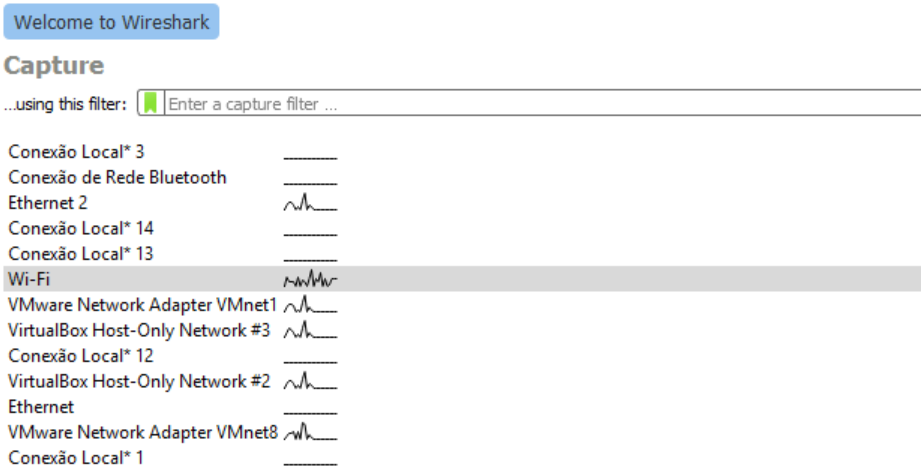
Quando estabelecemos uma sessão de forma segura com o HTTPS o servidor envia para o cliente uma chave pública, dentro de um certificado digital, a qual será utilizada posteriormente pelo cliente para que possa criptografar os dados que só poderão ser descriptografados pela chave privada que está no servidor.

Vamos acessar uma aplicação que trabalha com HTTPS para que possamos ver esse fluxo, primeiramente inicialize o Wireshark no seu computador local e escolha para o wireshark mostrar os resultados respectivos ao adaptador de rede que está sendo utilizado para conexão na internet, por exemplo, se seu computador estiver utilizando wi-fi para se conectar na internet, utiliza o adaptador wireless correspondente, se estiver utilizando conexão cabeada, utilize o adaptador respectivo.



Para facilitar o filtro posteriormente no Wireshark, feche todas as abas no browser e abra somente uma jabela para acessar a aplicação original da Alura www.alura.com.br

Ao acessarmos a aplicação da Alura, devemos ter capturado no Wireshark todos os pacotes referentes a comunicação entre nosso computador e o servidor com a aplicação da Alura. Para filtrarmos esses dados de comunicação, vamos utilizar a ferramenta administrativa do nslookup para sabermos qual endereço IP que responde pelo domínio **alura.com.br**

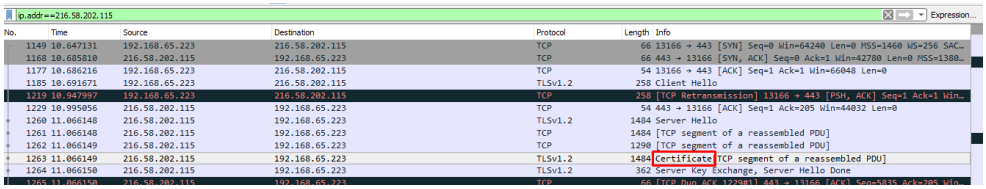
```
C:\Users\Rafael>nslookup www.alura.com.br
Servidor:  dlinkrouter
Address:  192.168.65.1

Não é resposta autoritativa:
Nome:    ghs.googlehosted.com
Addresses:  2800:3f0:4001:80d::2013
          216.58.202.115
Aliases:  www.alura.com.br
```

Copie o endereço IP e coloque no Wireshark o seguinte fitro:

```
ip.addr==[Endereço IP obtido com nslookup]
```

COPIAR CÓDIGO

Procure pelo pacote **Certificate** para ver o certificado digital passado do servidor para o cliente:



Na sequência, na parte inferior do Wireshark, temos os detalhes referentes a esse pacote, dentro da aba **Secure sockets layer** procure pelo certificado referente ao domínio da Alura. Qual o resultado? Você consegue encontrar a chave pública dentro do certificado digital?

Opinião do instrutor

Ao analisarmos o resultado referente a esse pacote, nós temos justamente os dados do certificado digital com a chave pública passada para o nosso cliente, com isso nosso browser sabe que de fato estamos acessando a aplicação verdadeira da Alura, fornecendo assim uma segurança para o usuário final.