思澈平台 Log 抓取指南

前言

概述

- 本文档主要介绍思澈平台产品各种类型 Log 的抓取方法及注意事项，相关操作以手表产品类型为例来进行介绍

读者对象

- 适用于产品测试以及研发工作人员，帮助在分析解决对应问题过程中顺利抓取 Log 信息

适用平台

芯片平台	软件版本
SF32LB55X	SDK / Solution all version
SF32LB58X	SDK / Solution all version
SF32LB56X	SDK / Solution all version
SF32LB52X	SDK / Solution all version

缩略语/术语/关键字

关键字	英文全名	中文释义
HCI	Host Controller Interface	主机控制接口，属于蓝牙协议栈的一部分

更新记录

文档版本	发布日期	作者	修改说明
1.0	2024-11-06	yungao	Initial release.

1. 大/小核 HCPU/LCPU 及 HCI Log 抓取方法

1.1 所需工具及资源

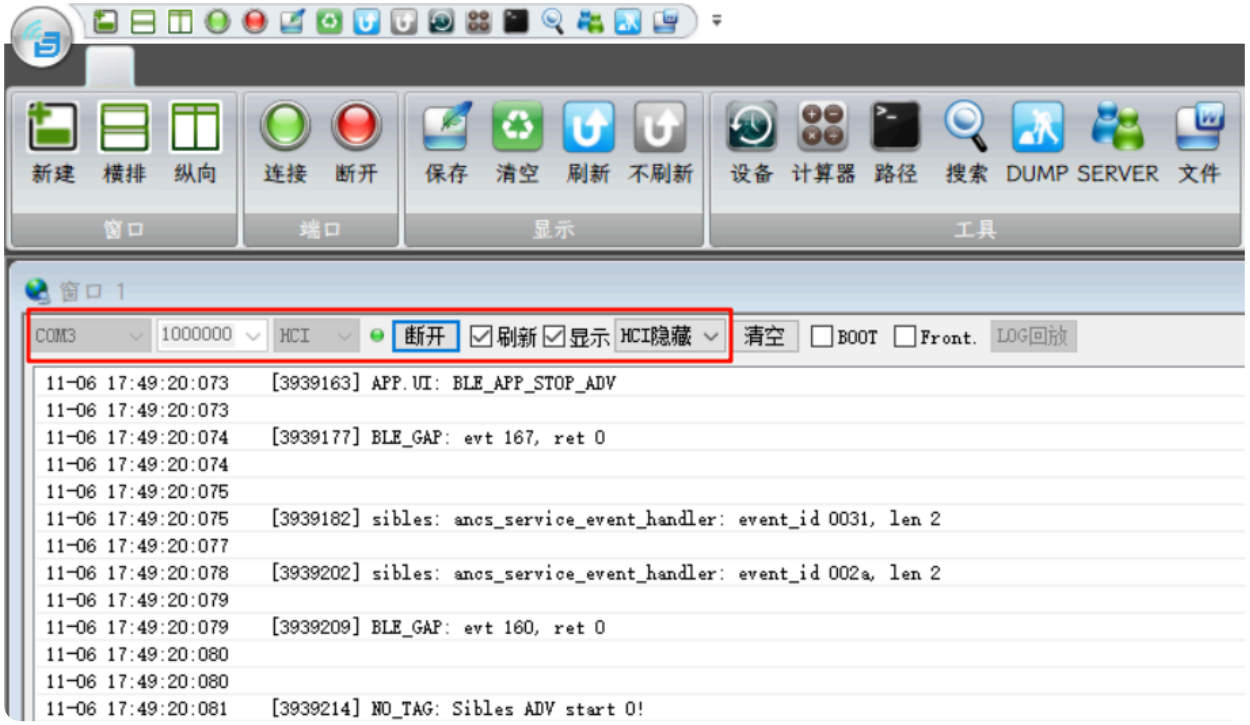
- 硬件
  - 测试产品 (如手表)，需要飞线 (串口或 JLINK SWD)，具体飞线可以参见对应手表 SCH/PCB 飞线图
  - 串口板或 J-Link (JTAG 仿真器)

- 软件/工具
  - SifliTrace，如版本 SifliTrace_v2.2.5

1.2 抓取方法

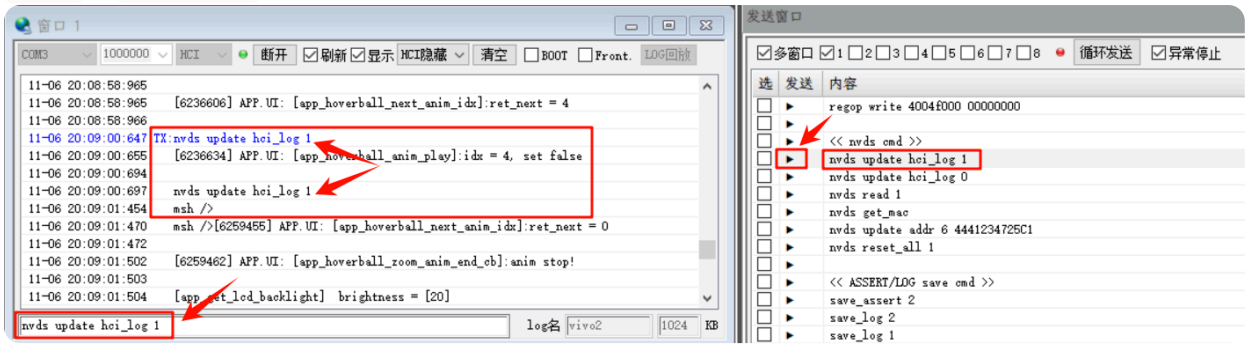
1.2.1 通过串口抓取方法

1. 将手表串口 GND/TX/RX 连线分别连接至串口板的 GND/RX/TX 端口，将串口板插入 PC USB 口，同时确认对应正确的 COM 口
2. PC 侧打开 SifliTrace 工具，选择对应正确的串口 (如 `COM3`) 、波特率 (如 `1000000` bps)、数据类型 (如 `HCI`) 及 HCI 数据显示选项 (如 `HCI隐藏`)，手表侧上电开机，SifliTrace 工具中点击 `连接` 按钮进行连接，正常情况下会有对应 Log 输出显示。`连接` 按钮旁边的指示灯显示了当前的端口连接状态，红色为未连接，灰色为连接失效，绿色为连接成功状态

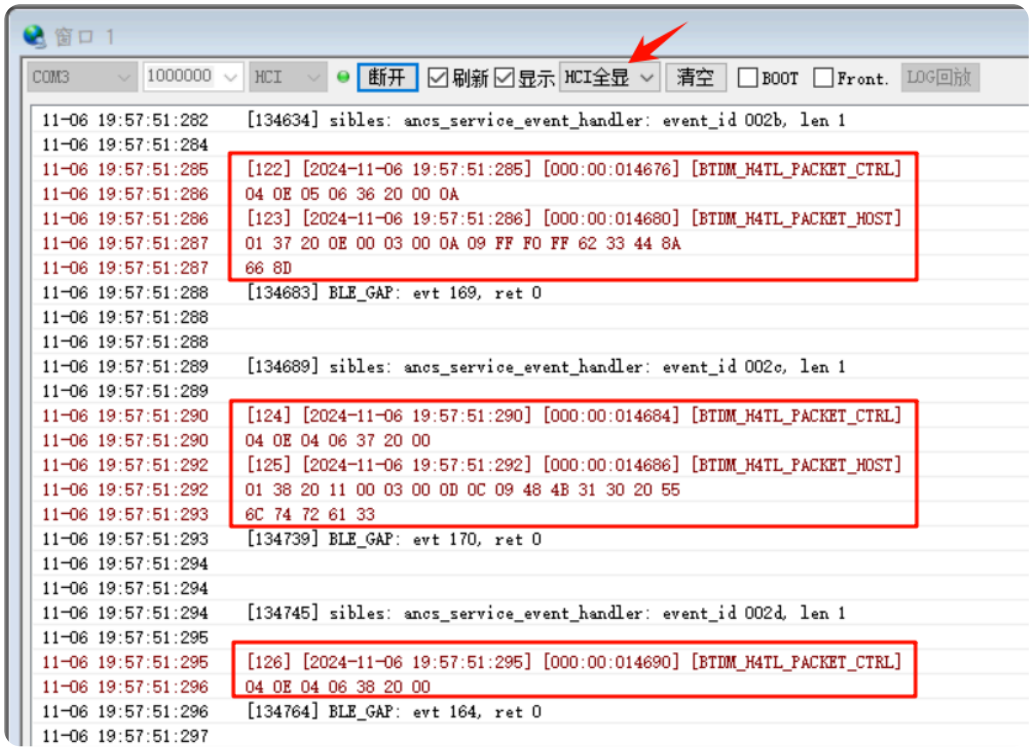


3. 抓取完毕以后，通过点击 `断开` 按钮以停止 Log 抓取，点击 `保存` 按钮后对应 Log 信息会以文件形式保存下来，存储位置可以通过点击 `路径` 按钮直接打开，Log 对应文件分为如下几种类型，对应 Log 文件名会包含对应窗口序号、端口号、时间戳信息
   - `.txt` -- 对应串口大、小核 Log
     - 示例
       - `窗口1_COM3_(2024-11-06-17-43-44)_ui.txt`
   - `.bin`、`.bintime`、`.pcap` -- 对应 HCI 及网络 Log
     - 示例
       - `窗口1_COM3_(2024-11-06-17-43-44).bin`
       - `窗口1_COM3_(2024-11-06-17-43-44).bintime`
       - `窗口1_COM3_(2024-11-06-17-43-44).pcap`

4. 抓取 HCI Log 需要手表侧配置打开 HCI Log，具体配置方法为通过串口下发 `nvds update hci_log 1` 指令来打开 HCI Log 输出 (反之关闭 HCI Log 输出通过指令 `nvds update hci_log 0`)，具体打开方法可以手动输入指令并回车执行，或者直接点击执行已有常用命令 (参见图例)。如果关闭了 HCI Log 输出，在 SifliTrace 打印界面 (即使打开了 HCI 选项及 HCI 显示选项) 就不会显示对应 HCI Log 信息，同时对应的存储 `.bin`、`.bintime` 文件 Size 会比较小或为 0

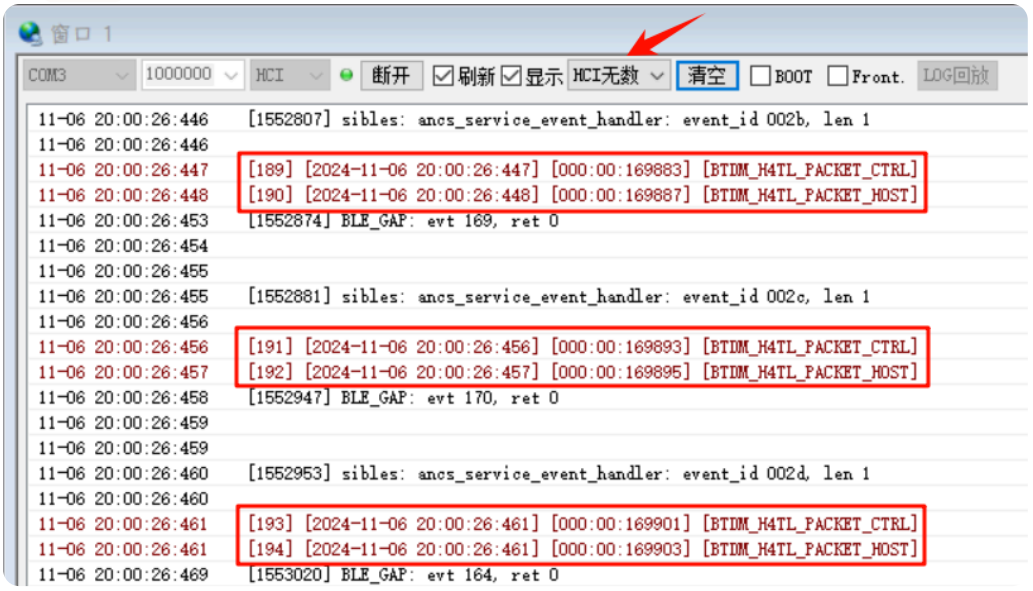


- **注意事项**
  - 如果只抓取 HCPU/LCPU 串口 Log (不需要抓取 HCI)，数据类型选项可以设置为 `字符`
  - 抓取 HCI Log 需要将数据类型选项设置为 `HCI`，另外为避免在 HCI 数据量较大的 (如蓝牙通话、A2DP 音乐等) 情况下出现 HCI 数据抓取不全的问题，需要将 HCI 数据显示选项设置为 `HCI隐藏` 或 `HCI无数据`，这样对应的 HCI Log 不会显示及保存到 `.txt` 文件中 (而是保存到了对应的 `.bin`、`.bintime` 文件中)，HCI 显示选项及示例如下
    - `HCI全显示`
      - 在 `.txt` 中包含所有 HCI 数据

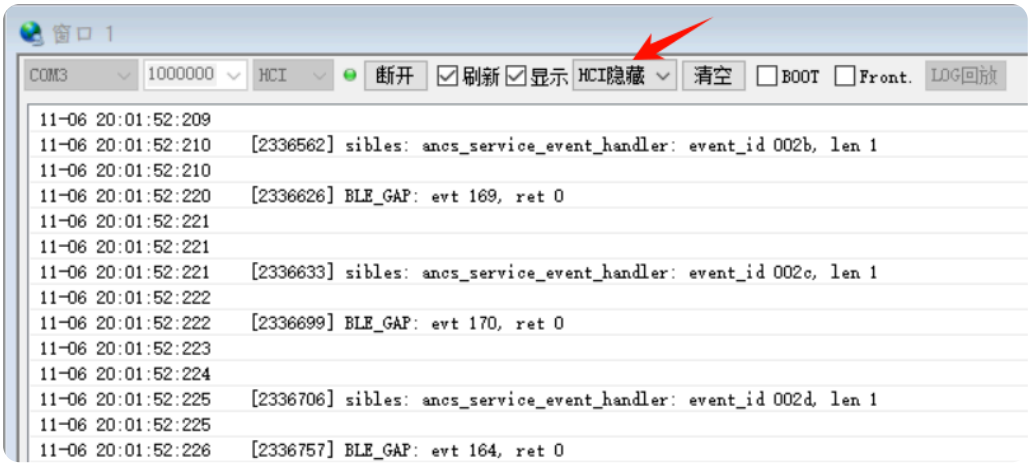


    - `HCI无数据`

- 在 `.txt` 中包含 HCI 头信息，但不包括完整数据



- `HCI隐藏`
  - 在 `.txt` 中不包含任何 HCI 信息，HCI 信息包含在另外的 `.bin` 文件中



- 通过指令 `nvds update hci_log 1` 打开 HCI Log 以后发现还是没有 HCI Log 输出，可以尝试将手表进行一次正常关机/重启，部分芯片 (如 SF32LB52X) 下发开关 HCI Log 指令后需要重启手表才能生效
- SifliTrace 工具支持打开多个 Log 窗口，如果需要同时抓取多个串口 Log 数据 (如同时抓取 HCPU 大核和 LCPU 小核对应的串口 Log)，可以打开多个窗口同时进行连接和 Log 抓取

1.2.2 通过 J-Link 抓取方法

1. 将手表 (JLINK SWD) 与 J-Link 仿真器通过各连接线进行连接，并通过 USB 线将 J-Link 仿真器连接至 PC USB 端口，PC 端需要安装 Segger J-Link 程序及对应驱动 (参见 思澈编译开发环境配置指导 文档说明)
2. PC 侧打开 SifliTrace 工具，除端口选择 J-Link segger 对应的端口外，其他选项与通过串口抓取 Log 配置相同
3. 开始抓取、停止和保存 Log 与通过串口抓取 Log 方法相同

- **注意事项**
  - 通过 J-Link segger 端口抓取 Log 过程中，如果手表进入休眠状态后 Log 信息也会停止输出，所以在需要抓取系统休眠状态下 Log 信息的场景是不能使用 J-Link 来抓取的

2. 手机侧 HCI Log 抓取方法

- 有时分析问题需要参考手机侧的 HCI log，由于手机系统及型号又比较多，不同系统和型号打开或抓取 HCI Log 方法会存在差异，基本上分为 Android、iOS、HarmonyOS 几类，以下介绍几种主要品牌抓取 HCI Log 的方法，供实际抓取过程中进行参考

2.1 Android / HarmonyOS 手机

2.1.1 HUAWEI / Honor

1. 手机打开 HCI Log 相关设置
   - 手机系统中依次进入 `设置` → `关于手机`，连接点击版本号信息后提示打开开发者模式后并打开 `USB调试` 选项，进入 `系统和更新`，点击 `开发者选项` 菜单项，打开 `开启蓝牙HCI信息收集日志` 选项
2. 进行测试或复现问题直至完成
3. 提取记录的 HCI Log 信息，手机侧存储的 HCI Log 位置在 `/data/log/bt` 路径下
   - 手机连接 PC，保证 adb 可正常使用 (如果不可用或不能识别到手机设备，则需要安装对应产品驱动程序)
   - 打开 CMD 控制台 (如按下快捷键 `Windows + R` 后输入 `cmd`) 窗口，执行 `adb pull /data/log/bt d:\log` 即将 Log 信息从 `/data/log/bt` 路径下拷贝至 PC 的 `d:\log` 路径下，HCI Log 文件命令格式如 `btsnoop_hci_xxxxxxxx.log`

- **注意事项**
  - 如果发现手机侧没有 HCI Log 保存下来，可以尝试将手机重启后再进行测试抓取和提取日志信息

2.1.2 OPPO / Realme

1. 手机打开 HCI Log 相关设置
   - 进入设置，打开开发者模式
   - 在拨号界面输入 `*#800#` 进入异常反馈界面，选择蓝牙异常项，点击红框设置项改为开发者模式，然后返回点击开始抓取，选择为不重启方式抓取
2. 进行测试或复现问题，抓取 HCI Log 会先自动关闭手机蓝牙，需手动再次打开蓝牙，测试或复现问题完毕后选择结束抓取
3. 提取记录的 HCI Log 信息
   - 提取手机内部存储空间中如下路径下的 `.caf` 文件

- `\内部共享存储空间\oppo_log\`
- `\内部共享存储空间\Android\data\com.coloros.logkit\files\Log\`
- `/storage/emulated/0/oppo_log`
- `/storage/emulated/0/Android/data/com.coloros.logkit/files/Log`

2.1.3 MIUI 小米、红米

1. 手机打开 HCI Log 相关设置
   - 拨号界面输入 `*#*#5959#*#*` 执行日志开启抓取，任务栏提示执行进度
2. 进行测试或复现问题直至完成，拨号界面输入 `*#*#5959#*#*` 结束日志抓取
3. 提取记录的 HCI Log 信息
   - 将存储于手机 `/MIUI/debug_log` 路径下的日志取出
   - 连接手机至 PC 通过 `adb bugreport` 指令同步抓取 bugreport 信息 (如 `bugreport-0227-14564.zip`)

2.1.4 三星

1. 手机打开 HCI Log 相关设置
   - 手机系统中依次进入 `设置` → `关于手机` → `软件信息`，连接点击版本号信息后提示打开开发者模式后，进入 `开发者选项` 菜单，点击 `启用蓝牙HCI监听日志` 设置为 `启用`
2. 重启手机，开始测试或复现问题直至完成
3. 提取记录的 HCI Log 信息
   - 进入拨号界面输入 `*#9900#` 然后点击 `RUN DUMPSTATE/LOGCAT` 选项并等待结束后按 `COPY TO SDCARD(INCLUDE CP RAMDUMP)`
   - 将手机连接到 PC 并找到 `log` 文件夹，导出对应 Log 信息如 `log\bluetooth\btsnoop_hci_xxxxxxxx.cfa`

2.1.5 Google

1. 手机打开 HCI Log 相关设置
   - 打开手机 `开发者模式`
   - 在开发者模式中打开 `蓝牙HCI获取`
2. 进行测试或复现问题直至完成
3. 连接手机至 PC 通过执行 `adb bugreport` 指令，会在当前 PC 目录下生成包含 HCI Log 的 `debuglogger` 目录，获取对应 Log 文件如 `debuglogger\connsyslog\bthci\CsLog_xxxxxxxx`

2.1.6 IQOO

1. 手机打开 HCI Log 相关设置过程与 Google 手机类似
2. 进行测试或复现问题直至完成

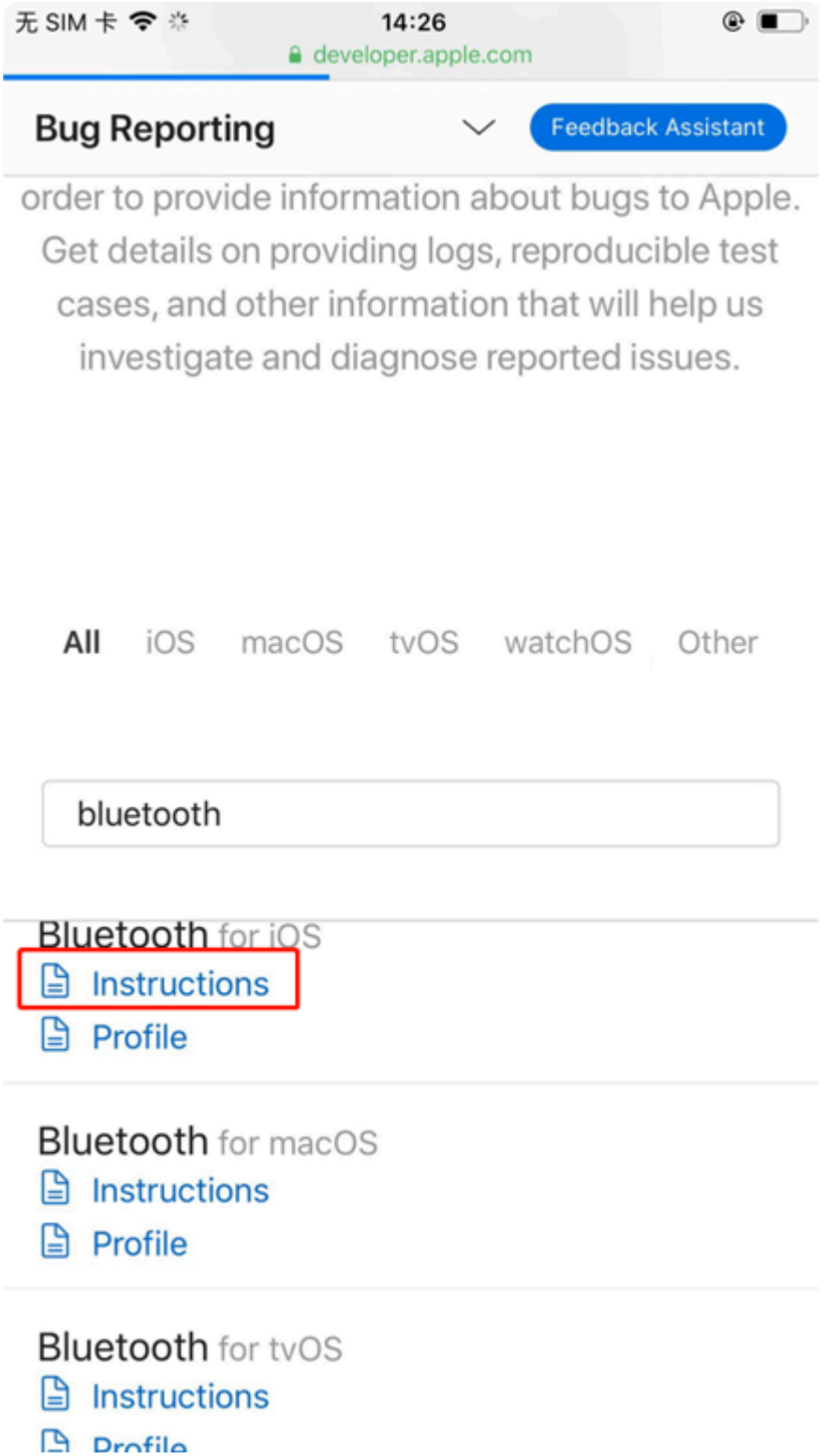
3. 提取记录的 HCI Log 信息
    - 通过 `adb bugreport` 指令提取 bugreport 信息
    - 通过手机上的蓝牙配置文件 `bt_stack.conf` 中的 `BtSnoopFileName` 配置项值来确认具体 HCI Log 存储路径，如 `BtSnoopFileName=/sdcard/btsnoop_hci.log`
        - 蓝牙配置文件路径 - `/etc/bluetooth/bt_stack.conf`
        - HCI Log 默认存储路径
            - MTK - `/sdcard/mtklog/btlog/btsnoop_hci.log`
            - QualComm (高通) - `/sdcard/btsnoop_hci.log`

2.1.7 ViVo

1. 手机打开 HCI Log 相关设置
    - 进入拨号界面输入 `*#*#112#*#*` 开启日志抓取，任务栏提示执行进度
2. 进行测试或复现问题直至完成
3. 提取记录的 HCI Log 信息
    - 在拨号界面输入 `*#*#112#*#*` 结束日志抓取，日志文件存放于内部存储中的 `Android/data/com.vivo/logs/system/` 路径下
    - HCI Log 在手机中的存储路径是通过 `/system/bt/conf/bt_stack.conf` 定义，根据定义到对应路径下提取 HCI Log，注: 访问此路径需要 root 权限

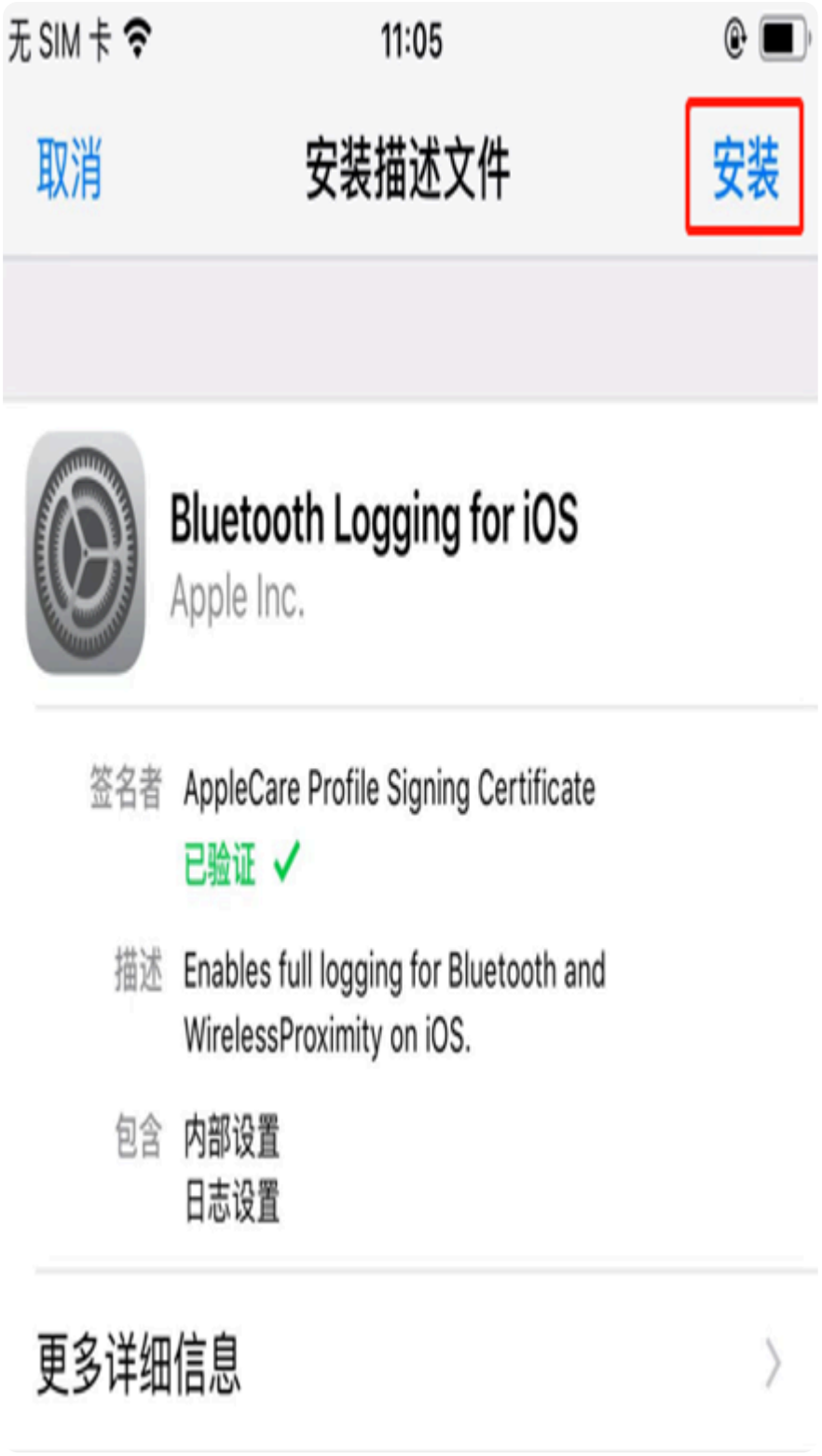
2.2 iOS 手机

1. 手机端配置文件的下载和安装，需要注册 Apple Developer 账号
    - 手机浏览器打开 https://developer.apple.com/bug-reporting/profiles-and-logs/?name=bluetooth 链接，登录 Apple Developer 账号，找到 `Bluetooth for iOS`、 `Instructions` 内容并下载


无 SIM 卡
14:26
developer.apple.com
Bug Reporting
Feedback Assistant
order to provide information about bugs to Apple.
Get details on providing logs, reproducible test
cases, and other information that will help us
investigate and diagnose reported issues.
All
iOS
macOS
tvOS
watchOS
Other
bluetooth
Bluetooth for iOS
Instructions
Profile
Bluetooth for macOS
Instructions
Profile
Bluetooth for tvOS
Instructions


无 SIM 卡
16:00
download.developer.apple.com
Bluetooth Logs: iOS
For Bluetooth issues on iOS devices, please follow the instructions below to collect logs.
Enabling Logging
1. Download the profile and install it on the iOS device.
If necessary, email the profile or use AirDrop to transfer the profile to the iOS device.
2. Reboot the iOS device.
3. Reproduce the issue. Important: Note the date and time issue occurred and add this information to your report.
4. Trigger a sysdiagnose by simultaneously pressing and releasing both volume buttons + Side (or Top) button.
Notes:
- The sysdiagnose is triggered upon button release.
- On an iPhone you will feel a short vibration when a sysdiagnose is successfully triggered.
- It's important to trigger the sysdiagnose process as soon as possible after the problem occurs, even if the logs can't be synced off the device until later. Also, the profile expires after 3 days so you'll need to reinstall the profile after 3 days in case you want to trigger another sysdiagnose.
5. Wait 10 minutes for the diagnostic gathering to complete.
6. AirDrop the file to your Mac computer or sync the device with your host computer to transfer the file.
7. Attach the file listed at the path below under Log Locations to your report.
iPhone Log Locations
iOS:
Go to: Settings.app > Privacy > Analytics > Analytics Data > (Locate the sysdiagnose file and AirDrop it to your Mac computer).
macOS:
~/Library/Logs/CrashReporter/MobileDevice/[Your_Device_Name]/DiagnosticLogs/sysdiagnose
Note: "~/Library/.." actually translates to: /Users/[Your User Name]/Library/..
The "/Users/[Your User Name]/Library/.." folder is hidden by default in macOS. To expose the folder, hold the option key while clicking the Finder's Go menu and the Library folder will appear in the menu. Any time you see a placeholder like "[Your Device Name]" or, "[Your User Name]" you should

- 安装配置文件及确认安装状态 (在 `设置` 里面的 `通用` 界面查看是否有描述文件，如有表明已经安装完成)


无 SIM 卡
11:05
取消
安装描述文件
安装
Bluetooth Logging for iOS
Apple Inc.
签名者 AppleCare Profile Signing Certificate
已验证
描述 Enables full logging for Bluetooth and WirelessProximity on iOS.
包含 内部设置
日志设置
更多详细信息


17:31
已安装描述文件
完成
Bluetooth Logging for iOS
Apple Inc.
签名者 AppleCare Profile Signing Certificate
已验证
描述 Enables full logging for Bluetooth and WirelessProximity on iOS.
包含 内部设置
日志设置
更多详细信息

2. PC 端下载、安装 `iTunes` 并打开和登录 iOS 帐号
3. 进行测试或复现问题直至完成
4. 连接电脑和手机，同时按下和释放两个音量按键 + 侧方 (或顶部) 按键触发系统诊断，在 iPhone 上当系统诊断成功触发时会感到短暂的震动，等待几分钟以保证 sysdiagnose 日志存储完毕，通过 `iTunes` 导出日志信息，PC 端 Log 位置 `C:\Users\<User_Name>\AppData\Roaming\AppleComputer\Logs\CrashReporter\MobileDevice<Device_Name>\DiagnosticLogs\sysdiagnose`，从压缩包中提取 `logs\Bluetooth` 目录下的内容

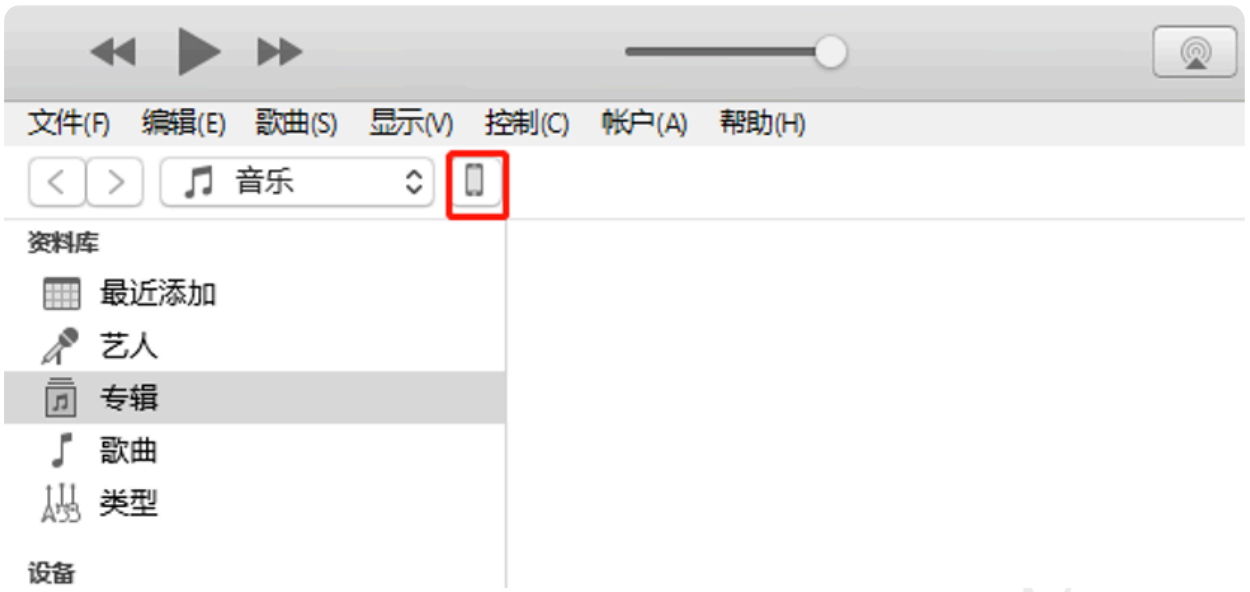
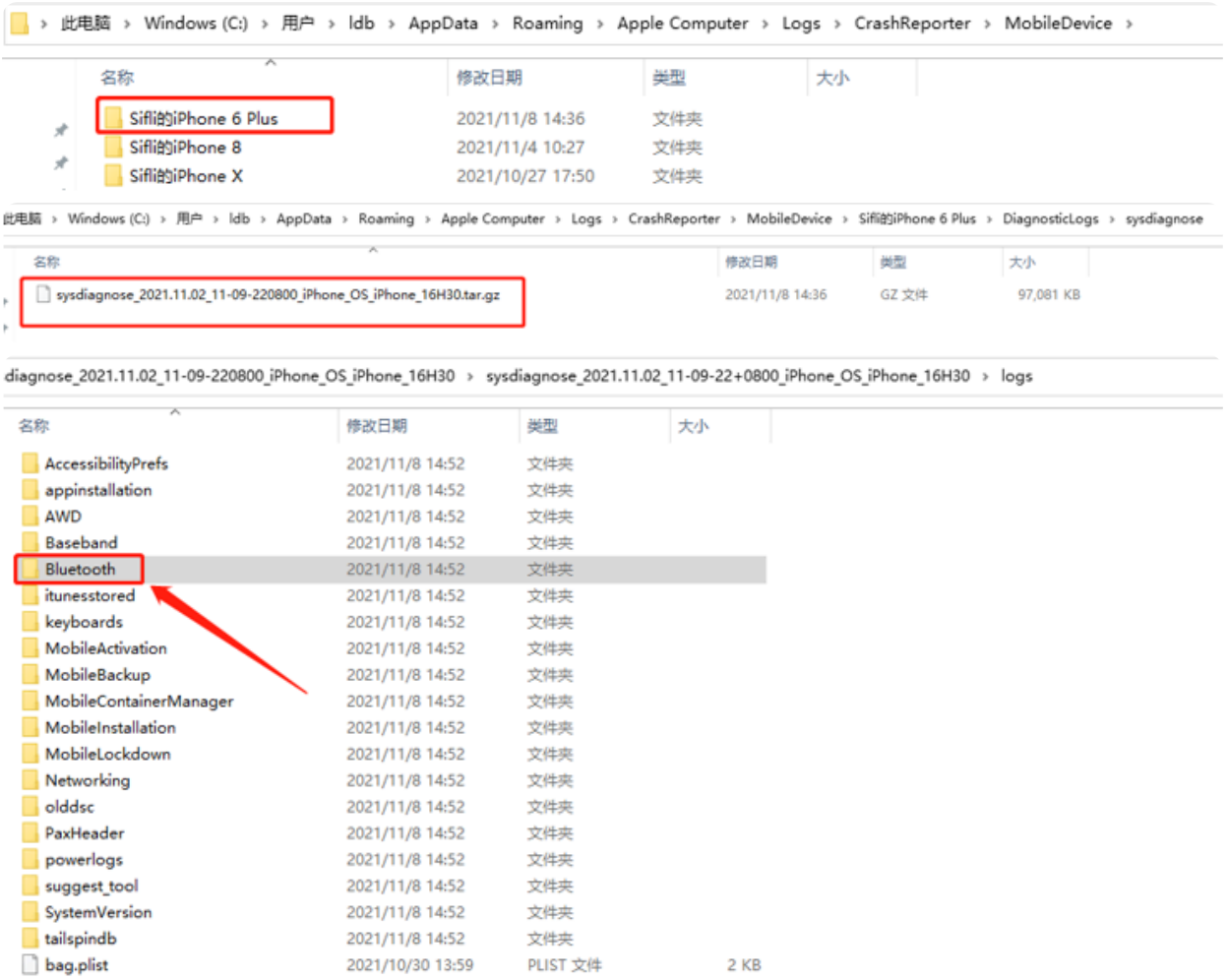

文件(F)
编辑(E)
歌曲(S)
显示(V)
控制(C)
帐户(A)
帮助(H)
音乐
资料库
最近添加
艺人
专辑
歌曲
类型
设备

图 3- 1 连接手机


iPhone 6 Plus
备份
选项


iPhone 6 Plus
备份
选项



3. 大/小核 HCPU/LCPU Dump 信息抓取方法

- 当手表系统出现死机问题或需要分析特定功能性问题时需要抓取 Dump 现场信息

3.1 所需工具及资源

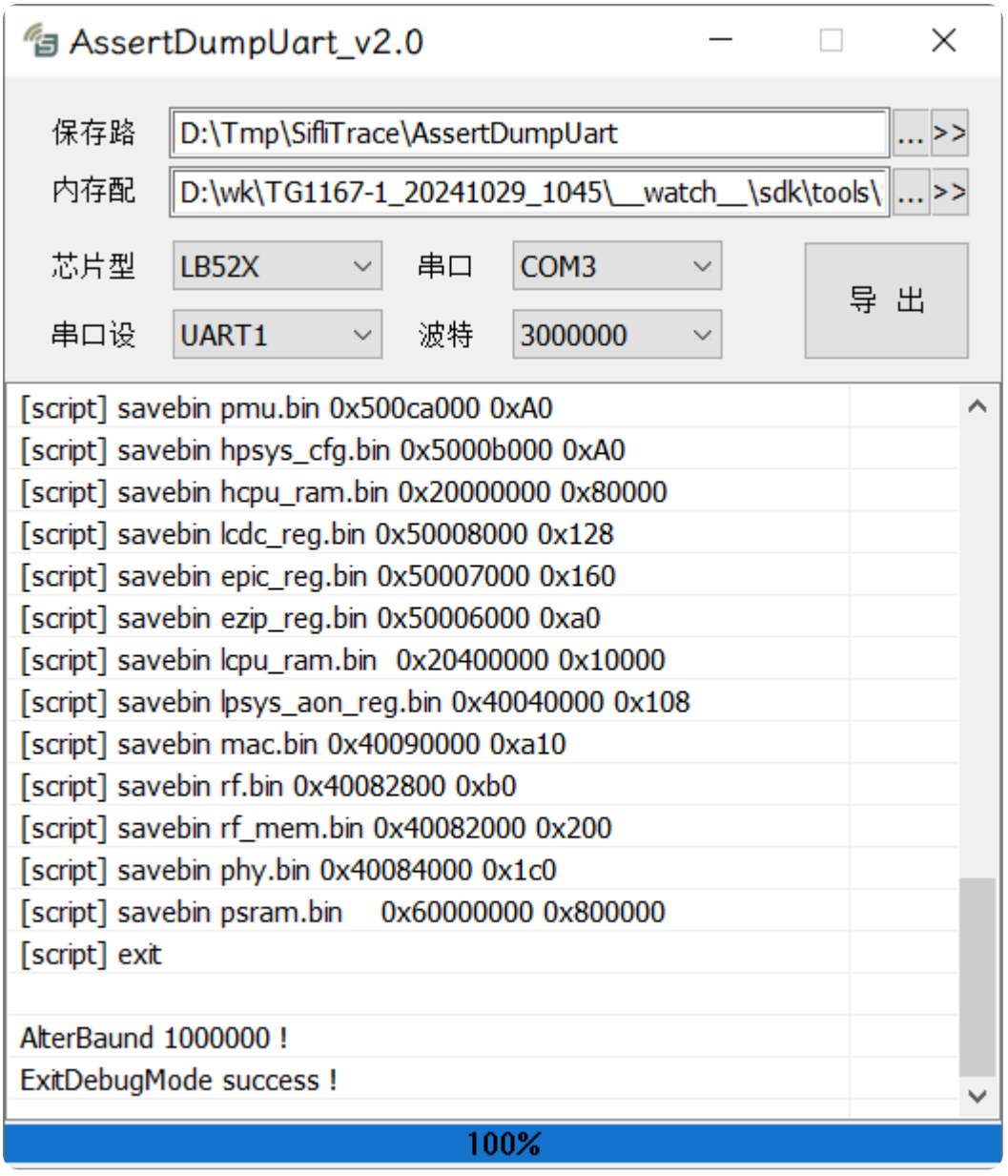
- 硬件
  - 测试产品 (如手表)，需要飞线 (串口或 JLINK SWD)，具体飞线可以参见对应手表 SCH/PCB 飞线图
  - 串口板或 J-Link (JTAG 仿真器)
- 软件/工具
  - AssertDumpUart，如版本 AssertDumpUart_v2.0
  - crash_dump_analyser / save_ram_5xx_psram_xxx.bat

3.2 抓取方法

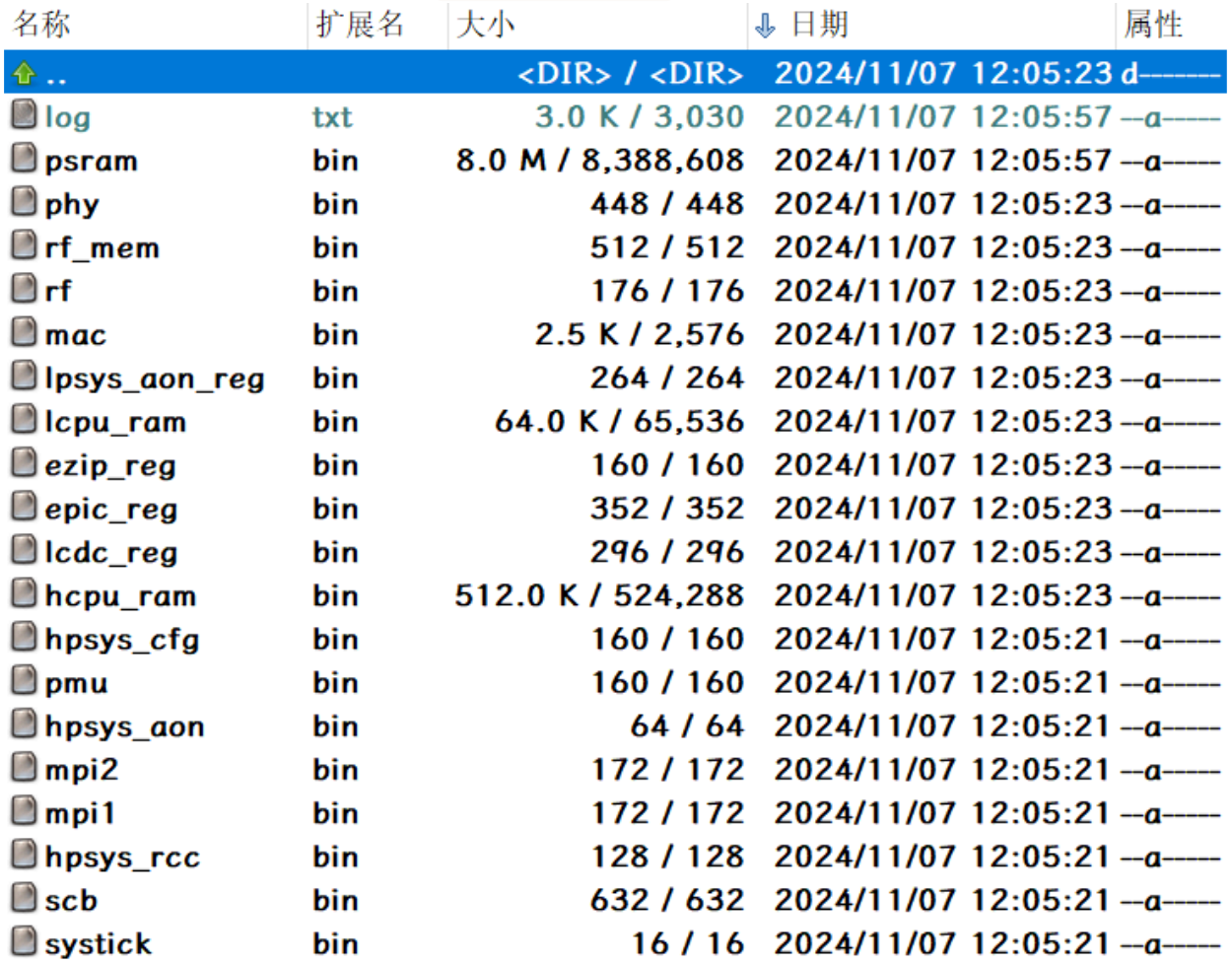
3.2.1 通过串口抓取 Dump 信息

1. 将手表通过串口板或 J-Link 连接至 PC (具体参考抓取手表 HCI Log 相关章节信息)

2. 根据当前连接手表的芯片类型选择对应的 `芯片型号` (如 `LB52X`)、 `内存配置` (如 `sf32lb52x_psram_8MB.jlink`)、 `串口` (PC 侧串口如 `COM3`)、 `串口设置` (手表侧对应串口如 `UART1`)、 `波特率` (如 `3000000` bps)，然后点击 `导出`，导出过程及状态参见 Log 信息打印列表中输出的信息



3. 所有 Dump 信息会存储于工具 `AssertDumpUart` 目录下



名称	扩展名	大小	日期	属性
..		<DIR> / <DIR>	2024/11/07 12:05:23	d-------
log	txt	3.0 K / 3,030	2024/11/07 12:05:57	--a-----
psram	bin	8.0 M / 8,388,608	2024/11/07 12:05:57	--a-----
phy	bin	448 / 448	2024/11/07 12:05:23	--a-----
rf_mem	bin	512 / 512	2024/11/07 12:05:23	--a-----
rf	bin	176 / 176	2024/11/07 12:05:23	--a-----
mac	bin	2.5 K / 2,576	2024/11/07 12:05:23	--a-----
lpsys_aon_reg	bin	264 / 264	2024/11/07 12:05:23	--a-----
lcpu_ram	bin	64.0 K / 65,536	2024/11/07 12:05:23	--a-----
ezip_reg	bin	160 / 160	2024/11/07 12:05:23	--a-----
epic_reg	bin	352 / 352	2024/11/07 12:05:23	--a-----
lcdc_reg	bin	296 / 296	2024/11/07 12:05:23	--a-----
hcpu_ram	bin	512.0 K / 524,288	2024/11/07 12:05:23	--a-----
hpsys_cfg	bin	160 / 160	2024/11/07 12:05:21	--a-----
pmu	bin	160 / 160	2024/11/07 12:05:21	--a-----
hpsys_aon	bin	64 / 64	2024/11/07 12:05:21	--a-----
mpi2	bin	172 / 172	2024/11/07 12:05:21	--a-----
mpi1	bin	172 / 172	2024/11/07 12:05:21	--a-----
hpsys_rcc	bin	128 / 128	2024/11/07 12:05:21	--a-----
scb	bin	632 / 632	2024/11/07 12:05:21	--a-----
systick	bin	16 / 16	2024/11/07 12:05:21	--a-----

- **注意事项**
  - 为了能够通过 Trace32 解决和分析 Dump 现场信息，需要将手表中对应固件编译时生成的 `.axf` 一起提供，所以将编译生成的 `.axf` 文件拷贝至 Dump 文件同一目录下即可

3.2.2 通过 J-Link 抓取 Dump 信息

- 将手表通过 J-Link 及 USB 数据线连接至 PC (参见抓取手表 HCI Log 相关章节信息)，注意需要 PC 侧安装 Segger J-Link 程序及配置好对应 J-Link 驱动，否则会导致无法连接手表设备的情况
- 在 PC 侧通过 J-Link Commander 控制台 `connect` 指令连接至手表设备，确认连接状态正常
- 执行 `crash_dump_analyser\script` 下的 save_ram bat 脚本，以抓取 SF32LB551 芯片手表为例，双击执行 `save_ram_55x.bat` 脚本，根据控制台打印信息确认 Dump 信息导出进度及状态，同样为了能够通过 Trace32 解决和分析 Dump 现场信息，需要将手表中对应固件编译时生成的 `.axf` 一起提供
- **注意事项**
  - 使用 J-Link 导出 Dump 信息时需要保证手表不能处于休眠状态，否则会由于休眠状态下连接异常而导致导出信息失败

4. 整机异常信息 BLE 方式抓取方法

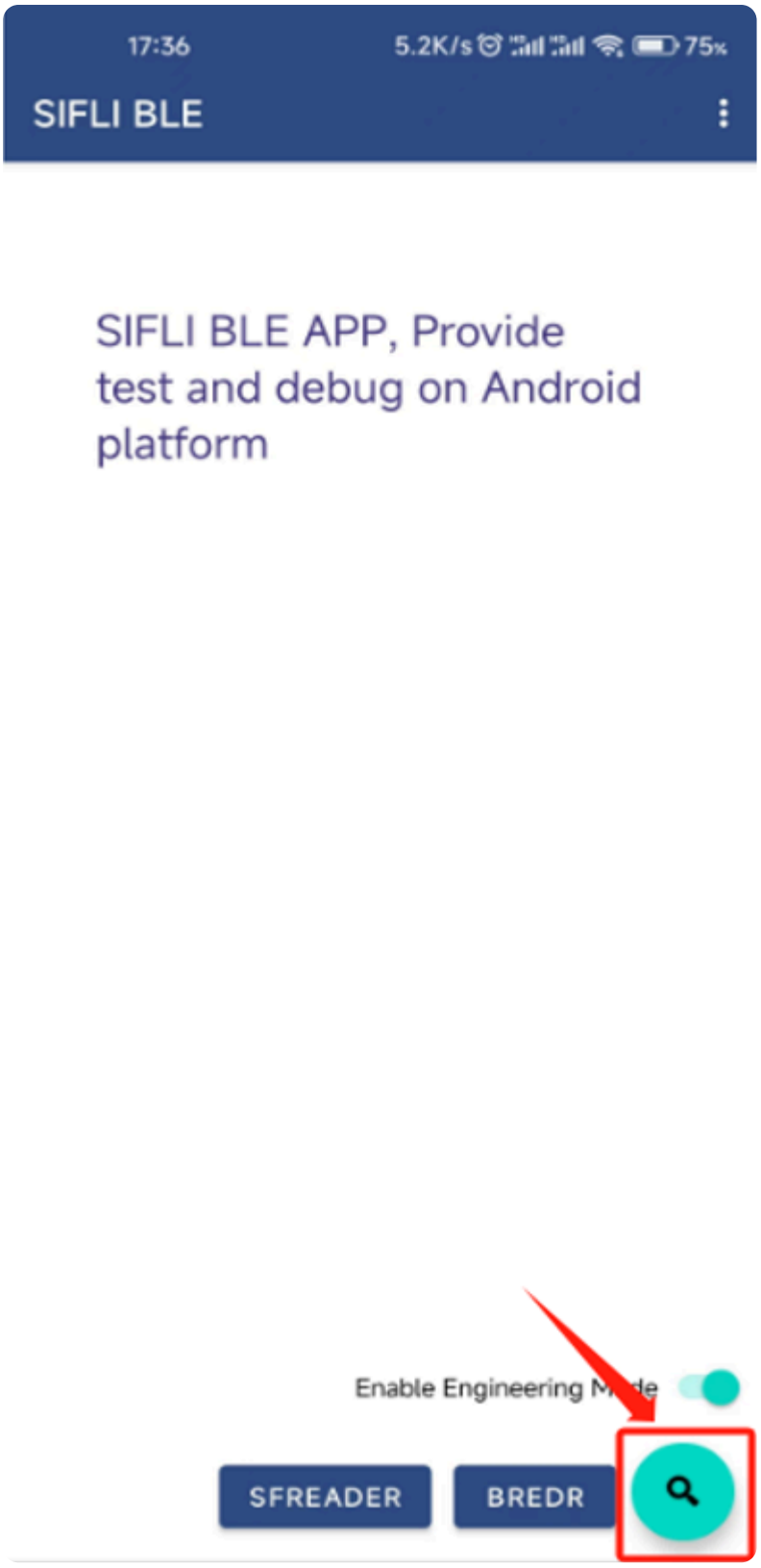
- 在手表整机 (没有飞线) 情况下无法通过有线进行信息导出，所以需要通过无线 (如 BLE) 方式进行信息的导出 (当手表运行时出现死机异常情况，系统 Assert 机制会自动将系统异常信息存储至手表的 Flash 空间中)

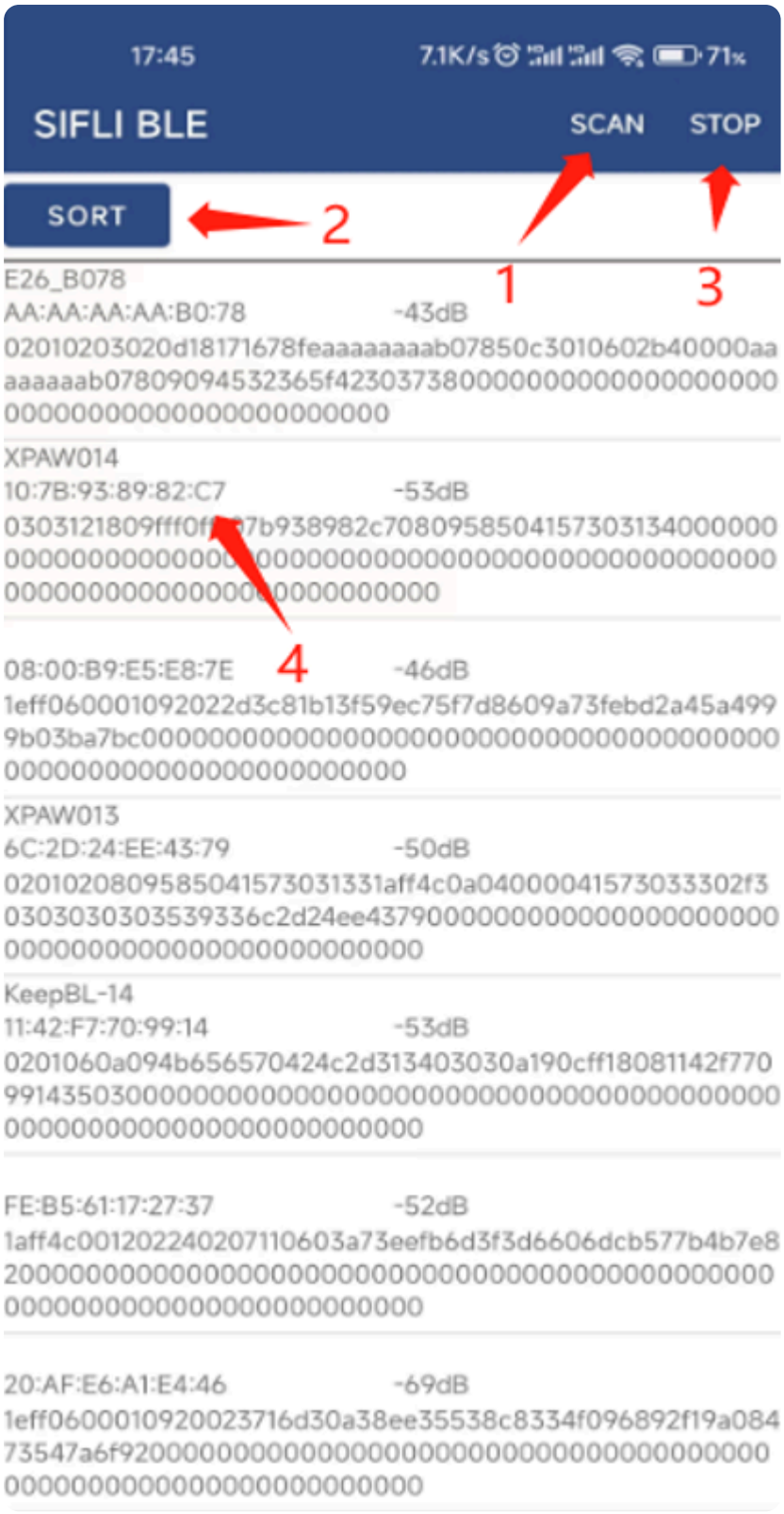
4.1 所需工具及资源

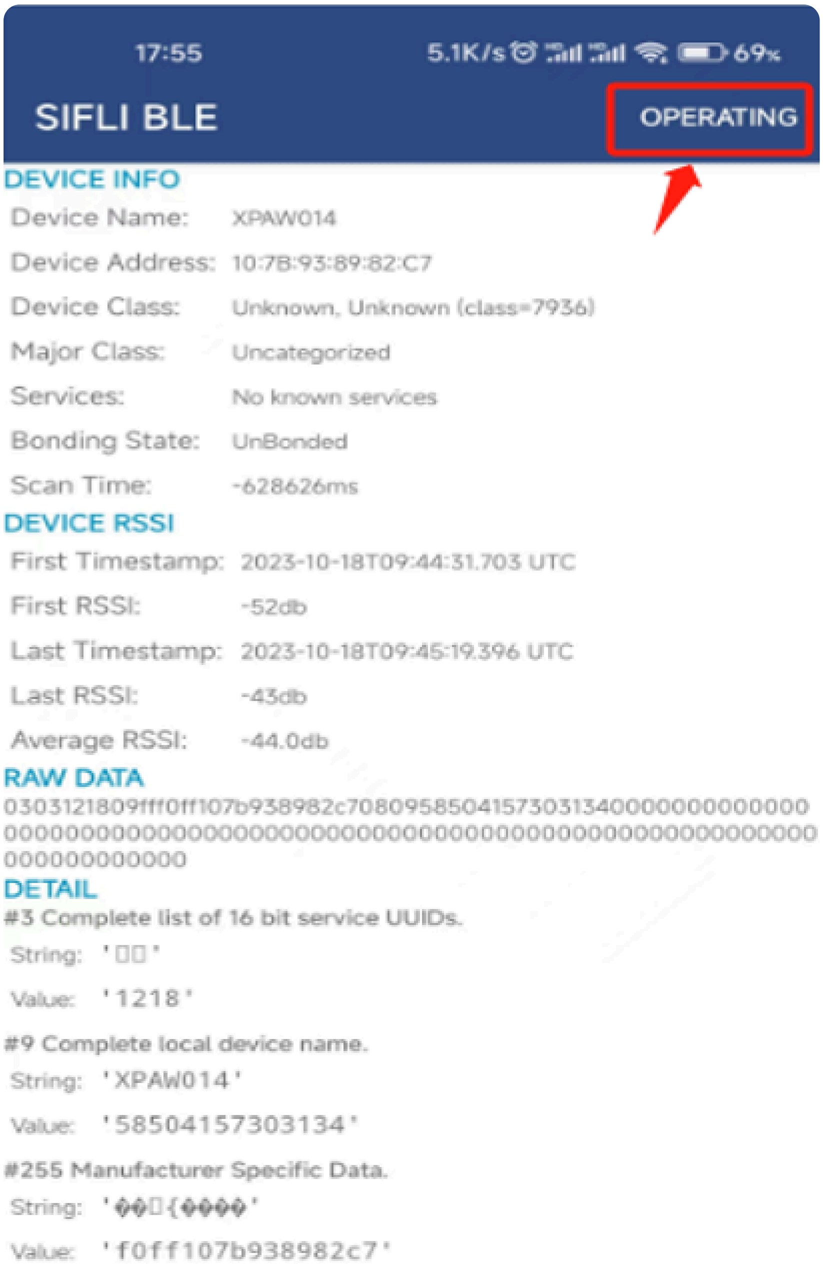
- 硬件
  - 手表整机 (无需飞线)
- 软件/工具
  - SifliBLE App (分为 Android 和 iOS 版本)

4.2 抓取方法

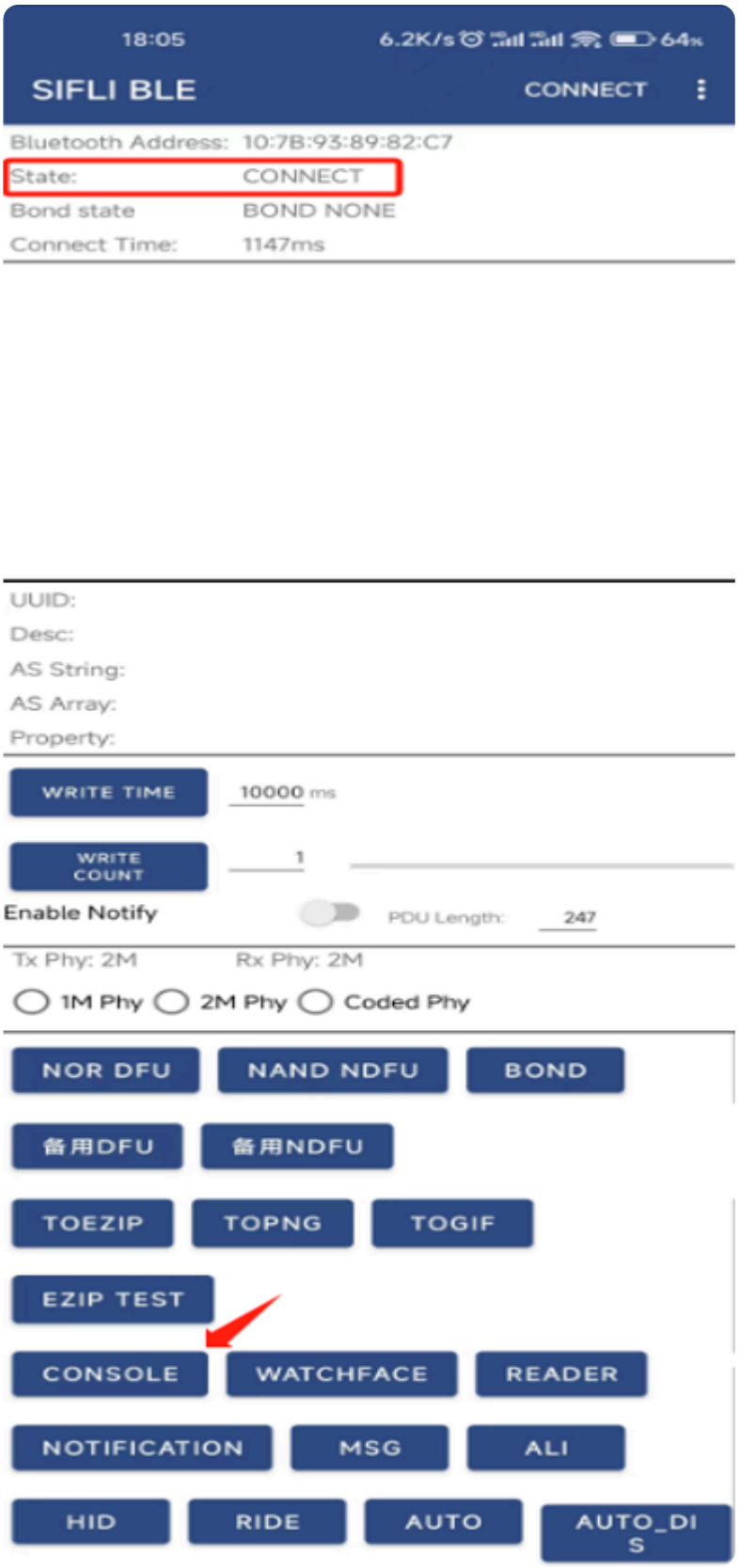
1. 手机安装 SifliBLE App (如 Android 版本) 后并打开
2. BLE 搜索到手表设备 (根据 BLE 设备名及 Mac 地址进行区分，可通过 `SORT` 操作进行设备名称排序)，选择需要连接的设备进行连接


17:36
5.2K/s
75%
SIFLI BLE
SIFLI BLE APP, Provide test and debug on Android platform
Enable Engineering Mode
SFREADER
BREDR

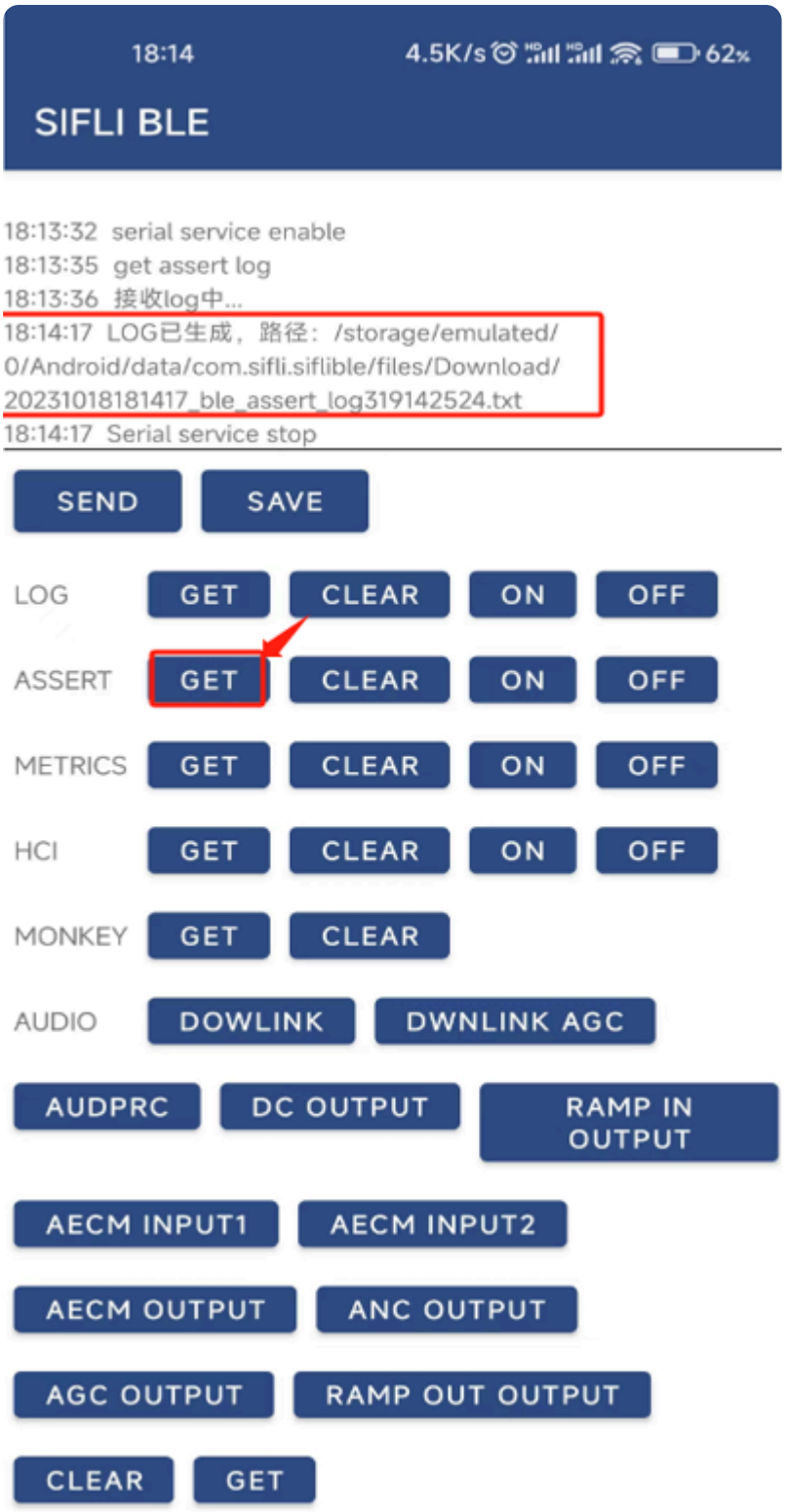

17:45
7.1K/s
71%
SIFLI BLE
SCAN
STOP
SORT
2
1
3
E26_B078
AA:AA:AA:AA:B0:78
-43dB
02010203020d18171678feaaaaaaaab07850c3010602b40000aa
aaaaaab07809094532365f42303738000000000000000000
00000000000000000000000
XPAW014
10:7B:93:89:82:C7
-53dB
0303121809fff0f
7b938982c708095850415730313400000
0000000000000
0000000000000000000000000000000000
0000000000000000000000000
4
08:00:B9:E5:E8:7E
-46dB
1eff060001092022d3c81b13f59ec75f7d8609a73febd2a45a499
9b03ba7bc0000000000000000000000000000000000000
00000000000000000000000
XPAW013
6C:2D:24:EE:43:79
-50dB
02010208095850415730313 31aff4c0a040000415730333 02f3
0303030303539336c2d24ee437900000000000000000000
00000000000000000000000
KeepBL-14
11:42:F7:70:99:14
-53dB
0201060a094b656570424c2d313403030a190cff18081142f770
99143503000000000000000000000000000000000000000
00000000000000000000000
FE:B5:61:17:27:37
-52dB
1aff4c00120224020711060 3a73eefb6d3f3d6606dcb577b4b7e8
20000000000000000000000000000000000000000000000
00000000000000000000000
20:AF:E6:A1:E4:46
-69dB
1eff06000109200237 16d30a38ee35538c8334f096892f19a084
73547a6f92000000000000000000000000000000000000
00000000000000000000000


17:55
5.1K/s 69%
SIFLI BLE
OPERATING
DEVICE INFO
Device Name: XPAW014
Device Address: 10:7B:93:89:82:C7
Device Class: Unknown, Unknown (class=7936)
Major Class: Uncategorized
Services: No known services
Bonding State: UnBonded
Scan Time: -628626ms
DEVICE RSSI
First Timestamp: 2023-10-18T09:44:31.703 UTC
First RSSI: -52db
Last Timestamp: 2023-10-18T09:45:19.396 UTC
Last RSSI: -43db
Average RSSI: -44.0db
RAW DATA
0303121809fff0ff107b938982c708095850415730313400000000000000
000000000000000000000000000000000000000000000000000000000000
000000000000
DETAIL
#3 Complete list of 16 bit service UUIDs.
String:
Value: '1218'
#9 Complete local device name.
String: 'XPAW014'
Value: '58504157303134'
#255 Manufacturer Specific Data.
String:
Value: 'f0ff107b938982c7'

3. 连接以后点击 `CONSOLE` 进入 Log 控制界面，通过点击 `ASSERT`、 `HCI` 栏对应的 `GET` 按钮来获取异常 Assert 、HCI Log，Log 导出状态参见文本区域信息打印，如导出的 Log



在手机存储区对应的路径信息



5. 蓝牙空口包抓取方法

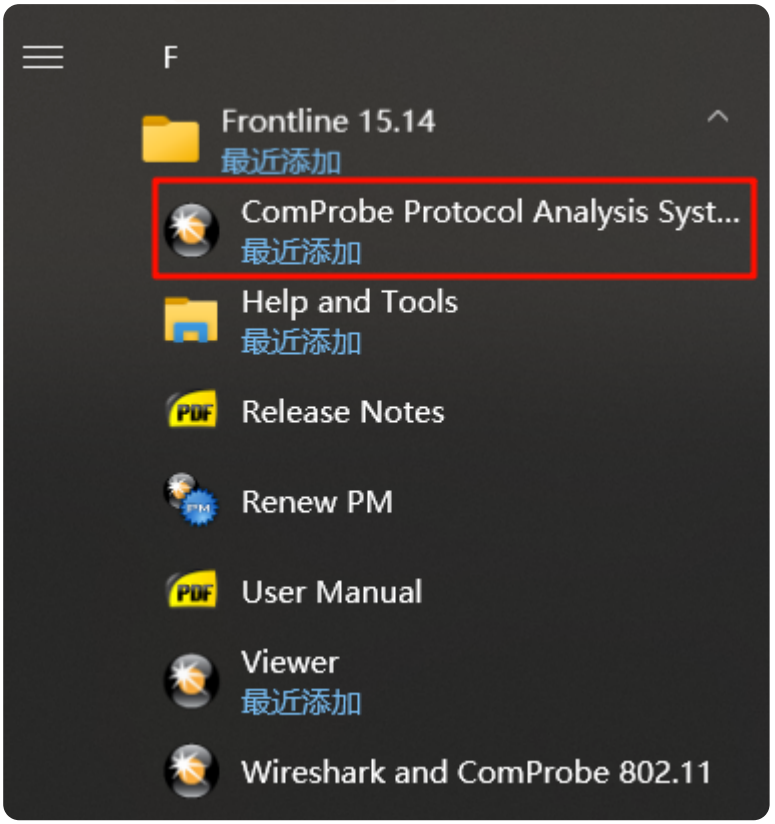
5.1 所需工具及资源

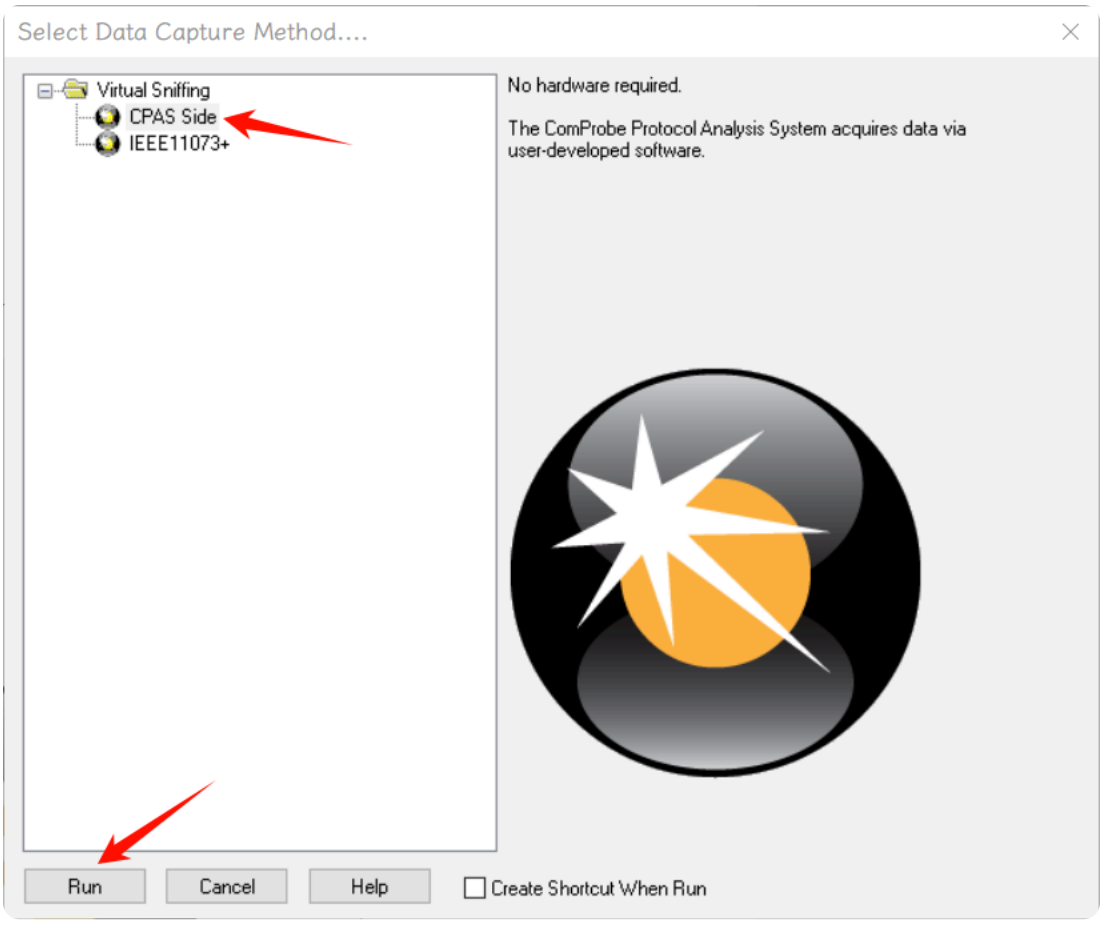
- 硬件
  - 测试产品 (如手表)，需要飞线 (串口或 JLINK SWD)，具体飞线可以参见对应手表 SCH/PCB 飞线图
  - 串口板或 J-Link (JTAG 仿真器)

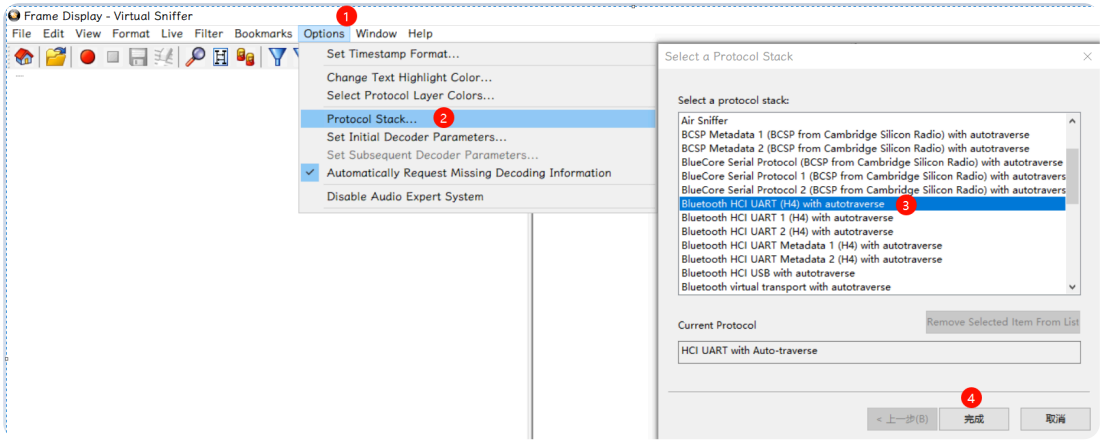
    - Ellisys 抓包器
- 软件/工具
    - SifliTrace
    - Frontline
    - Ellisys Bluetooth Analyzer

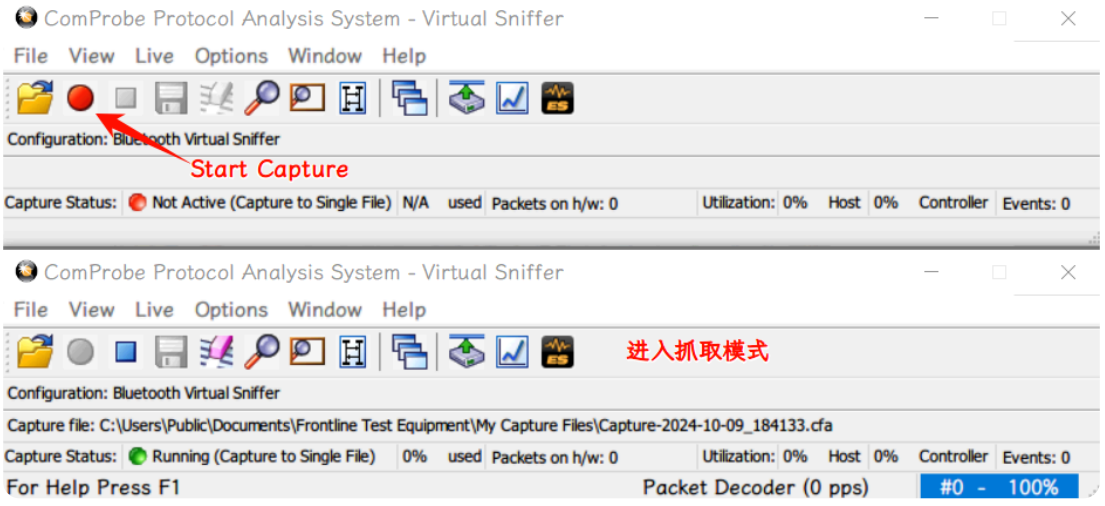
5.2 抓取方法

1. 链路密钥 Link Key 的提取，Link Key 用于设备间连接时认证鉴权并加密相互交互的数据
    1. 从手表侧提取 LinkKey
        - 打开 Frontline - ComProbe Protocol Analysis System，双击运行 `CPAS Side` 或选中 `CPAS Side` 项后点击 `Run` ，依次打开 `Options` → `Protocol Stack ...` ，并在 `Select a Protocol Stack` 界面中选择 `Bluetooth HCI UART (H4) with autotraverse` 并点击 `完成` ，打开 `Frame Display` 视图窗口后，点击 `Start Capture` 进入 Capture 模式





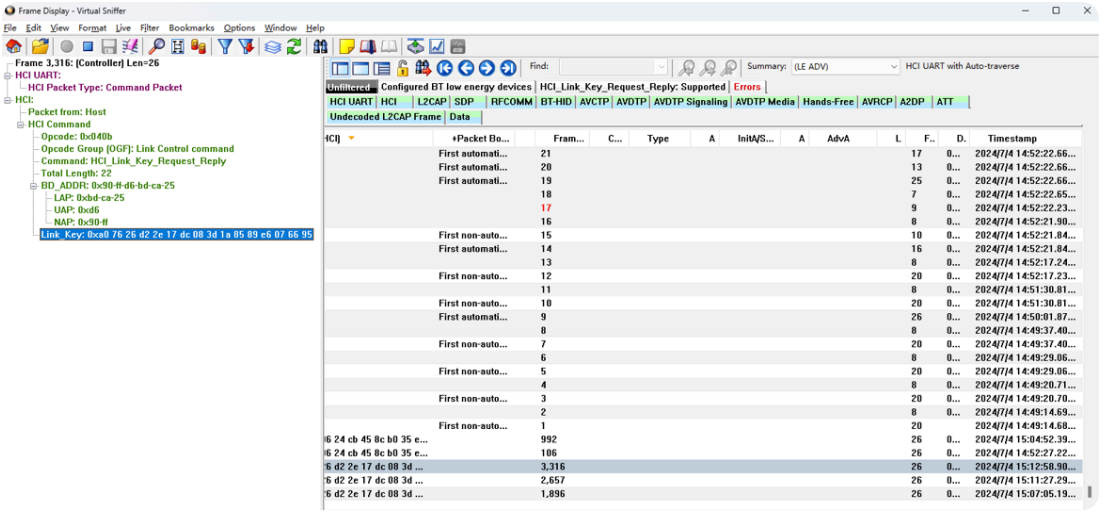


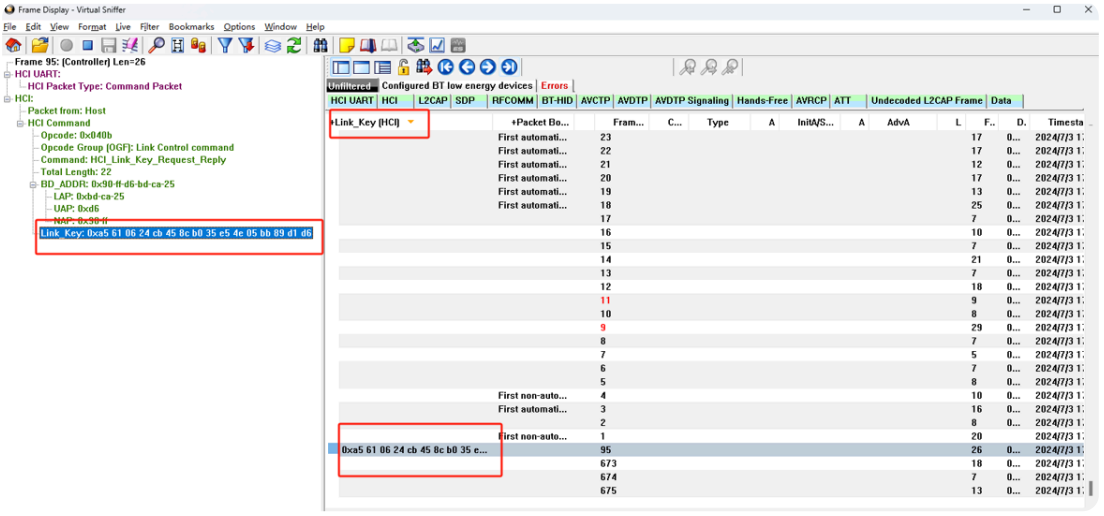


- 连接手表至 PC，打开 SifliTrace工具，相关设置参见抓取手表 HCI Log 相关章节内容，另外再勾选 `Front.` 选项，在 `Frame Display` 窗口中会有信息输

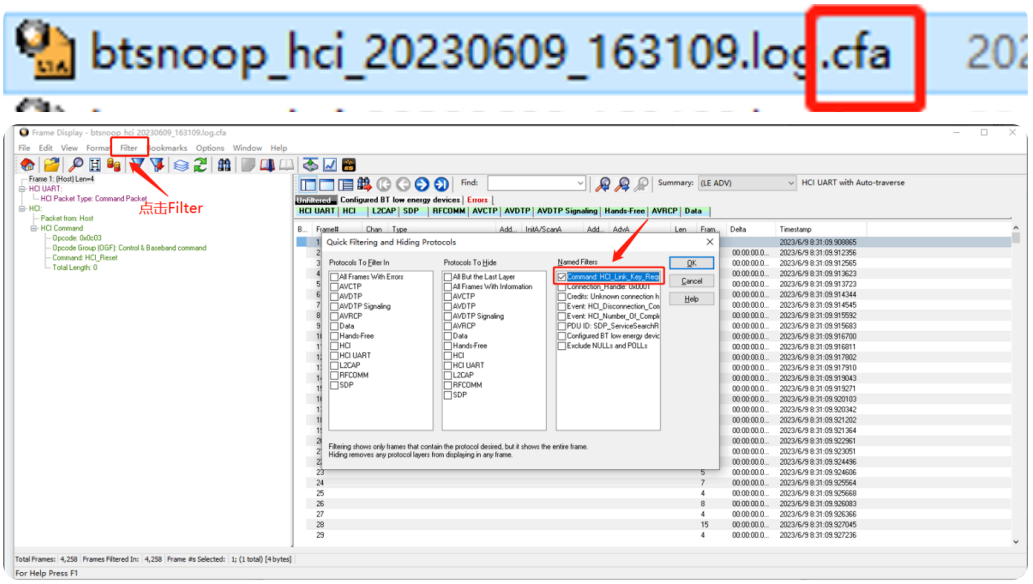
出

- 选择排序 Link Key 选项，将 Link Key 排序保持在最下方以方便查找 Link Key，调整好排序后可以在下面找到对应的 Link Key，选择最新时间的 Link Key 并复制以便后面在 Ellisys Bluetooth Analyzer 中配置 LinkKey 以抓取空口包信息

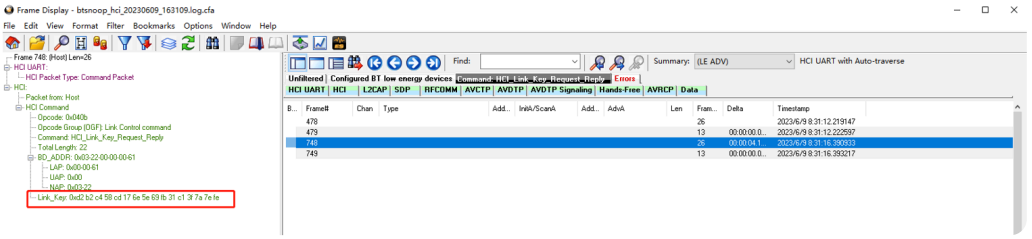




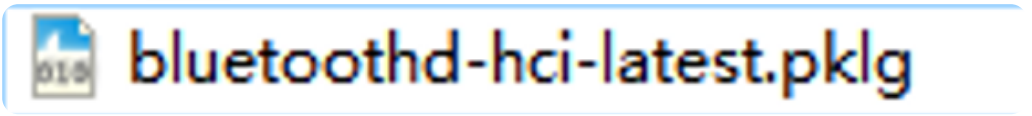
2. 从手机侧 HCI Log 中提取 Link Key (分别以华为和 iOS 手机为例)
    1. 华为手机
        1. 将从华为手机导出的 HCI Log (抓取方法参见前面章节内容，文件类型为 `.cfa`) 使用 Frontline 打开，点击 `Filter` → `Quick Filtering and Hiding Protocols`，勾选 `Named Filters` 选项框中 HCI_Link_Key 项



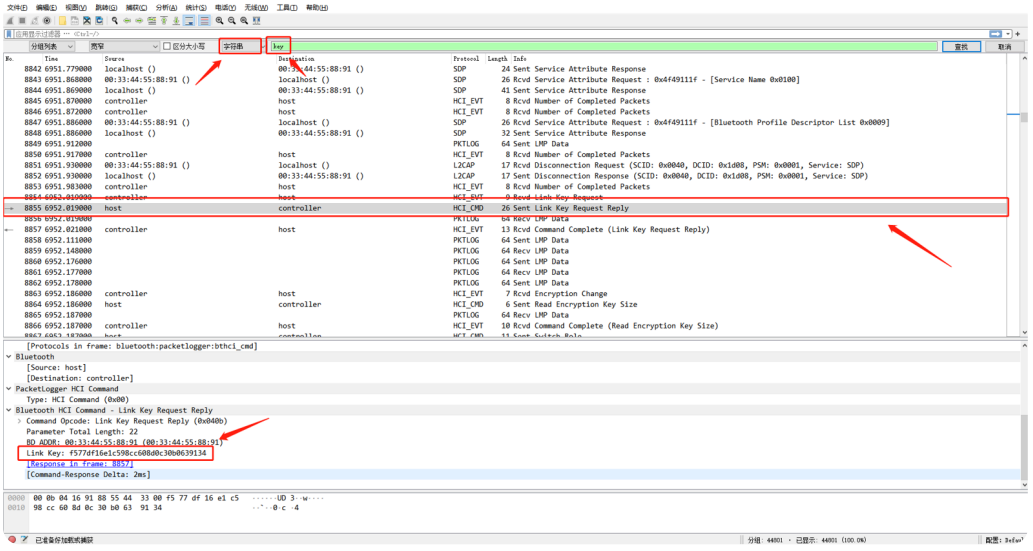
2. 在过滤内容中选中 `Link_Key` 项，进行复制即可



2. iOS 手机
    1. 安装 WireShark 工具并用 WireShark 打开从 iOS 手机中导出的 HCI Log 文件 `.pklg`



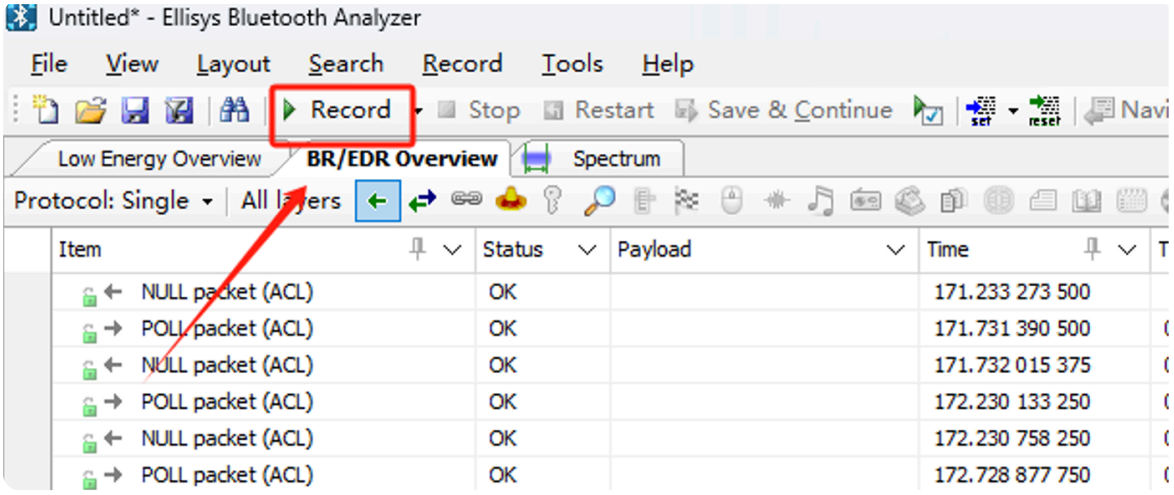
    2. 在 WireShark 窗口中按 `Ctrl + F` 快捷键开启搜索，更改搜索类型为 `字符串`，搜索关键字填入 `Link Key`，在过滤项中点击 `Link Key Request Reply` 项，在底部窗口中展开 `Bluetooth HCI Command - Link Key Request Reply` 后复制 Link Key 内容



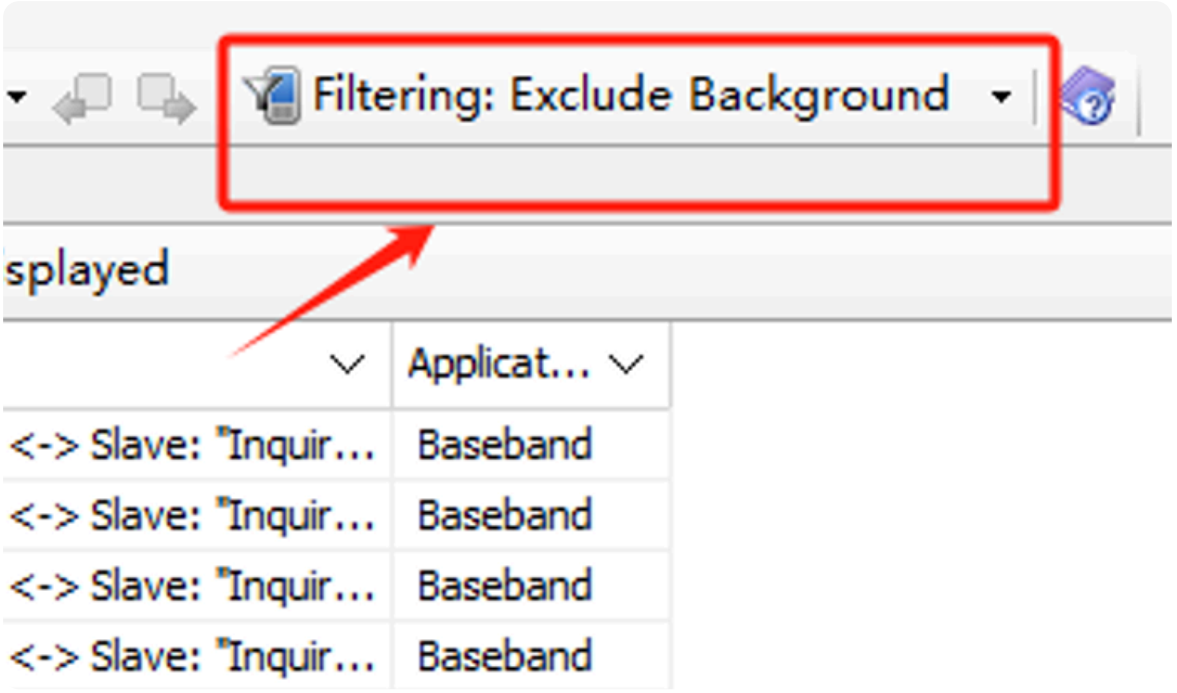
- **注意事项**

- 密钥不但可以用于当前的连接中，还可以用于两个设备后续的重连过程中，但是鉴权过程中如果比较双方的 Link Key 不一致，则必须重新开始配对流程，从而创建新的链路密钥 (Link Key) 用于新的连接交互流程
- 手表和手机每一次匹配的 Link Key 都是不相同的

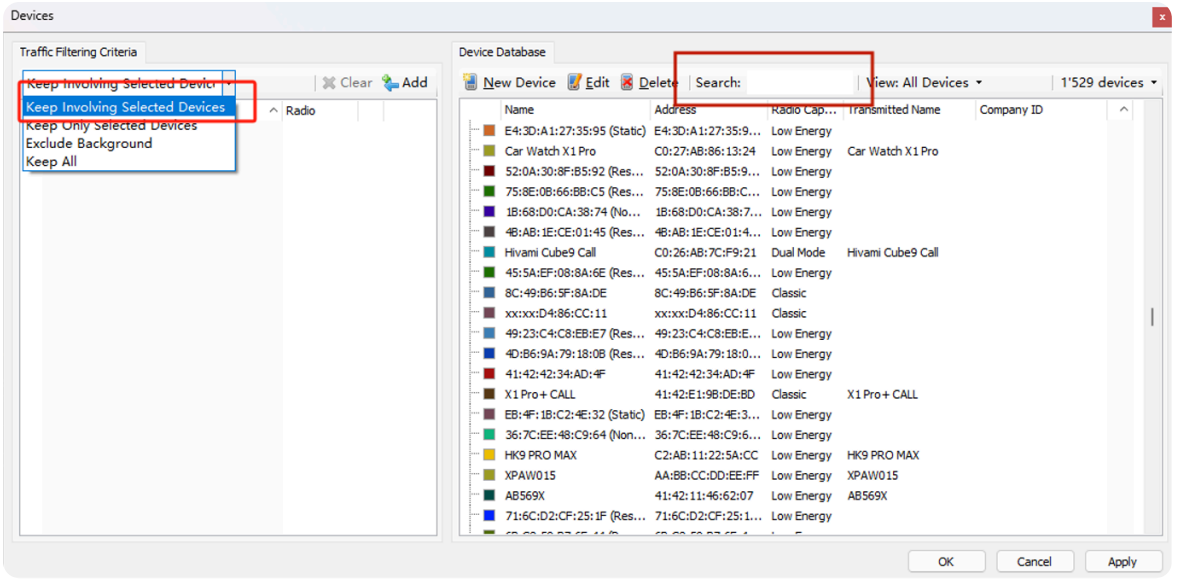
2. 使用仪器通过 Link Key 锁定需要抓取空口包的设备并抓取空口包
    1. 打开 Ellisys Bluetooth Analyzer 后，点击 `Record` 开始记录



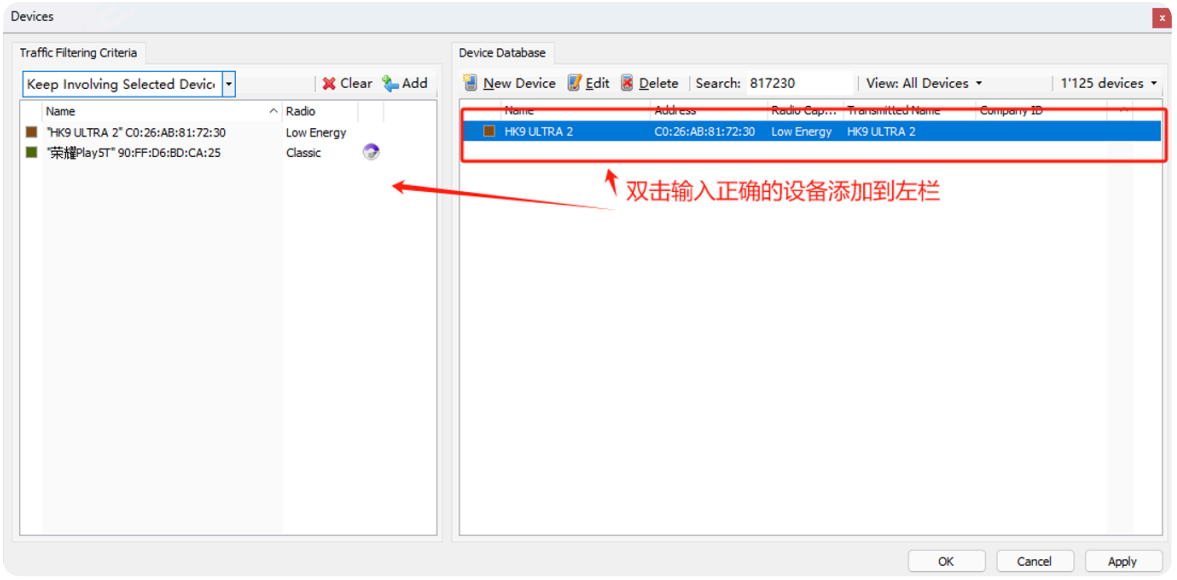
    2. 点击 `Filtering` 过滤对应的设备



    3. 选择 `Keep Involving Selected Devices`，然后在 `Search` 输入框中依次输入手机和手表的蓝牙地址

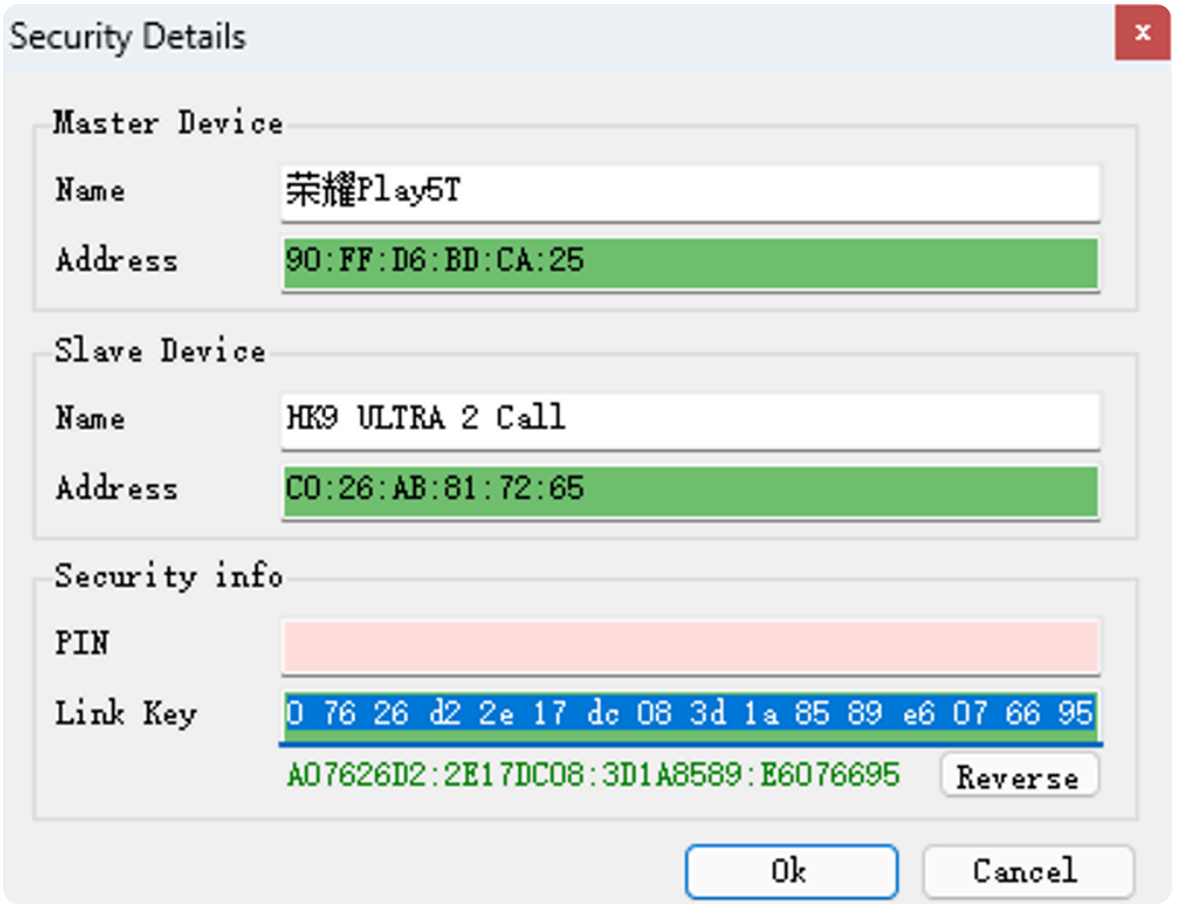


4. 输入地址之后双击对应的设备将对应设备添加到 `Traffic Filtering Criteria` 列表框中

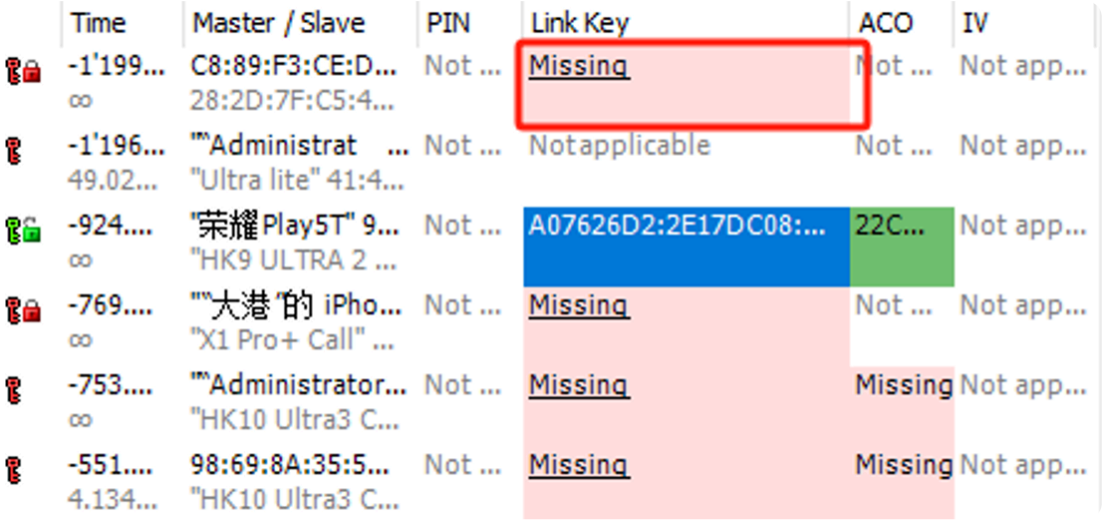


5. 在 `Security Details` 界面 `Link Key` 栏双击 `Missing` 项后输入与对应设备匹配的 Link Key (输入 Link Key 后会覆盖原来的 `Missing` 字样)，注意: 如果输入了不

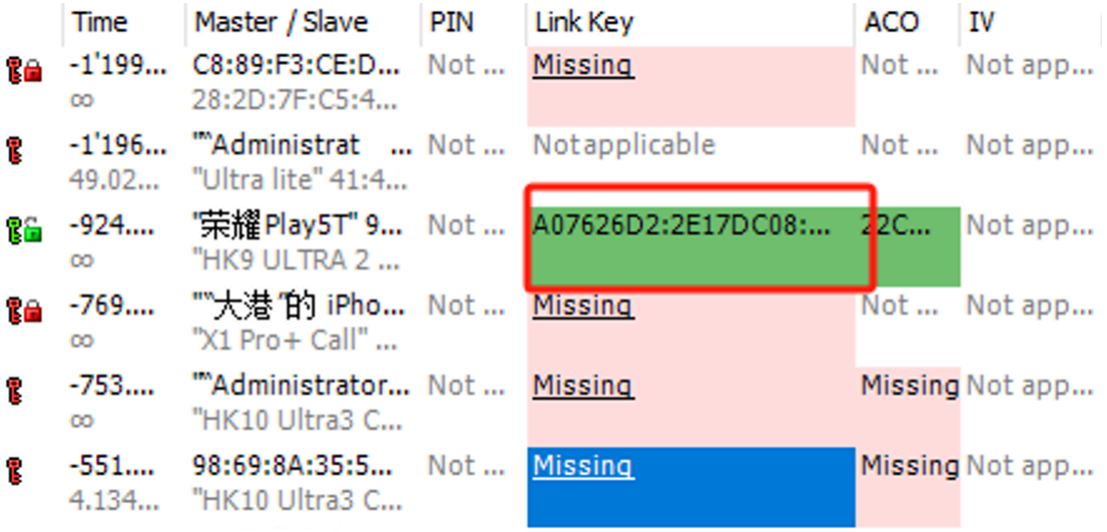
正确的 Link Key，则会显示为红色，有效的 Link Key 会显示为绿色



- 未输入 Link Key 的状态如下



- 输入 Link Key 后的状态如下



	Time	Master / Slave	PIN	Link Key	ACO	IV
	-1'199... ∞	C8:89:F3:CE:D... 28:2D:7F:C5:4...	Not ...	Missing	Not ...	Not app...
	-1'196... 49.02...	""Administrat ... "Ultra lite" 41:4...	Not ...	Not applicable	Not ...	Not app...
	-924.... ∞	"荣耀 Play5T" 9... "HK9 ULTRA 2 ...	Not ...	A07626D2:2E17DC08:...	22C...	Not app...
	-769.... ∞	""大港"的 iPho... "X1 Pro+ Call" ...	Not ...	Missing	Not ...	Not app...
	-753.... ∞	""Administrator... "HK10 Ultra3 C...	Not ...	Missing	Missing	Not app...
	-551.... 4.134...	98:69:8A:35:5... "HK10 Ultra3 C...	Not ...	Missing	Missing	Not app...

6. 检查连接状态正常 (设备指示为绿色连接状态) 后，开始测试或复现问题直至完成以后，关闭窗口、Save Recording / Yes 并填写保存为 `.btt` 格式的文件名完成空口包文件的保存