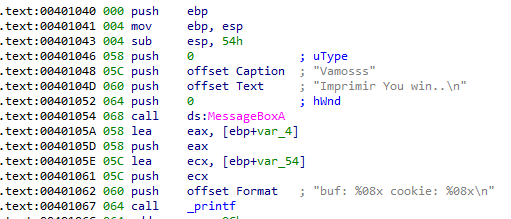
Resuelto el 3 pasamos al cuarto :P y como vemos la primera parte es todo igual, se sigue reservando **0s54 (80) bytes**, se llama un MessageBox y se imprimen las direcciones del **buffer** y de la **cookie.**

****

Lo único que cambio es en la comparación de la cookie, que como vemos ahora es **0x0D0A00.**

En litle endian seria algo como **00 0A 0D 00**



**0x00 : Carácter nulo**

**0x0A: Nueva línea**

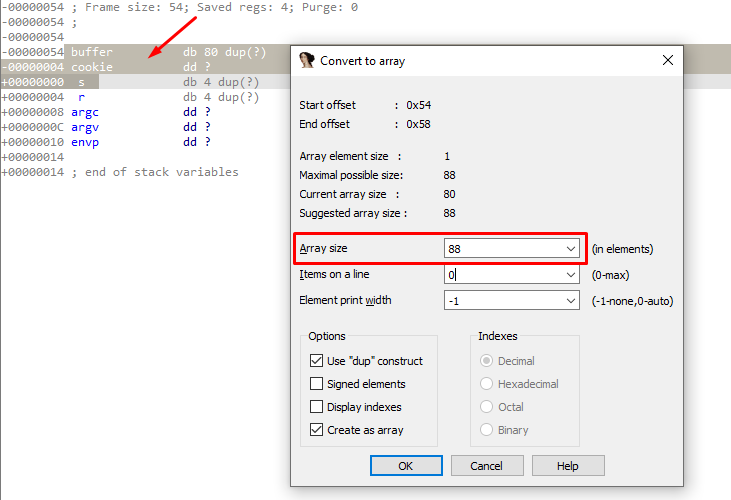
**0x0D: retorno de carro**

Como ya vimos, el carácter nulo no nos va afectar, pero ahí tenemos un **0x0A** (newline) que si nos afectara cortando la cadena -.- .

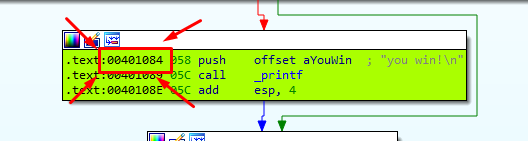
Una solución posible es pisar el **retn**  y hacer que salte directamente al mensaje de “**you win!”**

**¿Como hacemos esto?¿** Pues bien, desbordamos el **buffer** hasta pisar la dirección de retorno :P

Nos vamos a la pila y seleccionamos hasta **s (base pointer)** para ver la cantidad de bytes que hay hasta ahí, con clic derecho y **array** podemos verlo.

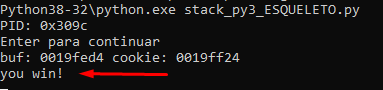


Entonces después de 88 bytes tenemos que poner la dirección a la cual queremos que salte nuestro **retn,** y esta dirección es **0x00401084**

****

De esta forma se imprimirá el mensaje de **“You win!”**

| import sys from subprocess import Popen, PIPE  buffer = b"A" \* 80 cookie = b"B" \* 4 s = b"C" \* 4 r = b"\x84\x10\x40\x00"  payload = buffer + cookie + s + r  p1 = Popen("STACK4\_VS\_2017.exe", stdin=PIPE) print ("PID: %s" % hex(p1.pid)) print ("Enter para continuar")  p1.communicate(payload) p1.wait() input() |
| --- |



Ejercicio anterior [03 Stack Nro 3](https://docs.google.com/document/d/1f4_MbTtzIt03H4hTP_0T-LWgD44xoxzf70-OgCmvWz8/edit?usp=sharing)

Ejercicio siguiente [05 - STACK 2 x64](https://docs.google.com/document/d/1XsnCZYtYih_n4xXtP_bX08aVRewBSdFAfJSzY4kdagU/edit?usp=sharing)