Networks

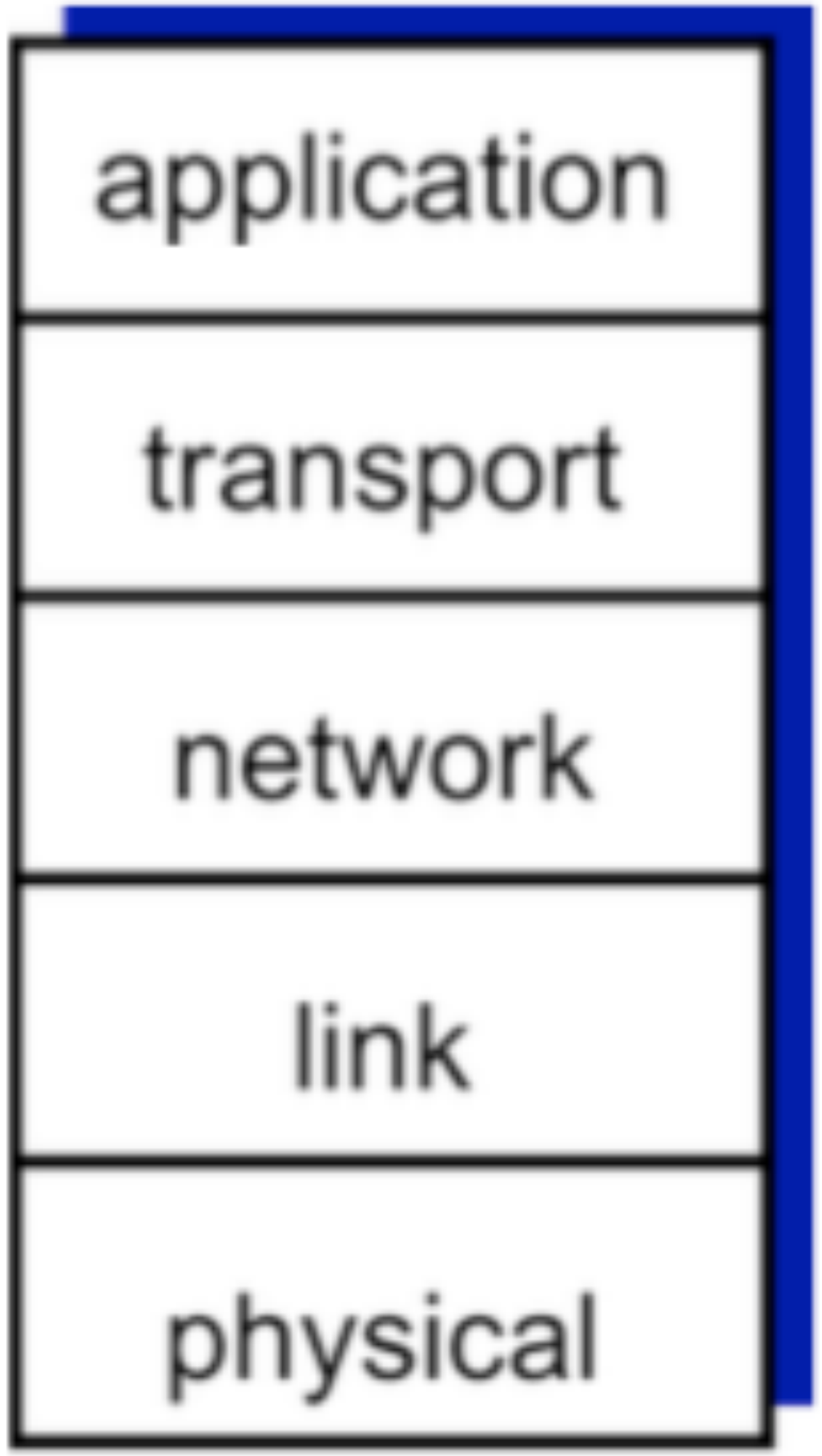
Lab5 - SMTP protocol

Lab goal:

1 - Explore SMTP protocol

2 - Send email using SMTP protocol

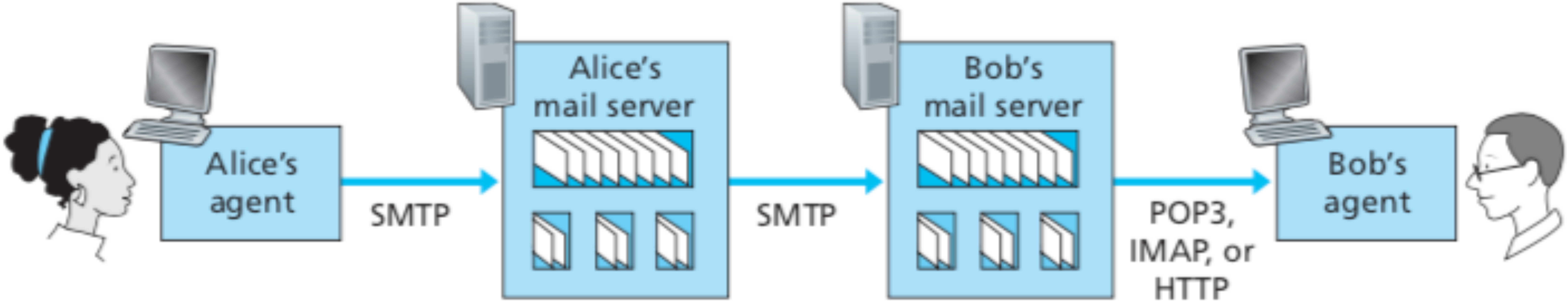
TCP/IP stack



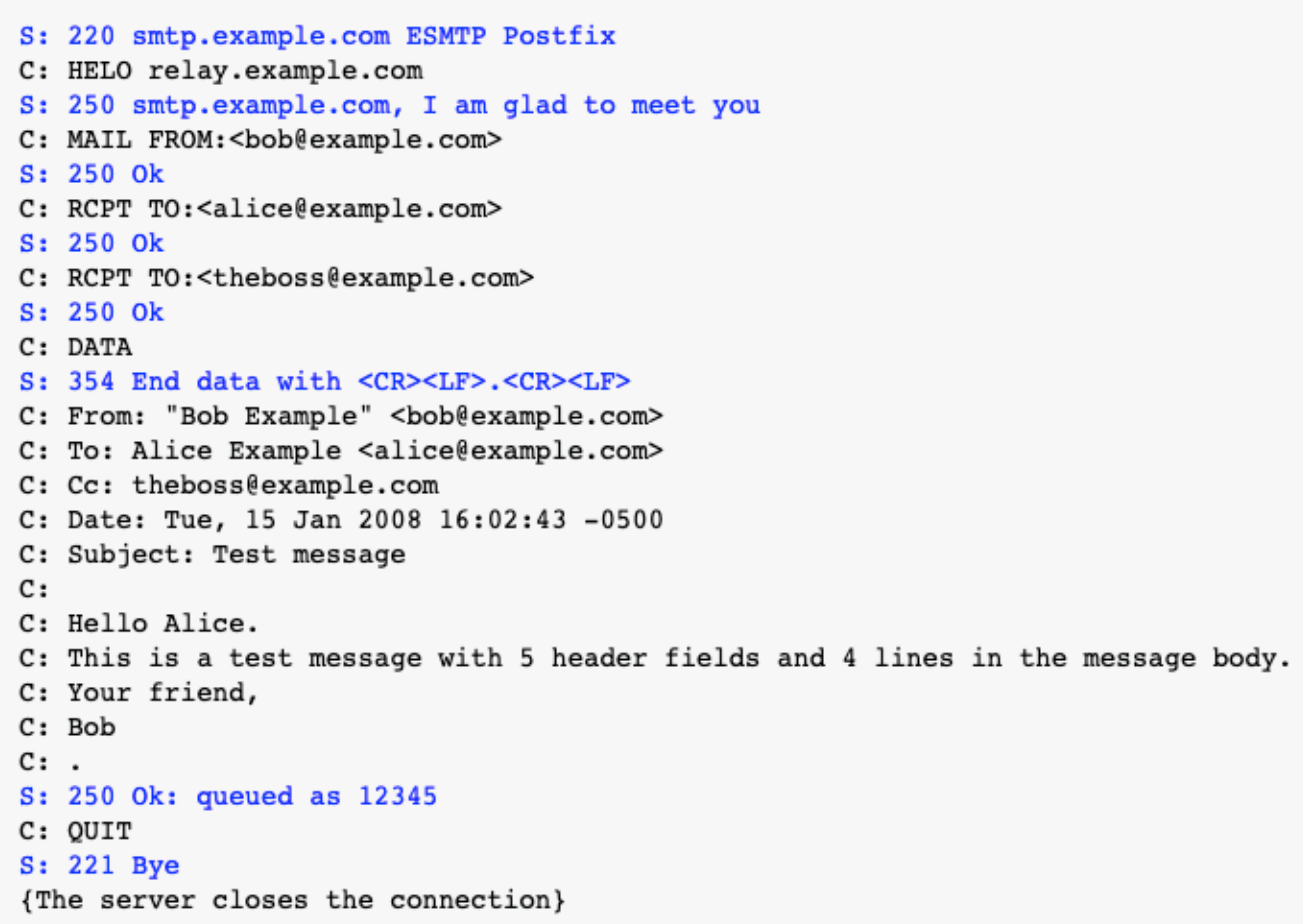
SMTP POP3 IMAP

TCP

E-mail protocols and their communicating entities



SMTP transport example



```
S: 220 smtp.example.com ESMTP Postfix
C: HELO relay.example.com
S: 250 smtp.example.com, I am glad to meet you
C: MAIL FROM:<bob@example.com>
S: 250 Ok
C: RCPT TO:<alice@example.com>
S: 250 Ok
C: RCPT TO:<theboss@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: From: "Bob Example" <bob@example.com>
C: To: Alice Example <alice@example.com>
C: Cc: theboss@example.com
C: Date: Tue, 15 Jan 2008 16:02:43 -0500
C: Subject: Test message
C:
C: Hello Alice.
C: This is a test message with 5 header fields and 4 lines in the message body.
C: Your friend,
C: Bob
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye
{The server closes the connection}
```

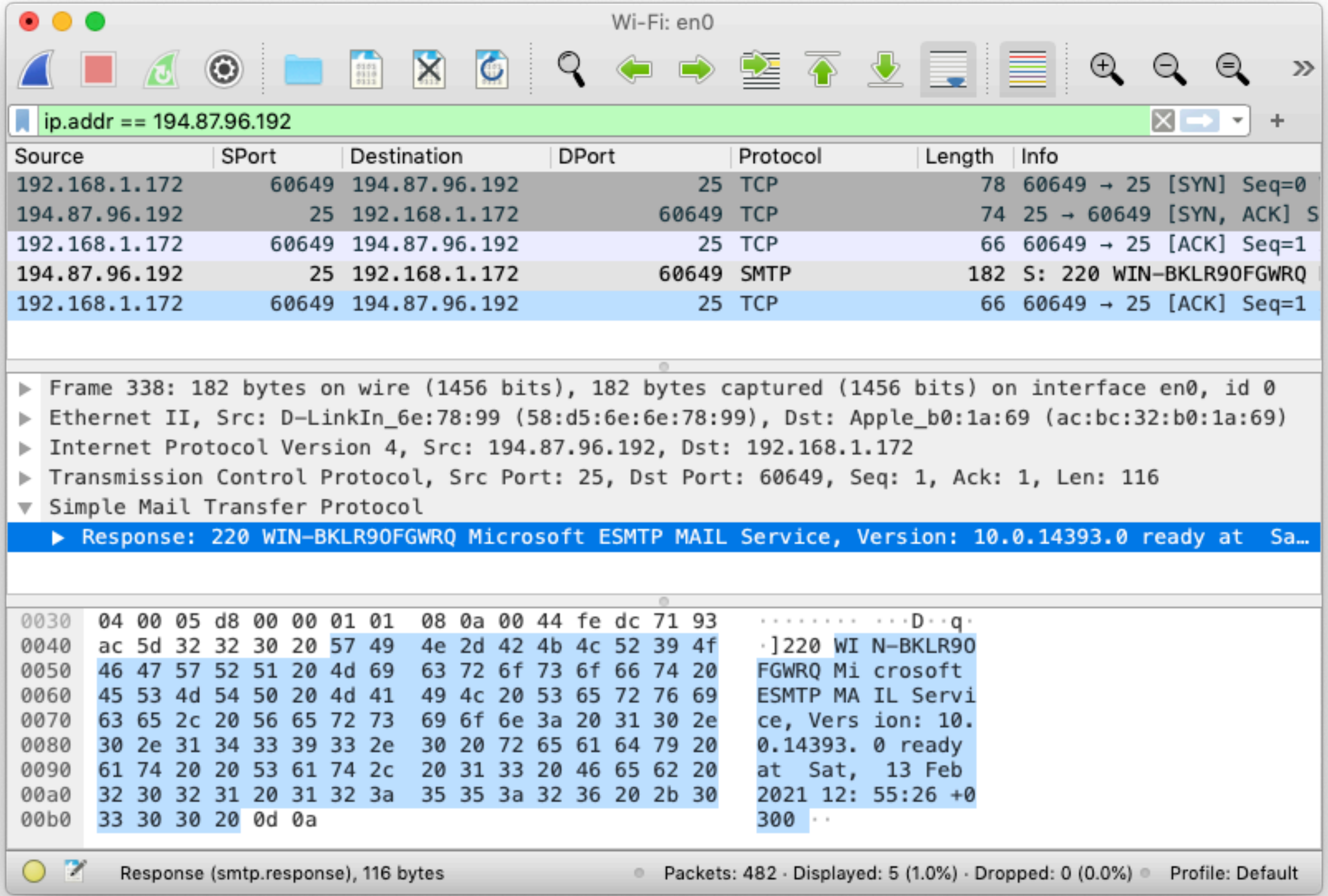
Putty

PuTTY is an SSH and telnet client, developed originally by Simon Tatham for the Windows platform. PuTTY is open source software that is available with source code and is developed and supported by a group of volunteers.

Telnet

Telnet is a network protocol that provides a command-line interface to communicate with a device. Telnet is used most often for remote management but also sometimes for the initial setup for some devices, especially network hardware such as switches and access points. Telnet is also used to manage files on a website.

telnet 194.87.96.192 25



ip.addr == 194.87.96.192

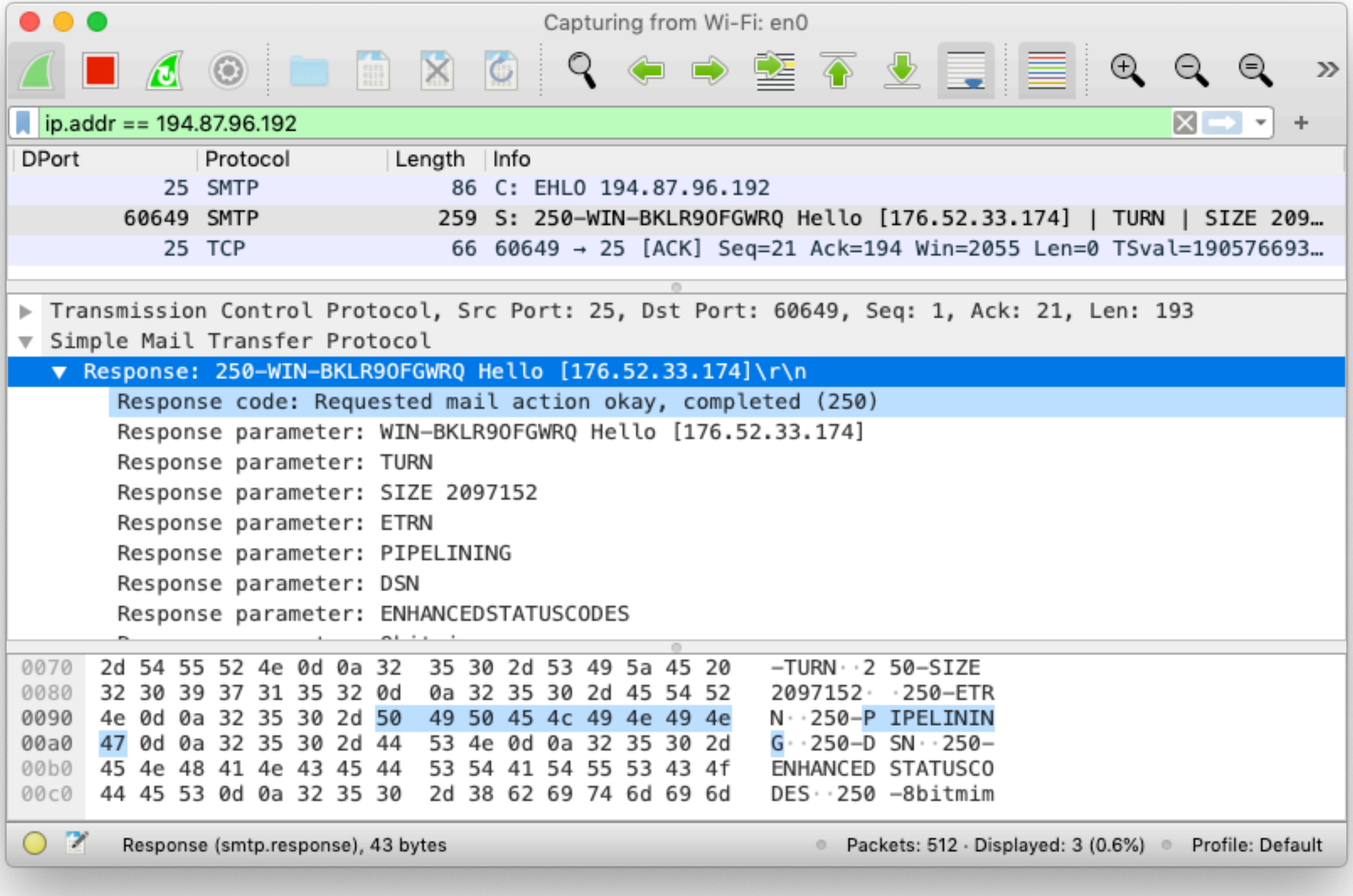
```
Source          SPort  Destination      DPort  Protocol  Length  Info
192.168.1.172   60649  194.87.96.192       25  TCP           78  60649 → 25 [SYN] Seq=0
194.87.96.192      25  192.168.1.172    60649  TCP           74  25 → 60649 [SYN, ACK] S
192.168.1.172   60649  194.87.96.192       25  TCP           66  60649 → 25 [ACK] Seq=1
194.87.96.192      25  192.168.1.172    60649  SMTP         182  S: 220 WIN-BKLR9OFGWRQ
192.168.1.172   60649  194.87.96.192       25  TCP           66  60649 → 25 [ACK] Seq=1
```

```
▶ Frame 338: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits) on interface en0, id 0
▶ Ethernet II, Src: D-LinkIn_6e:78:99 (58:d5:6e:6e:78:99), Dst: Apple_b0:1a:69 (ac:bc:32:b0:1a:69)
▶ Internet Protocol Version 4, Src: 194.87.96.192, Dst: 192.168.1.172
▶ Transmission Control Protocol, Src Port: 25, Dst Port: 60649, Seq: 1, Ack: 1, Len: 116
▼ Simple Mail Transfer Protocol
   ▶ Response: 220 WIN-BKLR9OFGWRQ Microsoft ESMTP MAIL Service, Version: 10.0.14393.0 ready at  Sa…
```

```
0030  04 00 05 d8 00 00 01 01  08 0a 00 44 fe dc 71 93   ········ ···D··q·
0040  ac 5d 32 32 30 20 57 49  4e 2d 42 4b 4c 52 39 4f   ·]220 WI N-BKLR9O
0050  46 47 57 52 51 20 4d 69  63 72 6f 73 6f 66 74 20   FGWRQ Mi crosoft 
0060  45 53 4d 54 50 20 4d 41  49 4c 20 53 65 72 76 69   ESMTP MA IL Servi
0070  63 65 2c 20 56 65 72 73  69 6f 6e 3a 20 31 30 2e   ce, Vers ion: 10.
0080  30 2e 31 34 33 39 33 2e  30 20 72 65 61 64 79 20   0.14393. 0 ready 
0090  61 74 20 20 53 61 74 2c  20 31 33 20 46 65 62 20   at  Sat,  13 Feb 
00a0  32 30 32 31 20 31 32 3a  35 35 3a 32 36 20 2b 30   2021 12: 55:26 +0
00b0  33 30 30 20 0d 0a                                  300 ··
```

Response (smtp.response), 116 bytes · Packets: 482 · Displayed: 5 (1.0%) · Dropped: 0 (0.0%) · Profile: Default

EHLO 194.87.96.192



ip.addr == 194.87.96.192

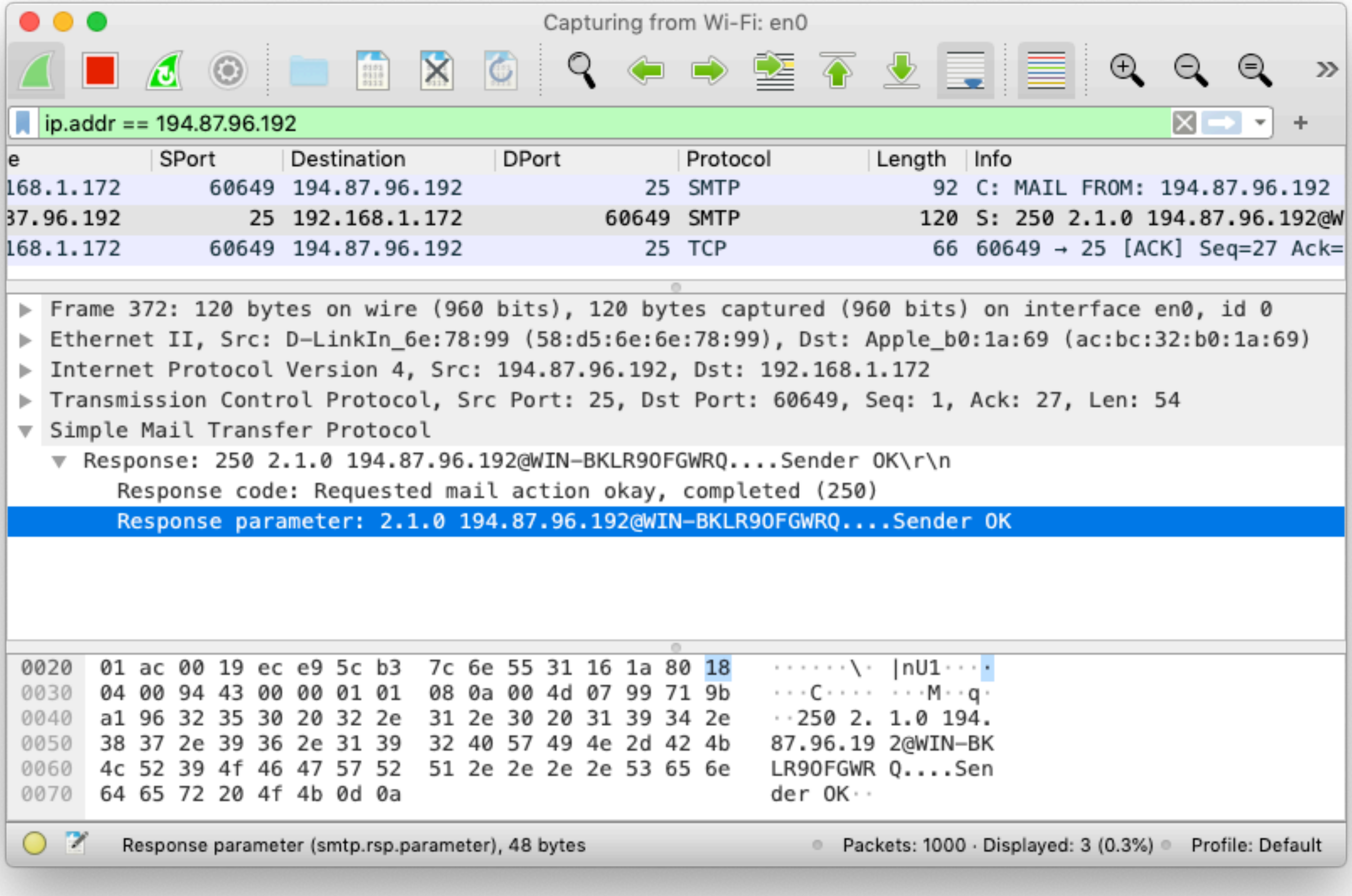
```
DPort        Protocol       Length  Info
       25  SMTP                 86  C: EHLO 194.87.96.192
    60649  SMTP                259  S: 250-WIN-BKLR9OFGWRQ Hello [176.52.33.174] | TURN | SIZE 209…
       25  TCP                  66  60649 → 25 [ACK] Seq=21 Ack=194 Win=2055 Len=0 TSval=190576693…
```

```
▶ Transmission Control Protocol, Src Port: 25, Dst Port: 60649, Seq: 1, Ack: 21, Len: 193
▼ Simple Mail Transfer Protocol
  ▼ Response: 250-WIN-BKLR9OFGWRQ Hello [176.52.33.174]\r\n
        Response code: Requested mail action okay, completed (250)
        Response parameter: WIN-BKLR9OFGWRQ Hello [176.52.33.174]
        Response parameter: TURN
        Response parameter: SIZE 2097152
        Response parameter: ETRN
        Response parameter: PIPELINING
        Response parameter: DSN
        Response parameter: ENHANCEDSTATUSCODES
```

```
0070  2d 54 55 52 4e 0d 0a 32  35 30 2d 53 49 5a 45 20   -TURN··2 50-SIZE
0080  32 30 39 37 31 35 32 0d  0a 32 35 30 2d 45 54 52   2097152· ·250-ETR
0090  4e 0d 0a 32 35 30 2d 50  49 50 45 4c 49 4e 49 4e   N··250-P IPELININ
00a0  47 0d 0a 32 35 30 2d 44  53 4e 0d 0a 32 35 30 2d   G··250-D SN··250-
00b0  45 4e 48 41 4e 43 45 44  53 54 41 54 55 53 43 4f   ENHANCED STATUSCO
00c0  44 45 53 0d 0a 32 35 30  2d 38 62 69 74 6d 69 6d   DES··250 -8bitmim
```

Response (smtp.response), 43 bytes · Packets: 512 · Displayed: 3 (0.6%) · Profile: Default

MAIL FROM: 194.87.96.192



ip.addr == 194.87.96.192

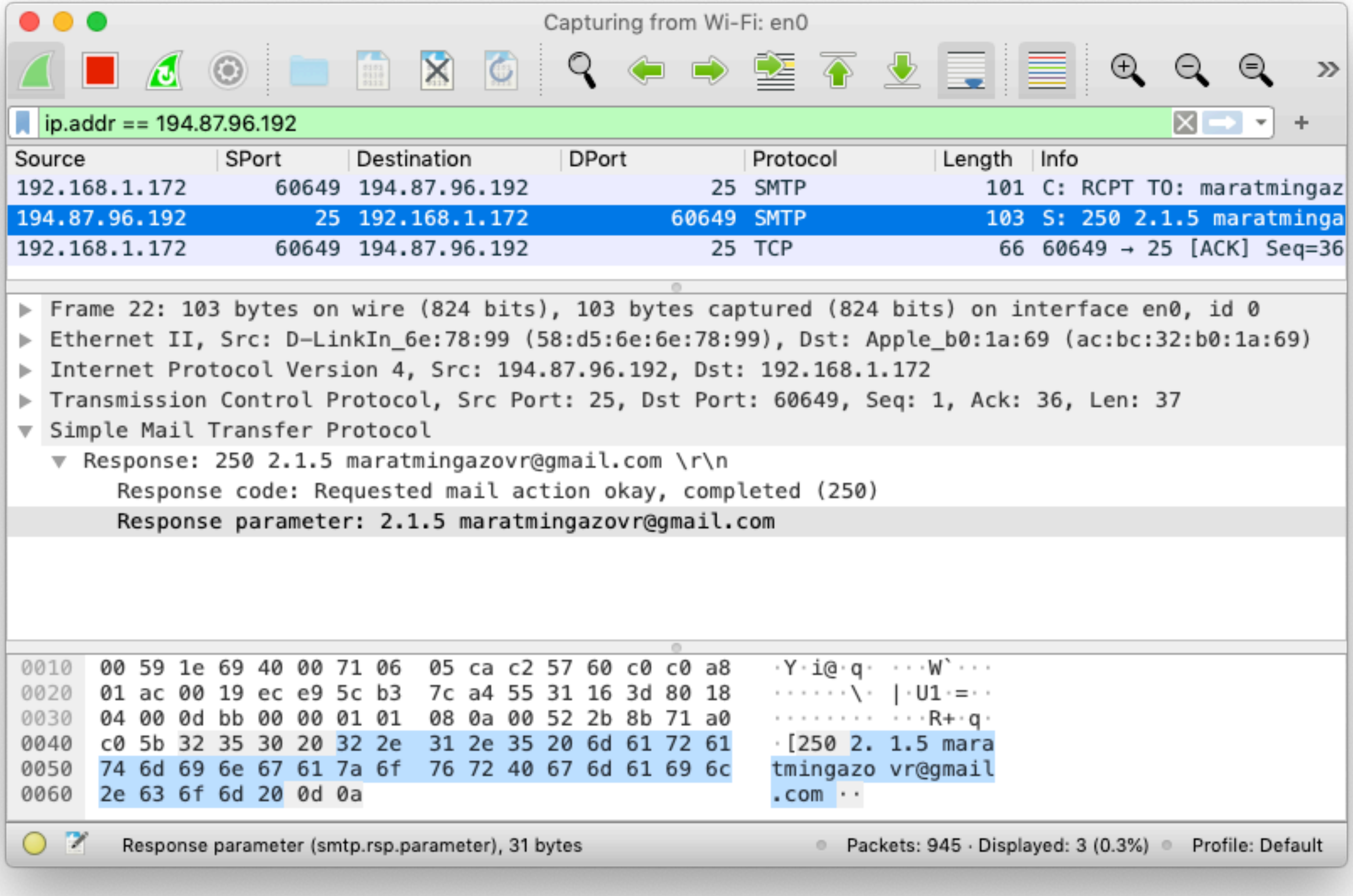
```
e              SPort  Destination     DPort  Protocol  Length  Info
168.1.172      60649  194.87.96.192      25  SMTP          92  C: MAIL FROM: 194.87.96.192
37.96.192         25  192.168.1.172   60649  SMTP         120  S: 250 2.1.0 194.87.96.192@W
168.1.172      60649  194.87.96.192      25  TCP           66  60649 → 25 [ACK] Seq=27 Ack=
```

```
▶ Frame 372: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface en0, id 0
▶ Ethernet II, Src: D-LinkIn_6e:78:99 (58:d5:6e:6e:78:99), Dst: Apple_b0:1a:69 (ac:bc:32:b0:1a:69)
▶ Internet Protocol Version 4, Src: 194.87.96.192, Dst: 192.168.1.172
▶ Transmission Control Protocol, Src Port: 25, Dst Port: 60649, Seq: 1, Ack: 27, Len: 54
▼ Simple Mail Transfer Protocol
  ▼ Response: 250 2.1.0 194.87.96.192@WIN-BKLR9OFGWRQ....Sender OK\r\n
      Response code: Requested mail action okay, completed (250)
      Response parameter: 2.1.0 194.87.96.192@WIN-BKLR9OFGWRQ....Sender OK
```

```
0020  01 ac 00 19 ec e9 5c b3  7c 6e 55 31 16 1a 80 18   ······\· |nU1···
0030  04 00 94 43 00 00 01 01  08 0a 00 4d 07 99 71 9b   ···C···· ···M··q·
0040  a1 96 32 35 30 20 32 2e  31 2e 30 20 31 39 34 2e   ··250 2. 1.0 194.
0050  38 37 2e 39 36 2e 31 39  32 40 57 49 4e 2d 42 4b   87.96.19 2@WIN-BK
0060  4c 52 39 4f 46 47 57 52  51 2e 2e 2e 2e 53 65 6e   LR9OFGWR Q....Sen
0070  64 65 72 20 4f 4b 0d 0a                            der OK··
```

Response parameter (smtp.rsp.parameter), 48 bytes · Packets: 1000 · Displayed: 3 (0.3%) · Profile: Default

RCPT TO: maratmingazovr@gmail.com



Capturing from Wi-Fi: en0

ip.addr == 194.87.96.192

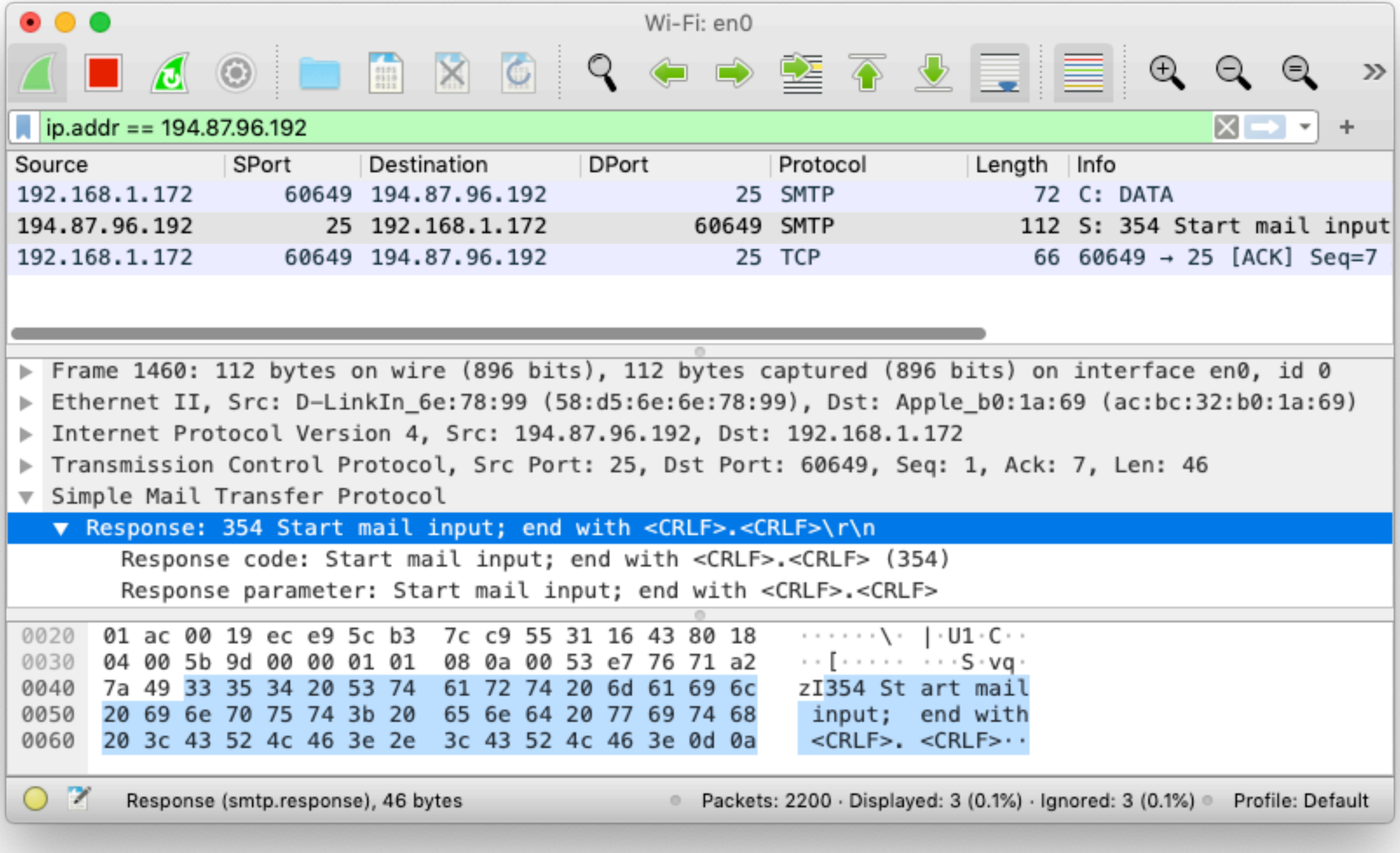
Source	SPort	Destination	DPort	Protocol	Length	Info
192.168.1.172	60649	194.87.96.192	25	SMTP	101	C: RCPT TO: maratmingaz
194.87.96.192	25	192.168.1.172	60649	SMTP	103	S: 250 2.1.5 maratminga
192.168.1.172	60649	194.87.96.192	25	TCP	66	60649 → 25 [ACK] Seq=36

```
▶ Frame 22: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface en0, id 0
▶ Ethernet II, Src: D-LinkIn_6e:78:99 (58:d5:6e:6e:78:99), Dst: Apple_b0:1a:69 (ac:bc:32:b0:1a:69)
▶ Internet Protocol Version 4, Src: 194.87.96.192, Dst: 192.168.1.172
▶ Transmission Control Protocol, Src Port: 25, Dst Port: 60649, Seq: 1, Ack: 36, Len: 37
▼ Simple Mail Transfer Protocol
  ▼ Response: 250 2.1.5 maratmingazovr@gmail.com \r\n
      Response code: Requested mail action okay, completed (250)
      Response parameter: 2.1.5 maratmingazovr@gmail.com
```

```
0010  00 59 1e 69 40 00 71 06  05 ca c2 57 60 c0 c0 a8   ·Y·i@·q· ···W`···
0020  01 ac 00 19 ec e9 5c b3  7c a4 55 31 16 3d 80 18   ······\· |·U1·=··
0030  04 00 0d bb 00 00 01 01  08 0a 00 52 2b 8b 71 a0   ········ ···R+·q·
0040  c0 5b 32 35 30 20 32 2e  31 2e 35 20 6d 61 72 61   ·[250 2. 1.5 mara
0050  74 6d 69 6e 67 61 7a 6f  76 72 40 67 6d 61 69 6c   tmingazo vr@gmail
0060  2e 63 6f 6d 20 0d 0a                               .com ··
```

Response parameter (smtp.rsp.parameter), 31 bytes · Packets: 945 · Displayed: 3 (0.3%) · Profile: Default

DATA



```
ip.addr == 194.87.96.192
```

```
Source          SPort  Destination      DPort  Protocol  Length  Info
192.168.1.172   60649  194.87.96.192       25  SMTP          72  C: DATA
194.87.96.192      25  192.168.1.172    60649  SMTP         112  S: 354 Start mail input
192.168.1.172   60649  194.87.96.192       25  TCP           66  60649 → 25 [ACK] Seq=7
```

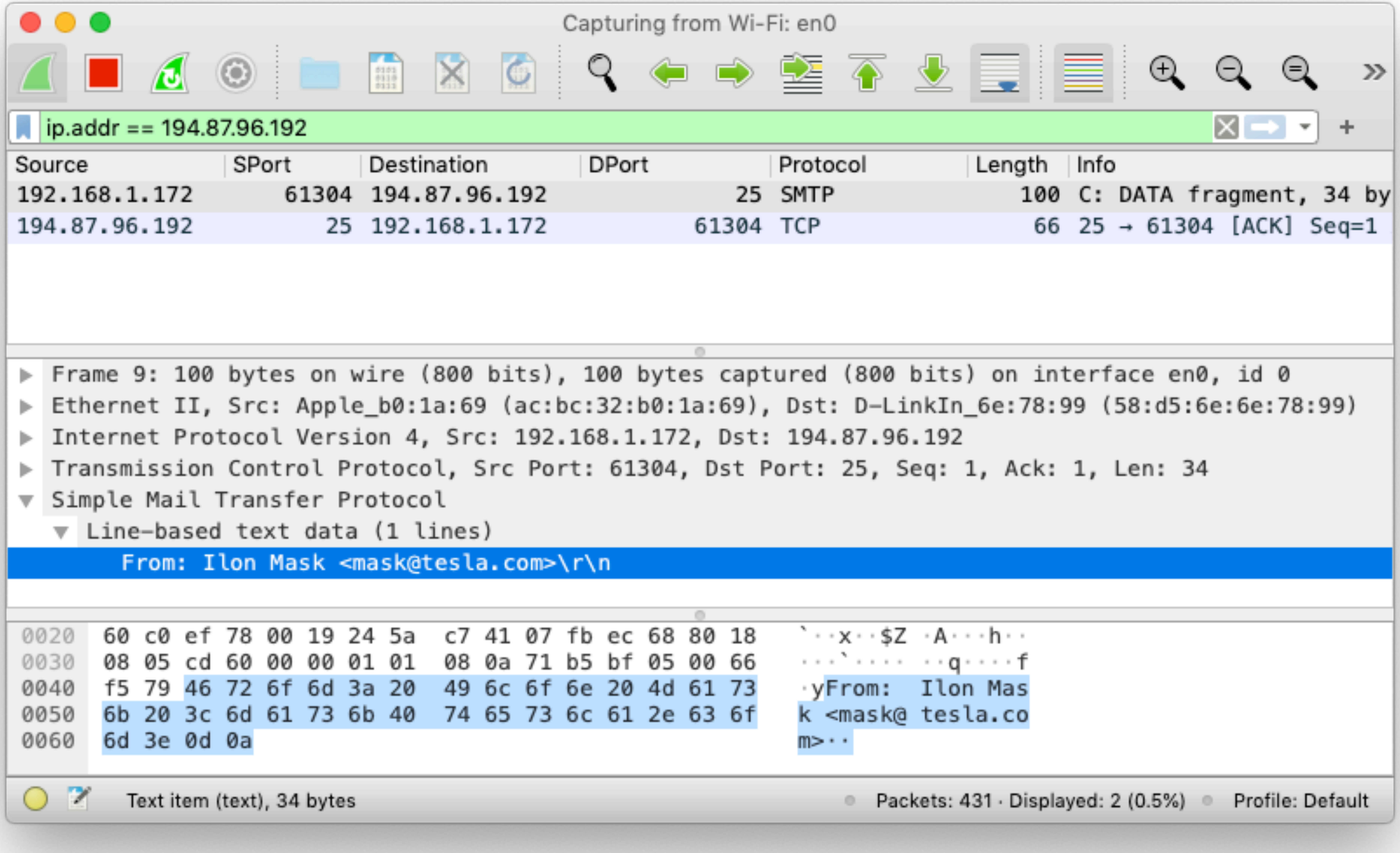
```
▶ Frame 1460: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface en0, id 0
▶ Ethernet II, Src: D-LinkIn_6e:78:99 (58:d5:6e:6e:78:99), Dst: Apple_b0:1a:69 (ac:bc:32:b0:1a:69)
▶ Internet Protocol Version 4, Src: 194.87.96.192, Dst: 192.168.1.172
▶ Transmission Control Protocol, Src Port: 25, Dst Port: 60649, Seq: 1, Ack: 7, Len: 46
▼ Simple Mail Transfer Protocol
  ▼ Response: 354 Start mail input; end with <CRLF>.<CRLF>\r\n
      Response code: Start mail input; end with <CRLF>.<CRLF> (354)
      Response parameter: Start mail input; end with <CRLF>.<CRLF>
```

```
0020  01 ac 00 19 ec e9 5c b3  7c c9 55 31 16 43 80 18   ······\· |·U1·C··
0030  04 00 5b 9d 00 00 01 01  08 0a 00 53 e7 76 71 a2   ··[····· ···S·vq·
0040  7a 49 33 35 34 20 53 74  61 72 74 20 6d 61 69 6c   zI354 St art mail
0050  20 69 6e 70 75 74 3b 20  65 6e 64 20 77 69 74 68    input;  end with
0060  20 3c 43 52 4c 46 3e 2e  3c 43 52 4c 46 3e 0d 0a    <CRLF>. <CRLF>··
```

Response (smtp.response), 46 bytes · Packets: 2200 · Displayed: 3 (0.1%) · Ignored: 3 (0.1%) · Profile: Default

From: Ilon Mask <mask@tesla.com>

Dangerous



ip.addr == 194.87.96.192

```
Source          SPort  Destination     DPort  Protocol   Length  Info
192.168.1.172   61304  194.87.96.192      25  SMTP          100  C: DATA fragment, 34 by
194.87.96.192      25  192.168.1.172   61304  TCP            66  25 → 61304 [ACK] Seq=1
```

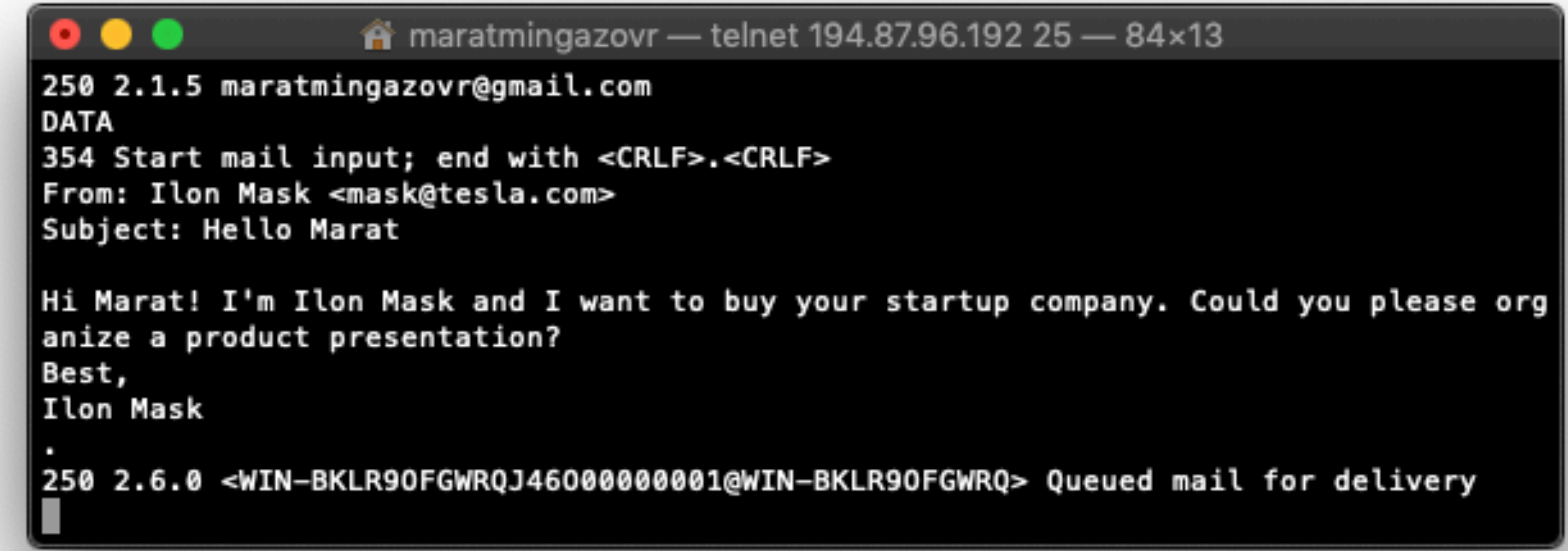
```
▶ Frame 9: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_b0:1a:69 (ac:bc:32:b0:1a:69), Dst: D-LinkIn_6e:78:99 (58:d5:6e:6e:78:99)
▶ Internet Protocol Version 4, Src: 192.168.1.172, Dst: 194.87.96.192
▶ Transmission Control Protocol, Src Port: 61304, Dst Port: 25, Seq: 1, Ack: 1, Len: 34
▼ Simple Mail Transfer Protocol
  ▼ Line-based text data (1 lines)
      From: Ilon Mask <mask@tesla.com>\r\n
```

```
0020  60 c0 ef 78 00 19 24 5a  c7 41 07 fb ec 68 80 18   `··x··$Z ·A···h··
0030  08 05 cd 60 00 00 01 01  08 0a 71 b5 bf 05 00 66   ···`···· ··q···f
0040  f5 79 46 72 6f 6d 3a 20  49 6c 6f 6e 20 4d 61 73   ·yFrom:  Ilon Mas
0050  6b 20 3c 6d 61 73 6b 40  74 65 73 6c 61 2e 63 6f   k <mask@ tesla.co
0060  6d 3e 0d 0a                                        m>··
```

Text item (text), 34 bytes · Packets: 431 · Displayed: 2 (0.5%) · Profile: Default

From: Ilon Mask <mask@tesla.com>
Subject: Hello Marat

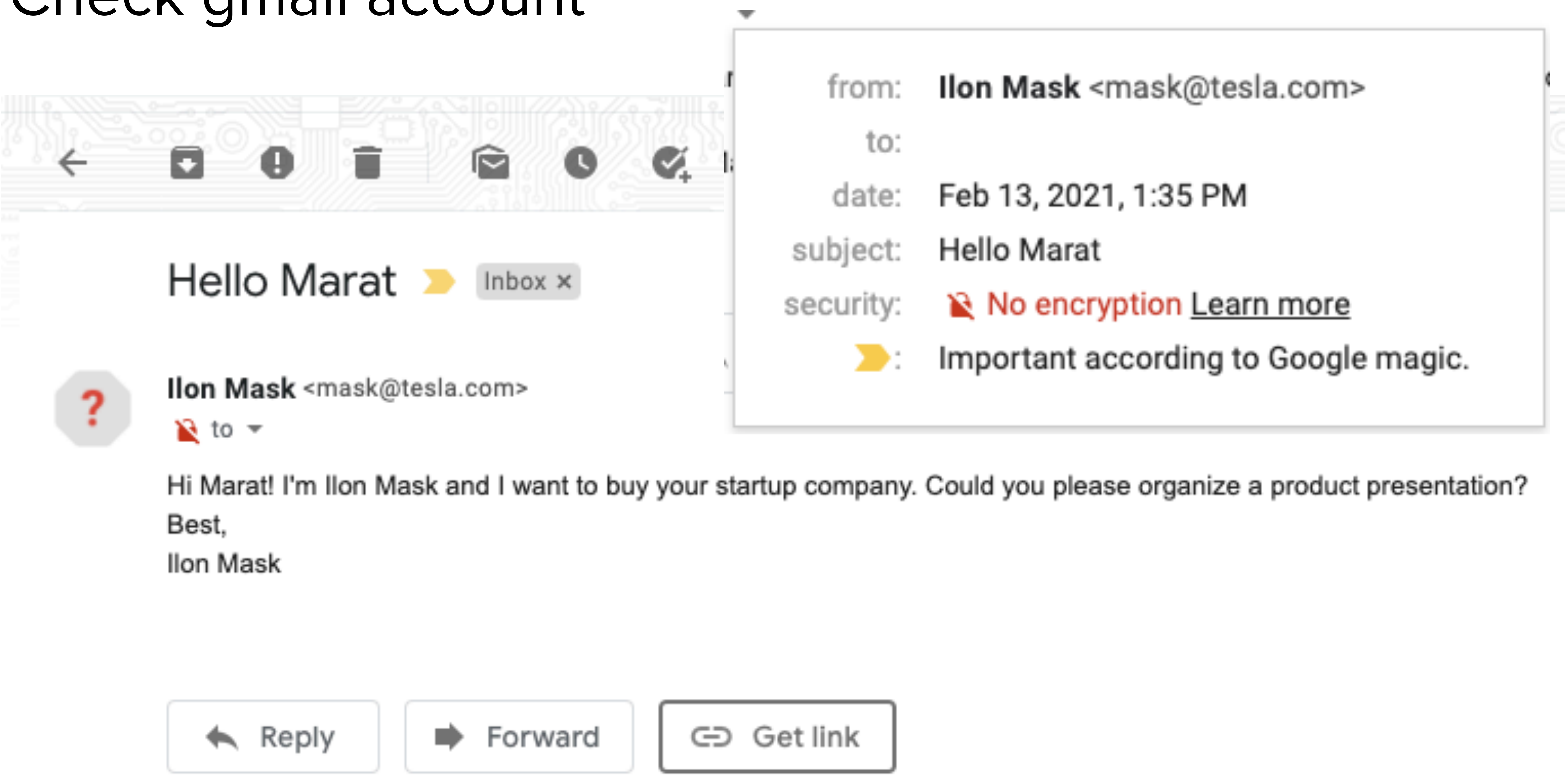
Hi Marat! I'm Ilon Mask and I want to buy your startup company. Could you please organize a product presentation?
Best,
Ilon Mask
.



```
250 2.1.5 maratmingazovr@gmail.com
DATA
354 Start mail input; end with <CRLF>.<CRLF>
From: Ilon Mask <mask@tesla.com>
Subject: Hello Marat

Hi Marat! I'm Ilon Mask and I want to buy your startup company. Could you please org
anize a product presentation?
Best,
Ilon Mask
.
250 2.6.0 <WIN-BKLR9OFGWRQJ46O00000001@WIN-BKLR9OFGWRQ> Queued mail for delivery
```

Check gmail account



from: **Ilon Mask** <mask@tesla.com>

to:

date: Feb 13, 2021, 1:35 PM

subject: Hello Marat

security: No encryption Learn more

: Important according to Google magic.

Hello Marat

Ilon Mask <mask@tesla.com>

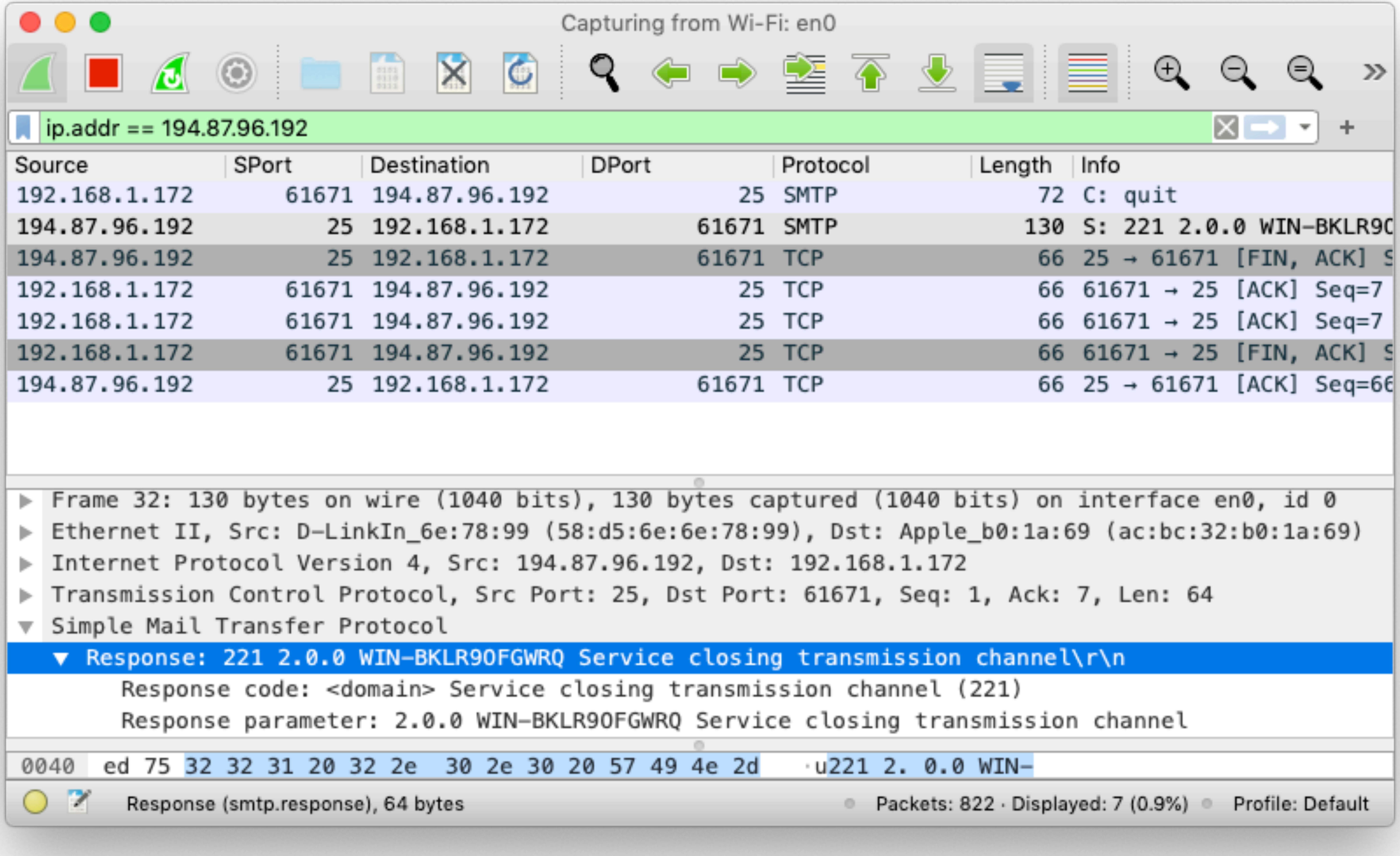
to

Hi Marat! I'm Ilon Mask and I want to buy your startup company. Could you please organize a product presentation?

Best,

Ilon Mask

quit



```
ip.addr == 194.87.96.192
```

```
Source            SPort  Destination     DPort  Protocol  Length  Info
192.168.1.172     61671  194.87.96.192      25  SMTP          72  C: quit
194.87.96.192        25  192.168.1.172   61671  SMTP         130  S: 221 2.0.0 WIN-BKLR9C
194.87.96.192        25  192.168.1.172   61671  TCP           66  25 → 61671 [FIN, ACK] S
192.168.1.172     61671  194.87.96.192      25  TCP           66  61671 → 25 [ACK] Seq=7
192.168.1.172     61671  194.87.96.192      25  TCP           66  61671 → 25 [ACK] Seq=7
192.168.1.172     61671  194.87.96.192      25  TCP           66  61671 → 25 [FIN, ACK] S
194.87.96.192        25  192.168.1.172   61671  TCP           66  25 → 61671 [ACK] Seq=66
```

```
▶ Frame 32: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface en0, id 0
▶ Ethernet II, Src: D-LinkIn_6e:78:99 (58:d5:6e:6e:78:99), Dst: Apple_b0:1a:69 (ac:bc:32:b0:1a:69)
▶ Internet Protocol Version 4, Src: 194.87.96.192, Dst: 192.168.1.172
▶ Transmission Control Protocol, Src Port: 25, Dst Port: 61671, Seq: 1, Ack: 7, Len: 64
▼ Simple Mail Transfer Protocol
  ▼ Response: 221 2.0.0 WIN-BKLR9OFGWRQ Service closing transmission channel\r\n
        Response code: <domain> Service closing transmission channel (221)
        Response parameter: 2.0.0 WIN-BKLR9OFGWRQ Service closing transmission channel
```

```
0040  ed 75 32 32 31 20 32 2e  30 2e 30 20 57 49 4e 2d   ·u221 2. 0.0 WIN-
```

Response (smtp.response), 64 bytes · Packets: 822 · Displayed: 7 (0.9%) · Profile: Default