Trabalho de Redes II

Aluno: Gabriel Oliveira Campos

Introdução

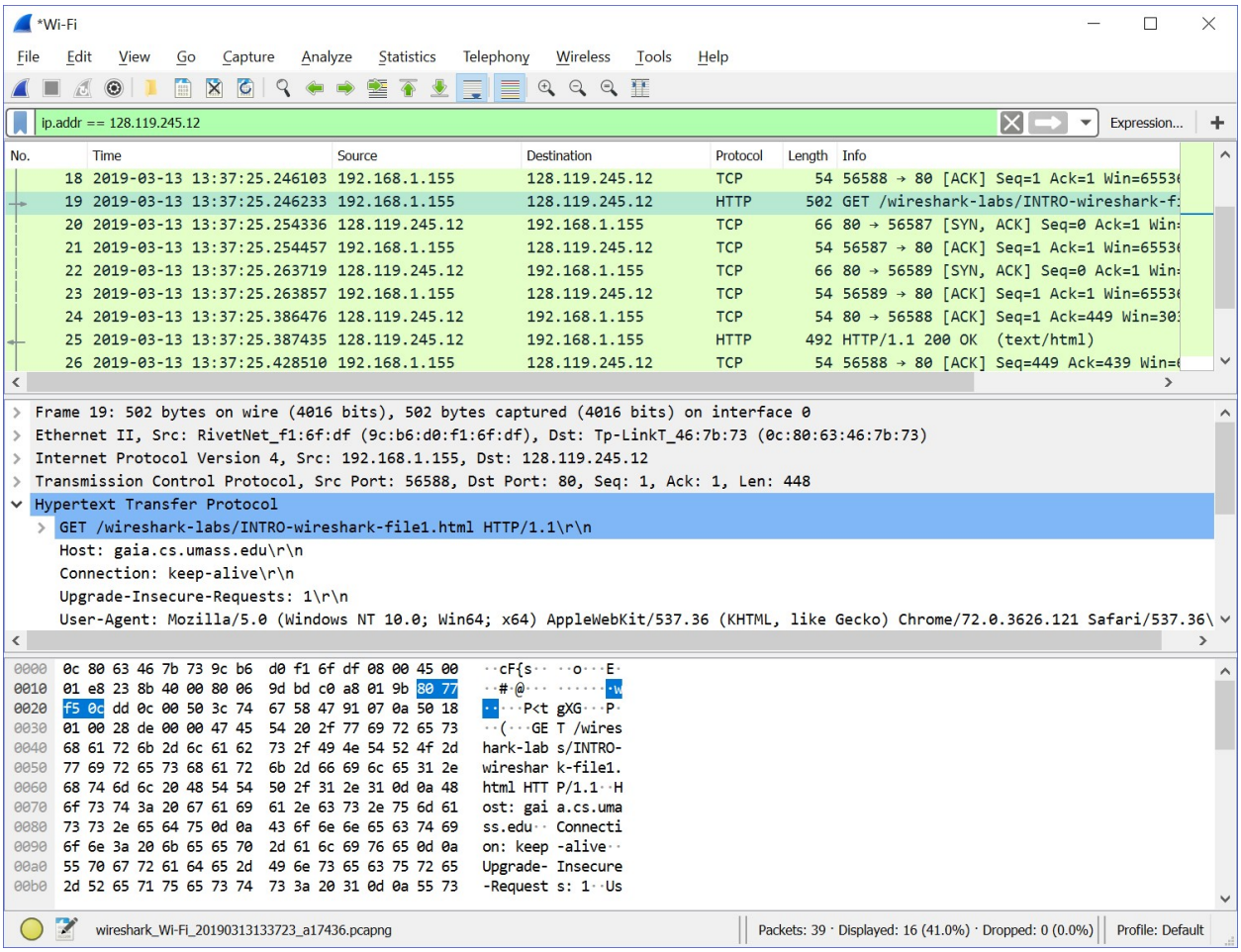
1- HTTP e TCP foram os protocolos encontrados

2- 141,202 milissegundos

3- IP Rede -> 192.168.1.155

IP Gaia -> 128.119.245.12

4-



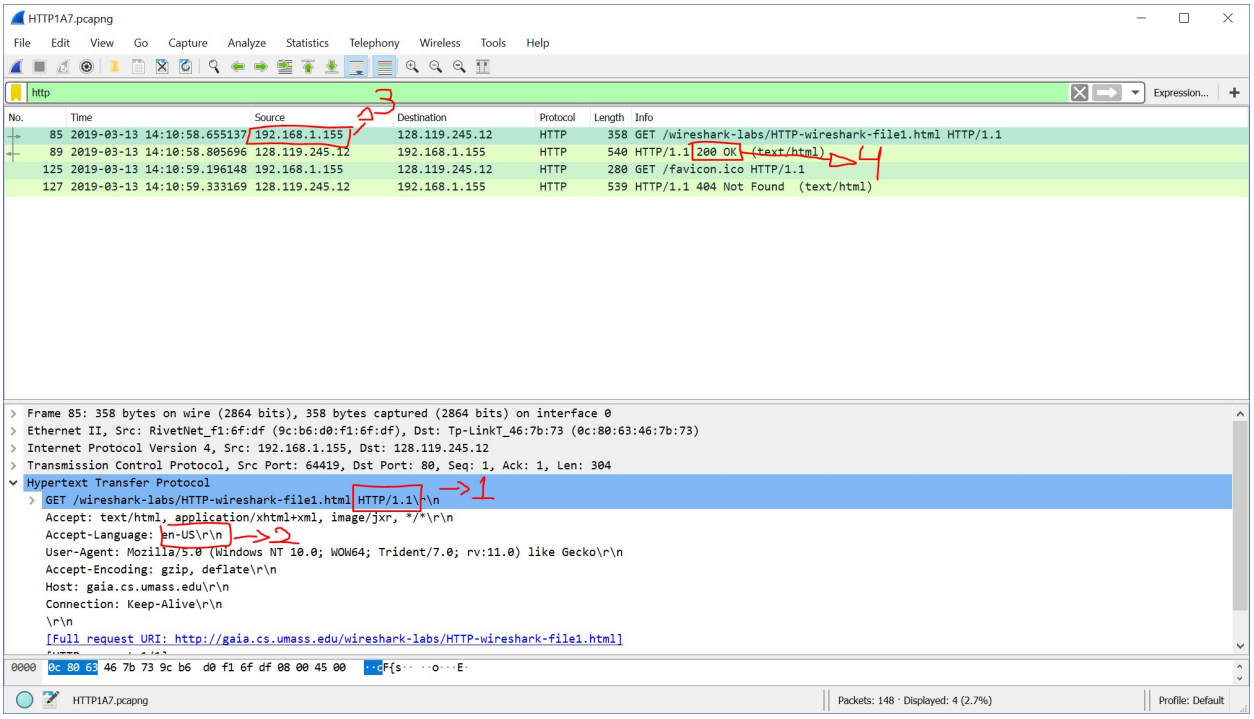
HTTP

1- O navegar utiliza o HTTP 1.1, o mesmo ao qual o servidor roda.

2- O servidor aceita a linguagem en-US (english - USA)

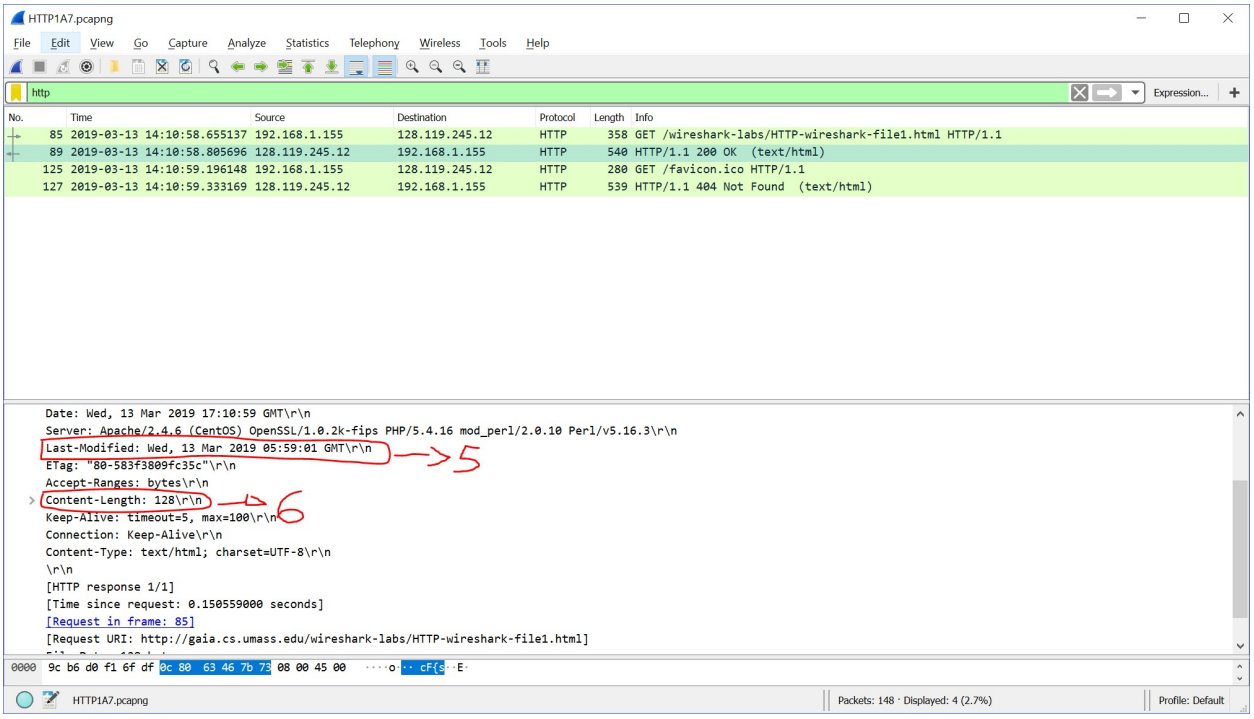
3- O meu endereço IP é 192.168.1.155 e o do servidor é 128.119.245.12

4- Código de status: 200 OK



5- Última vez que foi modificado foi no dia 13 de março de 2019 as 05:59:01 GMT

6- Content Lenght foi de 128 bytes



7- Não

8- Não

9- Sim, pois toda resposta do arquivo HTML está dentro do pacote

10- Sim, segue a mensagem: "Wed, 13 Mar 2019 05:59:01 GMT \r\n"

11- 304 Not modified. O servidor não retornou explicitamente o conteúdo pois não houve alteração no mesmo.

12- Apenas 1 Mensagem HTTP GET foi enviada.

13- Foram necessários 4 segmentos TCP (#15, #16, #17, #18)

14- Código de status: 200 OK

15- Não

16- 3 HTTP GET foram enviados.

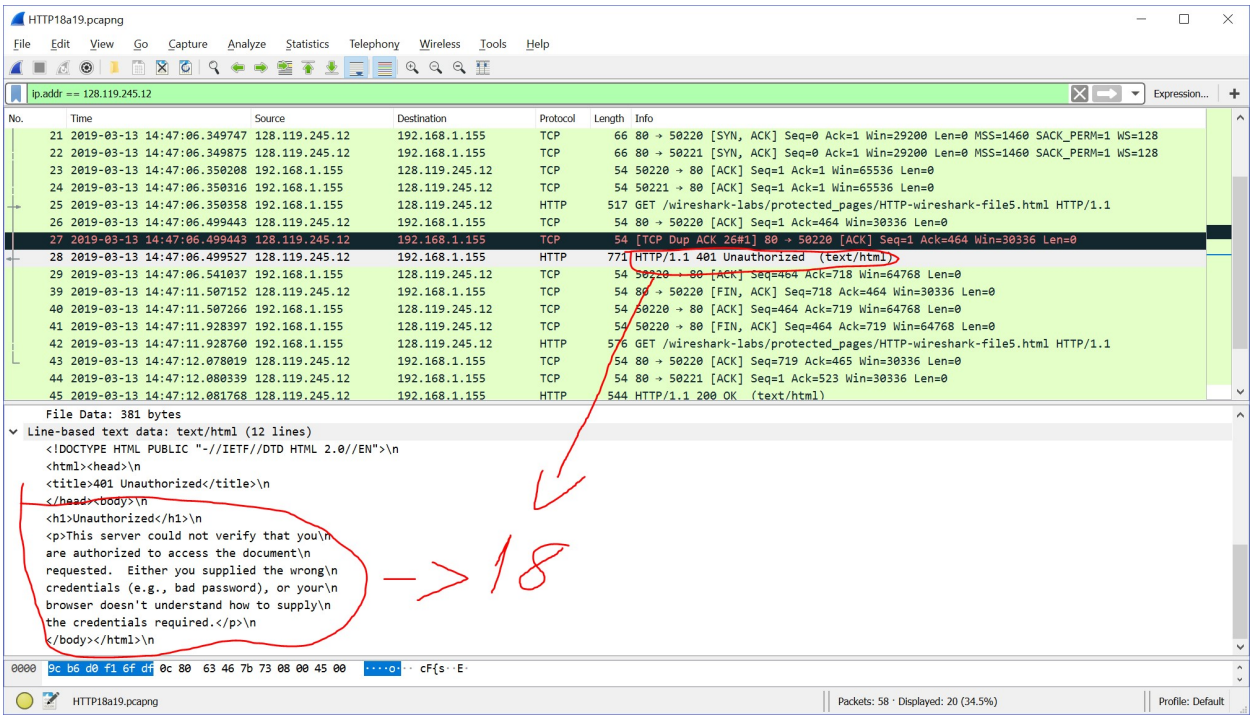
IP:http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html

IP:http://gaia.cs.umass.edu/pearson.png

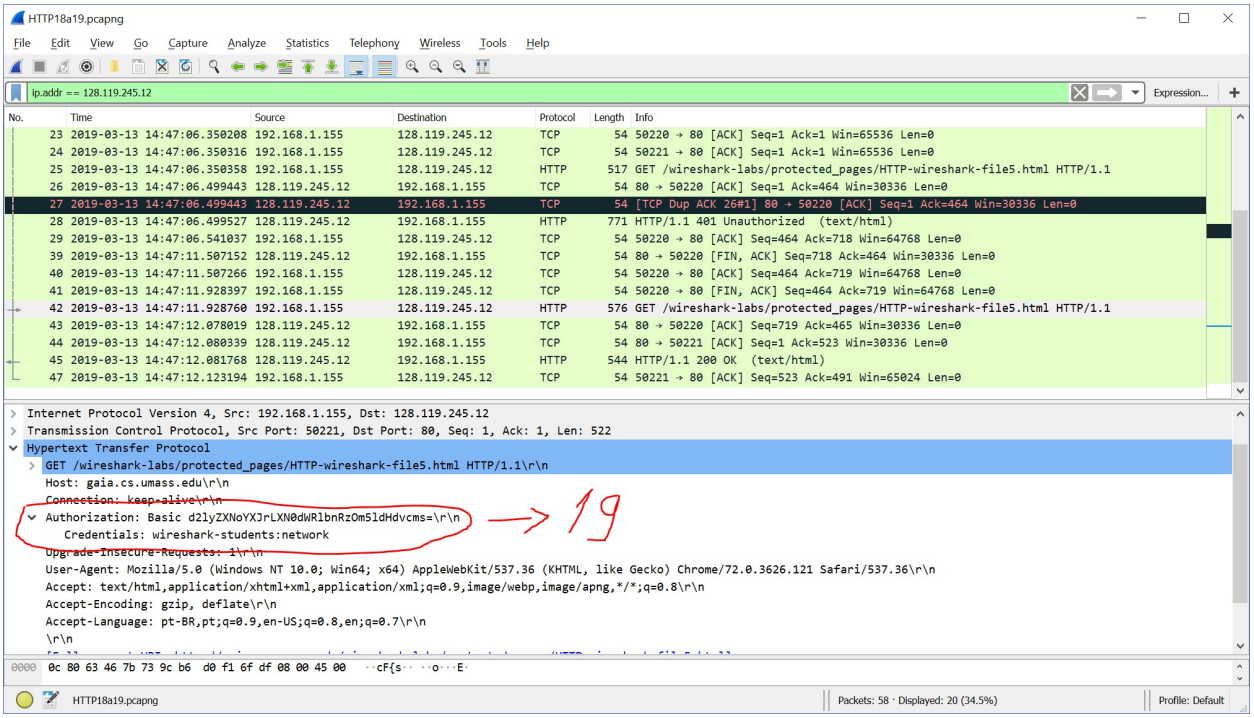
IP:http://manic.cs.umass.edu/~kurose/cover_5th_ed.jpg

17- Foi baixada em sequencial, pois esperaram a resposta OK do servidor para iniciar a próxima.

18- 401 Unauthorized



19- Apareceu o campo Authorization, pois o servidor aceitou o login e senha.



DNS

1 - Site: www.square-enix.co.jp IP:201.17.166.139

2 - site da Universidade de Cambridge:

cam.ac.uk nameserver = sns-pb.isc.org

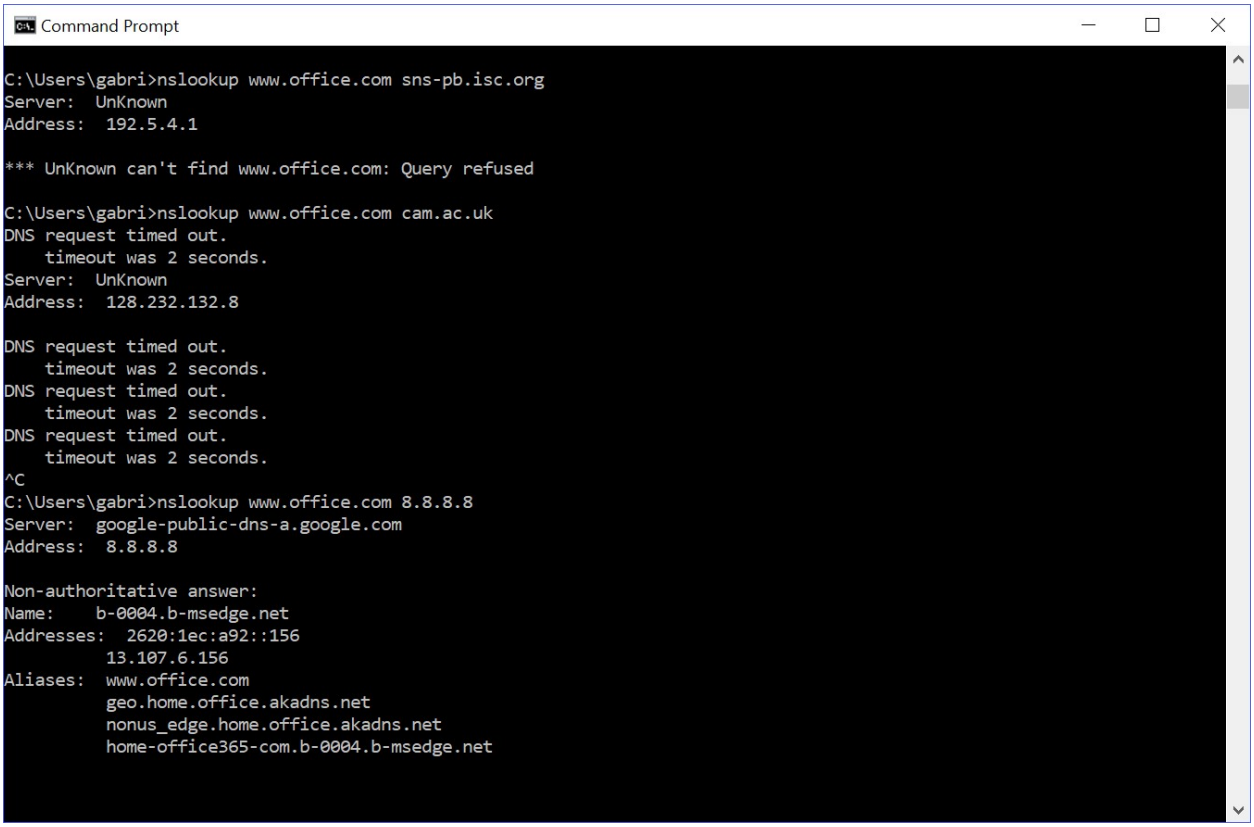
cam.ac.uk nameserver = ns2.ic.ac.uk

cam.ac.uk nameserver = authdns0.csx.cam.ac.uk

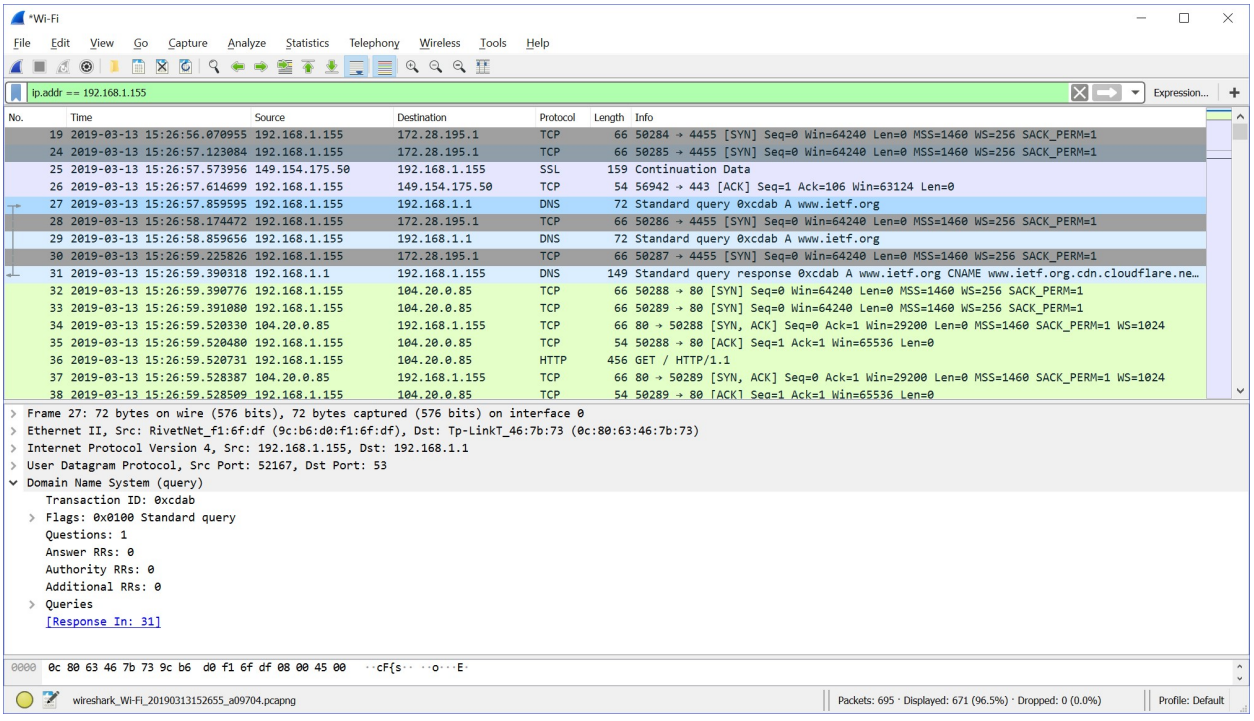
cam.ac.uk nameserver = dns0.cl.cam.ac.uk

cam.ac.uk nameserver = dns0.eng.cam.ac.uk

3-


Command Prompt
C:\Users\gabri>nslookup www.office.com sns-pb.isc.org
Server: UnKnown
Address: 192.5.4.1
*** UnKnown can't find www.office.com: Query refused
C:\Users\gabri>nslookup www.office.com cam.ac.uk
DNS request timed out.
timeout was 2 seconds.
Server: UnKnown
Address: 128.232.132.8
DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
^C
C:\Users\gabri>nslookup www.office.com 8.8.8.8
Server: google-public-dns-a.google.com
Address: 8.8.8.8
Non-authoritative answer:
Name: b-0004.b-msedge.net
Addresses: 2620:1ec:a92::156
13.107.6.156
Aliases: www.office.com
geo.home.office.akadns.net
nonus_edge.home.office.akadns.net
home-office365-com.b-0004.b-msedge.net

4-


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.1.155
Expression...
No. Time Source Destination Protocol Length Info
19 2019-03-13 15:26:56.070955 192.168.1.155 172.28.195.1 TCP 66 50284 → 4455 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
24 2019-03-13 15:26:57.123084 192.168.1.155 172.28.195.1 TCP 66 50285 → 4455 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
25 2019-03-13 15:26:57.573956 149.154.175.50 192.168.1.155 SSL 159 Continuation Data
26 2019-03-13 15:26:57.614699 192.168.1.155 149.154.175.50 TCP 54 56942 → 443 [ACK] Seq=1 Ack=106 Win=63124 Len=0
27 2019-03-13 15:26:57.859595 192.168.1.155 192.168.1.1 DNS 72 Standard query 0xcdab A www.ietf.org
28 2019-03-13 15:26:58.174472 192.168.1.155 172.28.195.1 TCP 66 50286 → 4455 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
29 2019-03-13 15:26:58.859656 192.168.1.155 192.168.1.1 DNS 72 Standard query 0xcdab A www.ietf.org
30 2019-03-13 15:26:59.225826 192.168.1.155 172.28.195.1 TCP 66 50287 → 4455 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
31 2019-03-13 15:26:59.390318 192.168.1.1 192.168.1.155 DNS 149 Standard query response 0xcdab A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.ne…
32 2019-03-13 15:26:59.390776 192.168.1.155 104.20.0.85 TCP 66 50288 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
33 2019-03-13 15:26:59.391080 192.168.1.155 104.20.0.85 TCP 66 50289 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
34 2019-03-13 15:26:59.520330 104.20.0.85 192.168.1.155 TCP 66 80 → 50288 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=1024
35 2019-03-13 15:26:59.520480 192.168.1.155 104.20.0.85 TCP 54 50288 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
36 2019-03-13 15:26:59.520731 192.168.1.155 104.20.0.85 HTTP 456 GET / HTTP/1.1
37 2019-03-13 15:26:59.528387 104.20.0.85 192.168.1.155 TCP 66 80 → 50289 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=1024
38 2019-03-13 15:26:59.528509 192.168.1.155 104.20.0.85 TCP 54 50289 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
Frame 27: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
Ethernet II, Src: RivetNet_f1:6f:df (9c:b6:d0:f1:6f:df), Dst: Tp-LinkT_46:7b:73 (0c:80:63:46:7b:73)
Internet Protocol Version 4, Src: 192.168.1.155, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 52167, Dst Port: 53
Domain Name System (query)
Transaction ID: 0xcdab
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
[Response In: 31]
0000 0c 80 63 46 7b 73 9c b6 d0 f1 6f df 08 00 45 00
wireshark_Wi-Fi_20190313152655_a09704.pcapng
Packets: 695 · Displayed: 671 (96.5%) · Dropped: 0 (0.0%)
Profile: Default

5 - Porta Fonte: 52167 Porta Destino: 53

6 - IP->192.168.1.1. Sim são os mesmos endereços

7 - Type A. não foi encontrado campo Answer

8 - Existem 3 campos Answer. Os servidores DNS

9- Não, nenhum deles corresponde.

10- Não

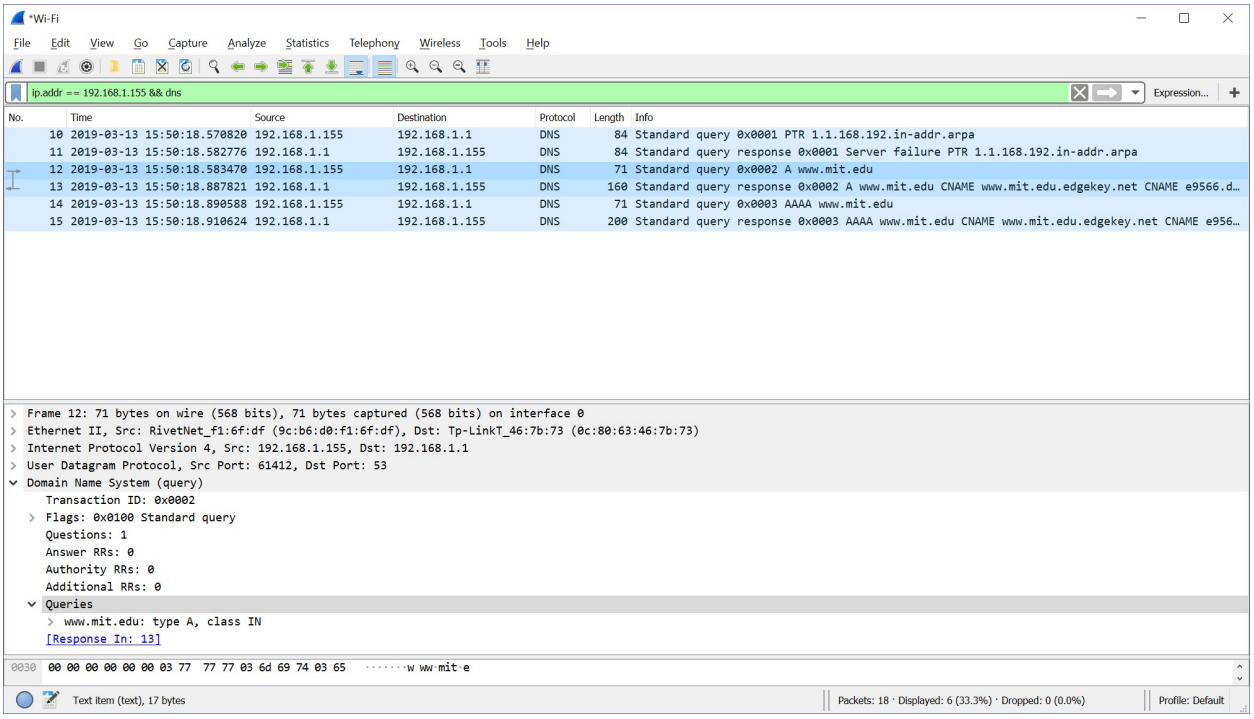
11- Porta origem: 61412 Porta Destino: 53

12- 192.168.1.1. Sim esse é um de meus endereços IP's

13- Type A, sem campo Answer

14- Existem 3 campos Answer. São os servidores DNS

15-



16- Endereço: 192.168.1.1. Sim é um de meus endereços

17- Type NS porém não existe campo Answer

18- Servidores listados:

ns01.telmex.net.br

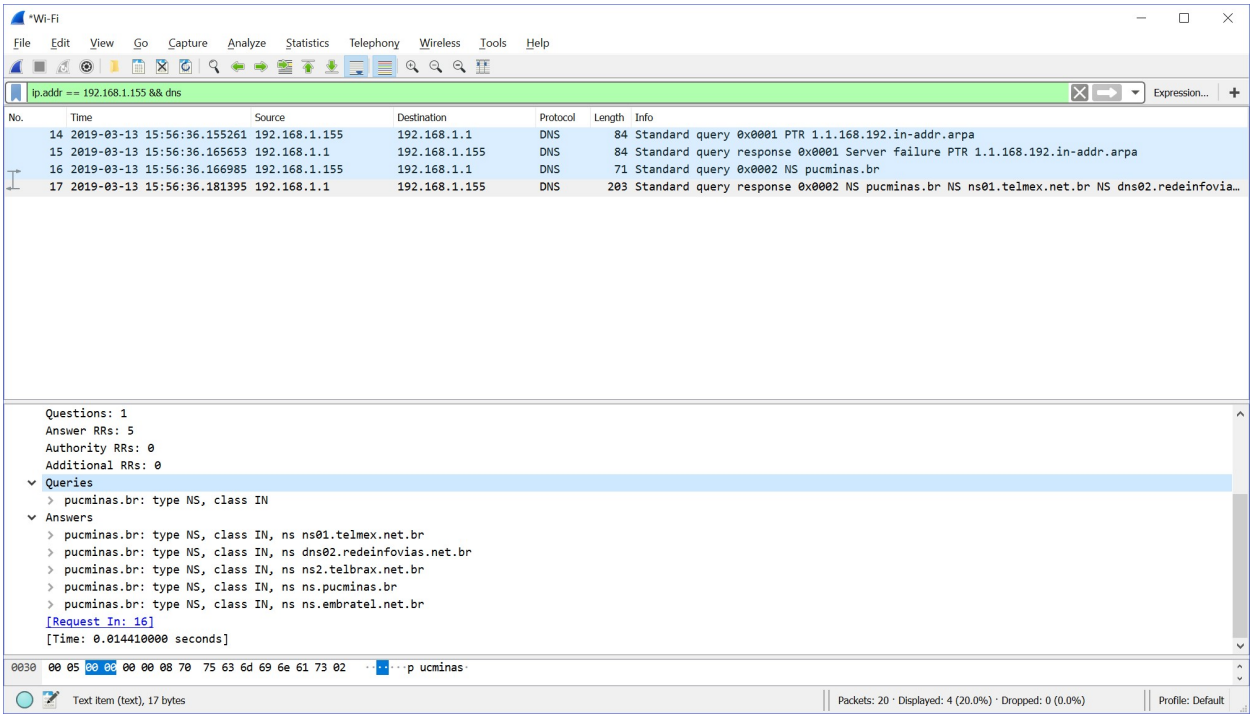
dns02.redeinfovias.net.br

ns2.telbrax.net.br

ns.pucminas.br

ns.embratel.net.br

19- Não, os IPs dos servidores DNS não foram fornecidos.



20- 192.168.1.1, ainda é um de meus endereços locais.

21- Type A. Não possui campo Answer

22- Apenas um campo anwser, com o endereço de ip que foi solicitado.

23-