Collecte des données des signaux BT avec PC en Linux
Jérôme R. – 22/11/2021

Btscan-shell	**Btmon**	**Info des répertoires officiels *Company id* (1) et *OUI* (2)**
Mon Nov 22 10:00:11 2021 4A:9E:BD:B5:74:31 UUIDs: 0000fe78-0000-1000-8000-00805f9b34fb Mon Nov 22 10:00:11 2021 4A:9E:BD:B5:74:31 ManufacturerData Key: 0x0065 Mon Nov 22 10:00:11 2021 4A:9E:BD:B5:74:31 ManufacturerData Value:	LE Address: 4A:9E:BD:B5:74:31 (OUI 4A-9E-BD) RSSI: -92 dBm (0xa4) Flags: 0x00000004 Not Connectable Data length: 11 16-bit Service UUIDs (complete): 1 entry Hewlett-Packard Company (0xfe78) Company: Hewlett-Packard Company (101) Data: 01c901	0x0065 : HP, Inc. Remarque : Btmon indique que l'adresse est publique (avec OUI 4A-9E-BD) or cet OUI n'est pas référencé dans le répertoire des OUI.
Mon Nov 22 10:00:11 2021 40:D7:74:20:8C:32 ManufacturerData Key: 0x004c Mon Nov 22 10:00:11 2021 40:D7:74:20:8C:32 ManufacturerData Value:	LE Address: 40:D7:74:20:8C:32 (Resolvable) RSSI: -79 dBm (0xb1) Flags: 0x00000000 Data length: 17 Flags: 0x1a LE General Discoverable Mode Simultaneous LE and BR/EDR (Controller) Simultaneous LE and BR/EDR (Host) TX power: 12 dBm Company: Apple, Inc. (76) Type: Unknown (16) Data: 471c39fe70	0x004c : Apple, Inc.

(1) https://www.bluetooth.com/specifications/assigned-numbers/company-identifiers/

(2) http://standards-oui.ieee.org/oui/oui.txt

Btscan-shell : petit programme maison qui utilise bluetoothctl . Détecte et affiche signaux BT (classique ou LE).
Scan BT pendant 10s puis pause 5s et réinitialisation

Exemple de sortie :

```
********  lun. 22 nov. 2021 10:00:06 CET
Mon Nov 22 10:00:08 2021 4A:5B:E7:D1:90:F4 4A-5B-E7-D1-90-F4
Mon Nov 22 10:00:08 2021 4B:E2:A7:C6:11:0F 4B-E2-A7-C6-11-0F
Mon Nov 22 10:00:08 2021 E4:9E:12:2D:0E:D0 RSSI: -81
Mon Nov 22 10:00:09 2021 4A:9E:BD:B5:74:31 4A-9E-BD-B5-74-31
Mon Nov 22 10:00:09 2021 72:24:A2:35:7A:C2 ManufacturerData Key: 0x004c
Mon Nov 22 10:00:09 2021 72:24:A2:35:7A:C2 ManufacturerData Value:
Mon Nov 22 10:00:10 2021 6E:21:12:F7:D3:36 6E-21-12-F7-D3-36
Mon Nov 22 10:00:11 2021 00:0A:9B:77:6E:61 RSSI: -84
Mon Nov 22 10:00:11 2021 4A:9E:BD:B5:74:31 UUIDs: 0000fe78-0000-1000-8000-00805f9b34fb
Mon Nov 22 10:00:11 2021 4A:9E:BD:B5:74:31 ManufacturerData Key: 0x0065
Mon Nov 22 10:00:11 2021 4A:9E:BD:B5:74:31 ManufacturerData Value:
Mon Nov 22 10:00:11 2021 40:D7:74:20:8C:32 ManufacturerData Key: 0x004c
Mon Nov 22 10:00:11 2021 40:D7:74:20:8C:32 ManufacturerData Value:
Mon Nov 22 10:00:11 2021 12:22:BC:5D:81:7B 12-22-BC-5D-81-7B
Mon Nov 22 10:00:11 2021 EC:6C:9A:D0:2F:6E Bouygtel4K 1596
Mon Nov 22 10:00:12 2021 7F:E9:B0:43:B6:51 7F-E9-B0-43-B6-51
Mon Nov 22 10:00:15 2021 54:85:62:9C:7C:1D 54-85-62-9C-7C-1D

********  lun. 22 nov. 2021 10:00:21 CET
Mon Nov 22 10:00:23 2021 40:D7:74:20:8C:32 ManufacturerData Key: 0x004c
Mon Nov 22 10:00:23 2021 40:D7:74:20:8C:32 ManufacturerData Value:
Mon Nov 22 10:00:23 2021 D3:81:93:95:BB:D4 D3-81-93-95-BB-D4
Mon Nov 22 10:00:24 2021 E4:9E:12:2E:F2:F2 Freebox Player Mini v2
Mon Nov 22 10:00:28 2021 72:EF:46:E4:FD:4C 72-EF-46-E4-FD-4C
Mon Nov 22 10:00:29 2021 54:85:62:9C:7C:1D ManufacturerData Key: 0x004c
Mon Nov 22 10:00:29 2021 54:85:62:9C:7C:1D ManufacturerData Value:
Mon Nov 22 10:00:29 2021 E4:9E:12:2D:0E:D0 RSSI: -92

********  lun. 22 nov. 2021 10:00:36 CET
Mon Nov 22 10:00:40 2021 D3:D1:94:0D:43:46 TT214H BlueFrog
Mon Nov 22 10:00:40 2021 40:D7:74:20:8C:32 RSSI: -82
Mon Nov 22 10:00:42 2021 75:C0:F3:E3:86:E8 75-C0-F3-E3-86-E8
Mon Nov 22 10:00:42 2021 E4:9E:12:2D:0E:D0 RSSI: -84
Mon Nov 22 10:00:43 2021 D3:D1:94:0D:43:46 ManufacturerData Key: 0x00ab
Mon Nov 22 10:00:43 2021 D3:D1:94:0D:43:46 ManufacturerData Value:
```

Btmon : outil intégré dans BlueZ (le gestionnaire BT de base des distro Linux) qui fournit toutes les infos liées à un signal BT (classique ou LE).

Exemple de sortie :

```
@ MGMT Event: Device Found (0x0012) plen 25          {0x0002} [hci0] 88.120790
      LE Address: 4A:9E:BD:B5:74:31 (OUI 4A-9E-BD)
      RSSI: -92 dBm (0xa4)
      Flags: 0x00000004
        Not Connectable
      Data length: 11
      16-bit Service UUIDs (complete): 1 entry
        Hewlett-Packard Company (0xfe78)
      Company: Hewlett-Packard Company (101)
        Data: 01c901> HCI Event: LE Meta Event (0x3e) plen 43              #113 [hci0] 88.387775
    LE Extended Advertising Report (0x0d)
      Num reports: 1
      Entry 0
        Event type: 0x0013
          Props: 0x0013
            Connectable
            Scannable
            Use legacy advertising PDUs
          Data status: Complete
        Legacy PDU Type: ADV_IND (0x0013)
        Address type: Random (0x01)
        Address: 40:D7:74:20:8C:32 (Resolvable)
        Primary PHY: LE 1M
        Secondary PHY: No packets
        SID: no ADI field (0xff)
        TX power: 127 dBm
        RSSI: -79 dBm (0xb1)
        Periodic advertising invteral: 0.00 msec (0x0000)
        Direct address type: Public (0x00)
        Direct address: 00:00:00:00:00:00 (OUI 00-00-00)
        Data length: 0x11
      02 01 1a 02 0a 0c 0a ff 4c 00 10 05 47 1c 39 fe  ........L...G.9.
      70                                               p
> HCI Event: LE Meta Event (0x3e) plen 26              #114 [hci0] 88.388750
    LE Extended Advertising Report (0x0d)
      Num reports: 1
      Entry 0
```

```
        Event type: 0x001b
          Props: 0x001b
            Connectable
            Scannable
            Scan response
            Use legacy advertising PDUs
          Data status: Complete
        Legacy PDU Type: SCAN_RSP to an ADV_SCAN_IND (0x001b)
        Address type: Random (0x01)
        Address: 40:D7:74:20:8C:32 (Resolvable)
        Primary PHY: LE 1M
        Secondary PHY: No packets
        SID: no ADI field (0xff)
        TX power: 127 dBm
        RSSI: -79 dBm (0xb1)
        Periodic advertising invteral: 0.00 msec (0x0000)
        Direct address type: Public (0x00)
        Direct address: 00:00:00:00:00:00 (OUI 00-00-00)
        Data length: 0x00
@ MGMT Event: Device Found (0x0012) plen 31          {0x0004} [hci0] 88.388786
      LE Address: 40:D7:74:20:8C:32 (Resolvable)
      RSSI: -79 dBm (0xb1)
      Flags: 0x00000000
      Data length: 17
      Flags: 0x1a
        LE General Discoverable Mode
        Simultaneous LE and BR/EDR (Controller)
        Simultaneous LE and BR/EDR (Host)
      TX power: 12 dBm
      Company: Apple, Inc. (76)
        Type: Unknown (16)
        Data: 471c39fe70
@ MGMT Event: Device Found (0x0012) plen 31          {0x0001} [hci0] 88.388786
      LE Address: 40:D7:74:20:8C:32 (Resolvable)
      RSSI: -79 dBm (0xb1)
      Flags: 0x00000000
      Data length: 17
      Flags: 0x1a
        LE General Discoverable Mode
        Simultaneous LE and BR/EDR (Controller)
        Simultaneous LE and BR/EDR (Host)
      TX power: 12 dBm
```

```
      Company: Apple, Inc. (76)
        Type: Unknown (16)
        Data: 471c39fe70
@ MGMT Event: Device Found (0x0012) plen 31          {0x0003} [hci0] 88.388786
      LE Address: 40:D7:74:20:8C:32 (Resolvable)
      RSSI: -79 dBm (0xb1)
      Flags: 0x00000000
      Data length: 17
      Flags: 0x1a
        LE General Discoverable Mode
        Simultaneous LE and BR/EDR (Controller)
        Simultaneous LE and BR/EDR (Host)
      TX power: 12 dBm
      Company: Apple, Inc. (76)
        Type: Unknown (16)
        Data: 471c39fe70
```