Лабораторная работа №16. Основы работы с отладчиком gdb. Особенности Runtime Stack x86-64. Знакомство с набором инструкций SSE3

Макаров П. А.

1 Краткая теория

1. GNU Debugger — Wikipedia.
2. Tom Doeppner. gdb Cheatsheet.
3. Стек — Википедия.
4. x86 Disassembly/The Stack — Wikibooks.
5. Юрий Георгиев. x86/x64 CPU architecture: the stack & stack frames.
6. Eli Bendersky Stack frame layout on x86-64.
7. Tom Doeppner. x64 Cheatsheet.
8. Julia Evans. How to look at the stack with gdb.
9. SSE — Wikibooks.

2 Задания для самостоятельного решения

1. Изучите все материалы, перечисленные в разделе 1.
2. Исследуйте в отладчике `gdb` работу следующей программы.

Листинг 1: Содержимое файла `x86-64_stack.nasm`

```
global _start
```

```
section .data
    a db 0xA7
    b dw 0xCAFE
    c dd 0xDEADBEEF
    d dq 0x0123456789ABCDEF

section .text
_start:
    xor rax, rax
    mov al, [a]
    push rax
    mov ax, [b]
    push rax
    mov eax, [c]
    push rax
    mov rax, [d]
    push rax
    ; pusha is excluded in x86_64
    pushf

exit:
    mov rax, 60
    mov rdi, 0
    syscall
```

Для трансляции программы выполните следующие команды

Листинг 2: Трансляция исходного файла x86-64_stack.nasm

```
$ nasm -f elf64 -g x86-64_stack.nasm
$ ld x86-64_stack.o -o x86-64_stack
```

Для отладки полученной программы выполните

Листинг 3: Отладка программы x86-64_stack

```
$ gdb -q ./x86-64_stack
help x
break _start
run
disass
step
p $rax
step
x/40xb $sp
x/5xg $sp
step
p $rax
step
x/40xb $sp
x/5xg $sp
... etc ...
```

```
quit
```

3. Исследуйте в отладчике gdb работу следующей программы.

Листинг 4: Содержимое файла sse3test.nasm

```
global _start

section .data
    v1: dd 1.2, 1.1, 2.3, 1.1    ; first set of 4 numbers
    v2: dd 3.4, 1.1, 4.5, 1.1    ; second set

section .bss
    v3: resd 4          ; result

section .text
_start:
    movups xmm0, [v1]   ; load v1 into xmm0
    movups xmm1, [v2]   ; load v2 into xmm1
    hsubps xmm0, xmm1   ; Horizontal-Subtract-Packed-Single
    movups [v3], xmm0   ; store xmm0 in v3

    mov rax, 60
    mov rdi, 0
    syscall
```

Для трансляции программы выполните следующие команды

Листинг 5: Трансляция исходного файла sse3test.nasm

```
$ nasm -f elf64 -g sse3test.nasm
$ ld sse3test.o -o sse3test
```

Для отладки полученной программы выполните

Листинг 6: Отладка программы sse3test

```
break _start
run
disass
stepi
p $xmm0
p $xmm0.v4_float
stepi
p $xmm1.v4_float
stepi
x/4f &v3
quit
```