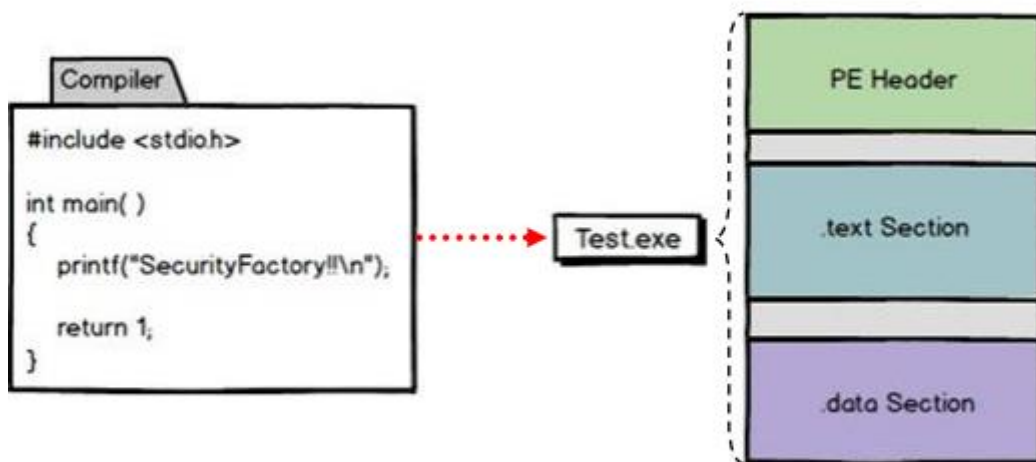


## [PE File Format 이해하기]

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 헤더의 값을 잘 뜯어보기만 하면 쉽게 분석할 수 있을 것입니다.

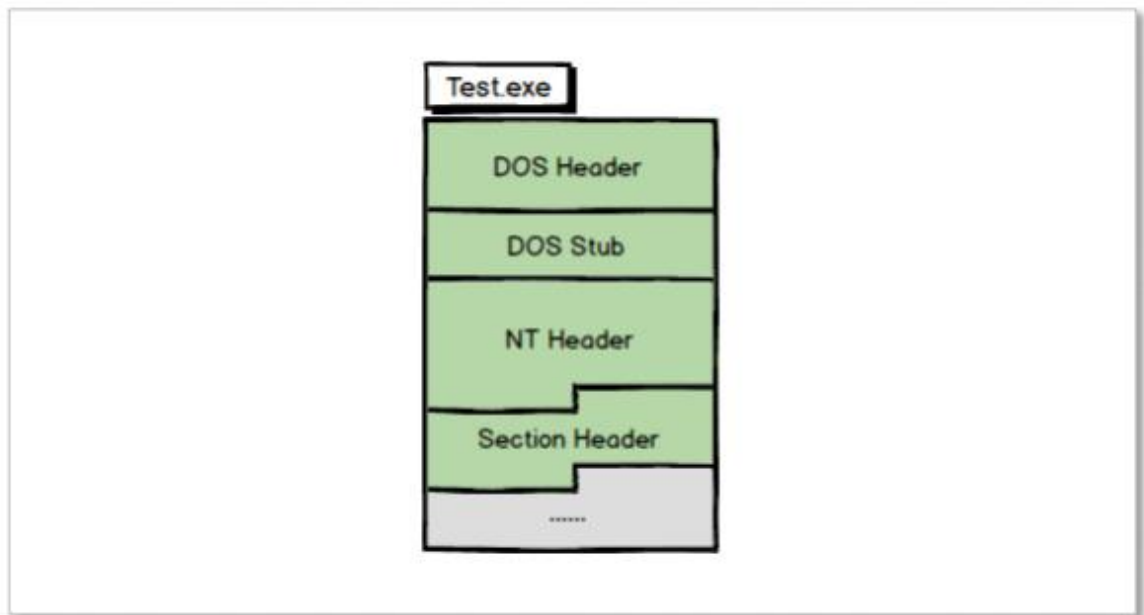


그림 2-1 PE 헤더

이제 그림 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 HxD를 통해서 파일을 볼 수 있습니다.

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F		
00000000	DOS Sign																	
00000010																		
00000020																		
00000030																NT 헤더 오프셋		
00000040	DOS Stub																	
00000050	PE Signature			Machine		섹션 개수												
00000060				OH Size		파일 특성		Magic										
00000070							Address of Entry Point											
00000080				ImageBase			Section Alignment			File Alignment								
00000090							Major Ver											
000000A0	Size of Image			Size of Headers									Subsys					
000000B0																		
000000C0				Data Directory 개수														
000000D0	Data Directory 정보																	
000000E0																		
000000F0																		
00000100																		
00000110																		
00000110																		

HxD - [C:\Users\V0xe1\Documents\Hacking\VC++\_code\Test.exe]

파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 도구(T) 창 설정(W) 도움말(H)

16 Windows (ANSI) 16진수

Test.exe

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ.....yy..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	.....@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	80	00	00	00	.....e...
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	...°.!.Li!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....\$. ....
00000080	50	45	00	00	4C	01	0D	00	90	7B	D0	60	00	70	00	00	PE..L....{B`.p..
00000090	DB	01	00	00	E0	00	07	01	0B	01	02	1C	00	2C	00	00	U...à.....,
000000A0	00	46	00	00	00	02	00	00	E0	12	00	00	00	10	00	00	.F.....à.....
000000B0	00	40	00	00	00	00	40	00	10	00	00	00	00	02	00	00	.@....@.....
000000C0	04	00	00	00	01	00	00	00	04	00	00	00	00	00	00	00	.....ôÀ.....
000000D0	00	10	01	00	00	04	00	00	D4	C1	00	00	03	00	00	00	.....
000000E0	00	00	20	00	00	10	00	00	00	00	00	10	00	00	00	00	.....
000000F0	00	00	00	00	10	00	00	00	00	00	00	00	00	00	00	00	.....
00000100	00	80	00	00	FC	05	00	00	00	00	00	00	00	00	00	00	.e...ü.....
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000140	04	A0	00	00	18	00	00	00	00	00	00	00	00	00	00	00	.....
00000150	00	00	00	00	00	00	00	00	44	81	00	00	E0	00	00	00	.....D...à...
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000170	00	00	00	00	00	00	00	00	2E	74	65	78	74	00	00	00	.....text...
00000180	F4	2B	00	00	00	10	00	00	00	2C	00	00	00	04	00	00	6+.....
00000190	00	00	00	00	00	00	00	00	00	00	00	00	60	00	50	60	.....P`
000001A0	2E	64	61	74	61	00	00	1C	00	00	00	00	40	00	00	00	..data.....@..
000001B0	00	02	00	00	00	30	00	00	00	00	00	00	00	00	00	00	.....0.....
000001C0	00	00	00	00	40	00	30	C0	2E	72	64	61	74	61	00	00	....@.À..rdata..
000001D0	F8	02	00	00	00	50	00	00	00	04	00	00	00	32	00	00	ø....P.....2..
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	40	00	30	40	.....@.00
000001F0	2F	34	00	00	00	00	00	00	B0	09	00	00	00	60	00	00	/4.....°.....
00000200	00	0A	00	00	00	36	00	00	00	00	00	00	00	00	00	00	.....6.....
00000210	00	00	00	00	40	00	30	40	2E	62	73	73	00	00	00	00	....@.00.bss....
00000220	70	00	00	00	00	70	00	00	00	00	00	00	00	00	00	00	P....P.....
00000230	00	00	00	00	00	00	00	00	00	00	00	80	00	30	C0	00	.....e.0A
00000240	2E	69	64	61	74	61	00	00	FC	05	00	00	00	80	00	00	..idata...ü....e..
00000250	00	06	00	00	40	00	00	00	00	00	00	00	00	00	00	00	.....
00000260	00	00	00	00	40	00	30	C0	2E	43	52	54	00	00	00	00	....@.0A.CRT....

오프셋(h): 0

특수 편집기

데이터 변환기

2진수 (8비트) 01001101

Int8 이동: 77

UInt8 이동: 77

Int16 이동: 23117

UInt16 이동: 23117

Int24 이동: -7316915

UInt24 이동: 9460301

Int32 이동: 9460301

UInt32 이동: 9460301

Int64 이동: 12894362189

UInt64 이동: 12894362189

LEB128 이동: -51

ULEB128 이동: 77

AnsiChar / char\_t M

WideChar / char16\_t M

UTF-8 code point M (U+004D)

Single (float32) 1.32567052633505E-38

Double (float64) 6.37066138261923E-314

OLETIME 1899-12-30

FILETIME 1601-01-01 오전 12:21:29

DOS date 2025-02-13

DOS time 오전 11:18:26

DOS time & date 1980-04-16 오전 11:18:26

time\_t (32비트) 1970-04-20 오전 11:51:41

time\_t (64비트) 2378-08-10 오전 7:16:29

GUID {00905A4D-0003-0000-0400-00000000}

디스어셈블리 (x86-16) dec bp

바이트 순서 (Byte Order)

☒ 리틀 엔디언 ☐ 빅 엔디언

☐ 16진수 형식으로 변환 (정수)

덮어쓰기

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