Universidade Federal de Uberlândia – UFU
Bacharelado em Sistemas de Informação - Campus Monte Carmelo
GSI524 - Redes de computadores - 2021/1
RENAN JUSTINO REZENDE SILVA - 11921BSI223

Atividade 4
Domain Name System (DNS)

1. **Execute o nslookup para obter o endereço IP de um servidor Web na Ásia. Qual é o endereço IP desse servidor?**

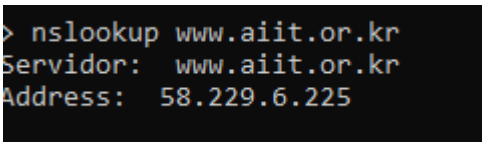
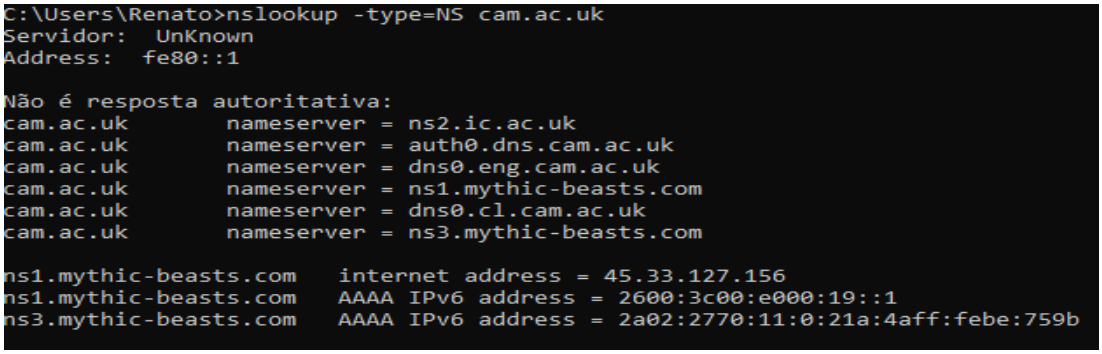
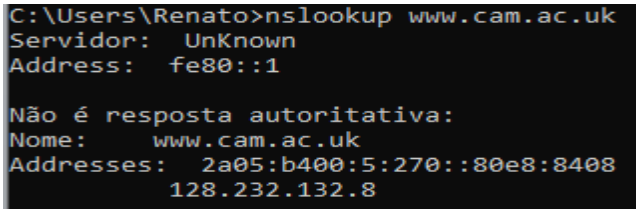


Figura 1: nslookup no servidor do www.aiit.or.kr , Advanced Institute of Information Technology (in Korea).

R = O endereço IP do servidor do Instituto avançado de tecnologia da informação da Coreia é o: 58.229.6.225

2. **Execute o nslookup para determinar os servidores DNS autorizados para uma Universidadena Europa.**





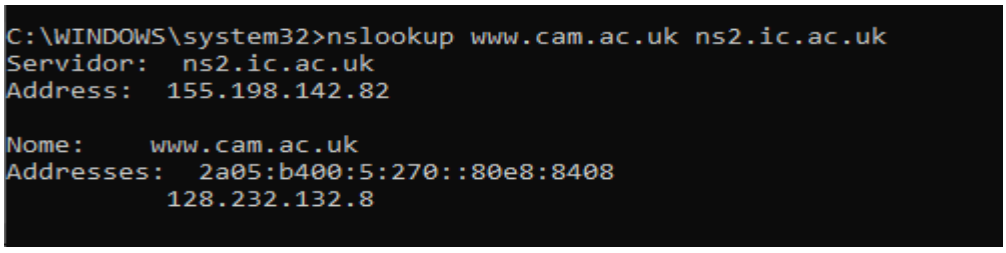


Figura 2: nslookup no servidor da Universidade de Cambridge (cam.ac.uk)

R = Os servidores listados nos prints acima, o dns ns2.ic.ac.uk corresponde ao IP 155.198.142.82, o ns1.mytyc-beasts.com corresponde ao ip 45.33.127.156, dois servidores dns como dns0.eng.cam.ac.uk e dns0.c1.cam.ac.uk, o auth0.dns.cam.ac.uk e os ns1,2 e 3. O endereço IP do servidor do cam.ac.uk é o 128.232.132.8

3. **Execute o nslookup para que um dos servidores DNS obtidos na Pergunta 2 seja consultadopara os servidores de e-mail do Yahoo! Mail. Qual é o endereço IP dele?**

```
C:\WINDOWS\system32>nslookup edge.gypci.b.yahoodns.net ns2.ic.ac.uk
Servidor:   ns2.ic.ac.uk
Address:  155.198.142.82

*** ns2.ic.ac.uk não encontrou edge.gypci.b.yahoodns.net: Query refused
```

```
Server:  BITSY.MIT.EDU
Address:  18.72.0.3

Non-authoritative answer:
Name:    login.yahoo.akadns.net
Address:  216.109.127.60
Aliases:  mail.yahoo.com, login.yahoo.com
```

Figura 3: nslookup no servidor do yahoo

Usando os servidores da questão 2 a query era recusada, mas através de outro servidor foi possível localizar o ip do yahoo mail. O endereço IP do Yahoo mail é o: 216.109.127.60

Para as próximas questões foi feito os passos do wireshark pdf, usado ipconfig /flushdns, foi limpo o cache do navegador, filtrado meu ip no wireshark, iniciado a captura de pacotes e acessado a página http://www.ietf.org como pedido, depois parado a captura e printado os pacotes selecionados.

4. **Localize a consulta DNS e as mensagens de resposta. Em seguida, são enviados por UDP ou TCP?**

No.	Time	Source	Destination	Protocol	Length	Info
1	15:02:31,659141	fe80::3441:6cd8:880…	fe80::1	DNS	94	Standard query 0xa3d9 A www.google.com
2	15:02:31,666116	fe80::1	fe80::3441:6cd8:880…	DNS	110	Standard query response 0xa3d9 A www.google.com A 142.251.129.228
1…	15:02:32,449435	fe80::3441:6cd8:880…	fe80::1	DNS	92	Standard query 0x2d57 A www.ietf.org
1…	15:02:32,456357	fe80::1	fe80::3441:6cd8:880…	DNS	169	Standard query response 0x2d57 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99
4…	15:02:32,861308	fe80::3441:6cd8:880…	fe80::1	DNS	98	Standard query 0x7b8f A analytics.ietf.org
4…	15:02:32,868093	fe80::1	fe80::3441:6cd8:880…	DNS	114	Standard query response 0x7b8f A analytics.ietf.org A 4.31.198.45

```
    Payload Length: 38
    Next Header: UDP (17)
    Hop Limit: 64
    Source Address: fe80::3441:6cd8:8809:54d
    Destination Address: fe80::1
▾ User Datagram Protocol, Src Port: 57294, Dst Port: 53
    Source Port: 57294
    Destination Port: 53
    Length: 38
    Checksum: 0xa48f [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  › [Timestamps]
    UDP payload (30 bytes)
▾ Domain Name System (query)
    Transaction ID: 0x2d57
  › Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
```

```
0010  65 22 00 26 11 40 fe 80  00 00 00 00 00 00 34 41   e".&.@·· ·····4A
0020  6c d8 88 09 05 4d fe 80  00 00 00 00 00 00 00 00   l····M·· ········
0030  00 00 00 00 00 01 df ce  00 35 00 26 a4 8f 2d 57   ········ ·5·&··-W
0040  01 00 00 01 00 00 00 00  00 00 03 77 77 77 04 69   ········ ···www·i
```

Figura 4: Consulta DNS ietf.org

Figura 5: DNS resposta ietf.org

R = Ambos são enviados por UDP.

5. **Qual é a porta de destino para a mensagem de consulta DNS? Qual é a porta de origem da mensagem de resposta DNS?**

   R = De acordo com os prints acima da Figura 5, dá pra localizar que a Destination Port (Porta de Destino) para a mensagem da Consulta DNS é a 53 e a origem é 57294. Já para a mensagem de reposta DNS a porta de origem (Source Port) é a 53 e a porta de destino é a 57294.

6. **Para qual endereço IP a mensagem de consulta DNS é enviada? Use ipconfig para determinar o endereco IP do seu servidor DNS local. Esses dois endereços IP são iguais?**

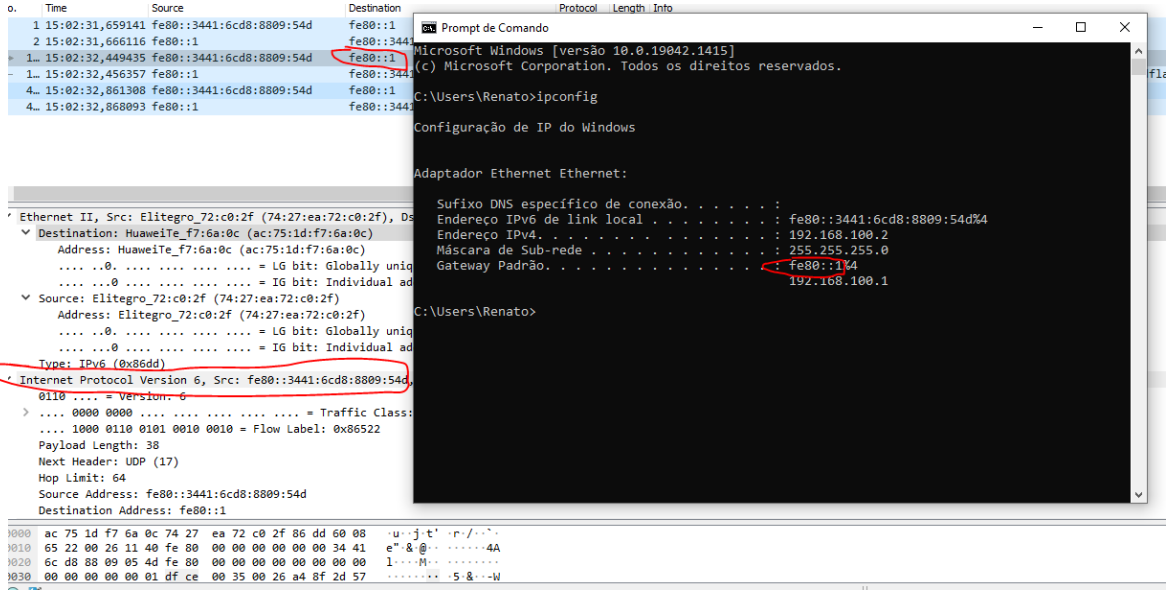


Figura 6: Envio da mensagem consulta DNS

R = Foi enviado para fe80::1 que corresponde ao mesmo de minha rede.

7. **Examine a mensagem de consulta DNS. Qual é o "tipo" de consulta DNS? A mensagem de consulta contém alguma "resposta"?**

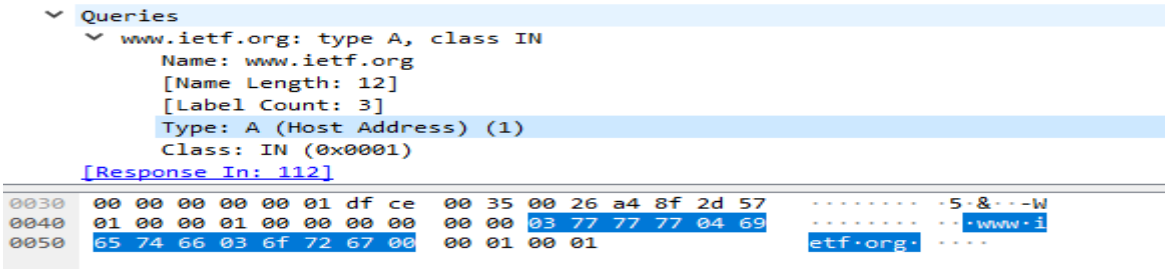


Figura 7: Tipo resposta consulta mensagem DNS

R = O tipo é o “A”, standard query. Não possui a aba de resposta, apenas a de Queries.

8. **Examine a mensagem de resposta DNS. Quantas “respostas” são fornecidas? O que cada uma dessas respostas contém?**

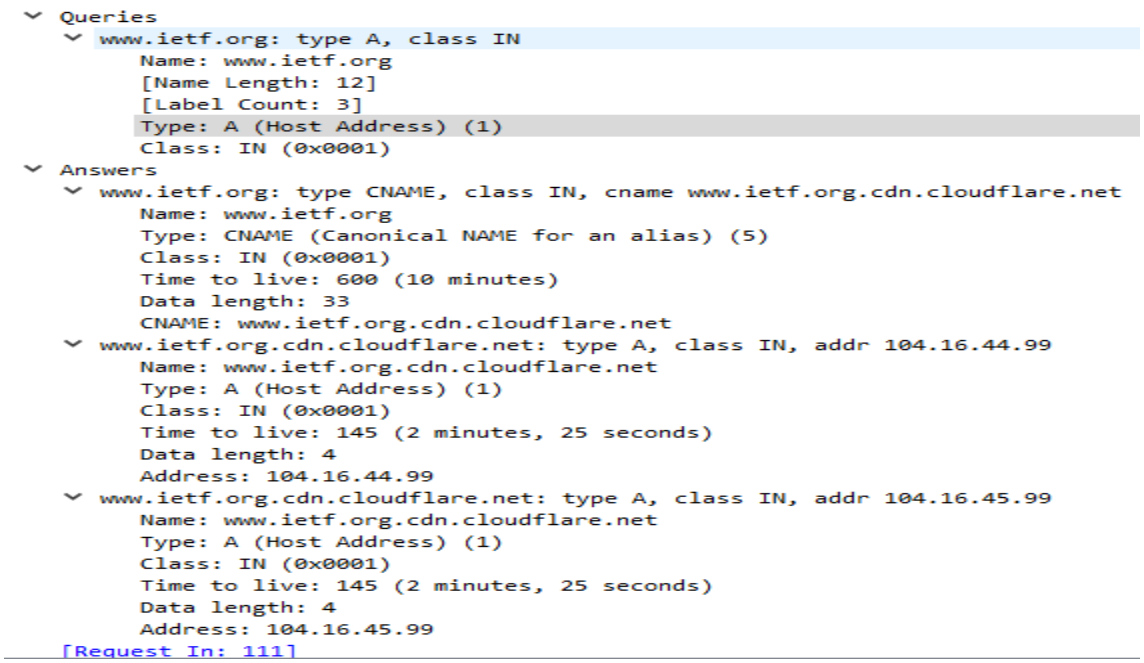


Figura 8: Mensagem de resposta DNS

R = São fornecidas 3 respostas DNS. As respostas contêm o nome do host, tipo de endereço, tamanho de dados, classe, ttl e o endereço.

9. **Considere o pacote TCP SYN subsequente enviado por seu host. O endereço IP de destino do pacote SYN corresponde a algum dos endereços IP fornecidos na mensagem de resposta DNS?**

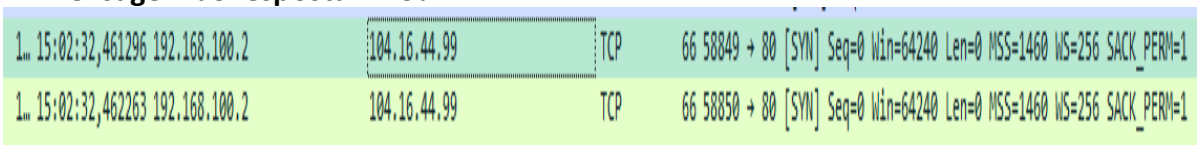


Figura 9: pacote TCP SYN

R = Sim corresponde ao endereço IP 104.16.44.99 da mensagem de resposta DNS que consta na figura 8.

10. **Esta página da web contém imagens. Antes de recuperar cada imagem, seu host emite novas consultas DNS?**
R = Não emite.

Realizado os próximos procedimentos da próxima etapa acessando www.mit.edu com nslookup.

11. **Qual é a porta de destino para a mensagem de consulta DNS? Qual é a porta de origem da mensagem de resposta DNS?**

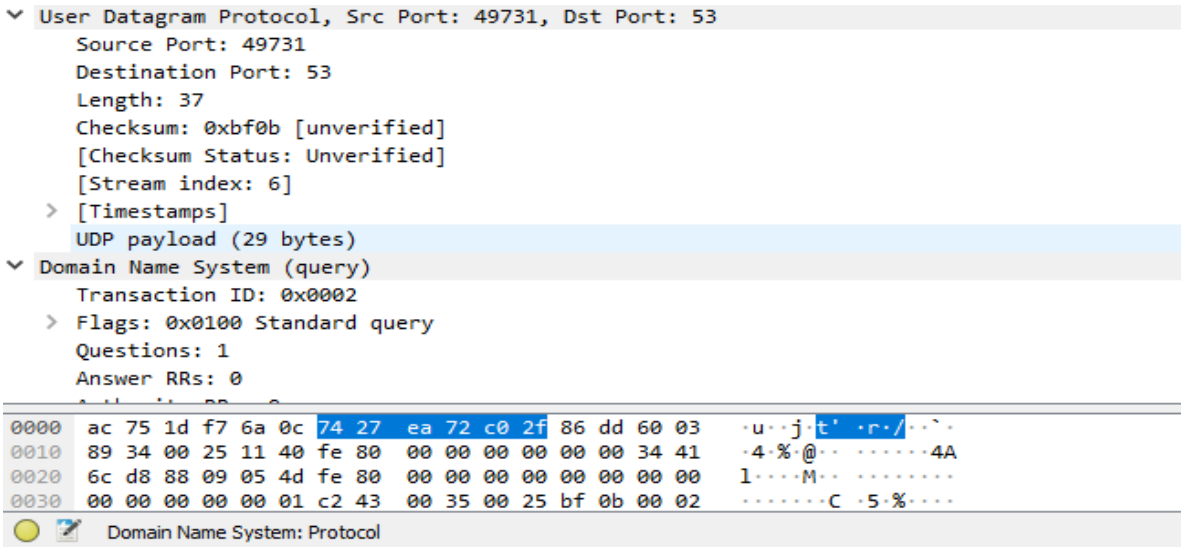


Figura 10: Mensagem consulta DNS www.mit.edu

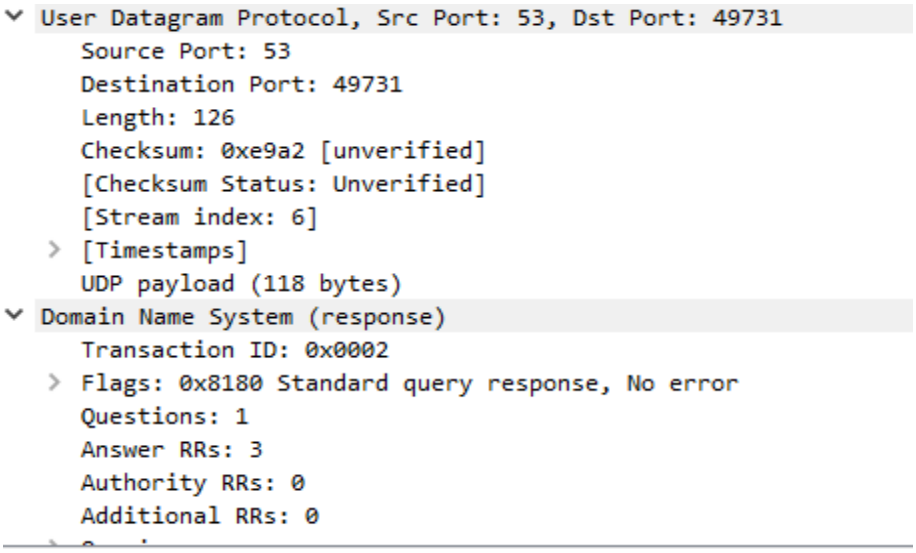


Figura 11: Mensagem resposta DNS www.mit.edu

R = A porta de destino da mensagem de consulta DNS é a 53. A porta de origem da mensagem de resposta DNS é a 53 também.

12. **Para qual endereco IP a mensagem de consulta DNS é enviada? Este é o endereço IP do seu servidor DNS local padrão?**

R = Foi enviada para o mesmo IP do meu servidor usando o ipconfig, assim como na questão 6.

13. **Examine a mensagem de consulta DNS. Qual é o "tipo" de consulta DNS? A mensagem de consulta contém alguma "resposta"?**

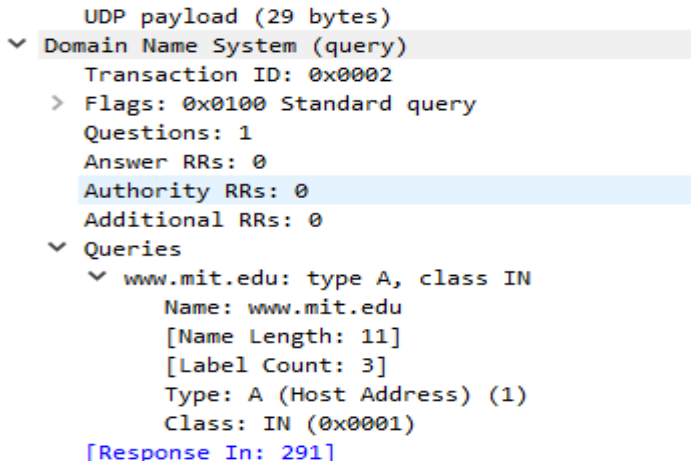


Figura 12: Tipo mensagem consulta DNS www.mit.edu

R = Tipo A de mensagem, standard query, classe IN. Não contém a aba de resposta, só a de queries.

14. **Examine a mensagem de resposta DNS. Quantas "respostas" são fornecidas? O que cada uma dessas respostas contém?**

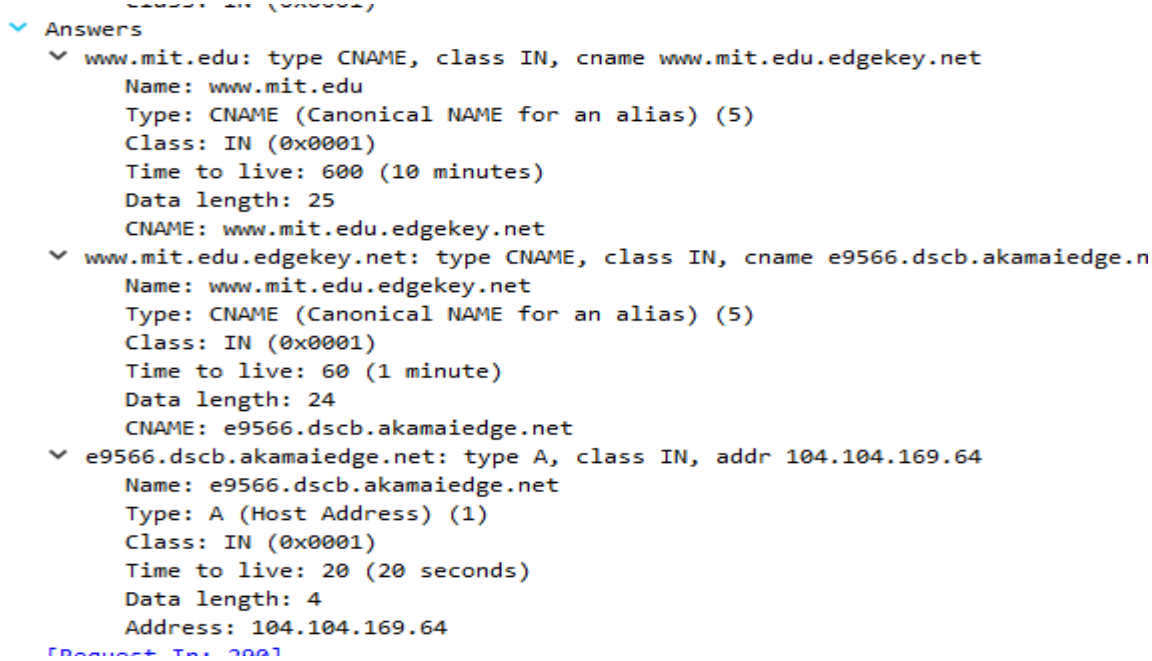


Figura 13: Mensagem resposta DNS www.mit.edu

R = São fornecidas 3 respostas, cada uma contém o nome do host, tipo, classe, ttl, tamanho de dados e o endereço.

15. **Faça uma captura de tela e coloque aqui.**

R = Capturas acima.

Realizado os próximos procedimentos da próxima etapa acessando www.mit.edu com nslookup –type=NS mit.edu

16. **Para qual endereco IP a mensagem de consulta DNS é enviada? Este é o endereço IP do seu servidor DNS local padrão?**

    R = Enviado para o mesmo endereço IP do meu 192.168.100.2 e fe80::1 (endereço de rede gateway)

17. **Examine a mensagem de consulta DNS. Qual é o "tipo" de consulta DNS? A mensagem de consulta contém alguma "resposta"?**

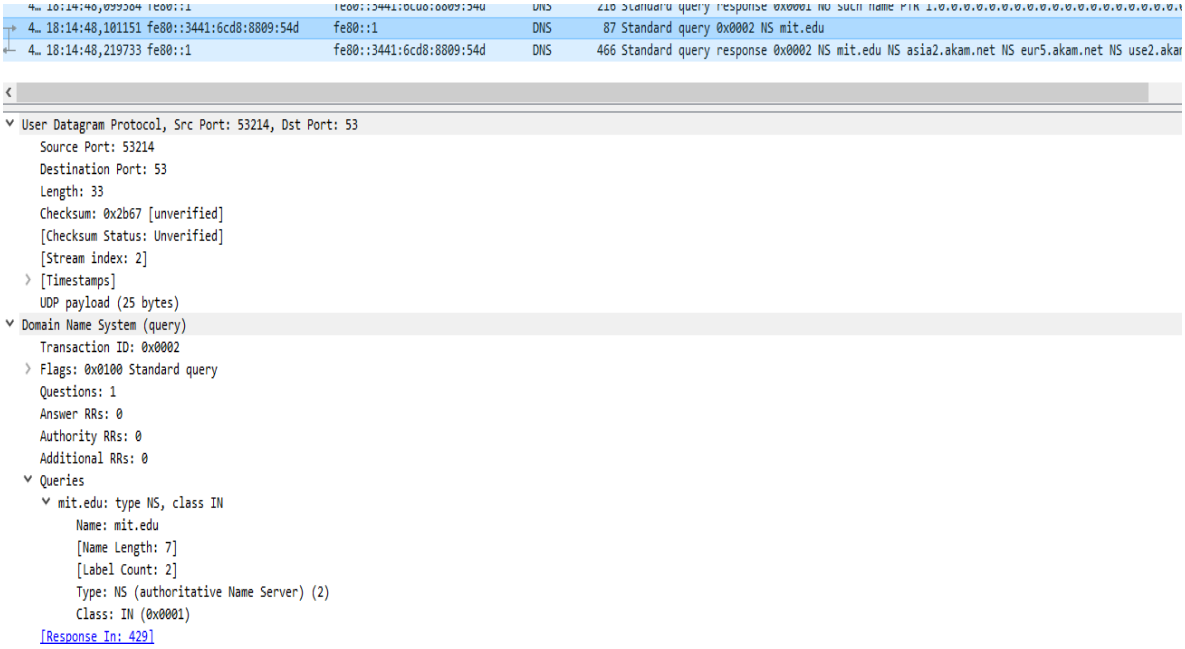


Figura 14: Mensagem consulta DNS nslookup –type=NS mit.edu

R = O tipo da mensagem de consulta é a NS, está escrito type NS, class IN. Não há a aba de resposta nem contém respostas.

18. **Examine a mensagem de resposta DNS. Quais servidores de nomes do MIT a mensagem de resposta fornece? Esta mensagem de resposta também fornece os endereços IP dos nomes do MIT?**

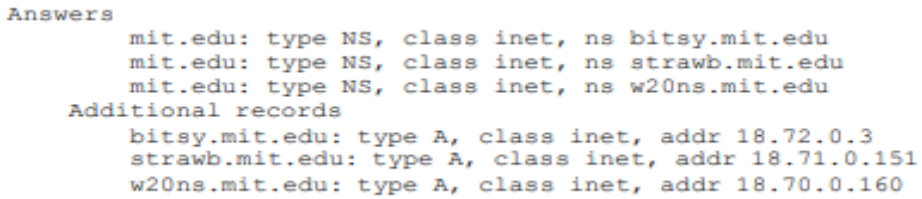


Figura 15: Mensagem resposta DNS nslookup –type=NS mit.edu

R = Mostra os servidores bitsy.mit.edu, strawb.mit.edu e w20ns.mit.edu
Os endereços IPS respectivamente são: 18.72.0.3, 18.71.0.151 e 18.70.0.160

19. **Faça uma captura de tela e coloque aqui.**
    R = Capturas listadas acima.

```
C:\Users\Renato>nslookup www.aiit.or.kr dns.google.com
Servidor:  dns.google
Address:  8.8.8.8

Não é resposta autoritativa:
Nome:    www.aiit.or.kr
Address:  58.229.6.225
```

Figura 16: nslookup www.aiit.or.kr dns.google.com

20. **1. Para qual endereço IP a mensagem de consulta DNS é enviada? Este é o endereço IP do seu servidor DNS local padrão? Se não, a que corresponde o endereço IP?**

    R = Para o endereço de DNS 8.8.8.8, correspondente ao do google.

21. **Examine a mensagem de consulta DNS. Qual é o "tipo" de consulta DNS? A mensagem de consulta contém alguma "resposta"?**

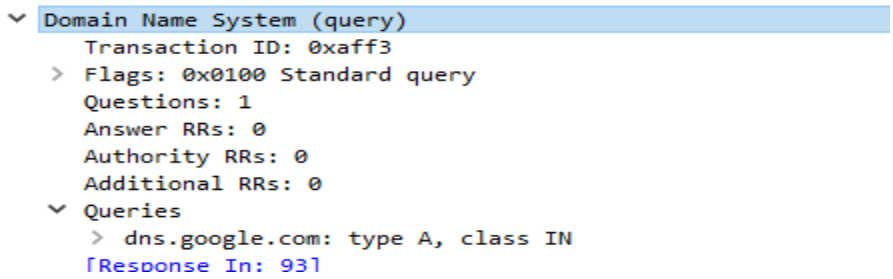


Figura 17: Mensagem consulta dns nslookup www.aiit.or.kr dns.google.com

R = O tipo da mensagem é A. Não contém alguma resposta.

22. **Examine a mensagem de resposta DNS. Quantas "respostas" são fornecidas? O que cada uma dessas respostas contém?**

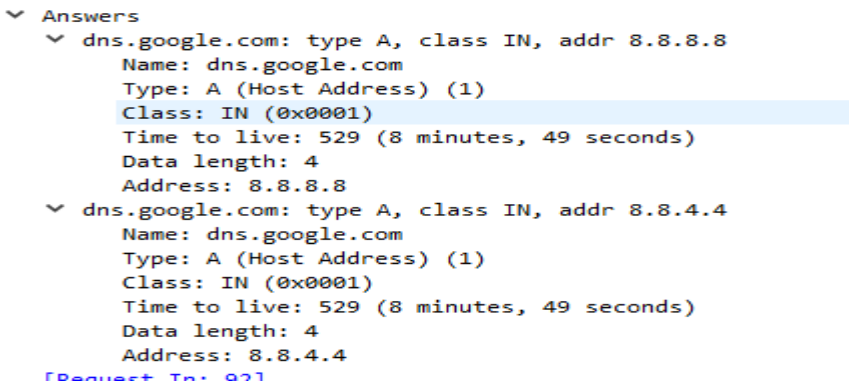


Figura 18: Mensagem resposta dns nslookup www.aiit.or.kr dns.google.com

R = Duas respostas. Contém o nome do host, tipo, classe, endereço, tamanho de dados. Uma o endereço é 8.8.8.8 e o outro servidor dns do Google é o 8.8.4.4

23. **Faça uma captura de tela e coloque aqui.**

    R = Capturas realizadas acima.