Universidade Presbiteriana Mackenzie
Faculdade de Computação e Informática

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 esse endereço para cada um desses sites. Para evitar decorar o endereço IP de todos os sites que acessamos, uma rede de servidores distribuídos opera de maneira a facilitar o acesso aos sites traduzindo os endereços digitados no browser (URL), para o número de IP do servidor web correspondente. Esse serviço é conhecido como DNS.

Procedimento

Para realizar a atividade, faça o download do arquivo ***DNS.pcap*** *no moodle e abra o arquivo no Wireshark.*

- Para criar o arquivo que será analisado em nossa atividade, foi realizado os seguintes procedimentos:

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

Observação 1: *Caso queira verificar as diferenças entre o arquivo disponibilizado e um arquivo gerado na sua casa, realize o procedimento passo a passo acima no seu computador e compare os dois arquivos.*

Após abrir o arquivo no Wireshark responda as questões abaixo:

Observação 2: Todas as respostas devem estar em negrito na cor vermelha

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(0,5 ponto)**. Qual o protocolo de transporte foi utilizado para o envio das mensagens DNS (TCP ou UDP)? Justifique sua resposta (pode apresentar um print da tela).*

O protocolo utilizado para o envio de mensagens DNS foi o UDP.

```
7 7.605117      172.18.10.18      172.18.100.1      DNS                77 Standard query 0x44a7 A www.google.com.br
```

```
Protocol: UDP (17)
```

Questão 2(1,0 ponto)**. Qual é o número da porta do servidor DNS? Qual é ao número da porta do cliente DNS? **(a verdadeira porta do DNS só será visível quando a experiencia for realizada sem proxy – Pode escolher qualquer solicitação de DNS presente no arquivo).

Porta de cliente: 51528

Porta do servidor: 53

```
User Datagram Protocol, Src Port: 51528, Dst Port: 53
```

***Questão 3(3,0 pontos).** As informações apresentadas abaixo (quadro da esquerda) representam os campos do cabeçalho DNS.*

***A)** Preencha o quadro (direita) abaixo com as informações extraídas da resposta do servidor DNS para a consulta da URL www.ietr.fr.*

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)	

0xeb90	***0x8180***
1	***2***
0	***0***
1	
2	
Autoridade (não preencher)	
Informação Adicional (não preencher)	

***B)** Preencha o quadro (direita) abaixo com as informações extraídas da resposta do servidor DNS para a consulta ao servidor do www.lsi.usp.br.*

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)	

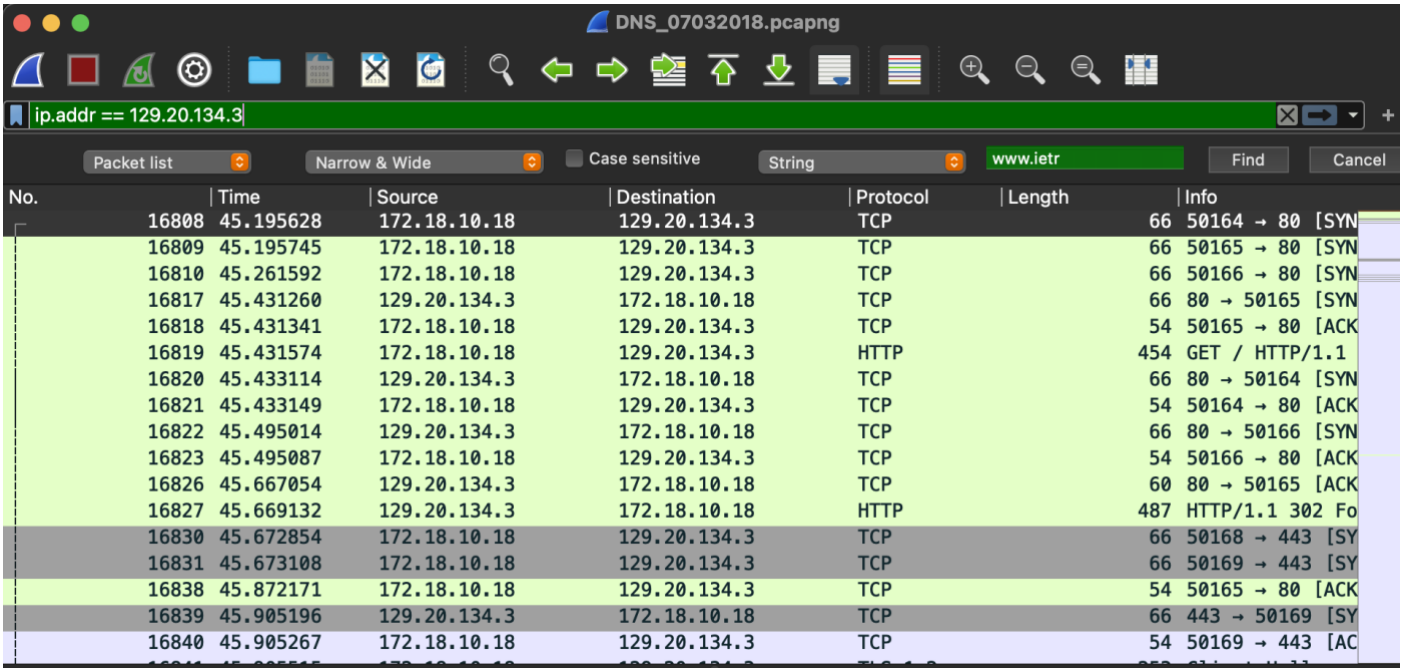
0x0336	***0x0100***
1	***1***
0	***0***
1	
1	
Autoridade (não preencher)	
Informação Adicional (não preencher)	

c) *Analise o cabeçalho de resposta do servidor DNS das alternativas "A" e "B. Com base nas informações contidas no* ***registro de recurso (RR)****, explique o motivo da diferença entre as respostas.*

A diferença entre os dois se dá porque na primeira requisição o servidor devolveu duas respostas de registros de recursos (RR) uma apontando para um IP e outra para um registro CNAME, enquanto a segunda requisição só devolveu uma resposta com o IP.

Questão 6(0,5 ponto)*. Localize a solicitação DNS para a URL www.ietr.fr . Com base no RR da resposta, extraia o endereço IP do servidor WEB e o filtro do wireshark para selecionar todos os pacotes com esse endereço IP. Para isso, use no campo filtro o comando "ip.addr ==* ***endereço IP-servidor****" , onde* ***endereço IP-servidor*** *é o endereço IP do servidor www.ietr.fr fornecido pelo servidor DNS. Apresente o print da tela com a troca de mensagens entre o cliente e o servidor.*

Obs*. Questão usada somente para ensinar como filtrar pacotes por endereço IP*

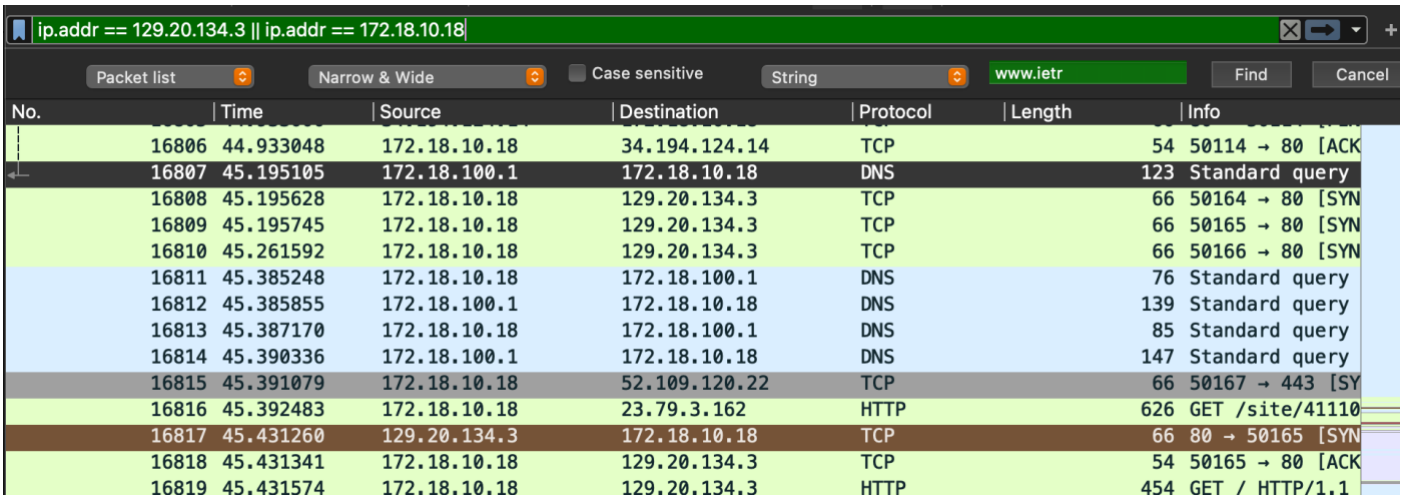


Questão 7 (0,5 ponto). *Aplicando o mesmo filtro da mensagem anterior adicione o operador "ou" (||) no filtro e adicione o protocolo DNS a sua procura.*

> ***e.g.*** *ip.addr == **endereço IP-servidor** || DNS*
>
> *Onde **endereço IP-servidor** é o endereço IP do servidor www.ietr.fr fornecido pelo servidor DNS.*

Após o uso do filtro, observe os pacotes disponíveis para análise. Com base nas informações de resumo, notamos que foram usados os protocolos DNS, TCP e HTTP. Apresente um print da tela com a ordem que os pacotes foram apresentados.

Obs. *Questão usada somente para ensinar como filtrar pacotes por endereço IP e o operador lógico OR.*



PARTE 2 - NSLOOKUP

Nesta segunda parte da atividade, usaremos a ferramenta ***nslookup****, que está disponível em muitas plataformas Linux/Unix e Microsoft Windows. Essa ferramenta pode ser utilizada para 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 na CLI (ou terminal). Na sua operação mais básica, nslookup permite que um host faça solicitações (query) a um servidor DNS que irá responder a solicitação conforme imagem apresentado na Figura 1.*

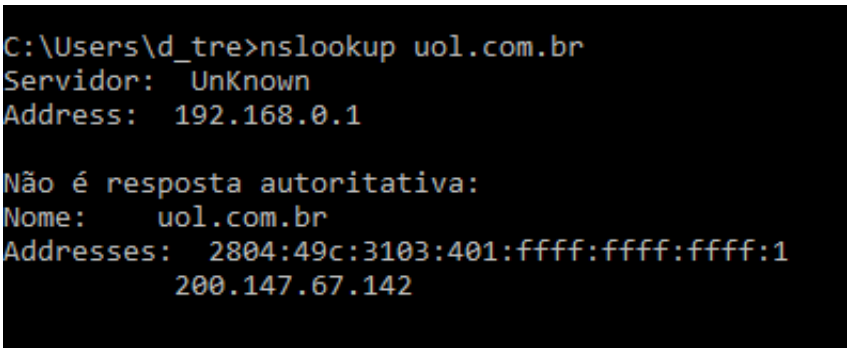


Figura 1. Resposta a uma solicitação NSLOOKUP

A Figura 1 mostra o resultado da execução do nslookup para determinar o endereço IP correspondente a URL www.uol.com.br. O nslookup também permite realizar consultas a registros específicos desde que o usuário informe o tipo da consulta. Na figura 2, temos um exemplo de consulta para saber quais servidores de nomes respondem ao domínio www.uol.com.br.

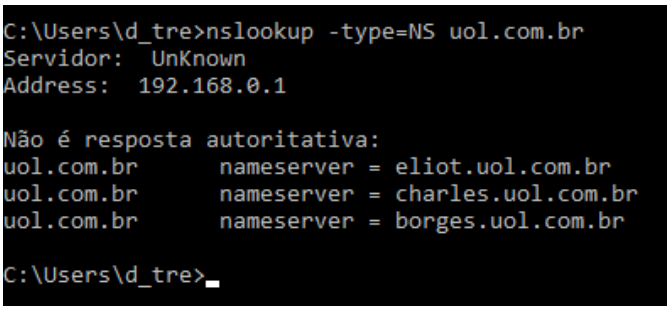


Figura 2. Consulta NSLOOKUP para servidores de nome

Para realizar a consulta apresentada na figura 2, foi necessário especificar o tipo do recurso (no caso do exemplo foi usado Type = NS). Assim como vimos na aula de teoria, os tipos de registro podem ser: A, AAAA, MX, SOA, entre outros.

Com base nessas informações iniciais, responda as seguintes questões(todas as respostas devem ter o print da tela:

Questão 8 (1,5 ponto). Realize uma consulta ao nome Mackenzie.br e responda:

a) *Qual endereço IP associado ao domínio?*
18.228.171.139

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

dns.mackenzie.com.br.
ns3.mackenzie.com.br.
ns2.mackenzie.com.br.

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

Start of authority dns.mackenzie.com.br.

Email root@mackenzie.com.br

Serial 2014122501

Essas informações estão relacionadas ao registro de SOA (Start of Authority) do domínio "mackenzie.com.br" no sistema DNS (Domain Name System).

Questão 9 (1,5 ponto). Realize uma consulta ao nome ***uol.com.br*** e ao nome ***folha.uol.com.br*** e responda:

a) *O endereço IP associado as URL's solicitadas são iguais?*

Não.

b) *O que significa ter endereços IP's diferentes associadas as URL's?*

Significa que o o domínio e esse subdomínio não apontam para o mesmo servidor.

Questão 10 (1,5 ponto). 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.'

uol.com.br tem ipv6.