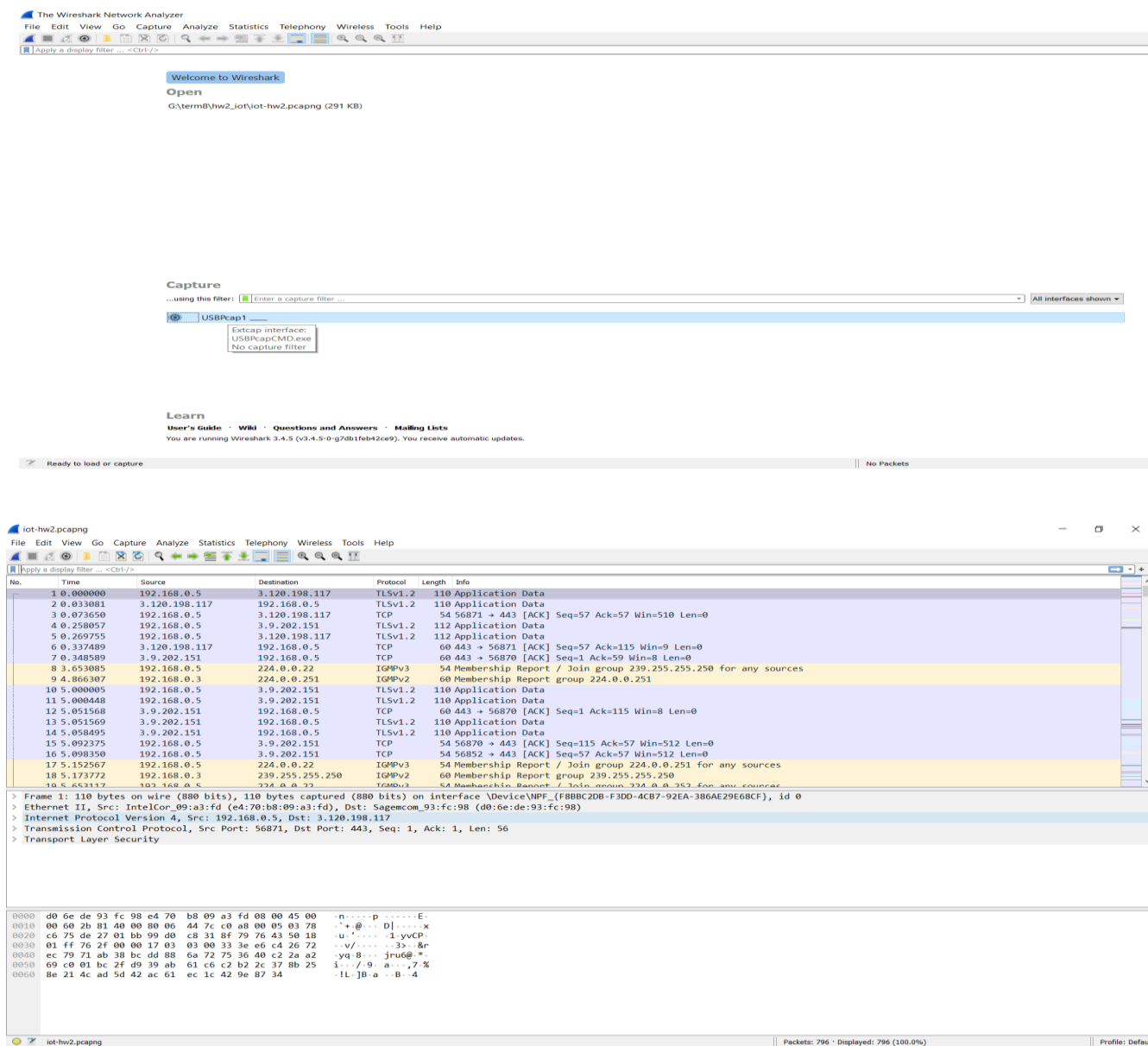


بخش دوم: تحلیل ترافیک MQTT

هدف کلی از این بخش آشنایی بیشتر شما با پکت های MQTT و تحلیل آن است. همراه صورت پروژه، فایل pcapng در اختیار شما قرار گرفته شده است که مربوط به ترافیک MQTT از قبل ضبط شده بین دو سیستم میباشد . شما باید به کمک Wireshark فایل pcapng را خوانده و پیام قابل خواندن منتشر شده را از پکت های MQTT استخراج کنید .برای تحویل این بخش گزارشی مختصر از نحوه استخراج پیام آماده کرده و به همراه پیام در پوشه گیت قرار دهید.

برای تحلیل ترافیک MQTT ابتدا نرم افزار wireshark را نصب کردیم و بعد فایل pcap موجود را ریکورد میکنیم



The screenshot displays the Wireshark Network Analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture, and analysis. The main window is divided into three panes: Packet List, Packet Details, and Packet Bytes.

Packet List: Shows a list of captured packets. The selected packet is No. 110, a TLSv1.2 Application Data packet, with a length of 110 bytes. The source is 192.168.0.5 and the destination is 192.168.0.5.

Packet Details: Shows the structure of the selected packet. The top section is 'Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface DeviceNPF_{F8B8C2DB-F3DD-4CB7-92EA-386AE29E68CF}, id 0'. The bottom section shows the 'Internet Protocol Version 4' and 'Transmission Control Protocol' details.

Packet Bytes: Shows the raw data of the selected packet in hexadecimal and ASCII. The data is displayed in a table with columns for offset, hexadecimal, and ASCII.

حال فیلتر میکنیم

No.	Time	Source	Destination	Protocol	Length	Info
30	8.518449	192.168.0.5	3.125.24.152	MQTT	68	Connect Command
31	8.522195	192.168.0.5	3.125.24.152	MQTT	1514	Publish Message [sensors/radar/1], Publish Message [sensors/radar/2], Publish Message [sensors/radar/2], Publish Message [s...
37	8.522207	192.168.0.5	3.125.24.152	MQTT	799	Publish Message [radio/message/1]
42	8.550523	3.125.24.152	192.168.0.5	MQTT	60	Connect Ack
46	8.557492	3.125.24.152	192.168.0.5	MQTT	152	Publish Message [sensors/radar/1], Publish Message [sensors/radar/2]
47	8.557493	3.125.24.152	192.168.0.5	MQTT	140	Publish Message [sensors/radar/2], Publish Message [sensors/radar/2]
54	8.557501	3.125.24.152	192.168.0.5	MQTT	615	Publish Message [radio/message/1]
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

> Frame 30: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface \Device\NPF_{F88BC20B-F3DD-4CB7-92EA-386AE29E68CF}, id 0
 > Ethernet II, Src: IntelCor_09:a3:fd (e4:70:b8:09:a3:fd), Dst: Sagemcom_93:fc:98 (d0:6e:de:93:fc:98)
 > Internet Protocol Version 4, Src: 192.168.0.5, Dst: 3.125.24.152
 > Transmission Control Protocol, Src Port: 56886, Dst Port: 1883, Seq: 1, Ack: 1, Len: 14
 > MQ Telemetry Transport Protocol, Connect Command

```

0000  d0 6e de 93 fc 98 e4 70 b8 09 a3 fd 08 00 45 00  .n....p.....E-
0010  00 36 84 90 40 00 80 06 99 6f c0 a8 00 05 03 7d  -6..@...o.....
0020  18 98 de 36 07 5b 61 d3 ab e2 1b b2 32 26 50 18  --6.[a.....2&P-
0030  02 01 d9 e7 00 00 10 0c 00 04 d4 51 54 54 04 02  .....--MQTT...
0040  00 3c 00 00                                     .<...
  
```

✓ حال info ها را تحلیل میکنیم

با توجه به info ها به طور کل میتوان گفت :

- پروتکل MQTT مبتنی بر TCP / IP است و هر دو client و broker باید یک پشته TCP / IP داشته باشند.
- publisher و subscriber هر دو به عنوان مشتری MQTT در نظر گرفته می شوند.
- ارتباط MQTT همیشه بین client و broker برقرار می شود ، هیچ client مستقیماً به client دیگری متصل نیست.
- به محض برقراری اتصال ، تا زمانی که client دستور قطع ارتباط را ارسال نکند یا اتصال را قطع کند ، broker آن را باز نگه خواهد داشت.
- MQTT از دستگاه های پشت دستگاه NAT (برای Ex-Router یا Firewall) پشتیبانی می کند.
- شناسه client (ClientId کوتاه) شناسه هر مشتری MQTT است که به یک کارگزار MQTT (broker) متصل می شود.

- Keep Alive یک بازه زمانی است ، client متعهد می شود به ارسال پیام های PING Request منظم به broker. این broker با PING Response پاسخ می دهد و این مکانیسم به هر دو طرف امکان می دهد تشخیص دهند که دیگری هنوز زنده است و قابل دسترسی است.

- پیام هایی که از نوع publish هستند در آن ها دیتا موجود هست و در آن دیتا جابه جا میشود اما بقیه پیام ها در جهت کنترل بسته هستند.

- اتصال از طریق client ارسال پیام "connect command" به broker آغاز می شود. پاسخ broker با "Connect Ack" و کد بازگشت است.

حال به بررسی هر کدام از پکت ها طبق تعاریف بالا میپردازیم

- آغاز اتصال از طریق client به broker و ارسال پیام "connect command" ارتباط mqtt بین مشتری و کارگزار است و هرگز مستقیماً با مشتری دیگری ارتباط برقرار نمی کند. شروع این اتصال با استفاده از یک دستور اتصال ارسال شده از مشتری به کارگزار است. اتصال ، پس از برقراری ارتباط ، تا زمانی که فرمان قطع ارتباط از مشتری را دریافت نمی کند ، باز نگه داشته می شود و قطع نمیشود .

Port مقصد 1883 است

- header flags: اطلاعات مربوط به نوع بسته کنترل mqtt را در خود نگه می دارد.
- Connect flags: بایت پرچم اتصال شامل پارامترهایی است که رفتار اتصال mqtt را مشخص می کند. این وجود یا عدم وجود فیلدها در محموله را نشان می دهد.
- Clean session: بیت 1 پرچم های اتصال. این پرچم نشانگر کارگزار است که آیا با مشتری می خواهد یک اتصال مداوم برقرار کند یا خیر. پرچم ، هنگامی که روی "true" تنظیم می شود ، منجر به یک clean session می شود که در آن قطع اشتراک ها در هنگام قطع اتصال است و هنگامی که روی "false" تنظیم می شود ، می توان در صورت باقی ماندن اشتراک ها و ارسال پیام های با کیفیت بالا در هنگام اتصال مجدد ، یک اتصال مداوم برقرار شود
- will flag: بیت 2 از پرچم های اتصال. این پرچم ، هنگام تنظیم ، به این معنی است که ، در صورت پذیرفته شدن درخواست اتصال ، پیام باید در سرور ذخیره شود. یک پیام یک پیام mqtt با یک موضوع و یک پیام است. این در حالی است که به سایر مشتریان در مورد قطع ارتباط اطلاع داده می شود. با قطع ارتباط مشتری ، کارگزار این پیام را از طرف وی ارسال می کند. هنگامی که پرچم will به 1 تنظیم شود ، will qos و will retain زمینه هایی را در پرچم های اتصال که توسط سرور استفاده می شود حفظ می کند.
- will qos: بیت 4 و 3 از پرچم های اتصال. سطح qos را نشان می دهد تا هنگام انتشار پیام will استفاده شود.
- Will retain: بیت 5 از پرچم های اتصال. اگر Retain روی 0 تنظیم شده است ، سرور باید پیام will را به عنوان پیام غیرقابل نگهداری منتشر کند و وقتی روی 1 تنظیم شود ، پیام will به عنوان یک پیام retained منتشر می شود.

- Username , password: بیت 7 و 6 پرچم اتصال به ترتیب. هنگامی که این زمینه ها تنظیم می شود ، انتظار می رود اعتبار در محموله بارگیری شود. mqtt اجازه می دهد تا نام کاربری و رمز عبور را برای احراز هویت مشتری و مجوز ارسال کنید. اگر رمز عبور در زیر رمزگذاری نشده باشد ، به متن ساده ارسال می شود.
- Keep alive: از alive timer استفاده می شود تا بدانند مشتری mqtt در شبکه ای است که مشتری پیامهای درخواست پینگ منظم را به کارگزار ارسال می کند. کارگزار با پاسخ پینگ پاسخ می دهد.
- Client id: شناسه ای است برای هر مشتری mqtt که به یک کارگزار mqtt متصل می شود. این باید برای هر کارگزار منحصر به فرد باشد.
- payload: payload شامل شناسه مشتری است ، در قسمت عنوان ، پیام ، نام کاربر و قسمت های رمز عبور که حضور آنها توسط پرچم ها تعیین می شود ، خواهد بود.

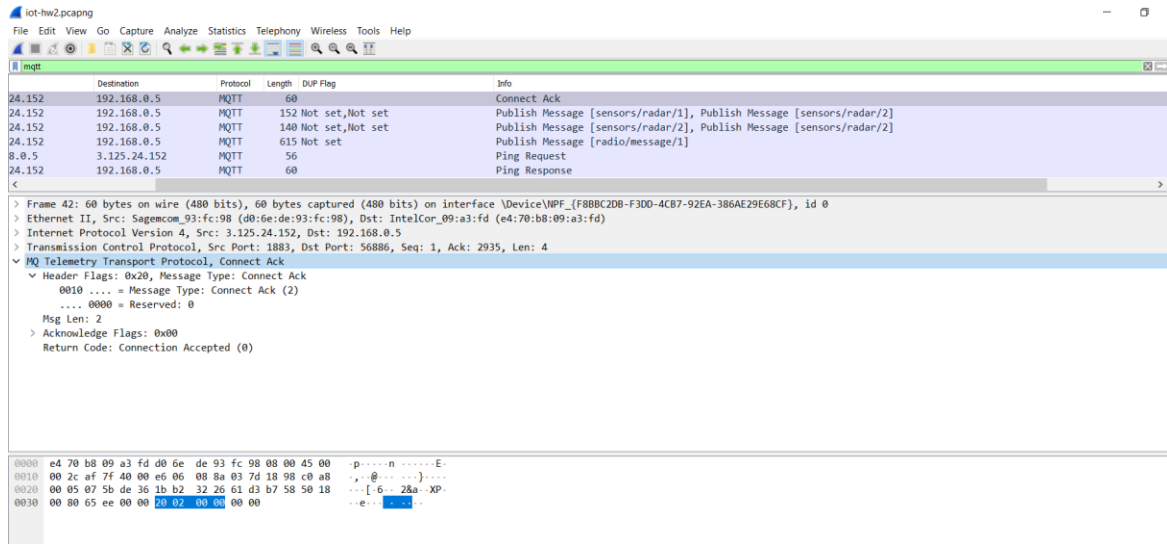
mqtt						
No.	Time	Source	Destination	Protocol	Length	Info
	30 8.518449	192.168.0.5	3.125.24.152	MQTT	68	Connect Command
> Frame 30: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface \Device\NPF_{F8BBC2DB-F3DD-4CB7-92EA-386AE29E68CF}, id 0						
> Ethernet II, Src: IntelCor_09:a3:fd (e4:70:b8:09:a3:fd), Dst: Sagemcom_93:fc:98 (d0:6e:de:93:fc:98)						
> Internet Protocol Version 4, Src: 192.168.0.5, Dst: 3.125.24.152						
> Transmission Control Protocol, Src Port: 56886, Dst Port: 1883, Seq: 1, Ack: 1, Len: 14						
MQ Telemetry Transport Protocol, Connect Command						
Header Flags: 0x10, Message Type: Connect Command						
0001 = Message Type: Connect Command (1)						
.... 0000 = Reserved: 0						
Msg Len: 12						
Protocol Name Length: 4						
Protocol Name: MQTT						
Version: MQTT v3.1.1 (4)						
Connect Flags: 0x02, QoS Level: At most once delivery (Fire and Forget), Clean Session Flag						
0... = User Name Flag: Not set						
.0.. = Password Flag: Not set						
..0. = Will Retain: Not set						
...0 0... = QoS Level: At most once delivery (Fire and Forget) (0)						
.... .0.. = Will Flag: Not set						
.... ..1. = Clean Session Flag: Set						
.... ...0 = (Reserved): Not set						
Keep Alive: 60						
Client ID Length: 0						
Client ID:						

- Connect ack پاسخ broker هست که با کد بازگشتی همراه است. که کد بازگشتی 0 هست یعنی accept connection

- header flags: اطلاعات مربوط به نوع بسته کنترل mqtt را در خود نگه می دارد.
- session present: بیت 0 اتصال که ack byte پرچم جلسه فعلی است. این پرچم نشان می دهد که آیا کارگزار از تعاملات قبلی جلسه مداوم مشتری را دارد یا خیر.
- Return code: مقادیر و پاسخ های کد بازگشت

Return Code	Return Code Response
0	Connection Accepted
1	Connection Refused, unacceptable protocol version
2	Connection Refused, identifier rejected
3	Connection Refused, Server unavailable
4	Connection Refused, bad user name or password
5	Connection Refused, not authorized

- payload: بسته اتصال هیچ محموله ای ندارد.



- ما در اینجا 5 تا مسیج داریم و قابل خواندن هستن چون از نوع publish هستند و پیام ان ها مشخص هست.
 - هنگامی که مشتری mqtt به کارگزار متصل شد ، می تواند پیام ها را منتشر کند.
 - header flags: اطلاعات مربوط به نوع بسته کنترل mqtt را در خود نگه می دارد.
 - dup flag: وقتی که dup flag صفر باشد ، به این معنی است که این اولین تلاش برای ارسال این بسته انتشار است. اگر dup flag 1 باشد ، نشانگر تلاش مجدد برای ارسال پیام است.
 - qos: سطح qos سطح اطمینان پیام را تعیین می کند.
 - retain flag: اگر retain flag روی 1 تنظیم شده باشد ، سرور باید پیام و qos آن را ذخیره کند ، تا بتواند اشتراک های آینده را با موضوع مطابقت دهد. هنگامی که یک بسته انتشار به یک مشتری مشترک ارسال می شود ، اگر بسته به دلیل اشتراک جدید ارسال شود ، سرور باید پرچم نگهدارنده را روی 1 تنظیم کند. هنگام ارسال بسته ، سرور باید پرچم نگهدارنده را روی 0 تنظیم کند زیرا صرف نظر از اینکه پرچم هنگام دریافت پیام تنظیم شده باشد ، با یک اشتراک ثابت مطابقت دارد.
 - Topic name: رشته utf-8 که در صورت نیاز به ساختار سلسله مراتبی ، می تواند حاوی اسلش های رو به جلو نیز باشد. پیام انتشار باید حاوی موضوعی باشد که توسط کارگزار برای فیلتر کردن موضوع استفاده می شود. به این ترتیب کارگزار برای مشتریانی که در این موضوع مشترک شده اند پیام می فرستد.
 - message: پیام payload همراه با موضوع است که شامل داده های واقعی برای انتقال است. از آنجا که mqtt داده های تجربی است ، می توان محموله را بر اساس مورد استفاده ساخت.
 - payload: محموله شامل پیامی است که منتشر می شود.

- Decode کردن پیام های payload پکت ها :

1. روی چنل sensors و radar مقدار یک را پابلیش کن

Message:

206465746563746564206f626a6563742033206d696c6c696f6e206b6d

detected object 3 million km

2. روی sensor و radar مقدار دو را پابلیش کن

Message:

f6e2c20636865636b696e672075706c696e6b7261646172206465746374696

radar detction, checking uplink

3. روی sensor و radar مقدار دو را پابلیش کن

Message:

d6465746563746564206461746173747265616

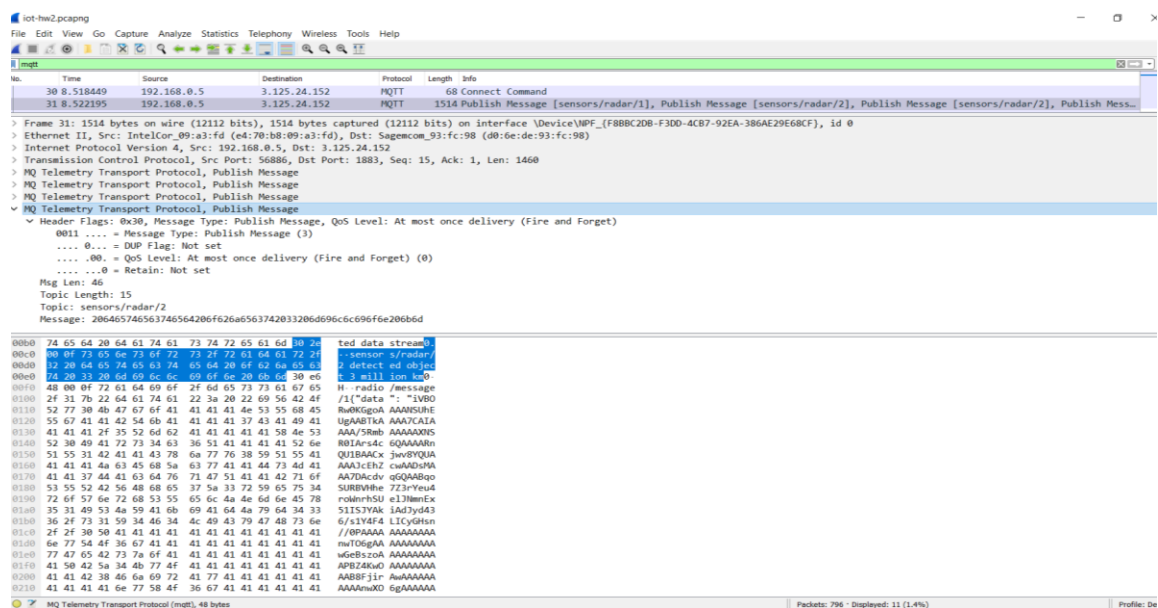
detected datastream

4. روی sensor و radar مقدار دو را پابلیش کن

Message:

f626a6563742033206d696c6c696f6e206b6d206465746563746564206

detected object 3 million km



1. روی چنل sensors و message مقدار یک را پابلیش کن

یک فایل json بر میگرداند

- ابتدا کلید های پکت رو پیدا میکنیم همین طور که در تصویر پایین میبینید شامل `data` , `pos` , `pic_id` , `c_id` , `size` ("pos": 0, "pic_id": "ojyheibq", "size": 0.0) هست و از کلید های ان میتوان حدس زد قالب تصویر است پس فایل جیسون رمزگذاری شده و `encode` شده را `decode` میکنیم توسط سایت زیر

<https://codebeautify.org/base64-to-image-converter>

Time	Source	Destination	Protocol	Length	DUP Flag	Info
30 8.518449	192.168.0.5	3.125.24.152	MQTT	68		Connect Command
31 8.522195	192.168.0.5	3.125.24.152	MQTT	1514	Not set,Not set,Not set	Publish Message [sensors/radar/1], Publish Message [sensors/radar/2], Pu
37 8.522207	192.168.0.5	3.125.24.152	MQTT	799	Not set	Publish Message [radio/message/1]

Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (Fire and Forget)

```
0011 .... = Message Type: Publish Message (3)
.... 0... = DUP Flag: Not set
.... .00. = QoS Level: At most once delivery (Fire and Forget) (0)
.... ...0 = Retain: Not set
```

Msg Len: 9318

Topic Length: 15

Topic: radio/message/1

Message: 7b2264617461223a20226956424f5277304b47676f41414141e53556845556741414254.

74	75	79	68	69	2b	32	48	33	75	36	2f	6a	62	78	tuylj1+12	H3u6/cj			
76	36	6d	67	6b	41	41	41	43	41	45	43	43	77	49	63	vbmKAAa	JAbxJb		
4d	65	4c	71	45	36	36	49	48	74	41	34	41	44	71	74	MeLqE6L	HTAAAD01		
35	4f	49	74	39	45	46	4c	26	74	37	2b	63	71	58	61	OU097613	137+cqct		
77	65	67	66	25	53	51	5d	2f	79	51	59	41	41	41	41	72	guf/UZQ	MYAYAA	
42	75	42	59	63	45	66	35	4d	43	56	6c	41	46	32	32	BU9YCNK	5KcVIA47		
77	66	41	48	78	34	2f	3f	71	67	38	46	66	77	60	77	ufvAhKd/7	g8bFgm		
50	26	79	73	32	47	33	71	4d	38	74	66	31	63	70	37	Pyys3G5	8KbfL7147		
59	48	41	41	41	41	41	42	72	67	48	77	66	36	36	71	UJbAaAa	rgbfuHfAA		
77	66	41	41	41	41	41	41	41	41	41	41	41	41	41	41	72	guf/UZQ	MYAYAA	
38	75	48	75	32	4f	58	68	32	39	34	2f	5a	2b	33	33	78	X0u200x	2+04/32	
48	6a	33	32	61	47	2f	71	62	65	78	35	77	66	67	32	32	BK132aG	qbeu5XAA	
63	41	41	41	41	41	41	41	41	41	41	44	34	4c	6e	4e	4d	U8AAAAA	AAAADLNA	
55	42	41	41	41	41	41	41	41	41	41	49	44	50	41	6d	4d	U8AAAAA	AAAADPAA	
42	5a	48	51	41	41	41	41	41	41	41	41	41	41	41	41	41	U9HAAAA	AAAADLNA	
78	56	67	63	41	41	41	41	41	41	41	41	41	41	41	41	41	5aVcAAa	AAAAAAAA	
34	4c	4e	55	42	41	41	41	41	41	41	41	41	41	41	41	41	41	41	NU8AAAA
44	50	41	64	64	31	41	41	41	41	41	41	41	41	41	41	41	41	41	DPAAADJAA
46	73	38	42	56	48	51	41	41	41	41	41	41	41	41	41	41	41	41	41
41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41
41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41
41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41
67	76	72	51	48	28	49	41	41	41	41	41	41	41	41	41	41	41	41	41
35	42	52	6b	46	67	67	67	32	22	2c	20	22	60	77	60	41	41	41	41
50	22	70	20	30	28	29	29	62	71	63	57	60	64	22	38	38	38	38	38
50	22	67	20	30	28	29	29	62	71	63	57	60	64	22	38	38	38	38	38
7a	62	67	20	30	28	29	29	62	71	63	57	60	64	22	38	38	38	38	38

A screenshot of the 'Base64 to Image' web application. The interface includes a navigation bar at the top with links like 'JSON Formatter', 'XML Formatter', etc., and a 'Login' button. The main heading is 'Base64 to Image'. Below it is a text input area labeled 'Enter Base64 String' containing a long base64 string. To the right of the input are icons for sample, copy, and paste, along with an 'Auto Update' checkbox. A green 'Generate Image' button is prominent. Below this are smaller buttons for 'File' and 'URL' upload methods, and a 'Download Image' button. The generated image is displayed below the buttons, showing the decoded message: 'TG20{THIS IS A SHIP 2 SHIP MESSAGE: Prepare your disk spce for boarding}'. At the bottom right, the file size is indicated as '9.03 KB, 9244 chars'.

و تصویری که به ما میدهد این متن هست

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

1. روی چنل sensors و radar مقدار یک را پابلیش کن

Message:

f626a6563742033206d696c6c696f6e206b6d206465746563746564206

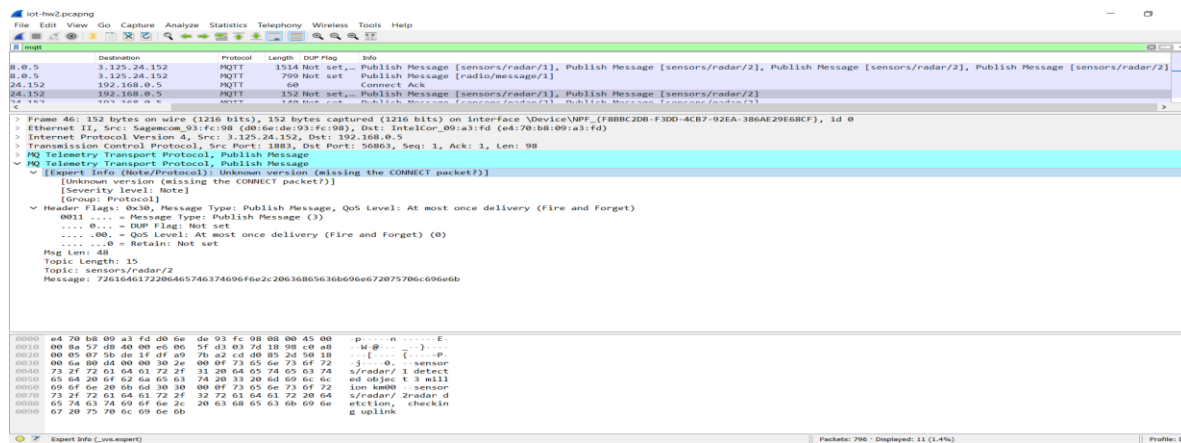
detected object 3 million km

2. روی چنل sensors و radar مقدار دو را پابلیش کن

Message:

f6e2c20636865636b696e672075706c696e6b7261646172206465746374696

radar detction, checking uplink



1. روی چنل sensors و radar مقدار دو را پابلیش کن

Message:

d6465746563746564206461746173747265616

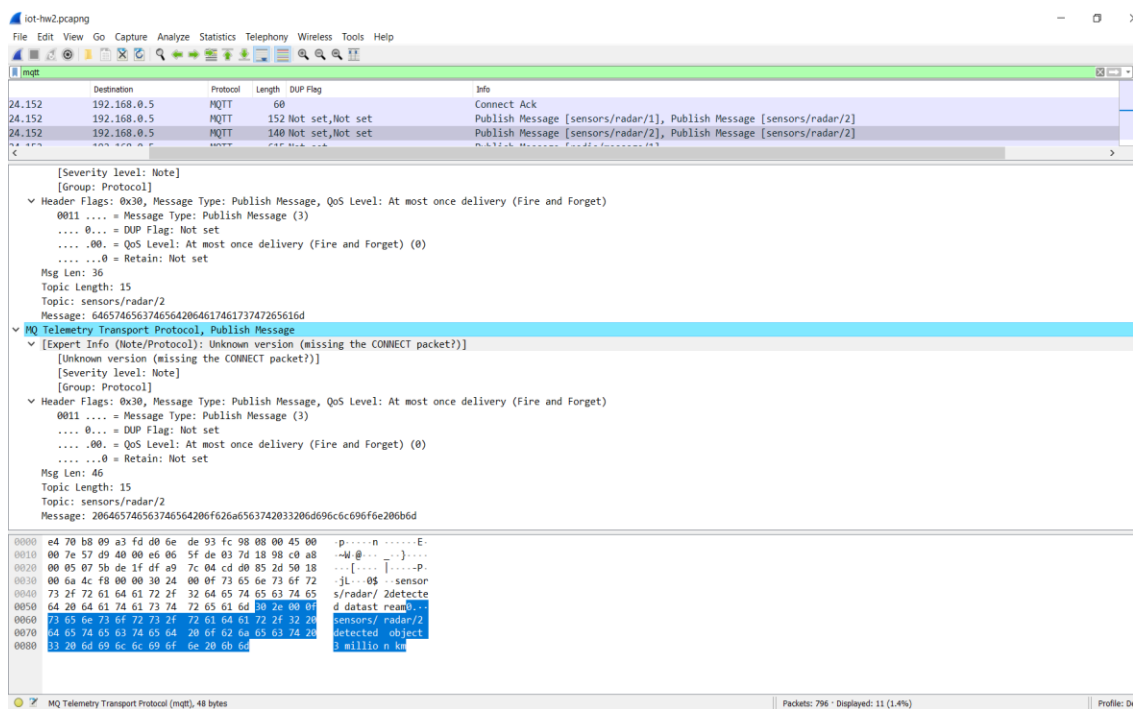
detected datastream

2. روی چنل sensors و radar مقدار دو را پابلیش کن

Message:

f626a6563742033206d696c6c696f6e206b6d206465746563746564206

detected object 3 million km

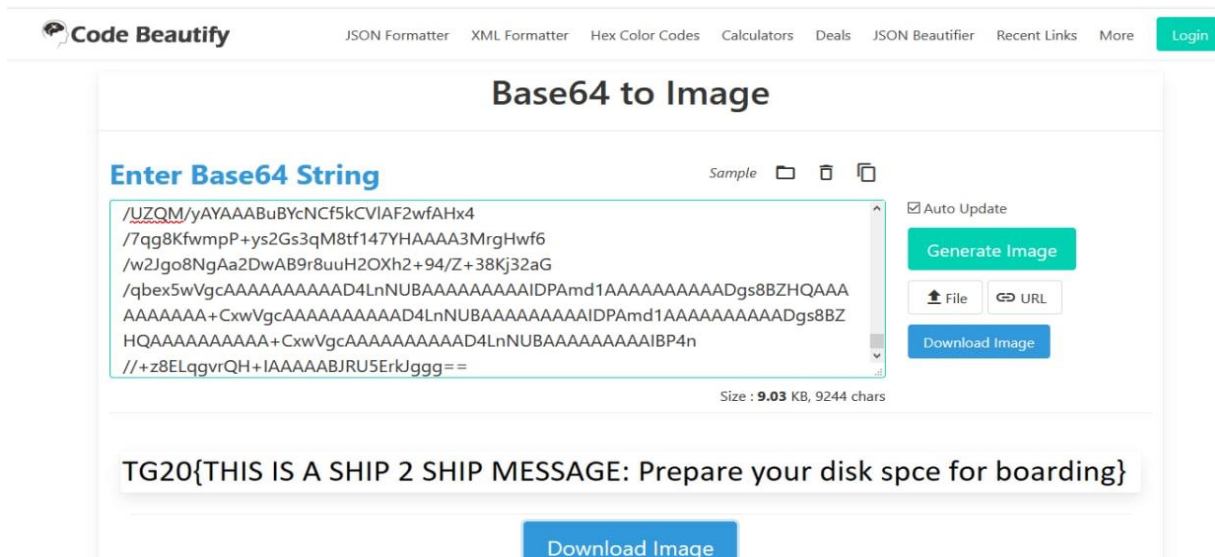


1. روی چنل sensors و radar مقدار یک را پابلیش کن

یک فایل json برمیگردونه.

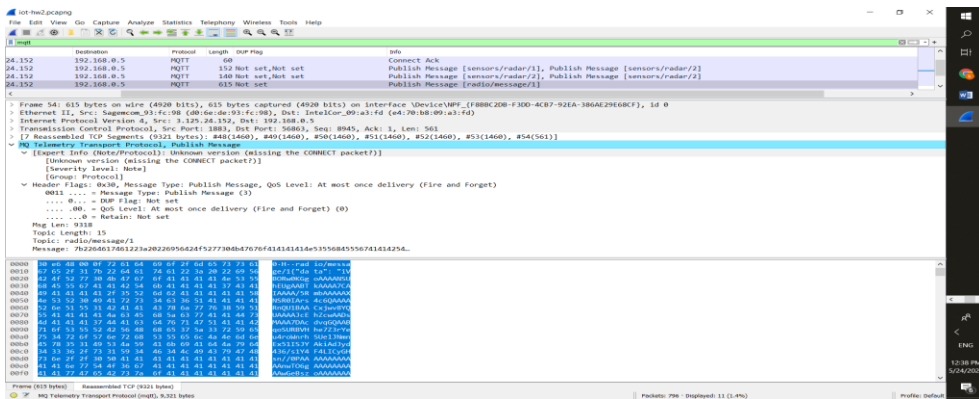
- ابتدا کلید های پکت رو پیدا میکنیم همین طور که در تصویر پایین میبینید شامل data , pos , pic_id , size , c_id , size ("pos": 0, "pic_id": "ojyheibq", "size": 0.0) هست و از کلید های ان میتوان حدس زد قالب تصویر است پس فایل جیسون رمزگذاری شده و encode شده را decode میکنیم توسط سایت زیر

<https://codebeautify.org/base64-to-image-converter>



و تصویری که به ما میدهد این متن هست

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



- قطع اتصال پیام بسته کنترل نهایی است که توسط مشتری به کارگزار ارسال می شود. این به معنای قطع ارتباط پاک توسط مشتری است.

- header flags: اطلاعات مربوط به نوع بسته کنترل mqtt را در خود نگه می دارد.
- payload: بسته disconnect فاقد محموله است.

❖ Mqtt keep alive

Keep alive با پیام های pingreq و pingresp حفظ می شود.

8.0.5	3.125.24.152	MQTT	56	Ping Request
24.152	192.168.0.5	MQTT	60	Ping Response
8.0.5	3.125.24.152	MQTT	56	Ping Request
24.152	192.168.0.5	MQTT	60	Ping Response

- پیام ping req که مشتری در یک بازه زمانی این پیام را به broker ارسال میکند . که ببیند هنوز کارگزار وجود دارد یا نه .

mqtt specification می گوید:

"این مسئولیت مشتری است که اطمینان حاصل کند که فاصله بین بسته های کنترل ارسال شده از حد زنده نگه ندارد. در صورت عدم ارسال بسته های کنترل دیگر ، مشتری باید یک بسته pingreq ارسال کند.

- header flags: اطلاعات مربوط به نوع بسته کنترل mqtt را در خود نگه می دارد.
- payload: بسته pingreq فاقد محموله است.

iot-hw2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

mqtt

	Destination	Protocol	Length	DUP Flag	Info
8.0.5	3.125.24.152	MQTT	68		Connect Command
8.0.5	3.125.24.152	MQTT	1514	Not set, Not set, Not set, Not set	Publish Message [sensors/radar/1], Publish Message [sensors/radar/2], Publish Message [sensors/radar/2]
8.0.5	3.125.24.152	MQTT	799	Not set	Publish Message [radio/message/1]
24.152	192.168.0.5	MQTT	60		Connect Ack
24.152	192.168.0.5	MQTT	152	Not set, Not set	Publish Message [sensors/radar/1], Publish Message [sensors/radar/2]
24.152	192.168.0.5	MQTT	140	Not set, Not set	Publish Message [sensors/radar/2], Publish Message [sensors/radar/2]
24.152	192.168.0.5	MQTT	615	Not set	Publish Message [radio/message/1]
8.0.5	3.125.24.152	MQTT	56		Ping Request
24.152	192.168.0.5	MQTT	60		Ping Response

<

> Frame 223: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF_{F8B8C2D8-F3D0-4CB7-92EA-386AE29E68CF}, id 0
 > Ethernet II, Src: IntelCor_09:a3:fd (e4:70:b8:09:a3:fd), Dst: Sagemcom_93:fc:98 (d0:6e:de:93:fc:98)
 > Internet Protocol Version 4, Src: 192.168.0.5, Dst: 3.125.24.152
 > Transmission Control Protocol, Src Port: 56863, Dst Port: 1883, Seq: 1, Ack: 9506, Len: 2

▼ **MQ Telemetry Transport Protocol, Ping Request**

- ▼ [Expert Info (Note/Protocol): Unknown version (missing the CONNECT packet?)]
 - [Unknown version (missing the CONNECT packet?)]
 - [Severity level: Note]
 - [Group: Protocol]
- ▼ Header Flags: 0xc0, Message Type: Ping Request
 - 1100 = Message Type: Ping Request (12)
 - 0000 = Reserved: 0

Msg Len: 0

```

0000 d0 6e de 93 fc 98 e4 70 b8 09 a3 fd 08 00 45 00  .n.....p .....E.
0010 00 2a 84 9d 0d 00 00 06 99 6e c0 a8 00 05 03 7d  .*..@... .n.....}
0020 18 98 de 1f 07 5b cd d0 85 2d df a9 a0 c3 50 18  ....[... ..P.
0030 01 fc 58 25 00 00 c0 00  .X%...
  
```

- پیام ping res که کارگزار در یک بازه زمانی این پیام را به مشتری ارسال میکند. این نشان دهنده در دسترس بودن کارگزار برای مشتری است.
- header flags: اطلاعات مربوط به نوع بسته کنترل mqtt را در خود نگه می دارد.
- payload: بسته pingresp فاقد محموله است.

iot-hw2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

mqtt

	Destination	Protocol	Length	DUP Flag	Info
24.152	192.168.0.5	MQTT	615	Not set	Publish Message [radio/message/1]
8.0.5	3.125.24.152	MQTT	56		Ping Request
24.152	192.168.0.5	MQTT	60		Ping Response
8.0.5	3.125.24.152	MQTT	56		Ping Request
24.152	192.168.0.5	MQTT	60		Ping Response

<

> Frame 224: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{F8B8C2D8-F3D0-4CB7-92EA-386AE29E68CF}, id 0
 > Ethernet II, Src: Sagemcom_93:fc:98 (d0:6e:de:93:fc:98), Dst: IntelCor_09:a3:fd (e4:70:b8:09:a3:fd)
 > Internet Protocol Version 4, Src: 3.125.24.152, Dst: 192.168.0.5
 > Transmission Control Protocol, Src Port: 1883, Dst Port: 56863, Seq: 9506, Ack: 3, Len: 2

▼ **MQ Telemetry Transport Protocol, Ping Response**

- ▼ [Expert Info (Note/Protocol): Unknown version (missing the CONNECT packet?)]
 - [Unknown version (missing the CONNECT packet?)]
 - [Severity level: Note]
 - [Group: Protocol]
- ▼ Header Flags: 0xd0, Message Type: Ping Response
 - 1101 = Message Type: Ping Response (13)
 - 0000 = Reserved: 0

Msg Len: 0

```

0000 e4 70 b8 09 a3 fd d0 6e de 93 fc 98 08 00 45 00  p.....n .....E.
0010 00 2a 57 e1 00 00 e0 06 60 2a 03 7d 18 98 c0 a8  .*..@... .n.....}
0020 00 05 07 5b de 1f df a9 a0 c3 cd d0 85 2f 50 18  ....[... ..P.
0030 00 6a 49 b5 00 00 d0 00  .jI... ..
  
```