UCLA Samueli School of Engineering

CS 33

MIDTERM EXAM

All answers should be written on the answer sheet.

All work should be written directly on the exam pages, use the backs of pages if needed.

This is an open book, open notes quiz – but you cannot share books or notes.

We will follow the departmental guidelines on reporting incidents of academic dishonesty.

Keep your eyes on your own exam!

NAME: _____

ID: _____

Problem 1: _____ (15)

Problem 2: _____ (20)

Problem 3: _____ (20)

Problem 4: _____ (20)

Problem 5: _____ (25)

Total: _____ (out of 100)

1. ***This Problem Bytes (15 points)***: Suppose we are implementing a set of procedures to operate on a data structure where 4 signed bytes are packed into a 32-bit unsigned. The following prototype is used:

```
typedef unsigned packed_t;
```

Suppose that variable `x` is declared as type `packed_t`. One function you need to support is summation: you need to create code that will add the 4 signed values together. Suppose that the current implementation is the following:

```
(((x+(x>>16)+(x>>8)+(x>>24))&0xFF)<<24)>>24
```

Let's see how well this code works – for the test values of `x` on your answer sheet, what would be the result of the expression above (write the answers on the answer sheet in hex)?

2. ***Lost at C? (20 points)***: For the C puzzles listed on your answer sheet, determine whether each statement is always true (e.g. true for all values of x and y). If the statement can be false, give a counter example value for x or y that would make the statement false. Assume that x and y are signed integers and could have any value. For example, for the puzzle

`x < 0` → `-x > 0`

the answer would be:

FALSE

And the counter example would be:

x = Tmin

3. ***Down in the Dumps (20 points)***: Consider the following data structure:

```
short ** table0[8];
```

This array of pointers is initialized with the following code:

```
for (k=0; k<8; k++) {
  table0[k]=malloc(5*sizeof(short*));
  for (i=0; i<5; i++) {
    table0[k][i]=malloc(5*sizeof(short));
    for (j=0; j<5; j++) {
      table0[k][i][j]=rand()%100;
    }
  }
}
```

And then accessed with the following code:

```
void table_lookup(int x, int w, int v)
{
  int index;

  index=(x ^(x>>3))&7;

  printf("%d[w][v]:%d\n", index, table0[index][w][v]);
}
```

For the values of x, w, and v given on your answer sheet, use the gdb interaction and memory dump from the program in execution below to figure out the value of table0[index][w][v] in the code above. Answer the questions on your answer sheet and show any work below.

gdb Interaction:

```
(gdb) x/64xb &table0
0x6022a0: 0x10 0x35 0x60 0x00 0x00 0x00 0x00 0x00
0x6022a8: 0xe0 0x35 0x60 0x00 0x00 0x00 0x00 0x00
0x6022b0: 0xb0 0x36 0x60 0x00 0x00 0x00 0x00 0x00
0x6022b8: 0x80 0x37 0x60 0x00 0x00 0x00 0x00 0x00
0x6022c0: 0x50 0x38 0x60 0x00 0x00 0x00 0x00 0x00
0x6022c8: 0x20 0x39 0x60 0x00 0x00 0x00 0x00 0x00
0x6022d0: 0xf0 0x39 0x60 0x00 0x00 0x00 0x00 0x00
0x6022d8: 0xc0 0x3a 0x60 0x00 0x00 0x00 0x00 0x00
```

Memory Dump:

```
0x603500: 0xb0 0x34 0x60 0x00 0x00 0x00 0x00 0x00
0x603508: 0x31 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603510: 0x40 0x35 0x60 0x00 0x00 0x00 0x00 0x00
0x603518: 0x60 0x35 0x60 0x00 0x00 0x00 0x00 0x00
0x603520: 0x80 0x35 0x60 0x00 0x00 0x00 0x00 0x00
0x603528: 0xa0 0x35 0x60 0x00 0x00 0x00 0x00 0x00
0x603530: 0xc0 0x35 0x60 0x00 0x00 0x00 0x00 0x00
0x603538: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603540: 0x0b 0x00 0x44 0x00 0x43 0x00 0x1d 0x00
0x603548: 0x52 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603550: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603558: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603560: 0x1e 0x00 0x3e 0x00 0x17 0x00 0x43 0x00
0x603568: 0x23 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603570: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603578: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603580: 0x1d 0x00 0x02 0x00 0x16 0x00 0x3a 0x00
0x603588: 0x45 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603590: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603598: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6035a0: 0x43 0x00 0x5d 0x00 0x38 0x00 0x0b 0x00
0x6035a8: 0x2a 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6035b0: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6035b8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6035c0: 0x1d 0x00 0x49 0x00 0x15 0x00 0x13 0x00
0x6035c8: 0x54 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6035d0: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6035d8: 0x31 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6035e0: 0x10 0x36 0x60 0x00 0x00 0x00 0x00 0x00
0x6035e8: 0x30 0x36 0x60 0x00 0x00 0x00 0x00 0x00
0x6035f0: 0x50 0x36 0x60 0x00 0x00 0x00 0x00 0x00
0x6035f8: 0x70 0x36 0x60 0x00 0x00 0x00 0x00 0x00
0x603600: 0x90 0x36 0x60 0x00 0x00 0x00 0x00 0x00
0x603608: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603610: 0x25 0x00 0x62 0x00 0x18 0x00 0x0f 0x00
0x603618: 0x46 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603620: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603628: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603630: 0x0d 0x00 0x1a 0x00 0x5b 0x00 0x50 0x00
0x603638: 0x38 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603640: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603648: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603650: 0x49 0x00 0x3e 0x00 0x46 0x00 0x60 0x00
0x603658: 0x51 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603660: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603668: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603670: 0x05 0x00 0x19 0x00 0x54 0x00 0x1b 0x00
```

```
0x603678: 0x24 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603680: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603688: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603690: 0x05 0x00 0x2e 0x00 0x1d 0x00 0x0d 0x00
0x603698: 0x39 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6036a0: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6036a8: 0x31 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6036b0: 0xe0 0x36 0x60 0x00 0x00 0x00 0x00 0x00
0x6036b8: 0x00 0x37 0x60 0x00 0x00 0x00 0x00 0x00
0x6036c0: 0x20 0x37 0x60 0x00 0x00 0x00 0x00 0x00
0x6036c8: 0x40 0x37 0x60 0x00 0x00 0x00 0x00 0x00
0x6036d0: 0x60 0x37 0x60 0x00 0x00 0x00 0x00 0x00
0x6036d8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6036e0: 0x18 0x00 0x5f 0x00 0x52 0x00 0x2d 0x00
0x6036e8: 0x0e 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6036f0: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6036f8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603700: 0x43 0x00 0x22 0x00 0x40 0x00 0x2b 0x00
0x603708: 0x32 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603710: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603718: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603720: 0x57 0x00 0x08 0x00 0x4c 0x00 0x4e 0x00
0x603728: 0x58 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603730: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603738: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603740: 0x54 0x00 0x03 0x00 0x33 0x00 0x36 0x00
0x603748: 0x63 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603750: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603758: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603760: 0x20 0x00 0x3c 0x00 0x4c 0x00 0x44 0x00
0x603768: 0x27 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603770: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603778: 0x31 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603780: 0xb0 0x37 0x60 0x00 0x00 0x00 0x00 0x00
0x603788: 0xd0 0x37 0x60 0x00 0x00 0x00 0x00 0x00
0x603790: 0xf0 0x37 0x60 0x00 0x00 0x00 0x00 0x00
0x603798: 0x10 0x38 0x60 0x00 0x00 0x00 0x00 0x00
0x6037a0: 0x30 0x38 0x60 0x00 0x00 0x00 0x00 0x00
0x6037a8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6037b0: 0x0c 0x00 0x1a 0x00 0x56 0x00 0x5e 0x00
0x6037b8: 0x27 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6037c0: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6037c8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6037d0: 0x5f 0x00 0x46 0x00 0x22 0x00 0x4e 0x00
0x6037d8: 0x43 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6037e0: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6037e8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6037f0: 0x01 0x00 0x61 0x00 0x02 0x00 0x11 0x00
0x6037f8: 0x5c 0x00 0x00 0x00 0x00 0x00 0x00 0x00
```

```
0x603800: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603808: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603810: 0x34 0x00 0x38 0x00 0x01 0x00 0x50 0x00
0x603818: 0x56 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603820: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603828: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603830: 0x29 0x00 0x41 0x00 0x59 0x00 0x2c 0x00
0x603838: 0x13 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603840: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603848: 0x31 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603850: 0x80 0x38 0x60 0x00 0x00 0x00 0x00 0x00
0x603858: 0xa0 0x38 0x60 0x00 0x00 0x00 0x00 0x00
0x603860: 0xc0 0x38 0x60 0x00 0x00 0x00 0x00 0x00
0x603868: 0xe0 0x38 0x60 0x00 0x00 0x00 0x00 0x00
0x603870: 0x00 0x39 0x60 0x00 0x00 0x00 0x00 0x00
0x603878: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603880: 0x28 0x00 0x1d 0x00 0x1f 0x00 0x11 0x00
0x603888: 0x61 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603890: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603898: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6038a0: 0x47 0x00 0x51 0x00 0x4b 0x00 0x09 0x00
0x6038a8: 0x1b 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6038b0: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6038b8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6038c0: 0x43 0x00 0x38 0x00 0x61 0x00 0x35 0x00
0x6038c8: 0x56 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6038d0: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6038d8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6038e0: 0x41 0x00 0x06 0x00 0x53 0x00 0x13 0x00
0x6038e8: 0x18 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6038f0: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6038f8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603900: 0x1c 0x00 0x47 0x00 0x20 0x00 0x1d 0x00
0x603908: 0x03 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603910: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603918: 0x31 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603920: 0x50 0x39 0x60 0x00 0x00 0x00 0x00 0x00
0x603928: 0x70 0x39 0x60 0x00 0x00 0x00 0x00 0x00
0x603930: 0x90 0x39 0x60 0x00 0x00 0x00 0x00 0x00
0x603938: 0xb0 0x39 0x60 0x00 0x00 0x00 0x00 0x00
0x603940: 0xd0 0x39 0x60 0x00 0x00 0x00 0x00 0x00
0x603948: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603950: 0x13 0x00 0x46 0x00 0x44 0x00 0x08 0x00
0x603958: 0x0f 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603960: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603968: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603970: 0x28 0x00 0x31 0x00 0x60 0x00 0x17 0x00
0x603978: 0x12 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603980: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
```

```
0x603988: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603990: 0x2d 0x00 0x2e 0x00 0x33 0x00 0x15 0x00
0x603998: 0x37 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6039a0: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6039a8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6039b0: 0x4f 0x00 0x58 0x00 0x40 0x00 0x1c 0x00
0x6039b8: 0x29 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6039c0: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6039c8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6039d0: 0x32 0x00 0x5d 0x00 0x00 0x00 0x22 0x00
0x6039d8: 0x40 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6039e0: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6039e8: 0x31 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6039f0: 0x20 0x3a 0x60 0x00 0x00 0x00 0x00 0x00
0x6039f8: 0x40 0x3a 0x60 0x00 0x00 0x00 0x00 0x00
0x603a00: 0x60 0x3a 0x60 0x00 0x00 0x00 0x00 0x00
0x603a08: 0x80 0x3a 0x60 0x00 0x00 0x00 0x00 0x00
0x603a10: 0xa0 0x3a 0x60 0x00 0x00 0x00 0x00 0x00
0x603a18: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603a20: 0x18 0x00 0x0e 0x00 0x57 0x00 0x38 0x00
0x603a28: 0x2b 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603a30: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603a38: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603a40: 0x5b 0x00 0x1b 0x00 0x41 0x00 0x3b 0x00
0x603a48: 0x24 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603a50: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603a58: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603a60: 0x20 0x00 0x33 0x00 0x25 0x00 0x1c 0x00
0x603a68: 0x4b 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603a70: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603a78: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603a80: 0x07 0x00 0x4a 0x00 0x15 0x00 0x3a 0x00
0x603a88: 0x5f 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603a90: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603a98: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603aa0: 0x1d 0x00 0x25 0x00 0x23 0x00 0x5d 0x00
0x603aa8: 0x12 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603ab0: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603ab8: 0x31 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603ac0: 0xf0 0x3a 0x60 0x00 0x00 0x00 0x00 0x00
0x603ac8: 0x10 0x3b 0x60 0x00 0x00 0x00 0x00 0x00
0x603ad0: 0x30 0x3b 0x60 0x00 0x00 0x00 0x00 0x00
0x603ad8: 0x50 0x3b 0x60 0x00 0x00 0x00 0x00 0x00
0x603ae0: 0x70 0x3b 0x60 0x00 0x00 0x00 0x00 0x00
0x603ae8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603af0: 0x1c 0x00 0x2b 0x00 0x0b 0x00 0x1c 0x00
0x603af8: 0x1d 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603b00: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603b08: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
```

```
0x603b10: 0x4c 0x00 0x04 0x00 0x2b 0x00 0x3f 0x00
0x603b18: 0x0d 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603b20: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603b28: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603b30: 0x26 0x00 0x06 0x00 0x28 0x00 0x04 0x00
0x603b38: 0x12 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603b40: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603b48: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603b50: 0x1c 0x00 0x58 0x00 0x45 0x00 0x11 0x00
0x603b58: 0x11 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603b60: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603b68: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603b70: 0x60 0x00 0x18 0x00 0x2b 0x00 0x46 0x00
0x603b78: 0x53 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603b80: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603b88: 0x81 0x04 0x02 0x00 0x00 0x00 0x00 0x00
```

4. ***Mineshafts and Manticores (20 points)***: You are playing a new role playing game called Mineshafts and Manticores, and you are trying to figure out how to defeat the manticore (a large monster). There are different heroes in the game, and different weapons the heroes can wield – but you need the right combination of hero and weapon to beat the manticore. You discover a leak of the source code that tells you that the game uses a lot of "magic numbers" in its code. For example, this #define statement:

```
#define MANTICORE 43
```

means that wherever the string MANTICORE is in the code, it is substituted by 43 in the preprocessor of the compiler. For example, in this code sequence the source code reads:

```
if (monster == MANTICORE)
  if (manticoreHandler(hero,weapon))
    printf("You defeated the manticore!\n");
  else
    printf("The manticore defeated you!\n");
```

If the monster is a MANTICORE, the function manticoreHandler() is invoked to see if you win or lose. But the actual assembly code would not have the term MANTICORE in it, but would instead just compare against the value 43, as such:

```
cmp    $0x2b,%ebp
```

The variables monster, hero, and weapon are all declared as integers:

```
int monster;
int hero;
int weapon;
```

And so the code will actually check if (monster == 43) since MANTICORE is replaced with 43 because of the #define statement.

The game defines the following heroes:

```
#define PALADIN 360
#define CAVALIER 363
#define CHAMPION 362
#define KNIGHT 359
#define BERSERKER 358
#define GLADIATOR 365
```

The game defines the following weapons:

```
#define SPEAR 10
#define AXE 12
#define MACE 14
#define SWORD 8
#define HALBERD 6
#define GLAIVE 17
```

You have disassembled manticoreHandler():

```
00000000004005d0 <manticoreHandler>:
  4005d0:       81 ef 66 01 00 00       sub    $0x166,%edi
  4005d6:       83 ff 07                cmp    $0x7,%edi
  4005d9:       77 5d                   ja     400638
  4005db:       ff 24 fd d0 06 40 00    jmpq   *0x4006d0(,%rdi,8)
  4005e2:       66 0f 1f 44 00 00       nopw   0x0(%rax,%rax,1)
  4005e8:       31 c0                   xor    %eax,%eax
  4005ea:       83 fe 0c                cmp    $0xc,%esi
  4005ed:       0f 94 c0                sete   %al
  4005f0:       c3                      retq
  4005f1:       0f 1f 80 00 00 00 00    nopl   0x0(%rax)
  4005f8:       31 c0                   xor    %eax,%eax
  4005fa:       83 fe 0a                cmp    $0xa,%esi
  4005fd:       0f 94 c0                sete   %al
  400600:       c3                      retq
  400601:       0f 1f 80 00 00 00 00    nopl   0x0(%rax)
  400608:       31 c0                   xor    %eax,%eax
  40060a:       83 fe 06                cmp    $0x6,%esi
  40060d:       0f 94 c0                sete   %al
  400610:       c3                      retq
  400611:       0f 1f 80 00 00 00 00    nopl   0x0(%rax)
  400618:       31 c0                   xor    %eax,%eax
  40061a:       83 fe 11                cmp    $0x11,%esi
  40061d:       0f 94 c0                sete   %al
  400620:       c3                      retq
  400621:       0f 1f 80 00 00 00 00    nopl   0x0(%rax)
  400628:       31 c0                   xor    %eax,%eax
  40062a:       83 fe 0e                cmp    $0xe,%esi
  40062d:       0f 94 c0                sete   %al
  400630:       c3                      retq
  400631:       0f 1f 80 00 00 00 00    nopl   0x0(%rax)
  400638:       31 c0                   xor    %eax,%eax
  40063a:       c3                      retq
  40063b:       0f 1f 44 00 00          nopl   0x0(%rax,%rax,1)
```

Using your knowledge of x86-64, can you figure out how to beat the manticore? This memory dump may help:

```
(gdb) x/64xb 0x4006d0
0x4006d0: 0xf8 0x05 0x40 0x00 0x00 0x00 0x00 0x00
0x4006d8: 0x08 0x06 0x40 0x00 0x00 0x00 0x00 0x00
0x4006e0: 0x18 0x06 0x40 0x00 0x00 0x00 0x00 0x00
0x4006e8: 0x38 0x06 0x40 0x00 0x00 0x00 0x00 0x00
0x4006f0: 0x18 0x06 0x40 0x00 0x00 0x00 0x00 0x00
0x4006f8: 0x28 0x06 0x40 0x00 0x00 0x00 0x00 0x00
0x400700: 0x38 0x06 0x40 0x00 0x00 0x00 0x00 0x00
0x400708: 0xe8 0x05 0x40 0x00 0x00 0x00 0x00 0x00
```

5. ***Reaching My Breaking Point (25 points)***: You are analyzing code that has a linked list of this node type:

```
struct node_t {
  short key;
  char * stringy;
  struct node_t * nextptr;
};
```

Here is the x86-64 assembly implementation of a function called search_node(), which searches the linked list for a specific key, and then prints the string `stringy` for the node with that matching key in the linked list:

```
0000000000400837 <search_node>:
  400837:       48 83 ec 08             sub    $0x8,%rsp
  40083b:       48 85 ff                test   %rdi,%rdi
  40083e:       74 36                   je     400876 <search_node+0x3f>
  400840:       0f b7 07                movzwl (%rdi),%eax
  400843:       66 39 f0                cmp    %si,%ax
  400846:       75 1d                   jne    400865 <search_node+0x2e>
  400848:       48 8b 7f 08             mov    0x8(%rdi),%rdi
  40084c:       0f bf f0                movswl %ax,%esi
  40084f:       89 d1                   mov    %edx,%ecx
  400851:       48 89 fa                mov    %rdi,%rdx
  400854:       bf 4f 0b 40 00          mov    $0x400b4f,%edi
  400859:       b8 00 00 00 00          mov    $0x0,%eax
  40085e:       e8 9d fc ff ff          callq  400500 <printf@plt>
  400863:       eb 1b                   jmp    400880 <search_node+0x49>
  400865:       83 c2 01                add    $0x1,%edx
  400868:       0f bf f6                movswl %si,%esi
  40086b:       48 8b 7f 10             mov    0x10(%rdi),%rdi
  40086f:       e8 c3 ff ff ff          callq  400837 <search_node>
  400874:       eb 0a                   jmp    400880 <search_node+0x49>
  400876:       bf 68 0b 40 00          mov    $0x400b68,%edi
  40087b:       e8 70 fc ff ff          callq  4004f0 <puts@plt>
  400880:       48 83 c4 08             add    $0x8,%rsp
  400884:       c3                      retq
```

Using this information, and the three memory dumps below, can you answer the questions listed on your answer sheet?

Memory Dump #1:

```
(gdb) x/2048xb 0x603000
0x603000: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603008: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603010: 0x53 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603018: 0x68 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x603020: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603028: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603030: 0x53 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603038: 0xba 0x0b 0x40 0x00 0x00 0x00 0x00 0x00
```

```
0x603040: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603048: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603050: 0x56 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603058: 0x68 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x603060: 0x10 0x30 0x60 0x00 0x00 0x00 0x00 0x00
0x603068: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603070: 0x56 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603078: 0xf3 0x0b 0x40 0x00 0x00 0x00 0x00 0x00
0x603080: 0x30 0x30 0x60 0x00 0x00 0x00 0x00 0x00
0x603088: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603090: 0x4d 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603098: 0x68 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x6030a0: 0x50 0x30 0x60 0x00 0x00 0x00 0x00 0x00
0x6030a8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6030b0: 0x4d 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6030b8: 0x85 0x0b 0x40 0x00 0x00 0x00 0x00 0x00
0x6030c0: 0x70 0x30 0x60 0x00 0x00 0x00 0x00 0x00
0x6030c8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6030d0: 0x0f 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6030d8: 0x68 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x6030e0: 0x90 0x30 0x60 0x00 0x00 0x00 0x00 0x00
0x6030e8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6030f0: 0x0f 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6030f8: 0x2d 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x603100: 0xb0 0x30 0x60 0x00 0x00 0x00 0x00 0x00
0x603108: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603110: 0x5d 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603118: 0x61 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x603120: 0xd0 0x30 0x60 0x00 0x00 0x00 0x00 0x00
0x603128: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603130: 0x5d 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603138: 0xb4 0x0b 0x40 0x00 0x00 0x00 0x00 0x00
0x603140: 0xf0 0x30 0x60 0x00 0x00 0x00 0x00 0x00
0x603148: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603150: 0x23 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603158: 0x61 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x603160: 0x10 0x31 0x60 0x00 0x00 0x00 0x00 0x00
0x603168: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603170: 0x23 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603178: 0xee 0x0b 0x40 0x00 0x00 0x00 0x00 0x00
0x603180: 0x30 0x31 0x60 0x00 0x00 0x00 0x00 0x00
0x603188: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603190: 0x56 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603198: 0x61 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x6031a0: 0x50 0x31 0x60 0x00 0x00 0x00 0x00 0x00
0x6031a8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6031b0: 0x56 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6031b8: 0x7f 0x0b 0x40 0x00 0x00 0x00 0x00 0x00
0x6031c0: 0x70 0x31 0x60 0x00 0x00 0x00 0x00 0x00
```

```
0x6031c8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6031d0: 0x5c 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6031d8: 0x61 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x6031e0: 0x90 0x31 0x60 0x00 0x00 0x00 0x00 0x00
0x6031e8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6031f0: 0x5c 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6031f8: 0x28 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x603200: 0xb0 0x31 0x60 0x00 0x00 0x00 0x00 0x00
0x603208: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603210: 0x31 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603218: 0x5b 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x603220: 0xd0 0x31 0x60 0x00 0x00 0x00 0x00 0x00
0x603228: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603230: 0x31 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603238: 0xaf 0x0b 0x40 0x00 0x00 0x00 0x00 0x00
0x603240: 0xf0 0x31 0x60 0x00 0x00 0x00 0x00 0x00
0x603248: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603250: 0x15 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603258: 0x5b 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x603260: 0x10 0x32 0x60 0x00 0x00 0x00 0x00 0x00
0x603268: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603270: 0x15 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603278: 0xe7 0x0b 0x40 0x00 0x00 0x00 0x00 0x00
0x603280: 0x30 0x32 0x60 0x00 0x00 0x00 0x00 0x00
0x603288: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603290: 0x3e 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603298: 0x5b 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x6032a0: 0x50 0x32 0x60 0x00 0x00 0x00 0x00 0x00
0x6032a8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6032b0: 0x3e 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6032b8: 0x79 0x0b 0x40 0x00 0x00 0x00 0x00 0x00
0x6032c0: 0x70 0x32 0x60 0x00 0x00 0x00 0x00 0x00
0x6032c8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6032d0: 0x1b 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6032d8: 0x5b 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x6032e0: 0x90 0x32 0x60 0x00 0x00 0x00 0x00 0x00
0x6032e8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6032f0: 0x1b 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6032f8: 0x23 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x603300: 0xb0 0x32 0x60 0x00 0x00 0x00 0x00 0x00
0x603308: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603310: 0x5a 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603318: 0x56 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x603320: 0xd0 0x32 0x60 0x00 0x00 0x00 0x00 0x00
0x603328: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603330: 0x5a 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603338: 0xaa 0x0b 0x40 0x00 0x00 0x00 0x00 0x00
0x603340: 0xf0 0x32 0x60 0x00 0x00 0x00 0x00 0x00
0x603348: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
```

```
0x603350: 0x3b 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603358: 0x56 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x603360: 0x10 0x33 0x60 0x00 0x00 0x00 0x00 0x00
0x603368: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603370: 0x3b 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603378: 0xe1 0x0b 0x40 0x00 0x00 0x00 0x00 0x00
0x603380: 0x30 0x33 0x60 0x00 0x00 0x00 0x00 0x00
0x603388: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603390: 0x3f 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603398: 0x56 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x6033a0: 0x50 0x33 0x60 0x00 0x00 0x00 0x00 0x00
0x6033a8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6033b0: 0x3f 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6033b8: 0x74 0x0b 0x40 0x00 0x00 0x00 0x00 0x00
0x6033c0: 0x70 0x33 0x60 0x00 0x00 0x00 0x00 0x00
0x6033c8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6033d0: 0x1a 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6033d8: 0x56 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x6033e0: 0x90 0x33 0x60 0x00 0x00 0x00 0x00 0x00
0x6033e8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6033f0: 0x1a 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6033f8: 0x1c 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x603400: 0xb0 0x33 0x60 0x00 0x00 0x00 0x00 0x00
0x603408: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603410: 0x28 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603418: 0x52 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x603420: 0xd0 0x33 0x60 0x00 0x00 0x00 0x00 0x00
0x603428: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603430: 0x28 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603438: 0xa4 0x0b 0x40 0x00 0x00 0x00 0x00 0x00
0x603440: 0xf0 0x33 0x60 0x00 0x00 0x00 0x00 0x00
0x603448: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603450: 0x1a 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603458: 0x52 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x603460: 0x10 0x34 0x60 0x00 0x00 0x00 0x00 0x00
0x603468: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603470: 0x1a 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603478: 0xdb 0x0b 0x40 0x00 0x00 0x00 0x00 0x00
0x603480: 0x30 0x34 0x60 0x00 0x00 0x00 0x00 0x00
0x603488: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603490: 0x48 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603498: 0x52 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x6034a0: 0x50 0x34 0x60 0x00 0x00 0x00 0x00 0x00
0x6034a8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6034b0: 0x48 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6034b8: 0x6e 0x0b 0x40 0x00 0x00 0x00 0x00 0x00
0x6034c0: 0x70 0x34 0x60 0x00 0x00 0x00 0x00 0x00
0x6034c8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6034d0: 0x24 0x00 0x00 0x00 0x00 0x00 0x00 0x00
```

```
0x6034d8: 0x52 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x6034e0: 0x90 0x34 0x60 0x00 0x00 0x00 0x00 0x00
0x6034e8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6034f0: 0x24 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6034f8: 0x18 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x603500: 0xb0 0x34 0x60 0x00 0x00 0x00 0x00 0x00
0x603508: 0x31 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603510: 0x40 0x35 0x60 0x00 0x00 0x00 0x00 0x00
0x603518: 0x60 0x35 0x60 0x00 0x00 0x00 0x00 0x00
0x603520: 0x80 0x35 0x60 0x00 0x00 0x00 0x00 0x00
0x603528: 0xa0 0x35 0x60 0x00 0x00 0x00 0x00 0x00
0x603530: 0xc0 0x35 0x60 0x00 0x00 0x00 0x00 0x00
0x603538: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603540: 0x0b 0x00 0x44 0x00 0x43 0x00 0x1d 0x00
0x603548: 0x52 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603550: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603558: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603560: 0x1e 0x00 0x3e 0x00 0x17 0x00 0x43 0x00
0x603568: 0x23 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603570: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603578: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603580: 0x1d 0x00 0x02 0x00 0x16 0x00 0x3a 0x00
0x603588: 0x45 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603590: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603598: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6035a0: 0x43 0x00 0x5d 0x00 0x38 0x00 0x0b 0x00
0x6035a8: 0x2a 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6035b0: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6035b8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6035c0: 0x1d 0x00 0x49 0x00 0x15 0x00 0x13 0x00
0x6035c8: 0x54 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6035d0: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6035d8: 0x31 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6035e0: 0x10 0x36 0x60 0x00 0x00 0x00 0x00 0x00
0x6035e8: 0x30 0x36 0x60 0x00 0x00 0x00 0x00 0x00
0x6035f0: 0x50 0x36 0x60 0x00 0x00 0x00 0x00 0x00
0x6035f8: 0x70 0x36 0x60 0x00 0x00 0x00 0x00 0x00
0x603600: 0x90 0x36 0x60 0x00 0x00 0x00 0x00 0x00
0x603608: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603610: 0x25 0x00 0x62 0x00 0x18 0x00 0x0f 0x00
0x603618: 0x46 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603620: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603628: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603630: 0x0d 0x00 0x1a 0x00 0x5b 0x00 0x50 0x00
0x603638: 0x38 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603640: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603648: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603650: 0x49 0x00 0x3e 0x00 0x46 0x00 0x60 0x00
0x603658: 0x51 0x00 0x00 0x00 0x00 0x00 0x00 0x00
```

```
0x603660: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603668: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603670: 0x05 0x00 0x19 0x00 0x54 0x00 0x1b 0x00
0x603678: 0x24 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603680: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603688: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603690: 0x05 0x00 0x2e 0x00 0x1d 0x00 0x0d 0x00
0x603698: 0x39 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6036a0: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6036a8: 0x31 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6036b0: 0xe0 0x36 0x60 0x00 0x00 0x00 0x00 0x00
0x6036b8: 0x00 0x37 0x60 0x00 0x00 0x00 0x00 0x00
0x6036c0: 0x20 0x37 0x60 0x00 0x00 0x00 0x00 0x00
0x6036c8: 0x40 0x37 0x60 0x00 0x00 0x00 0x00 0x00
0x6036d0: 0x60 0x37 0x60 0x00 0x00 0x00 0x00 0x00
0x6036d8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6036e0: 0x18 0x00 0x5f 0x00 0x52 0x00 0x2d 0x00
0x6036e8: 0x0e 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6036f0: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6036f8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603700: 0x43 0x00 0x22 0x00 0x40 0x00 0x2b 0x00
0x603708: 0x32 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603710: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603718: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603720: 0x57 0x00 0x08 0x00 0x4c 0x00 0x4e 0x00
0x603728: 0x58 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603730: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603738: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603740: 0x54 0x00 0x03 0x00 0x33 0x00 0x36 0x00
0x603748: 0x63 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603750: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603758: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603760: 0x20 0x00 0x3c 0x00 0x4c 0x00 0x44 0x00
0x603768: 0x27 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603770: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603778: 0x31 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x603780: 0xb0 0x37 0x60 0x00 0x00 0x00 0x00 0x00
0x603788: 0xd0 0x37 0x60 0x00 0x00 0x00 0x00 0x00
0x603790: 0xf0 0x37 0x60 0x00 0x00 0x00 0x00 0x00
0x603798: 0x10 0x38 0x60 0x00 0x00 0x00 0x00 0x00
0x6037a0: 0x30 0x38 0x60 0x00 0x00 0x00 0x00 0x00
0x6037a8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6037b0: 0x0c 0x00 0x1a 0x00 0x56 0x00 0x5e 0x00
0x6037b8: 0x27 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6037c0: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6037c8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6037d0: 0x5f 0x00 0x46 0x00 0x22 0x00 0x4e 0x00
0x6037d8: 0x43 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6037e0: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
```

```
0x6037e8: 0x21 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x6037f0: 0x01 0x00 0x61 0x00 0x02 0x00 0x11 0x00
0x6037f8: 0x5c 0x00 0x00 0x00 0x00 0x00 0x00 0x00
```

Memory Dump #2:

```
(gdb) x/512xb 0x400b00
0x400b00: 0x64 0x61 0x74 0x61 0x20 0x74 0x65 0x73
0x400b08: 0x74 0x20 0x30 0x78 0x25 0x78 0x3a 0x20
0x400b10: 0x25 0x64 0x0a 0x00 0x25 0x64 0x5b 0x33
0x400b18: 0x5d 0x5b 0x32 0x5d 0x3a 0x25 0x64 0x0a
0x400b20: 0x00 0x25 0x64 0x5b 0x32 0x5d 0x5b 0x31
0x400b28: 0x5d 0x3a 0x25 0x64 0x0a 0x00 0x25 0x64
0x400b30: 0x5b 0x32 0x5d 0x5b 0x33 0x5d 0x3a 0x25
0x400b38: 0x64 0x0a 0x00 0x25 0x64 0x5b 0x31 0x5d
0x400b40: 0x5b 0x31 0x5d 0x3a 0x25 0x64 0x0a 0x00
0x400b48: 0x25 0x64 0x20 0x25 0x73 0x0a 0x00 0x66
0x400b50: 0x6f 0x75 0x6e 0x64 0x20 0x25 0x64 0x3d
0x400b58: 0x25 0x73 0x20 0x61 0x74 0x20 0x64 0x65
0x400b60: 0x70 0x74 0x68 0x20 0x25 0x64 0x0a 0x00
0x400b68: 0x4e 0x6f 0x70 0x65 0x21 0x00 0x77 0x68
0x400b70: 0x61 0x6c 0x65 0x00 0x73 0x65 0x61 0x6c
0x400b78: 0x00 0x6f 0x74 0x74 0x65 0x72 0x00 0x73
0x400b80: 0x68 0x61 0x72 0x6b 0x00 0x73 0x68 0x72
0x400b88: 0x69 0x6d 0x70 0x00 0x63 0x72 0x61 0x62
0x400b90: 0x00 0x63 0x6c 0x61 0x6d 0x00 0x66 0x69
0x400b98: 0x73 0x68 0x00 0x66 0x72 0x6f 0x67 0x00
0x400ba0: 0x65 0x65 0x6c 0x00 0x68 0x6f 0x72 0x73
0x400ba8: 0x65 0x00 0x62 0x65 0x61 0x72 0x00 0x6c
0x400bb0: 0x69 0x6f 0x6e 0x00 0x74 0x69 0x67 0x65
0x400bb8: 0x72 0x00 0x77 0x6f 0x6c 0x66 0x00 0x63
0x400bc0: 0x6f 0x77 0x00 0x67 0x6f 0x61 0x74 0x00
0x400bc8: 0x73 0x68 0x65 0x65 0x70 0x00 0x64 0x65
0x400bd0: 0x65 0x72 0x00 0x67 0x6f 0x72 0x69 0x6c
0x400bd8: 0x6c 0x61 0x00 0x67 0x72 0x61 0x70 0x65
0x400be0: 0x00 0x61 0x70 0x70 0x6c 0x65 0x00 0x62
0x400be8: 0x61 0x6e 0x61 0x6e 0x61 0x00 0x70 0x65
0x400bf0: 0x61 0x72 0x00 0x6d 0x65 0x6c 0x6f 0x6e
0x400bf8: 0x00 0x6f 0x72 0x61 0x6e 0x67 0x65 0x00
0x400c00: 0x70 0x6c 0x75 0x6d 0x00 0x70 0x65 0x61
0x400c08: 0x63 0x68 0x00 0x61 0x70 0x72 0x69 0x63
0x400c10: 0x6f 0x74 0x00 0x6b 0x69 0x77 0x69 0x00
0x400c18: 0x74 0x65 0x61 0x00 0x63 0x6f 0x66 0x66
0x400c20: 0x65 0x65 0x00 0x6d 0x69 0x6c 0x6b 0x00
0x400c28: 0x73 0x6f 0x64 0x61 0x00 0x6a 0x75 0x69
0x400c30: 0x63 0x65 0x00 0x77 0x61 0x74 0x65 0x72
0x400c38: 0x00 0x73 0x6d 0x6f 0x6f 0x74 0x68 0x69
0x400c40: 0x65 0x00 0x66 0x6c 0x6f 0x61 0x74 0x00
0x400c48: 0x63 0x6f 0x6c 0x61 0x00 0x6d 0x61 0x6c
```

```
0x400c50: 0x74 0x00 0x72 0x65 0x64 0x00 0x62 0x6c
0x400c58: 0x75 0x65 0x00 0x67 0x72 0x65 0x65 0x6e
0x400c60: 0x00 0x79 0x65 0x6c 0x6c 0x6f 0x77 0x00
0x400c68: 0x62 0x72 0x6f 0x77 0x6e 0x00 0x77 0x68
0x400c70: 0x69 0x74 0x65 0x00 0x62 0x6c 0x61 0x63
0x400c78: 0x6b 0x00 0x67 0x72 0x65 0x79 0x00 0x70
0x400c80: 0x75 0x72 0x70 0x6c 0x65 0x00 0x00 0x00
0x400c88: 0x01 0x1b 0x03 0x3b 0x74 0x00 0x00 0x00
```

Memory Dump #3:

```
Contents of section .rodata:
 400af0 01000200 00000000 00000000 00000000  ................
 400b00 64617461 20746573 74203078 25783a20  data test 0x%x:
 400b10 25640a00 25645b33 5d5b325d 3a25640a  %d..%d[3][2]:%d.
 400b20 0025645b 325d5b31 5d3a2564 0a002564  .%d[2][1]:%d..%d
 400b30 5b325d5b 335d3a25 640a0025 645b315d  [2][3]:%d..%d[1]
 400b40 5b315d3a 25640a00 25642025 730a0066  [1]:%d..%d %s..f
 400b50 6f756e64 2025643d 25732061 74206465  ound %d=%s at de
 400b60 70746820 25640a00 4e6f7065 21007768  pth %d..Nope!.wh
```

And here's an ASCII table if you need it:

ASCII Table

Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char
0	0	0		32	20	40	[space]	64	40	100	@	96	60	140	`
1	1	1		33	21	41	!	65	41	101	A	97	61	141	a
2	2	2		34	22	42	"	66	42	102	B	98	62	142	b
3	3	3		35	23	43	#	67	43	103	C	99	63	143	c
4	4	4		36	24	44	$	68	44	104	D	100	64	144	d
5	5	5		37	25	45	%	69	45	105	E	101	65	145	e
6	6	6		38	26	46	&	70	46	106	F	102	66	146	f
7	7	7		39	27	47	'	71	47	107	G	103	67	147	g
8	8	10		40	28	50	(	72	48	110	H	104	68	150	h
9	9	11		41	29	51	)	73	49	111	I	105	69	151	i
10	A	12		42	2A	52	*	74	4A	112	J	106	6A	152	j
11	B	13		43	2B	53	+	75	4B	113	K	107	6B	153	k
12	C	14		44	2C	54	,	76	4C	114	L	108	6C	154	l
13	D	15		45	2D	55	-	77	4D	115	M	109	6D	155	m
14	E	16		46	2E	56	.	78	4E	116	N	110	6E	156	n
15	F	17		47	2F	57	/	79	4F	117	O	111	6F	157	o
16	10	20		48	30	60	0	80	50	120	P	112	70	160	p
17	11	21		49	31	61	1	81	51	121	Q	113	71	161	q
18	12	22		50	32	62	2	82	52	122	R	114	72	162	r
19	13	23		51	33	63	3	83	53	123	S	115	73	163	s
20	14	24		52	34	64	4	84	54	124	T	116	74	164	t
21	15	25		53	35	65	5	85	55	125	U	117	75	165	u
22	16	26		54	36	66	6	86	56	126	V	118	76	166	v
23	17	27		55	37	67	7	87	57	127	W	119	77	167	w
24	18	30		56	38	70	8	88	58	130	X	120	78	170	x
25	19	31		57	39	71	9	89	59	131	Y	121	79	171	y
26	1A	32		58	3A	72	:	90	5A	132	Z	122	7A	172	z
27	1B	33		59	3B	73	;	91	5B	133	[	123	7B	173	{
28	1C	34		60	3C	74	<	92	5C	134	\	124	7C	174	|
29	1D	35		61	3D	75	=	93	5D	135	]	125	7D	175	}
30	1E	36		62	3E	76	>	94	5E	136	^	126	7E	176	~
31	1F	37		63	3F	77	?	95	5F	137	_	127	7F	177	