

# 성장하는 개발자 황영준입니다

"도전하지 않으면 결과도 없다."

항상 더 발전하기 위해서는 저는 하나의 관점만으로 보는 것이 아닌 다양한 관점으로 볼 필요가 있다 생각합니다. 그렇기 때문에 저는 끊임 없이 새로운 것에 도전하고 그 결과를 보는 프로그래머가 되고 싶습니다.

## 황영준 / YoungJun Hwang

1997.01.10 / 인천광역시

Tel. 010-9788-4822

Email. hyj765@naver.com

인천광역시 동구 화도진로 113

Github <https://github.com/hyj765>

### GRADUATION

2015 제물포고등학교 졸업

2015 남서울대학교 소프트웨어공학과 입학

2022 남서울대학교 소프트웨어공학과 졸업

### 사용 가능한 언어

### 응용 레벨

JAVA

중급

C++

중급

Python

중급

C

중급

### AWARDS

2020 디지털포렌식학회 동계학술대회 우수논문상

### PROJECT

2020 AIS 분석 툴 개발 프로젝트

2021 파일복구 및 AI 바이러스 탐지 툴 개발 프로젝트

2021 딥러닝을 활용한 SNS 감성분석 시에 욕설데이터 정확도 분석 프로젝트

2022 범죄수치에 따른 치안도기반 도시 추천 프로젝트

2023 웹 화상면접 솔루션 프로젝트

### ETC

차세대 보안리더 양성프로그램 BOB 9기 수료  
선박식별장치의 아티팩트 수집 및 분석 방법  
공동 저자

Journal of WebEngineering Accepted A Study of Profanity Effect in Sentiment Analysis on Natural Language Processing Using ANN 공동 저자  
삼성청년 소프트웨어 아카데미 8기 교육 이수

# 개발 경험



## AI 프로젝트 개발 경험

AI 모델을 활용한 프로젝트 경험을 통하여  
딥러닝지식을 가지고 있습니다.

## 파일시스템 분석 경험

파일시스템 분석을 통한 파일 복구  
프로그램 개발 경험을 통한 파일 시스템 관련  
프로그램에 대한 지식을 가지고 있습니다.

## Backend/ 배포 경험

Spring을 통하여 백엔드 서버를 구축하고  
Vue를 통하여 프론트엔드를 구축하여  
MVVM 모델의 서비스를 EC2서버에서  
Jenkins/Docker를 사용하여 자동배포까지  
수행한 경험을 가지고 있습니다.

## Pcap을 사용한 네트워크

### 패킷 프로그래밍

리눅스 환경에서 Pcap 라이브러리를 사용  
하여 패킷을 받고 받은 패킷을 출력하는 프  
로그램을 만든 경험을 가지고 있습니다.

# 파일 복구 및 AI를 활용한 바이러스 탐지 툴 개발

USB에 넣어다니면서 사용할 수 있는 바이러스를 검사하는 툴이 있으면 어떨까라는 생각하에 만든 Portable 형태의 바이러스 탐지 툴입니다. 해당 탐지 툴은 크게 파일의 해시로 바이러스토탈을 통하여 시그니처 탐지를 하는 일반 파일검사, USB를 지정하고 데이터 영역에서 삭제된 파일을 복구하는 파일복구기능, 훈련된 AI를 통하여 검사를 진행하는 AI 검사 3가지 기능으로 이루어져있습니다.

프로젝트인원

3명

맡은 역할

개발 기간

5개월

기여도

기획

70%

개발

60%

- 1. AI 학습
- 2. API 추출 모듈 개발
- 3. 파일 복구 모듈 개발
- 4. 프로젝트 기획 / 관리
- 5. VirusTotal 라이브러리를 통한 시그니처 탐지 모듈 개발
- 6. 프로젝트 발표

바이러스 검사

\*주의 : 제로데이 공격에 대해서는 탐지가 불가능합니다.



파일 0 oCam\_v515.0.exe

Cyren W32/Trojan.TQCT-1685  
GData Win32.Application.Oort.A  
Jiangmin Trojan.Miner.gsu

결과 Secure File 감지 횟수 3 / 70

Target C:/Users/kskjl/Desktop/캡스톤 자료들 (1)/

검사 시작

해시 값  
게시기

# 개발 세부사항

## 개발 환경

- Python Visual Studio Code [파일 복구 및 시그니처 탐지]
- Colab Google Cloud Jupiter Notebook [AI 학습]



## 주요 라이브러리

- Keras Deep Learning High Level API
- Sklearn Machine Learning API[훈련 셋과 검증 셋 분리]
- PEfile Feature로부터 IAT 추출
- Virustotal 바이러스 시그니처 탐지
- VBA\_Parser Word파일 VBA Code 추출

## 세부 사항



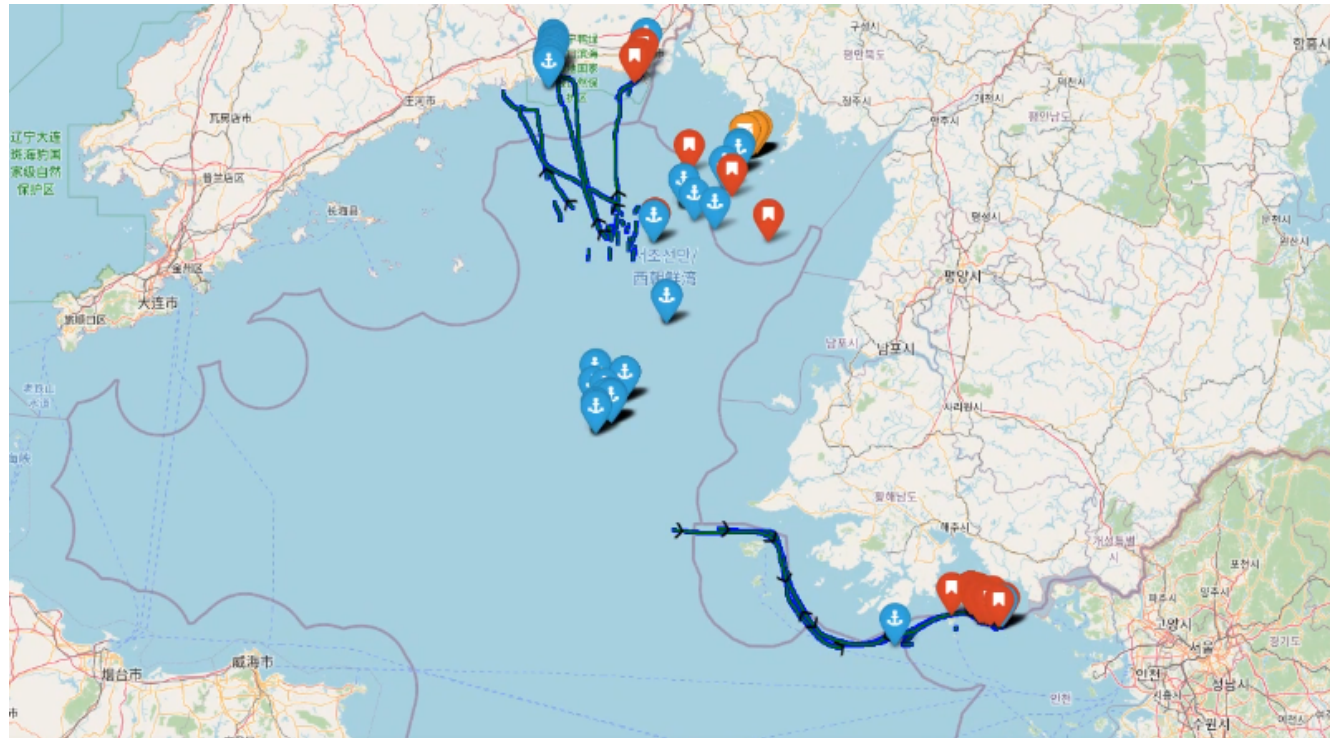
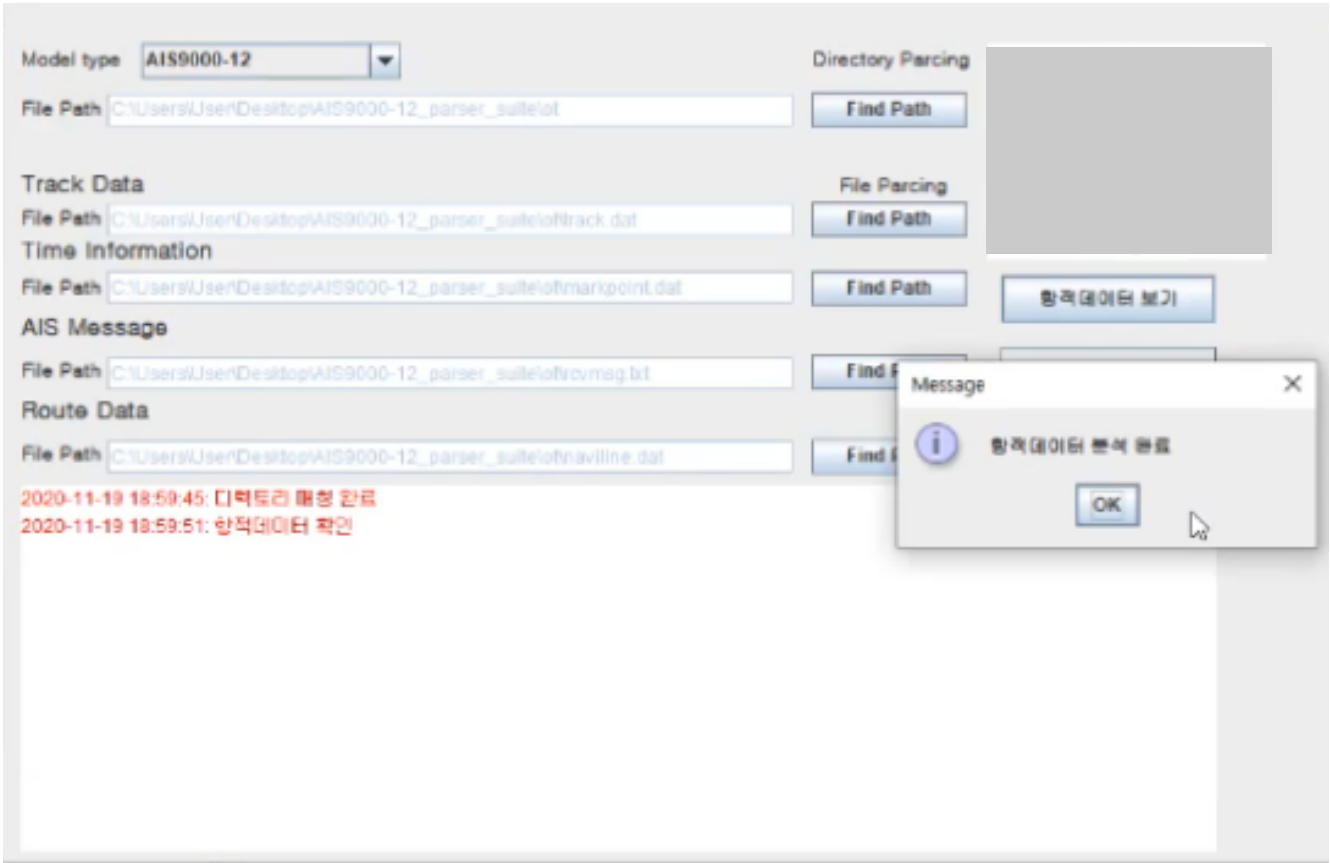
본 프로젝트는 Keras를 통하여 인공신경망을 구현하였습니다. 구성된 인공신경망은 Fully Connected Layer(Dense)로만 구성되어있으며 마지막에는 계층에 활성화함수로 Sigmoid를 사용하여 악성 파일 또는 정상파일 두가지로만 도출하게 설계하였습니다.



시그니처 탐색 기능은 바이러스 토탈 API를 사용하여 구현하였습니다. 먼저 Hashlib을 통하여 파일의 SHA-1 해시를 구하고 해시 값을 통하여 시그니처 탐색을 구현하였습니다. 또한 오탐을 대비하여 일정 수량 이상의 백신이 탐지해야만 바이러스로 판단하게 설계하였습니다.

# AIS 분석 툴 개발 프로젝트

불법 조업 등의 사고 발생 시에 AIS기기를 확보하면 해당 배의 경로를 내부데이터 구조를 분석하여 불법 조업 어선이 국내 해양 경계를 넘어온 지점과 배의 GPS 데이터를 분석하여 방향을 예측하여 시각화해주는 프로그램입니다.



## 프로젝트인원

8명

## 맡은 역할

- 1. 분석 툴 개발
- 2. GUI 디자인
- 3. AIS 기기 분석

## 개발 기간

4개월

## 기여도

기획  
개발

15%  
60%

# 개발 세부사항

## 개발 환경

- Python Visual Studio Code [분석 모듈 및 시각화 모듈]
- JAVA Eclipse [GUI]
- IDA 추출된 데이터 분석
- Trace32 메모리 동적분석



## 주요 라이브러리

- Folium 시각화 모듈
- Struct 임베디드 데이터 분석
- Shapely 영해침범 판단 모듈
- Swing GUI

## 세부사항



본 프로젝트의 분석은 확보된 불업조업 AIS기기에서 데이터를 추출한 뒤 임베디드 디버거 Trace32를 사용하여 시스템 부팅 시에 작동하는 함수 메모리 주소를 확인하고 IDA를 통하여 함수에서 fopen을 사용한 데이터를 확인하여 선박의 GPS가 저장되는 데이터를 팀원들과 협업하여 분석하였습니다.



영해 침범 확인 기능은 구글 지도를 통하여 해양 영토 경계의 위도 경도를 수집한 후 기하학 라이브러리 Shapely를 사용하여 GPS 상에 좌표가 설정한 도형 안에 포함되는 경우 인식하는 방식으로 구현하였습니다.



# Focus 면접 특화 웹 솔루션

화상 면접 프로세스가 없는 기업을 대상으로 만든 화상면접 특화 웹솔루션입니다. 본 프로젝트에서는 프로세스가 없는 기업에게 화상 면접 등록, 평가, 합격처리 등 면접 편의기능들을 제공함으로써 면접관의 업무피로도 및 프로세스 준비 시 고려사항을 줄여주는 것을 목적으로 한 B2B 솔루션입니다. 본 프로젝트는 4가지의 권한을 가진 계정으로 이루어져있으며 각 계정의 권한에 따라 다른 면접 편의기능을 사용할 수 있습니다.

프로젝트인원

개발 기간

기여도

기획  
개발

6명

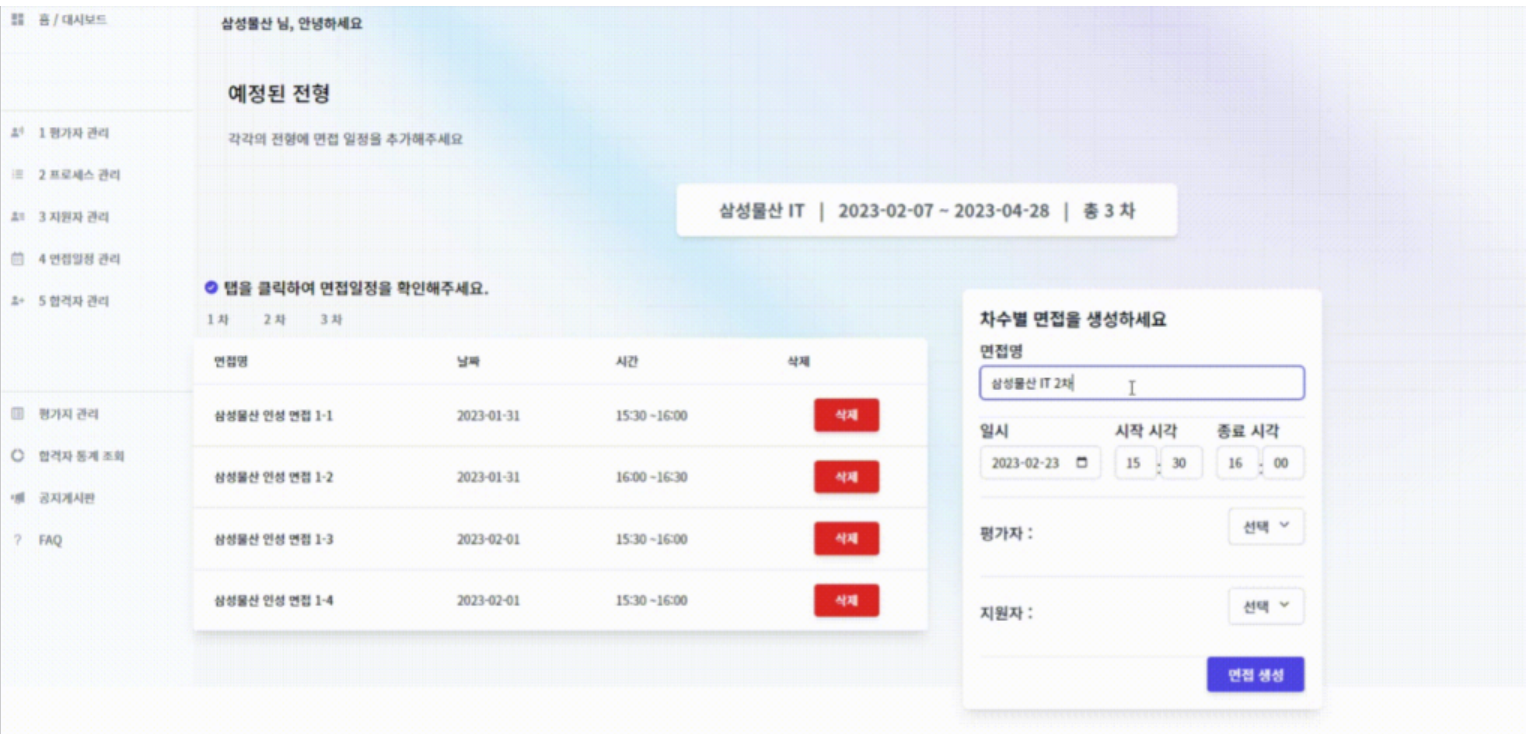
1개월

20%

20%

맡은 역할

- 1. Backend
- 2. FrontEnd 기능구현
- 3. 자동 CI/CD 구축



# 개발 세부사항

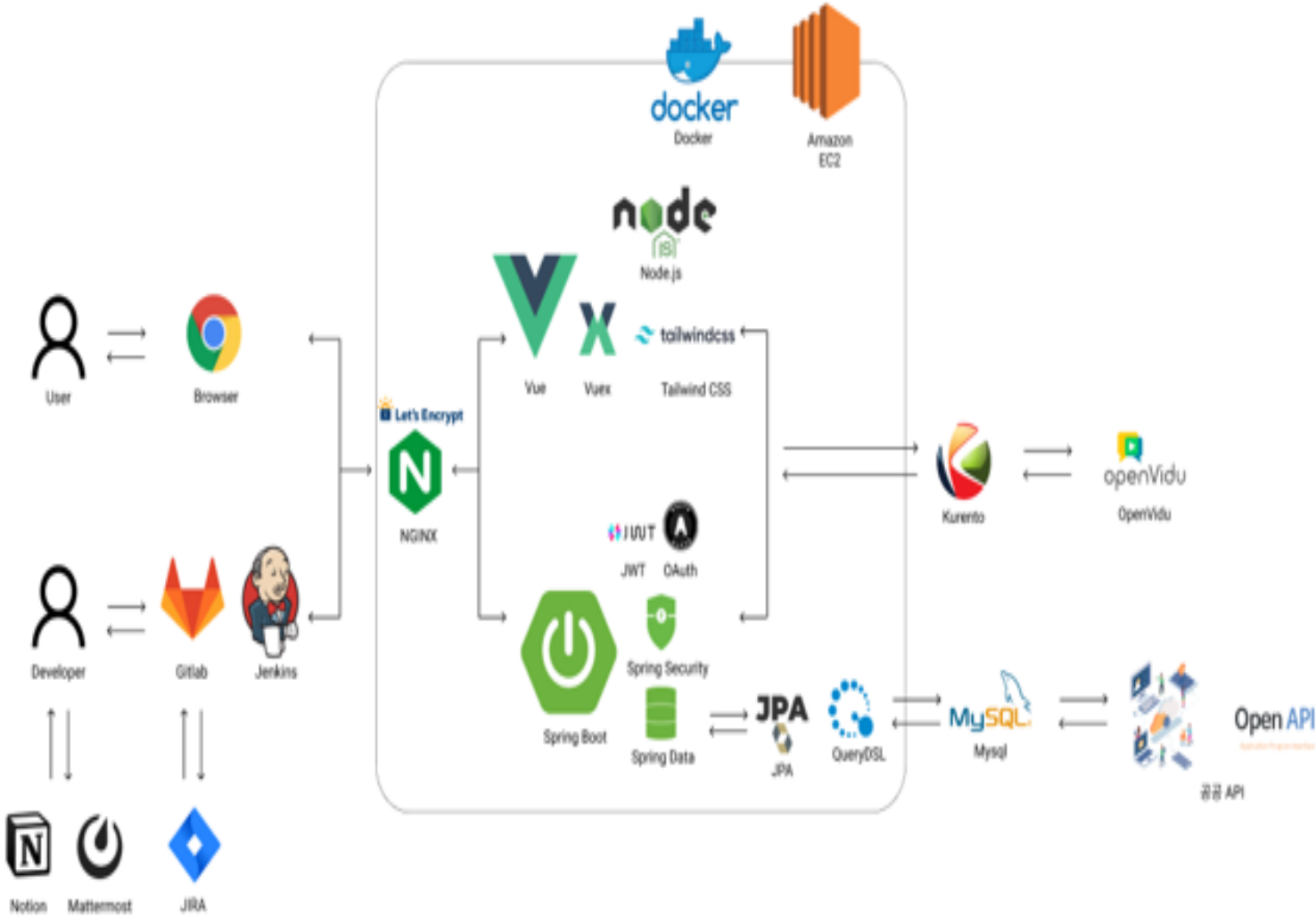
## 개발 환경

Vue3      FrontEnd [Visual Studio]  
Spring    BackEnd [IntelliJ]  
EC2      Ubuntu  
Mysql, Redis    DataBase  
Docker, Jenkins CI/CD  
OPENVIDU 화상서버  
협업툴    Git, JiRa  
ERD Cloud 데이터베이스 설계  
NGINX, CERTBOT REVERSE PROXY, 인증서

## 주요 기술

JPA	데이터 베이스 저장 및 조회
SpringBoot	Backend API 서버 구축
SpringSecurity	JWT
Web RTC	화상면접

## 세부사항



FOCUS 프로젝트의 아키텍처입니다. 모든 서버는 Docker를 통하여 구축하였습니다. 그리고 MYSQL, BACKEND서버는 도커 네트워크를 통하여 통신이 가능하게 하고 NGINX와 CertBot을 통하여 HTTPS 통신으로만 접근이 가능하게 하였습니다. Backend에서는 개발 편의를 위하여 JPA를 사용하여 데이터베이스에 접근하였습니다. 그리고 Openvidu를 사용하여 화상면접 기능인 구현하였습니다.

협업툴은 Git, JiRa를 통하여 형상관리 및 일정관리를 하였습니다.