

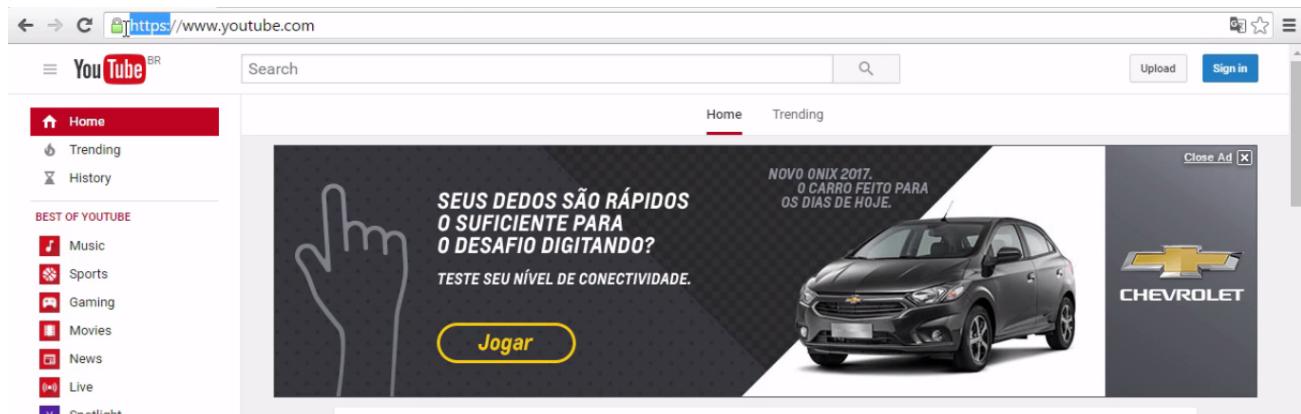
09

5 - Wireshark https final

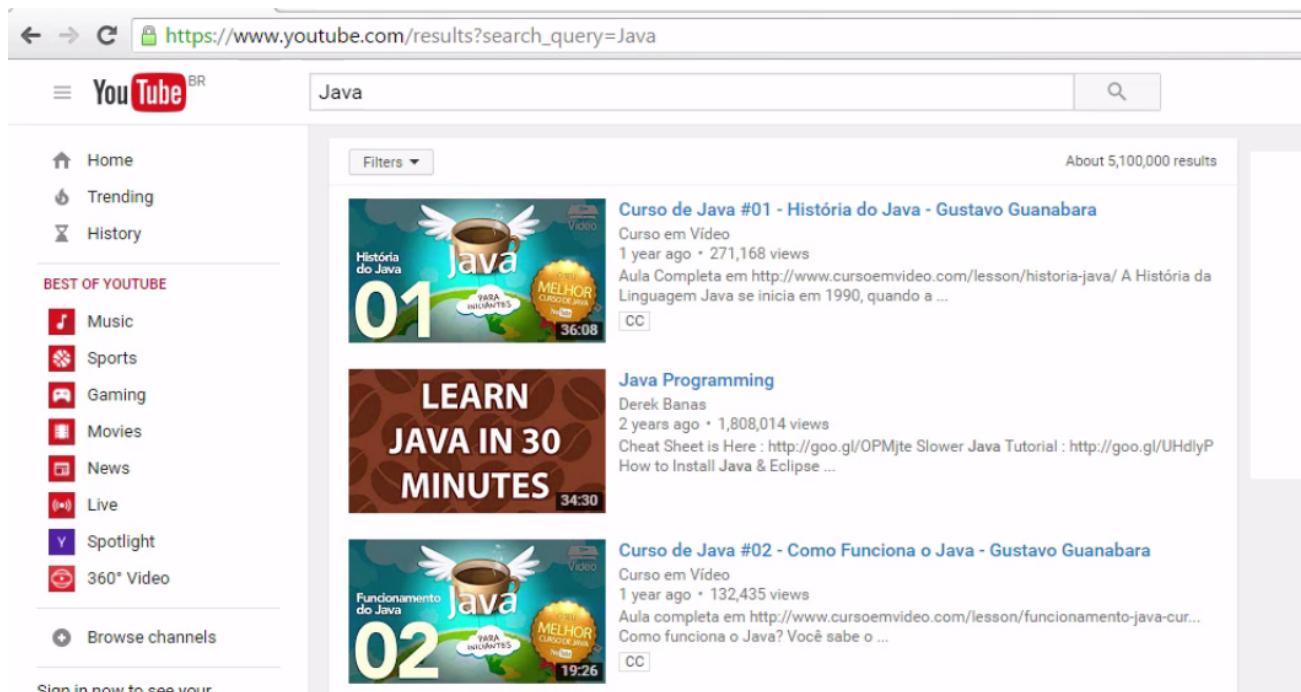
Transcrição

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.



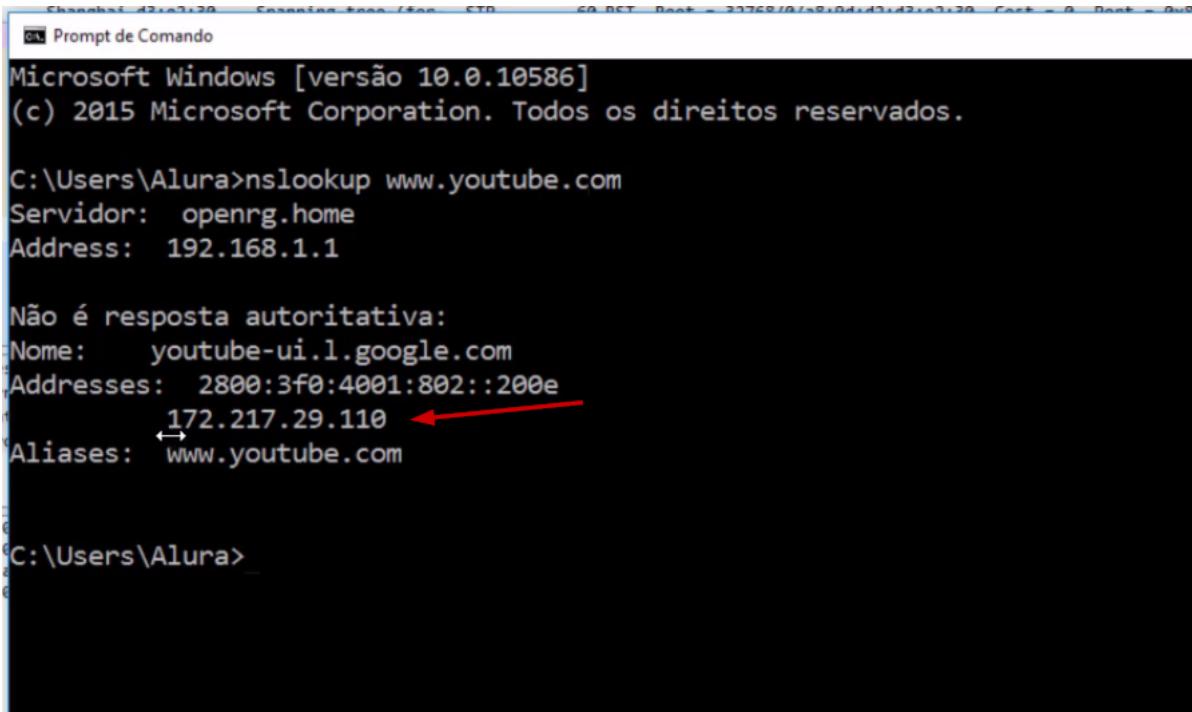
O protocolo do [Youtube \(https://www.youtube.com\)](https://www.youtube.com) é **Https**, sendo que o **s** se refere a uma camada de criptografia. Vamos supor que alguém pesquise por "Java".



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

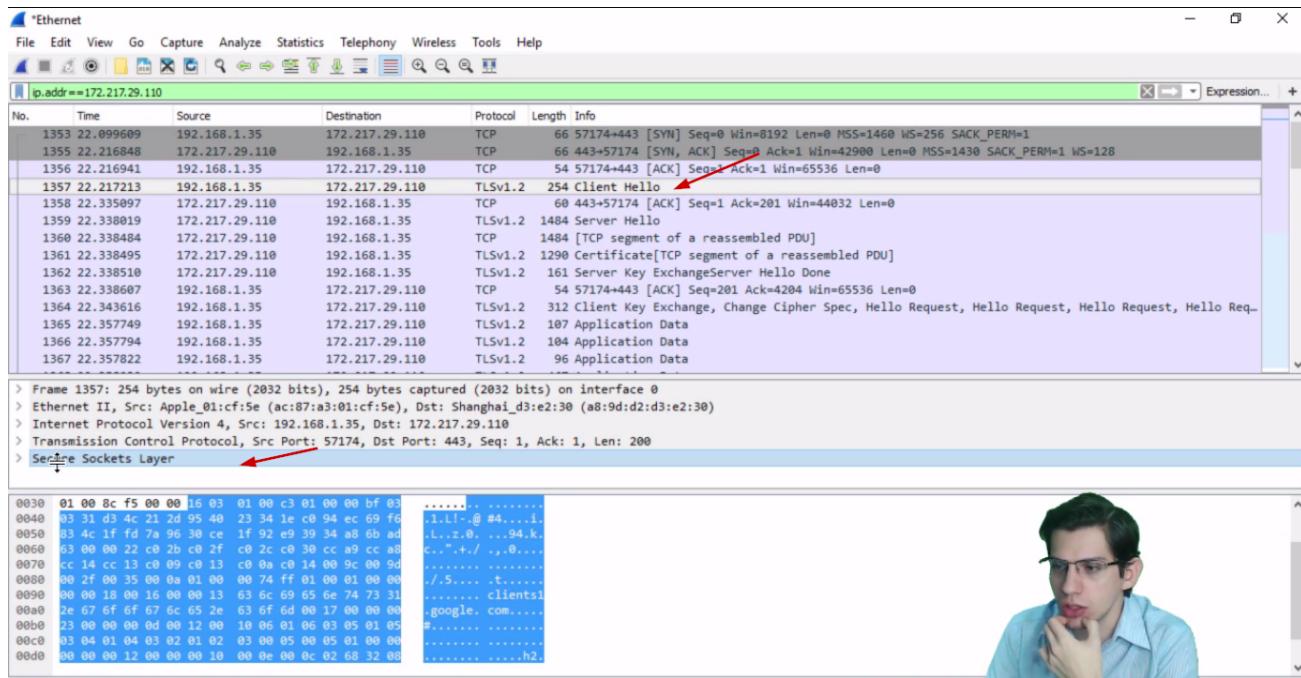
Não é resposta autoritativa:
Nome: youtube-ui.l.google.com
Addresses: 2800:3f0:4001:802::200e
          172.217.29.110 ←
Aliases: www.youtube.com

C:\Users\Alura>

```

Depois, no filtro do Wireshark, ele digitará:

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



No.	Time	Source	Destination	Protocol	Length	Info
1353	22.099609	192.168.1.35	172.217.29.110	TCP	66	57174-443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1355	22.216848	172.217.29.110	192.168.1.35	TCP	66	443-57174 [SYN, ACK] Seq=0 Ack=1 Win=42900 Len=0 MSS=1430 SACK_PERM=1 WS=128
1356	22.216941	192.168.1.35	172.217.29.110	TCP	54	57174-443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
1357	22.217213	192.168.1.35	172.217.29.110	TLSv1.2	254	Client Hello
1358	22.335097	172.217.29.110	192.168.1.35	TCP	60	443-57174 [ACK] Seq=1 Ack=201 Win=44032 Len=0
1359	22.338819	172.217.29.110	192.168.1.35	TLSv1.2	1484	Server Hello
1360	22.338484	172.217.29.110	192.168.1.35	TCP	1484	[TCP segment of a reassembled PDU]
1361	22.338495	172.217.29.110	192.168.1.35	TLSv1.2	1290	Certificate[TCP segment of a reassembled PDU]
1362	22.338510	172.217.29.110	192.168.1.35	TLSv1.2	161	Server Key Exchange/Server Hello Done
1363	22.338607	192.168.1.35	172.217.29.110	TCP	54	57174-443 [ACK] Seq=201 Ack=4204 Win=65536 Len=0
1364	22.343616	192.168.1.35	172.217.29.110	TLSv1.2	312	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request, Hello Request, Hello Request
1365	22.357749	192.168.1.35	172.217.29.110	TLSv1.2	107	Application Data
1366	22.357794	192.168.1.35	172.217.29.110	TLSv1.2	104	Application Data
1367	22.357822	192.168.1.35	172.217.29.110	TLSv1.2	96	Application Data

> Frame 1357: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface 0
> Ethernet II, Src: Apple_01:cf:5e (ac:87:a3:01:c1:f5e), Dst: Shanghai_d3:e2:30 (a8:9d:d2:d3:e2:30)
> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 172.217.29.110
> Transmission Control Protocol, Src Port: 57174, Dst Port: 443, Seq: 1, Ack: 1, Len: 200
> **Secure Sockets Layer**

```

0030  01 00 8c f5 00 00 16 03 01 00 c3 01 00 00 bf 03  .....
0040  03 31 d3 4c 21 2d 95 40 23 34 1e c0 94 ec 69 f6  .1.11-@ #4...1.
0050  03 4c 1f fd 7a 96 30 ce 1f 92 e9 39 34 a8 6b ad  .1...z.0...94.k.
0060  63 00 00 22 c0 b2 c0 2f c0 2c c0 30 cc a9 cc a8  c...+./ ..,0...
0070  cc 14 cc 13 c0 09 c0 13 c0 0a c0 14 00 90 00 9d  ...
0080  00 2f 00 35 00 0a 01 00 74 ff 01 00 01 00 00 00  ./5....t...
0090  00 00 18 00 16 00 00 13 63 6c 69 65 6e 74 73 31  .....
00a0  2e 67 6f 67 6c 65 2e 63 6c 69 65 6e 74 73 31  ..clients1.
00b0  23 00 00 00 00 0d 00 12 00 10 06 01 06 03 05 01 05  .google. com..
00c0  03 04 01 04 03 02 01 02 03 00 05 00 05 01 00 00  #.....
00d0  00 00 12 00 00 00 10 00 0e 00 0c 02 68 32 00  ....h2.

```

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.