PEviewer는 Windows 운영 체제에서 실행되는 PE (Portable Executable) 파일의 구조를 분석하고 시각화하는 도구이다. PE 파일은 실행 파일, DLL 파일, 시스템 파일 등 다양한 형태로 존재한다. PEviewer를 사용하면 이러한 파일의 헤더, 섹션 테이블, import 테이블, export 테이블 등을 쉽게 확인할 수 있습니다. PEviewer의 주요 기능 중 하나는 파일의 헤더 정보를 읽어오는 것이다. 이 헤더 정보에는 파일의 기본적인 속성, 엔트리 포인트, 이미지 베이스, 섹션 개수 등이 포함된다. 또한, 섹션 테이블을 분석하여 각 섹션의 이름, 크기, 위치, 속성 등을 확인할 수 있다. 이는 파일이 메모리에 로드될 때 어떻게 배치되는지를 이해하는 데 도움이 된다. import 테이블과 export 테이블을 분석하면 해당 파일이 외부 라이브러리와 어떻게 상호작용하는지, 어떤 함수들을 호출하거나 제공하는지를 알 수 있습니다. 이는 특히 악성코드 분석 시 중요한 정보를 제공한다

Python의 pefile 라이브러리는 PE 파일 형식을 분석하고 조작하는 데 유용한 도구입니다. 이 라이브러리는 PE 파일의 다양한 헤더와 섹션을 쉽게 접근하고 읽을 수 있는 기능을 제공합니다. pefile을 사용하면 DOS 헤더, NT 헤더, 파일 헤더, 옵션 헤더 및 섹션 헤더의 정보를 손쉽게 추출할 수 있습니다. 이번 프로젝트에서는 pefile 라이브러리를 활용하여 PE 파일을 로드하고, 주요 헤더와 섹션 헤더의 정보를 출력하는 PE 파일 뷰어를 구현했습니다.