

Nome: Fernando Henrique Ratusznei Caetano

```
$ ping -c 3 gaia.cs.umass.edu.
PING gaia.cs.umass.edu (128.119.245.12) 56(84) bytes of data.
64 bytes from gaia.cs.umass.edu (128.119.245.12): icmp_seq=1 ttl=47 time=140 ms
64 bytes from gaia.cs.umass.edu (128.119.245.12): icmp_seq=2 ttl=47 time=140 ms
64 bytes from gaia.cs.umass.edu (128.119.245.12): icmp_seq=3 ttl=47 time=140 ms

--- gaia.cs.umass.edu ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 140.102/140.168/140.206/0.047 ms
```

A seguir seguem as capturas correspondentes no Wireshark. Os comandos de interesse são marcados com protocolo ICMP (em rosa). Existem 6 mensagens na captura, correspondendo a três pares Requisição/Resposta.

A primeira tela apresenta detalhes do datagrama da requisição ECHO e a segunda apresenta detalhes da resposta. Podemos observar os campos Type, Code, Checksum, Identifier, Sequence Number e Data e seus conteúdos conforme explicado na página anterior.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.100.100	128.119.245.12	ICMP	98	Echo (ping) request id=0x0007, seq=1/256, ttl=64 (reply in 2)
2	0.140180737	128.119.245.12	192.168.100.100	ICMP	98	Echo (ping) reply id=0x0007, seq=1/256, ttl=47 (request in 1)
3	0.746960312	fe80::1	ff05::c	SSDP	188	M-SEARCH * HTTP/1.1
4	1.000760775	192.168.100.100	128.119.245.12	ICMP	98	Echo (ping) request id=0x0007, seq=2/512, ttl=64 (reply in 6)
5	1.000513725	fe80::1	ff05::c	SSDP	188	M-SEARCH * HTTP/1.1
6	1.140946858	128.119.245.12	192.168.100.100	ICMP	98	Echo (ping) reply id=0x0007, seq=2/512, ttl=47 (request in 4)
7	1.266940586	fe80::1	ff02::c	SSDP	188	M-SEARCH * HTTP/1.1
8	1.526638954	fe80::1	ff02::c	SSDP	188	M-SEARCH * HTTP/1.1
9	1.786623159	192.168.100.1	239.255.255.250	SSDP	174	M-SEARCH * HTTP/1.1
10	2.001278066	192.168.100.100	128.119.245.12	ICMP	98	Echo (ping) request id=0x0007, seq=3/768, ttl=64 (reply in 12)
11	2.046383810	192.168.100.1	239.255.255.250	SSDP	174	M-SEARCH * HTTP/1.1
12	2.141353015	128.119.245.12	192.168.100.100	ICMP	98	Echo (ping) reply id=0x0007, seq=3/768, ttl=47 (request in 10)
13	2.306447788	fe80::1	ff05::c	SSDP	189	M-SEARCH * HTTP/1.1
14	2.566166423	fe80::1	ff05::c	SSDP	189	M-SEARCH * HTTP/1.1
15	2.826134725	fe80::1	ff02::c	SSDP	189	M-SEARCH * HTTP/1.1
16	3.086052307	fe80::1	ff02::c	SSDP	189	M-SEARCH * HTTP/1.1
17	3.345822639	192.168.100.1	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
18	3.605926088	192.168.100.1	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1

▶ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp6s0, id 0
 ▶ Ethernet II, Src: BiostarMicro_57:52:ed (f4:b5:20:57:52:ed), Dst: HuaweiTechno_c0:39:a9 (3c:78:43:c0:39:a9)
 ▶ Internet Protocol Version 4, Src: 192.168.100.100, Dst: 128.119.245.12
 ▶ Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0xbe10 [correct]
 [Checksum Status: Good]
 Identifier (BE): 7 (0x0007)
 Identifier (LE): 1792 (0x0700)
 Sequence Number (BE): 1 (0x0001)
 Sequence Number (LE): 256 (0x0100)
 [Response frame: 2]
 Timestamp from icmp data: Oct 19, 2024 11:11:36.192332000 -03
 [Timestamp from icmp data (relative): 0.000018049 seconds]
 Data (40 bytes)
 Data: 101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637
 [Length: 40]

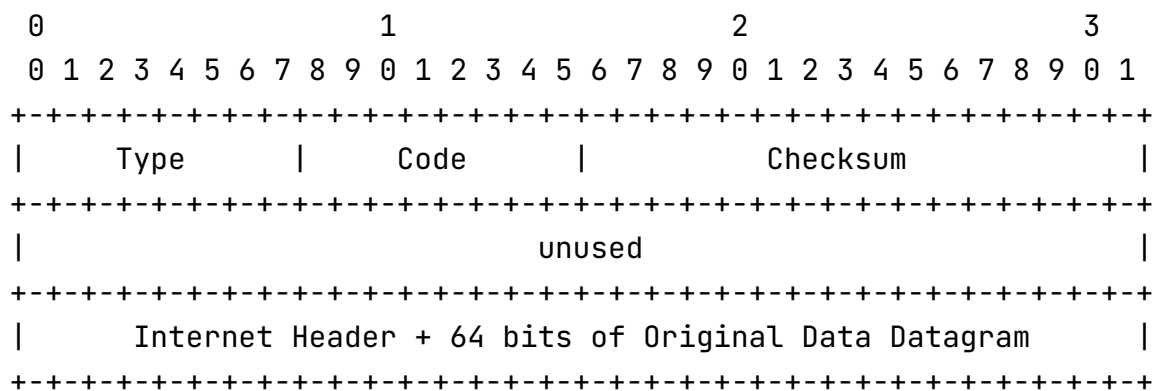
▶ Frame 2: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp6s0, id 0
 ▶ Ethernet II, Src: HuaweiTechno_c0:39:a9 (3c:78:43:c0:39:a9), Dst: BiostarMicro_57:52:ed (f4:b5:20:57:52:ed)
 ▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.100.100
 ▶ Internet Control Message Protocol
 Type: 0 (Echo (ping) reply)
 Code: 0
 Checksum: 0xc610 [correct]
 [Checksum Status: Good]
 Identifier (BE): 7 (0x0007)
 Identifier (LE): 1792 (0x0700)
 Sequence Number (BE): 1 (0x0001)
 Sequence Number (LE): 256 (0x0100)
 [Request frame: 1]
 [Response time: 140,181 ms]
 Timestamp from icmp data: Oct 19, 2024 11:11:36.192332000 -03
 [Timestamp from icmp data (relative): 0.140198786 seconds]
 Data (40 bytes)
 Data: 101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637
 [Length: 40]

Comando traceroute

O comando traceroute também utiliza o protocolo ICMP, porém dessa vez da mensagem TIME_EXCEEDED. Quando o campo TTL do header do protocolo IP atinge zero, o roteador pode enviar uma mensagem TIME_EXCEEDED para o remetente.

O comando traceroute envia pacotes, em grupos de três, com TTL cada vez maiores e recebendo mensagens TIME_EXCEEDED de roteadores cada vez mais distantes. Lendo os endereços IP dos roteadores que nos enviaram essas mensagens podemos reconstruir a rota que os datagramas tomaram.

A seguir segue o formato da mensagem TIME_EXCEEDED:



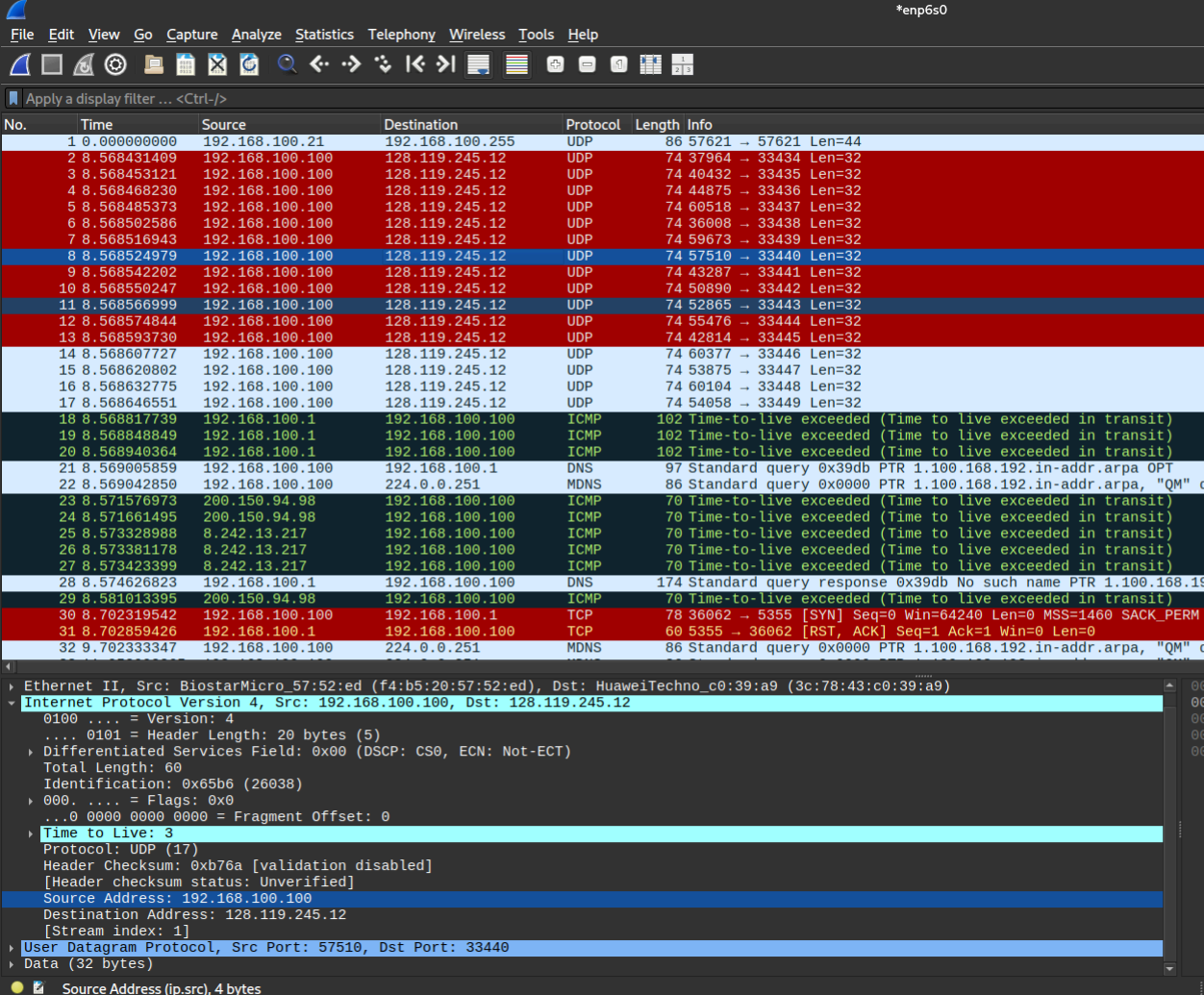
- Type: Tipo da mensagens, 11 para TIME_EXCEEDED;
- Code: 0 ou 1 dependendo se o TTL atingiu zero ou se o roteador não conseguiu reconstruir o fragmento no tempo estabelecido;
- Checksum: Valor computado a partir do conteúdo da mensagem;
- E o header da mensagem enviada que atingiu o tempo limite.

A seguir segue o comando traceroute e sua resposta. Cada linha corresponde a um TTL diferente e apresenta até três tempos de resposta, um para cada datagrama enviado. São apresentados também IP e DNS reverso dos roteadores que responderam. Como a mensagem TIME_EXCEEDED é opcional, para os TTLs que não receberam resposta o comando simplesmente imprime “* * *”. É possível que diferentes roteadores respondam as três mensagens enviadas para cada TTL, nesse caso o comando imprime mais de um IP por linha.

```
* traceroute gaia.cs.umass.edu.

traceroute to gaia.cs.umass.edu. (128.119.245.12), 30 hops max, 60 byte packets
 1 _gateway (192.168.100.1) 0.394 ms 0.488 ms 0.388 ms
 2 * * *
 3 200.150.94.98 (200.150.94.98) 3.138 ms 3.040 ms 12.465 ms
 4 8.242.13.217 (8.242.13.217) 4.862 ms 4.755 ms 4.788 ms
 5 * * *
 6 * * *
 7 be3087.ccr22.mia01.atlas.cogentco.com (154.54.88.233) 117.663 ms 117.649 ms be3081.ccr21.mia01.atlas.cogentco.com (154.54.88.225) 120.497 ms
 8 be3483.ccr42.atl01.atlas.cogentco.com (154.54.28.49) 131.720 ms be3482.ccr41.atl01.atlas.cogentco.com (154.54.24.145) 132.448 ms 132.434 ms
 9 154.54.7.157 (154.54.7.157) 174.399 ms be2113.ccr42.dca01.atlas.cogentco.com (154.54.24.221) 135.732 ms 135.717 ms
10 port-channel5042.ccr92.dca04.atlas.cogentco.com (154.54.162.221) 370.042 ms port-channel5927.ccr92.dca04.atlas.cogentco.com (154.54.163.101) 134.32
 2 ms port-channel5042.ccr92.dca04.atlas.cogentco.com (154.54.162.221) 133.458 ms
11 be4155.ccr41.jfk02.atlas.cogentco.com (154.54.30.42) 134.302 ms be4188.ccr42.jfk02.atlas.cogentco.com (154.54.30.122) 134.396 ms 132.968 ms
12 154.54.90.98 (154.54.90.98) 138.431 ms be3471.ccr31.bos01.atlas.cogentco.com (154.54.40.153) 139.616 ms 154.54.46.33 (154.54.46.33) 136.797 ms
13 be2729.ccr51.orh01.atlas.cogentco.com (154.54.40.182) 138.716 ms be2735.ccr51.orh01.atlas.cogentco.com (154.54.82.58) 138.922 ms 138.730 ms
14 38.104.218.14 (38.104.218.14) 140.284 ms 140.263 ms 140.493 ms
15 69.16.0.8 (69.16.0.8) 139.657 ms 145.815 ms 140.099 ms
16 69.16.1.0 (69.16.1.0) 138.971 ms 140.860 ms 138.793 ms
17 192.80.83.113 (192.80.83.113) 139.002 ms 192.80.83.109 (192.80.83.109) 139.278 ms 140.747 ms
18 128.119.0.216 (128.119.0.216) 139.776 ms n1-rt-1-1-et-10-0-0.gw.umass.edu (128.119.0.120) 143.452 ms n1-rt-1-1-et-0-0-0.gw.umass.edu (128.119.0.216
 ) 141.015 ms
19 128.119.7.74 (128.119.7.74) 145.563 ms 142.777 ms 142.594 ms
20 128.119.7.66 (128.119.7.66) 144.921 ms 144.870 ms 144.391 ms
21 128.119.0.217 (128.119.0.217) 144.159 ms 144.286 ms 144.413 ms
22 n5-rt-1-1-xe-2-1-0.gw.umass.edu (128.119.3.33) 146.059 ms 146.222 ms 146.772 ms
23 c1cs-rt-xe-0-0-0.gw.umass.edu (128.119.3.32) 145.741 ms 144.499 ms 145.181 ms
24 nscs1bbs1.cs.umass.edu (128.119.240.253) 148.324 ms 152.796 ms 150.034 ms
25 gaia.cs.umass.edu (128.119.245.12) 140.363 ms !X 139.738 ms !X 140.325 ms !X
```

A seguir segue a captura do wireshark com detalhes de um pacote enviado com TTL de 3. O comando traceroute inicialmente enviou 15 mensagens UDP para diferentes portas com TTLs de 1 até 5 (em vermelho e azul claro). O IP destino de interesse é 128.119.245.12. A seguir já começamos a receber pacotes ICMP (em letras verdes e fundo escuro) com info “Time-to-live exceeded”. Como cada datagrama UDP é enviado para uma porta diferente, o comando pode utilizar o header retorna para criar pares Requisição/Resposta;



The image shows a Wireshark packet capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. A display filter is applied: "Apply a display filter ... <Ctrl-/>". The packet list table shows 32 packets. Packets 1-15 are UDP packets from 192.168.100.100 to 128.119.245.12 with various destination ports. Packets 16-20 are ICMP "Time-to-live exceeded" messages. Packets 21-22 are DNS queries. Packets 23-27 are ICMP "Time-to-live exceeded" messages. Packets 28-29 are DNS query responses. Packets 30-31 are TCP SYN and RST/ACK packets. Packet 32 is a DNS query. The packet details pane for packet 32 shows the Ethernet II header, Internet Protocol Version 4 header, and User Datagram Protocol header. The packet bytes pane shows the source address (ip.src), 4 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.100.21	192.168.100.255	UDP	86	57621 → 57621 Len=44
2	8.568431409	192.168.100.100	128.119.245.12	UDP	74	37964 → 33434 Len=32
3	8.568453121	192.168.100.100	128.119.245.12	UDP	74	40432 → 33435 Len=32
4	8.568468230	192.168.100.100	128.119.245.12	UDP	74	44875 → 33436 Len=32
5	8.568485373	192.168.100.100	128.119.245.12	UDP	74	60518 → 33437 Len=32
6	8.568502586	192.168.100.100	128.119.245.12	UDP	74	36008 → 33438 Len=32
7	8.568516943	192.168.100.100	128.119.245.12	UDP	74	59673 → 33439 Len=32
8	8.568524979	192.168.100.100	128.119.245.12	UDP	74	57510 → 33440 Len=32
9	8.568542202	192.168.100.100	128.119.245.12	UDP	74	43287 → 33441 Len=32
10	8.568550247	192.168.100.100	128.119.245.12	UDP	74	50890 → 33442 Len=32
11	8.568566999	192.168.100.100	128.119.245.12	UDP	74	52865 → 33443 Len=32
12	8.568574844	192.168.100.100	128.119.245.12	UDP	74	55476 → 33444 Len=32
13	8.568593730	192.168.100.100	128.119.245.12	UDP	74	42814 → 33445 Len=32
14	8.568607727	192.168.100.100	128.119.245.12	UDP	74	60377 → 33446 Len=32
15	8.568620802	192.168.100.100	128.119.245.12	UDP	74	53875 → 33447 Len=32
16	8.568632775	192.168.100.100	128.119.245.12	UDP	74	60104 → 33448 Len=32
17	8.568646551	192.168.100.100	128.119.245.12	UDP	74	54058 → 33449 Len=32
18	8.568917739	192.168.100.1	192.168.100.100	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
19	8.568948849	192.168.100.1	192.168.100.100	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
20	8.568940304	192.168.100.1	192.168.100.100	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
21	8.569005859	192.168.100.100	192.168.100.1	DNS	97	Standard query 0x39db PTR 1.100.168.192.in-addr.arpa OPT
22	8.569042850	192.168.100.100	224.0.0.251	MDNS	86	Standard query 0x0000 PTR 1.100.168.192.in-addr.arpa, "QM" c
23	8.571576973	200.150.94.98	192.168.100.100	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
24	8.571661495	200.150.94.98	192.168.100.100	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
25	8.573328988	8.242.13.217	192.168.100.100	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
26	8.573381178	8.242.13.217	192.168.100.100	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
27	8.573423399	8.242.13.217	192.168.100.100	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
28	8.574626823	192.168.100.1	192.168.100.100	DNS	174	Standard query response 0x39db No such name PTR 1.100.168.192.in-addr.arpa, "QM" c
29	8.581013395	200.150.94.98	192.168.100.100	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
30	8.702319542	192.168.100.100	192.168.100.1	TCP	78	36062 → 5355 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
31	8.702859426	192.168.100.1	192.168.100.100	TCP	60	5355 → 36062 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
32	9.702333347	192.168.100.100	224.0.0.251	MDNS	86	Standard query 0x0000 PTR 1.100.168.192.in-addr.arpa, "QM" c

Packet Details:

- Ethernet II, Src: BiostarMicro_57:52:ed (f4:b5:20:57:52:ed), Dst: HuaweiTechno_c0:39:a9 (3c:78:43:c0:39:a9)
- Internet Protocol Version 4, Src: 192.168.100.100, 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: 60
 - Identification: 0x65b6 (26038)
 - 000. = Flags: 0x0
 - ...0 0000 0000 0000 = Fragment Offset: 0
 - Time to Live: 3
 - Protocol: UDP (17)
 - Header Checksum: 0xb76a [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 192.168.100.100
 - Destination Address: 128.119.245.12
 - [Stream index: 1]
- User Datagram Protocol, Src Port: 57510, Dst Port: 33440
- Data (32 bytes)
 - Source Address (ip.src), 4 bytes

Referências:

- RFC do ICMP: <https://datatracker.ietf.org/doc/html/rfc792>
- Manual do ping acessado pelo comando man ping
- Manual do traceroute acessado pelo comando man traceroute