Capturing Wireless Traffic from a Client Machine

Wireless packet captures are incredibly useful while troubleshooting specific events on a WLAN. The most common use is to see all communication (data, management and control frames) between a station (STA) and an access point (AP).

This is easily possible while using an AirPCAP adapter however these can be expensive and may not be available while experiencing connectivity issues.

In order to do this without using the dedicated hardware mentioned above, a Mac or a PC using Linux is needed.

Viewing wireless traffic is a two step process:

1. Put the wireless adapter in monitor/promiscuous mode
2. View the traffic using Wireshark in Monitor Mode

NOTE: When capturing wireless traffic on an SSID with encryption enabled, such as WPA2-PSK, ensure that the monitor mode capture is started before associating the client to the SSID so that the client traffic can be properly decrypted for later examination of the captures.

Monitoring on macOS

Monitoring on Macs running Sierra and High Sierra (10.12.x and 10.13.x)

Make sure you are not connected to any networks (including wired.)
Hold the Option key and click on the Wireless icon in the upper right. By holding the Option key, it will show a hidden option.

Choose "Open Wireless Diagnostics…"

Once it opens, go to the upper left under the "Window" section and choose "Sniffer"

Pick the appropriate Channel and Channel width to capture. This example shows an example of capturing on 5ghz – Channel 56 with a channel width of 80 Mhz.
Use your Mac as a dedicated sniffer to capture Wi-Fi traffic. Choose a channel and channel width, then click 'Start' to begin.

Click 'Stop' when you are finished and a wireless capture file will be created in /var/tmp.

Channel: 1
Width: 20 MHz

Start
Once you have set your channel and width, click “Start.” Note the directory that it will put the capture in. (/var/tmp)

Stop the capture once you have captured the event.

To navigate to the folder, switch to Finder. Then select Go at the top, and then “Go to folder…”

Fill in the folder /var/tmp and click “Go”
In the folder you’ll find your Monitor mode Capture
Monitoring on Macs running Yosemite (10.10.x)

Open the Wireless Diagnostics program from spotlight (Command + Spacebar):

When at the Introduction page, press **Command + 6** to open the Sniffer:

*Note: On 10.9 Mavericks, use **Command + 2**, then go to the Frame Capture tab.*

Pick the **Channel** and channel **Width**, and press **Start**. This should match the channel currently in use by the client/AP that is to be monitored.

During the capture you’ll see the eye icon over the wireless monitor indicating that the interface is in Monitor Mode:

This capture can be viewed live from Wireshark running in Monitor Mode (instructions found at the bottom of the article). Traffic collected will also be automatically saved to a temporary .wcap file on the desktop. To open this capture in Wireshark, simply change the suffix from .wcap to .pcap and open from Wireshark.

To end the capture, simply click the **Stop** button.

---

**Monitoring on Linux**
Monitoring on Kali Linux

Find out which wireless interfaces are available by running the `iwconfig` command in a terminal:

```
root@kali:~# iwconfig
eth0    no wireless extensions.
lo      no wireless extensions.
wlan0   IEEE 802.11abgn ESSID:off/any
        Mode:Managed  Access Point: Not-Associated  Tx-Power=15 dBm
        Retry short limit:7  RTS thr:off  Fragment thr:off
        Encryption key:off
        Power Management:off
```

In order to set an interface to Monitor Mode (usually wlan0), run `airmon-ng start wlan0`. If monitoring another interface, replace `wlan0` with the desired interface name. When running this command, a message may appear that indicates processes that “could cause trouble”:

```
root@kali:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after a short period of time, you may want to kill (some of) them!
-e

PID     Name
3004    NetworkManager
3118    wpa_supplicant

Interface  Chipset        Driver
wlan0      Intel 6300     iwlwifi - [phy0] (monitor mode enabled on mon0)
```

If `airmon-ng` indicates that there are interfering processes, find the processes and kill them by typing `kill [PID]`:
Now that those processes have been killed, start the process over. Kill the mon0 interface using `airmon-ng stop mon0`:

```
root@kali:~# kill 3004
root@kali:~# kill 3118
```

...and recreate it now that there aren't any interfering processes. This is done by running `airmon-ng start wlan0` again:

```
root@kali:~# airmon-ng start wlan0
```

Notice above that when running `airmon-ng start wlan0` this time, it didn't say that there were any conflicting processes.

Finally, specify the channel to monitor on by using `airodump-ng mon0 --channel [CHANNEL]`. In the example below, channel 1 is being monitored:

```
root@kali:~# airodump-ng mon0 --channel 1
```
Using Wireshark in Monitor Mode

Once a wireless card is in monitor/promiscuous mode, the data can be viewed live using Wireshark in Monitor Mode.

Note: The following screenshots were taken using an old (pre v2.0) version of Wireshark. To enable Monitor Mode in newer versions, please reference the Wireshark Wiki for details.

In the example below, interface en0 (Mac) or mon0 (Linux) was selected and specified to use monitor mode.

Once this mode is selected and the capture is started in Wireshark, the 802.11 frames will start to fill the screen. This will be the majority of the traffic, and since there aren't any coloring rules for 802.11 traffic by default, they should be white:
NOTE: For more information about decrypting 802.11 traffic in Wireshark, please refer to this [link](#).