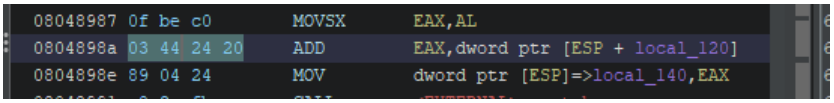
Level09

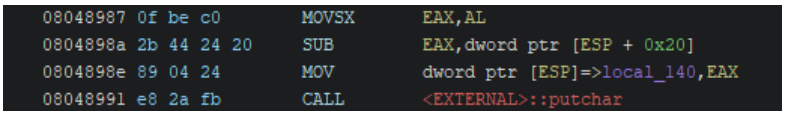
Al abrir el proyecto tenemos de nuevo un script y un archivo llamado token. Este script no se le puede hacer debug y cuando lo ejecutamos con el token nos da una cadena con caracteres no imprimibles.

Para ello voy a optar por usar `ghidra` un software open source de reversing de binarios. Con Ghidra vemos lo siguiente. Nuestro binario procesa el argumento que recibe tras hacer varias comprobaciones anti debug.

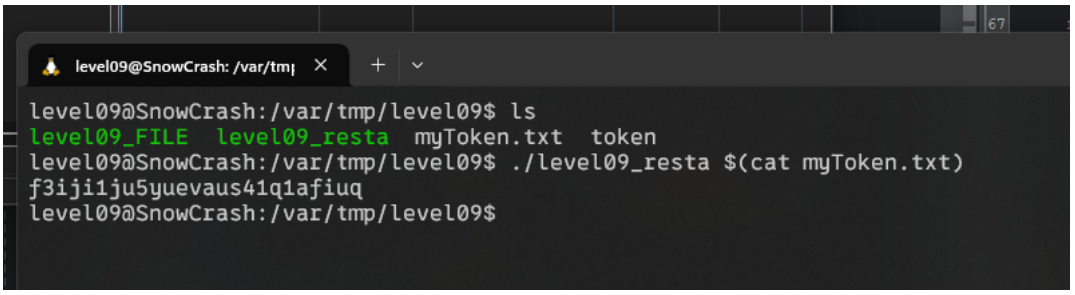
Nuestro script lo que hace es ofuscar una cadena sumándole un valor al hexadecimal de cada carácter. Eso lo hace aquí:



Lo único que tenemos que hacer es modificar esa operación para que en lugar de sumar reste.



Ahora ejecutamos el script pasándole el token como argumento y sacamos la cadena facilmente.



Pass para flag09: `f3iji1ju5yuevaus41q1afiuq`

Flag final `s5cAJpM8ev6XHw998pRWG728z`