|  |
| --- |
|  |
|  |
|  |

Redes de computares

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> |

***Prof. Dr. Bruno da Silva Rodrigues***

[Bruno.rodrigues@mackenzie.br](mailto: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](http://www.lsi.usp.br/)

[www.ietr.fr](http://www.ietr.fr/)

[www.mackenzie.br](http://www.mackenzie.br/)

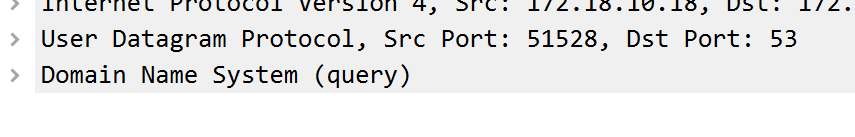
***Observação 1:*** *Caso queira verificar as diferenças entre o arquivo disponibilizado e um arquivo gerado na sua casa, realize o procedimento passo a passo acima no seu computador e compare os dois arquivos.*

***Após abrir o arquivo no Wireshark responda as questões abaixo:***

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

***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).*

**UDP**



***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***

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

1. *Preencha o quadro (direita) abaixo com as informações extraídas da resposta do servidor DNS para a consulta da URL* [www.ietr.fr](http://www.ietr.fr/)*.*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  |  | | --- | --- | |  | | | **0xeb90** | **0x8180** | | **1** | **2** | | **0** | **0** | | **www.ietr.fr: type A, class IN** | | | **www.ietr.fr: type CNAME, class IN, cname vmebene3.univ-rennes1.fr**  **vmebene3.univ-rennes1.fr: type A, class IN, addr 129.20.134.3** | | | *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*](http://www.lsi.usp.br/)*.*

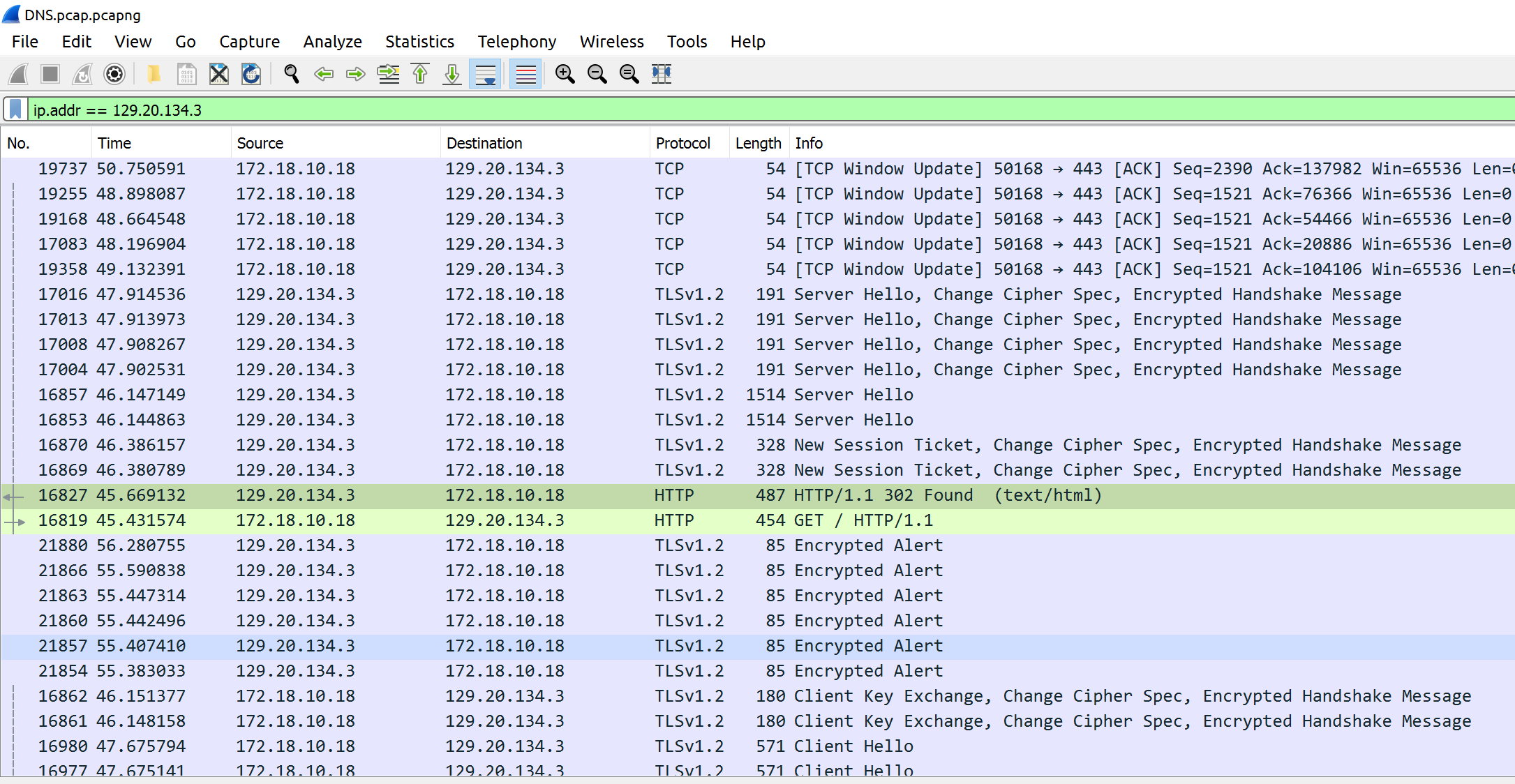
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  |  | | --- | --- | |  | | | **0x0336** | **0x8180** | | **1** | **1** | | **0** | **0** | | **www.lsi.usp.br: type A, class IN**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

**0**

***Questão 6(0,5 ponto)****. Localize a solicitação DNS para a URL* [www.ietr.fr](http://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](http://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*

**

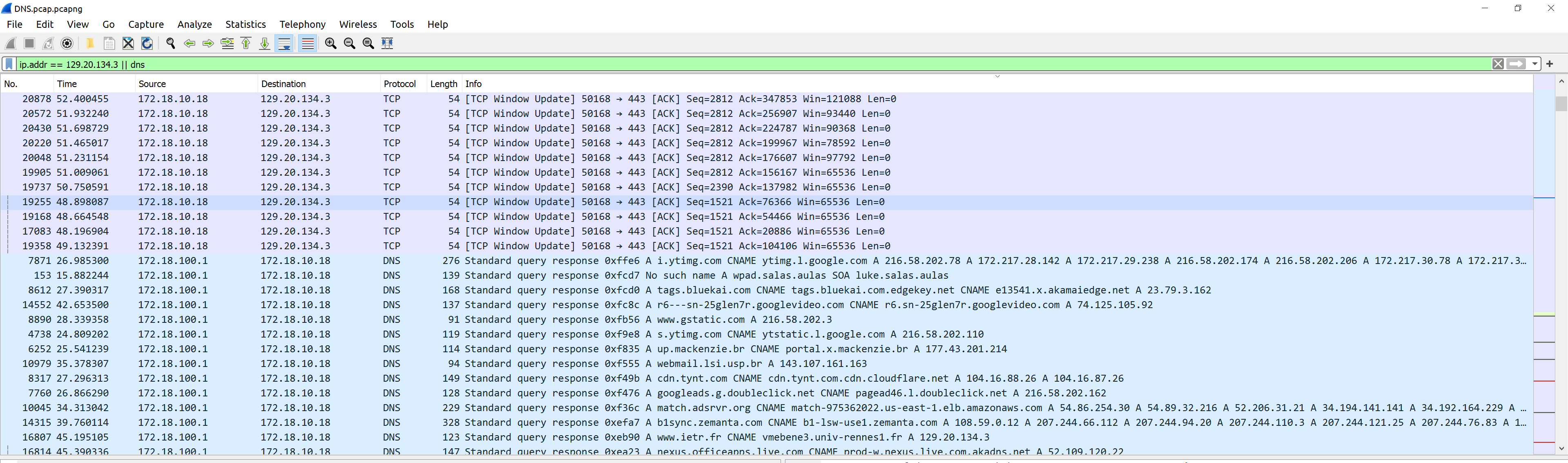
***Questão 7 (0,5 ponto)****. Aplicando o mesmo filtro da mensagem anterior adicione o operador “ou” (||) no filtro e adicione o protocolo DNS a sua procura.*

***e.g.*** *ip.addr ==****endereço IP-servidor*** *|| DNS*

*Onde* ***endereço IP-servidor*** *é o endereço IP do servidor* [www.ietr.fr](http://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.*

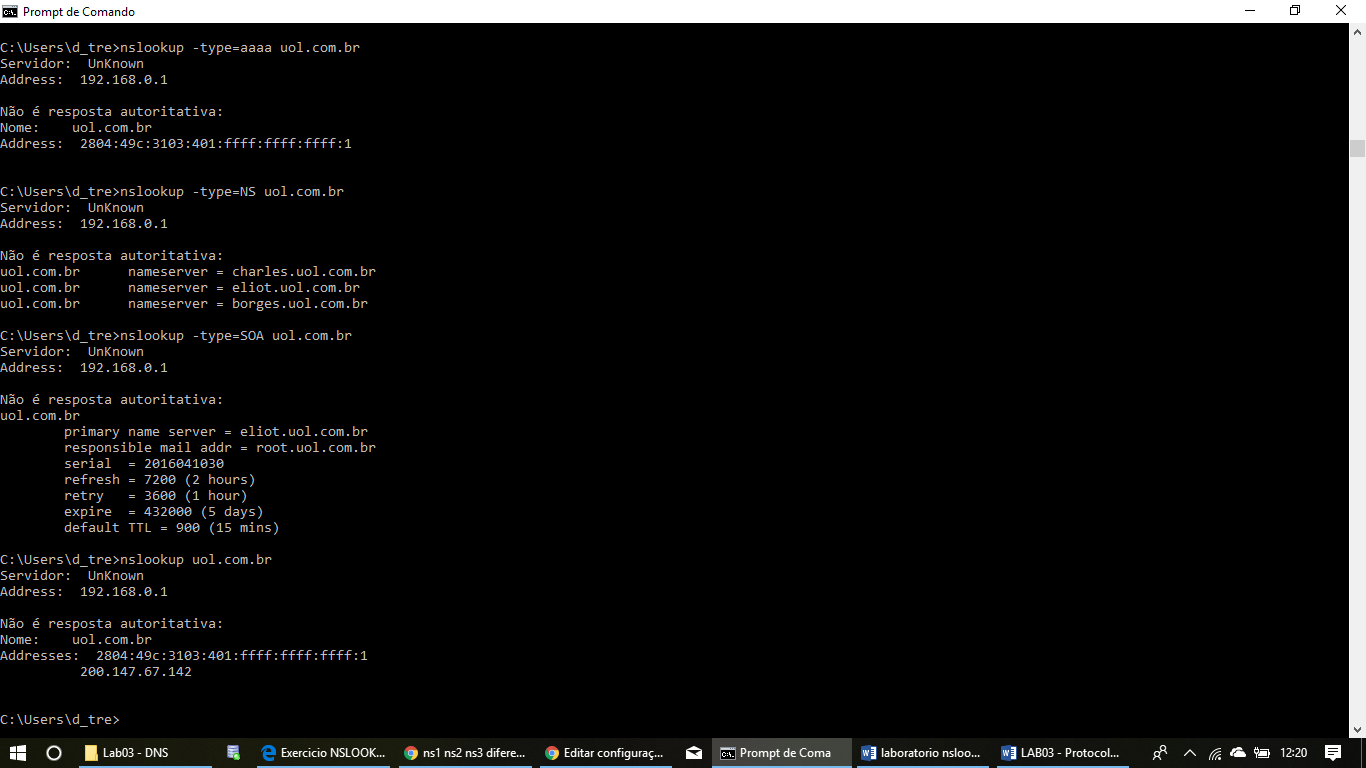


Figura 1. Resposta a uma solicitação NSLOOKUP

*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.*

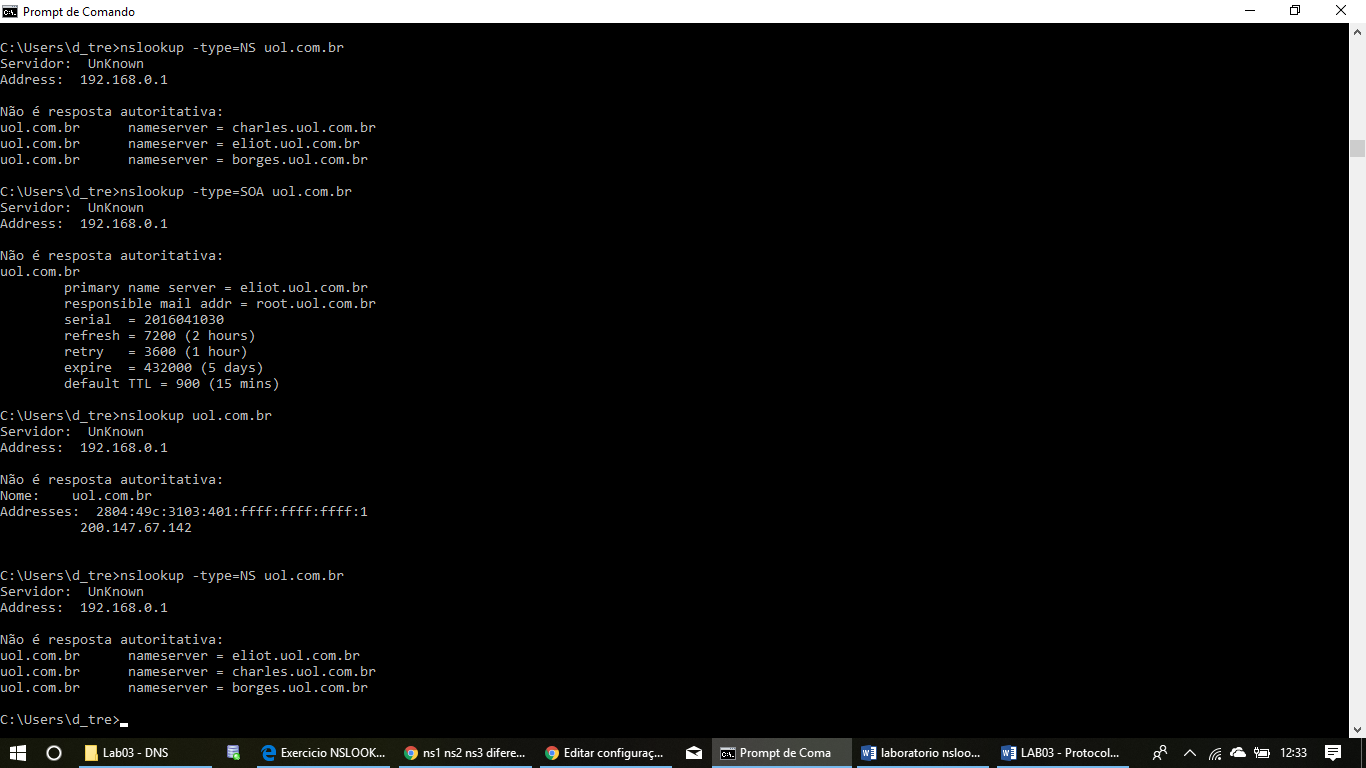


Figura 2. Consulta NSLOOKUP para servidores de nome

*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:

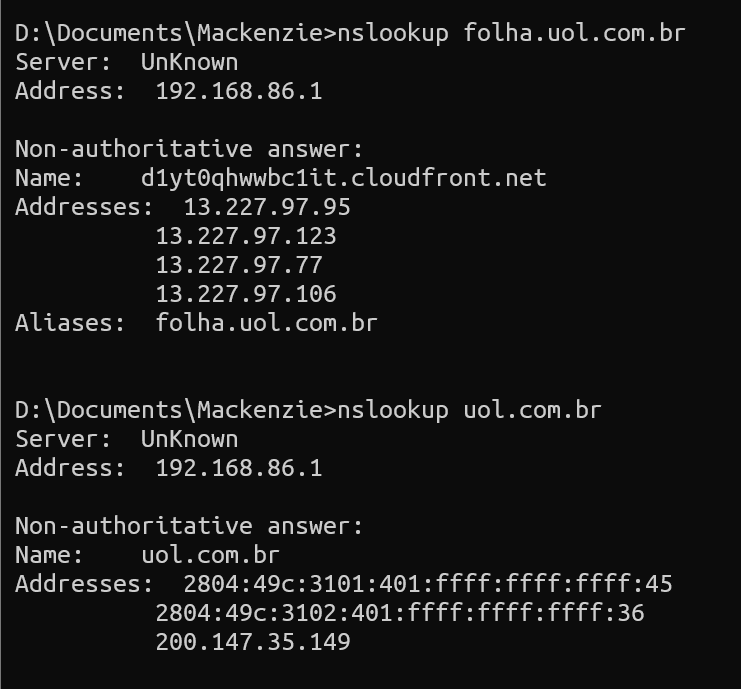
1. *Qual endereço IP associado ao domínio?* **18.228.171.139**
2. *Qual o nome dos servidores DNS do Mackenzie?* **dns.mackenzie.com.br, ns2.mackenzie.com.br, ns3.mackenzie.com.br**
3. *Qual o endereço do servidor de e-mail do Mackenzie?* **mackenzie-br.mail.protection.outlook.com**
4. Realize uma consulta ao registro do tipo SOA (Start Of Authority) do nome mackenzie.br. Explique o que são as informações apresentadas.

"primary name server = dns.mackenzie.com.br" indica o servidor DNS autoritativo para o domínio consultado. Esse servidor é responsável por fornecer informações de autoridade para o domínio.

* **"responsible mail addr = root.mackenzie.com.br" indica o endereço de e-mail do responsável pelo domínio. Esse campo é opcional e pode não estar presente em todas as consultas SOA.**
* **"serial = 2014122501" é um número de série que indica a versão atual da zona DNS do domínio. Esse número é atualizado cada vez que a zona é modificada.**
* **"refresh = 3600 (1 hour)" indica o intervalo de tempo em segundos após o qual o servidor DNS autoritativo para o domínio deve ser consultado novamente para atualizar as informações de autoridade.**
* **"retry = 1800 (30 mins)" indica o intervalo de tempo em segundos após o qual o servidor DNS local deve tentar novamente uma consulta SOA, caso a primeira consulta falhe.**
* **"expire = 1209600 (14 days)" indica o tempo em segundos após o qual a zona DNS do domínio será considerada inválida, caso o servidor DNS local não seja capaz de contatar o servidor DNS autoritativo para renovar as informações de autoridade.**
* **"default TTL = 3600 (1 hour)" é o tempo em segundos pelo qual os registros DNS no cache de outros servidores DNS devem ser mantidos antes de serem descartados e atualizados a partir do servidor DNS autoritativo.**

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

1. *O endereço IP associado as URL’s solicitadas são iguais?* **Não**

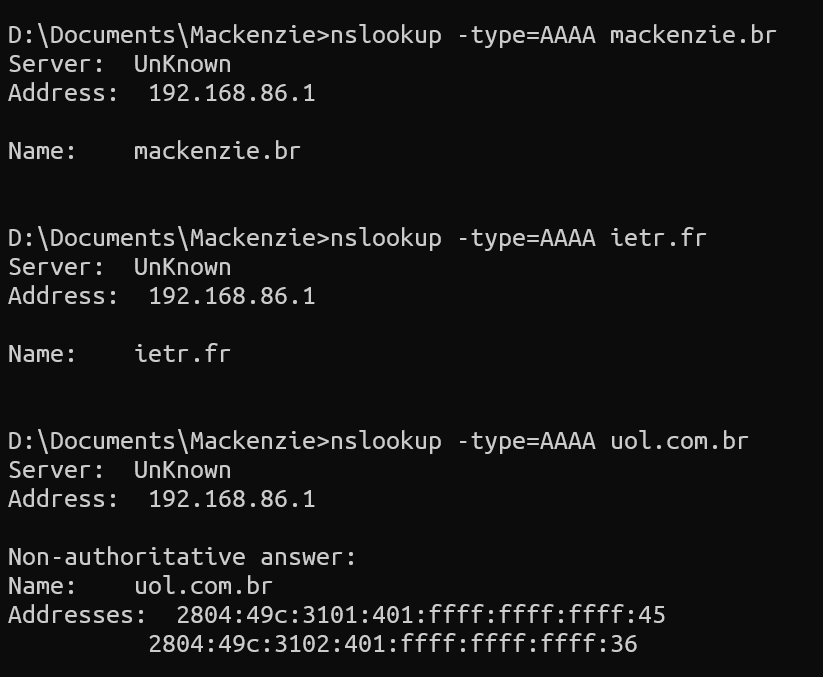
**

1. *O que significa ter endereços IP’s diferentes associadas as URL’s?*

**Ter endereços IPs diferentes associados a URLs do mesmo subdomínio pode significar que existem vários servidores que estão hospedando o conteúdo desse subdomínio. Cada endereço IP está associado a um servidor específico que contém uma cópia do conteúdo do subdomínio.**

***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.’

**Somente o UOL tem IPv6.**

****