



はじめての広帯域記録

データを正しく記録するための方法

はじめに

Ellisysの広帯域同時記録型のスニッファは、初めての方でも非常に使いやすく設計されています。例えば、設定をしなくても、ワンクリックで記録を開始できます。記録を開始し、対象となるデバイスを接続すると、設計基準への適合性、信頼性の側面、エラー、干渉問題など、さまざまな性能やその他の動作をすぐに把握することができます。

広帯域同時記録方式では、すべてのトラフィックがすぐに捕捉され、リアルタイムで表示されます。これを有効活用するために、解析対象のデバイスに関する情報のみを表示させる方法があります。今回、ユーザーの皆様にとって理想的なデータを取得するために、いくつかの役立つ情報を紹介していきます。このエキスパートノートでは、Ellisysアナライザの効果を最大限に引き出すために必要な複数のステップを理解頂くことができます。

ファーストステップ

Ellisysの広帯域同時記録型スニッファは、記録した情報や、リンクキーなどのユーザーが入力した情報から、デバイスの重要なパラメータを学習し、保持するように設計されています。→情報を正常に表示するためには、BD_ADDR、デバイス名、SDPパラメータ、L2CAPチャンネル、リンクキー、オーディオコーデックなどの情報が必要です。

リンクキーは、HCIを介して記録したり、手動で入力したり、あるいはプログラムを用いて入力したりすることができ、今後の接続にも使用できるように保存されます。デバイスがIRK (Identity Resolving Key) を使用している場合も同様で、アナライザがそれを捕捉し、ソフトウェアがそれを記憶します。

ヒント: 無線が非常に混雑した環境では、Instant Piconetのツールバーにある“目”のアイコンの選択を解除して、ブロードキャストトラフィックを非表示にします。これにより確立された、または確立しつつあるピコネットを視覚的に分離することができます。Device filterにデバイスが認識されたら、これを再びオンにして、フィルタに含まれるデバイスによって作成されたブロードキャストイベントを見ることができます。

フィルタリング

ソフトウェアで情報をフィルタリングする方法は数多くあります。広帯域同時記録装置の場合、これらの様々なフィルタを使いこなすことが、対象デバイス、対象プロトコル、対象パケットなどを迅速かつ効率的に切り分けるための鍵となります。最も広い範囲のフィルタはデバイスベースのフィルタで、ユーザーが指定したデバイスを表示または非表示にするものです。

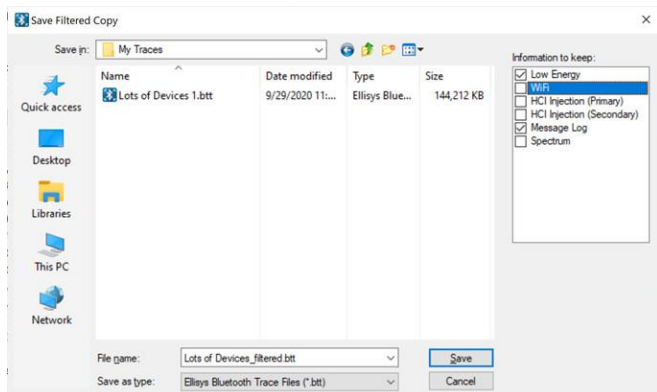


図1 Saving a Filtered Copy

最初の記録では、何十、何百ものデバイスが表示され、そのうちのいくつかが解析対象となるため、多くのユーザーはデバイスフィルタを設定することを最初のステップとしています。デバイスベースのフィルタを適用するには、Piconetウィンドウでピコネットを右クリックしたり、OverviewのCommunication欄で通信しているペアを右クリックしたり、Deviceウィンドウを使用したり、ユーザーマニュアルで詳しく説明されているその他の方法があります。

ヒント: デバイスフィルタをかけた後、そのフィルタによって識別されたデバイスだけの新しいトレースファイルとして保存することができます。この機能を実行するにはFileメニューのSave Filtered Copyで実行できます。図 1 を参照してください。さらに、スペクトラム、Wi-Fi、HCIなど特定のデータを削除することもできます。

これにより、ファイルサイズが大幅に削減され、ファイルの共有が容易になります。(Fileメニューにあるshare to cloudを参照してください)。元のトレースファイルは置き換えられず、新しいトレースファイルが作成されます。

記録のプロセス

1 ポジション

アナライザと機器を適度に近づけて配置する。(最適な配置の詳細については、エキスパートノートEEN_BT04「Analyzerの最適な配置」を参照してください)。



2 設定

必要に応じて、記録設定を行います (“Record” → “Recording Options”)。これにより、記録したい無線トラフィックの種類や有線トラフィックの種類をアナライザに伝え、無線の感度やトレースファイルの自動分割など、その他の項目を制御します。



3 記録

これで、メインツールバーの“Record”ボタンを選択するだけで、記録を開始する準備が整いました。



4 接続

テスト対象のBluetooth機器を接続します。



5 停止

デバイスのトラフィックを十分に記録したら、Stopボタンを選択して記録を停止します。これで、Ellisysソフトウェアの多くのウィンドウを使ってデータを掘り下げることができます。この作業は、記録中にも行うことができます。



6 保存

将来の分析のためにトレースを保存します。エリア内のすべてのデバイスが保存されますが、解析対象のデバイスだけを保存できる方法もあります (後述)。

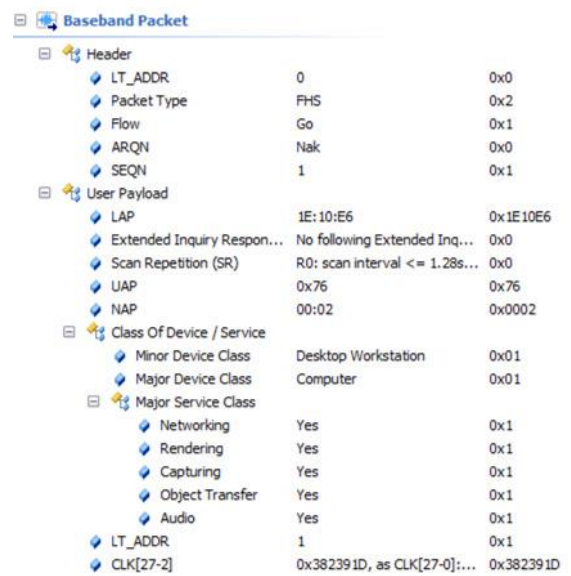


デバイスデータベースの自動生成

前述のように、Ellisysのアナライザソフトウェアは、記録したトラフィックから、デバイスに関する様々な詳細情報を学習します。Ellisysのアナライザソフトウェアが必要とする最初の情報は、デバイスのBD_ADDR (Bluetoothデバイスアドレス) です。

通信している2つのデバイスの一方のBD_ADDRは、接続が記録されたときに決定されますが (BR/EDRまたはLow Energyの使用に応じて、それぞれページングまたはアドバタイジングのいずれか)、接続しているデバイスのBD_ADDRは、接続からは知ることができません。すべてのデバイスにBD_ADDRを送信させる簡単な方法は、Bluetoothデバイスからのディスクバリーを行うことです。例えば、Bluetoothの問い合わせ (BR/EDR) が送信されると、近くにあるすべてのデバイスは、自分のBD_ADDRやその他の有用な情報を含むFHSパケットを送信します。

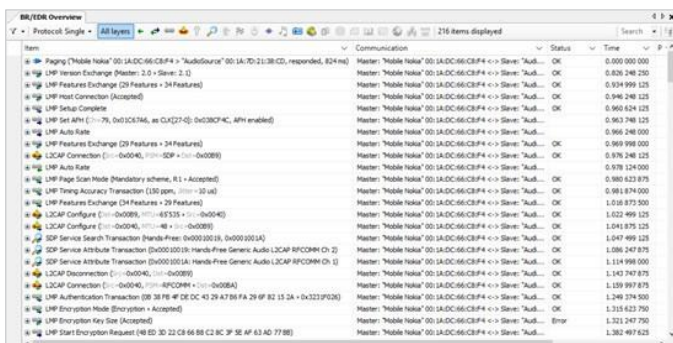
典型的なFHSパケットの内容については、[図2](#)を参照してください。



Field	Value	Hex
Header		
LT_ADDR	0	0x0
Packet Type	FHS	0x2
Flow	Go	0x1
ARQN	Nak	0x0
SEQN	1	0x1
User Payload		
LAP	1E:10:E6	0x1E10E6
Extended Inquiry Respon...	No following Extended Inq...	0x0
Scan Repetition (SR)	R0: scan interval <= 1.28s...	0x0
UAP	0x76	0x76
NAP	00:02	0x0002
Class Of Device / Service		
Minor Device Class	Desktop Workstation	0x01
Major Device Class	Computer	0x01
Major Service Class		
Networking	Yes	0x1
Rendering	Yes	0x1
Capturing	Yes	0x1
Object Transfer	Yes	0x1
Audio	Yes	0x1
LT_ADDR	1	0x1
CLK[27-2]	0x382391D, as CLK[27-0]...	0x382391D

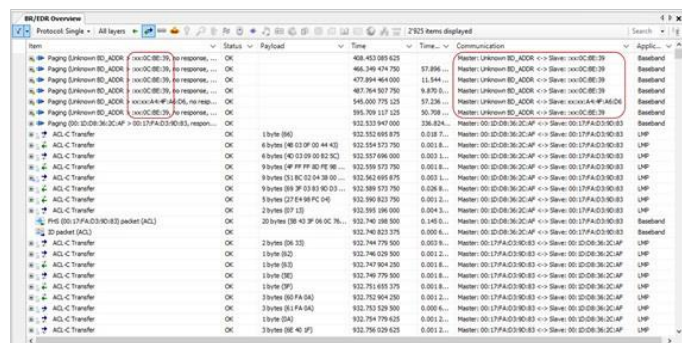
図2 典型的なFHSパケットコンテンツ

ヒント: メニューアイコンのFilterボタンの押下で表示されるDevices ウィンドウでは、デバイス名を変更することができます。Device Databaseタブでデバイスを選択し、Edit ボタンを押すと、Edit Deviceダイアログが表示され、そのNickname欄に任意の名前を入れることで変更できます。



Item	Communication	Status	Time
Paging (Mobile Nokia) [00:1A:DC:66:C8:F4] <-> [AudioSource] [00:1A:7D:21:38:CD, responded, 824 ms]	Master: 'Mobile Nokia' [00:1A:DC:66:C8:F4] <-> Slave: 'Aud...'	OK	0.000 000 000
LMP Version Exchange (Master: 2.0 > Slave: 2.1)	Master: 'Mobile Nokia' [00:1A:DC:66:C8:F4] <-> Slave: 'Aud...'	OK	0.826 248 250
LMP Features Exchange (29 Features > 34 Features)	Master: 'Mobile Nokia' [00:1A:DC:66:C8:F4] <-> Slave: 'Aud...'	OK	0.934 999 125
LMP Host Connection (Accepted)	Master: 'Mobile Nokia' [00:1A:DC:66:C8:F4] <-> Slave: 'Aud...'	OK	0.946 248 125
LMP Setup Complete	Master: 'Mobile Nokia' [00:1A:DC:66:C8:F4] <-> Slave: 'Aud...'	OK	0.960 624 125
LMP Set APH ([-79, Div 0x76], as CLK[27-0], 0x382391D, APH enabled)	Master: 'Mobile Nokia' [00:1A:DC:66:C8:F4] <-> Slave: 'Aud...'	OK	0.963 748 125
LMP Auto Rate	Master: 'Mobile Nokia' [00:1A:DC:66:C8:F4] <-> Slave: 'Aud...'	OK	0.966 248 000
LMP Features Exchange (29 Features > 34 Features)	Master: 'Mobile Nokia' [00:1A:DC:66:C8:F4] <-> Slave: 'Aud...'	OK	0.969 999 000
L2CAP Connection ([-0x045], [-0x045], [-0x0000])	Master: 'Mobile Nokia' [00:1A:DC:66:C8:F4] <-> Slave: 'Aud...'	OK	0.976 248 125
LMP Auto Rate	Master: 'Mobile Nokia' [00:1A:DC:66:C8:F4] <-> Slave: 'Aud...'	OK	0.978 124 000
LMP Page Scan Mode (Transition scheme, E1 > Accepted)	Master: 'Mobile Nokia' [00:1A:DC:66:C8:F4] <-> Slave: 'Aud...'	OK	0.980 623 875
LMP Paging Acceptance (Transition scheme, E1 > Accepted)	Master: 'Mobile Nokia' [00:1A:DC:66:C8:F4] <-> Slave: 'Aud...'	OK	0.983 874 000
LMP Features Exchange (34 Features > 29 Features)	Master: 'Mobile Nokia' [00:1A:DC:66:C8:F4] <-> Slave: 'Aud...'	OK	1.018 873 000
L2CAP Configure ([-0x0009], [0x0009], [-0x0000])	Master: 'Mobile Nokia' [00:1A:DC:66:C8:F4] <-> Slave: 'Aud...'	OK	1.022 499 125
L2CAP Disconnect ([-0x0000], [0x0000])	Master: 'Mobile Nokia' [00:1A:DC:66:C8:F4] <-> Slave: 'Aud...'	OK	1.044 875 125
L2CAP Service Search Transaction (Hands-Free: 0x00000010, 0x0000001A)	Master: 'Mobile Nokia' [00:1A:DC:66:C8:F4] <-> Slave: 'Aud...'	OK	1.047 499 125
L2CAP Service Attribute Transaction (0x00000010: Hands-Free Generic Audio L2CAP RFCOMM Ch 2)	Master: 'Mobile Nokia' [00:1A:DC:66:C8:F4] <-> Slave: 'Aud...'	OK	1.086 247 875
L2CAP Service Attribute Transaction (0x0000001A: Hands-Free Generic Audio L2CAP RFCOMM Ch 2)	Master: 'Mobile Nokia' [00:1A:DC:66:C8:F4] <-> Slave: 'Aud...'	OK	1.114 998 000
L2CAP Disconnect ([-0x0000], [0x0000])	Master: 'Mobile Nokia' [00:1A:DC:66:C8:F4] <-> Slave: 'Aud...'	OK	1.142 747 875
L2CAP Connection ([-0x0040], [0x0040], [-0x0000])	Master: 'Mobile Nokia' [00:1A:DC:66:C8:F4] <-> Slave: 'Aud...'	OK	1.159 997 875
LMP Authentication Transaction (0x 38 FE #F DE DC 43 29 A7 88 FA 29 #F 82 15 1A + 0x321F026)	Master: 'Mobile Nokia' [00:1A:DC:66:C8:F4] <-> Slave: 'Aud...'	OK	1.248 374 500
LMP Encryption Mode (Encryption > Accepted)	Master: 'Mobile Nokia' [00:1A:DC:66:C8:F4] <-> Slave: 'Aud...'	OK	1.321 423 750
LMP Encryption Key Size (Accepted)	Master: 'Mobile Nokia' [00:1A:DC:66:C8:F4] <-> Slave: 'Aud...'	Error	1.321 423 750
LMP Start Encryption Request (48 5D: 3D 2C 68 68 C2 3C 3F 3E AF 63 6D 77 8E)	Master: 'Mobile Nokia' [00:1A:DC:66:C8:F4] <-> Slave: 'Aud...'	OK	1.382 407 625

図3 LMP名のキャプチャと表示



Item	Communication	Status	Time	Time...	Time...
Paging (Unknown BD_ADDR [xx:xx:xx:xx:xx:xx]) <-> [no response, ...]	Master: 'Unknown BD_ADDR' [xx:xx:xx:xx:xx:xx] <-> Slave: 'no:CC:8E:39'	OK	408 453 885 625		Baseband
Paging (Unknown BD_ADDR [xx:xx:xx:xx:xx:xx]) <-> [no response, ...]	Master: 'Unknown BD_ADDR' [xx:xx:xx:xx:xx:xx] <-> Slave: 'no:CC:8E:39'	OK	466 249 474 750	57 896...	Baseband
Paging (Unknown BD_ADDR [xx:xx:xx:xx:xx:xx]) <-> [no response, ...]	Master: 'Unknown BD_ADDR' [xx:xx:xx:xx:xx:xx] <-> Slave: 'no:CC:8E:39'	OK	472 994 640 000	11 544...	Baseband
Paging (Unknown BD_ADDR [xx:xx:xx:xx:xx:xx]) <-> [no response, ...]	Master: 'Unknown BD_ADDR' [xx:xx:xx:xx:xx:xx] <-> Slave: 'no:CC:8E:39'	OK	487 764 807 250	9 876...	Baseband
Paging (Unknown BD_ADDR [xx:xx:xx:xx:xx:xx]) <-> [no response, ...]	Master: 'Unknown BD_ADDR' [xx:xx:xx:xx:xx:xx] <-> Slave: 'no:CC:8E:39'	OK	545 000 775 125	35 226...	Baseband
Paging (Unknown BD_ADDR [xx:xx:xx:xx:xx:xx]) <-> [no response, ...]	Master: 'Unknown BD_ADDR' [xx:xx:xx:xx:xx:xx] <-> Slave: 'no:CC:8E:39'	OK	595 769 117 125	50 768...	Baseband
Paging (00:1A:DC:66:C8:F4 > 00:17FA:03:90:83, no resp...	Master: '00:1A:DC:66:C8:F4' <-> Slave: '00:17FA:03:90:83'	OK	632 533 947 000	238 824...	Baseband
ACL-C Transfer	1 byte (96)	OK	632 532 068 875	0.018...	Baseband
ACL-C Transfer	4 bytes (48 03 0F 00 44 03)	OK	632 534 037 500	0.018...	Baseband
ACL-C Transfer	6 bytes (4D 03 09 00 82 0C)	OK	632 537 696 000	0.013...	Baseband
ACL-C Transfer	9 bytes (FF FF FF 00 FE 1E ...)	OK	632 539 173 750	0.013...	Baseband
ACL-C Transfer	9 bytes (51 8C 02 0A 38 00 ...)	OK	632 552 668 875	0.013...	Baseband
ACL-C Transfer	9 bytes (08 3F 03 83 90 03 ...)	OK	632 558 573 750	0.026...	Baseband
ACL-C Transfer	5 bytes (27 E4 08 FC D6 ...)	OK	632 569 823 750	0.013...	Baseband
ACL-C Transfer	20 bytes (07 15 ...)	OK	632 565 086 000	0.043...	Baseband
PRE (00:17FA:03:90:83 packet (ACL))	20 bytes (08 43 3F 04 0C 7E ...)	OK	632 746 088 500	0.140...	Baseband
IP packet (ACL)	20 bytes (0A 32)	OK	632 746 823 375	0.008...	Baseband
ACL-C Transfer	19 byte (82)	OK	632 746 829 500	0.012...	Baseband
ACL-C Transfer	1 byte (82)	OK	632 747 804 250	0.013...	Baseband
ACL-C Transfer	1 byte (0E)	OK	632 749 779 500	0.013...	Baseband
ACL-C Transfer	1 byte (0F)	OK	632 751 683 375	0.016...	Baseband
ACL-C Transfer	3 bytes (00 FA 04)	OK	632 752 804 250	0.012...	Baseband
ACL-C Transfer	3 bytes (61 FA 04)	OK	632 753 529 500	0.008...	Baseband
ACL-C Transfer	1 byte (04)	OK	632 754 774 625	0.012...	Baseband
ACL-C Transfer	3 bytes (0E 40 3F)	OK	632 756 029 625	0.012...	Baseband

図4 完全なBD_ADDRが不明なケース

さらに、ほとんどのBluetoothスタックはLMP名を定めていますので、これもEllisysのアナライザが学習し、ソフトウェアの様々な場所で使用されます。[図3](#)のCommunicationの欄をご覧ください。

デバイスのトラフィックを記録する前に、アナライザがデバイスの完全なBD_ADDRを知らない場合でも、スニッパはほとんどの場合、BD_ADDRを部分的に判断することができます。この場合、[図4](#)に示すように、BD_ADDRに「xx」と表示され、上位バイトが欠落していることがわかります。トラフィックは正常に記録できますが、BD_ADDRが完全にわからない場合、その場でトラフィックを復号することはできません。これは、BD_ADDRはセキュリティアルゴリズムが必要とする情報の1つであるためです。

手動でのデバイスデータベースの作成

アナライザソフトウェアにデバイスアドレスを通知する別の方法として、デバイスデータベースを手動で入力する方法があります。この方法は、Deviceウィンドウで行います。ウィンドウを表示するには、メインメニューから”View” → ”Device”を選択します（またはメインツールバーの”Filtering:”と書かれたドロップダウンメニューから”Configure”を選択します）。

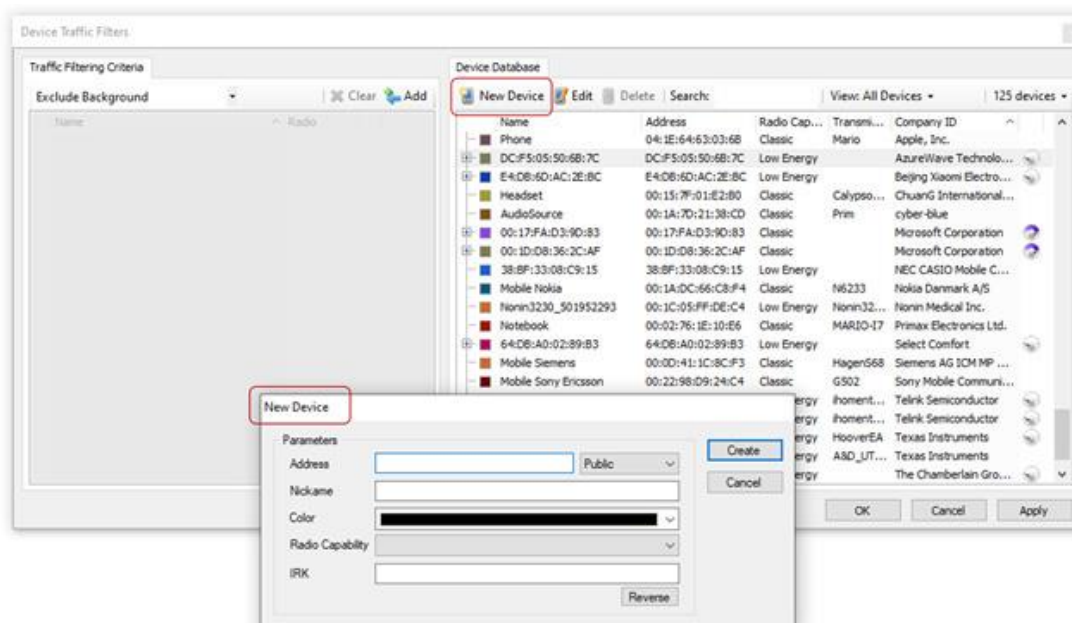


図5 手動でのデバイスデータベースの作成

ヒント: ペアリングプロセスを記録することが重要です。

New Deviceボタン（図5）をクリックすると、BD_ADDR、デバイス名、表示色などを含む新規デバイス情報を一から作成することができます。新しいデバイス情報を作成する前に、そのデバイスがまだデータベースに存在しないかどうかを確認すると便利です。**Search**フィールドはこの確認に非常に役立ちます。このウィンドウでは、既存のデバイスの情報を更新することができ、特に一部のBD_ADDRしか解らなかったデバイスのアドレスを補完するのに便利です（上記のセクションで説明しています）。また、不要になった既存のデバイスを削除することもできます。

次に必要な情報を入手

デバイスのBD_ADDRを完全に把握した上で、ペアリングの手順を記録することで、Ellisysソフトウェアは不足している部分を学習することができます。デバイスはペアリングしてリンクを確立する際、お互いの機能情報を交換（Service Discovery）します。アナライザは、この情報を元にプロトコル、プロファイル、サービス等を正し

図5 手動でのデバイスデータベースの作成

ペアリングは、リンクキーを決定するのにも有効です。PINコードベースのペアリングの場合、またはデバッグモードのSSPペアリングの場合、Ellisysのアナライザは自動的にリンクキーを推測します。その他のケースでは、リンクキーをSecurityウィンドウに入力する必要があります（HCIが記録されている場合、そのインターフェース上でリンクキーが交換されると、ソフトウェアは自動的にリンクキーを抽出します）。これらの手順を踏めば、この2つのデバイスを含むすべての接続は、スニッファによって完璧に解読されます。

スニッファは、データを復号するためのリンクキーを含め、有用な情報を表示するために必要なすべてのデータを記憶します。

異なるアプローチ

上記の手順は当然ながら提案に過ぎず、他にも様々なアプローチが可能です。最も重要なことは、上述のデバイス情報は、データを復号化し、様々なプロトコルにデコードするためにのみ必要であるということです。広帯域同時記録装置は、このような情報がなく、暗号化されたトラフィックであっても、あらゆるBluetoothパケットを記録することができるからです。

もう一つの重要なコンセプトは、Ellisysソフトウェアが復号化に必要な情報を取得した際に、その情報をPC内のデータベースとトレースファイル自体に保存するということです。記録時にいくつかの情報が欠落している場合、トレースはすぐには使用できないかもしれません。しかし、不足している情報は後から更新される可能性があり、複合化に必要な情報がソフトウェアによって学習されると、暗号化されていた古いトレースファイルも正常に復号化できます。

簡単な例を見てみましょう。全く新しい2つのデバイスをアナライザで記録します。この2つのデバイスはすでにペアリングされており、再度ペアリングする必要はありません。また、問い合わせも行わずに、すぐに接続の記録を開始します。

この場合、EllisysのアナライザはマスターデバイスのBD_ADDRを知るだけで、他の情報は何もないので、データを復号化することはできません。一度この記録を保存します。

次に、スレーブだったデバイスをマスターにして、新たに2回目の記録を行います。この時点で、両方のデバイスのBD_ADDRがわかり、リンクキーが提供されると、データを復号することができます。すべての情報がわかったところで、最初の記録を再度開くと、必要な情報がソフトウェアによって学習されているため、復号化とデコードに成功します。新たに判明した情報は、必要な情報がすべて含まれているこのトレースに保存されます。この情報は、実際のデバイスにアクセスしたことのない遠隔地にいるスタッフと交換することができます。

おわりに

このEllisysエキスパートノートでは、広帯域同時記録装置が、一般的な記録の一部として、スニッフィングされたすべてのトラフィックを記録することを学びました。また、より完璧な記録を実現するために、デバイスデータベースを自動または手動で入力する方法、デバイスベースのフィルタを使用してファイルをより効率的に保存する方法、アナライザがリンクキー、IRK、コーデックなどの重要な要素をどのように記録して保存するかについて、新しい方法を探り、学びました。

詳細はellisys.comをご覧ください。es@gailogic.co.jp までご連絡ください。

本文書について

本文書は、" EEN_BT03 - Your First Wide-band Capture.pdf (Rev. C Updated 2021-09)" 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。

その他の関連資料

- EEN_BT06J- Bluetooth セキュリティのウソ？ホント？



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)

 042-26-8211

 es@gailogic.co.jp

 <https://www.gailogic.co.jp/db/bt>

Copyright© 2021 Ellisys. 全ての権利はEllisysに帰属します。Ellisys、Ellisysロゴ、Better Analysis、Bluetooth Explorer、Bluetooth Tracker、Bluetooth Vanguard、Ellisys Grid、Bluetooth QualifierはEllisysの商標であり、一部の管轄区域では登録されている可能性があります。Bluetooth®のワードマークおよびロゴは、Bluetooth SIG, Inc.が所有する登録商標であり、Ellisysによるこれらのマークの使用はライセンスに基づくものです。Wi-Fi®およびWi-Fi Allianceのロゴは、Wi-Fi Allianceの商標です。その他の商標および商号は、それぞれの所有者に帰属します。ここに記載されている情報は例示を目的としたものであり、設計の参考にすることを意図したものではありません。具体的な設計指針については、最新の技術仕様書を参照してください。