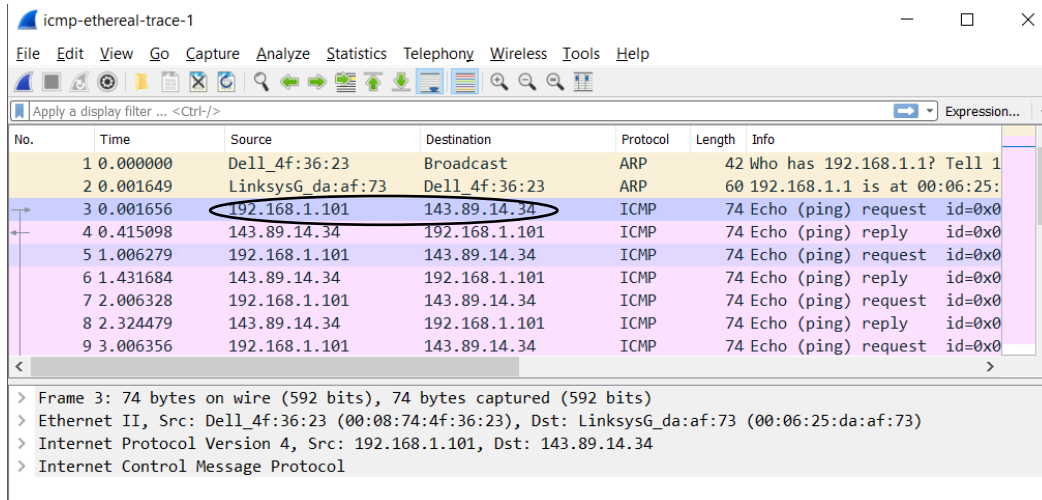


1. Host IP: 192.168.1.101

Destination Host IP: 143.89.14.34



icmph-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

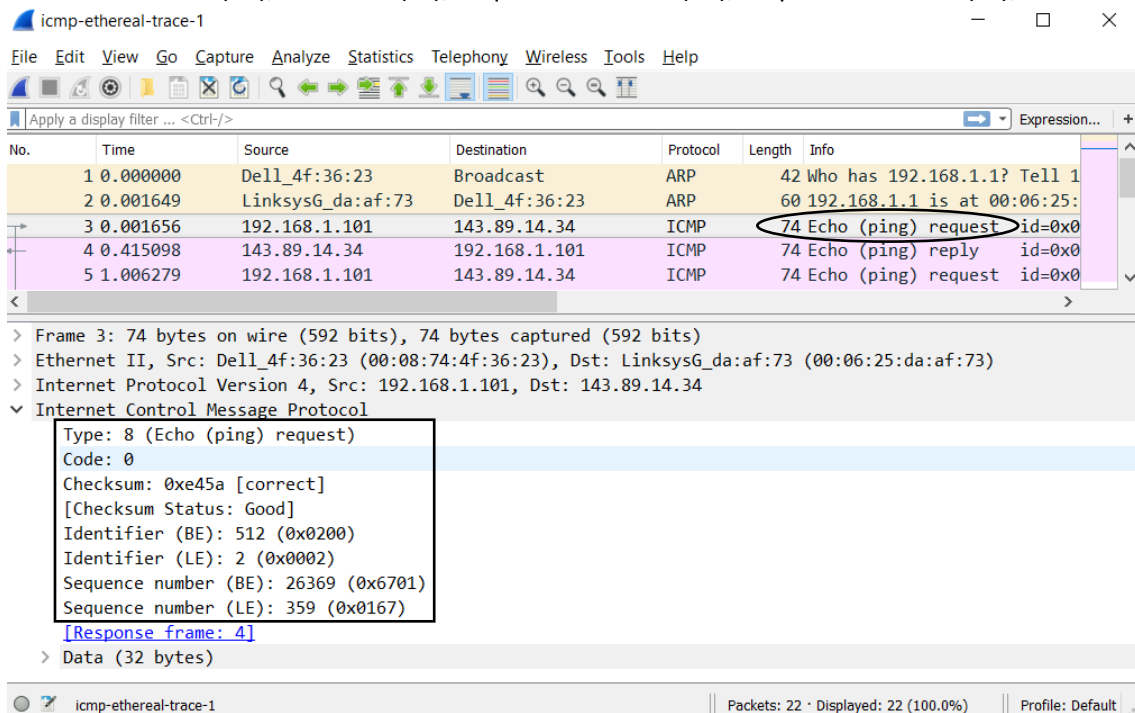
Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Dell_4f:36:23	Broadcast	ARP	42	Who has 192.168.1.1? Tell 1
2	0.001649	LinksysG_da:af:73	Dell_4f:36:23	ARP	60	192.168.1.1 is at 00:06:25:
3	0.001656	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0
4	0.415098	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0
5	1.006279	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0
6	1.431684	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0
7	2.006328	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0
8	2.324479	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0
9	3.006356	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0

> Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 143.89.14.34
> Internet Control Message Protocol

2. An ICMP does not have source and destination ports since communication is done between hosts and routers within the network layer.

3. The ICMP Type is 8 (Echo (ping) request) and the Code is 0. The other fields are Checksum, Identifier (BE), Identifier (LE), Sequence number (BE), Sequence number (LE), and Data.



icmph-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

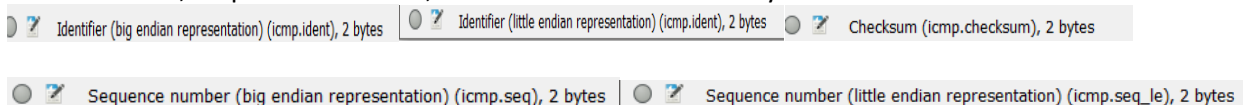
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Dell_4f:36:23	Broadcast	ARP	42	Who has 192.168.1.1? Tell 1
2	0.001649	LinksysG_da:af:73	Dell_4f:36:23	ARP	60	192.168.1.1 is at 00:06:25:
3	0.001656	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0
4	0.415098	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0
5	1.006279	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0

> Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 143.89.14.34
> Internet Control Message Protocol

Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xe45a [correct]
[Checksum Status: Good]
Identifier (BE): 512 (0x0200)
Identifier (LE): 2 (0x0002)
Sequence number (BE): 26369 (0x6701)
Sequence number (LE): 359 (0x0167)
[\[Response frame: 4\]](#)
> Data (32 bytes)

icmph-ethereal-trace-1 | Packets: 22 · Displayed: 22 (100.0%) | Profile: Default

The Checksum, Sequence Numbers, and Identifier Fields are 2 bytes each.



Identifier (big endian representation) (icmp.ident), 2 bytes | Identifier (little endian representation) (icmp.ident_le), 2 bytes | Checksum (icmp.checksum), 2 bytes

Sequence number (big endian representation) (icmp.seq), 2 bytes | Sequence number (little endian representation) (icmp.seq_le), 2 bytes

4. The ICMP Type is 0 (Echo (ping) reply) and the Code is 0. The other fields are Checksum, Identifier (BE), Identifier (LE), Sequence number (BE), Sequence number (LE), and Data.

The screenshot shows the Wireshark interface with the packet list pane displaying four packets. The selected packet (No. 4) is an ICMP Echo (ping) reply. The packet details pane shows the following fields:

- Type: 0 (Echo (ping) reply)
- Code: 0
- Checksum: 0xec5a [correct]
- [Checksum Status: Good]
- Identifier (BE): 512 (0x0200)
- Identifier (LE): 2 (0x0002)
- Sequence number (BE): 26369 (0x6701)
- Sequence number (LE): 359 (0x0167)
- [Request frame: 3]
- [Response time: 413.442 ms]
- Data (32 bytes)

The packet list pane shows the following data:

No.	Time	Source	Destination	Protocol	Length	Info
4	0.415098	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0
5	1.006279	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0
6	1.431684	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0
7	2.006328	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0

The Checksum, Sequence Numbers, and Identifier Fields are 2 bytes each.

The screenshot shows the Wireshark interface with the packet list pane displaying four packets. The selected packet (No. 1) is an ICMP Echo (ping) request. The packet details pane shows the following fields:

- Identifier (big endian representation) (icmp.ident), 2 bytes
- Identifier (little endian representation) (icmp.ident), 2 bytes
- Checksum (icmp.checksum), 2 bytes
- Sequence number (big endian representation) (icmp.seq), 2 bytes
- Sequence number (little endian representation) (icmp.seq_le), 2 bytes

5. Host IP: 192.168.1.101 Destination Host IP: 138.96.146.2

The screenshot shows the Wireshark interface with the packet list pane displaying four packets. The selected packet (No. 1) is an ICMP Echo (ping) request. The packet details pane shows the following fields:

- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0x0000 [correct]
- [Checksum Status: Good]
- Identifier (BE): 512 (0x0200)
- Identifier (LE): 2 (0x0002)
- Sequence number (BE): 26369 (0x6701)
- Sequence number (LE): 359 (0x0167)
- [Request frame: 1]
- [Response time: 413.442 ms]
- Data (32 bytes)

The packet list pane shows the following data:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x0
2	0.012151	10.0.0.0	10.0.0.0	ICMP	70	Time to live exceeded (TTL)
3	0.012151	10.0.0.0	10.0.0.0	ICMP	70	Time to live exceeded (TTL)
4	0.012151	10.0.0.0	10.0.0.0	ICMP	70	Time to live exceeded (TTL)

6. The UDP protocol is 17 (0x11), so the protocol number for the probe packets would not be 01 (Which we saw in our UDP lab in question 6).

7. The Checksum, Sequence numbers, and Data are different between the two Echo (ping) requests. Additionally, there was no response in this part, but there was a response in the first part (Comparisons made with question 3 screenshot).

The screenshot shows a Wireshark packet capture titled 'icmp-ethereal-trace-2'. The packet list shows five ICMP Echo (ping) requests. The first packet (No. 1) is an Echo (ping) request from 192.168.1.101 to 138.96.146.2. The second packet (No. 2) is a 'Time-to-live exceeded' message from 10.216.228.1 to 192.168.1.101. The third packet (No. 3) is another Echo (ping) request from 192.168.1.101 to 138.96.146.2. The fourth packet (No. 4) is a 'Time-to-live exceeded' message from 10.216.228.1 to 192.168.1.101. The fifth packet (No. 5) is another Echo (ping) request from 192.168.1.101 to 138.96.146.2. The packet details pane shows the structure of the first packet (No. 1): Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol (Type: 8, Code: 0). The ICMP section is expanded, showing fields: Checksum: 0x51fe [correct], [Checksum Status: Good], Identifier (BE): 512 (0x0200), Identifier (LE): 2 (0x0002), Sequence number (BE): 41985 (0xa401), Sequence number (LE): 420 (0x01a4), [No response seen], and Data (64 bytes).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x0
2	0.013151	10.216.228.1	192.168.1.101	ICMP	70	Time-to-live exceeded (Time
3	0.013258	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x0
4	0.025551	10.216.228.1	192.168.1.101	ICMP	70	Time-to-live exceeded (Time
5	0.025634	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x0

Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 138.96.146.2
v Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x51fe [correct]
[Checksum Status: Good]
Identifier (BE): 512 (0x0200)
Identifier (LE): 2 (0x0002)
Sequence number (BE): 41985 (0xa401)
Sequence number (LE): 420 (0x01a4)
> [No response seen]
> Data (64 bytes)

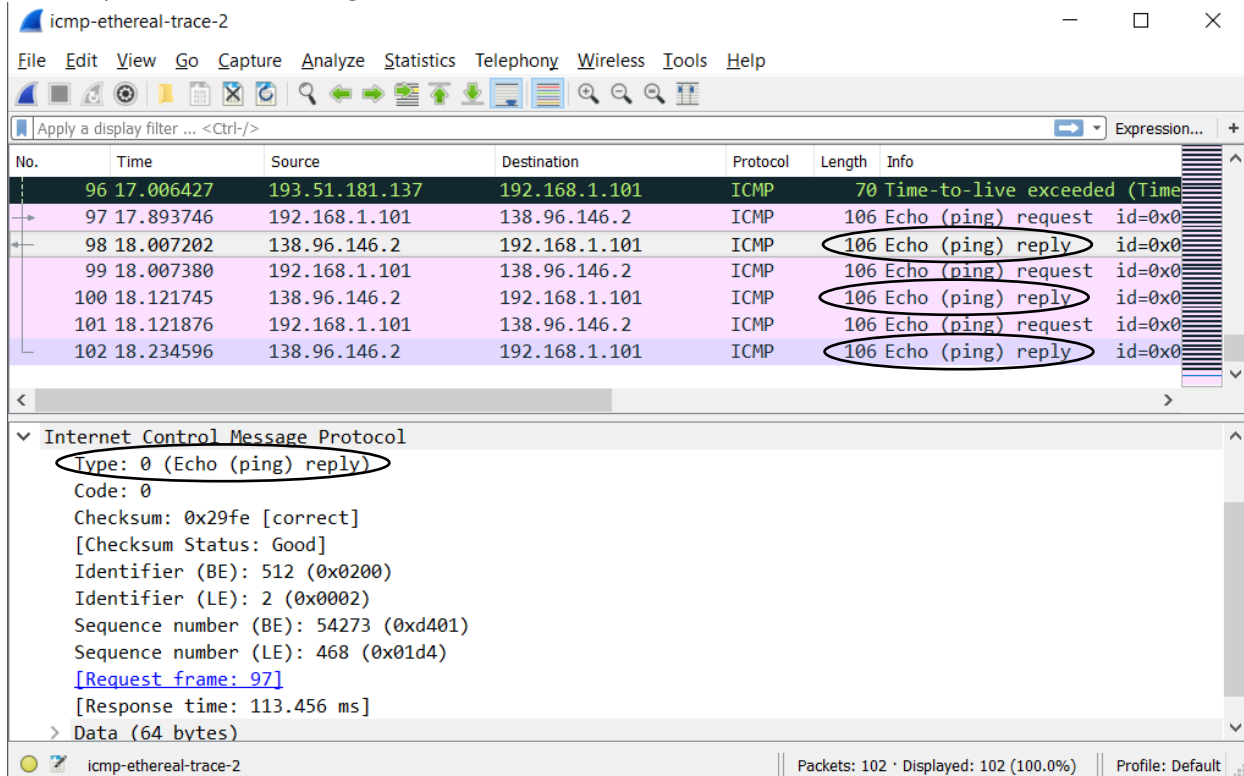
8. The error packet includes fields from the previous request packet (belonging to that request packet) as well as its own Type, Code, and Checksum field (individual to the error packet).

The screenshot shows the same Wireshark packet capture. The packet list shows three packets. The first packet (No. 1) is an Echo (ping) request from 192.168.1.101 to 138.96.146.2. The second packet (No. 2) is a 'Time-to-live exceeded' message from 10.216.228.1 to 192.168.1.101. The third packet (No. 3) is another Echo (ping) request from 192.168.1.101 to 138.96.146.2. The packet details pane shows the structure of the second packet (No. 2): Internet Protocol Version 4, Src: 10.216.228.1, Dst: 192.168.1.101, and Internet Control Message Protocol (Type: 11, Code: 0). The ICMP section is expanded, showing fields: Type: 11 (Time-to-live exceeded), Code: 0 (Time to live exceeded in transit), Checksum: 0x2c16 [correct], [Checksum Status: Good], Internet Protocol Version 4, Src: 192.168.1.101, Dst: 138.96.146.2, and Internet Control Message Protocol (Type: 8, Code: 0). The ICMP section is expanded, showing fields: Type: 8 (Echo (ping) request), Code: 0, Checksum: 0x51fe [unverified] [in ICMP error packet], [Checksum Status: Unverified], Identifier (BE): 512 (0x0200), Identifier (LE): 2 (0x0002), Sequence number (BE): 41985 (0xa401), and Sequence number (LE): 420 (0x01a4).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x0
2	0.013151	10.216.228.1	192.168.1.101	ICMP	70	Time-to-live exceeded (Time
3	0.013258	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x0

> Internet Protocol Version 4, Src: 10.216.228.1, Dst: 192.168.1.101
v Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0x2c16 [correct]
[Checksum Status: Good]
> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 138.96.146.2
v Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x51fe [unverified] [in ICMP error packet]
[Checksum Status: Unverified]
Identifier (BE): 512 (0x0200)
Identifier (LE): 2 (0x0002)
Sequence number (BE): 41985 (0xa401)
Sequence number (LE): 420 (0x01a4)

9. These packets are different because they are of Type 0, indicating a reply, rather than Type 11, which would indicate TTL-exceeded. They are different because they reached their destination prior to the TTL being exceeded.



10. Yes, there is a link with a delay significantly longer than the rest. The delay that is significantly longer than the others is from 9 to 10. Link 9 is in New York, USA (**nyc.opentransit.net**) and link 10 is in Pastourelle, France (**Pastourelle.opentransit.net** and the **.fr** extension).

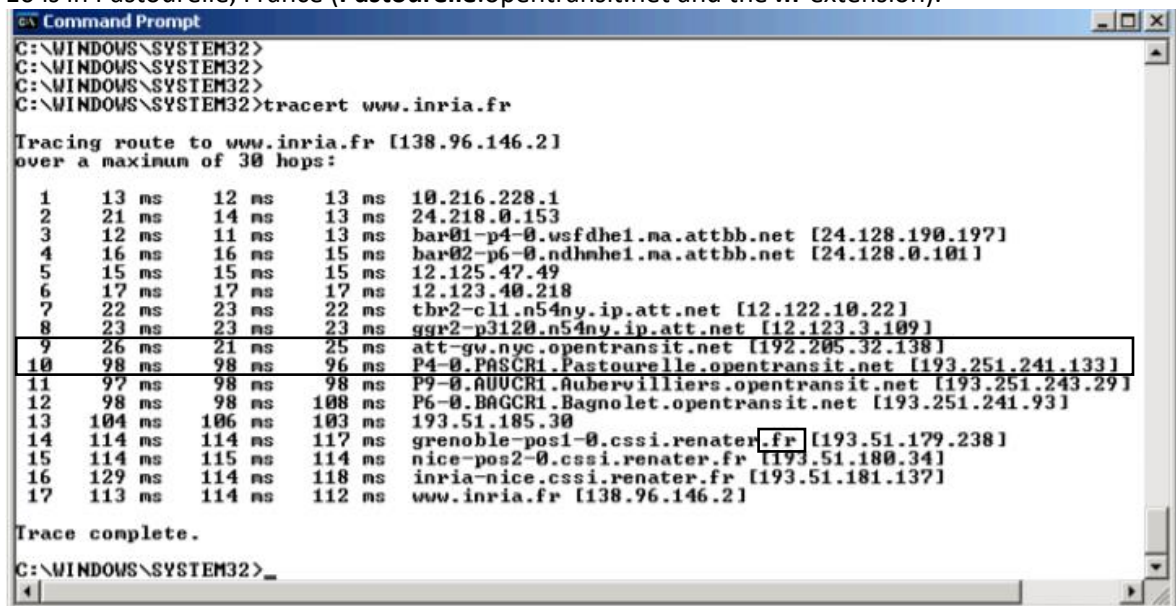


Figure 4 Command Prompt window displays the results of the Traceroute program.