Atividade 1 - Usando o Wireshark para observar o Handshake Triplo do TCP (Modificado)

Nome: Igor Correa RA: 15.00588-7  
Nome: Rodrigo Franciozi RA: 14.04014-0

Nome: RA:

Topologia



1. Objetivos

Parte 1: Preparar o Wireshark para Capturar Pacotes

Parte 2: Capturar, Localizar e Examinar Pacotes

1. Histórico/cenário

Nesta laboratório, você usará o Wireshark para capturar e examinar pacotes gerados entre o navegador do computador usando protocolo HTTP e um servidor Web, como [www.google.com](http://www.google.com). Quando uma aplicação, como HTTP ou FTP (File Transfer Protocol), inicia em um host, o TCP usa o handshake triplo para estabelecer uma sessão TCP confiável entre os dois hosts. Por exemplo, quando um computador usa um navegador Web para surfar na Internet, um handshake triplo é iniciado e uma sessão é estabelecida entre o computador host e um servidor Web. Um computador pode ter várias sessões TCP ativas simultâneas com vários websites.

1. Recursos Necessários

1 PC (Windows com um acesso ao prompt de comando, acesso à Internet e Wireshark instalado)

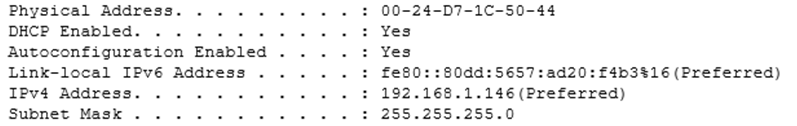
1. Preparar o Wireshark para Capturar Pacotes

Na Parte 1, você iniciará o Wireshark e selecionará a interface adequada para dar início à captura dos pacotes.

* 1. Recuperar os endereços das interfaces do computador.

Para este laboratório, é necessário recuperar o endereço IP do seu PC e o endereço físico da placa de interface de rede (NIC), também conhecido como endereço MAC.

* + 1. Abra uma janela de prompt de comandos, digite **ipconfig /all** e pressione Enter.

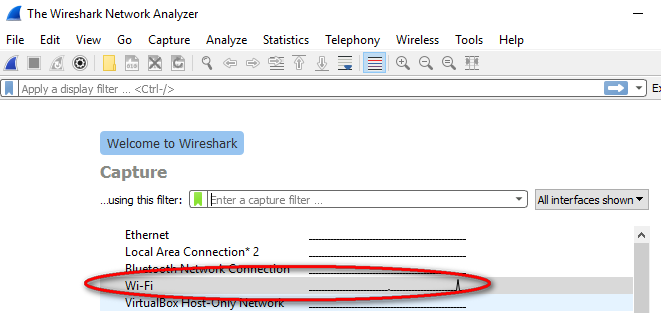


* + 1. Escreva os endereços IP e MAC associados ao adaptador Ethernet selecionado. Este é o endereço de origem para análise, quando examinar os pacotes capturados.

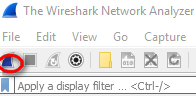
O endereço IP do computador host: 192.168.56.1\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

O endereço MAC do computador host: 0A-00-27-00-00-12\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

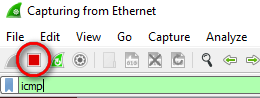
* 1. Iniciar o Wireshark e selecionar a interface adequada.
     1. Clique no botão **Iniciar** do Windows. No menu pop-up, clique duas vezes em **Wireshark**.
     2. Após iniciar o Wireshark, selecione a interface ativa para a captura de dados. A interface ativa mostrará as atividades de tráfego.



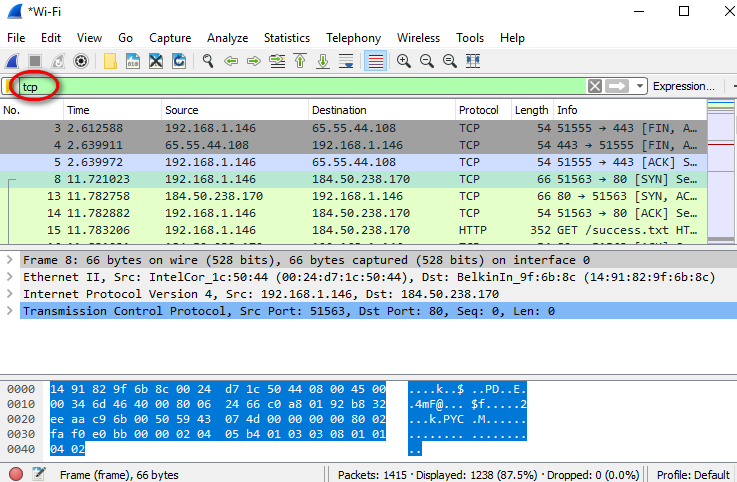
1. Capturar, Localizar e Examinar Pacotes
   1. Capture os dados.
      1. Clique no botão **Start** (Iniciar) para iniciar a captura de dados.



* + 1. Abra um navegador Web e acesse [**www.altoromutual.com/bank/login.aspx**](http://www.altoromutual.com/bank/login.aspx)
    2. Minimize o navegador e volte para o Wireshark. Pare a captura de dados.

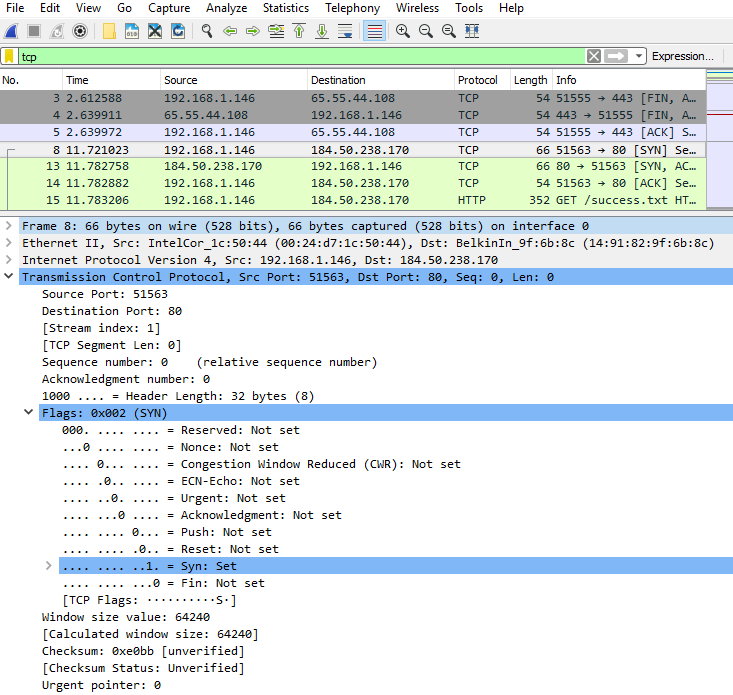


* + 1. Se houver muitos pacotes não relacionados à conexão TCP, pode ser necessário usar a ferramenta de filtro do Wireshark. Digite tcp na área de entrada do filtro dentro do Wireshark e pressione Enter.



* 1. Examinar as informações dentro dos pacotes incluindo os endereços IP, números de porta TCP e flags de controle TCP.
     1. No exemplo, o quadro 8 é o início do handshake triplo entre o computador e o servidor Web do Google. No painel da lista de pacotes (a seção superior da janela principal) selecione o quadro. Isso destaca a linha e exibe as informações decodificadas desse pacote em dois painéis menores. Examine as informações do TCP no painel de detalhes do pacote (a seção central da janela principal).
     2. Clique no ícone **+** à esquerda do TCP, no painel de detalhes do pacote, para ampliar a exibição das informações do TCP.
     3. Clique no ícone **+** à esquerda dos flags. Verifique as portas origem e destino e os flags que estão ligados.

**Observação**: pode ser necessário ajustar o tamanho da janela superior e central dentro do Wireshark para exibir as informações necessárias.



Qual é o número da porta TCP origem? 53304\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Como você classificaria essa porta de origem? Porta não regulamentada\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

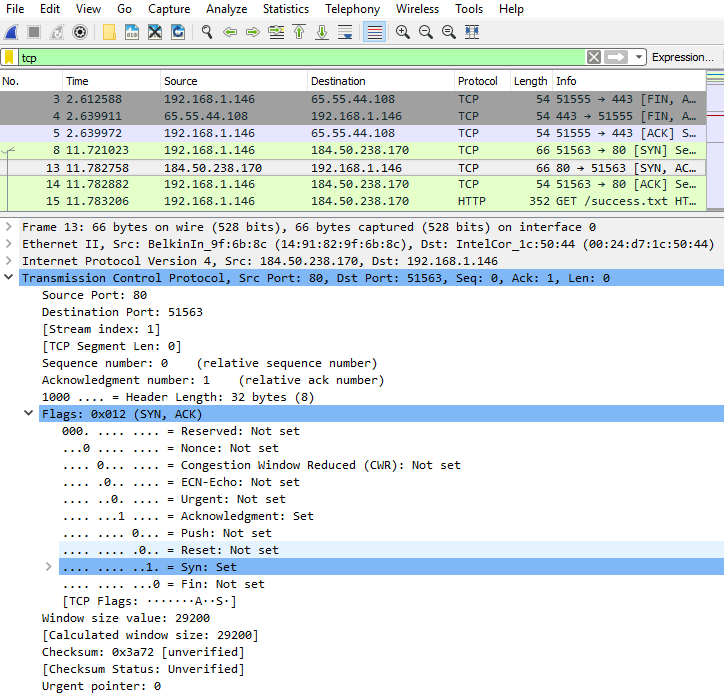
Qual é o número da porta TCP destino? 80\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Como você classificaria essa porta de destino? Porta padrão\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Qual flag (ou flags) estão ligados? Apenas o Flag Syn está ligado\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Qual o valor do número de sequência relativo? 0\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Para selecionar o próximo quadro no handshake triplo, selecione **Go** (Ir) no menu do Wireshark e selecione **Next Packet In Conversation** (Próximo Pacote da Conversação). Neste exemplo, é o quadro 13. Esta é a resposta do servidor Web do Google para a requisição de início de uma sessão.



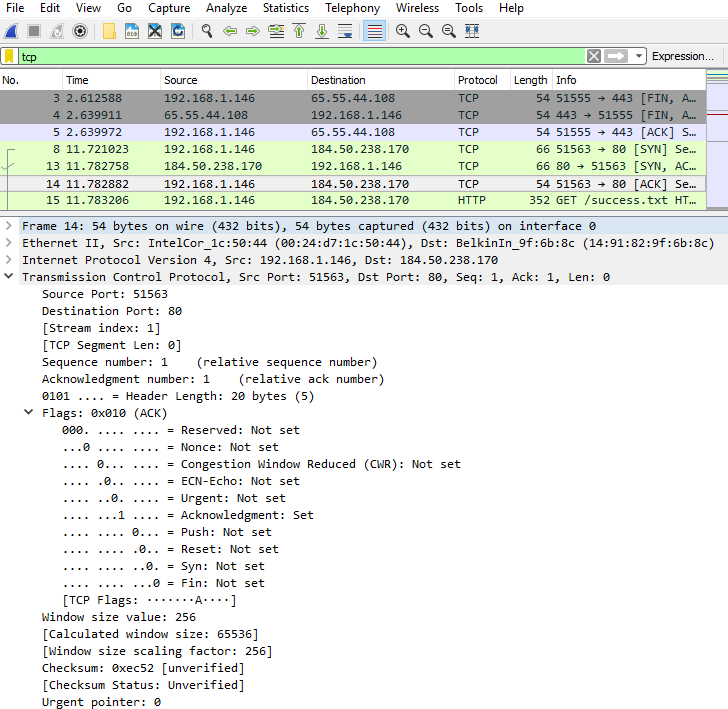
Quais são os valores das portas origem e destino? Origem 80 e destino 53304

Que flags estão ligados? Ack e Syn

Quais os valores dos números de sequência e confirmação relativos?

Sequência 0 e confirmação 1\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Por fim, examine o terceiro pacote do handshake triplo fornecido no exemplo. Clique no quadro 14 na parte superior da janela para exibir as seguintes informações neste exemplo:



Examine o terceiro e último pacote do handshake.

Qual flag (ou flags) está ligado? Apenas o Ack\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Os números de sequência e confirmação relativos estão com valor 1 como um ponto de partida. A conexão TCP é estabelecida e a conversação entre o computador origem e o servidor Web pode iniciar.

* + 1. Feche o Wireshark.