

Relatório 3

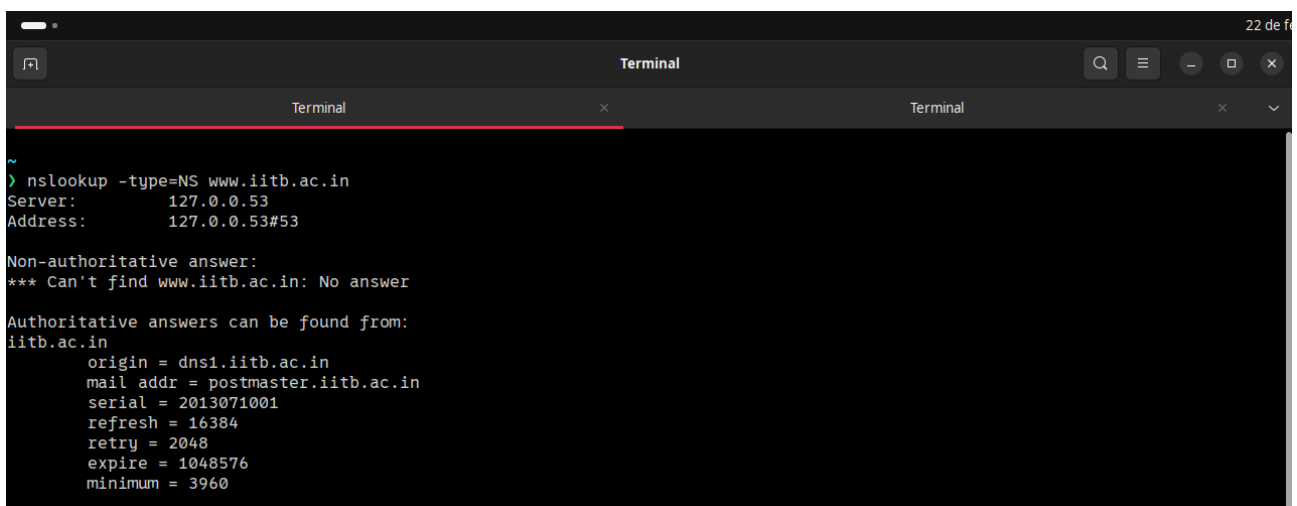
Domain Name System (DNS)



Figura 1: Logo da UFU.

1. Execute o `nslookup` para obter o endereço IP de um servidor Web do Indian Institute of Technology em Bombaim, Índia: `www.iitb.ac.in`. Qual é o endereço IP desse servidor?

Resposta:



```
~  
> nslookup -type=NS www.iitb.ac.in  
Server:      127.0.0.53  
Address:     127.0.0.53#53  
  
Non-authoritative answer:  
*** Can't find www.iitb.ac.in: No answer  
  
Authoritative answers can be found from:  
iitb.ac.in  
    origin = dns1.iitb.ac.in  
    mail addr = postmaster.iitb.ac.in  
    serial = 2013071001  
    refresh = 16384  
    retry = 2048  
    expire = 1048576  
    minimum = 3960
```

Figura 2: `nslookup` para o servidor `www.iitb.ac.in` (Questão 01)

2. Qual é o endereço IP do servidor DNS que forneceu a resposta para o comando `nslookup` da questão 1?

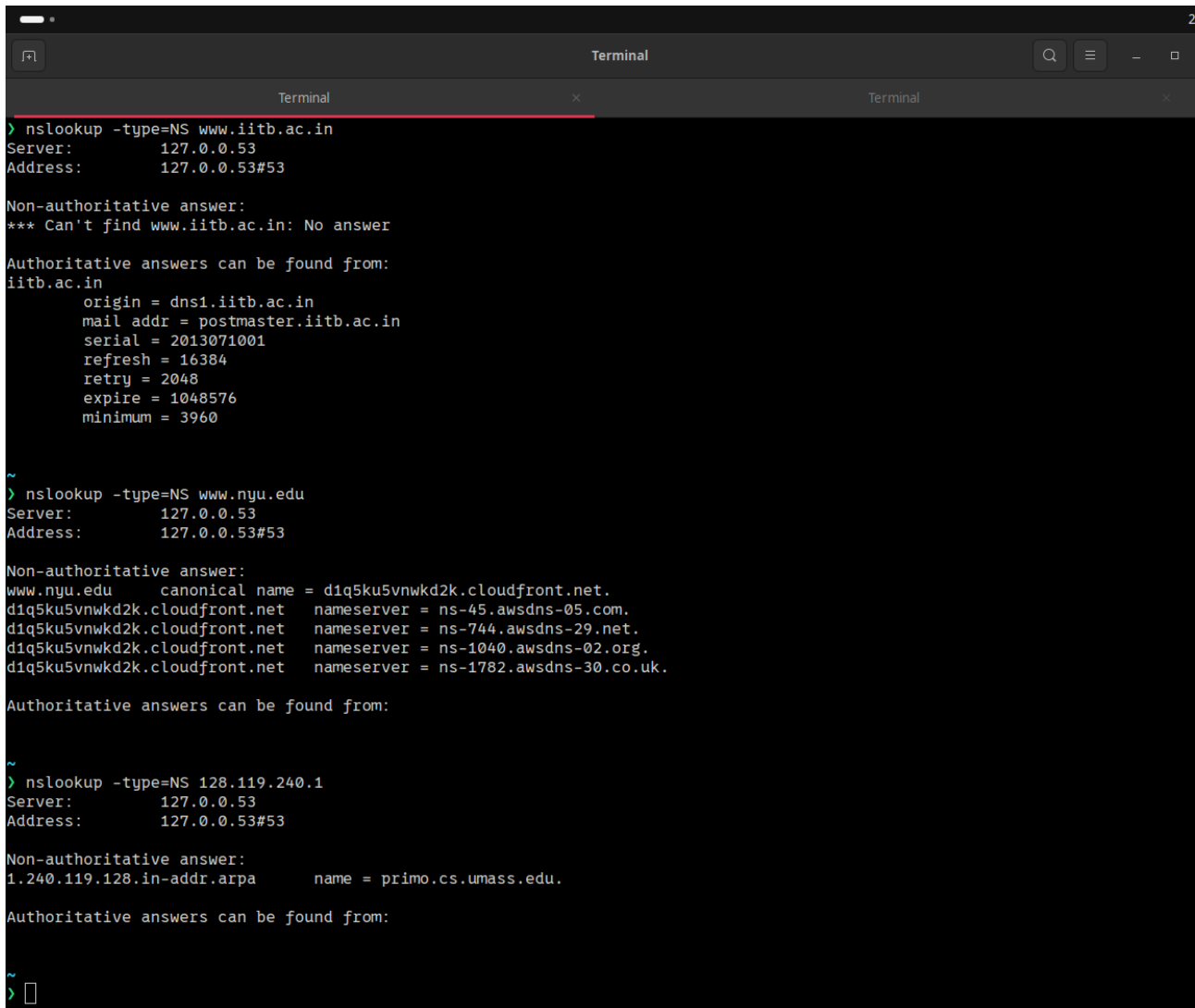
Resposta: O endereço IP do servidor DNS que forneceu a resposta, conforme mostrado na imagem 1 é 127.0.0.53.

3. A resposta do comando `nslookup` da questão 1 foi obtida de um servidor DNS authoritative ou non-authoritative?

Resposta: A resposta do comando `nslookup` da questão 1 foi obtida de um servidor DNS **non-authoritative**.

4. Execute o comando `nslookup` para determinar os servidores DNS autorizados para uma universidade na Europa.

Resposta:



```
> nslookup -type=NS www.iitb.ac.in
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
*** Can't find www.iitb.ac.in: No answer

Authoritative answers can be found from:
iitb.ac.in
    origin = dns1.iitb.ac.in
    mail addr = postmaster.iitb.ac.in
    serial = 2013071001
    refresh = 16384
    retry = 2048
    expire = 1048576
    minimum = 3960

~
> nslookup -type=NS www.nyu.edu
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
www.nyu.edu    canonical name = d1q5ku5vnwkd2k.cloudfront.net.
d1q5ku5vnwkd2k.cloudfront.net    nameserver = ns-45.awsdns-05.com.
d1q5ku5vnwkd2k.cloudfront.net    nameserver = ns-744.awsdns-29.net.
d1q5ku5vnwkd2k.cloudfront.net    nameserver = ns-1040.awsdns-02.org.
d1q5ku5vnwkd2k.cloudfront.net    nameserver = ns-1782.awsdns-30.co.uk.

Authoritative answers can be found from:

~
> nslookup -type=NS 128.119.240.1
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
1.240.119.128.in-addr.arpa    name = primo.cs.umass.edu.

Authoritative answers can be found from:

~
> 
```

Figura 3: `nslookup` para determinar os servidores DNS autorizados (Questão 04)

5. Localize a consulta DNS e as mensagens de resposta. Essas mensagens são enviadas via UDP ou TCP?

Resposta: Via UDP.

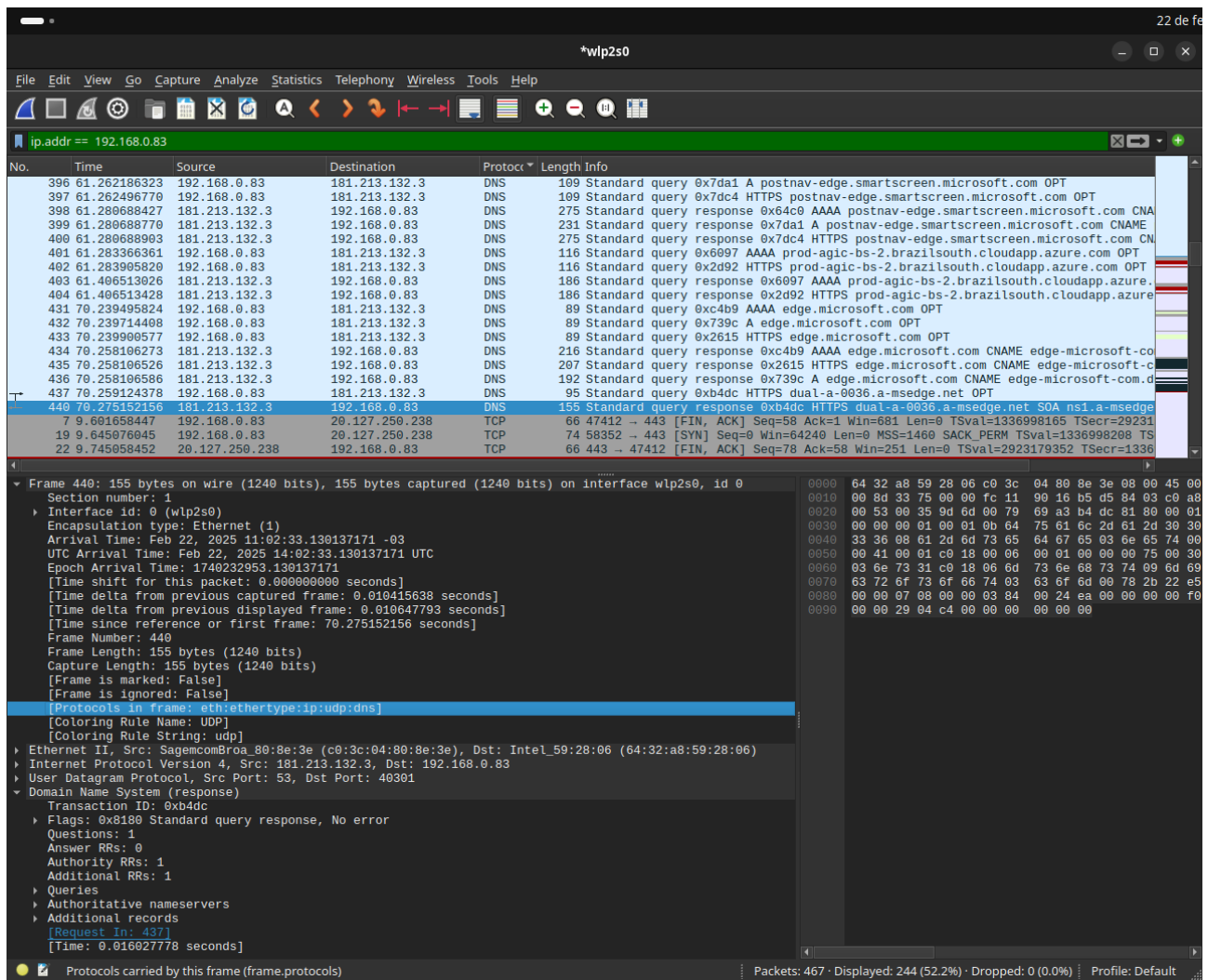


Figura 4: Como as mensagens foram enviadas (Questão 05)

6. Qual é a porta de destino da mensagem de consulta DNS? E qual é a porta de origem da mensagem de resposta DNS?

Resposta: Source Port: 40301 e Destination Port: 53. Agora em Standard Query Response, Source Port: 53 e Destination Port: 40301.

7. Para qual endereço IP é enviada a mensagem de consulta DNS? Utilize o comando `ipconfig` para verificar o endereço IP do seu servidor DNS local. Esses dois endereços IP são iguais?

Resposta:

```
REDES/atividade3 on ~ main [!?]
> sudo resolvectl flush-caches

REDES/atividade3 on ~ main [!?]
> nmcli device show | grep 'IP4.DNS'
IP4.DNS[1]: 181.213.132.2
IP4.DNS[2]: 181.213.132.3

REDES/atividade3 on ~ main [!?]
>

▼ Internet Protocol Version 4, Src: 181.213.132.3, Dst: 192.168.0.83
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 141
    Identification: 0x3375 (13173)
    ▶ 0000 .... = Flags: 0x0
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 252
      Protocol: UDP (17)
      Header Checksum: 0x9016 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 181.213.132.3
      Destination Address: 192.168.0.83
  ▶ User Datagram Protocol, Src Port: 53, Dst Port: 40301
  ▶ Domain Name System (response)
```

Figura 5: Endereço IP do servidor DNS local (Questão 07)

8. Analise a mensagem de consulta DNS: qual é o “tipo” de consulta realizada? A mensagem de consulta contém alguma “resposta”?

Resposta:

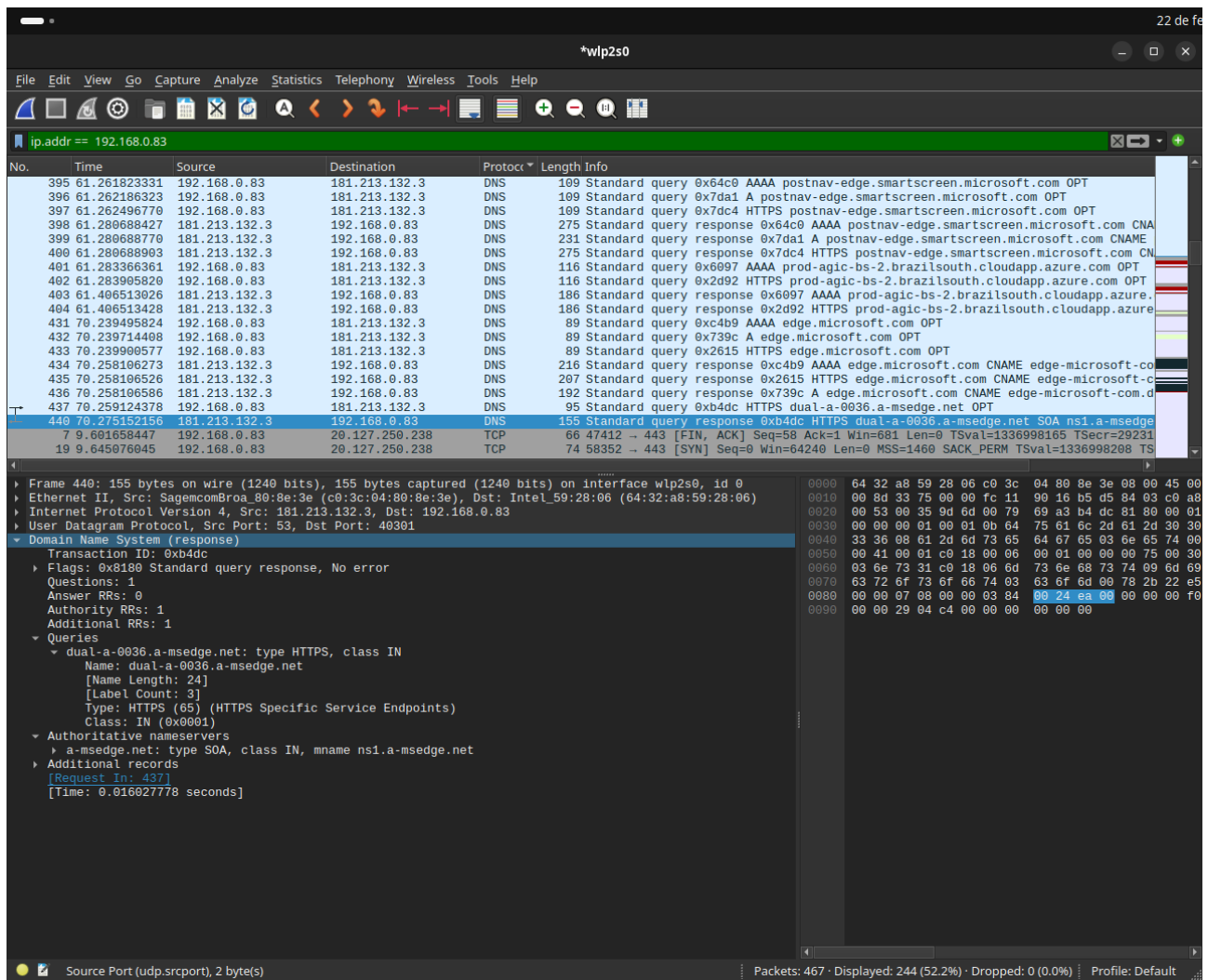


Figura 6: Tipo de consulta realizada (Questão 08)

9. Analise a mensagem de resposta DNS: quantas “respostas” são fornecidas e o que cada uma delas contém?

Resposta: Nenhuma resposta.

10. Considere o pacote TCP SYN subsequente enviado pelo seu host. O endereço IP de destino desse pacote corresponde a algum dos endereços IP apresentados na mensagem de resposta DNS?

Resposta: Não consegui entender muito bem essa.

11. A página base disponível em http://gaia.cs.umass.edu/kurose_ross/ faz referência à imagem http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E_2.jpg, sendo ambas hospedadas em gaia.cs.umass.edu.

- (a) Qual é o número do pacote no rastreamento da solicitação HTTP GET inicial para o arquivo base?

Resposta:

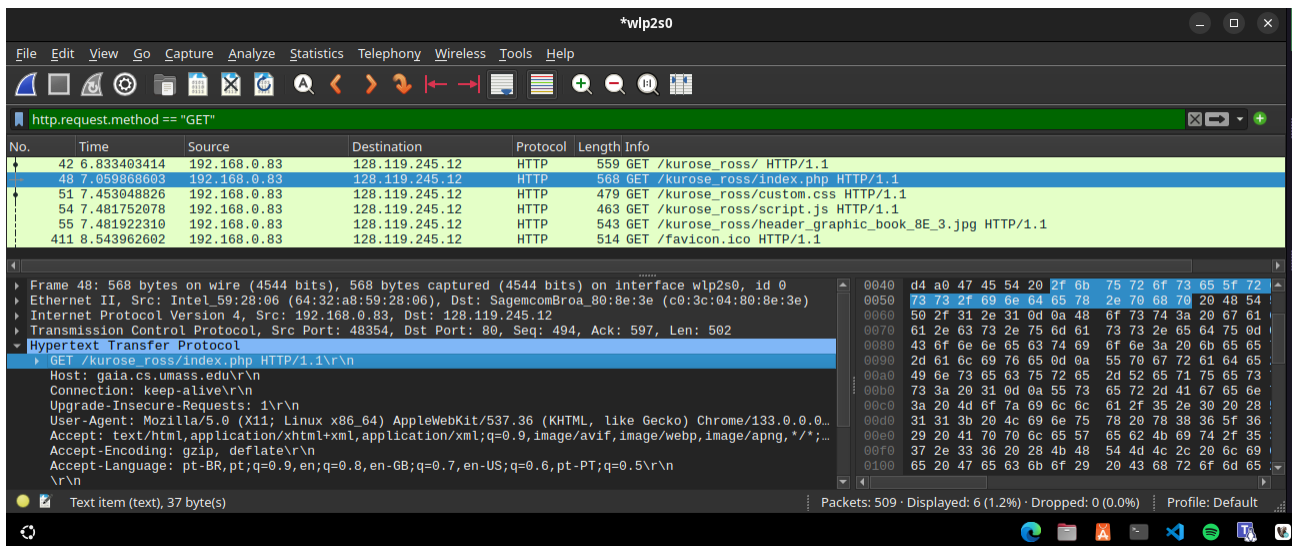


Figura 7: Número do pacote no rastreamento da solicitação HHTP GET inicial (Questão 11 a)

- (b) Qual é o número do pacote no rastreamento da consulta DNS realizada para resolver gaia.cs.umass.edu, permitindo o envio da solicitação HTTP inicial para o endereço IP correspondente?

Resposta: O número do pacote é 11. Conforme mostra a figura 11b.

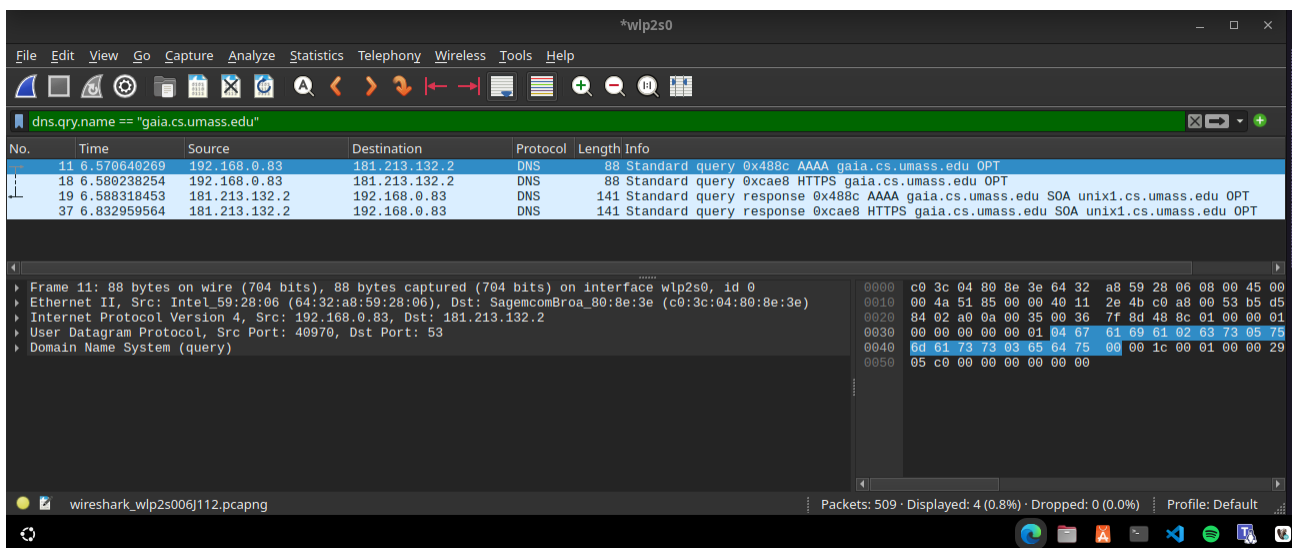


Figura 8: Número do pacote no rastreamento da consulta DNS (Questão 11 b)

- (c) Qual é o número do pacote no rastreamento da resposta DNS recebida?

Resposta: Está no pacote 19 conforme mostra a figura 11b.

- (d) Qual é o número do pacote no rastreamento da solicitação HTTP GET para o objeto de imagem?

Resposta: pacote de numero 55 conforme a imagem abaixo.

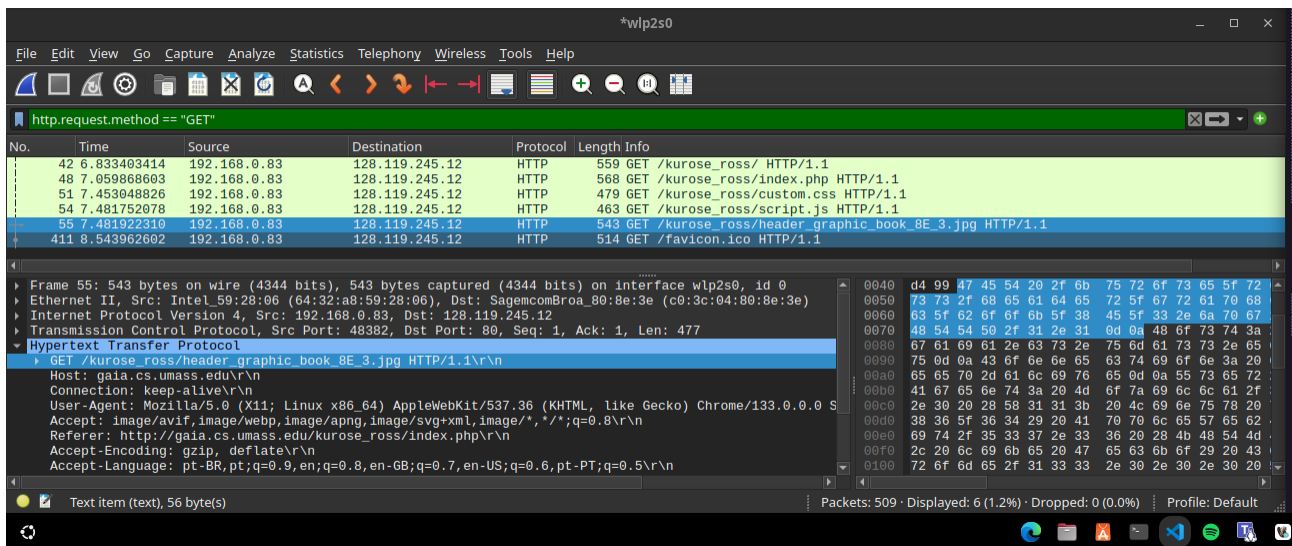


Figura 9: Número do pacote no rastreamento da solicitação HTTP GET para o objeto de imagem (Questão 11 d)

- (e) Qual é o número do pacote referente à consulta DNS efetuada para para resolver gaia.cs.umass.edu para que esta segunda solicitação HTTP possa ser enviada para o endereço IP gaia.cs.umass.edu?

Resposta: pacote de numero 18 conforme a imagem abaixo.

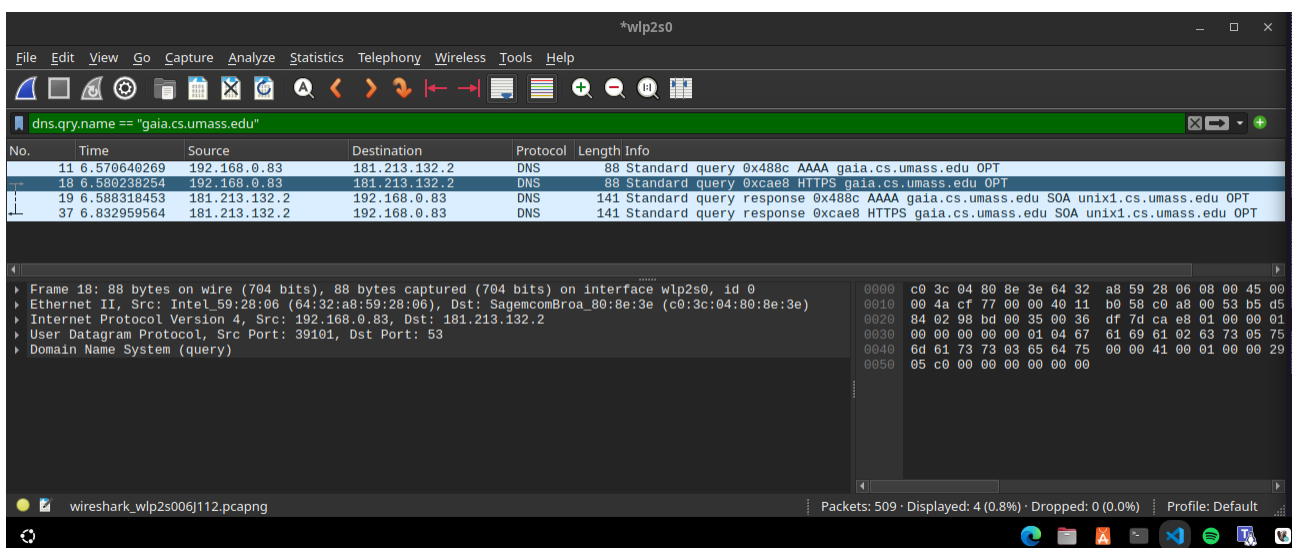


Figura 10: Número do pacote referente à consulta DNS (Questão 11 e)

12. Qual é a porta de destino para a mensagem de consulta DNS? E qual é a porta de origem da mensagem de resposta DNS?

Resposta: porta de destino 53 e porta de origem 53. Conforme mostra a imagem abaixo, usando a porta 19 como exemplo.

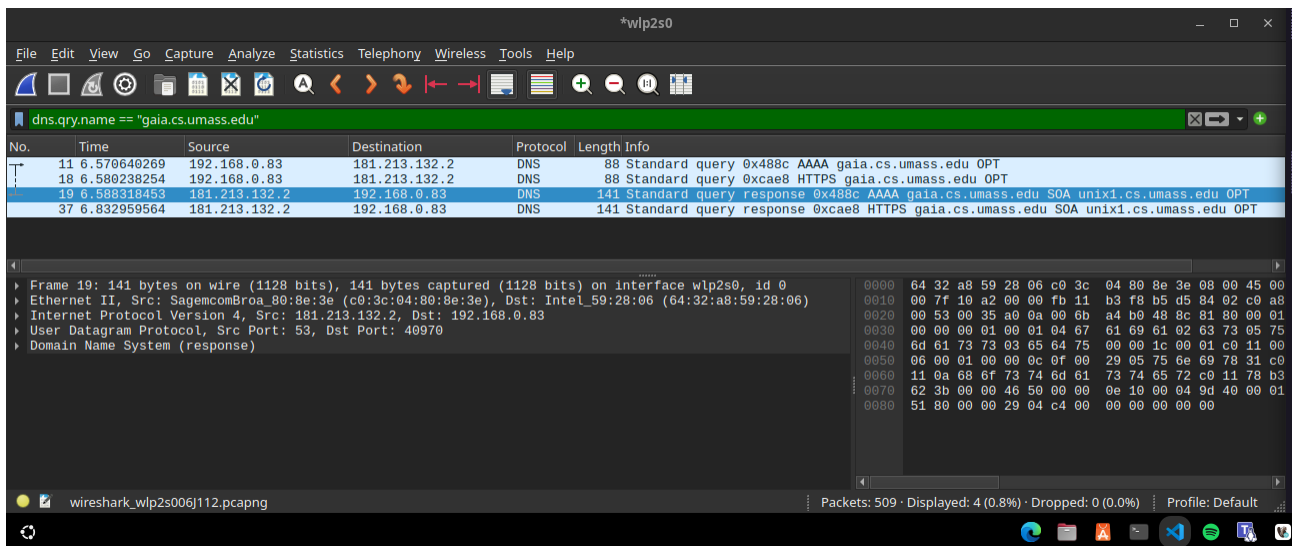


Figura 11: Portas de destino e origem (Questão 12)

13. Para qual endereço IP é enviada a mensagem de consulta DNS? Esse endereço IP corresponde ao do seu servidor DNS local padrão?

Resposta: a consulta DNS foi enviada para o endereço IP 181.213.132.2. Sim, corresponde ao endereço IP do servidor DNS local padrão, veja na imagem abaixo.

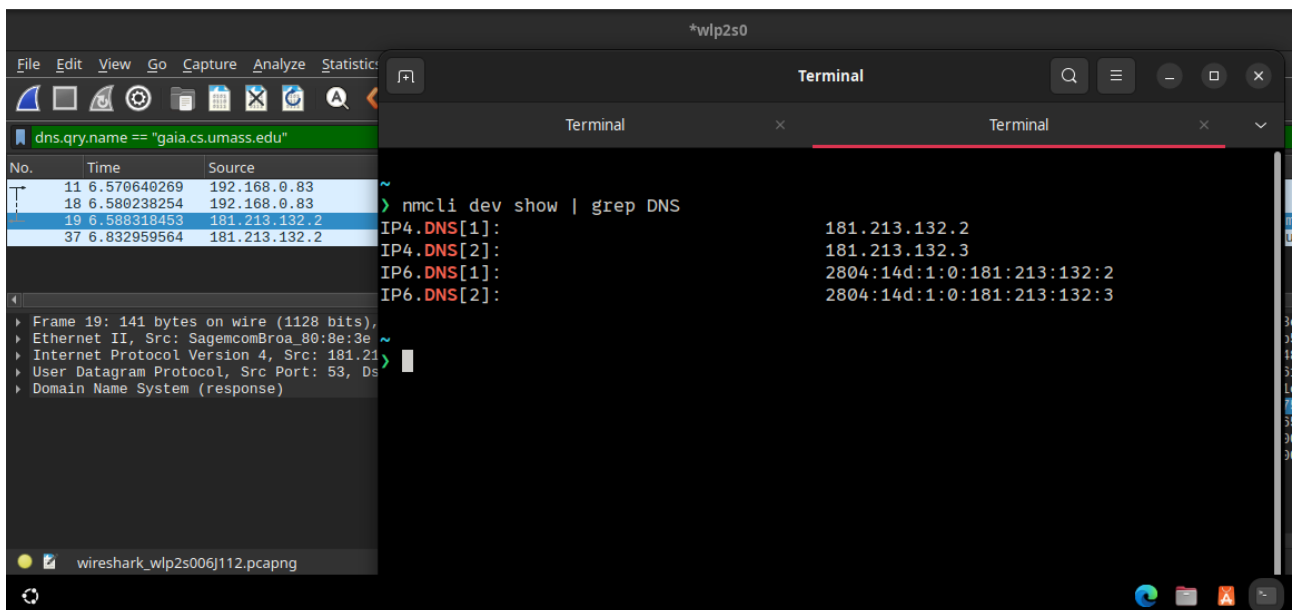


Figura 12: Endereço IP do servidor DNS local padrão (Questão 13)

14. Analise a mensagem de consulta DNS: qual é o “tipo” de consulta efetuada? A mensagem de consulta contém alguma “resposta”?

Resposta: Foi o tipo de query AAAA. Não contém resposta.

15. Analise a mensagem de resposta DNS: quantas “respostas” são fornecidas e o que cada uma delas contém?

Resposta: Contém duas respostas, pacotes 19 e 37. Contém uma resposta para o pacote 11 e outra para o pacote 18, respectivamente.

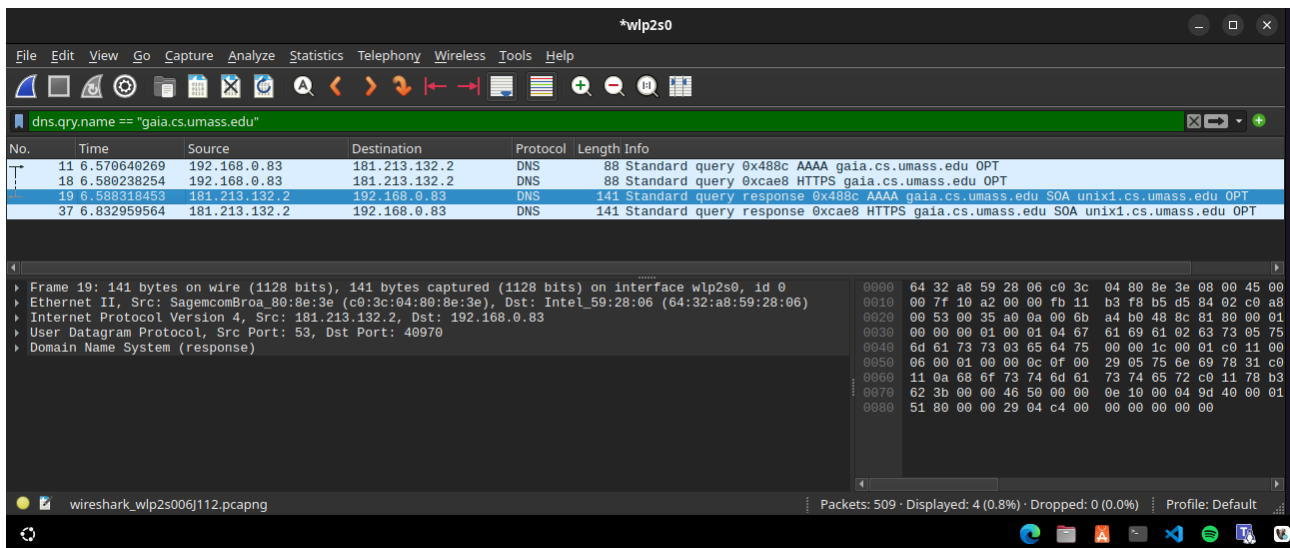


Figura 13: Respostas fornecidas (Questão 15)

16. Para qual endereço IP é enviada a mensagem de consulta DNS? Esse endereço IP corresponde ao do seu servidor DNS local padrão?

Resposta: Já foi respondido na questão 13.

17. Analise novamente a mensagem de consulta DNS: qual é o “tipo” de consulta efetuada? A mensagem de consulta contém alguma “resposta”?

Resposta: Já foi respondido na questão 14.

18. Analise a mensagem de resposta do DNS:

(a) Quantas respostas estão presentes?

Resposta: Duas respostas, conforme o print da questão 15.

(b) Quais informações estão contidas em cada uma dessas respostas?

Resposta: Resposta está na questão 15.

(c) Quantos registros de recursos adicionais foram retornados?

Resposta: Os dois prints abaixo mostram os registros adicionais retornados.

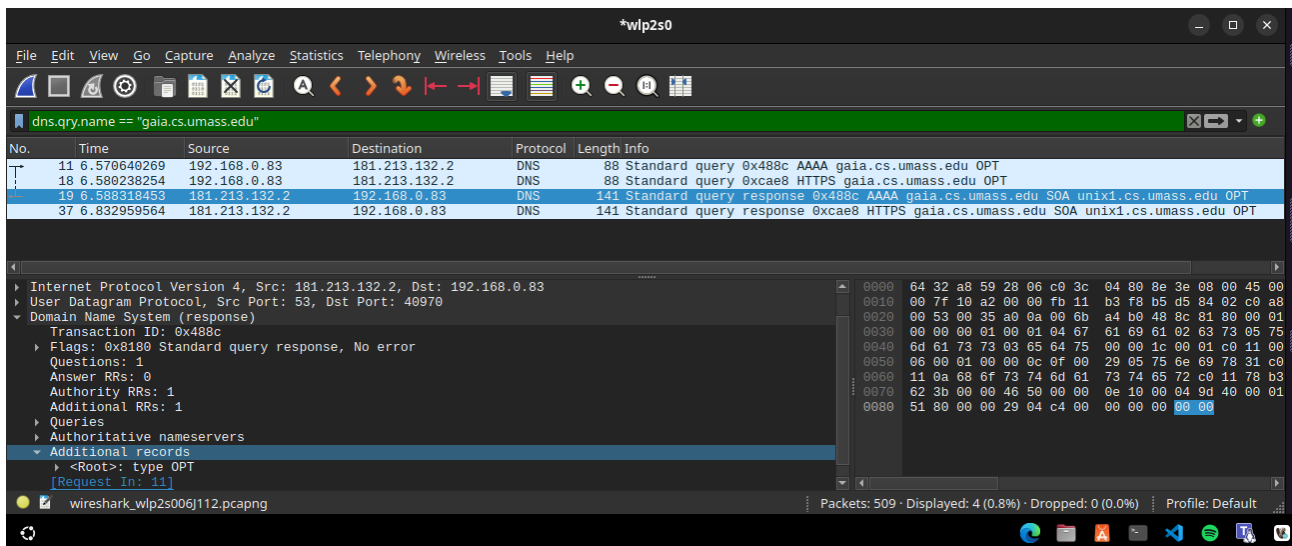


Figura 14: Registros adicionais retornados (Questão 18 c)

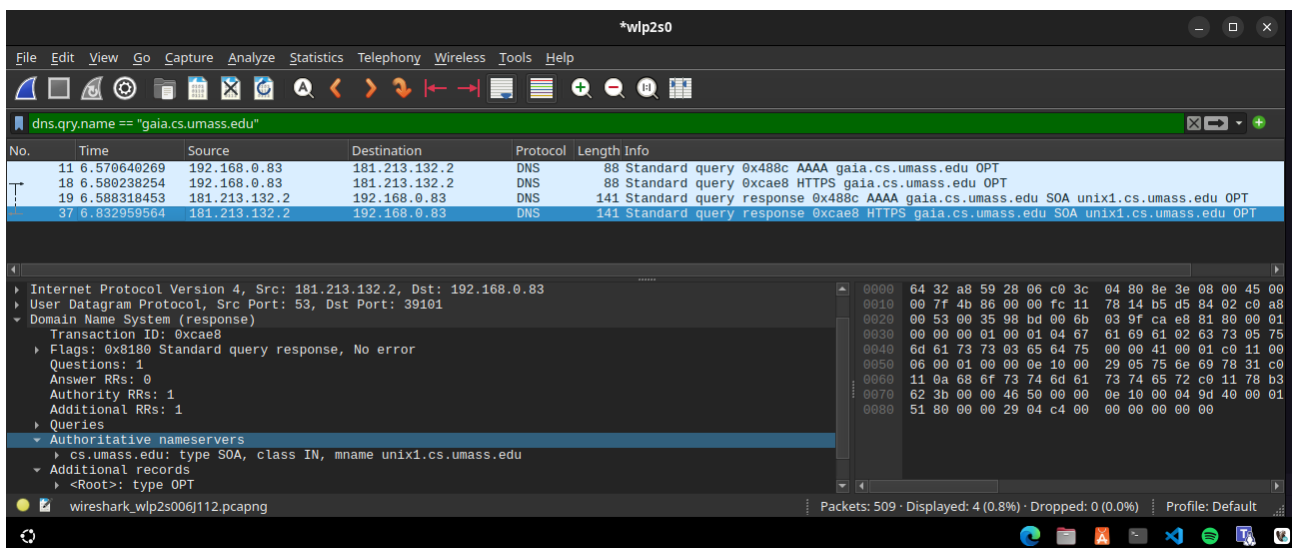


Figura 15: Registros adicionais retornados (Questão 18 c)

(d) Quais informações adicionais estão incluídas nesses registros?

Resposta: <Root>: type OPT.

19. Para qual endereço IP é enviada a mensagem de consulta DNS? Esse é o endereço IP do seu servidor DNS local padrão? Caso contrário, a que endereço IP ele corresponde?

Resposta: Respondido na questão 13. Caso contrário eu não entendi muito bem.

20. Analise a mensagem de consulta DNS: qual é o “tipo” de consulta efetuada? A mensagem de consulta contém alguma “resposta”?

Resposta: Respondido na questão 14.

21. Analise a mensagem de resposta DNS: quantas “respostas” são fornecidas e o que cada uma delas contém?

Resposta: Questão 18 responde aqui também.