3th HolyShield Forensics Probs Writeups

13lackc4t

13lackc4t@naver.com

http://13lackc4t.blog.me

Jeon Chang-bae

Index

1. About Holyshield

2. Forensics 200

3. Forensics 300

4. Forensics 400

5. Q & A

About Holyshield

About Holyshield

Overview

- 가톨릭대학교 침해사고대응팀(CAT-CERT)에서 주최하는 해킹방어대회
- 2010년부터 매년 개최
- 여러가지 분야에서 16문제를 출제
- 온라인 CTF 형태로 진행

3th Holyshield

- 2012년 11월 16일 18:00 ~ 2012년 11월 18일 06:00(UTC+9:00)
- 총 상금 180만원

  (1등 100만원, 2등 50만원, 3등 30만원)
- PACKET 1문제, WEB 5문제, REVERSING 4문제,

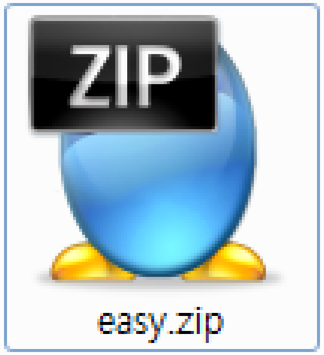
  PWNABLE 3문제, FORENSICS 3문제 출제
- 2번의 이벤트 진행
- 1등 : Class is permanent
  2등 : KAIST GoN
  3등 : B10S

Forensics 200

Forensics 200

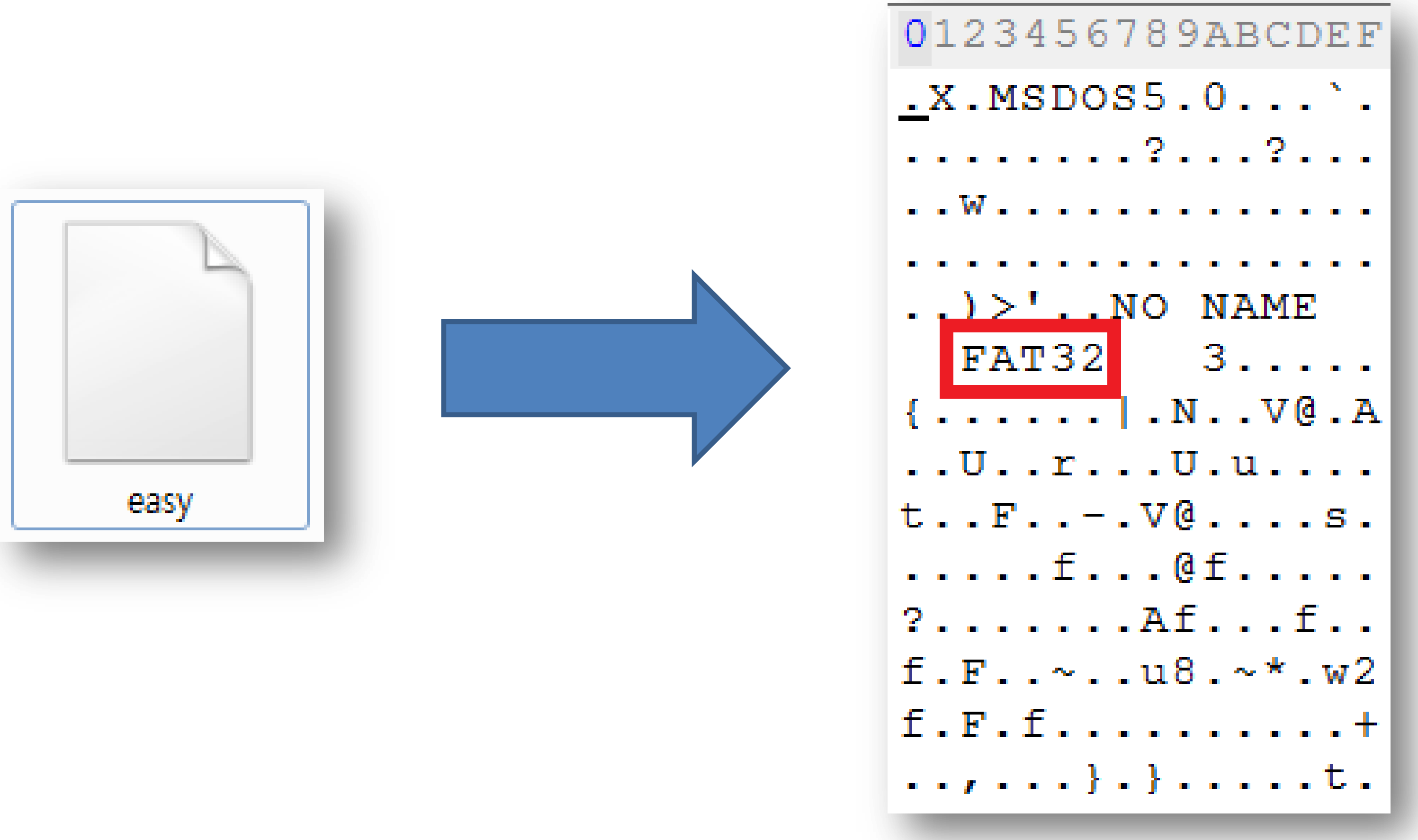
Overview

- Find the Key :)



Explanation (1)

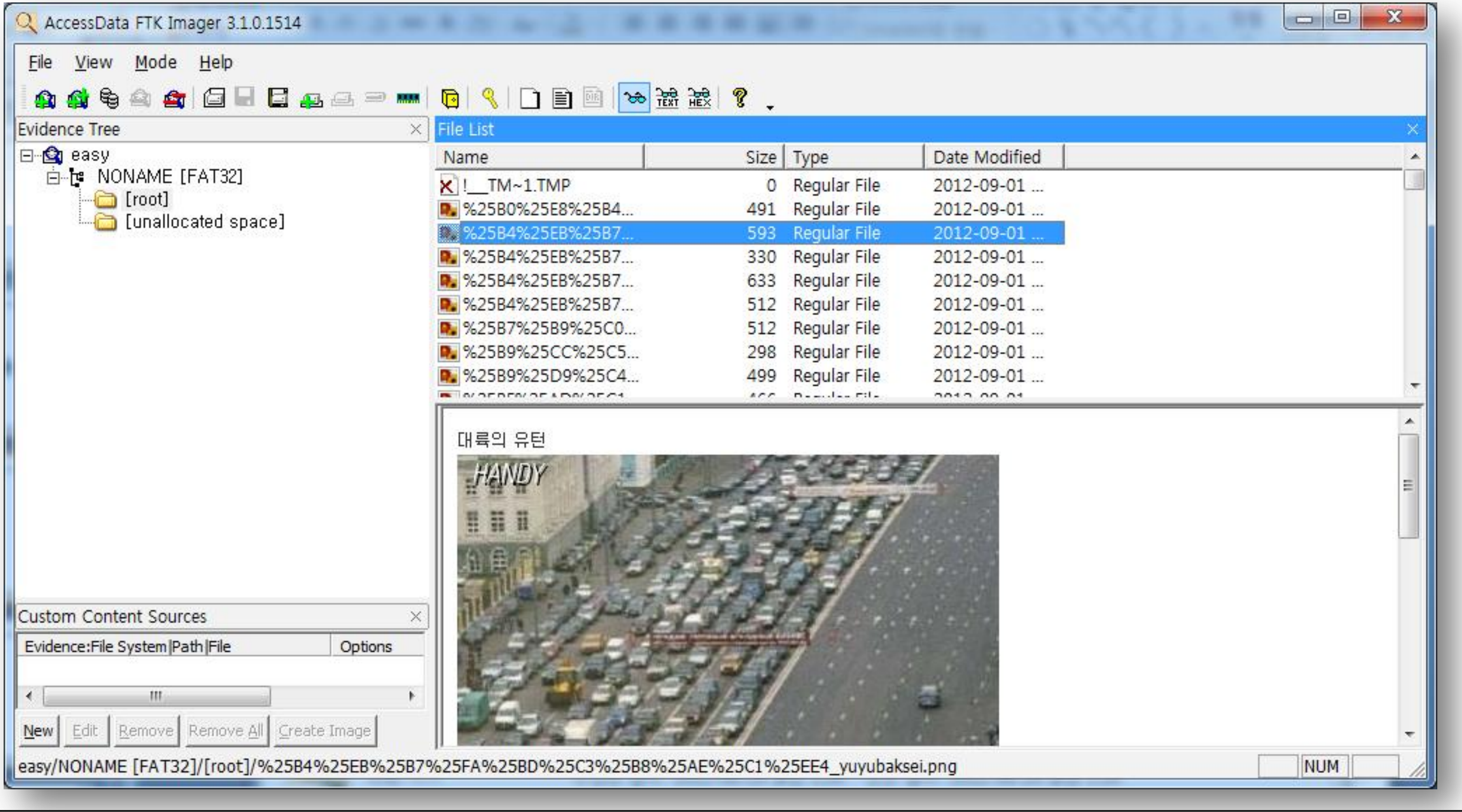
- Identify filesystem



```
0123456789ABCDEF
.X.MSDOS5.0...`.
........?...?...
..w.............
................
..)>'..NO NAME  
  FAT32   3.....
{......|.N..V@.A
..U..r...U.u....
t..F..-.V@....s.
.....f...@f.....
?.......Af...f..
f.F..~..u8.~*.w2
f.F.f..........+
..,...}.}.....t.
```

Explanation (2)

- Mount image

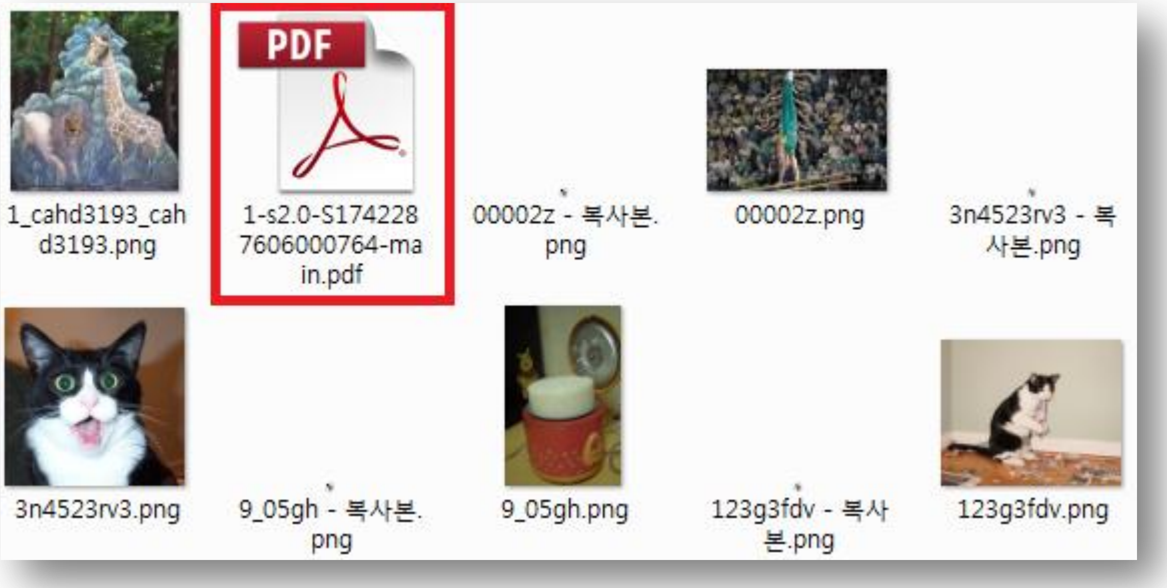


Name	Size	Type	Date Modified
!__TM~1.TMP	0	Regular File	2012-09-01 ...
%25B0%25E8%25B4...	491	Regular File	2012-09-01 ...
%25B4%25EB%25B7...	593	Regular File	2012-09-01 ...
%25B4%25EB%25B7...	330	Regular File	2012-09-01 ...
%25B4%25EB%25B7...	633	Regular File	2012-09-01 ...
%25B4%25EB%25B7...	512	Regular File	2012-09-01 ...
%25B7%25B9%25C0...	512	Regular File	2012-09-01 ...
%25B9%25CC%25C5...	298	Regular File	2012-09-01 ...
%25B9%25D9%25C4...	499	Regular File	2012-09-01 ...

easy/NONAME [FAT32]/[root]/%25B4%25EB%25B7%25FA%25BD%25C3%25B8%25AE%25C1%25EE4_yuyubaksei.png

Explanation (3)

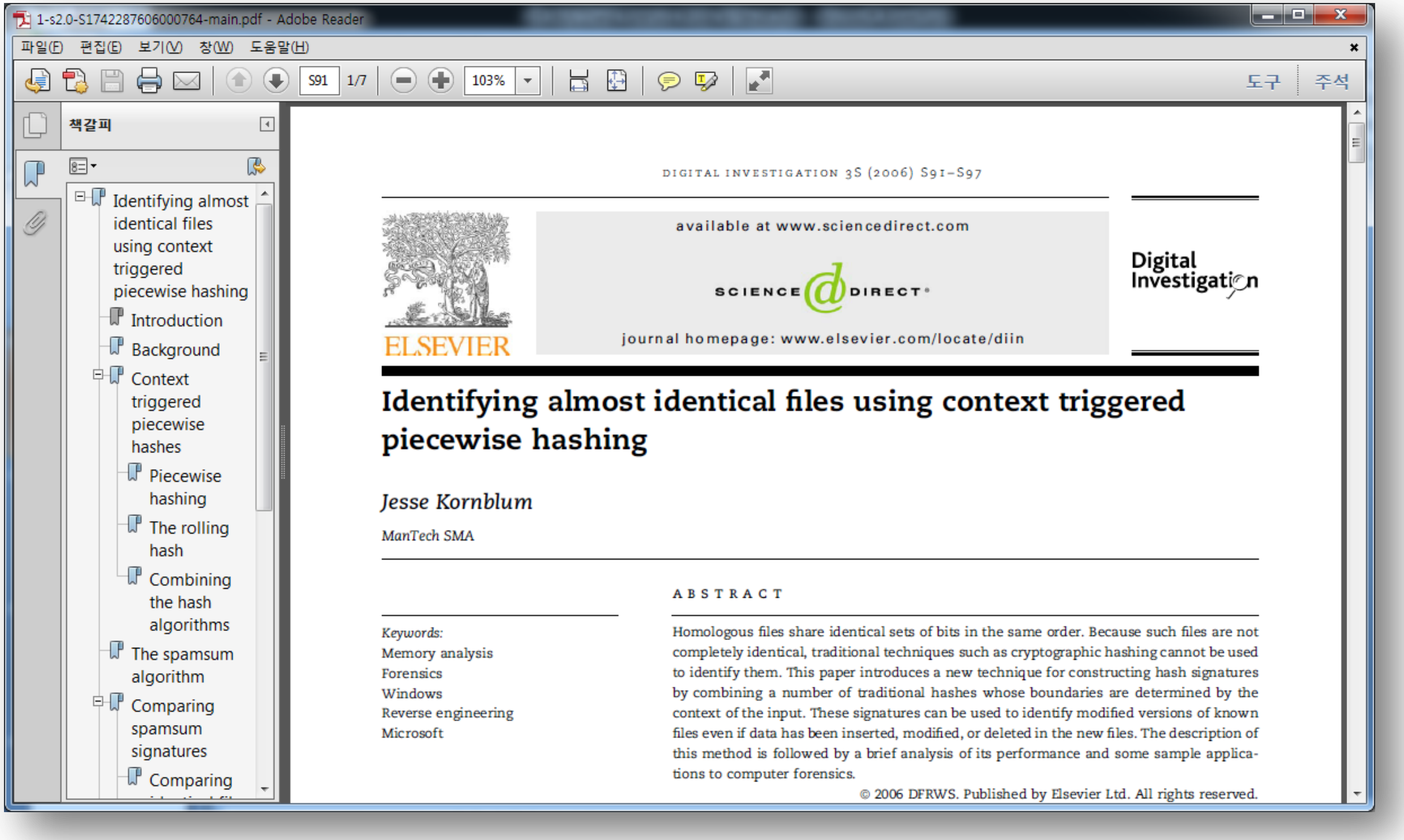
- Extract all files
- only one adobe document file



Explanation (4)

- Context triggered piecewise hashing

1-s2.0-S1742287606000764-main.pdf


1-s2.0-S1742287606000764-main.pdf - Adobe Reader
파일(F) 편집(E) 보기(V) 창(W) 도움말(H)
S91
1/7
103%
도구
주석
책갈피
Identifying almost identical files using context triggered piecewise hashing
Introduction
Background
Context triggered piecewise hashes
Piecewise hashing
The rolling hash
Combining the hash algorithms
The spamsum algorithm
Comparing spamsum signatures
Comparing

DIGITAL INVESTIGATION 3S (2006) S91–S97

available at www.sciencedirect.com

SCIENCE DIRECT®

journal homepage: www.elsevier.com/locate/diin

ELSEVIER

Digital Investigation

Identifying almost identical files using context triggered piecewise hashing

Jesse Kornblum

ManTech SMA

ABSTRACT

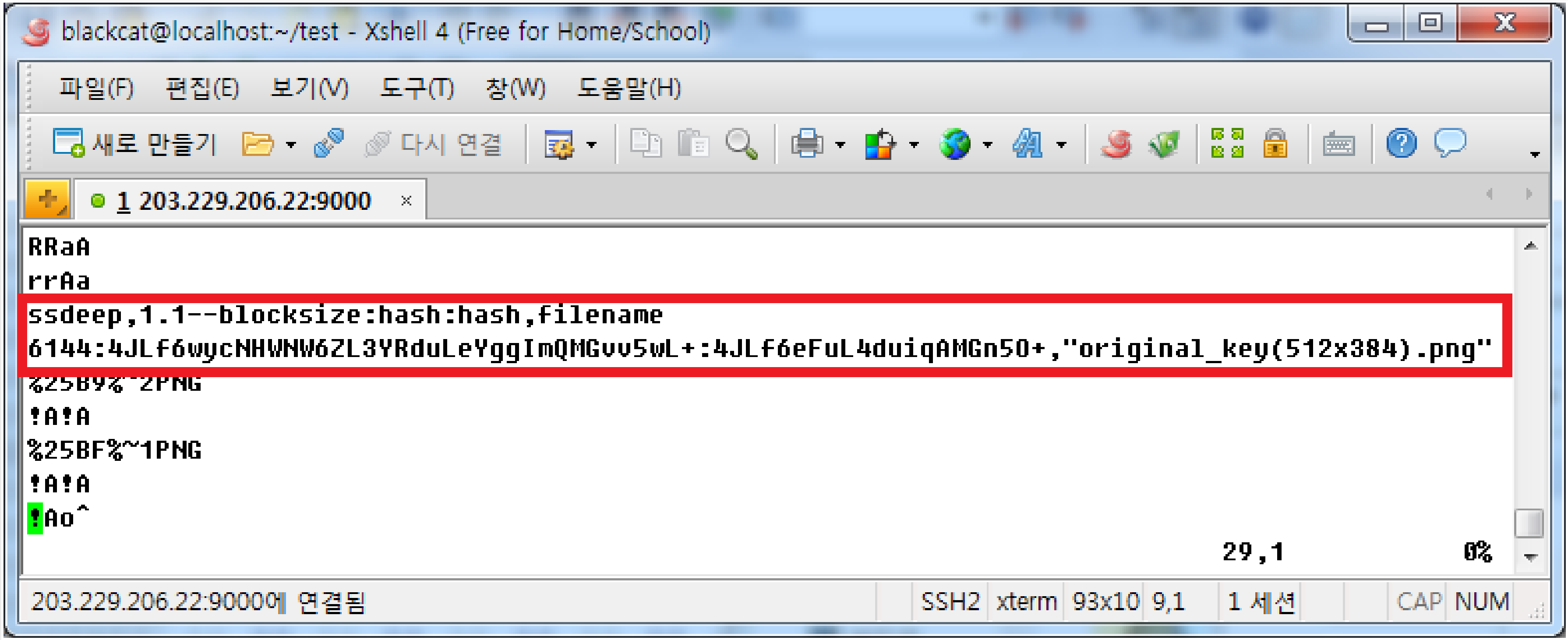
Keywords:
Memory analysis
Forensics
Windows
Reverse engineering
Microsoft

Homologous files share identical sets of bits in the same order. Because such files are not completely identical, traditional techniques such as cryptographic hashing cannot be used to identify them. This paper introduces a new technique for constructing hash signatures by combining a number of traditional hashes whose boundaries are determined by the context of the input. These signatures can be used to identify modified versions of known files even if data has been inserted, modified, or deleted in the new files. The description of this method is followed by a brief analysis of its performance and some sample applications to computer forensics.

© 2006 DFRWS. Published by Elsevier Ltd. All rights reserved.

Explanation (5)

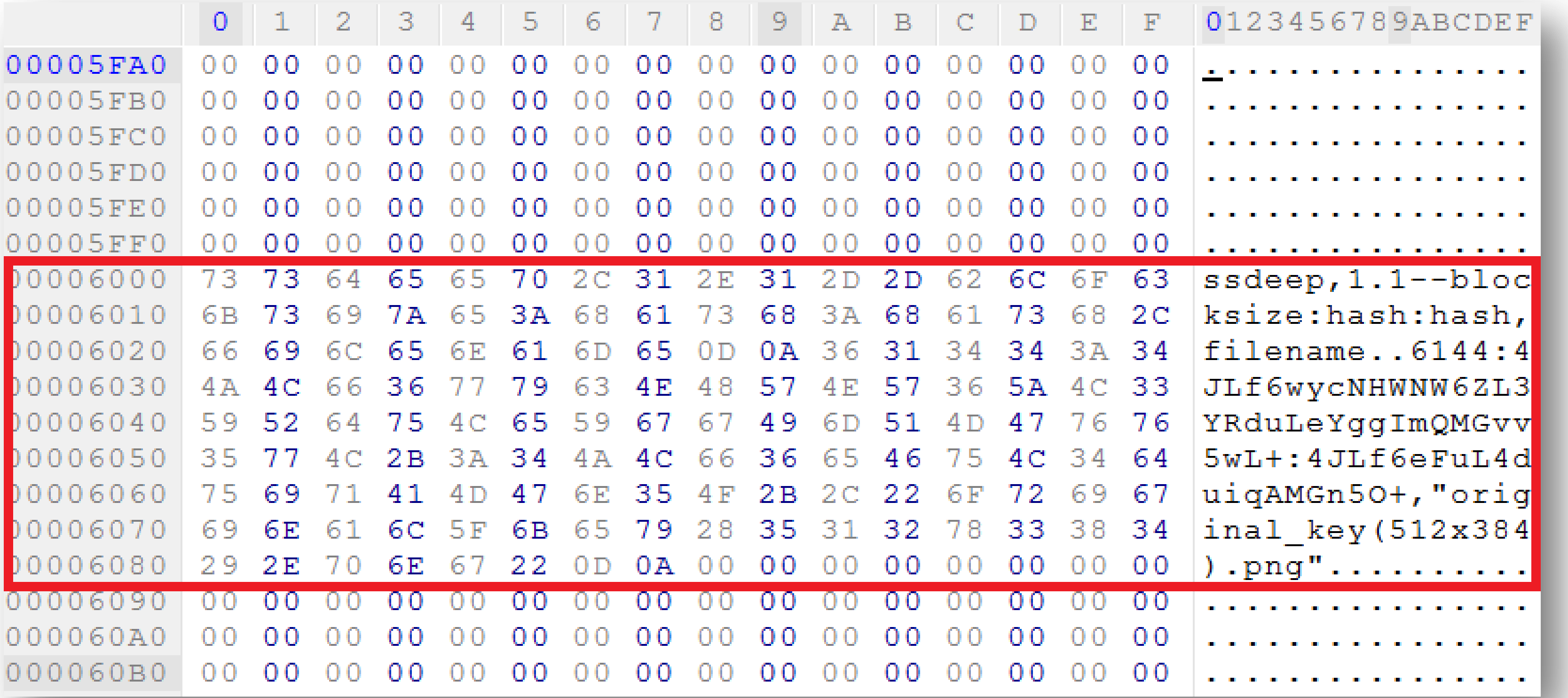
- Get special string
- This show original file's name, size and hash value


blackcat@localhost:~/test - Xshell 4 (Free for Home/School)
파일(F) 편집(E) 보기(V) 도구(T) 창(W) 도움말(H)
새로 만들기
다시 연결
1 203.229.206.22:9000
203.229.206.22:9000에 연결됨
SSH2
xterm
93x10
9,1
1 세션
CAP
NUM

```
RRaA
rrAa
ssdeep,1.1--blocksize:hash:hash,filename
6144:4JLf6wycNHWNW6ZL3YRduLeYggImQMGvv5wL+:4JLf6eFuL4duiqAMGn5O+,"original_key(512x384).png"
%25B9%^2PNG
!A!A
%25BF%~1PNG
!A!A
!Ao^
                                                                            29,1          0%
```

Explanation (6)

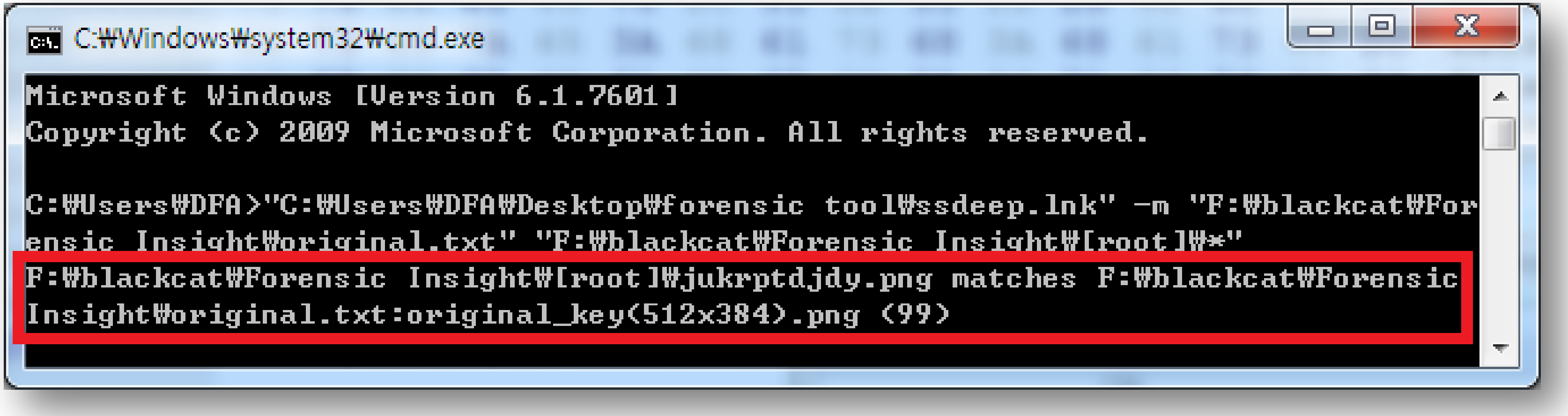
- Ssdeep hash value in slack space



```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
00005FA0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00005FB0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00005FC0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00005FD0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00005FE0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00005FF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00006000  73 73 64 65 65 70 2C 31 2E 31 2D 2D 62 6C 6F 63  ssdeep,1.1--bloc
00006010  6B 73 69 7A 65 3A 68 61 73 68 3A 68 61 73 68 2C  ksize:hash:hash,
00006020  66 69 6C 65 6E 61 6D 65 0D 0A 36 31 34 34 3A 34  filename..6144:4
00006030  4A 4C 66 36 77 79 63 4E 48 57 4E 57 36 5A 4C 33  JLf6wycNHWNW6ZL3
00006040  59 52 64 75 4C 65 59 67 67 49 6D 51 4D 47 76 76  YRduLeYggImQMGvv
00006050  35 77 4C 2B 3A 34 4A 4C 66 36 65 46 75 4C 34 64  5wL+:4JLf6eFuL4d
00006060  75 69 71 41 4D 47 6E 35 4F 2B 2C 22 6F 72 69 67  uiqAMGn5O+,"orig
00006070  69 6E 61 6C 5F 6B 65 79 28 35 31 32 78 33 38 34  inal_key(512x384
00006080  29 2E 70 6E 67 22 0D 0A 00 00 00 00 00 00 00 00  ).png"..........
00006090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000060A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000060B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Explanation (7)

- Make a file stored original file’s hash value
- Using ssdeep, find the file be nearest original file

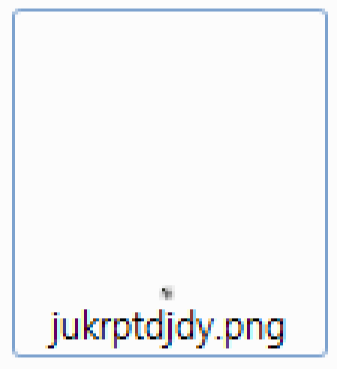


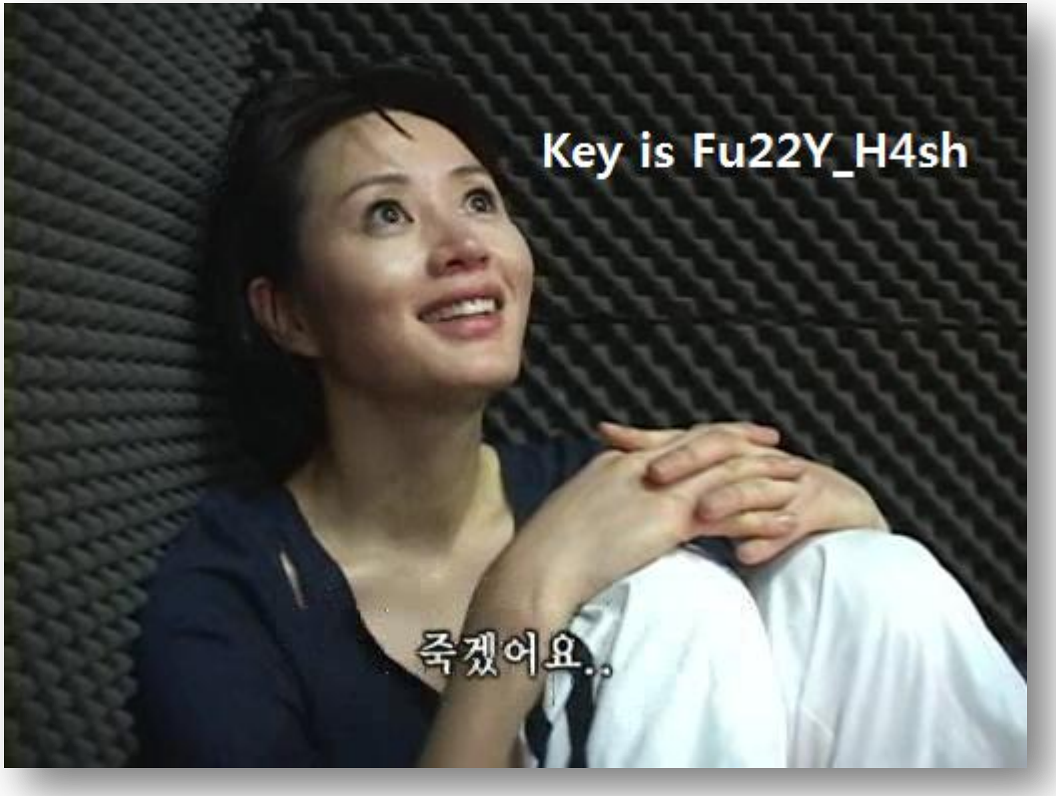
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:₩Users₩DFA>"C:₩Users₩DFA₩Desktop₩forensic tool₩ssdeep.lnk" -m "F:₩blackcat₩For
ensic Insight₩original.txt" "F:₩blackcat₩Forensic Insight₩[root]₩*"
F:₩blackcat₩Forensic Insight₩[root]₩jukrptdjdy.png matches F:₩blackcat₩Forensic
Insight₩original.txt:original_key(512x384).png (99)
```

Explanation (8)

- Change the pic's width and height





Behind

- Context triggered piecewise hashing
- Slack space
- Number of pics?

Forensics 300

Forensics 300

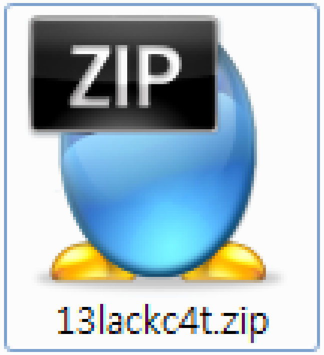
Overview

- There are Digital Evidences collected on secret informant's computer.

  Find the secret file!

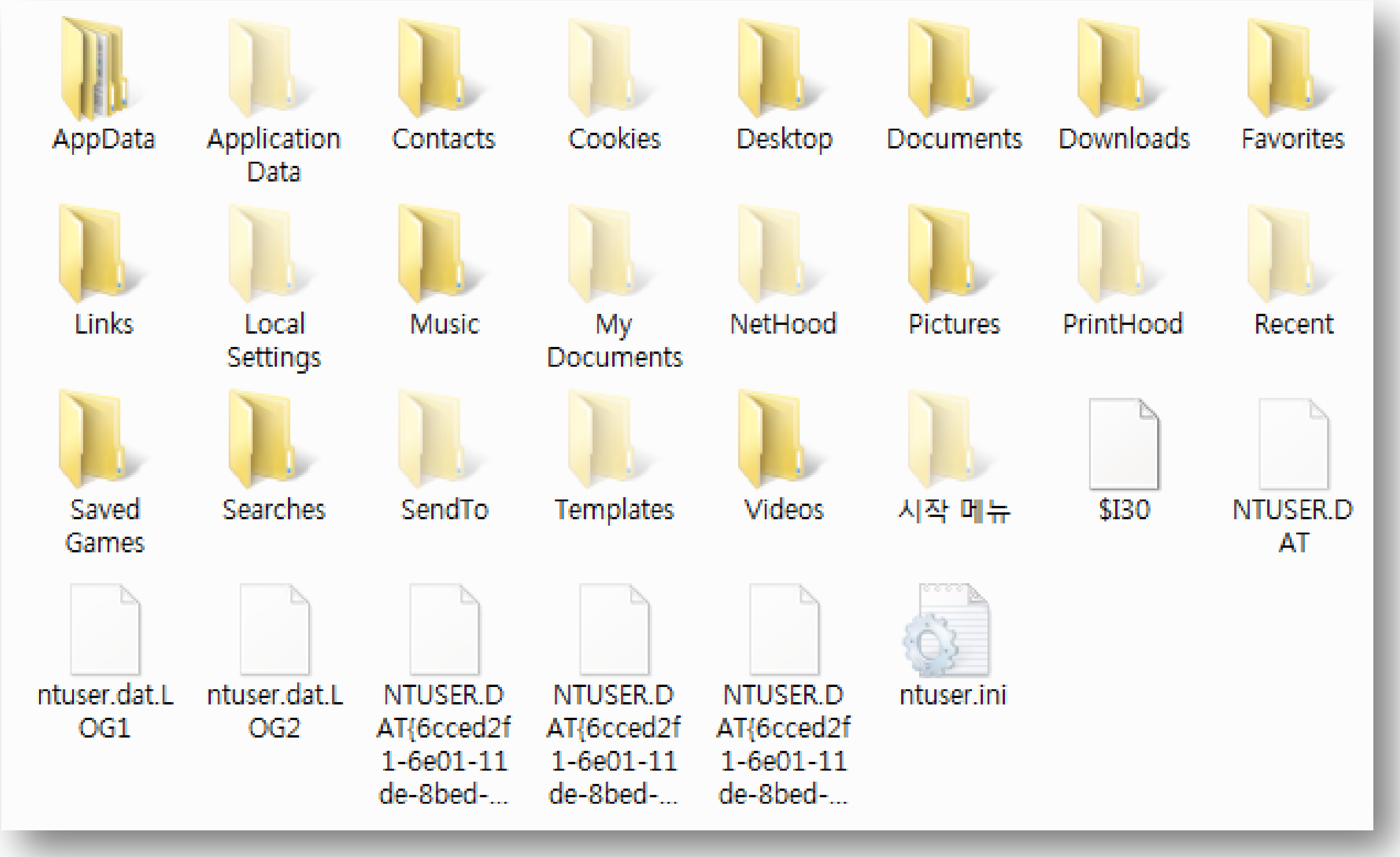
- 아래는 기밀유출자의 컴퓨터에서 수집된 디지털 증거입니다.

  기밀파일을 찾으십시오!



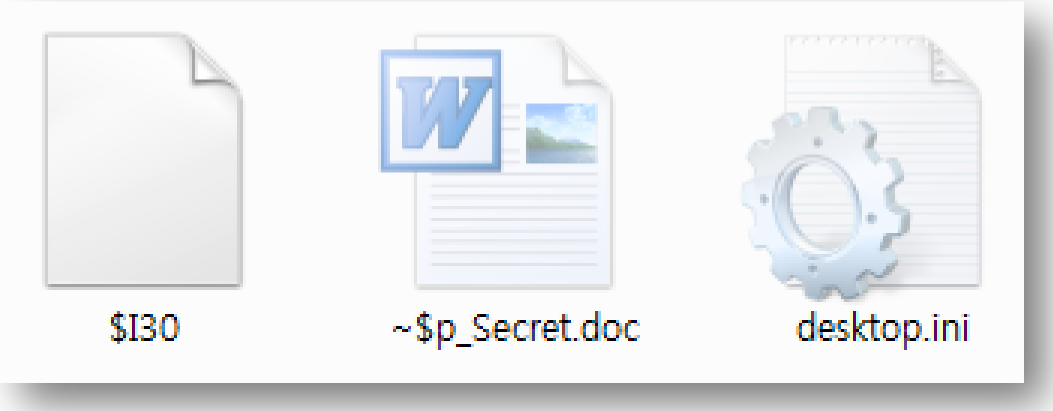
Explanation (1)

- User Folder



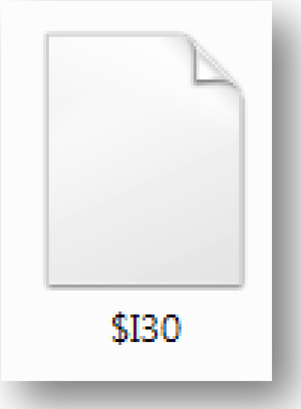
Explanation (2)

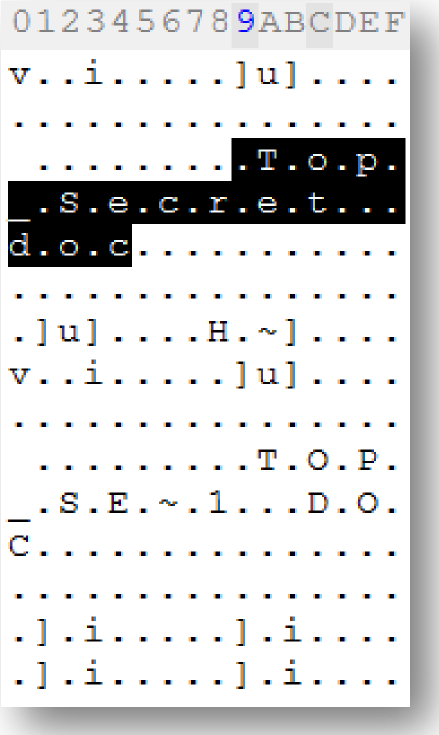
- Under Downloads folder
  - ~$p_Secret.doc -> MS words file's temporary file
  - $I30 -> store $FILE_NAME attribute about current folder



Explanation (3)

- Identify the download file's name

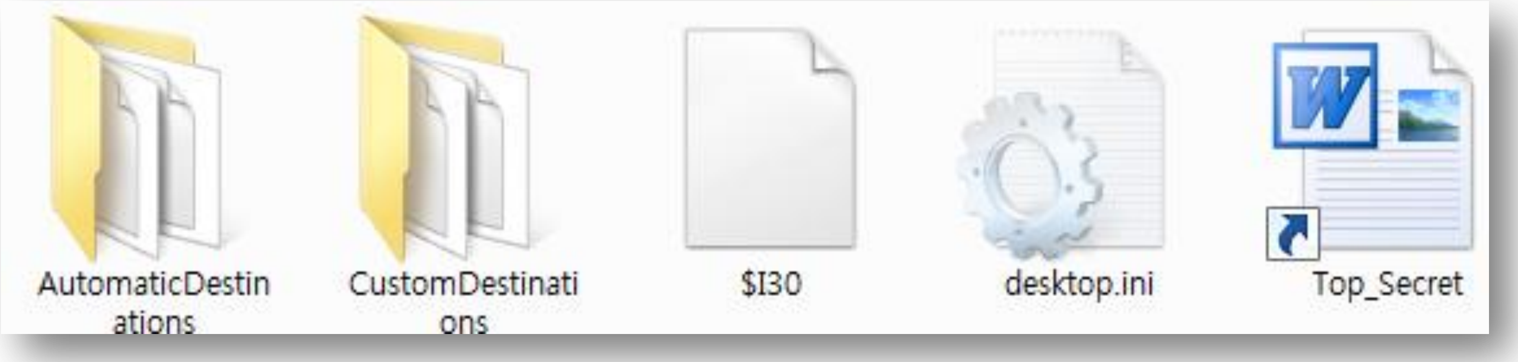




```
0123456789ABCDEF
v..i.....]u]....
................
 ........ .T.o.p.
_.S.e.c.r.e.t...
d.o.c...........
................
.]u]....H.~]....
v..i.....]u]....
................
 .........T.O.P.
_.S.E.~.1...D.O.
C...............
................
.].i.....].i....
.].i.....].i....
```

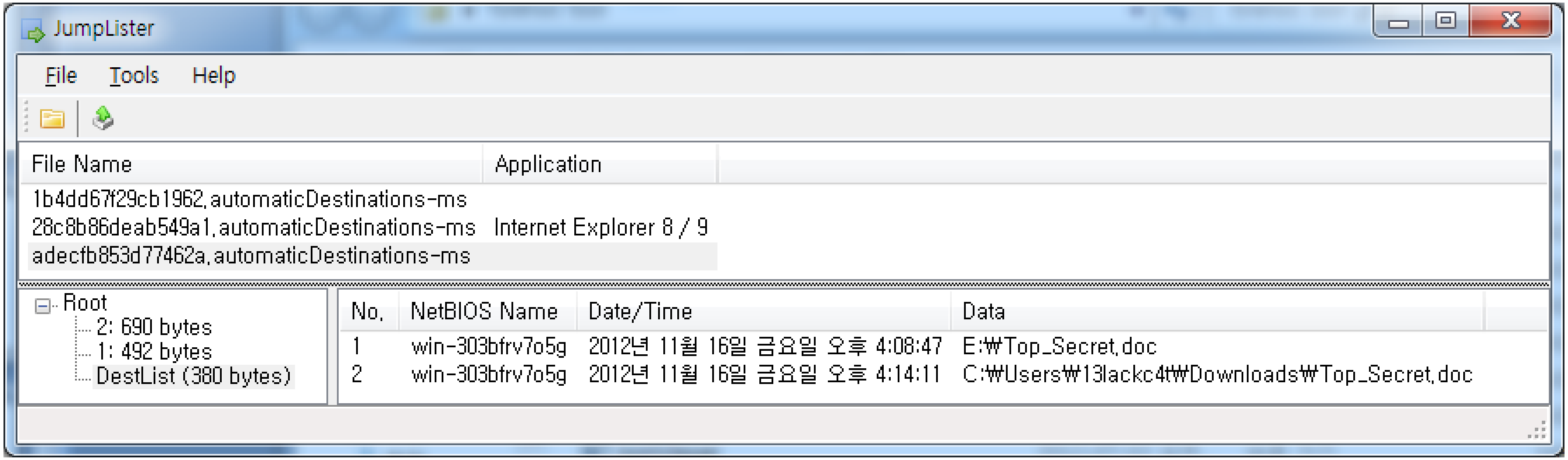
Explanation (4)

- Under "AppData₩Roaming₩Microsoft₩Windows₩Recent"
- AutomaticDestinations -> Jumplist
- CustomDestinations -> Jumplist



Explanation (5)

- Using Jumplister
- MS words file has same name different place



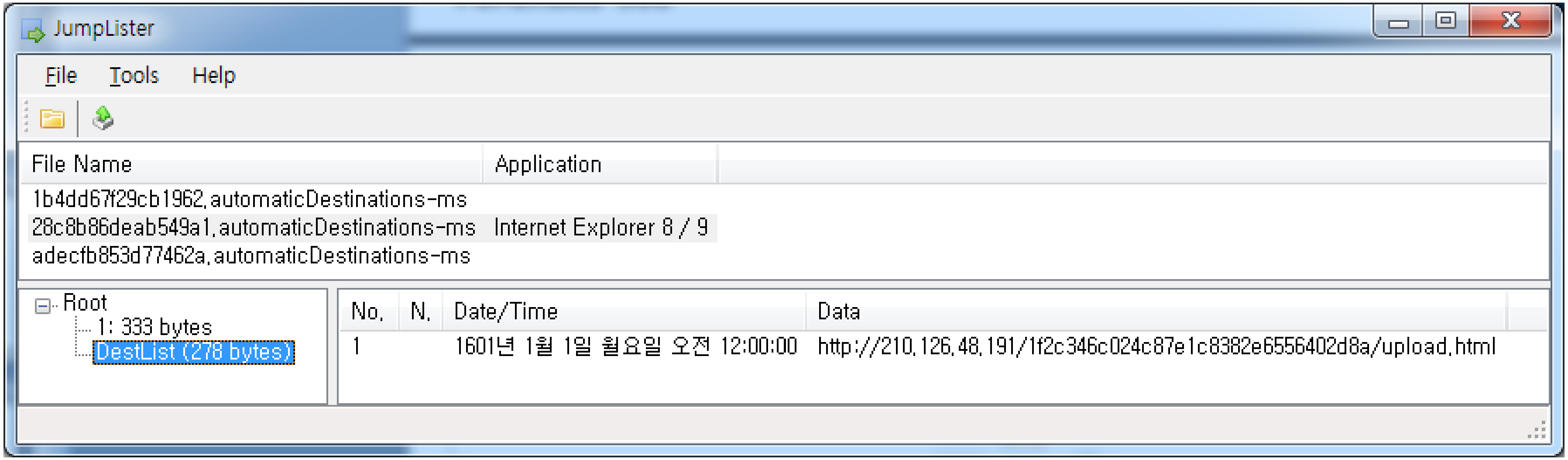
File Name	Application
1b4dd67f29cb1962.automaticDestinations-ms	
28c8b86deab549a1.automaticDestinations-ms	Internet Explorer 8 / 9
adecfb853d77462a.automaticDestinations-ms	

```
Root
  2: 690 bytes
  1: 492 bytes
  DestList (380 bytes)
```

No.	NetBIOS Name	Date/Time	Data
1	win-303bfrv7o5g	2012년 11월 16일 금요일 오후 4:08:47	E:₩Top_Secret.doc
2	win-303bfrv7o5g	2012년 11월 16일 금요일 오후 4:14:11	C:₩Users₩13lackc4t₩Downloads₩Top_Secret.doc

Explanation (6)

- Strange Date/Time -> pinned
- upload.html ?

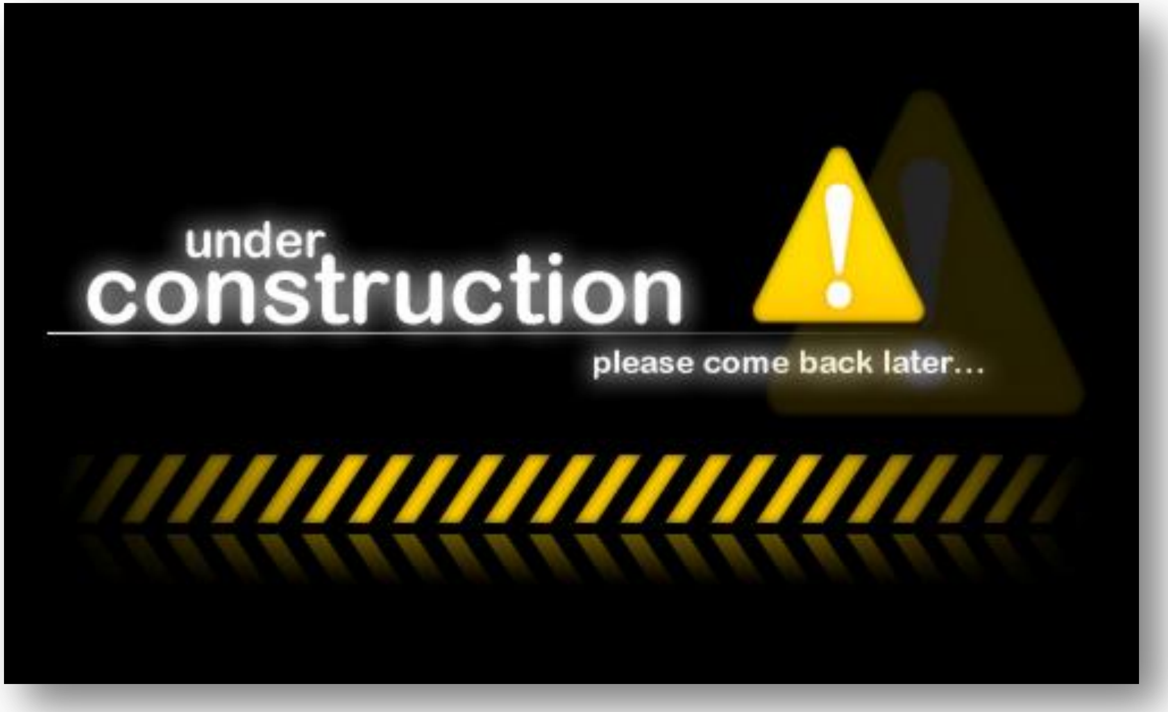


File Name	Application
1b4dd67f29cb1962.automaticDestinations-ms	
28c8b86deab549a1.automaticDestinations-ms	Internet Explorer 8 / 9
adecfb853d77462a.automaticDestinations-ms	

No.	N.	Date/Time	Data
1		1601년 1월 1일 월요일 오전 12:00:00	http://210.126.48.191/1f2c346c024c87e1c8382e6556402d8a/upload.html

Explanation (7)

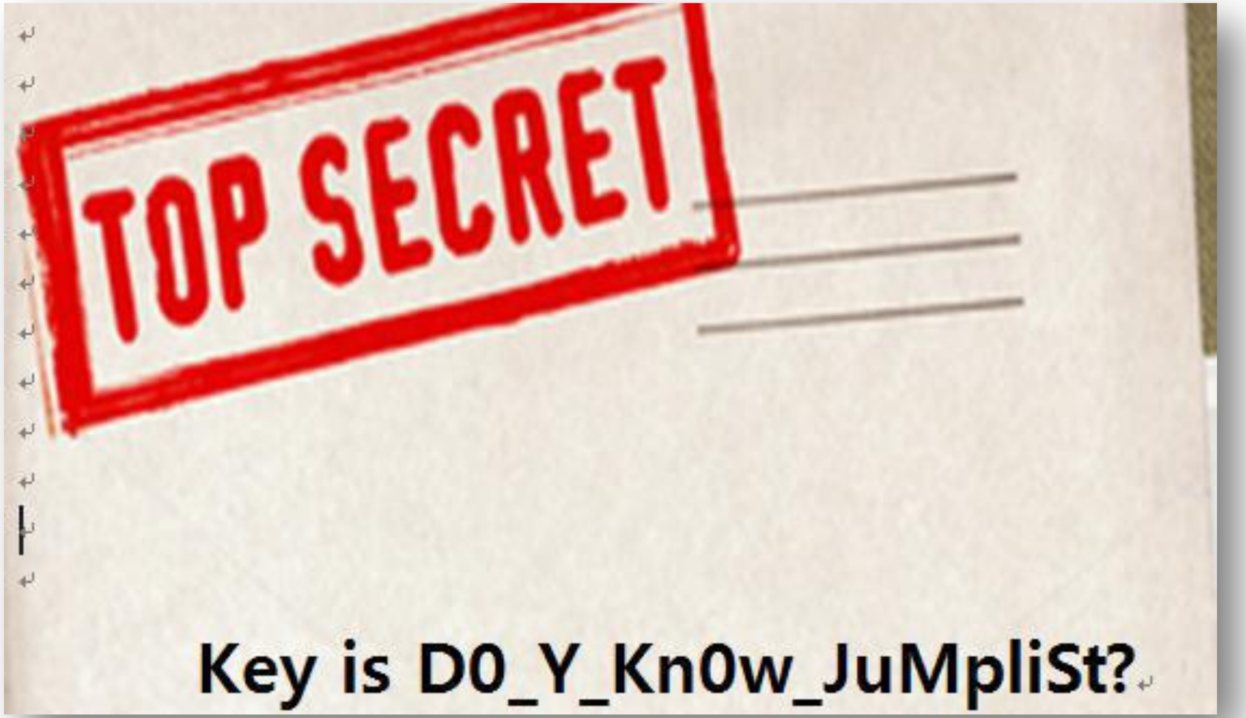
- Url -> Under construction



Explanation (8)

- Guess URL

  -> http://210.126.48.191/1f2c346c024c87e1c8382e6556402d8a/Top_Secret.doc



Key is D0_Y_Kn0w_JuMpliSt?

Behind

- Jumplist
- Using egrep
- Change Prob?

Forensics 400

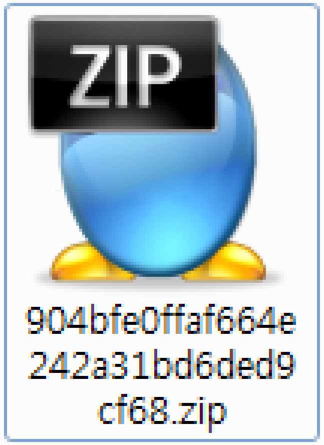
Forensics 400

Overview

- 국제공항의 항공기 관제시스템이 외부해커집단에 의해 침해당하여 Access키가 유출되었다는 신고를 접수했다.

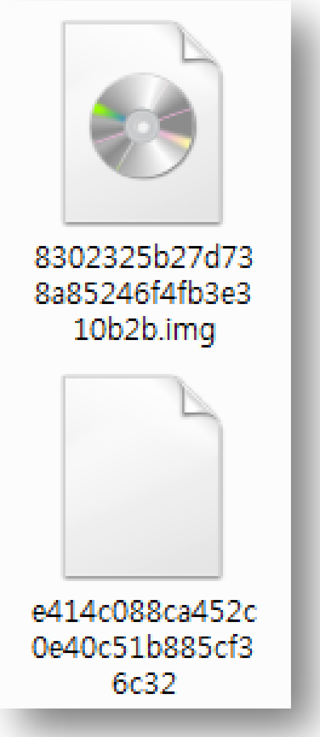
  역추적한 결과 공항 내 내부PC에서 해킹이 이루어졌다고 판단, 켜져있던 PC의 이미지 등을 입수했으며, 이 PC에서 Lucifer 라는 해커에게 Key를 전송한 것으로 보여진다.

  Key 를 찾아라.



904bfe0ffaf664e
242a31bd6ded9
cf68.zip

Explanation (1)



8302325b27d738a85246f4fb3e310b2b.img

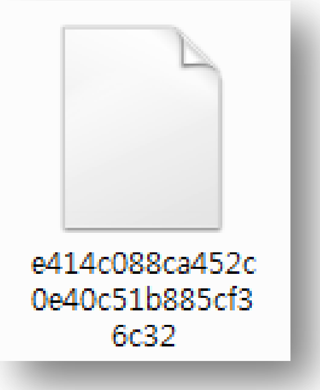
e414c088ca452c0e40c51b885cf36c32

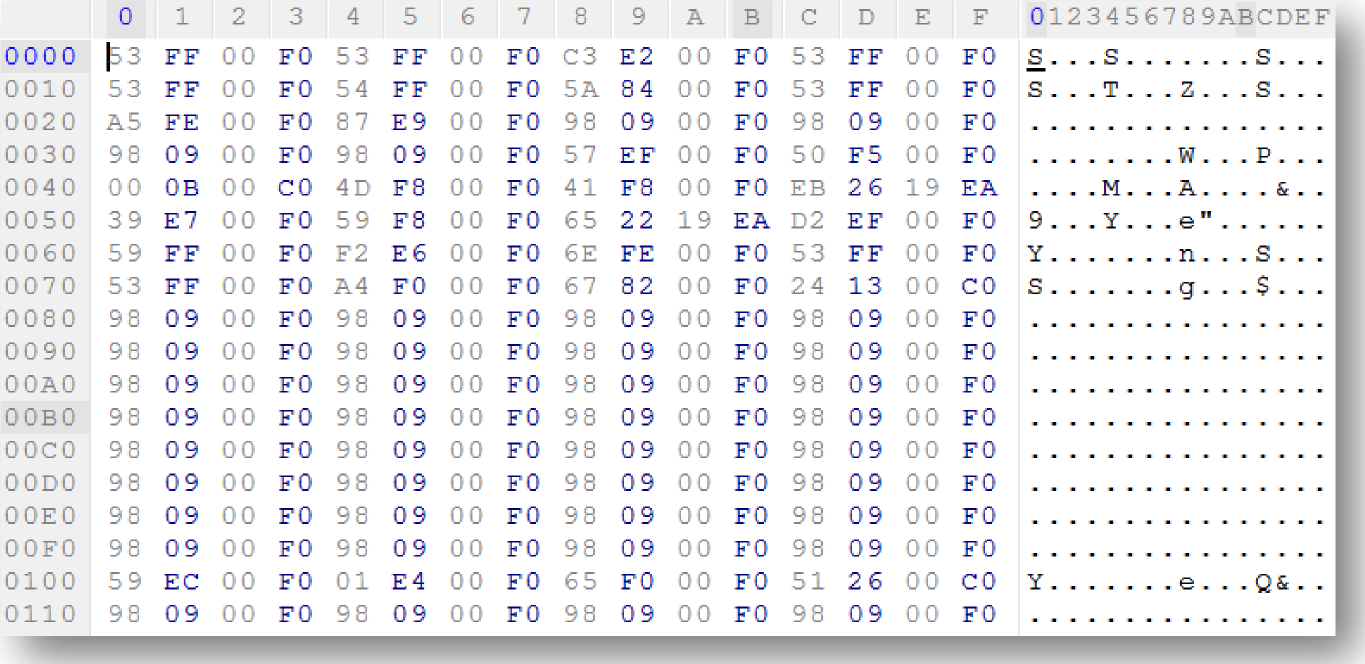
- Memory
- Disk

Forensics 400

Explanation (2)

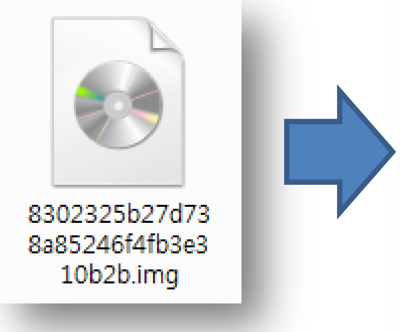
- Cannot indentify filesystem



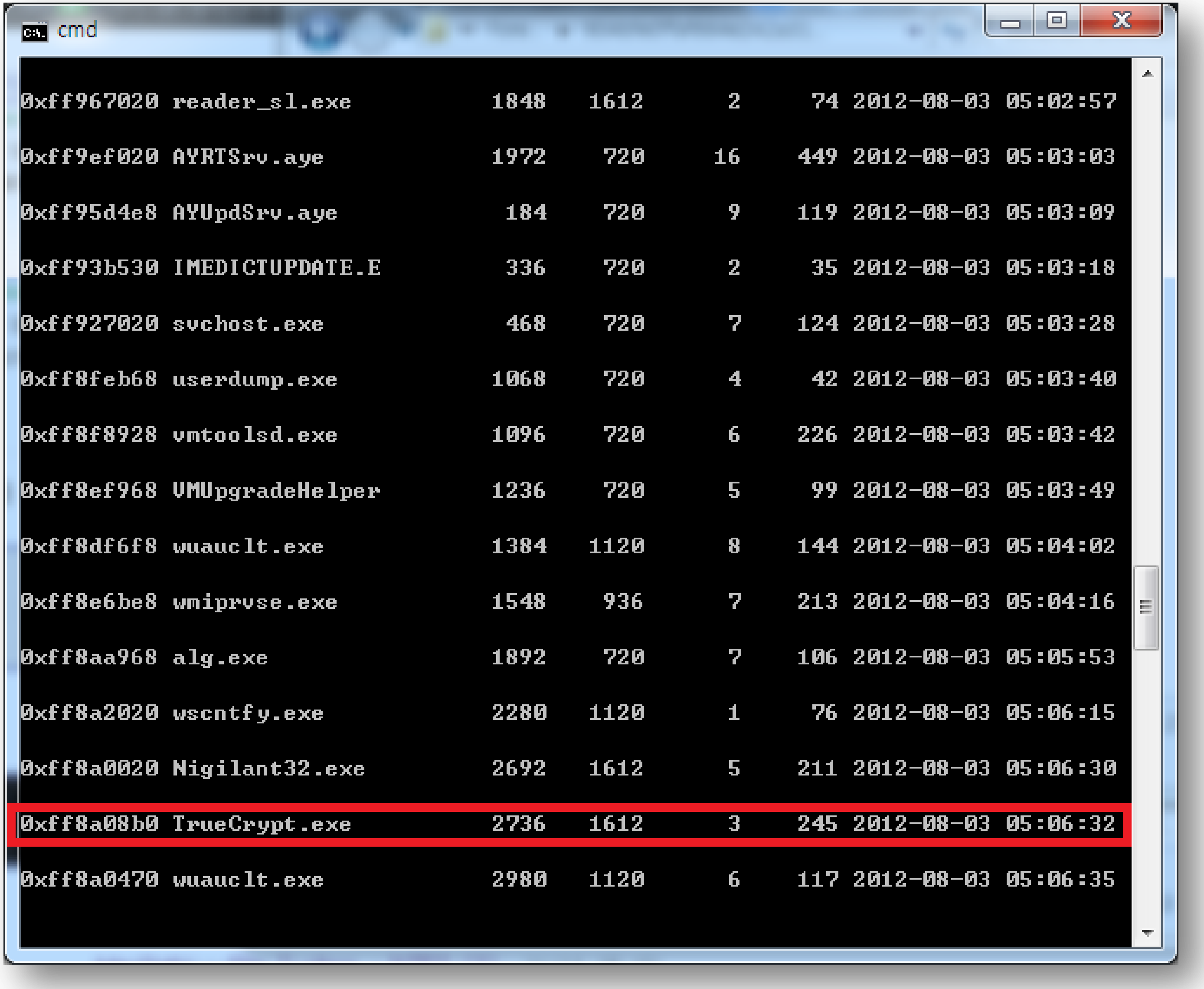


```
      0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000  53 FF 00 F0 53 FF 00 F0 C3 E2 00 F0 53 FF 00 F0  S...S.......S...
0010  53 FF 00 F0 54 FF 00 F0 5A 84 00 F0 53 FF 00 F0  S...T...Z...S...
0020  A5 FE 00 F0 87 E9 00 F0 98 09 00 F0 98 09 00 F0  ................
0030  98 09 00 F0 98 09 00 F0 57 EF 00 F0 50 F5 00 F0  ........W...P...
0040  00 0B 00 C0 4D F8 00 F0 41 F8 00 F0 EB 26 19 EA  ....M...A....&..
0050  39 E7 00 F0 59 F8 00 F0 65 22 19 EA D2 EF 00 F0  9...Y...e"......
0060  59 FF 00 F0 F2 E6 00 F0 6E FE 00 F0 53 FF 00 F0  Y.......n...S...
0070  53 FF 00 F0 A4 F0 00 F0 67 82 00 F0 24 13 00 C0  S.......g...$...
0080  98 09 00 F0 98 09 00 F0 98 09 00 F0 98 09 00 F0  ................
0090  98 09 00 F0 98 09 00 F0 98 09 00 F0 98 09 00 F0  ................
00A0  98 09 00 F0 98 09 00 F0 98 09 00 F0 98 09 00 F0  ................
00B0  98 09 00 F0 98 09 00 F0 98 09 00 F0 98 09 00 F0  ................
00C0  98 09 00 F0 98 09 00 F0 98 09 00 F0 98 09 00 F0  ................
00D0  98 09 00 F0 98 09 00 F0 98 09 00 F0 98 09 00 F0  ................
00E0  98 09 00 F0 98 09 00 F0 98 09 00 F0 98 09 00 F0  ................
00F0  98 09 00 F0 98 09 00 F0 98 09 00 F0 98 09 00 F0  ................
0100  59 EC 00 F0 01 E4 00 F0 65 F0 00 F0 51 26 00 C0  Y.......e...Q&..
0110  98 09 00 F0 98 09 00 F0 98 09 00 F0 98 09 00 F0  ................
```

Explanation (2)



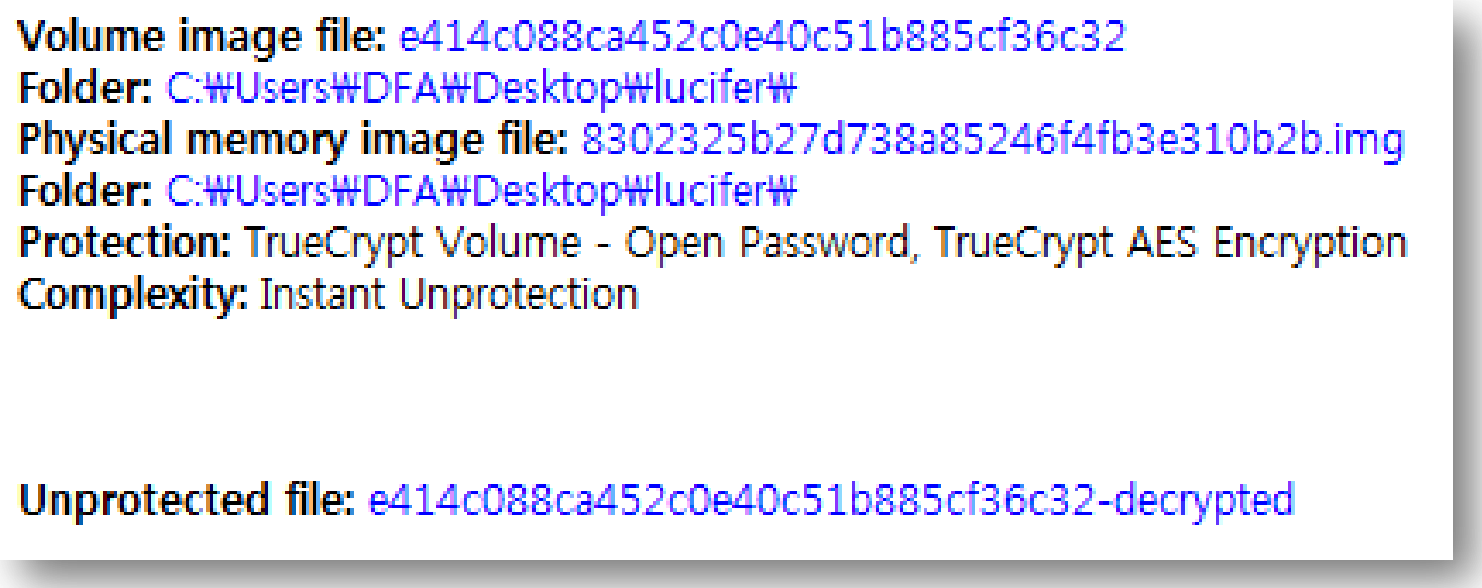
8302325b27d738a85246f4fb3e310b2b.img



```
0xff967020 reader_sl.exe          1848   1612      2      74 2012-08-03 05:02:57
0xff9ef020 AYRTSrv.aye            1972    720     16     449 2012-08-03 05:03:03
0xff95d4e8 AYUpdSrv.aye            184    720      9     119 2012-08-03 05:03:09
0xff93b530 IMEDICTUPDATE.E         336    720      2      35 2012-08-03 05:03:18
0xff927020 svchost.exe             468    720      7     124 2012-08-03 05:03:28
0xff8feb68 userdump.exe           1068    720      4      42 2012-08-03 05:03:40
0xff8f8928 vmtoolsd.exe           1096    720      6     226 2012-08-03 05:03:42
0xff8ef968 VMUpgradeHelper        1236    720      5      99 2012-08-03 05:03:49
0xff8df6f8 wuauclt.exe            1384   1120      8     144 2012-08-03 05:04:02
0xff8e6be8 wmiprvse.exe           1548    936      7     213 2012-08-03 05:04:16
0xff8aa968 alg.exe                1892    720      7     106 2012-08-03 05:05:53
0xff8a2020 wscntfy.exe            2280   1120      1      76 2012-08-03 05:06:15
0xff8a0020 Nigilant32.exe         2692   1612      5     211 2012-08-03 05:06:30
0xff8a08b0 TrueCrypt.exe          2736   1612      3     245 2012-08-03 05:06:32
0xff8a0470 wuauclt.exe            2980   1120      6     117 2012-08-03 05:06:35
```

Explanation (3)

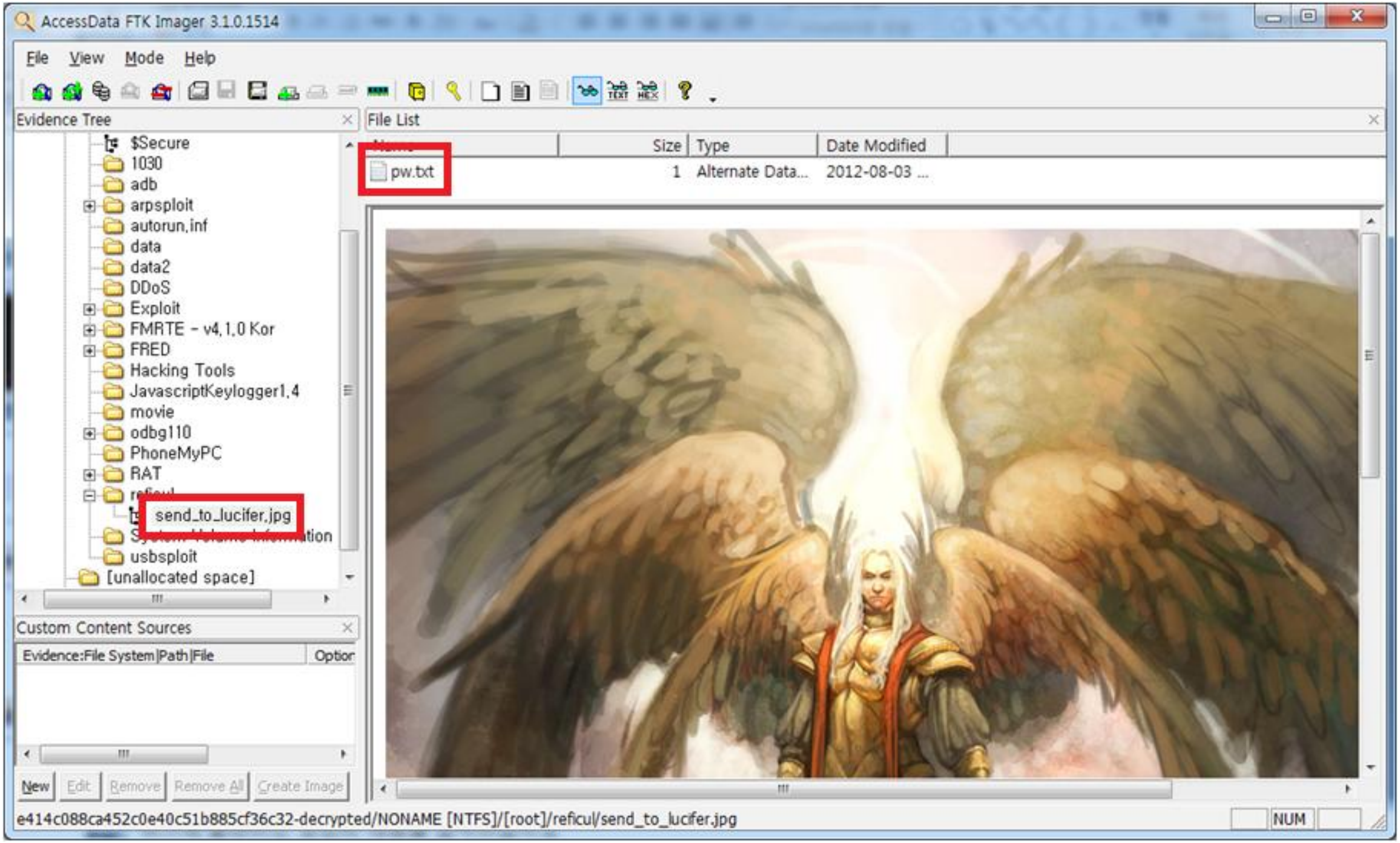
- Using Passware password recovery kit



Volume image file: e414c088ca452c0e40c51b885cf36c32
Folder: C:₩Users₩DFA₩Desktop₩lucifer₩
Physical memory image file: 8302325b27d738a85246f4fb3e310b2b.img
Folder: C:₩Users₩DFA₩Desktop₩lucifer₩
Protection: TrueCrypt Volume - Open Password, TrueCrypt AES Encryption
Complexity: Instant Unprotection

Unprotected file: e414c088ca452c0e40c51b885cf36c32-decrypted

Explanation (4)

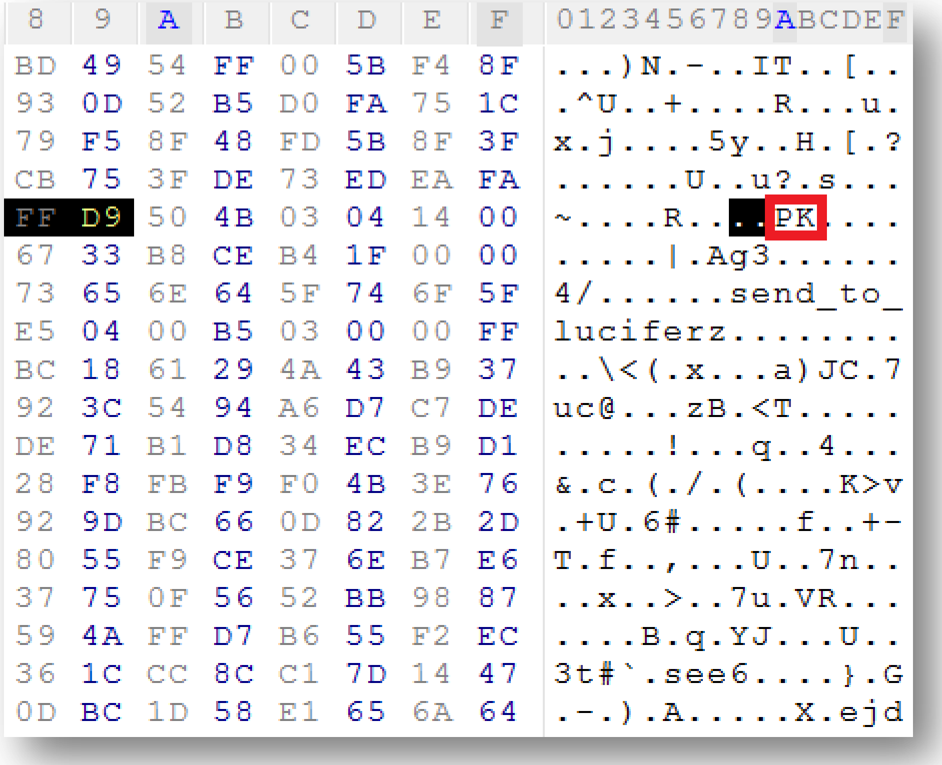


Name	Size	Type	Date Modified
pw.txt	1	Alternate Data...	2012-08-03 ...

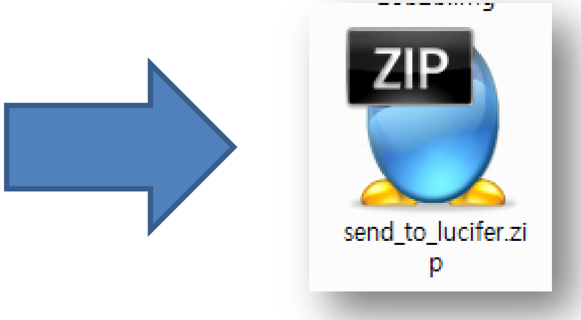
e414c088ca452c0e40c51b885cf36c32-decrypted/NONAME [NTFS]/[root]/reficul/send_to_lucifer.jpg

Explanation (5)

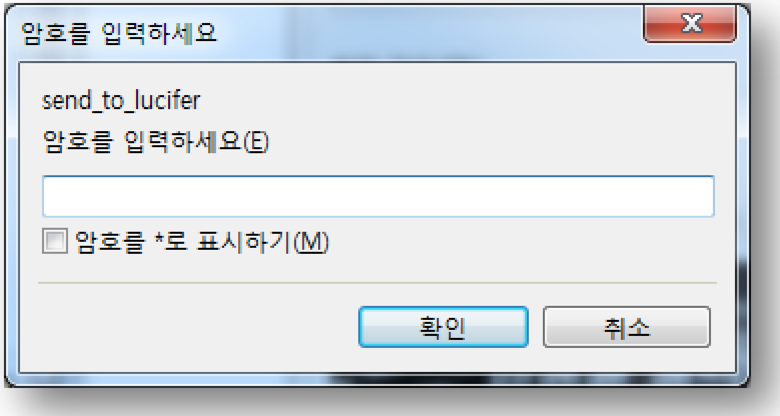
- Zip file in send_to_lucifer.jpg



```
 8  9  A  B  C  D  E  F   0123456789ABCDEF
BD 49 54 FF 00 5B F4 8F   ...)N.-..IT..[..
93 0D 52 B5 D0 FA 75 1C   .^U..+....R...u.
79 F5 8F 48 FD 5B 8F 3F   x.j....5y..H.[.?
CB 75 3F DE 73 ED EA FA   ......U..u?.s...
FF D9 50 4B 03 04 14 00   ~....R....PK....
67 33 B8 CE B4 1F 00 00   .....|.Ag3......
73 65 6E 64 5F 74 6F 5F   4/......send_to_
E5 04 00 B5 03 00 00 FF   luciferz........
BC 18 61 29 4A 43 B9 37   ..\<(.x...a)JC.7
92 3C 54 94 A6 D7 C7 DE   uc@...zB.<T.....
DE 71 B1 D8 34 EC B9 D1   ......!...q..4...
28 F8 FB F9 F0 4B 3E 76   &.c.(./.(....K>v
92 9D BC 66 0D 82 2B 2D   .+U.6#.....f..+-
80 55 F9 CE 37 6E B7 E6   T.f..,...U..7n..
37 75 0F 56 52 BB 98 87   ..x..>..7u.VR...
59 4A FF D7 B6 55 F2 EC   ....B.q.YJ...U..
36 1C CC 8C C1 7D 14 47   3t#`.see6....}.G
0D BC 1D 58 E1 65 6A 64   .-.).A.....X.ejd
```



Explanation (6)

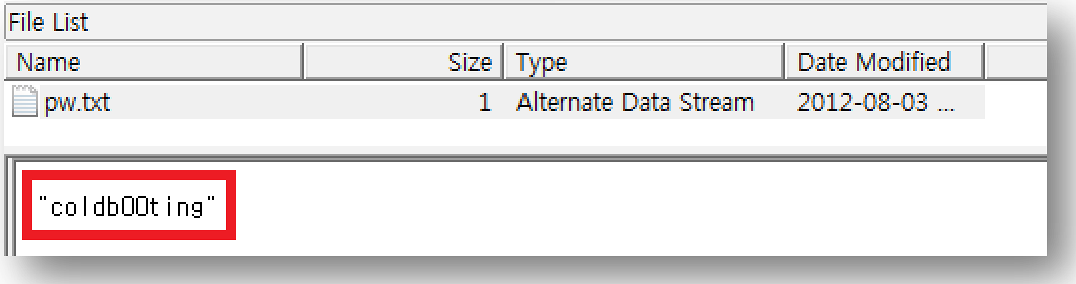


암호를 입력하세요

send_to_lucifer

암호를 입력하세요(E)

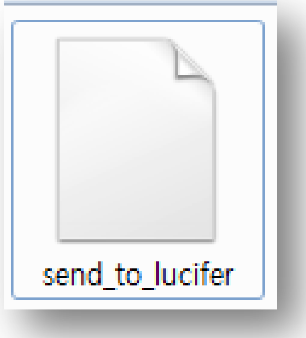
□ 암호를 *로 표시하기(M)



File List

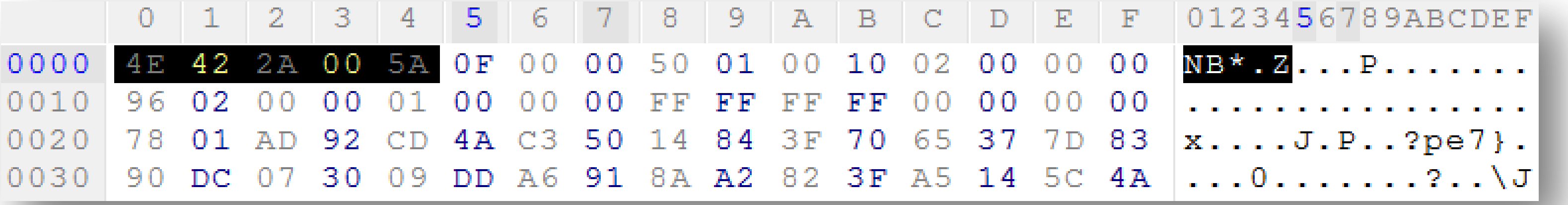
Name	Size	Type	Date Modified
pw.txt	1	Alternate Data Stream	2012-08-03 ...

"coldb00ting"

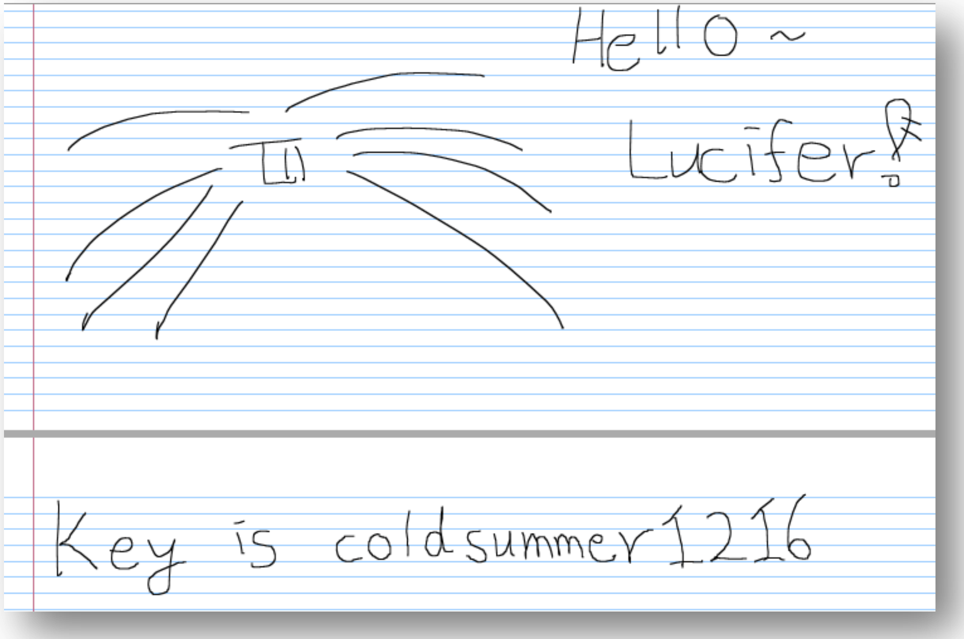


Explanation (7)

- Send_to_lucifer is Windows journal file(*.jnt)



```
      0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
0000  4E 42 2A 00 5A 0F 00 00 50 01 00 10 02 00 00 00  NB*.Z...P.......
0010  96 02 00 00 01 00 00 00 FF FF FF FF 00 00 00 00  ................
0020  78 01 AD 92 CD 4A C3 50 14 84 3F 70 65 37 7D 83  x....J.P..?pe7}.
0030  90 DC 07 30 09 DD A6 91 8A A2 82 3F A5 14 5C 4A  ...0.......?..\J
```



Hello ~

Lucifer!

Key is coldsummer1216

Behind

- Coldbooting Attack

Question and Answer