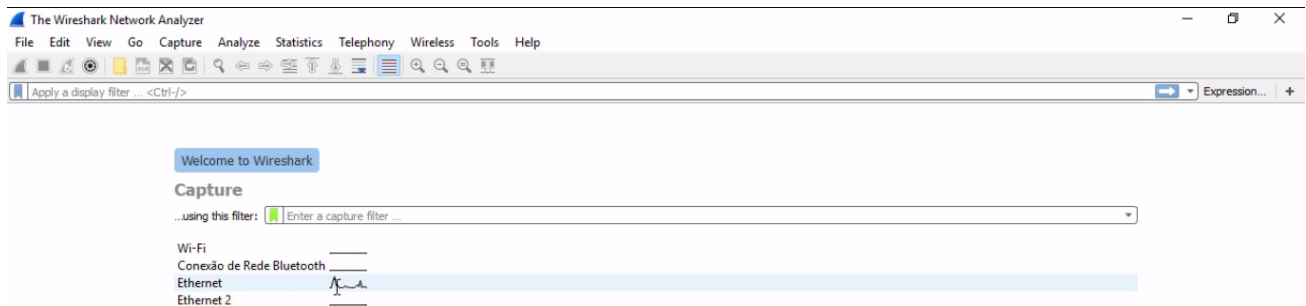


## 4 - Wireshark http final

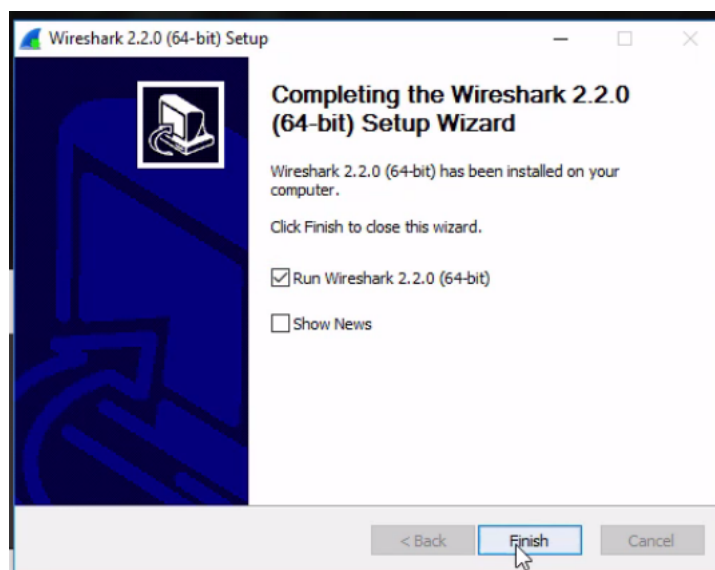
### Transcrição

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 simular os dois papéis - o da vítima e o do usuário malicioso. Para isto, usaremos um programa para a análise de protocolos chamado [wireshark](https://www.wireshark.org/) (<https://www.wireshark.org/>).

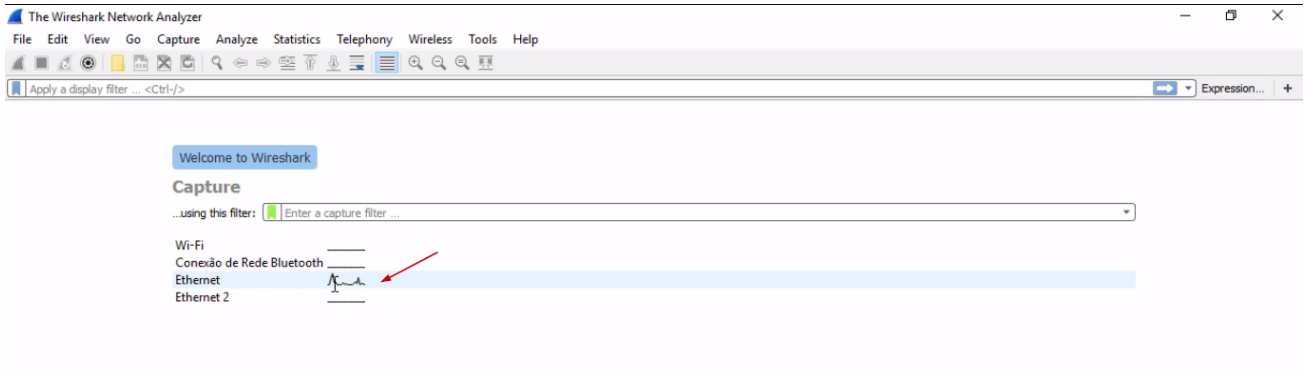


Faremos o download na página, selecionaremos o sistema operacional. No caso, escolheremos "Windows Installer (64-bit)". Se você estiver usando o Mac, encontrará orientações [nos exercícios](https://cursos.alura.com.br/course/redes-introducao/task/21288) (<https://cursos.alura.com.br/course/redes-introducao/task/21288>).

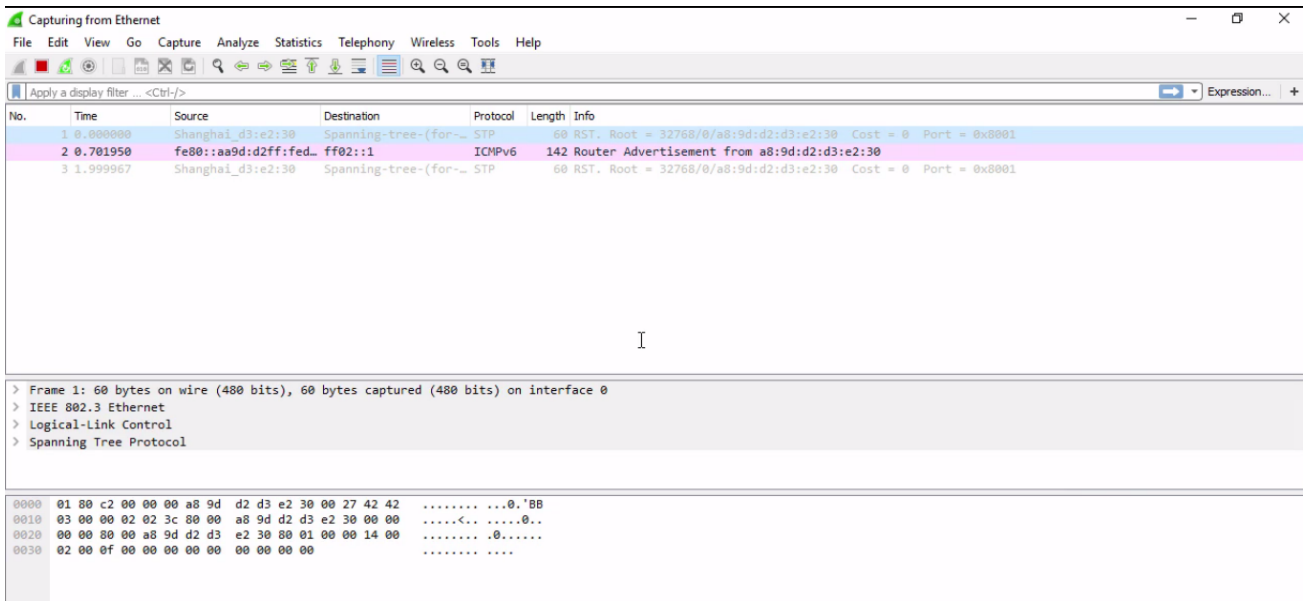
Nós já temos instalados na máquina, mas vamos executar e fazer a passagem da instalação. Nos primeiros passos, só clicaremos e "Next", até chegarmos em "Install". Depois de finalizada, basta clicar em "Next" e "Finish" na janela de Setup.



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.

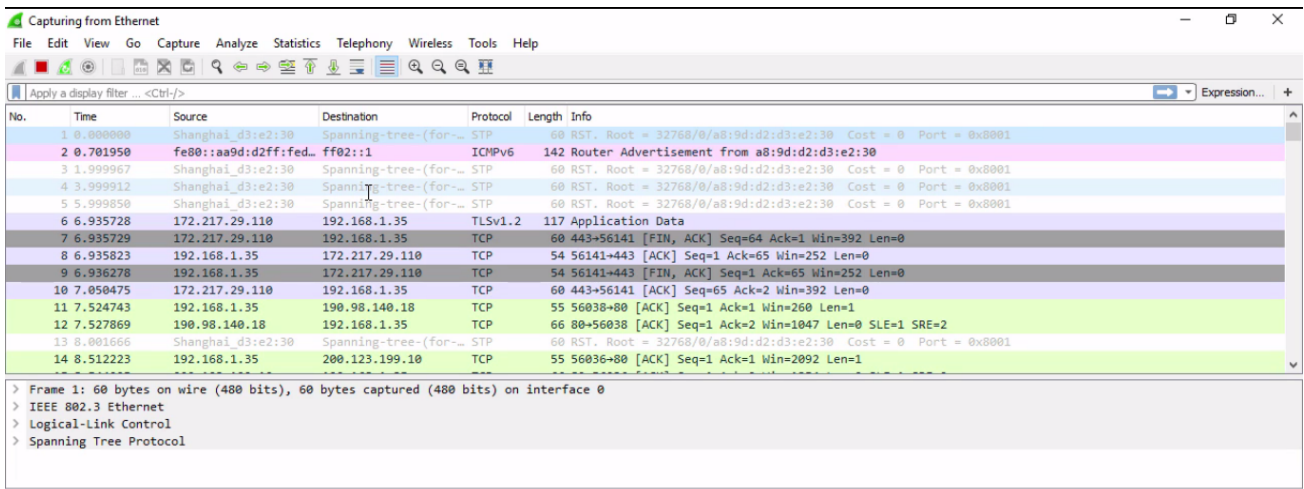


Observe que temos uma atividade na placa sinalizada. Ao clicarmos nela, veremos que temos alguns protocolos passando pela rede.



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.

www.buscape.com.br/camera-digital/canon

buscape canon BUSCAR ENTRAR

Veja também em outras categorias: Cartucho para Impressora | Impressora | Filmadora | Mais categorias

Canon x

Lojas com: Reputação: Todas Ordenar por:

Palavra-Chave

Avaliação

Câmera Digital **Canon** EOS Rebel T5  
18.0 Megapixels Info

De: **R\$ 1.529,10**  
até: **R\$ 3.999,00**  
em 13 lojas

★★★★★ 42 pessoas avaliaram

Adicione à lista Compare lado a lado

COMPRE 49 PREÇOS

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
```

\*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

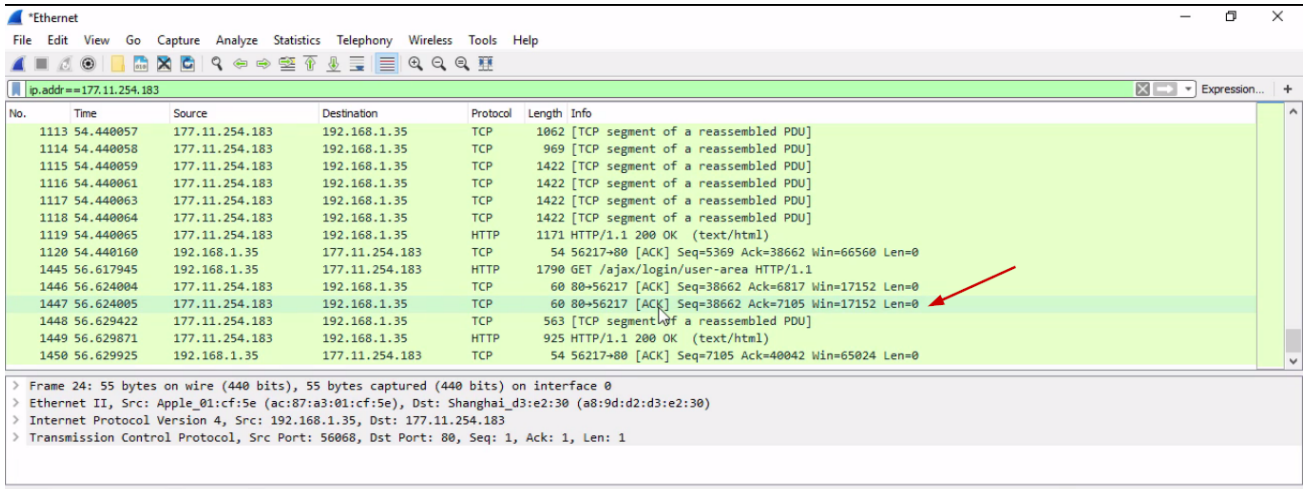
ip.addr==177.11.254.183

No.	Time	Source	Destination	Protocol	Length	Info
24	11.673719	192.168.1.35	177.11.254.183	TCP	55	56068→80 [ACK] Seq=1 Ack=1 Win=255 Len=1
25	11.678682	177.11.254.183	192.168.1.35	TCP	66	80→56068 [ACK] Seq=1 Ack=2 Win=33 Len=0 SLE=1 SRE=2
31	12.045045	192.168.1.35	177.11.254.183	TCP	55	56009→80 [ACK] Seq=1 Ack=1 Win=257 Len=1
32	12.049615	177.11.254.183	192.168.1.35	TCP	66	80→56009 [ACK] Seq=1 Ack=2 Win=66 Len=0 SLE=1 SRE=2
442	45.416874	192.168.1.35	177.11.254.183	TCP	54	56068→80 [FIN, ACK] Seq=2 Ack=1 Win=255 Len=0
443	45.416909	192.168.1.35	177.11.254.183	TCP	54	56009→80 [FIN, ACK] Seq=2 Ack=1 Win=257 Len=0
454	45.422395	177.11.254.183	192.168.1.35	TCP	60	80→56068 [FIN, ACK] Seq=1 Ack=3 Win=33 Len=0
455	45.422484	192.168.1.35	177.11.254.183	TCP	54	56068→80 [ACK] Seq=3 Ack=2 Win=255 Len=0
457	45.422800	177.11.254.183	192.168.1.35	TCP	60	80→56009 [FIN, ACK] Seq=1 Ack=3 Win=66 Len=0
459	45.422883	192.168.1.35	177.11.254.183	TCP	54	56009→80 [ACK] Seq=3 Ack=2 Win=257 Len=0
550	47.219529	192.168.1.35	177.11.254.183	TCP	66	56208→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
551	47.225024	177.11.254.183	192.168.1.35	TCP	66	80→56208 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1448 WS=256 SACK_PERM=1
552	47.225122	192.168.1.35	177.11.254.183	TCP	54	56208→80 [ACK] Seq=1 Ack=1 Win=66560 Len=0
553	47.225312	192.168.1.35	177.11.254.183	HTTP	1716	GET /ajax/produtos?ids=345394&maisbuscados=true HTTP/1.1

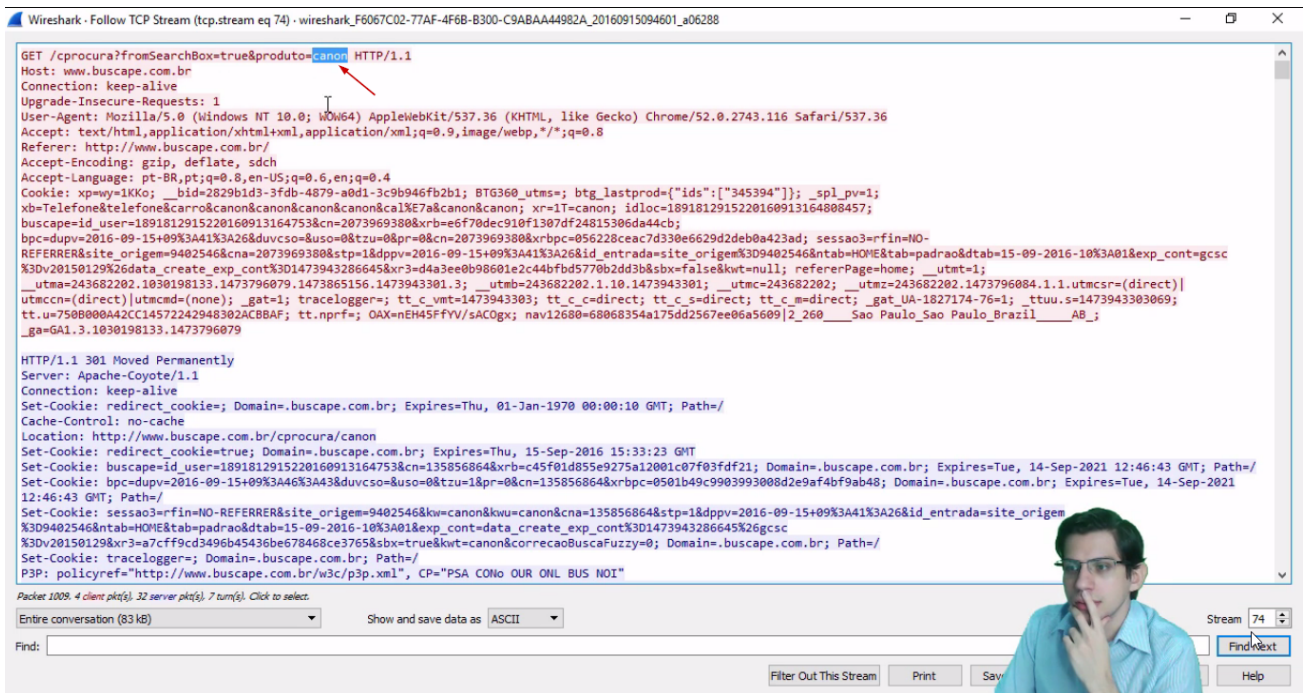
> Frame 24: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0  
> Ethernet II, Src: Apple\_01:cf:5e (ac:87:a3:01:cf:5e), Dst: Shanghai\_d3:e2:30 (a8:9d:d2:d3:e2:30)  
> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 177.11.254.183  
> Transmission Control Protocol, Src Port: 56068, Dst Port: 80, Seq: 1, Ack: 1, Len: 1

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 headers 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.