

# 4 - Montando nossa rede no programa

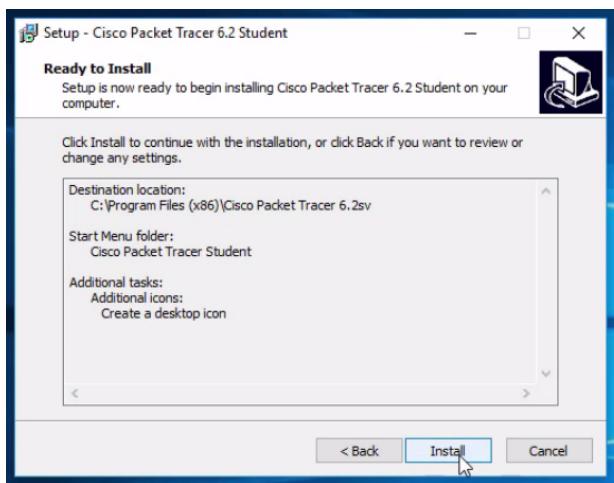
## Instalando Packet Tracer

A nossa rede está crescendo e já interconectamos três computadores, imagine quando fizermos o mesmo com cinco máquinas. Ficará muito confuso... A partir de agora, para ficar mais fácil para trabalharmos com estas redes, usaremos um software para simularmos o comportamento das redes. Ele foi criado pela Cisco, um dos fabricantes de elementos de redes.

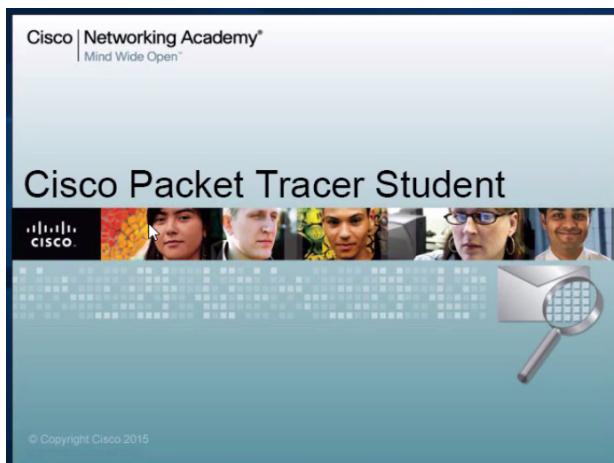
Vamos abrir o guia de instalação do Packet Tracer.

Você encontrará instruções de como instalar o Packet Tracer clicando [aqui](#). A demonstração de como instalar em Mac será feita no próximo vídeo.

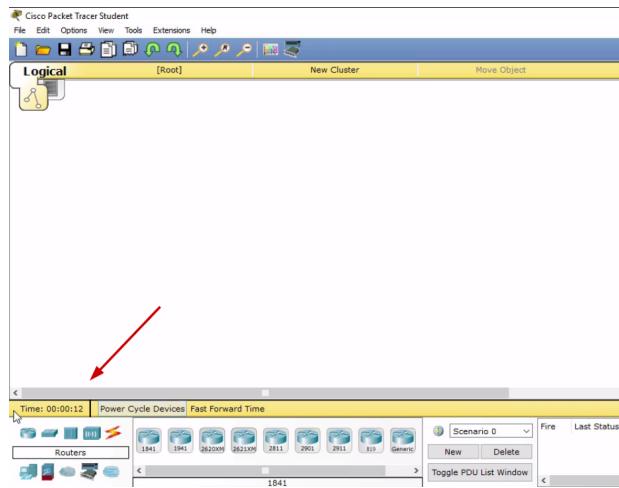
Inicialmente, clicaremos em "Next" para os primeiros passos da instalação, até chegarmos na tela "REady to Install", em que clicaremos no botão "Install".



Depois, esperaremos pelo fim do processo de instalação. Será aberta uma janela perguntando se queremos inicializar o Packet Tracer, depois, O processo será finalizado ao clicarmos em "Finish". Então, o programa será inicializado.

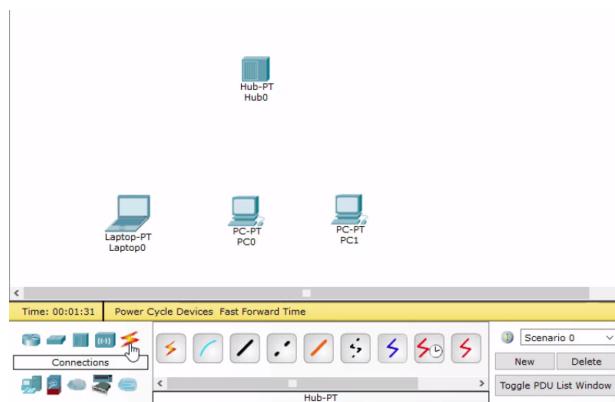


Todas as configurações do equipamentos que utilizaremos, será selecionado na parte do canto inferior da esquerda.

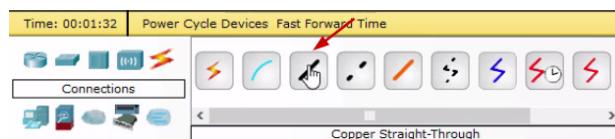


Vamos montar o projeto da última rede feita por nós. Começaremos, clicando nos "End Device" que são os dispositivos finais usados efetivamente pelos usuários.

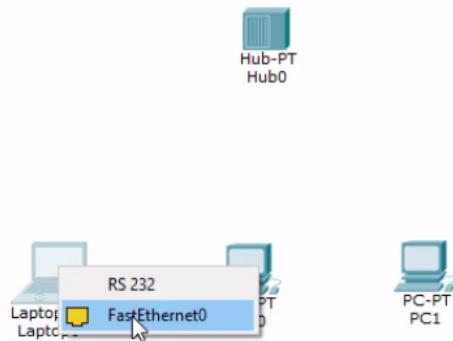
Vamos criar uma situação em que usamos três computadores e o hub.



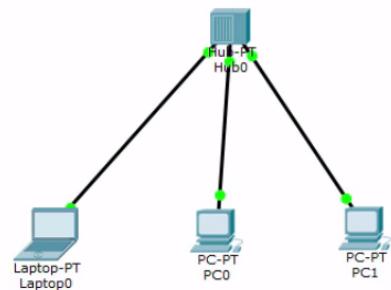
Para interconectá-los precisaremos de um cabo direto. Selecionaremos a terceira opção.



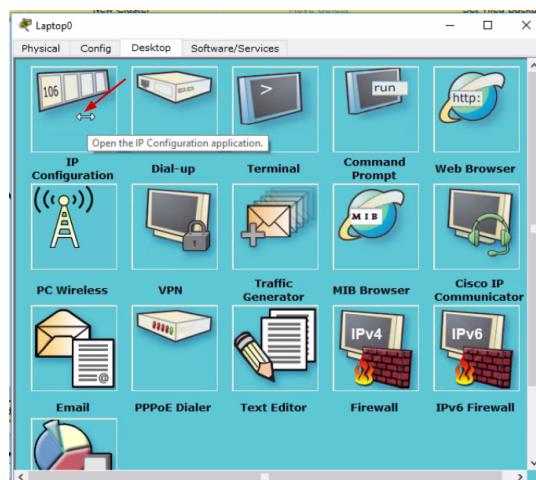
Depois, clicaremos no primeiro laptop com o botão direito e selecionaremos "FastEthernet()".



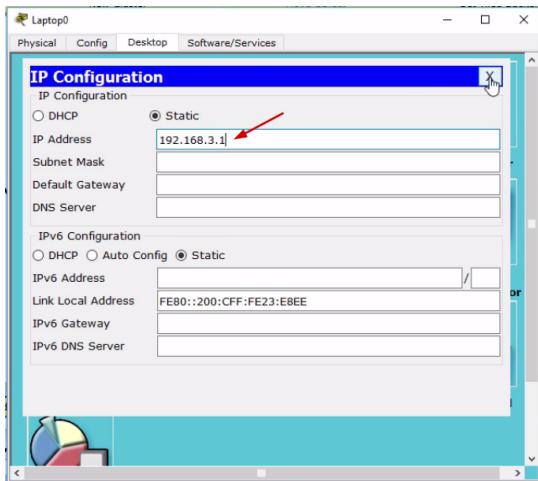
Vamos arrastar até o hub e selecionaremos um porta livre. Repetiremos o mesmo processo com as outras duas máquinas.



Já conseguimos fazer a instalação do Packet que iremos utilizar e criamos o projeto feito por nós. Mas está faltando uma parte importante, falamos que é preciso configurar um endereço de IP. Nós precisaremos criá-los manualmente. Faremos isto clicando sobre o Laptop do projeto, será aberta uma nova janela em que selecionaremos a aba "Desktop" e depois, em "IP Configuration".



Vamos preenche-lo com o mesmo IP que usamos no computador do curso.



Faremos o mesmo com as máquinas do projeto, com a diferença que mudaremos o fim dos números dos IPs, que terminaram em 2 e 3. Isto significa que o segundo terá o IP 192.168.3.2 e o terceiro 192.168.3.3.

Agora o projeto montado no estúdio está representado no Packet Tracer. Em seguida faremos alguns testes.

## Mãos à obra: Instalando o packet tracer

Etapas para o download do Packet Tracer:

- 1) Acesse o link: <https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer> e escolha a opção **Sign up today!** do *Hands-On Practice*

**Hands-On Practice**

Enroll, download and start learning valuable tips and best practices for using our innovative, virtual simulation tool, Cisco Packet Tracer. This self-paced course is designed for beginners with no prior networking knowledge. It teaches basic operations of the tool with multiple hands-on activities helping you to visualize a network using everyday examples, including Internet of Things (IoT). This introductory course is extremely helpful for anyone who plans to take one of the Networking Academy courses which utilizes the powerful simulation tool. No prerequisites required!

You'll Learn These Core Skills:

- Simulate data interactions traveling through a network.
- Visualize the network in both logical and physical modes.
- Apply skills through practice, using labs and Cisco Packet Tracer activities.
- Develop critical thinking and problem-solving skills.

[Sign up today!](#)

Length: 10 hours

Cost: Free\*

Level: Beginning

Learning Type: Online self-paced

Achievements: Badge

Languages: English, Український

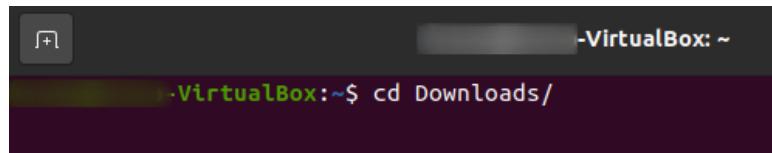
\*Self-paced classes at NetAcad.com are free. Cost for Instructor-led classes is determined by the institution.

- 2) Na janela que irá abrir, em *Enroll now*, coloque seus dados (país, mês e ano de nascimento)
- 3) Em seguida, preencha com um e-mail válido, primeiro e último nome, país, estado e o resultado de uma operação matemática.
- 4) Entre no seu e-mail e confirme que seu e-mail é válido clicando em **Activate account**
- 5) Na nova janela que irá abrir, escolha uma senha de acesso
- 6) Em seguida, ao final da página, na seção **Resources**, selecione a opção **Packet Tracer**
- 7) Atualmente a Cisco disponibilizou uma nova versão 8.0.1 que poderá ser feito o download nessa parte selecionando Download no seu sistema operacional. Caso deseje fazer o download de uma versão mais antiga que mais se assemelha à utilizada no curso, siga para o próximo item
- 8) Caso deseje fazer o download da versão mais antiga, siga para o fim da página em **Previous versions** e faça o download respectivo ao seu sistema operacional

**Obs:** Caso seja Linux:

- 1) Fazer o download da versão do Packet Tracer para Ubuntu Desktop;
- 2) Abrir o Terminal de Comandos através das teclas Ctrl + Alt + T ou através do menu de aplicativos;
- 3) Navegar até o diretório onde se encontra o arquivo de instalação do Packet Tracer através do comando: `cd <caminho do download>`

Exemplo:



- 4) Digitar, em sequencia, os seguintes códigos para atualizar a fonte de pacotes do Linux e instalar algumas dependências:

- `sudo apt update`
- `sudo apt upgrade`
- `sudo apt install dialog`
- `sudo apt install libgl1-mesa-glx`
- `sudo apt install libxcb-xinerama0-dev`

(Será requisitado a sua senha de usuário administrador e, caso seja necessário, confirme a instalação dos pacotes selecionando a opção `<S>` ou `<Y>`).

- 5) Em seguida, digite o seguinte código com o nome do arquivo de instalação para prosseguir com a instalação do Packet Tracer:

- `sudo dpkg -i <nome do arquivo de instalação>`

- 6) Por fim, basta aceitar os termos da licença que será mostrada no processo de instalação:

Após esse processo, o programa deverá estar instalado com sucesso no computador!

**Obs:** Caso seja MAC:

- Faça o download para a versão do sistema operacional **Mac OS**;
- Acesse o arquivo de instalação e siga os passos indicados, aceitando os termos e inserindo a senha de usuário quando requisitada.

Pronto! O Packet Tracer já está instalado!

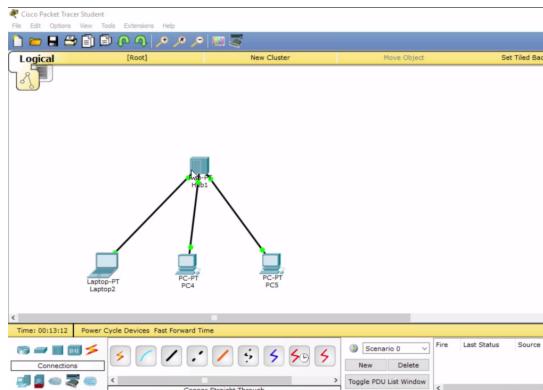
## Mãos à obra: Criando nossa primeira rede

- No canto inferior esquerdo, clique em `End Devices` e arraste o computador para a área de trabalho. Faça isso ao todo 3 vezes;
- Posteriormente, clique no ícone `Hubs` e arraste o objeto para área de trabalho;
- Clique no ícone `Connections`, selecione `Copper straight-through` (Cabo direto), normalmente a terceira opção, e faça a conexão na porta `FastEthernet` dos computadores com o Hub;
- Clique em cada um dos computadores -> aba `Desktop` -> `IP Configuration`. Atribua um IP para cada computador: `192.168.3.1`, `192.168.3.2` e `192.168.3.3`

- Na aba **Desktop**, selecione **Command prompt** e escreva **ping (#endereço IP de um dos outros dois computadores#)**. Cada computador deverá conseguir realizar o **ping** dos outros dois!
- Então, clique na opção de simulação, abra o **Command prompt** e digite novamente **ping (#endereço IP de um dos outros dois computadores#)** e depois vá clicando no botão **Capture/Forward** para verificar como a informação vai passando.

## Limitação Hub

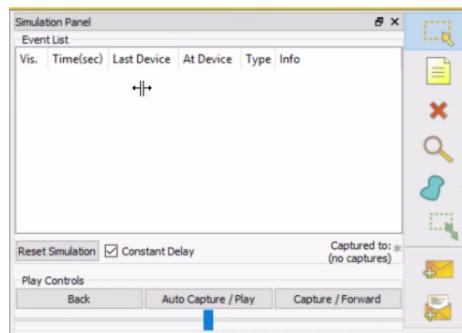
Temos no programa de simulação a rede criamos anteriormente em que temos três computadores interconectados com o hub.



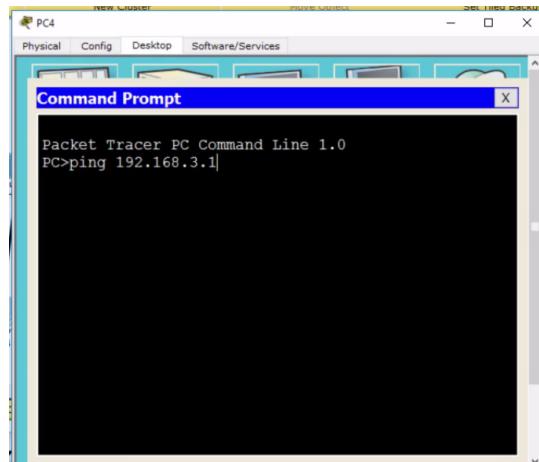
Nós temos os IPs de cada uma das máquinas e agora, iremos testar a conectividade entre eles. Mesmo usando um programa de simulação, teremos que ir no Terminal como teríamos que fazer em outros casos. Mas antes, iremos quebrar em algumas etapas menores que serão analisadas. No canto direito do Packet Tracer mudaremos o modo de operação de "Realtime" para "Simulation".



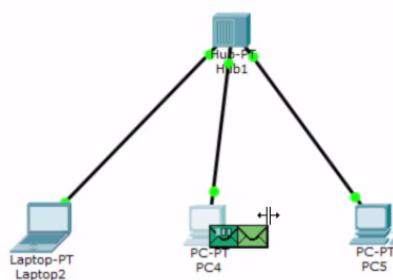
Observe que surgirá a coluna "Simulation Panel".



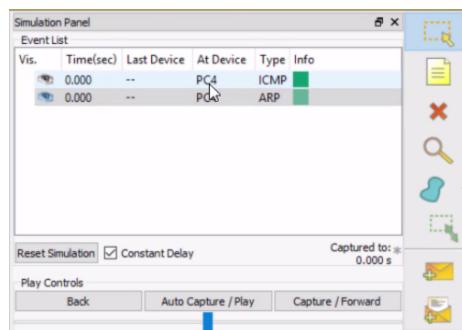
Nela, começará a parecer alguns protocolos de rede que analisaremos. O computador "PC-PT PC4" realizará meu teste de conectividade com o "Laptop-PT Laptop 2". Clicaremos sobre o ícone, clicaremos em "Command Prompt" e digitaremos `ping` e o endereço IP do desktop.



Observe que agora veremos pequenos envelopes acima do ícone de representação do computador.

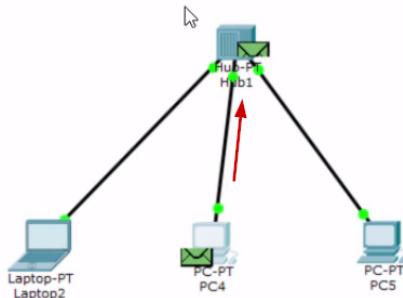


Eles também aparecerão nos protocolos.

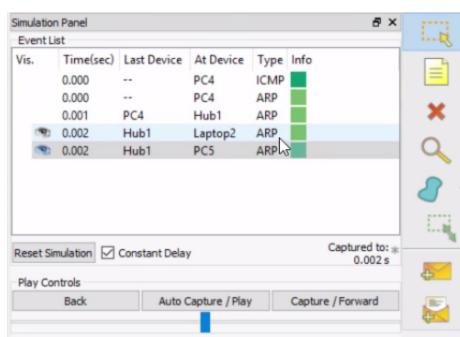


Dentro do `ping` digitado no Command, teremos o protocolo ICMP, que está aparecendo na coluna. E o que significa o ARP? A primeira vez que o computador quer se comunicar com o IP, ele não sabe onde estará localizado. É preciso perguntar para todos os dispositivos que estão na nossa rede.

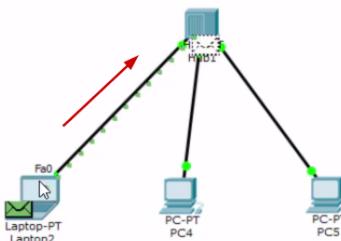
Então, clicaremos em "Capture/Forward".



O hub não tem informação aonde está conectado o equipamento com o IP do laptop, então, ele passará pelas outras portas perguntando quem tem essa informação. Observe que ele enviará protocolo ARP para descobrir.



O terceiro computador recebeu a requisição e descartou a informação. Isto aconteceu, porque ele não tem o IP que estamos procurando. Estamos buscando o IP **192.168.3.1** e a terceira máquina tem o IP **192.168.3.3**. Já o primeiro computador recebeu a informação e terá que devolvê-la informando sua informação.



Já sabemos que a requisição veio da segunda máquina e a terceira não deveria receber a requisição. Mas a última máquina continua recebendo informação. Esta é uma das limitações do hub: ele não consegue aprender aonde os computadores estão interconectados e sempre passará as informações para todos os dispositivos conectados com a porta, com exceção de quem enviou a requisição. O nome disso é Broadcast. Imagine um usuário fazendo o download de 500 mb e todos os dispositivos recebendo essa informação... Causa uma lentidão na rede.

Em relação ao hub, precisamos falar também sobre a segurança da informação. A requisição que fizemos entre o segundo computador e o laptop, o hub desconhece aonde está conectado o laptop. Logo, ele enviará para todos os dispositivos que estiverem conectados. Se uma das máquinas tiver um usuário malicioso, ele pode fazer o que chamamos de análise de protocolo e decifrar o que está sendo

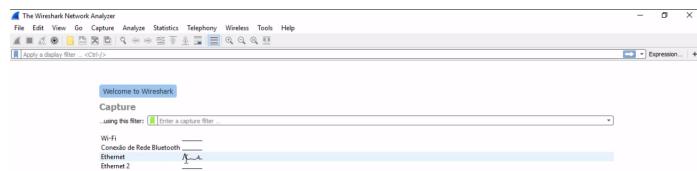
enviado pelo segundo computador. O hub representa uma lentidão, além da vulnerabilidade da segurança.

## Qual seria duas das principais limitações do Hub?

**Segurança e lentidão:** Os hubs não conseguem aprender onde está localizado cada máquina, dessa forma, ele repassa a informação para todas as demais máquinas conectadas. Isso quer dizer que caso ocorra um fluxo intenso de tráfego na rede, teremos essa informação sendo encaminhada para todos os demais usuários causando lentidão na rede. Além disso, quando usuários mandam a informação destinada para um usuário específico, os demais usuários recebem essa informação, causando assim uma vulnerabilidade de segurança.

## Wireshark http final

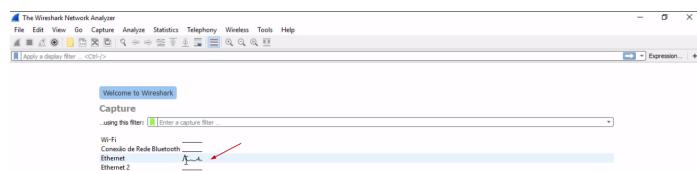
Vamos mostrar a vulnerabilidade dos hubs que conversamos. Um usuário malicioso pode entrar na nossa rede e analisar as informações que são trafegadas, por exemplo, entre um site e outra máquina. Estou no site do Buscapé, e vou simular os dois papéis - o da vítima e o do usuário malicioso. Para isto,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



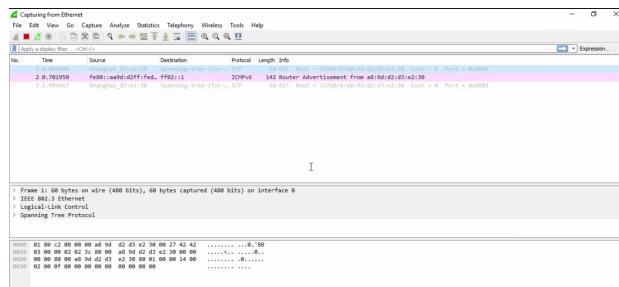
Faremos o download na página, selecionaremos o sistema operacional. No caso, escolheremos "Windows Installer (64-bit)". Se você estiver usando o Mac, encontrará orientações [nos exercícios](#).

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.

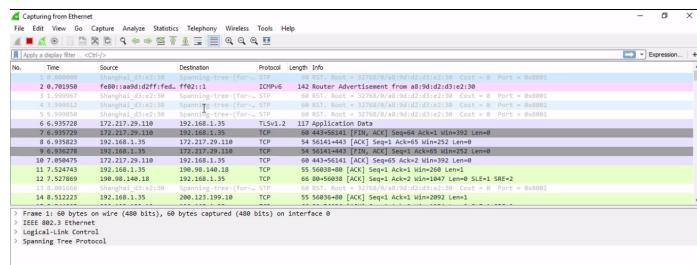


Observe que temos uma atividade na placa sinalizada. Ao clicarmos nela, veremos que temos alguns protocolos passando pela rede.

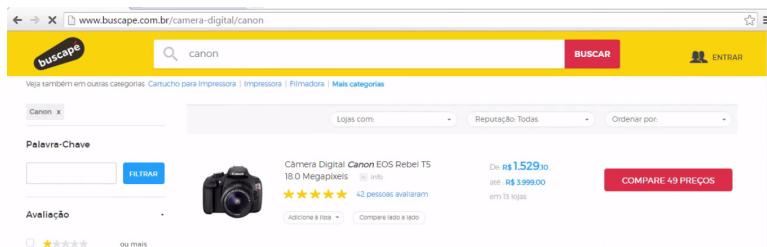


Nós não nos aprofundaremos na parte de análise de protocolo do Wireshark, porque o nosso foco é demonstrar a vulnerabilidade de um hub conectado a um usuário malicioso.

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.

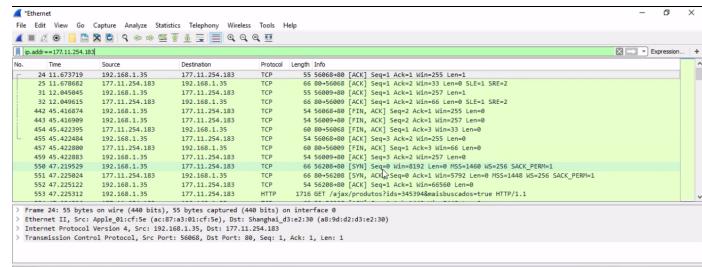


De volta ao Wireshark, veremos o que está sendo analisado pelo usuário malicioso. Ele quer descobrir qual foi o último termo de busca pesquisado pelo usuário no Buscapé. Primeiramente, será filtrado os protocolos referentes ao site Buscapé por meio do IP da máquina da empresa. É possível fazer isso no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

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

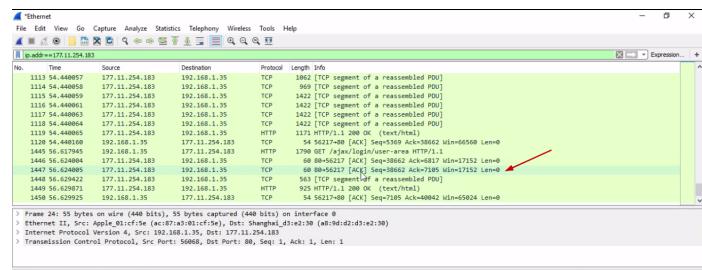
Será retornado o endereço IP da máquina do Buscapé. Após copiar o endereço IP, e vamos colocar um filtro no Wireshark para encontrarmos a máquina do Buscapé.

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

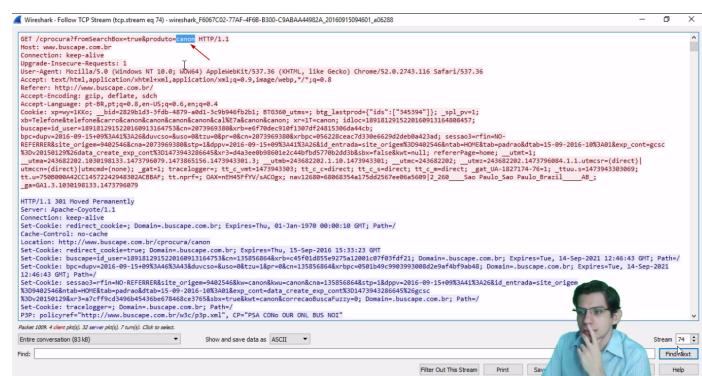


Observe a coluna de protocolo e veja que aparece diversas vezes **TCP**. O protocolo **TCP** está uma camada acima do IP, e será responsável por indicar como a comunicação será estabelecida e será transportada a informação. Se conseguirmos reconstruir o protocolo TCP, podemos ver eventualmente os **headers**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

Vamos escolher um protocolo no fim da análise.



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.

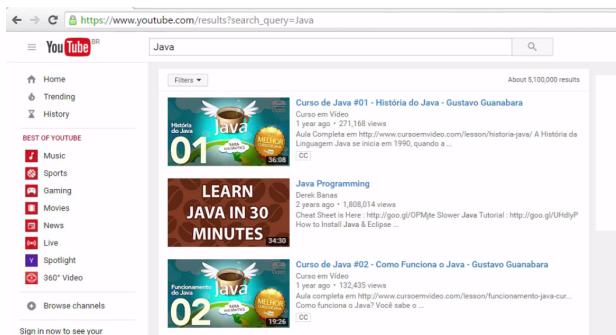
## Wireshark https final

Por que o usuário malicioso consegue ver o que a vítima pesquisou no site do Buscapé? Isto acontece porque o site não usa um sistema de criptografia. Então, é possível com uma análise de protocolo ver o que o usuário está digitando.

Vamos ver um outro cenário, acessaremos um site com sistema de criptografia, e o usuário malicioso continuará fazendo uma análise de protocolo. Vamos ver o que ele consegue descobrir. Neste caso, o site acessado será o Youtube.



O protocolo do Youtube é [Https](https://www.youtube.com), sendo que o [s](#) se refere a uma camada de criptografia. Vamos supor que alguém pesquise por "Java".



Já o usuário malicioso tentará analisar a pesquisa feita por ele. Primeiramente, será necessário descobrir o IP do Youtube. No Terminal digitaremos:

```
c:\Users\Alura>nslookup www.youtube.com
```

Teremos o seguinte retorno:

```
Prompt de Comando
Microsoft Windows [versão 10.0.10586]
(c) 2015 Microsoft Corporation. Todos os direitos reservados.

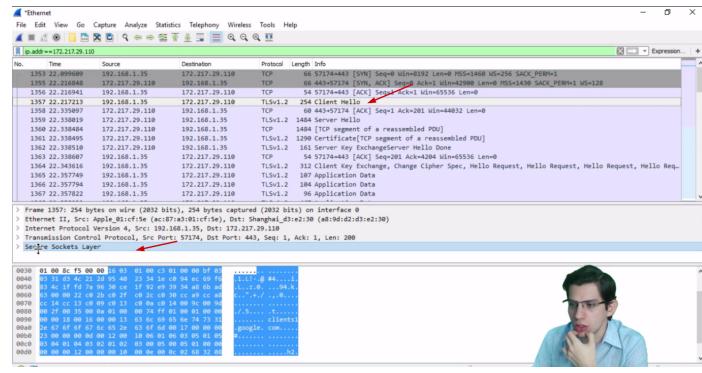
C:\Users\Alura>nslookup www.youtube.com
Servidor: openrg.home
Address: 192.168.1.1

Não é resposta autoritativa:
Nome: youtube-ui.l.google.com
Addresses: 2800:3f0:4001:802::2000
          ← 172.217.29.110
Aliases: www.youtube.com

C:\Users\Alura>
```

Depois, no filtro do Wireshark, ele digitará:

```
ip.addr == 172.217.29.110
```



É possível identificar que o Youtube foi acessado. Mas vamos clicar no protocolo indicado.

Observe que aparece a mensagem **Secure Sockets Layer**, este é um protocolo que coloca a camada de segurança na informação. É por conta desses protocolos que talvez não seja possível descobrir qual foi o termo de busca da vítima.

Mas faremos o mesmo que fizemos no exemplo passado, depois, procuraremos o protocolo **TCP** e iremos clicar sobre ele. A nova janela que será aberta, não trará informação como a anterior.



Vemos várias letras e caracteres especiais, mas está difícil identificar o que está escrito. O Youtube usou a camada de criptografia e nós não conseguimos ver o que o usuário está pesquisando.

## para saber mais: camada de protocolos

Durante a explicação eu comento que o protocolo TCP está acima da camada onde o protocolo IP está presente. Os protocolos em redes de telecomunicações seguem uma hierarquia e cada um é responsável por determinada função na comunicação.

O que acontecia antigamente no início do desenvolvimento das redes de telecomunicações é que cada fabricante desenvolvia protocolos proprietários e não era possível assim se comunicar com equipamentos de redes de outros fabricantes, criando assim o chamado "vendor lock-in".

Dessa forma, foi criado um modelo que tinha como intuito padronizar o desenvolvimento de hardware e software dos mais variados tipos de fabricantes para que pudessem assim se comunicar, mesmo que um tivesse alguns recursos a mais que o do outro fabricante, a comunicação deveria ser estabelecida. Para isso, foi definido que esses protocolos de comunicação seriam divididos em 7 camadas de comunicação, o chamado modelo OSI (Open System Interconnection). O protocolo TCP por exemplo, encontra-se na camada 4 que é conhecida como camada de transporte, o protocolo IP encontra-se na camada 3 que é conhecida como camada de rede.

A parte de protocolos é um assunto muito vasto e não é o foco desse nosso curso, mas sugiro que faça uma pesquisa sobre o modelo OSI e os principais protocolos que temos em cada camada :)

## **Qual a principal utilização do programa Wireshark?**

O Wireshark tem como principal utilização analisar protocolos que trafegam na rede com o intuito de verificar problemas que possam existir.

## **Protocolo e criptografia: protocolo utilizado para criptografar minha informação**

TLS (Transport Layer Security) seria um protocolo de criptografia utilizado para segurança da informação. Ele seria a evolução do protocolo SSL (Secure Sockets Layer).

## **Qual seria a responsabilidade do protocolo TCP?**

O protocolo TCP encontra-se acima da camada onde o IP está localizado e ele é responsável por realizar o transporte da minha informação. Além do protocolo TCP, essa camada possui também outro protocolo bastante conhecido, o UDP.

## **HTTPS: Porque não foi possível visualizar a informação que o usuário (vítima) digitou na página do youtube?**

O youtube usa em seu site um sistema de criptografia das informações, onde o protocolo TLS é responsável por essa atividade. Pelo fato das informações, estarem criptografadas não foi possível reconstruir a informação e visualizar o que o usuário estava digitando.