**********Draft**********

Crypto-Socket
Using AraratSnyapse Library
05/27/20

**********Draft**********

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

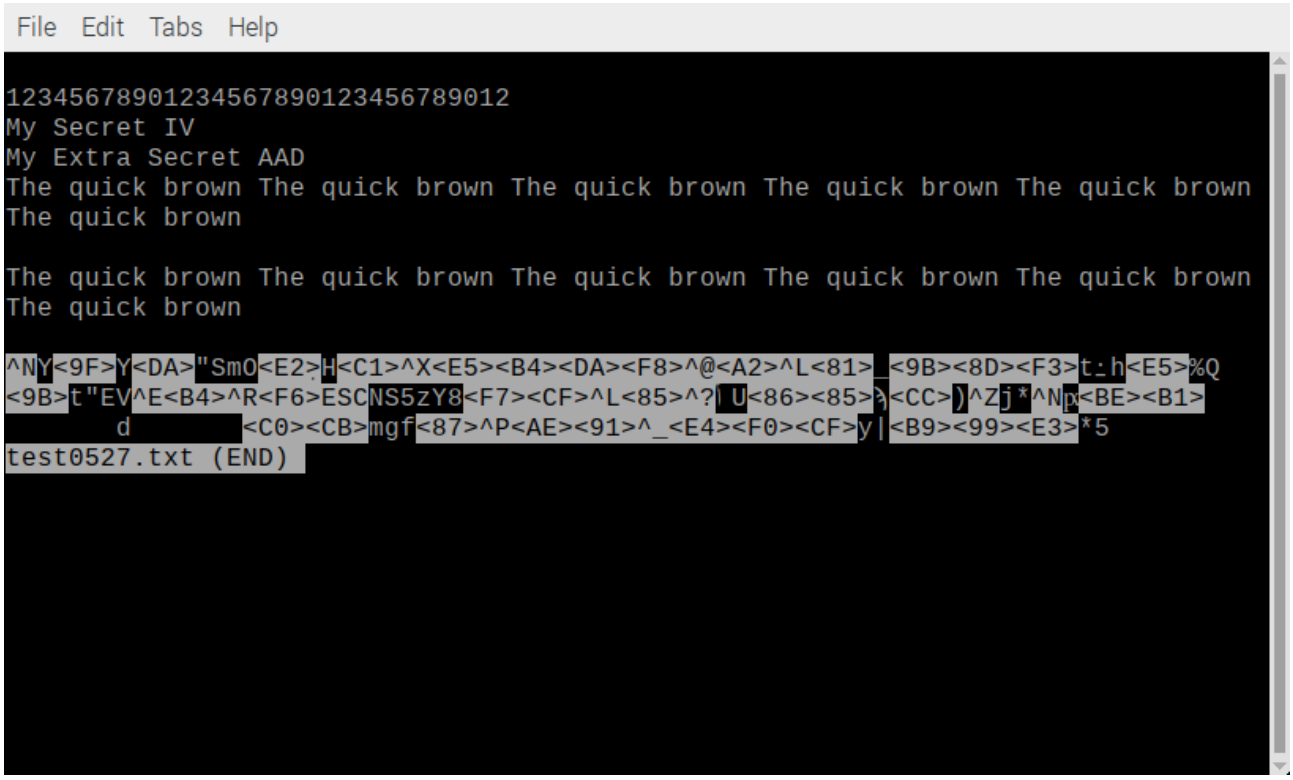
The initial values were below.
MyKey: AnsiString = '1234567890123456'; {Must be 16, 24 or 32 bytes}
MyIV: AnsiString = 'My Secret IV';
MyAAD: AnsiString = 'My Extra Secret AAD';
MyData: AnsiString = 'The quick brown fox jumps over the lazy dog.The quick brown fox jumps over the lazy dog.';

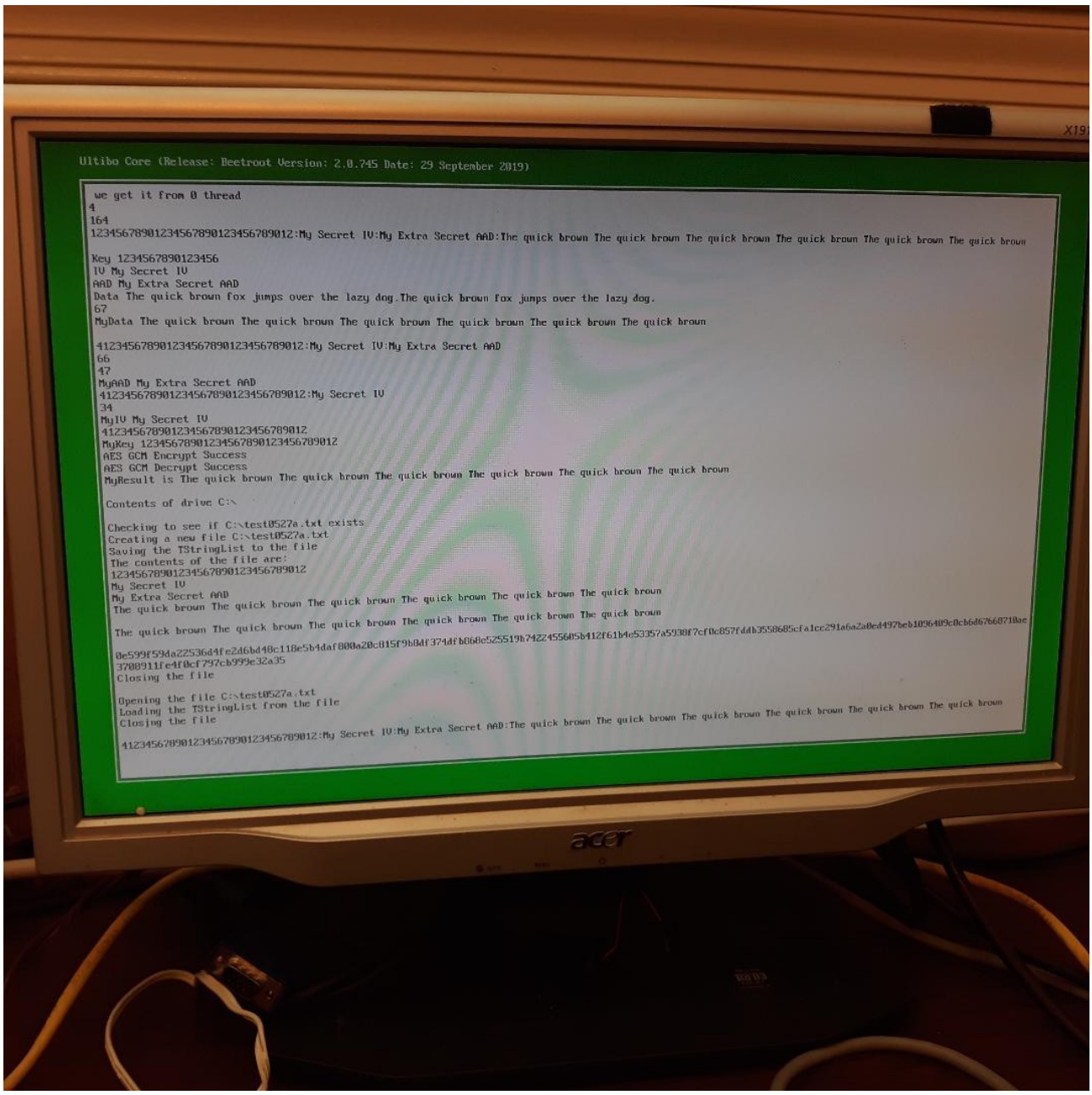
when the string below is sent to the Ultibo System

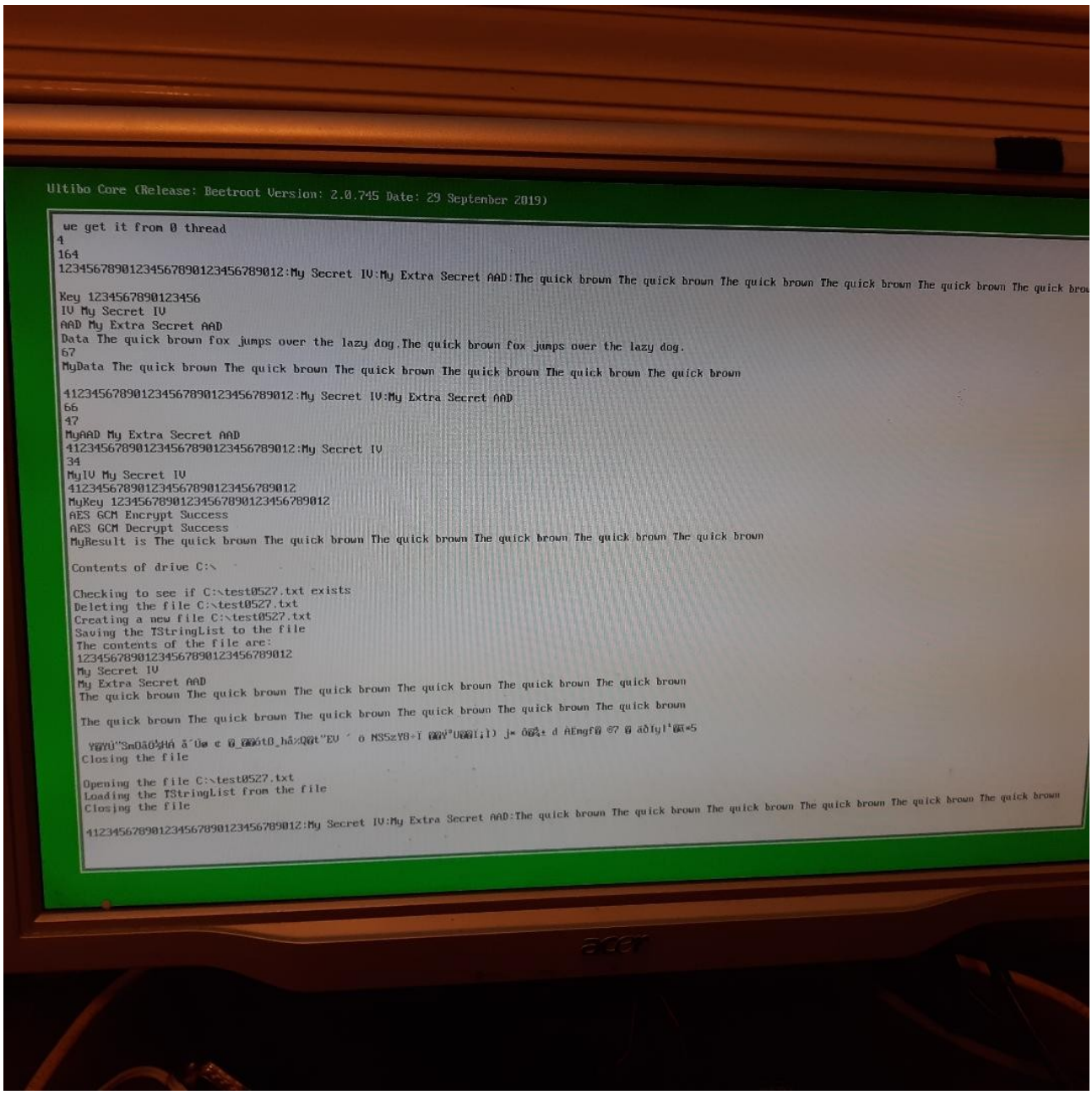
412345678901234567890123456789012:My Secret IV:My Extra Secret AAD:The quick brown The quick brown The quick brown The quick brown The quick brown The quick brown
The delimiter is :
MyKey 12345678901234567890123456789012
MyIV My Secret IV
MyAAD My Extra Secret AAD
MyData The quick brown The quick brown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

The results are writen 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
^NY<9F>Y<DA>"SmO<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*^N<BE><B1>
d <C0><CB>mgf<87>^P<AE><91>^_<E4><F0><CF>y<B9><99><E3>*5
test0527.txt (END)


Ultibo Core (Release: Beetroot Version: 2.0.745 Date: 29 September 2019)
we get it from 0 thread
4
164
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
Key 12345678901234567
IV My Secret IV
AAD My Extra Secret AAD
Data The quick brown fox jumps over the lazy dog.The quick brown fox jumps over the lazy dog.
67
MyData The quick brown The quick brown The quick brown The quick brown The quick brown The quick brown
412345678901234567890123456789012:My Secret IV:My Extra Secret AAD
66
47
MyAAD My Extra Secret AAD
412345678901234567890123456789012:My Secret IV
34
MyIV My Secret IV
412345678901234567890123456789012
MyKey 12345678901234567890123456789012
AES GCM Encrypt Success
AES GCM Decrypt Success
MyResult is The quick brown The quick brown The quick brown The quick brown The quick brown The quick brown
Contents of drive C:\
Checking to see if C:\test0527a.txt exists
Creating a new file C:\test0527a.txt
Saving the TStringList to the file
The contents of the file are:
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
0e599f59da22536d4fe2d6bd48c118e5b4daf800a20c815f9b0df374dfb068e5255191b742245560 5b412f61b4e53357a5938f7cf0c857fddb3558685cfa1cc291a6a2a0ed497beb10964d9c0cb6d6766871bae
3708911fe4f0cf797cb999e32a35
Closing the file
Opening the file C:\test0527a.txt
Loading the TStringList from the file
Closing the file
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
acer



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

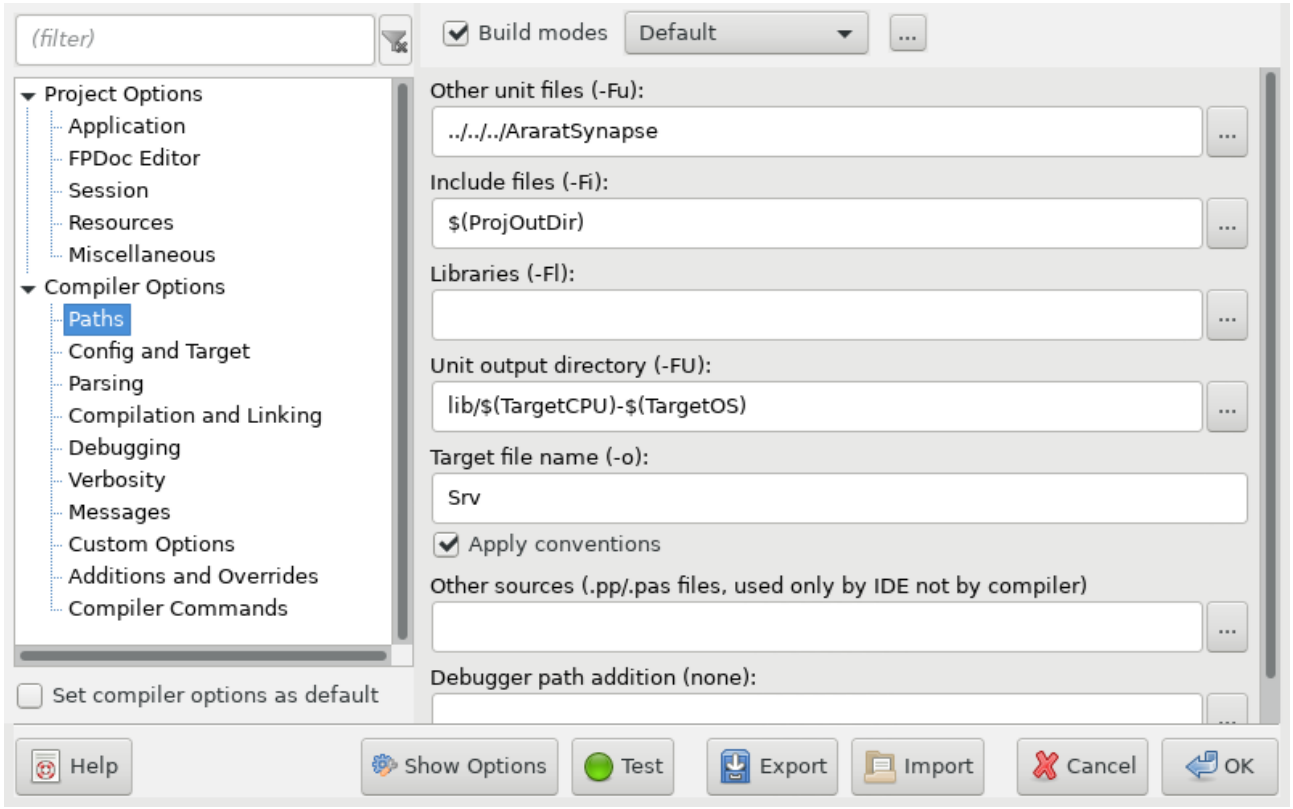
fpc -vi -B -Tultibo -Parm -CpARMV7A -WpRPI3B -Fu../../../AraratSynapse
@/home/devel/ultibo/core/fpc/bin/RPI3.CFG -O2 Srv.lpr

or

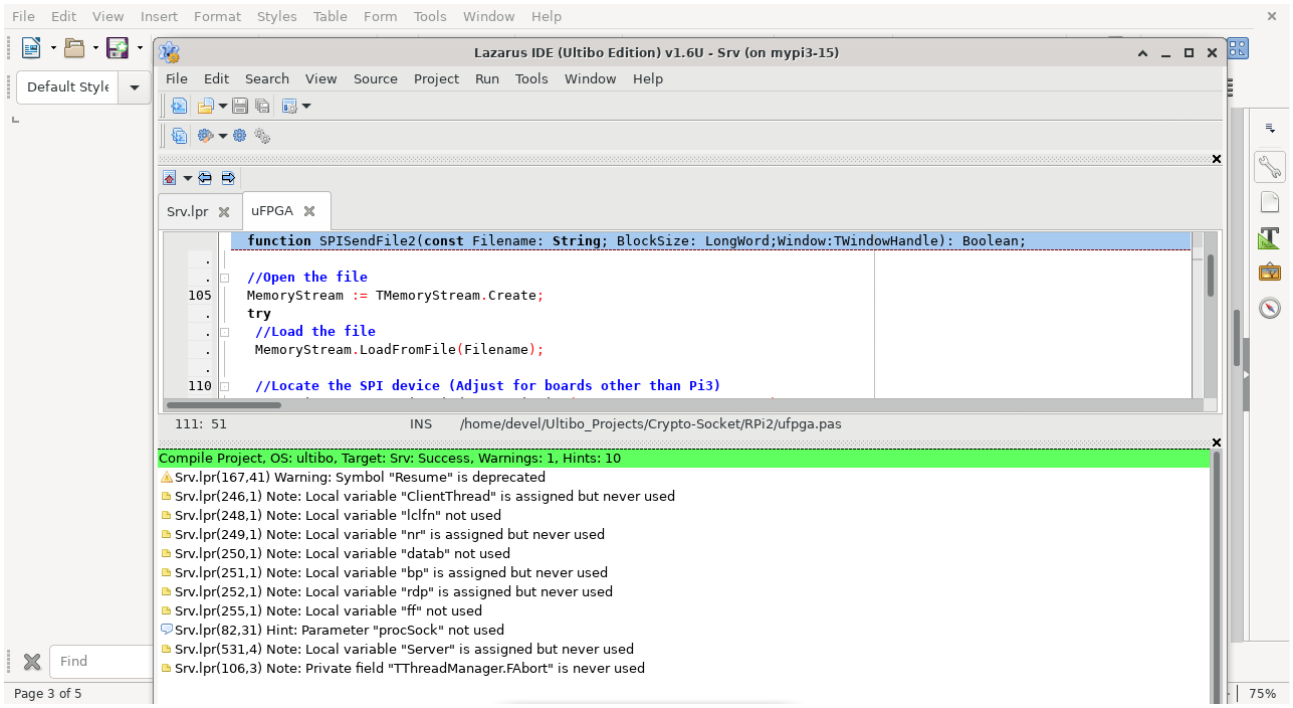
fpc -vi -B -Tultibo -Parm -CpARMV7A -WpRPI2B -Fu../../../AraratSynapse
@/home/devel/ultibo/core/fpc/bin/RPI2.CFG -O2 Srv.lpr
Transfer kernel7.img

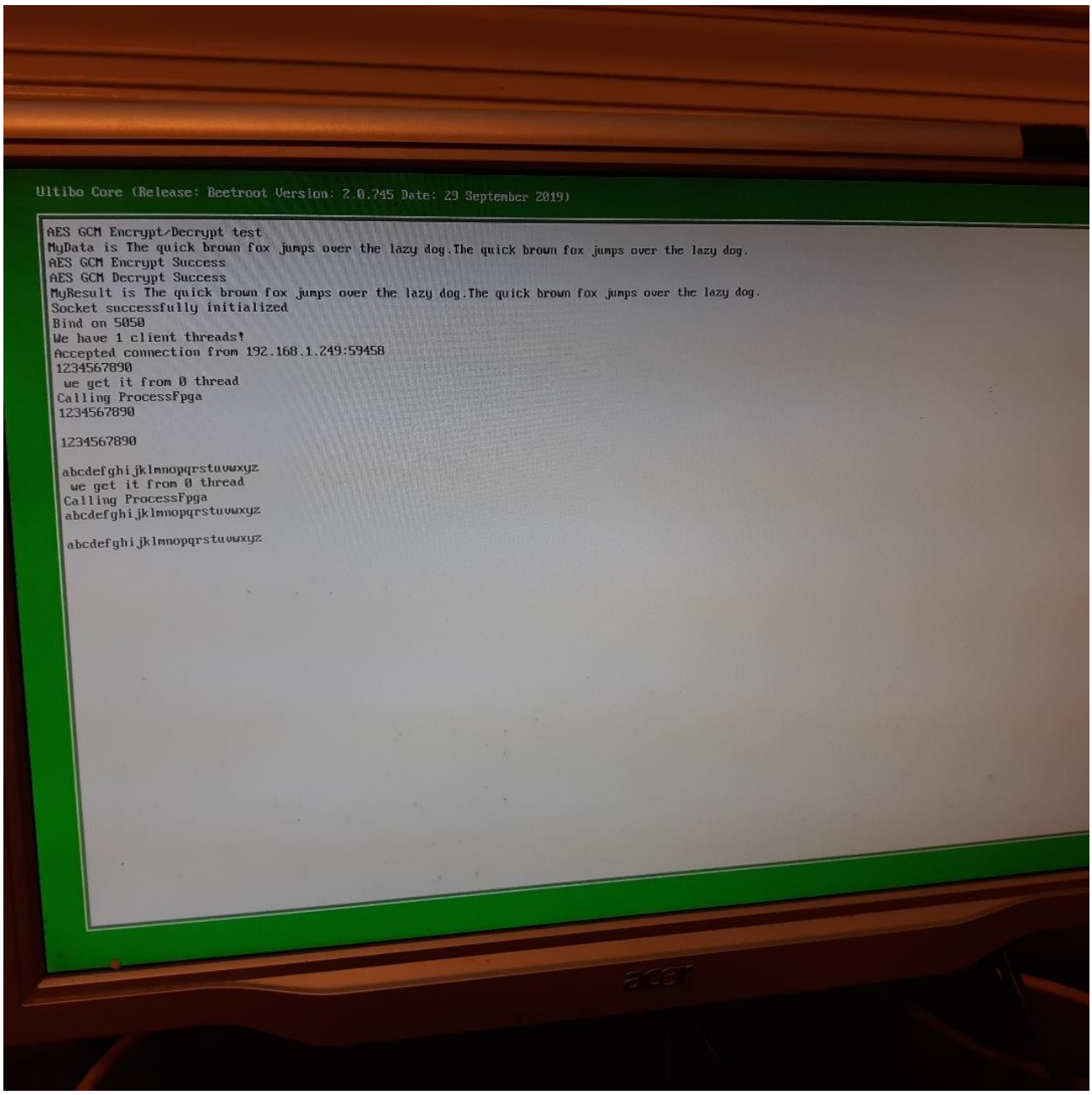
To transfer kernel7.img
tftp 192.168.1.69 < cmdstftp
tftp> tftp> Sent 2701996 bytes in 5.3 seconds

Compiling with Lazaraus.

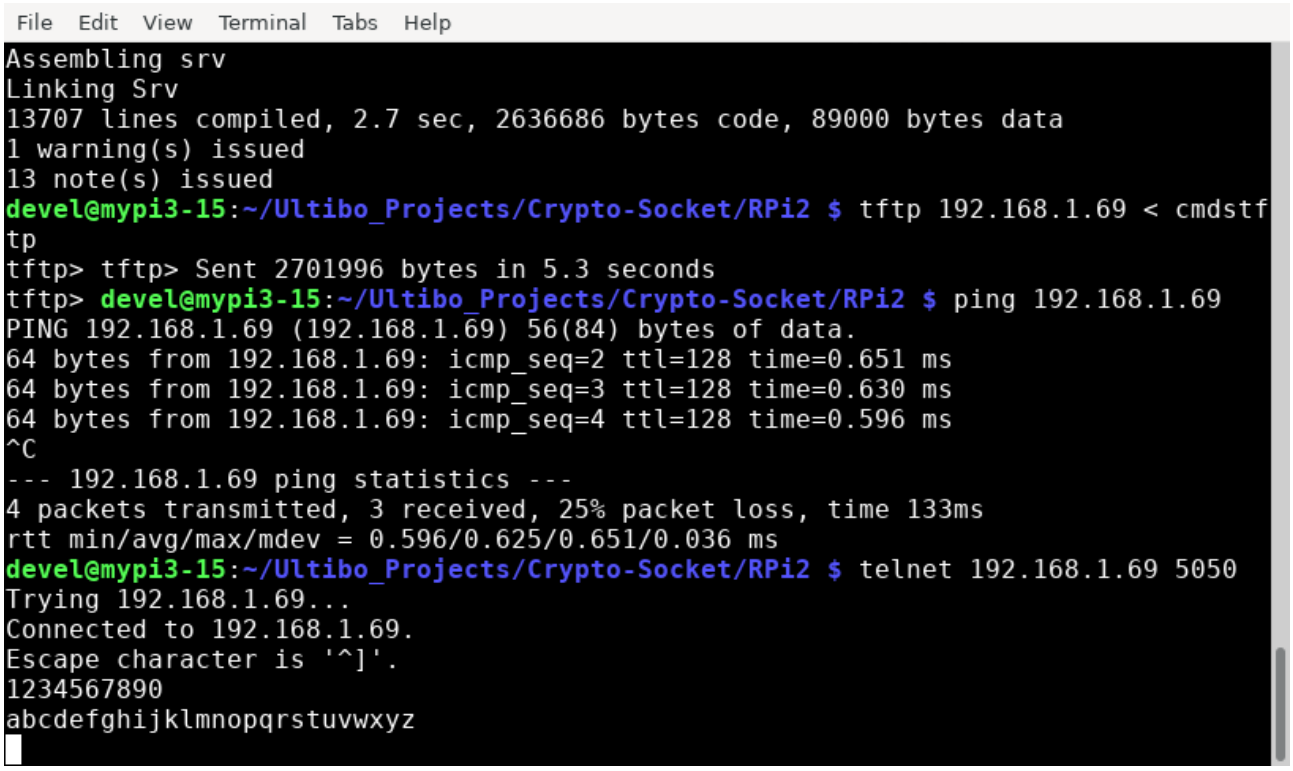


Depress Run/Compile




Ultibo Core (Release: Beetroot Version: 2.0.745 Date: 29 September 2019)
AES GCM Encrypt/Decrypt test
MyData is The quick brown fox jumps over the lazy dog.The quick brown fox jumps over the lazy dog.
AES GCM Encrypt Success
AES GCM Decrypt Success
MyResult is The quick brown fox jumps over the lazy dog.The quick brown fox jumps over the lazy dog.
Socket successfully initialized
Bind on 5050
We have 1 client threads!
Accepted connection from 192.168.1.249:59458
1234567890
we get it from 0 thread
Calling ProcessFpga
1234567890
1234567890
abcdefghijklmnopqrstuvwxyz
we get it from 0 thread
Calling ProcessFpga
abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyz
acer

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