BEAUTIFUL

OPEN SOURCE

HUGO TESO

ALLOW ME TO...

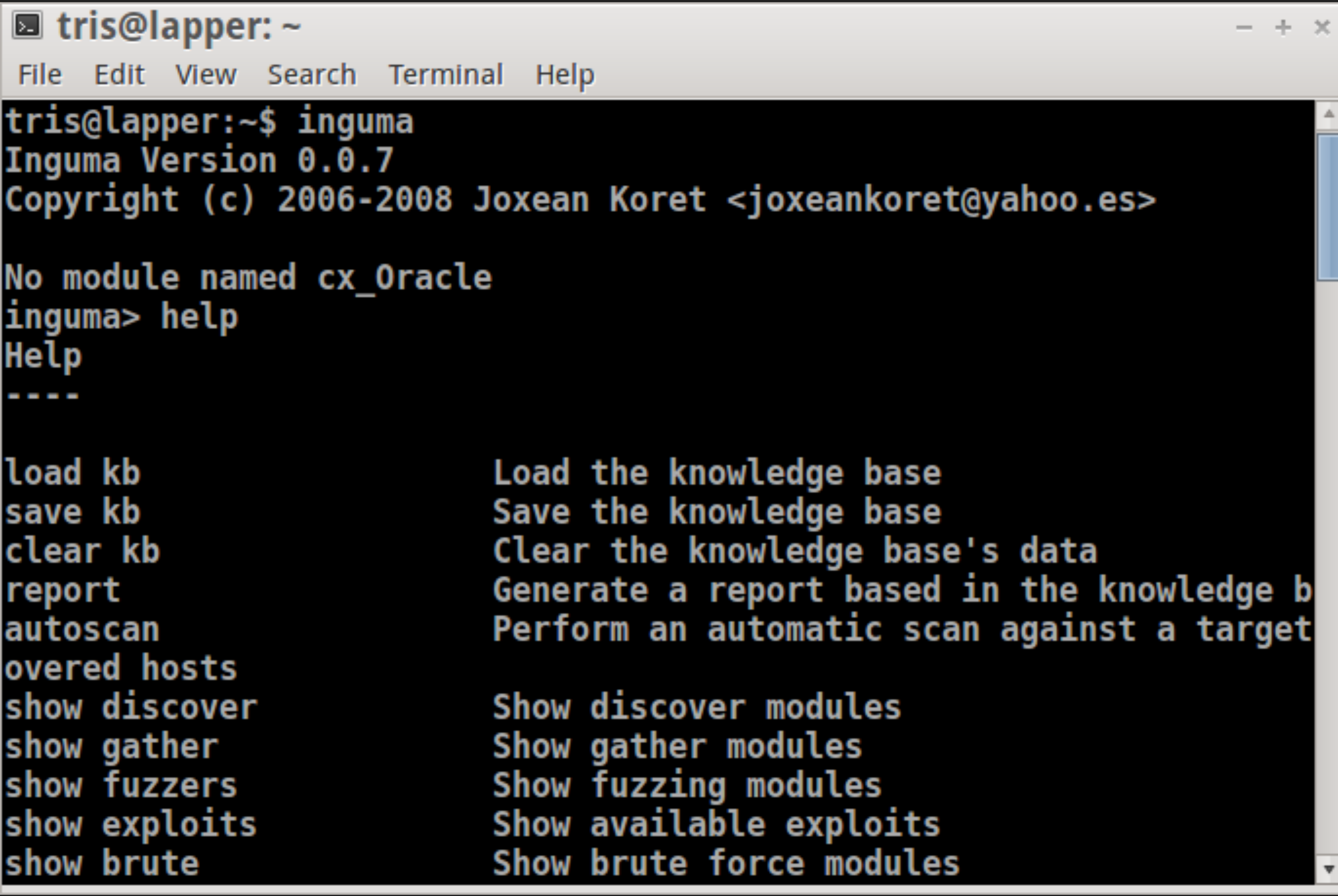
CYBER-CYBER AIRPLANES!

NDA… :'(

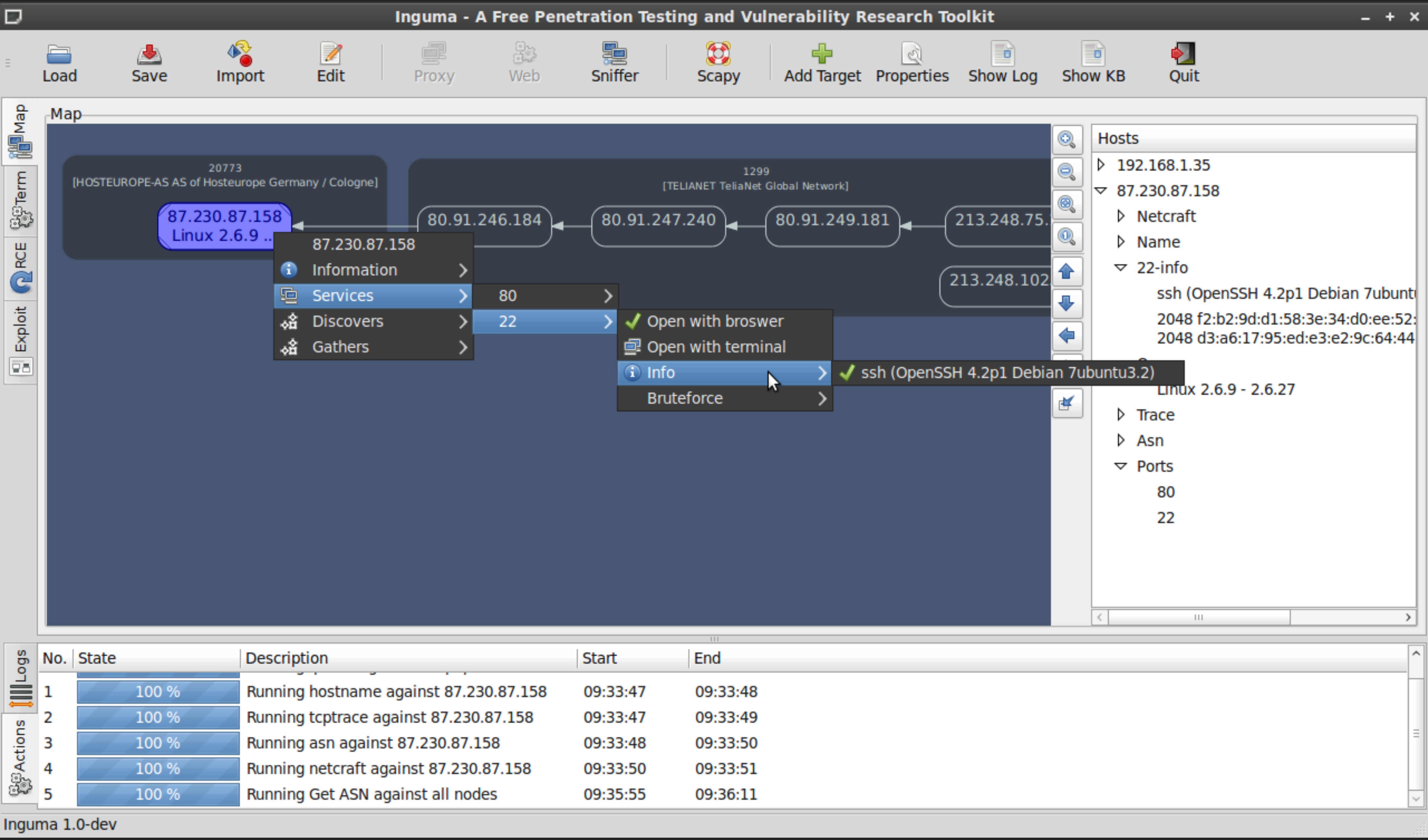
I DO OPEN SAUCE!

Hugo Teso

INGUMA

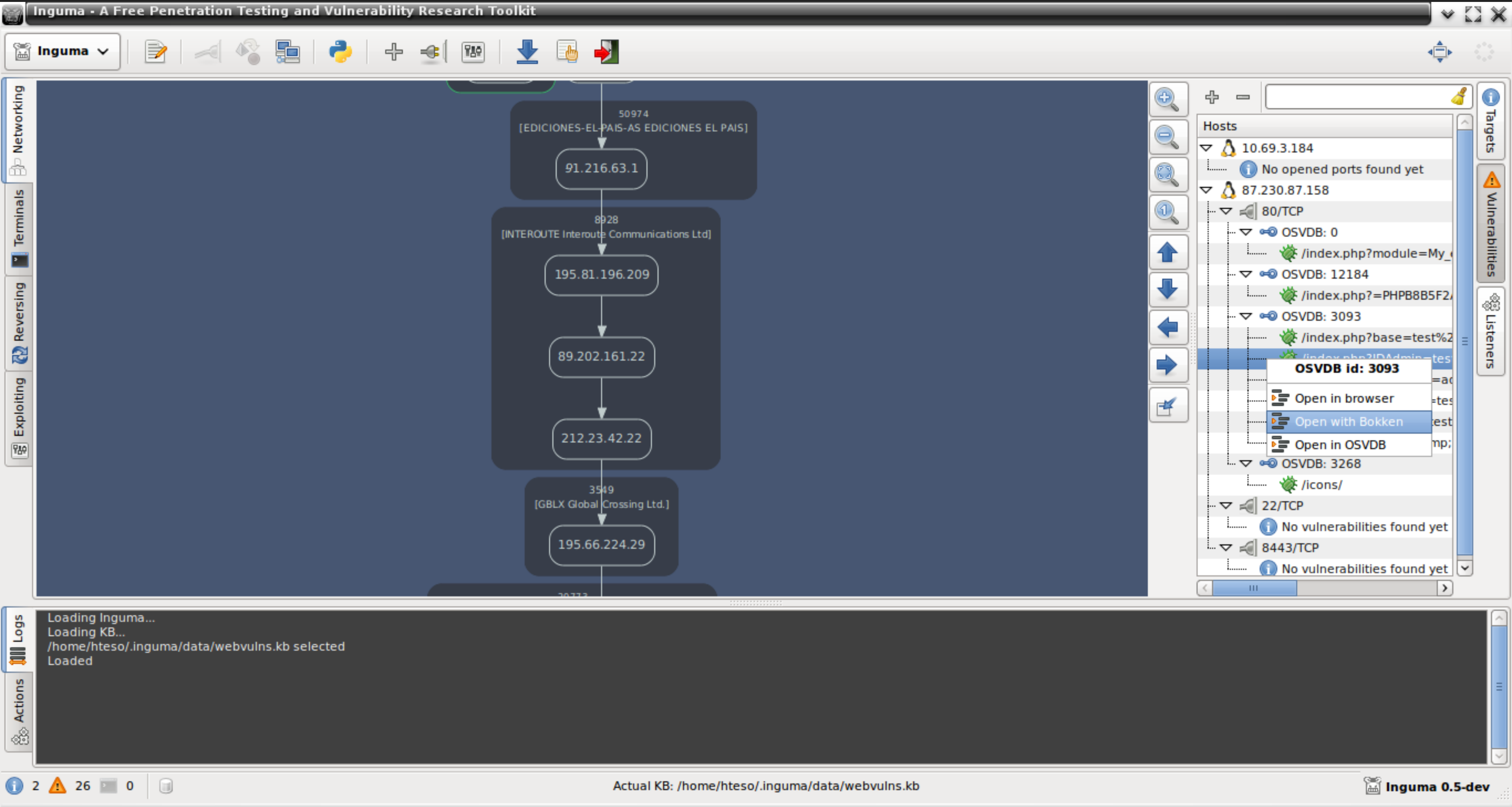


```
tris@lapper:~$ inguma
Inguma Version 0.0.7
Copyright (c) 2006-2008 Joxean Koret <joxeankoret@yahoo.es>

No module named cx_Oracle
inguma> help
Help
----

load kb                  Load the knowledge base
save kb                  Save the knowledge base
clear kb                 Clear the knowledge base's data
report                   Generate a report based in the knowledge b
autoscan                 Perform an automatic scan against a target
overed hosts
show discover            Show discover modules
show gather              Show gather modules
show fuzzers             Show fuzzing modules
show exploits            Show available exploits
show brute               Show brute force modules
```



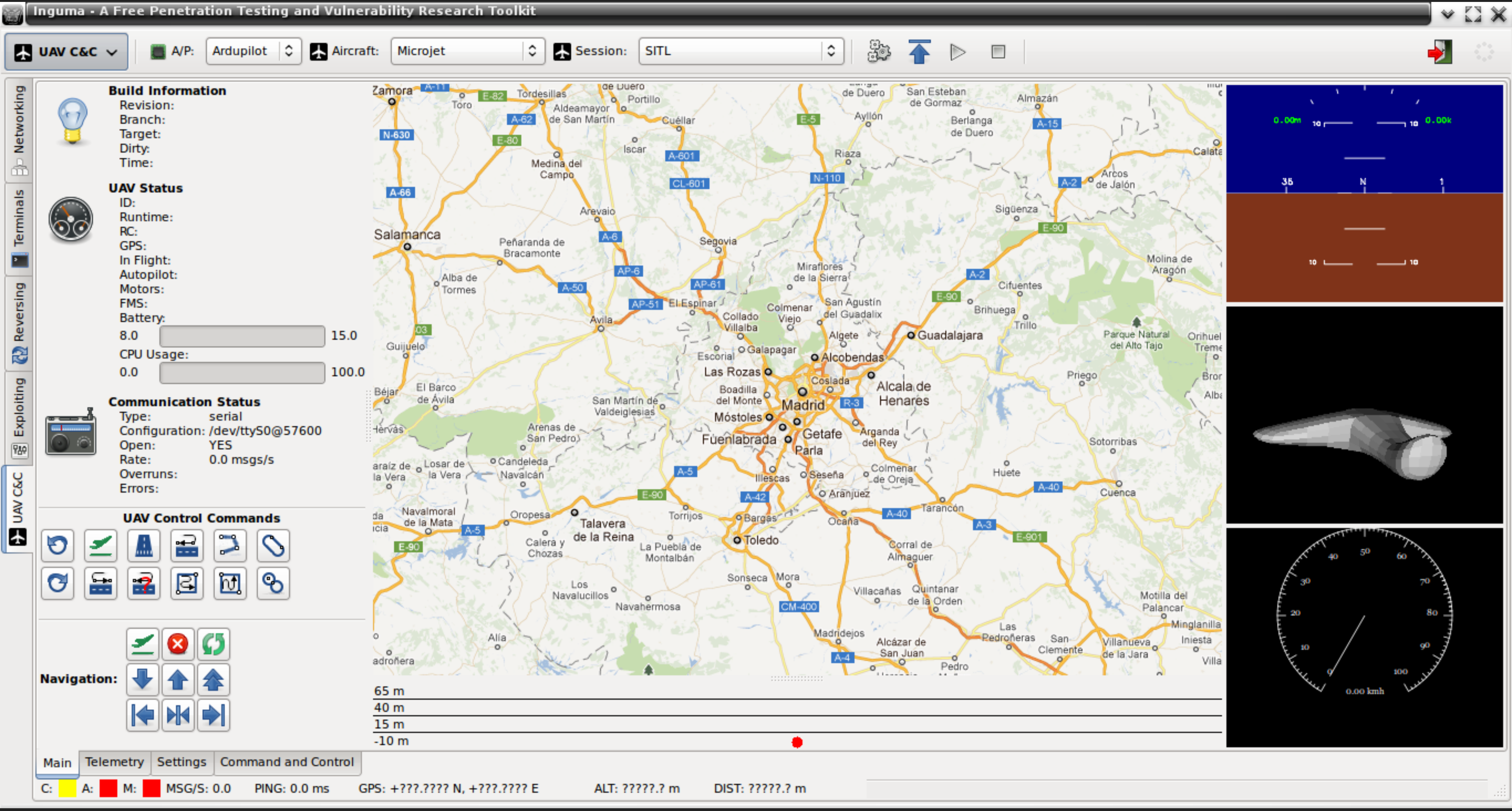
No.	State	Description	Start	End
1	100 %	Running hostname against 87.230.87.158	09:33:47	09:33:48
2	100 %	Running tcptrace against 87.230.87.158	09:33:47	09:33:49
3	100 %	Running asn against 87.230.87.158	09:33:48	09:33:50
4	100 %	Running netcraft against 87.230.87.158	09:33:50	09:33:51
5	100 %	Running Get ASN against all nodes	09:35:55	09:36:11

Inguma 1.0-dev



```
Loading Inguma...
Loading KB...
/home/hteso/.inguma/data/webvulns.kb selected
Loaded
```

Actual KB: /home/hteso/.inguma/data/webvulns.kb



Inguma - A Free Penetration Testing and Vulnerability Research Toolkit

UAV C&C | A/P: Ardupilot | Aircraft: Microjet | Session: SITL

Build Information
Revision:
Branch:
Target:
Dirty:
Time:

UAV Status
ID:
Runtime:
RC:
GPS:
In Flight:
Autopilot:
Motors:
FMS:
Battery:
8.0 15.0
CPU Usage:
0.0 100.0

Communication Status
Type: serial
Configuration: /dev/ttyS0@57600
Open: YES
Rate: 0.0 msgs/s
Overruns:
Errors:

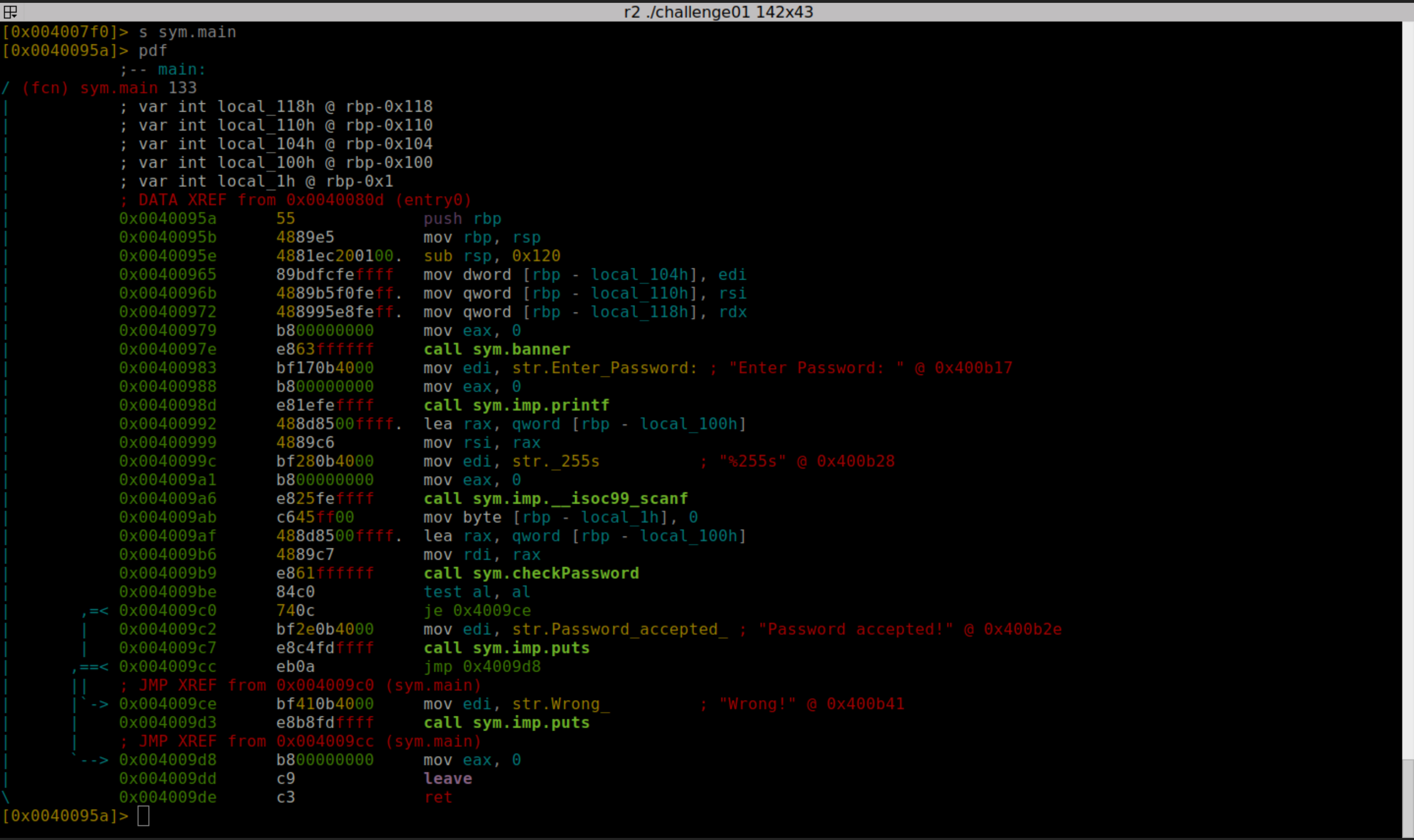
UAV Control Commands

Navigation:

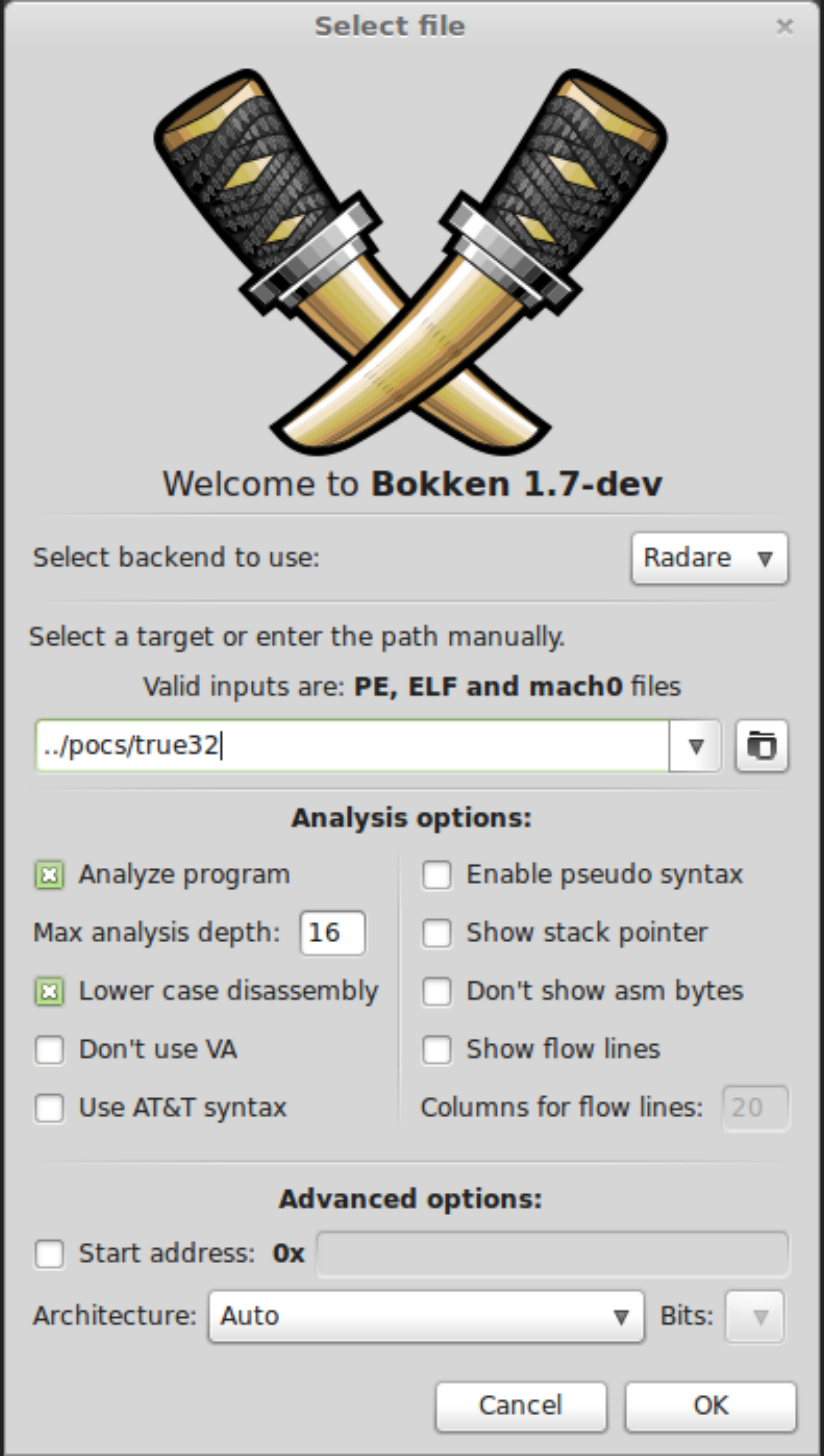
Main | Telemetry | Settings | Command and Control

C: 🟨 A: 🟥 M: 🟥 MSG/S: 0.0 PING: 0.0 ms GPS: +???.???? N, +???.???? E ALT: ?????.? m DIST: ?????.? m

BOKKEN



```
[0x004007f0]> s sym.main
[0x0040095a]> pdf
            ;-- main:
/ (fcn) sym.main 133
|           ; var int local_118h @ rbp-0x118
|           ; var int local_110h @ rbp-0x110
|           ; var int local_104h @ rbp-0x104
|           ; var int local_100h @ rbp-0x100
|           ; var int local_1h @ rbp-0x1
|           ; DATA XREF from 0x0040080d (entry0)
|           0x0040095a      55             push rbp
|           0x0040095b      4889e5         mov rbp, rsp
|           0x0040095e      4881ec200100.  sub rsp, 0x120
|           0x00400965      89bdfcfeffff   mov dword [rbp - local_104h], edi
|           0x0040096b      4889b5f0feff.  mov qword [rbp - local_110h], rsi
|           0x00400972      488995e8feff.  mov qword [rbp - local_118h], rdx
|           0x00400979      b800000000     mov eax, 0
|           0x0040097e      e863ffffff     call sym.banner
|           0x00400983      bf170b4000     mov edi, str.Enter_Password: ; "Enter Password: " @ 0x400b17
|           0x00400988      b800000000     mov eax, 0
|           0x0040098d      e81efeffff     call sym.imp.printf
|           0x00400992      488d8500ffff.  lea rax, qword [rbp - local_100h]
|           0x00400999      4889c6         mov rsi, rax
|           0x0040099c      bf280b4000     mov edi, str._255s          ; "%255s" @ 0x400b28
|           0x004009a1      b800000000     mov eax, 0
|           0x004009a6      e825feffff     call sym.imp.__isoc99_scanf
|           0x004009ab      c645ff00       mov byte [rbp - local_1h], 0
|           0x004009af      488d8500ffff.  lea rax, qword [rbp - local_100h]
|           0x004009b6      4889c7         mov rdi, rax
|           0x004009b9      e861ffffff     call sym.checkPassword
|           0x004009be      84c0           test al, al
|       ,=< 0x004009c0      740c           je 0x4009ce
|       |   0x004009c2      bf2e0b4000     mov edi, str.Password_accepted_ ; "Password accepted!" @ 0x400b2e
|       |   0x004009c7      e8c4fdffff     call sym.imp.puts
|      ,==< 0x004009cc      eb0a           jmp 0x4009d8
|      ||   ; JMP XREF from 0x004009c0 (sym.main)
|      |`-> 0x004009ce      bf410b4000     mov edi, str.Wrong_         ; "Wrong!" @ 0x400b41
|      |    0x004009d3      e8b8fdffff     call sym.imp.puts
|      |    ; JMP XREF from 0x004009cc (sym.main)
|      `--> 0x004009d8      b800000000     mov eax, 0
|           0x004009dd      c9             leave
\           0x004009de      c3             ret
[0x0040095a]>
```



Welcome to **Bokken 1.7-dev**

Select backend to use: Radare

Select a target or enter the path manually.

Valid inputs are: **PE, ELF and mach0** files

../pocs/true32

Analysis options:

☒ Analyze program

Max analysis depth: 16

☒ Lower case disassembly

□ Don't use VA

□ Use AT&T syntax

□ Enable pseudo syntax

□ Show stack pointer

□ Don't show asm bytes

□ Show flow lines

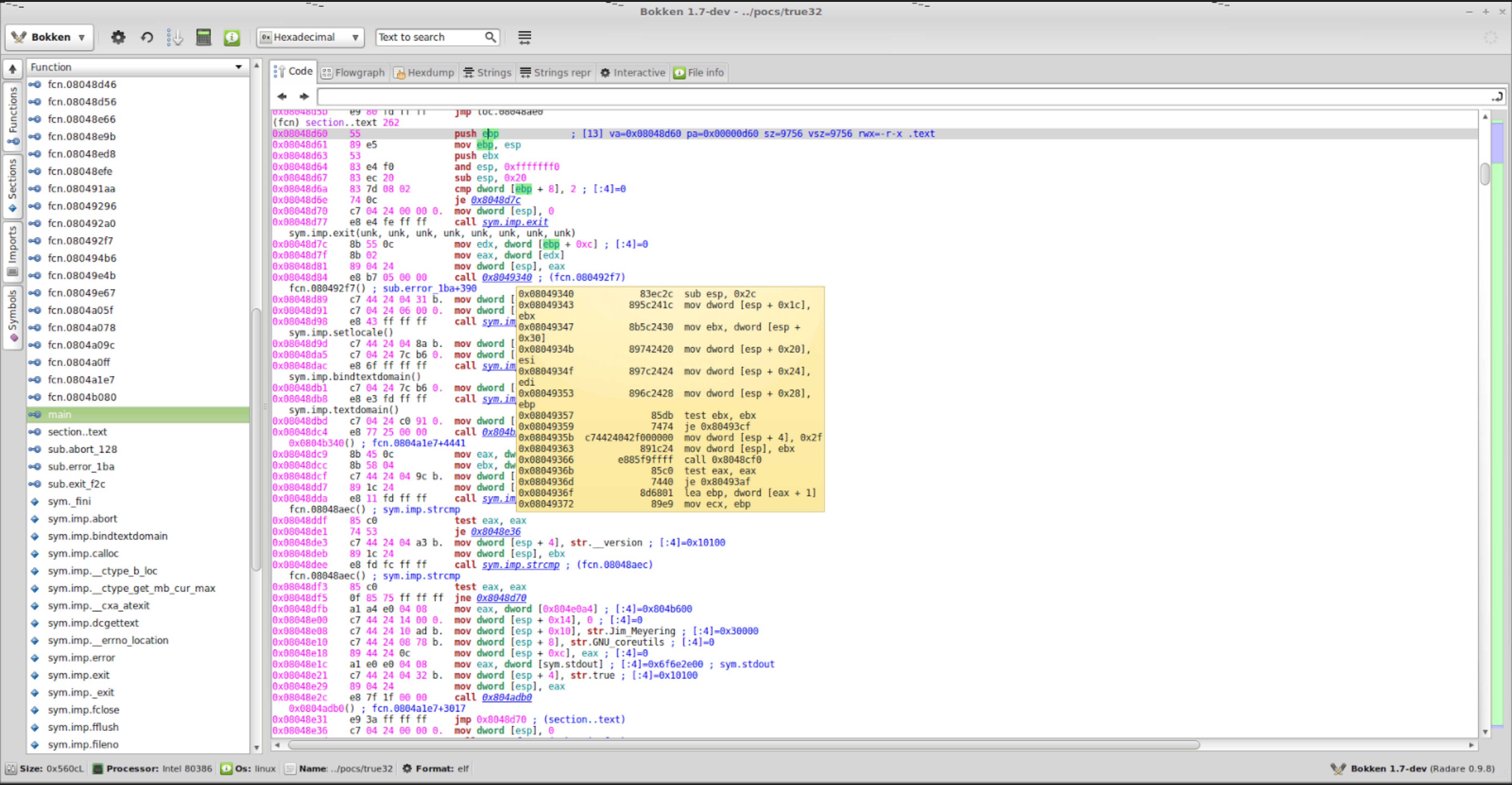
Columns for flow lines: 20

Advanced options:

□ Start address: **0x**

Architecture: Auto

Bits:

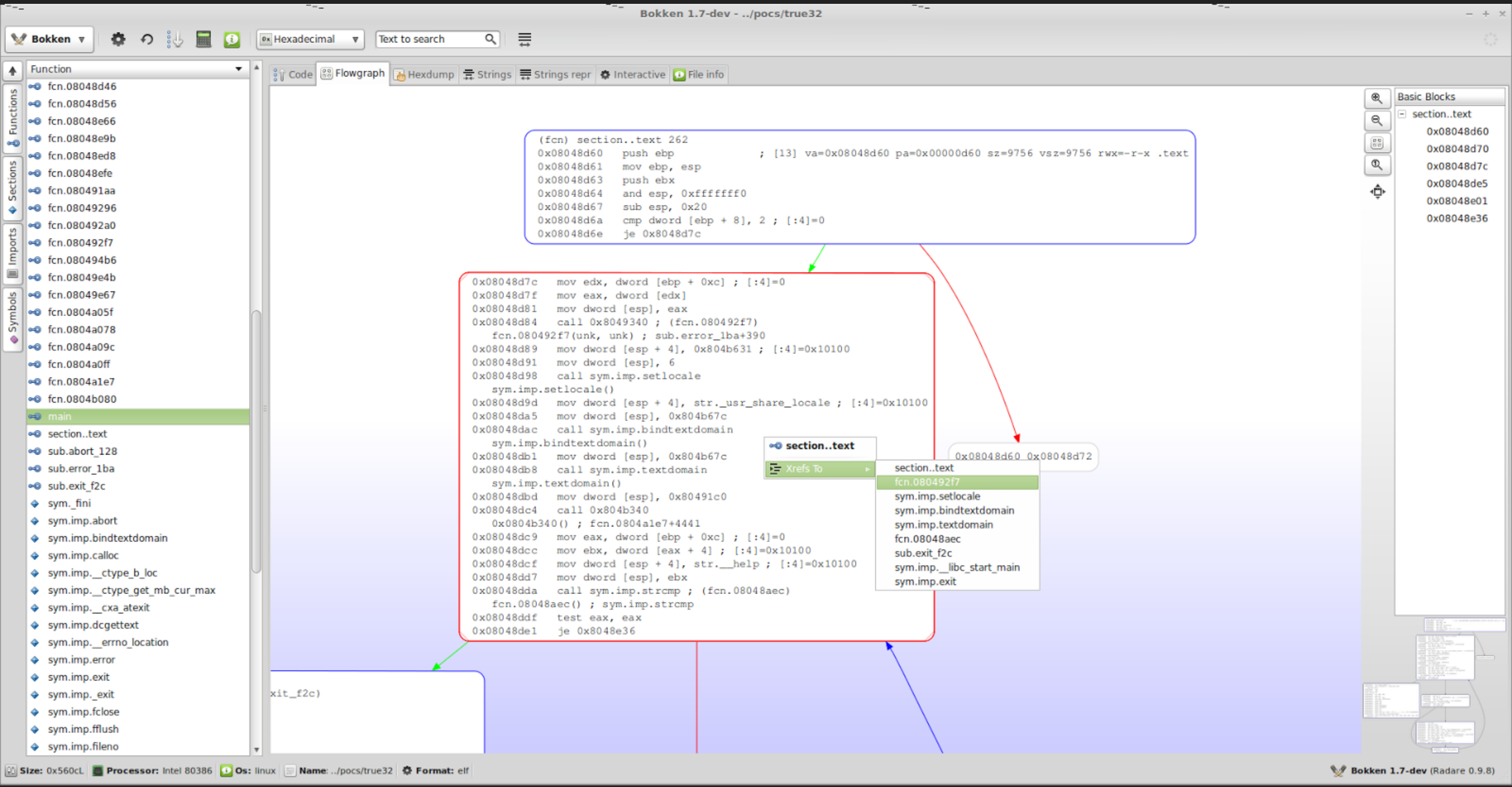


fcn.08048d46
fcn.08048d56
fcn.08048e66
fcn.08048e9b
fcn.08048ed8
fcn.08048efe
fcn.080491aa
fcn.08049296
fcn.080492a0
fcn.080492f7
fcn.080494b6
fcn.08049e4b
fcn.08049e67
fcn.0804a05f
fcn.0804a078
fcn.0804a09c
fcn.0804a0ff
fcn.0804a1e7
fcn.0804b080
main
section..text
sub.abort_128
sub.error_1ba
sub.exit_f2c
sym._fini
sym.imp.abort
sym.imp.bindtextdomain
sym.imp.calloc
sym.imp.__ctype_b_loc
sym.imp.__ctype_get_mb_cur_max
sym.imp.__cxa_atexit
sym.imp.dcgettext
sym.imp.__errno_location
sym.imp.error
sym.imp.exit
sym.imp._exit
sym.imp.fclose
sym.imp.fflush
sym.imp.fileno

```
0x08048d5b    e9 80 fd ff ff      jmp loc.08048ae0
(fcn) section..text 262
0x08048d60    55                  push ebp              ; [13] va=0x08048d60 pa=0x00000d60 sz=9756 vsz=9756 rwx=-r-x .text
0x08048d61    89 e5               mov ebp, esp
0x08048d63    53                  push ebx
0x08048d64    83 e4 f0            and esp, 0xfffffff0
0x08048d67    83 ec 20            sub esp, 0x20
0x08048d6a    83 7d 08 02         cmp dword [ebp + 8], 2 ; [:4]=0
0x08048d6e    74 0c               je 0x8048d7c
0x08048d70    c7 04 24 00 00 0.   mov dword [esp], 0
0x08048d77    e8 e4 fe ff ff      call sym.imp.exit
   sym.imp.exit(unk, unk, unk, unk, unk, unk, unk, unk)
0x08048d7c    8b 55 0c            mov edx, dword [ebp + 0xc] ; [:4]=0
0x08048d7f    8b 02               mov eax, dword [edx]
0x08048d81    89 04 24            mov dword [esp], eax
0x08048d84    e8 b7 05 00 00      call 0x8049340 ; (fcn.080492f7)
   fcn.080492f7() ; sub.error_1ba+390
0x08048d89    c7 44 24 04 31 b.   mov dword [
0x08048d91    c7 04 24 06 00 0.   mov dword [
0x08048d98    e8 43 ff ff ff      call sym.im
   sym.imp.setlocale()
0x08048d9d    c7 44 24 04 8a b.   mov dword [
0x08048da5    c7 04 24 7c b6 0.   mov dword [
0x08048dac    e8 6f ff ff ff      call sym.im
   sym.imp.bindtextdomain()
0x08048db1    c7 04 24 7c b6 0.   mov dword [
0x08048db8    e8 e3 fd ff ff      call sym.im
   sym.imp.textdomain()
0x08048dbd    c7 04 24 c0 91 0.   mov dword [
0x08048dc4    e8 77 25 00 00      call 0x804b
   0x0804b340() ; fcn.0804a1e7+4441
0x08048dc9    8b 45 0c            mov eax, dw
0x08048dcc    8b 58 04            mov ebx, dw
0x08048dcf    c7 44 24 04 9c b.   mov dword [
0x08048dd7    89 1c 24            mov dword [
0x08048dda    e8 11 fd ff ff      call sym.im
   fcn.08048aec() ; sym.imp.strcmp
0x08048ddf    85 c0               test eax, eax
0x08048de1    74 53               je 0x8048e36
0x08048de3    c7 44 24 04 a3 b.   mov dword [esp + 4], str.__version ; [:4]=0x10100
0x08048deb    89 1c 24            mov dword [esp], ebx
0x08048dee    e8 fd fc ff ff      call sym.imp.strcmp ; (fcn.08048aec)
   fcn.08048aec() ; sym.imp.strcmp
0x08048df3    85 c0               test eax, eax
0x08048df5    0f 85 75 ff ff ff   jne 0x8048d70
0x08048dfb    a1 a4 e0 04 08      mov eax, dword [0x804e0a4] ; [:4]=0x804b600
0x08048e00    c7 44 24 14 00 0.   mov dword [esp + 0x14], 0 ; [:4]=0
0x08048e08    c7 44 24 10 ad b.   mov dword [esp + 0x10], str.Jim_Meyering ; [:4]=0x30000
0x08048e10    c7 44 24 08 78 b.   mov dword [esp + 8], str.GNU_coreutils ; [:4]=0
0x08048e18    89 44 24 0c         mov dword [esp + 0xc], eax ; [:4]=0
0x08048e1c    a1 e0 e0 04 08      mov eax, dword [sym.stdout] ; [:4]=0x6f6e2e00 ; sym.stdout
0x08048e21    c7 44 24 04 32 b.   mov dword [esp + 4], str.true ; [:4]=0x10100
0x08048e29    89 04 24            mov dword [esp], eax
0x08048e2c    e8 7f 1f 00 00      call 0x804adb0
   0x0804adb0() ; fcn.0804a1e7+3017
0x08048e31    e9 3a ff ff ff      jmp 0x8048d70 ; (section..text)
0x08048e36    c7 04 24 00 00 0.   mov dword [esp], 0
```

```
0x08049340             83ec2c  sub esp, 0x2c
0x08049343           895c241c  mov dword [esp + 0x1c],
ebx
0x08049347           8b5c2430  mov ebx, dword [esp +
0x30]
0x0804934b           89742420  mov dword [esp + 0x20],
esi
0x0804934f           897c2424  mov dword [esp + 0x24],
edi
0x08049353           896c2428  mov dword [esp + 0x28],
ebp
0x08049357               85db  test ebx, ebx
0x08049359               7474  je 0x80493cf
0x0804935b c74424042f000000  mov dword [esp + 4], 0x2f
0x08049363             891c24  mov dword [esp], ebx
0x08049366         e885f9ffff  call 0x8048cf0
0x0804936b               85c0  test eax, eax
0x0804936d               7440  je 0x80493af
0x0804936f             8d6801  lea ebp, dword [eax + 1]
0x08049372               89e9  mov ecx, ebp
```

Size: 0x560cL Processor: Intel 80386 Os: linux Name: ../pocs/true32 Format: elf Bokken 1.7-dev (Radare 0.9.8)



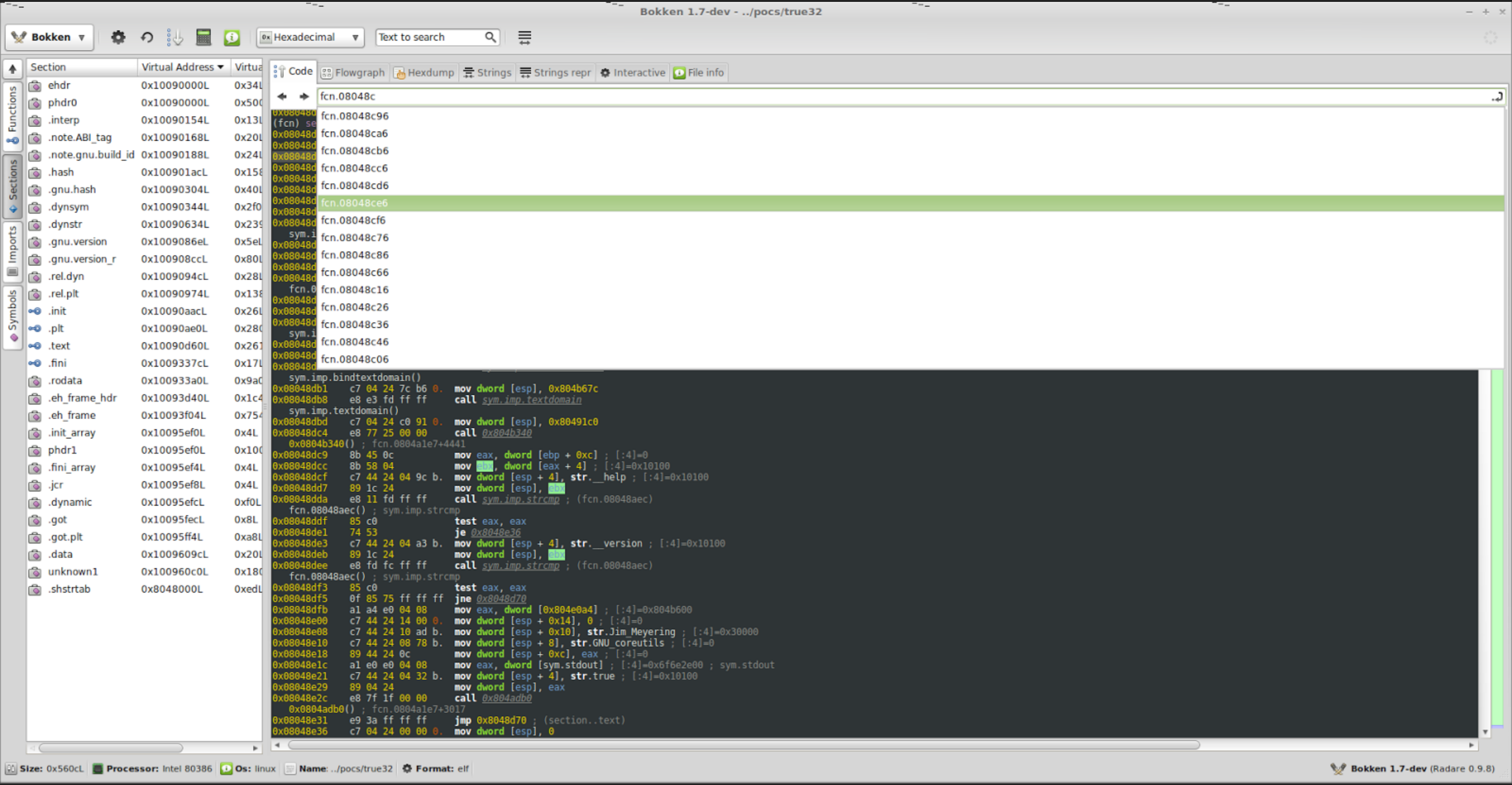
Bokken 1.7-dev - ../pocs/true32

```
(fcn) section..text 262
0x08048d60   push ebp           ; [13] va=0x08048d60 pa=0x00000d60 sz=9756 vsz=9756 rwx=-r-x .text
0x08048d61   mov ebp, esp
0x08048d63   push ebx
0x08048d64   and esp, 0xfffffff0
0x08048d67   sub esp, 0x20
0x08048d6a   cmp dword [ebp + 8], 2 ; [:4]=0
0x08048d6e   je 0x8048d7c
```

```
0x08048d7c   mov edx, dword [ebp + 0xc] ; [:4]=0
0x08048d7f   mov eax, dword [edx]
0x08048d81   mov dword [esp], eax
0x08048d84   call 0x8049340 ; (fcn.080492f7)
   fcn.080492f7(unk, unk) ; sub.error_1ba+390
0x08048d89   mov dword [esp + 4], 0x804b631 ; [:4]=0x10100
0x08048d91   mov dword [esp], 6
0x08048d98   call sym.imp.setlocale
   sym.imp.setlocale()
0x08048d9d   mov dword [esp + 4], str._usr_share_locale ; [:4]=0x10100
0x08048da5   mov dword [esp], 0x804b67c
0x08048dac   call sym.imp.bindtextdomain
   sym.imp.bindtextdomain()
0x08048db1   mov dword [esp], 0x804b67c
0x08048db8   call sym.imp.textdomain
   sym.imp.textdomain()
0x08048dbd   mov dword [esp], 0x80491c0
0x08048dc4   call 0x804b340
   0x0804b340() ; fcn.0804a1e7+4441
0x08048dc9   mov eax, dword [ebp + 0xc] ; [:4]=0
0x08048dcc   mov ebx, dword [eax + 4] ; [:4]=0x10100
0x08048dcf   mov dword [esp + 4], str.__help ; [:4]=0x10100
0x08048dd7   mov dword [esp], ebx
0x08048dda   call sym.imp.strcmp ; (fcn.08048aec)
   fcn.08048aec() ; sym.imp.strcmp
0x08048ddf   test eax, eax
0x08048de1   je 0x8048e36
```

Size: 0x560cL **Processor:** Intel 80386 **Os:** linux **Name:** ../pocs/true32 **Format:** elf

Bokken 1.7-dev (Radare 0.9.8)



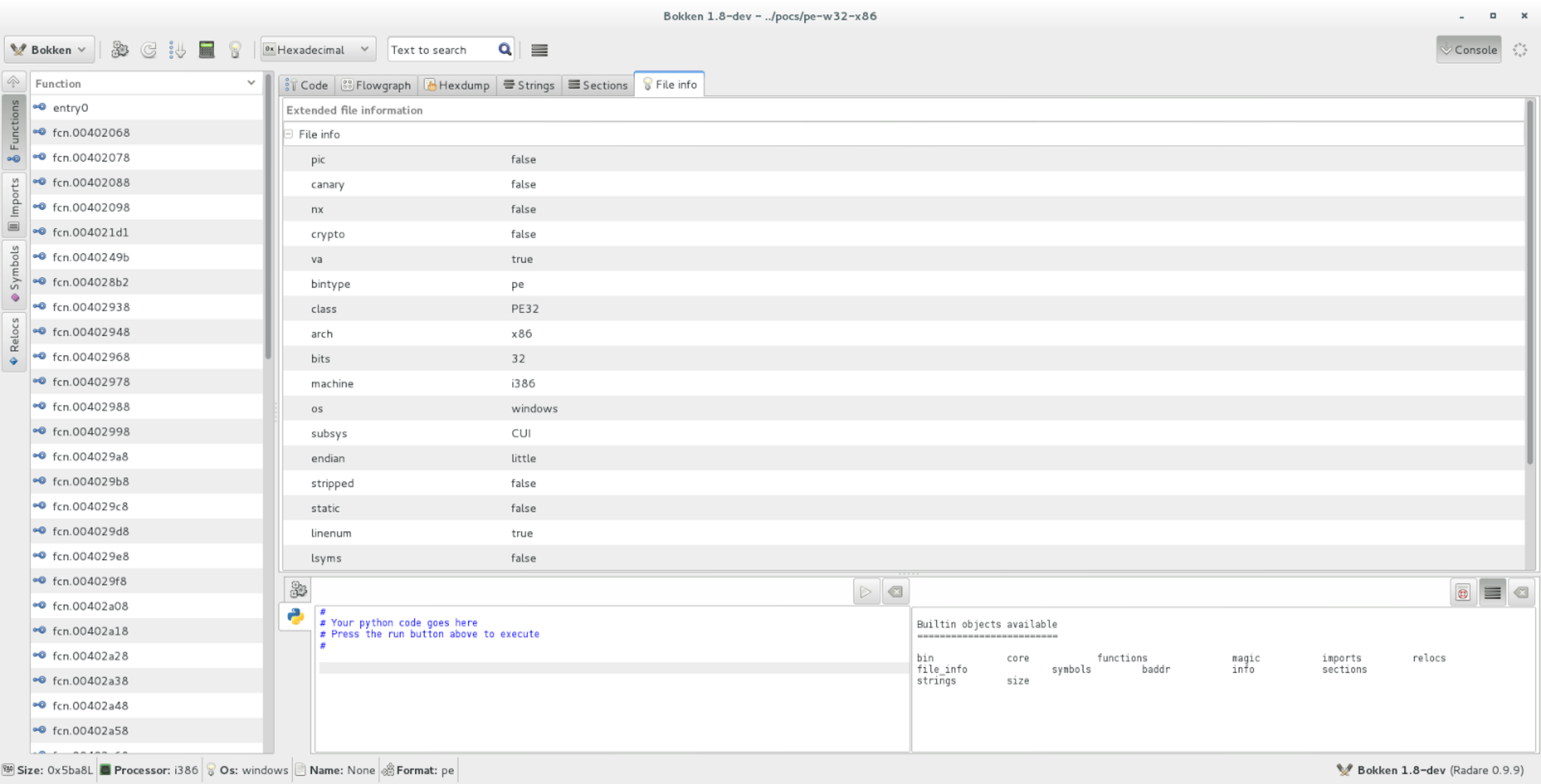
Section	Virtual Address	Virtua
ehdr	0x10090000L	0x34L
phdr0	0x10090000L	0x50(
.interp	0x10090154L	0x13L
.note.ABI_tag	0x10090168L	0x20L
.note.gnu.build_id	0x10090188L	0x24L
.hash	0x100901acL	0x158
.gnu.hash	0x10090304L	0x40L
.dynsym	0x10090344L	0x2f0
.dynstr	0x10090634L	0x239
.gnu.version	0x1009086eL	0x5eL
.gnu.version_r	0x100908ccL	0x80L
.rel.dyn	0x1009094cL	0x28L
.rel.plt	0x10090974L	0x138
.init	0x10090aacL	0x26L
.plt	0x10090ae0L	0x280
.text	0x10090d60L	0x261
.fini	0x1009337cL	0x17L
.rodata	0x100933a0L	0x9a0
.eh_frame_hdr	0x10093d40L	0x1c4
.eh_frame	0x10093f04L	0x754
.init_array	0x10095ef0L	0x4L
phdr1	0x10095ef0L	0x100
.fini_array	0x10095ef4L	0x4L
.jcr	0x10095ef8L	0x4L
.dynamic	0x10095efcL	0xf0L
.got	0x10095fecL	0x8L
.got.plt	0x10095ff4L	0xa8L
.data	0x1009609cL	0x20L
unknown1	0x100960c0L	0x180
.shstrtab	0x8048000L	0xedL

```
fcn.08048c
fcn.08048c96
fcn.08048ca6
fcn.08048cb6
fcn.08048cc6
fcn.08048cd6
fcn.08048ce6
fcn.08048cf6
fcn.08048c76
fcn.08048c86
fcn.08048c66
fcn.08048c16
fcn.08048c26
fcn.08048c36
fcn.08048c46
fcn.08048c06
```

```
   sym.imp.bindtextdomain()
0x08048db1    c7 04 24 7c b6 0.  mov dword [esp], 0x804b67c
0x08048db8    e8 e3 fd ff ff     call sym.imp.textdomain
   sym.imp.textdomain()
0x08048dbd    c7 04 24 c0 91 0.  mov dword [esp], 0x80491c0
0x08048dc4    e8 77 25 00 00     call 0x804b340
   0x0804b340() ; fcn.0804a1e7+4441
0x08048dc9    8b 45 0c           mov eax, dword [ebp + 0xc] ; [:4]=0
0x08048dcc    8b 58 04           mov ebx, dword [eax + 4] ; [:4]=0x10100
0x08048dcf    c7 44 24 04 9c b.  mov dword [esp + 4], str.__help ; [:4]=0x10100
0x08048dd7    89 1c 24           mov dword [esp], ebx
0x08048dda    e8 11 fd ff ff     call sym.imp.strcmp ; (fcn.08048aec)
   fcn.08048aec() ; sym.imp.strcmp
0x08048ddf    85 c0              test eax, eax
0x08048de1    74 53              je 0x8048e36
0x08048de3    c7 44 24 04 a3 b.  mov dword [esp + 4], str.__version ; [:4]=0x10100
0x08048deb    89 1c 24           mov dword [esp], ebx
0x08048dee    e8 fd fc ff ff     call sym.imp.strcmp ; (fcn.08048aec)
   fcn.08048aec() ; sym.imp.strcmp
0x08048df3    85 c0              test eax, eax
0x08048df5    0f 85 75 ff ff ff  jne 0x8048d70
0x08048dfb    a1 a4 e0 04 08     mov eax, dword [0x804e0a4] ; [:4]=0x804b600
0x08048e00    c7 44 24 14 00 0.  mov dword [esp + 0x14], 0 ; [:4]=0
0x08048e08    c7 44 24 10 ad b.  mov dword [esp + 0x10], str.Jim_Meyering ; [:4]=0x30000
0x08048e10    c7 44 24 08 78 b.  mov dword [esp + 8], str.GNU_coreutils ; [:4]=0
0x08048e18    89 44 24 0c        mov dword [esp + 0xc], eax ; [:4]=0
0x08048e1c    a1 e0 e0 04 08     mov eax, dword [sym.stdout] ; [:4]=0x6f6e2e00 ; sym.stdout
0x08048e21    c7 44 24 04 32 b.  mov dword [esp + 4], str.true ; [:4]=0x10100
0x08048e29    89 04 24           mov dword [esp], eax
0x08048e2c    e8 7f 1f 00 00     call 0x804adb0
   0x0804adb0() ; fcn.0804a1e7+3017
0x08048e31    e9 3a ff ff ff     jmp 0x8048d70 ; (section..text)
0x08048e36    c7 04 24 00 00 0.  mov dword [esp], 0
```

Size: 0x560cL **Processor:** Intel 80386 **Os:** linux **Name:** ../pocs/true32 **Format:** elf

Bokken 1.7-dev (Radare 0.9.8)



Function

- entry0
- fcn.00402068
- fcn.00402078
- fcn.00402088
- fcn.00402098
- fcn.004021d1
- fcn.0040249b
- fcn.004028b2
- fcn.00402938
- fcn.00402948
- fcn.00402968
- fcn.00402978
- fcn.00402988
- fcn.00402998
- fcn.004029a8
- fcn.004029b8
- fcn.004029c8
- fcn.004029d8
- fcn.004029e8
- fcn.004029f8
- fcn.00402a08
- fcn.00402a18
- fcn.00402a28
- fcn.00402a38
- fcn.00402a48
- fcn.00402a58

Extended file information

File info

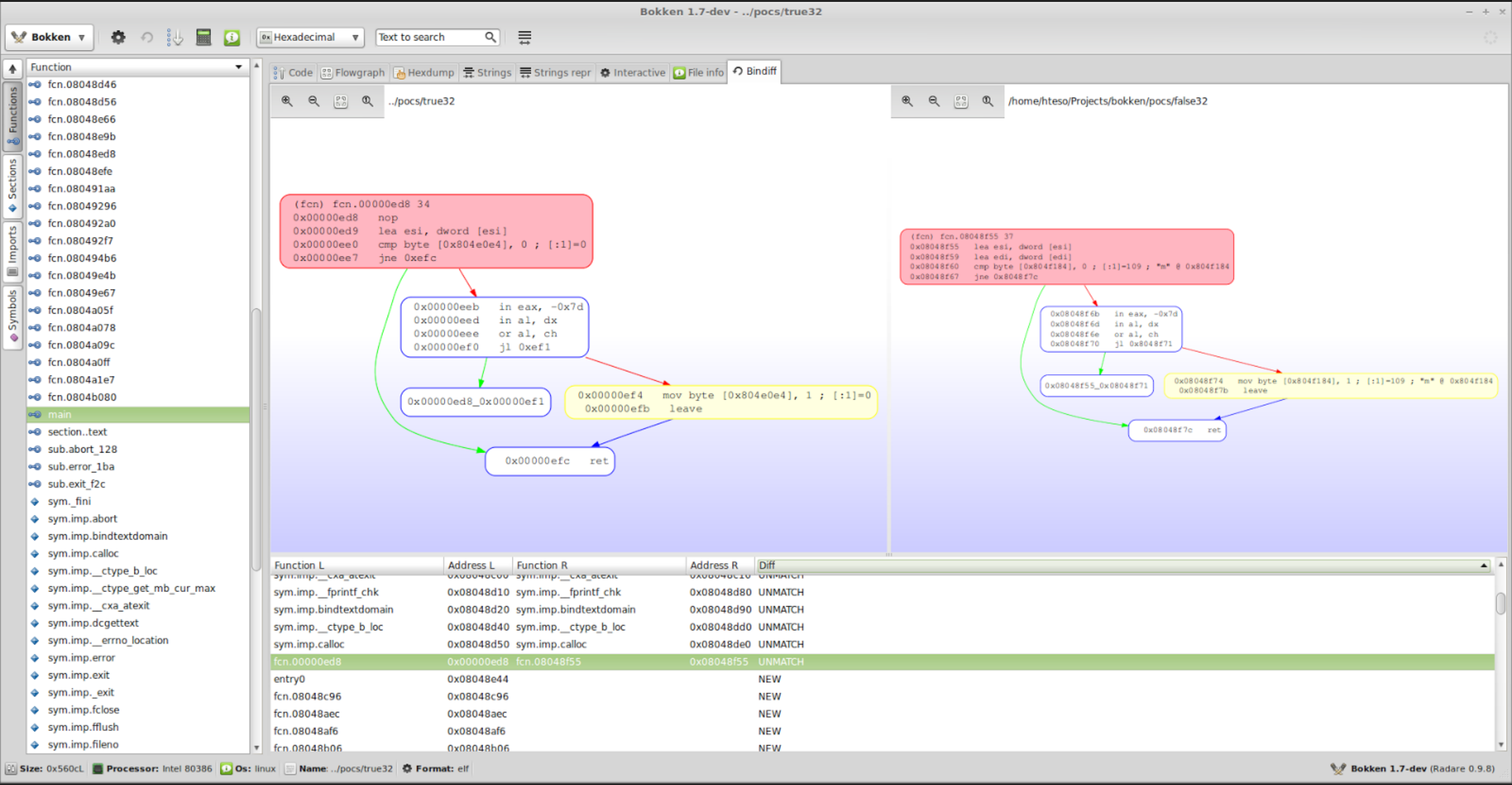
pic	false
canary	false
nx	false
crypto	false
va	true
bintype	pe
class	PE32
arch	x86
bits	32
machine	i386
os	windows
subsys	CUI
endian	little
stripped	false
static	false
linenum	true
lsyms	false

```
#
# Your python code goes here
# Press the run button above to execute
#
```

```
Builtin objects available
=========================

bin          core          functions          magic         imports        relocs
file_info              symbols         baddr       info          sections
strings      size
```

Size: 0x5ba8L Processor: i386 Os: windows Name: None Format: pe

Bokken 1.8-dev (Radare 0.9.9)



Bokken 1.7-dev - ../pocs/true32

Function

fcn.08048d46
fcn.08048d56
fcn.08048e66
fcn.08048e9b
fcn.08048ed8
fcn.08048efe
fcn.080491aa
fcn.08049296
fcn.080492a0
fcn.080492f7
fcn.080494b6
fcn.08049e4b
fcn.08049e67
fcn.0804a05f
fcn.0804a078
fcn.0804a09c
fcn.0804a0ff
fcn.0804a1e7
fcn.0804b080
main
section..text
sub.abort_128
sub.error_1ba
sub.exit_f2c
sym._fini
sym.imp.abort
sym.imp.bindtextdomain
sym.imp.calloc
sym.imp.__ctype_b_loc
sym.imp.__ctype_get_mb_cur_max
sym.imp.__cxa_atexit
sym.imp.dcgettext
sym.imp.__errno_location
sym.imp.error
sym.imp.exit
sym.imp._exit
sym.imp.fclose
sym.imp.fflush
sym.imp.fileno

../pocs/true32

```
(fcn) fcn.00000ed8 34
0x00000ed8   nop
0x00000ed9   lea esi, dword [esi]
0x00000ee0   cmp byte [0x804e0e4], 0 ; [:1]=0
0x00000ee7   jne 0xefc
```

```
0x00000eeb   in eax, -0x7d
0x00000eed   in al, dx
0x00000eee   or al, ch
0x00000ef0   jl 0xef1
```

```
0x00000ed8_0x00000ef1
```

```
0x00000ef4   mov byte [0x804e0e4], 1 ; [:1]=0
 0x00000efb   leave
```

```
0x00000efc   ret
```

/home/hteso/Projects/bokken/pocs/false32

```
(fcn) fcn.08048f55 37
0x08048f55   lea esi, dword [esi]
0x08048f59   lea edi, dword [edi]
0x08048f60   cmp byte [0x804f184], 0 ; [:1]=109 ; "m" @ 0x804f184
0x08048f67   jne 0x8048f7c
```

```
0x08048f6b   in eax, -0x7d
0x08048f6d   in al, dx
0x08048f6e   or al, ch
0x08048f70   jl 0x8048f71
```

```
0x08048f55_0x08048f71
```

```
0x08048f74   mov byte [0x804f184], 1 ; [:1]=109 ; "m" @ 0x804f184
 0x08048f7b   leave
```

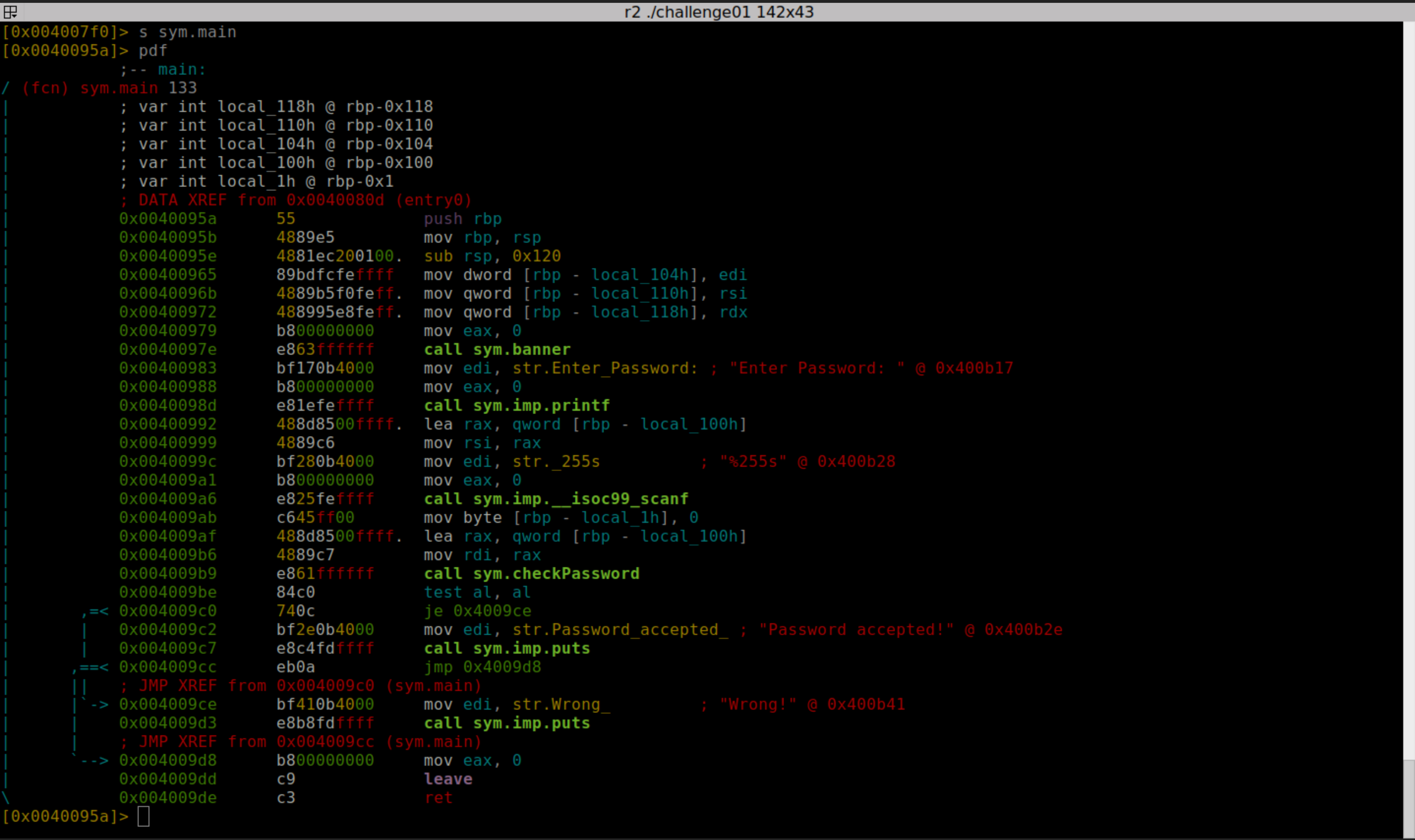
```
0x08048f7c   ret
```

Function L	Address L	Function R	Address R	Diff
sym.imp.__cxa_atexit	0x08048c00	sym.imp.__cxa_atexit	0x08048c10	UNMATCH
sym.imp.__fprintf_chk	0x08048d10	sym.imp.__fprintf_chk	0x08048d80	UNMATCH
sym.imp.bindtextdomain	0x08048d20	sym.imp.bindtextdomain	0x08048d90	UNMATCH
sym.imp.__ctype_b_loc	0x08048d40	sym.imp.__ctype_b_loc	0x08048dd0	UNMATCH
sym.imp.calloc	0x08048d50	sym.imp.calloc	0x08048de0	UNMATCH
fcn.00000ed8	0x00000ed8	fcn.08048f55	0x08048f55	UNMATCH
entry0	0x08048e44			NEW
fcn.08048c96	0x08048c96			NEW
fcn.08048aec	0x08048aec			NEW
fcn.08048af6	0x08048af6			NEW
fcn.08048b06	0x08048b06			NEW

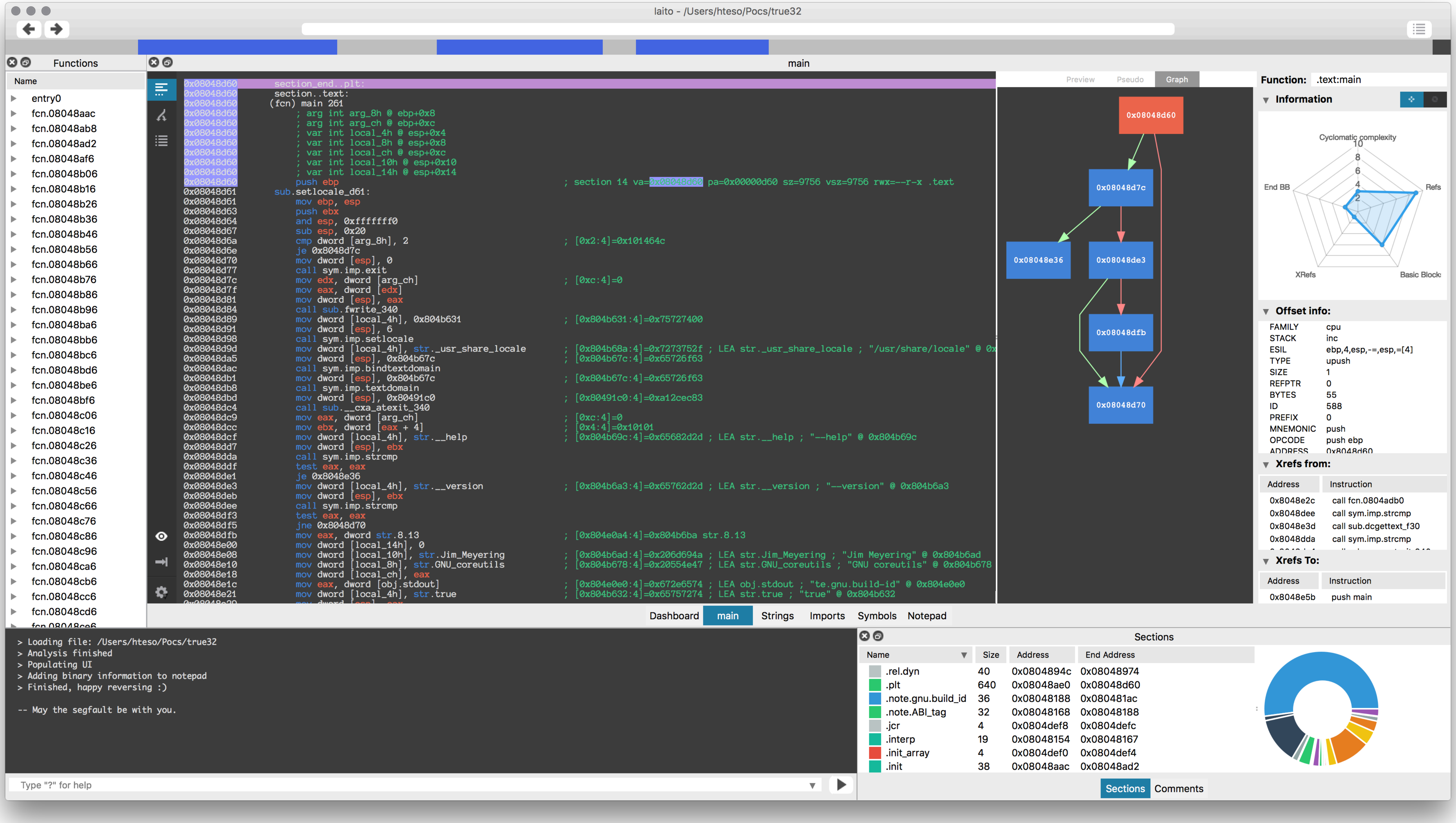
Size: 0x560cL **Processor:** Intel 80386 **Os:** linux **Name**: ../pocs/true32 **Format:** elf

Bokken 1.7-dev (Radare 0.9.8)

IAITÖ



```
[0x004007f0]> s sym.main
[0x0040095a]> pdf
            ;-- main:
/ (fcn) sym.main 133
|           ; var int local_118h @ rbp-0x118
|           ; var int local_110h @ rbp-0x110
|           ; var int local_104h @ rbp-0x104
|           ; var int local_100h @ rbp-0x100
|           ; var int local_1h @ rbp-0x1
|           ; DATA XREF from 0x0040080d (entry0)
|           0x0040095a      55             push rbp
|           0x0040095b      4889e5         mov rbp, rsp
|           0x0040095e      4881ec200100.  sub rsp, 0x120
|           0x00400965      89bdfcfeffff   mov dword [rbp - local_104h], edi
|           0x0040096b      4889b5f0feff.  mov qword [rbp - local_110h], rsi
|           0x00400972      488995e8feff.  mov qword [rbp - local_118h], rdx
|           0x00400979      b800000000     mov eax, 0
|           0x0040097e      e863ffffff     call sym.banner
|           0x00400983      bf170b4000     mov edi, str.Enter_Password: ; "Enter Password: " @ 0x400b17
|           0x00400988      b800000000     mov eax, 0
|           0x0040098d      e81efeffff     call sym.imp.printf
|           0x00400992      488d8500ffff.  lea rax, qword [rbp - local_100h]
|           0x00400999      4889c6         mov rsi, rax
|           0x0040099c      bf280b4000     mov edi, str._255s          ; "%255s" @ 0x400b28
|           0x004009a1      b800000000     mov eax, 0
|           0x004009a6      e825feffff     call sym.imp.__isoc99_scanf
|           0x004009ab      c645ff00       mov byte [rbp - local_1h], 0
|           0x004009af      488d8500ffff.  lea rax, qword [rbp - local_100h]
|           0x004009b6      4889c7         mov rdi, rax
|           0x004009b9      e861ffffff     call sym.checkPassword
|           0x004009be      84c0           test al, al
|       ,=< 0x004009c0      740c           je 0x4009ce
|       |   0x004009c2      bf2e0b4000     mov edi, str.Password_accepted_ ; "Password accepted!" @ 0x400b2e
|       |   0x004009c7      e8c4fdffff     call sym.imp.puts
|      ,==< 0x004009cc      eb0a           jmp 0x4009d8
|      ||   ; JMP XREF from 0x004009c0 (sym.main)
|      |`-> 0x004009ce      bf410b4000     mov edi, str.Wrong_         ; "Wrong!" @ 0x400b41
|      |    0x004009d3      e8b8fdffff     call sym.imp.puts
|      |    ; JMP XREF from 0x004009cc (sym.main)
|      `--> 0x004009d8      b800000000     mov eax, 0
|           0x004009dd      c9             leave
\           0x004009de      c3             ret
[0x0040095a]>
```



Name

entry0
fcn.08048aac
fcn.08048ab8
fcn.08048ad2
fcn.08048af6
fcn.08048b06
fcn.08048b16
fcn.08048b26
fcn.08048b36
fcn.08048b46
fcn.08048b56
fcn.08048b66
fcn.08048b76
fcn.08048b86
fcn.08048b96
fcn.08048ba6
fcn.08048bb6
fcn.08048bc6
fcn.08048bd6
fcn.08048be6
fcn.08048bf6
fcn.08048c06
fcn.08048c16
fcn.08048c26
fcn.08048c36
fcn.08048c46
fcn.08048c56
fcn.08048c66
fcn.08048c76
fcn.08048c86
fcn.08048c96
fcn.08048ca6
fcn.08048cb6
fcn.08048cc6
fcn.08048cd6

```
0x08048d60        section_end..plt:
0x08048d60        section..text:
0x08048d60       (fcn) main 261
0x08048d60            ; arg int arg_8h @ ebp+0x8
0x08048d60            ; arg int arg_ch @ ebp+0xc
0x08048d60            ; var int local_4h @ esp+0x4
0x08048d60            ; var int local_8h @ esp+0x8
0x08048d60            ; var int local_ch @ esp+0xc
0x08048d60            ; var int local_10h @ esp+0x10
0x08048d60            ; var int local_14h @ esp+0x14
0x08048d60            push ebp                                 ; section 14 va=0x08048d60 pa=0x00000d60 sz=9756 vsz=9756 rwx=--r-x .text
0x08048d61        sub.setlocale_d61:
0x08048d61            mov ebp, esp
0x08048d63            push ebx
0x08048d64            and esp, 0xfffffff0
0x08048d67            sub esp, 0x20
0x08048d6a            cmp dword [arg_8h], 2                    ; [0x2:4]=0x101464c
0x08048d6e            je 0x8048d7c
0x08048d70            mov dword [esp], 0
0x08048d77            call sym.imp.exit
0x08048d7c            mov edx, dword [arg_ch]                  ; [0xc:4]=0
0x08048d7f            mov eax, dword [edx]
0x08048d81            mov dword [esp], eax
0x08048d84            call sub.fwrite_340
0x08048d89            mov dword [local_4h], 0x804b631          ; [0x804b631:4]=0x75727400
0x08048d91            mov dword [esp], 6
0x08048d98            call sym.imp.setlocale
0x08048d9d            mov dword [local_4h], str._usr_share_locale  ; [0x804b68a:4]=0x7273752f ; LEA str._usr_share_locale ; "/usr/share/locale" @ 0x
0x08048da5            mov dword [esp], 0x804b67c               ; [0x804b67c:4]=0x65726f63
0x08048dac            call sym.imp.bindtextdomain
0x08048db1            mov dword [esp], 0x804b67c               ; [0x804b67c:4]=0x65726f63
0x08048db8            call sym.imp.textdomain
0x08048dbd            mov dword [esp], 0x80491c0               ; [0x80491c0:4]=0xa12cec83
0x08048dc4            call sub.__cxa_atexit_340
0x08048dc9            mov eax, dword [arg_ch]                  ; [0xc:4]=0
0x08048dcc            mov ebx, dword [eax + 4]                 ; [0x4:4]=0x10101
0x08048dcf            mov dword [local_4h], str.__help         ; [0x804b69c:4]=0x65682d2d ; LEA str.__help ; "--help" @ 0x804b69c
0x08048dd7            mov dword [esp], ebx
0x08048dda            call sym.imp.strcmp
0x08048ddf            test eax, eax
0x08048de1            je 0x8048e36
0x08048de3            mov dword [local_4h], str.__version      ; [0x804b6a3:4]=0x65762d2d ; LEA str.__version ; "--version" @ 0x804b6a3
0x08048deb            mov dword [esp], ebx
0x08048dee            call sym.imp.strcmp
0x08048df3            test eax, eax
0x08048df5            jne 0x8048d70
0x08048dfb            mov eax, dword str.8.13                  ; [0x804e0a4:4]=0x804b6ba str.8.13
0x08048e00            mov dword [local_14h], 0
0x08048e08            mov dword [local_10h], str.Jim_Meyering  ; [0x804b6ad:4]=0x206d694a ; LEA str.Jim_Meyering ; "Jim Meyering" @ 0x804b6ad
0x08048e10            mov dword [local_8h], str.GNU_coreutils  ; [0x804b678:4]=0x20554e47 ; LEA str.GNU_coreutils ; "GNU coreutils" @ 0x804b678
0x08048e18            mov dword [local_ch], eax
0x08048e1c            mov eax, dword [obj.stdout]              ; [0x804e0e0:4]=0x672e6574 ; LEA obj.stdout ; "te.gnu.build-id" @ 0x804e0e0
0x08048e21            mov dword [local_4h], str.true           ; [0x804b632:4]=0x65757274 ; LEA str.true ; "true" @ 0x804b632
```

Function: .text:main

▼ **Information**

▼ **Offset info:**

FAMILY	cpu
STACK	inc
ESIL	ebp,4,esp,-=,esp,=[4]
TYPE	upush
SIZE	1
REFPTR	0
BYTES	55
ID	588
PREFIX	0
MNEMONIC	push
OPCODE	push ebp
ADDRESS	0x8048d60

▼ **Xrefs from:**

Address	Instruction
0x8048e2c	call fcn.0804adb0
0x8048dee	call sym.imp.strcmp
0x8048e3d	call sub.dcgettext_f30
0x8048dda	call sym.imp.strcmp

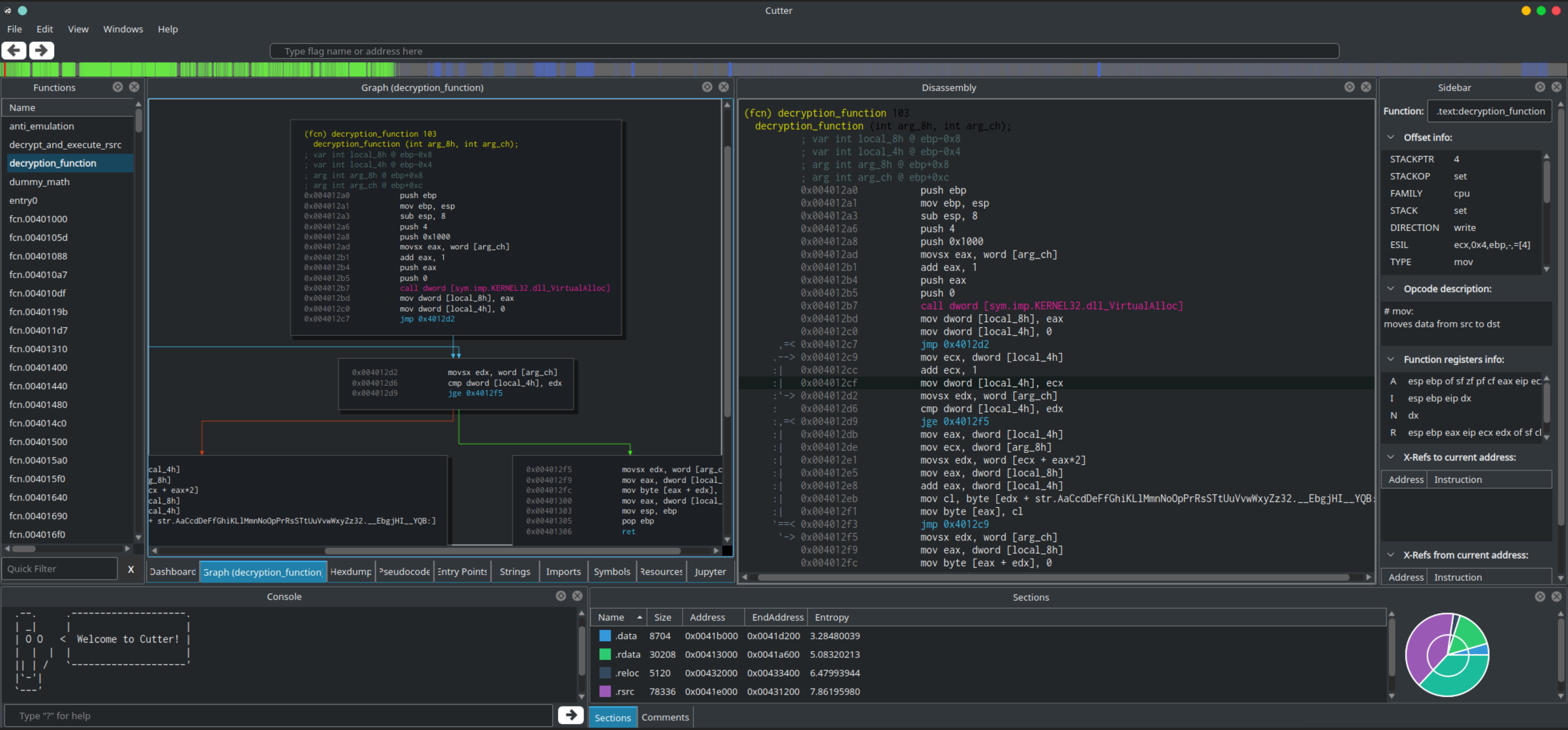
▼ **Xrefs To:**

Address	Instruction
0x8048e5b	push main

```
> Loading file: /Users/hteso/Pocs/true32
> Analysis finished
> Populating UI
> Adding binary information to notepad
> Finished, happy reversing :)

-- May the segfault be with you.
```

Sections

	Name	Size	Address	End Address
⬜	.rel.dyn	40	0x0804894c	0x08048974
🟩	.plt	640	0x08048ae0	0x08048d60
🟦	.note.gnu.build_id	36	0x08048188	0x080481ac
🟩	.note.ABI_tag	32	0x08048168	0x08048188
⬜	.jcr	4	0x0804def8	0x0804defc
🟩	.interp	19	0x08048154	0x08048167
🟥	.init_array	4	0x0804def0	0x0804def4
🟩	.init	38	0x08048aac	0x08048ad2



```
(fcn) decryption_function 103
  decryption_function (int arg_8h, int arg_ch);
          ; var int local_8h @ ebp-0x8
          ; var int local_4h @ ebp-0x4
          ; arg int arg_8h @ ebp+0x8
          ; arg int arg_ch @ ebp+0xc
          0x004012a0          push ebp
          0x004012a1          mov ebp, esp
          0x004012a3          sub esp, 8
          0x004012a6          push 4
          0x004012a8          push 0x1000
          0x004012ad          movsx eax, word [arg_ch]
          0x004012b1          add eax, 1
          0x004012b4          push eax
          0x004012b5          push 0
          0x004012b7          call dword [sym.imp.KERNEL32.dll_VirtualAlloc]
          0x004012bd          mov dword [local_8h], eax
          0x004012c0          mov dword [local_4h], 0
      ,=< 0x004012c7          jmp 0x4012d2
     .--> 0x004012c9          mov ecx, dword [local_4h]
     :|   0x004012cc          add ecx, 1
     :|   0x004012cf          mov dword [local_4h], ecx
     :`-> 0x004012d2          movsx edx, word [arg_ch]
     :    0x004012d6          cmp dword [local_4h], edx
     :,=< 0x004012d9          jge 0x4012f5
     :|   0x004012db          mov eax, dword [local_4h]
     :|   0x004012de          mov ecx, dword [arg_8h]
     :|   0x004012e1          movsx edx, word [ecx + eax*2]
     :|   0x004012e5          mov eax, dword [local_8h]
     :|   0x004012e8          add eax, dword [local_4h]
     :|   0x004012eb          mov cl, byte [edx + str.AaCcdDeFfGhiKLlMmnNoOpPrRsSTtUuVvwWxyZz32.__EbgjHI__YQB:
     :|   0x004012f1          mov byte [eax], cl
     `==< 0x004012f3          jmp 0x4012c9
      `-> 0x004012f5          movsx edx, word [arg_ch]
          0x004012f9          mov eax, dword [local_8h]
          0x004012fc          mov byte [eax + edx], 0
```

Function: .text:decryption_function

Offset info:

STACKPTR	4
STACKOP	set
FAMILY	cpu
STACK	set
DIRECTION	write
ESIL	ecx,0x4,ebp,-,=[4]
TYPE	mov

Opcode description:

mov:
moves data from src to dst

Function registers info:

A	esp ebp of sf zf pf cf eax eip ec:
I	esp ebp eip dx
N	dx
R	esp ebp eax eip ecx edx of sf cl

X-Refs to current address:

Address	Instruction

X-Refs from current address:

Address	Instruction

```
 .--.      .-------------------.
 | _|      |                   |
 | O O   <  Welcome to Cutter! |
 |  |  |   |                   |
 || | /    `-------------------'
 |`-'|
 `---'
```

Type "?" for help

Name	Size	Address	EndAddress	Entropy
🟦 .data	8704	0x0041b000	0x0041d200	3.28480039
🟩 .rdata	30208	0x00413000	0x0041a600	5.08320213
■ .reloc	5120	0x00432000	0x00433400	6.47993944
🟪 .rsrc	78336	0x0041e000	0x00431200	7.86195980

DO YOU SEE THE PATTERN?

Hugo Teso

DO YOU SEE THE PATTERN? CYBER-CYBER?

Hugo Teso

DO YOU SEE THE PATTERN?

~~CYBER CYBER?~~

UI/UX

Hugo Teso

OPEN SOURCE PROBLEM IS “NOT” SECURITY…

Hugo Teso

OPEN SOURCE PROBLEM IS
“NOT” SECURITY..
IS USABILITY!!

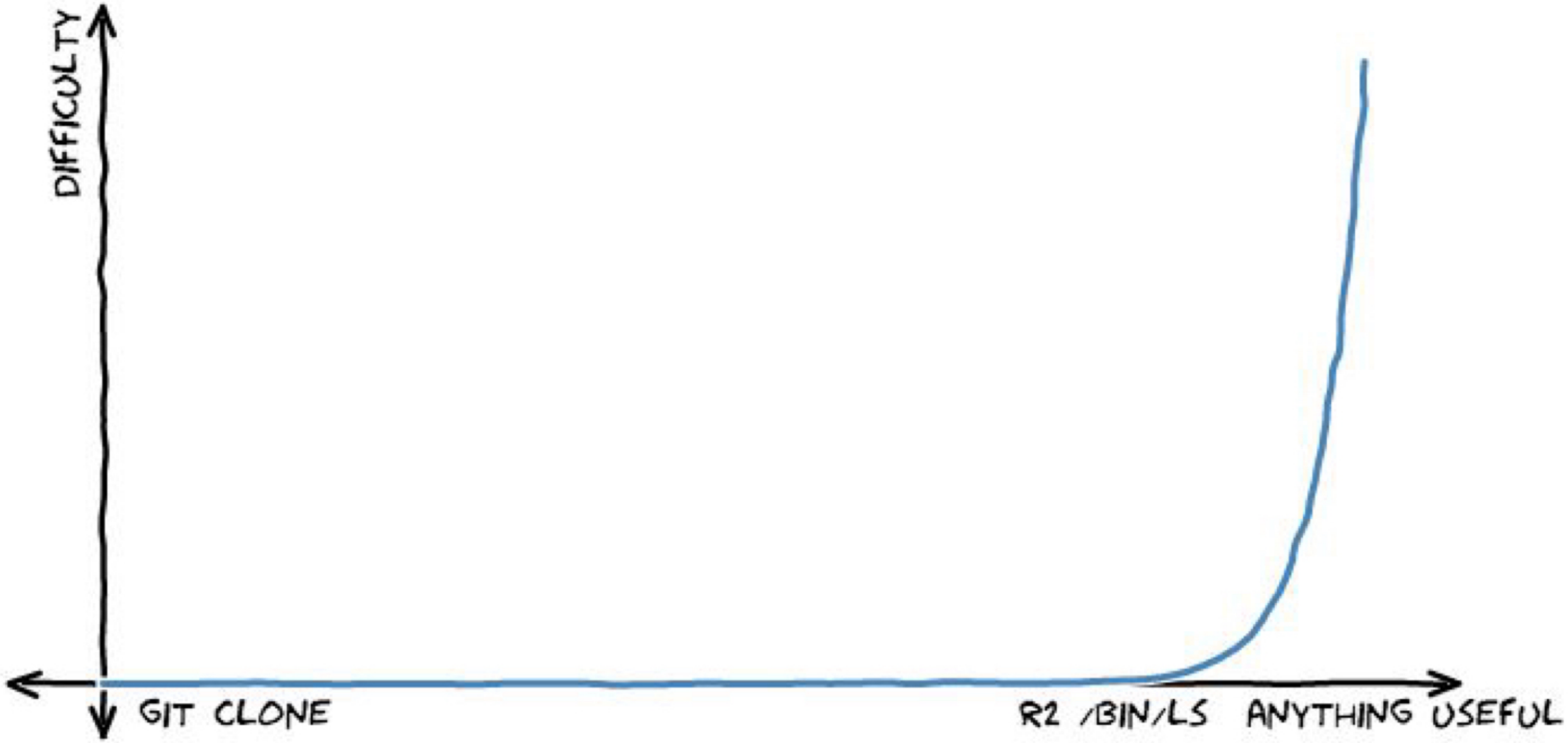
Hugo Teso

Origins of Cutter

- Iaito
- Qt/C++
- Developed for a while by only one person (Hugo Teso)
- Took a few years to become open source
- After it became open source, no more maintenance

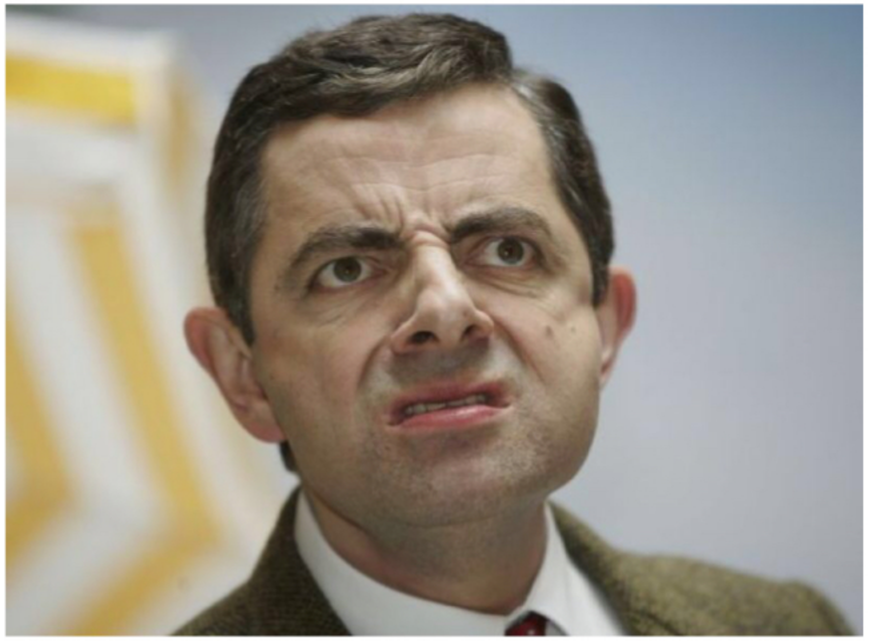
“Cutter is not aimed at existing radare2 users. It instead focuses on those whose are not yet radare2 users because of the learning curve, because they don't like CLI applications or because of the difficulty/instability of radare2.”

R2 LEARNING CURVE



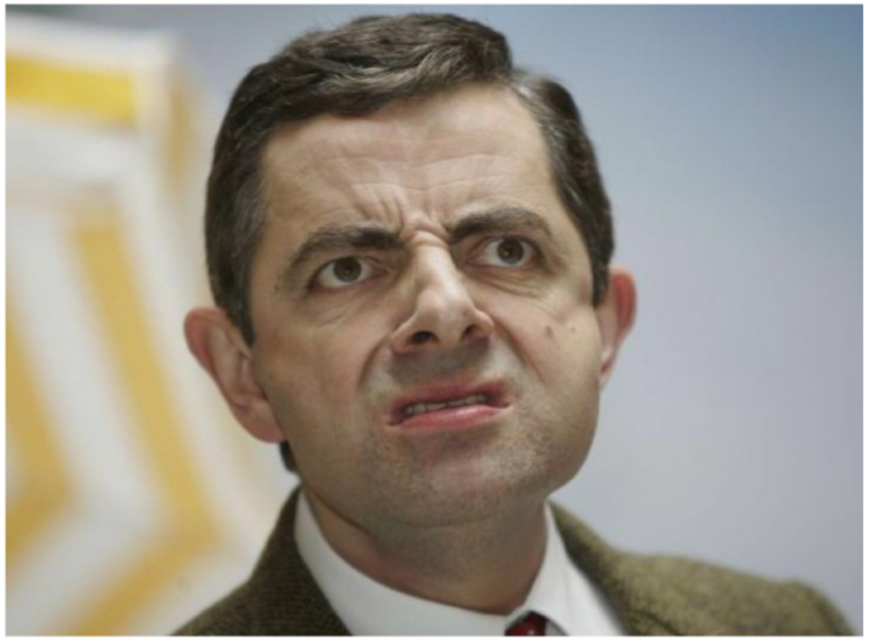
Old code...

- Many useless or unusable features (from a Reverse Engineer point of view)
- Displayed graphs with HTML (Qt WebEngine)



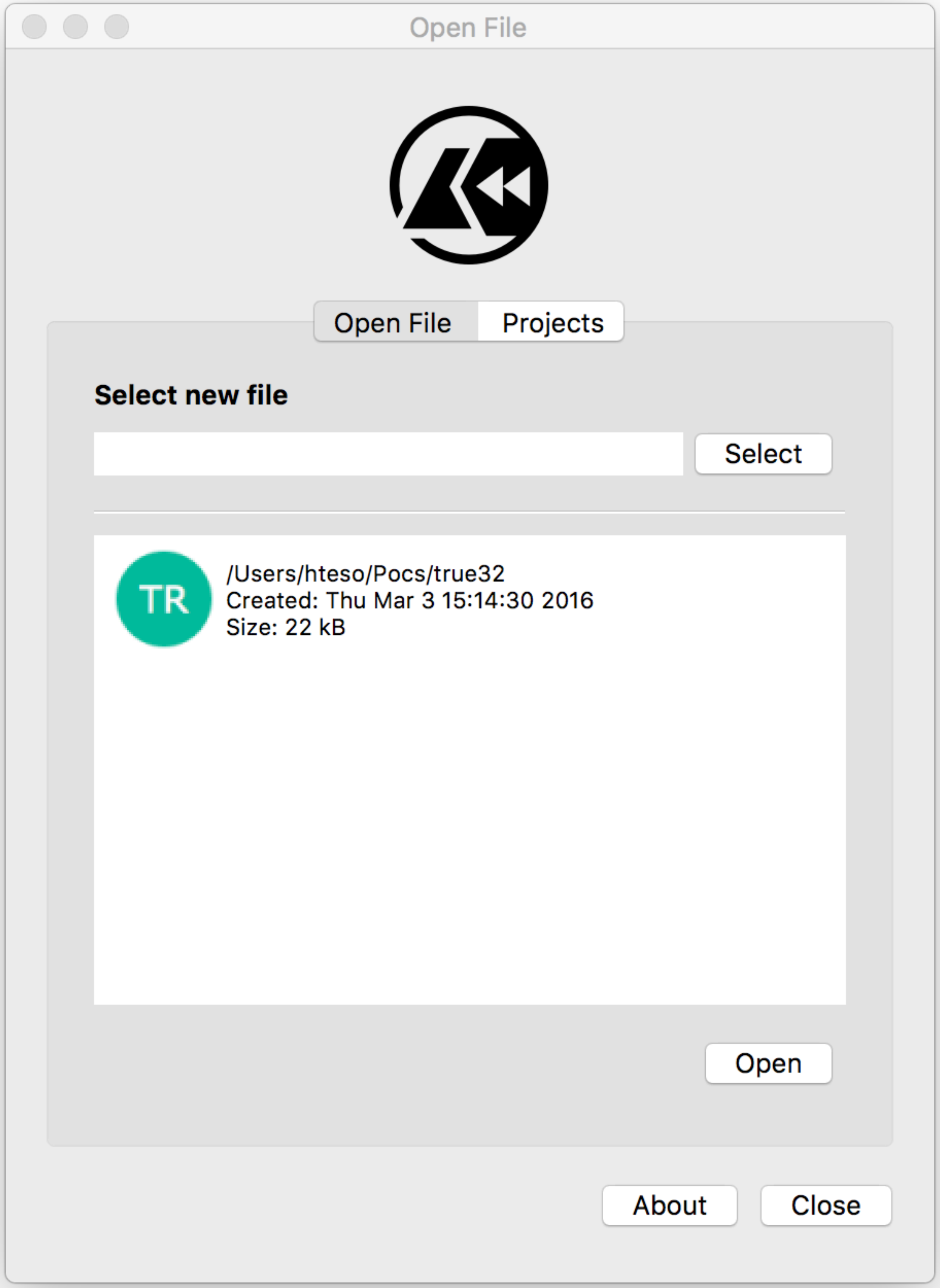
Old code...

- Many useless or unusable features (from a Reverse Engineer point of view)
- Displayed graphs with HTML (Qt WebEngine)

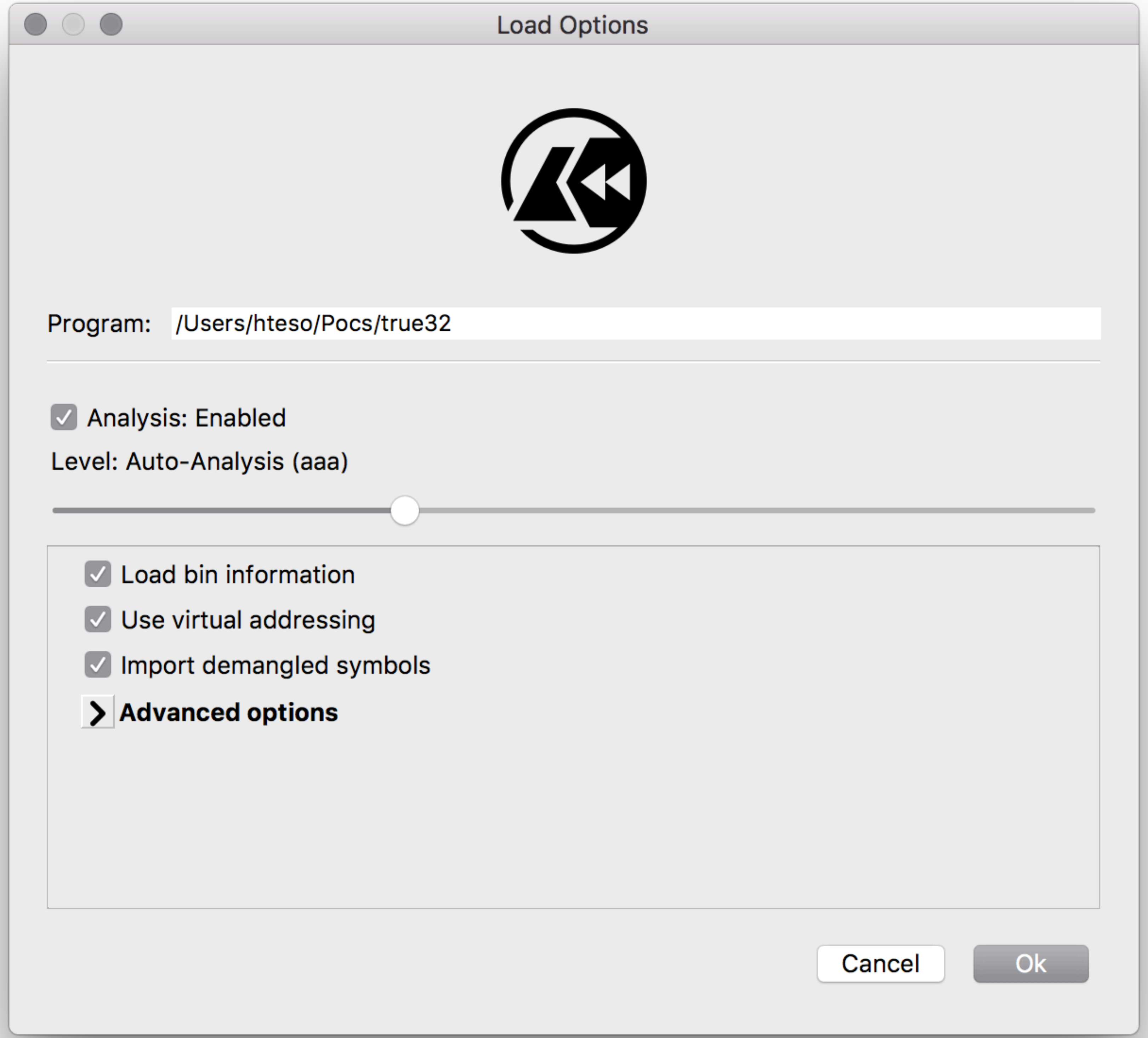


> A UI IS MUCH MORE THAN A CLI INSIDE A WINDOW

Hugo Teso



/Users/hteso/Pocs/true32
Created: Thu Mar 3 15:14:30 2016
Size: 22 kB



Program: /Users/hteso/Pocs/true32

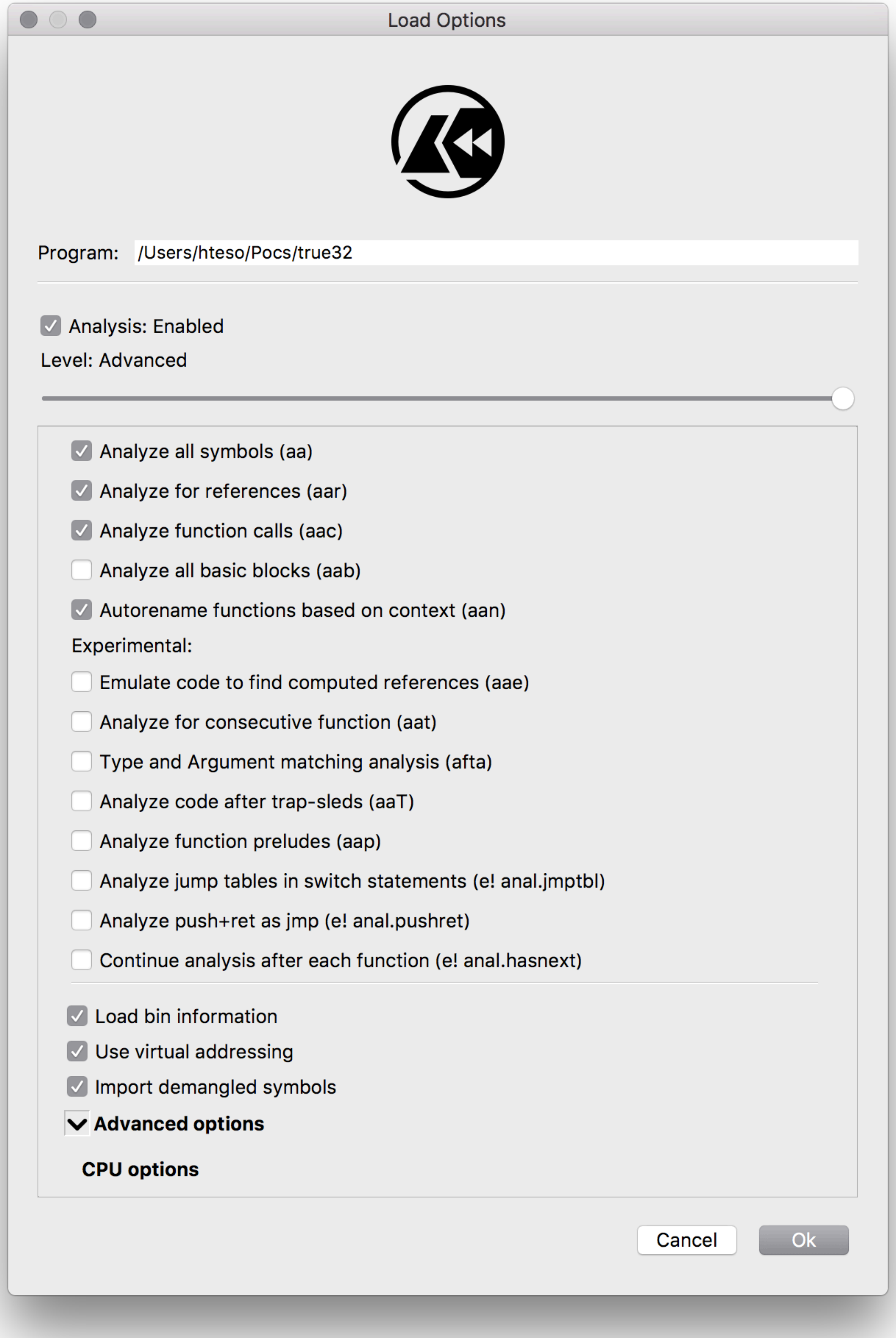
☑ Analysis: Enabled

Level: Auto-Analysis (aaa)

☑ Load bin information

☑ Use virtual addressing

☑ Import demangled symbols



Program: /Users/hteso/Pocs/true32

☑ Analysis: Enabled

Level: Advanced

☑ Analyze all symbols (aa)

☑ Analyze for references (aar)

☑ Analyze function calls (aac)

☐ Analyze all basic blocks (aab)

☑ Autorename functions based on context (aan)

Experimental:

☐ Emulate code to find computed references (aae)

☐ Analyze for consecutive function (aat)

☐ Type and Argument matching analysis (afta)

☐ Analyze code after trap-sleds (aaT)

☐ Analyze function preludes (aap)

☐ Analyze jump tables in switch statements (e! anal.jmptbl)

☐ Analyze push+ret as jmp (e! anal.pushret)

☐ Continue analysis after each function (e! anal.hasnext)

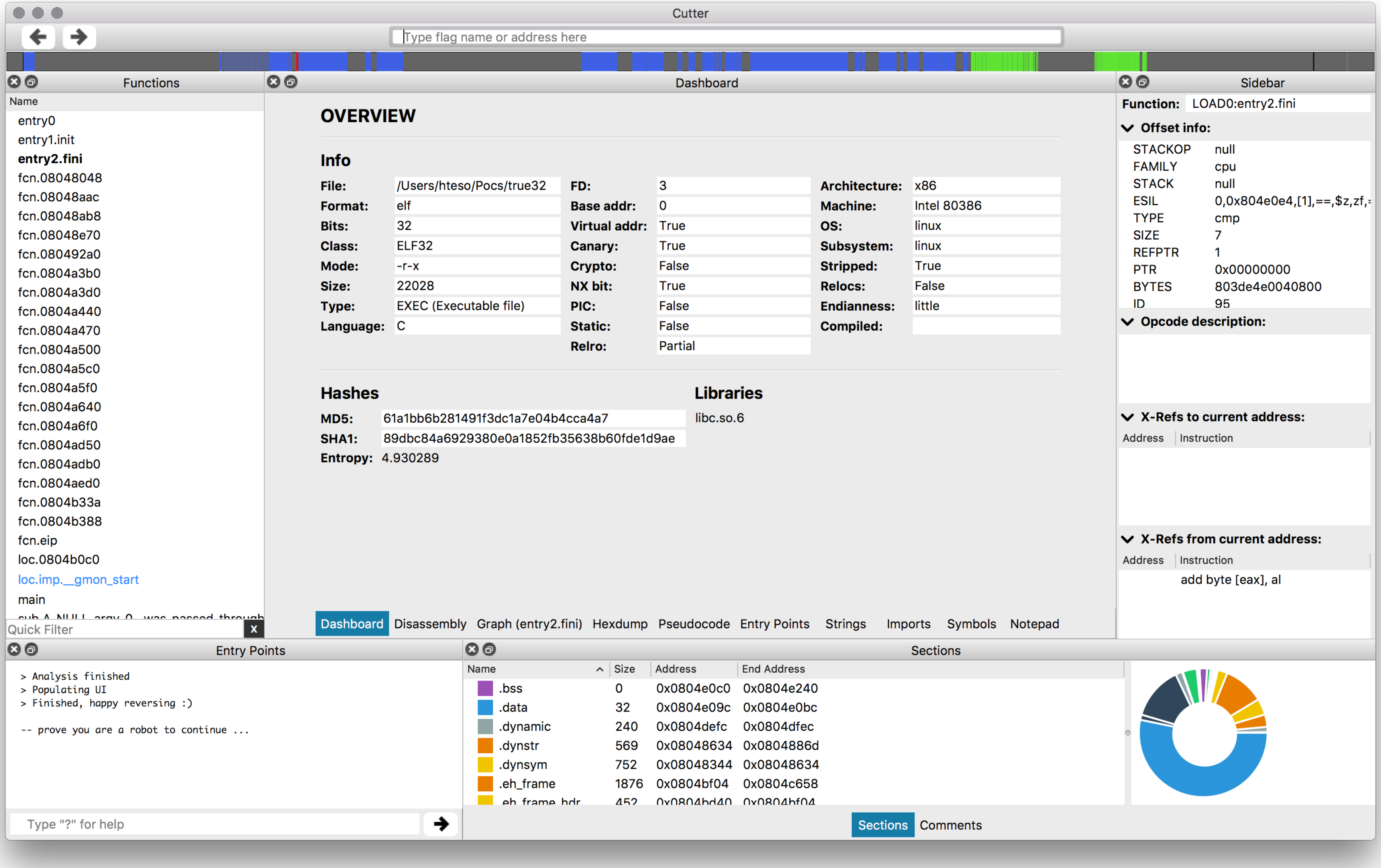
☑ Load bin information

☑ Use virtual addressing

☑ Import demangled symbols

Advanced options

CPU options



Name

entry0
entry1.init
entry2.fini
fcn.08048048
fcn.08048aac
fcn.08048ab8
fcn.08048e70
fcn.080492a0
fcn.0804a3b0
fcn.0804a3d0
fcn.0804a440
fcn.0804a470
fcn.0804a500
fcn.0804a5c0
fcn.0804a5f0
fcn.0804a640
fcn.0804a6f0
fcn.0804ad50
fcn.0804adb0
fcn.0804aed0
fcn.0804b33a
fcn.0804b388
fcn.eip
loc.0804b0c0
loc.imp.__gmon_start
main
sub.A_NULL_argv_0__was_passed_through

OVERVIEW

Info

File:	/Users/hteso/Pocs/true32	**FD:**	3	**Architecture:**	x86
Format:	elf	**Base addr:**	0	**Machine:**	Intel 80386
Bits:	32	**Virtual addr:**	True	**OS:**	linux
Class:	ELF32	**Canary:**	True	**Subsystem:**	linux
Mode:	-r-x	**Crypto:**	False	**Stripped:**	True
Size:	22028	**NX bit:**	True	**Relocs:**	False
Type:	EXEC (Executable file)	**PIC:**	False	**Endianness:**	little
Language:	C	**Static:**	False	**Compiled:**	
		Relro:	Partial		

Hashes

MD5: 61a1bb6b281491f3dc1a7e04b4cca4a7
SHA1: 89dbc84a6929380e0a1852fb35638b60fde1d9ae
Entropy: 4.930289

Libraries

libc.so.6

Function: LOAD0:entry2.fini

Offset info:

STACKOP	null
FAMILY	cpu
STACK	null
ESIL	0,0x804e0e4,[1],==,$z,zf,:
TYPE	cmp
SIZE	7
REFPTR	1
PTR	0x00000000
BYTES	803de4e0040800
ID	95

Opcode description:

X-Refs to current address:

Address	Instruction

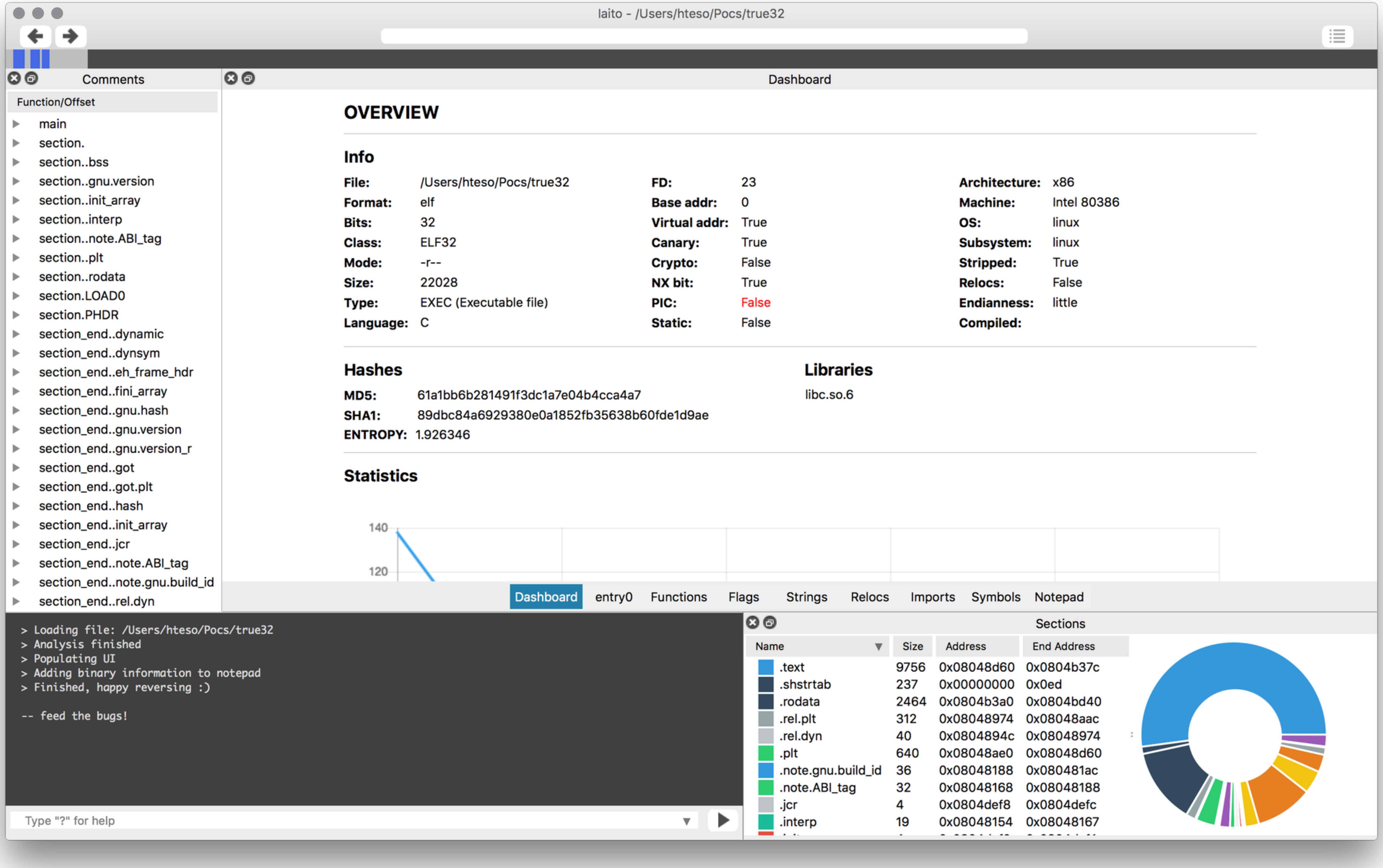
X-Refs from current address:

Address	Instruction
	add byte [eax], al

```
> Analysis finished
> Populating UI
> Finished, happy reversing :)

-- prove you are a robot to continue ...
```

	Name	Size	Address	End Address
🟪	.bss	0	0x0804e0c0	0x0804e240
🟦	.data	32	0x0804e09c	0x0804e0bc
◼	.dynamic	240	0x0804defc	0x0804dfec
🟧	.dynstr	569	0x08048634	0x0804886d
🟨	.dynsym	752	0x08048344	0x08048634
🟧	.eh_frame	1876	0x0804bf04	0x0804c658
🟨	.eh_frame_hdr	452	0x0804bd40	0x0804bf04

BACK TO THE FUTURE



Function/Offset

- main
- section.
- section..bss
- section..gnu.version
- section..init_array
- section..interp
- section..note.ABI_tag
- section..plt
- section..rodata
- section.LOAD0
- section.PHDR
- section_end..dynamic
- section_end..dynsym
- section_end..eh_frame_hdr
- section_end..fini_array
- section_end..gnu.hash
- section_end..gnu.version
- section_end..gnu.version_r
- section_end..got
- section_end..got.plt
- section_end..hash
- section_end..init_array
- section_end..jcr
- section_end..note.ABI_tag
- section_end..note.gnu.build_id
- section_end..rel.dyn

OVERVIEW

Info

File:	/Users/hteso/Pocs/true32	**FD:**	23	**Architecture:**	x86
Format:	elf	**Base addr:**	0	**Machine:**	Intel 80386
Bits:	32	**Virtual addr:**	True	**OS:**	linux
Class:	ELF32	**Canary:**	True	**Subsystem:**	linux
Mode:	-r--	**Crypto:**	False	**Stripped:**	True
Size:	22028	**NX bit:**	True	**Relocs:**	False
Type:	EXEC (Executable file)	**PIC:**	False	**Endianness:**	little
Language:	C	**Static:**	False	**Compiled:**	

Hashes

MD5: 61a1bb6b281491f3dc1a7e04b4cca4a7

SHA1: 89dbc84a6929380e0a1852fb35638b60fde1d9ae

ENTROPY: 1.926346

Libraries

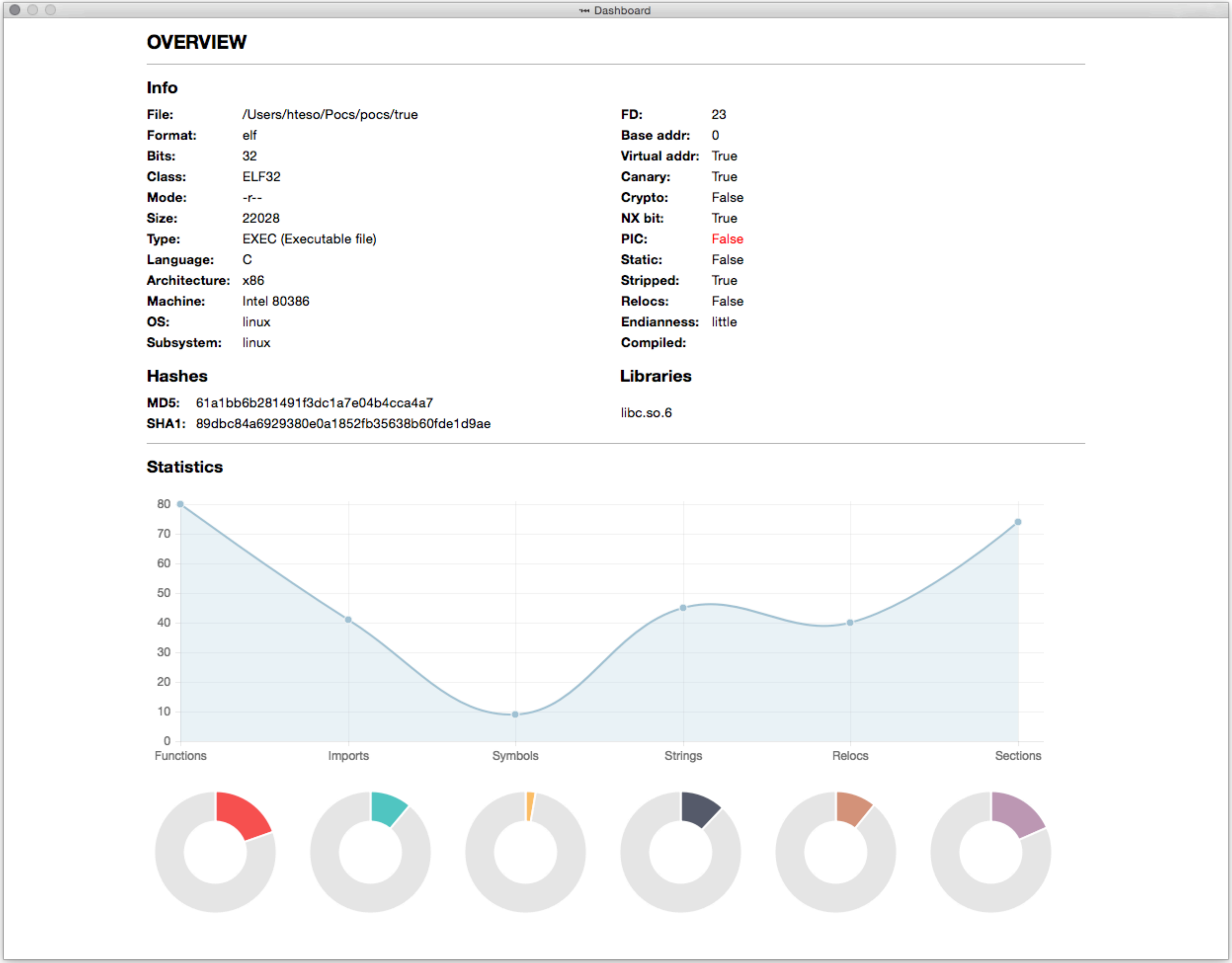
libc.so.6

Statistics

```
> Loading file: /Users/hteso/Pocs/true32
> Analysis finished
> Populating UI
> Adding binary information to notepad
> Finished, happy reversing :)

-- feed the bugs!
```

Type "?" for help

Name	Size	Address	End Address
.text	9756	0x08048d60	0x0804b37c
.shstrtab	237	0x00000000	0x0ed
.rodata	2464	0x0804b3a0	0x0804bd40
.rel.plt	312	0x08048974	0x08048aac
.rel.dyn	40	0x0804894c	0x08048974
.plt	640	0x08048ae0	0x08048d60
.note.gnu.build_id	36	0x08048188	0x080481ac
.note.ABI_tag	32	0x08048168	0x08048188
.jcr	4	0x0804def8	0x0804defc
.interp	19	0x08048154	0x08048167



Dashboard

OVERVIEW

Info

File:	/Users/hteso/Pocs/pocs/true	**FD:**	23
Format:	elf	**Base addr:**	0
Bits:	32	**Virtual addr:**	True
Class:	ELF32	**Canary:**	True
Mode:	-r--	**Crypto:**	False
Size:	22028	**NX bit:**	True
Type:	EXEC (Executable file)	**PIC:**	False
Language:	C	**Static:**	False
Architecture:	x86	**Stripped:**	True
Machine:	Intel 80386	**Relocs:**	False
OS:	linux	**Endianness:**	little
Subsystem:	linux	**Compiled:**	

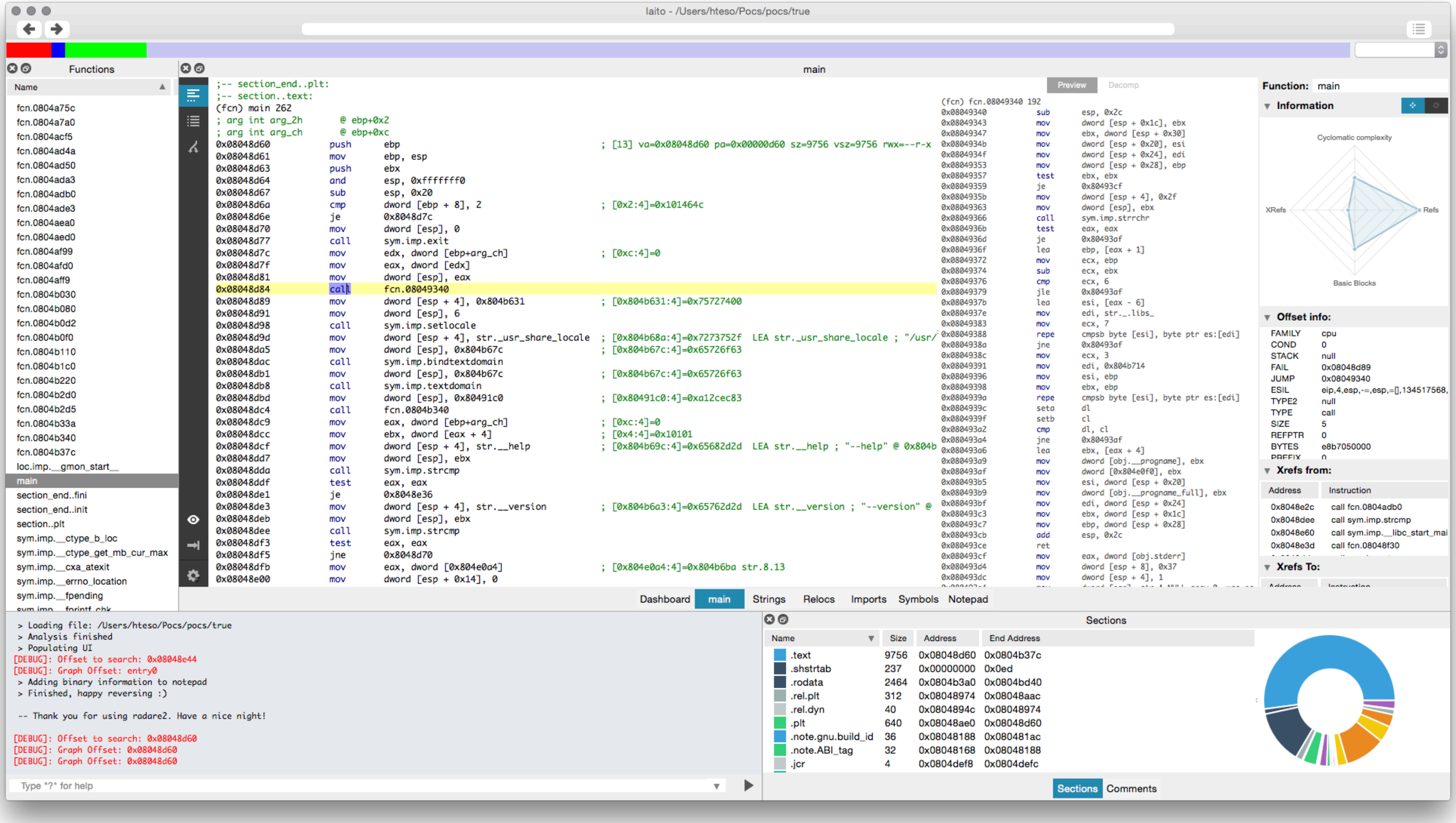
Hashes

MD5:	61a1bb6b281491f3dc1a7e04b4cca4a7
SHA1:	89dbc84a6929380e0a1852fb35638b60fde1d9ae

Libraries

libc.so.6

Statistics



Functions

fcn.0804a75c
fcn.0804a7a0
fcn.0804acf5
fcn.0804ad4a
fcn.0804ad50
fcn.0804ada3
fcn.0804adb0
fcn.0804ade3
fcn.0804aea0
fcn.0804aed0
fcn.0804af99
fcn.0804afd0
fcn.0804aff9
fcn.0804b030
fcn.0804b080
fcn.0804b0d2
fcn.0804b0f0
fcn.0804b110
fcn.0804b1c0
fcn.0804b220
fcn.0804b2d0
fcn.0804b2d5
fcn.0804b33a
fcn.0804b340
fcn.0804b37c
loc.imp.__gmon_start__
main
section_end..fini
section_end..init
section..plt
sym.imp.__ctype_b_loc
sym.imp.__ctype_get_mb_cur_max
sym.imp.__cxa_atexit
sym.imp.__errno_location
sym.imp.__fpending

main

```
;-- section_end..plt:
;-- section..text:
(fcn) main 262
; arg int arg_2h        @ ebp+0x2
; arg int arg_ch        @ ebp+0xc
0x08048d60         push    ebp                                 ; [13] va=0x08048d60 pa=0x00000d60 sz=9756 vsz=9756 rwx=--r-x
0x08048d61         mov     ebp, esp
0x08048d63         push    ebx
0x08048d64         and     esp, 0xfffffff0
0x08048d67         sub     esp, 0x20
0x08048d6a         cmp     dword [ebp + 8], 2                  ; [0x2:4]=0x101464c
0x08048d6e         je      0x8048d7c
0x08048d70         mov     dword [esp], 0
0x08048d77         call    sym.imp.exit
0x08048d7c         mov     edx, dword [ebp+arg_ch]             ; [0xc:4]=0
0x08048d7f         mov     eax, dword [edx]
0x08048d81         mov     dword [esp], eax
0x08048d84         call    fcn.08049340
0x08048d89         mov     dword [esp + 4], 0x804b631          ; [0x804b631:4]=0x75727400
0x08048d91         mov     dword [esp], 6
0x08048d98         call    sym.imp.setlocale
0x08048d9d         mov     dword [esp + 4], str._usr_share_locale  ; [0x804b68a:4]=0x7273752f  LEA str._usr_share_locale ; "/usr/
0x08048da5         mov     dword [esp], 0x804b67c              ; [0x804b67c:4]=0x65726f63
0x08048dac         call    sym.imp.bindtextdomain
0x08048db1         mov     dword [esp], 0x804b67c              ; [0x804b67c:4]=0x65726f63
0x08048db8         call    sym.imp.textdomain
0x08048dbd         mov     dword [esp], 0x80491c0              ; [0x80491c0:4]=0xa12cec83
0x08048dc4         call    fcn.0804b340
0x08048dc9         mov     eax, dword [ebp+arg_ch]             ; [0xc:4]=0
0x08048dcc         mov     ebx, dword [eax + 4]                ; [0x4:4]=0x10101
0x08048dcf         mov     dword [esp + 4], str.__help         ; [0x804b69c:4]=0x65682d2d  LEA str.__help ; "--help" @ 0x804b
0x08048dd7         mov     dword [esp], ebx
0x08048dda         call    sym.imp.strcmp
0x08048ddf         test    eax, eax
0x08048de1         je      0x8048e36
0x08048de3         mov     dword [esp + 4], str.__version      ; [0x804b6a3:4]=0x65762d2d  LEA str.__version ; "--version" @
0x08048deb         mov     dword [esp], ebx
0x08048dee         call    sym.imp.strcmp
0x08048df3         test    eax, eax
0x08048df5         jne     0x8048d70
0x08048dfb         mov     eax, dword [0x804e0a4]              ; [0x804e0a4:4]=0x804b6ba str.8.13
0x08048e00         mov     dword [esp + 0x14], 0
```

```
(fcn) fcn.08049340 192
0x08049340         sub     esp, 0x2c
0x08049343         mov     dword [esp + 0x1c], ebx
0x08049347         mov     ebx, dword [esp + 0x30]
0x0804934b         mov     dword [esp + 0x20], esi
0x0804934f         mov     dword [esp + 0x24], edi
0x08049353         mov     dword [esp + 0x28], ebp
0x08049357         test    ebx, ebx
0x08049359         je      0x80493cf
0x0804935b         mov     dword [esp + 4], 0x2f
0x08049363         mov     dword [esp], ebx
0x08049366         call    sym.imp.strrchr
0x0804936b         test    eax, eax
0x0804936d         je      0x80493af
0x0804936f         lea     ebp, [eax + 1]
0x08049372         mov     ecx, ebp
0x08049374         sub     ecx, ebx
0x08049376         cmp     ecx, 6
0x08049379         jle     0x80493af
0x0804937b         lea     esi, [eax - 6]
0x0804937e         mov     edi, str._.libs_
0x08049383         mov     ecx, 7
0x08049388         repe    cmpsb byte [esi], byte ptr es:[edi]
0x0804938a         jne     0x80493af
0x0804938c         mov     ecx, 3
0x08049391         mov     edi, 0x804b714
0x08049396         mov     esi, ebp
0x08049398         mov     ebx, ebp
0x0804939a         repe    cmpsb byte [esi], byte ptr es:[edi]
0x0804939c         seta    dl
0x0804939f         setb    cl
0x080493a2         cmp     dl, cl
0x080493a4         jne     0x80493af
0x080493a6         lea     ebx, [eax + 4]
0x080493a9         mov     dword [obj.__progname], ebx
0x080493af         mov     dword [0x804e0f0], ebx
0x080493b5         mov     esi, dword [esp + 0x20]
0x080493b9         mov     dword [obj.__progname_full], ebx
0x080493bf         mov     edi, dword [esp + 0x24]
0x080493c3         mov     ebx, dword [esp + 0x1c]
0x080493c7         mov     ebp, dword [esp + 0x28]
0x080493cb         add     esp, 0x2c
0x080493ce         ret
0x080493cf         mov     eax, dword [obj.stderr]
0x080493d4         mov     dword [esp + 8], 0x37
0x080493dc         mov     dword [esp + 4], 1
```

Function: main

Information

Offset info:

FAMILY	cpu
COND	0
STACK	null
FAIL	0x08048d89
JUMP	0x08049340
ESIL	eip,4,esp,-=,esp,=[],134517568,
TYPE2	null
TYPE	call
SIZE	5
REFPTR	0
BYTES	e8b7050000
PREFIX	0

Xrefs from:

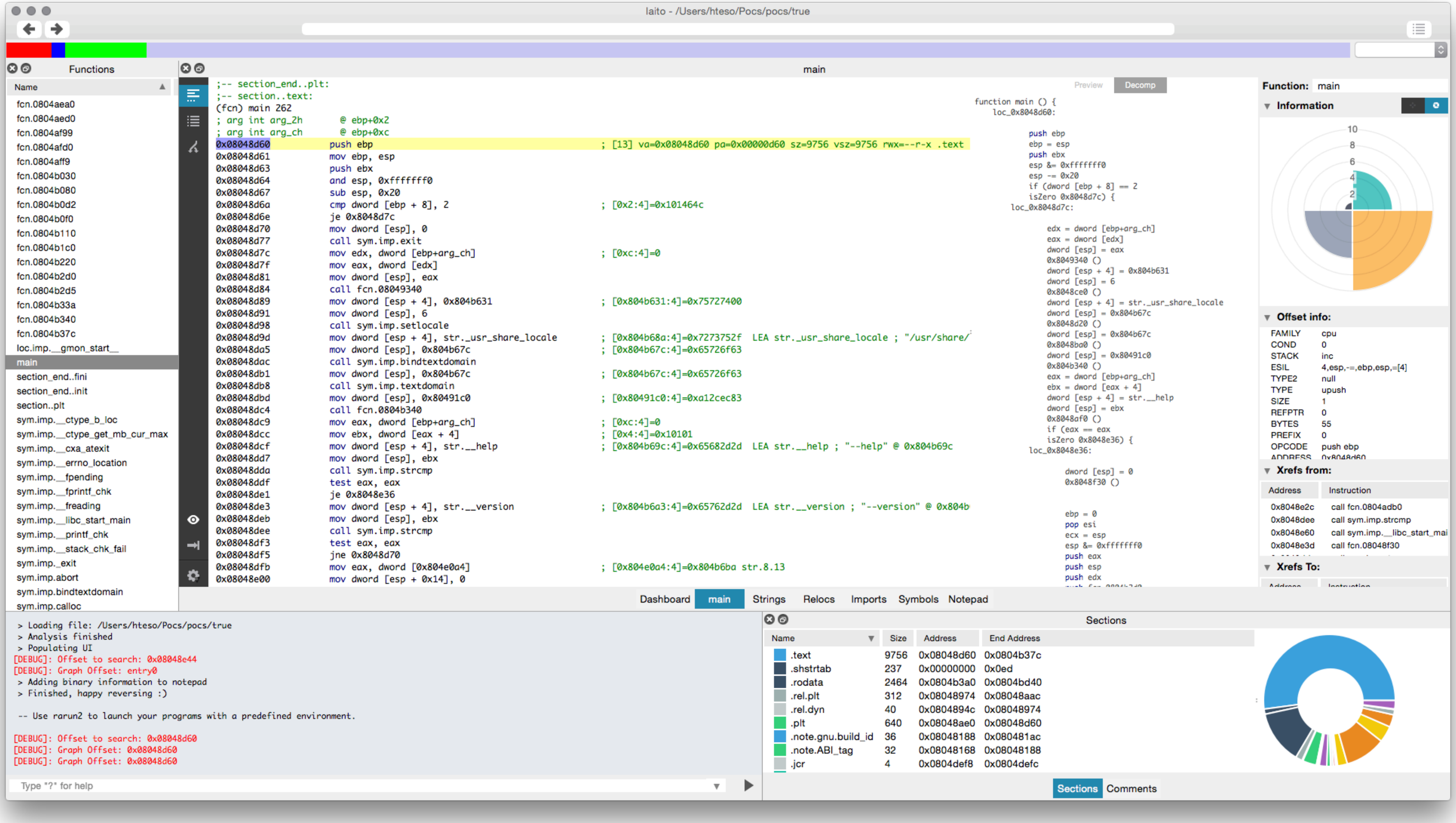
Address	Instruction
0x8048e2c	call fcn.0804adb0
0x8048dee	call sym.imp.strcmp
0x8048e60	call sym.imp.__libc_start_mai
0x8048e3d	call fcn.08048f30

Xrefs To:

```
 > Loading file: /Users/hteso/Pocs/pocs/true
 > Analysis finished
 > Populating UI
[DEBUG]: Offset to search: 0x08048e44
[DEBUG]: Graph Offset: entry0
 > Adding binary information to notepad
 > Finished, happy reversing :)

 -- Thank you for using radare2. Have a nice night!

[DEBUG]: Offset to search: 0x08048d60
[DEBUG]: Graph Offset: 0x08048d60
[DEBUG]: Graph Offset: 0x08048d60
```

Sections

Name	Size	Address	End Address
.text	9756	0x08048d60	0x0804b37c
.shstrtab	237	0x00000000	0x0ed
.rodata	2464	0x0804b3a0	0x0804bd40
.rel.plt	312	0x08048974	0x08048aac
.rel.dyn	40	0x0804894c	0x08048974
.plt	640	0x08048ae0	0x08048d60
.note.gnu.build_id	36	0x08048188	0x080481ac
.note.ABI_tag	32	0x08048168	0x08048188
.jcr	4	0x0804def8	0x0804defc



```
fcn.0804aea0
fcn.0804aed0
fcn.0804af99
fcn.0804afd0
fcn.0804aff9
fcn.0804b030
fcn.0804b080
fcn.0804b0d2
fcn.0804b0f0
fcn.0804b110
fcn.0804b1c0
fcn.0804b220
fcn.0804b2d0
fcn.0804b2d5
fcn.0804b33a
fcn.0804b340
fcn.0804b37c
loc.imp.__gmon_start__
main
section_end..fini
section_end..init
section..plt
sym.imp.__ctype_b_loc
sym.imp.__ctype_get_mb_cur_max
sym.imp.__cxa_atexit
sym.imp.__errno_location
sym.imp.__fpending
sym.imp.__fprintf_chk
sym.imp.__freading
sym.imp.__libc_start_main
sym.imp.__printf_chk
sym.imp.__stack_chk_fail
sym.imp._exit
sym.imp.abort
sym.imp.bindtextdomain
sym.imp.calloc
```

```
;-- section_end..plt:
;-- section..text:
(fcn) main 262
; arg int arg_2h       @ ebp+0x2
; arg int arg_ch       @ ebp+0xc
0x08048d60          push ebp                                    ; [13] va=0x08048d60 pa=0x00000d60 sz=9756 vsz=9756 rwx=--r-x .text
0x08048d61          mov ebp, esp
0x08048d63          push ebx
0x08048d64          and esp, 0xfffffff0
0x08048d67          sub esp, 0x20
0x08048d6a          cmp dword [ebp + 8], 2                      ; [0x2:4]=0x101464c
0x08048d6e          je 0x8048d7c
0x08048d70          mov dword [esp], 0
0x08048d77          call sym.imp.exit
0x08048d7c          mov edx, dword [ebp+arg_ch]                 ; [0xc:4]=0
0x08048d7f          mov eax, dword [edx]
0x08048d81          mov dword [esp], eax
0x08048d84          call fcn.08049340
0x08048d89          mov dword [esp + 4], 0x804b631              ; [0x804b631:4]=0x75727400
0x08048d91          mov dword [esp], 6
0x08048d98          call sym.imp.setlocale
0x08048d9d          mov dword [esp + 4], str._usr_share_locale  ; [0x804b68a:4]=0x7273752f  LEA str._usr_share_locale ; "/usr/share/
0x08048da5          mov dword [esp], 0x804b67c                  ; [0x804b67c:4]=0x65726f63
0x08048dac          call sym.imp.bindtextdomain
0x08048db1          mov dword [esp], 0x804b67c                  ; [0x804b67c:4]=0x65726f63
0x08048db8          call sym.imp.textdomain
0x08048dbd          mov dword [esp], 0x80491c0                  ; [0x80491c0:4]=0xa12cec83
0x08048dc4          call fcn.0804b340
0x08048dc9          mov eax, dword [ebp+arg_ch]                 ; [0xc:4]=0
0x08048dcc          mov ebx, dword [eax + 4]                    ; [0x4:4]=0x10101
0x08048dcf          mov dword [esp + 4], str.__help             ; [0x804b69c:4]=0x65682d2d  LEA str.__help ; "--help" @ 0x804b69c
0x08048dd7          mov dword [esp], ebx
0x08048dda          call sym.imp.strcmp
0x08048ddf          test eax, eax
0x08048de1          je 0x8048e36
0x08048de3          mov dword [esp + 4], str.__version          ; [0x804b6a3:4]=0x65762d2d  LEA str.__version ; "--version" @ 0x804b
0x08048deb          mov dword [esp], ebx
0x08048dee          call sym.imp.strcmp
0x08048df3          test eax, eax
0x08048df5          jne 0x8048d70
0x08048dfb          mov eax, dword [0x804e0a4]                  ; [0x804e0a4:4]=0x804b6ba str.8.13
0x08048e00          mov dword [esp + 0x14], 0
```

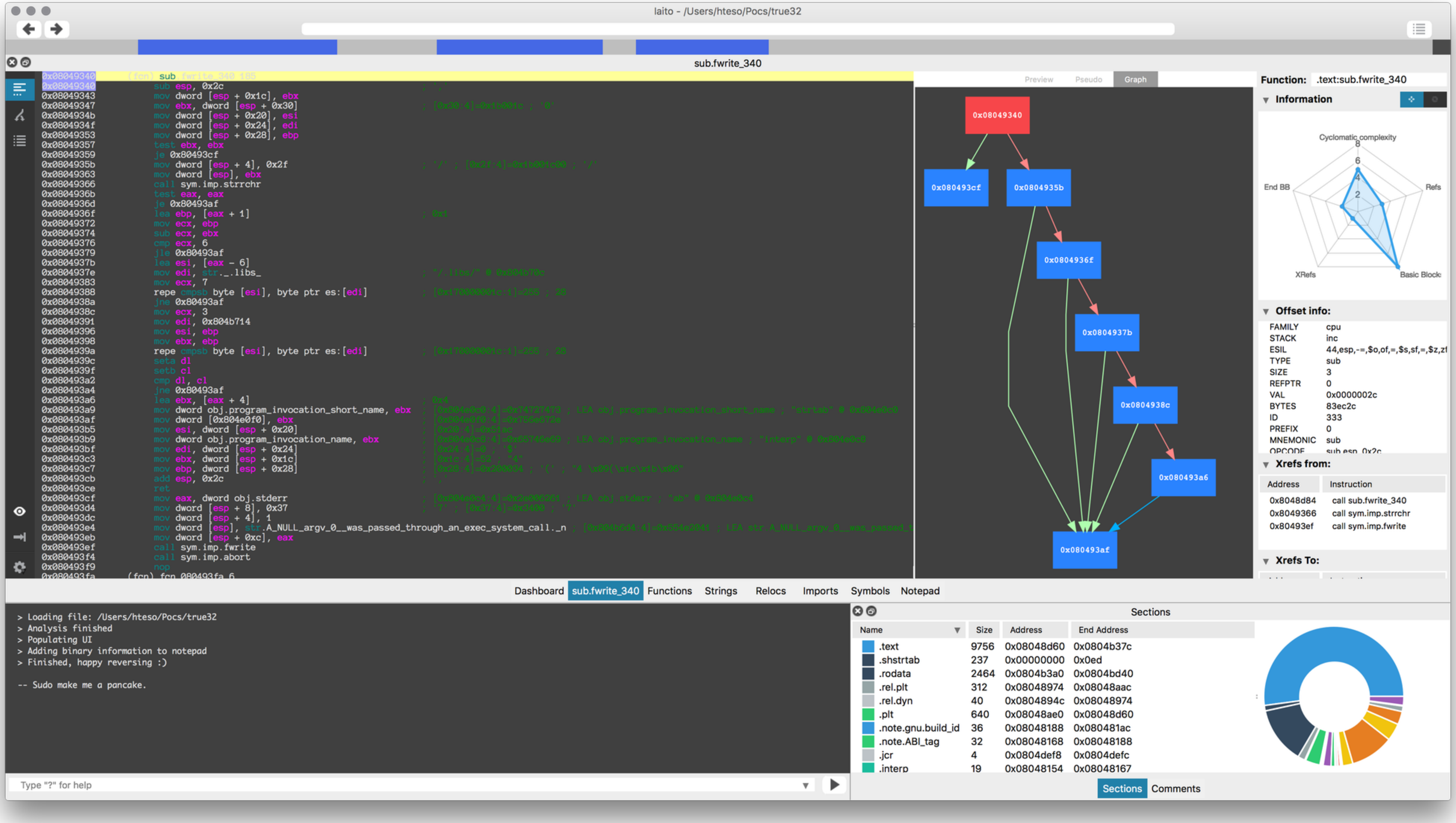
```
function main () {
    loc_0x8048d60:

          push ebp
          ebp = esp
          push ebx
          esp &= 0xfffffff0
          esp -= 0x20
          if (dword [ebp + 8] == 2
          isZero 0x8048d7c) {
       loc_0x8048d7c:

             edx = dword [ebp+arg_ch]
             eax = dword [edx]
             dword [esp] = eax
             0x8049340 ()
             dword [esp + 4] = 0x804b631
             dword [esp] = 6
             0x8048ce0 ()
             dword [esp + 4] = str._usr_share_locale
             dword [esp] = 0x804b67c
             0x8048d20 ()
             dword [esp] = 0x804b67c
             0x8048ba0 ()
             dword [esp] = 0x80491c0
             0x804b340 ()
             eax = dword [ebp+arg_ch]
             ebx = dword [eax + 4]
             dword [esp + 4] = str.__help
             dword [esp] = ebx
             0x8048af0 ()
             if (eax == eax
             isZero 0x8048e36) {
          loc_0x8048e36:

                dword [esp] = 0
                0x8048f30 ()


                ebp = 0
                pop esi
                ecx = esp
                esp &= 0xfffffff0
                push eax
                push esp
                push edx
```

FAMILY	cpu
COND	0
STACK	inc
ESIL	4,esp,-=,ebp,esp,=[4]
TYPE2	null
TYPE	upush
SIZE	1
REFPTR	0
BYTES	55
PREFIX	0
OPCODE	push ebp
ADDRESS	0x8048d60

Address	Instruction
0x8048e2c	call fcn.0804adb0
0x8048dee	call sym.imp.strcmp
0x8048e60	call sym.imp.__libc_start_mai
0x8048e3d	call fcn.08048f30

```
 > Loading file: /Users/hteso/Pocs/pocs/true
 > Analysis finished
 > Populating UI
[DEBUG]: Offset to search: 0x08048e44
[DEBUG]: Graph Offset: entry0
 > Adding binary information to notepad
 > Finished, happy reversing :)

 -- Use rarun2 to launch your programs with a predefined environment.

[DEBUG]: Offset to search: 0x08048d60
[DEBUG]: Graph Offset: 0x08048d60
[DEBUG]: Graph Offset: 0x08048d60
```

Name	Size	Address	End Address
.text	9756	0x08048d60	0x0804b37c
.shstrtab	237	0x00000000	0x0ed
.rodata	2464	0x0804b3a0	0x0804bd40
.rel.plt	312	0x08048974	0x08048aac
.rel.dyn	40	0x0804894c	0x08048974
.plt	640	0x08048ae0	0x08048d60
.note.gnu.build_id	36	0x08048188	0x080481ac
.note.ABI_tag	32	0x08048168	0x08048188
.jcr	4	0x0804def8	0x0804defc



Iaito - /Users/hteso/Pocs/true32

sub.fwrite_340

```
0x08049340      (fcn) sub.fwrite_340 185
0x08049340          sub esp, 0x2c                                   ; ','
0x08049343          mov dword [esp + 0x1c], ebx
0x08049347          mov ebx, dword [esp + 0x30]                     ; [0x30:4]=0x1b001c ; '0'
0x0804934b          mov dword [esp + 0x20], esi
0x0804934f          mov dword [esp + 0x24], edi
0x08049353          mov dword [esp + 0x28], ebp
0x08049357          test ebx, ebx
0x08049359          je 0x80493cf
0x0804935b          mov dword [esp + 4], 0x2f                       ; '/' ; [0x2f:4]=0x1b001c00 ; '/'
0x08049363          mov dword [esp], ebx
0x08049366          call sym.imp.strrchr
0x0804936b          test eax, eax
0x0804936d          je 0x80493af
0x0804936f          lea ebp, [eax + 1]                              ; 0x1
0x08049372          mov ecx, ebp
0x08049374          sub ecx, ebx
0x08049376          cmp ecx, 6
0x08049379          jle 0x80493af
0x0804937b          lea esi, [eax - 6]
0x0804937e          mov edi, str._.libs_                            ; "/.libs/" @ 0x804b70c
0x08049383          mov ecx, 7
0x08049388          repe cmpsb byte [esi], byte ptr es:[edi]        ; [0x170000001c:1]=255 ; 28
0x0804938a          jne 0x80493af
0x0804938c          mov ecx, 3
0x08049391          mov edi, 0x804b714
0x08049396          mov esi, ebp
0x08049398          mov ebx, ebp
0x0804939a          repe cmpsb byte [esi], byte ptr es:[edi]        ; [0x170000001c:1]=255 ; 28
0x0804939c          seta dl
0x0804939f          setb cl
0x080493a2          cmp dl, cl
0x080493a4          jne 0x80493af
0x080493a6          lea ebx, [eax + 4]                              ; 0x4
0x080493a9          mov dword obj.program_invocation_short_name, ebx  ; [0x804e0c0:4]=0x74727473 ; LEA obj.program_invocation_short_name ; "strtab" @ 0x804e0c0
0x080493af          mov dword [0x804e0f0], ebx                      ; [0x804e0f0:4]=0x756e672e
0x080493b5          mov esi, dword [esp + 0x20]                     ; [0x20:4]=0x51ac
0x080493b9          mov dword obj.program_invocation_name, ebx      ; [0x804e0c8:4]=0x65746e69 ; LEA obj.program_invocation_name ; "interp" @ 0x804e0c8
0x080493bf          mov edi, dword [esp + 0x24]                     ; [0x24:4]=0 ; '$'
0x080493c3          mov ebx, dword [esp + 0x1c]                     ; [0x1c:4]=52 ; "4"
0x080493c7          mov ebp, dword [esp + 0x28]                     ; [0x28:4]=0x200034 ; '(' ; "4 \x09(\x1c\x1b\x06"
0x080493cb          add esp, 0x2c                                   ; ','
0x080493ce          ret
0x080493cf          mov eax, dword obj.stderr                       ; [0x804e0c4:4]=0x2e006261 ; LEA obj.stderr ; "ab" @ 0x804e0c4
0x080493d4          mov dword [esp + 8], 0x37                       ; '7' ; [0x37:4]=0x3400 ; '7'
0x080493dc          mov dword [esp + 4], 1
0x080493e4          mov dword [esp], str.A_NULL_argv_0__was_passed_through_an_exec_system_call._n ; [0x804b6d4:4]=0x554e2041 ; LEA str.A_NULL_argv_0__was_passed_t
0x080493eb          mov dword [esp + 0xc], eax
0x080493ef          call sym.imp.fwrite
0x080493f4          call sym.imp.abort
0x080493f9          nop
0x080493fa      (fcn) fcn.080493fa 6
```

Function: .text:sub.fwrite_340

Information

Offset info:

FAMILY	cpu
STACK	inc
ESIL	44,esp,-=,$o,of,=,$s,sf,=,$z,zf
TYPE	sub
SIZE	3
REFPTR	0
VAL	0x0000002c
BYTES	83ec2c
ID	333
PREFIX	0
MNEMONIC	sub
OPCODE	sub esp, 0x2c

Xrefs from:

Address	Instruction
0x8048d84	call sub.fwrite_340
0x8049366	call sym.imp.strrchr
0x80493ef	call sym.imp.fwrite

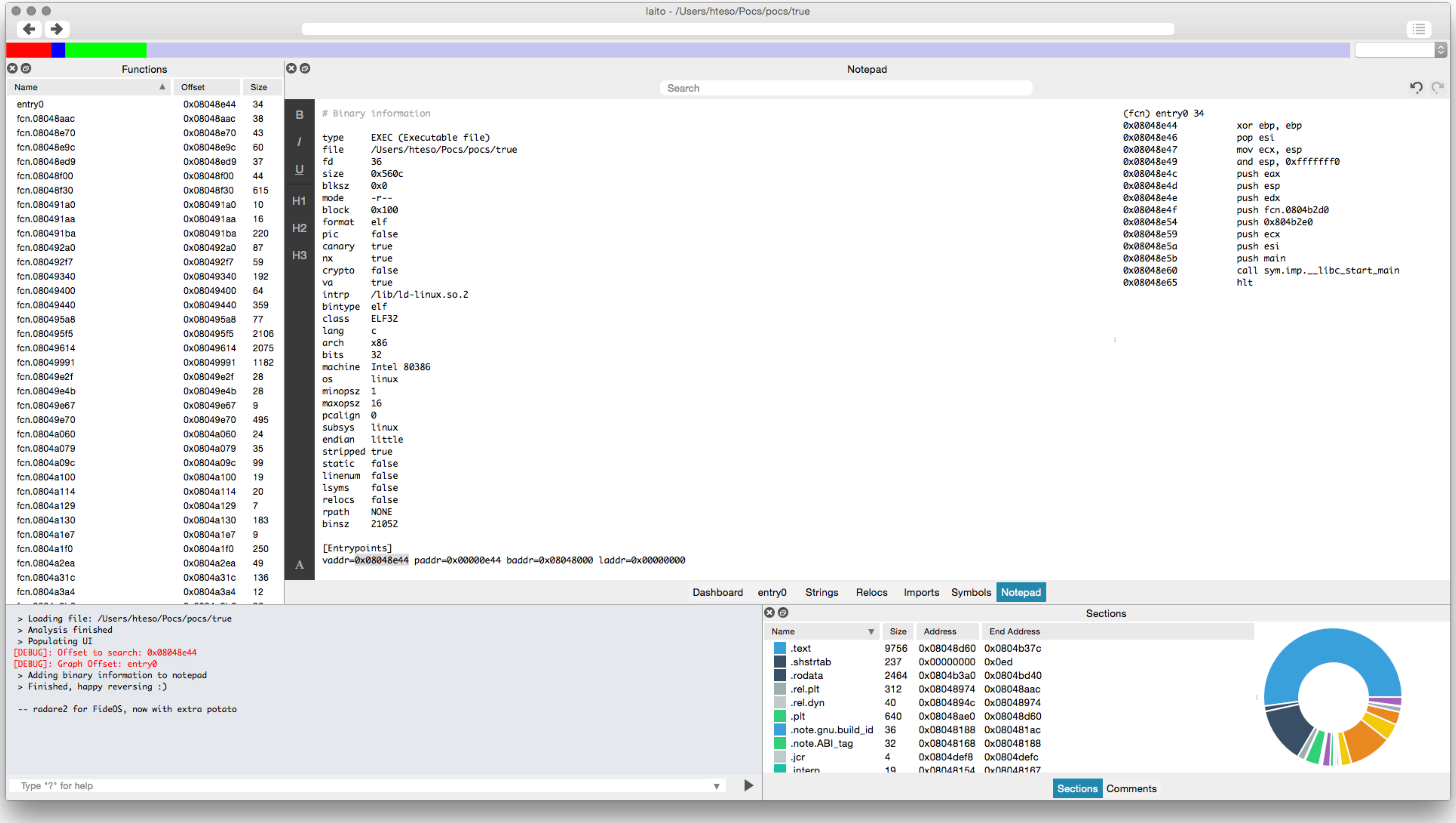
Xrefs To:

```
> Loading file: /Users/hteso/Pocs/true32
> Analysis finished
> Populating UI
> Adding binary information to notepad
> Finished, happy reversing :)

-- Sudo make me a pancake.
```

Type "?" for help

Sections

Name	Size	Address	End Address
.text	9756	0x08048d60	0x0804b37c
.shstrtab	237	0x00000000	0x0ed
.rodata	2464	0x0804b3a0	0x0804bd40
.rel.plt	312	0x08048974	0x08048aac
.rel.dyn	40	0x0804894c	0x08048974
.plt	640	0x08048ae0	0x08048d60
.note.gnu.build_id	36	0x08048188	0x080481ac
.note.ABI_tag	32	0x08048168	0x08048188
.jcr	4	0x0804def8	0x0804defc
.interp	19	0x08048154	0x08048167



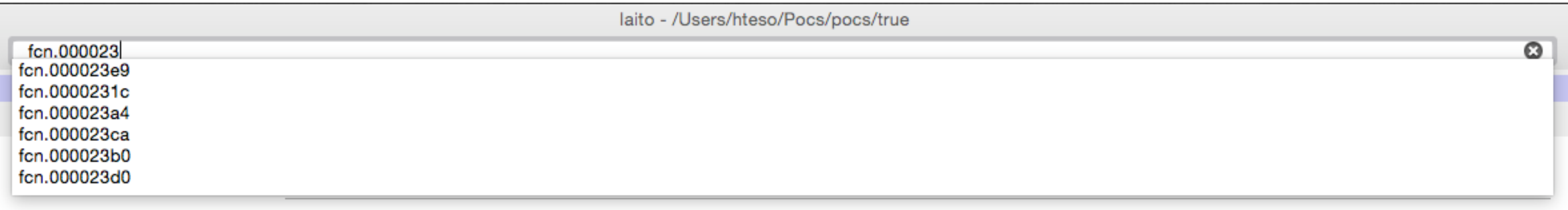
Name	Offset	Size
entry0	0x08048e44	34
fcn.08048aac	0x08048aac	38
fcn.08048e70	0x08048e70	43
fcn.08048e9c	0x08048e9c	60
fcn.08048ed9	0x08048ed9	37
fcn.08048f00	0x08048f00	44
fcn.08048f30	0x08048f30	615
fcn.080491a0	0x080491a0	10
fcn.080491aa	0x080491aa	16
fcn.080491ba	0x080491ba	220
fcn.080492a0	0x080492a0	87
fcn.080492f7	0x080492f7	59
fcn.08049340	0x08049340	192
fcn.08049400	0x08049400	64
fcn.08049440	0x08049440	359
fcn.080495a8	0x080495a8	77
fcn.080495f5	0x080495f5	2106
fcn.08049614	0x08049614	2075
fcn.08049991	0x08049991	1182
fcn.08049e2f	0x08049e2f	28
fcn.08049e4b	0x08049e4b	28
fcn.08049e67	0x08049e67	9
fcn.08049e70	0x08049e70	495
fcn.0804a060	0x0804a060	24
fcn.0804a079	0x0804a079	35
fcn.0804a09c	0x0804a09c	99
fcn.0804a100	0x0804a100	19
fcn.0804a114	0x0804a114	20
fcn.0804a129	0x0804a129	7
fcn.0804a130	0x0804a130	183
fcn.0804a1e7	0x0804a1e7	9
fcn.0804a1f0	0x0804a1f0	250
fcn.0804a2ea	0x0804a2ea	49
fcn.0804a31c	0x0804a31c	136
fcn.0804a3a4	0x0804a3a4	12

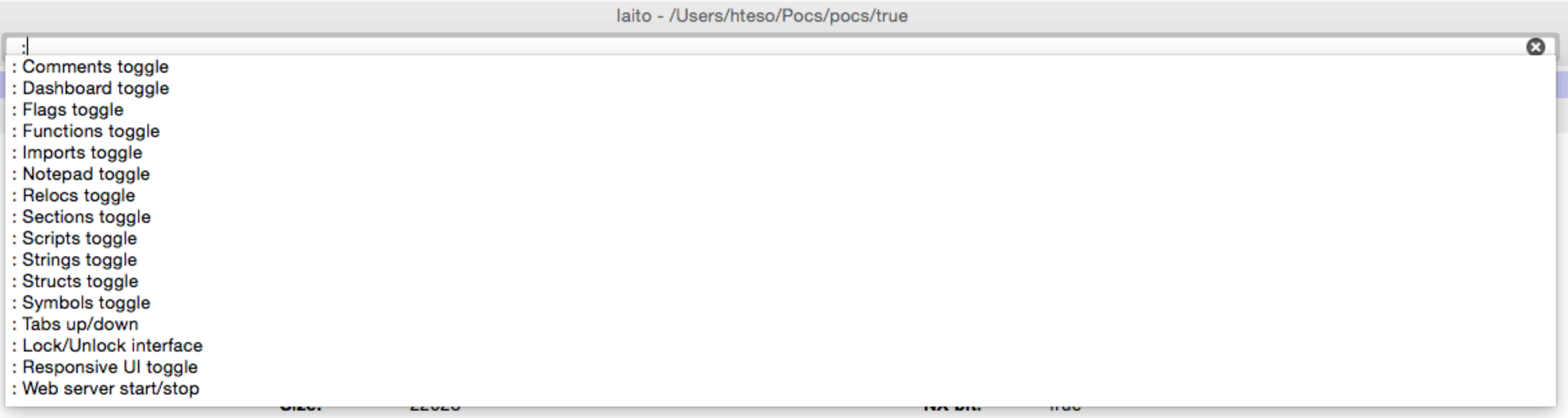
```
# Binary information

type     EXEC (Executable file)
file     /Users/hteso/Pocs/pocs/true
fd       36
size     0x560c
blksz    0x0
mode     -r--
block    0x100
format   elf
pic      false
canary   true
nx       true
crypto   false
va       true
intrp    /lib/ld-linux.so.2
bintype  elf
class    ELF32
lang     c
arch     x86
bits     32
machine  Intel 80386
os       linux
minopsz  1
maxopsz  16
pcalign  0
subsys   linux
endian   little
stripped true
static   false
linenum  false
lsyms    false
relocs   false
rpath    NONE
binsz    21052

[Entrypoints]
vaddr=0x08048e44 paddr=0x00000e44 baddr=0x08048000 laddr=0x00000000
```

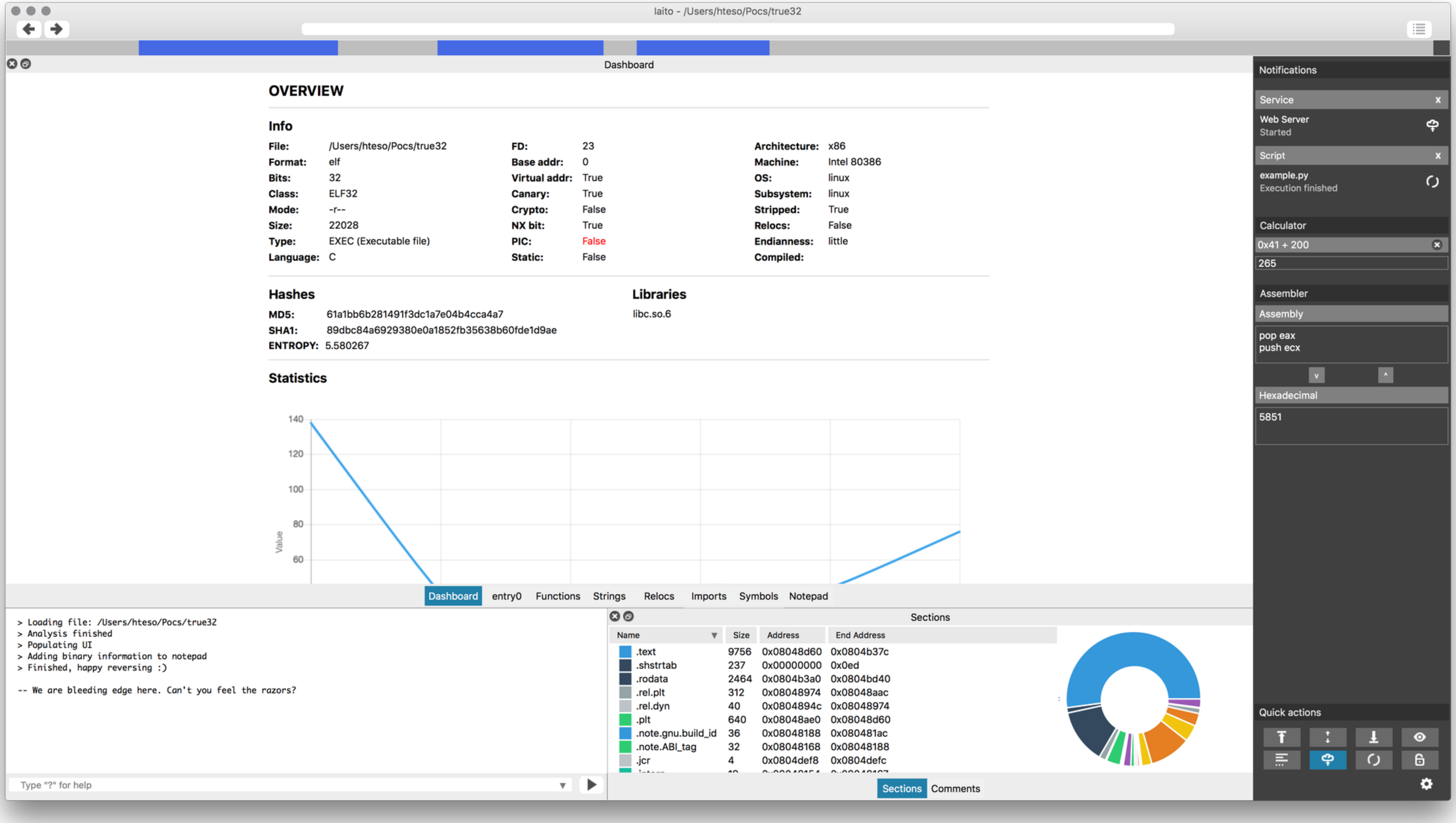
```
(fcn) entry0 34
0x08048e44          xor ebp, ebp
0x08048e46          pop esi
0x08048e47          mov ecx, esp
0x08048e49          and esp, 0xfffffff0
0x08048e4c          push eax
0x08048e4d          push esp
0x08048e4e          push edx
0x08048e4f          push fcn.0804b2d0
0x08048e54          push 0x804b2e0
0x08048e59          push ecx
0x08048e5a          push esi
0x08048e5b          push main
0x08048e60          call sym.imp.__libc_start_main
0x08048e65          hlt
```

```
 > Loading file: /Users/hteso/Pocs/pocs/true
 > Analysis finished
 > Populating UI
[DEBUG]: Offset to search: 0x08048e44
[DEBUG]: Graph Offset: entry0
 > Adding binary information to notepad
 > Finished, happy reversing :)

 -- radare2 for FideOS, now with extra potato
```

Name	Size	Address	End Address
.text	9756	0x08048d60	0x0804b37c
.shstrtab	237	0x00000000	0x0ed
.rodata	2464	0x0804b3a0	0x0804bd40
.rel.plt	312	0x08048974	0x08048aac
.rel.dyn	40	0x0804894c	0x08048974
.plt	640	0x08048ae0	0x08048d60
.note.gnu.build_id	36	0x08048188	0x080481ac
.note.ABI_tag	32	0x08048168	0x08048188
.jcr	4	0x0804def8	0x0804defc
.interp	19	0x08048154	0x08048167


Iaito - /Users/hteso/Pocs/pocs/true
fcn.000023
fcn.000023e9
fcn.0000231c
fcn.000023a4
fcn.000023ca
fcn.000023b0
fcn.000023d0


Iaito - /Users/hteso/Pocs/pocs/true
:
: Comments toggle
: Dashboard toggle
: Flags toggle
: Functions toggle
: Imports toggle
: Notepad toggle
: Relocs toggle
: Sections toggle
: Scripts toggle
: Strings toggle
: Structs toggle
: Symbols toggle
: Tabs up/down
: Lock/Unlock interface
: Responsive UI toggle
: Web server start/stop



OVERVIEW

Info

File:	/Users/hteso/Pocs/true32	**FD:**	23	**Architecture:**	x86
Format:	elf	**Base addr:**	0	**Machine:**	Intel 80386
Bits:	32	**Virtual addr:**	True	**OS:**	linux
Class:	ELF32	**Canary:**	True	**Subsystem:**	linux
Mode:	-r--	**Crypto:**	False	**Stripped:**	True
Size:	22028	**NX bit:**	True	**Relocs:**	False
Type:	EXEC (Executable file)	**PIC:**	False	**Endianness:**	little
Language:	C	**Static:**	False	**Compiled:**	

Hashes

MD5:	61a1bb6b281491f3dc1a7e04b4cca4a7
SHA1:	89dbc84a6929380e0a1852fb35638b60fde1d9ae
ENTROPY:	5.580267

Libraries

libc.so.6

Statistics

```
> Loading file: /Users/hteso/Pocs/true32
> Analysis finished
> Populating UI
> Adding binary information to notepad
> Finished, happy reversing :)

-- We are bleeding edge here. Can't you feel the razors?
```

Name	Size	Address	End Address
.text	9756	0x08048d60	0x0804b37c
.shstrtab	237	0x00000000	0x0ed
.rodata	2464	0x0804b3a0	0x0804bd40
.rel.plt	312	0x08048974	0x08048aac
.rel.dyn	40	0x0804894c	0x08048974
.plt	640	0x08048ae0	0x08048d60
.note.gnu.build_id	36	0x08048188	0x080481ac
.note.ABI_tag	32	0x08048168	0x08048188
.jcr	4	0x0804def8	0x0804defc

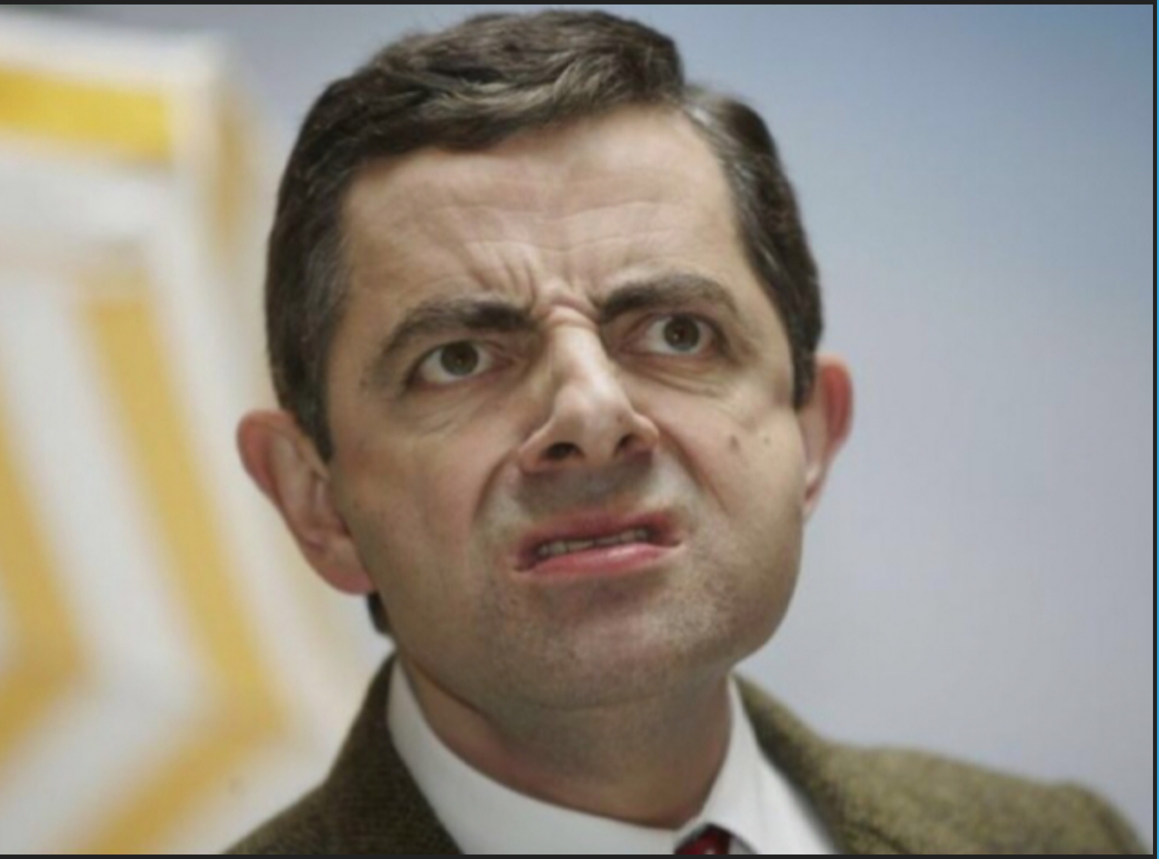
Web Server
Started

example.py
Execution finished

0x41 + 200
265

```
pop eax
push ecx
```

5851



I GET WEEKLY REQUESTS OF IAITÖ INSTALLERS

DO YOU SEE THE PROBLEM NOW?

Hugo Teso

DEVELOPERS != DESIGNERS AND THAT'S GOOD!

Hugo Teso

SO LONG, AND DANKE FOR ALL THE FISH!

Hugo Teso