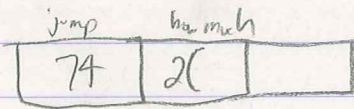


- je DONE 09004040



EIP = 09004042 before exec

74 is op code for jmp

$$\begin{array}{r} \text{DONE:} \quad 09004042 \\ + \quad 04004042 \\ \hline \quad 2C \\ \hline \text{DONE:} \quad 0900406E \end{array}$$

- je DONE 09004040



EIP = 09004042

$$\begin{array}{r} + \text{FFFFFFCE} \\ \hline \text{DONE: } \textcircled{1} \quad 09004010 \end{array}$$

- TEST

- no flags are set for the NOT instruction

- Recursion Review

$$; f(n) = n + f(n-1)$$

; 00409100

f proc near 32

push ebp

mov ebp, esp

n equ [ebp+8]

push ebx

mov eax, 0

cmp dword ptr n, 0

; N=0?

je done

mov ebx, n

dec ebx

done:

push ebx

pop ebx

call f

pop ebp

add esp, 4

ret

add eax, n

f endp

- 1 + 2 + 3

1. n down 3
; sum = f(n),
push n
call sum
add esp, 4
mov sum, eax

; 0x00401000

1. esp = 100h eip = 00401000 ebp = F4 ebx = 0 eax = 0

FC	DC	4200	E4	3	0
F8	E0	4100	D4	2	0
F4	E4	-	C4	2	0
F0	E8	-	D4	1	1
EC	EC	4200	E4	1	3
E8	F0	4100	F4	0	6
E4	F4	-	-1	0	
E0	F8	4200		1	
DC	FC	4100		1	
D8	100	4200		0	
D4		-			
DD		-			
CC		4200			
C8		4000			
C4					
C0					
C4					
C8					
CC					
D0					
D4					
DB					

C0	0	
C4	D4	[ebp]
C8	4200	
CC	0	N
D0	1	
D4	E4	[ebp]
D8	4200	
DC	1	N
E0	2	
E4	F4	[ebp]
E8	4200	
EC	2	N
F0	0	
F4	FFFFFFFF	[ebp]
F8	4200	
FC	3	N

$$; f(n) = n \cdot f(n-1)$$

f proc new 32