



# Cutter

Free and Open Source RE Platform  
powered by **radare2**

# WHO ARE WE?

## Itay Cohen

aka **Megabeets**  
**Malware Researcher**  
Check Point Research



@megabeets\_

## Antide Petit

aka **xarkes**  
Student at **Ensimag**  
**GreHack** conference  
organizer



@xarkes\_

## Florian Märkl

aka **thestr4ng3r**  
Student at the **Technical University of Munich**  
Recently released “**Chiaki**”  
(made possible by Cutter)



@thestr4ng3r

# AGENDA

## 01 BACKGROUND

What is Cutter & a brief history

## 02 FEATURES

What can Cutter do?

## 03 NEW ADDITIONS

What we have done during the last year? + surprise

## 04 FUTURE PLANS

What are we planning to do next?

# Cutter

Free, Open Source and Cross-Platform RE  
framework powered by **radare2**.

Cutter was designed for non-radare2 users  
and ones that prefer a flexible GUI for their workflow.



Type flag name or address here

## Functions

Name	Siz
entry.init0	15
entry0	4
fcn.00002000	2
fcn.00002130	4
fcn.00002200	8E
fcn.00002630	1E
fcn.000026e0	2E
fcn.000027f0	487
fcn.0000344e	364
fcn.000034e1	465
fcn.0000355c	454
fcn.000035ce	454
fcn.00003b00	695
fcn.00004240	15
fcn.00004470	10E
fcn.00004950	22
fcn.00004ac0	E
fcn.00004b20	24
fcn.00004cd0	4
fcn.00004d20	5
fcn.00004d60	12
fcn.00004dff	10C
fcn.00004e60	5
fcn.00004ec0	E
<b>fcn.00004f00</b>	11
fcn.00004f90	E
fcn.00004fe0	E
fcn.000050c0	1
... ...	...

## Quick Filter



Dashboard

Strings

Imports

Search Disassembly Hexdump

## Disassembly

```
(fcn) fcn.00004f00 128
    fcn.00004f00 (int32_t arg1);
    ; arg int32_t arg1 @ rdi
    push r12
    0x000004f00  push rbp
    0x000004f03  push rbx
    0x000004f04  mov rbx rdi
    0x000004f07  call qword [reloc.fileno]
    0x000004f0d  mov rdi rbx
    0x000004f10  test eax, eax
    0x000004f12  js 0x4f71
    0x000004f14  call qword [reloc.__freading]
    0x000004f1a  test eax, eax
    0x000004f1c  jne 0x4f50
    0x000004f1e  mov rdi rbx
    0x000004f21  call fcn.00004f90
    0x000004f27  test eax, eax
    0x000004f29  je 0x4f6e
    0x000004f2b  call qword [reloc.__errno_location]
    0x000004f31  mov rdi rbx
    0x000004f34  mov r12d, dword [rax]
    0x000004f37  mov rbp rax
    0x000004f3a  call qword [reloc.fclose]
    0x000004f3d  test r12d, r12d
    0x000004f43  jne 0x4f80
    0x000004f45  pop rbx
    0x000004f46  pop rbp
    0x000004f47  pop r12
    0x000004f49  ret
    0x000004f4a  nop word [rax + rax]
    0x000004f50  mov rdi rbx
    0x000004f53  call qword [reloc.fileno]
    0x000004f59  xor esi, esi
    0x000004f5b  mov edx 1
    0x000004f60  mov edi eax
    0x000004f62  call qword [reloc.lseek]
    0x000004f68  cmp rax, 0xffffffffffff
    0x000004f6c  jne 0x4f1e
    0x000004f6e  mov rdi rbx
    0x000004f71  pop rbp
    0x000004f72  pop r12
    0x000004f73  pop r12
    0x000004f75  jmp qword [reloc.fclose]
    0x000004f7b  nop dword [rax + rax]
    0x000004f80  mov dword [rbp], r12d
    0x000004f84  mov eax, 0xffffffff
    0x000004f88  imm 0x4fad5
    0x000004f89  imm 0x4fad5

```

## Graph (fcn.00004f00)



## Graph Overview

## Console

-- Beer in mind.

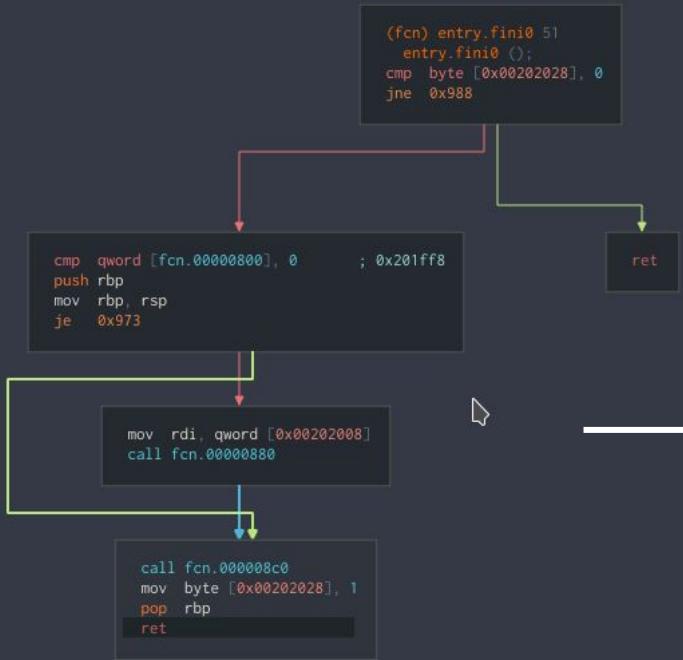
```
[0x00004f1c]>.px 32
- offset - 0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0x00004f1c 79 32 48 89 07 e8 69 00 00 00 85 c0 74 43 ff u2R..g.i....tc...
0x00004f2c 15 7f 3f 00 00 48 89 df 44 8b 20 48 89 c5 ff 15 0a 3f 00 00
0x00004f3c 45 85 e4 75 3b 20 5d 41 5c 66 0f 1f 44 00 00 E..u2A..f..D...
0x00004f50 48 89 df ff 15 0f 48 00 00 31 f6 ba 01 00 00 00 H.....0..1....
0x00004f60 89 c7 ff 15 b8 3f 00 00 48 83 f8 ff 75 b0 48 89 ...7..H..uH...
```

Type "?" for help

## Hexdump

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
41	54	55	53	48	89	fb	ff	15	5b	40	00	00	48	89	df	ATUSH...[0..H..
c0	78	5d	ff	00	15	6e	40	00	00	85	c0	75	32	48	89	1..x]..@...u2H..
0f	67	e8	69	00	00	00	85	c0	74	43	ff	15	7f	3f	00	..g.i....tc...?..
00	48	89	df	44	8b	20	48	89	c5	ff	15	0a	3f	00	00	H.....0..1....
0x000004f1c	45	85	e4	75	3b	20	5d	41	5c	66	0f	1f	44	00	00	E..u2A..f..D...
0x000004f3c	48	89	df	ff	15	0f	48	00	00	31	f6	ba	01	00	00	H.....0..1....
0x000004f60	89	c7	ff	15	b8	3f	00	00	48	83	f8	ff	75	b0	48	89

- Cutter is **cross platform!**   
- Developed in **C++** with the **Qt** Library
- Cooked on top of **radare2** (uses the r2 libraries)
- Uses the API and commands from radare2
- More than **160,000** Downloads



## A FULLY INTERACTIVE GRAPH FOR EASY NAVIGATION

Quickly inspect function's flow,  
rename functions and variables, apply  
types and add comments

```
(fcn) sym.beet 112
    sym.beet (char *src);
; var char *s2 @ ebp-0x92
; var int32_t var_8eh @ ebp-0x8e
; var int32_t var_8ah @ ebp-0x8a
; var char *dest @ ebp-0x88
; arg char *src @ ebp+0x8
0x08048585    push ebp
0x08048586    mov ebp, esp
0x08048588    sub esp, 0x98
0x0804858e    sub esp, 8
0x08048591    push dword [src] ; const char *src
0x08048594    lea eax, [dest]
0x0804859a    push eax ; char *dest
0x0804859b    call sym.imp.strcpy ; char *strcpy(char *dest, const char *src)
0x080485a0    add esp, 0x10
0x080485a3    mov dword [s2], 0x6167654d ; 'Mega'
0x080485ad    mov dword [var_8eh], 0x74656562 ; 'beet'
0x080485b7    mov word [var_8ah], 0x73 ; 's' ; 115
0x080485c0    sub esp, 0xc
0x080485c3    lea eax, [s2]
0x080485c9    push eax
0x080485ca    call sym.rot13
0x080485cf    add esp, 0x10
0x080485d2    sub esp, 8
0x080485d5    lea eax, [s2]
0x080485db    push eax ; const char *s2
0x080485dc    lea eax, [dest]
0x080485e2    push eax ; const char *s1
0x080485e3    call sym.impstrcmp ; int strcmp(const char *s1, const char *s2)
0x080485e8    add esp, 0x10
0x080485eb    test eax, eax
0x080485ed    sete al
0x080485f0    movzx eax, al
0x080485f3    leave
0x080485f4    ret
(fcn) main 127
int main (int argc, char **argv, char **envp);
; var int32_t var_8h @ ebp-0x8
; arg int32_t arg_4h @ esp+0x4
0x080485f5    lea ecx, [arg_4h]
0x080485f9    and esp, 0xffffffff
0x080485fc    push dword [ecx - 4]
0x080485ff    push ebp
0x08048600    mov ebp, esp
0x08048602    push ebx
0x08048603    push ecx
0x08048604    mov ebx, ecx
0x08048606    sub esp, 0xc
0x08048609    push str:::_Megabeets_:: ; 0x8048700 ; "\n :: Megabeets ::"
0x0804860a    add esp, 0x10
```

## AN INTERACTIVE LINEAR DISASSEMBLY VIEW

Inspect and interact with the program in linear disassembly view.

0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF

Address	Value	Byte View	Hex View	ASCII View
0080483d0	a0 04 08 ff d0 83 c4 10 c9 f3 c3 90 8d 74 26 00	.....t&.		
0080483e0	b4 24 a0 04 08 2d 24 a0 04 08 c1 f8 02 89 c1	.\$...-\$.....t.		
0080483f0	ea 1f 01 d0 d1 f8 74 1b ba 00 00 00 00 85 d2 74	.t.....t.		
008048400	12 55 89 e5 83 ec 10 50 68 24 a0 04 ff d2 83	.U.....Ph\$.		
008048410	c4 18 c9 f3 c3 8d 74 26 00 8d bc 27 00 00 00	....&.		
008048420	80 3d 24 a0 04 08 00 75 13 55 89 e5 83 ec 08 e8	=\$...u.U.....		
008048430	7c ff ff fc c5 05 24 a0 04 08 01 c9 f3.c3 66 98	....\$. ....f.		
008048440	b8 18 9f 04 08 8b 18 85 d2 75 05 eb 93 8d 76 00	....u...V.		
008048450	ba 00 00 00 00 85 d2 74 f2 55 89 e5 83 ec 14 50	....t.U..P.		
008048460	ff d2 83 c4 10 c9 e9 75 ff ff f5 89 e5 83 ec	....u..U.		
008048470	18 83 7d 08 00 84 07 01 00 00 07 45 fc 00 00	.).....E.		
008048480	00 00 e9 e6 00 00 00 8b 55 fc 8b 45 08 01 d0 0f	....U.E.		
008048490	b6 00 3c 60 7e 2c 8b 55 fc 8b 45 08 01 d0 0f b6	..<~..U.E.		
0080484a0	00 3c 6d 7f 1d 8b 55 fc 8b 45 08 01 d0 8b 4d fc	.<m...[U]E..M.		
0080484b0	80 55 08 01 ca 0f b6 12 83 c2 0d 88 10 e9 a7 00	U.....		
0080484c0	00 00 8b 55 fc 8b 45 08 01 d0 0f b6 00 3c 40 7e	...U..E....<0>		
0080484d0	29 8b 55 fc 8b 45 08 01 d0 0f b6 00 3c 4d 7f 1a	).U..E....<M..		
0080484e0	8b 55 fc 8b 45 08 01 d0 8b 4d fc 8b 55 08 01 ca	U..E....M.U.		
0080484f0	0f b6 12 83 c2 0d 88 10 eb 6f 8b 55 fc 8b 45 08	....,0.U.E.		
008048500	01 d0 0f b6 00 3c 6d 7e 29 8b 55 fc 8b 45 08 01	....<m>.U.E.		
008048510	d0 0f b6 00 3c 7a 7f 1a 8b 55 fc 8b 45 08 01 d0	...<z...U.E.		
008048520	8b 4d fc 8b 55 08 01 ca 0f b6 12 83 ea 0d 88 10	M..U.		
008048530	37 8b 55 fc 8b 45 08 01 d0 0f b6 00 3c 4d 7f	...U..E....<N>		
008048540	28 8b 55 fc 8b 45 08 01 d0 0f b6 00 3c 5a 7f 19	(.U..E....<Z..		
008048550	8b 55 fc 8b 45 08 01 d0 8b 4d fc 8b 55 08 01 ca	U..E....M.U.		
008048560	0f b6 12 83 ea 0d 88 10 90 83 45 fc 01 8b 55 fc	....E..U.		
008048570	8b 45 08 01 d0 0f b6 00 84 c0 0f 85 07 ff ff ff	E.....		
008048580	eb 01 00 c9 c3 55 89 e5 81 ec 98 00 00 00 83 ec	.....U.		
008048590	ff 75 08 8d 85 78 ff ff ff 50 e8 90 fd ff ff	..u...x...P..		
0080485a0	83 c4 10 c7 85 6e ff ff 4d 65 67 61 c7 85 72	....n..Mega..r		
0080485b0	ff ff ff 62 65 65 74 66 c7 85 76 ff ff ff 73 00	...beetf..v..s.		
0080485c0	83 ec 9c 8d 85 6e ff ff ff 50 e8 9c fe ff ff 83	....n..P..		
0080485d0	c4 10 83 ec 08 8d 85 6e ff ff ff 50 8d 85 78 ff	....n..P..x.		
0080485e0	ff ff 50 e8 38 ff ff 83 c4 10 85 c0 0f 94 c0	.P..8.....		
0080485f0	0f b6 c0 c9 c3 8d 4c 24 04 83 e4 f0 ff 71 fc 55	....L\$....q.U		
008048600	89 e5 53 51 89 cb 83 ec 0c 68 00 87 04 08 e8 2d	..SQ...h..-		
008048610	fd ff ff 83 c4 10 83 ec 0c 68 15 87 04 08 e8 1d	....h.....		
008048620	fd ff ff 83 c4 10 83 3b 01 7e 2a 8b 43 04 83 c0	....;.^*..C..		
008048630	84 80 00 83 ec 0c 50 e8 49 ff ff 83 c4 10 85	....P.I.....		
008048640	c4 74 12 83 ec 0c 68 2c 87 04 08 e8 f0 fc ff ff	t...h.....		
008048650	83 c4 10 eb 10 83 ec 0c 68 36 87 04 08 e8 de fc	.....h6.....		
008048660	ff ff 83 c4 10 b8 00 00 00 00 8d 65 f8 59 5b 5d	....e.Y[]		
008048670	8d 61 fc f3 66 90 66 90 66 90 66 90 66 90 66 90	,a,f,f,f,f,f,f,		
008048680	55 57 56 53 e8 17 fd ff ff 81 c3 77 19 00 00 83	UVWS.....w...		
008048690	ec 0c 8b 6c 24 20 8d b3 0c ff ff e8 4b fc ff	..ls.....K..		
0080486a0	ff 8d 83 08 ff ff 29 c5 c1 fe 02 85 f6 74 25	.....)....,%		
0080486b0	31 ff 8d b6 00 00 00 00 83 ec 04 ff 74 24 2c ff	I.....t\$..		
0080486c0	74 24 2c 55 ff 94 bb 08 ff ff ff 83 c7 01 83 c4	t\$,U..		
0080486d0	10 39 75 e3 83 c4 0c 5b 5e 5f 5d c3 8d 76 00	.9.u...[~_.]..v.		
0080486e0	f3 c3 00 00 53 83 ec 08 e8 b3 fc ff ff 81 c3 13	....S.....		
0080486f0	19 00 00 83 c4 08 5b c3 03 00 00 00 01 00 02 00	....L.....		
008048700	0e 20 20 2e 3a 2a 20 4d 65 61 62 65 65 74 73	...,: Megabeets		
008048710	20 3a 3a 2e 00 54 68 69 6e 6b 20 79 6f 75 20 63	...,: Think you c		
008048720	61 6e 20 6d 61 6b 65 20 69 74 3f 00 53 75 63 63	an make it?.Succ		
008048730	65 73 21 0a 00 4e 6f 70 2c 20 57 72 6f 66 67	ess!.Nop, Wrong		
008048740	29 61 72 67 75 6d 65 6e 74 2e 00 00 01 1b 03 3b	argument .....		

Parsing Information

Python Endian Lit

Select bytes to display information

# AN INTERACTIVE HEXDUMP TO INSPECT DATA

---

Easily **export selected bytes** to your favorite programming language. Including unique features such as entropy and hashin.



## EMBEDDED RADARE2 CONSOLE WITH ALL THE COMMANDS

Run your favorite radare2 commands from inside Cutter. Use features that are not available in the GUI yet.



X-Refs for 0x0000cd0

X-Refs to 0x0000cd0:

Address	Code
0x00004666	call fcn.0000cd0
0x000045fb	call fcn.0000cd0
0x00004548	call fcn.0000cd0
0x000044fb	call fcn.0000cd0
0x000044b5	call fcn.0000cd0
0x00004431	call fcn.0000cd0
0x000043ed	call fcn.0000cd0

X-Refs from 0x0000cd0:

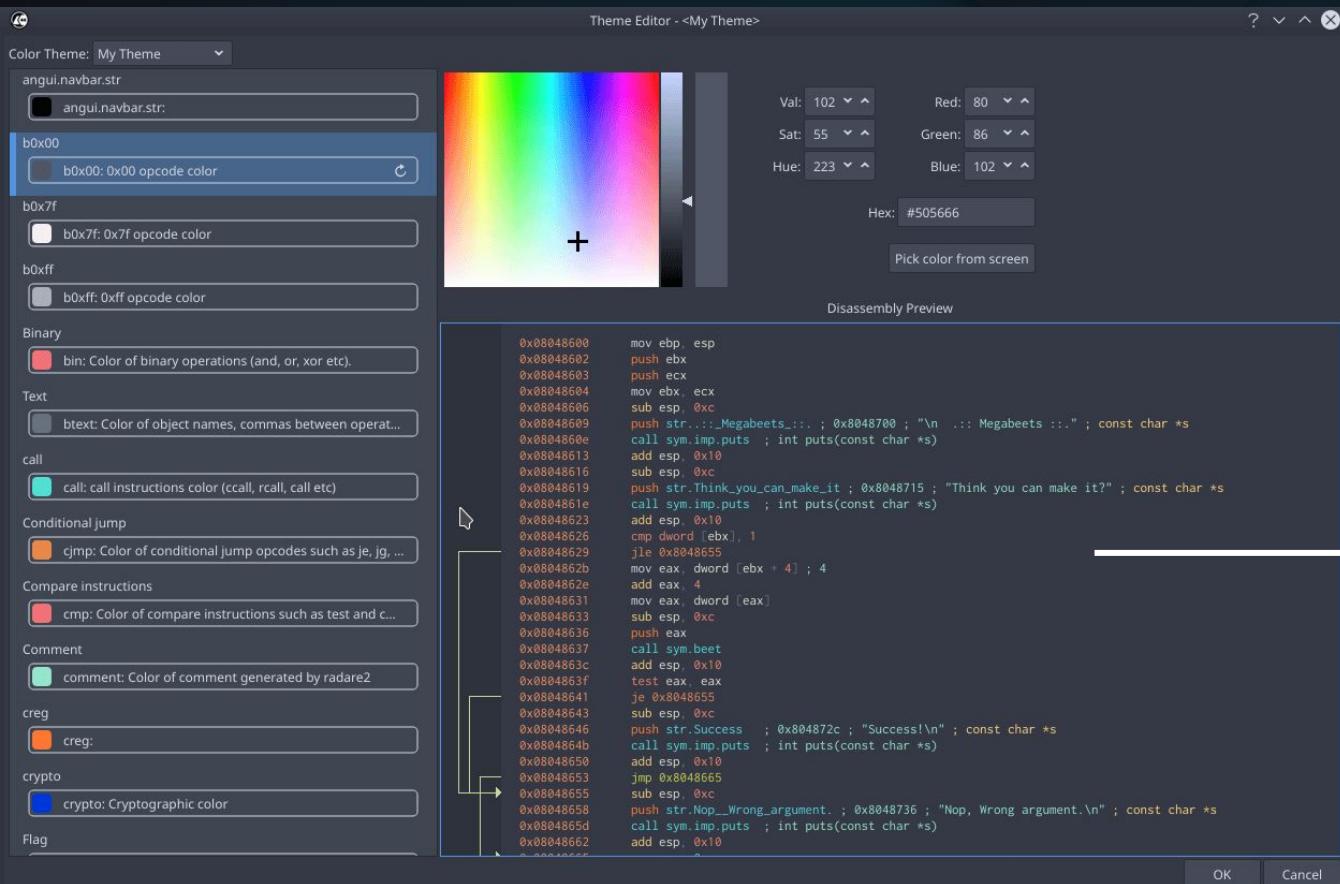
Address	Code	Type
0x000044be	jle 0x4535	
0x000044c0	add dword [rax], eax	
0x000044c2	xor edi, edi	
0x000044c4	mov esi, dword [rdx + rax*4]	
0x000044c7	call fcn.00014270	
0x000044cd	jmp loc.000042c8 ; fcn.00004260+0x68	
0x000044d2	lea rdx, [0x000219a0]	
0x000044d9	mov r9, qword [0x000221f0]	
0x000044e0	mov r8d, 4	
0x000044e6	lea rcx, [0x000177f0]	
0x000044ed	mov rsi, qword [obj.optarg] ; 0x22298	
0x000044f4	lea rdi, str.indicator_style ; 0x18b27 ; "--indi	
0x000044fb	call fcn.0000cd0	
0x00004501	lea rdx, [0x000177f0]	
0x00004502	lea edx, [0x000177f0]	
0x00004508	mov eax, dword [rdx + rax*4]	
0x0000450b	mov dword [0x00023314], eax	
0x00004511	jmp loc.000042c8 ; fcn.00004260+0x68	

Close

## X-REFS DIALOG WITH INSTANT PREVIEW

So you would not need to jump back and forth to find the interesting references.

# UNIQUE THEME EDITOR TO EASILY CUSTOMIZE CUTTER



# IN THE PAST YEAR

## PLUGINS

Python & Native C++  
Plugins

## GRAPH OVERVIEW

## HEXDUMP REFACTORING

## THEME EDITOR

Build your own  
themes for Cutter

## TRANSLATIONS

The community  
translated Cutter to  
many languages

## STABILITY++

We fixed dozens of  
bugs and improved  
Cutter's stability

# **DEMO**

Cutter Basic Usage



CodeBrowser: megabeets\_0x1

File Edit Analysis Navigation Search Select Tools Window Help

Functions - 24 items Listing: megabeets\_0x1 megabeets\_0x1

Label	Fun...	Sy...
_init	35	IMP...
FUN_08048310	12	DE...
strcmp	6	DE...
strcpy	6	DE...
puts	6	DE...
_libc_start_main	6	DE...
_gmon_start	6	DE...
_start	34	IMP...
_x86.get_pc_th...	4	IMP...
deregister_tm_cl...	43	IMP...
register_tm_clones	53	IMP...
_do_global_dtors...	30	IMP...
frame_dummy	40	IMP...
rotl3	282	IMP...
beet	112	IMP...
main	127	IMP...
_libc_csu_init	93	IMP...
_libc_csu_fini	2	IMP...
_fini	20	IMP...
strcmp	1	DE...
strcpy	1	DE...
puts	1	DE...
_gmon_start	1	IMP...
_libc_start_main	1	DE...

```

080485e8 83 c4 10    AUW    ESP,UX10
080485eb 83 c0        TEST   EAX,EAX
080485ed 0f 94 c0    SETZ   AL
080485f0 0f b6 c0    MOVZX  EAX,AL
080485f3 c9          LEAVE
080485f4 c3          RET
*****
*           FUNCTION
* 
undefined main(undefined4 param_1, undefined4 param_2)
{
    int iVar1;

    puts("n :: Megabeets ::");
    puts("Think you can make it?");
    if ((1 < param_1) && (iVar1 = beet(*(&param_2 + 4)), iVar1 != 0)) {
        puts("Success!\n");
        return 0;
    }
    puts("Nop. Wrong argument.\n");
    return 0;
}

```

Function Graph - main - 5 vertices (megabeets\_0x1)

080485f5 8d 4c 24 04 LEA ECX=>param\_1,[ESP + 0x4]
080485f9 83 e4 f0 AND ESP,0xfffffff0
080485fc ff 71 fc PUSH dword ptr [ECX + local\_res0]
080485ff 55 PUSH EB
08048600 89 e5 MOV EB,ESP
08048602 53 PUSH EBX
08048603 51 PUSH ECX
08048604 89 cb MOV EBX,ECX
08048606 83 ec 0c SUB ESP,0xc
08048609 68 00 87 PUSH s\_::Megabeets:::\_08048700 = "n :: Megabeets ::"
0804860e 04 08 ADD ESP,0x10
0804860e e8 2d fd CALL puts
08048613 83 c4 10 ADD ESP,0x10
08048616 83 ec 0c SUB ESP,0xc
08048619 68 15 87 PUSH s\_Think\_you\_can\_make\_it?\_08048715 = "Think you can make it?"
0804861e e8 1d fd CALL puts
08048623 83 c4 10 ADD ESP,0x10
08048626 83 3b 01 CMP dword ptr [EBX]=>param\_1,0x1
08048629 7e 2a JLE LAB\_08048655
0804862b 8b 43 04 MOV EAX,dword ptr [EBX + param\_2]
0804862e 83 c0 04 ADD EAX,0x4
08048631 8b 00 MOV EAX,dword ptr [EAX]
08048633 83 ec 0c SUB ESP,0xc
08048636 50 PUSH EAX
08048637 e8 49 ff CALL beet
0804863c ff ff ADD ESP,0x10
0804863f 85 c0 TEST EAX,EAX
08048641 74 12 JZ LAB\_08048655
08048643 83 ec 0c SUB ESP,0xc
08048646 68 2c 87 PUSH s\_Success!\_0804872c = "Success!"
08048646 f4 00 00 ADD ESP,0x10

080485f5 8d 4c 24 04 LEA ECX,[ESP + 0x4]

080485f9 83 e4 f0 AND ESP,0xfffffff0

080485fc ff 71 fc PUSH dword ptr [ECX + local\_res0]

080485ff 55 PUSH EB

08048600 89 e5 MOV EB,ESP

08048602 53 PUSH EBX

08048603 51 PUSH ECX

08048604 89 cb MOV EBX,ECX

08048606 83 ec 0c SUB ESP,0xc

08048609 68 00 87 PUSH s\_::Megabeets:::\_08048700 = "n :: Megabeets ::"

0804860e 04 08 ADD ESP,0x10

0804860e e8 2d fd CALL puts

08048613 83 c4 10 ADD ESP,0x10

08048616 83 ec 0c SUB ESP,0xc

08048619 68 15 87 PUSH s\_Think\_you\_can\_make\_it?\_08048715 = "Think you can make it?"

0804861e e8 1d fd CALL puts

08048623 83 c4 10 ADD ESP,0x10

08048626 83 3b 01 CMP dword ptr [EBX]=>param\_1,0x1

08048629 7e 2a JLE LAB\_08048655

0804862b 8b 43 04 MOV EAX,dword ptr [EBX + param\_2]

0804862e 83 c0 04 ADD EAX,0x4

08048631 8b 00 MOV EAX,dword ptr [EAX]

08048633 83 ec 0c SUB ESP,0xc

08048636 50 PUSH EAX

08048637 e8 49 ff CALL beet

0804863c ff ff ADD ESP,0x10

0804863f 85 c0 TEST EAX,EAX

08048641 74 12 JZ LAB\_08048655

08048643 83 ec 0c SUB ESP,0xc

08048646 68 2c 87 PUSH s\_Success!\_0804872c = "Success!"

08048646 f4 00 00 ADD ESP,0x10





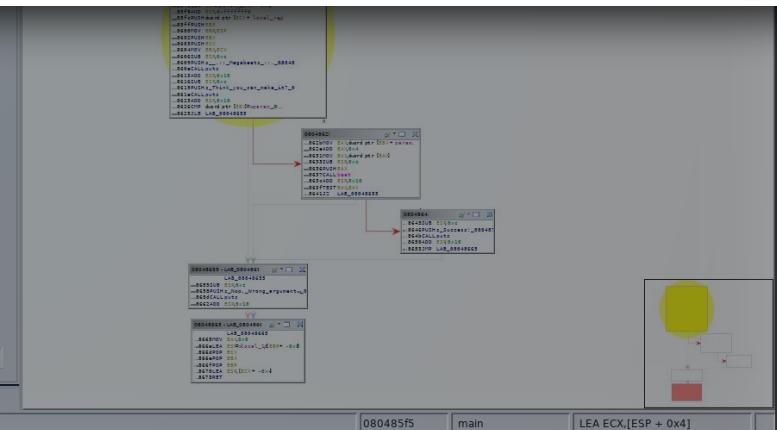
The screenshot shows the CodeBrowser interface with two main panes. The left pane, titled "Functions - 24 it...", lists various symbols and their details. The right pane, titled "Listing: megabeets\_0x1", displays the assembly code for the function. A vertical dashed line connects the two panes.

Label	Fun...	Sy...
_init	35	IMP...
FUN_00848310	12	DE...
strcmp	6	DE...
strcpy	6	DE...
puts	6	DE...
__libc_start_main	6	DE...
_gmon_start_	6	DE...
_start	34	IMP...
_x86.get_pc_th...	4	IMP...
deregister_tm_cl...	43	IMP...
register_tm_clones	53	IMP...
_do_global_dtors_	30	IMP...
frame_dummy	40	IMP...
rotl3	282	IMP...
beet	112	IMP...
main	127	IMP...
__libc_csu_init	93	IMP...
__libc_csu_fini	2	IMP...
_fini	20	IMP...
strcmp	1	DE...
strcpy	1	DE...
puts	1	DE...
_gmon_start_	1	IMP...
__libc_start_main	1	DE...

Listing: megabeets\_0x1

Address	OpCode	OpName	Description
00048529	83 c4 10	LEA	
00048528	83 e0 f0	AND	
000485ed	0f 94 c0	SETZ	
000485f0	0f b6 c0	MOVZX	
000485f3	c9	LEAVE	
000485f4	c3	RET	
*****			
000485f5	8d 4c 24 04	LEA	
000485f9	83 e4 00	ADD	
000485fc	ff 71 fc	PUSH	
000485ff	55	PUSH	
00048600	89 e5	MOV	
00048602	53	PUSH	
00048603	51	PUSH	
00048604	89 cb	MOV	
00048606	83 ec 0c	SUB	
00048609	68 00 87	PUSH	
04 08			
0004860e	e8 2d fd ff ff	CALL	
00048613	83 c4 10	ADD	
00048616	83 ec 0c	SUB	
00048619	68 15 87	PUSH	
04 00			
0004861e	e8 1d fd ff ff	CALL	
00048623	83 c4 10	ADD	
00048626	83 30 01	CMP	
00048629	7e 2a	JLE	
0004862b	8b 43 04	MOV	
0004862e	83 c0 04	ADD	
00048631	8b 00	MOV	
00048633	83 ec 0c	SUB	
00048636	50	PUSH	
00048637	e8 49 ff ff ff	CALL	
0004863c	83 c4 10	ADD	
0004863f	85 c0	TEST	
00048641	74 12	JZ	
00048643	83 ec 0c	SUB	
00048646	68 2c 87	PUSH	
04 08			

```
2 undefined4 main(int param_1,int param_2)
3
4 {
5     int iVar1;
6
7     puts("\n    :: Megabeets :::");
8     puts("Think you can make it?");
9     if ((1 < param_1) && (iVar1 = beet(*(
0         puts("Success!\n");
1         return 0;
2     }
3     puts("Nop, Wrong argument.\n");
4     return 0;
5 }
```



[Code](#)[Issues 310](#)[Pull requests 50](#)[Projects 0](#)[Wiki](#)[Security](#)[Insights](#)Branch: [master](#) [▼](#)[ghidra](#) / [Ghidra](#) / [Features](#) / [Decompiler](#) / [src](#) / [decompile](#) / [cpp](#) /[Create new file](#) [Upload files](#) [Find file](#) [History](#) [caheckman](#) fix for result based sign-bit extraction in optimized division

Latest commit 29221c1 25 days ago

..

	<a href="#">.gitignore</a>	Candidate release of source code.	5 months ago
	<a href="#">Doxyfile</a>	Candidate release of source code.	5 months ago
	<a href="#">Makefile</a>	Candidate release of source code.	5 months ago
	<a href="#">action.cc</a>	Candidate release of source code.	5 months ago
	<a href="#">action.hh</a>	Candidate release of source code.	5 months ago
	<a href="#">address.cc</a>	Refactor ParamEntry look-up allowing "contained by" discovery	last month
	<a href="#">address.hh</a>	Refactor ParamEntry look-up allowing "contained by" discovery	last month
	<a href="#">architecture.cc</a>	bumping decompiler minor version number	2 months ago
	<a href="#">architecture.hh</a>	Suggestions from github issue #382	4 months ago
	<a href="#">bfd_arch.cc</a>	Candidate release of source code.	5 months ago
	<a href="#">bfd_arch.hh</a>	Candidate release of source code.	5 months ago
	<a href="#">block.cc</a>	reads and constraint adjustments	2 months ago
	<a href="#">block.hh</a>	reads and constraint adjustments	2 months ago
	<a href="#">blockaction.cc</a>	Fix for switches in infinite loop decompiler bug	3 months ago
	<a href="#">blockaction.hh</a>	Candidate release of source code.	5 months ago
	<a href="#">callgraph.cc</a>	Candidate release of source code.	5 months ago
	<a href="#">callgraph.hh</a>	Candidate release of source code.	5 months ago
	<a href="#">capability.cc</a>	Candidate release of source code.	5 months ago
	<a href="#">capability.hh</a>	Candidate release of source code.	5 months ago
	<a href="#">cast.cc</a>	Candidate release of source code.	5 months ago

<xml>Decompile Function X</xml>



decompile

<xml>What is at 0x1337?</xml>

<xml>printf</xml>

<xml>void X() { /\* ... \*/ }</xml>



# R2Ghidra Decompiler

# DEMO

Ghidra Decompiler

**ETAWEN?  
NOW!**

[radareorg / r2ghidra-dec](#)

Unwatch 8 Star 0 Fork 0

Code Issues 7 Pull requests 0 Actions Projects 0 Wiki Security Insights Settings

Deep ghidra decompiler integration for radare2

Manage topics

101 commits 3 branches 0 releases 5 contributors LGPL-3.0

Branch: master New pull request Create new file Upload files Find File Clone or download

thestr4ng3r More README

Latest commit e971a6e 4 minutes ago

assets	Add Logo	12 days ago
cmake	More Windows Fixes	2 days ago
cutter-plugin	More Windows Fixes	2 days ago
ghidra	More Windows Fixes	2 days ago
src	Disable symbol name mangling (#25)	yesterday
third-party	Basic XML Output Parsing	9 days ago
.gitignore	Initial Commit	2 months ago
.gitmodules	Basic XML Output Parsing	9 days ago
.travis.yml	Fix typo in .travis.yml	4 days ago
CMakeLists.txt	Some Fixes for Windows	2 days ago
COPYING	Add Basic Core Plugin	2 months ago
README.md	More README	3 minutes ago

README.md

 r2ghidra-dec

build passing

This is an integration of the Ghidra decompiler for [radare2](#). It is solely based on the decompiler part of Ghidra, which is written entirely in C++, so Ghidra itself is not required at all and the plugin can be built self-contained.

## Installing

github.com/radareorg/r2ghidra-dec

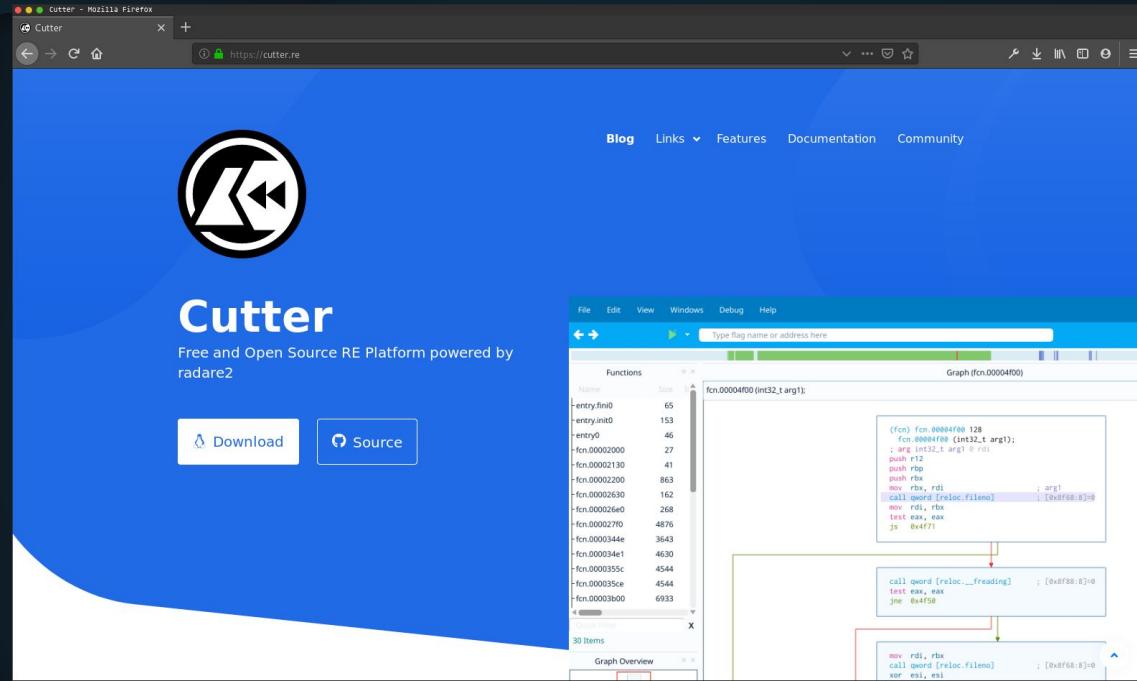
r2pm -i r2ghidra-dec

**Cutter**  
**v1.9**

**WHAT'S  
NEXT?**

# WHAT'S NEXT?

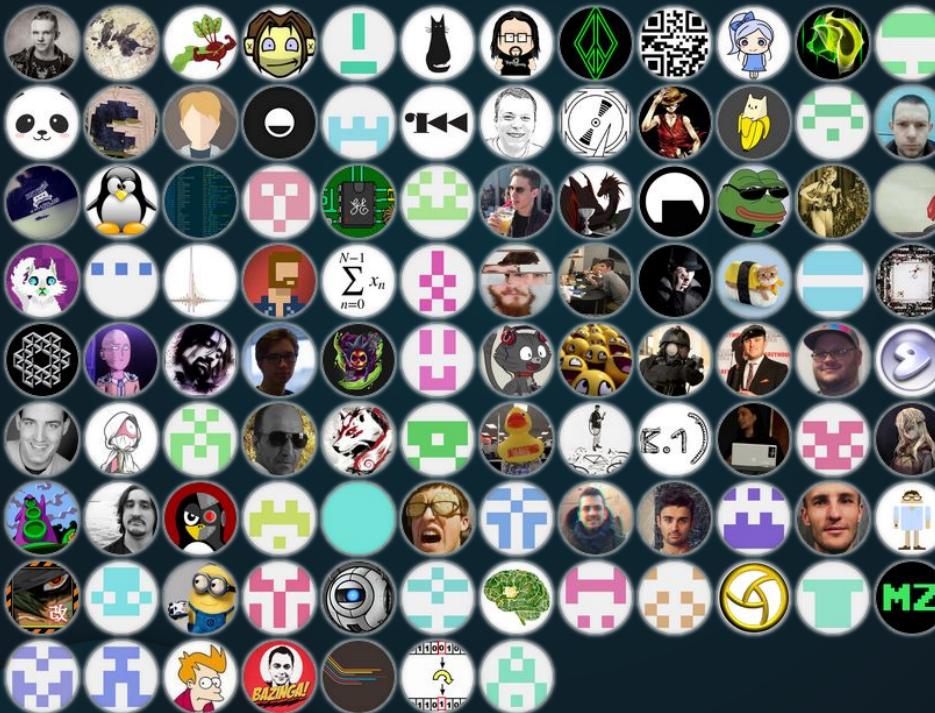
- Debugger
- Projects
- Package Manager (r2pm-go)
- IPython Console
- Improved API
- Documentation



<https://cutter.re>

# THANK YOU

## To all of our **contributors**





@optizone



@adikso



@pelijah



@karliss



@maijin



@a1ext



@fcasal

# SPECIAL THANKS

---

TO OUR **DEVELOPMENT TEAM**

AND **AK42** FOR HIS CONTRIBUTIONS  
TO R2GHIDRA



@vane11ope



@m0nk3ydluffy

# JOIN US!

---

We are looking for more people to join the team!

# Questions?

---