Wireshark - Laboratório

Luiza Ávila

01)

A - Endereço MAC do computador

```
Ethernet II, Src: IntelCor_0c:52:15 (5c:cd:5b:0c:52:15), Dst: ARRISGro_0d:54:c2 (5c:e3:0e:0d:54:c2)
```

B –

```
Ethernet II, Src: IntelCor_0c:52:15 (5c:cd:5b:0c:52:15)
Internet Protocol Version 4, Src: 192.168.0.16, Dst: 14
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d57 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 4 (0x0004)
    Sequence number (LE): 1024 (0x0400)
    [Response frame: 4738]
    Data (32 bytes)
```

C – Fabricante:

ARRIS Group, Inc.

ARRIS Group, Inc.

6450 Sequence Drive

San Diego CA 92121

US

D – IP Origem: 192.168.0.16

IP Destino: 143.54.31.24

```
4266 25.481241    192.168.0.16          143.54.31.24          ICMP     74 Echo (ping) request  id=0x0001, seq=1/256, ttl=128 (reply in 4275)
```

E – Consulta e resposta:

```
4227 25.258555    2804:14c:5b70:8501:15aa:c997:20db:65fa  2804:14d:1:0:181:213:132:2             DNS      94 Standard query 0x982d AAAA www.sbc.org.br
4232 25.316546    2804:14d:1:0:181:213:132:2             2804:14c:5b70:8501:15aa:c997:20db:65fa  DNS     149 Standard query response 0x982d AAAA www.sbc.org.br SOA ns1.ufrgs.br
```

F – Info da resposta:

```
Domain Name System (response)
    Transaction ID: 0x982d
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  > Queries
  > Authoritative nameservers
    [Request In: 4227]
    [Time: 0.057991000 seconds]
```

02)

A – Pacotes consulta e resposta:

```
881 5.743854  2804:14c:5b70:8501:15aa:c997:20db:65fa  2804:14d:1:0:181:213:132:3              DNS  96 Standard query 0x12a3 AAAA icei.pucminas.br
882 5.752163  2804:14d:1:0:181:213:132:2              2804:14c:5b70:8501:15aa:c997:20db:65fa  DNS  146 Standard query response 0x12a3 AAAA icei.pucminas.br SOA ns.pucmg.br
```

B – Detalhes resposta DNS

```
Domain Name System (response)
    Transaction ID: 0x12a3
  Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  Queries
    > icei.pucminas.br: type AAAA, class IN
  Authoritative nameservers
    > icei.pucminas.br: type SOA, class IN, mname ns.pucmg.br
    [Request In: 875]
    [Time: 0.040140000 seconds]
```

Endereço IP: 186.248.79.30

C - Handshake conexão

```
37 5.239170  192.168.0.16     186.248.79.30     TCP  66 51525 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
50 5.269626  192.168.0.16     104.109.28.235    TCP  66 51526 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
64 5.292873  186.248.79.30    192.168.0.16      TCP  66 80 → 51525 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
65 5.292939  192.168.0.16     186.248.79.30     TCP  54 51525 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
```

Handshake desconexão

```
2183 2020-08-21 11:45:16,605027 186.248.79.30  192.168.0.10    TCP  56 80 → 61904 [FIN, ACK] Seq=8875 Ack=2440 Win=35072 Len=0
2184 2020-08-21 11:45:16,605055 192.168.0.10   186.248.79.30   TCP  54 61904 → 80 [ACK] Seq=2440 Ack=8876 Win=65280 Len=0
3230 2020-08-21 11:45:21,837174 192.168.0.10   186.248.79.30   TCP  54 61904 → 80 [FIN, ACK] Seq=2440 Ack=8876 Win=65280 Len=0
3239 2020-08-21 11:45:21,891827 186.248.79.30  192.168.0.10    TCP  56 80 → 61904 [ACK] Seq=8876 Ack=2441 Win=35072 Len=0
```

D – Tempo: 0.260000 segundos

```
Arrival Time: Aug 14, 2020 12:48:22.956430000 Hora oficial do Brasil
```

```
Arrival Time: Aug 14, 2020 12:48:22.956690000 Hora oficial do Brasil
```

E- Ele manda novamente os pacotes

```
14270 2020-08-20 11:11:13,099508 192.168.0.10    186.248.79.30    HTTP   1250 GET /index.php/cursos HTTP/1.1
14458 2020-08-20 11:11:13,461894 186.248.79.30   192.168.0.10     HTTP    957 HTTP/1.1 200 OK  (text/html)
14656 2020-08-20 11:11:14,543346 192.168.0.10    186.248.79.30    HTTP   1220 GET /templates/ja_teline_v/favicon.ico HTTP/1.1
14668 2020-08-20 11:11:14,585651 186.248.79.30   192.168.0.10     HTTP   1387 HTTP/1.1 200 OK  (PNG)
```

03)

A -

```
17 2020-08-20 13:53:34,225886 2804:14c:5b70:8501:acb2:71b2:2680:5121  2804:14d:1:0:181:213:132:3            DNS    92 Standard query 0xac0a AAAA ftp.pucmg.br
18 2020-08-20 13:53:34,246087 2804:14d:1:0:181:213:132:3              2804:14c:5b70:8501:acb2:71b2:2680:5121 DNS   136 Standard query response 0xac0a AAAA ftp.pucmg.br SOA ns.pucmg.br
```

B -

```
Domain Name System (response)
    Transaction ID: 0xac0a
  Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  > Queries
  > Authoritative nameservers
    [Request In: 17]
    [Time: 0.020201000 seconds]
```

Endereço IP: 186.248.79.32

C -

Handshake conexão:

```
31 2020-08-20 14:12:24,144926 192.168.0.10    186.248.79.32    TCP    66 57844 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
33 2020-08-20 14:12:24,182223 186.248.79.32   192.168.0.10     TCP    66 21 → 57844 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=64
34 2020-08-20 14:12:24,182313 192.168.0.10    186.248.79.32    TCP    54 57844 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0
```

Handshake desconexão:

```
4015 2020-08-21 11:56:08,185038 186.248.79.32   192.168.0.10     TCP    56 45614 → 61937 [FIN, ACK] Seq=206 Ack=1 Win=14656 Len=0
4016 2020-08-21 11:56:08,185130 192.168.0.10    186.248.79.32    TCP    54 61937 → 45614 [ACK] Seq=1 Ack=207 Win=65280 Len=0
4017 2020-08-21 11:56:08,185729 192.168.0.10    186.248.79.32    TCP    54 61937 → 45614 [FIN, ACK] Seq=1 Ack=207 Win=65280 Len=0
4018 2020-08-21 11:56:08,185957 192.168.0.10    186.248.79.32    TCP    54 61936 → 21 [FIN, ACK] Seq=112 Ack=419 Win=65280 Len=0
4022 2020-08-21 11:56:08,224310 186.248.79.32   192.168.0.10     TCP    56 45614 → 61937 [ACK] Seq=207 Ack=2 Win=14656 Len=0
```

D – 13825 pacotes com 1460 bytes

```
12708 2020-08-21 12:03:44,424835 186.248.79.32   192.168.0.10     FTP-DATA  1514 FTP Data: 1460 bytes (PASV) (RETR /Computacao/Nova pasta/2020-1_aed1_
12711 2020-08-21 12:03:44,436022 186.248.79.32   192.168.0.10     FTP-DATA  1514 FTP Data: 1460 bytes (PASV) (RETR /Computacao/Nova pasta/2020-1_aed1_
12712 2020-08-21 12:03:44,436022 186.248.79.32   192.168.0.10     FTP-DATA  1514 FTP Data: 1460 bytes (PASV) (RETR /Computacao/Nova pasta/2020-1_aed1_
12713 2020-08-21 12:03:44,436022 186.248.79.32   192.168.0.10     FTP-DATA  1514 FTP Data: 1460 bytes (PASV) (RETR /Computacao/Nova pasta/2020-1_aed1_
12714 2020-08-21 12:03:44,436022 186.248.79.32   192.168.0.10     FTP-DATA  1514 FTP Data: 1460 bytes (PASV) (RETR /Computacao/Nova pasta/2020-1_aed1_
12715 2020-08-21 12:03:44,436022 186.248.79.32   192.168.0.10     FTP-DATA  1514 FTP Data: 1460 bytes (PASV) (RETR /Computacao/Nova pasta/2020-1_aed1_
12716 2020-08-21 12:03:44,436022 186.248.79.32   192.168.0.10     FTP-DATA  1514 FTP Data: 1460 bytes (PASV) (RETR /Computacao/Nova pasta/2020-1_aed1_
12719 2020-08-21 12:03:44,439182 186.248.79.32   192.168.0.10     FTP-DATA  1514 FTP Data: 1460 bytes (PASV) (RETR /Computacao/Nova pasta/2020-1_aed1_
12720 2020-08-21 12:03:44,454473 186.248.79.32   192.168.0.10     FTP-DATA  1514 FTP Data: 1460 bytes (PASV) (RETR /Computacao/Nova pasta/2020-1_aed1_
12721 2020-08-21 12:03:44,454473 186.248.79.32   192.168.0.10     FTP-DATA  1514 FTP Data: 1460 bytes (PASV) (RETR /Computacao/Nova pasta/2020-1_aed1_
12722 2020-08-21 12:03:44,454473 186.248.79.32   192.168.0.10     FTP-DATA  1514 FTP Data: 1460 bytes (PASV) (RETR /Computacao/Nova pasta/2020-1_aed1_
12723 2020-08-21 12:03:44,454473 186.248.79.32   192.168.0.10     FTP-DATA  1514 FTP Data: 1460 bytes (PASV) (RETR /Computacao/Nova pasta/2020-1_aed1_
12726 2020-08-21 12:03:44,462644 186.248.79.32   192.168.0.10     FTP-DATA  1514 FTP Data: 1460 bytes (PASV) (RETR /Computacao/Nova pasta/2020-1_aed1_
12728 2020-08-21 12:03:44,465040 186.248.79.32   192.168.0.10     FTP-DATA  1514 [TCP Previous segment not captured] FTP Data: 1460 bytes (PASV) (RETR
12730 2020-08-21 12:03:44,465040 186.248.79.32   192.168.0.10     FTP-DATA  1514 FTP Data: 1460 bytes (PASV) (RETR /Computacao/Nova pasta/2020-1_aed1_
12731 2020-08-21 12:03:44,465040 186.248.79.32   192.168.0.10     FTP-DATA  1514 FTP Data: 1460 bytes (PASV) (RETR /Computacao/Nova pasta/2020-1_aed1_
12732 2020-08-21 12:03:44,465040 186.248.79.32   192.168.0.10     FTP-DATA  1514 FTP Data: 1460 bytes (PASV) (RETR /Computacao/Nova pasta/2020-1_aed1_
12733 2020-08-21 12:03:44,465040 186.248.79.32   192.168.0.10     FTP-DATA  1514 FTP Data: 1460 bytes (PASV) (RETR /Computacao/Nova pasta/2020-1_aed1_
12737 2020-08-21 12:03:44,466167 186.248.79.32   192.168.0.10     FTP-DATA   211 FTP Data: 157 bytes (PASV) (RETR /Computacao/Nova pasta/2020-1_aed1_
```

E – Porta do ftp: 21

```
Source Port: 21
Destination Port: 57848
```

Porta do ftp-data: 42915

```
Source Port: 42915
Destination Port: 57845
```

F - Servidor: Debian Usuário: anônimo

35	2020-08-20 14:12:24,238045	186.248.79.32	192.168.0.10	FTP	104	Response: 220 ProFTPD 1.3.4a Server (Debian) [172.17.0.32]
36	2020-08-20 14:12:24,238222	192.168.0.10	186.248.79.32	FTP	70	Request: USER anonymous