Link Key取得について

CORNES
Technologies

Bluetoothログ解析方法

Bluetooth機器の通信は暗号化されており、解析時には暗号化を解く “Link Key”が必要となります。Sodera又はBPA600を使用したログ解析方法は以下の2通りです。

1. **測定機器のどちらかをSSP Debug Modeに設定する**

2. **Android端末の「btsnoop_hci.log」ファイルから Link Key を取得する**

CORNES Technologies

【方法１】 測定機器をSSP Debug Modeに設定する

Bluetooth機器は SSP Debug Mode と呼ばれる開発モードに設定可能です。
Master/Slave機器のいずれかをSSPデバッグモードに設定すると、Link Key
を入力せずに 暗号化以降の解析が可能になります。

SSP Debug Mode とは

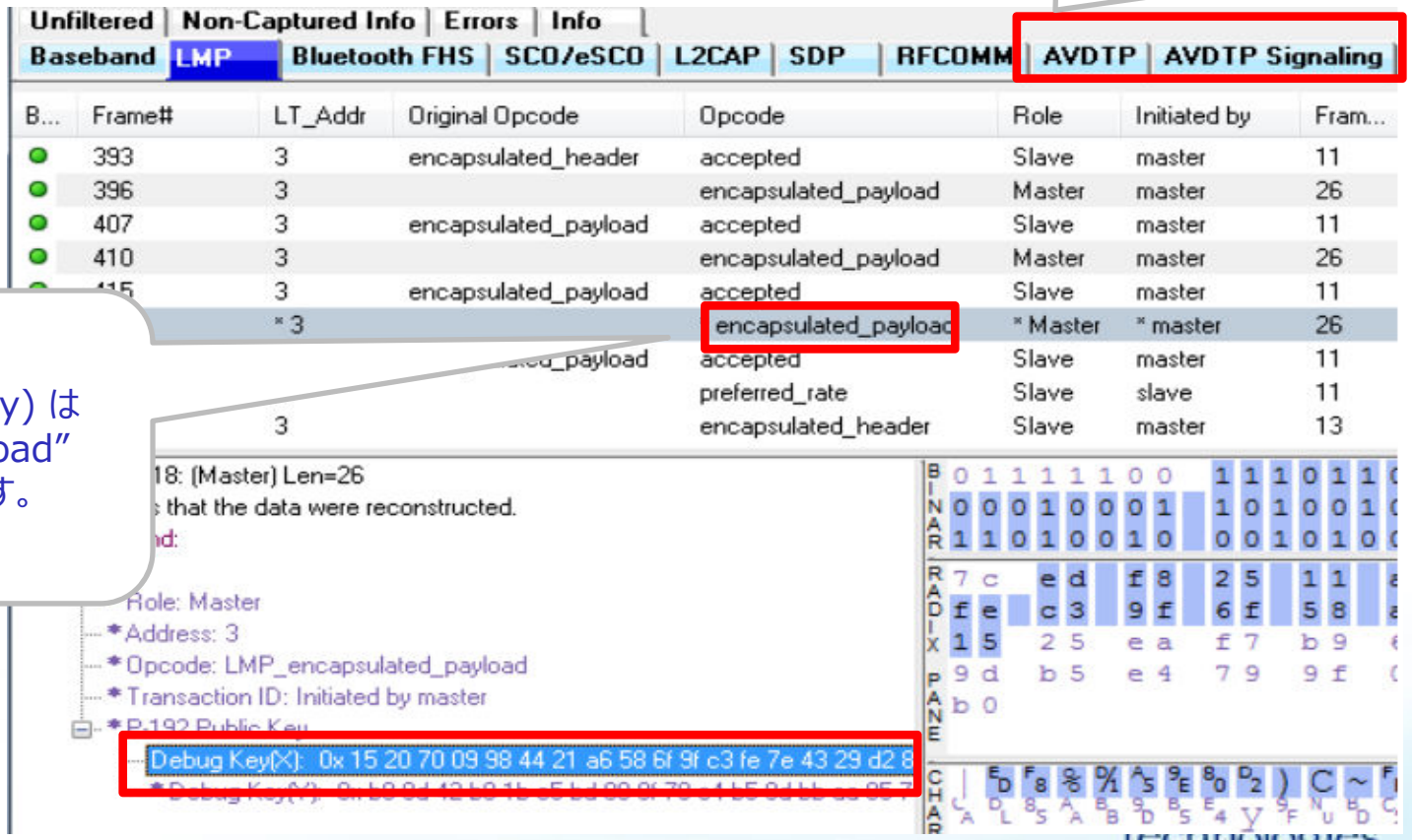
- Link Keyは通常、コネクション毎に毎回異なるKeyが生成されますが、
  Bluetooth機器を SSP Debug Mode に設定することにより、Link Key
  構成要素の一部が固定になります。
  そのため、CPASソフトウェアは Link Keyを自動認識 (計算)することが
  可能になります。
- SSP Debug Modeへの切替方法は各セットメーカーにより異なり、
  また対応していないBluetooth機器もあるため、必ず各セットメーカーへ
  ご確認ください。

CORNES Technologies

【方法1】SSP Debug Modeに設定した場合の表示例

Master/SlaveのいずれかがSSP Debug Mode
になっていると、Link keyを入力しなくても
暗号化以降のタブが表示されます。

Link key (Debug Key) は
”encapsulated payload”
パケット内で確認できます。



【方法2】Android端末から Link Keyを抜き出す

Android端末との通信を解析する場合、Android端末内に記録される
「btsnoop_hci.log」ファイルから、Link Keyを抜き出すことが可能です。

抜き出したLink KeyをCPASソフトウェアに入力することで
暗号化以降のプロトコル解析も可能になります。

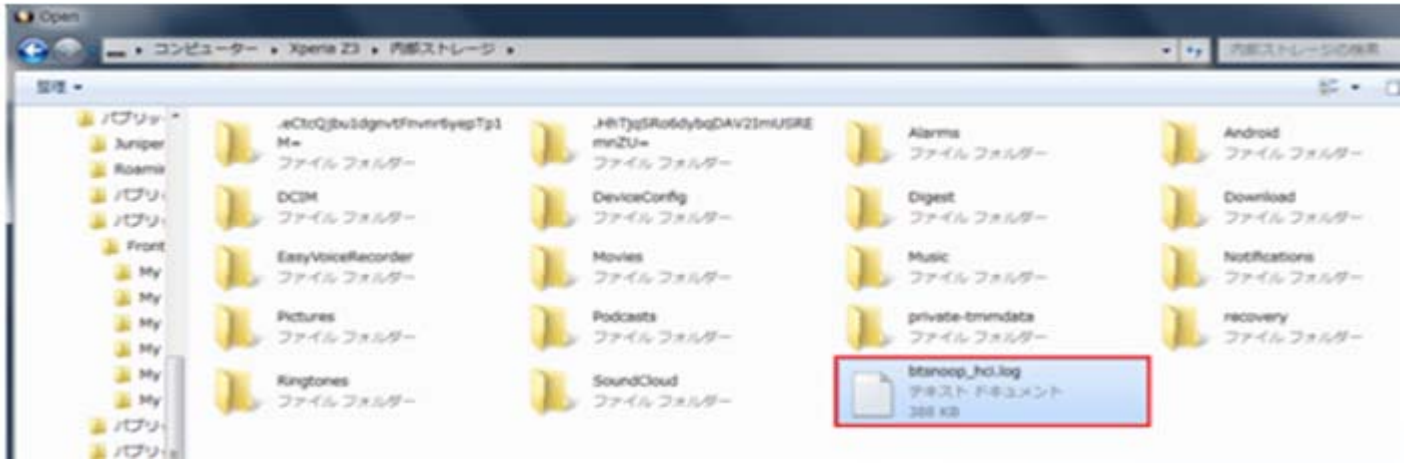
※本手法はAndroid端末(OS ver 4.4以降)のみ有効であり、
iPhone端末は非対応です。

CORNES Technologies

btsnoop_hci.log 取得方法 (1)

＜ログ取得前の確認事項＞

- **CPASソフトウェアが最新バージョンであることを確認する**
- **Android端末のペアリング履歴・デバイス情報を完全削除する**
- **一度端末をPCに接続し、古い「btsnoop_hci.log」が残っていないかを確認する**
  ⇒残っている場合は、削除する



CORNES Technologies

btsnoop_hci.log 取得方法 (2)

① 端末の「設定」画面を開く
→最下層の「端zz末情報」
→「ビルド番号」を７回タップ

②①で開発者モードになり
「設定」画面に開発者向けオプションが
表示される

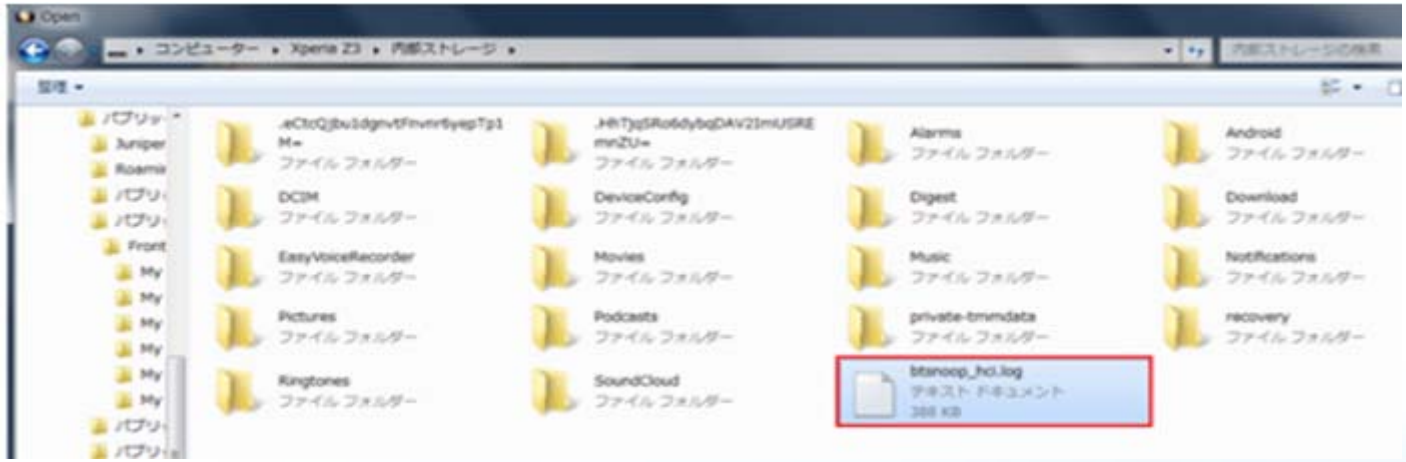
③ 開発者向けオプションをONに変更し、
Bluetooth HCIスヌープログを
「有効にする」をチェック

btsnoop_hci.log 取得方法 (3)

④ 端末とペアリングを行う

⑤ 端末を再起動

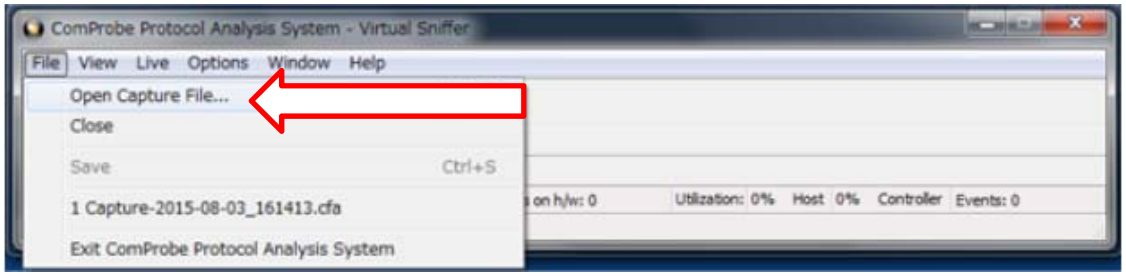
⑥ 再度端末をPCに接続し、「btsnoop_hci.log」をPCに保存



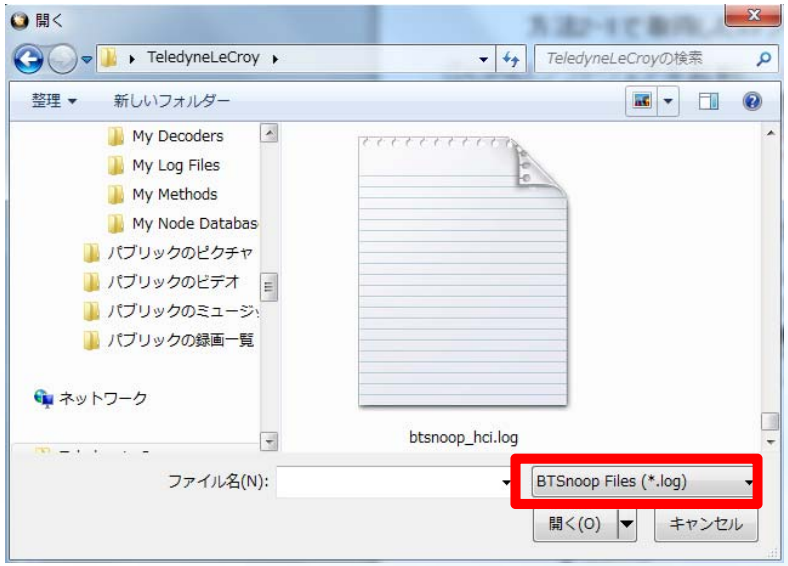
CORNES Technologies

取得した btsnoop_hci.log から Link Keyを確認

① CPASソフトウェアを起動し、「Open Capture File...」を選択



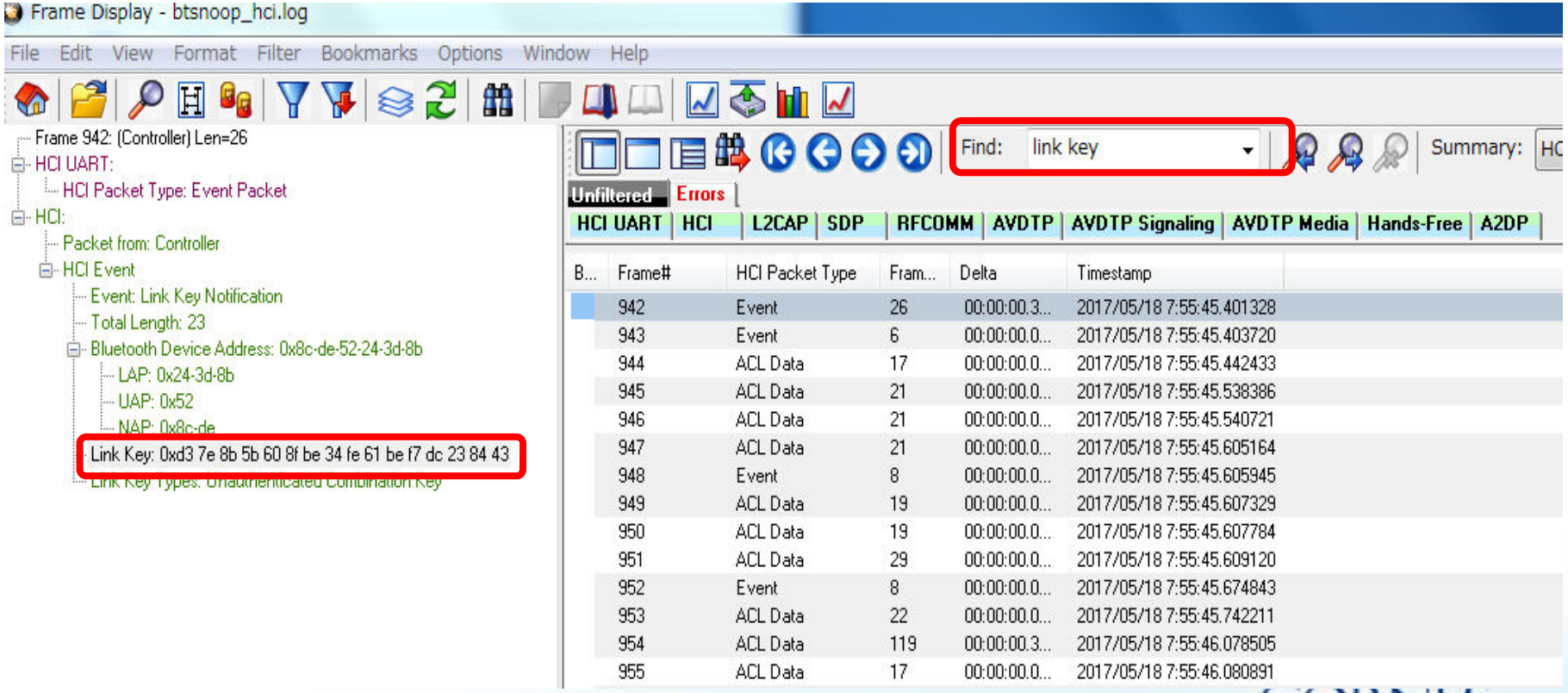
② 拡張子を「BT Snoop Files.log」に変更し、PCに保存した「btsnoop_hci.log」ファイルを開く



抜き出したLink Keyの表示例（1）

＊成功例＊

“Link key”を検索すると、以下の通り表示されます。



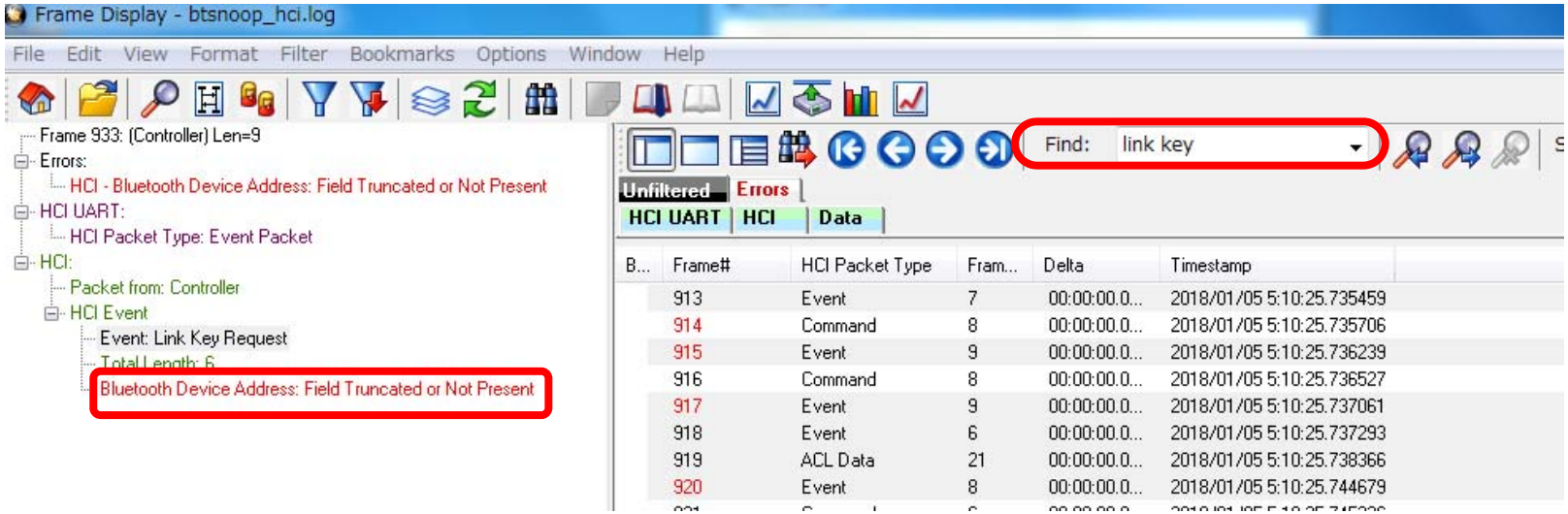
※検証機器：Android OS 6.0.1のXperiaとスマートスピーカーとの接続

CORNES Technologies

抜き出したLink Keyの表示例 (2)

＊失敗例＊

エラー表示となり、Link Keyが表示されない



※以下の場合はセットメーカー様へお問合せ下さい。

- 複数回試してもエラー表示が続いた場合
- 「btsnoop_hci.log」ファイル自体が取得できない場合

CORNES Technologies

ご不明点などございましたら、お気軽にご連絡ください

お問合せ先

〒105-0014
東京都港区芝3丁目5番1号コーンズハウス
コーンズテクノロジー株式会社
電子通信ソリューション営業部
TEL：03-5427-7566
Email：ctl-comm@cornes.jp

CORNES Technologies