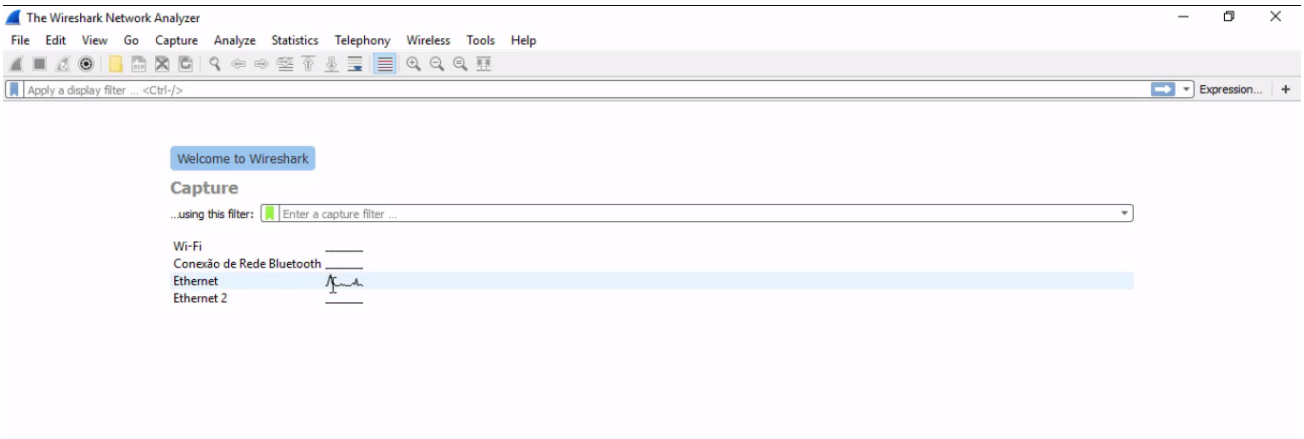
08

4 - Wireshark http final

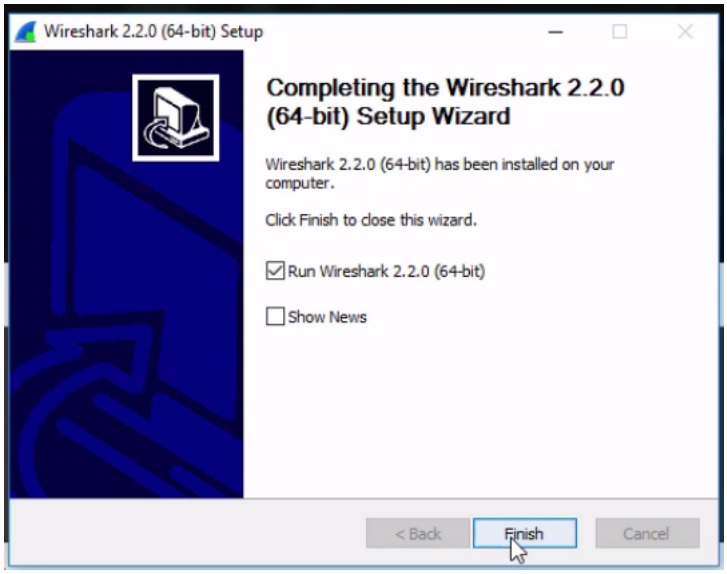
Transcrição

Vamos mostrar a vulnerabilidade dos hubs que conversamos. Um usuário malicioso pode entrar na nossa rede e analisar as informações que são trafegadas, por exemplo, entre um site e outra máquina. Estou no site do Buscapé, e vou simularar os dois papeis - o da vítima e o do usuário malicioso. Para isto, usaremos um programa para a análise de protocolos chamado **wireshark** (https://www.wireshark.org/).

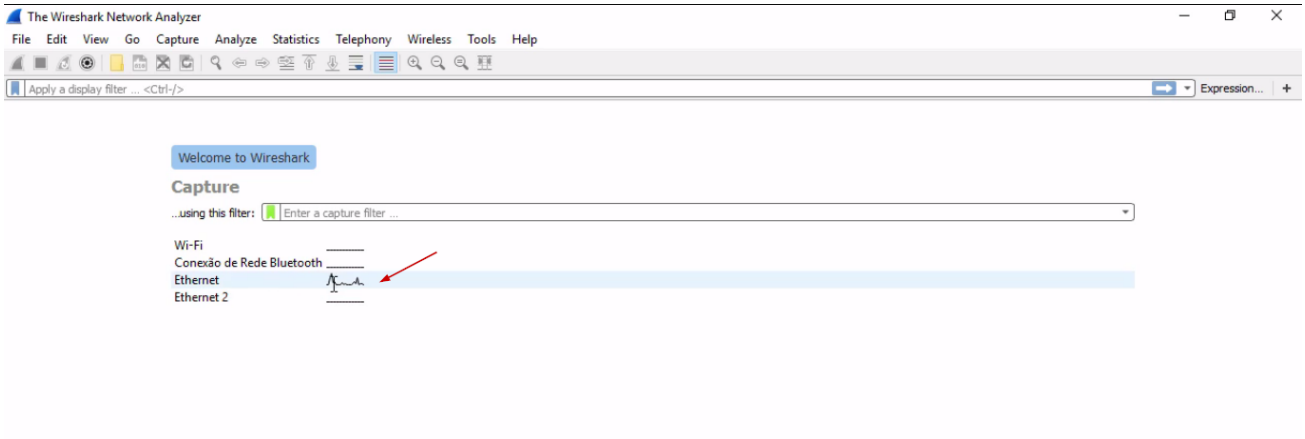


Faremos o download na página, selecionaremos o sistema operacional. No caso, escolheremos "Windows Installer (64-bit)". Se você estiver usando o Mac, encontrará orientações nos exercícios (https://cursos.alura.com.br/course/redes-introducao/task/21288).

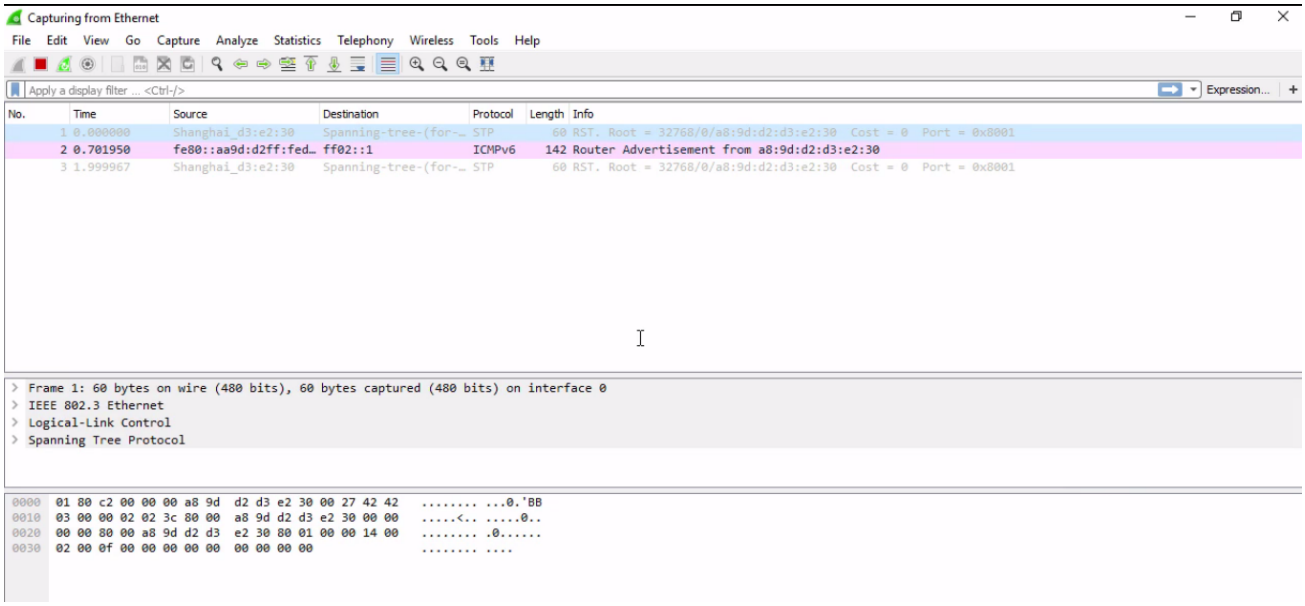
Nós já temos instalados na máquina, mas vamos executar e fazer a passagem da instalação. Nos primeiros passos, só clicaremos e "Next", até chegarmos em "Install". Depois de finalizada, basta clicar em "Next" e "Finish" na janela de Setup.



Aparecerá um ícone de barbatana de tubarão no seu desktop. No meu computador, ele precisará pegar as placas de redes conectadas a máquina e provavelmente, a saída seja diferente com você.

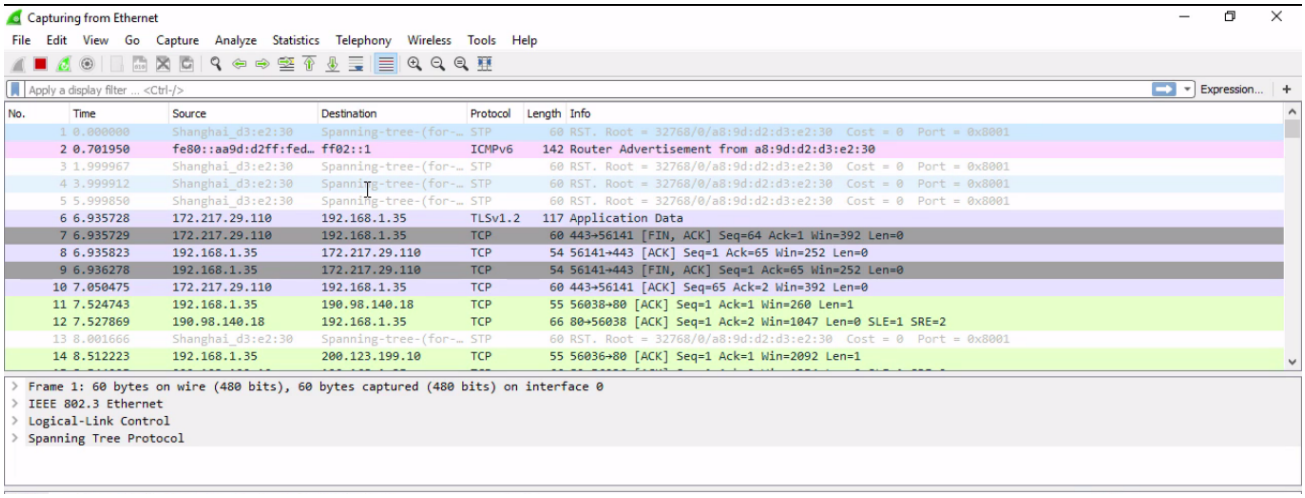


Observe que temos uma atividade na placa sinalizada. Ao clicarmos nela, veremos que temos alguns protocolos passando pela rede.

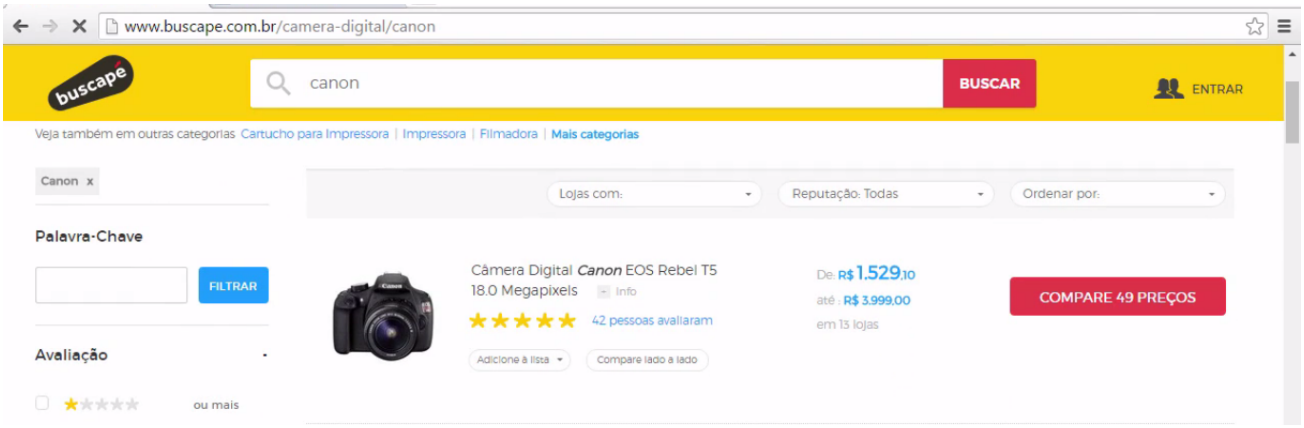


Nós não nos aprofundaremos na parte de análise de protocolo do Wireshark, porque o nosso foco é demonstrar a vulnerabilidade de um hub conectado a um usuário malicioso.

Vamos ver o que o Wireshark está nos mostrando:



O usuário malicioso colocou o computador na porta do hub e começará a analisar o tráfego da rede. Seguiremos com o exemplo, mostrando uma vítima acessando o site do Buscapé e fazendo uma pesquisa por câmeras Canon.

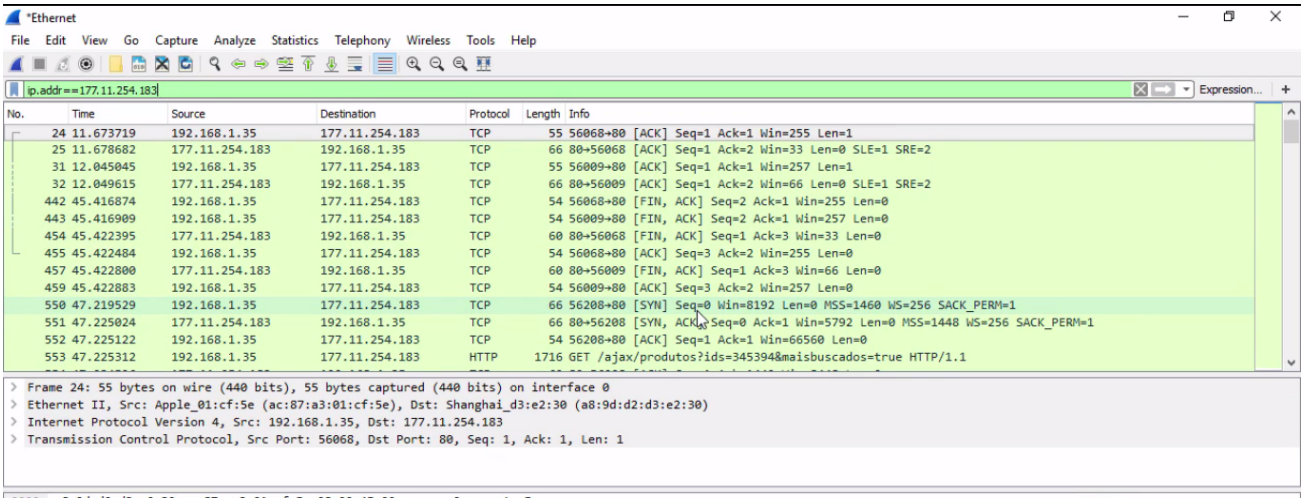


De volta ao Wireshark, veremos o que está sendo analisado pelo usuário malicioso. Ele quer descobrir qual foi o último termo de busca pesquisado pelo usuário no Buscapé. Primeiramente, será filtrado os protocolos referentes ao site Buscapé por meio do IP da máquina da empresa. É possível fazer isso no Prompt de Comando, digitando:

```
c:\Users\Alura>nslookup www.buscape.com.br
```

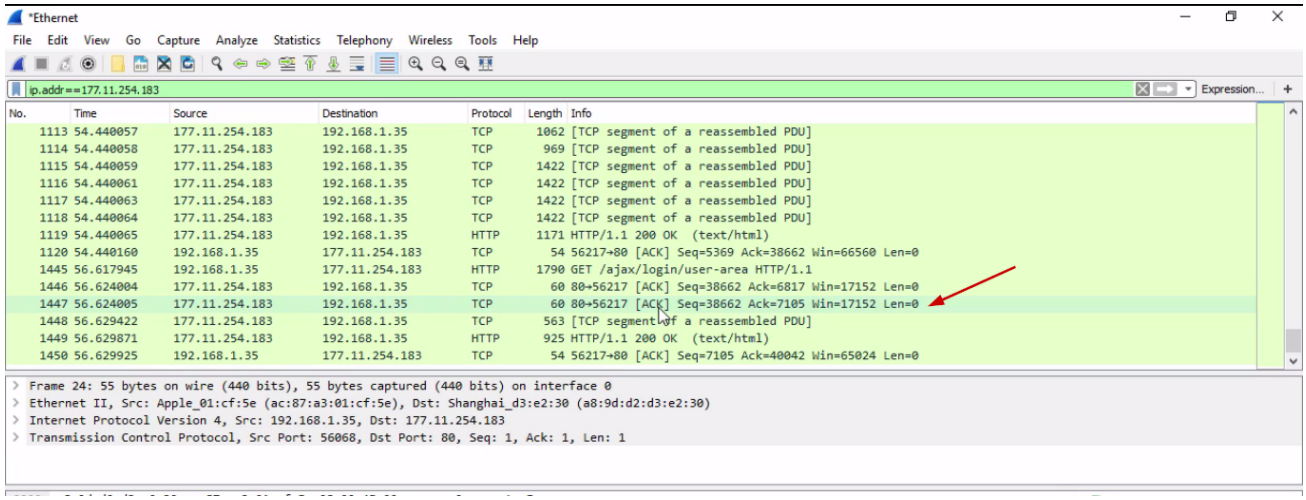
Será retornado o endereço IP da máquina do Buscapé. Após copiar o endereço IP, e vamos colocar um filtro no Wireshark para encontrarmos a máquina do Buscapé.

```
ip.addr == 177.11.254.183
```

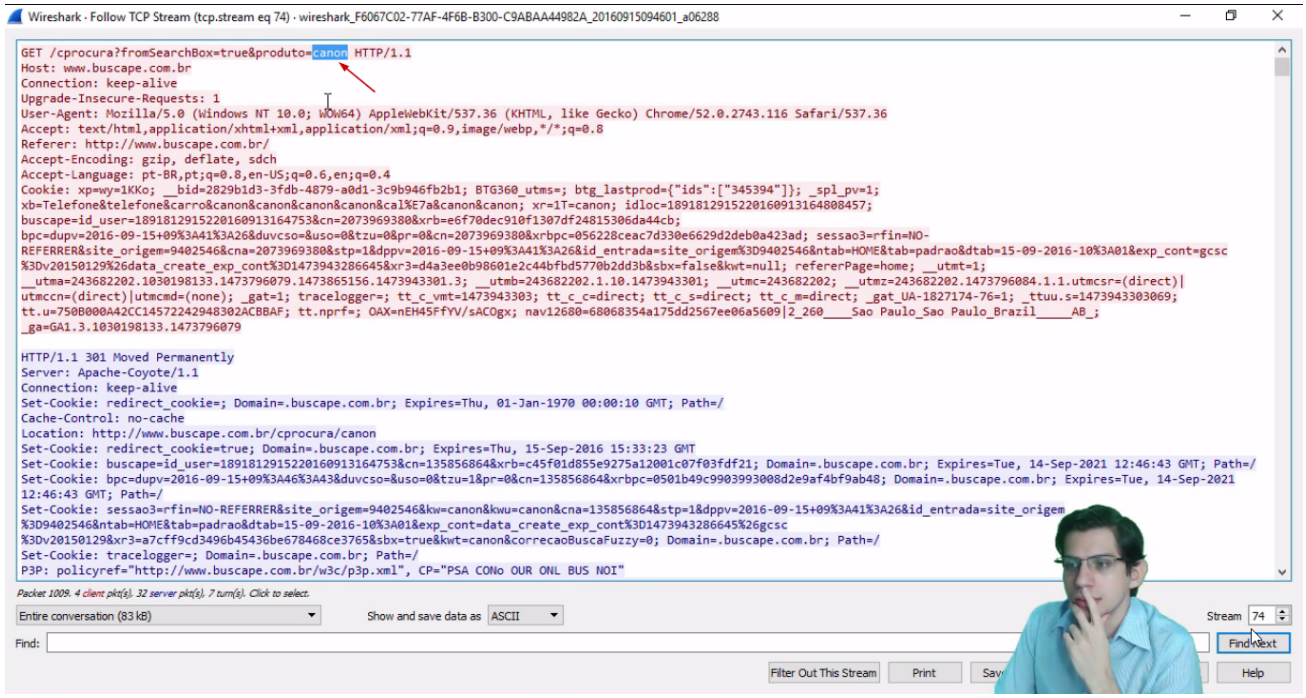


Observe a coluna de protocolo e veja que aparece diversas vezes `TCP`. O protocolo `TCP` está uma camada acima do IP, e será responsável por indicar como a comunicação será estabelecida e será transportada a informação. Se conseguirmos reconstruir o protocolo TCP, podemos ver eventualmente os `header`s do HTTP e descobrir algumas informações.

Vamos escolher um protocolo no fim da análise.



Clicaremos com o botão direito, logo será aberto um menu em que selecionaremos "Follow". Vamos fazer uma análise do HTTP.



Conseguimos identificar que o usuário pesquisou por `canon`, mas o usuário malicioso poderia descobrir outros tipos de informação. Percebemos como hub apresenta esse tipo de problema, porque ele passa as informações para todas as máquinas interconectadas. Com uma análise de protocolo é possível descobrir o que a vítima pesquisou no Buscapé.