MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA
CURSO DE ENGENHARIA DE TELECOMUNICAÇÕES – CÂMPUS SÃO JOSÉ

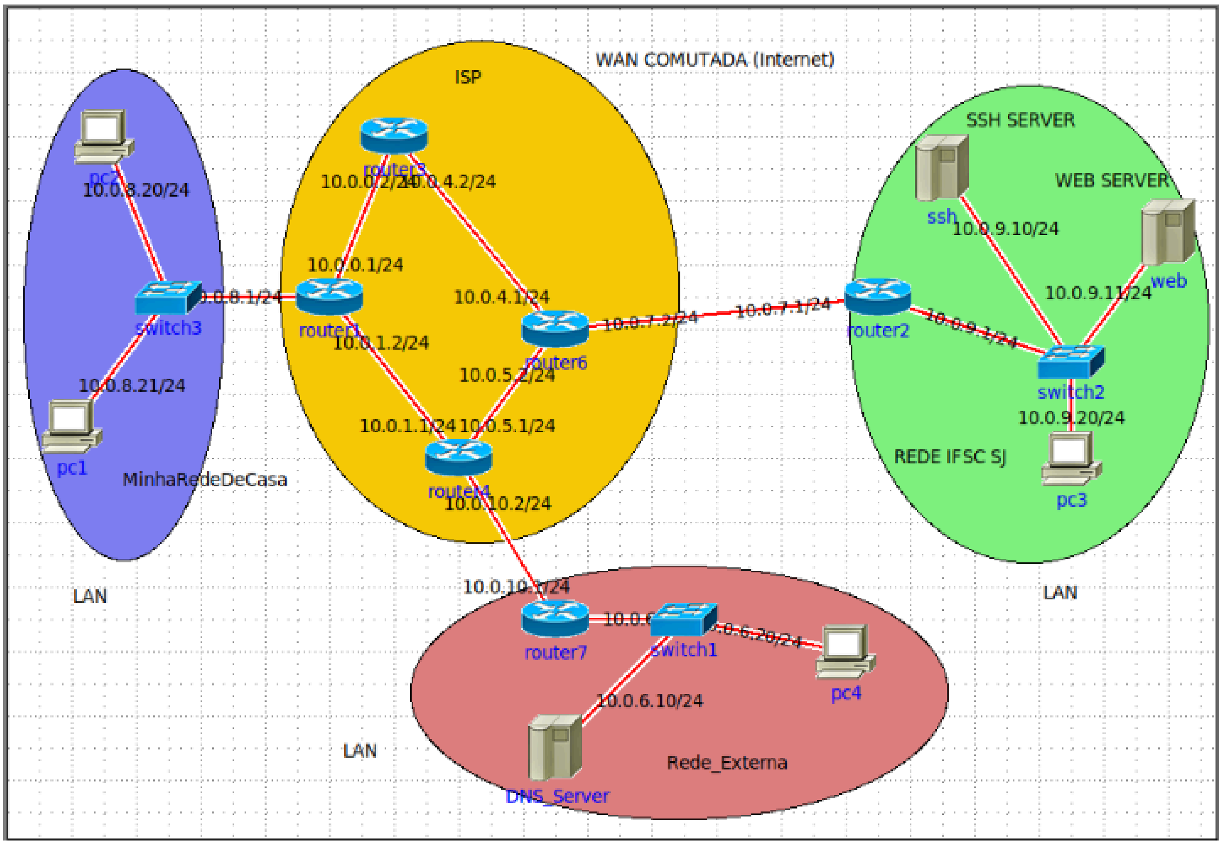
RELATÓRIO TÉCNICO

LABORATÓRIO HTTPS

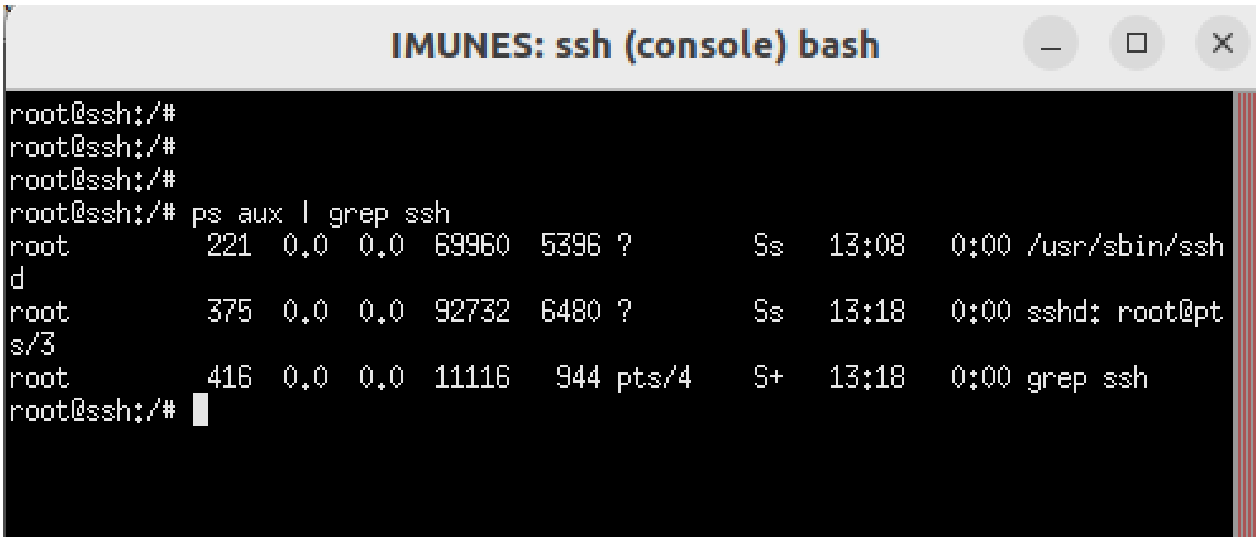
Arthur Cadore Matuella Barcella

TAREFA:

Rede a ser implementada

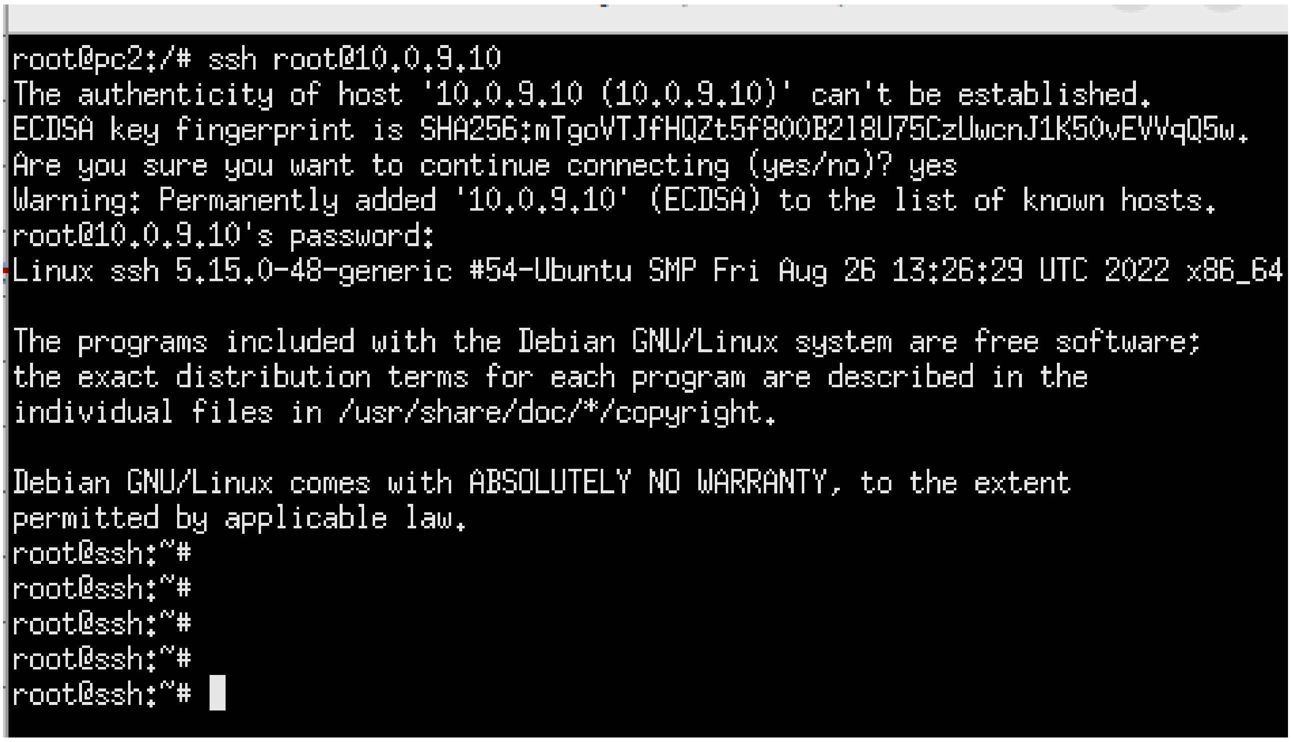


1) **Mostre que o serviço de SSH está rodando na máquina:**



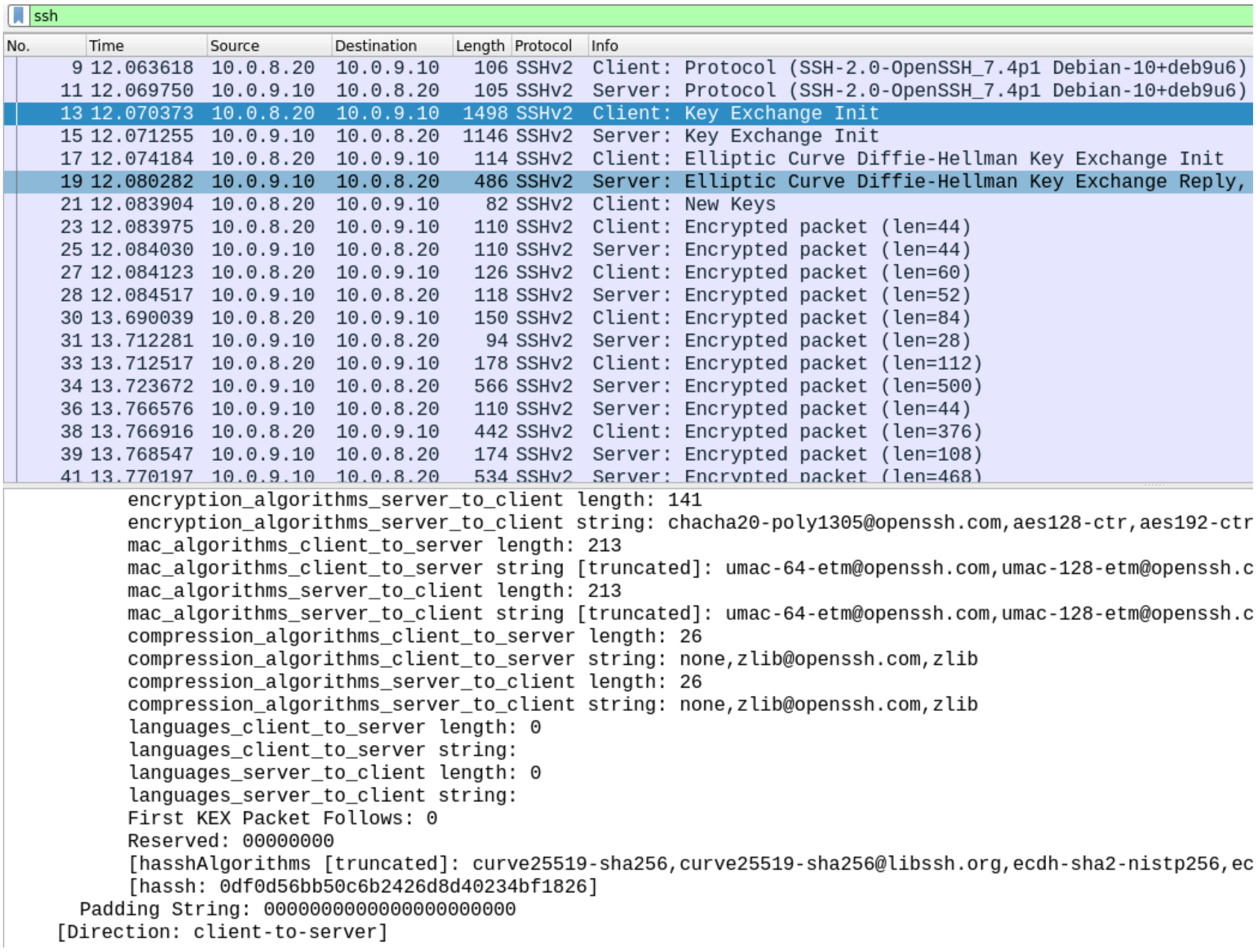
```
root@ssh:/#
root@ssh:/#
root@ssh:/#
root@ssh:/# ps aux | grep ssh
root         221  0.0  0.0  69960  5396 ?        Ss   13:08   0:00 /usr/sbin/ssh
d
root         375  0.0  0.0  92732  6480 ?        Ss   13:18   0:00 sshd: root@pt
s/3
root         416  0.0  0.0  11116   944 pts/4    S+   13:18   0:00 grep ssh
root@ssh:/# 
```

2) **Feito isso, vamos realizar a conexão SSH remota com o servidor:**



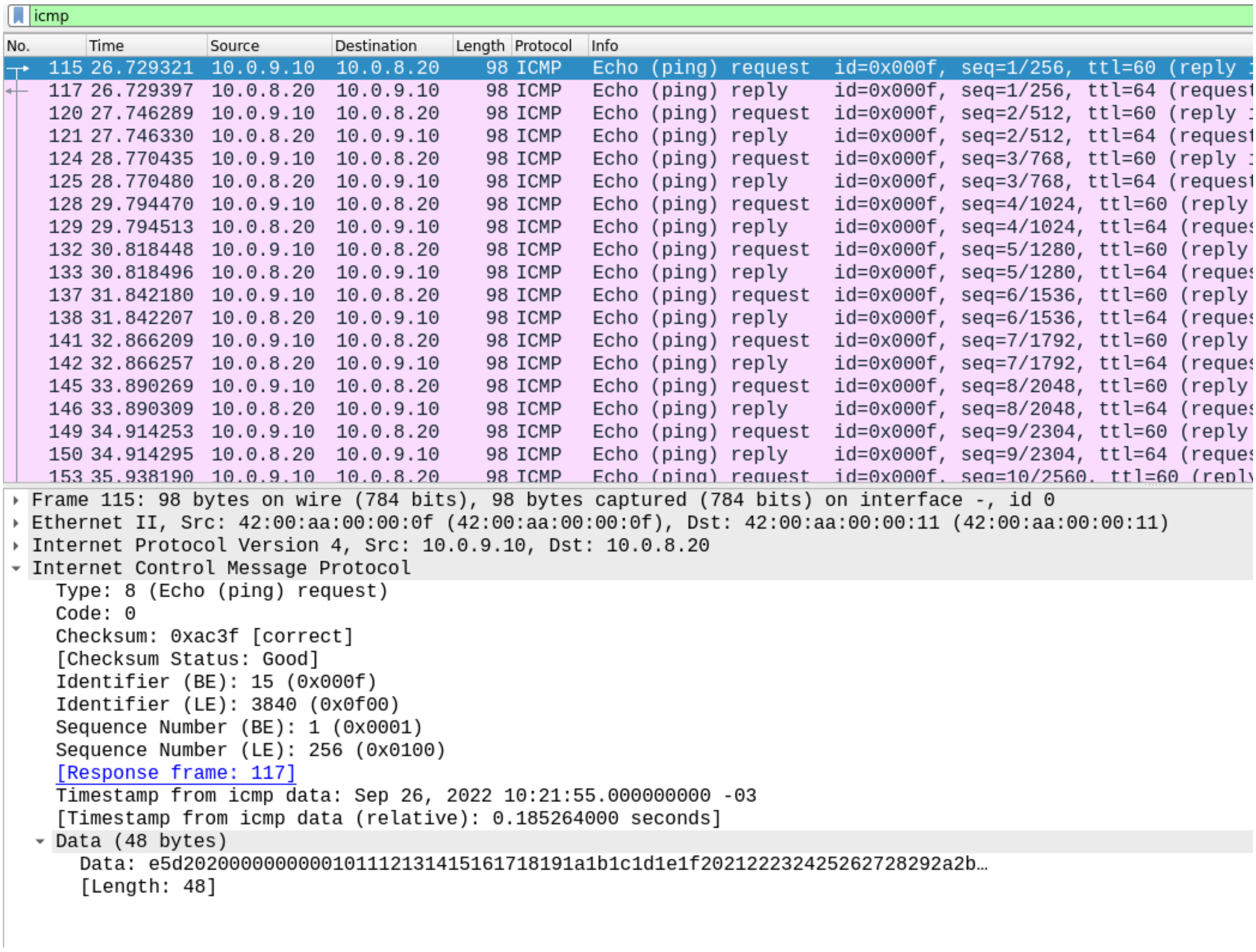
```
root@pc2:/# ssh root@10.0.9.10
The authenticity of host '10.0.9.10 (10.0.9.10)' can't be established.
ECDSA key fingerprint is SHA256:mTgoVTJfHQZt5f800B218U75CzUwcnJ1K50vEVVqQ5w.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.9.10' (ECDSA) to the list of known hosts.
root@10.0.9.10's password:
Linux ssh 5.15.0-48-generic #54-Ubuntu SMP Fri Aug 26 13:26:29 UTC 2022 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@ssh:~#
root@ssh:~#
root@ssh:~#
root@ssh:~#
root@ssh:~#
```

3) **Dentro do servidor, para realizar uma captura de acesso SSH e PING, fiz um ping reverso para a máquina de origem da comunicação SSH (cliente SSH):**



```
No.   Time      Source     Destination Length Protocol Info
    9 12.063618 10.0.8.20 10.0.9.10   106 SSHv2 Client: Protocol (SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u6)
   11 12.069750 10.0.9.10 10.0.8.20   105 SSHv2 Server: Protocol (SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u6)
   13 12.070373 10.0.8.20 10.0.9.10  1498 SSHv2 Client: Key Exchange Init
   15 12.071255 10.0.9.10 10.0.8.20  1146 SSHv2 Server: Key Exchange Init
   17 12.074184 10.0.8.20 10.0.9.10   114 SSHv2 Client: Elliptic Curve Diffie-Hellman Key Exchange Init
   19 12.080282 10.0.9.10 10.0.8.20   486 SSHv2 Server: Elliptic Curve Diffie-Hellman Key Exchange Reply,
   21 12.083904 10.0.8.20 10.0.9.10    82 SSHv2 Client: New Keys
   23 12.083975 10.0.8.20 10.0.9.10   110 SSHv2 Client: Encrypted packet (len=44)
   25 12.084030 10.0.9.10 10.0.8.20   110 SSHv2 Server: Encrypted packet (len=44)
   27 12.084123 10.0.8.20 10.0.9.10   126 SSHv2 Client: Encrypted packet (len=60)
   28 12.084517 10.0.9.10 10.0.8.20   118 SSHv2 Server: Encrypted packet (len=52)
   30 13.690039 10.0.8.20 10.0.9.10   150 SSHv2 Client: Encrypted packet (len=84)
   31 13.712281 10.0.9.10 10.0.8.20    94 SSHv2 Server: Encrypted packet (len=28)
   33 13.712517 10.0.8.20 10.0.9.10   178 SSHv2 Client: Encrypted packet (len=112)
   34 13.723672 10.0.9.10 10.0.8.20   566 SSHv2 Server: Encrypted packet (len=500)
   36 13.766576 10.0.9.10 10.0.8.20   110 SSHv2 Server: Encrypted packet (len=44)
   38 13.766916 10.0.8.20 10.0.9.10   442 SSHv2 Client: Encrypted packet (len=376)
   39 13.768547 10.0.9.10 10.0.8.20   174 SSHv2 Server: Encrypted packet (len=108)
   41 13.770197 10.0.9.10 10.0.8.20   534 SSHv2 Server: Encrypted packet (len=468)
```

```
          encryption_algorithms_server_to_client length: 141
          encryption_algorithms_server_to_client string: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr
          mac_algorithms_client_to_server length: 213
          mac_algorithms_client_to_server string [truncated]: umac-64-etm@openssh.com,umac-128-etm@openssh.c
          mac_algorithms_server_to_client length: 213
          mac_algorithms_server_to_client string [truncated]: umac-64-etm@openssh.com,umac-128-etm@openssh.c
          compression_algorithms_client_to_server length: 26
          compression_algorithms_client_to_server string: none,zlib@openssh.com,zlib
          compression_algorithms_server_to_client length: 26
          compression_algorithms_server_to_client string: none,zlib@openssh.com,zlib
          languages_client_to_server length: 0
          languages_client_to_server string:
          languages_server_to_client length: 0
          languages_server_to_client string:
          First KEX Packet Follows: 0
          Reserved: 00000000
          [hasshAlgorithms [truncated]: curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ec
          [hassh: 0df0d56bb50c6b2426d8d40234bf1826]
      Padding String: 0000000000000000000000
    [Direction: client-to-server]
```

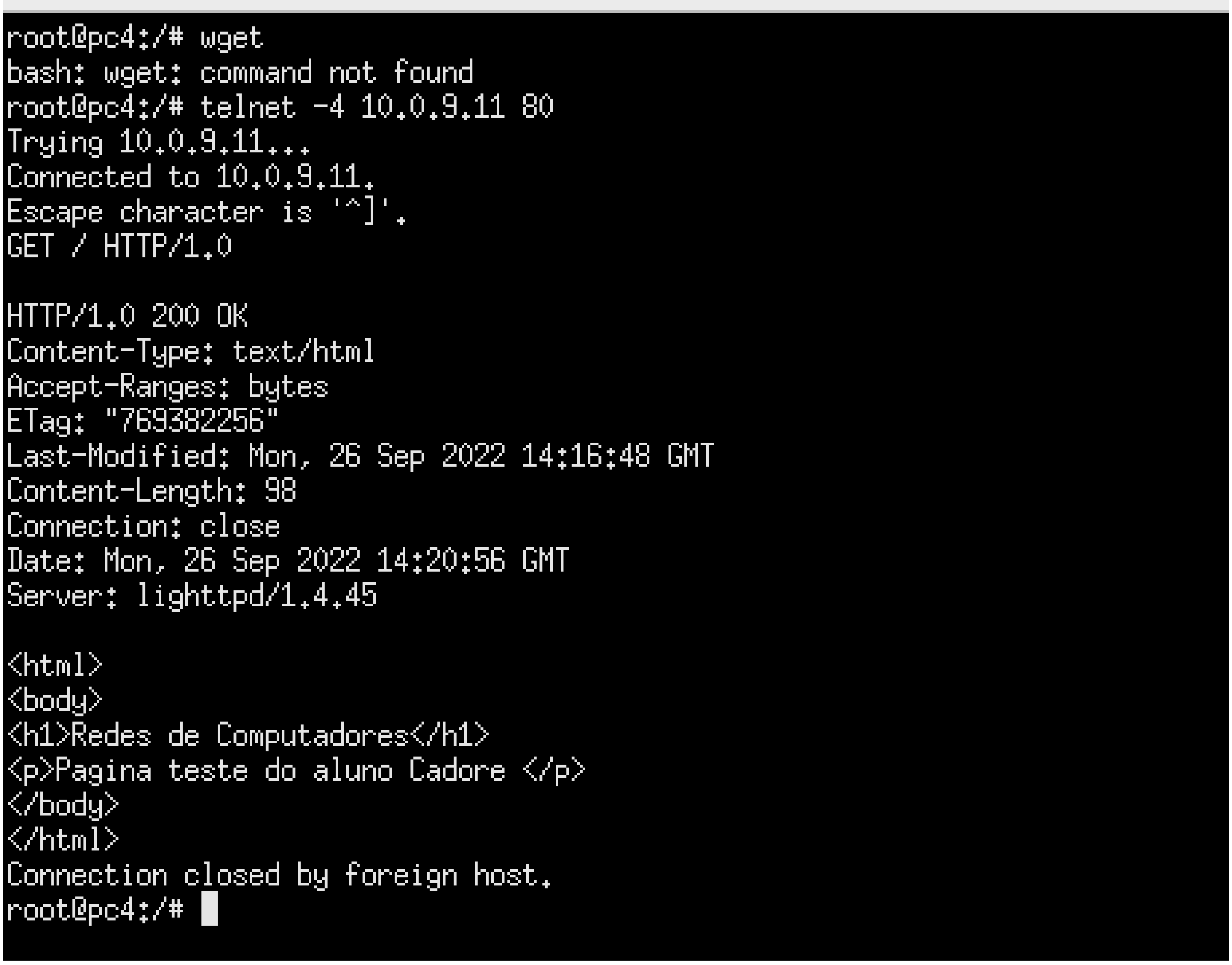


```
No.   Time          Source       Destination  Length Protocol  Info
  115 26.729321 10.0.9.10  10.0.8.20    98 ICMP   Echo (ping) request  id=0x000f, seq=1/256, ttl=60 (reply i
  117 26.729397 10.0.8.20  10.0.9.10    98 ICMP   Echo (ping) reply    id=0x000f, seq=1/256, ttl=64 (request
  120 27.746289 10.0.9.10  10.0.8.20    98 ICMP   Echo (ping) request  id=0x000f, seq=2/512, ttl=60 (reply i
  121 27.746330 10.0.8.20  10.0.9.10    98 ICMP   Echo (ping) reply    id=0x000f, seq=2/512, ttl=64 (request
  124 28.770435 10.0.9.10  10.0.8.20    98 ICMP   Echo (ping) request  id=0x000f, seq=3/768, ttl=60 (reply i
  125 28.770480 10.0.8.20  10.0.9.10    98 ICMP   Echo (ping) reply    id=0x000f, seq=3/768, ttl=64 (request
  128 29.794470 10.0.9.10  10.0.8.20    98 ICMP   Echo (ping) request  id=0x000f, seq=4/1024, ttl=60 (reply
  129 29.794513 10.0.8.20  10.0.9.10    98 ICMP   Echo (ping) reply    id=0x000f, seq=4/1024, ttl=64 (reques
  132 30.818448 10.0.9.10  10.0.8.20    98 ICMP   Echo (ping) request  id=0x000f, seq=5/1280, ttl=60 (reply
  133 30.818496 10.0.8.20  10.0.9.10    98 ICMP   Echo (ping) reply    id=0x000f, seq=5/1280, ttl=64 (reques
  137 31.842180 10.0.9.10  10.0.8.20    98 ICMP   Echo (ping) request  id=0x000f, seq=6/1536, ttl=60 (reply
  138 31.842207 10.0.8.20  10.0.9.10    98 ICMP   Echo (ping) reply    id=0x000f, seq=6/1536, ttl=64 (reques
  141 32.866209 10.0.9.10  10.0.8.20    98 ICMP   Echo (ping) request  id=0x000f, seq=7/1792, ttl=60 (reply
  142 32.866257 10.0.8.20  10.0.9.10    98 ICMP   Echo (ping) reply    id=0x000f, seq=7/1792, ttl=64 (reques
  145 33.890269 10.0.9.10  10.0.8.20    98 ICMP   Echo (ping) request  id=0x000f, seq=8/2048, ttl=60 (reply
  146 33.890309 10.0.8.20  10.0.9.10    98 ICMP   Echo (ping) reply    id=0x000f, seq=8/2048, ttl=64 (reques
  149 34.914253 10.0.9.10  10.0.8.20    98 ICMP   Echo (ping) request  id=0x000f, seq=9/2304, ttl=60 (reply
  150 34.914295 10.0.8.20  10.0.9.10    98 ICMP   Echo (ping) reply    id=0x000f, seq=9/2304, ttl=64 (reques
  153 35.938190 10.0.9.10  10.0.8.20    98 ICMP   Echo (ping) request  id=0x000f, seq=10/2560, ttl=60 (reply
```

```
› Frame 115: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
› Ethernet II, Src: 42:00:aa:00:00:0f (42:00:aa:00:00:0f), Dst: 42:00:aa:00:00:11 (42:00:aa:00:00:11)
› Internet Protocol Version 4, Src: 10.0.9.10, Dst: 10.0.8.20
⌄ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xac3f [correct]
    [Checksum Status: Good]
    Identifier (BE): 15 (0x000f)
    Identifier (LE): 3840 (0x0f00)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 117]
    Timestamp from icmp data: Sep 26, 2022 10:21:55.000000000 -03
    [Timestamp from icmp data (relative): 0.185264000 seconds]
  ⌄ Data (48 bytes)
      Data: e5d2020000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b…
      [Length: 48]
```

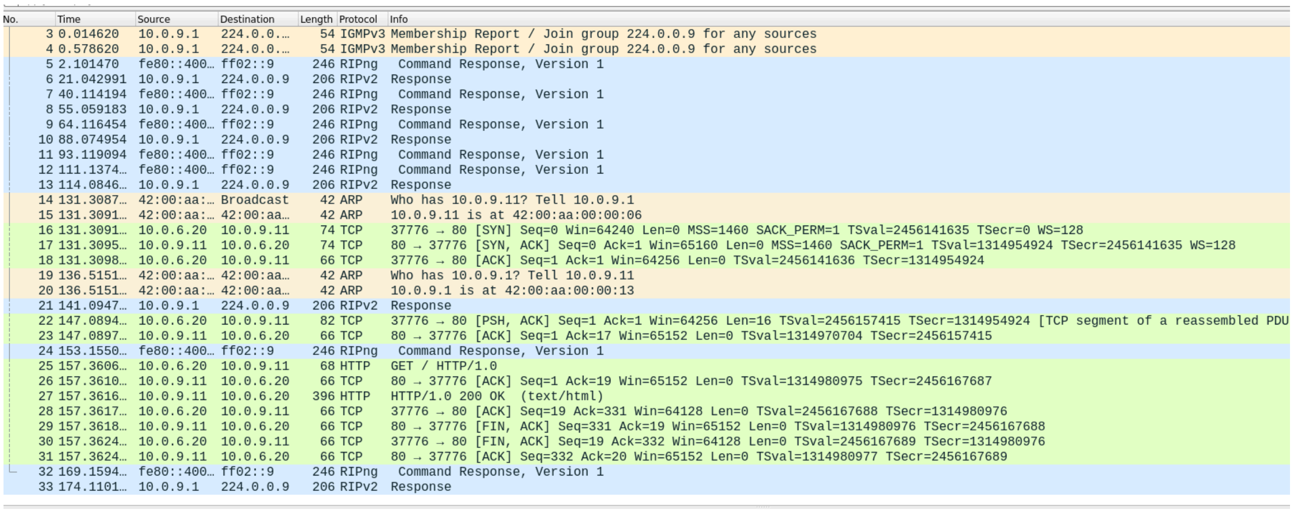
Realizando teste utilizando o HTTP para comparação:

3) O objetivo deste teste é garantir que o telnet conseguiria coletar uma página sem um protocolo criptografado.

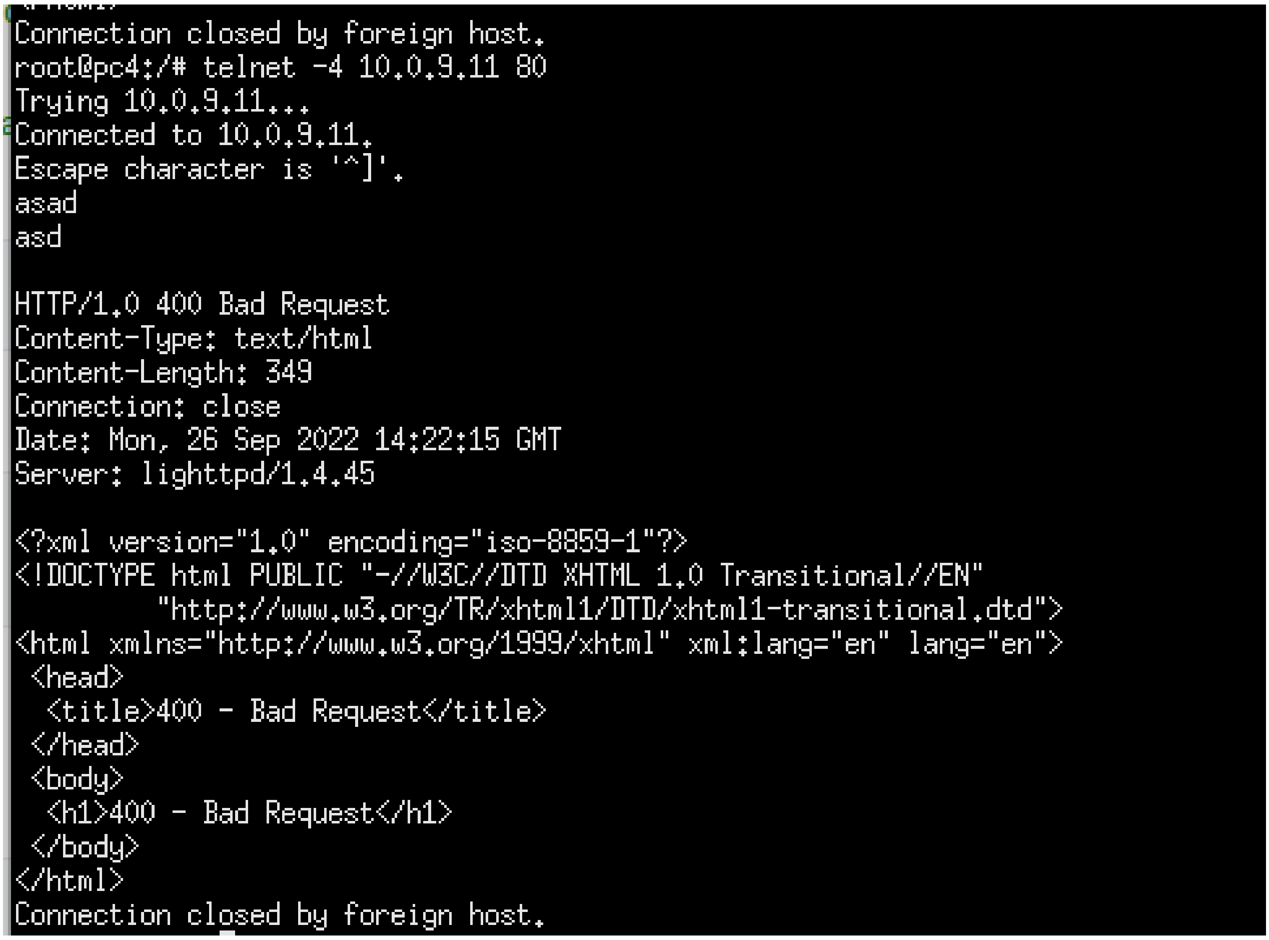


```
root@pc4:/# wget
bash: wget: command not found
root@pc4:/# telnet -4 10.0.9.11 80
Trying 10.0.9.11...
Connected to 10.0.9.11.
Escape character is '^]'.
GET / HTTP/1.0

HTTP/1.0 200 OK
Content-Type: text/html
Accept-Ranges: bytes
ETag: "769382256"
Last-Modified: Mon, 26 Sep 2022 14:16:48 GMT
Content-Length: 98
Connection: close
Date: Mon, 26 Sep 2022 14:20:56 GMT
Server: lighttpd/1.4.45

<html>
<body>
<h1>Redes de Computadores</h1>
<p>Pagina teste do aluno Cadore </p>
</body>
</html>
Connection closed by foreign host.
root@pc4:/#
```

Abaixo está a captura para comparação, note que não há troca de chaves via autenticação TLS antes de iniciar a troca de dados.



```
No.   Time      Source     Destination Length Protocol Info
    3 0.014620  10.0.9.1   224.0.0.…    54 IGMPv3 Membership Report / Join group 224.0.0.9 for any sources
    4 0.578620  10.0.9.1   224.0.0.…    54 IGMPv3 Membership Report / Join group 224.0.0.9 for any sources
    5 2.101470  fe80::400… ff02::9     246 RIPng   Command Response, Version 1
    6 21.042991 10.0.9.1   224.0.0.9   206 RIPv2  Response
    7 40.114194 fe80::400… ff02::9     246 RIPng   Command Response, Version 1
    8 55.059183 10.0.9.1   224.0.0.9   206 RIPv2  Response
    9 64.116454 fe80::400… ff02::9     246 RIPng   Command Response, Version 1
   10 88.074954 10.0.9.1   224.0.0.9   206 RIPv2  Response
   11 93.119094 fe80::400… ff02::9     246 RIPng   Command Response, Version 1
   12 111.1374… fe80::400… ff02::9     246 RIPng   Command Response, Version 1
   13 114.0846… 10.0.9.1   224.0.0.9   206 RIPv2  Response
   14 131.3087… 42:00:aa:… Broadcast    42 ARP    Who has 10.0.9.11? Tell 10.0.9.1
   15 131.3091… 42:00:aa:… 42:00:aa…    42 ARP    10.0.9.11 is at 42:00:aa:00:00:06
   16 131.3091… 10.0.6.20  10.0.9.11    74 TCP    37776 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2456141635 TSecr=0 WS=128
   17 131.3095… 10.0.9.11  10.0.6.20    74 TCP    80 → 37776 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=1314954924 TSecr=2456141635 WS=128
   18 131.3098… 10.0.6.20  10.0.9.11    66 TCP    37776 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2456141636 TSecr=1314954924
   19 136.5151… 42:00:aa:… 42:00:aa…    42 ARP    Who has 10.0.9.1? Tell 10.0.9.11
   20 136.5151… 42:00:aa:… 42:00:aa…    42 ARP    10.0.9.1 is at 42:00:aa:00:00:13
   21 141.0947… 10.0.9.1   224.0.0.9   206 RIPv2  Response
   22 147.0894… 10.0.6.20  10.0.9.11    82 TCP    37776 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=16 TSval=2456157415 TSecr=1314954924 [TCP segment of a reassembled PDU
   23 147.0897… 10.0.9.11  10.0.6.20    66 TCP    80 → 37776 [ACK] Seq=1 Ack=17 Win=65152 Len=0 TSval=1314970704 TSecr=2456157415
   24 153.1550… fe80::400… ff02::9     246 RIPng   Command Response, Version 1
   25 157.3606… 10.0.6.20  10.0.9.11    68 HTTP   GET / HTTP/1.0
   26 157.3610… 10.0.9.11  10.0.6.20    66 TCP    80 → 37776 [ACK] Seq=1 Ack=19 Win=65152 Len=0 TSval=1314980975 TSecr=2456167687
   27 157.3616… 10.0.9.11  10.0.6.20   396 HTTP   HTTP/1.0 200 OK  (text/html)
   28 157.3617… 10.0.6.20  10.0.9.11    66 TCP    37776 → 80 [ACK] Seq=19 Ack=331 Win=64128 Len=0 TSval=2456167688 TSecr=1314980976
   29 157.3618… 10.0.9.11  10.0.6.20    66 TCP    80 → 37776 [FIN, ACK] Seq=331 Ack=19 Win=65152 Len=0 TSval=1314980976 TSecr=2456167688
   30 157.3624… 10.0.6.20  10.0.9.11    66 TCP    37776 → 80 [FIN, ACK] Seq=19 Ack=332 Win=64128 Len=0 TSval=2456167689 TSecr=1314980976
   31 157.3624… 10.0.9.11  10.0.6.20    66 TCP    80 → 37776 [ACK] Seq=332 Ack=20 Win=65152 Len=0 TSval=1314980977 TSecr=2456167689
   32 169.1594… fe80::400… ff02::9     246 RIPng   Command Response, Version 1
   33 174.1101… 10.0.9.1   224.0.0.9   206 RIPv2  Response
```



```
Connection closed by foreign host.
root@pc4:/# telnet -4 10.0.9.11 80
Trying 10.0.9.11...
Connected to 10.0.9.11.
Escape character is '^]'.
asad
asd

HTTP/1.0 400 Bad Request
Content-Type: text/html
Content-Length: 349
Connection: close
Date: Mon, 26 Sep 2022 14:22:15 GMT
Server: lighttpd/1.4.45

<?xml version="1.0" encoding="iso-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
         "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
 <head>
  <title>400 - Bad Request</title>
 </head>
 <body>
  <h1>400 - Bad Request</h1>
 </body>
</html>
Connection closed by foreign host.
```