



NRC7394 Evaluation Kit

User Guide

(NewraPeek™)

Ultra-low power & Long-range Wi-Fi

Ver 1.0
Apr. 5, 2023

Newracom, Inc.

NRC7394 Evaluation Kit User Guide (NewraPeek™)

Ultra-low power & Long-range Wi-Fi

© 2023 Newracom, Inc.

All right reserved. No part of this document may be reproduced in any form without written permission from NEWRACOM.

NEWRACOM reserves the right to change in its products or product specification to improve function or design at any time without notice.

Office

NEWRACOM, Inc.

505 Technology Drive, Irvine, CA 92618 USA

<http://www.NEWRACOM.com>

Contents

- 1 Introduction 6**
- 2 Configuration 12**
 - 2.1 SW Prerequisites 12
 - 2.1.1 Install MobaXterm and VNC Viewer for Remote Control 12
 - 2.2 Control PC-Sniffer Device Configuration..... 14
 - 2.2.1 Sniffer Device Configuration 14
 - 2.2.2 Local Control Configuration 15
 - 2.2.3 Remote Control Configuration..... 16
 - 2.3 NewraPeek Local Capture Operation..... 17
 - 2.3.1 Install SW packages for Sniffer..... 17
 - 2.3.2 Open terminal with SSH..... 18
 - 2.3.3 Run Script 18
 - 2.3.4 Execute NewraPeek 19
 - 2.3.5 Change Channel 21
- 3 Revision History 22**

List of Tables

Table 1.1	Supported 802.11ah channels (US)	7
Table 1.2	Supported 802.11ah channels (JP).....	8
Table 1.3	Supported 802.11ah channels (TW)	8
Table 1.4	Supported 802.11ah channels (KR) – MIC Package	9
Table 1.5	Supported 802.11ah channels (KR) – USN Package.....	9
Table 1.6	Supported 802.11ah channels (EU)	9
Table 1.7	Supported 802.11ah channels (NZ)	9
Table 1.8	Supported 802.11ah channels (AU)	10
Table 1.9	Supported 802.11ah specific frames	11
Table 1.10	Supported 802.11ah specific element IDs	11

List of Figures

Figure 1.1 Wirehark-based NewraPeek Version Information.....	6
Figure 2.1 MobaXterm SSH Configuration	12
Figure 2.2 MobaXterm SSH Session	13
Figure 2.3 VNC Viewer Configuration	13
Figure 2.4 VNC Viewer Session	14
Figure 2.5 NRC7394 evaluation board (Top view)	15
Figure 2.6 Host mode configuration	15
Figure 2.7 Local Control Configuration	16
Figure 2.8 Remote Control Configuration.....	17
Figure 2.9 NewraPeek Directory	17
Figure 2.10 NewraPeek Run Script.....	18
Figure 2.11 NewraPeek Running Example under Local Control	19
Figure 2.12 NewraPeek Running Example under Remote Control (Initial Screen)	20
Figure 2.13 NewraPeek Running Example under Remote Control.....	20
Figure 2.14 Channel Change Example.....	21

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.

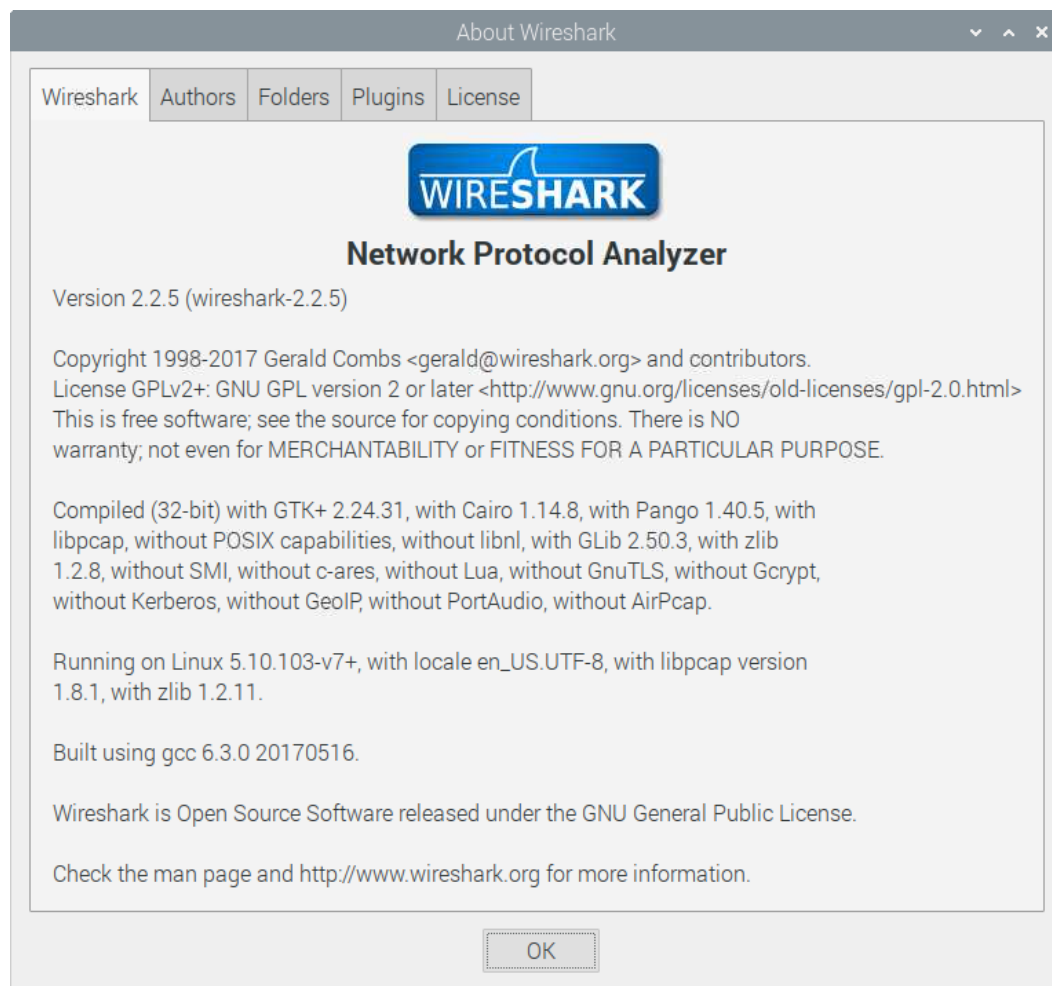


Figure 1.1 Wirehark-based NewraPeek Version Information

The following tables show the supported 802.11ah specific channels, frames, and information elements.

Table 1.1 Supported 802.11ah channels (US)

Frequency band index	Bandwidth (MHz)	Sub-1GHz frequency	2.4 / 5G frequency
1	1	902.5	2412
3	1	903.5	2422
5	1	904.5	2432
7	1	905.5	2442
9	1	906.5	2452
11	1	907.5	2462
36	1	908.5	5180
37	1	909.5	5185
38	1	910.5	5190
39	1	911.5	5195
40	1	912.5	5200
41	1	913.5	5205
42	1	914.5	5210
43	1	915.5	5215
44	1	916.5	5220
45	1	917.5	5225
46	1	918.5	5230
47	1	919.5	5235
48	1	920.5	5240
149	1	921.5	5745
150	1	922.5	5750
151	1	923.5	5755
152	1	924.5	5760
100	1	925.5	5500
104	1	926.5	5520
108	1	927.5	5540
2	2	903	2417
6	2	905	2437
10	2	907	2457
153	2	909	5765
154	2	911	5770
155	2	913	5775
156	2	915	5780
157	2	917	5785
158	2	919	5790
159	2	921	5795
160	2	923	5800
161 (Default)	2	925	5805
112	2	927	5560

8	4	906	2447
162	4	910	5810
163	4	914	5815
164	4	918	5820
165	4	922	5825
116	4	926	5580

Table 1.2 Supported 802.11ah channels (JP)

Frequency band index	Bandwidth (MHz)	Sub-1GHz frequency	2.4 / 5G frequency
40 (Default)	1	921.0	5200
42	1	923.0	5210
43	1	924.0	5215
44	1	925.0	5220
45	1	926.0	5225
46	1	927.0	5230
36	2	923.5	5180
37	2	924.5	5185
38	2	925.5	5190
39	2	926.5	5195
47	4	924.5	5235
48	4	925.5	5240

Table 1.3 Supported 802.11ah channels (TW)

Frequency band index	Bandwidth (MHz)	Sub-1GHz frequency	2.4 / 5G frequency
36	1	839.0	5180
37	1	840.0	5185
38	1	841.0	5190
39	1	842.0	5195
40	1	843.0	5200
41	1	844.0	5205
42	1	845.0	5210
43	1	846.0	5215
44	1	847.0	5220
45	1	848.0	5225
46	1	849.0	5230
47	1	850.0	5235
48	1	851.0	5240
149	2	839.5	5745
150	2	841.5	5750
151 (Default)	2	843.5	5755

152	2	845.5	5760
153	2	847.5	5765
154	2	849.5	5770
155	4	840.5	5775
156	4	844.5	5780
157	4	848.5	5785

Table 1.4 Supported 802.11ah channels (KR) – MIC Package

Frequency band index	Bandwidth (MHz)	Sub-1GHz frequency	2.4 / 5G frequency
37	1	926.5	5185
38	1	927.5	5190
39 (Default)	1	928.5	5195
40	1	929.5	5200
42	2	927.0	5210
43	2	929.0	5215

Table 1.5 Supported 802.11ah channels (KR) – USN Package

Frequency band index	Bandwidth (MHz)	Sub-1GHz frequency	2.4 / 5G frequency
44 (Default)	1	921.5	5220
45	1	922.5	5225

Table 1.6 Supported 802.11ah channels (EU)

Frequency band index	Bandwidth (MHz)	Sub-1GHz frequency	2.4 / 5G frequency
36 (Default)	1	863.5	5180
37	1	864.5	5185
38	1	865.5	5190
39	1	866.5	5195
40	1	867.5	5200

Table 1.7 Supported 802.11ah channels (NZ)

Frequency band index	Bandwidth (MHz)	Sub-1GHz frequency	2.4 / 5G frequency
36 (Default)	1	915.5	5180
37	1	916.5	5185
38	1	917.5	5190
39	1	918.5	5195
40	1	919.5	5200
41	1	920.5	5205
42	1	921.5	5210
43	1	922.5	5215

44	1	923.5	5220
45	1	924.5	5225
46	1	925.5	5230
47	1	926.5	5235
48	1	927.5	5240
153	2	917.0	5765
154	2	919.0	5770
155	2	921.0	5775
156	2	923.0	5780
157	2	925.0	5785
158	2	927.0	5790
162	4	918.0	5810
163	4	922.0	5815
164	4	926.0	5820

Table 1.8 Supported 802.11ah channels (AU)

Frequency band index	Bandwidth (MHz)	Sub-1GHz frequency	2.4 / 5G frequency
36 (Default)	1	915.5	5180
37	1	916.5	5185
38	1	917.5	5190
39	1	918.5	5195
40	1	919.5	5200
41	1	920.5	5205
42	1	921.5	5210
43	1	922.5	5215
44	1	923.5	5220
45	1	924.5	5225
46	1	925.5	5230
47	1	926.5	5235
48	1	927.5	5240
153	2	917.0	5765
154	2	919.0	5770
155	2	921.0	5775
156	2	923.0	5780
157	2	925.0	5785
158	2	927.0	5790
162	4	918.0	5810
163	4	922.0	5815
164	4	926.0	5820

Table 1.9 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 1.10 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.

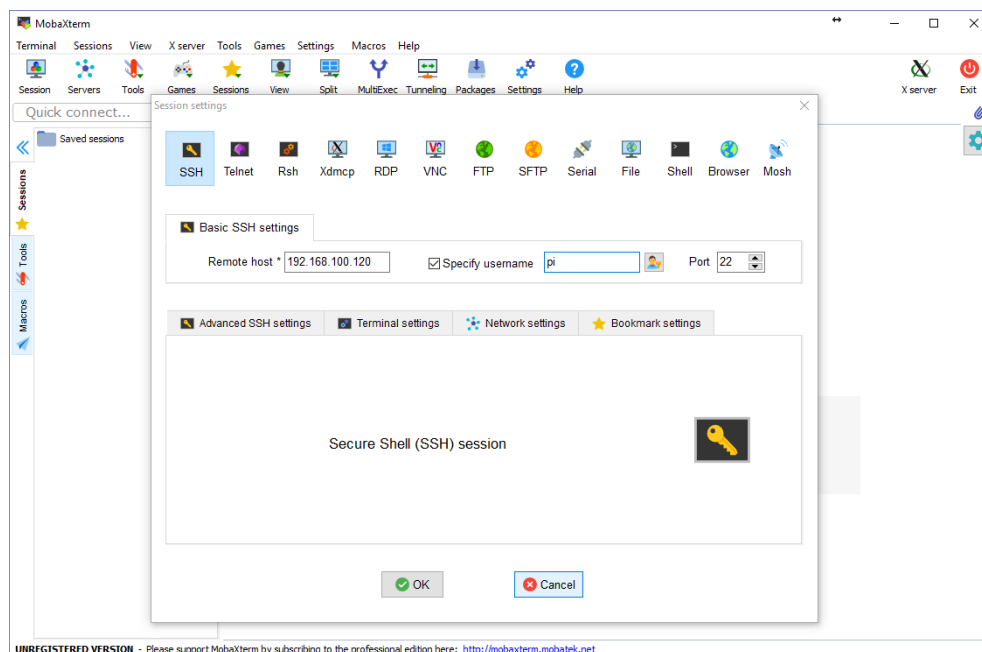


Figure 2.1 MobaXterm SSH Configuration

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.

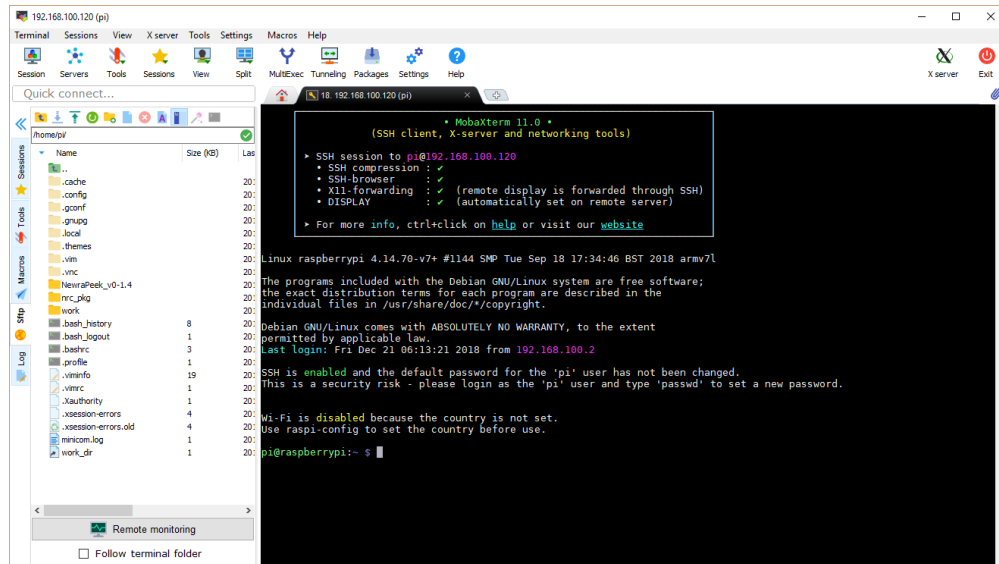


Figure 2.2 MobaXterm SSH Session

Or you can create VNC session as below.

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

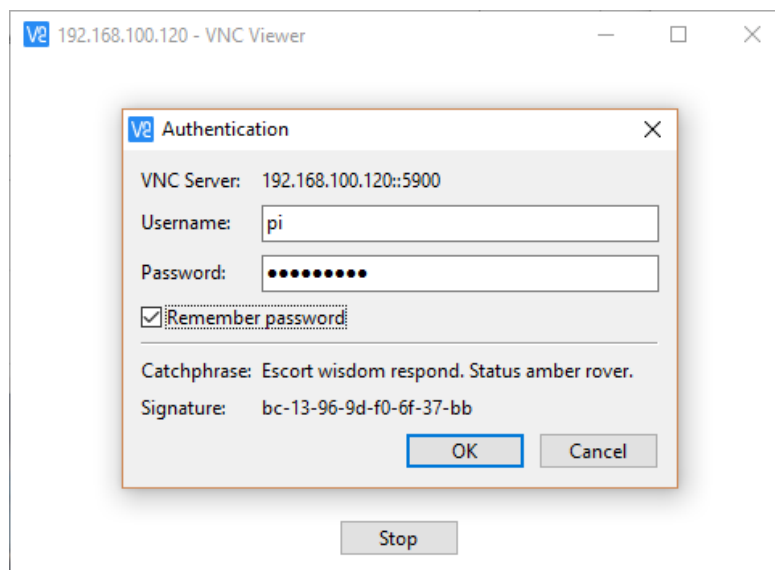


Figure 2.3 VNC Viewer Configuration

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

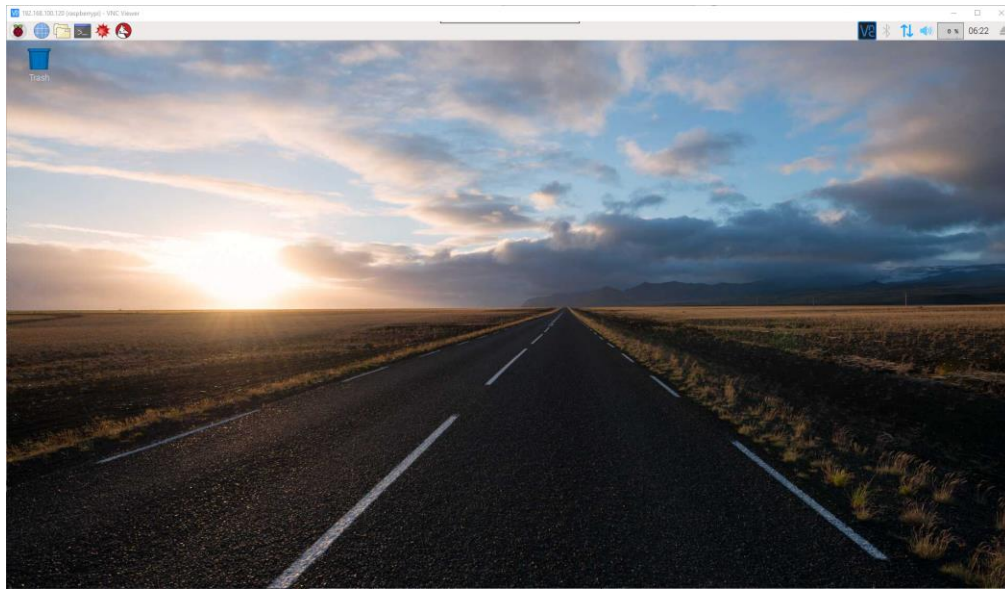


Figure 2.4 VNC Viewer Session

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 **Error! Reference source not found.** 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.

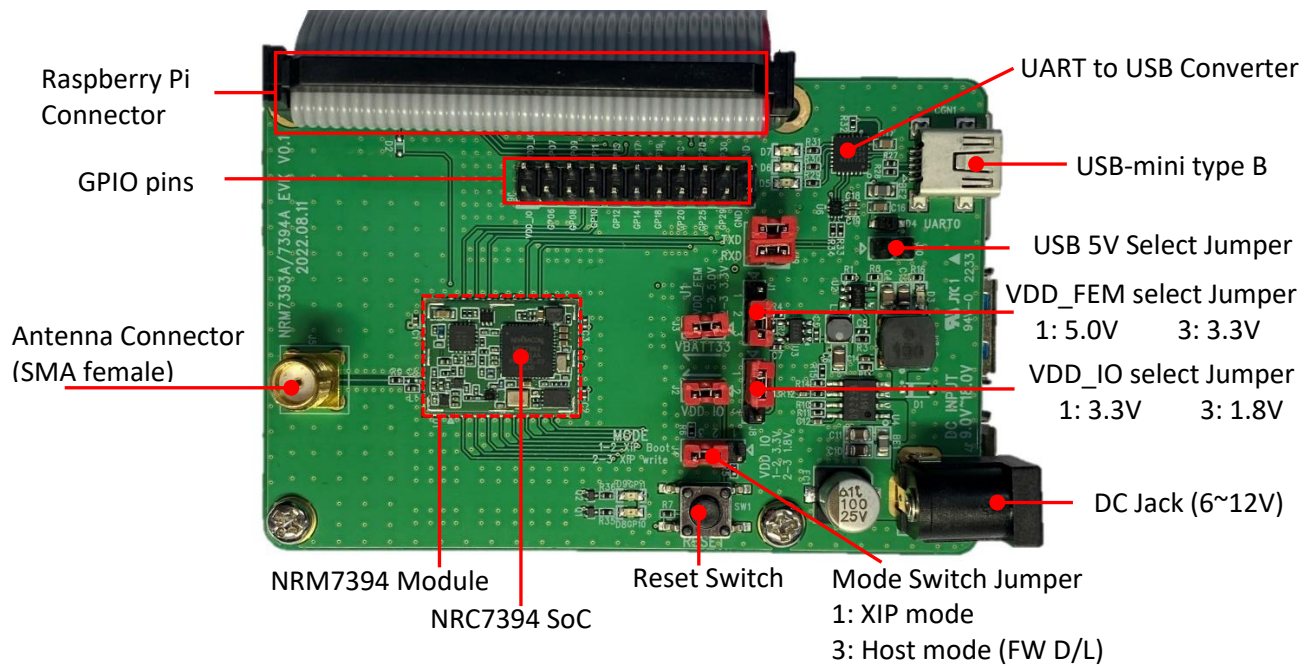


Figure 2.5 NRC7394 evaluation board (Top view)

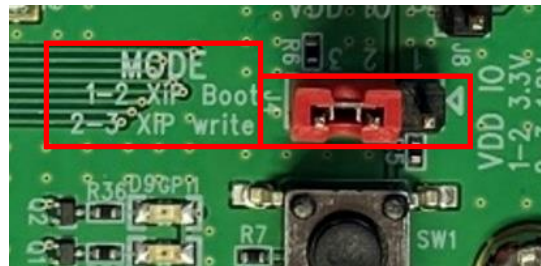


Figure 2.6 Host mode configuration

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.

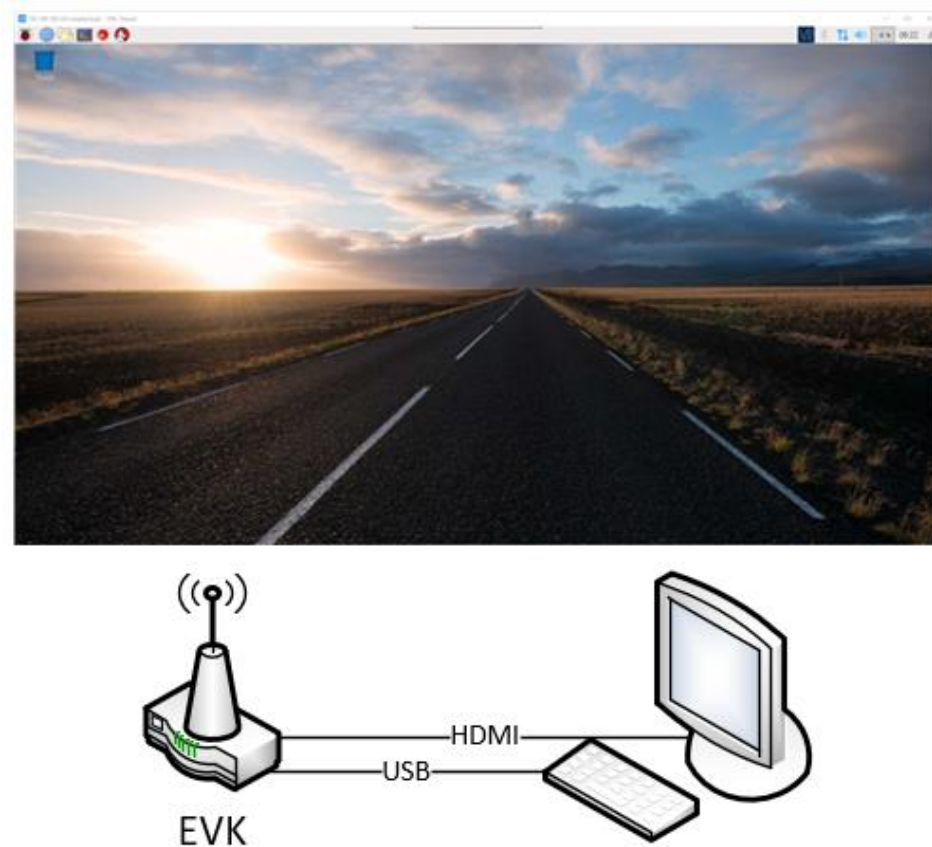


Figure 2.7 Local Control Configuration

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.

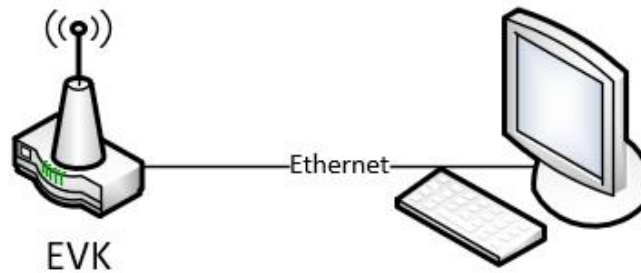
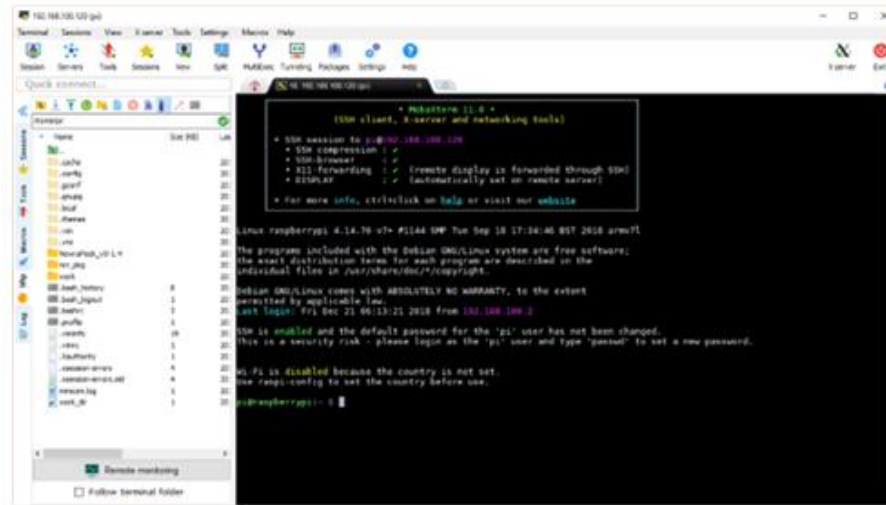


Figure 2.8 Remote Control Configuration

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 -la
total 12808
drwxrwxrwx 2 pi pi      4096 Jan  5 09:56 .
drwxrwxrwx 3 pi pi      4096 Jan  5 09:56 ..
-rwxrwxrwx 1 pi pi 11548922 Jan  5 09:56 newrapeek_0-1.4_armhf.deb
-rwxrwxrwx 1 pi pi      913 Jan  5 09:56 README.txt
-rwxrwxrwx 1 pi pi 1540772 Jan  5 09:56 rpcapd
-rwxrwxrwx 1 pi pi      834 Jan  5 09:56 run_rpcapd.py
-rwxrwxrwx 1 pi pi      964 Jan  5 09:56 run_tshark.py
pi@raspberrypi:~/nrc_pkg/script/sniffer/NewraPeek_v0-1.4 $
```

Figure 2.9 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
Done.
Done.
Usage:
start.py [sta_type] [security_mode] [country] [channel] [sniffer_mode]
start.py [sta_type] [security_mode] [country] [mesh_mode] [mesh_peering] [mesh_ip]
Argument:
sta_type      [0:STA | 1:AP | 2:SNIFFER | 3:RELAY | 4:MESH | 5:IBSS]
security_mode [0:Open | 1:WPA2-PSK | 2:WPA3-OWE | 3:WPA3-SAE | 4:WPS-PBC]
country       [US:USA | JP:Japan | TW:Taiwan | EU:EURO | CN:China |
               AU:Australia | NZ:New Zealand | K1:Korea-USN | K2:Korea-MIC]
-----
channel       [S1G Channel Number] * Only for Sniffer & AP
sniffer_mode  [0:Local | 1:Remote] * Only for Sniffer
mesh_mode     [0:MPP | 1:MP | 2:MAP] * Only for Mesh
mesh_peering  [Peer MAC address] * Only for Mesh
mesh_ip       [Static IP address] * Only for Mesh
ibss_ip       [0:DHCP or static IP | 1:DHCP] * Only for IBSS
Example:
OPEN mode STA for US : ./start.py 0 0 US
Security mode AP for US : ./start.py 1 1 US
Local Sniffer mode on CH 40 for Japan : ./start.py 2 0 JP 40 0
SAE mode Mesh AP for US : ./start.py 4 3 US 2
Mesh Point with static ip : ./start.py 4 3 US 1 192.168.222.1
Mesh Point with manual peering : ./start.py 4 3 US 1 8c:0f:fa:00:29:46
Mesh Point with manual peering & ip : ./start.py 4 3 US 1 8c:0f:fa:00:29:46 192.168.222.1

OPEN mode IBSS for US with DHCP server : ./start.py 5 0 US 1
Security mode IBSS for US with DHCP client : ./start.py 5 1 US 0
Security mode IBSS for US with static IP : ./start.py 5 1 US 0 192.168.200.17
Note:
sniffer_mode should be set as '1' when running sniffer on remote terminal
MPP, MP mode support only Open, WPA3-SAE security mode
pi@raspberrypi:~/nrc_pkg/script $
```

Figure 2.10 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, NZ, AU
 - [channel] need to use channel number listed in Table 1.1 ~ 1.8
 - [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.

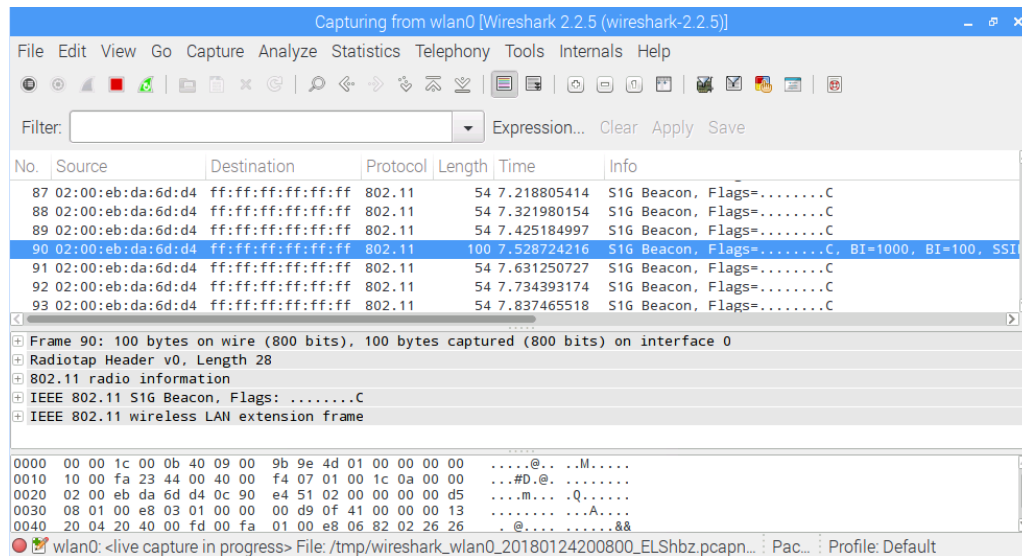


Figure 2.11 NewraPeek Running Example under Local Control

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

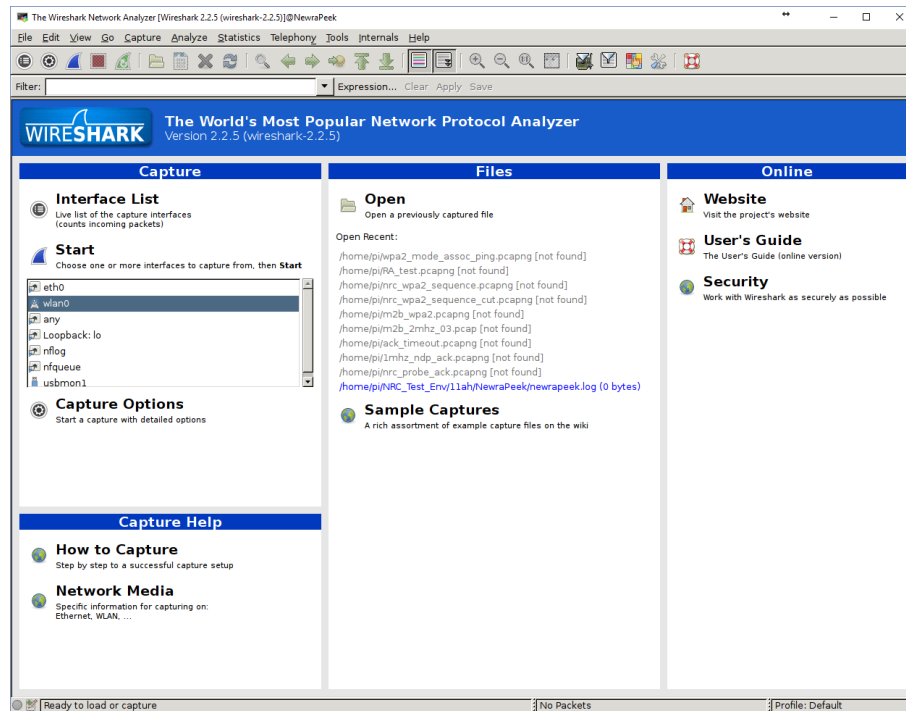


Figure 2.12 NewraPeek Running Example under Remote Control (Initial Screen)

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

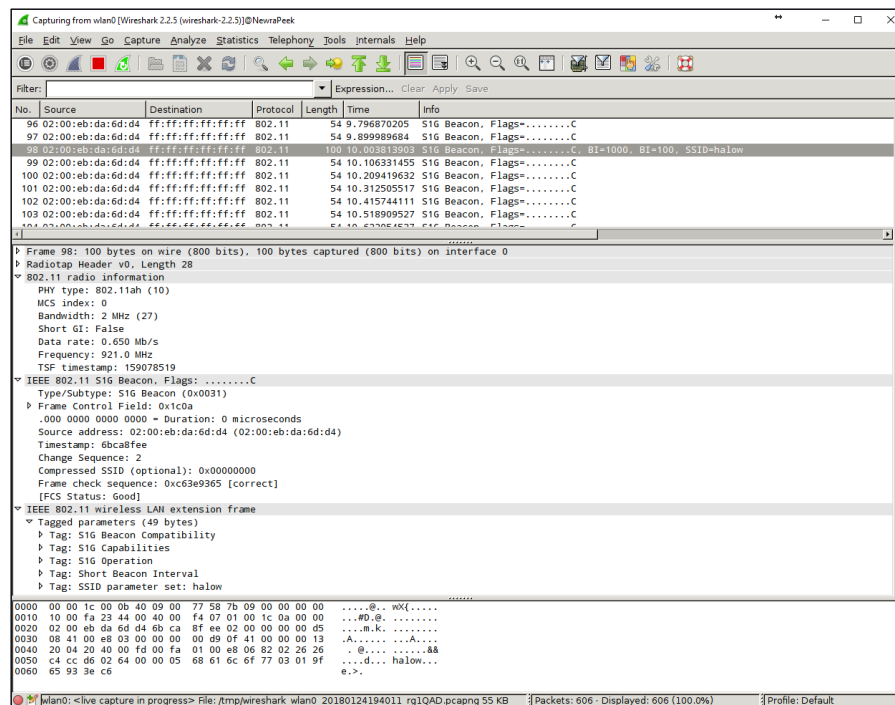


Figure 2.13 NewraPeek Running Example under Remote Control

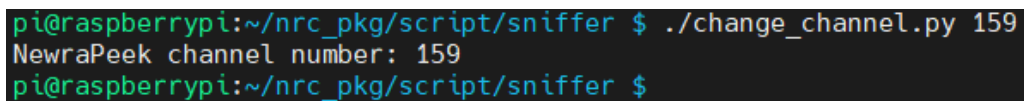
NewraPeek is based on Wireshark. So, user can always refer to Wireshark documents for additional information.

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.



```
pi@raspberrypi:~/nrc_pkg/script/sniffer $ ./change_channel.py 159
NewraPeek channel number: 159
pi@raspberrypi:~/nrc_pkg/script/sniffer $
```

Figure 2.14 Channel Change Example

3 Revision History

Revision No	Date	Comments
Ver 1.0	4/5/2023	Initial version