

시스템 상에서 일어나는 보안 이슈는 무엇이 있을까?

999+

Weaponized USB devices as an attack vector

Trojanized HID devices as well as surveilling or malicious cables are serious threats that can be used to compromise even air-gapped systems.



Alex Perekalin

April 17, 2019

JPEG 파일 통해 감염되는 신종 바이러스 경고

일반 | 입력 :2002/06/15 00:00

Robert Lemos |

**[동독하기] 카페24 | 새로운 커머스를 향한 NFT(대체불가토큰) 활용 이커머스 성공 전략 대공개**

보안 업체인 네트워크 어쏘시에이츠가 맨처음 'JPEG 감염(infector)'이라고 칭한 W32/페런 바이러스는 두 부분으로 구성돼 있다. 즉 하나는 바이러스의 페이로드를 포함하고 있는 감염된 JPEG 이미지이고, 또 하나는 이미지로부터 코드를 끌어낸 후 그림 파일이 열렸을 때 시스템에서 다른 JPEG 파일을 감염시키는 바이러스 프로그램이다. 네트워크 어쏘시에이츠의 안티바이러스 응급 대응팀 부사장인 빈센트 겔로트는 이미지 파일에 숨겨져 있는 어떤 코드가 PC에 영향을 주기 전에 PC는 익스트랙터에 의해 감염되기 때문에 이 프로그램은 위험이라기보다는 컴퓨터 과학에 대한 호기심이라고 말했다. 겔로트는 "우리는 이것이 문제라고 말하지 않는다. 별로 위험하다고 생각하지는 않지만, 예전에 본 적이 없는 것"이라고 말했다. 그는 W32/페런 코드를 전송하는 디지털 이미지는 새로운 코드에 의해 훼손되기 때문에 발견하기 쉽다고 말했다. PC 사용자들은 자신이 JPEG 이미지를 여는 것만으로는 감염되지 않는다는 것을 유념해야 한다. 오히려 감염된 컴퓨터의 바이러스가 코드를 디지털 이미지로 복사하고, JPEG 파일이 다른 감염된 시스템으로 전달되기를 기다린다. 이러한 시스템에 있는 바이러스는 JPEG 이미지에서 코드의 조각을 읽고 지시를 따를 것이다. 익스트랙터 바이러스에 감염된 적이 없는 사용자는 감염된 디지털 이미지를 열어도 아무 문제가 생기지 않는다. 익스트랙터 파일은 오직 MS 윈도우를 구



보안 이슈

[이슈분석]이동식 저장장치 노리는 악성코드 `오토런` 정체를 밝혀라

발행일 : 2016-04-21 17:00 지면 : 2016-04-22 5면

#직장인 A씨는 최근 USB에 저장해 둔 자료를 사용하려고 PC에 꽂았다가 황당한 일을 겪었다. USB 안에 있던 자료가 모두 사라지고 바로가기 아이콘만 남았다. 발표에 쓸 자료를 모두 잃어버린 A씨는 사내 보안팀에 문의, 오토런(Autorun) 악성코드의 존재를 알았다.

이동식 저장 매체를 감염시킨 오토런 악성코드는 치료해도 또다시 나타나는 좀비다. 안전하다고 믿고 있던 이동식 저장장치가 악성코드의 또 다른 서식처로 떠올랐다. 오토런 악성코드는 2000년대 후반에 등장해 10여년이 지났지만 여전히 영향력을 미치고 있다. 오토런은 PC에 설치된 안티바이러스 솔루션이 이동식 저장장치를 검사하기 이전에 실행돼 예방이 무엇보다 중요하다.

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

그들은 어떻게 정상 엑셀 파일을 감염시켰을까



AhnLab | 2022-04-13

최근 ASEC은 정상 엑셀 파일을 감염시키는 악성코드들의 유포 사례를 확인했다. 이런 유형의 악성코드는 정상 엑셀 파일을 감염시키는 바이러스 기능뿐만 아니라, 다운로드, DNS 스누핑 등의 추가 악성 행위까지 수행하고 있었다.

이번 글에서는 정상적인 엑셀 파일을 감염시키고 바이러스를 전파하는 두 가지 유형의 악성코드를 살펴본다.



디스크 안심 탐색기

간편하게. 쾌적하게. 강력하게.

크루 소개

참여

각 책임자가 총괄하는 파트를 나타낸 것으로서, 다른 팀원의 역할과 관련된 활동에도 참여했음.



김현도

Core Developer



박민우

Quality Assurance



백승우

Project Manager



이상원

UX Engineer

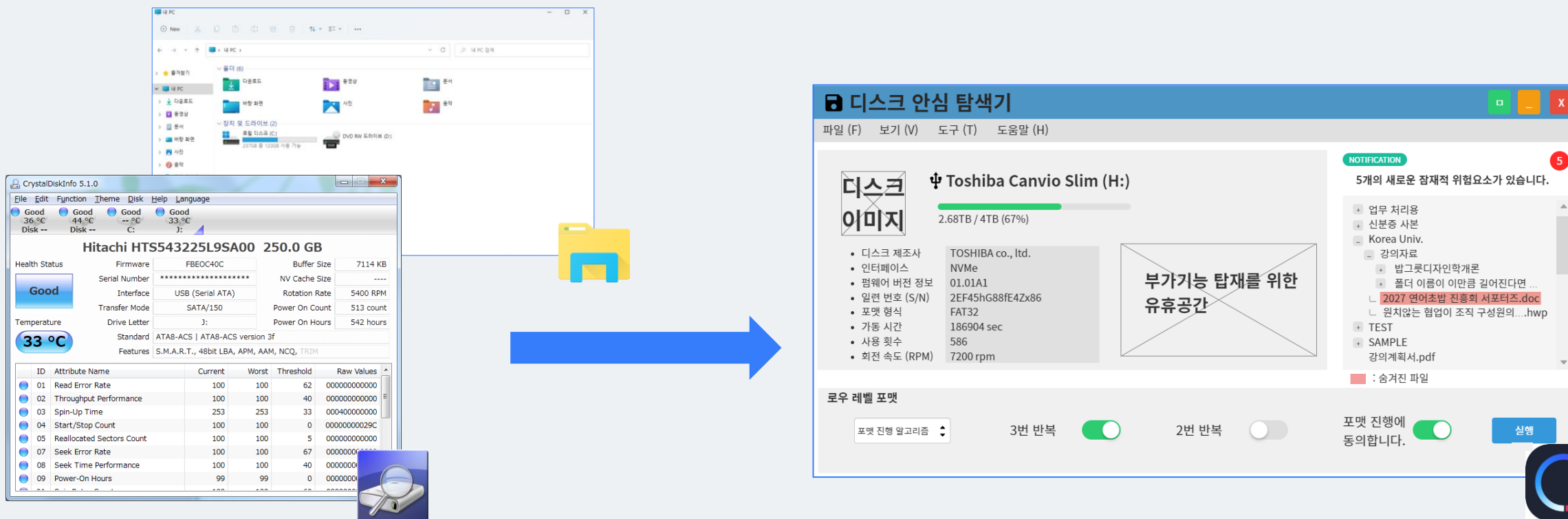
초기 기획안 구상

PROJECT DISK

초기 기획안

Disk Explorer with Security Knowledge (DESK)는 다음과 같은 특화 기능을 지원하도록 기획되었습니다.

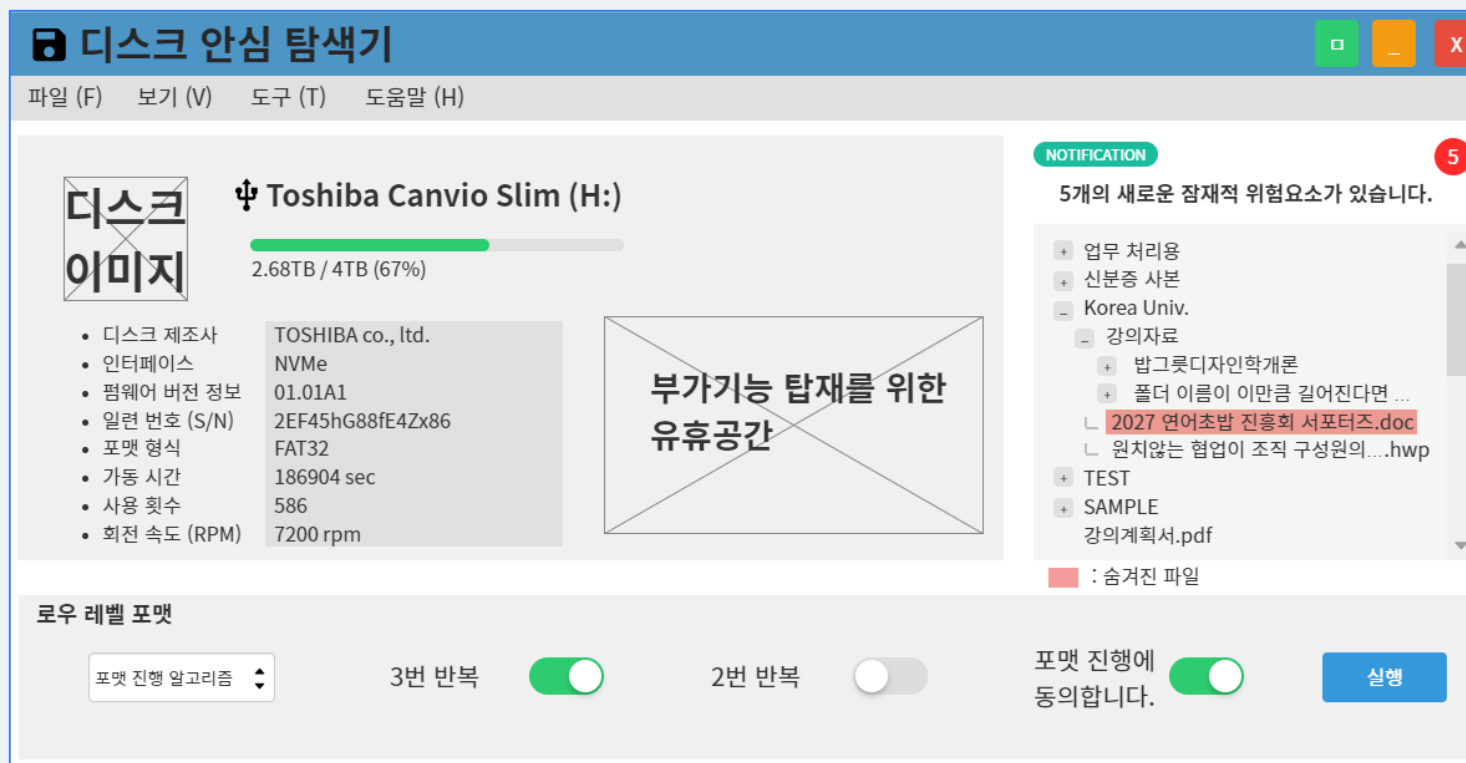
- 백신 엔진을 이용하여 파일들이 바이러스로부터 감염되어 있는지 확인할 수 있습니다.
- 저장장치에 숨김 파일이 있다면 모두 보여주고 보안상 숨겨야 하는 목적이 있는 파일이라면 파일을 숨길 수 있습니다.
- 바이러스에 감염된 파일이거나 USB 바이러스로 인한 의도적으로 숨겨진 파일이 있는지 점검하고, 이를 선택적으로 삭제할 수 있습니다.
- 디스크 사용 정보를 출력하여 제3자에 의한 의도치 않은 디스크 사용이 있었는지 확인할 수 있습니다.



초기 기획안

Disk Explorer with Security Knowledge (DESK)는 다음과 같은 특화 기능을 지원하도록 기획되었습니다.

- 백신 엔진을 이용하여 파일들이 바이러스로부터 감염되어 있는지 확인할 수 있습니다.
- 저장장치에 숨김 파일이 있다면 모두 보여주고 보안상 숨겨야 하는 목적이 있는 파일이라면 파일을 숨길 수 있습니다.
- 바이러스에 감염된 파일이거나 USB 바이러스로 인한 의도적으로 숨겨진 파일이 있는지 점검하고, 이를 선택적으로 삭제할 수 있습니다.
- 디스크 사용 정보를 출력하여 제3자에 의한 의도치 않은 디스크 사용이 있었는지 확인할 수 있습니다.



문제 상황

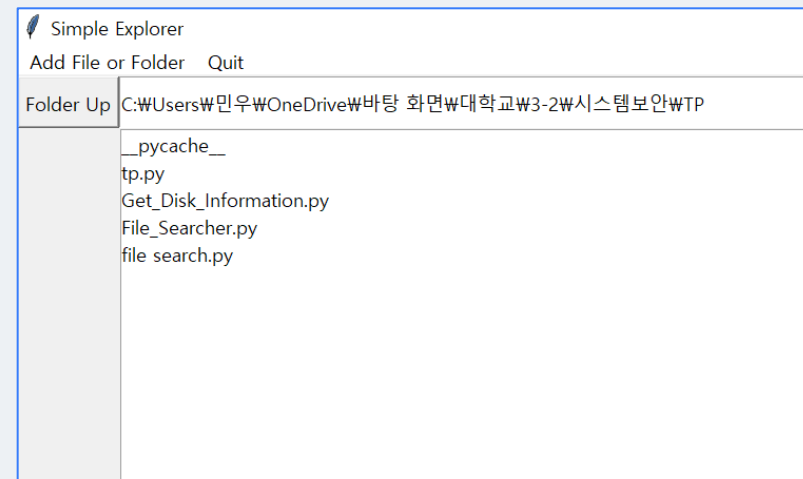
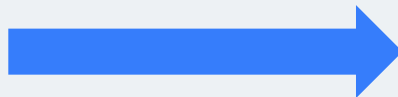
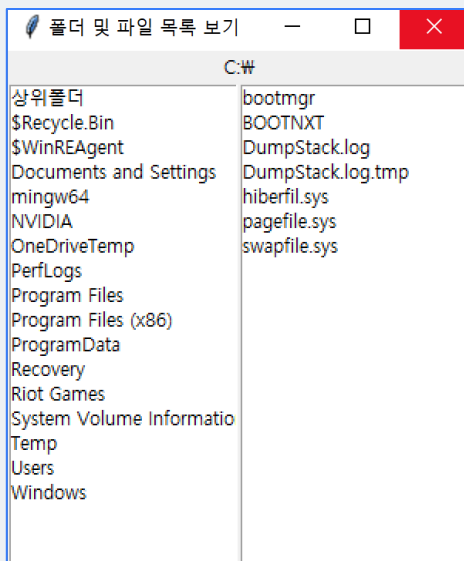
다음과 같은 문제점들을 발견할 수 있었습니다.

- 일반적인 다른 파일탐색기와 비교하였을 때, 컴포넌트의 배치가 일반적이지 아니하여 쉽게 적응하기 어렵다는 문제가 있었습니다.
- 파일 실행이 불가능하다는 문제가 있었습니다.

해결 방법

보다 직관적인 위치에 컴포넌트들을 재배치하여 사용성을 개선하였으며, 연결 프로그램이 지정되어 있는 파일이라면 더블 클릭을 통해 파일 실행이 가능하도록 개선하였습니다.

또한, 신규 파일 또는 디렉토리를 생성할 수 있는 기능을 새로이 추가하였습니다.



프로토타입의 구현

디스크 정보

PROJECT DISK

S.M.A.R.T.

Self-Monitoring, Analysis and Reporting Technology (디스크의 신뢰성을 검사하여 잠재적인 실패 가능성을 진단하고 감시하는 기술)

개선 방식

S.M.A.R.T. 를 이용한 모듈을 불러와 필요한 정보를 취사 선택하는 방식을 택하여 효율적으로 개선

```
Windows PowerShell
PS C:\Users\Wdnlab> smartctl -a /dev/sdb
smartctl 7.3 2022-02-28 r5338 [x86_64-w64-mingw32-w10-21H2] (sf-7.3-1)
Copyright (C) 2002-22, Bruce Allen, Christian Franke, www.smartmontools.org


=== START OF INFORMATION SECTION ===
Model Number:          Samsung SSD 970 PRO 1TB
Serial Number:         S462NF0M616898B
Firmware Version:      1B2QEXP7
PCI Vendor/Subsystem ID: 0x144d
IEEE OUI Identifier:   0x002538
Total NVM Capacity:    1,024,209,543,168 [1.02 TB]
Unallocated NVM Capacity: 0
Controller ID:         4
NVMe Version:          1.3
Number of Namespaces:  1
Namespace 1 Size/Capacity: 1,024,209,543,168 [1.02 TB]
Namespace 1 Utilization: 920,700,256,256 [920 GB]
Namespace 1 Formatted LBA Size: 512
Namespace 1 IEEE EUI-64: 002538 5691b54423
Local Time is:         Tue Nov 15 04:25:54 2022
Firmware Updates (0x16): 3 Slots, no Reset required
Optional Admin Commands (0x0037): Security Format Frmw_DL Self_Test Directvs
Optional NVM Commands (0x005f):  Comp Wr_Unc DS_Mngmt Wr_Zero Sav/Sel_Feat Timestmp
Log Page Attributes (0x03): S/H_per_NS Cmd_Eff_Lg
Maximum Data Transfer Size: 512 Pages
Warning Comp. Temp. Threshold: 81 Celsius
Critical Comp. Temp. Threshold: 81 Celsius

Supported Power States
St Op   Max      Active   Idle    RL RT WL WT  Ent_Lat  Ex_Lat
0 +    6.20W    -       -       0 0 0 0      0        0
1 +    4.30W    -       -       1 1 1 1      0        0
2 +    2.10W    -       -       2 2 2 2      0        0
3 -    0.0400W -       -       3 3 3 3     210    1200
4 -    0.0050W -       -       4 4 4 4     2000    8000

Supported LBA Sizes (NSID 0x1)
Id Fmt Data  Metadt Rel_Perf
0 +   512    0        0

=== START OF SMART DATA SECTION ===
SMART overall-health self-assessment test result: PASSED

SMART/Health Information (NVMe Log 0x02)
Critical Warning:      0x00
Temperature:          45 Celsius
Available Spare:       100%
Available Spare Threshold: 10%
Percentage Used:       1%
Data Units Read:       14,321,321 [7.33 TB]
```



Smartmontools.org

Control and Monitor Utility for SMART Disks

7 followers <https://smartmontools.org> Verified

Simple Explorer	
/dev/sda	/dev/sdb
Model Number	SAMSUNG MZVLW256HEHP-000
Serial Number	S38ZNX0J803549
Firmware Version	CXB70K1Q
PCI Vendor/Subsystem ID	0x144d
IEEE OUI Identifier	0x002538
Total NVM Capacity	256,060,514,304 [256 GB]
Unallocated NVM Capacity	0
Controller ID	2
NVMe Version	1.2
Number of Namespaces	1
Namespace 1 Size/Capacity	256,060,514,304 [256 GB]
Namespace 1 Utilization	244,682,801,152 [244 GB]
Namespace 1 Formatted LBA Size	512
Local Time is	23 2022
Firmware Updates (0x16)	3 Slots, no Reset required
Optional Admin Commands	Security Format Frmw_DL Self_Test
Optional NVM Commands	Comp Wr_Unc DS_Mngmt Wr_Zero Sav/Sel_Feat

프로토타입의 구현

디스크 정보

PROJECT
DISK

문제 상황

필요한 디스크 정보 요소들을 하나씩 파싱해 가져오기엔 리소스 낭비가 크고, 원하는 정보를 직접 파싱기 까다로운 경우도 존재하였습니다.

S.M.A.R.T.

Self-Monitoring, Analysis and Reporting Technology (디스크의 신뢰성을 검사하여 잠재적인 실패 가능성을 진단하고 감시하는 기술)

개선 방식

S.M.A.R.T. 를 이용한 모듈을 불러와 필요한 정보를 취사 선택하는 방식을 택하여 효율적으로 개선

```
sdiskpart(device='C:WW', mountpoint='C:WW', fstype='NTFS', opts='rw.fixed', maxfile=255, maxpath=260)
total = 1,023,533,481,984 byte / used = 952,624,566,272 byte / free = 70,908,915,712 byte
total = 976,117.59 MB / used = 908,493.58 MB / free = 67,624.01 MB / Rate of usage = 93.1%
read_count = 245, write_count = 0, read_bytes = 631808, write_bytes = 0, read_time = 0, write_time = 0
```



Simple Explorer

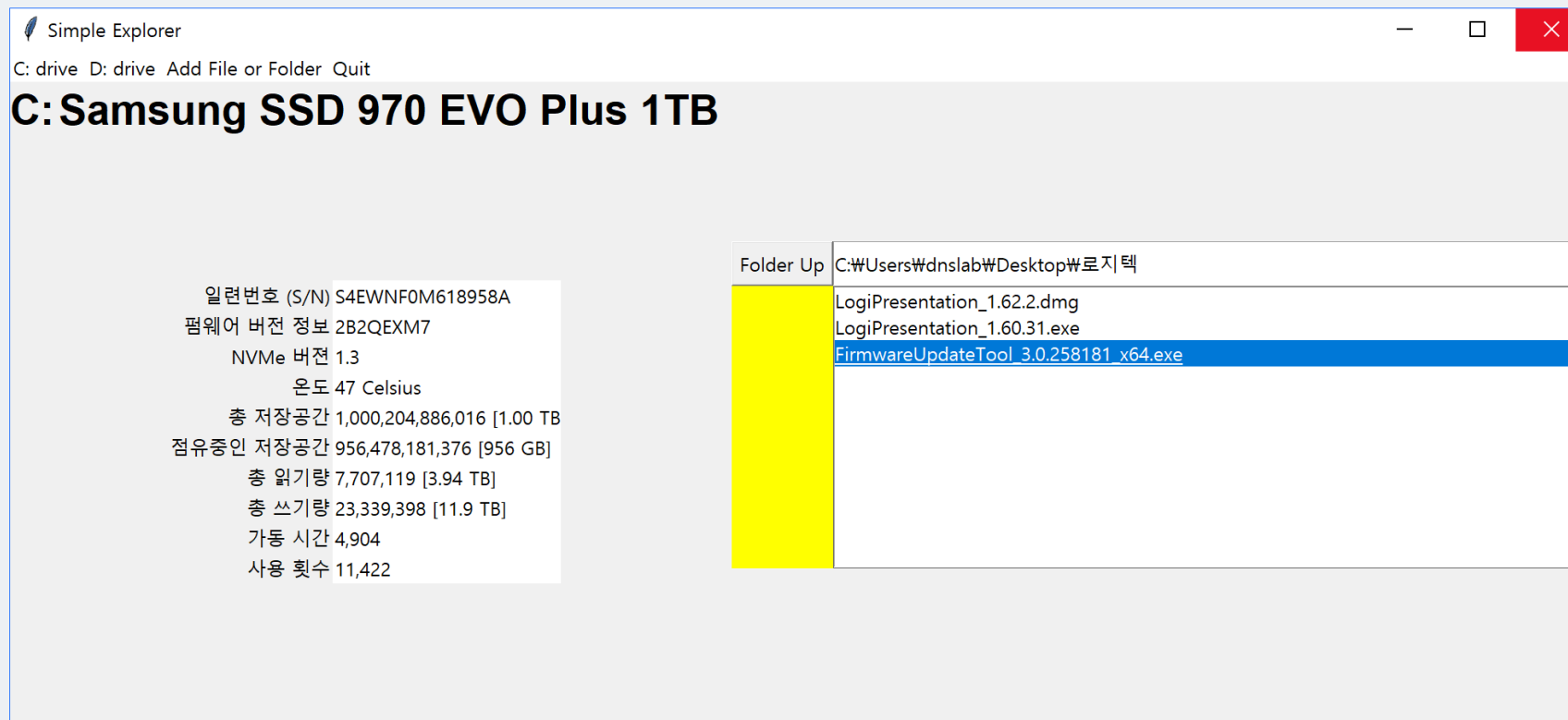
파일 보기 도구 도움말

C: SAMSUNG MZVLW256HEHP-000

일련번호 (S/N)	S38ZNX0J803549
펌웨어 버전 정보	CXB70K1Q
NVMe 버전	1.2
온도	29 Celsius
총 저장공간	256,060,514,304 [256 GB]
점유중인 저장공간	244,715,769,856 [244 GB]
총 읽기량	123,798,952 [63.3 TB]
총 쓰기량	36,692,441 [18.7 TB]
가동 시간	3,097
사용 횟수	6,063

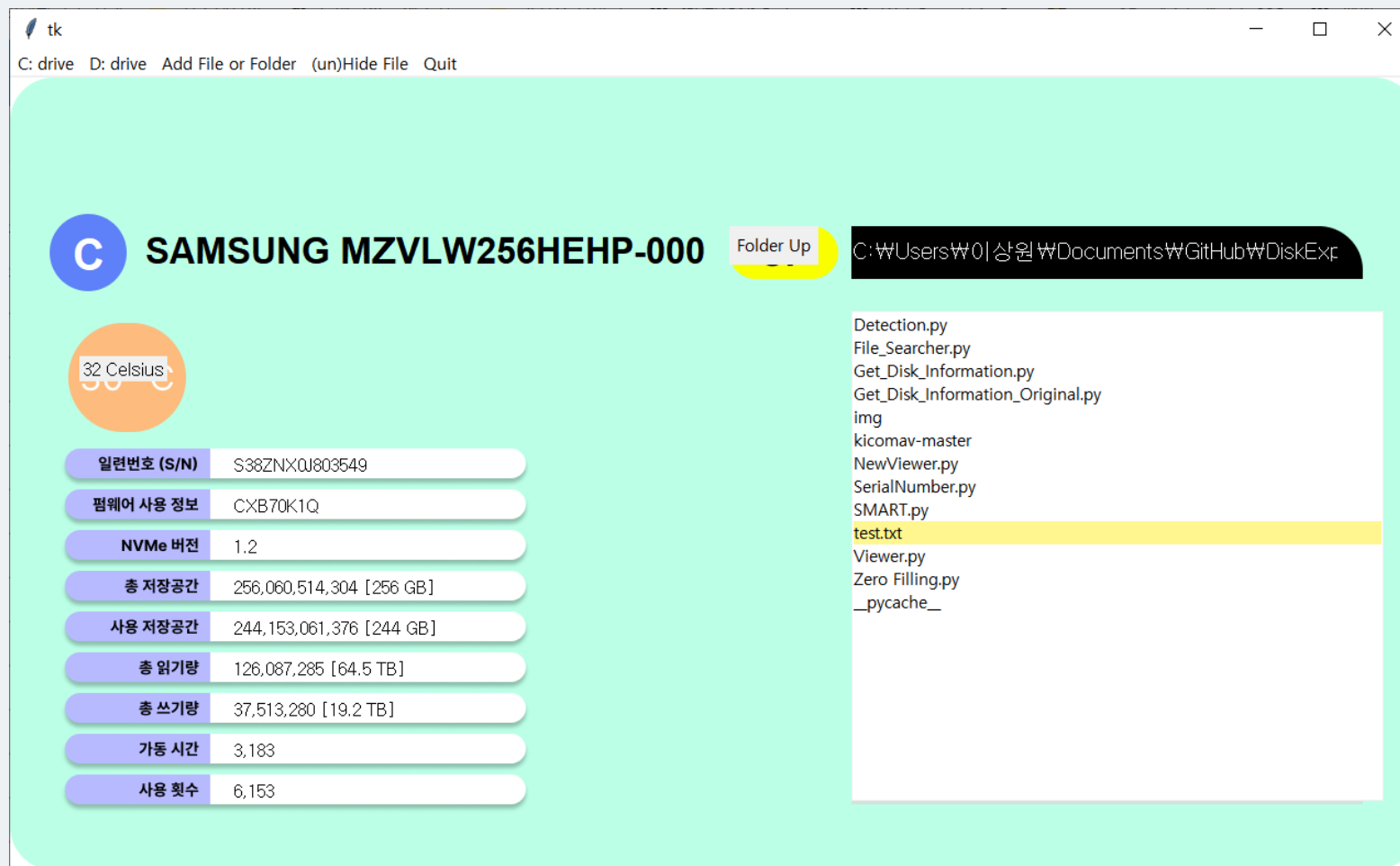
진행 상황

시스템에 설치된 디스크에 대하여 볼륨 정보를 포함한 메타 데이터를 확인할 수 있으며, 드라이브에 위치한 파일들을 확인하고 생성 또는 실행할 수 있습니다.



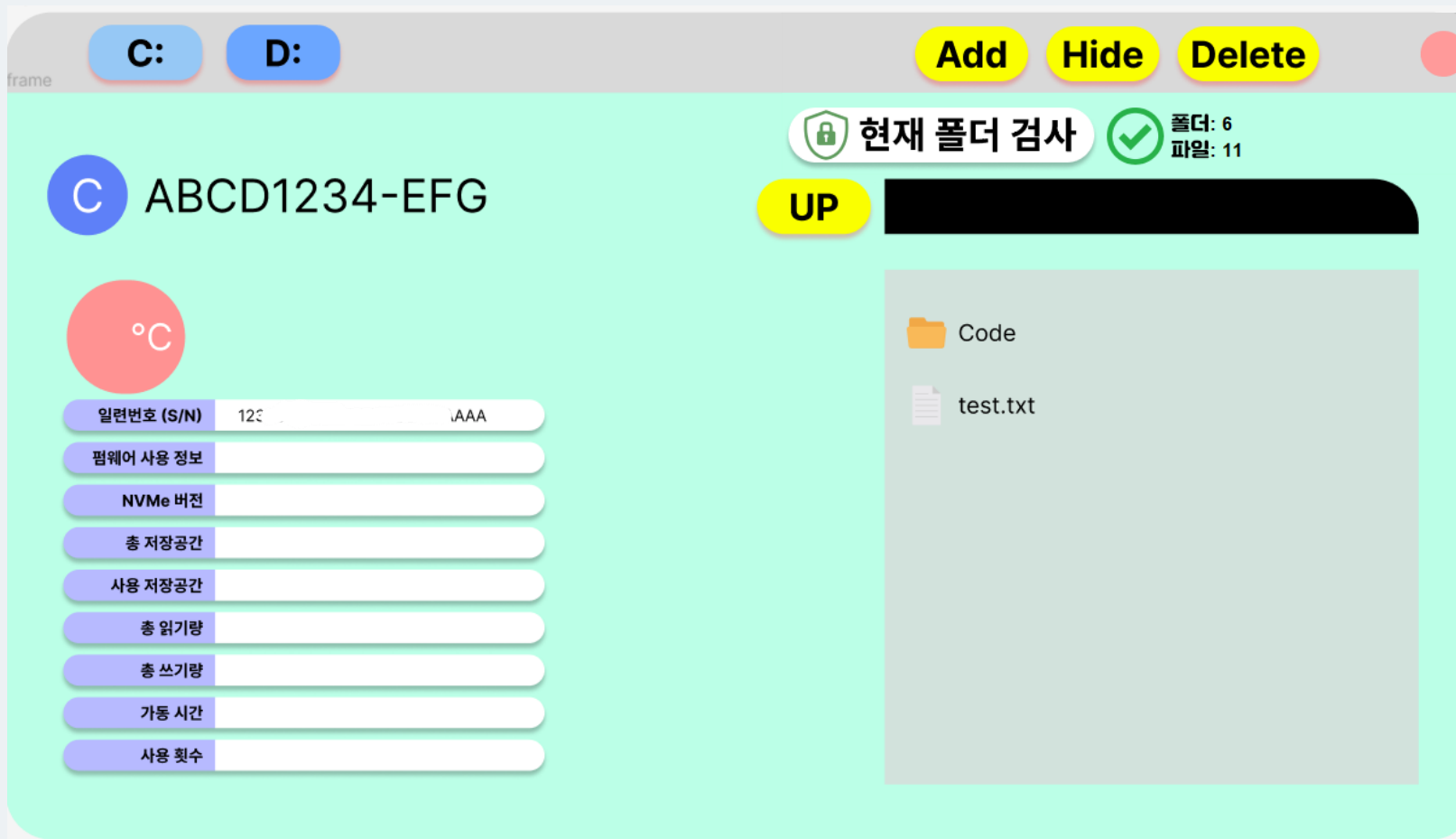
진행 상황

시스템에 설치된 디스크에 대하여 볼륨 정보를 포함한 메타 데이터를 확인할 수 있으며, 드라이브에 위치한 파일들을 확인하고 생성 또는 실행할 수 있습니다.



개선 사항

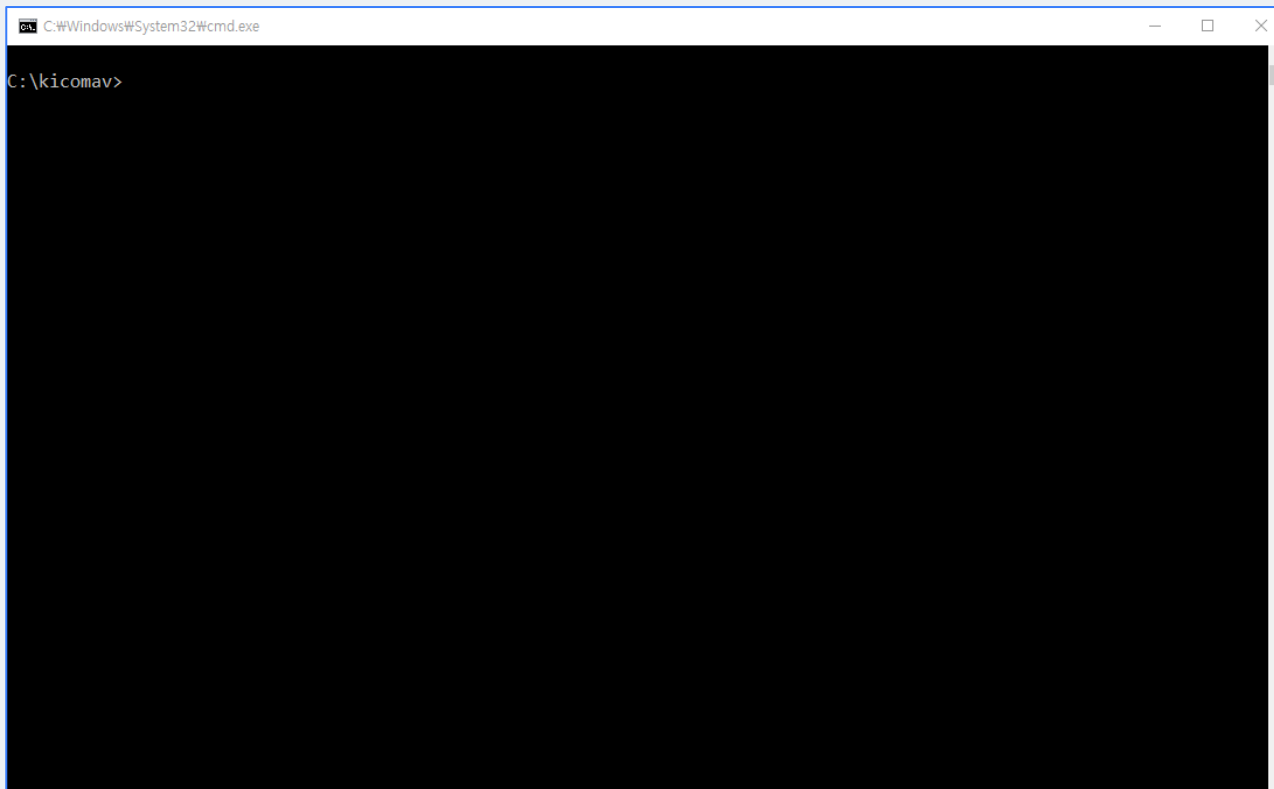
- 드라이브 포맷 기능을 더욱 실용적으로 활용할 수 있는 파일의 완전한 삭제 기능의 도입으로 개선하였습니다.
- 초기 기획안에서 제시했던 각종 설정 메뉴들을 비노출 처리하고 하위 메뉴로 이동시켜 가독성을 대폭 개선하였습니다.
- 기존의 고전적인 툴바 구성에서 벗어나 기능별, 목적별로 유사한 버튼을 묶어 한 눈에 이해할 수 있도록 배치하였습니다.



기능 구현

오픈 소스 백신 엔진의 하나인 KicomAV를 가져와 빠르면서도 보다 정확한 탐지를 가능하게 만들었습니다.

- 백신 엔진의 스캐닝 파트만 가져와서 사용하려고 했으나, 코드가 유기적으로 얹혀있어 어려움이 있었음.
- 메인 함수를 가져와서 파라미터를 조절해보려고 했으나 이 또한 제한적이었음.
- 파이썬의 subprocess 패키지를 이용하여 명령어를 전달하는 방식을 채택하였으나, 개별 컴퓨터에서 릴리즈가 필요함.



About KicomAV

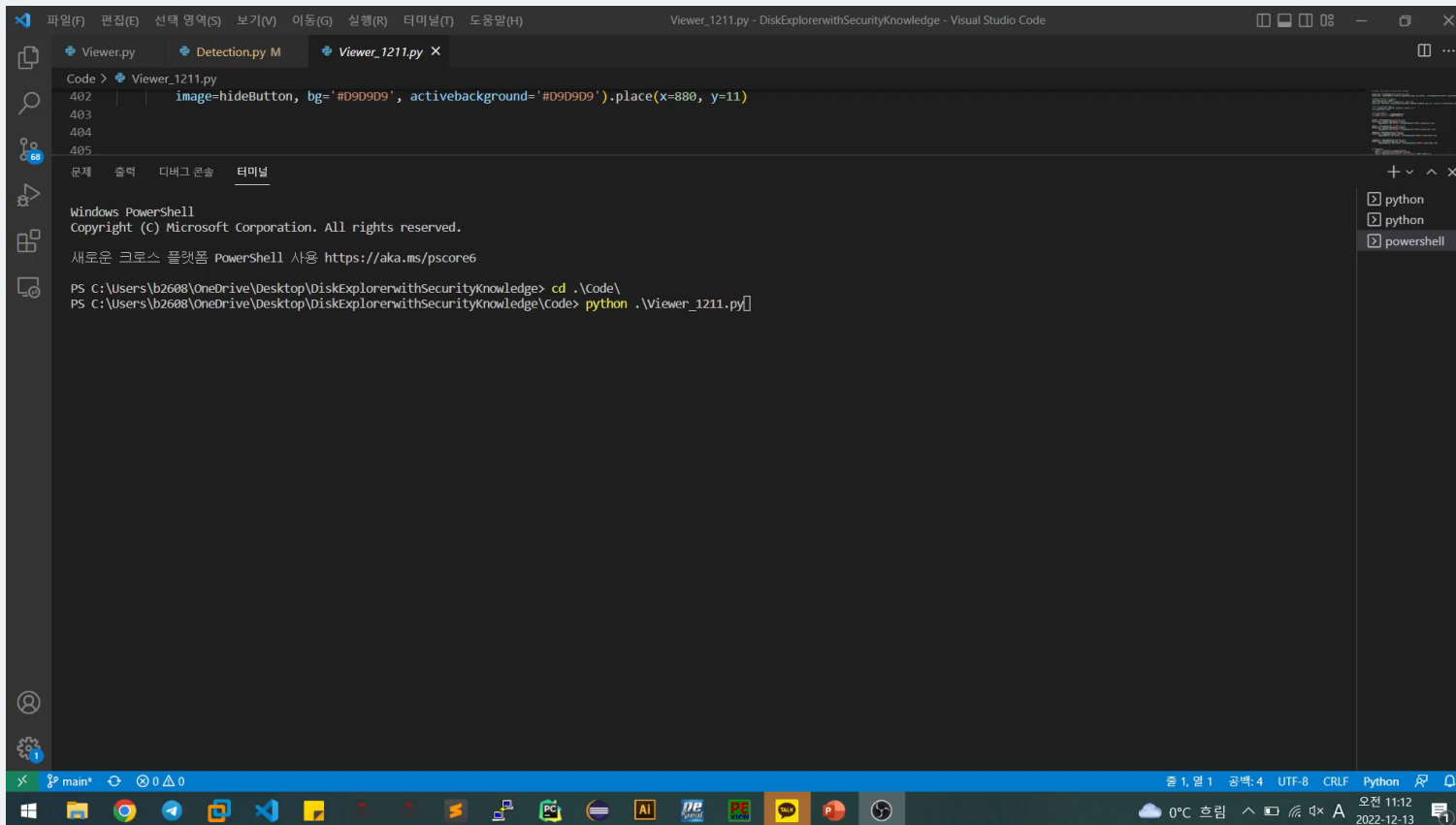
KicomAV is an open source (GPL v2) antivirus engine designed for detecting malware and disinfecting it. In fact, Since 1995, it has been written in C/C++ and it was integrated into the ViRobot engine of [HAURI](#), 1998. I decided to re-create a new KicomAV. So, this is developed in Python. Anyone can participate in the development easily.

악성 프로그램의 탐지

PROJECT
DISK

기능 구현

오픈 소스 백신 엔진의 하나인 KicomAV를 가져와 빠르면서도 보다 정확한 탐지를 가능하게 만들었습니다.

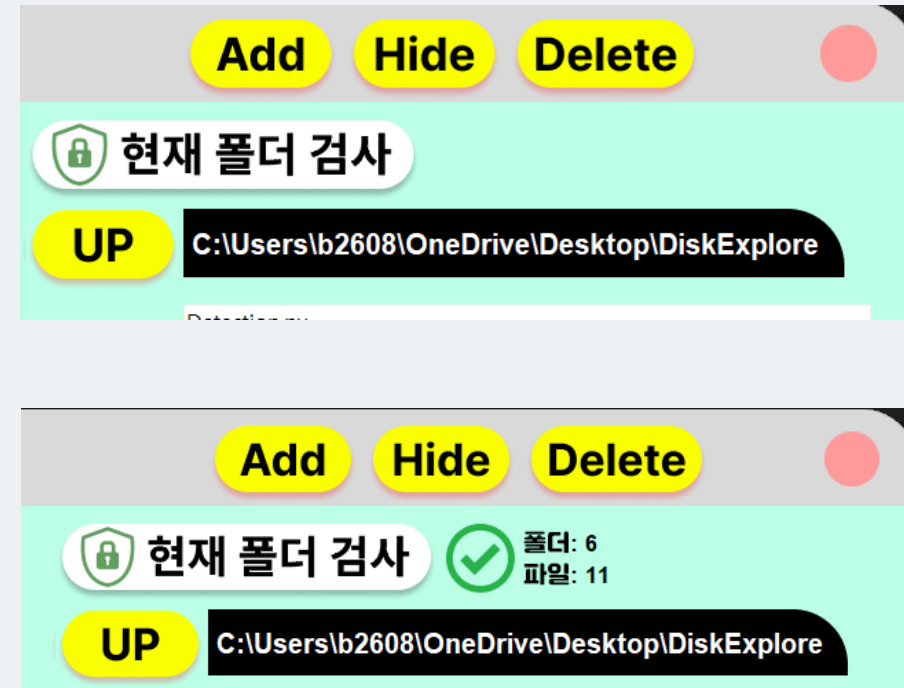


```
Viewer_1211.py
402 image=hideButton, bg='#D9D9D9', activebackground='#D9D9D9').place(x=880, y=11)
403
404
405

Windows PowerShell
Copyright (c) Microsoft Corporation. All rights reserved.

새로운 크로스 플랫폼 PowerShell 사용 https://aka.ms/pscore6

PS C:\Users\b2608\OneDrive\Desktop\DiskExplorerwithSecurityKnowledge> cd .\Code\
PS C:\Users\b2608\OneDrive\Desktop\DiskExplorerwithSecurityKnowledge\Code> python .\Viewer_1211.py
```

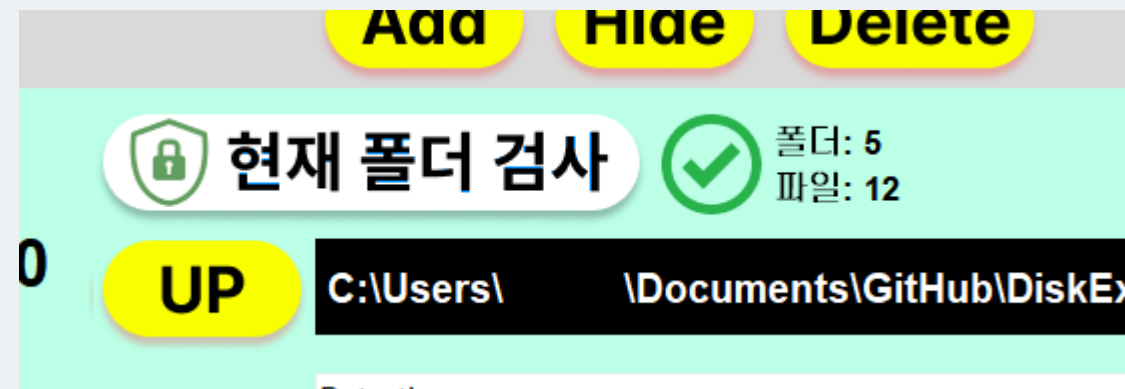
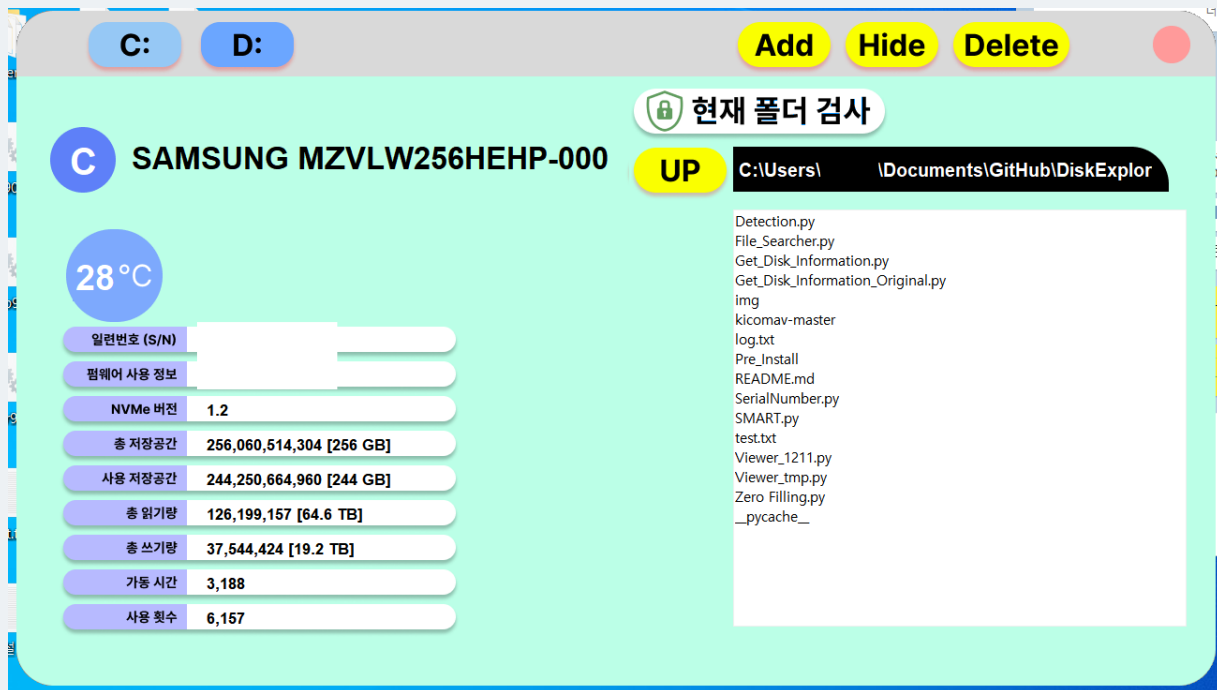


악성 프로그램의 탐지

PROJECT DISK

구현 내용

오픈 소스 백신 엔진의 하나인 KicomAV를 가져와 빠르면서도 보다 정확한 탐지를 가능하게 만들었습니다.



숨김 파일의 노출과 속성값 조절

PROJECT
DISK

구현 내용

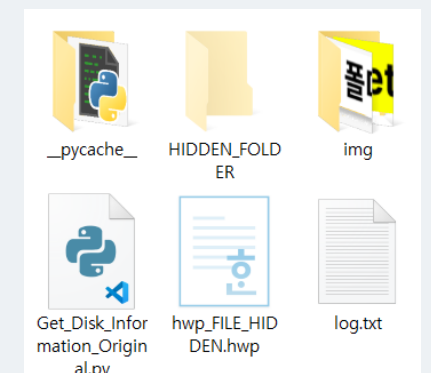
숨김 파일을 포함한 모든 파일을 항상 리스트에 노출하며, 사용자가 모든 파일에 대하여 속성값을 조절할 수 있도록 설계하였습니다.

- 숨겨진 파일은 배경 색상이 하이라이트 처리되어 한 눈에 알아볼 수 있도록 하였습니다.
- HIDE 버튼을 눌러 파일의 숨김 플래그를 변경할 수 있습니다.

The screenshot displays the PROJECT DISK application interface. At the top, there are buttons for 'C:', 'D:', 'Add', 'Hide', and 'Delete'. Below these, a status bar shows '현재 폴더 검사' (Current Folder Check) with a green checkmark, indicating '폴더: 6' (Folder: 6) and '파일: 11' (File: 11). The main section is titled 'C Samsung SSD 970 PRO 512GB' and shows a temperature of '46°C'. A table of disk specifications is provided:

일련번호 (S/N)	필터링
일련번호 (S/N)	
펌웨어 사용 정보	1B2QEXP7
NVMe 버전	1.3
총 저장공간	512,110,190,592 [512 GB]
사용 저장공간	438,262,738,944 [438 GB]
총 읽기량	24,822,331 [12.7 TB]
총 쓰기량	17,365,960 [8.89 TB]
가동 시간	740
사용 횟수	2,112

Below the table, a file list is shown for the path 'C:\Users\ \OneDrive\Desktop\DiskExplore'. The files listed are: Detection.py, File_Searcher.py, Get_Disk_Information.py, Get_Disk_Information_Original.py, HIDDEN_FOLDER (highlighted in yellow), hwp_FILE_HIDDEN.hwp (highlighted in yellow), img, kicomav-master, log.txt, Pre_Install, README.md, SMART.py, Viewer.py, Viewer_1211.py, Zero_Filling.py, and __pycache__.



구현 내용

Windows 파일 탐색기에서 제공하는 삭제 기능은 파일의 플래그만을 수정하는 것으로 얼마든지 삭제한 파일을 복구할 수 있다. 이에 우리는 보안을 신경쓰는 사용자들을 위해 파일을 복구 불가능하도록 완전히 삭제할 수 있는 Secure Erase 기능을 도입한다.

- Zero Filling 방식을 차용하여 파일이 존재하던 영역의 비트를 모두 0으로 덮어씌운다.

```
tempdir = os.path.join(args.basepath, f"files_tmp") #인수에 전달된 2개의 문자열을 결합해, 1개의 경로로 할 수 있음
if not os.path.exists(tempdir): os.makedirs(tempdir) #os.path.exists:tempdir존재 여부 확인, 존재하지 않으면 tempdir라는 dir 생성
print(f"tempdir : {tempdir} 0으로 채워진 파일을 보관하기 위해 생성") #{tempdir}에 tempdir명이 들어감

for i in range(int(free/len(buff))): #사용할 수 있는 양/buff길이 만큼 반복
    ff = open(os.path.join(tempdir, f"file_{i}.tmp"), "wb") #tempdir이랑 file_{i}.tmp경로를 합친 걸 이진수 쓰기 모드로 열기
    start = time.time() #시작
    byteswritten = ff.write(buff) #바이트쓰기 파일에 생성한 바이트 배열 쓰기
    end = time.time() #끝
    speed = byteswritten/1048576 / (end-start) #속도
    total, used, free = shutil.disk_usage(tempdir) #tempdir의 디스크 사용량

    print(f'free: {int(free/(1024*1024))} Mb, speed = {speed:.2f} Mb/sec')
    ff.close()

# 임시 파일 생성
ff = open(os.path.join(tempdir, f"file_final.tmp"), "wb") #os.path.join: tempdir와 file_final.tmp 경로를 합침 write binary
byteswritten = ff.write(bytearray(free)) #
ff.close()

# 임시 파일 삭제
print("드라이브 공간이 가득 참")
ans = input(f"삭제할건가요?: {tempdir} (Y/N)? ")
if "Y" == ans.upper():
    if os.path.exists(tempdir): shutil.rmtree(tempdir)
```

진행 방식

QA는 단순히 제품 출하 직전에 기능 테스트를 진행하는 작업만이 아니고, 개발 전 과정에 걸쳐 제품의 방향을 바로 잡고 이끌어 가는 과정임에 대한 이해를 가지고, 모든 과정에 있어 능동적으로 면밀히 검토하고 방향을 다듬는 과정을 거쳤습니다.

더불어, 개발과 동시에 추가되고 개선되는 기능들에 하자가 있지는 않은지, 기능 명세서를 통해 자체적인 테스트도 수행하였습니다.

Disk Explorer with Security Knowledge (DESK) Functional Implementation Test Specification (FITS)

Criteria	Implementation	디스크 정보 표시창		파일 탐색기			Tool Bar	
		S.M.A.R.T.	리스트 출력	디렉토리 주소창	Folder Up Btn.	파일 실행	숨김 파일 하이라이트	디스크 볼륨 이동
1	의도한 상황 하에서 기능이 정상적으로 작동하는가?							
2	기능의 동작이 프로그램의 다른 기능에 영향을 주지는 않는가?							
3	기능을 반복하여 실행하더라도 문제없이 정상적으로 작동하는가?							
4	다른 기능의 실행 직후에 해당 기능을 실행하더라도 잘 작동하는가?							
5	다른 기능의 실행 직전에 해당 기능을 실행하더라도 잘 작동하는가?							
6	의도하지 않은 자료형의 값을 기능에 넣어주더라도 잘 처리하는가?							
7	예상치 못한 길이의 값을 기능에 넣어주더라도 잘 처리하는가?							
8	기능의 실행을 도중에 취소하더라도 정상적으로 프로그램으로 복귀하는가?							
9	기능이 실행중인 도중에는 다른 기능이 작동하지 못하도록 잘 설계되어 있는가?							
10	기능이 작동중인 중간에 프로그램이 종료 될 경우 시스템에 악영향을 주지 않는가?							
11	경로 지정시에 한글이 포함된 경로를 지정하더라도 정상 작동하는가?							
12	버튼으로 지정된 구역을 클릭하는 이외의 행동으로 해당 기능을 트리거하지 않는가?							

디스크 안심 탐색기

간편하게. 쾌적하게. 강력하게.

Back-up Slides

PROJECT
DISK