

# **Reverse Engineering**

Spring-2020 Semester

Danh Pham

## Task1:

```

; Attributes: bp-based frame fuzzy-sp

; int __cdecl main(int argc, const char **argv, const char **envp)
public _main
_main proc near

    argc= dword ptr 8
    argv= dword ptr 0Ch
    envp= dword ptr 10h

    push    ebp
    mov     ebp, esp
    and     esp, 0FFFFFFF0h
    call    __main
    nop
    nop
    leave
    retn
_main endp

```

## Task2:

CPU - main thread, module ntdll

Address	Hex dump	ASCII	Disassembly	Registers (FPU)
7793CE37	74 0E		JE SHORT ntdll.7793CE47	EAX 00401400 nothing
7793CE39	8B 0D A8 87 9E 77		MOV ECX, DWORD PTR DS:[779E87A8]	ECX 00000000
7793CE3F	FF 15 E0 B1 9E 77		CALL DWORD PTR DS:[779EB1E0]	EDX 00000000
7793CE45	FF E1		JMP ECX	EBX 0024F000
7793CE47	89 44 24 04		MOV DWORD PTR SS:[ESP+4], EAX	ESP 0065FFF0
7793CE4B	89 5C 24 08		MOV DWORD PTR SS:[ESP+8], EBX	EBP 00000000
7793CE4F	E9 19 6C FFFF		JMP ntdll.77933A6D	ESI 00000000
7793CE54	8D A4 24 00 00 00 00		LEA ESP, DWORD PTR SS:[ESP]	EDI 00000000
7793CE5B	EB 03		JMP SHORT ntdll.KiFastSystemCall	EIP 7793CE37 ntdll.7
7793CE5D	CC		INT3	C 0 ES 002B 32bit 0
7793CE5E	CC		INT3	P 1 CS 0023 32bit 0
7793CE5F	CC		INT3	A 0 SS 002B 32bit 0
7793CE60	8B 04		MOV EDI, ESP	Z 1 DS 002B 32bit 0
7793CE62	0F 34		SYSENTER	S 0 FS 0053 32bit 2
7793CE64	8D A4 24 00 00 00 00		LEA ESP, DWORD PTR SS:[ESP]	T 0 GS 002B 32bit 0
7793CE6B	EB 03		JMP SHORT ntdll.KiFastSystemCall	D 0
7793CE6D	CC		INT3	O 0 LastErr ERROR_S
7793CE6E	CC		INT3	EFL 00000246 (NO, NB,
Jump is taken 7793CE47=ntdll.7793CE47				ST0 empty 0.0
00403000	0A 00 00 00 10 26 40 00	....&@.	0065FFA4 00000000	
00403008	FF FF FF FF FF FF FF FF	.....	0065FFA8 00000000	
00403010	FF 00 00 00 02 00 00 00	...@...	0065FFAC 00000000	
00403018	FF FF FF FF 60 25 40 00	...%e.	0065FFB0 00000000	
00403020	70 25 40 00 80 25 40 00	p%e, %e.	0065FFB4 00000000	
00403028	4E E6 40 B8 B1 19 BF 44	Np%e%&D	0065FFB8 00000000	
00403030	00 00 00 00 00 00 00 00	.....	0065FFBC 00000000	
00403038	00 00 00 00 00 00 00 00	.....	0065FFC0 00000000	
00403040	00 00 00 00 00 00 00 00	.....	0065FFC4 00000000	
00403048	00 00 00 00 00 00 00 00	.....	0065FFC8 00000000	
00403050	00 00 00 00 00 00 00 00	.....	0065FFCC 00000000	
00403058	00 00 00 00 00 00 00 00	.....	0065FFD0 00000000	
00403060	00 00 00 00 00 00 00 00	.....	0065FFD4 00000000	
			0065FFD8 00000000	

