トラフィックのフィルタ機能について

はじめに

Bluetooth のトポロジーは、技術の発展とともにますます複雑になり、斬新でより洗練されたアプリケーションが現れ始めました。混雑した実験室や公共のテストラボ（UPFなど）では数百ものデバイスが同時に動作することがあります。

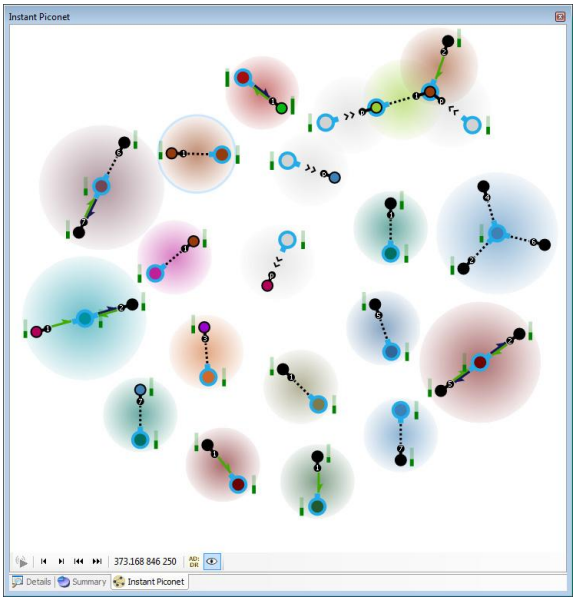
Ellisys BEX400 Explorer プロトコル解析システムは、全てのピコネットやスキャッターネットはもちろん、ページングや照会のような同期前のトラフィックも含めて、周辺の全ての *Bluetooth* トラフィックを記録するようにデザインされました。

しかし、どのようにして関心がある通信だけを選別して正確に表示させることができるのでしょうか？この挑戦に立ち向かうために、ＢＥＸ400 アナライザ ソフトウェアは 7つものアプローチで、トラフィックの記録中でも記録後の解析でも使える強力なフィルタ機能を、検索・編集が可能なデータベースと共に提供します。

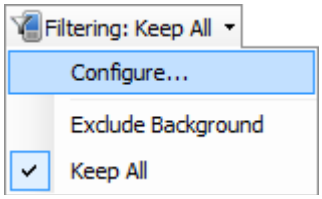
この文書は、この強力なデバイス トラフィック フィルタとそれに関連するデバイス データベースの使用手順を解説し、さらにその他のフィルタ関連機能について説明します。

デバイス トラフィック フィルタを用いたフィルタの作成

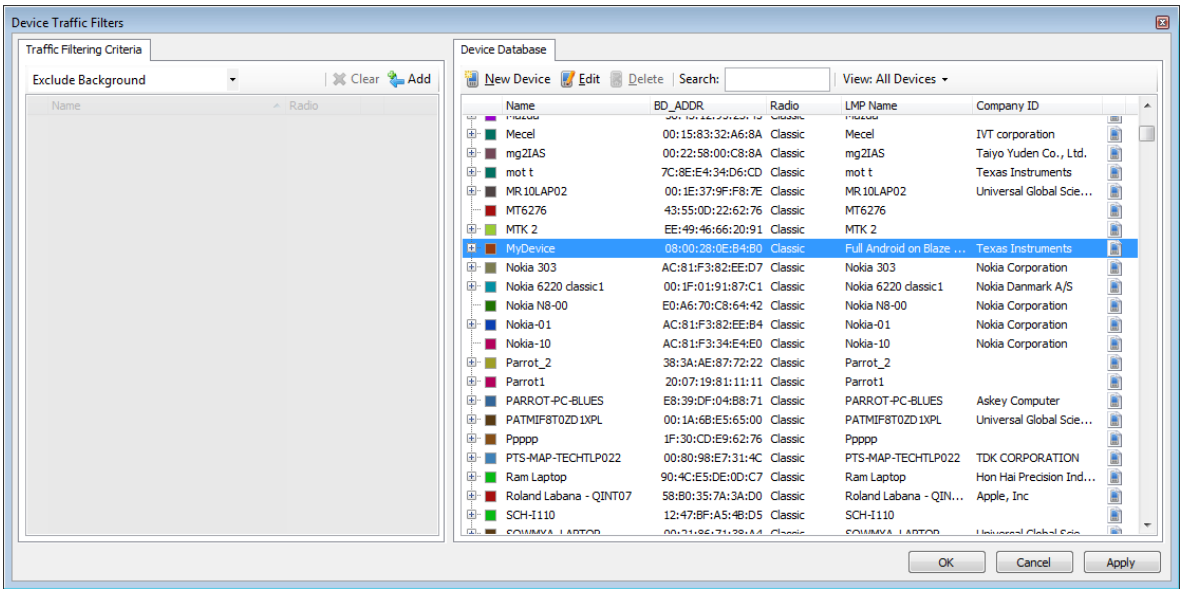
下図のインスタント ピコネットは、程よく混雑している *Bluetooth* 環境を表しています。ざっと見て18のピコネット、スキャッターネットの構成、いくつかのデータ転送やページング イベントが確認できます。このトラフィックはまたインスタント タイミングやオーバービューウィンドウなどでも見ることができます。



2つの *Bluetooth* デバイス間の通信、または特定のデバイスに関する全てのトラフィックのみを、そしてインスタント ピコネットだけでなく BEX400 アナライザ ソフトウェアで表示される全てのウィンドウで見たい場合はどうしたらいいでしょうか？それを実現するには、オーバービューでのインスタント フィルタの使用などいくつかの方法がありますが、ここでは下記のようにツールバーからアクセス可能なデバイス トラフィック フィルタを使ってみます。



すると、下図のようにデバイス トラフィック フィルタが表示されます。**デバイス データベース** と **トラフィック フィルタリング クライテリア** のタブがあり、これらを用いてアナライザ ソフトウェアのいたるところで何を表示するか正確に定義することができます。

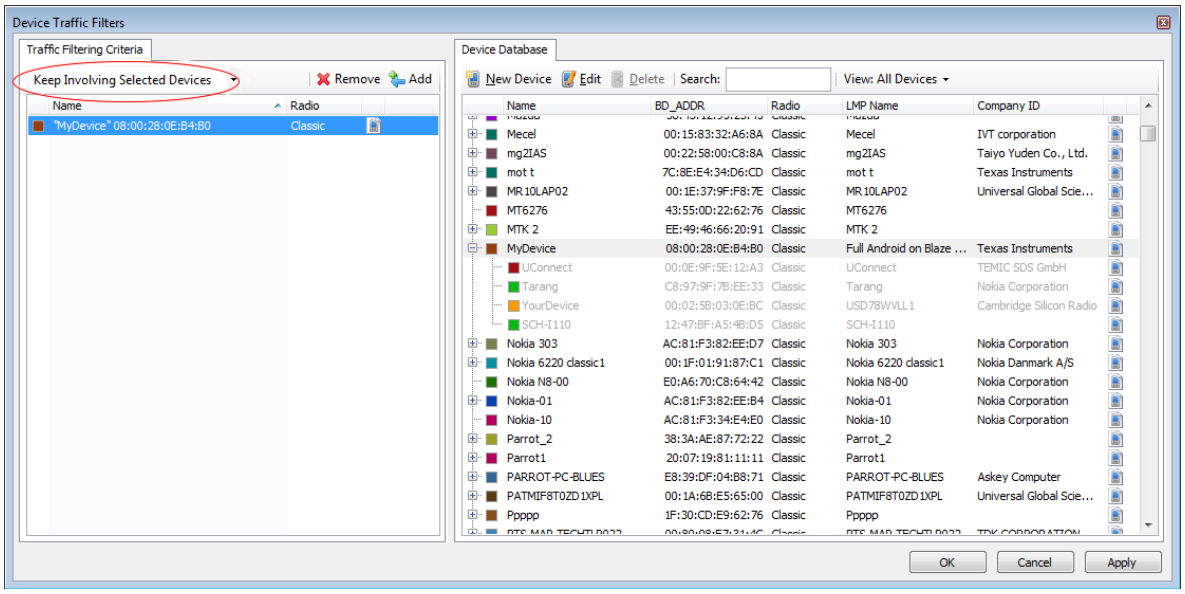


データベースは、過去に記録された全てのデバイスと現在のキャプチャで記録されたデバイスを、それらの間で確立された通信のリストとして表示します。

では、自分で **MyDevice** という名前に変えたものを含む全てのトラフィックを表示するフィルタ基準を作ってみましょう。必要な作業は、**デバイス データベース** に表示されている **MyDevice** を *トラフィック フィルタリング クライテリア* に追加するだけです。

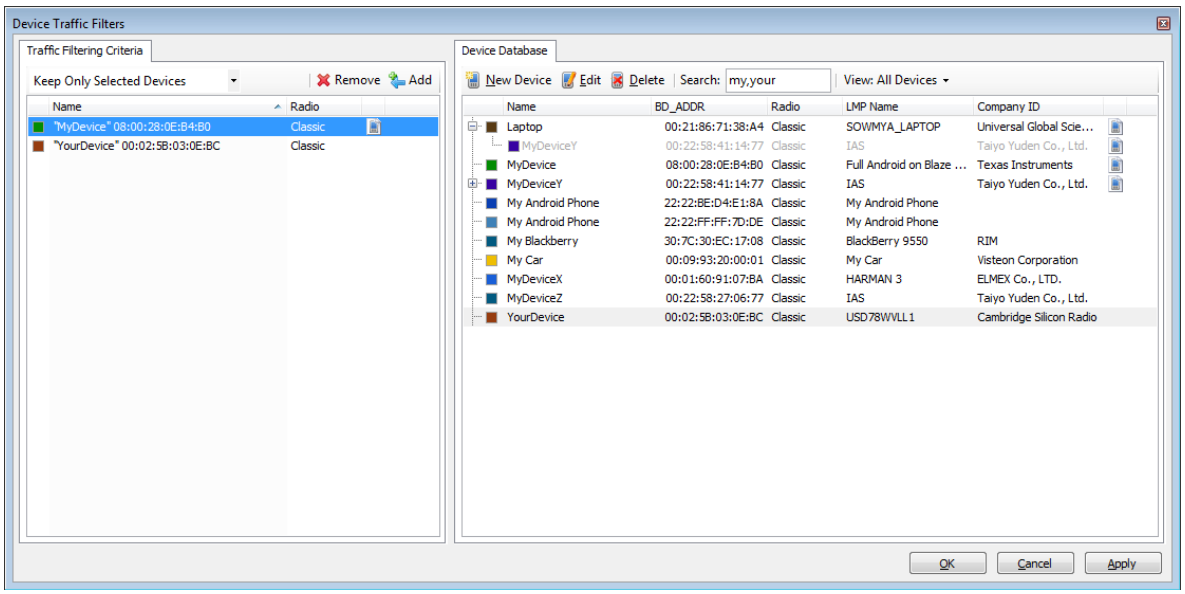
役立つヒント： データベース内の色々なカラムにある文字列の検索を **サーチ ボックス**を用いて行うことができます。また、カラムのヘッダーをクリックすることで全てのカラムのソートを行うことができます。

そして、**MyDevice** をダブルクリックすると **トラフィック フィルタリング クライテリア** に追加されます。**MyDevice** は、”Keep Involving Selected Devices” ラベルの下に追加されることに注意してください。この意味は、**MyDevice** を含むトラフィックのみを表示するということで、アナライザ ソフトウェアの全てのウィンドウからその他の全てのトラフィックが隠されます。



これで、当初は40個くらいあったデバイスの膨大な記録が、今はアナライザ ソフトウェアの全てにおいて **MyDevice** とそれと通信を行っている 4つのデバイスのトラフィックのみに減りました。
この場合、もう一つの利点があります。このフィルタをかけたかたちで記録を保存 （*File - Save Filtered Copy*）、すると、トレース ファイルのサイズを著しく小さくすることができます。

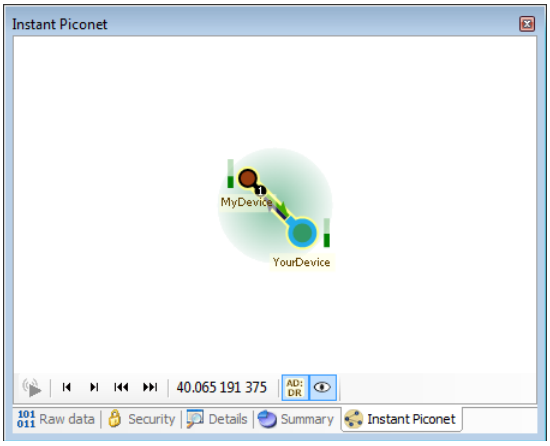
次に、**MyDevice** とそれと通信を行っている全てのデバイスと照らし合わせて、**MyDevice** と **YourDevice** 間のトラフィックのみを見たい場合にはどうすればいいのでしょうか？
問題ありません。下に示すように、**YourDevice** を *トラフィック フィルタリング クライテリア* に追加します。



たとえ **MyDevice** と **YourDevice** がその他のデバイスと通信していたとしても、それらのデバイスに関するトラフィックは表示されず、 **MyDevice** と **YourDevice** 間の通信のみが表示されることに注意してください。を *トラフィック フィルタリング クライテリア* のドロップダウンが“Keep Only Selected Devices”に更新されていることにも注意してください。

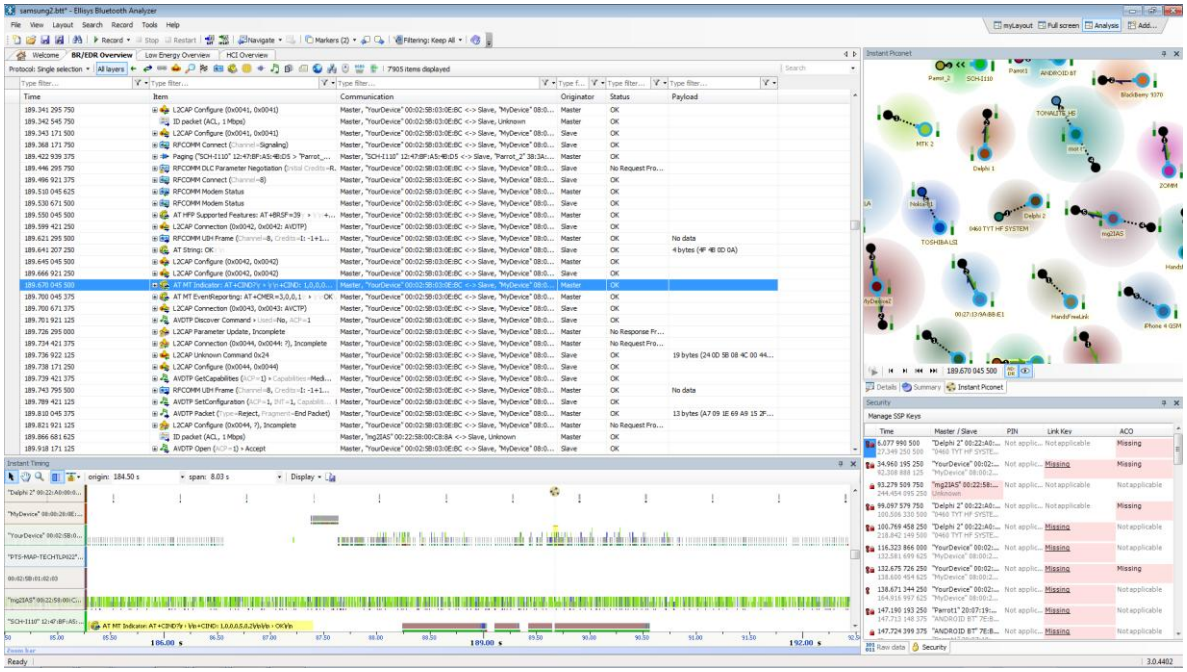
役立つヒント： **サーチ ボックス**は、”My”と”Your”で始まるデバイス名の AND検索を行う場合コンマ “,” を用います。

下図がフィルタを適用した後のインスタント ピコネットの様子です。

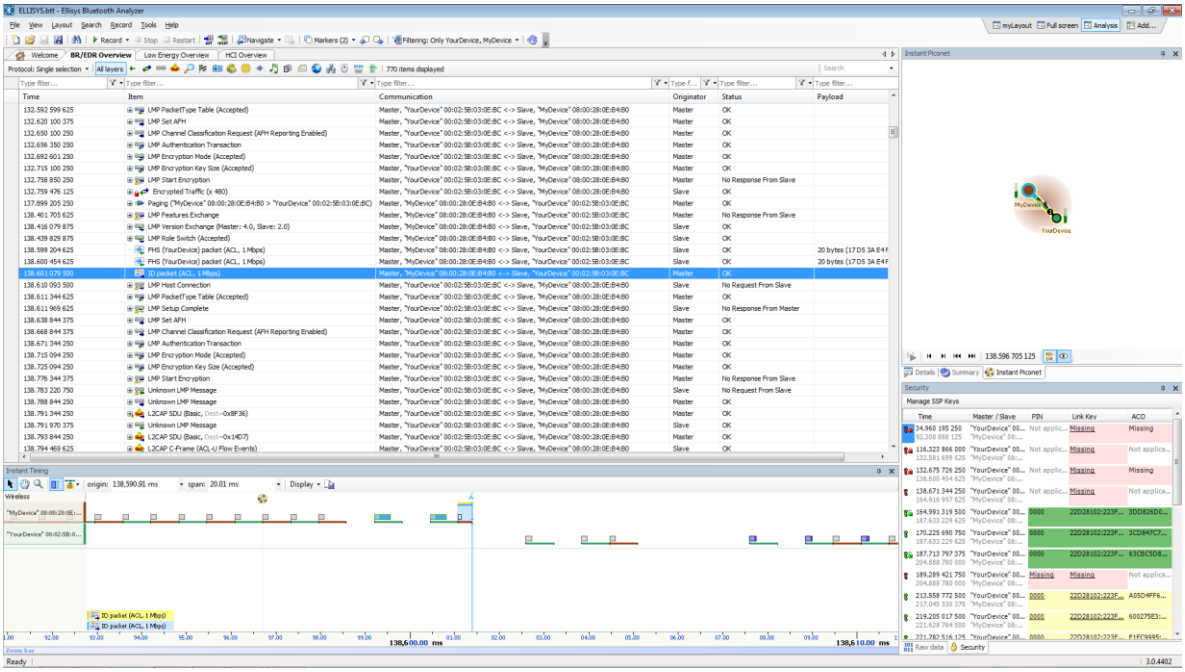


フィルタ適用前後のアナライザ ソフトウェア全体の様子を見ると、より解りやすくなっているのが理解できます。

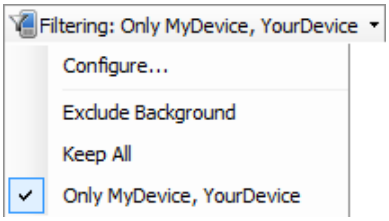
フィルタ適用前：



フィルタ適用後：

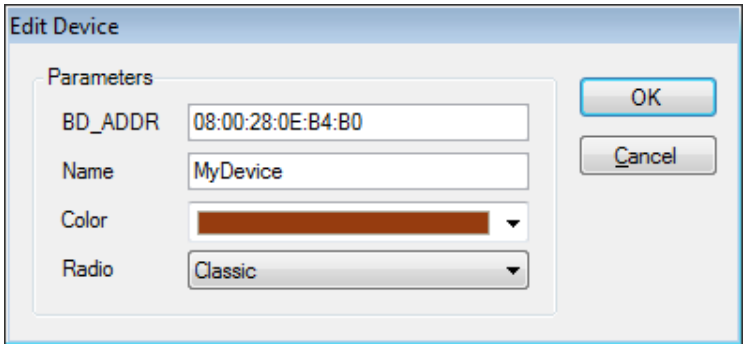


新しいフィルタ （ここでは、**MyDevice** と **YourDevice** 間通信のみ）機能は保存され、ツール バーの *フィルタリング ドロップダウン メニュー* から迅速にアクセスでき、簡単にそのフィルタの有効化・無効化を選択できます。



デバイス プロパティ編集の利点

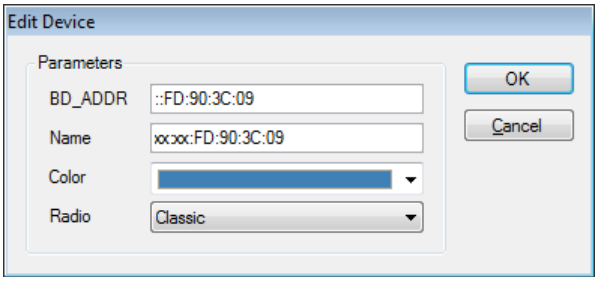
デバイス トラフィック フィルタは、BD_ADDR、名前、色、無線タイプといった様々なデバイスのプロパティの編集機能をユーザーに提供します。これらの編集は、アナライザ ソフトウェアのあらゆるところでデバイスを識別するために使われ、例えば **MyDevice** のような簡単な名前を付けるたり、関連しているデバイスの色を変えることでアナライザ ソフトウェア内での視認効果が著しく向上します。



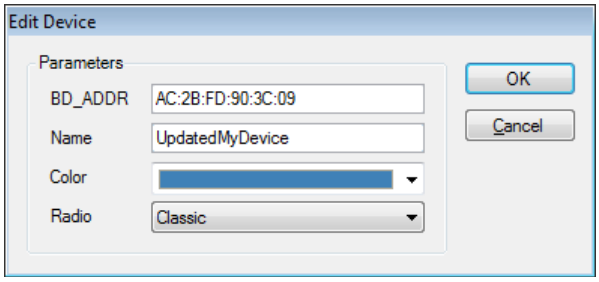
しかし、何故 BD_ADDR が編集可能なのでしょう？デバイスの BD_ADDR はいつも無線で送られるわけではありません。実際にほとんどの場合、無線ではその一部のみが送られます。完全な BD_ADDR は復号化に必要な情報の一つなので、このことはデバイスのトラフィック復号化を困難にしています。 より詳しい情報は、 EEN_BT07J - Secure Simple Pairing について (EEN_BT07 - Secure Simple Pairing Explained) を参照してください。

デバイスに完全な BD_ADDR を送らせる方法（デバイスを検出させるために自身の FHS パケットを送る照会を行わせる等）はありますが、デバイス データベースに BD_ADDR を追加するだけのやり方がより簡単でしょう。この情報はアナライザ ソフトウェアによって保存され、トラフィックを復号化するアナライザ ソフトウェアのセキュリティ機能で使用されます。

記録時：

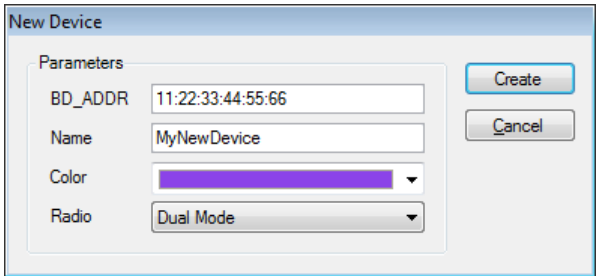


編集後：



新しいデバイスの追加

上記のように、デバイス データベース内にある特定デバイスの部分的な BD_ADDR を編集することができます。おもしろいことに、新しいデバイスの記録を採ることなく新しいデバイスを追加することができます。単純に、デバイス トラフィック フィルタ の **New Device** ボタンをクリックして、必要に応じでプロパティを編集するだけです。



このアプローチの利点は、自動検知の必要がなく、デバイスがアナライザ ソフトウェアによって直ちに認識され、特別なケースでの潜在的な問題を回避できることです。

有効な全てのフィルタ機能のまとめ

以下の表は、様々なフィルタ機能とその機能を要約したものです。フィルタ機能に関するより詳しい情報は、アナライザ ソフトウェアと一緒にインストールされる User Manual の第8章を参照してください。

フィルタ タイプ	フィルタ位置	フィルタ機能
インスタント フィルタ	オーバービュー： 各カラムの上	表示されている任意のカラムで include/exclude を指定できる高度に柔軟な文字列フィルタ。ワイルドカード使用可。
プロトコル/プロファイル フィルタ	オーバービュー： 上部のフィルタ バー	Single/Multiple/Custom Grouping を選択。選択されたプロトコル、プロファイルを表示。
インスタント ピコネット Keep-Only フィルタ	インスタント ピコネット： ピコネット上で右クリック	指定されたピコネット、LE 接続のみを表示。
デバイス フィルタ	メニューアイコン右側	現行のキャプチャまたはデバイス データベースに記録された全てのデバイスをリスト表示し、特定のデバイス通信を指定。バックグラウンド トラフィックの非表示指定。
インスタント タイミング表示フィルタ	インスタント タイミング： ツールバー Display ボタン	接続確立のトラフィックとアイドル トラフィックの表示/非表示選択
インスタント タイミング Keep-Only フィルタ	インスタント タイミング： パケット上で右クリック	選択されたピコネットのみを表示
オーバービュー Keep/Exclude フィルタ	オーバービュー： データ上で右クリック	任意のセルの内容に準じて Keep/ Exclude を選択

トラフィックのキャプチャ

EEN_BT03J - 初めてのワイド バンド キャプチャ (EEN_BT03 - Your First Wide-Band Capture) を参照してください。

ソフトウェアの入手

アナライザ ソフトウェアは、Ellisys のWebサイト
http://www.ellisys.com/products/bex400/download.php
から入手できます。

ダウンロードには、Ellisys の承認が必要ですが、Bluetooth SIG のメンバー または Bluetooth 開発に関わっている会社の場合、ほとんど承認されます。

本文書について

本文書は、" EEN_BT08 – Separating the Wheat from the Chaff (Rev. A Updated 2012-01)" を翻訳したものです。
原文、本文書及び Ellisys 製品に関するお問い合わせは、Ellisys 日本総代理店 ガイロジック株式会社 (0422-26-8211, es@gailogic.co.jp) までご連絡ください。
その他の翻訳版エキスパートノートは、https://www.gailogic.co.jp/db/bt/expert_notes をご覧ください。

Bluetooth プロトコル・アナライザ販売窓口 (ガイロジック株式会社)

0422-26-8211 es@gailogic.co.jp https://www.gailogic.co.jp/db/bt