

```
char globBuf[65536];          /* 1. BSS */
static char mbuf[10240000]; /* BSS */
```

```
raamb@ubuntu-18-04: ~/Desktop/maahot_work/Q1
File Edit View Search Terminal Help
0000000000005b0 t deregister_tm_clones
0000000000006a0 t doCalc
000000000000640 t __do_global_ctors_aux
000000000000db8 t __do_global_ctors_aux_fini_array_entry
0000000000001008 D __dso_handle
00000000000020dc0 d __dynamic
00000000000020dc0 d __DYNAMIC
000000000000378 r __dynstr
0000000000002b8 r __dynsym
00000000000021024 D __edata
0000000000000830 r __eh_frame
0000000000007e4 r __eh_frame_hdr
000000000000bd5060 B __end
00000000000007a4 U __exit@@GLIBC_2.2.5
00000000000007a4 t __fini
0000000000000db8 t __fini_array
000000000000680 t __frame_dummy
000000000000db0 t __frame_dummy_init_array_entry
000000000000974 r __FRAME_END__
000000000000fb0 d __GLOBAL_OFFSET_TABLE__
000000000000c5060 B globBuf
0000000000007e4 r __gmon_start__
0000000000007e4 r GNU_EH_FRAME_HDR

raamb@ubuntu-18-04: ~/Desktop/maahot_work/Q1
File Edit View Search Terminal Help
are, as well, depending on the object file format. If lowercase,
the symbol is usually local; if uppercase, the symbol is global
(external). There are however a few lowercase symbols that are
shown for special global symbols ("u", "v" and "w").

"A" The symbol's value is absolute, and will not be changed by
further linking.

"B"
"B" The symbol is in the BSS data section. This section typically
contains zero-initialized or uninitialized data, although the
exact behavior is system dependent.

"C" The symbol is common. Common symbols are uninitialized data.
When linking, multiple common symbols may appear with the same
name. If the symbol is defined anywhere, the common symbols
are treated as undefined references.

"D"
"D" The symbol is in the initialized data section.

"G"
"G" The symbol is in an initialized data section for small objects.
Manual page nm(1) line 34 (press h for help or q to quit)
```

```
int primes[] = { 2, 3, 5, 7 }; /* 2. initialized data section */
static int key = 9973;        /* initialized data section */
```

```
raamb@ubuntu-18-04: ~/Desktop/maahot_work/Q1
File Edit View Search Terminal Help
000000000000db0 t __init_array_start
000000000000238 r __interp
0000000000007b0 R __IO_stdin_used
0000000000007b0 w __ITM_deregisterTMCloneTable
0000000000007b0 w __ITM_registerTMCloneTable
0000000000001020 d key.2775
0000000000007a0 t __libc_csu_fini
000000000000730 t __libc_csu_init
000000000000730 U __libc_start_main@@GLIBC_2.2.5
000000000000702 T __main
0000000000001060 b __nbuf.2776
000000000000254 r __note.ABI-tag
000000000000274 r __note.gnu.build-id
000000000000540 t __plt
000000000000570 t __plt.got
0000000000001010 D primes
0000000000001010 U printf@@GLIBC_2.2.5
0000000000000000 a __process_layout_q.c
0000000000005f0 t __register_tm_clones
000000000000438 r __rela.dyn
0000000000004f8 r __rela.plt
0000000000007b0 r __rodata
00000000000068a t __square
000000000000580 T __start

raamb@ubuntu-18-04: ~/Desktop/maahot_work/Q1
File Edit View Search Terminal Help
shown for special global symbols ("u", "v" and "w").

"A" The symbol's value is absolute, and will not be changed by
further linking.

"B"
"B" The symbol is in the BSS data section. This section typically
contains zero-initialized or uninitialized data, although the
exact behavior is system dependent.

"C" The symbol is common. Common symbols are uninitialized data.
When linking, multiple common symbols may appear with the same
name. If the symbol is defined anywhere, the common symbols
are treated as undefined references.

"D"
"D" The symbol is in the initialized data section.

"G"
"G" The symbol is in an initialized data section for small objects.
Some object file formats permit more efficient access to small
data objects, such as a global int variable as opposed to a
large global array.
Manual page nm(1) line 37 (press h for help or q to quit)
```

```
square(int x)                /* 3. text (code) section */
doCalc(int val)              /* 6. text (code) section */
main(int argc, char* argv[]) /* text (code) section */
```

```
raamb@ubuntu-18-04: ~/Desktop/maahot_work/Q1
File Edit View Search Terminal Help
000000000000db0 t __init_array_start
000000000000238 r __interp
0000000000007b0 R __IO_stdin_used
0000000000007b0 w __ITM_deregisterTMCloneTable
0000000000007b0 w __ITM_registerTMCloneTable
0000000000001020 d key.2775
0000000000007a0 t __libc_csu_fini
000000000000730 t __libc_csu_init
000000000000730 U __libc_start_main@@GLIBC_2.2.5
000000000000702 T __main
0000000000001060 b __nbuf.2776
000000000000254 r __note.ABI-tag
000000000000274 r __note.gnu.build-id
000000000000540 t __plt
000000000000570 t __plt.got
0000000000001010 D primes
0000000000001010 U printf@@GLIBC_2.2.5
0000000000000000 a __process_layout_q.c
0000000000005f0 t __register_tm_clones
000000000000438 r __rela.dyn
0000000000004f8 r __rela.plt
0000000000007b0 r __rodata
00000000000068a t __square
000000000000580 T __start

raamb@ubuntu-18-04: ~/Desktop/maahot_work/Q1
File Edit View Search Terminal Help
"I" The symbol is an indirect reference to another symbol.

"N" The symbol is a debugging symbol.

"P" The symbol is in a stack unwind section.

"R"
"R" The symbol is in a read only data section.

"S"
"S" The symbol is in an uninitialized or zero-initialized data
section for small objects.

"T"
"T" The symbol is in the text (code) section.

"U" The symbol is undefined.

"u" The symbol is a unique global symbol. This is a GNU extension
to the standard set of ELF symbol bindings. For such a symbol
the dynamic linker will make sure that in the entire process
there is just one symbol with this name and type in use.
Manual page nm(1) line 70 (press h for help or q to quit)
```

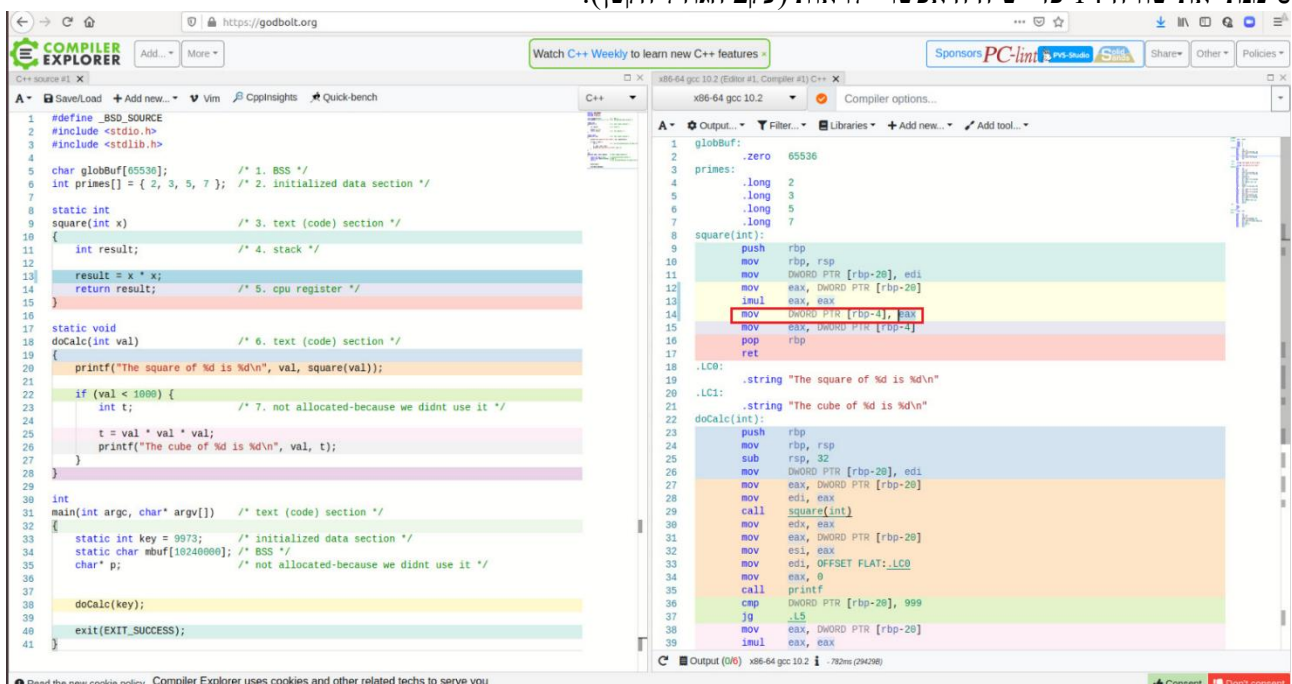
```
int result;          /* 4. stack */
```

המשתנה נמצא במחסנית, אפשר לראות זאת בעזרת הטווח הדצימאלי שמופיע בקטגוריה מחסנית בשורה הלפני אחרונה.
0x7fffffff→ff000<fdcb<de000

```
raamb@ubuntu-18-04: ~/Desktop/maahot_work/Q1
File Edit View Search Terminal Help
gnu/libc-2.27.so
0x7ffff7bcb000 0x7ffff7dcb000 0x200000 0x1e7000 /lib/x86_64-linux-
gnu/libc-2.27.so
0x7ffff7dcb000 0x7ffff7dcf000 0x4000 0x1e7000 /lib/x86_64-linux-
gnu/libc-2.27.so
0x7ffff7dcf000 0x7ffff7dd1000 0x2000 0x1eb000 /lib/x86_64-linux-
gnu/libc-2.27.so
0x7ffff7dd1000 0x7ffff7dd5000 0x4000 0x0
0x7ffff7dd5000 0x7ffff7dfc000 0x27000 0x0 /lib/x86_64-linux-
gnu/ld-2.27.so
0x7ffff7fdf000 0x7ffff7fe1000 0x2000 0x0
---Type <return> to continue, or q <return> to quit---c
0x7ffff7ffa000 0x7ffff7ffa000 0x3000 0x0 [vvar]
0x7ffff7ffa000 0x7ffff7ffc000 0x2000 0x0 [vdso]
0x7ffff7ffc000 0x7ffff7ffd000 0x1000 0x27000 /lib/x86_64-linux-
gnu/ld-2.27.so
0x7ffff7ffd000 0x7ffff7ffe000 0x1000 0x28000 /lib/x86_64-linux-
gnu/ld-2.27.so
0x7ffff7ffe000 0x7ffff7fff000 0x1000 0x0
0x7ffff7fff000 0x7ffff7fff000 0x21000 0x0 [stack]
0xffffffff600000 0xffffffff601000 0x1000 0x0 [vsyscall]
(gdb) p &result
$1 = (int *) 0x7ffff7ffdcbc
(gdb)
```

```
return result;      /* 5. cpu register */
```

המשתנה מוחזר בעזרת אוגרים, ניתן לראות את האוגרים באמצעות אתר:
Godbolt
סימנתי את שורה 14 כדי שיהיה אפשרי לראות (עקב הגודל הקטן).



```
int t;          /* 7. not allocated-because we didnt use it */  
char* p;        /* not allocated-because we didnt use it */
```

אנחנו לא משתמשים במשתנים הללו, לכן הם לא מוקצים.