07

TCP mundo real

Transcrição

Vamos ver na prática como esses protocolos funcionam. Para nos ajudar a fazer a analise dos protocolos que estão passando em nossa rede, usaremos um programa chamado Wireshark (https://www.wireshark.org/).

Após abrir o programa, como em nosso exemplo, usaremos a internet cabeada. Basta clicar em ***Ethernet*** para que o programa comece a fazer a analise. Agora vamos analisar o conteúdo do blog da Alura (http://blog.alura.com.br/) digitando o endereço no browser. Quando o site estiver completamente carregado poderemos parar a analise.

Agora precisamos filtrar apenas a análise da comunicação do nosso computador com o servidor que contém o conteúdo do blog da Alura. Vamos precisar descobrir o endereço IP do servidor usando o comando `nslookup blog.alura.com.br` no terminal ou prompt.

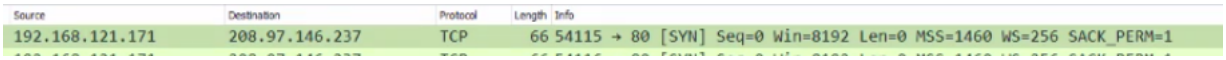
```
Non-authoritative answer:
Name:   blog.alura.com.br
Address: 208.97.146.237
```

Agora no campo de busca do Wireshark, basta digitarmos o comando `ip.addr==208.97.146.237` e pressionar a tecla enter para filtrar.

Perceba que temos a aba ***Source***, ela representa as informações da origem. Se olharmos o primeiro pacote enviado, na aba *source* deve conter o endereço IP do nosso computador. Para descobrir a conexão do computador, no Windows basta utilizar o comando `ipconfig` , no Linux e no Mac é só clicar no ícone de conexão e depois em "Informações da conexão" para o Linux e “Abrir Preferências de Rede” no Mac.

Na ***Destination*** representa as informações de destino. Analisando o primeiro pacote, como já descobrimos, contém o IP do servidor.

Já aprendemos que essas requisições de páginas web forma feitas para trabalhar com o protocolo TCP. Na aba ***Protocol*** vemos qual protocolo foi utilizado. Na aba ***Info*** vemos as informações dos pacotes enviados, SYN, SYN - ACK ou ACK.



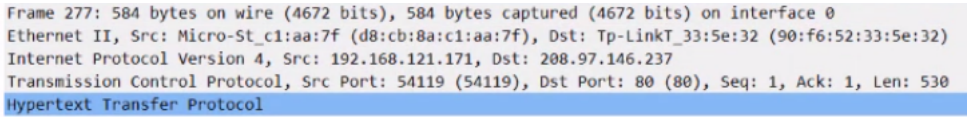
Se analisarmos os pacotes seguintes, poderemos ver a conexão sendo estabelecida, o *Three Way Handshake*.

```
192.168.121.171   208.97.146.237   TCP   66 54120 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
208.97.146.237    192.168.121.171  TCP   66 80 → 54119 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1448 SACK_PERM=1 WS=1024
192.168.121.171   208.97.146.237   TCP   54 54119 → 80 [ACK] Seq=1 Ack=1 Win=66560 Len=0
```

Agora que conexão foi estabelecida, a transmissão dos dados será iniciada. Como estamos **pedindo** a página web para o servidor, o protocolo *HTTP* entrará em ação com o método *GET*.

```
192.168.121.171   208.97.146.237   HTTP   584 GET / HTTP/1.1
```

Vamos clicar no pacote do protocolo HTTP para acessar os detalhes. Lembra-se da camada OSI? Aqui veremos o que aprendemos sobre as camadas, como os *frames*, endereçamentos IP de origem e destino, endereçamentos MAC de origem e destino, forma de transmissão e portas de comunicação.



As duas primeiras linhas representam as informações que estão dentro do ***Layer 2*** (camada 2), de enlace de dados. A terceira linha representa o ***Layer 3*** (camada 3) de rede. A quarta linha representa o **Layer 4** (camada 4), de transporte.