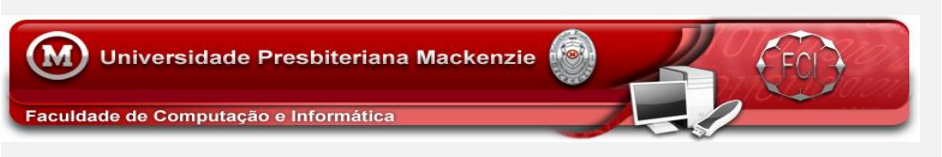


Redes de computares

Prof. Dr. Bruno da Silva Rodrigues
Bruno.rodrigues@mackenzie.br

Analise de consulta DNS usando Wireshark.

Introdução

Imagine ter que acessar seus sites preferidos através de números de IP (Internet Protocol), memorizando sequências de números para cada um deles. Para evitar decorar o endereço IP de todos os sites que acessamos, os servidores de DNS espalhados pelo mundo tem a importante função de traduzir os endereços digitados no browser, para o número de IP correspondente.

Procedimento

- ***Abra o arquivo DNS.pcapng no wireshark.***

O conteúdo do arquivo foi capturado após os seguintes passos:

- ✓ *Limpeza do cache DNS(**ipconfig /flushdns**);*
- ✓ *Inicio da captura de pacotes no Wireshark;*
- ✓ *Acesso aos seguintes sites:*
  www.lsi.usp.br
  www.ietr.fr
  www.mackenzie.br

Responda as questões no próprio arquivo com letras em negrito e na cor vermelha.

Após abrir o arquivo analise os pacotes e responda:

Objetivos da atividade:

- Apresentar aos alunos o princípio básico de funcionamento do protocolo DNS.

Bibliografias

KUROSE, J. F. e ROSS, K. W. Redes de Computadores e a Internet – Uma Nova Abordagem – Pearson

M. A. Filippetti - Samuel Henrique Bucke Brito - Visual books

Wireshark ORG
Disponível em:
https://www.wireshark.org/

Internet Engineering Task Force.
Disponível em:
https://www.ietf.org/rfc/rfc1035.txt

Questão 1. *Localize as mensagens de solicitação e resposta DNS. Essas mensagens foram enviadas com TCP ou UDP? Justifique sua resposta.*

```
> User Datagram Protocol, Src Port: 52198, Dst Port: 53
> Domain Name System (query)
```

Questão 2. *Qual é a porta destino para a mensagem de consulta DNS? Qual é a porta de origem da mensagem DNS?* ***(a verdadeira porta do DNS só será visível quando a experiencia for realizada sem proxy).***

A porta de destino é a porta 53, já a de origem é a 52198

Questão 3. *Procure a requisição DNS para o site www.ietr.fr e preencha o cabeçalho de resposta abaixo conforme resposta do servidor DNS ?*

Identificação	Flags
Número de perguntas	Número de RRs de resposta
Número de RRs com autoridade	Número de RRs adicionais
Perguntas (número variável de perguntas)	
Respostas (número variável de registros de recursos)	
Autoridade (número variável de registros de recursos)	
Informação adicional (número variável de registros de recursos)	

0x0336	**0x8180**
1	**1**
0	**0**
www.lsi.usp.br: type A, class IN	
www.lsi.usp.br: type A, class IN, addr 143.107.161.160	

Questão 4. *A página do moodle foi acessada a partir da página www.mackenzie.br , para acessar o servidor onde a página está hospedada uma nova requisição DNS foi realizada? Interprete os resultados e discorra sobre o assunto.*

Sim

```
> Frame 5383: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface \Device\NPF_{585A08AD-31CC-41A9-B532-B82A1345803D}, id 0
> Ethernet II, Src: HewlettP_7b:b1:71 (44:31:92:7b:b1:71), Dst: Dell_1e:9f:d7 (00:1e:c9:1e:9f:d7)
> Internet Protocol Version 4, Src: 172.18.100.1, Dst: 172.18.10.18
> User Datagram Protocol, Src Port: 53, Dst Port: 51932
v Domain Name System (response)
    Transaction ID: 0xcd92
  v Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    v moodle.mackenzie.br: type CNAME, class IN, cname www.x.uvmack.com.br
        Name: moodle.mackenzie.br
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 2662 (44 minutes, 22 seconds)
        Data length: 19
        CNAME: www.x.uvmack.com.br
    v www.x.uvmack.com.br: type A, class IN, addr 177.43.201.212
        Name: www.x.uvmack.com.br
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 15 (15 seconds)
        Data length: 4
        Address: 177.43.201.212
    [Request In: 4943]
```

Questão 5. *Procure a requisição DNS para a página do moodle e preencha o cabeçalho de resposta abaixo conforme resposta do servidor DNS ?*

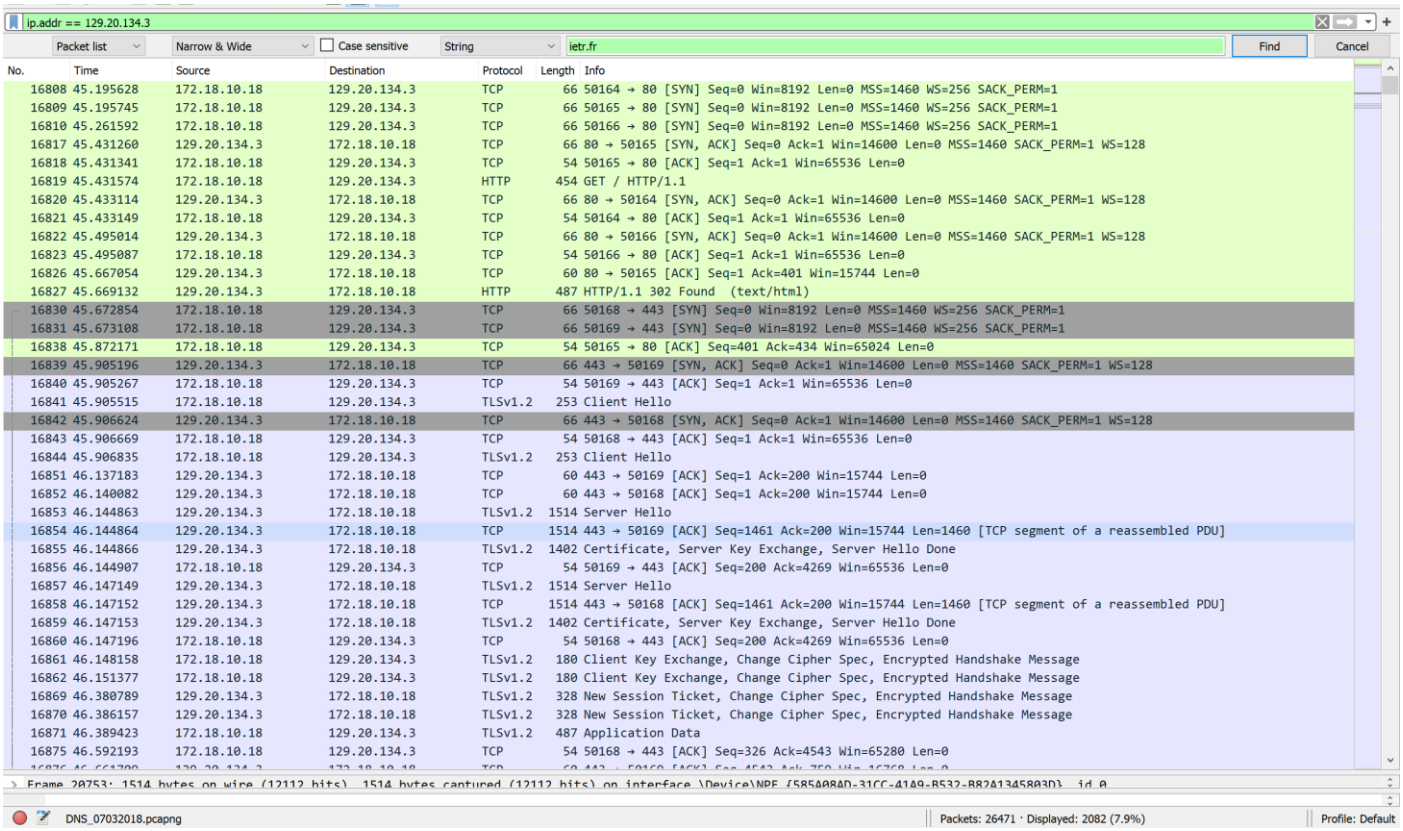
Identificação	Flags
Número de perguntas	Número de RRs de resposta
Número de RRs com autoridade	Número de RRs adicionais
Perguntas (número variável de perguntas)	
Respostas (número variável de registros de recursos)	
Autoridade (número variável de registros de recursos)	
Informação adicional (número variável de registros de recursos)	

0x0000cd92	**0x00008180**
1	**2**
0	**0**
moodle.mackenzie.br: type A, class IN	
moodle.mackenzie.br: type CNAME, class IN, cname www.x.uvmack.com.br **www.x.uvmack.com.br: type A, class IN, addr 177.43.201.212**	

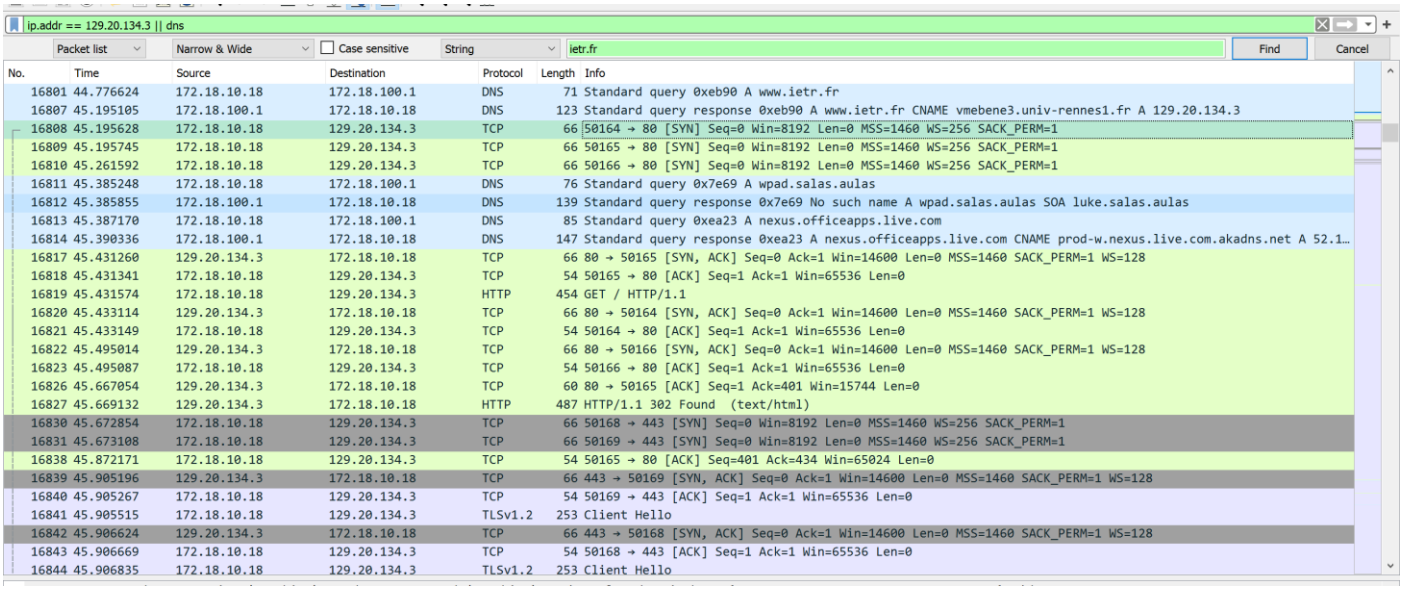
Questão 6. *Analise o cabeçalho de resposta do servidor DNS para www.lsi.usp.br e a resposta do servidor do www.Mackenzie.br. Analise registro de recurso (RR) e responda qual o* ***tipo*** *da resposta enviada pelo servidor em ambos os casos? Discorra sobre a diferença nos resultados*

No caso do Mackenzie, é realizado um redirecionamento para encontrar o IP do Mackenzie, enquanto o da USP é mandado apenas com uma resposta direta

Questão 7*. Aplique o filtro de endereçamento IP para selecionar os pacotes trocados com o servidor do www.ietr.fr "ip.addr == endereço_IP do servidor" ?Apresente o print da tela com a troca de mensagens entre o cliente e o servidor.*



Questão 8*. Aplicando o mesmo filtro da mensagem anterior adicione o operador "ou" (||) no filtro e adicione o protocolo dns a sua procura. Faça um print e interprete a diferença entre os resultados apresentados na questão 7 e 8.*



Primeiro faz a requisição do DNS, então faz a sincronização com o TCP também. Então há o get, ou seja, pega todas as mensagens do site na forma de http e por fim encerra a requisição por tcp também.

NSLOOKUP

*Neste exercício usaremos a ferramenta **nslookup**, que está disponível em muitas plataformas Linux/Unix e Microsoft Windows é utilizada para se obter informações sobre registros de DNS de um determinado domínio, host ou IP. Para executar o nslookup no Linux/Unix ou no Windows, você deve digitar o comando nslookup no Prompt de Comando (ou terminal). Na sua operação mais básica, nslookup permite que o host que roda a ferramenta faça perguntas a um servidor DNS específico. O DNS perguntado pode ser um servidor DNS raíz, um DNS de alto nível, um DNS com autoridade ou um servidor DNS intermediário. Para fazer essa tarefa, nslookup envia um questionamento (query) DNS para o servidor DNS específico, recebe a reposta desse DNS e mostra o resultado, veja o resultado de uma execução do nslookup na Figura 1.*

```
C:\Users\d_tre>nslookup uol.com.br
Servidor:  UnKnown
Address:  192.168.0.1

Não é resposta autoritativa:
Nome:    uol.com.br
Addresses:  2804:49c:3103:401:ffff:ffff:ffff:1
          200.147.67.142
```

Figura 1. Saída do NSLOOKUP

A Figura 1 mostra o resultado da execução do nslookup para determinar o endereço de www.uol.com.br. Neste exemplo a máquina onde a busca foi iniciada é o servidor DNS que está configurado nas propriedades de rede de seu sistema operacional (neste caso o servidor 192.169.0.1).

Caso eu queira saber quais servidores de nomes respondem por este domínio eu utilizo o seguinte comando: nslookup -type=NS uol.com.br

```
C:\Users\d_tre>nslookup -type=NS uol.com.br
Servidor:  UnKnown
Address:  192.168.0.1

Não é resposta autoritativa:
uol.com.br      nameserver = eliot.uol.com.br
uol.com.br      nameserver = charles.uol.com.br
uol.com.br      nameserver = borges.uol.com.br

C:\Users\d_tre>
```

Figura 2. Consulta NSLOOKUP para servidores de nome

Assim como vimos na aula de teoria, o tipo do registro pode ser A, AAAA, MX, SOA.

É possível consultar de algum registro diretamente ao servidor autoritativo DNS de um domínio, por meio da sintaxe:

nslookup REGISTRO nameserver

Vamos entender esta sintaxe. Na figura2 anterior a consulta para o domínio uol.com.br foi os servidores de nomes. Na figura 3 um exemplo de consulta ao servidor de nomes do site uol.com.br

```
C:\Users\d_tre>nslookup www.uol.com.br borges.uol.com.br
Servidor:  borges.uol.com.br
Address:  200.147.255.105

Nome:    www.uol.com.br
```

Figura 3. Consulta NSLOOKUP dos servidores de nome do uol.com.br

O comando nslookup serve para fazer consultas DNS. Pesquise sobre o funcionamento deste comando e responda as seguintes questões:

Questão 9. Realize uma consulta ao nome Mackenzie.br e responda:

a) *Qual endereço IP associado ao nome?*

```
168.197.92.195
```

b) *Qual o nome dos servidores DNS do Mackenzie?*

```
Nao é resposta autoritativa:
mackenzie.br    nameserver = ns2.mackenzie.com.br
mackenzie.br    nameserver = dns.mackenzie.com.br
mackenzie.br    nameserver = ns3.mackenzie.com.br

dns.mackenzie.com.br    internet address = 168.197.92.90
ns3.mackenzie.com.br    internet address = 187.72.64.90
ns2.mackenzie.com.br    internet address = 168.197.92.100
```

c) *Qual o endereço do servidor de e-mail do Mackenzie?*

```
Nao é resposta autoritativa:
mackenzie.br    MX preference = 0, mail exchanger = mackenzie-br.mail.protection.outlook.com
```

d) Realize uma consulta ao registro do tipo SOA (Start Of Authority) do nome mackenzie.br. Explique o que são as informações apresentadas.

```
Nao é resposta autoritativa:
mackenzie.br
        primary name server = dns.mackenzie.com.br
        responsible mail addr = root.mackenzie.com.br
        serial  = 2014122501
        refresh = 3600 (1 hour)
        retry   = 1800 (30 mins)
        expire  = 1209600 (14 days)
        default TTL = 3600 (1 hour)
```

O SOA são informações importantes sobre o domínio, como o nome primário do servirdor, email do administrador, o quanto o servidor deve esperar entre refresh

Questão 10. Realize uma consulta ao nome ***uol.com.br*** e ao nome ***folha.uol.com.br*** e responda:

a) *O endereço IP associado aos nomes são iguais?*

```
Nao é resposta autoritativa:
Nome:    uol.com.br
Addresses:  2804:49c:3102:401:ffff:ffff:ffff:36
          2804:49c:3101:401:ffff:ffff:ffff:45
          200.147.35.149
```

```
Nao é resposta autoritativa:
Nome:    folha.uol.com.br
Addresses:  2804:49c:319:430::339
          200.147.100.48
```

Os endereços são diferentes

b) *Os servidores DNS dos dois sites são iguais?*

```
C:\Users\gabri>nslookup -type=NS folha.uol.com.br
Servidor:  UnKnown
Address:  fe80::96ea:eaff:fee2:f54

Nao é resposta autoritativa:
folha.uol.com.br        nameserver = borges.uol.com.br
folha.uol.com.br        nameserver = charles.uol.com.br
folha.uol.com.br        nameserver = eliot.uol.com.br

borges.uol.com.br       internet address = 200.147.255.105
charles.uol.com.br      internet address = 200.147.38.8
eliot.uol.com.br        internet address = 200.221.11.98
```

```
C:\Users\gabri>nslookup -type=NS uol.com.br
Servidor:  UnKnown
Address:  fe80::96ea:eaff:fee2:f54

Nao é resposta autoritativa:
uol.com.br      nameserver = borges.uol.com.br
uol.com.br      nameserver = eliot.uol.com.br
uol.com.br      nameserver = charles.uol.com.br

eliot.uol.com.br        internet address = 200.221.11.98
charles.uol.com.br      internet address = 200.147.38.8
borges.uol.com.br       internet address = 200.147.255.105
```

c) *Com base nas respostas anteriores analise os endereços associados ao nome e os servidores explique por que os endereços são iguais ou diferentes.*

Os endereços de DNS são os mesmos, até por que os sites estão hospedados no mesmo domínio, porem o endereço IP de cada site é diferente

Questão 12. Realize uma consulta ao nome Mackenzie.br, ietr.fr e uol.com.br. Quais dos domínios possui endereço IPv6? Lembre-se de verificar essa informação mudando a função type da consulta.

```
C:\Users\gabri>nslookup -type=AAAA uol.com.br
Servidor:  UnKnown
Address:  fe80::96ea:eaff:fee2:f54

Nao é resposta autoritativa:
Nome:    uol.com.br
Addresses:  2804:49c:3101:401:ffff:ffff:ffff:45
          2804:49c:3102:401:ffff:ffff:ffff:36
```

```
C:\Users\gabri>nslookup -type=AAAA mackenzie.br
Servidor:  UnKnown
Address:  fe80::96ea:eaff:fee2:f54

Nome:    mackenzie.br
```

```
C:\Users\gabri>nslookup -type=AAAA ietr.fr
Servidor:  UnKnown
Address:  fe80::96ea:eaff:fee2:f54

Nome:    ietr.fr
```

Apenas o uol.com.br possui o endereço IPV6