

# *OLE File structure*

My name

송태현

SCP 2 grade

<https://r-ever-scp.tistory.com>

**Start**

The only thing worse than starting something and failing...  
is not starting something

## **1. What is OLE**

## **2. hwp file analysis**

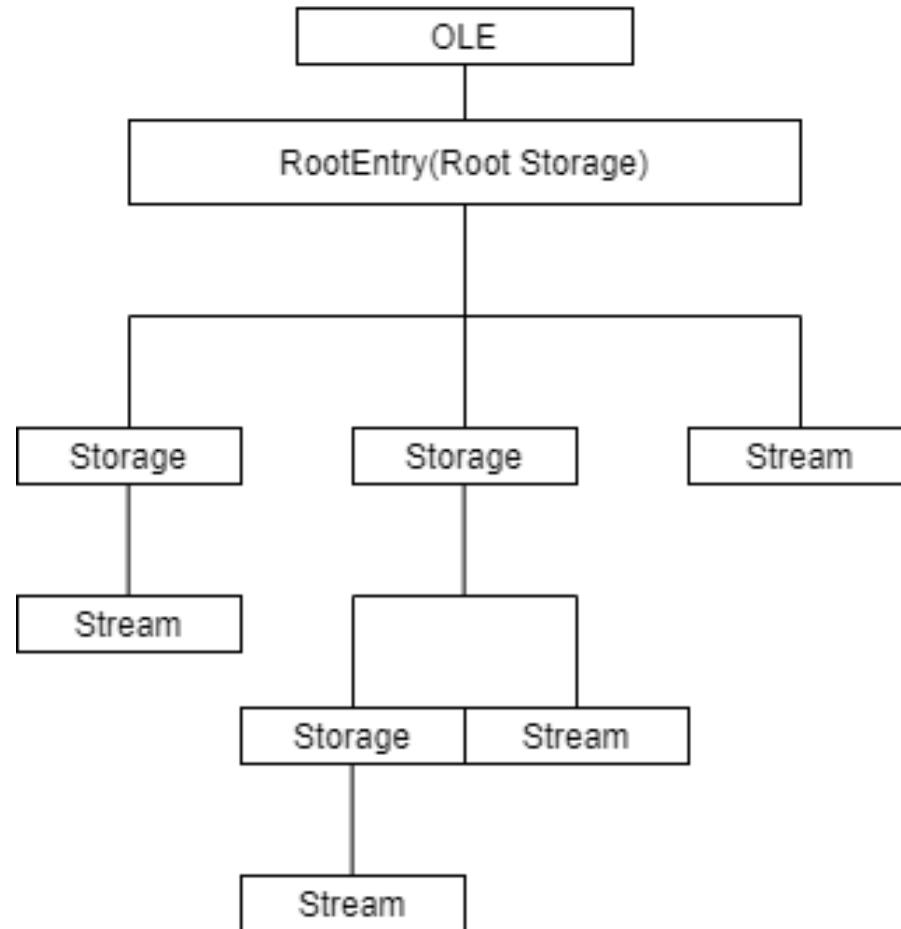
## **3. ETC**

## *1. What is OLE file*

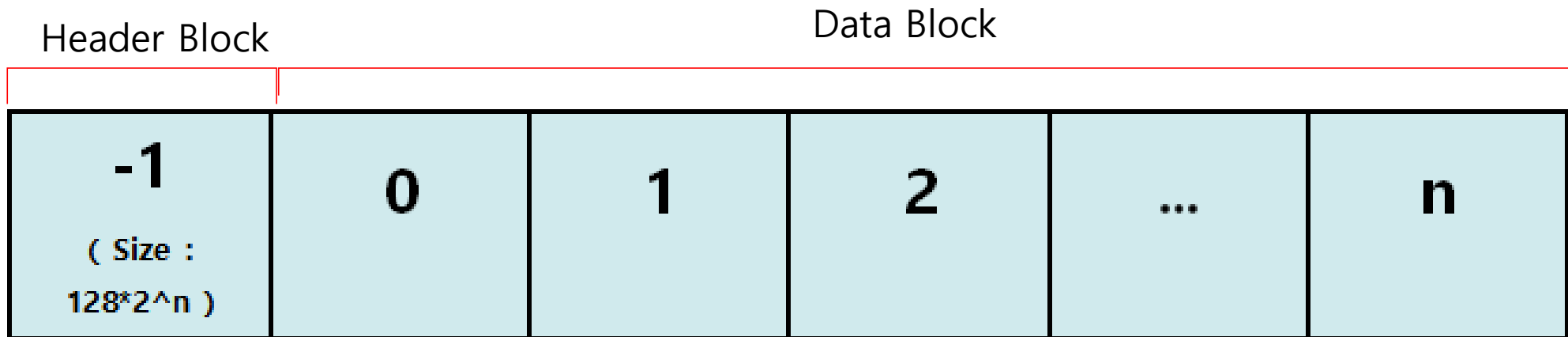


# 1. What is OLE file

OLE파일 구조



# 1. What is OLE file



00000000	D0 CF 11 E0 A1 B1 1A E1 00 00 00 00 00 00 00 00	Đİ.à;±.á.....
00000010	00 00 00 00 00 00 00 00 3E 00 03 00 FE FF 09 00	.....>...pÿ..
00000020	06 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00	.....
00000030	02 00 00 00 00 00 00 00 00 00 10 00 00 06 00 00	.....
00000040	01 00 00 00 FE FF FF FF 00 00 00 00 03 00 00 00	....pÿÿÿ.....
00000050	FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF	000000000000000000000000
00000060	FF FF FF FF F	
00000070	FF FF FF FF F	
00000080	FF FF FF FF F	
00000090	FF FF FF FF F	
000000A0	FF FF FF FF F	
000000B0	FF FF FF FF F	
000000C0	FF FF FF FF F	
000000D0	FF FF FF FF F	
000000E0	FF FF FF FF F	

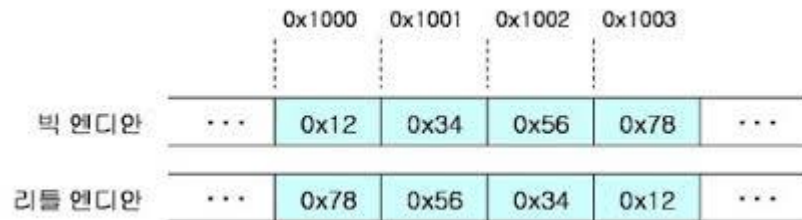
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x00	OLE File Signature (0xE11AB1A1E011CFD0)								Header CISID							
0x10									Mini Version		Major Version		Byte order Identifier		Sector Shift	
0x20	Mini Sector Shift		예약 영역						Directory Sectors 개수				FAT Sectors 개수			
0x30	SEC ID				Transaction Signature Number				Mini Stream Cutoff Size				Mini FAT 위치			
0x40	Mini FAT 개수				First DIFAT Sector Location				DIFAT Sector의 개수				FAT #N 위치			
~ 0x1F0	0xFFFFFFFF															

## 2 - 1. OLE Header

```

00000000 D0 CF 11 E0 A1 B1 1A E1 00 00 00 00 00 00 00 00
00000010 00 00 00 00 00 00 00 00 3E 00 03 00 FE FF 09 00
00000020 06 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00
00000030 02 00 00 00 00 00 00 00 00 10 00 00 06 00 00 00
00000040 01 00 00 00 FE FF FF FF 00 00 00 00 03 00 00 00
00000050 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000060 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000070 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000080 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000090 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000A0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000B0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000C0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000D0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000E0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

```



파일 시그니처 : hwp 뿐만 아니라 DOC 이나 PPT 파일등에서도 볼 수 있는 시그니처 입니다.

major Version : 변경사항과 관련된 버전 정보 0x0003(ver.3) 이나 0x0004(ver.4)로 된다.

Btpe order : 바이트 순서를 리틀 엔디안인지 빅엔디안인지 정하는 곳

sector shift : 섹터의 크기를 정의 하는 곳

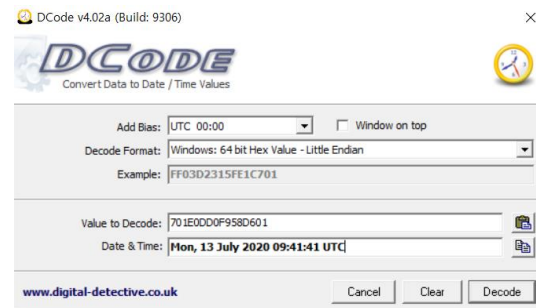
Root Storage Sector ID : Root Entry 시작 섹터 번호  
 $0x02 * 0x200(\text{Sector Size}) + 0x200 (\text{Header Size}) = 0x600$

FAT #n의 위치 : FAT의 위치를 말해준다..

## 2 - 2. Root Directory Entry

00000600	52 00 6F 00 6F 00 74 00 20 00 45 00 6E 00 74 00
00000610	72 00 79 00 00 00 00 00 00 00 00 00 00 00 00
00000620	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000630	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000640	16 00 05 00 FF FF FF FF FF FF FF FF 01 00 00 00
00000650	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000660	00 00 00 00 00 00 00 00 00 00 00 00 70 1E 0D D0
00000670	F9 58 D6 01 07 00 00 00 C0 0C 00 00 00 00 00 00

0 : Empty  
 1 : Storage  
 2 : Stream  
 3 : Lock bytes  
 4 : Property  
 5 : Root Storage



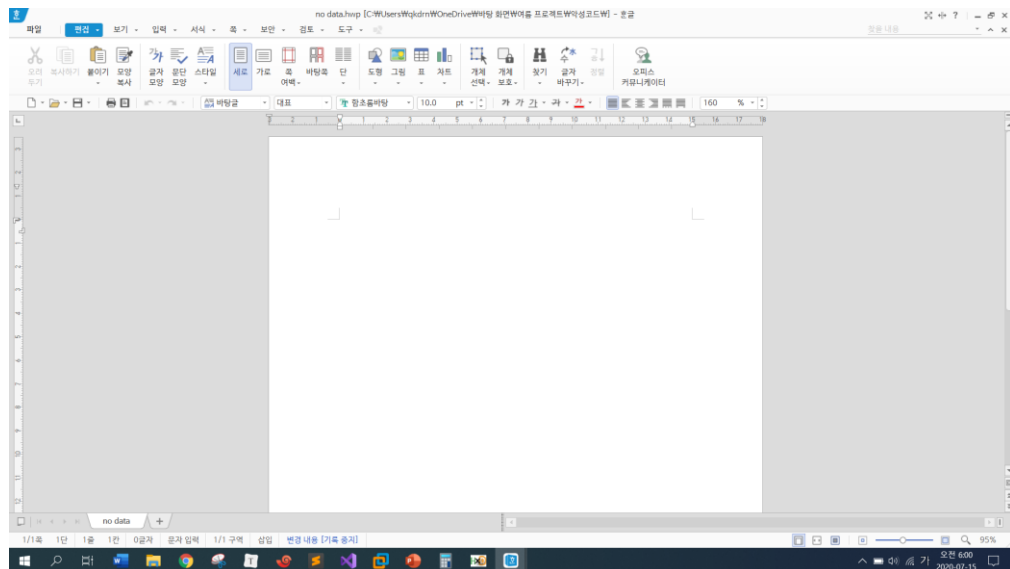
**Directory Entry Name**

**Object Type : 파일의 유형에 따라서 값이 달라집니다.**

**Creation Time : 생성시간**

**Modified Time : 수정시간 UTC 시간으로 저장**

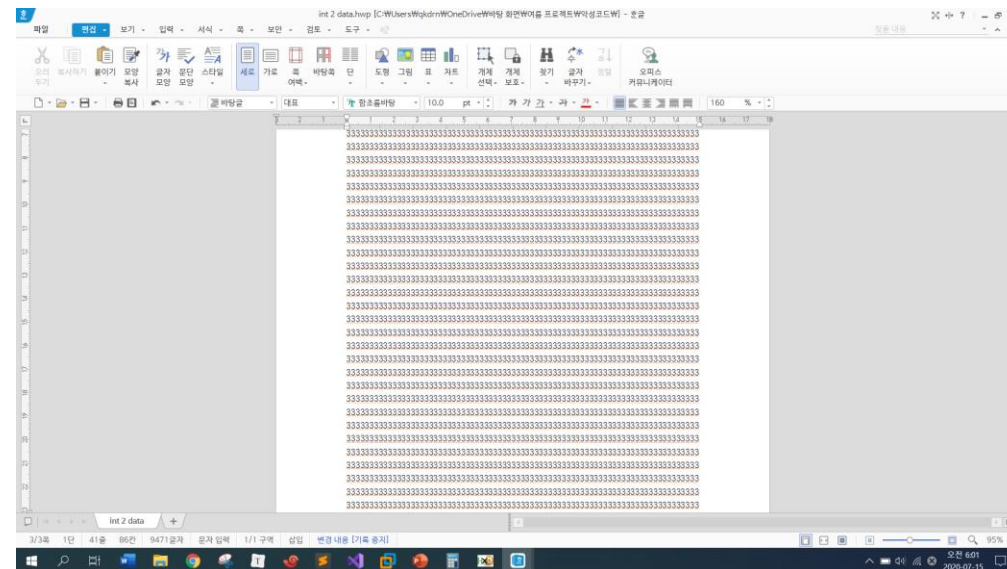




```

00000000 D0 CF 11 E0 A1 B1 1A E1 00 00 00 00 00 00 00
00000010 00 00 00 00 00 00 00 00 3E 00 03 00 FE FF 09 00
00000020 06 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00
00000030 02 00 00 00 00 00 00 00 00 10 00 00 06 00 00 00
00000040 01 00 00 00 FE FF FF FF 00 00 00 00 03 00 00 00

```



```

00000000 D0 CF 11 E0 A1 B1 1A E1 00 00 00 00 00 00 00 00
00000010 00 00 00 00 00 00 00 00 3E 00 03 00 FE FF 09 00
00000020 06 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00
00000030 02 00 00 00 00 00 00 00 00 10 00 00 06 00 00 00
00000040 01 00 00 00 FE FF FF FF 00 00 00 00 03 00 00 00

```

```

000005D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000005E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000005F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000600 52 00 6F 00 6F 00 74 00 20 00 45 00 6E 00 74 00 R.o.o.t. .E.n.t.
00000610 72 00 79 00 00 00 00 00 00 00 00 00 00 00 00 00 r.y.....
00000620 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000630 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000640 16 00 05 00 FF FF FF FF FF FF FF FF 01 00 00 00 ....yyyyyyyy...
00000650 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000660 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000670 20 5A D6 01 07 00 00 00 40 18 00 00 00 00 00 00 ZÖ.....[E
00000680 45 00 66 00 66 00 65 00 45 00 65 00 61 00 64 00 F.i.l.e.U.n.d.

```

```

000005E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000005F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000600 52 00 6F 00 6F 00 74 00 20 00 45 00 6E 00 74 00 R.o.o.t. .E.n.t.
00000610 72 00 79 00 00 00 00 00 00 00 00 00 00 00 00 00 r.y.....
00000620 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000630 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000640 16 00 05 00 FF FF FF FF FF FF FF FF 01 00 00 00 ...yyyyyyyy...
00000650 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000660 00 00 00 00 00 00 00 00 00 00 00 00 70 1E 0D D0 .....p.Ð
00000670 F9 58 D6 01 07 00 00 00 C0 0C 00 00 00 00 00 00 ùXÖ.....A...
00000680 46 00 69 00 6C 00 65 00 48 00 65 00 61 00 64 00 F.i.l.e.H.e.a.d

```

000016F0	31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00	1.1.1.1.1.1.1.1.
00001700	31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00	1.1.1.1.1.1.1.1.
00001710	31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00	1.1.1.1.1.1.1.1.
00001720	31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00	1.1.1.1.1.1.1.1.
00001730	31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00	1.1.1.1.1.1.1.1.
00001740	31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00	1.1.1.1.1.1.1.1.
00001750	31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00	1.1.1.1.1.1.1.1.
00001760	31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00	1.1.1.1.1.1.1.1.
00001770	31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00	1.1.1.1.1.1.1.1.
00001780	31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00	1.1.1.1.1.1.1.1.
00001790	31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00	1.1.1.1.1.1.1.1.
000017A0	31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00	1.1.1.1.1.1.1.1.
000017B0	31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00	1.1.1.1.1.1.1.1.
000017C0	31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00	1.1.1.1.1.1.1.1.
000017D0	31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00	1.1.1.1.1.1.1.1.
000017E0	31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00	1.1.1.1.1.1.1.1.
000017F0	31 00 31 00 31 00 31 00 31 00 31 00 00 00 00 00	1.1.1.1.1.1.....
00001800	89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52	%PNG.....IHDR
00001810	00 00 02 D4 00 00 04 00 08 06 00 00 00 C1 52 CE	...Ô.....ÁRİf
00001820	F3 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00	ó....sRGB.Ⓢİ.é..
00001830	00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00	..gAMA...±..üa...
00001840	00 09 70 48 59 73 00 00 0E C3 00 00 0E C3 01 C7	..pHYs...Ã...Ã.Ç
00001850	6F A8 64 00 00 5D 57 49 44 41 54 78 5E ED DD C1	o`d..)WIDATx^ıYÄ
00001860	89 A3 59 D7 AC D1 B4 2B 0D 4A 7B CA 9A 74 46 C6	%ŁY×-Ñ'+.J{ÊštFE
00001870	E8 12 D0 F0 F7 85 52 OF BE 13 0A 8E 60 2D D0 A0	è.Ðð÷~R.%...Ž~-Ð

*END*

Q & A