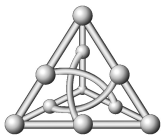

UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL
Faculdade de Computação

Trabalho 04: Consultas DNS e Wireshark

Redes de Computadores

1 Descrição

Você deve fazer este trabalho individualmente.

2 Wireshark

Baixe e execute o *wireshark* [1] em um sistema que você seja capaz de capturar pacotes (tenha acesso administrativo).

Depois de executar o wireshark, inicie a captura na sua interface de rede conectada na Internet (geralmente a `eth0` ou algo como isso), então defina o filtro [2] (um filtro regular na janela principal, não um filtro de captura no menu de opções) `udp port 53`. Veja o exemplo na Figura 1. Depois de fazer isso, execute um `ping` em `www.ufms.br`.

Anote as respostas e tire uma foto do seu wireshark mostrando esses pacotes para as seguintes perguntas:

- Quantas consultas foram enviadas pelo seu computador?
- Que tipo de consultas o seu computador fez?
- Quantas respostas o servidor de DNS fez?

Nota importante: ferramentas de varredura de rede como o wireshark podem ser usadas para propósitos maliciosos ou para depuração da rede. Se for detectado que, enquanto você estiver matriculado nesta disciplina, você usou o wireshark para obter informações alheias sem consentimento, você poderá ser reprovado instantaneamente na disciplina.

Perceba também que seu sistema pode estar realizando outras requisições de DNS independentemente de qualquer outra atividade que você esteja fazendo no computador. Nas respostas as questões, responda focando apenas aos pacotes de DNS trocados pelo comando `ping` executado.

Todos os usuários tem responsabilidades ao usar computadores da Universidade tanto no quesito ético quanto legal e responsável. Usuários devem respeitar a privacidade alheia como senhas, informações e comunicação.

[1] https://www.wireshark.org/
[2] https://wiki.wireshark.org/CaptureFilters

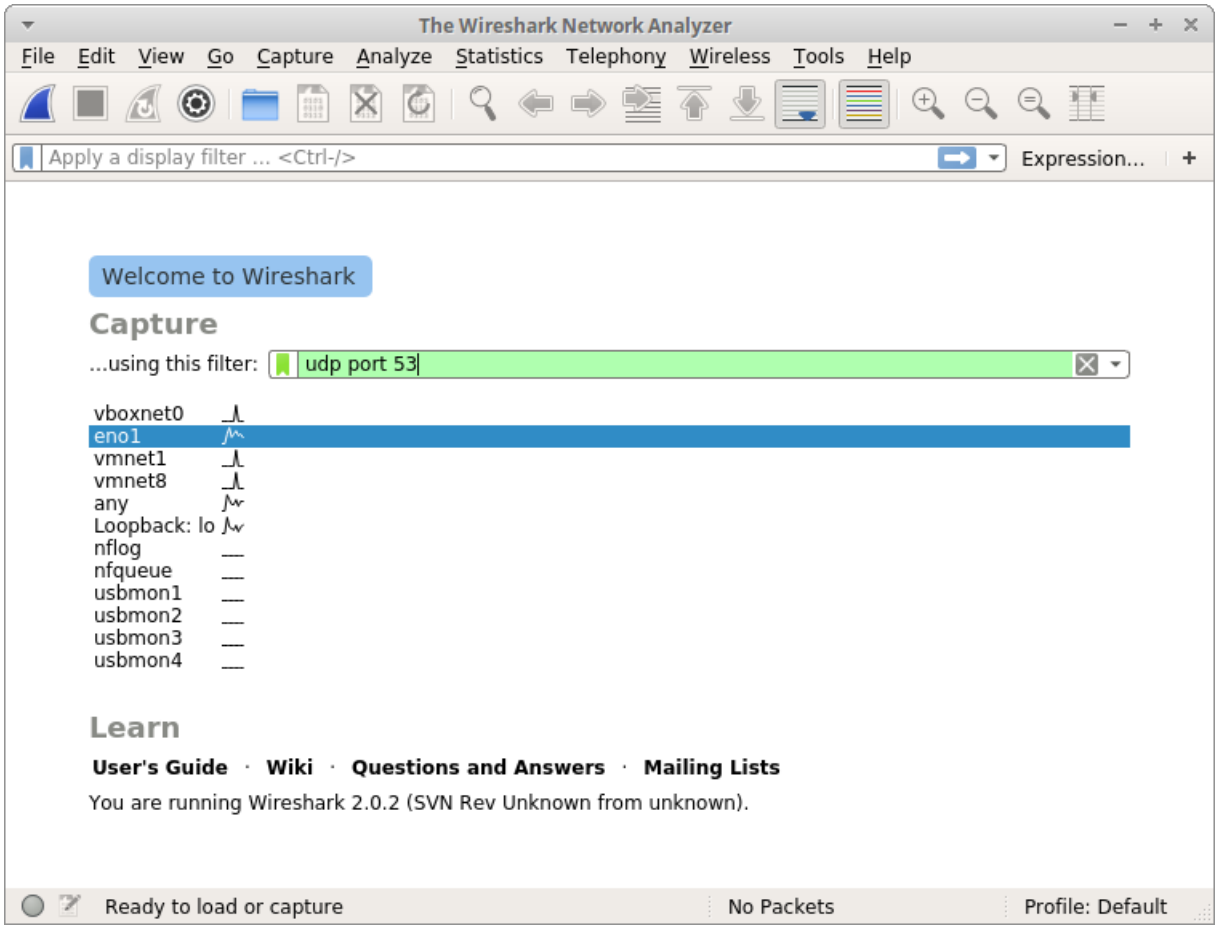

Figura 1: Exemplo de filtro para captura de pacotes.

3 Cliente DNS

Escreva um cliente DNS simples chamado `dns.c`.

O cliente deve como primeiro (e somente um) parâmetro de linha de comando, o nome do domínio. O nome do domínio pode ou não estar em FQDN (*Fully Qualified Domain Name*), que significa que é terminado por um '.'. Em outras palavras, seu cliente deve interpretar corretamente requisições para `www.ufms.br` e `www.ufms.br.`

O cliente deve poder aceitar também um segundo parâmetro opcional, que é um endereço IP de um servidor de nomes de domínio. O segundo parâmetro de linha de comando é opcional (seu código DEVE implementá-lo). Se o servidor não for especificado, use `127.0.0.1`, que é o seu endereço local do computador. Use as funções `inet_aton` ou `inet_pton` no seu código para converter o segundo parâmetro, se tiver um, para um número IP.

Se você quiser, pode usar o código a seguir:

```
int port = 53;
struct sockaddr_in sin;
sin.sin_family = AF_INET;
if (! inet_aton (server, &(sin.sin_addr))) {
  printf ("invalid server IP %s\n", server);
  exit (1);
}
sin.sin_port = htons (port);
```

O cliente deve abrir um *socket*, criar uma requisição DNS para um certo nome de domínio e `sendto` a requisição para o sevidor. O cliente deve então esperar (`sleep(2)`) por dois segundos para dar tempo do servidor resopnder (vamos ignorar essa resposta por enquanto) e então fechar o *socket*.

Esse processo (enviar uma requisição DNS) deve ser repetida três vezes. Uma para uma entrada do tipo A, uma para uma entrada do tipo AAAA e uma para uma entrada do tipo MX.

Você pode (a) abrir um *socket*, enviar a requisição, esperar, fechar o *socket* e repetir o processo três vezes, como descrito anteriormente, ou (b) abrir um *socket*, enviar as três requisições, esperar e fechar o *socket*.

Para mostrar que o seu código funcionou, envie as requisições usando seu endereço IP local (`127.0.0.1`) como o servidor e observe o resultado no wireshark. O resultado deve ser parecido com o da Figura 2.

Envie seu código e uma foto mostrando que o seu wireshark não mostrou qualquer erro nos seus pacotes.

Você pode ver no wireshark pacotes ICMP reportando que a porta está inalcalçável no seu computador – você pode ignorar esses pacotes (eles simplesmente querem dizer que não existe um servidor de DNS rodando no seu sistema). Qualquer outro erro deve ser corrigido antes de irmos para a próxima parte.

Note também que as requisições DNS enviadas pelo seu cliente irão ser diferentes de outras aplicações que realizam consultas DNS, pois eles provavelmente usam EDNS (*Extended DNS*). Você pode ler mais sobre DNS no livro texto da disciplina ou se aprofundar lendo as RFC 1035 [3] e RFC 3596 [4] (que adicionou o suporte ao tipo AAAA e tem o valor numérico 28 – lembre de usar o `htons`).

4 Opcional

Se o wireshark mostrar que as requisições do seu cliente ocorreram sem erros para vários nomes de domínio diferentes, envie requisições para o servidor de DNS padrão do seu

[3] http://tools.ietf.org/html/rfc1035
[4] http://tools.ietf.org/html/rfc3596

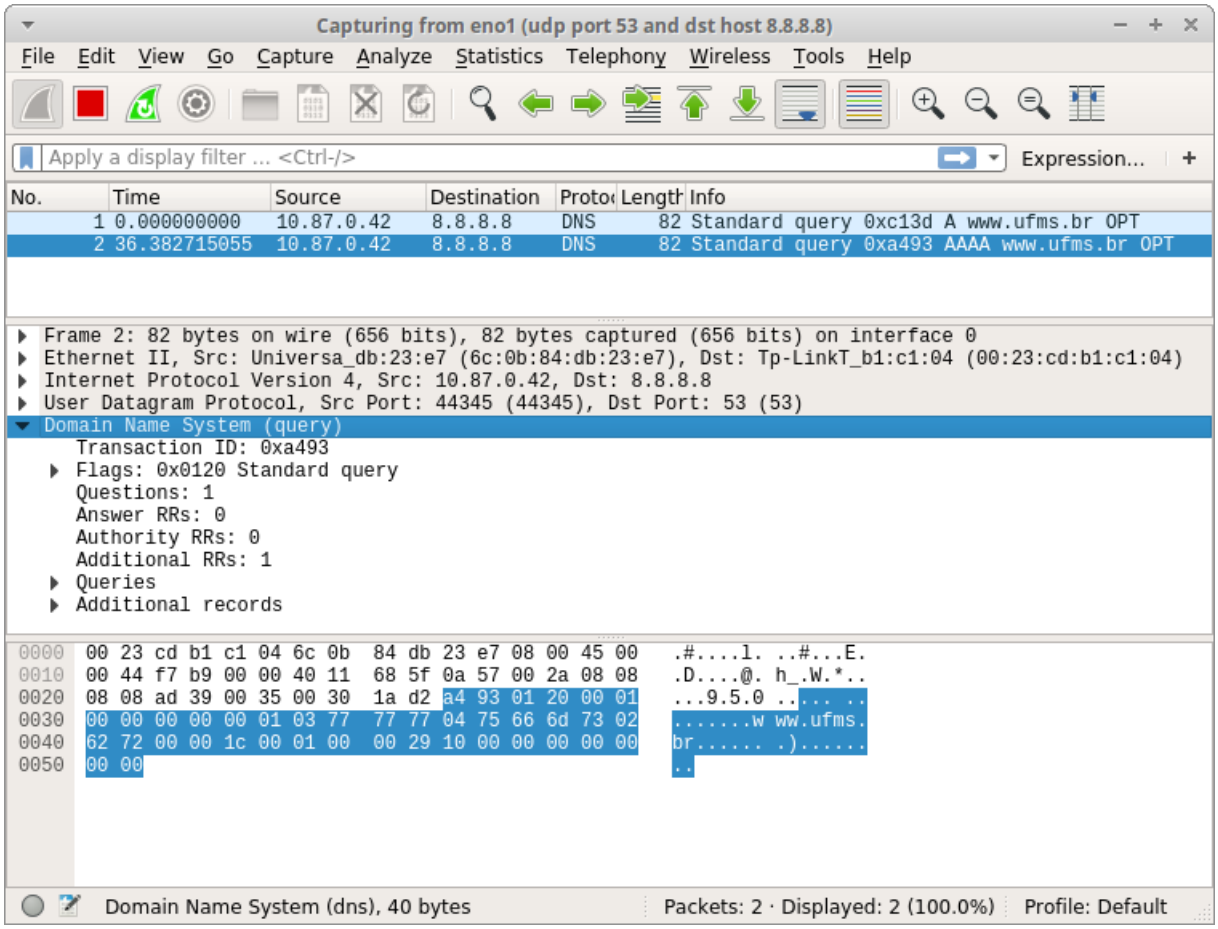

Figura 2: Exemplo de filtro para captura de pacotes.

computador ou algum servidor público como o DNS do Google (`8.8.8.8`) ou OpenDNS (`208.67.222.222`). Se tudo ocorrer corretamente, você receberá as respostas correspondentes. Tenha certeza de tentar com nomes de domínio que você conheça e também com nomes de domínio que não existem.