

*****Draft*****

Crypto-Socket
Using AraratSnyapse Library
05/27/20

*****Draft*****

A connection from RaspBian to Ultibo System "telnet 192.168.1.245 5050".

The initial values were below.

MyKey: AnsiString = '1234567890123456'; {Must be 16, 24 or 32 bytes}

MyIV: AnsiString = 'My Secret IV';

MyAAD: AnsiString = 'My Extra Secret AAD';

MyData: AnsiString = 'The quick brown fox jumps over the lazy dog.The quick brown fox jumps over the lazy dog.';

when the string below is sent to the Ultibo System

412345678901234567890123456789012:My Secret IV:My Extra Secret AAD:The quick brown
The quick brown The quick brown The quick brown The quick brown The quick brown
The delimiter is :
MyKey 12345678901234567890123456789012
MyIV My Secret IV
MyAAD My Extra Secret AAD
MyData The quick brown The quick brown The quick brown The quick brown The quick brown
The quick brown

The results are written to file test0527.txt

tftp 192.168.1.245
tftp> binary
tftp> get test0527.txt
Received 366 bytes in 0.0 seconds
tftp> quit

File Edit Tabs Help

12345678901234567890123456789012

My Secret IV

My Extra Secret AAD

The quick brown The quick brown The quick brown The quick brown The quick brown

The quick brown

The quick brown The quick brown The quick brown The quick brown The quick brown

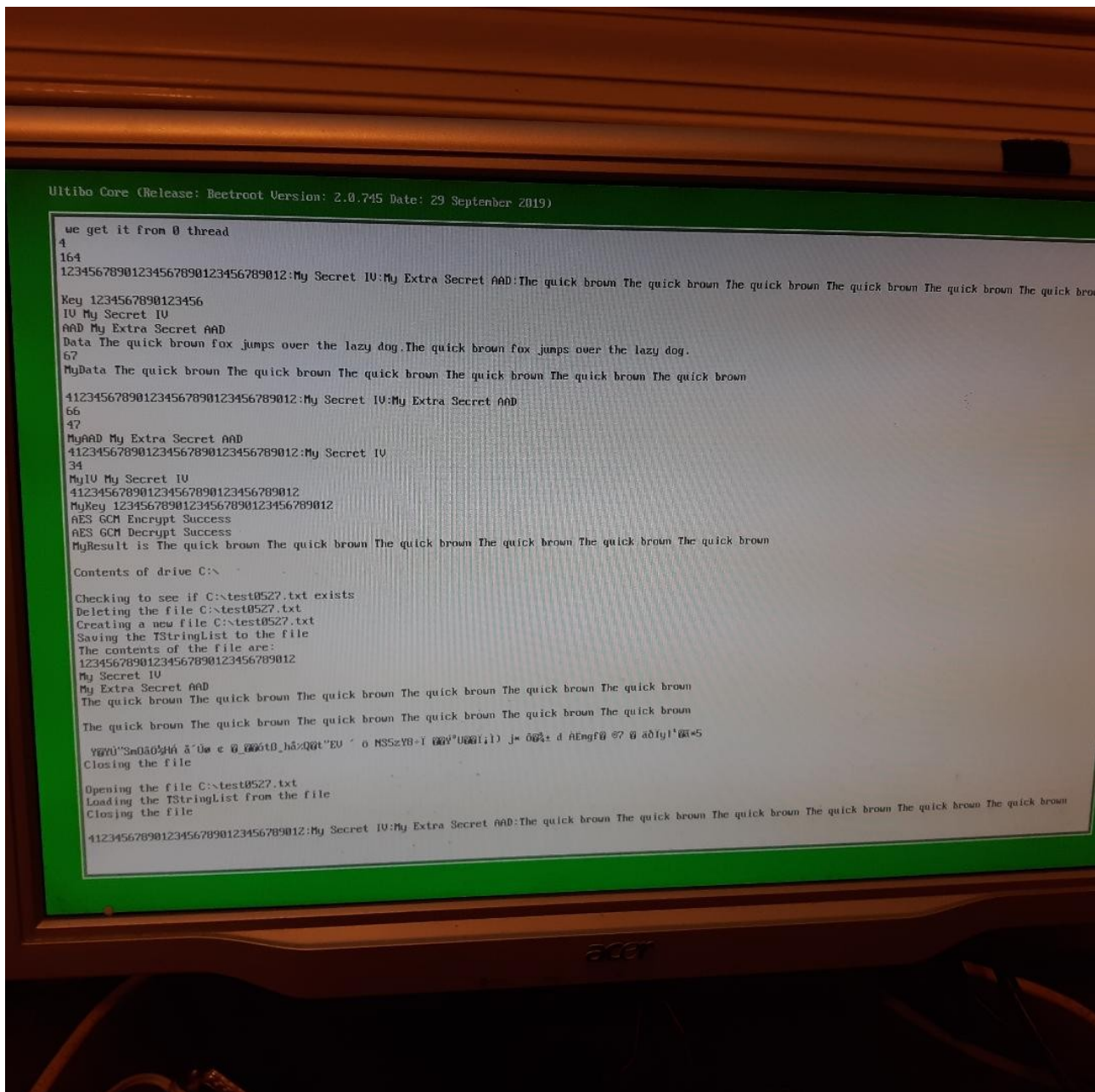
The quick brown

^N<9F>Y<DA>"Sm0<E2>H<C1>^X<E5><B4><DA><F8>^@<A2>^L<81>_<9B><8D><F3>t:h<E5>%Q

<9B>t"EV^E<B4>^R<F6>ESCNS5zY8<F7><CF>^L<85>^?U<86><85>}<CC>)^Zj*^Np<BE><B1>

d<C0><CB>mgf<87>^P<AE><91>^_<E4><F0><CF>y|<B9><99><E3>*5

test0527.txt (END)



Background: Started with 2 projects test_crypto.lpi & Srv.lpi from github devlone
Ultibo_Projects.

Commad line using FPC

Step 1

. ~/fpc.sh

Step 2

cd Ultibo_Projects/Crypto-Socket/Rpi3/ or cd Ultibo_Projects/Crypto-Socket/RPi2/

Step 3
compile

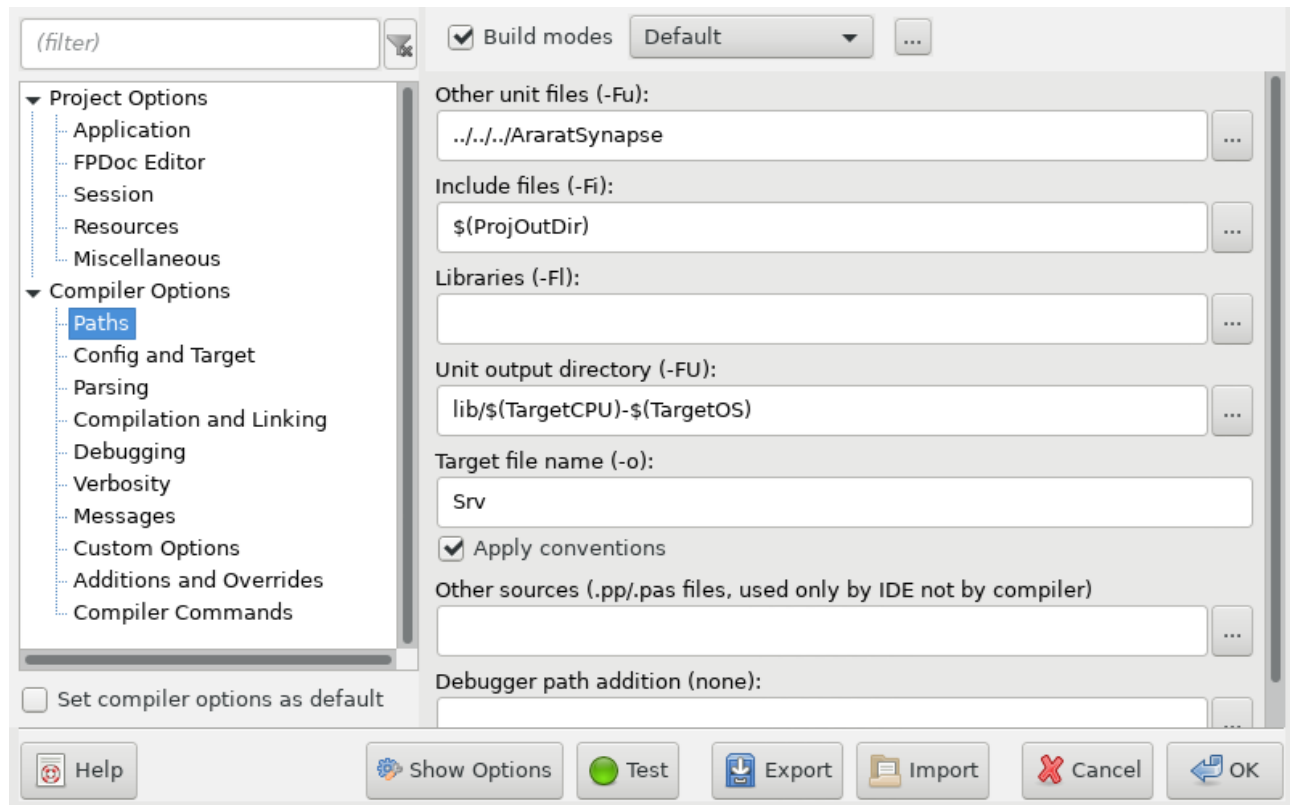
```
fpc -vi -B -Tultibo -Parm -CpARMV7A -WpRPI3B -Fu../../AraratSynapse  
@/home/devel/ultibo/core/fpc/bin/RPI3.CFG -O2 Srv.lpr
```

or

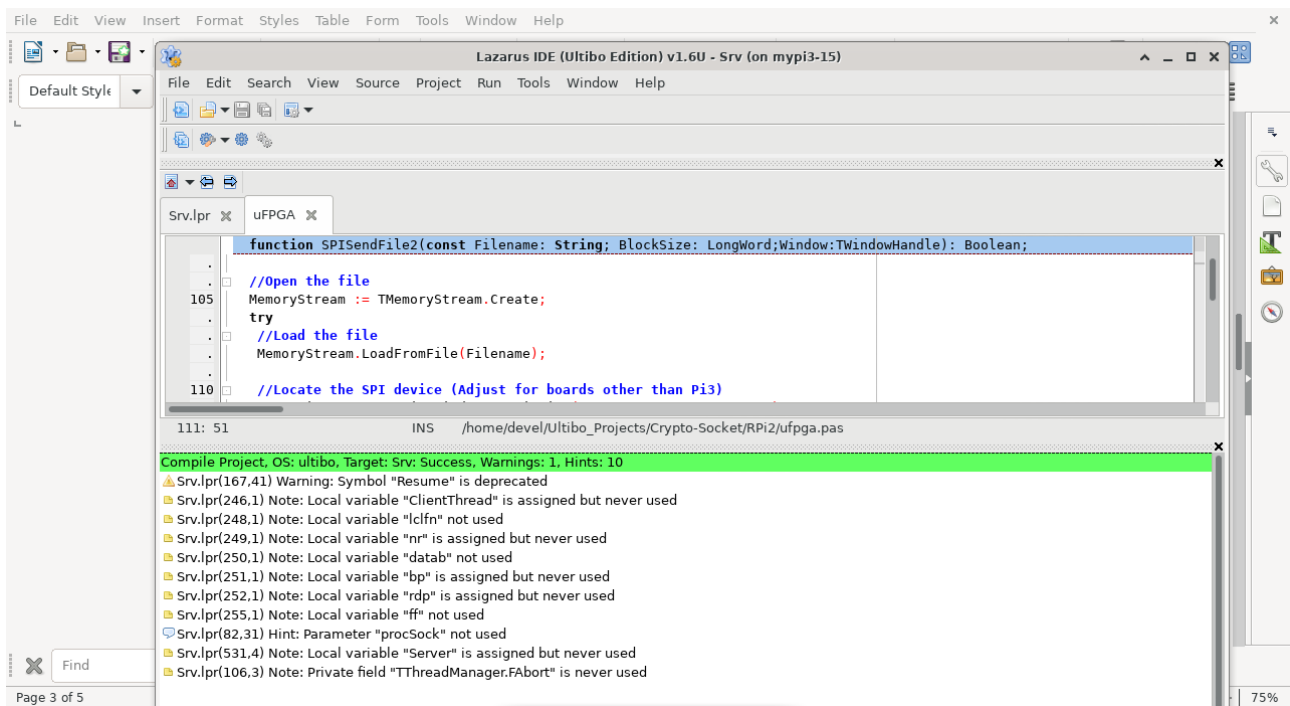
```
fpc -vi -B -Tultibo -Parm -CpARMV7A -WpRPI2B -Fu../../AraratSynapse  
@/home/devel/ultibo/core/fpc/bin/RPI2.CFG -O2 Srv.lpr  
Transfer kernel7.img
```

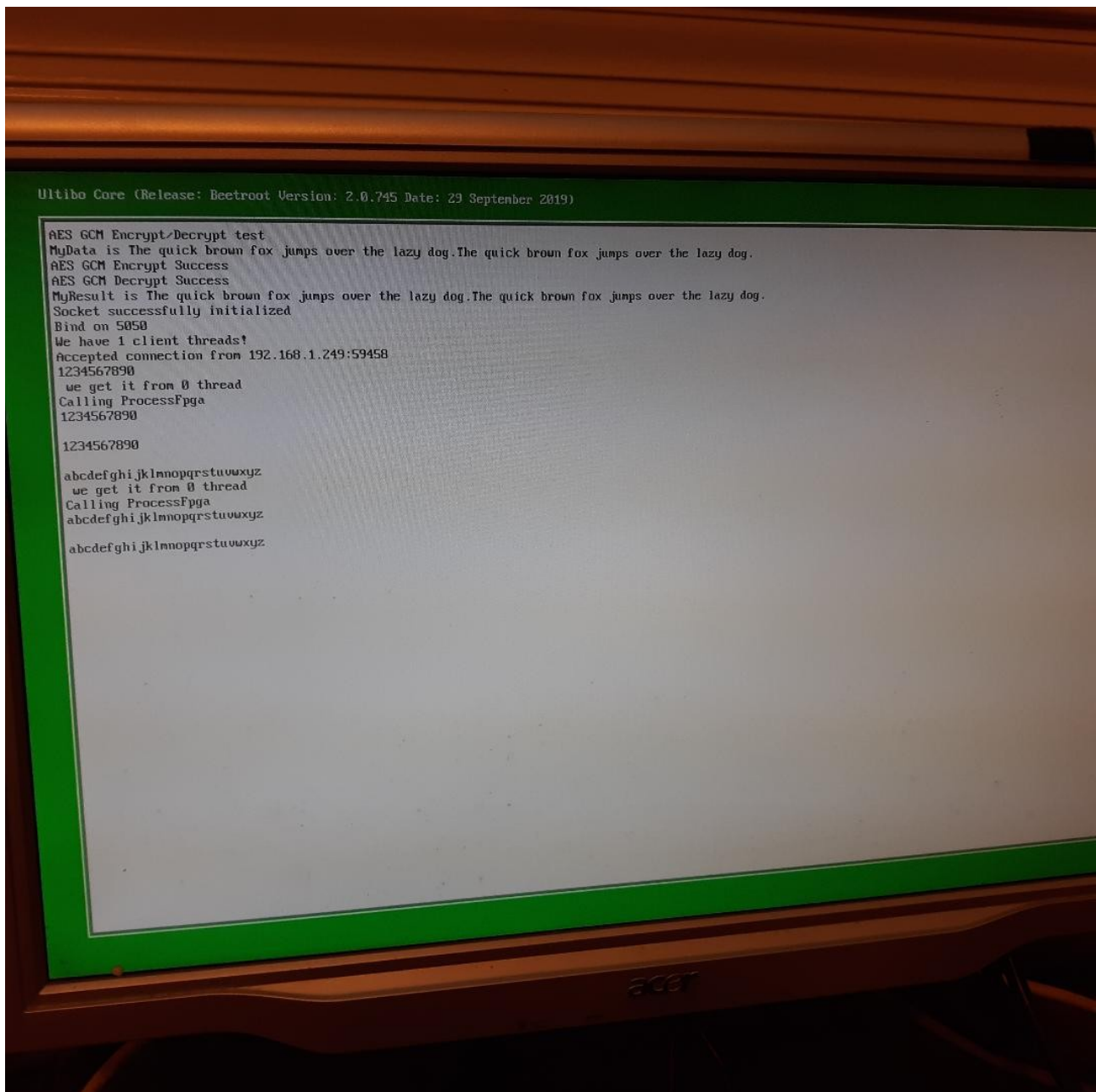
To transfer kernel7.img
tftp 192.168.1.69 < cmdstftp
tftp> tftp> Sent 2701996 bytes in 5.3 seconds

Compiling with Lazaraus.



Depress Run/Compile





Telnet

File Edit View Terminal Tabs Help

```
Assembling srv
Linking Srv
13707 lines compiled, 2.7 sec, 2636686 bytes code, 89000 bytes data
1 warning(s) issued
13 note(s) issued
devel@mypi3-15:~/Ultibo_Projects/Crypto-Socket/RPi2 $ tftp 192.168.1.69 < cmdstf
tp
tftp> tftp> Sent 2701996 bytes in 5.3 seconds
tftp> devel@mypi3-15:~/Ultibo_Projects/Crypto-Socket/RPi2 $ ping 192.168.1.69
PING 192.168.1.69 (192.168.1.69) 56(84) bytes of data.
64 bytes from 192.168.1.69: icmp_seq=2 ttl=128 time=0.651 ms
64 bytes from 192.168.1.69: icmp_seq=3 ttl=128 time=0.630 ms
64 bytes from 192.168.1.69: icmp_seq=4 ttl=128 time=0.596 ms
^C
--- 192.168.1.69 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 133ms
rtt min/avg/max/mdev = 0.596/0.625/0.651/0.036 ms
devel@mypi3-15:~/Ultibo_Projects/Crypto-Socket/RPi2 $ telnet 192.168.1.69 5050
Trying 192.168.1.69...
Connected to 192.168.1.69.
Escape character is '^]'.
1234567890
abcdefghijklmnopqrstuvwxyz
█
```