TELEDYNE LECROY
Everywhereyoulook™

Getting Android Link Key for Classic Decryption

Revision Date: 4/20/2020

Document Disclaimer

The information contained in this document has been carefully checked and is believed to be reliable. However, no responsibility can be assumed for inaccuracies that may not have been detected.

Teledyne LeCroy reserves the right to revise the information presented in this document without notice or penalty.

Trademarks and Servicemarks

Teledyne LeCroy, Frontline, Frontline Test System and Wireless Protocol Suite are registered trademarks of Teledyne LeCroy, Inc.

The following are trademarks of Teledyne LeCroy, Inc.
Sodera™
Sodera LE™
802.11™
X240™
Audio Expert System™
Audio Rating Metric™
ProbeSync™

The Bluetooth SIG, Inc. owns the Bluetooth® word mark and logos, and any use of such marks by Teledyne LeCroy, Inc. is under license.

Microsoft and Windows are registered trademarks of Microsoft Inc.

All other trademarks and registered trademarks are property of their respective owners. All other trademarks are property of their respective companies.

Copyright

Table of Contents

Introduction

Bluetooth devices on an encrypted link share a common “link key” used to exchange encrypted data. For a Bluetooth sniffer, such as the Frontline x240 and Sodera, 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.

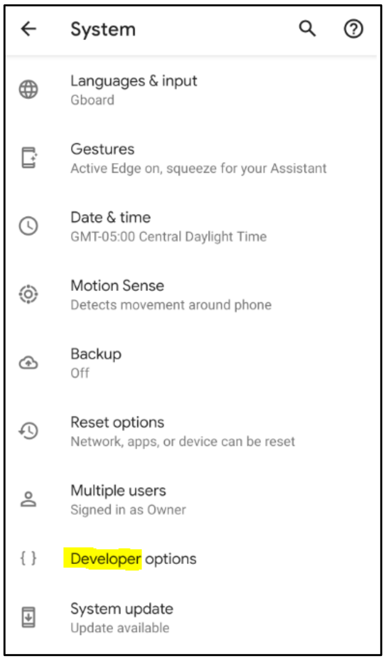
1. Android device with Bluetooth enabled and paired with another Bluetooth device
2. Wireless Protocol Suite installed on your computer
    - Resource: http://fte.com/support/WPS-download.aspx?demo=X240&iid=X240
3. Android Debug Bridge (adb)
    - Resource: https://developer.android.com/studio/command-line/adb

Note:
Each Android device model can vary in screen organization, layout and format. The directions in this paper are based on a known 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!"
4. Return to the Settings screen and you will see a Developer Options menu item



System

Languages & input
Gboard

Gestures
Active Edge on, squeeze for your Assistant

Date & time
GMT-05:00 Central Daylight Time

Motion Sense
Detects movement around phone

Backup
Off

Reset options
Network, apps, or device can be reset

Multiple users
Signed in as Owner

Developer options

System update
Update available

Note:
On some devices the Developer Options menu will be located under Settings -> System -> Advanced

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.

Generating the HCI Log

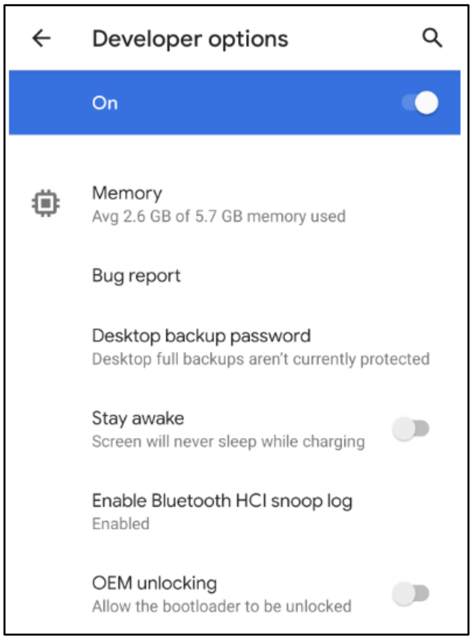
Note:
The process for obtaining a link key depends on the manufacturer, model and operating system of your device. Below is a general guide for Android devices. Please refer to any documentation specific to your device.

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

1. Go to Settings
2. Select System
3. Select the Advanced drop down
4. Select Developer Options
5. Turn Developer Options ON
6. Enable Bluetooth HCI snoop logging
7. Pair and Connect devices
8. Turn OFF Bluetooth

9. Turn ON Bluetooth

The HCI Bluetooth snoop log file is now being generated.



Developer options

On

Memory
Avg 2.6 GB of 5.7 GB memory used

Bug report

Desktop backup password
Desktop full backups aren't currently protected

Stay awake
Screen will never sleep while charging

Enable Bluetooth HCI snoop log
Enabled

OEM unlocking
Allow the bootloader to be unlocked

There are multiple ways to retrieve a link key, they are all very manufacturer and device dependent. Outlined below are the two most common ways.

Updated (Newer) Method:

Use ADB (Android Debug Bridge) to generate and save a bug report. The bug report folder will contain a Bluetooth HCI log containing link keys currently associated with the device.

After enabling Develop Options and enabling Bluetooth HCI snoop log, do the following:

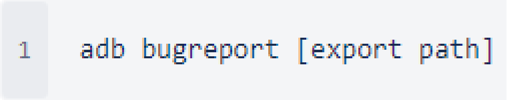
1. Open a terminal on your computer and run the following command

```
adb devices
```

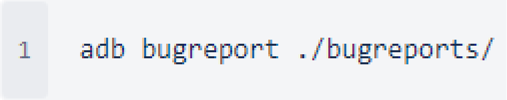
2. Confirm your device is connected

```
List of devices attached
9XX81FFAZ00XX3 device
```

3. Generate and save the bug report locally



```
adb bugreport [export path]
```



```
adb bugreport ./bugreports/
```

4. The bug report will now be saved to the folder specified in the previous command. Extract the generated .zip and locate the btsnoop_hci.log file on the device
    - Example log location: FS/data/misc/bluetooth/logs/

Note:
You may also use the “Bug report” or “Take bug report” within the Developer Options of the device. This option will save the bug report log in a manufacturer specific folder on the device.

Alternative (Older) Method:

After enabling Developer Options and enabling Bluetooth HCI snoop log, the HCI log file is now being generated and saved to the device, typically located at /sdcard/btsnoop_hci.log

Note:
Some devices have a different location for the btsnoop file, refer to its documentation.

Retrieving the HCI Log

The suggested 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.

    1. Copy the file to your PC via local file system explorer

B. Use Android Debug Bridge (ADB) and the following steps. The debug bridge is included with Android Software Developer Kit.

    1. On the Android device Development screen, select USB debugging
    2. Connect your computer and Android device with a USB cable
    3. Allow your PC access from the device, if necessary

4. Open a terminal on your computer and run the following command

```
adb devices
```

5. Your Android device should show up in this list confirming that ADB is working

```
List of devices attached
9XX81FFAZ00XX3 device
```

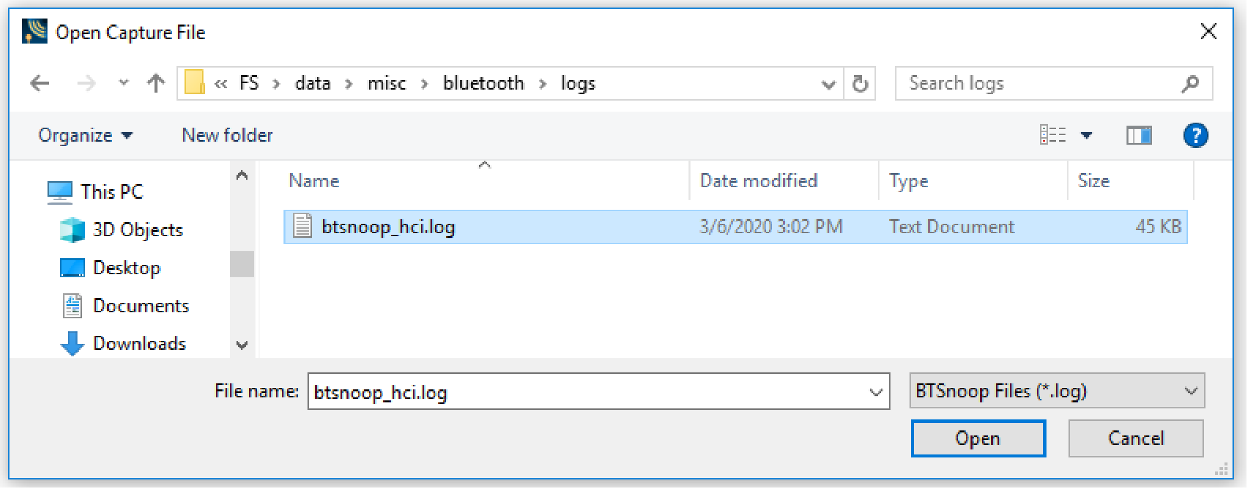
6. In the terminal use the pull command and save the file locally

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

Using the Wireless Protocol Suite to Get the Link Key

You will open the HCI Log file btsnoop_HCI.log with the Wireless Protocol Suite on your computer, similar to a capture file. Then, use the Summary view to search for the link key.

1. Launch the Wireless Protocol Suite. (Refer to the WPS User Manual located in the Help and Tools/Documentation desktop folder of your installation)
2. From the Start Page select File -> Open....
3. When the Open window appears, **set the file type to BTSnoop Files (*.log)**. and load your btsnoop_hci.log file



Open Capture File

« FS › data › misc › bluetooth › logs

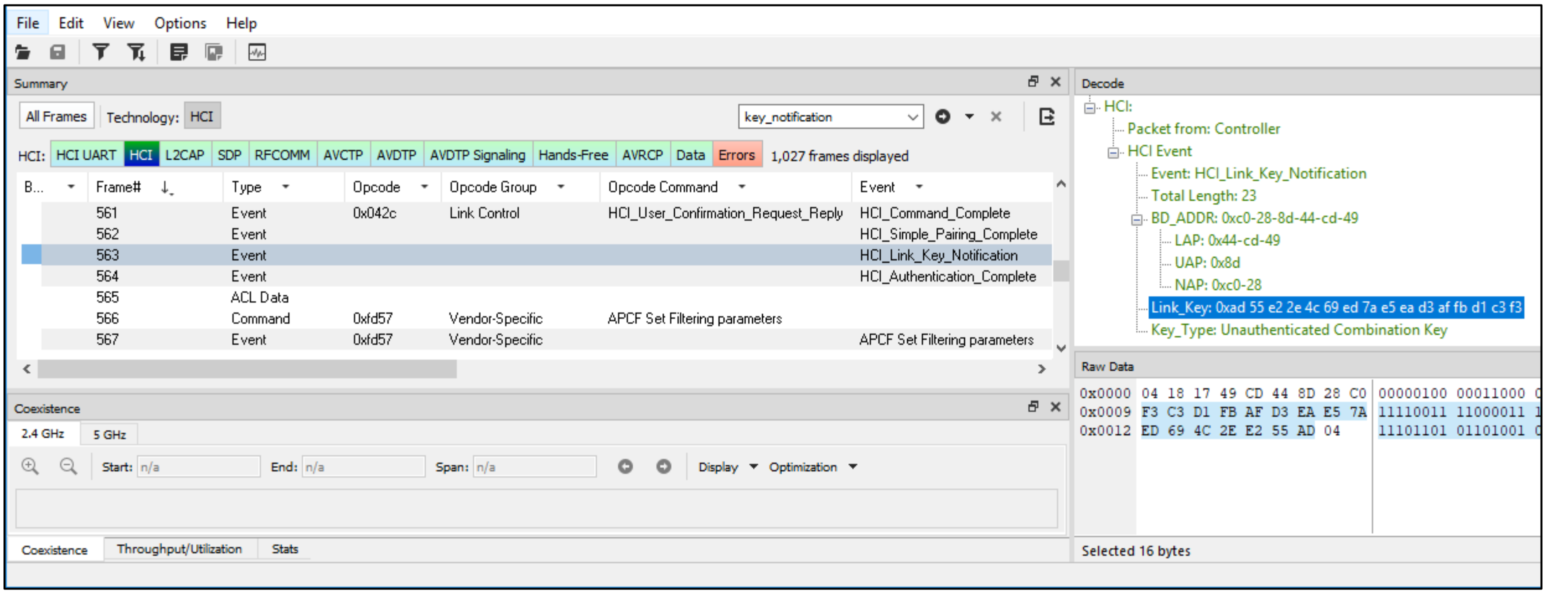
Name	Date modified	Type	Size
btsnoop_hci.log	3/6/2020 3:02 PM	Text Document	45 KB

File name: btsnoop_hci.log

BTSnoop Files (*.log)

Select Capture File

4. From the Summary pane select the HCI protocol tab. From the Search Box, search for the "HCI_Link_Key_Notification" event. Alternatively, you may search for "key_notification" or "link_key"
5. The Link Key should now be available in the Decode pane. You may right-click and copy it to paste into the appropriate WPS datasource dialog



1,027 frames displayed

B...	Frame#	Type	Opcode	Opcode Group	Opcode Command	Event
	561	Event	0x042c	Link Control	HCI_User_Confirmation_Request_Reply	HCI_Command_Complete
	562	Event				HCI_Simple_Pairing_Complete
	563	Event				HCI_Link_Key_Notification
	564	Event				HCI_Authentication_Complete
	565	ACL Data				
	566	Command	0xfd57	Vendor-Specific	APCF Set Filtering parameters	
	567	Event	0xfd57	Vendor-Specific		APCF Set Filtering parameters

```
HCI:
    Packet from: Controller
    HCI Event
        Event: HCI_Link_Key_Notification
        Total Length: 23
        BD_ADDR: 0xc0-28-8d-44-cd-49
            LAP: 0x44-cd-49
            UAP: 0x8d
            NAP: 0xc0-28
        Link_Key: 0xad 55 e2 2e 4c 69 ed 7a e5 ea d3 af fb d1 c3 f3
        Key_Type: Unauthenticated Combination Key
```

```
0x0000  04 18 17 49 CD 44 8D 28 C0  00000100 00011000 0
0x0009  F3 C3 D1 FB AF D3 EA E5 7A  11110011 11000011 1
0x0012  ED 69 4C 2E E2 55 AD 04     11101101 01101001 0
```

Selected 16 bytes

Link Key Shown in Decode Pane