Name: _____

Directions: Work only on this sheet (on both sides, if needed); do not turn in any supplementary sheets of paper. There is actually plenty of room for your answers, as long as you organize yourself BEFORE starting writing. In order to get full credit, SHOW YOUR WORK.

1. This problem is about the **read()** system call.

(a) (10) During execution of **read()** the CPU is in _____ mode. It got into this mode because the function is called via the _____ instruction instead of by the _____ instruction.

(b) (10) The OS will need to check which system call has been made, i.e. check whether it was a call to **write()**, a call to **read()**, a call to **open()**, etc. Give a single instruction from the Intel CMP family which checks whether the call was to **read()**.

2. Consider the following Java code and its compiled JVM machine language:

```
public class First8 {
   public static void main(String[] CLArgs)
   {  int X[];
      X = new int[3];
      X[0] = 4; X[1] = 8; X[2] = 1;
      System.out.println(First(X,8));
   }
   public static int First(int A[], int K)
   {  int I;
      for (I = 0; ; I++)
         if (A[I] == K) break;  // name this line L
      return I;
   }
}
...
Method void main(java.lang.String[])
   0 iconst_3
   1 newarray int
   3 astore_1
...
  17 getstatic #2 <Field java.io.PrintStream out>
  20 ________
  21 bipush ________
  23 invokestatic #3 <Method int First(int[], int)>
  26 invokevirtual #4 <Method void println(int)>
  29 return
Method int First(int[], int)
   0 iconst_0
   1 istore_2
   2 goto 5
   5 aload_0
   6 iload_2
   7 iaload
   8 iload_1
   9 if_icmpne 15
  12 goto 21
  15 iinc 2 1
  18 goto 5
  21 ________
  22 ireturn
```

(a) (20) The compiled code for the source line named L (see comment in source code) is in offsets _____ through _____ of **First()**.

(b) (15) Give the machine code for the instructions in offsets 8-9 of **First()**. Your answer must consist of four bytes of hex.

(c) (20) Fill in the blanks in offsets 20 and 21 of **main()** and in offset 21 of **First()**.

3. (25) The following MIPS code, which could be part of an OS, changes an entry in the page table to indicate that the given page is not resident in memory. The labels **pgtbl** and **pgnum** are in the **.data** segment; **pgtbl** is the beginning of the page table, and **pgnum** contains the number of the page to be recorded as nonresident. Assume the page table structure on p.16 of our PLN unit on OS. Fill in the blanks (MIPS pseudoinstructions are allowed).

```
lw $8,________
sll $9,$8,________
lw $10,________($9)
and $11,$10,0x________
sw $11, ________(________)
```

Solutions:

1. Kernel; **int**; **call**

2. Since **read()** is system call number 3, we should use

```
cmpl $3, %eax
```

3.a 5-12; note that offset 12 implements the **break**

3.b The opcode is 0x1b for **iload_1**. For **if_cmpne** the opcode is 0xa0 and there is a 2-byte operand for the distance to the jump target, in this case 15-9 = 6. So, the two instructions have machine code 0x1ba00006.

3.c In offsets 20 and 21 of **main()**, we need to pass the two arguments for the call to **First()**. The first argument, **X**, is an array name, thus an address, so we need an instruction from the **aload** family, in this case **aload_1** since **X** is in slot 1. The second argument is 8, which we push in offset 21. If offset 21 of **First()**, we need to push the return value, for use by the **ireturn** in offset 22. Since the return value is **I**, in offset 2, we need **iload_2**.

4.

```
lw $8,pgnum                    # index into the table
sll $9,$8,2                    # multiply by 4, since each entry is 4 bytes
lw $10,pgtbl(9)                # get the page table entry
and $11,$10,0xfffff7ff         # change the residence bit to 0
sw $11, pgtbl($9)              # store new entry
```