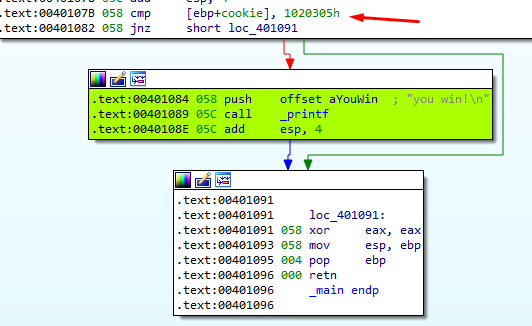
Ahora que ya resolvimos el primer ejercicio [01 Stack Nro 1](https://docs.google.com/document/d/1s28WppAv2U55NWb4uhFO55tlA0ORz4FjiG1deznUwkI/edit?usp=sharing) podemos pasar a este segundo **STACK2\_VS\_2017**.exe.

Como en el anterior al inicio de la función se reservan 0x54 (84) bytes para ser usados por las variables locales, etc.



También hay un MessageBox al que debemos aceptar y se imprime un mensaje de ayuda con las direcciones del **buffer** y de la **cookie**

Luego se le pasa como argumento un puntero al comienzo de la variable **var\_54** a la función **gets.** Vamos a renombrar a esta variable como **buffer,** me paro arriba y presionas la tecla **N** y le cambiamos el nombre.



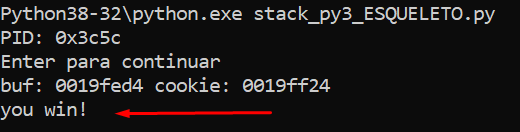
Lo único que cambia aquí es el valor contra la que se compara la **cookie**, ahora es un **0x01020305**

Mi script en python quedaria asi:

import sys

from subprocess import Popen, PIPE

| buffer = b"A" \* 80 cookie = b"\x05\x03\x02\x01"  payload = buffer + cookie  p1 = Popen("STACK2\_VS\_2017.exe", stdin=PIPE) print ("PID: %s" % hex(p1.pid)) print ("Enter para continuar")  p1.communicate(payload) p1.wait() input() |
| --- |

****

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