

Projet Bluetooth Expérience X



[Source : gloria.tv]

Par Germán Sarlangue

Blog – <https://gloria.tv/user/VPgx11CTuCb3pv1bbjveivjz>

Projet Bluetooth expérience X Version 1 – Révision 2

Étude rendue possible grâce au soutien financier de la LNPLV (infovaccin.fr), de EFVV (efvv.eu) et de nombreux donateurs anonymes. 30/11/2021

Résumé :

Objectivation de l'existence d'adresse MAC détectables sur la plage de fréquence Bluetooth suite à une inoculation de thérapie antigénique COVID et de test PCR de détection COVID.

Équipe :

- Germán Sarlangue
- Julien Devilleger
- Philippe Trillaud
- Steve Fouchet
- Lidwine Taillason
- Grégory Catteau

Lien source :

<https://ln5.sync.com/dl/195df4a10/5ab9apq6-q5vgawam-vgr3ktt9-7zr985rh>

1/ Avant propos

Depuis avril 2021 des rumeurs se sont propagées sur les réseaux sociaux concernant l'apparition de signaux de type bluetooth à la suite d'une ou plusieurs injections anti-covid proposées par les compagnies pharmaceutiques :

- Astra Zeneca
- Pfizer
- Johnson et Johnson
- Moderna

De nombreuses vidéos ont circulé qui semblent mettre en évidence l'apparition de phénomènes troublants, à savoir :

- Des phénomènes d'aimantation inexpliqués sur différents sites du corps de personnes injectées (qui ont donné lieu à une explosion des publications sur TikTok regroupées autour d'un mouvement communautaire, Le Magnet Challenge).

<https://www.youtube.com/watch?v=lYi3sjRZviA>

- L'apparition d'adresses MAC Bluetooth en présence de personnes injectées et en l'absence de tout dispositif technologique susceptible d'expliquer ces apparitions.
- L'apparition de signaux lors d'un scan effectué sur le corps d'une personne injectée par l'intermédiaire d'appareillage de détection de puce électronique animale utilisées couramment chez les vétérinaires.

@jasmine_0708

umm what ☐☐ #vaccine #vaccinesideeffect #chipped #chipfinder

#covidvaccine #covidvaccinesideeffects

♫ original sound – jasmine

Toutes ces rumeurs ont été démenties par les principaux médias et les agences de presse traditionnelles alors même que dans les réseaux alternatifs de nombreuses expérimentations empiriques effectuées par des citoyens ordinaires semblaient démontrer le contraire.

<https://www.reuters.com/article/factcheck-astrazeneca-bluetooth-idUSL2N2NC2G9>

<https://www.20minutes.fr/sante/3067959-20210623-coronavirus-non-vaccins-permettent-etre-detecte-bluetooth-gare-videos-trompeuses>

Pour autant les expériences citoyennes empiriques se multiplient :

<https://henrymakow.wordpress.com/2021/09/17/le-vaccin-contient-votre-code-barres/>

<https://echelledejacob.blogspot.com/2021/11/vaccines-et-puce-bluetooth-mise-ajour.html> <https://www.youtube.com/watch?v=q1VCRZNaHLE>

<https://odysee.com/@Hemeroteca:f/DrDeBenito-mac-address-:7>

https://odysee.com/@Pigeon_Pige-TouT_Traduction:6/bluetooth-2:e

En France la première expérimentation documentée sur le sujet a fait l'objet d'un article publié dans Agoravox

(<https://www.agoravox.fr/tribune-libre/article/operation-dent-bleue-235064>)

Cependant, comme le souligne Jérôme R. responsable de la publication de l'article, même si les résultats obtenus interpellent (De nombreuses adresses MAC non identifiées apparaissent), il ne pourrait s'agir d'en tirer une conclusion hâtive.

En effet, le terrain d'expérimentation était un jardin public d'où pouvaient partir de nombreux signaux légitimes émanant d'appareils non pris en compte et son matériel de détection (Un téléphone portable Archos tournant sous Android) pourrait également être l'objet de potentielles failles dans la détection

Bien évidemment ces expériences qui ne montrent qu'un résultat final, ne se sont inscrites dans aucun protocole assumé ne permettraient en aucun cas de démontrer la fiabilité des résultats.

En parallèle, de nombreuses études ont été effectuées pour objectiver la présence d'oxyde de graphène ou de l'un de ses dérivés dans la composition du vaccin.

Il est important de comprendre que l'oxyde de graphène a fait l'objet de pléthore d'études autour de ses propriétés physico-chimiques et électromagnétiques uniques.

Des applications commerciales sont d'ores et déjà disponibles :

Parallèlement à cela des dépôts officiels de brevets visant à l'élaboration de nanotechnologies implantées dans le corps humain, telles que des nanosenseurs, ou à des dispositifs variés utilisant les rayonnements électromagnétiques permettant toute sorte d'applicatifs potentiels existent.

- https://patents-google-com.translate.goog/patent/US4717343?_x_tr_sl=auto&_x_tr_tl=fr&_x_tr_hl=fr
- https://patents-google-com.translate.goog/patent/US3951134?_x_tr_sl=auto&_x_tr_tl=fr&_x_tr_hl=fr
- https://patents-google-com.translate.goog/patent/US5159703?_x_tr_sl=auto&_x_tr_tl=fr&_x_tr_hl=fr
- https://patents-google-com.translate.goog/patent/US5507291?_x_tr_sl=auto&_x_tr_tl=fr&_x_tr_hl=fr
- https://patents-google-com.translate.goog/patent/US6017302?_x_tr_sl=auto&_x_tr_tl=fr&_x_tr_hl=fr
- https://patents-google-com.translate.goog/patent/US6052336?_x_tr_sl=auto&_x_tr_tl=fr&_x_tr_hl=fr
- https://patents-google-com.translate.goog/patent/US6506148B2/en?_x_tr_sl=auto&_x_tr_tl=fr&_x_tr_hl=fr
- https://patents-google-com.translate.goog/patent/US10300240B2/en?_x_tr_sl=auto&_x_tr_tl=fr&_x_tr_hl=fr
- https://patents-google-com.translate.goog/patent/US5629678A/en?_x_tr_sl=auto&_x_tr_tl=fr&_x_tr_hl=fr

Enfin face au caractère secret de la composition des injections ainsi que l'impunité négociée des laboratoires pharmaceutiques quant aux éventuels effets indésirables liés aux injections, certaines études ont émergé mettant en évidence des éléments troublants :

- <https://corona2inspect.blogspot.com/2021/11/identificacion-patrones-vacunass-coronavirus-nanorouters.html>
- https://www.researchgate.net/publication/356507702_MICROSTRUCTURES_IN_COVID_VACCINES_inorganic_crystals_or_Wireless_Nanosensors_Network
- <https://corona2inspect.blogspot.com/2021/09/redes-nanocomunicacion-inalamb>

rica-nanotecnologia-cuerpo-humano.html

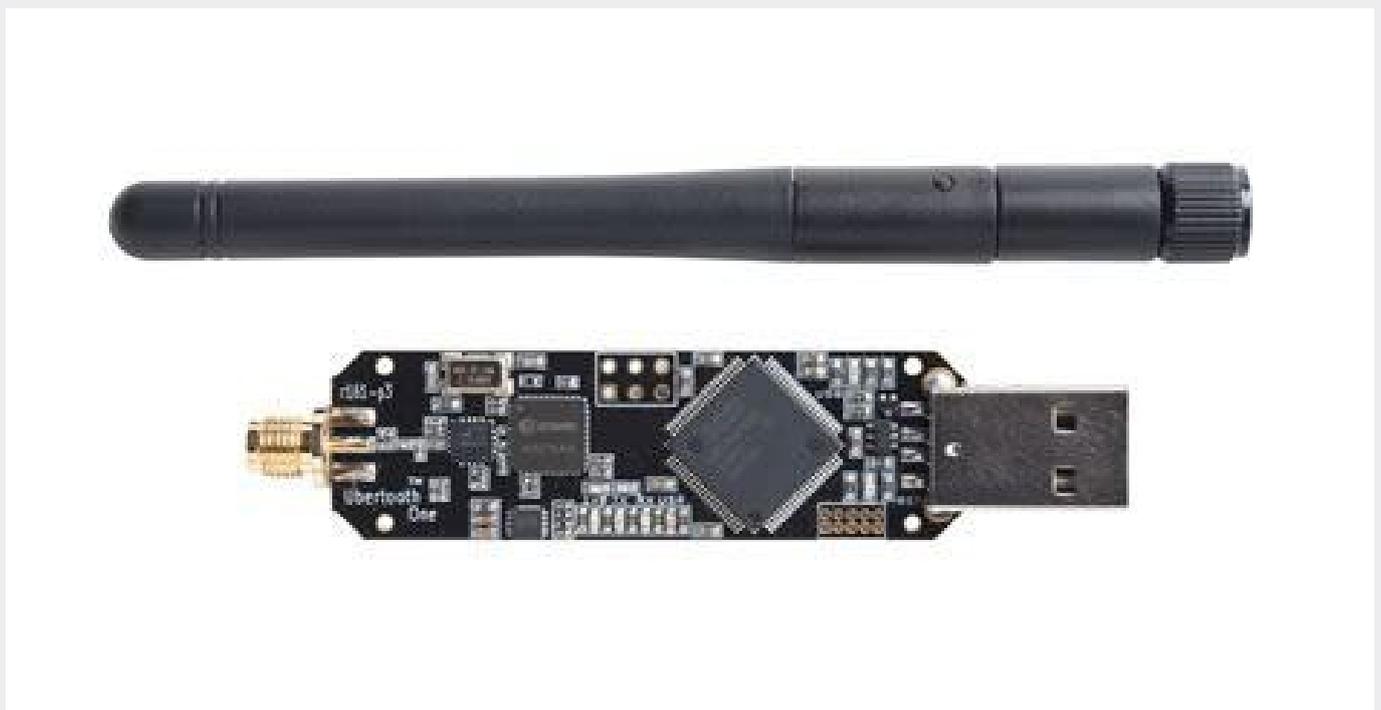
- https://drive.google.com/file/d/1M5T_pa4d87vznN0r0IUjrsb07sq09vh/view?usp=drivesdk

2/ Environnement matériel et configuration technique

Pour cette expérience il a été choisi de travailler avec une antenne Ubertooth one de Great Scott Gadgets dont voici les spécifications techniques :

- Connecteur RP-SMA (destiné à connecter l'antenne Bluetooth)
- Module de transmission sans fil CC2400 Full duplex 2.4 GHz
- Module RF front end CC 2591
- Microcontrôleur LPC175x ARM Cortex-M3
- Connection USB 2.0 Full-speed
- Support Bluetooth and Bluetooth Low Energy
- Ampérage approximatif de 220mA

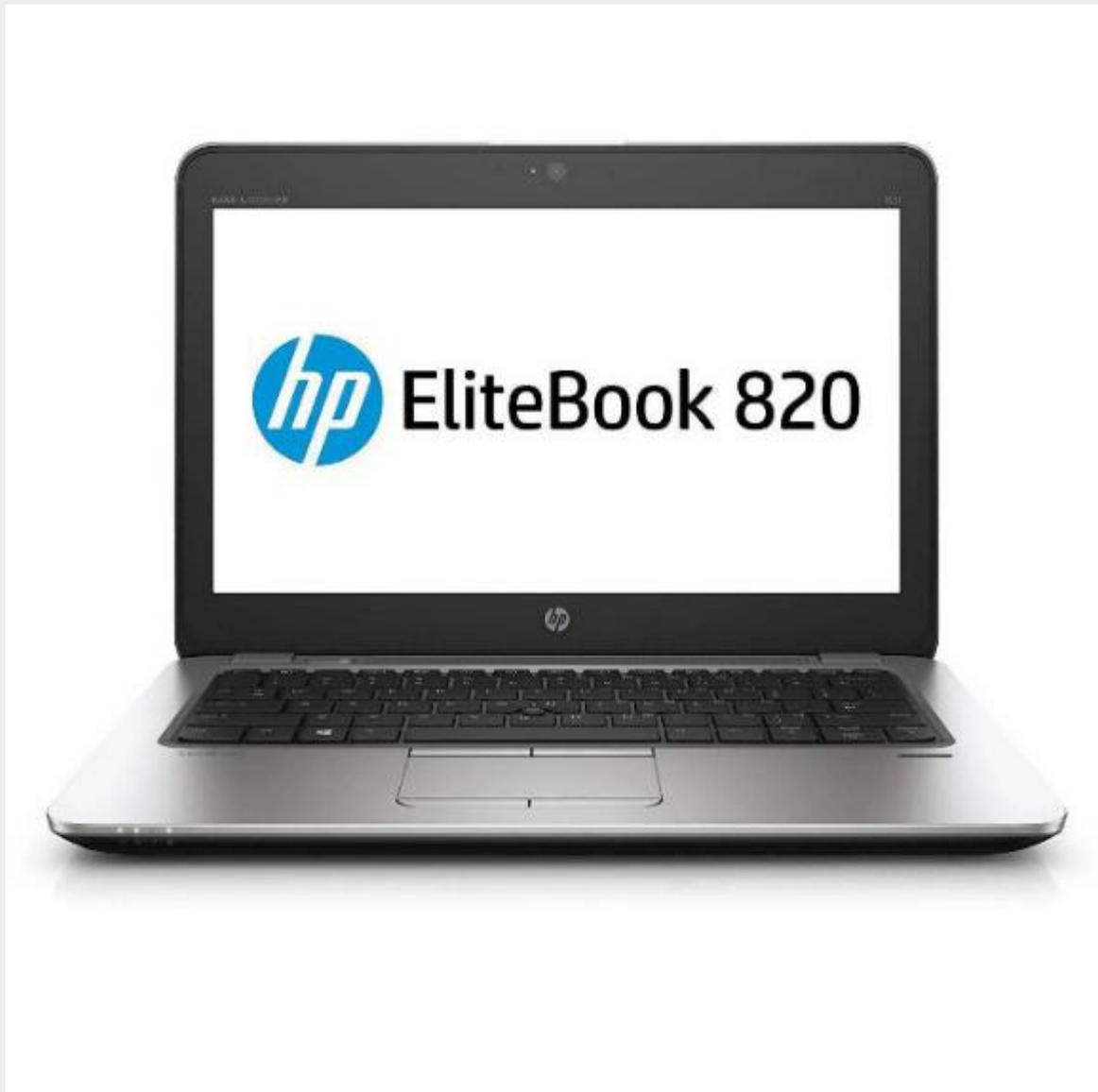
Il permet d'envoyer et de recevoir des paquets à 2,4 GHz, qui est la fréquence du Bluetooth, mais aussi de voir le trafic Bluetooth en temps réel en mode moniteur. L'appareil est comparable à un module Bluetooth de classe 1, c'est à dire qu'il a une puissance maximale de 100 mW (20 dBm) et une portée de 100 mètres sans obstacles.



Au niveau de l'ordinateur portable notre choix s'est porté sur une machine :

Hp EliteBook 820 G3 :

- Processeur Intel Core I7-6600U (2.6 Ghz)
- Mémoire RAM : 16 Go DDR3
- Carte graphique Intel HD Graphics 520
- Disque dur 240 Go SSD.



La version Bare metal installer 2021-3 de Kali linux a été téléchargée depuis :

<https://kali.download/base-images/kali-2021.3/kali-linux-2021.3-installer-amd64.iso.torrent>

En fichier ISO.

Elle a été montée sur une clé USB classique de 32 Go en image disque bootable

via l'application Rufus
(<https://rufus.ie/fr/>)

Une fois l'OS Kali linux installé sur la machine, une mise à niveau de ce dernier a été effectuée :

```
sudo apt-get update  
sudo apt-get upgrade.
```

Aucun conflit n'ayant été détecté, la machine a été redémarrée.

Le projet Ubertooth est un projet Open Source.

L'intégralité du code est disponible sur Git.

Nous avons donc commencé par installer les différents paquets nécessaires :

```
sudo apt-get install cmake libusb-1.0-0-dev make gcc g++ libbluetooth-dev \  
pkg-config libpcap-dev python-numpy python-pyside python-qt4
```

Suivi d'une mise à jour classique :

```
sudo apt-get update  
sudo apt-get upgrade
```

Nous avons ensuite procédé à l'installation de la dernière version de libbtbb.

```
sudo ldconfig  
wget https://github.com/greatscottgadgets/libbtbb/archive/2020-12-R1.tar.gz -  
O libbtbb-2020-12-R1.tar.gz  
tar xf libbtbb-2020-12-R1.tar.gz  
cd libbtbb-2020-12-R1  
mkdir build  
cd build  
cmake ..  
make  
sudo make install  
sudo apt-get update  
sudo apt-get upgrade
```

Puis nous avons installé les outils Ubertooth :

```
wget
https://github.com/greatscottgadgets/ubertooth/releases/download/2020-12-R1/ubertooth-2020-12-R1.tar.xz -O ubertooth-2020-12-R1.tar.xz
tar xf ubertooth-2020-12-R1.tar.xz
cd ubertooth-2020-12-R1/host
mkdir build
cd build
cmake ..
make
sudo make install
sudo apt-get update
sudo apt-get upgrade
```

Nous avons ensuite procédé à l'Update du firmware d'Ubertooth One :

```
cd ubertooth-2020-12-R1/ubertooth-one-firmware-bin
sudo ubertooth-dfu -d bluetooth_rxtx.dfu -r
cd ../../
sudo apt-get update
sudo apt-get upgrade
```

Nous avons effectué le contrôle grâce à la commande :

```
ubertooth-util -v
```

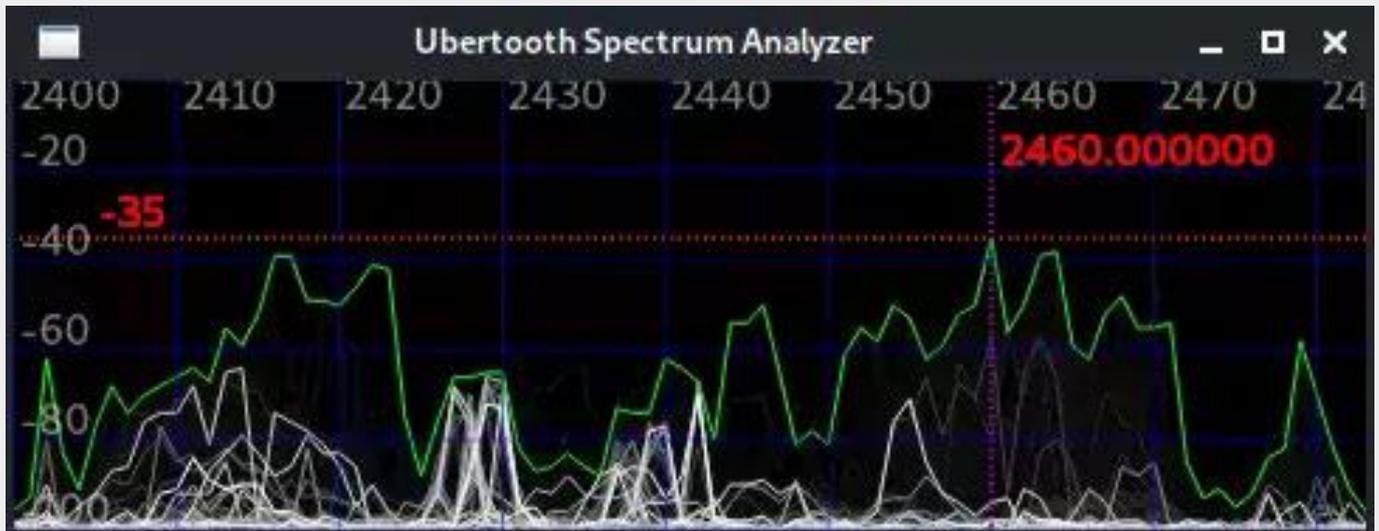
Qui nous a renvoyé :

```
Firmware version: 2020-12-R1 (API:1.07)
```

Nous avons donc connecté l'antenne Bluetooth à la carte mère de l'Ubertooth one et branché ce dernier sur un port USB de la machine et lancé la commande :

```
ubertooth-specan-ui
```

Qui nous a ouvert une fenêtre :



L'appareil étant configuré et fonctionnel nous avons refermé la fenêtre et procédé à l'installation des plugins.

Nous avons commencé par installer les plugins wireshark :

```
sudo apt-get install wireshark wireshark-dev libwireshark-dev cmake cd
libbtbb-2020-12-R1/wireshark/plugins/btbb mkdir build
cd build
cmake -DCMAKE_INSTALL_LIBDIR=/usr/lib/x86_64-linux-
gnu/wireshark/libwireshark3/plugins ..
make
sudo make install
cd libbtbb-2020-12-R1/wireshark/plugins/btbredr
mkdir build
cd build
cmake -DCMAKE_INSTALL_LIBDIR=/usr/lib/x86_64-linux-
gnu/wireshark/libwireshark3/plugins .. make
sudo make install
sudo apt-get update
sudo apt-get upgrade
```

Puis nous avons procédé à la configuration de Kismet.

Pour ce faire nous avons commencé par supprimer toutes les configurations pré existantes :

```
sudo rm -rfv /usr/local/bin/kismet* /usr/local/share/kismet*
/usr/local/etc/kismet*
```

Nous avons ensuite procédé à l'installation et à l'actualisation des paquets nécessaires :

```
python -m pip install --upgrade pip
pip install libpcap
sudo apt-get install libcap-dev pkg-config \ build-essential libnl-dev
libncurses-dev libpcrc3-dev \ libpcap-dev libcap-dev
```

Afin de pouvoir procéder à l'installation de la dernière version de kismet.
wget -O -

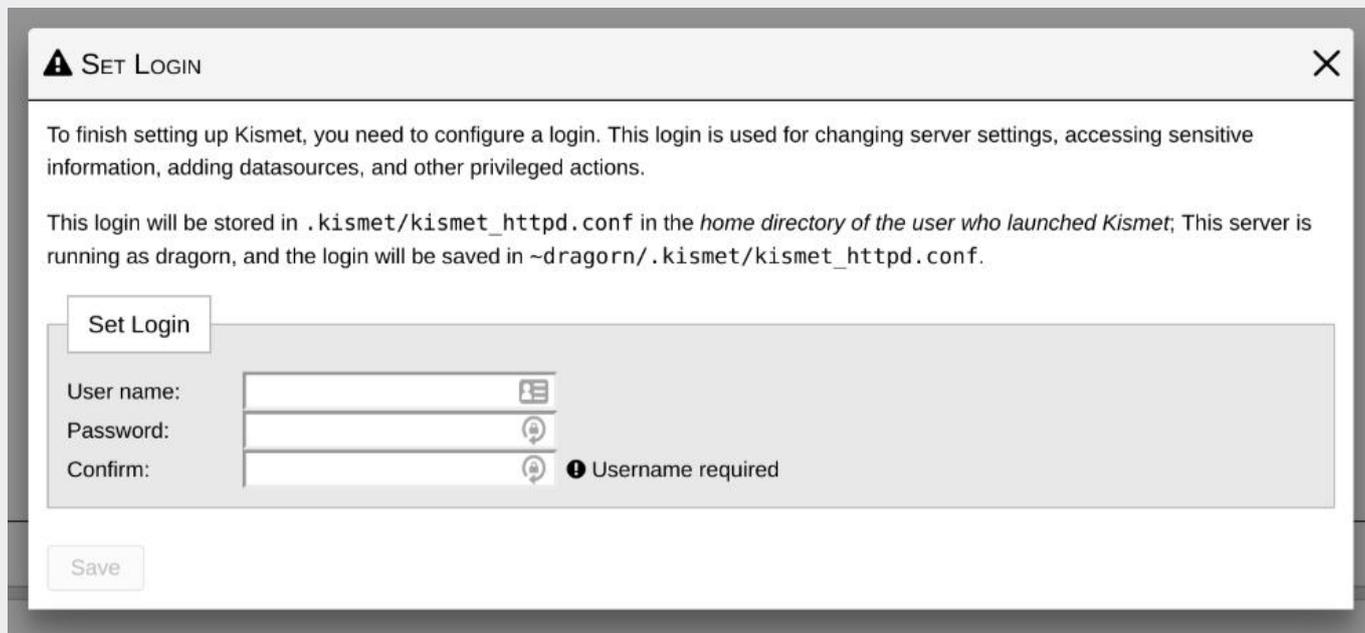
```
https://www.kismetwireless.net/repos/kismet-release.gpg.key | sudo apt-key
add -
$ echo 'deb https://www.kismetwireless.net/repos/apt/release/kali kali main'
| sudo tee /etc/apt/sources.list.d/kismet.list
wget http://www.kismetwireless.net/code/kismet-2021-08-R1.tar.gz tar xf
kismet-2021-08-R1.tar.gz
sudo mv kismet-2021-08-R1 /usr/src/kismet
ln -s ../ubertooth-2021-08-R1/host/kismet/plugin-ubertooth /usr/src/kismet
cd /usr/src/kismet
sudo ./configure
sudo make && sudo make plugins
sudo make suidinstall
sudo make plugins-install
cd ~
sudo apt-get update
sudo apt-get upgrade
sudo apt install kismet-core kismet-capture-linux-bluetooth kismet-capture-
linux-wifi kismet-capture-nrf-mousejack python-kismetcapturertl433 python-
kismetcapturertladsb python-kismetcapturertlamr python-
kismetcapturefreaklabszigbee kismet-logtools~
sudo apt-get update
sudo apt-get upgrade
sudo apt install kismet-capture-linux-bluetooth
```

Nous avons éteint et rallumé la machine puis procédé aux vérifications d'usage.

Lors du lancement de kismet via la commande

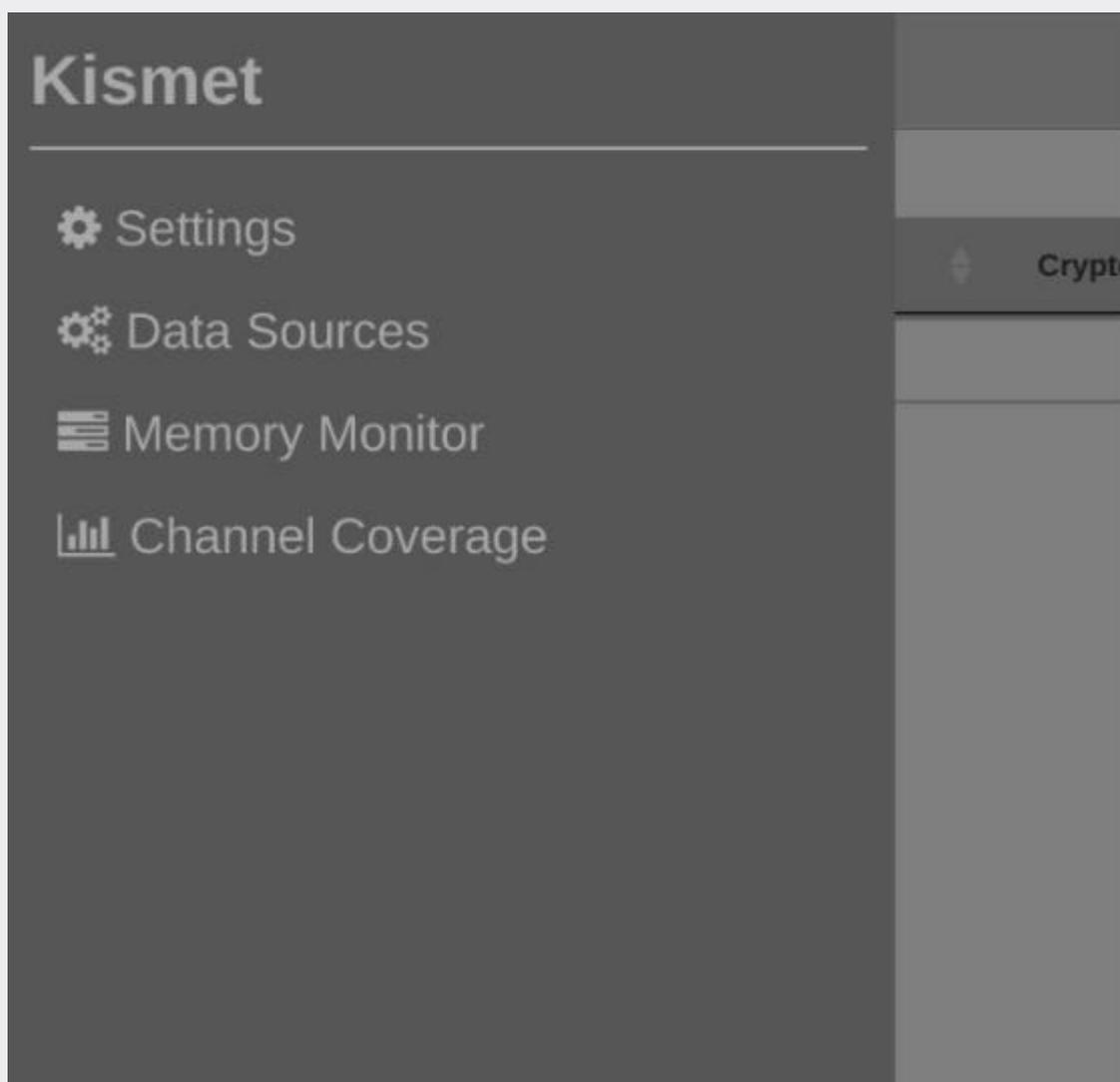
```
sudo kismet
```

Une fenêtre s'ouvre nous demandant de définir un login et un password.



Ce que nous avons fait.

Puis nous avons sélectionné ubertooth one dans la liste Data Sources :



Nous avons testé l'application : Cette dernière est parfaitement fonctionnelle.

Nous avons ensuite configuré Wireshark pour permettre la capture de paquets Bluetooth.

Pour ce faire nous avons configuré un pipe :

```
mkfifo /tmp/pipe
```

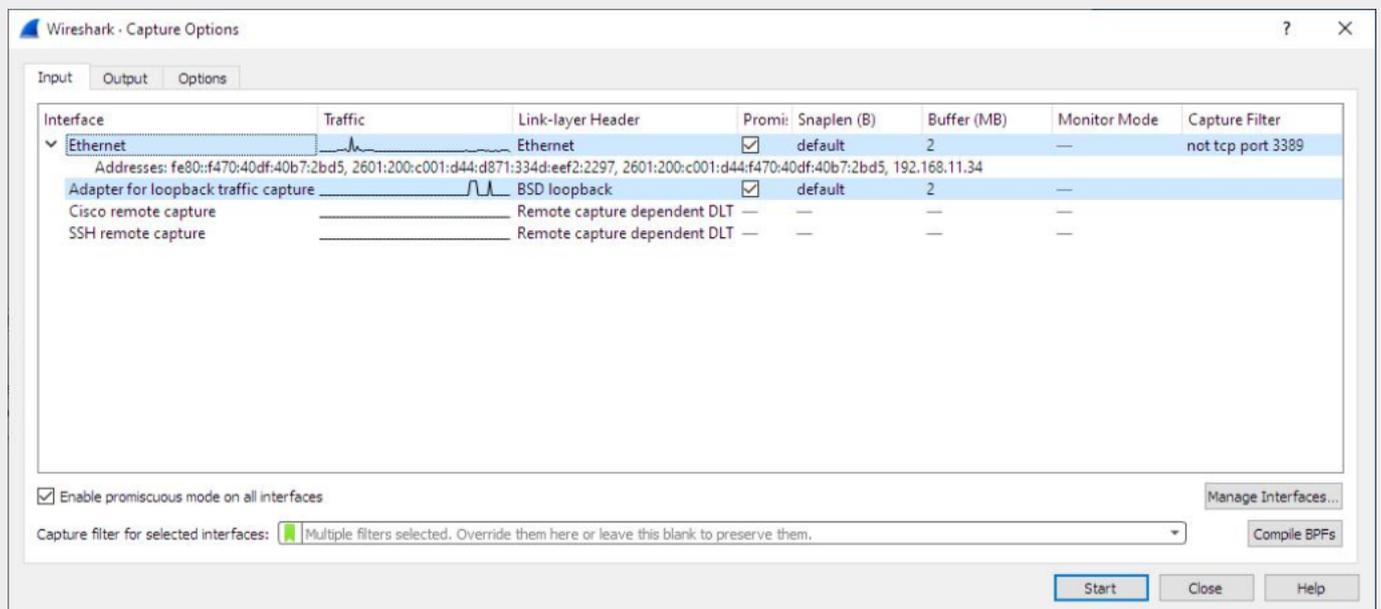
Puis nous avons ouvert wireshark depuis la commande :

```
sudo wireshark
```

Dans la fenêtre qui s'est ouverte nous avons cliqué sur capture -> Options-> Manage interfaces ->

Pipe -> New ou nous avons entré dans le champ « pipe » :

```
/tmp/pipe
```



Enfin sur le terminal nous avons entré la commande :

```
ubertooth-btle -f -c /tmp/pipe
```

Dans les sources nous avons choisi bluetooth et lancé la capture : parfaitement fonctionnel.

3/ Tests préliminaires

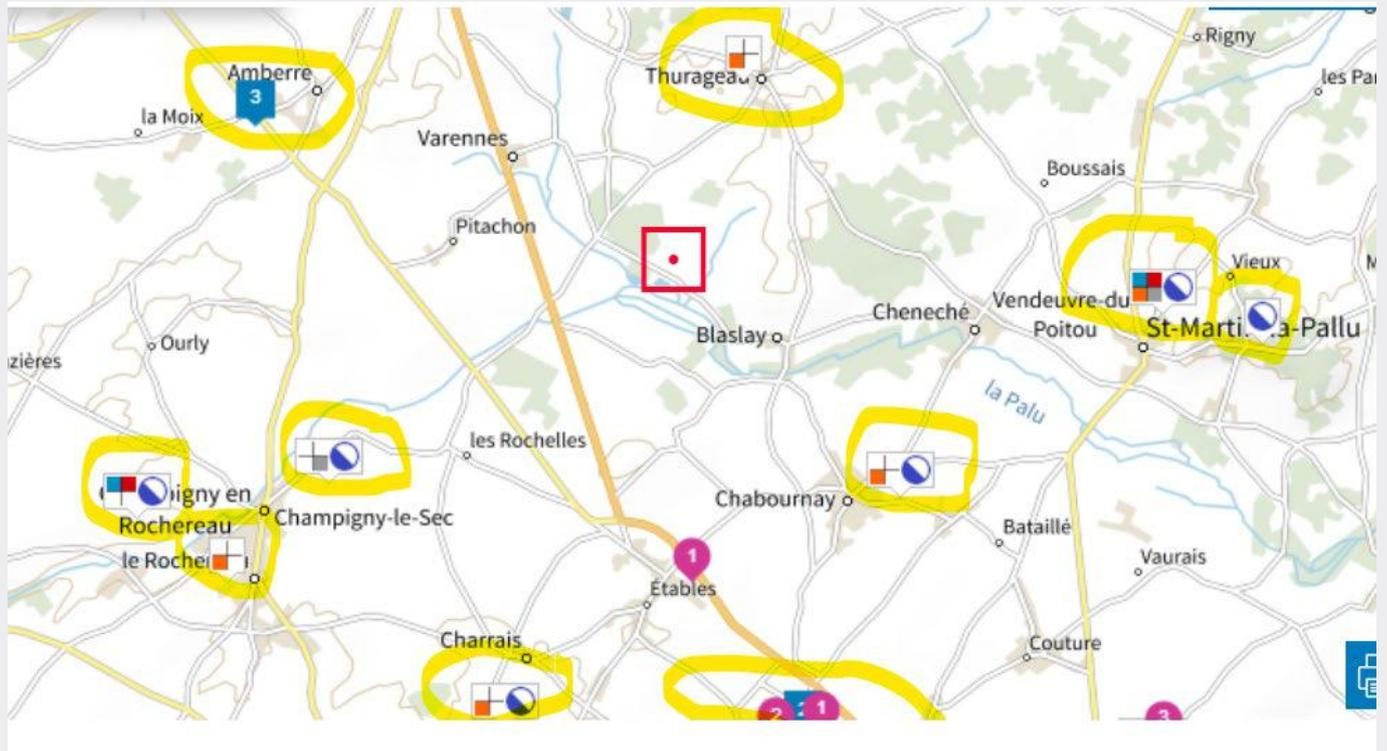
Le 16/10/2021 vers 09 h 30 nous avons procédé à des tests préliminaires dans un champ en plein air situé à proximité de la commune de Chabournay.

Les coordonnées GPS exactes du site sont les suivantes : $46^{\circ}44'49.6''N$
 $0^{\circ}13'32.0''E$.



Le point rouge marque l'endroit où a été installé le poste de détection.

Un repérage de la zone est effectué sur cartoradio :



L'endroit de l'expérimentation est indiqué par un point rouge dans un carré rouge.

Les différents sites surlignés correspondent à des antennes relais dont les caractéristiques sont accessibles [ici](#).

3/1 Déroulé des pré-tests

L'antenne est connectée, les serveurs activés.

Le protocole se lance.



Les candidats partent du point bleu et suivent le chemin (petits points verts) en direction du poste de détection (point rouge).

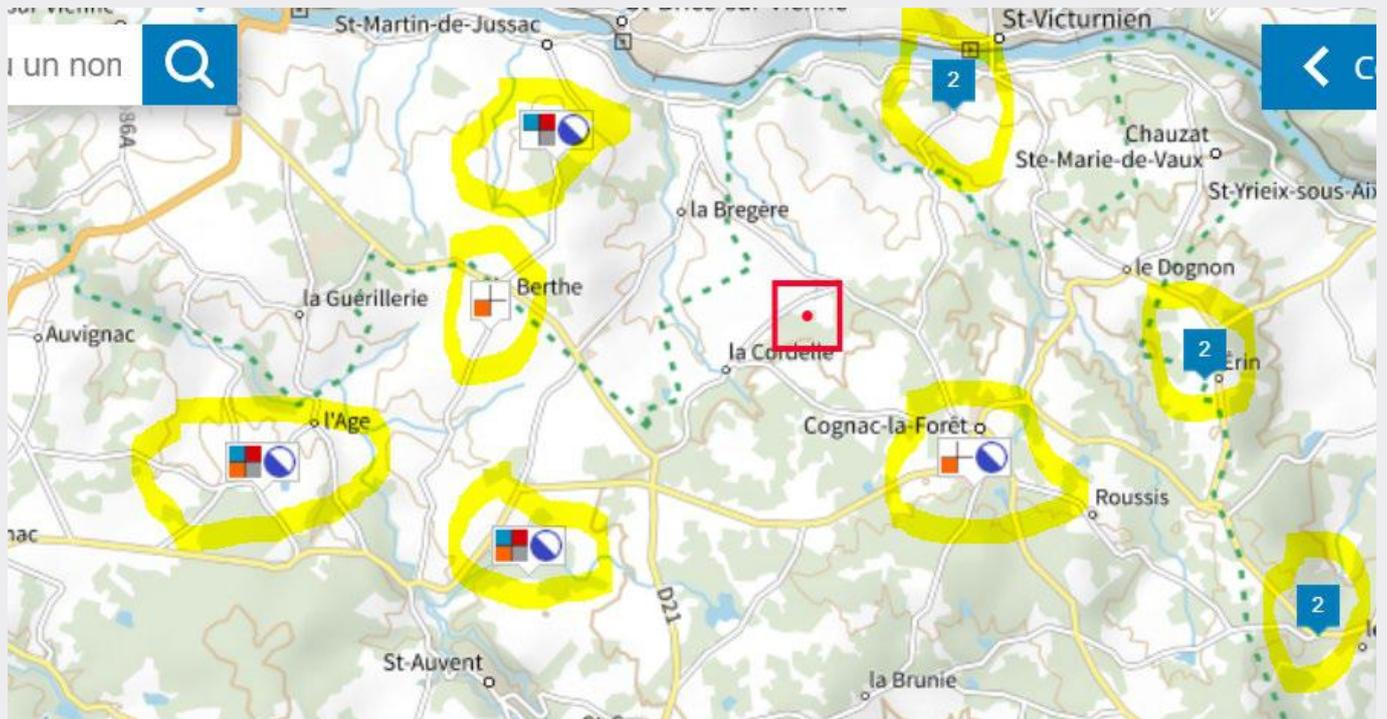
Dans un certain nombre de cas des signaux Bluetooth s'activent spontanément à environ 30 mètres du poste (point violet)

Le pré-test est concluant et fonctionnel, permettant de valider le protocole de test prévu pour le lendemain.

3/2 Déroulé de l'expérience

L'expérimentation a lieu le 17/10/2021 sur la commune de Cognac La forêt.

Un repérage Cartoradio donne la topographie suivante :



Les différents sites surlignés correspondent à des antennes relais dont les caractéristiques sont accessibles [ici](#).

Une reconnaissance des lieux nous amène à installer le matériel de détection à l'endroit indiqué sur la carte.



3/2/1 préparation technique

Les appareils de prise de vue sont soigneusement configurés et les personnels susceptibles d'intervenir dans la zone de détection sont testés les uns après les autres.

Les consignes suivantes leur ont été données :

- Pas de téléphone portable
- Pas de montre connectée
- Pas d'appareillage connecté (oreillette, casque,...)

Une fois ces préalables remplis ils passent le test plusieurs fois de suite :

- Seul et sans matériel
- Seul avec matériel éteint
- Seul avec matériel de prise de vue allumé.

Les caméras et le matériel de prise de son sont câblés et les systèmes de transmission sont tous désactivés.

Du fait de ces réglages deux passages additionnels sont effectués pour objectiver l'absence totale de signal détecté.

3/2/2 Déroulé de l'expérimentation

En parallèle, les postulants sont regroupés au niveau de l'aire d'accueil (A proximité de la zone de parking) et un questionnaire leur est donné à remplir.

Ils reçoivent tous les mêmes consignes et une personne vérifie physiquement l'exécution des consignes.

Ils suivent un à un le trajet identifié en violet comme « trajet des volontaires ».

Les points violets marquent les endroits où sont apparus les différents signaux.

3/2/3 Résultats obtenus

Le tableau ci-dessous donne l'ordre d'apparition des signaux.

Horaire	Numéro de passage	Détection de signal	Code retrouvé	Code retrouvé	OUI	Parasite ?	Identification
10:16							
10:21	1	Non	Néant			néant	
10:26	2	Oui	53:cd:58:dd:53:d2		Unknown	néant	
10:31	3	Oui	50:76:35:50:8f:36	73:dd:d1:6d58:f9	Unknown	néant	
10:36	4	Non	Néant			néant	
10:41	5	Non	Néant			néant	
10:46	6	Non	Néant			néant	
10:51	7	Non	Néant			néant	
10:56	8	Non	Néant			néant	
11:01	9	Non	Néant			néant	
11:06	10	Non	Néant			néant	
11:11	11	Non	Néant			néant	
11:16	12	Non	Néant			néant	
11:21	13	Non	Néant			néant	
11:26	14	Non	Néant			néant	
11:31	15	Oui	6f:12:bd:31:60:f9		Unknown	néant	
11:36	16	Oui	67:87:07:71:fb:ff		Unknown	néant	
11:41	17	Non	Néant			néant	

11:46	18	Oui	f1:5e:84:4c55:30	67:87:07:71:fb:ff	Unknown	néant	
11:51	19	Non	Néant			néant	
11:56	20	Non	Néant			néant	
12:01	21	Oui	57:58:87:13:a3:98			69:f4:76:99:6d:de	Android
12:06	22	Non	Néant			néant	
12:11	23	Non	Néant			néant	
12:16	24	Non	Néant			néant	
12:21	25	Non	Néant			néant	
12:26	26	Non	Néant			néant	
12:31	27	Non	Néant			néant	
12:36	28	Non	Néant			néant	
12:41	29	Non	Néant			néant	
12:46	30	Non	Néant			néant	
12:51	31	Non	Néant			néant	
12:56	32	Non	Néant			néant	
13:01	33	Non	Néant			néant	
13:06	34	Non	Néant			néant	
13:11	35	Non	Néant			néant	
13:16	36	Oui	55:la:e4:bc:ae:d9		Unknown	69:f4:76:99:6d:de	Android
13:21	37	Non	Néant			69:f4:76:99:6d:de	Android

3/3 Analyse brute des résultats

Les premières conclusions de l'expérimentation sont reportées dans les tableaux de synthèse suivants :

Données brutes		Émission	absence d'émission	Doute
Nombre de personnes	37	7	30	2
Injectées	15	6	9	2
Non injectées, testées	2	1	1	0
Non injectées, non testées	20	0	20	0
Soit en pourcentage :				
Pourcentages		Émission	absence d'émission	Doute
Nombre de personnes	37	19%	81%	5%
Injectées	15	40%	60%	13%
Non injectées, testées	2	50%	50%	0%
Non injectées, non testées	20	0%	100%	0%

Cette expérimentation met donc en évidence de manière indiscutable les éléments suivants :

- Aucune personne non injectée, non testée n'émet de signal
- Quelques personnes injectées émettent des signaux dans environ 40 % des cas
- Quelques personnes non injectées et testées émettent des signaux dans le 50 % des cas.

3/4 Exploration complémentaire

Au vu de ces expériences plusieurs incertitudes restent pleines et entières :

- Le temps de mesure
- Les interactions potentielles avec l'environnement électromagnétique
- Les interactions sociales
- La détectabilité de signaux émanant de personnes non injectées et testées.

Une nouvelle expérimentation a donc été entreprise le 07/11/2021 sur un lieu différent.

Ce nouveau lieu présente l'avantage de disposer de grottes troglodytes suffisamment hermétiques pour pouvoir agir comme une cage de Faraday.



3/4/1 : Déroulé de l'expérimentation

Lors de première journée les postulants ont été regroupés sous une tente d'accueil située sur la partie haute du terrain à plus de 50 mètres de l'opposée à l'entrée principale des grottes.

Les mêmes consignes leur ont été données et la même vigilance stricte a été observée quant à l'observance des consignes.

La répartition des postulants est la suivante :

- 2 personnes non injectées non testées
- 7 personnes non injectées et testées
- 8 personnes injectées

Un scan a été effectué en amont à l'intérieur de la grotte qui met en évidence l'absence totale de trafic Bluetooth.

L'expérimentation se déroule en deux jours :

Jour 1

Etaient présents 16 candidats se répartissant comme suit :

- 2 personnes non injectées non testées
- 6 personnes non injectées et testées
- 8 personnes injectées

Jour 2

Etait présent un candidat non injecté et testé

Durant ces deux jours, le protocole appliqué est le suivant :

Chaque candidat s'identifie en amont, sous la tente.

Il lui est attribué un numéro de passage.

Toutes les 20 minutes, un nouveau candidat se présente dans la grotte troglodyte où a été installé le matériel de scan et passe 20 minutes dans cette dernière en vue de la détection éventuelle d'un signal Bluetooth.

3/4/2 : Résultats de l'expérimentation

Jour 1 :

Les candidats se succèdent un par un.

Une seule adresse MAC est relevée :

c4:df:27:f9:45:b5

Il s'agit d'une personne doublement injectée

Jour 2 :

Un seul candidat est présent.

Il s'agit d'une personne non injectée mais muti testée par tests PCR (environ 70 tests)

Deux adresses Mac apparaissent simultanément avec des références quasi identiques :

4c:64:fd:da:fc:5f

4c:64:fd:da:fc:9f

Au vu de ces résultats, nous avons choisi de poursuivre l'expérience.

Nous avons éteint et rallumé le serveur kismet.

Les signaux captés n'apparaissent plus.

Nous sommes ensuite montés sur le plateau, sous la tente pour tester une éventuelle réactivation du signal en présence d'un environnement moins protégé.

Après 20 minutes de scan aucun nouveau signal n'apparait.

Nous avons alors demandé au candidat de se prêter à quelques exercices physiques afin de vérifier une potentielle relation entre l'énergie corporelle dégagée par le candidat et une activation de signal.

Après 20 minutes de scan aucun nouveau signal n'apparait.

Nous avons alors demandé à une personne de l'équipe de rapprocher progressivement le téléphone portable du candidat (Samsung) afin de commencer à vérifier de possibles interactions homme-portable.

Aucune activité particulière n'est détectée avec le portable en mode éteint.

Nous avons renouvelé l'expérience avec le portable en mode avion.

Aucune activité particulière n'est détectée avec le portable en mode éteint.

Nous avons renouvelé l'expérience avec le portable en mode normal, bluetooth éteint.

Aucune activité particulière n'est détectée avec le portable dans cette configuration.

Nous avons alors activé le bluetooth de l'appareil du candidat. Le Bluetooth est détecté, un trafic strictement normal se met en place, aucune adresse MAC suspecte n'apparait.

Nous avons ensuite amené un second téléphone portable (Également un Samsung) en mode normal, bluetooth activé.

Les appareils communiquent de manière cohérente entre eux et aucune adresse MAC additionnelle n'apparait.

Enfin, afin de récupérer des données additionnelles, nous avons continué à scanner le trafic en milieu ambiant, le candidat réintégrant l'intérieur de la maison dans laquelle était présents 6 téléphones portables dans des

conditions diverses, une box internet avec 2 relais wifi.

Nous avons progressivement éteint tous les dispositifs puis nous les avons rallumés un à un.

Il est à noter que sur toutes les personnes présentes seul le candidat a été testé par PCR.

On note des trafics strictement normaux qui correspond aux échanges de données entre les différents appareils.

On note également un nombre conséquent de trames non valides et des paquets inconnus ou ininterprétables avec le logiciel Wire Shark.

Nous pouvons donc raisonnablement conclure qu'à la fois les personnes injectées et les personnes testées émettent des signaux en dehors de toute activation induite par un champs électromagnétique environnemental.

Cependant ces signaux ne semblent pas constants dans le temps et leur activation semble dépendre de conditions qui restent à définir.

(Cf conclusions et perspectives ci-dessous.)

4/ Exploitation des données brutes

4/1 Rappel du contexte

Durant ces expériences, nous avons pu constater et capturer les échanges (trames) émises par des dispositifs inconnus dans des lieux vierges de tout signaux.

Lors de ces expériences ne disposant pas du matériel nécessaire à une analyse complète, nous avons pratiqué un scan employant un mode balayage à l'aide d'un équipement Ubertooth.

Cette carte nous a permis de balayer l'ensemble des fréquences employées par le protocole Bluetooth.

BTLE dans sa version 5 dispose de 40 canaux qui ont été scannés tour à tour et à intervalle régulière.

Le protocole Bluetooth BTLE est couramment utilisé pour de nombreuses applications et nous sommes donc partis de l'exploration des modes de construction classiques s'appuyant sur cette technologie.

De nombreuses ressources existent.

A titre d'exemple :

<https://www.bluetooth.com/bluetooth-resources/intro-to-bluetooth-low-energy-coded-phy/>

4/2 Volume des informations récupérées

Durant la première expérience, 37 participants se sont succédé ce qui a permis la capture d'un total de 43043 trames.

Durant l'expérimentation complémentaire, 17 participants se sont succédé ce qui a permis la capture d'un total de 30120 trames.

Ce qui nous donne donc un total de 73163 trames récupérées sur 6 h 30 de scan auprès de 34 personnes. (Personnes non injectées et non testées exclues).

1	0.000000			LE LL	24 Unknown[Malformed Packet]
2	8.046721	1f:a6:55:e0:2a:49	Broadcast	LE LL	27 Unknown[Malformed Packet]
3	27.697443	48:0a:b8:3c:2b:3a	88:e6:46:39:6f:79	LE LL	44 Unknown[Malformed Packet]
4	44.129321	a0:09:d7:19:b2:2e	Broadcast	LE LL	53 Unknown[Malformed Packet]
5	64.479816			LE LL	29 Unknown[Malformed Packet]
6	73.175723			LE LL	51 Unknown[Malformed Packet]
7	332.152347			LE LL	59 Unknown[Malformed Packet]
8	349.427467			LE LL	55 Unknown[Malformed Packet]
9	421.440920	Anonymous	Broadcast	LE LL	30 AUX_CONNECT_RSP[Malformed Packet]
10	747.384849	0e:01:c8:1a:76:ec	Broadcast	LE LL	40 AUX_CONNECT_RSP[Malformed Packet]
11	944.413346			LE LL	51 Unknown[Malformed Packet]
12	1033.379559			LE LL	57 Unknown[Malformed Packet]
13	1034.229202			LE LL	22 Unknown[Malformed Packet]
14	1587.518508	bd:08:25:e5:5e:97	5a:b6:b1:0b:32:83	LE LL	36 Unknown[Malformed Packet]
15	1719.226745	61:b6:db:ed:95:0f	Broadcast	LE LL	45 Unknown[Malformed Packet]
16	1744.372761	69:18:33:01:b2:5d	1e:29:68:e0:7a:11	LE LL	40 Unknown[Malformed Packet]
17	1762.492199	c5:07:a7:32:4f:4f	Broadcast	LE LL	52 Unknown[Malformed Packet]
18	1762.539511	45:05:d9:82:5b:a7	Broadcast	LE LL	52 Unknown
19	1762.565881	c5:07:f2:82:4d:67	Broadcast	LE LL	52 Unknown[Malformed Packet]
20	1762.585510	c5:07:f2:82:4d:67	Broadcast	LE LL	52 Unknown
21	1762.611218	c5:07:f2:82:4d:67	Broadcast	LE LL	52 Unknown
22	1762.657599	c5:07:f2:82:4d:67	Broadcast	LE LL	52 Unknown

Frame 1: 24 bytes on wire (192 bits), 24 bytes captured (192 bits) on interface ubertooth-0, id 0
 Bluetooth
 Bluetooth Low Energy RF Info
 Bluetooth Low Energy Link Layer
 Malformed Packet: BT LE LL

```
0000 25 9c 00 00 d6 be 89 8e 23 00 d6 be 89 8e 71 c5 %.....#.....q:
0010 53 13 4d 44 25 bd cd 2d S-M-%...
```

Time shift applied to this packet (frame.offset_shift)

Paquets: 30120 · Affichés: 30120 (100.0%)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0f:1b:24:25:77:4c	Broadcast	LE LL	31 Unknown[Malformed Packet]	
2	156.892293	c4:7a:e0:bb:25:28	Broadcast	LE LL	35 Unknown[Malformed Packet]	
3	214.975540			LE LL	23 Unknown[Malformed Packet]	
4	278.172317			LE LL	30 Unknown[Malformed Packet]	
5	279.046399	4b:bb:67:d5:b3:10	Broadcast	BT Mesh PB...	36 Transaction Continuation	
6	400.973496	d4:56:a9:41:6a:31	Broadcast	LE LL	55 Unknown[Malformed Packet]	
7	402.266091	d4:56:a9:41:6a:31	Broadcast	LE LL	55 Unknown[Malformed Packet]	
8	403.557693	d4:56:a9:41:6a:31	Broadcast	LE LL	55 Unknown	
9	406.137940	d4:56:a9:41:6a:31	Broadcast	LE LL	55 Unknown	
10	407.427118	d4:56:a9:41:6a:31	Broadcast	LE LL	55 Unknown	
11	408.721744	d4:56:a9:41:6a:31	Broadcast	LE LL	55 Unknown	
12	410.014943	d4:56:a9:41:6a:31	Broadcast	LE LL	55 Unknown	
13	411.307320	d4:56:a9:41:6a:31	Broadcast	LE LL	55 Unknown	
14	417.747753	d4:56:a9:41:6a:31	Broadcast	LE LL	55 Unknown	
15	422.908382	d4:56:a9:41:6a:31	Broadcast	LE LL	55 Unknown	
16	424.195783	d4:57:bb:41:6a:31	Broadcast	LE LL	55 Unknown[Malformed Packet]	
17	425.488372	d4:56:a9:41:6a:31	Broadcast	LE LL	55 Unknown	
18	428.071625	d4:56:a9:41:6a:31	Broadcast	LE LL	55 Unknown	
19	429.365760	d4:56:a9:41:6a:31	Broadcast	LE LL	55 Unknown	
20	430.657688	d4:56:a9:41:6a:31	Broadcast	LE LL	55 Unknown	
21	431.947614	d4:56:a9:41:6a:31	Broadcast	LE LL	55 Unknown	
22	437.899062	d4:56:a9:41:6a:30	Broadcast	LE LL	55 Unknown[Malformed Packet]	
23	439.873697	d4:16:a9:43:2a:31	Broadcast	LE LL	53 Unknown[Malformed Packet]	
24	440.966763	d4:56:a9:41:6a:31	Broadcast	LE LL	55 Unknown	

Frame 1: 31 bytes on wire (248 bits), 31 bytes captured (248 bits) on interface ubertooth-0, id 0

Interface id: 0 (ubertooth-0)
 Interface name: ubertooth-0
 Interface description: Kismet datasource ubertooth-0 (ubertooth-0 - ubertooth-0:type=ubertooth)
 Encapsulation type: Bluetooth Low Energy Link Layer RF (161)
 Arrival Time: Oct 17, 2021 10:17:27.338460000 CEST
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1634458647.338460000 seconds
 [Time delta from previous captured frame: 0.000000000 seconds]
 [Time delta from previous displayed frame: 0.000000000 seconds]
 [Time since reference or first frame: 0.000000000 seconds]
 Frame Number: 1
 Frame Length: 31 bytes (248 bits)
 Capture Length: 31 bytes (248 bits)
 [Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: bluetooth:btle_rf:btle:btcommon]

Bluetooth
 [Source: 0f:1b:24:25:77:4c (0f:1b:24:25:77:4c)]
 [Destination: Broadcast (ff:ff:ff:ff:ff:ff)]
 Bluetooth Low Energy RF Info
 RF Channel: 37, 2476 MHz, Data channel 35
 Signal dBm: -99
 Unused signed byte: 0
 Access Address Offenses: 0
 Unused word: 0x8e09bed6
 Flags: 0x0023
 = Deselected: True
 = Signal Power Valid: True
 = Noise Power Valid: False
 = Decrypted: False

```
0000 25 9d 00 00 d6 be 89 8e 23 00 d6 be 89 8e f2 0c %.....#.....
0010 4c 77 25 24 1b 0f 06 c7 9c 86 39 b6 62 9a bc Lw%....-9-b-
```

Absolute time when this frame was captured (frame.time)

Paquets: 43043 · Affichés: 43043 (100.0%)

4/3 : Premières analyses protocolaires :

Parmi ces trames pour la plupart malformées d'après les formats de trame

reconnus par le logiciel Wire Shark, ce qui indique à minima une personnalisation de la pile protocolaire, on retrouve des paquets cohérents avec le protocole Bluetooth pour des messages de type :

- BT MeSH
- BTLE AUX_SCAN
- AUX_CONNECT
- Messages inconnus (ou non reconnus et interprétés par Wire Shark)

4/3/1 : Paquets correspondant à des messages BT MeSH

No.	Time	Source	Destination	Protocol	Length	Info
7161	2960.543347	58:0a:c3:d2:48:97	Broadcast	BT Mesh	42	
7862	2994.097600	58:0a:d3:96:40:a7	Broadcast	BT Mesh	42	
7998	2999.604954	7d:b1:b8:db:56:e6	Broadcast	BT Mesh	50	
13087	3277.684980	58:0a:c3:96:c0:07	Broadcast	BT Mesh	42	
13563	3297.790018	78:1a:c7:96:c0:57	Broadcast	BT Mesh	38	
14530	3337.208369	78:8a:c3:96:c0:07	Broadcast	BT Mesh	42	
15508	3398.354239	58:0a:c3:96:c0:06	Broadcast	BT Mesh	42	
15912	3414.543270	4f:00:2e:b4:d6:b3	Broadcast	BT Mesh	42	
22146	4154.972222	71:38:40:70:59:96	Broadcast	BT Mesh	57	
22251	4164.171849	71:38:40:10:19:d6	Broadcast	BT Mesh	57	
22356	4173.301911	70:38:40:10:1a:d6	Broadcast	BT Mesh	54	
22994	4280.266887	7b:19:7f:bd:5a:05	Broadcast	BT Mesh	42	
24197	4499.638238	5b:69:30:24:20:b4	Broadcast	BT Mesh	54	
24261	4508.071784	5b:98:37:35:59:65	Broadcast	BT Mesh	42	
25393	4810.064219	7b:18:f7:35:59:1d	Broadcast	BT Mesh	42	
25423	4812.505216	3b:18:34:36:58:05	Broadcast	BT Mesh	46	
25648	4832.433580	6f:0d:83:7d:10:28	Broadcast	BT Mesh	49	
25797	4849.242354	5b:19:7f:b5:59:05	Broadcast	BT Mesh	42	
25860	4860.103327	7b:18:37:35:59:85	Broadcast	BT Mesh	42	
25909	4888.123186	73:18:27:35:59:05	Broadcast	BT Mesh	42	
26061	4909.584811	7b:18:56:b5:5b:05	Broadcast	BT Mesh	42	
27300	5175.108909	7b:18:17:05:41:64	Broadcast	BT Mesh	42	
27447	5195.515077	7f:18:37:35:59:c5	Broadcast	BT Mesh	46	
27930	5249.845923	2e:98:07:05:59:e5	Broadcast	BT Mesh	50	
27959	5252.568422	5b:18:37:35:59:05	Broadcast	BT Mesh	41	
28768	5356.703340	7b:19:16:35:59:05	Broadcast	BT Mesh	42	
28949	5384.963579	79:18:3f:34:d9:05	Broadcast	BT Mesh	42	
29127	5416.753762	7b:18:77:25:5a:25	Broadcast	BT Mesh	40	
31167	5797.233586	7b:18:37:34:59:05	Broadcast	BT Mesh	42	
32351	6482.234947	7b:98:17:35:58:05	Broadcast	BT Mesh	38	
32828	6681.500045	7b:1c:36:39:59:05	Broadcast	BT Mesh	56	
33633	7063.402140	7b:18:7f:15:55:05	Broadcast	BT Mesh	42	
33807	7369.145932	7b:19:37:3d:59:45	Broadcast	BT Mesh	42	
33851	7412.623025	7b:18:37:35:55:05	Broadcast	BT Mesh	42	
33854	7421.042417	7b:18:37:35:d9:04	Broadcast	BT Mesh	42	
33916	7678.175721	67:8f:1f:71:9b:ff	Broadcast	BT Mesh	50	
35130	8696.791045	67:87:17:b1:92:7e	Broadcast	BT Mesh	38	
36032	9723.610752	64:27:df:31:b3:38	Broadcast	BT Mesh	42	
37054	10202.237002	47:00:06:13:73:00	Broadcast	BT Mesh	42	
18560	77205.438502	52:8c:77:ca:79:d1	Broadcast	BT Mesh	43	
26029	77700.342759	6b:b6:44:7d:5e:f6	Broadcast	BT Mesh	42	
27103	77795.056748	6a:b6:44:7d:5e:f6	Broadcast	BT Mesh	42	
27138	77799.410775	6a:b6:c4:7d:5e:f6	Broadcast	BT Mesh	42	
56	3633.040370	Anonymous	ae:8d:df:99:a4:f8	LE LL	54	AUX_COMMON[Malformed Packet: length of contained item exceeds length of containing item]
1696	73551.913138	4e:43:b6:19:0e:31	22:f9:09:e4:0f:9c	LE LL	46	AUX_COMMON[Malformed Packet: length of contained item exceeds length of containing item]
1845	74818.992378	Anonymous	ae:8d:df:99:a4:f8	LE LL	37	AUX_COMMON[Malformed Packet: length of contained item exceeds length of containing item]
110	7644.661478	Anonymous	56:bb:b4:55:d6:b6	LE LL	25	AUX_COMMON[Malformed Packet]
137	9756.797208	Anonymous	12:d5:61:af:8e:f4	LE LL	36	AUX_COMMON[Malformed Packet]
1363	10812.102579	07:c9:b3:45:a0:26	Broadcast	LE LL	45	AUX_COMMON[Malformed Packet]
10433	76423.877844	Anonymous	f8:ca:b2:91:2c:ce	LE LL	49	AUX_COMMON[Malformed Packet]
12535	76784.972248	8f:6a:78:5e:db:82	0b:83:f5:cd:dd:58	LE LL	33	AUX_COMMON[Malformed Packet]
20724	77354.176792	40:a5:8b:e5:6b:86	Broadcast	LE LL	32	AUX_COMMON[Malformed Packet]
24501	77595.233191	Anonymous	d3:c9:b0:a8:98:b6	LE LL	45	AUX_COMMON[Malformed Packet]
24082	77566.227307	SamsungE_9b:14:8d	SamsungE_31:df:08	LE LL	53	AUX_CONNECT_REQ
37	2204.590729	32:f8:9d:3a:79:a0	b1:ab:e8:29:91:bd	LE LL	50	AUX_CONNECT_REQ[Malformed Packet]
38	2297.353324	83:63:47:31:4a:6f	eb:34:68:f1:01:c6	LE LL	32	AUX_CONNECT_REQ[Malformed Packet]
46	3150.335181	bf:64:9f:23:02:d4	1b:d2:d6:05:4e:bb	LE LL	53	AUX_CONNECT_REQ[Malformed Packet]
65	4693.766390	63:98:7d:51:5d:04	17:be:b8:11:e3:62	LE LL	35	AUX_CONNECT_REQ[Malformed Packet]
70	5224.232228	bb:9e:c0:3f:cf:b7	22:7c:bb:1d:c6:76	LE LL	43	AUX_CONNECT_REQ[Malformed Packet]
75	5482.152165	97:f1:62:3d:3e:2b	4e:f2:0b:62:39:2f	LE LL	40	AUX_CONNECT_REQ[Malformed Packet]
125	8919.895270	79:4b:3c:28:59:37	90:4a:68:2a:01:e4	LE LL	52	AUX_CONNECT_REQ[Malformed Packet]
1531	71911.775613	58:47:cc:be:98:6a	0e:16:ae:1c:f3:d6	LE LL	38	AUX_CONNECT_REQ[Malformed Packet]
1843	74809.429831	df:8f:ac:dc:4e:d7	f0:1a:c0:69:c8:70	LE LL	60	AUX_CONNECT_REQ[Malformed Packet]

4/3/2 : Paquets correspondant à des messages BTLE

AUX_SCAN

50	3412.517750	8c:78:99:09:e8:77	77:53:dd:9e:28:b4	LE LL	33 AUX_SCAN_REQ
113	7977.762969	6e:cb:c1:c3:cc:c6	c5:07:f2:82:4d:67	LE LL	31 AUX_SCAN_REQ
120	8539.343299	6e:cb:c1:c3:cc:c6	c5:07:f2:82:4d:67	LE LL	31 AUX_SCAN_REQ
152	10480.214139	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
199	10498.061199	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
206	10499.997550	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
214	10503.820931	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
233	10509.618182	78:72:86:87:43:39	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
244	10512.088668	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
246	10512.919916	39:14:69:77:a3:66	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
281	10523.650119	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
295	10528.322365	78:72:86:87:43:39	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
312	10535.176507	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
324	10539.011483	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
366	10549.631356	31:72:71:73:86:0d	22:22:1f:b0:64:3b	LE LL	31 AUX_SCAN_REQ
400	10557.729081	07:30:d2:82:4f:71	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
431	10566.568882	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
470	10576.299509	22:22:1f:b0:40:2b	3f:c7:14:c0:e1:7a	LE LL	38 AUX_SCAN_REQ
543	10598.868374	78:72:86:87:43:39	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
546	10599.417412	78:72:86:87:43:39	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
572	10606.560043	78:72:86:87:43:39	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
576	10607.380753	39:ba:05:8b:39:a9	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
599	10612.606970	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
614	10615.929050	78:72:86:87:43:39	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
625	10618.117552	2a:85:f0:ac:fa:ca	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
652	10625.287095	78:72:86:87:43:39	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
682	10634.640040	78:72:86:87:43:39	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
706	10640.694802	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
714	10642.615268	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
744	10650.363266	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
752	10652.843787	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
777	10659.269239	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
810	10669.971937	06:79:b1:ef:5f:62	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
838	10677.150524	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
841	10677.834623	42:22:1f:b0:64:3b	cc:07:11:22:01:02	LE LL	46 AUX_SCAN_REQ
853	10680.428943	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
889	10690.629287	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
948	10709.909550	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
981	10718.806804	78:72:86:87:43:39	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
991	10720.728517	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
1031	10732.843196	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
1048	10737.512873	78:72:86:87:43:39	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
1079	10744.372425	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
1102	10750.134793	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
1135	10759.479398	78:72:86:87:43:39	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
1169	10768.829247	78:72:86:87:43:39	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
1209	10778.173045	78:72:86:87:43:39	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
1216	10779.555746	1b:90:fc:44:0e:f1	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
1228	10781.489464	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
1268	10791.650203	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
1301	10798.785359	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
1319	10802.633898	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
1335	10805.095718	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
1351	10808.944769	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
1360	10810.871872	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
1378	10814.723734	61:20:c7:ac:82:a3	56:c0:23:54:e6:e7	LE LL	31 AUX_SCAN_REQ
1459	71538.374324	82:78:15:5f:aa:a0	07:e6:87:1e:9c:f6	LE LL	35 AUX_SCAN_REQ

No.	Time	Source	Destination	Protocol	Length	Info
50	3412.517750	8c:78:99:09:e8:77	77:53:dd:9e:28:b4	LE LL	33	AUX_SCAN_REQ
<pre> Frame 50: 33 bytes on wire (264 bits), 33 bytes captured (264 bits) on interface ubertooth-0, id 0 Interface id: 0 (ubertooth-0) Interface name: ubertooth-0 Interface description: Kismet datasource ubertooth-0 (ubertooth-0 - ubertooth-0:type=ubertooth) Encapsulation type: Bluetooth Low Energy Link Layer RF (161) Arrival Time: Nov 6, 2021 16:02:29.048614000 CET [Time shift for this packet: 0.000000000 seconds] Epoch Time: 1636210949.048614000 seconds [Time delta from previous captured frame: 17.181077000 seconds] [Time delta from previous displayed frame: 17.181077000 seconds] [Time since reference or first frame: 3412.517750000 seconds] Frame Number: 50 Frame Length: 33 bytes (264 bits) Capture Length: 33 bytes (264 bits) [Frame is marked: False] [Frame is ignored: False] [Protocols in frame: bluetooth:btle_rf:btle] Bluetooth [Source: 8c:78:99:09:e8:77 (8c:78:99:09:e8:77)] [Destination: 77:53:dd:9e:28:b4 (77:53:dd:9e:28:b4)] Bluetooth Low Energy RF Info RF Channel: 37, 2476 MHz, Data channel 35 Signal dBm: -99 Unused signed byte: 0 Access Address Offenses: 0 Unused word: 0x8e89bed6 Flags: 0x0023 1 = Dewhitened: True ...1. = Signal Power Valid: True ...0.. = Noise Power Valid: False ...0... = Decrypted: False ...0.... = Reference Access Address Valid: False ...1..... = Access Address Offenses Valid: True ...0..... = Channel Aliased: False ...000... = PDU Type: Advertising or Data (Unspecified Direction) (0) ...0... = CRC Checked: False ...0... = CRC Valid: False ...0... = MIC Checked: False ...0... = MIC Valid: False 00... = PHY: LE 1M (0) Bluetooth Low Energy Link Layer Access Address: 0x8e89bed6 Packet Header: 0x0ee3 (PDU Type: AUX_SCAN_REQ, TxAdd: Random, RxAdd: Random) ...0011 = PDU Type: 0x3 AUX_SCAN_REQ ...0.... = Reserved: 0 ...1.... = Reserved: 1 ...1... = Tx Address: Random ...1... = Rx Address: Random Length: 14 Scanning Address: 8c:78:99:09:e8:77 (8c:78:99:09:e8:77) Advertising Address: 77:53:dd:9e:28:b4 (77:53:dd:9e:28:b4) CRC: 0xe6efaa [Expert Info (Warning/Checksum): Incorrect CRC] [Incorrect CRC] [Severity level: Warning] </pre>						
0000	25 9d 00 00 d6 be 89 8e	23 00 d6 be 89 8e e3 0e	%.....#.....			
0010	77 e8 09 99 78 8c b4 28	9e dd 53 77 67 f7 55 47	w...x...(..Swg·UG			
0020	53	S				

4/3/2 : Paquets correspondant à des messages AUX_CONNECT

2352	1763.558555	71:ea:66:14:e0:20	64:0b:23:02:01:02	LE LL	54	AUX_CONNECT_REQ
4294	2492.944386	74:bf:67:2d:cf:24	4d:e6:b0:37:cf:44	LE LL	55	AUX_CONNECT_REQ
5397	2735.659536	4d:c9:4c:ed:8b:65	9a:55:58:f5:4b:f3	LE LL	57	AUX_CONNECT_REQ
7120	2958.139705	7e:b1:a8:d3:d2:e7	61:91:86:1e:e1:03	LE LL	58	AUX_CONNECT_REQ
28944	5384.105866	69:cf:45:c9:13:8b	06:8e:b0:31:55:26	LE LL	53	AUX_CONNECT_REQ
31768	6069.496377	62:64:df:5c:89:c6	0f:b9:ba:d5:26:07	LE LL	57	AUX_CONNECT_REQ
32201	6357.786142	af:cf:a3:cf:df:af	fe:73:3b:1a:55:76	LE LL	55	AUX_CONNECT_REQ
32845	6691.589539	b1:db:51:4d:58:f4	60:87:33:29:51:02	LE LL	54	AUX_CONNECT_REQ
32945	6734.820836	4e:f4:5a:72:92:d2	8e:8a:57:41:05:90	LE LL	57	AUX_CONNECT_REQ
37833	10571.702736	1a:9e:16:c7:0b:0e	4b:3c:9b:1b:03:02	LE LL	56	AUX_CONNECT_REQ

No.	Time	Source	Destination	Protocol	Length	Info
2352	1763.558555	71:ea:66:14:e0:20	64:0b:23:02:01:02	LE LL	54	AUX_CONNECT_REQ

```

4
▼ Frame 2352: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface ubertooth-0, id 0
  ▼ Interface id: 0 (ubertooth-0)
    Interface name: ubertooth-0
    Interface description: Kismet datasources ubertooth-0 (ubertooth-0 - ubertooth-0:type=ubertooth)
    Encapsulation type: Bluetooth Low Energy Link Layer RF (161)
  Arrival Time: Oct 17, 2021 10:46:50.897024000 CEST
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1634460410.897024000 seconds
  [Time delta from previous captured frame: 0.215241000 seconds]
  [Time delta from previous displayed frame: 0.215241000 seconds]
  [Time since reference or first frame: 1763.558555000 seconds]
  Frame Number: 2352
  Frame Length: 54 bytes (432 bits)
  Capture Length: 54 bytes (432 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: bluetooth:btle_rf:btle:btcommon]
  ▼ Bluetooth
    [Source: 71:ea:66:14:e0:20 (71:ea:66:14:e0:20)]
    [Destination: 64:0b:23:02:01:02 (64:0b:23:02:01:02)]
  ▼ Bluetooth Low Energy RF Info
    RF Channel: 37, 2476 MHz, Data channel 35
    Signal dBm: -89
    Unused signed byte: 0
    Access Address Offenses: 0
    Unused word: 0x8e89bed6
  ▼ Flags: 0x0023
    .... = Dewhitened: True
    ....1. = Signal Power Valid: True
    ....0.. = Noise Power Valid: False
    ....0... = Decrypted: False
    ....0... = Reference Access Address Valid: False
    ....1. .... = Access Address Offenses Valid: True
    ....0... = Channel Aliased: False
    ....000... = PDU Type: Advertising or Data (Unspecified Direction) (0)
    ....0... = CRC Checked: False
    ....0... = CRC Valid: False
    ....0... = MIC Checked: False
    ....0... = MIC Valid: False
    00... = PHY: LE 1M (0)
  ▼ Bluetooth Low Energy Link Layer
    Access Address: 0x8e89bed6
  ▼ Packet Header: 0x2345 (PDU Type: AUX_CONNECT_REQ, TxAdd: Random, RxAdd: Public)
    ....0101 = PDU Type: 0x5 AUX_CONNECT_REQ
    ...0... = Reserved: 0
    ..0... = Reserved: 0
    .1... = Tx Address: Random
    0... = Rx Address: Public
    Length: 35
    Initiator Address: 71:ea:66:14:e0:20 (71:ea:66:14:e0:20)
    Advertising Address: 64:0b:23:02:01:02 (64:0b:23:02:01:02)
  ▼ Link Layer Data
    Access Address: 0xec9615fd

```

Bluetooth Low Energy Link Layer

Access Address: 0x8e89bed6

Packet Header: 0x2345 (PDU Type: AUX_CONNECT_REQ, TxAdd: Random, RxAdd: Public)

... 0101 = PDU Type: 0x5 AUX_CONNECT_REQ

...0 = Reserved: 0

..0. = Reserved: 0

.1.. = Tx Address: Random

0... = Rx Address: Public

Length: 35

Initiator Address: 71:ea:66:14:e0:20 (71:ea:66:14:e0:20)

Advertising Address: 64:0b:23:02:01:02 (64:0b:23:02:01:02)

Link Layer Data

Access Address: 0xec9615fd

CRC Init: 0x9f1700

Window Size: 253 (316,25 msec)

Window Offset: 41994 (52492,5 msec)

Interval: 52166 (65207,5 msec)

Latency: 15595

Timeout: 5406 (54060 msec)

Channel Map: cf0a3d2720

...1 1101 = Hop: 29

010. = Sleep Clock Accuracy: 101 ppm to 150 ppm (2)

CRC: 0x0a9329

[Expert Info (Warning/Checksum): Incorrect CRC]

[Incorrect CRC]

[Severity level: Warning]

[Group: Checksum]

0000	25 a7 00 00 d6 be 89 8e 23 00 d6 be 89 8e 45 23	%.....#.....E#
0010	20 e0 14 66 ea 71 02 01 02 23 0b 64 fd 15 96 ec	..f.q..#d....
0020	00 17 9f fd 0a a4 c6 cb eb 3c 1e 15 cf 0a 3d 27<....='
0030	20 5d 50 c9 94 2f]P../

```
▼ Frame 24082: 53 bytes on wire (424 bits), 53 bytes captured (424 bits) on interface ubertooth-0, id 0
  ▼ Interface id: 0 (ubertooth-0)
    Interface name: ubertooth-0
    Interface description: Kismet datasources ubertooth-0 (ubertooth-0 - ubertooth-0:type=ubertooth)
    Encapsulation type: Bluetooth Low Energy Link Layer RF (161)
    Arrival Time: Nov 7, 2021 12:38:22.758171000 CET
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1636285102.758171000 seconds
    [Time delta from previous captured frame: 0.004566000 seconds]
    [Time delta from previous displayed frame: 0.004566000 seconds]
    [Time since reference or first frame: 77566.227307000 seconds]
    Frame Number: 24082
    Frame Length: 53 bytes (424 bits)
    Capture Length: 53 bytes (424 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: bluetooth:btle_rf:btle:btcommon]
  ▼ Bluetooth
    [Source: SamsungE_9b:14:8d (24:fc:e5:9b:14:8d)]
    [Destination: SamsungE_31:df:08 (b8:bc:5b:31:df:08)]
  ▼ Bluetooth Low Energy RF Info
    RF Channel: 37, 2476 MHz, Data channel 35
    Signal dBm: -87
    Unused signed byte: 0
    Access Address Offenses: 0
    Unused word: 0x8e89bed6
  ▼ Flags: 0x0023
    .... .1 = Dewhitened: True
    .... .1. = Signal Power Valid: True
    .... .0.. = Noise Power Valid: False
    .... 0... = Decrypted: False
    .... ..0... = Reference Access Address Valid: False
    .... ..1. .... = Access Address Offenses Valid: True
    .... ..0.. .... = Channel Aliased: False
    .... ..00 0... = PDU Type: Advertising or Data (Unspecified Direction) (0)
    .... .0.. .... = CRC Checked: False
    .... 0... .... = CRC Valid: False
    .... ..0... .... = MIC Checked: False
    .... ..0. .... = MIC Valid: False
    00.. .... .... = PHY: LE 1M (0)
  ▼ Bluetooth Low Energy Link Layer
    Access Address: 0x8e89bed6
  ▼ Packet Header: 0x2205 (PDU Type: AUX_CONNECT_REQ, TxAdd: Public, RxAdd: Public)
    .... 0101 = PDU Type: 0x5 AUX_CONNECT_REQ
    ...0 .... = Reserved: 0
    ..0. .... = Reserved: 0
    .0.. .... = Tx Address: Public
    0... .... = Rx Address: Public
    Length: 34
    Initiator Address: SamsungE_9b:14:8d (24:fc:e5:9b:14:8d)
    Advertising Address: SamsungE_31:df:08 (b8:bc:5b:31:df:08)
  ▼ Link Layer Data
    Access Address: 0x489905d6
    CRC Init: 0x4f604b
    Window Size: 5 (6,25 msec)
    Window Offset: 5 (6,25 msec)
    Interval: 6 (7,5 msec)
```

Bluetooth Low Energy Link Layer

Access Address: 0x8e89bed6

Packet Header: 0x2205 (PDU Type: AUX_CONNECT_REQ, TxAdd: Public, RxAdd: Public)

... 0101 = PDU Type: 0x5 AUX_CONNECT_REQ

...0 = Reserved: 0

..0. = Reserved: 0

.0.. = Tx Address: Public

0... = Rx Address: Public

Length: 34

Initiator Address: SamsungE_9b:14:8d (24:fc:e5:9b:14:8d)

Advertising Address: SamsungE_31:df:08 (b8:bc:5b:31:df:08)

Link Layer Data

Access Address: 0x489905d6

CRC Init: 0x4f604b

Window Size: 5 (6,25 msec)

Window Offset: 5 (6,25 msec)

Interval: 6 (7,5 msec)

Latency: 170

Timeout: 500 (5000 msec)

Channel Map: ffffffff1f

0000	25 a9 00 00 d6 be 89 8e 23 00 d6 be 89 8e 05 22	%..... #....."
0010	8d 14 9b e5 fc 24 08 df 31 5b bc b8 d6 05 99 48\$. 1[.....H
0020	4b 60 4f 05 00 06 00 aa 00 f4 01 ff ff ff ff	K'0.....
0030	1f 30 df 39 c2	.0.9.

4/3/2 : Paquets correspondant à des messages inconnus (ou non interprétables en tant que tel par le logiciel Wire Shark)

11871	76712.777979	57:88:2e:e1:b0:1d	09:01:00:06:ff:0e	LE LL	56 AUX_SCAN_REQ[Malformed Packet]
23514	77544.167918	4c:da:66:eb:5b:9f	58:11:01:3d:17:f3	LE LL	28 AUX_SCAN_REQ[Malformed Packet]
27534	77830.555531	22:02:1f:b0:64:3a	98:0f:15:02:01:42	LE LL	45 AUX_SCAN_REQ[Malformed Packet]
1508	71863.662070	5a:2f:be:42:d5:9f	Broadcast	BT Mesh PB...	43 Provisioning Bearer Control[Malformed Packet: length of contained item exceeds length of containing item]
27680	77842.705337	3d:1d:df:46:0d:16	Broadcast	BT Mesh PB...	48 Provisioning Bearer Control[Malformed Packet: length of contained item exceeds length of containing item]
28718	77896.179350	66:22:1f:b0:60:3b	Broadcast	BT Mesh PB...	46 Transaction Continuation[Malformed Packet]
18	1762.539511	45:05:09:02:5b:a7	Broadcast	LE LL	52 Unknown
20	1762.585510	c5:07:f2:02:4d:07	Broadcast	LE LL	52 Unknown

18560	77205.438502	52:8c:77:ca:79:d1	Broadcast	BT Mesh	43
26029	77700.342759	6b:b6:44:7d:5e:f6	Broadcast	BT Mesh	42
27183	77795.056748	6a:b6:44:7d:5e:f6	Broadcast	BT Mesh	42
27138	77799.410775	6a:b6:c4:7d:5e:f6	Broadcast	BT Mesh	42
56	3633.040370	Anonymous	ae:8d:df:99:a4:f8	LE LL	54 AUX_COMMON[Malformed Packet: length of contained item exceeds length of containing item]
1696	73551.913138	4e:43:b6:19:0e:31	22:f9:09:e4:0f:9c	LE LL	46 AUX_COMMON[Malformed Packet: length of contained item exceeds length of containing item]
1845	74818.992378	Anonymous	Broadcast	LE LL	37 AUX_COMMON[Malformed Packet: length of contained item exceeds length of containing item]
110	7644.661478	Anonymous	56:bb:b4:55:d6:b6	LE LL	25 AUX_COMMON[Malformed Packet]
137	9756.797208	Anonymous	12:d5:61:af:8e:f4	LE LL	36 AUX_COMMON[Malformed Packet]
1363	10812.102579	07:c9:b3:45:a0:26	Broadcast	LE LL	45 AUX_COMMON[Malformed Packet]
10433	76423.877844	Anonymous	f8:ca:b2:91:2c:ce	LE LL	49 AUX_COMMON[Malformed Packet]
12535	76784.972248	8f:6a:78:5e:db:82	0b:83:fs:cd:dd:58	LE LL	33 AUX_COMMON[Malformed Packet]
20724	77354.176792	40:a5:8b:e5:6b:86	Broadcast	LE LL	32 AUX_COMMON[Malformed Packet]
24501	77595.233191	Anonymous	d3:c9:b0:a8:98:b6	LE LL	45 AUX_COMMON[Malformed Packet]
24032	77535.022307	SamsungE_9b:14:8d	SamsungE_31:df:08	LE LL	53 AUX_CONNECT_REQ
37	2204.590729	32:f8:9d:3a:79:a0	81:9b:e8:29:91:bd	LE LL	50 AUX_CONNECT_REQ[Malformed Packet]
38	2297.353324	83:63:47:31:4a:6f	eb:34:68:f1:01:c6	LE LL	32 AUX_CONNECT_REQ[Malformed Packet]
46	3150.335181	bf:64:9f:23:02:d4	1b:d2:d6:85:4e:bb	LE LL	53 AUX_CONNECT_REQ[Malformed Packet]
65	4693.766390	63:98:7d:51:5d:84	17:be:b8:11:e3:62	LE LL	35 AUX_CONNECT_REQ[Malformed Packet]
70	5224.232228	bb:9e:c0:3f:cf:b7	22:7c:bb:1d:c6:76	LE LL	43 AUX_CONNECT_REQ[Malformed Packet]
75	5482.152165	97:f1:62:3d:3e:2b	4e:f2:8b:62:3a:2f	LE LL	40 AUX_CONNECT_REQ[Malformed Packet]
125	8919.895270	79:4b:3c:28:59:37	90:4a:68:2a:01:e4	LE LL	52 AUX_CONNECT_REQ[Malformed Packet]
1531	71911.775613	58:47:cc:be:98:6a	0e:16:ae:1c:f3:d6	LE LL	38 AUX_CONNECT_REQ[Malformed Packet]
1843	74809.429831	df:8f:ac:dc:4e:d7	f0:1a:c0:69:c8:70	LE LL	60 AUX_CONNECT_REQ[Malformed Packet]

17177	77130.972195	b5:db:d7:de:42:aa	0b:c4:56:af:cf:7a	LE LL	54 AUX_CONNECT_REQ[Malformed Packet]
22398	77469.256938	8d:09:59:38:ae:5e	70:0c:17:b5:b2:4b	LE LL	55 AUX_CONNECT_REQ[Malformed Packet]
41	2829.881733	92:64:1f:2c:1c:a3	Broadcast	LE LL	48 AUX_CONNECT_RSP[Malformed Packet: length of contained item exceeds length of containing item]
642	10622.724388	Anonymous	d1:74:57:58:98:25	LE LL	44 AUX_CONNECT_RSP[Malformed Packet: length of contained item exceeds length of containing item]
1456	71443.253806	Anonymous	Broadcast	LE LL	43 AUX_CONNECT_RSP[Malformed Packet: length of contained item exceeds length of containing item]
17178	77131.164184	81:02:38:62:17:b4	Broadcast	LE LL	46 AUX_CONNECT_RSP[Malformed Packet: length of contained item exceeds length of containing item]
17931	77172.541502	d5:f5:50:d9:dc:e5	Broadcast	LE LL	49 AUX_CONNECT_RSP[Malformed Packet: length of contained item exceeds length of containing item]
26013	77698.908571	Anonymous	Beijing0_b0:c4:e4	LE LL	42 AUX_CONNECT_RSP[Malformed Packet: length of contained item exceeds length of containing item]
26023	77700.073365	Anonymous	e9:42:6a:b6:40:3d	LE LL	41 AUX_CONNECT_RSP[Malformed Packet: length of contained item exceeds length of containing item]
26473	77739.610990	Anonymous	09:0d:78:ae:c6:7d	LE LL	37 AUX_CONNECT_RSP[Malformed Packet: length of contained item exceeds length of containing item]
9	421.440920	Anonymous	Broadcast	LE LL	30 AUX_CONNECT_RSP[Malformed Packet]
10	747.384849	0e:01:c8:1a:7e:ec	Broadcast	LE LL	40 AUX_CONNECT_RSP[Malformed Packet]
57	3765.709238	Anonymous	f4:71:49:68:eb:03	LE LL	25 AUX_CONNECT_RSP[Malformed Packet]
63	4658.945088	6d:7d:ef:3c:64:fb	Broadcast	LE LL	54 AUX_CONNECT_RSP[Malformed Packet]
94	5740.959393	Anonymous	36:cd:18:dc:e0:d1	LE LL	48 AUX_CONNECT_RSP[Malformed Packet]
118	8374.569051	Anonymous	Broadcast	LE LL	30 AUX_CONNECT_RSP[Malformed Packet]

29790	77931.071351	MS-NLB-PhysServer-32_0_...	Broadcast	LE LL	46 Unknown[Malformed Packet]
29854	77932.096104	22:20:5f:b0:64:3b	Broadcast	LE LL	46 Unknown[Malformed Packet]
29887	77932.591668	35:8c:77:ca:79:d1	Broadcast	LE LL	43 Unknown[Malformed Packet]
29908	77933.121222	2a:22:1f:70:64:3b	Broadcast	LE LL	46 Unknown[Malformed Packet]
29932	77933.686559	d0:89:05:5c:59:75	Broadcast	LE LL	60 Unknown[Malformed Packet]
911	10699.467115	56:c0:23:54:e6:e7	Broadcast	BT Mesh	43 [Malformed Packet]
1462	71630.384194	4c:64:fd:da:fc:5f	Broadcast	BT Mesh	43 [Malformed Packet]
1473	71702.347915	4c:64:fd:da:fc:5f	Broadcast	BT Mesh	43 [Malformed Packet]
1479	71705.650330	4c:64:bd:da:fc:5f	Broadcast	BT Mesh	43 [Malformed Packet]
1499	71858.409012	4a:3f:be:42:55:9b	Broadcast	BT Mesh	43 [Malformed Packet]

5/ Conclusions et perspectives

Nous pouvons au vu de ces résultats affirmer qu'un pourcentage significatif des personnes injectées et, dans une moindre mesure des personnes non injectées mais testées par des tests PCR émettent des signaux alphanumériques sur la plage de fréquence correspondant à celle d'utilisation du Bluetooth.

Ce pourcentage sera à préciser par des études futures afin de mettre en évidence l'impact potentiel des facteurs suivants :

- Marque du produit injecté
- Profil du candidat :
 - Nombre d'injection(s)s reçue(s)
 - Date de la dernière injection

De nombreuses trames apparaissent en lien avec ces signaux qui sont ininterprétables en l'état actuel des choses par le logiciel Wire Shark.

Une des caractéristiques communes de ces trames est le faible niveau dBm.

Parmi les explications probables du caractère incomplet voire ininterprétable de ces trames des hypothèses sont à explorer :

- Une modulation différente de celle usuellement utilisée pour les protocoles BTLE classiques
- Un problème d'insuffisance énergétique insuffisante pour activer un déclenchement d'action
- Une série d'actions ordonnancée sur des sauts de channels (A l'intérieur de la gamme de fréquence Bluetooth et/ou en dehors de cette dernière).

Il existe une très nette prééminence de signaux émis en milieu ambiant par rapport aux signaux émis en milieu sans activité électromagnétique.

Des tests additionnels devront donc confirmer cette tendance et dégager les facteurs de déclenchement des signaux pour en préciser la nature et surtout la ou les fonctionnalité(s).

Ces signaux alphanumériques ne sont pas constants dans le temps et leur

apparition est brève.

Il est possible qu'un ordonnancement programmé (à heure fixe ou aléatoire, en fonction d'éléments déclencheurs tels que des interactions sociales) soutende ces apparitions.

De nombreuses autres expériences seront sans nul doute nécessaires pour acquérir suffisamment de données afin d'identifier des redondances, des cycles, des patterns...