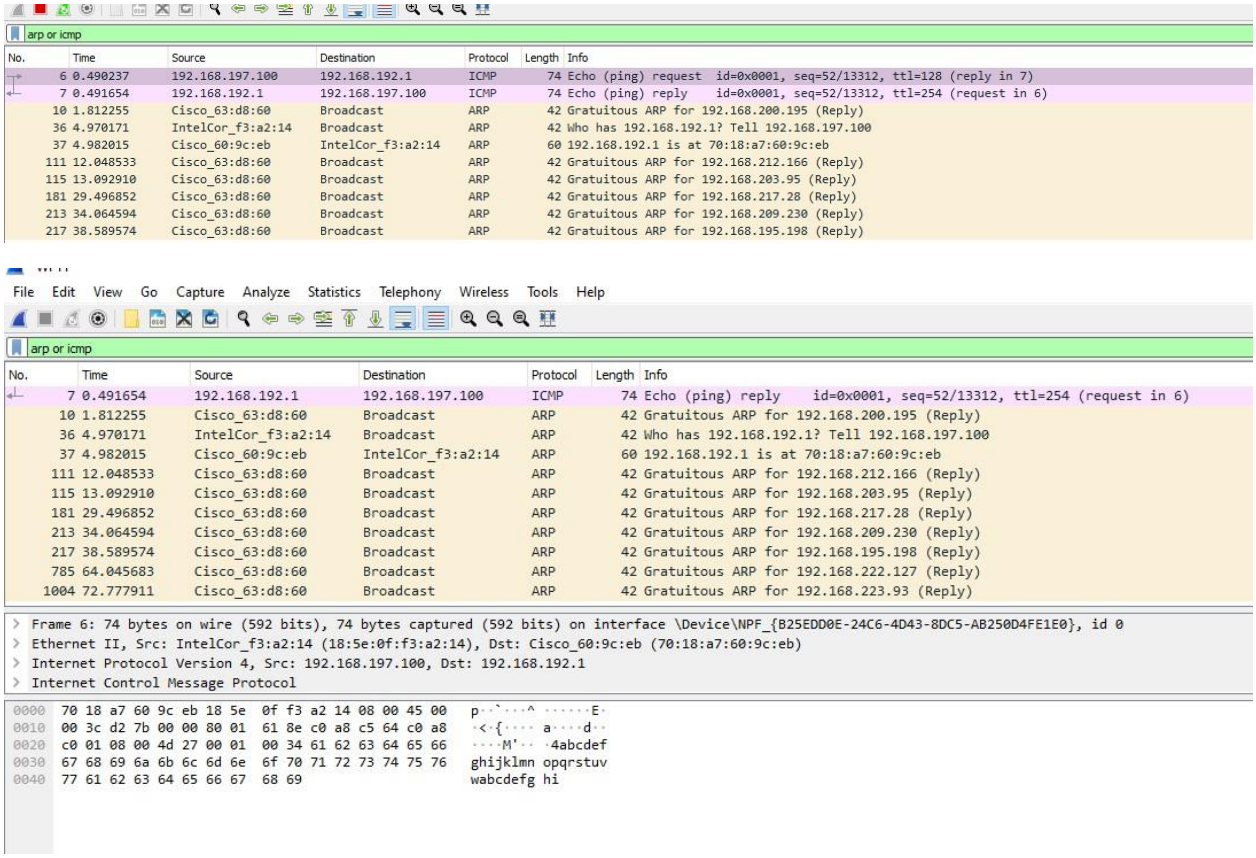
```
PS C:\Windows\system32> ping 192.168.192.1

Pinging 192.168.192.1 with 32 bytes of data:
Reply from 192.168.192.1: bytes=32 time=2ms TTL=254
Reply from 192.168.192.1: bytes=32 time=1ms TTL=254
Reply from 192.168.192.1: bytes=32 time=2ms TTL=254
Reply from 192.168.192.1: bytes=32 time=3ms TTL=254

Ping statistics for 192.168.192.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 2ms
PS C:\Windows\system32>
```

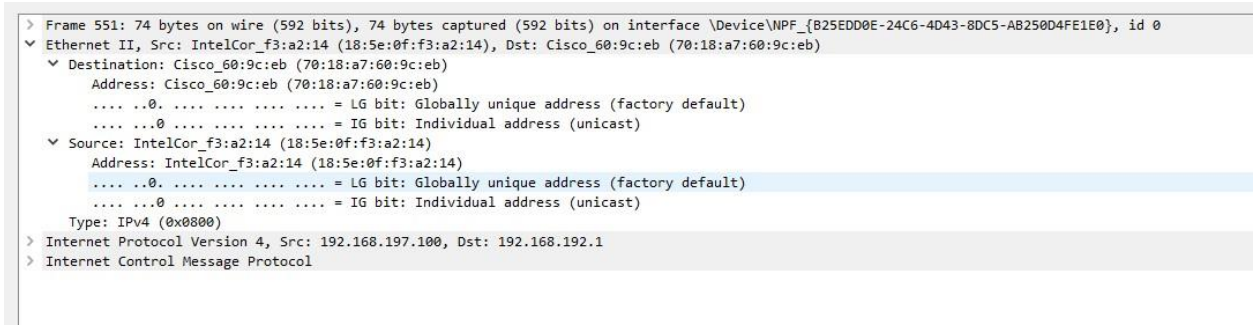
В Wireshark остановите захват трафика. В строке фильтра пропишите фильтр arp or icmp. Убедитесь, что в списке пакетов отобразятся только пакеты

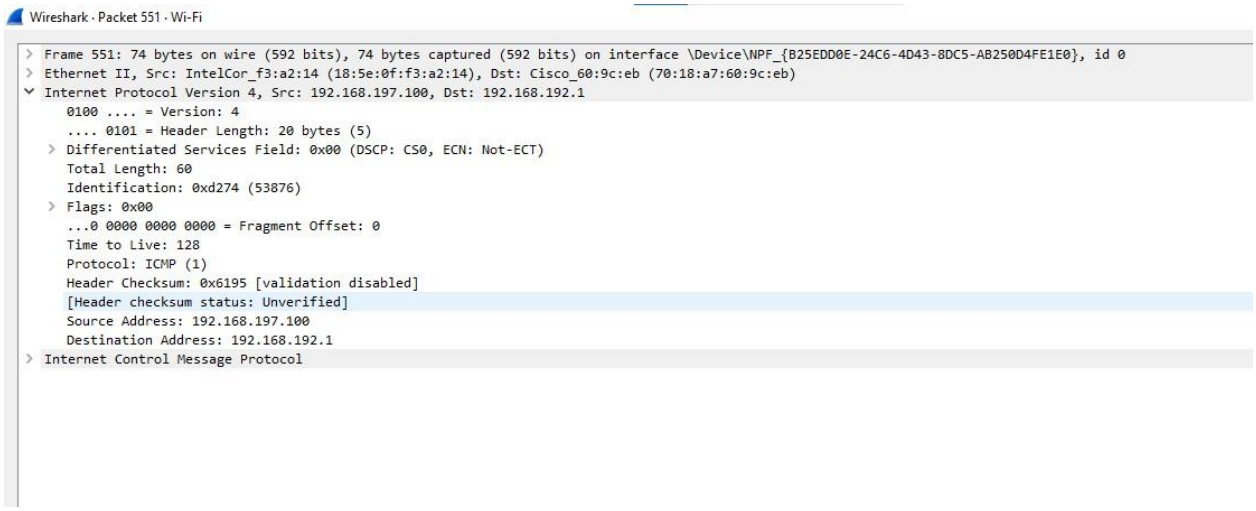
ARP или ICMP, в частности пакеты, которые были сгенерированы с помощью команды ping, отправленной с вашего устройства на шлюз по умолчанию.



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. 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

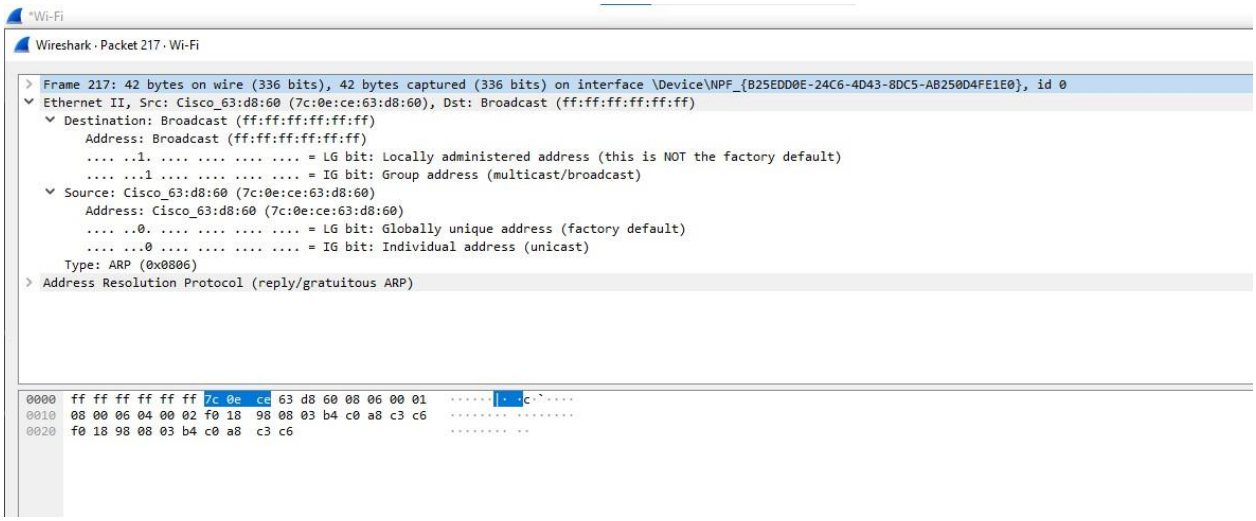
Ethernet относится кадр, определите MAC-адреса источника и шлюза, определите тип MAC-адресов.





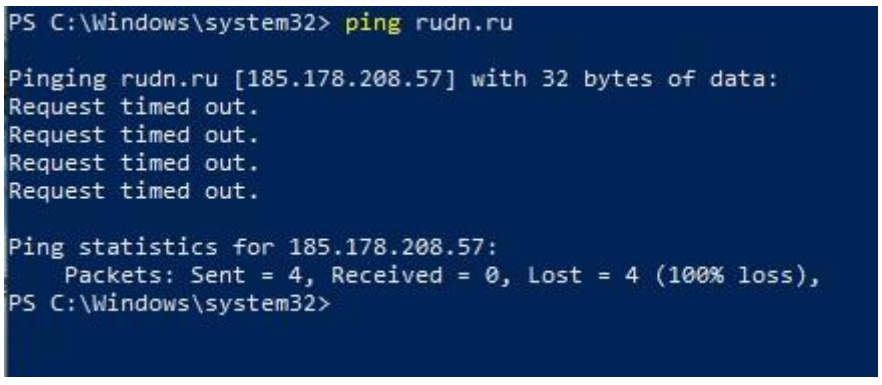
Изучите кадры данных протокола ARP. Изучите данные в полях заголовка

Ethernet II

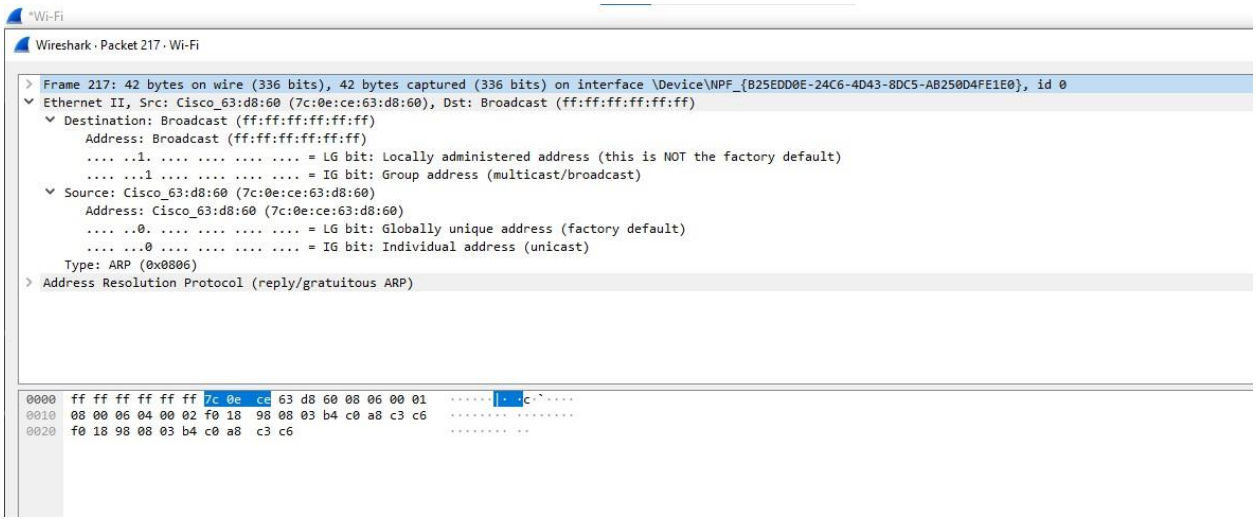


Начните новый процесс захвата трафика в Wireshark. На вашем устройстве

в консоли пропингуйте по имени какой-нибудь известный вам адрес, например ping rudn.ru.



В Wireshark остановите захват трафика. Изучите запросы и ответы протоколов ARP и ICMP. Определите MAC-адреса источника и получателя, определите тип MAC-адресов.



3.3.3. Анализ протоколов транспортного уровня в Wireshark

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

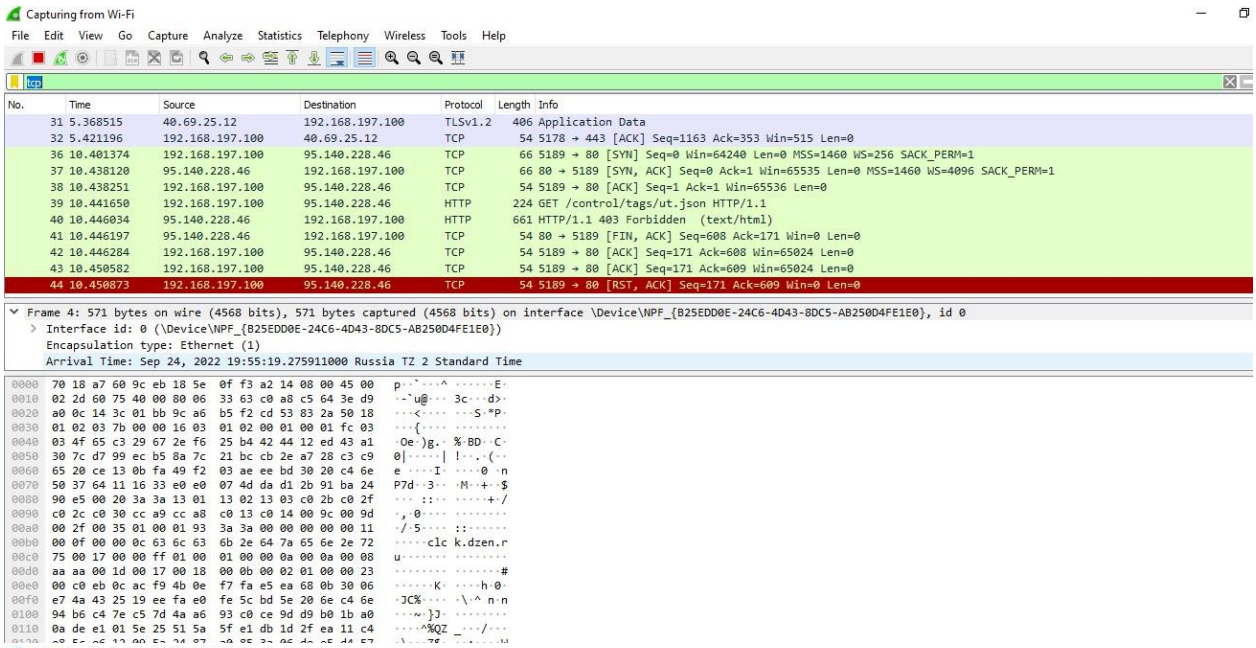
2. На вашем устройстве в браузере перейдите на сайт, работающий по протоколу HTTP (например, на сайт CERN http://info.cern.ch/). При необходимости получения большей информации для Wireshark поперемещайтесь по ссылкам или разделам сайта в браузере.

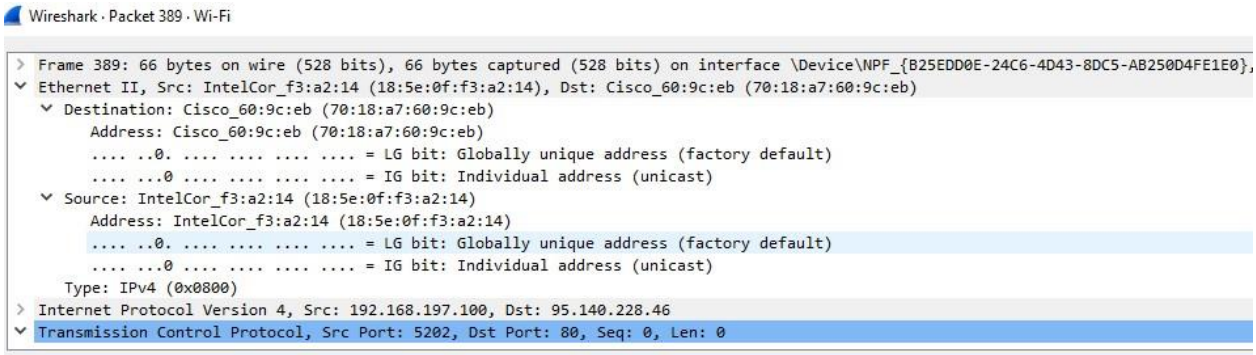
3. В Wireshark в строке фильтра укажите http и проанализируйте информацию по протоколу TCP в случае запросов и ответов. В отчёте приведите пояснение по информации, захваченной в Wireshark.

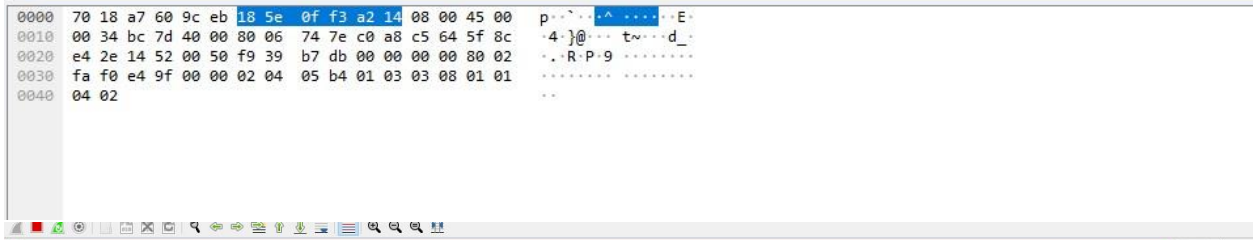
4. Wireshark в строке фильтра укажите dns и проанализируйте информацию по протоколу UDP в случае запросов и ответов. В отчёте приведите пояснение по информации, захваченной в Wireshark.

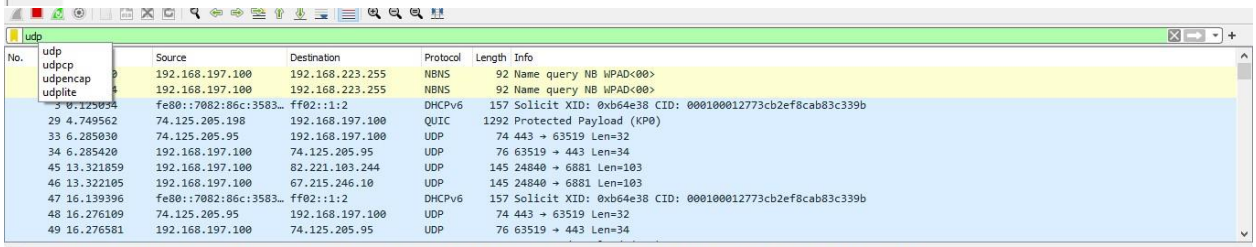
ВЫВОДЫ

В этой статье мы рассмотрели, как пользоваться Wireshark для анализа сетевого трафика, а также примеры решения проблем с сетью. Это очень мощная утилита, которая имеет очень много функций.

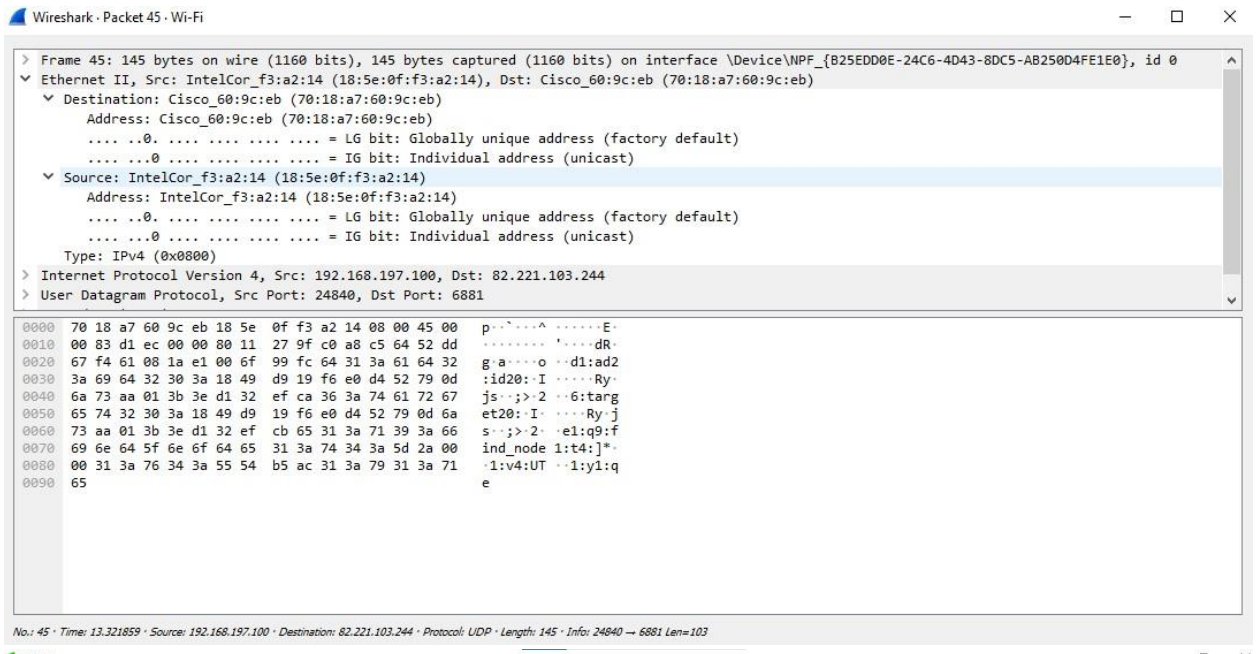

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
31 5.368515 40.69.25.12 192.168.197.100 TLSv1.2 406 Application Data
32 5.421196 192.168.197.100 40.69.25.12 TCP 54 5178 → 443 [ACK] Seq=1163 Ack=353 Win=515 Len=0
36 10.401374 192.168.197.100 95.140.228.46 TCP 66 5189 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
37 10.438120 95.140.228.46 192.168.197.100 TCP 66 80 → 5189 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=4096 SACK_PERM=1
38 10.438251 192.168.197.100 95.140.228.46 TCP 54 5189 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
39 10.441650 192.168.197.100 95.140.228.46 HTTP 224 GET /control/tags/ut.json HTTP/1.1
40 10.446034 95.140.228.46 192.168.197.100 HTTP 661 HTTP/1.1 403 Forbidden (text/html)
41 10.446197 95.140.228.46 192.168.197.100 TCP 54 80 → 5189 [FIN, ACK] Seq=608 Ack=171 Win=0 Len=0
42 10.446284 192.168.197.100 95.140.228.46 TCP 54 5189 → 80 [ACK] Seq=171 Ack=608 Win=65024 Len=0
43 10.450582 192.168.197.100 95.140.228.46 TCP 54 5189 → 80 [ACK] Seq=171 Ack=609 Win=65024 Len=0
44 10.450873 192.168.197.100 95.140.228.46 TCP 54 5189 → 80 [RST, ACK] Seq=171 Ack=609 Win=0 Len=0
Frame 4: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface \Device\NPF_{B25EDD0E-24C6-4D43-8DC5-AB250D4FE1E0}, id 0
Interface id: 0 (\Device\NPF_{B25EDD0E-24C6-4D43-8DC5-AB250D4FE1E0})
Encapsulation type: Ethernet (1)
Arrival Time: Sep 24, 2022 19:55:19.275911000 Russia TZ 2 Standard Time

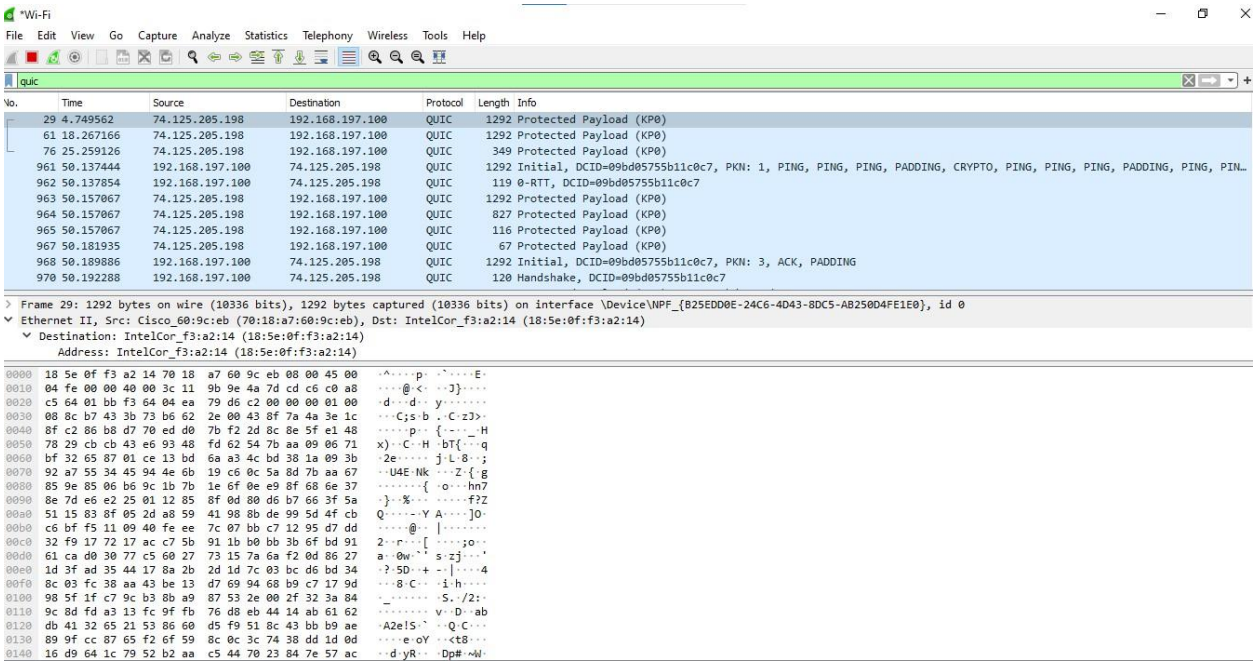

Wireshark · Packet 389 · Wi-Fi
Frame 389: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{B25EDD0E-24C6-4D43-8DC5-AB250D4FE1E0},
Ethernet II, Src: IntelCor_f3:a2:14 (18:5e:0f:f3:a2:14), Dst: Cisco_60:9c:eb (70:18:a7:60:9c:eb)
Destination: Cisco_60:9c:eb (70:18:a7:60:9c:eb)
Address: Cisco_60:9c:eb (70:18:a7:60:9c:eb)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: IntelCor_f3:a2:14 (18:5e:0f:f3:a2:14)
Address: IntelCor_f3:a2:14 (18:5e:0f:f3:a2:14)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.197.100, Dst: 95.140.228.46
Transmission Control Protocol, Src Port: 5202, Dst Port: 80, Seq: 0, Len: 0

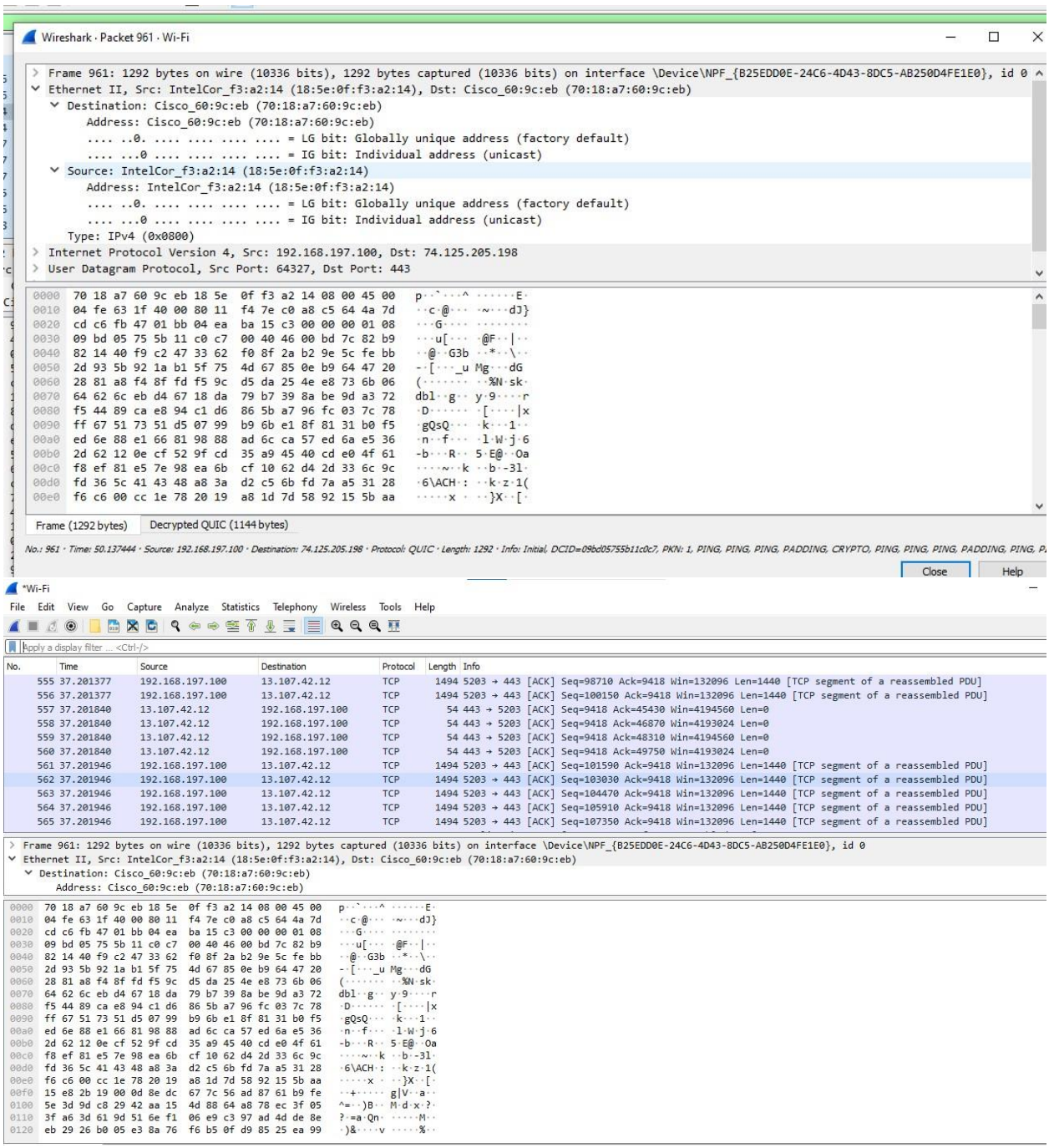

0000 70 18 a7 60 9c eb 18 5e 0f f3 a2 14 08 00 45 00
0010 00 34 bc 7d 40 00 80 06 74 7e c0 a8 c5 64 5f 8c
0020 e4 2e 14 52 00 50 f9 39 b7 db 00 00 00 00 80 02
0030 fa f0 e4 9f 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02


udp
udp
udpcp
udpencap
udplite
No. Source Destination Protocol Length Info
192.168.197.100 192.168.223.255 NBNS 92 Name query NB WPAD<00>
192.168.197.100 192.168.223.255 NBNS 92 Name query NB WPAD<00>
fe80::7082:86c:3583… ff02::1:2 DHCPv6 157 Solicit XID: 0xb64e38 CID: 000100012773cb2ef8cab83c339b
29 4.749562 74.125.205.198 192.168.197.100 QUIC 1292 Protected Payload (KP0)
33 6.285030 74.125.205.95 192.168.197.100 UDP 74 443 → 63519 Len=32
34 6.285420 192.168.197.100 74.125.205.95 UDP 76 63519 → 443 Len=34
45 13.321859 192.168.197.100 82.221.103.244 UDP 145 24840 → 6881 Len=103
46 13.322105 192.168.197.100 67.215.246.10 UDP 145 24840 → 6881 Len=103
47 16.139396 fe80::7082:86c:3583… ff02::1:2 DHCPv6 157 Solicit XID: 0xb64e38 CID: 000100012773cb2ef8cab83c339b
48 16.276109 74.125.205.95 192.168.197.100 UDP 74 443 → 63519 Len=32
49 16.276581 192.168.197.100 74.125.205.95 UDP 76 63519 → 443 Len=34
Frame 388: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF_{B25EDD0E-24C6-4D43-8DC5-AB250D4FE1E0}, id 0
Ethernet II, Src: IntelCor_f3:a2:14 (18:5e:0f:f3:a2:14), Dst: IPv6mcast_fb (33:33:00:00:00:fb)
Destination: IPv6mcast_fb (33:33:00:00:00:fb)
Address: IPv6mcast_fb (33:33:00:00:00:fb)


0000 33 33 00 00 00 fb 18 5e 0f f3 a2 14 86 dd 60 02
0010 a9 93 00 30 11 01 fe 80 00 00 00 00 00 00 70 82
0020 08 6c 35 83 05 d7 ff 02 00 00 00 00 00 00 00 00
0030 00 00 00 00 00 fb 14 e9 14 e9 00 30 d8 dc 00 00
0040 00 00 00 01 00 00 00 00 00 00 0b 5f 67 6f 6f 67
0050 6c 65 63 61 73 74 04 5f 74 63 70 05 6c 6f 63 61
0060 6c 00 00 0c 00 01


Wireshark · Packet 45 · Wi-Fi
Frame 45: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface \Device\NPF_{B25EDD0E-24C6-4D43-8DC5-AB250D4FE1E0}, id 0
Ethernet II, Src: IntelCor_f3:a2:14 (18:5e:0f:f3:a2:14), Dst: Cisco_60:9c:eb (70:18:a7:60:9c:eb)
Destination: Cisco_60:9c:eb (70:18:a7:60:9c:eb)
Address: Cisco_60:9c:eb (70:18:a7:60:9c:eb)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: IntelCor_f3:a2:14 (18:5e:0f:f3:a2:14)
Address: IntelCor_f3:a2:14 (18:5e:0f:f3:a2:14)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.197.100, Dst: 82.221.103.244
User Datagram Protocol, Src Port: 24840, Dst Port: 6881
0000 70 18 a7 60 9c eb 18 5e 0f f3 a2 14 08 00 45 00
0010 00 83 d1 ec 00 00 80 11 27 9f c0 a8 c5 64 52 dd
0020 67 f4 61 08 1a e1 00 6f 99 fc 64 31 3a 61 64 32
0030 3a 69 64 32 30 3a 18 49 d9 19 f6 e0 d4 52 79 0d
0040 6a 73 aa 01 3b 3e d1 32 ef ca 36 3a 74 61 72 67
0050 65 74 32 30 3a 18 49 d9 19 f6 e0 d4 52 79 0d 6a
0060 73 aa 01 3b 3e d1 32 ef cb 65 31 3a 71 39 3a 66
0070 69 6e 64 5f 6e 6f 64 65 31 3a 74 34 3a 5d 2a 00
0080 00 31 3a 76 34 3a 55 54 b5 ac 31 3a 79 31 3a 71
0090 65
No.: 45 · Time: 13.321859 · Source: 192.168.197.100 · Destination: 82.221.103.244 · Protocol: UDP · Length: 145 · Info: 24840 → 6881 Len=103


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
quic
No. Time Source Destination Protocol Length Info
29 4.749562 74.125.205.198 192.168.197.100 QUIC 1292 Protected Payload (KP0)
61 18.267166 74.125.205.198 192.168.197.100 QUIC 1292 Protected Payload (KP0)
76 25.259126 74.125.205.198 192.168.197.100 QUIC 349 Protected Payload (KP0)
961 50.137444 192.168.197.100 74.125.205.198 QUIC 1292 Initial, DCID=09bd05755b11c0c7, PKN: 1, PING, PING, PING, PADDING, CRYPTO, PING, PING, PING, PADDING, PING, PIN…
962 50.137854 192.168.197.100 74.125.205.198 QUIC 119 0-RTT, DCID=09bd05755b11c0c7
963 50.157067 74.125.205.198 192.168.197.100 QUIC 1292 Protected Payload (KP0)
964 50.157067 74.125.205.198 192.168.197.100 QUIC 827 Protected Payload (KP0)
965 50.157067 74.125.205.198 192.168.197.100 QUIC 116 Protected Payload (KP0)
967 50.181935 74.125.205.198 192.168.197.100 QUIC 67 Protected Payload (KP0)
968 50.189886 192.168.197.100 74.125.205.198 QUIC 1292 Initial, DCID=09bd05755b11c0c7, PKN: 3, ACK, PADDING
970 50.192288 192.168.197.100 74.125.205.198 QUIC 120 Handshake, DCID=09bd05755b11c0c7
Frame 29: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \Device\NPF_{B25EDD0E-24C6-4D43-8DC5-AB250D4FE1E0}, id 0
Ethernet II, Src: Cisco_60:9c:eb (70:18:a7:60:9c:eb), Dst: IntelCor_f3:a2:14 (18:5e:0f:f3:a2:14)
Destination: IntelCor_f3:a2:14 (18:5e:0f:f3:a2:14)
Address: IntelCor_f3:a2:14 (18:5e:0f:f3:a2:14)
0000 18 5e 0f f3 a2 14 70 18 a7 60 9c eb 08 00 45 00
0010 04 fe 00 00 40 00 3c 11 9b 9e 4a 7d cd c6 c0 a8
0020 c5 64 01 bb f3 64 04 ea 79 d6 c2 00 00 00 01 00
0030 08 8c b7 43 3b 73 b6 62 2e 00 43 8f 7a 4a 3e 1c
0040 8f c2 86 b8 d7 70 ed d0 7b f2 2d 8c 8e 5f e1 48
0050 78 29 cb cb 43 e6 93 48 fd 62 54 7b aa 09 06 71
0060 bf 32 65 87 01 ce 13 bd 6a a3 4c bd 38 1a 09 3b
0070 92 a7 55 34 45 94 4e 6b 19 c6 0c 5a 8d 7b aa 67
0080 85 9e 85 06 b6 9c 1b 7b 1e 6f 0e e9 8f 68 6e 37
0090 8e 7d e6 e2 25 01 12 85 8f 0d 80 d6 b7 66 3f 5a
00a0 51 15 83 8f 05 2d a8 59 41 98 8b de 99 5d 4f cb
00b0 c6 bf f5 11 09 40 fe ee 7c 07 bb c7 12 95 d7 dd
00c0 32 f9 17 72 17 ac c7 5b 91 1b b0 bb 3b 6f bd 91
00d0 61 ca d0 30 77 c5 60 27 73 15 7a 6a f2 0d 86 27
00e0 1d 3f ad 35 44 17 8a 2b 2d 1d 7c 03 bc d6 bd 34
00f0 8c 03 fc 38 aa 43 be 13 d7 69 94 68 b9 c7 17 9d
0100 98 5f 1f c7 9c b3 8b a9 87 53 2e 00 2f 32 3a 84
0110 9c 8d fd a3 13 fc 9f fb 76 d8 eb 44 14 ab 61 62
0120 db 41 32 65 21 53 86 60 d5 f9 51 8c 43 bb b9 ae
0130 89 9f cc 87 65 f2 6f 59 8c 0c 3c 74 38 dd 1d 0d
0140 16 d9 64 1c 79 52 b2 aa c5 44 70 23 84 7e 57 ac


Wireshark · Packet 961 · Wi-Fi
Frame 961: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \Device\NPF_{B25EDD0E-24C6-4D43-8DC5-AB250D4FE1E0}, id 0
Ethernet II, Src: IntelCor_f3:a2:14 (18:5e:0f:f3:a2:14), Dst: Cisco_60:9c:eb (70:18:a7:60:9c:eb)
Destination: Cisco_60:9c:eb (70:18:a7:60:9c:eb)
Address: Cisco_60:9c:eb (70:18:a7:60:9c:eb)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: IntelCor_f3:a2:14 (18:5e:0f:f3:a2:14)
Address: IntelCor_f3:a2:14 (18:5e:0f:f3:a2:14)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.197.100, Dst: 74.125.205.198
User Datagram Protocol, Src Port: 64327, Dst Port: 443
0000 70 18 a7 60 9c eb 18 5e 0f f3 a2 14 08 00 45 00
0010 04 fe 63 1f 40 00 80 11 f4 7e c0 a8 c5 64 4a 7d
0020 cd c6 fb 47 01 bb 04 ea ba 15 c3 00 00 00 01 08
0030 09 bd 05 75 5b 11 c0 c7 00 40 46 00 bd 7c 82 b9
0040 82 14 40 f9 c2 47 33 62 f0 8f 2a b2 9e 5c fe bb
0050 2d 93 5b 92 1a b1 5f 75 4d 67 85 0e b9 64 47 20
0060 28 81 a8 f4 8f fd f5 9c d5 da 25 4e e8 73 6b 06
0070 64 62 6c eb d4 67 18 da 79 b7 39 8a be 9d a3 72
0080 f5 44 89 ca e8 94 c1 d6 86 5b a7 96 fc 03 7c 78
0090 ff 67 51 73 51 d5 07 99 b9 6b e1 8f 81 31 b0 f5
00a0 ed 6e 88 e1 66 81 98 88 ad 6c ca 57 ed 6a e5 36
00b0 2d 62 12 0e cf 52 9f cd 35 a9 45 40 cd e0 4f 61
00c0 f8 ef 81 e5 7e 98 ea 6b cf 10 62 d4 2d 33 6c 9c
00d0 fd 36 5c 41 43 48 a8 3a d2 c5 6b fd 7a a5 31 28
00e0 f6 c6 00 cc 1e 78 20 19 a8 1d 7d 58 92 15 5b aa
Frame (1292 bytes)
Decrypted QUIC (1144 bytes)
No.: 961 · Time: 50.137444 · Source: 192.168.197.100 · Destination: 74.125.205.198 · Protocol: QUIC · Length: 1292 · Info: Initial, DCID=09bd05755b11c0c7, PKN: 1, PING, PING, PING, PADDING, CRYPTO, PING, PING, PING, PADDING, PING, P
Close
Help
*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
555 37.201377 192.168.197.100 13.107.42.12 TCP 1494 5203 → 443 [ACK] Seq=98710 Ack=9418 Win=132096 Len=1440 [TCP segment of a reassembled PDU]
556 37.201377 192.168.197.100 13.107.42.12 TCP 1494 5203 → 443 [ACK] Seq=100150 Ack=9418 Win=132096 Len=1440 [TCP segment of a reassembled PDU]
557 37.201840 13.107.42.12 192.168.197.100 TCP 54 443 → 5203 [ACK] Seq=9418 Ack=45430 Win=4194560 Len=0
558 37.201840 13.107.42.12 192.168.197.100 TCP 54 443 → 5203 [ACK] Seq=9418 Ack=46870 Win=4193024 Len=0
559 37.201840 13.107.42.12 192.168.197.100 TCP 54 443 → 5203 [ACK] Seq=9418 Ack=48310 Win=4194560 Len=0
560 37.201840 13.107.42.12 192.168.197.100 TCP 54 443 → 5203 [ACK] Seq=9418 Ack=49750 Win=4193024 Len=0
561 37.201946 192.168.197.100 13.107.42.12 TCP 1494 5203 → 443 [ACK] Seq=101590 Ack=9418 Win=132096 Len=1440 [TCP segment of a reassembled PDU]
562 37.201946 192.168.197.100 13.107.42.12 TCP 1494 5203 → 443 [ACK] Seq=103030 Ack=9418 Win=132096 Len=1440 [TCP segment of a reassembled PDU]
563 37.201946 192.168.197.100 13.107.42.12 TCP 1494 5203 → 443 [ACK] Seq=104470 Ack=9418 Win=132096 Len=1440 [TCP segment of a reassembled PDU]
564 37.201946 192.168.197.100 13.107.42.12 TCP 1494 5203 → 443 [ACK] Seq=105910 Ack=9418 Win=132096 Len=1440 [TCP segment of a reassembled PDU]
565 37.201946 192.168.197.100 13.107.42.12 TCP 1494 5203 → 443 [ACK] Seq=107350 Ack=9418 Win=132096 Len=1440 [TCP segment of a reassembled PDU]
Frame 961: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \Device\NPF_{B25EDD0E-24C6-4D43-8DC5-AB250D4FE1E0}, id 0
Ethernet II, Src: IntelCor_f3:a2:14 (18:5e:0f:f3:a2:14), Dst: Cisco_60:9c:eb (70:18:a7:60:9c:eb)
Destination: Cisco_60:9c:eb (70:18:a7:60:9c:eb)
Address: Cisco_60:9c:eb (70:18:a7:60:9c:eb)
0000 70 18 a7 60 9c eb 18 5e 0f f3 a2 14 08 00 45 00
0010 04 fe 63 1f 40 00 80 11 f4 7e c0 a8 c5 64 4a 7d
0020 cd c6 fb 47 01 bb 04 ea ba 15 c3 00 00 00 01 08
0030 09 bd 05 75 5b 11 c0 c7 00 40 46 00 bd 7c 82 b9
0040 82 14 40 f9 c2 47 33 62 f0 8f 2a b2 9e 5c fe bb
0050 2d 93 5b 92 1a b1 5f 75 4d 67 85 0e b9 64 47 20
0060 28 81 a8 f4 8f fd f5 9c d5 da 25 4e e8 73 6b 06
0070 64 62 6c eb d4 67 18 da 79 b7 39 8a be 9d a3 72
0080 f5 44 89 ca e8 94 c1 d6 86 5b a7 96 fc 03 7c 78
0090 ff 67 51 73 51 d5 07 99 b9 6b e1 8f 81 31 b0 f5
00a0 ed 6e 88 e1 66 81 98 88 ad 6c ca 57 ed 6a e5 36
00b0 2d 62 12 0e cf 52 9f cd 35 a9 45 40 cd e0 4f 61
00c0 f8 ef 81 e5 7e 98 ea 6b cf 10 62 d4 2d 33 6c 9c
00d0 fd 36 5c 41 43 48 a8 3a d2 c5 6b fd 7a a5 31 28
00e0 f6 c6 00 cc 1e 78 20 19 a8 1d 7d 58 92 15 5b aa
00f0 15 e8 2b 19 00 0d 8e dc 67 7c 56 ad 87 61 b9 fe
0100 5e 3d 9d c8 29 42 aa 15 4d 88 64 a8 78 ec 3f 05
0110 3f a6 3d 61 9d 51 6e f1 06 e9 c3 97 ad 4d de 8e
0120 eb 29 26 b0 05 e3 8a 76 f6 b5 0f d9 85 25 ea 99