LABORATÓRIO WIRESHARK: DNS

Conforme descrito na seção 2.5 do livro, 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. Como mostrado nas Figuras 2.21 e 2.22 no livro, muito pode continuar "sob as cobertas", invisível para os clientes DNS, como os servidores DNS hierárquicos comunicam-se uns com os outros, quer de forma recursiva ou iterativa resolvendo consultas DNS do cliente. Do ponto de vista do cliente de DNS, no entanto, o protocolo é muito simples - uma consulta é formulado com o servidor de DNS local e é recebida uma resposta do servidor.

Antes de iniciar este laboratório, você provavelmente vai querer rever o DNS lendo a Seção 2.5 do texto. Em particular, você pode querer rever o material de servidores locais DNS, cache DNS, registros DNS e mensagens e o campo TYPE no registro DNS.

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. 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.

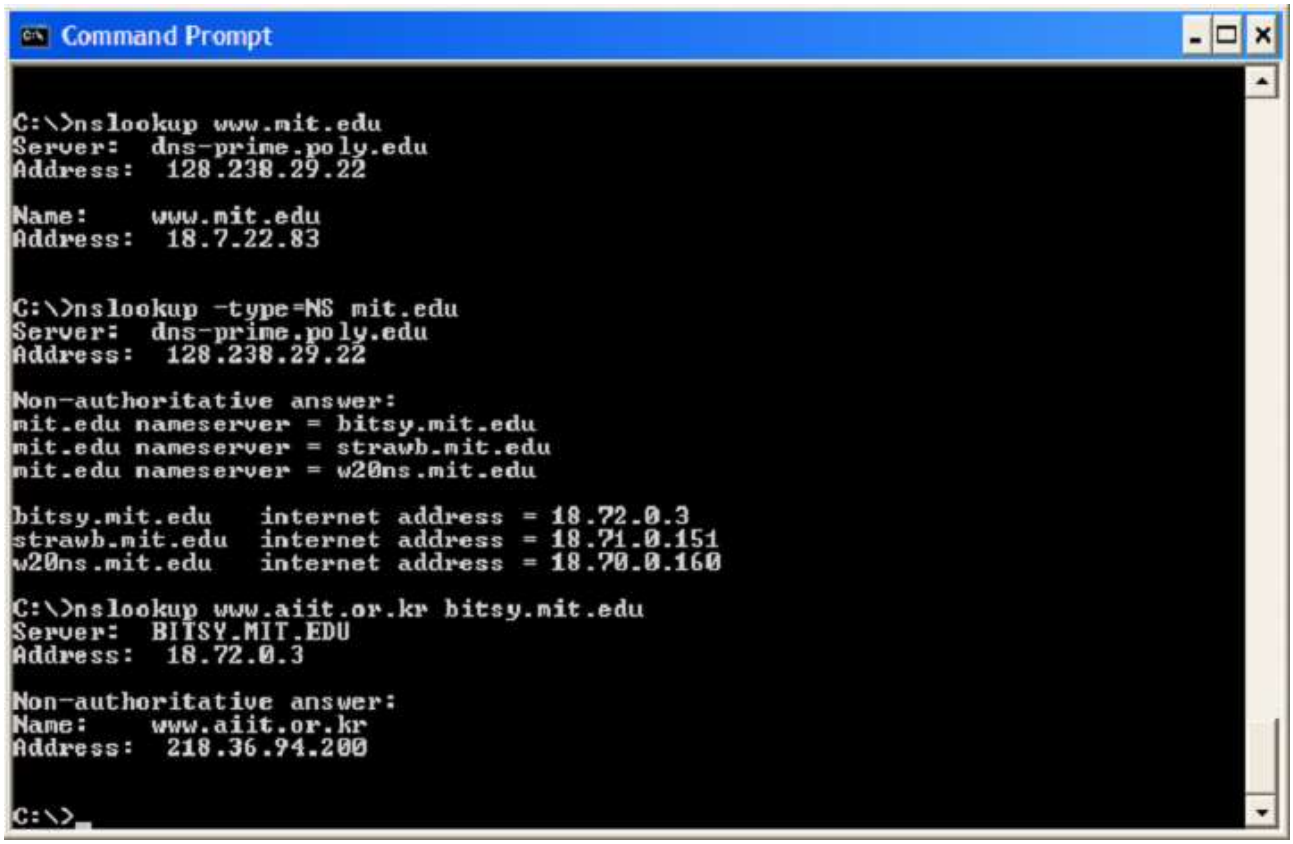

Figura 1

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):

a. Execute o nslookup para obter o endereço IP de um servidor Web na Asia.
b. Execute o nslookup para determinar os servidores autoritativos de uma universidade na Europa.
c. Execute o nslookup para que um dos servidores DNS obtidos na questão 2 consulte pelos servidores de correio do Yahoo!

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

ipconfig /all

no Prompt de comando conforme mostrado no screenshot abaixo:

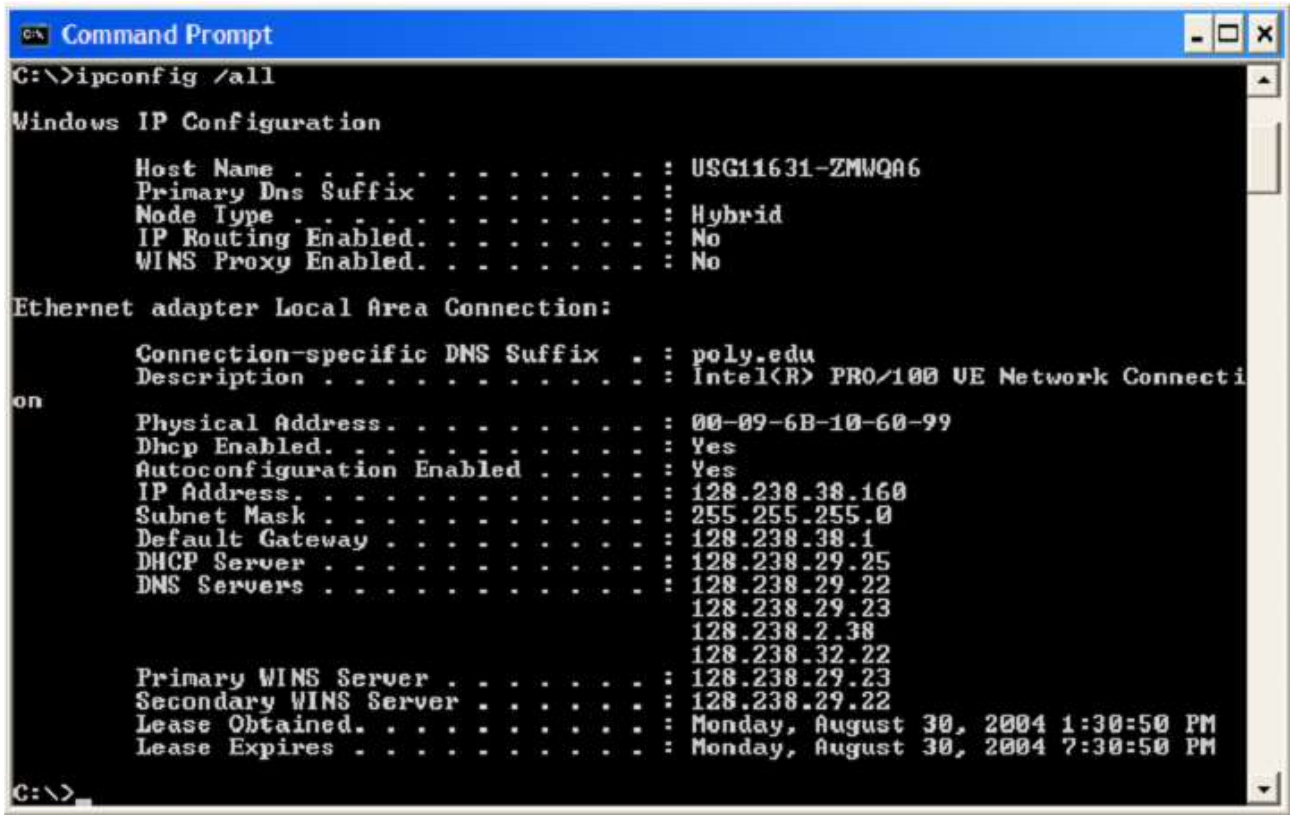

Figura 2

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:

ipconfig /displaydns

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

ipconfig /flushdns

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.

1. Use o ipconfig para limpar o cache DNS no seu computador.
2. 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).
3. 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.
4. Inicie a captura de pacote no Wireshark.
5. Com o seu navegador, visite a página Web: http://www.ietf.org

6. 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:

d. Localize as mensagens de consulta e resposta DNS. Elas são enviadas através do UDP ou TCP?
e. Qual a porta de destino para a mensagem de consulta DNS? Qual é a porta de origem da mensagem de resposta DNS?
f. Para qual endereço IP a mensagem de consulta DNS é enviada? Use o ipconfig para determinar o endereço IP do seu servidor DNS local. Esses dois endereços IP são os mesmos?
g. Examine a mensagem de consulta DNS. Qual o "Tipo" de consulta DNS é? A mensagem de consulta contém algumas "respostas (answers)"?
h. Examine a mensagem de resposta DNS. Quantas "respostas (answers)" são fornecidas? O que cada resposta contém?
i. Considere o pacote SYN TCP subsequente enviado pelo seu computador. O endereço IP do pacote SYN corresponde a algum endereço IP fornecido na mensagem de resposta DNS?
j. Esta página web contém imagens. Antes de obter cada imagem, o seu computador faz novas consultas DNS?

Agora vamos brincar com o nslookup[2].

1. Inicie a captura de pacote.
2. Faça um nslookup para www.mit.edu
3. 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.

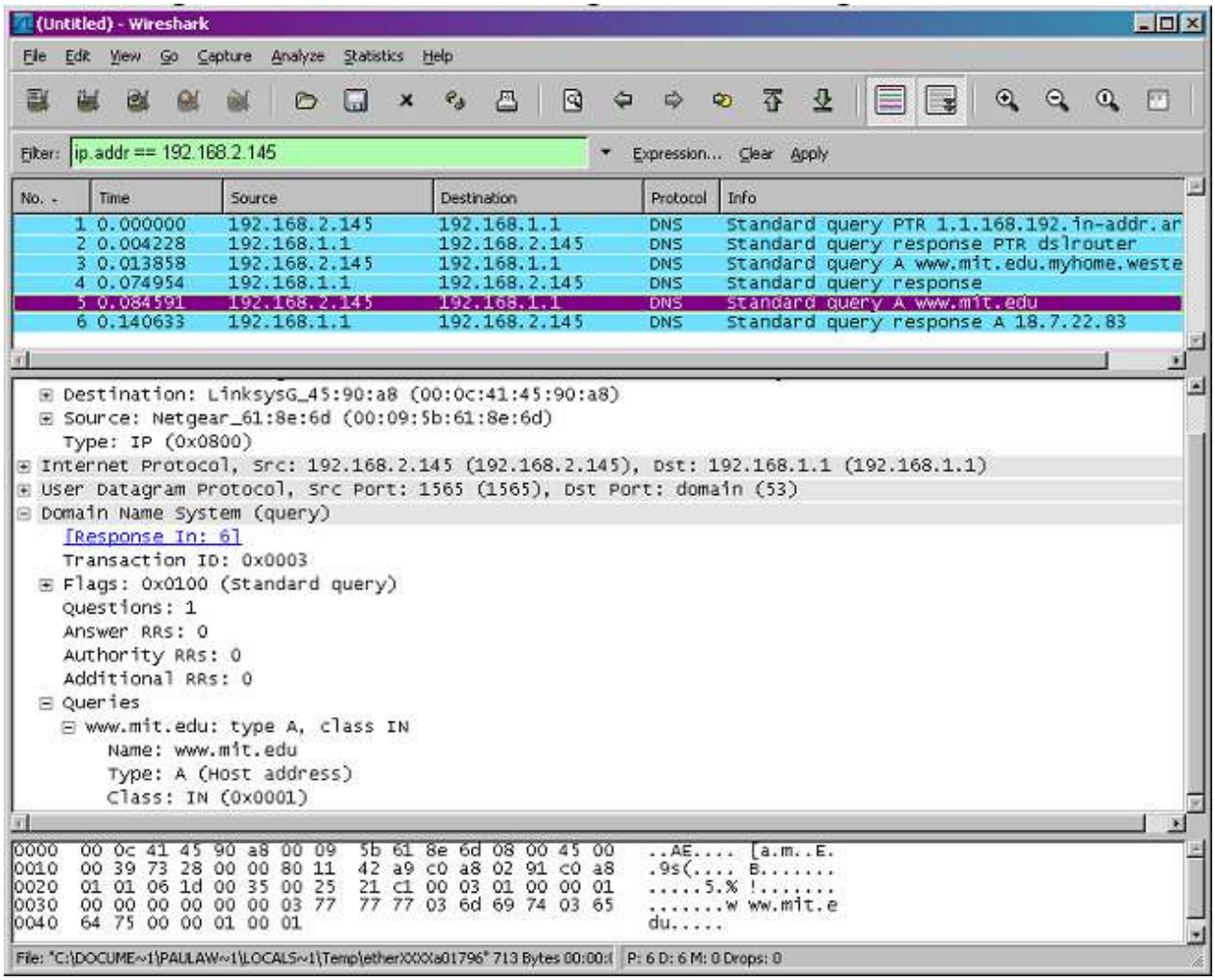

Figura 3

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.

k. Qual a porta de destino da mensagem de consulta DNS? Qual é a porta de origem da mensagem de resposta DNS?
l. Para qual endereço IP a mensagem de consulta DNS é enviada? Esse é o endereço IP do seu servidor DNS local padrão?
m. Examine a mensagem de consulta DNS. Qual o "tipo" de consulta DNS? A mensagem de consulta contém alguma "resposta (answers)"?
n. Examine a mensagem de resposta DNS. Quantas "respostas (answers)" são fornecidas? O que cada uma dessas respostas contém?

Agora repita o experimento anterior, mas, dessa vez, digite o comando:

nslookup -type=NS mit.edu

Responda as seguintes perguntas[3]:

o. Para qual endereço IP a mensagem de consulta DNS é enviada? Esse é o endereço IP do seu servidor DNS local padrão?
p. Examine a mensagem de consulta DNS. Qual o "tipo" de consulta DNS? A mensagem de consulta contém alguma "resposta (answers)"?
q. Examine a mensagem de resposta DNS. Quais servidores de nomes do MIT a resposta fornece? A mensagem de resposta também fornece os endereços IP dos servidores de nomes do MIT?

Agora repita o experimento anterior, mas, dessa vez, digite o comando:

nslookup bitsy.mit.edu asia1.akam.net

Responda as seguintes perguntas[4]:

r. Para qual endereço IP a mensagem de consulta DNS é enviada? Este é o endereço IP do seu servidor DNS local padrão? Se não, a que esse endereço IP corresponde?
s. Examine a mensagem de consulta DNS. Qual o "tipo" de consulta DNS? A mensagem de consulta contém alguma "resposta (answers)"?
t. Examine a mensagem de resposta DNS. Quantas "respostas (answers)" são fornecidas? O que cada uma dessas respostas contém?

[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.