

# Packet sniffer install guide

## Prerequisites

### Requirements:

- A raspberry pi 3 or newer
- A power supply for your raspberry pi
- A MicroSD card of at least 8GB
- An Ethernet cables
- A MicroSD Adapter (Optional)



## Raspberry Pi basic setup

Now that you have all your hardware, we should first start with installing Raspbian on your raspberry pi. This can easily be done by downloading Raspbian (preferably the lite version) from the official raspberry pi website:

<https://www.raspberrypi.org/downloads/raspbian/>

Here you can click the download link for Raspbian Buster lite. You will also need a program to “install” the OS on your MicroSD. We used balenaEtcher. You can install this program by going to:

<https://www.balena.io/etcher/>

and downloading + installing the program. When the program is installed and the MicroSD is attached to your computer you can “burn” the OS by opening balenaEtcher. Click Select image and select the zip you just downloaded (Raspbian buster). Select the target (Your micro-SD) and click flash. Wait a couple of minutes until the program is ready.

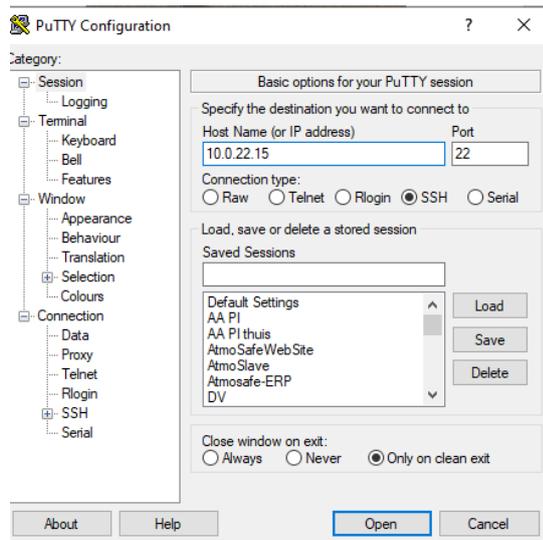
Now you will have to open your micro-SD card’s home folder. Add an empty file called SSH without an extension to enable SSH on your Raspberry Pi. Eject the SSD and insert it into your Raspberry Pi. Connect the pi to its power supply and the router.

You can find your raspberry pi’s IP by opening the terminal on your pc and running the following command:

```
Ping raspberrypi
```

Once you obtain the IP from your Pi you can access it remotely by using Putty. You can download this program here: <https://www.putty.org/>

Open Putty, enter the IP from your raspberry pi, port 22 and select SSH. A new window will open. Accept the certificates and log in with username: `pi` and password `raspberrypi`



Install RaspAP and hostapd

Open the terminal from your raspberry pi and run the following command:

```
sudo cp /etc/wpa_supplicant/wpa_supplicant.conf  
/etc/wpa_supplicant/wpa_supplicant.conf.sav
```

```
sudo cp /dev/null /etc/wpa_supplicant/wpa_supplicant.conf
```

Finally, edit in the file `/etc/wpa_supplicant/wpa_supplicant.conf` and add the following lines:

```
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev  
update_config=1
```

The Wi-Fi interface has now been made available.

Now we will install hostapd and a user-friendly interface by using RaspAP (for more info, go to <https://github.com/billz/raspap-webgui>)

The installation of RaspAP can easily be done by running a single command and following the steps shown in the terminal.

```
wget -q https://git.io/voEUQ -O /tmp/raspap && bash /tmp/raspap
```

In our case there was the need for some extra configuration before the network became available. If it is already available, you can skip the following steps:

Open the following file:

```
sudo nano /etc/hostapd/hostapd.conf
```

And add the following line:

```
logger_syslog=-1
```

Run the following command

```
sudo cat /var/log/syslog | grep hostapd
```

And:

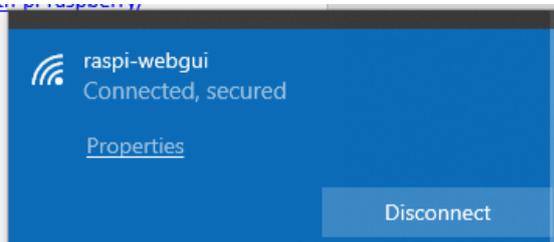
```
sudo systemctl unmask hostapd
```

```
sudo systemctl enable hostapd
```

```
sudo systemctl start hostapd
```

restart your raspberry pi with the `sudo reboot` command.

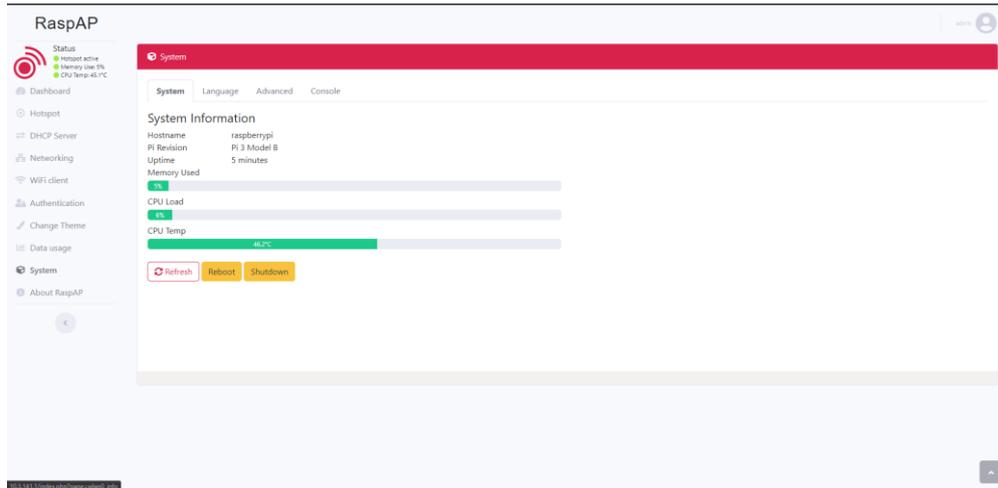
Connect to your Wi-Fi hotspot



Now a network called “raspi-webgui” should be available. When you connect to this Wi-Fi-network on your pc, you can access the interface by browsing to `10.3.141.1`. (The default Wi-Fi password is `ChangeMe` ). The default username and password for the interface are:

Username: `admin`

Password: `secret`



The console can also be accessed by browsing to your Raspberry Pi's IP-address obtained in the first step (while connected to the same router).

### Installing TCPDump

The last step to creating a packet sniffer is installing TCPDump. This tool is installed with the following command:

```
Sudo apt-get install tcpdump
```

When the installation finishes you can start to capture traffic from every device connected to the network of your raspberry pi. We recommend capturing data by specifying your host and creating a pcap file which later can be analyzed with Wireshark.

Example:

```
sudo tcpdump host 10.3.141.145 -i wlan0 -w test
```

This command captures all network packet going from and to the device 10.3.141.145 and creates a file called test.

Example pcap file:

# Sander Van Dessel & Joey Van Erum

The image shows a Wireshark network traffic capture. The main pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, Host, TCP\_FLAGS, and Info. The packets are primarily DNS queries and responses, as well as some HTTP requests. The source IP is consistently 10.3.141.145, and the destination is 239.255.255.250. The info pane at the bottom shows details for a selected packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Multiple Service Discovery Protocol.

No.	Time	Source	Destination	Protocol	Length	Host	TCP_FLAGS	Info
1	0.000000	10.3.141.145	239.255.255.250	SSDP	436	239.255.255.250:1900		NOTIFY * HTTP/1.1
2	0.121312	10.3.141.145	239.255.255.250	SSDP	424	239.255.255.250:1900		NOTIFY * HTTP/1.1
3	0.240573	10.3.141.145	239.255.255.250	SSDP	432	239.255.255.250:1900		NOTIFY * HTTP/1.1
4	0.361762	10.3.141.145	239.255.255.250	SSDP	379	239.255.255.250:1900		NOTIFY * HTTP/1.1
5	0.481981	10.3.141.145	239.255.255.250	SSDP	370	239.255.255.250:1900		NOTIFY * HTTP/1.1
6	10.875493	35.190.242.190	10.3.141.145	TCP	77			0.00000000 4876 - 68754 [PSH, ACK] Seq=1 Ack=12 Win=1 Len=1 TSval=1685895616 TSecr=568978
7	10.893164	10.3.141.145	35.190.242.190	TCP	66			0.013673000 68754 - 4876 [ACK] Seq=1 Ack=12 Win=393 Len=0 TSval=571564 TSecr=1685895616
8	14.633995	10.3.141.145	239.255.255.250	SSDP	434	239.255.255.250:1900		NOTIFY * HTTP/1.1
9	14.555587	10.3.141.145	239.255.255.250	SSDP	436	239.255.255.250:1900		NOTIFY * HTTP/1.1
10	14.673218	10.3.141.145	239.255.255.250	SSDP	424	239.255.255.250:1900		NOTIFY * HTTP/1.1
11	14.791332	10.3.141.145	239.255.255.250	SSDP	432	239.255.255.250:1900		NOTIFY * HTTP/1.1
12	14.924183	10.3.141.145	239.255.255.250	SSDP	379	239.255.255.250:1900		NOTIFY * HTTP/1.1
13	15.037448	10.3.141.145	239.255.255.250	SSDP	370	239.255.255.250:1900		NOTIFY * HTTP/1.1
14	15.868443	Raspberr_48:81:4a	Rose_4a:ad:50	ARP	42			who has 10.3.141.145? Tell 10.3.141.1
15	15.876637	Rose_4a:ad:50	Raspberr_48:81:4a	ARP	42			10.3.141.145 is at Ac:87:5d:4a:ad:50
16	16.043508	10.3.141.145	10.3.141.145	DNS	75			Standard query 84668 & 10.3.141.145
17	16.052363	10.3.141.145	10.3.141.145	DNS	162			Standard query response 84668 & 10.3.141.145
18	16.872384	10.3.141.145	10.3.141.145	TCP	74			0.00000000 59444 - 443 [SYN] Seq=0 Win=29280 Len=0 MSS=1460 SACK_PERM=1 TSval=5721218 TSecr=0 US=128
19	16.186138	10.3.141.145	10.3.141.145	DNS	75			Standard query 84668 & 10.3.141.145
20	16.186688	10.3.141.145	10.3.141.145	DNS	172			Standard query response 84668 & 10.3.141.145
21	16.218599	10.3.141.145	10.3.141.145	TCP	74			0.00000000 59444 - 443 [SYN] Seq=0 Win=29280 Len=0 MSS=1460 SACK_PERM=1 TSval=5721218 TSecr=0 US=128
22	16.252297	10.3.141.145	10.3.141.145	DNS	75			Standard query 84668 & 10.3.141.145
23	16.252853	10.3.141.145	10.3.141.145	DNS	172			Standard query response 84668 & 10.3.141.145
24	16.260345	10.3.141.145	10.3.141.145	TCP	74			0.00000000 59444 - 443 [SYN] Seq=0 Win=29280 Len=0 MSS=1460 SACK_PERM=1 TSval=5721218 TSecr=0 US=128
25	16.271374	34.237.118.27	10.3.141.145	TCP	74			0.00000000 443 - 59444 [SYN, ACK] Seq=0 Ack=1 Win=2912 Len=0 MSS=1460 TSval=324651939 TSecr=5721218 US=256
26	16.278213	10.3.141.145	34.237.118.27	TCP	66			0.004390000 59444 - 443 [ACK] Seq=1 Win=29312 Len=0 TSval=5721217 TSecr=324651939
27	16.281000	10.3.141.145	34.237.118.27	TLSv1.2	339			0.000595000 Client Hello
28	16.292346	34.237.118.27	10.3.141.145	TCP	74			0.102797000 443 - 59444 [SYN, ACK] Seq=0 Ack=1 Win=2912 Len=0 MSS=1460 TSval=324651939 TSecr=5721218 US=256
29	16.222335	10.3.141.145	34.237.118.27	TCP	66			0.007050000 59444 - 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=5721218 TSecr=324651939
30	16.222830	10.3.141.145	34.237.118.27	TLSv1.2	339			0.000595000 Client Hello
31	16.289808	34.237.118.27	10.3.141.145	TCP	74			0.000292000 443 - 59444 [SYN, ACK] Seq=0 Ack=1 Win=2912 Len=0 MSS=1460 TSval=324651939 TSecr=5721218 US=256
32	16.272179	10.3.141.145	34.237.118.27	TCP	66			0.011312000 59444 - 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=5721218 TSecr=324651939
33	16.275846	10.3.141.145	34.237.118.27	TLSv1.2	339			0.000567000 Client Hello
34	16.282281	34.237.118.27	10.3.141.145	TCP	66			0.100393000 443 - 59444 [ACK] Seq=1 Ack=274 Win=2912 Len=0 TSval=324652050 TSecr=5721217
35	16.283978	34.237.118.27	10.3.141.145	TLSv1.2	1514			0.001300000 Server Hello

Sources:

<https://howtoraspberrypi.com/create-a-wi-fi-hotspot-in-less-than-10-minutes-with-pi-raspberry/>