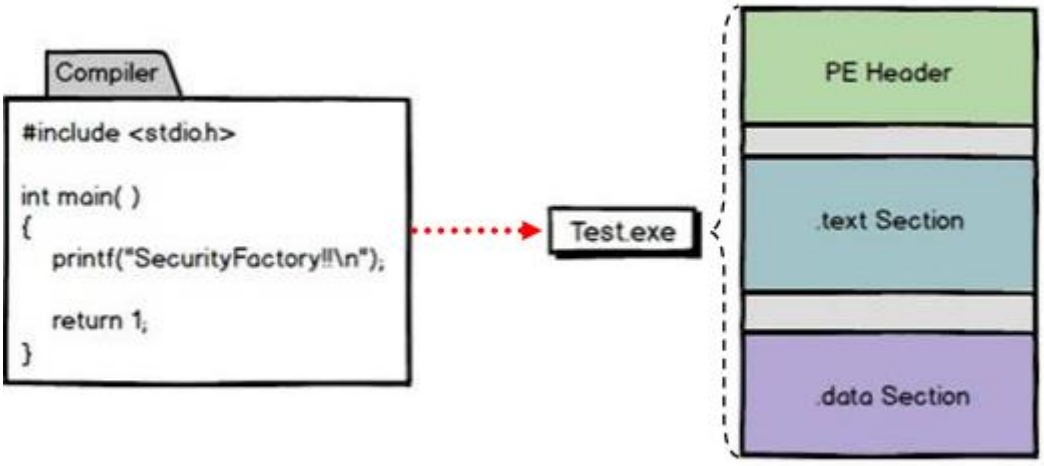
[PE File Format 이해하기]

1. PE File Format은 Windows 실행 파일의 구성 방식이다.

   해당 실행 파일을 어떻게 구성되어야 하는지 정의해 놓은 것.

   예를 들어 "SecurityFactory!!"라는 문자열을 출력하는 코드를 Test.exe로 컴파일 한다고 합시다. 그럼 컴파일러가 아래와 같은 PE File Format으로 생성해 줄 것입니다.



   여기서 가장 눈여겨 봐야 할 것은, PE Header입니다. PE File을 분석하기에 가장 기본적인 정보들이 담기는 공간입니다. 해당 헤더는 작은 구조체들의 덩어리입니다. 크기가 정해져 있고, 정해진 값들이 들어갑니다. 따라서, 해당 해더의 값을 잘 뜯어보기만 하면 쉽게 분석할 수 있을 것입니다.

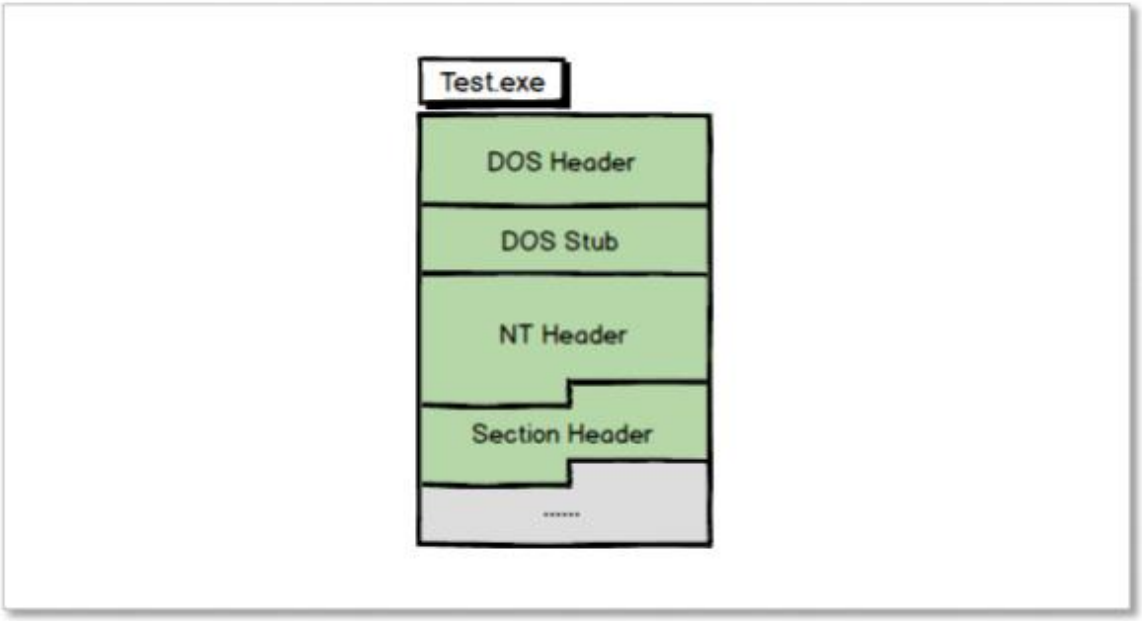


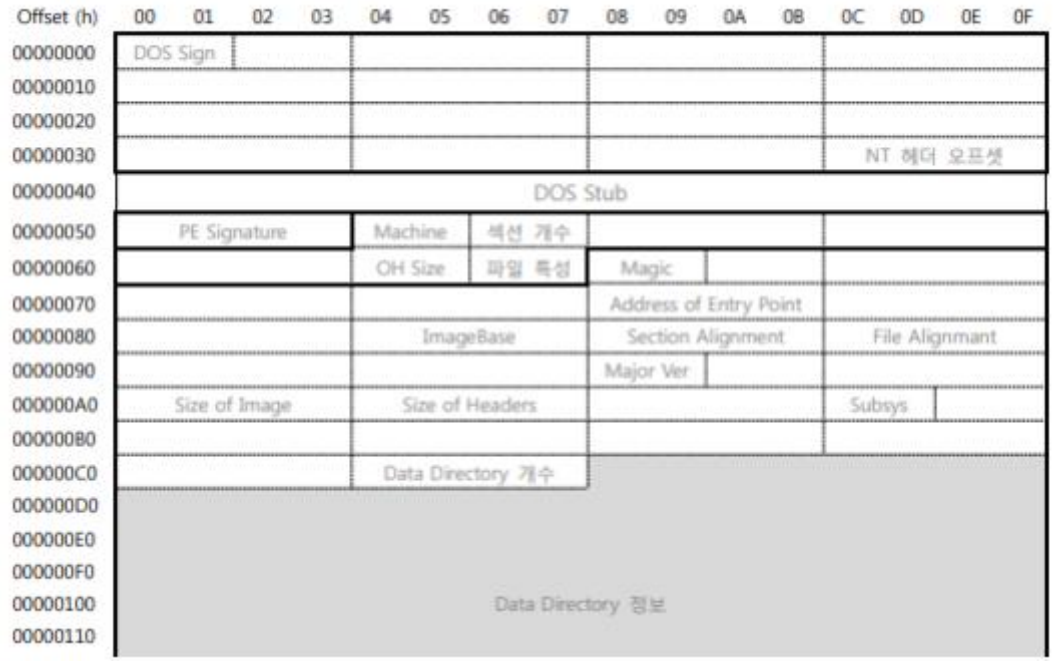
그림 2-1 PE 헤더

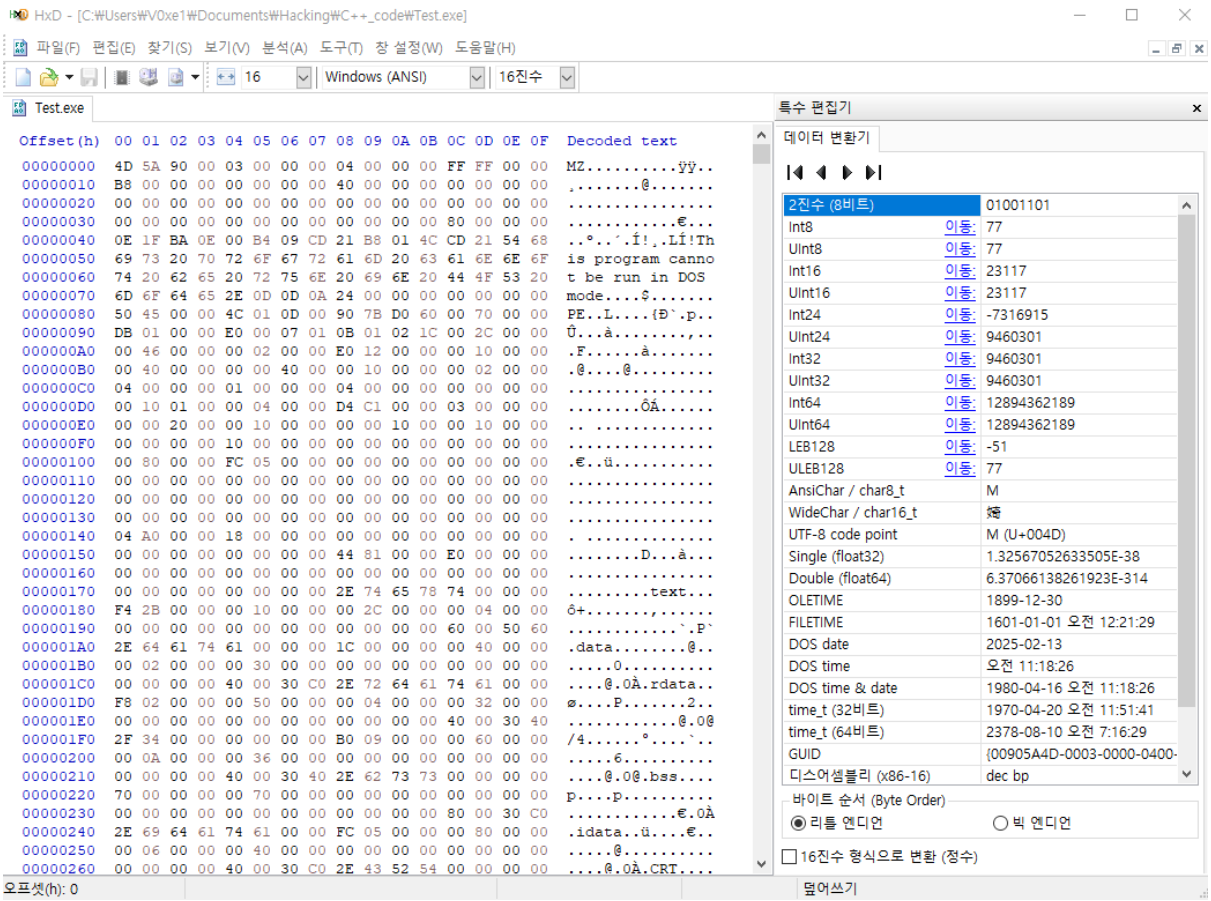
이제 그럼 PE Header의 내용을 봅시다. PDF에 설명이 잘 되어 있습니다.

DOS Header	DOS Header는 DOS와 호환성을 위해서 만들었습니다. 파일의 처음에 위치하고, 0x40 크기를 가집니다.
DOS Stub	PE 파일이 MS-DOS에서 실행 될 경우, 화면에 출력될 메시지와 코드가 기록되어 있습니다. DOS Stub은 옵션이기 때문에 파일 실행에 영향이 없습니다. 크기가 일정하지 않고, 없어도 되는 영역입니다.
NT Header	파일 실행에 필요한 전반적인 정보를 가지고 있습니다. 0xF8 크기를 가집니다.
Section Header	각 섹션의 속성 정보를 가지고 있습니다.

표 2-1 PE 헤더 주요 항목 정보

그럼 이러한 정보들을 어떻게 보고, 확인할 수 있는냐면, 바로 이전 문서에서 다룬 HxD 를 통해서 파일을 볼 수 있습니다.





해당 사진을 보면, Test.exe를 HxD로 열었을 때 데이터가 각의 공간에 값들이 알맞게 적혀있음을 알 수 있습니다.