Morse Micro
reaching farther™

How to do a Sniffer Capture

APPNOTE-36

Table of Contents

1 Scope

This document describes how to capture over-the-air (OTA) packet traffic using the MM6108 radio to listen to and capture packets on a Wi-Fi HaLow network. This can be used to observe all traffic being sent on the channel, not just traffic destined for the sniffer device.

2 Theory of Operation

Network traffic or packet sniffing is the process of intercepting and logging traffic as it passes across a computer network. For wireless networks this is particularly feasible as the transmissions are visible to any listening radio within range of the device sending the traffic. Many network adaptors and wireless radios can be configured into a monitoring mode where it will passively listen to and log all transmissions on a given channel. Once logged (referred to as a 'packet capture'), the details of the traffic can be examined using a specialised analyzer application such as Wireshark. Note that encryption can mean that while the packet is intercepted, its contents cannot be read without also having the security key.

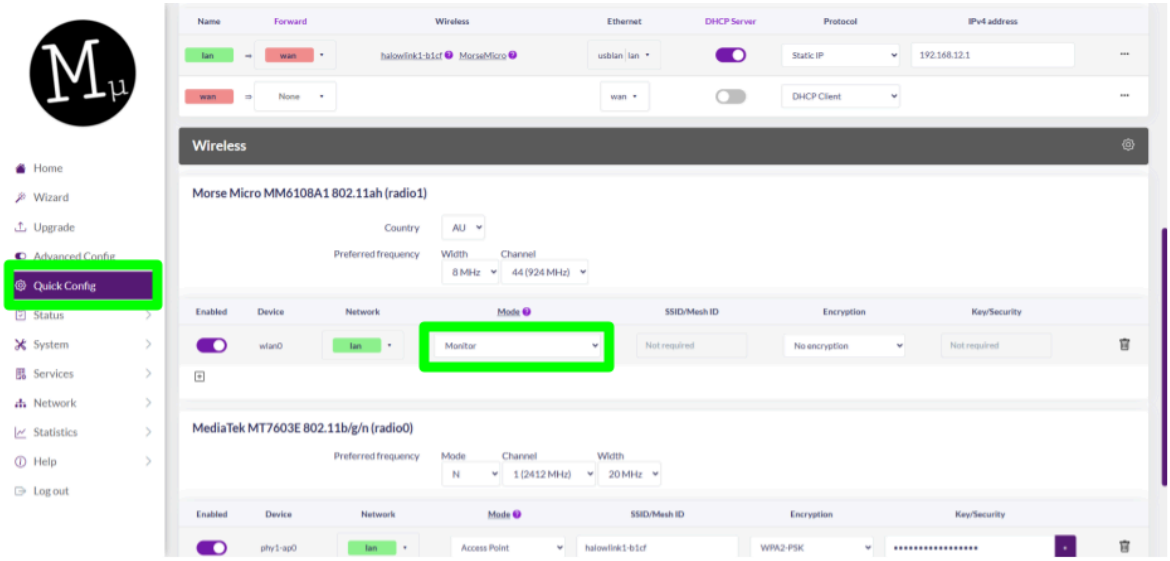
The MM6108 is able to be configured in a monitor mode, and the following sections outline how to capture traffic and load it into Wireshark. For the purpose of this guide it is assumed that the user has an evaluation kit running OpenWrt from Morse Micro.

3 How to Configure

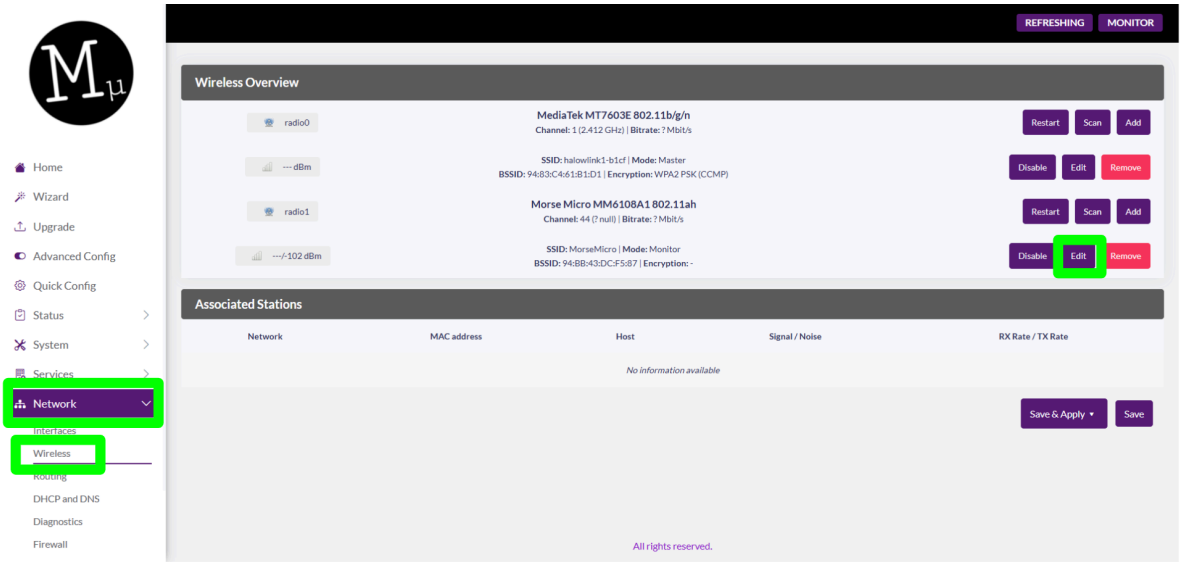
3.1 Configure Monitor Mode and Channel

3.1.1 GUI Configuration

For OpenWrt versions 2.7.x and higher, monitor mode can be set from the UI. Select **Quick Config**, and set the mode of the 802.11ah radio as **Monitor**. The channel and bandwidth are able to be set here. Click **Save & Apply** for changes to take effect.

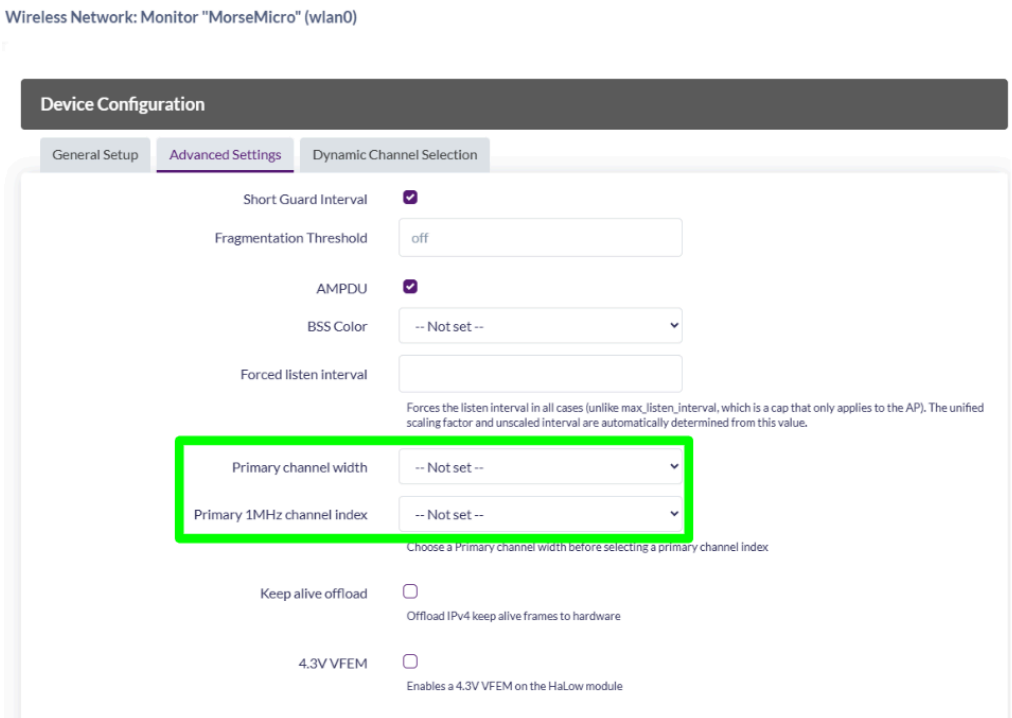


To set the primary bandwidth and channel index, these can be set by navigating to **Network → Wireless**, and clicking **Edit** on the HaLow radio.

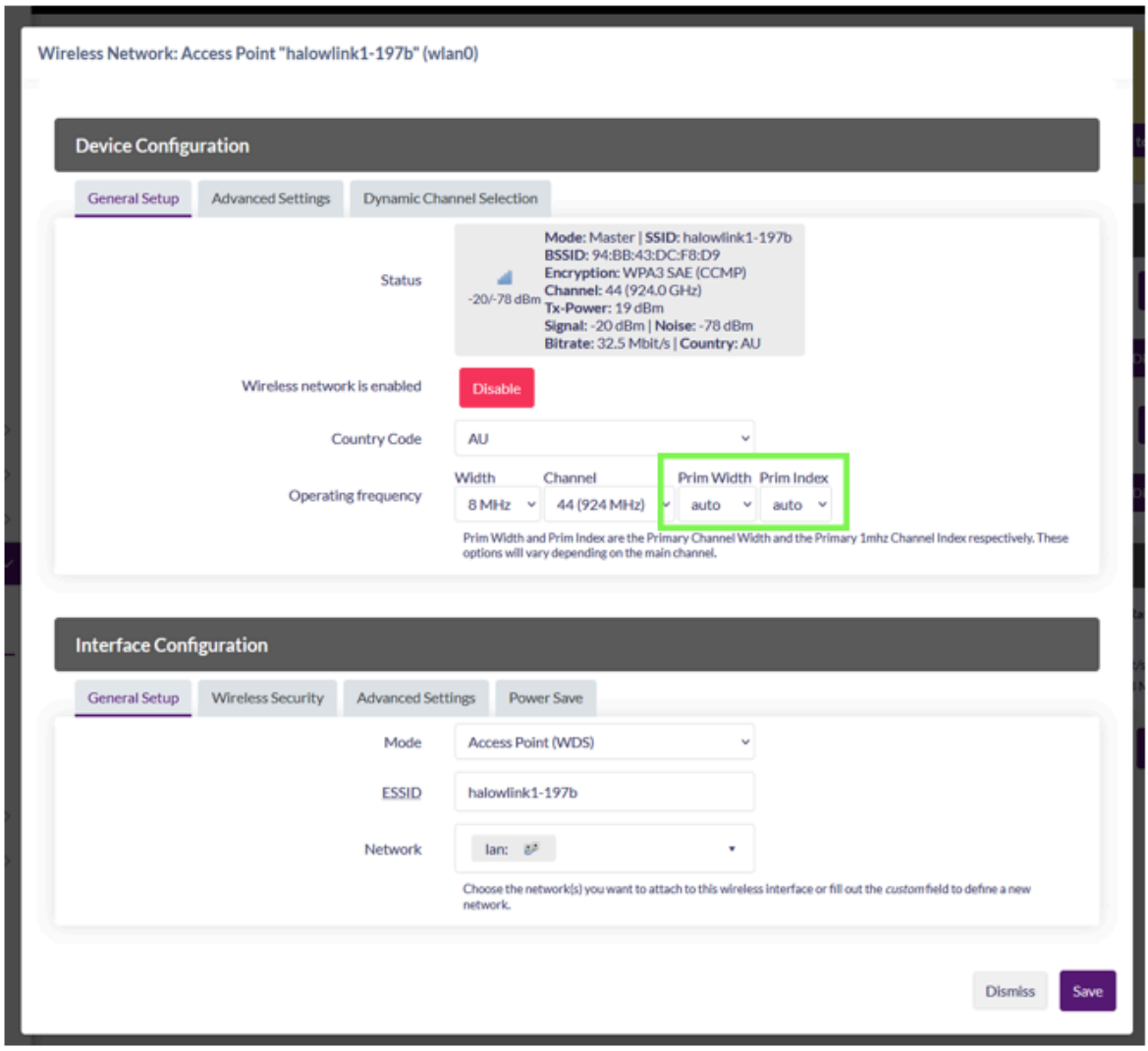


Set the intended **Primary channel width** and **Primary 1MHz channel index**, and click **Save & Apply**.

In release 2.7.2 it appears in Advanced Settings:



In release 2.8.2 (and onwards) it has moved under General Setup:



3.1.2 CLI Configuration

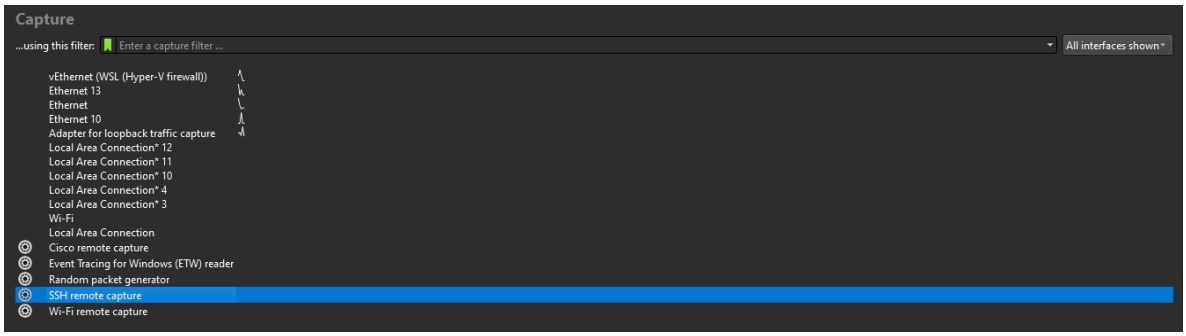
Run the following commands to put the device into sniffer mode and configure the channel to sniff on. In this example, the sniffer will look at packets on the 908MHz channel.

```
iw dev wlan0 del

iw phy phy1 interface add mon0 type monitor

ifconfig mon0 up && ifconfig morse0 up


# Configure channel

# -c channel frequency

# -o channel bw

# -p primary bw

# -n primary ch index

morse_cli -i mon0 channel -c 908000 -o 8 -p 2 -n 0
```

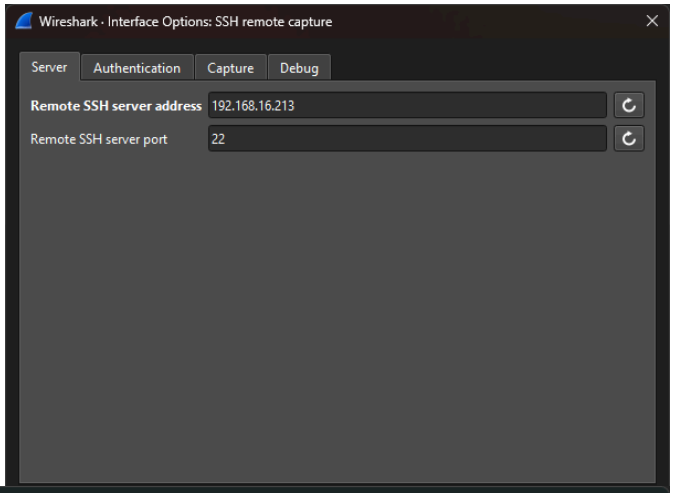
3.2 Capture with SSHdump

Modern versions of Wireshark prompts for the installation of sshdump as an external capture utility. Selecting to install this feature presents the user with an **SSH remote capture** interface which simplifies (and saves) the connection and authentication configuration and allows for the ability to stop/restart the packet capture natively in Wireshark.

To capture with sshdump, select the **SSH remote capture** interface.

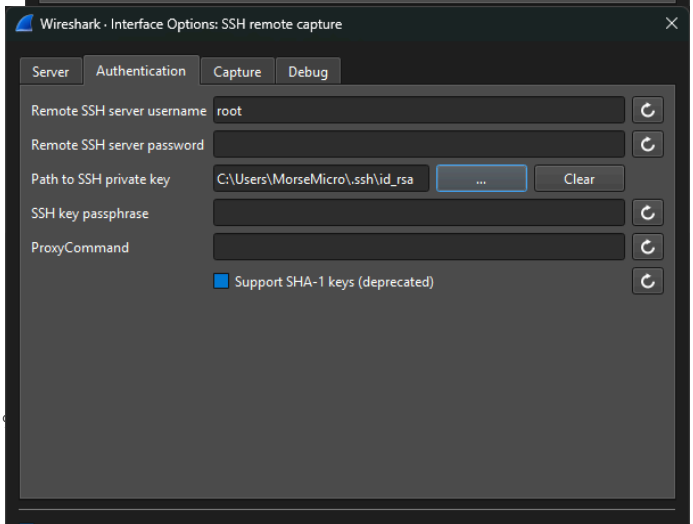


The first time this capture interface is started, Wireshark will prompt for configuration. The required configuration is outlined below.



Server:

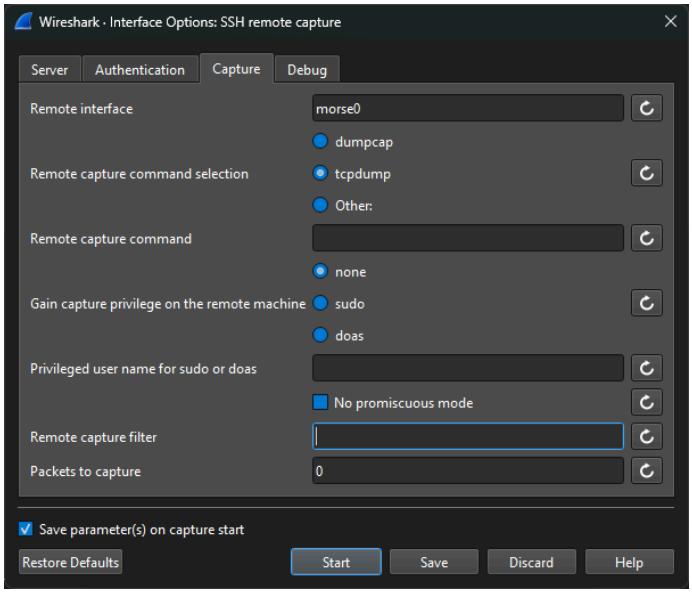
Configure the IP address and port used to access the device.



Authentication:

Configure the SSH details to access the device. Supports access via either the device password or using private keys.

If the underlying device for a given IP address regularly changes in the test set up, consider disabling StrictHostKeyChecking for that IP address..

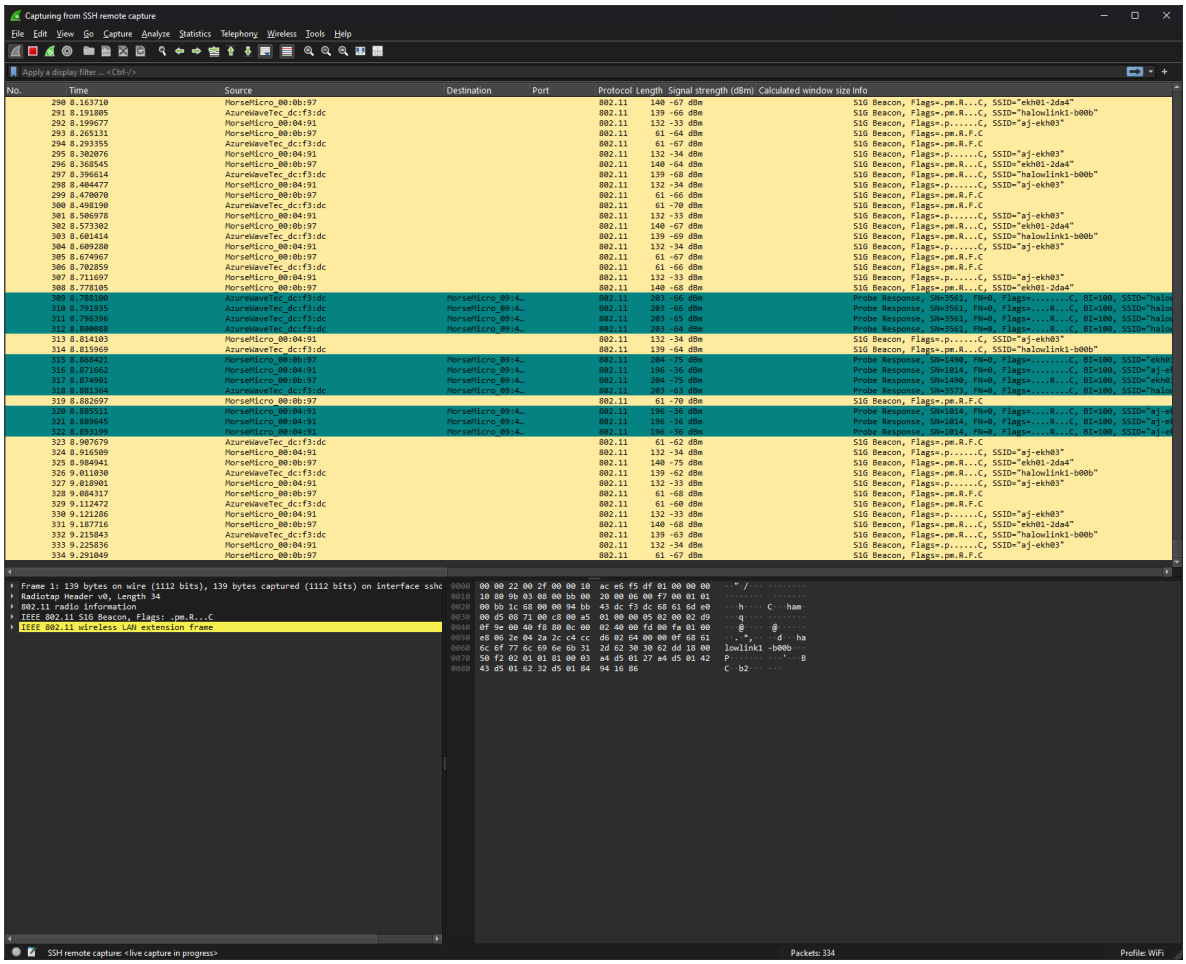


Capture:

Set the remote interface to morse0 to capture 802.11ah frames. Use tcpdump on the remote host.

The remote capture filter should only be required if connecting to the remote device over HaLow. Wireshark provides a default filter here to eliminate noise from the SSH connection.

Click ‘Start’ to initiate the capture and observe the results.



3.3 Alternative Options

For legacy purposes, this document retains the previous instructions to call tcpdump directly via SSH and pipe the output to Wireshark. This may be helpful in environments with older versions of Wireshark which do not support configuration of sshdump directly.

3.3.1 Launch Wireshark with SSHdump from the command line

```
wireshark -oextcap.sshdump.remotehost:10.42.0.1
-oextcap.sshdump.remoteinterface:morse0 -i sshdump -k
```

3.3.2 Capture with tcpdump

Then start tcpdump to capture the packets and write it to a file on the device.

```
tcpdump -i morse0 -w capture.pcap
```

Sniffer captures can become large quickly so make sure there is enough space on the filesystem if you want to do a long capture.

Once the capture is done, download the .pcap file to your computer and open it with Wireshark to view the packets.

3.3.3 Pipe tcpdump directly to Wireshark on local machine

It is possible to pipe the tcpdump output directly into Wireshark on a local machine through an SSH connection to the sniffer device. To do so, run the following command on the local machine:

On a Mac:

```
ssh root@10.42.0.1 tcpdump -i morse0 -U -s0 -w - |
/Applications/Wireshark.app/Contents/MacOS/Wireshark -k -i -
```

On Linux:

```
ssh root@10.42.0.1 tcpdump -i morse0 -U -s0 -w - | sudo wireshark
-k -i -
```

On Windows:

```
ssh root@10.42.0.1 tcpdump -i morse0 -U -s0 -w - | "C:\Program
Files\Wireshark\Wireshark.exe" -k -i -
```

This assumes the IP address of the device is 10.42.0.1 and Wireshark is installed in the default location. Once the command is run, Wireshark should open up and start displaying all the captured packets in the channel.

4 Revision History

Release Number	Release Date	Release Notes
01	20/03/2025	Initial release

Morse Micro
reaching farther™

Morse Micro Pty. Ltd. - HQ
Level 8, 10-14 Waterloo Street,
Surry Hills, NSW 2010, AUSTRALIA

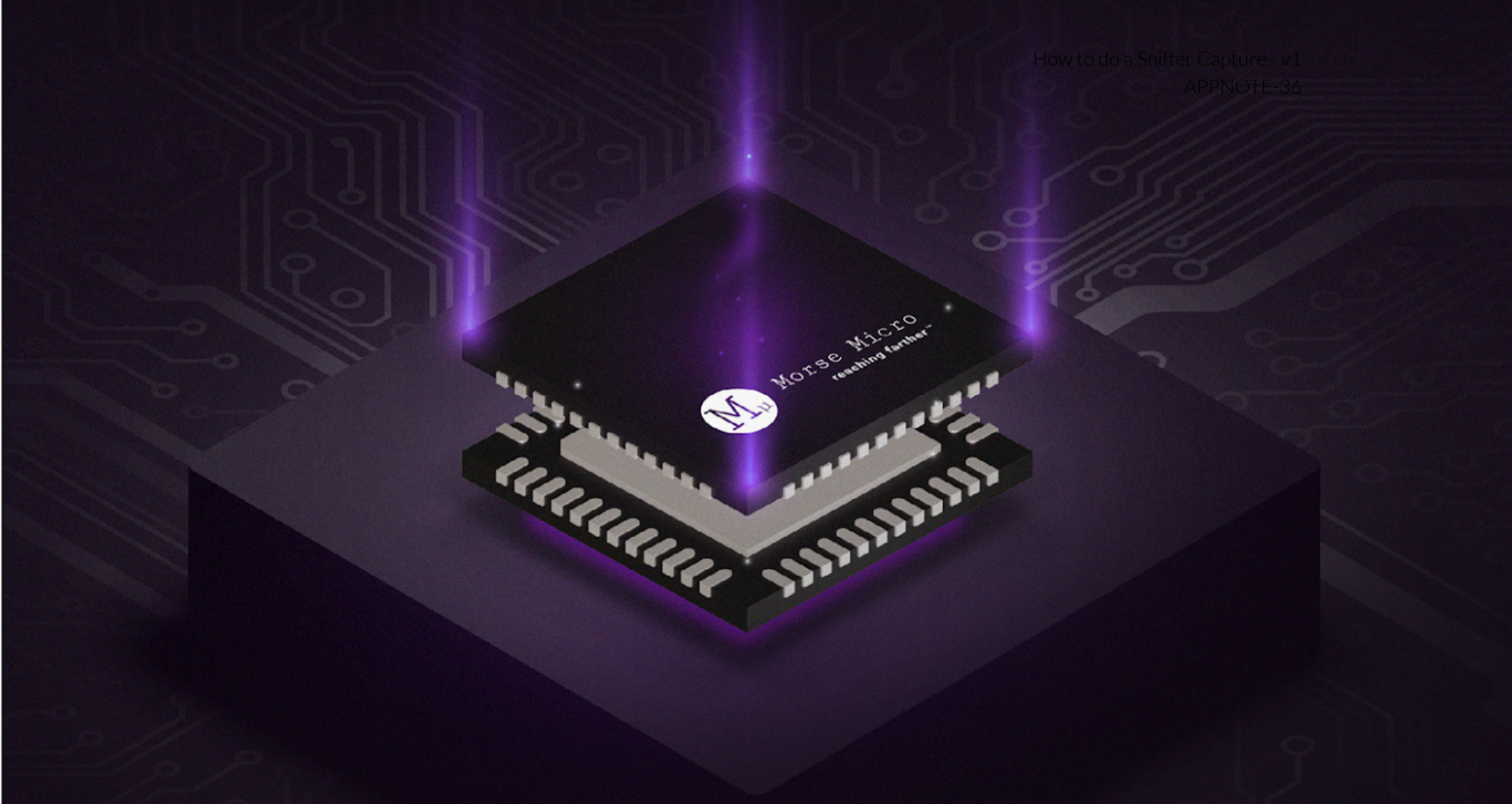
Morse Micro Inc. – USA
40 Waterworks Way
Irvine, CA 92618, UNITED STATES

Office Locations:
Bangalore, India
Cambridge, UK
Hangzhou, China
Irvine, CA - USA
Picton, NSW - Australia
Portola Valley, CA - USA
Shenzhen, China
Taipei, Taiwan

sales@morsemicro.com

www.morsemicro.com

About Morse Micro
Morse Micro is a leading Wi-Fi HaLow fabless semiconductor company based in Sydney, with global offices. As the world's premier Wi-Fi HaLow company, we pioneer next-gen IoT wireless connectivity solutions. Morse Micro is now sampling its Wi-Fi CERTIFIED HaLow MM6108 production silicon: the fastest, smallest, lowest power and longest-range Wi-Fi HaLow chip available in the market.



Morse Micro
reaching farther™