

NET3720 - Fall 2021 – Jenkins

Lab 3 – 802.11 Frame Capture

Erika Hernandez

Lab Objectives:

- Capture packets from the configured AP

Hardware needed:

- Cisco Aironet 3700 AP
- ZYCEL PoE Switch
- USB to RS232 cable
- Computer

Software:

- Console application
 - PuTTY <http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe>
 - Instructions on how to download PuTTY
 - <https://www.weber.edu/CS/remote-access.html>
 - Wire-shark
 - <https://www.wireshark.org/index.html#download>

Instructions:

In this lab you will learn how to configure a Cisco AP unit using the CLI. You will also learn how to capture packets from your network.

Method:

Internet is connected to the ZYXEL switch with Cat.6 cables. The switch is then connected to the Cisco AP unit with Cat.6 cables. In order to configure the AP it needs to be controlled by a computer. You are able to do this with USB to RS232 + VGA to RJ-45, green light on the AP unit means its on. Open up PuTTY and click on **Serial** then type **COM4** and then open.

Connections:

Get Cat.6 cable connect one end to modem and other to ZYXEL switch **port 5**. connect the power to the switch. Get Cat.6 cable and connect one end to **port 1** on switch and the other end to **Ethernet** port on the Cisco switch. The RJ-45 end connect to **Console** connect the VGA to RS232, then the USB to a USB port on the computer. See Figure 1 for layout of how things are connected.

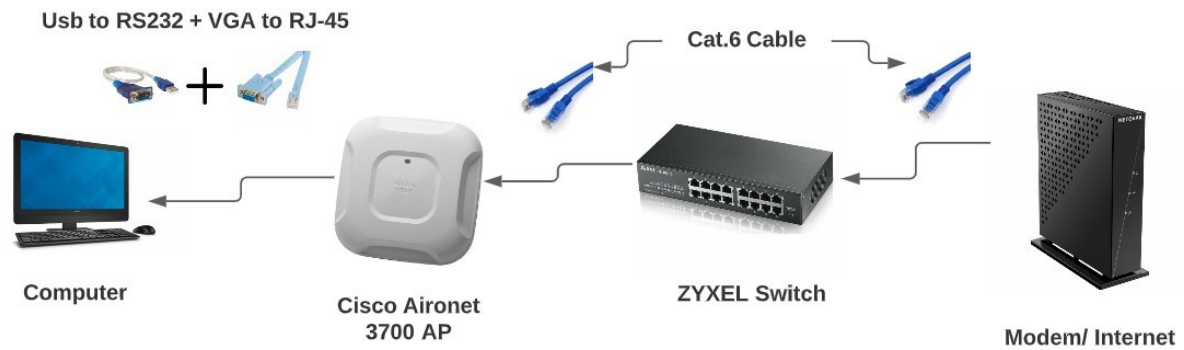


Illustration 1: Network layout

Turn on the **ZYXEL switch** on, and make sure the USB is plug and play and picks up on the computer.
 Go to the **Start** menu on your windows computer
 click on the **Device Manager**
 Go down on ports for my device it is on (**COM4**)



Figure 1: Device Manager getting ports

Open **PuTTY Configuration**

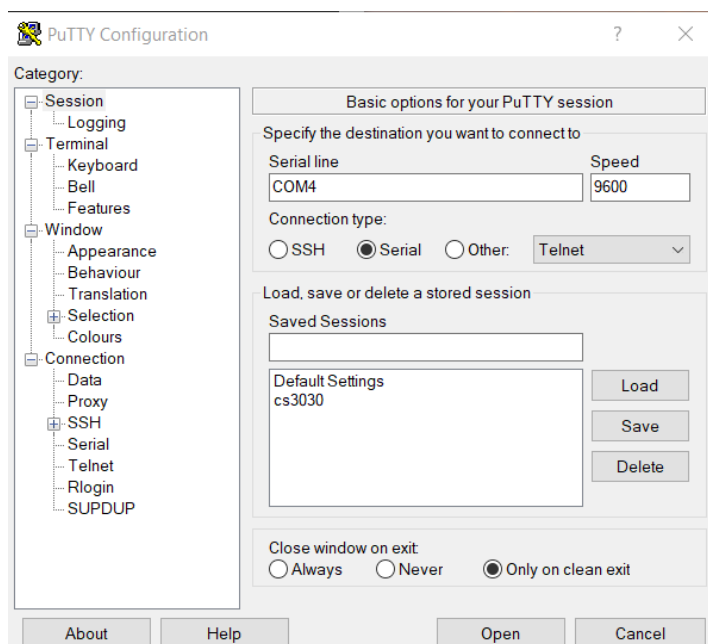


Figure 2: PuTTY- Entering COM4

Access Cisco AP
Click on **Serial**
on Serial line you put **COM4** (or whatever yours says)
Speed **9600**
Then click on **Open**

This is what will show up press **Enter**

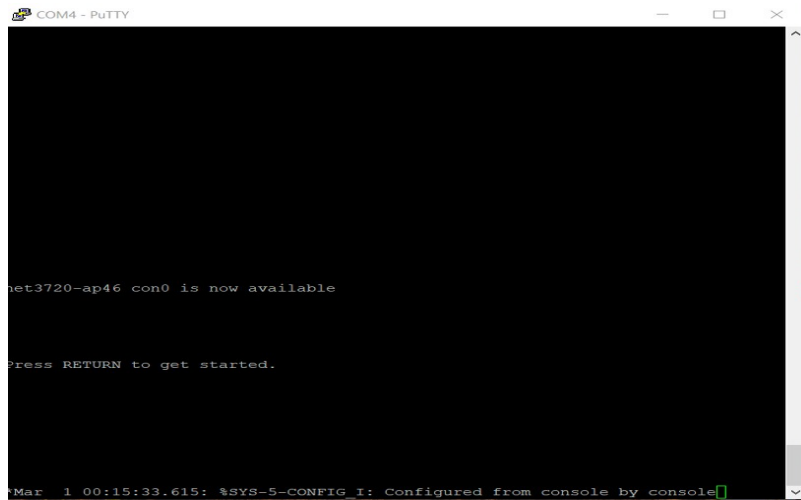


Figure 3: Start up on PuTTY

This is what will show up when you Press **Enter**

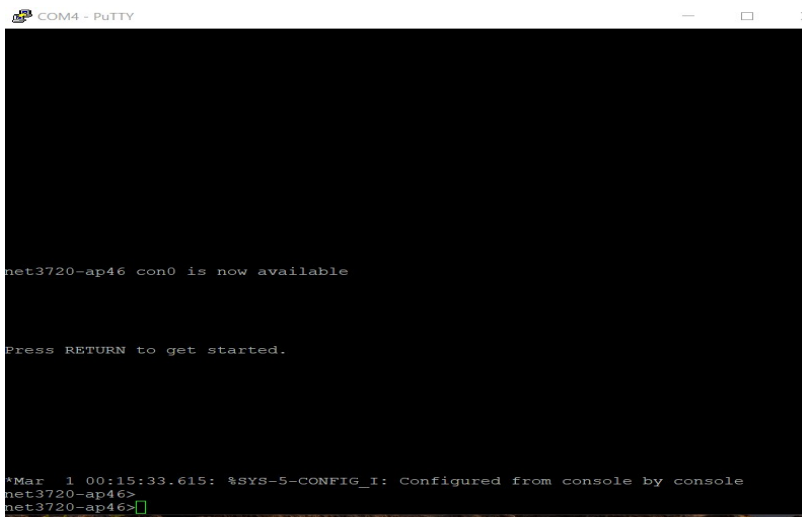


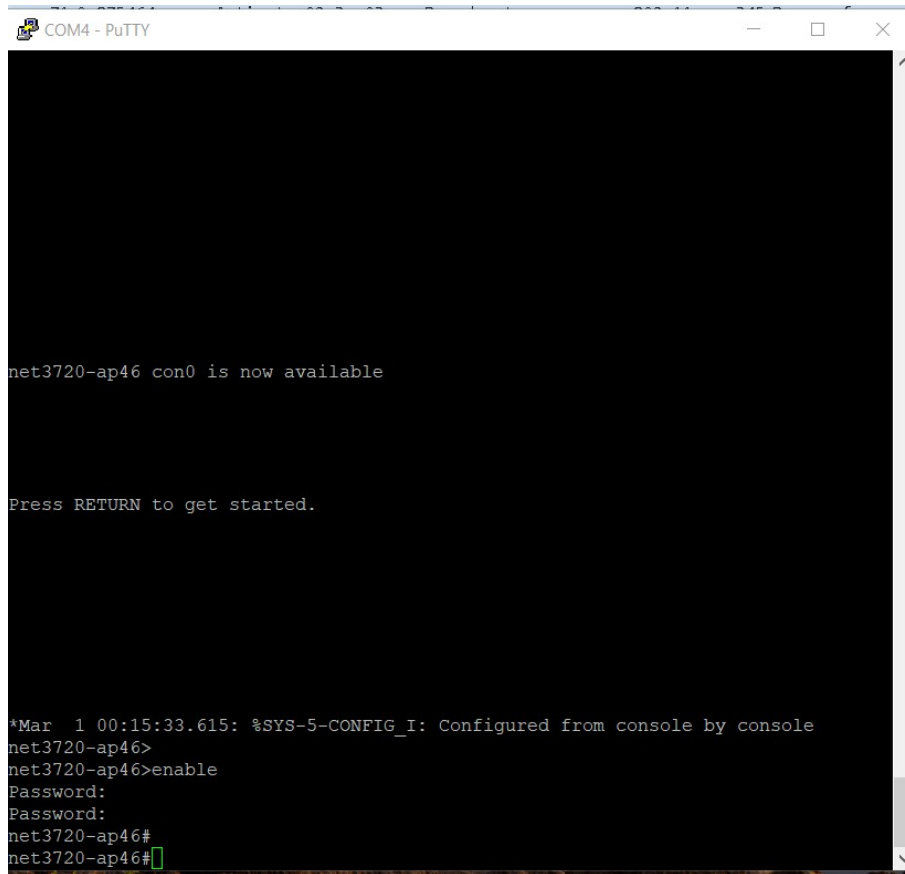
Figure 4: Press Enter and this is what it should look like

Type in password: Cisco

Then type enable

net3720-ap46> enable

password: Cisco



The screenshot shows a PuTTY terminal window titled 'COM4 - PuTTY'. The terminal output is as follows:

```
net3720-ap46 con0 is now available

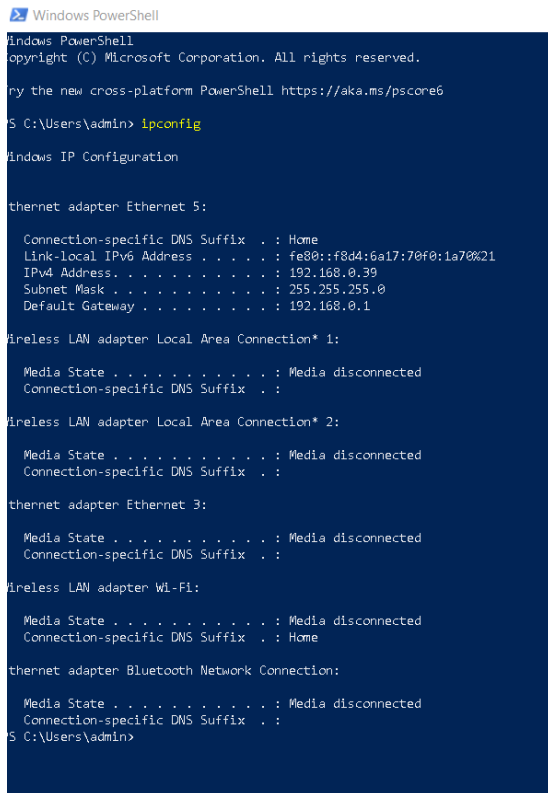
Press RETURN to get started.

*Mar  1 00:15:33.615: %SYS-5-CONFIG_I: Configured from console by console
net3720-ap46>
net3720-ap46>enable
Password:
Password:
net3720-ap46#
net3720-ap46#
```

The terminal shows the device name 'net3720-ap46' and the prompt changing from '>' to '#', indicating that the user has successfully entered the enable password and is now in configuration mode.

Figure 5: Look for the # this shows you are in configuration mode

Open PowerShell or CMD to get your IPv6 address and your default address



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

C:\Users\admin> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 5:

    Connection-specific DNS Suffix  . : Home
    Link-local IPv6 Address . . . . . : fe80::f8d4:6a17:70f0:1a70%21
    IPv4 Address. . . . . : 192.168.0.39
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter WL-Fi:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : Home

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
C:\Users\admin>
```

Figure 6: PowerShell

```
net3720-ap46#show run
Building configuration...
```

```
Current configuration : 1556 bytes
!
version 15.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname net3720-ap46
!
!
logging rate-limit console 9
enable secret 5 $1$S15Q$GxOM3JNohU0hWnUdqIYtx0
!
no aaa new-model
no ip source-route
no ip cef
!
```

```

!
!
!
dot11 pause-time 100
dot11 syslog
!
!
no ipv6 cef
!
!
username Cisco password 7 13261E010803
!
!
bridge irb
!
!
!

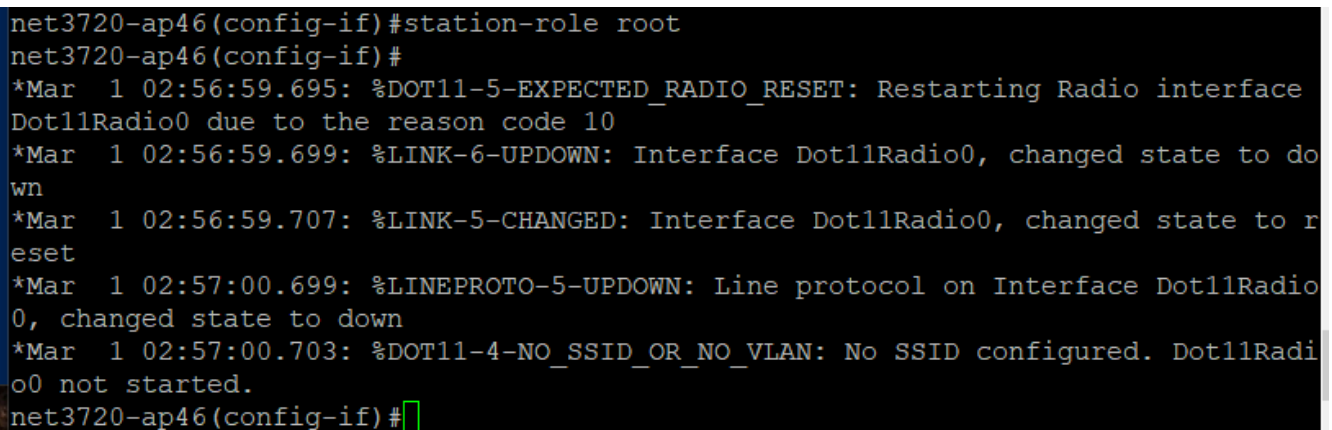
```

net3720-ap46# conf terminal

```

net3720-ap46(config)# interface Dot11Radio0
net3720-ap46(config-if)# no ip address
net3720-ap46(config-if)# shutdown
net3720-ap46(config-if)# antenna gain 0
net3720-ap46(config-if)# station-role root

```



```

net3720-ap46(config-if)#station-role root
net3720-ap46(config-if)#
*Mar  1 02:56:59.695: %DOT11-5-EXPECTED_RADIO_RESET: Restarting Radio interface
Dot11Radio0 due to the reason code 10
*Mar  1 02:56:59.699: %LINK-6-UPDOWN: Interface Dot11Radio0, changed state to do
wn
*Mar  1 02:56:59.707: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to r
eset
*Mar  1 02:57:00.699: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radi
o0, changed state to down
*Mar  1 02:57:00.703: %DOT11-4-NO_SSID_OR_NO_VLAN: No SSID configured. Dot11Radi
o0 not started.
net3720-ap46(config-if)#

```

Figure 7

```

net3720-ap46(config-if)# bridge-group 1
net3720-ap46(config-if)# bridge-group 1 subscriber-loop-control
net3720-ap46(config-if)# bridge-group 1 spanning-disabled
net3720-ap46(config-if)# bridge-group 1 block-unknown-source
net3720-ap46(config-if)# no bridge-group 1 source-learning

```

net3720-ap46(config-if)# no bridge-group 1 unicast-flooding

```
o0 not started.
net3720-ap46(config-if)#brid
net3720-ap46(config-if)#bridge-group 1
net3720-ap46(config-if)#brid
net3720-ap46(config-if)#bridge-group 1 su
net3720-ap46(config-if)#bridge-group 1 subscriber-loop-control
net3720-ap46(config-if)#bri
net3720-ap46(config-if)#bridge-group 1 sp
net3720-ap46(config-if)#bridge-group 1 spanning-disabled
net3720-ap46(config-if)#bir
net3720-ap46(config-if)#bri
net3720-ap46(config-if)#bridge-group 1 bloc
net3720-ap46(config-if)#bridge-group 1 block-unknown-source
net3720-ap46(config-if)#no br
net3720-ap46(config-if)#no bridg
net3720-ap46(config-if)#no bridge-group 1 so
net3720-ap46(config-if)#no bridge-group 1 source-learning
net3720-ap46(config-if)#no br
net3720-ap46(config-if)#no bri
net3720-ap46(config-if)#no bridge-group 1 un
net3720-ap46(config-if)#no bridge-group 1 unicast-flooding
```

Figure 8

!

```
net3720-ap46(config)# interface dot11Radio1
net3720-ap46(config-if)# no ip address
net3720-ap46(config-if)# shutdown
net3720-ap46(config-if)# antenna gain 0
```

```
net3720-ap46(config-if)#exit
net3720-ap46(config)#int
net3720-ap46(config)#interface do
net3720-ap46(config)#interface dot11Radio 1
net3720-ap46(config-if)#no ip addr
net3720-ap46(config-if)#no ip address
net3720-ap46(config-if)#shu
net3720-ap46(config-if)#shutdown
net3720-ap46(config-if)#antenna gai
net3720-ap46(config-if)#antenna gain 0
```

Figure 9

net3720-ap46(config-if)# peakdetect

```
net3720-ap46(config-if)#peakdetect
net3720-ap46(config-if)#
*Mar  1 03:09:41.767: %DOT11-5-EXPECTED_RADIO_RESET: Restarting Radio interface
Dot11Radio1 due to the reason code 40
net3720-ap46(config-if)#
```

Figure 10

```
net3720-ap46(config-if)# no dfs band block
net3720-ap46(config-if)# channel dfs
net3720-ap46(config-if)# station-role root
net3720-ap46(config-if)# bridge-group 1
net3720-ap46(config-if)# bridge-group 1 subscriber-loop-control
net3720-ap46(config-if)# bridge-group 1 spanning-disabled
net3720-ap46(config-if)# bridge-group 1 block-unknown-source
net3720-ap46(config-if)# no bridge-group 1 source-learning
net3720-ap46(config-if)# no bridge-group 1 unicast-flooding
```



```

Dot11Radio1 due to the reason code 40
net3720-ap46(config-if)#no dfs
net3720-ap46(config-if)#no dfs b
net3720-ap46(config-if)#no dfs band bloc
net3720-ap46(config-if)#no dfs band block
net3720-ap46(config-if)#chan
net3720-ap46(config-if)#channel dfs
net3720-ap46(config-if)#
*Mar  1 03:11:19.175: %DOT11-5-EXPECTED_RADIO_RESET: Restarting Radio interface
Dot11Radio1 due to the reason code 10
net3720-ap46(config-if)#station
net3720-ap46(config-if)#station-role root
net3720-ap46(config-if)#station-role root
net3720-ap46(config-if)#bridge
net3720-ap46(config-if)#bridge-group 1
net3720-ap46(config-if)#bri
net3720-ap46(config-if)#bridge-group 1
net3720-ap46(config-if)#bridge-group 1 s
net3720-ap46(config-if)#bridge-group 1 su
net3720-ap46(config-if)#bridge-group 1 subscriber-loop-control
net3720-ap46(config-if)#bri
net3720-ap46(config-if)#bridge-group 1 sp
net3720-ap46(config-if)#bridge-group 1 spanning-disabled
net3720-ap46(config-if)#brid
net3720-ap46(config-if)#bridge-group 1
net3720-ap46(config-if)#bridge-group 1 bl
net3720-ap46(config-if)#bridge-group 1 block-unknown-source
net3720-ap46(config-if)#no bri
net3720-ap46(config-if)#no bridge-group so
net3720-ap46(config-if)#no bridge-group sour
net3720-ap46(config-if)#no bridge-group 1 sou
net3720-ap46(config-if)#no bridge-group 1 source-learning
net3720-ap46(config-if)#no bri
net3720-ap46(config-if)#no bridge-group 1 un
net3720-ap46(config-if)#no bridge-group 1 unicast-flooding

```

Figure 11

```

!
net3720-ap46(config-if)# exit
net3720-ap46(config-if)# interface GigabitEthernet0
net3720-ap46(config-if)# no ip address
net3720-ap46(config-if)# duplex auto
net3720-ap46(config-if)# speed auto
net3720-ap46(config-if)# bridge-group 1
net3720-ap46(config-if)# bridge-group 1 spanning-disabled
net3720-ap46(config-if)# no bridge-group 1 source-learning

```

```

net3720-ap46(config)#interface gigabitEthernet 0
net3720-ap46(config-if)#no ip add
net3720-ap46(config-if)#no ip address
net3720-ap46(config-if)#dup
net3720-ap46(config-if)#duplex auto
net3720-ap46(config-if)#speed auto
net3720-ap46(config-if)#br
net3720-ap46(config-if)#bridge-
net3720-ap46(config-if)#bridge-group 1
net3720-ap46(config-if)#brid
net3720-ap46(config-if)#bridge-
net3720-ap46(config-if)#bridge-group 1 spa
net3720-ap46(config-if)#bridge-group 1 spanning-disabled
net3720-ap46(config-if)#no brig
net3720-ap46(config-if)#no brid
net3720-ap46(config-if)#no bridge-
net3720-ap46(config-if)#no bridge-group 1 sou
net3720-ap46(config-if)#no bridge-group 1 source-learning

```

Figure 12

```

!
net3720-ap46(config-if)# interface BVI1
net3720-ap46(config-if)# mac-address 5c83.8f44.4634
net3720-ap46(config-if)# ip address dhcp client-id GigabitEthernet0

```

```

net3720-ap46(config)#interface bvi 1
net3720-ap46(config-if)#ma
net3720-ap46(config-if)#mac-address 5c
net3720-ap46(config-if)#mac-address 5c83.8f44.4634
net3720-ap46(config-if)#ip add
net3720-ap46(config-if)#ip address dh
net3720-ap46(config-if)#ip address dhcp cl
net3720-ap46(config-if)#ip address dhcp client-id gi
net3720-ap46(config-if)#ip address dhcp client-id gigabitEthernet 0

```

Figure 13

```

net3720-ap46(config-if)# ipv6 address dhcp
net3720-ap46(config-if)# ipv6 address autoconfig
net3720-ap46(config-if)# ipv6 enable

```

```

net3720-ap46(config-if)#ipv6 address dhcp
net3720-ap46(config-if)#ipv6 address au
net3720-ap46(config-if)#ipv6 address autoconfig
net3720-ap46(config-if)#ip
net3720-ap46(config-if)#ipv6 enb
net3720-ap46(config-if)#ipv6 enba
net3720-ap46(config-if)#ipv6 enable

```

Figure 14

```

!
net3720-ap46(config-if)# exit
net3720-ap46(config)# ip forward-protocol nd
net3720-ap46(config)# no ip http server
net3720-ap46(config)# no ip http secure-server
net3720-ap46(config)# ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag

```

```

net3720-ap46(config)#
net3720-ap46(config)#no ip ht
net3720-ap46(config)#no ip http se
net3720-ap46(config)#no ip http sec
net3720-ap46(config)#no ip http secure-ser
net3720-ap46(config)#no ip http secure-server
net3720-ap46(config)#ip http he
net3720-ap46(config)#ip http help-path htt
net3720-ap46(config)#ip http help-path http
net3720-ap46(config)#$sco.com/warp/public/779/smbiz/prodconfig/help/eag
net3720-ap46(config)#

```

Figure 15

```

!
!
net3720-ap46(config)#bridge 1 route ip
!
!
!
net3720-ap46(config)#line con 0
net3720-ap46(config-line)# line vty 0 4
net3720-ap46(config-line)# login local
net3720-ap46(config-line)# transport input all

```

```

net3720-ap46(config)#bridge 1 rou
net3720-ap46(config)#bridge 1 route ip
net3720-ap46(config)#line con 0
net3720-ap46(config-line)#line vty 0 4
net3720-ap46(config-line)#login loc
net3720-ap46(config-line)#login local
net3720-ap46(config-line)#tran
net3720-ap46(config-line)#transport in
net3720-ap46(config-line)#transport input all
net3720-ap46(config-line)#

```

Figure 16

!
end

```

net3720-ap46#copy fl
net3720-ap46#copy flash:?

```

```

net3720-ap46#copy fl
net3720-ap46#copy flash:?
flash:ap3g2-k9w7-mx.153-3.JPK2  flash:config.txt
flash:config.txt.bak           flash:crashinfo_19930301-000753-UTC
flash:default-config           flash:env_vars
flash:event.log                 flash:event.r0
flash:info                     flash:private-config
flash:private-multiple-fs
net3720-ap46#copy flash:

```

Figure 17

```

flash:ap3g2-k9w7-mx.153-3.JPK2 flash:config.txt
flash:config.txt.bak           flash:crashinfo_19930301-000753-UTC
flash:default-config           flash:env_vars
flash:event.log                 flash:event.r0
flash:info                     flash:private-config
flash:private-multiple-fs

```

```

net3720-ap46#copy flash:exit
% Incomplete command.

```

```

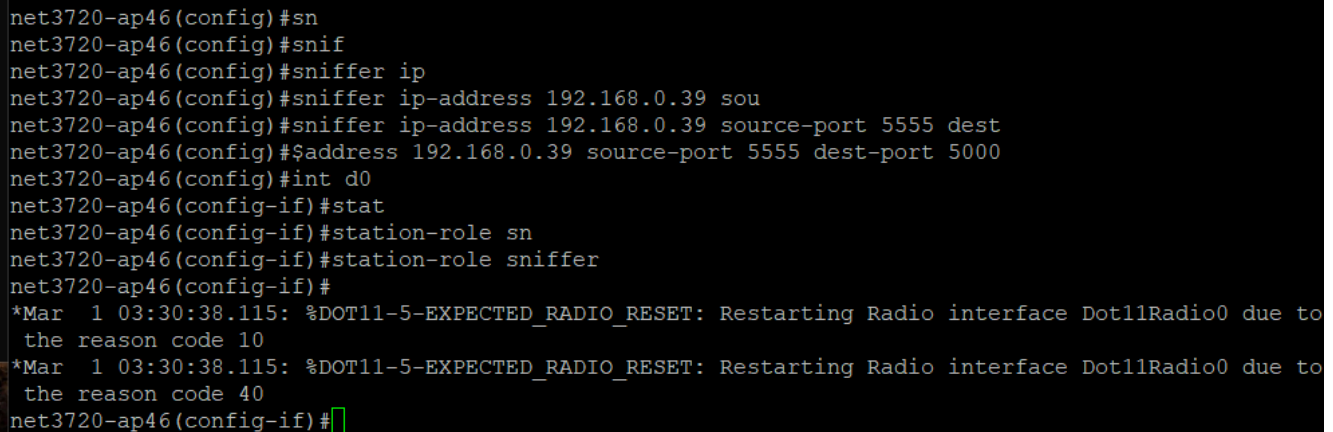
net3720-ap46#conf t
Enter configuration commands, one per line. End with CNTL/Z.c
net3720-ap46(config)#int d0
net3720-ap46(config-if)#shut

```

```

net3720-ap46(config-if)#exit
net3720-ap46(config)#snif
net3720-ap46(config)#sniffer ip
net3720-ap46(config)#sniffer ip-address 192.168.0.39 sour
net3720-ap46(config)#sniffer ip-address 192.168.0.39 source-port 5555 dest
net3720-ap46(config)#$address 192.168.0.39 source-port 5555 dest-port 5000
net3720-ap46(config)#int d0
net3720-ap46(config-if)#stat
net3720-ap46(config-if)#station-role sniffer
net3720-ap46(config-if)#
*Mar 1 00:05:12.379: %DOT11-5-EXPECTED_RADIO_RESET: Restarting Radio interface
Dot11Radio0 due to the reason code 10
*Mar 1 00:05:12.379: %DOT11-5-EXPECTED_RADIO_RESET: Restarting Radio interface
Dot11Radio0 due to the reason code 40
net3720-ap46(config-if)#
net3720-ap46(config-if)#no shut
net3720-ap46(config-if)#
*Mar 1 00:05:22.687: %DOT11-5-EXPECTED_RADIO_RESET: Restarting Radio interface
Dot11Radio0 due to the reason code 10
*Mar 1 00:05:22.691: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset
*Mar 1 00:05:23.767: %DOT11-6-FREQ_SCAN: Interface Dot11Radio0, Scanning frequencies for 24
seconds
*Mar 1 00:05:23.779: %LINK-6-UPDOWN: Interface Dot11Radio0, changed state to up
*Mar 1 00:05:24.779: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0,
changed state to up
net3720-ap46(config-if)#exit

```



```

net3720-ap46(config)#sn
net3720-ap46(config)#snif
net3720-ap46(config)#sniffer ip
net3720-ap46(config)#sniffer ip-address 192.168.0.39 sou
net3720-ap46(config)#sniffer ip-address 192.168.0.39 source-port 5555 dest
net3720-ap46(config)#$address 192.168.0.39 source-port 5555 dest-port 5000
net3720-ap46(config)#int d0
net3720-ap46(config-if)#stat
net3720-ap46(config-if)#station-role sn
net3720-ap46(config-if)#station-role sniffer
net3720-ap46(config-if)#
*Mar 1 03:30:38.115: %DOT11-5-EXPECTED_RADIO_RESET: Restarting Radio interface Dot11Radio0 due to
the reason code 10
*Mar 1 03:30:38.115: %DOT11-5-EXPECTED_RADIO_RESET: Restarting Radio interface Dot11Radio0 due to
the reason code 40
net3720-ap46(config-if)#

```

Figure 18

```

net3720-ap46(config-if)#exit
net3720-ap46#

```

Wireshark Section

Open – The application Wireshark now. For me the Ethernet5 is where I will be doing the packet trace

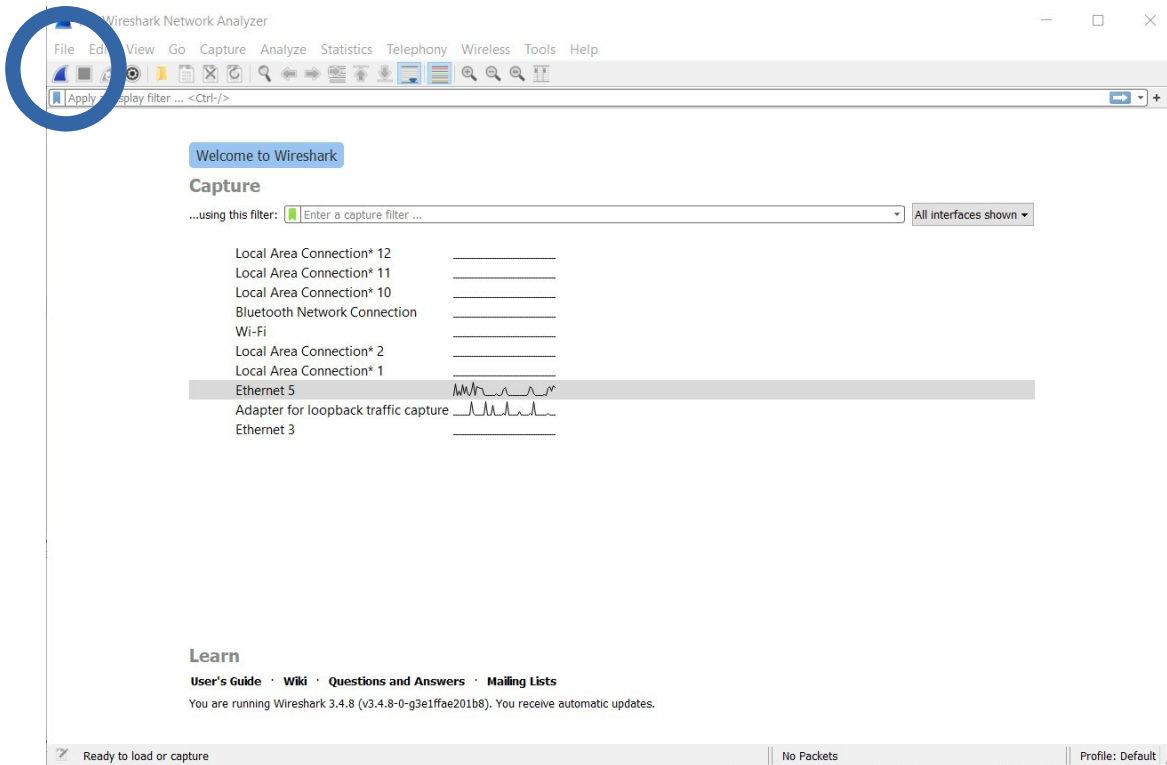


Figure 19: Wireshark- Start up

Click on the blue shark fin, o start capturing packets. Run this for about 5 minutes.

Once you have ran that for about 5 minutes click on the **red** box to stop the capturing.

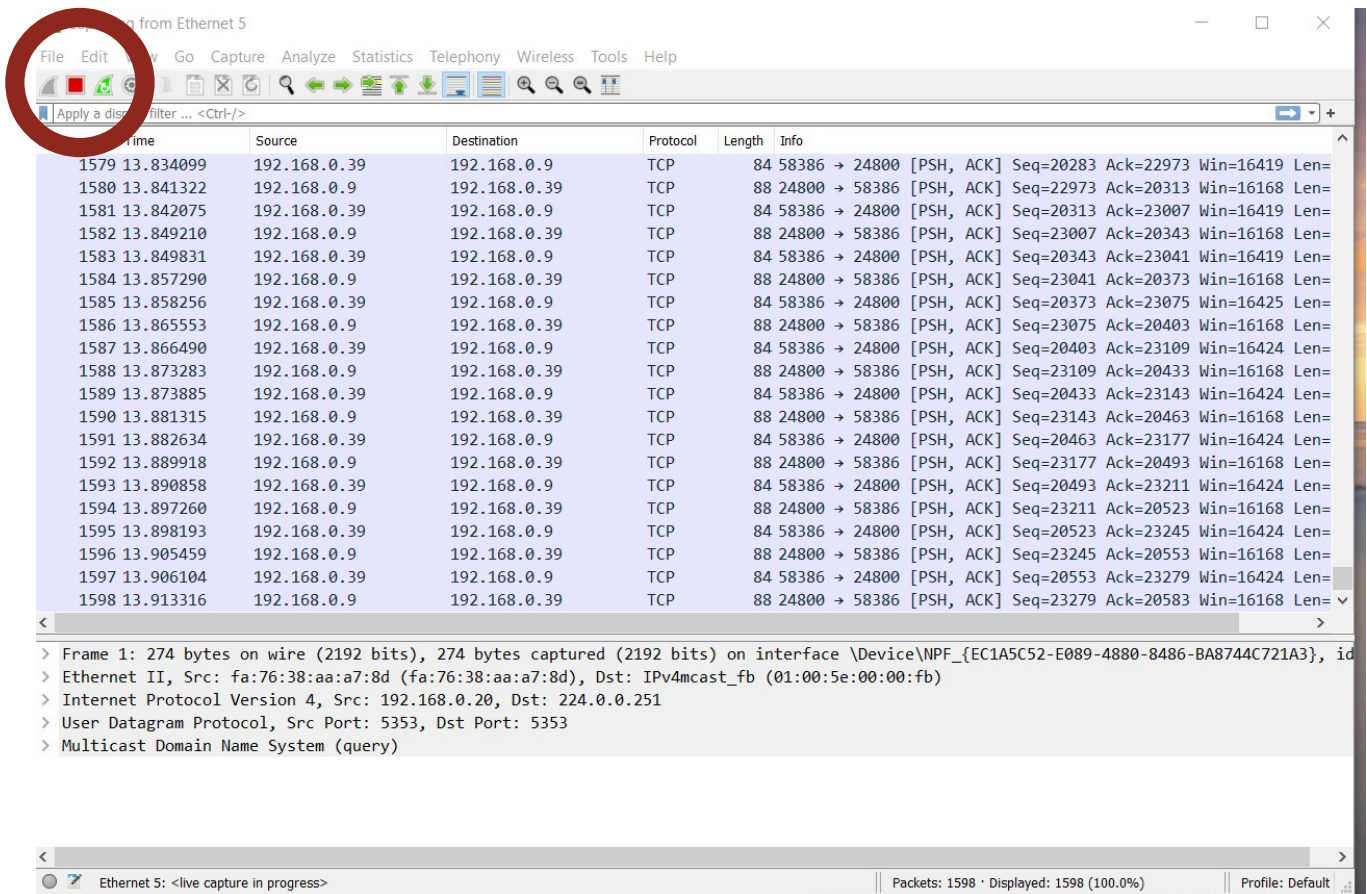


Figure 20: Wireshark- Stop button

Click on the **Analyze** tab on the top of the Wireshark.

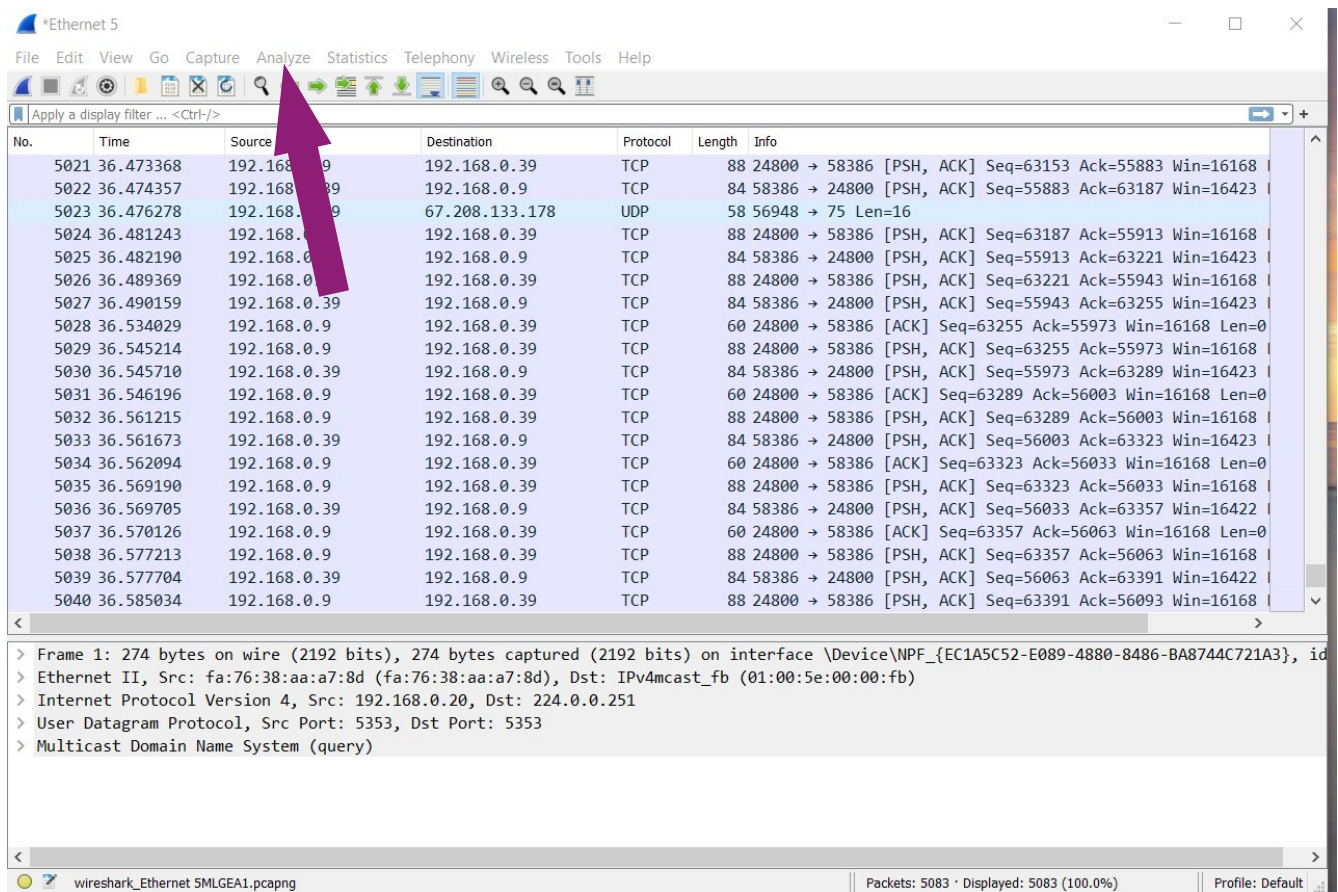


Figure 21: Wireshark- Analyze tab

Here you will see that you have port 5555 open and you are capturing you network.

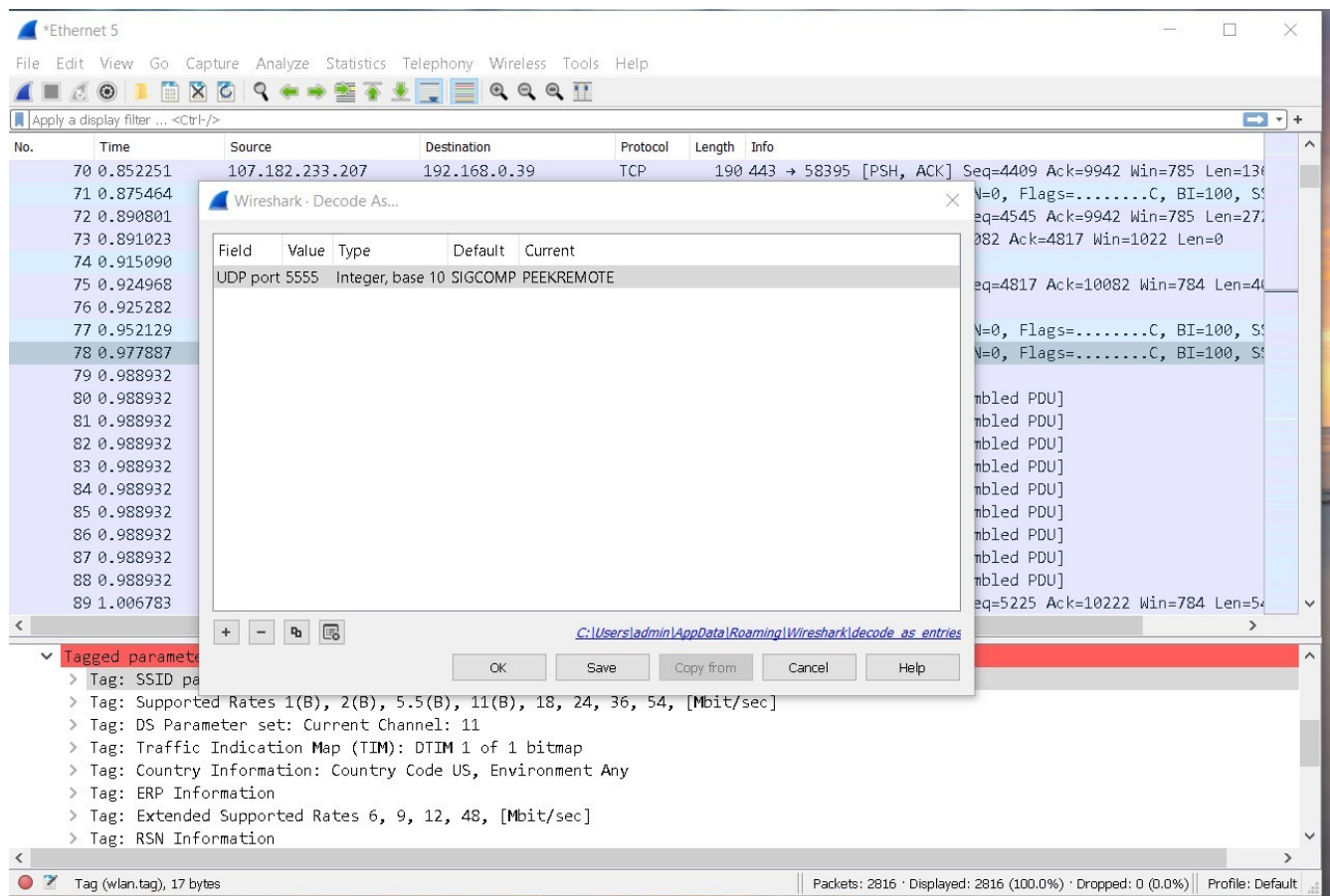


Figure 22: Wireshark- UDP port 5555

Here you will see that you have my wifi and that we are getting the 802.11 as well.

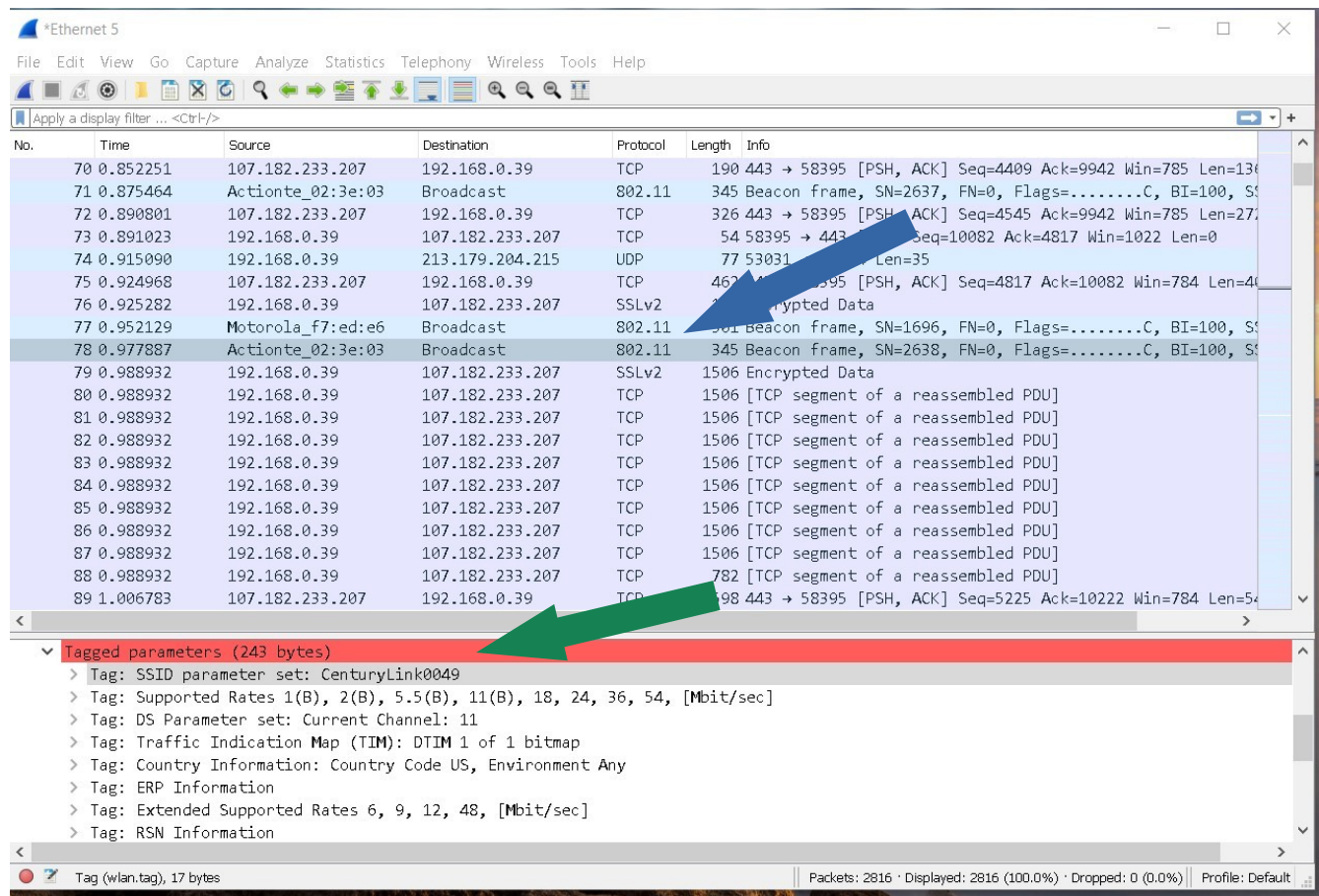


Figure 23: Wireshark- 801.11 and on my network

Here you see that SSID tag is on my network and able to get the packets.

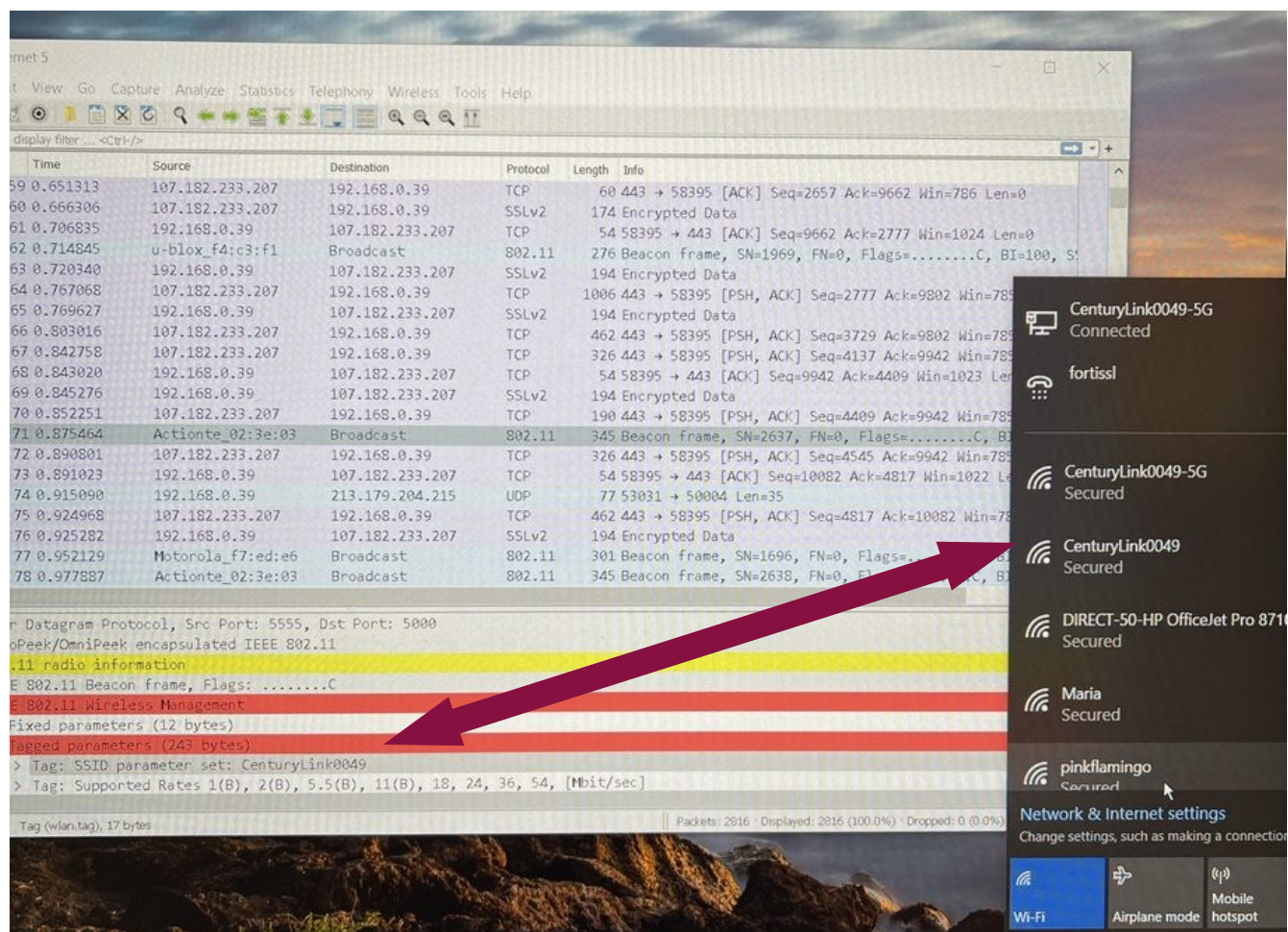


Figure 24: Wireshark - Showing up in capture

References

- IT Support People. (2020, December 29). Configure Cisco Access Point using CLI with WPAv2 Authentication [Video]. Retrieved from <https://www.youtube.com/watch?v=JkUfTXuwj2U>
- 802.11 Wlan Packets (WiFi Hacking Series Part -5) [Video]. (2013, December 16). Retrieved from <https://duckduckgo.com/?q=802.11+Frame+Capture&iax=videos&ia=videos&iai=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3Dzn5FJHua1a4>
- WiFi captures with sniffer mode AP. (2018, April 8). Retrieved from <https://mrncciew.com/2018/04/07/wifi-captures-with-sniffer-mode-ap/>