



ENGENHARIA DA COMPUTAÇÃO
REDES DE COMPUTADORES A

ATIVIDADE 5

EQUIPE:

| | |
|--|--------------|
| Agostinho Sanches de Araújo ----- | RA: 16507915 |
| Evandro Douglas Capovilla Junior ----- | RA: 16023905 |
| Lucas Tenani Felix Martins ----- | RA: 16105744 |
| Pedro Andrade Caccavaro ----- | RA: 16124679 |

09/04/2019



SUMÁRIO

| | |
|--------------------|----|
| INTRODUÇÃO..... | 03 |
| OBJETIVO..... | 03 |
| RESULTADOS..... | 03 |
| 1. INTRODUÇÃO..... | 03 |
| 2. HTTP..... | 05 |
| 3. DNS..... | 09 |



INTRODUÇÃO

O Wireshark é um programa que analisa tráfego de redes e os organiza por protocolos em uma interface gráfica interativa com várias informações a possibilidade da utilização de filtros. O nslookup é uma ferramenta utilizada no Windows e no Linux para obter informações sobre o registro de DNS de um IP, host ou domínio, além de retornar o canonical name, que é um alias de um nome de domínio.

OBJETIVO

Aprender sobre o funcionamento de programas e comandos para interceptar respostas de conexão entre um computador e outro, além de identificar *IP'S*, *DNS'S* e *STATUS* da mesma.

RESULTADOS

1. Introdução

1. Liste os diferentes protocolos que aparecem na coluna Protocol na janela de listagem de pacotes após o passo 7;

R: ARP
TCP
TLSv1.2
UDP
SSDP
IGMPv3
DNS

2. Quanto tempo passou de quando a mensagem HTTP GET foi enviada até que a resposta OK foi recebida? (por default, o valor da coluna Time na janela de listagem de pacotes é a quantidade de tempo, em segundos, desde que a captura iniciou). Para exibir o campo Time no formato hora do dia, selecione o menu View, depois Time Display Format, então selecione Time of day.

R: 0,191351966 seg.



3. Qual é o endereço IP do site www.aw.com? Qual é o endereço IP da interface de rede do seu computador?

R: 216.87.148.114
10.0.0.106

4. Imprima as mensagens HTTP GET e a resposta a ela (HTTP/1.1 200 OK). Para fazer isso, selecione Print no menu File, e depois “Selected Packet Only” e “Print as Displayed”. Ok (ou Imprimir) para confirmar.

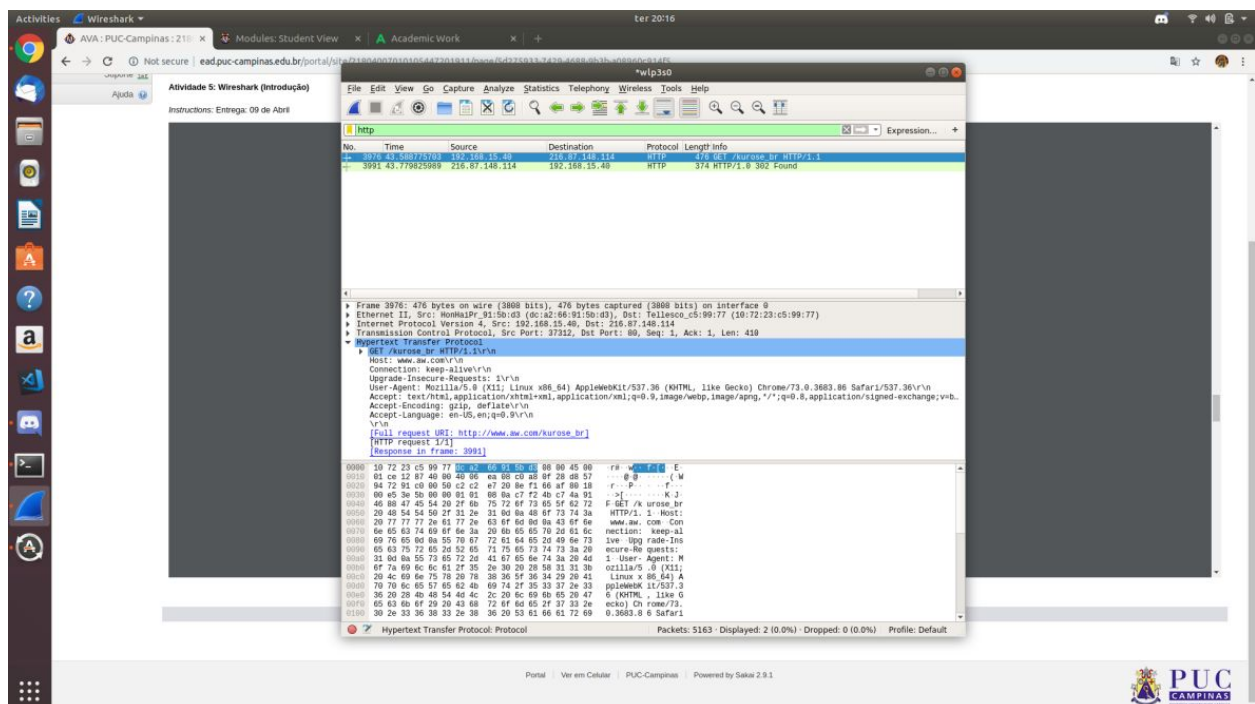
| No. | Time | Source | Destination | Protocol | Length | Info |
|------|--------------------|------------|----------------|----------|--------|----------------|
| 3537 | 18:12:28,759903511 | 10.0.0.106 | 216.87.148.114 | HTTP | 393 | GET /kurose_br |

HTTP/1.1
Frame 3537: 393 bytes on wire (3144 bits), 393 bytes captured (3144 bits) on interface 0
Ethernet II, Src: CompalIn_54:d2:0f (1c:39:47:54:d2:0f), Dst: Tp-LinkT_b9:c4:72 (ac:84:c6:b9:c4:72)
Internet Protocol Version 4, Src: 10.0.0.106, Dst: 216.87.148.114
Transmission Control Protocol, Src Port: 35894, Dst Port: 80, Seq: 1, Ack: 1, Len: 327
Hypertext Transfer Protocol
GET /kurose_br HTTP/1.1\r\n
Host: www.aw.com\r\n
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:66.0) Gecko/20100101 Firefox/66.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
\r\n
[Full request URI: http://www.aw.com/kurose_br]
[HTTP request 1/1]
[Response in frame: 3540]

2. Http

1. O seu navegador executa HTTP 1.0 ou 1.1? Qual a versão de HTTP do servidor?

R: 1.1, ambos.



2. Quais linguagens (se alguma) o seu navegador indica que pode aceitar ao servidor?

R: en-US.

```
Accept: text/html,application/xhtml+xml
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
```

3. Qual o endereço IP do seu computador? E do servidor gaia.cs.umass.edu?

R: 128.119.245.12

10.0.0.106

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|----------------|----------------|----------|--------|--|
| 172 | 2.001667512 | 192.168.15.40 | 128.119.245.12 | HTTP | 623 | GET /ethereal-labs/HTTP-ethereal-file1.html HTTP/1.1 |
| 191 | 2.178137830 | 128.119.245.12 | 192.168.15.40 | HTTP | 305 | HTTP/1.1 304 Not Modified |

4. Qual o código de status retornado do servidor para o seu navegador?

R: 200.

5. Quando o arquivo em HTML que você baixou foi modificado no servidor pela última vez?

R: Dom, 07 de Abril 2019.

Accept-Language: en-US,en;q=0.9\r\n

If-None-Match: "7e-58612a6579a74"\r\n

If-Modified-Since: Tue, 09 Apr 2019 05:59:01 GMT\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file1.html]

[HTTP request 1/1]

[Response in frame: 191]

6. Quantos bytes de conteúdo são retornados ao seu navegador?

R: 126 bytes.

[Request in frame: 3/3]

File Data: 126 bytes

▼ Line-based text data: text/html (4 lines)

<html>\n

Congratulations. You've downloaded the file \n

http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file1.html!\n

</html>\n

7. Inspeccionando os dados na janela de conteúdo do pacote, você vê algum cabeçalho dentro dos dados que não são exibidos na janela de listagem de pacotes? Caso a resposta seja afirmativa, indique um.

R: Sim, ETag: "7e-585ea6aa9092e".

```

Last-Modified: Tue, 09 Apr 2019 05:59:01 GMT\r\n
ETag: "7e-58612a6579a74"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 126\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.165736681 seconds]
[Request in frame: 375]
File Data: 126 bytes
Line-based text data: text/html (4 lines)
<html>\n
Congratulations. You've downloaded the file \n
http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file1.html!\n
</html>\n
100 0a 45 54 61 67 3a 20 22 37 65 2d 35 38 36 31 32 .ETag: "7e-58612
110 61 36 35 37 39 61 37 34 22 0d 0a 41 63 63 65 70 a6579a74 ".Accep
120 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65 73 0d t-Ranges: bytes-
130 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a .Content -Length:
140 20 31 32 36 0d 0a 4b 65 65 70 2d 41 6c 69 76 65 126..Ke ep-Alive
150 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20 6d 61 78 : timeout=5, max
160 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e =100..Co nnection
170 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43 6f : Keep-A live..Co
180 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 ntent-Ty pe: text
190 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 /html; c harset=U
Response line (http.response.line), 26 bytes
Packets: 750 · Displayed: 2 (0.3%) · Dropped: 0 (0.0%)
Profile: Default

```

8. Inspecione o conteúdo da primeira mensagem HTTP GET do seu navegador para o

servidor. Você vê uma linha “IF-MODIFIED-SINCE”?

R: Não.

9. Inspecione o conteúdo da resposta do servidor. O servidor retornou explicitamente o conteúdo do arquivo? Como você pode dizer isso?

R: Sim, pois o tamanho da mensagem e o conteúdo conferem com o que foi lido.

10. Agora inspecione o conteúdo da segunda mensagem HTTP GET do seu navegador para o servidor. Você vê uma linha “IF-MODIFIED-SINCE”? Caso a resposta seja afirmativa, qual informação segue o cabeçalho “IF-MODIFIED-SINCE”?

R: Sim, If-Modified-Since: Sun, 07 Apr 2019 05:59:01 GMT.

11. Qual é o código de status e a frase retornada do servidor na resposta à segunda mensagem HTTP GET? O servidor retornou explicitamente o conteúdo do arquivo? Explique.

R: 304. Não, na verdade o arquivo foi apenas recarregado, pois foi checado que não houve alteração do arquivo já existente.

12. Quantas mensagens HTTP GET foram enviadas pelo seu navegador?

R: 1.

13. Quantos segmentos TCP foram necessários para carregar a resposta?

R: 2.

14. Qual é o código de status e a frase associada com a resposta à mensagem HTTP GET?

R: 200 OK.

| | | | | | | | | |
|------|------------|----------------|---------------|------|-----|----------|--------|-------------|
| 3... | 16.6203... | 128.119.245... | 192.168.15... | HTTP | 607 | HTTP/1.1 | 200 OK | (text/html) |
|------|------------|----------------|---------------|------|-----|----------|--------|-------------|

15. Há alguma linha de status HTTP nos dados transmitidos associados com um “Continuation” TCP?

R: Não.

16. Quantas mensagens HTTP GET foram enviadas pelo seu navegador? Para quais endereços na Internet estas mensagens foram enviadas?

R: 3 GET

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|------------|----------------|----------------|----------|--------|--|
| 2... | 13.0860... | 192.168.15... | 128.119.245.12 | HTTP | 512 | GET /ethereal-labs/HTTP-ethereal-file4.html HTTP/1.1 |
| 2... | 13.2470... | 128.119.245... | 192.168.15.40 | HTTP | 1114 | HTTP/1.1 200 OK (text/html) |
| 2... | 13.6993... | 192.168.15... | 159.182.31.51 | HTTP | 473 | GET /catalog/images/pearson-logo-footer.gif HTTP/1.1 |
| 2... | 13.8400... | 192.168.15... | 128.119.245.12 | HTTP | 457 | GET /~kurose/cover.jpg HTTP/1.1 |
| 2... | 13.8733... | 159.182.31... | 192.168.15.40 | HTTP | 600 | HTTP/1.1 403 Forbidden (text/html) |
| 2... | 14.4905... | 128.119.245... | 192.168.15.40 | HTTP | 2686 | HTTP/1.1 200 OK (JPEG JFIF image) |

17. Você consegue dizer se o seu navegador baixou as duas imagens em seqüência, ou se foram baixadas dos dois locais distintos em paralelo? Explique.

R: Elas não foram baixadas ao mesmo tempo, pois a requisição da imagem 1 foi feita antes, depois a imagem 2 foi requisitada e recebida e, somente depois, a imagem 1 foi recebida.

18. Qual é a resposta do servidor (código de status e frase) para a primeiro mensagem HTTP GET do seu navegador?

R: 401, Unauthorized.

19. Quando o seu navegador envia a mensagem HTTP GET pela segunda vez, qual o novo campo que está incluído na mensagem?

R: Basic ZXRoLXN0dWRLbnRzOm5ldHdvcms=

3. DNS

Sobre a execução nslookup :

1. Obtenha o endereço IP de um servidor web na Ásia;

```
evandro@evandro-capo:~$ nslookup www.aait.or.kr
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   www.aait.or.kr
Address: 58.229.6.225

evandro@evandro-capo:~$
```

R:

2. Determine os servidores DNS autoritários para uma universidade na Europa;

```
evandro@evandro-capo:~$ nslookup -type=NS cam.ac.uk
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
cam.ac.uk       nameserver = ns2.ic.ac.uk.
cam.ac.uk       nameserver = dns0.eng.cam.ac.uk.
cam.ac.uk       nameserver = sns-pb.isc.org.
cam.ac.uk       nameserver = dns0.cl.cam.ac.uk.
cam.ac.uk       nameserver = authdns0.csx.cam.ac.uk.

Authoritative answers can be found from:
```

R:

Sobre rastreamento DNS com Wireshark:

1. Localize as mensagens de solicitação e resposta DNS. Foram enviadas com TCP ou UDP?

R: TCP.

2. Qual é a porta destino para a mensagem de consulta DNS? Qual é a porta fonte da mensagem de resposta DNS?

R: Porta de entrada é 443 e a porta de saída é 56116.

3. A qual endereço IP a mensagem de consulta DNS é enviada? Utilize `ipconfig` para determinar o endereço IP do seu servidor DNS local. Estes endereços são os mesmos?

R: O endereço é o 192.168.15.40. Não.

4. Examine a mensagem de consulta DNS. Qual o campo “type” desta mensagem? A mensagem de consulta contém algum campo “answer”?

R: A (Host Address). 0

5. Examine a mensagem de resposta DNS. Quantos campos com “answer” existem? O que há em cada uma destas mensagens?

R: 1.

▼ Answers

▼ ietf.org: type A, class IN, addr 4.31.198.44

Name: ietf.org

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 300

Data length: 4

Address: 4.31.198.44

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

R: Sim.

7. A página web visitada contém imagens. Antes de recuperar cada imagem, o host realiza novas consultas DNS?

R: Não.

Sobre o comando `nslookup www.mit.edu` :

1. Qual é a porta destino para a mensagem de consulta DNS? Qual é a porta fonte para a mensagem de resposta DNS?

R: Porta destino 53, porta fonte 42848.

2. A qual endereço IP a mensagem de consulta DNS está endereçada? Este endereço é o de algum dos seus servidores DNS locais?

R: 192.168.15.1, sim.

3. Examine a mensagem de consulta DNS. Qual o campo “type” que há nela? A mensagem de consulta contém algum campo “answer”?

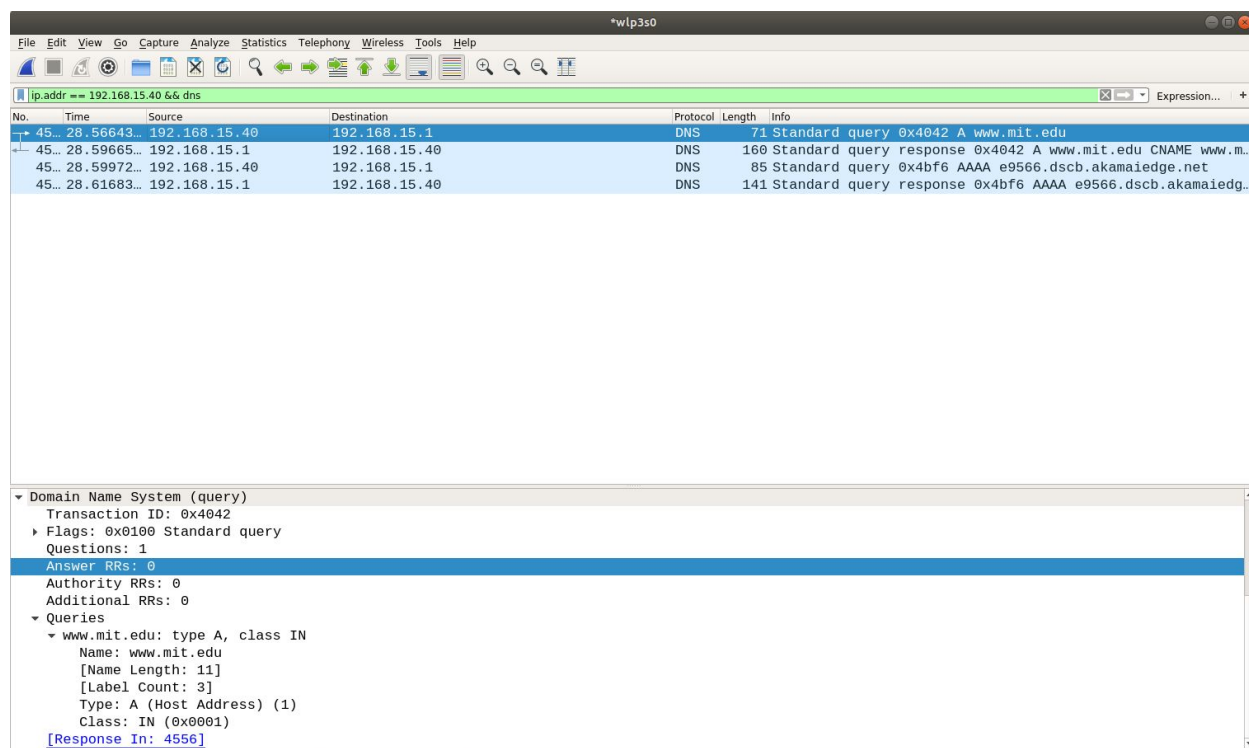
R: A (host address). 0

4. Examine a mensagem de resposta DNS. Quantos campos com “answer” existem? 0 que há em cada uma destas respostas?

R: 3.

5. Grave a tela de captura de pacotes.

R:



Sobre o comando `nslookup -type=NS mit.edu` :

1. A qual endereço IP a mensagem de consulta DNS está endereçada? Este endereço é o de algum dos seus servidores DNS locais?

R: 192.168.15.1, sim.

2. Examine a mensagem de consulta DNS. Qual o campo “type” que há nela? A mensagem de consulta contém algum campo “answer”?

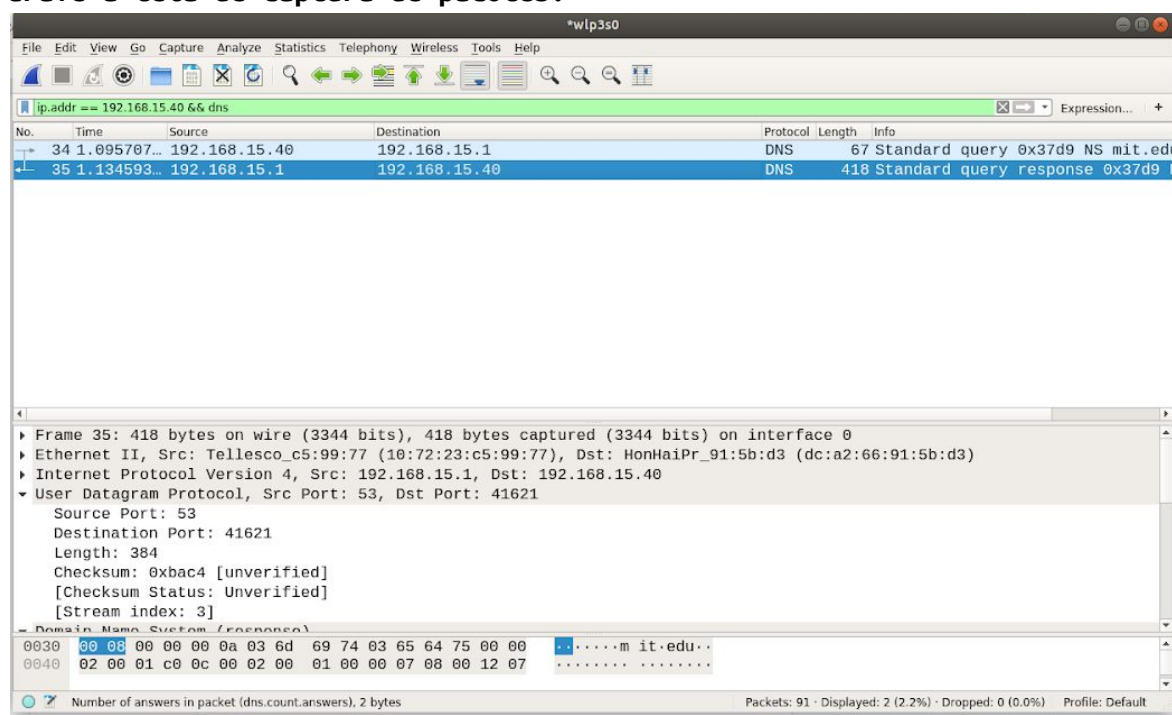
R: NS (authoritative Name Server).

3. Examine a mensagem de resposta DNS. Quais servidores DNS do MIT são fornecidos na resposta? Esta mensagem de resposta também fornece os endereços IP dos servidores DNS do MIT?

- ▶ mit.edu: type NS, class IN, ns ns1-173.akam.net
- ▶ mit.edu: type NS, class IN, ns use5.akam.net
- ▶ mit.edu: type NS, class IN, ns eur5.akam.net
- ▶ mit.edu: type NS, class IN, ns usw2.akam.net
- ▶ mit.edu: type NS, class IN, ns asia1.akam.net
- ▶ mit.edu: type NS, class IN, ns ns1-37.akam.net
- ▶ mit.edu: type NS, class IN, ns use2.akam.net
- ▶ mit.edu: type NS, class IN, ns asia2.akam.net

R:

4. Grave a tela de captura de pacotes.



R:

Sobre o comando `nslookup www.aiit.or.kr bitsy.mit.edu` :

1. A qual endereço IP a mensagem de consulta DNS está endereçada? Este endereço é o de algum dos seus servidores DNS locais? Caso contrário, qual o host para este endereço IP?

R: 192.168.15.1

2. Examine a mensagem de consulta DNS. Qual o campo “type” que há nela? A mensagem de consulta contém algum campo “answer”?

R: A (HOST ADDRESS). 0

3. Examine a mensagem de resposta DNS. Quantos campos com “answer” existem? 0 que há em cada uma destas respostas?

R: 1.

▼ Answers

▼ bitsy.mit.edu: type A, class IN, addr 18.72.0.3

Name: bitsy.mit.edu

Type: A (Host Address) (1)

Class: IN (0x0001)

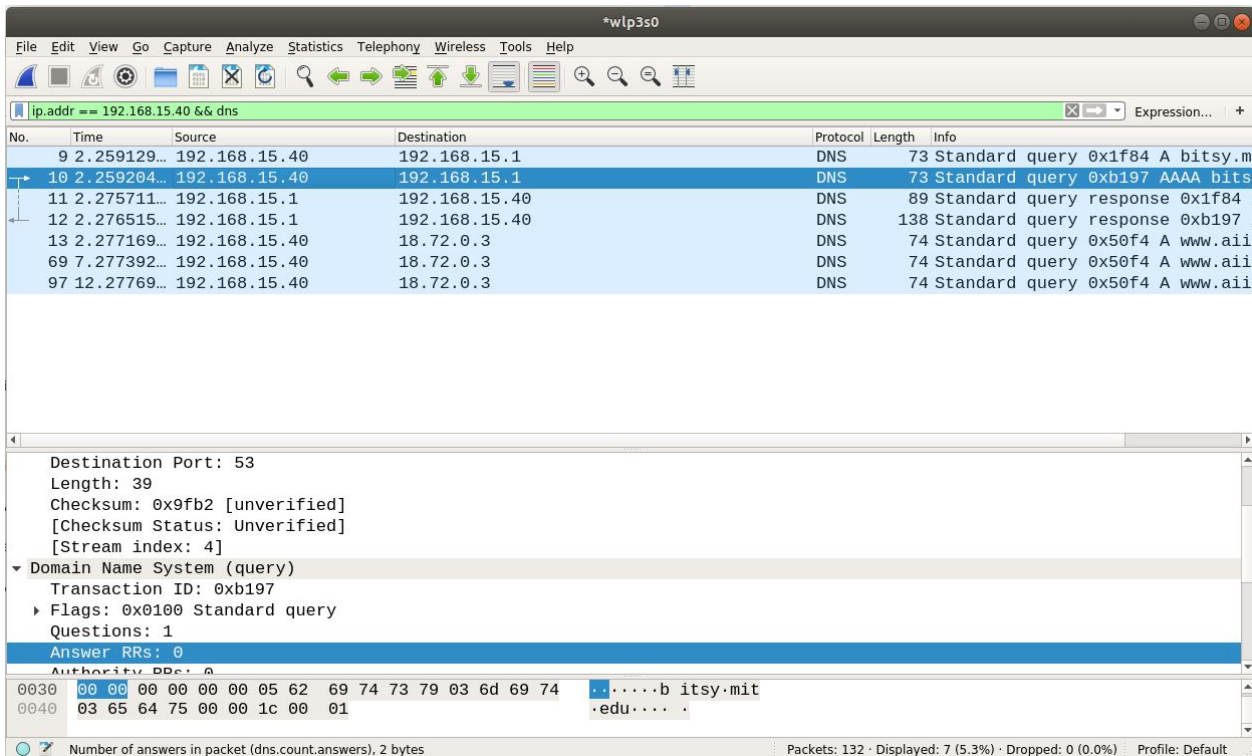
Time to live: 1800

Data length: 4

Address: 18.72.0.3

4. Grave a tela de captura de pacotes.

R:



Wireshark packet capture showing a DNS query and response. The packet list shows a query for bitsy.mit.edu and a response from 192.168.15.1. The packet details pane shows the DNS query structure.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|---------------|---------------|----------|--------|---------------------------------|
| 9 | 2.259129... | 192.168.15.40 | 192.168.15.1 | DNS | 73 | Standard query 0x1f84 A bitsy.m |
| 10 | 2.259204... | 192.168.15.40 | 192.168.15.1 | DNS | 73 | Standard query 0xb197 AAAA bits |
| 11 | 2.275711... | 192.168.15.1 | 192.168.15.40 | DNS | 89 | Standard query response 0x1f84 |
| 12 | 2.276515... | 192.168.15.1 | 192.168.15.40 | DNS | 138 | Standard query response 0xb197 |
| 13 | 2.277169... | 192.168.15.40 | 18.72.0.3 | DNS | 74 | Standard query 0x50f4 A www.iii |
| 69 | 7.277392... | 192.168.15.40 | 18.72.0.3 | DNS | 74 | Standard query 0x50f4 A www.iii |
| 97 | 12.27769... | 192.168.15.40 | 18.72.0.3 | DNS | 74 | Standard query 0x50f4 A www.iii |

Destination Port: 53
Length: 39
Checksum: 0x9fb2 [unverified]
[Checksum Status: Unverified]
[Stream index: 4]

▼ Domain Name System (query)
Transaction ID: 0xb197
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0

0030 00 00 00 00 00 05 62 69 74 73 79 03 6d 69 74b itsy.mit
0040 03 65 64 75 00 00 1c 00 01 .edu....

Number of answers in packet (dns.count.answers), 2 bytes

Packets: 132 · Displayed: 7 (5.3%) · Dropped: 0 (0.0%) · Profile: Default