The main function calls printf with the string “Win!”.Text

Description automatically generated

And printf address is 00401040h.

Timeline

Description automatically generated with medium confidence

The second function is from microsoft’s api and it’s called atoi. This function receives a string and returns an integer value.

Text

Description automatically generated

This function is external so it’s address is 00402048h in .idata section:

Graphical user interface, text

Description automatically generated with medium confidence

In order to win the game, open cmd in the directory you have the file in, and type “vegas 21”:



From the structure of the program we can see that there is a loop (probably for-loop), that sets var\_8 to the sum of var\_8 + var\_4, and increments var\_4 by 1 every iteration. At the end of the loop, var\_8 equals 21, and if the input equals 21 we go to the block that calls printf.

Graphical user interface, application

Description automatically generated