

Foi gerado o programa de startup:

```
.section INTERRUPT_VECTOR, "x"
.global _Reset
_Reset:
    B Reset_Handler /* Reset */
    B Undefined_Handler /* Undefined */
    B . /* SWI */
    B . /* Prefetch Abort */
    B . /* Data Abort */
    B . /* reserved */
    B . /* IRQ */
    B . /* FIQ */

Reset_Handler:
    LDR sp, =svc_stack_top

    MRS r0, cpsr /* salvando o modo corrente em R0 */
    MSR cpsr_ctl, #0b11011011 /* alterando o modo para undefined - o SP é
automaticamente chaveado ao chavear o modo */
    LDR sp, =undefined_stack_top /* a pilha de undefined é setada */
    MSR cpsr, r0 /* volta para o modo anterior */

    .word 0xffffffff
    BL c_entry
    B .

Undefined_Handler:
    STMFD sp!, {r0-r12, lr}
    BL Undefined
vesaida:
    LDMFD sp!, {r0-r12, pc}^
```

Inicialmente foi executado o programa acima, e foram feitos os prints em cada etapa, observando ao fim que a função Undefined foi executada e depois o código retornou ao ponto onde estava em Reset\_Handler, onde foi chamado c\_entry:

```

Register group: general
r0      0x400001d3      1073742291    r1      0x0      0
r2      0x0      0      r3      0x0      0
r4      0x0      0      r5      0x0      0
r6      0x0      0      r7      0x0      0
r8      0x0      0      r9      0x0      0
r10     0x0      0      r11     0x0      0

startup.s
16      MRS r0, cpsr /* salvando o modo corrente em R0*/
17      MSR cpsr_ctl, #0b11011011 /* alterando o modo para undefined - o SP M-CM-) automaticamente chave
18      LDR sp, =undefined stack top /* a pilha de undefined M-CM-) setada */
> 19      MSR cpsr, r0 /* volta para o modo anterior */
20
21      .word 0xffffffff

remote Thread 1 In: Reset Handler                                Line: 19   PC: 0x30
(gdb) s
Reset_Handler () at startup.s:16
(gdb) s
(gdb) s
Reset_Handler () at startup.s:18
(gdb) s
Reset_Handler () at startup.s:19
(gdb)

```

```

Register group: general
r0      0x400001d3      1073742291    r1      0x0      0
r2      0x0      0      r3      0x0      0
r4      0x0      0      r5      0x0      0
r6      0x0      0      r7      0x0      0
r8      0x0      0      r9      0x0      0
r10     0x0      0      r11     0x0      0

startup.s
24
25      Undefined Handler:
> 26      STMFD sp!, {r0-r12,lr}
27      BL Undefined
28      LDMFD sp!, {r0-r12,pc}^
29

remote Thread 1 In: Undefined Handler                            Line: 26   PC: 0x40
(gdb) s
(gdb) s
Reset_Handler () at startup.s:18
(gdb) s
Reset_Handler () at startup.s:19
(gdb) s
Undefined_Handler () at startup.s:26
(gdb)

```

```

Register group: general
r0      0x400001d3      1073742291    r1      0x0      0
r2      0x0      0      r3      0x0      0
r4      0x0      0      r5      0x0      0
r6      0x0      0      r7      0x0      0
r8      0x0      0      r9      0x0      0
r10     0x0      0      r11     0x0      0

startup.s
20
21      .word 0xffffffff
> 22      BL c entry
23      B .
24
25      Undefined Handler:

remote Thread 1 In: Reset Handler                                Line: 22   PC: 0x38
Reset_Handler () at startup.s:19
(gdb) s
Undefined_Handler () at startup.s:26
(gdb) s
(gdb) s
(gdb) s
Reset_Handler () at startup.s:22
(gdb)

```

```

Register group: general
r0      0xe8      232
r2      0xa       10
r4      0x0       0
r6      0x0       0
r8      0x0       0
r10     0x0       0
r1      0x0       0
r3      0x0       0
r5      0x0       0
r7      0x0       0
r9      0x0       0
r11     0x0       0

startup.s
20
21      .word 0xffffffff
22      BL c_entry
> 23      B .
24
25      Undefined Handler:

remote Thread 1 In: Reset_Handler                               Line: 23  PC: 0x3c
(gdb) s
Undefined_Handler () at startup.s:26
(gdb) s
(gdb) s
(gdb) s
Reset_Handler () at startup.s:22
(gdb) n
(gdb)

```

```

sexta@bancada8:~/projects/labproc/src/e9/tarefa/src$ qemu program.bin
pulseaudio: set_sink_input_volume() failed
pulseaudio: Reason: Invalid argument
pulseaudio: set_sink_input_mute() failed
pulseaudio: Reason: Invalid argument
instrução inválida!Hello world!

```

Parando o programa antes da instrução em vesaida, foram feitos os prints a seguir:

```

Breakpoint 1, Undefined_Handler () at startup.s:27
(gdb) p ($sp+4*13)
$1 = (void *) 0x1ffc
(gdb) x/x ($sp+4*13)
0x1ffc: 0x00000038
(gdb)

```

```

$1 = (void *) 0x1ffc
(gdb) x/x ($sp+4*13)
0x1ffc: 0x00000038
(gdb) x/i {int *}($sp+4*13)
0x38 <Reset_Handler+24>:      bl      0xac <c_entry>
(gdb)

```

Isso é o esperado, pois a próxima instrução a ser executada ao sair de Undefined\_Handler é o branch para c\_entry.