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 choisissez 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

Found HackRF board 0:
USB descriptor string: 0000000000000000a06063c82540b45f
Board ID Number: 2 (HackRF One)
Firmware Version: 2017.02.1
Part ID Number: 0xa000cb3c 0x005f435e
Serial Number: 0x00000000 0x00000000 0xa06063c8 0x2540b45f
```

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

linux; GNU C++ version 6.3.0 20170221; Boost_106200; UHD_003.009.005-0-unknown
ARFCN:  976, Freq:  925.4M, CID: 20002, LAC:   609, MCC: 208, MNC:  20, Pwr: -56
ARFCN:  980, Freq:  926.2M, CID: 63691, LAC:   609, MCC: 208, MNC:  20, Pwr: -59
ARFCN:  981, Freq:  926.4M, CID: 27745, LAC:   609, MCC: 208, MNC:  20, Pwr: -56
ARFCN:  983, Freq:  926.8M, CID: 49557, LAC:   609, MCC: 208, MNC:  20, Pwr: -49
ARFCN: 1004, Freq:  931.0M, CID: 26992, LAC:   609, MCC: 208, MNC:  20, Pwr: -37
ARFCN: 1014, Freq:  933.0M, CID: 26992, LAC:   609, MCC: 208, MNC:  20, Pwr: -36
ARFCN: 1016, Freq:  933.4M, CID: 26990, LAC:   609, MCC: 208, MNC:  20, Pwr: -43
ARFCN:    0, Freq:  935.0M, CID:  6016, LAC:  1540, MCC: 208, MNC:   1, Pwr: -50
ARFCN:    6, Freq:  936.2M, CID: 26892, LAC:  1540, MCC: 208, MNC:   1, Pwr: -47
ARFCN:    7, Freq:  936.4M, CID:  6042, LAC:  1540, MCC: 208, MNC:   1, Pwr: -54
ARFCN:   10, Freq:  937.0M, CID:  6016, LAC:  1540, MCC: 208, MNC:   1, Pwr: -41
ARFCN:   16, Freq:  938.2M, CID: 26892, LAC:  1540, MCC: 208, MNC:   1, Pwr: -60
ARFCN:   87, Freq:  952.4M, CID:     0, LAC: 49943, MCC: 208, MNC:  10, Pwr: -57
ARFCN:  109, Freq:  956.8M, CID: 43310, LAC: 49926, MCC: 208, MNC:  10, Pwr: -46
ARFCN:  119, Freq:  958.8M, CID: 43310, LAC: 49926, MCC: 208, MNC:  10, Pwr: -43
ARFCN:  122, Freq:  959.4M, CID: 43348, LAC: 49926, MCC: 208, MNC:  10, Pwr: -59
```

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 &
```

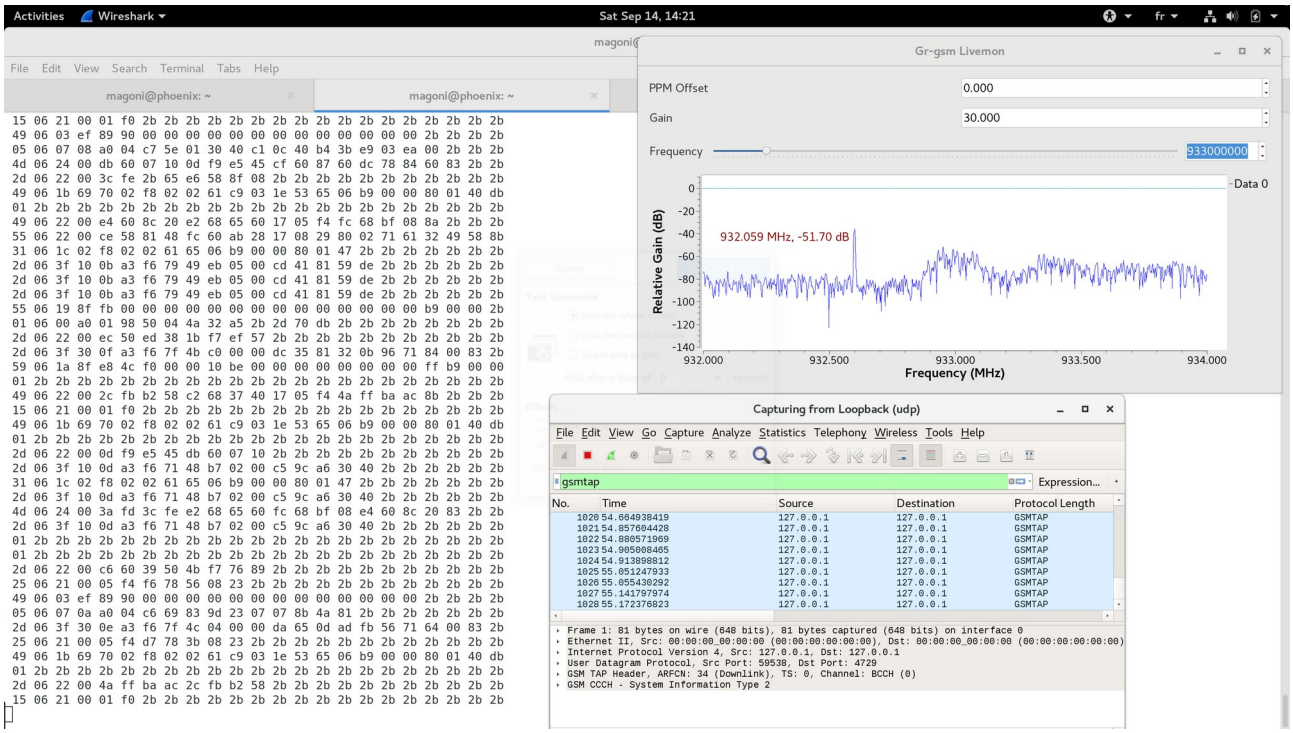
Expliquez ces commandes. Que voyez vous ?

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: 0000000000000000a06063c82540b45f 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 ?



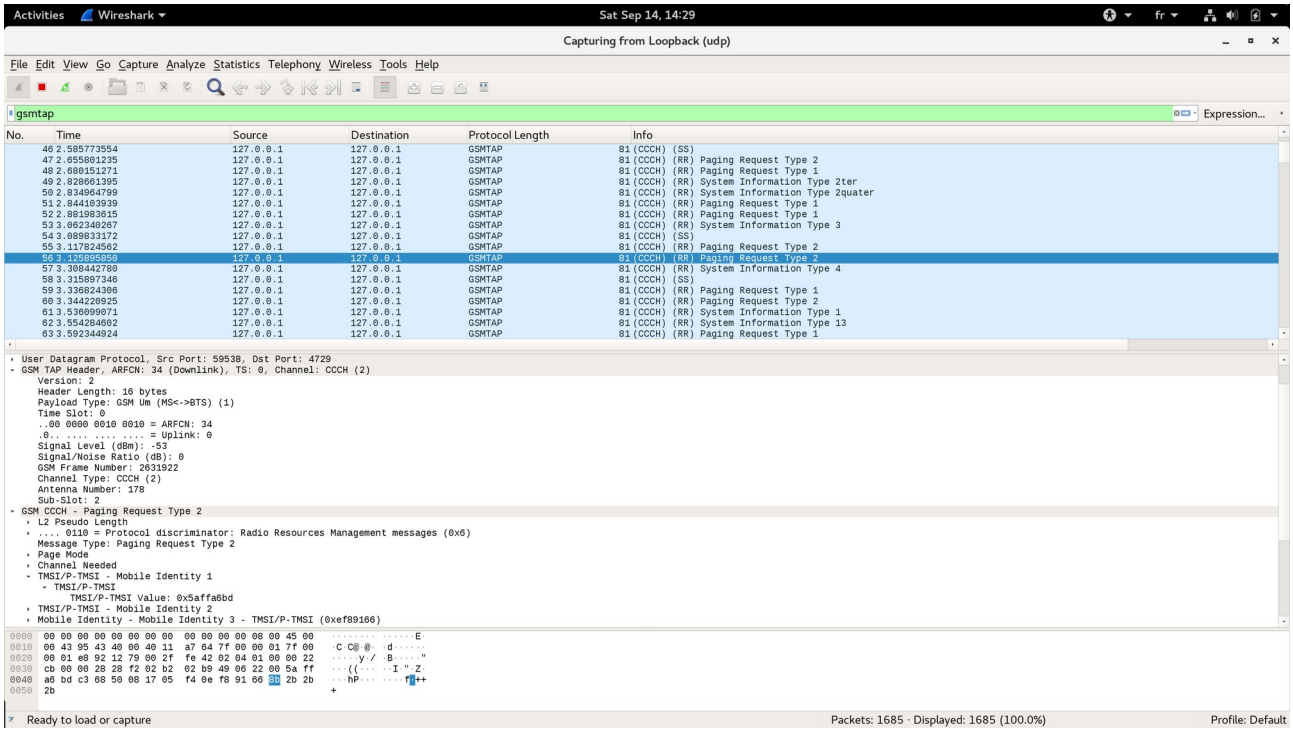
Vous devriez voir les mêmes éléments que sur l'image ci-dessus.

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

```
...
Number of USB devices: 13
USB device 1d50:6089: 0000000000000000a06063c82540b45f match
Using HackRF One with firmware 2017.02.1
 59 06 1a 8f e8 4c f0 00 00 10 be 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
 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 c9 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 2b 2b 2b 2b 2b 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 2b 2b 2b 2b
01 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 d3 58 9a 58 23 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 2b 2b 2b 2b
05 06 07 00 a0 30 0a 2e 18 99 f3 b6 30 d8 de 01 15 db f8 ba 12 2f 0b
15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
...
```

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



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

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

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