1 Subject

I've try many time, and I've reproduced same situation at the end « not working ». Also I've two Elock, with the second one I've only test the out of the box kit (with the official first version of the software, and it still not working).

But after several investigations, I found the default was coming from a bad IP setting (regarding the DNS).

In order to help others, I've make this quick documentation to explain the full configuration of the ELock. Most of step has been taken from the official documentation and several contributions from the forum: http://www.elektor-labs.com/project/elektor-chip-e-lock-reference-project-130499130280.13916.html

Yoann Darche

yoannd _@_ Hotmail _dot_ com

2 Generating SSL Keys and Certficate

2.1 Context

All the process has been done on a workstation with Window 7 x64. I've carefully deactivate any Virtual Network, Wifi and Bluetooth Interface. Only the main INet interface is still up and running.

2.2 Preparing OpenSSL

- Downloading the latest version : http://slproweb.com/products/Win32OpenSSL.html
    - I've selected Win64 OpenSSL v1.0.2 (16 Mo)
- Downloading the Microsoft Visual Studio 2008 redistrib : http://www.microsoft.com/en-us/download/confirmation.aspx?id=29
- Launch installation in the folder D:_APP_\OpenSSL
- Create a directory : D:\ElkOpenSSL
- Backup the template D:_APP_\OpenSSL\bin\openssl.cnf to D:_APP_\OpenSSL\bin_REF_openssl.cnf

2.3 OpenSLL config

Following the « network-configuration.pdf », §2.1, I've updated the D:\OpenSSL\openssl.cnf file as highlighted in red :

```
#
# OpenSSL example configuration file.
# This is mostly being used for generation of certificate requests.
#

# This definition stops the following lines choking if HOME isn't
# defined.
HOME                  = D:/ElkOpenSSL
RANDFILE              = $ENV::HOME/.rnd

# Extra OBJECT IDENTIFIER info:
#oid_file             = $ENV::HOME/.oid
oid_section           = new_oids

# To use this configuration file with the "-extfile" option of the
# "openssl x509" utility, name here the section containing the
# X.509v3 extensions to use:
# extensions          =
# (Alternatively, use a configuration file that has only
# X.509v3 extensions in its main [= default] section.)

[ new_oids ]

# We can add new OIDs in here for use by 'ca', 'req' and 'ts'.
# Add a simple OID like this:
# testoid1=1.2.3.4
# Or use config file substitution like this:
# testoid2=${testoid1}.5.6

# Policies used by the TSA examples.
tsa_policy1 = 1.2.3.4.1
tsa_policy2 = 1.2.3.4.5.6
tsa_policy3 = 1.2.3.4.5.7

####################################################################
[ ca ]
default_ca     = CA_default          # The default ca section

####################################################################
[ CA_default ]

dir            = D:/ElkOpenSSL              # Where everything is kept
certs          = $dir/certs         # Where the issued certs are kept
crl_dir        = $dir/crl           # Where the issued crl are kept
database       = $dir/index.txt     # database index file.
#unique_subject       = no                  # Set to 'no' to allow creation of
                                     # several ctificates with same subject.
new_certs_dir  = $dir/newcerts              # default place for new certs.

certificate    = $dir/cacert.pem     # The CA certificate
serial         = $dir/serial         # The current serial number
crlnumber      = $dir/crlnumber      # the current crl number
                                     # must be commented out to leave a V1 CRL
crl            = $dir/crl.pem               # The current CRL
private_key    = $dir/private/cakey.pem# The private key
RANDFILE       = $dir/private/.rand  # private random number file

x509_extensions       = usr_cert            # The extentions to add to the cert

# Comment out the following two lines for the "traditional"
# (and highly broken) format.
name_opt       = ca_default          # Subject Name options
cert_opt       = ca_default          # Certificate field options

[... The rest of the file has not been changed ...]
```

2.4 Preparing the file system

- Creation of the folder D:\ElkOpenSSL\private
- Creation of the folder D:\ElkOpenSSL\newcerts
- Create a text file D:\ElkOpenSSL\index.txt

- Create a text file D:\ElkOpenSSL\serial that contains one row with the string 1000

```
D:\ElkOpenSSL>echo 1000 > serial
```

2.4.1 Check of the OpenSSL version:

```
D:\ElkOpenSSL>set OPENSSL_CONF=D:\ElkOpenSSL\openssl.cfg
D:\ElkOpenSSL>D:\_APP_\OpenSSL\bin\openssl.exe version
OpenSSL 1.0.2 22 Jan 2015
```

2.5 Generating the main certificate

```
D:\ElkOpenSSL>D:\_APP_\OpenSSL\bin\openssl.exe req -new -x509 -days 1000 -extensions v3_ca -
keyout private/cakey.pem -out cacert.pem

Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
....................................+++
.....................................................+++
writing new private key to 'private/cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:Toulouse
Locality Name (eg, city) []:Toulouse
Organization Name (eg, company) [Internet Widgits Pty Ltd]:NA
Organizational Unit Name (eg, section) []:NA
Common Name (e.g. server FQDN or YOUR name) []:NA
Email Address []:NA@NA.NA

D:\ElkOpenSSL>
```

And the following file has been created:

```
D:\ElkOpenSSL>dir
12/03/2015  18:17             1 024 .rnd
12/03/2015  18:18             1 350 cacert.pem

D:\ElkOpenSSL>dir .\private
12/03/2015  18:18             1 834 cakey.pem
```

2.6 Generating the Certificate and Key for Server side

2.6.1 Generating the Server request

```
D:\ElkOpenSSL>D:\_APP_\OpenSSL\bin\openssl.exe req -new -nodes -out ISLserver-req.pem -keyout
private/ISLserver-key.pem
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
......................................+++
....................................+++
writing new private key to 'private/ISLserver-key.pem'
-----
You are about to be asked to enter information that will be incorporated
```

```
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:Toulouse
Locality Name (eg, city) []:Toulouse
Organization Name (eg, company) [Internet Widgits Pty Ltd]:NA
Organizational Unit Name (eg, section) []:NA
Common Name (e.g. server FQDN or YOUR name) []:NA
Email Address []:NA@NA.NA

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:***
An optional company name []:
```

And the following file has been created :

```
D:\ElkOpenSSL>dir
12/03/2015  18:28             1 050 ISLserver-req.pem


D:\ElkOpenSSL>dir .\private
12/03/2015  18:28             1 704 ISLserver-key.pem
```

2.6.2 Generating the certificate

```
D:\ElkOpenSSL>D:\_APP_\OpenSSL\bin\openssl.exe ca -out ISLserver-cert.pem -infiles ISLserver-
req.pem
Using configuration from D:\ElkOpenSSL\openssl.cfg
Loading 'screen' into random state - done
Enter pass phrase for D:/ElkOpenSSL/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: Mar 12 17:47:32 2015 GMT
            Not After : Mar 11 17:47:32 2016 GMT
        Subject:
            countryName               = FR
            stateOrProvinceName       = Toulouse
            organizationName          = NA
            organizationalUnitName    = NA
            commonName                = NA
            emailAddress              = NA@NA.NA
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                FB:99:F8:0A:1E:DD:B6:0B:2B:10:A1:7A:8A:B3:41:11:9F:FA:EC:0A
            X509v3 Authority Key Identifier:
                keyid:D2:C3:A2:7E:AA:9D:34:B0:A7:61:66:17:09:D4:10:FE:CA:98:5B:84

Certificate is to be certified until Mar 11 17:47:32 2016 GMT (365 days)
Sign the certificate? [y/n]:y
```

```
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

And the following file has been created:

```
D:\ElkOpenSSL>dir
12/03/2015  18:47              4 507 ISLserver-cert.pem
D:\ElkOpenSSL>dir .\newcerts
12/03/2015  18:47              4 507 1000.pem
```

2.7 Generating the Certificate and Key for Client side

2.7.1 Generating the Client request and Certificate

```
D:\ElkOpenSSL>D:\_APP_\OpenSSL\bin\openssl.exe req -new -nodes -out ISLclient-req.pem -keyout
private/ISLclient-key.pem

Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.+++
......................................+++
writing new private key to 'private/ISLclient-key.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:Toulouse
Locality Name (eg, city) []:Toulouse
Organization Name (eg, company) [Internet Widgits Pty Ltd]:NA
Organizational Unit Name (eg, section) []:NA
Common Name (e.g. server FQDN or YOUR name) []:NA
Email Address []:NA@NA.COM

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:***
An optional company name []:

D:\ElkOpenSSL>D:\_APP_\OpenSSL\bin\openssl.exe ca -out ISLclient-cert.pem -infiles ISLclient-
req.pem
Using configuration from D:\ElkOpenSSL\openssl.cfg
Loading 'screen' into random state - done
Enter pass phrase for D:/ElkOpenSSL/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4097 (0x1001)
        Validity
            Not Before: Mar 12 17:53:28 2015 GMT
            Not After : Mar 11 17:53:28 2016 GMT
        Subject:
            countryName               = FR
            stateOrProvinceName       = Toulouse
            organizationName          = NA
            organizationalUnitName    = NA
            commonName                = NA
            emailAddress              = NA@NA.COM
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                45:07:50:3A:CF:7F:91:7A:71:8C:30:2B:71:72:40:F2:8C:07:B2:CC
            X509v3 Authority Key Identifier:
                keyid:D2:C3:A2:7E:AA:9D:34:B0:A7:61:66:17:09:D4:10:FE:CA:98:5B:84

Certificate is to be certified until Mar 11 17:53:28 2016 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

The following file has been created:

```
D:\ElkOpenSSL>dir
12/03/2015  18:53             1 024 .rnd
12/03/2015  18:46             1 350 cacert.pem
12/03/2015  18:53               175 index.txt
12/03/2015  18:53                21 index.txt.attr
12/03/2015  18:47                21 index.txt.attr.old
12/03/2015  18:47                87 index.txt.old
12/03/2015  18:53             4 508 ISLclient-cert.pem
12/03/2015  18:53             1 050 ISLclient-req.pem
12/03/2015  18:47             4 507 ISLserver-cert.pem
12/03/2015  18:47             1 050 ISLserver-req.pem
12/03/2015  18:53    <DIR>          newcerts
12/03/2015  17:42            10 852 openssl.cfg
12/03/2015  18:52    <DIR>          private
12/03/2015  18:53                 5 serial
12/03/2015  18:47                 5 serial.old
              13 File(s)         24 655 bytes
D:\ElkOpenSSL>dir .\private
12/03/2015  18:46             1 834 cakey.pem
12/03/2015  18:53             1 708 ISLclient-key.pem
12/03/2015  18:47             1 708 ISLserver-key.pem
               3 File(s)          5 250 bytes
D:\ElkOpenSSL>dir .\newcerts
12/03/2015  18:47             4 507 1000.pem
12/03/2015  18:53             4 508 1001.pem
               2 File(s)          9 015 bytes
```

3 Network setup of the Elock

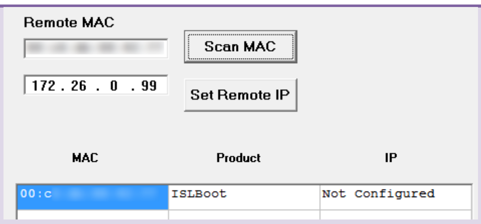
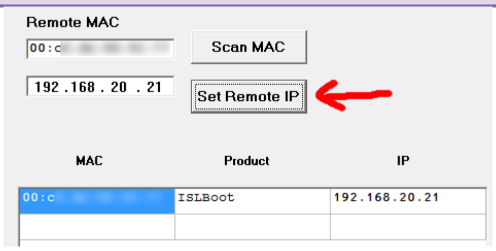
Following the document « network-configuration.pdf » and the thread: http://www.elektor-labs.com/contribution/how-to-reinstall-firmware.14225.html

3.1 Resetting the firmware

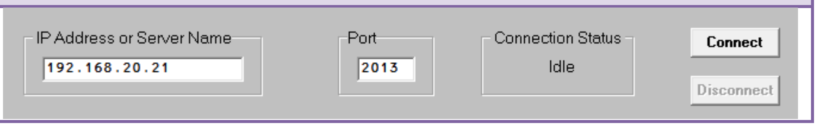
Step	Result
Disconnect the board from power.	OK
Connect pins 1-2 on jumper JP3.	OK
Power the board. Wait three or four seconds.	OK
Disconnect pins 1-2 on jumper JP3.	OK

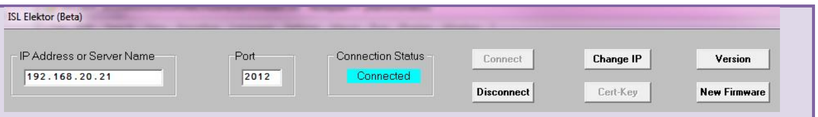
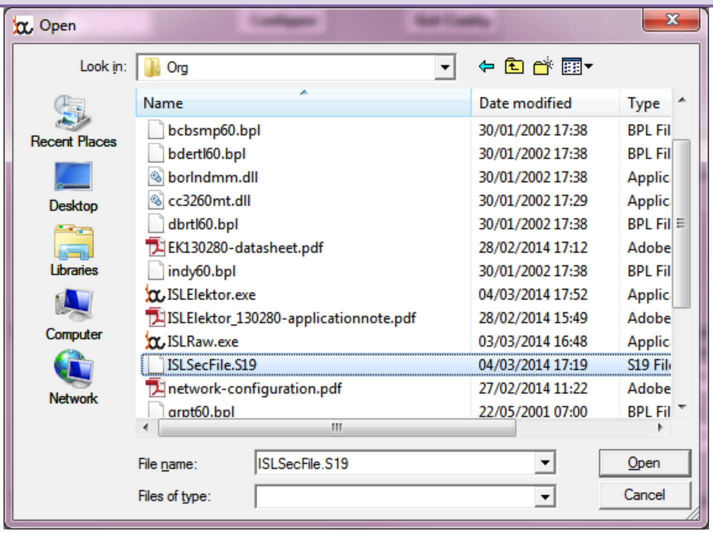
Disconnect the board from power.	OK
Connect pins 2-3 on jumper JP3.	OK
Power the board. Wait three or four seconds	OK
Disconnect pins 2-3 on jumper JP3.	OK
Disconnect the board from power.	OK
Connect the RJ-45 cable.	OK
Power the board.	The light is on and not blinking. Now, the chip is empty. We can begin to upload the firmware. ⇨ OK

3.2 Set the card IP address

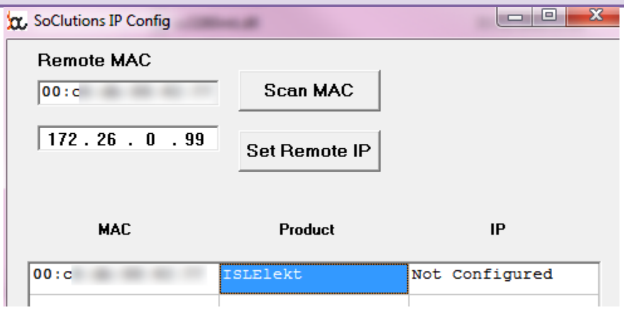
Step	**Result**
Execute ISLRaw with Admin rights. Be sure the IP address belongs to the network the e-Lock board is connected to.	
Wait some seconds for the IP connection to settle down.	
Click on "Scan MAC" button.	 Remote MAC [redacted] 172 . 26 . 0 . 99 MAC Product IP 00:c[redacted] ISLBoot Not configured ⇨ The e-Lock MAC address would appear in the device list as "ISLBoot" and "not configured". ⇨ The card has been detected.
Re-check the IP address, select the device to be configured and click "Set remote IP"	 Remote MAC 00:c[redacted] 192 .168 . 20 . 21 MAC Product IP 00:c[redacted] ISLBoot 192.168.20.21 ⇨ The e-Lock has been updated ⇨ The board's light must be blinking fast.
Close ISLRaw.	⇨ OK

3.3 Upload the firmware (original one)

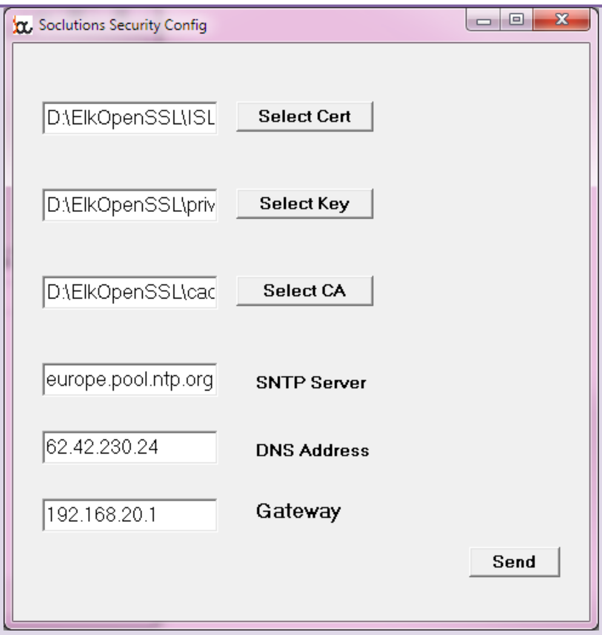
Step	**Result**
Execute ISLElektor.	
Enter the IP fixed on previous step.	 IP Address or Server Name: 192.168.20.21 Port: 2013 Connection Status: Idle

Click "Connect" button	 ISL Elektor (Beta) IP Address or Server Name: 192.168.20.21 Port: 2012 Connection Status: Connected Connect Disconnect Change IP Cert-Key Version New Firmware ⇨ After few seconds, "port" would be "2012" and there would be a blue tag saying "connected". The board's light is blinking fast. ⇨ OK
Click "New firmware" button.	 Open Look in: Org Name | Date modified | Type bcbsmp60.bpl | 30/01/2002 17:38 | BPL Fil bdertl60.bpl | 30/01/2002 17:38 | BPL Fil borlndmm.dll | 30/01/2002 17:38 | Applic cc3260mt.dll | 30/01/2002 17:29 | Applic dbrtl60.bpl | 30/01/2002 17:38 | BPL Fil EK130280-datasheet.pdf | 28/02/2014 17:12 | Adobe indy60.bpl | 30/01/2002 17:38 | BPL Fil ISLElektor.exe | 04/03/2014 17:52 | Applic ISLElektor_130280-applicationnote.pdf | 28/02/2014 15:49 | Adobe ISLRaw.exe | 03/03/2014 16:48 | Applic ISLSecFile.S19 | 04/03/2014 17:19 | S19 Fil network-configuration.pdf | 27/02/2014 11:22 | Adobe qrpt60.bpl | 22/05/2001 07:00 | BPL Fil File name: ISLSecFile.S19 Files of type: Recent Places Desktop Libraries Computer Network Open Cancel ⇨ In the File Open dialog, select the encrypted .S19 file ⇨ The tag turns yellow and should say "Transfer..."
Once the transfer ends, the connection is reset and ISLElektor app is closed automatically	⇨ OK
	The firmware is loaded now, and the board is in the "factory state". From now on, the board is as you received it first time.

3.4 Setting the keys

Step	**Result**
Run again ISLRaw as admin	Remember to have antivirus, firewalls, anti-malware, etc, disconnected
After several seconds, click "Scan MAC".	 SoClutions IP Config Remote MAC 00:c[redacted] 172 . 26 . 0 . 99 MAC | Product | IP 00:c[redacted] | ISLElekt | Not Configured ⇨ The e-Lock MAC address would appear in the device list as "ISLElekt" and "not configured". ⇨ The card has been detected.

Select device and click "Set remote IP".
Don’t forget to set the correct IP address before click on the “Set Remote IP” button
Proceed as indicated in 1.3 of Network Configuration manual.
DON'T FORGET to test the DNS and the Gateway IP address. Both must be valid



Soclutions Security Config

D:\ElkOpenSSL\ISL Select Cert

D:\ElkOpenSSL\priv Select Key

D:\ElkOpenSSL\cac Select CA

europe.pool.ntp.org SNTP Server

62.42.230.24 DNS Address

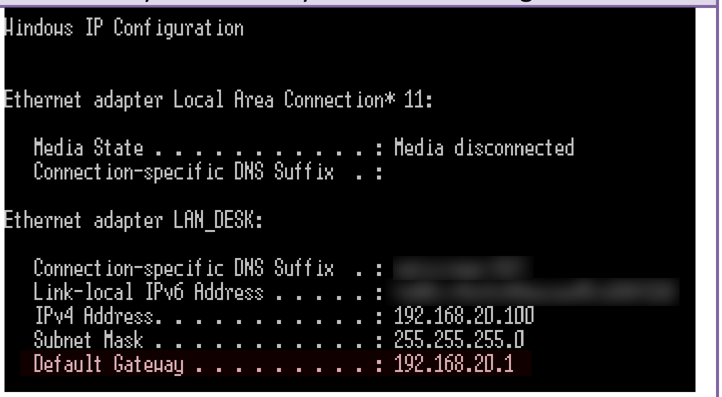
192.168.20.1 Gateway

Send

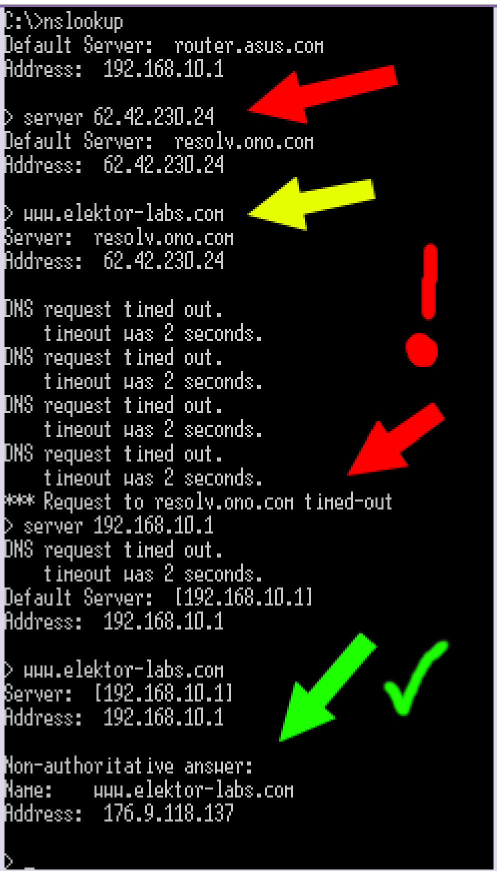
Server Cert	D:\ElkOpenSSL\ISLserver-cert.pem
Sever Key	D:\ElkOpenSSL\private\ ISLserver-key.pem
Server CA	D:\ElkOpenSSL\cacert.pem

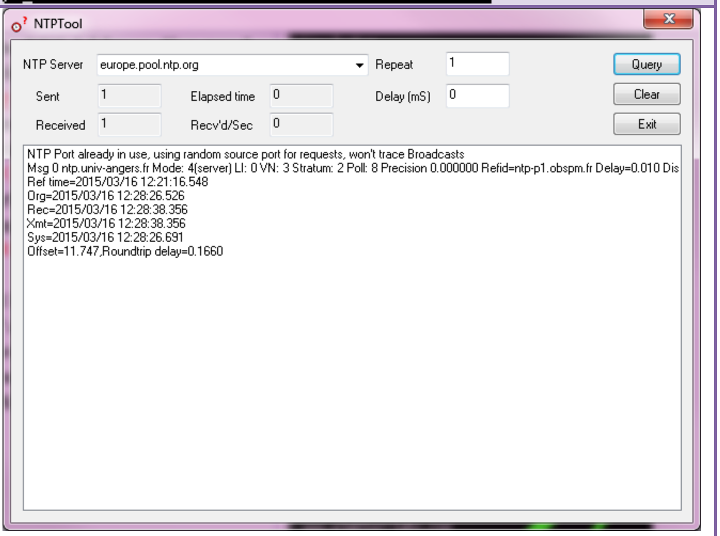
Then modify the Gateway as the local configuration.

Find the gateway. In my case I’ve use the default gate of my computer that is on the same network : “ipconfig”



```
Windows IP Configuration


Ethernet adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter LAN_DESK:

   Connection-specific DNS Suffix  . : [redacted]
   Link-local IPv6 Address . . . . . : [redacted]
   IPv4 Address. . . . . . . . . . . : 192.168.20.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.20.1
```

Testing the DNS Address, I've used the following command :
`nslookup`
In order to fix a server to use, enter the following commande :
`server <Ip>`
The to perform a test juste enter a domaine name like :
`www.elektor-labs.com`
 	
In my test I've found that the default IP address set in the dialog box, not works for me. So I've replaced with my local network default DNS.
	

Testing the NTP Server. **To test the NTP Server I've downloaded this utility :** http://www.ntp-time-server.com/ntp-server-tool.html	 ⇨ OK
Click on the "Send" button	⇨ OK
Close the application	⇨ OK

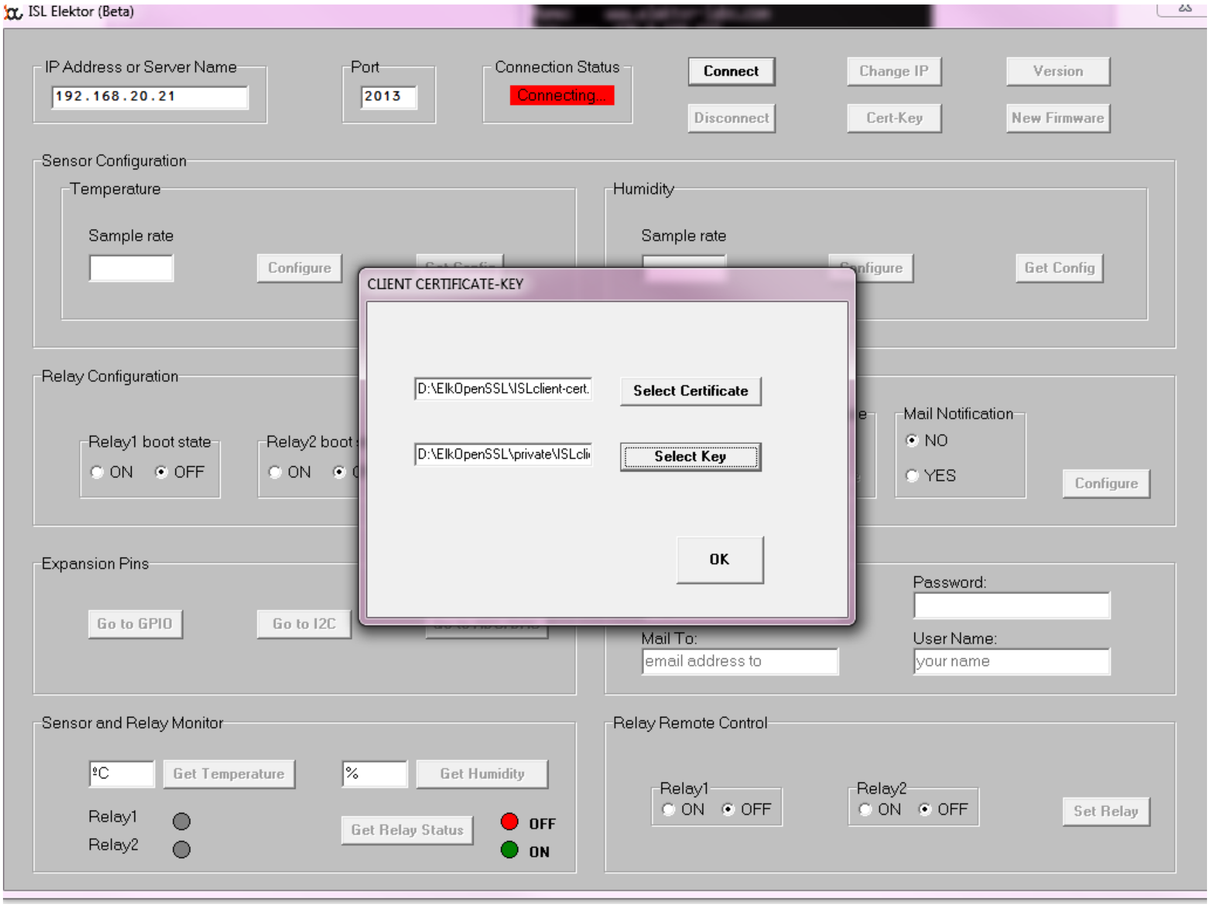
```
C:\>nslookup
Default Server:  router.asus.com
Address:  192.168.10.1

> server 62.42.230.24
Default Server:  resolv.ono.com
Address:  62.42.230.24

> www.elektor-labs.com
Server:  resolv.ono.com
Address:  62.42.230.24

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to resolv.ono.com timed-out
> server 192.168.10.1
DNS request timed out.
    timeout was 2 seconds.
Default Server:  [192.168.10.1]
Address:  192.168.10.1

> www.elektor-labs.com
Server:  [192.168.10.1]
Address:  192.168.10.1

Non-authoritative answer:
Name:    www.elektor-labs.com
Address:  176.9.118.137

> _
```

NTP Server: europe.pool.ntp.org
Repeat: 1
Sent: 1
Elapsed time: 0
Delay (mS): 0
Received: 1
Recv'd/Sec: 0

```
NTP Port already in use, using random source port for requests, won't trace Broadcasts
Msg 0 ntp.univ-angers.fr Mode: 4(server) LI: 0 VN: 3 Stratum: 2 Poll: 8 Precision 0.000000 Refid=ntp-p1.obspm.fr Delay=0.010 Dis
Ref time=2015/03/16 12:21:16.548
Org=2015/03/16 12:28:26.526
Rec=2015/03/16 12:28:38.356
Xmt=2015/03/16 12:28:38.356
Sys=2015/03/16 12:28:26.691
Offset=11.747,Roundtrip delay=0.1660
```

4 Lauching ISLElektor to connect

Launch the software ISLElektor, set the IP address then click on Connect



ISL Elektor (Beta) [redacted]

IP Address or Server Name: 192.168.20.21

Port: 2013

Connection Status: Connecting...

CLIENT CERTIFICATE-KEY

D:\ElkOpenSSL\ISLclient-cert.

D:\ElkOpenSSL\private\ISLcli

Mail Notification: ● NO ○ YES

Relay1 boot state: ○ ON ● OFF

Relay2 boot: ○ ON ●

Mail To: email address to

Password:

User Name: your name

Relay1 ●

Relay2 ●

● OFF

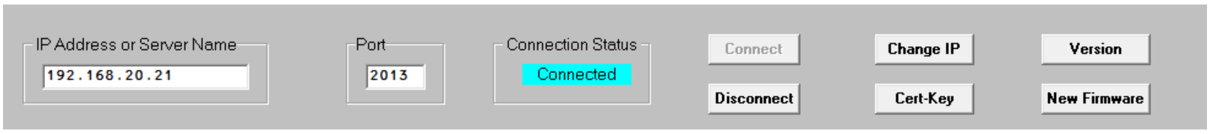
● ON

Relay Remote Control — Relay1: ○ ON ● OFF; Relay2: ○ ON ● OFF

Now you can enter the client key in the dialog box :

Server Cert	D:\ElkOpenSSL\ISLclient-cert.pem
Sever Key	D:\ElkOpenSSL\private\ ISLclient-key.pem

Then click OK, After few seconds (around 10 in my case) :



IP Address or Server Name: 192.168.20.21

Port: 2013

Connection Status: Connected