

Universidade Federal de Uberlândia – UFU

Bacharelado em Sistemas de Informação - Campus Monte Carmelo

GS1524 - Redes de computadores - 2021/1

RENAN JUSTINO REZENDE SILVA - 11921BSI223

Atividade 9

ICMP

- O objetivo desta atividade é entender melhor o ICMP. Leia o texto e execute os passos que estão no arquivo (Wireshark_ICMP.pdf). Durante os passos no arquivo, serão indicados itens para serem respondidos. As perguntas a seguir referem-se à atividade no arquivo (Wireshark_ICMP.pdf).

```
C:\Users\Renato>ping -n 10 www.ust.hk

Disparando www.ust.hk [143.89.12.134] com 32 bytes de dados:
Resposta de 143.89.12.134: bytes=32 tempo=325ms TTL=48
Resposta de 143.89.12.134: bytes=32 tempo=325ms TTL=48
Resposta de 143.89.12.134: bytes=32 tempo=328ms TTL=48
Resposta de 143.89.12.134: bytes=32 tempo=326ms TTL=48
Resposta de 143.89.12.134: bytes=32 tempo=326ms TTL=48
Resposta de 143.89.12.134: bytes=32 tempo=330ms TTL=48
Resposta de 143.89.12.134: bytes=32 tempo=328ms TTL=48
Resposta de 143.89.12.134: bytes=32 tempo=326ms TTL=48
Resposta de 143.89.12.134: bytes=32 tempo=329ms TTL=48

Estatísticas do Ping para 143.89.12.134:
    Pacotes: Enviados = 10, Recebidos = 10, Perdidos = 0 (0% de
              perda),
    Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 325ms, Máximo = 330ms, Média = 326ms
```

Figura 1: ping -n 10 www.ust.hk

1. Qual é o endereço IP do seu host? Qual é o endereço IP do host de destino?

The image shows a Wireshark packet capture of ICMP Echo (ping) traffic. The top pane displays a list of 20 packets, alternating between requests (seq=1158, 1159, 1160, 1161, 1162, 1163, 1164, 1165, 1166, 1167) and replies (seq=34308, 34564, 34820, 35076, 35332, 35588, 35844, 36100, 36356, 36612). The source IP is consistently 192.168.100.2 and the destination is 143.89.12.134. The bottom pane shows the details of packet 585, which is an ICMP Echo request. It identifies the Ethernet II frame, the IP version 4 header, and the ICMP Echo request protocol. The hex dump and ASCII representation of the packet data are also visible at the bottom.

No.	Time	Source	Destination	Protocol	Length	Info
585	5.845265	192.168.100.2	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=1158/34308, ttl=128 (reply in 619)
619	6.170704	143.89.12.134	192.168.100.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1158/34308, ttl=48 (request in 585)
700	6.861721	192.168.100.2	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=1159/34564, ttl=128 (reply in 735)
735	7.187569	143.89.12.134	192.168.100.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1159/34564, ttl=48 (request in 700)
796	7.866962	192.168.100.2	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=1160/34820, ttl=128 (reply in 833)
833	8.193154	143.89.12.134	192.168.100.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1160/34820, ttl=48 (request in 796)
895	8.882337	192.168.100.2	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=1161/35076, ttl=128 (reply in 927)
927	9.208728	143.89.12.134	192.168.100.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1161/35076, ttl=48 (request in 895)
1001	9.899436	192.168.100.2	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=1162/35332, ttl=128 (reply in 1032)
1032	10.225422	143.89.12.134	192.168.100.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1162/35332, ttl=48 (request in 1001)
1110	10.917761	192.168.100.2	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=1163/35588, ttl=128 (reply in 1144)
1144	11.243621	143.89.12.134	192.168.100.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1163/35588, ttl=48 (request in 1110)
1216	11.933429	192.168.100.2	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=1164/35844, ttl=128 (reply in 1251)
1251	12.259056	143.89.12.134	192.168.100.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1164/35844, ttl=48 (request in 1216)
1321	12.949913	192.168.100.2	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=1165/36100, ttl=128 (reply in 1355)
1355	13.275642	143.89.12.134	192.168.100.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1165/36100, ttl=48 (request in 1321)
1426	13.968975	192.168.100.2	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=1166/36356, ttl=128 (reply in 1460)
1460	14.294881	143.89.12.134	192.168.100.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1166/36356, ttl=48 (request in 1426)
1524	14.979751	192.168.100.2	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=1167/36612, ttl=128 (reply in 1563)
1563	15.305214	143.89.12.134	192.168.100.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1167/36612, ttl=48 (request in 1524)

Frame 585: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF{0DEA2AF1-DF66-4FB3-90F2-FE83EEC0FAB7}, id 0
> Ethernet II, Src: Elitro_72:c0:2f (74:27:ea:72:c0:2f), Dst: HuaweiTe_f7:6a:0c (ac:75:1d:f7:6a:0c)
> Internet Protocol Version 4, Src: 192.168.100.2, Dst: 143.89.12.134
> Internet Control Message Protocol

0000 ac 75 1d f7 6a 0c 74 27 ea 72 c0 2f 08 00 45 00 ..u.j.t'..r./..E
0010 00 3c 48 09 00 00 80 01 32 2e c0 a8 64 02 8f 59 <H.....2...d..Y
0020 0c 86 08 00 48 d5 00 01 04 86 61 62 63 64 65 66H.....abcdf

Internet Control Message Protocol: Protocol

Packets: 2020 • Displayed: 20 (1.0%) • Dropped: 0 (0.0%)

Figura 2: Pacotes ICMP do ping

R = O endereço IP de meu host é o 192.168.100.2 e o endereço IP do host de destino é o 143.89.12.134

2. Por que um pacote ICMP não tem números de porta de origem e destino?

R = Pelo fato de que o pacote ICMP ter sido feito para comunicar informações da camada de rede dos hosts e não nos processos da camada de aplicação. O pacote ICMP tem seu tipo, código que identifica o recebimento da mensagem. Não há uso de portas para direcionamento de mensagem.

3. Examine um dos pacotes de solicitação de ping enviados por seu host. Quais são o tipo de ICMP e os números de código? Que outros campos este pacote ICMP possui? Quantos bytes são os campos de checksum, número de sequência e identificador?

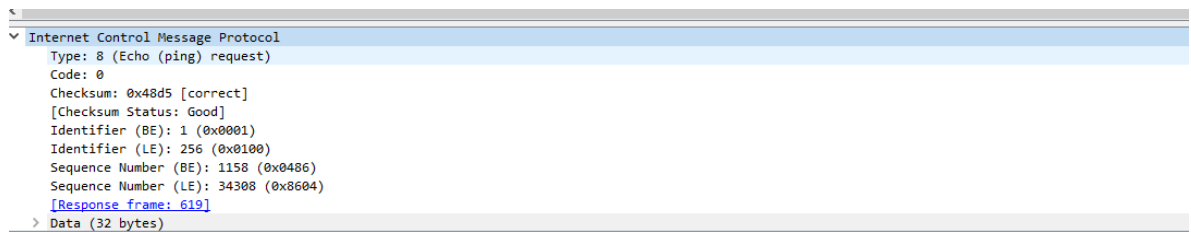


Figura 3: Um dos pacotes ICMP

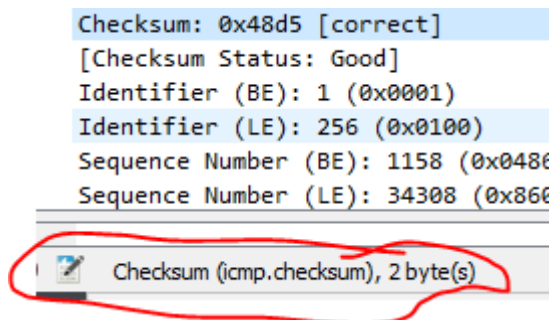


Figura 4: Checksum 2 bytes

R = O tipo de ICMP é o 8 (Echo) (Ping) request). O código é o 0. Possui os campos checksum, identificador, número de sequência, dados. Os campos checksum, sequence number e identifier possuem 2 bytes cada um.

4. Examine o pacote de resposta de ping correspondente. Quais são o tipo de ICMP e os números de código? Que outros campos este pacote ICMP possui? Quantos bytes são os campos de checksum, número de sequência e identificador?

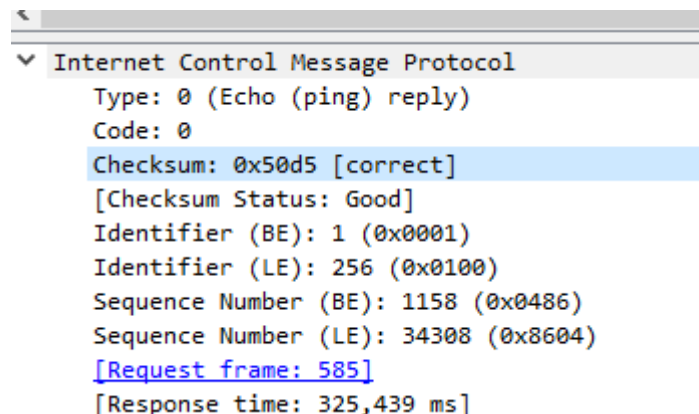


Figura 5: Ping reply

R = O tipo de ICMP é o 0. (Echo (ping) reply). O código é numero 0. Possui os campos de checksum, identificador, número de sequência, tempo de resposta, frame request. Os campos identificador, número de sequência e checksum possuem 2 bytes cada um.

5. Qual é o endereço IP do seu host? Qual é o endereço IP do host de destino de destino?

```
C:\Users\Renato>tracert www.inria.fr

Rastreando a rota para inria.fr [128.93.162.83]
com no máximo 30 saltos:

 1  <1 ms    <1 ms    <1 ms    192.168.100.1
 2  *        11 ms    *        terra-200-225-254-248.dynamic.idial.com.br [200.225.254.248]
 3  2 ms     3 ms     3 ms     100.127.5.35
 4  *        3 ms     *        187-032-149-225.static.ctbctelecom.com.br [187.32.149.225]
 5  121 ms   121 ms   122 ms   100.126.3.206
 6  123 ms   121 ms   124 ms   100.127.6.98
 7  18 ms    14 ms    22 ms    100.127.6.154
 8  121 ms   120 ms   121 ms   et-2-1-2-0.sac.border-b.mia.algartelem.com.br [168.197.23.185]
 9  120 ms   131 ms   129 ms   ae40.cr6-mia1.ip4.gtt.net [98.124.189.121]
10  221 ms   220 ms   220 ms   et-3-3-0.cr2-par7.ip4.gtt.net [213.200.119.214]
11  220 ms   221 ms   223 ms   renater-gw-ix1.gtt.net [77.67.123.206]
12  222 ms   221 ms   228 ms   te1-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
13  221 ms   221 ms   221 ms   inria-roquencourt-gi3-2-inria-rtr-021.noc.renater.fr [193.51.184.177]
14  222 ms   221 ms   222 ms   unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
15  221 ms   228 ms   221 ms   prod-inriafr-cms.inria.fr [128.93.162.83]

Rastreamento concluído.
```

Figura 6: tracert www.inria.fr

No.	Time	Source	Destination	Protocol	Length	Info
587	4.886343	192.168.100.2	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=1184/40964, ttl=1 (no response found!)
588	4.886759	192.168.100.1	192.168.100.2	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
589	4.887313	192.168.100.2	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=1185/41220, ttl=1 (no response found!)
590	4.887534	192.168.100.1	192.168.100.2	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
591	4.888139	192.168.100.2	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=1186/41476, ttl=1 (no response found!)
592	4.888362	192.168.100.1	192.168.100.2	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
613	4.931932	192.168.100.1	192.168.100.2	ICMP	120	Destination unreachable (Port unreachable)
819	6.434811	192.168.100.1	192.168.100.2	ICMP	120	Destination unreachable (Port unreachable)
1019	7.947937	192.168.100.1	192.168.100.2	ICMP	120	Destination unreachable (Port unreachable)
1354	10.459731	192.168.100.2	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=1187/41732, ttl=2 (no response found!)
1730	14.046270	192.168.100.2	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=1188/41988, ttl=2 (no response found!)
1732	14.048911	200.225.254.248	192.168.100.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1738	14.059043	192.168.100.2	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=1189/42244, ttl=2 (no response found!)
2145	18.061936	192.168.100.2	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=1190/42500, ttl=3 (no response found!)
2146	18.064547	100.127.5.35	192.168.100.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2148	18.065705	192.168.100.2	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=1191/42756, ttl=3 (no response found!)
2149	18.068832	100.127.5.35	192.168.100.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2150	18.069470	192.168.100.2	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=1192/43012, ttl=3 (no response found!)
2151	18.073019	100.127.5.35	192.168.100.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2305	19.084365	192.168.100.2	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=1193/43268, ttl=4 (no response found!)
2871	23.049817	192.168.100.2	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=1194/43524, ttl=4 (no response found!)

> Frame 587: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{0DEA2AF1-DFF6-4FB3-9DF2-FE83EEC0FAB7}, id 0
> Ethernet II, Src: Elitegro_72:c0:2f (74:27:ea:72:c0:2f), Dst: HuaweiTe_f7:6a:0c (ac:75:1d:f7:6a:0c)
> Internet Protocol Version 4, Src: 192.168.100.2, Dst: 128.93.162.83
> Internet Control Message Protocol

Figura 7: Pacotes ICMP tracert

R = O endereço IP de meu host é o 192.168.100.2 e o endereço IP do host de destino é o 128.93.162.83

6. Se o ICMP enviar pacotes UDP (como no Unix/Linux), o número do protocolo IP ainda seria 01 para os pacotes examinados? Se não, o que seria?

R = Não, pois caso o ICMP enviar pacotes UDP o número do protocolo IP é o 0x11 no lugar de 01.

7. Examine o pacote de eco ICMP em sua captura de tela. Isso é diferente dos pacotes de consulta de ping ICMP na primeira metade deste laboratório? Se sim, como assim?

587	4.886343	192.168.100.2	128.93.162.83	ICMP	106 Echo (ping) request id=0x0001, seq=1184/40964, ttl=1 (no response found!)
588	4.886759	192.168.100.1	192.168.100.2	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
589	4.887313	192.168.100.2	128.93.162.83	ICMP	106 Echo (ping) request id=0x0001, seq=1185/41220, ttl=1 (no response found!)
590	4.887534	192.168.100.1	192.168.100.2	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
591	4.888139	192.168.100.2	128.93.162.83	ICMP	106 Echo (ping) request id=0x0001, seq=1186/41476, ttl=1 (no response found!)
592	4.888362	192.168.100.1	192.168.100.2	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
613	4.931932	192.168.100.1	192.168.100.2	ICMP	120 Destination unreachable (Port unreachable)
819	6.434811	192.168.100.1	192.168.100.2	ICMP	120 Destination unreachable (Port unreachable)
1019	7.947937	192.168.100.1	192.168.100.2	ICMP	120 Destination unreachable (Port unreachable)
1354	10.459731	192.168.100.2	128.93.162.83	ICMP	106 Echo (ping) request id=0x0001, seq=1187/41732, ttl=2 (no response found!)
1730	14.046270	192.168.100.2	128.93.162.83	ICMP	106 Echo (ping) request id=0x0001, seq=1188/41988, ttl=2 (no response found!)
1732	14.048911	200.225.254.248	192.168.100.2	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
1738	14.059043	192.168.100.2	128.93.162.83	ICMP	106 Echo (ping) request id=0x0001, seq=1189/42244, ttl=2 (no response found!)
2145	18.061936	192.168.100.2	128.93.162.83	ICMP	106 Echo (ping) request id=0x0001, seq=1190/42500, ttl=3 (no response found!)
2146	18.064547	100.127.5.35	192.168.100.2	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
2148	18.065705	192.168.100.2	128.93.162.83	ICMP	106 Echo (ping) request id=0x0001, seq=1191/42756, ttl=3 (no response found!)
2149	18.068832	100.127.5.35	192.168.100.2	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
2150	18.069470	192.168.100.2	128.93.162.83	ICMP	106 Echo (ping) request id=0x0001, seq=1192/43012, ttl=3 (no response found!)
2151	18.073019	100.127.5.35	192.168.100.2	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
2305	19.084365	192.168.100.2	128.93.162.83	ICMP	106 Echo (ping) request id=0x0001, seq=1193/43268, ttl=4 (no response found!)
2871	23.049817	192.168.100.2	128.93.162.83	ICMP	106 Echo (ping) request id=0x0001, seq=1194/43524, ttl=4 (no response found!)

Internet Control Message Protocol					
Type:	8 (Echo (ping) request)				
Code:	0				
Checksum:	0xf35e [correct]				
[Checksum Status:	Good]				
Identifier (BE):	1 (0x0001)				
Identifier (LE):	256 (0x0100)				
Sequence Number (BE):	1184 (0x04a0)				
Sequence Number (LE):	40964 (0xa004)				
> [No response seen]					
> Data (64 bytes)					

Figura 8: Pacotes ICMP tracer Echo

R = Não, possuem os mesmos campos ICMP, o que muda no pacote em si seria o valor de ttl e o no response found.

8. Examine o pacote de erro ICMP em sua captura de tela. Ele tem mais campos do que o pacote de eco ICMP. O que está incluído nesses campos?

Internet Control Message Protocol	
Type:	11 (Time-to-live exceeded)
Code:	0 (Time to live exceeded in transit)
Checksum:	0xf4ff [correct]
[Checksum Status:	Good]
Unused:	00000000
Internet Protocol Version 4, Src: 192.168.100.2, Dst: 128.93.162.83	
0100 = Version:	4
.... 0101 = Header Length:	20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)	
Total Length:	92

Figura 8: Pacote erro ICMP ttl exceeded

R = O pacote não é o mesmo de ping, ele possui alguns campos diferentes, como unused, tipo diferente que é o 11, embaixo o cabeçalho ipv4. Considerando os campos apenas da aba ICMP, possuem menos campos do que o pacote eco.

9. Examine os últimos três pacotes ICMP recebidos pelo host de origem. Como esses pacotes são diferentes dos pacotes de erro ICMP? Por que eles são diferentes?

5414	43.935616	192.168.100.2	128.93.162.83	ICMP	106 Echo (ping) request id=0x0001, seq=1226/51716, ttl=15 (reply in 5439)
5439	44.157395	128.93.162.83	192.168.100.2	ICMP	106 Echo (ping) reply id=0x0001, seq=1226/51716, ttl=53 (request in 5414)
5440	44.158966	192.168.100.2	128.93.162.83	ICMP	106 Echo (ping) request id=0x0001, seq=1227/51972, ttl=15 (reply in 5457)
5457	44.381525	128.93.162.83	192.168.100.2	ICMP	106 Echo (ping) reply id=0x0001, seq=1227/51972, ttl=53 (request in 5440)
5461	44.388636	192.168.100.2	128.93.162.83	ICMP	106 Echo (ping) request id=0x0001, seq=1228/52228, ttl=15 (reply in 5475)

Source Address: 128.93.162.83

Destination Address: 192.168.100.2

Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

Checksum: 0xfb32 [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence Number (BE): 1228 (0x04cc)

Sequence Number (LE): 52228 (0xcc04)

[Request frame: 5461]

[Response time: 221,737 ms]

> Data (64 bytes)

Figura 9: Um dos três últimos pacotes

R = O tipo é o 0, diferente do de erro que é o 11, os pacotes são diferentes pelo fato dos datagramas irem pro host de destino antes de expirar o TTL.

10. Dentro das medições do tracer, existe um link cujo atraso é significativamente maior do que outros? Consulte a captura de tela na Figura 4, há um link cujo atraso é significativamente maior do que outros? Com base nos nomes dos roteadores, você consegue supor a localização dos dois roteadores no final deste link?

```
DOWS\SYSTEM32>
DOWS\SYSTEM32>
DOWS\SYSTEM32>
DOWS\SYSTEM32>tracert www.inria.fr

g route to www.inria.fr [138.96.146.2]
maximum of 30 hops:
 13 ms      12 ms      13 ns      10.216.228.1
 21 ms      14 ms      13 ns      24.218.0.153
 12 ms      11 ms      13 ns      bar01-p4-0.wsfdhe1.ma.attbb.net [24.128.190.197]
 16 ms      16 ms      15 ns      bar02-p6-0.ndhmhe1.ma.attbb.net [24.128.0.101]
 15 ms      15 ms      15 ns      12.125.47.49
 17 ms      17 ms      17 ns      12.123.40.218
 22 ms      23 ms      22 ns      thr2-cl1.n54ny.ip.att.net [12.122.10.22]
 23 ms      23 ms      23 ns      ggr2-p3120.n54ny.ip.att.net [12.123.3.109]
 26 ms      21 ms      25 ns      att-gw.nyc.opentransit.net [192.205.32.138]
 98 ms      98 ms      96 ns      P4-0.PASCR1.Pastourelle.opentransit.net [193.251.241.133]
 97 ms      98 ms      98 ns      P9-0.AUUCR1.Aubervilliers.opentransit.net [193.251.243.29]
 98 ms      98 ms      108 ns      P6-0.BAGCR1.Bagnolet.opentransit.net [193.251.241.93]
 104 ms     106 ms      103 ns      193.51.185.30
 14 ms      114 ms      117 ns      grenoble-pos1-0.cssi.renater.fr [193.51.179.238]
 114 ms     115 ms      114 ns      nice-pos2-0.cssi.renater.fr [193.51.180.34]
 129 ms     114 ms      118 ns      inria-nice.cssi.renater.fr [193.51.181.137]
 113 ms     114 ms      112 ns      www.inria.fr [138.96.146.2]
```

Figura 10: Figura 4 do Wireshark ICMP lab usado para esta questão

R = Há um link de cidades e países, como por exemplo, nyc.opentransit.net para PASCR1.pastourelle, ou seja de New York (EUA) para Pastourelle, depois de Pastourelle para Aubervilliers que fica na França, depois de Aubervilliers para Bagnolet.