

1. The IP address of the computer is **192.168.1.102**

8	6.163045	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request	id=0x0300, seq=20483/848, ttl=1 (no response found!)
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request	id=0x0300, seq=20739/849, ttl=2 (no response found!)
11	6.202957	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
12	6.208597	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request	id=0x0300, seq=20995/850, ttl=3 (no response found!)
13	6.234505	24.128.190.197	192.168.1.102	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)
14	6.238695	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request	id=0x0300, seq=21251/851, ttl=4 (no response found!)
15	6.257672	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exceeded	(Time to live exceeded in transit)

> Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0x32d0 (13008)
> Flags: 0x00
Fragment Offset: 0
> Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x2d2c [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.59.23.100

2. The value in the upper layer protocol field is **ICMP**.

3. In the IP header there are **20 bytes**.

The total bytes length is **84 bytes**.

the payload of the IP datagram is 84 bytes-20 bytes = **64 bytes**.

8	6.163045	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request	id=0x0300, seq=20483/848, ttl=1 (no response found!)
---	----------	---------------	---------------	------	----	---------------------	------------------------------------------------------

> Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84

4. The IP datagram has not been fragmented. We can see in the screenshot below that the "More fragments" flag is set to 0.

8	6.163045	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request	id=0x0300, seq=20483/848, ttl=1 (no response found!)
---	----------	---------------	---------------	------	----	---------------------	------------------------------------------------------

> Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0x32d0 (13008)
v Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment Offset: 0

5. The fields in the IP datagram the always change from one datagram to the next within the series of ICMP messages sent by my computer are: **Identification, Time to live, Header checksum**.

8485	27.948581	192.168.30.105	128.119.245.12	ICMP	554	Echo (ping) request	id=0x0001, seq=3549/56589, ttl=12 (no response found!)
------	-----------	----------------	----------------	------	-----	---------------------	--------------------------------------------------------

> Frame 8512: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface \Device\NPF_{1141279D-B53B-4E02-81E0-3162C086E92D}, id 0
> Ethernet II, Src: HonHaiPr_d0:18:71 (74:40:bb:d0:18:71), Dst: Fortinet_5a:df:eb (70:4c:a5:5a:df:eb)
v Internet Protocol Version 4, Src: 192.168.30.105, Dst: 128.119.245.12
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 540
Identification: 0x7faa (32682)
v Flags: 0x0172
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 2960
> Time to live: 3
Protocol: ICMP (1)
Header checksum: 0xe02f [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.30.105
Destination: 128.119.245.12
> [3 IPv4 Fragments (3480 bytes): #8510(1480), #8511(1480), #8512(520)]

Version: we are using IPv4 for all packets.

Header Length: we are talking about ICMP packets – the headers are the same length.

Total Length: same reason.

Differentiated Services Fields: all packets are ICMP, therefore they use the same type of service class.

Source IP: all packets were sent from the same source.

Destination IP: all packets were sent to the same destination.

The fields that must change:

Identification: each packet has a unique id.

Time to live: the traceroute increments each subsequent packet.

Header checksum: the header itself changes, therefore the checksum changes to.

7. The patterns I see in the values in the identification field to the IP datagram: for each ICMP request, the identification increments.

8. The value in the identification field: 20429

The value in the TTL field: **243**

377	54.774816	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
320	49.770176	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
266	44.763963	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
212	39.227649	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
170	34.212107	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
129	29.207167	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
88	16.468603	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
62	11.467036	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
34	6.467979	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
370	53.973964	12.125.47.49	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Frame 377: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)

Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)

Internet Protocol Version 4, Src: 128.59.1.41, Dst: 192.168.1.102

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentially Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 56
Identification: 0x4fcd (20429)
Flags: 0x00
Fragment Offset: 0
Time to Live: 243
Protocol: ICMP (1)
Header Checksum: 0x3485 [validation disabled]
[Header checksum status: Unverified]
Source Address: 128.59.1.41
Destination Address: 192.168.1.102

Internet Control Message Protocol

9. The TTL remain unchanged for all the ICMP TTL exceeded replies sent to my computer by the nearest router because the TTL for the first hop router is always the same.

The identification changes for all the ICMP TTL exceeded replies sent to my computer because the identification field has a unique value.

10. The message has been fragmented (attached screenshot).

3369	8.729421	128.119.3.32	192.168.30.105	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
3370	8.772401	128.119.240.253	192.168.30.105	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
3371	8.835992	128.119.245.12	192.168.30.105	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
3372	9.001084	192.168.30.47	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
3373	9.016406	192.168.30.105	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=7e8f) [Reassembled in #3374]
3374	9.016428	192.168.30.105	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=3271/50956, ttl=255 (reply in 3385)
3375	9.066922	192.168.30.105	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=7e90) [Reassembled in #3376]
3376	9.066930	192.168.30.105	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=3272/51212, ttl=1 (no response found!)
3377	9.069504	192.168.30.254	192.168.30.105	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
3378	9.117210	192.168.30.105	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=7e91) [Reassembled in #3379]
3379	9.117217	192.168.30.105	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=3273/51468, ttl=2 (no response found!)
3380	9.122113	fe80::5aef:68ff:fe8c:5d...	ff02::2	ICMPv6	70	Router Solicitation from 58:ef:68:8c:5d:95
3381	9.128179	185.167.110.17	192.168.30.105	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
3382	9.167540	192.168.30.105	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=7e92) [Reassembled in #3383]
3383	9.167544	192.168.30.105	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=3274/51724, ttl=3 (no response found!)
3384	9.185167	128.119.245.12	192.168.30.105	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=8aae) [Reassembled in #3385]
3385	9.185365	128.119.245.12	192.168.30.105	ICMP	534	Echo (ping) reply id=0x0001, seq=3271/50956, ttl=48 (request in 3374)

11. The “More fragments” bit in the flags in set to 1 which indicated the datagram has been fragmented.

Also, the fragment offset in set to 0, which indicates this is the first fragment.

The IP datagram total length is 1500.

3374	9.016428	192.168.30.105	128.119.245.12	ICMP	534 Echo (ping) request id=0x0001, seq=3271/50956, ttl=255 (reply in 3385)
3375	9.066922	192.168.30.105	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=7e90) [Reassembled in #3376]
3376	9.066930	192.168.30.105	128.119.245.12	ICMP	534 Echo (ping) request id=0x0001, seq=3272/51212, ttl=1 (no response found!)
3377	9.069504	192.168.30.254	192.168.30.105	ICMP	590 Time-to-live exceeded (Time to live exceeded in transit)
3378	9.117210	192.168.30.105	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=7e91) [Reassembled in #3379]
3379	9.117217	192.168.30.105	128.119.245.12	ICMP	534 Echo (ping) request id=0x0001, seq=3273/51468, ttl=2 (no response found!)
Frame 3375: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{1141279D-B53B-4E02-81E0-3162C086E92D}, id 0					
Ethernet II, Src: HonHaiPr_d0:18:71 (74:40:bb:d0:18:71), Dst: Fortinet_5a:df:eb (70:4c:a5:5a:df:eb)					
Internet Protocol Version 4, Src: 192.168.30.105, Dst: 128.119.245.12					
0100 = Version: 4					
... 0101 = Header Length: 20 bytes (5)					
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)					
Total Length: 1500					
Identification: 0x7e90 (32400)					
v Flags: 0x2000, More fragments					
0... .. = Reserved bit: Not set					
.0... .. = Don't fragment: Not set					
..1... .. = More fragments: Set					
Fragment offset: 0					
> Time to live: 1					
Protocol: ICMP (1)					
Header checksum: 0xc0fb [validation disabled]					
[Header checksum status: Unverified]					
Source: 192.168.30.105					
Destination: 128.119.245.12					
Reassembled IPv4 in frame: 3376					
Data (1480 bytes)					

12. As we can see, the fragment offset is set to 1480, which indicates this is not the first fragment. There are no more fragments. The “More fragments” flag is set to 0.

3373	9.016406	192.168.30.105	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=7e8f) [Reassembled in #3374]
3374	9.016428	192.168.30.105	128.119.245.12	ICMP	534 Echo (ping) request id=0x0001, seq=3271/50956, ttl=255 (reply in 3385)
3375	9.066922	192.168.30.105	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=7e90) [Reassembled in #3376]
3376	9.066930	192.168.30.105	128.119.245.12	ICMP	534 Echo (ping) request id=0x0001, seq=3272/51212, ttl=1 (no response found!)
3377	9.069504	192.168.30.254	192.168.30.105	ICMP	590 Time-to-live exceeded (Time to live exceeded in transit)
3378	9.117210	192.168.30.105	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=7e91) [Reassembled in #3379]
3379	9.117217	192.168.30.105	128.119.245.12	ICMP	534 Echo (ping) request id=0x0001, seq=3273/51468, ttl=2 (no response found!)
> Frame 3376: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface \Device\NPF_{1141279D-B53B-4E02-81E0-3162C086E92D}, id 0					
> Ethernet II, Src: HonHaiPr_d0:18:71 (74:40:bb:d0:18:71), Dst: Fortinet_5a:df:eb (70:4c:a5:5a:df:eb)					
> Internet Protocol Version 4, Src: 192.168.30.105, Dst: 128.119.245.12					
0100 = Version: 4					
... 0101 = Header Length: 20 bytes (5)					
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)					
Total Length: 520					
Identification: 0x7e90 (32400)					
v Flags: 0x00b9					
0... .. = Reserved bit: Not set					
.0... .. = Don't fragment: Not set					
..0... .. = More fragments: Not set					
Fragment offset: 1480					
> Time to live: 1					
Protocol: ICMP (1)					
Header checksum: 0xe416 [validation disabled]					
[Header checksum status: Unverified]					
Source: 192.168.30.105					
Destination: 128.119.245.12					
> [2 IPv4 Fragments (1980 bytes): #3375(1480), #3376(500)]					

14. There are 3 fragments that were created from the original datagram.

6332	18.679809	192.168.30.105	2.21.69.67	TCP	54 57254 → 443 [ACK] Seq=5922 Ack=6822708 Win=16470 Len=0
6333	18.728815	192.168.30.105	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=7f1c) [Reassembled in #6335]
6334	18.728818	192.168.30.105	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=7f1c) [Reassembled in #6335]
6335	18.728819	192.168.30.105	128.119.245.12	ICMP	554 Echo (ping) request id=0x0001, seq=3412/21517, ttl=1 (no response found!)
6336	18.733008	192.168.30.254	192.168.30.105	ICMP	590 Time-to-live exceeded (Time to live exceeded in transit)
6337	18.740120	192.168.30.119	192.168.30.105	SNMP	566 get-response 1.3.6.1.4.1.2435.2.3.9.2.11.1.1.0 1.3.6.1.4.1.2435.2.3.9.2.11.1.1.0 1.3.6.1.4.1.2435.2.3.9.2.11.1.1.0

15. The fields that were changed in the IP header among the fragments:

Fragment offset (changed between all three fragments), **Checksum** (changed between all three fragments), **Total Length** (for two first fragments total length is 1500, and the last total length is 540), **Flags** (for two first fragments the “More fragments” flag is set to 1, and in the last fragment is set to 0).