

PRAKTIKUM SISTEM OPERASI
MODUL 3
MENGENAL CARA ‘DEBUGGING’ PROGRAM BOOTSTRAP-LOADER



Disusun Oleh :
MUHAMMAD WAHYU SYAFI'UDDIN
L200210056

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
UNIVERSITAS MUHAMMADIYAH SURAKARTA
TAHUN 2021/2022

A. Langkah – langkah

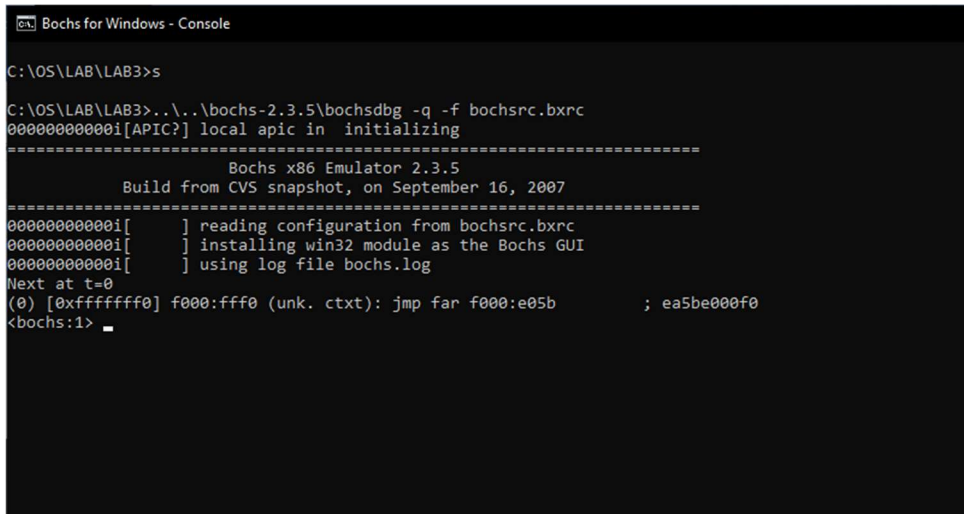
1. Masuk ke direktori LAB\LAB3



```
C:\OS\LAB\LAB3>
```

Gambar 3.1 – Direktori kerja pada CMD

2. Memulai debugging dengan memasukkan perintah “S” pada CMD

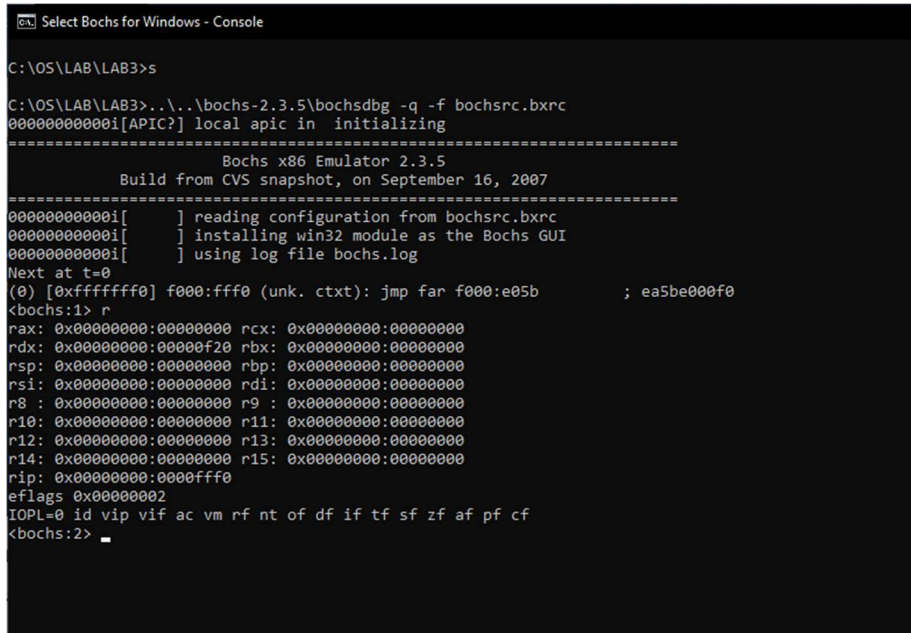


```
Bochs for Windows - Console

C:\OS\LAB\LAB3>s
C:\OS\LAB\LAB3>..\..\bochs-2.3.5\bochsdbg -q -f bochsrc.bxrc
00000000000i[APIC?] local apic in  initializing
=====
                        Bochs x86 Emulator 2.3.5
                        Build from CVS snapshot, on September 16, 2007
=====
00000000000i[      ] reading configuration from bochsrc.bxrc
00000000000i[      ] installing win32 module as the Bochs GUI
00000000000i[      ] using log file bochs.log
Next at t=0
(0) [0xffffffff] f000:fff0 (unk. ctxt): jmp far f000:e05b      ; ea5be00f0
<bochs:1> _
```

Gambar 3.2 – BOCHS saat debugging mode

3. Pada BOCHS, kondisi diatas dinamakan “Real Mode”, dan untuk melanjutkan debugging dapat memasukkan perintah “r”, lalu enter



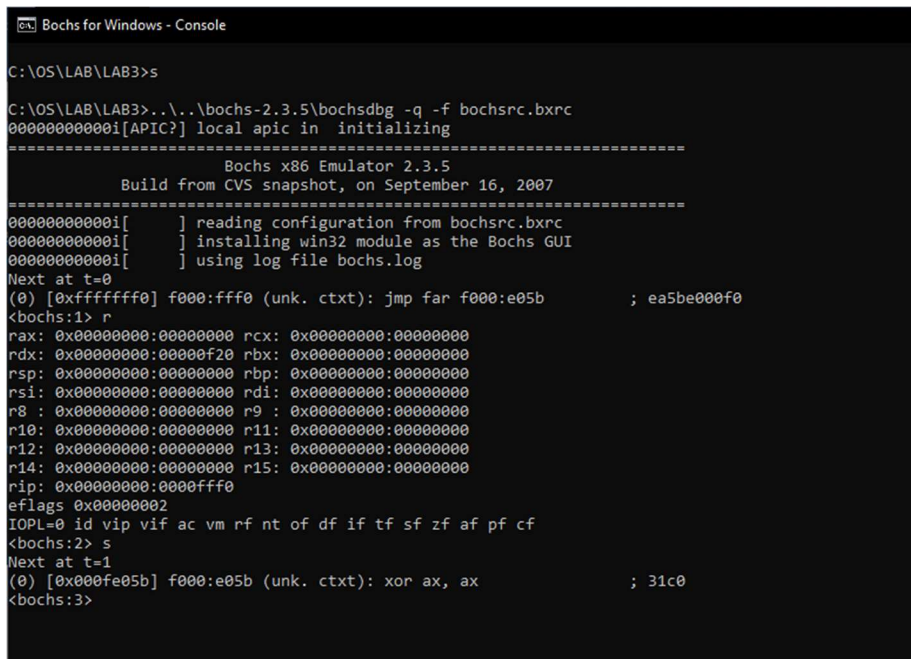
```
Select Bochs for Windows - Console

C:\OS\LAB\LAB3>s

C:\OS\LAB\LAB3>..\..\bochs-2.3.5\bochsdbg -q -f bochsrc.bxrc
0000000000i[APIC?] local apic in  initializing
=====
Bochs x86 Emulator 2.3.5
Build from CVS snapshot, on September 16, 2007
=====
0000000000i[      ] reading configuration from bochsrc.bxrc
0000000000i[      ] installing win32 module as the Bochs GUI
0000000000i[      ] using log file bochs.log
Next at t=0
(0) [0xffffffff] f000:fff0 (unk. ctxt): jmp far f000:e05b      ; ea5be00f0
<bochs:1> r
rax: 0x00000000:00000000 rcx: 0x00000000:00000000
rdx: 0x00000000:00000f20 rbx: 0x00000000:00000000
rsp: 0x00000000:00000000 rbp: 0x00000000:00000000
rsi: 0x00000000:00000000 rdi: 0x00000000:00000000
r8 : 0x00000000:00000000 r9 : 0x00000000:00000000
r10: 0x00000000:00000000 r11: 0x00000000:00000000
r12: 0x00000000:00000000 r13: 0x00000000:00000000
r14: 0x00000000:00000000 r15: 0x00000000:00000000
rip: 0x00000000:0000fff0
eflags 0x00000002
IOPL=0 id vip vif ac vm rf nt of df if tf sf zf af pf cf
<bochs:2> _
```

Gambar 3.3 – Membaca register saat debugging mode

4. Selanjutnya, untuk memberikan 1 clock ke PC, dapat menggunakan perintah “s”



```
Bochs for Windows - Console

C:\OS\LAB\LAB3>s

C:\OS\LAB\LAB3>..\..\bochs-2.3.5\bochsdbg -q -f bochsrc.bxrc
0000000000i[APIC?] local apic in  initializing
=====
Bochs x86 Emulator 2.3.5
Build from CVS snapshot, on September 16, 2007
=====
0000000000i[      ] reading configuration from bochsrc.bxrc
0000000000i[      ] installing win32 module as the Bochs GUI
0000000000i[      ] using log file bochs.log
Next at t=0
(0) [0xffffffff] f000:fff0 (unk. ctxt): jmp far f000:e05b      ; ea5be00f0
<bochs:1> r
rax: 0x00000000:00000000 rcx: 0x00000000:00000000
rdx: 0x00000000:00000f20 rbx: 0x00000000:00000000
rsp: 0x00000000:00000000 rbp: 0x00000000:00000000
rsi: 0x00000000:00000000 rdi: 0x00000000:00000000
r8 : 0x00000000:00000000 r9 : 0x00000000:00000000
r10: 0x00000000:00000000 r11: 0x00000000:00000000
r12: 0x00000000:00000000 r13: 0x00000000:00000000
r14: 0x00000000:00000000 r15: 0x00000000:00000000
rip: 0x00000000:0000fff0
eflags 0x00000002
IOPL=0 id vip vif ac vm rf nt of df if tf sf zf af pf cf
<bochs:2> s
Next at t=1
(0) [0x000fe05b] f000:e05b (unk. ctxt): xor ax, ax              ; 31c0
<bochs:3>
```

Gambar 3.4 – Memberikan 1 clock

5. Perintah “s” dapat diberikan secara terus menerus, tetapi proses Booting tidak akan cepat selesai, pada kasus ini kita akan memberikan sebuah **Breakpoints** dengan perintah “vb 0:0x7C00”, yang artinya adalah memberikan Breakpoints pada alamat 0000:7C00. Lalu selanjutnya tekan “c” untuk continue sampai ke Breakpoints

```
Bochs for Windows - Console
C:\OS\LAB\LAB3>s
C:\OS\LAB\LAB3>.\..\bochs-2.3.5\bochsrc -q -f bochsrc.bxrc
00000000000i[APIC?] local apic in initializing
=====
Bochs x86 Emulator 2.3.5
Build from CVS snapshot, on September 16, 2007
=====
00000000000i[ ] reading configuration from bochsrc.bxrc
00000000000i[ ] installing win32 module as the Bochs GUI
00000000000i[ ] using log file bochs.log
Next at t=0
(0) [0xfffffff0] f000:fff0 (unk. ctxt): jmp far f000:e05b ; ea5be00f0
<bochs:1> r
rax: 0x00000000:00000000 rcx: 0x00000000:00000000
rdx: 0x00000000:00000f20 rbx: 0x00000000:00000000
rsp: 0x00000000:00000000 rbp: 0x00000000:00000000
rsi: 0x00000000:00000000 rdi: 0x00000000:00000000
r8 : 0x00000000:00000000 r9 : 0x00000000:00000000
r10: 0x00000000:00000000 r11: 0x00000000:00000000
r12: 0x00000000:00000000 r13: 0x00000000:00000000
r14: 0x00000000:00000000 r15: 0x00000000:00000000
rip: 0x00000000:0000fff0
eflags 0x00000002
IOPL=0 id vip vif ac vm rf nt of df if tf sf zf af pf cf
<bochs:2> s
Next at t=1
(0) [0x000fa05b] f000:e05b (unk. ctxt): xor ax, ax ; 31c0
<bochs:3> vb 0:0x7c00
<bochs:4> c
(2003042265) Breakpoint 10285608, in 0000:7c00 (0x00007c00)
Next at t=2082128
(0) [0x00007c00] 0000:7c00 (unk. ctxt): jmp .+0x003b (0x00007c3e) ; e93b00
<bochs:5>
```

Gambar 3.5 – set Breakpoints dan Continue

6. Setelah sampai di Breakpoint tersebut, lanjutkan dengan memberikan 10x perintah “s” dan membandingkan hasilnya dengan boot.asm

```
Bochs for Windows - Console
<bochs:3> vb 0:0x7c00
<bochs:4> c
(2003042265) Breakpoint 10285608, in 0000:7c00 (0x00007c00)
Next at t=2082128
(0) [0x00007c00] 0000:7c00 (unk. ctxt): jmp .+0x003b (0x00007c3e) ; e93b00
<bochs:5> s
Next at t=2082129
(0) [0x00007c3e] 0000:7c3e (unk. ctxt): cli ; fa
<bochs:6> s
Next at t=2082130
(0) [0x00007c3f] 0000:7c3f (unk. ctxt): mov ax, 0x07c0 ; b8c007
<bochs:7> s
Next at t=2082131
(0) [0x00007c42] 0000:7c42 (unk. ctxt): mov ds, ax ; 8ed8
<bochs:8> s
Next at t=2082132
(0) [0x00007c44] 0000:7c44 (unk. ctxt): mov es, ax ; 8ec0
<bochs:9> s
Next at t=2082133
(0) [0x00007c46] 0000:7c46 (unk. ctxt): mov fs, ax ; 8ee0
<bochs:10> s
Next at t=2082134
(0) [0x00007c48] 0000:7c48 (unk. ctxt): mov gs, ax ; 8ee8
<bochs:11> s
Next at t=2082135
(0) [0x00007c4a] 0000:7c4a (unk. ctxt): mov ax, 0x0000 ; b80000
<bochs:12> s
Next at t=2082136
(0) [0x00007c4d] 0000:7c4d (unk. ctxt): mov ss, ax ; 8ed0
<bochs:13> s
Next at t=2082137
(0) [0x00007c4f] 0000:7c4f (unk. ctxt): mov sp, 0xffff ; bcffff
<bochs:14> s
Next at t=2082138
(0) [0x00007c52] 0000:7c52 (unk. ctxt): sti ; fb
<bochs:15>
```

Gambar 3.6 – Memberikan clock sebanyak 10x

7. Selanjutnya, mulai dari awal dan set Breakpoints ke alamat memori waktu loading Kernel, yaitu di alamat 0100:0000. Berikan perintah “vb 0x0100:0x0000”. Setelah itu, dapat memberikan perintah “s” sebanyak 10x dan membandingkan output dengan kernel.asm

Gambar 3.7 – Mengulangi proses diatas, di alamat kernel

B. Tugas

1. Buatlah tabel pemetaan memori pada PC selengkap mungkin.

Pemetaan Memori secara *Direct Mapping*

Item	Keterangan
Panjang alamat	$(s+w)$ bits
Jumlah unit yang dapat dialamati	2^{s+w} words or bytes
Ukuran Bloks sama dengan ukuran Line	2^w words or bytes
Jumlah blok memori utama	$2^s + w/2^w = 2^s$
Jumlah line di chace	$M = 2^r$
Besarnya tag	$(s - r)$ bits

Pemetaan Memori secara *Associative Mapping*

Item	Keterangan
Panjang alamat	$(s+w)$ bits
Jumlah unit yang dapat dialamati	2^{s+w} words or bytes
Ukuran Bloks sama dengan ukuran Line	2^w words or bytes
Jumlah blok memori utama	$2^s + w/2^w = 2^s$
Jumlah line di chace	Undetermined
Besarnya tag	s bits

2. Baca buku referensi, jelaskan Perbedaan antara mode kerja 'Real-Mode' dan mode kerja 'Protect-Mode' pada PC IBM Compatible.

Real Mode, adalah sebuah modus di mana prosesor Intel x86 berjalan seolaholah dirinya adalah sebuah prosesor Intel 8085 atau Intel 8088, meski ia merupakan prosesor Intel 80286 atau lebih tinggi. Karenanya, modus ini juga disebut sebagai modus 8086 (8086 Mode). Dalam modus ini, prosesor hanya dapat mengeksekusi instruksi 16-bit saja dengan menggunakan register internal yang berukuran 16-bit, serta hanya dapat mengakses hanya 1024 KB dari memori karena hanya menggunakan 20-bit jalur bus alamat. Semua program DOS berjalan pada modus ini.

Protect Mode, adalah sebuah modus di mana terdapat proteksi ruang alamat memori yang ditawarkan oleh mikroprosesor untuk digunakan oleh sistem operasi. Modus ini datang dengan mikroprosesor Intel 80286 atau yang lebih tinggi. Karena memiliki proteksi ruang alamat memori, maka dalam modus ini sistem operasi dapat melakukan multitasking.