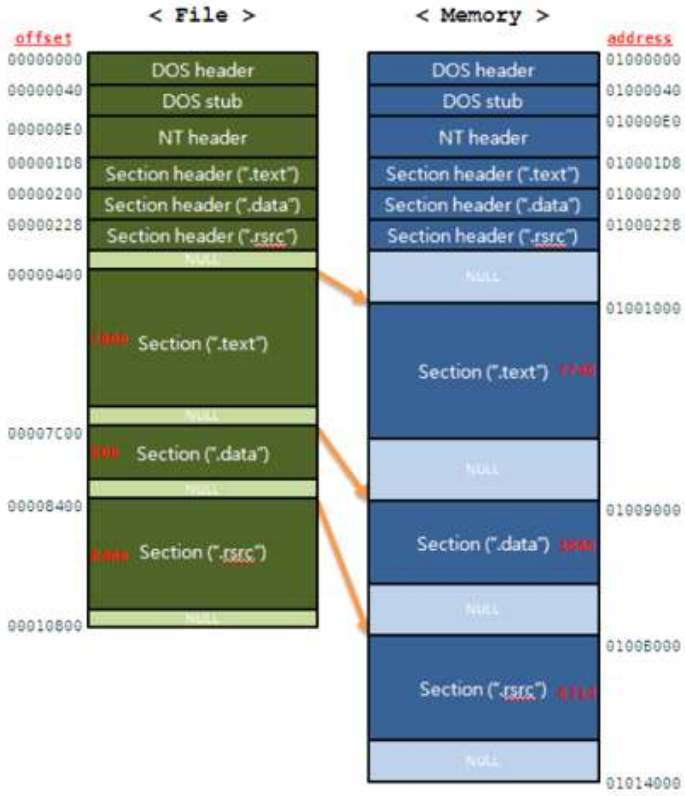
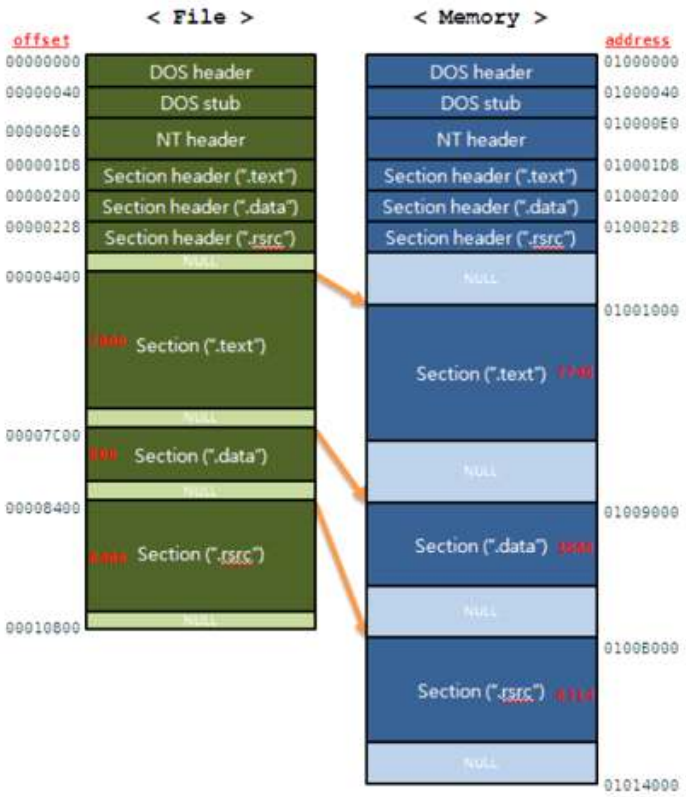


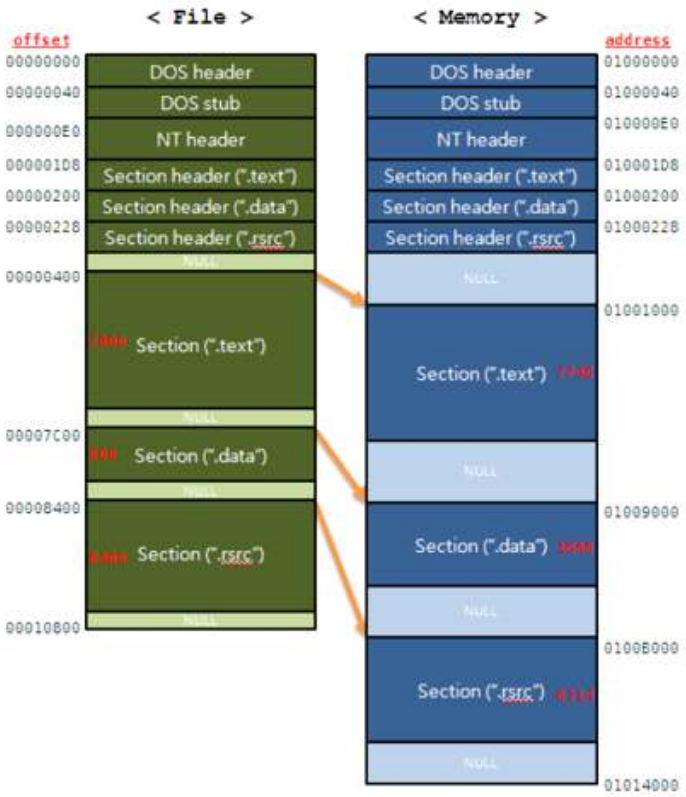
RAW (Realative Virtual Address) : 하드디스크에서 데이터가 실제로 위치하는 주소
PointerToRawData : 하드디스크에서 특정 섹션의 주소

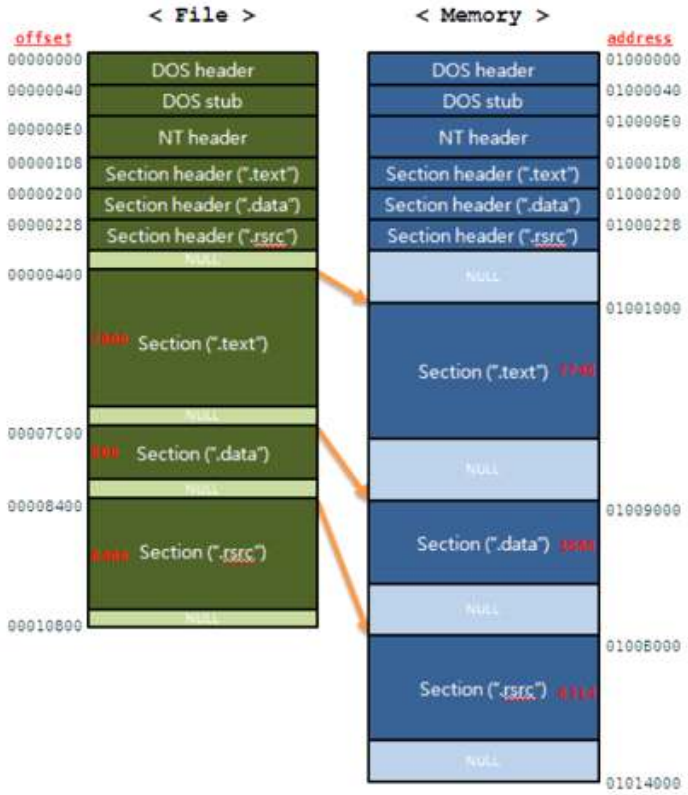
RVA : 특정 코드나 데이터가 메모리 내에서 상대적인 위치
virtualAddress : 메모리에서 특정 섹션에 대한 가상 주소
imagebase : 메모리에서 전체 파일의 시작 주소
VA : 메모리에서 절대 주소를 지칭

RAW - PointerToRawData = RVA - virtualaddress
RAW = RVA - VirtualAddress + PointerToRawData
(메모리 시작 주소 pe)=imagebase

hdd에서 데이터의 실제 위치 = 메모리에서의 위치 - 메모리에서의 특정 섹션의 주소 + 하드 디스크에서 특정 섹션의 주소

실습분류 항목	PE File Analysis	분류번호	Chapter-03
세부분석 항목	RAW(File Offset)	분석대상	RAW 값 구하기 1
RAW 공식	RAW – PointerToRawData = RVA – virtualaddress RAW = RVA – VirtualAddress + PointerToRawData (메모리 시작 주소 pe)=imagebase		
File / Memory Capture			
Question	■ RVA = 5000h ■ PointerToRawData = 400h ▷ RAW(File Offset) 값을 구하시오.		
결과값(RAW)	VA : 01001000 – 01000000 = 1000 5000 – 1000 + 400 = 4400 RAW = 4400 같은 Section으로 메핑이 잘되었다.		

실습분류 항목	PE File Analysis	분류번호	Chapter-03
세부분석 항목	RAW(File Offset)	분석대상	RAW 값 구하기 2
RAW 공식	RAW – PointerToRawData = RVA – virtualaddress RAW = RVA – VirtualAddress + PointerToRawData (메모리 시작 주소 pe)=imagebase		
File / Memory Capture			
Question	■ RVA = 13314h ■ PointerToRawData = 8400h ▷ RAW(File Offset) 값을 구하시오.		
결과값(RAW)	VA : 0100B000 – 01000000 = B000 13314h – B000 + 8400 78612 – + 45056 = 33792 67348 = 10714 메핑이 잘되었다.		

실습분류 항목	PE File Analysis	분류번호	Chapter-03
세부분석 항목	RAW(File Offset)	분석대상	RAW 값 구하기 3
RAW 공식	RAW – PointerToRawData = RVA – virtualaddress RAW = RVA – VirtualAddress + PointerToRawData (메모리 시작 주소 pe)=imagebase		
File / Memory Capture			
Question	■ RVA = ABA8h ■ PointerToRawData = 7C00h ▷ RAW(File Offset) 값을 구하시오.		
결과값(RAW)	VA : 010090000 – 01000000 = 9000 ABA8 – 9000+ 7C00 43944 – 36864 + 31744 38824 = 97A8 해당 프로세스는 메핑 과정에서 오류가 발생함. data –> rsrc		

실습분류 항목	PE File Analysis	분류번호	Chapter-03
세부분석 항목	RAW(File Offset)	분석대상	notepad.exe
Question	▷NOTEPAD.EXE에서 Import되는 첫 번째 리소스(.dll)의 RAW(File Offset) 값을 RAW 공식에 맞춰 구하시오.		
공식에 대비한 PEFILE 멤버 캡처	첫 번째 DLL 이름: ADVAPI32.dll RVA: 0x1000 00001000 00 00 00 FF 15 A4 11 00 01 85 C0 74 48 FF 75 EC . . . . . tH. u. 00000400 2E 63 CD 77 CC 64 CD 77 29 82 CA 77 F0 E8 CB 77 . c. w. d. w) . . w. . . w		
최종 계산식	RVA = 0x1000 PointerToRawData = 0x400 (0x1000 - 0x1000) + 0x400 = 0x0 + 0x400 = 0x400		
공식데 대비한 최종 결과값과 맵핑된 결과값(RAW) 캡처	00000400 2E 63 CD 77 CC 64 CD 77 29 82 CA 77 F0 E8 CB 77 . c. w. d. w) . . w. . . w 계산된 RAW 오프셋: 0x400 .text 섹션의 시작 위치이며, 계산된 최종 결과값 0x400과 일치한다		