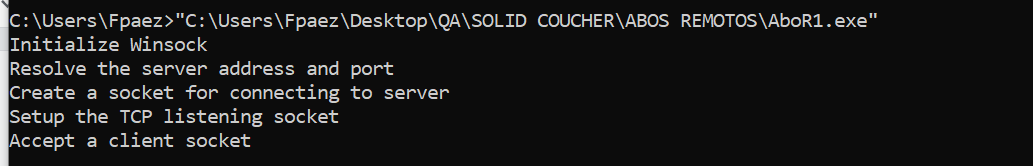
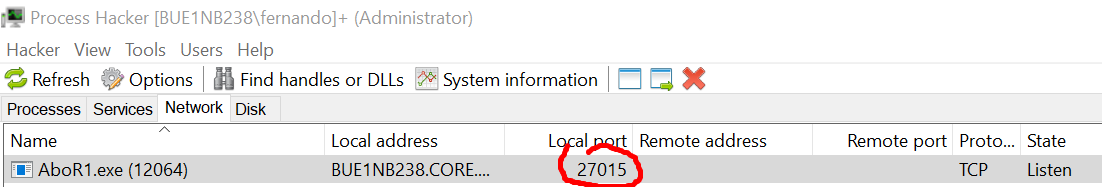
Llegamos a los **ABOS REMOTOS**, vamos a ver el primero que se llama **AboR1.exe**

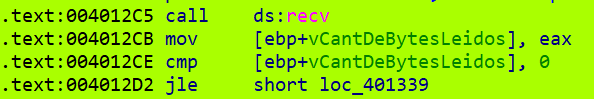
Al correrlo sobre una consola nos aparece el siguiente mensaje.



Con **Process Hacker**, vemos que está escuchando en el puerto **27015**



Aquí tenemos la función que recibe los bytes que le mandemos.



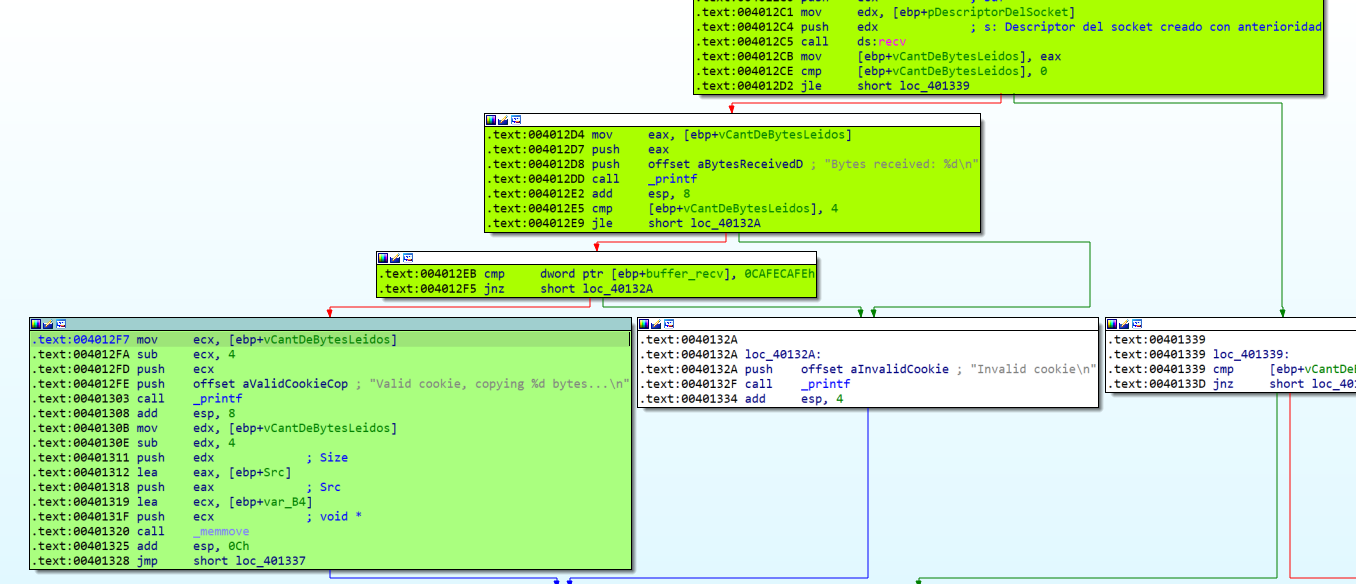
Vemos que imprime en la consola la cantidad de bytes que se recibieron, además esta cantidad debe ser mayor a 4 bytes.



Si hay mas de 4 bytes recibidos, y los primeros bytes del buffer son **0xCAFECAFE**

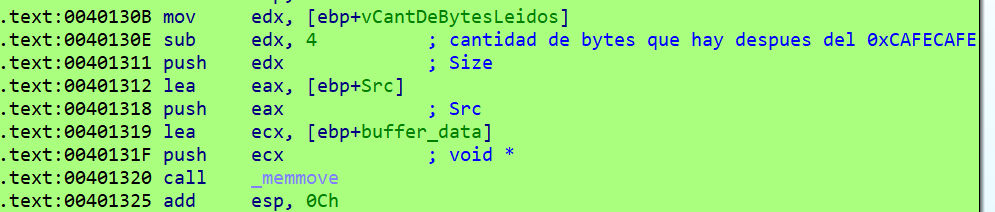


nos muestra el mensaje de “**valid cookie!”** por lo que habremos conseguido el objetivo de este **abo.**

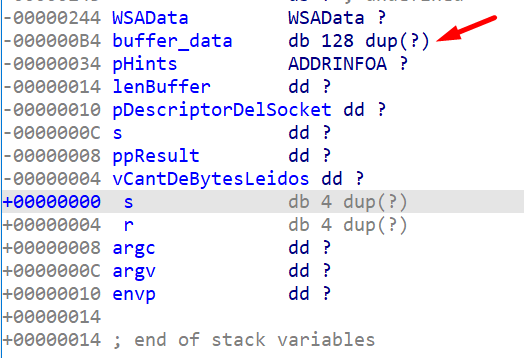
****

Okey, igual aquí no termina jaja, después a la cantidad de bytes que se recibieron le resta 4 (por el 0xCAFECAFE), y así se tiene la cantidad de bytes que hay después de esta frase.

Luego mueve todos estos bytes que hay despues del CAFECAFE al **buffer\_data**

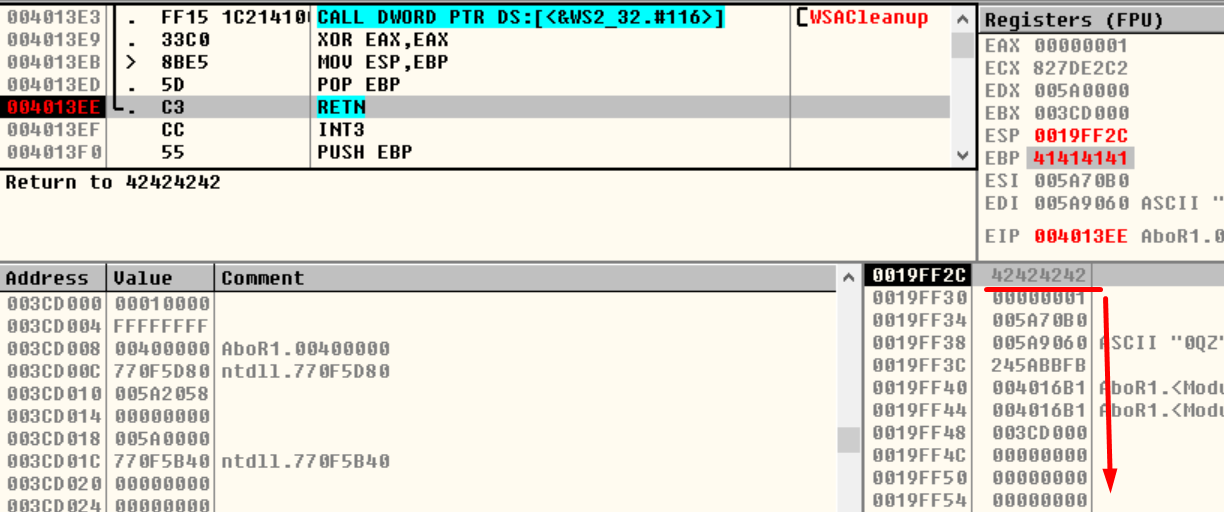


La variable **buffer\_data** tiene un tamaño de 128 bytes ¿que pasa si le pasamos mas de 128 -.- ?¿



Pues podemos pisar las variables que se encuentran por debajo de ella, hasta el **return address,** en la que pondremos un puntero a nuestro **shellcode**  que ejecuta la calculadora.

Estamos parados sobre el **retn**, en la pila vemos que estamos por retornar a **0x42424242**



La forma que encontré de saltar a la **shellcode** es a traves de un **jmp esp**, la cual lo encontramos aquí:



Ahora bien, en teoría este salto nos dejaría por debajo del **0x42424242,**  y en este lugar vamos a colocar la shellcode de la calculadora.

