



Ellisys Expert Note | EEN\_BT03 Rev. C

# 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。

Save in:	My Traces		~	3 🕫 📁 🖽	•	Information to keep:		
Quick access Desktop Libraries This PC	Name	← ces 1.btt	Date modified 9/29/2020 11:	Type Ellisys Blue	Size 144,212 KB	Lew Every     Kill Nector (Presy)     Kill Nector (Presy)     Kill Nector (Secondary     Kessay Eventual     Spectrum		
	File game:	Lots of Devices	_filtered.btt	~	Save			
		-	Trans Eles (* Las)	1252	Connect			

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 別されたデバイスのみ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。



## 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 カ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。



図2 典型的なFHSパケットコンテンツ

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。

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。

BR/EDR Overview	RA/DDR Overview									
' + Protocol Single + 📶 layers + 🕫 👄 🍦 🖓 💭 🐑 🕫 🔶 + 🎝 📾 🚳 🕼 🌐										
item	Communication 🗸	Status v Time	v p.A	item v S	ltatus 🗢 Payload	~	Time	v Time_ v	Communication	v Applic
# Pacing (Noble Noble Noble 100: 14:00: 66: CB/F4 > "AudioSource" 00: 14:70: 21:38:CD. responded, 824 no.	Master: "Mobile Noka" 00: 18:00:68:08:F4 <-> Save: "Aud	OK 0.00	0 000 000	Paging (Unknown BD_ADOR \$ coci0Ci8E:39, to response,	ok		408.453 085 625		Haster: Unknown 3D_ADOR <-> Slave: :xx:0C:8E:39	Baseband
a lig (MD Version Exchange Master: 3.0 x Gauer 2.1)	Master: "Mobile Mobile" (0): 12-00" ddi C'Biffé cuis Taver: "Aud	05 0.62	6 248 250	R Paging (Unknown BD_ADDR > soci0C8E:39, no response, 0	OK -		465.349 474 750	57.896	Heater: Unknown BD_ADOR <-> Slave: pxc0Ci8E:39	Seebard
with UNE Features Purtante (29 Features - 34 Features)	Master: "Mobile Notes" 00:14-00" 66:02/F4 con Save: "Aut	OK 0.93	4 999 125	R Paging (Unknown 80_ADDR > INVIDEREID), no response,	OK .		477.894 464 000	11.544	Haster: Unknown 80_ADDR <> Save: cor00.8E:39	Beeberd
a life the send Connection (Accented)	Martine: "Mobile Moles" (0) 12 (0) dd (78 dd (78 dd c. 5 (Bener, "And	00 0.04	0.748 175	R Paging (Unknown 8D_ADDR > 1000008E139, to response,	ok		487.764 507 750	9.870 0	Master: Unknown 8D_ADDR <>> Save: :xx:0C:8E:39	Baseband
A MULTINE Set of Consister	Marter: "Molda Isola" (h) 18 (h) 48 (h) 48 (h) 48 (h)	CV 0.00	0.674 175	R Paging Univouri 6D_ADDR > xxxxxA4:#544-D6, no resp	ox		545.000 775 125	57.236	Naster: Unknown 8D_ADDR <>> Save: x0:x0:A40#1A6:D6	Basebant
THE DEPARTMENT OF THE CONTRACT OF THE CONTRACT OF THE	Marter: Make Value 100 10 00 46 00 46 4 5 10 10 10	0.00	3 745 156	# Paging (Unknown 60_ADDR 1_coci0CI8E:39, ho response,	ox		595.709 117 125	50.708	Master: Unknown SD_ADOR <>> Save: :xxx0C6E:39	/ Baseband
a manufacture of the second seco	Harter, House House on skipcing carry or y party, skip-	0.90	1 749 649	# Paging (00:10:08:36:30:4F > 00:17/FA:03:90:83, respon	ok		932.533 947 000	336.824	Master: 00:10:08:36:20:AF <-> Save: 00:17/FA:03:90:83	. Baseband
A VE AUDINE	Haster Proce Note Of SAUCHERSPECT Server Auto	~ 0.90	0 246 000	₩1.2 ACLCTransfer	OK Löyte (66)		932.552 695 875	0.038 7	Master: 00:10:08:36:2C:AF <-> Save: 00:17/FA:03:90:83	UP
and the restrict crowde (to restrict - preserve)	Pater Poperson of provide Carry Constant and	04 0.90	9 998 000	in _ € ACLC Transfer	OK 6 bytes (48 0	0 0F 00 44 43	922.554 573 750	0.0018	Master: 00:10:08:36:2C:AF <-> Save: 00:17/FA:03:90:83	UP
a 👽 LaCAP connection (Jin - 0x0040, Han - 50P + Can - 0x0089)	Masteri Mobie Noka 0011A.DC.66/CB/P4 <-> Seve: Aud	OK 0.97	6 246 125	a 12 ACLC transfer	OK 6 byses (40 0	1 09 00 82 SC)	932.557 696 000	0.003 1	Master: 00:10:08:36:2C:AF <-> Save: 00:17/FA:03:90:83	Dib
a mg UAP Auto Rate	Master: "Hoble Noka" 00: 14:0C:66:CB/F4 <-> Save: "Aud	0.97	8 124 000	a je ACL-C transfer	OK 9 Dytes (4P P	PP 30 PE 98	932.559 573 750	0.0018	Mether: 00: IDID8:36:2CIAF <-> Seve: 00: L7/FAID3:90:83	0.00
Hig LMP Page Scan Mode (Mandatory scheme, R1 + Accepted)	Master: "Mobile Nokia" 07: 1A:DC:66:C8:F4 <-> Save: "Aud	OK 0.98	0 623 875	R. 2 ACLC Transfer	OK POYNER (51.8	02 04 38 00	932.562.095.875	0.003 1	Manari oo solda acadaa <-> savel oo sira acadadaa	1994
R Mg LMP Tining Accuracy Transaction (LS0 ppm, 1/111 - 30 us)	Master: "Hobie Noka" 00: 1A:DC:66:CB:F4 <-> Slave: "Aud	OK 0.98	1874.000	E_6 ACLC Transfer	OK VOYTES (NV J	03839003	932.589 573 750	0.025 8	Masteri 00: D/DB/36/2C/AP <-> Save: 00: D/PA/D3/90/83	0.00
In Fig. UPP Features Exchange (34 Features + 29 Features)	Master: "Hoble Noka" 00: 1A:DC:66:C8:F4 <-> Save: "Au8	OK 1.01	6 873 500	E + ALCHASE	OK 50y9es (276	198 PC 040	932.590 823 750	0.0012.	Master) 00:30:08:36:20:4P <-> Save: 00:37PA.03(90)83	09
🗑 🐳 L2CAP Configure (1)11-0x0089, 1011-165'535 + 5rc-0x0040)	Master: "Hoble Noka" 00: 1A:DC:66:C8:F4 <-> Save: "Aud	OK 1.02	2 499 125	a 7 ACLC haste	OK 2 bytes (07 L		932.595 296 000	0.004 3.	Marteri doi sobel de de la sevel doi si PACISIO ES	
iii 🙀 L2CAP Configure (110-0x0040, 1111-48 + (10-0x0089)	Master: "Hoble Noka" 00: 1A:DC:66:C8:F4 <-> Slave: "Aud	DE 1.04	1875 125	The for the work of the second s	OK TO DAMA DO	0 3P 08 0C 78.	932,740 298 500	0.145 0.1	Marter Do Expensional Annual Seven do Englandida	beseband
B A SDP Service Search Transaction (Hands-Pree: 0x00000018, 0x0000001A)	Master: "Noble Noka" 00: 1A:DC:66:C8/F4 <-> Save: "Aud	OK 1.04	7 499 125	- D beget (ACT)	an and a second second		932.740.823.375	0.000 8	Partier OLED BLBC ALAP 415 Server OLED PARD 2001	- Desegand
# 2 SDP Service Attribute Transaction (Dx00010019: Hands-Free Generic Audo L3CAP RFCORM Ch 2)	Master: "Noble Noka" 00: SA:DC:66:CB:F4 <-> Slave: "Aud	OK 1.08	6 247 875	N N AD Charles	OK Zoynes (US 3	¥.	932,744 779 500	0.003 %.	Nation OF LYPICOLOGIA CO SILVE OF LODE RED. W	199
# 2 SDP Service Attribute Transaction (Dv0001001A: Hands-Free Generic Audio L3CAP RECOMM Ch 1)	Haster: "Hoble Noka" 00: 1A:DC:66:C8:F4 <-> Save: "Aud	OK 1.11	4 998 000	and an Charles	OF These (51)		972 747 009 750	0.001.6	Nation OF 1744 (1240-81 con Same Of 1746 18 20 B	110
# 🖕 L3CAP Deconnection (Int - 0x0040, Int - 0x0089)	Haster: "Hoble Noka" 02: LA:DC:K6:C8:F4 <-> Slave: "Aud	OK 1.14	3 747 875	a + AD C Transfer	OK Libute /SE1		\$12,749 779 500	0.0018.	Master: 00:17/54/03:90:81 c-> Slave: 00:10:08:36:20.4F	LINE
a 🕹 L2CAP Connection (His -0x0040, HIM - AFCOMM + His -0x008A)	Master: "Hoble Noka" 00:1A/DC/66/CB/F4 <-> Save: "Aud	OK 1.15	9 997 875	E 2 ACL C Transfer	OK there (94)		912 751 655 375	0.0018	Naster: 00:17/64/03:90:83 <-> Slave: 00:10:08:36:20.6F	LMP
# 987 UMP Authentication Transaction (08 38 FB # DE DC 43 29 A7 85 FA 29 6F 82 15 2A + 0x3231/F026)	Master: "Mobile Nokia" 00: 18-DC-66-CB:#4 <-> Save: "Aud	OK 1.24	9 374 500	a 2 AO C Transfer	OK 3 bytes (60 F)	1043	932,752 904 250	0.0012.	Marter: 00:17/FA/D3/90:83 <-> Slave: 00:10:08:36:20:4F	Line:
a mile LIMP Encrystein Mode Encrystein + Accepted)	Master: "Mobile Nokia" 00: 18:00:166-08:F4 <-> Save: "Aud	OK 1.31	5 623 750	# 5 + AQ-C Transfer	OK 3 bytes (K1 P	640	932,753 529 500	0.000 6	Nester: 00:17/FA:03/90:83 <-> Save: 00:10:08:36:30:AF	UP
a wa UNP Encryption Key Size (Accented)	Master: "Mobile Noise" 00: 18-DC-66-CB/F4 <-> Gave: "Aut	fmy 1.37	1 247 750	# 2 AD Charafer	OK 10vte (DA)		932,754 779 625	0.0012.	Master: 00:17/FA/03:90:83 <>> Slave: 00:10:06:36:20:AF	UP
H HILL LIMP Start Encryption Request (HILED 3D 22 C8 66 88 C2 8C 3F 55 AF 63 AD 77 88)	Master: "Hoble Noka" 00:1A:DC:66:CB:F4> Save: "Aud-	1.38	2 497 625	H 1 ACL-C Transfer	OK 3 bytes (KE 4	193	932.756 029 625	0.001 2.	Naster: 00:17/FA:03:90:83 <-> Slave: 00:10:08:36:20:AF	1349
				¢						

図3 LMP名のキャプチャと表示

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、スニッファはほとんどの場合、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。



図4 完全なBD\_ADDRが不明なケース



## 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)。

raffic Filtering Criteria			Device Databas	ie .							
Exclude Background	•	• 🔅 Clear 🗞 Add		🗑 New Device 🖉 Edit 🏢 Delete   Search:				View: All 0	levices •	125 devi	vices •
Same	^ Kado		Name Phone P		Address 04:1E:64:63:03:68 DC:F5:05:50:68:70 64:08:60:AC:28:80 00:15:77:60:122:80 00:14:70:21:38:08 00:10:76:40:33:08:08 00:10:76:83:20:47 00:10:65:62:64 00:10:65:77:10:65 00:14:10:66:68:71 00:12:81:10:66 64:08:40:02:89:83		Radio Cap Classic Low Energy Cassic Classic Classic Low Energy Classic Low Energy Classic Low Energy Classic Low Energy	Transmi Mario Calypso Prim Nonin32 MARIO-17 Hagen568 GS02 Homent homent homent	Company ID Apple, Inc. AzurelWave Technolo Beijng Xiaoni Bictro ChaarG International cyber-Blue Microsoft Corporation Microsoft Corporation NEC CASIO Mobile C Nokia Demmark A/S Nonin Medical Inc. Primark Bectonics Ltd Select Confort	• • • • • • • • • • • • • • • • • • •	
	New Device Parameters Address		Mobile Sony Encision 00:22:9			Creat	Classic Classic ergy ergy ergy ergy ergy		Siemens AG 104 MP Sony Mobile Commu Telink Semiconductor Texas Instruments Texas Instruments The Chamberlain Gro	5	
	Color				~	h		ОК	Cancel	App	ίγ
	Radio C IRK	apability		[	~ Reverse						

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。

ヒント:ペアリングプロセスを記録することが重要です。



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をご覧いただくか、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、<u>https://www.gailogic.co.jp/db/bt/expert\_notes</u> をご覧ください。



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□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。