Examen “Transmissions Numériques” – L3

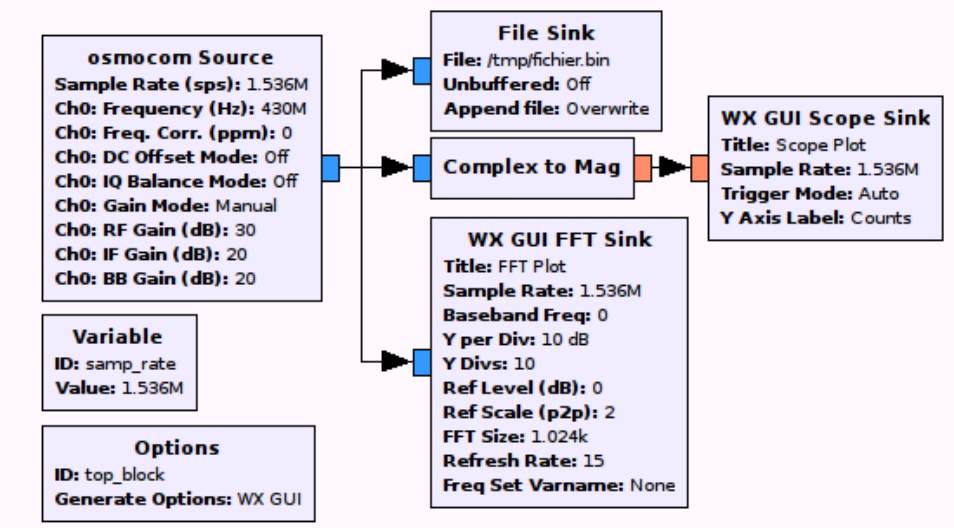
J.-M Friedt, 20 mai 2015

1 Transmission radiofréquence

Un schéma bloc trivial est utilisé pour enregistrer un fichier binaire contenant les coefficients I et Q d'un récepteur radiofréquence sans fréquence intermédiaire. Il est rappelé que dans cette architecture de récepteur, le signal radiofréquence reçu par une antenne est amplifié, mélangé avec un oscillateur radiofréquence local programmable pour ramener le signal dans la bande de fréquences d'échantillonnage du convertisseur analogique-numérique, et deux signaux sont numérisés simultanémenent, le premier dit en identité (I) et le second en quadrature (Q).

1. Comment calculer l'amplitude du signal radiofréquence, connaissant les coefficients I et Q ?
2. Lors du tracé du spectre du signal (domaine de Fourier), comment est gradué l'axe des abscisses ? Noter que le signal complexe n'est pas nécessairement symétrique par rapport à la fréquence nulle et que les fréquences négatives doivent aussi être considérées.

Dans un premier temps, un signal est synthétisé par un générateur radiofréquence, et émis sur une antenne sur une porteuse de 430 MHz (choisie arbitrairement). Le fichier `http://jmfriedt.sequanux.org/exam_TN2015/fichier1.bin` contient un tel enregistrement obtenu selon le schéma de traitement ci-dessous.



On pourra au choix charger ce fichier dans `gnuradio-companion` pour l'analyser, ou charger les coefficients complexes I/Q dans GNU/Octave au moyen de la fonction `read_complex_binary` [1] qui prend en argument le nom du fichier à charger.

3. Sachant que la fréquence d'échantillonnage est de $32 \times 48 = 1536$ kHz, comment définir sous GNU/Octave (ou Matlab) l'axe du temps pour dater chaque échantillon ?
4. Noter que les oscillateurs locaux de l'émetteur et du récepteur sont légèrement décalés : de quelle fréquence sont-ils décalés ? Comment compenser ce décalage une fois l'acquisition achevée et le fichier enregistré ?
5. Quelle est la nature de la modulation qui a été appliquée au signal radiofréquence ? À quelle fréquence l'information aurait été transmise si au lieu de synthétiser un signal périodique nous avions encodé des bits dans ce mode de modulation ?
6. Est-ce que ce mode de modulation est sensible au décalage en fréquence entre émetteur et récepteur ? Justifier.
7. L'opérateur a bougé autour du récepteur au cours de l'enregistrement : quelle est la faiblesse de ce mode de modulation qui s'observe sur le fichier enregistré ? Justifier.

Étant désormais familier avec la lecture et l'analyse d'un fichier contenant des signaux I/Q issus d'un récepteur radiofréquence, nous nous proposons d'étudier une télécommande d'ouverture de portail de garage. La photographie d'un tel émetteur radiofréquence – commercialisé par la société italienne Openout S.r.l – est proposée sur la Fig. 1.

On note en particulier sur la gauche de l'émetteur 10 interrupteurs (DIP-switch) pouvant prendre deux états, ON ou OFF. Une seconde rangée de 4 interrupteurs est visible sur la partie supérieure du circuit. Deux boutons poussoirs

1. `http://gnuradio.org/redmine/projects/gnuradio/repository/revisions/253018c6cdb114f5662a2d7ba8ed748c6e68e3a7/entry/gnuradio-core/src/utils/read_complex_binary.m`, dont on trouvera aussi une copie sur le site contenant les fichiers à analyser.

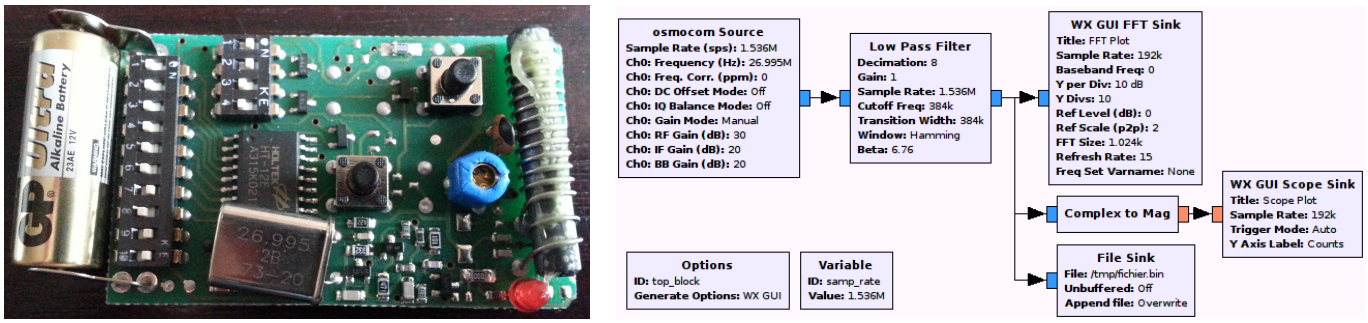


FIGURE 1 – Photographie du circuit émetteur d'un dispositif pour ouvrir à distance un portail de garage, et schéma d'acquisition `gnuradio-companion` des signaux émis.

permettent d'activer deux fonctionnalités du récepteur (par exemple, l'ouverture de deux portails). Nous allons enregistrer le signal radiofréquence émis autour de 26,995 MHz (fréquence du résonateur à quartz visible au dessus du composant de référence Holtek HT-12E [2]) en modifiant l'état des interrupteurs. Divers fichiers sont disponibles dans le répertoire `http://jmfriedt.sequanux.org/exam_TN2015/` avec des noms comportant des séquences de 1 et de 0 et l'extension `.bin`. Le nom de chaque fichier correspond à l'état des 10 interrupteurs, 1 signifiant ON et 0 pour OFF. Lors de chaque mesure, nous avons appuyé pendant environ 1 seconde sur le premier bouton poussoir, puis 1 seconde se le second bouton poussoir.

8. Analyser le contenu de ces fichiers, et indiquer l'encodage observé pour transmettre le code d'ouverture de chaque portail.
9. Comment se nomme le mode d'encodage transmis ? Comment est-il relié au mode de modulation du signal synthétisé dans la première partie de cet exercice ?
10. Proposer le mode d'encodage des valeurs de 1 et de 0 lors de la transmission.
11. Quel est le débit de communication (en bits/seconde) ?
12. Compte tenu du nombre de bits transmis et de la durée du message, combien de temps faut-il pour émettre toutes les combinaisons possibles de bits (*i.e.*, pour attaque de force brute générant tous les codes possibles ?)
13. Qu'en déduisez vous sur le niveau de sécurité de ce type d'émetteur radiofréquence ?

Ce sujet a été inspiré par l'article de D. Bodor intitulé "SDR et télécommande – qui peut entrer dans mon garage en pratique ?" dans le numéro 6 du magazine Hackable (2015).

2 Transmission compatible internet

Le fichier `http://jmfriedt.sequanux.org/exam_TN2015/log.tcpdump` a été acquis lors d'une transaction entre deux ordinateurs connectés à internet pour établir un échange de fichiers. Nous nous proposons d'analyser ces échanges.

Pour ce faire, on chargera le fichier dans `wireshark` ou on en affichera le contenu au moyen de `tcpdump` dont l'option `-r log.tcpdump` permet de charger un fichier enregistré au préalable au lieu de capturer les paquets en cours de transmission.

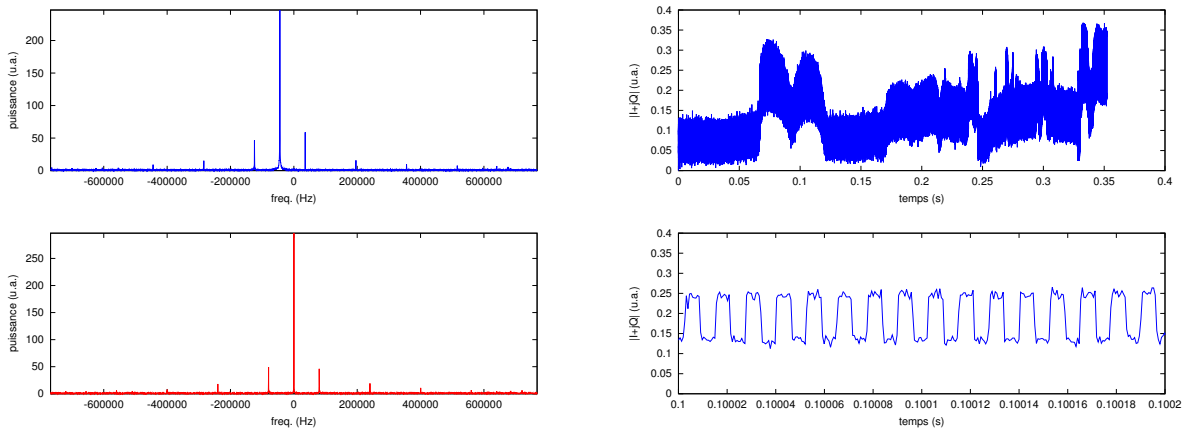
14. Rappeler la différence entre adresse MAC et adresse IP. Quel protocole effectue la relation entre ces deux informations ? Fournir le paquet représentant la notification de cette information dans le log.
15. Quelle est l'adresse IP des interlocuteurs ?
16. Quelle est l'adresse MAC des interlocuteurs ?
17. Quel protocole a été mis en œuvre au cours de ces échanges ? on pourra s'inspirer du port sur lequel se font les échanges pour identifier le protocole (il peut être utile de consulter pour cela le format des paquets TCP, par exemple décrits à `http://en.wikipedia.org/wiki/Transmission_Control_Protocol`).
18. Trouver le RFC qui décrit ce protocole : de quel RFC s'agit-il ?
19. Un second port est ouvert au cours des transactions : lequel ?
20. Quelle est la nature de la transaction ? Quelle information a été échangée par l'utilisateur des deux ordinateurs ?
21. Quel est l'identifiant (login) de l'utilisateur ?
22. Quel est son mot de passe ?
23. Quelle solution proposer pour que ces deux informations ne soient pas transmises en clair sur internet ?

2. `http://www.holtek.com/pdf/consumer/2_12ev120.pdf`

3 Solutions

3.1 Émetteur pour ouverture de portail de garage

1. module $= \sqrt{I^2+Q^2} = |I+jQ|$
2. Pour une fréquence d'échantillonnage f_e, la transformée de Fourier s'étend de $-f_e/2$ à $+f_e/2$. Sous GNU/Octave, l'axe des fréquences est défini par `freq=linspace(-fe/2,fe/2,N);` pour une transformée de Fourier sur `N` points (`fft(data,N);`).
3. les échantillons sont acquis tous les $1/f_e$ avec $f_e = 1,536$ MHz. Dans ce cas les N points acquis sont distribués à intervalles de temps régulier entre la date 0 et $N/1,536$ μs. Sous GNU/Octave, on définira `fe=1.536e6;temps=[0:1/fe:N/fe];` et on notera que le vecteur résultant comporte `N+1` points donc on retire le dernier élément : `temps=temps(1:end-1);`. Alternativement, `temps=linspace(0,N/fe,N);`.
4. Le tracé de la transformée de Fourier du signal présente un pic significatif autour de 44393.4 Hz (identifier cette fréquence nécessite de convenablement graduer l'axe des abscisses du spectre).

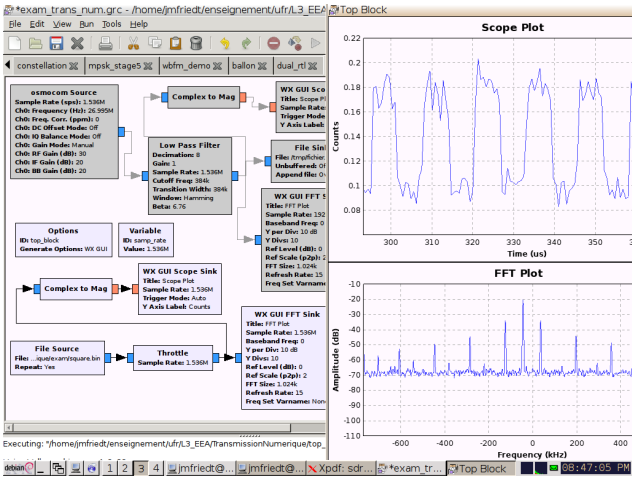


Le code GNU/Octave permettant d'afficher ces figures est :

```
clear;close
set (0,"defaultaxesfontname","Helvetica")
fe=48000*32;
d=read_complex_binary('square.bin');

freq=linspace(-fe/2,fe/2,4096); % length(d));
temps=[0:1/fe:length(d)/fe];temps=temps(1:end-1)';

subplot(211);plot(freq,fftshift(abs(fft(d,4096))));
xlabel('freq. (Hz)');ylabel('puissance (u.a.)');axis tight

monsin=exp(j*temps*2*pi*44393.4);
signal=d.*monsin;
subplot(212);plot(freq,fftshift(abs(fft(signal,4096))),'r')
xlabel('freq. (Hz)');ylabel('puissance (u.a.)');axis tight
figure;subplot(211); plot(temps,abs(d-d(1)),'b')
xlabel('temps (s)');ylabel('|I+jQ| (u.a.)')
subplot(212); plot(temps,abs(d-d(1)),'b');xlim([0.1 0.1002])
xlabel('temps (s)');ylabel('|I+jQ| (u.a.)')
```

Ce code contient aussi la solution pour compenser le décalage de fréquences en post-traitement : ce décalage de fréquence Δf entre les deux oscillateurs se compense par multiplication du signal reçu par une version numérique de l'oscillateur local (NCO). Pour ce faire, il fallait une définition correcte de l'axe du temps (question précédente) afin de générer le signal du NCO $\exp(j \cdot 2\pi\Delta f \cdot t)$.

La solution `gnuradio-companion` s'obtient en ouvrant le fichier (`File Source`), en pensant à insérer le block `Throttle` qui cadence la lecture, et en affichant en formats oscilloscope et transformée de Fourier, le signal :

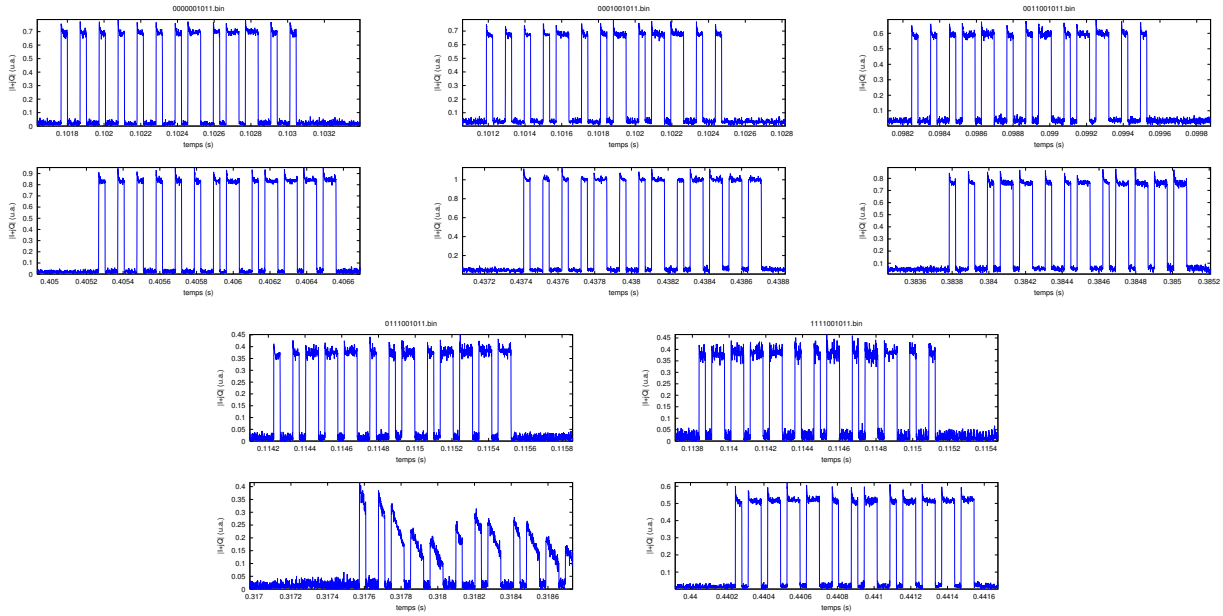


Dans ce cas, le `Frequency Xlating FIR Filter` fournit la solution pour transposer la fréquence de façon logicielle afin de compenser l'écart entre les oscillateurs de l'émetteur et du récepteur.

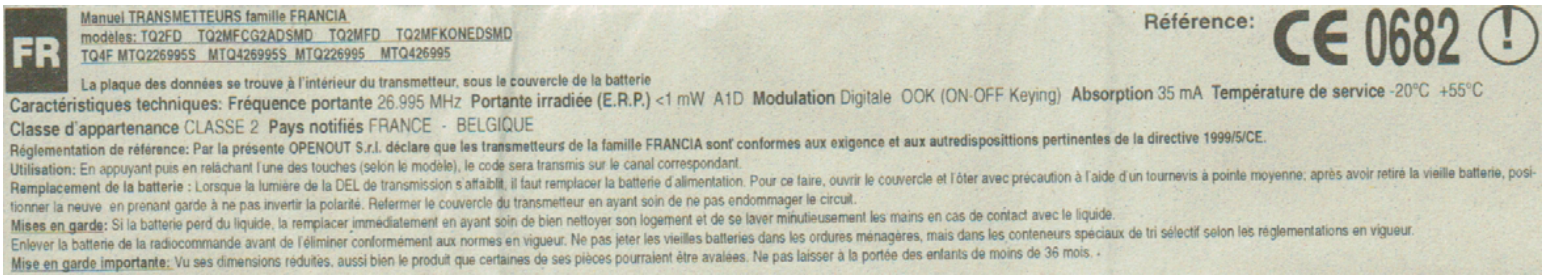
5. Un signal périodique du signal est observé sur l'amplitude du signal (tracé du module du signal $I + jQ$. Il s'agit donc d'une modulation d'amplitude. L'intervalle de temps entre deux transitions d'état est de 100 μs, donc un débit de 10 kbauds. Cette information se retrouve dans le domaine spectral par la position des raies de modulation de part et d'autre de la porteuse.
6. La modulation d'amplitude est peu sensible aux décalages de fréquence entre émetteur et récepteur. En effet le filtre passe bas présente une fréquence de coupure bien plus faible que la fréquence de porteuse. Formellement, si a et b sont deux séquences de complexe, alors $|a \cdot b| = |a| \cdot |b|$ et si $b = \exp(j2\pi\Delta f \cdot t)$, alors $|b| = 1$ et $|a \cdot b| = |a|$.
7. Il s'agit d'une modulation d'amplitude, très sensible au bilan de liaison entre émetteur et récepteur et interférences dues aux chemins multiples. Ceci explique les fluctuations observées sur l'enregistrement long (350 ms) pendant lequel l'environnement entre émetteur et récepteur a varié. Les signaux transmis restent observables tout au long de l'enregistrement et les fluctuations lentes pourraient être éliminées par un filtre passe-haut.
8. Le contenu des fichiers s'affiche sous forme des figures ci-dessous par le code GNU/Octave suivant :

```
clear;close
set (0,"defaultaxesfontname","Helvetica")
fe=48000*32;
nom=dir('./[01]*.bin');
for k=1:length(nom)
  d=read_complex_binary(nom(k).name);d=abs(d);
  if (k==2) d=d(1:675000);endif
  if (k==4) d=d(1:491000);endif
  temps=[0:1/fe:length(d)/fe];temps=temps(1:end-1)';
  u=find(d>min(d)+0.2);
  subplot(211);plot(temps([u(1)-200:u(1)+2500]),d([u(1)-200:u(1)+2500]));axis tight
  xlabel('temps␣(s)');ylabel('|I+jQ|␣(u.a.)');eval(['title(''',nom(k).name,''');']);
  subplot(212);plot(temps([u(end)-2500:u(end)+200]),d([u(end)-2500:u(end)+200]));axis tight
  xlabel('temps␣(s)');ylabel('|I+jQ|␣(u.a.)')
  eval(['print␣-depsc␣',nom(k).name,'.eps']);
end
```

pour donner



9. L'observation du module $|I + jQ|$ des signaux acquis montre qu'il s'agit d'une modulation On/Off – ou OOK (ou Morse) – dans laquelle la valeur de chaque bit est indiquée par la durée de l'impulsion émise. OOK est le cas asymptotique de la modulation d'amplitude avec un coefficient de 100% : aucun signal pour 0 et un signal présent pour 1. La notice confirme ce mode d'encodage :


Manuel TRANSMETTEURS famille FRANCIA
modèles: TQ2FD TQ2MFCG2ADSMD TQ2MFD TQ2MFKONEDSMD
TQ4F MTQ226995S MTQ426995S MTQ226995 MTQ426995
FR
Référence:
CE 0682
La plaque des données se trouve à l'intérieur du transmetteur, sous le couvercle de la batterie
Caractéristiques techniques: Fréquence portante 26.995 MHz Portante irradiée (E.R.P.) <1 mW A1D Modulation Digitale OOK (ON-OFF Keying) Absorption 35 mA Température de service -20°C +55°C
Classe d'appartenance CLASSE 2 Pays notifiés FRANCE - BELGIQUE
Réglementation de référence: Par la présente OPENOUT S.r.l. déclare que les transmetteurs de la famille FRANCIA sont conformes aux exigence et aux autredispositions pertinentes de la directive 1999/5/CE.
Utilisation: En appuyant puis en relâchant l'une des touches (selon le modèle), le code sera transmis sur le canal correspondant.
Remplacement de la batterie : Lorsque la lumière de la DEL de transmission s'affaiblit, il faut remplacer la batterie d'alimentation. Pour ce faire, ouvrir le couvercle et l'ôter avec précaution à l'aide d'un tournevis à pointe moyenne; après avoir retiré la vieille batterie, positionner la neuve en prenant garde à ne pas invertir la polarité. Refermer le couvercle du transmetteur en ayant soin de ne pas endommager le circuit.
Mises en garde: Si la batterie perd du liquide, la remplacer immédiatement en ayant soin de bien nettoyer son logement et de se laver minutieusement les mains en cas de contact avec le liquide.
Enlever la batterie de la radiocommande avant de l'éliminer conformément aux normes en vigueur. Ne pas jeter les vieilles batteries dans les ordures ménagères, mais dans les conteneurs spéciaux de tri sélectif selon les réglementations en vigueur.
Mise en garde importante: Vu ses dimensions réduites, aussi bien le produit que certaines de ses pièces pourraient être avalées. Ne pas laisser à la portée des enfants de moins de 36 mois.

10. Par rapport au codage sélectionné sur les interrupteurs, nous constatons que le message commence par un 0 (ou OFF), suivi du code des interrupteurs sur 10 bits, avec impulsion longue pour On et courte pour Off, pour finalement se conclure par 1100 pour le premier bouton (graphiques du haut) et 1111 pour le second bouton (graphiques du bas).
11. Les bits sont transmis au rythme de 160±5 points ou 9600±300 bits/s.
12. Deux trames successives sont séparées de 3825 points environ, soit 2,5 ms. Il y a 13 bits transmis dont le premier semble toujours à 0, donc 12 bits soient 4096 combinaisons possibles. Il faut donc $4096 \times 2,5$ ms ou 10,25 secondes pour tester toutes les combinaisons possibles.
13. Il semble donc que le niveau de sécurité soient très médiocre, voir inexistant.

3.2 Analyser une séquence de communication par ftp

14. L'adresse MAC est un identifiant lié au matériel : elle est unique à chaque interface. L'adresse IP est un identifiant logiciel associé au site auquel est connecté l'ordinateur : elle est unique à chaque connexion. La correspondance est fournie par le protocole ARP (Address Resolution Protocol).

```
# tcpdump -r ftp_sqnx_success.tcpdump -XX | grep ARP
reading from file ftp_sqnx_success.tcpdump, link-type EN10MB (Ethernet)
14:28:55.026929 ARP, Request who-has 192.168.0.1 tell 192.168.0.11, length 28
14:28:55.027929 ARP, Reply 192.168.0.1 is-at 30:46:9a:5b:1c:d4 (oui Unknown), length 46
```

Le premier paquet est émis (au niveau du protocole ethernet) comme un *broadcast* puisque le destinataire est d'adresse MAC ff :ff :ff :ff :ff :ff. La réponse est quant à elle ciblée vers l'émetteur.

15. L'émetteur des signaux est 192.168.0.11, le routeur est 192.168.0.1, et le destinataire est 188.165.36.56. Lorsqu'on s'intéresse uniquement à la couche IP, l'affichage se fait par `# tcpdump -r ftp_sqnx_success.tcpdump -X | less` afin de s'affranchir de la couche ethernet.

16. Les adresses MAC des interlocuteurs sont prises en charge par le couche ethernet donc il faut afficher les données enregistrées par `# tcpdump -r ftp_sqnx_success.tcpdump -XX | less`. L'émetteur est cc :7e :e7 :5f :cf :6e et le routeur est 30 :46 :9a :5b :1c :d4. Ce sont les deux interlocuteurs visibles puisque une fois émis, les paquets circulent derrière le routeur.
17. La séquence qui a permis la capture par `tcpdump -w log.tcpdump` est

```
$ ftp sequanux.org
Connected to sequanux.org.
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 2 of 50 allowed.
220-Local time is now 13:28. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (sequanux.org:jmfriedt):
331 User jmfriedt OK. Password required
Password:
230 OK. Current directory is /home/jmfriedt
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> asc
200 TYPE is now ASCII
ftp> passive
Passive mode on.
ftp> get t.c
local: t.c remote: t.c
227 Entering Passive Mode (188,165,36,56,19,164)
150 Accepted data connection
226-File successfully transferred
226 0.000 seconds (measured here), 1.15 Mbytes per second
59 bytes received in 0.00 secs (528.5980 kB/s)
ftp> quit
221-Goodbye. You uploaded 0 and downloaded 1 kbytes.
221 Logout.
```

    Il s'agit donc d'un échange de fichier par le protocole FTP (File Transfer Protocol). Nous aurions pu identifier ce protocole en observant que le port ouvert pour la transmission TCP/IP est le numéro 21, qui est assigné au protocole ftp dans `/etc/services` : le port accédé dans TCP est indiqué par 0015 (hexadécimal).
18. Le protocole du service FTP est décrit par le RFC959 (`https://www.ietf.org/rfc/rfc959.txt` tel que obtenu en recherchant File Transfer Protocol sur `https://www.ietf.org/`). Nous apprenons dans ce RFC que les commandes `USER` transmettent l'identifiant et `PASS` le mot de passe.
19. Le second port ouvert pour les transactions – en plus du port 21 qui sert aux commandes – est le port 5028. Nous le voyons soit par le décodage proposé par l'option `-XX` de `tcpdump` (`vm1.sequanux.org.5028`) soit en analysant les paquets TCP/IP (le port se trouve dans le paquet IP – on rappelle que la norme OSI impose la hiérarchie ethernet-IP-TCP et ce n'est que le niveau d'abstraction le plus élevé qui introduit le notion de port) : le port d'origine des messages issus lors du transfert de fichiers de sequanux.org est 5028. Finalement, on retrouve cette information dans la réponse à la commande PASV qui passe le serveur en mode passif : 19,164 indique que le port utilisé est $19 \times 256 + 164 = 5028$.
20. Le fichier échangé contient un programme en C qui se contente de définir un tableau d'entiers puis d'en incrémenter un élément qui n'existe pas afin d'induire une erreur d'accès à un segment mémoire erroné (*segmentation fault*).
21. `tcpdump -r ftp_sqnx_success.tcpdump -A | grep USER` nous enseigne que l'identifiant est `jmfriedt` ...
22. ... et son mot de passe est (`tcpdump -r ftp_sqnx_success.tcpdump -A | grep PASS`) `mot_de_passe`.
23. Exploiter un protocole encrypté permet d'éviter de sonder de façon automatique les transactions. RFC2228 propose une solution exploiant le cryptage SSL dans FTPS, et ce afin explicitement de résoudre le problème de transfert en clair du login et mot de passe : "The File Transfer Protocol (FTP) ... uses usernames and passwords passed in cleartext to authenticate clients to servers (via the USER and PASS commands)". SFTP propose des fonctonnalités proches de FTP mais selon un protocole très différent. Sous Debian/GNU Linux, le paquet `ftp-ssl` fournit un client sécurisé. Le serveur Pure-FTPd supporte l'encryption (TLS – Transport Layer Security).