

**Міністерство освіти і науки України  
Національний технічний університет України «КПІ» імені Ігоря  
Сікорського  
Кафедра обчислювальної техніки ФІОТ**

**ЗВІТ  
з лабораторної роботи №6  
з навчальної дисципліни  
«Архітектура комп'ютерів-2. Процесори»**

**Виконав:**

Студент 3 курсу кафедри  
ОТ ФІОТ,  
Навчальної групи ІВ-93  
Гуцалюк О.Б.

**Перевірив:**

Нікольський С. С.

**Київ 2021**

Hello.c

```
#include <linux/init.h>
```

```
#include <linux/module.h>
```

```
#include <linux/printk.h>
```

```
#include <linux/ktime.h>
```

```
#include <linux/slab.h>
```

```
struct head_list {  
    struct head_list *next;  
    ktime_t time;  
};
```

```
MODULE_AUTHOR("Hutsaliuk Oleh IV-93");
```

```
MODULE_DESCRIPTION("Lab6");
```

```
MODULE_LICENSE("Dual BSD/GPL");
```

```
static struct head_list *head;
```

```
static int amount = 1;
```

```
module_param(amount, uint, 0444);
```

```
MODULE_PARM_DESC(amount, "Amount Hello worlds");
```

```
static int __init helloinit(void)
```

```
{
```

```
    uint i;
```

```
    struct head_list *var_1, *var_2;
```

```
    head = kmalloc(sizeof(struct head_list *), GFP_KERNEL);
```

```
    var_1 = head;
```

```

if (amount == 0) {
    pr_warn("0 was entered, doing nothing....");
} else if (amount >= 5 && amount <= 10) {
    pr_warn("Entered parameter is between 5 and 10");
} BUG_ON(amount > 10);

for (i = 0; i < amount; i++) {
    var_1->next = kmalloc(sizeof(struct head_list), GFP_KERNEL);
    if (i == 1) var_1 = NULL;
    var_1->time = ktime_get();
    pr_info("Hello World!");
    var_2 = var_1;
    var_1 = var_1->next;
}

if (amount != 0) {
    kfree(var_2->next);
    var_2->next = NULL;
}

pr_info("Amount: %d\n", amount);

return 0;
}

static void __exit helloexit(void)
{
    struct head_list *var;

    while (head != NULL && amount != 0) {
        var = head;
    }
}

```

```
pr_info("Time: %lld", var->time);
```

```
head = var->next;
```

```
kfree(var);
```

```
}
```

```
pr_info("");
```

```
}
```

```
module_init(helloinit);
```

```
module_exit(helloexit);
```

```
langelius@langelius-Ubuntu: ~/repos/busybox
Please press Enter to activate this console.
# insmod hello.ko amount=5
15.506429 hello: loading out-of-tree module taints kernel.
15.511710 Entered parameter is between 5 and 10
15.511741 Hello World!
15.511971 Unhandled fault: page domain fault (0x1b) at 0x00000000
15.512289 pgd = (ptrval)
15.512377 [00000000] *pgd=4b049835, *pte=00000000, *ppte=00000000
15.513006 Internal error: 81b [#1] SMP ARM
15.513385 Modules linked in: hello(0+)
15.513770 CPU: 0 PID: 62 Comm: insmod Tainted: G          0 4.19.220 #1
15.513959 Hardware name: Generic DT based system
15.514641 PC is at helloinit+0xc0/0x1000 [hello]
15.514814 LR is at 0x17
15.514897 pc : [ffff000c0] lr : [000000017] psr: 900f0013
15.515058 sp : c8affdb8 ip : 00000000 fp : 00000000
15.515199 r10: 000000c0 r9 : bf0010c4 r8 : c135a34c
15.515332 r7 : 00000000 r6 : 00000000 r5 : bf0a2000 r4 : 00000002
15.515492 r3 : 00000003 r2 : d0000000 r1 : 00000003 r0 : 9bd8c710
15.515697 Flags: Nzcv IRQs on FIQs on Mode SVC_32 ISA ARM Segment none
15.515809 Control: 10c5387d Table: 4b05c06a DMC: 00000051
15.516076 Process: insmod (pid: 62, stack limit = 0x(ptrval))
15.516282 Stack: (0xc8affdb8 to 0xc8b00000)
15.516525 fdao:
15.516872 fdc0: fffff000 bf005000 00000000 c104c4b8 bf002040 c030204c c1783300 c104c4b8
15.517203 fde0: 00210d00 00000002 c104c4b8 c8b3c500 c8b8b264 c04f143c 00000000 e097afff
15.517551 fe00: ffe00000 fffff000 0040003f c8b3c3c0 d0cf03e0 d0c644ae d0cf03e0 c8b3c500
15.517878 fed0: bf002040 d0c644ae bf002040 00000002 c8bb2240 00000002 c8bb2240 c8d3d1ba
15.518211 fe40: 00000001 c03d3f04 c8afff30 c8afff30 00000002 c8bb2240 00000002 c03d3f20
15.518538 fe60: bf00204c 00007fff bf002040 c03d0d00 c8b76818 bf002088 c8b76a9c bf002234
15.518861 fe80: bf002170 c1350b18 00000000 c121f204 c121f274 c104c4b8 c100f0f4 c8ae0000
15.519185 fea0: fffff000 e0800000 c8ae9800 c8b3c500 00000000 00000000 00000000 00000000
15.519511 fec0: 00000000 00000000 0e7265b0 00006c65 00000000 00000000 00000000 00000000
15.519834 fee0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
15.520174 ffo0: 00000000 d0c644ae 00000000 00001400 00000000 e0979400 0012c050 c104c4b8
15.520499 ff20: 001b1bf8 fffff000 00000051 c03d4380 e09682a2 e0968380 e0968000 00011400
15.520783 ffa0: e0978c80 e0978aa0 e097529c 00003000 00003040 00000000 00000000 00000000
15.521092 ffb0: 0000171c 00000020 00000017 00000000 00000010 00000000 d0c644ae
15.521411 ffb0: 000f411e 001b1bf8 b0f9c950 00011400 00000080 c0301204 c8afe000 00000080
15.521724 ffa0: 000f411e c0301000 001b1bf8 b0f9c950 0011b250 00011400 001b1bf8 00000000
15.522030 ffc0: 001b1bf8 b0f9c950 00011400 00000080 00000001 bef43ea0 001086c4 000f411e
15.522336 ffe0: bef43b58 bef43b48 0001b270 b0e561b0 000f0010 0011b250 00000000 00000000
15.523358 [ffff000c0] (helloinit [hello]) from [c0302d4c] (do_one_initcall+0x54/0x208)
15.523719 [c0302d4c] (do_one_initcall) from [c03d1ba8] (do_init_module+0x45/0x224)
15.523917 [c03d1ba8] (do_init_module) from [c03d3f20] (load_module+0x2150/0x2550)
15.524151 [c03d3f20] (load_module) from [c03d4380] (sys_init_module+0x158/0x18c)
15.524364 [c03d4380] (sys_init_module) from [c0301000] (ret_fast_syscall+0x0/0x54)
15.524585 Exception stack(0xc8afffa0 to 0xc8afff00)
15.524797 ffa0: 001b1bf8 b0f9c950 0011b250 00011400 001b1bf8 00000000
15.525116 ffc0: 001b1bf8 b0f9c950 00011400 00000080 00000001 bef43ea0 001086c4 000f411e
15.525399 ffb0: bef43b58 bef43b48 0001b270 b0e561b0
15.525795 Code: e5060000 03a06000 eb4ce52 e1a07006 (elc000f8)
15.526271 ---[ end trace 74292fd3f13b5428 ]---
```

```
segmentation fault
```

```
langelius@langelius-Ubuntu: ~/repos/busybox

Please press Enter to activate this console.
# insmod hello.ko amount=5
15.506429] hello: loading out-of-tree module taints kernel.
15.511761] Entered parameter is between 5 and 10
15.511761] Hello World!
15.511971] Unhandled fault: page domain fault (0x8b) at 0x00000008
15.512289] pgd = (ptrval)
15.512277] [00000000] *pte=40b49835, *pte=00000000, *ppte=00000000
15.513006] Internal error: : 81b [0] SMP ARM
15.513395] Modules linked in: hello(0+)
15.513778] CPU: 0 PID: 62 Comm: insmod Tainted: G      0      4.19.220 #1
15.513959] Hardware name: Generic DT based system
15.514641] PC is at helloinit+0xc8/0x1000 [hello]
15.514814] LR is at 0x17
15.514897] pc : [c0050dc8] lr : [c0000017] psr: 900f0013
15.515058] sp : c0affdb8 ip : 00000000 fp : 00000000
15.515199] r10: 006000c0 r9 : bf0010c4 r8 : c135a34c
15.515332] r7 : 00000000 r6 : 00000000 r5 : bf002000 r4 : 00000002
15.515492] r3 : 00000003 r2 : d8000000 r1 : 00000003 r0 : 9bdc710
15.515697] Flags: NzCv IRQs on FIQs on Mode SVC_32 ISA ARM Segment none
15.515889] Control: 10c387d0 Table: 40b5c0ea DAC: 00000051
15.516076] Process insmod (pid: 62, stack limit = 0x(ptrval))
15.516282] Stack: (0xc0affdb8 to 0xc0b00000)
15.516525] f0a0: fffffe00 bf005000 00000000 c1604c48 bf002040 c0302d4c c1788300 c1604c48
15.516872] fdc0: fffffe00 bf005000 00000000 c1604c48 bf002040 c0302d4c c080b200 c04fa040
15.517203] fde0: 00210d00 00000002 c1604c48 c0b3c500 c0b0b204 c04f143c 00000000 e097a7ff
15.517551] fe00: ffe00000 fffff000 8040003f c0b3c3c0 d0cf03e0 ddc644ae d0cf03e0 c0b3c500
15.517878] fe20: bf002040 ddc644ae bf002040 00000002 c0b0b340 00000002 c0b0b200 c03d1ba8
15.518211] fe40: 00000001 c03d1f0e c0afff30 c0afff30 00000002 c0b0b240 00000002 c03d1f20
15.518538] fe60: bf00204c 00007fff bf002040 c03d0d00 c0b76018 bf002088 c0b76a9c bf002234
15.518861] fe80: bf002170 c1358b18 00000000 c121f204 c121f274 c1604c48 c1608f04 c0ae9800
15.519185] fea0: fffff000 e0000000 c0ae9800 c0b3c500 00000000 00000000 00000000 00000000
15.519511] fec0: 00000000 00000000 6e7255b0 00000c65 00000000 00000000 00000000 00000000
15.519834] fee0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
15.520174] ffe0: 00000000 ddc644ae 00000000 00001400 00000000 e0979400 0012c550 c1604c48
15.520499] f000: 0011b1f8 ffff0000 00000051 c03d3f20 e0908242 e0908300 e0908000 00011400
15.520783] f040: e0978c00 e0978aa8 e097529c 00003000 00003040 00000000 00000000 00000000
15.521092] f060: 0000171c 0000002d 0000002e 00000017 00000000 00000010 00000000 ddc644ae
15.521411] f080: 000f411e 0011b1f8 bf09c950 00114000 00000000 c0312104 c0afe000 00000000
15.521724] f0a0: 000f411e c0301000 0011b1f8 bf09c950 0011b250 00011400 0011b1f8 00000000
15.522030] f0c0: 0011b1f8 bf09c950 00011400 00000000 00000001 bef43ea0 001086c4 000f411e
15.522365] f0e0: bef43b58 bef43b48 0003b270 b0e501b0 d00f0010 0011b250 00000000 00000000
15.522658] [c0050dc8] (helloinit [hello]) from [c0302d4c] (do_one_initcall+0x54/0x208)
15.522719] [c0302d4c] (do_one_initcall) from [c03d1ba8] (do_init_module+0x64/0x224)
15.522917] [c03d1ba8] (do_init_module) from [c03d3f20] (load_module+0x2150/0x2450)
15.524511] [c03d3f20] (load_module) from [c03d4300] (sys_init_module+0x150/0x18c)
15.524364] [c03d4300] (sys_init_module) from [c0301000] (ret_fast_syscall+0x0/0x54)
15.524585] Exception stack(0xc0afffa8 to 0xc0afff00)
15.524997] f0a0: 0011b1f8 bf09c950 0011b250 00011400 0011b1f8 00000000
15.525116] f0c0: 0011b1f8 bf09c950 00011400 00000000 00000001 bef43ea0 001086c4 000f411e
15.525399] f0e0: bef43b58 bef43b48 0003b270 b0e501b0
15.525795] Code: e5060000 03a06000 eb4ece52 e1a07006 (e1c600f8)
15.526271] --[ end trace 74292fd3f13b5428 ]---
Segmentation fault
```

## Objdump:

```
langelius@langelius-Ubuntu: ~/AKLab/lab6

90: e3a04000    mov     r4, #0
94: e5953000    ldr     r3, [r5]
98: e1530004    cmp     r3, r4
9c: 9a00000e    bls     dc <init_module+0xd0>
a0: e3a02010    mov     r2, #16
a4: e1a0100a    mov     r1, sl
a8: e5980018    ldr     r0, [r8, #24]
ac: ebfffffe    bl      0 <kmem_cache_alloc_trace>
    if (i == 1) var_1 = NULL;
b0: e3540001    cmp     r4, #1
for (i = 0; i < amount; i++) {
b4: e2844001    add     r4, r4, #1
    var_1->next = kmalloc(sizeof(struct head_list), GFP_KERNEL);
b8: e5860000    str     r0, [r6]
    if (i == 1) var_1 = NULL;
bc: 03a06000    moveq   r6, #0
    var_1->time = ktime_get();
c0: ebfffffe    bl      0 <ktime_get>
    var_2 = var_1;
c4: e1a07006    mov     r7, r6
    var_1->time = ktime_get();
c8: e1c600f8    strd    r0, [r6, #8]
    pr_info("Hello World!");
cc: e1a00009    mov     r0, r9
d0: ebfffffe    bl      0 <prntk>
    var_1 = var_1->next;
d4: e5966000    ldr     r6, [r6]
d8: eafffffd    b       94 <init_module+0x94>
}

if (amount != 0) {
dc: e3530000    cmp     r3, #0
e0: 0a000003    beq     f4 <init_module+0xf4>
    kfree(var_2->next);
e4: e5970000    ldr     r0, [r7]
e8: ebfffffe    bl      0 <kfree>
    var_2->next = NULL;
ec: e3a03000    mov     r3, #0
f0: e5873000    str     r3, [r7]
}

pr_info("Amount: %d\n", amount);
f4: e5951000    ldr     r1, [r5]
f8: e3000000    movw    r0, #0
fc: e3400000    movt    r0, #0
100: ebfffffe    bl      0 <prntk>

return 0;
}
104: e3a00000    mov     r0, #0
108: e8bd87f0    pop     {r4, r5, r6, r7, r8, r9, sl, pc}
```

Disassembly of section .exit.text: