PE parser 분석

▼ PE 구조

파일이 이식 가능한 다른 곳에 옮겨져도 실행이 가능하도록 만들어놓은 포맷, PE 구조체의 모든 변수 설명은 불필요하며 리버싱에 중요하게 사용되는 멤버 변수 위주

PE 파일의 시작 'MZ' 시그니처

IMAGE_DOS_HEADER : 16 bit 시스템을 위한 구조체, 매직 넘버와 NT 헤더의 위치를 알려주는 두 가지 멤버 변수만 기억 → e_magic, e_lfanew

IMAGE_NT_HEADER

IMAGE_FILE_HEADER

IMAGE_OPTIONAL_HEADER

IMAGE_SECTION_HEADER

PE 시그니처, 코드 사이즈, image base

AddressOfEntryPoint, Data Directory

IAT, 섹션 테이블

▼ **프로그램에 구현할 기능 list**

파일 첨부(경로), hex 뷰어, RVA 계산, PE 구조 다이어그램 색 변화로 현재 보고 있는 지점 확인(?)

메모나 주석을 달 수 있는 기능이 있으면 좋겠다

간이 분석+전체 분석 탭 (원하는 정보를 빠르게 확인할 수 있는 창과 전체 정보를 보여주는 창을 분리)

▼ **기존 툴 분석 - vxpeviewer**

- 제공하는 기능
- **장점**

트리 구조로 헤더 표현, RVA 계산 결과 제공, hex view와 Ascii 값을 직관적으로 보여주어 파일 전체의 구조와 분석 위치를 알기 편리함

hex 값을 다양한 단위로 나누어 확인 가능

인쇄 가능

특정 부분 클릭 시 자동 스크롤로 값 확인 편리(시각화)

다양한 화면 배치 지원(New window, Cascade, Tile, arrange icons)

*PEiD에 비해 **시각화**하여 정보를 보여줘서 좋다! **(파일의 어느 지점에 있는 값인지 확인 가능)***

- **단점**

  사실 단점이 없는 듯.. 보기도 나름 편리하고 편의 기능도 제공하는 좋은 툴인 듯..

  여러 파일을 다중 창으로 볼 수 없다!

  한 번에 한 파일만 열어 구조를 확인할 수 있음

  리버싱에서 주로 확인하는 정보들은 어느 정도 한정되어 있는데, 과도하게 많은 정보를 제공해 실행파일 분석이나 학습 시 어려운 점이 있었음.

  간이 분석(summary)과 전체 분석 두 가지 탭을 제공하면 좋을 듯

  메모나 주석 등을 달고 이를 문서/이미지 형태로 저장하면 좋겠다→용량이 크고 복잡한 파일 분석 시 용이할 것

- 중간발표 자료

  프로젝트 목표 = 처음 보는 사람도 쉽게 사용할 수 있고 내용을 확인할 수 있는 파서 제작(학습에 용이하도록)

  화면 구성 : 파일 hex 값, 각 헤더나 정보에 대한 설명 추가(마우스 오른쪽 버튼 클릭 시), RAW to RVA 주소 출력 창,

<발표 목차>

1. 프로젝트 개요
2. 프로젝트 목적
3. 기획 및 설계
   a. 기존 파서 분석(PEiD, vxpeviewer)
   b. 초기 설계

    c. 문제 발생 → 해결을 위한 과정, 최종 설계
4. 구현 환경 구축
5. pe parser 코드 설명
6. 현재 진행 상황
7. 향후 계획