



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](#)

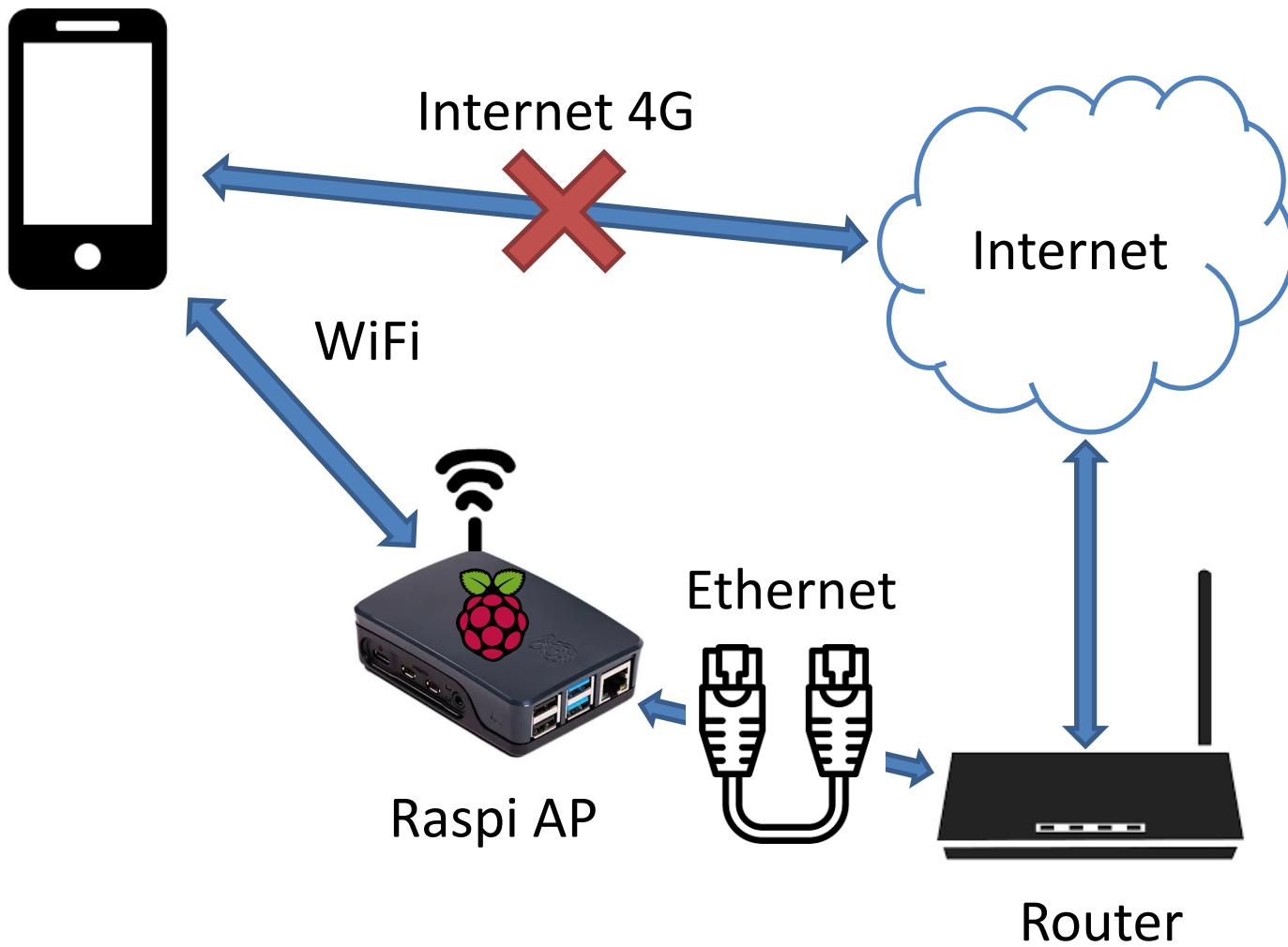
Initial Setup: raspberry Pi 4

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



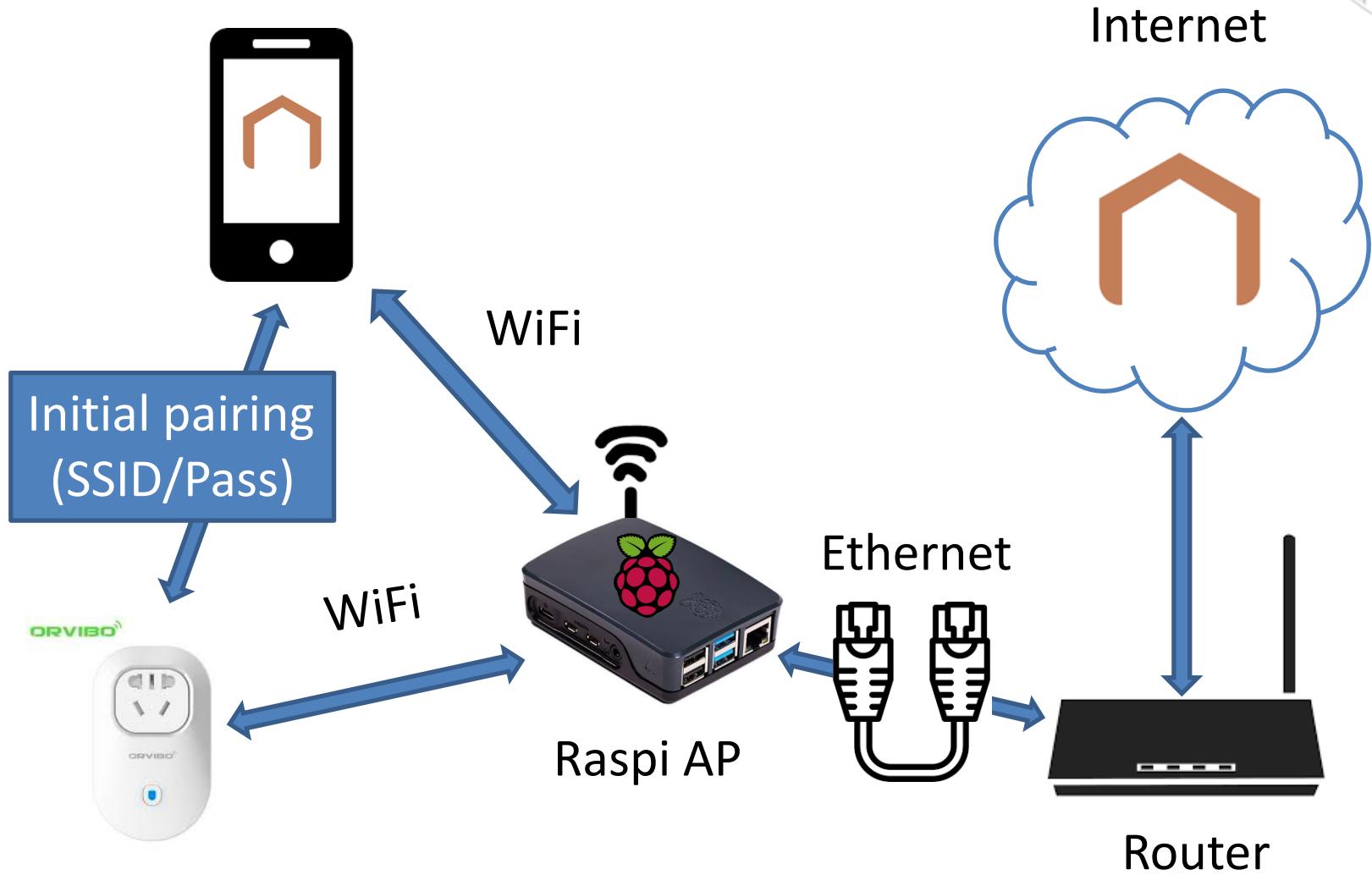
Initial Setup: Smart Socket

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

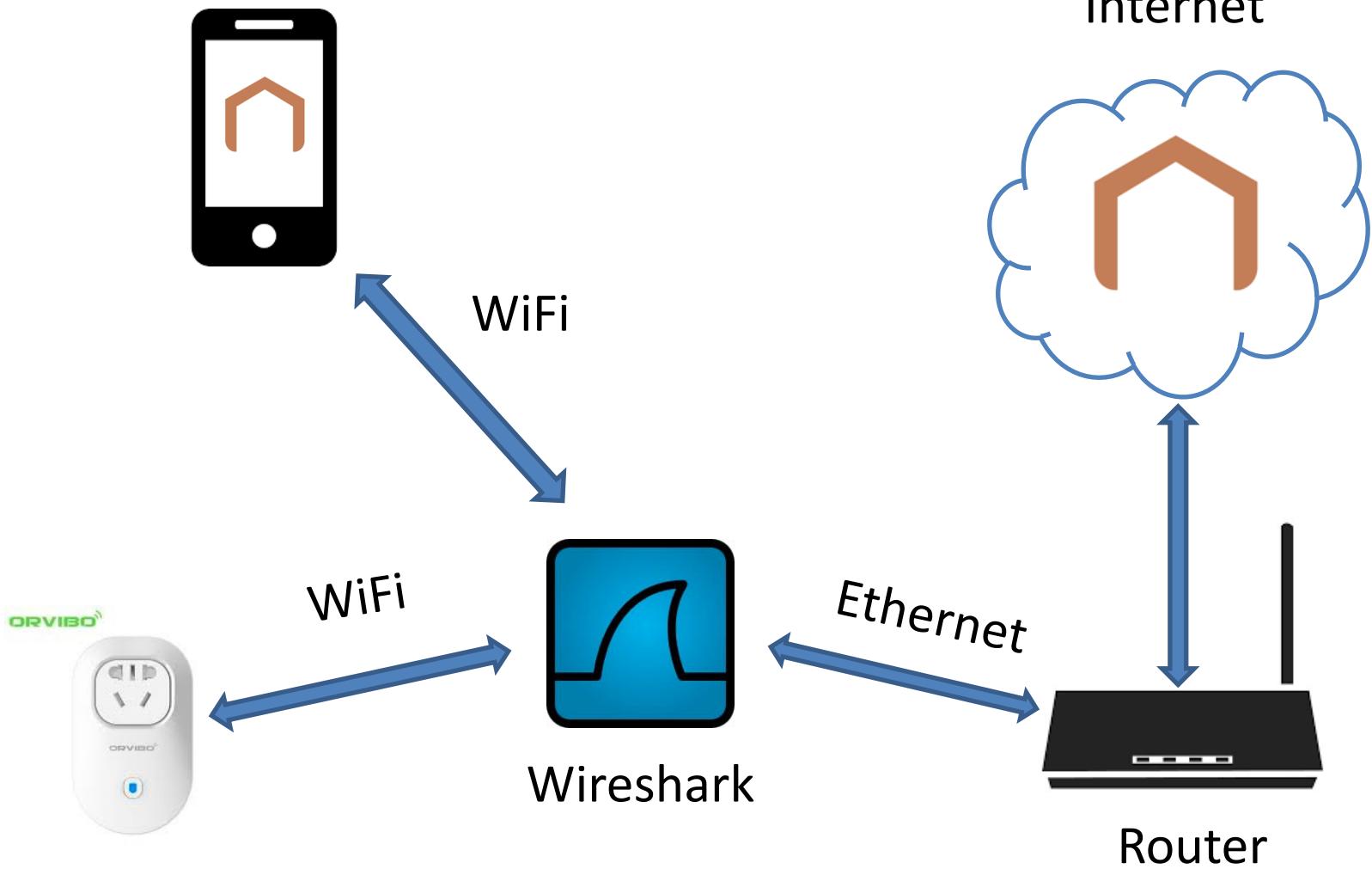
1. Initial Setup

- Linux Virtual Machine
- Raspberry Pi
- Pair the Smart Socket

2. Capture Traffic

3. Traffic analysis

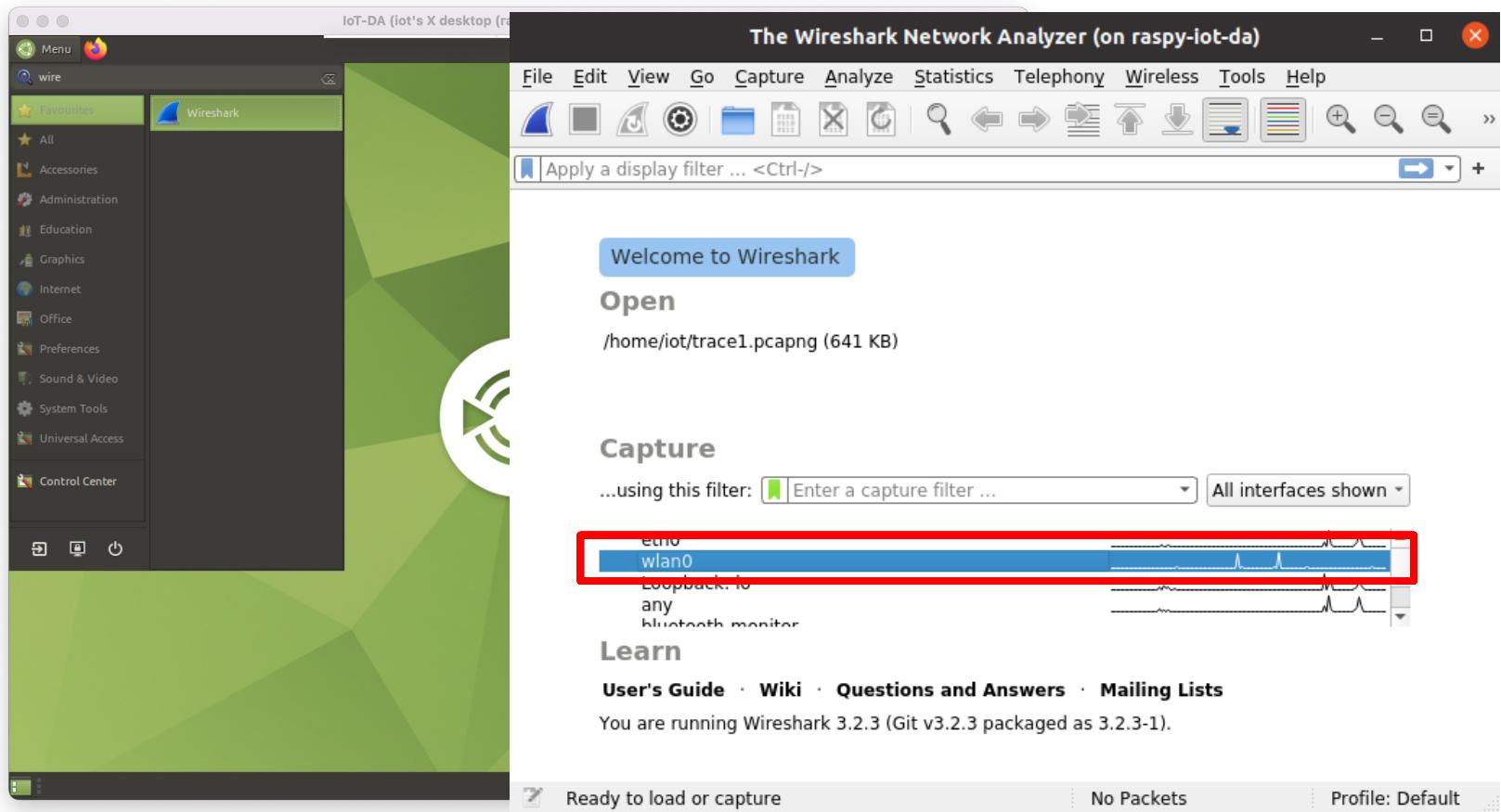
Study communications:



Open Raspi Wireshark



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





Open Raspi Wireshark

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

```
ubuntu@ubuntu2004:~$ ssh -X iot@192.168.1.211
The authenticity of host '192.168.1.211 (192.168.1.211)' can't be established.
ECDSA key fingerprint is SHA256:ZuhIdGqZPfRuX+08wVQ1B9zmeS8K8X81ISPPryWjNMM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.211' (ECDSA) to the list of known hosts.
iot@192.168.1.211's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-1059-raspi aarch64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

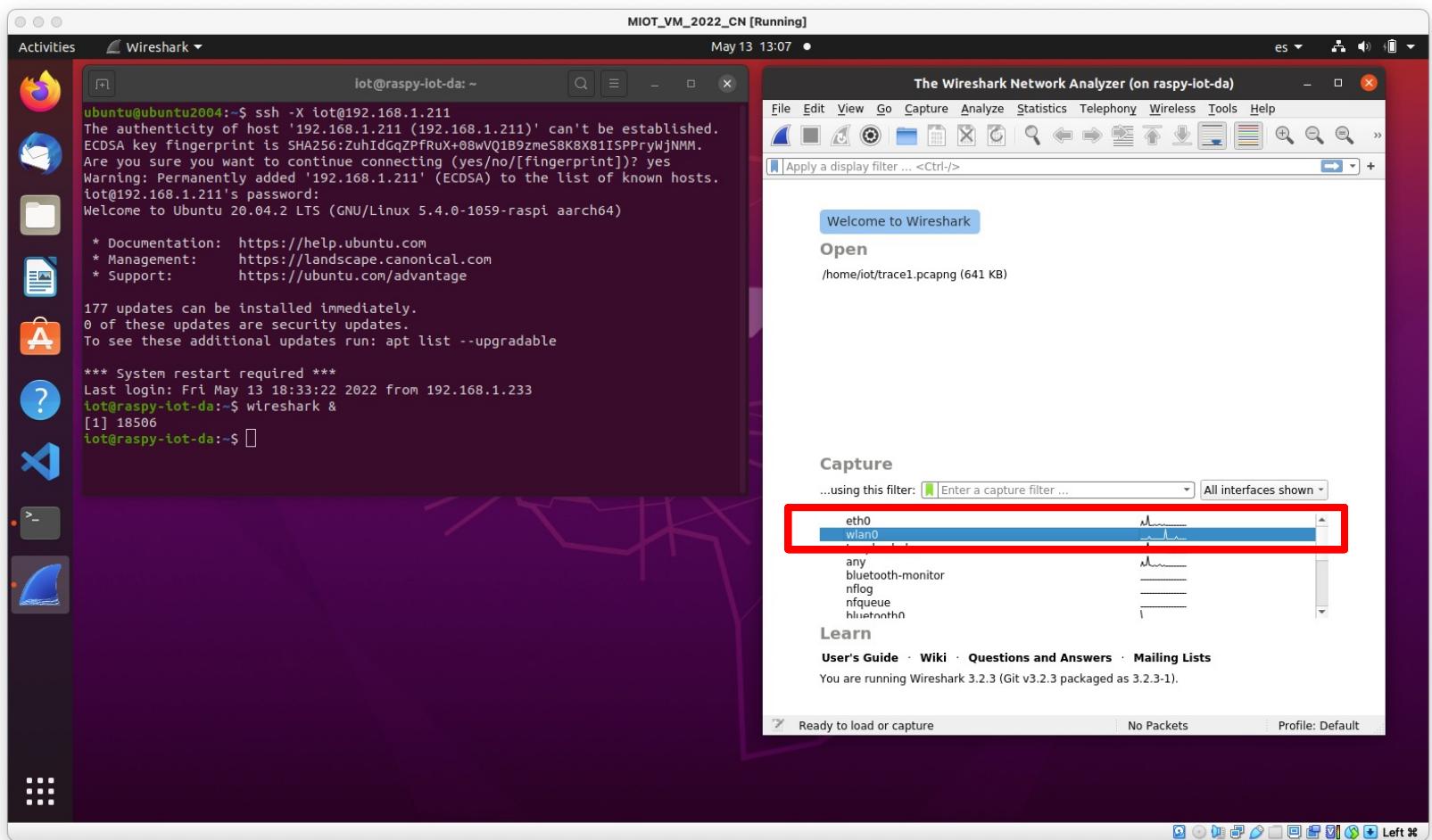
177 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

*** System restart required ***
Last login: Fri May 13 18:33:22 2022 from 192.168.1.233
iot@raspy-iot-da:~$ wireshark &
[1] 18506
iot@raspy-iot-da:~$
```



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

*wlan0 (on raspb-iot-da)

File Edit View Go Capture Analyze Statistics Telephony Wireless

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol
1	0.000000000	172.217.17.10	10.42.0.64	TCP
2	0.005833383	142.250.178.182	10.42.0.64	TCP
3	0.012553439	172.217.17.10	10.42.0.64	TCP
4	0.020183557	142.250.178.182	10.42.0.64	TCP
5	0.070418702	172.217.17.10	10.42.0.64	TCP
6	0.079019288	142.250.178.182	10.42.0.64	TCP
7	0.101189076	10.42.0.64	172.217.17.10	TCP
8	0.101380629	10.42.0.64	142.250.178.182	TCP
9	0.102402560	10.42.0.64	172.217.17.10	TCP
10	0.102538021	10.42.0.64	142.250.178.182	TCP
11	0.740288024	66.102.1.113	10.42.0.64	TCP
12	0.740808813	66.102.1.113	10.42.0.64	TCP
13	0.816176076	10.42.0.64	66.102.1.113	TCP
14	0.877785899	10.42.0.64	66.102.1.113	TCP
15	1.145358566	10.42.0.64	149.154.167.91	TCP
16	1.180902894	149.154.167.91	10.42.0.64	TCP
17	1.187791818	10.42.0.64	149.154.167.91	TCP
18	1.189188503	10.42.0.64	149.154.167.91	SSL
19	1.225080270	149.154.167.91	10.42.0.64	SSL
20	1.225173602	149.154.167.91	10.42.0.64	SSL
21	1.227372813	10.42.0.64	149.154.167.91	TCP
22	1.317773370	10.42.0.64	149.154.167.91	TCP
23	1.473306832	172.217.168.174	10.42.0.64	TLSv1...
24	1.473306832	172.217.168.174	10.42.0.64	TCP

Frame 1: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface wlan0, id 0
 Ethernet II, Src: Raspberry_41:bc:9c (dc:a6:32:41:bc:9c), Dst: 6a:ff:ff:99:c6:e0 (6a:ff:ff:99:c6:e0)
 Internet Protocol Version 4, Src: 172.217.17.10, Dst: 10.42.0.64
 Transmission Control Protocol, Src Port: 443, Dst Port: 48528, Seq: 1, Ack: 1, Len: 56
 Source Port: 443
 Destination Port: 48528
 Stream index: 01

Hex	Dec	Text
0000	6a ff ff 99 c6 e0 dc a6	j..... 2A....E
0010	00 6c f3 19 00 00 77 06	l..... W....%....*
0020	00 40 01 bb bd 90 8a 4e	@..... N yk....*
0030	01 05 c5 5b 00 00 01 01	[..... W....:C
0040	82 e7 17 03 03 00 33 053....M....
0050	b1 5d 20 11 e7 8f 47 17]....G....Lm
0060	87 b2 96 89 89 fc e1 ec[....4....
0070	14 62 c4 db 13 ad 31 fe	b....1....T

wireshark_wlan0_20220513193214_cScqUa.pcapng

Packets: 195 · Displayed: 195 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

Too much information!!
 you have to search and filter:

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



Network

- Raspberry Pi AP network:
 - Router: 10.42.0.1

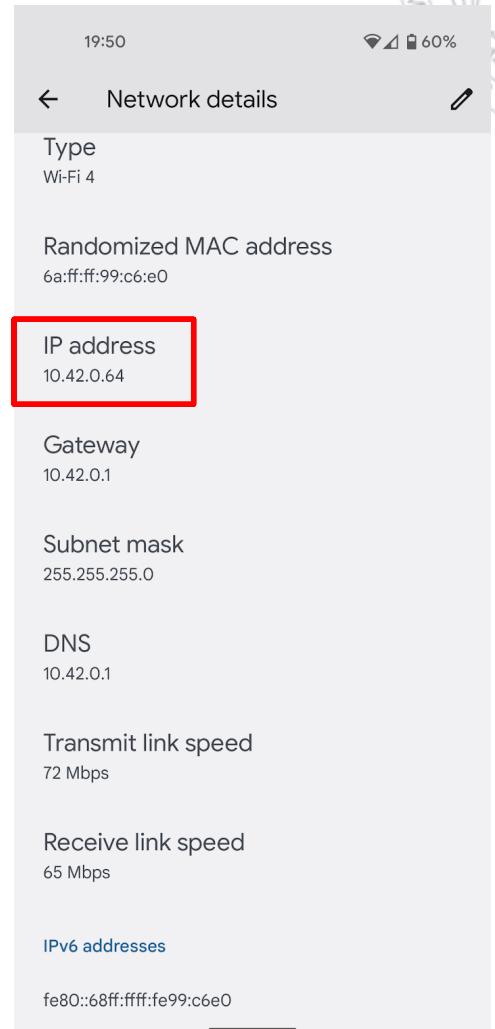
```
iot@raspy-iot-da:~$ ifconfig wlan0
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.42.0.1 netmask 255.255.255.0 broadcast 10.42.0.255
        ether dc:a6:32:41:bc:9c txqueuelen 1000 (Ethernet)
        RX packets 71491 bytes 13157214 (13.1 MB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 168574 bytes 160175587 (160.1 MB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

iot@raspy-iot-da:~$
```

Network



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



Module 7: Smart Socket Pentest

Wireshark Screenshot showing network traffic on interface wlan0 (on raspb-iot-da). A search filter for "orvibo" has been applied.

The search results highlight a DNS query from 10.42.0.199 to 10.42.0.1 for the domain homemate.orvibo.com.

Packet details:

- Frame 56: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface wlan0, id 0
- Ethernet II, Src: Espressi_ff:ff:e1:c4 (bc:dd:c2:ff:e1:c4), Dst: Raspberry_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)

Hex dump of the DNS query:

0000 dc a6 32 41 bc 9c bc dd c2 ff e1 c4 08 00 45 00	.2A.....E.
0010 00 41 00 03 00 00 ff 11 a6 8d 0a 2a 00 c7 0a 2a	.A.....*.**
0020 00 01 13 88 00 35 00 2d 74 e0 00 01 01 00 00 015..t.....
0030 00 00 00 00 00 08 68 6f 6d 65 6d 61 74 65 06h omemate.
0040 6f 72 76 69 62 6f 03 63 6f 6d 00 00 01 00 01	orvibo.c om.....



Orvibo server IP

```
user-iot@VM-IOT: ~
user-iot@VM-IOT:~$ dig homemate.orvibo.com

; <>> DiG 9.10.3-P4-Ubuntu <>> homemate.orvibo.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21097
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;homemate.orvibo.com.           IN      A

;; ANSWER SECTION:
homemate.orvibo.com.    60      IN      CNAME    access-web-prd-de2-80189dd559508282.elb.eu-cen
tral-1.amazonaws.com.
access-web-prd-de2-80189dd559508282.elb.eu-central-1.amazonaws.com. 60 IN A 18.197.83.128

;; Query time: 57 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Feb 04 12:50:09 CET 2020
;; MSG SIZE  rcvd: 141

user-iot@VM-IOT:~$
```

*wlan0 (on raspb-iot-da)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 18.197.83.128

No.	Time	Source	Destination	Protocol	Length	Info
29	10.457953448	10.42.0.64	18.197.83.128	TLSv1...	249	Application Data
30	10.484814710	18.197.83.128	10.42.0.64	TLSv1...	201	Application Data
31	10.493538720	10.42.0.64	18.197.83.128	TCP	66	40392 → 10002 [ACK] Seq=184 Ack=136 Win=625 Len=0 TSval=...
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...	157	Application Data
69	16.105993705	18.197.83.128	10.42.0.64	TCP	66	10002 → 40392 [ACK] Seq=136 Ack=623 Win=603 Len=0 TSval=...
70	16.109279475	10.42.0.199	18.197.83.128	TCP	66	10001 → 23160 [RST, ACK] Seq=1 Ack=491 Win=5840 Len=0
71	16.135988924	18.197.83.128	10.42.0.199	TCP	66	23160 → 10001 [ACK] Seq=1 Ack=491 Win=5840 Len=0
72	16.138475501	10.42.0.199	18.197.83.128	TCP	66	10001 → 23160 [RST, ACK] Seq=1 Ack=491 Win=5840 Len=0
73	16.237487478	18.197.83.128	10.42.0.64	TLSv1...	249	Application Data
78	16.277976478	10.42.0.64	18.197.83.128	TCP	66	10002 → 40392 [ACK] Seq=136 Ack=623 Win=603 Len=0 TSval=...
81	16.370402638	10.42.0.199	18.197.83.128	TCP	66	40392 → 10002 [ACK] Seq=623 Ack=319 Win=637 Len=0 TSval=...
83	16.397203252	18.197.83.128	10.42.0.199	TCP	66	40392 → 10002 [ACK] Seq=623 Ack=582 Win=648 Len=0 TSval=...
84	16.397318176	18.197.83.128	10.42.0.199	TCP	66	40392 → 10002 [ACK] Seq=623 Ack=582 Win=648 Len=0 TSval=...
85	16.516181622	10.42.0.199	18.197.83.128	TCP	66	40392 → 10002 [ACK] Seq=623 Ack=582 Win=648 Len=0 TSval=...
86	16.543164234	18.197.83.128	10.42.0.199	TCP	66	40392 → 10002 [ACK] Seq=623 Ack=582 Win=648 Len=0 TSval=...
87	16.500462446	10.42.0.64	10.42.0.64	TLSv1...	249	Application Data

```

Frame 31: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: 6a:ff:ff:99:c6:e0 (6a:ff:ff:99:c6:e0), Dst: Raspbian (08:00:27:12:7e:a0)
Internet Protocol Version 4, Src: 10.42.0.64, Dst: 18.197.83.128
Transmission Control Protocol, Src Port: 40392, Dst Port: 10002, Seq: 184, Ack: 136, Len: 0
  Source Port: 40392
  Destination Port: 10002
  Stream index: 51

```

```

0000 dc a6 32 41 bc 9c 6a ff ff 99 c6 e0 08 00 45 00 .2A..j
0010 00 34 d3 65 40 00 40 06 f6 af 0a 2a 00 40 12 c5 .4.e@.C
0020 53 80 9d c8 27 12 7e a0 84 17 a3 d5 07 7a 80 10 S...!.
0030 02 71 3a 4c 00 00 01 01 08 0a 9f 21 64 2b f8 72 .q:L....!d+r
0040 5a af Z.

```

Packets: 195 · Displayed: 105 (53.8%) · Dropped: 0 (0.0%) · Profile: Default

Two communication channels with Orvibo server:

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

Smartsocket IP 10.42.0.199



*wlan0 (on raspb-iot-da)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 18.197.83.128

No.	Time	Source	Destination	Protocol	Length	Info
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
71	16.135988924	18.197.83.128	10.42.0.199	TCP	58	10001 → 38107 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS...
72	16.138475501	10.42.0.199	18.197.83.128	TCP	54	38107 → 10001 [ACK] Seq=1 Ack=1 Win=5840 Len=0
73	16.237487478	18.197.83.128	10.42.0.64	TLSv1...	633	Application Data
78	16.277976478	10.42.0.64	18.197.83.128	TCP	66	40392 → 10002 [ACK] Seq=1014 Ack=1149 Win=659 Len=0 TSval...
81	16.370402638	10.42.0.199	18.197.83.128	TCP	240	38107 → 10001 [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=186
83	16.397203252	18.197.83.128	10.42.0.199	TCP	54	10001 → 38107 [ACK] Seq=1 Ack=187 Win=27872 Len=0
84	16.397318176	18.197.83.128	10.42.0.199	TCP	160	10001 → 38107 [PSH, ACK] Seq=1 Ack=187 Win=27872 Len=106
85	16.516181622	10.42.0.199	18.197.83.128	TCP	256	38107 → 10001 [PSH, ACK] Seq=187 Ack=107 Win=5734 Len=202
86	16.543164234	18.197.83.128	10.42.0.199	TCP	272	10001 → 38107 [PSH, ACK] Seq=107 Ack=389 Win=28944 Len=2...
87	16.5900446345	18.197.83.128	10.42.0.64	TLSv1...	249	Application Data
88	16.593922908	18.197.83.128	10.42.0.64	TLSv1...	329	Application Data
89	16.605328326	10.42.0.199	18.197.83.128	TCP	54	38107 → 10001 [ACK] Seq=389 Ack=325 Win=5516 Len=0
90	16.678870448	18.197.83.128	10.42.0.64	TCP	329	[TCP Retransmission] 10002 → 40392 [PSH, ACK] Seq=1332 A...
91	16.693713337	10.42.0.64	18.197.83.128	TCP	66	40392 → 10002 [ACK] Seq=1014 Ack=1332 Win=671 Len=0 TSval...
92	16.693899575	10.42.0.64	18.197.83.128	TCP	66	40392 → 10002 [ACK] Seq=1014 Ack=1595 Win=682 Len=0 TSval...

Frame 84: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface wlan0, id 0

Ethernet II, Src: Raspberry_41:bc:9c (dc:a6:32:41:bc:9c), Dst: Espressi_ff:e1:c4 (bc:dd:c2:ff:e1:c4)

Internet Protocol Version 4, Src: 18.197.83.128, Dst: 10.42.0.199

Transmission Control Protocol, Src Port: 10001, Dst Port: 38107, Seq: 1, Ack: 187, Len: 106

Data (106 bytes)

```
0030  6c e0 7c 98 00 00 68 64  00 6a 70 6b 5d e9 aa 77  1·|...hd·jpk]·w
0040  37 35 35 38 37 37 30 66  65 65 31 31 34 32 33 62  7558770f ee11423b
0050  61 66 38 65 62 36 62 39  32 65 64 66 66 64 35 36  af8eb6b9 2edffd56
0060  cf d8 20 a3 59 b2 44 22  55 13 cc 7c 9c e1 a2 cd  ...·Y·D" U··|.....
0070  f7 c1 8e e7 f4 f0 52 ab  92 b1 c8 51 eb da d9 cf  ....R·...Q.....
0080  fd 5b 82 79 49 6d 03 0b  5c b3 25 e4 fc e2 2d f7  ·[·yIm··\.%....
```

Encrypted data!!

Data (Selected Data), 106 bytes

Packets: 195 · Displayed: 105 (53.8%) · Dropped: 0 (0.0%) · Profile: Default



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**