

HW10

1

The image shows a Wireshark packet capture window titled '*Ethernet'. The main pane displays a list of captured packets, with the filter 'icmp' applied. The packet list shows several ICMP messages, including Echo (ping) requests and replies, and Time-to-live exceeded messages. The packet details pane for the selected packet (No. 211) shows the following information:

- Internet Protocol Version 4, Src: 192.168.1.63, Dst: 184.51.132.45
- Version: 4
- Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 56
- Identification: 0xbeb6 (48822)
- Flags: 0x00
- Fragment Offset: 0
- Time to Live: 255
- Protocol: ICMP (1)
- Header Checksum: 0x0000 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 192.168.1.63
- Destination Address: 184.51.132.45
- Internet Control Message Protocol

The packet bytes pane shows the raw data of the packet, with the first 20 bytes highlighted in blue, corresponding to the ICMP header.

Source Address (p.src), 4 byte(s) | Пакеты: 397 · Показаны: 103 (25.9%) · Потеряно: 0 (0.0%) | Профиль: Default

1) Source Address: 192.168.1.63

2) Protocol: ICMP (1)

3) Total Length: 56

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

Полезная нагрузка тогда $56 - 20 = 36$

*Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

icmp

No.	Time	Source	Destination	Protocol	Length	Info
216	12.572458	192.168.1.1	192.168.1.63	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
287	15.084945	192.168.1.1	192.168.1.63	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
359	17.585196	192.168.1.1	192.168.1.63	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
211	12.533400	192.168.1.63	184.51.132.45	ICMP	70	Echo (ping) request id=0x0001, seq=5775/36630, ttl=255 (reply in 212)
215	12.571983	192.168.1.63	184.51.132.45	ICMP	70	Echo (ping) request id=0x0001, seq=5776/36886, ttl=1 (no response found!)
218	12.575002	192.168.1.63	192.168.1.1	ICMP	254	Destination unreachable (Port unreachable)
219	12.611124	192.168.1.63	184.51.132.45	ICMP	70	Echo (ping) request id=0x0001, seq=5777/37142, ttl=2 (no response found!)
221	12.649213	192.168.1.63	184.51.132.45	ICMP	70	Echo (ping) request id=0x0001, seq=5778/37398, ttl=3 (no response found!)
223	12.688391	192.168.1.63	184.51.132.45	ICMP	70	Echo (ping) request id=0x0001, seq=5779/37654, ttl=4 (no response found!)

> Ethernet II, Src: HewlettP_0e:f2:25 (84:a9:3e:0e:f2:25), Dst: Keenetic_1e:95:c8 (50:ff:20:1e:95:c8)

> Internet Protocol Version 4, Src: 192.168.1.63, Dst: 184.51.132.45

0100 = Version: 4

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

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 56

Identification: 0xbeb6 (48822)

> Flags: 0x00

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 255

Protocol: ICMP (1)

Header Checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.63

Destination Address: 184.51.132.45

> Internet Control Message Protocol

0000 50 ff 20 1e 95 c8 84 a9 3e 0e f2 25 08 00 45 00 P: >...%..E-

0010 00 38 be b6 00 00 ff 01 00 00 c0 a8 01 3f b8 33 .8.....?..3

0020 84 2d 08 00 1f ae 00 01 16 8f 20 20 20 20 20 20

Header length in 32-bit words (p_hdr.len), 1 byte(s)

Пакеты: 397 · Показаны: 103 (25.9%) · Потеряно: 0 (0.0%) · Профиль: Default

*Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

icmp

No.	Time	Source	Destination	Protocol	Length	Info
216	12.572458	192.168.1.1	192.168.1.63	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
287	15.084945	192.168.1.1	192.168.1.63	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
359	17.585196	192.168.1.1	192.168.1.63	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
211	12.533400	192.168.1.63	184.51.132.45	ICMP	70	Echo (ping) request id=0x0001, seq=5775/36630, ttl=255 (reply in 212)
215	12.571983	192.168.1.63	184.51.132.45	ICMP	70	Echo (ping) request id=0x0001, seq=5776/36886, ttl=1 (no response found!)
218	12.575002	192.168.1.63	192.168.1.1	ICMP	254	Destination unreachable (Port unreachable)
219	12.611124	192.168.1.63	184.51.132.45	ICMP	70	Echo (ping) request id=0x0001, seq=5777/37142, ttl=2 (no response found!)
221	12.649213	192.168.1.63	184.51.132.45	ICMP	70	Echo (ping) request id=0x0001, seq=5778/37398, ttl=3 (no response found!)
223	12.688391	192.168.1.63	184.51.132.45	ICMP	70	Echo (ping) request id=0x0001, seq=5779/37654, ttl=4 (no response found!)

> Ethernet II, Src: HewlettP_0e:f2:25 (84:a9:3e:0e:f2:25), Dst: Keenetic_1e:95:c8 (50:ff:20:1e:95:c8)

> Internet Protocol Version 4, Src: 192.168.1.63, Dst: 184.51.132.45

0100 = Version: 4

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

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 56

Identification: 0xbeb7 (48823)

> Flags: 0x00

...0 0000 0000 0000 = Fragment Offset: 0

> Time to Live: 1

Protocol: ICMP (1)

Header Checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.63

Destination Address: 184.51.132.45

> Internet Control Message Protocol

0000 50 ff 20 1e 95 c8 84 a9 3e 0e f2 25 08 00 45 00 P: >...%..E-

0010 00 38 be b7 00 00 01 01 00 00 c0 a8 01 3f b8 33 .8.....?..3

0020 84 2d 08 00 1f ad 00 01 16 90 20 20 20 20 20 20

Header length in 32-bit words (p_hdr.len), 1 byte(s)

Пакеты: 397 · Показаны: 103 (25.9%) · Потеряно: 0 (0.0%) · Профиль: Default

- 4) a) TTL, Identification
- b) Version, Length, Protocol, Checksum. TTL, Identification должны меняться (возможно еще Checksum, но везде 0x0000), остальные нет
- c) Увеличивается на 1
- 5) Identification: 0xbeb6 (48822), Time to Live: 255

6) Нет, меняются

Wireshark packet capture analysis of ICMP Echo (ping) requests and replies. The packet list shows several ICMP Echo (ping) requests and replies. The packet details pane shows the structure of an ICMP Echo (ping) request, including the header, differentiated services field, total length, identification, flags, fragment offset, time to live, protocol, header checksum, and source address.

No.	Time	Source	Destination	Protocol	Length	Info
395	18.363625	184.51.132.45	192.168.1.63	ICMP	70	Echo (ping) reply id=0x0001, seq=5825/49430,
394	18.345093	192.168.1.63	184.51.132.45	ICMP	70	Echo (ping) request id=0x0001, seq=5825/49430,
393	18.310888	62.115.38.47	192.168.1.63	ICMP	70	Time-to-live exceeded (Time to live exceeded in
392	18.287910	192.168.1.63	184.51.132.45	ICMP	70	Echo (ping) request id=0x0001, seq=5824/49174,
391	18.255572	62.115.122.40	192.168.1.63	ICMP	110	Time-to-live exceeded (Time to live exceeded in
390	18.237197	192.168.1.63	184.51.132.45	ICMP	70	Echo (ping) request id=0x0001, seq=5823/48918,
389	18.199510	80.91.247.209	192.168.1.63	ICMP	182	Time-to-live exceeded (Time to live exceeded in
388	18.187004	192.168.1.63	184.51.132.45	ICMP	70	Echo (ping) request id=0x0001, seq=5822/48662,
387	18.150485	62.115.135.108	192.168.1.63	ICMP	182	Time-to-live exceeded (Time to live exceeded in

Frame 393: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{45939136-950B-4A86-B5D2-5B4810D26...}

Ethernet II, Src: Keenetic_1e:95:c8 (50:ff:20:1e:95:c8), Dst: HewlettP_0e:f2:25 (84:a9:3e:0e:f2:25)

Internet Protocol Version 4, Src: 62.115.38.47, Dst: 192.168.1.63

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 56
- Identification: 0x3264 (12900)
- > Flags: 0x40, Don't fragment
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 242
- Protocol: ICMP (1)
- Header Checksum: 0x2fd7 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 62.115.38.47

0000 84 a9 3e 0e f2 25 50 ff 20 1e 95 c8 08 00 45 00 ..>...%P.E.

0010 00 38 32 64 40 00 f2 01 2f d7 3e 73 26 2f c0 a8 .82d@... />s&/..

0020 01 3f 0b 00 b6 c1 00 00 00 00 45 00 00 38 be e7 .?..... ..E..8..

wireshark_EthernetZ9KDN1.pcapng || Пакеты: 397 · Показаны: 103 (25.9%) · Потеряно: 0 (0.0%) || Профиль: Default

7) Identification: 0x3264 (12900), Time to Live: 242

*Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

icmp

No.	Time	Source	Destination	Protocol	Length	Info
16	2.120684	192.168.1.63	184.51.132.45	ICMP	554	Echo (ping) request id=0x0001, seq=5860/58390,
19	2.140393	184.51.132.45	192.168.1.63	ICMP	554	Echo (ping) reply id=0x0001, seq=5860/58390,
22	2.158734	192.168.1.63	184.51.132.45	ICMP	554	Echo (ping) request id=0x0001, seq=5861/58646,
23	2.159489	192.168.1.1	192.168.1.63	ICMP	590	Time-to-live exceeded (Time to live exceeded in
28	2.197891	192.168.1.63	184.51.132.45	ICMP	554	Echo (ping) request id=0x0001, seq=5862/58902,
29	2.199290	217.79.5.113	192.168.1.63	ICMP	70	Time-to-live exceeded (Time to live exceeded in
31	2.225691	192.168.1.63	192.168.1.1	ICMP	254	Destination unreachable (Port unreachable)
34	2.236006	192.168.1.63	184.51.132.45	ICMP	554	Echo (ping) request id=0x0001, seq=5863/59158,
35	2.237723	172.29.194.27	192.168.1.63	ICMP	70	Time-to-live exceeded (Time to live exceeded in

...0 1011 1001 0000 = Fragment Offset: 2960
Time to Live: 255
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.63
Destination Address: 184.51.132.45
[3 IPv4 Fragments (3480 bytes): #14(1480), #15(1480), #16(520)]
[Frame: 14, payload: 0-1479 (1480 bytes)]
[Frame: 15, payload: 1480-2959 (1480 bytes)]
[Frame: 16, payload: 2960-3479 (520 bytes)]
[Fragment count: 3]
[Reassembled IPv4 length: 3480]
[Reassembled IPv4 data: 08000741000116e420...]
> Internet Control Message Protocol

0010 02 1c bf 0b 01 72 ff 01 00 00 c0 a8 01 3f b8 33r.?3

Frame (554 bytes) Reassembled IPv4 (3480 bytes)

Time to Live (ip.ttl), 1 byte(s) || Пакеты: 292 · Показаны: 100 (34.2%) · Потеряно: 0 (0.0%) || Профиль: Default

8) а) Да, [Fragment count: 3]

*Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

icmp

No.	Time	Source	Destination	Protocol	Length	Info
16	2.120684	192.168.1.63	184.51.132.45	ICMP	554	Echo (ping) request id=0x0001, seq=5860/58390,
19	2.140393	184.51.132.45	192.168.1.63	ICMP	554	Echo (ping) reply id=0x0001, seq=5860/58390,
22	2.158734	192.168.1.63	184.51.132.45	ICMP	554	Echo (ping) request id=0x0001, seq=5861/58646,
23	2.159489	192.168.1.1	192.168.1.63	ICMP	590	Time-to-live exceeded (Time to live exceeded in
28	2.197891	192.168.1.63	184.51.132.45	ICMP	554	Echo (ping) request id=0x0001, seq=5862/58902,

> Frame 16: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface \Device\NPF_{45939136-950B-4A86-B5D2-5B4816}

> Ethernet II, Src: HewlettP_0e:f2:25 (84:a9:3e:0e:f2:25), Dst: Keenetic_1e:95:c8 (50:ff:20:1e:95:c8)

> Internet Protocol Version 4, Src: 192.168.1.63, Dst: 184.51.132.45

0100 = Version: 4

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

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 540

Identification: 0xbf0b (48907)

> Flags: 0x01

...0 1011 1001 0000 = Fragment Offset: 2960

Time to Live: 255

Protocol: ICMP (1)

Header Checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.63

Destination Address: 184.51.132.45

> [3 IPv4 Fragments (3480 bytes): #14(1480), #15(1480), #16(520)]

[Frame: 14, payload: 0-1479 (1480 bytes)]

```

0010 02 1c bf 0b 01 72 ff 01 00 00 c0 a8 01 3f b8 33  ....r. ....?.3
0020 84 2d 20 20 20 20 20 20 20 20 20 20 20 20 20  --
0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

```

Frame (554 bytes) Reassembled IPv4 (3480 bytes)

Total Length (ip.len), 2 byte(s) | Пакеты: 292 · Показаны: 100 (34.2%) · Потеряно: 0 (0.0%) | Профиль: Default

b) По сравнению с прошлым поменялись Length, Flags, Fragment Offset