Getting the Android Link Key for Classic Bluetooth® Decryption

Bluetooth devices on an encrypted link share a common “link key” used to exchange encrypted data. For a *Bluetooth* sniffer, such as the ComProbe BPA 600, to be able to decrypt the encrypted data, it must also have this shared link key. For obvious security reasons, the link key is never sent over the air, so either the user must get the key out of one of the devices being sniffed and supply the key to the sniffer or the sniffer must create the key itself.

Bluetooth devices using the Android operating system have a "developer" option that will provide the link key for Classic *Bluetooth* decryption. This procedure will use the developer options to obtain the Android HCI (Host Controller Interface) log that contains the link keys for all active links..

What You Need to Get the Android Link Key

The process applies to the Android 4.4 or later operating system.

- Android device with Bluetooth enabled and paired with another *Bluetooth* device.
- ComProbe Protocol Analysis System installed on your computer
- Android Debug Bridge (optional)

Note: Each Android device model can vary in screen organization, layout and format. The directions in this paper are based on known typical Android device. Refer to the manufacturer's manual,on-line help, or technical support for detailed information about your particular device.

Activating Developer options

The Android HCI log will contain the link key for an active *Bluetooth* link.

1. On the Android device go to Settings,
2. Select About.
3. In the About screen tap on Build number eight times. At some point you will see a notice similar to "You are now a developer!".

Note: On some devices the build information may be under one or more sub-screens below the About screen. Also the number of taps may vary; in most cases the screen will provide

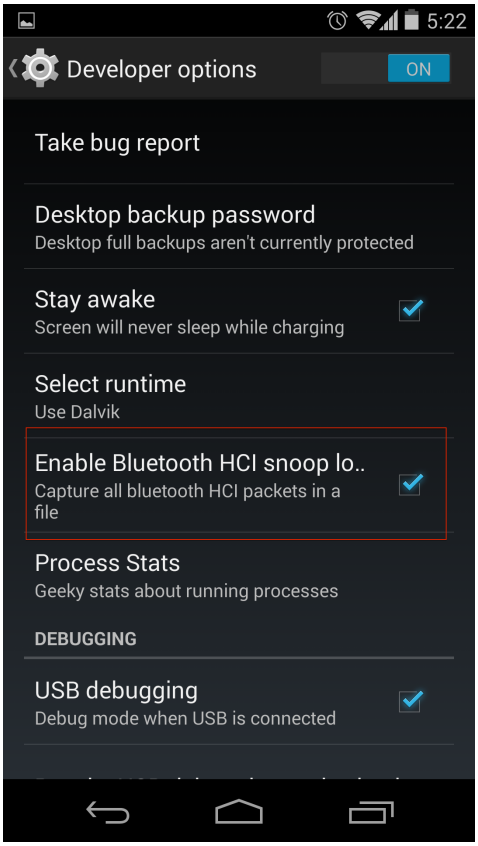
status of your tap count.

4. Return to the Settings screen and you will see Developer options

Retrieving the HCI Log

Now that Developer options have been activated on the Android device, you can retrieve the HCI log.

1. On the Android device go to Settings.
2. Select Developer options.
3. Click to enable Bluetooth HCI snoop logging.
4. Return to the Settings screen and select Developer options.
5. In the Developer options screen select Enable Bluetooth HCI snoop log. The log file is now enabled.



Typical Android Developer options screen

6. On the Android device turn off *Bluetooth*.
7. Turn on *Bluetooth*.
8. Reboot the Android device.

The HCI log file is now being generated and is saved to */sdcard/btsnoop_hci.log*.

Note: Samsung devices have a slightly different location for the btsnoop file.

There are two options for retrieving the HCI log from the Android device.

a. Attach the Android device to your computer. The file */sdcard/btsnoop_hci.log* is in the root of one of the mountable drives. Copy the file to directory *C:/Users/Public/Public Documents/Frontline Test Equipement/My Capture File/*.

b. The second option is to use the Android Debug Bridge (ADB)using the following steps. The debug bridge is included with Android Software Developer Kit.

(1). On the Androd device Development screen, select Android debugging or USB debugging.

(2). Connect your computer and Android device with a USB cable.

(3). Open a terminal on your computer and run the following command.

```
adb devices.
```

(4). Your Android device should show up in this list confirming that ADB is working.

```
List of devices attached
XXXXXXXXXXX device
```

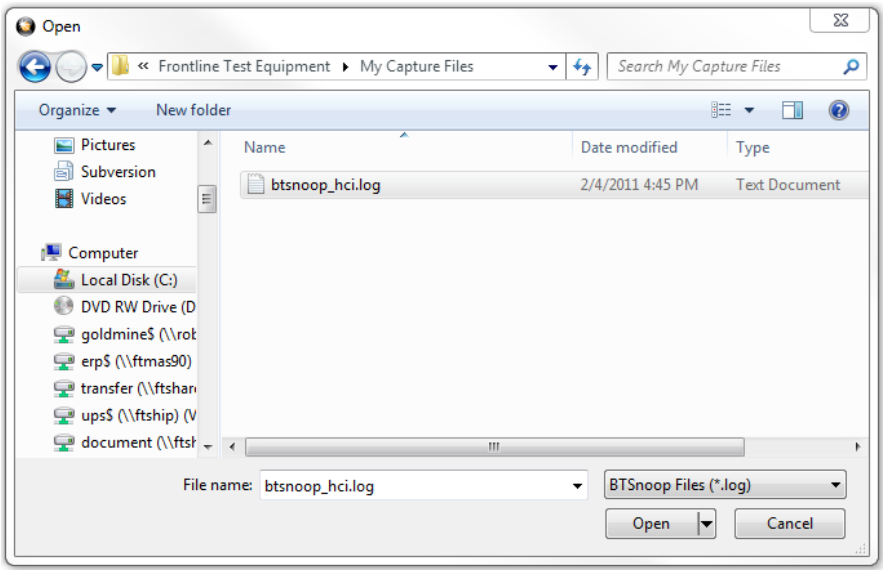
(5). In the terminal enter the following command to copy the HCI Log to your computer.

```
adb pull /sdcard/btsnoop_hci.log
```

Using the ComProbe Software to Get the Link Key

You will load the HCI Log file *btsnoop_HCI.log* into the ComProbe Protocol Analysis System on your computer as a capture file. Then you can use the Frame Display to locate the link key.

1. Activate the ComProbe Protocol Analysis System. (Refer to the ComProbe BPA 600 User Manual on fte.com).
2. From the Control window menu select File, Open Capture File....
3. When the Open window appears, set the file type to BTSnoop Files (*.log). If not already selected navigate to the *My Capture Files* directory and select *btsnoop_hci.log*.

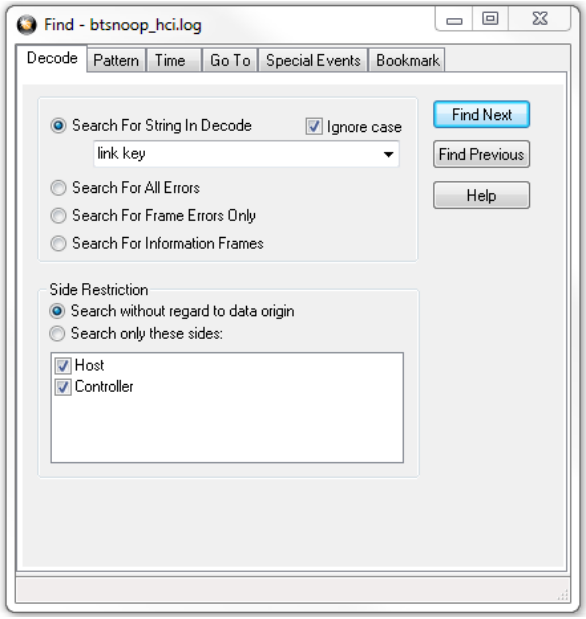


Select Capture File

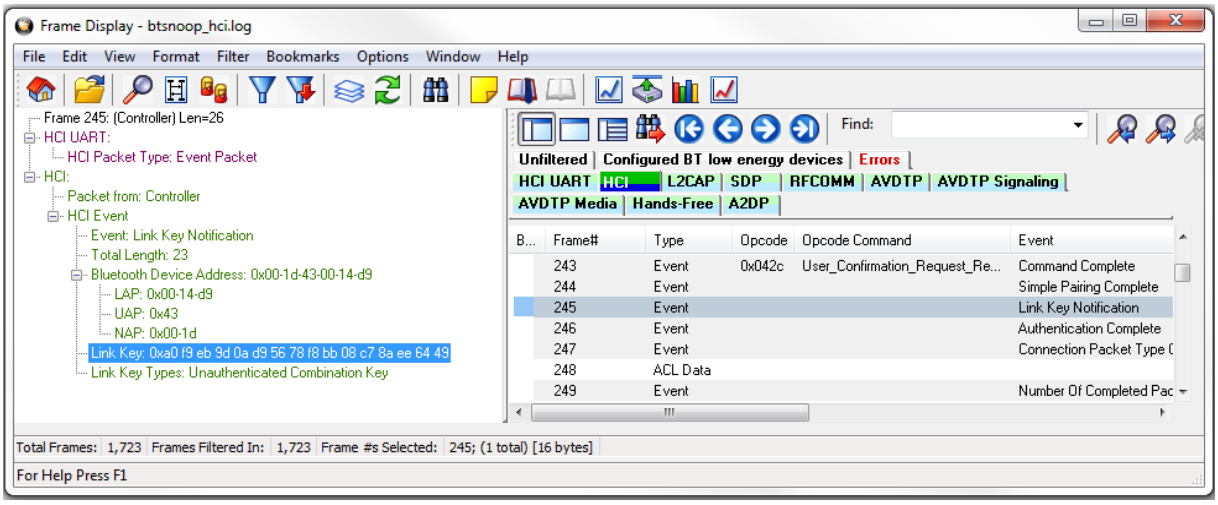
4. Open the Frame Display

5. In the Frame Display protocol tabs select HCI. (See image below)

6. Select Find , click on the Decode tab, and enter "link key" in the Search for String in Decode. Check the Ignore Case option. Click on Find Next until the Event column shows Link Key Notification.



In the Frame Display Detail pane, expand HCI and HCI Event where the Link Key is shown. Copy and paste the Link Key into the appropriate BPA 600 datasource dialog. (See the example below)



Frame Display Showing Link Key Notification Event with the Link Key

Technical Support

Technical support is available in several ways. The online help system provides answers to many user related questions. Frontline's website has documentation on common problems, as well as software upgrades and utilities to use with our products.

Web: http://www.fte.com, click Support

Email: tech_support@fte.com

If you need to talk to a technical support representative, support is available between 9am and 5pm, U.S. Eastern time, Monday through Friday. Technical support is not available on U.S. national holidays.

Phone: +1 (434) 984-4500

Fax: +1 (434) 984-4505

Author: John Trinkle with Joe Skupniewitz

Publish Date: 30 September 2014