

# 캡스톤 발표 자료

인공지능 기반 Windows 악성코드 탐지 및 PE파일 분석 서비스

# 주제 및 개발 목적

- 주제: 인공지능 기반 Windows 악성코드 탐지 및 PE 파일 분석 서비스
- 목적: 악성코드 분석가를 위한, 클라우드/웹 기반 분석 시스템 구현
- (가능하면) 악성코드 분석가를 찾아가 어떤 기능이 필요한지 자문해 볼 예정

# 목차

- Back-end: 악성코드 탐지 및 PE 파일 분석 (담당: 김동영)
  - 인공지능 기반 Windows 악성코드 탐지
  - PE 파일 분석
- Front-end: 웹 서비스 구성 등등.. (담당: 우건희)
  - 웹, DB 서버 구축
  - 웹 페이지 설계

인공지능 기반 Windows 악성코드  
탐지

# 인공지능 기반 Windows 악성코드 탐지

## 개발 과정 및 설명

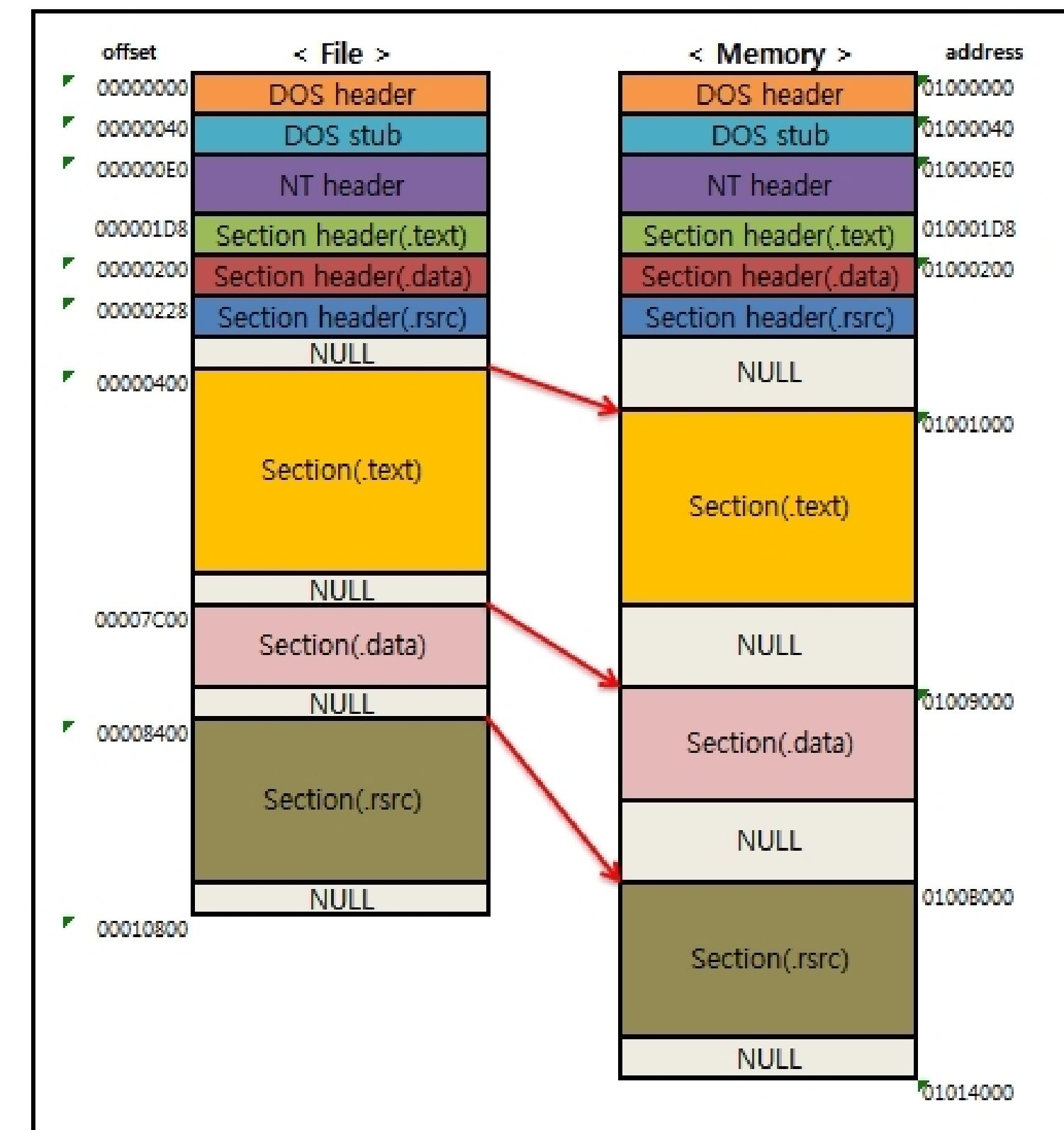
- 개발 과정 (예상)
  - Windows 악성코드 수집: 크롤러 제작, 악성코드 [Dataset](#) 활용
  - 특성 공학: 자연어 처리, 악성코드의 이미지화 등
  - 모델 개발 / 구성: 앙상블학습, CNN, 강화학습, 회귀 등등 사용
  - 모델 학습: Tensorflow / Keras 이용
  - 모델 수집: .h5 파일 저장
- 논문 활용 & 참고도서 활용하여 모델 개발 예정

# PE 파일 분석

# PE 파일 분석

## PE 파일이란?

- PE 파일이란?
  - Windows에서 사용되는 실행 파일 형식으로, 실행파일에 필요한 정보들이 저장됨.
- PE 구조를 가진 Windows 파일의 종류
  - EXE, DLL, SYS 등등
- PE 파일의 기본 구조



# PE 파일 분석

## 악성코드 분석가들이 많이 참고하는 PE값 #1.

- NT Header 내의 File Header
  - NumberOfSections: 섹션의 갯수
  - Machine: CPU별로 가지는 고유한 값 (예; 0x14c // Intel 386 및 이후 호환 CPU)
- NT Header 내의 Optional Header
  - AddressOfEntryPoint: EP의 RVA값
  - ImageBase: PE파일이 시작되는 주소
  - SectionAlignment / FileAlignment: 메모리/파일에서의 섹션크기의 배수
  - SizeOfImage: 가상메모리에서 PE Image가 차지하는 크기
  - SizeOfHeader: PE 헤더의 전체 크기



# PE 파일 분석

## 악성코드 분석가들이 많이 참고하는 PE값 :

- Section Header (섹션별 출력)
  - VirtualSize: 메모리 내 섹션의 크기
  - VirtualAddress: 메모리에서 섹션의 시작주소(상대 가상 주소)
  - SizeOfRawData: 파일에서 섹션이 차지하는 크기
  - PointerToRawData: 파일에서 섹션의 시작위치
- IAT (Import Address Table), IDT(Import Directory Table)을 통해 프로그램이 사용한 Windows API함수 Import 내역 출력.
- PE 파일의 출력은, Python의 pefile이라는 라이브러리를 활용
- PEiD 시그니처 기반 (pefile) or Yara ruleset 기반, 패커(실행 압축 파일) 탐지 기능 추가 계획 중
- 출처: <https://dyoerr9030.tistory.com/13>

```
import pefile
pe = pefile.PE('./python-3.10.2-amd64.exe')

for section in pe.sections:
    print("섹션이름: ", section.Name, "\nVirtualSize: ", hex(section.Misc_VirtualSize),
          "\ VirtualAddress: ", hex(section.VirtualAddress), "\nSizeOfRawData: ", section.SizeOfRawData, "\ PointerToRawData: ", section.PointerToRawData)
    print("\n")
```

섹션이름: b'.text\x00\x00\x00'  
VirtualSize: 0x49937 \ VirtualAddress: 0x1000  
SizeOfRawData: 301568 \ PointerToRawData: 1024

섹션이름: b'.rdata\x00\x00'  
VirtualSize: 0x1ed60 \ VirtualAddress: 0x4b000  
SizeOfRawData: 126464 \ PointerToRawData: 302592

섹션이름: b'.data\x00\x00\x00'  
VirtualSize: 0x1730 \ VirtualAddress: 0x6a000  
SizeOfRawData: 2560 \ PointerToRawData: 429056

섹션이름: b'.wixburn'  
VirtualSize: 0x38 \ VirtualAddress: 0x6c000  
SizeOfRawData: 512 \ PointerToRawData: 431616

섹션이름: b'.rsrc\x00\x00\x00'  
VirtualSize: 0x165fc \ VirtualAddress: 0x6d000  
SizeOfRawData: 91648 \ PointerToRawData: 432128

섹션이름: b'.reloc\x00\x00'  
VirtualSize: 0x3dfc \ VirtualAddress: 0x84000  
SizeOfRawData: 15872 \ PointerToRawData: 523776

웹, DB 서버 구현

# 웹, DB 서버 구현

## Cloud Computing을 이용하여 서버 구축

- Cloud Computing이란?

- IT 리소스를 인터넷을 통해 온디맨드로 제공하고 사용한 만큼만 비용을 지불하는 것

- 사용할 CC



- 사용할 Web Server



- 사용할 DB Server



# 웹, DB 서버 구현

## DB 설계

- PE 파일 NT Header를 분리, Section Header 분리
- ID키를 공용키로 적용

File Header
NumberOfSections
Machine
id

Optional Header
AddressOfEntryPoint
ImageBase
SectionAlignment / FileAlignment
SizeOfImage
SizeOfHeader
id

Section Header
VirtualSize
VirtualAddress
SizeOfRawData
PointerToRawData
id

# 웹 페이지 설계

# 웹 페이지 설계

## 웹페이지 설계

### 메인 페이지

 Ameba

≡

Currunt selected Menu name




choose your windows virus file  
This text is sample

upload Button

footer area

### 바이러스 탐지 페이지

 Ameba

≡

Currunt selected Menu name

DETAILS

VIRUS NAME

FILE HEADER

NumberOfSections

Machine

OPTIONAL HEADER

AddressOfEntryPoint

ImageBase

SectionAlignment / FileAlignment

SizeOfImage

SizeOfHeader

SECTION HEADER

VirtualSize


VirtualAddress

SizeOfRawData

PointerToRawData


footer area

### 어바웃 페이지

 Ameba

≡


Currunt selected Menu name






Name


Major

Tel / e-mail

 GitHub


This is smaple text.If there is anyone out there who still doubts that America is a place where all things are possible, who still wonders if the dream of our founders is alive in our time, who still questions the power of our democracy, tonight is your answer.






Name

Major

Tel / e-mail

 GitHub

This is smaple text.If there is anyone out there who still doubts that America is a place where all things are possible, who still wonders if the dream of our founders is alive in our time, who still questions the power of our democracy, tonight is your answer.

footer area

감사합니다.