Обзор инструментов IDA, Olly и все все все

Михаил Вяцков & Виктор Дворецкий

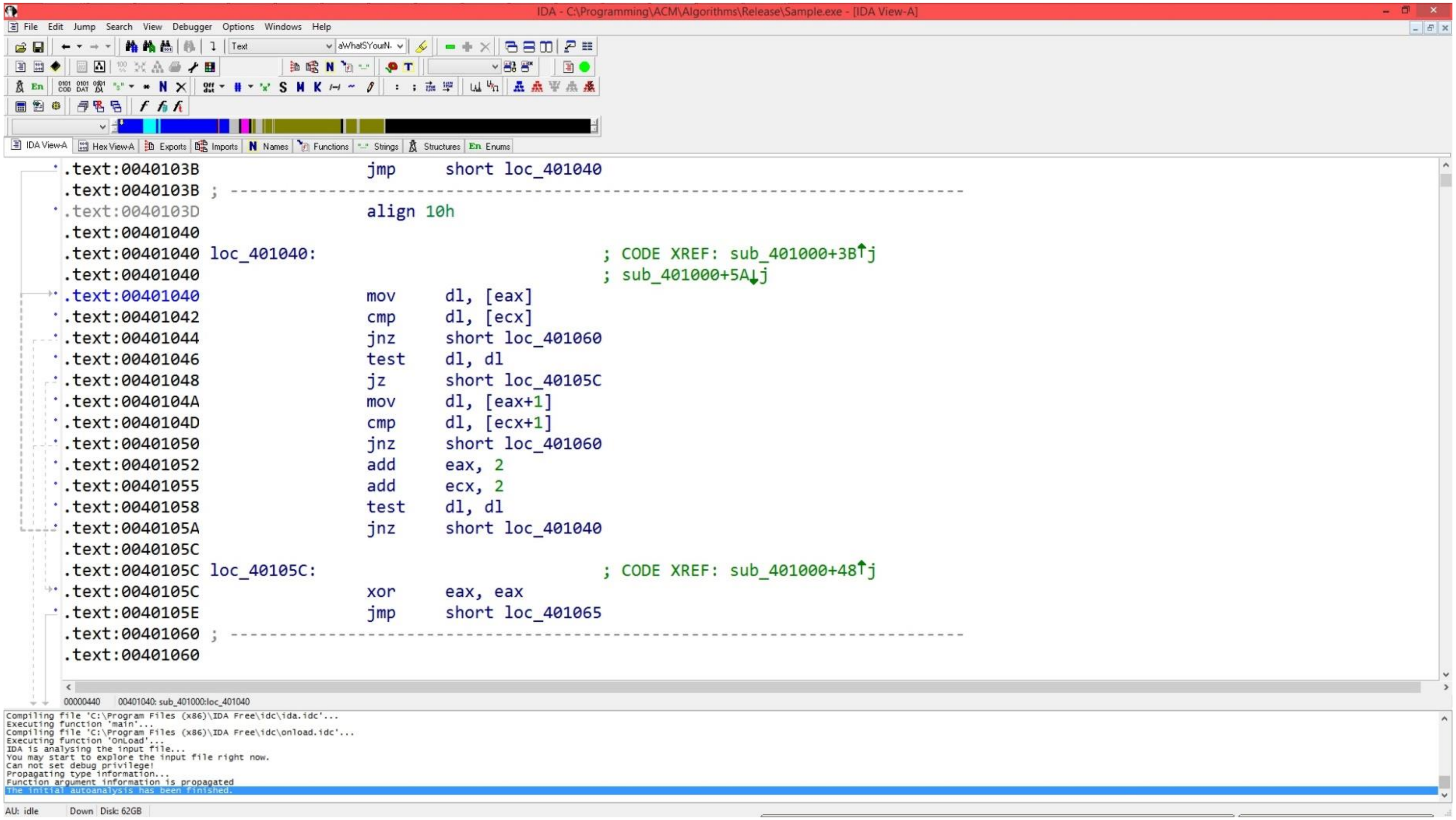
Tools

- Disassembler
- Debugger
- Decompiler
- MOAR

IDA

Interactive Disassembler

Code


IDA - C:\Programming\ACM\Algorithms\Release\Sample.exe - [IDA View-A]
File Edit Jump Search View Debugger Options Windows Help
Text
aWhatSYouN
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums

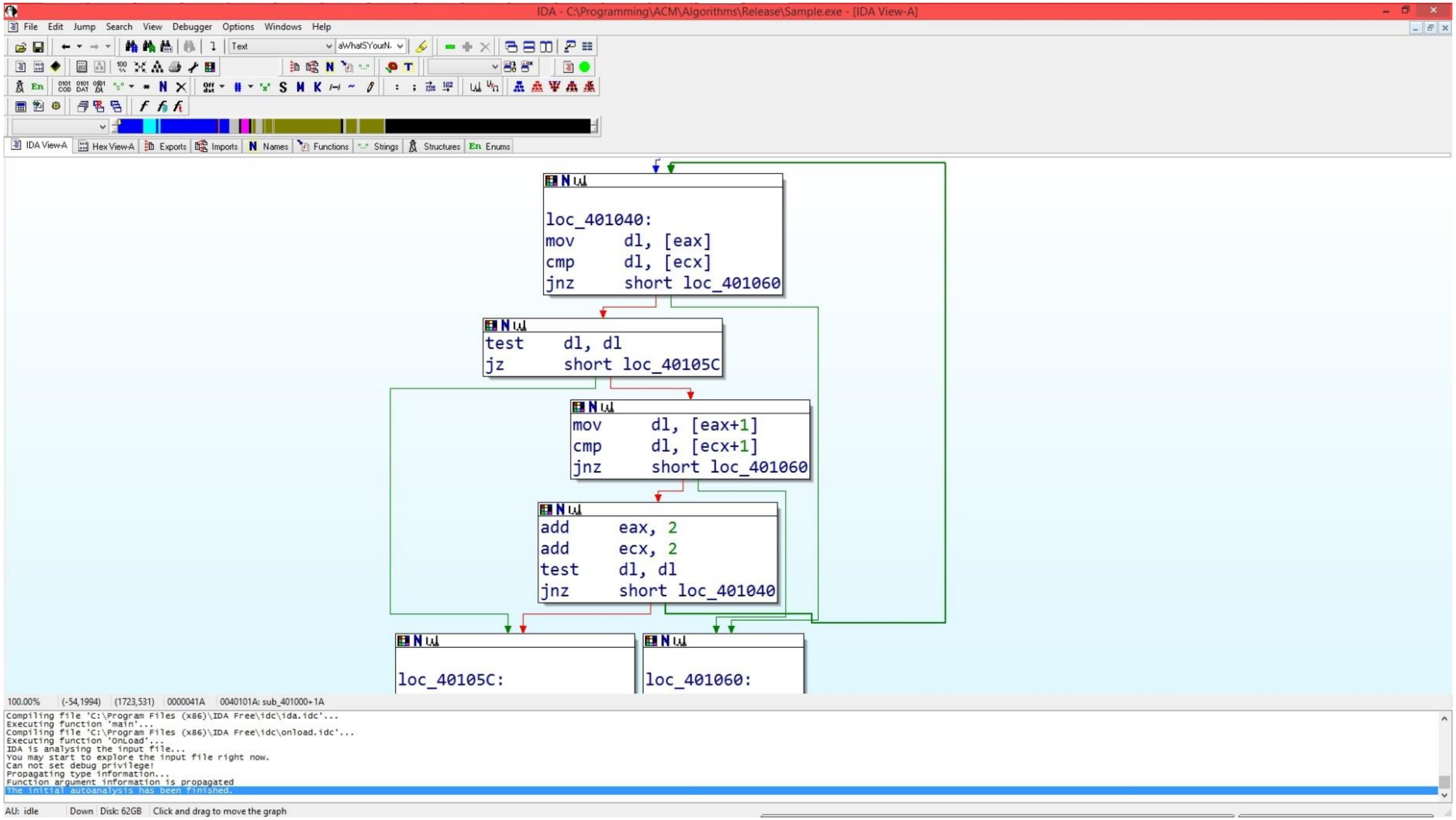
```
.text:0040103B                 jmp     short loc_401040
.text:0040103B ; ---------------------------------------------------------------------------
.text:0040103D                 align 10h
.text:00401040
.text:00401040 loc_401040:                             ; CODE XREF: sub_401000+3B↑j
.text:00401040                                         ; sub_401000+5A↓j
.text:00401040                 mov     dl, [eax]
.text:00401042                 cmp     dl, [ecx]
.text:00401044                 jnz     short loc_401060
.text:00401046                 test    dl, dl
.text:00401048                 jz      short loc_40105C
.text:0040104A                 mov     dl, [eax+1]
.text:0040104D                 cmp     dl, [ecx+1]
.text:00401050                 jnz     short loc_401060
.text:00401052                 add     eax, 2
.text:00401055                 add     ecx, 2
.text:00401058                 test    dl, dl
.text:0040105A                 jnz     short loc_401040
.text:0040105C
.text:0040105C loc_40105C:                             ; CODE XREF: sub_401000+48↑j
.text:0040105C                 xor     eax, eax
.text:0040105E                 jmp     short loc_401065
.text:00401060 ; ---------------------------------------------------------------------------
.text:00401060
```

00000440 00401040: sub_401000:loc_401040

```
Compiling file 'C:\Program Files (x86)\IDA Free\idc\ida.idc'...
Executing function 'main'...
Compiling file 'C:\Program Files (x86)\IDA Free\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Can not set debug privilege!
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
```

AU: idle Down Disk: 62GB

Graph



IDA - C:\Programming\ACM\Algorithms\Release\Sample.exe - [IDA View-A]
File Edit Jump Search View Debugger Options Windows Help
Text
aWhatSYourN
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums

```
loc_401040:
mov     dl, [eax]
cmp     dl, [ecx]
jnz     short loc_401060
```

```
test    dl, dl
jz      short loc_40105C
```

```
mov     dl, [eax+1]
cmp     dl, [ecx+1]
jnz     short loc_401060
```

```
add     eax, 2
add     ecx, 2
test    dl, dl
jnz     short loc_401040
```

```
loc_40105C:
```

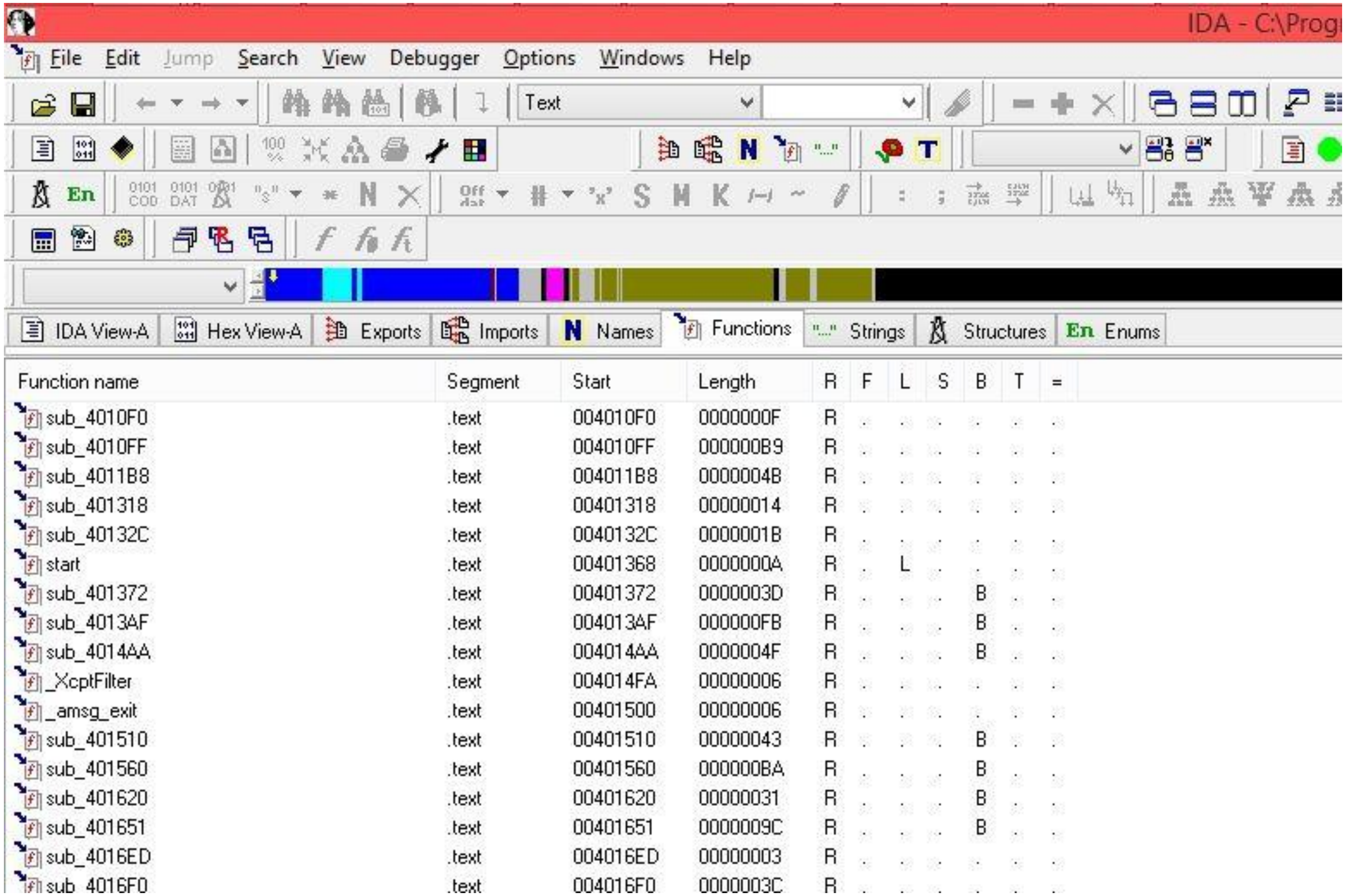
```
loc_401060:
```

```
100.00%   (-54,1994)   (1723,531)   0000041A   0040101A: sub_401000+1A
```

```
Compiling file 'C:\Program Files (x86)\IDA Free\idc\ida.idc'...
Executing function 'main'...
Compiling file 'C:\Program Files (x86)\IDA Free\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Can not set debug privilege!
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
```

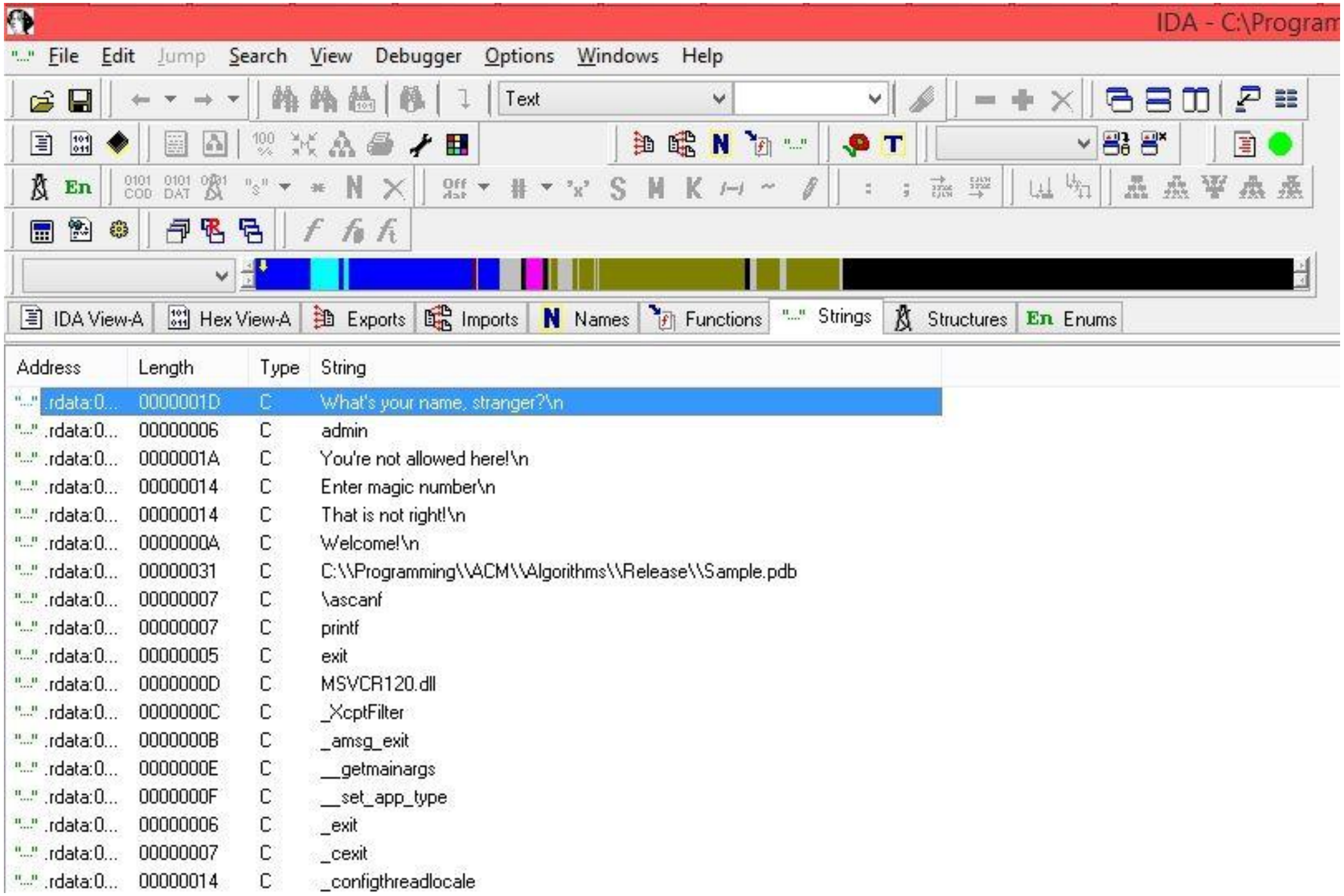
```
AU: idle   Down   Disk: 62GB   Click and drag to move the graph
```

Functions



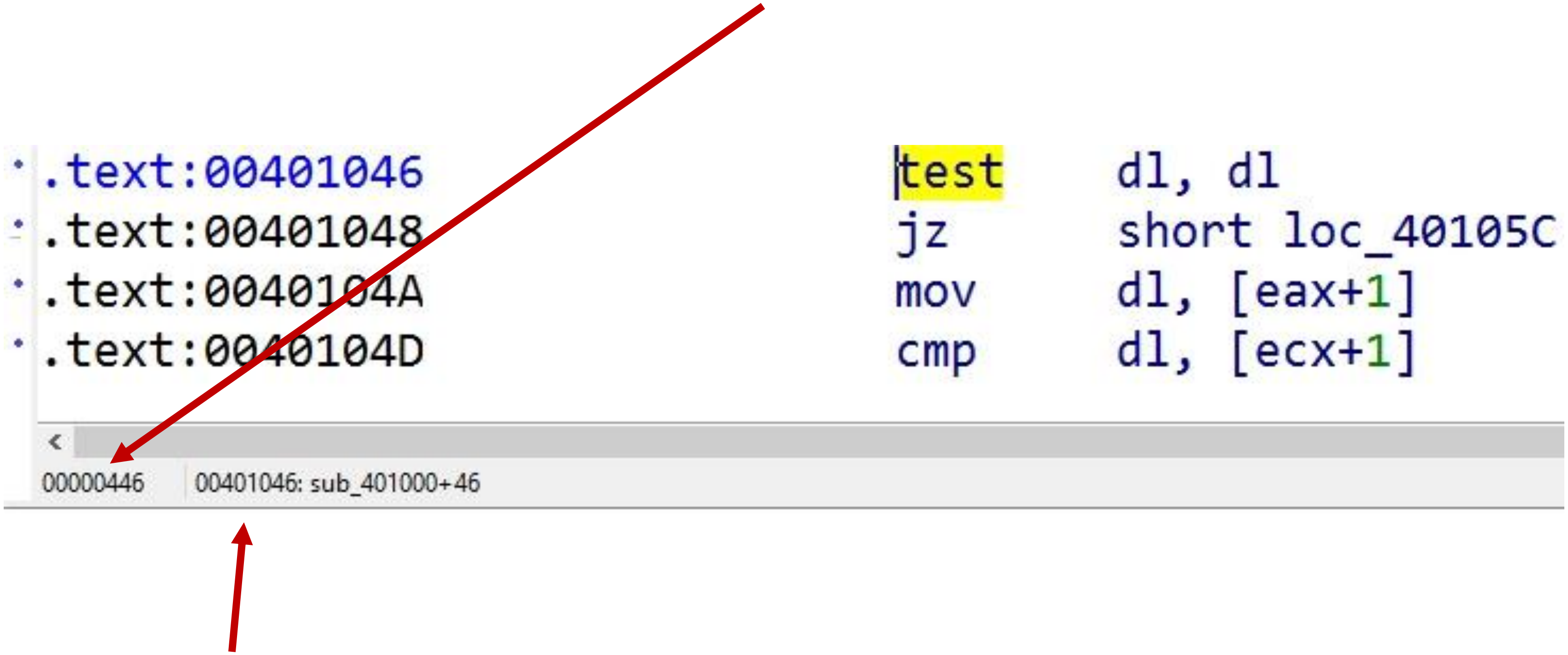
Function name	Segment	Start	Length	R	F	L	S	B	T	=
sub_4010F0	.text	004010F0	0000000F	R	.	.	.	.	.	.
sub_4010FF	.text	004010FF	000000B9	R	.	.	.	.	.	.
sub_4011B8	.text	004011B8	0000004B	R	.	.	.	.	.	.
sub_401318	.text	00401318	00000014	R	.	.	.	.	.	.
sub_40132C	.text	0040132C	0000001B	R	.	.	.	.	.	.
start	.text	00401368	0000000A	R	.	L	.	.	.	.
sub_401372	.text	00401372	0000003D	R	.	.	.	B	.	.
sub_4013AF	.text	004013AF	000000FB	R	.	.	.	B	.	.
sub_4014AA	.text	004014AA	0000004F	R	.	.	.	B	.	.
_XcptFilter	.text	004014FA	00000006	R	.	.	.	.	.	.
_amsg_exit	.text	00401500	00000006	R	.	.	.	.	.	.
sub_401510	.text	00401510	00000043	R	.	.	.	B	.	.
sub_401560	.text	00401560	000000BA	R	.	.	.	B	.	.
sub_401620	.text	00401620	00000031	R	.	.	.	B	.	.
sub_401651	.text	00401651	0000009C	R	.	.	.	B	.	.
sub_4016ED	.text	004016ED	00000003	R	.	.	.	.	.	.
sub_4016F0	.text	004016F0	0000003C	R	.	.	.	.	.	.

Strings



Address	Length	Type	String
.rdata:0...	0000001D	C	What's your name, stranger?\n
.rdata:0...	00000006	C	admin
.rdata:0...	0000001A	C	You're not allowed here!\n
.rdata:0...	00000014	C	Enter magic number\n
.rdata:0...	00000014	C	That is not right!\n
.rdata:0...	0000000A	C	Welcome!\n
.rdata:0...	00000031	C	C:\\Programming\\ACM\\Algorithms\\Release\\Sample.pdb
.rdata:0...	00000007	C	\ascanf
.rdata:0...	00000007	C	printf
.rdata:0...	00000005	C	exit
.rdata:0...	0000000D	C	MSVCR120.dll
.rdata:0...	0000000C	C	_XcptFilter
.rdata:0...	0000000B	C	_amsg_exit
.rdata:0...	0000000E	C	__getmainargs
.rdata:0...	0000000F	C	__set_app_type
.rdata:0...	00000006	C	_exit
.rdata:0...	00000007	C	_cexit
.rdata:0...	00000014	C	_configthreadlocale

Addresses



```
.text:00401046                 test    dl, dl
.text:00401048                 jz      short loc_40105C
.text:0040104A                 mov     dl, [eax+1]
.text:0040104D                 cmp     dl, [ecx+1]
```

```
00000446    00401046: sub_401000+46
```

File offset

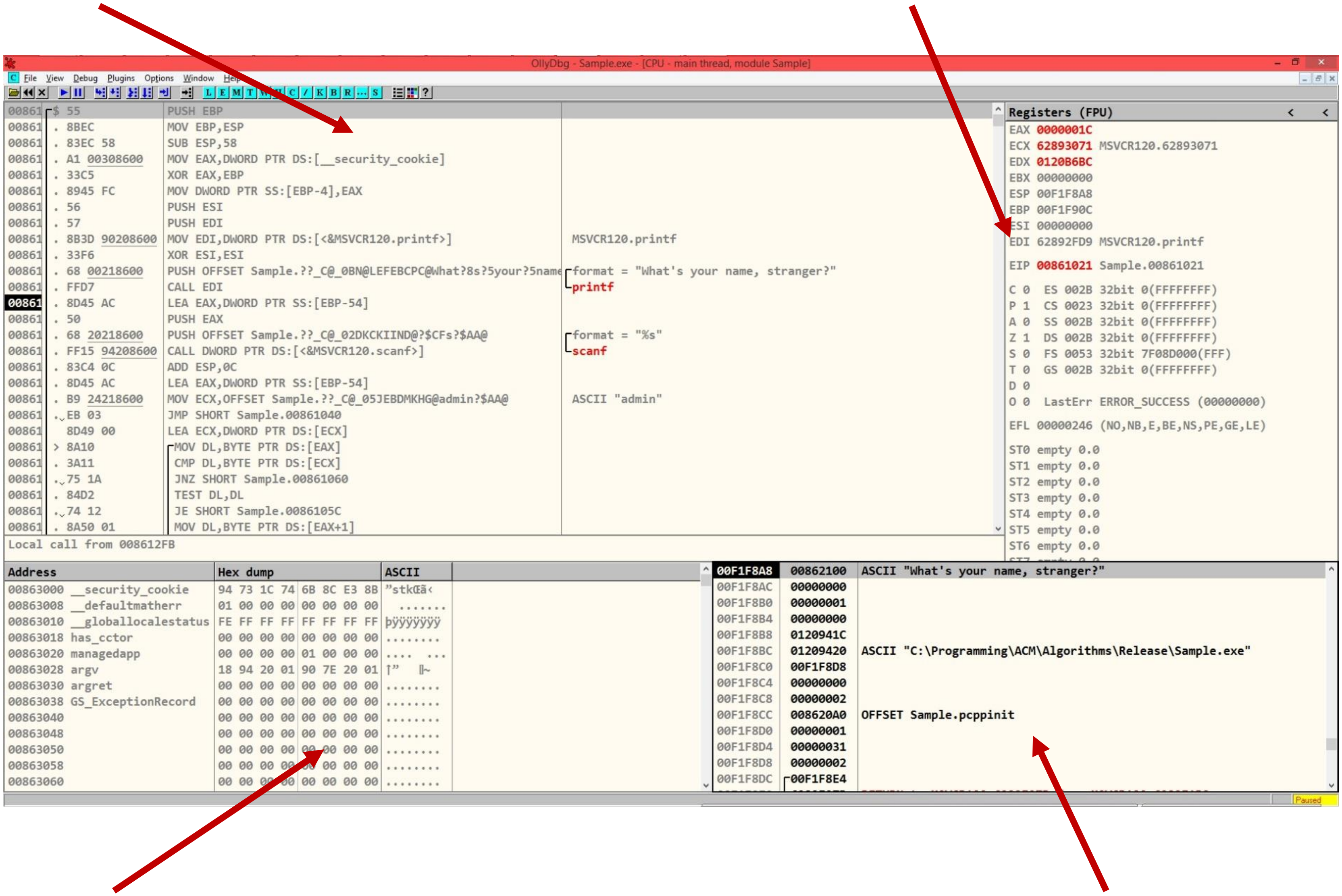
Memory offset

OllyDbg

Windows debugger

Instructions

Registers


OllyDbg - Sample.exe - [CPU - main thread, module Sample]
C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S
Paused

```
00861 ┌$ 55             PUSH EBP
00861 │. 8BEC           MOV EBP,ESP
00861 │. 83EC 58        SUB ESP,58
00861 │. A1 00308600    MOV EAX,DWORD PTR DS:[__security_cookie]
00861 │. 33C5           XOR EAX,EBP
00861 │. 8945 FC        MOV DWORD PTR SS:[EBP-4],EAX
00861 │. 56             PUSH ESI
00861 │. 57             PUSH EDI
00861 │. 8B3D 90208600  MOV EDI,DWORD PTR DS:[<&MSVCR120.printf>]          MSVCR120.printf
00861 │. 33F6           XOR ESI,ESI
00861 │. 68 00218600    PUSH OFFSET Sample.??_C@_0BN@LEFEBCPC@What?8s?5your?5name ┌format = "What's your name, stranger?"
00861 │. FFD7           CALL EDI                                             └printf
00861 │. 8D45 AC        LEA EAX,DWORD PTR SS:[EBP-54]
00861 │. 50             PUSH EAX
00861 │. 68 20218600    PUSH OFFSET Sample.??_C@_02DKCKIIND@?$CFs?$AA@      ┌format = "%s"
00861 │. FF15 94208600  CALL DWORD PTR DS:[<&MSVCR120.scanf>]               └scanf
00861 │. 83C4 0C        ADD ESP,0C
00861 │. 8D45 AC        LEA EAX,DWORD PTR SS:[EBP-54]
00861 │. B9 24218600    MOV ECX,OFFSET Sample.??_C@_05JEBDMKHG@admin?$AA@   ASCII "admin"
00861 │.⌄EB 03          JMP SHORT Sample.00861040
00861 │  8D49 00        LEA ECX,DWORD PTR DS:[ECX]
00861 │> 8A10           ┌MOV DL,BYTE PTR DS:[EAX]
00861 │. 3A11           │CMP DL,BYTE PTR DS:[ECX]
00861 │.⌄75 1A          │JNZ SHORT Sample.00861060
00861 │. 84D2           │TEST DL,DL
00861 │.⌄74 12          │JE SHORT Sample.0086105C
00861 │. 8A50 01        │MOV DL,BYTE PTR DS:[EAX+1]
Local call from 008612FB
```

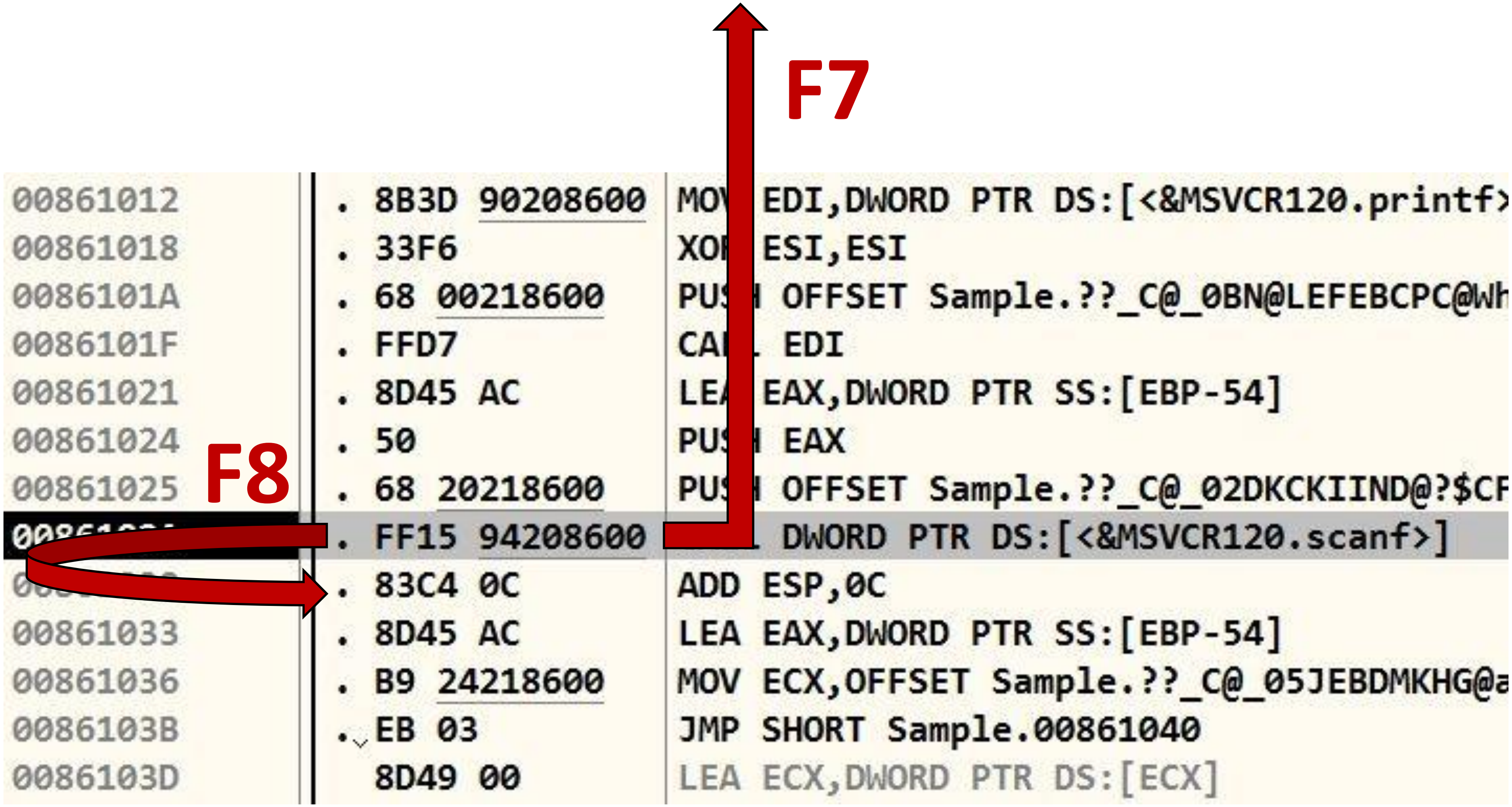
```
Registers (FPU)
EAX 0000001C
ECX 62893071 MSVCR120.62893071
EDX 0120B6BC
EBX 00000000
ESP 00F1F8A8
EBP 00F1F90C
ESI 00000000
EDI 62892FD9 MSVCR120.printf

EIP 00861021 Sample.00861021

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 7F08D000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
```

```
Address                     Hex dump                  ASCII
00863000 __security_cookie  94 73 1C 74 6B 8C E3 8B   ”stkŒã‹
00863008 __defaultmatherr   01 00 00 00 00 00 00 00    .......
00863010 __globallocalestatus FE FF FF FF FF FF FF FF þÿÿÿÿÿÿÿ
00863018 has_cctor          00 00 00 00 00 00 00 00   ........
00863020 managedapp         00 00 00 00 01 00 00 00   ....  ...
00863028 argv               18 94 20 01 90 7E 20 01   ↑”    ~
00863030 argret             00 00 00 00 00 00 00 00   ........
00863038 GS_ExceptionRecord 00 00 00 00 00 00 00 00   ........
00863040                    00 00 00 00 00 00 00 00   ........
00863048                    00 00 00 00 00 00 00 00   ........
00863050                    00 00 00 00 00 00 00 00   ........
00863058                    00 00 00 00 00 00 00 00   ........
00863060                    00 00 00 00 00 00 00 00   ........
```

```
00F1F8A8  00862100  ASCII "What's your name, stranger?"
00F1F8AC  00000000
00F1F8B0  00000001
00F1F8B4  00000000
00F1F8B8  0120941C
00F1F8BC  01209420  ASCII "C:\Programming\ACM\Algorithms\Release\Sample.exe"
00F1F8C0  00F1F8D8
00F1F8C4  00000000
00F1F8C8  00000002
00F1F8CC  008620A0  OFFSET Sample.pcppinit
00F1F8D0  00000001
00F1F8D4  00000031
00F1F8D8  00000002
00F1F8DC ┌00F1F8E4
```

Heap

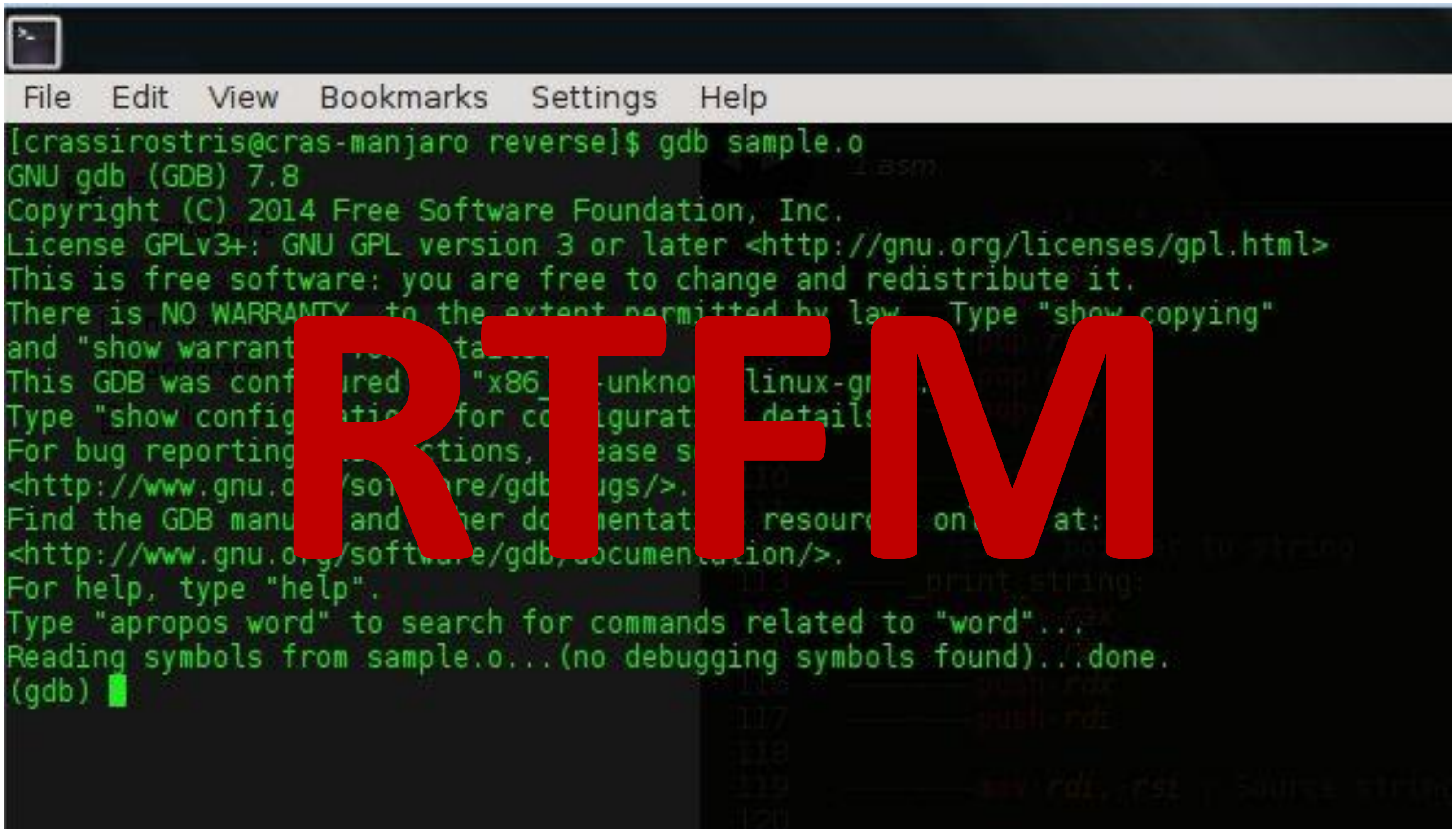
Stack



```
00861012    . 8B3D 90208600  MOV EDI,DWORD PTR DS:[<&MSVCR120.printf>
00861018    . 33F6           XOR ESI,ESI
0086101A    . 68 00218600    PUSH OFFSET Sample.??_C@_0BN@LEFEBCPC@Wh
0086101F    . FFD7           CALL EDI
00861021    . 8D45 AC        LEA EAX,DWORD PTR SS:[EBP-54]
00861024    . 50             PUSH EAX
00861025    . 68 20218600    PUSH OFFSET Sample.??_C@_02DKCKIIND@?$CF
0086102A    . FF15 94208600  CALL DWORD PTR DS:[<&MSVCR120.scanf>]
00861030    . 83C4 0C        ADD ESP,0C
00861033    . 8D45 AC        LEA EAX,DWORD PTR SS:[EBP-54]
00861036    . B9 24218600    MOV ECX,OFFSET Sample.??_C@_05JEBDMKHG@a
0086103B    .⌄ EB 03         JMP SHORT Sample.00861040
0086103D      8D49 00        LEA ECX,DWORD PTR DS:[ECX]
```

GDB

GNU Debugger



```
[crassirostris@cras-manjaro reverse]$ gdb sample.o
GNU gdb (GDB) 7.8
Copyright (C) 2014 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warrant     ta
This GDB was conf  ured   "x86_  -unkno  linux-gn  .
Type "show config  atio  for co  igurat  details
For bug reporting    ctions,   ease s
<http://www.gnu.o  /so  re/gdb  ugs/>.
Find the GDB manu  and   her do  mentat  resourc  on   at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from sample.o...(no debugging symbols found)...done.
(gdb)
```

RTFM