**CSE 484 In-section Worksheet #3**

Q1. Which gdb command allows us to:

view the four words starting at ebp in hex?

view the next five instructions at eip?

view all instructions for function foo?

Q2. Which register does the x86 instruction RET affect? How, exactly?

Q3. What do tmalloc() and tfree() do?

Q4. Why is it safe for the implementation of tmalloc.c to use the least significant bit of the right pointer of a chunk to determine if said chunk is free?

Q4. What’s the issue with this code?

char \*p; char \*q;

if ( (p = tmalloc(128)) == NULL)

{ exit(EXIT\_FAILURE); }

if ( (q = tmalloc(128)) == NULL)

{exit(EXIT\_FAILURE); }

A

tfree(p);

tfree(q);

B

if ( (p = tmalloc(256)) == NULL)

{exit(EXIT\_FAILURE); }

obsd\_strlcpy(p, arg, 256);

C

tfree(q);

Q5. Based on tmalloc.c, draw what the heap/free list looks like at points, A, B, and C. Include chunk structure and label p (at or before point B), p (at point C), and q. Where is buf copied?

Q6. Given your diagrams and the following code for chunk consolidation (from tmalloc.c), what do the following statements do when executed in the call tfree(q) after point C?

q->s.r = p->s.r;

p->s.r->s.l = q;