# Notes for valgrind

Author : Vikas Nagpal (https://github.com/vikasnagpaliitd)
Version 1.0

# Memory related issues

- Memory Leak : allocated memory but did not free
- Memory Errors : e.g. reading beyond the array limit, reading/writing dangling pointer or already freed  pointers
  - double free
  - reading memory beyond valid area
  - uninitialized memory read
  -

# How to compile code for valgrind?

```
$ gcc -g main.c func.c
```

# How to run a program under valgrind

```
$ valgrind ./a.out
```

OR

```
$ valgrind --tool=memcheck --leak-check=full ./a.out
```

val1.c : Conditional jump or move depends on uninitialised value(s)

val2.c:

```
=17777== Invalid read of size 4
==17777==    at 0x1091B3: main (prog.c:17)
==17777==  Address 0x4a56040 is 0 bytes inside a block of size 400 free'd
```

```
==17777==    at 0x483CA3F: free (in
/usr/lib/x86_64-linux-gnu/valgrind/vgpreload_memcheck-amd64-linux.so)
==17777==    by 0x1091AE: main (prog.c:15)
==17777==  Block was alloc'd at
==17777==    at 0x483B7F3: malloc (in
/usr/lib/x86_64-linux-gnu/valgrind/vgpreload_memcheck-amd64-linux.so)
==17777==    by 0x10919E: main (prog.c:13)
```

val3.c :

```
==17960== Invalid free() / delete / delete[] / realloc()
==17960==    at 0x483CA3F: free (in
/usr/lib/x86_64-linux-gnu/valgrind/vgpreload_memcheck-amd64-linux.so)
==17960==    by 0x109197: main (prog.c:16)
==17960==  Address 0x1ffefffedc is on thread 1's stack
==17960==  in frame #1, created by main (prog.c:7)
```

val4.c:

```
==18078== Invalid free() / delete / delete[] / realloc()
==18078==    at 0x483CA3F: free (in
/usr/lib/x86_64-linux-gnu/valgrind/vgpreload_memcheck-amd64-linux.so)
==18078==    by 0x10919A: main (prog.c:16)
==18078==  Address 0x4a56040 is 0 bytes inside a block of size 400 free'd
==18078==    at 0x483CA3F: free (in
/usr/lib/x86_64-linux-gnu/valgrind/vgpreload_memcheck-amd64-linux.so)
==18078==    by 0x10918E: main (prog.c:14)
==18078==  Block was alloc'd at
==18078==    at 0x483B7F3: malloc (in
/usr/lib/x86_64-linux-gnu/valgrind/vgpreload_memcheck-amd64-linux.so)
==18078==    by 0x10917E: main (prog.c:12)
==
```

val5.c:

```
==18224== 400 bytes in 1 blocks are definitely lost in loss record 1 of 1
==18224==    at 0x483B7F3: malloc (in
/usr/lib/x86_64-linux-gnu/valgrind/vgpreload_memcheck-amd64-linux.so)
==18224==    by 0x10917E: main (prog.c:12)
==18224==
```

# References

1. https://www.cprogramming.com/debugging/valgrind.html