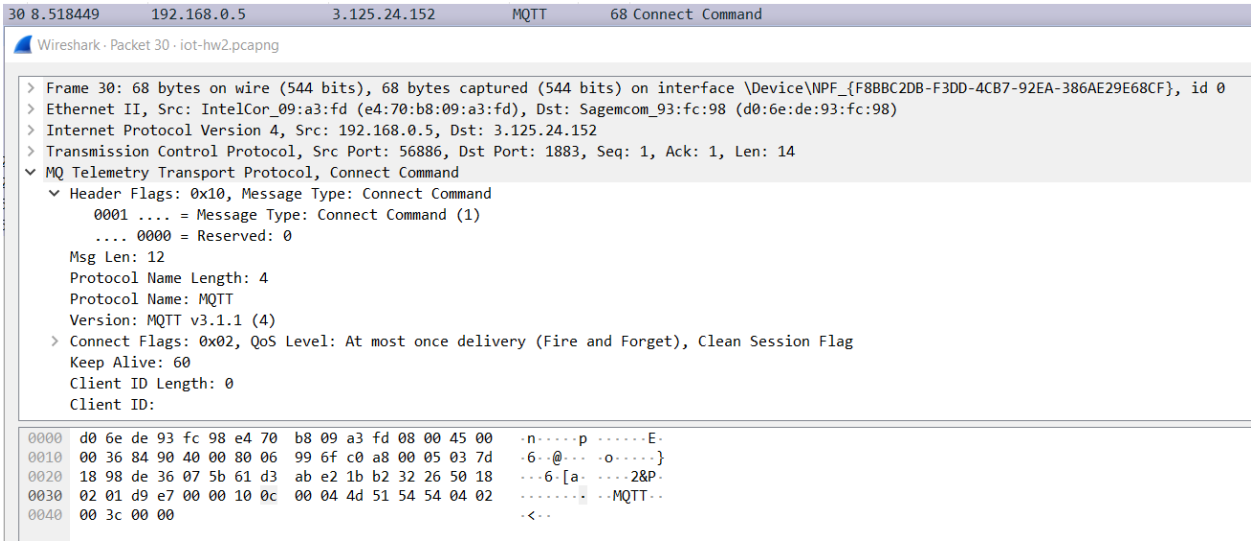
بنام خدا

برای تحلیل فایل ابتدا نرم‌افزار Wireshark را نصب کرده و سپس فایل با فرمت pcap را باز می‌کنیم و سپس ترافیک mqtt را فیلتر می‌کنیم.

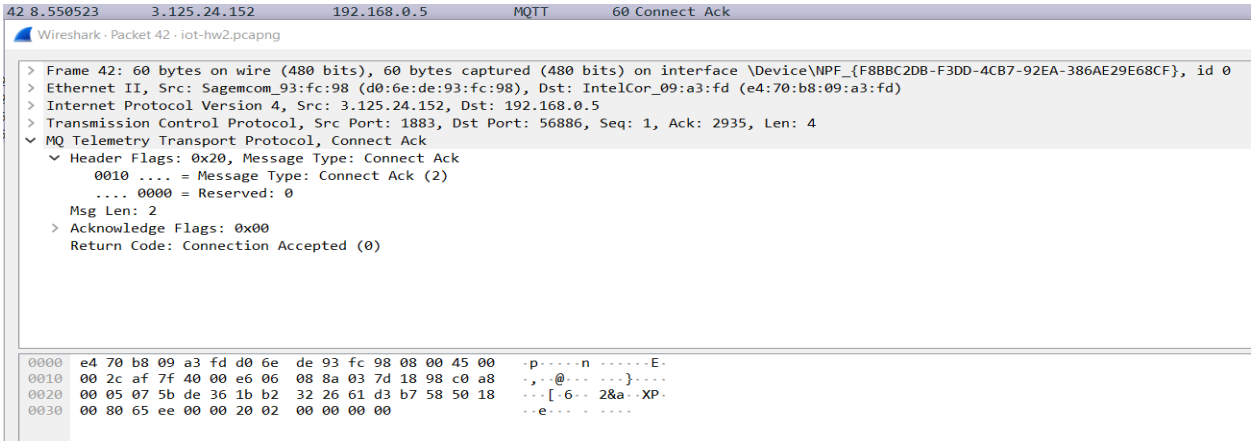
بنابر مفاهیمی که در کلاس درس توضیح داده شد تنها بسته‌های publish حاوی داده هستند. حال به بررسی آن‌ها می‌پردازیم.

بررسی بسته connect command:



همانطور که در شکل مشاهده می‌شود این پیغام connect command بوده و توسط مشتری برای درخواست ایجاد ارتباط به سمت بروکر ارسال می‌شود. این پیغام فاقد Payload است.

بررسی بسته connect ack:



همانطور که در شکل مشاهده می‌شود این پیغام Connect ack هست که پاسخ بروکر می‌باشد. همانطور که در شکل مشخص است بروکر مقدار 0 را برگردانده که بیان‌کننده قبول درخواست Connection می‌باشد. همانطور که مشخص است این پیغام Payload ندارد.

بررسی پیغام publish اول:

.1

```
MQ Telemetry Transport Protocol, Publish Message
  Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (Fire and Forget)
  Msg Len: 46
  Topic Length: 15
  Topic: sensors/radar/1
  Message: 20646574656374656420 6f626a6563742033206d696c6c696f6e206b6d
```

همانطور که در تصویر بالا مشخص است با توجه به Topic روی کانال sensor/data مقدار 1 publish می‌شود.

```
s/radar/ 1 detect
ed objec t 3 mill
ion km00 ··sensor
```

قسمت آبی در تصویر بالا نیز نشان‌دهنده Payload دیکد شده فیلد Message است.

.2

```
MQ Telemetry Transport Protocol, Publish Message
  Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (Fire and Forget)
  Msg Len: 48
  Topic Length: 15
  Topic: sensors/radar/2
  Message: 726164617220646574637469 6f6e2c20636865636b696e672075706c696e6b
```

بررسی Topic همانند پیغام قبلی بوده و Payload دیکد شده در تصویر زیر قابل مشاهده است.

```
s/radar/ 2radar d
etction,  checkin
g uplink 0$··sens
```

.3

```
MQ Telemetry Transport Protocol, Publish Message
  Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (Fire and Forget)
  Msg Len: 36
  Topic Length: 15
  Topic: sensors/radar/2
  Message: 6465746563746564206461746173747265616d
```

همانند موارد قبلی.

```
ors/rada r/2detec
ted data stream0.
```

.4

```
MQ Telemetry Transport Protocol, Publish Message
  > Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (Fire and Forget)
    Msg Len: 46
    Topic Length: 15
    Topic: sensors/radar/2
    Message: 2064657465637465642066f626a6563742033206d696c6c696f6e206b6d
```

```
2 detect ed objec
t 3 mill ion km0.
```

بررسی پیغام Publish دوم:

```
MQ Telemetry Transport Protocol, Publish Message
  > Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (Fire and Forget)
    Msg Len: 9318
    Topic Length: 15
    Topic: radio/message/1
    Message: 7b22646174612231a20226956424f5277304b47676f414141414e53556845556741414254…
```

همانطور که در قسمت Topic دیده می‌شود این پیام روی کانال radio/message مقدار 1 را publish می‌کند. با توجه به Payload این بسته و سرنخ‌هایی که در انتهای آن پیدا می‌شود می‌توان حدس زد که یک تصویر Decode شده و بصورت فایل json برگردانده می‌شود. با استفاده از سایت https://www.base64decode.net/base64-image-decoder محتوای درون فایل json را دیکد کرده و مشاهده می‌کنیم.

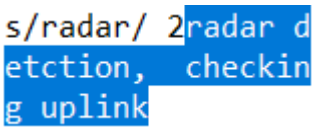
TG20{THIS IS A SHIP 2 SHIP MESSAGE: Prepare your disk spce for boarding}

بررسی پیغام publish سوم:

.1

```
MQ Telemetry Transport Protocol, Publish Message
  [Expert Info (Note/Protocol): Unknown version (missing the CONNECT packet?)]
  Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (Fire and Forget)
  Msg Len: 46
  Topic Length: 15
  Topic: sensors/radar/1
  Message: 2064657465637465642064f626a6563742033206d696c6c696f6e206b6d
```

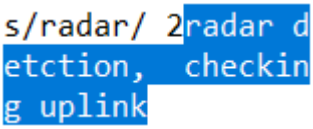
تحلیل این عکس نیز همانند دیگر پیغام‌ها است. Payload را در شکل زیر مشاهده می‌کنید.



.2

```
MQ Telemetry Transport Protocol, Publish Message
  [Expert Info (Note/Protocol): Unknown version (missing the CONNECT packet?)]
  Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (Fire and Forget)
  Msg Len: 48
  Topic Length: 15
  Topic: sensors/radar/2
  Message: 726164617220646574637469 6f6e2c20636865636b696e672075706c696e6b
```

مقدار Payload را در شکل زیر مشاهده می‌کنید.

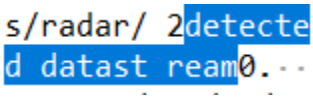


بررسی پیغام publish چهارم:

.1

```
MQ Telemetry Transport Protocol, Publish Message
  [Expert Info (Note/Protocol): Unknown version (missing the CONNECT packet?)]
  Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (Fire and Forget)
  Msg Len: 36
  Topic Length: 15
  Topic: sensors/radar/2
  Message: 646574656374656420646174617347265616d
```

همانند پیغام‌های قبلی.



.2

```
MQ Telemetry Transport Protocol, Publish Message
  > [Expert Info (Note/Protocol): Unknown version (missing the CONNECT packet?)]
  > Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (Fire and Forget)
    Msg Len: 46
    Topic Length: 15
    Topic: sensors/radar/2
    Message: 20646574656374656420f626a6563742033206d696c6c696f6e206b6d
```

```
0000  e4 70 b8 09 a3 fd d0 6e  de 93 fc 98 08 00 45 00   ·p·····n ·····E·
0010  00 7e 57 d9 40 00 e6 06  5f de 03 7d 18 98 c0 a8   ·~W·@··· _··}····
0020  00 05 07 5b de 1f df a9  7c 04 cd d0 85 2d 50 18   ···[···· |····-P·
0030  00 6a 4c f8 00 00 30 24  00 0f 73 65 6e 73 6f 72   ·jL···0$ ··sensor
0040  73 2f 72 61 64 61 72 2f  32 64 65 74 65 63 74 65   s/radar/ 2detecte
0050  64 20 64 61 74 61 73 74  72 65 61 6d 30 2e 00 0f   d datast ream0.··
0060  73 65 6e 73 6f 72 73 2f  72 61 64 61 72 2f 32 20   sensors/ radar/2
0070  64 65 74 65 63 74 65 64  20 6f 62 6a 65 63 74 20   detected  object
0080  33 20 6d 69 6c 6c 69 6f  6e 20 6b 6d               3 millio n km
```

بررسی پیغام publish پنجم:

.1

```
MQ Telemetry Transport Protocol, Publish Message
  > [Expert Info (Note/Protocol): Unknown version (missing the CONNECT packet?)]
  > Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (Fire and Forget)
    Msg Len: 9318
    Topic Length: 15
    Topic: radio/message/1
    Message: 7b2264617461223a20226956424f5277304b47676f414141414e5356845556741414254…
```

```
0010  67 65 2f 31 7b 22 64 61  74 61 22 3a 20 22 69 56   ge/1{"da ta": "iV
0020  42 4f 52 77 30 4b 47 67  6f 41 41 41 41 4e 53 55   BORw0KGg oAAAANSU
0030  68 45 55 67 41 41 42 54  6b 41 41 41 41 37 43 41   hEUgAABT kAAAA7CA
0040  49 41 41 41 41 2f 35 52  6d 62 41 41 41 41 41 58   IAAAA/5R mbAAAAAX
0050  4e 53 52 30 49 41 72 73  34 63 36 51 41 41 41 41   NSR0IArs 4c6QAAAA
0060  52 6e 51 55 31 42 41 41  43 78 6a 77 76 38 59 51   RnQU1BAA Cxjwv8YQ
0070  55 41 41 41 41 4a 63 45  68 5a 63 77 41 41 44 73   UAAAAJcE hZcwAADs
0080  4d 41 41 41 37 44 41 63  64 76 71 47 51 41 41 42   MAAA7DAc dvqGQAAB
0090  71 6f 53 55 52 42 56 48  68 65 37 5a 33 72 59 65   qoSURBVH he7Z3rYe
00a0  75 34 72 6f 57 6e 72 68  53 55 65 6c 4a 4e 6d 6e   u4roWnrh SUelJNmn
00b0  45 78 35 31 49 53 4a 59  41 6b 69 41 64 4a 79 64   Ex51ISJY AkiAdJyd
00c0  34 33 36 2f 73 31 59 34  46 34 4c 49 43 79 47 48   436/s1Y4 F4LICyGH
00d0  73 6e 2f 2f 30 50 41 41  41 41 41 41 41 41 41 41   sn//0PAA AAAAAAAA
00e0  41 41 6e 77 54 4f 36 67  41 41 41 41 41 41 41 41   AAnwTO6g AAAAAAAA
00f0  41 41 77 47 65 42 73 7a  6f 41 41 41 41 41 41 41   AAwGeBsz oAAAAAAA
0100  41 41 41 50 42 5a 34 4b  77 4f 41 41 41 41 41 41   AAAPBZ4K wOAAAAAA
0110  41 41 41 41 42 38 46 6a  69 72 41 77 41 41 41 41   AAAAB8Fj irAwAAAA
0120  41 41 41 41 41 41 6e 77  58 4f 36 67 41 41 41 41   AAAAAAnw XO6gAAAA
0130  41 41 41 41 41 41 77 47  65 42 73 7a 6f 41 41 41   AAAAAAwG eBszoAAA
```

این پیغام نیز همانند پیغام اول حاوی پیغامی انکد شده است که باید مانند همان پیغام دیکد شود. دیکد-شده این پیغام در تصویر زیر قابل مشاهده است.

TG20{THIS IS A SHIP 2 SHIP MESSAGE: Prepare your disk spce for boarding}

بررسی پیغام‌های MQTT Keep Alive:

223	28.573266	192.168.0.5	3.125.24.152	MQTT	56 Ping Request
224	28.606179	3.125.24.152	192.168.0.5	MQTT	60 Ping Response
558	88.648757	192.168.0.5	3.125.24.152	MQTT	56 Ping Request
559	88.682557	3.125.24.152	192.168.0.5	MQTT	60 Ping Response

این پیغام‌ها برای باز نگه داشتن ارتباط است. وظیفه چک‌کردن وضعیت ارتباط و حفظ آن بوسیله پیغام ping request به عهده مشتری است. مشتری باید این پیغام‌ها را در بازه‌های زمانی مشخص ارسال کرده و از باز بودن ارتباط اطمینان حاصل نماید. این بسته فاقد Payload می‌باشد. در جواب این پیغام بروکر باید با پیغام ping response پیام مشتری را تائید کند. این پیغام نیز فاقد Payload است. در شکل‌های زیر جزئیات این بسته‌ها را مشاهده می‌کنید.