## **TD GSM SNIFFING**

Remarque : l'interception des communications provenant d'un réseau mobile public peut être illégal dans le pays concerné.

Ce TD nécessite la carte SDR HackRF One et les logiciels gnuradio, gr-osmosdr et gr-gsm. La distribution Debian *Stretch* ne contient pas tous les paquets nécessaires, il faut alors compiler et installer gr-gsm à la main.

La distribution Debian *Buster* contient tous les paquets.

Nous allons utiliser l'hyperviseur QEMU qui permet i) de créer une VM dans laquelle nous aurons accès au compte *root*, ii) de faire de l'USB *Passthrough* et iii) d'y installer une distribution *Buster*.

## 1 Création d'une machine virtuelle

1. Créer un disque dur virtuel de 50GB au format QCOW2 nommé buster.qcow2 dans un dossier situé sous /espace sur la machine locale :

\$ qemu-img create -f qcow2 buster.qcow2 50G

2. Téléchargez la petite image ISO (360MB environ) de *Buster* sur /net/stockage/dmagoni ou sur le site de Debian :

debian-10.1.0-amd64-netinst.iso

3. Lancez la VM sur l'hyperviseur QEMU et faite l'installation :

```
$ qemu-system-x86_64 -name buster -machine type=q35,accel=kvm:tcg \
-cpu host -smp cpus=2,cores=1,threads=1,maxcpus=2 \
-drive file=buster.qcow2,index=0,media=disk,if=virtio,aio=native,format=qcow2,cache.direct=on \
-drive file=debian-10.1.0-amd64-netinst.iso,index=2,media=cdrom \
-boot order=d,menu=on -m size=2G,slots=1,maxmem=4G -k fr \
-display gtk -vga virtio -usb -device usb-tablet \
-netdev user,id=n1 -device e1000,netdev=n1
```

Expliquez en détail la ligne de commande ci-dessus grâce à la doc de QEMU. Lors de l'installation, créez une partition LVM unique et choississez l'environnement Gnome. A la fin de l'installation, installez Grub dans /dev/vda puis éteignez la VM.

4. Connectez la carte HackRF One en USB à l'un des ports de votre machine puis vérifiez que la carte est bien reconnue par le host avec :

\$ hackrf\_info

## 2 Capture du trafic radio

5. Relancez la VM avec la commande :

```
$ qemu-system-x86_64 -name buster \
-machine type=q35,accel=kvm:tcg \
-cpu host -smp cpus=2,cores=1,threads=1,maxcpus=2 \
-drive file=buster.qcow2,index=0,media=disk,if=virtio,aio=native,format=qcow2,cache.direct=on \
-boot order=cd,menu=on -m size=2G,slots=1,maxmem=4G \
-k fr -display gtk -vga virtio -usb -device usb-tablet \
-device usb-host,vendorid=0x1d50,productid=0x6089 \
-netdev user,id=net1 -device virtio-net-pci,netdev=net1
```

Expliquez les différences de cette commande avec la précédente. Que permet-elle de réaliser ?

- 6. Dans la VM, vérifiez que la carte HackRF One est accessible dans le *guest*.
- 7. Dans la VM, installez les paquets suivants :

# apt install vim htop

```
# apt install gnuradio gnuradio-dev hackrf libhackrf0 libhackrf-dev \
gr-osmosdr gr-gsm wireshark
```

8. Cherchez les canaux GSM des tours BTS proches en lançant la commande en tant que root :

# grgsm\_scanner

GNU C-	++ vers	ion 6.3.0	0 201	70221;	Boost_	106200	; UHD_	_003.	009.0	)05-0-i	unknov	vn
976,	Freq:	925.4M,	CID:	20002,	LAC:	609,	MCC:	208,	MNC:	20,	Pwr:	-56
980,	Freq:	926.2M,	CID:	63691,	LAC:	609,	MCC:	208,	MNC:	20,	Pwr:	-59
981,	Freq:	926.4M,	CID:	27745,	LAC:	609,	MCC:	208,	MNC:	20,	Pwr:	-56
983,	Freq:	926.8M,	CID:	49557,	LAC:	609,	MCC:	208,	MNC:	20,	Pwr:	-49
1004,	Freq:	931.0M,	CID:	26992,	LAC:	609,	MCC:	208,	MNC:	20,	Pwr:	-37
1014,	Freq:	933.0M,	CID:	26992,	LAC:	609,	MCC:	208,	MNC:	20,	Pwr:	-36
1016,	Freq:	933.4M,	CID:	26990,	LAC:	609,	MCC:	208,	MNC:	20,	Pwr:	-43
Θ,	Freq:	935.0M,	CID:	6016,	LAC:	1540,	MCC:	208,	MNC:	1,	Pwr:	-50
6,	Freq:	936.2M,	CID:	26892,	LAC:	1540,	MCC:	208,	MNC:	1,	Pwr:	-47
7,	Freq:	936.4M,	CID:	6042,	LAC:	1540,	MCC:	208,	MNC:	1,	Pwr:	-54
10,	Freq:	937.0M,	CID:	6016,	LAC:	1540,	MCC:	208,	MNC:	1,	Pwr:	-41
16,	Freq:	938.2M,	CID:	26892,	LAC:	1540,	MCC:	208,	MNC:	1,	Pwr:	-60
87,	Freq:	952.4M,	CID:	0,	LAC:	49943,	MCC:	208,	MNC:	10,	Pwr:	-57
109,	Freq:	956.8M,	CID:	43310,	LAC:	49926,	MCC:	208,	MNC:	10,	Pwr:	-46
119,	Freq:	958.8M,	CID:	43310,	LAC:	49926,	MCC:	208,	MNC:	10,	Pwr:	-43
122,	Freq:	959.4M,	CID:	43348,	LAC:	49926,	MCC:	208,	MNC:	10,	Pwr:	-59
	GNU C- 976, 980, 981, 983, 1004, 1014, 1016, 0, 6, 7, 10, 16, 87, 109, 119, 122,	GNU C++ vers 976, Freq: 980, Freq: 981, Freq: 983, Freq: 1004, Freq: 1014, Freq: 1016, Freq: 0, Freq: 0, Freq: 10, Freq: 16, Freq: 87, Freq: 109, Freq: 119, Freq: 122, Freq:	<pre>GNU C++ version 6.3.0 976, Freq: 925.4M, 980, Freq: 926.2M, 981, Freq: 926.4M, 983, Freq: 926.8M, 1004, Freq: 931.0M, 1014, Freq: 933.0M, 1016, Freq: 933.4M, 0, Freq: 935.0M, 6, Freq: 936.2M, 7, Freq: 936.4M, 10, Freq: 938.2M, 87, Freq: 952.4M, 109, Freq: 956.8M, 119, Freq: 959.4M,</pre>	<pre>GNU C++ version 6.3.0 201 976, Freq: 925.4M, CID: 980, Freq: 926.2M, CID: 981, Freq: 926.4M, CID: 983, Freq: 926.8M, CID: 1004, Freq: 931.0M, CID: 1014, Freq: 933.0M, CID: 1016, Freq: 933.4M, CID: 0, Freq: 935.0M, CID: 0, Freq: 936.2M, CID: 7, Freq: 936.4M, CID: 10, Freq: 937.0M, CID: 16, Freq: 938.2M, CID: 16, Freq: 952.4M, CID: 109, Freq: 956.8M, CID: 119, Freq: 959.4M, CID:</pre>	<pre>GNU C++ version 6.3.0 20170221; 976, Freq: 925.4M, CID: 20002, 980, Freq: 926.2M, CID: 63691, 981, Freq: 926.4M, CID: 27745, 983, Freq: 926.8M, CID: 49557, 1004, Freq: 931.0M, CID: 26992, 1014, Freq: 933.0M, CID: 26992, 1016, Freq: 933.4M, CID: 26990, 0, Freq: 935.0M, CID: 26990, 0, Freq: 936.2M, CID: 26892, 7, Freq: 936.4M, CID: 6016, 16, Freq: 937.0M, CID: 6016, 16, Freq: 938.2M, CID: 26892, 87, Freq: 952.4M, CID: 0, 109, Freq: 956.8M, CID: 43310, 119, Freq: 958.8M, CID: 43348,</pre>	<pre>GNU C++ version 6.3.0 20170221; Boost_ 976, Freq: 925.4M, CID: 20002, LAC: 980, Freq: 926.2M, CID: 63691, LAC: 981, Freq: 926.4M, CID: 27745, LAC: 983, Freq: 926.8M, CID: 49557, LAC: 1004, Freq: 931.0M, CID: 26992, LAC: 1014, Freq: 933.0M, CID: 26992, LAC: 1016, Freq: 933.4M, CID: 26990, LAC: 0, Freq: 935.0M, CID: 6016, LAC: 0, Freq: 936.2M, CID: 26892, LAC: 7, Freq: 936.4M, CID: 6042, LAC: 10, Freq: 937.0M, CID: 6016, LAC: 10, Freq: 938.2M, CID: 26892, LAC: 16, Freq: 938.2M, CID: 26892, LAC: 87, Freq: 952.4M, CID: 0, LAC: 109, Freq: 956.8M, CID: 43310, LAC: 119, Freq: 958.8M, CID: 43348, LAC:</pre>	<pre>GNU C++ version 6.3.0 20170221; Boost_106200 976, Freq: 925.4M, CID: 20002, LAC: 609, 980, Freq: 926.2M, CID: 63691, LAC: 609, 981, Freq: 926.8M, CID: 27745, LAC: 609, 983, Freq: 926.8M, CID: 49557, LAC: 609, 1004, Freq: 931.0M, CID: 26992, LAC: 609, 1014, Freq: 933.0M, CID: 26992, LAC: 609, 1016, Freq: 933.4M, CID: 26990, LAC: 609, 0, Freq: 935.0M, CID: 26892, LAC: 1540, 6, Freq: 936.2M, CID: 26892, LAC: 1540, 7, Freq: 936.4M, CID: 6016, LAC: 1540, 10, Freq: 937.0M, CID: 6016, LAC: 1540, 16, Freq: 938.2M, CID: 26892, LAC: 1540, 87, Freq: 952.4M, CID: 0, LAC: 49943, 109, Freq: 956.8M, CID: 43310, LAC: 49926, 119, Freq: 958.8M, CID: 43348, LAC: 49926,</pre>	<pre>GNU C++ version 6.3.0 20170221; Boost_106200; UHD 976, Freq: 925.4M, CID: 20002, LAC: 609, MCC: 980, Freq: 926.2M, CID: 63691, LAC: 609, MCC: 981, Freq: 926.4M, CID: 27745, LAC: 609, MCC: 983, Freq: 926.8M, CID: 49557, LAC: 609, MCC: 1004, Freq: 931.0M, CID: 26992, LAC: 609, MCC: 1014, Freq: 933.0M, CID: 26992, LAC: 609, MCC: 1016, Freq: 933.4M, CID: 26990, LAC: 609, MCC: 0, Freq: 935.0M, CID: 6016, LAC: 1540, MCC: 6, Freq: 936.2M, CID: 26892, LAC: 1540, MCC: 7, Freq: 936.4M, CID: 6042, LAC: 1540, MCC: 10, Freq: 937.0M, CID: 6016, LAC: 1540, MCC: 10, Freq: 938.2M, CID: 6016, LAC: 1540, MCC: 16, Freq: 938.2M, CID: 26892, LAC: 1540, MCC: 87, Freq: 952.4M, CID: 0, LAC: 49943, MCC: 119, Freq: 956.8M, CID: 43310, LAC: 49926, MCC: 122, Freq: 959.4M, CID: 43348, LAC: 49926, MCC:</pre>	<ul> <li>GNU C++ version 6.3.0 20170221; Boost_106200; UHD_003.</li> <li>976, Freq: 925.4M, CID: 20002, LAC: 609, MCC: 208, 980, Freq: 926.2M, CID: 63691, LAC: 609, MCC: 208, 981, Freq: 926.4M, CID: 27745, LAC: 609, MCC: 208, 983, Freq: 926.8M, CID: 49557, LAC: 609, MCC: 208, 1004, Freq: 931.0M, CID: 26992, LAC: 609, MCC: 208, 1014, Freq: 933.0M, CID: 26992, LAC: 609, MCC: 208, 1016, Freq: 933.4M, CID: 26990, LAC: 609, MCC: 208, 0, Freq: 935.0M, CID: 6016, LAC: 1540, MCC: 208, 6, Freq: 936.2M, CID: 26892, LAC: 1540, MCC: 208, 7, Freq: 936.4M, CID: 6042, LAC: 1540, MCC: 208, 10, Freq: 937.0M, CID: 6016, LAC: 1540, MCC: 208, 16, Freq: 938.2M, CID: 26892, LAC: 1540, MCC: 208, 87, Freq: 952.4M, CID: 0, LAC: 49943, MCC: 208, 109, Freq: 956.8M, CID: 43310, LAC: 49926, MCC: 208, 119, Freq: 958.8M, CID: 43310, LAC: 49926, MCC: 208, 122, Freq: 959.4M, CID: 43348, LAC: 49926, MCC: 208,</li> </ul>	<ul> <li>GNU C++ version 6.3.0 20170221; Boost_106200; UHD_003.009.0</li> <li>976, Freq: 925.4M, CID: 20002, LAC: 609, MCC: 208, MNC: 980, Freq: 926.2M, CID: 63691, LAC: 609, MCC: 208, MNC: 981, Freq: 926.4M, CID: 27745, LAC: 609, MCC: 208, MNC: 983, Freq: 926.8M, CID: 49557, LAC: 609, MCC: 208, MNC: 1004, Freq: 931.0M, CID: 26992, LAC: 609, MCC: 208, MNC: 1014, Freq: 933.0M, CID: 26992, LAC: 609, MCC: 208, MNC: 1016, Freq: 933.4M, CID: 26990, LAC: 609, MCC: 208, MNC: 0, Freq: 935.0M, CID: 26892, LAC: 1540, MCC: 208, MNC: 6, Freq: 936.2M, CID: 26892, LAC: 1540, MCC: 208, MNC: 7, Freq: 936.4M, CID: 6016, LAC: 1540, MCC: 208, MNC: 10, Freq: 937.0M, CID: 6016, LAC: 1540, MCC: 208, MNC: 16, Freq: 938.2M, CID: 26892, LAC: 1540, MCC: 208, MNC: 16, Freq: 938.2M, CID: 26892, LAC: 1540, MCC: 208, MNC: 16, Freq: 938.2M, CID: 43310, LAC: 49943, MCC: 208, MNC: 119, Freq: 958.8M, CID: 43310, LAC: 49926, MCC: 208, MNC: 122, Freq: 959.4M, CID: 43348, LAC: 49926, MCC: 208, MNC:</li> </ul>	<pre>GNU C++ version 6.3.0 20170221; Boost_106200; UHD_003.009.005-0-u 976, Freq: 925.4M, CID: 20002, LAC: 609, MCC: 208, MNC: 20, 980, Freq: 926.2M, CID: 63691, LAC: 609, MCC: 208, MNC: 20, 981, Freq: 926.4M, CID: 27745, LAC: 609, MCC: 208, MNC: 20, 983, Freq: 926.8M, CID: 49557, LAC: 609, MCC: 208, MNC: 20, 1004, Freq: 931.0M, CID: 26992, LAC: 609, MCC: 208, MNC: 20, 1014, Freq: 933.0M, CID: 26992, LAC: 609, MCC: 208, MNC: 20, 1016, Freq: 933.4M, CID: 26990, LAC: 609, MCC: 208, MNC: 20, 0, Freq: 935.0M, CID: 6016, LAC: 1540, MCC: 208, MNC: 1, 6, Freq: 936.2M, CID: 26892, LAC: 1540, MCC: 208, MNC: 1, 7, Freq: 936.4M, CID: 6042, LAC: 1540, MCC: 208, MNC: 1, 10, Freq: 937.0M, CID: 6016, LAC: 1540, MCC: 208, MNC: 1, 16, Freq: 938.2M, CID: 26892, LAC: 1540, MCC: 208, MNC: 1, 16, Freq: 938.2M, CID: 26892, LAC: 1540, MCC: 208, MNC: 1, 16, Freq: 937.0M, CID: 6016, LAC: 1540, MCC: 208, MNC: 1, 16, Freq: 938.2M, CID: 26892, LAC: 1540, MCC: 208, MNC: 1, 16, Freq: 938.2M, CID: 26892, LAC: 1540, MCC: 208, MNC: 1, 17, Freq: 952.4M, CID: 0, LAC: 49943, MCC: 208, MNC: 1, 19, Freq: 956.8M, CID: 43310, LAC: 49926, MCC: 208, MNC: 10, 119, Freq: 958.8M, CID: 43310, LAC: 49926, MCC: 208, MNC: 10, 122, Freq: 959.4M, CID: 43348, LAC: 49926, MCC: 208, MNC: 10,</pre>	<ul> <li>GNU C++ version 6.3.0 20170221; Boost_106200; UHD_003.009.005-0-unknow 976, Freq: 925.4M, CID: 20002, LAC: 609, MCC: 208, MNC: 20, Pwr: 980, Freq: 926.2M, CID: 63691, LAC: 609, MCC: 208, MNC: 20, Pwr: 981, Freq: 926.4M, CID: 27745, LAC: 609, MCC: 208, MNC: 20, Pwr: 983, Freq: 926.8M, CID: 49557, LAC: 609, MCC: 208, MNC: 20, Pwr: 1004, Freq: 931.0M, CID: 26992, LAC: 609, MCC: 208, MNC: 20, Pwr: 1014, Freq: 933.0M, CID: 26992, LAC: 609, MCC: 208, MNC: 20, Pwr: 1016, Freq: 933.4M, CID: 26990, LAC: 609, MCC: 208, MNC: 20, Pwr: 0, Freq: 935.0M, CID: 26990, LAC: 609, MCC: 208, MNC: 1, Pwr: 0, Freq: 936.2M, CID: 26892, LAC: 1540, MCC: 208, MNC: 1, Pwr: 7, Freq: 936.4M, CID: 6016, LAC: 1540, MCC: 208, MNC: 1, Pwr: 10, Freq: 937.0M, CID: 6016, LAC: 1540, MCC: 208, MNC: 1, Pwr: 16, Freq: 938.2M, CID: 26892, LAC: 1540, MCC: 208, MNC: 1, Pwr: 16, Freq: 938.2M, CID: 26892, LAC: 1540, MCC: 208, MNC: 1, Pwr: 16, Freq: 938.2M, CID: 26892, LAC: 1540, MCC: 208, MNC: 1, Pwr: 16, Freq: 938.2M, CID: 26892, LAC: 1540, MCC: 208, MNC: 1, Pwr: 109, Freq: 952.4M, CID: 0, LAC: 49943, MCC: 208, MNC: 1, Pwr: 109, Freq: 956.8M, CID: 43310, LAC: 49926, MCC: 208, MNC: 10, Pwr: 122, Freq: 959.4M, CID: 43348, LAC: 49926, MCC: 208, MNC: 10, Pwr: 122, Freq: 959.4M, CID: 43348, LAC: 49926, MCC: 208, MNC: 10, Pwr: 122, Freq: 959.4M, CID: 43348, LAC: 49926, MCC: 208, MNC: 10, Pwr: 122, Freq: 959.4M, CID: 43348, LAC: 49926, MCC: 208, MNC: 10, Pwr:</li> </ul>

Notez le canal ayant le plus haut niveau de puissance. Expliquez en détail tous les champs présentés ci-dessus (ARFCN, CID, LAC, etc). Vous pouvez aussi installer et utiliser gqrx au lieu de grgsm\_scanner.

9. Lancez l'analyseur de trafic avec la commande :

# wireshark -k -Y 'gsmtap && !icmp' -i lo &

Ou bien avec la commande :

# wireshark -k -f udp -Y gsmtap -i lo &

Expliquez ces commandes. Que voyez vous ?

10. Lancez la réception en temps réel :

# grgsm\_livemon &

linux; GNU C++ version 6.3.0 20170221; Boost\_106200; UHD\_003.009.005-0-unknown
gr-osmosdr 0.1.4 (0.1.4) gnuradio 3.7.10
built-in source types: file osmosdr fcd rtl rtl\_tcp uhd miri hackrf bladerf
rfspace airspy soapy redpitaya
Number of USB devices: 13
USB device 1d50:6089: 000000000000000000000806063c82540b45f match
Using HackRF One with firmware 2017.02.1

11. Réglez la fréquence sur le canal trouvé ci-dessus. Que se passe-t-il dans le terminal ? Dans l'analyseur ?



Vous devriez voir les mêmes éléments que sur l'image ci-dessus.

Les données sont reçues et écrites directement sur la sortie standard du terminal :

Number of USB devices: 13																						
USB device 1d50:6089:						00000000000000000000000000000000000000								match								
Using HackRF One with						Lth	fir	rmwa	are	2017.02.1												
59	06	1a	8f	e8	4c	f0	00	00	10	be	00	00	00	00	00	00	00	00	ff	b9	00	00
01	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b
59	06	21	00	08	29	80	02	80	79	73	62	68	17	08	29	80	02	41	20	09	58	68
15	06	21	00	01	f0	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b
49	06	1b	69	70	02	f8	02	02	61	с9	03	1e	53	65	06	b9	00	00	80	01	40	db
01	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b
4d	06	21	00	05	f4	ec	50	ed	38	17	08	29	80	02	41	20	90	74	86	23	2b	2b
55	06	22	00	cf	60	2e	10	ec	78	38	00	17	08	29	80	02	01	60	92	78	96	8b
31	06	1c	02	f8	02	02	61	65	06	b9	00	00	80	01	47	2b						
01	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b
25	06	21	00	05	f4	4a	fd	de	20	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b
2d	06	22	00	2a	f7	d4	b5	c0	60	55	38	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b

01	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b						
01	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b						
25	06	21	00	05	f4	d3	58	9a	58	23	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b
4d	06	24	00	0e	f8	91	66	4d	f9	bc	23	3d	fd	61	47	3c	fe	2b	65	83	2b	2b
49	06	03	ef	89	90	00	00	00	00	00	00	00	00	00	00	00	00	00	2h	2h	2h	2h
05	06	07	00	a0	30	0a	2e	18	99	f3	h6	30	8h	de	01	15	dh	f8	ha	12	2f	0h
15	06	21	00	01	f0	2h	2h	2h	2h	2h	2h	2h	2h	2h	2h	2h	2h	2h	2h	2h	2h	2h
	00		00	01		20	2.0	2.0	2.0		2.0	2.0	2.0	2.0	2.0		2.0	2.0	2.0	2.0	2.0	

12. Observez les données récupérées dans wireshark à l'aide des panneaux 1 et 2 :

Activities 🛛 🥖 Wireshark 🔻				Sat Sep 14, 14:29	🔂 🕶 fr 🖛 🛔 🐠 🖻 💌			
			Ca	turing from Loopback (udp)	_ = ×			
<u>File Edit View Go Capture Analy</u>	vze <u>S</u> tatistics Telephon	<u>y W</u> ireless <u>T</u> ools <u>H</u> elp						
	Q & -> & K		<u>a</u>					
smtap					Expression *			
Image           No.         Time           A0.         Time           A2.55773554         47.2.655773554           A7.2.65591235         48.2.680713554           A7.2.65591235         48.2.68071355           A8.2.68071355         55.2.84063759           55.2.84063759         55.2.84093155           55.3.117224502         55.3.117224502           55.3.117224502         55.3.3627348           56.3.117224502         56.3.3557346           56.3.355246892         53.355246892           57.3.355246892         53.355246892           58.3.55246892         54.3.55246892           59.3.355246892         54.3.55246892           50.3.55246892         54.3.55246892           50.3.55246892         54.3.55246892           59.3.55246892         54.3.55246892           50.3.55246892         54.3.55246892           50.3.55246892         54.3.55246892           50.3.55246892         54.3.55246892           50.3.55246892         54.3.55246892           50.3.55246892         54.3.55246892           50.3.55246892         54.3.55246892           50.3.55246892         54.3.55246892           50.3.551775         54.42289555	Source 127.0.0.1 127	Destination           127.0.0.1           27.0.0.1 </th <th>Protocol Length           GSMTAP           GSMTAP</th> <th>Info B1 (CCCH) (SS) S1 (CCCH) (RR) Paging Request Type 2 S1 (CCCH) (RR) Paging Request Type 1 S1 (CCCH) (RR) System Information Type 2duater S1 (CCCH) (RR) Paging Request Type 1 S1 (CCCH) (RR) Paging Request Type 2 S1 (CCCH) (RR) Paging Request Type 1 S1 (CCCH) (RR) Paging Request Type 1</th> <th>Expression •</th>	Protocol Length           GSMTAP           GSMTAP	Info B1 (CCCH) (SS) S1 (CCCH) (RR) Paging Request Type 2 S1 (CCCH) (RR) Paging Request Type 1 S1 (CCCH) (RR) System Information Type 2duater S1 (CCCH) (RR) Paging Request Type 1 S1 (CCCH) (RR) Paging Request Type 2 S1 (CCCH) (RR) Paging Request Type 1 S1 (CCCH) (RR) Paging Request Type 1	Expression •			
<ul> <li>TMSI/P-TMSI - Mobile Identi</li> <li>TMSI/P-TMSI</li> <li>TMSI/P-TMSI Value: 0x:</li> <li>TMSI/P-TMSI - Mobile Identi</li> <li>Mobile Identity - Mobile Identi</li> </ul>	ty 1 Saffa6bd ty 2 entity 3 - TMSI/P-TMSI	(0xef89166)						
000         10         00         00         00         00         00         10         00         00         00         00         00         00         10         00	0 00 00 00 08 00 45 00 7 64 7f 00 00 01 7f 00 e 42 02 04 01 00 00 22 b9 49 06 22 00 5a ff 4 0e f8 91 66 30 2b 2b	· C · C ⊕ ⊕ · d · · · · · Z · · · · Z · · · · · · ·						
<ul> <li>Ready to load or capture</li> </ul>				Packets: 1685 · Displayed:	1685 (100.0%) Profile: Default			

Détaillez tous les types de messages reçus et expliquez leur signification en vous servant des documents disponibles sur : <u>www.etsi.org</u>, <u>https://www.rfwireless-world.com</u>, <u>http://www.teletopix.org</u>.

Les usages des outils gr-gsm sont décrits ici : <u>https://github.com/ptrkrysik/gr-gsm/wiki/Usage</u>.

13. (optionnel) Si vous avez une distribution Stretch, il faudra compiler gr-gsm en suivant les instructions données sur cette page :

https://osmocom.org/projects/gr-gsm/wiki/Installation

14. (optionnel) Si vous avez la clé de session de l'algo de chiffrement A5, vous pouvez décoder les parties chiffrées :

https://github.com/ptrkrysik/gr-gsm/wiki/Usage:-Decoding-How-To