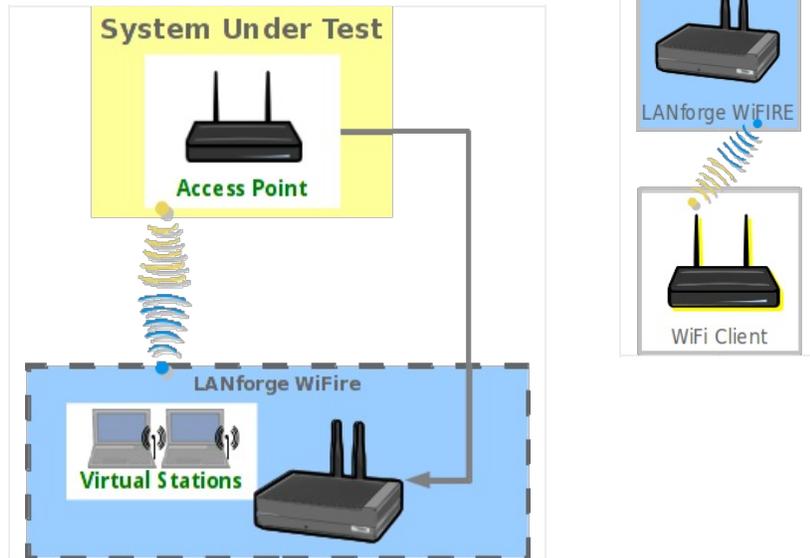


Using Wireshark to Sniff WiFi Monitors

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.

The screenshot shows the LANforge Manager GUI, Version 5.3.5, with the Port Manager tab selected. The 'wiphy1' device is selected and its status is 'Down'. The 'Up' arrow button is highlighted with a red circle.

Port	Pha...	Down	IP	SEC	Alias	Parent Dev	RX Bytes	RX Pkts	Pps RX	bps RX	TX Bytes	TX Pkts	Pps TX
1.1.0		<input type="checkbox"/>	192.168.100.192	0	eth0		28,204,301	78,708	4	3,995	138,989,512	119,168	3
1.1.1		<input type="checkbox"/>	0.0.0.0	0	eth1		0	0	0	0	0	0	0
1.1.2		<input type="checkbox"/>	0.0.0.0	0	wiphy0		119,166,145	546,717	14	23,808	234,792	1,431	0
1.1.3		<input checked="" type="checkbox"/>	0.0.0.0	0	wiphy1		0	0	0	0	0	0	0
1.1.4		<input type="checkbox"/>	0.0.0.0	0	wiphy2		92,304,964	438,217	16	26,589	77,221	2,413	0

Logged in to: brent-523:4002 as: Admin

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**.

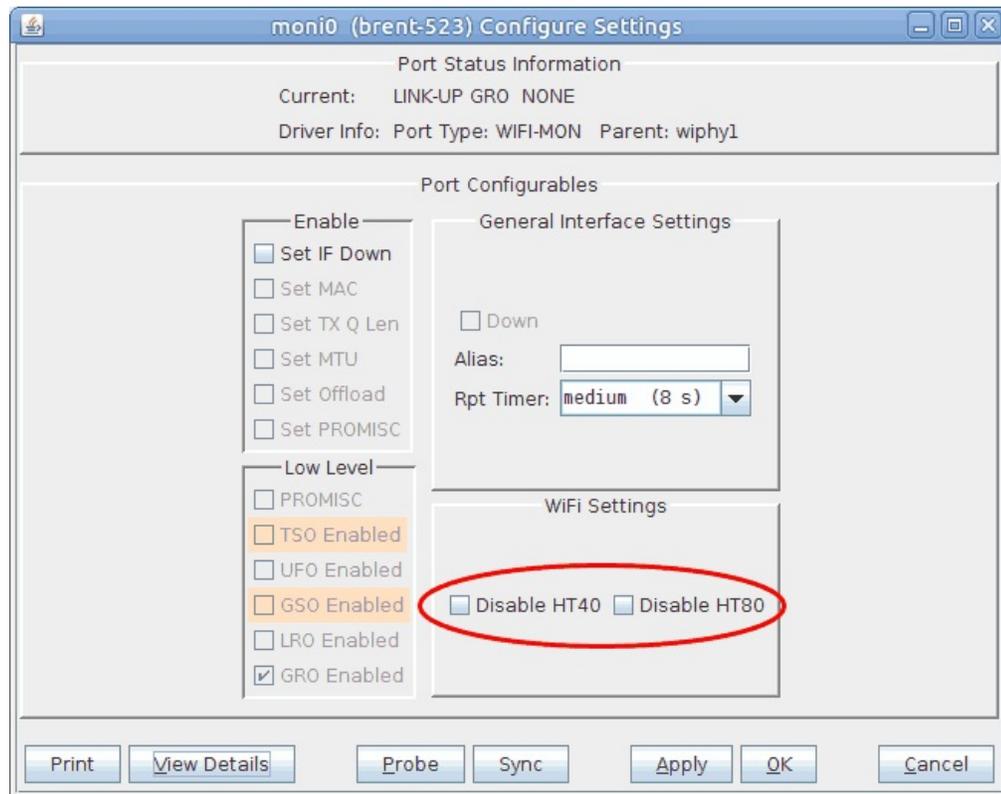
A. Select the **WiFi Monitor** option at the top.

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.

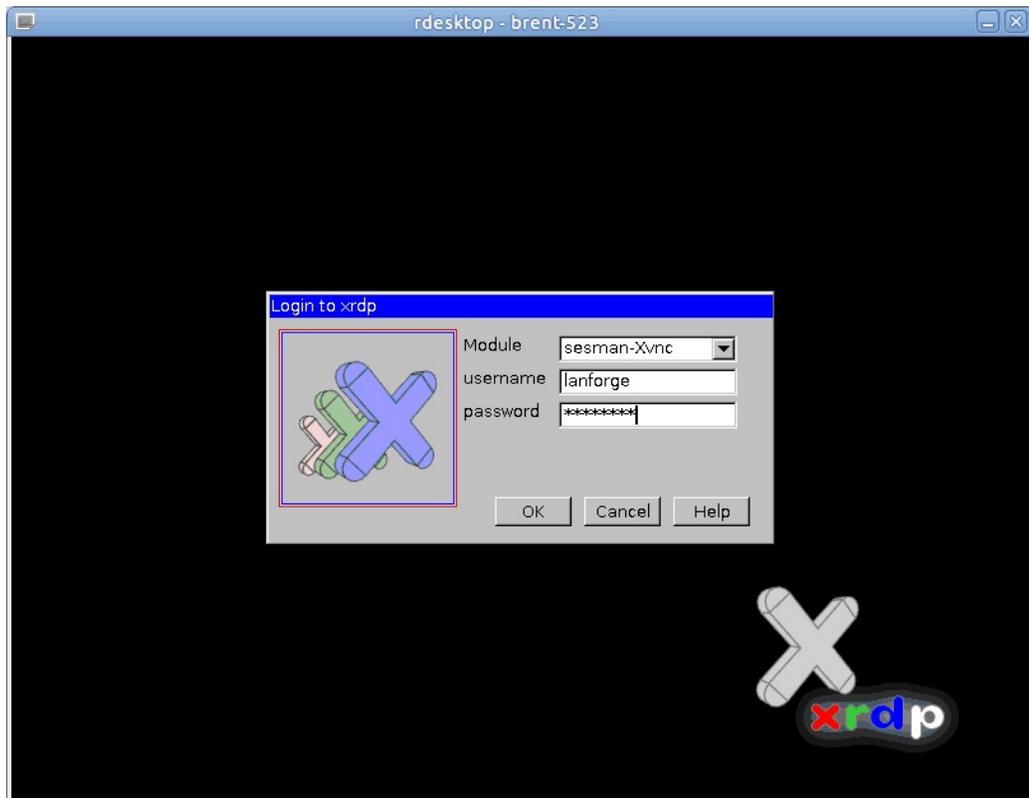
2. For this current setup, traffic will be generated with a layer 3 UDP connection between two stations.
For more information see [Generating Traffic for WLAN Testing](#)

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
```

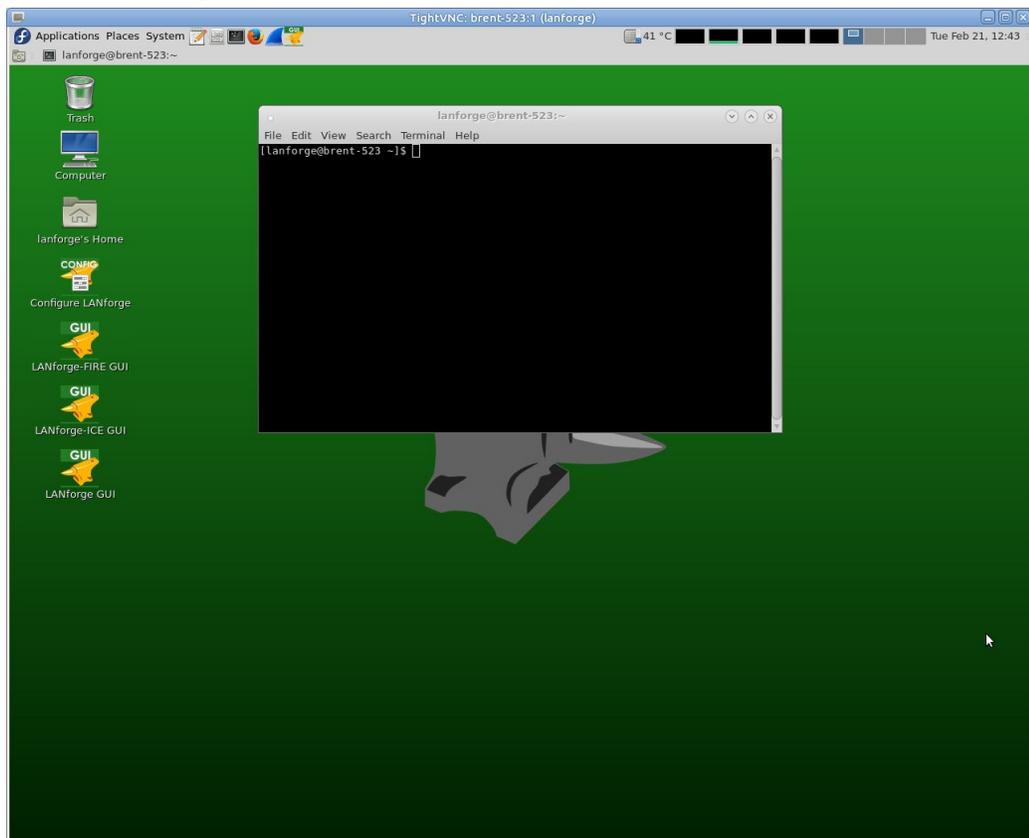


- I. The login info is username/password **lanforge/lanforge**

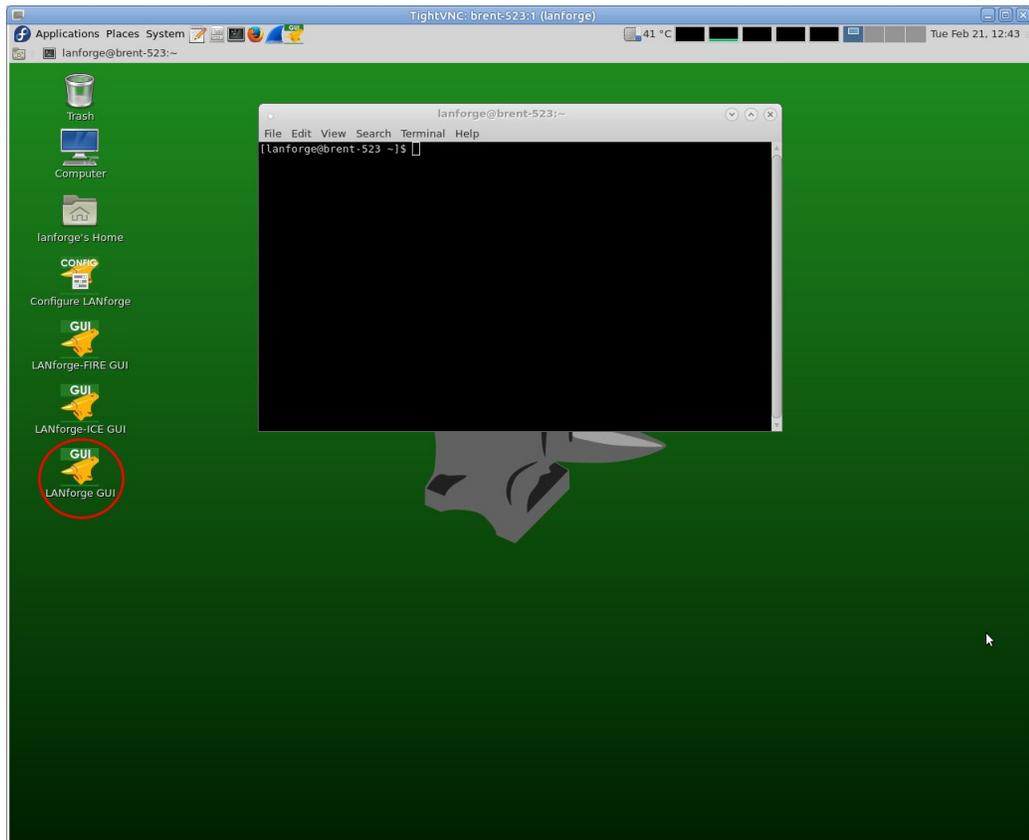
- B. To connect via **vnc**, type the following command into a console (replace LANforge-IP with the IP of your LANforge system. **Don't forget to add the ':1' after the IP**):

```
vncviewer [LANforge-IP]:1
```

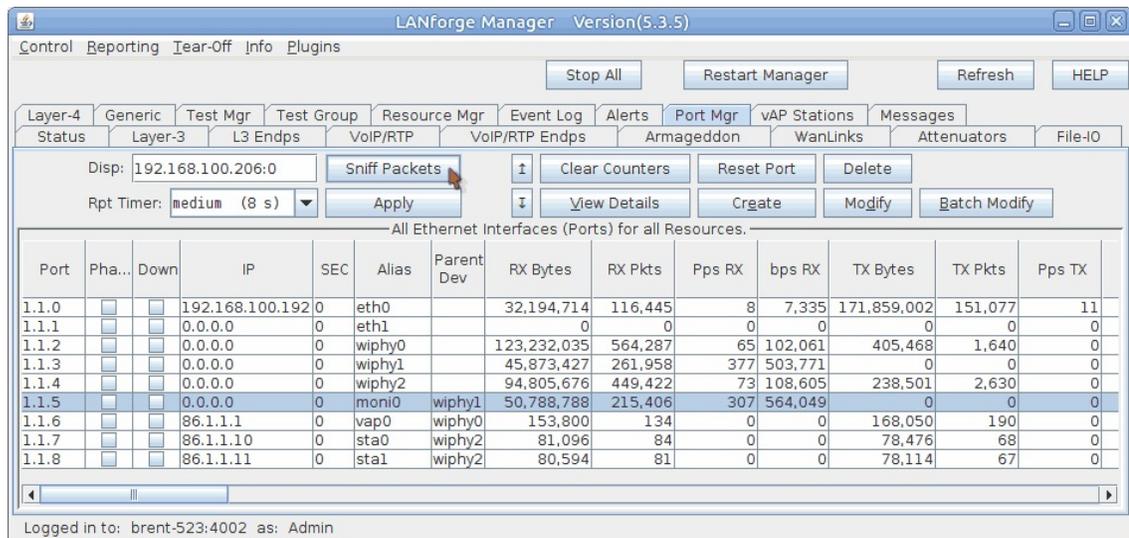
The password is **lanforge**.



- 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.

The screenshot shows the Wireshark 2.1.1 interface with the following components:

- Filter:** `ip.addr==86.1.1.10`
- Packet List Table:**

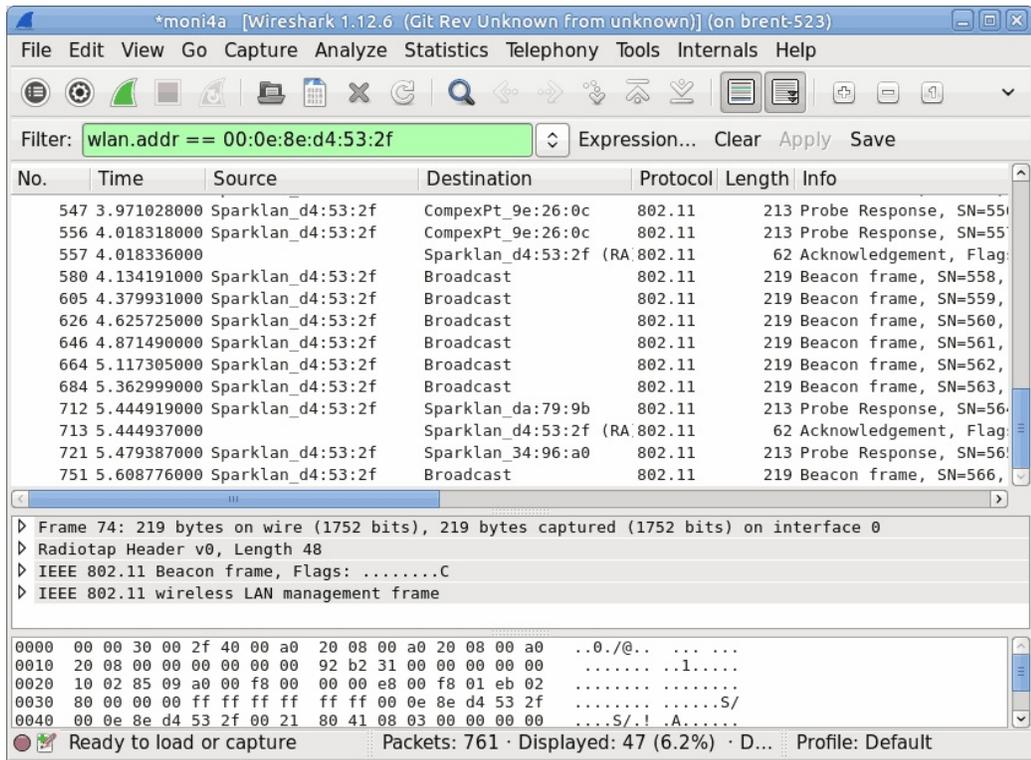
No.	Time	Source	Destination	Protocol	Length	Info
20957	60.58598743	86.1.1.11	86.1.1.10	LANforge	1563	Seq: 259
21000	60.79451758	86.1.1.10	86.1.1.11	LANforge	1563	Seq: 260
21002	60.79527032	86.1.1.10	86.1.1.11	LANforge	1563	Seq: 260
21004	60.79559189	86.1.1.11	86.1.1.10	LANforge	1563	Seq: 260
21006	60.79642158	86.1.1.11	86.1.1.10	LANforge	1563	Seq: 260
21060	61.00557988	86.1.1.10	86.1.1.11	LANforge	1563	Seq: 261
21062	61.00633398	86.1.1.10	86.1.1.11	LANforge	1563	Seq: 261
21064	61.00672896	86.1.1.11	86.1.1.10	LANforge	1563	Seq: 261
21066	61.00751672	86.1.1.11	86.1.1.10	LANforge	1563	Seq: 261
21117	61.21560615	86.1.1.10	86.1.1.11	LANforge	1563	Seq: 262
21119	61.21597788	86.1.1.11	86.1.1.10	LANforge	1563	Seq: 262
21121	61.21674900	86.1.1.10	86.1.1.11	LANforge	1563	Seq: 262
21123	61.21706741	86.1.1.11	86.1.1.10	LANforge	1563	Seq: 262
21169	61.42599177	86.1.1.10	86.1.1.11	LANforge	1563	Seq: 263
21171	61.42621316	86.1.1.11	86.1.1.10	LANforge	1563	Seq: 263
21173	61.42700193	86.1.1.10	86.1.1.11	LANforge	1563	Seq: 263
21175	61.42722277	86.1.1.11	86.1.1.10	LANforge	1563	Seq: 263
21227	61.63506546	86.1.1.10	86.1.1.11	LANforge	1563	Seq: 264
21229	61.63581659	86.1.1.10	86.1.1.11	LANforge	1563	Seq: 264
21231	61.63621495	86.1.1.11	86.1.1.10	LANforge	1563	Seq: 264
21234	61.63699300	86.1.1.11	86.1.1.10	LANforge	1563	Seq: 264
- Packet Details:**
 - Frame 1586: 1563 bytes on wire (12504 bits), 1563 bytes captured (12504 bits) on interface 0
 - Radiotap Header v0, Length 29
 - 802.11 radio information
 - IEEE 802.11 QoS Data, Flags:T
 - Logical-Link Control
 - Internet Protocol Version 4, Src: 86.1.1.11, Dst: 86.1.1.10
 - User Datagram Protocol, Src Port: 33003, Dst Port: 33002
 - LANforge Traffic Generator
- Packet Bytes:**

```

0000 00 00 1d 00 2b 48 08 00 b6 52 12 48 00 00 00 00 ...+H.. .R.H...
0010 00 00 3c 14 40 01 ea 00 00 00 07 04 12 88 01 30 ..<.@... ..0
0020 00 00 0e 8e 1c b7 2f 00 0e 8e 45 37 43 00 0e 8e ...../. ..E7C...
0030 fc 9e 43 b0 02 00 00 aa aa 03 00 00 00 08 00 45 ..C.... ..E
0040 00 05 dc a3 2a 40 00 40 11 e3 cf 56 01 01 0b 56 ....*@.@ ...V...V
0050 01 01 0a 80 eb 80 ea 05 c8 0e 0e 00 00 00 00 1a .....
0060 2b 3c 4d 00 02 00 01 05 9c 00 00 00 00 00 00 58 +<M.... ..X
0070 20 bc 32 10 06 66 d8 00 00 00 00 00 00 00 00 00 .2..f...
0080 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 .....
0090 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 .....

```

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](#).