Name - KARNATI CHARAN
Roll No. - 422169
Section - A

UNIX COMMANDS AND SHELL SCRIPTING LAB

ASSIGNMENT – 04

Q). Generate different C programs that induce a segmentation fault error, select these examples of your choice, and employ the GDB utility for debugging on Linux.

1)CODE WITH ARRAY INDEX OUT OF BOUND ERROR:

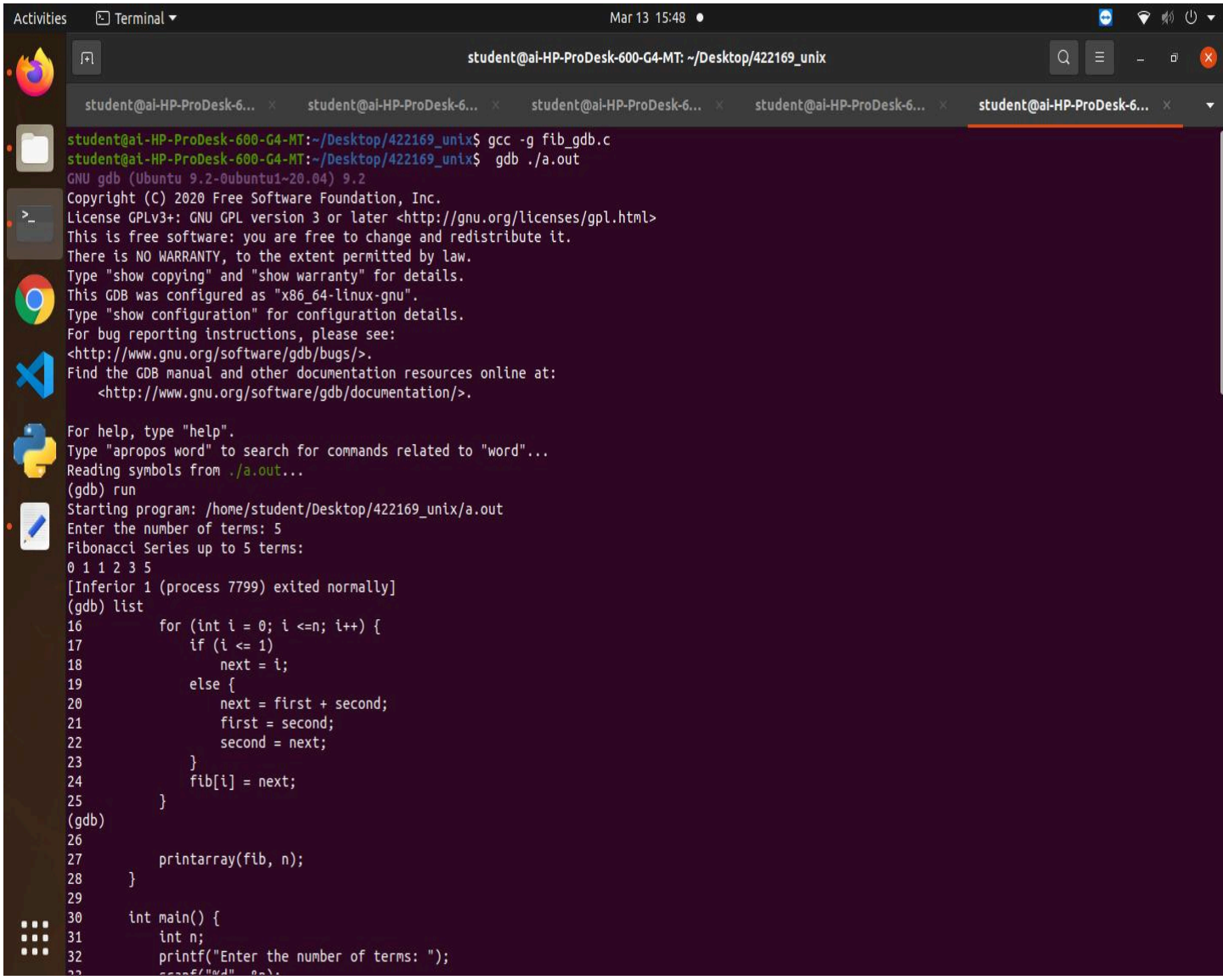
```
#include <stdio.h>

void printarray(int arr[], int size) {

    for (int i = 0; i <=size; i++) {

       //error is array index out of bounds

printf("%d ", arr[i]);

    }

    printf("\n");}

void fibonacci(int n) {

    int fib[n];

    int first = 0, second = 1, next;

    printf("Fibonacci Series up to %d terms:\n", n);



        for (int i = 0; i <=n; i++) {
```

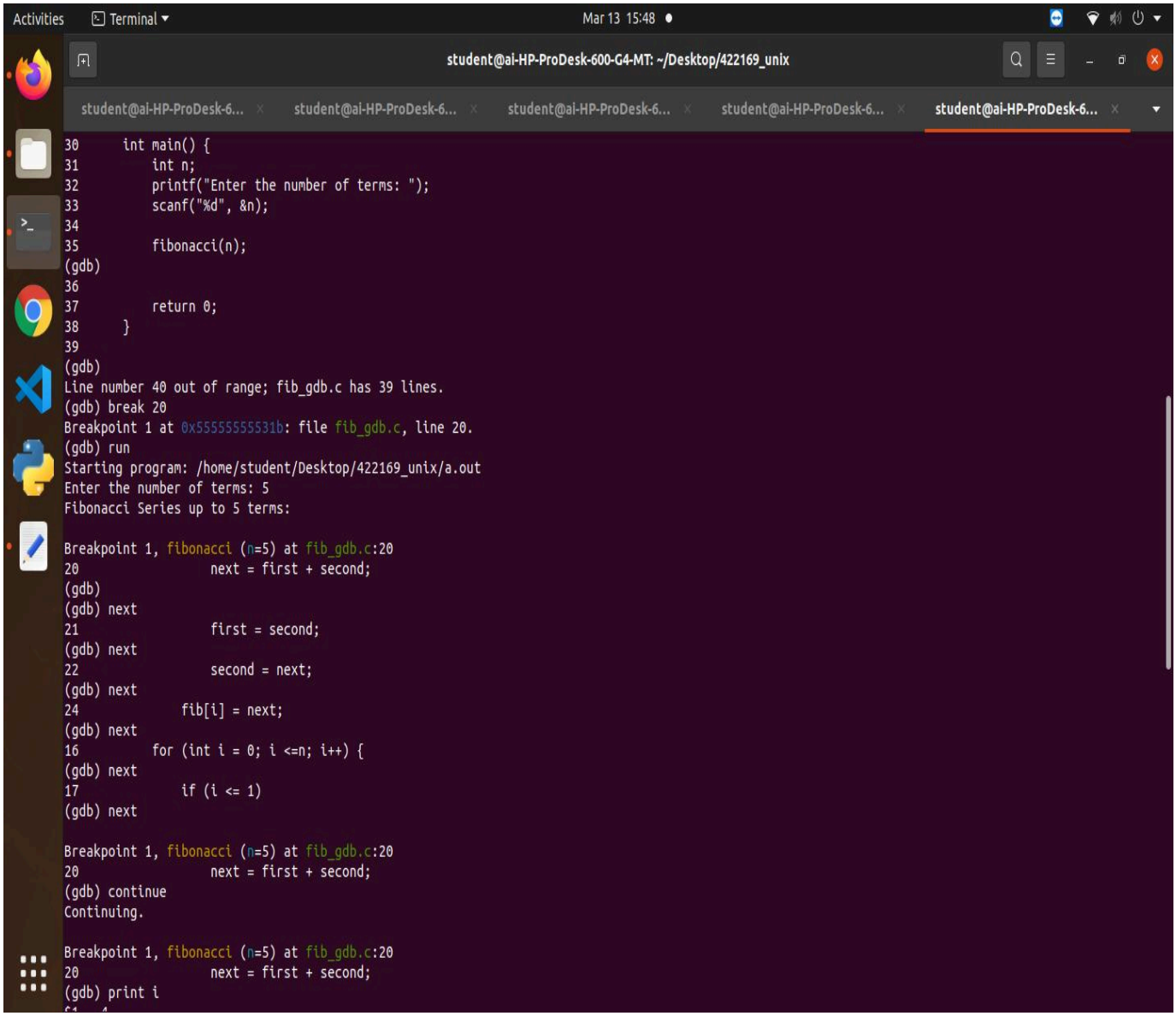
```
        if (i <= 1)
            next = i;
        else {
            next = first + second;
            first = second;
            second = next;
        }
        fib[i] = next;
    }

    printarray(fib, n);
}

int main() {
    int n;
    printf("Enter the number of terms: ");
    scanf("%d", &n);

    fibonacci(n); return 0;
}
```

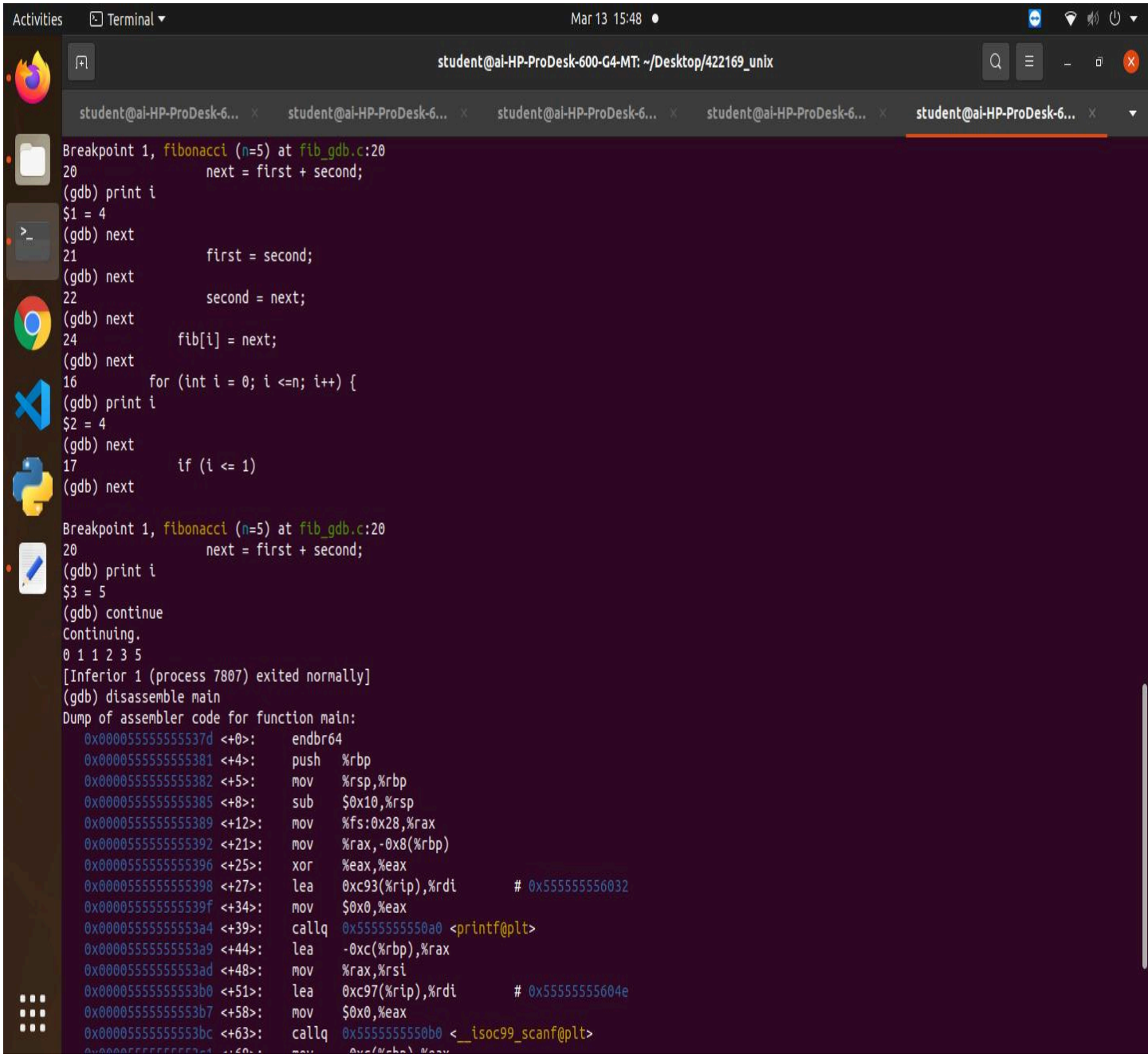
2)ANOTHER C PROGRAM

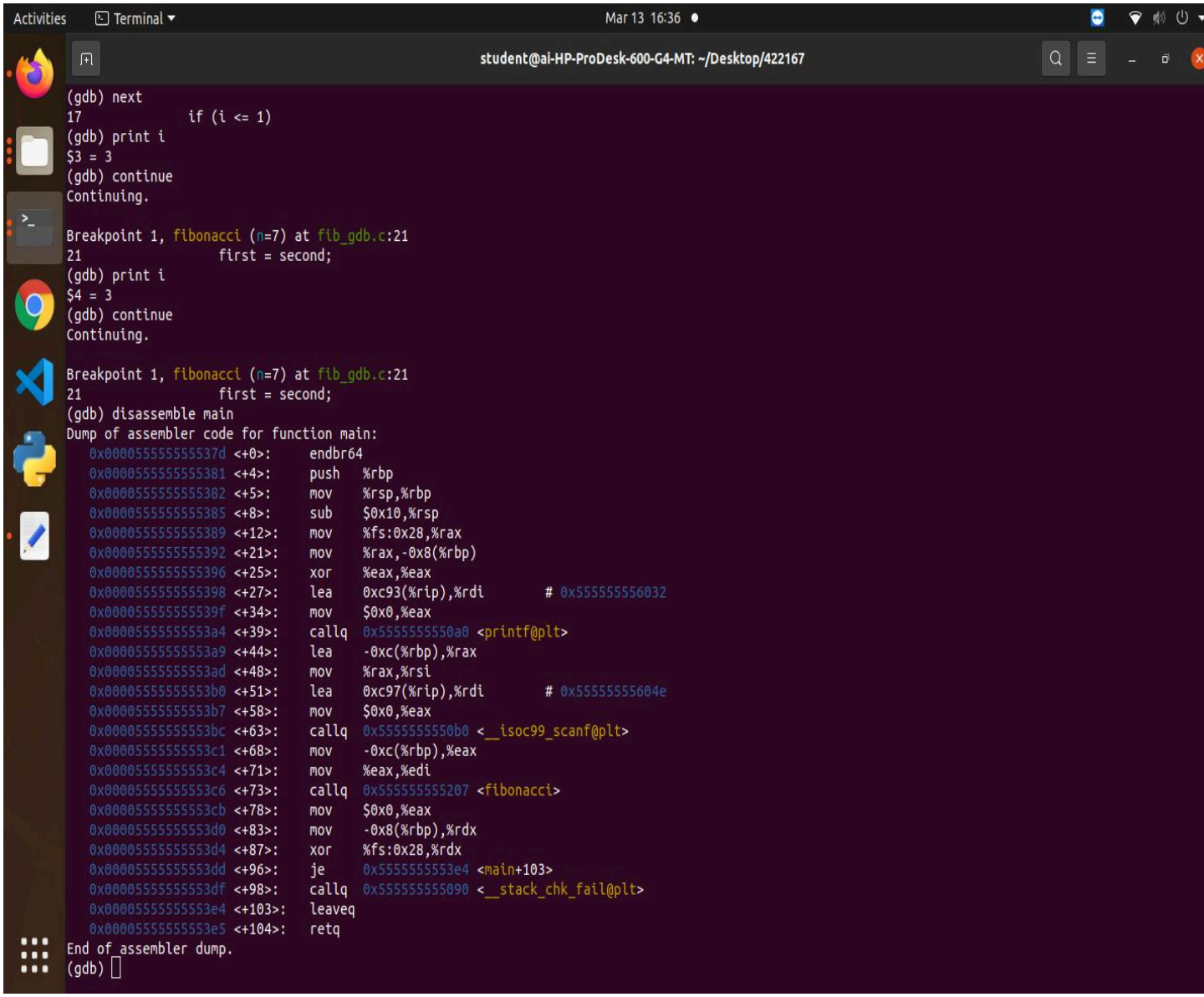
```
#include <stdio.h>
 int linearSearch(int arr[], int size, int target) {
    for (int i = 0; i <= size; i++) {
        if (arr[i] == target) {
            return i;
        }
    }
    return -1;
 }
 int main() {
    int arr[] = {1, 2, 3, 4, 5};
    int size = sizeof(arr) / sizeof(arr[0]);
    int target = 3;
    int result = linearSearch(arr, size, target);
    if (result != -1) {
        printf("Element found at index %d\n", result);
    } else {
        printf("Element not found\n");
    }
    return 0;
 }
```

1)

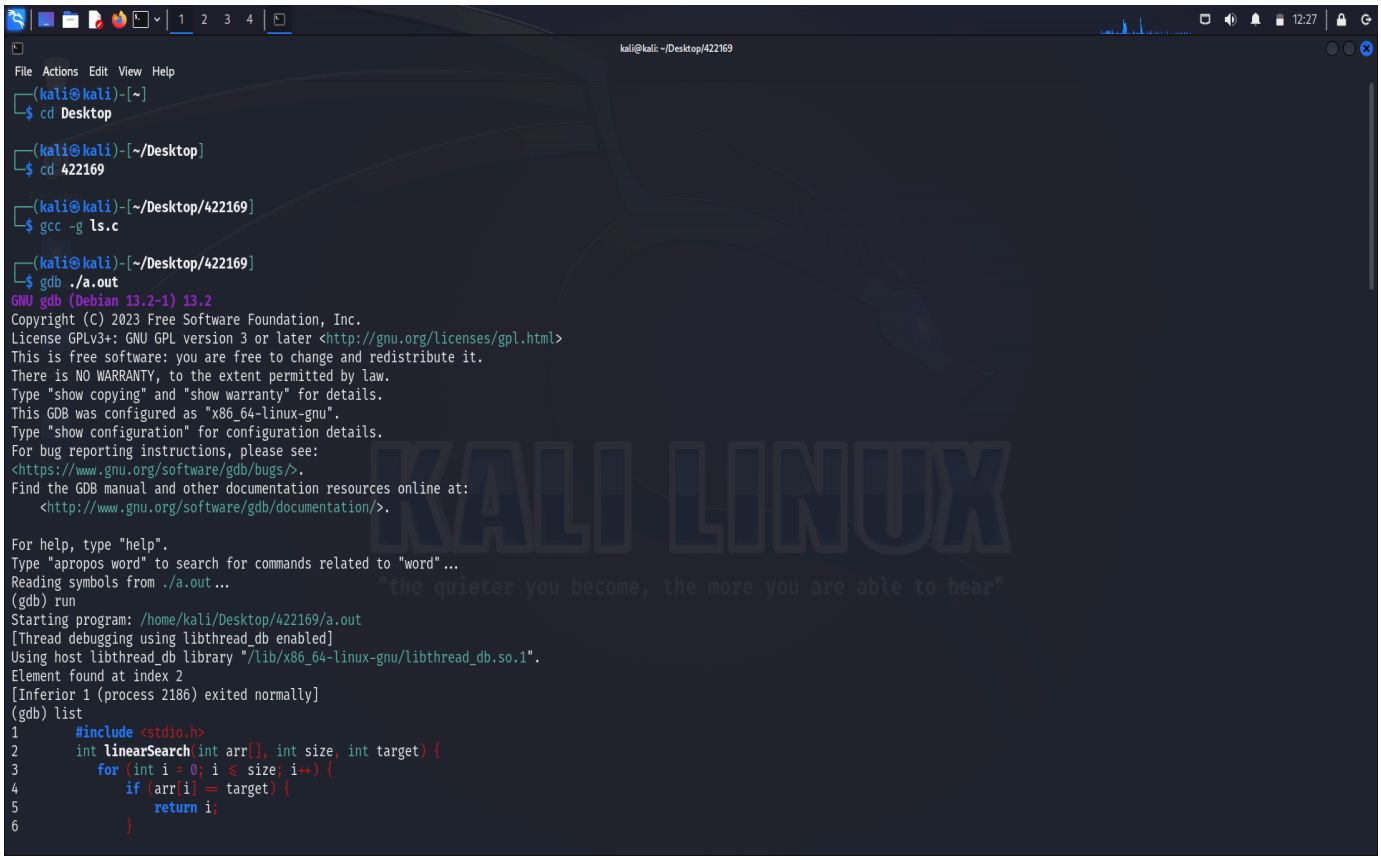

Activities
Terminal
Mar 13 15:48
student@ai-HP-ProDesk-600-G4-MT: ~/Desktop/422169_unix
student@ai-HP-ProDesk-600-G4-MT:~/Desktop/422169_unix$ gcc -g fib_gdb.c
student@ai-HP-ProDesk-600-G4-MT:~/Desktop/422169_unix$ gdb ./a.out
GNU gdb (Ubuntu 9.2-0ubuntu1~20.04) 9.2
Copyright (C) 2020 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ./a.out...
(gdb) run
Starting program: /home/student/Desktop/422169_unix/a.out
Enter the number of terms: 5
Fibonacci Series up to 5 terms:
0 1 1 2 3 5
[Inferior 1 (process 7799) exited normally]
(gdb) list
16 for (int i = 0; i <=n; i++) {
17 if (i <= 1)
18 next = i;
19 else {
20 next = first + second;
21 first = second;
22 second = next;
23 }
24 fib[i] = next;
25 }
(gdb)
26
27 printarray(fib, n);
28 }
29
30 int main() {
31 int n;
32 printf("Enter the number of terms: ");

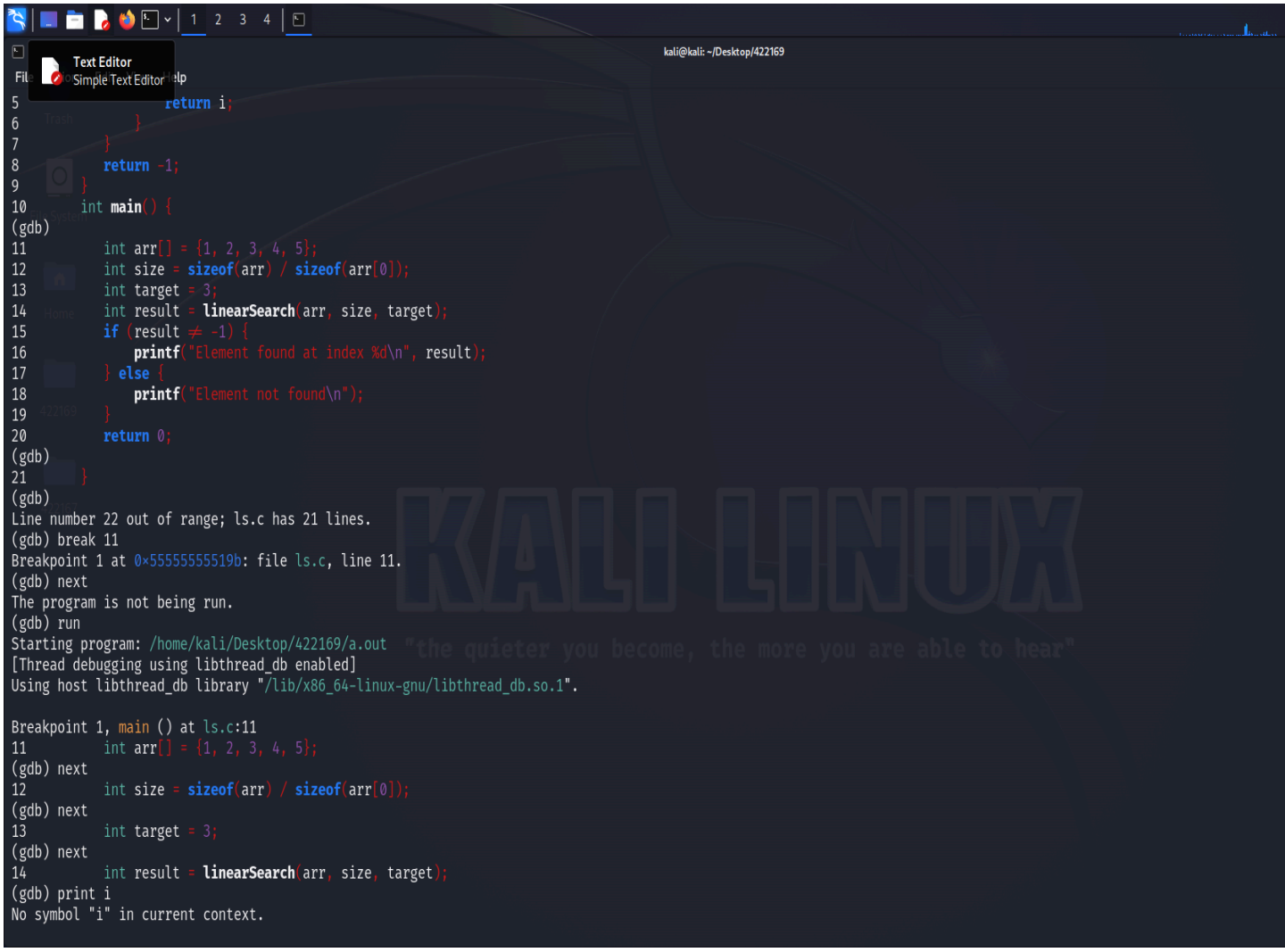

Activities
Terminal
Mar 13 15:48
student@ai-HP-ProDesk-600-G4-MT: ~/Desktop/422169_unix
student@ai-HP-ProDesk-6...
student@ai-HP-ProDesk-6...
student@ai-HP-ProDesk-6...
student@ai-HP-ProDesk-6...
student@ai-HP-ProDesk-6...
30 int main() {
31 int n;
32 printf("Enter the number of terms: ");
33 scanf("%d", &n);
34
35 fibonacci(n);
(gdb)
36
37 return 0;
38 }
39
(gdb)
Line number 40 out of range; fib_gdb.c has 39 lines.
(gdb) break 20
Breakpoint 1 at 0x55555555531b: file fib_gdb.c, line 20.
(gdb) run
Starting program: /home/student/Desktop/422169_unix/a.out
Enter the number of terms: 5
Fibonacci Series up to 5 terms:
Breakpoint 1, fibonacci (n=5) at fib_gdb.c:20
20 next = first + second;
(gdb)
(gdb) next
21 first = second;
(gdb) next
22 second = next;
(gdb) next
24 fib[i] = next;
(gdb) next
16 for (int i = 0; i <=n; i++) {
(gdb) next
17 if (i <= 1)
(gdb) next
Breakpoint 1, fibonacci (n=5) at fib_gdb.c:20
20 next = first + second;
(gdb) continue
Continuing.
Breakpoint 1, fibonacci (n=5) at fib_gdb.c:20
20 next = first + second;
(gdb) print i

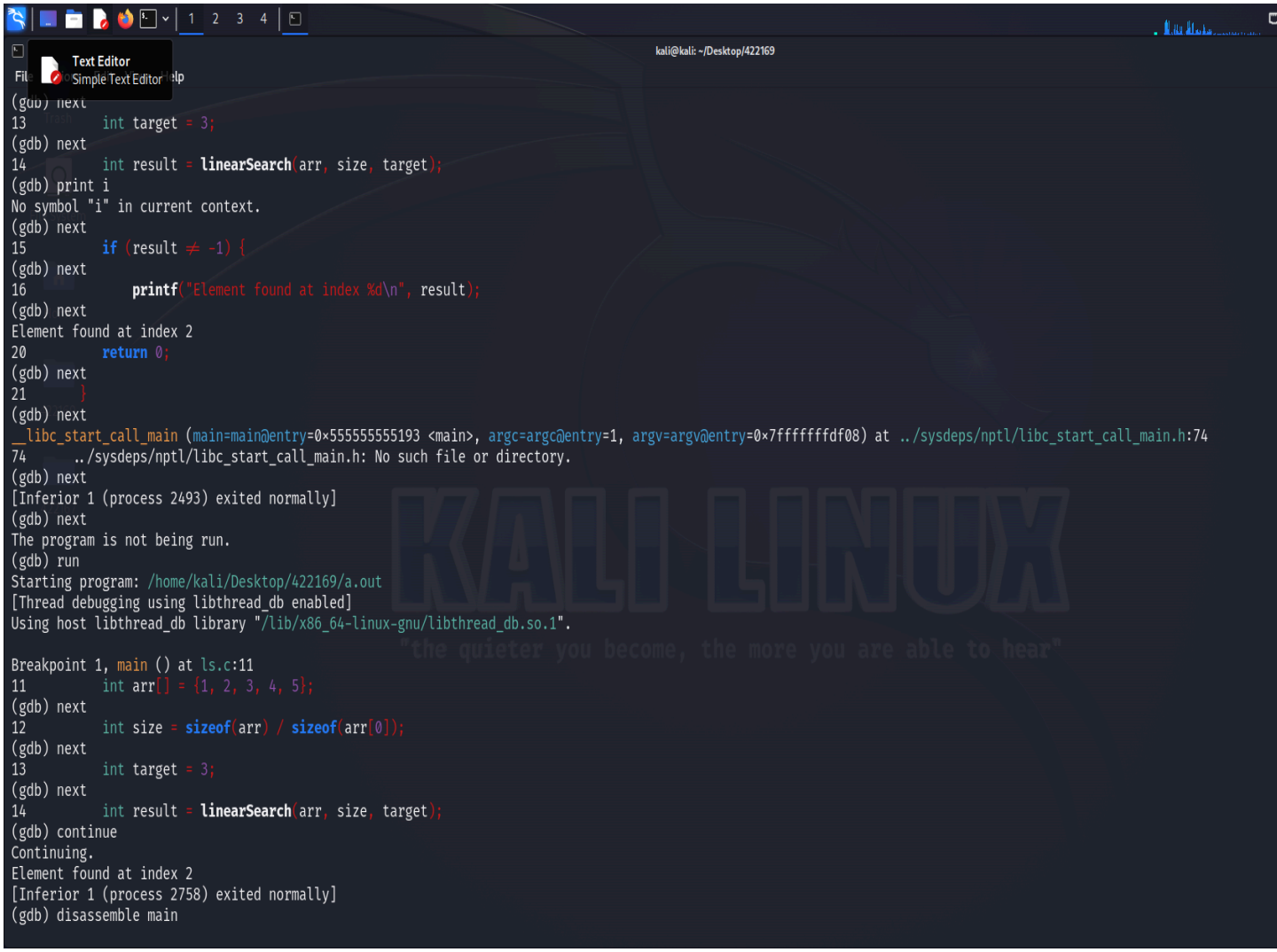

Activities
Terminal
Mar 13 15:48
student@ai-HP-ProDesk-600-G4-MT: ~/Desktop/422169_unix
student@ai-HP-ProDesk-6...
student@ai-HP-ProDesk-6...
student@ai-HP-ProDesk-6...
student@ai-HP-ProDesk-6...
student@ai-HP-ProDesk-6...
Breakpoint 1, fibonacci (n=5) at fib_gdb.c:20
20 next = first + second;
(gdb) print i
$1 = 4
(gdb) next
21 first = second;
(gdb) next
22 second = next;
(gdb) next
24 fib[i] = next;
(gdb) next
16 for (int i = 0; i <=n; i++) {
(gdb) print i
$2 = 4
(gdb) next
17 if (i <= 1)
(gdb) next
Breakpoint 1, fibonacci (n=5) at fib_gdb.c:20
20 next = first + second;
(gdb) print i
$3 = 5
(gdb) continue
Continuing.
0 1 1 2 3 5
[Inferior 1 (process 7807) exited normally]
(gdb) disassemble main
Dump of assembler code for function main:
0x000055555555537d <+0>: endbr64
0x0000555555555381 <+4>: push %rbp
0x0000555555555382 <+5>: mov %rsp,%rbp
0x0000555555555385 <+8>: sub $0x10,%rsp
0x0000555555555389 <+12>: mov %fs:0x28,%rax
0x0000555555555392 <+21>: mov %rax,-0x8(%rbp)
0x0000555555555396 <+25>: xor %eax,%eax
0x0000555555555398 <+27>: lea 0xc93(%rip),%rdi # 0x555555556032
0x000055555555539f <+34>: mov $0x0,%eax
0x00005555555553a4 <+39>: callq 0x5555555550a0 <printf@plt>
0x00005555555553a9 <+44>: lea -0xc(%rbp),%rax
0x00005555555553ad <+48>: mov %rax,%rsi
0x00005555555553b0 <+51>: lea 0xc97(%rip),%rdi # 0x55555555604e
0x00005555555553b7 <+58>: mov $0x0,%eax
0x00005555555553bc <+63>: callq 0x5555555550b0 <__isoc99_scanf@plt>

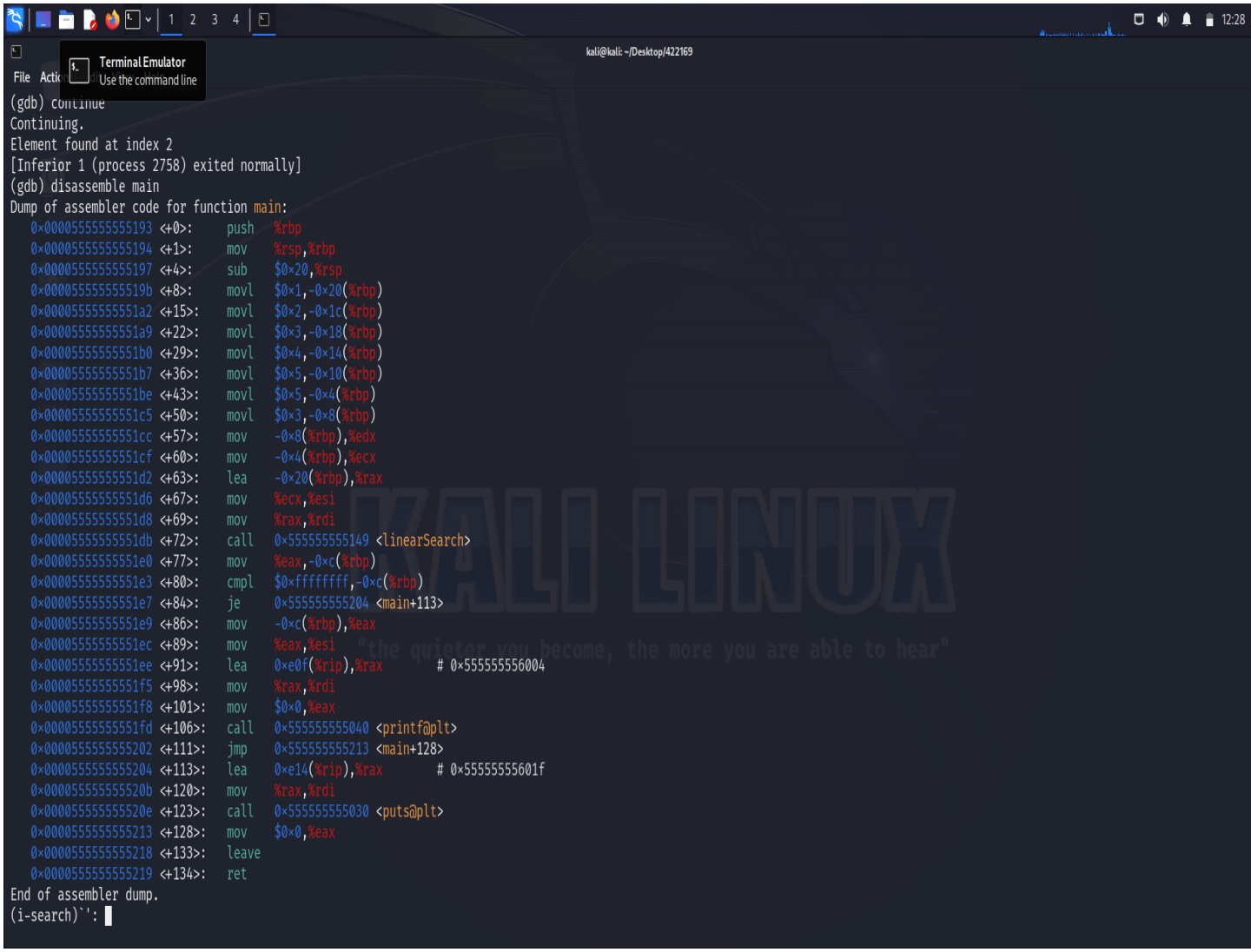

Activities
Terminal
Mar 13 16:36
student@ai-HP-ProDesk-600-G4-MT: ~/Desktop/422167
(gdb) next
17   if (i <= 1)
(gdb) print i
$3 = 3
(gdb) continue
Continuing.
Breakpoint 1, fibonacci (n=7) at fib_gdb.c:21
21   first = second;
(gdb) print i
$4 = 3
(gdb) continue
Continuing.
Breakpoint 1, fibonacci (n=7) at fib_gdb.c:21
21   first = second;
(gdb) disassemble main
Dump of assembler code for function main:
0x000055555555537d <+0>: endbr64
0x0000555555555381 <+4>: push %rbp
0x0000555555555382 <+5>: mov %rsp,%rbp
0x0000555555555385 <+8>: sub $0x10,%rsp
0x0000555555555389 <+12>: mov %fs:0x28,%rax
0x0000555555555392 <+21>: mov %rax,-0x8(%rbp)
0x0000555555555396 <+25>: xor %eax,%eax
0x0000555555555398 <+27>: lea 0xc93(%rip),%rdi # 0x555555556032
0x000055555555539f <+34>: mov $0x0,%eax
0x00005555555553a4 <+39>: callq 0x5555555550a0 <printf@plt>
0x00005555555553a9 <+44>: lea -0xc(%rbp),%rax
0x00005555555553ad <+48>: mov %rax,%rsi
0x00005555555553b0 <+51>: lea 0xc97(%rip),%rdi # 0x55555555604e
0x00005555555553b7 <+58>: mov $0x0,%eax
0x00005555555553bc <+63>: callq 0x5555555550b0 <__isoc99_scanf@plt>
0x00005555555553c1 <+68>: mov -0xc(%rbp),%eax
0x00005555555553c4 <+71>: mov %eax,%edi
0x00005555555553c6 <+73>: callq 0x555555555207 <fibonacci>
0x00005555555553cb <+78>: mov $0x0,%eax
0x00005555555553d0 <+83>: mov -0x8(%rbp),%rdx
0x00005555555553d4 <+87>: xor %fs:0x28,%rdx
0x00005555555553dd <+96>: je 0x5555555553e4 <main+103>
0x00005555555553df <+98>: callq 0x555555555090 <__stack_chk_fail@plt>
0x00005555555553e4 <+103>: leaveq
0x00005555555553e5 <+104>: retq
End of assembler dump.
(gdb)

2)


kali@kali: ~/Desktop/422169
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ cd Desktop
┌──(kali㉿kali)-[~/Desktop]
└─$ cd 422169
┌──(kali㉿kali)-[~/Desktop/422169]
└─$ gcc -g ls.c
┌──(kali㉿kali)-[~/Desktop/422169]
└─$ gdb ./a.out
GNU gdb (Debian 13.2-1) 13.2
Copyright (C) 2023 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ./a.out...
(gdb) run
Starting program: /home/kali/Desktop/422169/a.out
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Element found at index 2
[Inferior 1 (process 2186) exited normally]
(gdb) list
1 #include <stdio.h>
2 int linearSearch(int arr[], int size, int target) {
3 for (int i = 0; i <= size; i++) {
4 if (arr[i] == target) {
5 return i;
6 }


1 2 3 4
kali@kali: ~/Desktop/422169
Text Editor
Simple Text Editor
File Edit View Search Terminal Help
5 return i;
6 }
7 }
8 return -1;
9 }
10 int main() {
(gdb)
11 int arr[] = {1, 2, 3, 4, 5};
12 int size = sizeof(arr) / sizeof(arr[0]);
13 int target = 3;
14 int result = linearSearch(arr, size, target);
15 if (result != -1) {
16 printf("Element found at index %d\n", result);
17 } else {
18 printf("Element not found\n");
19 }
20 return 0;
(gdb)
21 }
(gdb)
Line number 22 out of range; ls.c has 21 lines.
(gdb) break 11
Breakpoint 1 at 0x55555555519b: file ls.c, line 11.
(gdb) next
The program is not being run.
(gdb) run
Starting program: /home/kali/Desktop/422169/a.out
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Breakpoint 1, main () at ls.c:11
11 int arr[] = {1, 2, 3, 4, 5};
(gdb) next
12 int size = sizeof(arr) / sizeof(arr[0]);
(gdb) next
13 int target = 3;
(gdb) next
14 int result = linearSearch(arr, size, target);
(gdb) print i
No symbol "i" in current context.
KALI LINUX
"the quieter you become, the more you are able to hear"


1 2 3 4
kali@kali: ~/Desktop/422169
Text Editor
Simple Text Editor
(gdb) next
13 int target = 3;
(gdb) next
14 int result = linearSearch(arr, size, target);
(gdb) print i
No symbol "i" in current context.
(gdb) next
15 if (result != -1) {
(gdb) next
16 printf("Element found at index %d\n", result);
(gdb) next
Element found at index 2
20 return 0;
(gdb) next
21 }
(gdb) next
__libc_start_call_main (main=main@entry=0x555555555193 <main>, argc=argc@entry=1, argv=argv@entry=0x7fffffffdf08) at ../sysdeps/nptl/libc_start_call_main.h:74
74 ../sysdeps/nptl/libc_start_call_main.h: No such file or directory.
(gdb) next
[Inferior 1 (process 2493) exited normally]
(gdb) next
The program is not being run.
(gdb) run
Starting program: /home/kali/Desktop/422169/a.out
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Breakpoint 1, main () at ls.c:11
11 int arr[] = {1, 2, 3, 4, 5};
(gdb) next
12 int size = sizeof(arr) / sizeof(arr[0]);
(gdb) next
13 int target = 3;
(gdb) next
14 int result = linearSearch(arr, size, target);
(gdb) continue
Continuing.
Element found at index 2
[Inferior 1 (process 2758) exited normally]
(gdb) disassemble main


1 2 3 4
12:28
Terminal Emulator
Use the command line
File
kali@kali: ~/Desktop/422169
(gdb) continue
Continuing.
Element found at index 2
[Inferior 1 (process 2758) exited normally]
(gdb) disassemble main
Dump of assembler code for function main:
0x0000555555555193 <+0>: push %rbp
0x0000555555555194 <+1>: mov %rsp,%rbp
0x0000555555555197 <+4>: sub $0x20,%rsp
0x000055555555519b <+8>: movl $0x1,-0x20(%rbp)
0x00005555555551a2 <+15>: movl $0x2,-0x1c(%rbp)
0x00005555555551a9 <+22>: movl $0x3,-0x18(%rbp)
0x00005555555551b0 <+29>: movl $0x4,-0x14(%rbp)
0x00005555555551b7 <+36>: movl $0x5,-0x10(%rbp)
0x00005555555551be <+43>: movl $0x5,-0x4(%rbp)
0x00005555555551c5 <+50>: movl $0x3,-0x8(%rbp)
0x00005555555551cc <+57>: mov -0x8(%rbp),%edx
0x00005555555551cf <+60>: mov -0x4(%rbp),%ecx
0x00005555555551d2 <+63>: lea -0x20(%rbp),%rax
0x00005555555551d6 <+67>: mov %ecx,%esi
0x00005555555551d8 <+69>: mov %rax,%rdi
0x00005555555551db <+72>: call 0x555555555149 <linearSearch>
0x00005555555551e0 <+77>: mov %eax,-0xc(%rbp)
0x00005555555551e3 <+80>: cmpl $0xffffffff,-0xc(%rbp)
0x00005555555551e7 <+84>: je 0x555555555204 <main+113>
0x00005555555551e9 <+86>: mov -0xc(%rbp),%eax
0x00005555555551ec <+89>: mov %eax,%esi
0x00005555555551ee <+91>: lea 0xe0f(%rip),%rax # 0x555555556004
0x00005555555551f5 <+98>: mov %rax,%rdi
0x00005555555551f8 <+101>: mov $0x0,%eax
0x00005555555551fd <+106>: call 0x555555555040 <printf@plt>
0x0000555555555202 <+111>: jmp 0x555555555213 <main+128>
0x0000555555555204 <+113>: lea 0xe14(%rip),%rax # 0x55555555601f
0x000055555555520b <+120>: mov %rax,%rdi
0x000055555555520e <+123>: call 0x555555555030 <puts@plt>
0x0000555555555213 <+128>: mov $0x0,%eax
0x0000555555555218 <+133>: leave
0x0000555555555219 <+134>: ret
End of assembler dump.
(i-search)``:
KALI LINUX
"the quieter you become, the more you are able to hear"