



CyberCamp at UNK

WiFi Pineapple NANO

What you will learn with this tutorial...

*This tutorial will guide you through the installation and configuration processes of a **WiFi Pineapple NANO**. We will discuss what it is in a few moments, but basically this is a powerful piece of hardware that is a wireless auditing platform. We will go through the pre installation, installation, configuration, and understand some of the features and how to use them properly. Let's start!*

1 What is the WiFi Pineapple NANO?

A *WiFi Pineapple NANO* is a portable network auditing platform. It is a small device that is connected to a computer via USB, using a Y USB cable.

With this device you are able to do a lot of things, among them:

- Scan the WiFi networks of your surroundings, recognizing SSIDs and clients;
- Configure an Access Point (AP) with the Pineapple, so you act as a sniffer on the requests of all your connected clients;
- Record and analyze logs, generating emailed reports;
- Identify vulnerable devices inside an organization.

The Pineapple NANO can be executed in Windows, Linux and Android devices. In this guide we will learn how to install and configure the Pineapple for Windows and Linux platforms, and we will also learn how to use some of its basic features.

2 Before starting

All the features provided by the Pineapple are controlled throughout a Web interface. This interface is properly loaded when using either Mozilla Firefox or Google Chrome browsers. Make sure you have one of these browsers installed on your machine.

Raspberry Pi does not have Google Chrome nor Mozilla Firefox available so far, however, you can install Chromium, another browser that runs the same engine as Google Chrome. To install Chromium on your Raspberry Pi open your terminal and type the following commands:

```
1 wget -qO - http://bintray.com/user/downloadSubjectPublicKey?username=bintray
   | sudo apt-key add -
2 echo "deb http://dl.bintray.com/kusti8/chromium-rpi jessie main" | sudo tee
   -a /etc/apt/sources.list
3 sudo apt-get update
4 sudo apt-get install chromium-browser rpi-youtube -y
```

If you are using Windows and do not have Google Chrome installed yet, download the executable from this link: <https://www.google.com/chrome/browser/desktop/>, execute it and follow the instructions on the screen to complete the installation.

Now you have a compatible browser to the Pineapple Web interface. We can start installing and configuring our device.

3 Updating the firmware and setting up the AP

After the first connection of a Pineapple NANO to a computer, it's necessary to update the firmware on it. What we are going to cover now is how to do it, and how to set up our Access Point after the firmware is updated.

In order to install the latest firmware available, proceed as follow:

- Connect the Pineapple NANO to a computer using the Y USB cable provided in the device box and wait until the blue light stops blinking;
- Go to wifipineapple.com/nano, select the desired operating system, and click **Download** to obtain the firmware file;
- Open your browser and navigate to <http://172.16.42.1:1471> to start the WiFi Pineapple NANO configuration;
- You should obtain a screen like the one below:

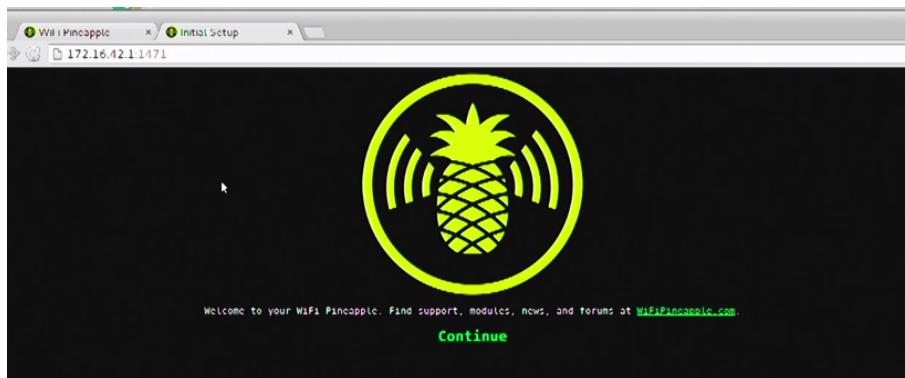


Figure 1: WiFi Pineapple NANO initial screen

- Follow the next steps provided in the screen in order to finish updating the firmware of the device. **Important note:** After you select the firmware file, the upgrade takes up to 5 minutes to finish. In the meantime, don't disconnect your device. The update is done when the blue light stops blinking;
- After the update is done, you should obtain the screen below, if you didn't refresh your page.

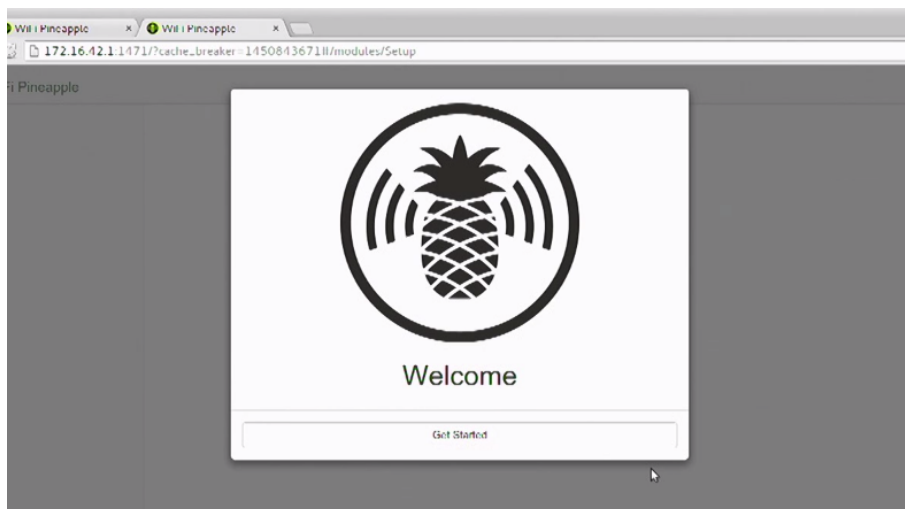


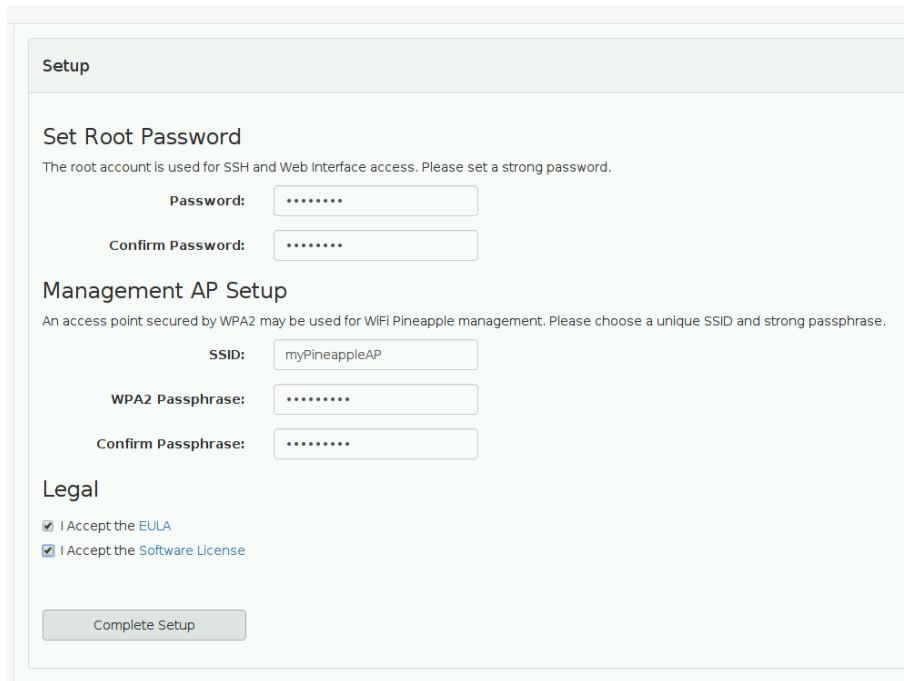
Figure 2: WiFi Pineapple NANO welcome screen

The firmware is successfully installed now. Next thing is to set up your Pineapple Access Point. To do so, start clicking on the button **Get started**. You will be asked to press the reset button at the back of the Pineapple, go ahead and do it. After that a form will load where you will set up the root user for the device, and the SSID and password for your WiFi AP.

To maintain a certain pattern, put **admin123** as the password of the root user. Of course, if you are auditing networks professionally you should use a stronger password, for now since we are just learning this one will be okay.

Name your SSID as you please, and also choose a password for it.

When everything is filled, select **I Accept the EULA** and **I Accept the Software License** boxes and click on **Complete Setup**.



The screenshot shows the 'Setup' page of the WiFi Pineapple NANO. It is divided into three main sections: 'Set Root Password', 'Management AP Setup', and 'Legal'. In the 'Set Root Password' section, there are two password fields, both containing seven asterisks. The 'Management AP Setup' section has three fields: 'SSID' with the value 'myPineappleAP', and two 'WPA2 Passphrase' fields, both containing seven asterisks. The 'Legal' section has two checkboxes, both of which are checked; the first is labeled 'I Accept the EULA' and the second is 'I Accept the Software License'. At the bottom of the form is a 'Complete Setup' button.

Figure 3: WiFi Pineapple NANO AP setup

Now the Pineapple AP is configured! All devices that have WiFi can now connect to this Access Point we had just created. However, there is no Internet connection yet. So far we just have created the network. In the next section we will learn how to redirect the Internet connection of the PC the Pineapple is on to our AP.

4 Internet connection share

What we need to do now is redirect our computer's Internet connection to the Pineapple Access Point we created. Think of it like building a bridge that connects the Internet to our NANO device. This process is different for Linux and Windows. Now we will see, step by step, how to configure the Internet connection share for these two different operating systems.

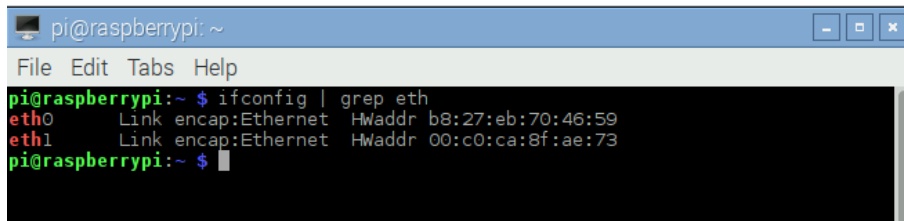
4.1 Linux

Follow these steps to enable the Internet connection share at Linux:

1. First thing to do is to be sure of which network interface is the Pineapple NANO. Type the following command in your terminal to see all the interfaces of your computer:

```
ifconfig | grep eth
```

You should obtain something like this:

A terminal window titled 'pi@raspberrypi: ~' with a menu bar 'File Edit Tabs Help'. The terminal shows the command 'ifconfig | grep eth' and its output: 'eth0 Link encap:Ethernet HWaddr b8:27:eb:70:46:59' and 'eth1 Link encap:Ethernet HWaddr 00:c0:ca:8f:ae:73'. The prompt 'pi@raspberrypi:~ \$' is visible at the bottom.

```
pi@raspberrypi:~ $ ifconfig | grep eth
eth0    Link encap:Ethernet  HWaddr b8:27:eb:70:46:59
eth1    Link encap:Ethernet  HWaddr 00:c0:ca:8f:ae:73
pi@raspberrypi:~ $
```

Figure 4: Connected network interfaces

Most probably, the computer default network interface will be **eth0**, and the Pineapple NANO is the other one, in this case **eth1**. To be sure of this, execute the following command:

ifconfig eth1

With this command we take a look at the properties of the network interface passed as parameter, in this case we suspect **eth1** is our NANO. Among the fields this command brings to us, there is one called *inet addr*, that contains the IP given to the device, if this address is in the range of **172.16.42.XX** you can be sure that this is the Pineapple interface. This is the range of operation for this device.

2. Now that you are sure of what each one of your interfaces do, we need to download a bash script that will help us configuring the Internet connection share. Disconnect the Pineapple from your machine (we will need Internet to download the script, and right now we still don't have it when Pineapple is connected to the computer), and execute the following command:

wget wifipineapple.com/wp6.sh

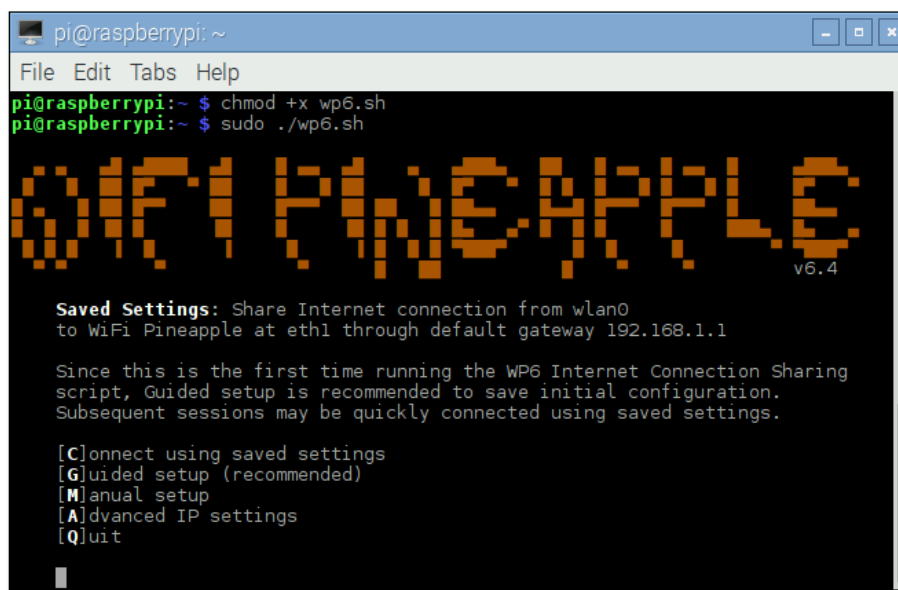
3. Connect your Pineapple NANO once again to your computer.
4. Grant file permissions to be able to execute the script:

chmod +x wp6.sh

5. Run the script as superuser using the following command:

sudo ./wp6.sh

6. You should now be presented to this menu:



```
pi@raspberrypi: ~  
File Edit Tabs Help  
pi@raspberrypi:~$ chmod +x wp6.sh  
pi@raspberrypi:~$ sudo ./wp6.sh  
  
WP6 PINEAPPLE v6.4  
  
Saved Settings: Share Internet connection from wlan0  
to WiFi Pineapple at eth1 through default gateway 192.168.1.1  
  
Since this is the first time running the WP6 Internet Connection Sharing  
script, Guided setup is recommended to save initial configuration.  
Subsequent sessions may be quickly connected using saved settings.  
  
[C]onnect using saved settings  
[G]uided setup (recommended)  
[M]anual setup  
[A]dvanced IP settings  
[Q]uit
```

Figure 5: Internet connection share script menu

- Type **G**.
- Disconnect your Pineapple from computer and press any key.
- Type **Y** and hit enter to accept the default gateway.
- Confirm your Internet interface, type **Y** and hit enter.
- Reconnect the Pineapple to the computer.
- Confirm your Pineapple interface, type **Y** and hit enter.
- You will be back to the menu, type **C** to connect.

You should now be connected to the Internet with your Linux computer when Pineapple NANO is plugged on it.

4.2 Windows

Follow these steps to enable the Internet connection share at Windows:

1. Connect the WiFi Pineapple NANO to your Windows computer.
2. Navigate to **Control Panel > Network and Internet > Network and Sharing Center**. This path may vary according to the Windows version you are using. But in general, it will always be available through the Network section present inside the Control Panel. When in the *Network and Sharing Center* select *Change adapter settings*. See the figure below:

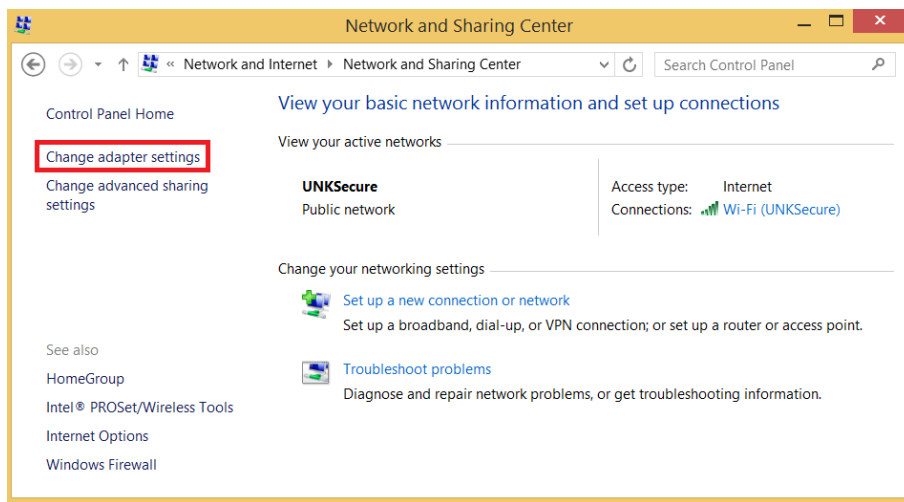


Figure 6: Windows Network and Sharing Center

When you click on *Change adapter settings* you will be redirected to a window where you will be able to see all the network interfaces available on your computer.

Click once over the network whose vendor is **ASIX AX88772A USB2.0**, hit **F2** and rename it to **WiFi Pineapple**. This is how it should be like now:

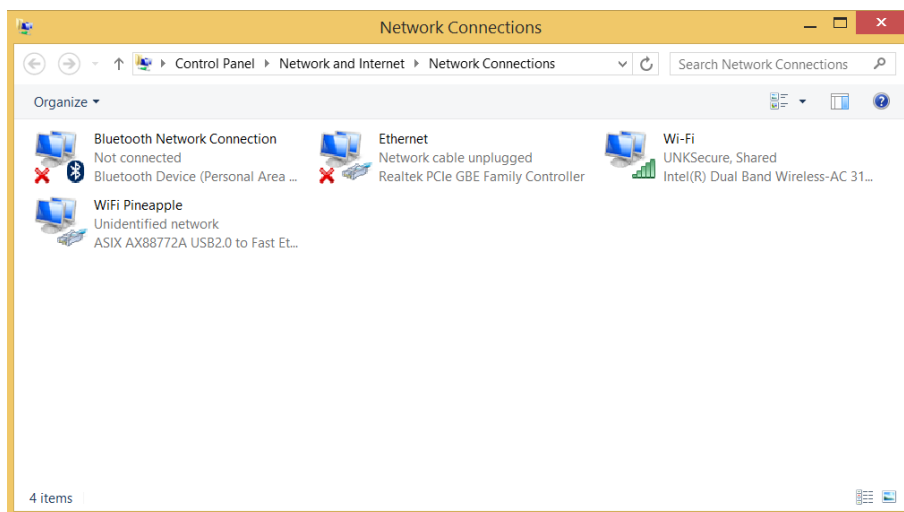


Figure 7: Windows Network Connections

- Now we will allow our interface network who is connected to the Internet share this connection with our WiFi Pineapple interface. Right click on your network that is connected to the Internet (in this case, **Wi-Fi**), **Properties**, and click on the tab **Sharing**. Mark the box that says **Allow other network users to connect through this computer's Internet connection**, and in the drop-down menu below it select **WiFi Pineapple**. After that hit OK and close the window.

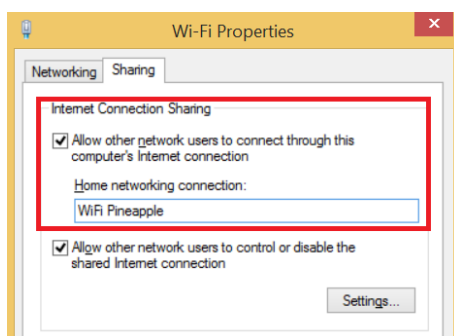


Figure 8: Wi-Fi Properties

- Last step is to set up the IP of our WiFi Pineapple interface to the same range of our device. Right click on **WiFi Pineapple**, **Properties**, and on the **Networking** tab, select **IPV4** from the list, and hit **Properties**. In the field **IP address** type: **172.16.42.42**. Hit OK and close the window.

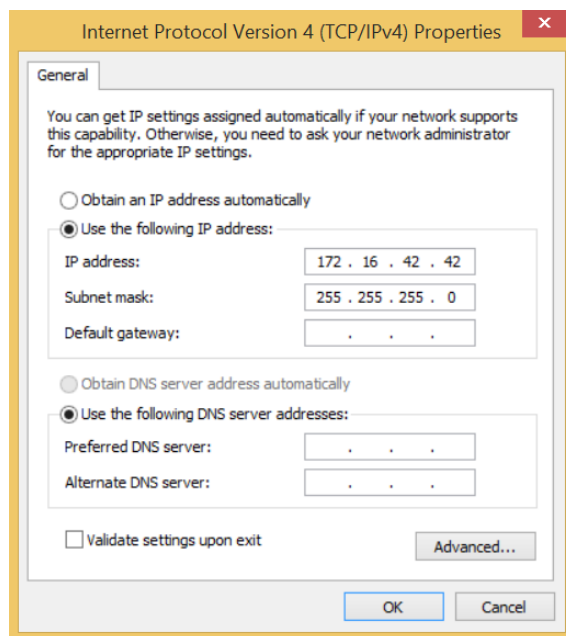


Figure 9: WiFi Pineapple IPV4 configuration

You should now be connected to the Internet with your Windows computer when Pineapple NANO is plugged on it.

5 Configuring some WiFi Pineapple NANO features

As said before, this device provides a lot of interesting features. We will now briefly discuss three of them: *PineAP*, *Recon* and *Landing page*.

5.1 PineAP

So far we have our device updated, our AP created, and Internet being redirected from our computer's interface to our Pineapple. However we still need to configure our AP. We can do that with **PineAP**. Browse to `http://172.16.42.1:1471/#/modules/Dashboard` and on the left side menu select **PineAP**.

In order to be able perform sniffing and injections through the Pineappl, click on the button **switch**, right after *PineAP Daemon: Disabled*. This will enable it. Some other options are interesting to be checked:

- **Allow associations**: allow clients to connect to the Pineapple.
- **Log Probes** and **Log Associations**: generate logs that you can see and save later.
- **Beacon Response** and **Capture SSIDs to Pool**: captures all the SSIDs on the vicinity and add to a list.

We will not select *Broadcast SSID Pool*, if we do so, the Pineapple will broadcast all networks it found at the vicinity, and it can be hard to locate the network we want when we are going to connect some device to it.

When you are done with the selections, click on **Save PineAP settings** button.

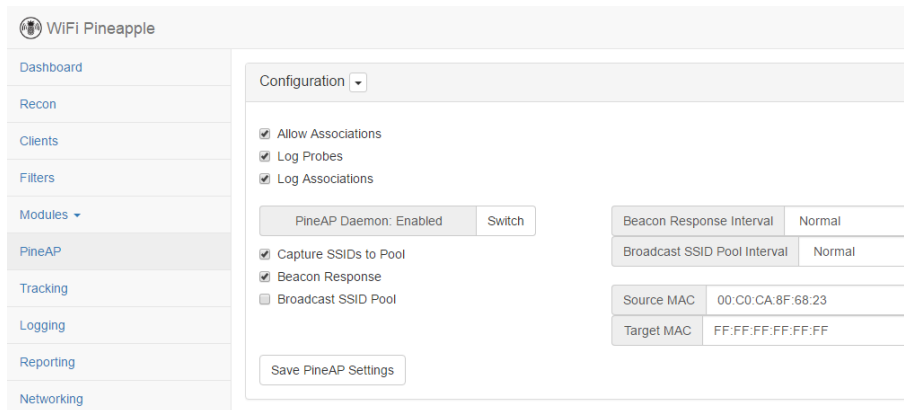


Figure 10: WiFi Pineapple PineAP module

5.2 Recon

The **Recon** module is really easy to use and really important. It allows us to recognize and obtain the names and MAC addresses of clients and APs near the Pineapple. Check *AP & Client*, select the amount of time that you want the scan to execute, and hit the button **Scan**. After the scan is completed you will obtain a list of what Pineapple was able to find near you. If you want it to continuously execute the scan, just mark the box *Continuous*.

SSID	MAC
UNKSecure	D8:C7:C8:EF:F0:F0
	20:A2:E4:BF:C3:94
UNKGuest	D8:C7:C8:EF:F0:F1
Hidden	D8:C7:C8:EF:F0:F2

Figure 11: WiFi Pineapple Recon module

5.3 Landing Page

The last feature we are going to cover for now is how to set up a landing page for your access point. Landing page is the page that is loaded and showed in the user's device right after it is connected to the access point. A lot of free WiFi hot-spots make use of this feature.

To set your own landing page select **Configuration** in the left menu. On the right side click on the button **Switch**, to enable *Landing Page*. On the box located below it you can code your customized page, using HTML, CSS and PHP (it's totally up to you). When you are done just click on **Save**. Next time some device connect to you AP it will be redirected to your customized page.

6 Sniffing the network with Wireshark

As you could notice already, the WiFi Pineapple NANO is quite a powerful tool. This guide showed you how to install and configure it, and how to use some of its basic features.

Wireshark is an open source traffic analyzer. After your Pineapple is configured and running, and you have some clients connected to your AP, you can run Wireshark to sniff the packets traffic of the devices connected to your wireless network.

To install Wireshark on **Linux**:

```
sudo apt-get update  
sudo apt-get install wireshark
```

To install Wireshark on **Windows** browse to <https://www.wireshark.org/download.html>, download the correct version for your computer, execute and install it.

You must be a superuser to run Wireshark with its full functionality. To open it as superuser on **Linux**:

```
sudo wireshark
```

If you are on **Windows** right click on the launch icon and choose: **Run as administrator**.

After Wireshark is opened, select the WiFi Pineapple in the interfaces list. You will now be able to see the traffic of all of your clients.