
 INSTITUTO DE INFORMÁTICA UFG	Universidade Federal de Goiás Instituto de Informática	 UFG
Professor: Kleber Vieira Cardoso		
Laboratório: camada de aplicação – DNS		

A menos que haja alguma orientação contrária, os exercícios se referem à máquina virtual (Kali Linux) disponibilizada para uso no VirtualBox (usuário: **root**, senha: **toor**).

Nesta aula de laboratório, a ferramenta **Wireshark** será usada novamente, dessa vez para permitir a captura e análise de pacotes que estejam transportando mensagens da aplicação DNS. Para reduzir a quantidade de pacotes capturados e facilitar a atividade de análise dos pacotes é sugerido o uso de um filtro para capturar apenas pacotes que tenham como origem ou destino o seu computador (`ip.addr == <endereço_IP_do_seu_computador>`). Caso o número de pacotes ainda seja muito grande, acrescente um filtro específico para a aplicação DNS (`dns`).

Há diferentes ferramentas para interagir com o DNS, por exemplo: **dig**, **nslookup** (também disponível no Windows) e **host**. A ferramenta **dig** apresenta a maior quantidade de informações e o faz de uma maneira estruturada, similar à abordagem didática mostrada no livro. Portanto, **dig** será a ferramenta utilizada nos exercícios a seguir.

1. Faça algumas consultas com **dig** e identifique todas as informações apresentadas na figura abaixo. Identifique também o tempo gasto para trazer a resposta (**Query time**).

Identificação	Flags	
Número de perguntas	Número de RRs de resposta	12 bytes
Número de RRs com autoridade	Número de RRs adicionais	
Perguntas (número variável de perguntas)		Nome, campos de tipo para uma consulta
Respostas (número variável de registros de recursos)		RRs de resposta à consulta
Autoridade (número variável de registros de recursos)		Registros para servidores com autoridade
Informação adicional (número variável de registros de recursos)		Informação adicional 'útil', que pode ser usada

- Faça algumas consultas sucessivas para o mesmo nome. Tente escolher algum site diferente dos seus colegas. Há diferença de tempo entre as consultas? Comente.
- Faça algumas consultas sucessivas para o mesmo nome, mas utilizando o servidor de nomes autorizado (ou oficial) do domínio que você está consultando. Verifique o que mudou com relação ao tempo de consulta e as *flags*. Comente.
- Escolha 5 *sites* e encontre os endereços do servidor de nomes e do servidor de *e-mail* de cada um deles.

2. Neste exercício, será utilizado um navegador *Web*. Realize os seguintes passos:

- Inicie um navegador *Web* (**Chrome** ou **Firefox**);
- Aguarde algum tempo após o navegador ter sido iniciado, pois é comum o navegador carregar uma página ou buscar alguma informação sobre atualização e não estamos interessados em capturar esses dados;
- Inicie a captura de pacotes com **Wireshark**;
- Acesse o *site* do IETF (www.ietf.org);
- Pare a captura de pacotes do **Wireshark**.

Responda o que é pedido nas questões a seguir:

- a) Localize a(s) consulta(s) e resposta(s) que utilizem **DNS**. Essas mensagens são transmitidas sobre UDP ou TCP?
- b) Para qual endereço IP a mensagem de consulta DNS é enviada? Olhe o conteúdo do arquivo **/etc/resolv.conf** e veja o endereço IP que aparece na frente da palavra **nameserver**. São o mesmo endereço?
- c) Qual é a porta de destino de uma mensagem de consulta DNS? Qual é a porta de origem de uma mensagem de resposta DNS?
- d) Examine uma mensagem de consulta DNS. Qual campo identifica o tipo da mensagem DNS? Qual valor há nesse campo? Há respostas na mensagem de consulta?
- e) Examine uma mensagem de resposta DNS. Quantas respostas estão em uma única mensagem? O que está contido em cada resposta?
- f) Após uma mensagem de resposta DNS, provavelmente há um pacote **TCP SYN** enviado pelo navegador do seu computador. O endereço IP do pacote TCP SYN corresponde a algum dos endereços fornecido na mensagem de resposta do DNS?
- g) A página *Web* inicial do IETF contém vários objetos embutidos. Antes de tentar buscar cada objeto, o seu computador envia novas mensagens de consulta DNS? Comente.

3. Nesse exercício, será utilizada a ferramenta **dig**. Realize os seguintes passos:

- i. Inicie a captura de pacotes com **Wireshark**;
- ii. Faça uma consulta com **dig** sobre o site www.google.com;
- iii. Pare a captura de pacotes do **Wireshark**.

3.1 Responda o que é pedido nas questões a seguir.

- a) Qual é a porta de destino de uma mensagem de consulta DNS? Qual é a porta de origem de uma mensagem de resposta DNS?
- b) Para qual endereço IP a mensagem de consulta DNS é enviada? Esse é o endereço IP do seu servidor DNS local?
- c) Examine a mensagem de consulta DNS. Qual campo identifica o tipo da mensagem DNS? Qual valor há nesse campo? Há respostas na mensagem de consulta?
- d) Examine a mensagem de resposta DNS. Quantas respostas estão em uma única mensagem? O que está contido em cada resposta?

3.2. Repita o experimento, mas consultando pelo servidor de nomes: **dig google.com ns**

Responda o que é pedido nas questões a seguir.

- a) Para qual endereço IP a mensagem de consulta DNS é enviada? Esse é o endereço IP do seu servidor DNS local?
- b) Examine a mensagem de consulta DNS. Qual campo identifica o tipo da mensagem DNS? Qual valor há nesse campo? Há respostas na mensagem de consulta?
- c) Examine a mensagem de resposta DNS. Quais servidores de nomes foram fornecidos na mensagem de resposta? A mensagem de resposta também forneceu os endereços IP dos servidores de nome do MIT?

3.3. Repita o experimento, mas usando o servidor de nomes do google para consultar outro nome (ex.: Google):

dig @8.8.8.8 www.inf.ufg.br

Responda o que é pedido nas questões a seguir.

- a) Para qual endereço IP a mensagem de consulta DNS é enviada? Esse é o endereço IP do seu servidor DNS local? Se não, a qual equipamento corresponde esse endereço IP?
- b) Examine a mensagem de consulta DNS. Qual campo identifica o tipo da mensagem DNS? Qual valor há nesse campo? Há respostas na mensagem de consulta?
- c) Examine a mensagem de resposta DNS. Quantas respostas estão em uma única mensagem? O que está contido em cada resposta?

3.4. Repita o experimento, mas enviando a mensagem de consulta ao servidor através do protocolo TCP:
dig @8.8.8.8 www.inf.ufg.br +tcp

Responda o que é pedido nas questões a seguir.

- a) Há pacotes antes do envio da consulta e depois do recebimento da resposta. Para que servem esses pacotes?
- b) Examine a mensagem de consulta DNS. Qual campo identifica o tipo da mensagem DNS? Qual valor há nesse campo? Há respostas na mensagem de consulta?
- c) Qual é a porta de destino de uma mensagem de consulta DNS? Qual é a porta de origem de uma mensagem de resposta DNS?
- d) Há diferença de desempenho entre as consultas feitas com TCP em relação ao UDP? Se os valores estiverem variando muito, faça a média de 30 testes. Provavelmente, você se baseou na informação **Query time** para responder essa questão. Faça novamente os testes, mas medindo o tempo com o comando **time (time dig @8.8.8.8 www.inf.ufg.br +tcp)**