Internet of Things

Challenge 1

Politecnico di Milano

A.A. 2021-2022

Student : Valeria Maria Fortina

ID: 10537962

COAP

QUESTION 1

What are the differences between the request with MID: 53533 and the one with MID: 42804

Using the filter `coap.mid==MESSAGE_ID` on Wireshark I found the information on these two requests. The request with MID: 53533 is of the type CONFIRMABLE and so it needs to be acknowledged, and it is also a GET. The other one is NON-CONFIRMABLE and it's a DELETE.

QUESTION 2

What is the response of message No. 2428, if any?

Using the filter `frame.number==2428` on Wireshark I found a message with MID = 12935 and token 67c7229a. Then with `coap.token == 67:c7:22:9a` I have found the response which has mid=844, the response is that the path /living_room/door is deleted.

Internet of Things

Challenge 1

QUESTION 3

How many replies to requests of type confirmable, having result code "Content" are received by the client "localhost"?

Since the client must be "localhost" I used the filter `ip.addr==127.0.0.1` where 127.0.0.1 is the localhost IP address. I combined this filter with the filter `coap.code==69` for the code "2.05 Content". I have found 8 ACK with these constraints.

```
ip.addr==127.0.0.1 && coap.code==69
```

QUESTION 4

*How many GET requests, **excluding OBSERVE requests**, have been directed to non existing resources?*

Identifying only requests directed to non-existing resources means filtering for the code of "4.04 Not found" and for doing that I used the filter `coap.code==132,` then I compared the MID number to find the matched requests, and I selected only the GET with the filter coap.code==1. I used the filter `coap.opt.observe` with a negation to exclude any observe requests.

I have found 6 requests which satisfy these constraints.

Internet of Things

Challenge 1

MQTT

QUESTION 5

How many messages containing the topic "factory/department/+" are published by a client with user password: "admin"? Where * replaces only the dep. number [0-9], e.g. factory/department1/+, factory/department2/+ and so on. (* is NOT an MQTT wildcard)*

To identify the client I used the Wireshark filter `mqtt.passwd="admin",` I added with && the filter `mqtt.topic ~ "^factory\/department[0-9]+\/[^\/]+$"` for selecting "factory/department*/+". I used [^\/]+$ to ensure that the one level operator "+" was respected, at this level I haven't found any messages, so the answer is 0.

QUESTION 6

How many clients connected to the public broker "mosquitto" have specified a will message?

To identify the broker I can use the IP address, I used the filter:

`dns.a && dns.qry.name=="test.mosquitto.org"` and I have found the IP: 5.196.95.208

Then I used a composition of Wireshark filters: `ip.addr == 5.196.95.208 && mqtt.conflag.willflag == 1`

I have found 9 results.

Internet of Things

Challenge 1

QUESTION 7

How many publishes with QoS 2 don't receive the PUBREL?

I used the filter `mqtt.qos==2` to get only QoS 2, then I combined it with && `mqtt.msgtype==3` for selecting the publish messages, and I have found 94 results. Then I used the filter `mqtt.msgtype==6,` which corrispond to the Publish Release`,` to find the number of PUBREL. The result is 0. This means that 94 packets (with QoS 2) didn't receive the PUBREL.

QUESTION 8

What is the average Will Topic Length specified by clients with empty Client ID?

To get all the empty Client Id I used the filter `Mqtt.clientid==“”`. Then I combined with &&! the filter `_ws.malformed` to get rid of all the malformed messages, finally, I added with && the filter `mqtt.willmsg` to find all the messages with the last will. I have found 22 results. After that, I easly computed the average with a computation, which is 37.

Internet of Things

Challenge 1

QUESTION 9

How many ACKs received the client with ID "6M5H8y3HJD5h4EEscWknTD"? What type(s) is(are) it(them)?

Using the filter `mqtt.clientId` I have found the message from this client and with that, I have found the src port and the dst port, then I used the filter `tcp.dstport=46295` combined with `mqtt.msgtype==2` then `mqtt.msgtype==4` and finally `mqtt.msgtype==9` using an or. I have found 5 ACK, 1 connect, 1 publish and 3 subscribe.

```
tcp.dstport=46295 && (mqtt.msgtype==2 ||
mqtt.msgtype==4 || mqtt.msgtype==9)
```

QUESTION 10

What is the average MQTT message length of the CONNECT messages using mqttv3.1 protocol? Why messages have different size?

I used the filter `mqtt.ver==3` to get the right protocol, then combined the filter with && `mqtt.msgtype==1` to get only connect messages, I have found 47 results. After a calculation, I have found that the average message length is 63 bytes. Messages have different sizes due to the fact that a Connect message could have optional fields.