McGill School of Computer Science

COMP310/ECSE427 Lab4

Advanced Debugging in C

Jason Zixu Zhou

McGill Sep-20 2024

Overview

- **Concurrency in C Programs**
- **Common Concurrency IssuesTools for Debugging**
  - ThreadSanitizer (TSan)
  - GDB
  - Valgrind (Helgrind)
- **Examples**
  - Race Conditions
  - Deadlocks
  - Atomic Operations

What is Concurrency?

- **Concurrency**: Multiple tasks make progress, but not necessarily at the same time. They are *interleaved*.
  - Example: A single-core CPU switches between multiple tasks.
- **Parallelism**: Multiple tasks run *simultaneously* on multiple cores or processors.
  - Example: A multi-core CPU running multiple threads at the same time.
- Concurrency is about *dealing with* lots of tasks at once.
- Parallelism is about *doing* lots of tasks at once.
- Not equivalent to parallelism (Concurrency ≠ Parallelism)

Common Concurrency Issues

- **Race Conditions**
  - When multiple threads access shared data concurrently without proper synchronization
- **Deadlocks**
  - When two or more threads are waiting for each other to release resources
- **Atomic Violations**
  - Non-atomic operations interrupted by another thread

Tools for Debugging Concurrency

GDB: Used for interactive debugging.

Good for step-by-step execution and conditional breakpoints.

Valgrind: Used for detecting memory management issues.

Ideal for finding memory leaks and memory corruption.

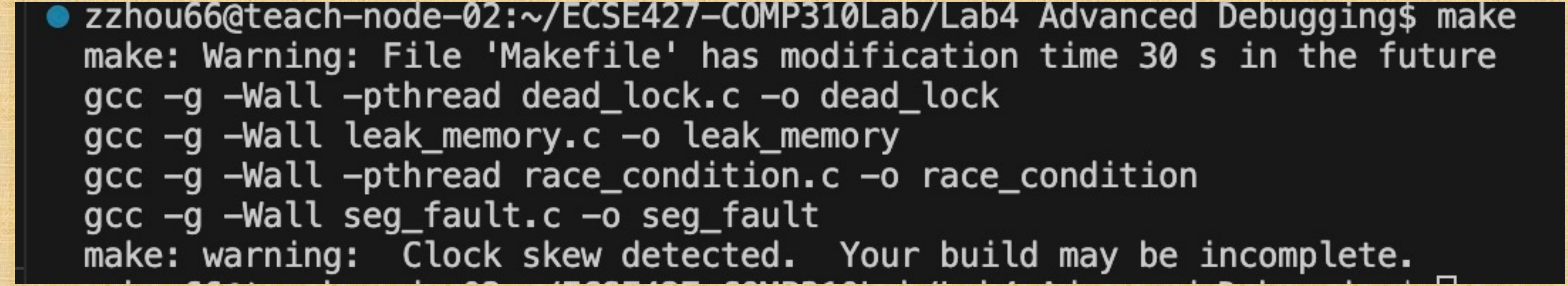
Helgrind: Used for detecting concurrency issues in multithreaded applications.

Focuses on race conditions and deadlocks.

When to Use Which Tool?

- **Memory Management Issues**: Choose Valgrind.
- **Concurrency/Synchronization Issues**: Choose Helgrind.
- **Interactive Step-by-Step Debugging**: Choose GDB.
- **Complex Problems**: Combine tools for comprehensive analysis.

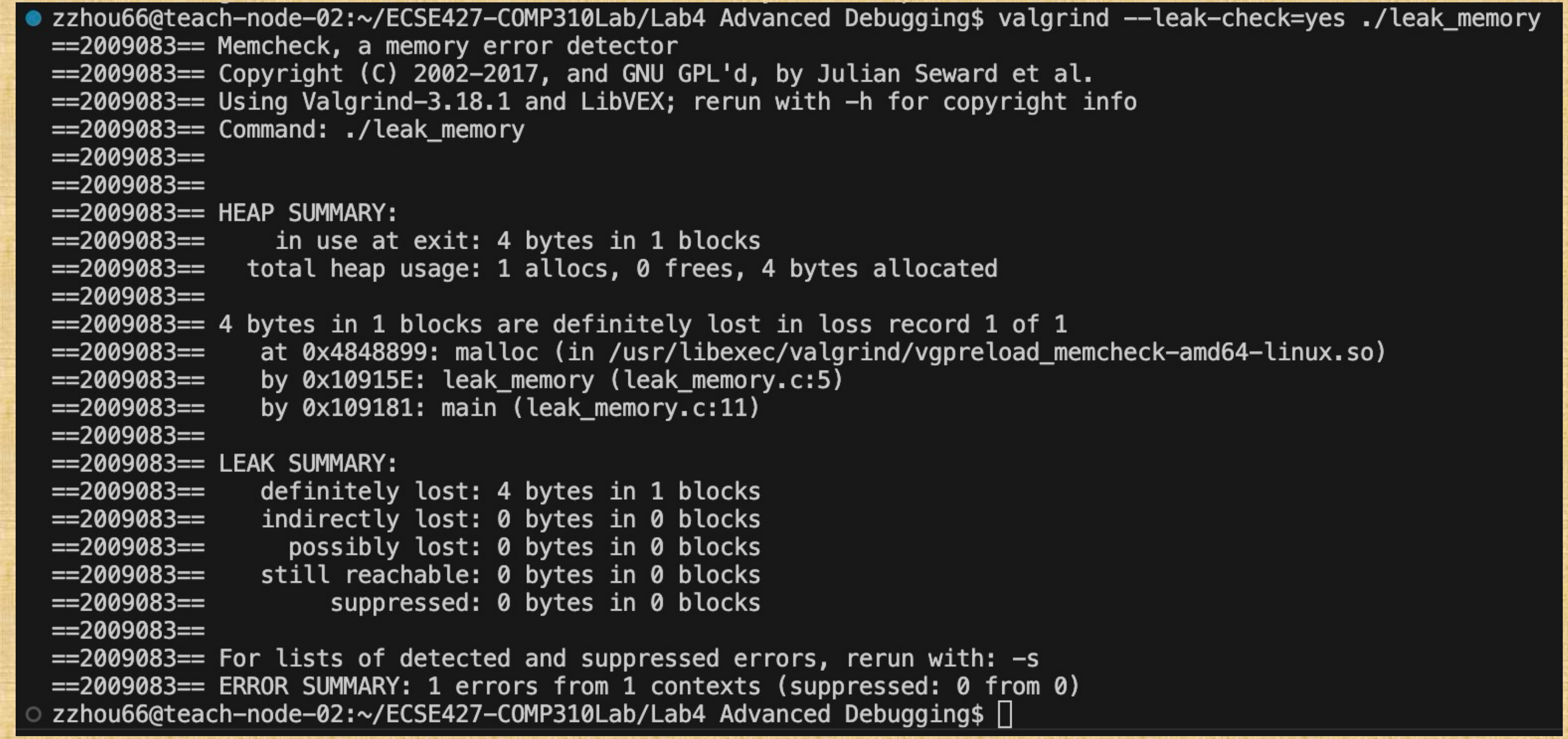
Build with Makefile



```
zzhou66@teach-node-02:~/ECSE427-COMP310Lab/Lab4 Advanced Debugging$ make
make: Warning: File 'Makefile' has modification time 30 s in the future
gcc -g -Wall -pthread dead_lock.c -o dead_lock
gcc -g -Wall leak_memory.c -o leak_memory
gcc -g -Wall -pthread race_condition.c -o race_condition
gcc -g -Wall seg_fault.c -o seg_fault
make: warning:  Clock skew detected.  Your build may be incomplete.
```

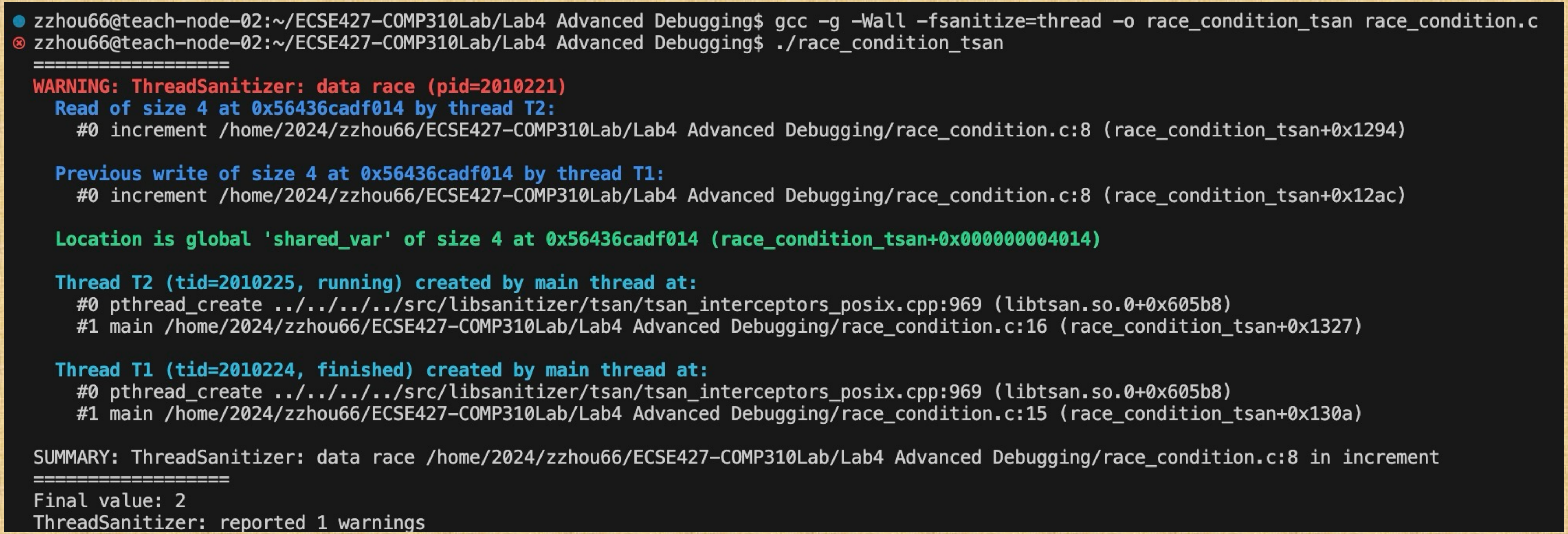
Using Valgrind - Memory Leak Example

- valgrind --leak-check=yes ./leak_memory



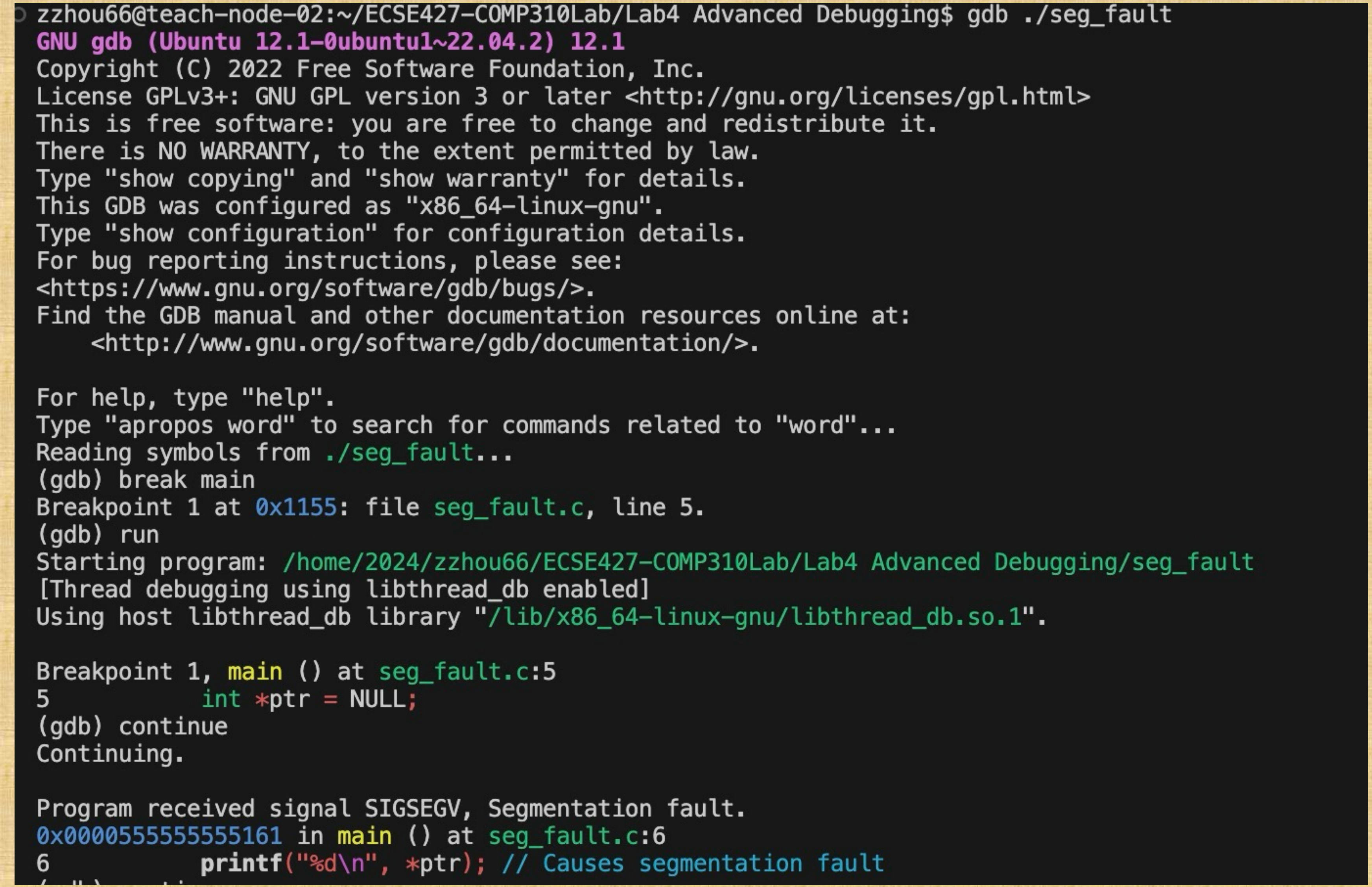
```
zzhou66@teach-node-02:~/ECSE427-COMP310Lab/Lab4 Advanced Debugging$ valgrind --leak-check=yes ./leak_memory
==2009083== Memcheck, a memory error detector
==2009083== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==2009083== Using Valgrind-3.18.1 and LibVEX; rerun with -h for copyright info
==2009083== Command: ./leak_memory
==2009083==
==2009083==
==2009083== HEAP SUMMARY:
==2009083==     in use at exit: 4 bytes in 1 blocks
==2009083==   total heap usage: 1 allocs, 0 frees, 4 bytes allocated
==2009083==
==2009083== 4 bytes in 1 blocks are definitely lost in loss record 1 of 1
==2009083==    at 0x4848899: malloc (in /usr/libexec/valgrind/vgpreload_memcheck-amd64-linux.so)
==2009083==    by 0x10915E: leak_memory (leak_memory.c:5)
==2009083==    by 0x109181: main (leak_memory.c:11)
==2009083==
==2009083== LEAK SUMMARY:
==2009083==    definitely lost: 4 bytes in 1 blocks
==2009083==    indirectly lost: 0 bytes in 0 blocks
==2009083==      possibly lost: 0 bytes in 0 blocks
==2009083==    still reachable: 0 bytes in 0 blocks
==2009083==         suppressed: 0 bytes in 0 blocks
==2009083==
==2009083== For lists of detected and suppressed errors, rerun with: -s
==2009083== ERROR SUMMARY: 1 errors from 1 contexts (suppressed: 0 from 0)
zzhou66@teach-node-02:~/ECSE427-COMP310Lab/Lab4 Advanced Debugging$
```

Detecting Race Conditions with ThreadSanitizer



```
● zzhou66@teach-node-02:~/ECSE427-COMP310Lab/Lab4 Advanced Debugging$ gcc -g -Wall -fsanitize=thread -o race_condition_tsan race_condition.c
⊗ zzhou66@teach-node-02:~/ECSE427-COMP310Lab/Lab4 Advanced Debugging$ ./race_condition_tsan
  ==================
  WARNING: ThreadSanitizer: data race (pid=2010221)
    Read of size 4 at 0x56436cadf014 by thread T2:
      #0 increment /home/2024/zzhou66/ECSE427-COMP310Lab/Lab4 Advanced Debugging/race_condition.c:8 (race_condition_tsan+0x1294)

    Previous write of size 4 at 0x56436cadf014 by thread T1:
      #0 increment /home/2024/zzhou66/ECSE427-COMP310Lab/Lab4 Advanced Debugging/race_condition.c:8 (race_condition_tsan+0x12ac)

    Location is global 'shared_var' of size 4 at 0x56436cadf014 (race_condition_tsan+0x000000004014)

    Thread T2 (tid=2010225, running) created by main thread at:
      #0 pthread_create ../../../../src/libsanitizer/tsan/tsan_interceptors_posix.cpp:969 (libtsan.so.0+0x605b8)
      #1 main /home/2024/zzhou66/ECSE427-COMP310Lab/Lab4 Advanced Debugging/race_condition.c:16 (race_condition_tsan+0x1327)

    Thread T1 (tid=2010224, finished) created by main thread at:
      #0 pthread_create ../../../../src/libsanitizer/tsan/tsan_interceptors_posix.cpp:969 (libtsan.so.0+0x605b8)
      #1 main /home/2024/zzhou66/ECSE427-COMP310Lab/Lab4 Advanced Debugging/race_condition.c:15 (race_condition_tsan+0x130a)

  SUMMARY: ThreadSanitizer: data race /home/2024/zzhou66/ECSE427-COMP310Lab/Lab4 Advanced Debugging/race_condition.c:8 in increment
  ==================
  Final value: 2
  ThreadSanitizer: reported 1 warnings
```

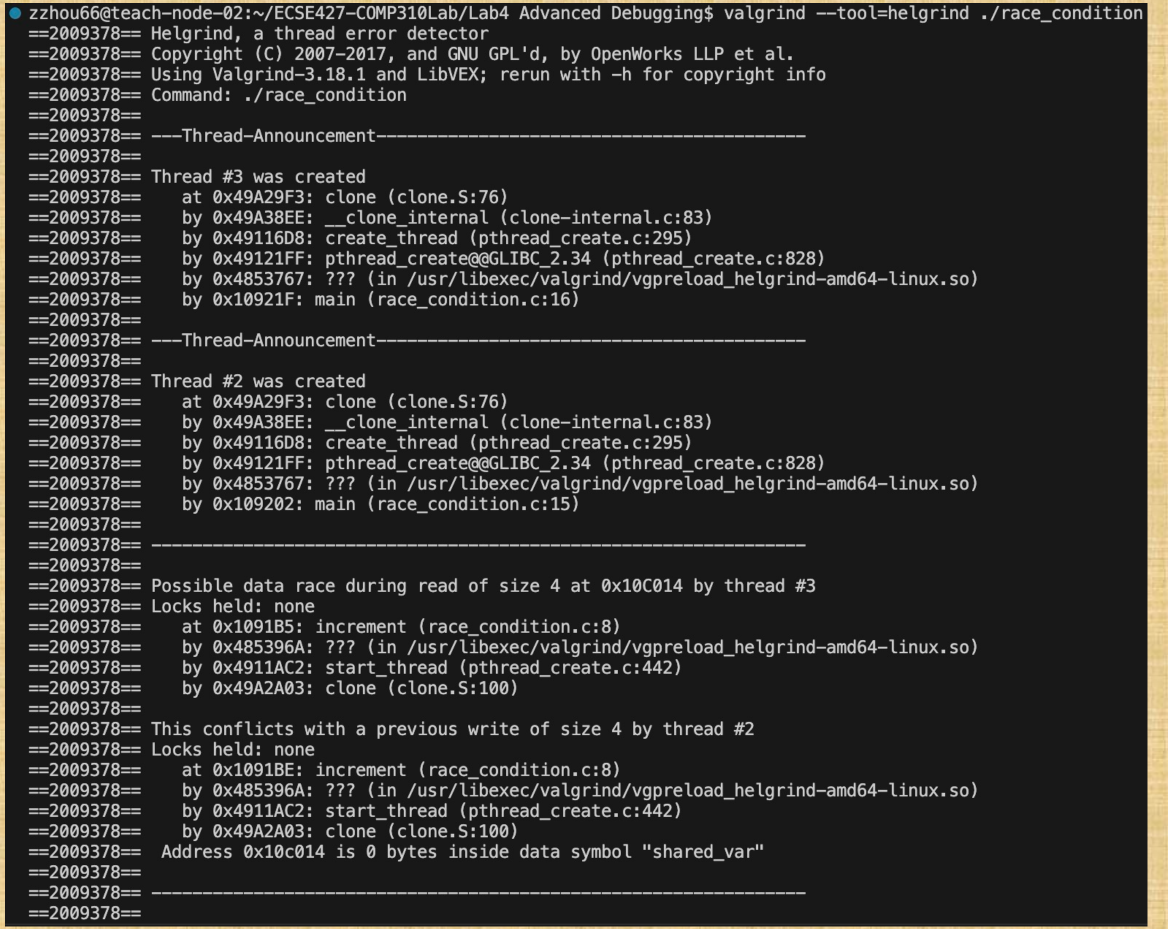
GDB - Debugging Segmentation Faults



```
zzhou66@teach-node-02:~/ECSE427-COMP310Lab/Lab4 Advanced Debugging$ gdb ./seg_fault
GNU gdb (Ubuntu 12.1-0ubuntu1~22.04.2) 12.1
Copyright (C) 2022 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 ./seg_fault...
(gdb) break main
Breakpoint 1 at 0x1155: file seg_fault.c, line 5.
(gdb) run
Starting program: /home/2024/zzhou66/ECSE427-COMP310Lab/Lab4 Advanced Debugging/seg_fault
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, main () at seg_fault.c:5
5           int *ptr = NULL;
(gdb) continue
Continuing.

Program received signal SIGSEGV, Segmentation fault.
0x0000555555555161 in main () at seg_fault.c:6
6           printf("%d\n", *ptr); // Causes segmentation fault
```

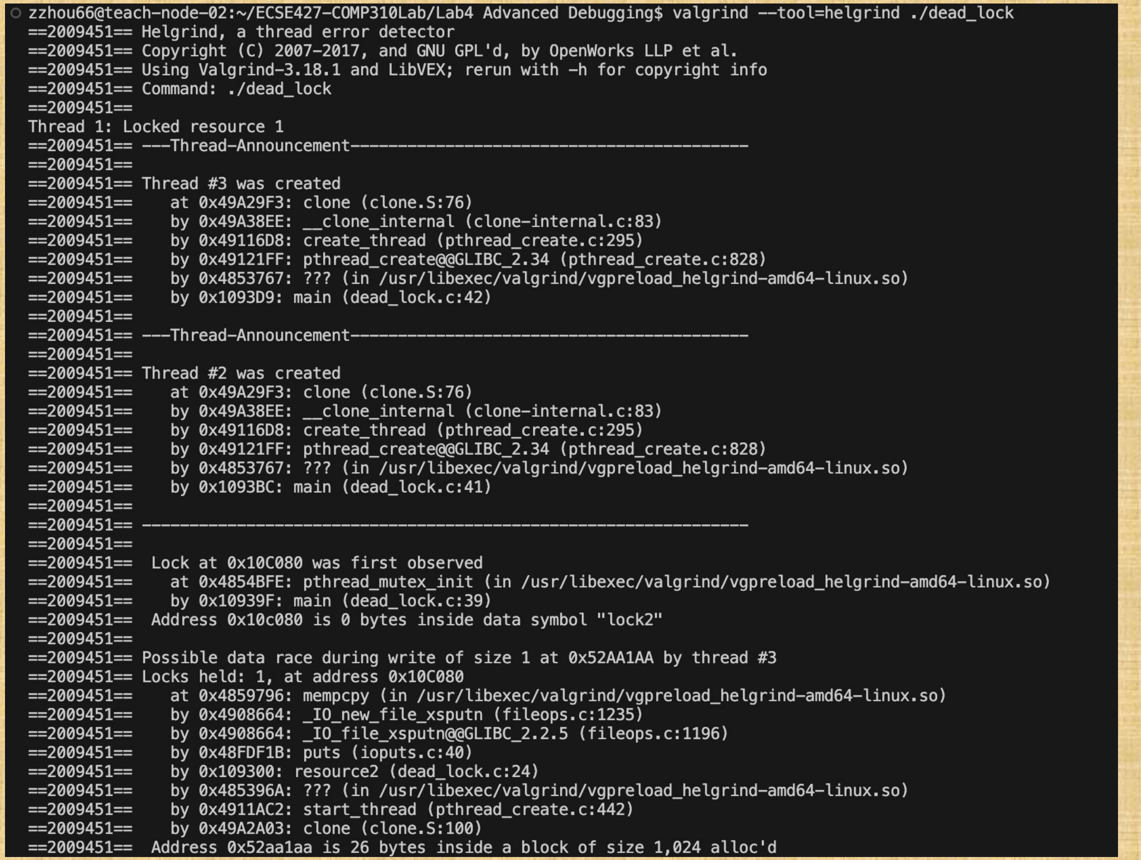
Using Helgrind - Race Condition Example

- valgrind --tool=helgrind ./race_condition

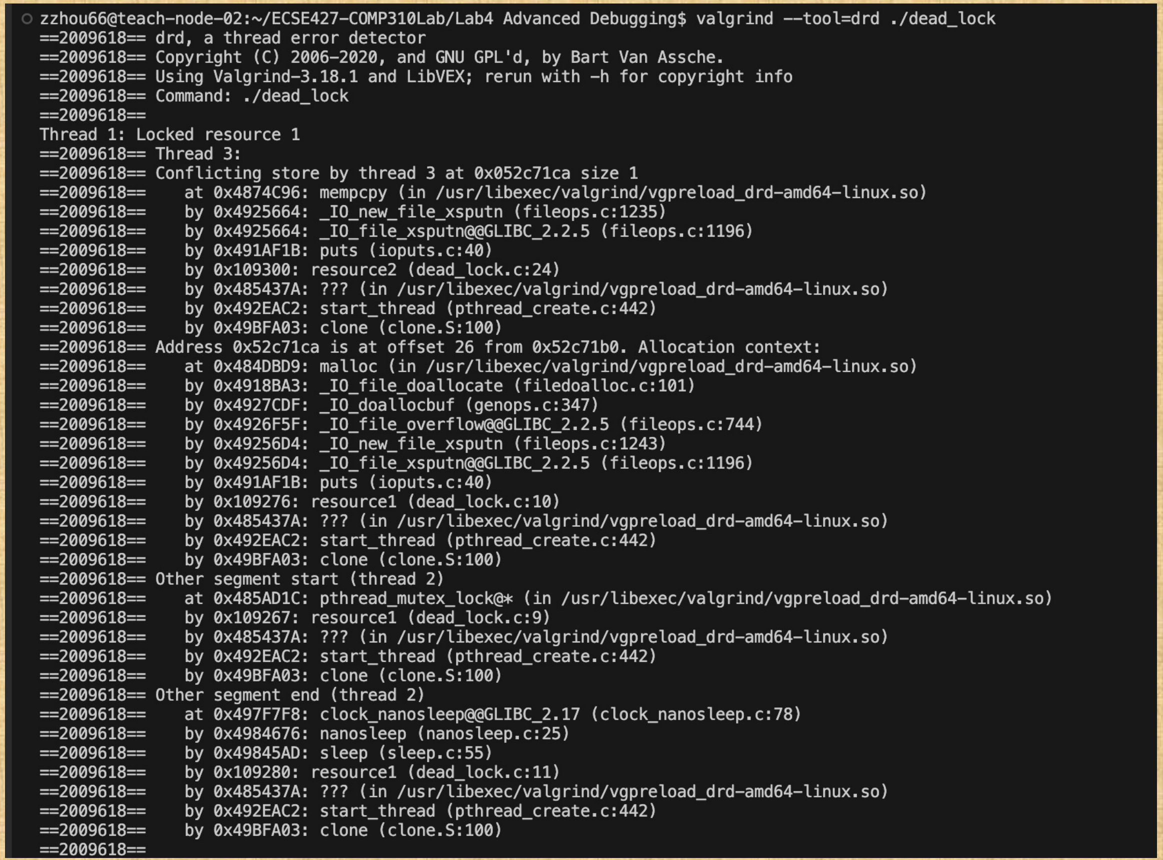


```
zzhou66@teach-node-02:~/ECSE427-COMP310Lab/Lab4 Advanced Debugging$ valgrind --tool=helgrind ./race_condition
==2009378== Helgrind, a thread error detector
==2009378== Copyright (C) 2007-2017, and GNU GPL'd, by OpenWorks LLP et al.
==2009378== Using Valgrind-3.18.1 and LibVEX; rerun with -h for copyright info
==2009378== Command: ./race_condition
==2009378==
==2009378== ---Thread-Announcement------------------------------------------
==2009378==
==2009378== Thread #3 was created
==2009378==    at 0x49A29F3: clone (clone.S:76)
==2009378==    by 0x49A38EE: __clone_internal (clone-internal.c:83)
==2009378==    by 0x49116D8: create_thread (pthread_create.c:295)
==2009378==    by 0x49121FF: pthread_create@@GLIBC_2.34 (pthread_create.c:828)
==2009378==    by 0x4853767: ??? (in /usr/libexec/valgrind/vgpreload_helgrind-amd64-linux.so)
==2009378==    by 0x10921F: main (race_condition.c:16)
==2009378==
==2009378== ---Thread-Announcement------------------------------------------
==2009378==
==2009378== Thread #2 was created
==2009378==    at 0x49A29F3: clone (clone.S:76)
==2009378==    by 0x49A38EE: __clone_internal (clone-internal.c:83)
==2009378==    by 0x49116D8: create_thread (pthread_create.c:295)
==2009378==    by 0x49121FF: pthread_create@@GLIBC_2.34 (pthread_create.c:828)
==2009378==    by 0x4853767: ??? (in /usr/libexec/valgrind/vgpreload_helgrind-amd64-linux.so)
==2009378==    by 0x109202: main (race_condition.c:15)
==2009378==
==2009378== ----------------------------------------------------------------
==2009378==
==2009378== Possible data race during read of size 4 at 0x10C014 by thread #3
==2009378== Locks held: none
==2009378==    at 0x1091B5: increment (race_condition.c:8)
==2009378==    by 0x485396A: ??? (in /usr/libexec/valgrind/vgpreload_helgrind-amd64-linux.so)
==2009378==    by 0x4911AC2: start_thread (pthread_create.c:442)
==2009378==    by 0x49A2A03: clone (clone.S:100)
==2009378==
==2009378== This conflicts with a previous write of size 4 by thread #2
==2009378== Locks held: none
==2009378==    at 0x1091BE: increment (race_condition.c:8)
==2009378==    by 0x485396A: ??? (in /usr/libexec/valgrind/vgpreload_helgrind-amd64-linux.so)
==2009378==    by 0x4911AC2: start_thread (pthread_create.c:442)
==2009378==    by 0x49A2A03: clone (clone.S:100)
==2009378==  Address 0x10c014 is 0 bytes inside data symbol "shared_var"
==2009378==
==2009378== ----------------------------------------------------------------
==2009378==
```

Exercise: Dead lock



```
○ zzhou66@teach-node-02:~/ECSE427-COMP310Lab/Lab4 Advanced Debugging$ valgrind --tool=helgrind ./dead_lock
==2009451== Helgrind, a thread error detector
==2009451== Copyright (C) 2007-2017, and GNU GPL'd, by OpenWorks LLP et al.
==2009451== Using Valgrind-3.18.1 and LibVEX; rerun with -h for copyright info
==2009451== Command: ./dead_lock
==2009451==
Thread 1: Locked resource 1
==2009451== ---Thread-Announcement------------------------------------------
==2009451==
==2009451== Thread #3 was created
==2009451==    at 0x49A29F3: clone (clone.S:76)
==2009451==    by 0x49A38EE: __clone_internal (clone-internal.c:83)
==2009451==    by 0x49116D8: create_thread (pthread_create.c:295)
==2009451==    by 0x49121FF: pthread_create@@GLIBC_2.34 (pthread_create.c:828)
==2009451==    by 0x4853767: ??? (in /usr/libexec/valgrind/vgpreload_helgrind-amd64-linux.so)
==2009451==    by 0x1093D9: main (dead_lock.c:42)
==2009451==
==2009451== ---Thread-Announcement------------------------------------------
==2009451==
==2009451== Thread #2 was created
==2009451==    at 0x49A29F3: clone (clone.S:76)
==2009451==    by 0x49A38EE: __clone_internal (clone-internal.c:83)
==2009451==    by 0x49116D8: create_thread (pthread_create.c:295)
==2009451==    by 0x49121FF: pthread_create@@GLIBC_2.34 (pthread_create.c:828)
==2009451==    by 0x4853767: ??? (in /usr/libexec/valgrind/vgpreload_helgrind-amd64-linux.so)
==2009451==    by 0x1093BC: main (dead_lock.c:41)
==2009451==
==2009451== ----------------------------------------------------------------
==2009451==
==2009451==  Lock at 0x10C080 was first observed
==2009451==    at 0x4854BFE: pthread_mutex_init (in /usr/libexec/valgrind/vgpreload_helgrind-amd64-linux.so)
==2009451==    by 0x10939F: main (dead_lock.c:39)
==2009451==  Address 0x10c080 is 0 bytes inside data symbol "lock2"
==2009451==
==2009451== Possible data race during write of size 1 at 0x52AA1AA by thread #3
==2009451== Locks held: 1, at address 0x10C080
==2009451==    at 0x4859796: mempcpy (in /usr/libexec/valgrind/vgpreload_helgrind-amd64-linux.so)
==2009451==    by 0x4908664: _IO_new_file_xsputn (fileops.c:1235)
==2009451==    by 0x4908664: _IO_file_xsputn@@GLIBC_2.2.5 (fileops.c:1196)
==2009451==    by 0x48FDF1B: puts (ioputs.c:40)
==2009451==    by 0x109300: resource2 (dead_lock.c:24)
==2009451==    by 0x485396A: ??? (in /usr/libexec/valgrind/vgpreload_helgrind-amd64-linux.so)
==2009451==    by 0x4911AC2: start_thread (pthread_create.c:442)
==2009451==    by 0x49A2A03: clone (clone.S:100)
==2009451==  Address 0x52aa1aa is 26 bytes inside a block of size 1,024 alloc'd
```



```
○ zzhou66@teach-node-02:~/ECSE427-COMP310Lab/Lab4 Advanced Debugging$ valgrind --tool=drd ./dead_lock
==2009618== drd, a thread error detector
==2009618== Copyright (C) 2006-2020, and GNU GPL'd, by Bart Van Assche.
==2009618== Using Valgrind-3.18.1 and LibVEX; rerun with -h for copyright info
==2009618== Command: ./dead_lock
==2009618==
Thread 1: Locked resource 1
==2009618== Thread 3:
==2009618== Conflicting store by thread 3 at 0x052c71ca size 1
==2009618==    at 0x4874C96: mempcpy (in /usr/libexec/valgrind/vgpreload_drd-amd64-linux.so)
==2009618==    by 0x4925664: _IO_new_file_xsputn (fileops.c:1235)
==2009618==    by 0x4925664: _IO_file_xsputn@@GLIBC_2.2.5 (fileops.c:1196)
==2009618==    by 0x491AF1B: puts (ioputs.c:40)
==2009618==    by 0x109300: resource2 (dead_lock.c:24)
==2009618==    by 0x485437A: ??? (in /usr/libexec/valgrind/vgpreload_drd-amd64-linux.so)
==2009618==    by 0x492EAC2: start_thread (pthread_create.c:442)
==2009618==    by 0x49BFA03: clone (clone.S:100)
==2009618== Address 0x52c71ca is at offset 26 from 0x52c71b0. Allocation context:
==2009618==    at 0x484DBD9: malloc (in /usr/libexec/valgrind/vgpreload_drd-amd64-linux.so)
==2009618==    by 0x4918BA3: _IO_file_doallocate (filedoalloc.c:101)
==2009618==    by 0x4927CDF: _IO_doallocbuf (genops.c:347)
==2009618==    by 0x4926F5F: _IO_file_overflow@@GLIBC_2.2.5 (fileops.c:744)
==2009618==    by 0x49256D4: _IO_new_file_xsputn (fileops.c:1243)
==2009618==    by 0x49256D4: _IO_file_xsputn@@GLIBC_2.2.5 (fileops.c:1196)
==2009618==    by 0x491AF1B: puts (ioputs.c:40)
==2009618==    by 0x109276: resource1 (dead_lock.c:10)
==2009618==    by 0x485437A: ??? (in /usr/libexec/valgrind/vgpreload_drd-amd64-linux.so)
==2009618==    by 0x492EAC2: start_thread (pthread_create.c:442)
==2009618==    by 0x49BFA03: clone (clone.S:100)
==2009618== Other segment start (thread 2)
==2009618==    at 0x485AD1C: pthread_mutex_lock@* (in /usr/libexec/valgrind/vgpreload_drd-amd64-linux.so)
==2009618==    by 0x109267: resource1 (dead_lock.c:9)
==2009618==    by 0x485437A: ??? (in /usr/libexec/valgrind/vgpreload_drd-amd64-linux.so)
==2009618==    by 0x492EAC2: start_thread (pthread_create.c:442)
==2009618==    by 0x49BFA03: clone (clone.S:100)
==2009618== Other segment end (thread 2)
==2009618==    at 0x497F7F8: clock_nanosleep@@GLIBC_2.17 (clock_nanosleep.c:78)
==2009618==    by 0x4984676: nanosleep (nanosleep.c:25)
==2009618==    by 0x49845AD: sleep (sleep.c:55)
==2009618==    by 0x109280: resource1 (dead_lock.c:11)
==2009618==    by 0x485437A: ??? (in /usr/libexec/valgrind/vgpreload_drd-amd64-linux.so)
==2009618==    by 0x492EAC2: start_thread (pthread_create.c:442)
==2009618==    by 0x49BFA03: clone (clone.S:100)
==2009618==
```