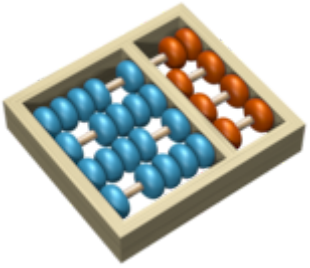


MC833 - Laboratório de Redes

Atividade 1 Ferramentas e *Sniffers*

Aluna: Naomi Takemoto

Instituto de Computação

Universidade Estadual de Campinas

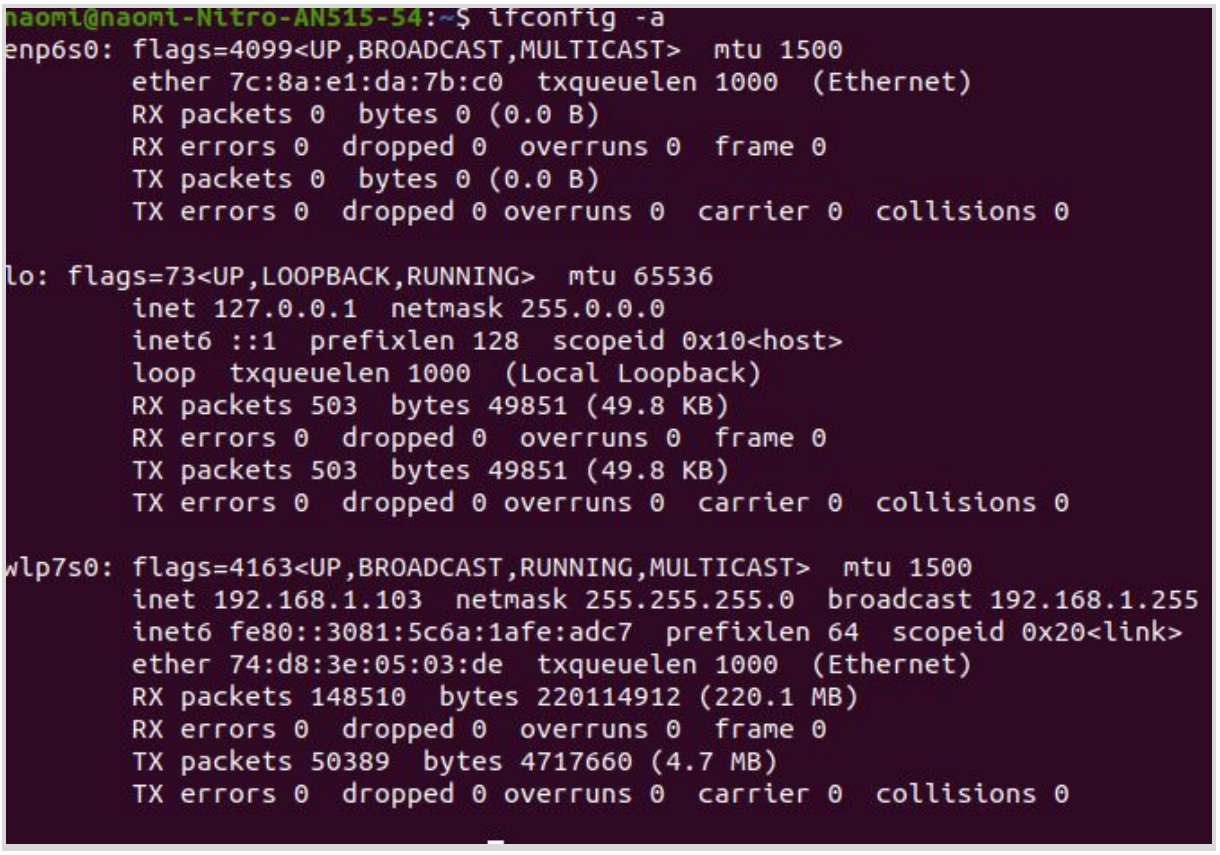
Segundo semestre de 2020

1. Considere para esta questão o comando ifconfig.

a. Qual opção deve ser usada para exibir informações sobre todas as interfaces de rede?

ifconfig -a

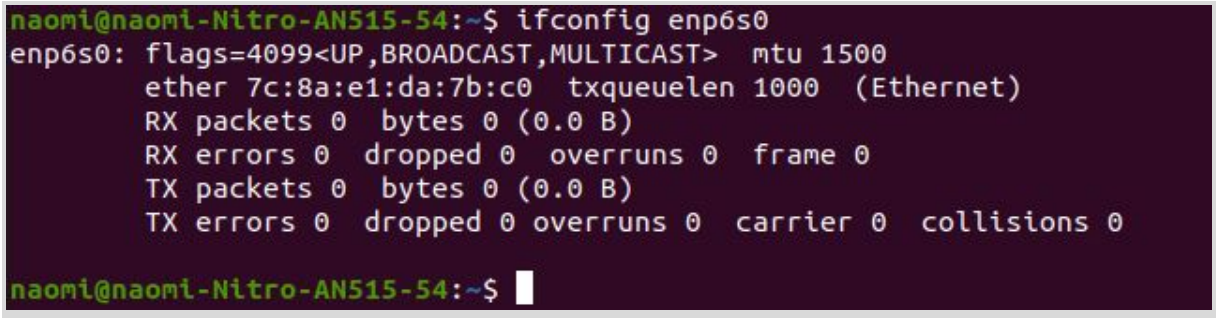
Exemplo:



b. O que deve ser feito para exibir somente informações de uma interface específica?

ifconfig <nome da interface desejada>

Exemplo:



2. Através da execução do comando nslookup seguido dos parâmetros adequados, responda às seguinte questões:

a. Quais são os endereços IP do host www.unicamp.br?

O comando nslookup (name server lookup) busca obter os mapeamentos de nome e endereço IP. Na figura a seguir são listados os endereços IP do site:

```
NAOMI$ nslookup www.unicamp.br
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.unicamp.br  canonical name = 143-106-143-186.nuvem.unicamp.br.
Name:   143-106-143-186.nuvem.unicamp.br
Address: 143.106.143.186
```

b. Há alguma vantagem em haver mais de um endereço IP?

No caso acima, pode-se perceber que existem duas respostas distintas, uma autoritativa e uma não autoritativa. Esta última está relacionada ao caching feito pelo servidor DNS local. Tal procedimento permite a redução do tráfego na rede, bem como diminui o tempo de resposta para se acessar um site por exemplo. A primeira por sua vez é a resposta dada pelo servidor autoritativo que é acessado quando a versão em cache não existe ou está desatualizada.

3. Através da execução do comando traceroute seguido dos parâmetros adequados, responda à seguinte questão:

a. Quantos roteadores estão entre a sua estação e o host www.amazon.com? Pelos nomes dos roteadores, quantos deles estão localizados no Brasil?

```
NAOMI$ traceroute www.amazon.com
traceroute to www.amazon.com (13.227.106.126), 30 hops max, 60 byte packets
 1  _gateway (192.168.1.1)  1.434 ms  1.398 ms  1.368 ms
 2  10.80.80.1 (10.80.80.1)  2.605 ms  2.561 ms  2.508 ms
 3  172.16.17.1 (172.16.17.1)  2.937 ms  2.960 ms  2.935 ms
 4  AS-269685.nipbr.com.br (200.220.143.73)  3.412 ms  4.039 ms  4.634 ms
 5  200.220.128.157.nipcable.com (200.220.128.157)  4.238 ms  4.548 ms  4.531 ms
 6  aws-peering.nipbr.com.br (200.220.143.106)  8.324 ms  6.903 ms  6.603 ms
 7  150.222.69.131 (150.222.69.131)  8.788 ms 150.222.69.135 (150.222.69.135)  7
.948 ms 150.222.69.145 (150.222.69.145)  9.471 ms
 8  52.93.146.46 (52.93.146.46)  9.426 ms 54.240.244.135 (54.240.244.135)  7.845
 ms 54.240.244.151 (54.240.244.151)  7.793 ms
 9  * * *
10  52.93.44.20 (52.93.44.20)  7.681 ms 52.93.146.81 (52.93.146.81)  9.191 ms 52
.93.44.102 (52.93.44.102)  8.235 ms
11  150.222.70.53 (150.222.70.53)  8.171 ms 150.222.70.43 (150.222.70.43)  10.65
8 ms  10.597 ms
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  server-13-227-106-126.gru50.r.cloudfront.net (13.227.106.126)  9.171 ms  6.2
93 ms  7.211 ms
```

Existem 17 roteadores entre a minha localização e o host da Amazon. Dos roteadores que possuem nomes, com por exemplo

- AS-269685.nipbr.com.br (200.220.143.73)

- aws-peering.nipbr.com.br (200.220.143.106)

Percebe-se que eles estão no Brasil (.br) e o host do site também, uma vez que

- server-13-227-106-126.gru50.r.cloudfront.net (13.227.106.126)

É parte do serviço Cloud Front da AWS, que é uma solução de Content Delivery Network (ou Rede de Distribuição de Conteúdo) que distribui o conteúdo para áreas geograficamente mais próximas de onde ele é consumido. O GRU50 em particular é localizado em São Paulo [1]. Assim é possível especular que todos os roteadores do 1 (doméstico) ao 17, estão no Brasil. O que justificável, dado que o isso diminui o tempo de acesso ao site para os clientes dentro do país. O "*" indica que a resposta do roteador não chegou em um dado timeout para um probe, no exemplo acima o número de probes era o padrão de 3. Em alguns roteadores percebe-se que todos os 3 probes não foram respondidos.

4. Através da execução do comando telnet, seguido dos parâmetros adequados, responda às seguintes questões:

a. É possível conectar-se com este comando em um servidor HTTP? Se sim, como deve se executar o comando para conectar-se no host www.amazon.com na porta padrão do HTTP?

Com o comando telnet <host> <porta>, como mostrado a seguir, foi possível estabelecer uma conexão TCP com o host na porta 80, convenção para o protocolo HTTP.

```
NAOMI$ telnet www.amazon.com 80
Trying 13.227.106.126...
Connected to d3ag4hukkh62yn.cloudfront.net.
```

b. Caso não haja um servidor escutando na porta passada pelo comando telnet, o que ocorre? Justifique.

Para simular a situação em que não há servidor escutando na porta passada, foi executado o comando telnet <host> <port>, como mostrado a seguir, acessando-se o localhost na porta 80 que no momento não tinha nenhum servidor escutando. A conexão foi recusada:

```
NAOMI$ telnet localhost 80
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
```

c. A qual a camada da rede o telnet pertence?

O telnet é um protocolo pertencente à camada de aplicação [2] ele se apoia no protocolo TCP e proporciona interface de terminais baseada na comunicação orientada à texto. O comando telnet por sua vez implementa o *client side* do protocolo.

5. Acesse o site da DAC (https://www.dac.unicamp.br/) e, em paralelo em um terminal, verifique a saída do comando netstat. Quais são as informações fornecidas a respeito da conexão ao site da DAC?

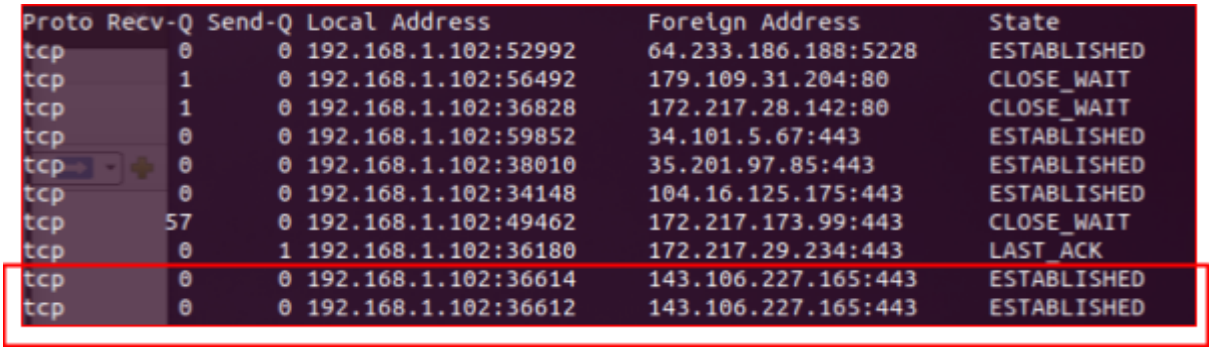
O netstat é uma ferramenta que permite a geração de estatísticas sobre as conexões, em sua saída não são mostrados de forma fácil o nome de um site em específico e respectivo IP. Para conseguir essa informação foi preciso obter o endereço IP com o auxílio de outro comando, no caso o nslookup.

Para obter os endereços de IP:

```
NAOMI$ nslookup www.dac.unicamp.br
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.dac.unicamp.br      canonical name = 143-106-227-165.nuvem.unicamp.br.
Name:   143-106-227-165.nuvem.unicamp.br
Address: 143.106.227.165
```

Com o comando `netstat -na`, obtém-se a saída indicada abaixo;
Neste comando, a flag -a define que todos os sockets devem ser listados (o padrão é somente os ativos), e -n indica que os nomes não devem ser resolvidos (assim podemos obter os endereços IP). A saída indica o protocolo (TCP), o endereço local e a porta sendo utilizada, o endereço do host e o estado da conexão, conforme mostrado na figura a seguir (em destaque as conexões com o site da DAC):



```
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.1.102:52992    64.233.186.188:5228     ESTABLISHED
tcp        1      0 192.168.1.102:56492    179.109.31.204:80       CLOSE_WAIT
tcp        1      0 192.168.1.102:36828    172.217.28.142:80       CLOSE_WAIT
tcp        0      0 192.168.1.102:59852    34.101.5.67:443         ESTABLISHED
tcp        0      0 192.168.1.102:38010    35.201.97.85:443        ESTABLISHED
tcp        0      0 192.168.1.102:34148    104.16.125.175:443      ESTABLISHED
tcp       57      0 192.168.1.102:49462    172.217.173.99:443      CLOSE_WAIT
tcp        0      1 192.168.1.102:36180    172.217.29.234:443      LAST_ACK
tcp        0      0 192.168.1.102:36614    143.106.227.165:443     ESTABLISHED
tcp        0      0 192.168.1.102:36612    143.106.227.165:443     ESTABLISHED
```

6. Considere a ferramenta TCPDUMP, e responda às seguintes questões (precisa de acesso root):

a. Utilizando o TCPDUMP corretamente com os filtros é possível somente capturar o tráfego HTTPS? Se sim, execute o comando junto com os filtros e anexe uma figura que comprove sua resposta no relatório. Se sua resposta foi não, então justifique-a.

Por convenção o tráfego HTTPS usa a porta TCP 443. Então ao filtra o tráfego pelo número da porta com o comando `tcpdump port 443` espera-se também filtrar o tráfego HTTPS. E usando as flags `-nnSX` para tentar visualizar o conteúdo interceptado, observa-se que ele está de fato cifrado.

```
NAOMI$ sudo tcpdump port -nnSX 443
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlp7s0, link-type EN10MB (Ethernet), capture size 262144 bytes
21:59:45.995209 IP 192.168.1.102.55779 > 172.217.30.174.443: UDP, length 1350
        0x0000:  4500 0562 2a33 4000 4011 7dc2 c0a8 0166  E..b*3@.@.}....f
        0x0010:  acd9 1eae d9e3 01bb 054e 92f5 cf51 3035  .........N...Q05
        0x0020:  3008 7cfa ce2b 9d4b e298 0000 4534 d72a  0.|..+.K....E4.*
        0x0030:  02b1 e89b 4716 cb54 426a 1ac6 0a7b 4704  ....G..TBj...{G.
        0x0040:  fa95 758c c70e 80c2 91d8 e5a1 a2a6 781e  ..u...........x.
        0x0050:  4376 f61c 376f e901 6087 64d4 d85b 3e72  Cv..7o..`.d..[>r
        0x0060:  4a03 14c9 88d4 550b b7b4 5f1b b53b 94a4  J.....U..._..;..
        0x0070:  adb1 0bee cbbd b582 551e 8a67 43ea 3d9d  ........U..gC.=.
        0x0080:  2d1b a726 681e e938 5689 98d2 2c9f 5801  -..&h..8V...,.X.
        0x0090:  4212 6e87 f4cf 4b92 5fac 19dc a860 1073  B.n...K._....`.s
        0x00a0:  285a 1482 5e5b dca4 7c44 21e7 27c5 e337  (Z..^[..|D!.'..7
        0x00b0:  c3b8 9d74 a335 74f7 e23a a258 613f 2f68  ...t.5t..:.Xa?/h
        0x00c0:  7531 38da 456b 874e e504 7b71 0642 dfe1  u18.Ek.N..{q.B..
        0x00d0:  9b9a a0d3 7a5c 5bcd 549c 44e9 7619 8069  ....z\[.T.D.v..i
        0x00e0:  8bbd 0a50 b7cc 9f41 7816 3bf2 e300 2ff9  ...P...Ax.;.../.
        0x00f0:  9ee9 0a61 97d9 cbe3 b0e2 70b9 e2b1 f232  ...a......p....2
        0x0100:  501b ad92 7918 385f b4d6 0041 c786 3e49  P...y.8_...A..>I
        0x0110:  9582 9251 b19a cade 208d 37ac 0d56 215b  ...Q...... 7..V![
        0x0120:  f06d 7ed8 7779 c5a7 2cb4 32ab f8b5 9842  .m~.wy..,.2....B
        0x0130:  baad 5063 1a67 7359 db28 dbb9 432f e4a3  ..Pc.gsY.(..C/..
        0x0140:  e463 9f89 8aec 6bd4 8cc9 f4b5 d21b 04c2  .c....k.........
        0x0150:  e757 262c e22d e3c2 bb57 eaba 2aaa d7a6  .W&,.-...W..*...
        0x0160:  17bb b881 f7b4 6589 a092 cc02 47cd 4b2d  ......e.....G.K-
        0x0170:  5b77 5ca6 5eab 691a 8d80 b133 2b37 fdf4  [w\.^.i....3+7..
        0x0180:  10cc b31f e19c 2fc8 3e8c 50b8 8d1c c8b7  ....../.>.P.....
        0x0190:  12ca 6ce7 e0f7 a11e 7200 4a0d d6d1 4c04  ..l.....r.J...L.
        0x01a0:  adaa 88bf 3b8d c19a 0951 25fe 1d20 7581  ....;....Q%...u.
        0x01b0:  4021 d146 8d6f 1b73 9b80 251b 999f 84ad  @!.F.o.s..%.....
```

Utilizando o comando `sudo tcpdump host -nnSX 177.184.0.239` onde o enderço IP apresentado é do site http://www.cesgranrio.org.br/, que usa o protocolo HTTP, percebe-se que a conexão não é cifrada, sendo possível ler vários termos. Ver figura abaixo:

```
naomi@naomi-Nitro-AN515-54:~$ sudo tcpdump host -nnSX 177.184.0.239
[sudo] password for naomi:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlp7s0, link-type EN10MB (Ethernet), capture size 262144 bytes
22:05:12.407885 IP 192.168.1.102.56004 > 177.184.0.239.80: Flags [F.], seq 3133166913, ack 3298908657
, win 502, options [nop,nop,TS val 1618370255 ecr 2895714647], length 0
        0x0000:  4500 0034 c38b 4000 4006 0283 c0a8 0166  E..4..@.@......f
        0x0010:  b1b8 00ef dac4 0050 bac0 5541 c4a1 59f1  .......P..UA..Y.
        0x0020:  8011 01f6 74dc 0000 0101 080a 6076 5ecf  ....t.......`v^.
        0x0030:  ac99 1957                                ...W
22:05:12.408135 IP 192.168.1.102.56006 > 177.184.0.239.80: Flags [P.], seq 254815371:254816036, ack 3
02809534, win 1371, options [nop,nop,TS val 1618370255 ecr 2895714933], length 665: HTTP: GET /imagen
s/internas01_mobile.jpg HTTP/1.1
        0x0000:  4500 02cd ec7b 4000 4006 d6f9 c0a8 0166  E....{@.@......f
        0x0010:  b1b8 00ef dac6 0050 0f30 2c8b 120c 81be  .......P.0,.....
        0x0020:  8018 055b 7775 0000 0101 080a 6076 5ecf  ...[wu......`v^.
        0x0030:  ac99 1a75 4745 5420 2f69 6d61 6765 6e73  ...uGET./imagens
        0x0040:  2f69 6e74 6572 6e61 7330 315f 6d6f 6269  /internas01_mobi
        0x0050:  6c65 2e6a 7067 2048 5454 502f 312e 310d  le.jpg.HTTP/1.1.
        0x0060:  0a48 6f73 743a 2077 7777 2e63 6573 6772  .Host:.www.cesgr
        0x0070:  616e 7269 6f2e 6f72 672e 6272 0d0a 436f  anrio.org.br..Co
        0x0080:  6e6e 6563 7469 6f6e 3a20 6b65 6570 2d61  nnection:.keep-a
        0x0090:  6c69 7665 0d0a 5573 6572 2d41 6765 6e74  live..User-Agent
        0x00a0:  3a20 4d6f 7a69 6c6c 612f 352e 3020 2858  :.Mozilla/5.0.(X
        0x00b0:  3131 3b20 4c69 6e75 7820 7838 365f 3634  11;.Linux.x86_64
        0x00c0:  2920 4170 706c 6557 6562 4b69 742f 3533  ).AppleWebKit/53
        0x00d0:  372e 3336 2028 4b48 544d 4c2c 206c 696b  7.36.(KHTML,.lik
        0x00e0:  6520 4765 636b 6f29 2043 6872 6f6d 652f  e.Gecko).Chrome/
        0x00f0:  3835 2e30 2e34 3138 332e 3132 3120 5361  85.0.4183.121.Sa
        0x0100:  6661 7269 2f35 3337 2e33 360d 0a41 6363  fari/537.36..Acc
        0x0110:  6570 743a 2069 6d61 6765 2f61 7669 662c  ept:.image/avif,
        0x0120:  696d 6167 652f 7765 6270 2c69 6d61 6765  image/webp,image
        0x0130:  2f61 706e 672c 696d 6167 652f 2a2c 2a2f  /apng,image/*,*/
        0x0140:  2a3b 713d 302e 380d 0a52 6566 6572 6572  *;q=0.8..Referer
        0x0150:  3a20 6874 7470 3a2f 2f77 7777 2e63 6573  :.http://www.ces
```

b. Utilizando o comando TCPDUMP seguido dos parâmetros corretos imprima somente os pacotes superiores a 64 bits. Indique qual foi a sequência de comandos utilizada.

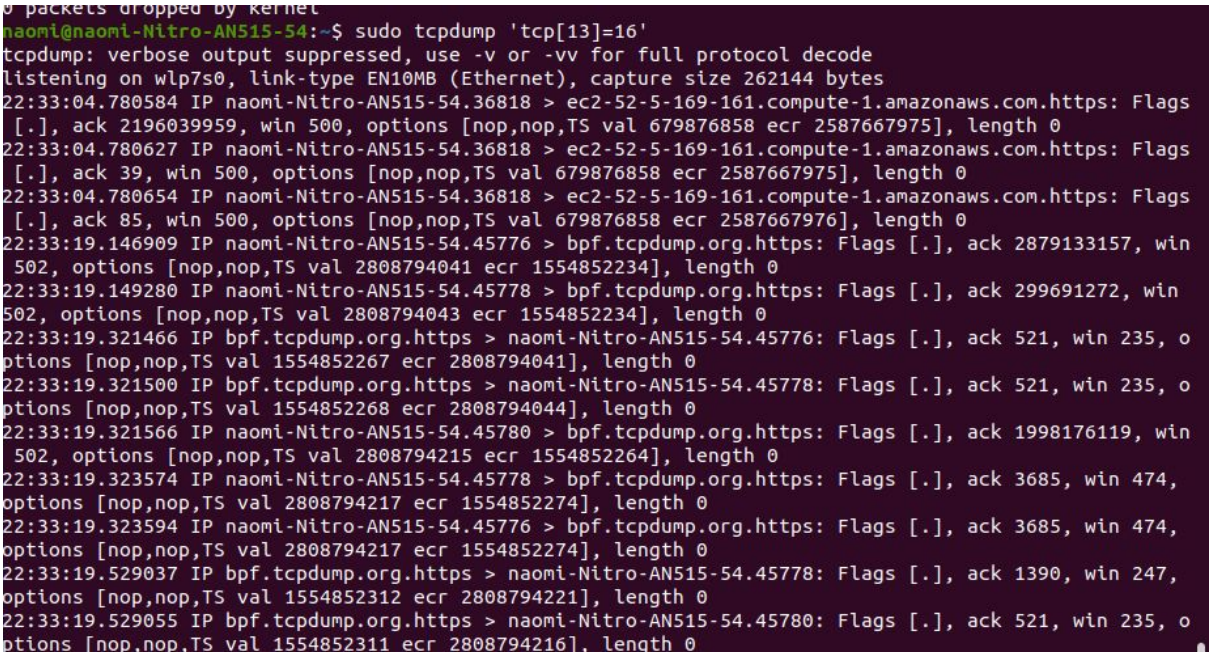
Foi utilizado o comando `sudo tcpdump greater 8` o número 8 é o número de bytes equivalente a 64 bits.

```
NAOMI$ sudo tcpdump greater 8
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlp7s0, link-type EN10MB (Ethernet), capture size 262144 bytes
22:19:23.935186 IP 192.168.1.105.2008 > 192.168.1.255.2008: UDP, length 20
22:19:23.935753 IP naomi-Nitro-AN515-54.47417 > _gateway.domain: 61755+ [1au] PTR? 255.1.168.192.in-a
ddr.arpa. (55)
22:19:23.936300 IP 192.168.1.105.2007 > 192.168.1.255.2007: UDP, length 20
22:19:23.944977 IP _gateway.domain > naomi-Nitro-AN515-54.47417: 61755 NXDomain* 0/1/1 (114)
22:19:23.945097 IP naomi-Nitro-AN515-54.47417 > _gateway.domain: 61755+ PTR? 255.1.168.192.in-addr.ar
pa. (44)
22:19:23.948743 IP _gateway.domain > naomi-Nitro-AN515-54.47417: 61755 NXDomain* 0/1/1 (114)
22:19:23.949185 IP naomi-Nitro-AN515-54.35551 > _gateway.domain: 43428+ [1au] PTR? 105.1.168.192.in-a
ddr.arpa. (55)
22:19:23.950560 IP _gateway.domain > naomi-Nitro-AN515-54.47417: 61755 NXDomain* 0/1/0 (103)
22:19:23.950570 IP naomi-Nitro-AN515-54 > _gateway: ICMP naomi-Nitro-AN515-54 udp port 47417 unreacha
ble, length 139
22:19:23.951445 IP _gateway.domain > naomi-Nitro-AN515-54.35551: 43428 NXDomain* 0/1/1 (114)
22:19:23.951550 IP naomi-Nitro-AN515-54.35551 > _gateway.domain: 43428+ PTR? 105.1.168.192.in-addr.ar
pa. (44)
```

c. Utilizando o TCPDUMP seguido de filtros, imprima somente os resultados que tiverem a flag ‘ACK’. Insira o comando seguido dos filtros e uma figura no seu relatório para
comprovar o sucesso.

`sudo tcpdump 'tcp[13]=16'`

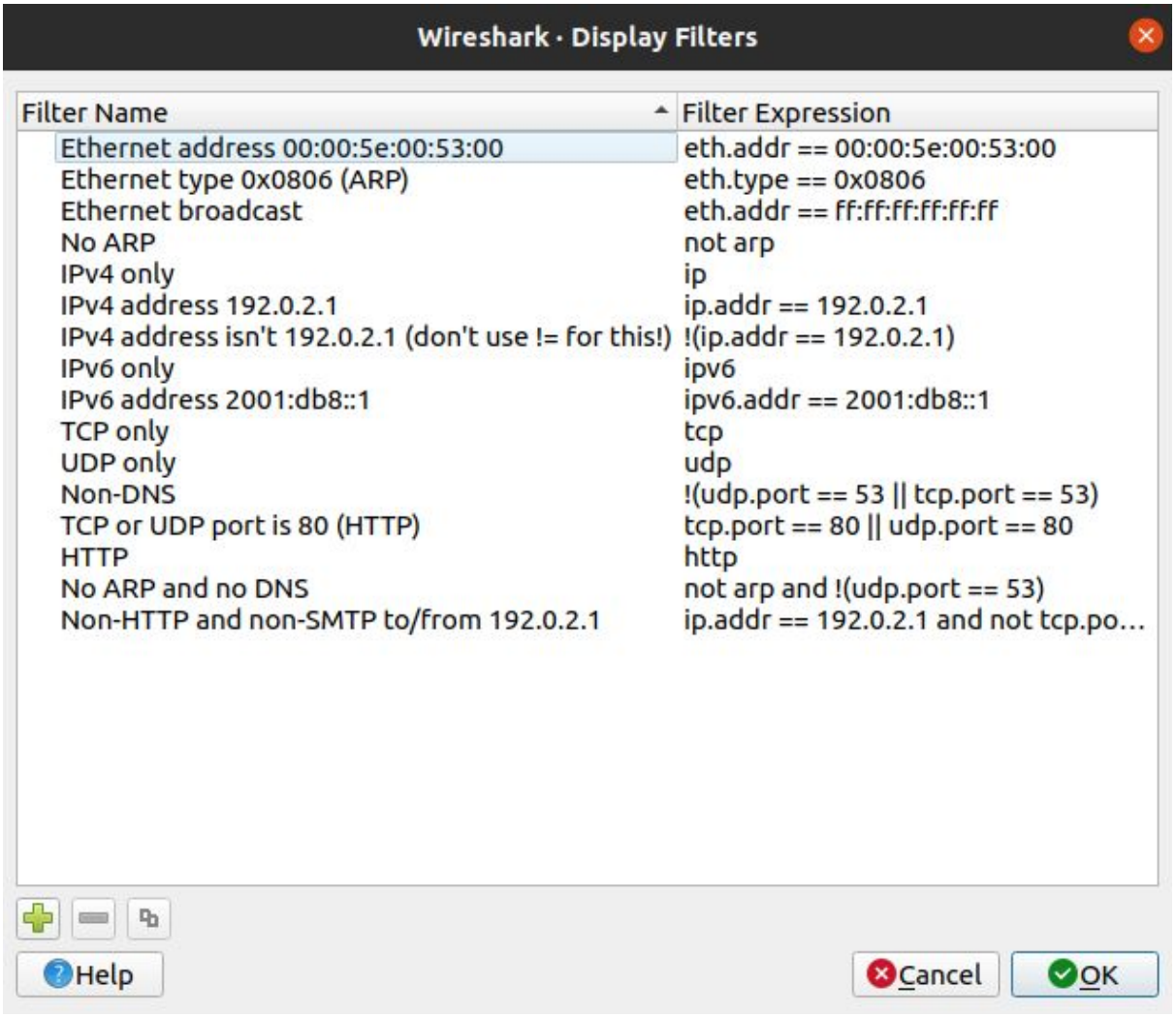
No octeto 13 do header tcp, é avaliado se o bit de eeACK está setado (valor 16).



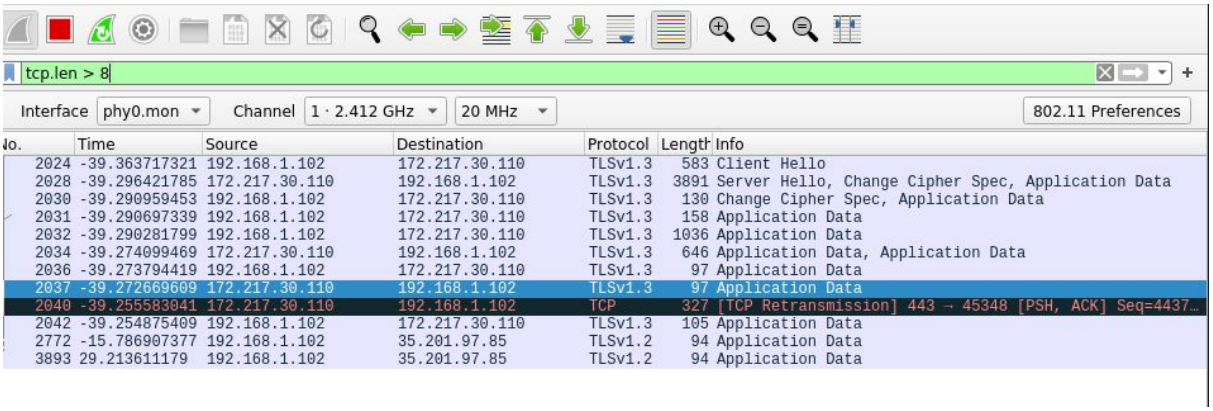
7. Considere a ferramenta Wireshark para responder às questões a seguir: (pergunta teórica)

a. Comparado às demais ferramentas apresentadas na aula de MC833 descreva quais são principais diferenças e vantagens de usar o Wireshark? Escolha pelo menos uma ferramenta/sniffer e elabore uma tabela comparativa para responder a questão.

Em comparação com o TCPDump, o Wireshark apresenta uma interface mais intuitiva, sendo mais fácil localizar e utilizar filtros mais comuns como os listados abaixo:



Usando os filtros é possível filtrar facilmente os pacotes, no exemplo a seguir filtra-se por tamanho de pacote para o protocolo tcp. A inserção deste filtro é bastantes mais intuitiva que a do TCPDump feita em um exercício anterior. Sendo fácil também escolher que tipo de tráfego será visualizado, escolhendo por exemplo WiFi, Bluetooth, etc.



Além do uso de filtros, no Wireshark é possível gravar em arquivo o que foi interceptado usando os recursos da interface gráfica (botões em destaque na figura acima).

b. Com o conhecimento adquirido sobre ferramentas e sniffers responda:

i. Em uma rede com vários processos acontecendo ao mesmo tempo é possível gerenciar de forma isolada um único processo específico na rede utilizando ferramentas/sniffers apresentados nesta disciplina? Se sim, quais ferramentas e/ou sniffers você usaria? Justifique sua resposta. (OBS: Não é necessário apresentar comandos ou prints)

Os sniffers vistos não fornecem uma maneira fácil de encontrar o PID dos processos, uma vez que eles apenas capturam pacotes que podem vir de qualquer máquina conectada à rede sendo analisada. Para que seja possível capturar informações relativas a um processo em específico é preciso combinar os *sniffers* com o netstat por exemplo, ou alguma outra ferramenta do sistema operacional que relaciona o PID de um processo ao par endereço IP:porta que o processo escuta. Assim, com algum sniffer pode-se definir filtros mais específicos (ex IP: porta) para selecionar os pacotes relativos ao processo em questão.

Referências

[1] Amazon Cloud Front. Disponível em: https://www.gocache.com.br/cdn/o-que-e-cloudfront-da-amazon/. Acesso em 6 de outubro de 2020.

[2] Telnet. Disponível em: https://en.wikipedia.org/wiki/Telnet. Acesso em 6 de outubro de 2020.