[써니나타스 29번 이어서 풀기]

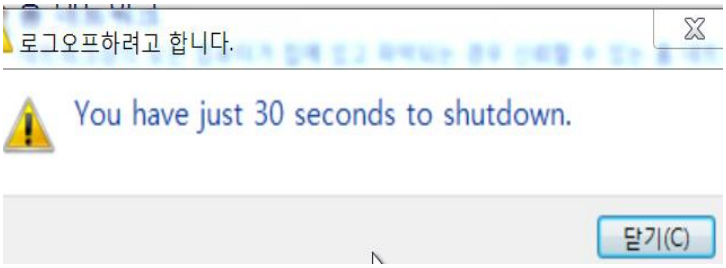
이번에는 구글링을 통해 도움을 얻었습니다.

1.

EGGA로 시작하는 것은 압축이 egg파일로 압축되어야 한다는 것이라고 한다. 따라서 확장자명을 .egg로 변경해주었다.

변경해줬더니 압축파일안에 파일들과 실행 프로그램이 들어있었다. 그리고 .vmx라고 되어있는 것을 실행시켜주었다.

이미 Vmware가 깔려져 있었는데, 자동으로 실행되면서 window7이 열렸다. 그랬더니 30초 후에 재부팅이 된다는 창이 떴다.



일단은 익스플로어를 실행하고 네이버에 접속하였더니 경찰청 사이트가 뜨는 것을 확인할 수 있었다. 구글링을 해보니, 이때 뜨는 것은 host파일이 변조되어 나타나는 현상이라고 그랬다. 그래서, 폴더 옵션에 들어가서 파일 형식의 파일 확장명을 숨기기를 눌러 설정을 바꿔주었다. host파일을 열어보니 다음과 같은 메모장이 떴다.

hosts - 메모장

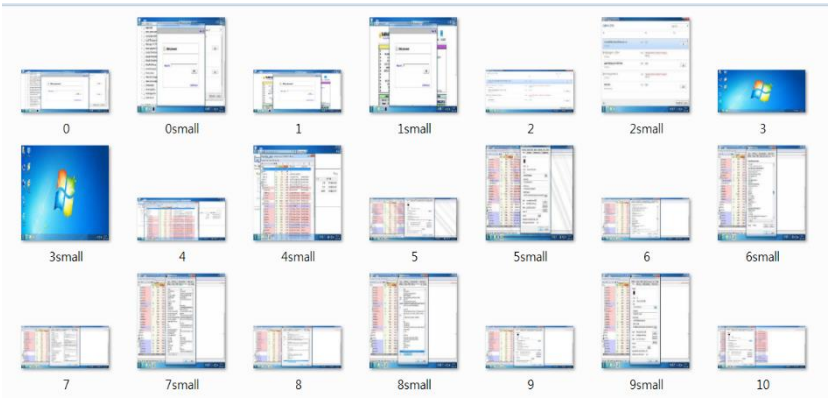
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

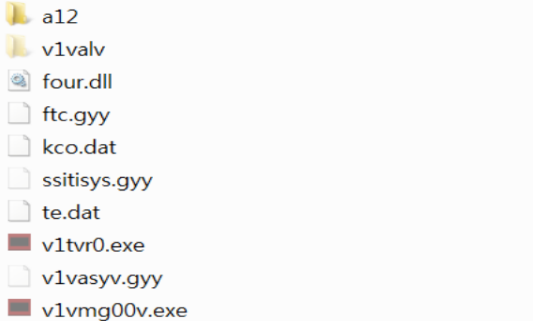
```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
       121.189.57.82    naver.com
       121.189.57.82    www.naver.com
#
#
#      COngr4tur4tiOns!! This is a Keeeeeeeeeeey : what_the_he11_1s_keey
#
#
```

맨 아래줄에 보니까 key는 what_the_he11_1s_keey라는 것을 알 수 있었다.

2.

유성준이 설치한 키로거의 절대경로 및 파일명을 알기 위해서 파일을 들어가서 살펴보았더니 이상한 사진들이 많이 있는 폴더가 있었다. 이때 발견한 키로거의 경로가 "C:₩v196vv8₩v1tvr0.exe"인 것을 알 수 있었다.





3.

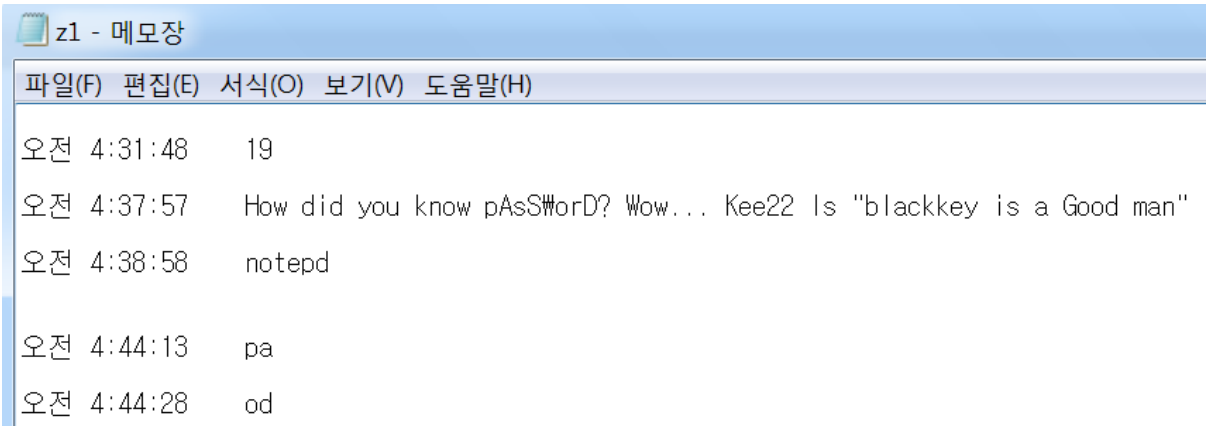
키로거가 다운로드 된 시간은 "**BrowsingHistoryView"**를 통해 알 수 있었다.(이것도 구글링 해봤다..)

-> 2016-05-24_04:25:06 였다.

4.

키로거를 통해서 알아내고자 했던 내용을 찾아야했다. 그래야 최종 키를 알 수 있으니...

여러 파일을 찾아 들어가보니 키에 대한 정보를 얻을 수 있는 텍스트 파일을 찾을 수 있었다.



마지막 키의 답은 "blackkey is a Good man"이였다.

위의 모든 값들을 조합해보니까

what_the_he11_1s_keeyc:₩v196vv8₩v1tvr0.exe2016-05-24_04:25:06blackkey is a Good man이 되었다.

사실 문제를 제대로 안읽고 바로 Authkey에 입력했더니 자꾸만 아니라고 창이 떠서 기분이 안좋았는데, 다시 읽어보니까 lowercase(MD5(1,2,3,4번키)) 였다. 이 말은 즉시, MD5로 인코딩을 해줘야 한다는 것이다. 바꿔보니, 970f891e3667fce147b222cc9a8699d4 가 나왔다. 이걸 정답창에 입력하니까 최종 정답이였다!