IoT Project : MQTT

Jorge Roa

How to Install Mosquitto MQTT Broker/Server

1. *sudo apt-add-repository ppa:mosquitto-dev/mosquitto-ppa*
2. *sudo apt-get update*
3. *sudo apt-get install mosquitto*
4. *sudo apt-get install mosquitto-clients*
5. *sudo apt clean*

Checking Mosquitto Service

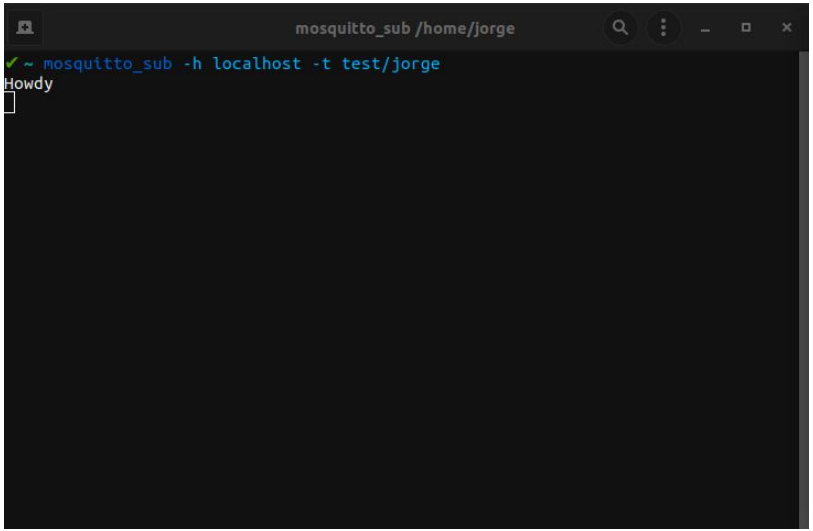
```
✔ ~ sudo systemctl status mosquitto
[sudo] password for jorge:
● mosquitto.service - Mosquitto MQTT Broker
     Loaded: loaded (/lib/systemd/system/mosquitto.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2021-04-17 16:13:37 CDT; 1 day 16h ago
       Docs: man:mosquitto.conf(5)
             man:mosquitto(8)
   Main PID: 1001 (mosquitto)
      Tasks: 1 (limit: 38161)
     Memory: 2.9M
     CGroup: /system.slice/mosquitto.service
             └─1001 /usr/sbin/mosquitto -c /etc/mosquitto/mosquitto.conf

Apr 17 16:13:37 georgeExotic systemd[1]: Starting Mosquitto MQTT Broker...
Apr 17 16:13:37 georgeExotic systemd[1]: Started Mosquitto MQTT Broker.
```

1. Check server status
   a. *Sudo systemctl status mosquitto.service*
2. Manage services Sudo
   a. *sudo systemctl restart/disable/enable mosquitto.service*

Testing Mosquitto MQTT Pub/Sub Broker

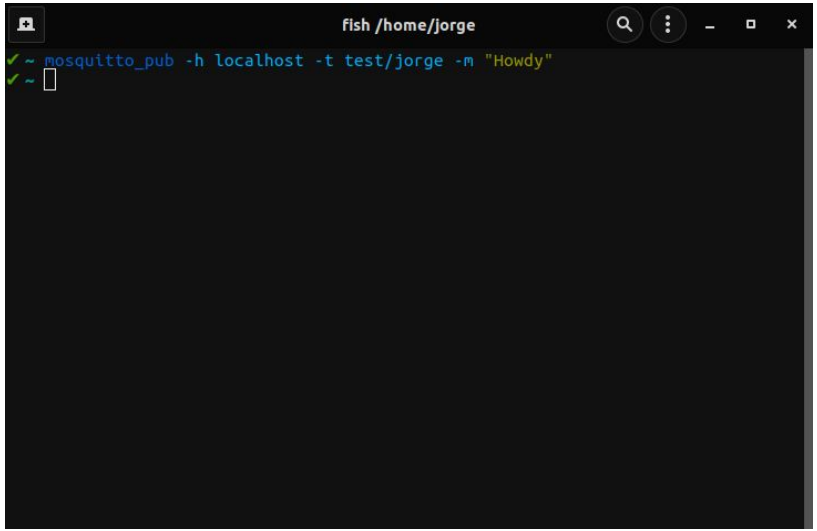
Subscribe to a *topic* : test/jorge

mosquitto_sub -h localhost -t test/jorge



Publish to *topic* : test/jorge

mosquitto_pub - h localhost -t test/jorge -m “howdy”



WireShark Results from Test

```
▸ Frame 30: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface lo, id 0
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▸ Transmission Control Protocol, Src Port: 1883, Dst Port: 38858, Seq: 10, Ack: 32, Len: 19
▸ MQ Telemetry Transport Protocol, Publish Message

0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ........ ......E·
0010  00 47 08 09 40 00 40 06  34 a6 7f 00 00 01 7f 00   ·G··@·@· 4·......
0020  00 01 07 5b 97 ca 79 91  c0 4d 7f b3 5a 07 80 18   ···[··y· ·M··Z···
0030  00 40 fe 3b 00 00 01 01  08 0a 9a 8d e5 ee 9a 8d   ·@·;···· ........
0040  dd a7 30 11 00 0a 74 65  73 74 2f 6a 6f 72 67 65   ··0···te st/jorge
0050  48 6f 77 64 79                                     Howdy
```

Observation:

1. Unauthenticated
2. Not encrypted

Adding Authentication to Mosquitto Broker

The username and password combination is transmitted in **clear text,** and is not secure without some form of **transport encryption**.(SSL)

Steps to set up authentication:

1. Create a password file
2. Edit the mosquitto.conf to force broker to force authentication

1. Create a password file:

a. sudo mosquitto_passwd -c /etc/mosquitto/passwd jorge

i. Usage - *sudo mosquitto_passwd -c passwordfile user*

Check user and password:

a. cat /etc/mosquitto/passwd

Delete user and password:

a. sudo mosquitto_passwd -D /etc/mosquitto/passwd jorge

i. Usage - *sudo mosquitto_passwd -D passwordfile user*

My authentication:
user: Jorge
passwd: temppwd

Passwd stored as hash

```
✓ ~ cat /etc/mosquitto/passwd
jorge:$7$101$9ifbglP5i8NKpL44$xFBngFP8RY+tE7jLcnMW8037rIrEZPmqbokQw6hxzpW6QM29OU5CAUsylYoUxhP6CScluAXhUibBd8VhGWDcIQ==
```

Adding Authentication to Mosquitto Broker

The username and password combination is transmitted in **clear text,** and is not secure without some form of **transport encryption**.(SSL)

Steps to set up authentication:

1. Create a password file
2. Edit the mosquitto.conf to force broker to force authentication

2. Edit the mosquitto.conf to force broker to force authentication:

a. *sudo nano /etc/mosquitto/conf.d/default.conf*
   i. add :
      1. *allow_anonymous false*
      2. *Password_file /etc/mosquitto/passwd*

b. Re-start mosquitto service
   i. *sudo systemctl restart mosquitto*
   ii. *sudo systemctl status mosquitto*

Systemctl status difference:

Before Authentication

```
✓ ~ sudo systemctl status mosquitto.service
● mosquitto.service - Mosquitto MQTT Broker
     Loaded: loaded (/lib/systemd/system/mosquitto.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2021-04-17 16:13:37 CDT; 1 day 20h ago
       Docs: man:mosquitto.conf(5)
             man:mosquitto(8)
   Main PID: 1001 (mosquitto)
      Tasks: 1 (limit: 38161)
     Memory: 3.1M
     CGroup: /system.slice/mosquitto.service
             └─1001 /usr/sbin/mosquitto -c /etc/mosquitto/mosquitto.conf

Apr 17 16:13:37 georgeExotic systemd[1]: Starting Mosquitto MQTT Broker...
Apr 17 16:13:37 georgeExotic systemd[1]: Started Mosquitto MQTT Broker.
```

After Authentication

Using authentication config

```
✗ ~ sudo systemctl status mosquitto.service
● mosquitto.service - Mosquitto MQTT Broker
     Loaded: loaded (/lib/systemd/system/mosquitto.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2021-04-19 13:04:54 CDT; 14s ago
       Docs: man:mosquitto.conf(5)
             man:mosquitto(8)
    Process: 98303 ExecStartPre=/bin/mkdir -m 740 -p /var/log/mosquitto (code=exited, status=0/SUCCESS)
    Process: 98304 ExecStartPre=/bin/chown mosquitto: /var/log/mosquitto (code=exited, status=0/SUCCESS)
    Process: 98305 ExecStartPre=/bin/mkdir -m 740 -p /var/run/mosquitto (code=exited, status=0/SUCCESS)
    Process: 98306 ExecStartPre=/bin/chown mosquitto: /var/run/mosquitto (code=exited, status=0/SUCCESS)
   Main PID: 98307 (mosquitto)
      Tasks: 1 (limit: 38161)
     Memory: 1.2M
     CGroup: /system.slice/mosquitto.service
             └─98307 /usr/sbin/mosquitto -c /etc/mosquitto/mosquitto.conf

Apr 19 13:04:54 georgeExotic systemd[1]: Starting Mosquitto MQTT Broker...
Apr 19 13:04:54 georgeExotic mosquitto[98307]: 1618855494: Loading config file /etc/mosquitto/conf.d/default.conf
Apr 19 13:04:54 georgeExotic systemd[1]: Started Mosquitto MQTT Broker.
```

Subscribing to broker with wrong credential

- Connection denied due to wrong password

```
✔ ~ mosquitto_sub -h localhost -t jorge/test -u "jorge" -P "temppw"
Connection error: Connection Refused: not authorised.
✗ ~
```

Publishing with wrong password

- Connection denied due to wrong password

```
✔ ~ mosquitto_pub -h localhost -u "jorge" -P "temppw" -t test/jorge -m "jorge"
Connection error: Connection Refused: not authorised.
Error: The connection was refused.
```

Testing Mosquitto MQTT Pub/Sub Broker

With Authentication

Authenticated subscribing

- *mosquitto_sub -h localhost -t test/jorge -u "jorge" -P "temppwd"*

```
✔ ~ mosquitto_sub -h localhost -t test/jorge -u "jorge" -P "temppwd"
jorge
```

Authenticated publishing

- *mosquitto_pub -h localhost -u "jorge" -P "temppwd" -t test/jorge -m "jorge"*

```
✔ ~ mosquitto_pub -h localhost -u "jorge" -P "temppwd" -t test/jorge -m "jorge"
```

WireShark Results With Authentication

Authentication Request From Subscriber to Broker

```
▾ MQ Telemetry Transport Protocol, Connect Command
  ▸ Header Flags: 0x10, Message Type: Connect Command
    Msg Len: 28
    Protocol Name Length: 4
    Protocol Name: MQTT
    Version: MQTT v3.1.1 (4)
  ▸ Connect Flags: 0xc2, User Name Flag, Password Flag, QoS Level: At most once delivery (Fire and Forget), Clean Session Flag
    Keep Alive: 60
    Client ID Length: 0
    Client ID:
    User Name Length: 5
    User Name: jorge
    Password Length: 7
    Password: temppwd

0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ........ ......E·
0010  00 52 f9 ea 40 00 40 06  42 b9 7f 00 00 01 7f 00   ·R··@·@· B·......
0020  00 01 ac 0e 07 5b b0 fc  de ef ad 3b a1 10 80 18   ·····[·· ···;····
0030  00 40 fe 46 00 00 01 01  08 0a 52 6b 7c 78 52 6b   ·@·F···· ··Rk|xRk
0040  7c 78 10 1c 00 04 4d 51  54 54 04 c2 00 3c 00 00   |x····MQ TT···<··
0050  00 05 6a 6f 72 67 65 00  07 74 65 6d 70 70 77 64   ··jorge· ·temppwd
```

Authenticated Message From Publisher to Broker

```
▾ MQ Telemetry Transport Protocol, Publish Message
  ▸ Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (Fire and Forget)
    Msg Len: 17
    Topic Length: 10
    Topic: test/jorge
    Message: 686f776479

0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ........ ......E·
0010  00 47 b0 c6 40 00 40 06  8b e8 7f 00 00 01 7f 00   ·G··@·@· ........
0020  00 01 07 5b ac 0e ad 3b  a1 19 b0 fc df 1e 80 18   ···[···; ........
0030  00 40 fe 3b 00 00 01 01  08 0a 52 6b 8d eb 52 6b   ·@·;···· ··Rk··Rk
0040  7c 7d 30 11 00 0a 74 65  73 74 2f 6a 6f 72 67 65   |}0···te st/jorge
0050  68 6f 77 64 79                                     howdy
```

Observation:

1. Authenticated
2. Not encrypted
3. Credentials can be snooped

Adding Encryption and Authentication with SSL

To secure MQTT connection with SSL, we need SSL certificates. Let's Encrypt is a certificate authority which offers free SSL certificates.

Requirements:

1. Mosquitto broker installed in server
2. A domain name pointed at your MQTT server. (free option www.my.noip.com)
3. Port 80 must be unused on your server and port-forwarded on your firewall and router
4. Make sure your server's firewall is set up to allow the following ports through:
   a. 22(ssh)
   b. 80 (http)
   c. 443(https)
   d. 8883(secured mqtt)
   e. 1883(mqtt)

```
➜  ~ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       Anywhere
8883                       ALLOW       Anywhere
1883                       ALLOW       Anywhere
443                        ALLOW       Anywhere
80                         ALLOW       Anywhere
22 (v6)                    ALLOW       Anywhere (v6)
8883 (v6)                  ALLOW       Anywhere (v6)
1883 (v6)                  ALLOW       Anywhere (v6)
443 (v6)                   ALLOW       Anywhere (v6)
80 (v6)                    ALLOW       Anywhere (v6)
```

My Domain

www.110ashop.ddns.net

Adding Encryption and Authentication with SSL

Steps

1. **Install Certbot (official Let's Encrypt client) :**

- *sudo apt install certbot*
- *sudo ufw allow 80*
- Create Certificate => *sudo certbot certonly --standalone --preferred-challenges http -d 110ashop.ddns.net*

My domain

```
➜ ~ sudo certbot certonly --standalone --preferred-challenges http -d 110ashop.ddns.net
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator standalone, Installer None
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for 110ashop.ddns.net
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/110ashop.ddns.net/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/110ashop.ddns.net/privkey.pem
   Your cert will expire on 2021-07-24. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot
   again. To non-interactively renew *all* of your certificates, run
   "certbot renew"
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
```

Successful Output

Adding Encryption and Authentication with SSL

Steps

2. Configuring Mosquitto SSL

- Open the mosquito configuration file
  - *sudo nano /etc/mosquitto/conf.d/default.conf*
- Add the following to your mosquitto configuration file

listener 8883
certfile /etc/letsencrypt/live/mqtt.example.com/cert.pem
cafile /etc/letsencrypt/live/mqtt.example.com/chain.pem
keyfile /etc/letsencrypt/live/mqtt.example.com/privkey.pem

listener 8083
protocol websockets
certfile /etc/letsencrypt/live/mqtt.example.com/cert.pem
cafile /etc/letsencrypt/live/mqtt.example.com/chain.pem
keyfile /etc/letsencrypt/live/mqtt.example.com/privkey.pem

```
  GNU nano 4.8
allow_anonymous false
password_file /etc/mosquitto/passwd

listener 1883 localhost

listener 8883
certfile /etc/letsencrypt/live/110ashop.ddns.net/cert.pem
cafile /etc/letsencrypt/live/110ashop.ddns.net/chain.pem
keyfile /etc/letsencrypt/live/110ashop.ddns.net/privkey.pem

listener 8083
protocol websockets
certfile /etc/letsencrypt/live/110ashop.ddns.net/cert.pem
cafile /etc/letsencrypt/live/110ashop.ddns.net/chain.pem
keyfile /etc/letsencrypt/live/110ashop.ddns.net/privkey.pem
```

Adding Encryption and Authentication with SSL

Steps

3. Configuring Mosquitto SSL

- Restart the Mosquitto service
  - *Sudo systemctl restart mosquitto.service*
- Check the Status of the MQTT Server
  - The output should look something like the following

```
➜  ~ sudo systemctl status mosquitto.service
● mosquitto.service - Mosquitto MQTT v3.1/v3.1.1 Broker
     Loaded: loaded (/lib/systemd/system/mosquitto.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2021-04-26 03:17:49 UTC; 30s ago
       Docs: man:mosquitto.conf(5)
             man:mosquitto(8)
   Main PID: 94671 (mosquitto)
      Tasks: 3 (limit: 560)
     Memory: 1.2M
     CGroup: /system.slice/mosquitto.service
             └─94671 /usr/sbin/mosquitto -c /etc/mosquitto/mosquitto.conf

Apr 26 03:17:49 ip-172-26-9-250 systemd[1]: mosquitto.service: Succeeded.
Apr 26 03:17:49 ip-172-26-9-250 systemd[1]: Stopped Mosquitto MQTT v3.1/v3.1.1 Broker.
Apr 26 03:17:49 ip-172-26-9-250 systemd[1]: Starting Mosquitto MQTT v3.1/v3.1.1 Broker...
Apr 26 03:17:49 ip-172-26-9-250 mosquitto[94671]: 1619407069: Loading config file /etc/mosquitto/conf>
Apr 26 03:17:49 ip-172-26-9-250 mosquitto[94671]: [430477.117646]~DLT~94671~INFO     ~FIFO /tmp/dlt c>
Apr 26 03:17:49 ip-172-26-9-250 systemd[1]: Started Mosquitto MQTT v3.1/v3.1.1 Broker.
lines 1-17/17 (END)
➜  ~
```

Testing Mosquitto MQTT Pub/Sub Broker

With SSL encryption

Authenticated subscribing

- *mosquitto_sub -h 110ashop.ddns.net -t jorge/test -p 8883 --capath /etc/ssl/certs/ -u "jorge" -P "temppwd"*

```
✔ ~ mosquitto_sub -h 110ashop.ddns.net -t jorge/test -p 8883 --capath /etc/ssl/certs/ -u "jorge" -P "temppwd"
jorge
```

Authenticated publishing

- *mosquitto_pub -h 110ashop.ddns.net -t jorge/test -m "jorge" -p 8883 --capath /etc/ssl/certs/ -u "jorge" -P "temppwd"*

```
✔ ~ mosquitto_pub -h 110ashop.ddns.net -t jorge/test -m "jorge" -p 8883 --capath /etc/ssl/certs/ -u "jorge" -P "temppwd"
```

WireShark Results With SSL Encryption

Authentication Request From <u>Subscriber</u> to Broker

```
Frame 50: 375 bytes on wire (3000 bits), 375 bytes captured (3000 bits) on interface wlp0s20f3, id 0
Ethernet II, Src: IntelCor_6d:c9:4b (3c:58:c2:6d:c9:4b), Dst: HewlettP_f1:90:99 (50:65:f3:f1:90:99)
Internet Protocol Version 4, Src: 10.1.0.111, Dst: 54.242.22.45
Transmission Control Protocol, Src Port: 36712, Dst Port: 8883, Seq: 1, Ack: 1, Len: 309
Transport Layer Security

0000  50 65 f3 f1 90 99 3c 58  c2 6d c9 4b 08 00 45 00   Pe····<X ·m·K··E·
0010  01 69 f2 bc 40 00 40 06  ef 43 0a 01 00 6f 36 f2   ·i··@·@· ·C···o6·
0020  16 2d 8f 68 22 b3 f9 5b  bc c1 b5 2b a3 9c 80 18   ·-·h"··[ ···+····
0030  00 3f 58 ea 00 00 01 01  08 0a 2a 1b fe ef c9 4e   ·?X····· ··*····N
0040  1e af 16 03 01 01 30 01  00 01 2c 03 03 28 de 1d   ····0··· ··,··(··
0050  4a ad e4 e6 ef fa 2b 0f  31 37 44 75 91 c3 a7 df   J·····+· 17Du····
0060  f8 1f 5c aa 54 2b 4a 35  69 46 aa 19 e6 20 56 c2   ··\·T+J5 iF··· V·
0070  01 cb ab 41 32 35 5f 22  a1 4a 4f e5 ec e7 e8 c0   ···A25_" ·JO·····
0080  ef ae e3 2c ce 76 b3 a4  f3 76 27 6f 83 81 00 3e   ···,·v·· ·v'o···>
0090  13 02 13 03 13 01 c0 2c  c0 30 00 9f cc a9 cc a8   ·******, ·0******
00a0  cc aa c0 2b c0 2f 00 9e  c0 24 c0 28 00 6b c0 23   ···+·/·· ·$·(·k·#
00b0  c0 27 00 67 c0 0a c0 14  00 39 c0 09 c0 13 00 33   ·'·g···· ·9·····3
00c0  00 9d 00 9c 00 3d 00 3c  00 35 00 2f 00 ff 01 00   ·····=·< ·5·/····
00d0  00 a5 00 00 00 16 00 14  00 00 11 31 31 30 61 73   ******** ···110as
00e0  68 6f 70 2e 64 64 6e 73  2e 6e 65 74 00 0b 00 04   hop.ddns .net····
00f0  03 00 01 02 00 0a 00 0c  00 0a 00 1d 00 17 00 1e   ******** ********
0100  00 19 00 18 00 23 00 00  00 16 00 00 00 17 00 00   *****#·· ********
0110  00 0d 00 2a 00 28 04 03  05 03 06 03 08 07 08 08   ···*·(·· ********
0120  08 09 08 0a 08 0b 08 04  08 05 08 06 04 01 05 01   ******** ********
0130  06 01 03 03 03 01 03 02  04 02 05 02 06 02 00 2b   ******** *******+
0140  00 05 04 03 04 03 03 00  2d 00 02 01 01 00 33 00   ******** -******3·
0150  26 00 24 00 1d 00 20 0a  7f 48 41 64 32 24 ea 6b   &·$··· · ·HAd2$·k
0160  97 3f 97 29 fc 3a 29 fc  a4 e3 02 34 24 44 a6 b2   ·?·)·:)· ···4$D··
0170  0d 98 53 d4 74 90 46                               ··S·t·F
```

Observation:

1. Authenticated
2. encrypted

WireShark Results With SSL Encryption

Encrypted Message From Publisher to secured Broker

```
▸ Frame 52: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface wlp0s20f3, id 0
▸ Ethernet II, Src: IntelCor_6d:c9:4b (3c:58:c2:6d:c9:4b), Dst: HewlettP_f1:90:99 (50:65:f3:f1:90:99)
▸ Internet Protocol Version 4, Src: 10.1.0.111, Dst: 54.242.22.45
▸ Transmission Control Protocol, Src Port: 36740, Dst Port: 8883, Seq: 483, Ack: 3551, Len: 48
▾ Transport Layer Security
  ▸ TLSv1.3 Record Layer: Application Data Protocol: mqtt
  ▾ TLSv1.3 Record Layer: Application Data Protocol: mqtt
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 19
      Encrypted Application Data: 14b6d8aff3996ad6c308cf843750063d19567e
      [Application Data Protocol: mqtt]

0000  50 65 f3 f1 90 99 3c 58  c2 6d c9 4b 08 00 45 00   Pe····<X ·m·K··E·
0010  00 64 f0 5d 40 00 40 06  f2 a7 0a 01 00 6f 36 f2   ·d·]@·@· ·····o6·
0020  16 2d 8f 84 22 b3 ef 7d  39 5b 3d 38 63 6d 80 19   ··-··"··} 9[=8cm··
0030  00 3f 57 e5 00 00 01 01  08 0a 2a 29 35 c8 c9 5b   ·?W····· ··*)5··[
0040  55 8a 17 03 03 00 13 94  e2 e8 a6 3a b5 fa 25 70   U····· ···:··%p
0050  e7 93 08 08 9d 40 cf 40  79 ee 17 03 03 00 13 14   ·····@·@ y·····
0060  b6 d8 af f3 99 6a d6 c3  08 cf 84 37 50 06 3d 19   ·····j·· ···7P·=·
0070  56 7e                                              V~
```

Observation:

1. Authenticated
2. Encrypted