TP4

Protocolo IPv4 (802.11)

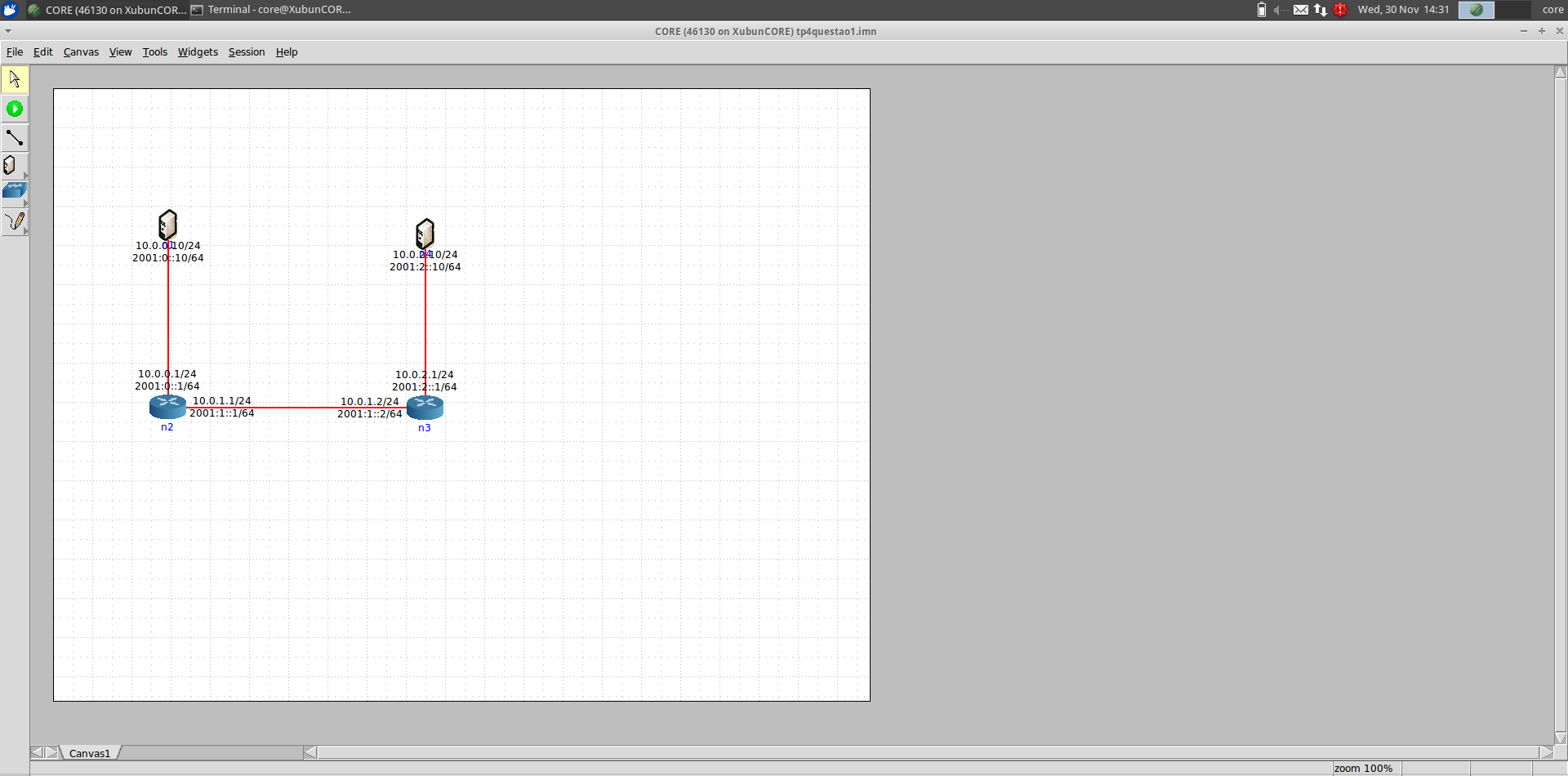
André Freitas A74619

Joel Morais A70841

Sofia Carvalho A76658

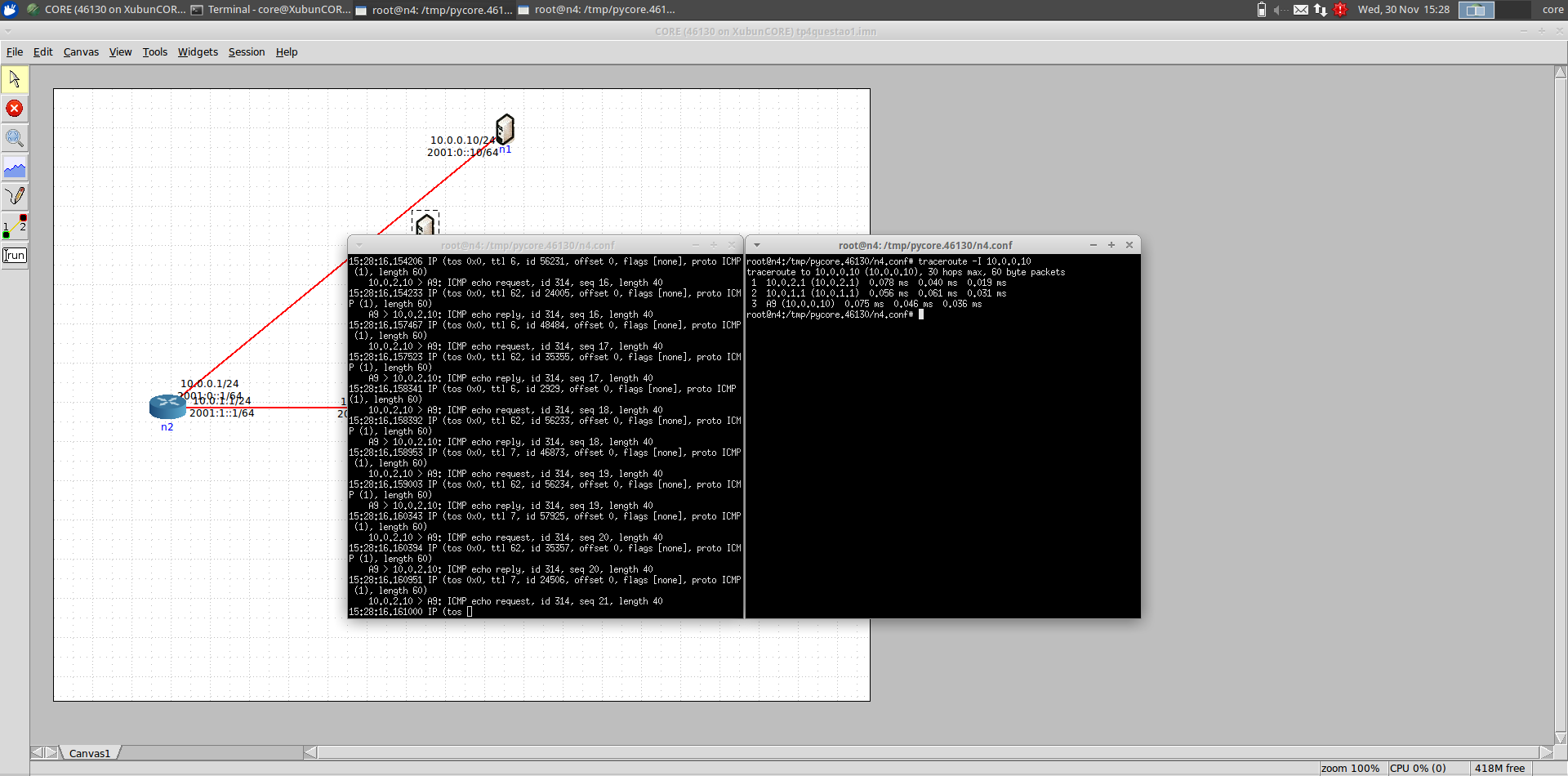
PARTE 1



****

* 1. Active o *wireshark* ou o *tcpdump* no *host* n4. Numa *shell* de n4, execute o comando *traceroute ‐I* para o endereço IP do *host* n1.

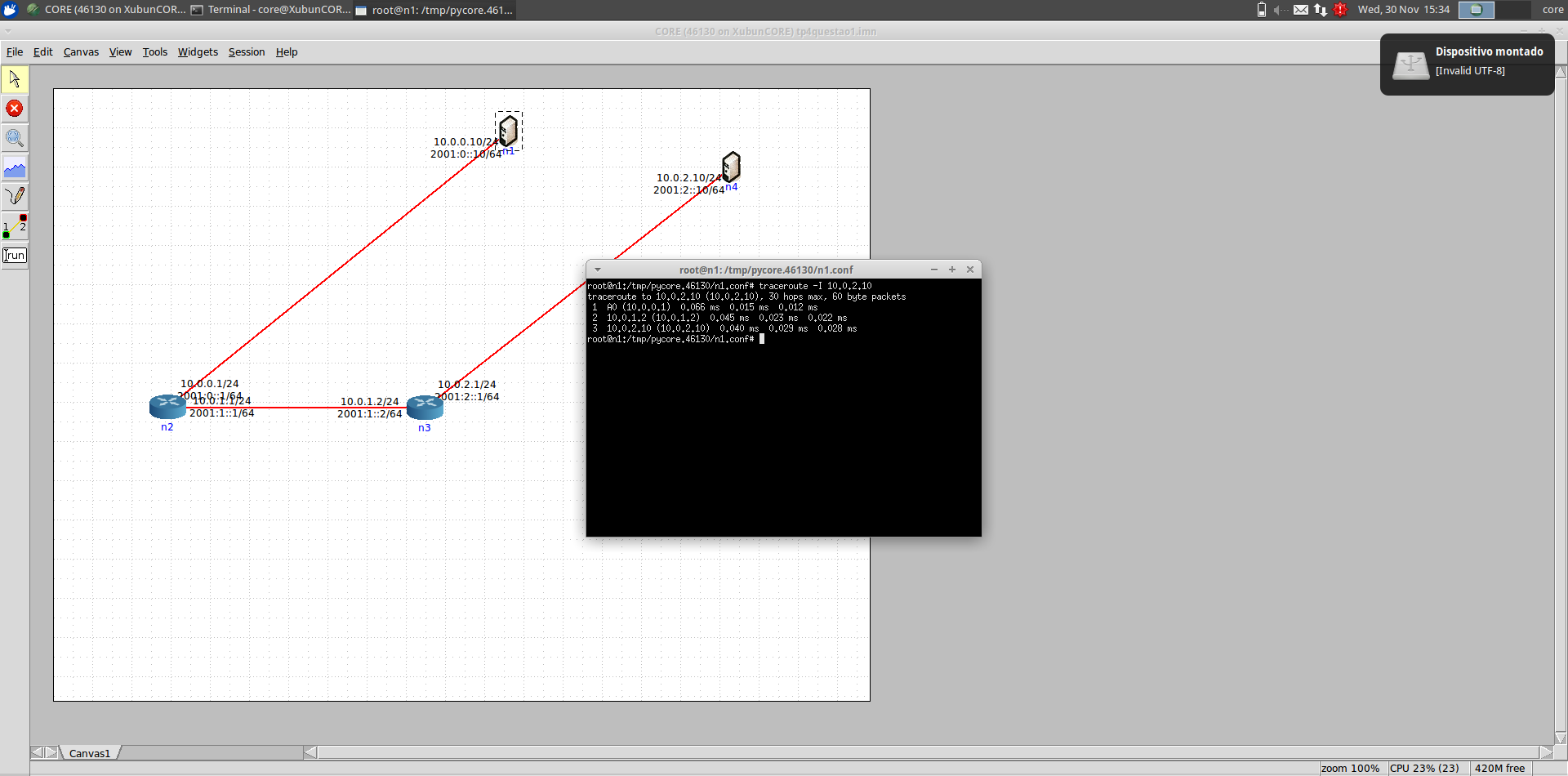
**R:**

****

* 1. Comente os resultados face ao comportamento esperado.

**R:** O tráfego ICMP enviado por n1 para 10.0.2.10 (n4) corresponde a 3 datagramas com o mesmo TTL de cada vez, pois não existe segurança na rede. Como por exemplo, pela análise da imagem acima, nos ICMP echo replies com TTL igual a 7.

* 1. Qual deve ser o valor inicial mínimo do campo TTL para alcançar o destino n1? Verifique na prática que a sua resposta está correta.



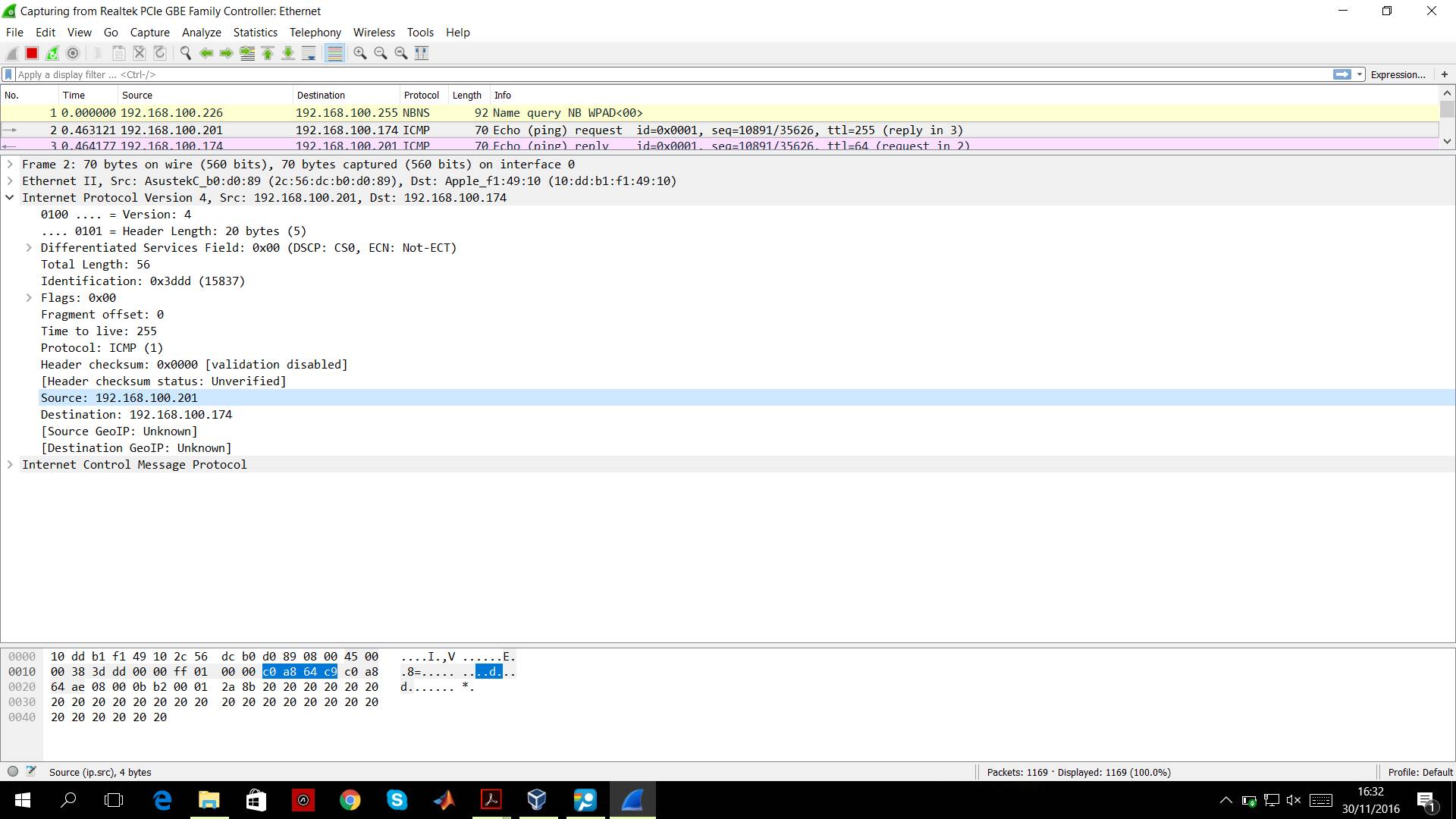
**R:** O tempo mínimo necessário para alcançar n4 é 3.

* 1. Qual o valor médio do tempo de ida-e-volta (Round-Trip Time) obtido?

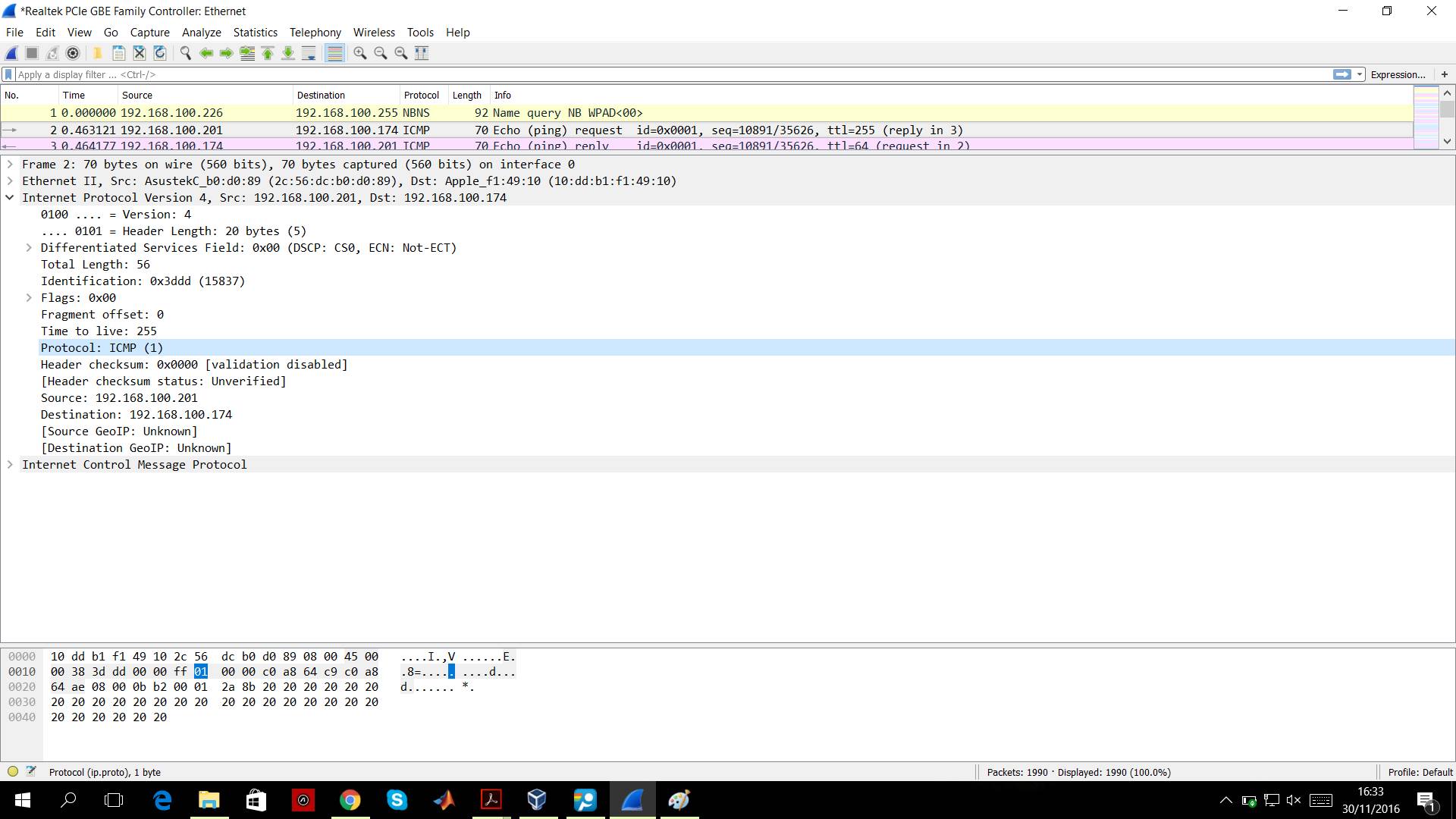
**R:** 1: (0.066 + 0.015 + 0.012) / 3 = 0.067 ms

2: (0.045 + 0.023 + 0.022) / 3 = 0.03 ms

3: (0.040 + 0.029 + 0.028) / 3 = 0.032(3) ms

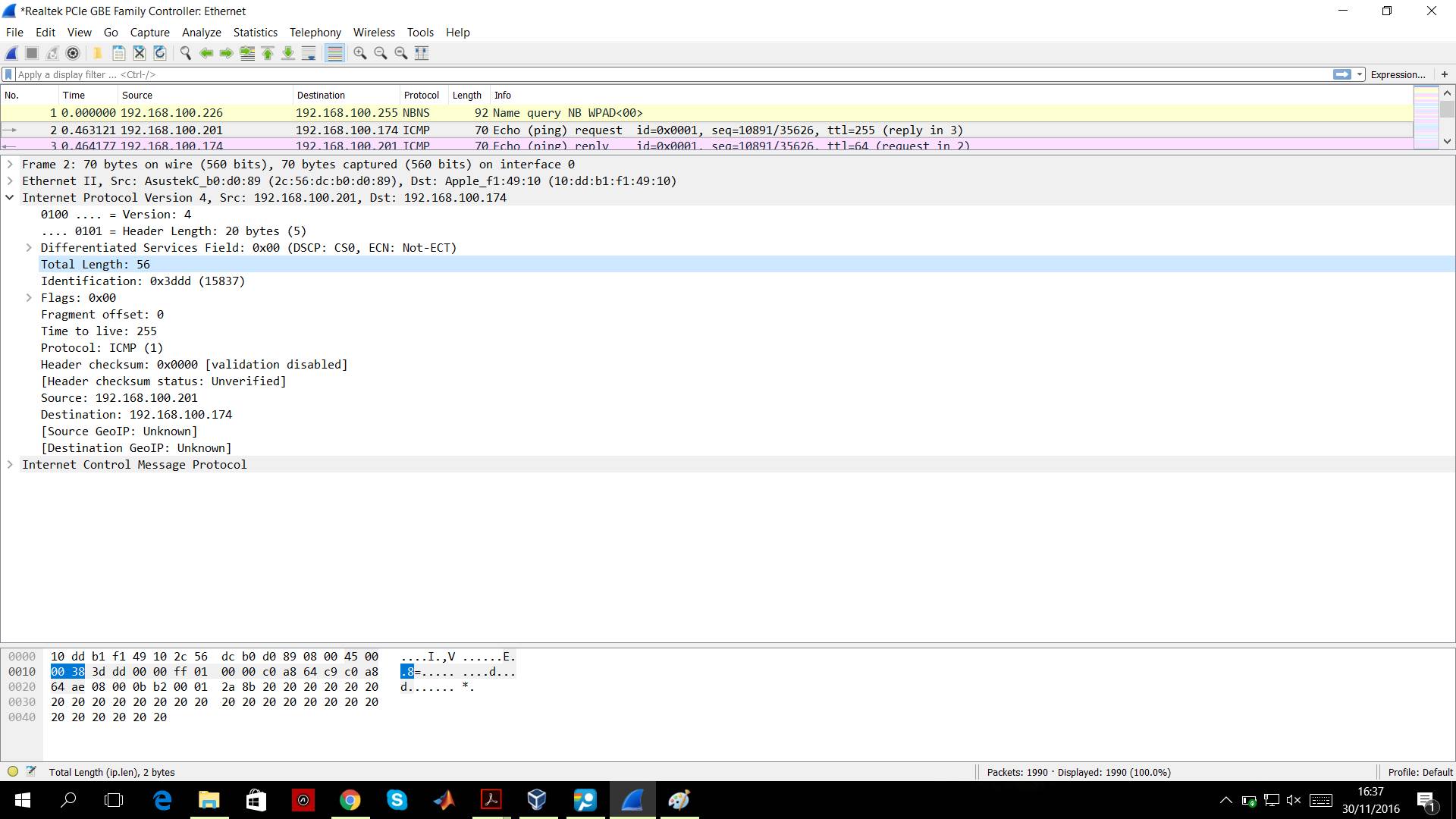
* 1. Qual é o endereço IP da interface ativa do seu computador?

**R:** O endereço IP da interface ativa do computador é o endereço “Source”, que tem o valor 192.168.100.201

* 1. Qual é o valor do campo protocolo? O que identifica?

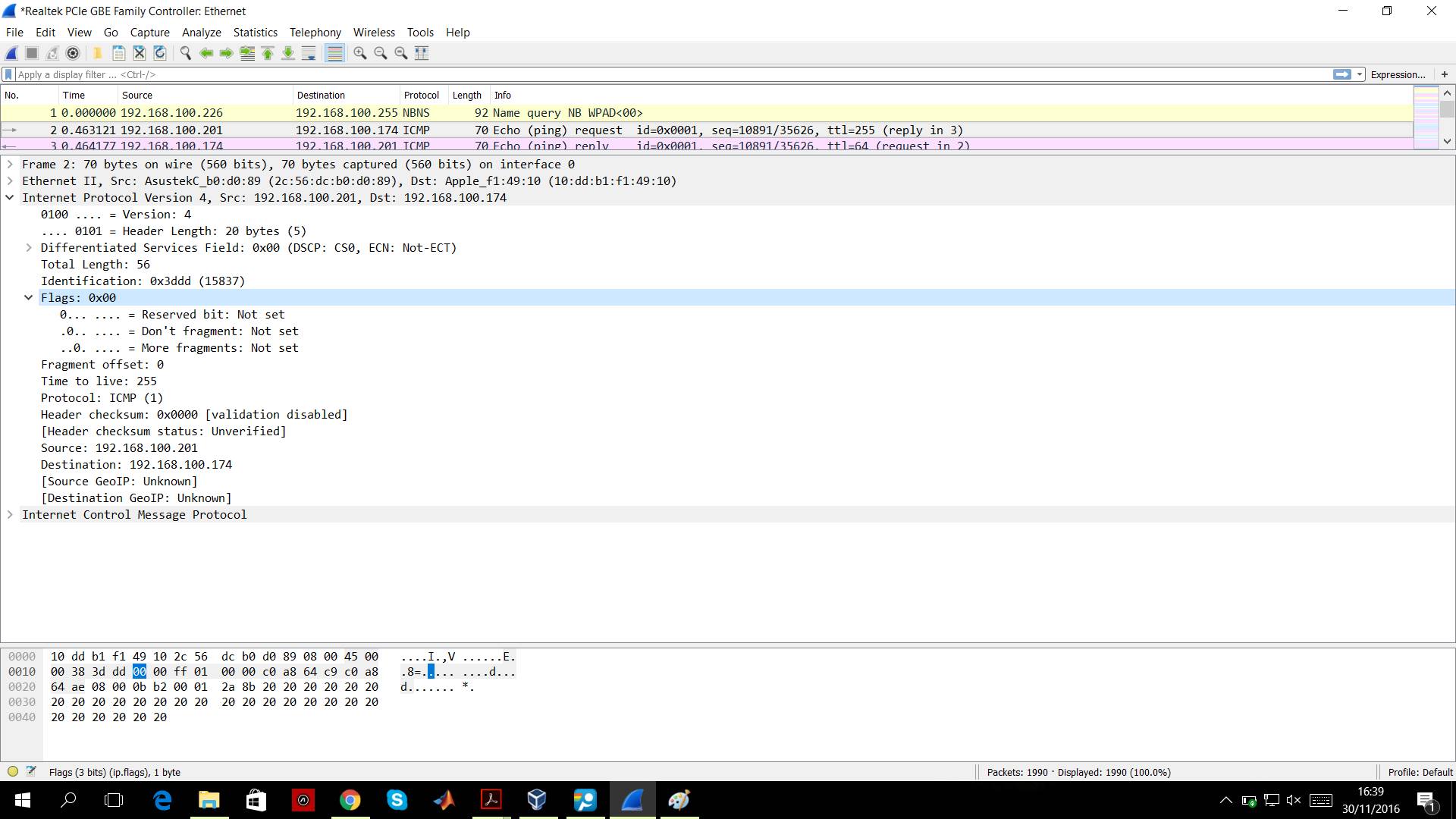
**R:** O valor do campo protocolo é 1. Este campo identifica o tipo de protocolo e neste caso trata-se de ICMP.

* 1. Quantos *bytes* tem o cabeçalho IP(v4)? Quantos *bytes* tem o campo de dados (*payload*)do datagrama? Como se calcula o tamanho do *payload*?

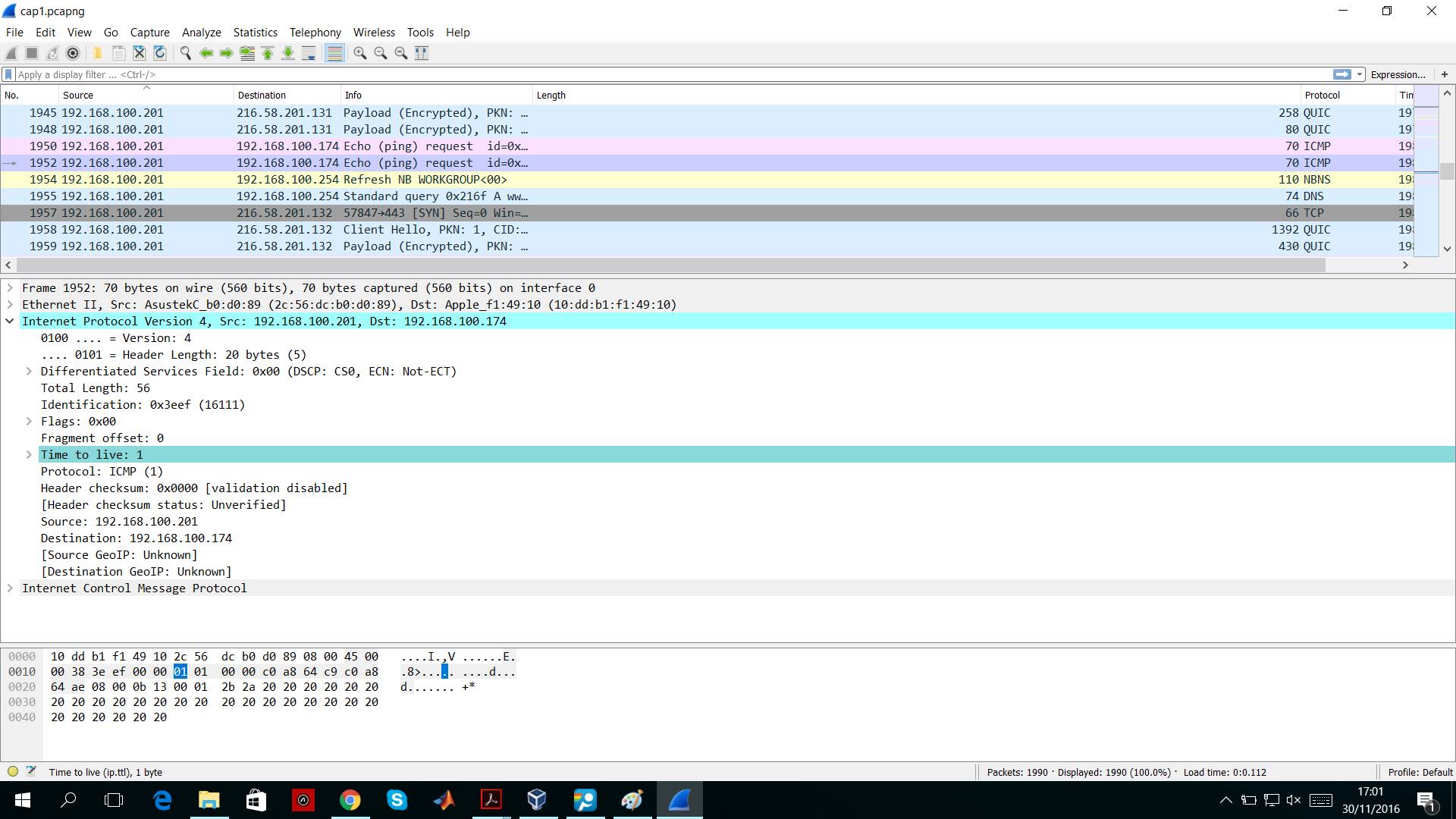
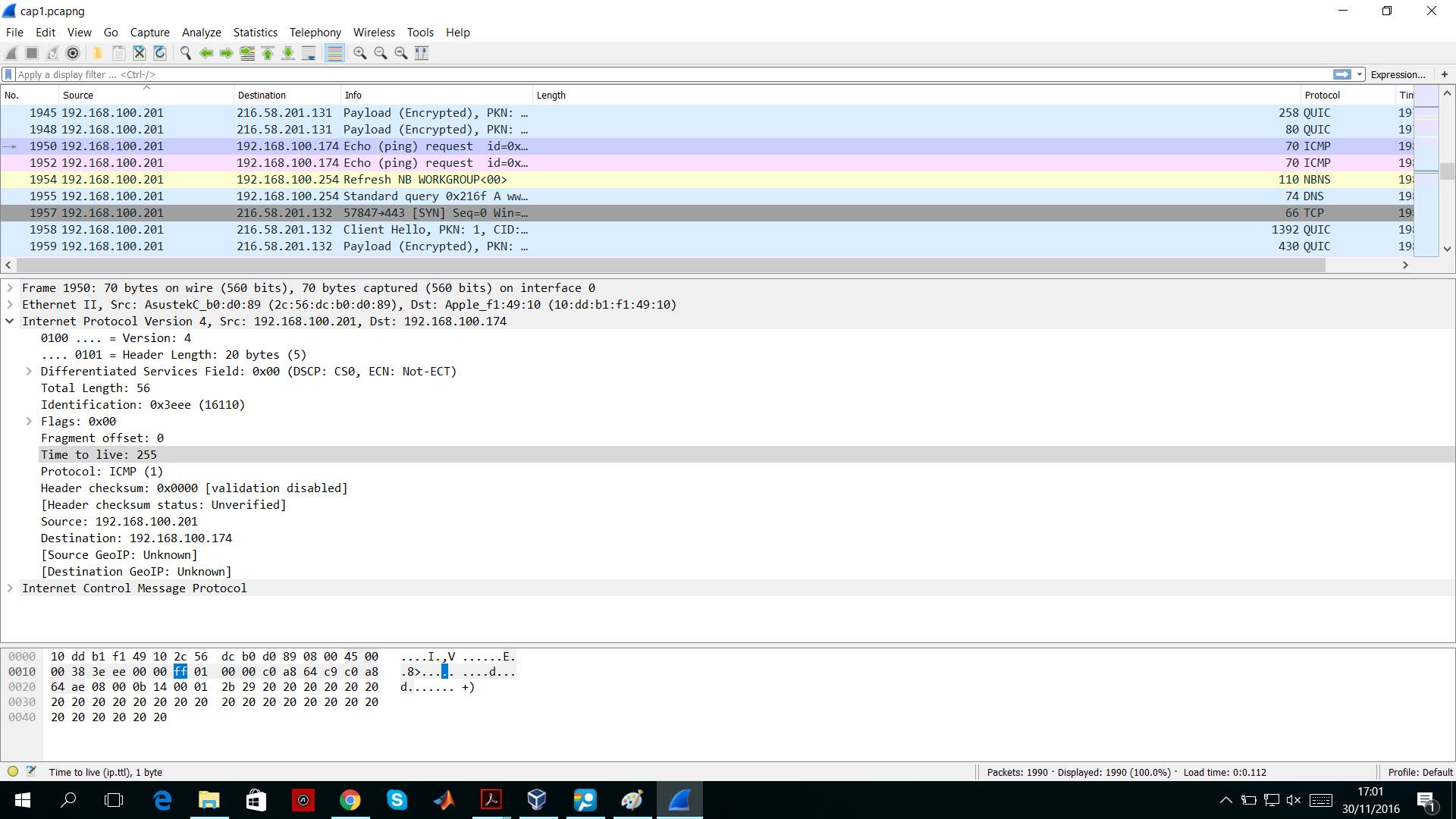


**R:** O cabeçalho IP(v4) tem 20 *bytes*. O tamanho do campo de dados é 56 e o número de *bytes* deste é 56-20=36 *bytes*.

* 1. O datagrama IP foi fragmentado?



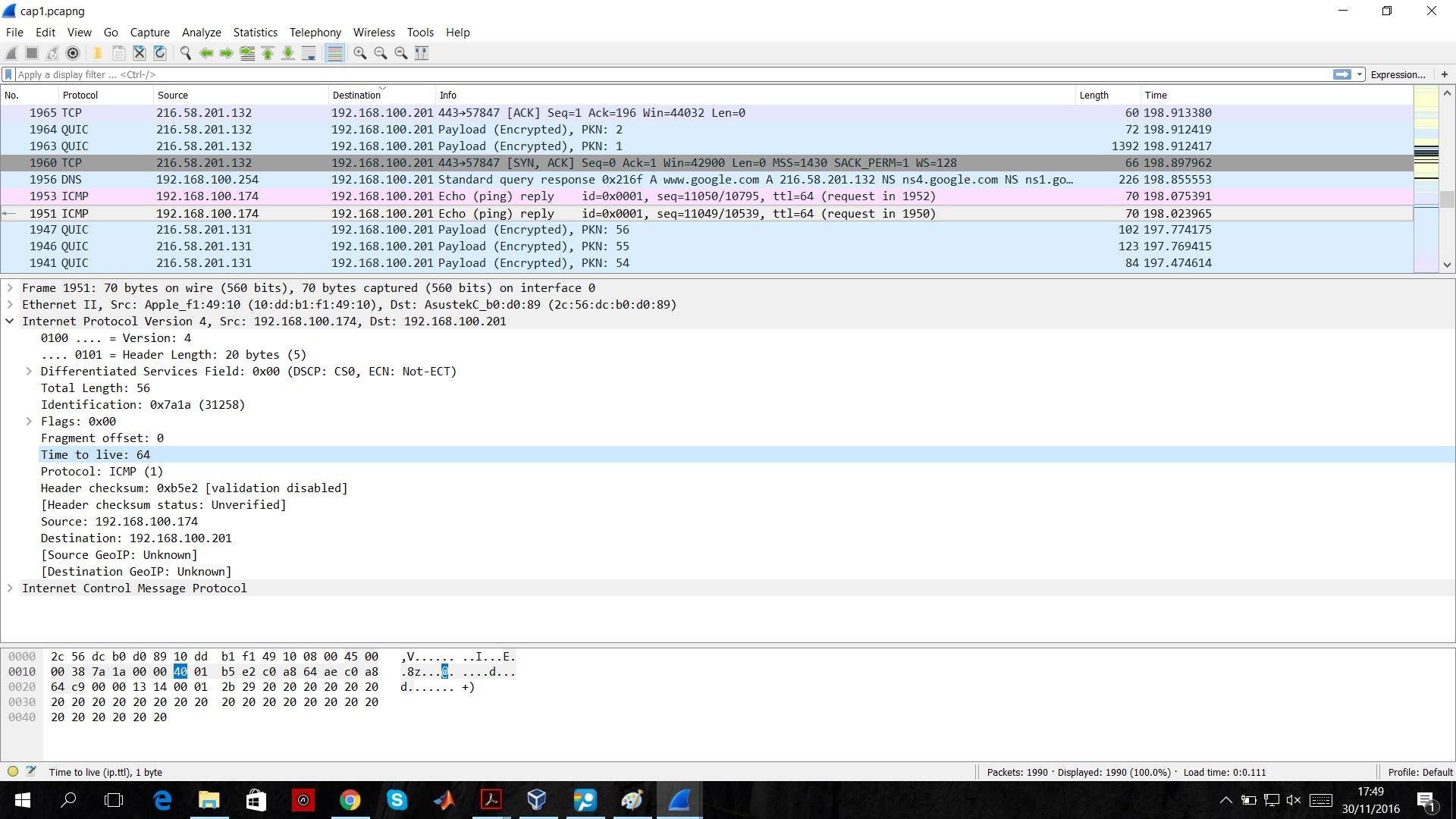
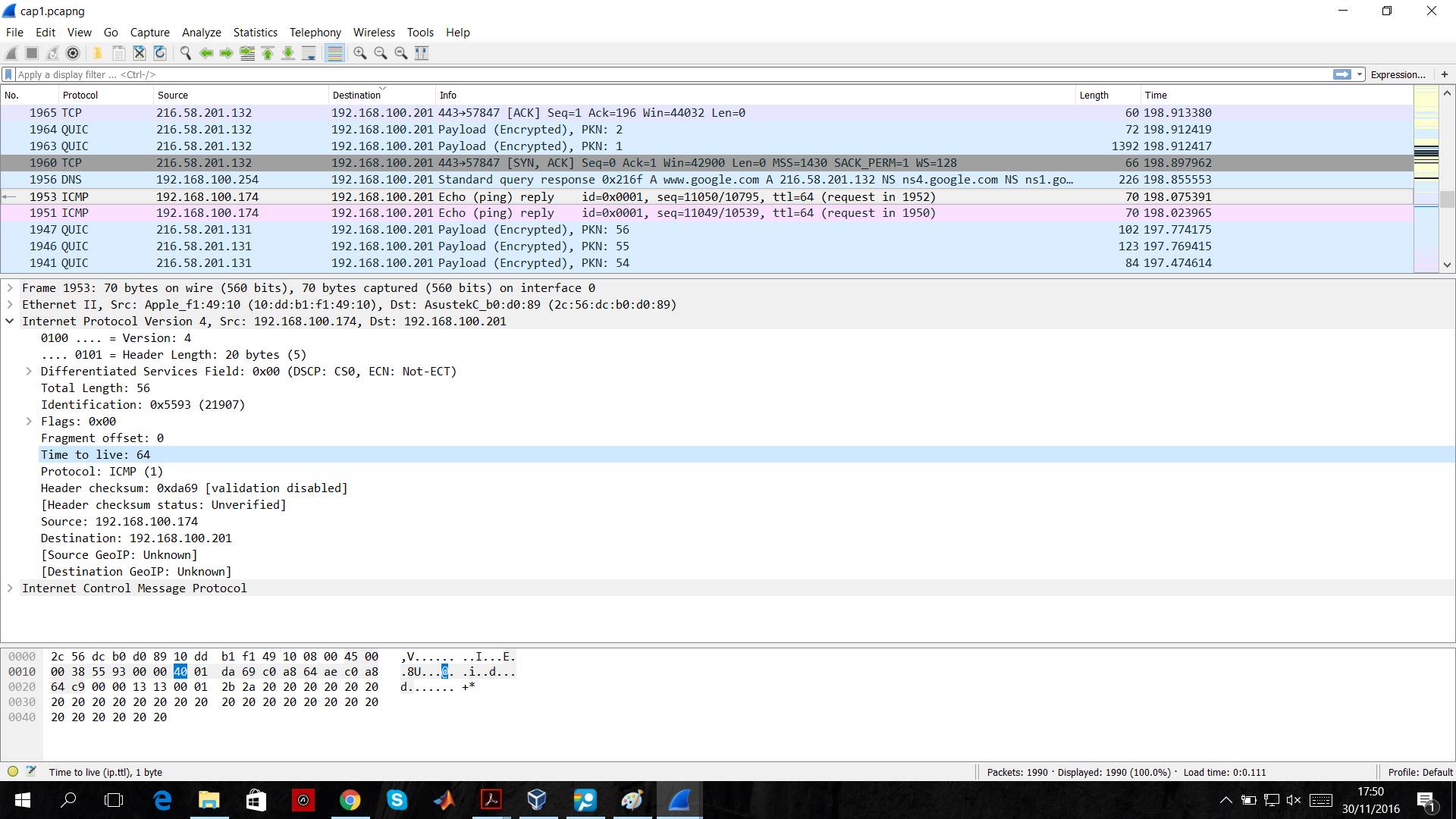
**R:** O datagrama IP não foi fragmentado, a partir da análise da informação das flags da imagem acima apresentada (“More Fragments: Not set”). Além disso, o offset toma o valor 0.

* 1. Ordene os pacotes capturados de acordo com o endereço IP fonte (e.g., selecionando o cabeçalho da coluna *Source*), e analise a sequência de tráfego ICMP gerado a partir do endereço IP atribuído à sua máquina. Para a sequência de mensagens ICMP enviadas pelo seu computador, indique que campos do cabeçalho IP variam de pacote para pacote.

**R:** Os campos do cabeçalho IP que variam de pacote para pacote são o “Time to live” e o “Identification”.

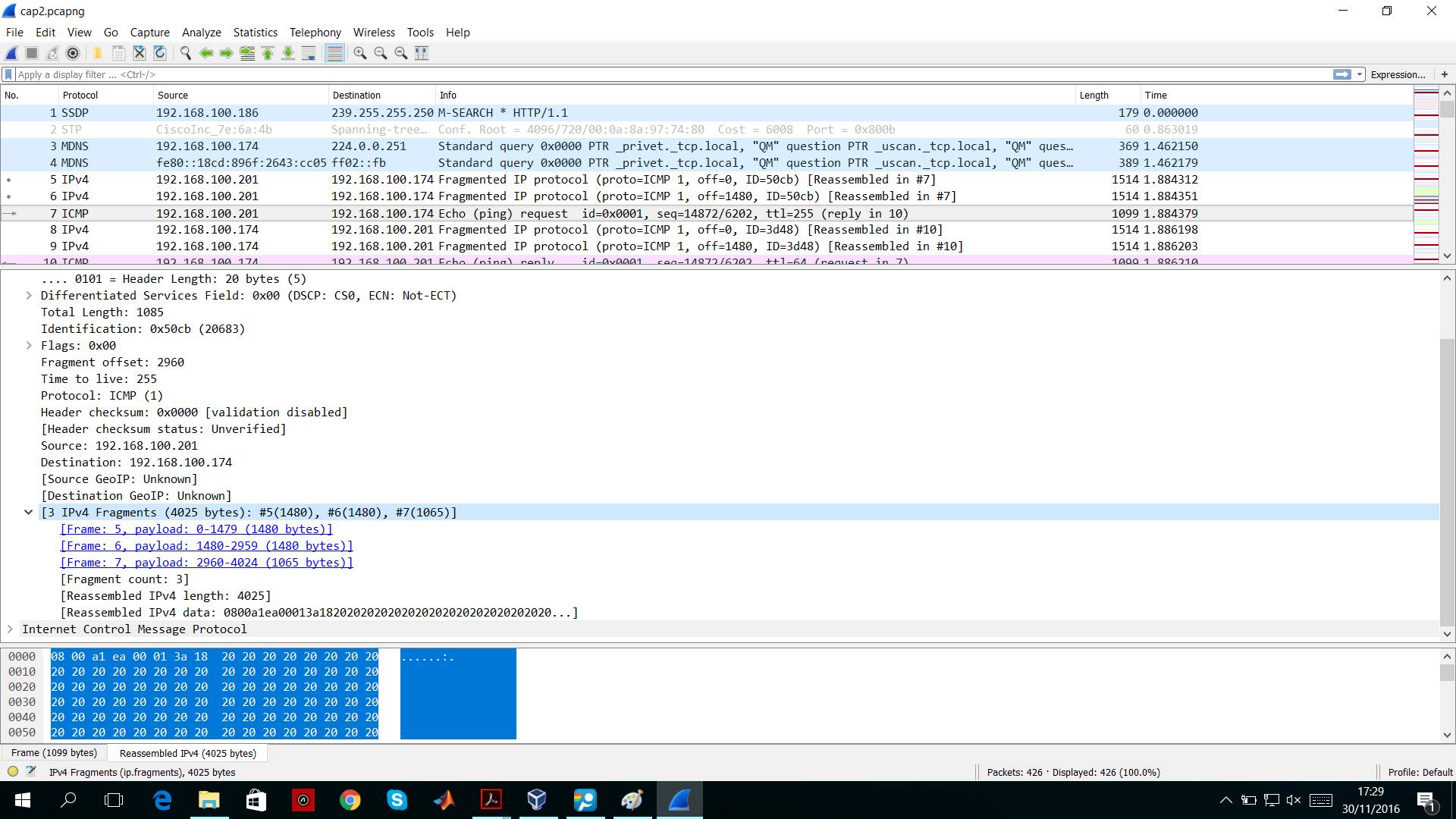
* 1. Observa algum padrão nos valores do campo de Identificação do datagrama IP e TTL?

**R:** Os campos de identificação do datagrama IP estão sequenciados (como se pode ver no campo *Identification* que consta nas imagens acima, sendo os seus valores 0x3eee e 0x3eef). O TTL também segue um padrão: verifica-se que os valores dos pedidos são sempre 255 e 1.

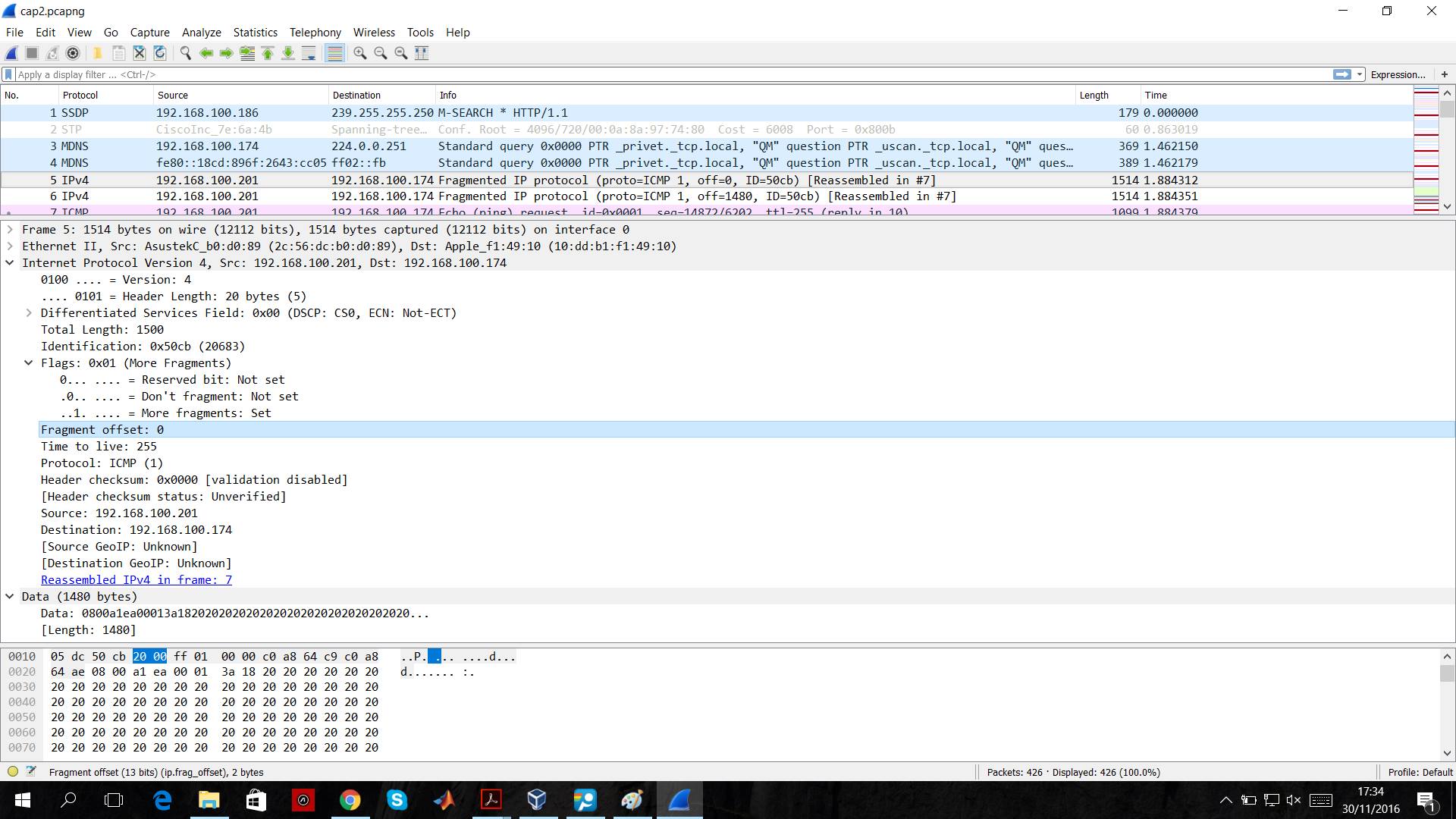
* 1. Ordene o tráfego capturado por endereço destino e encontre a série de respostas ICMP TTL *exceeded* enviadas ao seu computador. Qual é o valor do campo TTL? Esse valor permanece constate para todas as mensagens de resposta ICMP TTL *exceeded* enviados ao seu *host*? Porquê?

**R:** O valor do campo TTL é 64. Permanece constante para todas as mensagens de resposta enviadas, pois trata-se de um *reply* e, por isso, o tempo de vida tem, regra geral, um valor alto. Este valor de tempo de vida alto serve para garantir que o *reply* chega ao destino independentemente dos saltos que possa vir a dar.

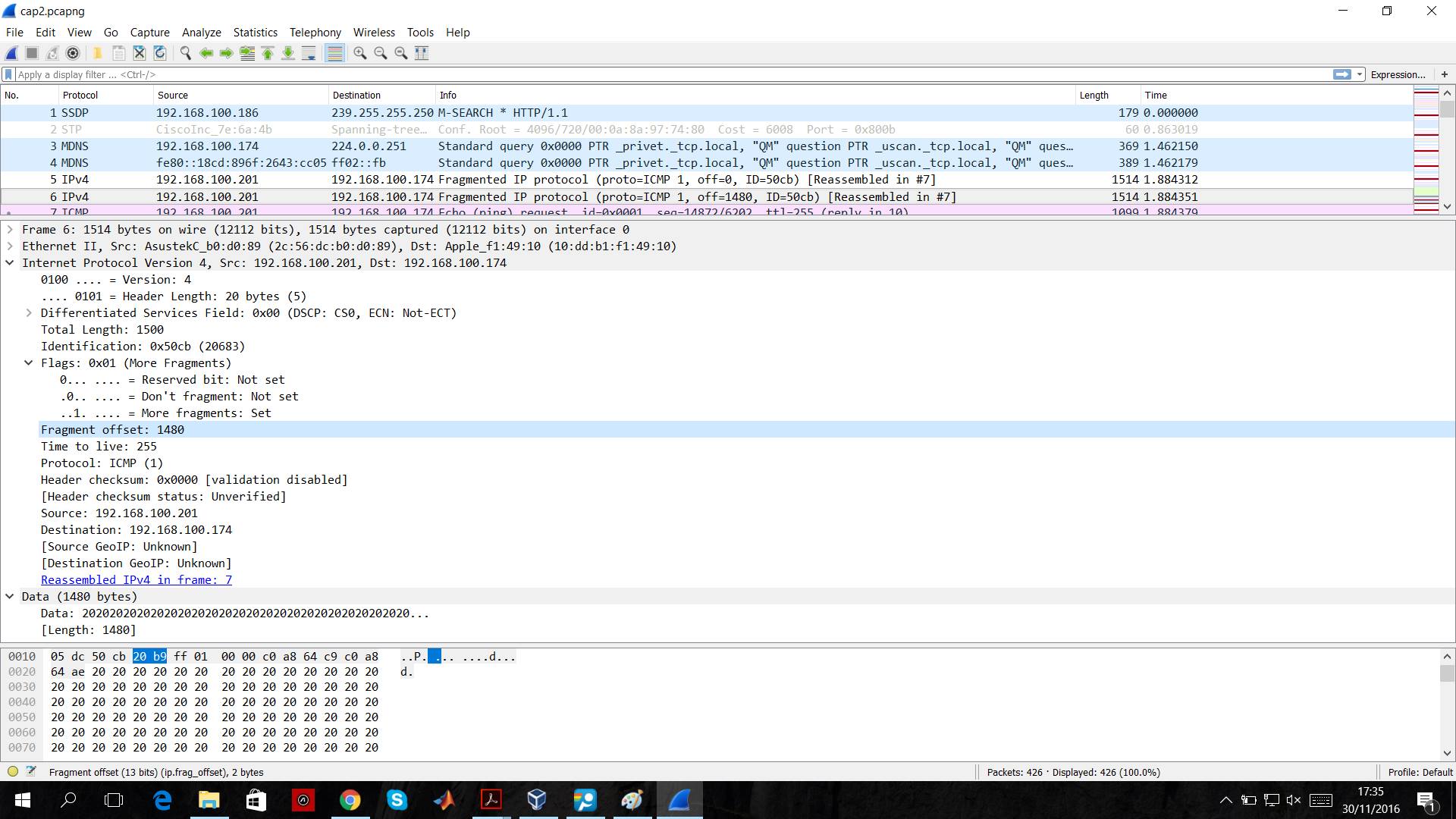
* 1. Localize a primeira mensagem ICMP. Porque é que houve necessidade de fragmentar o pacote inicial?



**R:** Houve necessidade de fragmentar o pacote inicial, pois este era demasiado grande, tendo de se dividir, neste caso, em 3 fragmentos.

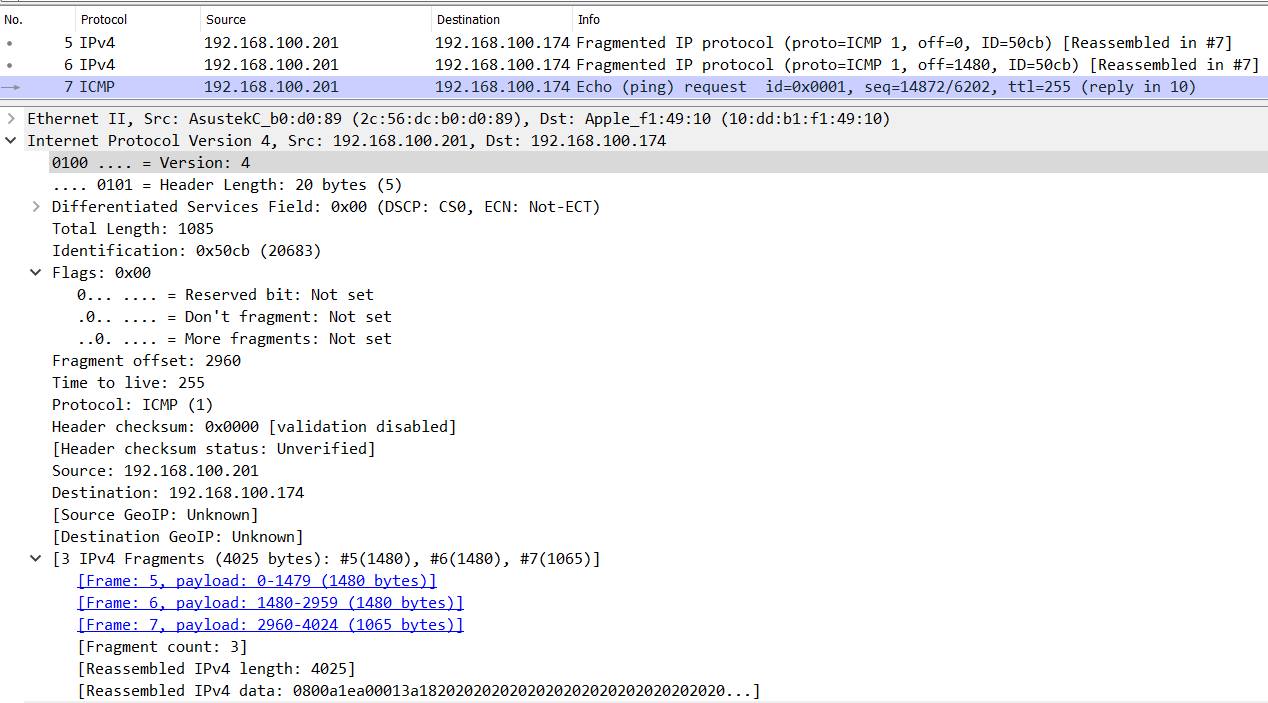
* 1. Imprima o primeiro fragmento do datagrama IP segmentado. Que informação no cabeçalho indica que o datagrama foi fragmentado? Que informação no cabeçalho IP indica que se trata do primeiro fragmento? Qual é o tamanho deste datagrama IP?

**R:** “Reassembled IPv4 in frame: 7” indica-nos que é um fragmento que vai ser reconstruído na trama 7. “More Fragments: Set” (toma valor 1) indica que existem mais fragmentos para além deste. Trata-se do primeiro fragmento pois o offset é igual a 0. O segundo fragmento vai ter o offset igual a 1480. Em relação ao tamanho, temos 1480 de dados e 20 de header, logo, no total, 1500.

* 1. Imprima o segundo fragmento do datagrama IP original. Que informação do cabeçalho IP indica que não se trata do 1º fragmento? Há mais fragmentos? O que nos permite afirmar isso?

**R:** O que indica que não se trata do 1º fragmento é o facto de o offset ter o valor 1480, ou seja, diferente de 0. Há mais fragmentos pois conseguimos ver na flag que “More Fragments : Set” (toma valor 1).

* 1. Quantos fragmentos foram criados a partir do datagrama original? Como se deteta o último fragmento correspondente ao datagrama original?



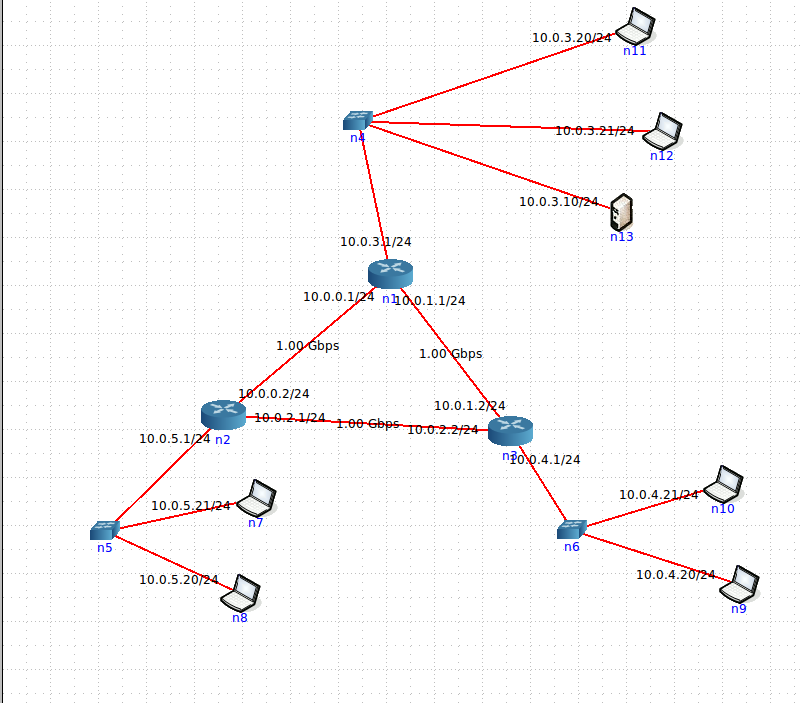
**R:** Foram criados 3 fragmentos a partir do datagrama original. Como estes 3 fragmentos vão ser reconstruídos na trama 7, a trama 7 corresponderá ao último fragmento do datagrama original. Através da flag “More Fragments: Not Set” (toma valor 0) sabemos que não há mais fragmentos, e através do offset igual a 2960 verifica-se que não se trata do primeiro fragmento, pois é diferente de 0, logo o fragmento em questão só pode ser o último.

* 1. Indique, resumindo, os campos que mudam no cabeçalho IP entre os diferentes fragmentos, e explique a forma como essa informação permite reconstruir o datagrama original.

**R:** Os campos que mudam no cabeçalho IP entre os diferentes fragmentos são o *offset* dos fragmentos, assim como a identificação de cada um destes. Através do *offset*, é possível reconstruir o datagrama, pois este fornece a posição de cada fragmento.

PARTE 2

1. Atenda aos endereços IP atribuídos automaticamente pelo CORE aos diversos equipamentos da topologia.
2. Indique que endereços IP e máscaras de rede foram atribuídos pelo CORE a cada equipamento. Se preferir, pode incluir uma imagem que ilustre de forma clara a topologia e o endereçamento.



R:

**R:** Atribuímos a seguinte máscara de rede pois temos /24 no endereço IP, o que significa que temos 24 bits identificadores da rede, sendo que isso corresponde ao endereço 255.255.255.0, visto que a máscara vai conter o limite máximo de valores decimais quando temos os primeiros 24 bits do endereço IP todos a 1.

N1 to N4: ip=10.0.3.1 Mascara de rede= 255.255.255.0

N12: ip = 10.0.3.21 Mascara de rede= 255.255.255.0

N1 to N2: ip=10.0.0.1 Mascara de rede= 255.255.255.0

N1 to N3: ip=10.0.1.2 Mascara de rede= 255.255.255.0

N11: ip=10.0.3.20 Mascara de rede= 255.255.255.0

N13: ip=10.0.3.10 Mascara de rede= 255.255.255.0

N3 to N1: ip= 10.0.1.2 Mascara de rede= 255.255.255.0

N3 to N2: ip=10.0.2.2 Mascara de rede= 255.255.255.0

N2 to N3: 10.0.2.1 Mascara de rede= 255.255.255.0

N2 to N1: 10.0.0.2 Mascara de rede= 255.255.255.0

N7: ip= 10.0.5.21 Mascara de rede= 255.255.255.0

N8: ip=10.0.5.20 Mascara de rede= 255.255.255.0

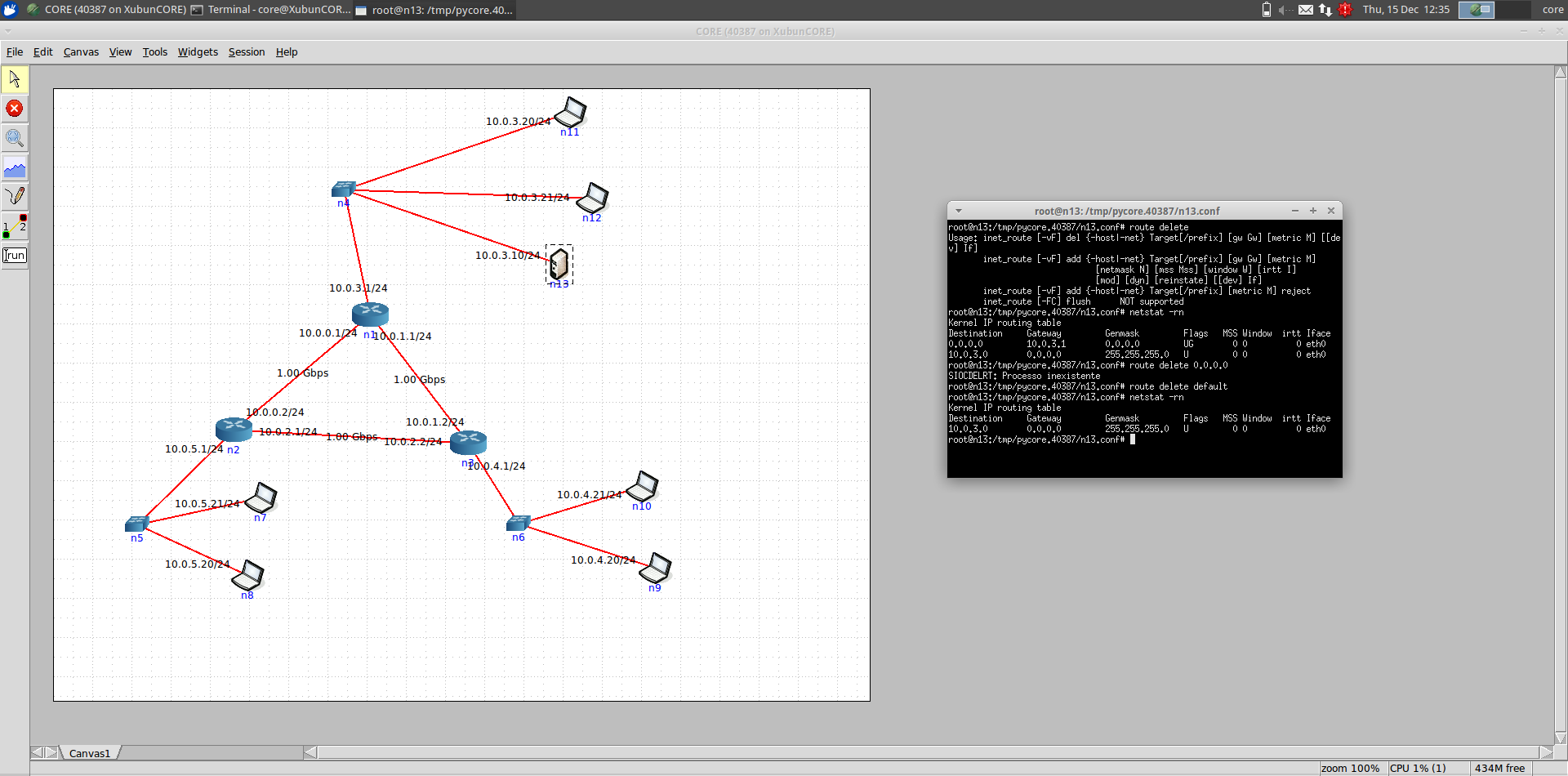
N9: ip=10.0.4.20 Mascara de rede= 255.255.255.0

N10: 10.0.4.21 Mascara de rede= 255.255.255.0

1. Tratam-se de endereços públicos ou privados? Porquê?

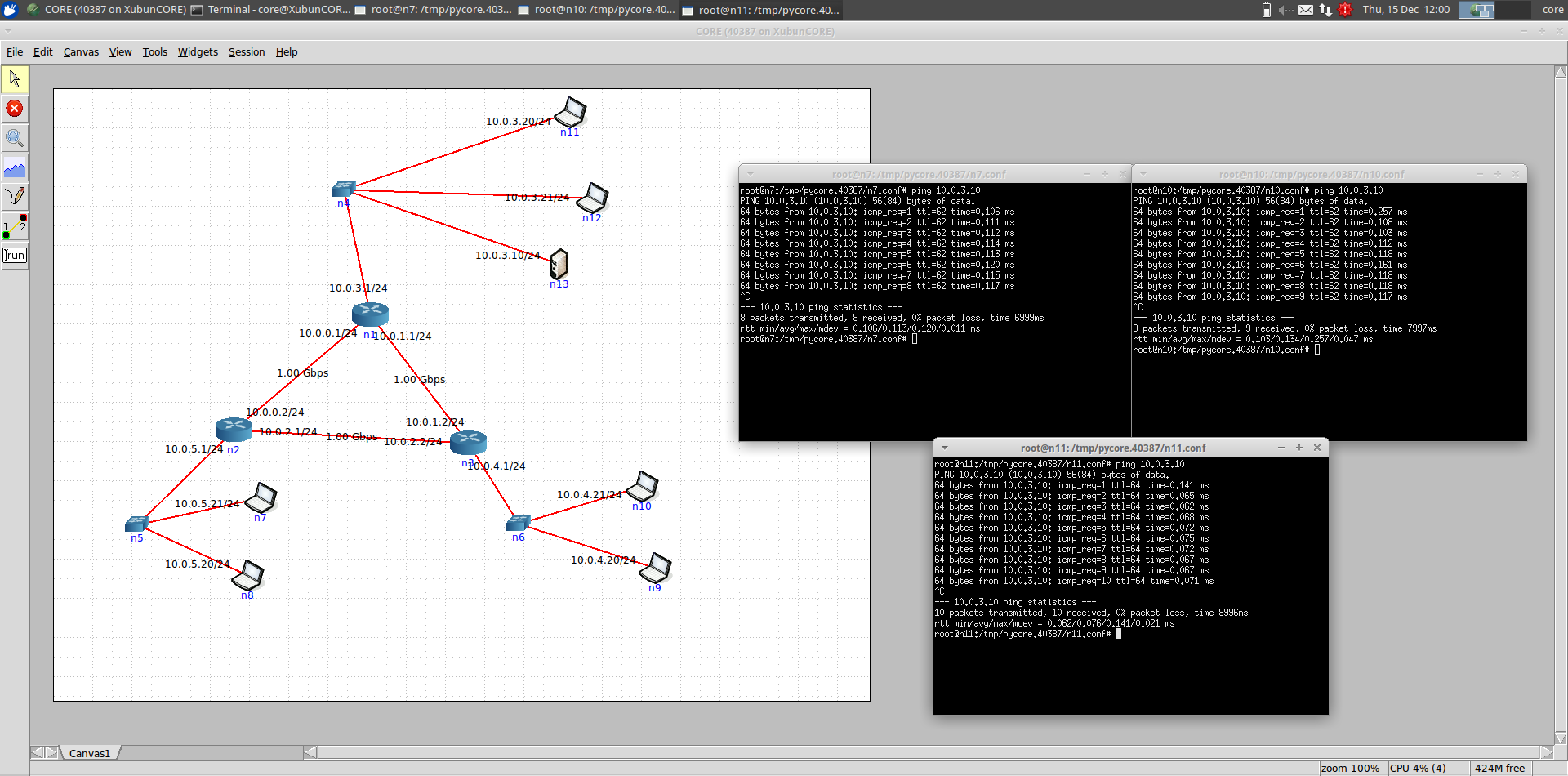
**R:** Estes endereçamentos vão ser privados, visto que eles não têm acesso direto à internet.

1. Porque razão não é atribuído um endereço IP aos *switches*?



**R:** Não é atribuído um endereço IP aos *switches* porque estes são usados em ligações de nível 2, e o endereço IP só irá ser atribuído em ligações de nível 3, nível de rede.

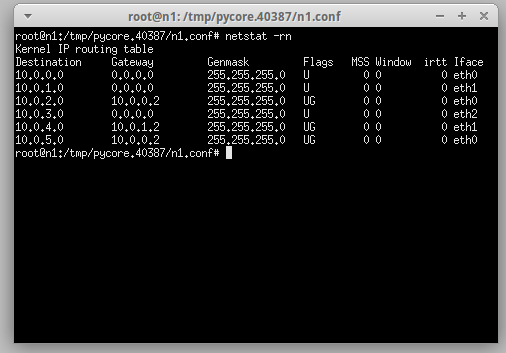
1. Usando o comando *ping* certifique-se que existe conectividade IP entre os laptops dos utilizadores e o servidor do departamento A (basta certificar a conectividade de um laptop por departamento).



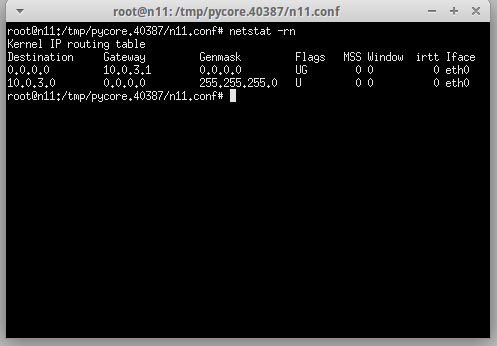
**R:** Como se pode ver pela figura acima, existe conetividade entre um laptop de cada departamento e o servidor do departamento A, sendo n7 do departamento B, n10 do departamento C, n11 do departamento A e 10.0.3.10 o endereço IP do servidor do departamento A.

1. Para o router e um laptop do departamento A:
2. Execute o comando netstat –rn por forma a poder consultar a tabela de encaminhamento unicast (Ipv4). Inclua no seu relatório as tabelas de encaminhamento obtidas; interprete as várias entradas de cada tabela. Se necessário, consulte o manual respetivo (man netstat).

*Router:*



*Laptop:*



**R:** Relativamente ao router N1: A primeira entrada da tabela tem como rede destino a rede entre os routers N1 e N2 (10.0.0.0) e o próximo salto vai corresponder ao próprio router N1 (10.0.0.1, sendo na tabela representado por 0.0.0.0), pois já estamos dentro dessa rede.

Para a segunda entrada, a rede destino é entre os routers N1 e N3 (10.0.1.0) e o próximo salto vai corresponder ao próprio router N1 (10.0.1.1, sendo na tabela representado por 0.0.0.0), pois já estamos dentro dessa rede.

Para a terceira entrada, o destino é a rede dos routers N2 e N3 (10.0.2.0) e o próximo salto vai corresponder ao router N2 (10.0.0.2) visto ser o caminho mais próximo de chegarmos a essa rede através do router N1.

Para a quarta entrada, o destino é a rede do departamento A (10.0.3.0) e o próximo salto vai corresponder ao router N1 (10.0.0.1, sendo na tabela representado por 0.0.0.0), pois já estamos dentro dessa rede.

Para a quinta entrada, o destino é a rede do departamento C (10.0.4.0) e o próximo salto vai corresponder ao *router* N3 (10.0.1.2) visto que é o caminho mais próximo de chegarmos a essa rede através do router N1.

Para a sexta entrada, o destino é a rede do departamento B (10.0.5.0) e o próximo salto vai corresponder ao *router* N2 (10.0.0.2) pois é o caminho mais próximo para chegarmos a essa rede através do router N1.

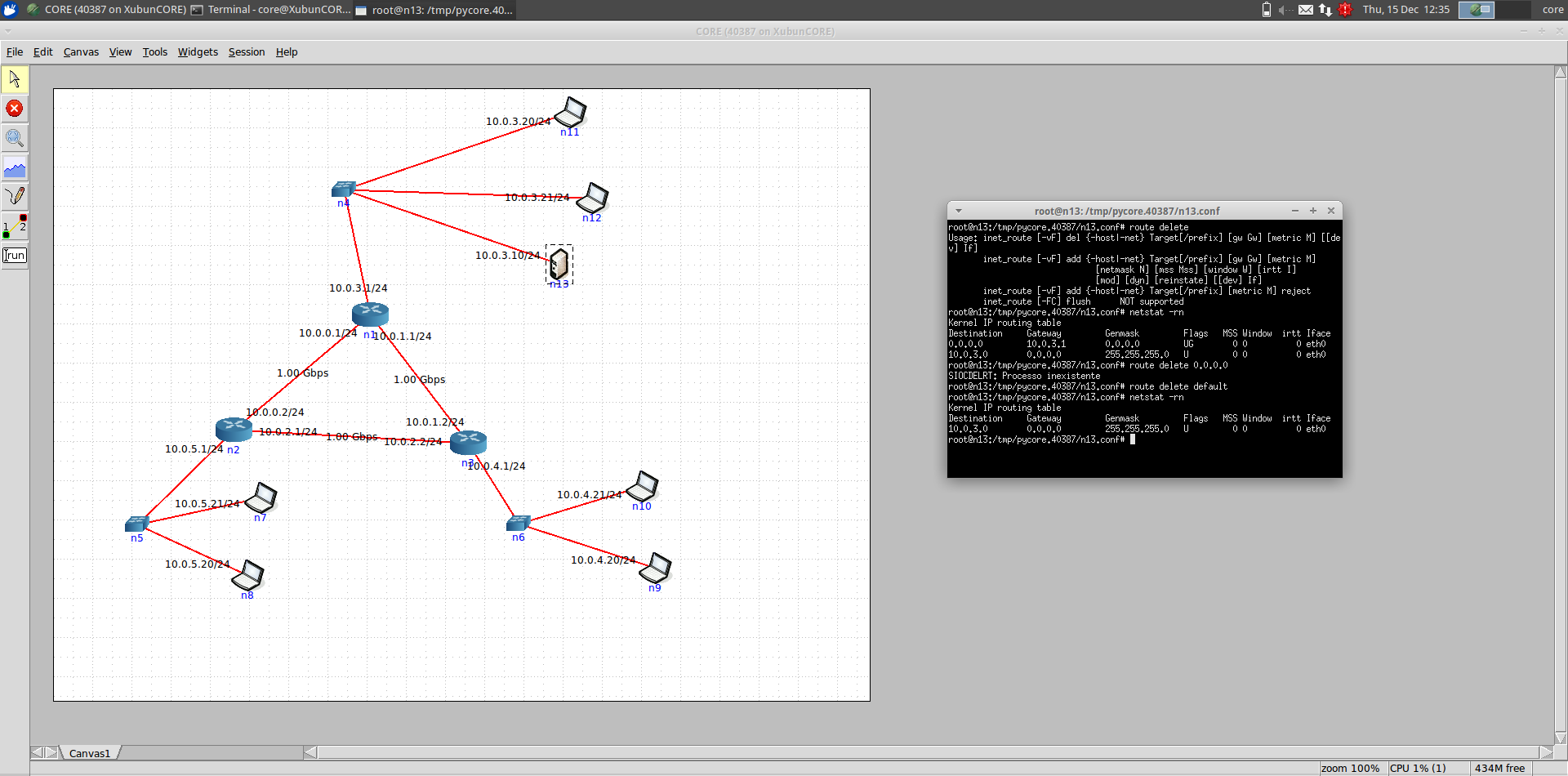
Relativamente ao laptop:Para a primeira entrada da tabela de encaminhamento, a rede destino é a rota por defeito (0.0.0.0) e o próximo salto vai corresponder ao *router* N1 (10.0.3.1).

Para a segunda entrada, a rede destino é a rede do departamento A (10.0.3.1) e o próximo salto vai corresponder ao próprio *host* (10.0.3.10, sendo que na tabela corresponde a 0.0.0.0).

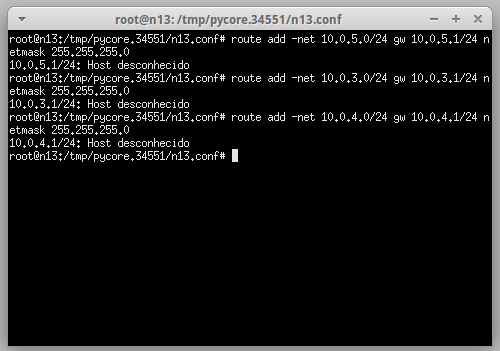
1. Diga, justificando, se está a ser usado encaminhamento estático ou dinâmico ( sugestão: analise que processos estão a correr em cada sistema ).

**R:** Está a ser usado encaminhamento estático nos três departamentos porque, além de ser uma rede de pequena dimensão, o endereçamento é baseado em rotas pré-definidas e estas rotas permanecem fixas e entre os routers dos três departamentos o encaminhamento é dinâmico.

1. Admita que, por questões administrativas, a rota por defeito (0.0.0.0 ou default ) deve ser retirada definitivamente da tabela de encaminhamento do servidor localizado no departamento A. Use o comando route delete para o efeito. Que implicações tem esta medida para os utilizadores da empresa que acedem ao servidor. Justifique.



**R:** A implementação desta medida não tem nenhuma implicação para os utilizadores que acedem ao servidor pois continua a existir a rota para a rede [10.0.3.0](http://l.facebook.com/l.php?u=http%3A%2F%2F10.0.3.0%2F&h=fAQEAfHBl) a partir do servidor.

1. Adicione as rotas estáticas necessárias para restaurar a conectividade para o servidor, por forma a contornar a restrição imposta em c). Utilize para o efeito o comando route add e registe os comandos que usou.

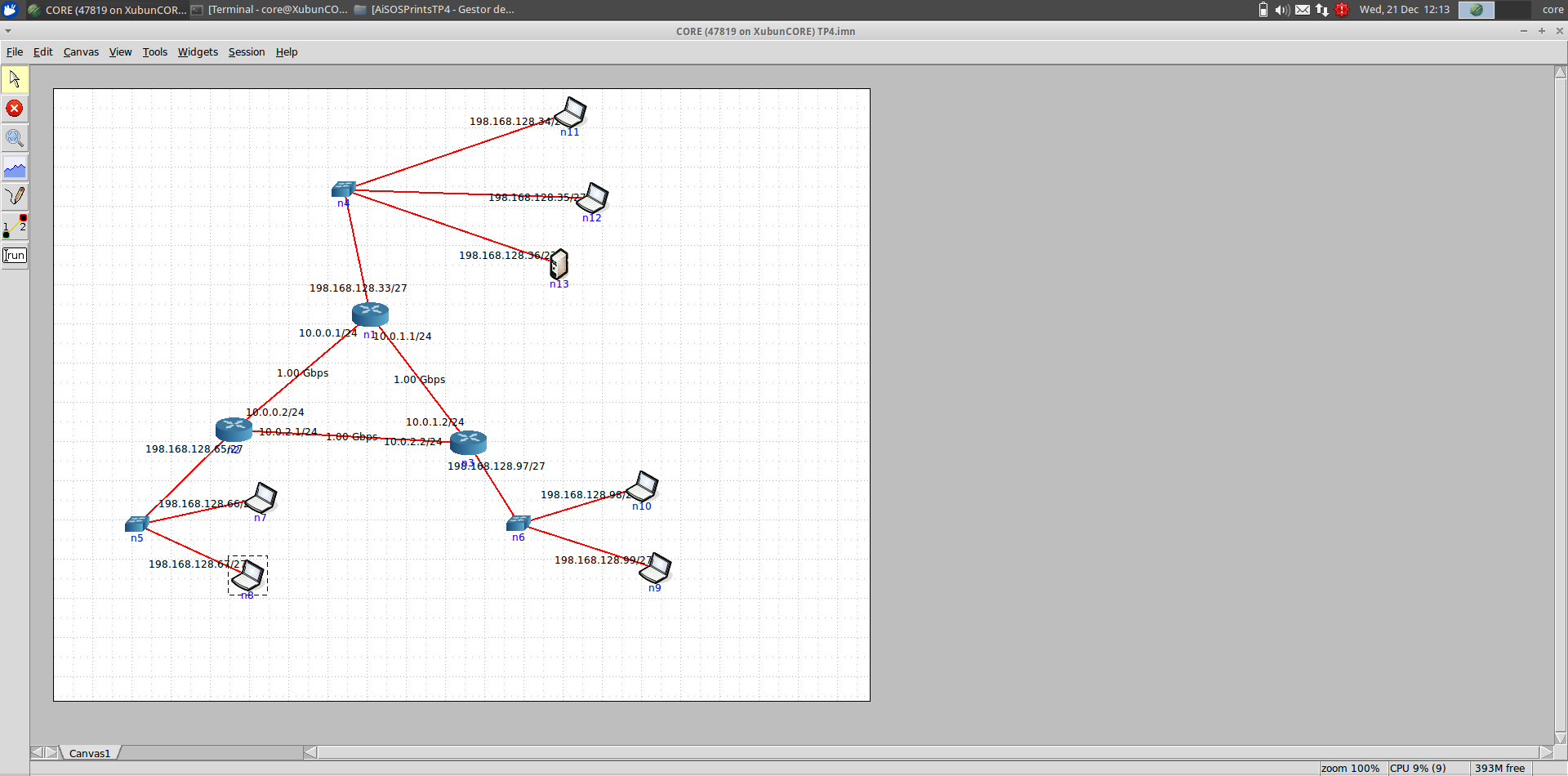
**R:** Como se pode ver pela figura acima tentamos restaurar a conetividade como pretendido, no entanto, encontramos um erro que não conseguimos ultrapassar.

1. Teste a nova política de encaminhamento garantindo que o servidor está novamente acessível, utilizando para o efeito o comando ping. Registe a nova tabela de encaminhamento do servidor.

**R:** Face à situação descrita anteriormente na questão d, o servidor não poderá estar acessível e a tabela de encaminhamento será aquela que obtivemos no final da questão c.

1. Assumindo que dispõe apenas de um único endereço de rede IP classe C 192.168.128.0/24, defina um novo esquema de endereçamento para as redes dos departamentos (mantendo a rede de core inalterada) e atribua endereços às interfaces dos vários sistemas envolvidos. Deve justificar as opções usadas.

**R:**



192.168.128.0/24

3 sub-redes (uma por departamento)

8 bits para gerir (32-24=8)

Usando 3 bits, é possível definir 23-2=6 sub-redes. Usando menos de 3 bits, apenas poderíamos definir 2 sub-redes ou menos (22-2=2). Para o *host*, usamos 5 bits pois permite obter 25-2=30 *hosts* diferentes. Estes 5 bits são suficientes para os dispositivos que temos ligados e permite um bom crescimento desta sub-rede a nível do número de *hosts* ligados.

SR1: 198.168.128.32/27 -> 198.168.33 até .62

SR2: 198.168.128.64/27 -> 198.168.128.65 até .94

SR3: 198.168.128.96/27 -> 198.168.128.97 até .126

SR1 – departamento A

n1: 198.168.128.33/27

n11: 198.168.128.34/27

n12: 198.168.128.35/27

n13: 198.168.128.36/27

SR2 – departamento B

n2: 198.168.128.65/27

n7: 198.168.128.66/27

n8: 198.168.128.67/27

SR3 – departamento C

n3: 198.168.128.97/27

n9: 198.168.128.98/27

n10: 198.168.128.99/27

1. Qual a máscara de rede que usou (em formato decimal)? Justifique.

Identificam a rede

**R:** 11111111.11111111.11111111.111000002

3 bits da sub-rede

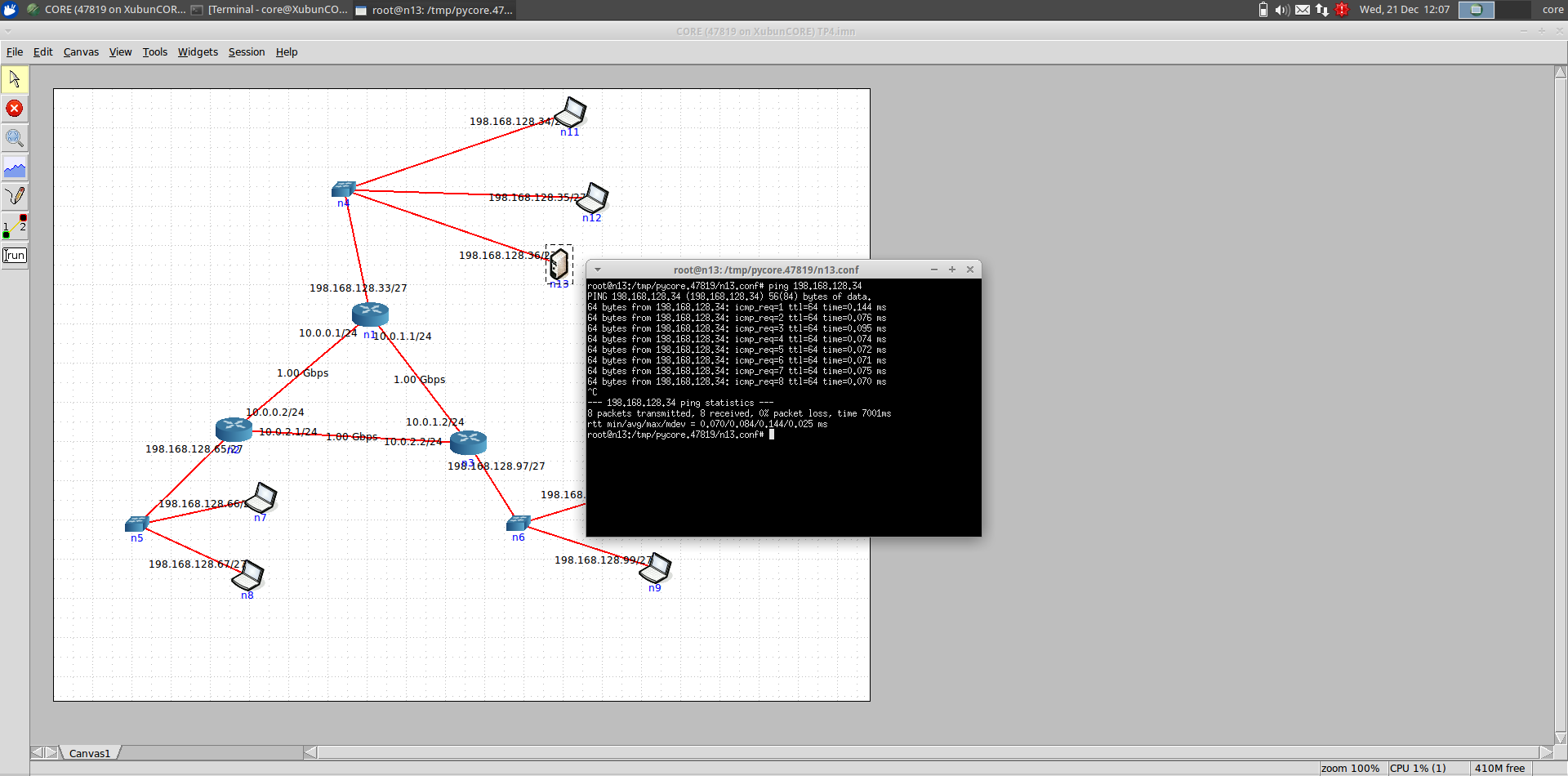
255.255.255.22410. Existem 27 bits para identificar a rede, sendo 3 destes usados para especificar a sub-rede. Por isso, e como para criar a máscara de rede é necessário colocar todos os bits identificadores da rede a 1, o número obtido em decimal foi 255.255.255.22410.

1. Quantos *hosts* IP pode interligar em cada departamento? Justifique.

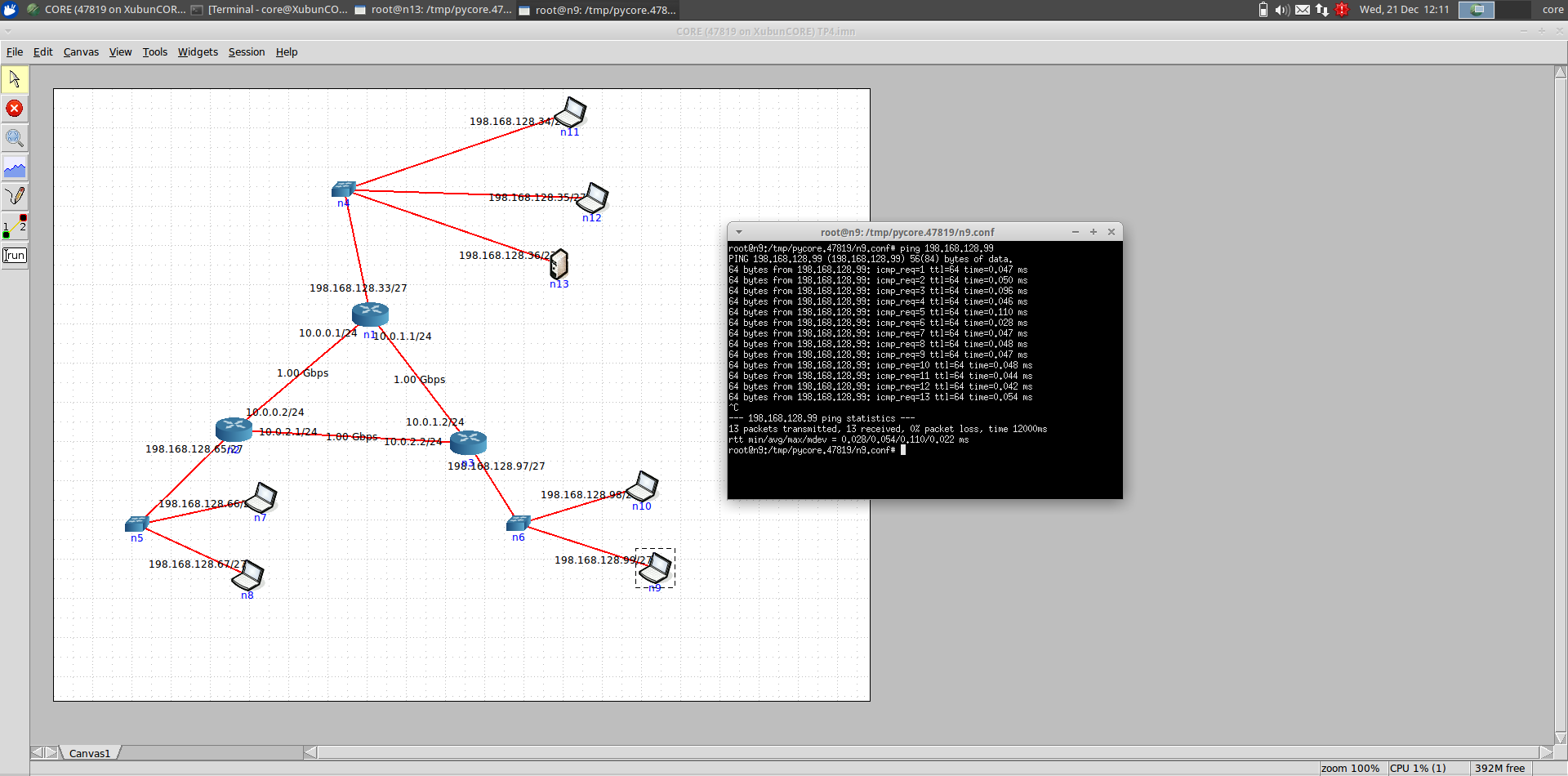
**R:** 5 bits para *hosts* -> 25 = 32. Há dois endereços reservados, logo há 32-2 = 30 endereços possíveis para *hosts.* Assim, é possível interligar 30 *hosts* em cada departamento, assumindo que apenas vamos ligar *hosts*.

1. Garanta que conectividade IP entre as várias redes locais da empresa MIEInet é mantida.

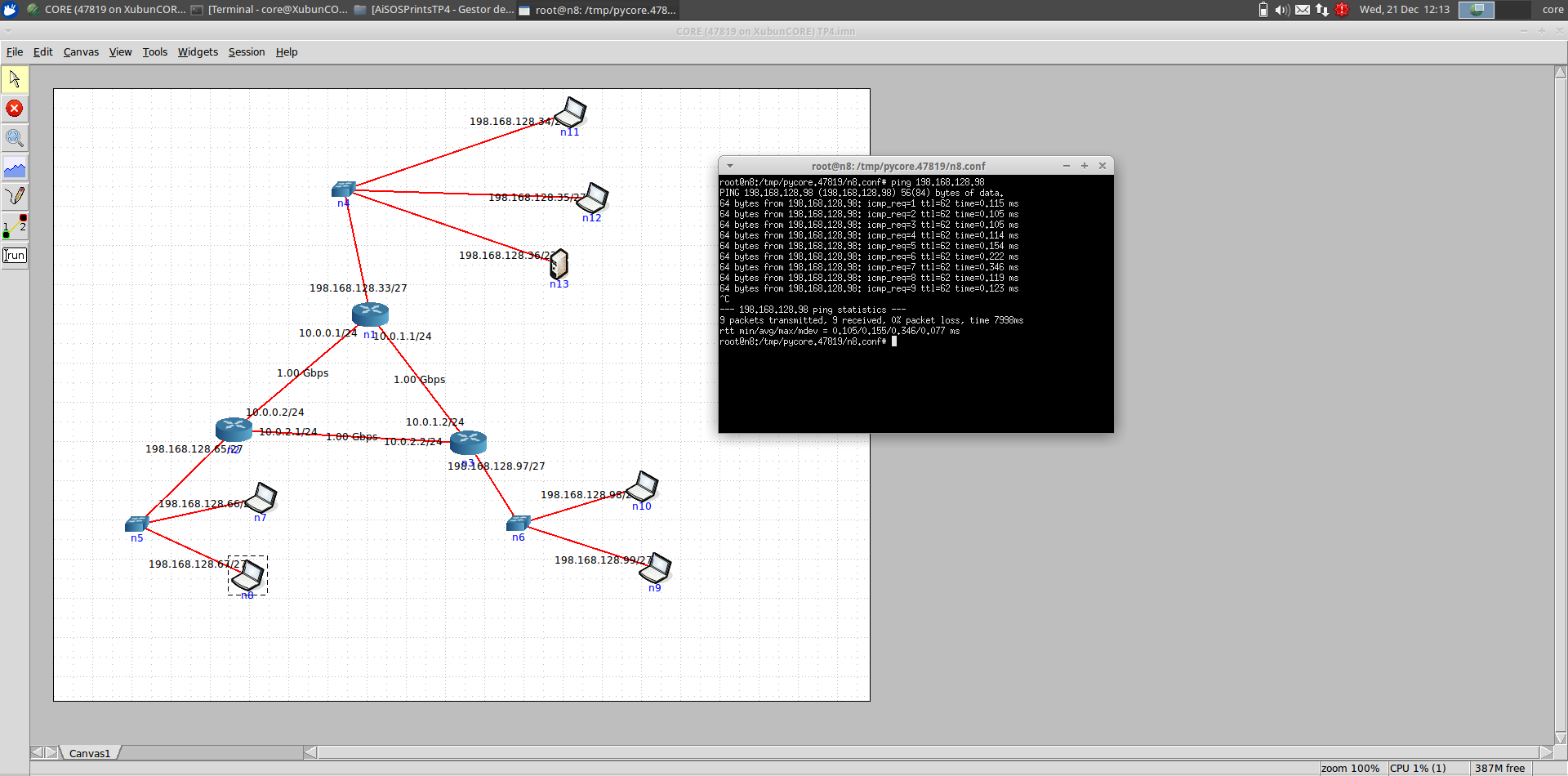
**R:** Como se pode ver nas figuras abaixo, há conetividade entre todas as redes locais da empresa.



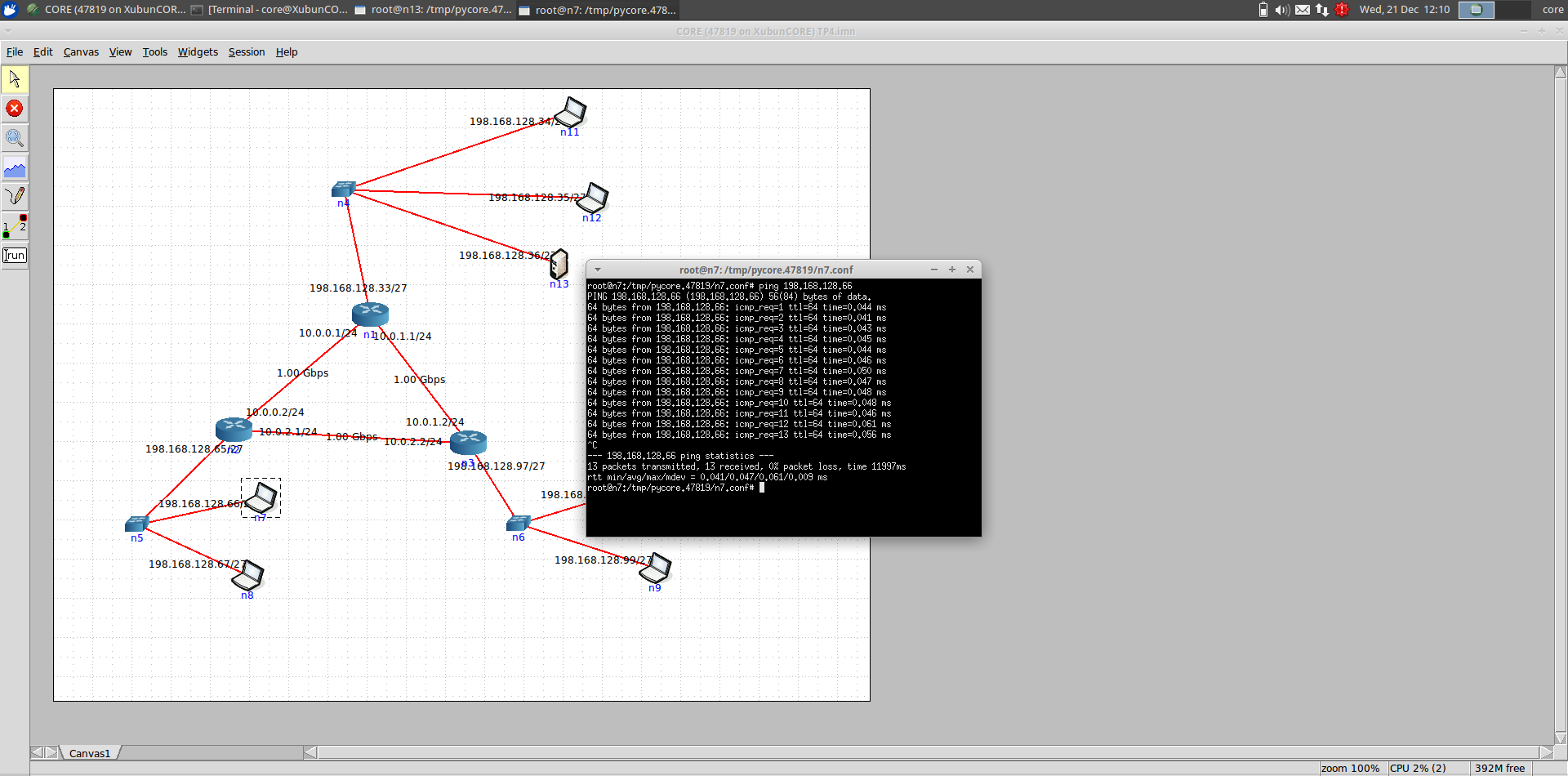
Ping feito dentro da rede do departamento A



Ping feito dentro da rede do departamento A para uma máquina do departamento C



Ping feito dento da rede do departamento B para uma máquina do departamento C



Ping feito dento da rede do departamento A para uma máquina do departamento B