

Practica 1 - Parte 2 - EC | David Rodríguez Aparicio

Ejercicio 3

```
• david@david-VirtualBox:~/Escritorio/Ingenieria-Informatica-2/EC/Practica 1$ objdump -d p1.o

p1.o:      formato del fichero elf32-i386

Desensamblado de la sección .text:

00000000 <sum>:
  0:  8b 44 24 08      mov     0x8(%esp),%eax
  4:  03 44 24 04      add     0x4(%esp),%eax
  8:  c3               ret

• david@david-VirtualBox:~/Escritorio/Ingenieria-Informatica-2/EC/Practica 1$ objdump -t p1.o

p1.o:      formato del fichero elf32-i386

SYMBOL TABLE:
00000000 l    df *ABS*  00000000 p1.c
00000000 l    d  .text 00000000 .text
00000000 g    F  .text 00000009 sum

• david@david-VirtualBox:~/Escritorio/Ingenieria-Informatica-2/EC/Practica 1$ nm p1.o
00000000 T sum

• david@david-VirtualBox:~/Escritorio/Ingenieria-Informatica-2/EC/Practica 1$ objdump -S p1.o

p1.o:      formato del fichero elf32-i386

Desensamblado de la sección .text:

00000000 <sum>:
  0:  8b 44 24 08      mov     0x8(%esp),%eax
  4:  03 44 24 04      add     0x4(%esp),%eax
  8:  c3               ret

• david@david-VirtualBox:~/Escritorio/Ingenieria-Informatica-2/EC/Practica 1$ gcc -m32 -g -O -c p1.c
• david@david-VirtualBox:~/Escritorio/Ingenieria-Informatica-2/EC/Practica 1$ objdump -S p1.o

p1.o:      formato del fichero elf32-i386

Desensamblado de la sección .text:

00000000 <sum>:
int sum(int x, int y){
  int t = x+y;
  0:  8b 44 24 08      mov     0x8(%esp),%eax
  4:  03 44 24 04      add     0x4(%esp),%eax
  return t;
  8:  c3               ret
}

• david@david-VirtualBox:~/Escritorio/Ingenieria-Informatica-2/EC/Practica 1$ objdump -t p1.o

p1.o:      formato del fichero elf32-i386

SYMBOL TABLE:
00000000 l    df *ABS*  00000000 p1.c
00000000 l    d  .text 00000000 .text
00000000 l    d  .debug_info 00000000 .debug_info
00000000 l    d  .debug_abbrev 00000000 .debug_abbrev
00000000 l    d  .debug_loclists 00000000 .debug_loclists
00000000 l    d  .debug_line 00000000 .debug_line
00000000 l    d  .debug_str 00000000 .debug_str
00000000 l    d  .debug_line_str 00000000 .debug_line_str
00000000 g    F  .text 00000009 sum

• david@david-VirtualBox:~/Escritorio/Ingenieria-Informatica-2/EC/Practica 1$ objdump -h p1.o

p1.o:      formato del fichero elf32-i386

Secciones:
Idx Name          Size      VMA           LMA             File off  Algn
 0 .text           00000009 00000000 00000000 00000034 2**0
 1 .data           00000000 00000000 00000000 0000003d 2**0
 2 .bss            00000000 00000000 00000000 0000003d 2**0
 3 .debug_info     00000071 00000000 00000000 0000003d 2**0
```

```
david@david-VirtualBox:~/Escritorio/Ingenieria-Informatica-2/EC/Practica 1$ objdump -h p1.o
```

```
p1.o:      formato del fichero elf32-i386
```

```
Secciones:
```

Idx	Name	Size	VMA	LMA	File off	Algn
0	.text	00000009	00000000	00000000	00000034	2**0
	CONTENTS, ALLOC, LOAD, READONLY, CODE					
1	.data	00000000	00000000	00000000	0000003d	2**0
	CONTENTS, ALLOC, LOAD, DATA					
2	.bss	00000000	00000000	00000000	0000003d	2**0
	ALLOC					
3	.debug_info	00000071	00000000	00000000	0000003d	2**0
	CONTENTS, RELOC, READONLY, DEBUGGING, OCTETS					
4	.debug_abbrev	00000063	00000000	00000000	000000ae	2**0
	CONTENTS, READONLY, DEBUGGING, OCTETS					
5	.debug_loclists	00000022	00000000	00000000	00000111	2**0
	CONTENTS, READONLY, DEBUGGING, OCTETS					
6	.debug_aranges	00000020	00000000	00000000	00000133	2**0
	CONTENTS, RELOC, READONLY, DEBUGGING, OCTETS					
7	.debug_line	00000050	00000000	00000000	00000153	2**0
	CONTENTS, RELOC, READONLY, DEBUGGING, OCTETS					
8	.debug_str	00000084	00000000	00000000	000001a3	2**0
	CONTENTS, READONLY, DEBUGGING, OCTETS					
9	.debug_line_str	0000008b	00000000	00000000	00000227	2**0
	CONTENTS, READONLY, DEBUGGING, OCTETS					
10	.comment	0000002c	00000000	00000000	000002b2	2**0
	CONTENTS, READONLY					
11	.note.GNU-stack	00000000	00000000	00000000	000002de	2**0
	CONTENTS, READONLY					
12	.eh_frame	0000002c	00000000	00000000	000002e0	2**2
	CONTENTS, ALLOC, LOAD, RELOC, READONLY, DATA					

```
david@david-VirtualBox:~/Escritorio/Ingenieria-Informatica-2/EC/Practica 1$
```

```
david@david-VirtualBox:~/Escritorio/Ingenieria-Informatica-2/EC/Practica 1$ gcc -m32 -O -c p1.c
```

```
david@david-VirtualBox:~/Escritorio/Ingenieria-Informatica-2/EC/Practica 1$ objdump -S p1.o
```

```
p1.o:      formato del fichero elf32-i386
```

```
Desensamblado de la sección .text:
```

```
00000000 <sum>:
```

```
0: 8b 44 24 08      mov     0x8(%esp),%eax
4: 03 44 24 04      add     0x4(%esp),%eax
8: c3              ret
```

```
david@david-VirtualBox:~/Escritorio/Ingenieria-Informatica-2/EC/Practica 1$ objdump -h p1.o
```

```
p1.o:      formato del fichero elf32-i386
```

```
Secciones:
```

Idx	Name	Size	VMA	LMA	File off	Algn
0	.text	00000009	00000000	00000000	00000034	2**0
	CONTENTS, ALLOC, LOAD, READONLY, CODE					
1	.data	00000000	00000000	00000000	0000003d	2**0
	CONTENTS, ALLOC, LOAD, DATA					
2	.bss	00000000	00000000	00000000	0000003d	2**0
	ALLOC					
3	.comment	0000002c	00000000	00000000	0000003d	2**0
	CONTENTS, READONLY					
4	.note.GNU-stack	00000000	00000000	00000000	00000069	2**0
	CONTENTS, READONLY					
5	.eh_frame	0000002c	00000000	00000000	0000006c	2**2
	CONTENTS, ALLOC, LOAD, RELOC, READONLY, DATA					

```
david@david-VirtualBox:~/Escritorio/Ingenieria-Informatica-2/EC/Practica 1$
```

Ejercicio 4

```

EC > Practica 1 > Ejercicio Practica > saludos.s
1 # saludo.s: Imprimir por pantalla
2 # "Hola a todos!"
3 # "Hello, World!"
4 # retorna: código retorno 0, programado en la penúltima línea
5 # comprobar desde línea de comandos bash con "echo $?"
6
7 # =====
8 # SECCIÓN DE DATOS (.data, variables globales inicializadas)
9 # =====
10 .section .data          # directivas comienzan por punto
11                          # no son instrucciones máquina
12                          # sirven para reservar memoria o definir datos
13
14 saludo:
15     .ascii "Hola a todos!\nHello, World!\n"    # \n = salto de línea
16
17 longsaludo:
18     .int    . - saludo    # calcula la longitud del string automáticamente
19
20 PROBLEMAS  SALIDA  CONSOLA DE DEPURACIÓN  TERMINAL  PUERTOS

david@david-VirtualBox:~/Escritorio/Ingenieria-Informatica-2/EC/Practica 1/Ejercicio Practica$ as --32 -g saludo.s -o saludo.o
david@david-VirtualBox:~/Escritorio/Ingenieria-Informatica-2/EC/Practica 1/Ejercicio Practica$ ld -m elf_i386 saludo.o -o saludo
david@david-VirtualBox:~/Escritorio/Ingenieria-Informatica-2/EC/Practica 1/Ejercicio Practica$ ./saludo
Hola a todos!
Hello, World!
david@david-VirtualBox:~/Escritorio/Ingenieria-Informatica-2/EC/Practica 1/Ejercicio Practica$ ddd saludo &
[1] 24031
david@david-VirtualBox:~/Escritorio/Ingenieria-Informatica-2/EC/Practica 1/Ejercicio Practica$ Creating "/home/david/.ddd/"...
Creating "/home/david/.ddd/sessions/"...done.
Creating "/home/david/.ddd/themes/"...done.
Creating "/home/david/.ddd/themes/"...done.
Warning: Cannot convert string "-*-lucidatypewriter-medium-r-*-*120-*-*-*iso8859-*" to type FontStruct
(Annoyed? Try 'Edit->Preferences->General->Suppress X Warnings!')
Warning: Cannot convert string "-*-lucidatypewriter-bold-r-*-*120-*-*-*iso8859-*" to type FontStruct
Warning: Could not load font "-*-lucidatypewriter-medium-r-*-*120-*-*-*iso8859-*", using font "fixed" instead
Warning: Could not load font "-*-lucidatypewriter-medium-r-*-*120-*-*-*iso8859-*", using font "fixed" instead
Warning: Could not load font "-*-lucidatypewriter-bold-r-*-*120-*-*-*iso8859-*", using font "fixed" instead
david@david-VirtualBox:~/Escritorio/Ingenieria-Informatica-2/EC/Practica 1/Ejercicio Practica$

```

```

DDB: /home/david/Escritorio/Ingenieria-Informatica-2/EC/Practica 1/Ejercicio Practica/saludo.o
File Edit View Program Commands Status Source Data Help

main
# saludo.s: Imprimir por pantalla
# "Hola a todos!"
# "Hello, World!"
# retorna: código retorno 0, programado en la penúltima línea
# comprobar desde línea de comandos bash con "echo $?"
# =====
# SECCIÓN DE DATOS (.data, variables globales inicializadas)
# =====
.section .data          # directivas comienzan por punto
                          # no son instrucciones máquina
                          # sirven para reservar memoria o definir datos
saludo:
    .ascii "Hola a todos!\nHello, World!\n"    # \n = salto de línea
longsaludo:
    .int    . - saludo    # calcula la longitud del string automáticamente
.int      . - saludo    # calcula la longitud del string automáticamente

# SECCIÓN DE CÓDIGO (.text, instrucciones máquina)
# =====
.section .text          # punto de entrada del programa (como main en C)
.global _start          # inicio del programa en ensamblador
_start:
    # llamada al sistema WRITE
    # size_t write(int fd, const void *buf, size_t count)
    mov     $4, %eax      # syscall 4 = sys_write
    mov     $1, %ebx      # fd = 1 (stdout)
    mov     $saludo, %ecx  # puntero al texto
    mov     $longsaludo, %edx # longitud del texto
    int     $0x80          # interrupción para salir del programa

    # llamada al sistema EXIT
    # void _exit(int status)
    mov     $1, %eax      # syscall 1 = sys_exit
    mov     $0, %ebx      # status = 0 (OK)
    int     $0x80          # interrupción para salir del programa

GNU DDB 3.3.12 (x86_64-pc-linux-gnu), by Dorothea M. Lohr
(gdb)
Welcome to DDB 3.3.12 "Dale Head" (x86_64-pc-linux-gnu)

```

```

david@david-VirtualBox:~/Escritorio/Ingenieria-Informatica-2/EC/Practica 1/Ejercicio Practica$ ddd saludo &
[3] 24871
david@david-VirtualBox:~/Escritorio/Ingenieria-Informatica-2/EC/Practica 1/Ejercicio Practica$ Warning: Cannot convert string "-*-lucidatypewriter-medium-r-*-*120-*-*-*iso8859-*" to type FontStruct
(Annoyed? Try 'Edit->Preferences->General->Suppress X Warnings!')
Warning: Cannot convert string "-*-lucidatypewriter-bold-r-*-*120-*-*-*iso8859-*" to type FontStruct
Warning: Could not load font "-*-lucidatypewriter-medium-r-*-*120-*-*-*iso8859-*", using font "fixed" instead
Warning: Could not load font "-*-lucidatypewriter-medium-r-*-*120-*-*-*iso8859-*", using font "fixed" instead
Warning: Could not load font "-*-lucidatypewriter-bold-r-*-*120-*-*-*iso8859-*", using font "fixed" instead
david@david-VirtualBox:~/Escritorio/Ingenieria-Informatica-2/EC/Practica 1/Ejercicio Practica$

```

```
(gdb) info break
Num      Type           Disp Enb Address      What
1        breakpoint     keep y   0x08049000  saludo.s:33
(gdb) run
Starting program: /home/david/Escritorio/Ingenieria-Informatica-2/EC/Practica 1/Ejercicio Practica/saludo

This GDB supports auto-downloading debuginfo from the following URLs:
<https://debuginfod.ubuntu.com>
Enable debuginfod for this session? (y or [n]) y
Debuginfod has been enabled.
To make this setting permanent, add 'set debuginfod enabled on' to .gdbinit.
Downloading separate debug info for system-supplied DSO at 0xf7ffc000

Breakpoint 1, _start () at saludo.s:33
33      mov     $4, %eax          # syscall 4 = sys_write
(gdb) disassemble
Dump of assembler code for function _start:
=> 0x08049000 <+0>:  mov     $0x4,%eax
    0x08049005 <+5>:  mov     $0x1,%ebx
    0x0804900a <+10>: mov     $0x804a000,%ecx
    0x0804900f <+15>: mov     0x804a01c,%edx
    0x08049015 <+21>: int     $0x80
    0x08049017 <+23>: mov     $0x1,%eax
    0x0804901c <+28>: mov     $0x0,%ebx
    0x08049021 <+33>: int     $0x80
End of assembler dump.
(gdb)
```

```
(gdb) print $eip
$1 = (void (*)()) 0x08049000 <_start>
(gdb) print $eax
$2 = 0
(gdb) info registers
Nombre de registro perdido
(gdb) stepi          # ejecuta UNA instrucci3n
Invalid character '#' in expression.
(gdb) stepi
34      mov     $1, %ebx          # fd = 1 (stdout)
(gdb) file saludo
A program is being debugged already.
Are you sure you want to change the file? (y or n) n
Archivo no cambiado.
(gdb) print $eip
print $ebx
A syntax error in expression, near `print $ebx'.
(gdb) print $eip
$3 = void
(gdb) print $ebx
$4 = 0
(gdb) si
35      mov     $saludo, %ecx     # puntero al texto
(gdb) p/x $ecx
$5 = 0x0
(gdb)
```

```
(gdb) info registers
eax      0x0      0
ecx      0x0      0
edx      0x0      0
ebx      0x0      0
esp      0xffffcd10 0xffffcd10
ebp      0x0      0x0
esi      0x0      0
edi      0x0      0
eip      0x08049000 0x08049000 <_start>
eflags   0x202     [ IF ]
cs       0x23     35
ss       0x2b     43
ds       0x2b     43
es       0x2b     43
fs       0x0      0
gs       0x0      0
(gdb) stepi
34      mov     $1, %ebx          # fd = 1 (stdout)
(gdb) print $ebx
$3 = 0
(gdb) si
35      mov     $saludo, %ecx     # puntero al texto
(gdb) print/x $ecx
$4 = 0x0
(gdb) print/x $ecx
$5 = 0x0
(gdb) x/32cb &saludo
0x0804a000:  72 'H' 111 'o' 108 'l' 97 'a' 32 ' ' 97 'a' 32 ' ' 116 't'
0x0804a008:  111 'o' 100 'd' 111 'o' 115 's' 33 '!' 10 '\n' 72 'H' 101 'e'
0x0804a010:  108 'l' 108 'l' 111 'o' 44 ',' 32 ' ' 87 'W' 111 'o' 114 'r'
0x0804a018:  108 'l' 100 'd' 33 '!' 10 '\n' 28 '\034' 0 '\000' 0 '\000' 0 '\000'
(gdb) x/1dw &longsaludo
0x0804a01c:  28
(gdb)
```

```

(gdb) si
36      mov     longsaludo, %edx# longitud del texto
(gdb) si
37      int     $0x80      # interrupción → llamada al sistema
(gdb) info reg
eax      0x4              4
ecx      0x804a000        134520832
edx      0x1c             28
ebx      0x1              1
esp      0xffffcd10       0xffffcd10
ebp      0x0              0
esi      0x0              0
edi      0x0              0
eip      0x8049015         0x8049015 <_start+21>
eflags   0x10202          [ IF RF ]
cs       0x23             35
ss       0x2b             43
ds       0x2b             43
es       0x2b             43
fs       0x0              0
gs       0x0              0
(gdb) si
Hola a todos!
Hello, World!
44      mov     $1, %eax      # syscall 1 = sys_exit
(gdb) set $ebx = 1
(gdb) stepi
45      mov     $0, %ebx      # status = 0 (OK)
(gdb)

```

```

(gdb) print (char*)saludo
$1 = 0x616c6648 <error: No se puede acceder a la memoria en la dirección 0x616c6f48>
(gdb) p (char*)&saludo+13
$2 = 0x804a00d "\nHello, World!\n\034"
(gdb) p *((char*)&saludo+13)
$3 = 10 '\n'
(gdb) set var *((char*)&saludo+13)='- '
No se puede acceder a la memoria en la dirección 0x804a00d
(gdb) print (char*)saludo
$4 = 0x616c6f48 <error: No se puede acceder a la memoria en la dirección 0x616c6f48>
(gdb) run
Starting program: /home/david/Escritorio/Ingenieria-Informatica-2/EC/Practica 1/Ejercicio Practica/saludo

This GDB supports auto-downloading debuginfo from the following URLs:
<https://debuginfod.ubuntu.com>
Enable debuginfod for this session? (y or [n]) y
Debuginfod has been enabled.
To make this setting permanent, add 'set debuginfod enabled on' to .gdbinit.
Hola a todos!
Hello, World!
[Inferior 1 (process 10432) exited normally]
(gdb)

```