

Universidade Federal do Tocantins, Câmpus Palmas

Disciplina: Redes de Computadores

Prof. Gentil Veloso

Alunos: Ana Flavia Moreira Pires e Romeu Miranda Borges

Data: 12/06/2024

ICMP e Ping

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

Podemos observar que o IP do meu host é 192.168.100.6, enquanto o IP do host de destino é 143.89.12.134.

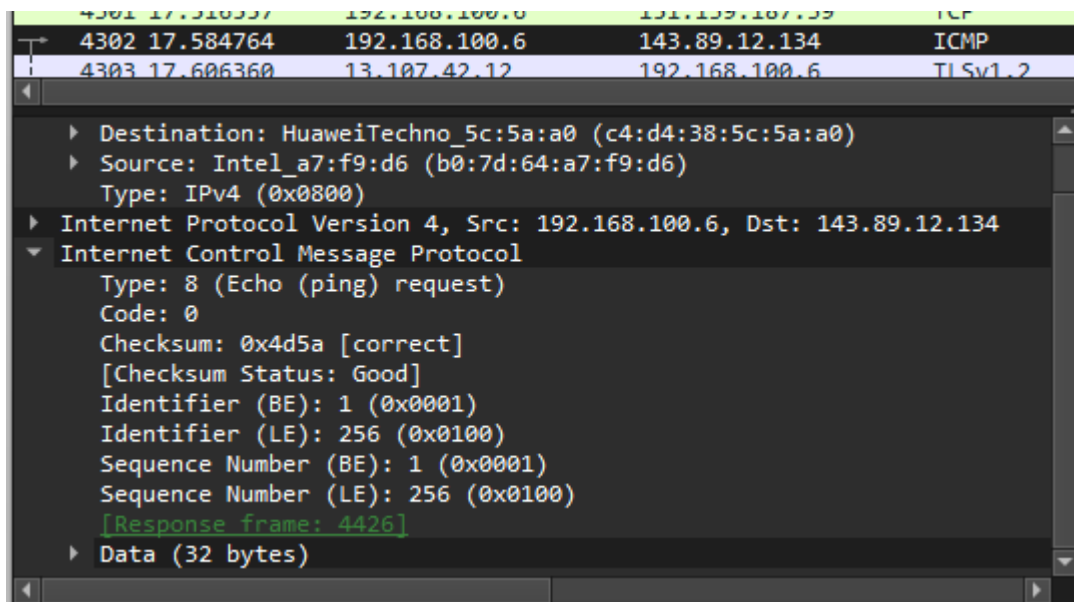
Time	Source	Destination	Protocol
17.516426	151.139.187.39	192.168.100.6	TCP
17.516426	151.139.187.39	192.168.100.6	TCP
17.516557	192.168.100.6	151.139.187.39	TCP
17.584764	192.168.100.6	143.89.12.134	ICMP

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

Porque os números de porta são dados pertencentes à camada de transporte, uma vez que identificam a aplicação de origem e destino em cada máquina e que a camada de transporte é responsável por levar o pacote até a porta desejada. O protocolo ICMP atua na camada de rede, por isso, apenas o endereço IP é suficiente para que ele faça o seu trabalho, pois ele não precisa transmitir dados entre as aplicações.

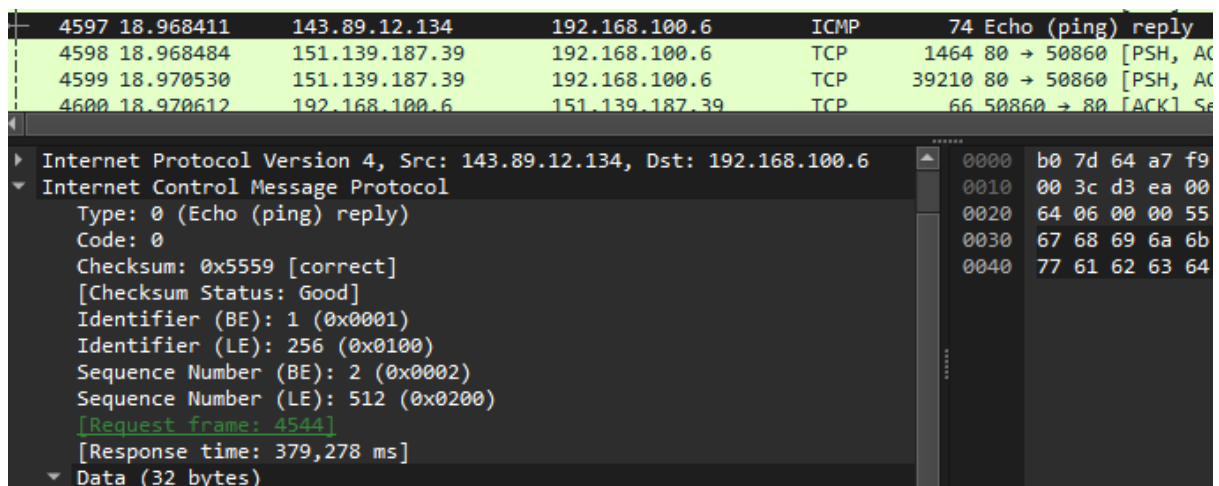
3. Examine um dos pacotes de solicitação de ping enviados pelo seu host. Quais são os números de tipo e código ICMP? Quais outros campos esse pacote ICMP possui? Quantos bytes têm os campos de checksum, número de sequência e identificador?

O número de tipo é 8, representando um tipo de solicitação de ping. O código ICMP é 0. O pacote ICMP possui os campos de identificador, número de sequência e checksum, que possuem 2 bytes, uma vez que são representados por números hexadecimais de 16 bits.



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

O número de tipo é 0, representando um tipo de resposta de ping. O código ICMP é 0. O pacote ICMP possui os campos de identificador, número de sequência e checksum, que possuem 2 bytes, uma vez que são representados por números hexadecimais de 16 bits.



ICMP e Traceroute

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

Podemos observar que o IP do meu host é 192.168.100.6, enquanto o IP do host de destino é 128.93.162.83.

No.	Time	Source	Destination	Protocol
1401	151.005014	192.168.100.6	128.93.162.83	ICMP
1402	151.470335	192.168.100.6	128.93.162.83	ICMP
1403	151.688402	128.93.162.83	192.168.100.6	ICMP
1404	151.689604	192.168.100.6	128.93.162.83	ICMP
1405	151.907570	128.93.162.83	192.168.100.6	ICMP
1406	151.908271	192.168.100.6	128.93.162.83	ICMP
1407	151.927885	2804:d59:8e25:c900::...	2800:3f0:4003:c03::...	TCP
1408	152.021752	2800:3f0:4003:c03::...	2804:d59:8e25:c900::...	TCP
1409	152.126105	128.93.162.83	192.168.100.6	ICMP
1410	152.137366	fe80::e234:a7a9:535...	fe80::1	DNS

```

Frame 1402: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on
Ethernet II, Src: Intel_a7:f9:d6 (b0:7d:64:a7:f9:d6), Dst: HuaweiTechno_5
Internet Protocol Version 4, Src: 192.168.100.6, Dst: 128.93.162.83
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xf7b1 [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 77 (0x004d)
  Sequence Number (LE): 19712 (0x4d00)
  [Response frame: 1403]
  Data (64 bytes)
  
```

2. Se o ICMP enviasse pacotes UDP em vez disso (como no Unix/Linux), o número do protocolo IP ainda seria 01 para os pacotes de sonda? Se não, qual seria?

Caso o ICMP enviasse pacotes UDP, o número do protocolo IP, que estaria no campo abaixo, seria 17.

```

Internet Protocol Version 4, Src: 192.168.100.6, Dst: 128.93.162.83
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-Set)
  Total Length: 92
  Identification: 0x18ef (6383)
  ▶ 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 14
  Protocol: ICMP (1)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.100.6
  Destination Address: 128.93.162.83
Internet Control Message Protocol
  
```

3. Examine o pacote ICMP echo na sua captura de tela. Este é diferente dos pacotes de consulta ping ICMP na primeira metade deste laboratório? Se sim, como?

Sim. Como podemos ver na imagem abaixo, os dados relacionados ao número de sequência são maiores, indicando que o procedimento de traceroute trabalha com uma quantidade maior de pacotes

```
Internet Protocol Version 4, Src: 192.168.100.6, Dst: 192.168.100.1
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xf7ca [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 52 (0x0034)
  Sequence Number (LE): 13312 (0x3400)
  [No response seen]
  Data (64 bytes)
```

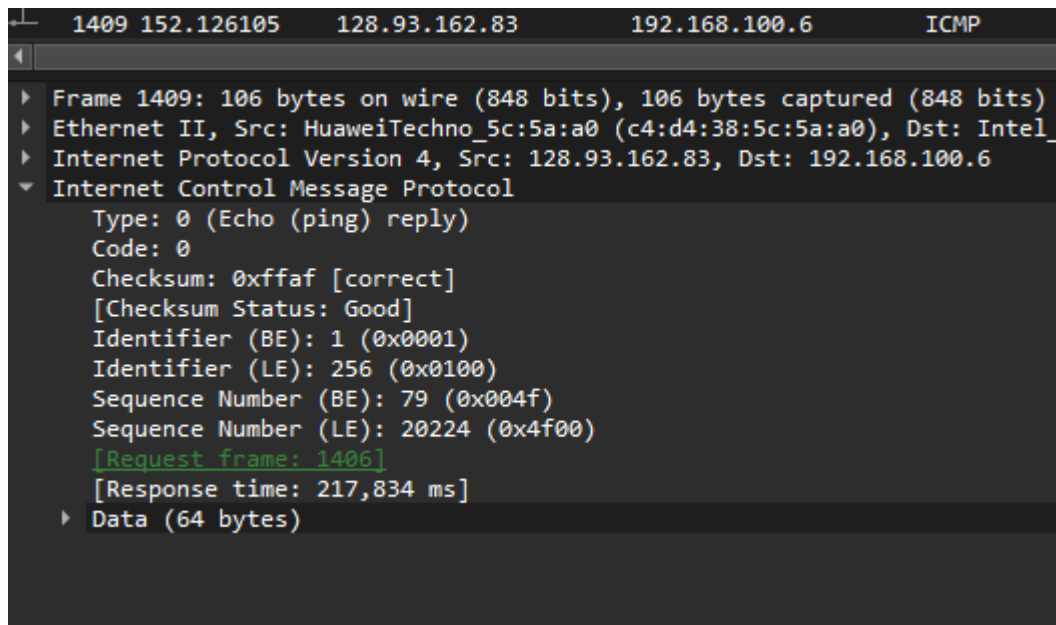
4. Examine o pacote de erro ICMP na sua captura de tela. Ele tem mais campos do que o pacote ICMP echo. O que está incluído nesses campos?

Dentro de um pacote de erro ICMP, estão incluídos os cabeçalhos do protocolo IP e ICMP do pacote relacionado ao erro.

```
Internet Protocol Version 4, Src: 192.168.100.1, Dst: 192.168.100.6
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: 192.168.100.6, Dst: 128.93.162.83
  Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7f3 [unverified] [in ICMP error packet]
    [Checksum Status: Unverified]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 11 (0x000b)
    Sequence Number (LE): 2816 (0x0b00)
    Data (64 bytes)
```

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

Esses pacotes são do tipo 0, contam com o campo checksum dado como correto e contém informações sobre o pacote enviado, como o tempo de resposta e o corpo da requisição, no campo Data.



6. Dentro das medições do tracert, há um link cujo atraso é significativamente maior que os outros? Consulte a captura de tela na Figura 4, há um link cujo atraso é significativamente maior que os outros? Com base nos nomes dos roteadores, você pode adivinhar a localização dos dois roteadores nas extremidades desse link?

As últimas requisições foram as mais demoradas, e, pelo nome do domínio (.fr), é possível que esses roteadores se situem na França.

```

MINIMO = 371ms, MAXIMO = 380ms, MEDIA = 374ms
PS C:\Users\romeu> tracert www.inria.fr

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

  1    1 ms    59 ms    38 ms    192.168.100.1
  2    7 ms     5 ms     5 ms    177-203-182-1.user3p.brasiltelecom.net.br [177.203.182.1]
  3    6 ms     4 ms     6 ms    100.120.66.177
  4   22 ms    24 ms    22 ms    100.120.25.31
  5    *      *      *      Esgotado o tempo limite do pedido.
  6    *      *      *      Esgotado o tempo limite do pedido.
  7   40 ms    40 ms    40 ms    45.238.97.194
  8   91 ms    76 ms    76 ms    200.16.69.44
  9  145 ms   145 ms   146 ms    200.16.69.2
 10    *      *      148 ms    ca-1-3-1.ter1.lga5.us.zip.zayo.com [208.185.175.77]
 11    *      *      *      Esgotado o tempo limite do pedido.
 12    *      *      *      Esgotado o tempo limite do pedido.
 13    *      *      *      Esgotado o tempo limite do pedido.
 14  217 ms   217 ms   220 ms    ae20.cr1.cdg12.fr.zip.zayo.com [64.125.31.99]
 15  216 ms   216 ms   217 ms    ae4.cr1.cdg11.fr.zip.zayo.com [64.125.20.113]
 16  219 ms   218 ms   221 ms    ae3.mcs1.cdg11.fr.zip.zayo.com [64.125.28.17]
 17    *      *      *      Esgotado o tempo limite do pedido.
 18  217 ms   273 ms   284 ms    hu0-4-0-1-ren-nr-orsay-rtr-091.noc.renater.fr [193.51.180.43]
 19  222 ms   221 ms   222 ms    te-0-0-0-ren-nr-jouy-rtr-091.noc.renater.fr [193.55.204.203]
 20  217 ms   216 ms   217 ms    te2-8-inria-rtr-021.noc.renater.fr [193.51.180.125]
 21  218 ms   218 ms   219 ms    inria-rocquencourt-vl1631-ta1-ll-inria-rtr-021.noc.renater.fr [193.51.180.125]
 22  221 ms   220 ms   220 ms    unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
 23  218 ms   218 ms   217 ms    prod-inriafr-cms.inria.fr [128.93.162.83]

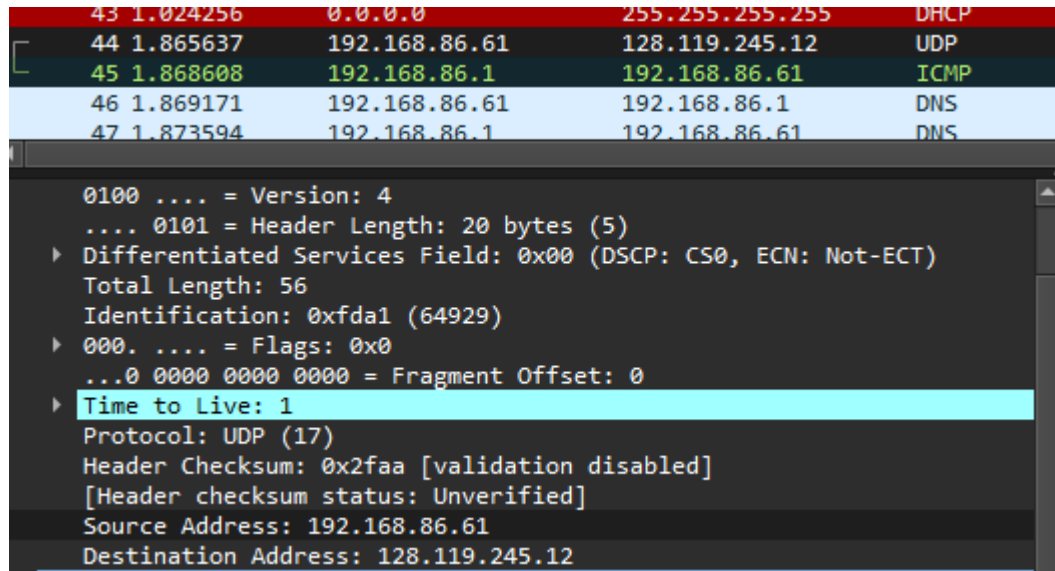
```

LABORATÓRIO IP 8.1

IPv4

1. Selecione o primeiro segmento UDP enviado pelo seu computador através do comando traceroute para gaia.cs.umass.edu. Expanda a parte do Protocolo da Internet (Internet Protocol) do pacote na janela de detalhes do pacote. Qual é o endereço IP do seu computador?

O endereço da máquina de origem é 192.168.86.61.



2. Qual é o valor no campo de tempo de vida (TTL) no cabeçalho deste datagrama IPv4?

Como é possível verificar no print acima, o TTL é igual a 1.

3. Qual é o valor no campo de protocolo de camada superior neste datagrama IPv4?
[Nota: as respostas para Linux/MacOS diferem das de Windows aqui.]

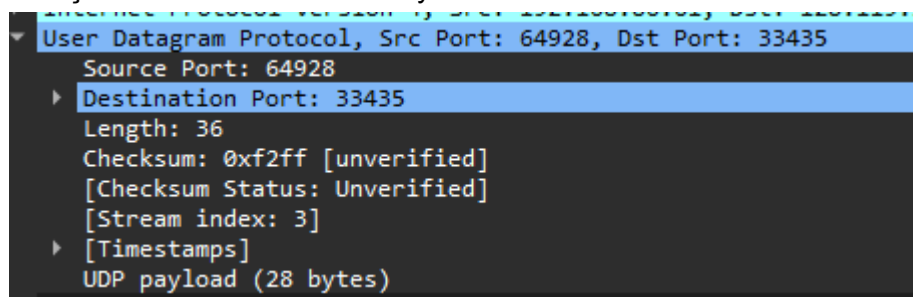
O valor é UDP (17).

4. Quantos bytes há no cabeçalho IP?

20 bytes, segundo o campo Header Length.

5. Quantos bytes há na carga útil (payload) do datagrama IP? Explique como você determinou o número de bytes da carga útil.

O número de bytes da carga útil pode ser determinado pela informação dada pelo cabeçalho UDP. O número de bytes é 28.



6. Este datagrama IP foi fragmentado? Explique como você determinou se o datagrama foi fragmentado ou não.

Existe um campo dentro do datagrama IP chamado Flags, que contém indicativos relacionados à fragmentação do datagrama. Neste caso, temos o campo Fragment Offset dado como zero, e todos os outros campos dados como Not set, indicando que o datagrama não está fragmentado.

43	1.024256	0.0.0.0	255.255.255.255	DHCP
44	1.865637	192.168.86.61	128.119.245.12	UDP
45	1.868608	192.168.86.1	192.168.86.61	ICMP
46	1.869171	192.168.86.61	192.168.86.1	DNS
47	1.873594	192.168.86.1	192.168.86.61	DNS


```
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 56
Identification: 0xfda1 (64929)
▼ 000. .... = Flags: 0x0
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..0. .... = More fragments: Not set
  ...0 0000 0000 0000 = Fragment Offset: 0
▶ Time to Live: 1
```

7. Quais campos no datagrama IP sempre mudam de um datagrama para o próximo dentro desta série de segmentos UDP enviados pelo seu computador com destino a 128.119.245.12, via traceroute? Por quê?

Os campos de identificação, TTL e checksum. Identificação e checksum mudam pois são procedimentos individuais de cada pacote. Já o campo TTL se incrementa sempre de 1 em 1, pois aumenta de acordo com a quantidade de roteadores pelos quais aquele pacote deve ser capaz de passar até que ele seja descartado, até que seja alcançado o host de destino.

8. Quais campos nesta sequência de datagramas IP (contendo segmentos UDP) permanecem constantes? Por quê?

Os campos de IP de origem e destino e de flags, que sempre indicam que o datagrama não é fragmentado. Eles não mudam, pois são dados relativos a todo o procedimento de traceroute.

9. Descreva o padrão que você observa nos valores no campo de Identificação dos datagramas IP sendo enviados pelo seu computador.

O número de identificação aumenta sempre de 1 em 1 de um pacote para outro, o que indica que os pacotes são enviados de forma sequencial e linear ao host de destino.

10. Qual é o protocolo de camada superior especificado nos datagramas IP retornados pelos roteadores? [Nota: as respostas para Linux/MacOS diferem das de Windows aqui].

ICMP

11. Os valores nos campos de Identificação (através da sequência de todos os pacotes ICMP de todos os roteadores) são semelhantes ao comportamento da sua resposta à pergunta 9 acima?

Não. Os campos de identificação são sempre iguais a zero, em todos os pacotes deste caso.

12. Os valores dos campos TTL são semelhantes através de todos os pacotes ICMP de todos os roteadores?

Não. Os campos de TTL são valores altos, provavelmente para garantir que o retorno de erro alcance o roteador de origem tranquilamente.

Fragmentação

1. Encontre o primeiro datagrama IP que contém a primeira parte do segmento enviado pelo seu computador para 128.119.245.12, via comando traceroute para gaia.cs.umass.edu, depois que você especificou que o comprimento do pacote traceroute deveria ser 3000 bytes. Esse segmento foi fragmentado através de mais de um datagrama IP?

Sim.

178	10.370823	52.114.132.176	192.168.86.61	TCP
179	12.788154	192.168.86.61	128.119.245.12	IPv4
180	12.788155	192.168.86.61	128.119.245.12	IPv4
181	12.788155	192.168.86.61	128.119.245.12	UDP
182	12.792190	192.168.86.1	192.168.86.61	ICMP

Source:	Apple_98:d9:27 (78:4f:43:98:d9:27)
Type:	IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.86.61, Dst: 128.119.245.12	
0100 = Version: 4	
.... 0101 = Header Length: 20 bytes (5)	
Differentially Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)	
Total Length: 1500	
Identification: 0xfda2 (64930)	
001. = Flags: 0x1, More fragments	
0... = Reserved bit: Not set	
.0.. = Don't Fragment: Not set	
..1. = More fragments: Set	
...0 0000 0000 0000 = Fragment Offset: 0	
Time to Live: 1	

2. Que informações no cabeçalho IP indicam que este datagrama foi fragmentado?

O campo Flags, que possui a Flag “More Fragments” definida.

3. Que informações no cabeçalho IP deste pacote indicam se este é o primeiro fragmento ou um fragmento posterior?

O campo fragment offset, que indica a posição do fragmento em relação ao início do datagrama original. Neste caso, o offset é zero, ou seja, este fragmento é o primeiro.

4. Quantos bytes há neste datagrama IP (cabeçalho mais carga útil)?

1500

5. Agora, inspecione o datagrama que contém o segundo fragmento do segmento UDP fragmentado. Que informações no cabeçalho IP indicam que este não é o primeiro fragmento do datagrama?

O campo fragment offset, que indica que este fragmento se inicia na posição 1480 do datagrama original, ou seja, não é o primeiro fragmento.

180	12.788155	192.168.86.61	128.119.245.12	IPv4	1514
• 181	12.788155	192.168.86.61	128.119.245.12	UDP	54
182	12.792190	192.168.86.1	192.168.86.61	ICMP	590
183	12.792881	192.168.86.61	128.119.245.12	IPv4	1514
184	12.792882	192.168.86.61	128.119.245.12	IPv4	1514
185	12.792882	192.168.86.61	128.119.245.12	UDP	54

▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0xfda2 (64930)
▶ 001. = Flags: 0x1, More fragments
...0 0000 1011 1001 = Fragment Offset: 1480
▶ Time to Live: 1
Protocol: UDP (17)

6. Quais campos mudam no cabeçalho IP entre o primeiro e o segundo fragmento?

O campo flags, por conta das mudanças na flag Fragment Offset, e o campo de checksum, por ser uma identificação individual do pacote.

7. Agora, encontre o datagrama IP que contém o terceiro fragmento do segmento UDP original. Que informações no cabeçalho IP indicam que este é o último fragmento desse segmento?

Fragment Offset é maior que zero e a flag More Fragments não está definida. Ou seja, este fragmento não é o primeiro, mas não existem outros depois dele, indicando que ele é o último.

181	12.788155	192.168.86.61	128.119.245.12	UDP	
182	12.792190	192.168.86.1	192.168.86.61	ICMP	
183	12.792881	192.168.86.61	128.119.245.12	IPv4	

▼ Internet Protocol Version 4, Src: 192.168.86.61, 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: 40
Identification: 0xfda2 (64930)
▼ 000. = Flags: 0x0
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
...0 0001 0111 0010 = Fragment Offset: 2960
▶ Time to Live: 1
Protocol: UDP (17)
Header Checksum: 0x2e47 [validation disabled]
[Header checksum status: Unverified]

IPv6

1. Qual é o endereço IPv6 do computador que está fazendo a solicitação DNS AAAA? Este é o endereço de origem do 20º pacote no rastreamento. Forneça o endereço IPv6 de origem para este datagrama na mesma forma exata exibida na janela do Wireshark.

2601:193:8302:4620:215c:f5ae:8b40:a27a

2. Qual é o endereço IPv6 de destino para este datagrama? Forneça este endereço IPv6 na mesma forma exata exibida na janela do Wireshark.

2001:558:feed::1

3. Qual é o valor do rótulo de fluxo (flow label) para este datagrama?

0x63ed0

4. Quantos dados de carga útil são transportados neste datagrama?

37 bytes.

5. Qual é o protocolo de camada superior para o qual a carga útil deste datagrama será entregue no destino?

UDP (17)

19	3.814364	2601:193:8302:4620:215c:f5ae:8b40:a27a	2001:558:feed::1	DNS	9
20	3.814489	2601:193:8302:4620:215c:f5ae:8b40:a27a	2001:558:feed::1	DNS	9
21	3.819370	2601:193:8302:4620:215c:f5ae:8b40:a27a	2001:558:feed::1	DNS	9
22	3.819905	2601:193:8302:4620:215c:f5ae:8b40:a27a	2001:558:feed::1	DNS	9
23	3.946846	2001:558:feed::1	2601:193:8302:4620:...	DNS	16
24	3.953852	2001:558:feed::1	2601:193:8302:4620:...	DNS	24
25	3.954763	2601:193:8302:4620:215c:f5ae:8b40:a27a	2001:558:feed::1	DNS	16
26	3.955402	2001:558:feed::1	2601:193:8302:4620:...	DNS	33
27	3.955405	2001:558:feed::1	2601:193:8302:4620:...	DNS	11

▶ Frame 20: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface	0000	44 1c 12 81 74 5a 7
▶ Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: VantivaUSA_81:	0010	3e d0 00 25 11 ff 2
▶ Internet Protocol Version 6, Src: 2601:193:8302:4620:215c:f5ae:8b40:a27a,	0020	f5 ae 8b 40 a2 7a 2
0110 = Version: 6	0030	00 00 00 00 00 01 1
▶ 0000 0000 = Traffic Class: 0x00 (DSCP: C	0040	01 00 00 01 00 00 0
.... 0110 0011 1110 1101 0000 = Flow Label: 0x63ed0	0050	62 65 03 63 6f 6d 0
Payload Length: 37		
Next Header: UDP (17)		
Hop Limit: 255		
Source Address: 2601:193:8302:4620:215c:f5ae:8b40:a27a		
Destination Address: 2001:558:feed::1		
User Datagram Protocol, Src Port: 64430, Dst Port: 53		

6. Quantos endereços IPv6 são retornados na resposta a esta solicitação AAAA?

São retornadas 5 respostas.

```

23 3.946846      2001:558:feed::1      2601:193:8302:4620:: DNS      107 Standard query response 0x4667 A youtube.w
24 3.953852      2001:558:feed::1      2601:193:8302:4620:: DNS      241 Standard query response 0x04fe AAAA www.y
25 3.954763      2601:193:8302:4620:215c:f5ae:8b40:a27a 2001:558:feed::1      DNS      103 Standard query 0x7884 A youtube-u1.l.goo
26 3.955402      2001:558:feed::1      2601:193:8302:4620:: DNS      337 Standard query response 0x7884 A www.yout
27 3.955405      2001:558:feed::1      2601:193:8302:4620:: DNS      119 Standard query response 0x920d AAAA youtu

Frame 24: 241 bytes on wire (1928 bits), 241 bytes captured (1928 bits) on
Ethernet II, Src: VantivaUSA 81:74:5a (44:1c:12:81:74:5a), Dst: Apple 98:
Internet Protocol Version 6, Src: 2001:558:feed::1, Dst: 2601:193:8302:46
User Datagram Protocol, Src Port: 53, Dst Port: 57174
Domain Name System (response)
Transaction ID: 0x04fe
  Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 5
    Authority RRs: 0
    Additional RRs: 0
  Queries
  Answers
    [Request In: 22]
    [Time: 0.133947000 seconds]

```

```

Boot file name not given
Magic cookie: DHCP
▼ Option: (53) DHCP Message Type (Request)
  Length: 1
  DHCP: Request (3)
▼ Option: (61) Client identifier
  Length: 7
  Hardware type: Ethernet (0x01)
  Client MAC address: Intel_cc:5c:45 (48:51:c5:cc:5c:45)
▼ Option: (12) Host Name
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0110 00 00 00 00 00 00 00 63 82 53 63 35 01 03 3d 07 01 .....c- Sc5.1=..
0120 48 51 c5 cc 5c 45 0c 06 6a 69 6a 5f 70 63 51 09 HQ..\E.. jij_pcQ.
0130 00 00 00 6a 69 6a 5f 70 63 3c 08 4d 53 46 54 20 ...jij_p c<-MSFT
0140 35 2e 30 37 0e 01 03 06 0f 1f 21 2b 2c 2e 2f 77 5.07.... ..!+_./w
0150 79 f9 fc ff 00 00 y.....

```

Qual é o endereço IP de destino usado no datagrama contendo a mensagem Discover? Há algo especial sobre este endereço? Explique.

192.168.100.1 esse endereço está assim pois já foi salvo o ip do servidor dhcp, mas caso não estivesse haveria uma broadcast com endereço ip de 255.255.255.255.

Qual é o valor no campo de ID de transação desta mensagem DHCP Discover?

```

▼ [Timestamps]
  [Time since first frame: 0.000000000 seconds]
  [Time since previous frame: 0.000000000 seconds]
  UDP payload (300 bytes)
▼ Dynamic Host Configuration Protocol (Request)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x637f072e
  Seconds elapsed: 0
▼ Bootp flags: 0x0000 (Unicast)

```

Agora inspecione o campo de opções na mensagem DHCP Discover. Quais são cinco peças de informação (além de um endereço IP) que o cliente está sugerindo ou solicitando receber do servidor DHCP como parte desta transação DHCP?

```

.000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 192.168.100.50
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: Intel_cc:5c:45 (48:51:c5:cc:5c:45)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP

```

Como você sabe que esta mensagem Offer está sendo enviada em resposta à mensagem DHCP Discover que você estudou nas perguntas 1-5 acima? pelo id de transação

No.	Time	Source	Destination	Protocol	Length	Info
287	15.887148	192.168.100.1	192.168.100.50	DHCP	598	DHCP ACK - Transaction ID 0x637f072e
286	15.859543	192.168.100.50	192.168.100.1	DHCP	342	DHCP Request - Transaction ID 0x637f072e

Qual é o endereço IP de origem usado no datagrama IP contendo a mensagem Offer? Há algo especial sobre este endereço? Explique.
endereço real do servidor e nao do broadcast

No.	Time	Source	Destination	Protocol	Length	Info
287	15.087148	192.168.100.1	192.168.100.50	DHCP	590	DHCP ACK - Transaction ID 0x637f072e

Qual é o endereço IP de destino usado no datagrama contendo a mensagem Offer? Há algo especial sobre este endereço? Explique.

No.	Time	Source	Destination	Protocol	Length	Info
287	15.087148	192.168.100.1	192.168.100.50	DHCP	590	DHCP ACK - Transaction ID 0x637f072e

foi dado o endereço ip sendo o mesmo que ele tinha

Agora inspecione o campo de opções na mensagem DHCP Offer. Quais são cinco peças de informação que o servidor DHCP está fornecendo ao cliente DHCP na mensagem DHCP Offer?

.000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 192.168.100.50
Your (client) IP address: 192.168.100.50
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: Intel_cc:5c:45 (48:51:c5:cc:5c:45)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (ACK)
Length: 1

00 48 51 c5 cc 5c 45 c4 d4 38 5c 5a a0 08 00 45 00 HQ \E 8 Z \E
10 02 40 00 00 00 00 00 40 11 2f 29 c0 a8 64 01 c0 a8 @ @ /) d
20 64 32 00 43 00 44 02 2c 03 ab 02 01 06 00 63 7f d2 C D , c
30 07 2e 00 00 00 00 c0 a8 64 32 c0 a8 64 32 00 00 d2 d2
40 00 00 00 00 00 00 48 51 c5 cc 5c 45 00 00 00 00 HQ \E
50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 63 82 53 63 35 01 05 36 04 c0 c Sc5 6

87 - Time: 15.087148 - Source: 192.168.100.1 - Destination: 192.168.100.50 - Protocol: DHCP - Length: 590 - Info: DHCP ACK - Transaction ID 0x637f072e

show packet bytes

Qual é o número da porta de origem UDP no datagrama IP contendo a primeira mensagem DHCP Request no seu rastreamento? Qual é o número da porta de destino UDP sendo usado?
porta de origem 68 e destino e 67 por padrão

Wireshark - Packet 286 - Wi-Fi

▶ Frame 286: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{AF5D1A48-1C5C-46C3-957E-8E7D2D521120}, id 0
▶ Ethernet II, Src: Intel_cc:5c:45 (48:51:c5:cc:5c:45), Dst: HuaweiTechno_5c:5a:a0 (c4:d4:38:5c:5a:a0)
▶ Internet Protocol Version 4, Src: 192.168.100.50, Dst: 192.168.100.1
▶ User Datagram Protocol, Src Port: 68, Dst Port: 67
▶ Dynamic Host Configuration Protocol (Request)

```

0000 0000 0000 0000 = Broadcast flag: Unicast
0000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 192.168.100.50
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0

```

deveria aparecer o endereço e broadcast mas ja estava em memoria no meu roteador o ip do servidor dhcp, portanto e o ip dele

No.	Time	Source	Destination	Protocol	Length	Info
287	15.087148	192.168.100.1	192.168.100.50	DHCP	590	DHCP ACK - Transaction ID 0x637f072e
286	15.059543	192.168.100.50	192.168.100.1	DHCP	342	DHCP Request - Transaction ID 0x637f072e

```

Option: (255) Parameter Request List
Length: 14
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (3) Router
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (31) Perform Router Discover
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (43) Vendor-Specific Information
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
Parameter Request List Item: (119) Domain Search
Parameter Request List Item: (121) Classless Static Route
Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
Parameter Request List Item: (252) Private/Proxy autodiscovery
Option: (255) End

```

[illegible]

Qual é o endereço IP de origem no datagrama IP contendo esta mensagem ACK? Há algo especial sobre este endereço? Explique

como observamos no print do ack temos que e o de ip do servidor de origem

No.	Time	Source	Destination	Protocol	Length	Info
287	15.087148	192.168.100.1	192.168.100.50	DHCP	590	DHCP ACK - Transaction ID 0x637f072e
286	15.059543	192.168.100.50	192.168.100.1	DHCP	342	DHCP Request - Transaction ID 0x637f072e

Qual é o endereço IP de destino usado no datagrama contendo esta mensagem ACK? Há algo especial sobre este endereço? Explique.

temos o ip do host no caso foi enviado o nosso ip que não alterado caso o dhcp estivesse fornecido outro ip teriamos que dar um broadcast para descobrir qual é o host

Qual é o nome do campo na mensagem DHCP ACK (como indicado na janela do Wireshark) que contém o endereço IP atribuído ao cliente?

```

Seconds elapsed: 0
▼ Bootp flags: 0x0000 (Unicast)
  0... .. = Broadcast flag: Unicast
  .000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 192.168.100.50
Your (client) IP address: 192.168.100.50
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: Intel cc:5c:45 (48:51:c5:cc:5c:45)

```

Por quanto tempo (o chamado “lease time”) o servidor DHCP atribuiu este endereço IP ao cliente?

```

▼ Option: (51) IP Address Lease Time
  Length: 4
  IP Address Lease Time: 1 day (86400)

```

Qual é o endereço IP (retornado pelo servidor DHCP ao cliente DHCP nesta mensagem DHCP ACK) do roteador de primeiro salto no caminho padrão do cliente para o resto da Internet?

```

Seconds elapsed: 0
▼ Bootp flags: 0x0000 (Unicast)
  0... .. = Broadcast flag: Unicast
  .000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 192.168.100.50
Your (client) IP address: 192.168.100.50
Next server IP address: 0.0.0.0

```

Laboratorio_Wireshark_NAT_v8.1

Qual é o endereço IP do cliente que envia a solicitação HTTP GET no rastreamento nat-inside-wireshark-trace1-1.pcapng? Qual é o número da porta de origem do segmento TCP neste datagrama que contém a solicitação HTTP GET? Qual é o endereço IP de destino desta solicitação HTTP GET? Qual é o número da porta de destino do segmento TCP neste datagrama que contém a solicitação HTTP GET?

```

► Internet Protocol Version 4, Src: 192.168.10.11, Dst: 138.76.29.8
▼ Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 1, Ack: 1, Len: 330
  Source Port: 53924
  Destination Port: 80
  [Stream index: 0]

```


Em que momento a mensagem HTTP 200 OK correspondente do servidor web é encaminhada pelo roteador NAT para o cliente no lado LAN do roteador?
apos a requisição

```
Frame 6: 613 bytes on wire (4904 bits), 613 bytes captured (4904 bits) on interface eth1, id 0
Ethernet II, Src: PCSSystemtec_82:36:d7 (08:00:27:82:36:d7), Dst: PCSSystemtec_89:c7:7c (08:00:27:89:c7:7c)
Internet Protocol Version 4, Src: 138.76.29.8, Dst: 192.168.10.11
Transmission Control Protocol, Src Port: 80, Dst Port: 53924, Seq: 1, Ack: 331, Len: 547
  Source Port: 80
  Destination Port: 53924
  [Stream index: 0]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 547]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 2574368914
  [Next Sequence Number: 548 (relative sequence number)]
  Acknowledgment Number: 331 (relative ack number)
  Acknowledgment number (raw): 2729790325
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x018 (PSH, ACK)
  Window: 507
  [Calculated window size: 64896]
  [Window size scaling factor: 128]
```

Quais são os endereços IP de origem e destino e as portas de origem e destino TCP no datagrama IP que transporta esta mensagem HTTP 200 OK?

src	dst	
6 0.030672101	138.76.29.8	192.168.10.11 HTTP 613 HTTP/1.1 200 OK (text/html)

A que horas esta mensagem HTTP GET aparece no arquivo de rastreamento nat-outside-wireshark-trace1-1.pcapng?

http

No.	Time	Source	Destination	Protocol	Length	Info
4	0.027356291	10.0.1.254	138.76.29.8	HTTP	396	GET / HTTP/1.1
6	0.030625966	138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (text/html)
8	0.231400190	10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
10	0.233043313	138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Found (text/html)

Frame 6: 613 bytes on wire (4904 bits), 613 bytes captured (4904 bits) on interface eth0, id 0

Section number: 1

Interface id: 0 (eth0)

Encapsulation type: Ethernet (1)

Arrival Time: Mar 29, 2021 00:50:27.774660820 Hora oficial do Brasil

UTC Arrival Time: Mar 29, 2021 03:50:27.774660820 UTC

Epoch Arrival Time: 1616989827.774660820

[Time shift for this packet: 0.000000000 seconds]

[Time delta from previous captured frame: 0.001287055 seconds]

[Time delta from previous displayed frame: 0.003269675 seconds]

[Time since reference or first frame: 0.030625966 seconds]

Frame Number: 6

Frame Length: 613 bytes (4904 bits)

Capture Length: 613 bytes (4904 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]

[Coloring Rule Name: HTTP]

[Coloring Rule String: http || tcp.port == 80 || http2]

Ethernet II, Src: PCSSystemtec_22:fd:74 (08:00:27:22:fd:74), Dst: PCSSystemtec_43:65:cd (08:00:27:43:65:cd)

Internet Protocol Version 4, Src: 138.76.29.8, Dst: 10.0.1.254

0100 = Version: 4

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

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

Total Length: 599

Quais são os endereços IP de origem e destino e os números de porta de origem e destino TCP no datagrama IP que transporta este HTTP GET (conforme registrado no arquivo de rastreamento nat-outside-wireshark-trace1-1.pcapng)?

```
Internet Protocol Version 4, Src: 10.0.1.254, Dst: 138.76.29.8
Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 331, Ack: 548, Len: 251
```

Quais destes quatro campos são diferentes da sua resposta à pergunta 1 acima?
os ips

Quais dos seguintes campos no datagrama IP que transporta o HTTP GET são alterados do datagrama recebido na rede local (interna) para o datagrama correspondente encaminhado no lado da Internet (externo) do roteador NAT: Versão, Comprimento do Cabeçalho, Flags, Soma de Verificação?

campos nos prints

version outside

```
Frame 8: 317 bytes on wire (2536 bits), 317 bytes captured (2536 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_43:65:cd (08:00:27:43:65:cd), Dst: PCSSystemtec_22:fd:74 (08:00:27:22:fd:74)
Internet Protocol Version 4, Src: 10.0.1.254, Dst: 138.76.29.8
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 303
  Identification: 0x6298 (25240)
  010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 63
  Protocol: TCP (6)
  Header Checksum: 0x24df [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.0.1.254
  Destination Address: 138.76.29.8
Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 331, Ack: 548, Len: 251
  Source Port: 53924
  Destination Port: 80
```

e version inside

```
Ethernet II, Src: PCSSystemtec_89:c7:7c (08:00:27:89:c7:7c), Dst: PCSSystemtec_62:9b:d7 (08:00:27:62:9b:d7)
Internet Protocol Version 4, Src: 192.168.10.11, Dst: 138.76.29.8
Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 1, Ack: 1, Len: 330
  Source Port: 53924
  Destination Port: 80
  [Stream index: 0]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 330]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 2729789995
  [Next Sequence Number: 331 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 2574368014
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x018 (PSH, ACK)
  Window: 502
  [Calculated window size: 64256]
  [Window size scaling factor: 128]
  Checksum: 0x1bee [unverified]
```

A que horas esta mensagem aparece no arquivo de rastreamento nat-outside-wireshark-trace1-1.pcapng?

```
Section number: 1
Interface id: 0 (eth0)
  Interface name: eth0
  Encapsulation type: Ethernet (1)
  Arrival Time: Mar 29, 2021 00:50:27.975435044 Hora oficial do Brasil
  UTC Arrival Time: Mar 29, 2021 03:50:27.975435044 UTC
  Epoch Arrival Time: 1616989827.975435044
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.199951520 seconds]
  [Time delta from previous displayed frame: 0.200774224 seconds]
  [Time since reference or first frame: 0.231400190 seconds]
  Frame Number: 8
  Frame Length: 317 bytes (2536 bits)
  Capture Length: 317 bytes (2536 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
```

Quais são os endereços IP de origem e destino e os números de porta de origem e destino TCP no datagrama IP que transporta esta mensagem de resposta HTTP ("200 OK") (conforme registrado no arquivo de rastreamento nat-outside-wireshark-trace1-1.pcapng)?

```
Internet Protocol Version 4, Src: 10.0.1.254, Dst: 138.76.29.8
Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 331, Ack: 548, Len: 251
```