Basic Program execution registers

<General-Purpose Registers>

EAX: Accumulator for operands and results data

EBX: Pointer to data in the DS segment

ECX: Counter for string and loop operations

EDX: I/O Pointer

주로 산술연산(ADD,SUB,XOR,OR 등) 명령어에서 상수/변수 값의 저장 용도로 많이 사용됩니다.

EBP: Pointer to data on the stack (in the SS segment)

ESI: source pointer for string operations

EDI: destination pointer for string operations

ESP: Stack pointer (in the SS segment)

주로 메모리 주소를 저장하는 포인터로 사용됩니다.

<System Tool>

Process Explorer

(https://technet.microsoft.com/en-us/sysinternals/default.aspx)

PEView.exe (http://magma.ca/~wjr/PEview.zip)