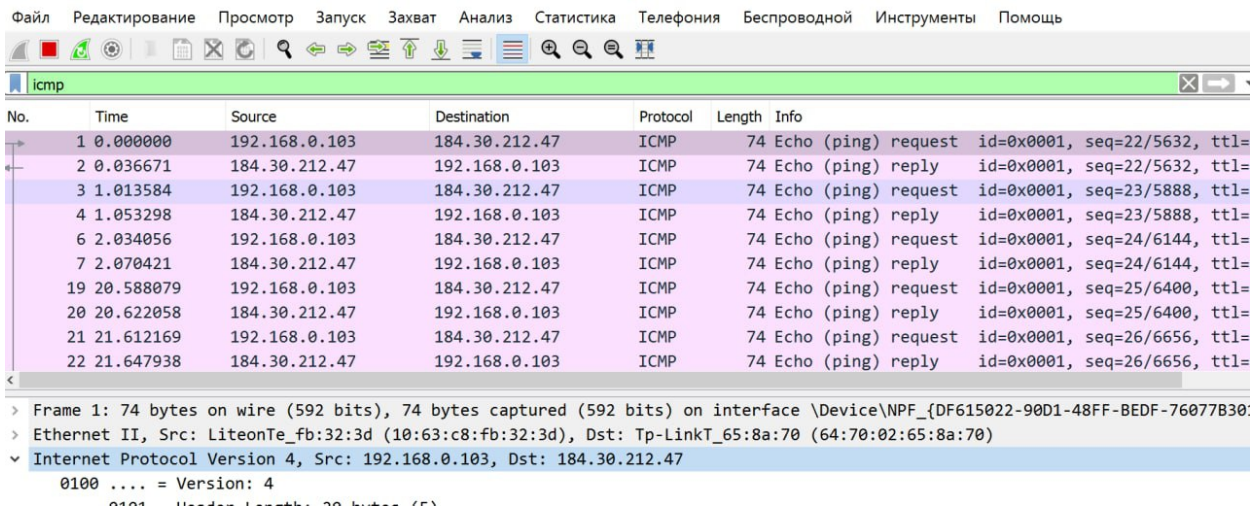


Wireshark (лабораторная 9)

Ping

1) Src: 192.168.0.103, Dst: 184.30.212.47



The screenshot shows the Wireshark interface with a packet capture of ICMP ping traffic. The packet list table is as follows:

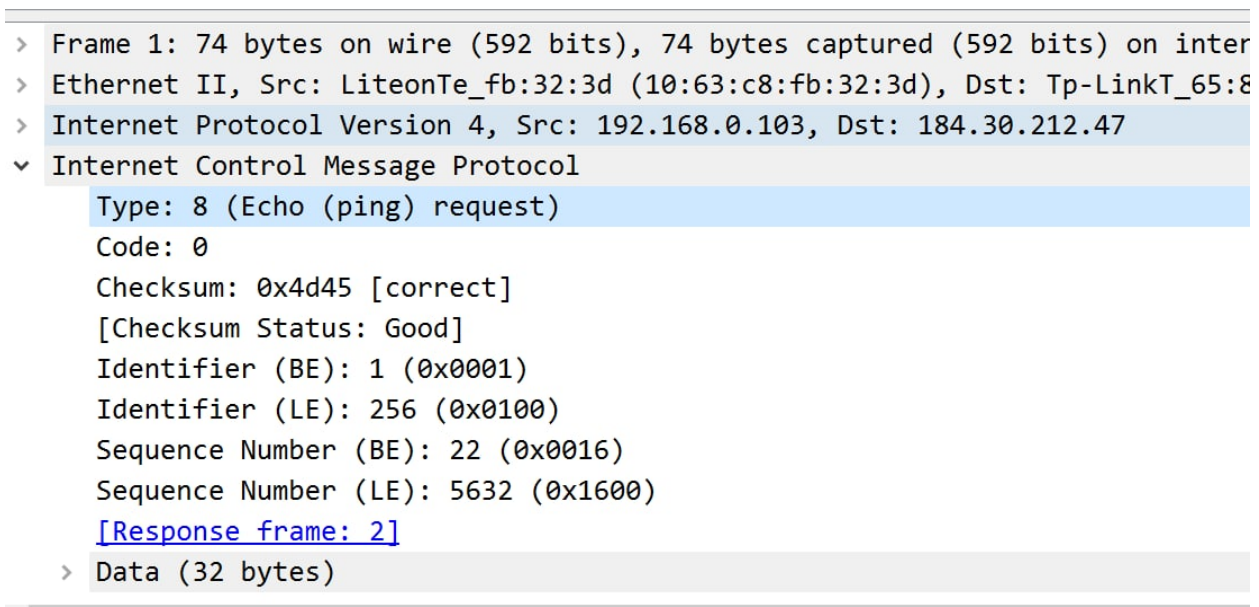
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.103	184.30.212.47	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=
2	0.036671	184.30.212.47	192.168.0.103	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=
3	1.013584	192.168.0.103	184.30.212.47	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=
4	1.053298	184.30.212.47	192.168.0.103	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=
6	2.034056	192.168.0.103	184.30.212.47	ICMP	74	Echo (ping) request id=0x0001, seq=24/6144, ttl=
7	2.070421	184.30.212.47	192.168.0.103	ICMP	74	Echo (ping) reply id=0x0001, seq=24/6144, ttl=
19	20.588079	192.168.0.103	184.30.212.47	ICMP	74	Echo (ping) request id=0x0001, seq=25/6400, ttl=
20	20.622058	184.30.212.47	192.168.0.103	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400, ttl=
21	21.612169	192.168.0.103	184.30.212.47	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=
22	21.647938	184.30.212.47	192.168.0.103	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=

The packet details pane for the selected packet (No. 1) shows:

- Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{DF615022-90D1-48FF-BEDF-76077B30:}
- Ethernet II, Src: LiteonTe_fb:32:3d (10:63:c8:fb:32:3d), Dst: Tp-LinkT_65:8a:70 (64:70:02:65:8a:70)
- Internet Protocol Version 4, Src: 192.168.0.103, Dst: 184.30.212.47
- 0100 = Version: 4
- 0001 ... = Header Length: 20 bytes (5)

2) Потому что это протокол сетевого уровня, а не транспортного

3) Type: 8 (Echo (ping) request), Code: 0. Еще поля: Checksum, Identifier (BE), Identifier (LE), Sequence Number (BE), Sequence Number (LE), Data. На поля контрольной суммы, порядкового номера и идентификатора приходится по 2 байта.



The screenshot shows the packet details pane for the first ICMP ping request (Frame 1). The details are as follows:

- Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on inter
- Ethernet II, Src: LiteonTe_fb:32:3d (10:63:c8:fb:32:3d), Dst: Tp-LinkT_65:8
- Internet Protocol Version 4, Src: 192.168.0.103, Dst: 184.30.212.47
- Internet Control Message Protocol
 - Type: 8 (Echo (ping) request)
 - Code: 0
 - Checksum: 0x4d45 [correct]
 - [Checksum Status: Good]
 - Identifier (BE): 1 (0x0001)
 - Identifier (LE): 256 (0x0100)
 - Sequence Number (BE): 22 (0x0016)
 - Sequence Number (LE): 5632 (0x1600)
 - [\[Response frame: 2\]](#)
 - Data (32 bytes)

4) Type: 0 (Echo (ping) reply), код 0. Все остальное такое же и тоже по 2 байта.

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.103	184.30.212.47	ICMP	74	Echo (ping) request id=0
2	0.036671	184.30.212.47	192.168.0.103	ICMP	74	Echo (ping) reply id=0
3	1.013584	192.168.0.103	184.30.212.47	ICMP	74	Echo (ping) request id=0
4	1.052200	184.30.212.47	192.168.0.103	ICMP	74	Echo (ping) reply id=0

> Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{DF615022-...}
 > Ethernet II, Src: Tp-LinkT_65:8a:70 (64:70:02:65:8a:70), Dst: LiteonTe_fb:32:3d (10:63:c8:fb:32:3d)
 > Internet Protocol Version 4, Src: 184.30.212.47, Dst: 192.168.0.103
 > Internet Control Message Protocol
 Type: 0 (Echo (ping) reply)
 Code: 0
 Checksum: 0x5545 [correct]
 [Checksum Status: Good]
 Identifier (BE): 1 (0x0001)
 Identifier (LE): 256 (0x0100)
 Sequence Number (BE): 22 (0x0016)
 Sequence Number (LE): 5632 (0x1600)
 [Request frame: 1]
 [Response time: 36,671 ms]
 > Data (32 bytes)

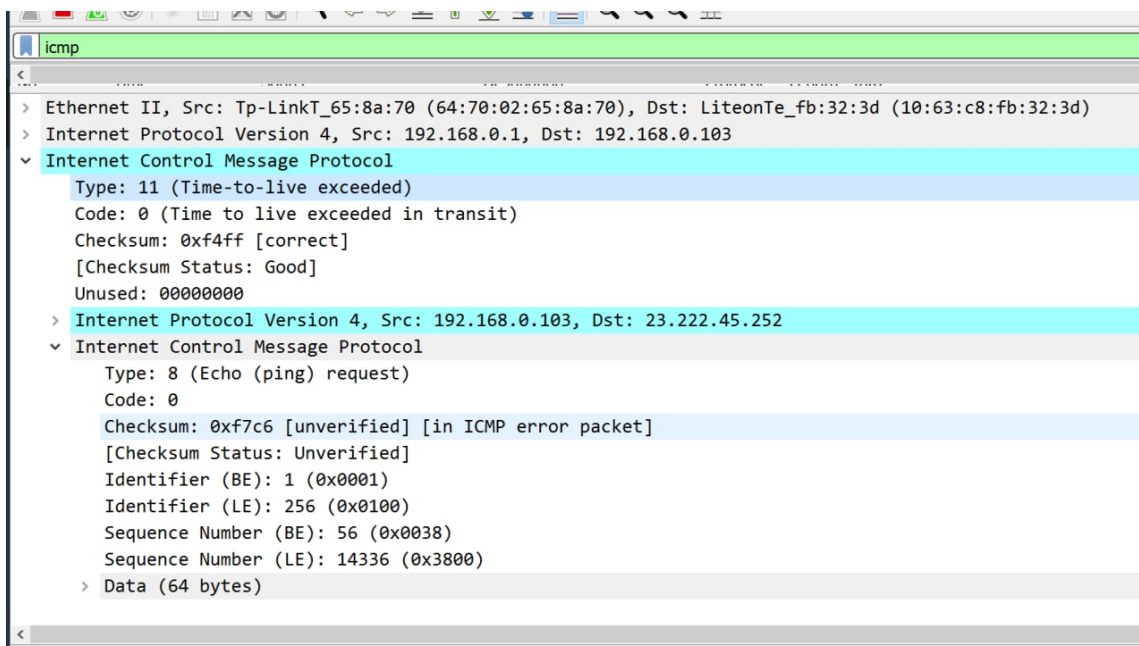
Traceroute

1) Не отличается

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
5	0.080948	192.168.0.103	23.222.45.252	ICMP	106	Echo (ping) request id=0x0001, seq=56
6	0.083845	192.168.0.1	192.168.0.103	ICMP	134	Time-to-live exceeded (Time to live ex
7	0.088806	192.168.0.103	23.222.45.252	ICMP	106	Echo (ping) request id=0x0001, seq=57
8	0.091100	192.168.0.1	192.168.0.103	ICMP	134	Time-to-live exceeded (Time to live ex
9	0.093549	192.168.0.103	23.222.45.252	ICMP	106	Echo (ping) request id=0x0001, seq=58

> Frame 5: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{DF615022-90D1-48FF-...}
 > Ethernet II, Src: LiteonTe_fb:32:3d (10:63:c8:fb:32:3d), Dst: Tp-LinkT_65:8a:70 (64:70:02:65:8a:70)
 > Internet Protocol Version 4, Src: 192.168.0.103, Dst: 23.222.45.252
 > Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0xf7c6 [correct]
 [Checksum Status: Good]
 Identifier (BE): 1 (0x0001)
 Identifier (LE): 256 (0x0100)
 Sequence Number (BE): 56 (0x0038)
 Sequence Number (LE): 14336 (0x3800)
 > [No response seen]
 > Data (64 bytes)

2) Появилось поле Unused, TTL, тип запроса изменился, информация о IP и ICMP эхо-запроса



3) В последних трёх пакетах имеется поле Response time, тип пакета 0, а не 11, как в пакете с ошибкой. Нет информации об ICMP эхо-запроса. Чексумма другая, длина.

4) Как видим, в какой-то момент время ожидания возрастает. Наверное, несколько первых маршрутизаторов находятся близко (рядом с СПб). А уже следующие далеко. Видно, что один из них в Амстердаме. Последующие сложно определить.

```
C:\WINDOWS\system32\cmd.exe
с максимальным числом прыжков 30:

 1  202 ms   45 ms   3 ms  192-168-0-1.local [192.168.0.1]
 2    8 ms    3 ms    3 ms  185-171-192-137.obit.ru [185.171.192.137]
 3    7 ms    3 ms    3 ms  vi-xx-1917.4900m.250.179.spb.obit.ru [172.29.192.38]
 4    6 ms    4 ms    3 ms  vi-xx-1916.zs33.126.95.spb.obit.ru [172.29.194.16]
 5    8 ms    3 ms    8 ms  vi-xx-1911.4900m.250.160.spb.obit.ru [172.29.192.213]
 6    9 ms    5 ms    6 ms  vi-xx-1920.ohr1.spb.obit.ru [172.29.194.77]
 7    5 ms    4 ms    4 ms  ^C

C:\Users\Lenovo>tracert mit.edu

Трассировка маршрута к mit.edu [23.222.45.252]
с максимальным числом прыжков 30:

 1    3 ms    2 ms    2 ms  192-168-0-1.local [192.168.0.1]
 2    7 ms    5 ms    3 ms  185-171-192-137.obit.ru [185.171.192.137]
 3    7 ms    3 ms    3 ms  vi-xx-1917.4900m.250.179.spb.obit.ru [172.29.192.38]
 4    7 ms    3 ms    4 ms  vi-xx-1916.zs33.126.95.spb.obit.ru [172.29.194.16]
 5    6 ms    3 ms    2 ms  vi-xx-1911.4900m.250.160.spb.obit.ru [172.29.192.213]
 6    6 ms    3 ms    7 ms  vi-xx-1920.ohr1.spb.obit.ru [172.29.194.77]
 7    6 ms    3 ms    3 ms  172.29.194.90
 8   12 ms    9 ms    7 ms  172.29.194.157
 9   14 ms    4 ms    7 ms  vi-xx-1664.zs33.250.59.spb.obit.ru [172.29.194.109]
10    3 ms    3 ms    4 ms  vi-xx-1692.brc1.spb.obit.ru [172.29.194.37]
11    7 ms    4 ms    4 ms  62.105.151.13
12   54 ms   53 ms   52 ms  mx01.Amsterdam.gldn.net [79.104.225.62]
13   54 ms   50 ms   57 ms  amsix-ams9.netarch.akamai.com [80.249.208.168]
14   62 ms   58 ms   57 ms  a23-222-45-252.deploy.static.akamaitechnologies.com [23.222.45.252]

Трассировка завершена.

C:\Users\Lenovo>
```