

1. Wireshark: ICMP.

1. Ping (4 балла)

1.

No.	Time	Source	Destination	Protocol	Length	Info
330	11.667775376	192.168.0.104	72.167.191.69	ICMP	98	Echo (ping) request id=0x0003,

IP-адрес моего хоста - 192.168.0.104, хоста назначения - 72.167.191.69

2. Потому что ICMP – это протокол сетевого уровня

3.

330	11.667775376	192.168.0.104	72.167.191.69	ICMP	98	Echo (ping) request id=0x0003, seq=1/256, ttl=64 (re
331	11.875371070	72.167.191.69	192.168.0.104	ICMP	98	Echo (ping) reply id=0x0003, seq=1/256, ttl=242 (re
342	12.668557003	192.168.0.104	72.167.191.69	ICMP	98	Echo (ping) request id=0x0003, seq=2/512, ttl=64 (re
348	12.853391459	72.167.191.69	192.168.0.104	ICMP	98	Echo (ping) reply id=0x0003, seq=2/512, ttl=242 (re
351	13.670366057	192.168.0.104	72.167.191.69	ICMP	98	Echo (ping) request id=0x0003, seq=3/768, ttl=64 (re
352	13.923488155	72.167.191.69	192.168.0.104	ICMP	98	Echo (ping) reply id=0x0003, seq=3/768, ttl=242 (re
375	14.671471845	192.168.0.104	72.167.191.69	ICMP	98	Echo (ping) request id=0x0003, seq=4/1024, ttl=64 (re
376	14.947415470	72.167.191.69	192.168.0.104	ICMP	98	Echo (ping) reply id=0x0003, seq=4/1024, ttl=242 (r

Ethernet II, Src: IntelCor_a6:38:ad (fc:b3:bc:a6:38:ad), Dst: TendaTec_d1:f2:70 (50:0f:f5:d1:f2:70)

Internet Protocol Version 4, Src: 192.168.0.104, Dst: 72.167.191.69

Internet Control Message Protocol

- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0xc450 [correct]
- [Checksum Status: Good]
- Identifier (BE): 3 (0x0003)
- Identifier (LE): 768 (0x0300)
- Sequence Number (BE): 1 (0x0001)
- Sequence Number (LE): 256 (0x0100)
- [Response frame: 331]
- Timestamp from icmp data: Apr 23, 2022 17:33:23.000000000 MSK
- [Timestamp from icmp data (relative): 0.550907102 seconds]
- Data (48 bytes)

ICMP-тип – 8, кодовый номер (Code) – 0.

Помимо Type и Code в пакете содержатся поля: Checksum, Identifier (BE), Identifier (LE), Sequence Number (BE), Sequence Number (LE). Все эти поля занимают 2 байта.

4.

No.	Time	Source	Destination	Protocol	Length	Info
330	11.667775376	192.168.0.104	72.167.191.69	ICMP	98	Echo (ping) request id=0x0003, seq=1/256, ttl=64 (re
331	11.875371070	72.167.191.69	192.168.0.104	ICMP	98	Echo (ping) reply id=0x0003, seq=1/256, ttl=242 (r
342	12.668557003	192.168.0.104	72.167.191.69	ICMP	98	Echo (ping) request id=0x0003, seq=2/512, ttl=64 (re
348	12.853391459	72.167.191.69	192.168.0.104	ICMP	98	Echo (ping) reply id=0x0003, seq=2/512, ttl=242 (r
351	13.670366057	192.168.0.104	72.167.191.69	ICMP	98	Echo (ping) request id=0x0003, seq=3/768, ttl=64 (re
352	13.923488155	72.167.191.69	192.168.0.104	ICMP	98	Echo (ping) reply id=0x0003, seq=3/768, ttl=242 (r
375	14.671471845	192.168.0.104	72.167.191.69	ICMP	98	Echo (ping) request id=0x0003, seq=4/1024, ttl=64 (r
376	14.947415470	72.167.191.69	192.168.0.104	ICMP	98	Echo (ping) reply id=0x0003, seq=4/1024, ttl=242 (r

Internet Control Message Protocol

- Type: 0 (Echo (ping) reply)
- Code: 0
- Checksum: 0xcc50 [correct]
- [Checksum Status: Good]
- Identifier (BE): 3 (0x0003)
- Identifier (LE): 768 (0x0300)
- Sequence Number (BE): 1 (0x0001)
- Sequence Number (LE): 256 (0x0100)
- [Request frame: 330]
- [Response time: 207.596 ms]
- Timestamp from icmp data: Apr 23, 2022 17:33:23.000000000 MSK
- [Timestamp from icmp data (relative): 0.758502796 seconds]
- Data (48 bytes)

0020 00 68 00 00 cc 50 00 03 00 01 33 0e 64 62 00 00 .h...P...3.db..
0030 00 00 d5 67 08 00 00 00 00 00 10 11 12 13 14 15 ...g.....

ICMP-тип – 0, кодовый номер – 0.

Помимо Type и Code в пакете содержатся поля: Checksum, Identifier (BE), Identifier (LE), Sequence Number (BE), Sequence Number (LE). Все эти поля занимают 2 байта.

2. Traceroute (4 балла).

1.

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
46	5.565354881	192.168.0.104	72.167.191.69	ICMP	74	Echo (ping) request id=0x0005, seq=1/256, ttl=1 (no response seen)
47	5.565383652	192.168.0.104	72.167.191.69	ICMP	74	Echo (ping) request id=0x0005, seq=2/512, ttl=1 (no response seen)
48	5.565390260	192.168.0.104	72.167.191.69	ICMP	74	Echo (ping) request id=0x0005, seq=3/768, ttl=1 (no response seen)
49	5.565397578	192.168.0.104	72.167.191.69	ICMP	74	Echo (ping) request id=0x0005, seq=4/1024, ttl=2 (no response seen)

Frame 46: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface wlp0s20f3, id 0
Ethernet II, Src: IntelCor_a6:38:ad (fc:b3:bc:a6:38:ad), Dst: TendaTec_d1:f2:70 (50:0f:f5:d1:f2:70)
Internet Protocol Version 4, Src: 192.168.0.104, Dst: 72.167.191.69
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x8274 [correct]
[Checksum Status: Good]
Identifier (BE): 5 (0x0005)
Identifier (LE): 1280 (0x0500)
Sequence Number (BE): 1 (0x0001)
Sequence Number (LE): 256 (0x0100)
[No response seen]
Data (32 bytes)

ICMP-пакеты с traceroute-запросами отличаются от ICMP-пакетов с ping-запросами значениями ttl (в первом случае в последовательности пакетов можно проследить целый диапазон ttl от 1 до 242, а во втором он всегда равен 64), размером поля Data (в первом случае это 32 байта, а во втором – 48 байт), а также тем, что на все ping-запросы были получены ответы, что не так в случае traceroute.

2.

icmp						
Time	Source	Destination	Protocol	Length	Info	
5.565475943	192.168.0.104	72.167.191.69	ICMP	74	Echo (ping) request	id=0x0005, seq=16/4096, ttl=6 (no response seen)
5.567785942	192.168.0.1	192.168.0.104	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
5.567887490	192.168.0.1	192.168.0.104	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
5.568207396	192.168.0.1	192.168.0.104	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
5.568631441	192.168.0.104	72.167.191.69	ICMP	74	Echo (ping) request	id=0x0005, seq=17/4352, ttl=6 (no response seen)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.104
Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0x6a85 [correct]
[Checksum Status: Good]
Unused: 00000000
Internet Protocol Version 4, Src: 192.168.0.104, Dst: 72.167.191.69
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x8274 [unverified] [in ICMP error packet]
[Checksum Status: Unverified]
Identifier (BE): 5 (0x0005)
Identifier (LE): 1280 (0x0500)
Sequence Number (BE): 1 (0x0001)
Sequence Number (LE): 256 (0x0100)

В доп. полях содержатся данные IPv4 и ICMP исходного запроса.

3.

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
128	7.392211320	192.168.0.104	72.167.191.69	ICMP	74	Echo (ping) request id=0x0005, seq=49/12544, ttl=17
129	7.392217856	192.168.0.104	72.167.191.69	ICMP	74	Echo (ping) request id=0x0005, seq=50/12800, ttl=17
130	7.392224002	192.168.0.104	72.167.191.69	ICMP	74	Echo (ping) request id=0x0005, seq=51/13056, ttl=17
131	7.392231472	192.168.0.104	72.167.191.69	ICMP	74	Echo (ping) request id=0x0005, seq=52/13312, ttl=18
132	7.680029345	72.167.191.69	192.168.0.104	ICMP	74	Echo (ping) reply id=0x0005, seq=49/12544, ttl=242
133	7.680029690	72.167.191.69	192.168.0.104	ICMP	74	Echo (ping) reply id=0x0005, seq=50/12800, ttl=242
134	7.680029742	72.167.191.69	192.168.0.104	ICMP	74	Echo (ping) reply id=0x0005, seq=51/13056, ttl=242
135	7.680029797	72.167.191.69	192.168.0.104	ICMP	74	Echo (ping) reply id=0x0005, seq=52/13312, ttl=242

Frame 133: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface wlp0s20f3, id 0
 Ethernet II, Src: TendaTec_d1:f2:70 (50:0f:f5:d1:f2:70), Dst: IntelCor_a6:38:ad (fc:b3:bc:a6:38:ad)
 Internet Protocol Version 4, Src: 72.167.191.69, Dst: 192.168.0.104
 Internet Control Message Protocol
 Type: 0 (Echo (ping) reply)
 Code: 0
 Checksum: 0x8a43 [correct]
 [Checksum Status: Good]
 Identifier (BE): 5 (0x0005)
 Identifier (LE): 1280 (0x0500)
 Sequence Number (BE): 50 (0x0032)
 Sequence Number (LE): 12800 (0x3200)
 [Request frame: 129]
 [Response time: 287.812 ms]

Отличия: тип пакета (в данном случае он равен 0), отсутствие доп. полей, которые были в пакетах, сообщающих об ошибках.

Эти отличия объясняются тем, что ошибок не произошло, т.е. все три запроса дошли до нужного хоста, а хост в свою очередь отослал три ответа.

4.

```
[dword@fedora ~]$ traceroute -I amazon.com
traceroute to amazon.com (205.251.242.103), 30 hops max, 60 byte packets
 1 _gateway (192.168.0.1)  2.755 ms  2.810 ms  3.139 ms
 2 vlan591.schevchenko.bb.pu.ru (81.89.176.1)  10.774 ms  11.116 ms  11.168 ms
 3 vlan3.kronos.pu.ru (195.70.196.3)  6.268 ms  6.553 ms  6.656 ms
 4 spb-81-211-104-177.sovintel.ru (81.211.104.177)  7.587 ms  8.473 ms  8.580 ms
 5 * * *
 6 s-b5-link.ip.twelve99.net (62.115.44.72)  17.962 ms  16.228 ms  17.055 ms
 7 s-bb2-link.ip.twelve99.net (62.115.136.110)  17.001 ms  15.994 ms  17.355 ms
 8 kbn-bb2-link.ip.twelve99.net (62.115.139.173)  102.970 ms  104.607 ms  103.773 ms
```

Существенно превышает среднее значение задержка канала между хостами 7 и 8. Оба хоста находятся в Швеции.