ØVELSE 3

DAT103

Magnus Ødegård Bergersen (181182) & Søren Johan Schnitler (138168)

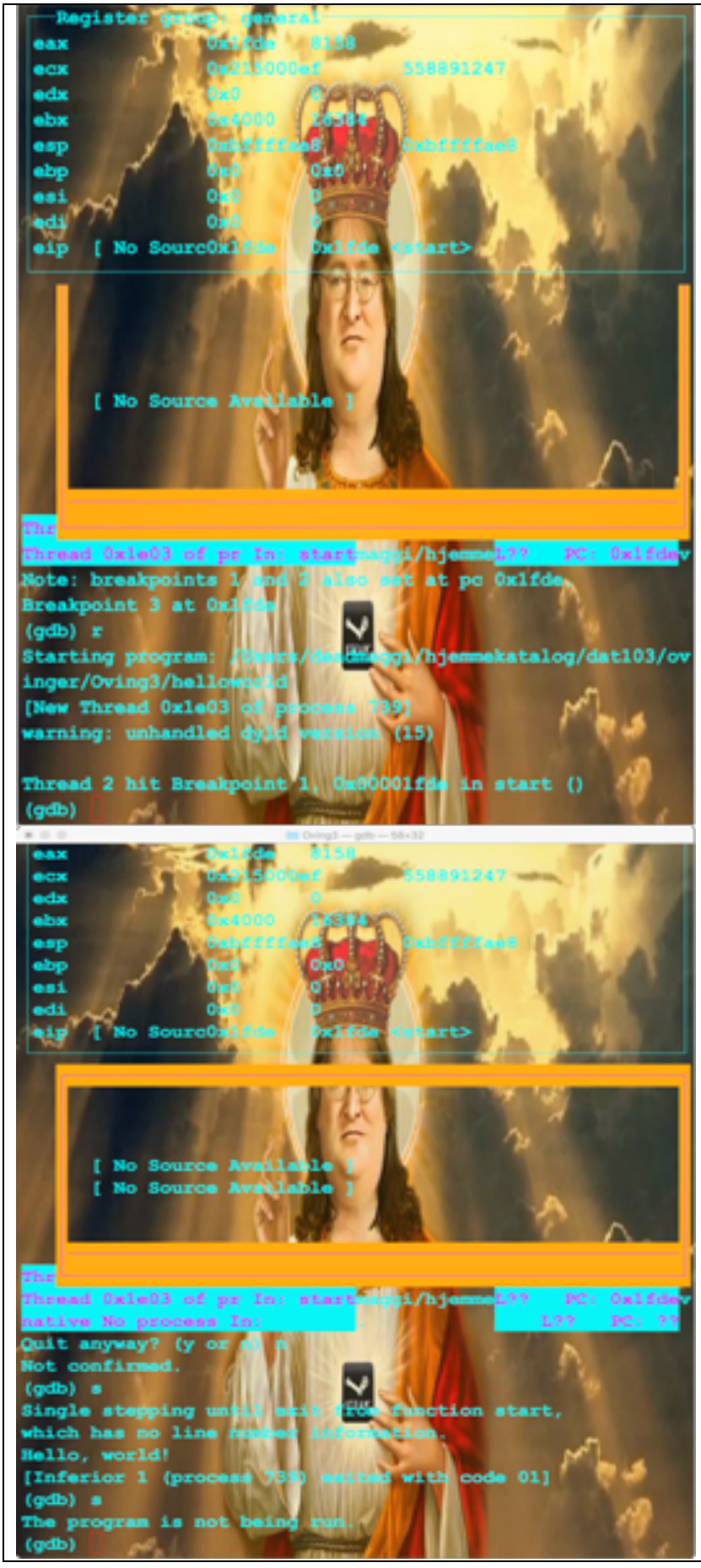
Table of Contents

Oppgave 1

```
global start

section .text
start:
        push dword msg.len
        push dword msg
        push dword 1
        mov eax, 4
        sub esp, 4
        int     0x80
        add esp, 16

        push dword 0
        mov eax, 1
        sub esp, 12
        int 0x80

section .data

msg:    db      "Hello, world!", 10
.len    equ     $ - msg
```

Kode skrevet for macOS.

```
#vim helloworld.asm

#nasm -f macho32 helloworld.asm
(macho32 er macOS sin versjon av elf)

#ld -macosx_version_min 10.7.0 -lSystem -o helloworld helloworld.o

#./helloworld
Hello, world!

#gdb

#tui enable

#layout reg

#b start
(Må starte på start og ikke _start ettersom macOS akseptere ikke understrek før navn)

#r

#s -> enter enter enter
```


Register group: general
eax 0x1fde 8158
ecx 0x215000ef 558891247
edx 0x0 0
ebx 0x4000 16384
esp 0xbffffae8 0xbffffae8
ebp 0x0 0x0
esi 0x0 0
edi 0x0 0
eip [No Source 0x1fde 0x1fde <start>
[No Source Available]
Thread 0x1e03 of pr In: start L?? PC: 0x1fde
Note: breakpoints 1 and 2 also set at pc 0x1fde.
Breakpoint 3 at 0x1fde
(gdb) r
Starting program: /Users/deathegyi/hjemmekatalog/dat103/oving/Oving3/hellowworld
[New Thread 0x1e03 of process 739]
warning: unhandled dyld version (15)
Thread 2 hit Breakpoint 1, 0x00001fde in start ()
(gdb)
[No Source Available]
[No Source Available]
Quit anyway? (y or n) n
Not confirmed.
(gdb) s
Single stepping until exit from function start,
which has no line number information.
Hello, world!
[Inferior 1 (process 739) exited with code 01]
(gdb) s
The program is not being run.
(gdb)

Oppgave 2

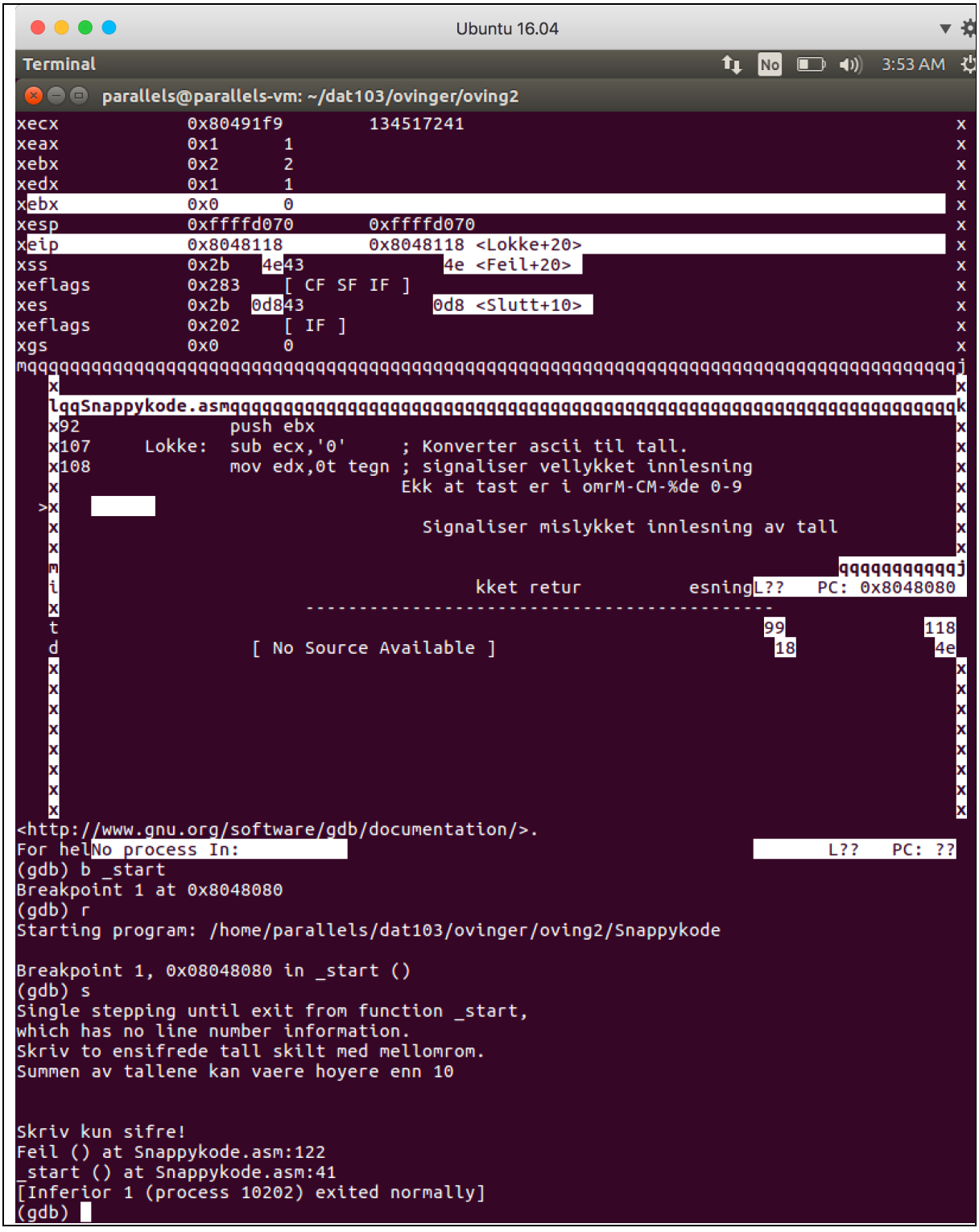
```
; Inndata Programmet leser inn to sifre skilt med ett eller flere mellomrom
; Utdata Programmet skriver ut summen av de to sifrene,
; forutsatt at summen er mindre enn 10.
; Konstanter
        cr equ 13 ; Vognretur
        lf equ 10 ; Linjeskift
        SYS_EXIT equ 1
        SYS_READ equ 3
        SYS_WRITE equ 4
        STDIN equ 0
        STDOUT equ 1
        STDERR equ 2
; Datasegment
        section .bss
                siffer resb 4
; Datasegment
        section .data
                meld db "Skriv to ensifrede tall skilt med mellomrom.",cr,lf
                db "Summen av tallene kan vaere hoyere enn 10",cr,lf
                meldlen equ $ - meld
                feilmeld db cr,lf, "Skriv kun sifre!",cr,lf
                feillen equ $ - feilmeld
                crlf db cr,lf
                crlflen equ $ - crlf

; Kodesegment med program
section .text
global _start


_start:
        mov edx,meldlen
        mov ecx,meld
        mov ebx,STDOUT
        mov eax,SYS_WRITE
        int 80h

 ; Les tall, innlest tall returneres i ecx
 ; Vellykket retur dersom edx=0
 call lessiffer
 cmp edx,0 ; Test om vellykket innlesning
 jne Slutt ; Hopp tilavslutning ved feil i innlesing
 mov eax,ecx ; Første tall/siffer lagres i reg eax
 call lessiffer
```

```
 ; Les andre tall/siffer
 ; vellykket: edx=0, tall i ecx
 cmp edx,0 ;Test om vellykket innlesning
 jne Slutt
 mov ebx,ecx ; andre tall/siffer lagres i reg ebx

 call nylinje
 add eax,ebx
 mov ecx,eax

 cmp ecx,10
 jge beregns

 cmp ecx,9
 jle beregnm


 call skrivsiffer ; Skriv ut verdi i ecx som ensifret tall

Slutt:
        mov eax,SYS_EXIT
        mov ebx,0
        int 80h
; ------------------------------------------------------
skrivsiffer:
        ; Skriver ut sifferet lagret i ecx. Ingen sjekk på verdiområde.
        push eax
        push ebx
        push ecx
        push edx
        add ecx,'0' ; converter tall til ascii.
        mov [siffer],ecx
        mov ecx,siffer
        mov edx,1
        mov ebx,STDOUT
        mov eax,SYS_WRITE
        int 80h
        pop edx
        pop ecx
        pop ebx
        pop eax
        ret
; ------------------------------------------------------
lessiffer:
        ; Leter forbi alle blanke til neste ikke-blank
        ; Neste ikke-blank returneres i ecx
        push eax
```

```
        push ebx
Lokke:
        ; Leser et tegn fra tastaturet
        mov eax,3
        mov ebx,0
        mov ecx,siffer
        mov edx,1
        int 80h
        mov ecx,[siffer]
        cmp ecx,' '
        je Lokke
        cmp ecx,'0' ; Sjekk at tast er i område 0-9
        jb Feil
        cmp ecx,'9'
        ja Feil
        sub ecx,'0'     ; Konverter ascii til tall.
        mov edx,0       ; signaliser vellykket innlesning
        pop ebx
        pop eax
        ret             ; Vellykket retur

Feil:
        mov edx,feillen
        mov ecx,feilmeld
        mov ebx,STDERR
        mov eax,SYS_WRITE
        int 80h
        mov edx,1       ; Signaliser mislykket innlesning av tall
        pop ebx
        pop eax
        ret             ; Mislykket retur
; ------------------------------------------------------------
; Flytt cursor helt til venstre på neste linje
nylinje:
        push eax
        push ebx
        push ecx
        push edx
        mov edx,crlflen
        mov ecx,crlf
        mov ebx,STDOUT
        mov eax,SYS_WRITE
        int 80h
        pop edx
        pop ecx
        pop ebx
        pop eax
```

```
        ret

beregns:
        mov ecx,1
        call skrivsiffer
        sub eax,10
        mov ecx,eax
        call skrivsiffer
        call nylinje
        pop ecx
        call Slutt
        beregnm:
        call skrivsiffer
        call Slutt

; End _start
```

```
#gedit
(Kode skrevet i gedit)

# nasm -f elf -F dwarf -g Snappykode.asm

# ld -m elf_i386 -o Snappykode Snappykode.o

./Snappykode

Skriv to ensifrede tall skilt med mellomrom.
Summen av tallene kan vaere hoyere enn 10
87

15

#gdb –tui Snappykode
#layout regs
#b _start
#r
#s
```


Ubuntu 16.04
Terminal
3:53 AM
parallels@parallels-vm: ~/dat103/ovinger/oving2
xecx 0x80491f9 134517241
xeax 0x1 1
xebx 0x2 2
xedx 0x1 1
xebx 0x0 0
xesp 0xffffd070 0xffffd070
xeip 0x8048118 0x8048118 <Lokke+20>
xss 0x2b 4e43 4e <Feil+20>
xeflags 0x283 [CF SF IF]
xes 0x2b 0d843 0d8 <Slutt+10>
xeflags 0x202 [IF]
xgs 0x0 0
lqqSnappykode.asm
x92 push ebx
x107 Lokke: sub ecx,'0' ; Konverter ascii til tall.
x108 mov edx,0t tegn ; signaliser vellykket innlesning
Ekk at tast er i omrM-CM-%de 0-9
Signaliser mislykket innlesning av tall
kket retur esningL?? PC: 0x8048080
[No Source Available]
99 118
18 4e
<http://www.gnu.org/software/gdb/documentation/>.
For helNo process In: L?? PC: ??
(gdb) b _start
Breakpoint 1 at 0x8048080
(gdb) r
Starting program: /home/parallels/dat103/ovinger/oving2/Snappykode
Breakpoint 1, 0x08048080 in _start ()
(gdb) s
Single stepping until exit from function _start,
which has no line number information.
Skriv to ensifrede tall skilt med mellomrom.
Summen av tallene kan vaere hoyere enn 10
Skriv kun sifre!
Feil () at Snappykode.asm:122
_start () at Snappykode.asm:41
[Inferior 1 (process 10202) exited normally]
(gdb)

Oppgave 3

```
        ; Konstanter

        SYS_WRITE equ 4
        SYS_EXIT equ 1
        STDOUT equ 1
section .bss
        buffer resb 1

section .text

global _start
_start:

        mov ecx, 0 ;Lokkeantall
        mov eax, 0 ;Variabel a
        call lokke



exit:

        mov edx,1 ;Lengde
        mov ecx,eax ; Skriv ut variable a
        add ecx,'0' ;Convert Ascii
        mov [buffer],ecx
        mov ecx,buffer
        mov ebx,STDOUT
        mov eax,SYS_WRITE
        int 80h ;Call Kernel

        mov eax,SYS_EXIT
        mov ebx,0
        int 80h

lokke:
        cmp ecx, 20
        jz exit

        cmp ecx, 10 ;Test om mindre enn 10
        jb Under
        cmp ecx, 10 ;Test om storre enn 10
        jae Over
;       cmp ecx, 0
;       jz lokke
;       ret
```

```
Under:
        add eax, 1
        add ecx, 1
        jmp lokke


Over:
        sub eax, 1
        add ecx, 1
        jmp lokke
```

```
# nasm -f elf -F dwarf -g lokke.asm

# ld -m elf_i386 -o lokke lokke.o

./lokke
0

#gdb –tui lokke
#layout regs
#b _start
#r
#s
```

```
Ubuntu 16.04
Terminal                                                          3:57 AM
parallels@parallels-vm: ~/dat103/ovinger/oving2
lqqRegister group: generalqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
xeax           0x1      1                                                     x
xecx           0x80490dc        134516956                                     x
xedx           0x1      1                                                     x
xebx           0x0      0                                                     x
xesp           0xffffd06c       0xffffd06c                                    x
xebp           0x0      0x0                                                   x
xesi           0x0      0                                                     x
xedi           0x0      0                                                     x
xeip           0x80480ba        0x80480ba <exit+43>                           x
xeflags        0x206    [ PF IF ]                                             x
xcs            0x23     35                                                    x
xss            0x2b     43                                                    x
xds            0x2b     43                                                    x
xes            0x2b     43                                                    x
xfs            0x0      0                                                     x
xgs            0x0      0                                                     x
   lqqlokke.asmqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
   x35      lokke:                                                            x
   x36              cmp ecx, 20                                               x
   x37              jz exit                                                   x
   x38                                                                        x
   x39              cmp ecx, 10 ;Test om mindre enn 10                        x
   x40              jb Under                                                  x
   x41              cmp ecx, 10 ;Test om storre enn 10                        x
   x42              jae Over                                                  x
   x43      ;       cmp ecx, 0                                                x
   x44      ;       jz lokke                                                  x
   x45      ;       ret                                                       x
   x46                                                                        x
   x47                                                                        x
   x48                                                                        x
   x49                                                                        x
   x50      Under:                                                            x
   x51              add eax, 1                                                x
   mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
exec No process In:                                                L??   PC: ??
(gdb) b _start
Breakpoint 1 at 0x8048080
(gdb) r
Starting program: /home/parallels/dat103/ovinger/oving2/lokke

Breakpoint 1, 0x08048080 in _start ()
(gdb) s
Single stepping until exit from function _start,
which has no line number information.
[Inferior 1 (process 10851) exited normally]
The program is not being run.
The program is not being run.
The program is not being run.
The program is not being run.
The program is not being run.
The program is not being run.
The program is not being run.
(gdb)
```