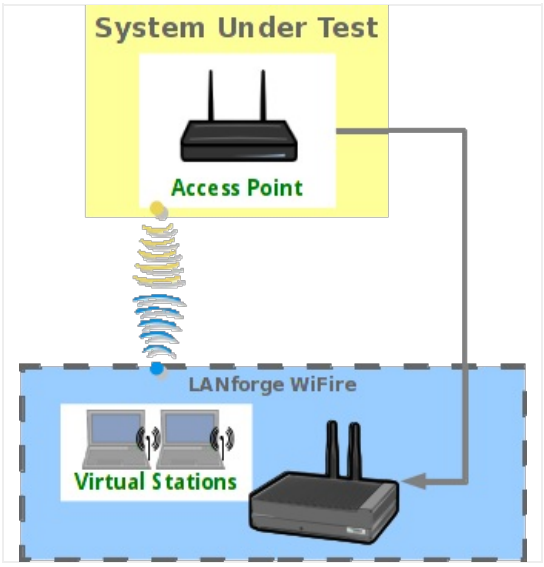
sales@candelatech.com
support@candelatech.com
+1 (360) 380-1618 [PST, GMT -8]

Using Wireshark to Sniff WiFi Monitors

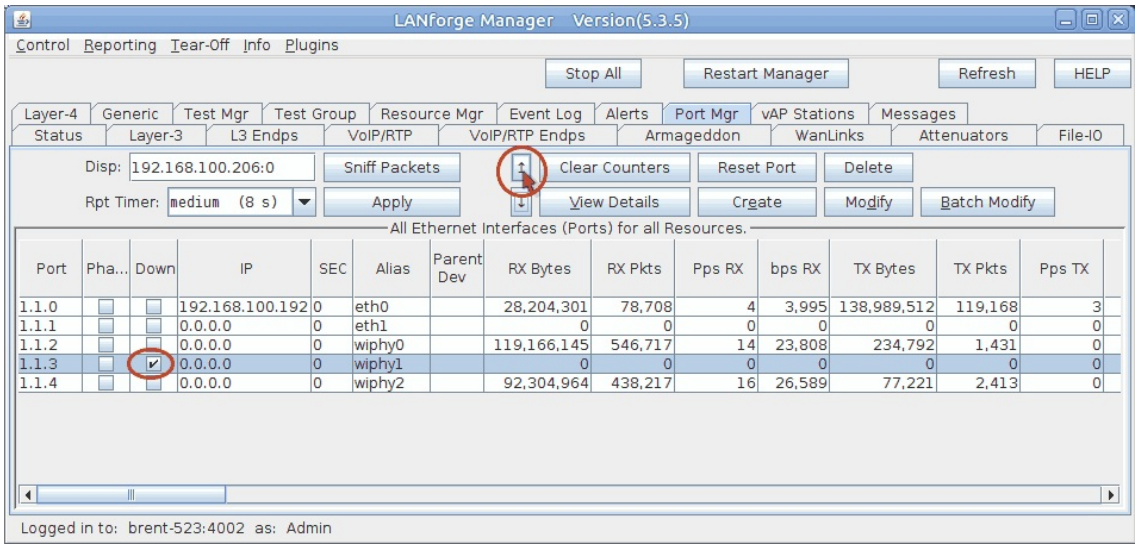
Goal: Sniff wireless traffic from a LANforge radio using Wireshark and a WiFi Monitor port.

The best way to sniff wireless packets via Wireshark in LANforge is from a monitor port that is on its own radio (no other AP, STAs, etc.). This example will walk through the monitor port creation, sniffing the monitor port, as well as Wireshark filter recommendations.

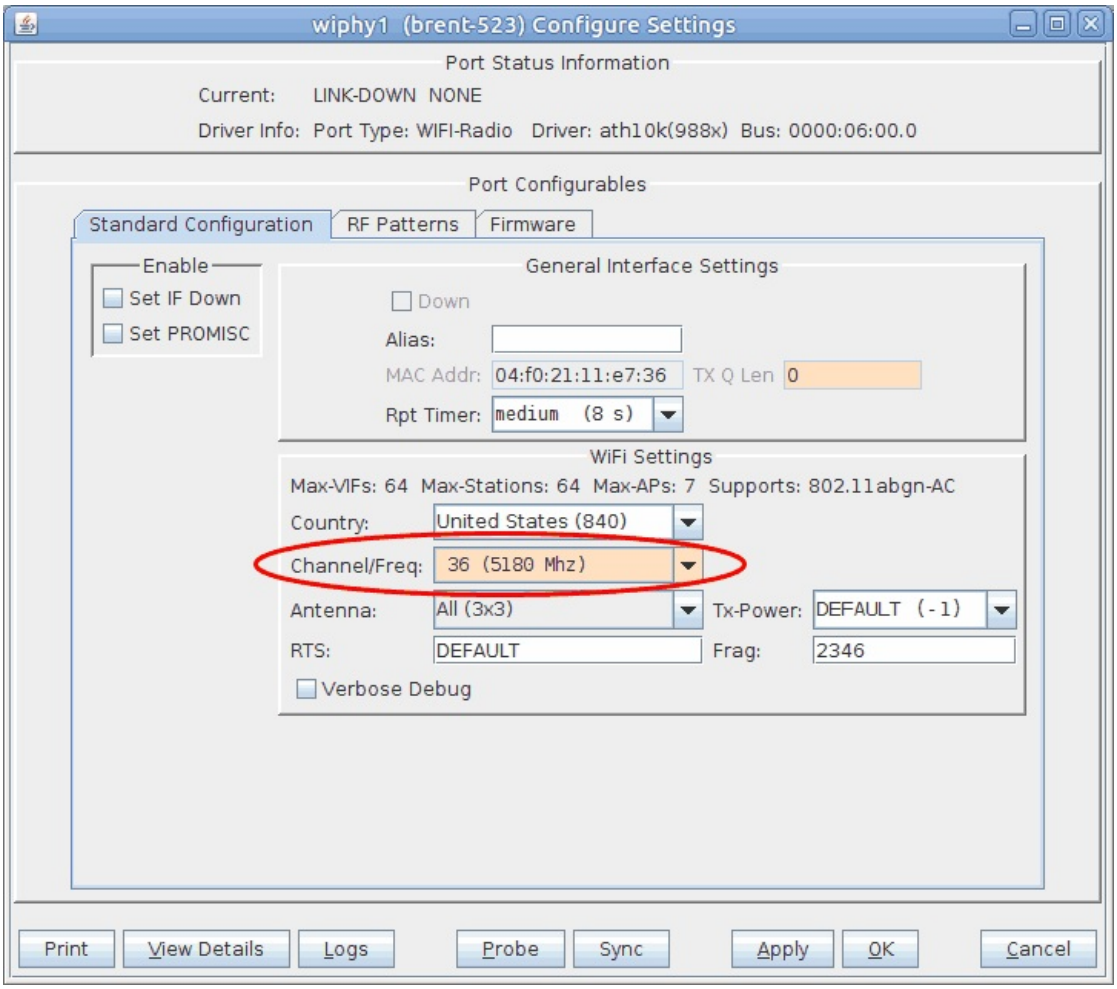
This example uses a LANforge CT523 system but the procedure should work on a CT522, CT525, or similar system.



1. Create a monitor port.
   A. In the **Port Mgr** tab, select a wiphy device that you wish to sniff with (this example will use wiphy1, an ath10k radio).
   B. If the wiphy device is down, click the up arrow to enable it.



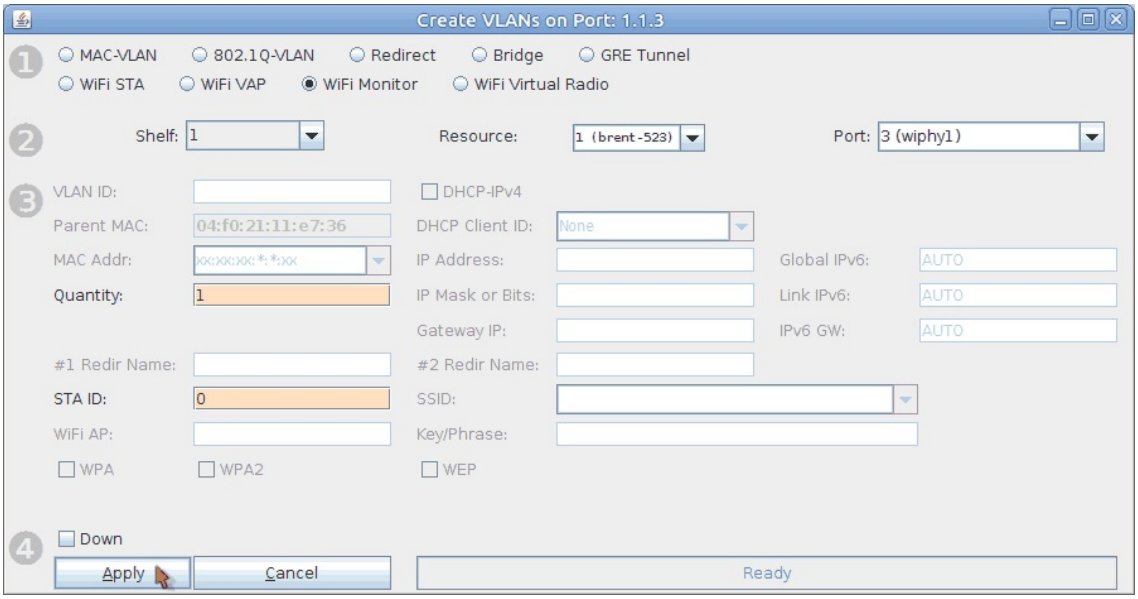
C. Click **Modify**.



A. Select the channel you wish to sniff. Channel 36 will be used for this test.

B. Click **OK**.

D. Back in the **Port Mgr** tab, with the wiphy device still selected, click **Create**.



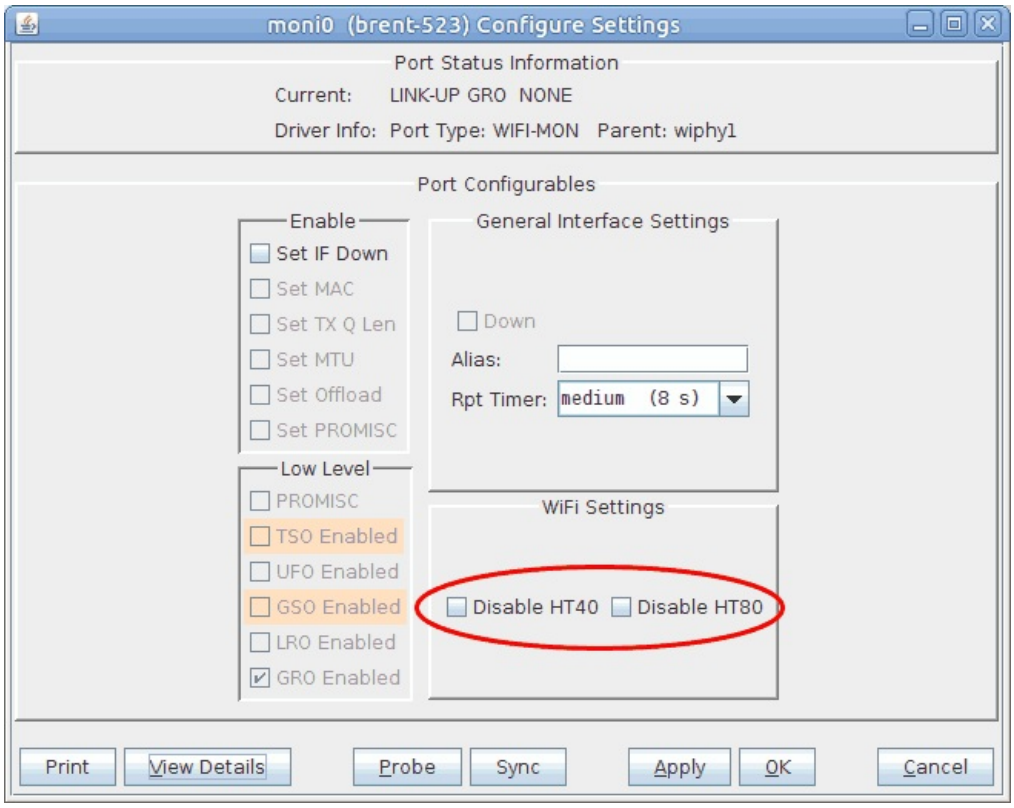
A. Select the **WiFi Monitor** option at the top.

B. Set the **Quantity** to **1**.

C. Set the **STA ID** to **0**.

D. Click **Apply** and close the Create Port window.

E. In the **Port Mgr** tab again, modify **moni0**.



A. You can disable **HT40** and **HT80** here if needed.

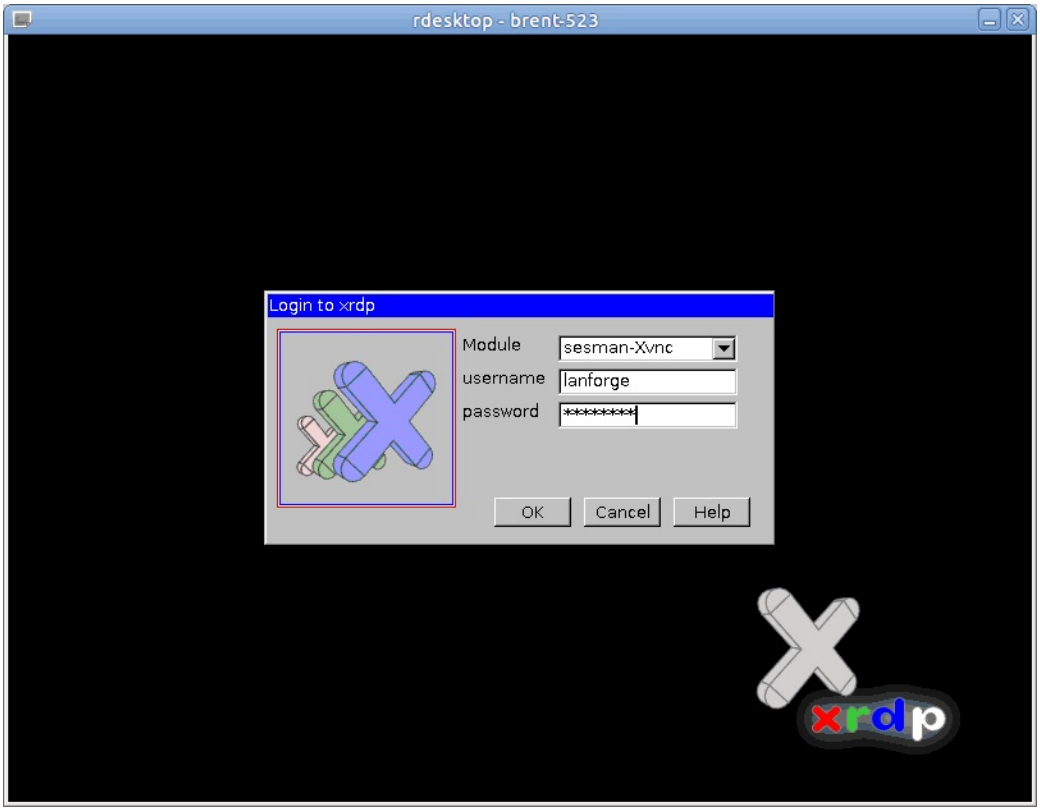
B. Click **OK** to close the window.

2. For this current setup, traffic will be generated with a layer 3 UDP connection between two stations. For more information see Generating Traffic for WLAN Testing

3. Use Wireshark to sniff **moni0**.

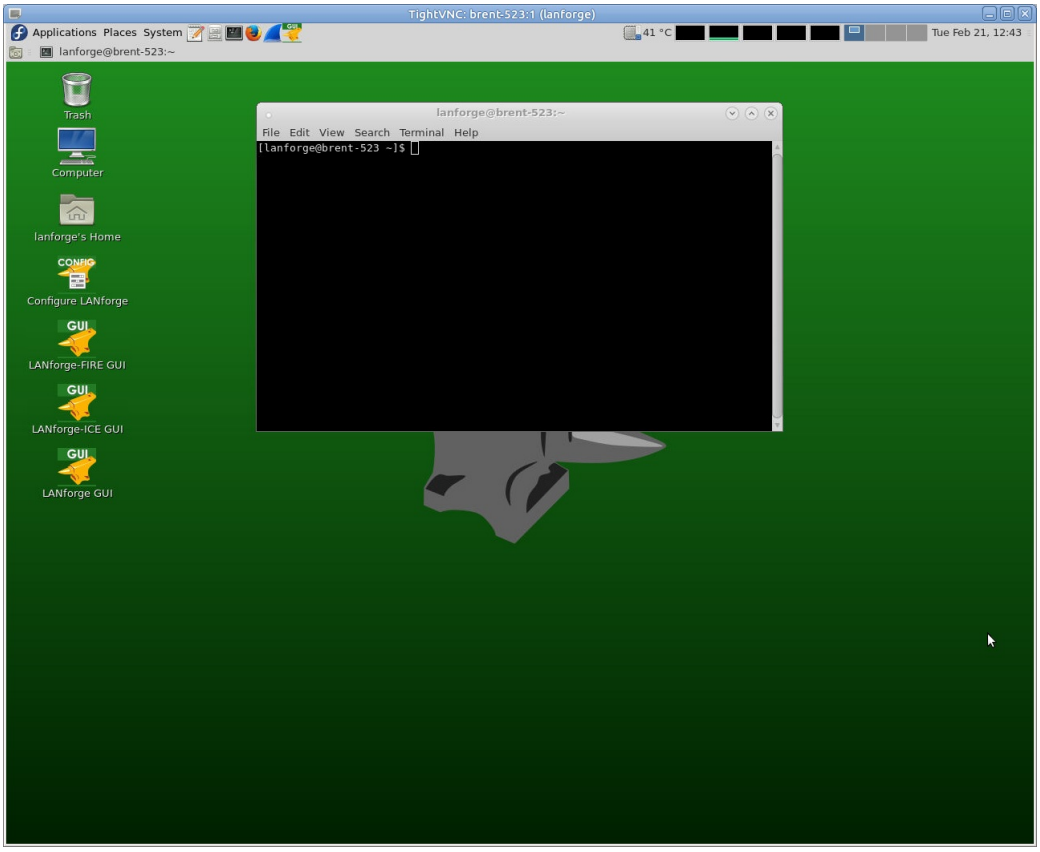
   A. If you are running the LANforge GUI from a Windows machine without x server installed, you will need to connect remotely to the LANforge system via **rdesktop** or **vnc**.

A. To connect via **rdesktop**, type the following command into a console (replace LANforge-IP with the IP of your LANforge system):
`rdesktop LANforge-IP`

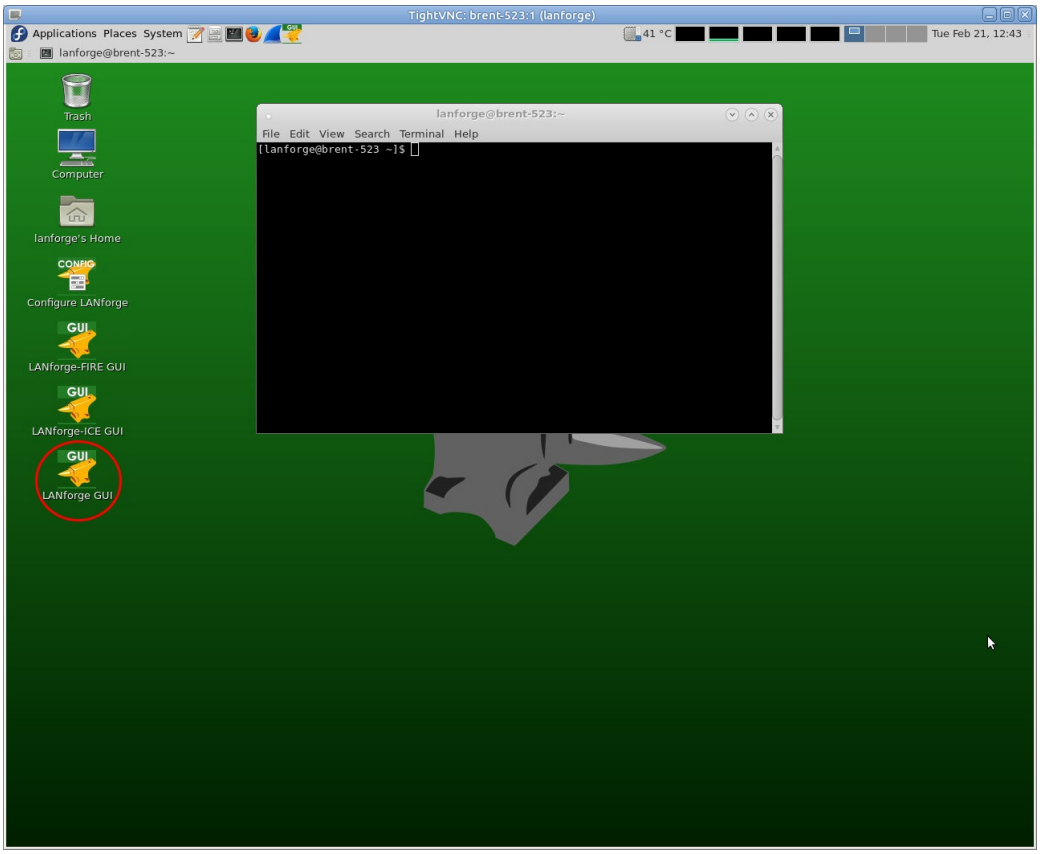


I. The login info is username/password **lanforge/lanforge**

B. To connect via **vnc**, type the following command into a console (replace LANforge-IP with the IP of your LANforge system. **Don't forget to add the ':1' after the IP**):
`vncviewer [LANforge-IP]:1`
The password is **lanforge**.

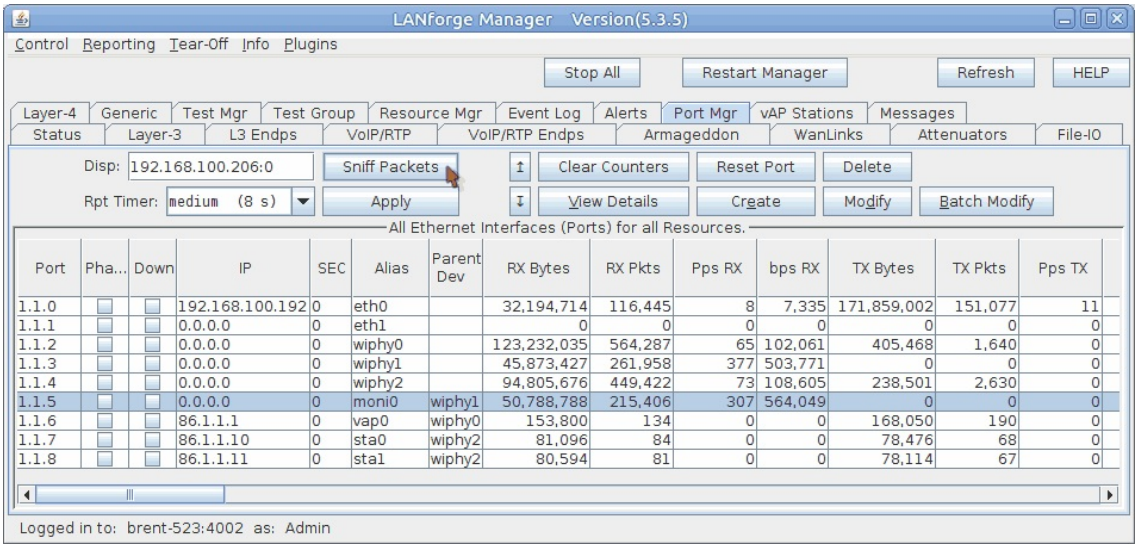


C. Once you have accessed the LANforge system via rdesktop or vnc, open the LANforge GUI with the desktop icon shown below.

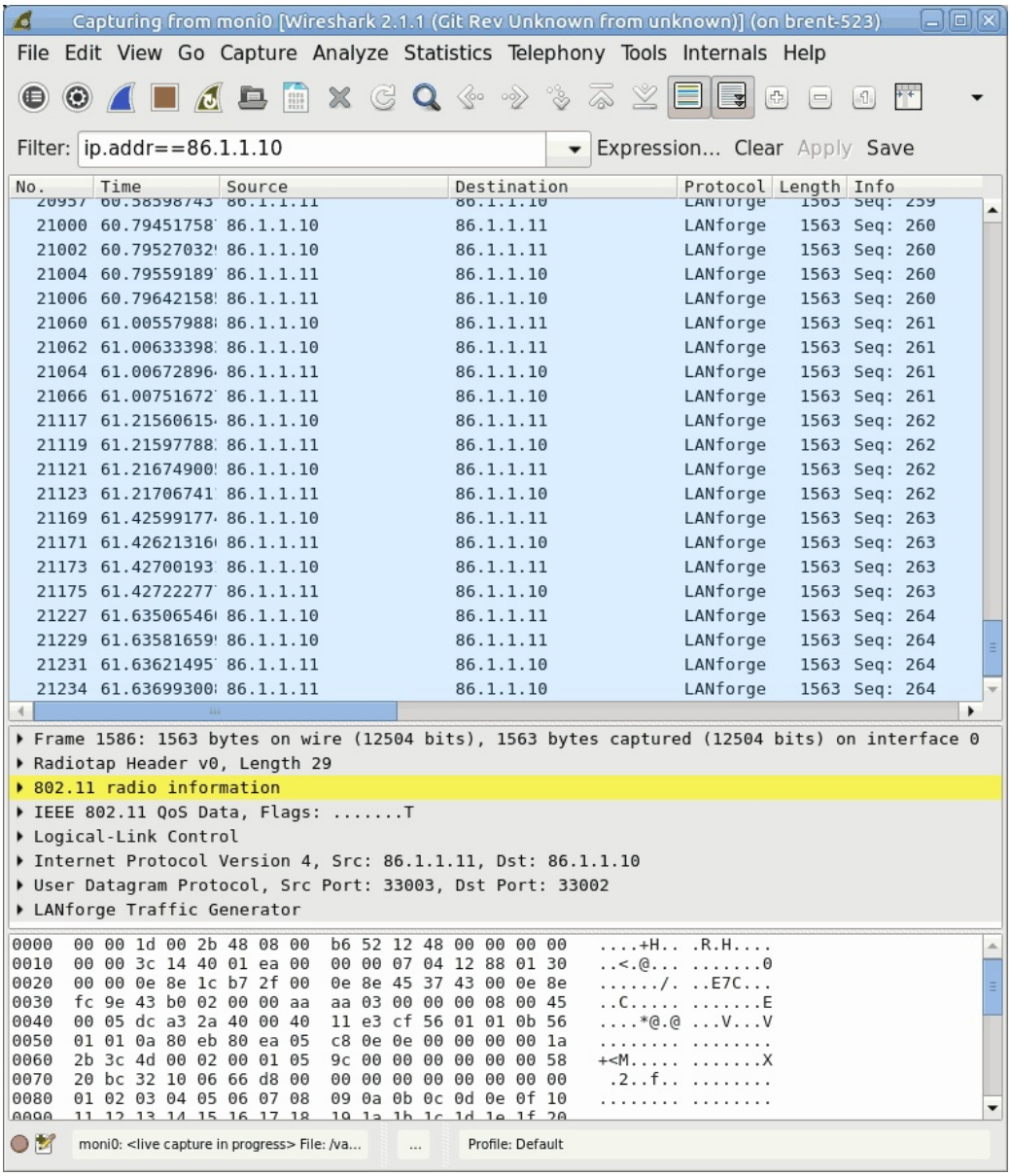


B. Select **moni0** in the **Port Mgr** tab.

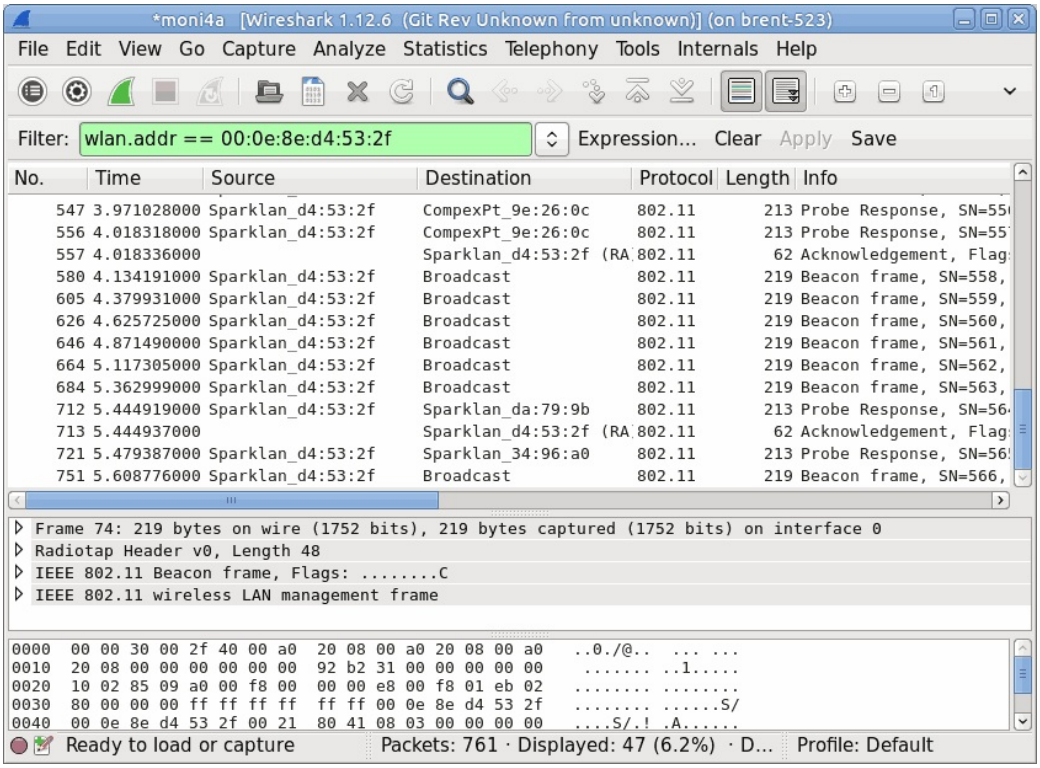
C. Click the **Sniff Packets** button. Wireshark will now open and automatically start scanning for packets. If you get a window that warns about running as user root, click **OK**.



A. To use a filter, simply add the filter constraints to the filter text box as seen below and click **Apply** to the right. The below screenshot has wireshark filtering on a specific IP.



B. If you'd like to only see traffic to/from a single AP use the filter **wlan.addr == [bssid]**



D. There are many filters that can be used in Wireshark. Some handy ones include:
IP: `ip.addr==x.x.x.x`
wlan MAC: `wlan.addr==xx:xx:xx:xx:xx:xx`
Association request `wlan.fc.type_subtype eq 0`
Association response `wlan.fc.type_subtype eq 1`
Probe request `wlan.fc.type_subtype eq 4`
Probe response `wlan.fc.type_subtype eq 5`
Beacon `wlan.fc.type_subtype eq 8`
Authentication `wlan.fc.type_subtype eq 11`
Deauthentication `wlan.fc.type_subtype eq 12`

E. Filters can be combined to specify if packets should match all filters (with **&&**) or any filters (with ||).
For example, if you wanted to view packets that **only contain both** IPs 1.1.1.1 and 2.2.2.2 you could use the following: `ip.addr==1.1.1.1 && ip.addr==2.2.2.2`
Or, if you want to see all packets containing 1.1.1.1 and all packets containing 2.2.2.2, you could use the following: `ip.addr=1.1.1.1 || ip.addr==2.2.2.2`

F. You can visit https://wiki.wireshark.org/DisplayFilters for more tips on filters.
A handy 'cheat sheet' with most filters can be found here.