NRC7292 Evaluation Kit User Guide

(NewraPeek™)

Ultra-low power & Long-range Wi-Fi

Ver1.1
Apr 12, 2019

NEWRACOM, Inc.

NRC7292 EVK User Guide (NewraPeek™)
Ultra-low power & Long-range Wi-Fi

Office

NEWRACOM, Inc.
25361 Commercentre Drive, Lake Forest, CA 92630 USA
http://www.NEWRACOM.com

Contents

List of Tables

List of Figures

1 Introduction

NewraPeek (Newracom IEEE 802.11ah/WFA HaLow Sniffer) is a Wireshark based 802.11ah packet analyzer. The sniffer can capture network packets delivered by 802.11ah and display the details of the packet data.

NewraPeek provides stable full functions in release version 2.2.5 of Wireshark and 802.11ah packet analyzing function.

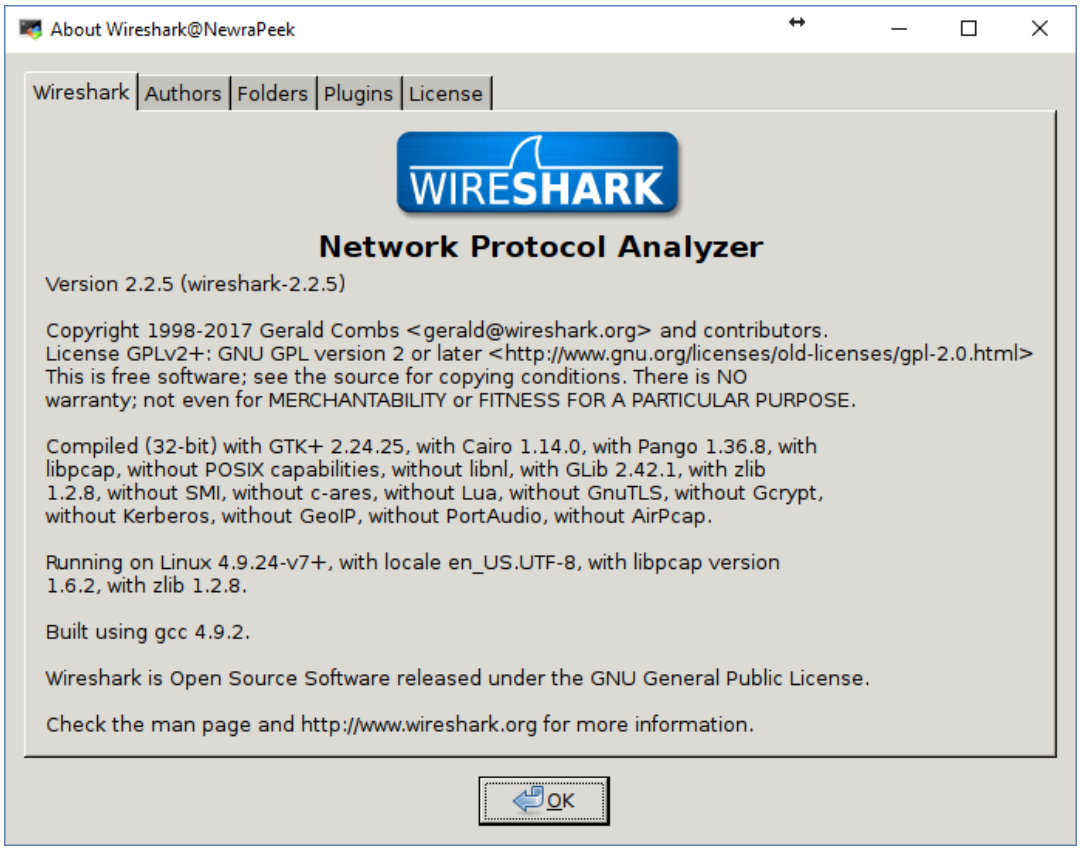


Figure 1.1 Wirehark-based NewraPeek Version Information

The following Table 1.1 shows the supported 802.11ah specific channels, frames, and information elements.

Table 1.1 Supported 802.11ah channels (US)

Country Code	Center Freq. (MHz)	1MHz		2MHz		4MHz		Supported CH # for Linux		
		Ch. Center Freq. Idx	S1G Operating Class	Ch. Center Freq. Idx	S1G Operating Class	Ch. Center Freq. Idx	S1G Operating Class			
US	902.5	1	1	2	2					
	903.5	3	1							
	904.5	5	1	6	2	8	3			
	905.5	7	1							
	906.5	9	1	10	2					
	907.5	11	1							
	908.5	**13**	1	**14**	2	**16**	3	36	153	162
	909.5	**15**	1					37		
	910.5	**17**	1	**18**	2			38	154	
	911.5	**19**	1					39		
	912.5	**21**	1	**22**	2	**24**	3	40	155	163
	913.5	**23**	1					41		
	914.5	**25**	1	**26**	2			42	156	
	915.5	**27**	1					43		
	916.5	**29**	1	**30**	2	**32**	3	44	157	164
	917.5	**31**	1					45		
	918.5	**33**	1	**34**	2			46	158	
	919.5	**35**	1					47		
	920.5	**37**	1	**38**	2	**40**	3	48	159	165
	921.5	**39**	1					149		
	922.5	**41**	1	**42**	2			150	160	
	923.5	**43**	1					151		
	924.5	**45**	1	**46**	2	48	3	152	161	
	925.5	47	1							
	926.5	49	1	50	2					
	927.5	51	1							

HaLow Test Channel
CCA Type2 Channel
Linux Channel Number

Table 1.2 Supported 802.11ah channels (JP)

Country Code	Center Freq. (MHz)	1MHz		2MHz		4MHz		Supported CH # for Linux		
		Ch. Center Freq. Idx	S1G Operating Class	Ch. Center Freq. Idx	S1G Operating Class	Ch. Center Freq. Idx	S1G Operating Class			
JP	917	1	1					36		
	918	3	1					37		
	919	5	1					38		
	920	7	1					39		
	921	9	1					40		
	922	11	1					41		
	923	13	1					42		
	924	15	1					43		
	925	17	1					44		
	926	19	1					45		
	927	21	1					46		

Table 1.3 Supported 802.11ah channels (TW)

Country Code	Center Freq. (MHz)	1MHz		2MHz		4MHz		Supported CH # for Linux		
		Ch. Center Freq.Idx	S1G Operating Class	Ch. Center Freq.Idx	S1G Operating Class	Ch. Center Freq.Idx	S1G Operating Class			
TW	839	1	1	2	2	4	4	36	149	155
	840	3	1					37		
	841	5	1	6	2			38	150	
	842	7	1					39		
	843	9	1	10	2	12	4	40	151	156
	844	11	1					41		
	845	13	1	14	2			42	152	
	846	15	1					43		
	847	17	1	18	2	20	4	44	153	157
	848	19	1					45		
	849	21	1	22	2			46	154	
	850	23	1					47		
	851	25	1					48		

Table 1.4 Supported 802.11ah channels (KR)

Country Code	Center Freq. (MHz)	1MHz		2MHz		4MHz		Supported CH # for Linux		
		Ch. Center Freq.Idx	S1G Operating Class	Ch. Center Freq.Idx	S1G Operating Class	Ch. Center Freq.Idx	S1G Operating Class			
KR	**918**	**1**	1	**2**	2			36	42	
	919	**3**	1					37		
	920	**5**	1	**6**	2	**4**	4	38	43	45
	921	**7**	1					39		
	922	**9**	1	**10**	2			40	44	
	923	**11**	1					41		
	942.8	**21**	1	**22**	2	**24**	4	46	150	152
	943.8	**23**	1					47		
	944.8	**25**	1	**26**	2			48	151	
	945.8	**27**	1					149		

Table 1.5 Supported 802.11ah channels (EU)

Country Code	Center Freq. (MHz)	1MHz		2MHz		4MHz		Supported CH # for Linux		
		Ch. Center Freq.Idx	S1G Operating Class	Ch. Center Freq.Idx	S1G Operating Class	Ch. Center Freq.Idx	S1G Operating Class			
EU	**863.5**	**1**	1	**2**	2			36	41	
	864.5	**3**	1					37		
	865.5	**5**	1	**6**	2			38	42	
	866.5	**7**	1					39		
	867.5	**9**	1					40		

Table 1.6 Supported 802.11ah channels (CN 775 ~ 779MHz)

Country Code	Center Freq. (MHz)	1MHz		2MHz		4MHz		Supported CH # for Linux		
		Ch. Center Freq.Idx	S1G Operating Class	Ch. Center Freq.Idx	S1G Operating Class	Ch. Center Freq.Idx	S1G Operating Class			
CN	**755.5**	**1**	1					36		
	756.5	**3**	1					37		
	757.5	**5**	1					38		
	758.5	**7**	1					39		
	759.5	**9**	1					40		
	760.5	**11**	1					41		
	761.5	**13**	1					42		
	762.5	**15**	1					43		
	763.5	**17**	1					44		
	764.5	**19**	1					45		
	765.5	**21**	1					46		
	766.5	**23**	1					47		
	767.5	**25**	1					48		
	768.5	**27**	1					149		
	769.5	**29**	1					150		
	770.5	**31**	1					151		

Table 1.7 Supported 802.11ah channels (CN 779 ~ 787MHz)

Country Code	Center Freq. (MHz)	1MHz		2MHz		4MHz		Supported CH # for Linux		
		Ch. Center Freq.Idx	S1G Operating Class	Ch. Center Freq.Idx	S1G Operating Class	Ch. Center Freq.Idx	S1G Operating Class			
CN	**779.5**	**1**	1	2	2	**4**	4	152	160	164
	780.5	**3**	1					153		
	781.5	**5**	1	**6**	2			154	161	
	782.5	**7**	1					155		
	783.5	**9**	1	**10**	2	**12**	4	156	162	165
	784.5	**11**	1					157		
	785.5	**13**	1	14	2			158	163	
	786.5	**15**	1					159		

Table 1.8 Supported 802.11ah specific frames

Frame Category	Frame	NewraPeek Supportness
Control	TACK	Yes
Extension	S1G Beacon	Yes

Reference: 9.2 MAC frame formats of IEEE P802.11ah-2016

Table 1.9 Supported 802.11ah specific element IDs

802.11ah specific element	Element ID	NewraPeek Supportness
S1G Open-Loop Link Margin Index	207	Yes
RPS	**208**	**Yes**
Page Slice	209	Yes
AID Request	**210**	**Yes**
AID Response	211	Yes
S1G Sector Operation	**212**	**No**
S1G Beacon Compatibility	213	Yes
Short Beacon Interval	**214**	**Yes**
Change Sequence	215	Yes
TWT	**216**	**Yes**
S1G Capabilities	217	Yes
Subchannel Selective Transmission	**220**	**Yes**
Authentication Control	222	Yes
TSF Timer Accuracy	**223**	**Yes**
S1G Relay	224	Yes
Reachable Address	**225**	**Yes**
S1G Relay Discovery	226	Yes
AID Announcement	**228**	**Yes**
PV1 Probe Response Option	229	No
EL Operation	**230**	**Yes**
Sectorized Group ID List	231	Yes
S1G Operation	**232**	**Yes**
Header Compression	233	Yes
SST Operation	**234**	**Yes**
MAD	235	Yes
S1G Relay Activation	**236**	**Yes**

Reference: Table 9-77 of IEEE P802.11ah-2016

2 Configuration

In this section, detailed configuration procedure is described.

2.1 SW Prerequisites

SSH and VNC can be used to connect sniffer device. The followings show the procedures to install XTerm SW and VNC viewer on Windows OS for free. You can use other SW that supports the same functions.

2.1.1 Install MobaXterm and VNC Viewer for Remote Control

Download and install MobaXterm from https://mobaxterm.mobatek.net/download.html.

After running MobaXterm, create SSH session with following IP address and username.

- IP address: 192.168.100.120

  (You can change IP address after the NewraPeek initialization.)
- Username: pi
- Password: raspberry (enter later)

Example screen shot is shown in following figure below.

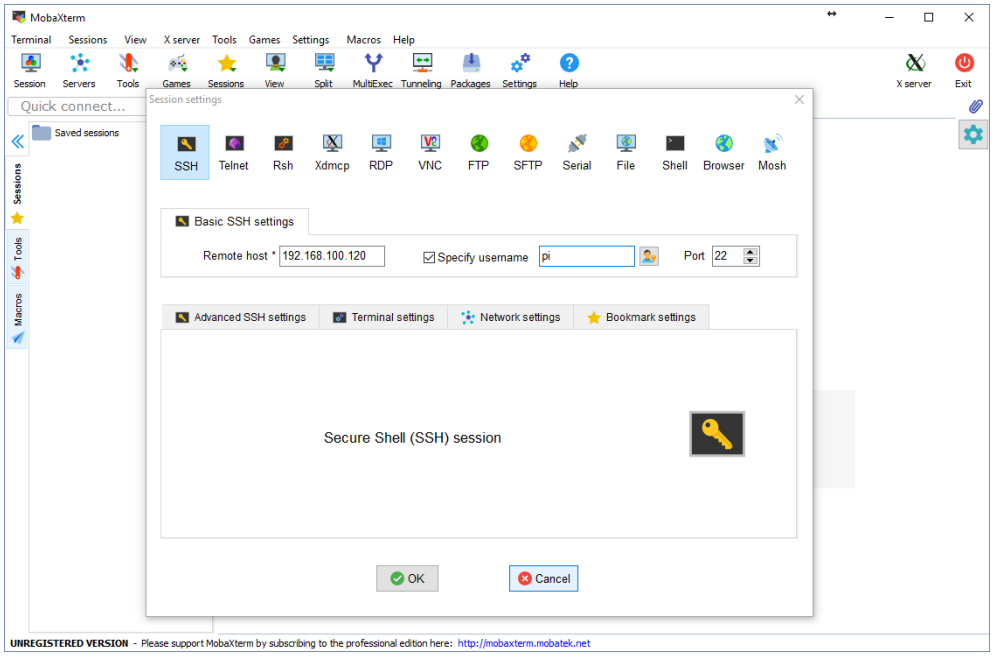


Figure 2.1 MobaXterm SSH Configuration

After creating SSH session and connecting to sniffer device, the window in the figure below will be displayed to user. If you want to control sniffer device via SSH, please check if 'X11_forwarding' is enabled.

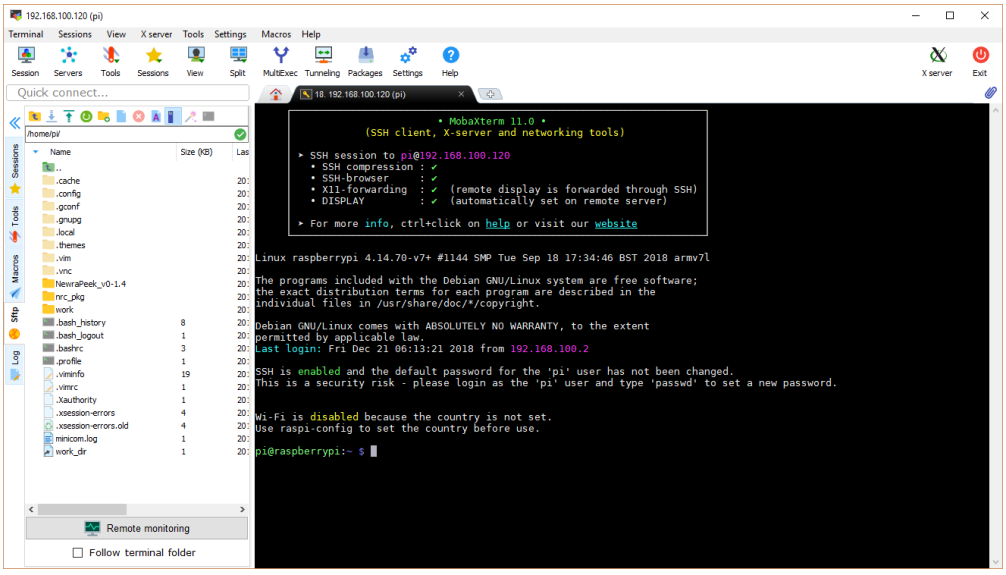


Figure 2.2 MobaXterm SSH Session

Or you can create VNC session as below.

You can download VNC viewer from https://www.realvnc.com/en/connect/download/viewer/.

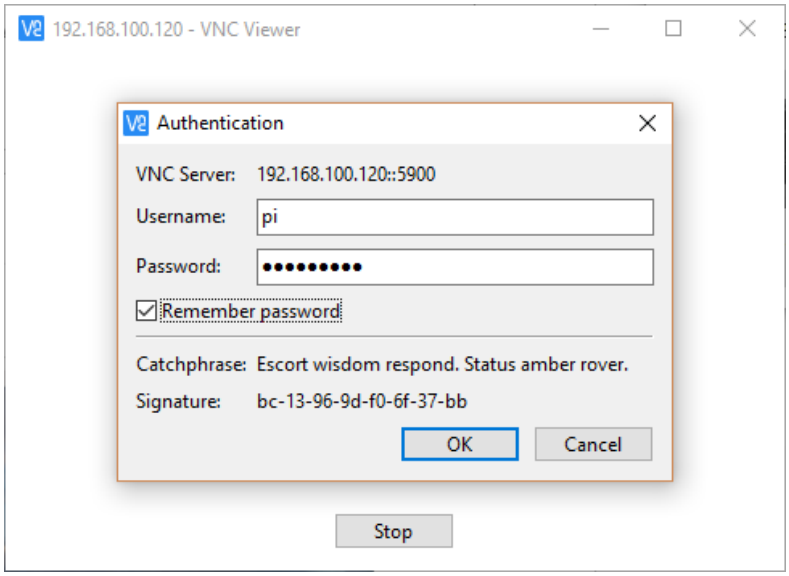


Figure 2.3 VNC Viewer Configuration

After creating VNC session and connecting to the sniffer device, you will see the window Figure 2.4 displayed.

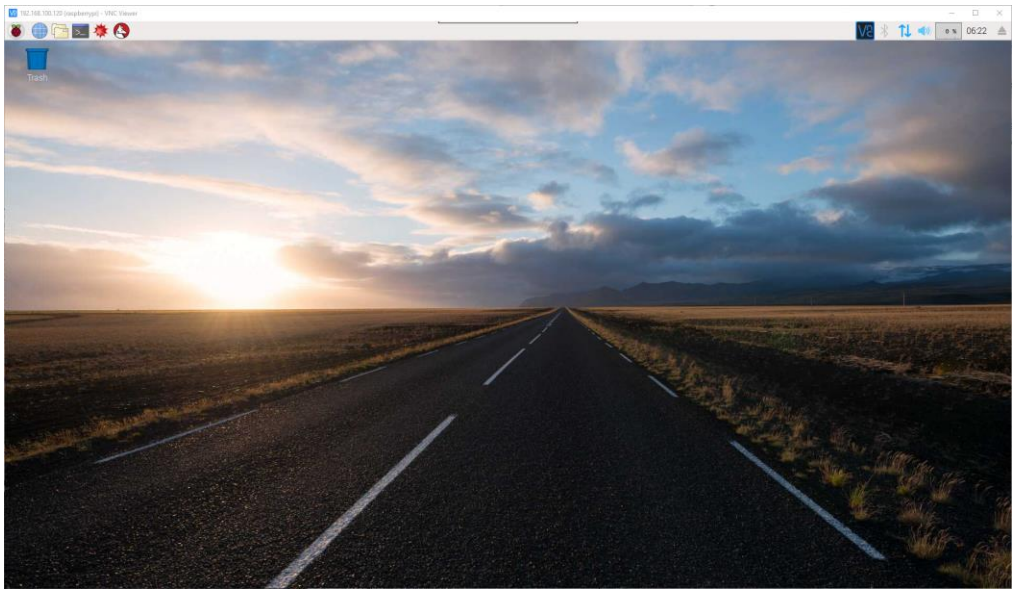


Figure 2.4 VNC Viewer Session

2.2 Control PC-Sniffer Device Configuration

First you need to configure the sniffer device for NewraPeek. After configuring sniffer device as described below, you can choose one of two options to control sniffer device: Remote Control and Local Control used for local capture operation. Or you can use remote capture operation as described in section 2.4 after finishing the device configuration in this chapter.

2.2.1 Sniffer Device Configuration

Following accessories are needed to configure sniffer device:

- Input Power Adapter (5V/1.5~2A)
- Ethernet Cable

If you want to control sniffer device locally, you also need:

- HDMI Cable
- USB Keyboard and Mouse

Detailed locations of the connections are shown in following figure.

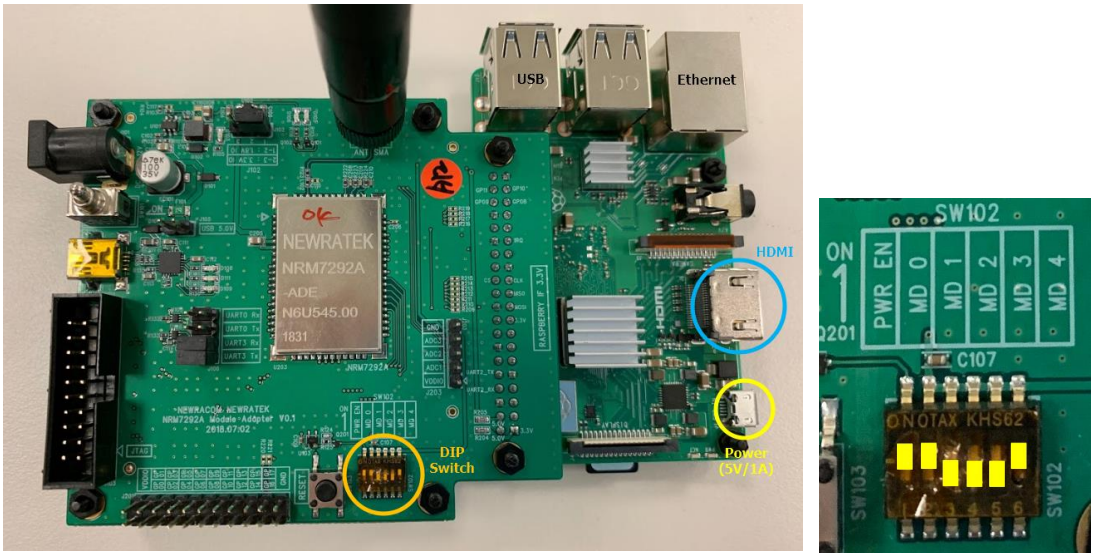


Figure 2.5 Sniffer Device and DIP Switch Configuration

2.2.2 Local Control Configuration

You can control sniffer device directly by using Raspberry Pi. Raspberry Pi supports HDMI and USB interfaces. Users can also configure as to the figure below.

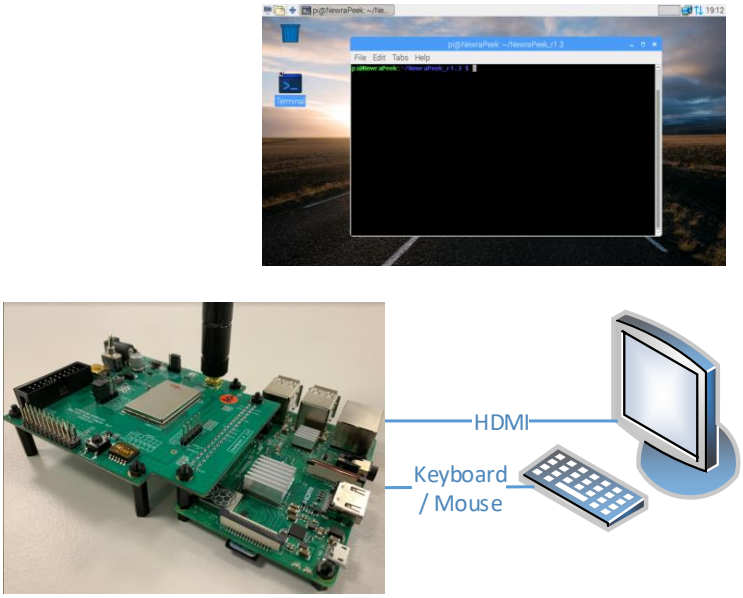


Figure 2.6 Local Control Configuration

2.2.3 Remote Control Configuration

When users first connect to a sniffer device, users must configure the IP address of Ethernet interface on your PC or laptop.

- IP address: 192.168.100.200

  (You can change IP address after the NewraPeek initialization.)

Detailed connection cabling is shown in following figure.

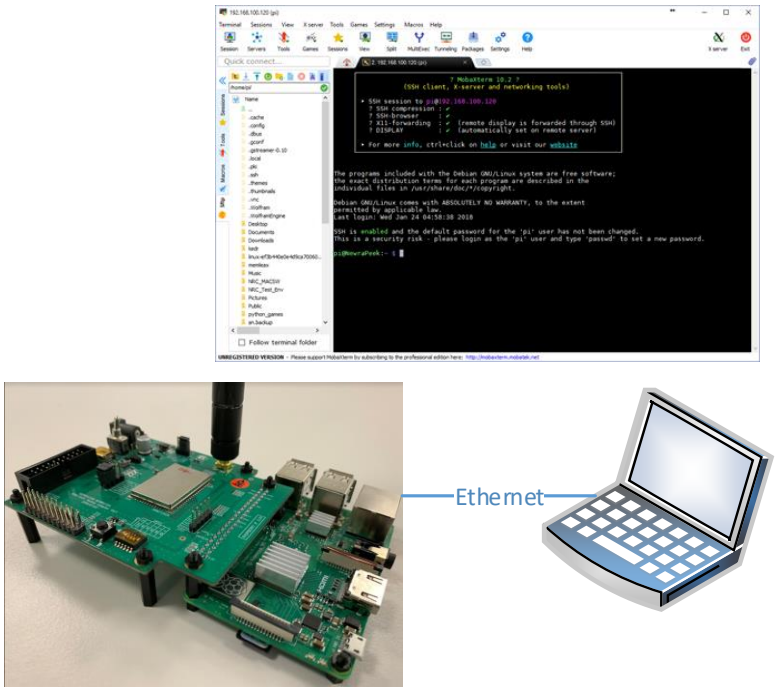


Figure 2.7 Remote Control Configuration

2.3 NewraPeek Local Capture Operation

2.3.1 Install SW packages for Sniffer

To run as Sniffer, SW packages should be installed in advance. Follow the procedures in README file in sniffer/NewraPeek_v0-1.4 directory.

```
pi@raspberrypi:~/nrc_pkg/script/sniffer/NewraPeek_v0-1.4 $ ls -al
total 12808
drwxr-xr-x 2 pi pi     4096 Feb  7 09:47 .
drwxr-xr-x 3 pi pi     4096 Feb  7 09:47 ..
-rwxr-xr-x 1 pi pi 11548922 Feb  7 09:47 newrapeek_0-1.4_armhf.deb
-rwxr-xr-x 1 pi pi      907 Feb  7 09:47 README.txt
-rwxr-xr-x 1 pi pi  1540772 Feb  7 09:47 rpcapd
-rwxr-xr-x 1 pi pi      834 Feb  7 09:47 run_rpcapd.py
-rwxr-xr-x 1 pi pi      964 Feb  7 09:47 run_tshark.py
pi@raspberrypi:~/nrc_pkg/script/sniffer/NewraPeek_v0-1.4 $
```

Figure 2.8 NewraPeek Directory

2.3.2 Open terminal with SSH

After boot-up of EVB, connect via SSH to the Sniffer by using the terminal emulator like MobaXterm. The ID and PW are as follows:

- ID : pi
- PW : raspberry

2.3.3 Run Script

```
pi@raspberrypi:~/nrc_pkg/script $ ./start.py
Usage:
        start.py [sta_type] [security_mode] [country] [channel] [sniffer_mode]
Argument:
        sta_type      [0:STA   |  1:AP  |  2:SNIFFER]
        security_mode [0:Open  |  1:Security]
        country       [US:USA  |  JP:Japan  |  TW:Taiwan  | KR:Korea | EU:EURO]
        ------------------------------------------------------------
        channel       [S1G Channel Number]   * Only for Sniffer
        sniffer_mode  [0:Local | 1:Remote]   * Only for Sniffer
```

Figure 2.9 NewraPeek Run Script

To run as Sniffer, parameters should be set like below:

- sta_type should be 2 (Sniffer)
- security_mode should be 0 (Open)
- country, channel, sniffer_mode might be set as you wish
    - [country] available country codes are US, JP, TW, KR, EU
    - [channel] need to use channel number listed in Table 1.1 ~ 1.5
    - [sniffer_mode] 0: run on local terminal, 1: run on remote terminal

- For example
    - Local Sniffer mode on CH 40 for Japan : ./start.py 2 0 JP 40 0
    - Remote Sniffer mode on CH 44 for Korea: ./start.py 2 0 KR 44 1

2.3.4 Execute NewraPeek

Following figures show the running examples on both remote and local controls.

When the sniffer mode is used as local, NewraPeek will automatically start capturing as displayed below.

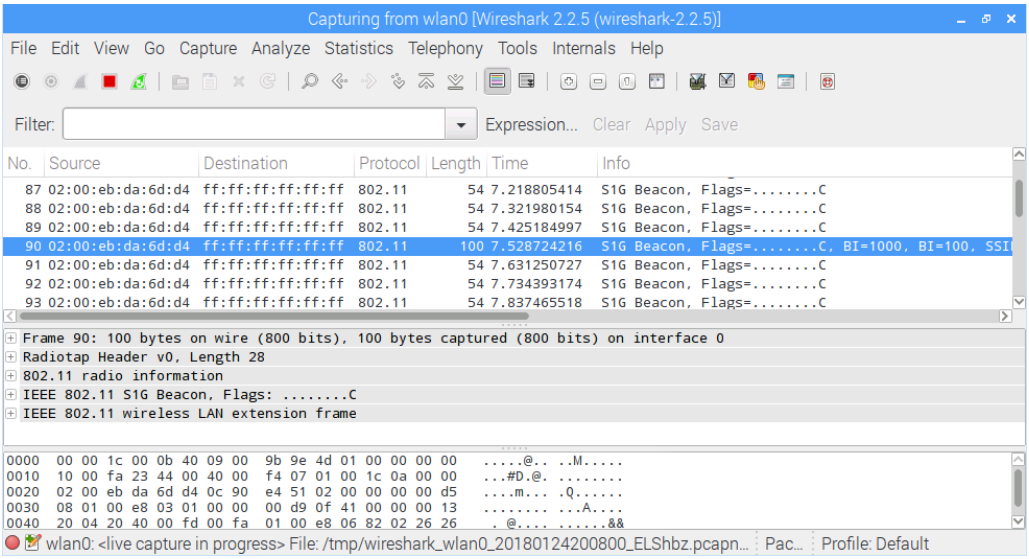


Figure 2.10 NewraPeek Running Example under Local Control

But if you use sniffer mode as remote, you must choose ‘wlan0’ interface and then click ‘Start’ on NewraPeek like below.

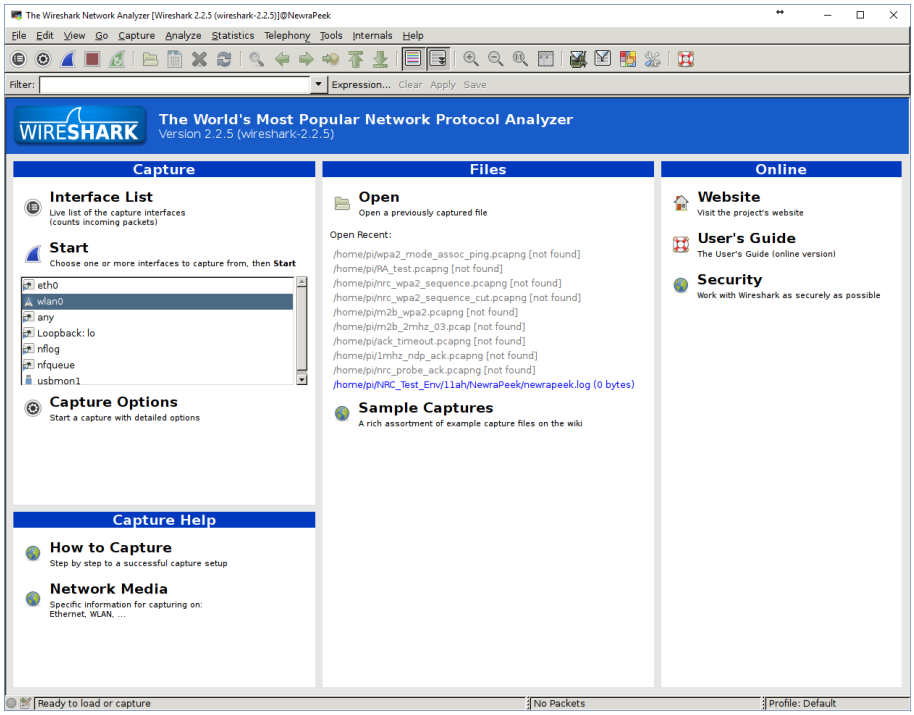


Figure 2.11 NewraPeek Running Example under Remote Control (Initial Screen)

After, the user will be able to see the operation of NewraPeek as displayed below.

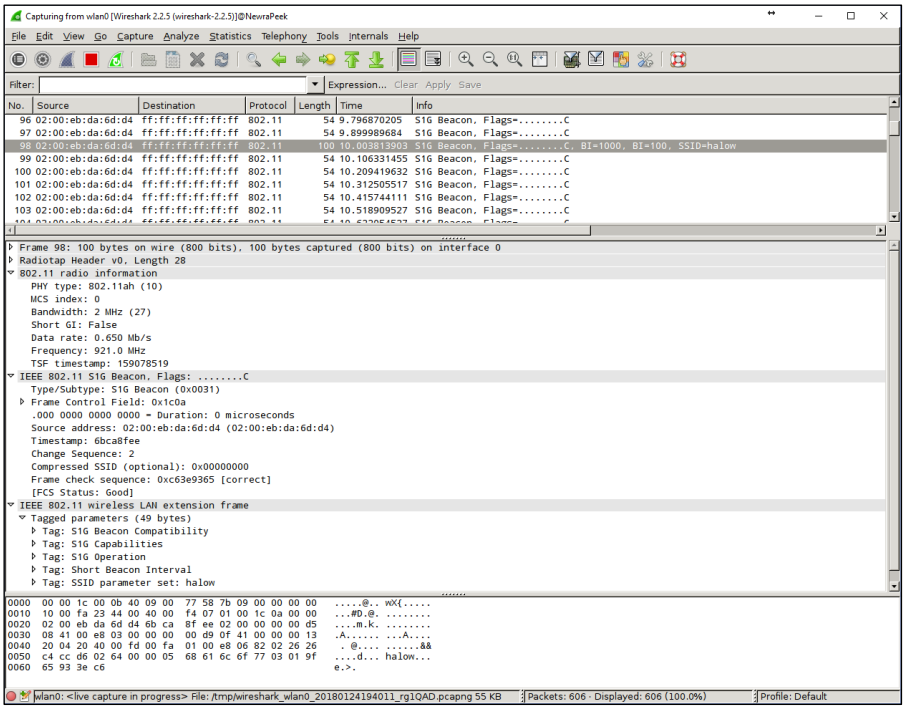


Figure 2.12 NewraPeek Running Example under Remote Control

NewraPeek is based on Wireshark. So, user can always refer to Wireshark documents for additional information.

If you need further information about Wireshark, please visit following URL:

- https://www.wireshark.org/docs/

2.3.5 Change Channel

If user prefer to change the channel in runtime, you can easily do so without closing and re-running NewraPeek. Users can run: 'change_channel.py' script to change channels. The figure below shows an example command. Please refer to the Linux Channel number which is listed in Table 1.1 - 1.5.

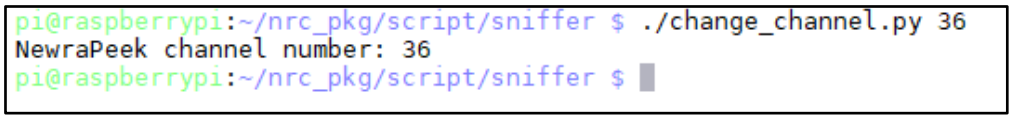


Figure 2.13 Channel Change Example

2.3.6 Print SNR&RSSI Value

You can see the current output value simply by SNR and RSSI through script.

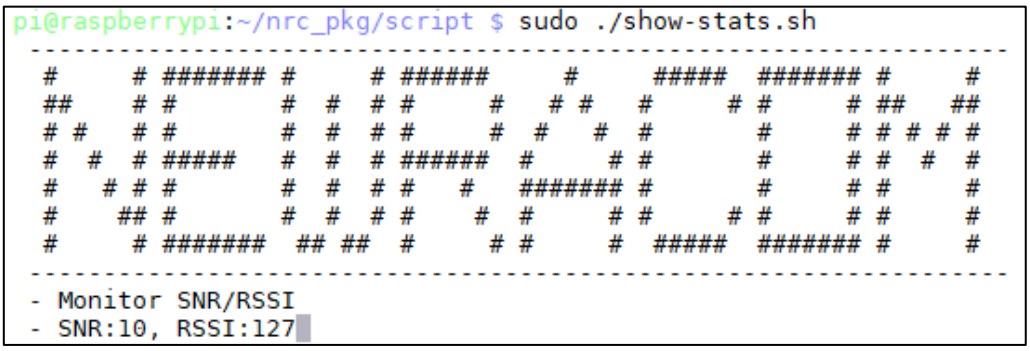


Figure 2.14 Print SNR&RSSI Values

2.4 NewraPeek Remote Capture Operation

NewraPeek also supports remote capture operation on Windows OS.
To do this, users must first run RPCAP daemon on sniffer device as explained below.

2.4.1 Run RPCAP Daemon on Sniffer Device

Instead of using scripts of local capture operation, you need to run 'run_rpcapd.py' script.

```
pi@raspberrypi:~/nrc_pkg/script/sniffer/NewraPeek_v0-1.4 $ ./run_rpcapd.py JP 36
NewraPeek country code:   JP
NewraPeek channel number: 36
```

Figure 2.15 RPCAP Daemon Running

- [country] available country codes are US, JP, TW, KR, EU
- [channel] need to use channel number listed in Table 1.1 ~ 1.5

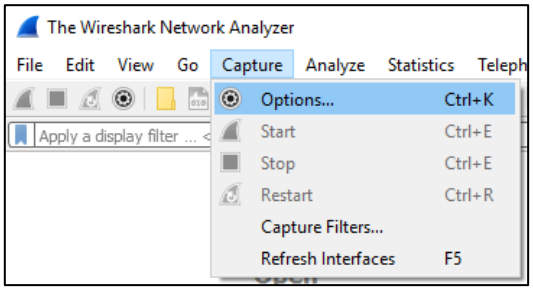
User must follow the same instruction for running NewraPeek and changing channels as described in 2.3.3 and 2.3.5. In this script, port numbers 1234 are used and port numbers can be changed to user's preference.

2.4.2 Run NewraPeek on Windows OS

After running NewraPeek Windows version by using Wireshark.exe under the directory 'NewaPeek_v0-1.4_for_WindowsOS', you first need to configure remote interface for the remote capture operation.

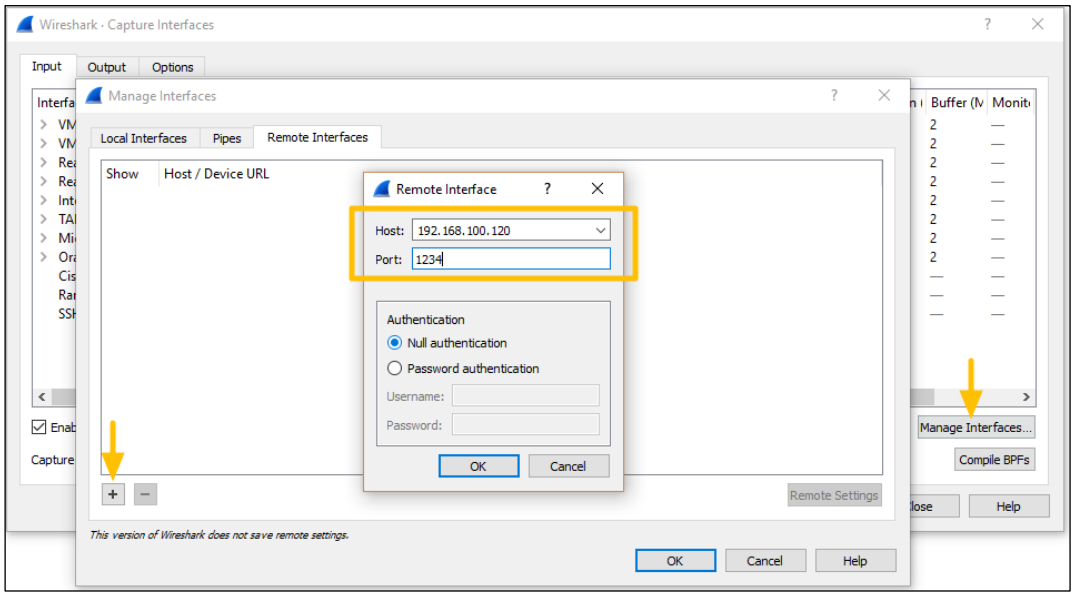
** Note: If you met dll library error messages at the time of NewraPeek run, please refer to the 'dll_libraries' directory.*
** Note: You need to make remote interface every time you run NewraPeek because Wireshark doesn't support the save function for remote interface.*

1) Click Options of Capture menu (Ctrl+K)

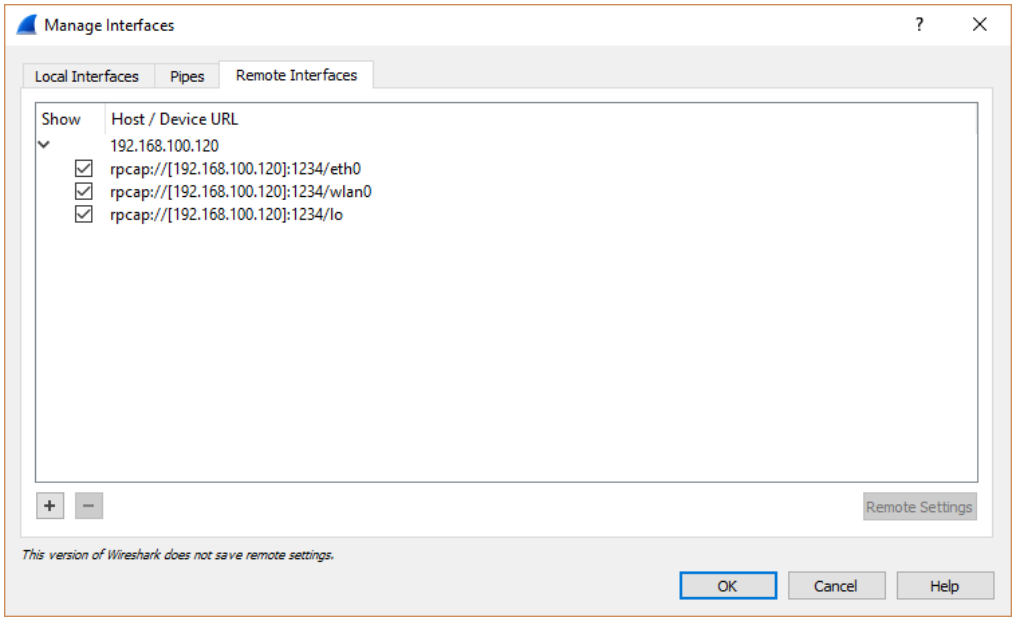


2) Click Manage Interfaces and then add remote interface in the ‘Remote Interfaces’ tab.

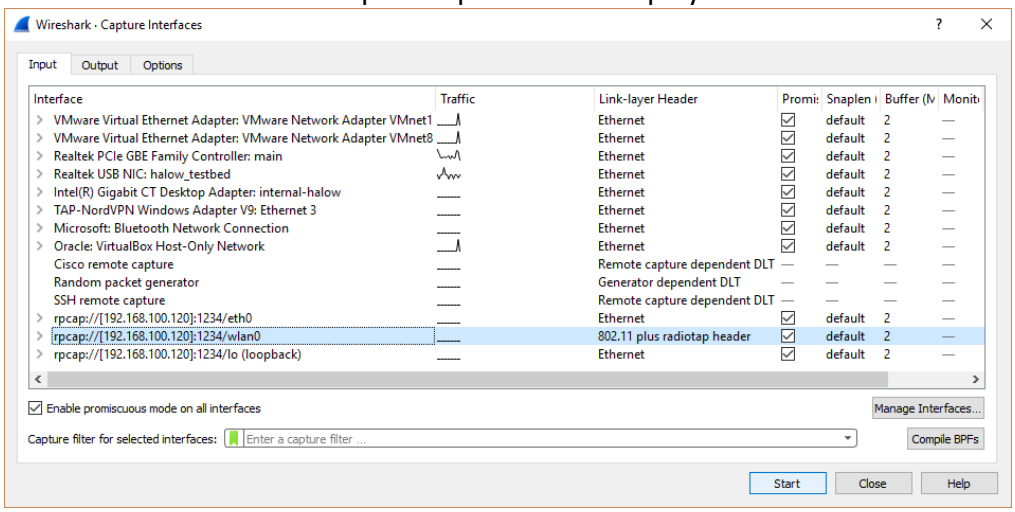
   - Host: 192.168.100.120 (Remote on Sniffer device)
   - Port: 1234



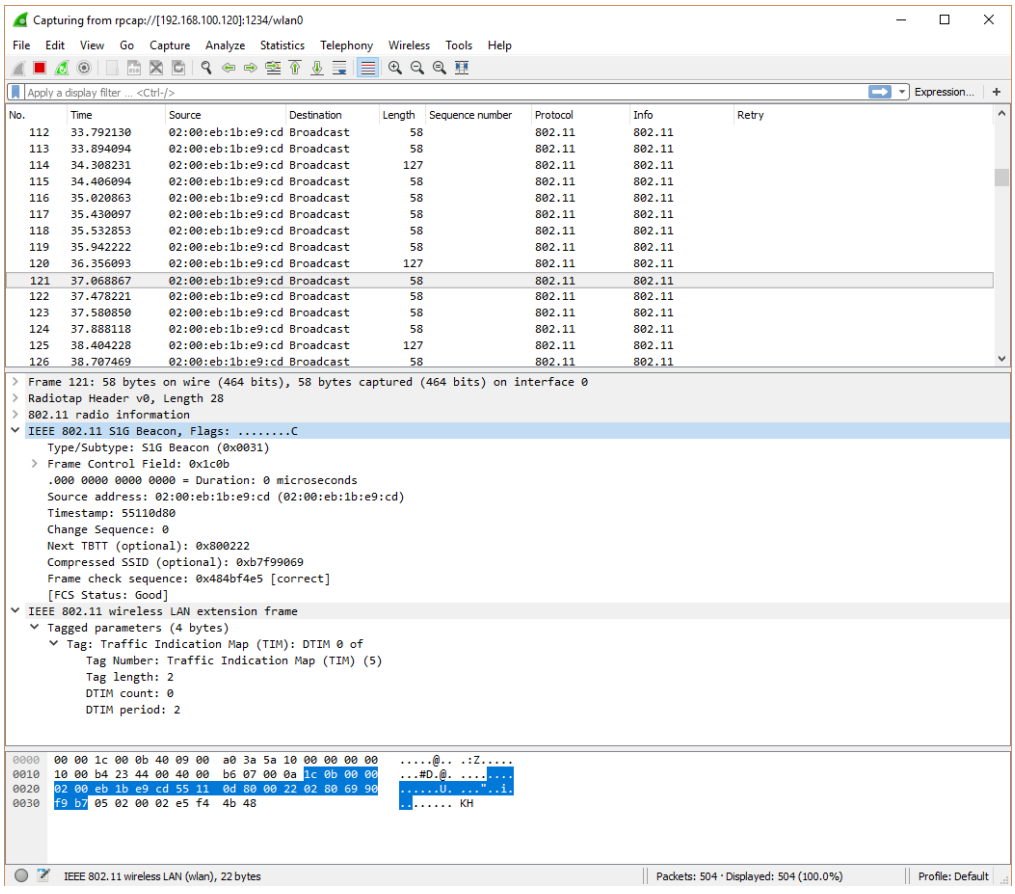
3) Now you can see the new remote interfaces. Please check if you run RPCAP daemon as described in 2.4.1.



4) Now click OK and start remote capture operation as displayed below.



5) If the previous step is successfully, the window below will be displayed.



2.4.3 Change Channel

If you want to change the channel in runtime, user can easily do so without closing and re-running NewraPeek. You can simply run 'change_channel.py' script in the same directory where users run RPCAP daemon. Below figure shows an example command. Please refer to the Linux Channel number which is listed in Table 1.1 ~ 1.5.

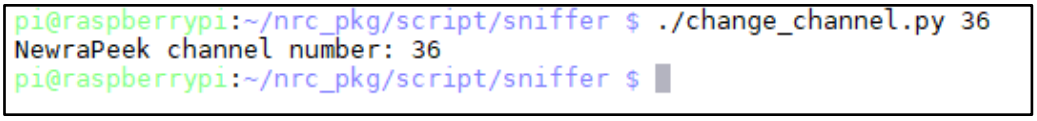


Figure 2.16 Channel Change Example

3 Revision History

Revision No	Date	Comments
Ver 1.0	01/15/2018	Initial version for customer release created
Ver 1.1	04/12/2019	CN Table added for China updated