;

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

WiFi: Emulating Degraded Stations

Goal: Create a scenario where WiFi stations send out corrupted packets that can cause handshake and authentication failures. Learn techniques to capture and inspect packets to view corruption and scan log files to find indications of LANforge corruption injections.

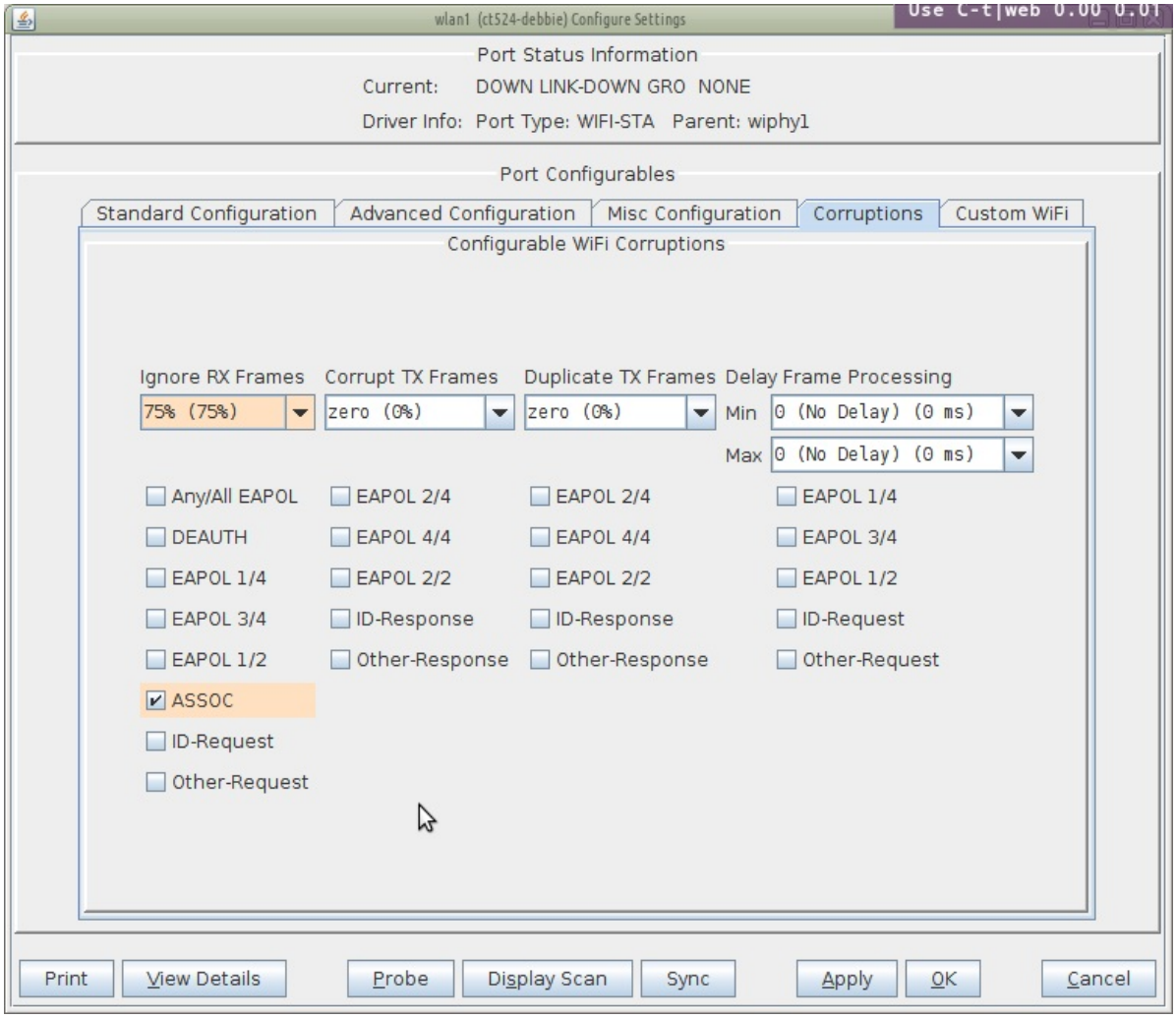
We will learn to use the some WiFi packet corruption features to emulate malfunctioning station equipment. This consists of enabling the corruption features and looking for errors when stations attempt to associate. Part of this will include capturing packets and inspecting them. This scenario requires LANforge version 5.3.6, and a two-radio LANforge system with one radio set in monitor mode.

Open Authentication Test Scenario

We will begin with a basic open authentication test scenario with a single virtual station on a LANforge system connecting to an AP. (See Also: Generating Traffic for WLAN Testing) This test scenario also works for Captive Portal testing.

Create a Station with Corruptions

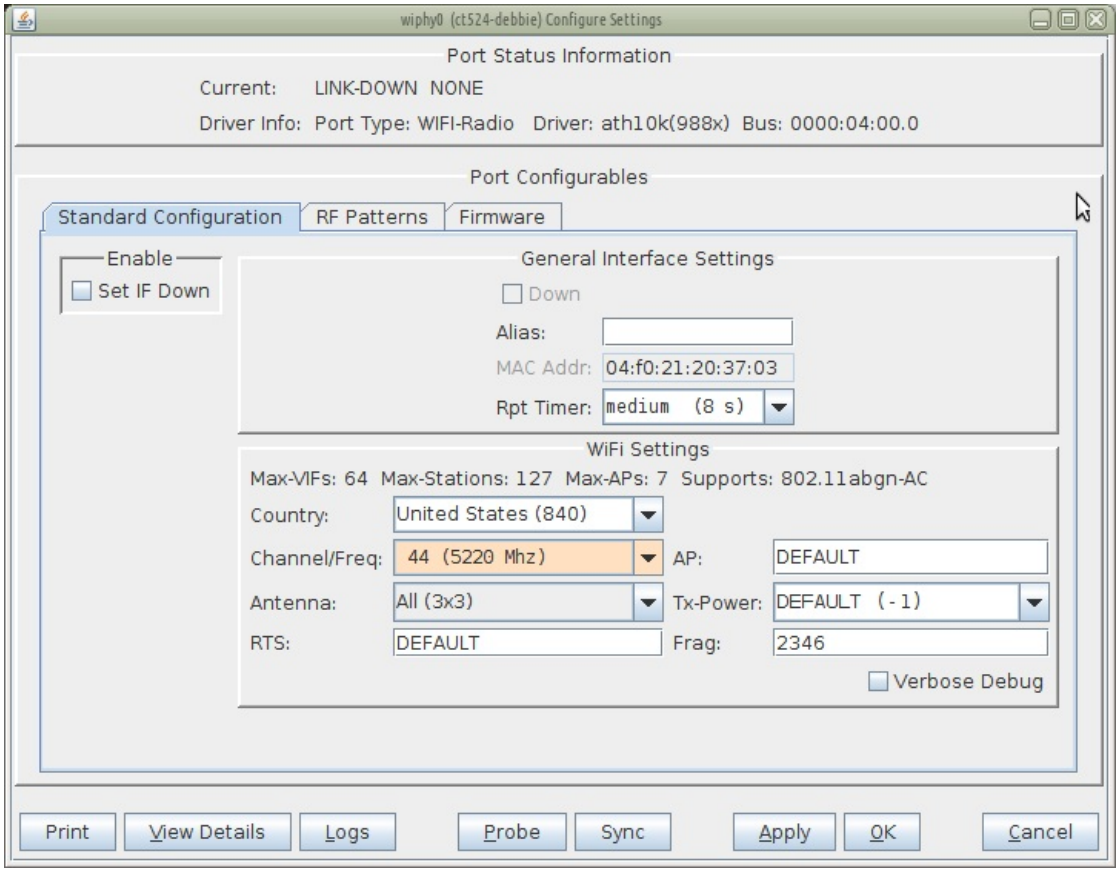
We will use the simplest form of corruption, ignored frames. Select the Port → Corruptions tab, and set Ignore RX Frames very high, like `75%`. To limit this to association frames, select **ASSOC**.



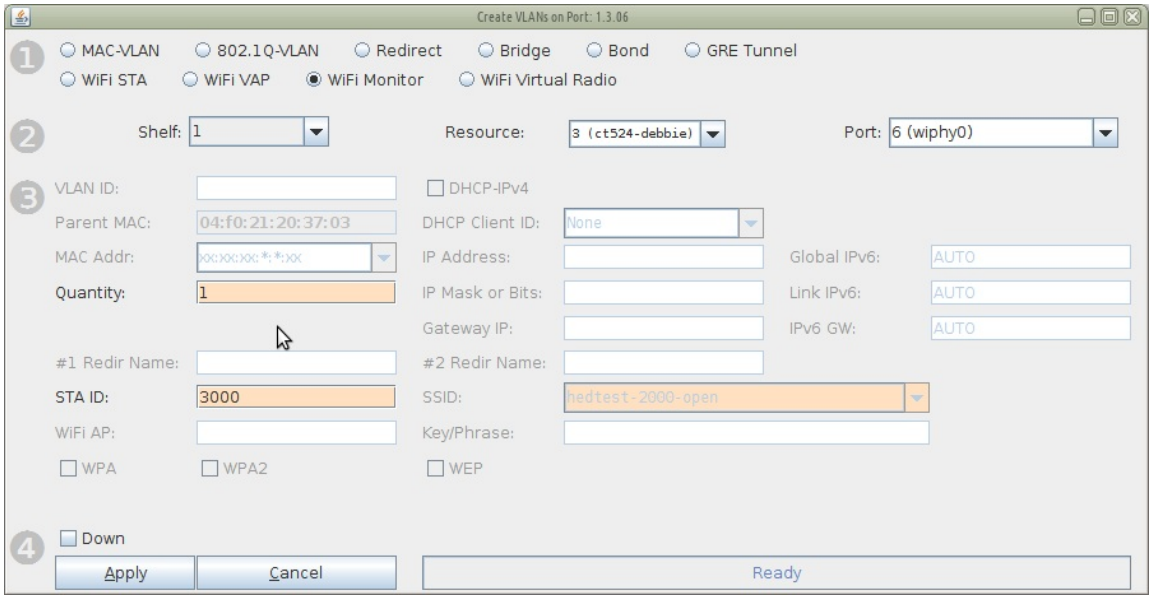
Associate a Station with Corruptions

Introducing corruptions is simple. Watching the effects takes some effort. With aggressive association corruptions, the basic effect will appear as if your station takes an unreasonably long time to associate. Let's set up Wireshark at different interfaces to understand better the kinds of traffic at play.

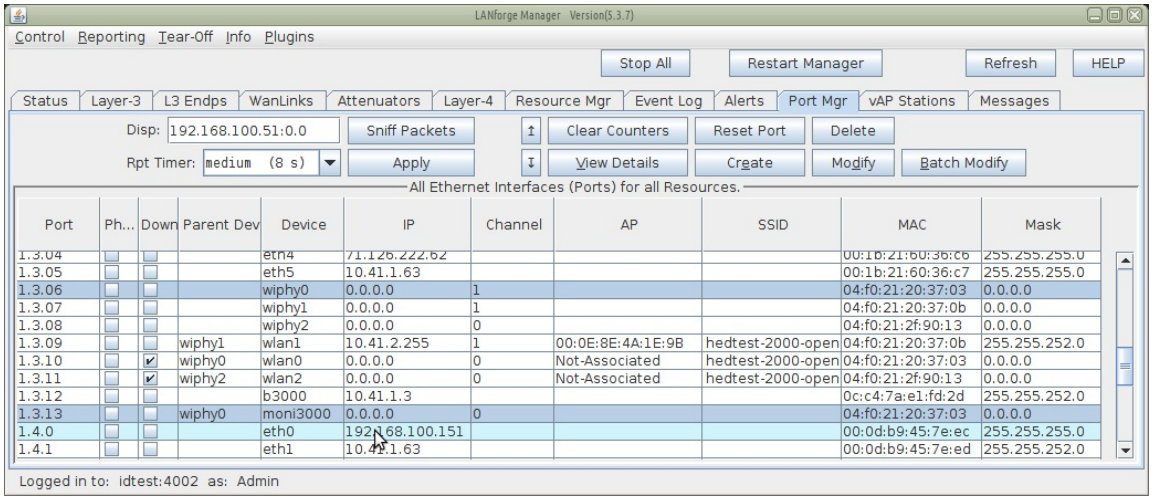
1. Select a radio for monitoring and set its channel to match the AP channel. If your AP is on channel 44, modify your LANforge wiphy monitor radio to also listen on channel 44. Our test AP is named hedtest-2000-open



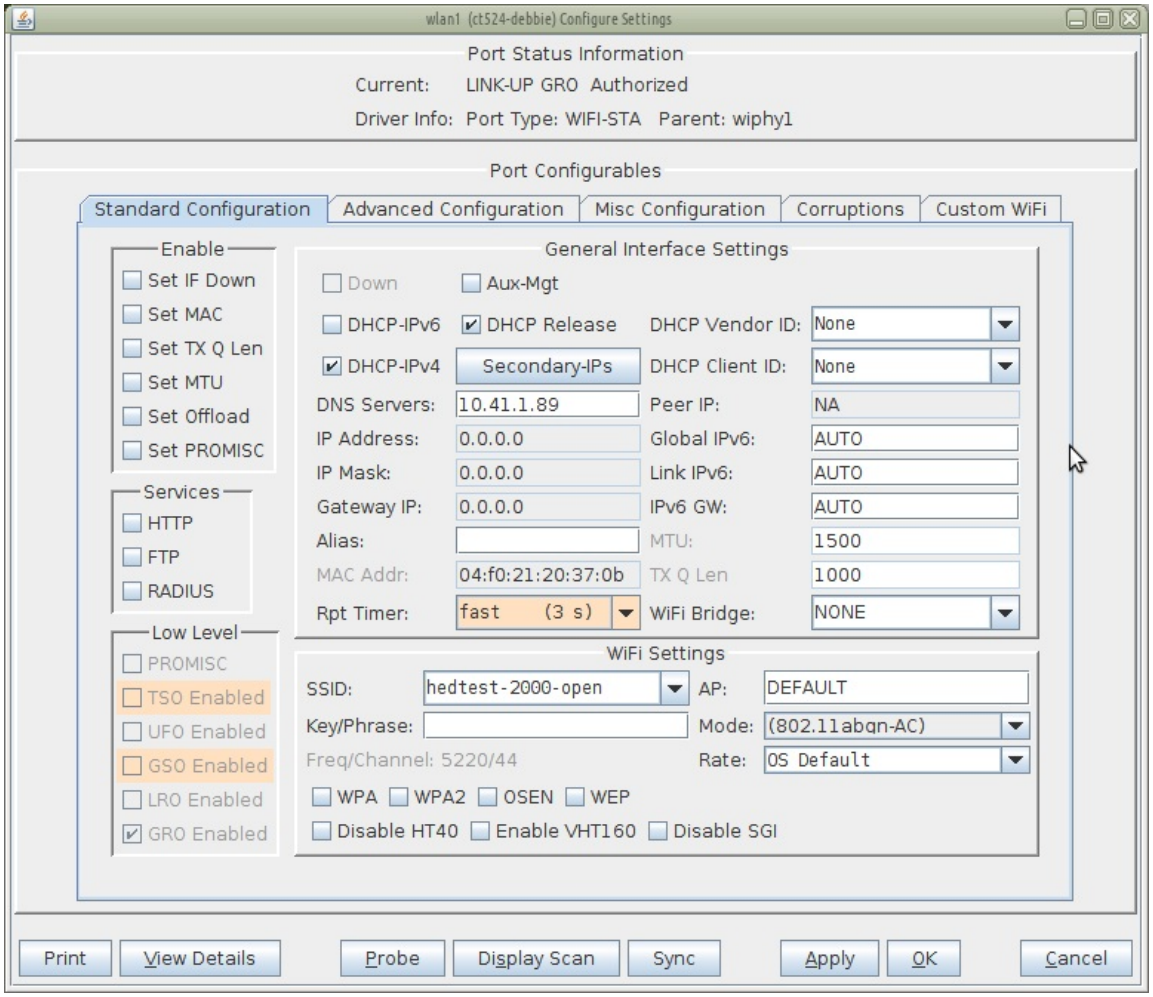
2. Create a **monitor** port (Port tab → Select Radio → Create → Monitor)



You will see the `moni3000` port below. The channel number will not display.

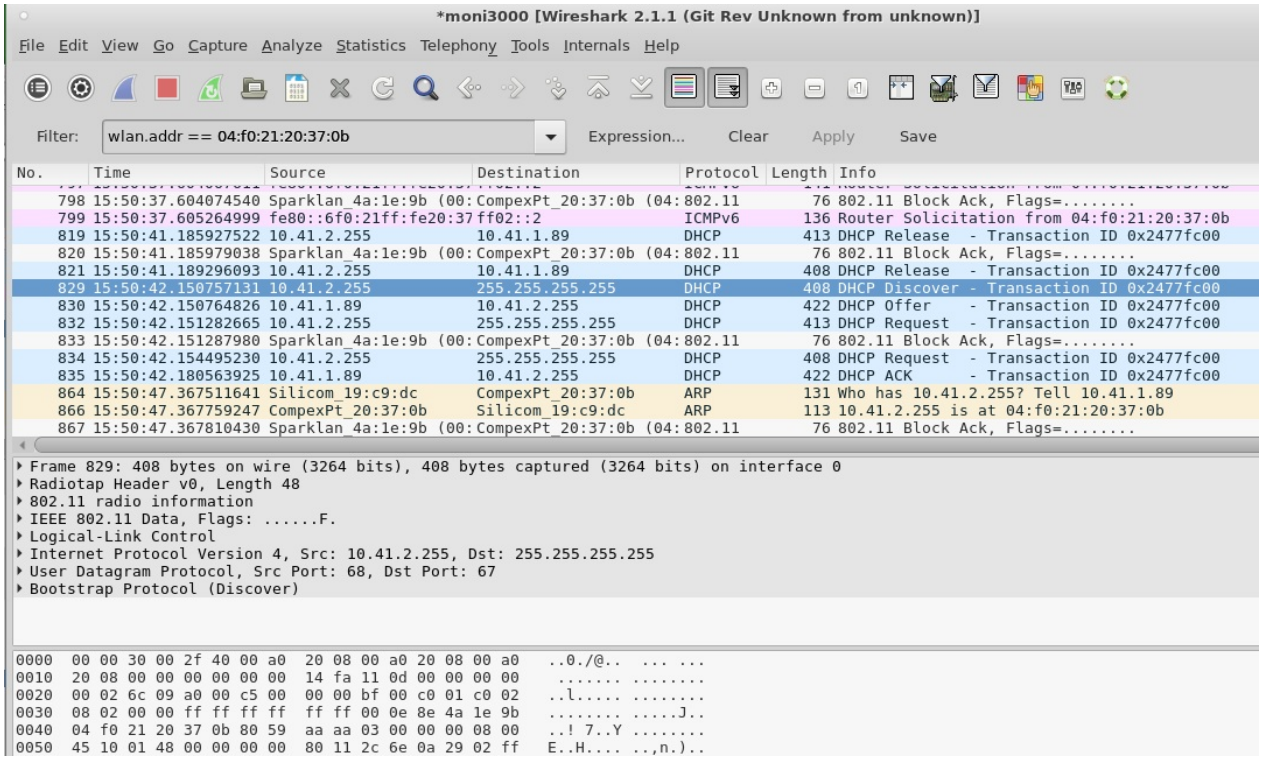


3. Create a station (wiphy1 → wlan1 will work) and associate it with hedtest-2000-open. Highlight the station in the Ports tab and bring it up.

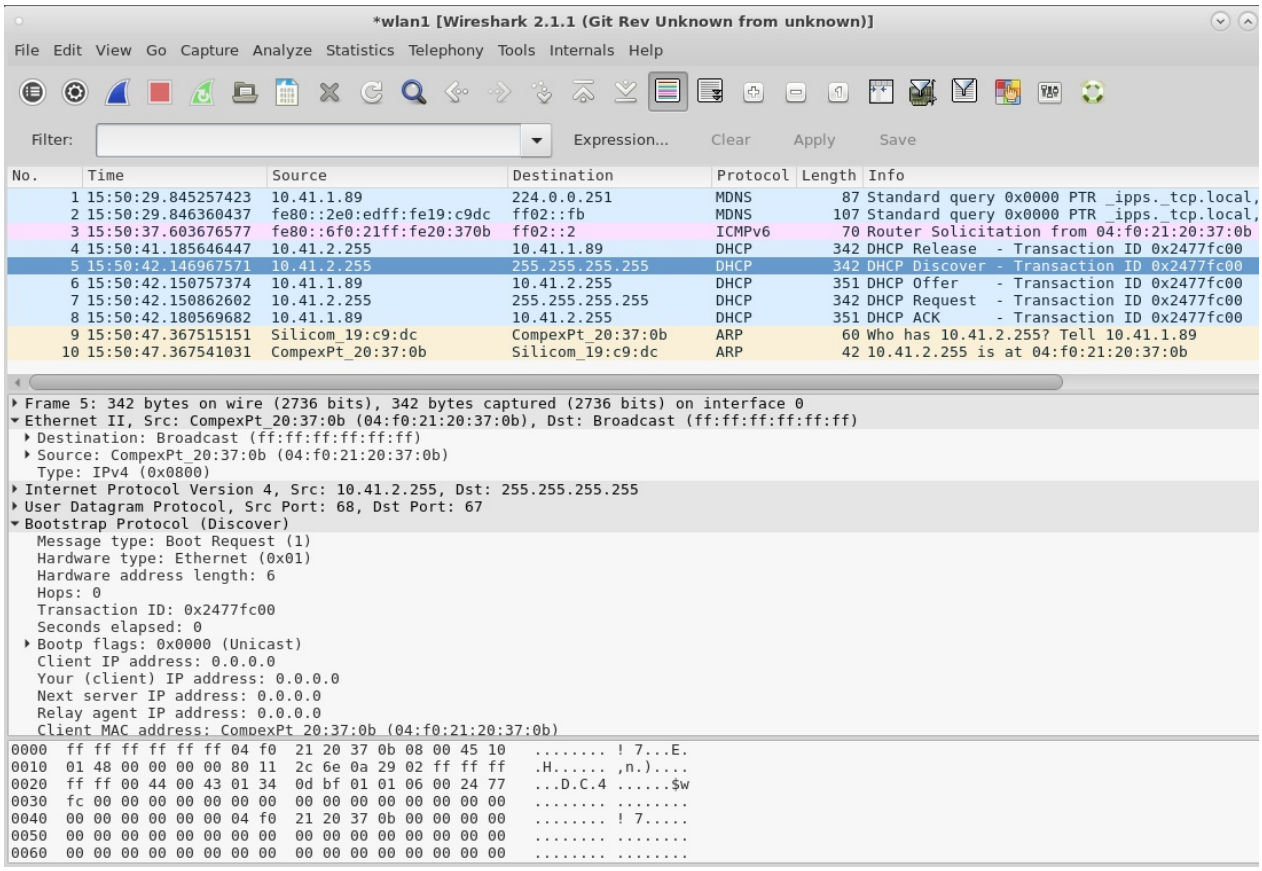


Watch Traffic

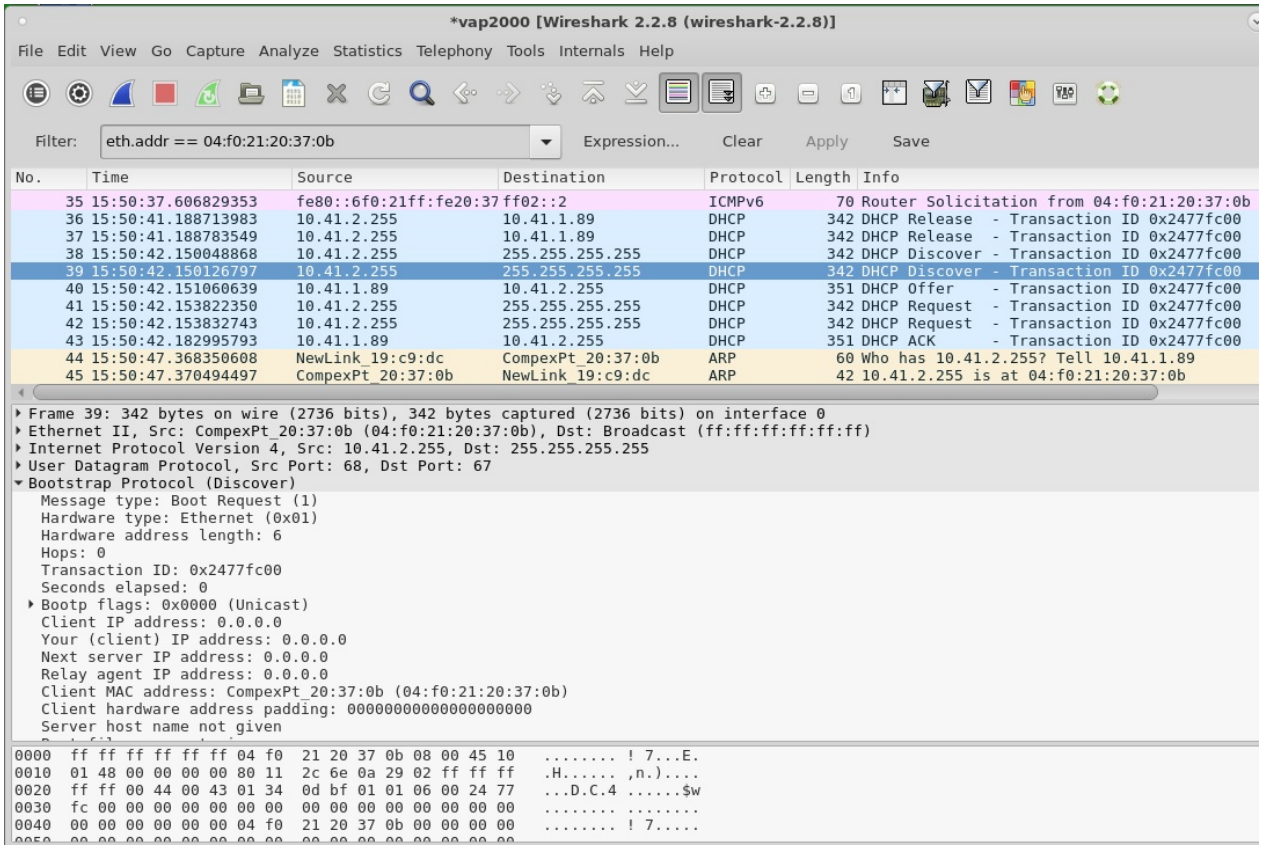
With 75% ignore the chances of the station actually associating are very port. On our monitor interface, we see that there are multiple discover and request packets.



On our station interface (wlan1), we see a different number of DHCP requests.



At our AP, we see repeated attempts.

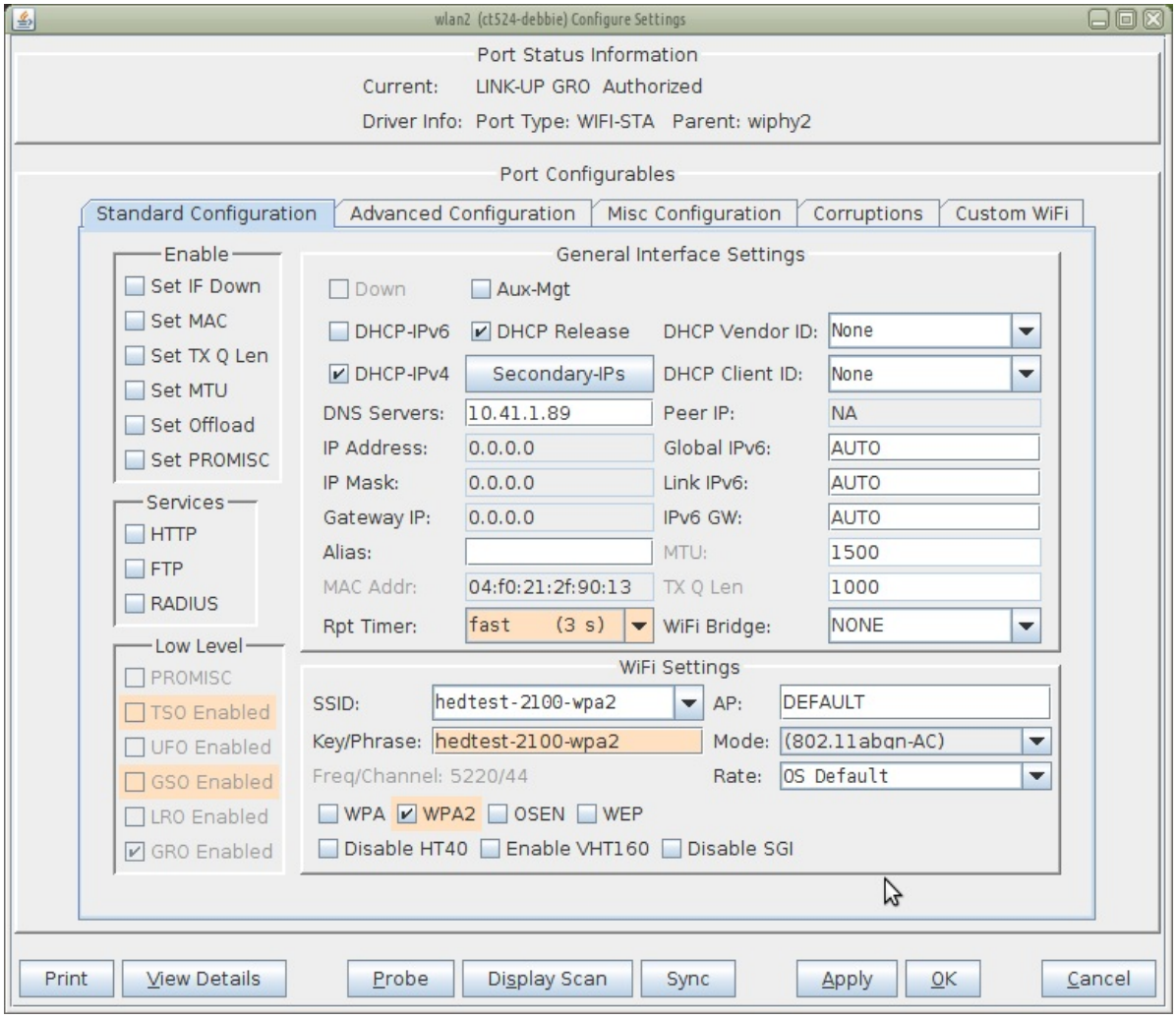


WPA2 Authentication Test Scenario

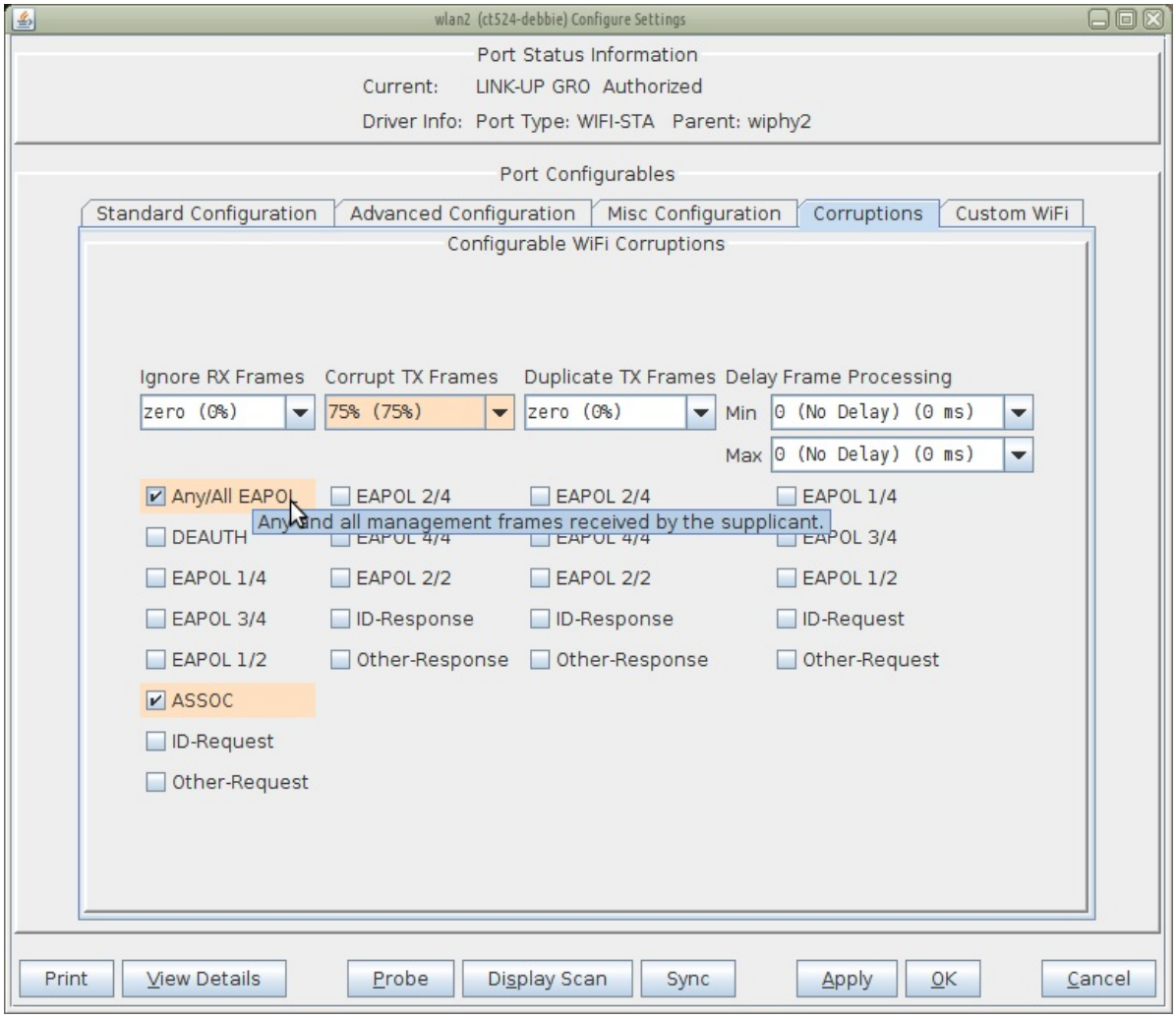
We will configure a station with WPA2 PSK encryption. We will also use Wireshark to decrypt the packets in order to see that they are corrupt.

Configure the Station

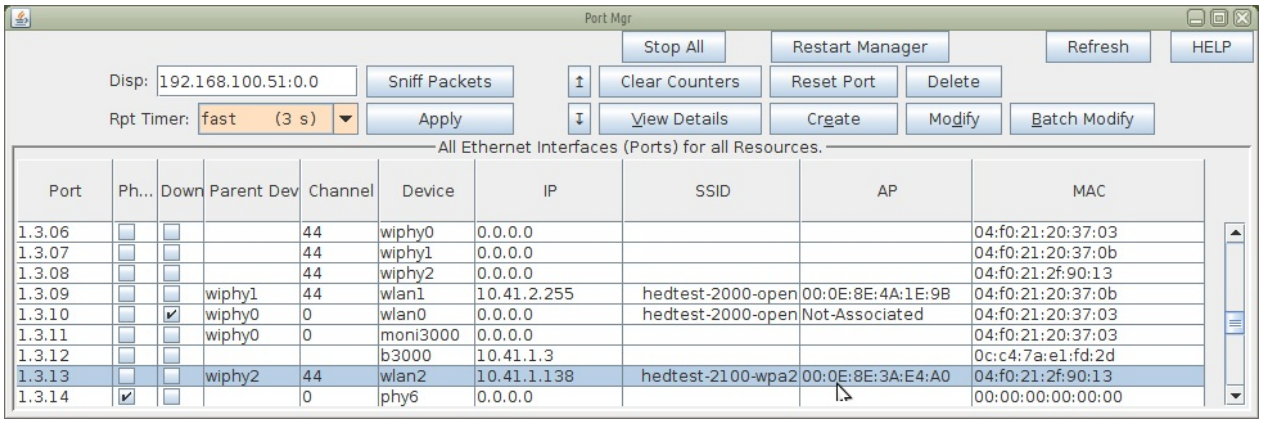
Configure station with WPA2 (See also: Test WiFi station upload throughput)



On the Corruptions tab, you can set stations:



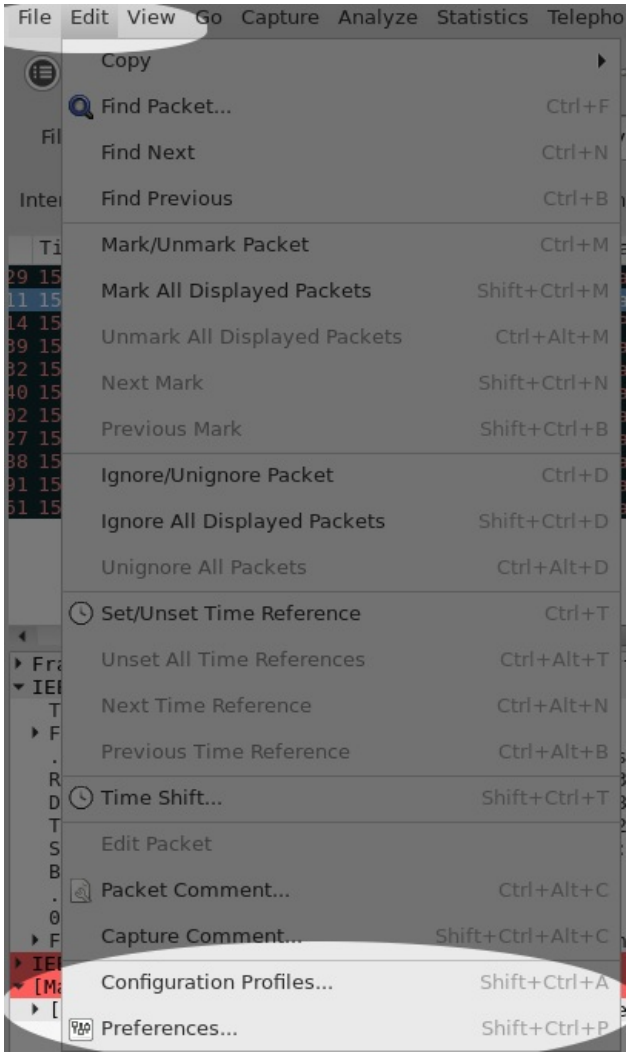
Highlight and activate the station:



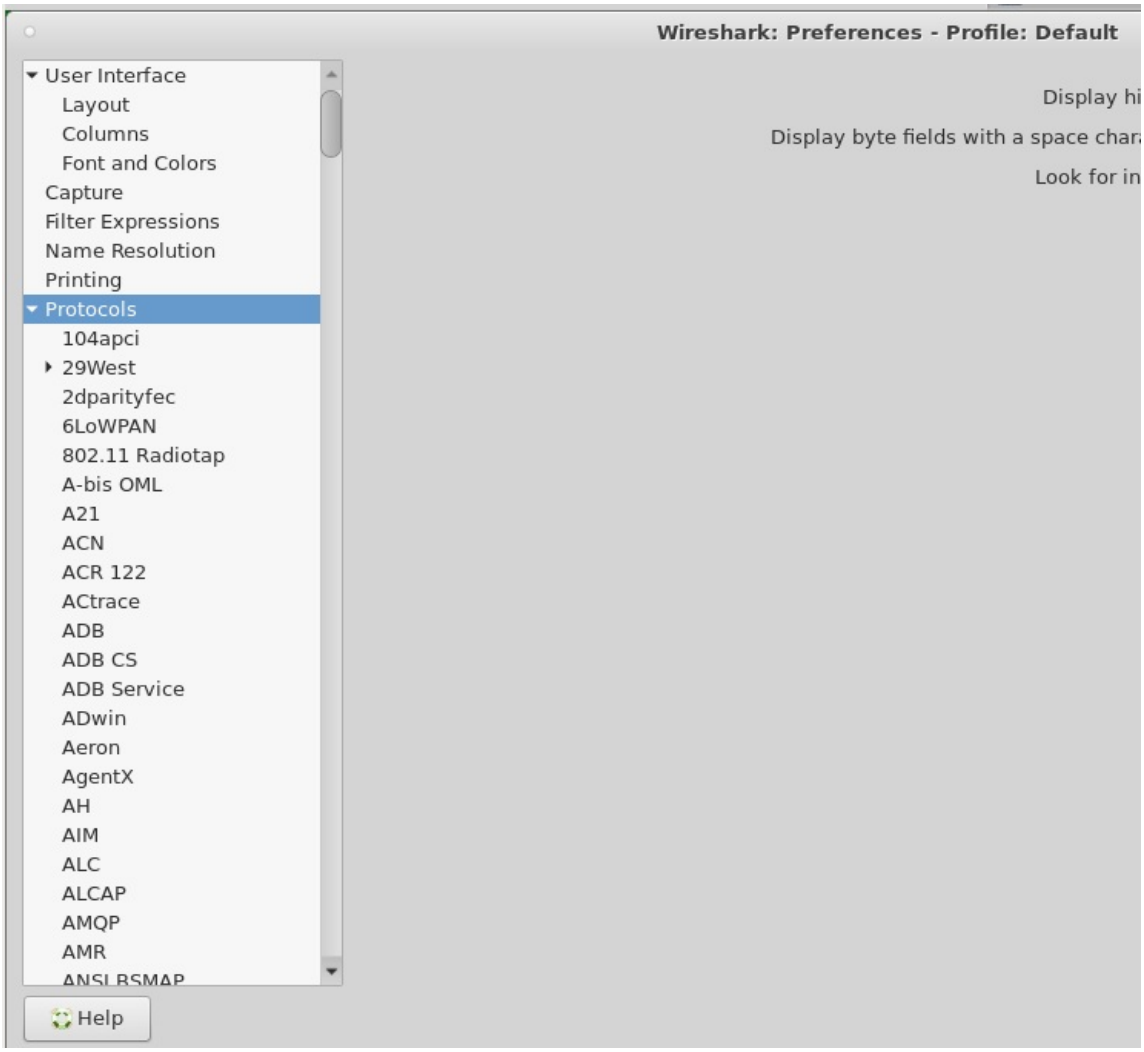
Setup Packet Decryption

We will not be able to inspect packets unless we configure Wireshark to decrypt the packets from this capture. Follow these steps:

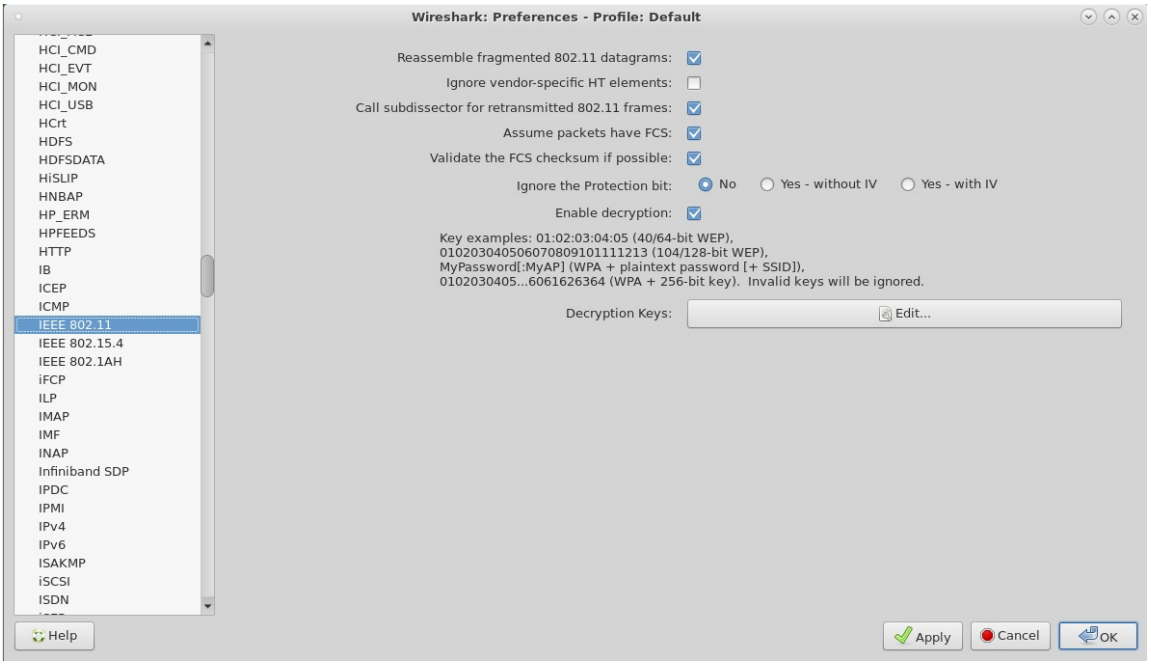
1. Wireshark Preferences (Edit → Preferences)



2. Protocol Preferences (Preferences → Protocols)



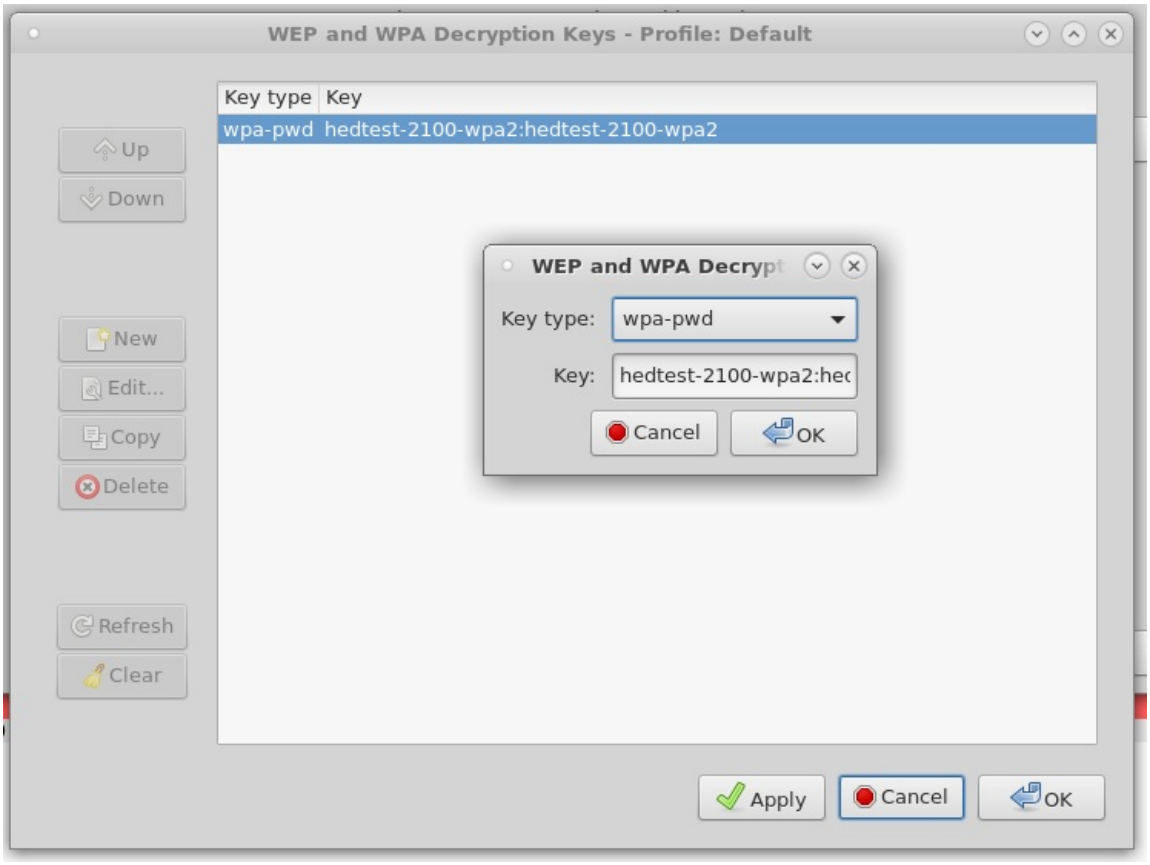
3. IEEE 802.11 Preferences (Protocols → IEEE 802.11)



- Select **Reassemble Fragmented 802.11 datagrams**
- Select **Call subdissector for retransmitted 802.11 frames**
- Select **Assume Packets have FCS**
- Select **Validate the FCS Checksum if possible**
- Select **No** for Ignore the Protection bit
- Select **Enable Decryption**

Add the SSID and password to the list of Decryption Keys. Select **wpa-pwd**: and type in the string `$SSID:$PSK` to match your password from your AP:

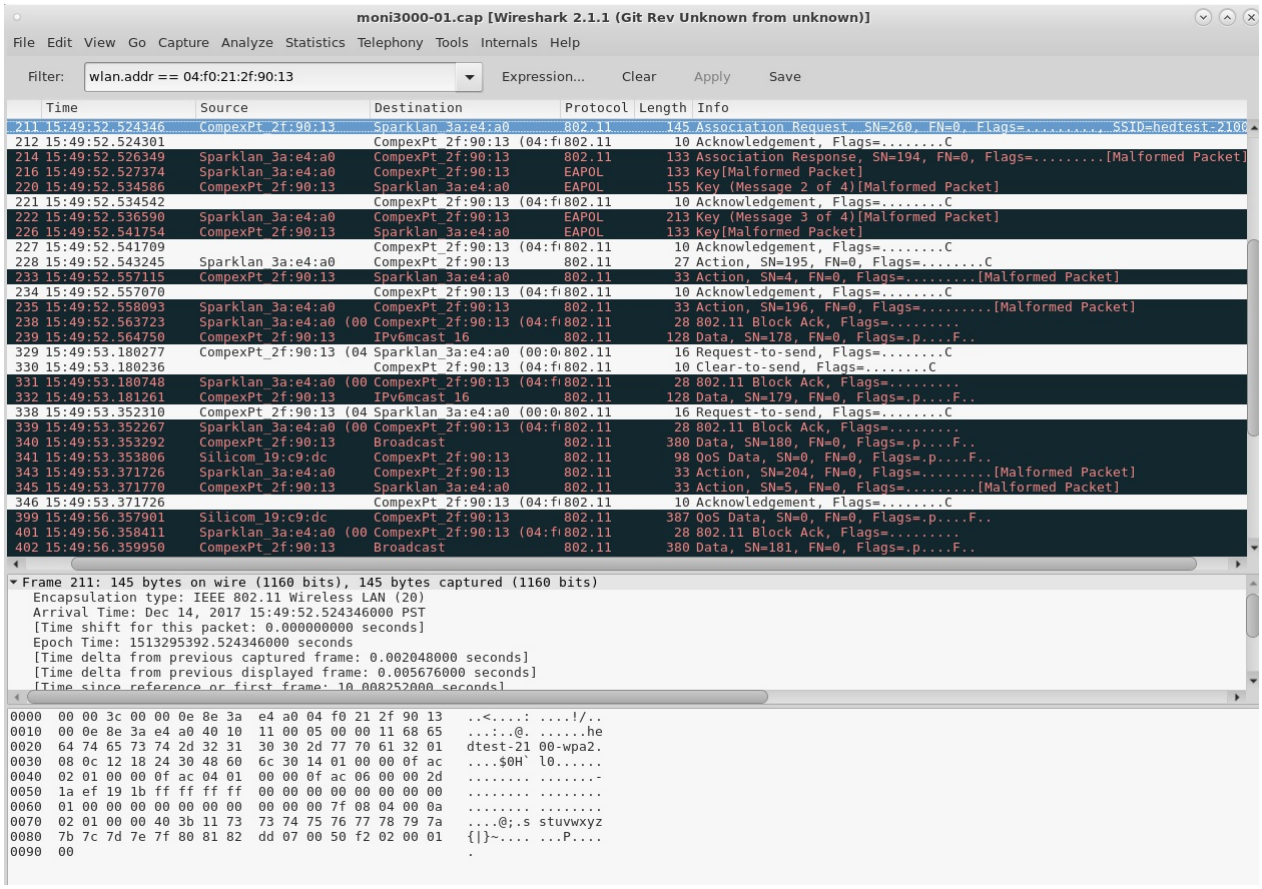
```
hedtest-2100-wpa2:hedtest-2100-wpa2
```



With our decryption enabled we can now inspect the captured packets:

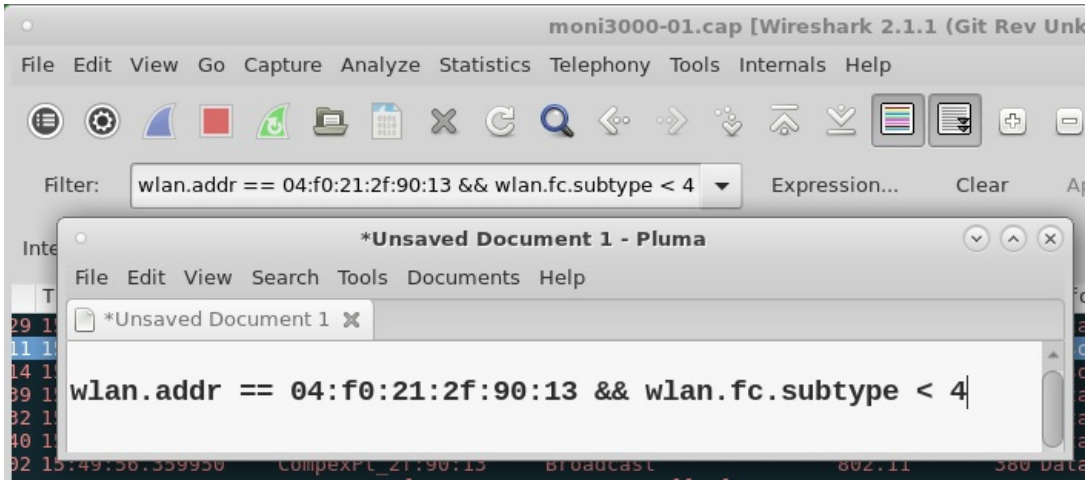
Packets from `moni3000` are filtered to show the station of interest using the display filter:

```
wlan.addr == 04:f0:21:2f:90:31
```

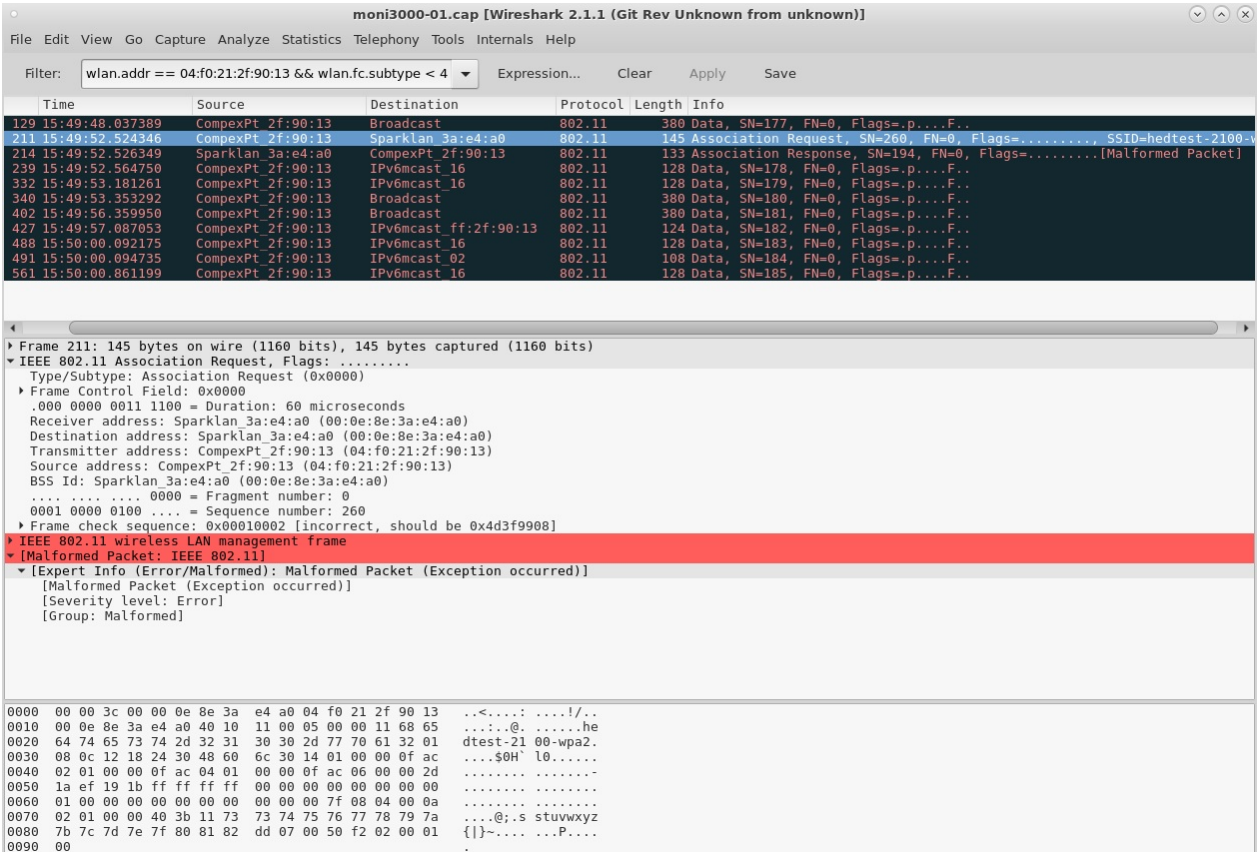


We can focus into the association by using a display filter:

```
wlan.addr == 04:f0:21:2f:90:31 && wlan.fc.subtype < 4
```



And the packets that form the association:



Notice how the AP only really gets the uncorrupted packets. What we hope will happen is that our WiFi drivers will discard corrupted packets before passing them up to userspace.

We did not need to decrypt packets from our AP (only possible if monitoring inside the AP) `vap2100:`