2020-07-06

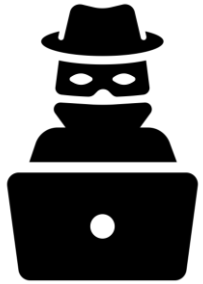
KICK - OFF

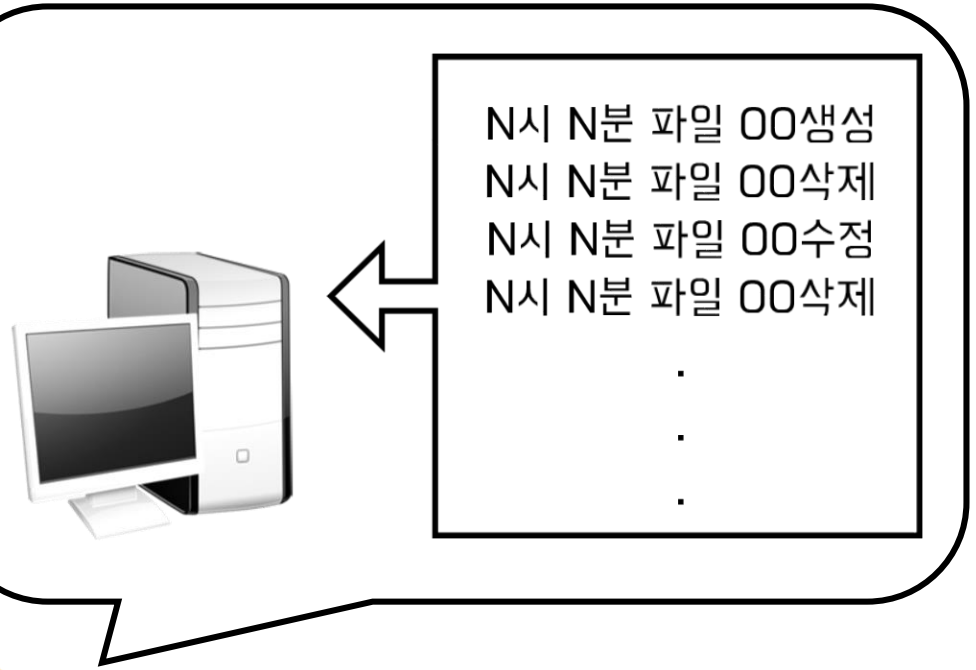
#2 SCP SUMMER PROJECT PRESENTATION

김평안, 김수현, 최송이

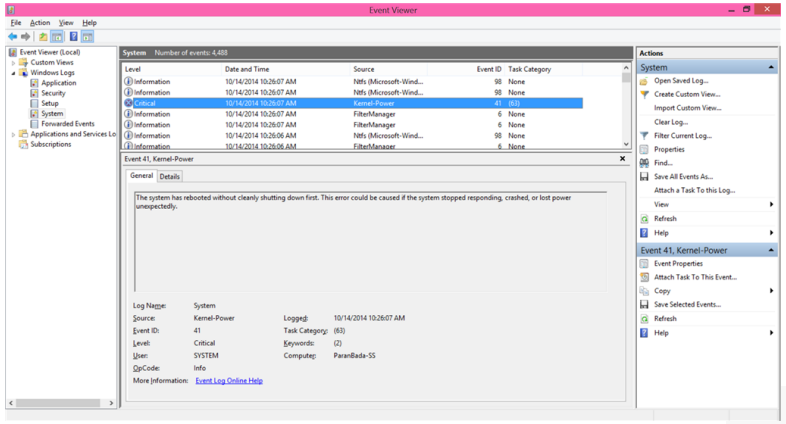
CONTENTS

배경

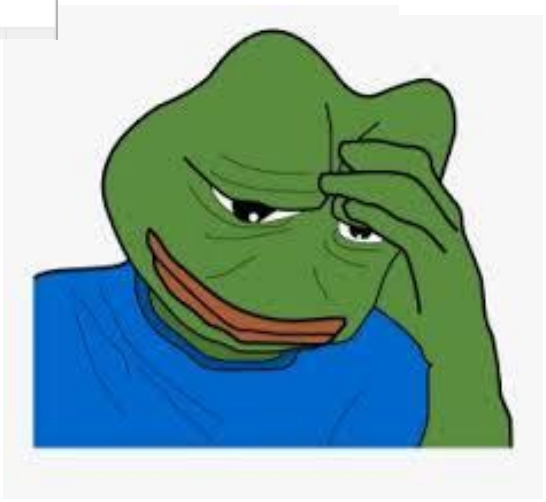




배경



Windows 이벤트 뷰어



Microsoft ReFS

ReFs

목표

프로젝트 결과물 (프로그램)

- 실행 후 백그라운드에서 계속 실행
- 파일에 이벤트가 발생할 시 로그를 남겨 기록
- 설정에 따라 알림 음을 내기도 함

학습

- 제작과정을 블로그에 포스팅해 학습효과 증가 및 지식공유

주제

미니필터 드라이버를 이용한 실시간 파일 이벤트 로거 제작

프로그램

특징
- 미니필터 드라이버를 이용해 실행 후 백그라운드에서 계속 감시
- 로그를 기록할 (텍스트 파일/엑셀 파일) 생성
- 파일에 이벤트 발생시, 알림으로 표시

로그
- 시간, 경로, 파일명, 이벤트 등을 표시

범위
- 검사 범위는 c드라이브 전체가 목표

프로그램

이벤트 발생 & 이벤트 감지

↓

당시의 시간, 경로, 파일명 등 로그(TXT)에 기록

↓

이벤트에 종류 및 설정에 따라 알림 음 재생

추진 계획

0. C언어/파이썬 항상 공부하며 스터디를 통한 정보공유

1. 미니필터 드라이버를 이용한 실시간 감시기 만들기

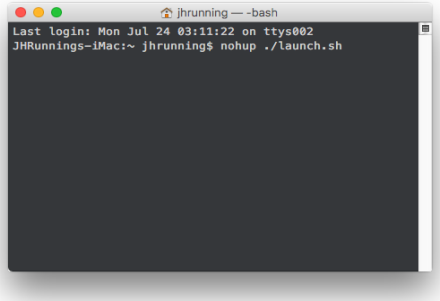
2. 키로거 프로그램 제작

3. 로그를 기록하는 프로그램 제작

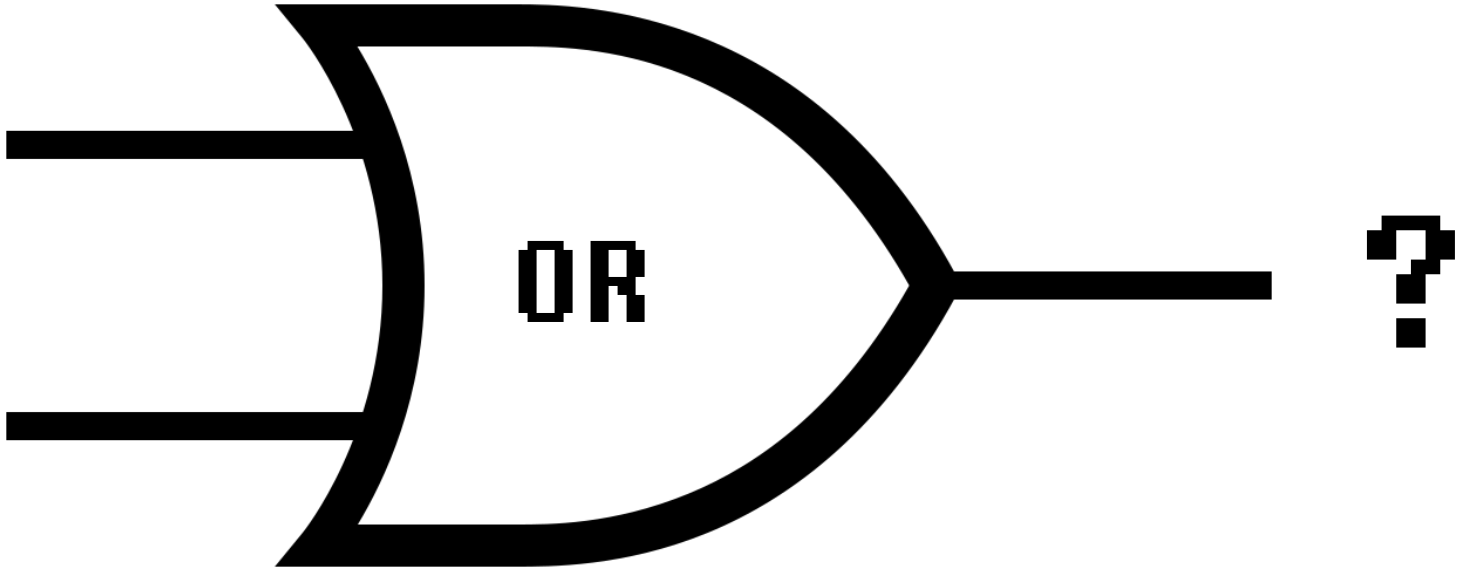
4. 셋을 합쳐 완성품 제작

로그 기록

외부파일 생성



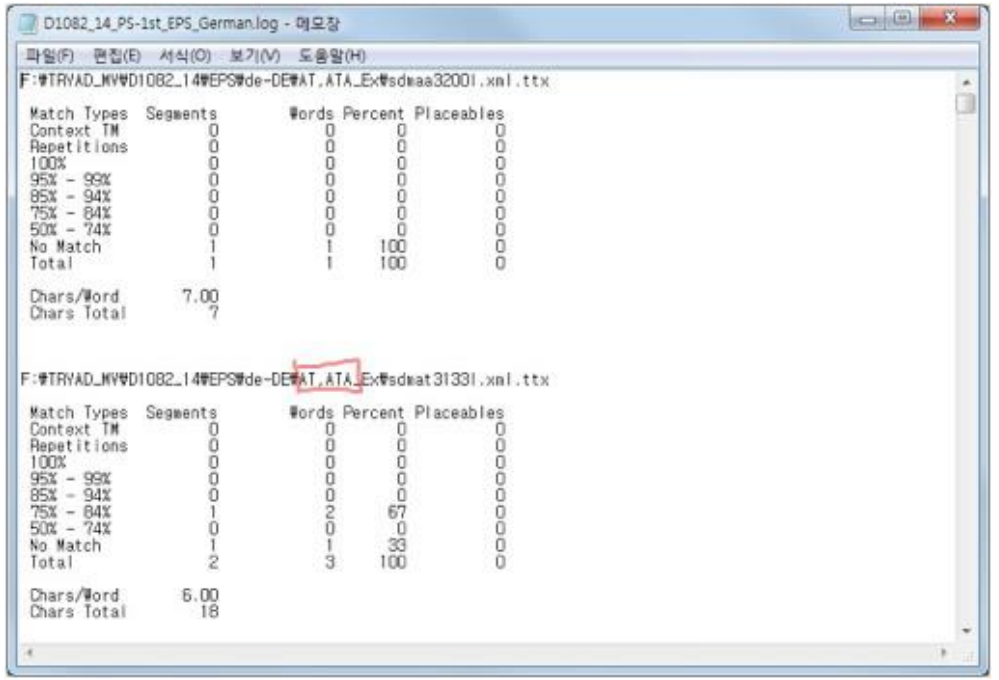
터미널 창



로그 기록

- 외부 파일에 로그를 기록

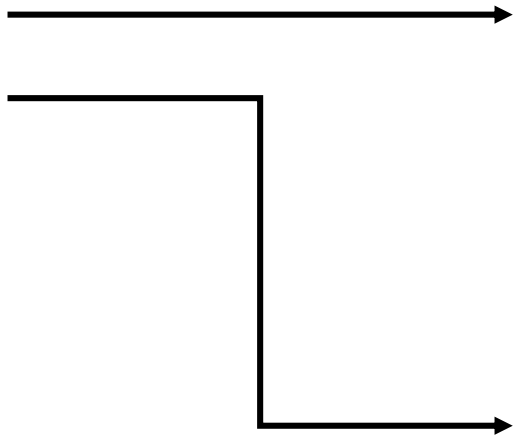
```
. log using mkim, text replace
(note: file C:\Users\kaiki\Documents\mkim.log not found)
-------------------------------------------------------------------------------
      name:  <unnamed>
       log:  C:\Users\kaiki\Documents\mkim.log
  log type:  text
 opened on:  11 Jun 2017, 18:08:45

.
```



329439	10/9/2015 20:54	2.87E+09	2054		File_Created	Normal	Directory
329440	10/9/2015 20:54	2.87E+09	2054		File_Created/ File_Closed	Normal	Directory
329441	10/9/2015 20:54	2.87E+09	2054		File_Renamed_Old	Normal	Directory
329442	10/9/2015 20:54	2.87E+09	2054		File_Renamed_New	Normal	Directory
329443	10/9/2015 20:54	2.87E+09	2054		File_Renamed_New/ File_Closed	Normal	Directory

알림 기능

- 변경점이 있을 때마다 알리는 기능
  - 알림 창을 띄우는 방식
  - 알림 음을 울리는 방식



- GUI는 어떻게 할 것인가?
- GUI를 포함하면 난이도는 괜찮은가?

- 단순히 소리만 재생한다면 쉬울 것이다
- '김평안'이 소리 관련해서 다뤄본 경험 있음

알림 기능

- 옵션선택으로 원하는 때에만 알림 음을 재생함
- TTS나 경고 효과음 중에 고를 예정

알림 음 재생

- [ ] 파일 접근
- [x] 파일 수정
- [ ] 파일 생성
- [ ] ETC...

블로그 포스팅

멘토링 시간에만 주로 사용하고 잘 사용하지 않게 된 블로그를 다시 한 번 이용해 자기 공부기록의 기회를 다시 한 번 만든다.

주로 포스팅 될 내용

- 제작 과정
- 소스코드 및 해설
- 사용된 함수에 대한 설명

Tistory

@ 추가사항 : 프로그램에 블로그 링크를 첨부해 블로그에 와서 배울 수 있게 한다.

오픈 활동

깃허브

- 소스 코드 업로드로 다른 사람들도 참고 할 수 있도록 도움

블로그

- 소스 코드, 제작 과정, 주로 사용된 함수 등을 설명해 놓는다.

기대 효과

프로젝트 팀원의 경우

- 미니필터(드라이버), 로그 분야에 대한 학습 및 경험
- 블로그 포스팅을 하며 정리를 통한 이해도의 향상

기대 효과

일반 사용자의 경우

- 정보의 유출 등의 보안 문제 발생시 대응할 수 있도록 돕는다.
- 이벤트 뷰어, Refs보다 더 쉽게 이벤트 로그에 접근할 수 있다.
- 블로그를 통해 제작 과정과 제작에 쓰인 기능을 배울 수 있다.

THANK YOU FOR WATCHING

2020-07-06-SCP