Le Mystère de la Dent Bleue

Point au 30 mars 2022 - Jeronimmo

Présentation

- Ordinateur avec OS Linux Mint.
- Données BT collectées via la carte wireless native, en utilisant l'outil **btmon**.
- Ces données sont analysées et affichées en temps réel avec **Wireshark**.

bthci_evt.bd_addr and !(bthci_evt.bd_addr == 40:60:7b:41:5c:5) + Apple_Inc | RSSI 80 | Source | Random | Alerte | UUID_128 | UUID_32 | Essentiel | Mystere

Time	BD_ADDR	Protocol	RSSI	Peer Address Type	Company ID	Device Name	Data	UUID 16	Service Data	Info	UUID 32	UUID 128	Custom UUID 32	Custom UUID
15:39:42,516565	ee:24:b3:de:98:55	HCI_EVT	-91dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
15:39:42,521571	64:5c:8d:c8:c6:ab	HCI_EVT	-90dBm	Random Device Address				0xfd64,0…	3edc1be05f2…	Rcvd LE Meta (LE Extended Advertising Report)				
15:39:42,522555	64:5c:8d:c8:c6:ab	HCI_EVT	-90dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
15:39:43,338567	6b:84:16:2b:20:20	HCI_EVT	-93dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
15:39:46,462633	71:aa:29:e6:91:93	HCI_EVT	-96dBm	Random Device Address	Apple, Inc.		10054a1c…			Rcvd LE Meta (LE Extended Advertising Report)				
15:39:51,602672	26:61:06:c9:1d:a8	HCI_EVT	-97dBm	Random Device Address	Apple, Inc.		09060305…			Rcvd LE Meta (LE Extended Advertising Report)				
15:39:56,638743	ee:24:b3:de:98:55	HCI_EVT	-86dBm	Random Device Address	Valve Corpora…	LHB-12EBA0…	00020201…			Rcvd LE Meta (LE Extended Advertising Report)				
15:39:56,639732	ee:24:b3:de:98:55	HCI_EVT	-86dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
15:39:58,233765	64:5c:8d:c8:c6:ab	HCI_EVT	-92dBm	Random Device Address				0xfd64,0…	3edc1be05f2…	Rcvd LE Meta (LE Extended Advertising Report)				
15:39:58,234749	64:5c:8d:c8:c6:ab	HCI_EVT	-91dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
15:40:06,786850	45:27:18:9f:75:60	HCI_EVT	-95dBm	Random Device Address	Apple, Inc.		10054b1c…			Rcvd LE Meta (LE Extended Advertising Report)				
15:40:06,852892	55:3d:ee:1c:8d:bd	HCI_EVT	-90dBm	Random Device Address	Apple, Inc.		0719010f…			Rcvd LE Meta (LE Extended Advertising Report)				
15:40:11,801890	ee:24:b3:de:98:55	HCI_EVT	-89dBm	Random Device Address	Valve Corpora…	LHB-12EBA0…	00020201…			Rcvd LE Meta (LE Extended Advertising Report)				
15:40:12,832841	ee:24:b3:de:98:55	HCI_EVT	-88dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
15:40:14,458782	26:61:06:c9:1d:a8	HCI_EVT	-96dBm	Random Device Address	Apple, Inc.		09060305…			Rcvd LE Meta (LE Extended Advertising Report)				
15:40:18,254659	7c:25:36:42:c9:d4	HCI_EVT	-99dBm	Random Device Address	Samsung Elect…		01000200…			Rcvd LE Meta (LE Extended Advertising Report)				
15:40:29,198325	ee:24:b3:de:98:55	HCI_EVT	-85dBm	Random Device Address	Valve Corpora…	LHB-12EBA0…	00020201…			Rcvd LE Meta (LE Extended Advertising Report)				
15:40:29,199308	ee:24:b3:de:98:55	HCI_EVT	-85dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
15:40:33,766184	71:aa:29:e6:91:93	HCI_EVT	-97dBm	Random Device Address	Apple, Inc.		10054a1c…			Rcvd LE Meta (LE Extended Advertising Report)				
15:40:33,767171	71:aa:29:e6:91:93	HCI_EVT	-97dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
15:40:41,647980	ee:24:b3:de:98:55	HCI_EVT	-86dBm	Random Device Address	Valve Corpora…	LHB-12EBA0…	00020201…			Rcvd LE Meta (LE Extended Advertising Report)				
15:40:41,648959	ee:24:b3:de:98:55	HCI_EVT	-85dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
15:40:42,582950	56:4a:e3:08:b4:80	HCI_EVT	-92dBm	Random Device Address	Apple, Inc.		10050a18…			Rcvd LE Meta (LE Extended Advertising Report)				
15:40:43,661928	64:5c:8d:c8:c6:ab	HCI_EVT	-98dBm	Random Device Address				0xfd64,0…	3edc1be05f2…	Rcvd LE Meta (LE Extended Advertising Report)				
15:40:45,572875	26:61:06:c9:1d:a8	HCI_EVT	-95dBm	Random Device Address	Apple, Inc.		09060305…			Rcvd LE Meta (LE Extended Advertising Report)				
15:40:46,597892	3d:13:dc:9f:c0:1b	HCI_EVT	-96dBm	Random Device Address	Microsoft		01092002…			Rcvd LE Meta (LE Extended Advertising Report)				
15:40:56,670616	ee:24:b3:de:98:55	HCI_EVT	-85dBm	Random Device Address	Valve Corpora…	LHB-12EBA0…	00020201…			Rcvd LE Meta (LE Extended Advertising Report)				
15:40:56,756604	ee:24:b3:de:98:55	HCI_EVT	-88dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
15:41:03,338452	26:61:06:c9:1d:a8	HCI_EVT	-97dBm	Random Device Address	Apple, Inc.		09060305…			Rcvd LE Meta (LE Extended Advertising Report)				
15:41:05,016432	44:41:f8:bd:d0:65	HCI_EVT	-95dBm	Random Device Address	Apple, Inc.		0215e2c5…			Rcvd LE Meta (LE Extended Advertising Report)				
15:41:12,033286	ee:24:b3:de:98:55	HCI_EVT	-88dBm	Random Device Address	Valve Corpora…	LHB-12EBA0…	00020201…			Rcvd LE Meta (LE Extended Advertising Report)				
15:41:13,057257	ee:24:b3:de:98:55	HCI_EVT	-85dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
15:41:19,930125	62:ee:c1:52:a2:39	HCI_EVT	-96dBm	Random Device Address	Apple, Inc.		10065c1e…			Rcvd LE Meta (LE Extended Advertising Report)				
15:41:20,991113	71:aa:29:e6:91:93	HCI_EVT	-96dBm	Random Device Address	Apple, Inc.		10054a1c…			Rcvd LE Meta (LE Extended Advertising Report)				
15:41:20,992099	71:aa:29:e6:91:93	HCI_EVT	-96dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				

Chaque ligne correspond à un « paquet » de données. Des filtres de couleurs permettent de visualiser certaines configurations :

: *Company Id* = « Apple, Inc. » : (Adresse de type *Random)* & (aucune info d'identification) & (Puissance > - 90 dB)

Répartition des adresses collectées

Ensemble des sessions analyse Wireshark

	Total	Adresses « MAC » détectées									
		dont adresses « 4-7 »					Autres adresses				
		Total	dont Apple	dont TAC	Autres sources					Apple Inc	Autres
					ident'	non Identifiées	Apple	Autres	non Identifiées		
ENSEMBLE	1328	824	**680**	**30**	94	20	**264**	238	3	**944**	384
		62%				1,5%	20%	18%	0,2%	**71%**	
			83%	4%	11%	2,4%					
> 3 paquets	563	387	**54**	**15**	310	8	**144**	32	0	**198**	365
		69%				1,4%				**35%**	
			14%	4%	80%	2,1%					

Cas d’une adresse « mystérieuse », c’est-à-dire dont la source n’est pas identifiable :

Time	BD_ADDR	Protocol	RSSI	Peer Address Type	Company ID	Device Name	Data	UUID 16	Service Data	Info	UUID 32	UUID 128	Custom UUID 32	Custom UUID 128
16:23:07,462002	4a:25:d5:70:71:8b	HCI_EVT	-96dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
16:23:17,526943	4a:25:d5:70:71:8b	HCI_EVT	-94dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
16:23:17,527934	4a:25:d5:70:71:8b	HCI_EVT	-94dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
16:23:35,146811	4a:25:d5:70:71:8b	HCI_EVT	-89dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
16:23:35,147806	4a:25:d5:70:71:8b	HCI_EVT	-89dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
16:23:44,350763	4a:25:d5:70:71:8b	HCI_EVT	-85dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
16:23:44,351756	4a:25:d5:70:71:8b	HCI_EVT	-85dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
16:24:00,138691	4a:25:d5:70:71:8b	HCI_EVT	-88dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
16:24:00,139653	4a:25:d5:70:71:8b	HCI_EVT	-88dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
16:24:18,948531	4a:25:d5:70:71:8b	HCI_EVT	-97dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
16:24:18,949534	4a:25:d5:70:71:8b	HCI_EVT	-95dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
16:24:51,452326	4a:25:d5:70:71:8b	HCI_EVT	-97dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				

- 12 paquets
- durée totale : environ 1 minute 40"
- aucune info permettant d’identifier la source du signal :
  - pas de valeur pour les champs *Company ID*, *Device Name*, *UUID 16*, *Service Data*, *UUID 32*, *UUID 128*, *Custom UUID 32*, *Custom UUID 128*.
  - l’adresse est de type *Random* (cf. champ *Peer Address Type*) : cela signifie qu’on ne peut pas déceler le fabriquant à l’aide de cette adresse (contrairement à une adresse de type *Public*).

1328 adresses différentes ont été détectées au fil des divers sessions. **Pour 563 d'entre elles, plus de 3 paquets ont été reçus. Dans ce lot, 8 adresses sont restées non identifiables (soit 1,4%).**

Ces adresses mystérieuses sont **toujours du type *random recognizable*** (*random* et 1er chiffre entre 4 et 7).

Lorsqu’une adresse d’un autre type *semble* mystérieuse, c’est en fait que l’on n’a reçu qu’un ou deux paquets, lesquels ne contiennent pas toujours d’information caractéristique. Voir le cas suivant.

POUR UNE TELLE SITUATION, PROCHAINE ÉTAPE : discuter avec la personne.

1. est-ce que l’adresse reste non identifiée au fil du temps ?
2. Est-ce que la personne transporte des appareils susceptibles d’être source ? (par exemple un appareil médical de type pompe à insuline, dispositif cardio...)

Cas de l’étiquette d’un smartphone

On désigne par « étiquette » le nom diffusé par un smartphone lorsque le BT est activé pour l’appairage avec d’autres appareils (échange de fichiers, audio…).

Dans ce cas :

- la technologie en œuvre est le BT Classic (*BR/EDR – Basic Rate / Enhance Data Rate)*
- l’adresse est de type *Public* : les 6 premiers chiffres hexadécimaux de l’adresse correspondent au code OUI du fabricant (OUI : *Organizationally Unique Identifier* - https://standards-oui.ieee.org/)

La capture ci-après affiche les paquets d’une adresse qui correspond à l’étiquette du smartphone « P30 lite Michèle ».
Dans ce cas, les 6 premiers chiffres de l’adresse sont « *8c:5a:c1* ». D’après le registre OUI, le fabricant est *Huawei*.

On voit sur cet exemple que le tout premier paquet ne comporte aucune info, ce qui pourrait donner l’impression que la source est mystérieuse mais il suffit qu’il y ait suffisamment de temps pour recevoir un second paquet et que la source soit identifiée.

Time	BD_ADDR	Protocol	RSSI	Peer Address Type	Company ID	Device Name	Data	UUID 16	Service Data	Info
16:15:04,984219	8c:5a:c1:5c:dd:f3	HCI_EVT	-93dBm							Rcvd Extended Inquiry Result
16:15:05,037249	8c:5a:c1:5c:dd:f3	HCI_EVT	-92dBm			P30 lite Michèle		OBEX Object Push,Audio Source,A/V Remote Control…		Rcvd Extended Inquiry Result
16:15:17,769131	8c:5a:c1:5c:dd:f3	HCI_EVT	-92dBm							Rcvd Extended Inquiry Result
16:15:30,556071	8c:5a:c1:5c:dd:f3	HCI_EVT	-92dBm							Rcvd Extended Inquiry Result
16:16:07,774822	8c:5a:c1:5c:dd:f3	HCI_EVT	-90dBm			P30 lite Michèle		OBEX Object Push,Audio Source,A/V Remote Control…		Rcvd Extended Inquiry Result
16:16:58,847474	8c:5a:c1:5c:dd:f3	HCI_EVT	-87dBm			P30 lite Michèle		OBEX Object Push,Audio Source,A/V Remote Control…		Rcvd Extended Inquiry Result
16:17:46,200241	8c:5a:c1:5c:dd:f3	HCI_EVT	-89dBm			P30 lite Michèle		OBEX Object Push,Audio Source,A/V Remote Control…		Rcvd Extended Inquiry Result
16:18:14,352965	8c:5a:c1:5c:dd:f3	HCI_EVT	-89dBm							Rcvd Extended Inquiry Result
16:18:20,829892	8c:5a:c1:5c:dd:f3	HCI_EVT	-91dBm			P30 lite Michèle		OBEX Object Push,Audio Source,A/V Remote Control…		Rcvd Extended Inquiry Result
16:18:32,282814	8c:5a:c1:5c:dd:f3	HCI_EVT	-90dBm			P30 lite Michèle		OBEX Object Push,Audio Source,A/V Remote Control…		Rcvd Extended Inquiry Result
16:18:49,054732	8c:5a:c1:5c:dd:f3	HCI_EVT	-91dBm							Rcvd Extended Inquiry Result
16:19:04,277636	8c:5a:c1:5c:dd:f3	HCI_EVT	-91dBm							Rcvd Extended Inquiry Result
16:20:04,498198	8c:5a:c1:5c:dd:f3	HCI_EVT	-89dBm							Rcvd Extended Inquiry Result

Cas d’une balise émise par un iPhone

Outre l’adresse BT de communication BR/EDR, les iPhone sont susceptibles d’émettre une adresse en BT LE appelée « balise ». Cette source est caractérisée par :

- une adresse de type *random recognizable* (« 4-7 »)
- l’info « Apple, Inc. » dans le champs *Company ID*.

Exemple :

Time	BD_ADDR	Protocol	RSSI	Peer Address Type	Company ID	Device Name	Data	UUID 16	Service Data	Info	UUID 32	UUID 128	Custom UUID 32	Custom UUID 128
16:48:50,005724	50:1d:c3:d8:5b:f0	HCI_EVT	-93dBm	Random Device Address	Apple, Inc.		1006211a…			Rcvd LE Meta (LE Extended Advertising Report)				
16:48:50,006737	50:1d:c3:d8:5b:f0	HCI_EVT	-93dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
16:49:07,950602	50:1d:c3:d8:5b:f0	HCI_EVT	-89dBm	Random Device Address	Apple, Inc.		1006211a…			Rcvd LE Meta (LE Extended Advertising Report)				
16:49:07,951603	50:1d:c3:d8:5b:f0	HCI_EVT	-89dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
16:49:17,215058	50:1d:c3:d8:5b:f0	HCI_EVT	-77dBm	Random Device Address	Apple, Inc.		1006211a…			Rcvd LE Meta (LE Extended Advertising Report)				
16:49:17,216038	50:1d:c3:d8:5b:f0	HCI_EVT	-77dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
16:49:36,502969	50:1d:c3:d8:5b:f0	HCI_EVT	-78dBm	Random Device Address	Apple, Inc.		1006211a…			Rcvd LE Meta (LE Extended Advertising Report)				
16:49:36,503951	50:1d:c3:d8:5b:f0	HCI_EVT	-79dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				
16:49:48,035504	50:1d:c3:d8:5b:f0	HCI_EVT	-94dBm	Random Device Address	Apple, Inc.		1006211a…			Rcvd LE Meta (LE Extended Advertising Report)				
16:49:48,036488	50:1d:c3:d8:5b:f0	HCI_EVT	-95dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)				

- 10 paquets
- durée totale : 1 minute
- un paquet sur deux contient l’indication « Apple, Inc. » et une indication de data.

Dans une telle situation, le fait que le signal soit émis par un iPhone a été constaté plus d’une dizaine de fois avec des utilisateurs différents. Lorsque le mode *Avion* est activé, le signal disparaît. Une autre adresse apparaît dès que le mode *Avion* est désactivé.
(cf. vidéo de 10’ ici : https://video.liberta.vip/w/cefo1RdeBLaYn6W4eFaxPB)

À partir de la version 7 de l’iOS, **une balise peut être émise alors que la fonction BT *semble* éteint**e. En fait, sur ces appareils il y a 2 niveaux d'activation du BT :

1. Un “gros” bouton qui rend le smartphone visible (avec son étiquette) et l'échange de fichiers possible ;
2. Si ce 1er bouton est “off”, cela coupe la visibilité nominative mais des émissions BT LE sont toujours possibles en tache de fond. Il faut se rendre dans les paramètres pour sélectionner les émissions autorisées.

Cas d’un signal émis par l’application TAC

Time	BD_ADDR	Protocol	RSSI	Peer Address Type	Company ID	Device Name	Data	UUID 16	Service Data	Info
15:38:36,899580	64:5c:8d:c8:c6:ab	HCI_EVT	-101d…	Random Device Address				0xfd64,0xfd64	3edc1be05f27b8280838387cfe…	Rcvd LE Meta (LE Extended Advertising Report)
15:38:45,271728	64:5c:8d:c8:c6:ab	HCI_EVT	-92dBm	Random Device Address				0xfd64,0xfd64	3edc1be05f27b8280838387cfe…	Rcvd LE Meta (LE Extended Advertising Report)
15:38:45,272709	64:5c:8d:c8:c6:ab	HCI_EVT	-91dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)
15:38:57,424932	64:5c:8d:c8:c6:ab	HCI_EVT	-95dBm	Random Device Address				0xfd64,0xfd64	3edc1be05f27b8280838387cfe…	Rcvd LE Meta (LE Extended Advertising Report)
15:38:57,425910	64:5c:8d:c8:c6:ab	HCI_EVT	-94dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)
15:39:11,976156	64:5c:8d:c8:c6:ab	HCI_EVT	-84dBm	Random Device Address				0xfd64,0xfd64	3edc1be05f27b8280838387cfe…	Rcvd LE Meta (LE Extended Advertising Report)
15:39:11,977135	64:5c:8d:c8:c6:ab	HCI_EVT	-84dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)
15:39:26,587357	64:5c:8d:c8:c6:ab	HCI_EVT	-85dBm	Random Device Address				0xfd64,0xfd64	3edc1be05f27b8280838387cfe…	Rcvd LE Meta (LE Extended Advertising Report)
15:39:26,588350	64:5c:8d:c8:c6:ab	HCI_EVT	-85dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)
15:39:42,521571	64:5c:8d:c8:c6:ab	HCI_EVT	-90dBm	Random Device Address				0xfd64,0xfd64	3edc1be05f27b8280838387cfe…	Rcvd LE Meta (LE Extended Advertising Report)
15:39:42,522555	64:5c:8d:c8:c6:ab	HCI_EVT	-90dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)
15:39:58,233765	64:5c:8d:c8:c6:ab	HCI_EVT	-92dBm	Random Device Address				0xfd64,0xfd64	3edc1be05f27b8280838387cfe…	Rcvd LE Meta (LE Extended Advertising Report)
15:39:58,234749	64:5c:8d:c8:c6:ab	HCI_EVT	-91dBm	Random Device Address						Rcvd LE Meta (LE Extended Advertising Report)
15:40:43,661928	64:5c:8d:c8:c6:ab	HCI_EVT	-98dBm	Random Device Address				0xfd64,0xfd64	3edc1be05f27b8280838387cfe…	Rcvd LE Meta (LE Extended Advertising Report)

- 14 paquets
- durée totale : 2 minutes 7"
- pour un paquet sur deux :
  - *UUID 16* : 0xFD64 est la valeur réservée à l’application TAC.
  - *Service Data* : chaîne de 36 caractères qui caractérise l’émetteur.