Security in IoT Ecosystem

Module 7

Smart Socket Pentest
Part II

Prof.: Joaquín Recas

Smart Socket Initial Setup

1. Initial Setup
   - Linux Virtual Machine
   - Raspberry Pi
   - Pair the Smart Socket
2. Capture Traffic
3. Traffic analysis

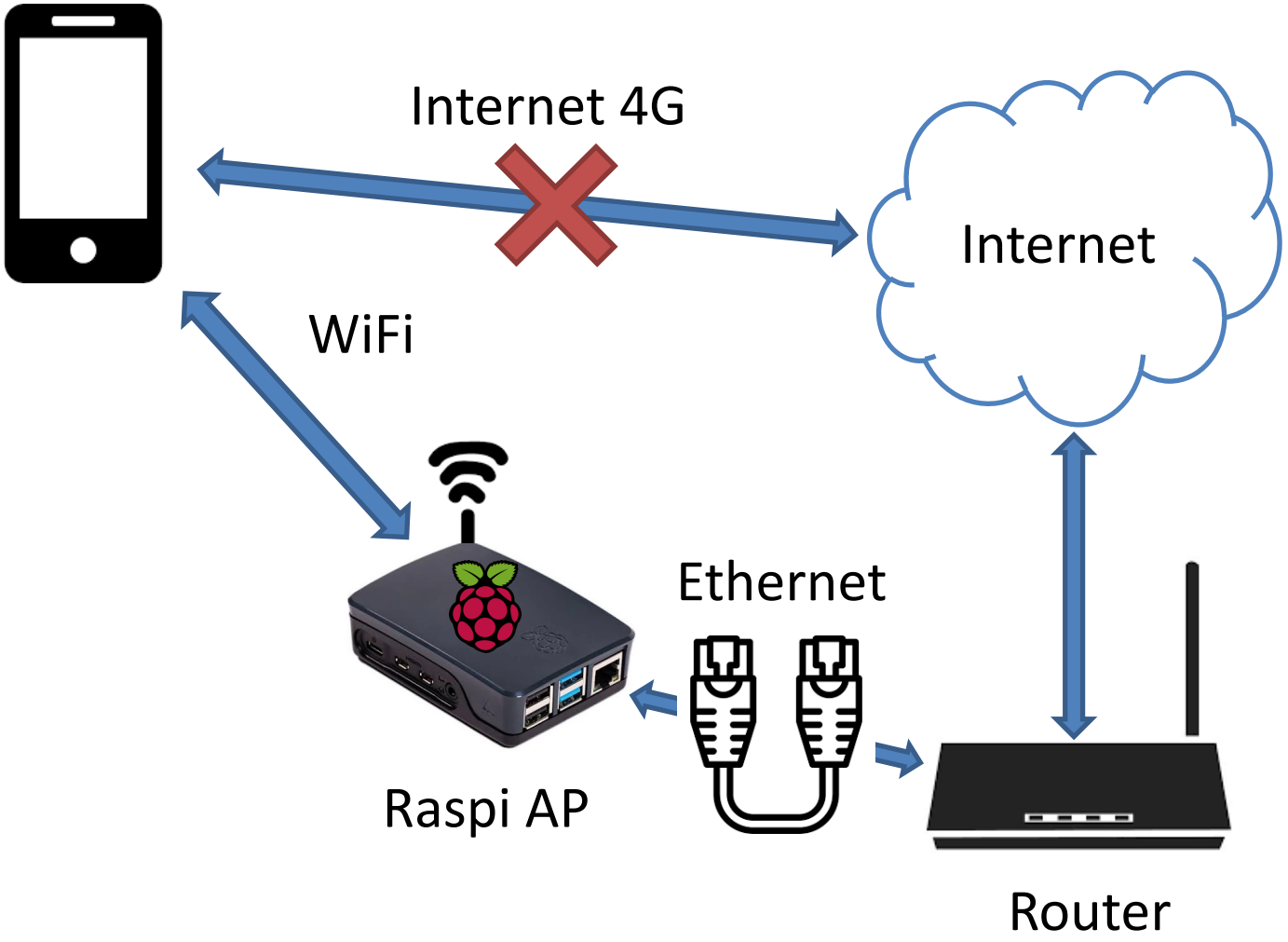
Initial Setup: Linux VM

1. Prepare the Linux Virtual Machine
   - Wireshark (already installed)
   - JADX Dex to Java decompiler
     - github project homepage
     - Download releases from github
   - Binary Ninja homepage link
     - Demo version link

Initial Setup: raspberry Pi 4

2. Prepare the Raspberry Pi:
   - Download Raspi-IoT-DA.img.zip image
   - Flash the image into the SD cart
   - Plug the SD card in the Raspberry Pi 4
   - Log in
   - By default the Raspi creates a WiFi Access Point
     - SSID/Password : `MasterIoT/MasterIoT`
   - Connect to the AP and check internet access

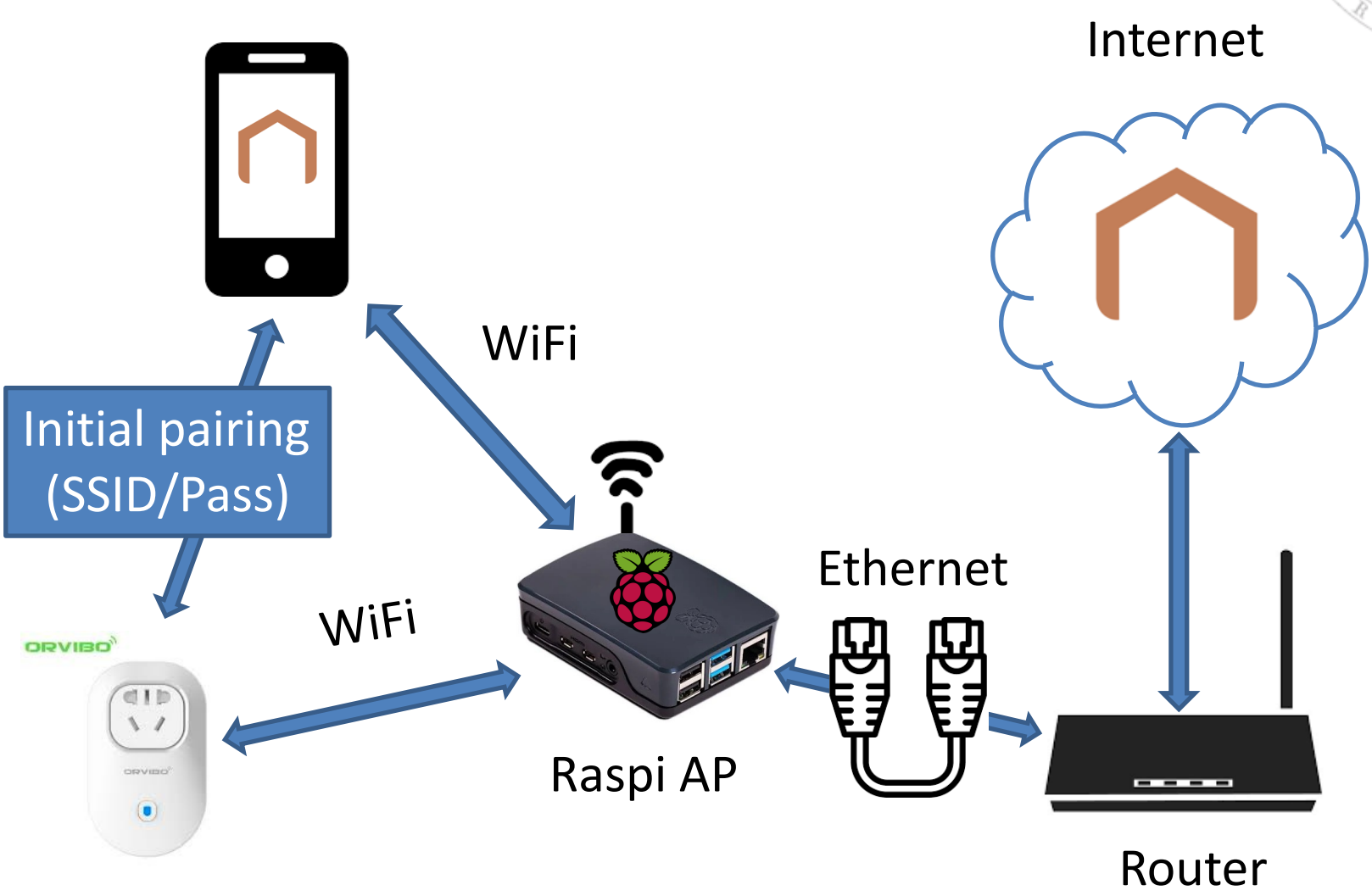
Access Point Setup



Initial Setup: Smart Socket

3. Pair the Smart Socket
   - Download the android App (HomeMate.apk)
   - Install it in your Android device
     - If you do not have and Android device contact me
   - Register into the App by creating a new user

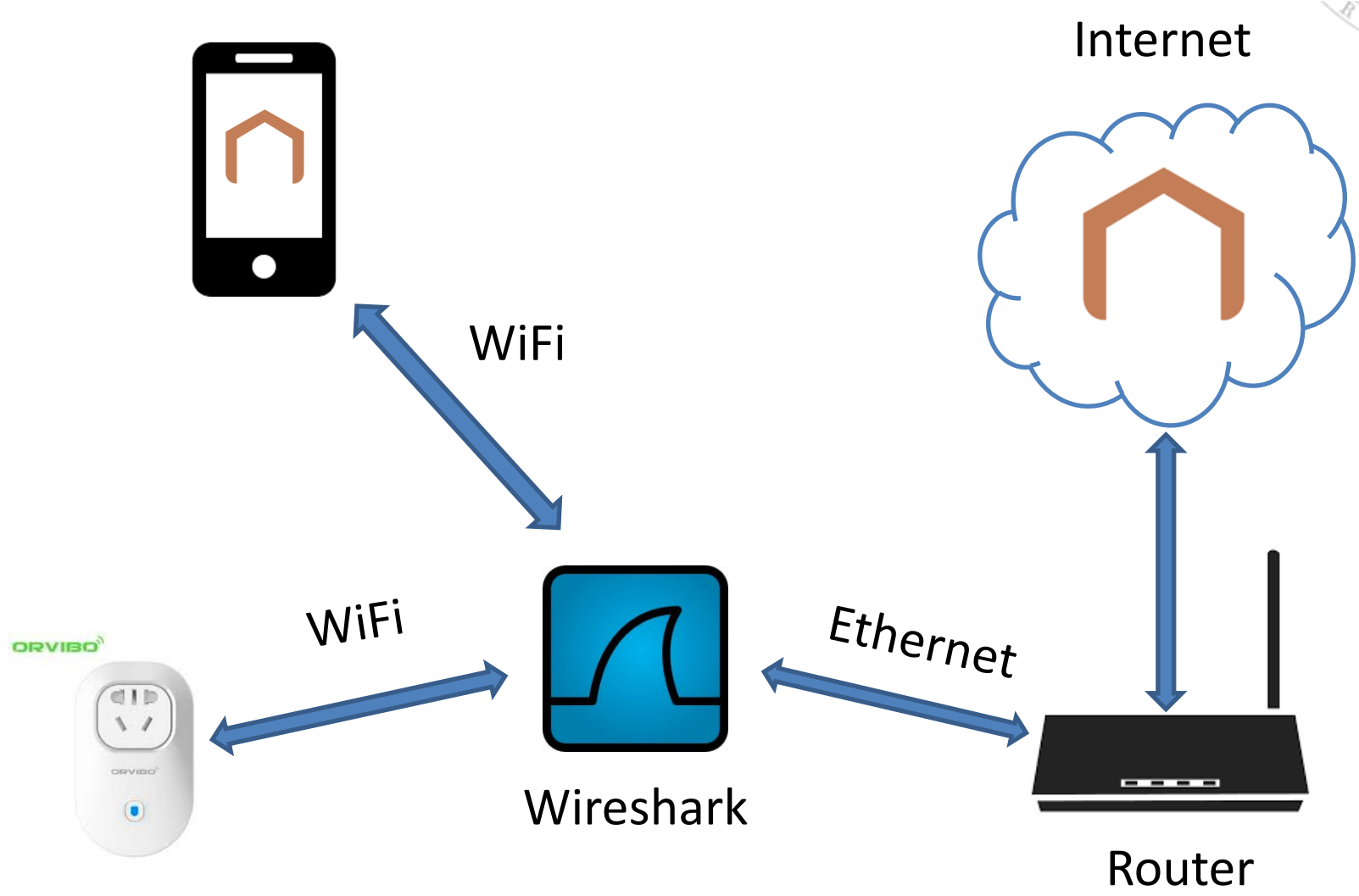
Study communications with Orvibo



Smart Socket Initial Setup

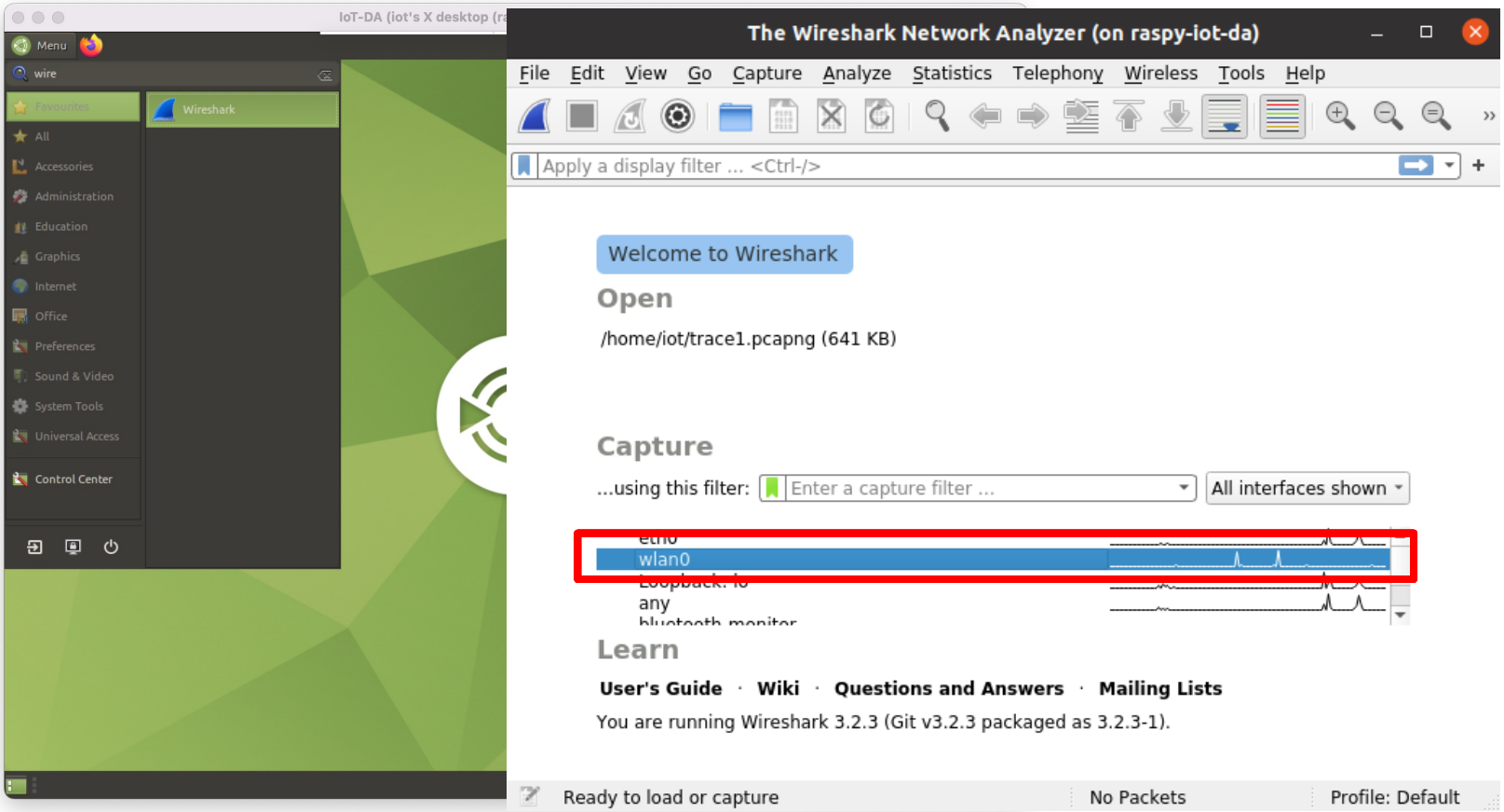
1. Initial Setup
   - Linux Virtual Machine
   - Raspberry Pi
   - Pair the Smart Socket
2. Capture Traffic
3. Traffic analysis

Study communications:



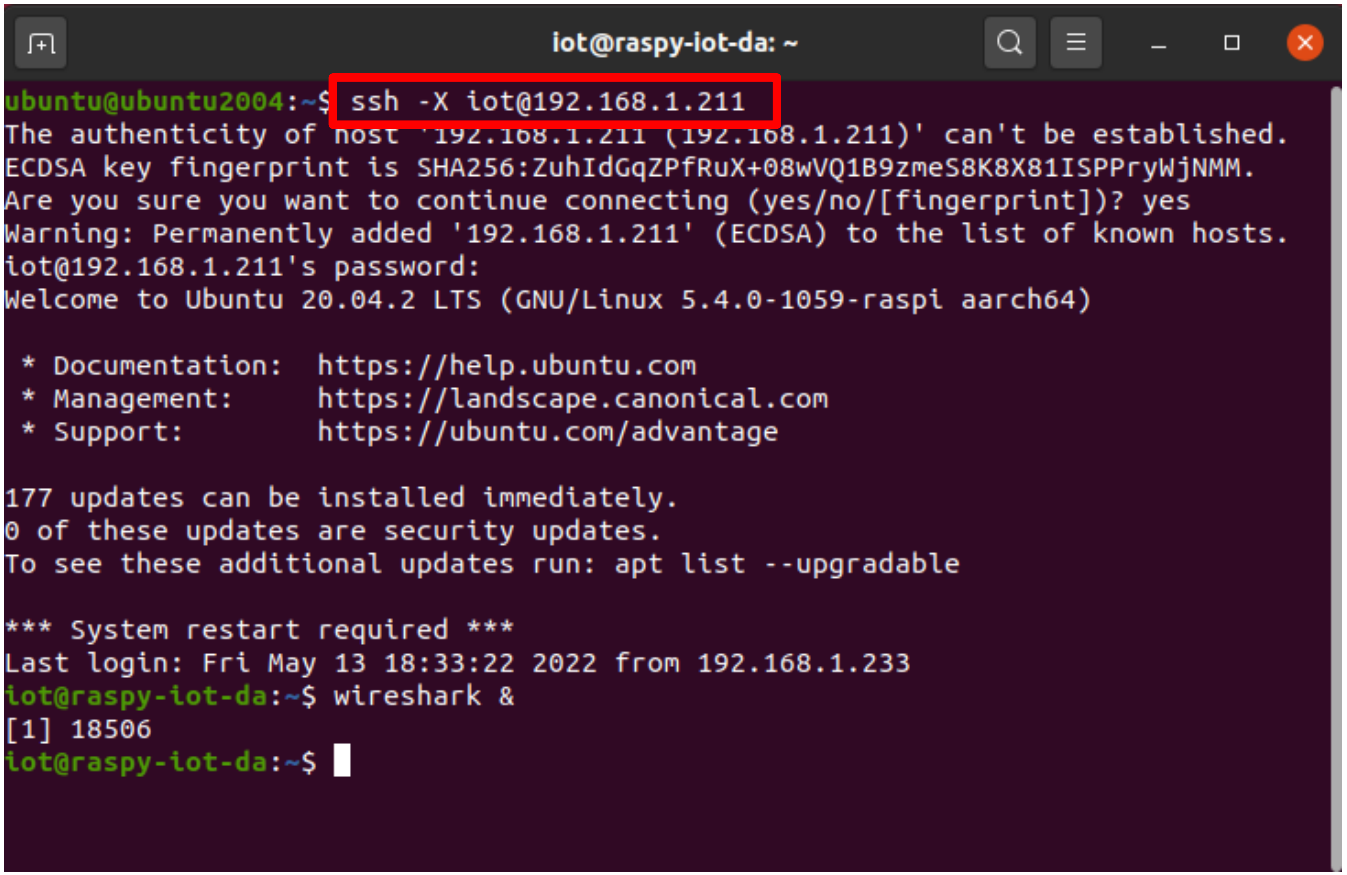
Open Raspi Wireshark

- Option 1: Use a keyboard, mouse and HDMI monitor



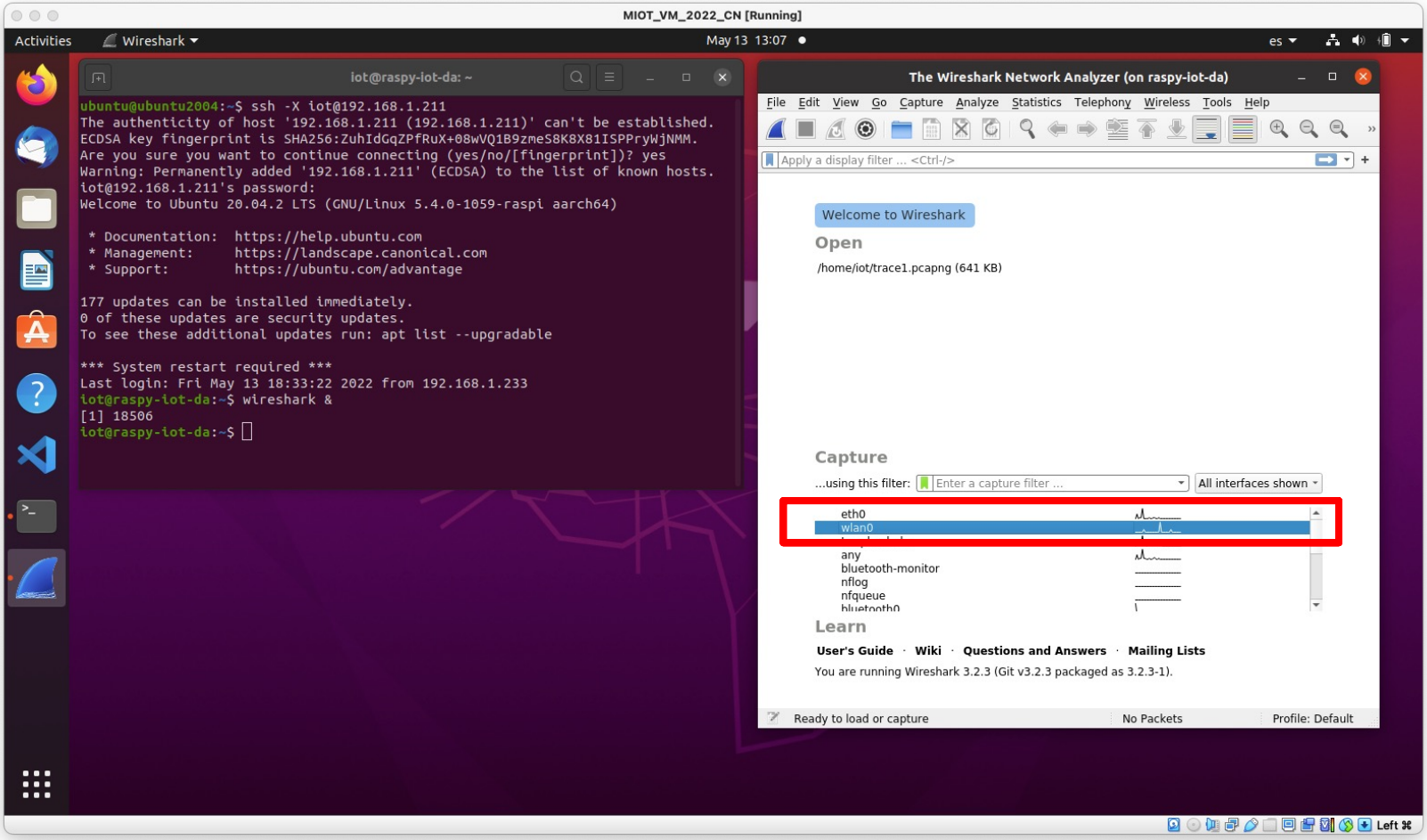
Open Raspi Wireshark

- Option 2: Use the Virtual Machine (`ssh -X`)



Open Raspi Wireshark

- Use the Virtual Machine



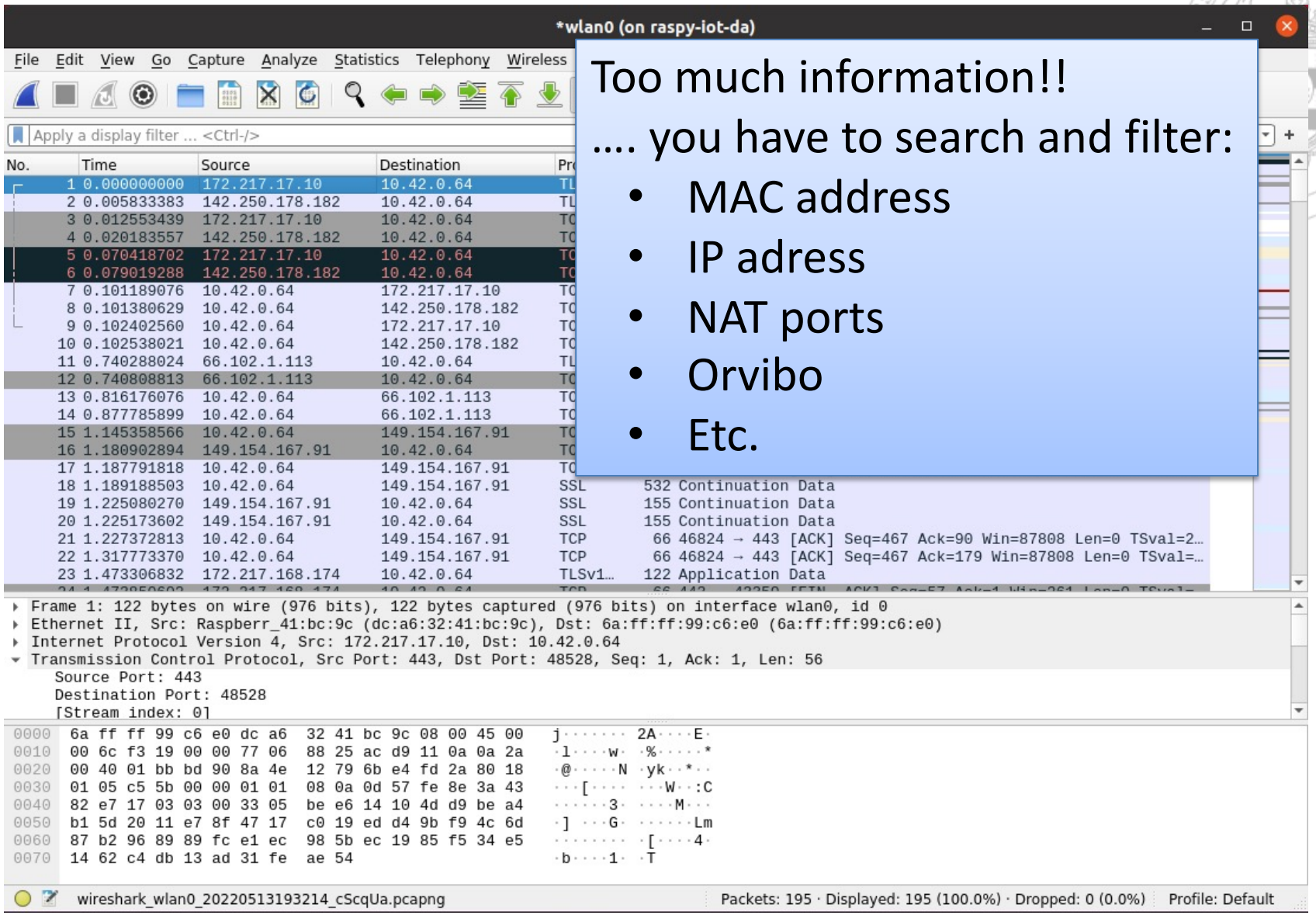
Capture traffic

1. Unplug the socket (if plugged)
2. Open Orvibo Home App
3. Start capturing traffic on `wlan0`
4. Wait 10 seconds
5. Turn on and off the socket until it responds
6. Stop traffic capture

Let's do it!!!

Smart Socket Initial Setup

1. Initial Setup
   - Linux Virtual Machine
   - Raspberry Pi
   - Pair the Smart Socket
2. Capture Traffic
3. Traffic analysis



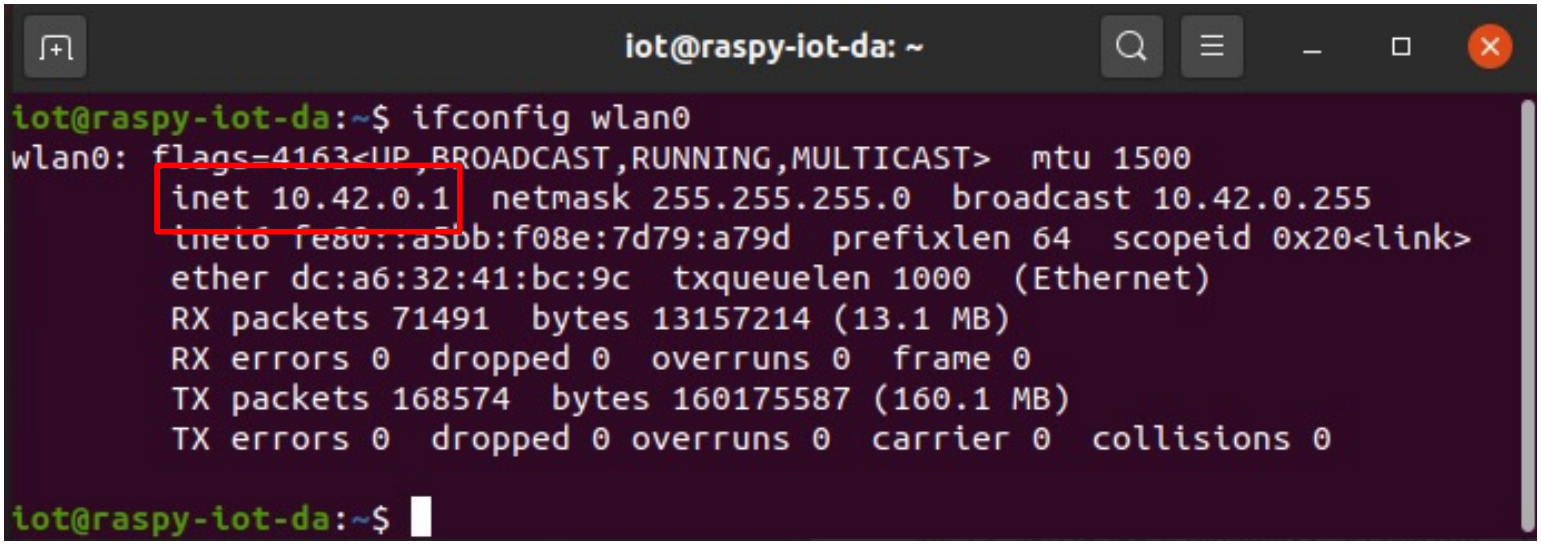
Too much information!!

…. you have to search and filter:

- MAC address
- IP adress
- NAT ports
- Orvibo
- Etc.

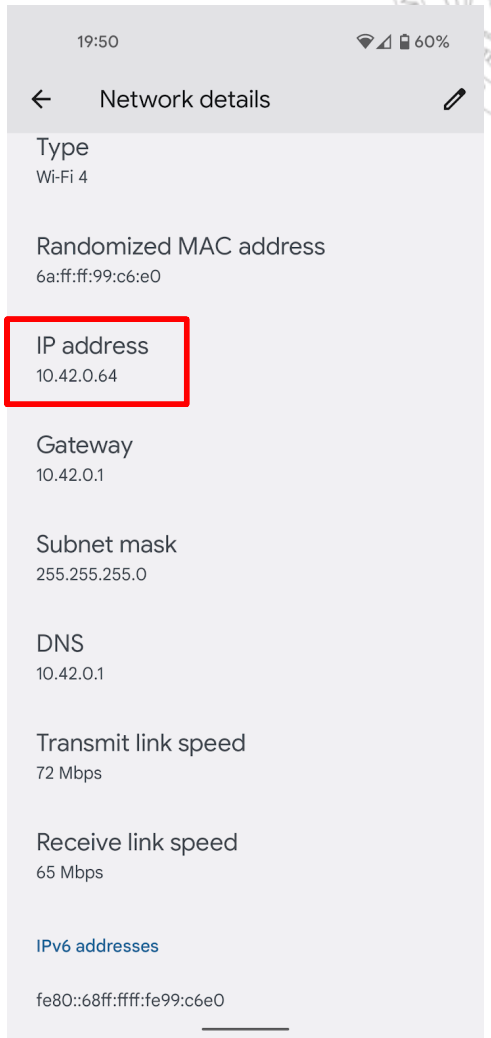
Network

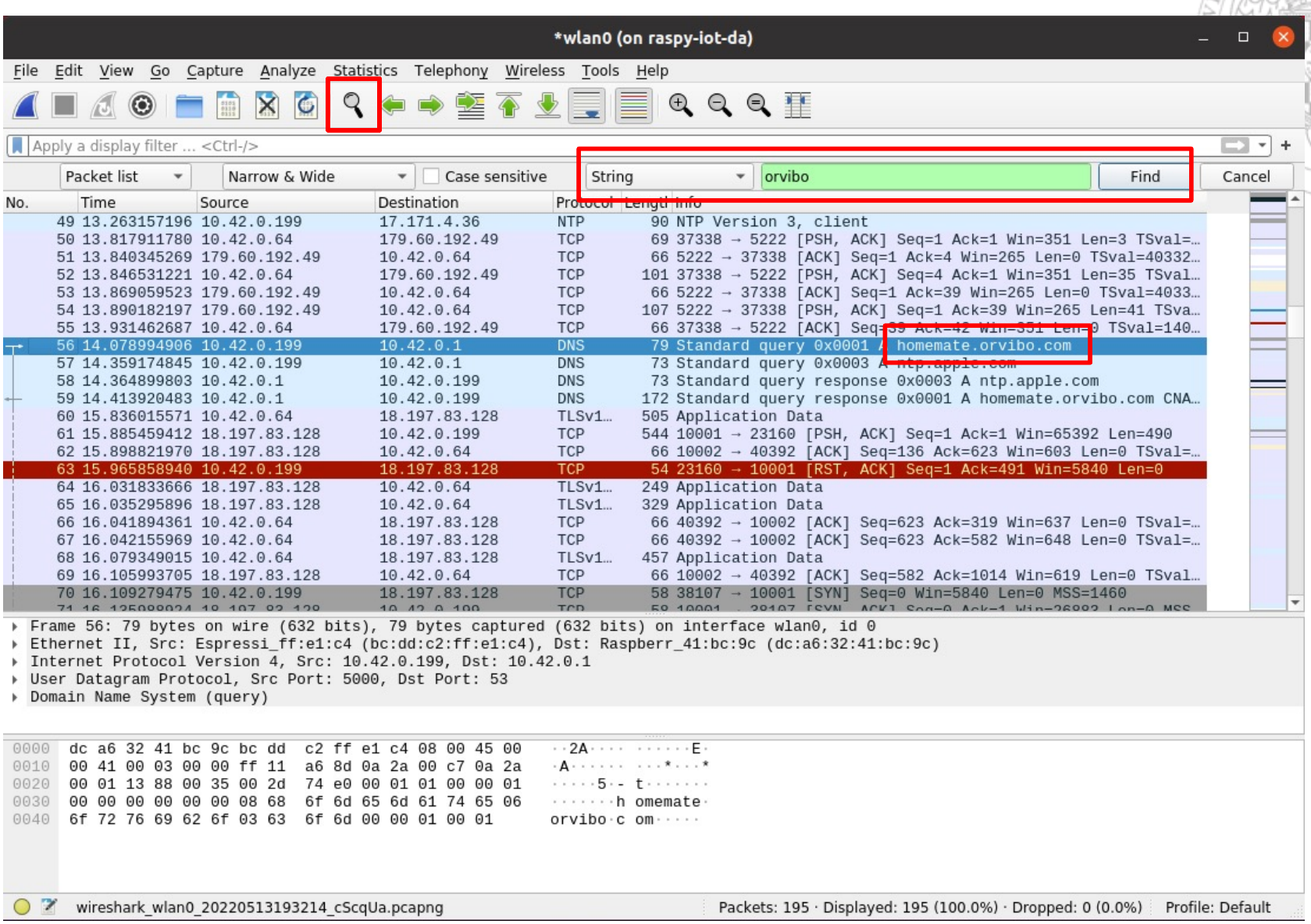
- Raspberry Pi AP network:
  - Router: 10.42.0.1



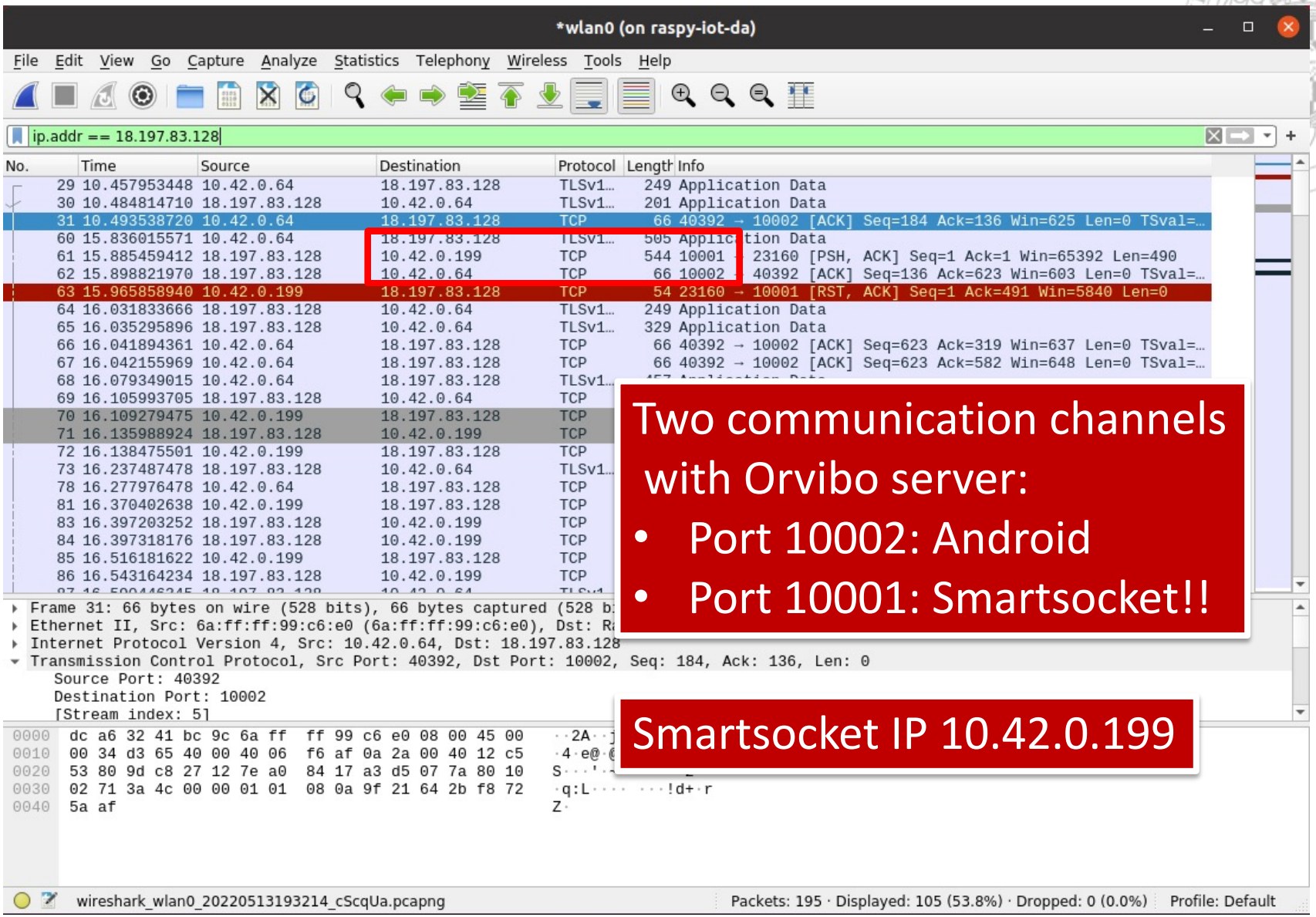
Network

- Raspberry Pi AP network:
  - Router: 10.42.0.1
  - Android: 10.42.0.64
  - Smartsocket? 10.42.0.X




*wlan0 (on raspy-iot-da)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Packet list
Narrow & Wide
Case sensitive
String
orvibo
Find
Cancel
No. Time Source Destination Protocol Length Info
49 13.263157196 10.42.0.199 17.171.4.36 NTP 90 NTP Version 3, client
50 13.817911780 10.42.0.64 179.60.192.49 TCP 69 37338 → 5222 [PSH, ACK] Seq=1 Ack=1 Win=351 Len=3 TSval=…
51 13.840345269 179.60.192.49 10.42.0.64 TCP 66 5222 → 37338 [ACK] Seq=1 Ack=4 Win=265 Len=0 TSval=40332…
52 13.846531221 10.42.0.64 179.60.192.49 TCP 101 37338 → 5222 [PSH, ACK] Seq=4 Ack=1 Win=351 Len=35 TSval…
53 13.869059523 179.60.192.49 10.42.0.64 TCP 66 5222 → 37338 [ACK] Seq=1 Ack=39 Win=265 Len=0 TSval=4033…
54 13.890182197 179.60.192.49 10.42.0.64 TCP 107 5222 → 37338 [PSH, ACK] Seq=1 Ack=39 Win=265 Len=41 TSva…
55 13.931462687 10.42.0.64 179.60.192.49 TCP 66 37338 → 5222 [ACK] Seq=39 Ack=42 Win=351 Len=0 TSval=140…
56 14.078994906 10.42.0.199 10.42.0.1 DNS 79 Standard query 0x0001 A homemate.orvibo.com
57 14.359174845 10.42.0.199 10.42.0.1 DNS 73 Standard query 0x0003 A ntp.apple.com
58 14.364899803 10.42.0.1 10.42.0.199 DNS 73 Standard query response 0x0003 A ntp.apple.com
59 14.413920483 10.42.0.1 10.42.0.199 DNS 172 Standard query response 0x0001 A homemate.orvibo.com CNA…
60 15.836015571 10.42.0.64 18.197.83.128 TLSv1… 505 Application Data
61 15.885459412 18.197.83.128 10.42.0.199 TCP 544 10001 → 23160 [PSH, ACK] Seq=1 Ack=1 Win=65392 Len=490
62 15.898821970 18.197.83.128 10.42.0.64 TCP 66 10002 → 40392 [ACK] Seq=136 Ack=623 Win=603 Len=0 TSval=…
63 15.965858940 10.42.0.199 18.197.83.128 TCP 54 23160 → 10001 [RST, ACK] Seq=1 Ack=491 Win=5840 Len=0
64 16.031833666 18.197.83.128 10.42.0.64 TLSv1… 249 Application Data
65 16.035295896 18.197.83.128 10.42.0.64 TLSv1… 329 Application Data
66 16.041894361 10.42.0.64 18.197.83.128 TCP 66 40392 → 10002 [ACK] Seq=623 Ack=319 Win=637 Len=0 TSval=…
67 16.042155969 10.42.0.64 18.197.83.128 TCP 66 40392 → 10002 [ACK] Seq=623 Ack=582 Win=648 Len=0 TSval=…
68 16.079349015 10.42.0.64 18.197.83.128 TLSv1… 457 Application Data
69 16.105993705 18.197.83.128 10.42.0.64 TCP 66 10002 → 40392 [ACK] Seq=582 Ack=1014 Win=619 Len=0 TSval…
70 16.109279475 10.42.0.199 18.197.83.128 TCP 58 38107 → 10001 [SYN] Seq=0 Win=5840 Len=0 MSS=1460
Frame 56: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface wlan0, id 0
Ethernet II, Src: Espressi_ff:e1:c4 (bc:dd:c2:ff:e1:c4), Dst: Raspberr_41:bc:9c (dc:a6:32:41:bc:9c)
Internet Protocol Version 4, Src: 10.42.0.199, Dst: 10.42.0.1
User Datagram Protocol, Src Port: 5000, Dst Port: 53
Domain Name System (query)
0000 dc a6 32 41 bc 9c bc dd c2 ff e1 c4 08 00 45 00
0010 00 41 00 03 00 00 ff 11 a6 8d 0a 2a 00 c7 0a 2a
0020 00 01 13 88 00 35 00 2d 74 e0 00 01 01 00 00 01
0030 00 00 00 00 00 00 08 68 6f 6d 65 6d 61 74 65 06
0040 6f 72 76 69 62 6f 03 63 6f 6d 00 00 01 00 01
wireshark_wlan0_20220513193214_cScqUa.pcapng
Packets: 195 · Displayed: 195 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

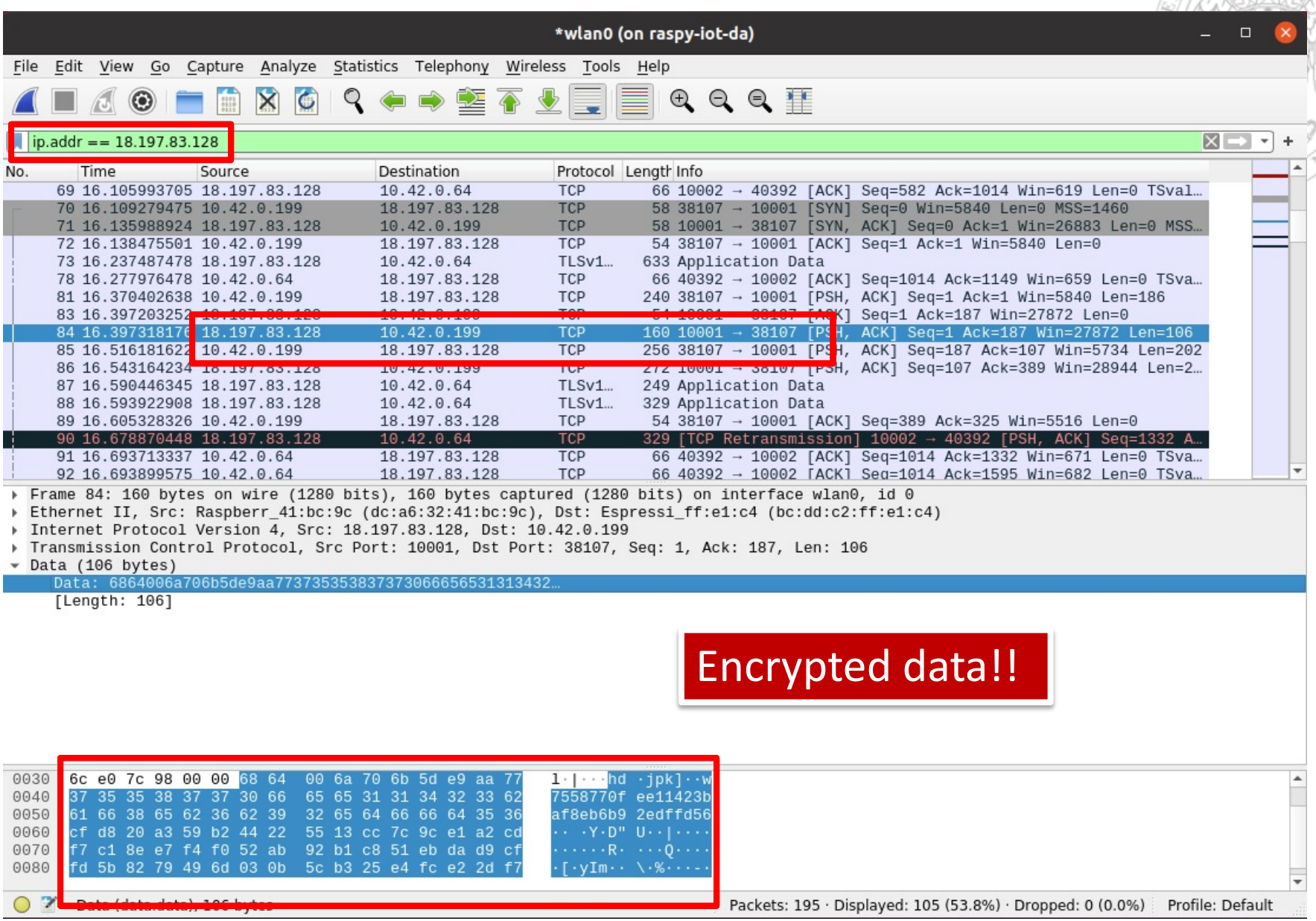
Orvibo server IP



Two communication channels with Orvibo server:

- Port 10002: Android
- Port 10001: Smartsocket!!

Smartsocket IP 10.42.0.199



Encrypted data!!

Tasks

- Obtain IP numbers:
  - Orvibo server
  - Raspberry Pi
  - Smartphone
  - Smartsocket
- Create a filter that shows the messages with data between Orvibo and the Smartsocket

Next step

- Can we decrypt the messages?
  - We need method and encryption key
- Where can we find the key?
  - Inside the device
  - On the Orvibo server
  - **In the HomeMate App**