

Лабараторная работа №09.

НКАбд-01-24

Подготовил:

Холов Икром Комронович

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	16

Список иллюстраций

2.1	Создал lab09-1.asm	6
2.2	Заполнил lab09-1.asm	7
2.3	Проверил lab09-1.asm	8
2.4	Создал lab09-2.asm	8
2.5	Заполнил lab09-2.asm	8
2.6	Проверил lab09-2.asm	9
2.7	Загрузил исполняемый файл	9
2.8	Проверил исполняемый файл	9
2.9	Установил брейкпоинт	10
2.10	Посмотрел дисассимилированный код	10
2.11	Переключился на отображение команд	11
2.12	Включил режим псевдографики	11
2.13	Перечислил различия	12
2.14	Установил еще одну точку останова	12
2.15	Посмотрел информацию о всех установленных точках останова . .	13
2.16	Посмотрел значение переменной msg1 по имени	13
2.17	Изменил первый символ переменной	13
2.18	Изменил значение регистра	13
2.19	Скопировал файл lab08-2.asm	13
2.20	Создал исполняемый файл	14
2.21	Загрузил исполняемый файл	14
2.22	Установил точку	14
2.23	Посмотрел остальные позиции стека	15

Список таблиц

1 Цель работы

Приобретение навыков написания программ с использованием подпрограмм.
Знакомство с методами отладки при помощи GDB и его основными возможностями

2 Выполнение лабораторной работы

1. Создал lab09-1.asm (рис. 2.1)

```
ikkholov@dk8n77 ~ $ mkdir ~/work/arch-pc/lab09
ikkholov@dk8n77 ~ $ cd ~/work/arch-pc/lab09
ikkholov@dk8n77 ~/work/arch-pc/lab09 $ touch lab09-1.asm
ikkholov@dk8n77 ~/work/arch-pc/lab09 $
```

Рис. 2.1: Создал lab09-1.asm

2. Заполнил lab09-1 (рис. 2.2)

```

1 %include 'in_out.asm'
2
3 SECTION .data
4     msg: DB 'Введите x: ',0
5     result: DB '2x+7=',0
6
7 SECTION .bss
8     x: RESB 80
9     res: RESB 80
10
11 SECTION .text
12 GLOBAL _start
13     _start:
14 mov eax, msg
15 call sprint
16
17 mov ecx, x
18 mov edx, 80
19 call sread
20
21 mov eax, x
22 call atoi
23
24 call _calcul ; Вызов подпрограммы _calcul
25
26 mov eax, result
27 call sprint
28
29 mov eax, [res]
30 call iprintLF
31
32 call quit
33
34 _calcul:
35     mov ebx, 2
36     mul ebx
37     add eax, 7
38 mov [res], eax
39
40 ret

```

Рис. 2.2: Заполнил lab09-1.asm

3. Проверил lab09-1 (рис. 2.3)

```
ikkholov@dk8n77 ~/work/arch-pc/lab09 $ nasm -f elf lab09-1.asm
ikkholov@dk8n77 ~/work/arch-pc/lab09 $ ld -m elf_i386 -o lab09-1 lab09-1.o
ikkholov@dk8n77 ~/work/arch-pc/lab09 $ ./lab09-1
Введите x: 49
2x+7=105
ikkholov@dk8n77 ~/work/arch-pc/lab09 $
```

Рис. 2.3: Проверил lab09-1.asm

4. Создал lab09-2.asm (рис. 2.4)

```
ikkholov@dk8n77 ~/work/arch-pc/lab09 $ touch lab09-2.asm
ikkholov@dk8n77 ~/work/arch-pc/lab09 $ gedit lab09-2.asm
```

Рис. 2.4: Создал lab09-2.asm

5. Заполнил lab09-2 (рис. 2.5)

```
1 SECTION .data
2     msg1: db "Hello, ",0x0
3     msg1Len: equ $ - msg1
4
5     msg2: db "world!",0xa
6     msg2Len: equ $ - msg2
7
8 SECTION .text
9     global _start
10
11 _start:
12     mov eax, 4
13     mov ebx, 1
14     mov ecx, msg1
15     mov edx, msg1Len
16     int 0x80
17
18     mov eax, 4
19     mov ebx, 1
20     mov ecx, msg2
21     mov edx, msg2Len
22     int 0x80
23
24     mov eax, 1
25     mov ebx, 0
26     int 0x80
```

Рис. 2.5: Заполнил lab09-2.asm

6. Проверил_lab09-2 (рис. 2.6)

```
ikkholov@dk8n77 ~/work/arch-pc/lab09 $ gedit lab09-2.asm
ikkholov@dk8n77 ~/work/arch-pc/lab09 $ nasm -f elf lab09-2.asm
ikkholov@dk8n77 ~/work/arch-pc/lab09 $ ld -m elf_i386 -o lab09-2 lab09-2.o
ikkholov@dk8n77 ~/work/arch-pc/lab09 $ ./lab09-2
Hello, world!
ikkholov@dk8n77 ~/work/arch-pc/lab09 $
```

Рис. 2.6: Проверил_lab09-2.asm

7. Загрузил исполняемый файл (рис. 2.7)

```
ikkholov@dk8n77 ~/work/arch-pc/lab09 $ gdb lab09-2
GNU gdb (Gentoo 14.2 vanilla) 14.2
Copyright (C) 2023 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-pc-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://bugs.gentoo.org/>.
Find the GDB manual and other documentation resources online at:
  <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from lab09-2...
(No debugging symbols found in lab09-2)
(gdb) run
```

Рис. 2.7: Загрузил исполняемый файл

8. Проверил исполняемый файл (рис. 2.8)

```
(gdb) run
Starting program: /afs/.dk.sci.pfu.edu.ru/home/i/k/ikkholov/work/arch-pc/lab09/lab09-2
Hello, world!
[Inferior 1 (process 14618) exited normally]
(gdb) break _start
```

Рис. 2.8: Проверил исполняемый файл

9. Установил брейкпоинт (рис. 2.9)

```
(gdb) break _start
Breakpoint 1 at 0x8049000
(gdb) run
Starting program: /afs/.dk.sci.pfu.edu.ru/home/i/k/ikkholov/work/arch-pc/lab09/lab09-2

Breakpoint 1, 0x8049000 in _start ()
(gdb) disassemble _start
```

Рис. 2.9: Установил брейкпоинт

10. Посмотрел дисассимилированный код (рис. 2.10)

```
(gdb) disassemble _start
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     $0x8,%edx
0x08049014 <+20>:     int     $0x80
0x08049016 <+22>:     mov     $0x4,%eax
0x0804901b <+27>:     mov     $0x1,%ebx
0x08049020 <+32>:     mov     $0x804a008,%ecx
0x08049025 <+37>:     mov     $0x7,%edx
0x0804902a <+42>:     int     $0x80
0x0804902c <+44>:     mov     $0x1,%eax
0x08049031 <+49>:     mov     $0x0,%ebx
0x08049036 <+54>:     int     $0x80
End of assembler dump.
(gdb) □
```

Рис. 2.10: Посмотрел дисассимилированный код

11. Переключился на отображение команд (рис. [@-fig:011])

```

(gdb) set disassembly-flavor intel
(gdb) disassemble _start
Dump of assembler code for function _start:
=> 0x08049000 <+0>:      mov     eax,0x4
    0x08049005 <+5>:      mov     ebx,0x1
    0x0804900a <+10>:     mov     ecx,0x804a000
    0x0804900f <+15>:     mov     edx,0x8
    0x08049014 <+20>:     int     0x80
    0x08049016 <+22>:     mov     eax,0x4
    0x0804901b <+27>:     mov     ebx,0x1
    0x08049020 <+32>:     mov     ecx,0x804a008
    0x08049025 <+37>:     mov     edx,0x7
    0x0804902a <+42>:     int     0x80
    0x0804902c <+44>:     mov     eax,0x1
    0x08049031 <+49>:     mov     ebx,0x0
    0x08049036 <+54>:     int     0x80
End of assembler dump.
(gdb) 

```

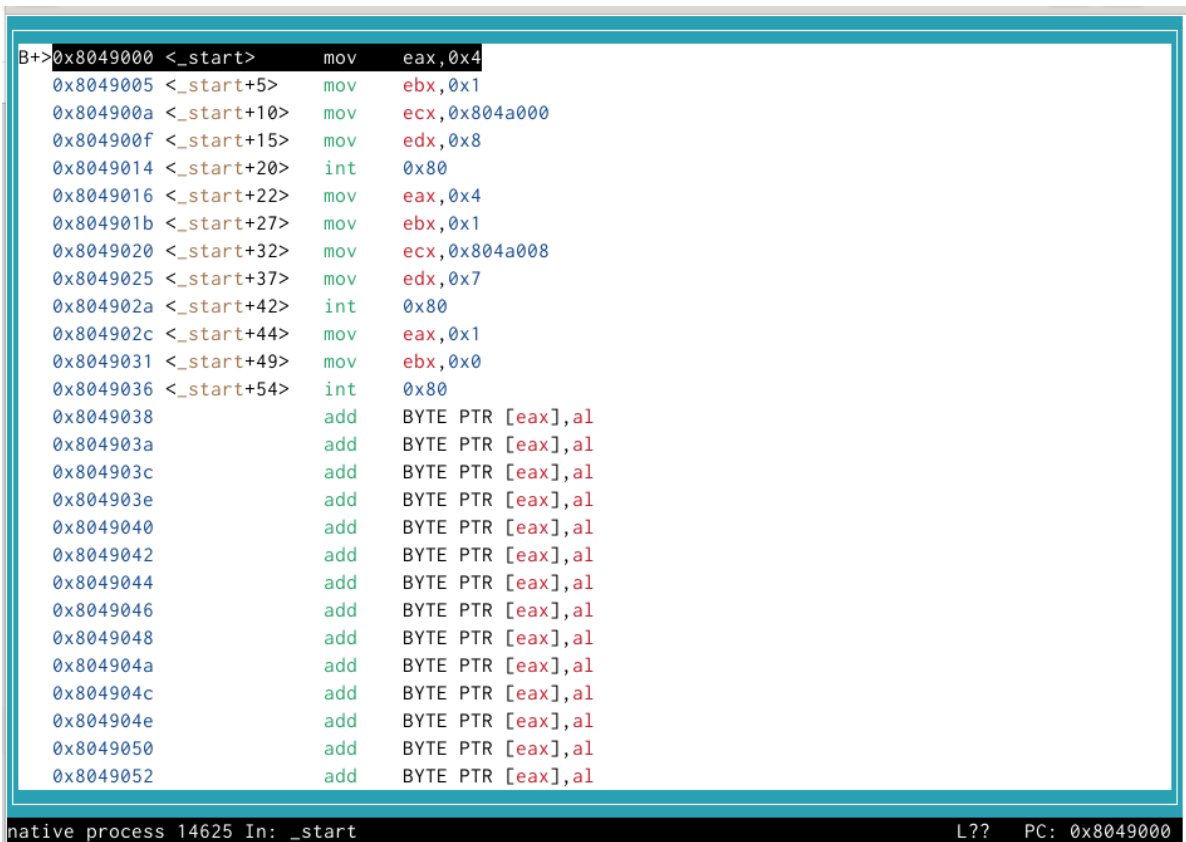
Рис. 2.11: Переключился на отображение команд

12. Включил режим псевдографики (рис. 2.12)



Рис. 2.12: Включил режим псевдографики

13. Перечислил различия (рис. 2.13)

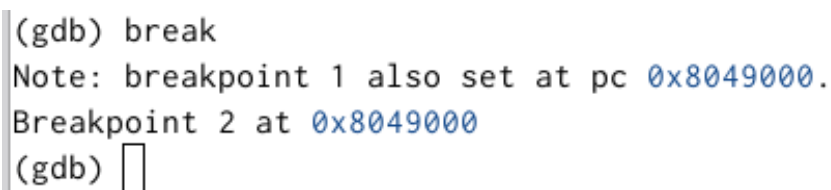


```
B+>0x8049000 <_start>    mov     eax,0x4
0x8049005 <_start+5>    mov     ebx,0x1
0x804900a <_start+10>   mov     ecx,0x804a000
0x804900f <_start+15>   mov     edx,0x8
0x8049014 <_start+20>   int     0x80
0x8049016 <_start+22>   mov     eax,0x4
0x804901b <_start+27>   mov     ebx,0x1
0x8049020 <_start+32>   mov     ecx,0x804a008
0x8049025 <_start+37>   mov     edx,0x7
0x804902a <_start+42>   int     0x80
0x804902c <_start+44>   mov     eax,0x1
0x8049031 <_start+49>   mov     ebx,0x0
0x8049036 <_start+54>   int     0x80
0x8049038          add     BYTE PTR [eax],al
0x804903a          add     BYTE PTR [eax],al
0x804903c          add     BYTE PTR [eax],al
0x804903e          add     BYTE PTR [eax],al
0x8049040          add     BYTE PTR [eax],al
0x8049042          add     BYTE PTR [eax],al
0x8049044          add     BYTE PTR [eax],al
0x8049046          add     BYTE PTR [eax],al
0x8049048          add     BYTE PTR [eax],al
0x804904a          add     BYTE PTR [eax],al
0x804904c          add     BYTE PTR [eax],al
0x804904e          add     BYTE PTR [eax],al
0x8049050          add     BYTE PTR [eax],al
0x8049052          add     BYTE PTR [eax],al

native process 14625 In: _start L?? PC: 0x8049000
```

Рис. 2.13: Перечислил различия

14. Установил еще одну точку останова (рис. 2.14)



```
(gdb) break
Note: breakpoint 1 also set at pc 0x8049000.
Breakpoint 2 at 0x8049000
(gdb) █
```

Рис. 2.14: Установил еще одну точку останова

15. Посмотрел информацию о всех установленных точках останова (рис. 2.15)

```
(gdb) i b
Num      Type           Disp Enb Address      What
1        breakpoint     keep y   0x08049000 <_start>
          breakpoint already hit 1 time
2        breakpoint     keep y   0x08049000 <_start>
(gdb) █
```

Рис. 2.15: Посмотрел информацию о всех установленных точках останова

16. Посмотрел значение переменной msg1 по имени (рис. 2.16)

```
(gdb) x/1sb &msg1
0x804a000:      "Hello, "
(gdb) █
```

Рис. 2.16: Посмотрел значение переменной msg1 по имени

17. Изменил первый символ переменной msg1 (рис. 2.17)

```
(gdb) set {char}&msg1='h'
(gdb) x/1sb &msg1
0x804a000:      "hello, "
      █
```

Рис. 2.17: Изменил первый символ переменной

18. Изменил значение регистра (рис. 2.18)

```
(gdb) set $ebx='2'
(gdb) p/s $ebx
$1 = 50
      █
```

Рис. 2.18: Изменил значение регистра

19. Скопировал файл lab08-2.asm (рис. 2.19)

```
ikkholov@dk8n77 ~/work/arch-pc/lab09 $ cp ~/work/arch-pc/lab08/lab08-2.asm ~/work/arch-pc/lab09/lab09-3.
asm
ikkholov@dk8n77 ~/work/arch-pc/lab09 $ █
```

Рис. 2.19: Скопировал файл lab08-2.asm

20. Создал исполняемый файл (рис. 2.20)

```
ikkholov@dk8n77 ~/work/arch-pc/lab09 $ nasm -f elf lab09-3.asm
ikkholov@dk8n77 ~/work/arch-pc/lab09 $ ld -m elf_i386 -o lab09-3 lab09-3.o
ikkholov@dk8n77 ~/work/arch-pc/lab09 $
```

Рис. 2.20: Создал исполняемый файл

21. Загрузил исполняемый файл (рис. 2.21)

```
ikkholov@dk8n77 ~/work/arch-pc/lab09 $ gdb lab09-2
GNU gdb (Gentoo 14.2 vanilla) 14.2
Copyright (C) 2023 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-pc-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://bugs.gentoo.org/>.
Find the GDB manual and other documentation resources online at:
  <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from lab09-2...
(No debugging symbols found in lab09-2)
(gdb) run
```

Рис. 2.21: Загрузил исполняемый файл

22. Установил точку (рис. 2.22)

```
(gdb) b _start
quit
Breakpoint 1 at 0x80490e8
(gdb) run

Starting program: /afs/.dk.sci.pfu.edu.ru/home/i/k/ikkholov/work/arch-pc/lab09/lab09-3 аргумент1 аргумен
т2 аргумент\ 3

Breakpoint 1, 0x80490e8 in _start ()
(gdb)
```

Рис. 2.22: Установил точку

23. Посмотрел остальные позиции стека (рис. ??)

```
(gdb) x/s *(void**)(esp + 4)

0xffffc6ce:      "/afs/.dk.sci.pfu.edu.ru/home/i/k/ikkholov/work/arch-pc/lab09/lab09-3"
(gdb) x/s *(void**)(esp + 8)

0xffffc713:      "аргумент1"
(gdb) x/s *(void**)(esp + 12)

0xffffc725:      "аргумент2"
(gdb) x/s *(void**)(esp + 16)

0xffffc737:      "аргумент 3"
(gdb) x/s *(void**)(esp + 20)

0x0:      <error: Cannot access memory at address 0x0>
(gdb) x/s *(void**)(esp + 24)

0xffffc74a:      "SHELL=/bin/bash"
(gdb) □
```

Рис. 2.23: Посмотрел остальные позиции стека

3 Выводы

Завершил лабораторную номер 9