GTS 34

13 de Dezembro de 2019 - São Paulo / SP

~~Sequestros de DNS existem! Como eles são feitos?~~
~~Como identificá-los?~~

Sequestros de DNS em ISPs existem! Como eles são feitos? Como identificá-los?

Autor: Douglas Fernando Fischer – fischerdouglas@gmail.com

Douglas Fernando Fischer

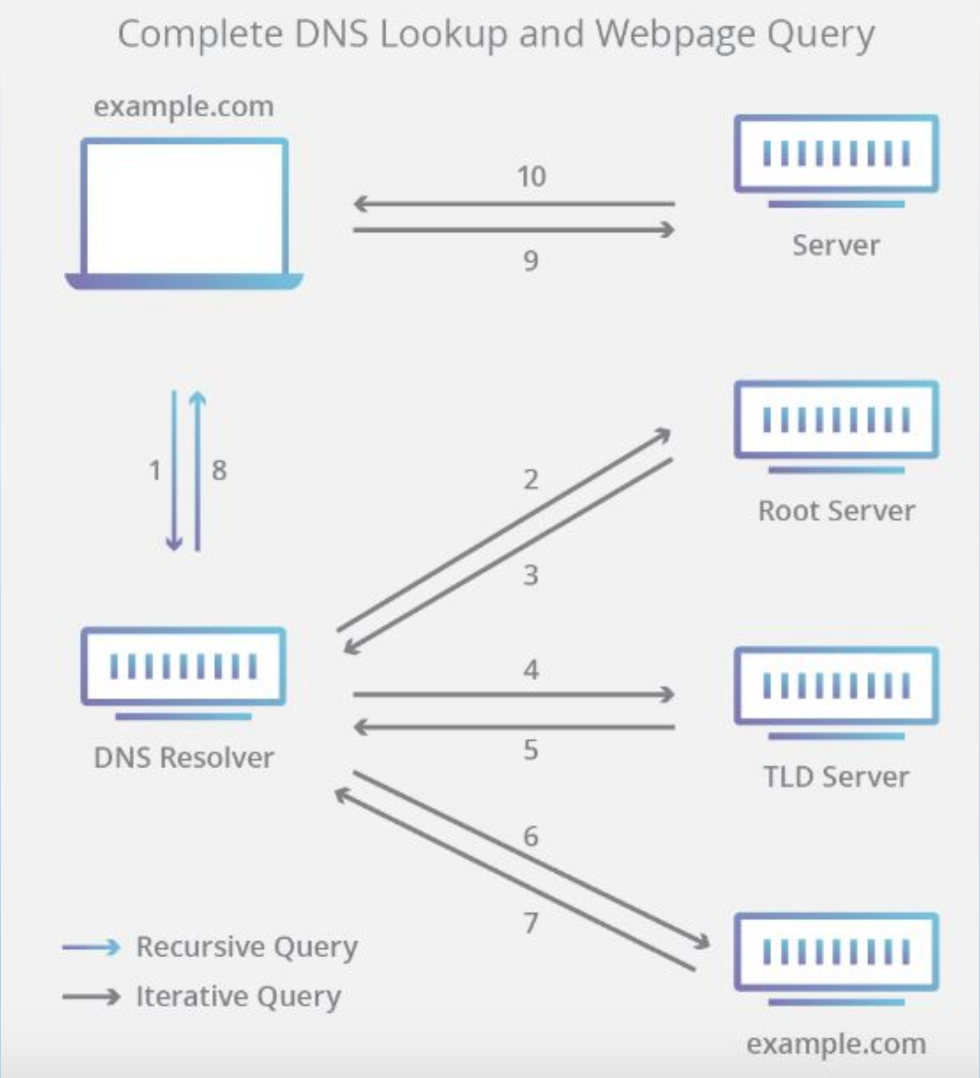
- Engenheiro de Controle e Automação
- Atua na área de redes de telecomunicações desde 1999
- Trabalhou como engenheiro de pré-vendas e implantação em integradores de tecnologia
- Consultor na área de redes e servidores no segmento corporativo e provedores de Internet
- BPF – http://brasilpeeringforum.org/
- Tretísta com fins produtivos nas horas vagas

EAÍ TELEFONIA INTELIGENTE

Intenções dessa apresentação?

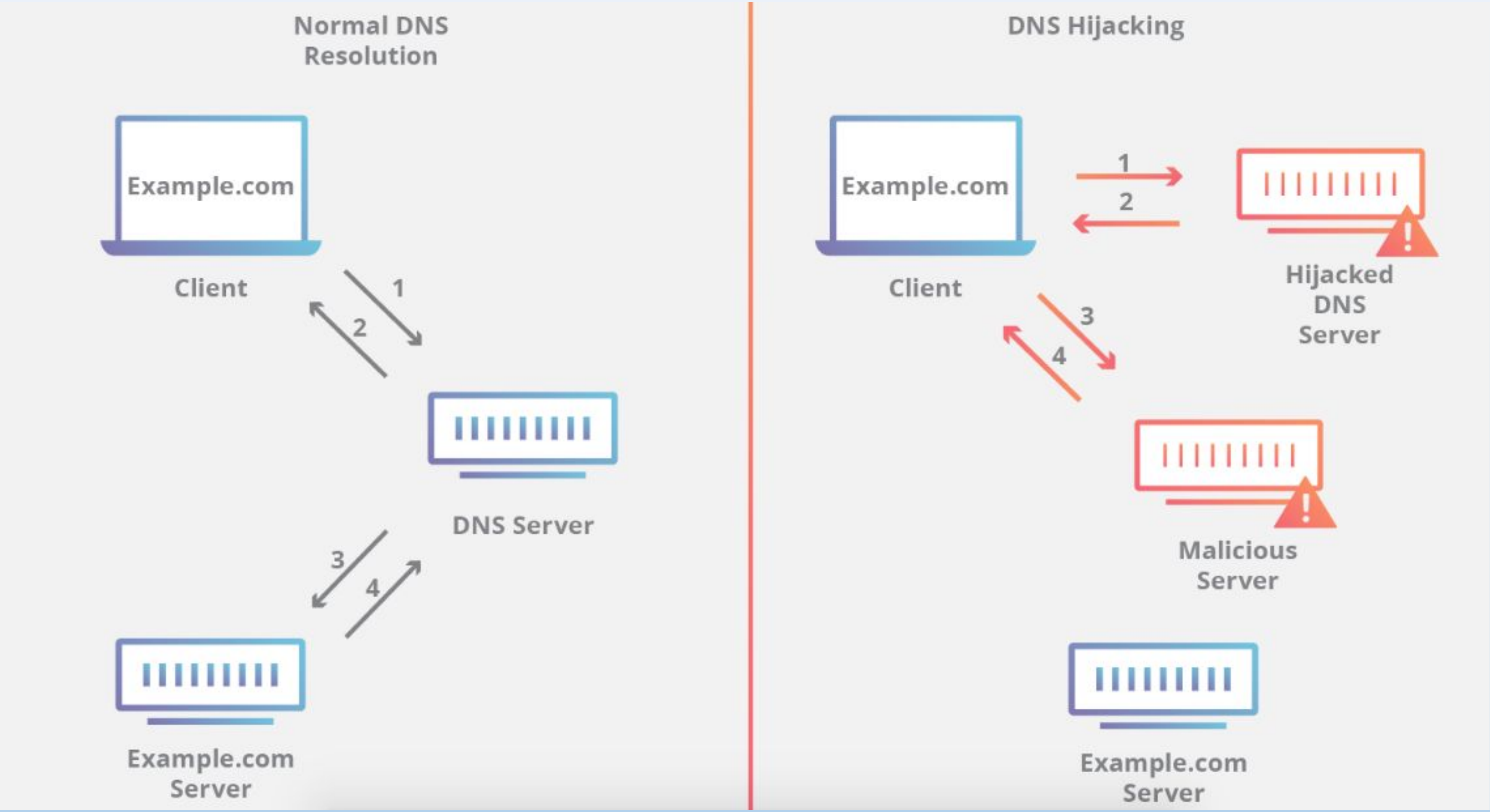
Fazer uma apresentação formal sobre o problema de sequestro de tráfego DNS no Brasil e no Mundo.

Como o DNS deveria funcionar?



https://www.cloudflare.com/learning/dns/what-is-dns/

O que é o sequestro de DNS?



https://www.cloudflare.com/learning/dns/dns-security/

Porque alguns ISPs sequestram tráfego DNS?

- DNSs Infectados - CPE Hackeadas

- Workaround em momentos de falha de serviços de DNS recursivo próprio ou de terceiros.

- Evitar que end-users enfrentem latência no DNS por escolhas "TOLAS"
  - "Meu sobrinho entende de Internet"
  - "Os caras do game disseram que trocar o DNS diminui a latência"

- Enganar os end-users "bobinhos" na hora de medir a latência
- Manipular respostas de DNS para "tentar influenciar" o consumo de tráfego de Caches CDN.

Pausa -> CPE(roteador no cliente) hackeado:

Dois tipos básicos sequestro de DNS em CPEs Hackeados

- Simples: Alteração do DNS Forwarder do CPE
- Avançados: DST-Nat no CPE

Como resolver? -> Opinião do Douglas

Solução errada

- Fazer DST-NAT de UDP/53 e TCP/53

Solução correta

- Liberar seus próprios DNS-Servers Recursivos
- Liberar apenas Well-Know Open Resolvers(Google, Quad9, Cloudflare)
- Liberar Root-Servers
- Bloquear todo o tráfego sainte para UDP/53 e TCP/53 restante

BCOP - Requisitos mínimos de segurança para aquisição de CPEs

https://www.lacnog.net/docs/lac-bcop-1

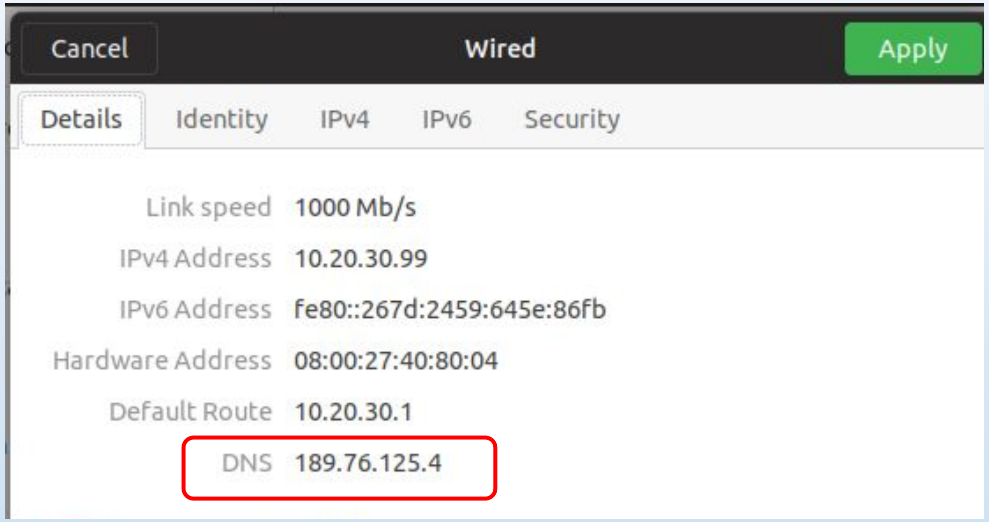
Tá Douglas, e como é esse tal de sequestro de DNS nos ISPs?

Existem basicamente dois modos

- Sequestro de prefixos dos DNS Open-Resolver na rede Interna do ISP
  - IPs desejados na loopback do NS-Resolver
    - Roteamento estático
    - Protocolos de roteamento(OSPF, BGP)

- NAT de Destino de tudo com destino a UDP/53 e TCP/53
  - Modo "Força-Bruta"
  - Sequestra "TUDO" que for DNS, inclusive autoritativos e Roots

Antes: Como ficam as coisas quando não há sequestro de tráfego DNS?



Link speed 1000 Mb/s

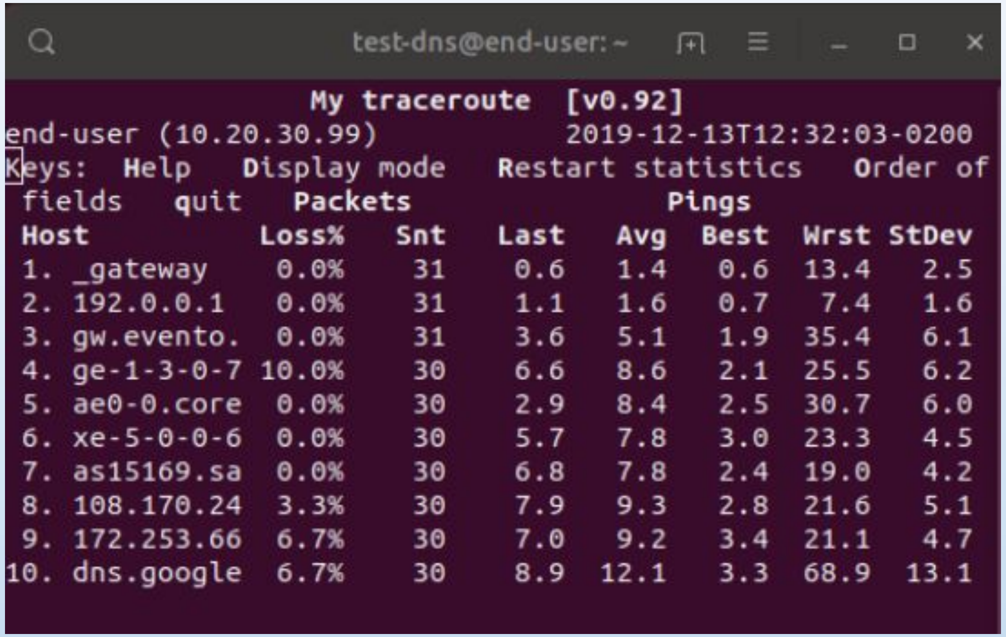
IPv4 Address 10.20.30.99

IPv6 Address fe80::267d:2459:645e:86fb

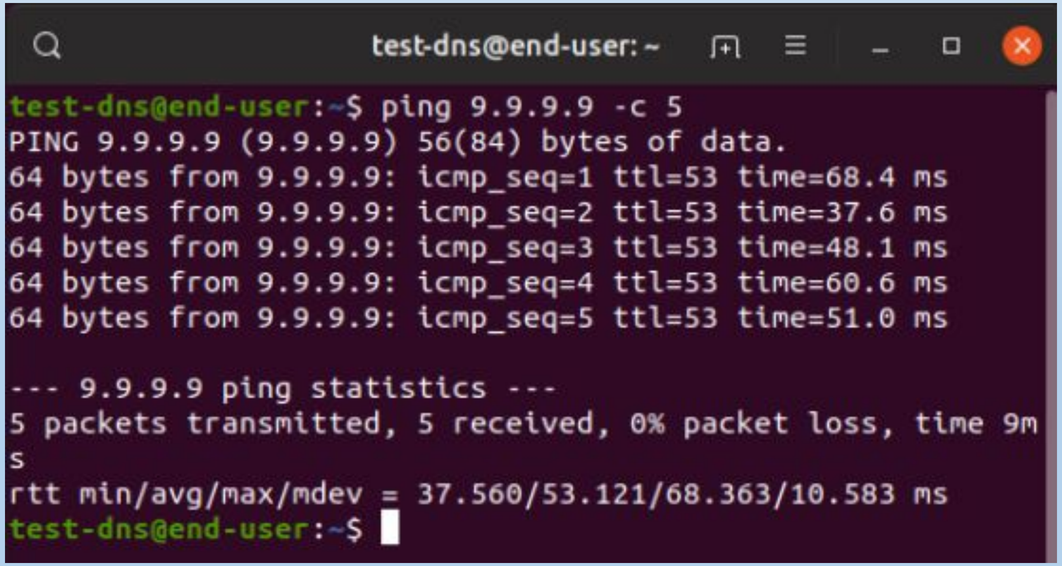
Hardware Address 08:00:27:40:80:04

Default Route 10.20.30.1

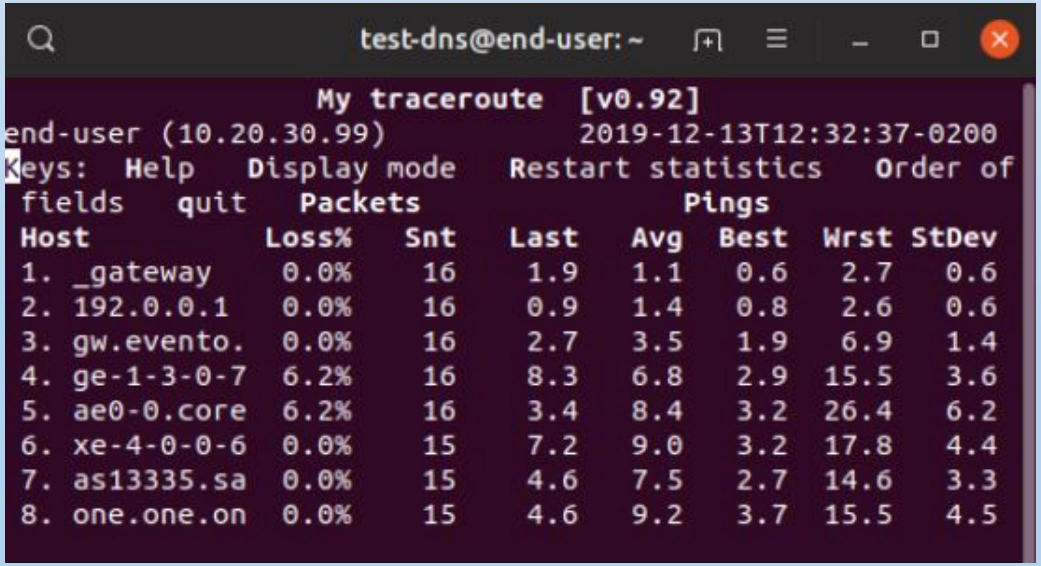
DNS 189.76.125.4



```
                         My traceroute  [v0.92]
end-user (10.20.30.99)             2019-12-13T12:32:03-0200
Keys:  Help   Display mode   Restart statistics   Order of
 fields   quit   Packets                Pings
 Host            Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. _gateway      0.0%    31    0.6   1.4   0.6  13.4   2.5
 2. 192.0.0.1     0.0%    31    1.1   1.6   0.7   7.4   1.6
 3. gw.evento.    0.0%    31    3.6   5.1   1.9  35.4   6.1
 4. ge-1-3-0-7   10.0%    30    6.6   8.6   2.1  25.5   6.2
 5. ae0-0.core    0.0%    30    2.9   8.4   2.5  30.7   6.0
 6. xe-5-0-0-6    0.0%    30    5.7   7.8   3.0  23.3   4.5
 7. as15169.sa    0.0%    30    6.8   7.8   2.4  19.0   4.2
 8. 108.170.24    3.3%    30    7.9   9.3   2.8  21.6   5.1
 9. 172.253.66    6.7%    30    7.0   9.2   3.4  21.1   4.7
10. dns.google    6.7%    30    8.9  12.1   3.3  68.9  13.1
```

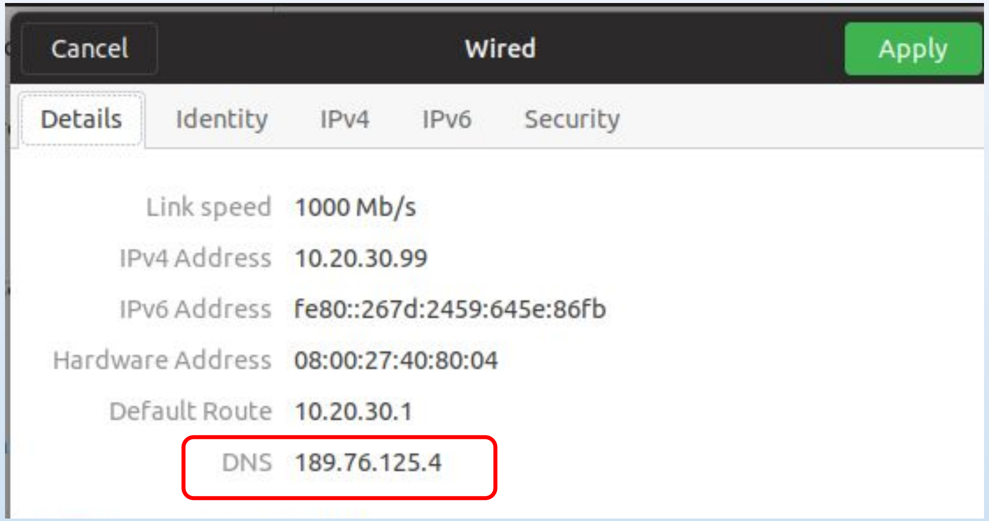


```
test-dns@end-user:~$ ping 9.9.9.9 -c 5
PING 9.9.9.9 (9.9.9.9) 56(84) bytes of data.
64 bytes from 9.9.9.9: icmp_seq=1 ttl=53 time=68.4 ms
64 bytes from 9.9.9.9: icmp_seq=2 ttl=53 time=37.6 ms
64 bytes from 9.9.9.9: icmp_seq=3 ttl=53 time=48.1 ms
64 bytes from 9.9.9.9: icmp_seq=4 ttl=53 time=60.6 ms
64 bytes from 9.9.9.9: icmp_seq=5 ttl=53 time=51.0 ms

--- 9.9.9.9 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 9m
s
rtt min/avg/max/mdev = 37.560/53.121/68.363/10.583 ms
test-dns@end-user:~$
```



```
                         My traceroute  [v0.92]
end-user (10.20.30.99)             2019-12-13T12:32:37-0200
Keys:  Help   Display mode   Restart statistics   Order of
 fields   quit   Packets                Pings
 Host            Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. _gateway      0.0%    16    1.9   1.1   0.6   2.7   0.6
 2. 192.0.0.1     0.0%    16    0.9   1.4   0.8   2.6   0.6
 3. gw.evento.    0.0%    16    2.7   3.5   1.9   6.9   1.4
 4. ge-1-3-0-7    6.2%    16    8.3   6.8   2.9  15.5   3.6
 5. ae0-0.core    6.2%    16    3.4   8.4   3.2  26.4   6.2
 6. xe-4-0-0-6    0.0%    15    7.2   9.0   3.2  17.8   4.4
 7. as13335.sa    0.0%    15    4.6   7.5   2.7  14.6   3.3
 8. one.one.on    0.0%    15    4.6   9.2   3.7  15.5   4.5
```

Antes: Como ficam as coisas quando não há sequestro de tráfego DNS?



Link speed 1000 Mb/s

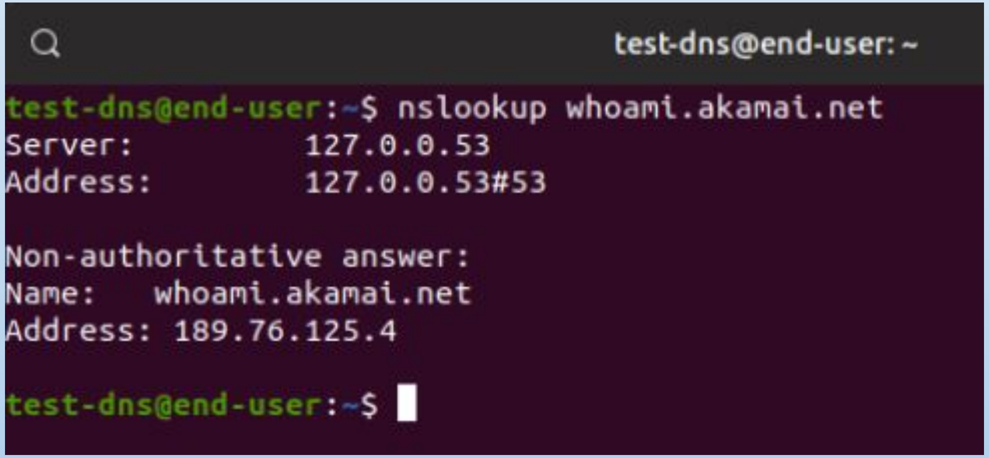
IPv4 Address 10.20.30.99

IPv6 Address fe80::267d:2459:645e:86fb

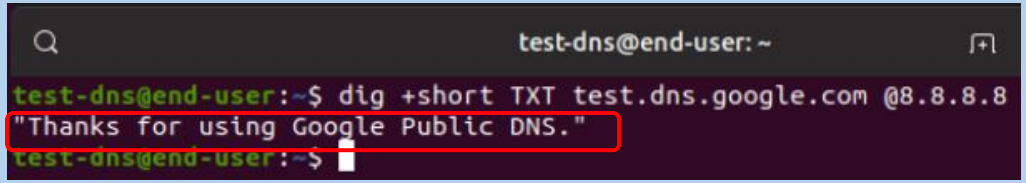
Hardware Address 08:00:27:40:80:04

Default Route 10.20.30.1

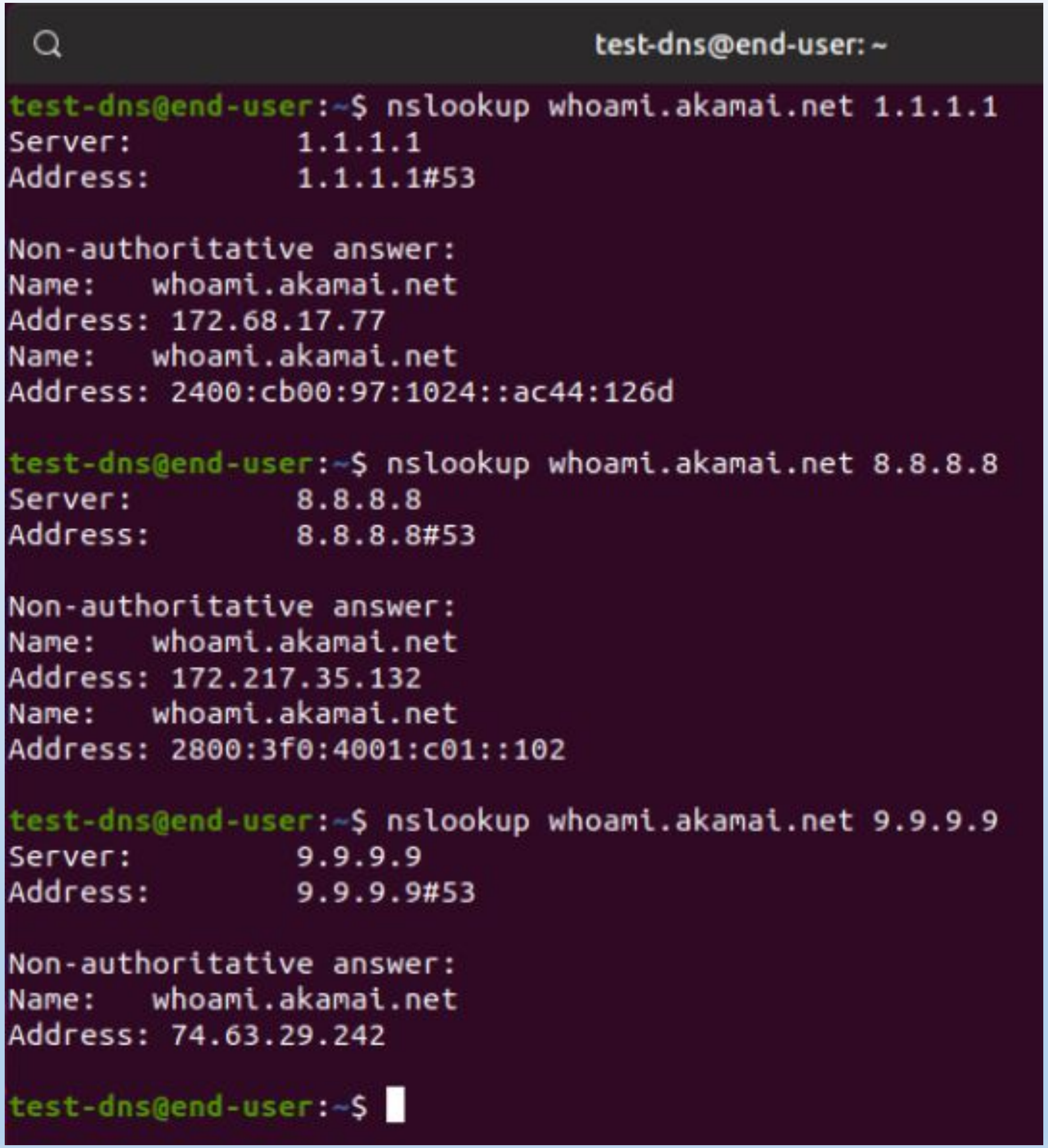
DNS 189.76.125.4



```
test-dns@end-user:~$ nslookup whoami.akamai.net
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   whoami.akamai.net
Address: 189.76.125.4

test-dns@end-user:~$
```

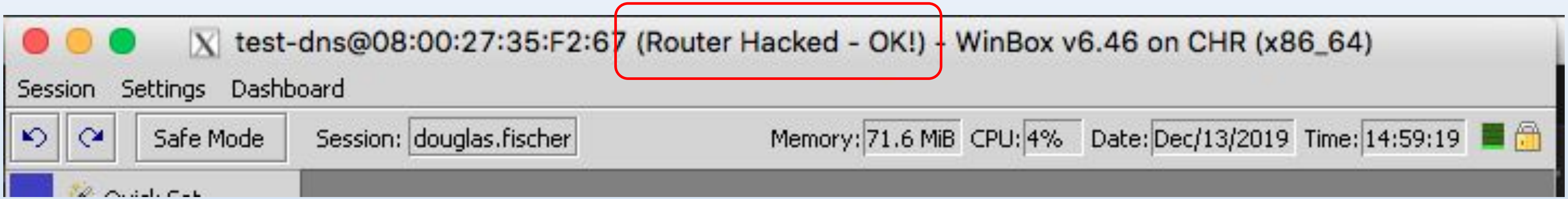


```
test-dns@end-user:~$ dig +short TXT test.dns.google.com @8.8.8.8
"Thanks for using Google Public DNS."
test-dns@end-user:~$
```



```
test-dns@end-user:~$ nslookup whoami.akamai.net 1.1.1.1
Server:         1.1.1.1
Address:        1.1.1.1#53

Non-authoritative answer:
Name:   whoami.akamai.net
Address: 172.68.17.77
Name:   whoami.akamai.net
Address: 2400:cb00:97:1024::ac44:126d

test-dns@end-user:~$ nslookup whoami.akamai.net 8.8.8.8
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   whoami.akamai.net
Address: 172.217.35.132
Name:   whoami.akamai.net
Address: 2800:3f0:4001:c01::102

test-dns@end-user:~$ nslookup whoami.akamai.net 9.9.9.9
Server:         9.9.9.9
Address:        9.9.9.9#53

Non-authoritative answer:
Name:   whoami.akamai.net
Address: 74.63.29.242

test-dns@end-user:~$
```

Agradecimentos...



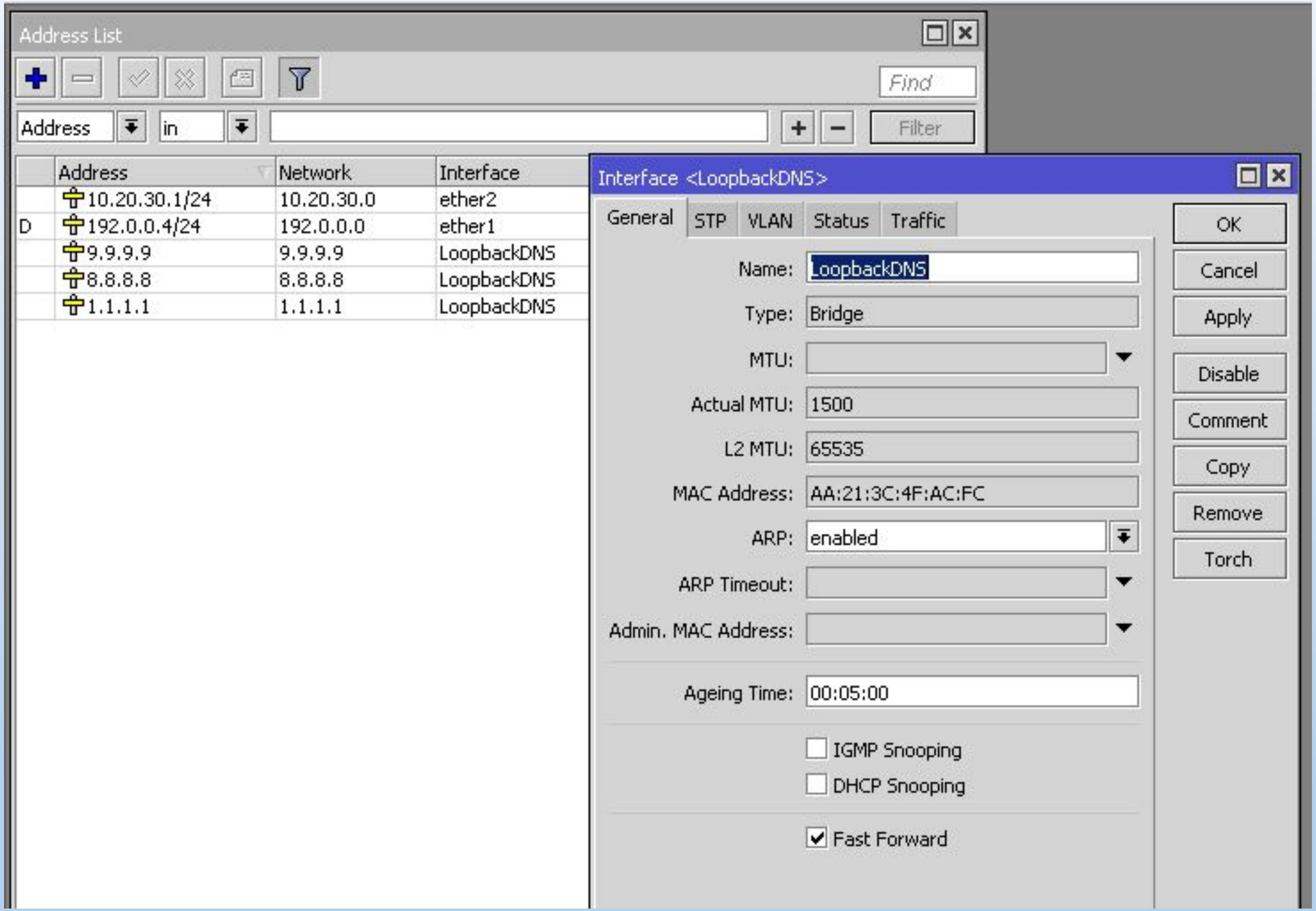
test-dns@08:00:27:35:F2:67 (Router Hacked - OK!) - WinBox v6.46 on CHR (x86_64)

Session: douglas.fischer

Memory: 71.6 MiB CPU: 4% Date: Dec/13/2019 Time: 14:59:19

Não seja um trouxa como eu…
Não deixe seu equipamento
com usuário e senha padrão.

Sequestrando DNS - Loopback



	Address	Network	Interface
	10.20.30.1/24	10.20.30.0	ether2
D	192.0.0.4/24	192.0.0.0	ether1
	9.9.9.9	9.9.9.9	LoopbackDNS
	8.8.8.8	8.8.8.8	LoopbackDNS
	1.1.1.1	1.1.1.1	LoopbackDNS

Name: LoopbackDNS

Type: Bridge

MTU:

Actual MTU: 1500

L2 MTU: 65535

MAC Address: AA:21:3C:4F:AC:FC

ARP: enabled

ARP Timeout:

Admin. MAC Address:

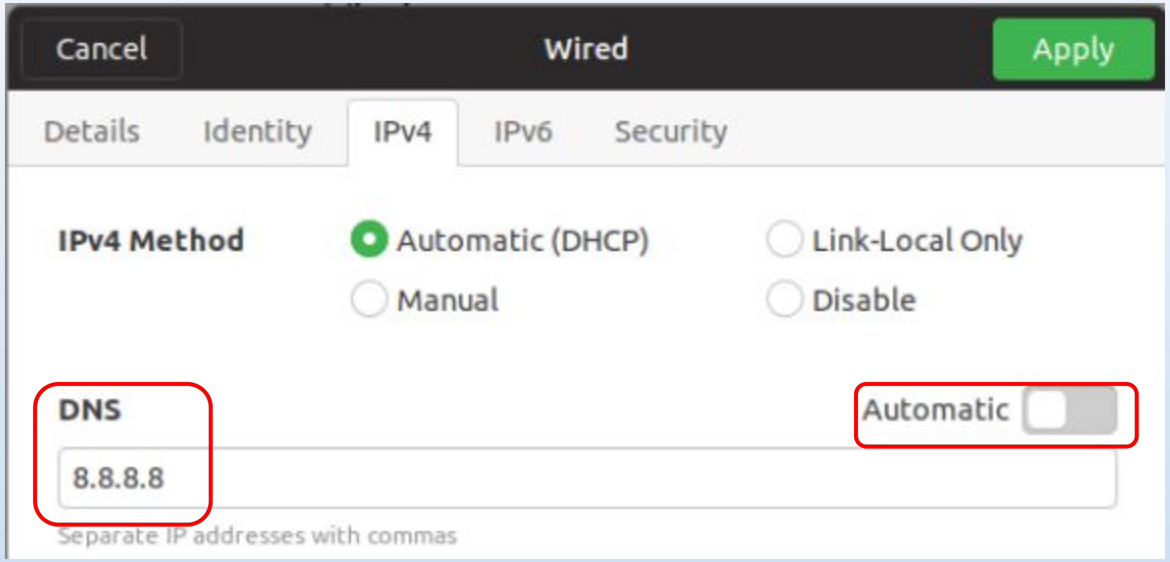
Ageing Time: 00:05:00

☐ IGMP Snooping

☐ DHCP Snooping

☑ Fast Forward

Sequestrando DNS - Loopback

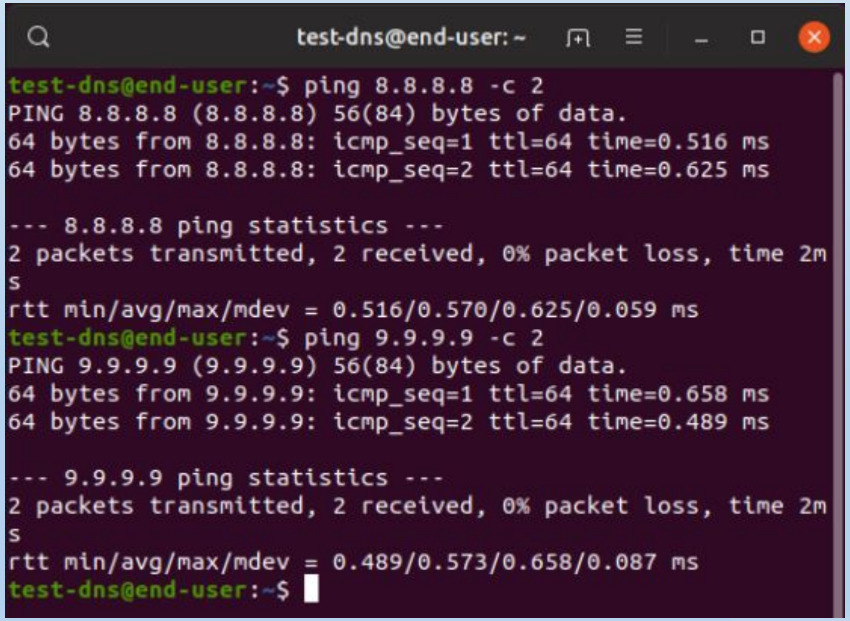


IPv4 Method: ● Automatic (DHCP) ○ Link-Local Only ○ Manual ○ Disable

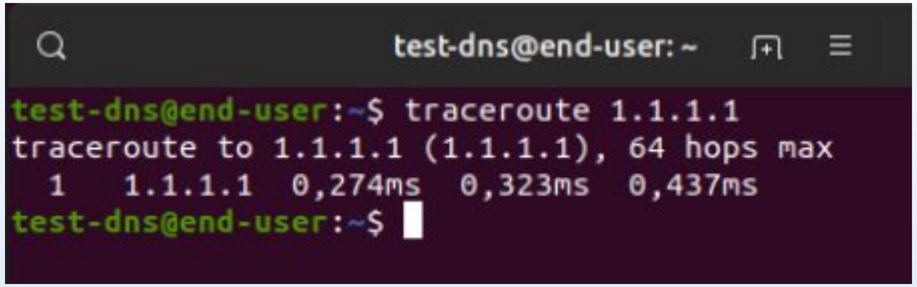
DNS — Automatic: off

8.8.8.8

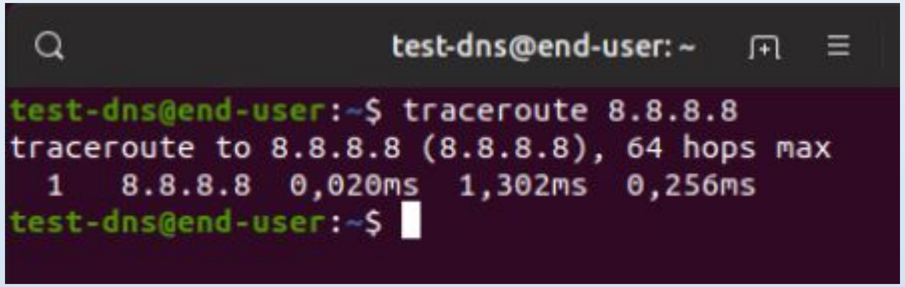
Separate IP addresses with commas



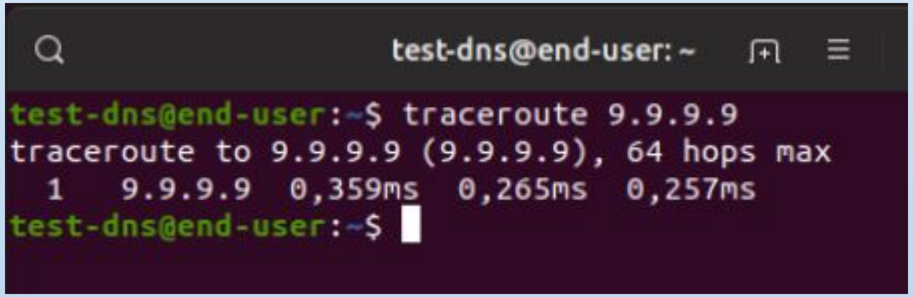
```
test-dns@end-user:~$ ping 8.8.8.8 -c 2
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=64 time=0.516 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=64 time=0.625 ms

--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2m
s
rtt min/avg/max/mdev = 0.516/0.570/0.625/0.059 ms
test-dns@end-user:~$ ping 9.9.9.9 -c 2
PING 9.9.9.9 (9.9.9.9) 56(84) bytes of data.
64 bytes from 9.9.9.9: icmp_seq=1 ttl=64 time=0.658 ms
64 bytes from 9.9.9.9: icmp_seq=2 ttl=64 time=0.489 ms

--- 9.9.9.9 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2m
s
rtt min/avg/max/mdev = 0.489/0.573/0.658/0.087 ms
test-dns@end-user:~$
```



```
test-dns@end-user:~$ traceroute 1.1.1.1
traceroute to 1.1.1.1 (1.1.1.1), 64 hops max
  1   1.1.1.1  0,274ms  0,323ms  0,437ms
test-dns@end-user:~$
```



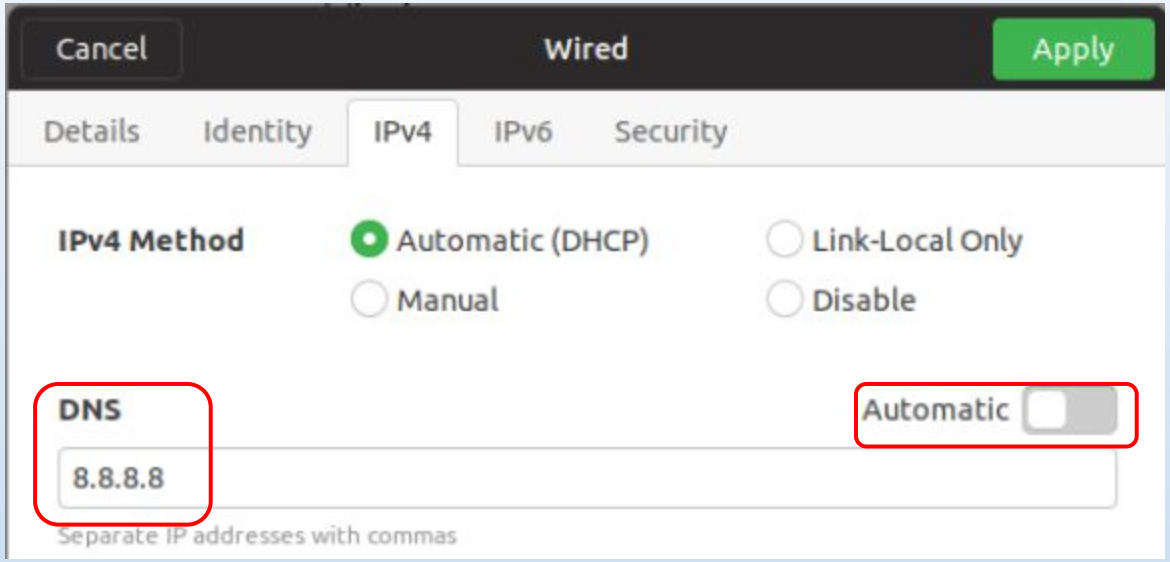
```
test-dns@end-user:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 64 hops max
  1   8.8.8.8  0,020ms  1,302ms  0,256ms
test-dns@end-user:~$
```



```
test-dns@end-user:~$ traceroute 9.9.9.9
traceroute to 9.9.9.9 (9.9.9.9), 64 hops max
  1   9.9.9.9  0,359ms  0,265ms  0,257ms
test-dns@end-user:~$
```

A latência do nosso provedor é a melhor de todos...

Sequestrando DNS - Loopback

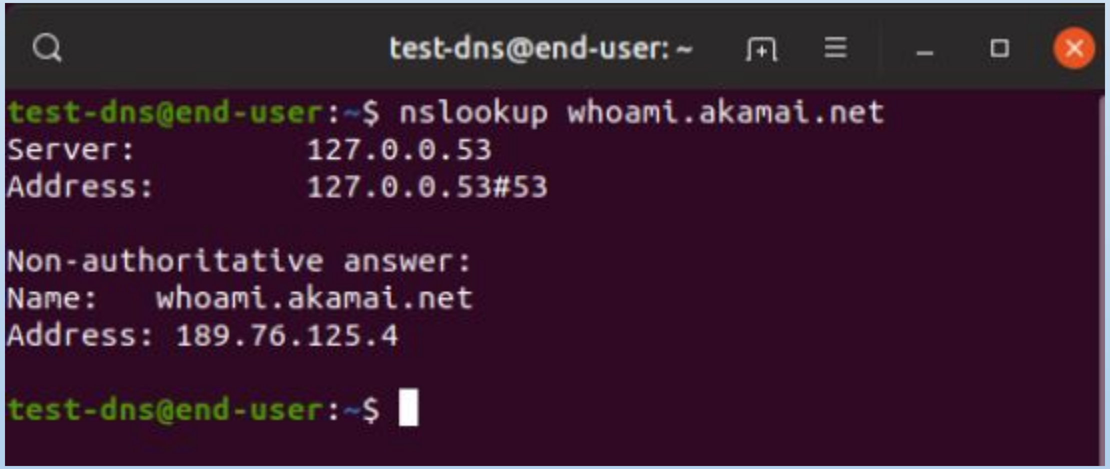


IPv4 Method ● Automatic (DHCP) ○ Link-Local Only ○ Manual ○ Disable

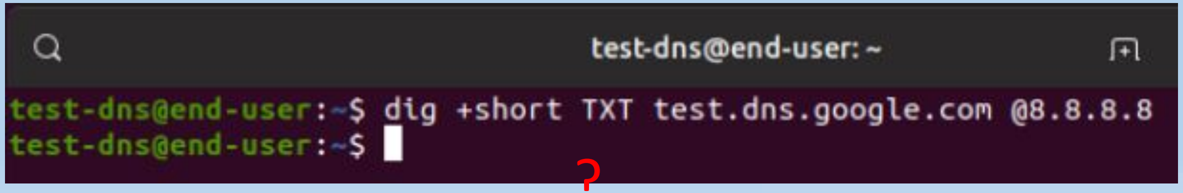
DNS Automatic ○

8.8.8.8

Separate IP addresses with commas

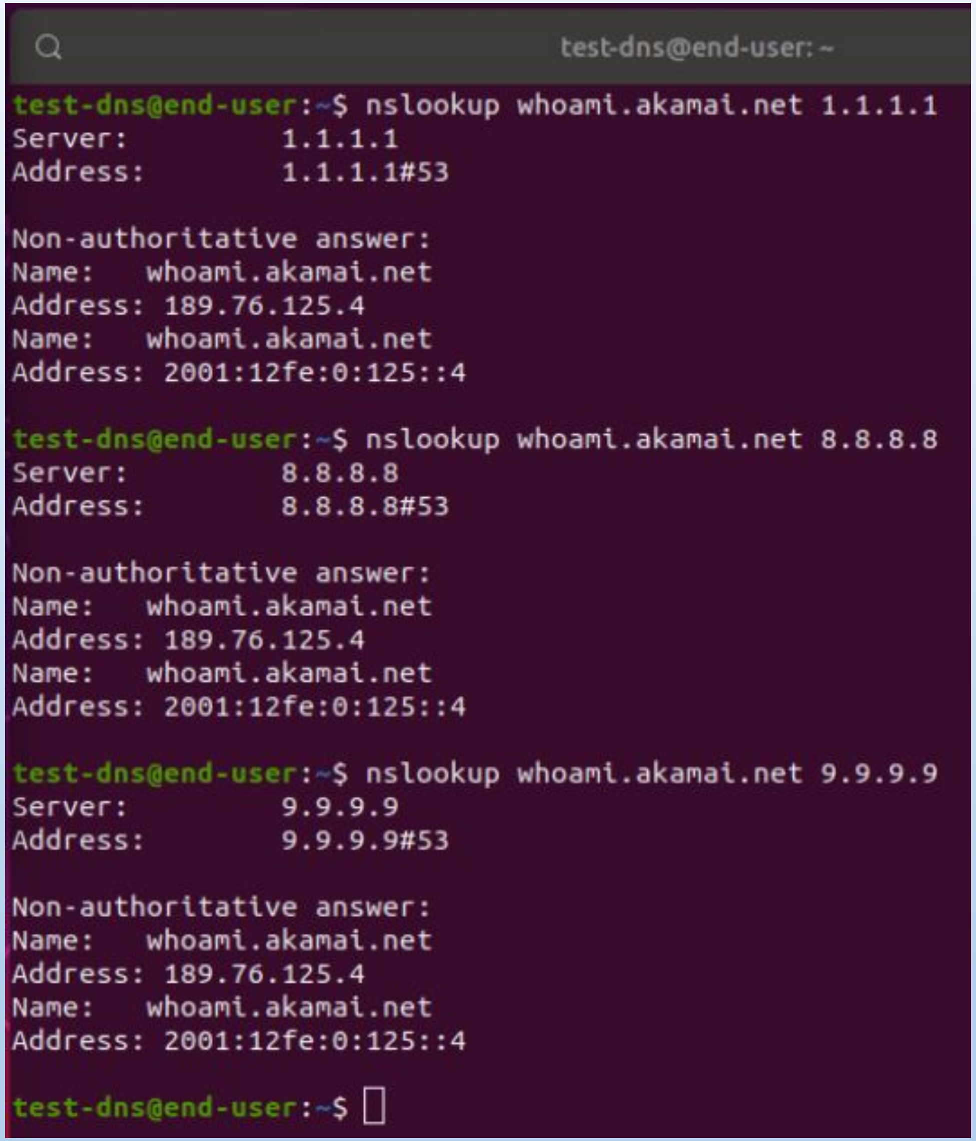


```
test-dns@end-user:~$ nslookup whoami.akamai.net
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   whoami.akamai.net
Address: 189.76.125.4

test-dns@end-user:~$ 
```



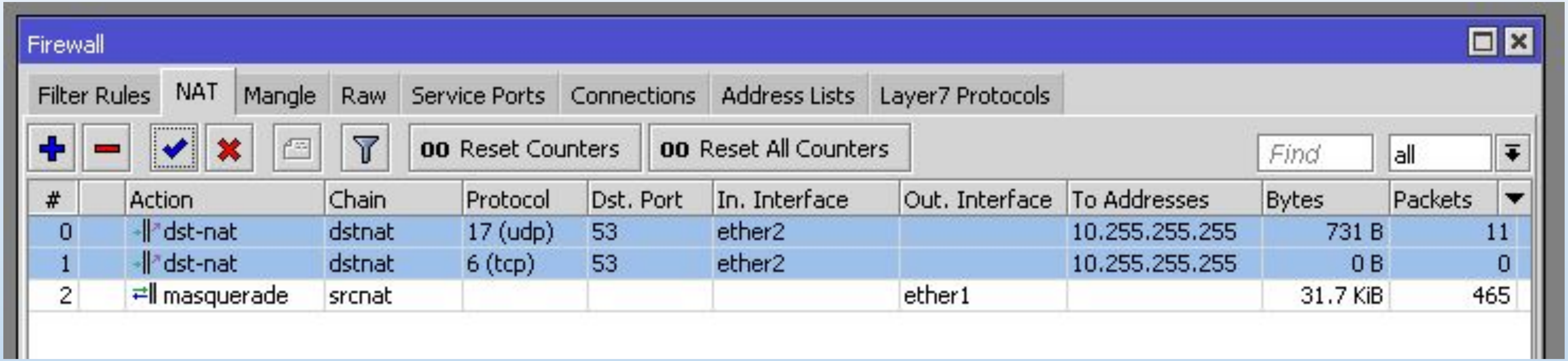
```
test-dns@end-user:~$ dig +short TXT test.dns.google.com @8.8.8.8
test-dns@end-user:~$ 
```

?



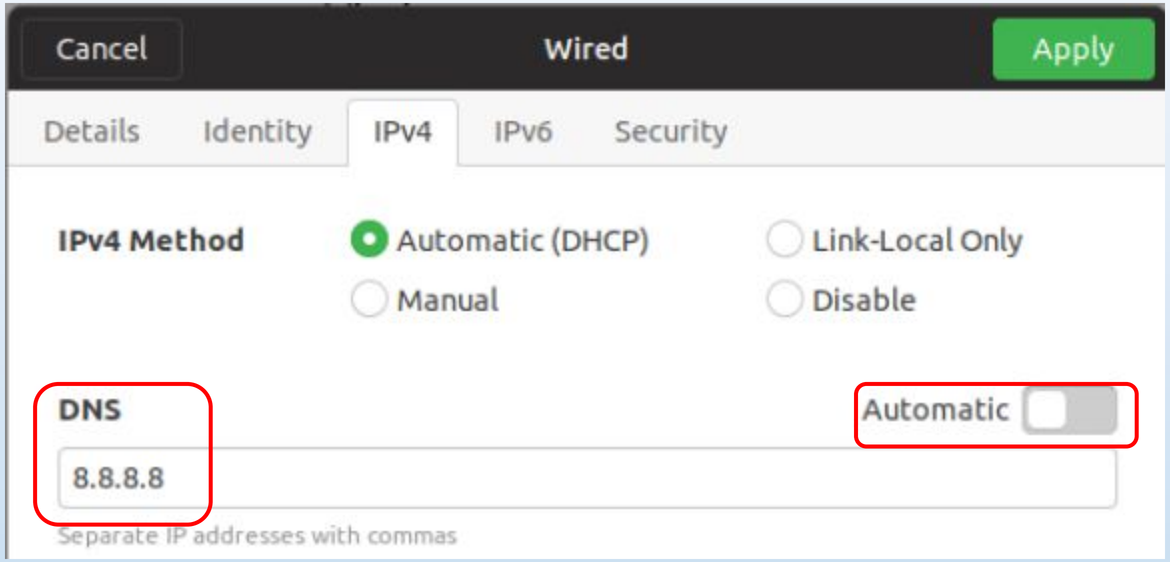
```
test-dns@end-user:~$ nslookup whoami.akamai.net 1.1.1.1
Server:         1.1.1.1
Address:        1.1.1.1#53

Non-authoritative answer:
Name:   whoami.akamai.net
Address: 189.76.125.4
Name:   whoami.akamai.net
Address: 2001:12fe:0:125::4

test-dns@end-user:~$ nslookup whoami.akamai.net 8.8.8.8
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   whoami.akamai.net
Address: 189.76.125.4
Name:   whoami.akamai.net
Address: 2001:12fe:0:125::4

test-dns@end-user:~$ nslookup whoami.akamai.net 9.9.9.9
Server:         9.9.9.9
Address:        9.9.9.9#53

Non-authoritative answer:
Name:   whoami.akamai.net
Address: 189.76.125.4
Name:   whoami.akamai.net
Address: 2001:12fe:0:125::4

test-dns@end-user:~$ 
```

Sequestrando DNS - DST-NAT



#		Action	Chain	Protocol	Dst. Port	In. Interface	Out. Interface	To Addresses	Bytes	Packets
0		dst-nat	dstnat	17 (udp)	53	ether2		10.255.255.255	731 B	11
1		dst-nat	dstnat	6 (tcp)	53	ether2		10.255.255.255	0 B	0
2		masquerade	srcnat				ether1		31.7 KiB	465

Sequestrando DNS - DST-NAT - ICMP continua Igual

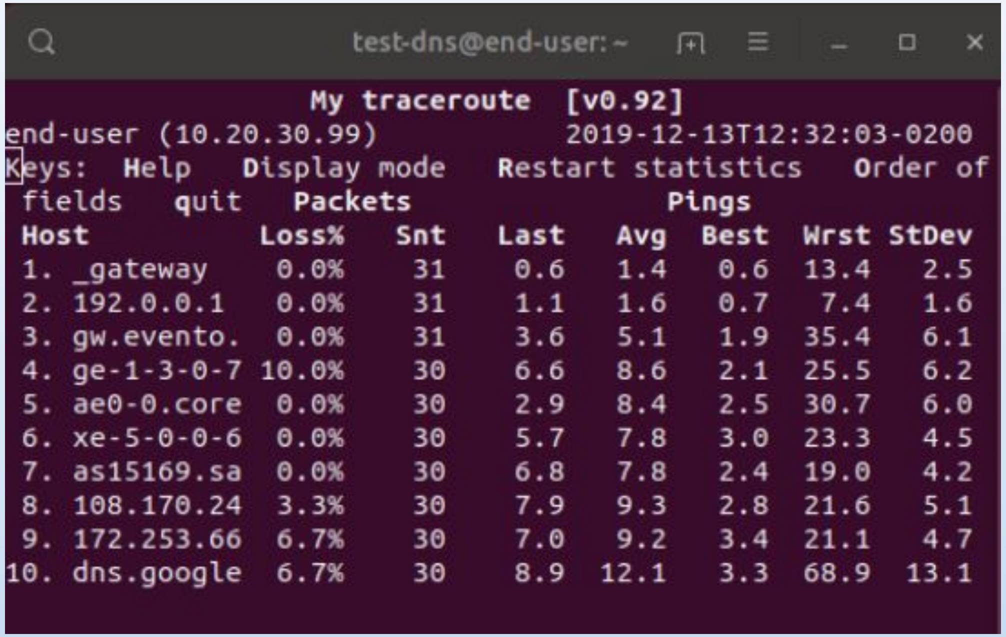


IPv4 Method ● Automatic (DHCP) ○ Link-Local Only ○ Manual ○ Disable

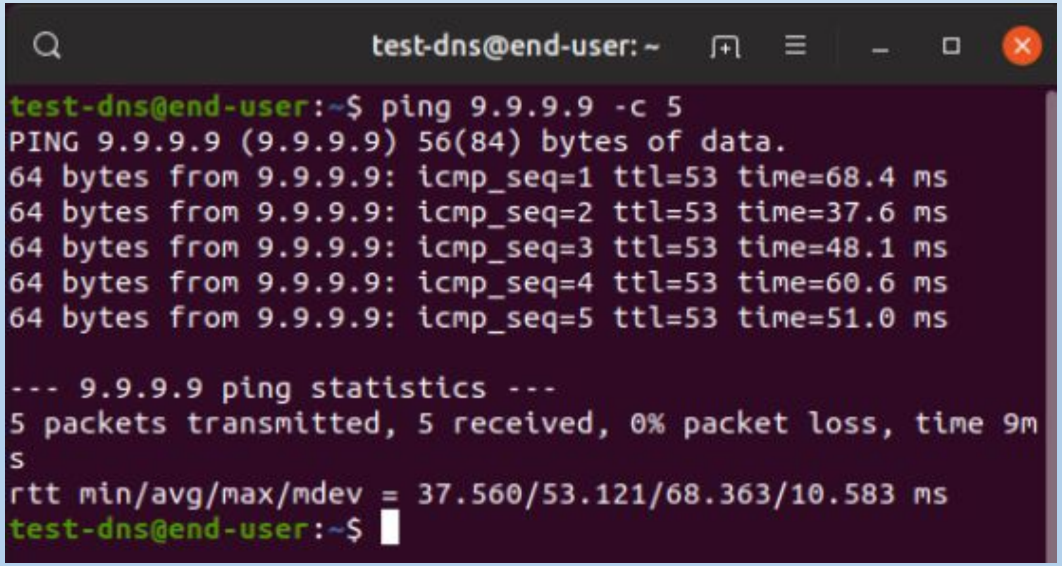
DNS — Automatic: off

8.8.8.8

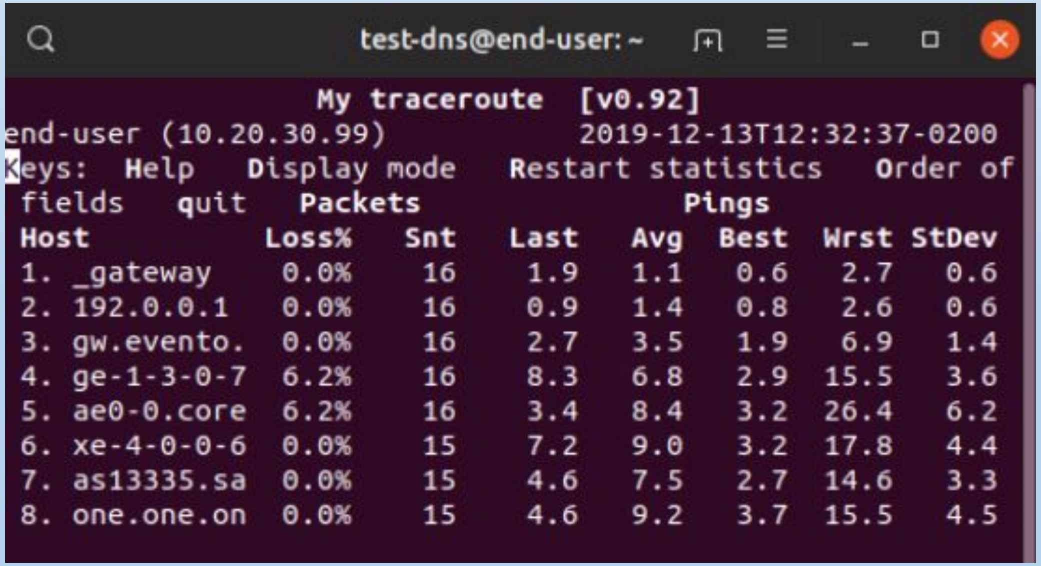
Separate IP addresses with commas



```
                       My traceroute  [v0.92]
end-user (10.20.30.99)                2019-12-13T12:32:03-0200
Keys:  Help   Display mode   Restart statistics   Order of
 fields   quit   Packets                   Pings
 Host              Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. _gateway        0.0%    31    0.6   1.4   0.6  13.4   2.5
 2. 192.0.0.1       0.0%    31    1.1   1.6   0.7   7.4   1.6
 3. gw.evento.      0.0%    31    3.6   5.1   1.9  35.4   6.1
 4. ge-1-3-0-7 10.0%    30    6.6   8.6   2.1  25.5   6.2
 5. ae0-0.core      0.0%    30    2.9   8.4   2.5  30.7   6.0
 6. xe-5-0-0-6      0.0%    30    5.7   7.8   3.0  23.3   4.5
 7. as15169.sa      0.0%    30    6.8   7.8   2.4  19.0   4.2
 8. 108.170.24      3.3%    30    7.9   9.3   2.8  21.6   5.1
 9. 172.253.66      6.7%    30    7.0   9.2   3.4  21.1   4.7
10. dns.google      6.7%    30    8.9  12.1   3.3  68.9  13.1
```

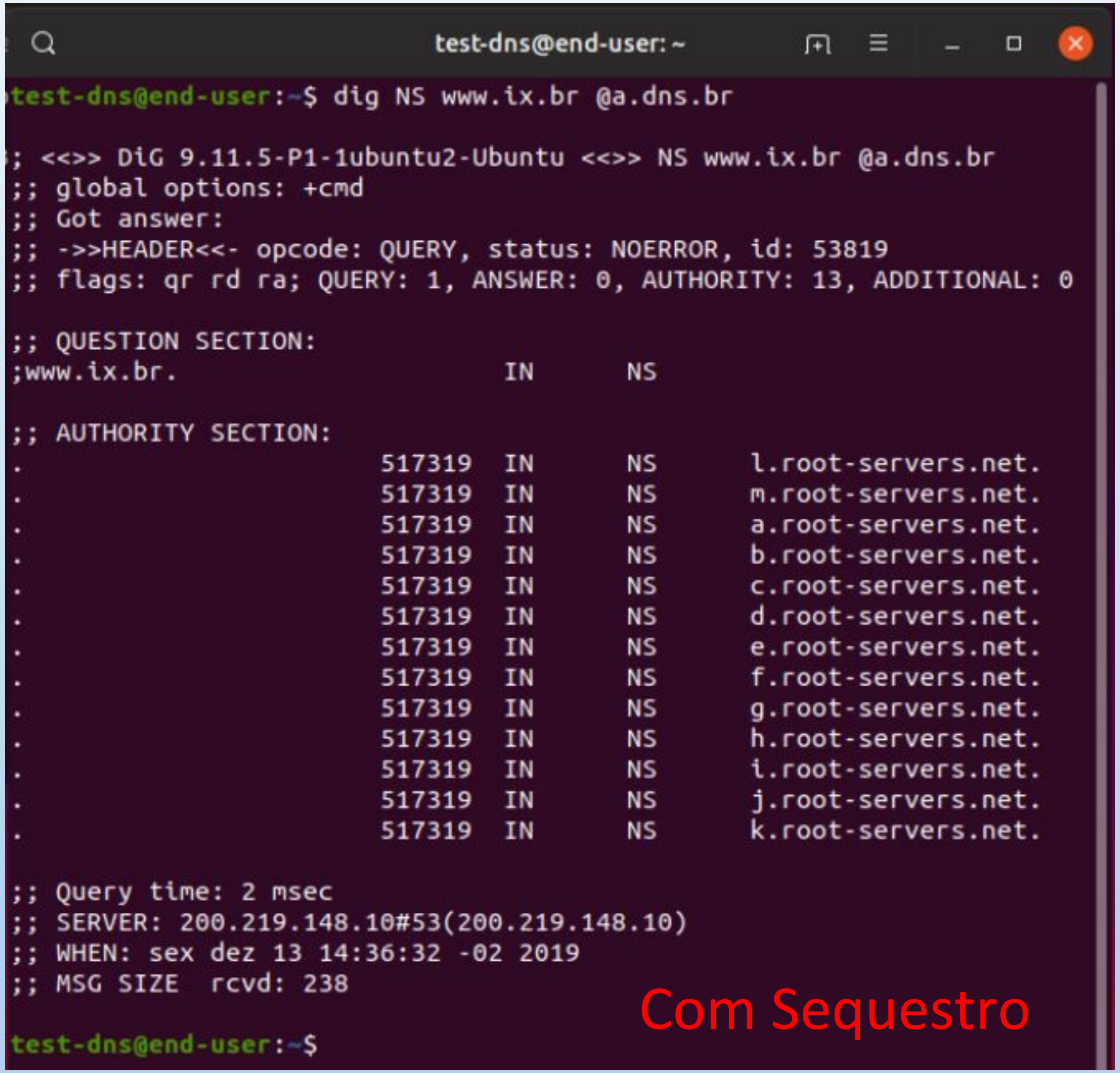


```
test-dns@end-user:~$ ping 9.9.9.9 -c 5
PING 9.9.9.9 (9.9.9.9) 56(84) bytes of data.
64 bytes from 9.9.9.9: icmp_seq=1 ttl=53 time=68.4 ms
64 bytes from 9.9.9.9: icmp_seq=2 ttl=53 time=37.6 ms
64 bytes from 9.9.9.9: icmp_seq=3 ttl=53 time=48.1 ms
64 bytes from 9.9.9.9: icmp_seq=4 ttl=53 time=60.6 ms
64 bytes from 9.9.9.9: icmp_seq=5 ttl=53 time=51.0 ms

--- 9.9.9.9 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 9m
s
rtt min/avg/max/mdev = 37.560/53.121/68.363/10.583 ms
test-dns@end-user:~$
```



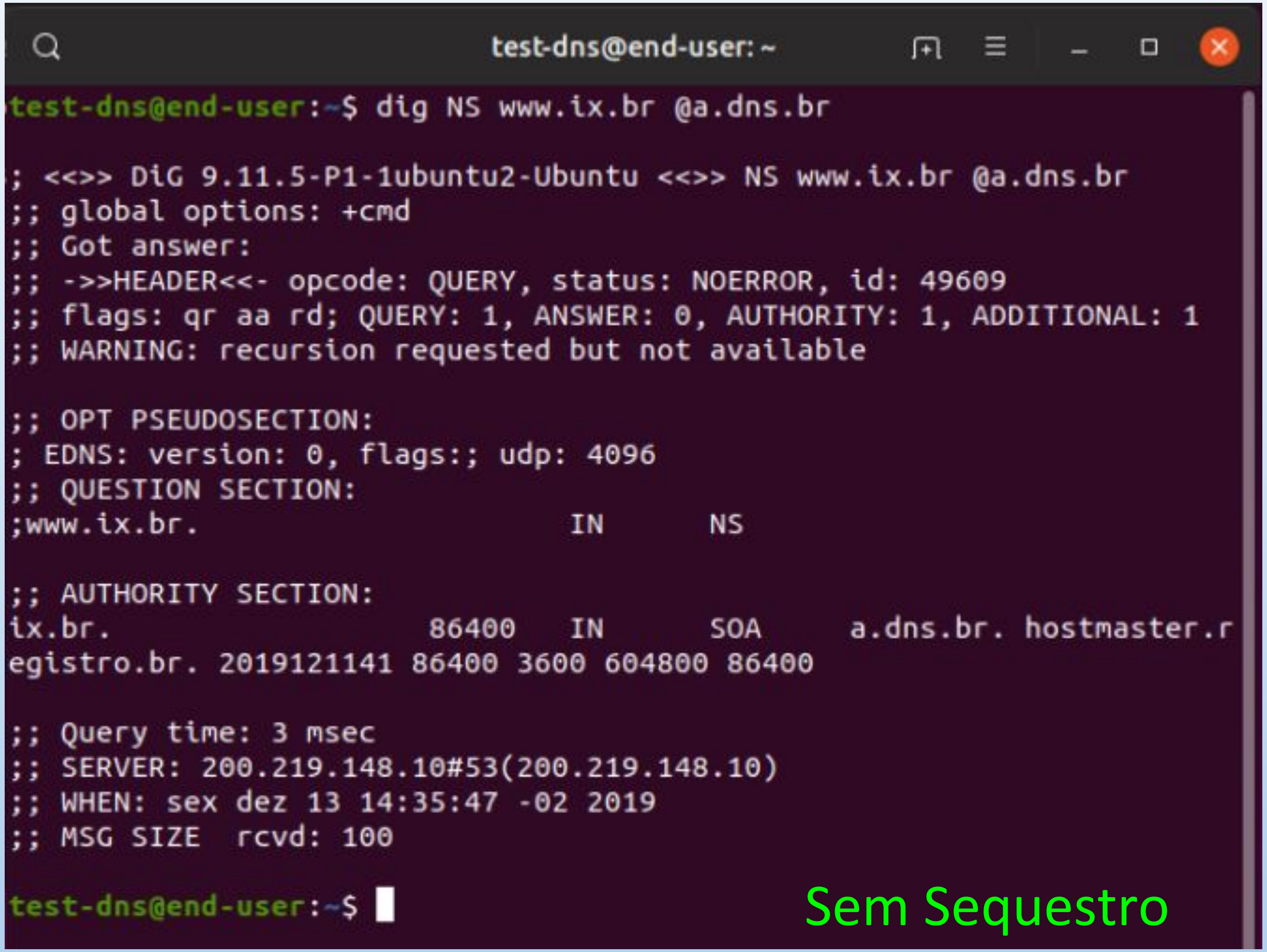
```
                       My traceroute  [v0.92]
end-user (10.20.30.99)                2019-12-13T12:32:37-0200
Keys:  Help   Display mode   Restart statistics   Order of
 fields   quit   Packets                   Pings
 Host              Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. _gateway        0.0%    16    1.9   1.1   0.6   2.7   0.6
 2. 192.0.0.1       0.0%    16    0.9   1.4   0.8   2.6   0.6
 3. gw.evento.      0.0%    16    2.7   3.5   1.9   6.9   1.4
 4. ge-1-3-0-7      6.2%    16    8.3   6.8   2.9  15.5   3.6
 5. ae0-0.core      6.2%    16    3.4   8.4   3.2  26.4   6.2
 6. xe-4-0-0-6      0.0%    15    7.2   9.0   3.2  17.8   4.4
 7. as13335.sa      0.0%    15    4.6   7.5   2.7  14.6   3.3
 8. one.one.on      0.0%    15    4.6   9.2   3.7  15.5   4.5
```

Sequestrando DNS - DST-NAT - Diferença na recursão



```
test-dns@end-user:~$ dig NS www.ix.br @a.dns.br

; <<>> DiG 9.11.5-P1-1ubuntu2-Ubuntu <<>> NS www.ix.br @a.dns.br
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53819
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 0

;; QUESTION SECTION:
;www.ix.br.                     IN      NS

;; AUTHORITY SECTION:
.                       517319  IN      NS      l.root-servers.net.
.                       517319  IN      NS      m.root-servers.net.
.                       517319  IN      NS      a.root-servers.net.
.                       517319  IN      NS      b.root-servers.net.
.                       517319  IN      NS      c.root-servers.net.
.                       517319  IN      NS      d.root-servers.net.
.                       517319  IN      NS      e.root-servers.net.
.                       517319  IN      NS      f.root-servers.net.
.                       517319  IN      NS      g.root-servers.net.
.                       517319  IN      NS      h.root-servers.net.
.                       517319  IN      NS      i.root-servers.net.
.                       517319  IN      NS      j.root-servers.net.
.                       517319  IN      NS      k.root-servers.net.

;; Query time: 2 msec
;; SERVER: 200.219.148.10#53(200.219.148.10)
;; WHEN: sex dez 13 14:36:32 -02 2019
;; MSG SIZE  rcvd: 238

test-dns@end-user:~$
```

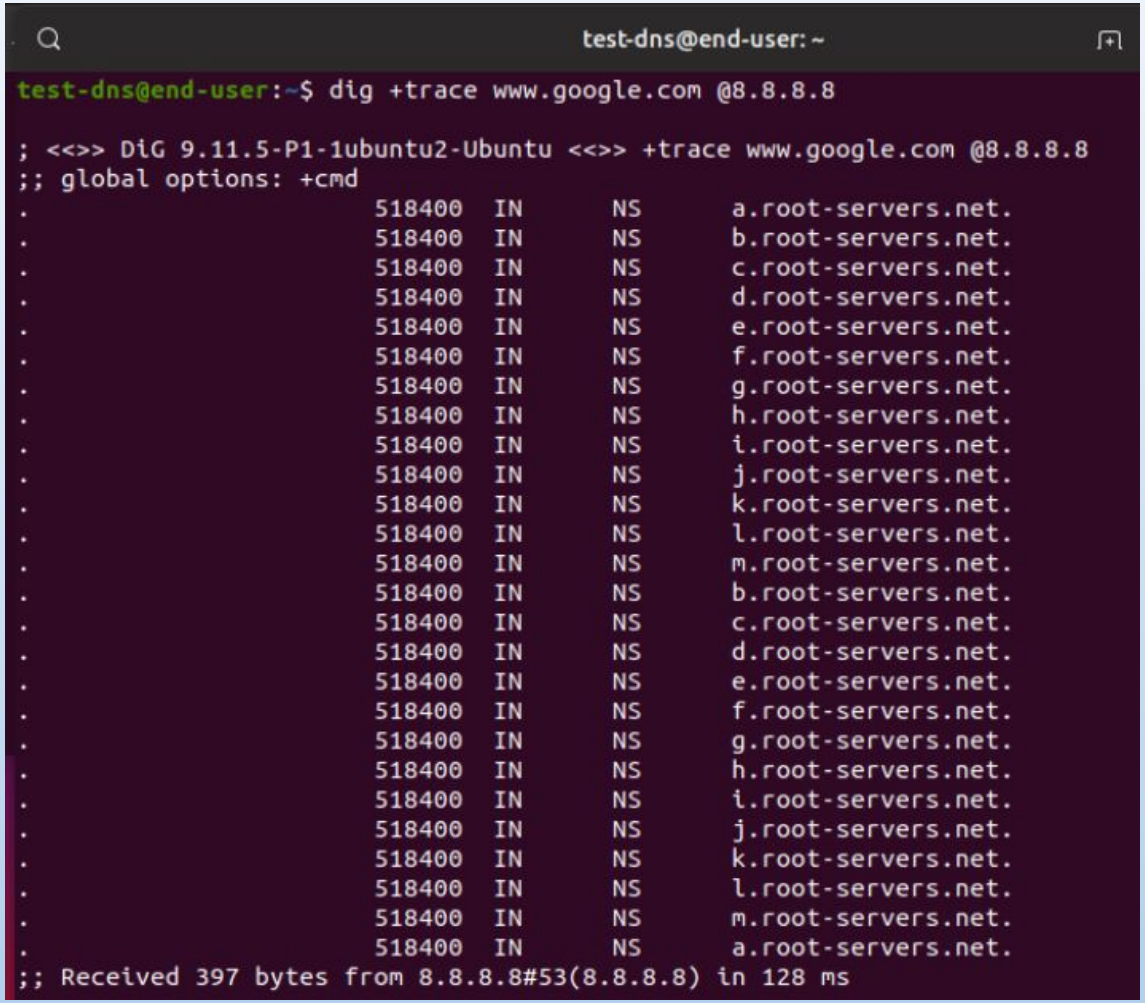
Com Sequestro



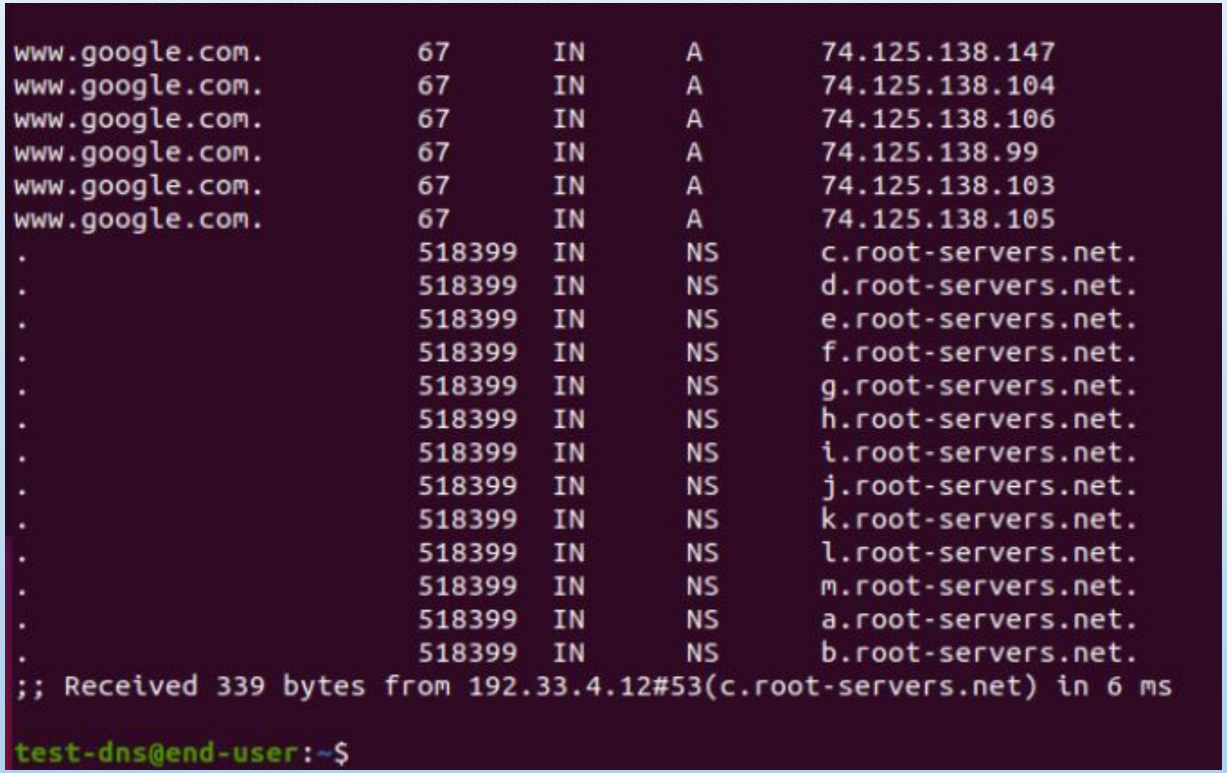
```
test-dns@end-user:~$ dig NS www.ix.br @a.dns.br

; <<>> DiG 9.11.5-P1-1ubuntu2-Ubuntu <<>> NS www.ix.br @a.dns.br
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49609
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.ix.br.                     IN      NS

;; AUTHORITY SECTION:
ix.br.                  86400   IN      SOA     a.dns.br. hostmaster.r
egistro.br. 2019121141 86400 3600 604800 86400

;; Query time: 3 msec
;; SERVER: 200.219.148.10#53(200.219.148.10)
;; WHEN: sex dez 13 14:35:47 -02 2019
;; MSG SIZE  rcvd: 100

test-dns@end-user:~$
```

Sem Sequestro

O DIG é seu amigo! - Trace com DNS Sequestrado via NAT...

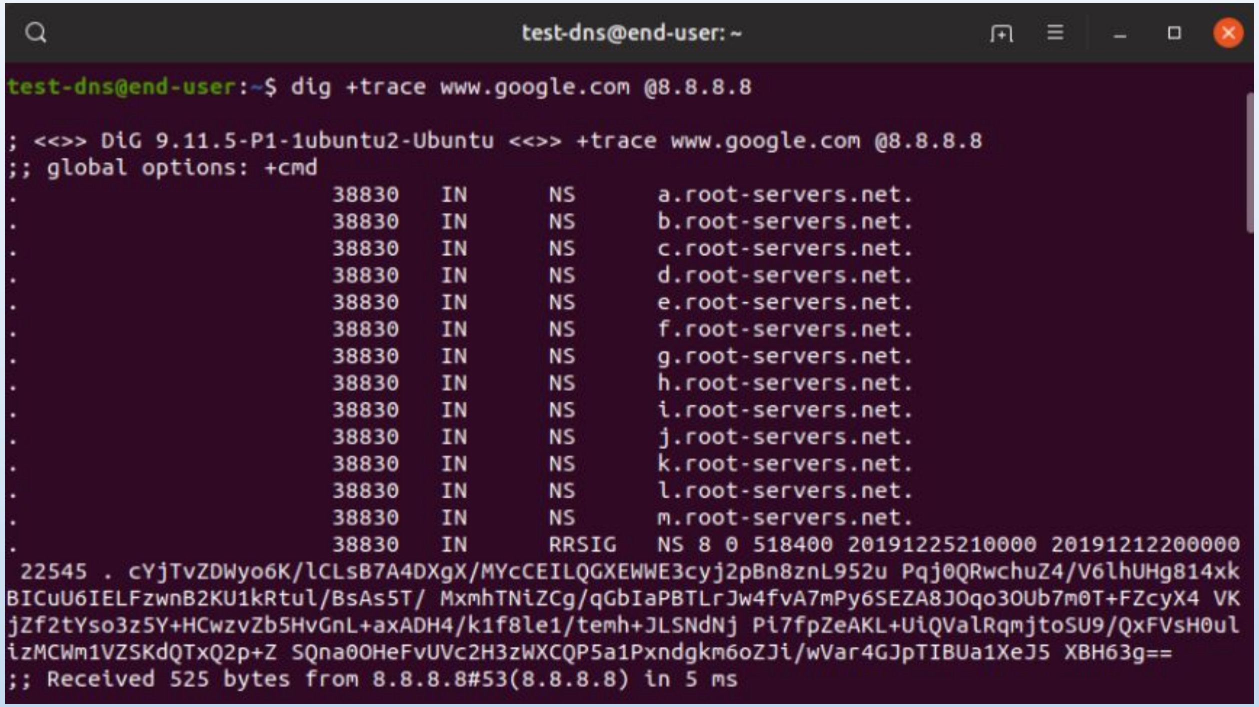


```
test-dns@end-user:~$ dig +trace www.google.com @8.8.8.8

; <<>> DiG 9.11.5-P1-1ubuntu2-Ubuntu <<>> +trace www.google.com @8.8.8.8
;; global options: +cmd
.                       518400  IN      NS      a.root-servers.net.
.                       518400  IN      NS      b.root-servers.net.
.                       518400  IN      NS      c.root-servers.net.
.                       518400  IN      NS      d.root-servers.net.
.                       518400  IN      NS      e.root-servers.net.
.                       518400  IN      NS      f.root-servers.net.
.                       518400  IN      NS      g.root-servers.net.
.                       518400  IN      NS      h.root-servers.net.
.                       518400  IN      NS      i.root-servers.net.
.                       518400  IN      NS      j.root-servers.net.
.                       518400  IN      NS      k.root-servers.net.
.                       518400  IN      NS      l.root-servers.net.
.                       518400  IN      NS      m.root-servers.net.
.                       518400  IN      NS      b.root-servers.net.
.                       518400  IN      NS      c.root-servers.net.
.                       518400  IN      NS      d.root-servers.net.
.                       518400  IN      NS      e.root-servers.net.
.                       518400  IN      NS      f.root-servers.net.
.                       518400  IN      NS      g.root-servers.net.
.                       518400  IN      NS      h.root-servers.net.
.                       518400  IN      NS      i.root-servers.net.
.                       518400  IN      NS      j.root-servers.net.
.                       518400  IN      NS      k.root-servers.net.
.                       518400  IN      NS      l.root-servers.net.
.                       518400  IN      NS      m.root-servers.net.
.                       518400  IN      NS      a.root-servers.net.
;; Received 397 bytes from 8.8.8.8#53(8.8.8.8) in 128 ms
```

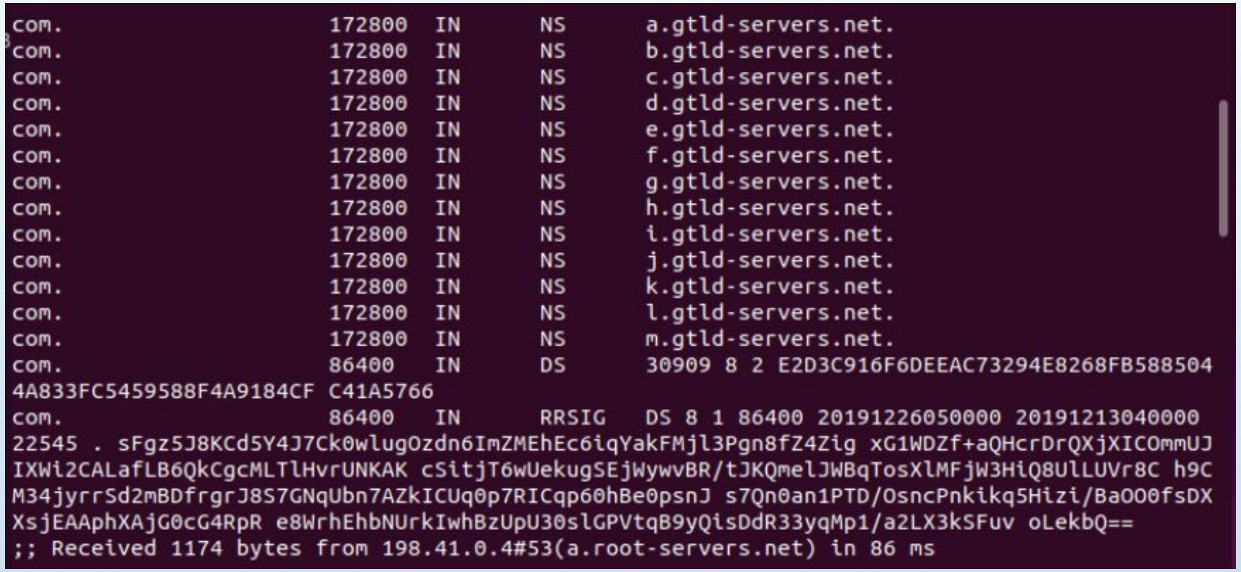


```
www.google.com.         67      IN      A       74.125.138.147
www.google.com.         67      IN      A       74.125.138.104
www.google.com.         67      IN      A       74.125.138.106
www.google.com.         67      IN      A       74.125.138.99
www.google.com.         67      IN      A       74.125.138.103
www.google.com.         67      IN      A       74.125.138.105
.                       518399  IN      NS      c.root-servers.net.
.                       518399  IN      NS      d.root-servers.net.
.                       518399  IN      NS      e.root-servers.net.
.                       518399  IN      NS      f.root-servers.net.
.                       518399  IN      NS      g.root-servers.net.
.                       518399  IN      NS      h.root-servers.net.
.                       518399  IN      NS      i.root-servers.net.
.                       518399  IN      NS      j.root-servers.net.
.                       518399  IN      NS      k.root-servers.net.
.                       518399  IN      NS      l.root-servers.net.
.                       518399  IN      NS      m.root-servers.net.
.                       518399  IN      NS      a.root-servers.net.
.                       518399  IN      NS      b.root-servers.net.
;; Received 339 bytes from 192.33.4.12#53(c.root-servers.net) in 6 ms

test-dns@end-user:~$
```

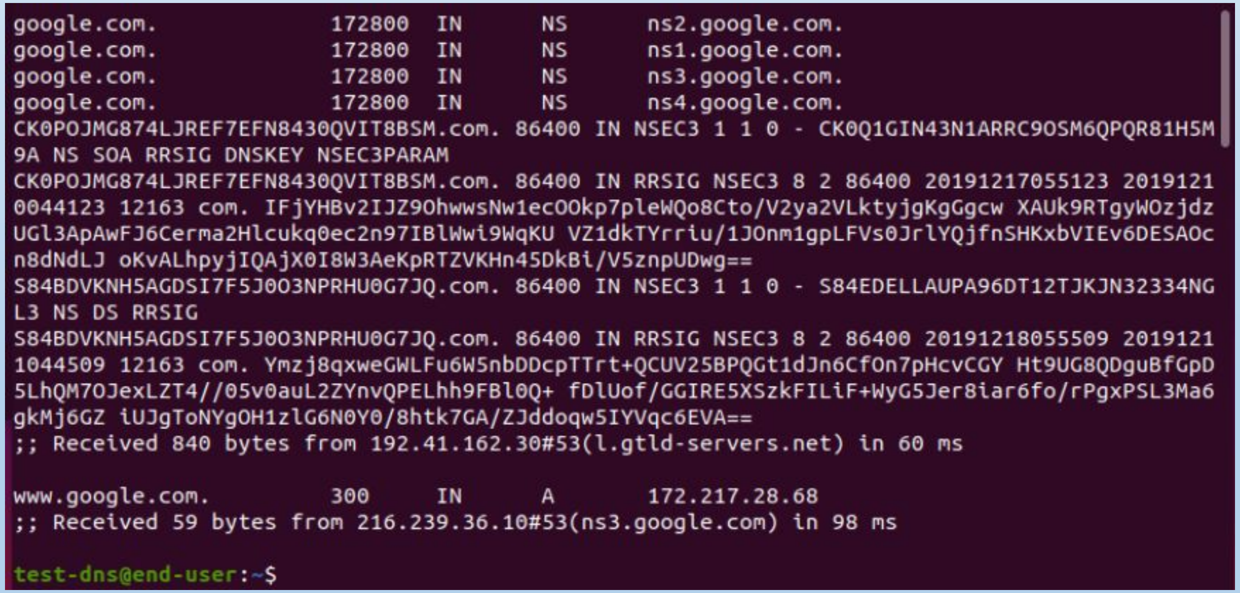
O DIG é seu amigo! - Trace sem Sequestro...



```
test-dns@end-user:~$ dig +trace www.google.com @8.8.8.8

; <<>> DiG 9.11.5-P1-1ubuntu2-Ubuntu <<>> +trace www.google.com @8.8.8.8
;; global options: +cmd
.                       38830   IN      NS      a.root-servers.net.
.                       38830   IN      NS      b.root-servers.net.
.                       38830   IN      NS      c.root-servers.net.
.                       38830   IN      NS      d.root-servers.net.
.                       38830   IN      NS      e.root-servers.net.
.                       38830   IN      NS      f.root-servers.net.
.                       38830   IN      NS      g.root-servers.net.
.                       38830   IN      NS      h.root-servers.net.
.                       38830   IN      NS      i.root-servers.net.
.                       38830   IN      NS      j.root-servers.net.
.                       38830   IN      NS      k.root-servers.net.
.                       38830   IN      NS      l.root-servers.net.
.                       38830   IN      NS      m.root-servers.net.
.                       38830   IN      RRSIG   NS 8 0 518400 20191225210000 20191212200000
 22545 . cYjTvZDWyo6K/lCLsB7A4DXgX/MYcCEILQGXEWWE3cyj2pBn8znL952u Pqj0QRwchuZ4/V6lhUHg814xk
BICuU6IELFzwnB2KU1kRtul/BsAs5T/ MxmhTNiZCg/qGbIaPBTLrJw4fvA7mPy6SEZA8JOqo3OUb7m0T+FZcyX4 VK
jZf2tYso3z5Y+HCwzvZb5HvGnL+axADH4/k1f8le1/temh+JLSNdNj Pi7fpZeAKL+UiQValRqmjtoSU9/QxFVsH0ul
izMCWm1VZSKdQTxQ2p+Z SQna0OHeFvUVc2H3zWXCQP5a1Pxndgkm6oZJi/wVar4GJpTIBUa1XeJ5 XBH63g==
;; Received 525 bytes from 8.8.8.8#53(8.8.8.8) in 5 ms
```



```
com.                    172800  IN      NS      a.gtld-servers.net.
com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      c.gtld-servers.net.
com.                    172800  IN      NS      d.gtld-servers.net.
com.                    172800  IN      NS      e.gtld-servers.net.
com.                    172800  IN      NS      f.gtld-servers.net.
com.                    172800  IN      NS      g.gtld-servers.net.
com.                    172800  IN      NS      h.gtld-servers.net.
com.                    172800  IN      NS      i.gtld-servers.net.
com.                    172800  IN      NS      j.gtld-servers.net.
com.                    172800  IN      NS      k.gtld-servers.net.
com.                    172800  IN      NS      l.gtld-servers.net.
com.                    172800  IN      NS      m.gtld-servers.net.
com.                    86400   IN      DS      30909 8 2 E2D3C916F6DEEAC73294E8268FB588504
4A833FC5459588F4A9184CF C41A5766
com.                    86400   IN      RRSIG   DS 8 1 86400 20191226050000 20191213040000
22545 . sFgz5J8KCd5Y4J7Ck0wlugOzdn6ImZMEhEc6iqYakFMjl3Pgn8fZ4Zig xG1WDZf+aQHcrDrQXjXICOmmUJ
IXWi2CALafLB6QkCgcMLTlHvrUNKAK cSitjT6wUekugSEjWywvBR/tJKQmelJWBqTosXlMFjW3HiQ8UlLUVr8C h9C
M34jyrrSd2mBDfrgrJ8S7GNqUbn7AZkICUq0p7RICqp60hBe0psnJ s7Qn0an1PTD/OsncPnkikq5Hizi/BaOO0fsDX
XsjEAAphXAjG0cG4RpR e8WrhEhbNUrkIwhBzUpU30slGPVtqB9yQisDdR33yqMp1/a2LX3kSFuv oLekbQ==
;; Received 1174 bytes from 198.41.0.4#53(a.root-servers.net) in 86 ms
```



```
google.com.             172800  IN      NS      ns2.google.com.
google.com.             172800  IN      NS      ns1.google.com.
google.com.             172800  IN      NS      ns3.google.com.
google.com.             172800  IN      NS      ns4.google.com.
CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN NSEC3 1 1 0 - CK0Q1GIN43N1ARRC9OSM6QPQR81H5M
9A NS SOA RRSIG DNSKEY NSEC3PARAM
CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN RRSIG NSEC3 8 2 86400 20191217055123 2019121
0044123 12163 com. IFjYHBv2IJZ9OhwwsNw1ecOOkp7pleWQo8Cto/V2ya2VLktyjgKgGgcw XAUk9RTgyWOzjdz
UGl3ApAwFJ6Cerma2Hlcukq0ec2n97IBlWwi9WqKU VZ1dkTYrriu/1JOnm1gpLFVs0JrlYQjfnSHKxbVIEv6DESAOc
n8dNdLJ oKvALhpyjIQAjX0I8W3AeKpRTZVKHn45DkBi/V5znpUDwg==
S84BDVKNH5AGDSI7F5J0O3NPRHU0G7JQ.com. 86400 IN NSEC3 1 1 0 - S84EDELLAUPA96DT12TJKJN32334NG
L3 NS DS RRSIG
S84BDVKNH5AGDSI7F5J0O3NPRHU0G7JQ.com. 86400 IN RRSIG NSEC3 8 2 86400 20191218055509 2019121
1044509 12163 com. Ymzj8qxweGWLFu6W5nbDDcpTTrt+QCUV25BPQGt1dJn6CfOn7pHcvCGY Ht9UG8QDguBfGpD
5LhQM7OJexLZT4//05v0auL2ZYnvQPELhh9FBl0Q+ fDlUof/GGIRE5XSzkFILiF+WyG5Jer8iar6fo/rPgxPSL3Ma6
gkMj6GZ iUJgToNYgOH1zlG6N0Y0/8htk7GA/ZJddoqw5IYVqc6EVA==
;; Received 840 bytes from 192.41.162.30#53(l.gtld-servers.net) in 60 ms

www.google.com.         300     IN      A       172.217.28.68
;; Received 59 bytes from 216.239.36.10#53(ns3.google.com) in 98 ms

test-dns@end-user:~$
```

Como evitar o sequestro de tráfego de DNS?

DNS-Crypt

- Portas UDP/443 e TCP/443
- https://github.com/DNSCrypt/dnscrypt-protocol/blob/master/DNSCRYPT-V2-PROTOCOL.txt

DNS-over-HTTPS

- Porta TCP/443
- https://tools.ietf.org/html/rfc8484

DNS-over-TLS

- Portas UDP/853 e TCP/853
- https://tools.ietf.org/html/rfc7858

Conclusões

Sim! É possível identificar que o DNS está sendo sequestrado, mesmo sem DNS-over-TLS ou DNS-over-HTTPs.

Sim! Sem você sequestra DNS você está sim interferindo numa parte dos tipos de consultas DNS. E isso é Ruim e errado!

Opiniões

Open-Resolvers centralizados são ruins para a experiência do usuário!

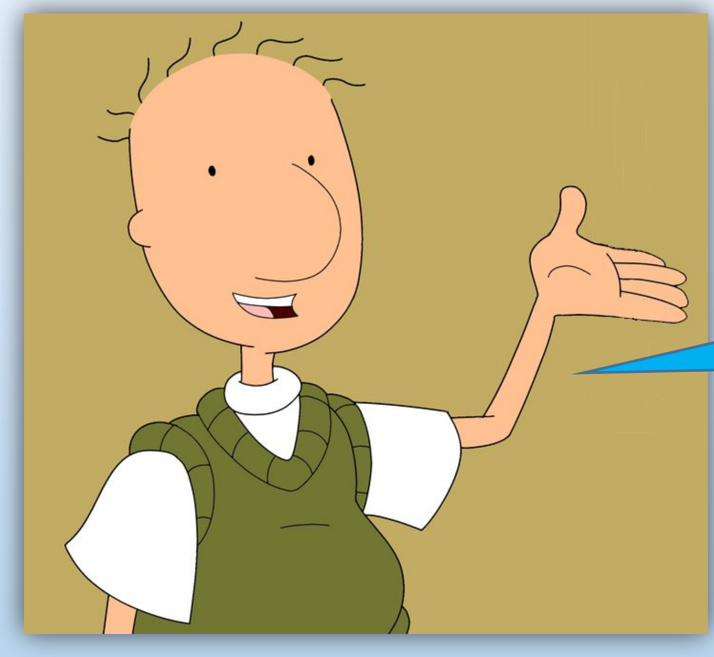
- Adicionam latência na resposta DNS.
- Quebram a privacidade do usuário.

Só tornam melhores a experiência de navegação se o serviço de DNS-Server recursivo de seu provedor for de péssima qualidade.

Pedidos

Não quebre a Internet!

- Se você fizer isso, sempre vai existir quem vai apontar o dedo para você e te classificar como alguém de má fé, ou sem a devida competência para fazer o que está se propondo.



Perguntas?

“Você tem que ser o que você realmente é.

Pois se você não for quem você é, afinal quem é você?”
Doug Funnie

Prévia de um projeto - Procurando ajuda!

DNS-Server Recursivo Aberto Anycat Self-Hosted

- Endereço IP mnemônico (bonito)
- Mais próximo o possível do End-User
- Privacidade com premissa imprescindível
- Virtual Machine
- Boa engine de DNS
- Hyper Local
- DNS / DoT / DoH
- Auto verificação de Saúde
- BGP para anunciar o Anycast
- Comando e controle centralizado de todos os nós
- Portal com Estatísticas de cada nó