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.

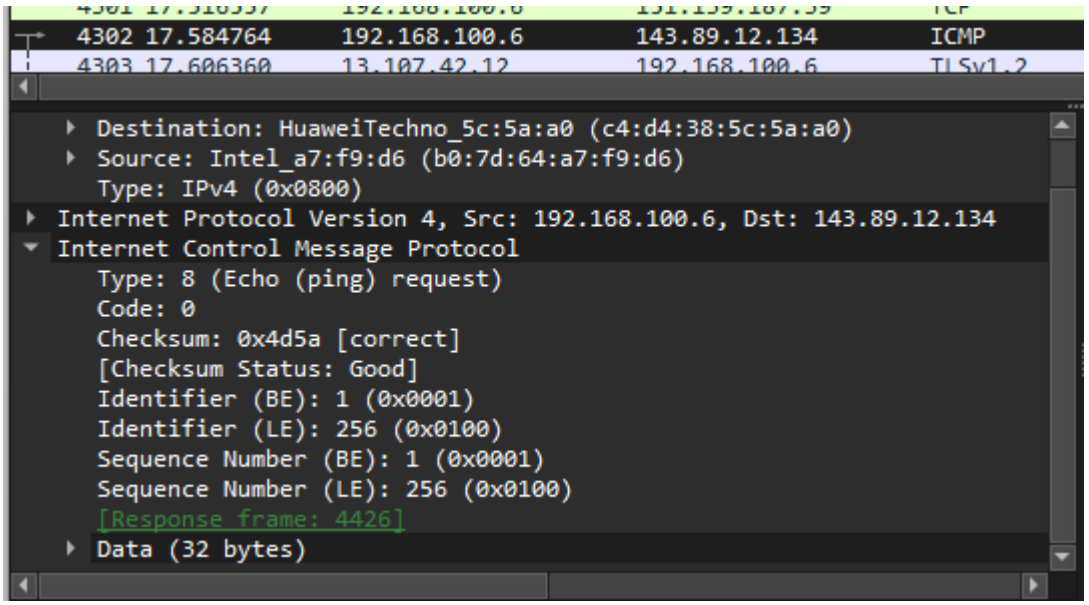
Time	Source	Destination	Protocol
17.516426	151.139.187.39	192.168.100.6	TCP
17.516426	151.139.187.39	192.168.100.6	TCP
17.516557	192.168.100.6	151.139.187.39	TCP
17.584764	192.168.100.6	143.89.12.134	ICMP

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.

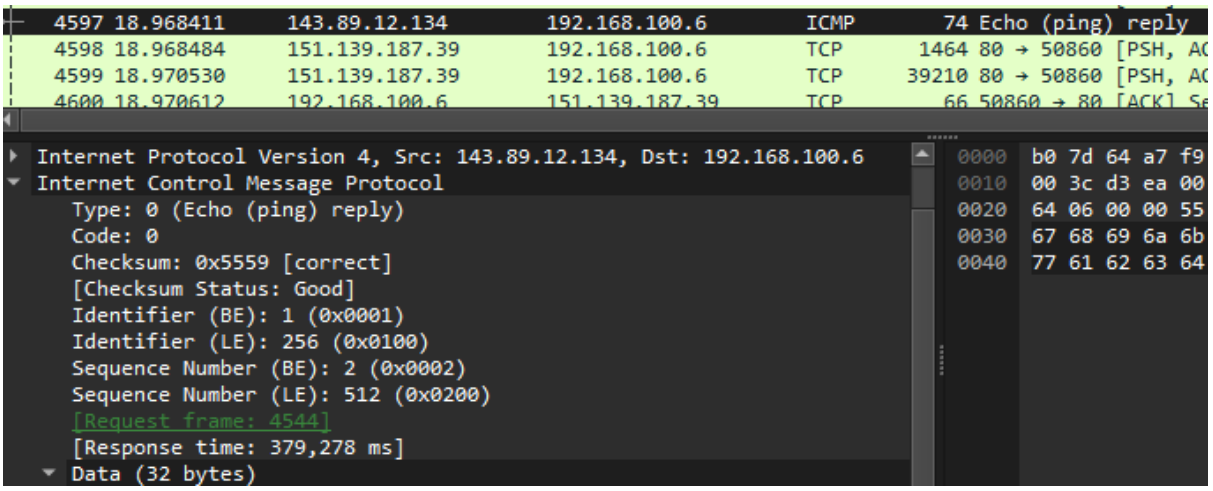
3. Examine um dos pacotes de solicitação de ping enviados pelo seu host. Quais são os números de tipo e código ICMP? Quais outros campos esse pacote ICMP possui? Quantos bytes têm os campos de checksum, número de sequência e identificador?

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.



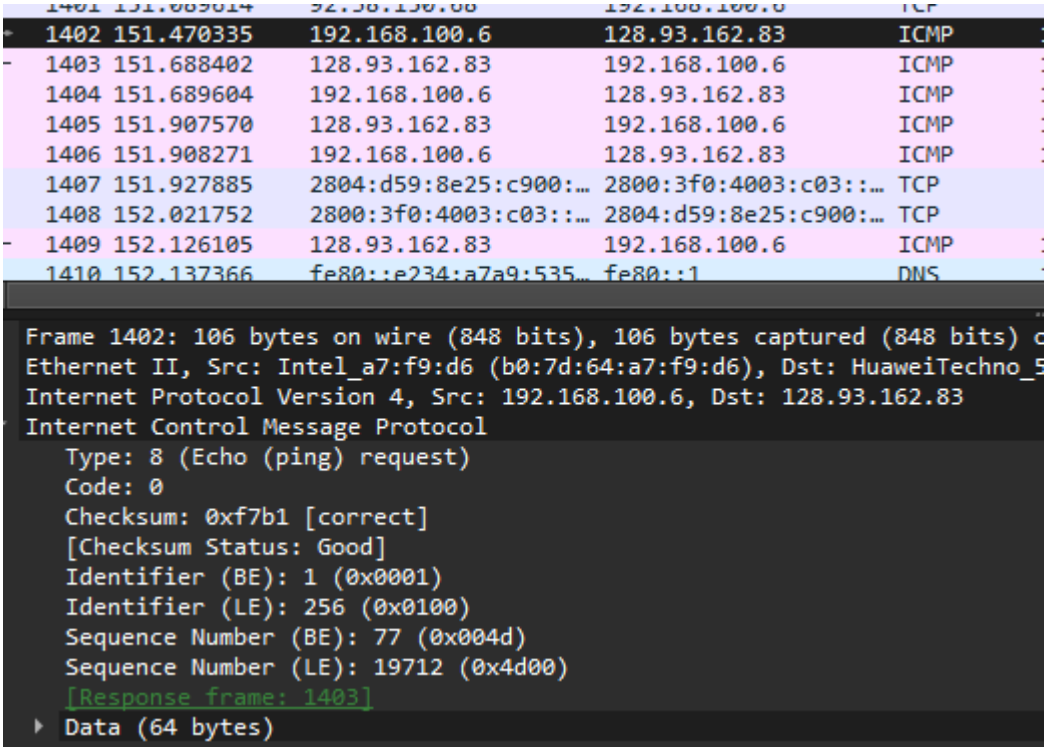
4. Examine o pacote de resposta de ping correspondente. Quais são os números de tipo e código ICMP? Quais outros campos esse pacote ICMP possui? Quantos bytes têm os campos de checksum, número de sequência e identificador?

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.



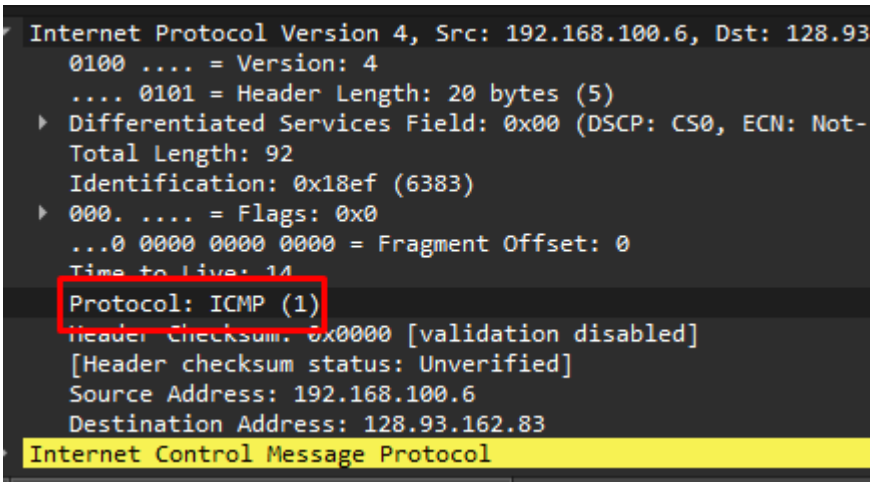
ICMP e Traceroute

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.



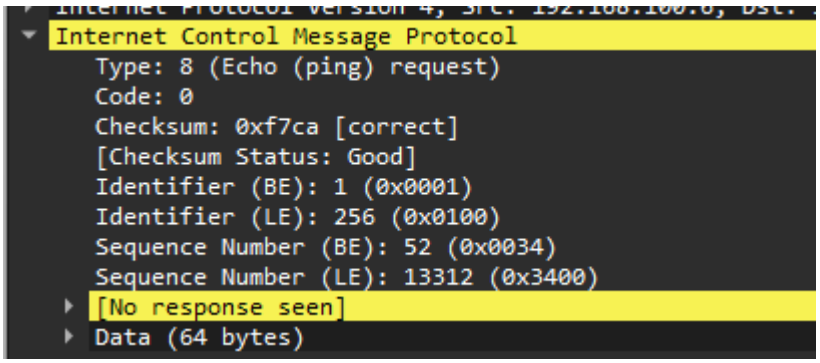
2. Se o ICMP enviasse pacotes UDP em vez disso (como no Unix/Linux), o número do protocolo IP ainda seria 01 para os pacotes de sonda? Se não, qual seria?

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



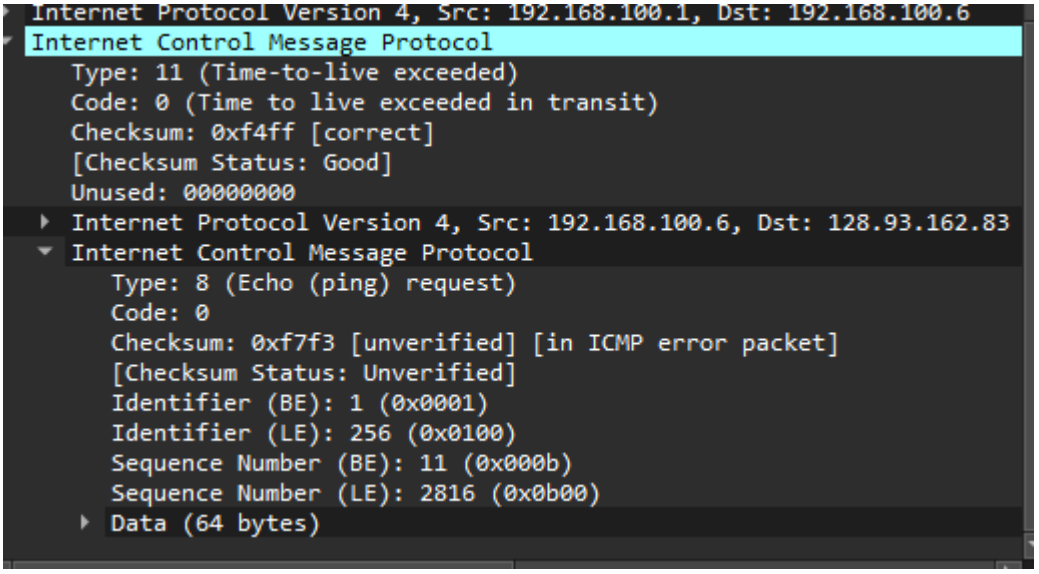
3. Examine o pacote ICMP echo na sua captura de tela. Este é diferente dos pacotes de consulta ping ICMP na primeira metade deste laboratório? Se sim, como?

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 uma quantidade maior de pacotes



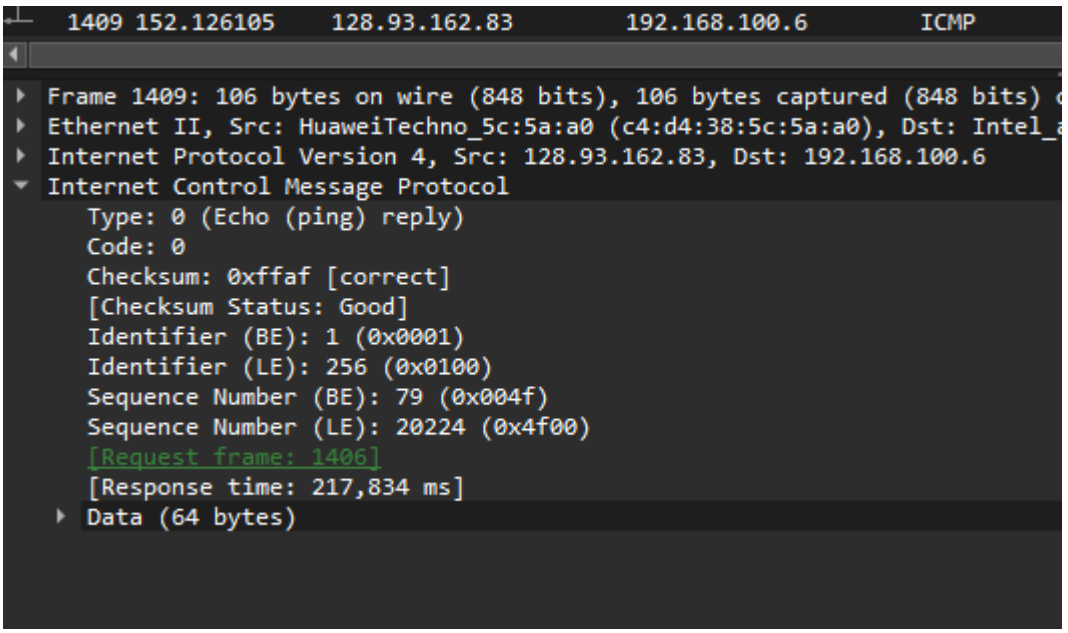
4. Examine o pacote de erro ICMP na sua captura de tela. Ele tem mais campos do que o pacote ICMP echo. O que está incluído nesses campos?

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



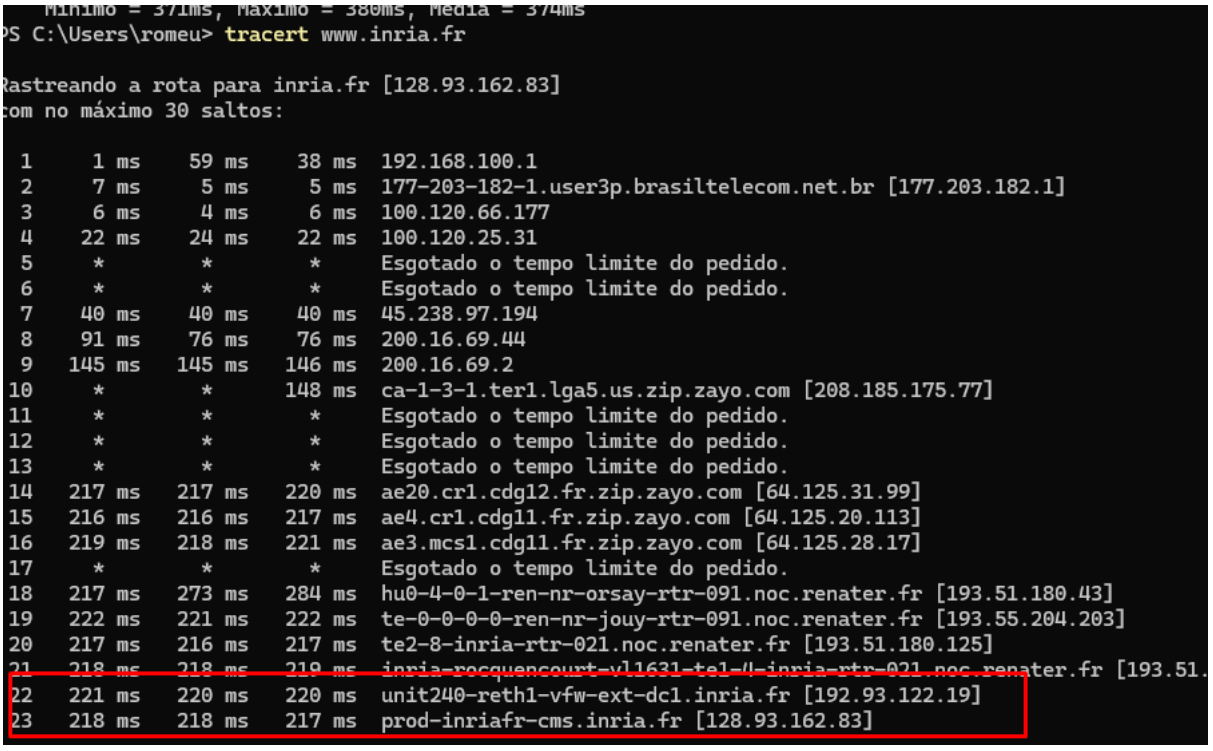
5. Examine os três últimos pacotes ICMP recebidos pelo host de origem. Como esses pacotes são diferentes dos pacotes de erro ICMP? Por que eles são diferentes?

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?

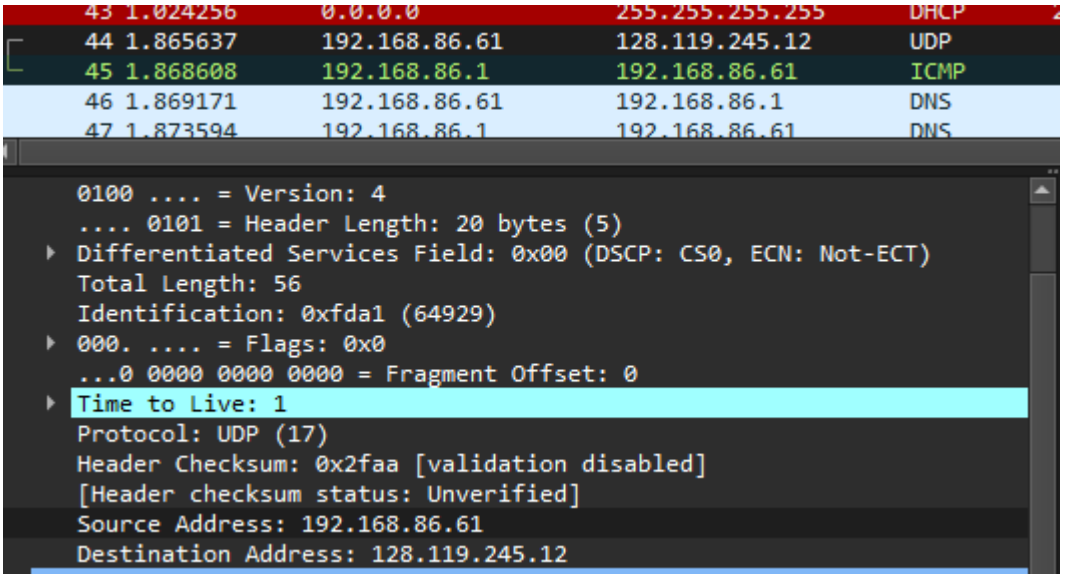
As últimas requisições foram as mais demoradas, e, pelo nome do domínio (.fr), é possível que esses roteadores se situem na França.



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.

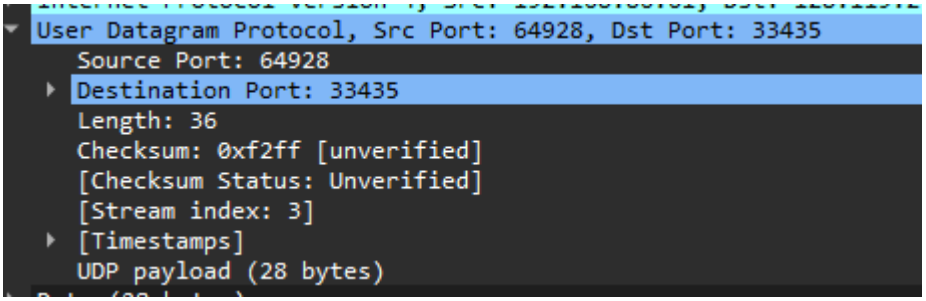


2. Qual é o valor no campo de tempo de vida (TTL) no cabeçalho deste datagrama IPv4?
Como é possível verificar no print acima, o TTL é igual a 1.

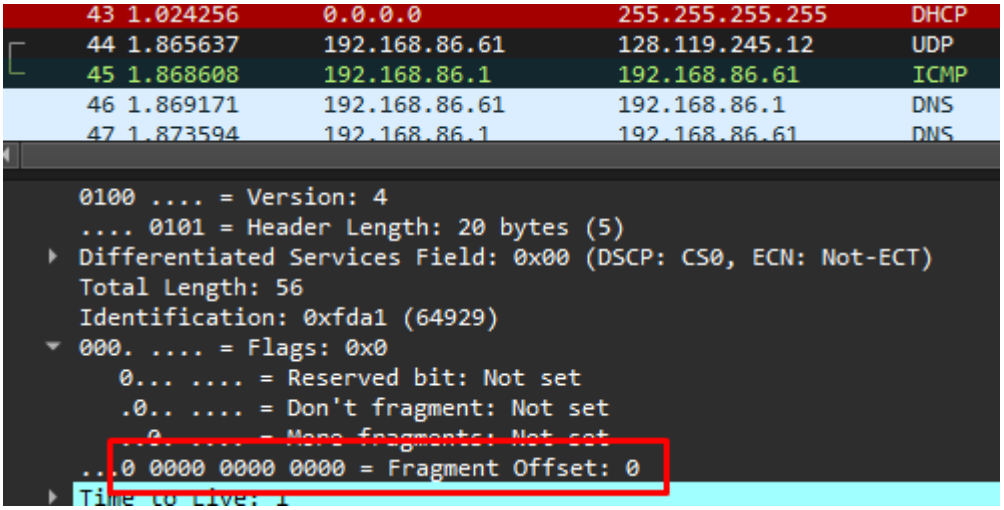
3. Qual é o valor no campo de protocolo de camada superior neste datagrama IPv4? [Nota: as respostas para Linux/MacOS diferem das de Windows aqui.]
O valor é UDP (17).

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.



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?

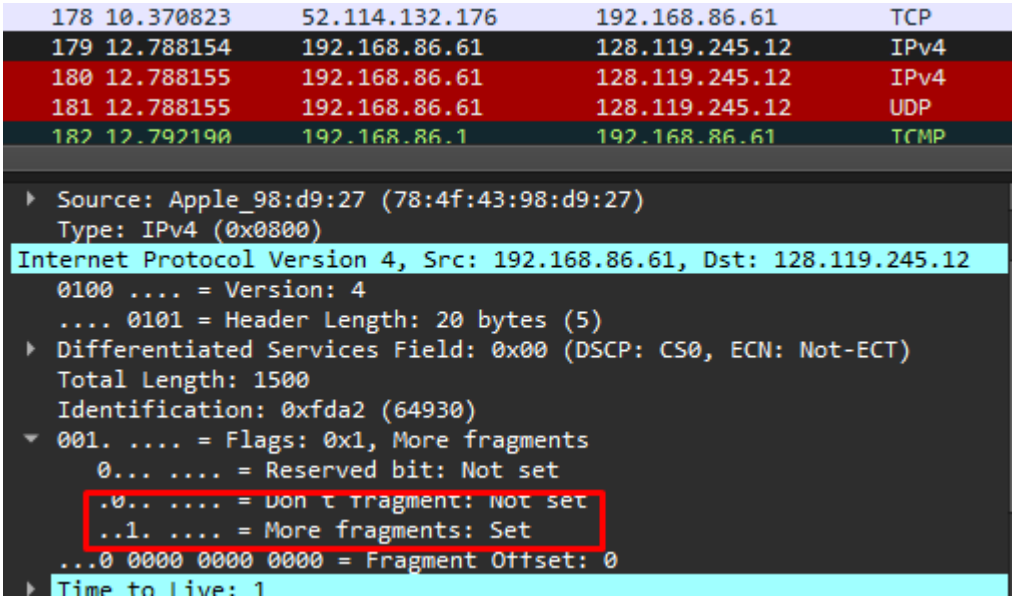
Não. Os campos de identificação são sempre iguais a zero, em todos os pacotes deste caso.

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

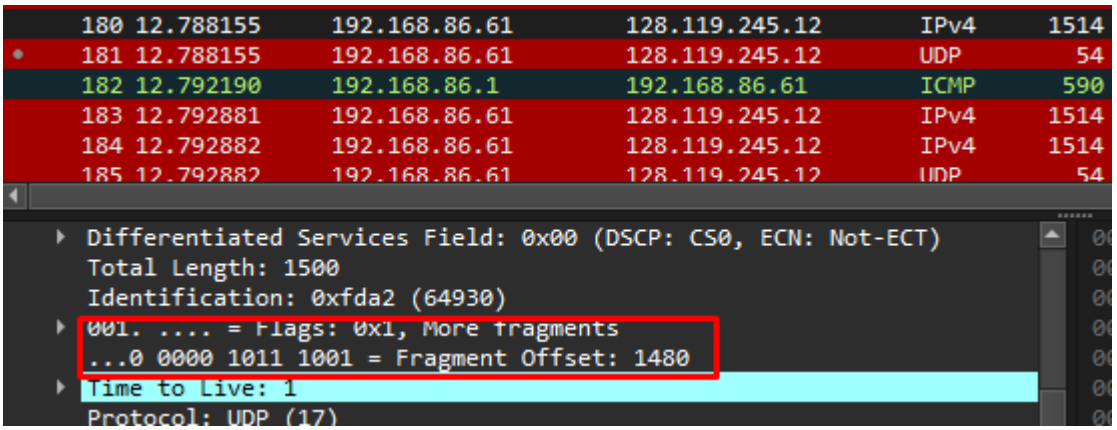
1. Encontre o primeiro datagrama IP que contém a primeira parte do segmento enviado pelo seu computador para 128.119.245.12, via comando traceroute para gaia.cs.umass.edu, depois que você especificou que o comprimento do pacote traceroute deveria ser 3000 bytes. Esse segmento foi fragmentado através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



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.

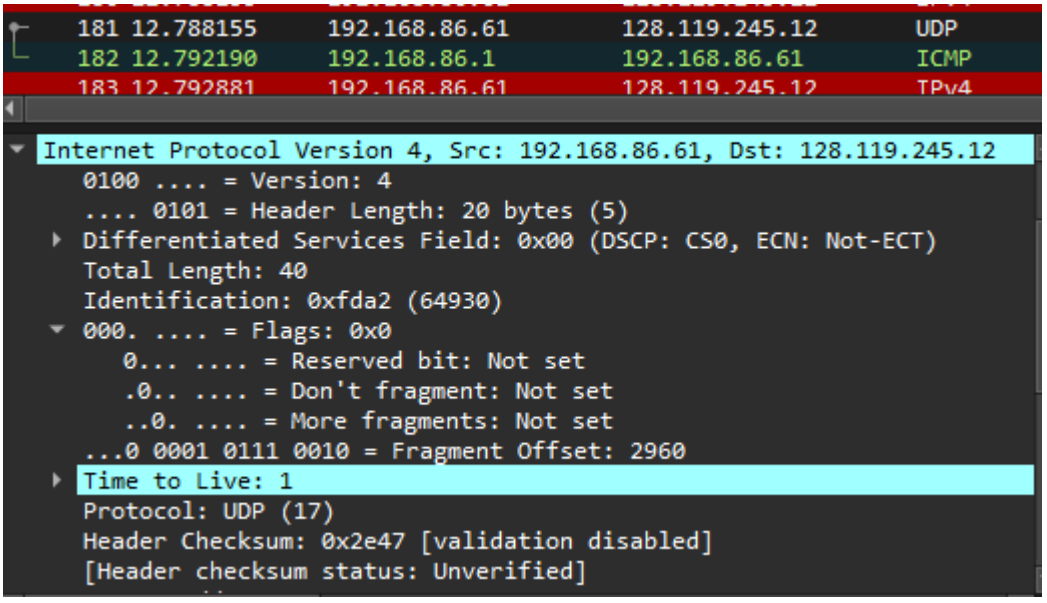


6. Quais campos mudam no cabeçalho IP entre o primeiro e o segundo fragmento?

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.



IPv6

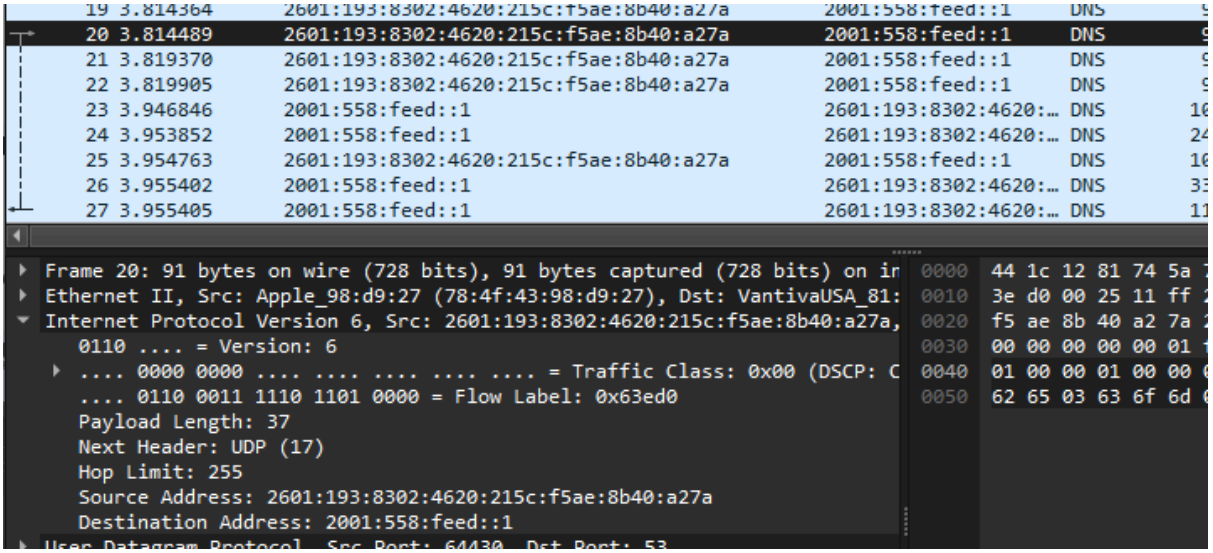
1. Qual é o endereço IPv6 do computador que está fazendo a solicitação DNS AAAA? Este é o endereço de origem do 20º pacote no rastreamento. Forneça o endereço IPv6 de origem para este datagrama na mesma forma exata exibida na janela do Wireshark.
2601:193:8302:4620:215c:f5ae:8b40:a27a

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

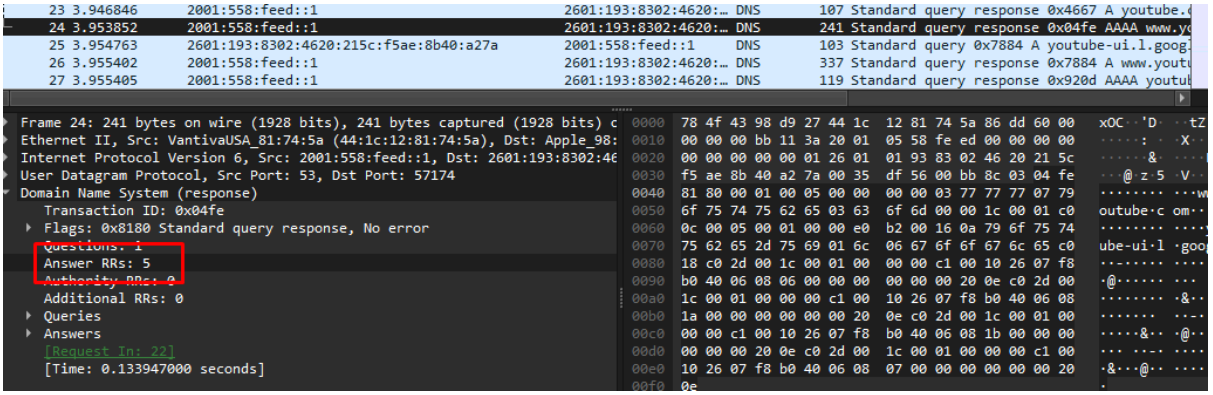
3. Qual é o valor do rótulo de fluxo (flow label) para este datagrama?
0x63ed0

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)



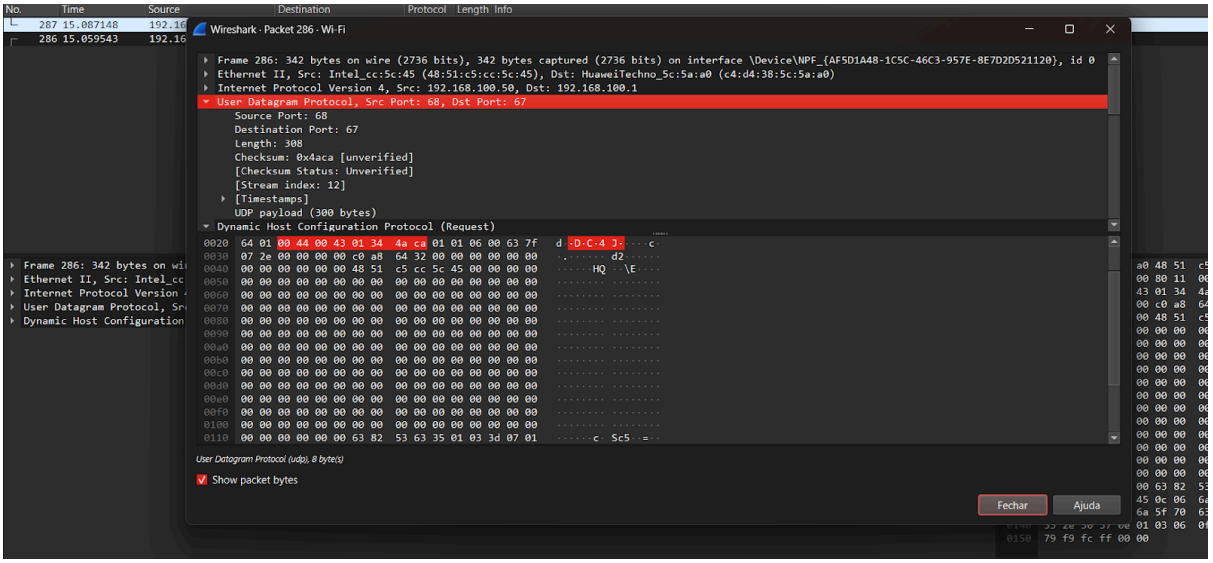
6. Quantos endereços IPv6 são retornados na resposta a esta solicitação AAAA?
São retornadas 5 respostas.



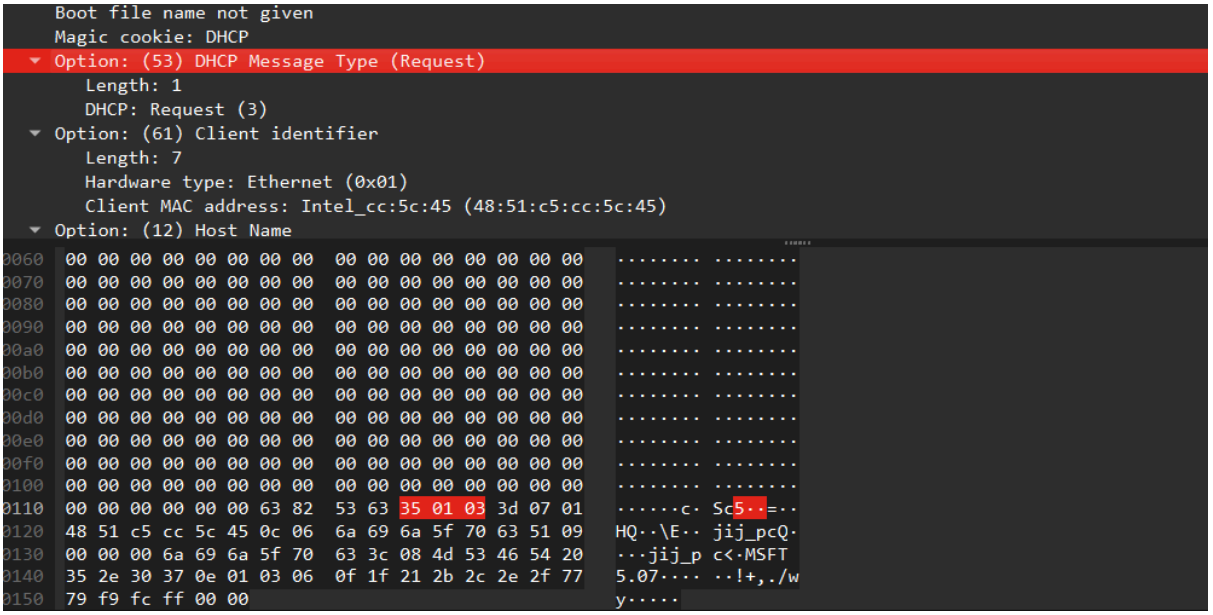
7. Qual é o primeiro dos endereços IPv6 retornados pelo DNS para youtube.com (no arquivo de rastreamento ip-wireshark-trace2-1.pcapng, este também é o endereço que é numericamente o menor)? Forneça este endereço IPv6 na mesma forma abreviada exata exibida na janela do Wireshark.
O primeiro endereço é youtube.com (172.217.10.142)

Laboratorio_Wireshark_DHCP_v8.1

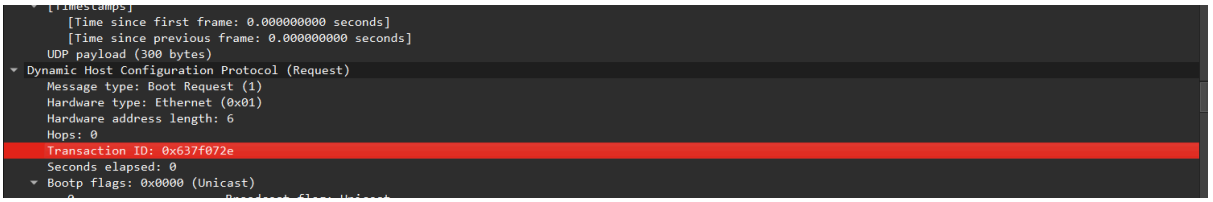
Esta mensagem DHCP Discover é enviada usando UDP ou TCP como protocolo de transporte subjacente?
UDP



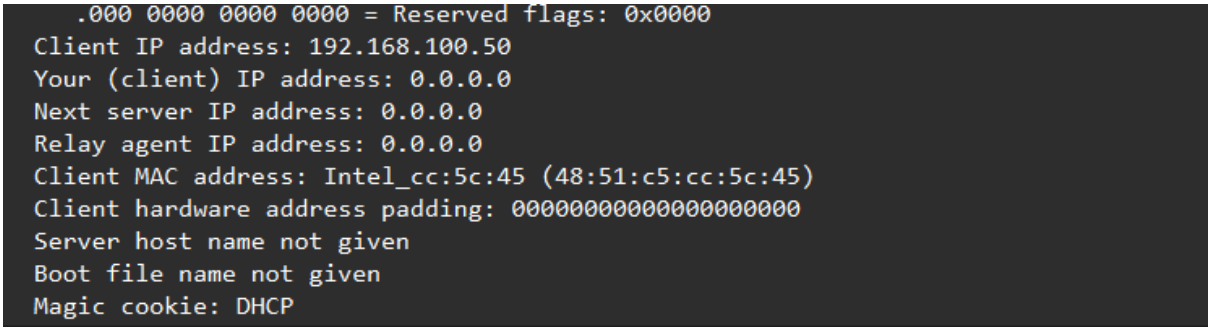
Qual é o endereço IP de origem usado no datagrama IP contendo a mensagem Discover? Há algo especial sobre este endereço? Explique.
o ip de origem é 192.168.100.50, esta sendo feito a requisição para um ip novo ao dhcp



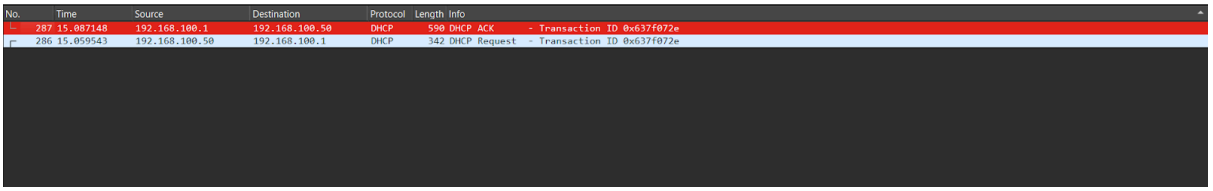
Qual é o endereço IP de destino usado no datagrama contendo a mensagem Discover? Há algo especial sobre este endereço? Explique.
192.168.100.1 esse endereço está assim pois já foi salvo o ip do servidor dhcp, mas caso nao estive salve haveria uma broadcast com endereço ip de 255.255.255.255.
Qual é o valor no campo de ID de transação desta mensagem DHCP Discover?



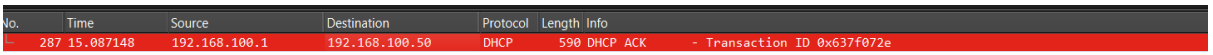
Agora inspecione o campo de opções na mensagem DHCP Discover. Quais são cinco peças de informação (além de um endereço IP) que o cliente está sugerindo ou solicitando receber do servidor DHCP como parte desta transação DHCP?



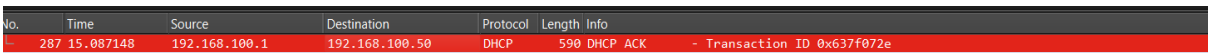
Como você sabe que esta mensagem Offer está sendo enviada em resposta à mensagem DHCP Discover que você estudou nas perguntas 1-5 acima?
pelo id de transação



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

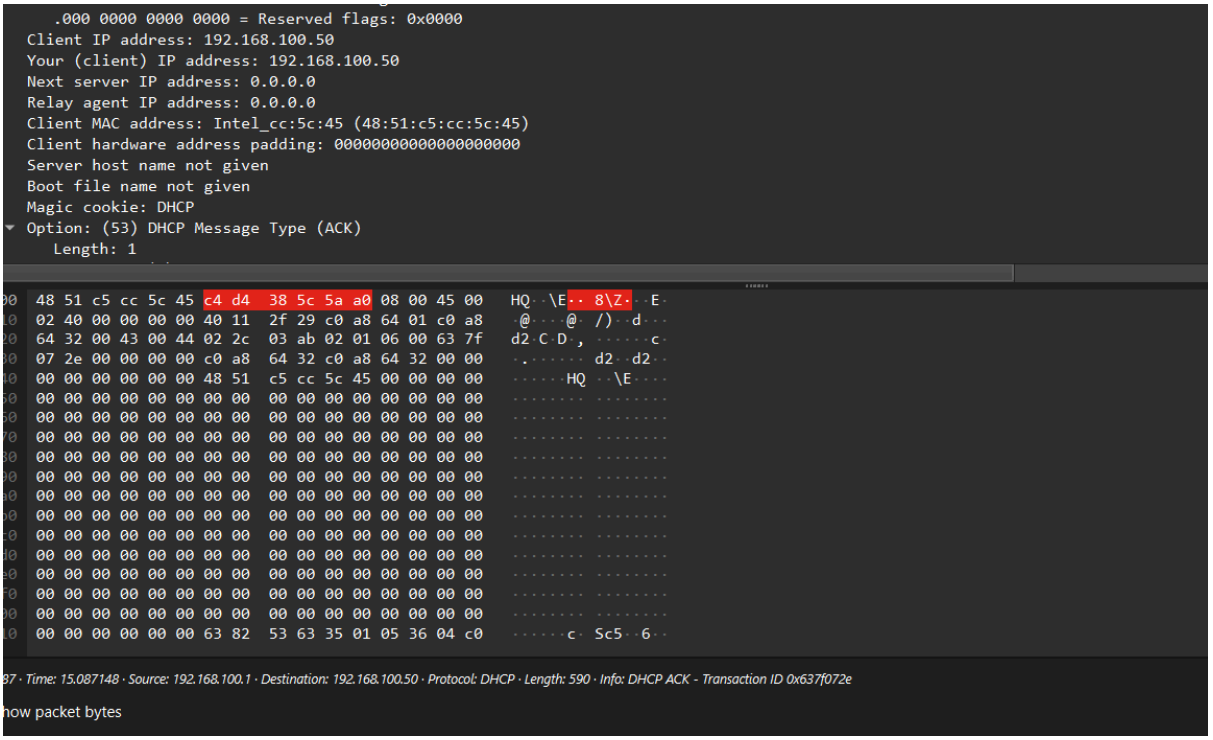


Qual é o endereço IP de destino usado no datagrama contendo a mensagem Offer? Há algo especial sobre este endereço? Explique.

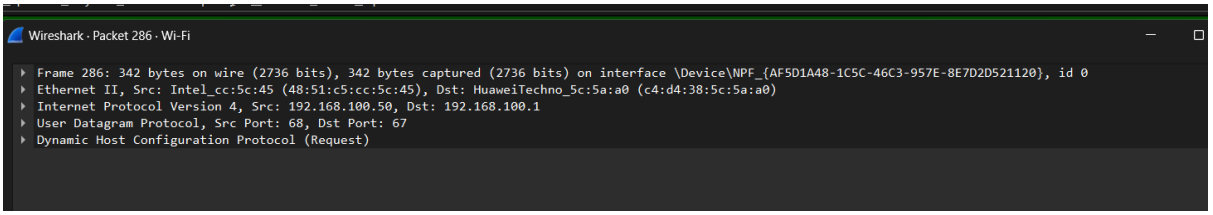


foi dado o endereço ip sendo o mesmo que ele tinha

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?



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

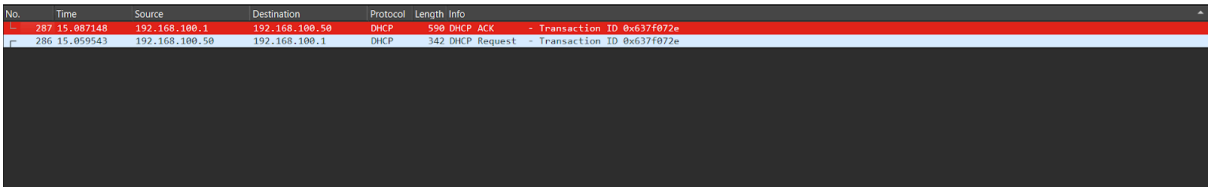


Qual é o endereço IP de origem no datagrama IP contendo esta mensagem Request? Há algo especial sobre este endereço? Explique.

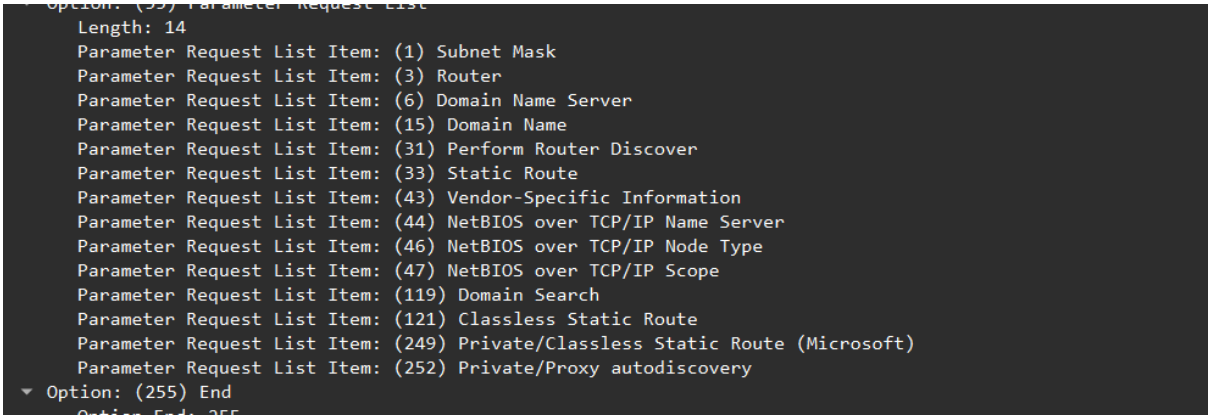
indicando que foi solicitado um novo endereço ip

Qual é o endereço IP de destino usado no datagrama contendo esta mensagem Request? Há algo especial sobre este endereço? Explique.
deveria aparecer o endereço e broadcast mas ja estava em memoria no meu roteador o ip do servidor dhcp, portanto e o ip dele

Qual é o valor no campo de ID de transação desta mensagem DHCP Request? Ele corresponde aos IDs de transação das mensagens Discover e Offer anteriores?
é o mesmo

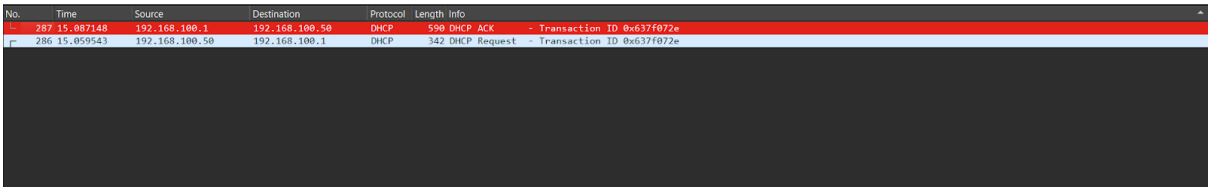


Agora inspecione o campo de opções na mensagem DHCP Discover e observe de perto a "Lista de Solicitação de Parâmetros". O RFC do DHCP observa que "o cliente pode informar ao servidor quais parâmetros de configuração o cliente está interessado em incluir na opção 'lista de solicitação de parâmetros'. A parte de dados dessa opção lista explicitamente as opções solicitadas por número de tag." Quais diferenças você vê entre as entradas na opção 'lista de solicitação de parâmetros' nesta mensagem Request e na mesma opção na mensagem Discover anterior?
request



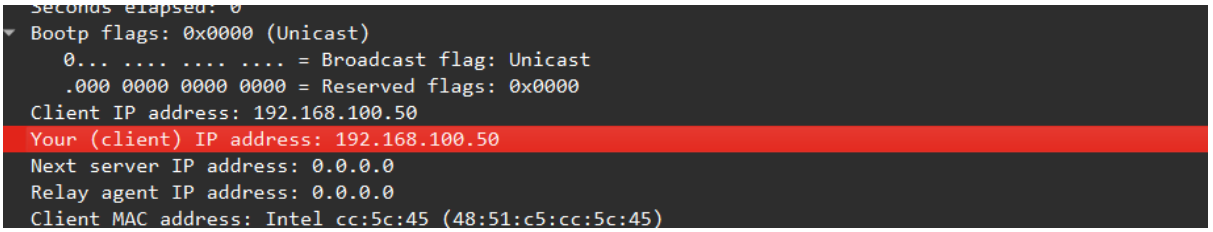
ack response

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

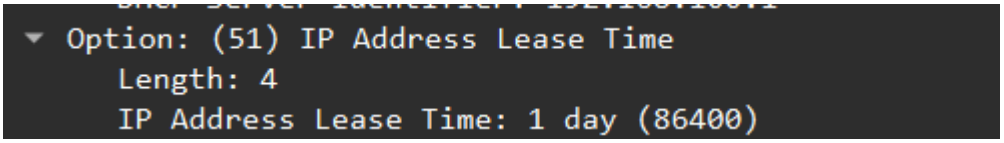


Qual é o endereço IP de destino usado no datagrama contendo esta mensagem ACK? Há algo especial sobre este endereço? Explique.
temos o ip do host no caso foi enviado o nosso ip que não alterado caso o dhcp estivesse fornecido outro ip teriamos que dar um broadcast para descobrir qual é o host

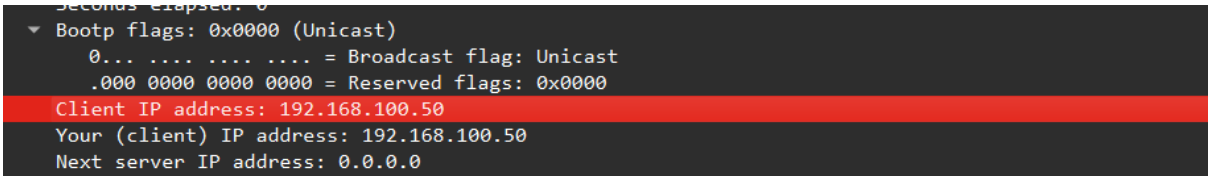
Qual é o nome do campo na mensagem DHCP ACK (como indicado na janela do Wireshark) que contém o endereço IP atribuído ao cliente?



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

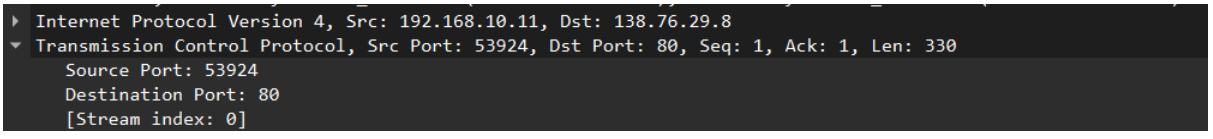


Qual é o endereço IP (retornado pelo servidor DHCP ao cliente DHCP nesta mensagem DHCP ACK) do roteador de primeiro salto no caminho padrão do cliente para o resto da Internet?

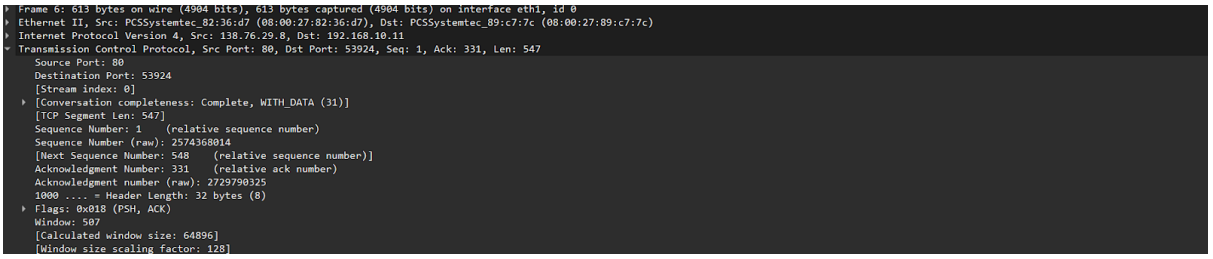


Laboratorio_Wireshark_NAT_v8.1

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?



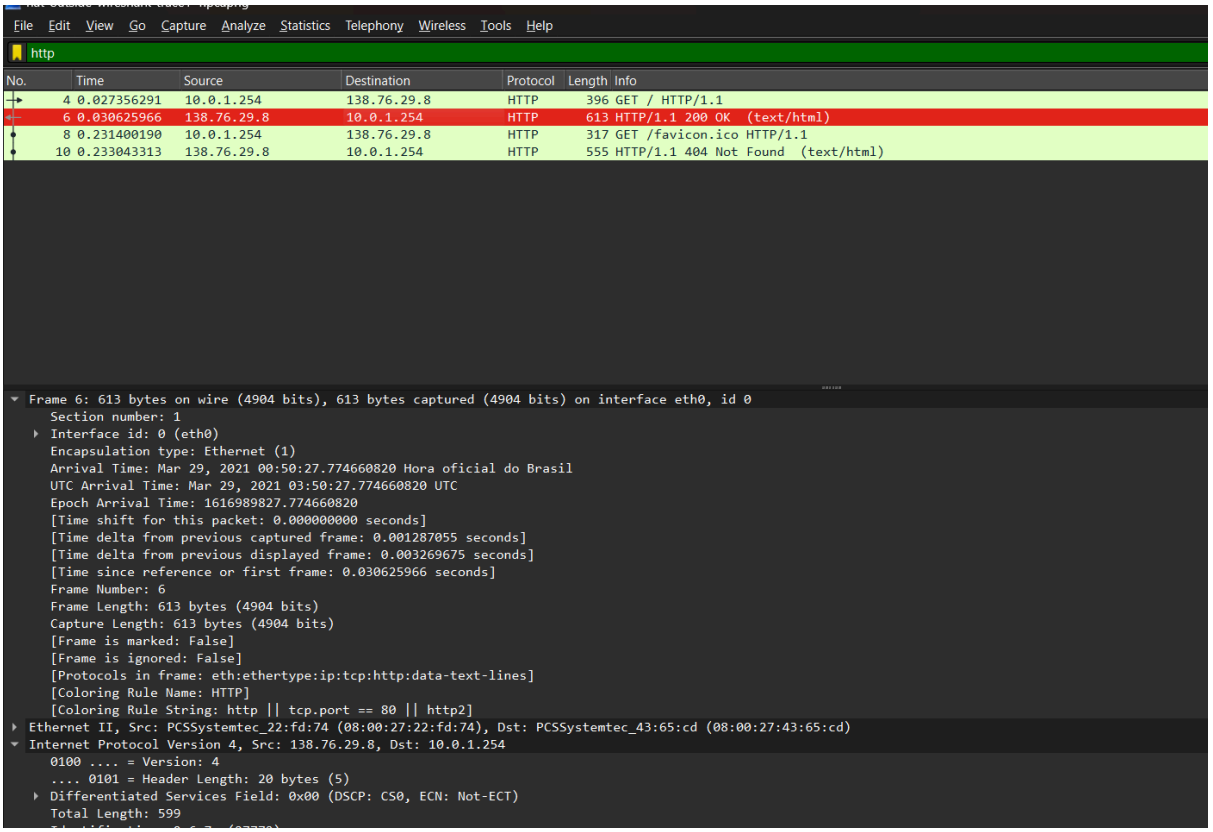
Em que momento a mensagem HTTP 200 OK correspondente do servidor web é encaminhada pelo roteador NAT para o cliente no lado LAN do roteador?
apos a requisição



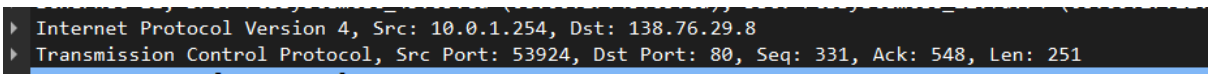
Quais são os endereços IP de origem e destino e as portas de origem e destino TCP no datagrama IP que transporta esta mensagem HTTP 200 OK?

src dst

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

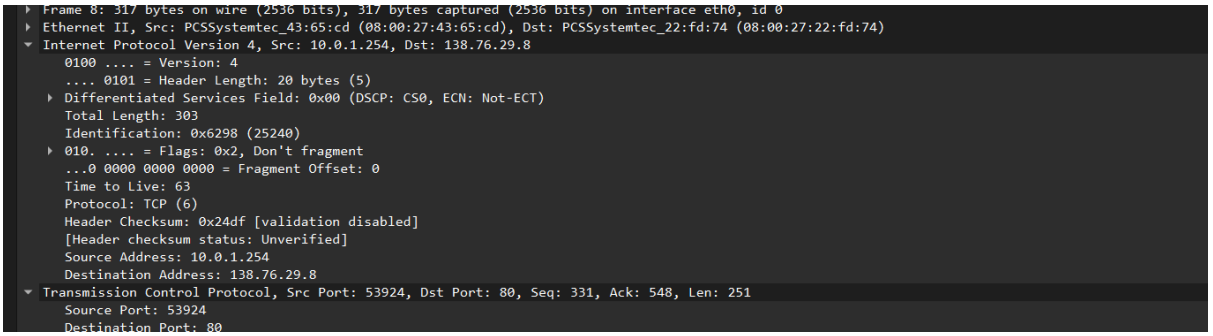


Quais são os endereços IP de origem e destino e os números de porta de origem e destino TCP no datagrama IP que transporta este HTTP GET (conforme registrado no arquivo de rastreamento nat-outside-wireshark-trace1-1.pcapng)?

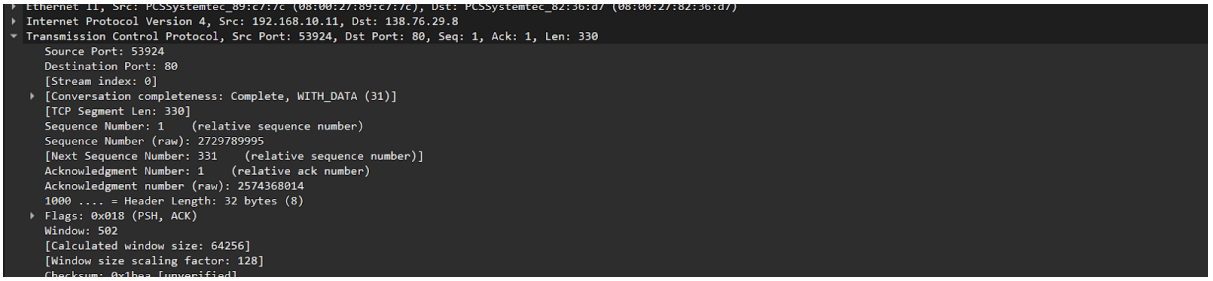


Quais destes quatro campos são diferentes da sua resposta à pergunta 1 acima?
os ips

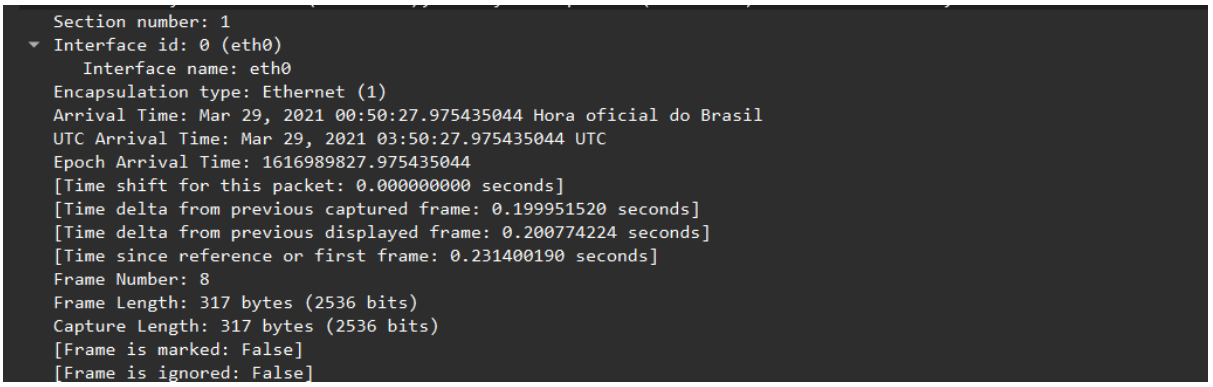
Quais dos seguintes campos no datagrama IP que transporta o HTTP GET são alterados do datagrama recebido na rede local (interna) para o datagrama correspondente encaminhado no lado da Internet (externo) do roteador NAT: Versão, Comprimento do Cabeçalho, Flags, Soma de Verificação?
campos nos prints
version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



e version inside



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



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)?