**WireShark Lab 03 - DNS v7.0**

Igor Augusto Reis Gomes – 12011BSI290 – [igor.augusto@ufu.br](mailto:igor.augusto@ufu.br)

Heitor Guimarães Da Fonseca Filho – 12011BSI203 – [heitor.filho@ufu.br](mailto: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.

Texto

Descrição gerada automaticamente

**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:

Texto

Descrição gerada automaticamente

**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

Texto

Descrição gerada automaticamente

**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. **Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente**

**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.*

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

**Texto

Descrição gerada automaticamente**

**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 contêm 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 lenght), e o endereço IP (address).

**Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente**

**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:  
Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

e a porta fonte de resposta é a 53:

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

**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 contêm nenhuma resposta**:**

**Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente**

**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 contêm o nome do host (name), o tipo (type), a classe (class), o tempo de vida (Time to Live), comprimento dos dados (data lenght), 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.**

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

**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.

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Uma imagem contendo Texto

Descrição gerada automaticamente

**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 abaxixo, 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.**

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

**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 contêm 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 contêm:

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.**

**Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente**