CIS.600
Internet of Things: Security and Privacy

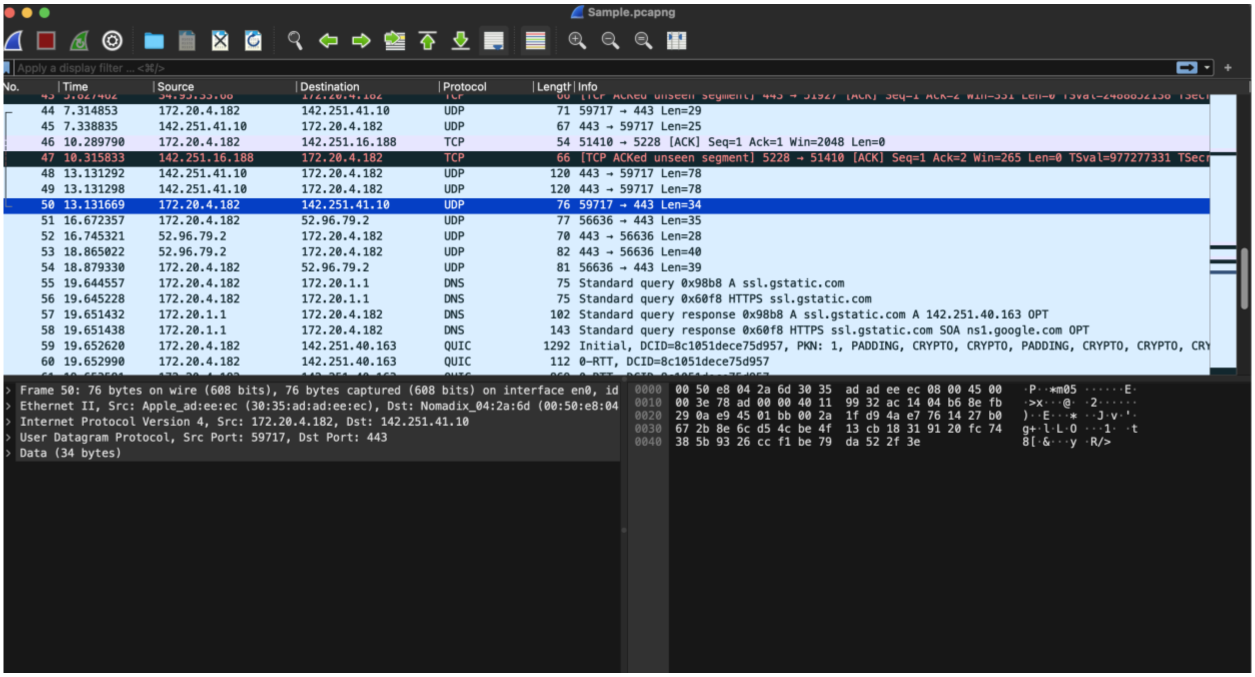
IN CLASS EXERCISE

ROHAN BHOWMICK
SUID: 658096139
rbhowmic@syr.edu

Exercise: 1

1) **How many packets are there?**
- As shown in Wireshark, there are 78 packets.

2) **What networking protocol is used?**
- The protocols in use are:
  a) UDP
  b) TCP



```
No. | Time      | Source         | Destination    | Protocol | Length | Info
 44  7.314853   172.20.4.182     142.251.41.10    UDP         71 59717 → 443 Len=29
 45  7.338835   142.251.41.10    172.20.4.182     UDP         67 443 → 59717 Len=25
 46  10.289790  172.20.4.182     142.251.16.188   TCP         54 51410 → 5228 [ACK] Seq=1 Ack=1 Win=2048 Len=0
 47  10.315833  142.251.16.188   172.20.4.182     TCP         66 [TCP ACKed unseen segment] 5228 → 51410 [ACK] Seq=1 Ack=2 Win=265 Len=0 TSval=977277331 TSecr
 48  13.131292  142.251.41.10    172.20.4.182     UDP        120 443 → 59717 Len=78
 49  13.131298  142.251.41.10    172.20.4.182     UDP        120 443 → 59717 Len=78
 50  13.131669  172.20.4.182     142.251.41.10    UDP         76 59717 → 443 Len=34
 51  16.672357  172.20.4.182     52.96.79.2       UDP         77 56636 → 443 Len=35
 52  16.745321  52.96.79.2       172.20.4.182     UDP         70 443 → 56636 Len=28
 53  18.865022  52.96.79.2       172.20.4.182     UDP         82 443 → 56636 Len=40
 54  18.879330  172.20.4.182     52.96.79.2       UDP         81 56636 → 443 Len=39
 55  19.644557  172.20.4.182     172.20.1.1       DNS         75 Standard query 0x98b8 A ssl.gstatic.com
 56  19.645228  172.20.4.182     172.20.1.1       DNS         75 Standard query 0x60f8 HTTPS ssl.gstatic.com
 57  19.651432  172.20.1.1       172.20.4.182     DNS        102 Standard query response 0x98b8 A ssl.gstatic.com A 142.251.40.163 OPT
 58  19.651438  172.20.1.1       172.20.4.182     DNS        143 Standard query response 0x60f8 HTTPS ssl.gstatic.com SOA ns1.google.com OPT
 59  19.652620  172.20.4.182     142.251.40.163   QUIC      1292 Initial, DCID=8c1051dece75d957, PKN: 1, PADDING, CRYPTO, CRYPTO, PADDING, CRYPTO, CRYPTO, CRY
 60  19.652990  172.20.4.182     142.251.40.163   QUIC       112 0-RTT, DCID=8c1051dece75d957
```

```
> Frame 50: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface en0, id
> Ethernet II, Src: Apple_ad:ee:ec (30:35:ad:ad:ee:ec), Dst: Nomadix_04:2a:6d (00:50:e8:04
> Internet Protocol Version 4, Src: 172.20.4.182, Dst: 142.251.41.10
> User Datagram Protocol, Src Port: 59717, Dst Port: 443
> Data (34 bytes)
```

```
0000  00 50 e8 04 2a 6d 30 35  ad ad ee ec 08 00 45 00   ·P··*m05 ······E·
0010  00 3e 78 ad 00 00 40 11  99 32 ac 14 04 b6 8e fb   ·>x···@· ·2······
0020  29 0a e9 45 01 bb 00 2a  1f d9 4a e7 76 14 27 b0   )··E···* ··J·v·'·
0030  67 2b 8e 6c d5 4c be 4f  13 cb 18 31 91 20 fc 74   g+·l·L·O ···1· ·t
0040  38 5b 93 26 cc f1 be 79  da 52 2f 3e               8[·&···y ·R/>
```

Referring the image above, source IP address and destination IP address can be observed.
For packet number- 50:

3) **What is the source IP address?**
- The source IP address is: 172.20.4.182

4) **What is the destination IP address?**
- The destination IP address is: 142.251.41.10

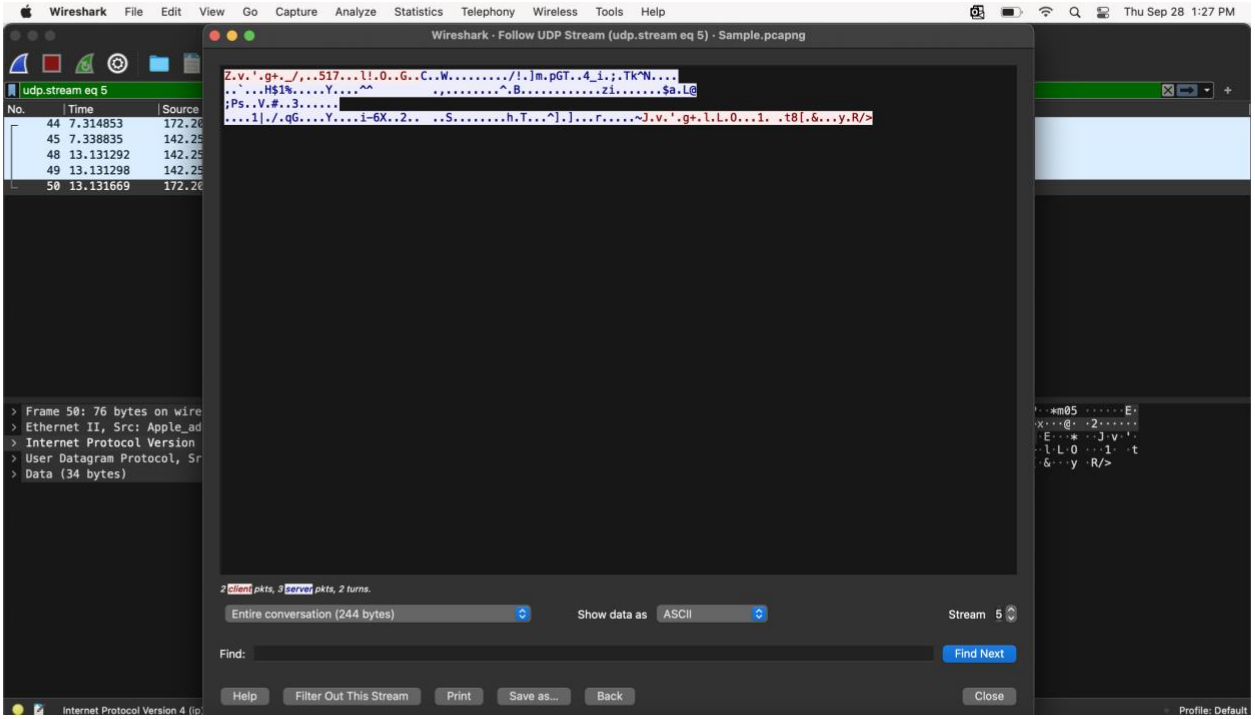
5) **What port number is the source using to communicate with the destination (or what port number is the destination listening on)?**
- The destination port number is: 443.

6) **Do you notice the "three-way handshake"?**
- No, there appears to be no three-way handshake present in this given case.

Exercise 2:

Reconstructing a conversation • Click on a packet (it will be highlighted in blue) • Right-click on packet • Go to "Follow" • Follow one of the following streams depending on protocol (UDP Stream is most common)

- **Refer the image below:**



Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Thu Sep 28 1:27 PM
Wireshark · Follow UDP Stream (udp.stream eq 5) · Sample.pcapng
udp.stream eq 5
Help
Filter Out This Stream
Print
Save as...
Back
Close
Find Next
Profile: Default

```
No.  Time        Source
 44  7.314853    172.20
 45  7.338835    142.25
 48  13.131292   142.25
 49  13.131298   142.25
 50  13.131669   172.20
```

```
Z.v.'.g+._/,..517...l!.O..G..C..W........./!.]m.pGT..4_i.;.Tk^N....
..`...H$1%.....Y....^^        .,........^.B............zi.......$a.L@
;Ps..V.#..3......
....1|./.qG....Y....i-6X..2..  ..S........h.T...^].]...r.....~J.v.'.g+.l.L.O...1. .t8[.&...y.R/>
```

```
> Frame 50: 76 bytes on wire
> Ethernet II, Src: Apple_ad
> Internet Protocol Version
> User Datagram Protocol, Sr
> Data (34 bytes)
```

2 client pkts, 3 server pkts, 2 turns.

Entire conversation (244 bytes)

Show data as ASCII

Stream 5

Find:

Internet Protocol Version 4 (ip

Conversation in text:

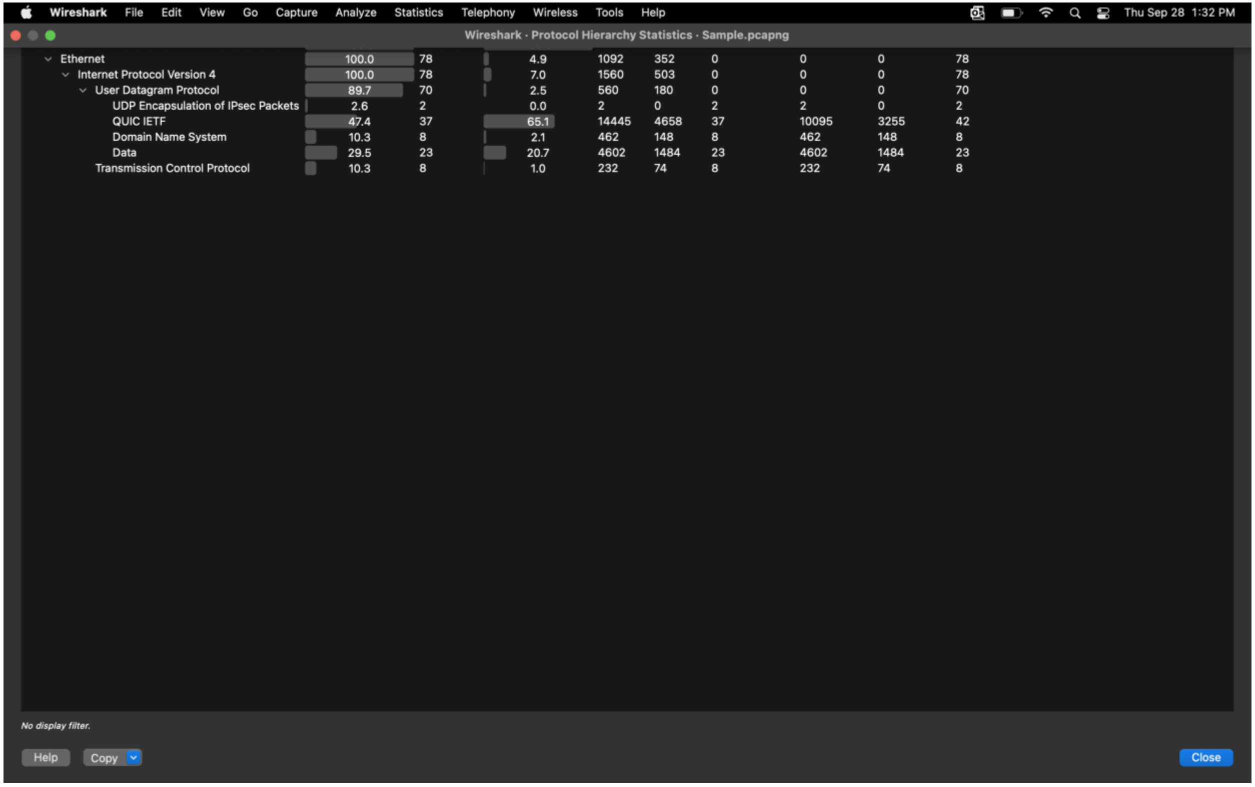
Z.v.'.g+._/,..517...l!.O..G..C..W........./!.]m.pGT..4_i.;.Tk^N....
..`...H$1%.....Y....^^ .,........^.B............zi.......$a.L@
;Ps..V.#..3......
....1|./.qG....Y....i-6X..2.. ..S........h.T...^].]...r.....~J.v.'.g+.l.L.O...1. .t8[.&...y.R/>

Exercise 3:

Finding transmission protocols
• To see all protocols in a Wireshark capture, you can go to Statistics > Protocol Hierarchy. This will show a list of all protocols, along with the number of packets and bytes for each protocol.
• You can also examine capture file properties by going to Statistics > Capture File Properties. This will show general information about the PCAP file, including the first and last packets, timestamps, and the total number of packets.
• To filter to a particular stream, you can select a packet in the packet list and then select the menu item Analyze → Follow → TCP Stream.

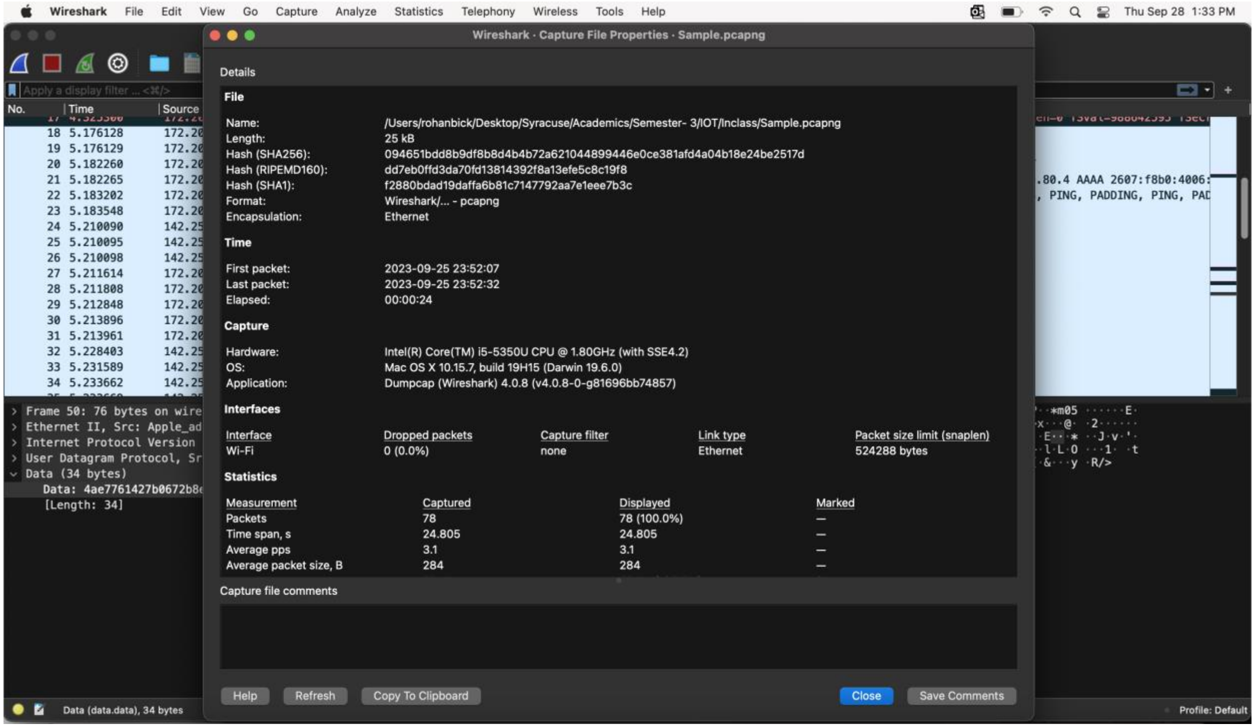
- **You can also find packets by selecting Edit → Find Packet in the main menu.**

  - **Seeing all protocols in a Wireshark capture:**


Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Thu Sep 28 1:32 PM
Wireshark · Protocol Hierarchy Statistics · Sample.pcapng
No display filter.
Help
Copy
Close

```
∨ Ethernet                              100.0  78    4.9   1092   352   0    0      0     78
  ∨ Internet Protocol Version 4         100.0  78    7.0   1560   503   0    0      0     78
    ∨ User Datagram Protocol             89.7  70    2.5    560   180   0    0      0     70
        UDP Encapsulation of IPsec Packets 2.6  2    0.0      2     0   2    2      0      2
        QUIC IETF                        47.4  37   65.1  14445  4658  37  10095  3255    42
        Domain Name System               10.3   8    2.1    462   148   8  462    148      8
        Data                             29.5  23   20.7   4602  1484  23  4602   1484     23
      Transmission Control Protocol      10.3   8    1.0    232    74   8  232     74       8
```

  - **Examining capture file properties:**


Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Thu Sep 28 1:33 PM
Wireshark · Capture File Properties · Sample.pcapng
Apply a display filter ... <⌘/>
Data (data.data), 34 bytes
Profile: Default
Help
Refresh
Copy To Clipboard
Close
Save Comments

Details

File

Name:	/Users/rohanbick/Desktop/Syracuse/Academics/Semester- 3/IOT/Inclass/Sample.pcapng
Length:	25 kB
Hash (SHA256):	094651bdd8b9df8b8d4b4b72a621044899446e0ce381afd4a04b18e24be2517d
Hash (RIPEMD160):	dd7eb0ffd3da70fd13814392f8a13efe5c8c19f8
Hash (SHA1):	f2880bdad19daffa6b81c7147792aa7e1eee7b3c
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2023-09-25 23:52:07
Last packet:	2023-09-25 23:52:32
Elapsed:	00:00:24

Capture

Hardware:	Intel(R) Core(TM) i5-5350U CPU @ 1.80GHz (with SSE4.2)
OS:	Mac OS X 10.15.7, build 19H15 (Darwin 19.6.0)
Application:	Dumpcap (Wireshark) 4.0.8 (v4.0.8-0-g81696bb74857)

Interfaces

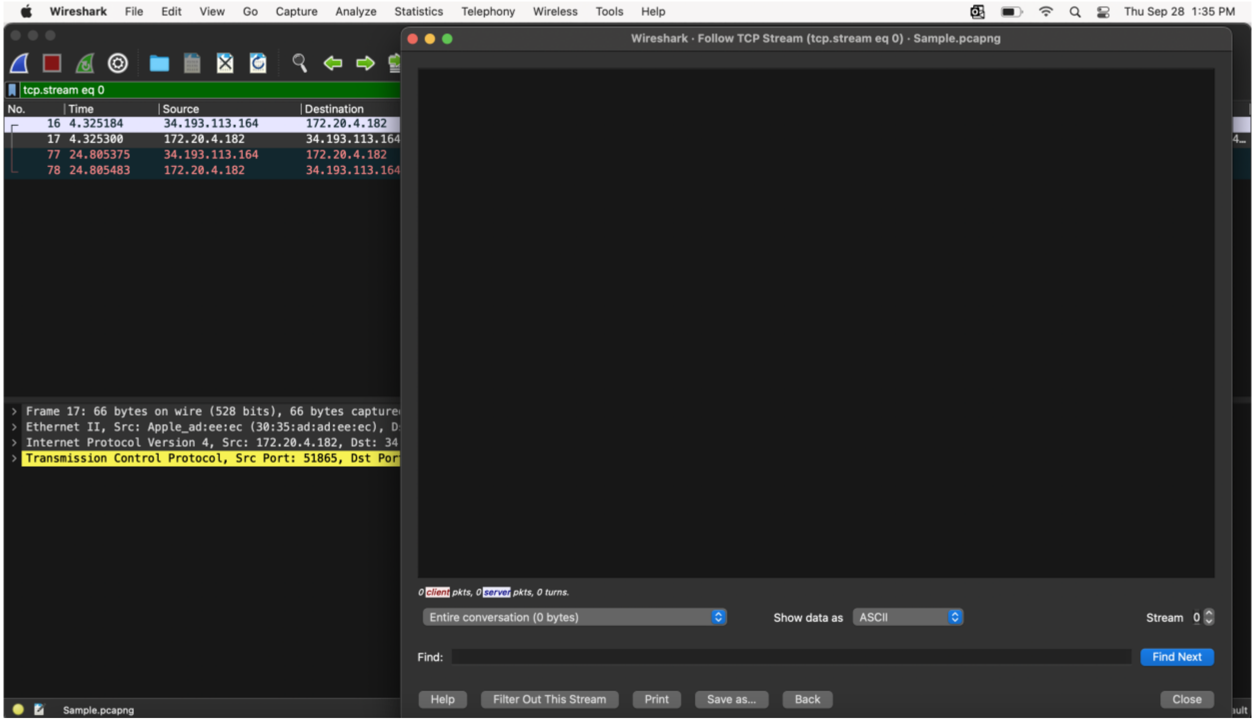
Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Wi-Fi	0 (0.0%)	none	Ethernet	524288 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	78	78 (100.0%)	—
Time span, s	24.805	24.805	—
Average pps	3.1	3.1	—
Average packet size, B	284	284	—

Capture file comments

- **Filtering to a particular stream using Analyze:**



tcp.stream eq 0

```
No.   Time       Source          Destination
   16 4.325184   34.193.113.164  172.20.4.182
   17 4.325300   172.20.4.182    34.193.113.164
   77 24.805375  34.193.113.164  172.20.4.182
   78 24.805483  172.20.4.182    34.193.113.164
```

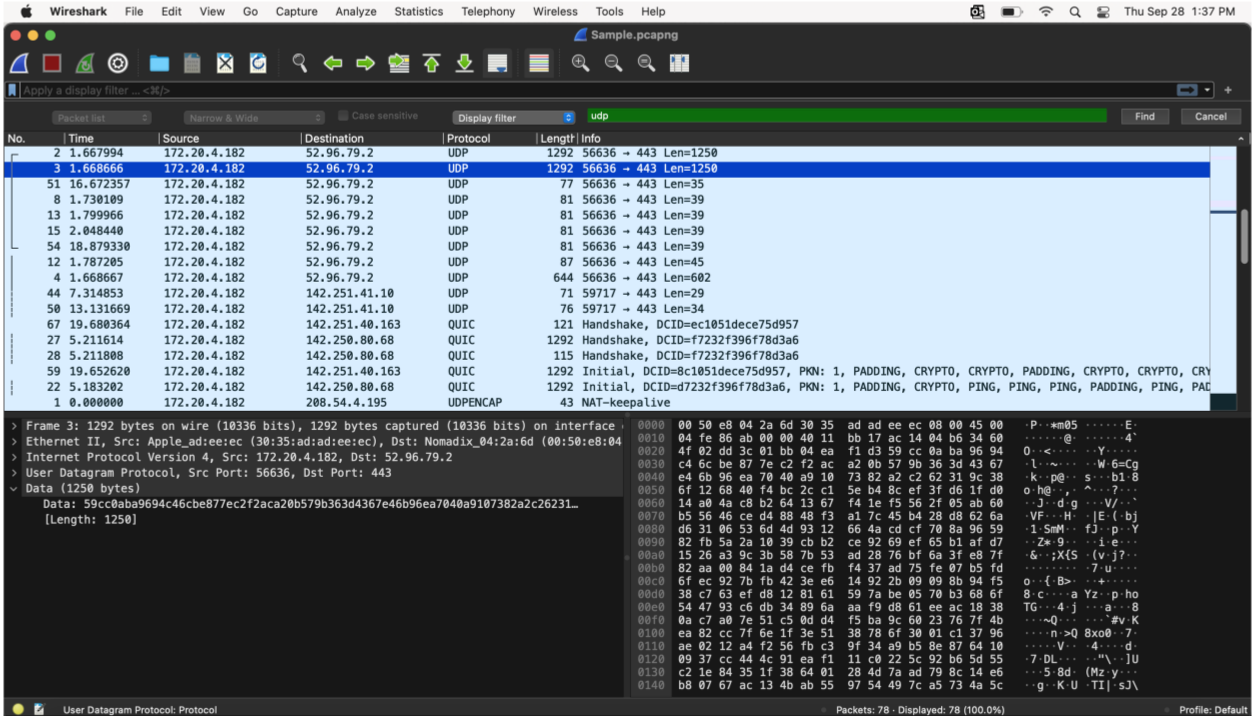
```
> Frame 17: 66 bytes on wire (528 bits), 66 bytes capture
> Ethernet II, Src: Apple_ad:ee:ec (30:35:ad:ad:ee:ec), D
> Internet Protocol Version 4, Src: 172.20.4.182, Dst: 34
> Transmission Control Protocol, Src Port: 51865, Dst Por
```

0 client pkts, 0 server pkts, 0 turns.

Entire conversation (0 bytes)   Show data as ASCII   Stream 0

Find:

- **Finding packets:**



Display filter: udp

```
No.   Time       Source        Destination     Protocol  Length Info
    2 1.667994   172.20.4.182  52.96.79.2      UDP       1292 56636 → 443 Len=1250
    3 1.668666   172.20.4.182  52.96.79.2      UDP       1292 56636 → 443 Len=1250
   51 16.672357  172.20.4.182  52.96.79.2      UDP         77 56636 → 443 Len=35
    8 1.730109   172.20.4.182  52.96.79.2      UDP         81 56636 → 443 Len=39
   13 1.799966   172.20.4.182  52.96.79.2      UDP         81 56636 → 443 Len=39
   15 2.048440   172.20.4.182  52.96.79.2      UDP         81 56636 → 443 Len=39
   54 18.879330  172.20.4.182  52.96.79.2      UDP         81 56636 → 443 Len=39
   12 1.787205   172.20.4.182  52.96.79.2      UDP         87 56636 → 443 Len=45
    4 1.668667   172.20.4.182  52.96.79.2      UDP        644 56636 → 443 Len=602
   44 7.314853   172.20.4.182  142.251.41.10   UDP         71 59717 → 443 Len=29
   50 13.131669  172.20.4.182  142.251.41.10   UDP         76 59717 → 443 Len=34
   67 19.680364  172.20.4.182  142.251.40.163  QUIC       121 Handshake, DCID=ec1051dece75d957
   27 5.211614   172.20.4.182  142.250.80.68   QUIC      1292 Handshake, DCID=f7232f396f78d3a6
   28 5.211808   172.20.4.182  142.250.80.68   QUIC       115 Handshake, DCID=f7232f396f78d3a6
   59 19.652620  172.20.4.182  142.251.40.163  QUIC      1292 Initial, DCID=8c1051dece75d957, PKN: 1, PADDING, CRYPTO, CRYPTO, PADDING, CRYPTO, CRYPTO, CRY
   22 5.183202   172.20.4.182  142.250.80.68   QUIC      1292 Initial, DCID=d7232f396f78d3a6, PKN: 1, PADDING, CRYPTO, PING, PING, PING, PADDING, PING, PAD
    1 0.000000   172.20.4.182  208.54.4.195    UDPENCAP    43 NAT-keepalive
```

```
> Frame 3: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface
> Ethernet II, Src: Apple_ad:ee:ec (30:35:ad:ad:ee:ec), Dst: Nomadix_04:2a:6d (00:50:e8:04
> Internet Protocol Version 4, Src: 172.20.4.182, Dst: 52.96.79.2
> User Datagram Protocol, Src Port: 56636, Dst Port: 443
v Data (1250 bytes)
    Data: 59cc0aba9694c46cbe877ec2f2aca20b579b363d4367e46b96ea7040a9107382a2c26231…
    [Length: 1250]
```

```
0000  00 50 e8 04 2a 6d 30 35  ad ad ee ec 08 00 45 00   ·P··*m05 ······E·
0010  04 fe 86 ab 00 00 40 11  bb 17 ac 14 04 b6 34 60   ······@· ······4`
0020  4f 02 dd 3c 01 bb 04 ea  f1 d3 59 cc 0a ba 96 94   O··<···· ··Y·····
0030  c4 6c be 87 7e c2 f2 ac  a2 0b 57 9b 36 3d 43 67   ·l··~··· ··W·6=Cg
0040  e4 6b 96 ea 70 40 a9 10  73 82 a2 c2 62 31 9c 38   ·k··p@·· s···b1·8
0050  6f 12 68 40 f4 bc 2c c1  5e b4 8c ef 3f d6 1f d0   o·h@··,· ^···?···
0060  14 a0 4a c8 b2 64 13 67  f4 1e f5 56 2f 05 ab 60   ··J··d·g ···V/··`
0070  b5 56 46 ce d4 88 48 f3  a1 7c 45 b4 28 d8 62 6a   ·VF···H· ·|E·(·bj
0080  d6 31 06 53 6d 4d 93 12  66 4a cd cf 70 8a 96 59   ·1·SmM·· fJ··p··Y
0090  82 fb 5a 2a 10 39 cb b2  ce 92 69 ef 65 b1 af d7   ··Z*·9·· ··i·e···
00a0  15 26 a3 9c 3b 58 7b 53  ad 28 76 bf 6a 3f e8 7f   ·&··;X{S ·(v·j?··
00b0  82 aa 00 84 1a d4 ce fb  f4 37 ad 75 fe 07 b5 fd   ········ ·7·u····
00c0  6f ec 92 7b fb 42 3e e6  14 92 2b 09 09 8b 94 f5   o··{·B>· ··+·····
00d0  38 c7 63 ef d8 12 81 61  59 7a be 05 70 b3 68 6f   8·c····a Yz··p·ho
00e0  54 47 93 c6 db 34 89 6a  aa f9 d8 61 ee ac 18 38   TG···4·j ···a···8
00f0  0a c7 a0 7e 51 c5 0d d4  f5 ba 9c 60 23 76 7f 4b   ···~Q··· ···`#v·K
0100  ea 82 cc 7f 6e 1f 3e 51  38 78 6f 30 01 c1 37 96   ····n·>Q 8xo0··7·
0110  ae 02 12 a4 f2 56 fb c3  9f 34 a9 b5 8e 87 64 10   ·····V·· ·4····d·
0120  09 37 cc 44 4c 91 ea f1  11 c0 22 5c 92 b6 5d 55   ·7·DL··· ··"\··]U
0130  c2 1e 84 35 1f 38 64 01  28 4d 7a ad 79 8c 14 e6   ···5·8d· (Mz·y···
0140  b8 07 67 ac 13 4b ab 55  97 54 49 7c a5 73 4a 5c   ··g··K·U ·TI|·sJ\
```

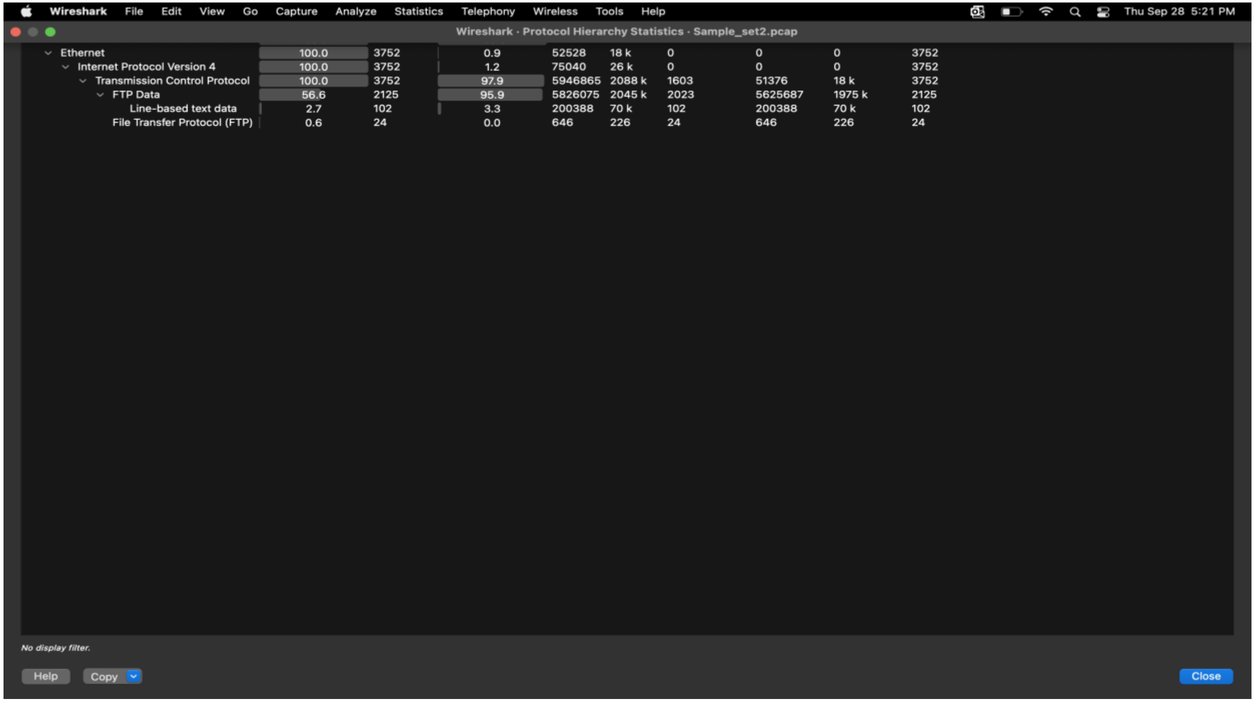
User Datagram Protocol: Protocol   Packets: 78 · Displayed: 78 (100.0%)   Profile: Default

1) What insecure protocol was used to transmit pictures on network?

- FTP protocol is the insecure protocol used here.

2) How many pictures were transmitted?

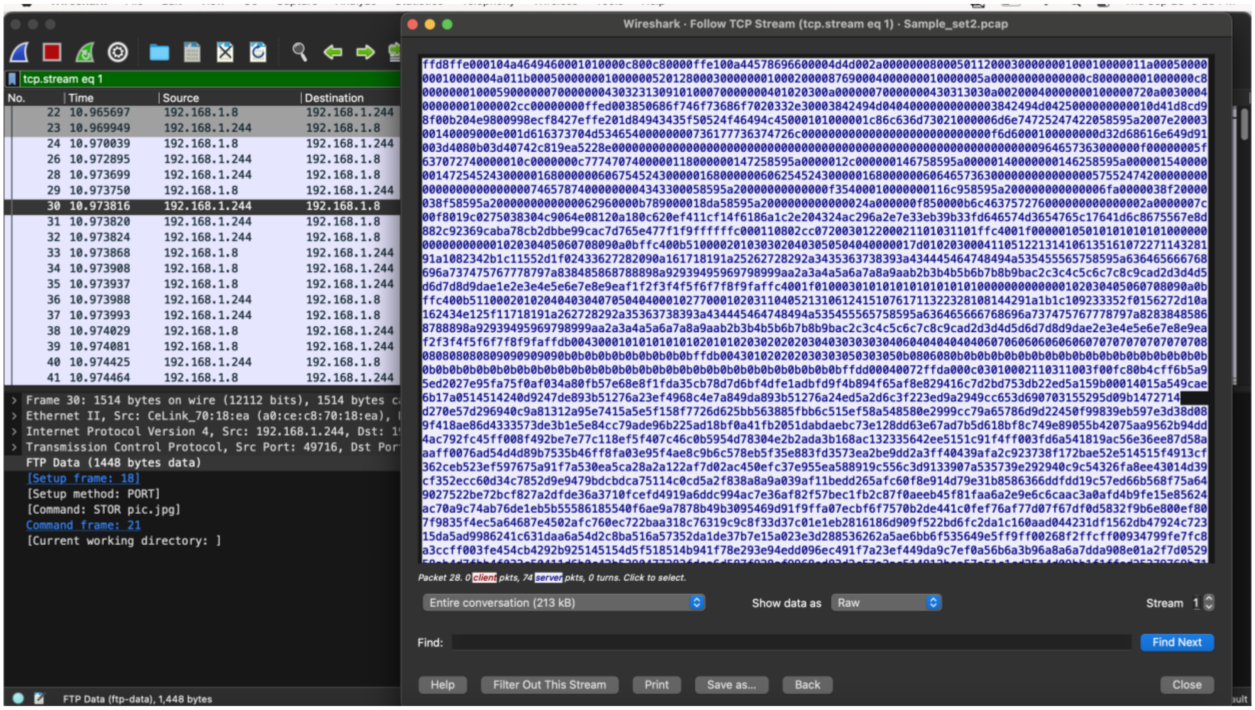
- 24 packets (pictures) were transmitted.


Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Thu Sep 28 5:21 PM
Wireshark · Protocol Hierarchy Statistics · Sample_set2.pcap

```
⌄ Ethernet                          100.0  3752   0.9   52528    18 k    0     0        0       3752
  ⌄ Internet Protocol Version 4     100.0  3752   1.2   75040    26 k    0     0        0       3752
    ⌄ Transmission Control Protocol 100.0  3752  97.9   5946865  2088 k  1603  51376    18 k    3752
      ⌄ FTP Data                     56.6  2125  95.9   5826075  2045 k  2023  5625687  1975 k  2125
          Line-based text data        2.7   102   3.3   200388   70 k    102   200388   70 k    102
        File Transfer Protocol (FTP)  0.6    24   0.0   646      226     24    646      226     24
```

No display filter.

3) Extract one of the pictures that was transmitted. HINT: show and save the picture as "Raw" format. (saved with .jpg extension)


tcp.stream eq 1

```
No.  Time       Source         Destination
 22  10.965697  192.168.1.8    192.168.1.244
 23  10.969949  192.168.1.244  192.168.1.8
 24  10.970039  192.168.1.8    192.168.1.244
 26  10.972895  192.168.1.244  192.168.1.8
 28  10.973699  192.168.1.244  192.168.1.8
 29  10.973750  192.168.1.8    192.168.1.244
 30  10.973816  192.168.1.244  192.168.1.8
 31  10.973820  192.168.1.244  192.168.1.8
 32  10.973824  192.168.1.244  192.168.1.8
 33  10.973868  192.168.1.8    192.168.1.244
 34  10.973908  192.168.1.8    192.168.1.244
 35  10.973937  192.168.1.8    192.168.1.244
 36  10.973988  192.168.1.244  192.168.1.8
 37  10.973993  192.168.1.244  192.168.1.8
 38  10.974029  192.168.1.8    192.168.1.244
 39  10.974081  192.168.1.8    192.168.1.244
 40  10.974425  192.168.1.244  192.168.1.8
 41  10.974464  192.168.1.8    192.168.1.244
```

```
> Frame 30: 1514 bytes on wire (12112 bits), 1514 bytes c
> Ethernet II, Src: CeLink_70:18:ea (a0:ce:c8:70:18:ea), I
> Internet Protocol Version 4, Src: 192.168.1.244, Dst: 1
> Transmission Control Protocol, Src Port: 49716, Dst Por
  FTP Data (1448 bytes data)
    [Setup frame: 18]
    [Setup method: PORT]
    [Command: STOR pic.jpg]
    Command frame: 21
    [Current working directory: ]
```

FTP Data (ftp-data), 1,448 bytes

Wireshark · Follow TCP Stream (tcp.stream eq 1) · Sample_set2.pcap

```
ffd8ffe000104a46494600010100000c800c80000ffe100a4457869660004d4d002a000000080005011200030000000100010000011a00050000
00010000004a011b0005000000010000005201280003000000010002000087690004000000010000005a000000000000000c800000001000000c8
00000001000590000007000000043032313091010007000000004010203000a00000070000000430313030a0020004000000010000720a0030004
00000001000002cc00000000ffed003850686f746f73686f7020332e30003842494d04040000000000003842494d0425000000000010d41d8cd9
8f00b204e9800998ecf8427effe201d84943435f50524f46494c4500010100001c86c636d73021000006d6e74725247422058595a2007e20003
00140009000e001d616373704d534654000000007361777363747426c0000000000000000000000000000f6d6000100000000d32d68616e649d91
003d4080b03d40742c819ea5228e00000000000000000000000000000000000000000000000000000000096465736300000f00000005f
63707274000000010c0000000c777470740000011800000147258595a0000012c000000146758595a0000014000000146258595a000001540000
00147254524300000168000000606754524300000168000000606254524300000168000000606465736300000000000000057552474200000000
000000000000000074657874000000004343300058595a200000000000000f35400010000000116c958595a2000000000000006fa0000038f20000
038f58595a20000000000000062960000b789000018da58595a200000000000000024a000000f850000b6c4637572760000000000000002a0000007c
00f8019c0275038304c9064e08120a180c620ef411cf14f6186a1c2e204324ac296a2e7e33eb39b33fd646574d3654765c17641d6c8675567e8d
882c92369caba78cb2dbbe99cac7d765e477f1f9ffffffc000110802cc0720030122000211010311101ffc4001f0000010501010101010100000
0000000000102030405060708090a0bffc400b5100002010303020403050504040000017d01020300041105122131410613516107227114328 1
91a1082342b1c11552d1f02433627282090a161718191a25262728292a3435363738393a434445464748494a535455565758595a636465666768
696a737475767778797a838485868788898a92939495969798999aa2a3a4a5a6a7a8a9aab2b3b4b5b6b7b8b9bac2c3c4c5c6c7c8c9cad2d3d4d5
d6d7d8d9dae1e2e3e4e5e6e7e8e9eaf1f2f3f4f5f6f7f8f9faffc4001f01000301010101010101010100000000000000102030405060708090a0b
ffc400b51100020102040403040705040400010277000102031104052131061241510761711322328108144291a1b1c109233352f0156272d10a
162434e125f11718191a262728292a35363738393a434445464748494a535455565758595a636465666768696a737475767778797a8283848586
8788898a92939495969798999aa2a3a4a5a6a7a8a9aab2b3b4b5b6b7b8b9bac2c3c4c5c6c7c8c9cad2d3d4d5d6d7d8d9dae2e3e4e5e6e7e8e9ea
f2f3f4f5f6f7f8f9faffdb004300010101010101020101020302020203040303030304060404040404060706060606060607070707070707070708
08080808080909090909090b0b0b0b0b0b0b0b0bffdb0043010202020303030503030500806080b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b
0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0bffdd00040072ffda000c03010002110311003f00fc80b4cff6b5a9
5ed2027e95fa75f0af034a80fb57e68e8f1fda35cb78d7d6bf4dfe1adbfd9f4b894f65af8e829416c7d2bd753db22ed5a159b00014015a549cae
6b17a0514514240d9247de893b51276a23ef4968c4e7a849da893b51276a24ed5a2d6c3f223ed9a2949cc653d690703155295d09b1472714
d270e57d296940c9a81312a95e7415a5e5f158f7726d625bb563885fbb6c515ef58a548580e2999cc79a65786d9d22450f99839eb597e3d38d08
9f418ae86d4333573de3b1e5e84cc79ade96b225ad18bf0a41fb2051dabdaebc73e128dd63e67ad7b5d618bf8c749e89055b42075aa9562b94dd
4ac792fc45ff008f492be7e77c118ef5f407c46c0b5954d78304e2b2ada3b168ac132335642ee5151c91f4ff003fd6a541819ac56e36ee87d58a
aaff0076ad54d4d89b7535b46ff8fa03e95f4ae8c9b6c578eb5f35e883fd3573ea2be9dd2a3ff40439afa2c923738f172bae52e514515f4913cf
362ceb523ef597675a91f7a530ea5ca28a2a122af7d02ac450efc37e955ea588919c556c3d9133907a535739e292940c9c54326fa8ee43014d39
cf352ecc60d34c7852d9e9479bdcbdca75114c0cd5a2f838a8a9a039af11bedd265afc60f8e914d79e31b8586366ddfdd19c57ed66b568f75a64
9027522be72bcf827a2dfde36a3710fcefd4919a6ddc994ac7e36af82f57bec1fb2c87f0aeeb45f81faa6a2e9e6c6caac3a0afd4b9fe15e85624
ac70a9c74ab76de1eb5b55586185540f6ae9a7878b49b3095469d91f9ffa07ecbf6f7570b2de441c0fef76af77d07f67df0d5832f9b6e800ef80
7f9835f4ec5a64687e4502afc760ec722baa318c76319c9c8f33d37c01e1eb2816186d909f522bd6fc2da1c160aad044231df1562db47924c723
15da5ad9986241c631daa6a54d2c8ba516a57352da1de37b7e15a023e3d288536262a5ae6bb6f535649e5ff9ff00268f2ffcff00934799fe7fc8
a3ccff003fe454cb4292b925145154d5f518514b941f78e293e94edd096ec491f7a23ef449da9c7ef0a56b6a3b96a8a6a7dda908e01a2f7d0529
```

Packet 28. 0 client pkts, 74 server pkts, 0 turns. Click to select.

Entire conversation (213 kB) Show data as Raw Stream 1

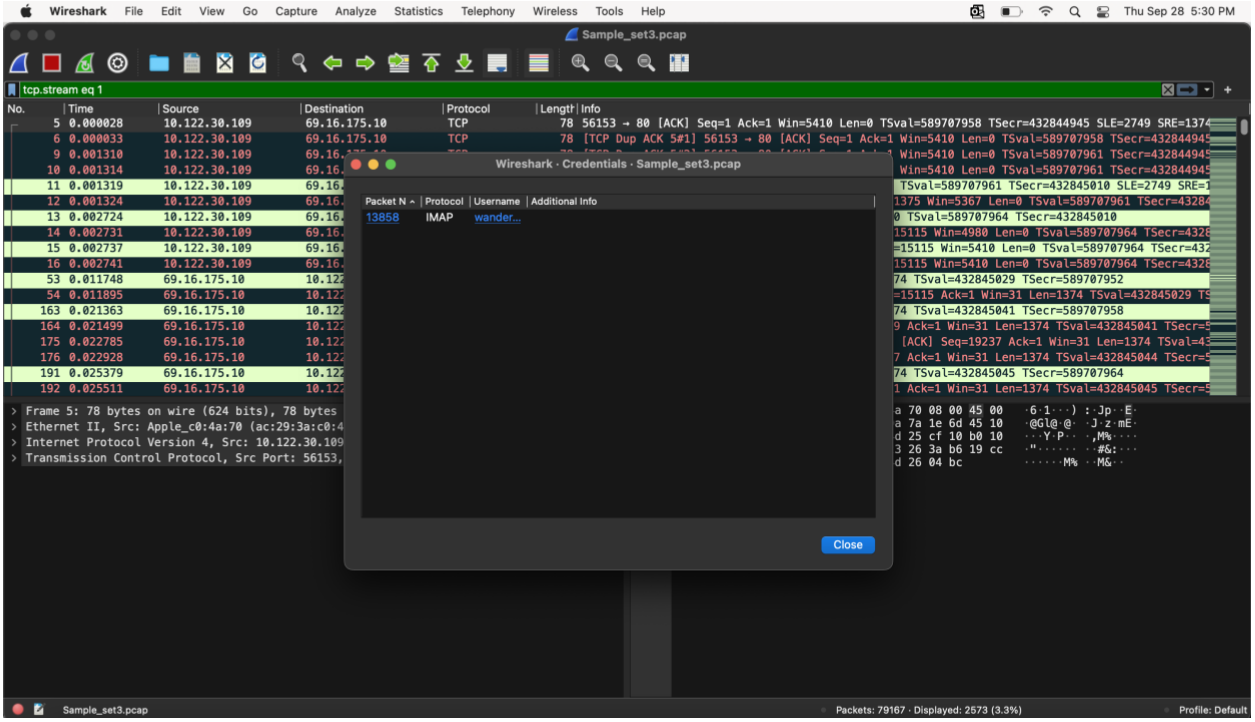
Find:

The image saved is shown below:

Exercise - 4:

1) **What protocol was used to transmit the username:password pair (credentials)?**

- IMAP protocol is used to transmit the credentials as shown in the image below.



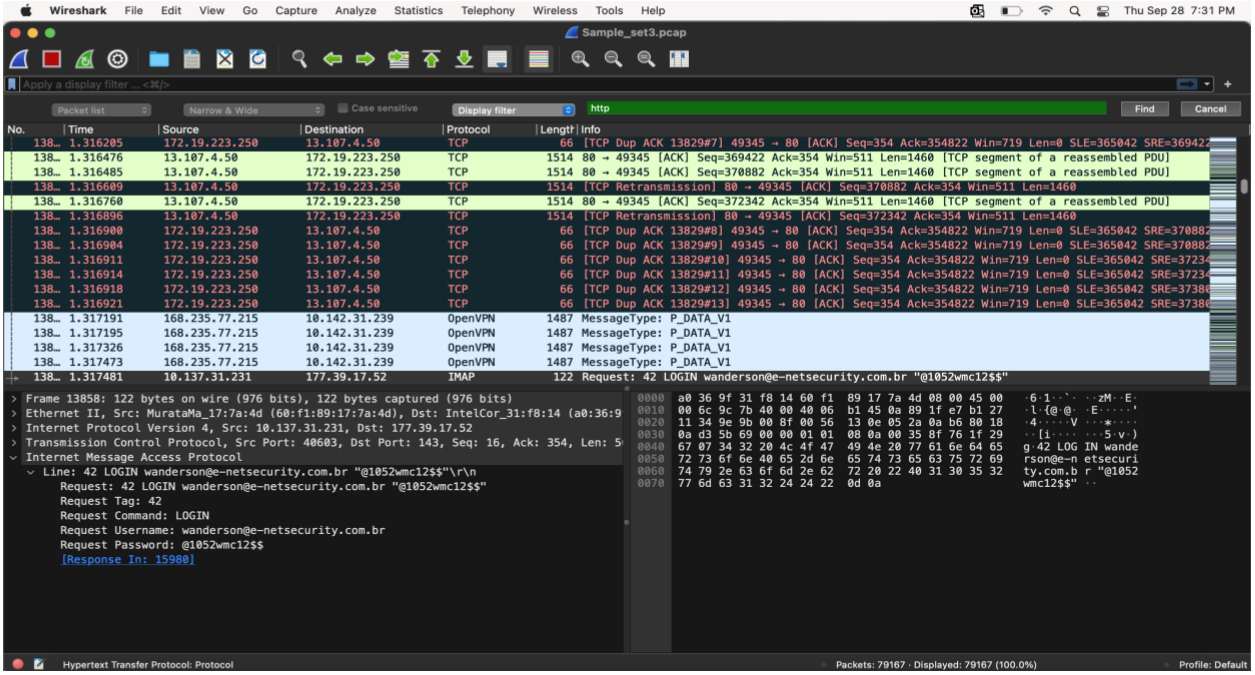
```
tcp.stream eq 1

No.   Time      Source          Destination    Protocol  Length Info
  5 0.000028  10.122.30.109   69.16.175.10   TCP       78 56153 → 80 [ACK] Seq=1 Ack=1 Win=5410 Len=0 TSval=589707958 TSecr=432844945 SLE=2749 SRE=1374
  6 0.000033  10.122.30.109   69.16.175.10   TCP       78 [TCP Dup ACK 5#1] 56153 → 80 [ACK] Seq=1 Ack=1 Win=5410 Len=0 TSval=589707958 TSecr=432844945
  9 0.001310  10.122.30.109   69.16.                    Win=5410 Len=0 TSval=589707961 TSecr=432844945
 10 0.001314  10.122.30.109   69.16.                    Win=5410 Len=0 TSval=589707961 TSecr=432844945
 11 0.001319  10.122.30.109   69.16.                    TSval=589707961 TSecr=432845010 SLE=2749 SRE=1
 12 0.001324  10.122.30.109   69.16.                   1375 Win=5367 Len=0 TSval=589707961 TSecr=43284
 13 0.002724  10.122.30.109   69.16.                   0 TSval=589707964 TSecr=432845010
 14 0.002731  10.122.30.109   69.16.                   15115 Win=4980 Len=0 TSval=589707964 TSecr=4328
 15 0.002737  10.122.30.109   69.16.                   =15115 Win=5410 Len=0 TSval=589707964 TSecr=432
 16 0.002741  10.122.30.109   69.16.                   15115 Win=5410 Len=0 TSval=589707964 TSecr=4328
 53 0.011748  69.16.175.10    10.122                   74 TSval=432845029 TSecr=589707952
 54 0.011895  69.16.175.10    10.122                   =15115 Ack=1 Win=31 Len=1374 TSval=432845029 TS
163 0.021363  69.16.175.10    10.122                   74 TSval=432845041 TSecr=589707958
164 0.021499  69.16.175.10    10.122                   9 Ack=1 Win=31 Len=1374 TSval=432845041 TSecr=5
175 0.022785  69.16.175.10    10.122                    [ACK] Seq=19237 Ack=1 Win=31 Len=1374 TSval=43
176 0.022928  69.16.175.10    10.122                   7 Ack=1 Win=31 Len=1374 TSval=432845044 TSecr=5
191 0.025379  69.16.175.10    10.122                   74 TSval=432845045 TSecr=589707964
192 0.025511  69.16.175.10    10.122                   1 Ack=1 Win=31 Len=1374 TSval=432845045 TSecr=5

> Frame 5: 78 bytes on wire (624 bits), 78 bytes          a 70 08 00 45 00    ·6·1···) :·Jp··E·
> Ethernet II, Src: Apple_c0:4a:70 (ac:29:3a:c0:4         a 7a 1e 6d 45 10    ·@Gl@·@· ·J·z·mE·
> Internet Protocol Version 4, Src: 10.122.30.109         d 25 cf 10 b0 10    ···Y·P·· ·,M%····
> Transmission Control Protocol, Src Port: 56153,         3 26 3a b6 19 cc    ·"······ ··#&:···
                                                          d 26 04 bc          ······M% ··M&··
```

Wireshark · Credentials · Sample_set3.pcap

Packet N	Protocol	Username	Additional Info
13858	IMAP	wander...	

2) What is one username:password pair in this PCAP set? (HINT: use Edit > Find Packet)

- When searched for requests containing ‘http’, got a request containing Login details that were part of a login request with username and password in it as shown below in the image.



```
No.    Time      Source          Destination     Protocol  Length Info
138… 1.316205  172.19.223.250  13.107.4.50     TCP         66 [TCP Dup ACK 13829#7] 49345 → 80 [ACK] Seq=354 Ack=354822 Win=719 Len=0 SLE=365042 SRE=369422
138… 1.316476  13.107.4.50     172.19.223.250  TCP       1514 80 → 49345 [ACK] Seq=369422 Ack=354 Win=511 Len=1460 [TCP segment of a reassembled PDU]
138… 1.316485  13.107.4.50     172.19.223.250  TCP       1514 80 → 49345 [ACK] Seq=370882 Ack=354 Win=511 Len=1460 [TCP segment of a reassembled PDU]
138… 1.316609  13.107.4.50     172.19.223.250  TCP       1514 [TCP Retransmission] 80 → 49345 [ACK] Seq=370882 Ack=354 Win=511 Len=1460
138… 1.316760  13.107.4.50     172.19.223.250  TCP       1514 80 → 49345 [ACK] Seq=372342 Ack=354 Win=511 Len=1460 [TCP segment of a reassembled PDU]
138… 1.316896  13.107.4.50     172.19.223.250  TCP       1514 [TCP Retransmission] 80 → 49345 [ACK] Seq=372342 Ack=354 Win=511 Len=1460
138… 1.316900  172.19.223.250  13.107.4.50     TCP         66 [TCP Dup ACK 13829#8] 49345 → 80 [ACK] Seq=354 Ack=354822 Win=719 Len=0 SLE=365042 SRE=370882
138… 1.316904  172.19.223.250  13.107.4.50     TCP         66 [TCP Dup ACK 13829#9] 49345 → 80 [ACK] Seq=354 Ack=354822 Win=719 Len=0 SLE=365042 SRE=370882
138… 1.316911  172.19.223.250  13.107.4.50     TCP         66 [TCP Dup ACK 13829#10] 49345 → 80 [ACK] Seq=354 Ack=354822 Win=719 Len=0 SLE=365042 SRE=37234
138… 1.316914  172.19.223.250  13.107.4.50     TCP         66 [TCP Dup ACK 13829#11] 49345 → 80 [ACK] Seq=354 Ack=354822 Win=719 Len=0 SLE=365042 SRE=37234
138… 1.316918  172.19.223.250  13.107.4.50     TCP         66 [TCP Dup ACK 13829#12] 49345 → 80 [ACK] Seq=354 Ack=354822 Win=719 Len=0 SLE=365042 SRE=37380
138… 1.316921  172.19.223.250  13.107.4.50     TCP         66 [TCP Dup ACK 13829#13] 49345 → 80 [ACK] Seq=354 Ack=354822 Win=719 Len=0 SLE=365042 SRE=37380
138… 1.317191  168.235.77.215  10.142.31.239   OpenVPN   1487 MessageType: P_DATA_V1
138… 1.317195  168.235.77.215  10.142.31.239   OpenVPN   1487 MessageType: P_DATA_V1
138… 1.317326  168.235.77.215  10.142.31.239   OpenVPN   1487 MessageType: P_DATA_V1
138… 1.317473  168.235.77.215  10.142.31.239   OpenVPN   1487 MessageType: P_DATA_V1
138… 1.317481  10.137.31.231   177.39.17.52    IMAP       122 Request: 42 LOGIN wanderson@e-netsecurity.com.br "@1052wmc12$$"
```

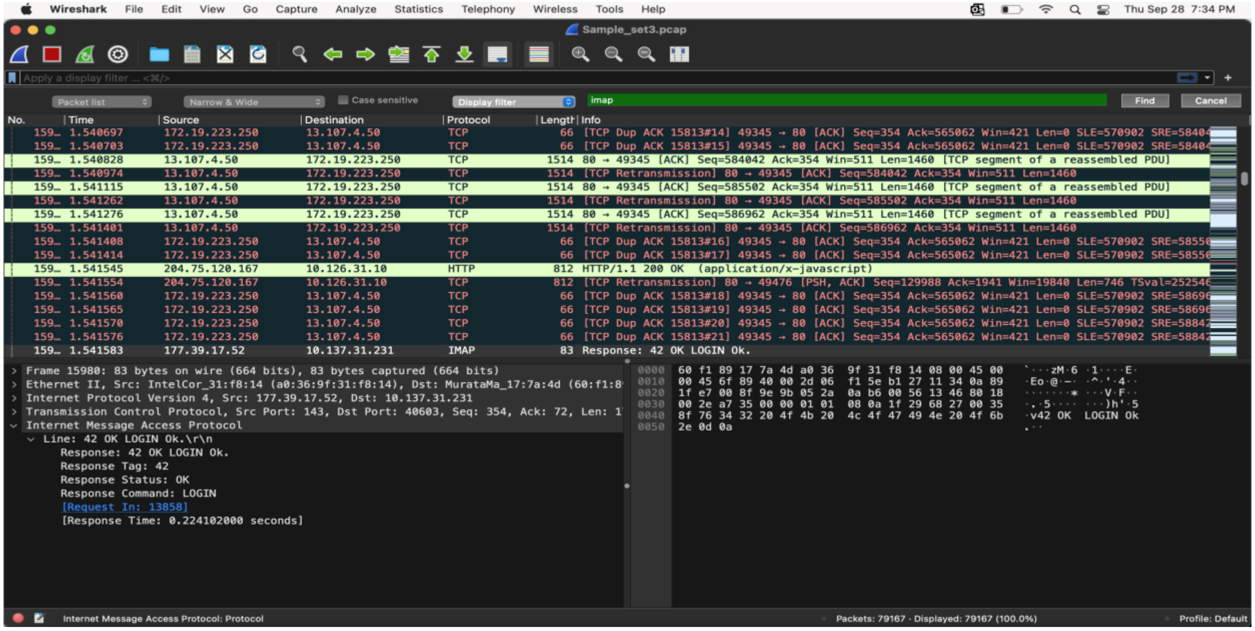
```
> Frame 13858: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
> Ethernet II, Src: MurataMa_17:7a:4d (60:f1:89:17:7a:4d), Dst: IntelCor_31:f8:14 (a0:36:9
> Internet Protocol Version 4, Src: 10.137.31.231, Dst: 177.39.17.52
> Transmission Control Protocol, Src Port: 40603, Dst Port: 143, Seq: 16, Ack: 354, Len: 5
v Internet Message Access Protocol
  v Line: 42 LOGIN wanderson@e-netsecurity.com.br "@1052wmc12$$"\r\n
      Request: 42 LOGIN wanderson@e-netsecurity.com.br "@1052wmc12$$"
      Request Tag: 42
      Request Command: LOGIN
      Request Username: wanderson@e-netsecurity.com.br
      Request Password: @1052wmc12$$
      [Response In: 15980]
```

```
0000  a0 36 9f 31 f8 14 60 f1  89 17 7a 4d 08 00 45 00   ·6·1··`· ··zM··E·
0010  00 6c 9c 7b 40 00 40 06  b1 45 0a 89 1f e7 b1 27   ·l·{@·@· ·E·····'
0020  11 34 9e 9b 00 8f 00 56  13 0e 05 2a 0a b6 80 18   ·4·····V ···*····
0030  0a d3 5b 69 00 00 01 01  08 0a 00 35 8f 76 1f 29   ··[i···· ···5·v·)
0040  67 07 34 32 20 4c 4f 47  49 4e 20 77 61 6e 64 65   g·42 LOG IN wande
0050  72 73 6f 6e 40 65 2d 6e  65 74 73 65 63 75 72 69   rson@e-n etsecuri
0060  74 79 2e 63 6f 6d 2e 62  72 20 22 40 31 30 35 32   ty.com.b r "@1052
0070  77 6d 63 31 32 24 24 22  0d 0a                     wmc12$$" ··
```

Hypertext Transfer Protocol: Protocol   Packets: 79167 · Displayed: 79167 (100.0%)   Profile: Default

3) Is the username:password pair valid? Why / why not?

- After getting the details of the http request as shown in above image with username and password.
- When clicked on the response, it showed the message containing Response Status as ‘OK’ with Response Tag as ‘42’ and Response Command as ‘LOGIN’.
- Hence, the username: password pair given in the request is valid.



```
No.    Time      Source          Destination     Protocol  Length Info
159… 1.540697  172.19.223.250  13.107.4.50     TCP         66 [TCP Dup ACK 15813#14] 49345 → 80 [ACK] Seq=354 Ack=565062 Win=421 Len=0 SLE=570902 SRE=58404
159… 1.540703  172.19.223.250  13.107.4.50     TCP         66 [TCP Dup ACK 15813#15] 49345 → 80 [ACK] Seq=354 Ack=565062 Win=421 Len=0 SLE=570902 SRE=58404
159… 1.540828  13.107.4.50     172.19.223.250  TCP       1514 80 → 49345 [ACK] Seq=584042 Ack=354 Win=511 Len=1460 [TCP segment of a reassembled PDU]
159… 1.540974  13.107.4.50     172.19.223.250  TCP       1514 [TCP Retransmission] 80 → 49345 [ACK] Seq=584042 Ack=354 Win=511 Len=1460
159… 1.541115  13.107.4.50     172.19.223.250  TCP       1514 80 → 49345 [ACK] Seq=585502 Ack=354 Win=511 Len=1460 [TCP segment of a reassembled PDU]
159… 1.541262  13.107.4.50     172.19.223.250  TCP       1514 [TCP Retransmission] 80 → 49345 [ACK] Seq=585502 Ack=354 Win=511 Len=1460
159… 1.541276  13.107.4.50     172.19.223.250  TCP       1514 80 → 49345 [ACK] Seq=586962 Ack=354 Win=511 Len=1460 [TCP segment of a reassembled PDU]
159… 1.541401  13.107.4.50     172.19.223.250  TCP       1514 [TCP Retransmission] 80 → 49345 [ACK] Seq=586962 Ack=354 Win=511 Len=1460
159… 1.541408  172.19.223.250  13.107.4.50     TCP         66 [TCP Dup ACK 15813#16] 49345 → 80 [ACK] Seq=354 Ack=565062 Win=421 Len=0 SLE=570902 SRE=58550
159… 1.541414  172.19.223.250  13.107.4.50     TCP         66 [TCP Dup ACK 15813#17] 49345 → 80 [ACK] Seq=354 Ack=565062 Win=421 Len=0 SLE=570902 SRE=58550
159… 1.541545  204.75.120.167  10.126.31.10    HTTP       812 HTTP/1.1 200 OK  (application/x-javascript)
159… 1.541554  204.75.120.167  10.126.31.10    TCP        812 [TCP Retransmission] 80 → 49476 [PSH, ACK] Seq=129988 Ack=1941 Win=19840 Len=746 TSval=252546
159… 1.541560  172.19.223.250  13.107.4.50     TCP         66 [TCP Dup ACK 15813#18] 49345 → 80 [ACK] Seq=354 Ack=565062 Win=421 Len=0 SLE=570902 SRE=58696
159… 1.541565  172.19.223.250  13.107.4.50     TCP         66 [TCP Dup ACK 15813#19] 49345 → 80 [ACK] Seq=354 Ack=565062 Win=421 Len=0 SLE=570902 SRE=58696
159… 1.541570  172.19.223.250  13.107.4.50     TCP         66 [TCP Dup ACK 15813#20] 49345 → 80 [ACK] Seq=354 Ack=565062 Win=421 Len=0 SLE=570902 SRE=58842
159… 1.541576  172.19.223.250  13.107.4.50     TCP         66 [TCP Dup ACK 15813#21] 49345 → 80 [ACK] Seq=354 Ack=565062 Win=421 Len=0 SLE=570902 SRE=58842
159… 1.541583  177.39.17.52    10.137.31.231   IMAP        83 Response: 42 OK LOGIN Ok.
```

```
> Frame 15980: 83 bytes on wire (664 bits), 83 bytes captured (664 bits)
> Ethernet II, Src: IntelCor_31:f8:14 (a0:36:9f:31:f8:14), Dst: MurataMa_17:7a:4d (60:f1:8
> Internet Protocol Version 4, Src: 177.39.17.52, Dst: 10.137.31.231
> Transmission Control Protocol, Src Port: 143, Dst Port: 40603, Seq: 354, Ack: 72, Len: 1
v Internet Message Access Protocol
  v Line: 42 OK LOGIN Ok.\r\n
      Response: 42 OK LOGIN Ok.
      Response Tag: 42
      Response Status: OK
      Response Command: LOGIN
      [Request In: 13858]
      [Response Time: 0.224102000 seconds]
```

```
0000  60 f1 89 17 7a 4d a0 36  9f 31 f8 14 08 00 45 00   `···zM·6 ·1····E·
0010  00 45 6f 89 40 00 2d 06  f1 5e b1 27 11 34 0a 89   ·Eo·@·-· ·^·'·4··
0020  1f e7 00 8f 9e 9b 05 2a  0a b6 00 56 13 46 80 18   ·······* ···V·F··
0030  00 2e a7 35 00 00 01 01  08 0a 1f 29 68 27 00 35   ·.·5···· ···)h'·5
0040  8f 76 34 32 20 4f 4b 20  4c 4f 47 49 4e 20 4f 6b   ·v42 OK  LOGIN Ok
0050  2e 0d 0a                                            .··
```

Internet Message Access Protocol: Protocol   Packets: 79167 · Displayed: 79167 (100.0%)   Profile: Default