

2020 SUMMER VACATION PROJECT

SCB

CONTENTS



주제

수행 목표

역할 분담

수행 일정

01

주제

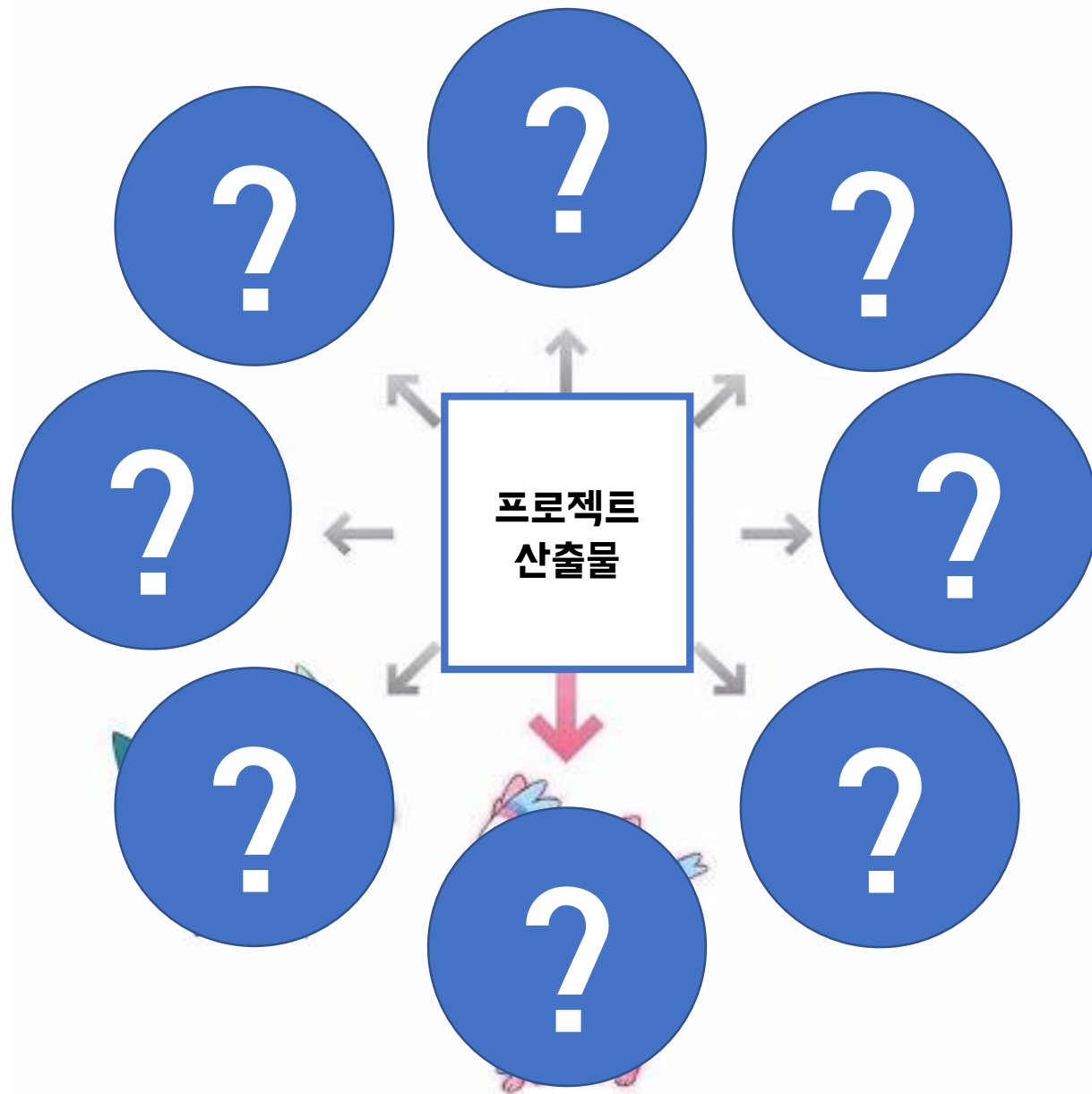
주제

미니필터 드라이버를 이용한 실시간 파일 이벤트 로거 제작

02

PROJECT 수행 목표

목표



목표

- 본래의 주제를 유지
- 느리더라도 현재 하고자 하는 것의 정확한 이해
- 이후 추가 기능을 이용한 실용성 추가

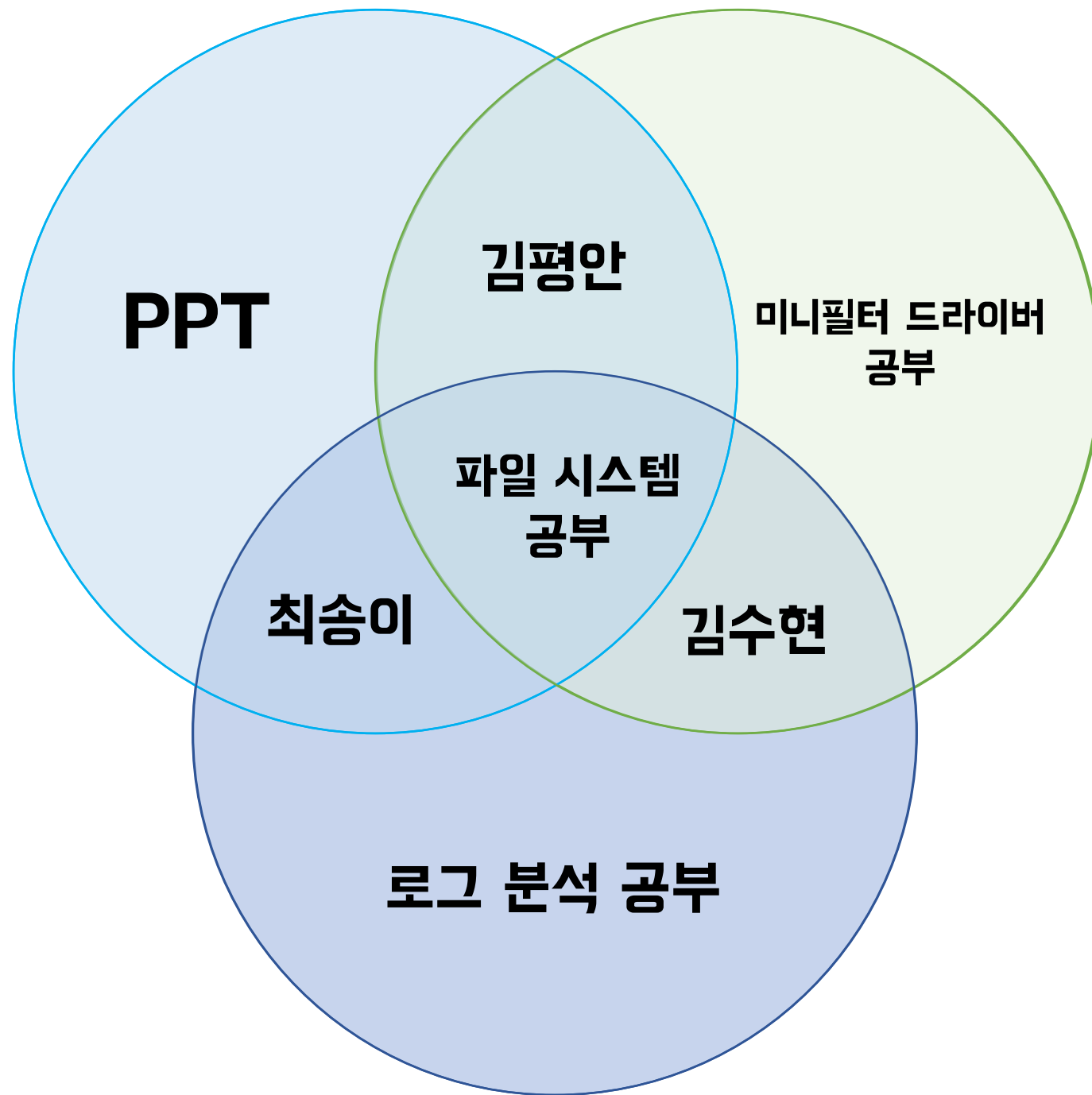
목표

**미니필터 드라이버를 이용한
실시간 파일 이벤트 로거 제작**

03

역할 분담

역할



04

PROJECT 수행 일정

진행

날짜 업무	7/6 킵오프	~	7/29 중간발표	~	8/5	~	8/19 최종발표
파일시스템 공부							
로그 분석 공부							
실시간감시기 제작							
이벤트 로거 제작							
기능 추가로 완성본 제작							



미니필터를 이용한 실시간 감시기 만들기



로그 분석



미니필터를 이용한 실시간 감시기 만들기

Windows 드라이버 키트 버전 7.1.0

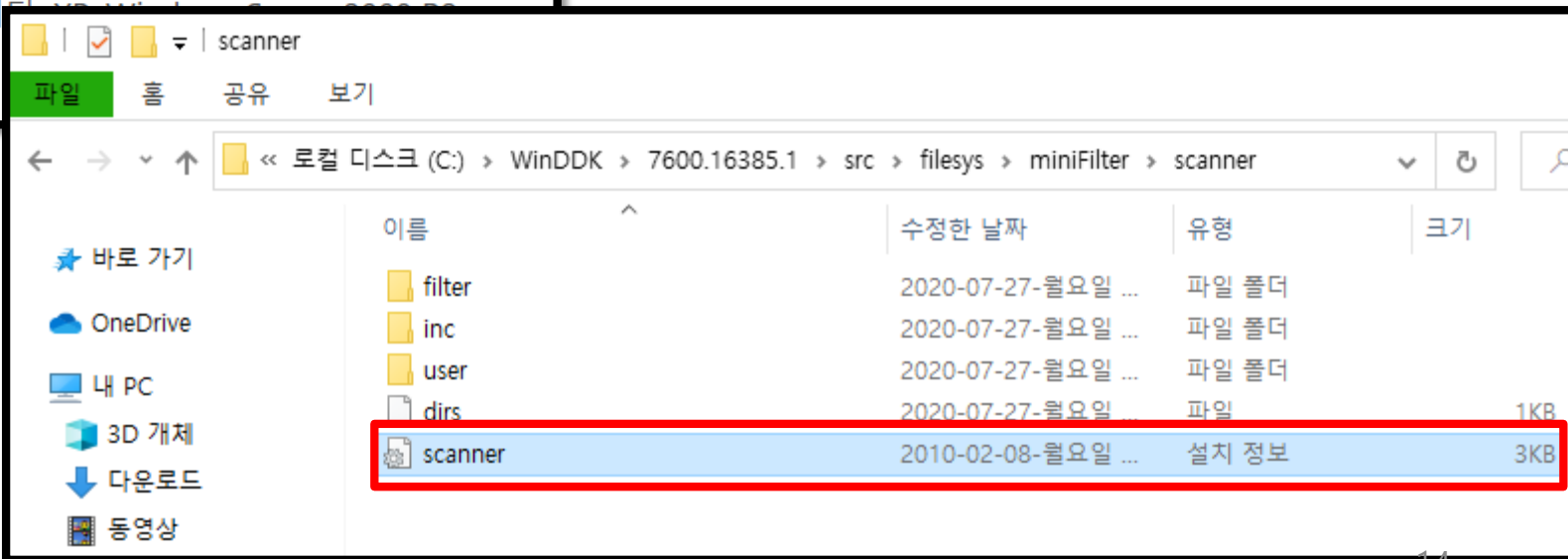
중대한! 아래에서 언어를 선택하면 전체 페이지 내용이 해당 언어로 동적으로 변경됩니다.

언어:

영어

다운로드

WDK (Windows Driver Kit) 버전 7.1.0은 WDK 7.0.0 릴리스의 업데이트이며 소프트웨어 개발자가 Windows 7, Windows Vista, Windows 용 드라이버를 작성하는 도구, 코드 샘플, 문서, 컴파일러, 헤더 및 라이브러리를 포함합니다. WDK 7.1.0은 Windows Server 2008 및 Windows Server 2003.





미니필터를 이용한 실시간 감시기 만들기

Windows Win7 x86 Checked Build Environment

Microsoft Windows [Version 10.0.18363.959]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\평안>cd

C:\>cd WinDDK\7600.16385.1\bin

C:\WinDDK\7600.16385.1\bin>setenv.bat c:\winDDK\7600.16385.1 chk Win7

C:\WinDDK\7600.16385.1>cd src\filesystem\miniFilter\scanner

C:\WinDDK\7600.16385.1\src\filesystem\miniFilter\scanner>build -cZ

path contains nonexistent c:\windows\system32\openssh, removing

BUILD: Compile and Link for x86

BUILD: Start time: Wed Jul 29 09:19:48 2020

BUILD: Examining directory tree for files to compile

File Name	Date	Type	Size
ia64mk.inc	2010-02-08-월요일 ...	Include File	14KB
makefile.ctrpp	2010-02-08-월요일 ...	CTRPP 파일	1KB
makefile.def	2010-01-13-수요일 ...	Export Definition ...	4KB
makefile.new	2010-02-08-월요일 ...	NEW 파일	353KB
makefile.plt	2010-02-08-월요일 ...	PLT 파일	20KB
oacr_base	2010-01-13-수요일 ...	구성 설정	8KB
projects.inc	2010-01-13-수요일 ...	Include File	1KB
setenv	2010-01-13-수요일 ...	Windows 배치 파일	14KB
setwdf	2010-02-08-월요일 ...	Windows 배치 파일	1KB
verify.src	2010-02-08-월요일 ...	SRC 파일	11KB

8 files c
2 execut

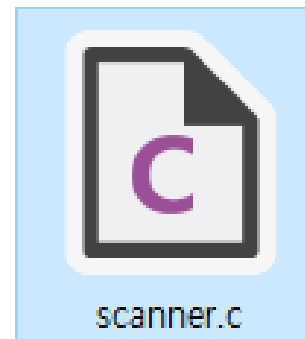
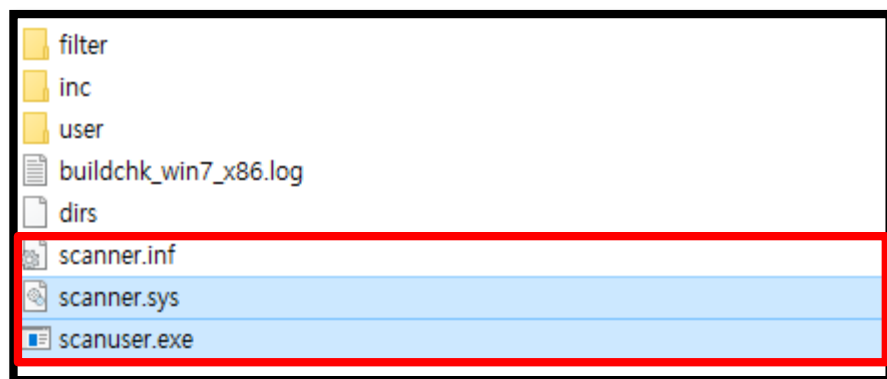
22개 항목 1개 항목 선택함 13.2KB

if "%1"=="-h" goto usage
if "%1"==" /h" goto usage

set BASEDIR=%1
IF "%BASEDIR:~-1%"=="W" SET
BASEDIR=%BASEDIR:~0,-1%
shift
@rem



미니필터를 이용한 실시간 감시기 만들기



```
Microsoft Windows [Version 10.0.18363.720]  
(c) 2019 Microsoft Corporation. All rights reserved.
```

```
C:\WINDOWS\system32>sc start scanner
```

```
SERVICE_NAME: scanner  
종류           : 2  FILE_SYSTEM_DRIVER  
상태           : 4  RUNNING  
                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)  
WIN32_EXIT_CODE : 0  (0x0)  
SERVICE_EXIT_CODE : 0  (0x0)  
검사점         : 0x0  
WAIT_HINT      : 0x0  
PID            : 0  
플래그         :
```

```
C:\wscanner>scanuser.exe
```

```
Scanner: Connecting to the filter ...
```

```
Scanner: Port = 0x00000090 Completion = 0x00000094
```

```
C:\WINDOWS\system32>
```




로그 분석 - 이벤트 로그 파싱

경로 c:/windows/system32/Winevt/logs/security.evtx

Forder	security.evtx	system.evtx	File
A 폴더 생성 감사 x	x	x	
A 폴더 생성 감사 o	A : 1	x	
A 폴더 안 B 폴더 생성	A : 4 B : 0	x	
A 폴더 안 B 폴더 삭제	A : 10 B : 4	x	
B 폴더 열기 (접근)	A : 10 B : 4	x	
	A : 많음 B : 5	?	A 폴더 안 B 텍스트 파일 생성
	A : 많음 B : 약 35	?	A 폴더 안 B 텍스트 파일 수정
	A : 많음 B : 많음	?	A 폴더 안 B 텍스트 파일 삭제
	B : 늘어남	?	B 텍스트 파일 열기 (접근)

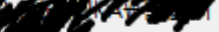
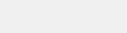
감사 정책 설정

고급 권한:

- ☐ 모든 권한
- ☒ 폴더 트래버스 / 파일 실행
- ☒ 폴더 목록 / 데이터 읽기
- ☐ 특성 읽기
- ☐ 확장 특성 읽기
- ☐ 파일 만들기 / 데이터 쓰기
- ☐ 폴더 만들기 / 데이터 추가

- ☐ 특성 쓰기
- ☐ 확장 특성 쓰기
- ☐ 하위 폴더 및 파일 삭제
- ☐ 삭제
- ☐ 사용 권한 읽기
- ☐ 사용 권한 변경
- ☐ 소유권 가져오기



개체를 삭제했습니다.	
주체:	
보안 ID:	
계정 이름:	
계정 도메인:	DESKTOP-LKBHUKA
로그온 ID:	0x38BB0
개체:	
개체 서버:	Security
핸들 ID: 0x960	
프로세스 정보:	
프로세스 ID:	0x1610
프로세스 이름:	C:\WINDOWS\explorer.exe 
트랜잭션 ID:	{00000000-0000-0000-0000-000000000000}