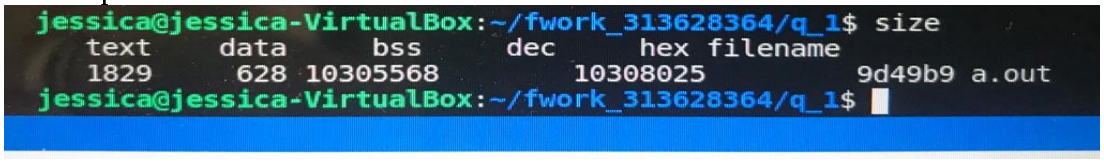
Q1:

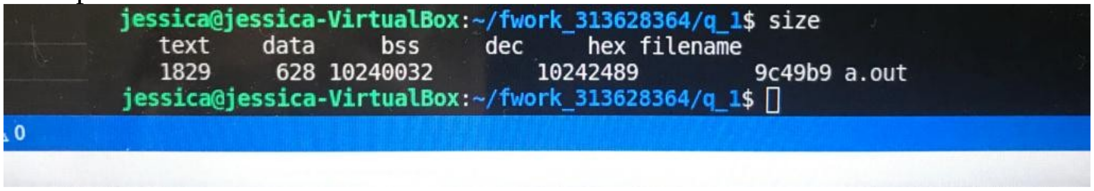
1. Line 5 (**char globBuf[65536];**) - stored in <u>BSS </u>or uninitialized data because the array of charsis not initialized only declaired in the global area of the program.
   - I used the command size to see where the uninitialized array is allocated. First time i ran size while the char array was part of the program and the seconds time i ran size when it was without the char array and saw that the amount that was missing was from BSS.

   - Before photo:



```
jessica@jessica-VirtualBox:~/fwork_313628364/q_1$ size
   text    data     bss     dec     hex filename
   1829     628 10305568        10308025         9d49b9 a.out
jessica@jessica-VirtualBox:~/fwork_313628364/q_1$ 
```

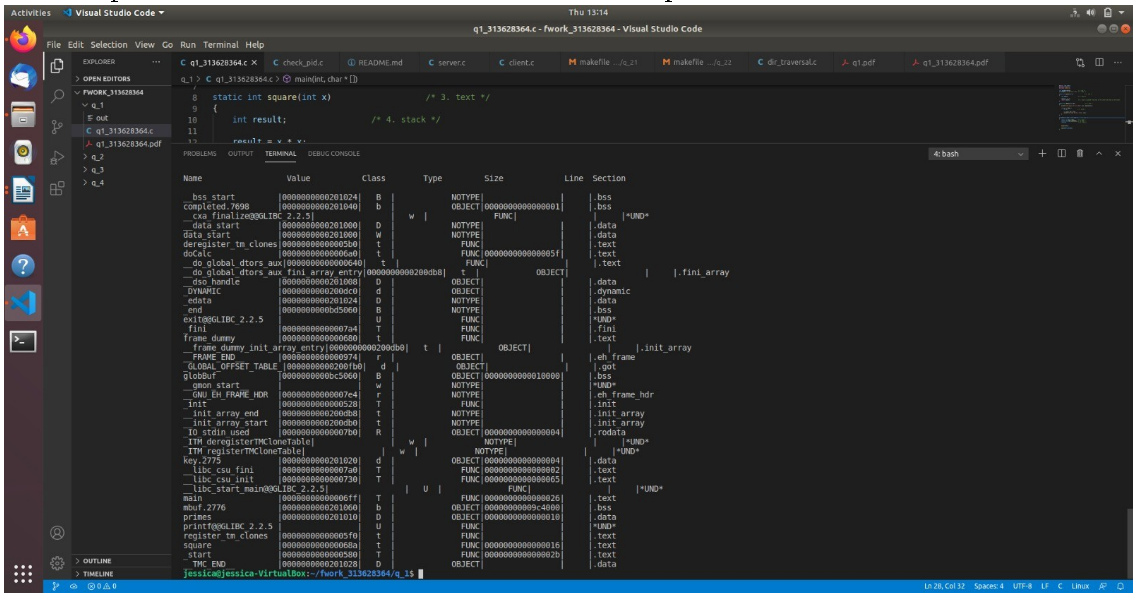
   - After photo:



```
jessica@jessica-VirtualBox:~/fwork_313628364/q_1$ size
   text    data     bss     dec     hex filename
   1829     628 10240032        10242489        9c49b9 a.out
jessica@jessica-VirtualBox:~/fwork_313628364/q_1$ 
```

2. Line 6 (**int primes[] = {2,3,5,7};**) - stored in <u>data segment </u>because there is an array of ints that is declared and initialized in the global area of the code.
   - I used the command size to see where the array is allocated. The First time i ran size while the array was part of the program and the second time when the array was not part of the program. When it wasn't part of the program I could see that the data wwnt down meaning less saved in data and thats how I know it was allocated in data.

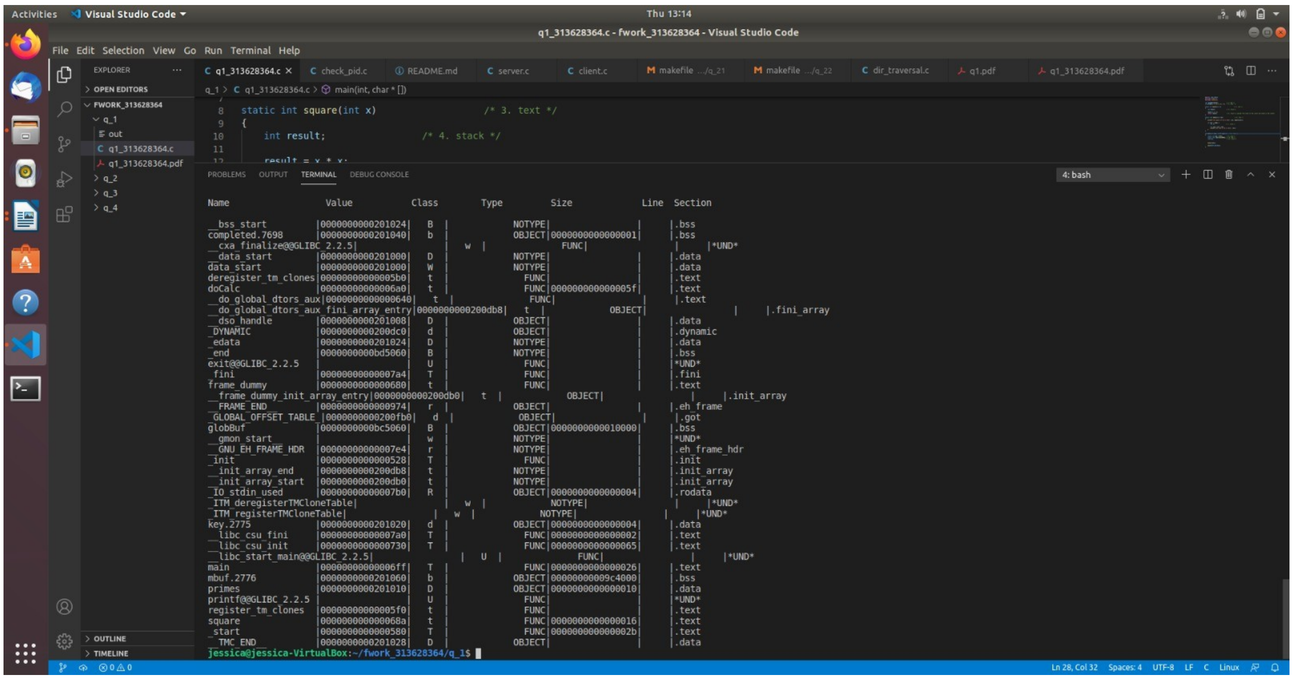
   - Second option is to use the nm command to see that primes is in data. Photo below.



```
static int square(int x)                /* 3. text */
{
    int result;                 /* 4. stack */

    result = x * x;
```

```
Name                  Value           Class        Type         Size             Line  Section

__bss_start         |0000000000201024|   B  |            NOTYPE|                |     |.bss
completed.7698      |0000000000201040|   b  |            OBJECT|0000000000000001|     |.bss
__cxa_finalize@@GLIBC_2.2.5|                |   w  |              FUNC|                |     |*UND*
__data_start        |0000000000201000|   D  |            NOTYPE|                |     |.data
data_start          |0000000000201000|   W  |            NOTYPE|                |     |.data
deregister_tm_clones|00000000000005b0|   t  |              FUNC|                |     |.text
doCalc              |00000000000006a0|   t  |              FUNC|000000000000005f|     |.text
__do_global_dtors_aux|0000000000000640|   t  |              FUNC|                |     |.text
__do_global_dtors_aux_fini_array_entry|0000000000200db8|   t  |            OBJECT|                |     |.fini_array
__dso_handle        |0000000000201008|   D  |            OBJECT|                |     |.data
_DYNAMIC            |0000000000200dc0|   d  |            OBJECT|                |     |.dynamic
_edata              |0000000000201024|   D  |            NOTYPE|                |     |.data
_end                |0000000000bd5060|   B  |            NOTYPE|                |     |.bss
exit@@GLIBC_2.2.5   |                |   U  |              FUNC|                |     |*UND*
_fini               |00000000000007a4|   T  |              FUNC|                |     |.fini
frame_dummy         |0000000000000680|   t  |              FUNC|                |     |.text
__frame_dummy_init_array_entry|0000000000200db0|   t  |            OBJECT|                |     |.init_array
__FRAME_END__       |0000000000000974|   r  |            OBJECT|                |     |.eh_frame
_GLOBAL_OFFSET_TABLE_|0000000000200fb0|   d  |            OBJECT|                |     |.got
globBuf             |0000000000bc5060|   B  |            OBJECT|0000000000010000|     |.bss
__gmon_start__      |                |   w  |            NOTYPE|                |     |*UND*
__GNU_EH_FRAME_HDR  |00000000000007e4|   r  |            NOTYPE|                |     |.eh_frame_hdr
_init               |0000000000000528|   T  |              FUNC|                |     |.init
__init_array_end    |0000000000200db8|   t  |            NOTYPE|                |     |.init_array
__init_array_start  |0000000000200db0|   t  |            NOTYPE|                |     |.init_array
_IO_stdin_used      |00000000000007b0|   R  |            OBJECT|0000000000000004|     |.rodata
_ITM_deregisterTMCloneTable|                |   w  |            NOTYPE|                |     |*UND*
_ITM_registerTMCloneTable|                |   w  |            NOTYPE|                |     |*UND*
key.2775            |0000000000201020|   d  |            OBJECT|0000000000000004|     |.data
__libc_csu_fini     |00000000000007a0|   T  |              FUNC|0000000000000002|     |.text
__libc_csu_init     |0000000000000730|   T  |              FUNC|0000000000000065|     |.text
__libc_start_main@@GLIBC_2.2.5|                |   U  |              FUNC|                |     |*UND*
main                |00000000000006ff|   T  |              FUNC|0000000000000026|     |.text
mbuf.2776           |0000000000201060|   b  |            OBJECT|00000000009c4000|     |.bss
primes              |0000000000201010|   D  |            OBJECT|0000000000000010|     |.data
printf@@GLIBC_2.2.5 |                |   U  |              FUNC|                |     |*UND*
register_tm_clones  |00000000000005f0|   t  |              FUNC|                |     |.text
square              |000000000000068a|   t  |              FUNC|0000000000000016|     |.text
_start              |0000000000000580|   T  |              FUNC|000000000000002b|     |.text
__TMC_END__         |0000000000201028|   D  |            OBJECT|                |     |.data
jessica@jessica-VirtualBox:~/fwork_313628364/q_1$ 
```

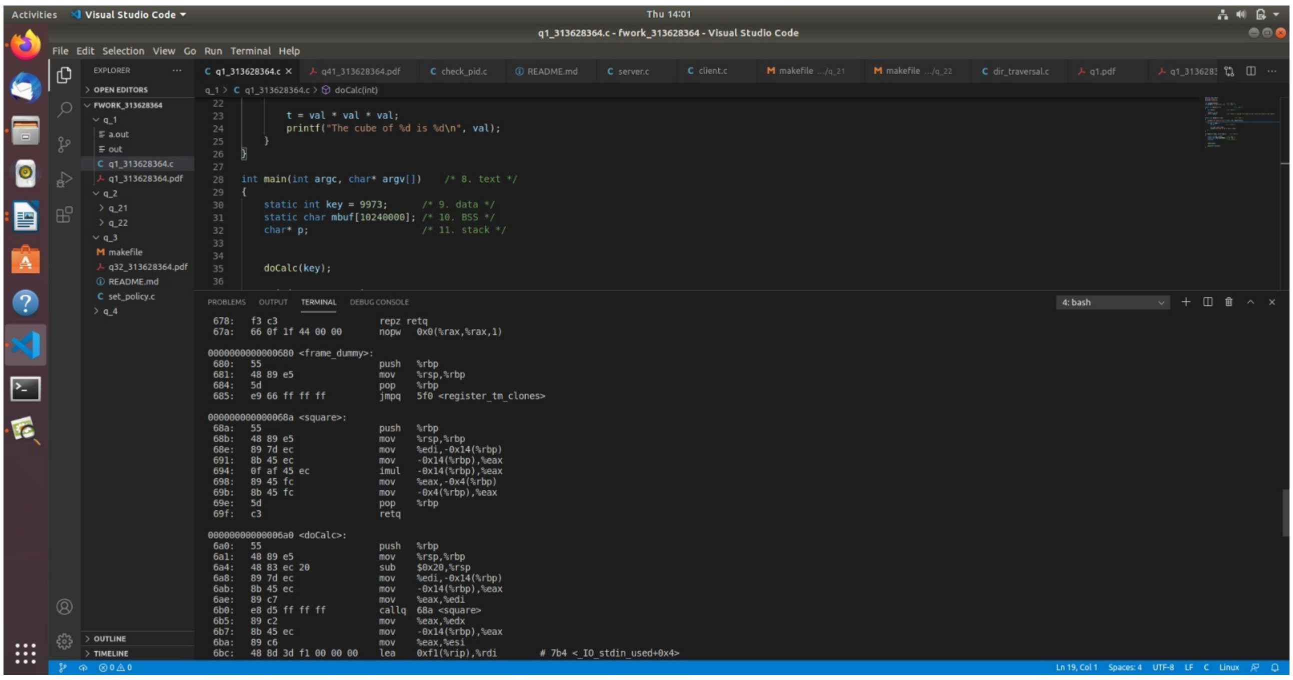
3. Line 8 (**static int square(int x)**) – stored in text because all functions are stored in text and i used the nm -f sys <fileName> commant to see where that function is located.



```c
 8  static int square(int x)             /* 3. text */
 9  {
10      int result;                 /* 4. stack */
11
12      result = x * x;
```

```
Name                  Value           Class        Type         Size             Line  Section

__bss_start         |0000000000201024|   B  |            NOTYPE|                |     |.bss
completed.7698      |0000000000201040|   b  |            OBJECT|0000000000000001|     |.bss
__cxa_finalize@@GLIBC_2.2.5|                |   w  |            FUNC|                |     |*UND*
__data_start        |0000000000201000|   D  |            NOTYPE|                |     |.data
data_start          |0000000000201000|   W  |            NOTYPE|                |     |.data
deregister_tm_clones|00000000000005b0|   t  |              FUNC|                |     |.text
doCalc              |00000000000006a0|   t  |              FUNC|000000000000005f|     |.text
__do_global_dtors_aux|0000000000000640|   t  |              FUNC|                |     |.text
__do_global_dtors_aux_fini_array_entry|0000000000200db8|   t  |            OBJECT|                |     |.fini_array
__dso_handle        |0000000000201008|   D  |            OBJECT|                |     |.data
_DYNAMIC            |0000000000200dc0|   d  |            OBJECT|                |     |.dynamic
_edata              |0000000000201024|   D  |            NOTYPE|                |     |.data
_end                |0000000000bd5060|   B  |            NOTYPE|                |     |.bss
exit@@GLIBC_2.2.5   |                |   U  |              FUNC|                |     |*UND*
_fini               |00000000000007a4|   T  |              FUNC|                |     |.fini
frame_dummy         |0000000000000680|   t  |              FUNC|                |     |.text
__frame_dummy_init_array_entry|0000000000200db0|   t  |            OBJECT|                |     |.init_array
__FRAME_END__       |0000000000000974|   r  |            OBJECT|                |     |.eh_frame
_GLOBAL_OFFSET_TABLE_|0000000000200fb0|   d  |            OBJECT|                |     |.got
globBuf             |0000000000bc5060|   B  |            OBJECT|0000000000010000|     |.bss
__gmon_start__      |                |   w  |            NOTYPE|                |     |*UND*
__GNU_EH_FRAME_HDR  |00000000000007e4|   r  |            NOTYPE|                |     |.eh_frame_hdr
_init               |0000000000000528|   T  |              FUNC|                |     |.init
__init_array_end    |0000000000200db8|   t  |            NOTYPE|                |     |.init_array
__init_array_start  |0000000000200db0|   t  |            NOTYPE|                |     |.init_array
_IO_stdin_used      |00000000000007b0|   R  |            OBJECT|0000000000000004|     |.rodata
_ITM_deregisterTMCloneTable|                |   w  |            NOTYPE|                |     |*UND*
_ITM_registerTMCloneTable|                |   w  |            NOTYPE|                |     |*UND*
key.2775            |0000000000201020|   d  |            OBJECT|0000000000000004|     |.data
__libc_csu_fini     |00000000000007a0|   T  |              FUNC|0000000000000002|     |.text
__libc_csu_init     |0000000000000730|   T  |              FUNC|0000000000000065|     |.text
__libc_start_main@@GLIBC_2.2.5|                |   U  |              FUNC|                |     |*UND*
main                |00000000000006ff|   T  |              FUNC|0000000000000026|     |.text
mbuf.2776           |0000000000201060|   b  |            OBJECT|00000000009c4000|     |.bss
primes              |0000000000201010|   D  |            OBJECT|0000000000000010|     |.data
printf@@GLIBC_2.2.5 |                |   U  |              FUNC|                |     |*UND*
register_tm_clones  |00000000000005f0|   t  |              FUNC|                |     |.text
square              |000000000000068a|   t  |              FUNC|0000000000000016|     |.text
_start              |0000000000000580|   T  |              FUNC|000000000000002b|     |.text
__TMC_END__         |0000000000201028|   D  |            OBJECT|                |     |.data
jessica@jessica-VirtualBox:~/fwork_313628364/q_1$
```

4. Line 10 (**int result;**) - stored in the stack like all variables in a C programs that are in the scope of a function. If we do not use the saved work new to save something into the heap it will automatically be saved to the functions stack. I used the objdump command to see the program as the assembly side of the program and see that we use a stock with push pop and mov.

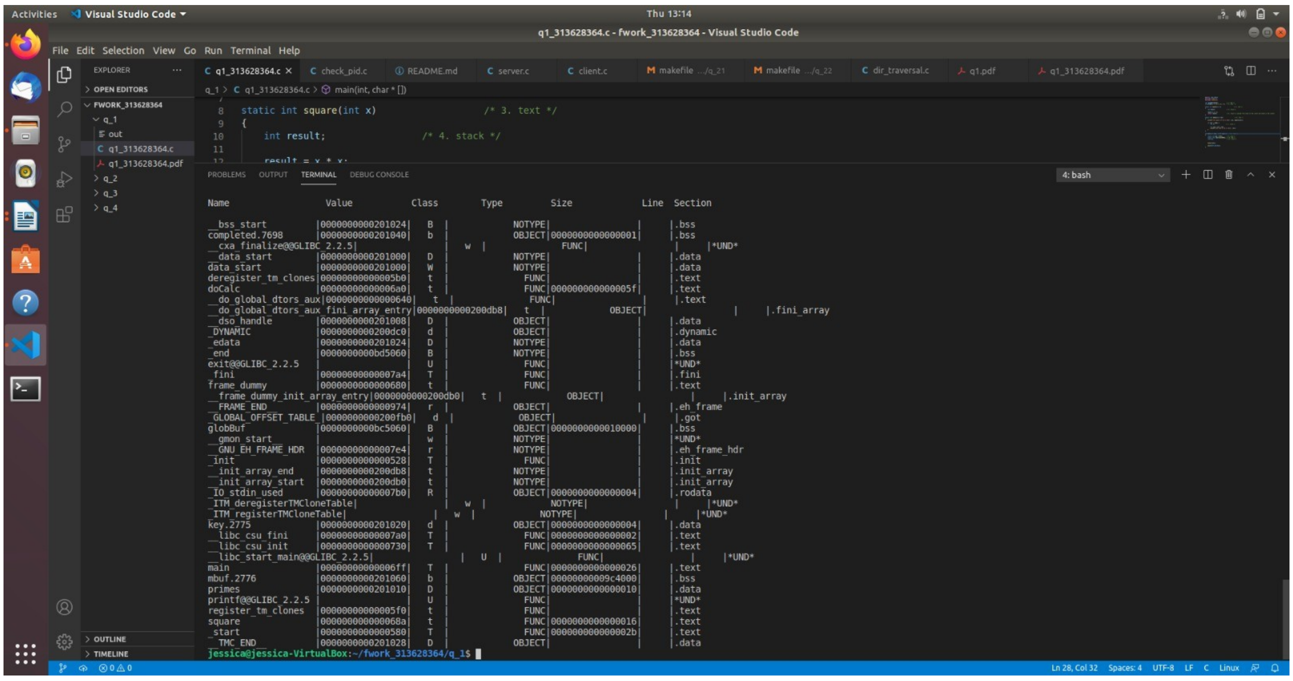


```c
            t = val * val * val;
            printf("The cube of %d is %d\n", val);
        }
}

int main(int argc, char* argv[])    /* 8. text */
{
    static int key = 9973;      /* 9. data */
    static char mbuf[10240000]; /* 10. BSS */
    char* p;                    /* 11. stack */


    doCalc(key);
```

```
 678:   f3 c3                   repz retq
 67a:   66 0f 1f 44 00 00       nopw   0x0(%rax,%rax,1)

0000000000000680 <frame_dummy>:
 680:   55                      push   %rbp
 681:   48 89 e5                mov    %rsp,%rbp
 684:   5d                      pop    %rbp
 685:   e9 66 ff ff ff          jmpq   5f0 <register_tm_clones>

000000000000068a <square>:
 68a:   55                      push   %rbp
 68b:   48 89 e5                mov    %rsp,%rbp
 68e:   89 7d ec                mov    %edi,-0x14(%rbp)
 691:   8b 45 ec                mov    -0x14(%rbp),%eax
 694:   0f af 45 ec             imul   -0x14(%rbp),%eax
 698:   89 45 fc                mov    %eax,-0x4(%rbp)
 69b:   8b 45 fc                mov    -0x4(%rbp),%eax
 69e:   5d                      pop    %rbp
 69f:   c3                      retq

00000000000006a0 <doCalc>:
 6a0:   55                      push   %rbp
 6a1:   48 89 e5                mov    %rsp,%rbp
 6a4:   48 83 ec 20             sub    $0x20,%rsp
 6a8:   89 7d ec                mov    %edi,-0x14(%rbp)
 6ab:   8b 45 ec                mov    -0x14(%rbp),%eax
 6ae:   89 c7                   mov    %eax,%edi
 6b0:   e8 d5 ff ff ff          callq  68a <square>
 6b5:   89 c2                   mov    %eax,%edx
 6b7:   8b 45 ec                mov    -0x14(%rbp),%eax
 6ba:   89 c6                   mov    %eax,%esi
 6bc:   48 8d 3d f1 00 00 00    lea    0xf1(%rip),%rdi        # 7b4 <_IO_stdin_used+0x4>
```

5. Line 13 (**return result**) – result is passed from the memory stack of the square function to the caller's stack and saves it in their stack. In this example the caller is the main function so the variable will be saved in mains stack.

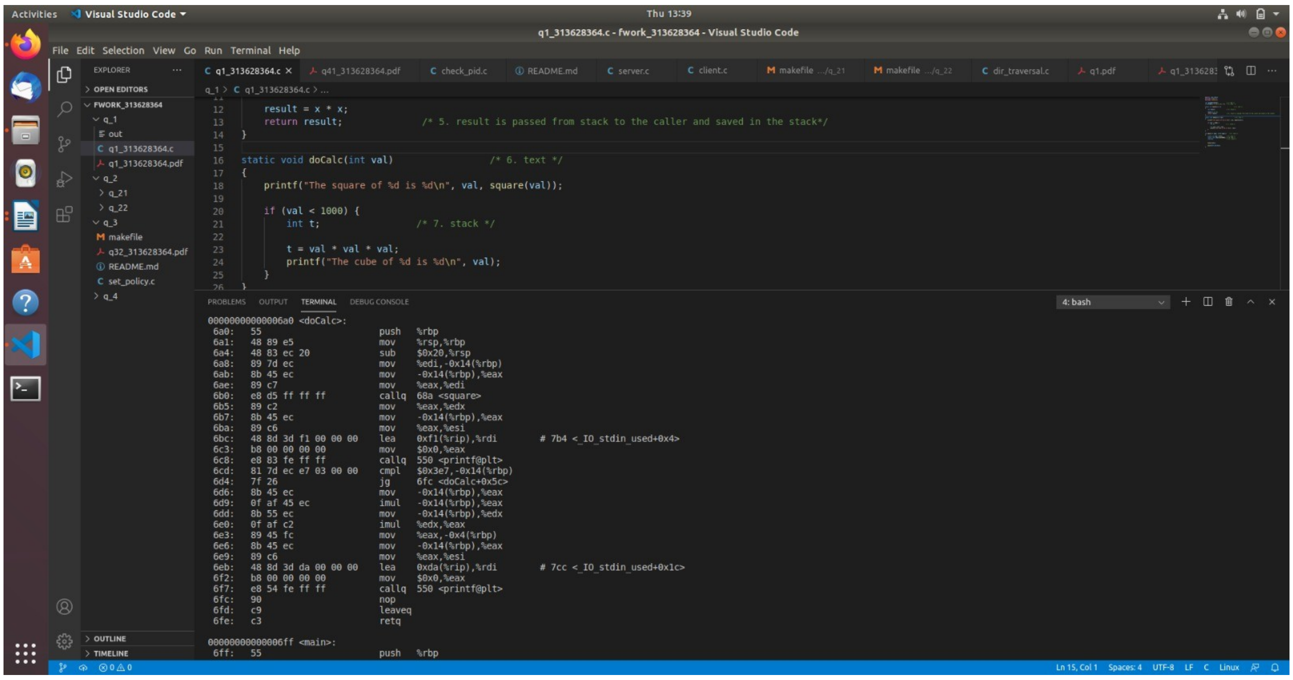
6. Line 16 (**static void doCalc(int val)**) – stored in <u>text</u> just like all the other functions. I used the nm command like in question 3.



```c
 8  static int square(int x)             /* 3. text */
 9  {
10      int result;              /* 4. stack */
11
12      result = x * x;
```

```
Name                  Value           Class        Type         Size             Line  Section

__bss_start          |0000000000201024|   B  |            NOTYPE|                |     |.bss
completed.7698       |0000000000201040|   b  |            OBJECT|0000000000000001|     |.bss
__cxa_finalize@@GLIBC_2.2.5|                 |   w  |            FUNC|                |     |*UND*
__data_start         |0000000000201000|   D  |            NOTYPE|                |     |.data
data_start           |0000000000201000|   W  |            NOTYPE|                |     |.data
deregister_tm_clones |00000000000005b0|   t  |              FUNC|                |     |.text
doCalc               |00000000000006a0|   t  |              FUNC|000000000000005f|     |.text
__do_global_dtors_aux|0000000000000640|   t  |              FUNC|                |     |.text
__do_global_dtors_aux_fini_array_entry|0000000000200db8|   t  |            OBJECT|                |     |.fini_array
__dso_handle         |0000000000201008|   D  |            OBJECT|                |     |.data
_DYNAMIC             |0000000000200dc0|   d  |            OBJECT|                |     |.dynamic
_edata               |0000000000201024|   D  |            NOTYPE|                |     |.data
_end                 |0000000000bd5060|   B  |            NOTYPE|                |     |.bss
exit@@GLIBC_2.2.5    |                |   U  |              FUNC|                |     |*UND*
_fini                |00000000000007a4|   T  |              FUNC|                |     |.fini
frame_dummy          |0000000000000680|   t  |              FUNC|                |     |.text
__frame_dummy_init_array_entry|0000000000200db0|   t  |            OBJECT|                |     |.init_array
__FRAME_END__        |0000000000000974|   r  |            OBJECT|                |     |.eh_frame
_GLOBAL_OFFSET_TABLE_|0000000000200fb0|   d  |            OBJECT|                |     |.got
globBuf              |0000000000bc5060|   B  |            OBJECT|0000000000010000|     |.bss
__gmon_start__       |                |   w  |            NOTYPE|                |     |*UND*
__GNU_EH_FRAME_HDR   |00000000000007e4|   r  |            NOTYPE|                |     |.eh_frame_hdr
_init                |0000000000000528|   T  |              FUNC|                |     |.init
__init_array_end     |0000000000200db8|   t  |            NOTYPE|                |     |.init_array
__init_array_start   |0000000000200db0|   t  |            NOTYPE|                |     |.init_array
_IO_stdin_used       |00000000000007b0|   R  |            OBJECT|0000000000000004|     |.rodata
_ITM_deregisterTMCloneTable|                |   w  |            NOTYPE|                |     |*UND*
_ITM_registerTMCloneTable|                |   w  |            NOTYPE|                |     |*UND*
key.2775             |0000000000201020|   d  |            OBJECT|0000000000000004|     |.data
__libc_csu_fini      |00000000000007a0|   T  |              FUNC|0000000000000002|     |.text
__libc_csu_init      |0000000000000730|   T  |              FUNC|0000000000000065|     |.text
__libc_start_main@@GLIBC_2.2.5|                |   U  |              FUNC|                |     |*UND*
main                 |00000000000006ff|   T  |              FUNC|0000000000000026|     |.text
mbuf.2776            |0000000000201060|   b  |            OBJECT|00000000009c4000|     |.bss
primes               |0000000000201010|   D  |            OBJECT|0000000000000010|     |.data
printf@@GLIBC_2.2.5  |                |   U  |              FUNC|                |     |*UND*
register_tm_clones   |00000000000005f0|   t  |              FUNC|                |     |.text
square               |000000000000068a|   t  |              FUNC|0000000000000016|     |.text
_start               |0000000000000580|   T  |              FUNC|000000000000002b|     |.text
__TMC_END__          |0000000000201028|   D  |            OBJECT|                |     |.data
jessica@jessica-VirtualBox:~/fwork_313628364/q_1$
```

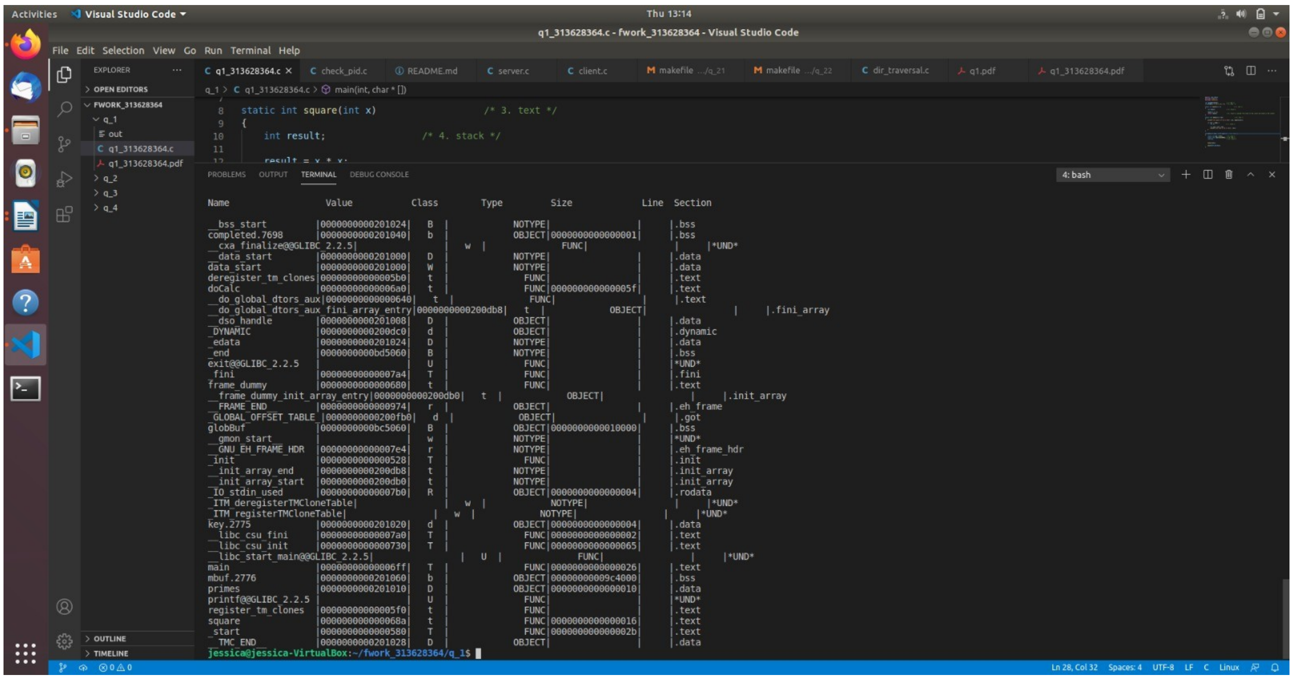
7. Line 21 (**int t;**) - stored in <u>stack</u> just like all variables in a function (non global or static variables meaning local variables). In the photo is shows that the doCalc function uses push meaning it enters variables to that functions stock.



```c
12      result = x * x;
13      return result;           /* 5. result is passed from stack to the caller and saved in the stack*/
14  }
15
16  static void doCalc(int val)              /* 6. text */
17  {
18      printf("The square of %d is %d\n", val, square(val));
19
20      if (val < 1000) {
21          int t;               /* 7. stack */
22
23          t = val * val * val;
24          printf("The cube of %d is %d\n", val);
25      }
26  }
```

```
00000000000006a0 <doCalc>:
 6a0:   55                      push   %rbp
 6a1:   48 89 e5                mov    %rsp,%rbp
 6a4:   48 83 ec 20             sub    $0x20,%rsp
 6a8:   89 7d ec                mov    %edi,-0x14(%rbp)
 6ab:   8b 45 ec                mov    -0x14(%rbp),%eax
 6ae:   89 c7                   mov    %eax,%edi
 6b0:   e8 d5 ff ff ff          callq  68a <square>
 6b5:   89 c2                   mov    %eax,%edx
 6b7:   8b 45 ec                mov    -0x14(%rbp),%eax
 6ba:   89 c6                   mov    %eax,%esi
 6bc:   48 8d 3d f1 00 00 00    lea    0xf1(%rip),%rdi        # 7b4 <_IO_stdin_used+0x4>
 6c3:   b8 00 00 00 00          mov    $0x0,%eax
 6c8:   e8 83 fe ff ff          callq  550 <printf@plt>
 6cd:   81 7d ec e7 03 00 00    cmpl   $0x3e7,-0x14(%rbp)
 6d4:   7f 26                   jg     6fc <doCalc+0x5c>
 6d6:   8b 45 ec                mov    -0x14(%rbp),%eax
 6d9:   0f af 45 ec             imul   -0x14(%rbp),%eax
 6dd:   8b 55 ec                mov    -0x14(%rbp),%edx
 6e0:   0f af c2                imul   %edx,%eax
 6e3:   89 45 fc                mov    %eax,-0x4(%rbp)
 6e6:   8b 45 ec                mov    -0x14(%rbp),%eax
 6e9:   89 c6                   mov    %eax,%esi
 6eb:   48 8d 3d da 00 00 00    lea    0xda(%rip),%rdi        # 7cc <_IO_stdin_used+0x1c>
 6f2:   b8 00 00 00 00          mov    $0x0,%eax
 6f7:   e8 54 fe ff ff          callq  550 <printf@plt>
 6fc:   90                      nop
 6fd:   c9                      leaveq
 6fe:   c3                      retq

00000000000006ff <main>:
 6ff:   55                      push   %rbp
```

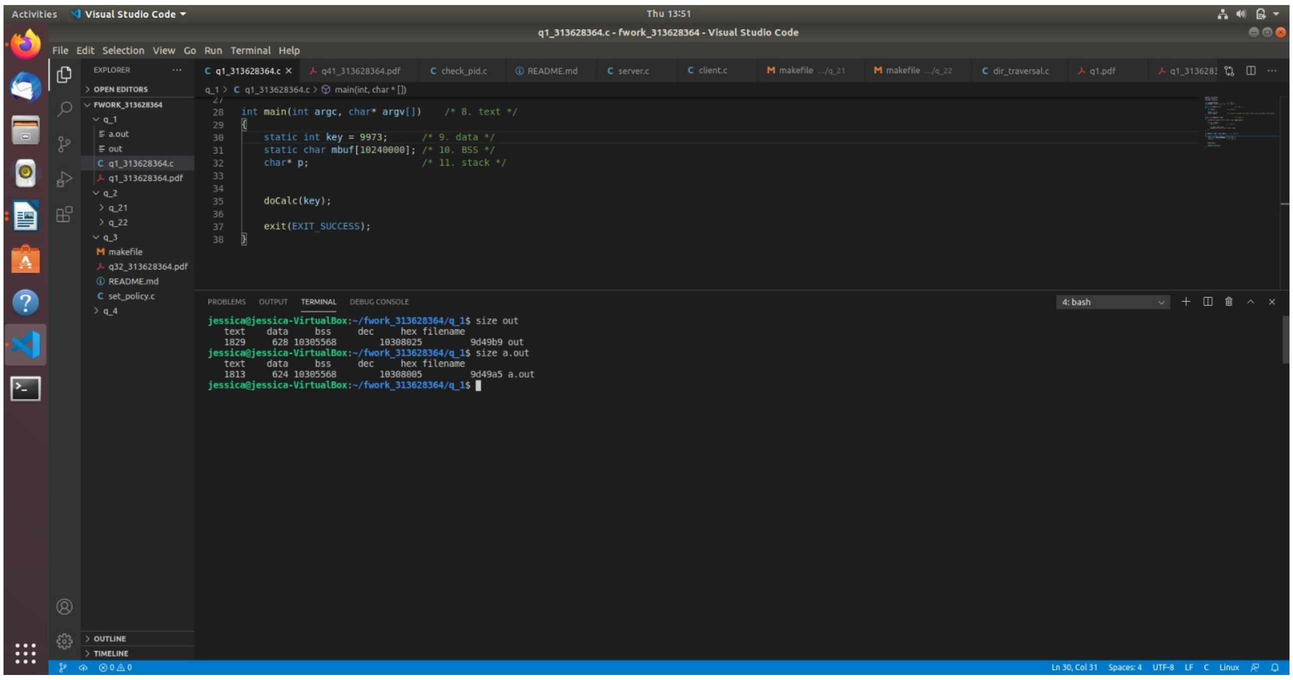
8. Line 28 (**int main(int argc, char* argv[])**)– All functions are saved in text as well as a main function because it is treated as any other function in the program. I used nm command to show that it is stored in text.



```
 8  static int square(int x)          /* 3. text */
 9  {
10      int result;               /* 4. stack */
11
12      result = x * x;
```

```
Name                  Value           Class        Type         Size             Line  Section

__bss_start          |0000000000201024|   B   |            NOTYPE|                |     |.bss
completed.7698       |0000000000201040|   b   |            OBJECT|0000000000000001|     |.bss
__cxa_finalize@@GLIBC_2.2.5|              |   w   |            FUNC|                |     |*UND*
__data_start         |0000000000201000|   D   |            NOTYPE|                |     |.data
data_start           |0000000000201000|   W   |            NOTYPE|                |     |.data
deregister_tm_clones |00000000000005b0|   t   |              FUNC|                |     |.text
doCalc               |00000000000006a0|   t   |              FUNC|000000000000005f|     |.text
__do_global_dtors_aux|0000000000000640|   t   |              FUNC|                |     |.text
__do_global_dtors_aux_fini_array_entry|0000000000200db8|   t   |           OBJECT|                |     |.fini_array
__dso_handle         |0000000000201008|   D   |            OBJECT|                |     |.data
_DYNAMIC             |0000000000200dc0|   d   |            OBJECT|                |     |.dynamic
_edata               |0000000000201024|   D   |            NOTYPE|                |     |.data
_end                 |0000000000bd5060|   B   |            NOTYPE|                |     |.bss
exit@@GLIBC_2.2.5    |                |   U   |              FUNC|                |     |*UND*
_fini                |00000000000007a4|   T   |              FUNC|                |     |.fini
frame_dummy          |0000000000000680|   t   |              FUNC|                |     |.text
__frame_dummy_init_array_entry|0000000000200db0|   t   |           OBJECT|                |     |.init_array
__FRAME_END__        |0000000000000974|   r   |            OBJECT|                |     |.eh_frame
_GLOBAL_OFFSET_TABLE_|0000000000200fb0|   d   |            OBJECT|                |     |.got
globBuf              |0000000000bc5060|   B   |            OBJECT|0000000000010000|     |.bss
__gmon_start__       |                |   w   |            NOTYPE|                |     |*UND*
__GNU_EH_FRAME_HDR   |00000000000007e4|   r   |            NOTYPE|                |     |.eh_frame_hdr
_init                |0000000000000528|   T   |              FUNC|                |     |.init
__init_array_end     |0000000000200db8|   t   |            NOTYPE|                |     |.init_array
__init_array_start   |0000000000200db0|   t   |            NOTYPE|                |     |.init_array
_IO_stdin_used       |00000000000007b0|   R   |            OBJECT|0000000000000004|     |.rodata
_ITM_deregisterTMCloneTable|              |   w   |            NOTYPE|                |     |*UND*
_ITM_registerTMCloneTable|                |   w   |            NOTYPE|                |     |*UND*
key.2775             |0000000000201020|   d   |            OBJECT|0000000000000004|     |.data
__libc_csu_fini      |00000000000007a0|   T   |              FUNC|0000000000000002|     |.text
__libc_csu_init      |0000000000000730|   T   |              FUNC|0000000000000065|     |.text
__libc_start_main@@GLIBC_2.2.5|           |   U   |              FUNC|                |     |*UND*
main                 |00000000000006ff|   T   |              FUNC|0000000000000026|     |.text
mbuf.2776            |0000000000201060|   b   |            OBJECT|00000000009c4000|     |.bss
primes               |0000000000201010|   D   |            OBJECT|0000000000000010|     |.data
printf@@GLIBC_2.2.5  |                |   U   |              FUNC|                |     |*UND*
register_tm_clones   |00000000000005f0|   t   |              FUNC|                |     |.text
square               |000000000000068a|   t   |              FUNC|0000000000000016|     |.text
_start               |0000000000000580|   T   |              FUNC|000000000000002b|     |.text
__TMC_END__          |0000000000201028|   D   |            OBJECT|                |     |.data
jessica@jessica-VirtualBox:~/fwork_313628364/q_1$
```

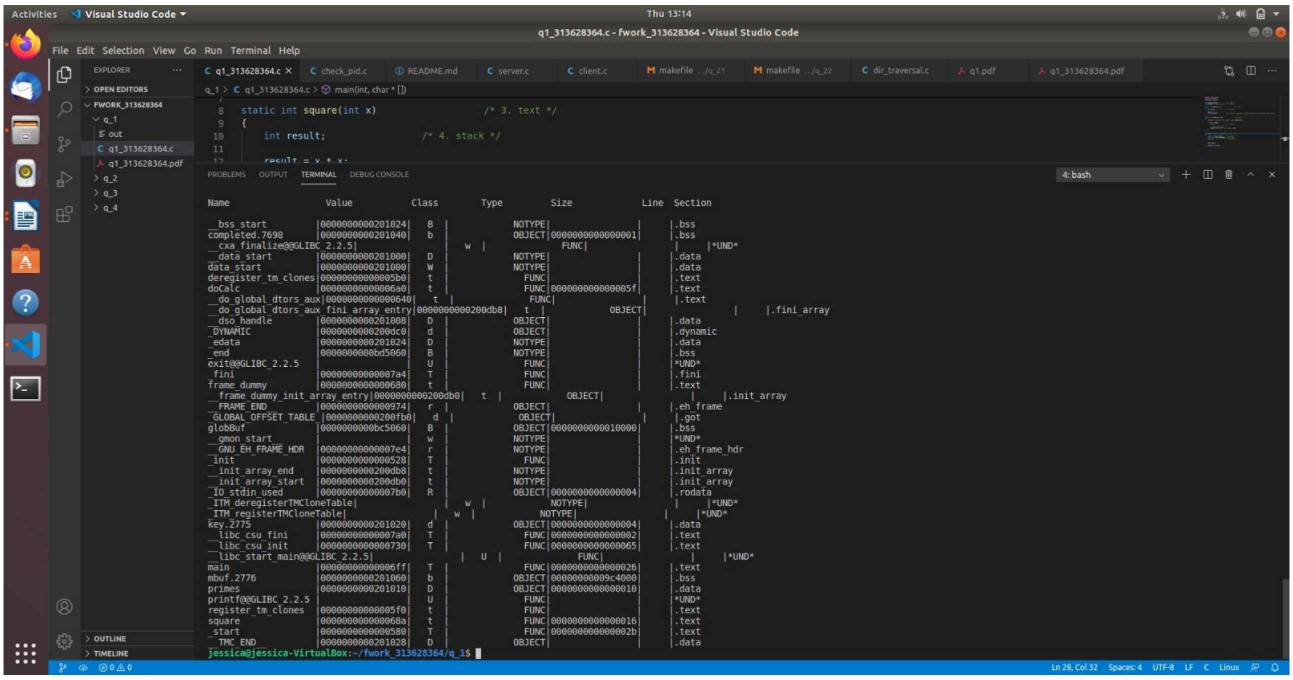
9. Line 30 (**static int key = 9973**) – stored in data segment because it is a static variable that is initialized. I used the size function to see that the stored data goes down when i delete the variable key from the program proving it is stored in data.



```
28  int main(int argc, char* argv[])    /* 8. text */
29  {
30      static int key = 9973;      /* 9. data */
31      static char mbuf[10240000]; /* 10. BSS */
32      char* p;                    /* 11. stack */
33
34
35      doCalc(key);
36
37      exit(EXIT_SUCCESS);
38  }
```

```
jessica@jessica-VirtualBox:~/fwork_313628364/q_1$ size out
   text    data     bss     dec     hex filename
   1829     628 10305568        10308025        9d49b9 out
jessica@jessica-VirtualBox:~/fwork_313628364/q_1$ size a.out
   text    data     bss     dec     hex filename
   1813     624 10305568        10308005        9d49a5 a.out
jessica@jessica-VirtualBox:~/fwork_313628364/q_1$
```

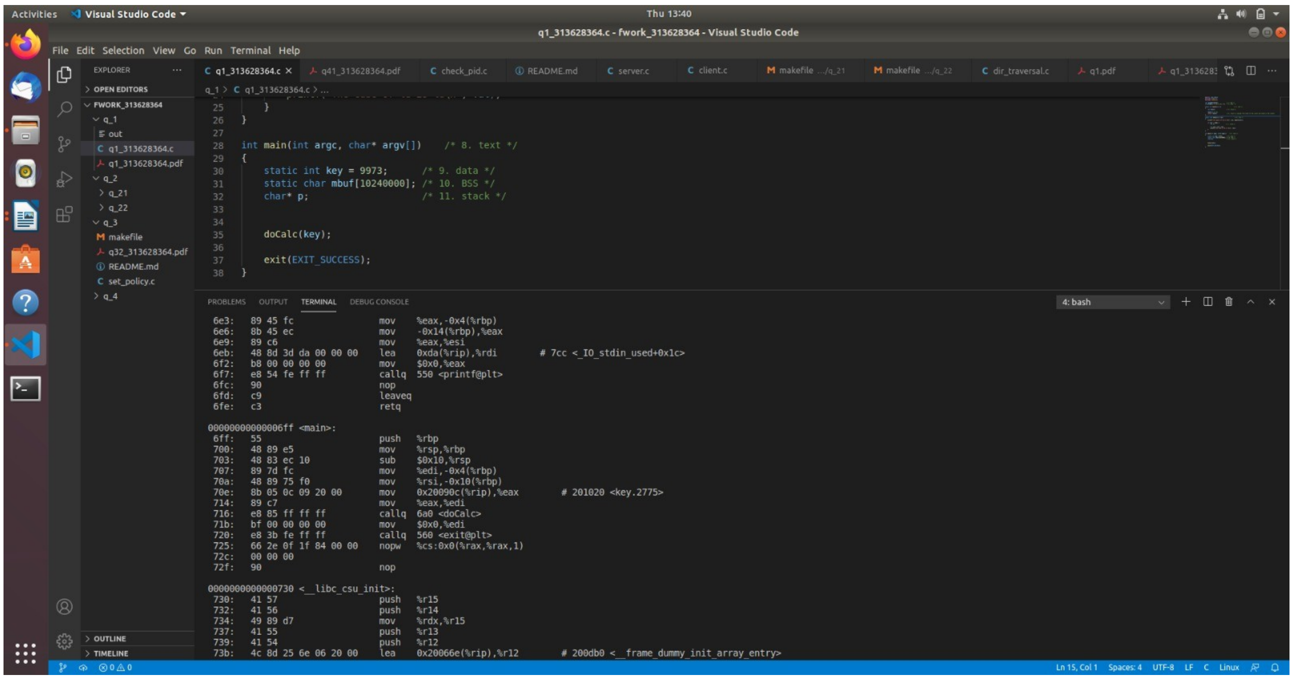
10. Line 31 (**static char mbuf[10240000]**) – I used the nm command to see that the variable is stored in <u>BSS </u> becuase it is a static array that is not initialized.



```
q_1 > C q1_313628364.c > main(int, char * [])
 8   static int square(int x)            /* 3. text */
 9   {
10       int result;                 /* 4. stack */
11
12       result = x * x;
```

```
Name                  Value           Class        Type         Size             Line  Section

__bss_start          |0000000000201024|   B  |            NOTYPE|                |     |.bss
completed.7698       |0000000000201040|   b  |            OBJECT|0000000000000001|     |.bss
__cxa_finalize@@GLIBC_2.2.5|                |   w  |            FUNC|                |     |*UND*
__data_start         |0000000000201000|   D  |            NOTYPE|                |     |.data
data_start           |0000000000201000|   W  |            NOTYPE|                |     |.data
deregister_tm_clones |00000000000005b0|   t  |              FUNC|                |     |.text
doCalc               |00000000000006a0|   t  |              FUNC|000000000000005f|     |.text
__do_global_dtors_aux|0000000000000640|   t  |              FUNC|                |     |.text
__do_global_dtors_aux_fini_array_entry|0000000000200db8|   t  |            OBJECT|                |     |.fini_array
__dso_handle         |0000000000201008|   D  |            OBJECT|                |     |.data
_DYNAMIC             |0000000000200dc0|   d  |            OBJECT|                |     |.dynamic
_edata               |0000000000201024|   D  |            NOTYPE|                |     |.data
_end                 |0000000000bd5060|   B  |            NOTYPE|                |     |.bss
exit@@GLIBC_2.2.5    |                |   U  |              FUNC|                |     |*UND*
_fini                |00000000000007a4|   T  |              FUNC|                |     |.fini
frame_dummy          |0000000000000680|   t  |              FUNC|                |     |.text
__frame_dummy_init_array_entry|0000000000200db0|   t  |            OBJECT|                |     |.init_array
__FRAME_END__        |0000000000000974|   r  |            OBJECT|                |     |.eh_frame
_GLOBAL_OFFSET_TABLE_|0000000000200fb0|   d  |            OBJECT|                |     |.got
globBuf              |0000000000bc5060|   B  |            OBJECT|0000000000010000|     |.bss
__gmon_start__       |                |   w  |            NOTYPE|                |     |*UND*
__GNU_EH_FRAME_HDR   |00000000000007e4|   r  |            NOTYPE|                |     |.eh_frame_hdr
_init                |0000000000000528|   T  |              FUNC|                |     |.init
__init_array_end     |0000000000200db8|   t  |            NOTYPE|                |     |.init_array
__init_array_start   |0000000000200db0|   t  |            NOTYPE|                |     |.init_array
_IO_stdin_used       |00000000000007b0|   R  |            OBJECT|0000000000000004|     |.rodata
_ITM_deregisterTMCloneTable|                |   w  |            NOTYPE|                |     |*UND*
_ITM_registerTMCloneTable|                |   w  |            NOTYPE|                |     |*UND*
key.2775             |0000000000201020|   d  |            OBJECT|0000000000000004|     |.data
__libc_csu_fini      |00000000000007a0|   T  |              FUNC|0000000000000002|     |.text
__libc_csu_init      |0000000000000730|   T  |              FUNC|0000000000000065|     |.text
__libc_start_main@@GLIBC_2.2.5|                |   U  |              FUNC|                |     |*UND*
main                 |00000000000006ff|   T  |              FUNC|0000000000000026|     |.text
mbuf.2776            |0000000000201060|   b  |            OBJECT|00000000009c4000|     |.bss
primes               |0000000000201010|   D  |            OBJECT|0000000000000010|     |.data
printf@@GLIBC_2.2.5  |                |   U  |              FUNC|                |     |*UND*
register_tm_clones   |00000000000005f0|   t  |              FUNC|                |     |.text
square               |000000000000068a|   t  |              FUNC|0000000000000016|     |.text
_start               |0000000000000580|   T  |              FUNC|000000000000002b|     |.text
__TMC_END__          |0000000000201028|   D  |            OBJECT|                |     |.data
jessica@jessica-VirtualBox:~/fwork_313628364/q_1$
```

11. Line 32 (**char* p;**) - stored in mains <u>stack</u>, I used thed objdump commant to see that the main functions used push pop and mov to save its variables and because the variable is not static or global and is not initialized with the saved word new it is saved in the stack.



```
q_1 > C q1_313628364.c > ...
25       }
26   }
27
28   int main(int argc, char* argv[])    /* 8. text */
29   {
30       static int key = 9973;      /* 9. data */
31       static char mbuf[10240000]; /* 10. BSS */
32       char* p;                    /* 11. stack */
33
34
35       doCalc(key);
36
37       exit(EXIT_SUCCESS);
38   }
```

```
 6e3:   89 45 fc                mov    %eax,-0x4(%rbp)
 6e6:   8b 45 ec                mov    -0x14(%rbp),%eax
 6e9:   89 c6                   mov    %eax,%esi
 6eb:   48 8d 3d da 00 00 00    lea    0xda(%rip),%rdi        # 7cc <_IO_stdin_used+0x1c>
 6f2:   b8 00 00 00 00          mov    $0x0,%eax
 6f7:   e8 54 fe ff ff          callq  550 <printf@plt>
 6fc:   90                      nop
 6fd:   c9                      leaveq
 6fe:   c3                      retq

00000000000006ff <main>:
 6ff:   55                      push   %rbp
 700:   48 89 e5                mov    %rsp,%rbp
 703:   48 83 ec 10             sub    $0x10,%rsp
 707:   89 7d fc                mov    %edi,-0x4(%rbp)
 70a:   48 89 75 f0             mov    %rsi,-0x10(%rbp)
 70e:   8b 05 0c 09 20 00       mov    0x20090c(%rip),%eax        # 201020 <key.2775>
 714:   89 c7                   mov    %eax,%edi
 716:   e8 85 ff ff ff          callq  6a0 <doCalc>
 71b:   bf 00 00 00 00          mov    $0x0,%edi
 720:   e8 3b fe ff ff          callq  560 <exit@plt>
 725:   66 2e 0f 1f 84 00 00    nopw   %cs:0x0(%rax,%rax,1)
 72c:   00 00 00
 72f:   90                      nop

0000000000000730 <__libc_csu_init>:
 730:   41 57                   push   %r15
 732:   41 56                   push   %r14
 734:   49 89 d7                mov    %rdx,%r15
 737:   41 55                   push   %r13
 739:   41 54                   push   %r12
 73b:   4c 8d 25 6e 06 20 00    lea    0x20066e(%rip),%r12        # 200db0 <__frame_dummy_init_array_entry>
```