Wi-Fi, Pt. 2

Palestra 4 - 23/05

IMEsec

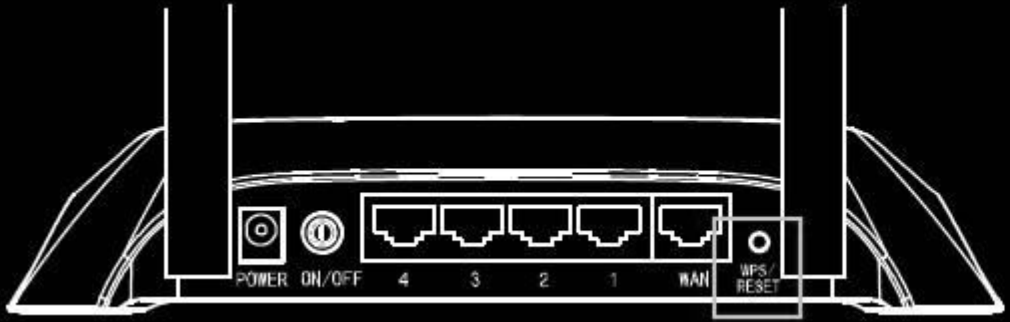
Cenário:

Usuário com poderes de editar
o roteador

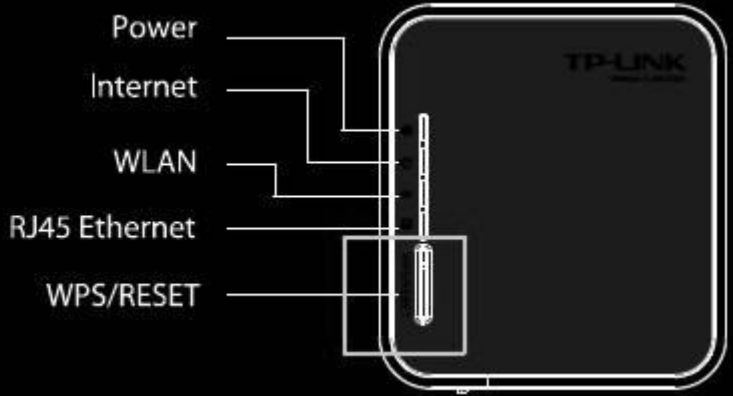
Mas como?

Acesso físico => Game Over

The Rear Panel

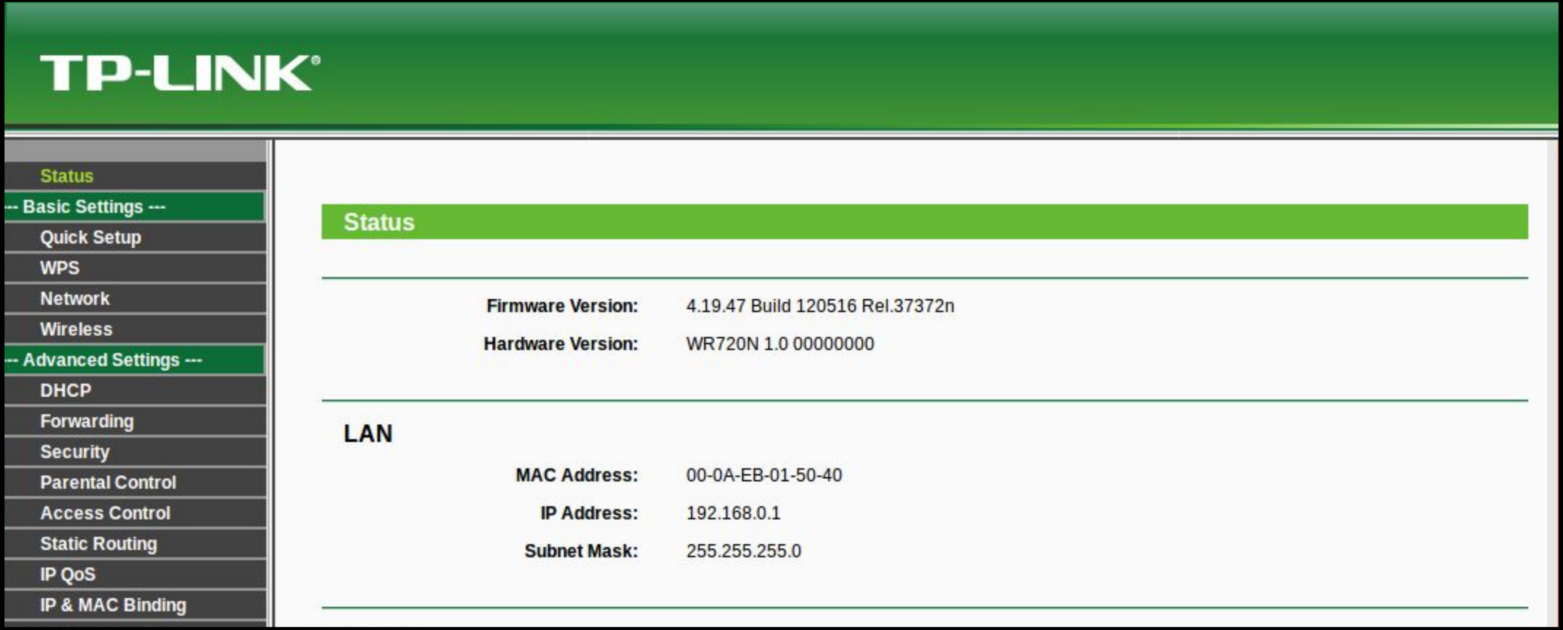


The Front Panel



Sem acesso físico?

Sem problema!



Status

Firmware Version: 4.19.47 Build 120516 Rel.37372n

Hardware Version: WR720N 1.0 00000000

LAN

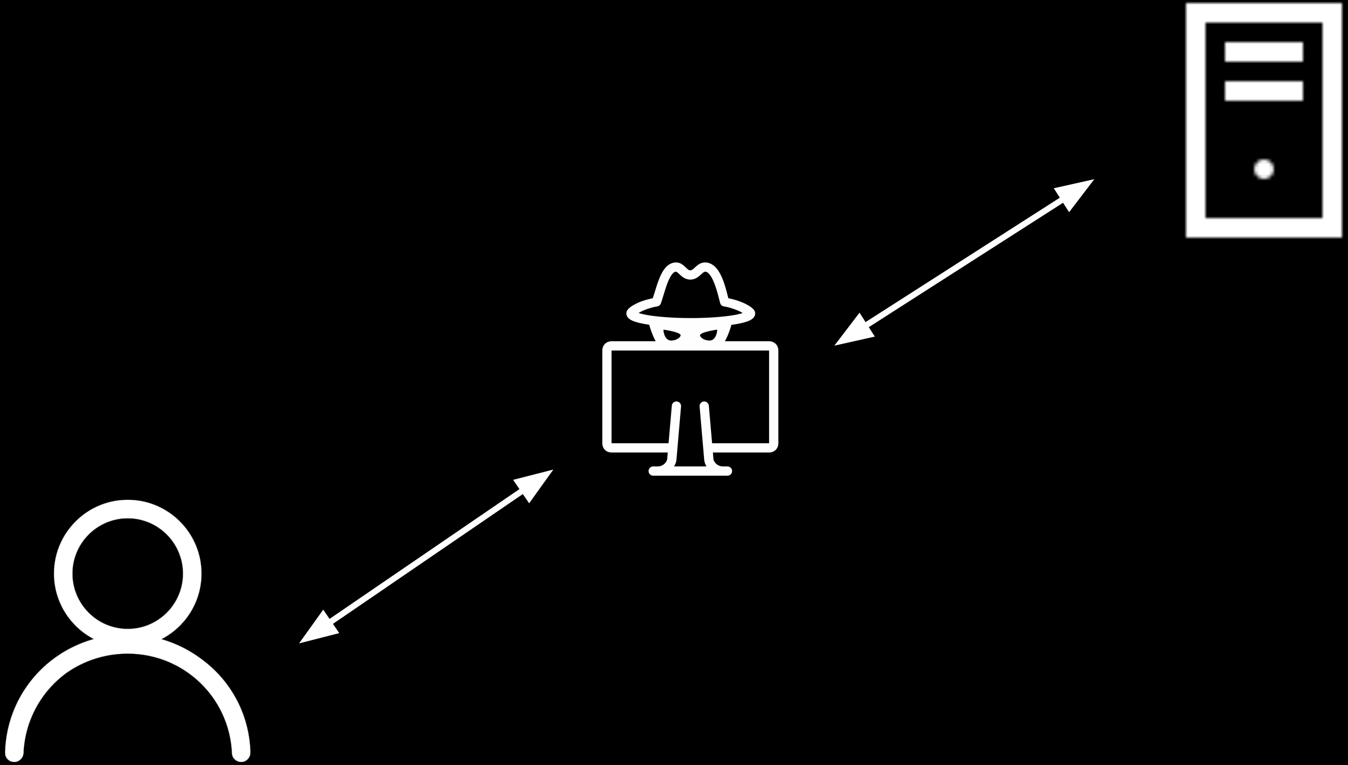
MAC Address: 00-0A-EB-01-50-40

IP Address: 192.168.0.1

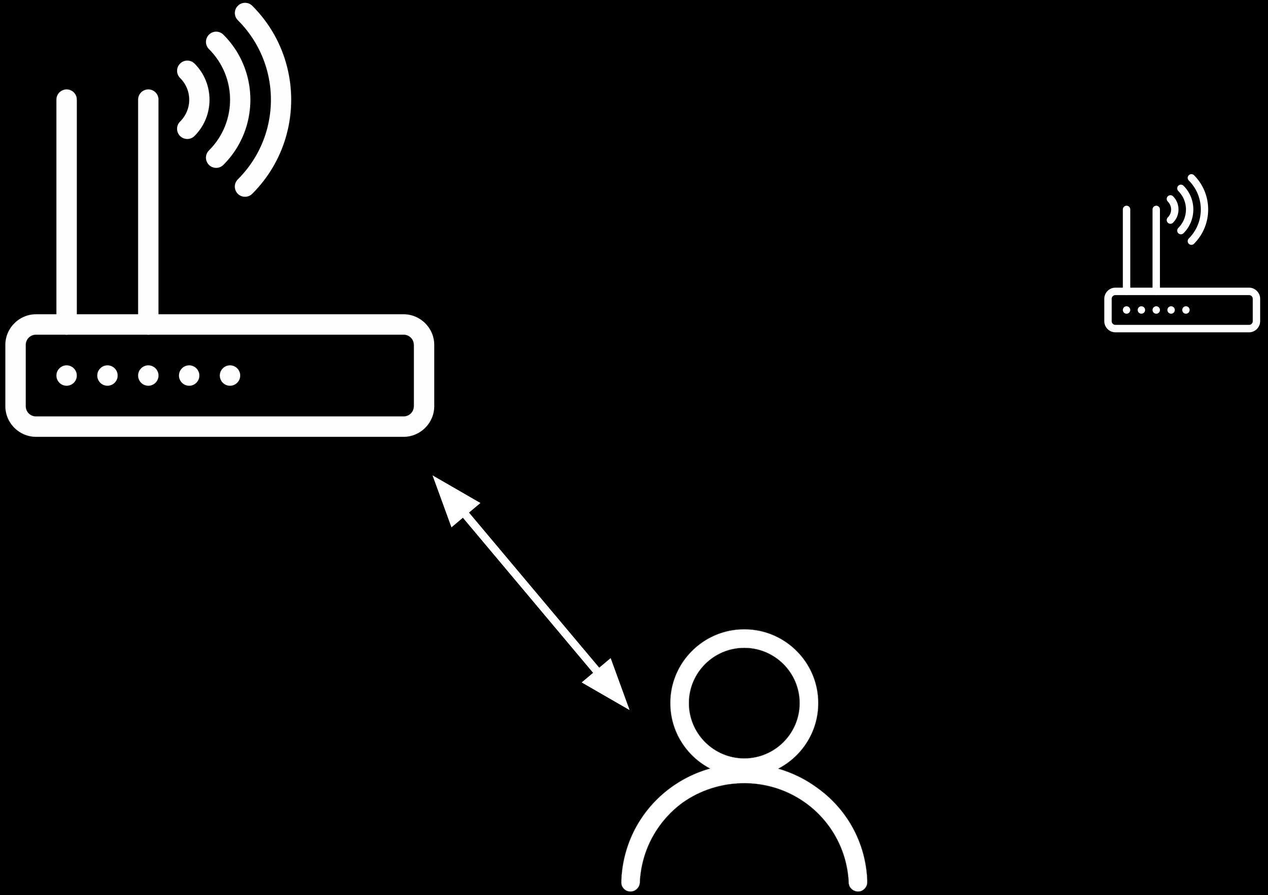
Subnet Mask: 255.255.255.0

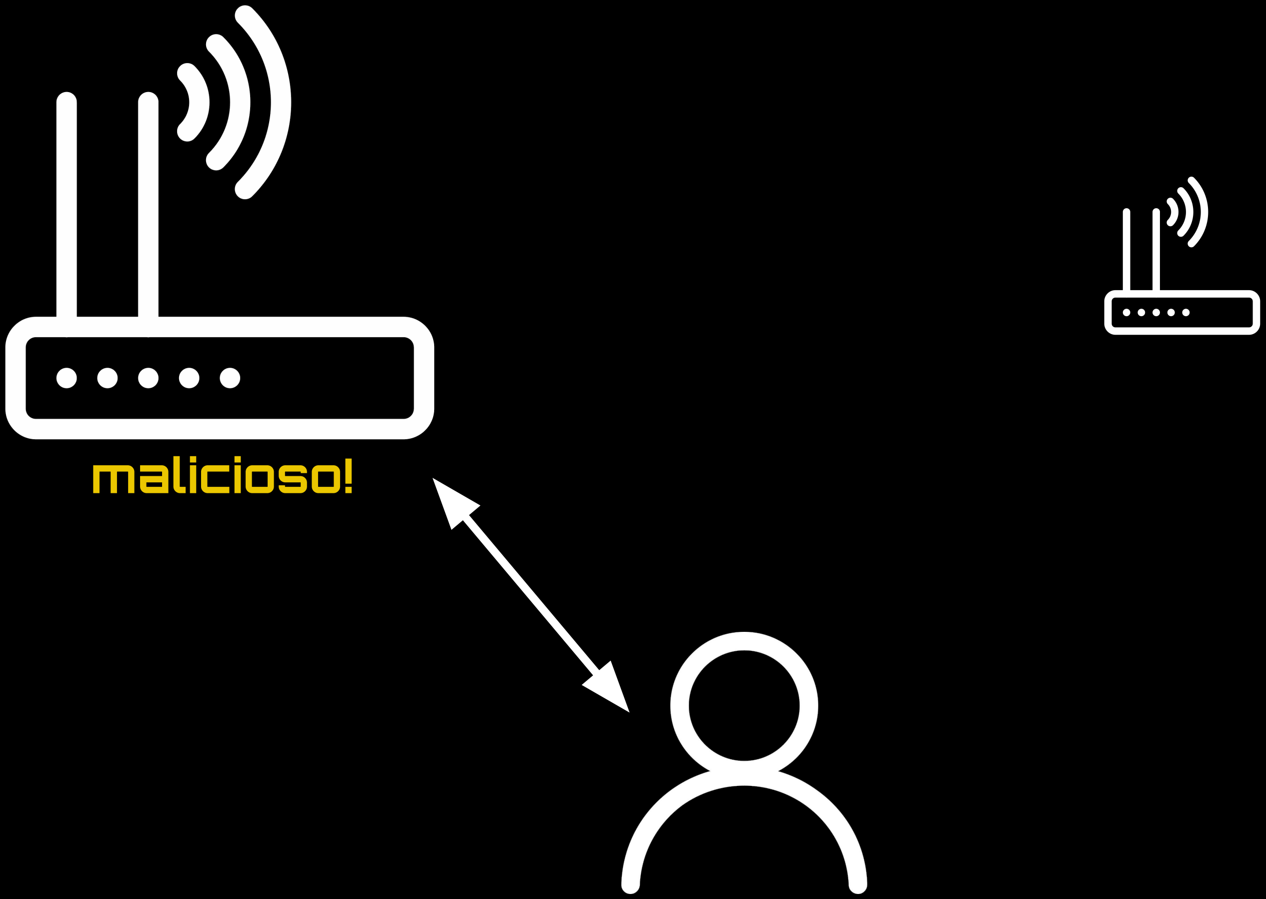
admin, admin.

Man-In-The-Middle

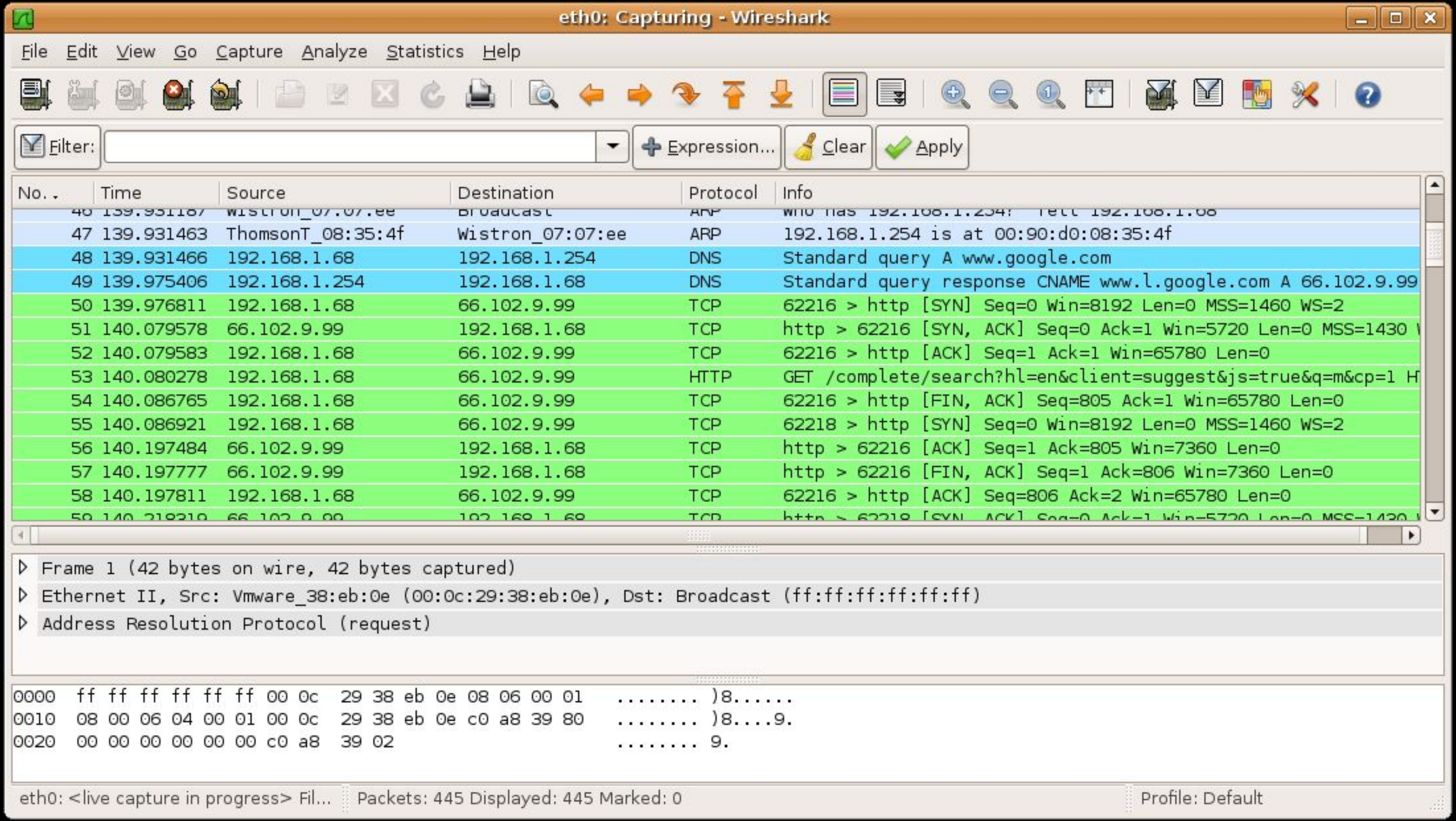


Como inserir alguém no meio…
em uma comunicação wireless?




malicioso!

Mas o que dá pra fazer?



```
No. .  Time        Source             Destination      Protocol  Info
    46 139.931187  Wistron_07:07:ee   Broadcast        ARP       Who has 192.168.1.254?  Tell 192.168.1.68
    47 139.931463  ThomsonT_08:35:4f  Wistron_07:07:ee ARP       192.168.1.254 is at 00:90:d0:08:35:4f
    48 139.931466  192.168.1.68       192.168.1.254    DNS       Standard query A www.google.com
    49 139.975406  192.168.1.254      192.168.1.68     DNS       Standard query response CNAME www.l.google.com A 66.102.9.99
    50 139.976811  192.168.1.68       66.102.9.99      TCP       62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
    51 140.079578  66.102.9.99        192.168.1.68     TCP       http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 W
    52 140.079583  192.168.1.68       66.102.9.99      TCP       62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
    53 140.080278  192.168.1.68       66.102.9.99      HTTP      GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
    54 140.086765  192.168.1.68       66.102.9.99      TCP       62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
    55 140.086921  192.168.1.68       66.102.9.99      TCP       62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
    56 140.197484  66.102.9.99        192.168.1.68     TCP       http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
    57 140.197777  66.102.9.99        192.168.1.68     TCP       http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
    58 140.197811  192.168.1.68       66.102.9.99      TCP       62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
    59 140.218319  66.102.9.99        192.168.1.68     TCP       http > 62218 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 W
```

```
▷ Frame 1 (42 bytes on wire, 42 bytes captured)
▷ Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Address Resolution Protocol (request)
```

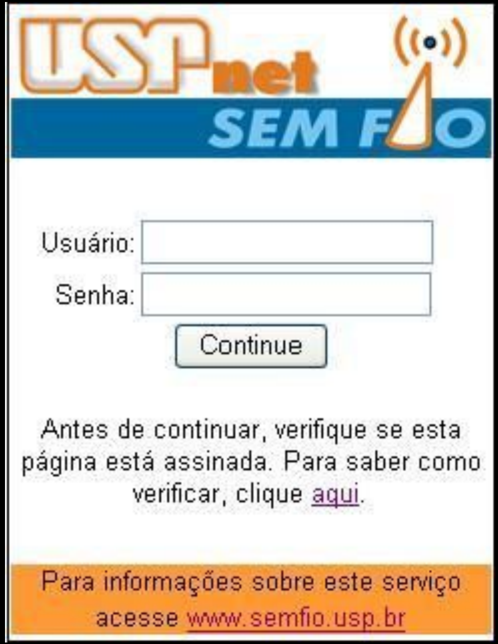
```
0000  ff ff ff ff ff ff 00 0c  29 38 eb 0e 08 06 00 01   ........ )8......
0010  08 00 06 04 00 01 00 0c  29 38 eb 0e c0 a8 39 80   ........ )8....9.
0020  00 00 00 00 00 00 c0 a8  39 02                     ........ 9.
```

eth0: <live capture in progress> Fil...

Packets: 445 Displayed: 445 Marked: 0

Profile: Default

Case: USPnet

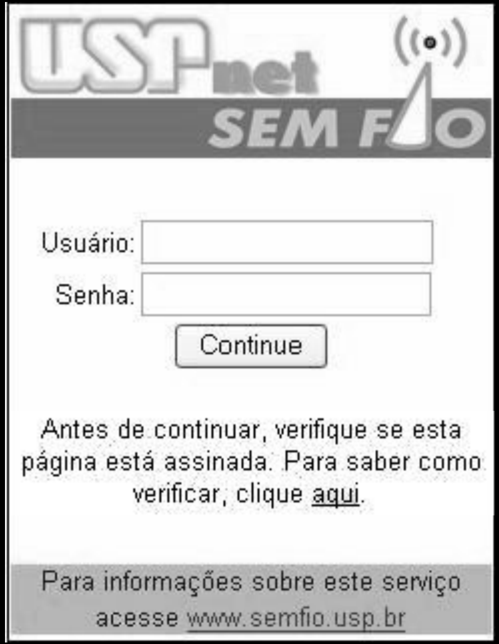


Usuário:

Senha:

Antes de continuar, verifique se esta página está assinada. Para saber como verificar, clique aqui.

Para informações sobre este serviço acesse www.semfio.usp.br



Usuário:

Senha:

Antes de continuar, verifique se esta página está assinada. Para saber como verificar, clique aqui.

Para informações sobre este serviço acesse www.semfio.usp.br

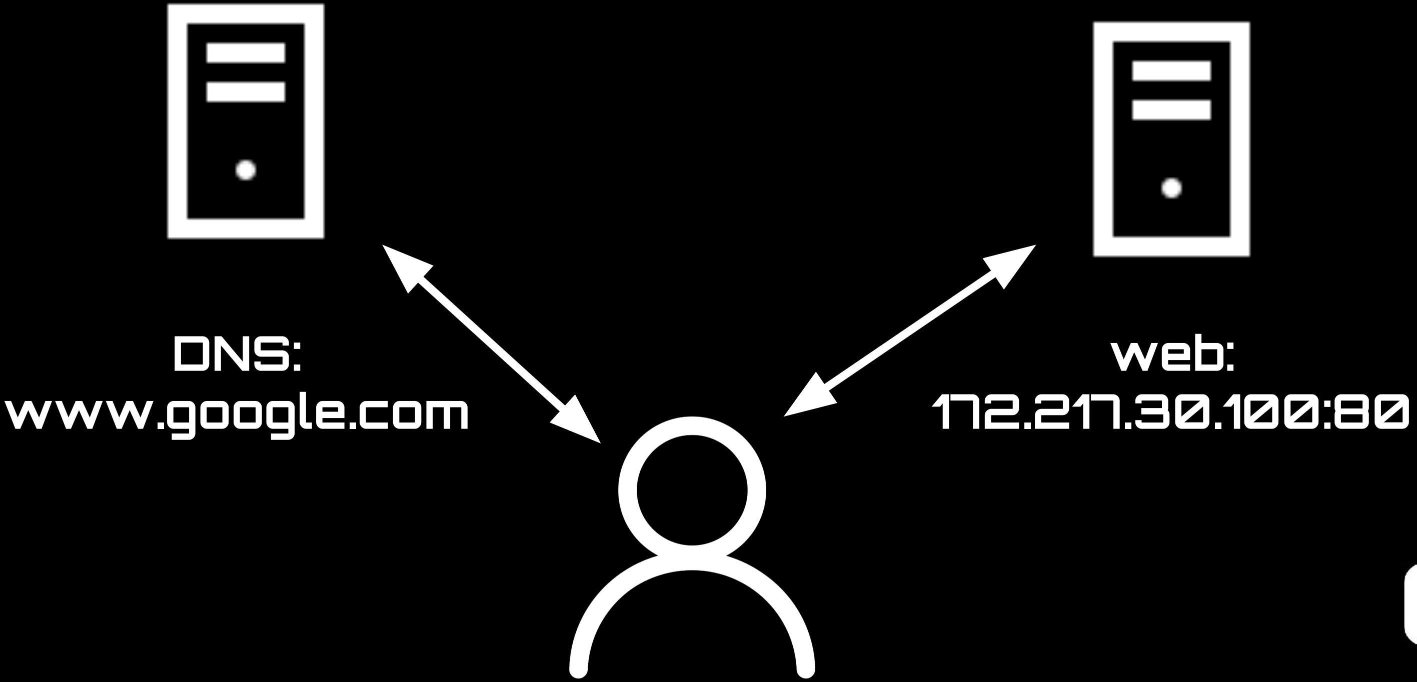
(Ninguém nem sabia o que isso queria dizer)

1. Copiar a página de login da USPnet
2. Começar um roteador no próprio computador
3. Esperar pessoas próximas a você se conectarem na USPnet
4. ???
5. Profit

Seria inútil se as pessoas utilizassem senhas diferentes em lugares diferentes

DNS Spoofing

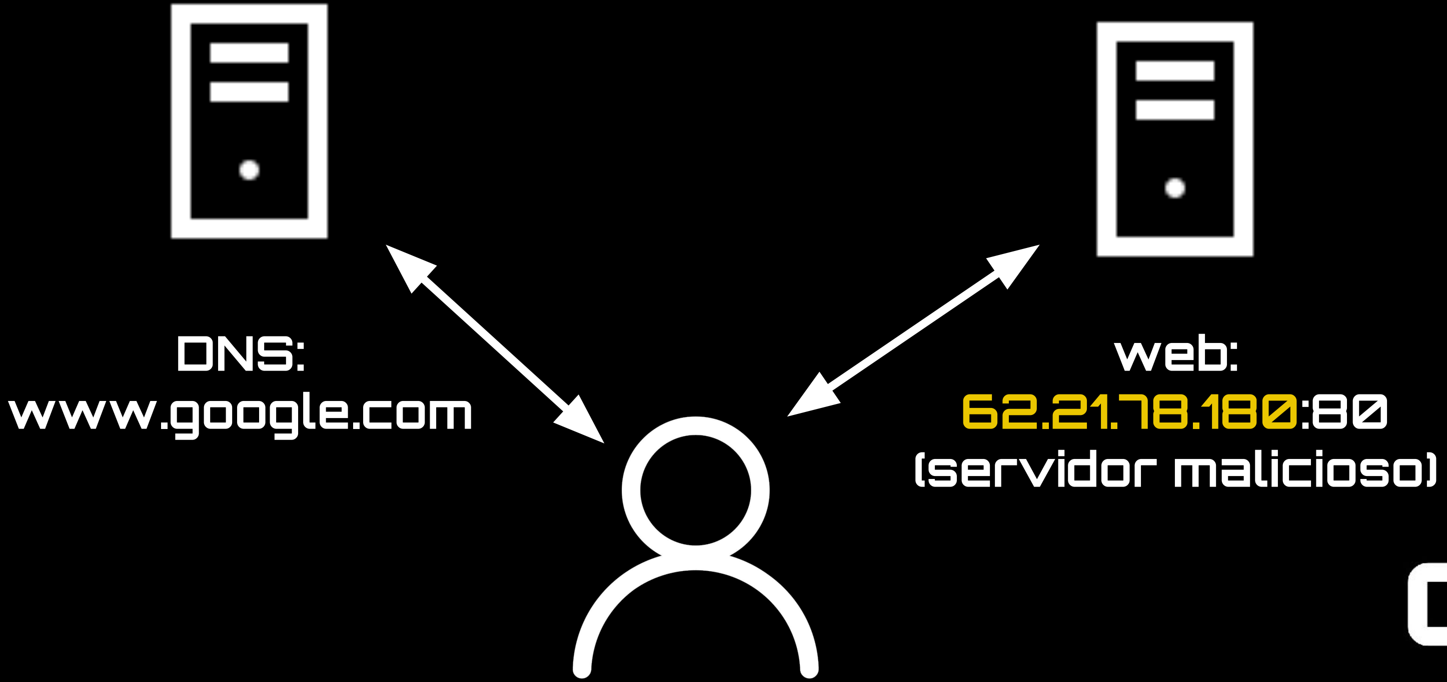
DNS Spoofing



DNS:
www.google.com

web:
172.217.30.100:80

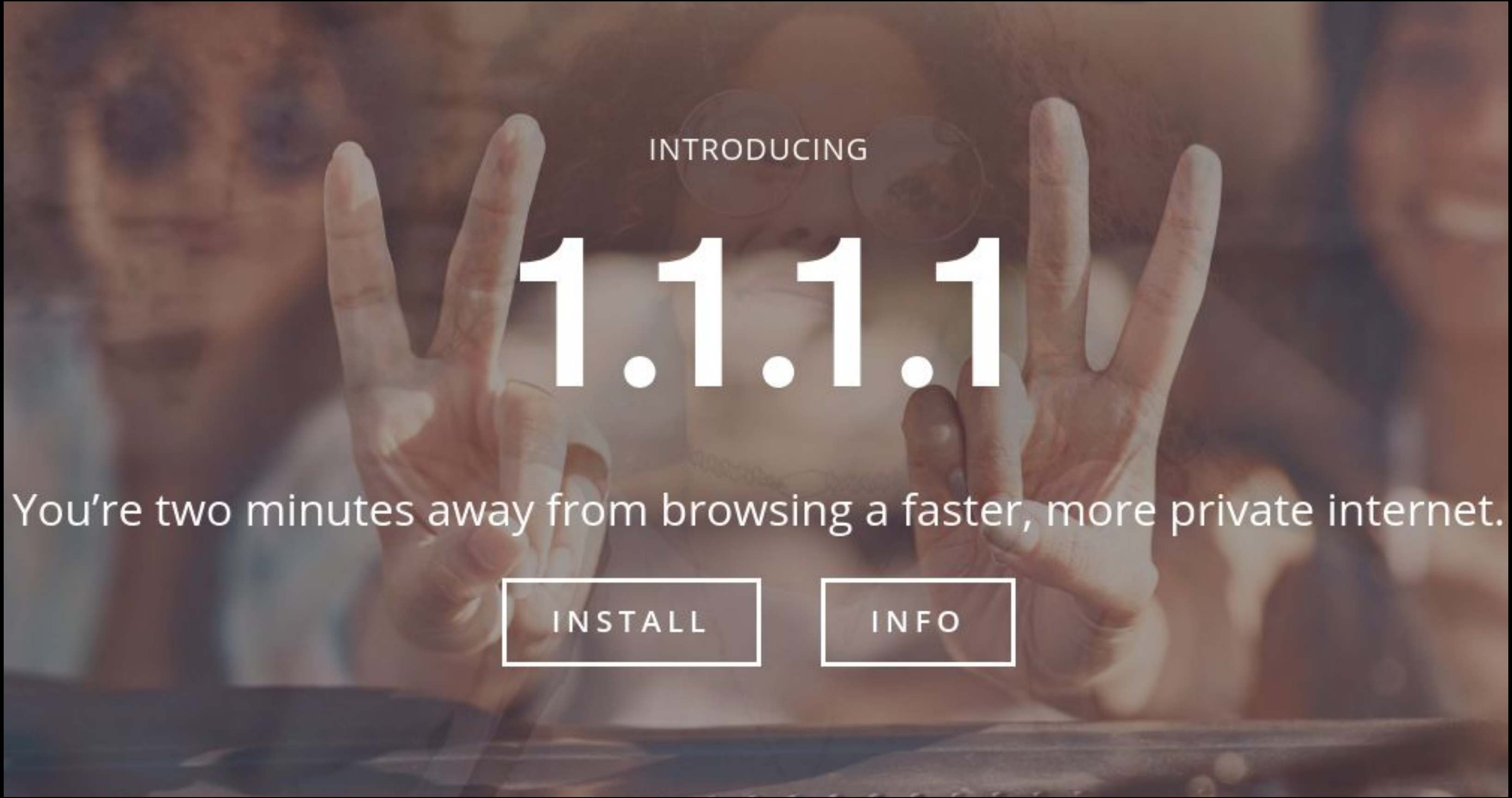
DNS Spoofing



DNS:
www.google.com

web:
62.21.78.180:80
(servidor malicioso)

Configuração automática de DNS pelo roteador



INTRODUCING

1.1.1.1

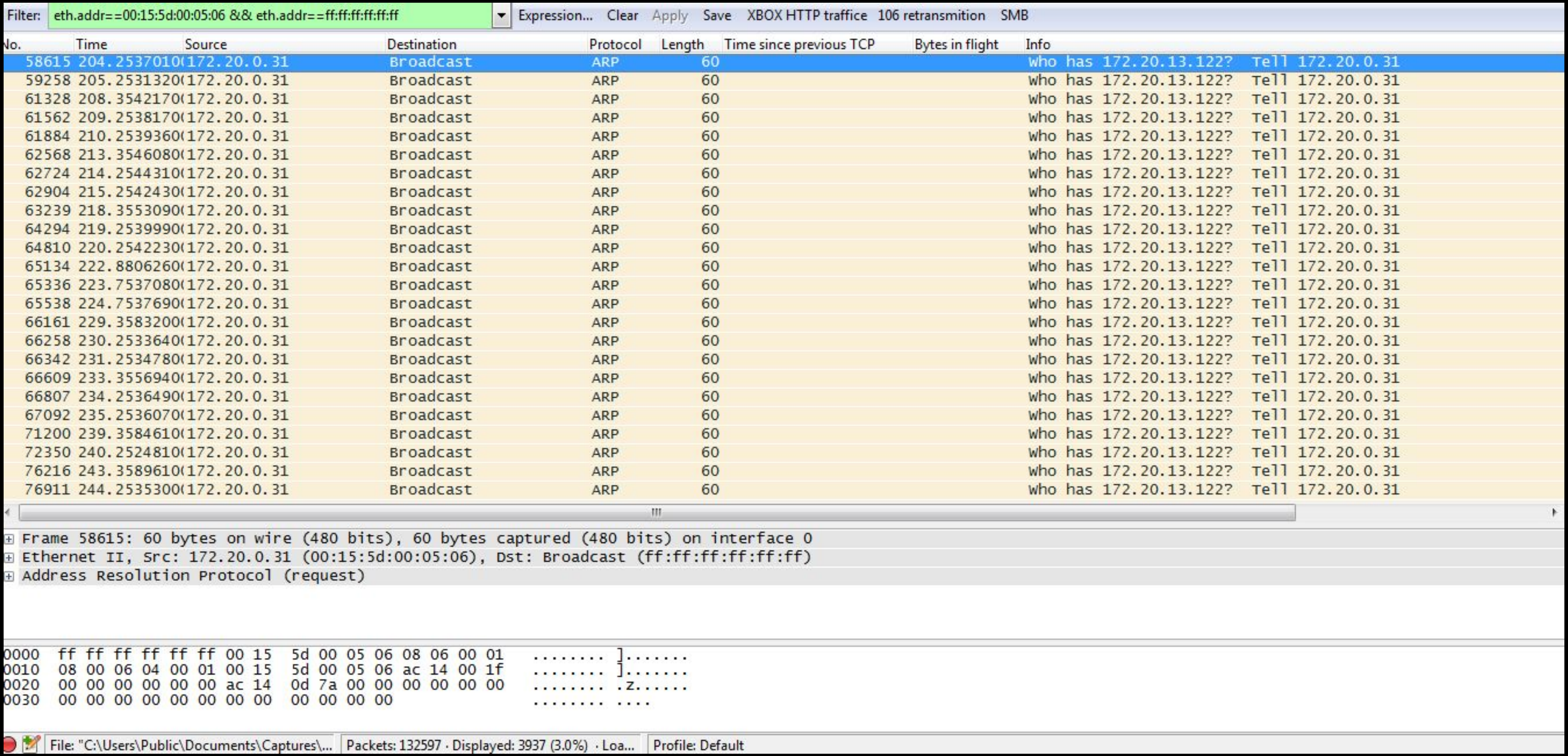
You’re two minutes away from browsing a faster, more private internet.

ARP Poisoning

(Address Resolution Protocol)

ARP

IP-1	MAC1
IP-2	MAC2
IP-3	MAC3
...	...



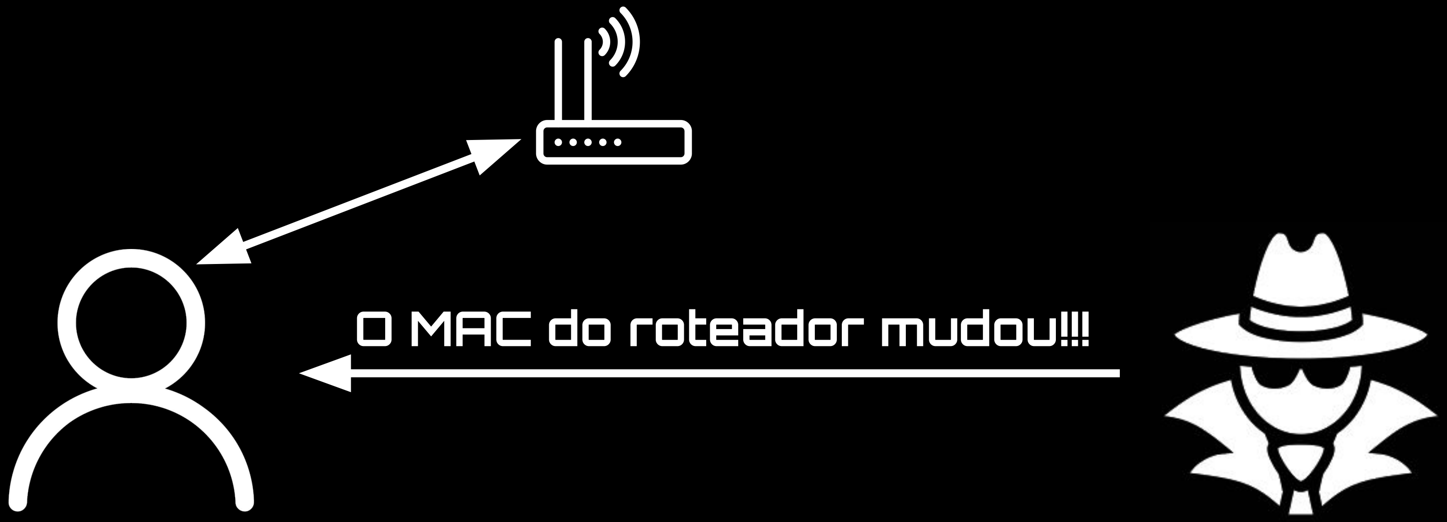
Filter: eth.addr==00:15:5d:00:05:06 && eth.addr==ff:ff:ff:ff:ff:ff

```
No.   Time        Source       Destination  Protocol  Length  Time since previous TCP  Bytes in flight  Info
58615 204.2537010(172.20.0.31  Broadcast    ARP           60                                           Who has 172.20.13.122?  Tell 172.20.0.31
59258 205.2531320(172.20.0.31  Broadcast    ARP           60                                           Who has 172.20.13.122?  Tell 172.20.0.31
61328 208.3542170(172.20.0.31  Broadcast    ARP           60                                           Who has 172.20.13.122?  Tell 172.20.0.31
61562 209.2538170(172.20.0.31  Broadcast    ARP           60                                           Who has 172.20.13.122?  Tell 172.20.0.31
61884 210.2539360(172.20.0.31  Broadcast    ARP           60                                           Who has 172.20.13.122?  Tell 172.20.0.31
62568 213.3546080(172.20.0.31  Broadcast    ARP           60                                           Who has 172.20.13.122?  Tell 172.20.0.31
62724 214.2544310(172.20.0.31  Broadcast    ARP           60                                           Who has 172.20.13.122?  Tell 172.20.0.31
62904 215.2542430(172.20.0.31  Broadcast    ARP           60                                           Who has 172.20.13.122?  Tell 172.20.0.31
63239 218.3553090(172.20.0.31  Broadcast    ARP           60                                           Who has 172.20.13.122?  Tell 172.20.0.31
64294 219.2539990(172.20.0.31  Broadcast    ARP           60                                           Who has 172.20.13.122?  Tell 172.20.0.31
64810 220.2542230(172.20.0.31  Broadcast    ARP           60                                           Who has 172.20.13.122?  Tell 172.20.0.31
65134 222.8806260(172.20.0.31  Broadcast    ARP           60                                           Who has 172.20.13.122?  Tell 172.20.0.31
65336 223.7537080(172.20.0.31  Broadcast    ARP           60                                           Who has 172.20.13.122?  Tell 172.20.0.31
65538 224.7537690(172.20.0.31  Broadcast    ARP           60                                           Who has 172.20.13.122?  Tell 172.20.0.31
66161 229.3583200(172.20.0.31  Broadcast    ARP           60                                           Who has 172.20.13.122?  Tell 172.20.0.31
66258 230.2533640(172.20.0.31  Broadcast    ARP           60                                           Who has 172.20.13.122?  Tell 172.20.0.31
66342 231.2534780(172.20.0.31  Broadcast    ARP           60                                           Who has 172.20.13.122?  Tell 172.20.0.31
66609 233.3556940(172.20.0.31  Broadcast    ARP           60                                           Who has 172.20.13.122?  Tell 172.20.0.31
66807 234.2536490(172.20.0.31  Broadcast    ARP           60                                           Who has 172.20.13.122?  Tell 172.20.0.31
67092 235.2536070(172.20.0.31  Broadcast    ARP           60                                           Who has 172.20.13.122?  Tell 172.20.0.31
71200 239.3584610(172.20.0.31  Broadcast    ARP           60                                           Who has 172.20.13.122?  Tell 172.20.0.31
72350 240.2524810(172.20.0.31  Broadcast    ARP           60                                           Who has 172.20.13.122?  Tell 172.20.0.31
76216 243.3589610(172.20.0.31  Broadcast    ARP           60                                           Who has 172.20.13.122?  Tell 172.20.0.31
76911 244.2535300(172.20.0.31  Broadcast    ARP           60                                           Who has 172.20.13.122?  Tell 172.20.0.31
```

```
⊞ Frame 58615: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
⊞ Ethernet II, Src: 172.20.0.31 (00:15:5d:00:05:06), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Address Resolution Protocol (request)
```

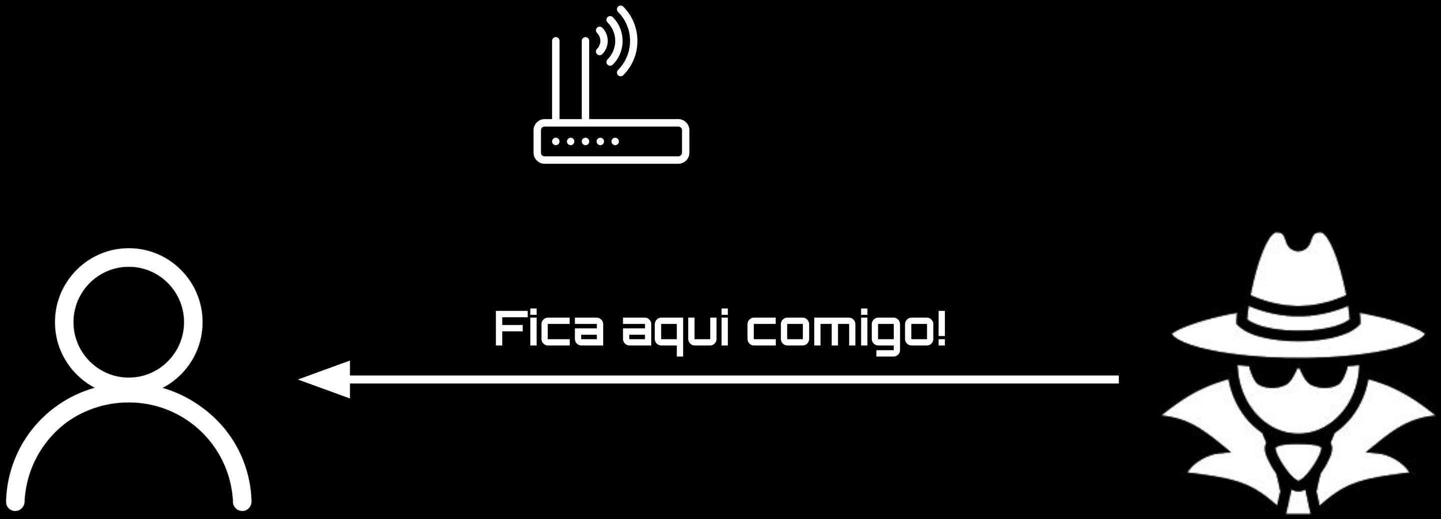
```
0000  ff ff ff ff ff ff 00 15  5d 00 05 06 08 06 00 01   ........ ].......
0010  08 00 06 04 00 01 00 15  5d 00 05 06 ac 14 00 1f   ........ ].......
0020  00 00 00 00 00 00 ac 14  0d 7a 00 00 00 00 00 00   ........ .z......
0030  00 00 00 00 00 00 00 00  00 00 00 00              ........ ....
```

File: "C:\Users\Public\Documents\Captures\... | Packets: 132597 · Displayed: 3937 (3.0%) · Loa... | Profile: Default

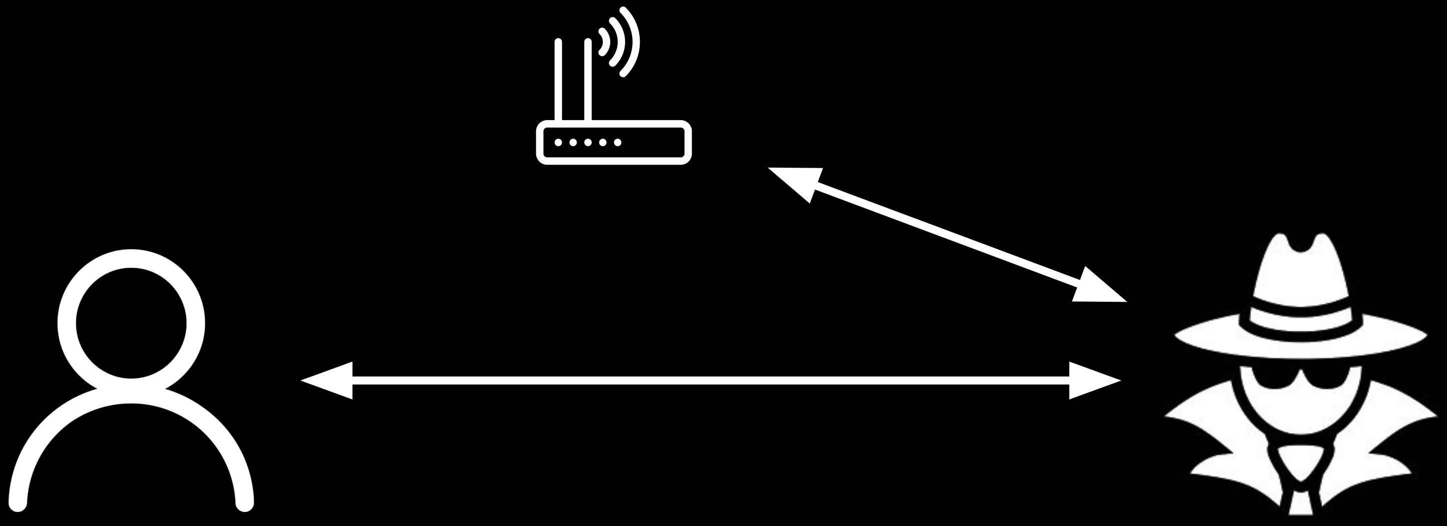


O MAC do roteador mudou!!!

Alguém sabe onde fica o roteador?



Fica aqui comigo!



Conclusão:

como se defender de tudo isso?

Coloque uma senha de administrador boa no seu roteador.

Instale um verificador de ARP poisoning, como o ArpON

Tenha dupla certeza na Wi-Fi que você está conectando!

Configure você mesmo o seu DNS.

Obrigado!