

WireShark Lab 03 - DNS v7.0

Igor Augusto Reis Gomes – 12011BSI290 – igor.augusto@ufu.br

Heitor Guimarães Da Fonseca Filho – 12011BSI203 – heitor.filho@ufu.br

1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?

O site <http://www.rediff.com/> tem o servidor localizado na Índia, com o IP: 92.242.140.6.

```
augus> nslookup http://www.rediff.com/
Servidor: dns-primario.ctbctelecom.com.br
Address: 200.225.197.34

Não é resposta autoritativa:
Nome: http://www.rediff.com/
Address: 92.242.140.6

augus> |
```

2. Run nslookup to determine the authoritative DNS servers for a university in Europe

Fiz uma checagem no servidor da Universidade de Oslo, na Noruega:

```
augus> nslookup -type=NS uio.no
Servidor: dns-primario.ctbctelecom.com.br
Address: 200.225.197.34

Não é resposta autoritativa:
uio.no nameserver = nn.uninett.no
uio.no nameserver = ns1.uio.no
uio.no nameserver = ns2.uio.no
uio.no nameserver = server.nordu.net

server.nordu.net internet address = 193.10.252.19
server.nordu.net AAAA IPv6 address = 2001:948:4:2::19
nn.uninett.no internet address = 158.38.0.181
nn.uninett.no AAAA IPv6 address = 2001:700:0:503::aa:5302
augus> |
```

3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

Addresses: 2001:700:100:118::130

129.240.118.130

```
augus> nslookup uio.no server.nordu.net
Servidor: server.nordu.net
Address: 193.10.252.19

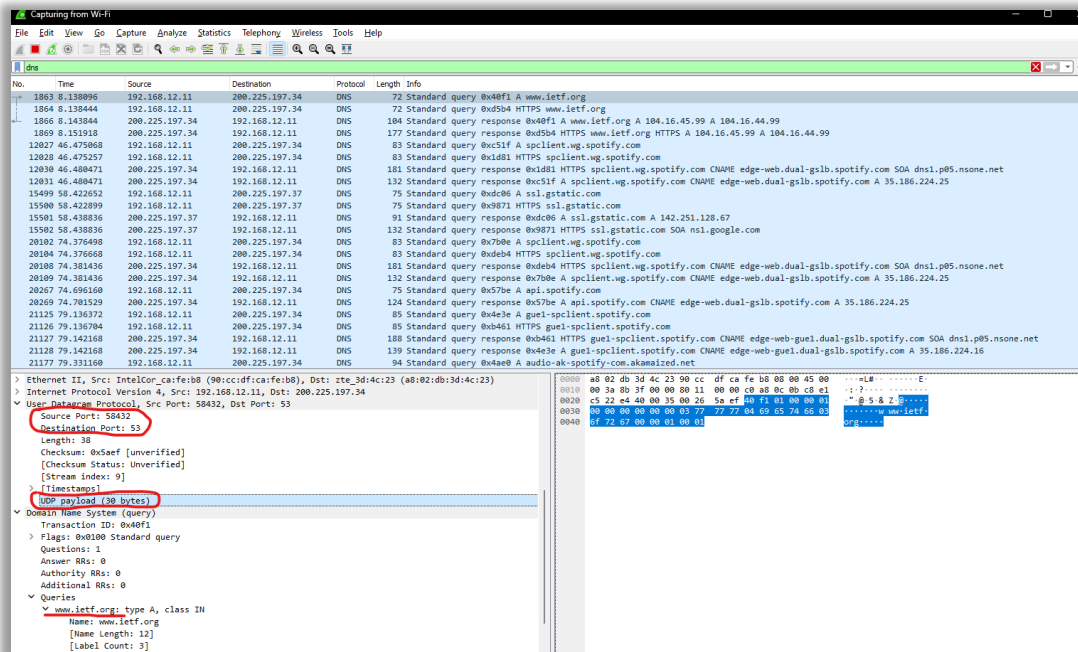
Nome: uio.no
Addresses: 2001:700:100:118::130
129.240.118.130
```

4. Locate the DNS query and response messages. Are then sent over UDP or TCP?

Eles são enviados por UDP, como pode ser visto no print abaixo.

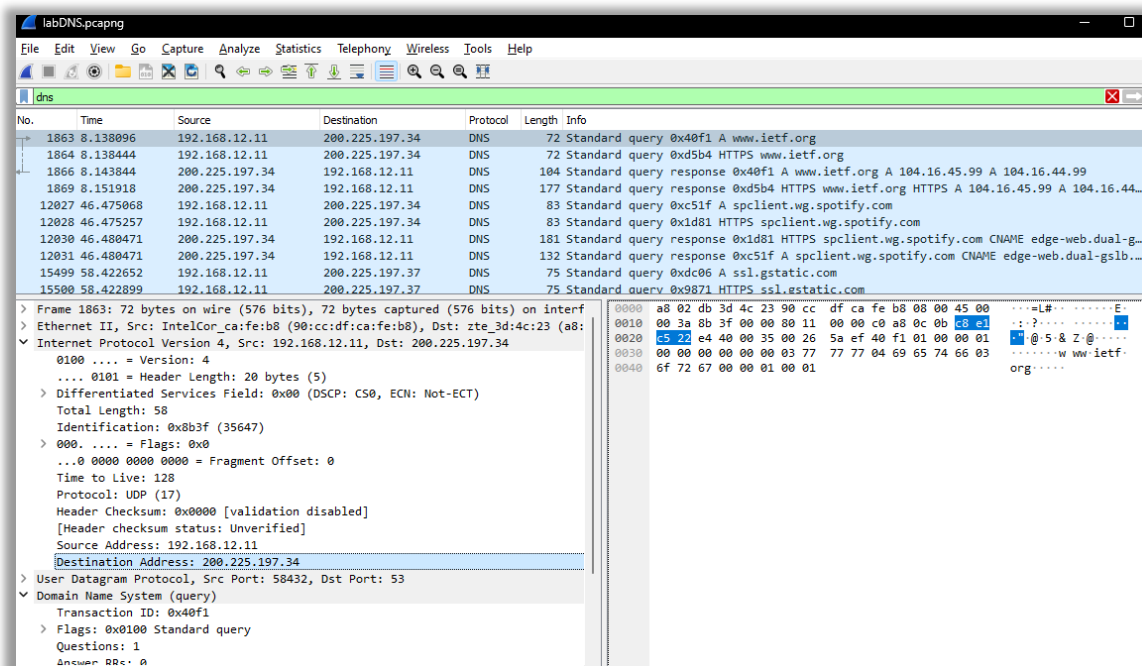
5. What is the destination port for the DNS query message? What is the source port of DNS response message?

A porta destino é 53, e a remetente/fonte é a 58432, como pode ser visto no print abaixo.



6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

A mensagem de consulta DNS é enviada para IP de endereço 200.225.197.34, no qual é o mesmo endereço de IP que aparece ao utilizar o comando *ipconfig /all*, como pode ser visto logo abaixo do *Wireshark*.



Adaptador de Rede sem Fio Wi-Fi:

```
Sufixo DNS específico de conexão. . . . . :
Descrição . . . . . : Intel(R) Wireless-AC 9560
Endereço Físico . . . . . : 90-CC-DF-CA-FE-B8
DHCP Habilitado . . . . . : Sim
Configuração Automática Habilitada. . . . . : Sim
Endereço IPv6 de link local . . . . . : fe80::91da:764c:e3d6:ee99%25(Preferencial)
Endereço IPv4. . . . . : 192.168.12.11(Preferencial)
Máscara de Sub-rede . . . . . : 255.255.255.0
Concessão Obtida. . . . . : domingo, 27 de agosto de 2023 10:45:34
Concessão Expira. . . . . : quarta-feira, 30 de agosto de 2023 17:17:54
Gateway Padrão. . . . . : 192.168.12.1
Servidor DHCP . . . . . : 192.168.12.1
IAID de DHCPv6. . . . . : 177261791
DUID de Cliente DHCPv6. . . . . : 00-01-00-01-28-9E-63-3D-90-CC-DF-CA-FE-B8
Servidores DNS. . . . . : 200.225.197.34 ←
                          200.225.197.37
NetBIOS em Tcpiip. . . . . : Habilitado
augus> |
```

7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Consulta DNS de tipo “A”, não contém nenhuma “resposta” (“answers”), por se tratar de uma operação de request, haveria se fosse uma response (replay).

8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Há duas mensagens nas quais contêm informações do nome do host (name), o tipo (type), a classe (class), o tempo de vida (Time to Live), comprimento dos dados (data length), e o endereço IP (address).

The image shows a Wireshark packet capture of DNS traffic. The packet list pane shows a query (packet 1863) and a response (packet 1864). The packet details pane for packet 1864 shows the response structure, including the domain name system (DNS) response, flags, questions, and answers. The answers section shows two answers for the query: one for www.ietf.org (type A, class IN, address 104.16.45.99) and one for www.ietf.org (type A, class IN, address 104.16.44.99). The packet bytes pane shows the raw data of the response.

9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Sim, o endereço IP de destino do pacote SYN corresponde ao endereço fornecido pelo DNS de resposta, 104.16.45.99.

10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

Não.

11. What is the destination port for the DNS query message? What is the source port of DNS response message?

A porta de destino da requisição DNS é 53:

The image shows a Wireshark packet capture of a DNS query. The packet list shows a standard query from 192.168.12.11 to 200.225.197.34 on port 53. The packet details pane shows the User Datagram Protocol (UDP) and Domain Name System (DNS) sections. The destination port is 53, and the source port is 51036. The DNS section shows a standard query for 'mit.edu'.

No.	Time	Source	Destination	Protocol	Length	Info
133	3.595240	192.168.12.11	200.225.197.34	DNS	87	Standard query 0x0001 PTR 34.197.225.200.in-addr.arpa
134	3.611158	192.168.12.11	140.82.113.26	TCP	55	61691 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1 [TCP segment of...
135	3.613931	200.225.197.34	192.168.12.11	DNS	132	Standard query response 0x0001 PTR 34.197.225.200.in-addr...
136	3.615212	192.168.12.11	200.225.197.34	DNS	67	Standard query 0x0002 A mit.edu
137	3.646500	200.225.197.34	192.168.12.11	DNS	83	Standard query response 0x0002 A mit.edu A 23.74.193.192
138	3.649676	192.168.12.11	200.225.197.34	DNS	67	Standard query 0x0003 AAAA mit.edu

e a porta fonte de resposta é a 53:

The image shows a Wireshark packet capture of a DNS response. The packet list shows a standard query response from 200.225.197.34 to 192.168.12.11 on port 53. The packet details pane shows the User Datagram Protocol (UDP) and Domain Name System (DNS) sections. The destination port is 53, and the source port is 51036. The DNS section shows a standard query response for 'mit.edu'.

No.	Time	Source	Destination	Protocol	Length	Info
136	3.615212	192.168.12.11	200.225.197.34	DNS	67	Standard query 0x0002 A mit.edu
137	3.646500	200.225.197.34	192.168.12.11	DNS	83	Standard query response 0x0002 A mit.edu A 23.74.193.192
138	3.649676	192.168.12.11	200.225.197.34	DNS	67	Standard query 0x0003 AAAA mit.edu
139	3.678942	200.225.197.34	192.168.12.11	DNS	123	Standard query response 0x0003 AAAA mit.edu AAAA 2600:141...
140	3.753183	140.82.113.26	192.168.12.11	TCP	66	443 → 61691 [ACK] Seq=1 Ack=2 Win=70 Len=0 SLE=1 SRE=2
141	4.000642	192.168.12.11	52.226.139.185	TCP	55	59957 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP segment...

12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

É enviada para o IP de endereço 200.225.197.34. Sim, é o endereço IP do meu servidor DNS padrão, como é possível ser visto no print na resposta da questão 6 anteriormente.

13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

É do tipo “A”, não contém nenhuma resposta:

The image shows a Wireshark packet capture of a DNS query. The packet list shows a standard query from 192.168.12.11 to 200.225.197.34 on port 53. The packet details pane shows the User Datagram Protocol (UDP) and Domain Name System (DNS) sections. The destination port is 53, and the source port is 51036. The DNS section shows a standard query for 'mit.edu'.

No.	Time	Source	Destination	Protocol	Length	Info
136	3.615212	192.168.12.11	200.225.197.34	DNS	67	Standard query 0x0002 A mit.edu
137	3.646500	200.225.197.34	192.168.12.11	DNS	83	Standard query response 0x0002 A mit.edu A 23.74.193.192
138	3.649676	192.168.12.11	200.225.197.34	DNS	67	Standard query 0x0003 AAAA mit.edu
139	3.678942	200.225.197.34	192.168.12.11	DNS	123	Standard query response 0x0003 AAAA mit.edu AAAA 2600:141...
140	3.753183	140.82.113.26	192.168.12.11	TCP	66	443 → 61691 [ACK] Seq=1 Ack=2 Win=70 Len=0 SLE=1 SRE=2
141	4.000642	192.168.12.11	52.226.139.185	TCP	55	59957 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP segment...

14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Foi fornecido apenas uma resposta (“answer”), na qual contém o nome do host (name), o tipo (type), a classe (class), o tempo de vida (Time to Live), comprimento dos dados (data length), e o endereço IP (address):

Answers

mit.edu: type A, class IN, addr 23.74.193.192

Name: mit.edu

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 20 (20 seconds)

Data length: 4

Address: 23.74.193.192

15. Provide a screenshot.

No.	Time	Source	Destination	Protocol	Length	Info
136	3.615212	192.168.12.11	200.225.197.34	DNS	67	Standard query 0x0002 A mit.edu
137	3.646500	200.225.197.34	192.168.12.11	DNS	83	Standard query response 0x0002 A mit.edu A 23.74.193.192
138	3.649676	192.168.12.11	200.225.197.34	DNS	67	Standard query 0x0003 AAAA mit.edu
139	3.678942	200.225.197.34	192.168.12.11	DNS	123	Standard query response 0x0003 AAAA mit.edu AAAA 2600:141
140	3.753183	140.82.113.26	192.168.12.11	TCP	66	443 → 61691 [ACK] Seq=1 Ack=2 Win=70 Len=0 SLE=1 SRE=2
141	4.008642	192.168.12.11	52.226.139.185	TCP	55	59957 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP segment

Domain Name System (response)

Transaction ID: 0x0002

> Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

> Queries

> Answers

mit.edu: type A, class IN, addr 23.74.193.192

Name: mit.edu

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 20 (20 seconds)

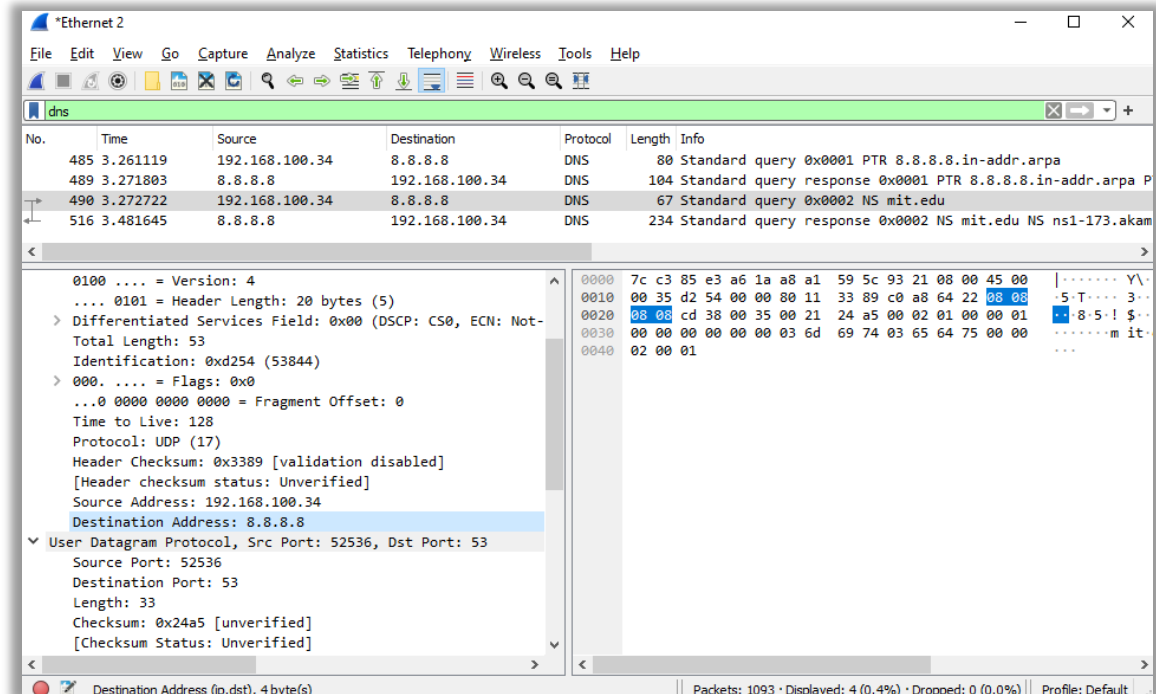
Data length: 4

Address: 23.74.193.192

[Request: Tel: 136]

16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

É enviada para o IP de endereço 200.225.197.34, no qual é o mesmo endereço IP do meu servidor DNS padrão.



```
Adaptador Ethernet Ethernet 2:

Sufixo DNS específico de conexão. . . . . :
Descrição . . . . . : Realtek PCIe GbE Family Controller
Endereço Físico . . . . . : A8-A1-59-5C-93-21
DHCP Habilitado . . . . . : Sim
Configuração Automática Habilitada. . . . : Sim
Endereço IPv6 . . . . . : 2804:1e68:c201:67b:caa6:d13b:9269:8838(Preferencial)
Endereço IPv6 Temporário. . . . . : 2804:1e68:c201:67b:c8b:5dc3:6610:610(Preferencial)
Endereço IPv6 de link local . . . . . : fe80::e96:2573:7d48:3a27%13(Preferencial)
Endereço IPv4. . . . . : 192.168.100.34(Preferencial)
Máscara de Sub-rede . . . . . : 255.255.255.0
Concessão Obtida. . . . . : quarta-feira, 30 de agosto de 2023 15:58:30
Concessão Expira. . . . . : quinta-feira, 31 de agosto de 2023 15:58:29
Gateway Padrão. . . . . : fe80::1%13
                          192.168.100.1
Servidor DHCP . . . . . : 192.168.100.1
IAID de DHCPv6. . . . . : 279486809
DUID de Cliente DHCPv6. . . . . : 00-01-00-01-2A-6B-58-61-D4-5D-64-8F-A5-4C
Servidores DNS. . . . . : 8.8.8.8 ←
                          8.8.4.4
NetBIOS em Tcpip. . . . . : Habilitado
```

17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

É uma consulta DNS do tipo NS (name server), não possuindo nenhuma “answer”.

18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers?

Os nomes de servidores (“nameservers”) do MIT fornecidos na resposta são os fornecidos logo abaixo, sendo que é possível encontrar os endereços de IP no campo de informações adicionais (“Additional records”).

Answers

mit.edu: type NS, class IN, ns ns1-173.akam.net

mit.edu: type NS, class IN, ns use2.akam.net

mit.edu: type NS, class IN, ns use5.akam.net

mit.edu: type NS, class IN, ns asia1.akam.net

mit.edu: type NS, class IN, ns asia2.akam.net

mit.edu: type NS, class IN, ns ns1-37.akam.net

mit.edu: type NS, class IN, ns eur5.akam.net

mit.edu: type NS, class IN, ns usw2.akam.net

Name: mit.edu

Type: NS (authoritative Name Server) (2)

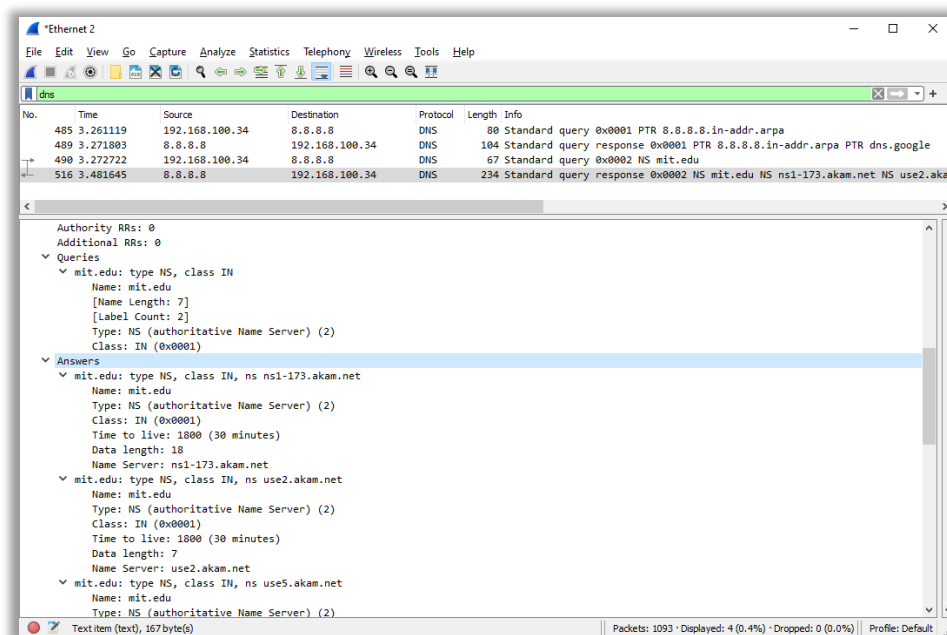
Class: IN (0x0001)

Time to live: 1800 (30 minutes)

Data length: 7

Name Server: usw2.akam.net

19. Provide a screenshot.



20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

A consulta é enviada para 18.72.0.3, sendo que não corresponde ao meu IP do meu servidor DNS local, mas sim do domínio bitsy.mit.edu.

21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Trata-se de uma consulta padrão de tipo A, na qual não contém nenhuma mensagem.

22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

Foi fornecido apenas uma resposta (“answer”), na qual contém:

bitsy.mit.edu: type A, class IN, addr 18.0.72.3

Name: bitsy.mit.edu

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 600 (10 minutes)

Data length: 4

Address: 18.0.72.3

23. Provide a screenshot.

