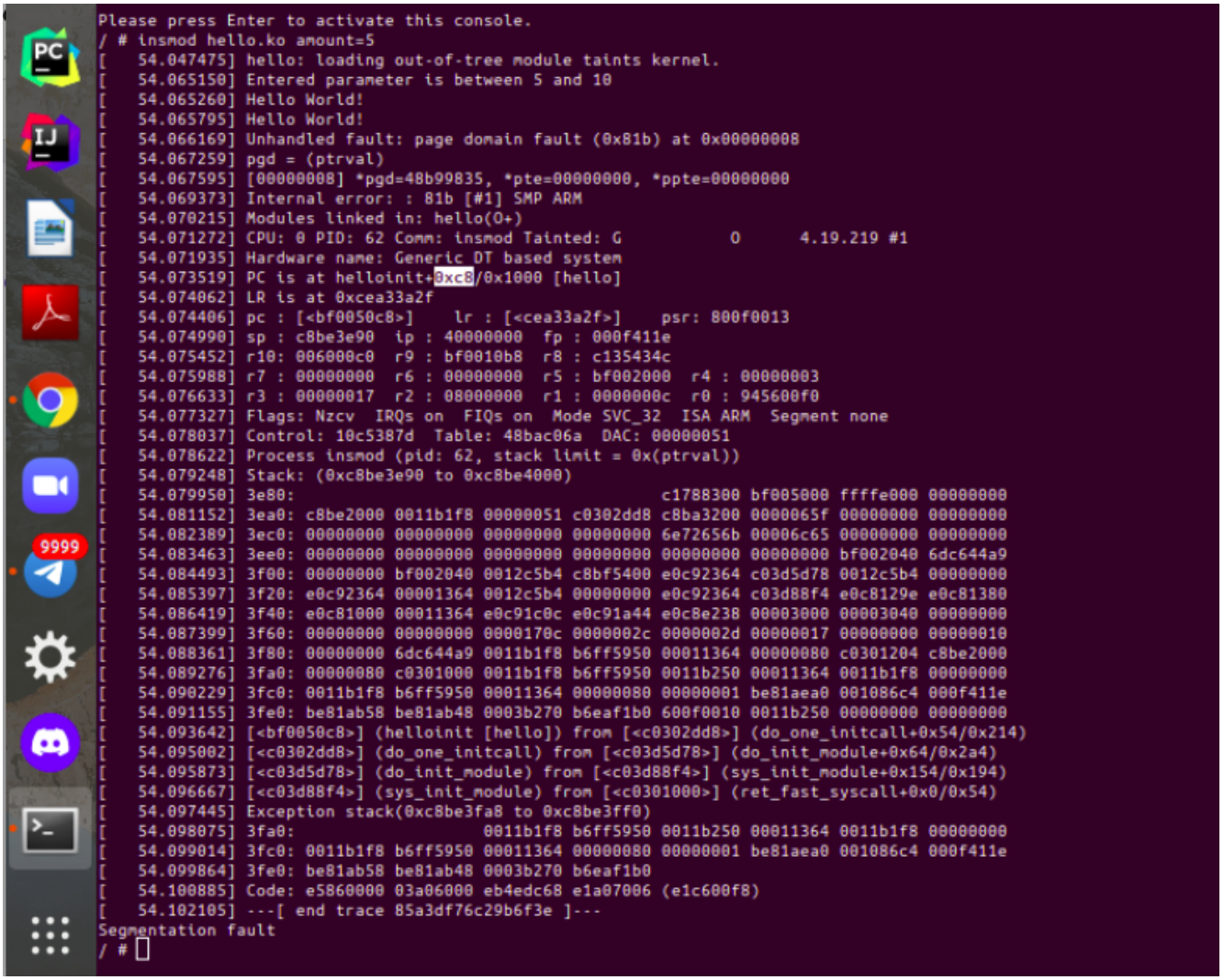
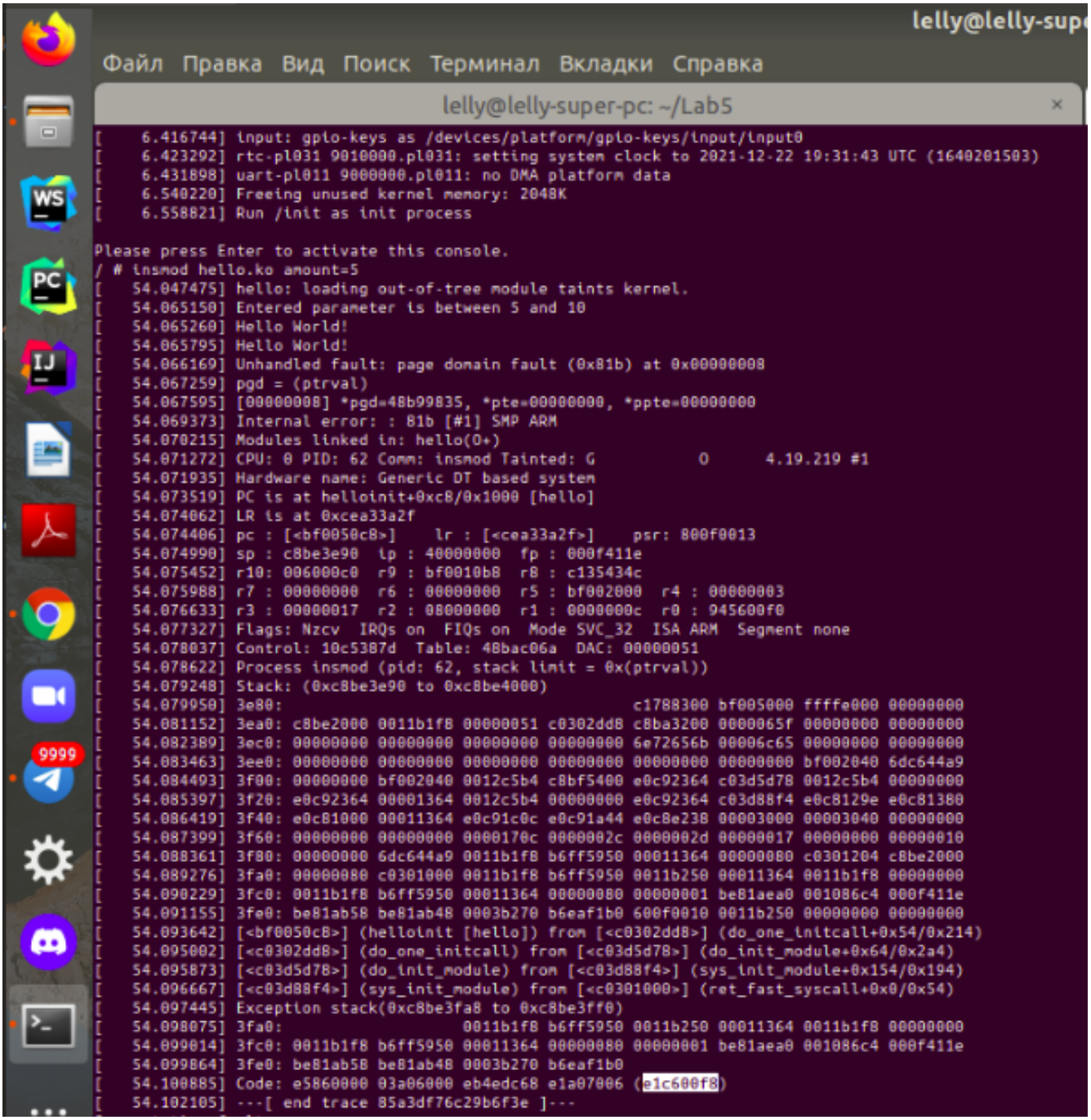
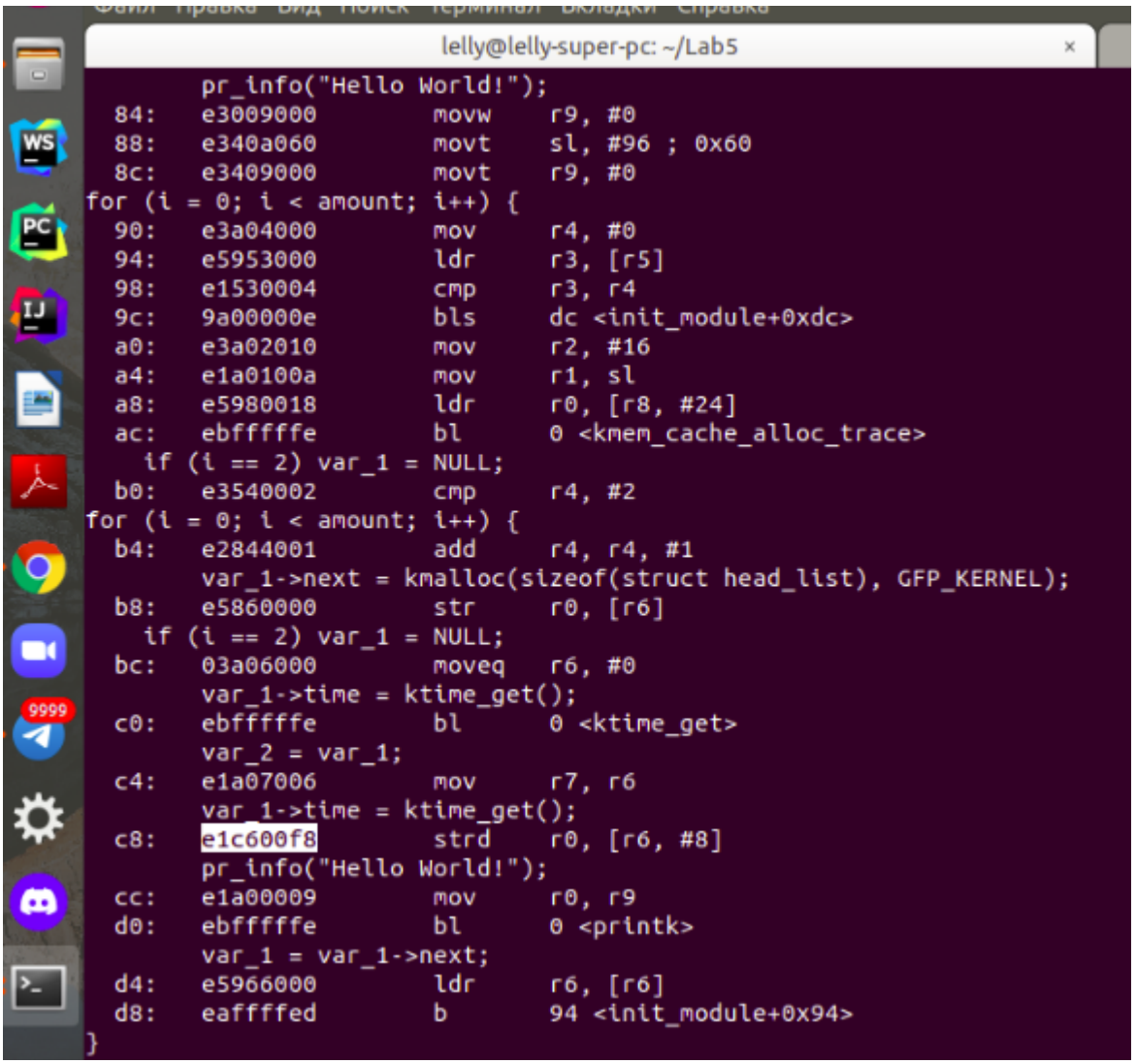
Запуск insmod з параметром amount=5 (var_1 == NULL при i = 2)





Запуск objdump:


lelly@lelly-super-pc: ~/Lab5
pr_info("Hello World!");
84: e3009000 movw r9, #0
88: e340a060 movt sl, #96 ; 0x60
8c: e3409000 movt r9, #0
for (i = 0; i < amount; i++) {
90: e3a04000 mov r4, #0
94: e5953000 ldr r3, [r5]
98: e1530004 cmp r3, r4
9c: 9a00000e bls dc <init_module+0xdc>
a0: e3a02010 mov r2, #16
a4: e1a0100a mov r1, sl
a8: e5980018 ldr r0, [r8, #24]
ac: ebffffe bl 0 <kmem_cache_alloc_trace>
if (i == 2) var_1 = NULL;
b0: e3540002 cmp r4, #2
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 == 2) var_1 = NULL;
bc: 03a06000 moveq r6, #0
var_1->time = ktime_get();
c0: ebffffe 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: ebffffe bl 0 <printk>
var_1 = var_1->next;
d4: e5966000 ldr r6, [r6]
d8: eafffed b 94 <init_module+0x94>
}