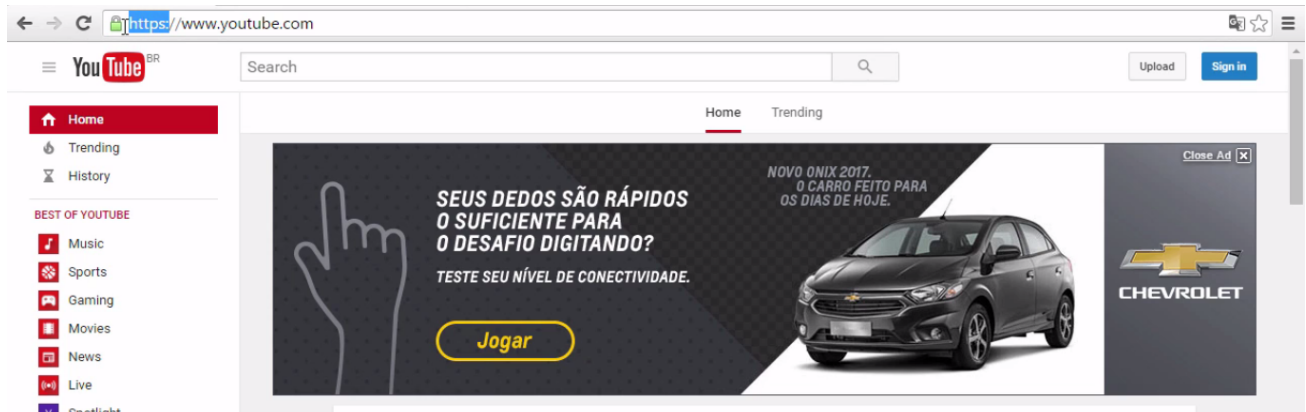


## 5 - Wireshark https final

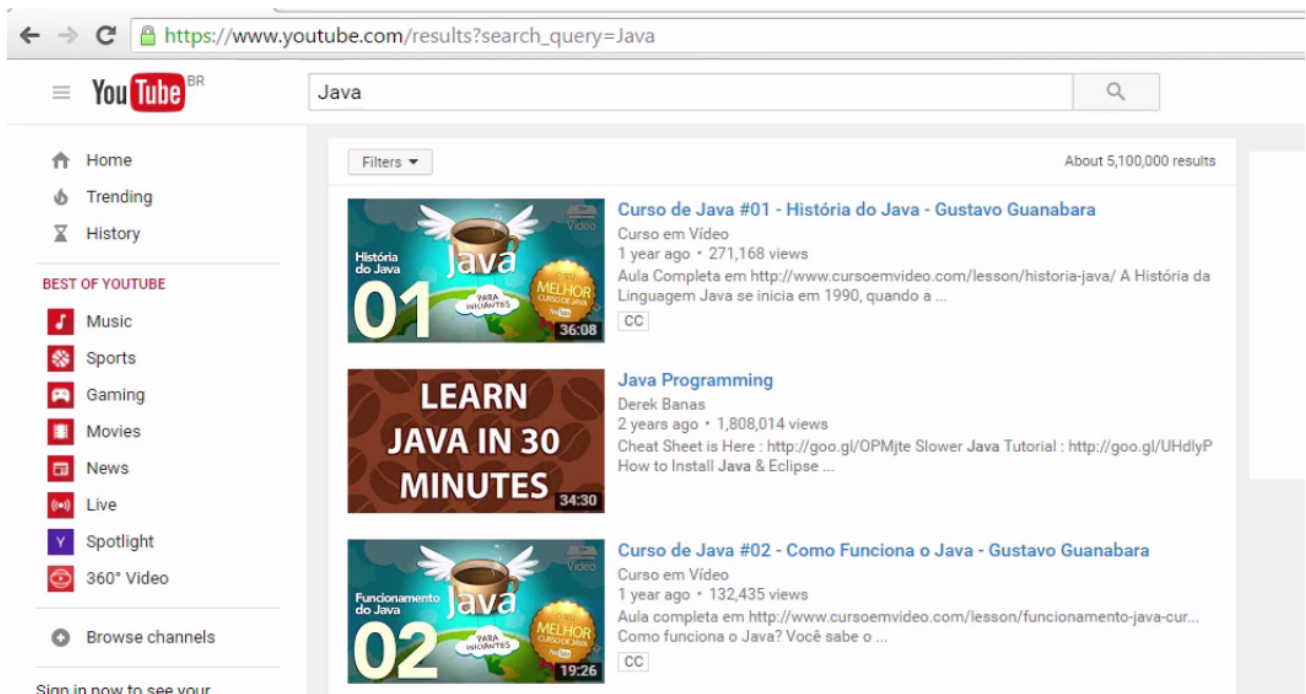
### Transcrição

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 \(https://www.youtube.com\)](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:

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

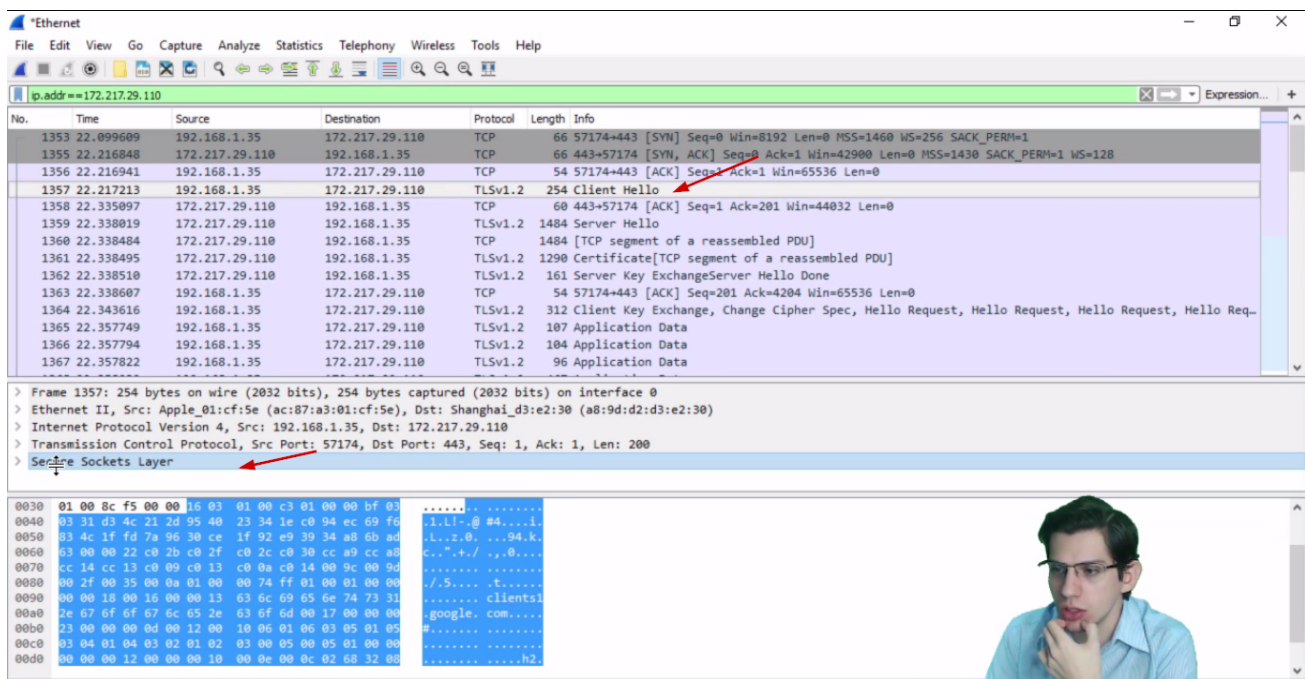
C:\Users\Alura>nslookup www.youtube.com
Servidor: openrg.home
Address: 192.168.1.1

Não é resposta autoritativa:
Nome: youtube-ui.l.google.com
Addresses: 2800:3f0:4001:802::200e
           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.

```

Wireshark - Follow TCP Stream (tcp.stream eq 35) - wireshark_f6067C02-77AF-4F6B-8300-CSABAA44982A_20160915102643_a05424

*.gstatic.com.
*.gvt1.com.
*.gvt2.com.*.metric.gstatic.com.*.urchin.com.*.url.google.com.*.youtube-nocookie.com.
*.youtube.com.*.youtubeeducation.com.*.ytimg.com..android.clients.google.com..andr.....0...0.....}.ui2g0
*.H.
.....0I1.0 ..U...U51.0...U.
.
Google IncI3W..U...Google Internet Authority G28..
1609140826352.
16129708190020f1.0 ..U...U51.0...U...
California.0...U...
Mountain View1.0...U.
.
Google IncI.0...U...*.google.com@v0...*.H=...*.H=...B.....E.....F.....rw.i,7"R..*&T(PA+..@.....'.....Z.....5...k.$.....0...0...U.%..0...+.....+.....
0..i..U...0...0...*.google.com.
*.android.com.*.appengine.google.com.*.cloud.google.com.*.google-
analytics.com.*.google.ca.*.google.cl.*.google.co.in.*.google.co.jp.*.google.co.uk.*.google.com.ar.*.google.com.au.*.google.com.br.*.google.com.co.*.google.com.mx.*
.google.com.tr.*.google.com.vn.*.google.de.*.google.es.*.google.fr.*.google.hu.*.google.it.*.google.nl.*.google.pl.*.google.pt.*.googleadapis.com.*.googleapis.cn.*
.googlecommerce.com.*.googlevideo.com.*.gstatic.cn.
*.gstatic.com.
*.gvt1.com.
*.gvt2.com.*.metric.gstatic.com.*.urchin.com.*.url.google.com.*.youtube-nocookie.com.
*.youtube.com.*.youtubeeducation.com.*.ytimg.com..android.clients.google.com..android.com..g.co..goo.gl..google-analytics.com.
google.com..googlecommerce.com..policy.eta-sts.google.com.
urchin.com.
www.goo.gl..youtu.be..youtube.com..youtubeeducation.com0...U.....0h..+.....\020+...+.....0...http://pki.google.com/GIAG2.crt0+...+.....0...http://clients1.google.com/
ocsp0...U.....0...}.Mp;| .....0...U.....0...U.#...0...3.....h.v...b..Z./0|.U...0.0..
+.....y...0...g.....00..U...}0"0k.#.l..http://pki.google.com/GIAG2.crt0

```

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.