Bluetooth Telemetry Test Module
User Manual and Assembly Instructions
Revision C

Scope	BTM User Guide
Tools & Equipment	Soldering equipment Heat gun ESD safe Hand tools 3/16” and 5/16”(8mm) socket/nut driver/Wrench Torx Plus drivers IP6 and IP8 Wire Strippers/cutter Bench Grinder Safety PPE as necessary
Materials	N/A
Reference Documents	BTM User Guide
Commands	Will be Italic and enclosed in quotes. E.g.”*command*” Keystrokes will be entered in bracketes [Enter]

Table of Contents

Revision History

REV	TECH/ENG	CHANGES
A	James Sievert	Initial Release
B	Deek Farah	Added Content
C	Larry Canady	Formatting edits and added Section 5

1. Introduction

This overview describes the various components, both hardware and firmware, of the Bluetooth Telemetry test Module (BTM). An understanding of these components is important especially when specific firmware elements require update.

2. The Bluetooth TTM (BTM)

The Bluetooth TM or BTM refers to the overall assembly of constituent hardware components. In general, the BTM consists of two main hardware components, a Beaglebone Black development kit and a USB dongle. The picture below shows the Beaglebone Black development kit along with the USB dongle. The Beaglebone Black development kit is circled in blue, while the USB dongle is circled in orange.

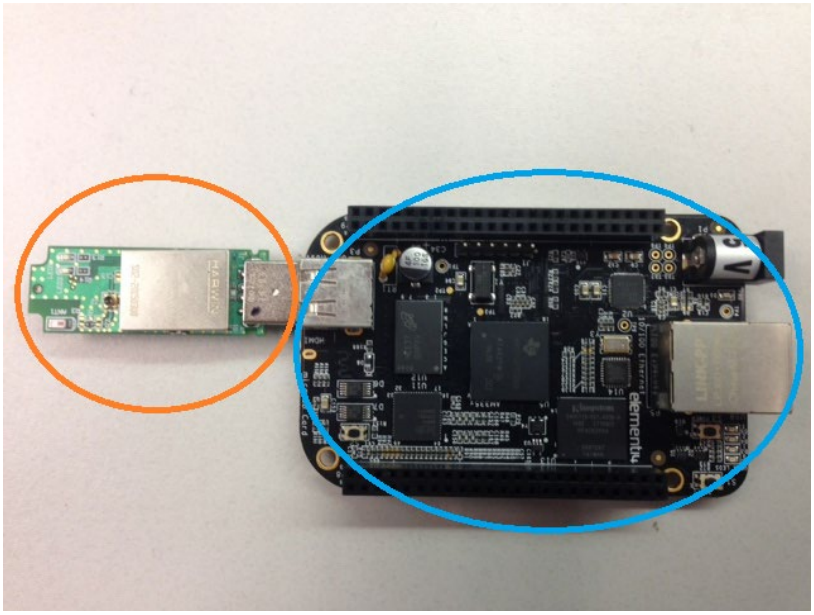


Figure 1: BTM Components

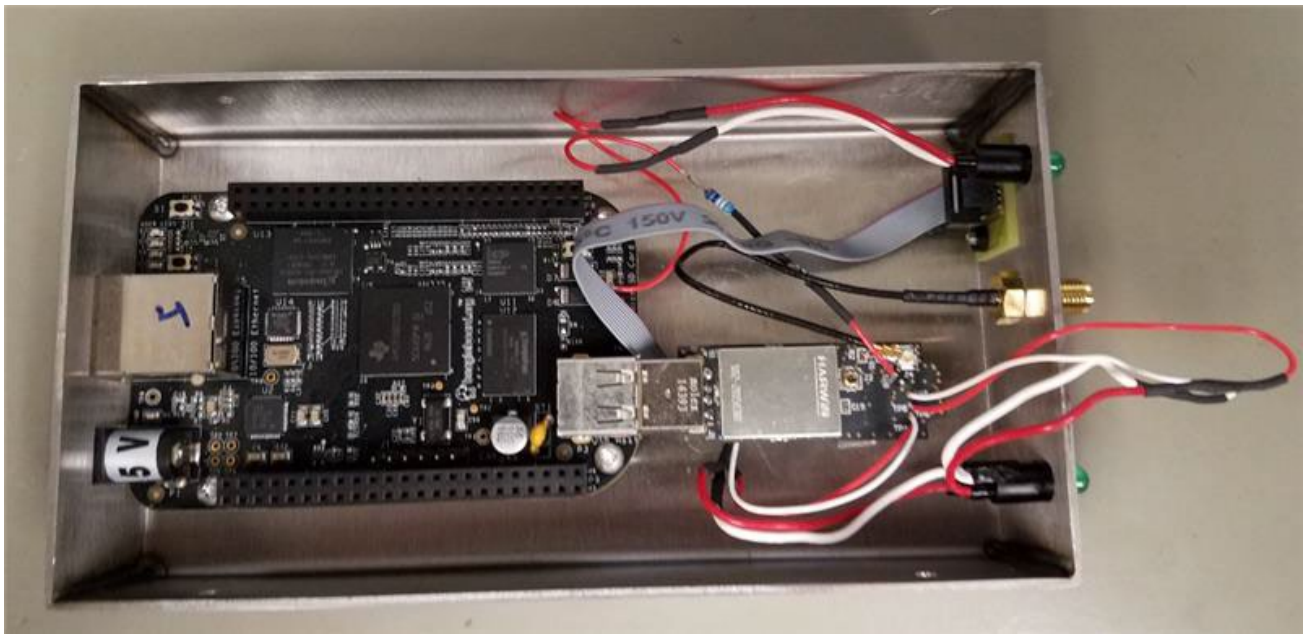


Figure 2: BLE Telemetry Test Module in Production Enclosure

2.1. The Bluetooth Telemetry Module (BTM)

The Bluetooth Telemetry Module or BTM refers to the USB dongle pictured above. The BTM is a Boston Scientific design based on a Nordic nRF52 BLE module. The BTM was conceived as a completely self-contained telemetry subsystem that provides CID-based communication capabilities for all Bluetooth-based Boston Scientific implantable devices. The BTM has applicability beyond that of the BTTM -- like Vision, for example.

The BTM implements the Native portion of the traditional CRM software stack. In general, there are two major firmware elements resident on the BTM:

- The Nordic SoftDevice is the actual BLE stack implementation; and
- The BTM firmware is the Native BSC Bluetooth telemetry implementation combined with a Nordic software framework (SDK) that handles various aspects of the overall nRF52 platform.

2.2. The Bluetooth Telemetry Module Host (Host)

The Bluetooth Telemetry Module Host or simply Host, refers to the Beaglebone Black development kit pictured above. The Host runs a software suite that provides two major functional capabilities:

1. A socket-based API for traditional CID-based CRM tools like RRP
2. An SSH-based command-line interface (CLI) for Host and BTM control.

In general, there are four major firmware elements resident on the Host:

1. The Linux distribution: this is the basic OS for the Host;
2. A number of base Linux customizations: this firmware package provides BSC-specific modifications to the Linux distribution;
3. The socket-based API for CID-based messaging, called the "BTM host firmware package"
4. The SSH-based CLI, called the "TTM firmware package".

The number and specific separation of the software elements are based on the anticipated frequency of update along with the degree of upgrade complexity . The anticipated frequency of update for the Linux distribution and the base Linux customizations is low, while the relative complexity of upgrade for both is high. On the other hand, the anticipated frequency of update for the BTM host and TTM firmware packages is high, while the relative complexity of upgrade for both is low.

3. BTM Packaging and Interfaces

Typical packaging of the complete BTM are shown in the following pictures.

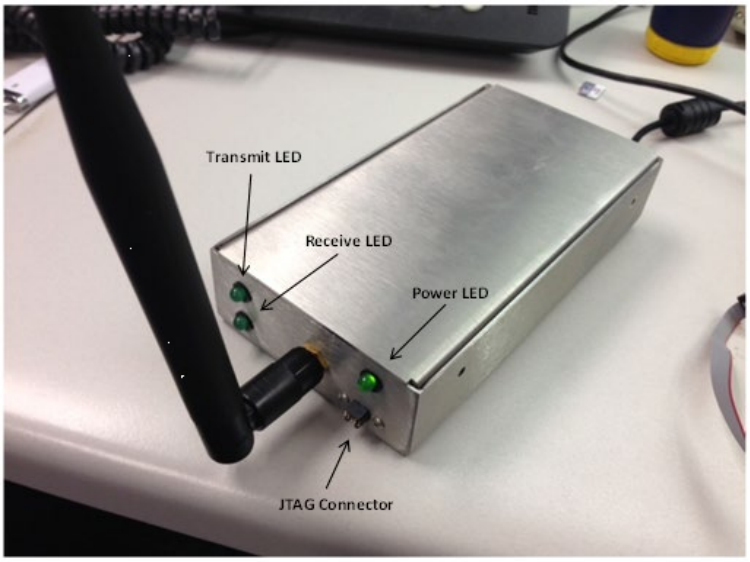


Figure 3: Modele with External Antenna

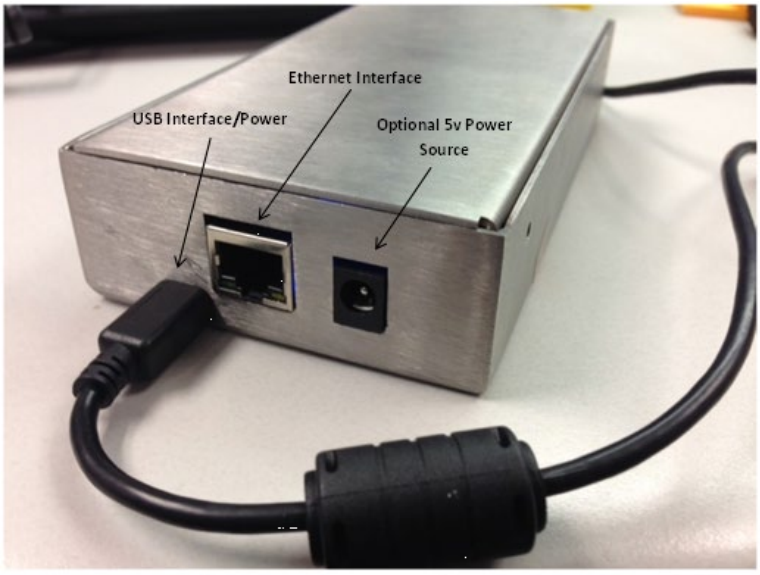


Figure 4: Module Connectivity Ports

Figure 5: Module Label and Antenna

3.1. BTM Connectivity

The BTM provides two primary connectivity options, USB tethering and Ethernet. The BTM may be tethered directly to a host computer via the USB interface. When tethered, the USB interface appears as a network device to the host computer. The BTM may also be directly connected to a network via Ethernet.

3.2. BTM Tethering

At the current time, only BSC Windows platforms support BTM tethering. Follow the procedure below to enable BTM tethering on the host computer:

1. In order to enable USB tethering on the host computer, a set of BeagleBone drivers require installation. These drivers can be found here. Follow the steps under "Step #2: Install drivers".
2. In Windows, go to Start/All Programs/BSC Administrative Tasks/Networks Access.
3. Take note of "Local Area Connection" icons.

4. Connect a mini-USB cable to BTM.
5. Connect the other end of the USB cable in #4 to your host computer.
6. At this point, the BTM platform will boot.
7. After about 30-seconds, a new "Local Area Connection" icon will appear.
8. Right click this icon and select "Properties".
9. Select "Internet Protocol Version 4" and "Properties".
10. Select "Use the following IP address:", and fill in:
    a. IP address: 192.168.7.1
    b. Subnet mask: 255.255.255.252
    c. Default gateway: blank
11. Click "OK", and then "OK" once more.
12. At this point, the BTM should be successfully tethered to the host computer.

3.3. BTM Power Interface

When tethered, the USB interface can be the sole power source to the BTM. When directly connected to a network via Ethernet, the BTM may be powered by via USB as pictured below:

Figure 6: External Power Option

When using Ethernet, the BTM may also be powered via a 5v power source as pictured below:

Figure 7: External 5V Power Option

3.4. BTM Transmit and Receive LEDs

As depicted in a preceding picture, the BTM has both a transmit and a receive LED. The BTM controls both of these LEDs. The BTM will illuminate the transmit LED while sending a data packet to the Host over the USB interface. Likewise, the BTM will illuminate the receive LED while receiving a data packet from the Host over the USB interface. Data packets moving across the USB interface are always less than 512-bytes in length. Given the speed of the USB interface and the relatively small data packet length, illumination of the transmit and receive LEDs is extremely brief unless a significant amount of data is continually streamed across the USB interface.

3.5. BTM Login

After at least 30-seconds following power up, connection to the BTM should be achievable using one of the following methods:

a. Tera Term

   i. File --> New Connection --> TCP/IP

Host: 192.168.7.2

TCP port#: 22

Service: SSH

SSH version: SSH2

Protocol: UNSPEC

b. PuTTY

i. Session:

Host Name (or IP address): 192.168.7.2

Port: 22

Connection type: SSH

[Open]

If you receive a dialog regarding security, respond [Yes]

The credentials for the BTM are ttm/ttm. Following login, the BTM presents the Host CLI which is described below.

3.6. Host CLI

When logged into the BTM, text like the following is presented:

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Oct  6 17:57:39 2016 from 192.168.7.1
>
```

The command prompt is that of the Host CLI mentioned earlier. To see the supported commands, type a question mark "?":

```
  btm         Bluetooth Telemetry Module related commands
  exit        Exits the CLI; equivalent to "quit"
  host        BTM host related commands
  interface   Network interface related commands
  quit        Exits the CLI; equivalent to "exit"

>
```

A question mark can be used at any point to get further command help. For example, type "btm ?", and the following text is presented:

```
> btm
  attach      Initiates a BTM connection to a target device
  connection  BTM connection parameter related commands
  detach      Initiates a BTM disconnect from a target device
  firmware    BTM firmware related commands
  reset       Resets the BTM along with the BTM host service
  rssi        Obtains RSSI samples during a BTM connection to a target device
  test        BTM test commands

> btm
```

Subsequent sections provide detail around most of these commands.

3.7. BTM Ethernet

At the moment, the BTM supports only DHCP addressing via Ethernet. In addition, the BTM supports network name (or hostname) announcement via DHCP. The network name of the BTM is "BTM-" followed by the last four characters of the Beaglebone serial number. The network name of the BTM is available from the Host CLI through the USB interface:

```
> interface network name
BTM-0296
>
```

Once booted, it may take some time for the BTM network name to propagate throughout the DHCP server infrastructure. Also, some network segments within BSC do not propagate this network name at all.

Furthermore, information about the BTM Ethernet interface is also available via the Host CLI through the USB interface:

```
> interface ethernet show
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.40.121.36  netmask 255.255.254.0  broadcast 10.40.121.255
        inet6 fe80::86eb:18ff:fee4:d691  prefixlen 64  scopeid 0x20<link>
        ether 84:eb:18:e4:d6:91  txqueuelen 1000  (Ethernet)
        RX packets 508  bytes 47411 (46.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 47  bytes 5962 (5.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 175

>
```

4. BTM Firmware Installation

The Host CLI can provide the current BTM firmware levels via the following command:

```
> btm firmware show
fw:0.2.149
sd:3.0.0
>
```

One installs BTM firmware via a JTAG pod using the JTAG connector on the front of the BTM. At the moment, only the J-Link JTAG pod is supported. The picture below shows such an installation configuration:

Figure 8: JTAG Interconnect

A keen observer will note that there is a specialized JTAG adapter/cable connecting the JTAG pod to the BTM. This cable can be obtained here.

Follow the procedure below to enable J-Link JTAG functionality on a Windows host:

1. Power the BTM via USB attached to the Windows host.
2. Obtain and install the most recent "nRF5x-Command-Line-Tools-Win32" from here.
3. Connect the J-Link JTAG pod to the Windows host via USB.
4. Connect the J-Link JTAG pod to the BTM as pictured above.
5. Take note of the J-Link JTAG pod serial number located at the bottom of the device (pictured below, circled in blue). This serial number is used in subsequent steps, denoted by `-s serialnumber`

Figure 9: J-Link Serial Number Location

6. On the Windows host, open a command prompt window.
7. cd C:\Program Files (x86)\Nordic Semiconductor\nrf5x\bin
8. As detailed under "The Bluetooth Telemetry Module (BTM)", there are two firmware elements. Updating the SoftDevice will erase all firmware on the BTM. Consequently, updating the SoftDevice implies updating the BTM Firmware.

i. SoftDevice firmware has a name similar to the following: `s132_nrf52_3.0.0_softdevice.hex`.

ii. Use the following commands to update the SoftDevice:

```
nrfjprog -s serialnumber --program s132_nrf52_3.0.0_softdevice.hex -f nrf52 --
chiperase

nrfjprog -s serialnumber -reset -f nrf52
```

iii. BTM Firmware has a name similar to the following: `btm_0.2.149.hex`.

iv. Use the following commands to update the BTM Firmware:

```
nrfjprog -s serialnumber --program btm_0.2.149.hex -f nrf52 --sectorerase
nrfjprog -s serialnumber -reset -f nrf52
```

9. At this point, the BTM firmware installation is complete. This can be confirmed through the Host CLI using the following command:

```
> btm firmware show
fw:0.2.149
sd:3.0.0
>
```

4.1. Host Firmware Installation

As detailed under "The Bluetooth Telemetry Module Host (Host)", there are four Host firmware elements. These four Host firmware elements are initially distributed together as a single .tgz file to form the root file system of the Host. In addition, the BTM host and TTM firmware packages are distributed as individual .deb (Debian installation) files for ease of upgrade. The Host root file system installation procedure uses a microSD card, while upgrades to the BTM host and TTM firmware packages make use the Host CLI.

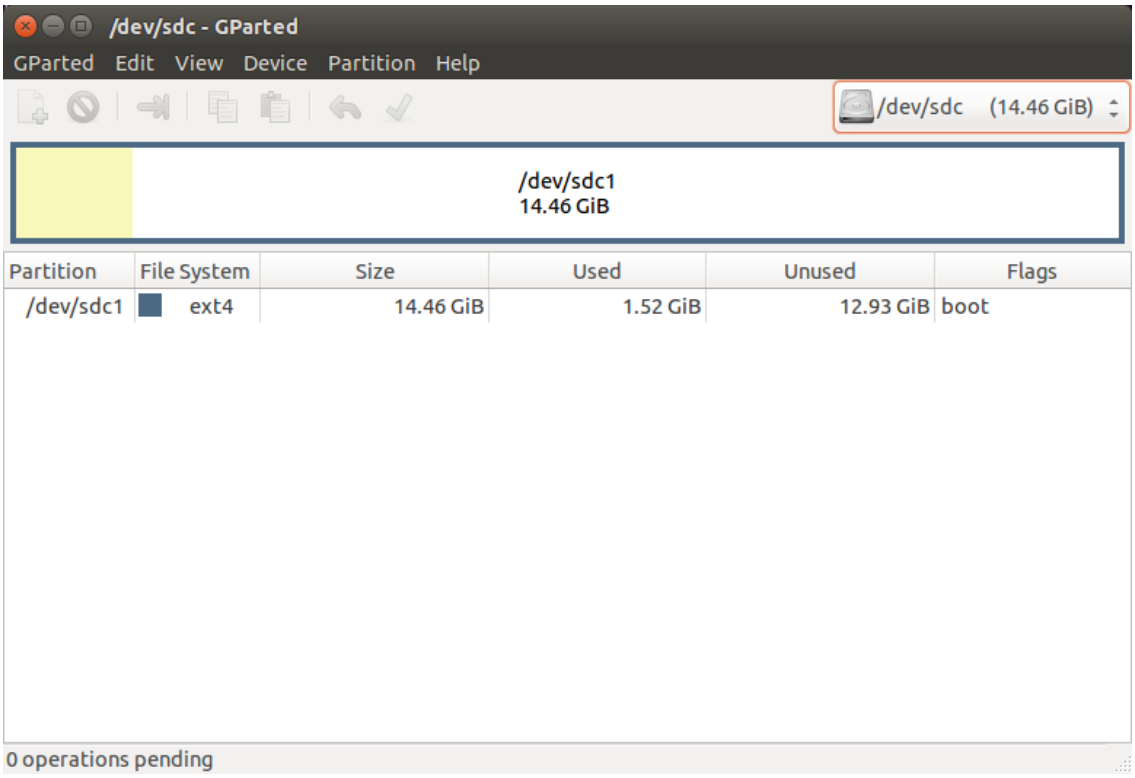
The Host CLI can provide the current Host firmware levels via the following command:

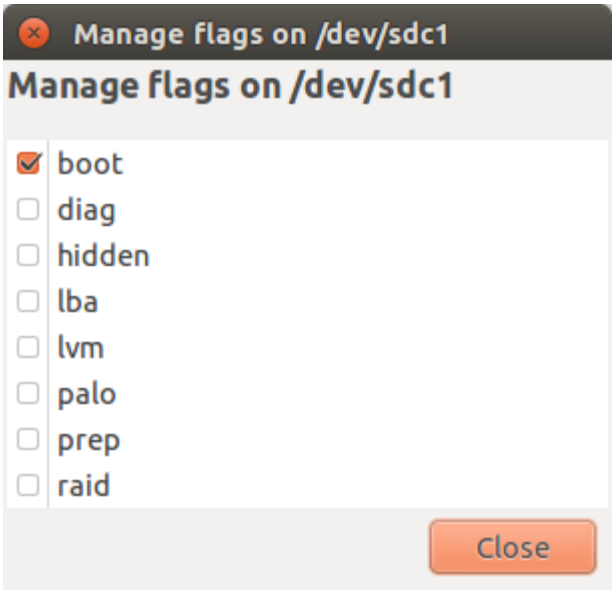
```
> host firmware show
linux:0.1-3
base:0.1-1
ttm:0.1-2
btmhost:0.1-2
>
```

4.2. microSD Card Creation

The Host root file system .tgz file has a name similar to the following: BTM-rootfs-0.1-3.tgz. This file is a compressed Linux tar archive. Its contents need to be expanded on to a microSD card. The microSD card must have a minimum size of 4G. The microSD card must consist of a single partition formatted as a Linux ext4 file system. Practically speaking, the creation of the microSD card must be done through Linux. While pretty much any Linux distribution can be used, these instructions pertain specifically to Ubuntu.

1. Use gparted to create a single ext4 file system on the microSD card. Also make sure that the "boot" flag is checked as pictured below:





2. If the partition already exists and the boot flags are set properly, simply format the partition to ext4. This will erase all data from the partition.

3. From a command prompt, untar Host root file system .tgz file to the microSD card. In general, Ubuntu will automatically mount the ext4 file system under /media/user-name/partition-UUID, e.g. /media/g041195/52481f28-3b13-448e-9d91-7170978ab824. Assuming such, use the following command to populate the microSD card:

```
sudo tar -xvzf BTM-rootfs-0.1-3.tgz -C /media/g041195/52481f28-3b13-448e-9d91-7170978ab824
```

4. Eject the microSD card, and the microSD card is now ready to use.

4.3. Host Root File System Installation

Flash memory on the Beaglebone host is the final destination for the root file system. The microSD card produced in the "microSD Card Creation" step facilitates installation to the Beaglebone host flash memory. The microSD slot is located on the bottom of the Beaglebone host as pictured below:

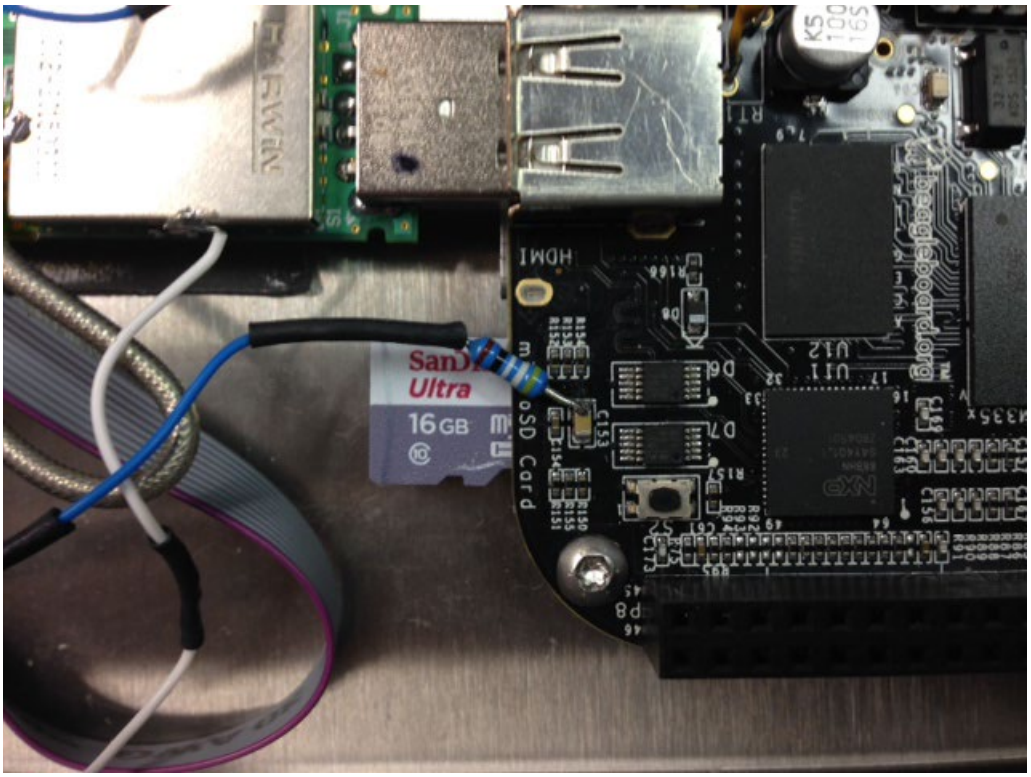


Figure 10: MicroSD Slot Location

1. Remove power to the BTM.
2. If necessary, remove the top of the BTM enclosure.
3. Insert the microSD card into the slot until the microSD card "clicks" into place.
4. Apply power to the BTM.
5. After a short period of time, blue LEDs on the Beaglebone host will "walk" back and forth as shown in the following video clip:

   <<Walking LEDs.MOV>>

6. After several minutes, the Beaglebone host will automatically power off.

   i. Note that occasionally, the Beaglebone does not power off after the LEDs complete the "walking" sequence. If this occurs, restart from Step #1 above.

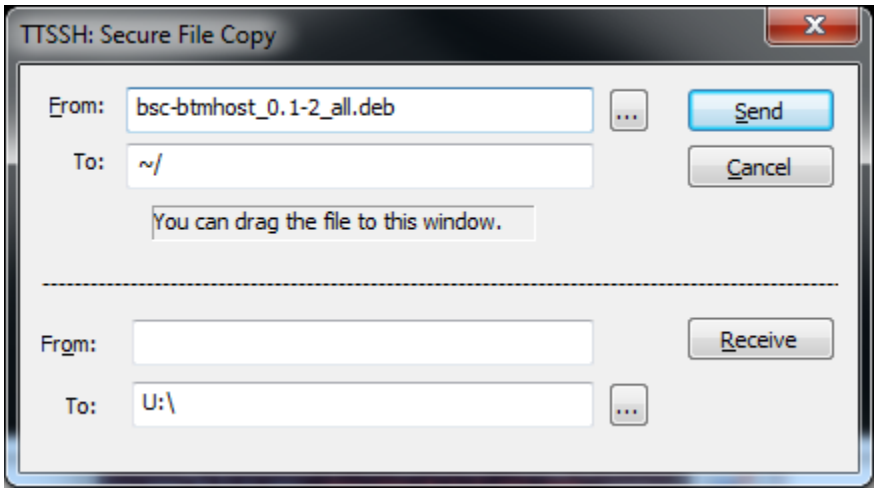
7. At this point, installation of the Host root file system to the Beaglebone host is complete.
8. Begin the microSD card removal process by pushing the card "in" slightly. The card will "click" free of the holder. The microSD card may now be removed from the holder.

4.4. BTM Host and TTM Firmware Package Installation

The BTM host firmware package has a name similar to the following: bsc-btmhost_0.1-2_all.deb. To install a BTM host firmware package:

1. Log into the BTM as detailed under "BTM Login".
2. Use SCP to transfer the BTM host firmware package to the BTM. TeraTerm provides direct support for SCP. Other SCP implementations may also exist.

   In TeraTerm, go to File/SSH SCP…. TeraTerm will display a "Secure File Copy" dialog. In the top-most "From" text box, enter the BTM host firmware package file name as shown below, and click on "Send":



3. Once the SCP operation completes, from the Host CLI, type the following and press enter:

   > host firmware install btmhost

4. Once complete, reboot the BTM from the Host CLI:

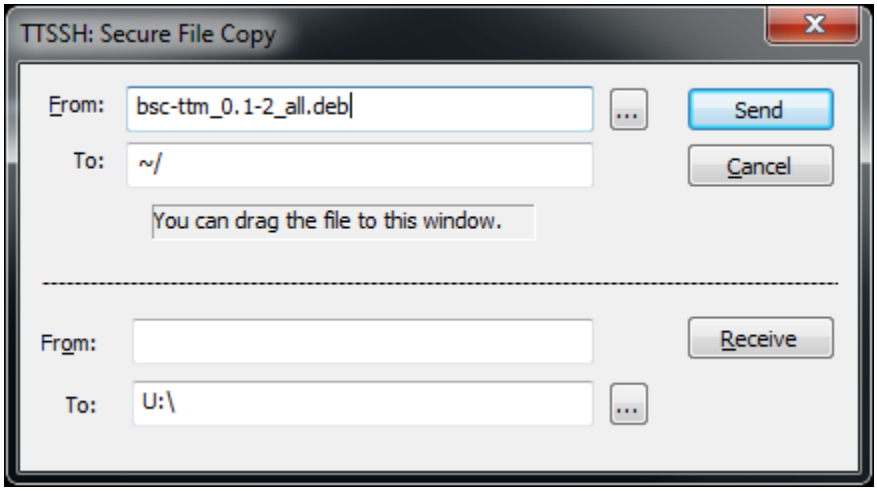
   > host reboot

The TTM firmware package has a name similar to the following: bsc-ttm_0.1-2_all.deb. To install a TTM firmware package:

1. Log into the BTM as detailed under "BTM Login".

2. Use SCP to transfer the BTM host firmware package to the BTM. TeraTerm provides direct support for SCP. Other SCP implementations may also exist.

In TeraTerm, go to File/SSH SCP…. TeraTerm will display a "Secure File Copy" dialog. In the top-most "From" text box, enter the BTM host firmware package file name as shown below, and click on "Send":



1. Once the SCP operation completes, from the Host CLI, enter the following and press enter:

   > host firmware install ttm

2. Once complete, reboot the BTM from the Host CLI:

   > host reboot

5. FCC Compliance

Testing has been performed to confirm the module is compliant per the applicable portions of the FCC rules and regulations:

- Per FCC 15.19(a)(3) and (a)(4) This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
- Per FCC 15.21, no modification of this equipment is allowed unless approved by Boston Scientific. Changes or modifications not expressly approved by Boston Scientific could void the user's authority to operate the equipment.

Per compliance requirements, this transmitter must not cause harmful interference to devices operating nearby and must accept interference that may be caused by such stations, including interference that may cause undesired operation. This transmitter shall be used only in accordance with the FCC Rules governing the Medical Device Radiocommunication Service. Analog and digital voice communications are prohibited. Although this transmitter has been approved by the Federal Communications Commission, there is no guarantee that it will not receive interference or that any particular transmission from this transmitter will be free from interference.