Recitation 11
More Malloc Lab

1 GDB Exercise 1

1. Form pairs and download the handout.

   ```
   $ wget http://www.cs.cmu.edu/~213/activities/rec11b.tar
   $ tar xf rec11b.tar
   $ cd rec11b
   $ make
   ```

2. Run `mdriver` using GDB.

   ```
   $ gdb --args ./mdriver -c ./traces/syn-array-short.rep -D
   ...
   (gdb) run
   ```

   You should see "garbled bytes" errors:

   ```
   ...
   Throughput targets: min=6528, max=11750, benchmark=13056
   Malloc size 9904 on address 0x800000010.
   Malloc size 50084 on address 0x8000026d0.
   ERROR [trace ./traces/syn-array-short.rep, line 7]: block 0 has 8 garbled byte
   s, starting at byte 0
   ...
   Terminated with 14 errors
   [Inferior 1 (process 30988) exited normally]
   ```

3. Set a watchpoint on the first garbled address.

   ```
   (gdb) watch *0x800000010
   (gdb) run
   ```

   ... a few `continues` ...

   ```
   Hardware watchpoint 1: *0x800000010

   Old value = -7350814
   New value = 9928
   mm_malloc (size=50084) at mm.c:276
   276         dbg_printf("Malloc size %zd on address %p.\n", size, bp);
   (gdb) c
   Continuing.
   Malloc size 50084 on address 0x8000026d0.
   ERROR [trace ./traces/syn-array-short.rep, line 7]: block 0 has 8 garbled byte
   s, starting at byte 0
   ```

4. What happened?

2 GDB Exercise 2

1. Run `mdriver-2` using GDB.

   ```
   $ gdb --args ./mdriver-2 -c traces/syn-array-short.rep
   ...
   (gdb) run
   ```

   You should see this error:

   ```
   Malloc size 9904 on address 0x8000036d0
   ERROR [trace ./traces/syn-array-short.rep, line 5]: Payload (0x8000036d0:0x80000
   5d7f) lies outside heap (0x800000000:0x8000036cf)
   ```

2. Set a watchpoint on the header of the payload.

   ```
   (gdb) watch *0x8000036c8
   (gdb) run
   ...
   Hardware watchpoint 1: *0x8000036c8

   Old value = 1
   New value = 9921
   write_header(block=0x8000036c8, size=9920, alloc=true) at mm-2.c:573
   573     }
   ```

3. Backtrace to see what function called `write_header`.

   ```
   (gdb) bt
   #0  write_header (block=0x8000036c8, size=9920, alloc=true) at mm-2.c:573
   #1  0x0000000000407d93 in place (block=0x8000036c8, asize=9920) at mm-2.c:458
   ...
   ```

4. The writes occurred in `place`. Is `place` implemented incorrectly, or was it given a bad argument?