Nome:

LABORATÓRIO WIRESHARK: DNS

Conforme material da webaula, o Domain Name System (DNS) traduz nomes de hosts para endereços IP, cumprindo um papel fundamental na infra-estrutura da Internet. Neste laboratório, vamos dar uma olhada no lado cliente do DNS. Lembre-se que o papel do cliente no DNS é relativamente simples - um cliente envia uma consulta para o servidor DNS local, e recebe de volta uma resposta.

1 NSLOOKUP

Neste laboratório, nós faremos uso extensivo da ferramenta nslookup, que está disponível na maioria das plataformas Linux/Unix e Microsoft hoje. Para executar o nslookup no Linux/Unix, você apenas digita o comando nslookup na linha de comando ou o comando dig. Para executá-lo no Windows, abra o Prompt de comando e execute nslookup na linha de comando.

Na operação mais básica, a ferramenta nslookup permite que o host que execute a ferramenta consulte qualquer servidor DNS especificado para um registro DNS. O servidor DNS consultado pode ser um servidor DNS raiz, um servidor de nível superior de domínio (TLD), um servidor DNS autoritário, ou um servidor DNS intermediário (ver o livro-texto para definições destes termos). Para realizar essa tarefa, o nslookup envia uma consulta DNS para o servidor DNS especificado, recebe uma resposta DNS do mesmo servidor, e exibe o resultado.

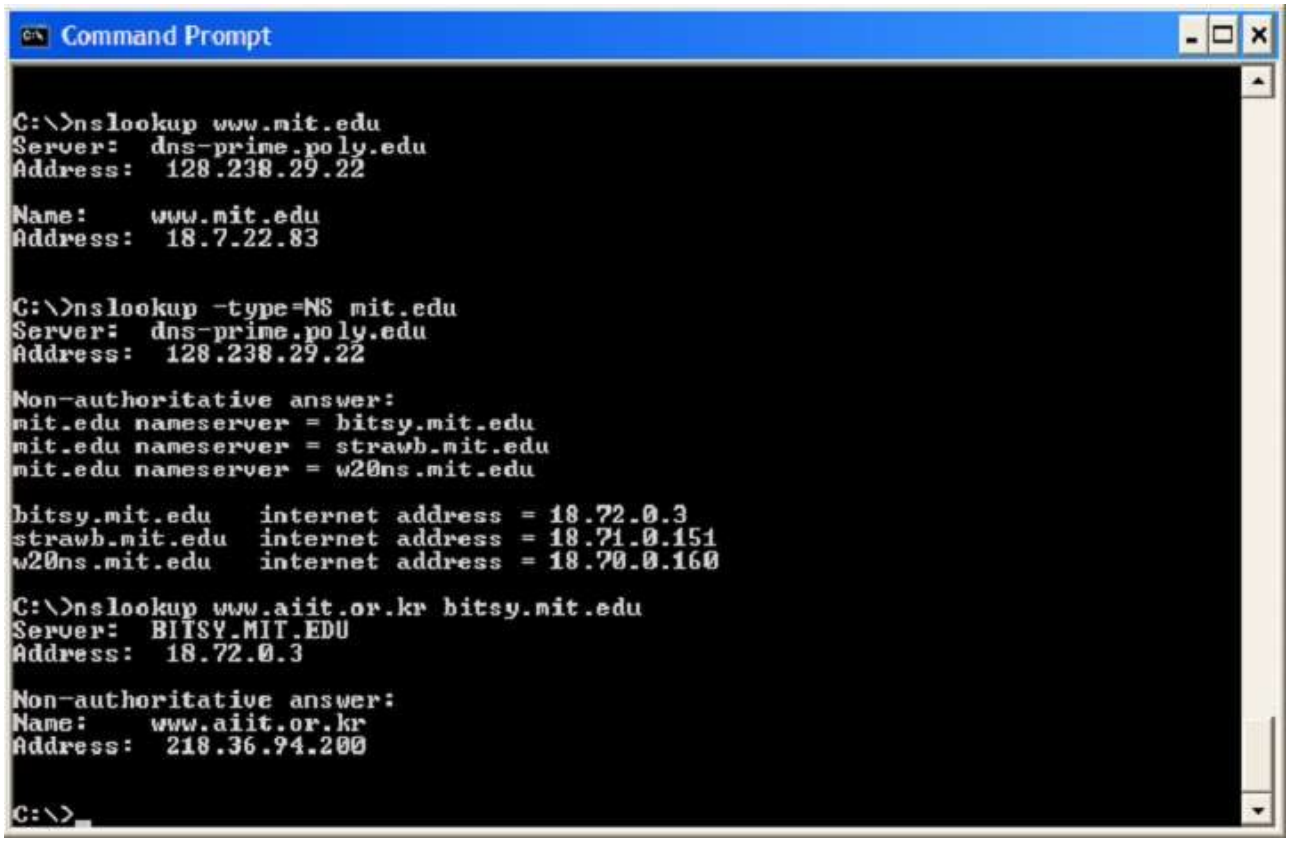


Figura 1

O screenshot acima mostra o resultado de três comandos nslookup independentes (exibidos no Prompt de comando do Windows). Nesse exemplo, o host cliente é localiza no campus da Universidade Politécnica do Brooklyn, onde o servidor DNS local padrão é dns-prime.poly.edu. Quando o nslookup é executado, se o servidor DNs não é especificado, então o nslookup envia a consulta para o servidor DNS padrão, que neste caso é dns-prime.poly.edu. Considere o primeiro comando:

nslookup www.mit.edu

Em palavras, este comando está dizendo "por favor, me envie o endereço IP do host www.mit.edu". Como mostrado no screenshot, a resposta do comando fornece duas partes de informação: (1) o nome e o endereço IP do servidor DNs que fornece a resposta; e (2) a resposta propriamente dita, que é o nome do host e endereço IP de www.mit.edu. Todavia a resposta vem do servidor DNS local na Universidade Politécnica, é muito possível que este servidor DNS local iterativamente contactou muitos outros servidores DNS para obter a resposta, conforme descrito na Seção 2.5 do livro-texto.

Agora considere o segundo comando:

nslookup -type=NS mit.edu

Neste exemplo, nós fornecemos a opção "-type=NS" e o domínio "mit.edu". Isso obriga o nslookup a enviar uma consulta pelo tipo de registro NS para o servidor DNS local padrão. Em palavras, essa consulta está dizendo, "por favor, me envie os nomes dos hosts dos DNS autoritativos de mit.edu".(quando a opção -type não é usada, o nslookup usa o padrão, que é consultar pelo tipo de registro A). A resposta, exibida no screenshot acima, primeiro indica o servidor DNS que está fornecendo a informação (que é o servidor DNS local padrão) juntamente com os três servidores de nome do MIT. Cada um desses servidores é defato um servidor DNS autoritativo para os hosts do

campus do MIT. Todavia, o nslookup também indica que a resposta é "não-autoritativa", significando que esta resposta vem do cache de algum servidor ao invés do servidor DNS autoritativo do MIT. (Apesar da consulta do tipo NS gerada pelo nslookup não ter perguntado explicitamento pelo endereço IP, o servidor DNS local retornou essa informações "gratuitamente" e o nslookup exibe o resultado).

Agora, finalmente, considere o terceiro comando:

nslookup www.aiit.or.kr bitsy.mit.edu

Neste exemplo, nós indicamos que nós queremos que a consulta seja enviada ao servidor DNS bitsy.mit.edu ao invés do servidor DNS padrão (dns-prime.poly.edu). Assim, a transação de consulta e resposta ocorre diretamente entre o host que está consultando e bitsy.mit.edu. Neste exemplo, o servidor DNS bitsy.mit.edu fornece o endereço IP do host www.aiit.or.kr, que é um servidor web no Instituto Avançado de Tecnologia da Informação (na Córea).

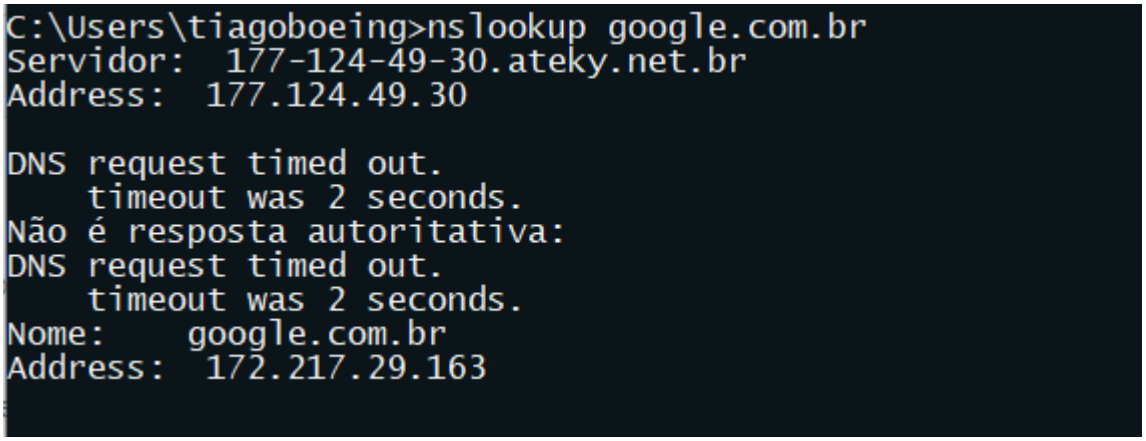
Agora que nós já passamos por alguns exemplos ilustrativos, você talvez esteja se perguntando sobre a sintaxe geral dos comandos do nslookup. A sintaxe é:

nslookup -option1 -option2 host_procurado servidor_dns

Em geral, o nslookup pode ser executado com zero, um, dois ou mais opções. E como nós vimos nos exemplos acima, o servidor dns é opcional também. Se ele não é fornecido, a consulta é enviada para o servidor DNS local padrão.

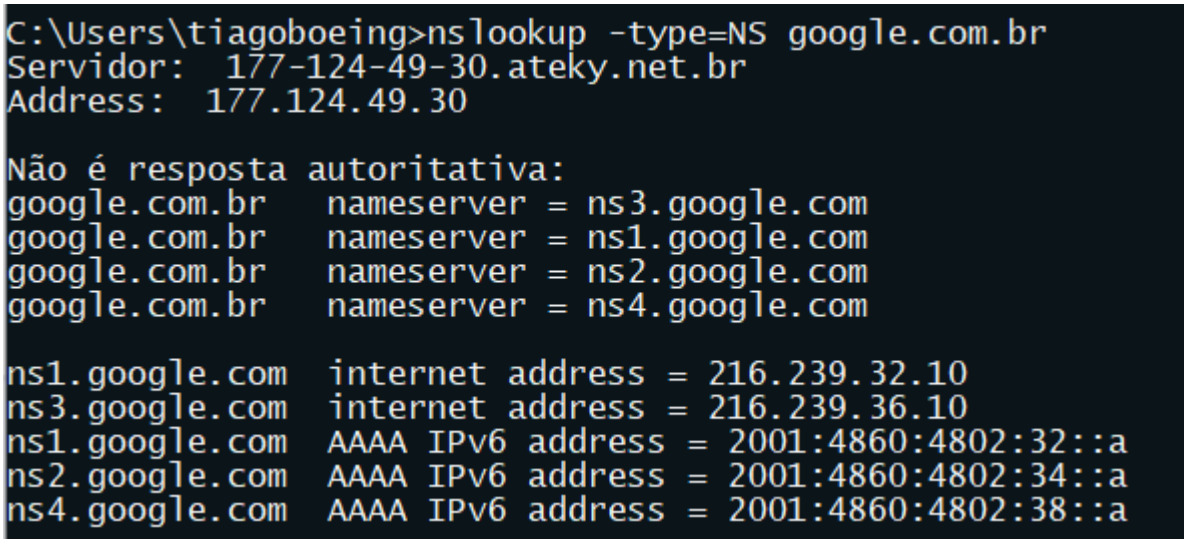
Agora que nós fornecemos uma visão geral do nslookup, é hora de você mesmo testar. Faça o seguinte (e escreva abaixo os resultados):

1. Execute nslookup para obter o endereço IP de um servidor Web no Brasil.



Para confirmar basta acessar o registro A diretamente e conferir que o mesmo se refere ao Google Brasil: 172.217.29.163

2. Execute nslookup para determinar o servidor de autoridade DNS para um endereço IP qualquer.



Percebemos que o google.com é o servidor autoritário do google.com.br e através de um balanceador de carga o tráfego é redirecionado de acordo com a região demográfica em que o acesso foi originado.

2 IPCONFIG

O ipconfig (para Windows) e ifconfig (para Linux/Unix) são, talvez, os pequenos utilitários mais úteis no seu computador, especialmente para depurar problemas de rede. Aqui vamos apenas descrever o ipconfig, uma vez que o ifconfig no Linux/Unix é muito parecido. O ipconfig pode ser usado para mostrar as informações TCP/IP atuais, incluindo seu endereço, endereço de servidor DNS, tipo de adaptador e assim por diante. Por exemplo, você pode ter todas as informações sobre o seu computador digitando simplesmente

3. *ipconfig /all*

no Prompt de comando conforme mostrado no screenshot abaixo:

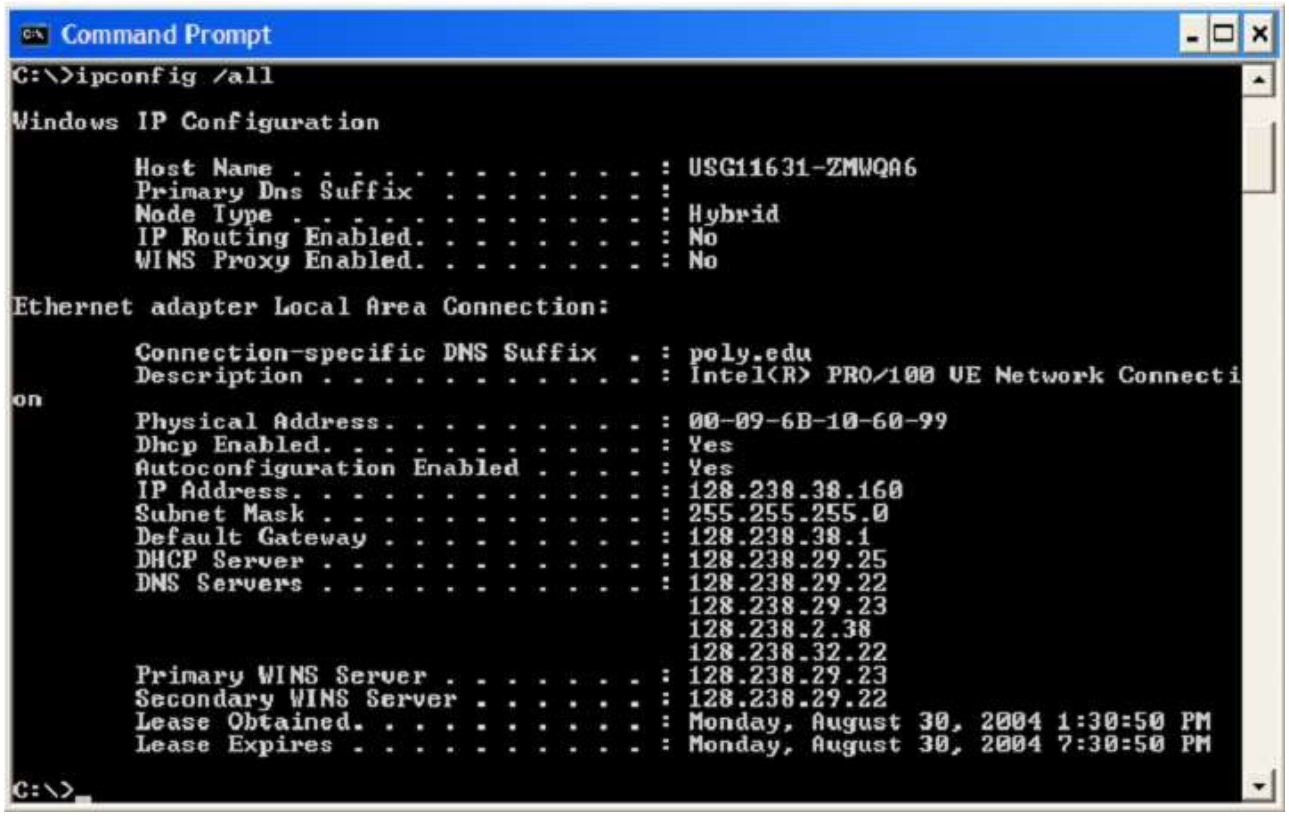


Figura 2

O ipconfig também é muito útil para gerenciar as informações DNS armazenadas no seu computador. Na seção 2.5 nós aprendemos que um host pode colocar registros DNS em cache que foram recentemente obtidos. Para ver esses registros em cache, depois do prompt C:\> forneça o seguinte comando:

4. *ipconfig /displaydns*

```
    Nome do Registro. . . . . : ns1.google.com
    Tipo de Registro. . . . . : 28
    Tempo de Vida . . . . . : 21
    Comprimento dos Dados . . . . . : 16
  Seção. . . . . : Adicional
  Registro AAAA. . . . . : 2001:4860:4802:32::a

    Nome do Registro. . . . . : ns3.google.com
    Tipo de Registro. . . . . : 28
    Tempo de Vida . . . . . : 21
    Comprimento dos Dados . . . . . : 16
  Seção. . . . . : Adicional
  Registro AAAA. . . . . : 2001:4860:4802:36::a

    Nome do Registro. . . . . : ns4.google.com
    Tipo de Registro. . . . . : 28
    Tempo de Vida . . . . . : 21
    Comprimento dos Dados . . . . . : 16
  Seção. . . . . : Adicional
  Registro AAAA. . . . . : 2001:4860:4802:38::a
```

Cada entrada mostra o tempo de vida (TTL) restante em segundos. Para limpar o cache, digite:

5. *ipconfig /flushdns*

Não pretendo fazer isto neste momento.

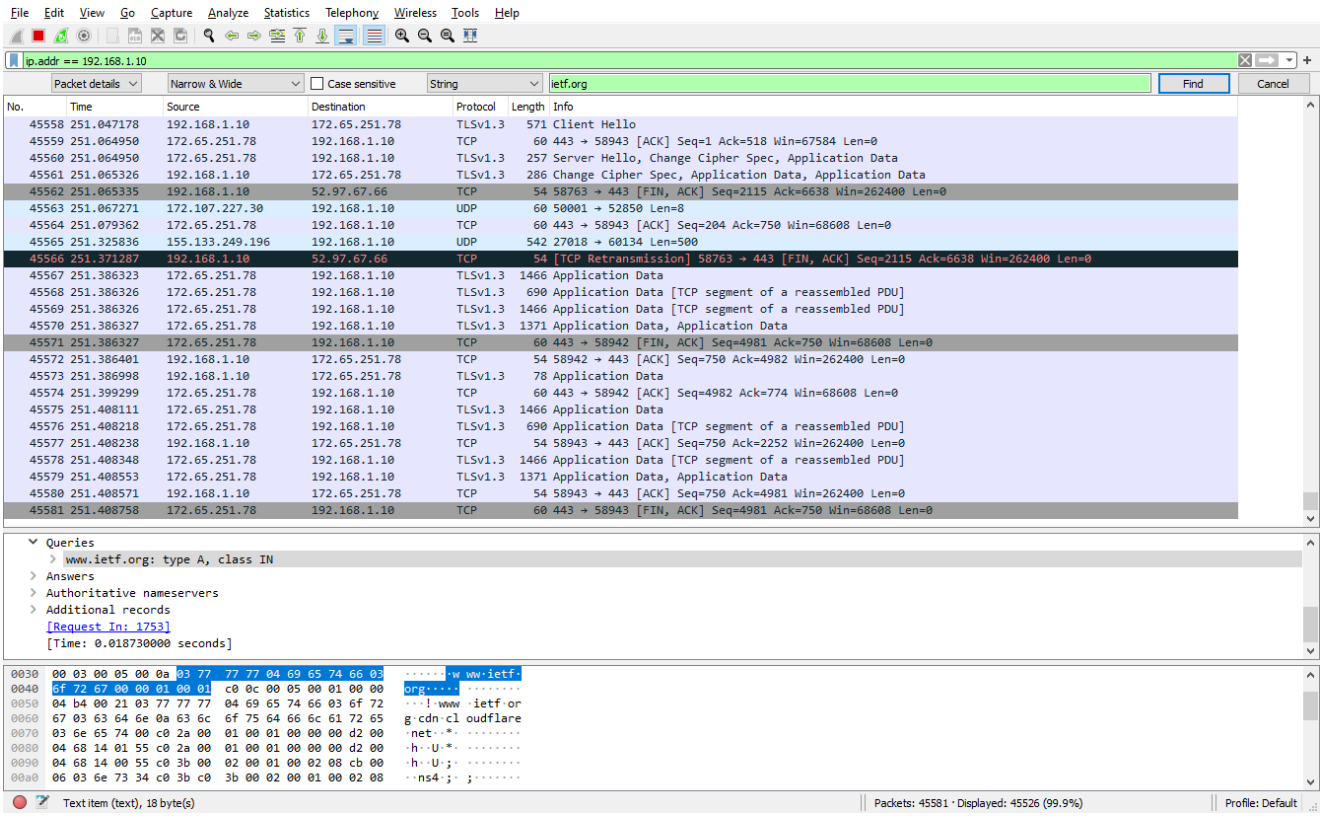
Limpar o cache DNS apaga todas as entradas e recarrega as entrada do arquivo hosts.

3 ANALISANDO O DNS COM O WIRESHARK

Agora que nós estamos familiarizados o nslookup e o ipconfig, nós estamos prontos para começar algo mais sério. Vamos primeiro capturar os pacotes de DNS que são gerados pela atividade de navegação na Web comum.

4 Use o ipconfig para limpar o cache DNS no seu computador. (ipconfig /flushdns)

- Abra o seu navegador e limpe o cache do seu navegador. (Com o Internet Explorer, vá no menu ferramentas e selecione as Opções de Internet; Então na aba Geral, selecione Deletar arquivos).
- Abra o Wireshark e digite "ip.addr == seu_endereço_IP" no campo "filter", o seu endereço IP você obtém com o ipconfig. Este filtro remove todos os pacotes que não se originam nem são destinados para o seu computador.
- Inicie a captura de pacote no Wireshark.
- Com o seu navegador, visite a página Web: http://www.ietf.org



Capturei os pacotes de filtrei pelo conteúdo dos mesmos, garantindo que apenas os destinados ao site sejam exibidos.

- Para a captura de pacote.

Se você não puder executar o Wireshark em uma rede com conexão à Internet, você pode baixar um arquivo que foi capturado seguindo os passos acima em um dos computadores do autor[1].

Respondas as seguintes perguntas:

6. Localize as mensagens de consulta e resposta DNS. Elas são enviadas através do UDPou TCP?

As consultas de DNS são UDP e a transferência de zona é TCP. A porta padrão do DNS é a 53. Adicional: devido a porta utilizada o serviço de gerenciamento de DNS da AWS se chama Route 53.

7. Qual a porta de destino para a mensagem de consulta DNS? Qual é a porta de origem da mensagem de resposta DNS?

Origem e destino utilizam a mesma porta (53).

8. Examine a mensagem de consulta DNS. Qual o "Tipo" de consulta DNS é? A mensagem de consulta contém algumas "respostas (answers)"?

Consulta registros do tipo A . A mensagem não contém respostas.

Agora vamos brincar com o nslookup[2].

- Inicie a captura de pacote.
- Faça um nslookup para www.mit.edu
- Pare a captura de pacote.

Você deve obter uma captura que parece com o seguinte:

[1] Baixe o arquivo zip http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip e extraia o arquivo dns-ethereal-trace-1. O rastreio no arquivo zip foi coletado pelo Wireshark em um dos computadores do autor enquanto realizava os passos indicados no laboratório Wireshark. Uma vez que você tenha baixado o arquivo, você pode abri-lo no Wireshark e visualizá-lo usando o menu File, escolhendo a opção Open, e então selecionando o arquivo dns-ethereal-trace-1.

[2] Se você não conseguir executar o Wireshark e capturar pacotes, use o arquivo dns-ethereal-trace-2 do arquivo zip http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip.

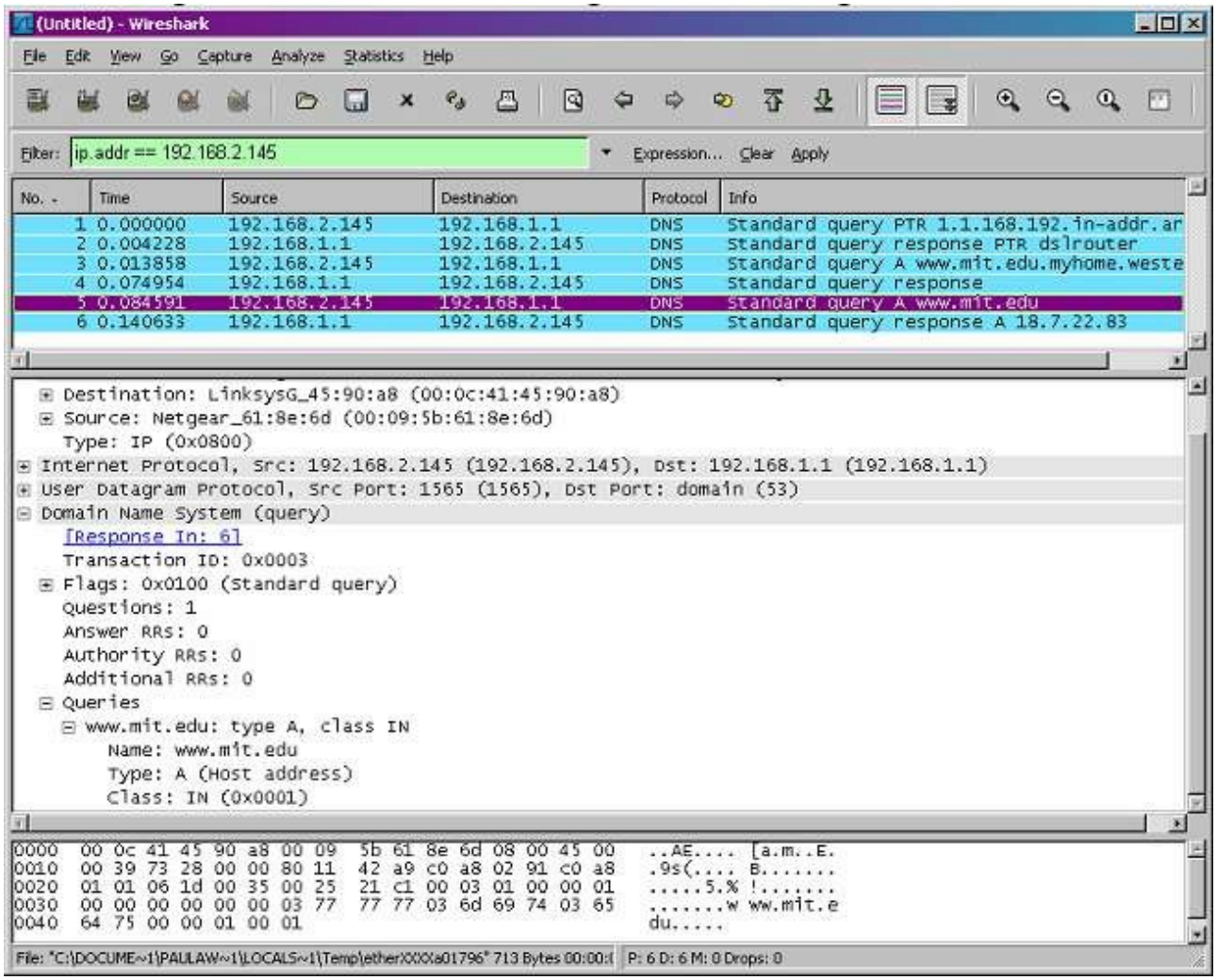


Figura 3

Nós vemos no screenshot acima que o nslookup realmente envia três perguntas DNS e recebe três respostas DNS. Pelo objetivo do exercício, ao responder as perguntas seguintes, ignore os dois primeiros conjuntos de consultas/respostas, pois eles são específicos para o nslookup e normalmente não são gerados por aplicações padrão da Internet. Ao invés disso, você deve focar nas últimas mensagens de consulta e resposta.

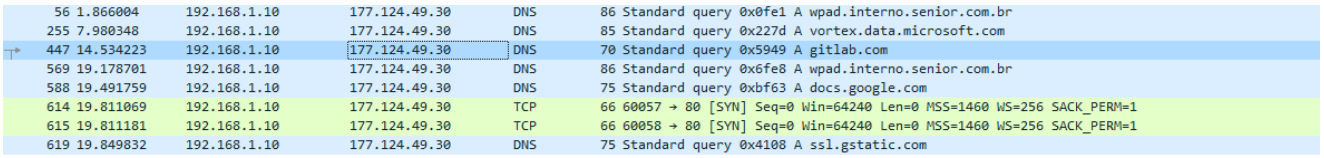
9. Qual a porta de destino da mensagem de consulta DNS? Qual é a porta de origem da mensagem de resposta DNS?

No meu caso por ter VPN configurada e a mesma realiza algumas modificações no DNS. A porta destino é a 53 e a origem é a 63958.

```
User Datagram Protocol, Src Port: 63958, Dst Port: 53
    Source Port: 63958
    Destination Port: 53
    Length: 59
    Checksum: 0x4a7a [unverified]
    [Checksum Status: Unverified]
    [Stream index: 10]
  > [Timestamps]
Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    > www.mit.edu.interno.senior.com.br: type A, class IN
```

10. Para qual endereço IP a mensagem de consulta DNS é enviada? Esse é o endereço IP do seu servidor DNS local padrão?

A consulta foi enviada para 177.124.49.30 . Sim é o DNS interno do provedor de internet.



56	1.866004	192.168.1.10	177.124.49.30	DNS	86 Standard query 0x0fe1 A wpad.interno.senior.com.br
255	7.980348	192.168.1.10	177.124.49.30	DNS	85 Standard query 0x227d A vortex.data.microsoft.com
447	14.534223	192.168.1.10	177.124.49.30	DNS	70 Standard query 0x5949 A gitlab.com
569	19.178701	192.168.1.10	177.124.49.30	DNS	86 Standard query 0x6fe8 A wpad.interno.senior.com.br
588	19.491759	192.168.1.10	177.124.49.30	DNS	75 Standard query 0xbf63 A docs.google.com
614	19.811069	192.168.1.10	177.124.49.30	TCP	66 60057 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
615	19.811181	192.168.1.10	177.124.49.30	TCP	66 60058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
619	19.849832	192.168.1.10	177.124.49.30	DNS	75 Standard query 0x4108 A ssl.gstatic.com

11. Examine a mensagem de consulta DNS. Qual o "tipo" de consulta DNS? A mensagem de consulta contém alguma "resposta (answers)"?

Não há resposta e a consulta é do tipo A (host address) (1).

[3] Se você não conseguir executar o Wireshark e capturar pacotes, use o arquivo dns-ethereal-trace-3 do arquivo zip http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip.

[4] Se você não conseguir executar o Wireshark e capturar pacotes, use o arquivo dns-ethereal-trace-4 do arquivo zip http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip.