Wireshark Lab: DNS

Versão 1.2

Tradução e adaptação para Wreshark.

Como descrito na seção 2.4 ou 2.5 do livro (dependendo da edição), o Domain Name System (DNS) traduz nomes de hosts em endereços Internet Protocol (IP), preenchendo uma lacuna crítica na infraestrutura da Internet. Neste laboratório, observaremos de mais perto o lado cliente do DNS. Lembre-se de que o papel do cliente no DNS é relativamente simples - um Cliente envia uma consulta ao seu DNS, e obtém uma resposta. Como exibido na figura 2.16 e 2.18 no livro (depende da edição a numeração das figuras pode ser outro), muito pode acontecer "por baixo dos panos", de forma invisível aos clientes DNS, enquanto os servidores DNS, organizados hierarquicamente, comunicam-se entre si para, recursivamente ou iterativamente, resolver uma consulta DNS de um cliente. Do ponto de vista do cliente DNS, contudo, o protocolo é bastante simples - uma consulta é feita ao seu servidor DNS e uma resposta é recebida deste servidor.

Antes de iniciar este laboratório, você provavelmente desejará revisar DNS lendo a seção 2.5 no livro. Em particular, você deve revisar os materiais: servidores DNS locais, cache DNS, mensagens e registros DNS e o campo TYPE no registro DNS.

1. nslookup

Neste laboratório, faremos um uso extensivo da ferramenta nslookup, que está disponível na maioria dos sistemas operacionais atuais, sejam Windows, Linux ou Unix. Para executar nslookup no Linux ou Unix, basta digitar nslookup em uma linha de comando. Para executá-lo no Windows, abra o Prompt de Comando e digite nslookup na linha de comando.

No seu modo de operação mais básico, nslookup permite que o host que o execute consulte qualquer servidor DNS para obter um registro. O servidor DNS consultado pode ser um servidor raiz, um servidor DNS responsável por um domínio, um servidor DNS autoritário, ou um servidor DNS intermediário (veja o livro para as definições destes termos). Para realizar esta tarefa, o nslookup envia uma consulta DNS ao servidor especificado e recebe uma resposta do mesmo servidor, exibindo o resultado no vídeo. As figuras 1, 2 e 3 mostram o resultado de três comandos nslookup independentes linha de comando do Linux). Nestas figuras, o host cliente é o laptop do Prof. Marco em seu dispositivo pessoal, sendo o servidor DNS padrão o endereço IP 172.17.0.18 (ns.pucmg.br).

Quando executa-se nslookup sem um servidor DNS especificado, ele consulta o servidor DNS padrão, que neste caso é ns.pucmg.br.

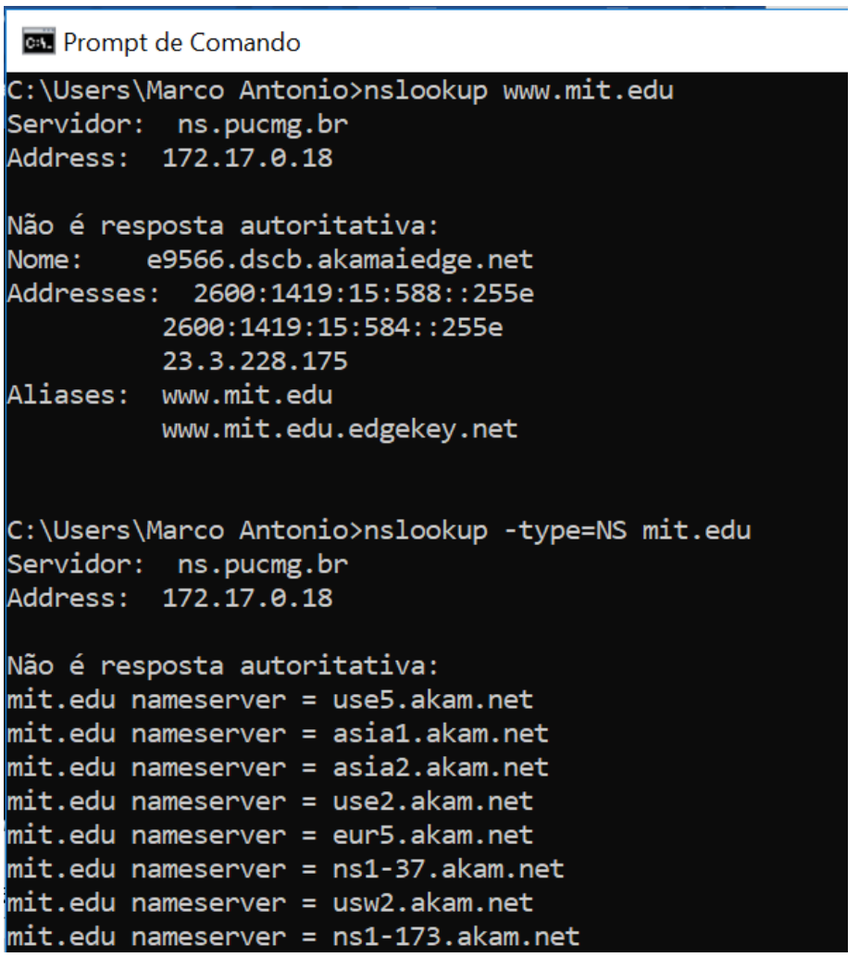

Figura 1. Primeiro exemplo de uso do nslookup

O screenshot da figura 1, mostra o resultado de dois comandos nslookup independentes. Neste exemplo, em particular, o servidor está localizado no campus da PUC Minas no Coração Eucarístico e atende a rede wifi e de laboratórios da instituição.

Em palavras, o primeiro comando “nslookup www.mit.edu” diz "por favor, envie-me o endereço IP do host www.mit.edu". A resposta exibida na mesma figura para este comando fornece duas informações:

- o nome e endereço IP do servidor DNS que foi consultado; (servidor: ns.pucmg.br, ip 172.17.0.18)
- a resposta em si, que é o nome do host o endereço IP. (e9655...., com dois ips da versão 6 e um ip da versão 4, com os alias desses nomes)
  O segundo comando “nslookup -type=NS mit.edu”, foi passado o parâmetro -type=NS (NameServer), logo esta pergunta quis dizer “por favor, envie-me o endereço(s) ip(s) do(s) servidor(es) autoritativo(s) de DNS para o domínio mit.edu”. Quando a opção -type não é utilizada, o nslookup usa o padrão, que é consultar por registros do tipo A e AAAA. A resposta exibida na mesma figura para este comando fornece duas informações:
- o nome e endereço IP do servidor DNS que foi consultado; (servidor: ns.pucmg.br, ip 172.17.0.18)
- a resposta em si, que é o nome dos hosts que estão configurados com este domínio, em particular 8 servidores para este caso. (use5.akam.net, asia1.....). O fato do nslookup indicar que a resposta é “não autoritária” significa que a resposta veio do cache de algum servidor ao invés de um servidor DNS autoritário do MIT.

Embora a resposta venha do servidor ns.pucmg.br, é bem possível que este servidor DNS tenha contatado diversos outros servidores DNS para obter a resposta, como descrito no livro e explicado pelo professor em sala de aula.

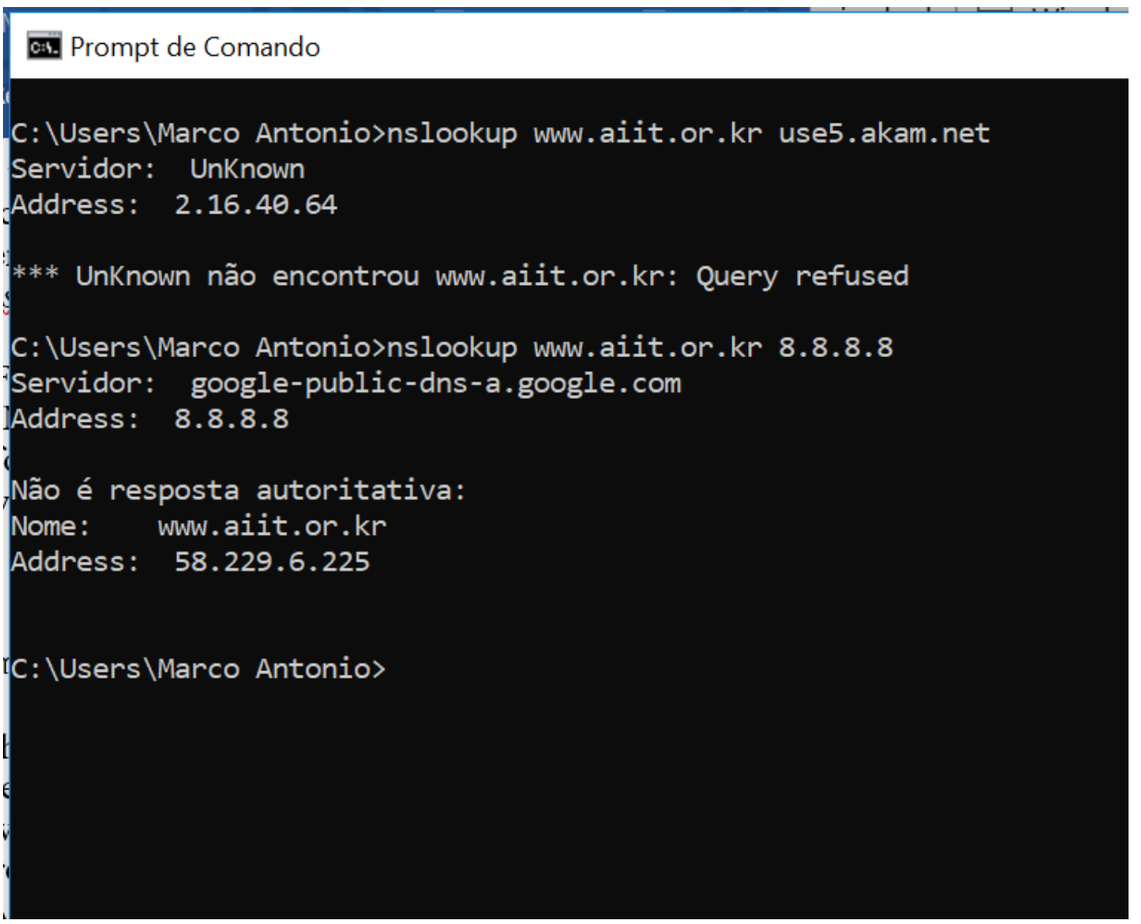

Figura 2. Mais dosi exemplos do uso do nslookup

Na figura 2, operamos mais dois comandos nslookup com o mesmo objetivo. Ambos querem descobrir o endereço ip do domínio www.aiit.or.kr, mas disparando a pergunta para outros servidores que não o padrão de nosso computador.

No caso do comando “nslookup www.aiit.or.kr use5.akam.net.” o objetivo foi pedir ao servidor use5.akam.net que ele retornasse o endereço ip do www.aiit.or.kr, como pode ser visto o servidor recusou a consulta “Query refused”, isto provavelmente aconteceu por causa de uma configuração local no servidor use5.akam.net. que define para quais blocos de ip este servidor atende as consultas, isto com o intuito de reduzir a carga no mesmo.

Já o comando “nslookup www.aiit.or.kr 8.8.8.8” direcionou a consulta para o servidor de DNS público da Google (8.8.8.8) e a resposta obtida foi o ip 58.229.6.225.

Agora que já passamos por alguns exemplos ilustrados, talvez você esteja se perguntando sobre a sintaxe genérica do cornando nolookup, A sintaxe é:

nslookup -opçáo1 -opção2 host-a-encontrar servidor-dns

Geralmente, o nslookup pode ser executado com nenhuma, uma, duas ou mais opções. Como vimos nos exemplos das figuras 1 e 2, o parâmetro servidor-dns é opcional'; se ele não é informado, a consulta é enviada ao servidor DNS local,

Agora que revisamos o comando nglookup, está na hora do você testá-lo sozinho.

Execute o nslookup para cada uma das questões, o escreva os resultados:

1. obtenha o endereço JP de um servidor wob na Ásia;
2. determine os servidores DNS autoritários para uma universidade na Europa;
3. utilize um dos servidores DNS obtido na questão 2 e consulte pelo endereço IP do Portal Office365.

2. ipconfig ou ifconfig

ipconfig, no Windows, e ifconfig, no Linux ou Unix, estão entre as mais úteis ferramentas de rede no seu host, especialmente para depuração. Esta seção está dividida em duas partes, uma que explica o ipconfig no Windows, e outra que explica o ifconfig no Linux.

2.1. ipconfig

0 comando ipconfig pode ser utilizado para mostrar a informação TCP/IP atual, incluindo: endereço IP, endereço de servidores DNS locais, tipo de adaptador de rede, entre outras. por exemplo, todas as informações de um host podem ser obtidas através da digitação no prompt de comando de ipconfig /all (figura 3).

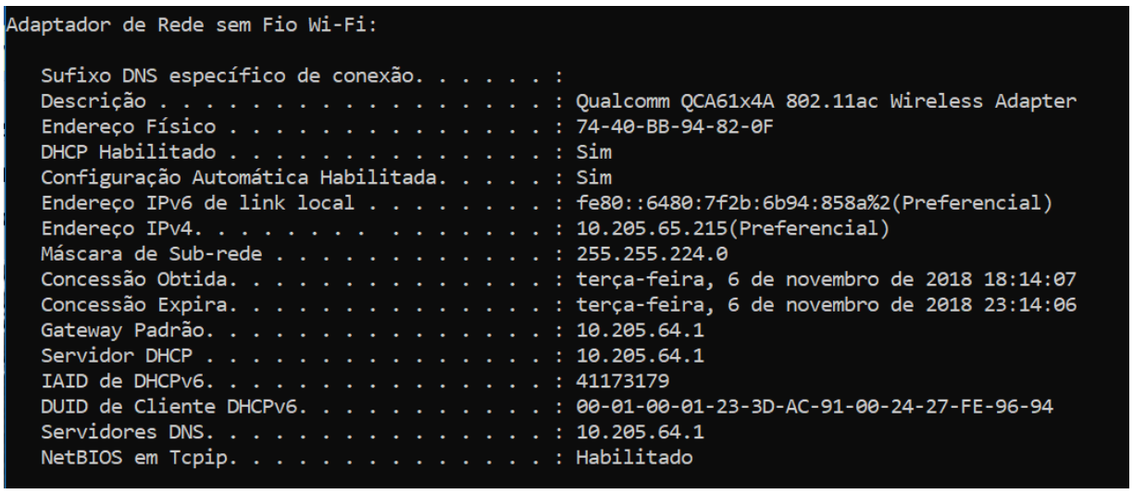

Figura 3. Resultado parcial do comando ipconfig /all

O comando ipconfig também é bastante útil para exibir as informações do DNS armazenados no host. Na seção 2.5, aprendemos que um host pode gravar em cache os registros de DNS obtidos recentemente. Para ver os registros gravados em cache, basta digitar na linha de comando:

ipconfig /displaydns

Cada entrada mostra o tempo de vida (TTL) restante em segundos. Para limpar o cache, digita-se

ipconfig /flushdns

Limpar o cache faz com que todas as entradas sejam apagadas e recarrega as entradas do arquivo hosts. Estes comandos funcionam no Windows porque ele executa automaticamente um servidor DNS cache no host.

Na figura 4, mostramos um exemplo de saída do comando “ipconfig /displaydns” nesta saída vemos dois registros que estão em cache do computador usado, ambas traduções são de endereços do Windows Update e que permanecerão na cache por mais 3 segundos (circulado na figura 4).

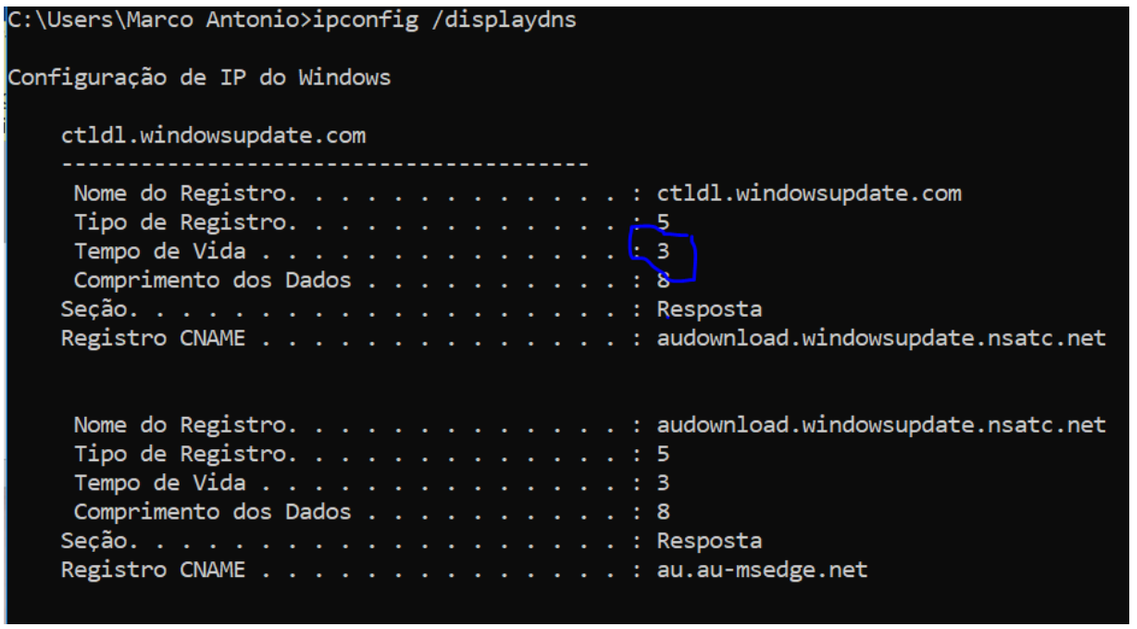

Figura 4. Exemplo de saída do comando ipconfig /displaydns

3. Rastreando DNS com o Wireshark

Agora que nos familiarizamos com o nslookup e ipconfig, estamos prontos para botar as mãos na massa. Inicialmente vamos capturar as mensagens DNS que são geradas por uma navegação na web. Para isso, siga os passos:

- utilize ipconfig para limpar o cache DNS do host;
- abra o navegador web e limpe o cache do mesmo;
- abra o Wireshark e digite "ip.addr == seu_endereço_IP" no filtro (sem as aspas). Este filtro só mostra os pacotes que ou são originados ou destinados ao seu host;
- inicie a captura de pacotes no Wireshark;
- no navegador web, visite a página http://www.ietf.org;
- pare a captura de pacotes.

Responda às questões:

4. localize as mensagens de solicitação e resposta DNS. Foram enviadas com TCP ou UDP?
5. qual é a porta destino para a mensagem de consulta DNS? Qual é a porta fonte da mensagem de resposta DNS?
6. a qual endereço IP a mensagem de consulta DNS é enviada? Utilize ipconfig para verificar qual é o endereço IP do seu servidor DNS local. Estes endereços são os mesmos?
7. examine a mensagem de consulta DNS. Qual o campo "type" desta mensagem? A mensagem de consulta contém algum campo "answer'?

8. examine a mensagem de resposta DNS. Quantos campos com "answer' existem? O que há em cada uma destas mensagens?
9. considere o segmento TCP SYN subsequente enviado pelo seu host. O endereço IP de destino do pacote SYN corresponde a algum dos endereços IP fornecidos na mensagem de resposta DNS?
10. a página web visitada contém imagens. Antes de recuperar cada imagem, o host realiza novas consultas DNS?

Salve esta captura com o nome dns4a10.pcap para entrega ao professor pelo SGA.

Agora vamos brincar com o nslookup. Siga os passos:

- adicione ao filtro " && dns", sem as aspas;
- inicie a captura de pacotes;
- execute o comando "nslookup www.mit.edu", sem as aspas;
- pare a captura de pacotes.

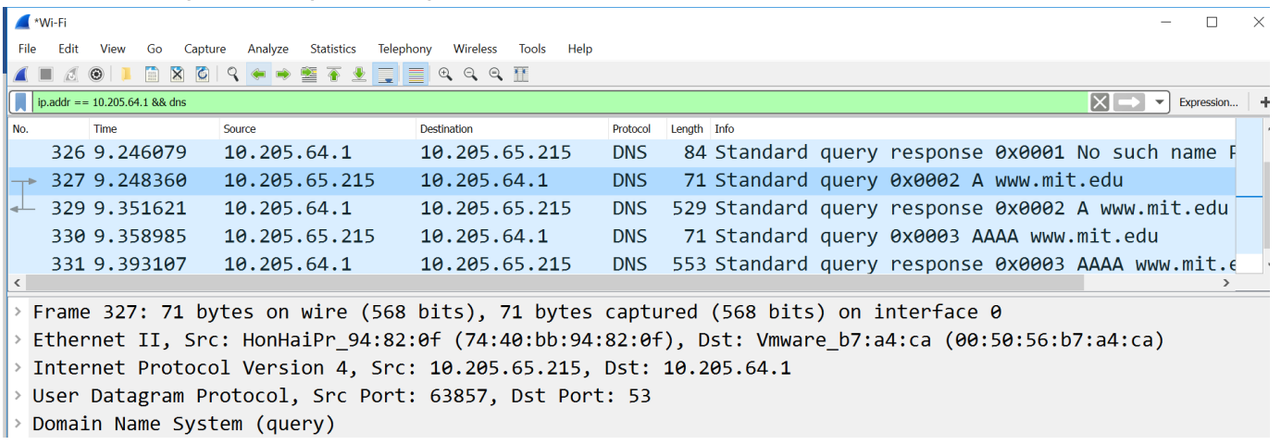

Figura 5. Captura dos pacotes para "nslookup www.mit.edu"

A figura 5 mostra o resultado da captura dos pacotes exemplo feitas pelo professor. Veja que foram colocados o ip.addr == 10.205.64.1 e o protocolo DNS. Olhando a primeira coluna nós podemos ver o número do pacote. O de número 327 foi a consulta do tipo A para o domínio www.mit.edu, o pacote de número 329 foi a resposta, já o 330 e 331 são a pergunta e reposta para o registro tipo AAAA, ou seja a tentativa de descoberta do IPv6.

Agora conferindo a sua captura, nela estão a mensagem de consulta e a resposta DNS de seu experimento. Responda às questões:

11. qual é a porta destino para a mensagem de consulta DNS? Qual é a porta fonte para a mensagem de resposta DNS?
12. a qual endereço IP a mensagem de consulta DNS está endereçada? Este endereço é o de algum dos seus servidores DNS locais?
13. examine a mensagem de consulta DNS. Qual o campo "type" que há nela? A mensagem de consulta contém algum campo "answer"?
14. examine a mensagem de resposta DNS. Quantos campos com "answer" existem? O que há em cada uma destas respostas?
15. grave a tela de captura de pacotes, assim como foi feita na figura 5 de exemplo.

Salve a captura com o nome dns11a15.pcap.

Repita o experimento anterior para o comando: "nslookup -type=NS pucminas.br", sem as aspas. Depois responda às questões:

16. a qual endereço IP a mensagem de consulta DNS está endereçada? Este endereço é o de algum dos seus servidores DNS locais?
17. examine a mensagem de consulta DNS. Qual o campo "type" que há nela? A mensagem de consulta contém algum campo "answer"?
18. examine a mensagem de resposta DNS. Quais servidores DNS da PUC Minas são fornecidos na resposta? Esta mensagem de resposta também fornece os endereços IP dos servidores DNS da PUC Minas?
19. grave a tela de captura de pacotes, assim como da figura 5.

Salve a captura com o nome dns16a19.pcap.

Repita o experimento anterior para o comando: "nslookup www.aiit.or.kr ns.pucminas.br", sem as aspas. Depois responda às questões:

20. a qual endereço IP a mensagem de consulta DNS está endereçada? Este endereço é o de algum dos seus servidores DNS locais? Caso contrário, qual o host para este endereço IP?
21. examine a mensagem de consulta DNS. Qual o campo "type" que há nela? A mensagem de consulta contém algum campo "answer"?
22. examine a mensagem de resposta DNS. Quantos campos com "answer" existem? O que há em cada uma destas respostas?
23. grave a tela de captura de pacotes, assim como a figura 5.

Salve a captura com o nome dns20a23.pcap.