Paul Parker

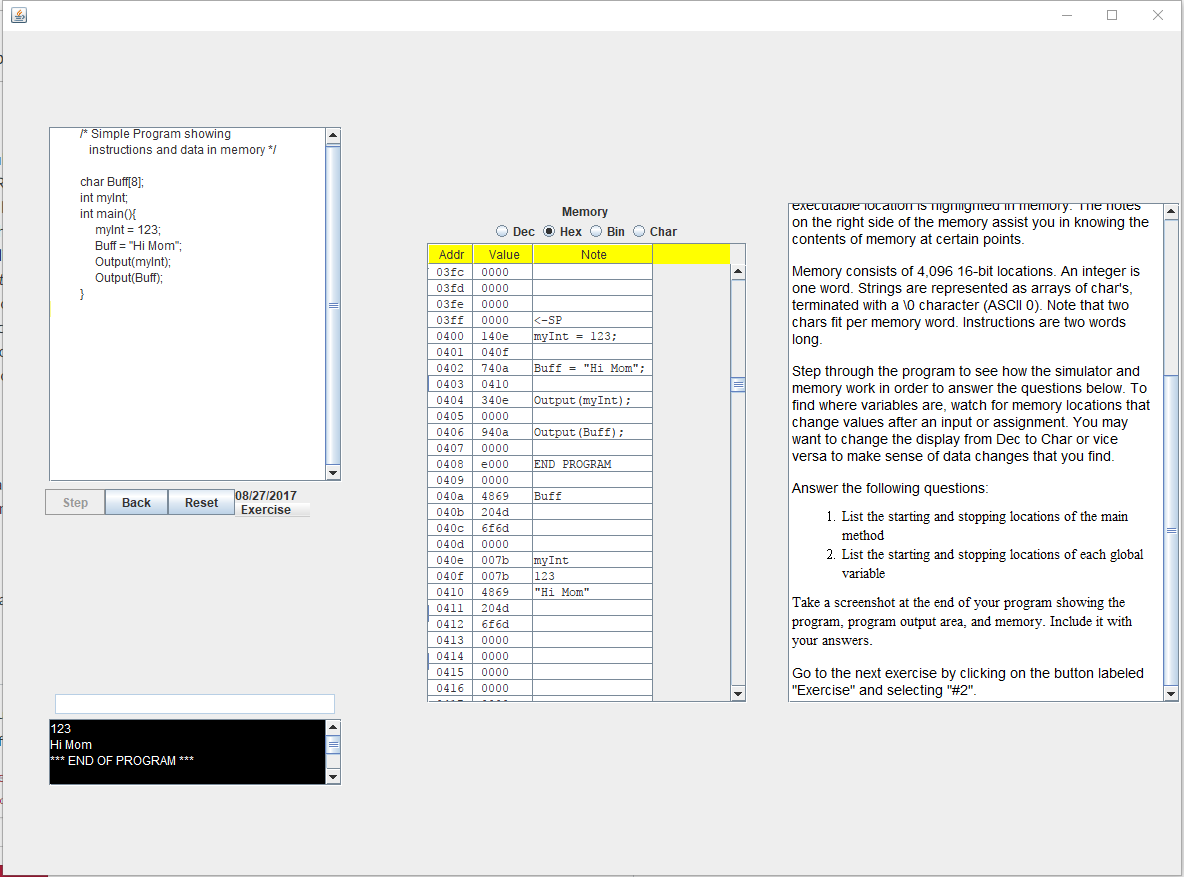
CS373

Unit 2: Homework

Exercise 1:

1: Program start: 0x0400, stop: 0x0408

2. Buff start: 0x040a, stop: 0x040c. myInt start: 0x040e, stop: 0x040e



Exercise 2:

1:

XYZ

ABCDEF

456

\*\*\* END OF PROGRAM \*\*\*

2:

XYZZY

Y

456

\*\*\* END OF PROGRAM \*\*\*

3:

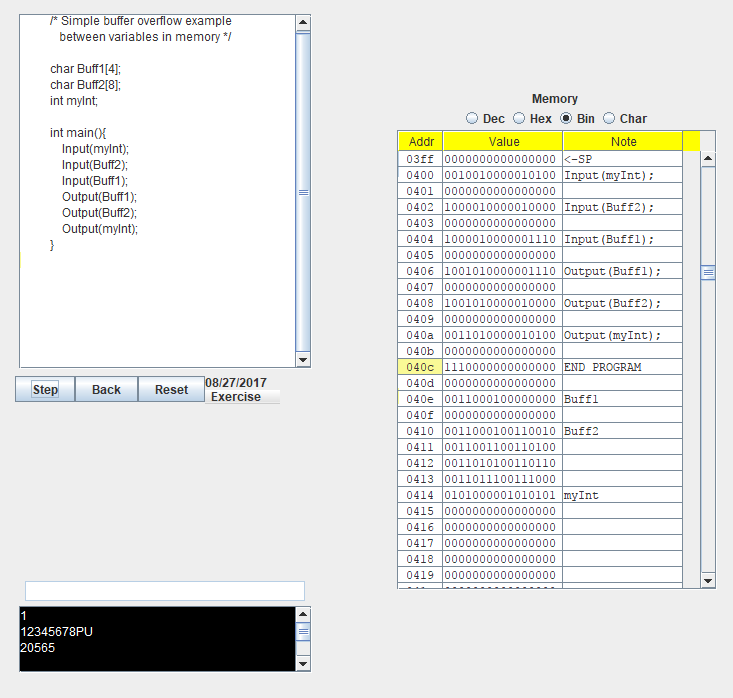
XYZ

ABCDEFGHIJ

18762

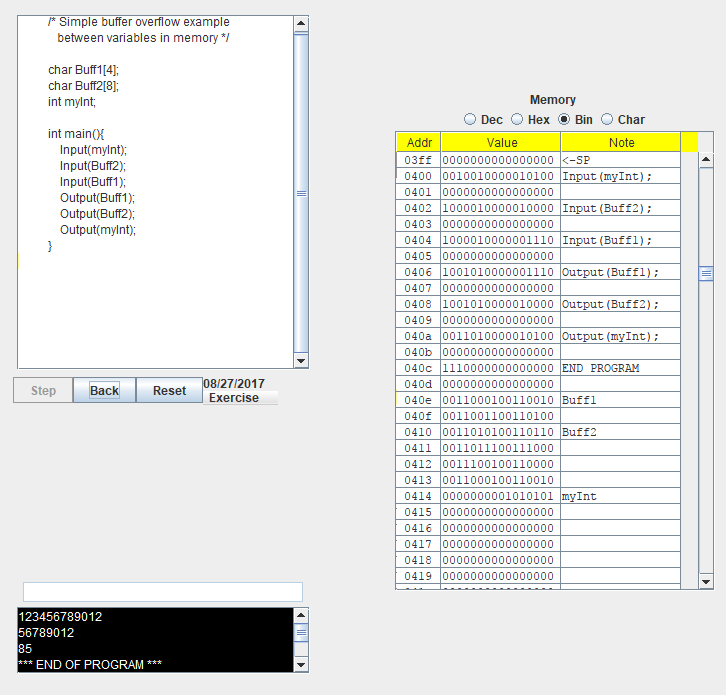
\*\*\* END OF PROGRAM \*\*\*

4:



To get this I converted 20565 to binary to get “

5:



Made sure that Buff2 was long enough to end the last 8 digits of myInt space with the binary needed for 85, or rather a string that was 10 characters long and ended in “U”. The made sure Buff1 was just long enough so that the null character “00000000” began right at myInt, or a string 12 characters long.

Exercise 3:

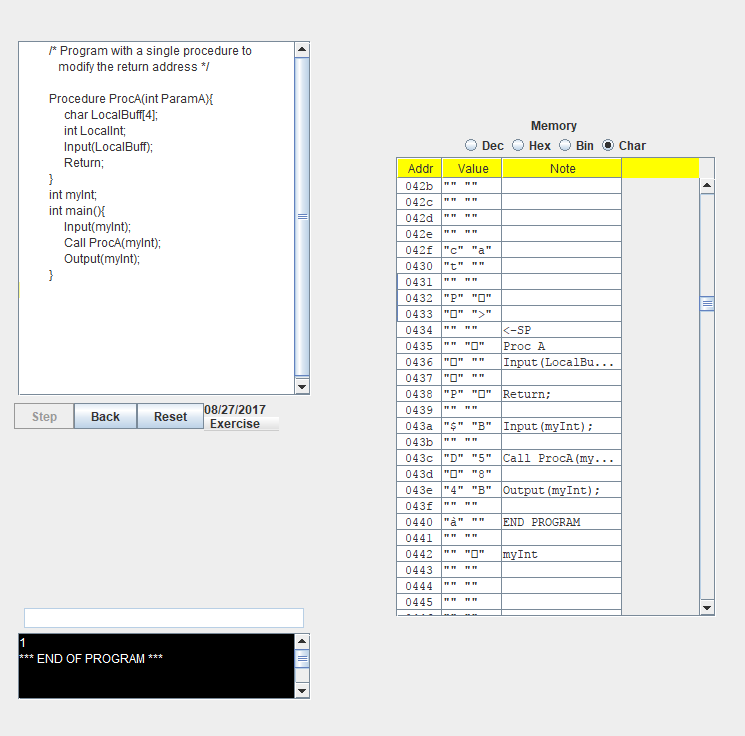
1: main program starts: 0x043a, stops: 0x0440

2: ProcA starts: 0x0435, stops: 0x0438

3: LocalBuff starts 0x042f, stops: 0x0430. LocalInt starts: 0x0431, stops: 0x0431

4: params starts: 0x0432, stops: 0x0432

5: return address is 0x043e and refers to ‘Output(myInt);’



Exercise 4:

String used to overflow: 123456789012345678à

This string writes up to the return statement than then overrides the instruction for the return statement with the “END PROGRAM” instruction 0xe000 “à” + the null character

