

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  Align
 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
```

```
• 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 000000a0 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$
```

davidrdgz-UGR (Hace 6 días) Lin. 4, col. 2 Espacios: 4 UTF-8 LF {} C Linux Q

- 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

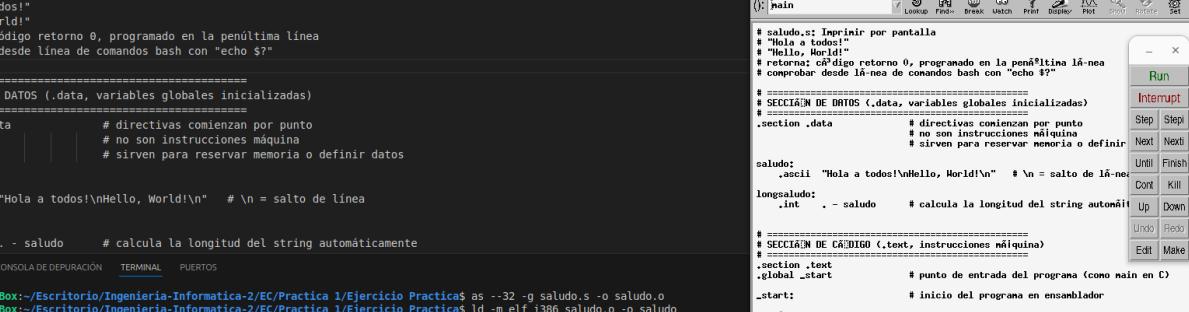
p1.o: formato del fichero elf32-i386

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



```
saludo.s X
EC > Práctica 1 > Ejercicio Práctica > saludo.s
1 # saludo.: Imprimir por pantalla
2 # "Hola a todos!"
3 # "Hello, World!"
4 # retorna: código retorno 0, programado en la penúltima línea
5 # comprobar desde linea 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

PROBLEMAS SALIDA CONSOLA DE DEPURACIÓN TERMINAL PUERTOS

• david@david-VirtualBox:~/Escritorio/Ingieria-Informatica-2/EC/Práctica 1/Ejercicio Práctica$ as -32 -g saludo.o -o saludo.o
• david@david-VirtualBox:~/Escritorio/Ingieria-Informatica-2/EC/Práctica 1/Ejercicio Práctica$ ld -m elf_i386 saludo.o -o saludo
• david@david-VirtualBox:~/Escritorio/Ingieria-Informatica-2/EC/Práctica 1/Ejercicio Práctica$ ./saludo
Hola a todos!
Hello, World!
• david@david-VirtualBox:~/Escritorio/Ingieria-Informatica-2/EC/Práctica 1/Ejercicio Práctica$ ddd saludo &
[1] 24801
david@david-VirtualBox:~/Escritorio/Ingieria-Informatica-2/EC/Práctica 1/Ejercicio Práctica$ Creating "/home/david/.ddd"...
Creating "/home/david/.ddd"...done.
Creating "/home/david/.ddd/sessions"...
Creating "/home/david/.ddd/sessions/themes"...
Creating "/home/david/.ddd/themes"...
Creating "/home/david/.ddd/themes"...done.
Warning: Cannot convert string "luciditypewriter-medium-r-*-*-120-*-*-*.iso8859-*" to type FontStruct
(Annoyed? Try Edit->Preferences->General->Suppress X Warnings!)
Warning: Cannot convert string "luciditypewriter-bold-r-*-*-120-*-*-*.iso8859-*" to type FontStruct
Warning: Could not load font "luciditypewriter-medium-*-*-120-*-*-*.iso8859-*", using font "fixed" instead
Warning: Could not load font "luciditypewriter-medium-r-*-*-120-*-*-*.iso8859-*", using font "fixed" instead
Warning: Could not load font "luciditypewriter-bold-*-*-120-*-*-*.iso8859-*", using font "fixed" instead
• david@david-VirtualBox:~/Escritorio/Ingieria-Informatica-2/EC/Práctica 1/Ejercicio Práctica$ [
```

The screenshot shows a terminal window with assembly code and a debugger session.

Assembly Code:

```
1 # saludos: 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 saludos:
15     .ascii  "Hola a todos!\nHello, World!\n"    # \n = salto de linea
16
17 longsaludo:
18     .int   . - saludos      # calcula la longitud del string automáticamente
```

Terminal Output:

```
PROBLEMAS SALIDA CONSOLA DE DEPURACIÓN TERMINAL PUERTOS

david@david-VirtualBox:~/Escritorio/Ingeneria-Informatica-2/EC/Practica 1/Ejercicio Practica$ ddd saludos &
[3] 24871
david@david-VirtualBox:~/Escritorio/Ingeneria-Informatica-2/EC/Practica 1/Ejercicio Practica$ Warning: Cannot convert string "-*(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-*-*-*120**-*-*iso8859-*", using font "fixed" instead
```

Debugger Session:

```
DDD: /home/david/Escritorio/Ingeneria-Informatica-2/EC/Practica 1/Ejercicio Practica$ File Edit View Program Commands Status Source Data Help
File Edit View Program Commands Status Source Data Help
(: main Lookup Find Break Watch Print Display Post Show Rotate Help
# saludos: 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
GNU DDD 3.3.12 (x86_64-pc-linux-gnu), by Borodoea |Reading symbols: Util|Finish
(gdb) list
1 # saludos: 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
(gdb) break 301
```

The debugger interface includes tabs for File, Edit, View, Program, Commands, Status, Source, Data, and Help. It also features a toolbar with icons for Lookup, Find, Break, Watch, Print, Display, Post, Show, Rotate, and Help. The status bar at the bottom shows the current file path and line number.

```
(gdb) file saludo.o
Cargar una tabla de símbolos nueva desde «saludo.o»? (y or n) y
Reading symbols from saludo.o...
(gdb) list
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 linea de comandos bash con "echo $?"
6
7     # =====
8     # SECCIÓN DE DATOS (.data, variables globales inicializadas)
9     # =====
10    .section .data          # directivas comienzan por punto
(gdb) break 30
Punto de interrupción 1 at 0x0: file saludo.s, line 33.
(gdb) info break
Num  Type      Disp Enb Address  What
1    breakpoint  keep y  0x00000000 saludo.s:33
(gdb) run
Starting program: /home/david/Escritorio/Ingenieria-Informatica-2/EC/Practica 1/Ejercicio Practica/saludo.o
/bin/bash: línea 1: /home/david/Escritorio/Ingenieria-Informatica-2/EC/Practica 1/Ejercicio Practica/saludo.o: Permisos denegados
/bin/bash: línea 1: exec: /home/david/Escritorio/Ingenieria-Informatica-2/EC/Practica 1/Ejercicio Practica/saludo.o: no se puede ejecutar: Permisos denegados
Durante el arranque el programa salió con el código 126.
(gdb)
```

```
(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 (*)()) 0x8049000 <_start>
(gdb) print $eax
$2 = 0
(gdb) info registers
Nombre de registro perdido
(gdb) stepi      # ejecuta UNA instrucción
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 $eix
$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          0xfffffc10  0xfffffc10
ebp          0x0          0x0
esi          0x0          0
edi          0x0          0
eip          0x8049000  0x8049000 <_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
0x804a000: 72 'H' 111 'o' 108 'l' 97 'a' 32 '' 97 'a' 32 '' 116 't'
0x804a008: 111 'o' 100 'd' 111 'o' 115 's' 33 '!' 10 '\n' 72 'H' 101 'e'
0x804a010: 108 'l' 108 'l' 111 'o' 44 ',' 32 '' 87 'W' 111 'o' 114 'r'
0x804a018: 108 'l' 100 'd' 33 '!' 10 '\n' 28 '\034' 0 '\000' 0 '\000'
(gdb) x/1dw &longsaludo
0x804a01c: 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            0xfffffc10    0xfffffc10
ebp            0x0          0x0
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 = 0x616c6f48 <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) █
```