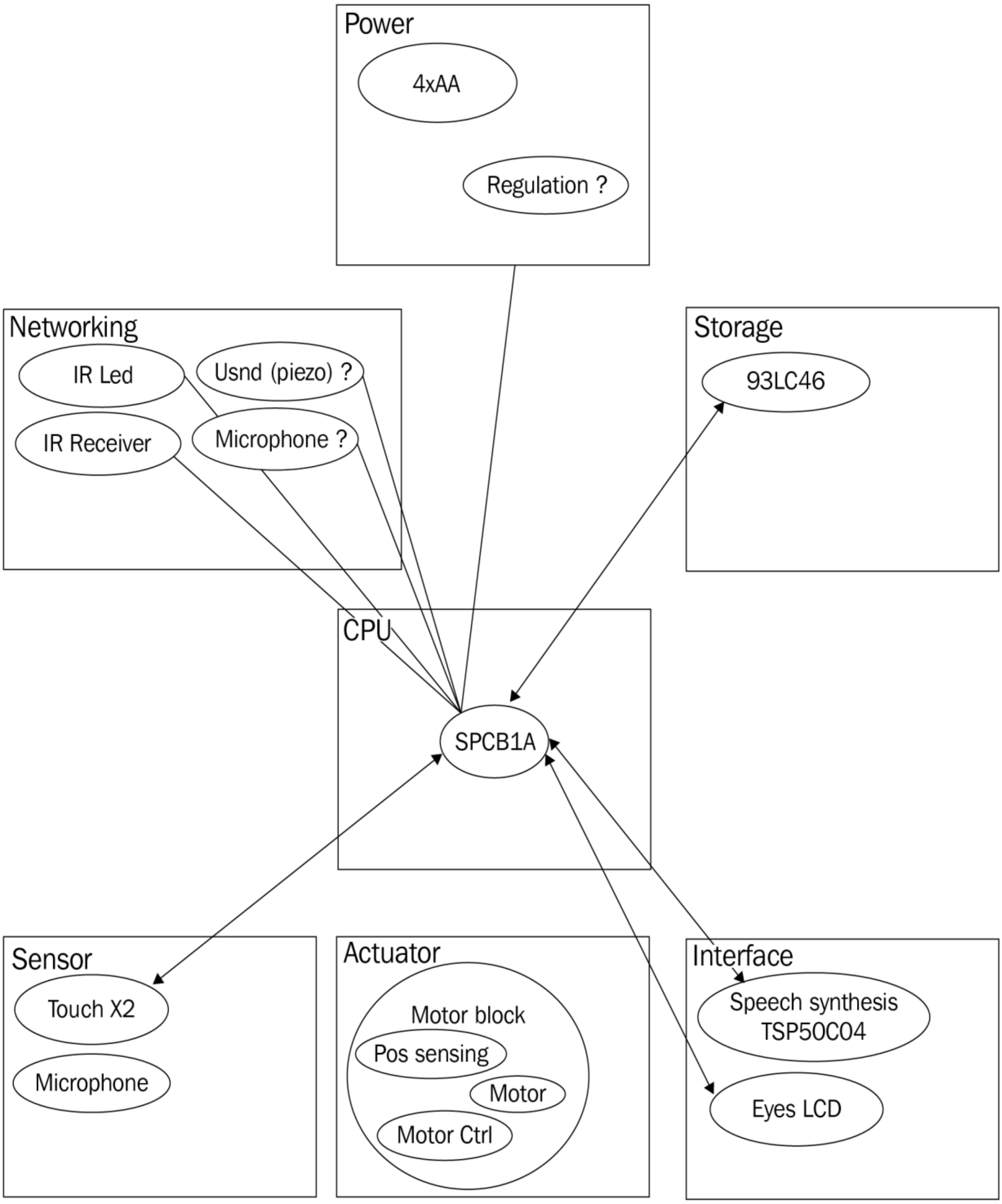
Chapter 1: Setting Up Your Pentesting Lab and Ensuring Lab Safety.

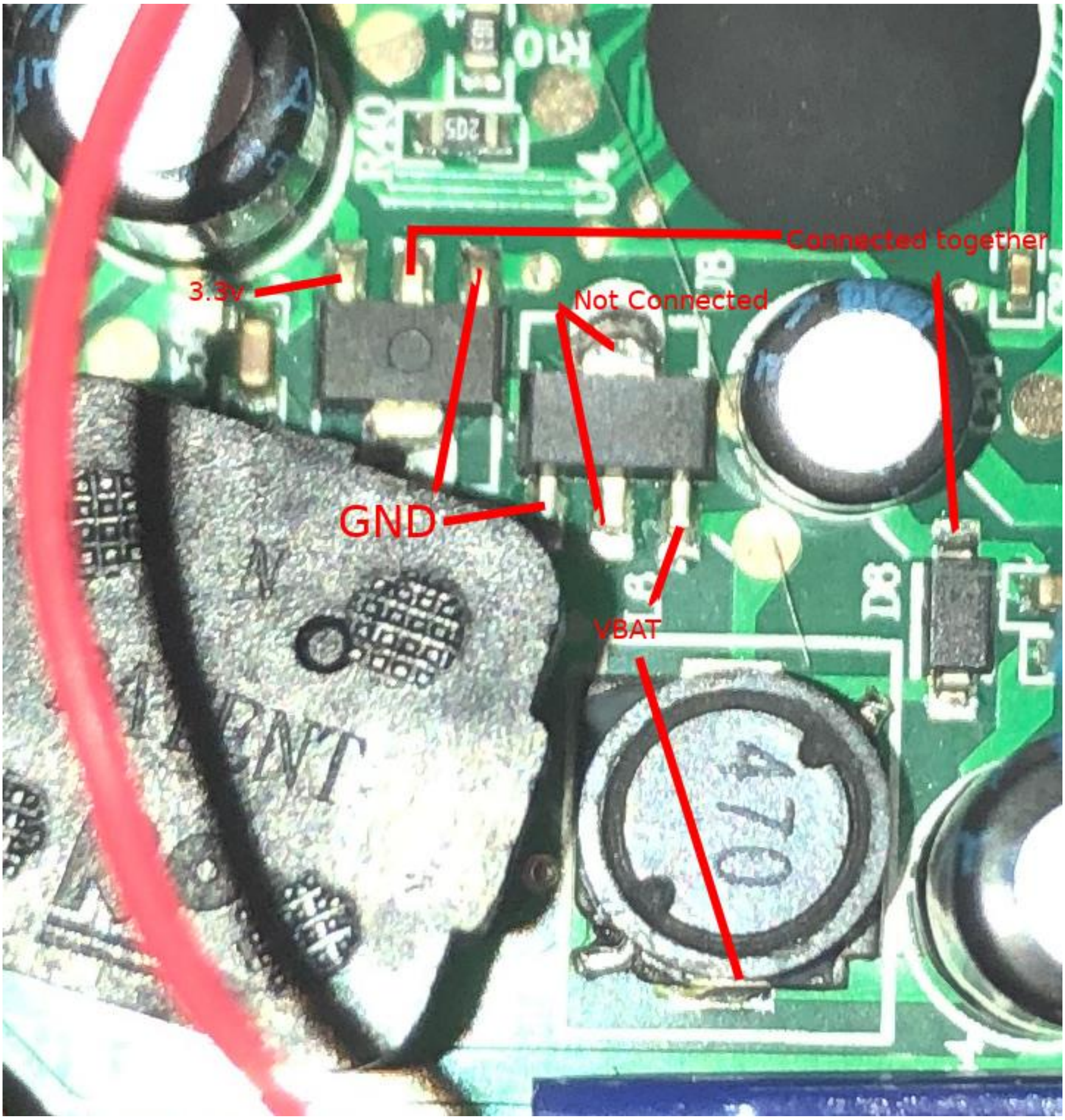
No Images

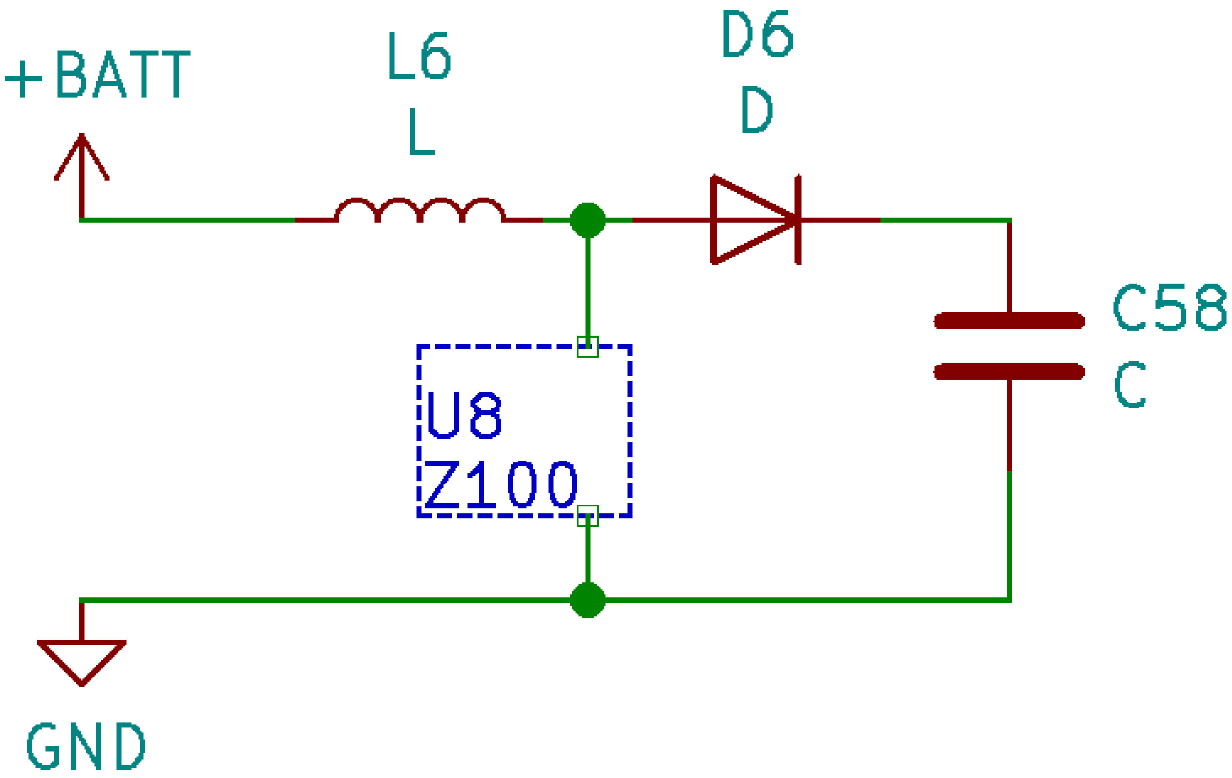
Chapter 2: Understanding Your Target.

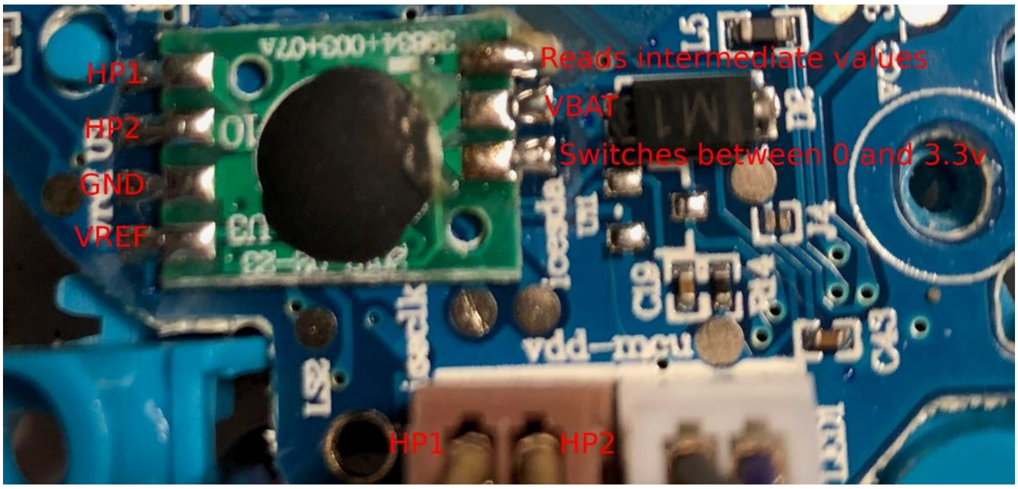
No Images.

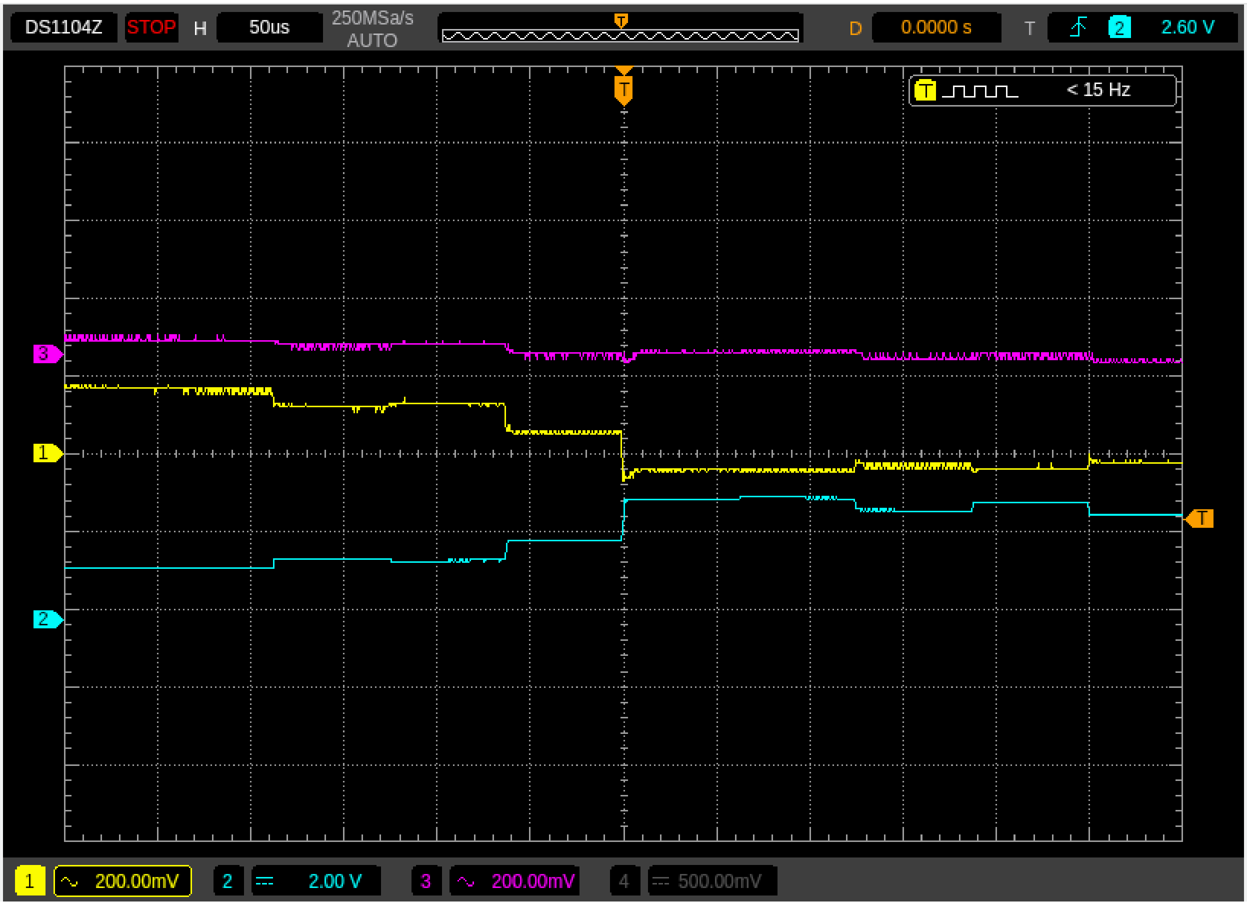
Chapter 3: Identifying the Components of Your Target.

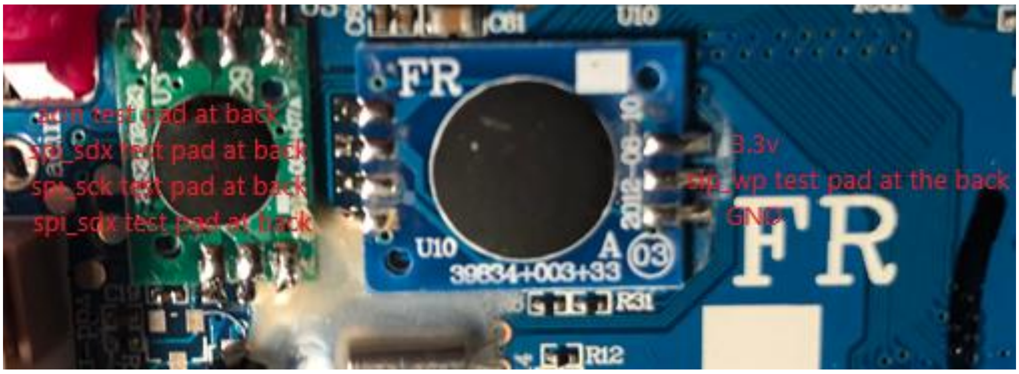


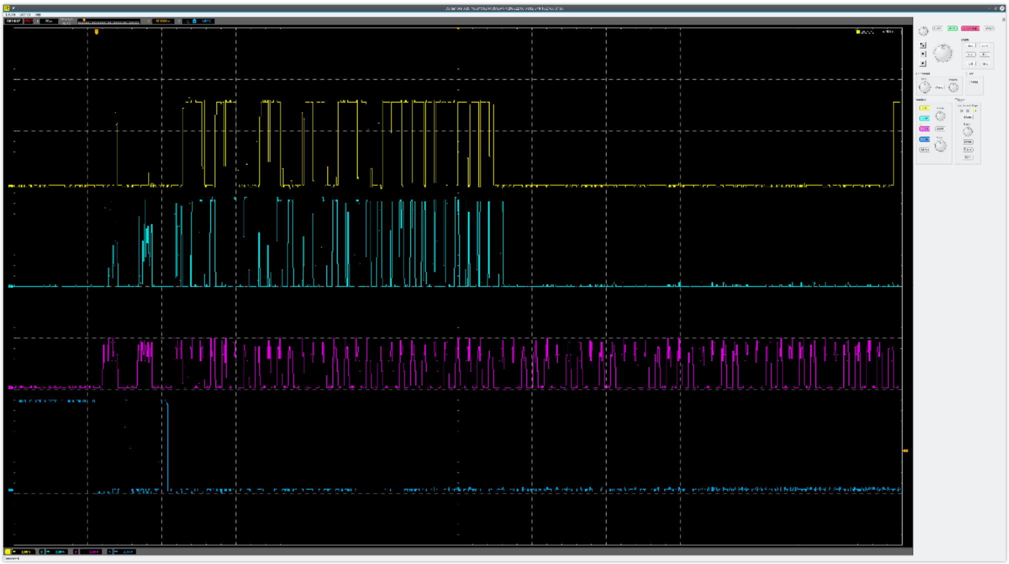

Connected together
3.3v
Not Connected
GND
VBAT
R40
R10
U4
D8
205
470

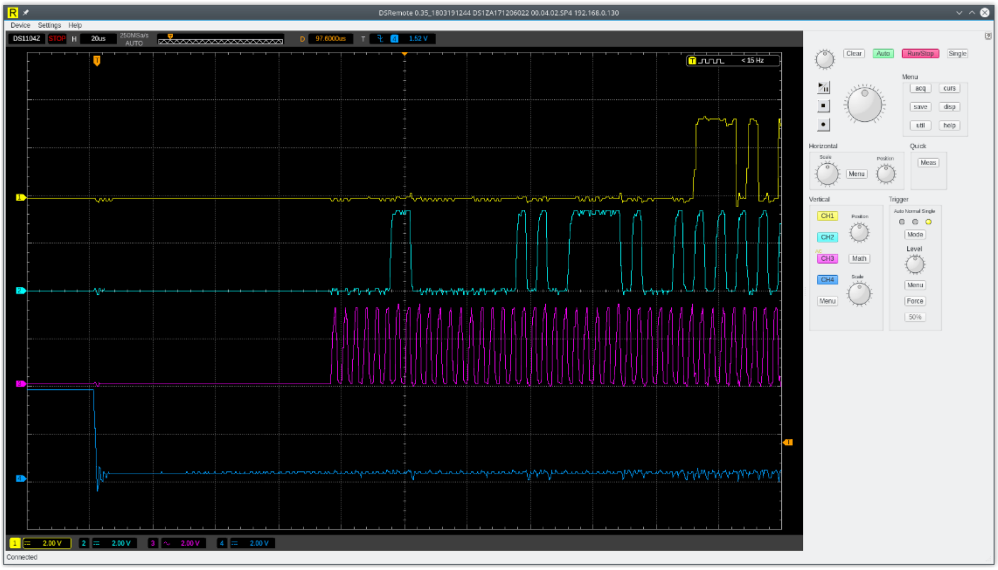

+BATT
L6
L
D6
D
C58
C
U8
Z100
GND


HP1
HP2
GND
VREF
Reads intermediate values
VBAT
Switches between 0 and 3.3v
HP1
HP2


DS1104Z
STOP
H
50us
250MSa/s
AUTO
D
0.0000 s
T
2
2.60 V
T
< 15 Hz
3
1
2
T
1
200.00mV
2
2.00 V
3
200.00mV
4
500.00mV


test pad at back
spi_sdx test pad at back
spi_sck test pad at back
spi_sdx test pad at back
3.3v
sip_wp test pad at the back
GND
FR
U10
C81
U10
2012-08-10
A
03
39834+003+33
R31
R12
FR





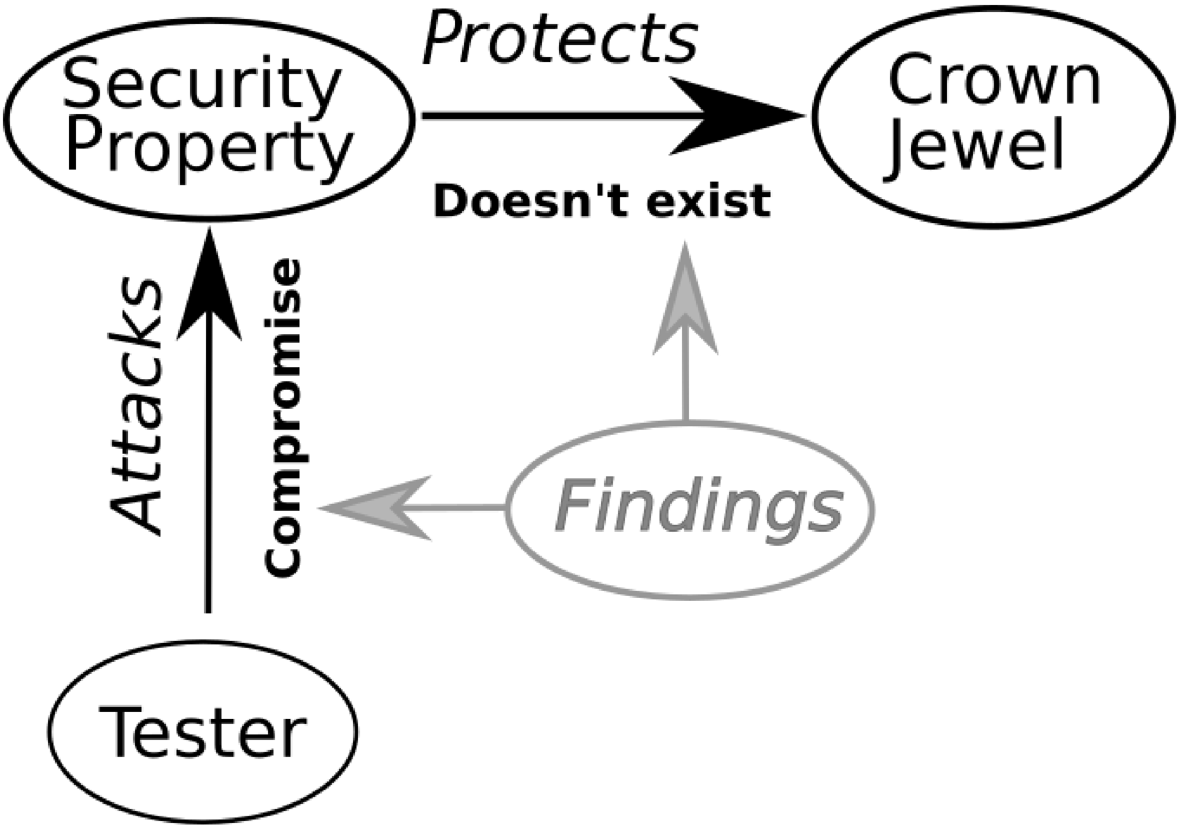
DSRemote 0.35_1803191244 DS1ZA171206022 00.04.02.SP4 192.168.0.130

DS1104Z STOP H 20us 250MSa/s AUTO D 97.6000us T 4 1.52 V

1 2.00 V 2 2.00 V 3 2.00 V 4 2.00 V

Connected

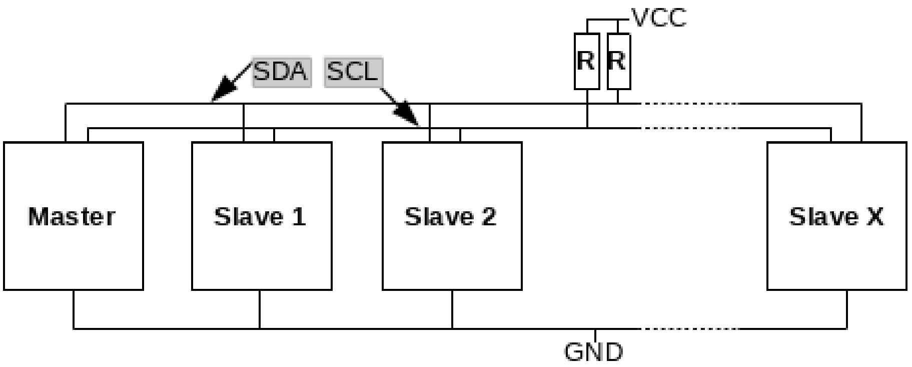
Chapter 4: Approaching and Planning the Test.

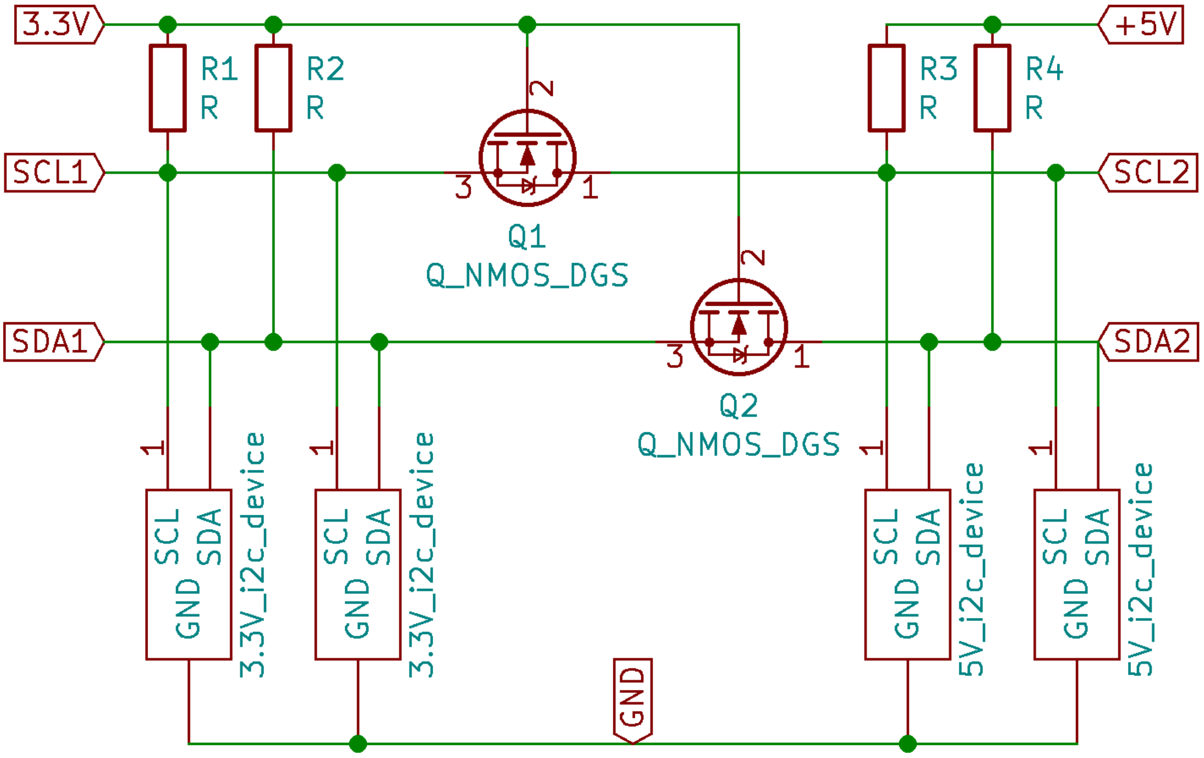


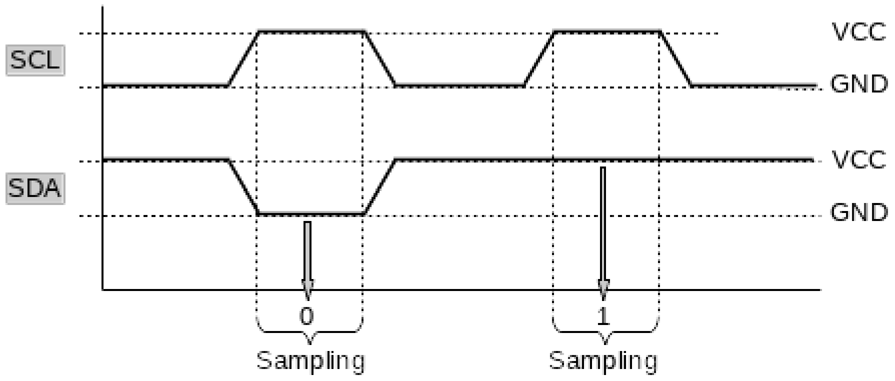
Chapter 5: Our Main Attack Platform.

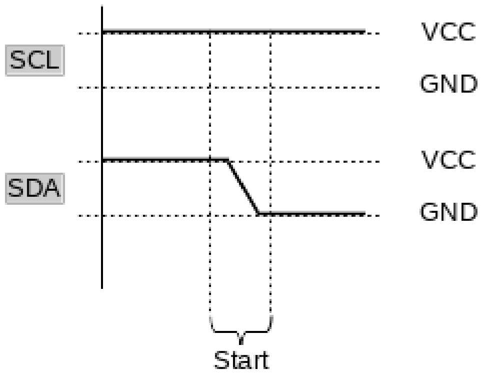
No Images

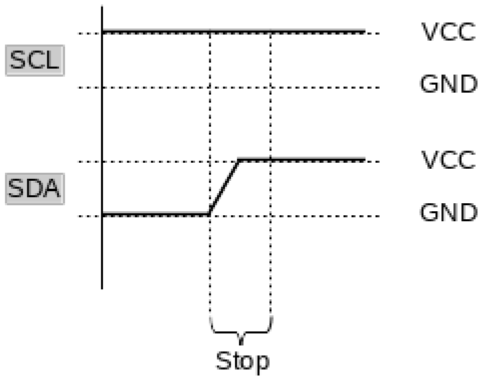
Chapter 6: Sniffing and Attacking the Most Common Protocols.

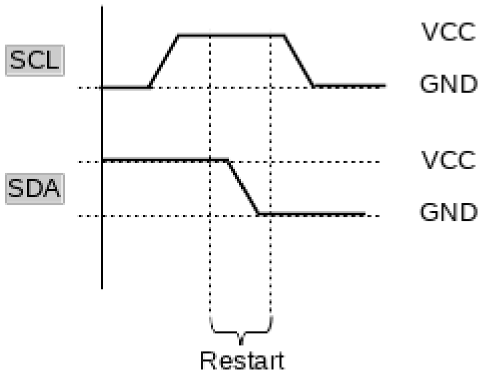


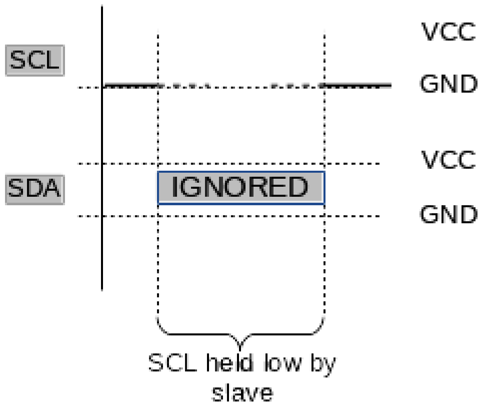


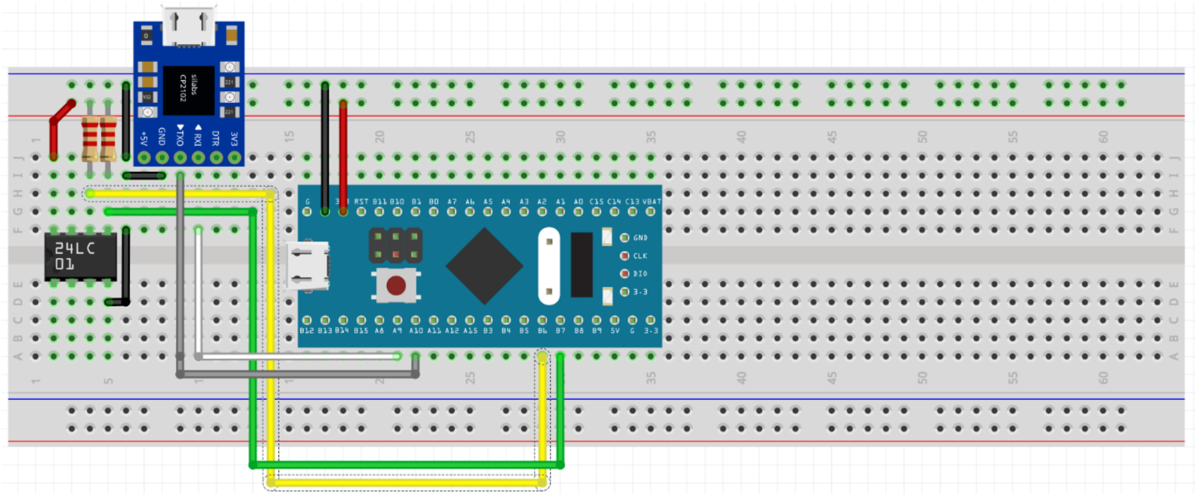


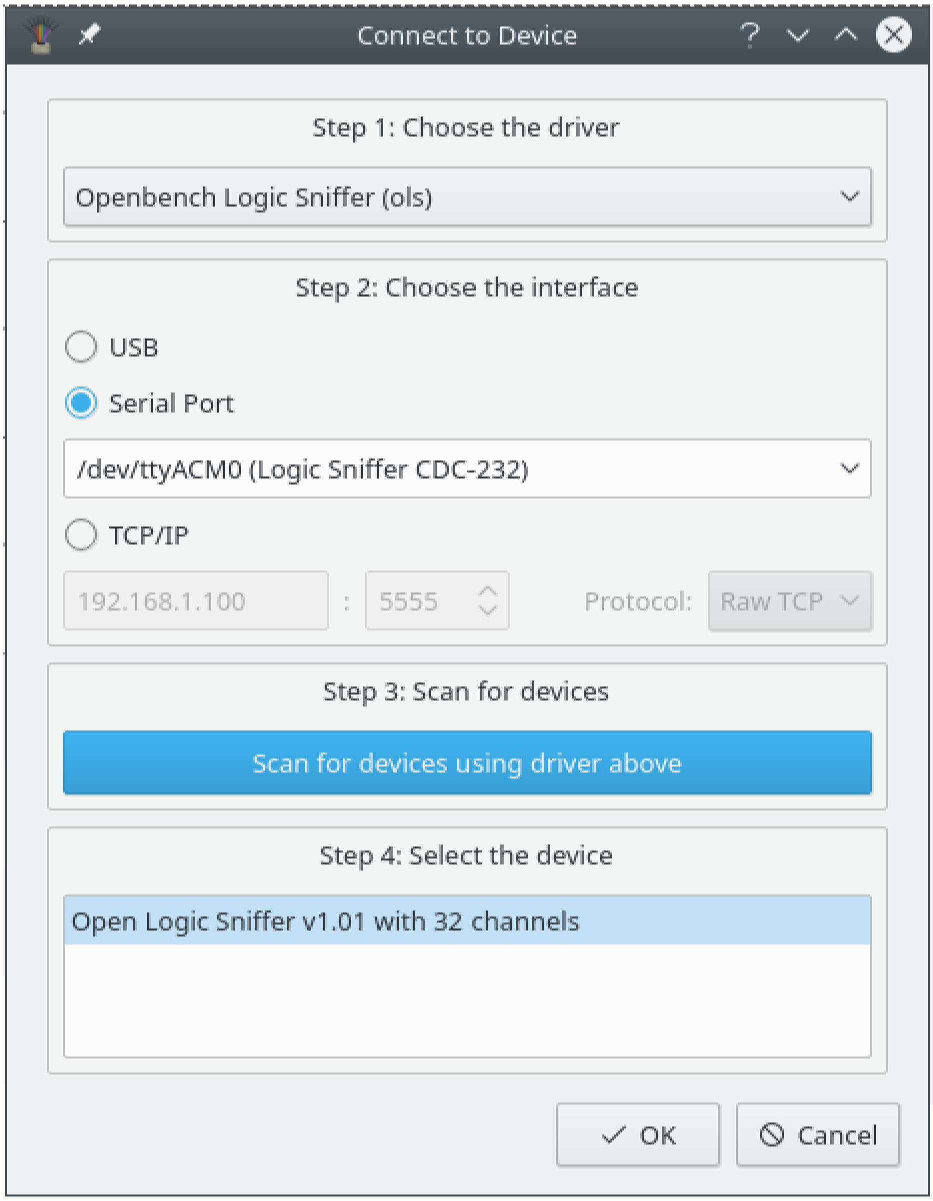

SCL
SDA
VCC
GND
VCC
GND
Start


SCL
SDA
VCC
GND
VCC
GND
Stop


SCL
SDA
VCC
GND
VCC
GND
Restart


SCL
SDA
VCC
GND
VCC
GND
IGNORED
SCL held low by
slave





Connect to Device

Step 1: Choose the driver

Openbench Logic Sniffer (ols)

Step 2: Choose the interface

○ USB

● Serial Port

/dev/ttyACM0 (Logic Sniffer CDC-232)

○ TCP/IP

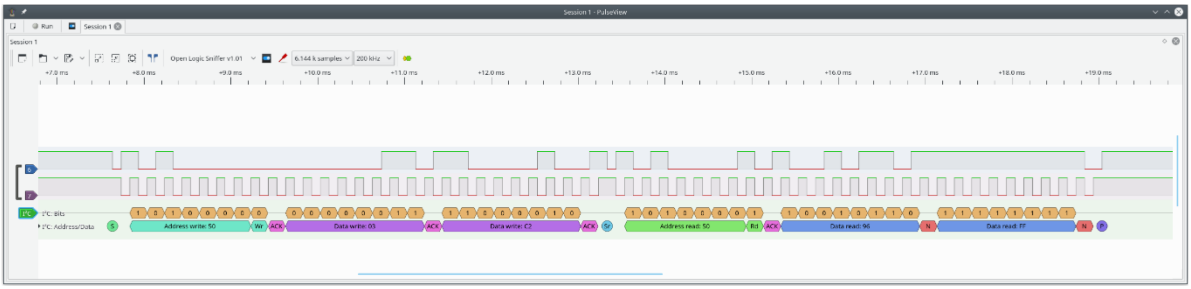
192.168.1.100 : 5555 Protocol: Raw TCP

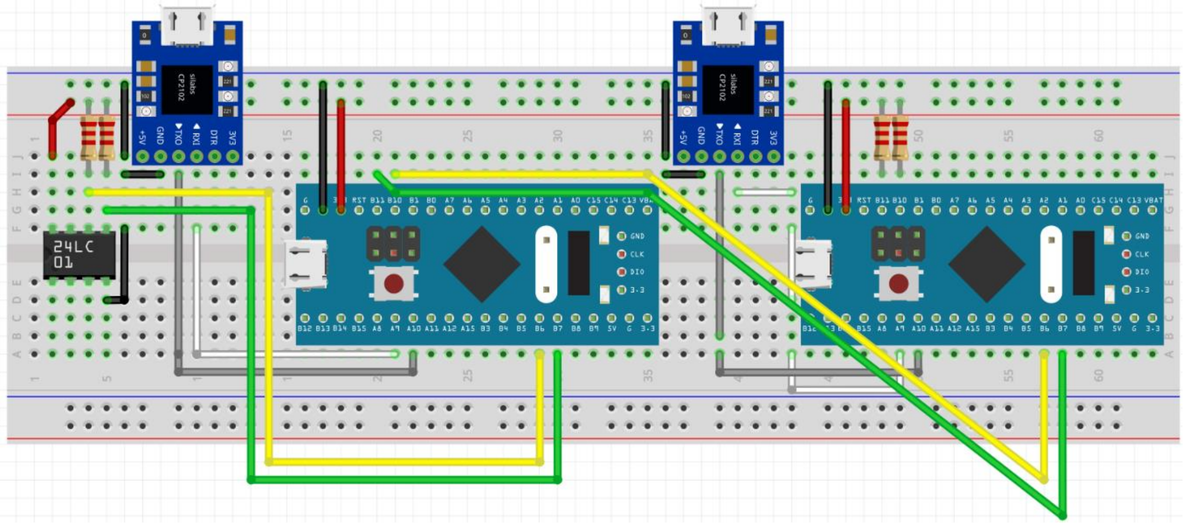
Step 3: Scan for devices

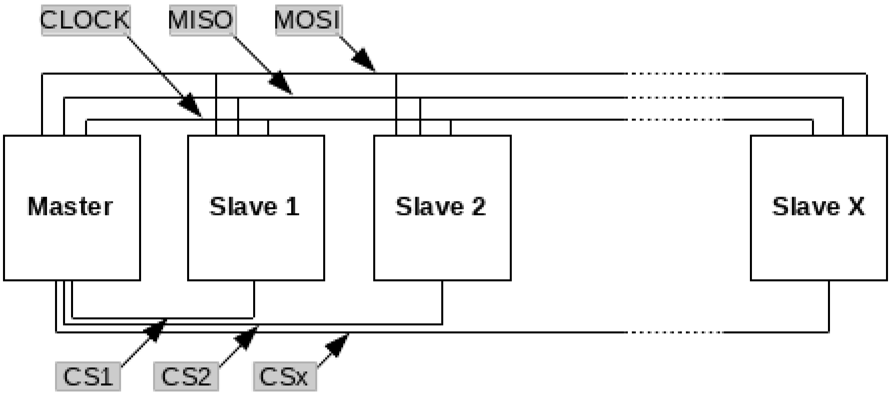
Scan for devices using driver above

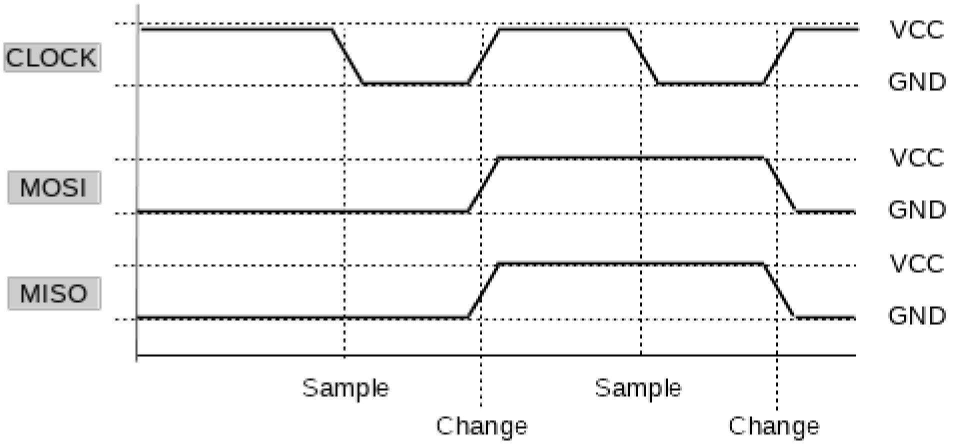
Step 4: Select the device

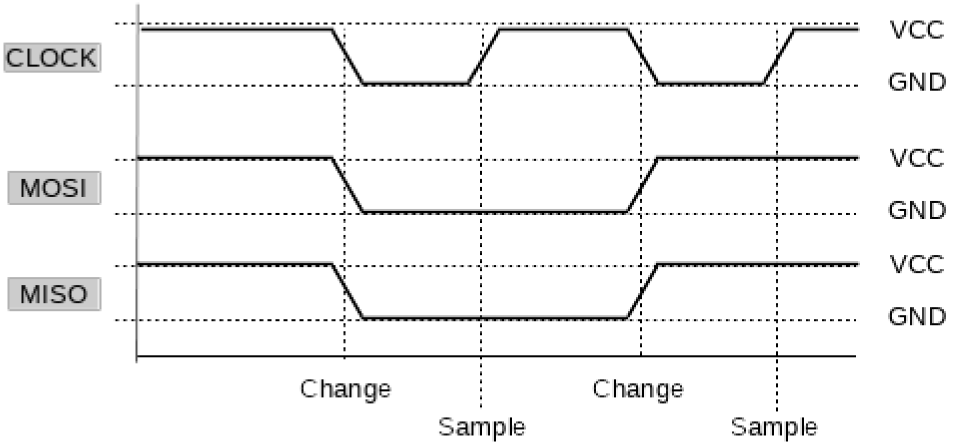
Open Logic Sniffer v1.01 with 32 channels

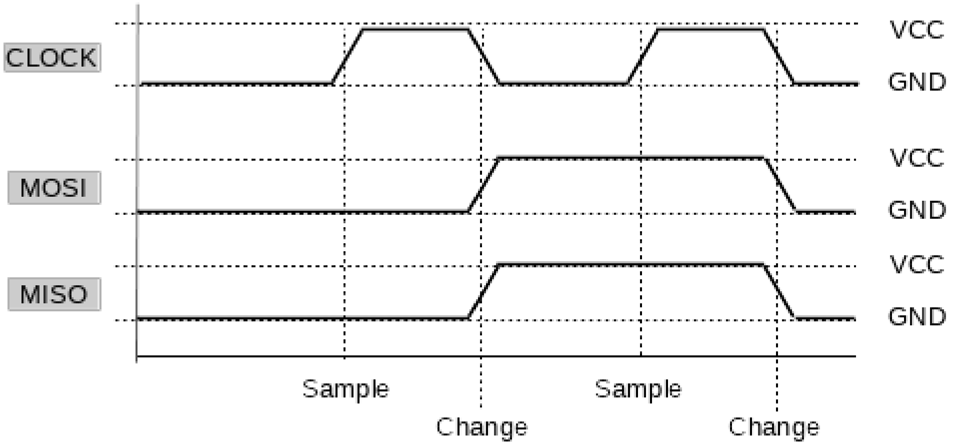

Session 1 - PulseView
Run
Session 1
Open Logic Sniffer v1.01
6.144 k samples
200 kHz
+7.0 ms
+8.0 ms
+9.0 ms
+10.0 ms
+11.0 ms
+12.0 ms
+13.0 ms
+14.0 ms
+15.0 ms
+16.0 ms
+17.0 ms
+18.0 ms
+19.0 ms
6
7
I²C
I²C: Bits
I²C: Address/Data
S
1 0 1 0 0 0 0 0
Address write: 50
Wr
ACK
0 0 0 0 0 0 1 1
Data write: 03
ACK
1 1 0 0 0 0 1 0
Data write: C2
ACK
Sr
1 0 1 0 0 0 0 1
Address read: 50
Rd
ACK
1 0 0 1 0 1 1 0
Data read: 96
N
1 1 1 1 1 1 1 1
Data read: FF
N
P

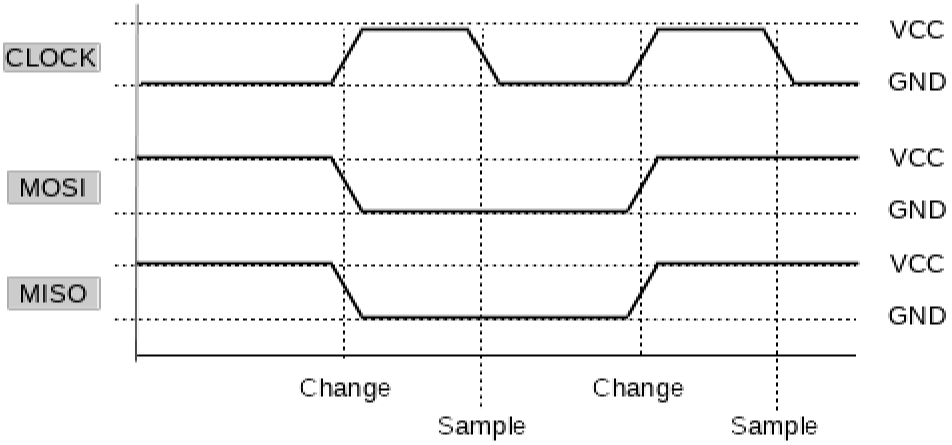

24LC
01
silabs
CP2102
+5V
GND
TXO
RXI
DTR
3V3
GND
CLK
DIO
3.3

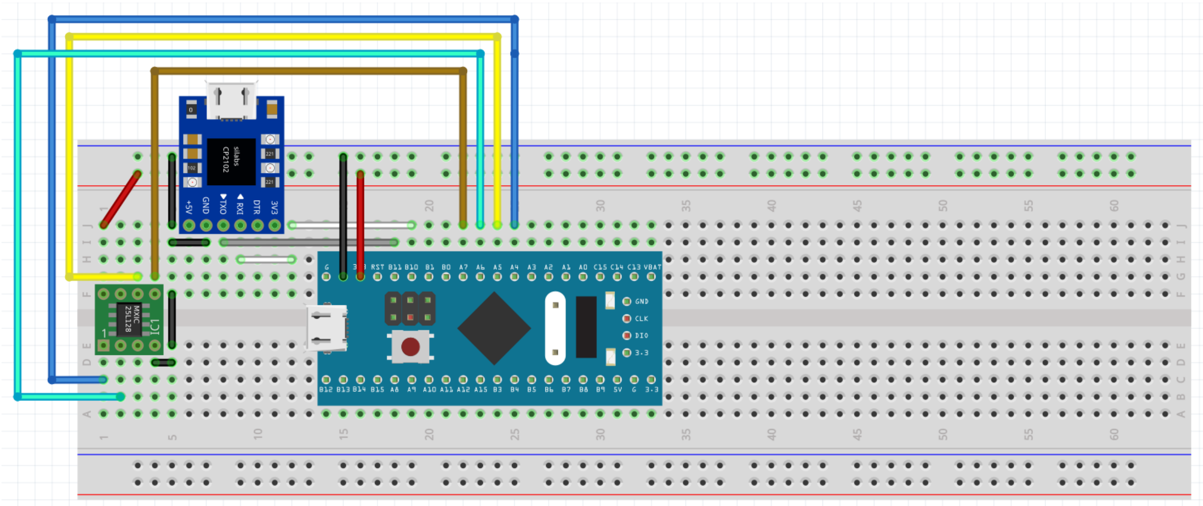

CLOCK
MISO
MOSI
Master
Slave 1
Slave 2
Slave X
CS1
CS2
CSx

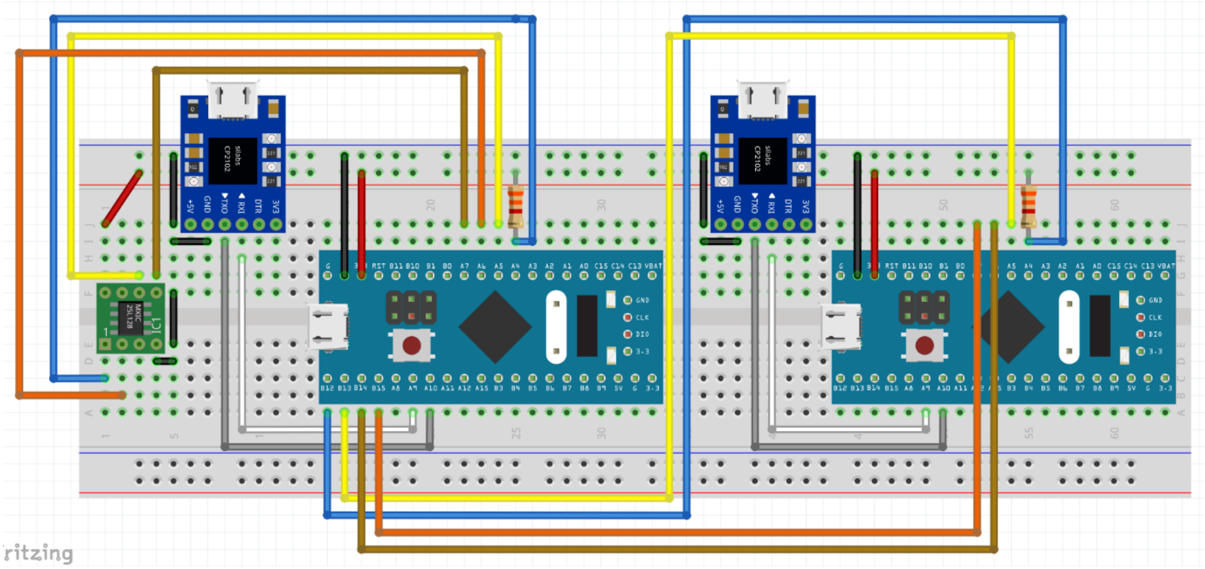

CLOCK
MOSI
MISO
VCC
GND
VCC
GND
VCC
GND
Sample
Change
Sample
Change

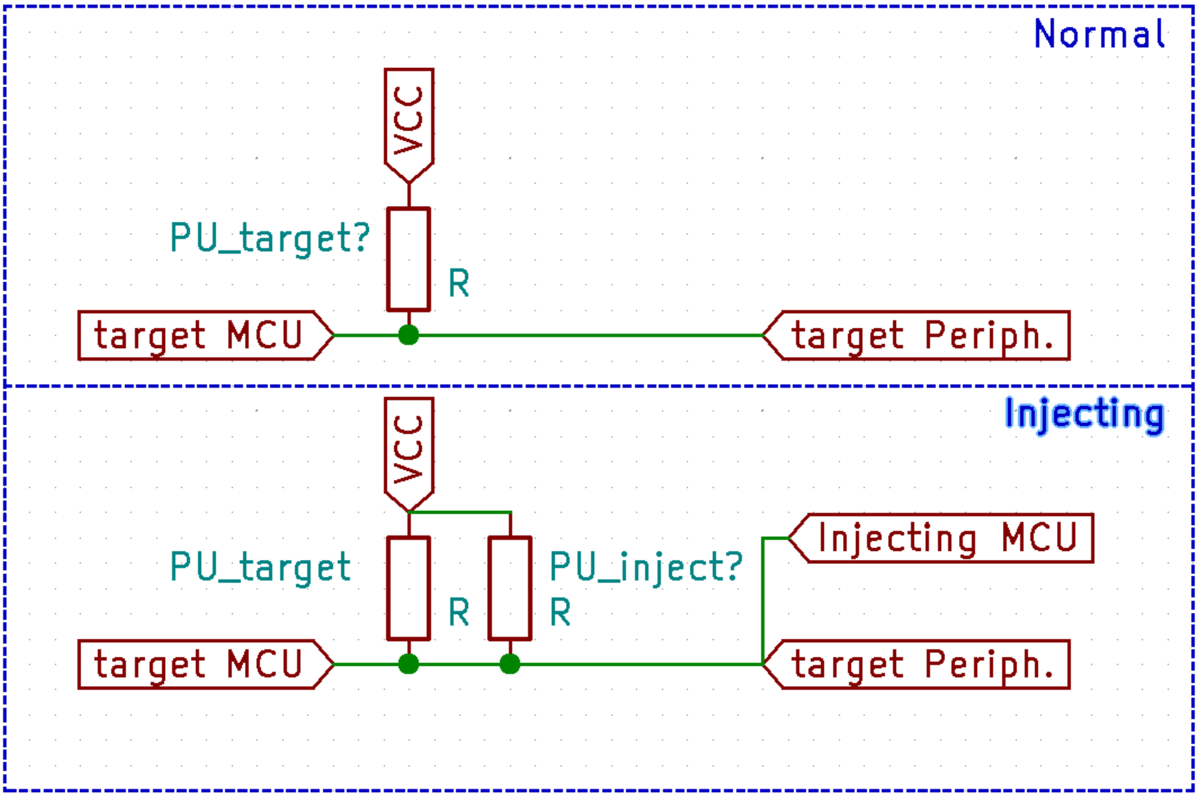

CLOCK
MOSI
MISO
VCC
GND
VCC
GND
VCC
GND
Change
Sample
Change
Sample

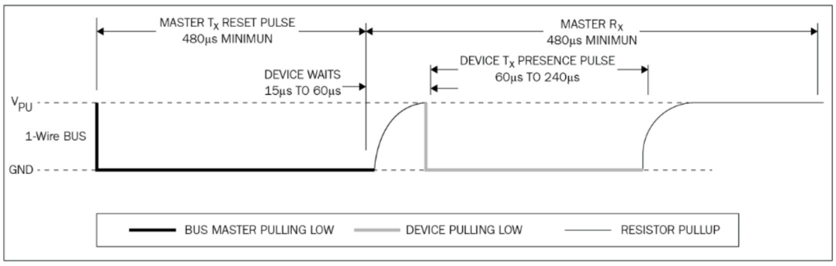

CLOCK
MOSI
MISO
VCC
GND
VCC
GND
VCC
GND
Sample
Change
Sample
Change

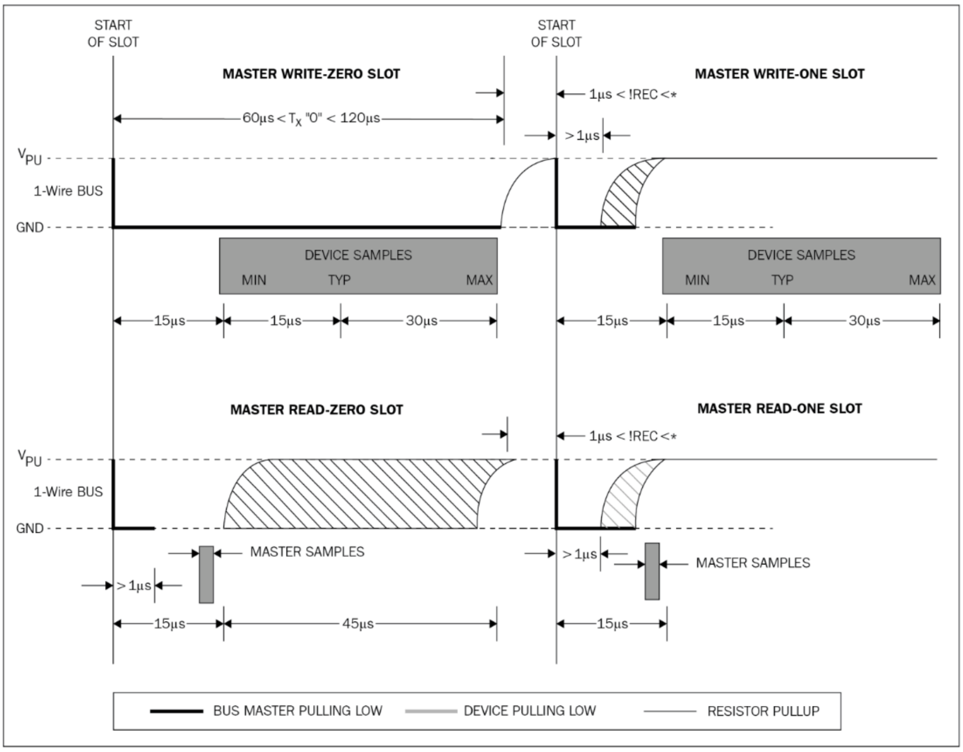

CLOCK
MOSI
MISO
VCC
GND
VCC
GND
VCC
GND
Change
Sample
Change
Sample

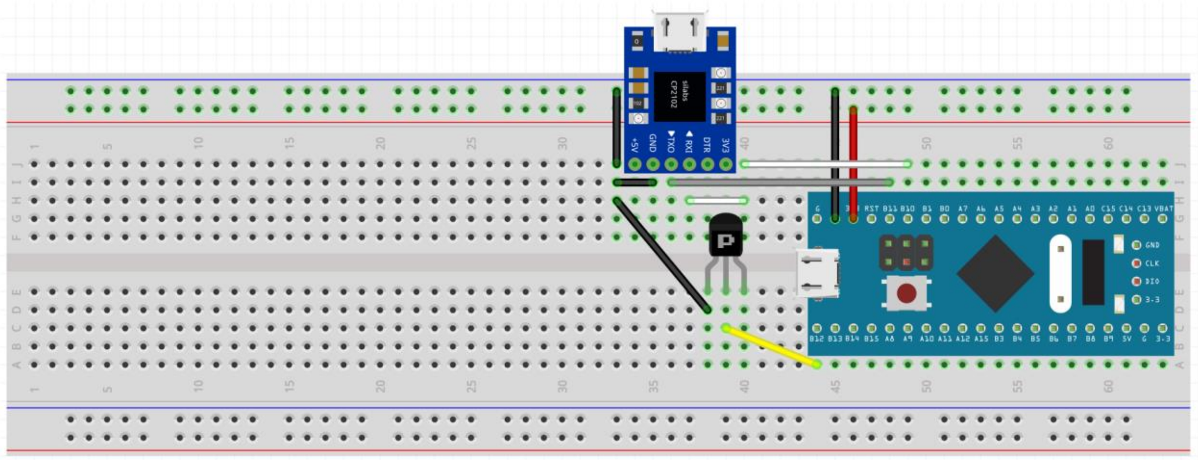

CP2102
25LC128

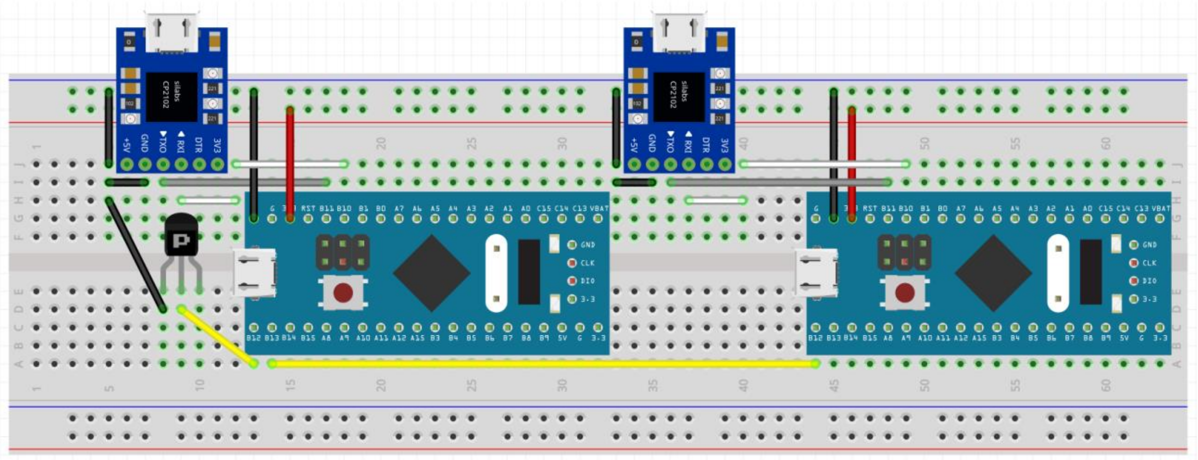

CP2102
25LC128
ritzing

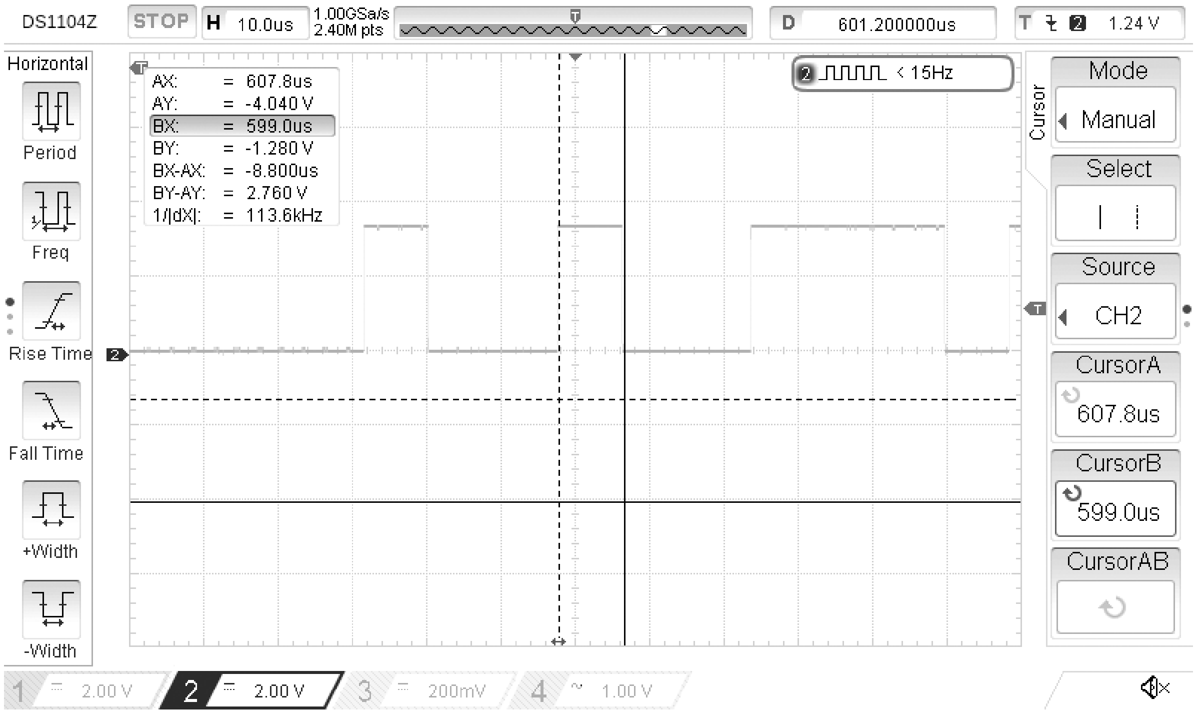

Normal
VCC
PU_target?
R
target MCU
target Periph.
Injecting
VCC
PU_target
R
PU_inject?
R
Injecting MCU
target MCU
target Periph.


MASTER T_X RESET PULSE
480µs MINIMUN
MASTER R_X
480µs MINIMUN
DEVICE WAITS
15µs TO 60µs
DEVICE T_X PRESENCE PULSE
60µs TO 240µs
V_{PU}
1-Wire BUS
GND
BUS MASTER PULLING LOW
DEVICE PULLING LOW
RESISTOR PULLUP


START OF SLOT
START OF SLOT
MASTER WRITE-ZERO SLOT
MASTER WRITE-ONE SLOT
60µs < Tx "0" < 120µs
1µs < !REC < *
> 1µs
VPU
1-Wire BUS
GND
DEVICE SAMPLES
MIN
TYP
MAX
15µs
15µs
30µs
MASTER READ-ZERO SLOT
MASTER READ-ONE SLOT
1µs < !REC < *
MASTER SAMPLES
> 1µs
45µs
BUS MASTER PULLING LOW
DEVICE PULLING LOW
RESISTOR PULLUP


silabs CP2102
+5V
GND
TXO
RXI
DTR
3V3
GND
CLK
DIO
3.3

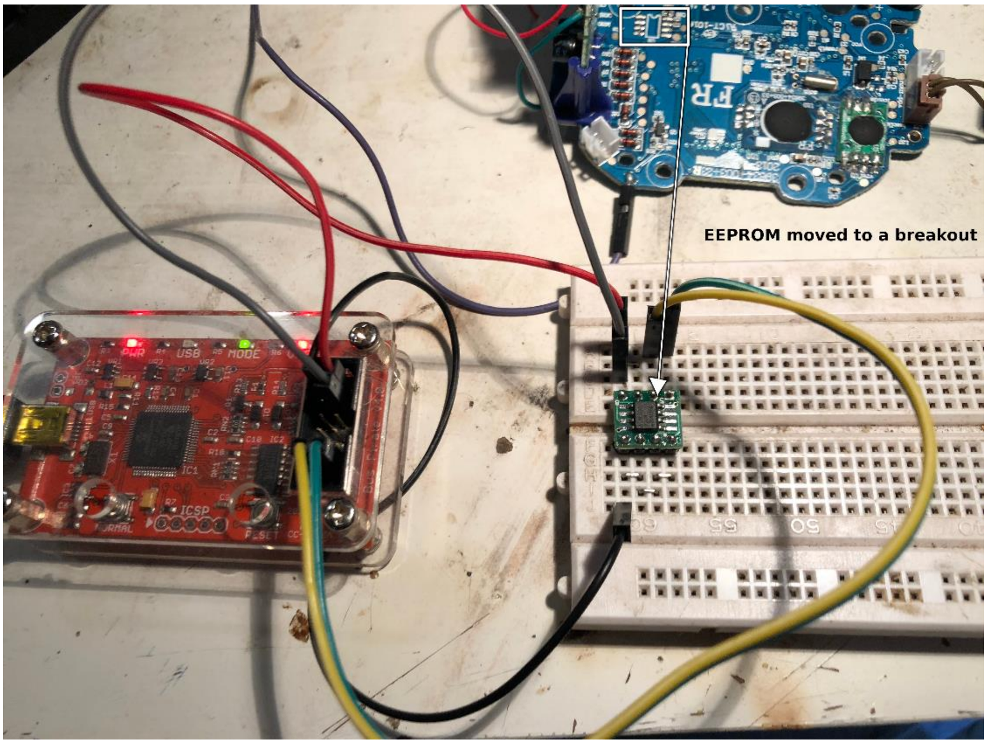

silabs CP2102
+5V
GND
TXO
RXI
DTR
3V3
GND
CLK
DIO
3.3

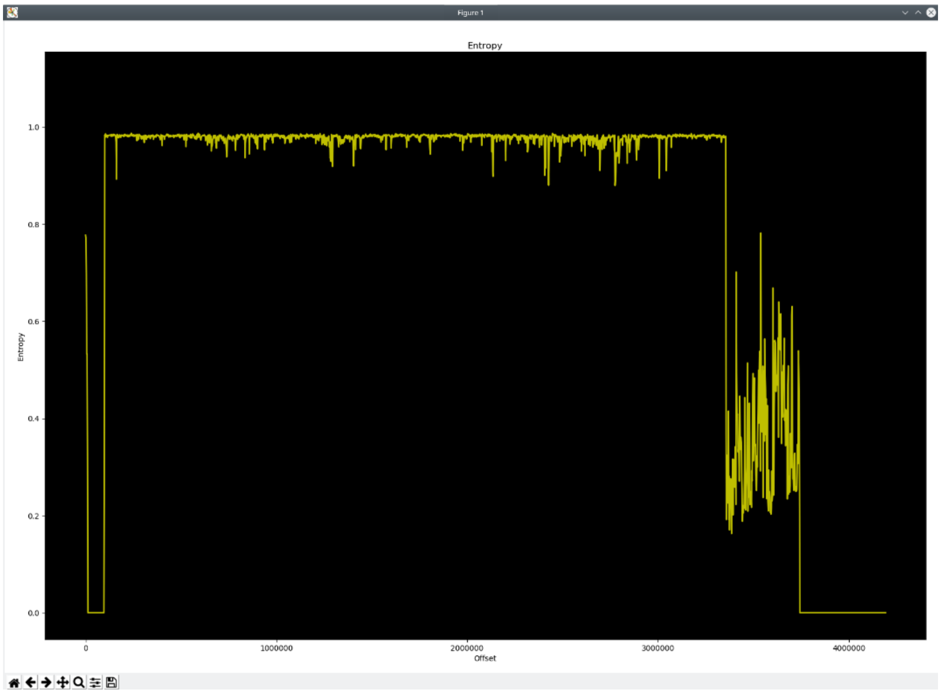


```
AX:      =  607.8us
AY:      =  -4.040 V
BX:      =  599.0us
BY:      =  -1.280 V
BX-AX:   =  -8.800us
BY-AY:   =  2.760 V
1/|dX|:  =  113.6kHz
```

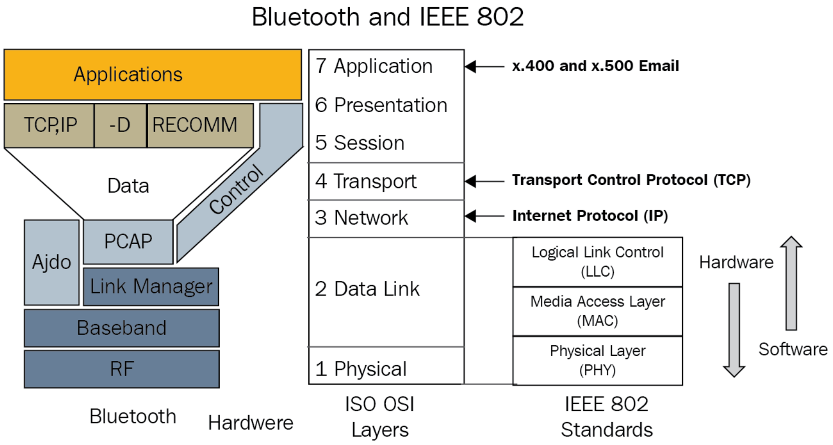
H 10.0us
1.00GSa/s 2.40M pts
D 601.200000us
T 2 1.24 V
Mode: Manual
Source: CH2
CursorA: 607.8us
CursorB: 599.0us
1 2.00 V
2 2.00 V
3 200mV
4 1.00 V

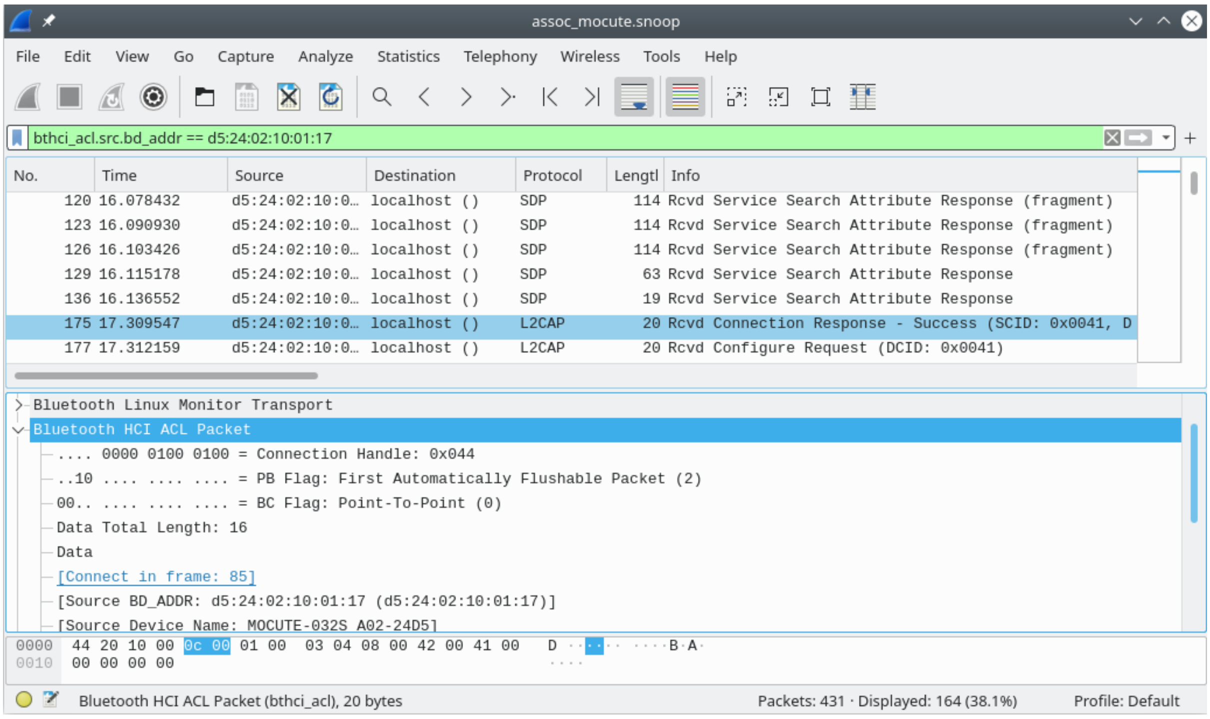
Chapter 7: Extracting and Manipulating Onboard Storage.





Chapter 8: Attacking Wi-Fi, Bluetooth, and BLE.




assoc_mocute.snoop
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

bthci_acl.src.bd_addr == d5:24:02:10:01:17

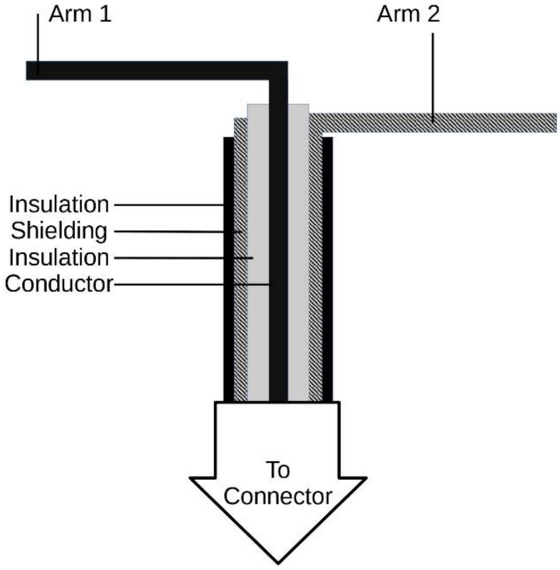
```
No.   Time       Source          Destination   Protocol  Lengtl Info
  120 16.078432  d5:24:02:10:0…  localhost ()  SDP       114 Rcvd Service Search Attribute Response (fragment)
  123 16.090930  d5:24:02:10:0…  localhost ()  SDP       114 Rcvd Service Search Attribute Response (fragment)
  126 16.103426  d5:24:02:10:0…  localhost ()  SDP       114 Rcvd Service Search Attribute Response (fragment)
  129 16.115178  d5:24:02:10:0…  localhost ()  SDP        63 Rcvd Service Search Attribute Response
  136 16.136552  d5:24:02:10:0…  localhost ()  SDP        19 Rcvd Service Search Attribute Response
  175 17.309547  d5:24:02:10:0…  localhost ()  L2CAP      20 Rcvd Connection Response - Success (SCID: 0x0041, D
  177 17.312159  d5:24:02:10:0…  localhost ()  L2CAP      20 Rcvd Configure Request (DCID: 0x0041)
```

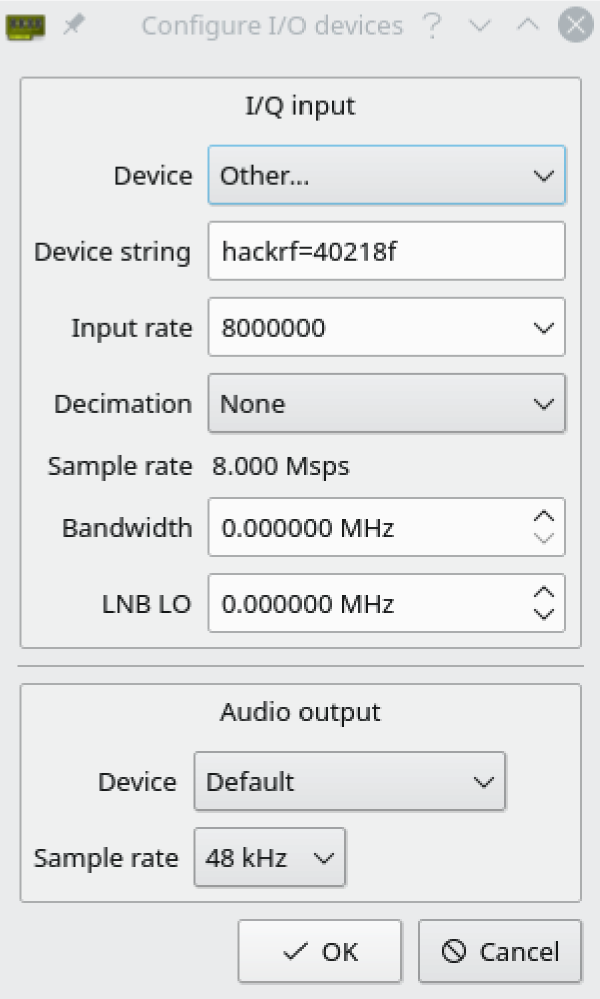
```
> Bluetooth Linux Monitor Transport
v Bluetooth HCI ACL Packet
    .... 0000 0100 0100 = Connection Handle: 0x044
    ..10 .... .... .... = PB Flag: First Automatically Flushable Packet (2)
    00.. .... .... .... = BC Flag: Point-To-Point (0)
    Data Total Length: 16
    Data
    [Connect in frame: 85]
    [Source BD_ADDR: d5:24:02:10:01:17 (d5:24:02:10:01:17)]
    [Source Device Name: MOCUTE-032S A02-24D5]
```

```
0000  44 20 10 00 0c 00 01 00  03 04 08 00 42 00 41 00   D·······  ····B·A·
0010  00 00 00 00                                        ····
```

Bluetooth HCI ACL Packet (bthci_acl), 20 bytes   Packets: 431 · Displayed: 164 (38.1%)   Profile: Default

Chapter 9: Software-Defined Radio Attacks.





I/Q input

Device: Other...

Device string: hackrf=40218f

Input rate: 8000000

Decimation: None

Sample rate: 8.000 Msps

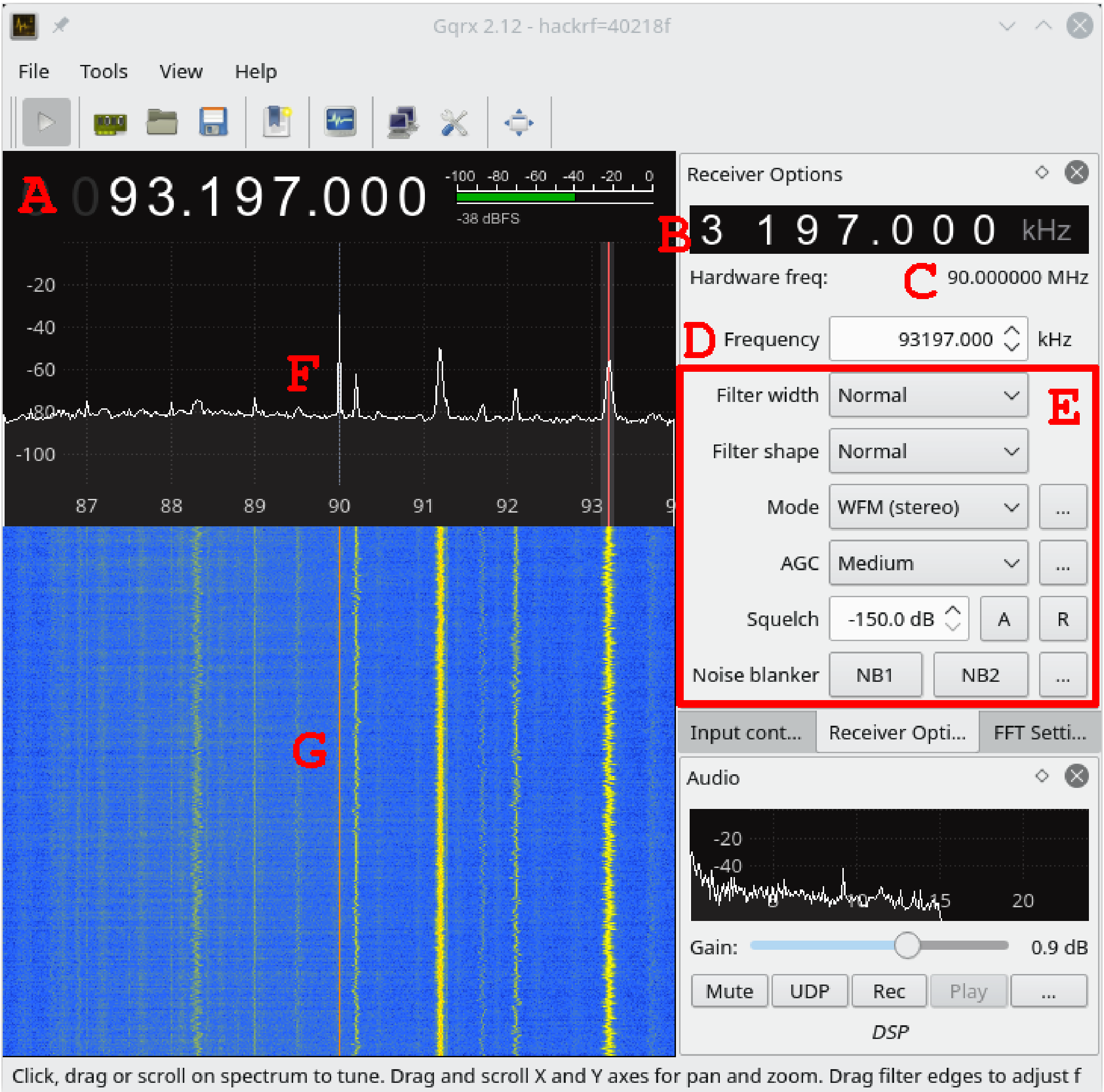
Bandwidth: 0.000000 MHz

LNB LO: 0.000000 MHz

Audio output

Device: Default

Sample rate: 48 kHz


Gqrx 2.12 - hackrf=40218f

Receiver Options

3 197.000 kHz

Hardware freq: 90.000000 MHz

Frequency 93197.000 kHz

Filter width: Normal

Filter shape: Normal

Mode: WFM (stereo)

AGC: Medium

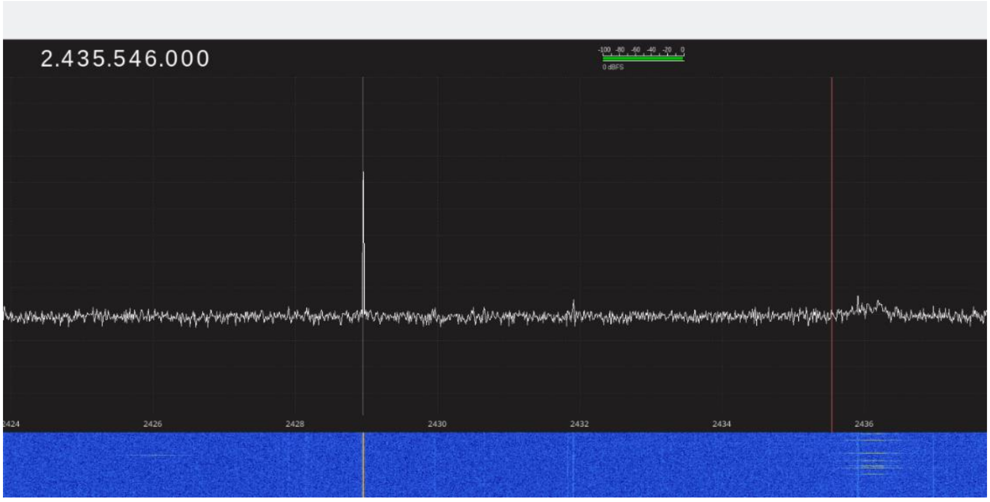
Squelch: -150.0 dB

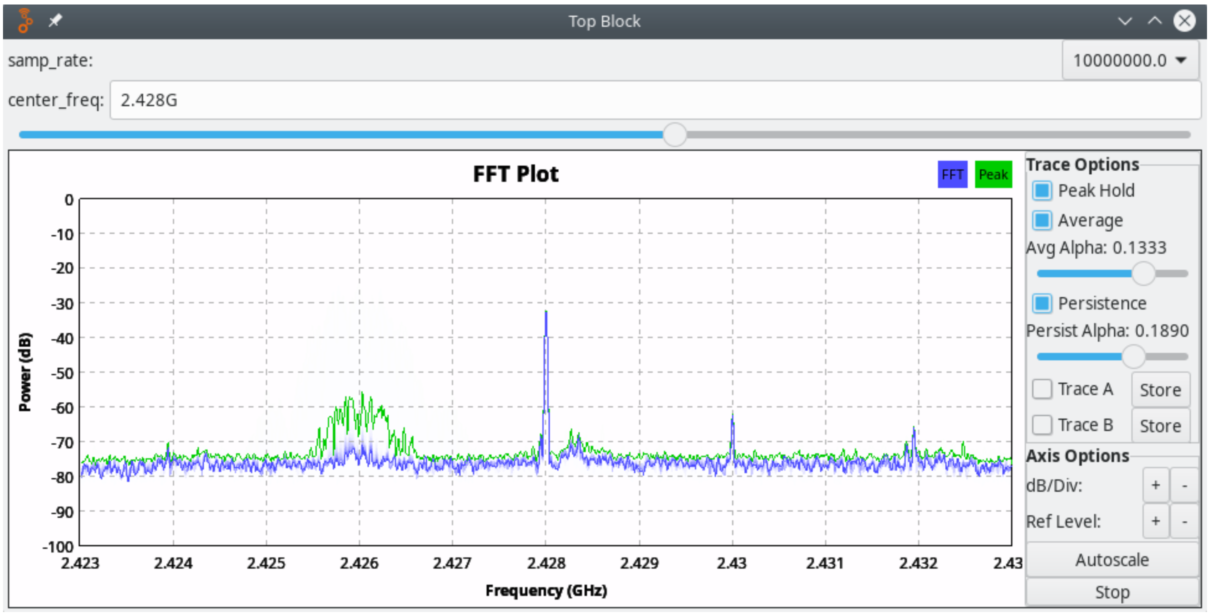
Noise blanker: NB1 NB2

Audio

Gain: 0.9 dB

Click, drag or scroll on spectrum to tune. Drag and scroll X and Y axes for pan and zoom. Drag filter edges to adjust f


2.435.546.000



samp_rate: 10000000.0

center_freq: 2.428G

☑ Peak Hold

☑ Average

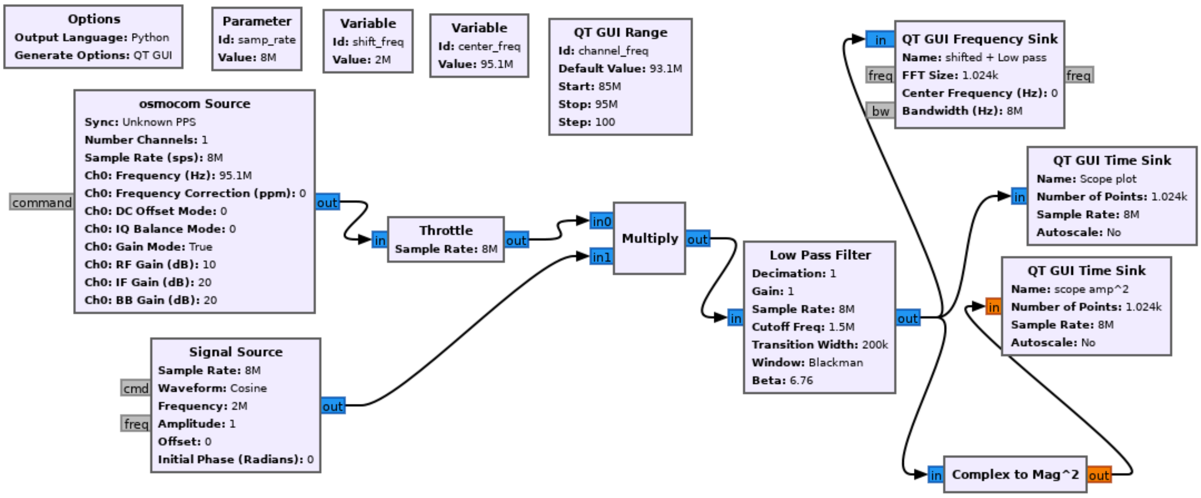
Avg Alpha: 0.1333

☑ Persistence

Persist Alpha: 0.1890

□ Trace A

□ Trace B



Options
Output Language: Python
Generate Options: QT GUI

Parameter
Id: samp_rate
Value: 8M

Variable
Id: shift_freq
Value: 2M

Variable
Id: center_freq
Value: 95.1M

QT GUI Range
Id: channel_freq
Default Value: 93.1M
Start: 85M
Stop: 95M
Step: 100

QT GUI Frequency Sink
Name: shifted + Low pass
FFT Size: 1.024k
Center Frequency (Hz): 0
Bandwidth (Hz): 8M

osmocom Source
Sync: Unknown PPS
Number Channels: 1
Sample Rate (sps): 8M
Ch0: Frequency (Hz): 95.1M
Ch0: Frequency Correction (ppm): 0
Ch0: DC Offset Mode: 0
Ch0: IQ Balance Mode: 0
Ch0: Gain Mode: True
Ch0: RF Gain (dB): 10
Ch0: IF Gain (dB): 20
Ch0: BB Gain (dB): 20

Throttle
Sample Rate: 8M

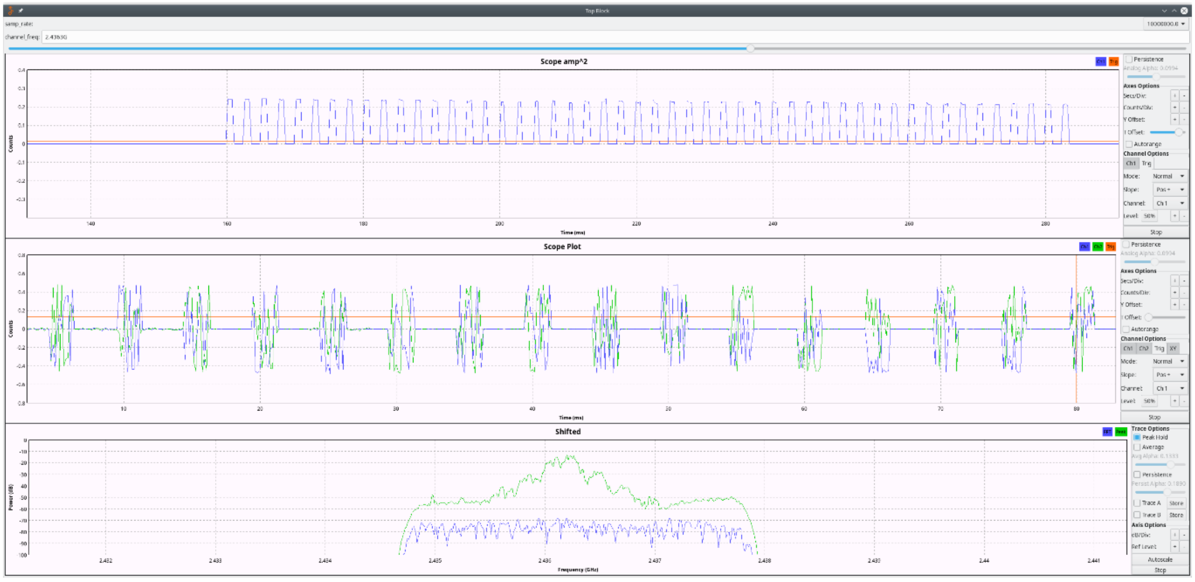
Multiply

QT GUI Time Sink
Name: Scope plot
Number of Points: 1.024k
Sample Rate: 8M
Autoscale: No

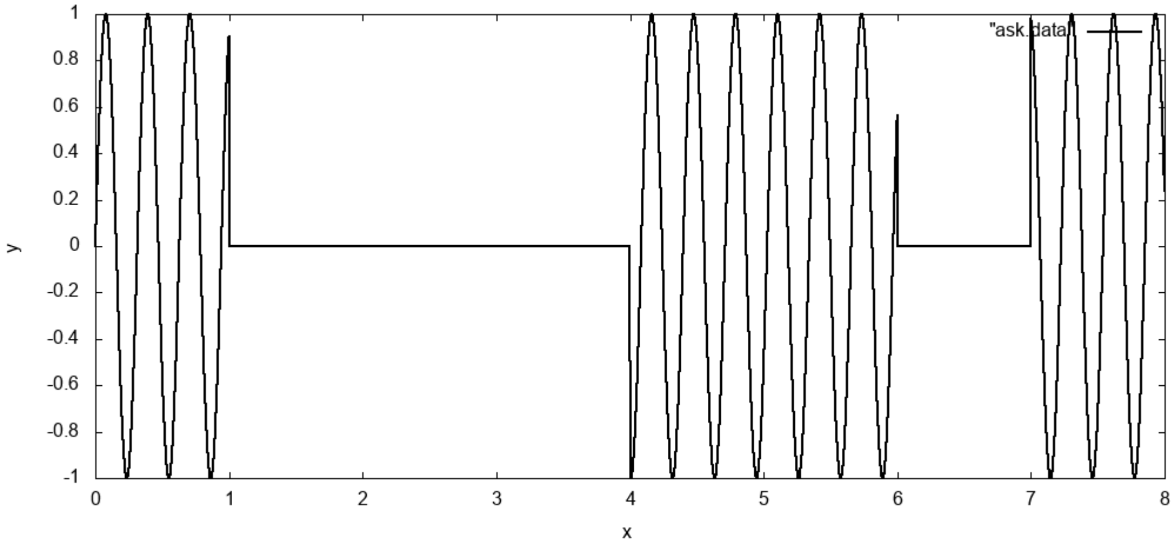
QT GUI Time Sink
Name: scope amp^2
Number of Points: 1.024k
Sample Rate: 8M
Autoscale: No

Low Pass Filter
Decimation: 1
Gain: 1
Sample Rate: 8M
Cutoff Freq: 1.5M
Transition Width: 200k
Window: Blackman
Beta: 6.76

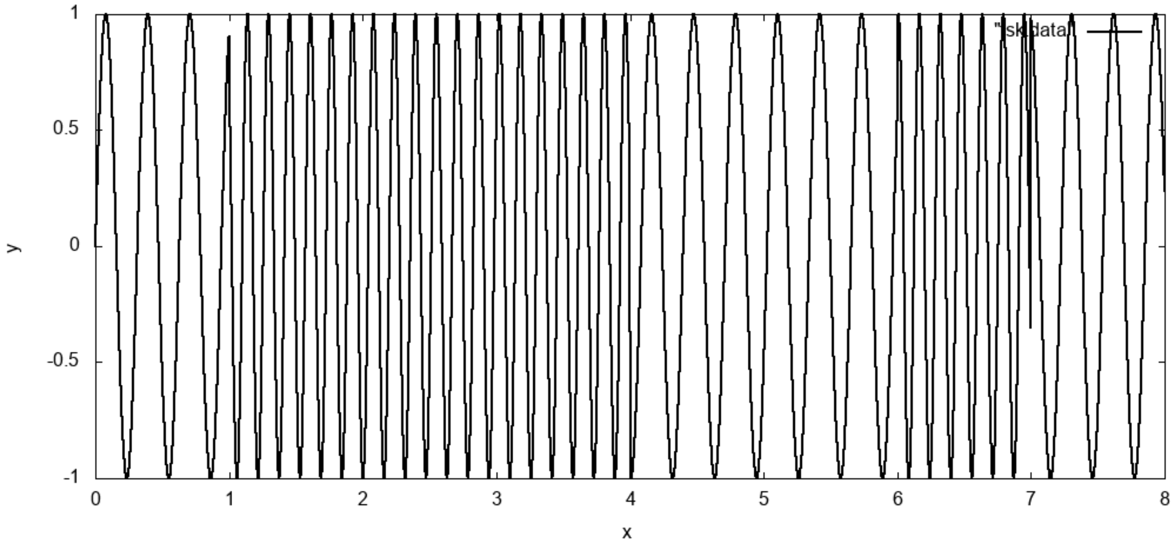
Signal Source
Sample Rate: 8M
Waveform: Cosine
Frequency: 2M
Amplitude: 1
Offset: 0
Initial Phase (Radians): 0

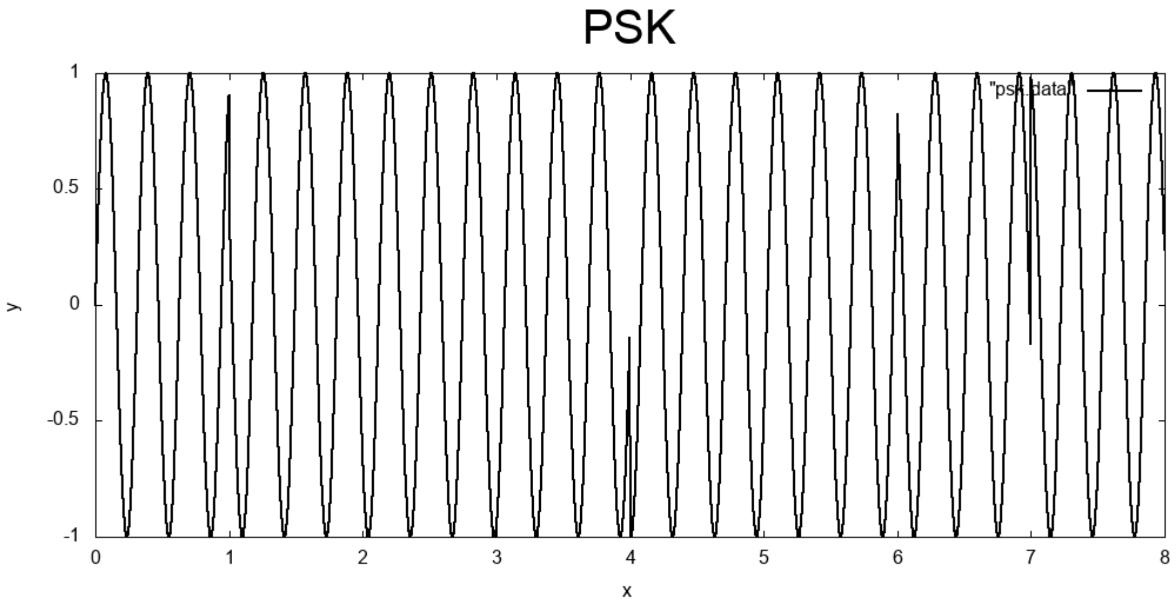


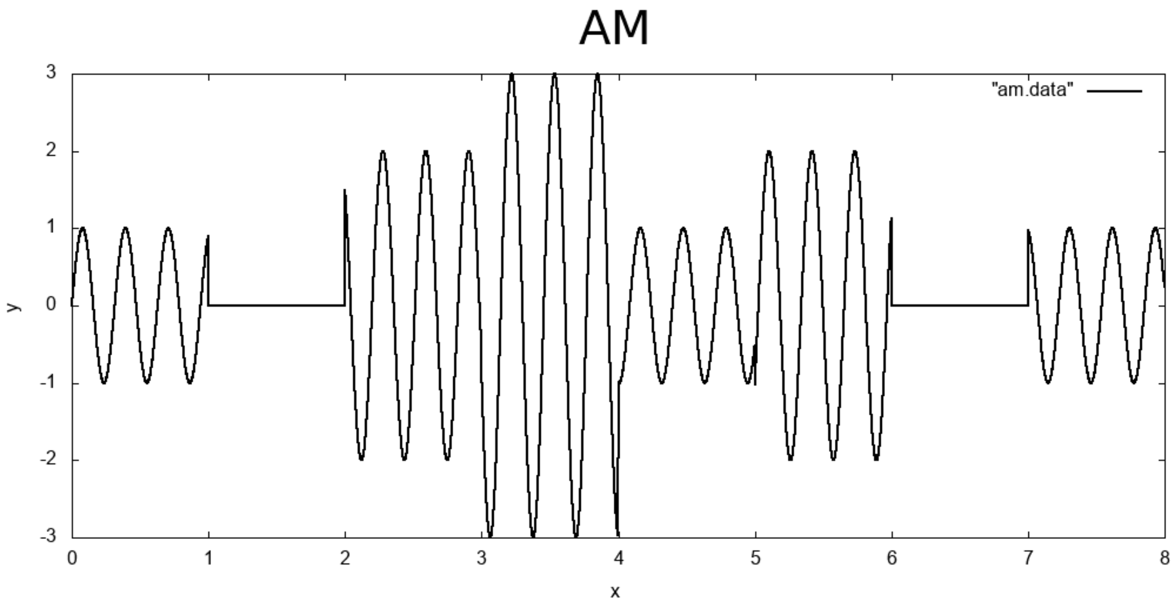
ASK

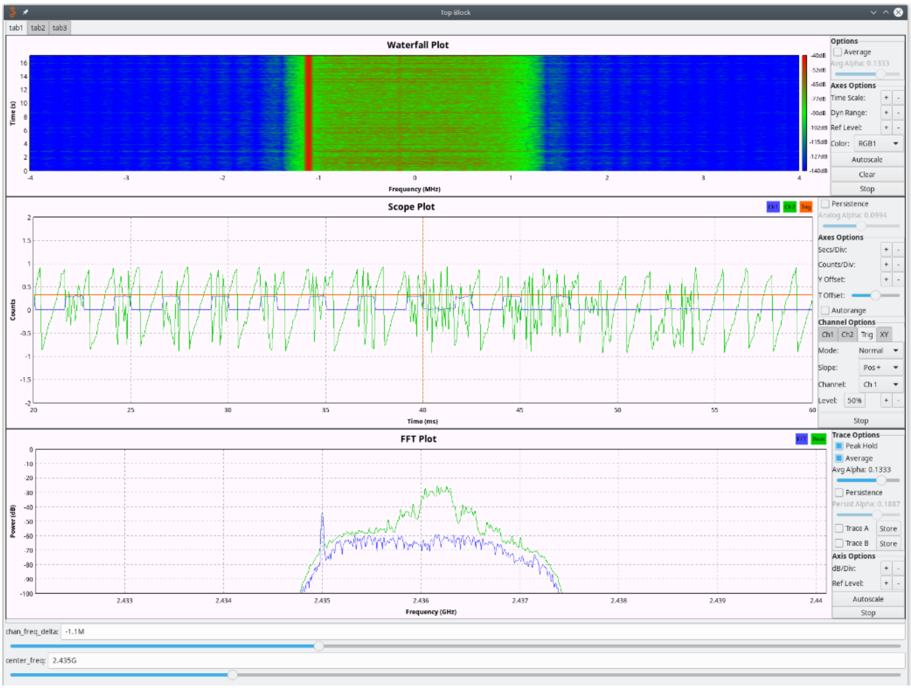

"ask.data"
y
1
0.8
0.6
0.4
0.2
0
-0.2
-0.4
-0.6
-0.8
-1
0
1
2
3
4
5
6
7
8
x

FSK


"fsk.data"
y
1
0.5
0
-0.5
-1
0
1
2
3
4
5
6
7
8
x


PSK
"psk.data"
y
1
0.5
0
-0.5
-1
0
1
2
3
4
5
6
7
8
x


AM
"am.data"
y
3
2
1
0
-1
-2
-3
0
1
2
3
4
5
6
7
8
x



Color: RGB1

Mode: Normal

Slope: Pos+

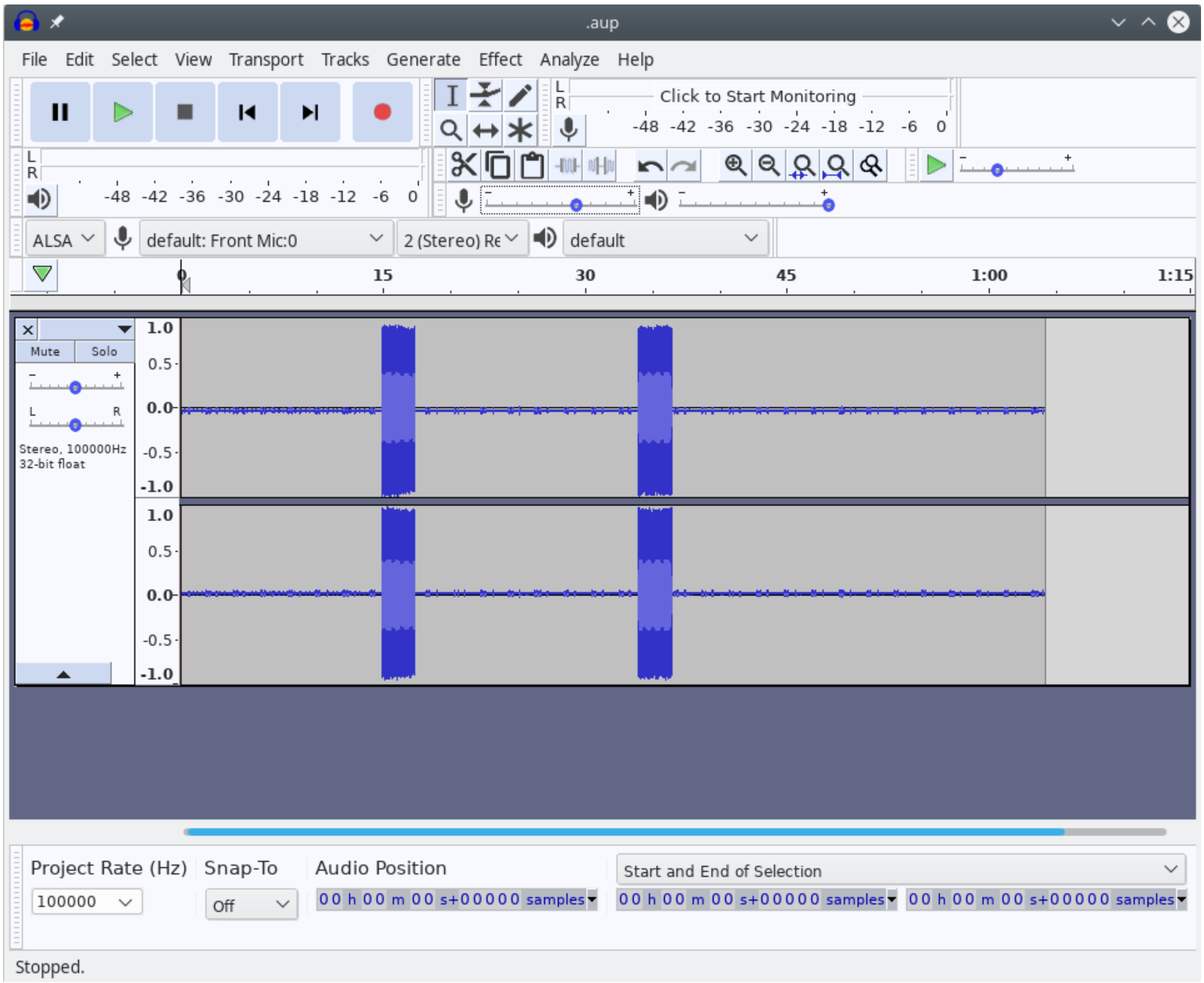
Channel: Ch1

Level: 50%

Avg Alpha: 0.1333

chan_freq_delta: -1.1M

center_freq: 2.435G



ALSA

default: Front Mic:0

2 (Stereo) Re

default

Stereo, 100000Hz
32-bit float

Project Rate (Hz) 100000

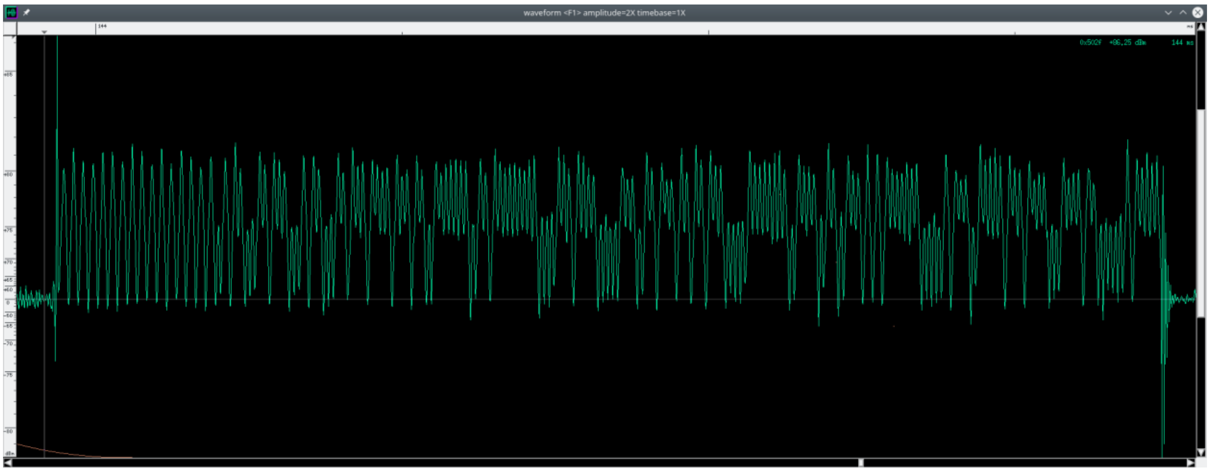
Snap-To Off

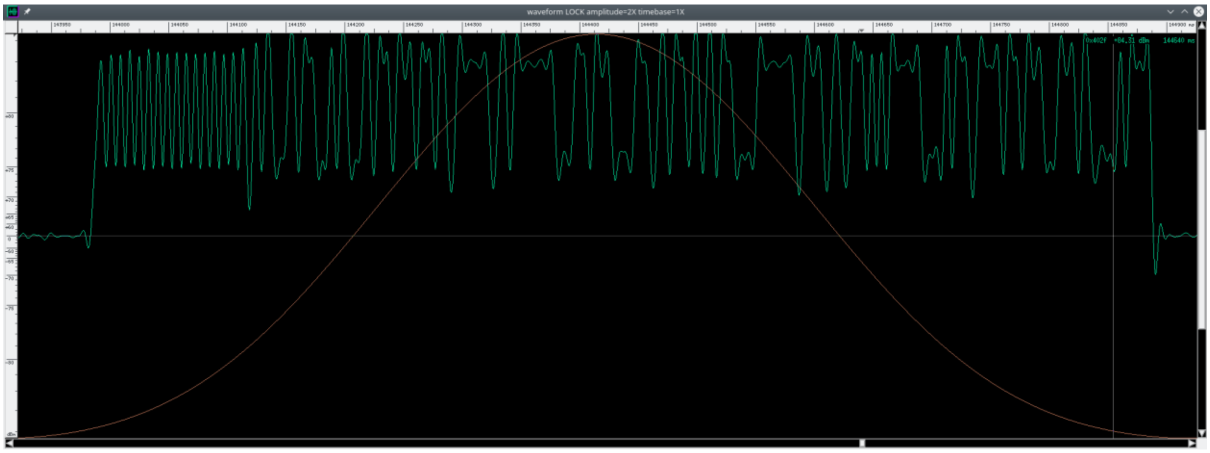
00 h 00 m 00 s+00000 samples

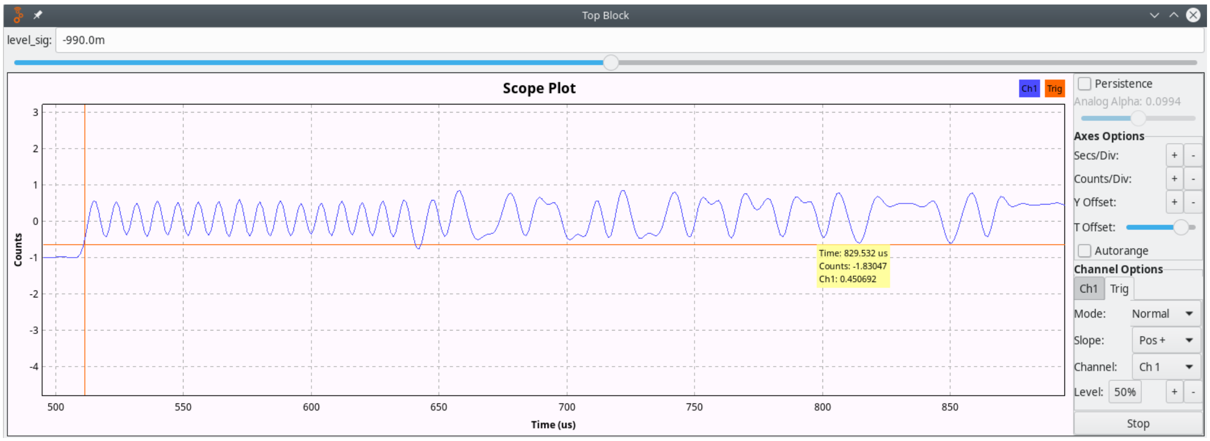
00 h 00 m 00 s+00000 samples

00 h 00 m 00 s+00000 samples

Stopped.







level_sig: -990.0m

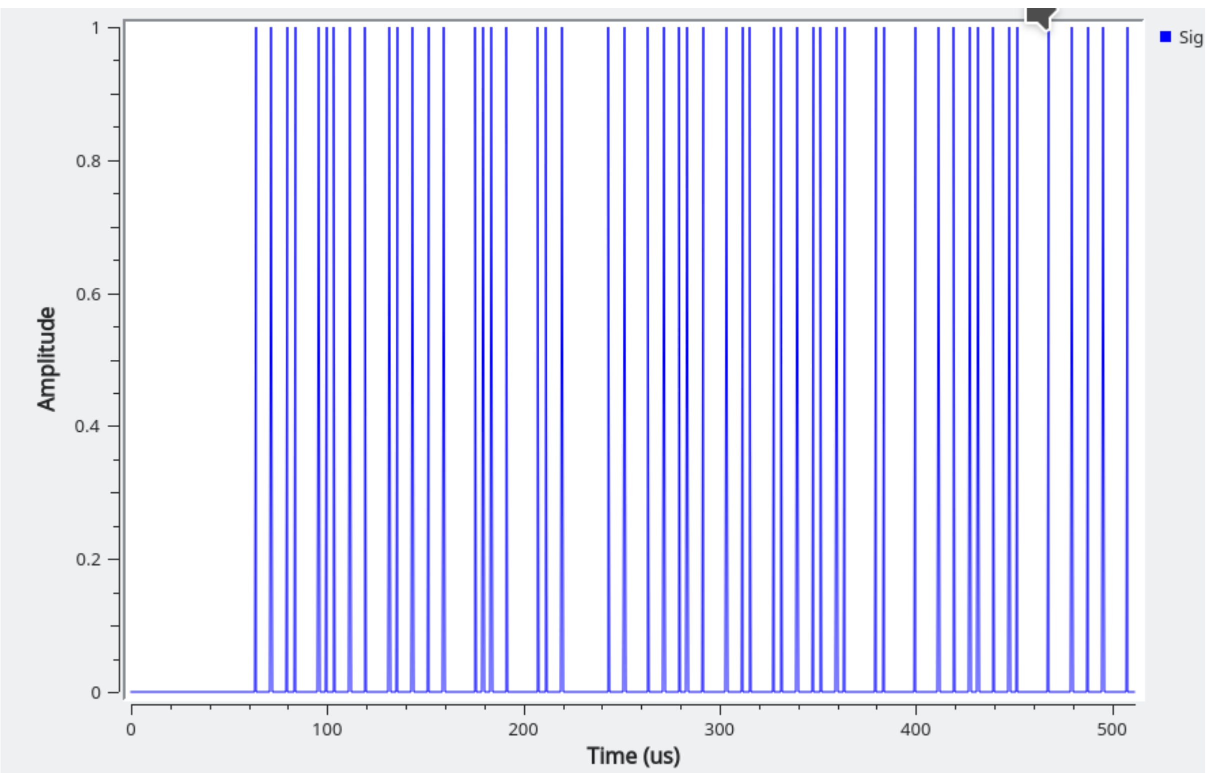
Time: 829.532 us
Counts: -1.83047
Ch1: 0.450692

□ Persistence
Analog Alpha: 0.0994

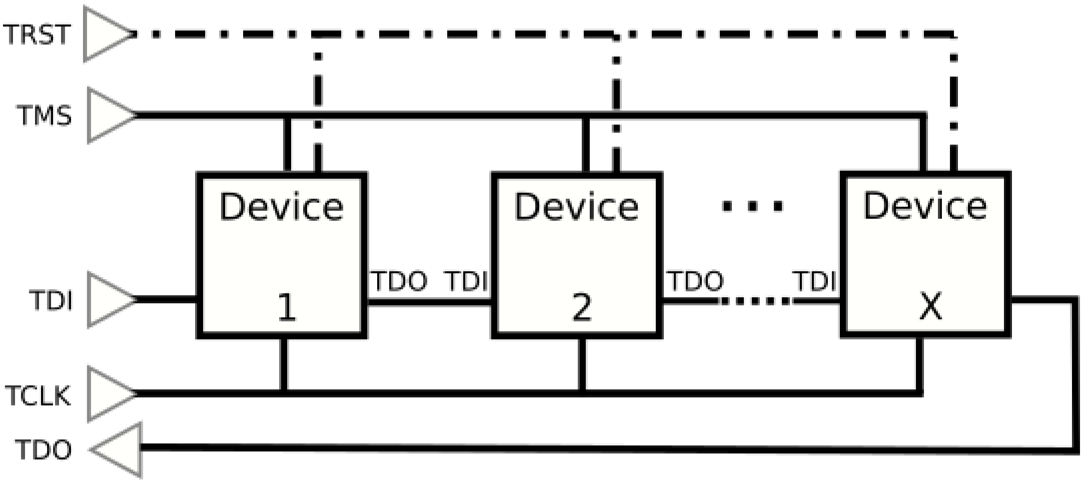
Secs/Div: + -
Counts/Div: + -
Y Offset: + -
T Offset:

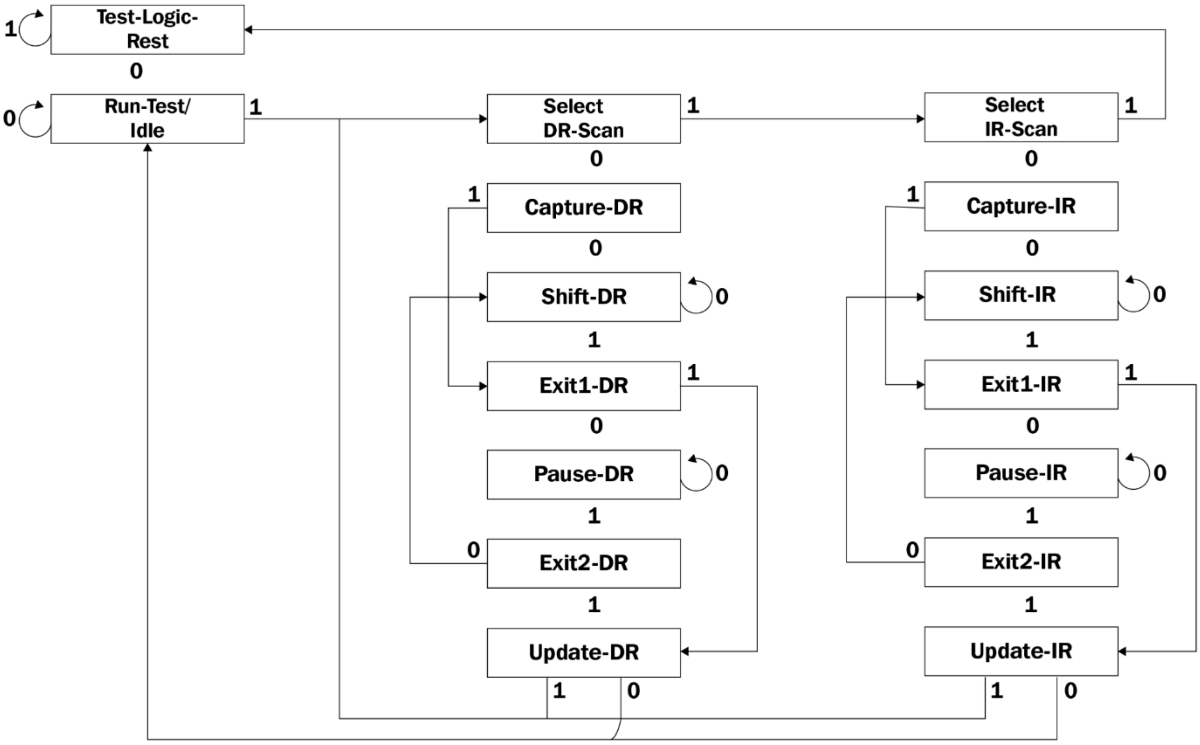
□ Autorange

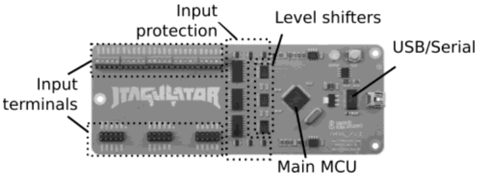
Mode: Normal
Slope: Pos +
Channel: Ch 1
Level: 50% + -

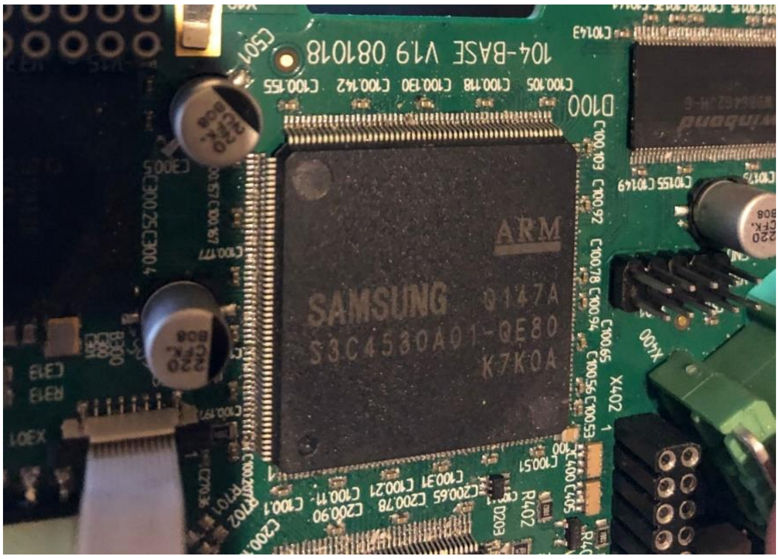

Amplitude
1
0.8
0.6
0.4
0.2
0
0
100
200
300
400
500
Time (us)
■ Sig

Chapter 10: Accessing the Debug Interfaces.

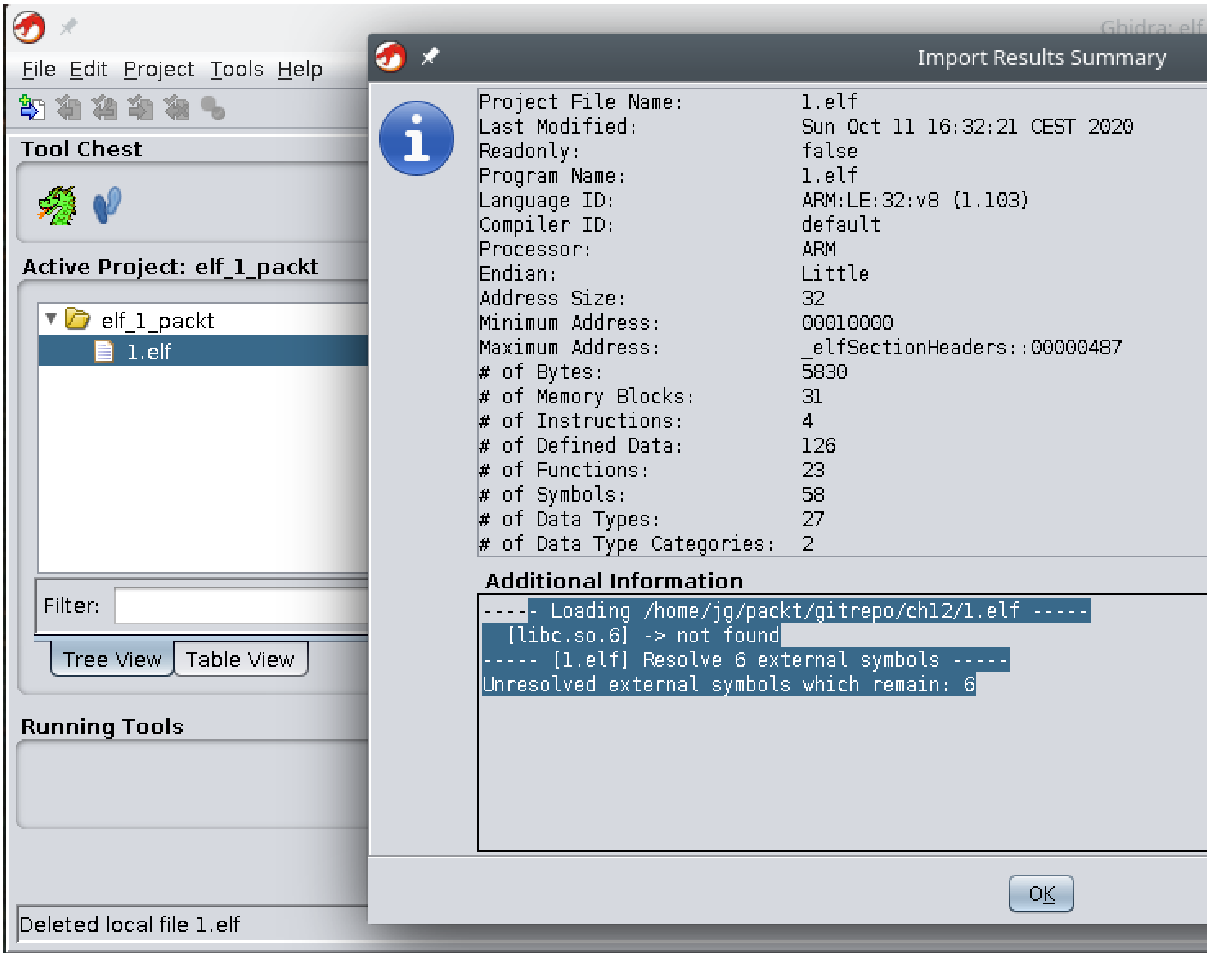






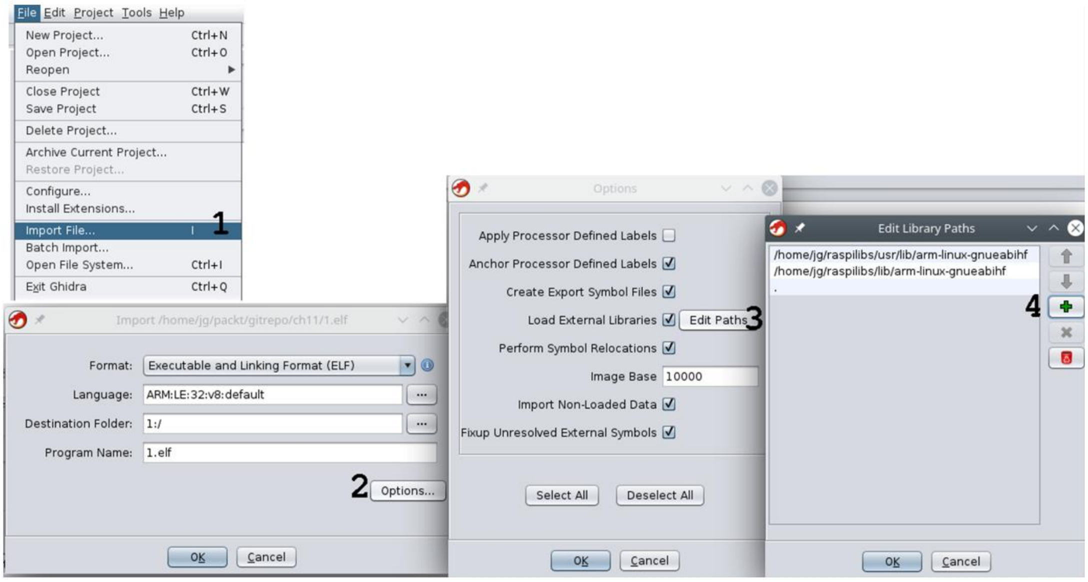

104-BASE V1.9 081018
D100
ARM
SAMSUNG
Q147A
S3C4530A01-QE80
K7K0A
X402
X400
R402

Chapter 11: Static Reverse Engineering and Analysis.



```
Project File Name:          1.elf
Last Modified:              Sun Oct 11 16:32:21 CEST 2020
Readonly:                   false
Program Name:               1.elf
Language ID:                ARM:LE:32:v8 (1.103)
Compiler ID:                default
Processor:                  ARM
Endian:                     Little
Address Size:               32
Minimum Address:            00010000
Maximum Address:            _elfSectionHeaders::00000487
# of Bytes:                 5830
# of Memory Blocks:         31
# of Instructions:          4
# of Defined Data:          126
# of Functions:             23
# of Symbols:               58
# of Data Types:            27
# of Data Type Categories:  2
```

```
----- Loading /home/jg/packt/gitrepo/ch12/1.elf -----
   [libc.so.6] -> not found
----- [1.elf] Resolve 6 external symbols -----
Unresolved external symbols which remain: 6
```



Format: Executable and Linking Format (ELF)

Language: ARM:LE:32:v8:default

Destination Folder: 1:/

Program Name: 1.elf

Apply Processor Defined Labels ☐

Anchor Processor Defined Labels ☑

Create Export Symbol Files ☑

Load External Libraries ☑

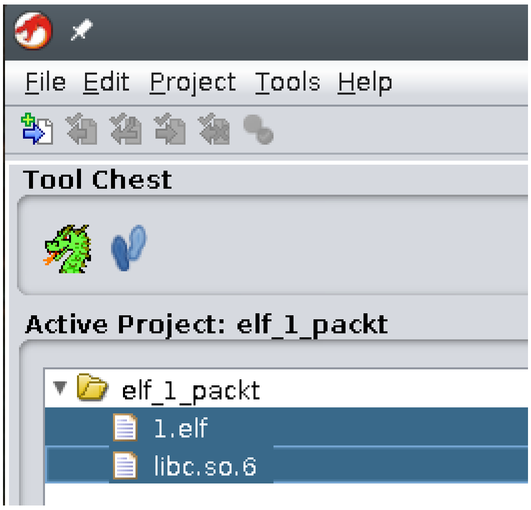
Perform Symbol Relocations ☑

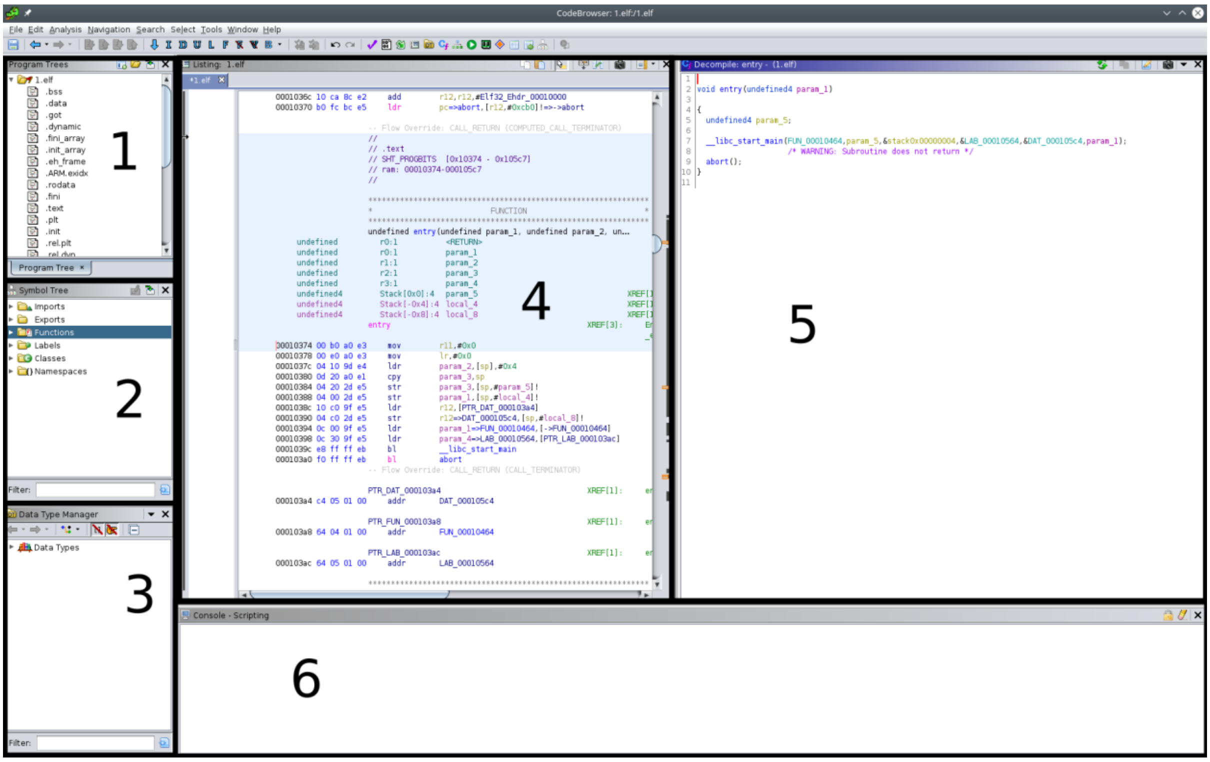
Image Base 10000

Import Non-Loaded Data ☑

Fixup Unresolved External Symbols ☑

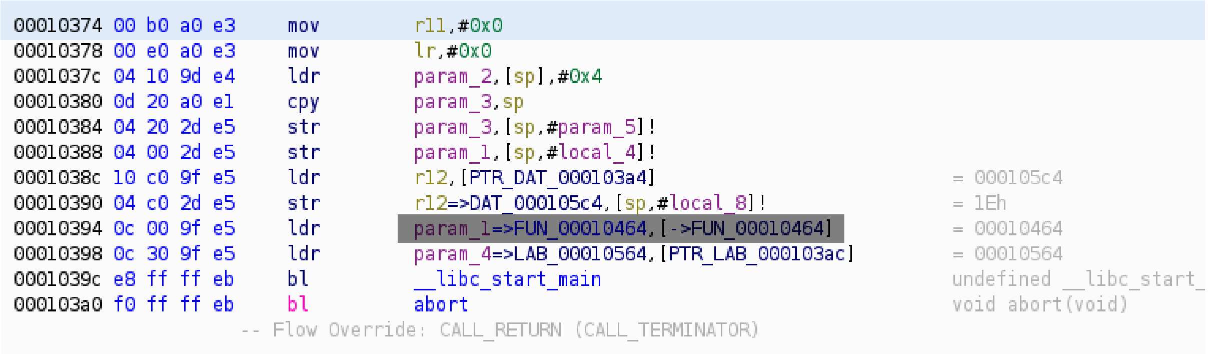
/home/jg/raspilibs/usr/lib/arm-linux-gnueabihf
/home/jg/raspilibs/lib/arm-linux-gnueabihf
.



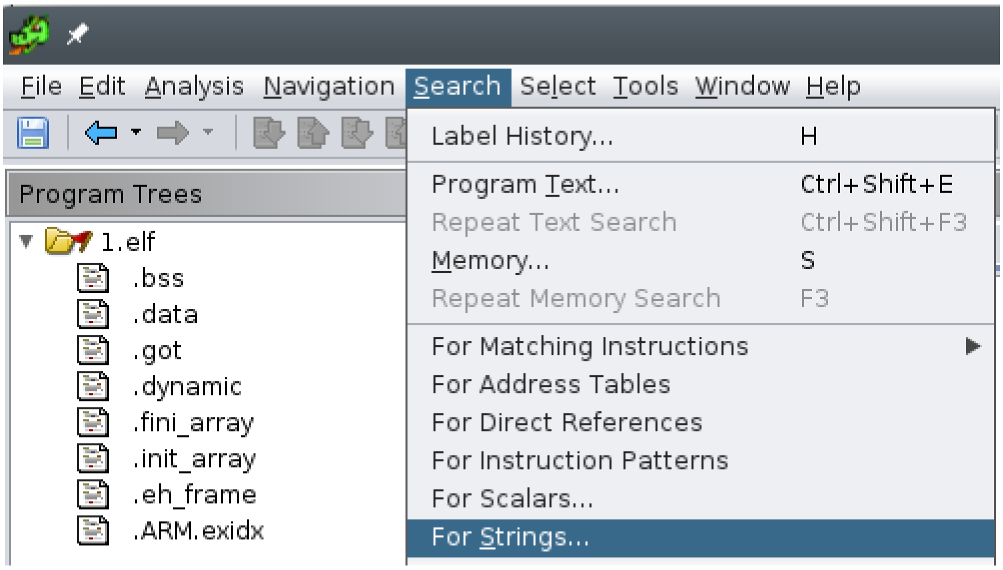


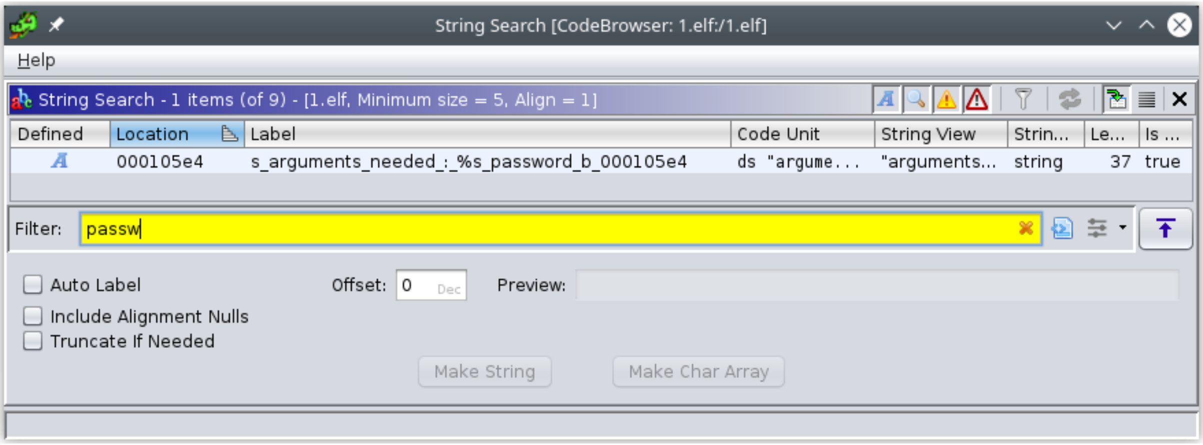
```
0001036c 10 ca 8c e2     add          r12,r12,#Elf32_Ehdr_00010000
00010370 b0 fc bc e5     ldr          pc=>abort,[r12,#0xcb0]!=>->abort

                      -- Flow Override: CALL_RETURN (COMPUTED_CALL_TERMINATOR)
                      //
                      // .text
                      // SHT_PROGBITS  [0x10374 - 0x105c7]
                      // ram: 00010374-000105c7
                      //

                      **************************************************************
                      *                          FUNCTION                          *
                      **************************************************************
                      undefined entry(undefined param_1, undefined param_2, un...
        undefined         r0:1           <RETURN>
        undefined         r0:1           param_1
        undefined         r1:1           param_2
        undefined         r2:1           param_3
        undefined         r3:1           param_4
        undefined4        Stack[0x0]:4   param_5
        undefined4        Stack[-0x4]:4  local_4
        undefined4        Stack[-0x8]:4  local_8
                      entry                                         XREF[3]:

00010374 00 b0 a0 e3     mov          r11,#0x0
00010378 00 e0 a0 e3     mov          lr,#0x0
0001037c 04 10 9d e4     ldr          param_2,[sp],#0x4
00010380 0d 20 a0 e1     cpy          param_3,sp
00010384 04 20 2d e5     str          param_3,[sp,#param_5]!
00010388 04 00 2d e5     str          param_1,[sp,#local_4]!
0001038c 10 c0 9f e5     ldr          r12,[PTR_DAT_000103a4]
00010390 04 c0 2d e5     str          r12=>DAT_000105c4,[sp,#local_8]!
00010394 0c 00 9f e5     ldr          param_1=>FUN_00010464,[->FUN_00010464]
00010398 0c 30 9f e5     ldr          param_4=>LAB_00010564,[PTR_LAB_000103ac]
0001039c e8 ff ff eb     bl           __libc_start_main
000103a0 f0 ff ff eb     bl           abort
                      -- Flow Override: CALL_RETURN (CALL_TERMINATOR)

                      PTR_DAT_000103a4                              XREF[1]:
000103a4 c4 05 01 00     addr         DAT_000105c4

                      PTR_FUN_000103a8                              XREF[1]:
000103a8 64 04 01 00     addr         FUN_00010464

                      PTR_LAB_000103ac                              XREF[1]:
000103ac 64 05 01 00     addr         LAB_00010564
```

```

void entry(undefined4 param_1)

{
  undefined4 param_5;

  __libc_start_main(FUN_00010464,param_5,&stack0x00000004,&LAB_00010564,&DAT_000105c4,param_1);
                    /* WARNING: Subroutine does not return */
  abort();
}

```



```
00010374 00 b0 a0 e3     mov          r11,#0x0
00010378 00 e0 a0 e3     mov          lr,#0x0
0001037c 04 10 9d e4     ldr          param_2,[sp],#0x4
00010380 0d 20 a0 e1     cpy          param_3,sp
00010384 04 20 2d e5     str          param_3,[sp,#param_5]!
00010388 04 00 2d e5     str          param_1,[sp,#local_4]!
0001038c 10 c0 9f e5     ldr          r12,[PTR_DAT_000103a4]                    = 000105c4
00010390 04 c0 2d e5     str          r12=>DAT_000105c4,[sp,#local_8]!          = 1Eh
00010394 0c 00 9f e5     ldr          param_1=>FUN_00010464,[->FUN_00010464]    = 00010464
00010398 0c 30 9f e5     ldr          param_4=>LAB_00010564,[PTR_LAB_000103ac]  = 00010564
0001039c e8 ff ff eb     bl           __libc_start_main                         undefined __libc_start_
000103a0 f0 ff ff eb     bl           abort                                     void abort(void)
                  -- Flow Override: CALL_RETURN (CALL_TERMINATOR)
```




String Search [CodeBrowser: 1.elf:/1.elf]
Help
String Search - 1 items (of 9) - [1.elf, Minimum size = 5, Align = 1]

Defined	Location	Label	Code Unit	String View	Strin...	Le...	Is ...
A	000105e4	s_arguments_needed_:_%s_password_b_000105e4	ds "argume...	"arguments...	string	37	true

Filter: passw

☐ Auto Label

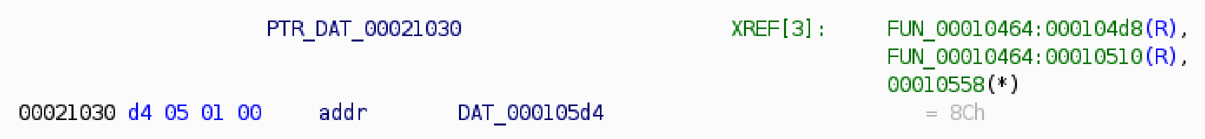
☐ Include Alignment Nulls

☐ Truncate If Needed

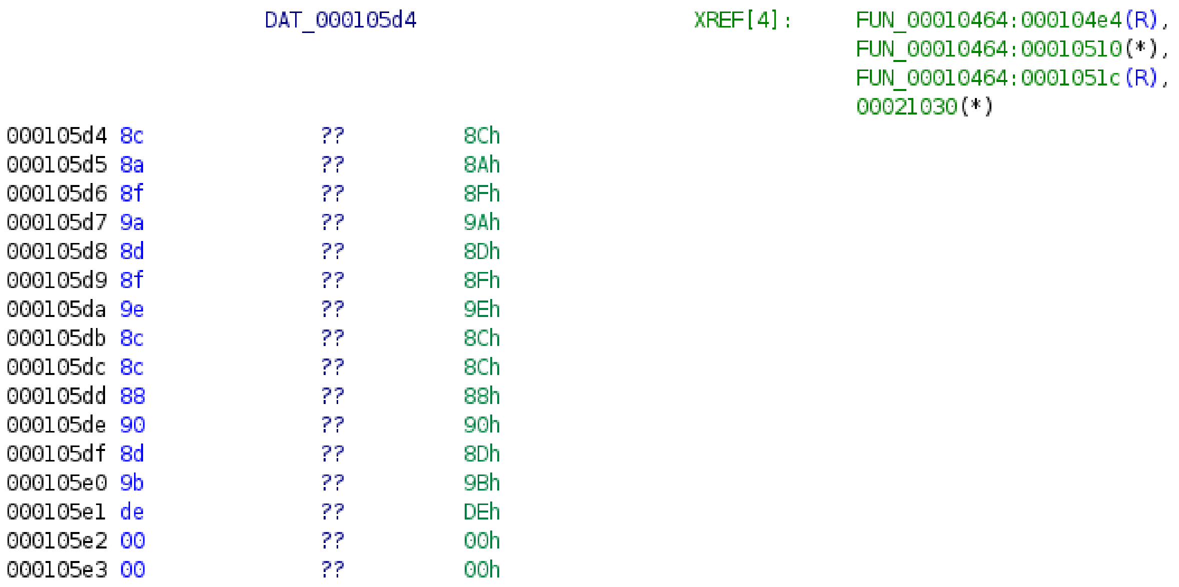
Offset: 0 Dec

Preview:

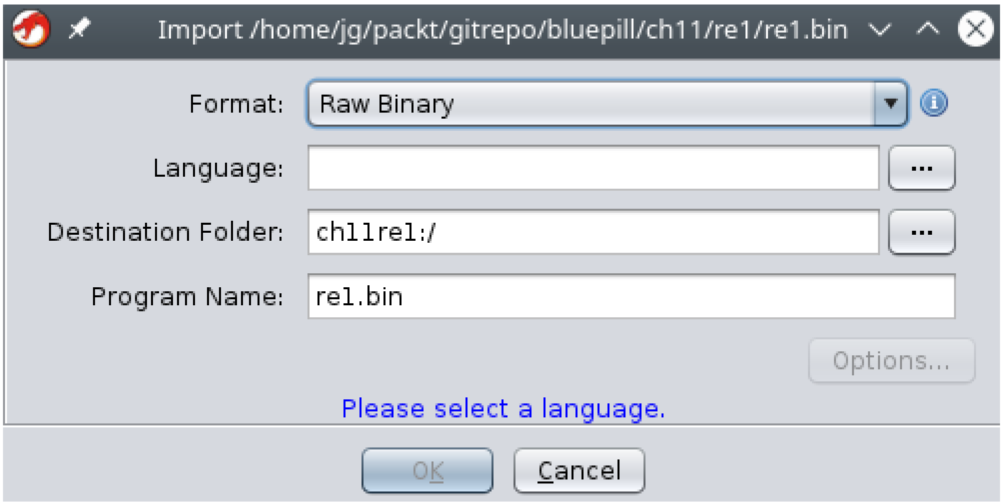
Make String
Make Char Array



```
                     PTR_DAT_00021030                        XREF[3]:     FUN_00010464:000104d8(R),
                                                                          FUN_00010464:00010510(R),
                                                                          00010558(*)
00021030 d4 05 01 00      addr        DAT_000105d4                            = 8Ch
```



```
                     DAT_000105d4                        XREF[4]:     FUN_00010464:000104e4(R),
                                                                      FUN_00010464:00010510(*),
                                                                      FUN_00010464:0001051c(R),
                                                                      00021030(*)
000105d4 8c                 ??         8Ch
000105d5 8a                 ??         8Ah
000105d6 8f                 ??         8Fh
000105d7 9a                 ??         9Ah
000105d8 8d                 ??         8Dh
000105d9 8f                 ??         8Fh
000105da 9e                 ??         9Eh
000105db 8c                 ??         8Ch
000105dc 8c                 ??         8Ch
000105dd 88                 ??         88h
000105de 90                 ??         90h
000105df 8d                 ??         8Dh
000105e0 9b                 ??         9Bh
000105e1 de                 ??         DEh
000105e2 00                 ??         00h
000105e3 00                 ??         00h
```



Import /home/jg/packt/gitrepo/bluepill/ch11/re1/re1.bin

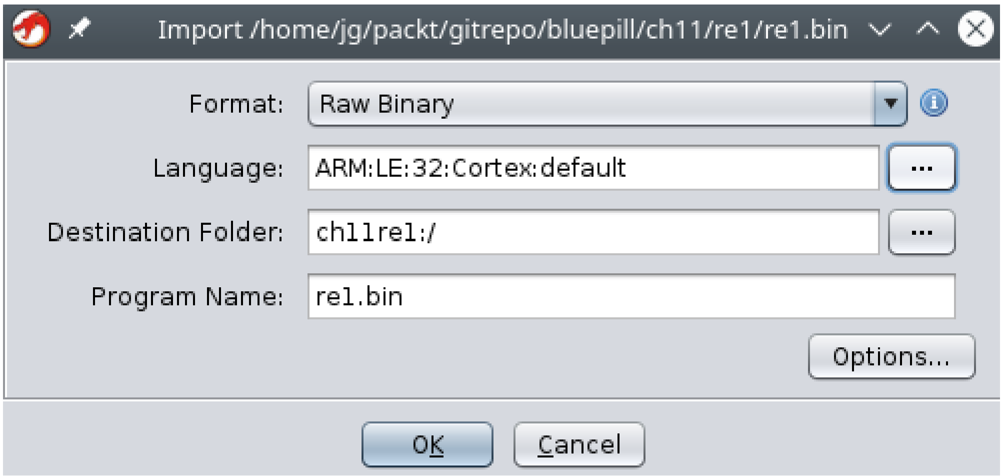
Format: Raw Binary

Language:

Destination Folder: ch11re1:/

Program Name: re1.bin

Please select a language.



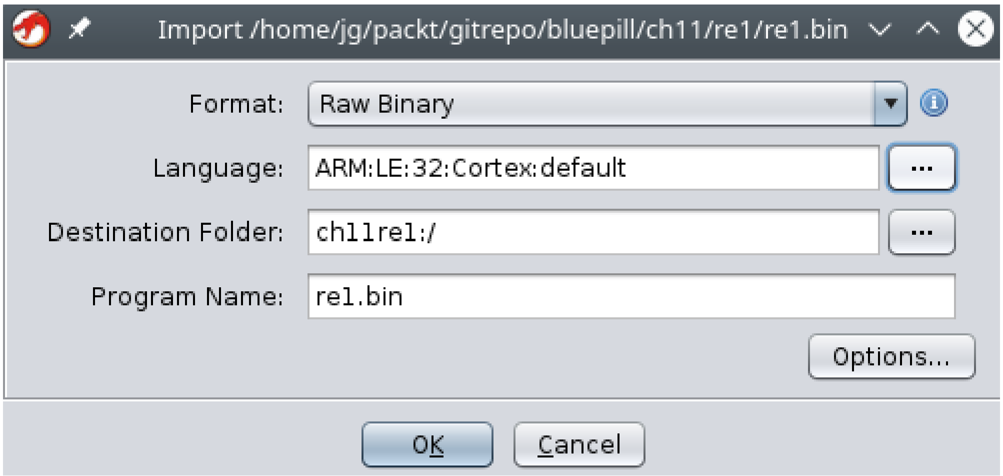
Import /home/jg/packt/gitrepo/bluepill/ch11/re1/re1.bin

Format: Raw Binary

Language: ARM:LE:32:Cortex:default

Destination Folder: ch11re1:/

Program Name: re1.bin



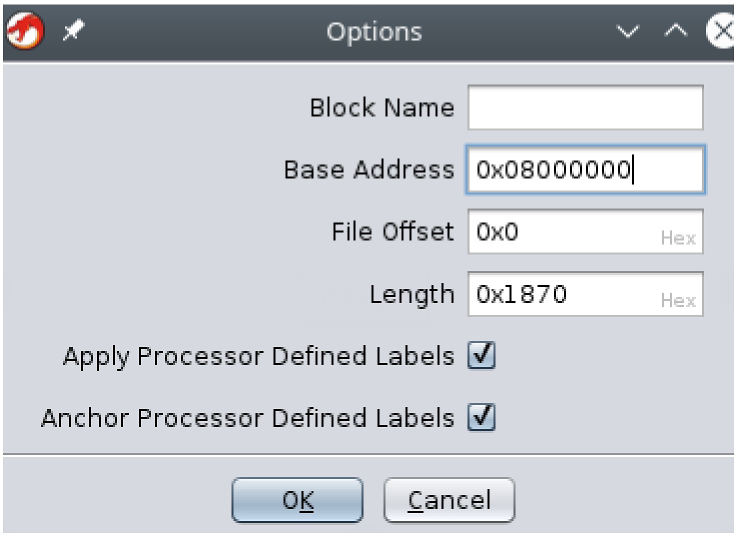
Import /home/jg/packt/gitrepo/bluepill/ch11/re1/re1.bin

Format: Raw Binary

Language: ARM:LE:32:Cortex:default

Destination Folder: ch11re1:/

Program Name: re1.bin



Options

Block Name:

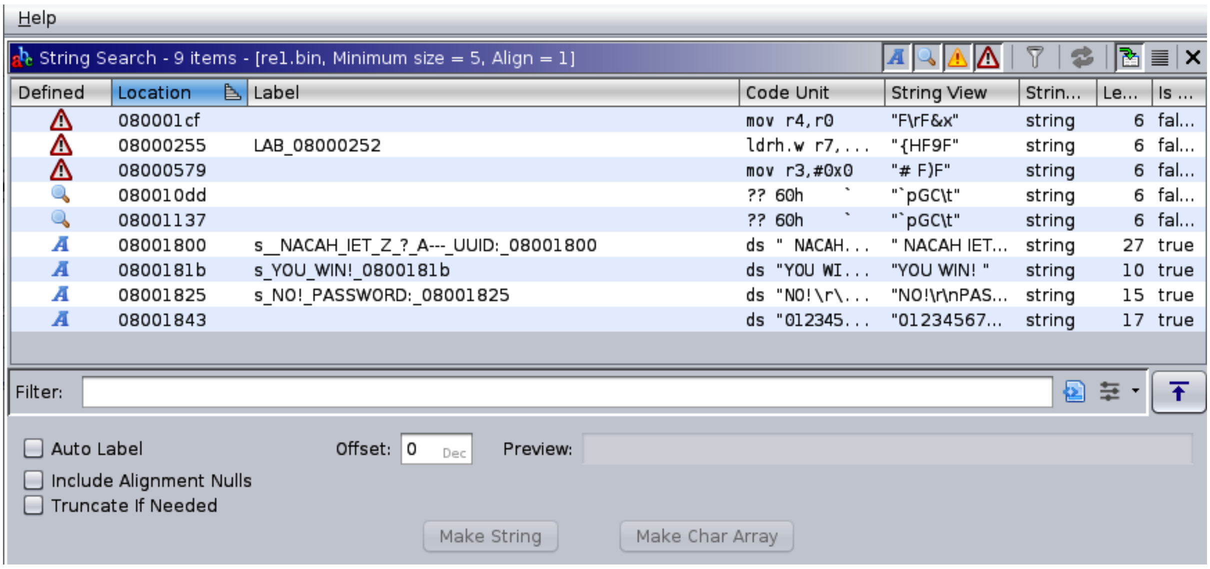
Base Address: 0x08000000

File Offset: 0x0 Hex

Length: 0x1870 Hex

Apply Processor Defined Labels ☑

Anchor Processor Defined Labels ☑



String Search - 9 items - [re1.bin, Minimum size = 5, Align = 1]

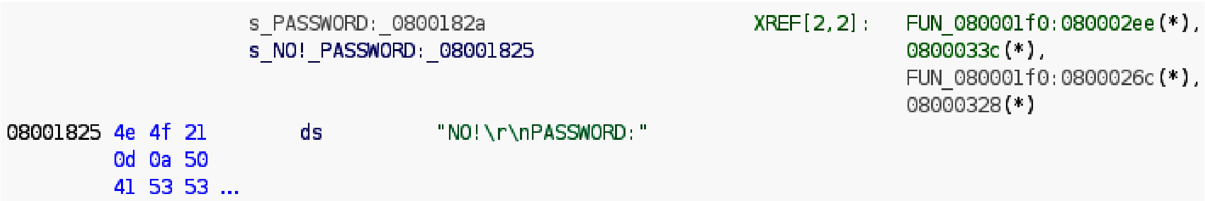
Defined	Location	Label	Code Unit	String View	Strin...	Le...	Is ...
⚠	080001cf		mov r4,r0	"F\rF&x"	string	6	fal...
⚠	08000255	LAB_08000252	ldrh.w r7,...	"{HF9F"	string	6	fal...
⚠	08000579		mov r3,#0x0	"# F)F"	string	6	fal...
🔍	080010dd		?? 60h `	"`pGC\t"	string	6	fal...
🔍	08001137		?? 60h `	"`pGC\t"	string	6	fal...
A	08001800	s__NACAH_IET_Z_?_A---_UUID:_08001800	ds " NACAH...	" NACAH IET...	string	27	true
A	0800181b	s_YOU_WIN!_0800181b	ds "YOU WI...	"YOU WIN! "	string	10	true
A	08001825	s_NO!_PASSWORD:_08001825	ds "NO!\r\...	"NO!\r\nPAS...	string	15	true
A	08001843		ds "012345...	"01234567...	string	17	true

Filter:

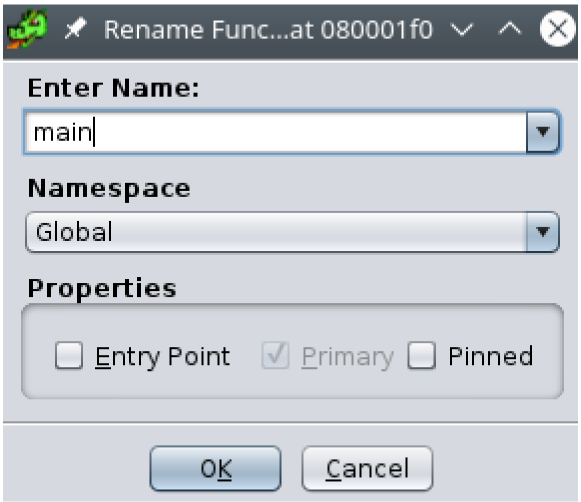
☐ Auto Label
☐ Include Alignment Nulls
☐ Truncate If Needed

Offset: 0 Dec

Preview:



```
                     s_PASSWORD:_0800182a                XREF[2,2]:   FUN_080001f0:080002ee(*),
                     s_NO!_PASSWORD:_08001825                         0800033c(*),
                                                                      FUN_080001f0:0800026c(*),
                                                                      08000328(*)
08001825 4e 4f 21        ds          "NO!\r\nPASSWORD:"
         0d 0a 50
         41 53 53 ...
```



Rename Func...at 080001f0

Enter Name:

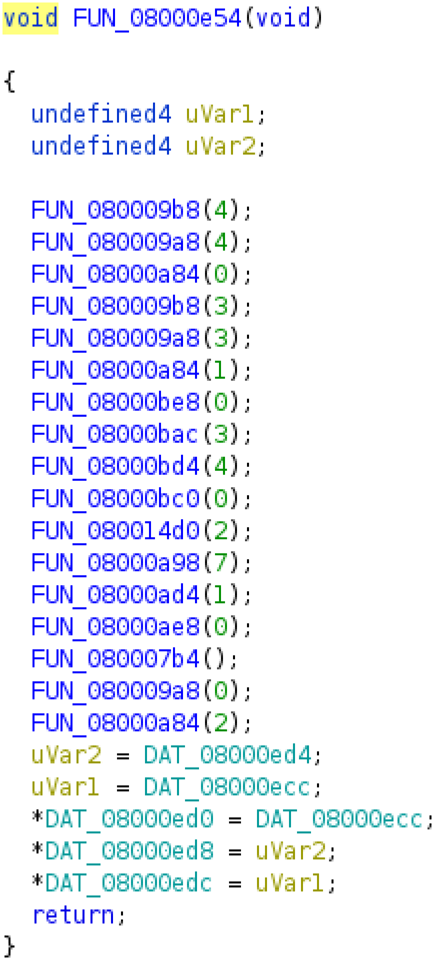
main

Namespace

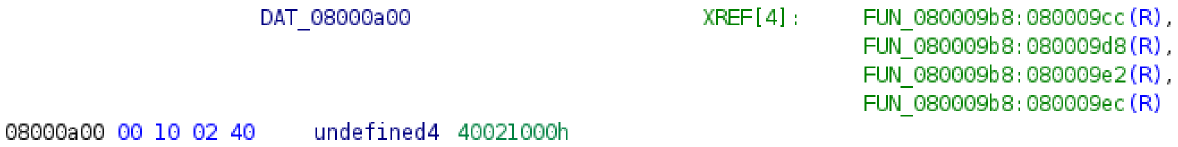
Global

Properties

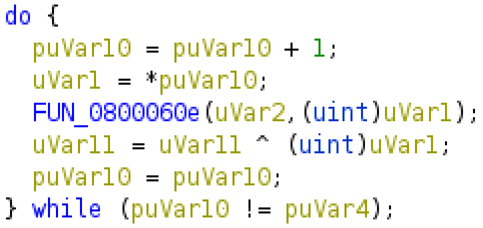
□ Entry Point ☑ Primary □ Pinned



```
void FUN_08000e54(void)

{
  undefined4 uVar1;
  undefined4 uVar2;

  FUN_080009b8(4);
  FUN_080009a8(4);
  FUN_08000a84(0);
  FUN_080009b8(3);
  FUN_080009a8(3);
  FUN_08000a84(1);
  FUN_08000be8(0);
  FUN_08000bac(3);
  FUN_08000bd4(4);
  FUN_08000bc0(0);
  FUN_080014d0(2);
  FUN_08000a98(7);
  FUN_08000ad4(1);
  FUN_08000ae8(0);
  FUN_080007b4();
  FUN_080009a8(0);
  FUN_08000a84(2);
  uVar2 = DAT_08000ed4;
  uVar1 = DAT_08000ecc;
  *DAT_08000ed0 = DAT_08000ecc;
  *DAT_08000ed8 = uVar2;
  *DAT_08000edc = uVar1;
  return;
}
```

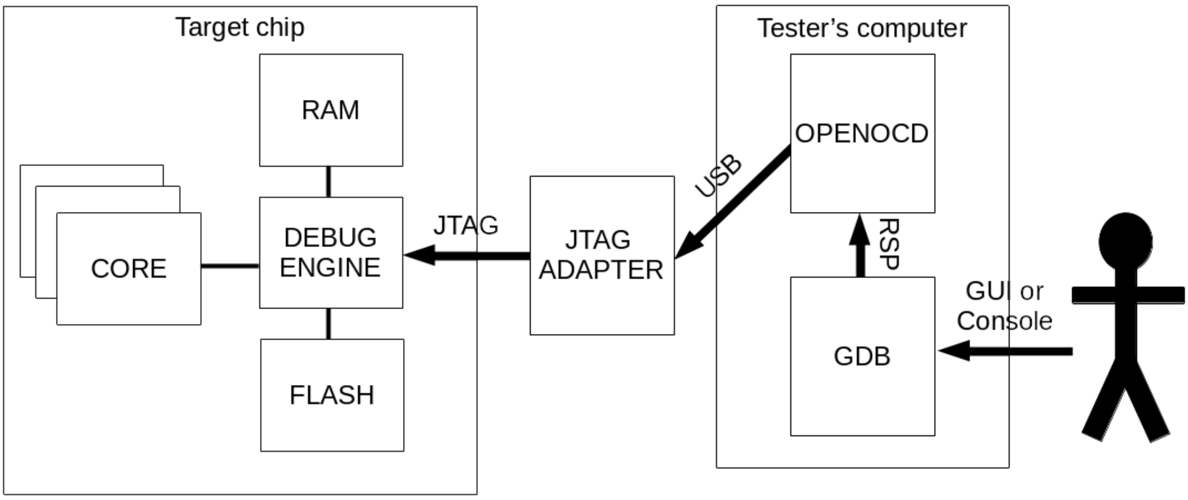


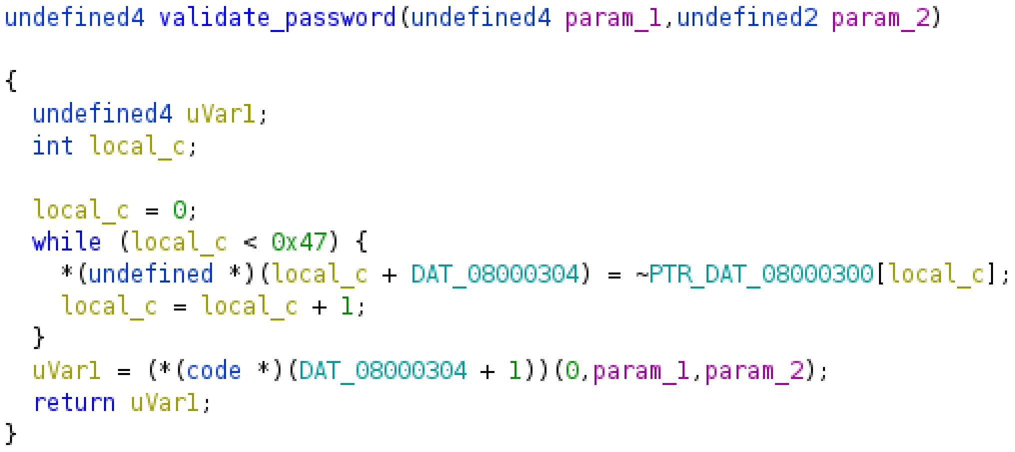
```
                    DAT_08000a00                        XREF[4]:     FUN_080009b8:080009cc(R),
                                                                     FUN_080009b8:080009d8(R),
                                                                     FUN_080009b8:080009e2(R),
                                                                     FUN_080009b8:080009ec(R)
08000a00 00 10 02 40     undefined4  40021000h
```



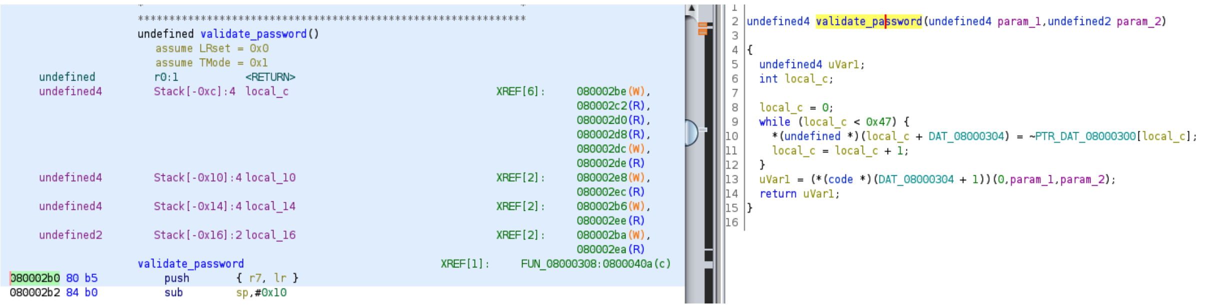
```
do {
  puVar10 = puVar10 + 1;
  uVar1 = *puVar10;
  FUN_0800060e(uVar2,(uint)uVar1);
  uVar11 = uVar11 ^ (uint)uVar1;
  puVar10 = puVar10;
} while (puVar10 != puVar4);
```

Chapter 12: Dynamic Reverse Engineering.





```
undefined4 validate_password(undefined4 param_1,undefined2 param_2)

{
  undefined4 uVar1;
  int local_c;

  local_c = 0;
  while (local_c < 0x47) {
    *(undefined *)(local_c + DAT_08000304) = ~PTR_DAT_08000300[local_c];
    local_c = local_c + 1;
  }
  uVar1 = (*(code *)(DAT_08000304 + 1))(0,param_1,param_2);
  return uVar1;
}
```



```
                    *************************************************************
                    undefined validate_password()
                      assume LRset = 0x0
                      assume TMode = 0x1
     undefined         r0:1            <RETURN>
     undefined4        Stack[-0xc]:4  local_c                          XREF[6]:     080002be(W),
                                                                                    080002c2(R),
                                                                                    080002d0(R),
                                                                                    080002d8(R),
                                                                                    080002dc(W),
                                                                                    080002de(R)
     undefined4        Stack[-0x10]:4 local_10                         XREF[2]:     080002e8(W),
                                                                                    080002ec(R)
     undefined4        Stack[-0x14]:4 local_14                         XREF[2]:     080002b6(W),
                                                                                    080002ee(R)
     undefined2        Stack[-0x16]:2 local_16                         XREF[2]:     080002ba(W),
                                                                                    080002ea(R)
                    validate_password                              XREF[1]:     FUN_08000308:0800040a(c)
080002b0 80 b5          push         { r7, lr }
080002b2 84 b0          sub          sp,#0x10
```

```

undefined4 validate_password(undefined4 param_1,undefined2 param_2)

{
  undefined4 uVar1;
  int local_c;

  local_c = 0;
  while (local_c < 0x47) {
    *(undefined *)(local_c + DAT_08000304) = ~PTR_DAT_08000300[local_c];
    local_c = local_c + 1;
  }
  uVar1 = (*(code *)(DAT_08000304 + 1))(0,param_1,param_2);
  return uVar1;
}

```

Chapter 13: Scoring and Reporting Your Vulnerabilities.

No Images

Chapter 14: Wrapping It Up – Mitigations and Good Practices.

No Images