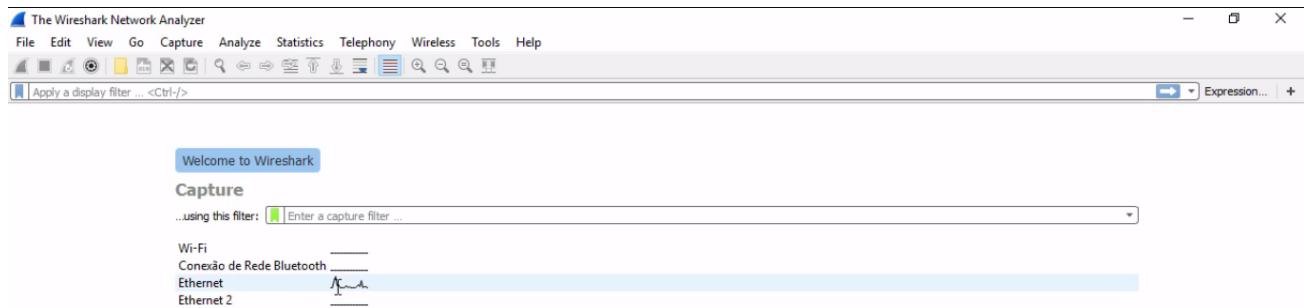


08

## 4 - Wireshark http final

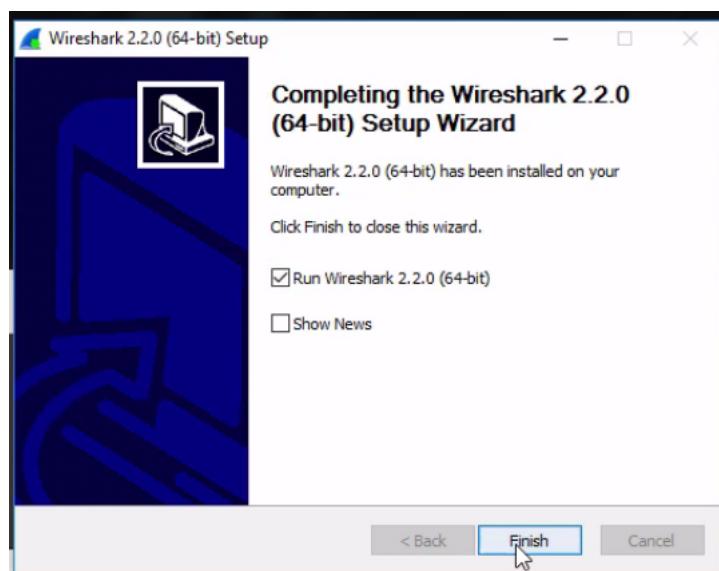
### Transcrição

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 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/>).

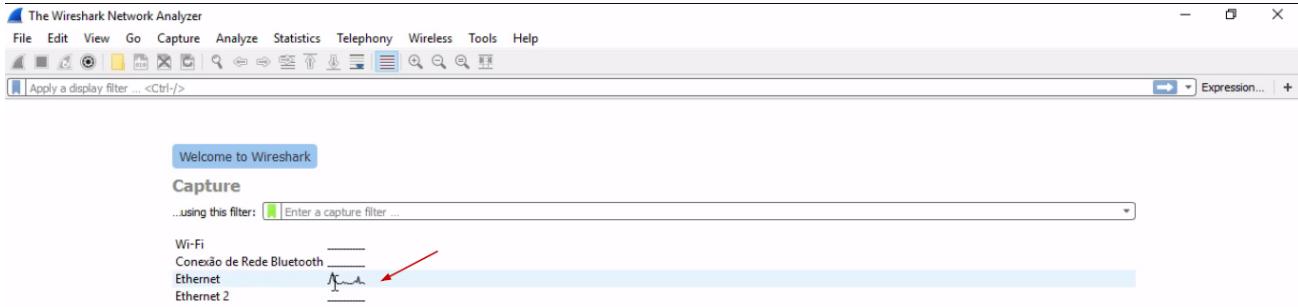


Faremos o download na página, selecionaremos o sistema operacional. No caso, escolheremos "Windows Installer (64-bit)". Se você estiver usando o Mac, encontrará orientações [nos exercícios](https://cursos.alura.com.br/course/redes-introducao/task/21288) (<https://cursos.alura.com.br/course/redes-introducao/task/21288>).

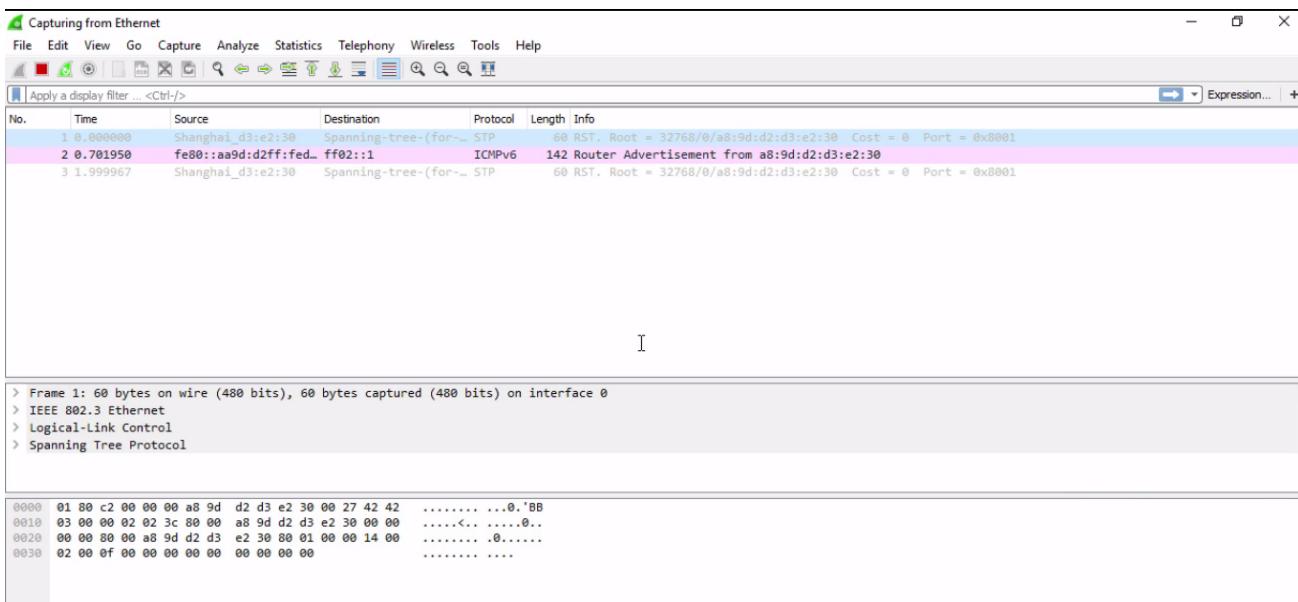
Nós já temos instalados na máquina, mas vamos executar e fazer a passagem da instalação. Nos primeiros passos, só clicaremos em "Next", até chegarmos em "Install". Depois de finalizada, basta clicar em "Next" e "Finish" na janela de Setup.



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.

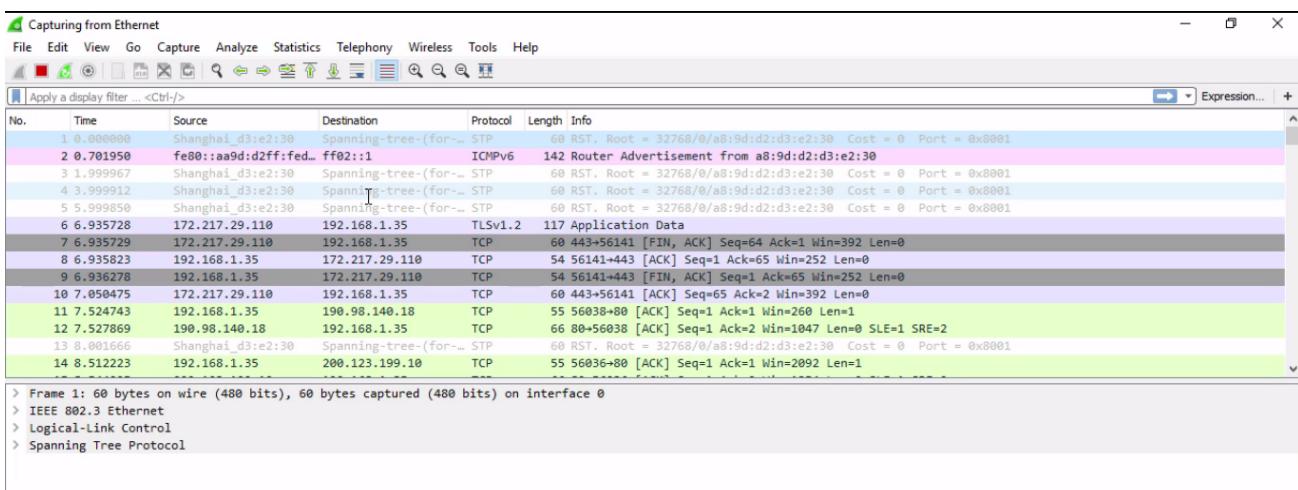


Observe que temos uma atividade na placa sinalizada. Ao clicarmos nela, veremos que temos alguns protocolos passando pela rede.



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 headers do HTTP e descobrir algumas informações.

Vamos escolher um protocolo no fim da análise.

The screenshot shows a Wireshark capture on the 'Ethernet' interface. The packet list pane shows 1450 frames. A red arrow points to the 1447 frame, which is a TCP segment (Seq=7105, Ack=17152, Len=0). The packet details and bytes panes are visible at the bottom, showing the structure of the TCP segment.

No.	Time	Source	Destination	Protocol	Length	Info
1113	54.440057	177.11.254.183	192.168.1.35	TCP	1062	[TCP segment of a reassembled PDU]
1114	54.440058	177.11.254.183	192.168.1.35	TCP	969	[TCP segment of a reassembled PDU]
1115	54.440059	177.11.254.183	192.168.1.35	TCP	1422	[TCP segment of a reassembled PDU]
1116	54.440061	177.11.254.183	192.168.1.35	TCP	1422	[TCP segment of a reassembled PDU]
1117	54.440063	177.11.254.183	192.168.1.35	TCP	1422	[TCP segment of a reassembled PDU]
1118	54.440064	177.11.254.183	192.168.1.35	TCP	1422	[TCP segment of a reassembled PDU]
1119	54.440065	177.11.254.183	192.168.1.35	HTTP	1171	HTTP/1.1 200 OK (text/html)
1120	54.440160	192.168.1.35	177.11.254.183	TCP	54	56217->80 [ACK] Seq=5369 Ack=38662 Win=66560 Len=0
1445	56.617945	192.168.1.35	177.11.254.183	HTTP	1790	GET /ajax/login/user-area HTTP/1.1
1446	56.624004	177.11.254.183	192.168.1.35	TCP	60	80->56217 [ACK] Seq=38662 Ack=6817 Win=17152 Len=0
1447	56.624005	177.11.254.183	192.168.1.35	TCP	60	80->56217 [ACK] Seq=38662 Ack=7105 Win=17152 Len=0
1448	56.629422	177.11.254.183	192.168.1.35	TCP	563	[TCP segment of a reassembled PDU]
1449	56.629871	177.11.254.183	192.168.1.35	HTTP	925	HTTP/1.1 200 OK (text/html)
1450	56.629925	192.168.1.35	177.11.254.183	TCP	54	56217->80 [ACK] Seq=7105 Ack=40042 Win=65024 Len=0

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

Wireshark - Follow TCP Stream (tcp.stream eq 74) - wireshark\_F6067C02-77AF-4F6B-B300-C9ABA44982A\_20160915094601\_a06288

GET /cprocura?fromSearchBox=true&produto=canon HTTP/1.1  
Host: www.buscape.com.br  
Connection: keep-alive  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8  
Referer: http://www.buscape.com.br/  
Accept-Encoding: gzip, deflate, sdch  
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.6,en;q=0.4  
Cookie: xpwmy=1Kk0; \_bid=28291b1d-3c9b0946fb2b1; BTG360\_utms=; btg\_lastprod=[{"ids": ["345394"]}; \_spl\_pv=1; xb=Telefone&telefone=Carro&canon=&canon&canon=&cal%5E7t%canon&canon; xr=1=canon; idloc=189181291520160913164808457; buscape=189181291520160913164753&cn=2073969380&rb=6719dc910f1307df24815072d04a44cb; bpc=dupv=2016-09-15+09%3A41%3A26&duvcso=%uso+0%tzu+0%pr=0%cn+e6719dc910f1307df24815072d04a44cb; sessao3=rfin=NO-REFERERERsite\_origem=9402546&kw=canon&kw=canon&cna=2073969380&st=1&dppv=2016-09-15+09%3A41%3A26&id\_entrad=site\_origem%3D9402546&ntab=HOME&tab=padrao&dtab=15-09-2016-10%3A01&exp\_cont=gcsc%3Dv20150129%2ddata\_create\_exp\_cont%3D147394326645&xr=3+4a3ee0b08601e2c4bfbd5770b2dd3b&bx=false&wt=null; refererPage=home; \_utmt=1; \_utma=243682202,1030198133,1473796079,1473865156,1473943301,3; \_utmb=243682202,1.10,1473943301; \_utmc=243682202,1473796084.1.1.utmc=rs(direct)|\_utmcn=(direct)|utmcn=(none); \_gat=1; tracelogger=; tt\_c\_vmt=1473943303; tt\_c\_s=direct; tt\_c\_m=direct; \_gat\_UA-1827174-76=1; \_ttuu.s=1473943303069; tt\_u=7508000442C14572242948302ACBBFA; tt\_npfr= OAX/nEH4FFV/yACOGx; nav12680=60868354a175dd2567ee06a5609\_2\_260\_Sao Paulo\_Sao Paulo\_Brazil\_AB; \_ga=GAI.3.1030198133.1473796079

HTTP/1.1 301 Moved Permanently  
Server: Apache-Coyote/1.1  
Connection: keep-alive  
Set-Cookie: redirect\_cookie=; Domain=.buscape.com.br; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/  
Cache-Control: no-cache  
Location: http://www.buscape.com.br/cprocura/canon  
Set-Cookie: redirect\_cookie=true; Domain=.buscape.com.br; Expires=Thu, 15-Sep-2016 15:33:23 GMT  
Set-Cookie: buscape=189181291520160913164753&cn=135856864&rb=c45f01d856e9275a12001c07f03fdd2f1; Domain=.buscape.com.br; Expires=Tue, 14-Sep-2021 12:46:43 GMT; Path=/  
Set-Cookie: bpc=dupv=2016-09-15+09%3A46%3A43&duvcso=%uso+0%tzu+1%pr=0%cn+135856864&rb=0501b49c9903993008d2e9af4bf9ab48; Domain=.buscape.com.br; Expires=Tue, 14-Sep-2021 12:46:43 GMT; Path=/  
Set-Cookie: sessao3=rfin=NO-REFERERERsite\_origem=9402546&kw=canon&kw=canon&cna=135856864&st=1&dppv=2016-09-15+09%3A41%3A26&id\_entrad=site\_origem%3D9402546&ntab=HOME&tab=padrao&dtab=15-09-2016-10%3A01&exp\_cont=gcsc%3Dv20150129&xr=3+a7cff9cd3496b4543be678468c3765&bx=true&wt=canon&correcao=BuscaFuzzy@; Domain=.buscape.com.br; Path=/  
Set-Cookie: tracelogger=; Domain=.buscape.com.br; Path=/  
P3P: policyref="http://www.buscape.com.br/w3c/p3p.xml", CP="PSA CONO OUR ONL BUS NOI"

Packet 1005. 4 client pkt(s), 32 server pkt(s), 7 turn(s). Click to select.

Entire conversation (83 KB) Show and save data as ASCII

Find: Filter Out This Stream Print Save Find Next Help

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.