1. Perform binary reversing on mystery2.exe and mystery2 (provided on Canvas). Determine the following:

a. Is the program built for 32-bit or 64-bit execution?

|  |
| --- |
| **mystery2.exe** |
| 32bits |
|  |
| **mystery2** |
| 32 bits |
|  |

b. What is the executable file format (e.g. PE, ELF, COFF, MachO)?

|  |
| --- |
| **mystery2.exe** |
| PE32 executable |
|  |
| **mystery2** |
| ELF 32-bits LSB executable |
|  |

c. Do the programs take input once started?

|  |
| --- |
| **mystery2.exe** |
| Yes, it accepts 3 inputs. |
|  |
| **mystery2** |
| Yes, it accepts 3 inputs. |
|  |

d. Do the programs accept input at startup on the command-line?

|  |
| --- |
| **mystery2.exe** |
| Yes, it accepts 3 inputs. |
|  |
| **mystery2** |
| Yes, it accepts 3 inputs. |
|  |

e. Are there functions that appear to be developed by the human and not gcc/standard c library functions?

|  |
| --- |
| **mystery2.exe** |
| mult\_ok |
|  |
| **mystery2** |
| mult\_ok |
|  |

f. What output does the program produce? How may the output vary based on user inputs?

|  |  |
| --- | --- |
| mystery2.exe | mystery2 |
| If input is a,b,c  The program output  If a\*b == a\*b\*c output a\*b==a\*b\*c  elif a\*b != a\*b\*c output a\*b!=a\*b\*c elif a==0 or b==0 or c==0 output a\*b!= a\*b\*c  elif the 16bits isn’t set  output something went horribly wrong | If input is a,b,c  The program output  If a\*b == a\*b\*c output a\*b==a\*b\*c  elif a\*b != a\*b\*c output a\*b!=a\*b\*c elif a==0 or b==0 or c==0 output a\*b!= a\*b\*c  elif the 16bits isn’t set  output something went horribly wrong |

g. Which library functions are called by the program (e.g. gets/puts)

|  |
| --- |
| mystery2.exe |
| Atexit  Fesetenv  wcstombs  vfprintf  tolower  strlen  strcoll  signal  setlocale  realloc  puts  printf  memcpy  mbstowcs  malloc  fwrite  free  calloc |
|  |
| mystery2 |
| printf  puts  atoi  malloc  calloc  realloc  free |
|  |

h. What calling convention is used?

|  |  |
| --- | --- |
| mystery2.exe | mystery2 |
| cdecl | cdecl |

2. How do the two files differ?

  Though, the output is similar, the two file differs in the import libraries and executable file format.