파이썬
기말 프로젝트

〈Anti-virus 프로그램 제작〉

목차

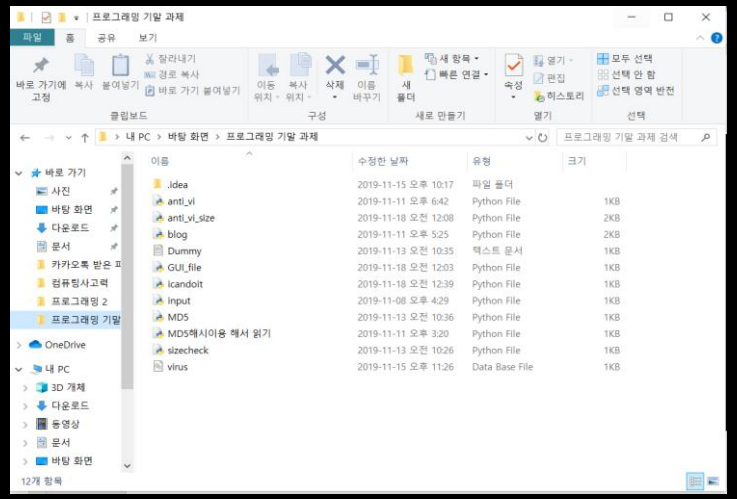
1. 선택 이유

2. 프로그램 구상

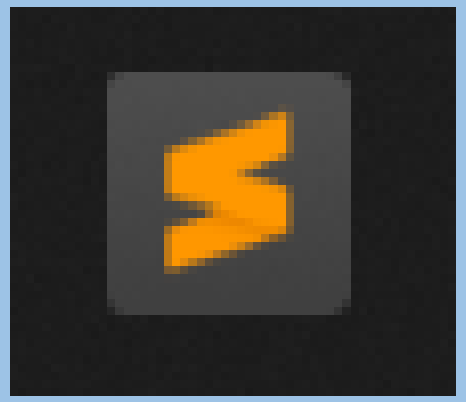
GUI환경에서 파일을 선택한다

파일의 MD5 해시값을 비교를 합니다.

만약 해시값이 악성코드와 같다면 프로그램 삭제



3. 제작 과정



```python
#-*-coding:utf-8 -*-
import sys # sys 모듈은 파이썬 인터프리터가 제공하는 변수와 함수를 직접 제어할 수 있게 해주는 모듈이다. cmd 창에서 실행 될수 있도록 하는 모듈
import os # OS 모듈은 환경 변수나 디렉터리, 파일 등의 OS 자원을 제어할 수 있게 해주는 모듈이다.
import hashlib # hash값을 구하기 위해 넣은 이 모듈은 다양한 보안 해시 및 메시지 요약 알고리즘에 대한 공통 인터페이스를 구현합니다.
from Tkinter import *
import tkFileDialog as filedialog

VirusDB = [] #virus.db를 열어서
vdb =[]
vsize =[]
root = Tk()
root.filename =  filedialog.askopenfilename(initialdir = "/",title = "choose me please",filetypes = (("txt files","*.txt"),("all files","*.*")))
#외부에 있는 파일 읽기
def LoadVirusDB():
    fp = open('virus.db', 'rb')#파일을 읽기

    while True:#파일을 전부 읽기
        line = fp.readline()#한줄 읽기
        if not line : break#파일이 끝날 때 까지 읽기

        line = line.strip()# 양쪽 공백(\n)을 삭제
        VirusDB.append(line)# VirusDB 리스트에 line 넣기

    fp.close()#폴더 닫기

def MakevirusDB():#폴더
    for pattern in VirusDB :
        t = []
        v = pattern.split(':')
        t.append(v[1])
        t.append(v[2])
        vdb.append(t)

        size = int(v[0])
        if vsize.count(size) == 0:
            vsize.append(size)

def SearchVDB(fmd5):
    for t in vdb :
        if t[0] == fmd5:
            return True, t[1]

        return False,''

if __name__ == '__main__':
    LoadVirusDB()
    MakevirusDB()


    fname = root.filename

    size = os.path.getsize(fname)
    if vsize.count(size):
        fp = open(fname,'rb')
        buf = fp.read()
        fp.close()
```

3. 제작 과정-<사용한 모듈>

os

OS 모듈은 환경 변수나 디렉터리, 파일 등의 OS 자원을 제어할 수 있게 해주는 모듈입니다.

hashlib

hash값을 구하기 위해 넣은 이 모듈은 다양한 보안 해시 및 메시지 요약 알고리즘에 대한 공통 인터페이스를 구현합니다.

tkinter

Tkinter 는 파일을 GUI 환경으로 불러 오기 위해 쓰는 모듈 입니다

3. 제작 과정

```
import sys # sys 모듈은 파이썬 인터프리터가 제공하는 변수와 함수를 직접 제어할 수 있게 해주는 모듈이다. cmd 창에서 실행 될수 있도록 하는 모듈
import os # OS 모듈은 환경 변수나 디렉터리, 파일 등의 OS 자원을 제어할 수 있게 해주는 모듈이다.
import hashlib # hash값을 구하기 위해 넣은 이 모듈은 다양한 보안 해시 및 메시지 요약 알고리즘에 대한 공통 인터페이스를 구현합니다.
from Tkinter import * #tkinter 는 GUI 환경을 구상하기 위해 필요
import tkFileDialog as filedialog # tkFileDialog

VirusDB = [] #virus.db를 열어서
vdb =[]
vsize =[]
root = Tk()
root.filename =  filedialog.askopenfilename(initialdir = "/",title = "choose me please",filetypes = (("txt files","*.txt"),("all files","*.*")))
```

```
(initialdir = "/"
```

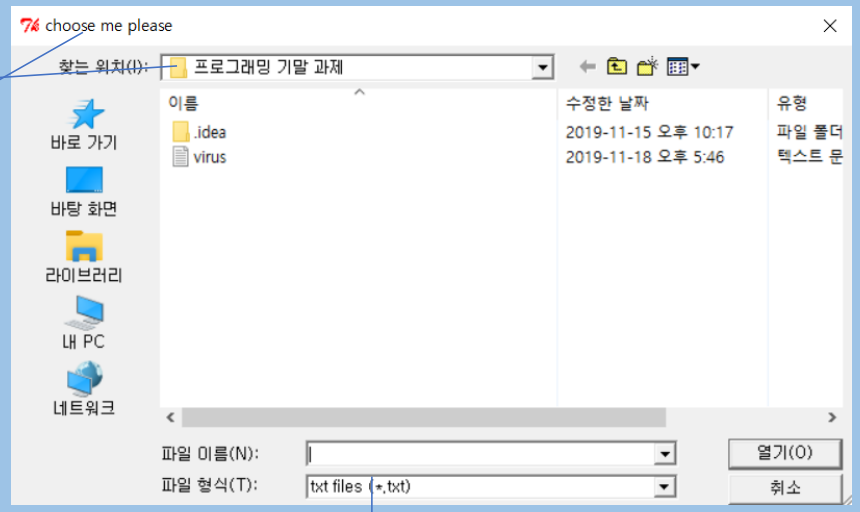
파일을 선택하는 창의 시작 path를 선택

```
,title = "choose me please"
```

창의 이름을 설정

```
,filetypes = (("txt files","*.txt"),("all files","*.*")
```

선택할 파일을 타입을 설정



3. 제작 과정

```
1   68:44d88612fea8a8f36de82e1278abb02f:eicar TEST
2   65:77bff0b143e4840ae73d4582a8914a43:Dummy TEST
```

```python
def LoadVirusDB():
    fp = open('virus.db', 'rb')#파일을 읽기

    while True:#파일을 전부 읽기
        line = fp.readline()#한줄 읽기
        if not line : break#파일이 끝날 때 까지 읽기

        line = line.strip()# 양쪽 공백(\n)을 삭제
        VirusDB.append(line)# VirusDB 리스트에 line 넣기

    fp.close()#폴더 닫기
```

```
== RESTART: C:₩Users₩qkdrn₩OneDrive₩바탕 화면₩프로그래밍 기말 과제₩newfi.py ==
['68:44d88612fea8a8f36de82e1278abb02f:eicar TEST', '65:77bff0b143e4840ae73d4582a
8914a43:Dummy TEST']
>>>
```

3. 제작 과정

```
def MakevirusDB():#폴더
    for pattern in VirusDB :
        t = []
        v = pattern.split(':')
        t.append(v[1])
        t.append(v[2])
        vdb.append(t)

        size = int(v[0])
        if vsize.count(size) == 0:
            vsize.append(size)
```

44d88612fea8a8f36de82e1278abb02f
:eicar TEST

68:

3. 제작 과정

```
def SearchVDB(fmd5):
    for t in vdb :
        if t[0] == fmd5:
            return True, t[1]

        return False,''
```

해시 값을 비교해서 만약 DB파일에 있는 악성코드의 해시값과 같다면 이름과 같이 반환합니다!!

#MD5는 128비트 암호화 해시 함수입니다.

3. 제작 과정

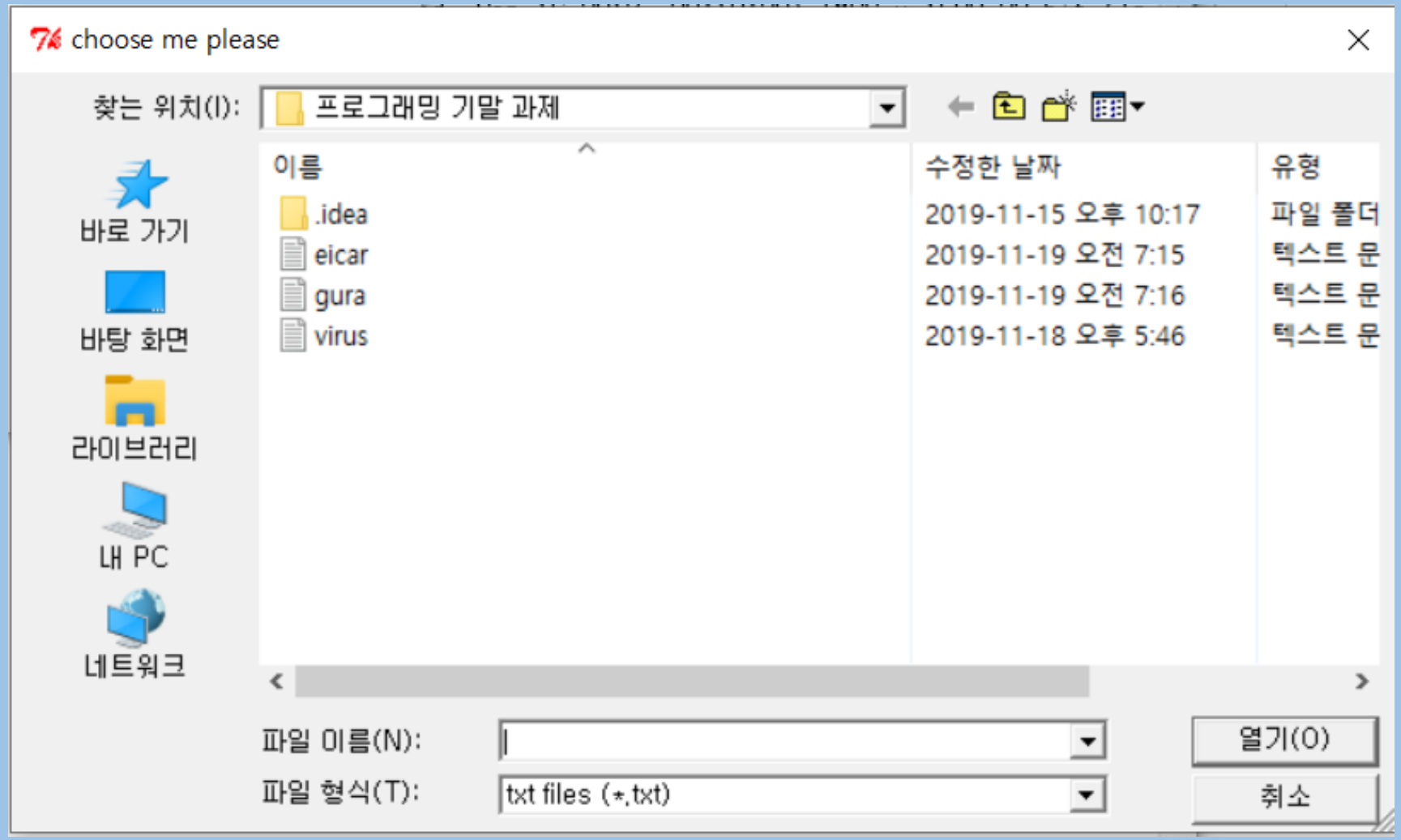
```
LoadVirusDB()
MakevirusDB()


fname = root.filename

size = os.path.getsize(fname)
if vsize.count(size):
    fp = open(fname,'rb')
    buf = fp.read()
    fp.close()

    m= hashlib.md5()
    m.update(buf)
    fmd5 = m.hexdigest()

    ret,vname = SearchVDB(fmd5)
```

대상 파일의 해시값과 db파일의 해시값을 비교합니다.

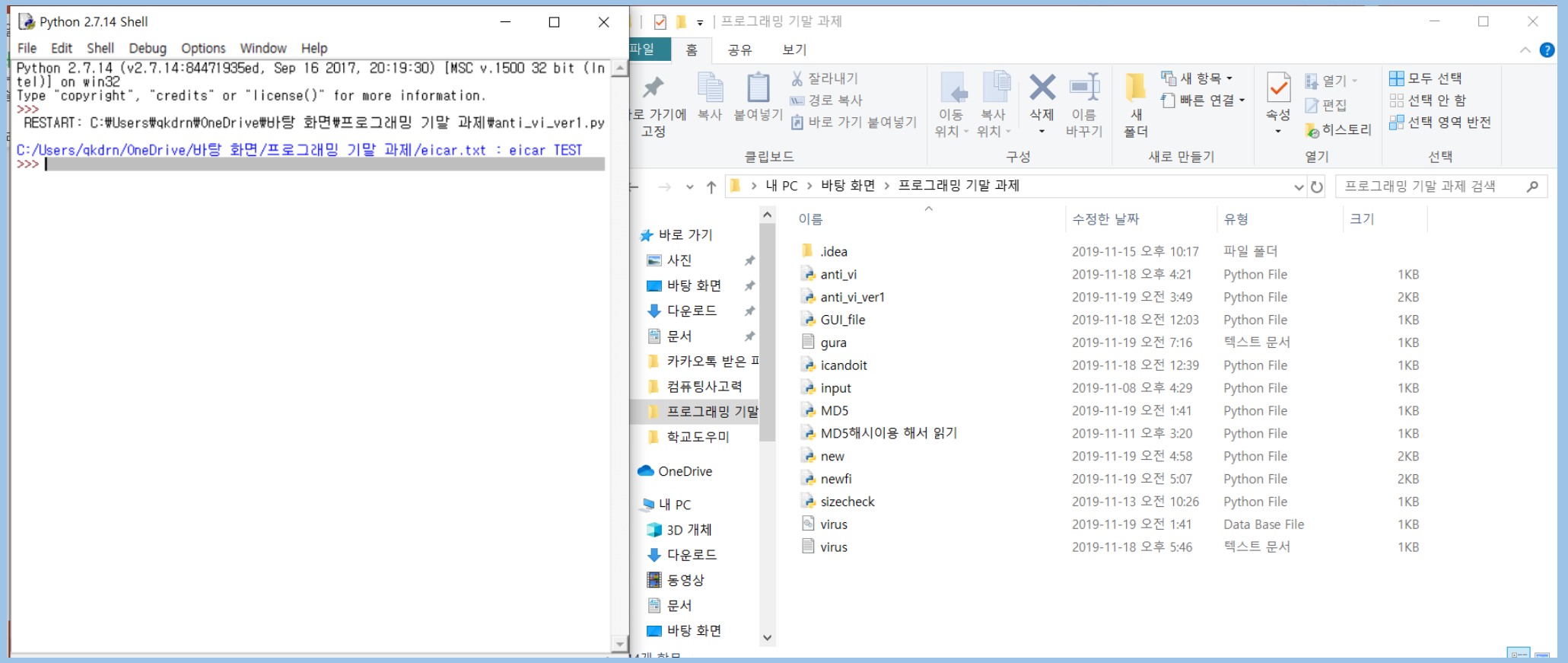
```
            if ret == True:
                print ('%s : %s' %(fname, vname))
                os.remove(fname)
            else:
                print '%s : ok' %(fname)
        else:
            print '%s : ok'%(fname)
```

해시 값이 동일하다면 이는 악성 코드 파일 이므로 삭제를 합니다.
아닐시 OK 싸인을 보냅니다.

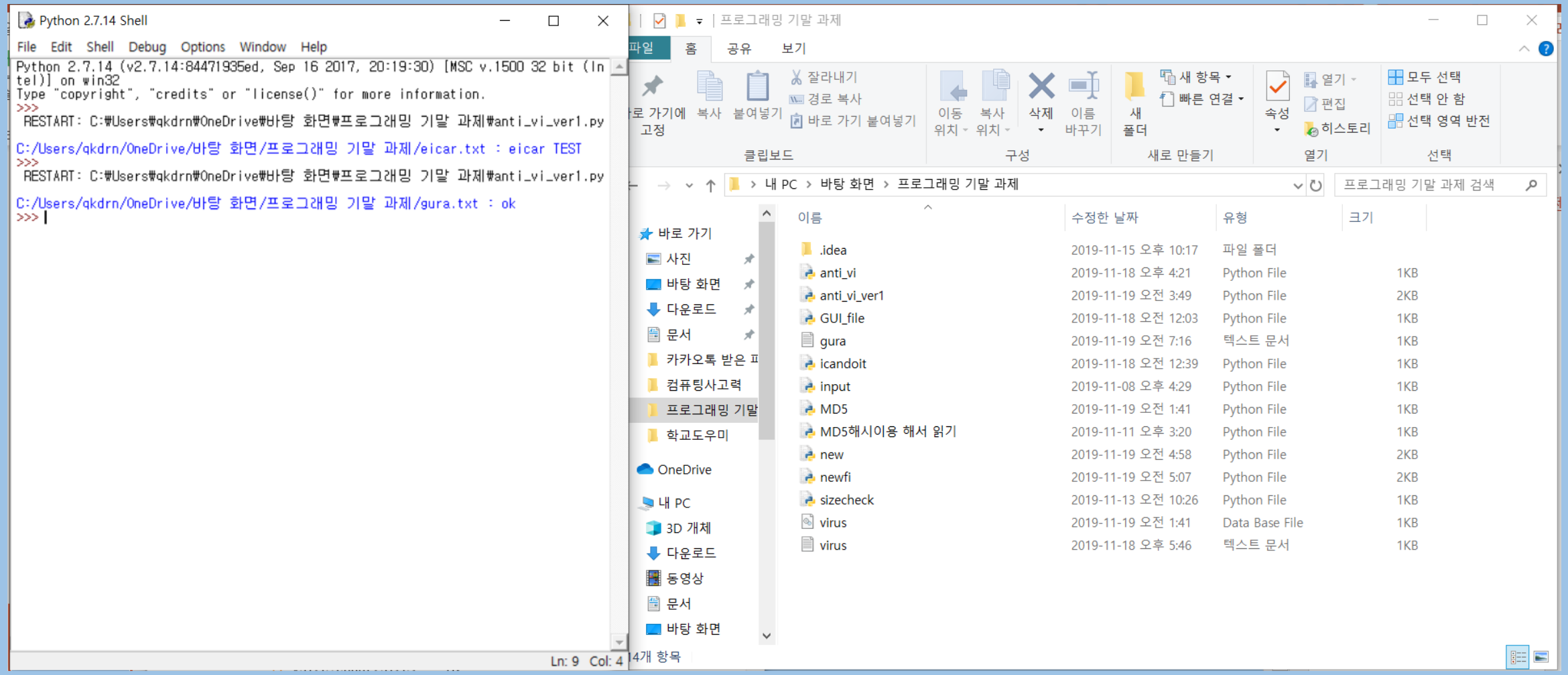
3. 제작 과정


choose me please
찾는 위치(I):
프로그래밍 기말 과제
바로 가기
바탕 화면
라이브러리
내 PC
네트워크
이름
수정한 날짜
유형
.idea
2019-11-15 오후 10:17
파일 폴더
eicar
2019-11-19 오전 7:15
텍스트 문
gura
2019-11-19 오전 7:16
텍스트 문
virus
2019-11-18 오후 5:46
텍스트 문
파일 이름(N):
파일 형식(T):
txt files (*.txt)
열기(O)
취소

3. 제작 과정


Python 2.7.14 Shell
File Edit Shell Debug Options Window Help
Python 2.7.14 (v2.7.14:84471935ed, Sep 16 2017, 20:19:30) [MSC v.1500 32 bit (Intel)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
RESTART: C:₩Users₩qkdrn₩OneDrive₩바탕 화면₩프로그래밍 기말 과제₩anti_vi_ver1.py
C:/Users/qkdrn/OneDrive/바탕 화면/프로그래밍 기말 과제/eicar.txt : eicar TEST
>>>
프로그래밍 기말 과제
파일 홈 공유 보기
내 PC › 바탕 화면 › 프로그래밍 기말 과제
프로그래밍 기말 과제 검색
바로 가기
사진
바탕 화면
다운로드
문서
카카오톡 받은 파
컴퓨팅사고력
프로그래밍 기말
학교도우미
OneDrive
내 PC
3D 개체
다운로드
동영상
문서
바탕 화면
이름 수정한 날짜 유형 크기
.idea 2019-11-15 오후 10:17 파일 폴더
anti_vi 2019-11-18 오후 4:21 Python File 1KB
anti_vi_ver1 2019-11-19 오전 3:49 Python File 2KB
GUI_file 2019-11-18 오전 12:03 Python File 1KB
gura 2019-11-19 오전 7:16 텍스트 문서 1KB
icandoit 2019-11-18 오전 12:39 Python File 1KB
input 2019-11-08 오후 4:29 Python File 1KB
MD5 2019-11-19 오전 1:41 Python File 1KB
MD5해시이용 해서 읽기 2019-11-11 오후 3:20 Python File 1KB
new 2019-11-19 오전 4:58 Python File 2KB
newfi 2019-11-19 오전 5:07 Python File 2KB
sizecheck 2019-11-13 오전 10:26 Python File 1KB
virus 2019-11-19 오전 1:41 Data Base File 1KB
virus 2019-11-18 오후 5:46 텍스트 문서 1KB

3. 제작 과정


Python 2.7.14 Shell
File Edit Shell Debug Options Window Help
Python 2.7.14 (v2.7.14:84471935ed, Sep 16 2017, 20:19:30) [MSC v.1500 32 bit (Intel)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
RESTART: C:₩Users₩qkdrn₩OneDrive₩바탕 화면₩프로그래밍 기말 과제₩anti_vi_ver1.py
C:/Users/qkdrn/OneDrive/바탕 화면/프로그래밍 기말 과제/eicar.txt : eicar TEST
>>>
RESTART: C:₩Users₩qkdrn₩OneDrive₩바탕 화면₩프로그래밍 기말 과제₩anti_vi_ver1.py
C:/Users/qkdrn/OneDrive/바탕 화면/프로그래밍 기말 과제/gura.txt : ok
>>>
Ln: 9 Col: 4
프로그래밍 기말 과제
파일 홈 공유 보기
클립보드
구성
새로 만들기
열기
선택
내 PC › 바탕 화면 › 프로그래밍 기말 과제
프로그래밍 기말 과제 검색
바로 가기
사진
바탕 화면
다운로드
문서
카카오톡 받은 파
컴퓨팅사고력
프로그래밍 기말
학교도우미
OneDrive
내 PC
3D 개체
다운로드
동영상
문서
바탕 화면
이름 수정한 날짜 유형 크기
.idea 2019-11-15 오후 10:17 파일 폴더
anti_vi 2019-11-18 오후 4:21 Python File 1KB
anti_vi_ver1 2019-11-19 오전 3:49 Python File 2KB
GUI_file 2019-11-18 오전 12:03 Python File 1KB
gura 2019-11-19 오전 7:16 텍스트 문서 1KB
icandoit 2019-11-18 오전 12:39 Python File 1KB
input 2019-11-08 오후 4:29 Python File 1KB
MD5 2019-11-19 오전 1:41 Python File 1KB
MD5해시이용 해서 읽기 2019-11-11 오후 3:20 Python File 1KB
new 2019-11-19 오전 4:58 Python File 2KB
newfi 2019-11-19 오전 5:07 Python File 2KB
sizecheck 2019-11-13 오전 10:26 Python File 1KB
virus 2019-11-19 오전 1:41 Data Base File 1KB
virus 2019-11-18 오후 5:46 텍스트 문서 1KB
14개 항목

4. 문제점과 업데이트 할 내용

```
Traceback (most recent call last):
  File "C:₩Users₩qkdrn₩OneDrive₩바탕 화면₩프로그래밍 기말 과제₩anti_vi_size.py",
 line 47, in <module>
    MakevirusDB()
  File "C:₩Users₩qkdrn₩OneDrive₩바탕 화면₩프로그래밍 기말 과제₩anti_vi_size.py",
 line 30, in MakevirusDB
    t.append(v[1])
IndexError: list index out of range
```

1. 휴먼 오류가 많았다.
(실수가 잦았다.)

```
1   68:44d88612fea8a8f36de82e1278abb02f:eicar TEST
2   65:77bff0b143e4840ae73d4582a8914a43:Dummy TEST
```

2. Db파일 에서 1번째 줄 이외의 줄은 안읽힌다.....

4. 문제점과 업데이트 할 내용

```
1   68:44d88612fea8a8f36de82e1278abb02f:eicar TEST
2   65:77bff0b143e4840ae73d4582a8914a43:Dummy TEST
```

1. Db 파일 안에 여러 해시값을 넣어서 여러 악성 코드를 치료 할수있게 만들기

2. 악성코드 패턴 파일 암호화 시키기

3. 파일을 읽는 것이 아닌 디렉토리를 선택하여 그 안에 있는 모든 파일을 읽어 악성코드 찾기


Q&A