악성코드 분석

2022년 1학기

한양대학교 컴퓨터소프트웨어학부

임을규

PE file structure

- PE (Portable Executable) file
  - EXE, DLL, SYS, OBJ 등 파일의 형식
  - File structure
    - Header
    - Sections

- WinNT.h 파일 내에 PE 파일 관련 struct가 정의되어 있음
  - IMAGE_DOS_HEADER
  - IMAGE_NT_HEADERS
  - IMAGE_FILE_HEADER
  - IMAGE_OPTIONAL_HEADER32

Header & Body

PE header

- DOS header ~ Section header
- 파일을 실행하기 위한 모든 정보를 포함
- 메모리 적재 방법, EP(entry point), 필요한 DLL 정보 등

PE body

- 실제 실행코드 등을 포함
- 각 정보가 해당하는 섹션에 나뉘어 저장되어 있음
  - .text : 파일의 코드 영역
  - .data : 파일의 데이터(전역 변수 혹은 정적 변수) 영역
  - .rsrc : 파일의 리소스(문자열이나 아이콘 같은 리소스 데이터) 영역

Process Memory Organization

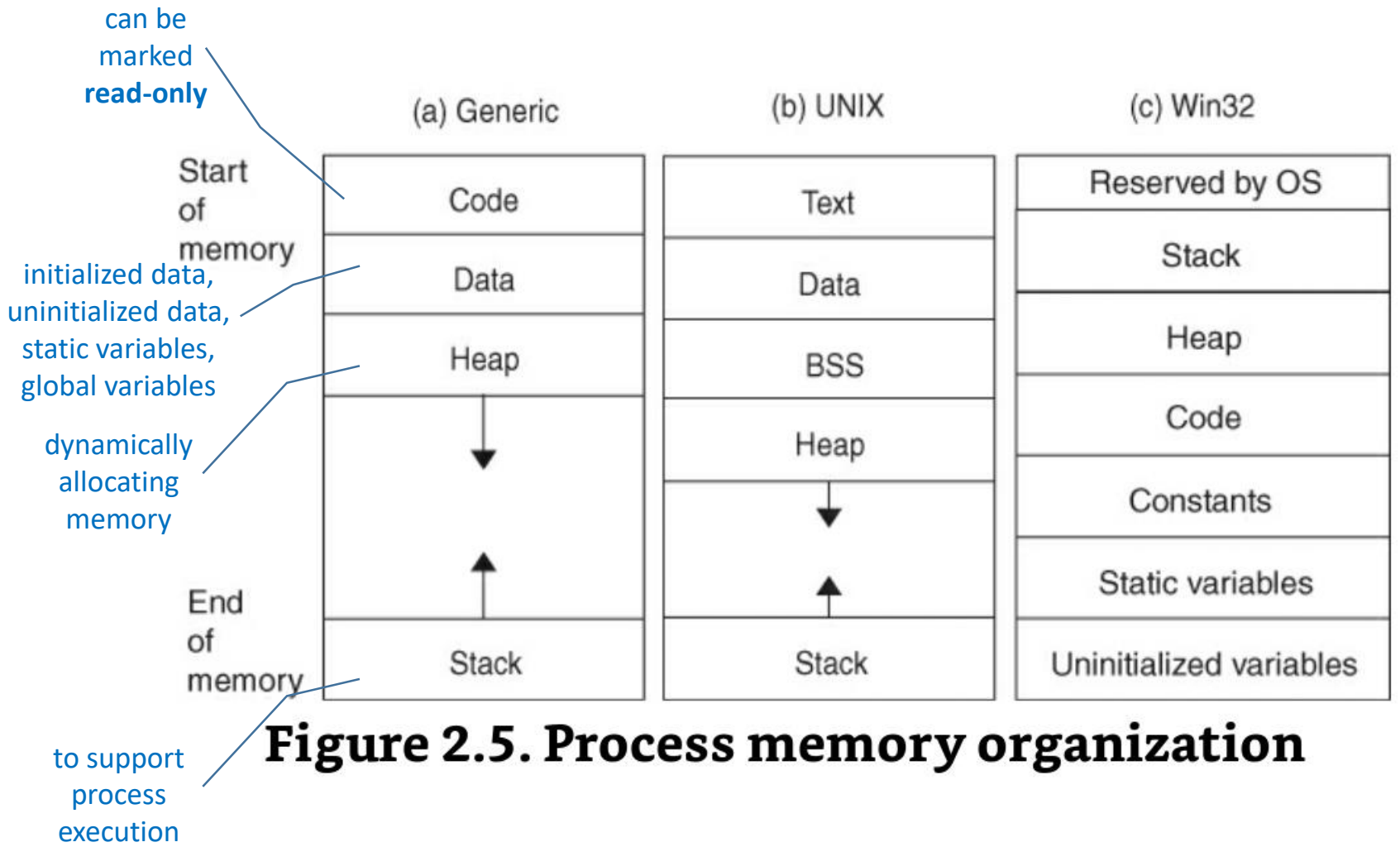
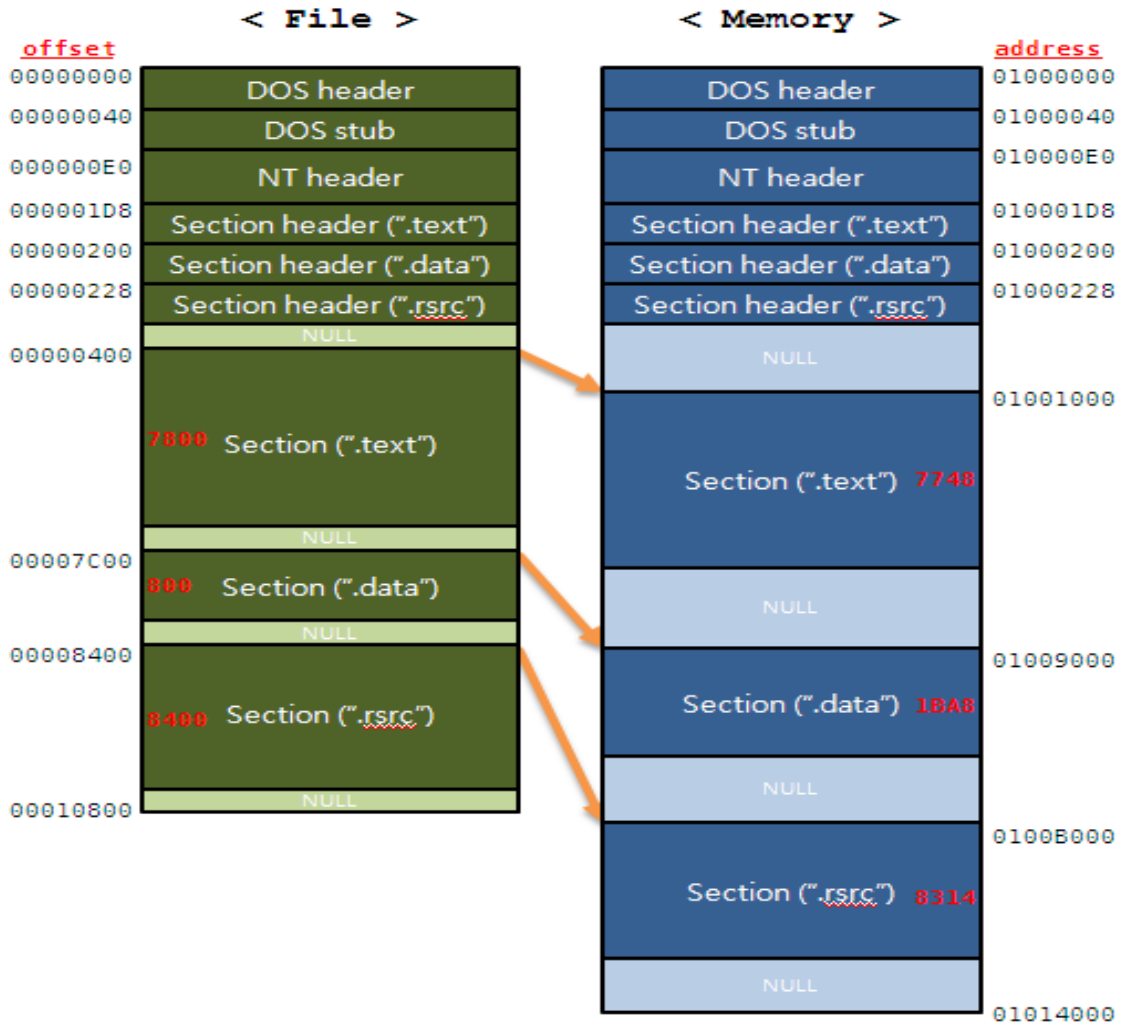


Figure 2.5. Process memory organization

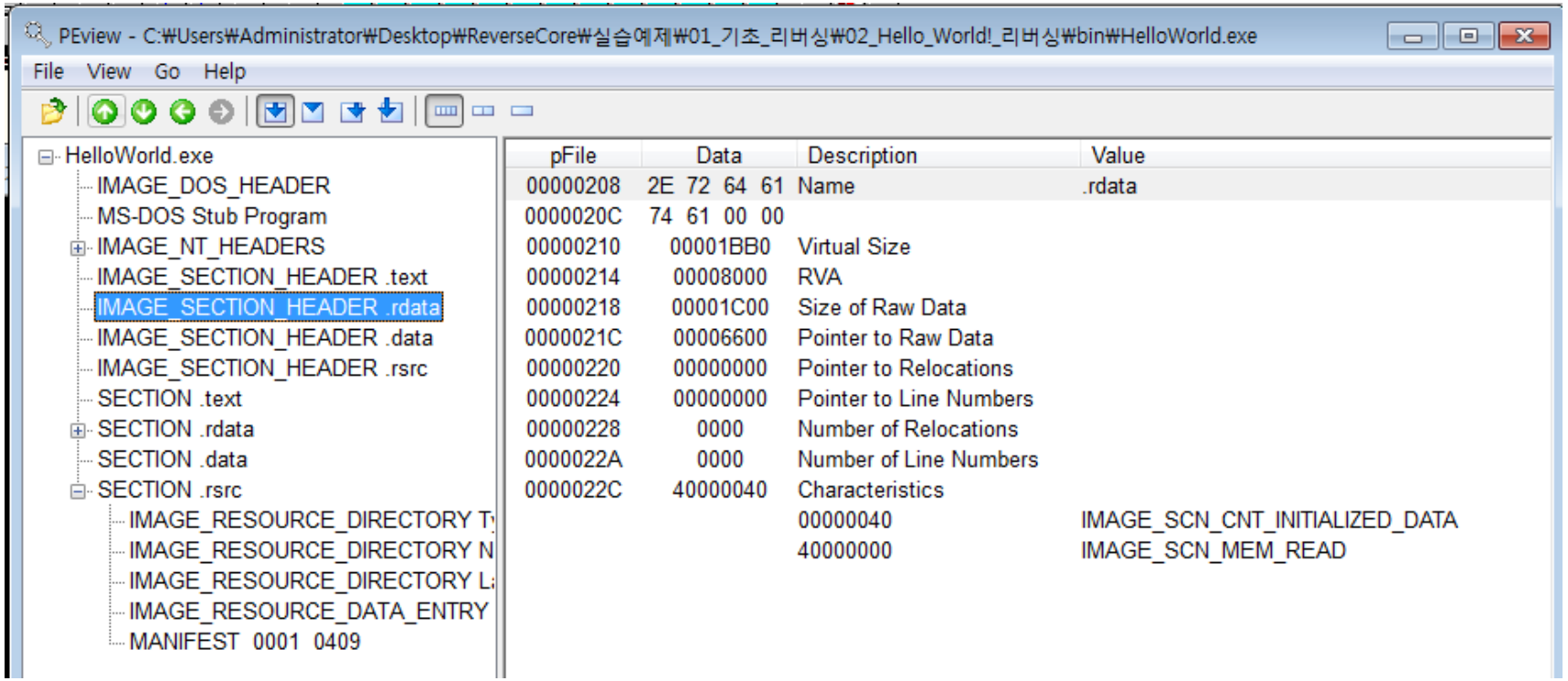
실행 코드

◆ 실행 파일이 memory에 맵핑될 때



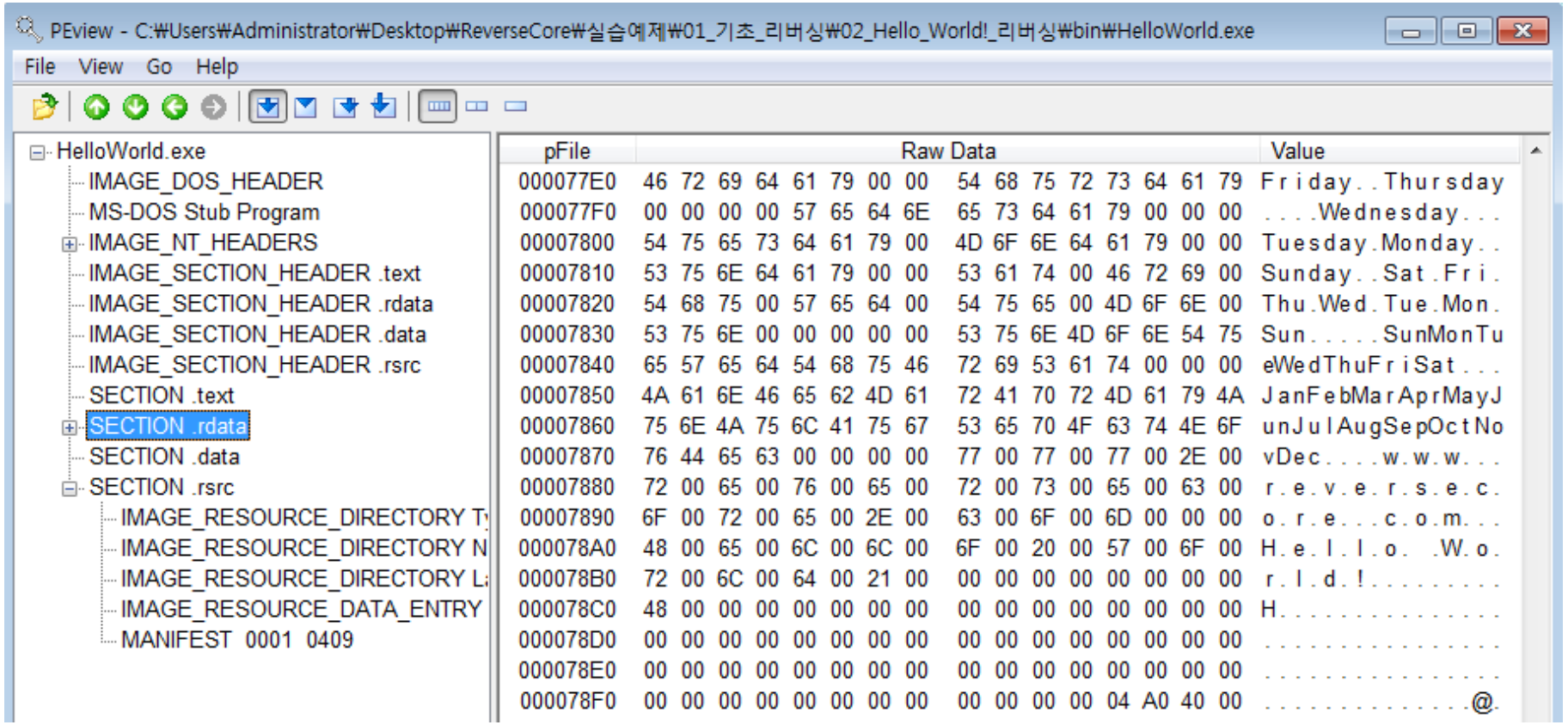
- 무료로 사용 가능한 PE 파일 전용 분석 프로그램
- 주요 기능
  - PE 파일 구조 분석
  - PE header 및 body 정보 출력
  - 구조체별로 정보를 보기 쉽게 표현
  - 각 section의 정보 분석
  - 파일에서의 위치와 메모리상의 위치 변환

Section Header



Section Contents

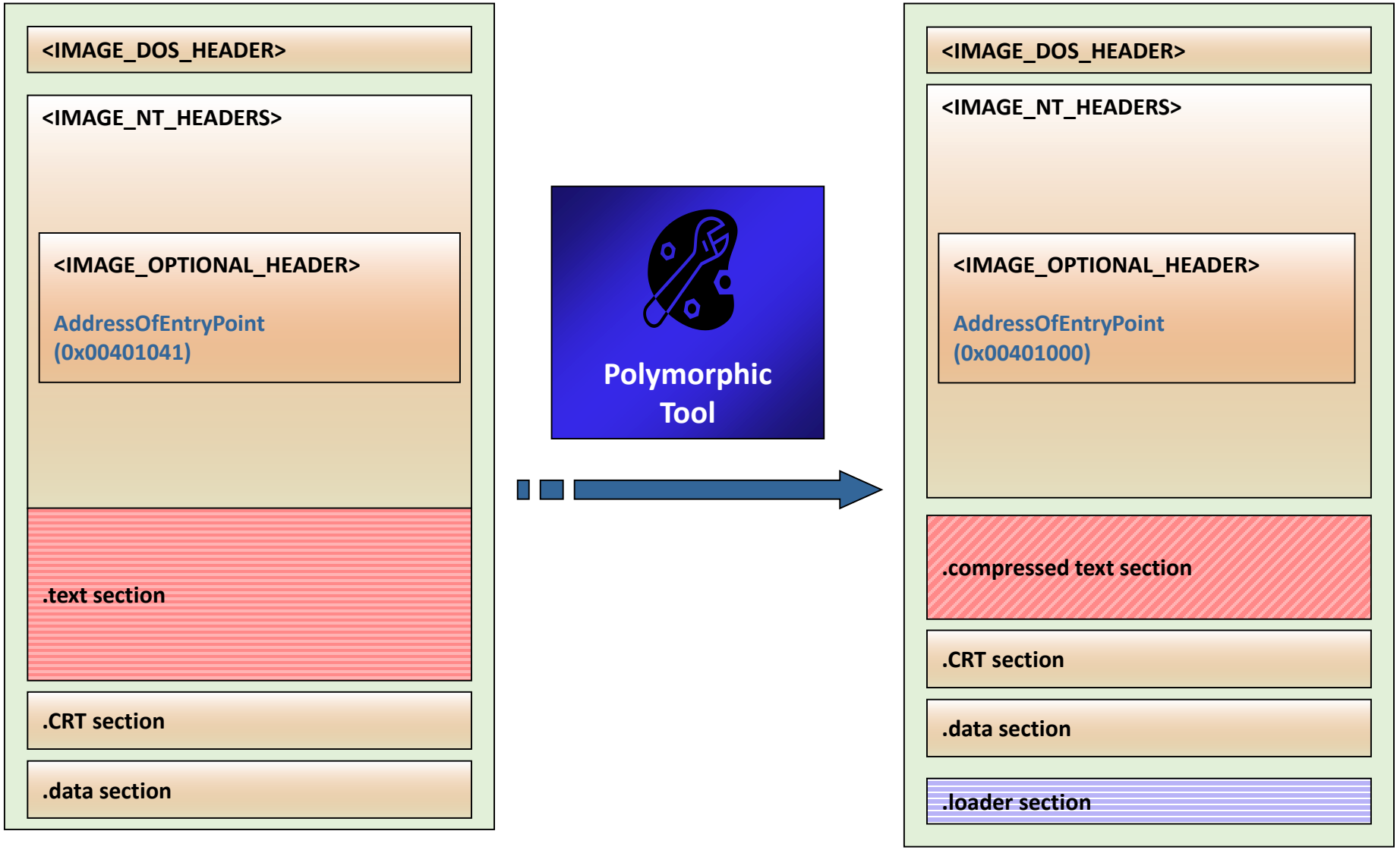
- PE file section 정보



악성코드 분석

- Features from PE files
  - Header information
  - Section names
- IAT (import address table)
  - Addresses of system library functions
- Byte code

Polymorphic malware – Packing technique



Packing detection

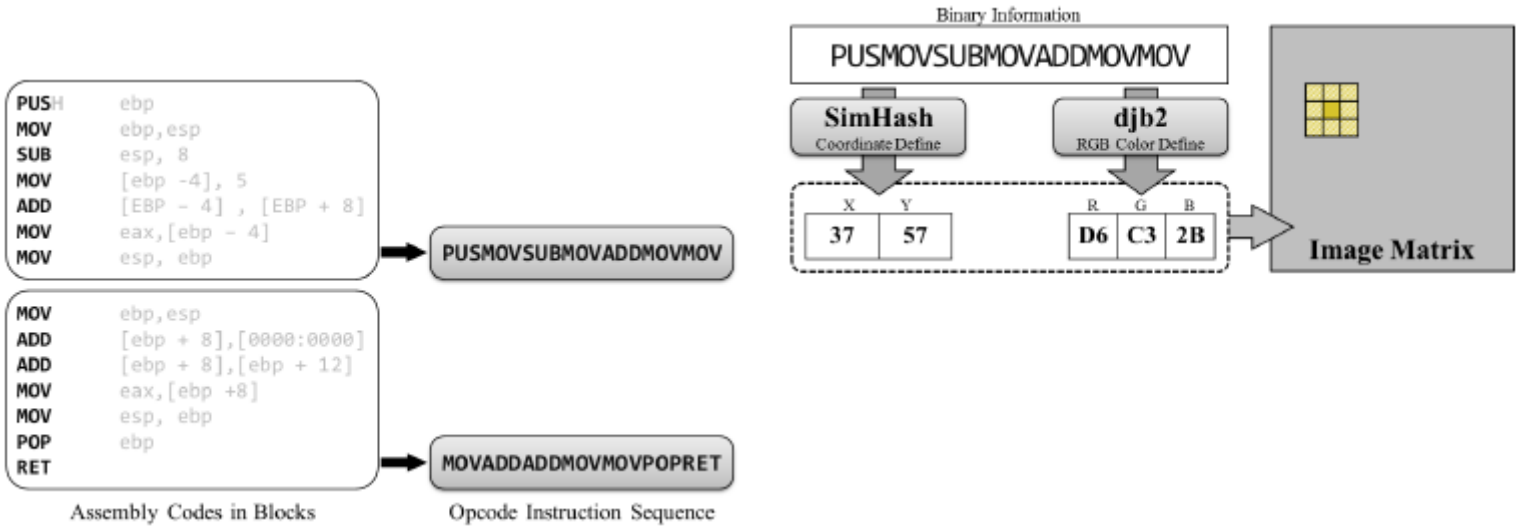
- Entropy
  - 혼잡도
  - $S = -\sum_i p_i \lg p_i$
    - 0.0 ~ 1.0 값을 가짐
    - 0일 때 같은 값으로 만 이루어짐
    - 1일 때는 여러 값이 고루 나타남
- Entropy 를 계산하여 packing 적용 여부를 판단할 수 있음
- Packing이 적용된 실행코드는 bytes 정보로 악성과 정상을 구분하기 어려움

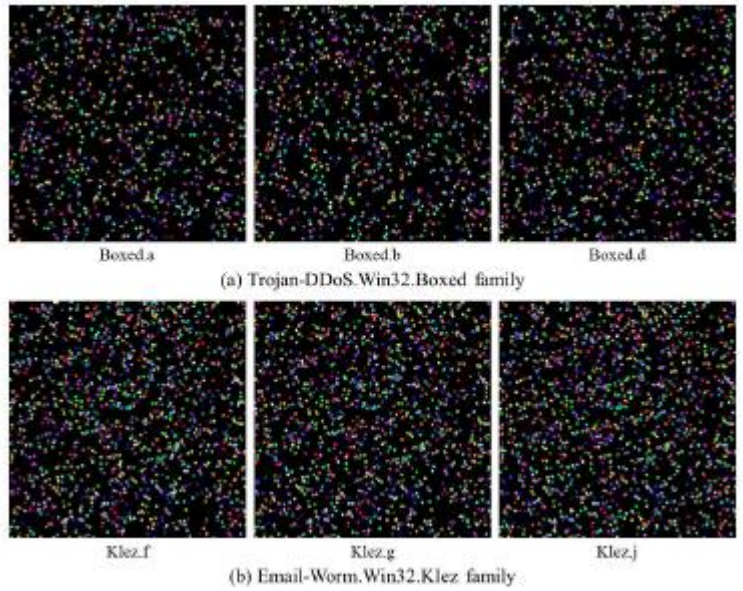
Dynamic Analysis

- 동적 분석 도구
  - Ollydbg
  - Intel PIN tool
  - IDA Pro
  - …
- 특징 정보
  - Instruction sequences
  - API sequences
  - …

Image-based malware analysis

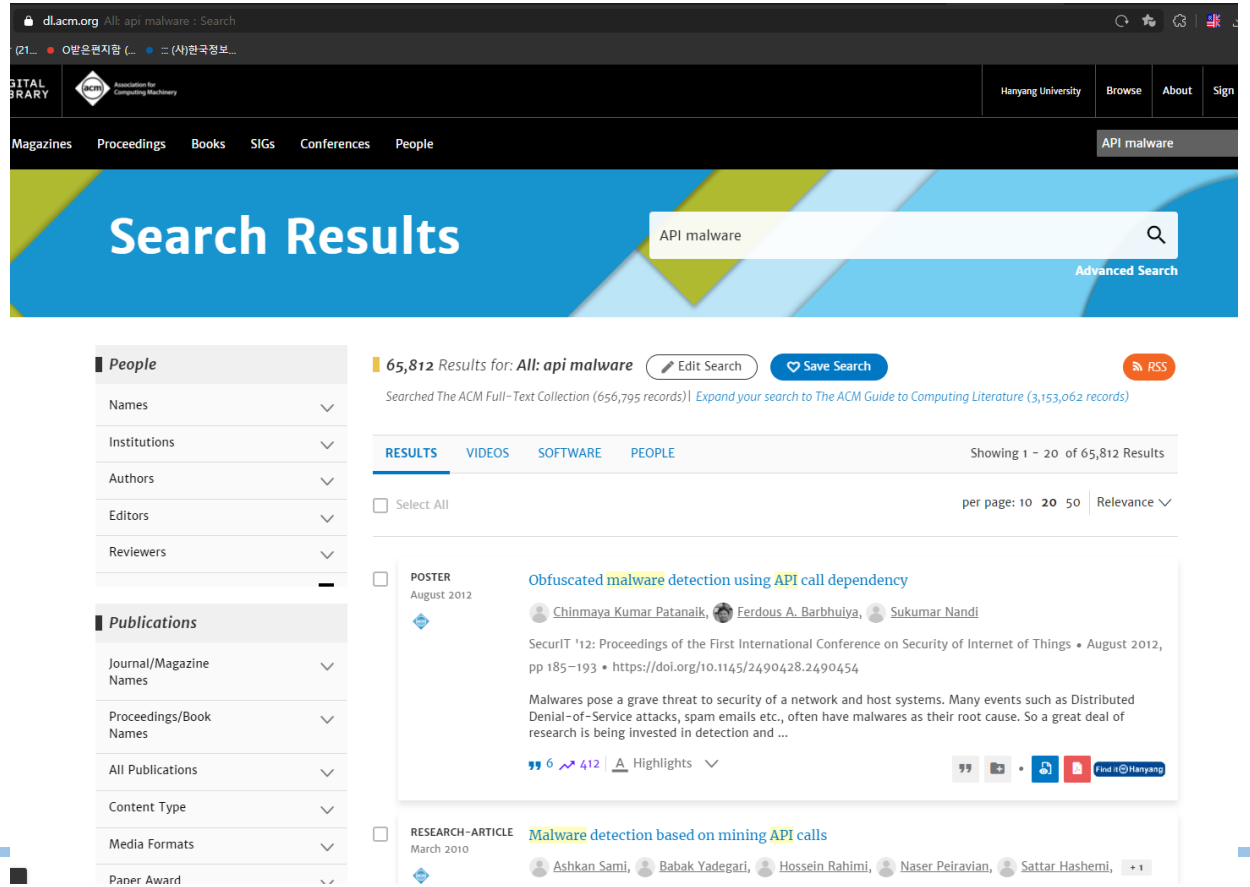
- 관련 논문
  - KS Han, JH Lim, EG Im, “Malware analysis method using visualization of binary files.” In Proceedings of the 2013 Research in Adaptive and Convergent Systems, pp.317-321
- Proposed method





API-based detection

- API sequence
  - 악성 행위를 하기 위해서는 system call을 호출해야 함
  - 호출되는 system call sequence를 분석하여 악성 코드 탐지
  - http://dl.acm.org/




Pytanie
viechoi
pregunta
질문
vraag
Soru
dieFrage
kysymys
quesito
pergunta
percontatio
Question
&
Answer
Bonpoc
pertanyaan
savol
fraga
Kerdes
masahala
tiwen
pyetje
Intrebare
Otazka
acyynT
valasz
balasan
respuesta
vastine
답변
reactie
cautraloi
javob
resposta
dabian
odpoved
magombezi
respons
cevap
responsio
antwoord
reponse
OTBeT
xapNy
RASPUNS
replika
respond
jawaban
Antwort
svar
risposta
referat
usemaji
mabishano