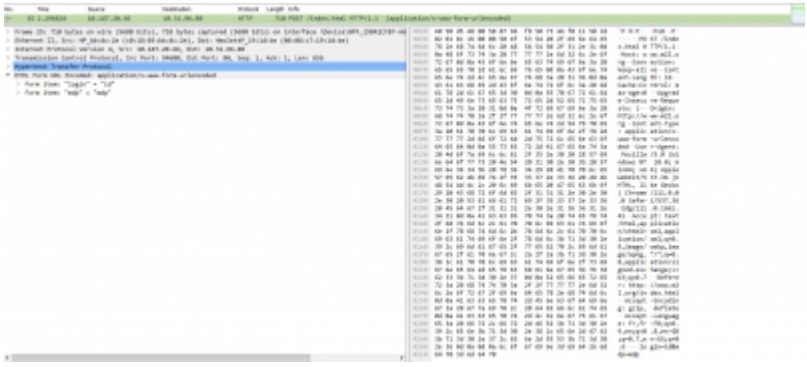
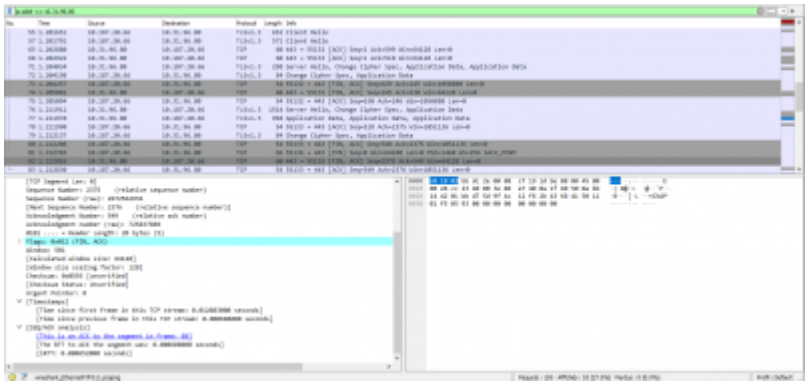
MISSION 7 : Chiffrement des communications HTTP et FTP avec SSL / TLS

I) Rappel sur le chiffrement SSL / TLS

Regardons une trame HTTP venant d'un formulaire sur le site www.m2l.org. En utilisant WireShark, nous pouvons voir les données du formulaire transmises en POST :



Maintenant regardons un même échange de formulaire mais avec le protocole HTTPS :



II) HTTPS

Pour pouvoir activer le chiffrement SSL, nous avons besoin de télécharger le paquet OpenSSL :

```
apt update
apt install openssl
```

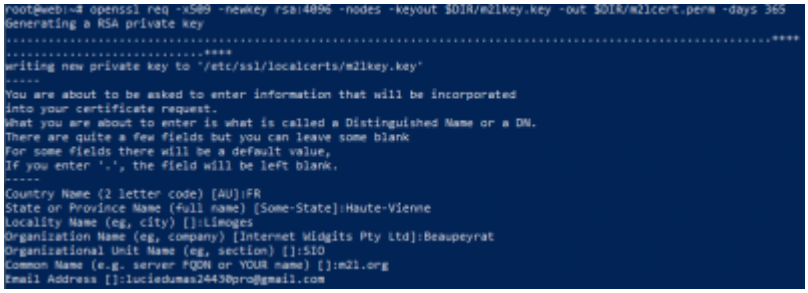
Ensuite, nous créons le répertoire qui accueillera la clé de chiffrement ainsi que le certificat :

```
mkdir /etc/ssl/localcerts
```

Nous créons ensuite la variable qui sera utilisée dans la commande de génération de clé et de certificats :

```
DIR=/etc/ssl/localcerts
openssl req -x509 -newkey rsa:4096 -nodes -keyout $DIR/m2lkey.key -out
$DIR/m2lcert.pem -days 365
```

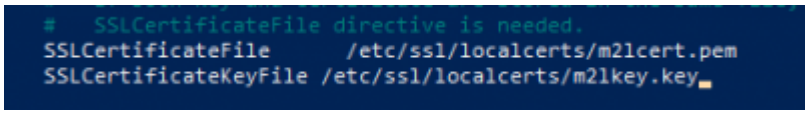
Nous entrons ensuite les différentes informations nécessaires à la création de la clé et du certificat :



Nous activons ensuite le Vhost SSL par défaut ainsi que le module SSL pour apache :

```
a2ensite default-ssl
a2enmod ssl
```

Nous modifions ensuite les chemins du Vhost SSL par défaut (/etc/apache2/sites-available/default-ssl.conf) :

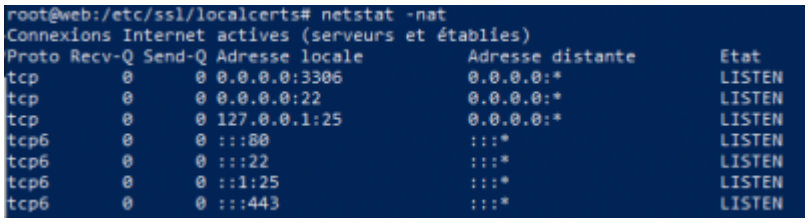


Nous redémarrons ensuite le service apache :

```
systemctl restart apache2
```

Nous regardons ensuite que le port 443 soit en train d'écouter :

```
netstat -nat
```



Nous ajoutons enfin à nos VirtualHosts les directives concernant le port 443 :

/etc/apache2/sites-available/www.m2l.org.conf :

```
<VirtualHost *:80>
     ServerName m2l.org
     ServerAlias www.m2l.org
     DocumentRoot /home/htdocs/m2l.org/www
  ErrorLog /var/log/apache2/www-error.log
     CustomLog /var/log/apache2/www-access.log combined
     <Directory /home/htdocs/m2l.org/www>
          Require all granted
     </Directory>
</VirtualHost>

<VirtualHost *:443>
     ServerName m2l.org
     ServerAlias www.m2l.org
     DocumentRoot /home/htdocs/m2l.org/www
  ErrorLog /var/log/apache2/www-error.log
     CustomLog /var/log/apache2/www-access.log combined
     <Directory /home/htdocs/m2l.org/www>
          Require all granted
     </Directory>
     SSLCertificateFile     /etc/ssl/localcerts/m2lcert.pem
     SSLCertificateKeyFile  /etc/ssl/localcerts/m2lkey.key
</VirtualHost>
```

/etc/apache2/sites-available/intranet.m2l.org.conf :

```
<VirtualHost *:80>
     ServerName m2l.org
     ServerAlias intranet.m2l.org
     DocumentRoot /home/htdocs/m2l.org/intranet
  ErrorLog /var/log/apache2/intranet-error.log
     CustomLog /var/log/apache2/intranet-access.log combined
     <Directory /home/htdocs/m2l.org/intranet>
          Require all granted
          AllowOverride All
     </Directory>
</VirtualHost>

<VirtualHost *:443>
     ServerName m2l.org
     ServerAlias intranet.m2l.org
     DocumentRoot /home/htdocs/m2l.org/intranet
  ErrorLog /var/log/apache2/intranet-error.log
```

```
     CustomLog /var/log/apache2/intranet-access.log combined
     <Directory /home/htdocs/m2l.org/intranet>
          Require all granted
          AllowOverride All
     </Directory>
     SSLCertificateFile     /etc/ssl/localcerts/m2lcert.pem
     SSLCertificateKeyFile  /etc/ssl/localcerts/m2lkey.key
</VirtualHost>
```

/etc/apache2/sites-available/extranet.m2l.org.conf :

```
<VirtualHost *:80>
     ServerName m2l.org
     ServerAlias extranet.m2l.org
     DocumentRoot /home/htdocs/m2l.org/extranet
  ErrorLog /var/log/apache2/extranet-error.log
     CustomLog /var/log/apache2/extranet-access.log combined
     <Directory /home/htdocs/m2l.org/extranet>
          Require all granted
     </Directory>
</VirtualHost>

<VirtualHost *:443>
     ServerName m2l.org
     ServerAlias extranet.m2l.org
     DocumentRoot /home/htdocs/m2l.org/extranet
  ErrorLog /var/log/apache2/extranet-error.log
     CustomLog /var/log/apache2/extranet-access.log combined
     <Directory /home/htdocs/m2l.org/extranet>
          Require all granted
     </Directory>
     SSLCertificateFile     /etc/ssl/localcerts/m2lcert.pem
     SSLCertificateKeyFile  /etc/ssl/localcerts/m2lkey.key
</VirtualHost>
```

/etc/apache2/sites-available/wiki.m2l.org.conf :

```
<VirtualHost *:80>
     ServerName m2l.org
     ServerAlias wiki.m2l.org
     DocumentRoot /home/htdocs/m2l.org/wiki
  ErrorLog /var/log/apache2/wiki-error.log
     CustomLog /var/log/apache2/wiki-access.log combined
     <Directory /home/htdocs/m2l.org/wiki>
          Require all granted
     </Directory>
```

```
</VirtualHost>

<VirtualHost *:443>
     ServerName m2l.org
     ServerAlias wiki.m2l.org
     DocumentRoot /home/htdocs/m2l.org/wiki
  ErrorLog /var/log/apache2/wiki-error.log
     CustomLog /var/log/apache2/wiki-access.log combined
     <Directory /home/htdocs/m2l.org/wiki>
          Require all granted
     </Directory>
     SSLCertificateFile     /etc/ssl/localcerts/m2lcert.pem
     SSLCertificateKeyFile  /etc/ssl/localcerts/m2lkey.key
</VirtualHost>
```

Nous redémarrons le service apache2

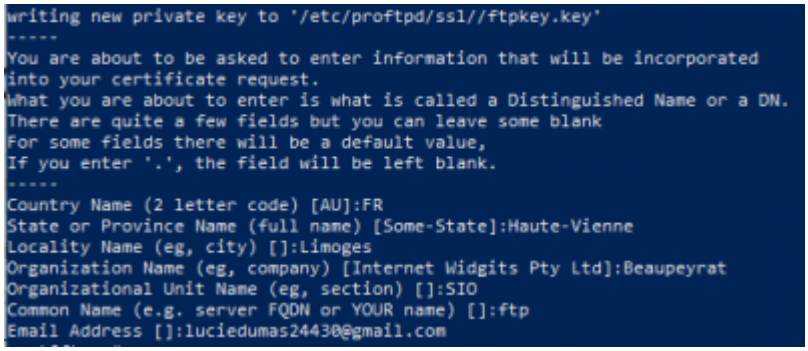
III) FTPS

Nous allons maintenant appliquer ce principe au protocole FTP. Pour ce faire, nous allons créer dans le conteneur ftp le répertoire qui accueillera la clé de chiffrement ainsi que le certificat :

```
mkdir /etc/proftpd/ssl/
```

Nous générons la clé et le certificat SSL :

```
DIR=/etc/proftpd/ssl/
openssl req -x509 -newkey rsa:4096 -nodes -keyout $DIR/ftpkey.key -out
$DIR/ftpcert.pem -days 365
```



Nous allons ensuite modifier le fichier /etc/proftpd/proftpd.conf pour décommenter la ligne incluant le TLS :

```
# This is used for FTPS connections
#
Include /etc/proftpd/tls.conf
```

Nous allons maintenant éditer le fichier /etc/proftpd/tls.conf pour modifier les lignes suivantes :

- TLSEngine (activer/désactiver TLS)
- TLSLog (logguer les connexions chiffrées dans un fichier à part)
- TLSRSACertificateFile (chemin vers le certificat)
- TLSRSACertificateKeyFile (chemin vers la clé)
- TLSOptions (voir http://www.proftpd.org/docs/contrib/mod_tls.html)

```
<IfModule mod_tls.c>
TLSEngine                               on
TLSLog                                  /var/log/proftpd/tls.log
#TLSProtocol                            SSLv23
#
# Server SSL certificate. You can generate a self-signed certificate using
# a command like:
#
# openssl req -x509 -newkey rsa:1024 \
#          -keyout /etc/ssl/private/proftpd.key -out /etc/ssl/certs/proftpd.crt \
#          -nodes -days 365
#
# The proftpd.key file must be readable by root only. The other file can be
# readable by anyone.
#
# chmod 0600 /etc/ssl/private/proftpd.key
# chmod 0640 /etc/ssl/private/proftpd.key
#
TLSRSACertificateFile                   /etc/proftpd/ssl/ftpcert.pem
TLSRSACertificateKeyFile                /etc/proftpd/ssl/ftpkey.key
```

Nous devons ensuite activer les modules TLS. Pour cela, nous modifions le fichier /etc/proftpd/modules.conf :

```
# Install proftpd-mod-crypto to use this module for TLS/SSL support.
LoadModule mod_tls.c
```

Nous installons ensuite les paquets nécessaires :

```
apt install proftpd-mod-crypto
```

Nous redémarrons ensuite le conteneur :

```
systemctl restart proftpd
```

Nous allons maintenant faire les modifications nécessaires sur le logiciel Filezilla client :