

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

◆ 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

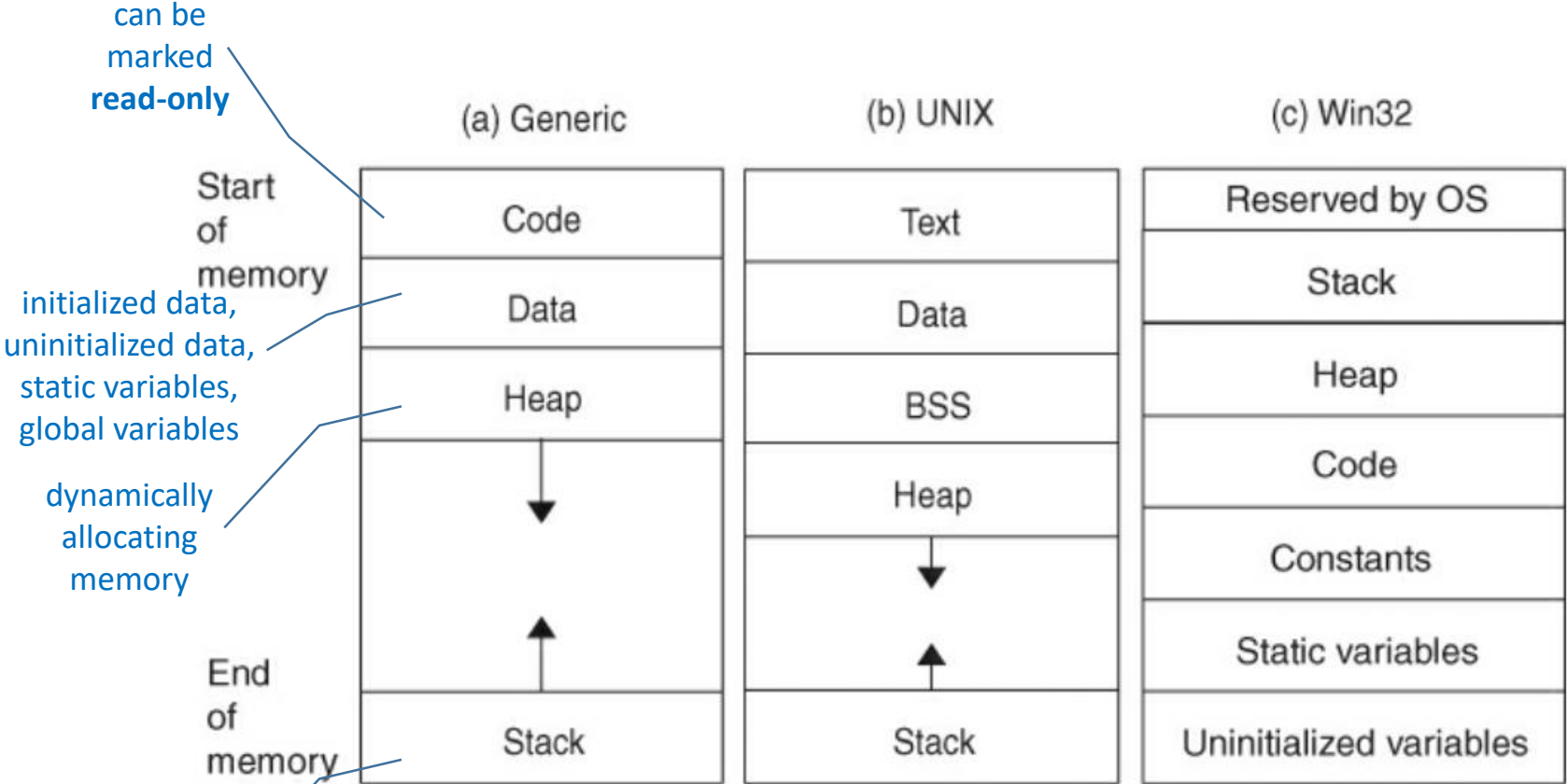
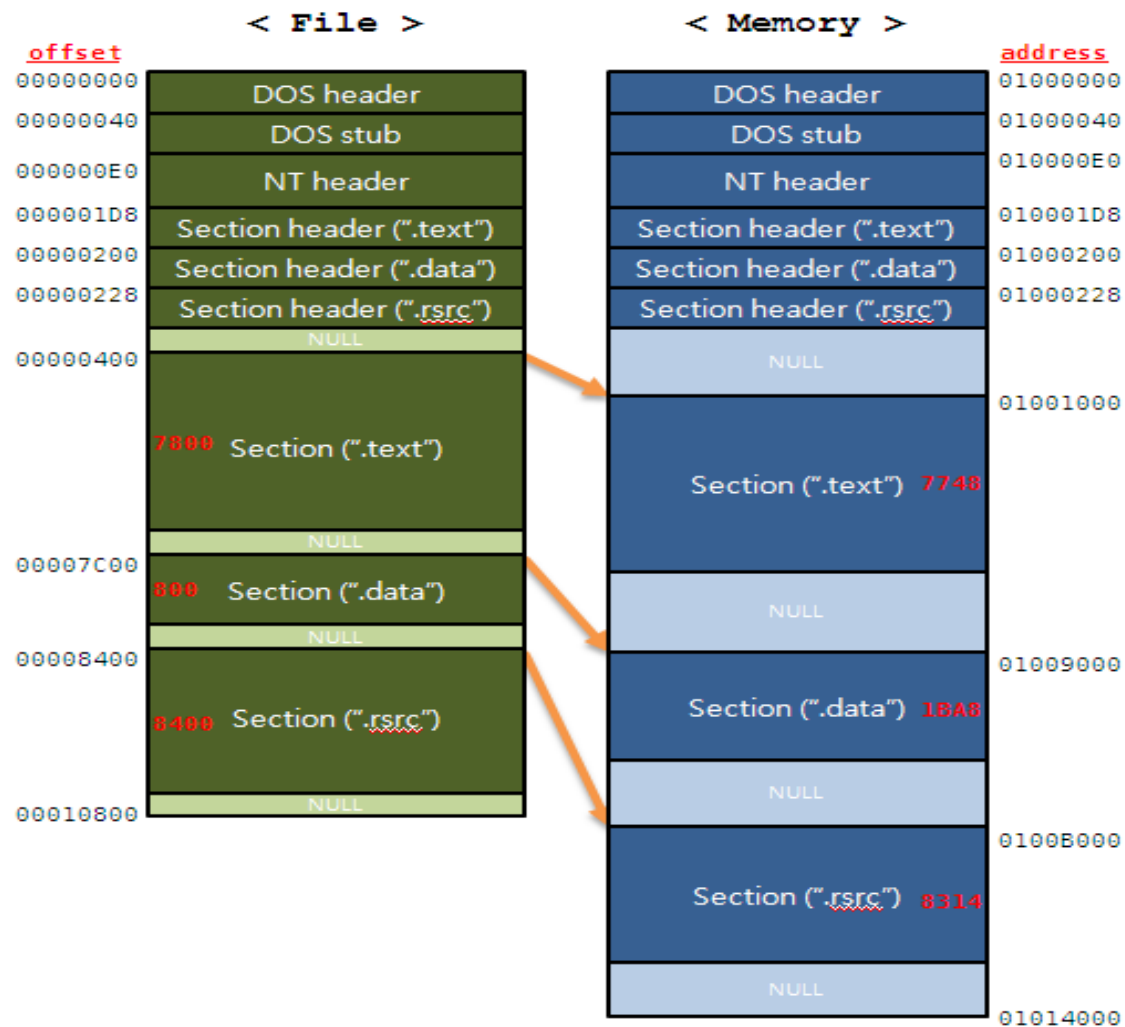


Figure 2.5. Process memory organization



◆ 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



PEView - C:\Users\Administrator\Desktop\ReverseCore\실습예제\W01_기초_리버싱\W02_Hello_World!\리버싱\bin\HelloWorld.exe

File View Go Help

Icons: Refresh, Run, Step Into, Step Over, Step Out, Breakpoints, Disassembly, Hex View, Comment, Find, Save, Print, Close

	pFile	Data	Description	Value
[-] HelloWorld.exe				
IMAGE_DOS_HEADER	00000208	2E 72 64 61	Name	.rdata
MS-DOS Stub Program	0000020C	74 61 00 00		
+ IMAGE_NT_HEADERS	00000210	00001BB0	Virtual Size	
IMAGE_SECTION_HEADER .text	00000214	00008000	RVA	
IMAGE_SECTION_HEADER .rdata	00000218	00001C00	Size of Raw Data	
IMAGE_SECTION_HEADER .data	0000021C	00006600	Pointer to Raw Data	
IMAGE_SECTION_HEADER .rsrc	00000220	00000000	Pointer to Relocations	
SECTION .text	00000224	00000000	Pointer to Line Numbers	
+ SECTION .rdata	00000228	0000	Number of Relocations	
SECTION .data	0000022A	0000	Number of Line Numbers	
[-] SECTION .rsrc	0000022C	40000040	Characteristics	
IMAGE_RESOURCE_DIRECTORY TEXT		00000040		IMAGE_SCN_CNT_INITIALIZED_DATA
IMAGE_RESOURCE_DIRECTORY NAME		40000000		IMAGE_SCN_MEM_READ
IMAGE_RESOURCE_DIRECTORY LANGUAGE				
IMAGE_RESOURCE_DATA_ENTRY				
MANIFEST 0001 0409				



◆ PE file section 정보

PEView - C:\Users\Administrator\Desktop\ReverseCore\실습예제\01_기초_리버싱\02_Hello_World!\리버싱\bin\HelloWorld.exe

File View Go Help

Icons: [Folder], [Up], [Down], [Refresh], [Find], [Save], [Print], [Zoom In], [Zoom Out], [Full Screen], [Close]

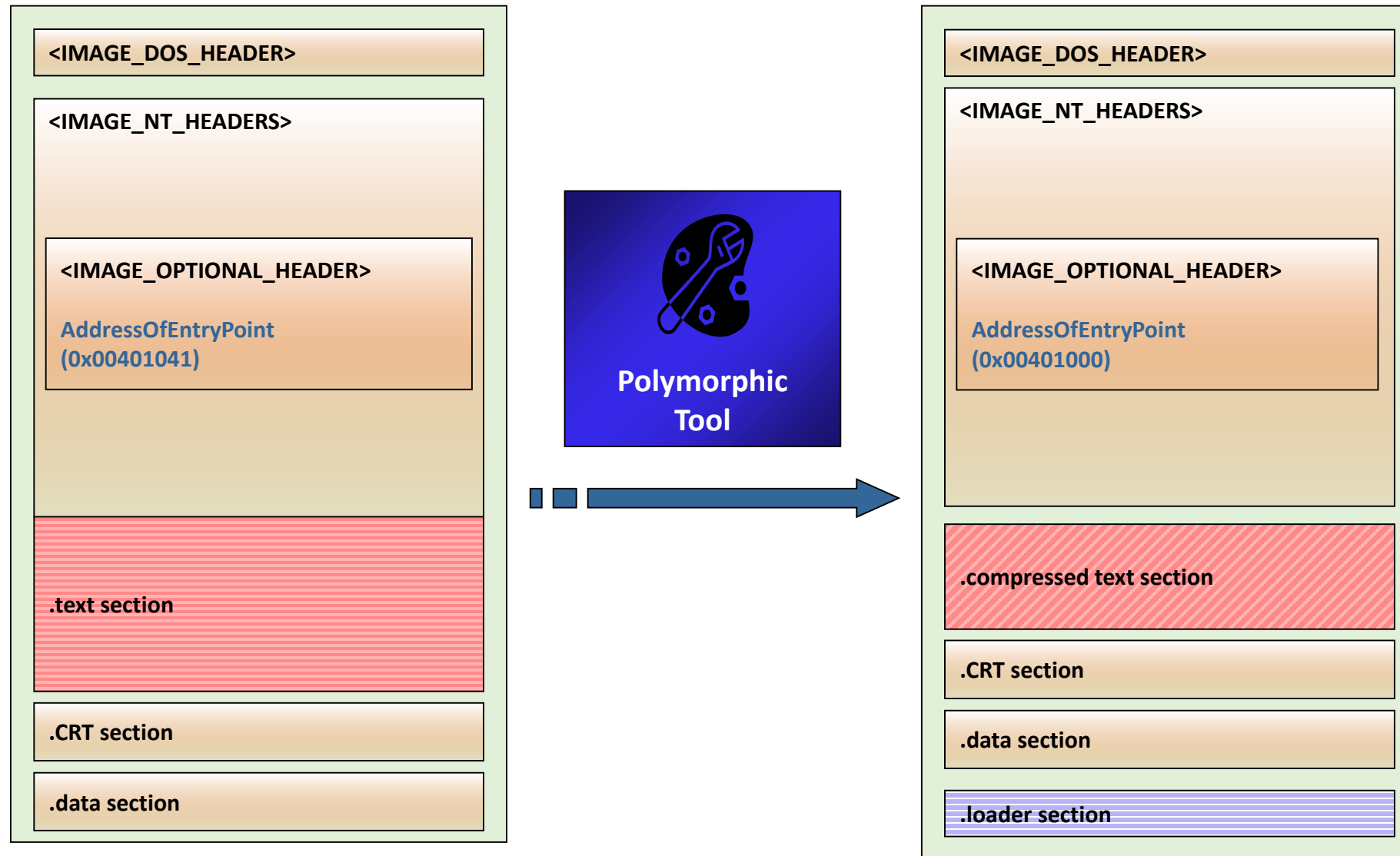
	pFile	Raw Data	Value
[-] HelloWorld.exe			
[-] IMAGE_DOS_HEADER	000077E0	46 72 69 64 61 79 00 00 54 68 75 72 73 64 61 79	Friday..Thursday
[-] MS-DOS Stub Program	000077F0	00 00 00 00 57 65 64 6E 65 73 64 61 79 00 00 00	...Wednesday...
[-] IMAGE_NT_HEADERS	00007800	54 75 65 73 64 61 79 00 4D 6F 6E 64 61 79 00 00	Tuesday.Monday..
[-] IMAGE_SECTION_HEADER .text	00007810	53 75 6E 64 61 79 00 00 53 61 74 00 46 72 69 00	Sunday..Sat.Fri.
[-] IMAGE_SECTION_HEADER .rdata	00007820	54 68 75 00 57 65 64 00 54 75 65 00 4D 6F 6E 00	Thu.Wed.Tue.Mon.
[-] IMAGE_SECTION_HEADER .data	00007830	53 75 6E 00 00 00 00 00 53 75 6E 4D 6F 6E 54 75	Sun.....SunMonTu
[-] IMAGE_SECTION_HEADER .rsrc	00007840	65 57 65 64 54 68 75 46 72 69 53 61 74 00 00 00	eWedThuFriSat...
[-] SECTION .text	00007850	4A 61 6E 46 65 62 4D 61 72 41 70 72 4D 61 79 4A	JanFebMarAprMayJ
[-] SECTION .rdata	00007860	75 6E 4A 75 6C 41 75 67 53 65 70 4F 63 74 4E 6F	unJulAugSepOctNo
[-] SECTION .data	00007870	76 44 65 63 00 00 00 00 77 00 77 00 77 00 2E 00	vDec.....w.w.w...
[-] SECTION .rsrc	00007880	72 00 65 00 76 00 65 00 72 00 73 00 65 00 63 00	r.e.v.e.r.s.e.c.
[-] IMAGE_RESOURCE_DIRECTORY T	00007890	6F 00 72 00 65 00 2E 00 63 00 6F 00 6D 00 00 00	o.r.e...c.o.m...
[-] IMAGE_RESOURCE_DIRECTORY N	000078A0	48 00 65 00 6C 00 6C 00 6F 00 20 00 57 00 6F 00	H.e.l.l.o..W.o.
[-] IMAGE_RESOURCE_DIRECTORY L	000078B0	72 00 6C 00 64 00 21 00 00 00 00 00 00 00 00 00	r.l.d.!.....
[-] IMAGE_RESOURCE_DATA_ENTRY	000078C0	48 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	H.....
[-] MANIFEST 0001 0409	000078D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	000078E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	000078F0	00 00 00 00 00 00 00 00 00 00 00 00 04 A0 40 00@.



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

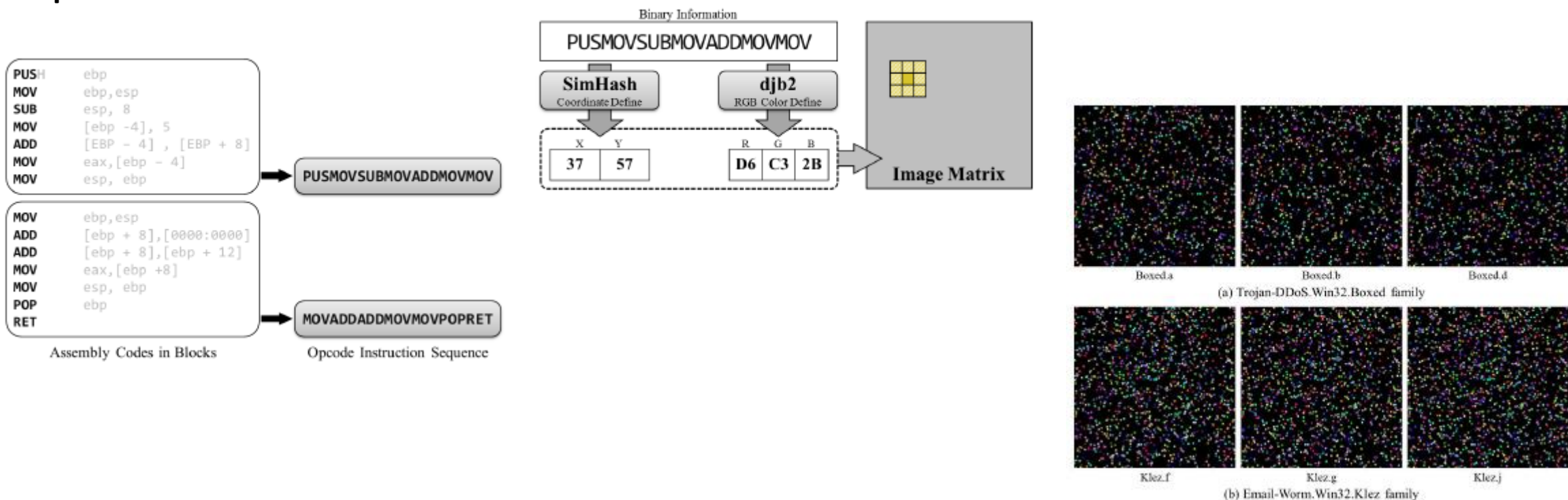
- Instruction sequences
- API sequences
- ...

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

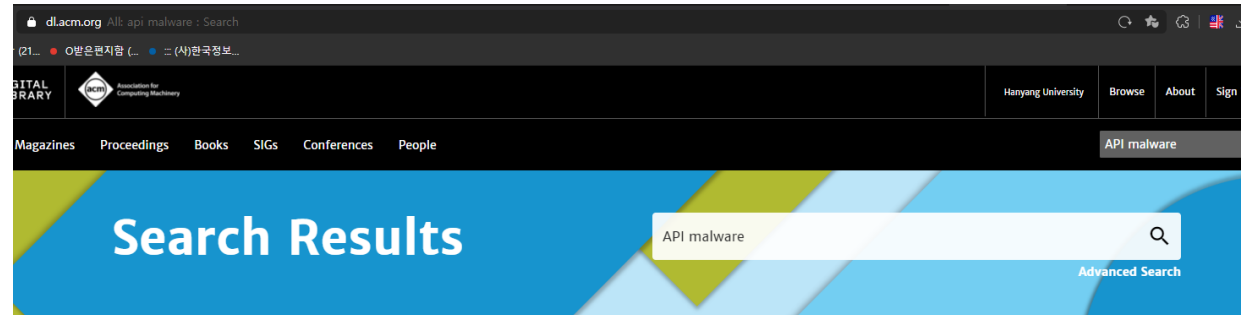
◆ Proposed method



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/>



People

- Names
- Institutions
- Authors
- Editors
- Reviewers

Publications

- Journal/Magazine Names
- Proceedings/Book Names
- All Publications
- Content Type
- Media Formats
- Paper Award

65,812 Results for: All: api malware [Edit Search](#) [Save Search](#) [RSS](#)

Searched The ACM Full-Text Collection (656,795 records) | Expand your search to The ACM Guide to Computing Literature (3,153,062 records)

RESULTS [VIDEOS](#) [SOFTWARE](#) [PEOPLE](#) Showing 1 - 20 of 65,812 Results

☐ Select All per page: 10 20 50 Relevance

☐ **POSTER** August 2012

Obfuscated malware detection using API call dependency

Chinmaya Kumar Patanaik, Ferdous A. Barbhuiya, Sukumar Nandi

SecurIT '12: Proceedings of the First International Conference on Security of Internet of Things • August 2012, pp 185–193 • <https://doi.org/10.1145/2490428.2490454>

Malwares pose a grave threat to security of a network and host systems. Many events such as Distributed Denial-of-Service attacks, spam emails etc., often have malwares as their root cause. So a great deal of research is being invested in detection and ...

6 412 Highlights

☐ **RESEARCH-ARTICLE** March 2010

Malware detection based on mining API calls

Ashkan Sami, Babak Yadegari, Hossein Rahimi, Naser Peiravian, Sattar Hashemi, ...

