

HW 7

4.

Main Proc

4040018

mov ecx, 0ABCDh

404001C

mov ebx, 1234h

★ EIP → 4040020

call FDIV

★ → 4040026
moves

mov eax, ebx

...

Main EndP

FDIV Proc

★ TARGET → 4041040

push ebx

4041044

push ecx

4041048

mov eax, edx

...

404A060

pop ecx

404A062

pop ebx

404A064

ret

FDIV EndP

Stack
addresses

memory
Addresses

STACK

19

← ESP₆₄

1C

← ESP₆₂

20

← ESP₆₀

24

← ESP₄₈

28

0ABCD

← ESP₄₄

2B

1234

← ESP₄₀

2F

4040026

← ESP₂₀

... ..

← ESP_{1C}

... ..