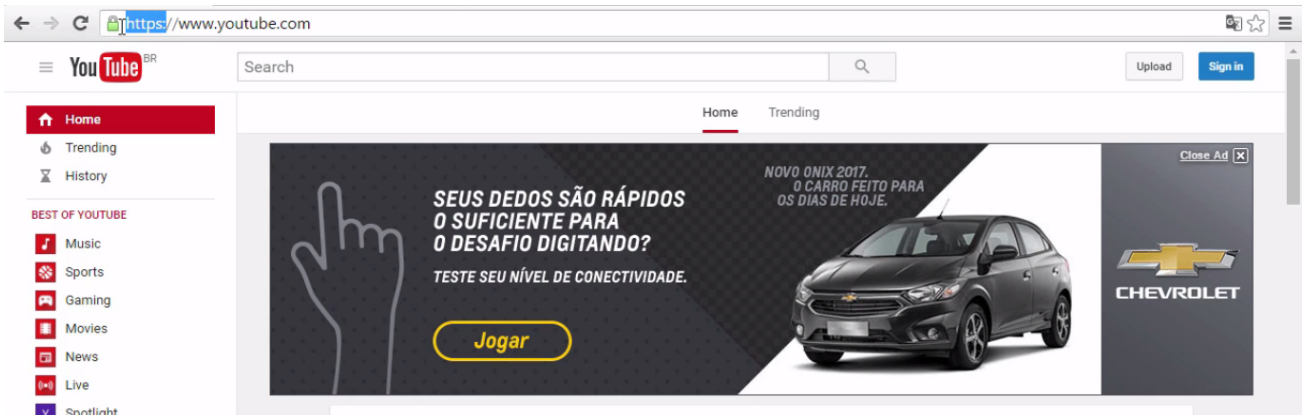
09

5 - Wireshark https final

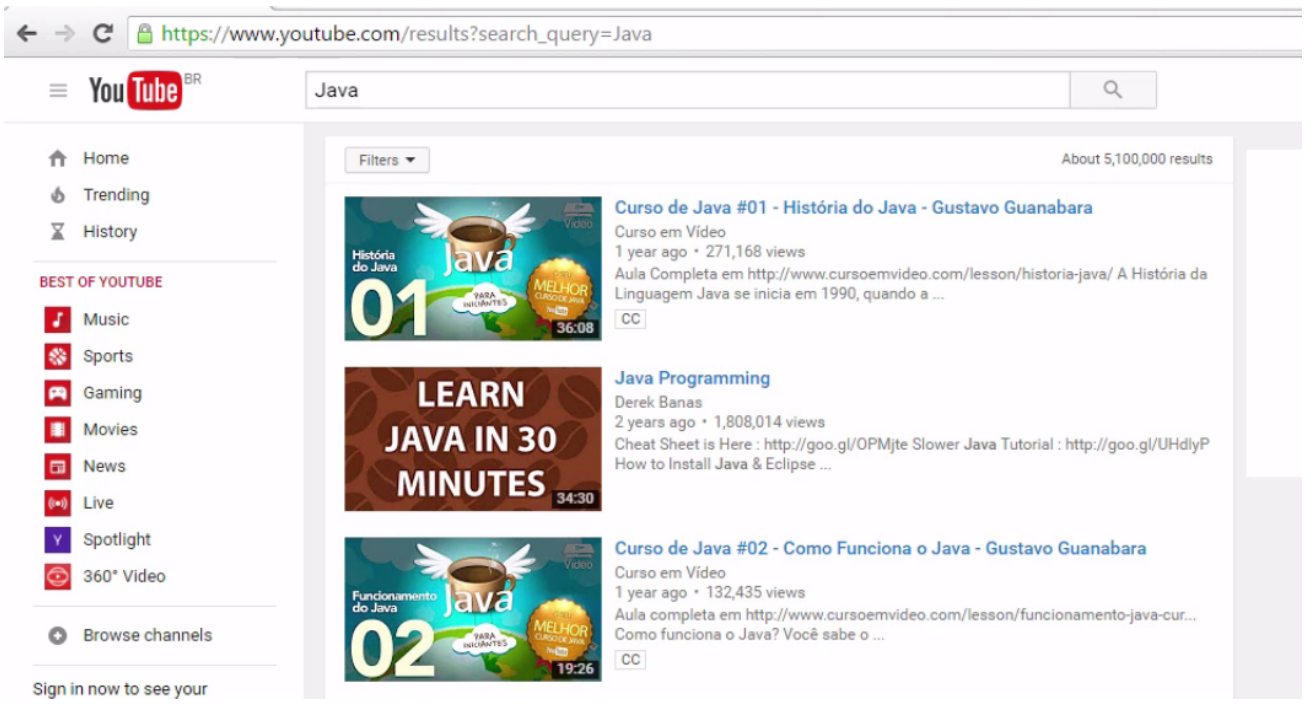
Transcrição

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.



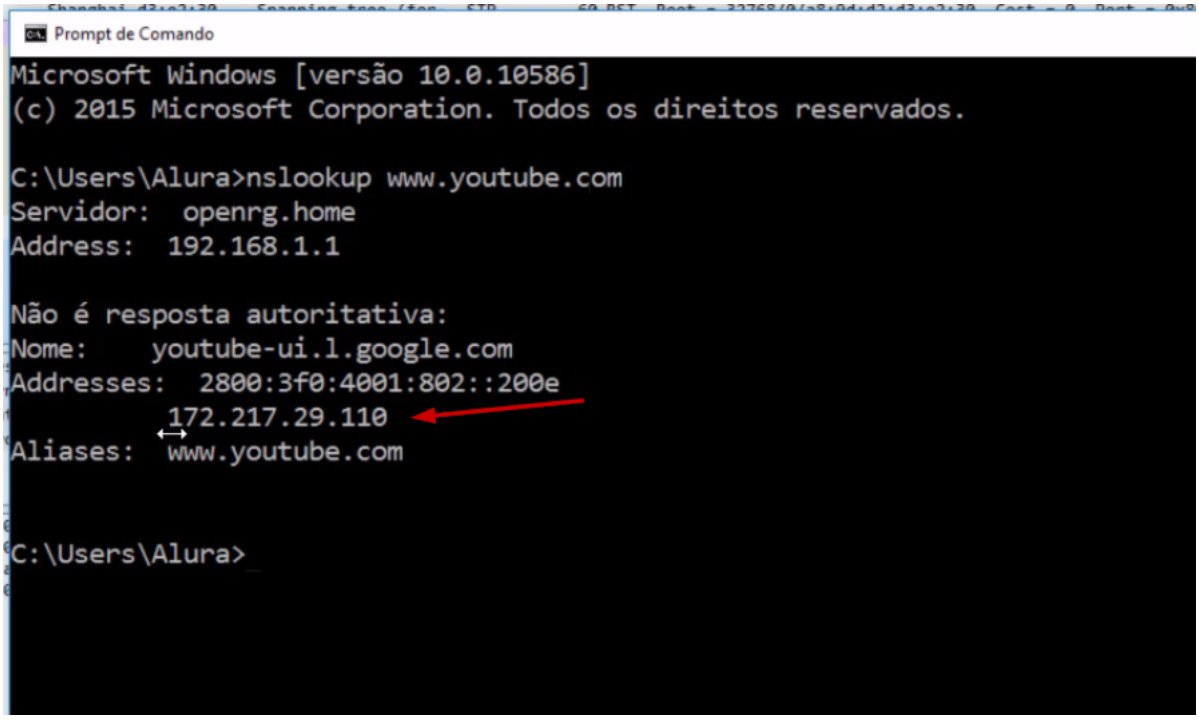
O protocolo do Youtube (https://www.youtube.com) é `Https` , sendo que o `s` se refere a uma camada de criptografia. Vamos supor que alguém pesquise por "Java".



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

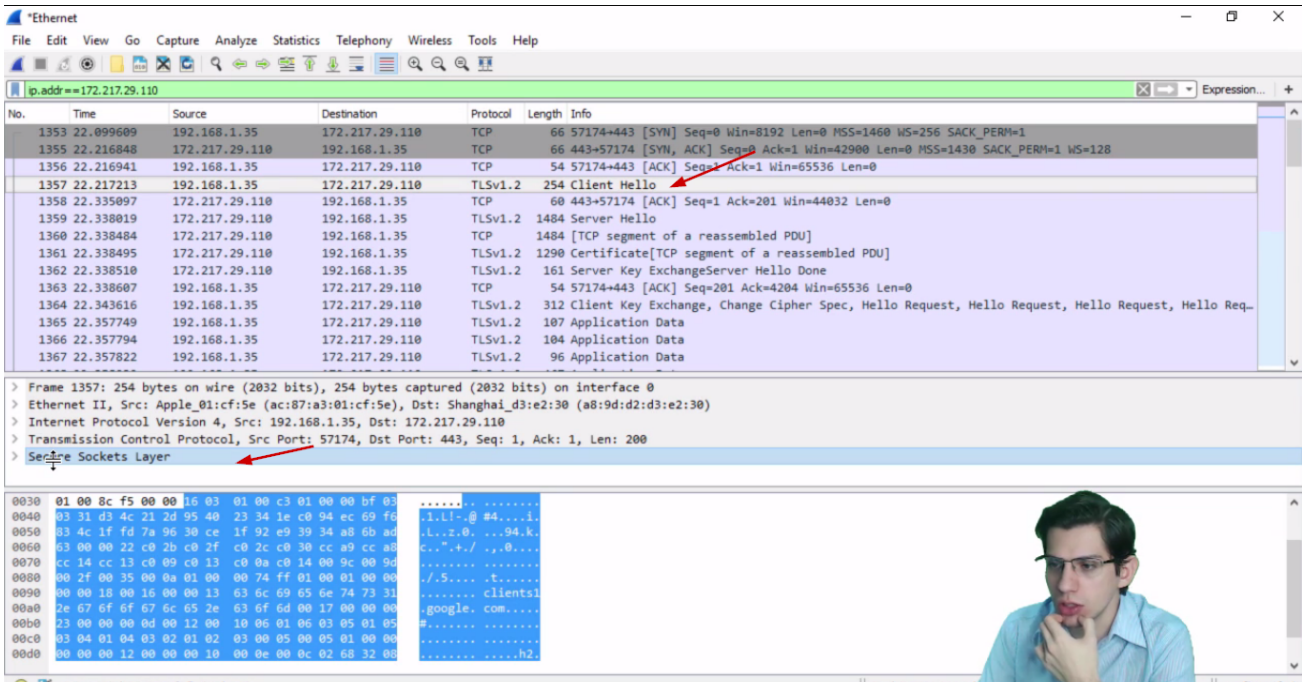
```
c:\Users\Alura>nslookup www.youtube.com
```

Teremos o seguinte retorno:



Depois, no filtro do Wireshark, ele digitará:

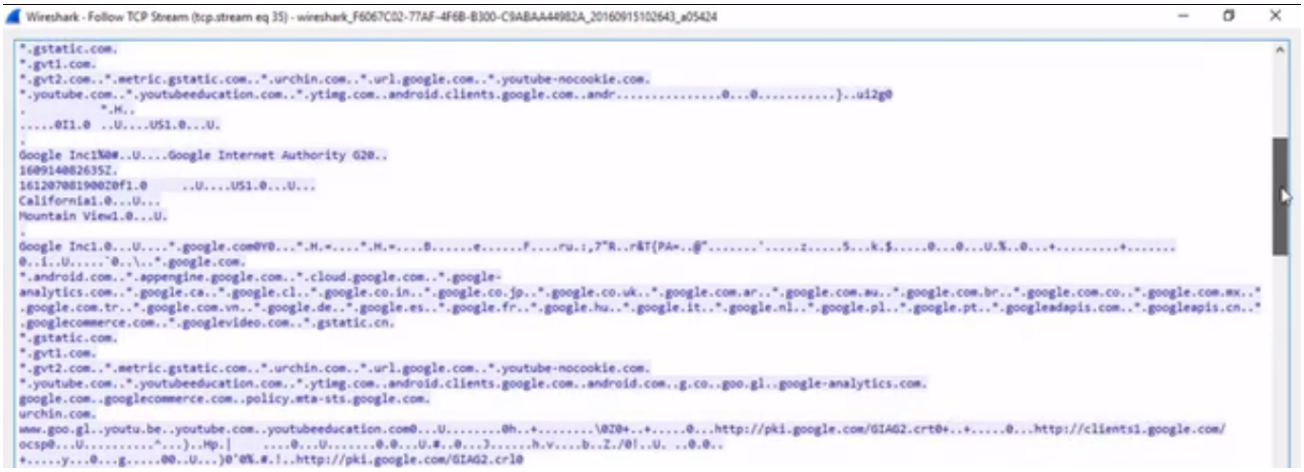
```
ip.addr == 172.217.29.110
```



È 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.