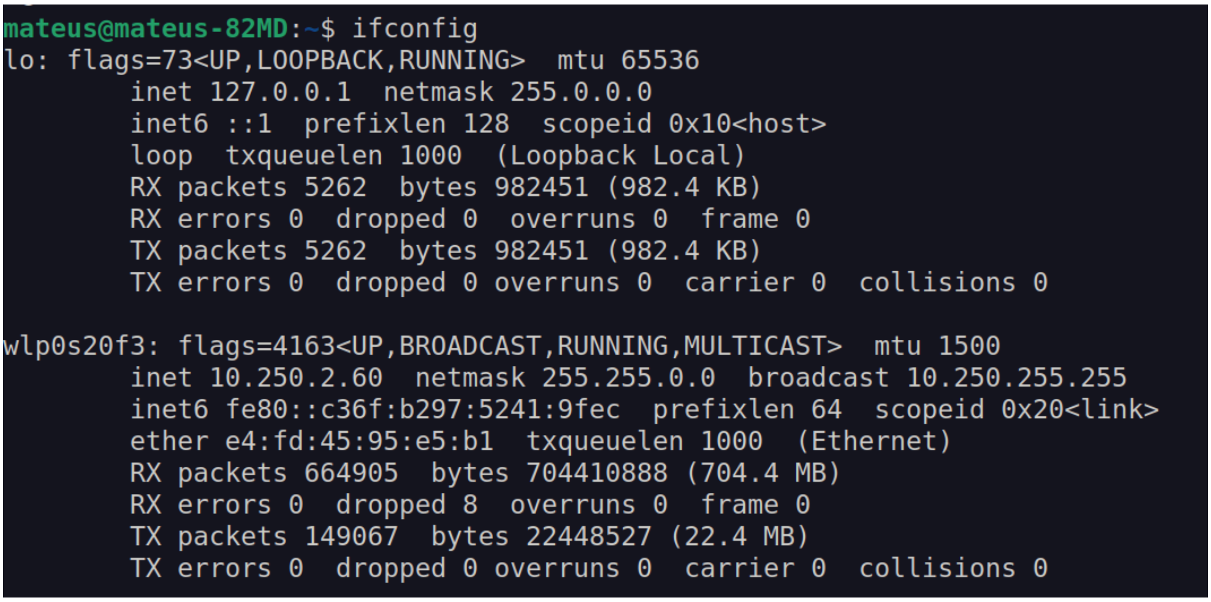
Atividade Avaliativa Wireshark
Data: 26/02/2025

Integrantes do Grupo: Mateus Fernandes Barbosa, Rafael Fleury Barcellos Ceolin de Oliveira, Victor Ferraz de Moraes

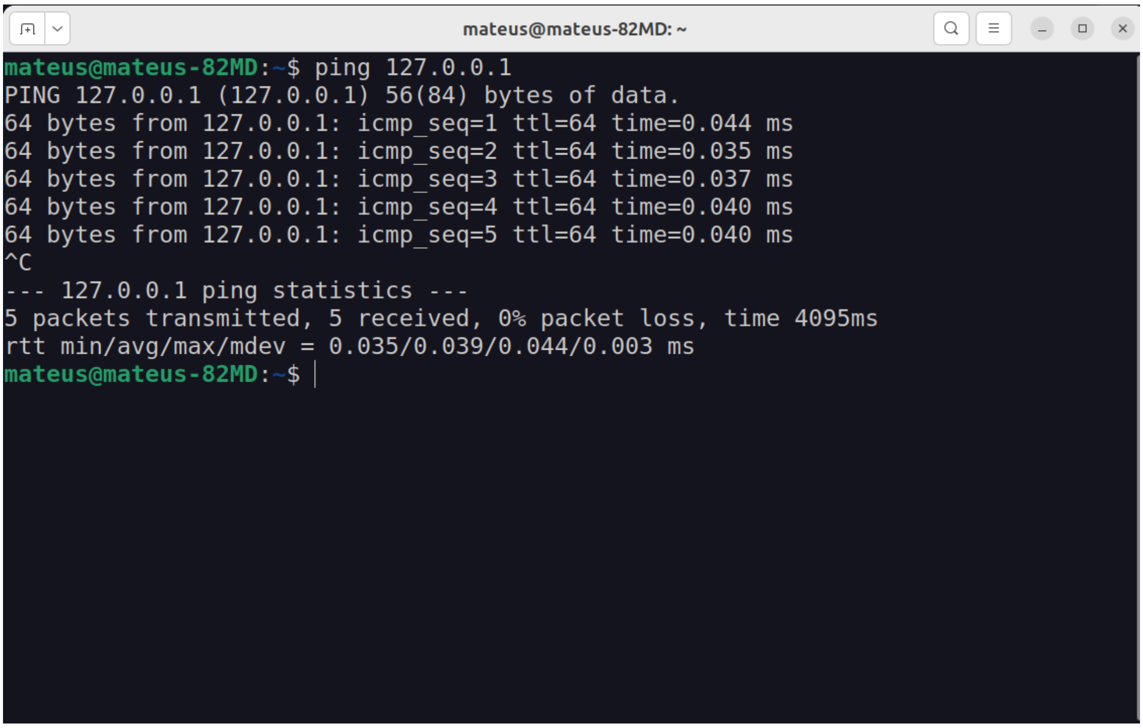
Ex(1):



```
mateus@mateus-82MD:~$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Loopback Local)
        RX packets 5262  bytes 982451 (982.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5262  bytes 982451 (982.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.250.2.60  netmask 255.255.0.0  broadcast 10.250.255.255
        inet6 fe80::c36f:b297:5241:9fec  prefixlen 64  scopeid 0x20<link>
        ether e4:fd:45:95:e5:b1  txqueuelen 1000  (Ethernet)
        RX packets 664905  bytes 704410888 (704.4 MB)
        RX errors 0  dropped 8  overruns 0  frame 0
        TX packets 149067  bytes 22448527 (22.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

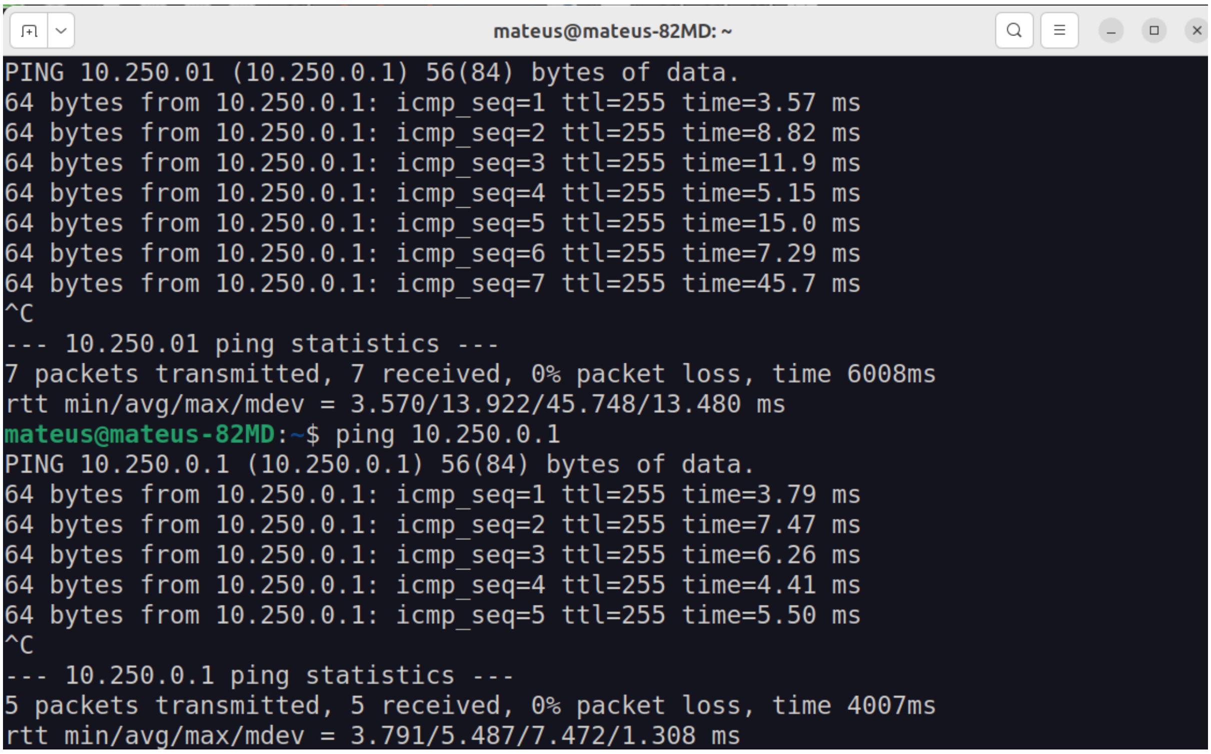
Ex(1.5):

Ping do LocalHost



```
mateus@mateus-82MD:~$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.044 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.035 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.037 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.040 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.040 ms
^C
--- 127.0.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4095ms
rtt min/avg/max/mdev = 0.035/0.039/0.044/0.003 ms
mateus@mateus-82MD:~$ 
```

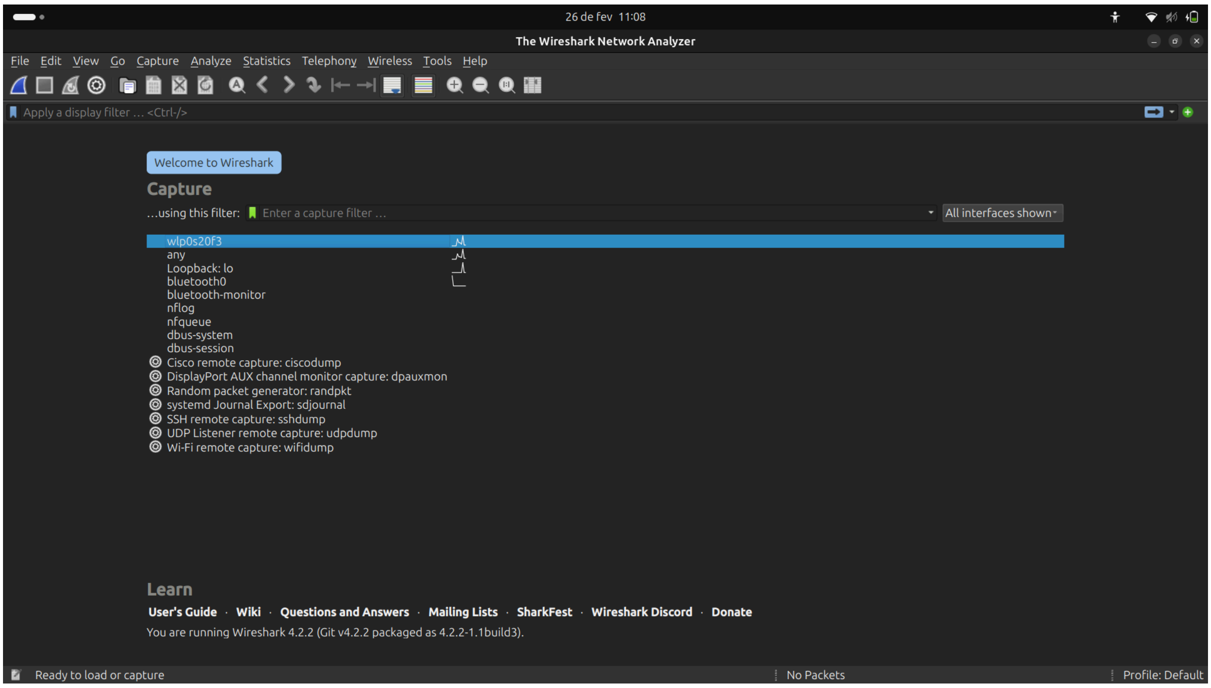
Ping no roteador local:



mateus@mateus-82MD: ~

```
PING 10.250.01 (10.250.0.1) 56(84) bytes of data.
64 bytes from 10.250.0.1: icmp_seq=1 ttl=255 time=3.57 ms
64 bytes from 10.250.0.1: icmp_seq=2 ttl=255 time=8.82 ms
64 bytes from 10.250.0.1: icmp_seq=3 ttl=255 time=11.9 ms
64 bytes from 10.250.0.1: icmp_seq=4 ttl=255 time=5.15 ms
64 bytes from 10.250.0.1: icmp_seq=5 ttl=255 time=15.0 ms
64 bytes from 10.250.0.1: icmp_seq=6 ttl=255 time=7.29 ms
64 bytes from 10.250.0.1: icmp_seq=7 ttl=255 time=45.7 ms
^C
--- 10.250.01 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 3.570/13.922/45.748/13.480 ms
mateus@mateus-82MD:~$ ping 10.250.0.1
PING 10.250.0.1 (10.250.0.1) 56(84) bytes of data.
64 bytes from 10.250.0.1: icmp_seq=1 ttl=255 time=3.79 ms
64 bytes from 10.250.0.1: icmp_seq=2 ttl=255 time=7.47 ms
64 bytes from 10.250.0.1: icmp_seq=3 ttl=255 time=6.26 ms
64 bytes from 10.250.0.1: icmp_seq=4 ttl=255 time=4.41 ms
64 bytes from 10.250.0.1: icmp_seq=5 ttl=255 time=5.50 ms
^C
--- 10.250.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 3.791/5.487/7.472/1.308 ms
```

Ex(2):



26 de fev 11:08
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark

Capture

…using this filter: Enter a capture filter … All interfaces shown

wlp0s20f3
any
Loopback: lo
bluetooth0
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump

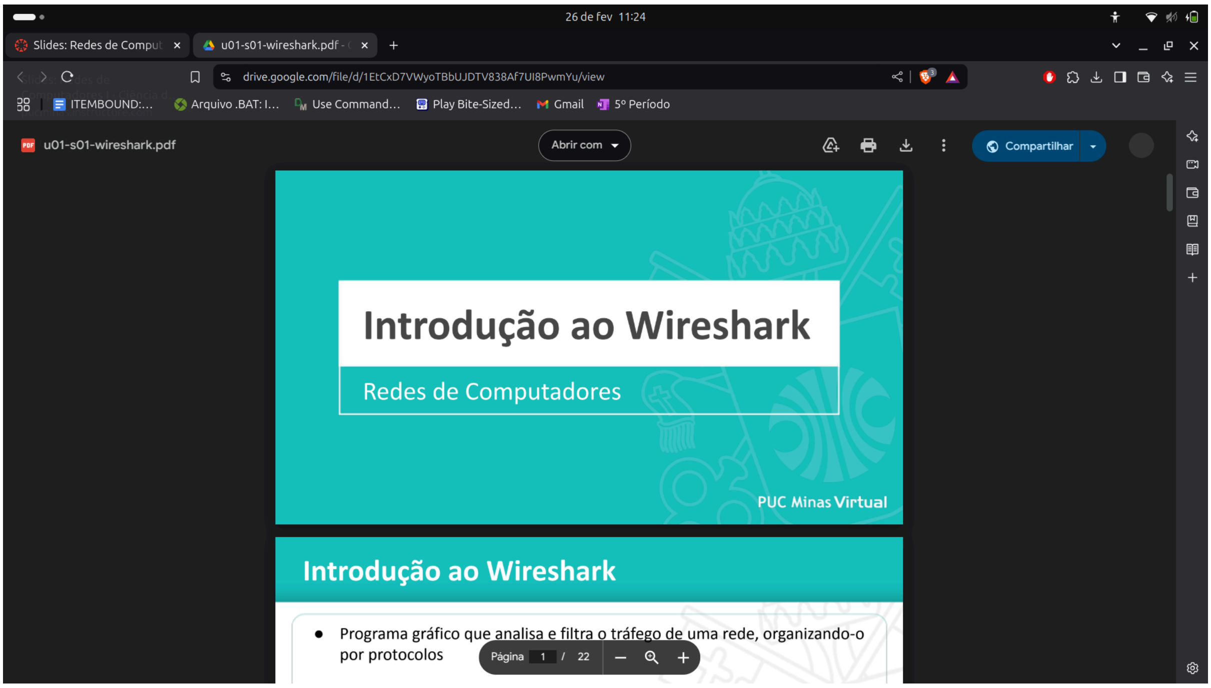
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.2.2 (Git v4.2.2 packaged as 4.2.2-1.1build3).

Ready to load or capture | No Packets | Profile: Default

Ex(3):



Introdução ao Wireshark

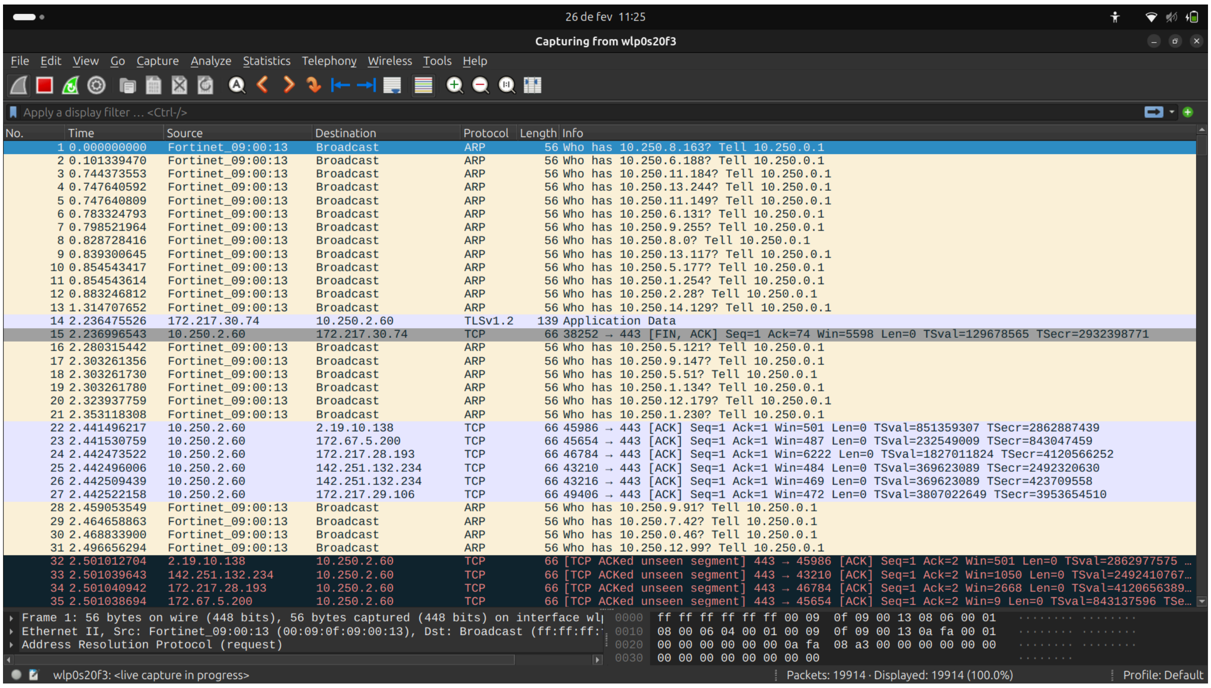
Redes de Computadores

PUC Minas Virtual

Introdução ao Wireshark

- Programa gráfico que analisa e filtra o tráfego de uma rede, organizando-o por protocolos

Ex(4):



26 de fev 11:25
Capturing from wlp0s20f3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time          Source              Destination      Protocol  Length Info
    1 0.000000000   Fortinet_09:00:13   Broadcast        ARP        56 Who has 10.250.8.163? Tell 10.250.0.1
    2 0.101339470   Fortinet_09:00:13   Broadcast        ARP        56 Who has 10.250.6.188? Tell 10.250.0.1
    3 0.744373553   Fortinet_09:00:13   Broadcast        ARP        56 Who has 10.250.11.184? Tell 10.250.0.1
    4 0.747640592   Fortinet_09:00:13   Broadcast        ARP        56 Who has 10.250.13.244? Tell 10.250.0.1
    5 0.747640809   Fortinet_09:00:13   Broadcast        ARP        56 Who has 10.250.11.149? Tell 10.250.0.1
    6 0.783324793   Fortinet_09:00:13   Broadcast        ARP        56 Who has 10.250.6.131? Tell 10.250.0.1
    7 0.798521964   Fortinet_09:00:13   Broadcast        ARP        56 Who has 10.250.9.255? Tell 10.250.0.1
    8 0.828728416   Fortinet_09:00:13   Broadcast        ARP        56 Who has 10.250.8.0? Tell 10.250.0.1
    9 0.839300645   Fortinet_09:00:13   Broadcast        ARP        56 Who has 10.250.13.117? Tell 10.250.0.1
   10 0.854543417   Fortinet_09:00:13   Broadcast        ARP        56 Who has 10.250.5.177? Tell 10.250.0.1
   11 0.854543614   Fortinet_09:00:13   Broadcast        ARP        56 Who has 10.250.1.254? Tell 10.250.0.1
   12 0.883246812   Fortinet_09:00:13   Broadcast        ARP        56 Who has 10.250.2.28? Tell 10.250.0.1
   13 1.314707652   Fortinet_09:00:13   Broadcast        ARP        56 Who has 10.250.14.129? Tell 10.250.0.1
   14 2.236475526   172.217.30.74       10.250.2.60      TLSv1.2   139 Application Data
   15 2.236996543   10.250.2.60         172.217.30.74    TCP        66 38252 → 443 [FIN, ACK] Seq=1 Ack=74 Win=5598 Len=0 TSval=129678565 TSecr=2932398771
   16 2.280315442   Fortinet_09:00:13   Broadcast        ARP        56 Who has 10.250.5.121? Tell 10.250.0.1
   17 2.303261356   Fortinet_09:00:13   Broadcast        ARP        56 Who has 10.250.9.147? Tell 10.250.0.1
   18 2.303261730   Fortinet_09:00:13   Broadcast        ARP        56 Who has 10.250.5.51? Tell 10.250.0.1
   19 2.303261780   Fortinet_09:00:13   Broadcast        ARP        56 Who has 10.250.1.134? Tell 10.250.0.1
   20 2.323937759   Fortinet_09:00:13   Broadcast        ARP        56 Who has 10.250.12.179? Tell 10.250.0.1
   21 2.353118308   Fortinet_09:00:13   Broadcast        ARP        56 Who has 10.250.1.230? Tell 10.250.0.1
   22 2.441496217   10.250.2.60         2.19.10.138      TCP        66 45986 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=851359307 TSecr=2862887439
   23 2.441530759   10.250.2.60         172.67.5.200     TCP        66 45654 → 443 [ACK] Seq=1 Ack=1 Win=487 Len=0 TSval=232549009 TSecr=843047459
   24 2.442473522   10.250.2.60         172.217.28.193   TCP        66 46784 → 443 [ACK] Seq=1 Ack=1 Win=6222 Len=0 TSval=1827011824 TSecr=4120566252
   25 2.442496006   10.250.2.60         142.251.132.234  TCP        66 43210 → 443 [ACK] Seq=1 Ack=1 Win=484 Len=0 TSval=369623089 TSecr=2492320630
   26 2.442509439   10.250.2.60         142.251.132.234  TCP        66 43216 → 443 [ACK] Seq=1 Ack=1 Win=469 Len=0 TSval=369623089 TSecr=423709558
   27 2.442522158   10.250.2.60         172.217.29.106   TCP        66 49406 → 443 [ACK] Seq=1 Ack=1 Win=472 Len=0 TSval=3807022649 TSecr=3953654510
   28 2.459053549   Fortinet_09:00:13   Broadcast        ARP        56 Who has 10.250.9.91? Tell 10.250.0.1
   29 2.464658863   Fortinet_09:00:13   Broadcast        ARP        56 Who has 10.250.7.42? Tell 10.250.0.1
   30 2.468833900   Fortinet_09:00:13   Broadcast        ARP        56 Who has 10.250.0.46? Tell 10.250.0.1
   31 2.496656294   Fortinet_09:00:13   Broadcast        ARP        56 Who has 10.250.12.99? Tell 10.250.0.1
   32 2.501012704   2.19.10.138         10.250.2.60      TCP        66 [TCP ACKed unseen segment] 443 → 45986 [ACK] Seq=1 Ack=2 Win=501 Len=0 TSval=2862977575 …
   33 2.501039643   142.251.132.234     10.250.2.60      TCP        66 [TCP ACKed unseen segment] 443 → 43210 [ACK] Seq=1 Ack=2 Win=1050 Len=0 TSval=2492410767…
   34 2.501040942   172.217.28.193      10.250.2.60      TCP        66 [TCP ACKed unseen segment] 443 → 46784 [ACK] Seq=1 Ack=2 Win=2668 Len=0 TSval=4120656389…
   35 2.501038694   172.67.5.200        10.250.2.60      TCP        66 [TCP ACKed unseen segment] 443 → 45654 [ACK] Seq=1 Ack=2 Win=9 Len=0 TSval=843137596 TSe…
```

```
› Frame 1: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface wl
› Ethernet II, Src: Fortinet_09:00:13 (00:09:0f:09:00:13), Dst: Broadcast (ff:ff:ff:
› Address Resolution Protocol (request)
```

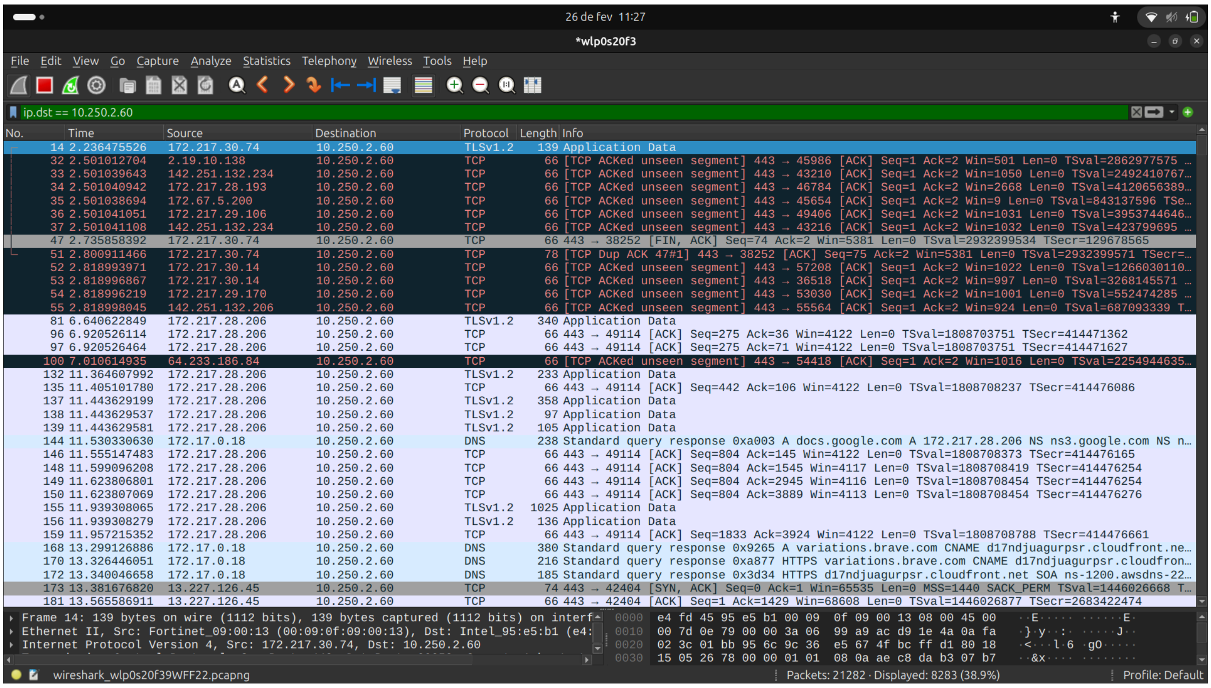
```
0000  ff ff ff ff ff ff 00 09  0f 09 00 13 08 06 00 01   ········ ········
0010  08 00 06 04 00 01 00 09  0f 09 00 13 0a fa 00 01   ········ ········
0020  00 00 00 00 00 00 0a fa  08 a3 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00                            ········
```

wlp0s20f3: <live capture in progress>

Packets: 19914 · Displayed: 19914 (100.0%)

Profile: Default

Ex(5):



```
ip.dst == 10.250.2.60
```

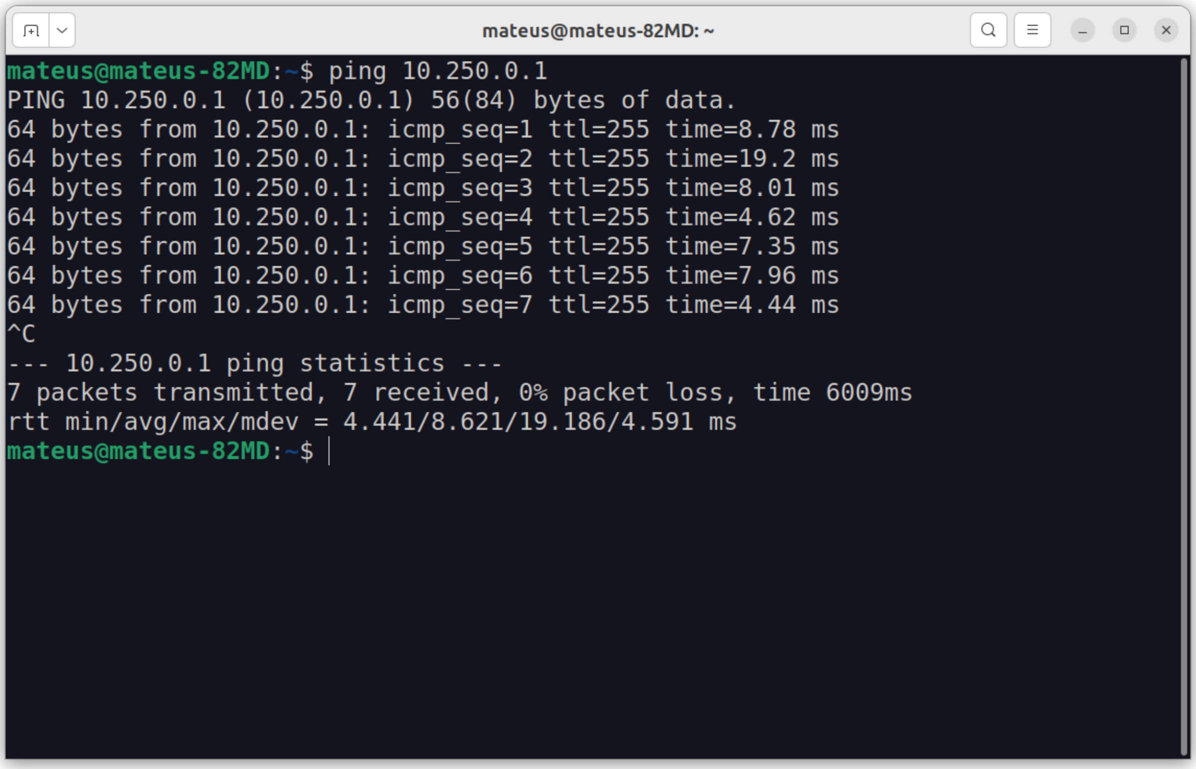
```
No.  Time          Source           Destination  Protocol Length Info
  14 2.236475526   172.217.30.74    10.250.2.60  TLSv1.2   139 Application Data
  32 2.501012704   2.19.10.138      10.250.2.60  TCP        66 [TCP ACKed unseen segment] 443 → 45986 [ACK] Seq=1 Ack=2 Win=501 Len=0 TSval=2862977575 …
  33 2.501039643   142.251.132.234  10.250.2.60  TCP        66 [TCP ACKed unseen segment] 443 → 43210 [ACK] Seq=1 Ack=2 Win=1050 Len=0 TSval=2492410767…
  34 2.501040942   172.217.28.193   10.250.2.60  TCP        66 [TCP ACKed unseen segment] 443 → 46784 [ACK] Seq=1 Ack=2 Win=2668 Len=0 TSval=4120656389…
  35 2.501038694   172.67.5.200     10.250.2.60  TCP        66 [TCP ACKed unseen segment] 443 → 45654 [ACK] Seq=1 Ack=2 Win=9 Len=0 TSval=843137596 TSe…
  36 2.501041051   172.217.29.106   10.250.2.60  TCP        66 [TCP ACKed unseen segment] 443 → 49406 [ACK] Seq=1 Ack=2 Win=1031 Len=0 TSval=3953744646…
  37 2.501041108   142.251.132.234  10.250.2.60  TCP        66 [TCP ACKed unseen segment] 443 → 43216 [ACK] Seq=1 Ack=2 Win=1032 Len=0 TSval=423799695 …
  47 2.735858392   172.217.30.74    10.250.2.60  TCP        66 443 → 38252 [FIN, ACK] Seq=74 Ack=2 Win=5381 Len=0 TSval=2932399534 TSecr=129678565
  51 2.800911466   172.217.30.74    10.250.2.60  TCP        78 [TCP Dup ACK 47#1] 443 → 38252 [ACK] Seq=75 Ack=2 Win=5381 Len=0 TSval=2932399571 TSecr=…
  52 2.818993971   172.217.30.14    10.250.2.60  TCP        66 [TCP ACKed unseen segment] 443 → 57208 [ACK] Seq=1 Ack=2 Win=1022 Len=0 TSval=1266030110…
  53 2.818996867   172.217.30.14    10.250.2.60  TCP        66 [TCP ACKed unseen segment] 443 → 36518 [ACK] Seq=1 Ack=2 Win=997 Len=0 TSval=3268145571 …
  54 2.818996219   172.217.29.170   10.250.2.60  TCP        66 [TCP ACKed unseen segment] 443 → 53030 [ACK] Seq=1 Ack=2 Win=1001 Len=0 TSval=552474285 …
  55 2.818998045   142.251.132.206  10.250.2.60  TCP        66 [TCP ACKed unseen segment] 443 → 55564 [ACK] Seq=1 Ack=2 Win=924 Len=0 TSval=687093339 T…
  81 6.640622849   172.217.28.206   10.250.2.60  TLSv1.2   340 Application Data
  96 6.920526114   172.217.28.206   10.250.2.60  TCP        66 443 → 49114 [ACK] Seq=275 Ack=36 Win=4122 Len=0 TSval=1808703751 TSecr=414471362
  97 6.920526464   172.217.28.206   10.250.2.60  TCP        66 443 → 49114 [ACK] Seq=275 Ack=71 Win=4122 Len=0 TSval=1808703751 TSecr=414471627
 100 7.010614935   64.233.186.84    10.250.2.60  TCP        66 [TCP ACKed unseen segment] 443 → 54418 [ACK] Seq=1 Ack=2 Win=1016 Len=0 TSval=2254944635…
 132 11.364607992  172.217.28.206   10.250.2.60  TLSv1.2   233 Application Data
 135 11.405101780  172.217.28.206   10.250.2.60  TCP        66 443 → 49114 [ACK] Seq=442 Ack=106 Win=4122 Len=0 TSval=1808708237 TSecr=414476086
 137 11.443629199  172.217.28.206   10.250.2.60  TLSv1.2   358 Application Data
 138 11.443629537  172.217.28.206   10.250.2.60  TLSv1.2    97 Application Data
 139 11.443629581  172.217.28.206   10.250.2.60  TLSv1.2   105 Application Data
 144 11.530330630  172.17.0.18      10.250.2.60  DNS       238 Standard query response 0xa003 A docs.google.com A 172.217.28.206 NS ns3.google.com NS n…
 146 11.555147483  172.217.28.206   10.250.2.60  TCP        66 443 → 49114 [ACK] Seq=804 Ack=145 Win=4122 Len=0 TSval=1808708373 TSecr=414476165
 148 11.599096208  172.217.28.206   10.250.2.60  TCP        66 443 → 49114 [ACK] Seq=804 Ack=1545 Win=4117 Len=0 TSval=1808708419 TSecr=414476254
 149 11.623806801  172.217.28.206   10.250.2.60  TCP        66 443 → 49114 [ACK] Seq=804 Ack=2945 Win=4116 Len=0 TSval=1808708454 TSecr=414476254
 150 11.623807069  172.217.28.206   10.250.2.60  TCP        66 443 → 49114 [ACK] Seq=804 Ack=3889 Win=4113 Len=0 TSval=1808708454 TSecr=414476276
 155 11.939308065  172.217.28.206   10.250.2.60  TLSv1.2  1025 Application Data
 156 11.939308279  172.217.28.206   10.250.2.60  TLSv1.2   136 Application Data
 159 11.957215352  172.217.28.206   10.250.2.60  TCP        66 443 → 49114 [ACK] Seq=1833 Ack=3924 Win=4122 Len=0 TSval=1808708788 TSecr=414476661
 168 13.299126886  172.17.0.18      10.250.2.60  DNS       380 Standard query response 0x9265 A variations.brave.com CNAME d17ndjuagurpsr.cloudfront.ne…
 170 13.326446051  172.17.0.18      10.250.2.60  DNS       216 Standard query response 0xa877 HTTPS variations.brave.com CNAME d17ndjuagurpsr.cloudfron…
 172 13.340046658  172.17.0.18      10.250.2.60  DNS       185 Standard query response 0x3d34 HTTPS d17ndjuagurpsr.cloudfront.net SOA ns-1200.awsdns-22…
 173 13.381676820  13.227.126.45    10.250.2.60  TCP        74 443 → 42404 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 SACK_PERM TSval=1446026668 T…
 181 13.565586911  13.227.126.45    10.250.2.60  TCP        66 443 → 42404 [ACK] Seq=1 Ack=1429 Win=68608 Len=0 TSval=1446026877 TSecr=2683422474
```

```
▸ Frame 14: 139 bytes on wire (1112 bits), 139 bytes captured (1112 bits) on interf
▸ Ethernet II, Src: Fortinet_09:00:13 (00:09:0f:09:00:13), Dst: Intel_95:e5:b1 (e4:
▸ Internet Protocol Version 4, Src: 172.217.30.74, Dst: 10.250.2.60
```

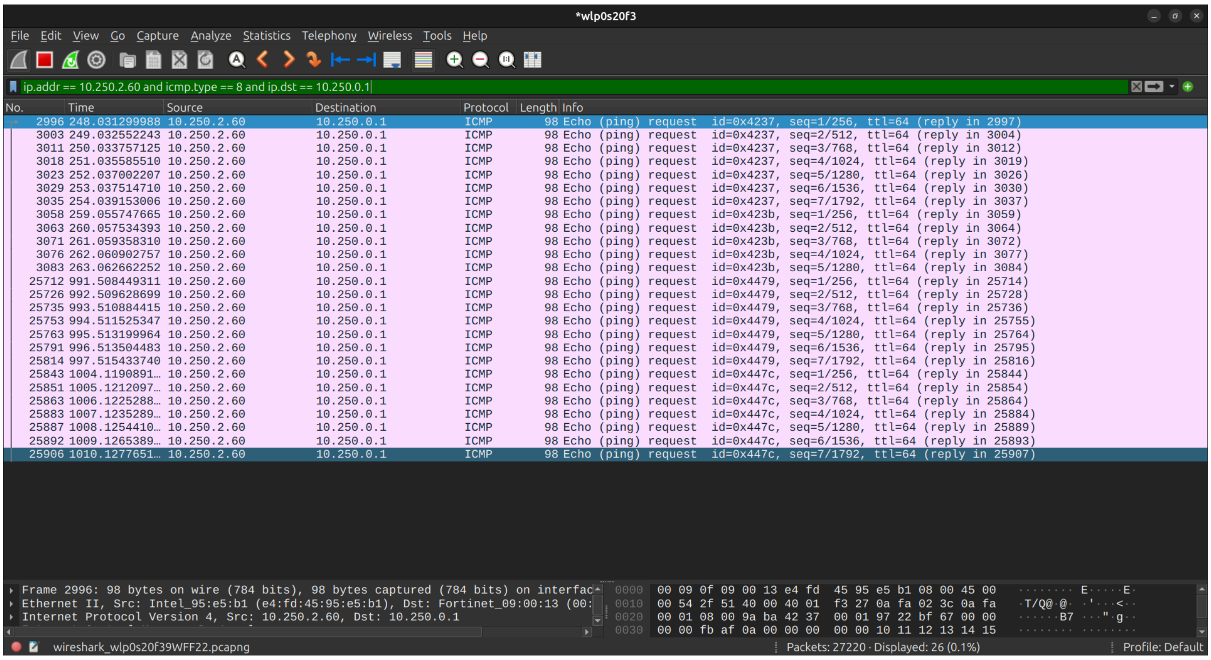
```
0000  e4 fd 45 95 e5 b1 00 09  0f 09 00 13 08 00 45 00   ··E·····  ······E·
0010  00 7d 0e 79 00 00 3a 06  99 a9 ac d9 1e 4a 0a fa   ·}·y··:·  ·····J··
0020  02 3c 01 bb 95 6c 9c 36  e5 67 4f bc ff d1 80 18   ·<···l·6  ·gO·····
0030  15 05 26 78 00 00 01 01  08 0a ae c8 da b3 07 b7   ··&x····  ········
```

wireshark_wlp0s20f39WFF22.pcapng   Packets: 21282 · Displayed: 8283 (38.9%)   Profile: Default

Ex(6):



```
mateus@mateus-82MD:~$ ping 10.250.0.1
PING 10.250.0.1 (10.250.0.1) 56(84) bytes of data.
64 bytes from 10.250.0.1: icmp_seq=1 ttl=255 time=8.78 ms
64 bytes from 10.250.0.1: icmp_seq=2 ttl=255 time=19.2 ms
64 bytes from 10.250.0.1: icmp_seq=3 ttl=255 time=8.01 ms
64 bytes from 10.250.0.1: icmp_seq=4 ttl=255 time=4.62 ms
64 bytes from 10.250.0.1: icmp_seq=5 ttl=255 time=7.35 ms
64 bytes from 10.250.0.1: icmp_seq=6 ttl=255 time=7.96 ms
64 bytes from 10.250.0.1: icmp_seq=7 ttl=255 time=4.44 ms
^C
--- 10.250.0.1 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6009ms
rtt min/avg/max/mdev = 4.441/8.621/19.186/4.591 ms
mateus@mateus-82MD:~$ 
```

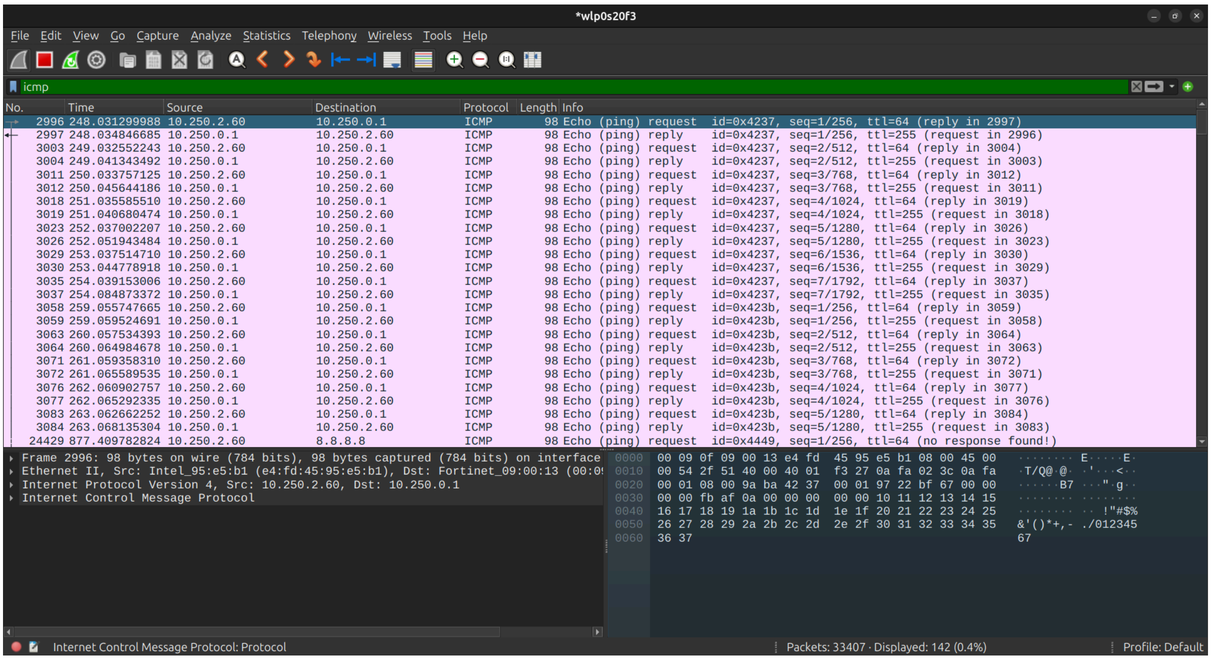


```
ip.addr == 10.250.2.60 and icmp.type == 8 and ip.dst == 10.250.0.1

No.   Time              Source       Destination  Protocol Length Info
 2996 248.031299988 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x4237, seq=1/256, ttl=64 (reply in 2997)
 3003 249.032552243 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x4237, seq=2/512, ttl=64 (reply in 3004)
 3011 250.033757125 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x4237, seq=3/768, ttl=64 (reply in 3012)
 3018 251.035585510 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x4237, seq=4/1024, ttl=64 (reply in 3019)
 3023 252.037002207 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x4237, seq=5/1280, ttl=64 (reply in 3026)
 3029 253.037514710 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x4237, seq=6/1536, ttl=64 (reply in 3030)
 3035 254.039153006 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x4237, seq=7/1792, ttl=64 (reply in 3037)
 3058 259.055747665 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x423b, seq=1/256, ttl=64 (reply in 3059)
 3063 260.057534393 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x423b, seq=2/512, ttl=64 (reply in 3064)
 3071 261.059358310 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x423b, seq=3/768, ttl=64 (reply in 3072)
 3076 262.060902757 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x423b, seq=4/1024, ttl=64 (reply in 3077)
 3083 263.062662252 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x423b, seq=5/1280, ttl=64 (reply in 3084)
25712 991.508449311 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x4479, seq=1/256, ttl=64 (reply in 25714)
25726 992.509628699 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x4479, seq=2/512, ttl=64 (reply in 25728)
25735 993.510884415 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x4479, seq=3/768, ttl=64 (reply in 25736)
25753 994.511525347 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x4479, seq=4/1024, ttl=64 (reply in 25755)
25763 995.513199964 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x4479, seq=5/1280, ttl=64 (reply in 25764)
25791 996.513504483 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x4479, seq=6/1536, ttl=64 (reply in 25795)
25814 997.515433740 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x4479, seq=7/1792, ttl=64 (reply in 25816)
25843 1004.1190891… 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x447c, seq=1/256, ttl=64 (reply in 25844)
25851 1005.1212097… 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x447c, seq=2/512, ttl=64 (reply in 25854)
25863 1006.1225288… 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x447c, seq=3/768, ttl=64 (reply in 25864)
25883 1007.1235289… 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x447c, seq=4/1024, ttl=64 (reply in 25884)
25887 1008.1254410… 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x447c, seq=5/1280, ttl=64 (reply in 25889)
25892 1009.1265389… 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x447c, seq=6/1536, ttl=64 (reply in 25893)
25906 1010.1277651… 10.250.2.60 10.250.0.1 ICMP  98 Echo (ping) request  id=0x447c, seq=7/1792, ttl=64 (reply in 25907)

› Frame 2996: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interfac
› Ethernet II, Src: Intel_95:e5:b1 (e4:fd:45:95:e5:b1), Dst: Fortinet_09:00:13 (00:
› Internet Protocol Version 4, Src: 10.250.2.60, Dst: 10.250.0.1

0000  00 09 0f 09 00 13 e4 fd  45 95 e5 b1 08 00 45 00   ········ E····E·
0010  00 54 2f 51 40 00 40 01  f3 27 0a fa 02 3c 0a fa   ·T/Q@·@· ·'···<··
0020  00 01 08 00 9a ba 42 37  00 01 97 22 bf 67 00 00   ······B7 ···"·g··
0030  00 00 fb af 0a 00 00 00  00 00 10 11 12 13 14 15   ········ ········

wireshark_wlp0s20f39WFF22.pcapng        Packets: 27220 · Displayed: 26 (0.1%)        Profile: Default
```

Exercício (1): Ping em 10.250.2.60:

Pode-se reduzir o comando de filtragem com sucesso, para ip.addr == meu_ip and ip.dst == 10.250.2.60, devido ao fato de que na aplicação em questão estamos apenas consultando a conexão entre a máquina pessoal e o roteador, portanto, há apenas requisições de ping

Ex(8):



icmp

```
No.     Time          Source        Destination   Protocol Length Info
   2996 248.031299988 10.250.2.60   10.250.0.1    ICMP       98 Echo (ping) request  id=0x4237, seq=1/256, ttl=64 (reply in 2997)
   2997 248.034846685 10.250.0.1    10.250.2.60   ICMP       98 Echo (ping) reply    id=0x4237, seq=1/256, ttl=255 (request in 2996)
   3003 249.032552243 10.250.2.60   10.250.0.1    ICMP       98 Echo (ping) request  id=0x4237, seq=2/512, ttl=64 (reply in 3004)
   3004 249.041343492 10.250.0.1    10.250.2.60   ICMP       98 Echo (ping) reply    id=0x4237, seq=2/512, ttl=255 (request in 3003)
   3011 250.033757125 10.250.2.60   10.250.0.1    ICMP       98 Echo (ping) request  id=0x4237, seq=3/768, ttl=64 (reply in 3012)
   3012 250.045644186 10.250.0.1    10.250.2.60   ICMP       98 Echo (ping) reply    id=0x4237, seq=3/768, ttl=255 (request in 3011)
   3018 251.035585510 10.250.2.60   10.250.0.1    ICMP       98 Echo (ping) request  id=0x4237, seq=4/1024, ttl=64 (reply in 3019)
   3019 251.040680474 10.250.0.1    10.250.2.60   ICMP       98 Echo (ping) reply    id=0x4237, seq=4/1024, ttl=255 (request in 3018)
   3023 252.037002207 10.250.2.60   10.250.0.1    ICMP       98 Echo (ping) request  id=0x4237, seq=5/1280, ttl=64 (reply in 3026)
   3026 252.051943484 10.250.0.1    10.250.2.60   ICMP       98 Echo (ping) reply    id=0x4237, seq=5/1280, ttl=255 (request in 3023)
   3029 253.037514710 10.250.2.60   10.250.0.1    ICMP       98 Echo (ping) request  id=0x4237, seq=6/1536, ttl=64 (reply in 3030)
   3030 253.044778918 10.250.0.1    10.250.2.60   ICMP       98 Echo (ping) reply    id=0x4237, seq=6/1536, ttl=255 (request in 3029)
   3035 254.039153006 10.250.2.60   10.250.0.1    ICMP       98 Echo (ping) request  id=0x4237, seq=7/1792, ttl=64 (reply in 3037)
   3037 254.084873372 10.250.0.1    10.250.2.60   ICMP       98 Echo (ping) reply    id=0x4237, seq=7/1792, ttl=255 (request in 3035)
   3058 259.055747665 10.250.2.60   10.250.0.1    ICMP       98 Echo (ping) request  id=0x423b, seq=1/256, ttl=64 (reply in 3059)
   3059 259.059524691 10.250.0.1    10.250.2.60   ICMP       98 Echo (ping) reply    id=0x423b, seq=1/256, ttl=255 (request in 3058)
   3063 260.057534393 10.250.2.60   10.250.0.1    ICMP       98 Echo (ping) request  id=0x423b, seq=2/512, ttl=64 (reply in 3064)
   3064 260.064984678 10.250.0.1    10.250.2.60   ICMP       98 Echo (ping) reply    id=0x423b, seq=2/512, ttl=255 (request in 3063)
   3071 261.059358310 10.250.2.60   10.250.0.1    ICMP       98 Echo (ping) request  id=0x423b, seq=3/768, ttl=64 (reply in 3072)
   3072 261.065589535 10.250.0.1    10.250.2.60   ICMP       98 Echo (ping) reply    id=0x423b, seq=3/768, ttl=255 (request in 3071)
   3076 262.060902757 10.250.2.60   10.250.0.1    ICMP       98 Echo (ping) request  id=0x423b, seq=4/1024, ttl=64 (reply in 3077)
   3077 262.065292335 10.250.0.1    10.250.2.60   ICMP       98 Echo (ping) reply    id=0x423b, seq=4/1024, ttl=255 (request in 3076)
   3083 263.062662252 10.250.2.60   10.250.0.1    ICMP       98 Echo (ping) request  id=0x423b, seq=5/1280, ttl=64 (reply in 3084)
   3084 263.068135304 10.250.0.1    10.250.2.60   ICMP       98 Echo (ping) reply    id=0x423b, seq=5/1280, ttl=255 (request in 3083)
  24429 877.409782824 10.250.2.60   8.8.8.8       ICMP       98 Echo (ping) request  id=0x4449, seq=1/256, ttl=64 (no response found!)
```

```
Frame 2996: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface
Ethernet II, Src: Intel_95:e5:b1 (e4:fd:45:95:e5:b1), Dst: Fortinet_09:00:13 (00:0
Internet Protocol Version 4, Src: 10.250.2.60, Dst: 10.250.0.1
Internet Control Message Protocol
```

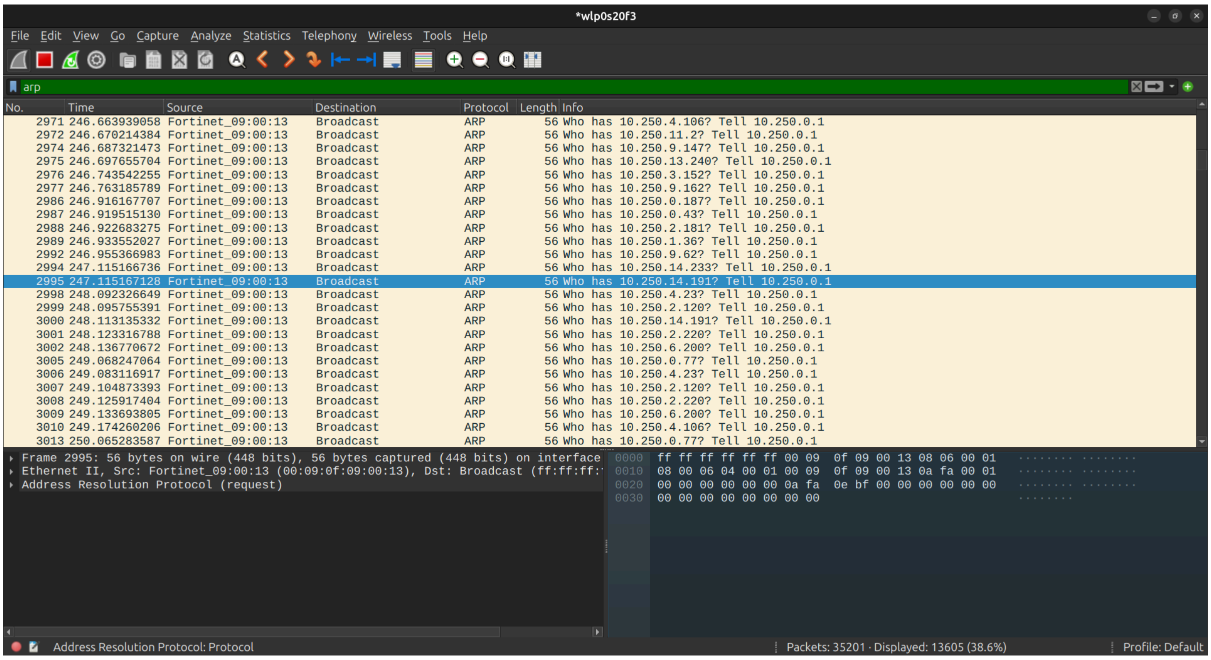
```
0000  00 09 0f 09 00 13 e4 fd  45 95 e5 b1 08 00 45 00   ········ E·····E·
0010  00 54 2f 51 40 00 40 01  f3 27 0a fa 02 3c 0a fa   ·T/Q@·@· ·'···<··
0020  00 01 08 00 9a ba 42 37  00 01 97 22 bf 67 00 00   ······B7 ···"·g··
0030  00 00 fb af 0a 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

Internet Control Message Protocol: Protocol

Packets: 33407 · Displayed: 142 (0.4%)

Profile: Default

Ex(9):


*wlp0s20f3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp

```
No.   Time           Source              Destination      Protocol  Length Info
 2971 246.663939058 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.4.106? Tell 10.250.0.1
 2972 246.670214384 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.11.2? Tell 10.250.0.1
 2974 246.687321473 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.9.147? Tell 10.250.0.1
 2975 246.697655704 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.13.240? Tell 10.250.0.1
 2976 246.743542255 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.3.152? Tell 10.250.0.1
 2977 246.763185789 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.9.162? Tell 10.250.0.1
 2986 246.916167707 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.0.187? Tell 10.250.0.1
 2987 246.919515130 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.0.43? Tell 10.250.0.1
 2988 246.922683275 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.2.181? Tell 10.250.0.1
 2989 246.933552027 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.1.36? Tell 10.250.0.1
 2992 246.955366983 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.9.62? Tell 10.250.0.1
 2994 247.115166736 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.14.233? Tell 10.250.0.1
 2995 247.115167128 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.14.191? Tell 10.250.0.1
 2998 248.092326649 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.4.23? Tell 10.250.0.1
 2999 248.095755391 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.2.120? Tell 10.250.0.1
 3000 248.113135332 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.14.191? Tell 10.250.0.1
 3001 248.123316788 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.2.220? Tell 10.250.0.1
 3002 248.136770672 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.6.200? Tell 10.250.0.1
 3005 249.068247064 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.0.77? Tell 10.250.0.1
 3006 249.083116917 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.4.23? Tell 10.250.0.1
 3007 249.104873393 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.2.120? Tell 10.250.0.1
 3008 249.125917404 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.2.220? Tell 10.250.0.1
 3009 249.133693805 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.6.200? Tell 10.250.0.1
 3010 249.174260206 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.4.106? Tell 10.250.0.1
 3013 250.065283587 Fortinet_09:00:13   Broadcast        ARP         56 Who has 10.250.0.77? Tell 10.250.0.1
```

```
› Frame 2995: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface
› Ethernet II, Src: Fortinet_09:00:13 (00:09:0f:09:00:13), Dst: Broadcast (ff:ff:ff:
› Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 09  0f 09 00 13 08 06 00 01   ········ ········
0010  08 00 06 04 00 01 00 09  0f 09 00 13 0a fa 00 01   ········ ········
0020  00 00 00 00 00 00 0a fa  0e bf 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00                            ········
```

Address Resolution Protocol: Protocol
Packets: 35201 · Displayed: 13605 (38.6%)
Profile: Default

Exercício (3): ARP

Se executarmos o primeiro comando (arp.opcode == 1), podemos ver as mensagens que o roteador envia para identificar o ip de uma determinada máquina, por meio de um broadcast, para todas as máquinas conectadas. Por outro lado, no segundo comando (arp.opcode == 2), podemos ver as mensagens que a máquina local envia para a rede, se identificando como dono do ip solicitado no primeiro comando.