Отчет по лабораторной работе №9

Дисциплина: Архитектура компьютера

Чипурной Михаил Евгеньевич

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Познакомиться с методами отладки при помощи GDB, его возможностями.

2 Выполнение лабораторной работы

2.1 Реализация подпрограмм в NASM

Создаем каталог для программ ЛБ9, и в нем создаем файл (рис. Рисунок 2.1).

```
mechipurnoyj@fedora:~$ mkdir ~/work/arch-pc/lab09
mechipurnoyj@fedora:~$ cd ~/work/arch-pc/lab09
mechipurnoyj@fedora:~/work/arch-pc/lab09$ touch lab09-1.asm
mechipurnoyj@fedora:~/work/arch-pc/lab09$
```

Рисунок 2.1: Создаем каталог с помощью команды mkdir и файл с помощью команды touch

Открываем файл в Midnight Commander и заполняем его в соответствии с листингом 9.1 (рис. Рисунок 2.2).

Рисунок 2.2: Заполняем файл

Создаем исполняемый файл и запускаем его (рис. Рисунок 2.3).

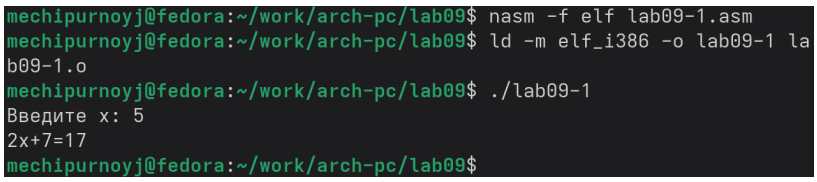

Рисунок 2.3: Запускаем файл и проверяем его работу

Снова открываем файл для редактирования и изменяем его, добавив подпрограмму в подпрограмму(по условию) (рис. Рисунок 2.4).

Рисунок 2.4: Изменяем файл, добавляя еще одну подпрограмму

Создаем исполняемый файл и запускаем его (рис. Рисунок 2.5).

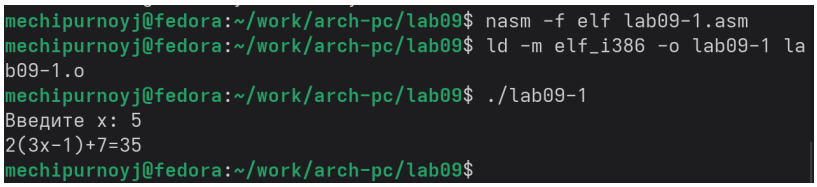

Рисунок 2.5: Запускаем файл и смотрим на его работу

2.2 Отладка программам с помощью GDB

Создаем новый файл в каталоге(рис. Рисунок 2.6).

```
mechipurnoyj@fedora:~/work/arch-pc/lab09$ touch lab09-2.asm
mechipurnoyj@fedora:~/work/arch-pc/lab09$
```

Рисунок 2.6: Создаем файл

Открываем файл в Midnight Commander и заполняем его в соответствии с листингом 9.2 (рис. Рисунок 2.7).

```
lab09-2.asm        [-M--]  4 L:[  1+20  21/ 22] *(357 / 366b) 0105 0x069
SECTION .data
    msg1: db "Hello, ",0x0
    msg1Len: equ $ - msg1
    msg2: db "world!",0xa
    msg2Len: equ $ - msg2
SECTION .text
    global _start
_start:
    mov eax, 4
    mov ebx, 1
    mov ecx, msg1
    mov edx, msg1Len
    int 0x80
    mov eax, 4
    mov ebx, 1
    mov ecx, msg2
    mov edx, msg2Len
    int 0x80
    mov eax, 1
    mov ebx, 0
    int 0x80
```

Рисунок 2.7: Заполняем файл

Получаем исходный файл с использованием отладчика gdb (рис. Рисунок 2.8).

```
mechipurnoyj@fedora:~/work/arch-pc/lab09$ nasm -f elf -g -l lab09-2.ls
t lab09-2.asm
mechipurnoyj@fedora:~/work/arch-pc/lab09$ ld -m elf_i386 -o lab09-2 la
b09-2.o
mechipurnoyj@fedora:~/work/arch-pc/lab09$ gdb lab09-2
GNU gdb (Fedora Linux) 16.2-3.fc42
Copyright (C) 2024 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gp
l.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-redhat-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
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...
(gdb)
```

Рисунок 2.8: Загружаем исходный файл в отладчик

Запускаем команду в отладчике (рис. Рисунок 2.9).

```
(gdb) run
Starting program: /home/mechipurnoyj/work/arch-pc/lab09/lab09-2
Hello, world!
[Inferior 1 (process 9651) exited normally]
(gdb)
```

Рисунок 2.9: Запускаем программу командой run

Устанавливаем брейкпоинт на метку _start и запускаем программу (рис. Рисунок 2.10).

```
(gdb) break _start
Breakpoint 1 at 0x8048080: file lab09-2.asm, line 9.
(gdb) run
Starting program: /home/mechipurnoyj/work/arch-pc/lab09/lab09-2

Breakpoint 1, _start () at lab09-2.asm:9
9           mov eax, 4
(gdb)
```

Рисунок 2.10: Запускаем программу с брейкпоином

Смотрим дисассимилированный код программы с помощью команды disassemble, начиная с метки _start(рис. Рисунок 2.11).

```
(gdb) disassemble _start
Dump of assembler code for function _start:
=> 0x08048080 <+0>:     mov    $0x4,%eax
   0x08048085 <+5>:     mov    $0x1,%ebx
   0x0804808a <+10>:    mov    $0x8049000,%ecx
   0x0804808f <+15>:    mov    $0x8,%edx
   0x08048094 <+20>:    int    $0x80
   0x08048096 <+22>:    mov    $0x4,%eax
   0x0804809b <+27>:    mov    $0x1,%ebx
   0x080480a0 <+32>:    mov    $0x8049008,%ecx
   0x080480a5 <+37>:    mov    $0x7,%edx
   0x080480aa <+42>:    int    $0x80
   0x080480ac <+44>:    mov    $0x1,%eax
   0x080480b1 <+49>:    mov    $0x0,%ebx
   0x080480b6 <+54>:    int    $0x80
End of assembler dump.
(gdb)
```

Рисунок 2.11: Смотрим дисассимилированный код программы

Переключаемся на отображение команд с Intel'овским синтаксисом (рис. Рисунок 2.12).

```
(gdb) set disassembly-flavor intel
(gdb) disassemble _start
Dump of assembler code for function _start:
=> 0x08048080 <+0>:     mov    eax,0x4
   0x08048085 <+5>:     mov    ebx,0x1
   0x0804808a <+10>:    mov    ecx,0x8049000
   0x0804808f <+15>:    mov    edx,0x8
   0x08048094 <+20>:    int    0x80
   0x08048096 <+22>:    mov    eax,0x4
   0x0804809b <+27>:    mov    ebx,0x1
   0x080480a0 <+32>:    mov    ecx,0x8049008
   0x080480a5 <+37>:    mov    edx,0x7
   0x080480aa <+42>:    int    0x80
   0x080480ac <+44>:    mov    eax,0x1
   0x080480b1 <+49>:    mov    ebx,0x0
   0x080480b6 <+54>:    int    0x80
End of assembler dump.
(gdb)
```

Рисунок 2.12: Переключаемся на синтаксис Intel

Различия отображения синтаксиса машинных команд в режимах ATT и Intel:

1. Порядок операндов: В ATT синтаксисе порядок операндов обратный, сначала указывается исходный операнд, а затем - результирующий операнд. В Intel синтаксисе порядок обычно прямой, результирующий операнд указывается первым, а исходный - вторым.

2. Разделители: В ATT синтаксисе разделители операндов - запятые. В Intel синтаксисе разделители могут быть запятые или косые черты (/).

3. Префиксы размера операндов: В ATT синтаксисе размер операнда указывается перед операндом с использованием префиксов, таких как «b» (byte), «w» (word), «l» (long) и «q» (quadword). В Intel синтаксисе размер операнда указывается после операнда с использованием суффиксов, таких как «b», «w», «d» и «q».

4. Знак операндов: В ATT синтаксисе операнды с позитивными значениями предваряются символом «".$Intel$"».

5. Обозначение адресов: В ATT синтаксисе адреса указываются в круглых скобках. В Intel синтаксисе адреса указываются без скобок.

6. Обозначение регистров: В ATT синтаксисе обозначение регистра начинается с символа «%». В Intel синтаксисе обозначение регистра может начинаться с символа «R» или «E» (например, «%eax» или «RAX»).

Включаем режим псевдографики (рис. Рисунок 2.13).

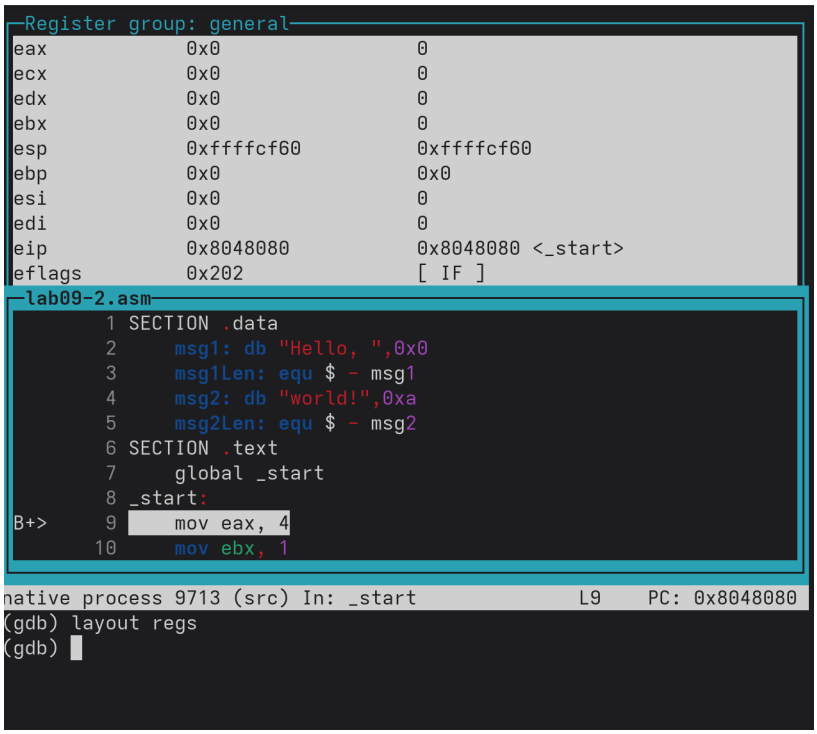

Рисунок 2.13: Включаем отображение регистров, их значений и результат дисассимилирования программы

Проверяем была ли установлена точка останова и устанавливаем точку останова предпоследней инструкции (рис. Рисунок 2.14).

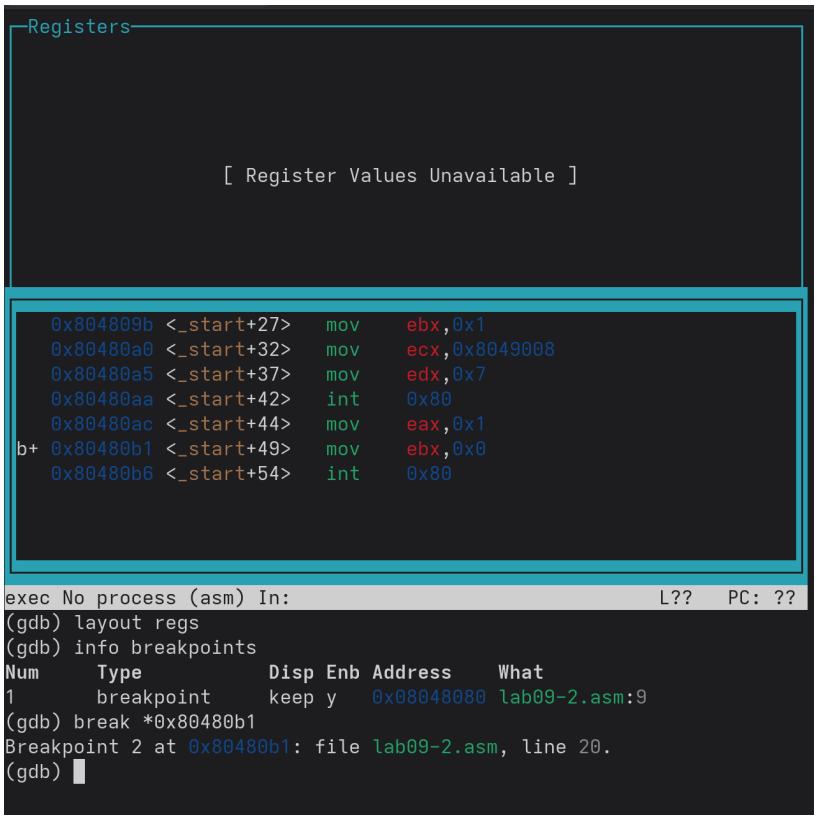

Рисунок 2.14: Используем команду info breakpoints и создаем новую точку останова

Посмотрим информацию о всех установленных точках останова (рис. Рисунок 2.15).

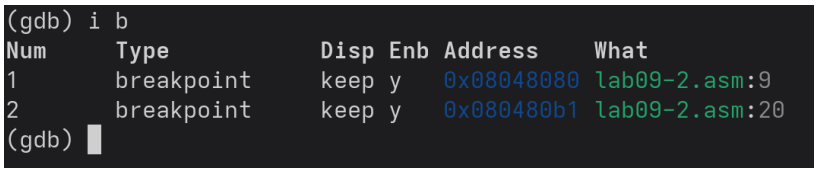

Рисунок 2.15: Смотрим информацию

Выполняем 5 инструкций командой si (рис. Рисунок 2.16).

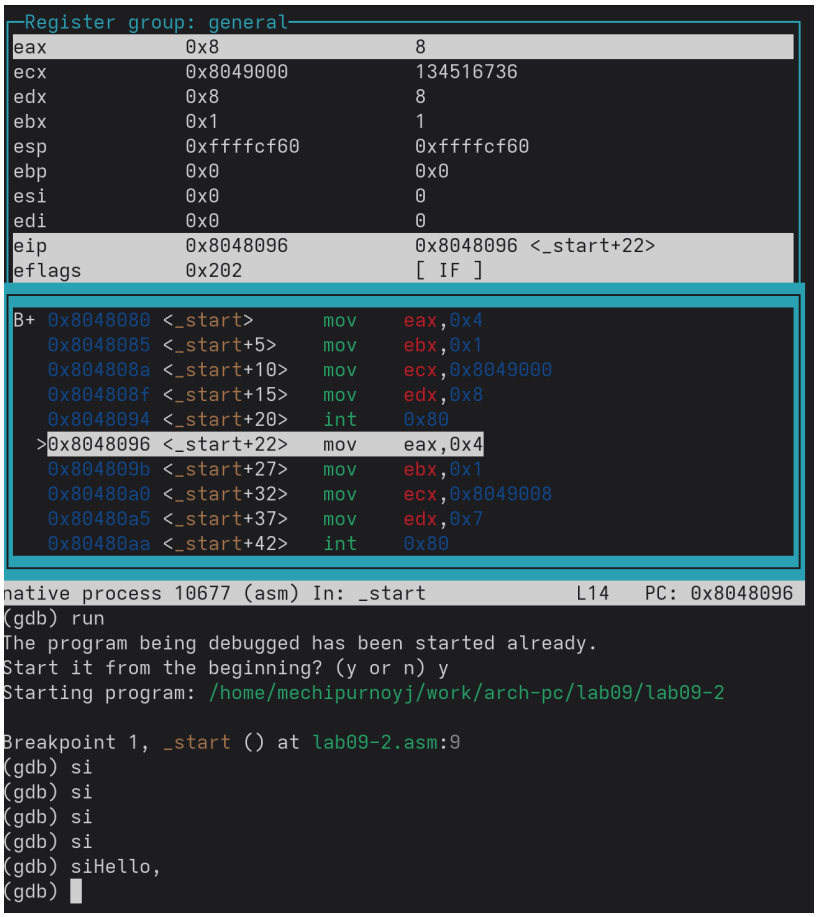

Рисунок 2.16: Отслеживаем регистры

Во время выполнения команд менялись регистры: ebx, ecx, edx,eax, eip.

Смотрим значение переменной msg1 по имени (рис. Рисунок 2.17).

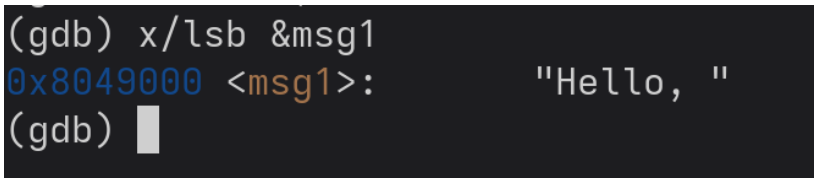

Рисунок 2.17: Смотрим значение переменной

Смотрим значение переменной msg2 по адресу (рис. Рисунок 2.18).

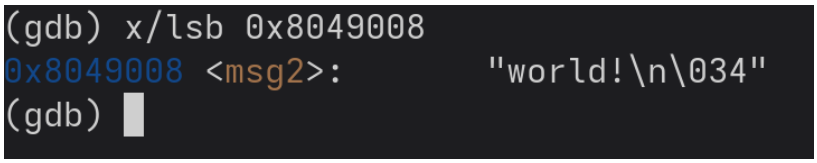

Рисунок 2.18: Смотрим значение переменной

Изменим первый символ переменной msg1 (рис. Рисунок 2.19).

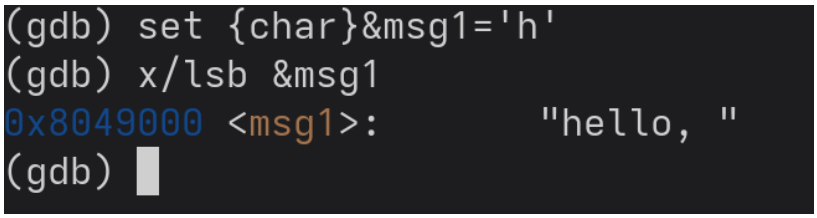

Рисунок 2.19: Меняем символ

Изменим первый символ переменной msg2 (рис. Рисунок 2.20).

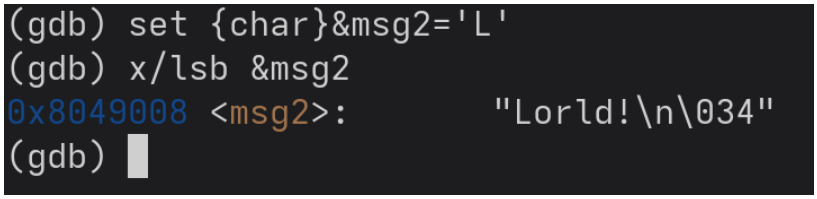

Рисунок 2.20: Меняем символ

Смотрим значение регистра edx в разных форматах (рис. Рисунок 2.21).

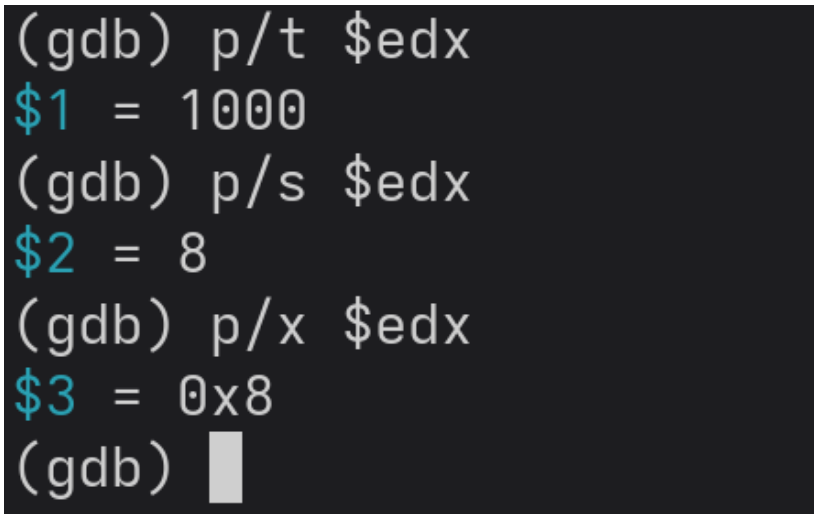

Рисунок 2.21: Смотрим значение регистра

Изменяем регистор ebx (рис. Рисунок 2.22).

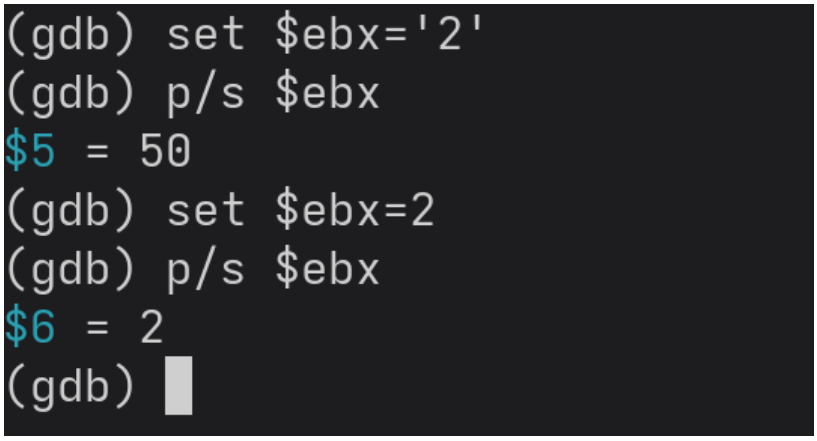

Рисунок 2.22: Изменяем регистор командой set

Выводится разные значения, так как команда без кеавычек присваивает регистру вводимое значение.

Прописываем команды для завершения программы и выхода из GDB (рис. Рисунок 2.23).

```
(gdb) cLorld!

Continuing.

Breakpoint 2, _start () at lab09-2.asm:20
(gdb)
```

Рисунок 2.23: Прописываем команды с и quit

Копируем файл lab8-2.asm в файл с именем lab09-3.asm (рис. Рисунок 2.24).

```
mechipurnoyj@fedora:~/work/arch-pc/lab09$ cp ~/work/arch-pc/lab08/lab8
-2.asm ~/work/arch-pc/lab09/lab09-3.asm
mechipurnoyj@fedora:~/work/arch-pc/lab09$
```

Рисунок 2.24: Копируем файл

Создаем исполняемый файл и запускаем его в отладчике GDB (рис. Рисунок 2.25).

```
mechipurnoyj@fedora:~/work/arch-pc/lab09$ nasm -f elf -g -l lab09-3.ls
t lab09-3.asm
mechipurnoyj@fedora:~/work/arch-pc/lab09$ ld -m elf_i386 -o lab09-3 la
b09-3.o
mechipurnoyj@fedora:~/work/arch-pc/lab09$ gdb --args lab09-3 2 3 '5'
GNU gdb (Fedora Linux) 16.2-3.fc42
Copyright (C) 2024 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gp
l.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-redhat-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
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 lab09-3...
(gdb)
```

Рисунок 2.25: Создаем и запускаем в отладчике файл

Установим точку останова перед первой инструкцией в программе и запустим ее (рис. Рисунок 2.26).

```
(gdb) b _start
Breakpoint 1 at 0x8048148: file lab09-3.asm, line 7.
(gdb) run
Starting program: /home/mechipurnoyj/work/arch-pc/lab09/lab09-3 2 3 5

This GDB supports auto-downloading debuginfo from the following URLs:
  <https://debuginfod.fedoraproject.org/>
Enable debuginfod for this session? (y or [n]) y
Debuginfod has been enabled.
To make this setting permanent, add 'set debuginfod enabled on' to .gd
binit.

Breakpoint 1, _start () at lab09-3.asm:7
7           pop ecx
(gdb) x/x $esp
0xffffcf70:     0x00000004
(gdb)
```

Рисунок 2.26: Устанавливаем точку останова

Смотрим позиции стека по разным адресам (рис. Рисунок 2.27).

```
(gdb) x/s *(void**)($esp + 4)
0xffffd14c:     "/home/mechipurnoyj/work/arch-pc/lab09/lab09-3"
(gdb) x/s *(void**)($esp + 8)
0xffffd17a:     "2"
(gdb) x/s *(void**)($esp + 12)
0xffffd17c:     "3"
(gdb) x/s *(void**)($esp + 16)
0xffffd17e:     "5"
(gdb) x/s *(void**)($esp + 20)
0x0:    <error: Cannot access memory at address 0x0>
(gdb)
```

Рисунок 2.27: Изучаем полученные данные

Шаг изменения адреса равен 4 потому что адресные регистры имеют размерность 32 бита(4 байта).

2.3 Задание для самостоятельной работы

2.3.1 Задание 1

Копируем файл lab8-4.asm(ср №1 в ЛБ8) в файл с именем lab09-3.asm (рис. Рисунок 2.28).

```
mechipurnoyj@fedora:~/work/arch-pc/lab09$ cp ~/work/arch-pc/lab08/lab8
-4.asm ~/work/arch-pc/lab09/lab09-4.asm
mechipurnoyj@fedora:~/work/arch-pc/lab09$
```

Рисунок 2.28: Копируем файл

Открываем файл в Midnight Commander и меняем его, создавая подпрограмму (рис. Рисунок 2.29).

```
lab09-4.asm       [-M--] 16 L:[  1+22  23/ 38] *(265 / 446b) 0010 0x00A
%include "in_out.asm"

SECTION .data
msg db "Результат: ",0

SECTION .bss
prm: resb 80

SECTION .text
global _start

_start:
    pop ecx
    pop edx
    sub ecx, 1
    mov esi, 0

next:
    cmp ecx, 0h
    jz _end
    pop eax
    call atoi
    call _calcul
    add esi, eax
    loop next

_end:
    mov eax, msg
    call sprint
    mov eax, esi
    call iprintLF
    call quit

_calcul:
    sub eax, 1
    mov ebx, 10
    mul ebx
    ret
```

Рисунок 2.29: Изменяем файл

Создаем исполняемый файл и запускаем его (рис. Рисунок 2.30).

```
mechipurnoyj@fedora:~/work/arch-pc/lab09$ nasm -f elf lab09-4.asm
mechipurnoyj@fedora:~/work/arch-pc/lab09$ ld -m elf_i386 -o lab09-4 la
b09-4.o
mechipurnoyj@fedora:~/work/arch-pc/lab09$ ./lab09-4 10 9 3
Результат: 190
mechipurnoyj@fedora:~/work/arch-pc/lab09$
```

Рисунок 2.30: Проверяем работу программы

2.3.2 Задание 2

Создаем новый файл в дирректории (рис. Рисунок 2.31).

```
mechipurnoyj@fedora:~/work/arch-pc/lab09$ touch lab09-5.asm
mechipurnoyj@fedora:~/work/arch-pc/lab09$
```

Рисунок 2.31: Создаем файл

Открываем файл в Midnight Commander и заполняем его в соответствии с листингом 9.3 (рис. Рисунок 2.32).

```
lab09-5.asm        [-M--] 13 L:[  1+20  21/ 21] *(295 / 295b) <EOF>
%include 'in_out.asm'

SECTION .data
div: DB 'Результат: ',0

SECTION .text
GLOBAL _start

_start:
    mov ebx, 3
    mov eax, 2
    add ebx, eax
    mov ecx, 4
    mul ecx
    add ebx, 5
    mov edi, ebx
    mov eax, div
    call sprint
    mov eax, edi
    call iprintLF
    call quit
```

Рисунок 2.32: Изменяем файл

Создаем исполняемый файл и запускаем его (рис. Рисунок 2.33).

```
mechipurnoyj@fedora:~/work/arch-pc/lab09$ nasm -f elf lab09-5.asm
mechipurnoyj@fedora:~/work/arch-pc/lab09$ ld -m elf_i386 -o lab09-5 la
b09-5.o
mechipurnoyj@fedora:~/work/arch-pc/lab09$ ./lab09-5
Результат: 10
mechipurnoyj@fedora:~/work/arch-pc/lab09$
```

Рисунок 2.33: Создаем и смотрим на работу программы(работает неправильно)

Создаем исполняемый файл и запускаем его в отладчике GDB и смотрим на изменение решистров командой si (рис. Рисунок 2.34).

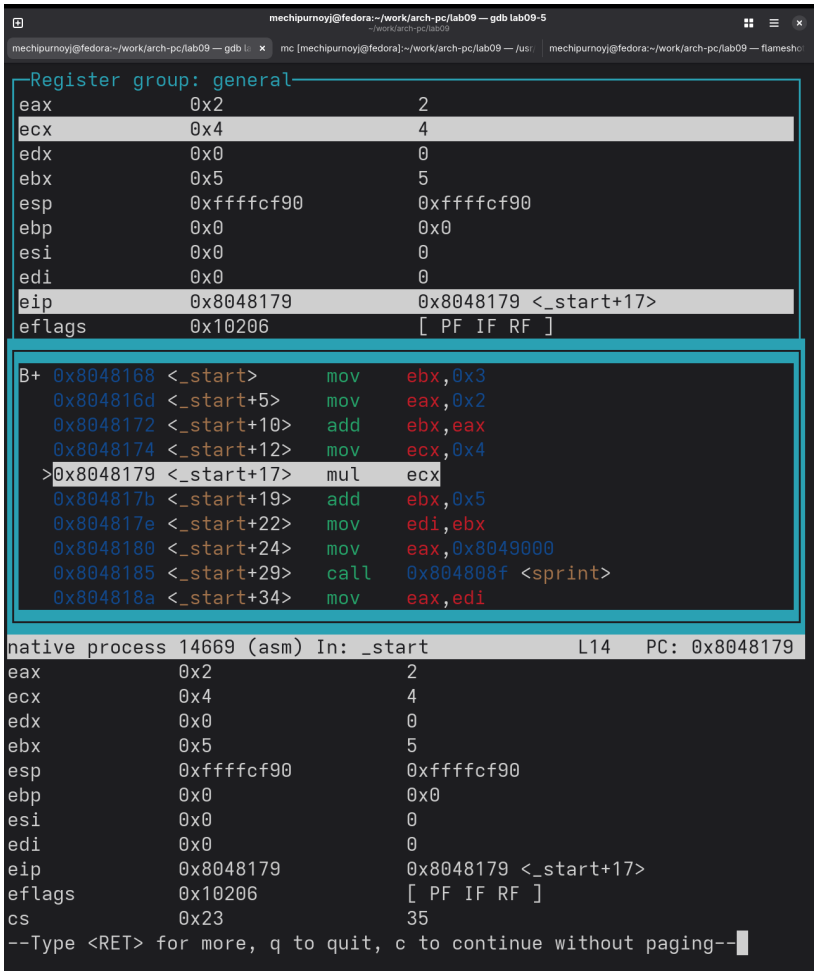

Рисунок 2.34: Ищем ошибку регистров в отладчике

Изменяем программу для корректной работы (рис. Рисунок 2.35).

```
lab09-5.asm          [-M--] 16 L:[  1+18  19/ 21] *(263 / 295b) 0010 0x00A
%include 'in_out.asm'

SECTION .data
div: DB 'Результат: ',0

SECTION .text
GLOBAL _start

_start:
    mov eax, 3
    mov ebx, 2
    add eax, ebx
    mov ecx, 4
    mul ecx
    add eax, 5
    mov edi, eax
    mov eax, div
    call sprint
    mov eax, edi
    call iprintLF
    call quit
```

Рисунок 2.35: Меняем файл

Создаем исполняемый файл и запускаем его (рис. Рисунок 2.36).

```
mechipurnoyj@fedora:~/work/arch-pc/lab09$ nasm -f elf lab09-5.asm
mechipurnoyj@fedora:~/work/arch-pc/lab09$ ld -m elf_i386 -o lab09-5 lab09-5.o
mechipurnoyj@fedora:~/work/arch-pc/lab09$ ./lab09-5
Результат: 25
mechipurnoyj@fedora:~/work/arch-pc/lab09$
```

Рисунок 2.36: Создаем и запускаем файл(работает корректно)

3 Выводы

Мы познакомились с методами отладки при помощи GDB и его возможностями.