

# REPORT:

## PE(Portable Executable) File / (un)packing

COLONY  
1824275 정상지

2021.05.23

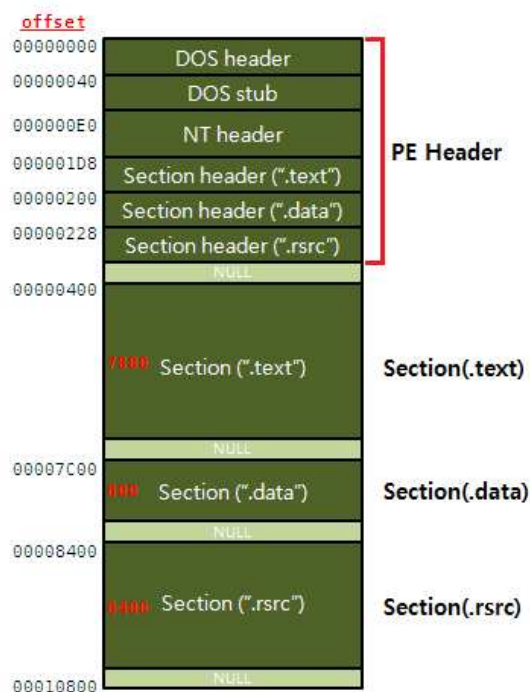
## 1. PE 파일

PE 포맷(Portable Executable)은 윈도우 운영 체제에서 사용되는 실행 파일, DLL, object 코드, FON 폰트 파일 등을 위한 파일 형식으로 PE 포맷은 윈도우 로더가 실행 가능한 코드를 관리하는데 필요한 정보를 캡슐화한 데이터 구조체

### 1) pe 파일 종류

- (1) 실행 계열 : EXE, SCR
- (2) 라이브러리 계열 : DLL, OCX, CPL, DRV
- (3) 드라이버 계열 : SYS, VXD
- (4) 오브젝트 파일 계열 : OBJ

## 2. PE 파일 구조



### 1) PE 구조

- 다양한 정보들이 PE Header에 구조체 형식으로 저장
- 위의 그림처럼 Dos header ~ Section header를 PE header, 그 이후를 PE body
- 파일에서는 offset, 메모리에서는 Virtual Address로 위치를 나타낸다.

### 2) Offset, Virtual Address

- Offset : 파일의 첫 바이트부터 거리
- Virtual Address : 프로세스 가상 메모리의 절대 주소

- RVA : 이미지가 해당 프로세스의 가상 주소 공간 내에 로드되었을 때에 그 시작주소에 대한 상대적 번지 개념. 메모리 상에서의 시작 주소에 대한 PE offset으로 생각하면 됨

### 3) NULL Padding

- PE 헤더 끝과 각 Section 사이사이에 NULL 값이 존재
- 파일 또는 메모리에서 섹션의 시작위치는 각각 최소 기본 단위의 배수에 해당하는 위치여야하므로 빈공간은 Null로 채움

### 4) PE header

#### (1) DOS Header

- DOS 파일에 대한 하위 호환성을 고려하여 만들었으나 Win32에서 PE 파일 실행시 NT header에 대한 offset이 저장되어 있어 해당 주소로 넘어간다

#### (2) DOS Stub

- DOS 환경에서 실행되는 코드를 가진 영역으로 DOS 환경에서 실행하면 "This program cannot be run in Dos mode"라는 문자열을 출력하고 종료한다

#### (3) NT Header

- 파일 실행에 필요한 정보가 저장
- Signature : NT header의 제일 첫 번째 멤버
- File Header : 파일의 계략적인 정보를 나타냄
- Optional Header : 파일 실행에 필요한 주요정보 저장

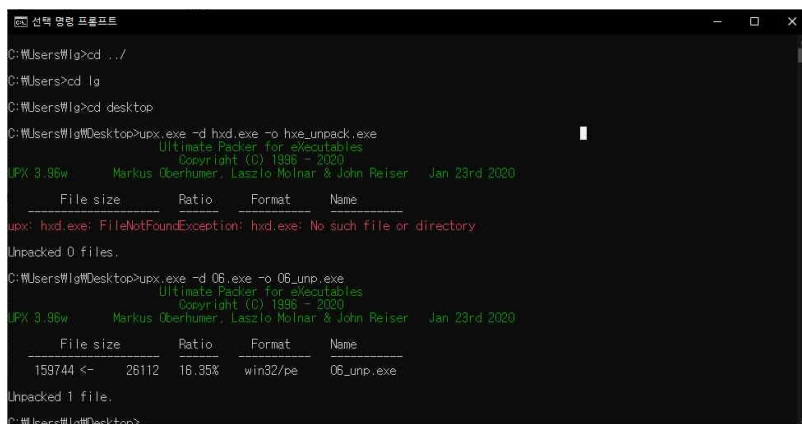
#### (4) Section Header

- 각 Section의 헤더들이 존재하며 Section들은 메타데이터를 저장하고 메모리에 로드될 때 필요한 정보를 포함하고 있다

## 2. PE 파일 패킹/언패킹

### 1) upx를 이용한 PE파일 패킹/언패킹

- upx를 이용하여 pe파일을 패킹 및 언패킹을 할 수 있다

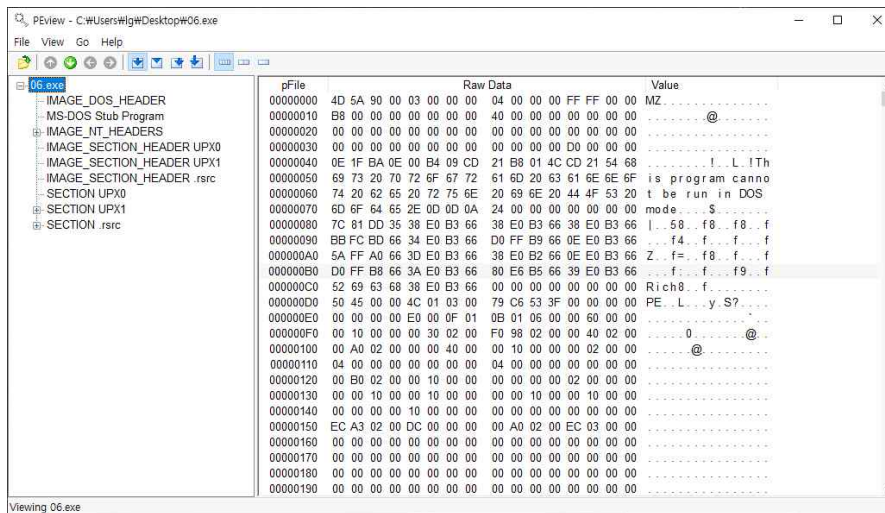


```
선택 명령 프롬프트
C:\Users\lg>cd ../
C:\Users>cd lg
C:\Users\lg>cd desktop
C:\Users\lg\Desktop>upx.exe -d hxd.exe -o hxe_unpack.exe
Ultimate Packer for executables
Copyright (C) 1996 - 2020
UPX 3.95w Markus Oberhumer, Laszlo Molnar & John Reiser Jan 23rd 2020

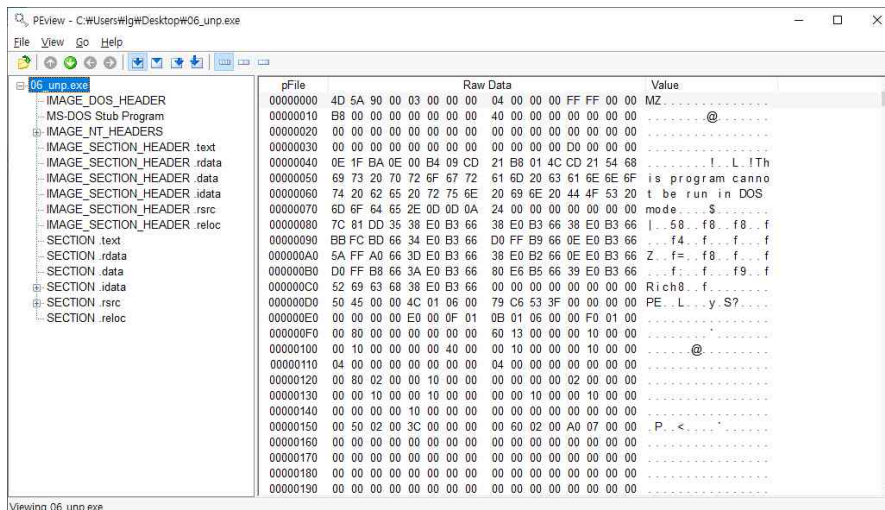
File size      Ratio      Format      Name
-----
upx: hxd.exe: FileNotFoundException: hxd.exe: No such file or directory
Unpacked 0 files.

C:\Users\lg\Desktop>upx.exe -d 06.exe -o 06_unp.exe
Ultimate Packer for executables
Copyright (C) 1996 - 2020
UPX 3.95w Markus Oberhumer, Laszlo Molnar & John Reiser Jan 23rd 2020

File size      Ratio      Format      Name
-----
159744 <-    28112    18.35%    win32/pe    06_unp.exe
Unpacked 1 file.
C:\Users\lg\Desktop>
```



- 언패킹 전의 파일을 pe view를 통해서 pe 헤더 및 바디를 볼 때 Section header UPX0 가 있는 것을 확인 할 수 있다



- 언패킹 후의 파일을 pe view를 통해서 pe 헤더 및 바디를 볼 때 upx의 섹션이 언패킹되어 나타나는 것을 알 수 있다