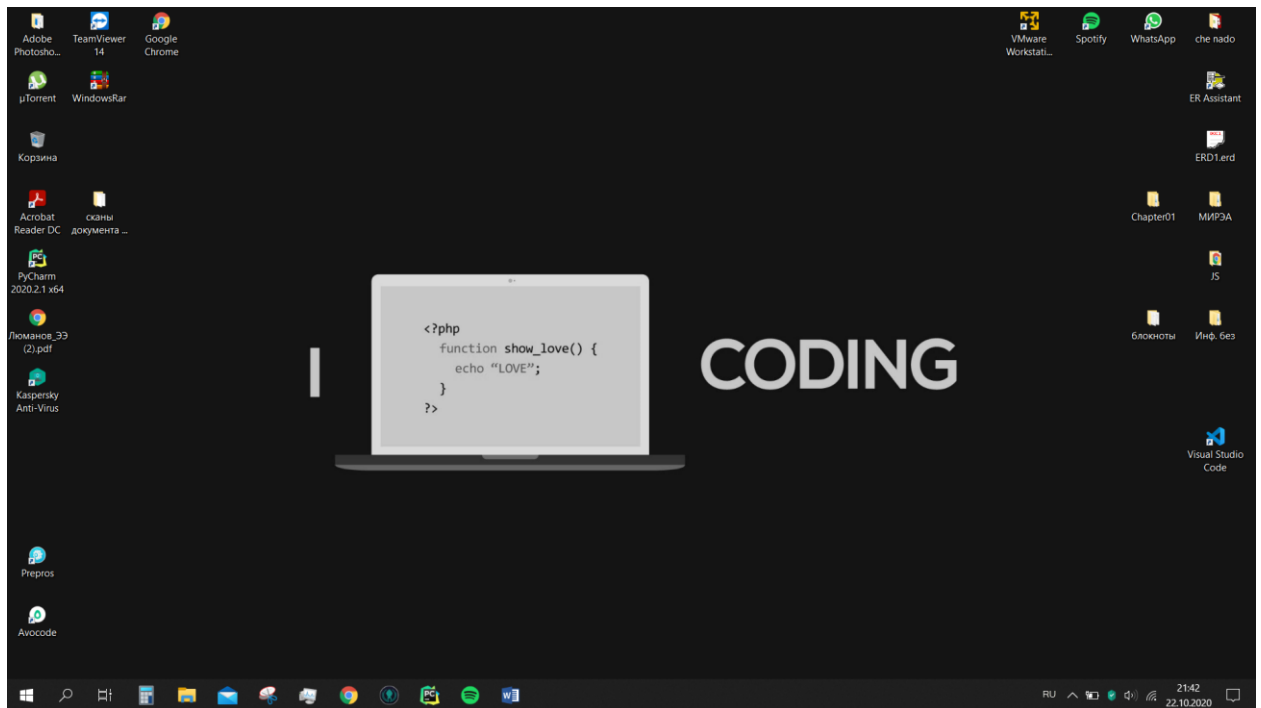


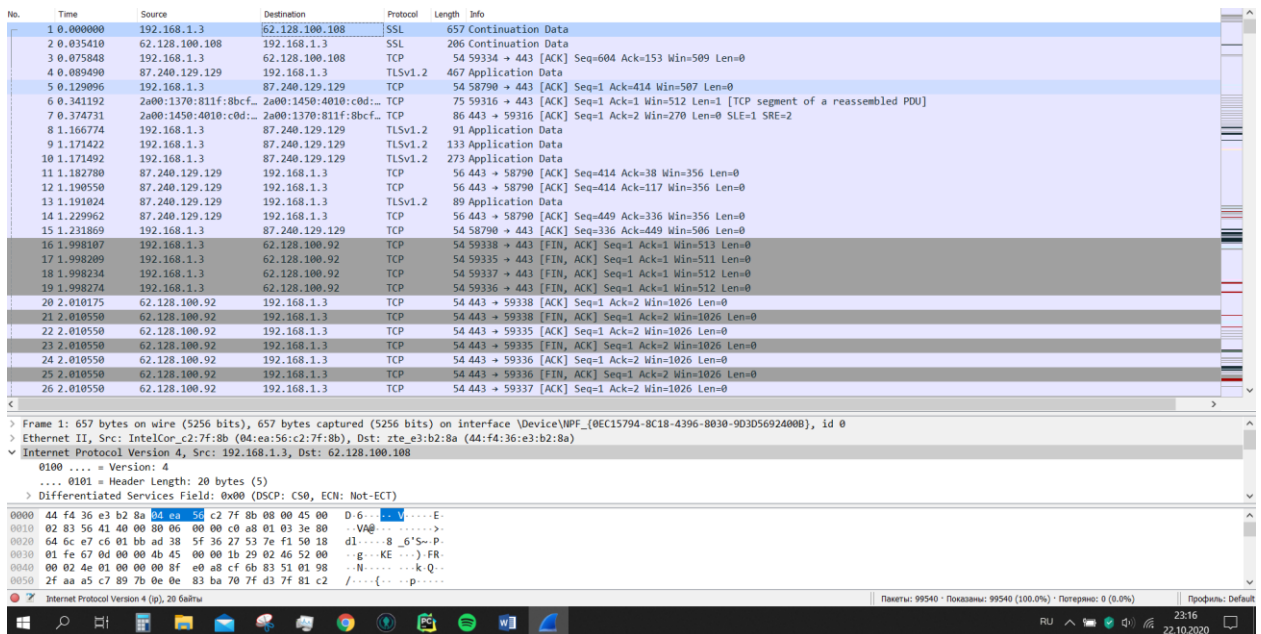
## Практическая работа №2

Рабочий стол:



Wireshark.

Задание 1:



## Задание 2:

В Wireshark представлены заголовки разных уровней протоколов, а именно:

1. Frame 1 – протокол физ. доступа
2. Ethernet II – протокол канального уровня
3. IPv4 – протокол сетевого уровня
4. UDP (User Datagram Protocol) – протокол транспортного уровня
5. Data (1238 bytes) – данные, передающиеся по сети

## Задание 3:

IP: 192.168.1.3

### Размер заголовка

Минимальный размер заголовка IP-пакет равен пяти частям, где каждое слово 32 бита, из этого следует, что обычный заголовок без дополнительных опций равен 160 бит (20 байт). Максимальное кол-во частей в заголовке равно пятнадцати.

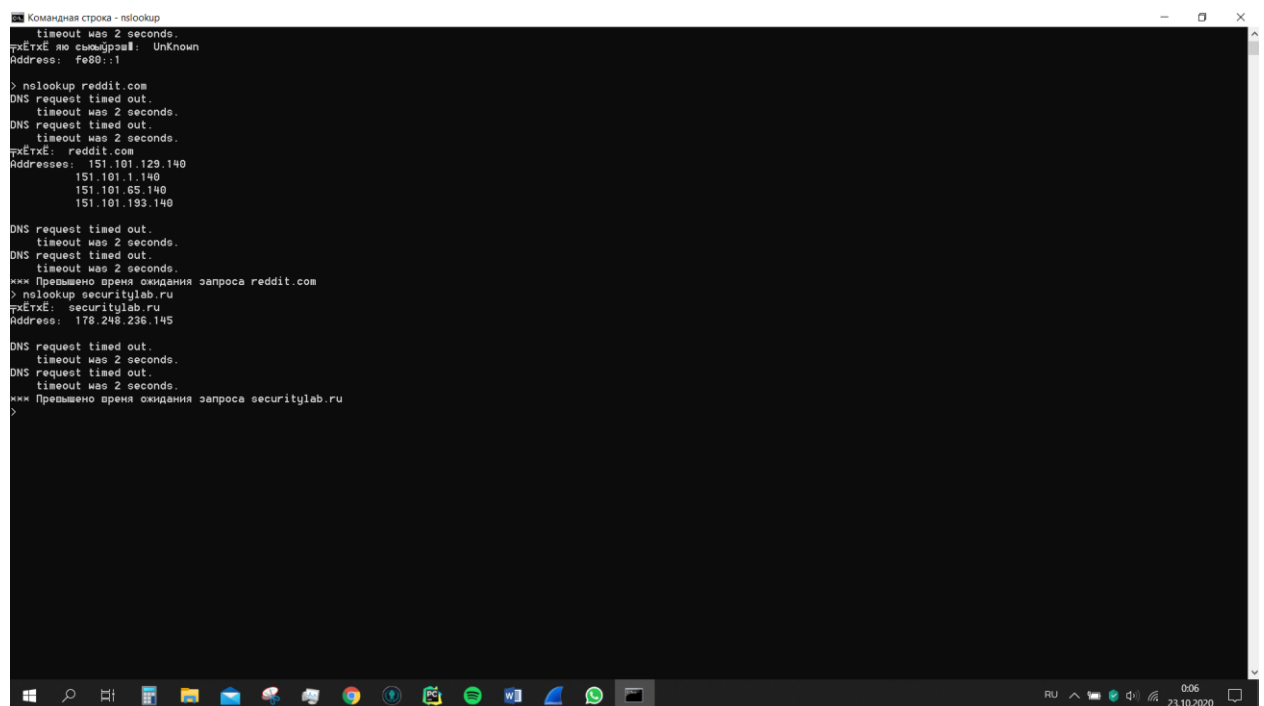
В нашем случае header length будет 20 байт, а total length 72 байт

TTL нашего пакета будет равным 128.

### DNS

## Задание 1:

Сайт - securitylab.ru



```
Командная строка - nslookup
timeout was 2 seconds.
тхЕтхЕ: яю сым/ррш: Unknown
Address: fe80::1

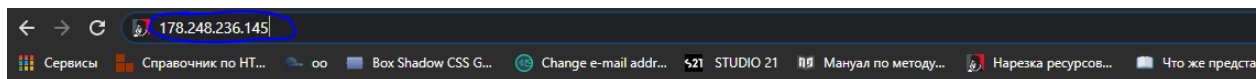
> nslookup reddit.com
DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
тхЕтхЕ: reddit.com
Addresses: 151.101.129.140
151.101.1.140
151.101.65.140
151.101.193.140

DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
*** Превышено время ожидания запроса reddit.com
> nslookup securitylab.ru
тхЕтхЕ: securitylab.ru
Address: 178.248.236.145

DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
*** Превышено время ожидания запроса securitylab.ru
>
```

## Задание 2:

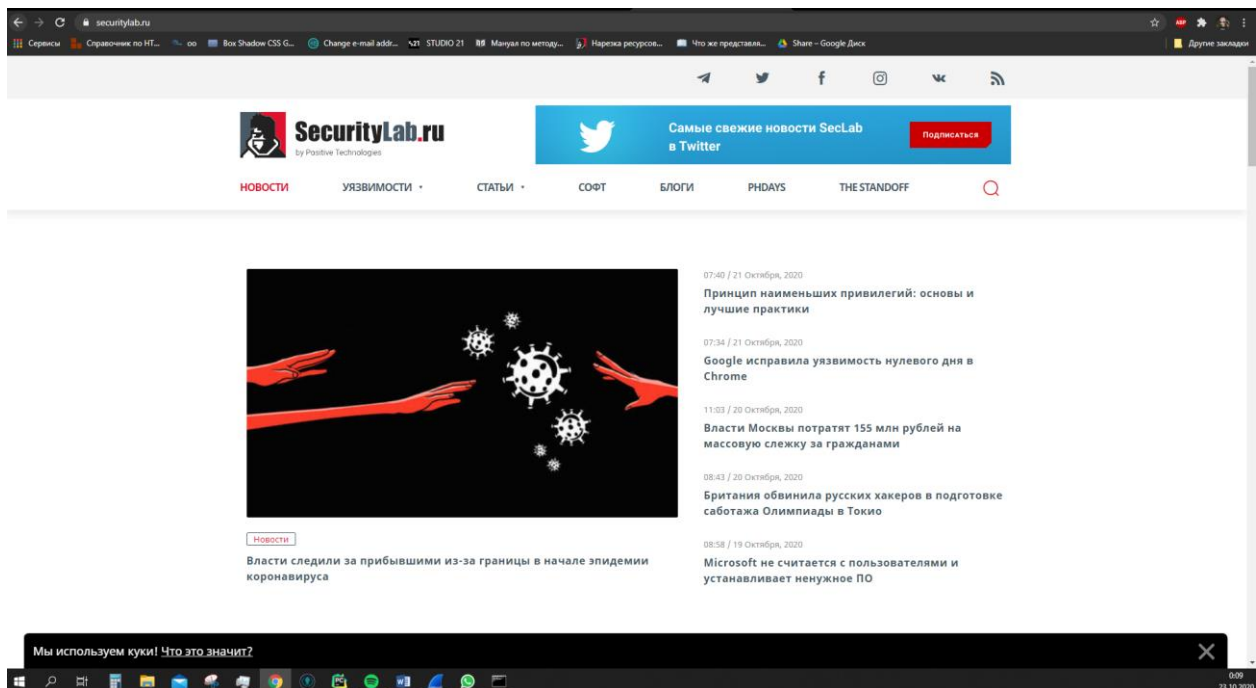
Перейти по данному IP-адресу, полученному с помощью утилиты nslookup



Google Search

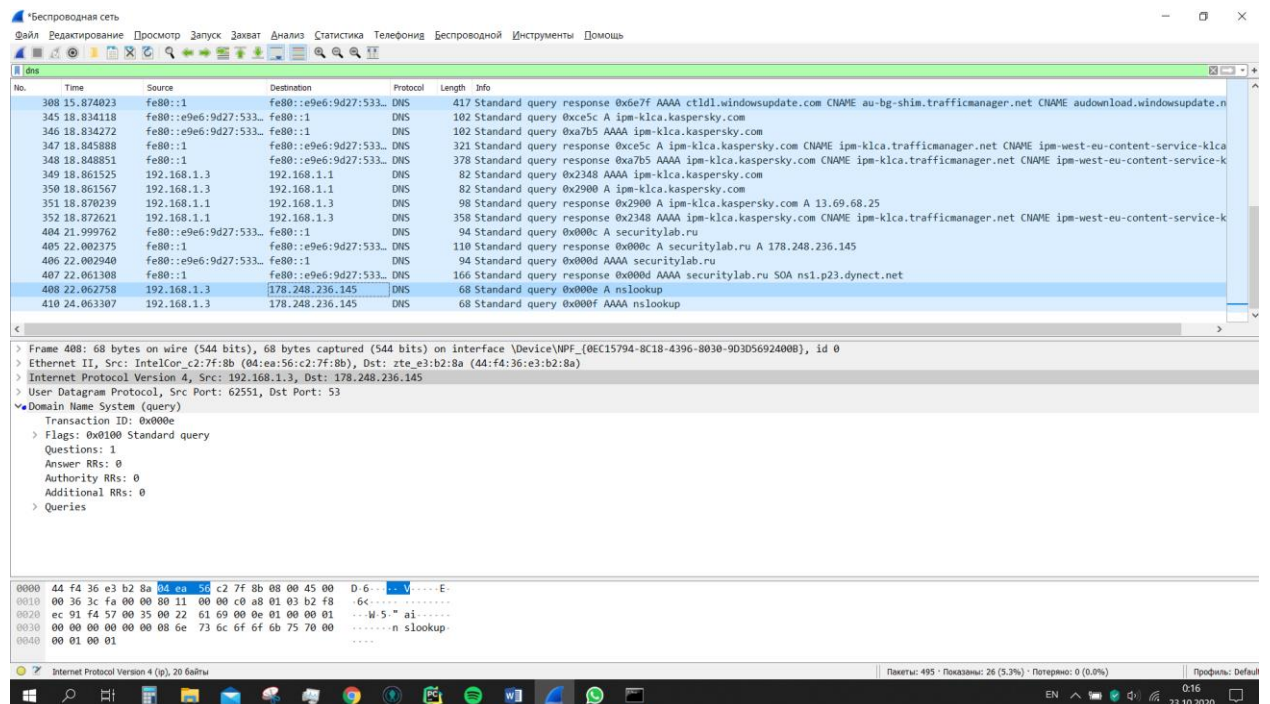
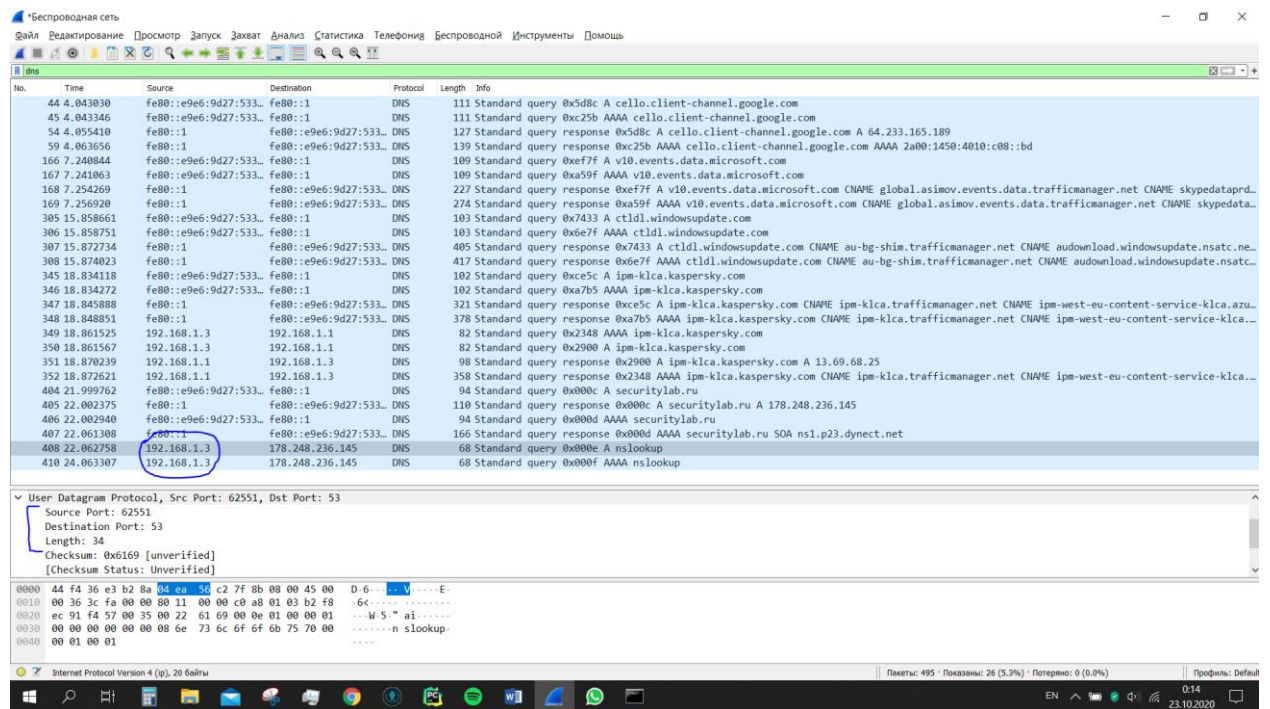
I'm Feeling Lucky

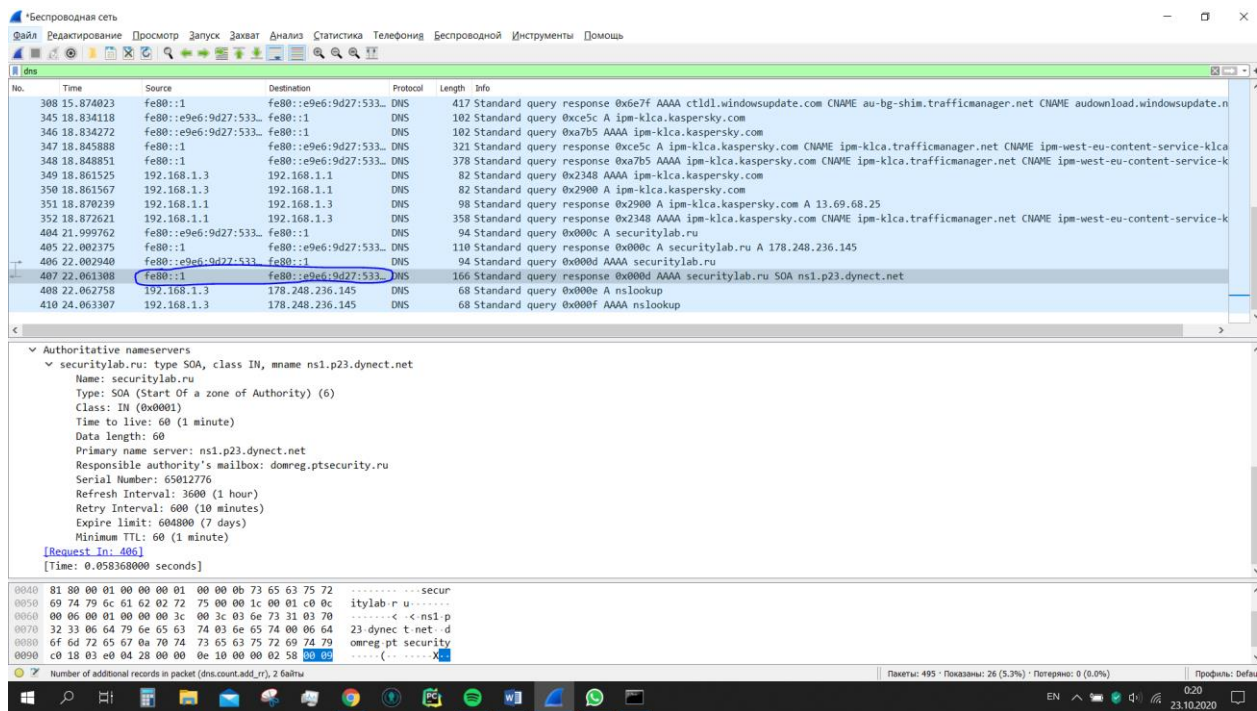
Google offered in: [русский](#)



### Задание 3:

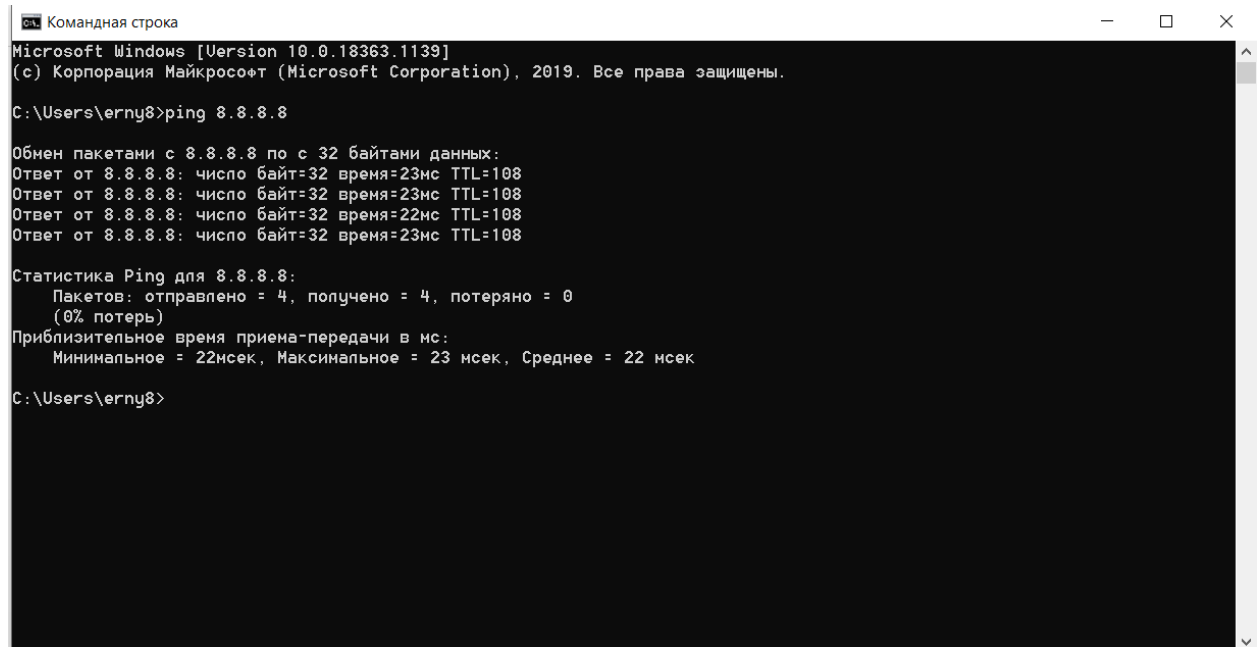
Запустить Wireshark установить фильтр по протоколу DNS, повтор запроса на выбранный сайт, с помощью nslookup.





## ICMP:

Запустить Wireshark, установить фильтр по протоколу ICMP и запустить сетевую утилиту Ping.





Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

icmp

No.	Time	Source	Destination	Protocol	Length	Info
401	8.784736	192.168.1.3	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 402)
402	8.807936	8.8.8.8	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=9/2304, ttl=108 (request in 401)
403	9.789326	192.168.1.3	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=10/2500, ttl=128 (reply in 404)
404	9.812497	8.8.8.8	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=10/2500, ttl=108 (request in 403)
410	10.792999	192.168.1.3	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, ttl=128 (reply in 411)
411	10.815739	8.8.8.8	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=11/2816, ttl=108 (request in 410)
412	11.797268	192.168.1.3	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, ttl=128 (reply in 413)
413	11.819611	8.8.8.8	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=12/3072, ttl=108 (request in 412)

Frame 401: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{0EC15794-8C18-4396-8030-903D56924008}, id 0

Interface id: 0 (\Device\NPF\_{0EC15794-8C18-4396-8030-903D56924008})

Encapsulation type: Ethernet (1)

Arrival Time: Oct 23, 2020 00:26:44.047235000 RTZ 2 (зима)

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1603482004.047235000 seconds

[Time delta from previous captured frame: 0.564887000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 8.784736000 seconds]

Frame Number: 401

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]

0000 44 f4 36 e3 b2 8a 04 ea 56 c2 7f 8b 08 00 45 00 D-6-----V-----E-

0010 00 3c b7 e1 00 00 01 00 00 c0 a8 01 03 08 08 -<-----

0020 08 08 08 00 4d 52 00 01 00 09 61 62 63 64 65 66 ---MR---abcdef

0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmopqrstuv

0040 77 61 62 63 64 65 66 67 68 69 wabdefgh

Wireshark: Беспроводная сеть\_20201023002633\_00552.pcapng

Пакеты: 450 - Показаны: 8 (1.8%)

Профиль: Default

RU 028 23.10.2020

## Запустить утилиту ping с флагом '-i 1'

icmp

No.	Time	Source	Destination	Protocol	Length	Info
6	4.073796	192.168.1.3	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=17/4352, ttl=1 (no response found!)
22	8.965565	192.168.1.3	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=18/4352, ttl=1 (no response found!)
50	13.964950	192.168.1.3	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=19/4352, ttl=1 (no response found!)
66	18.965273	192.168.1.3	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=20/4352, ttl=1 (no response found!)

Ethernet II, Src: IntelCor\_c2:7f:8b (04:ea:56:c2:7f:8b), Dst: 08:00:00:00:00:00 (00:00:00:00:00:00)

Internet Protocol Version 4, Src: 192.168.1.3, Dst: 8.8.8.8

0100 .... = Version: 4

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

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: 0)

Total Length: 60

Identification: 0xb7eb (47083)

Flags: 0x0000

Fragment offset: 0

> Time to live: 1

Protocol: ICMP (1)

Header checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.3

Destination: 8.8.8.8

Internet Control Message Protocol (icmp), 40 bytes

0000 44 f4 36 e3 b2 8a 04 ea 56 c2 7f 8b 08 00 45 00 D-6-----V-----E-

0010 00 3c b7 eb 00 00 01 01 00 00 c0 a8 01 03 08 08 -<-----

0020 08 08 08 00 4d 48 00 01 00 13 61 62 63 64 65 66 ---MR---abcdef

0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmopqrstuv

0040 77 61 62 63 64 65 66 67 68 69 wabdefgh

Internet Control Message Protocol (icmp), 40 bytes

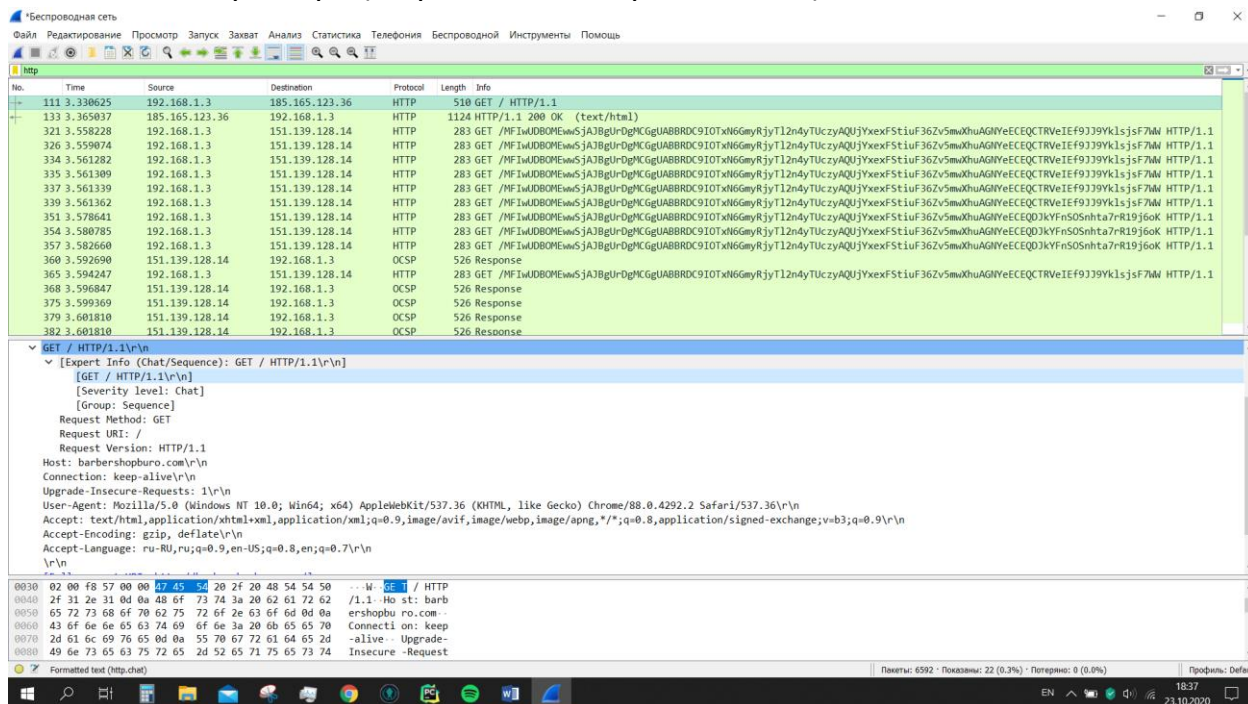
Пакеты: 3376 - Показаны: 4 (0.1%) - Потеряно: 0 (0.0%)

Профиль: Default

EN 035 23.10.2020

## HTTP:

Взял сайт из примера (<http://barbershopburo.com/>)



IP-адрес компьютера 192.168.1.3

IP-адрес сервера 185.165.123.36

Версия HTTP 1.1

Код состояния - 200 (успешное)

### ✓ Hypertext Transfer Protocol

#### ✓ HTTP/1.1 200 OK\r\n

##### ✓ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

[HTTP/1.1 200 OK\r\n]

[Severity level: Chat]

[Group: Sequence]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Server: nginx\r\n

Date: Fri, 23 Oct 2020 15:36:11 GMT\r\n

Content-Type: text/html; charset=UTF-8\r\n

Размер запроса – 4123 lines (text/html)