



2019 i-Keeper Hacking Festival

[SNOW_BALL]

상금은_토스로팀 강민송(비송실세)

Write-up

2019-11-27



Notice

본 보고서는 2019 년 2 학기 i-Keeper Hacking Festival 에 출제된 문제 풀이 방법을 기술한 보고서입니다.

본 보고서의 내용은 저작권법에 의하여 보호받는 저작물로 그 저작권은 문제 출제자에게 있음을 알립니다. 따라서 보고서의 내용을 무단 복제 및 배포는 원칙적으로 금지합니다.

본 보고서를 외부에 유출하거나 무단으로 사용하였을 경우에는 관련 규정에 따른 처벌을 받게 됩니다.

목 차

1. 문제 정보	4
1.1 문제 이름	4
1.2 문제 기술	4
1.3 문제 분야	4
1.4 문제 의도	4
1.5 문제 힌트 및 주의사항	4
1.6 문제 정답	4
 2. 풀이 방법	 5
2.1 필요 기술	5
2.1 상세 풀이	5

1. 문제 정보

1.1 문제 이름

SNOW_BALL

1.2 문제 기술

헤진이는 수많은 포렌식 툴 때문에 언제나 용량부족에 시달린다.

중요한 자료가 있는데 용량을 함부로 삭제할 수가 없다고 한다.

플래그 값을 찾아주자!

1.3 문제 분야

④ Forensics

1.4 문제 의도

용량의 중요성...

1.5 문제 힌트 및 주의사항

힌트없음!!!! ㅎㅎ

1.6 문제 정답

iKeeper{i_just_want_to_join_god_Google!!!!}

2. 풀이 방법

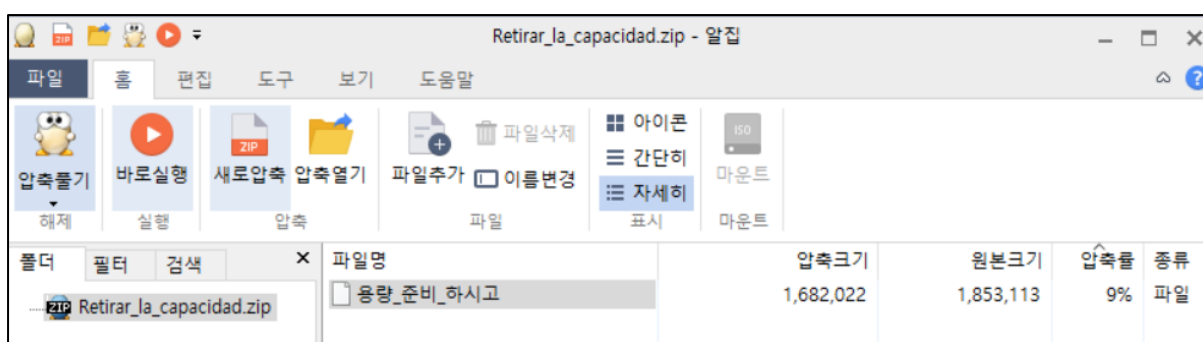
2.1 필요 기술

Strings.exe 툴 사용법

CRC 값의 이해

파일 시그니처 확인

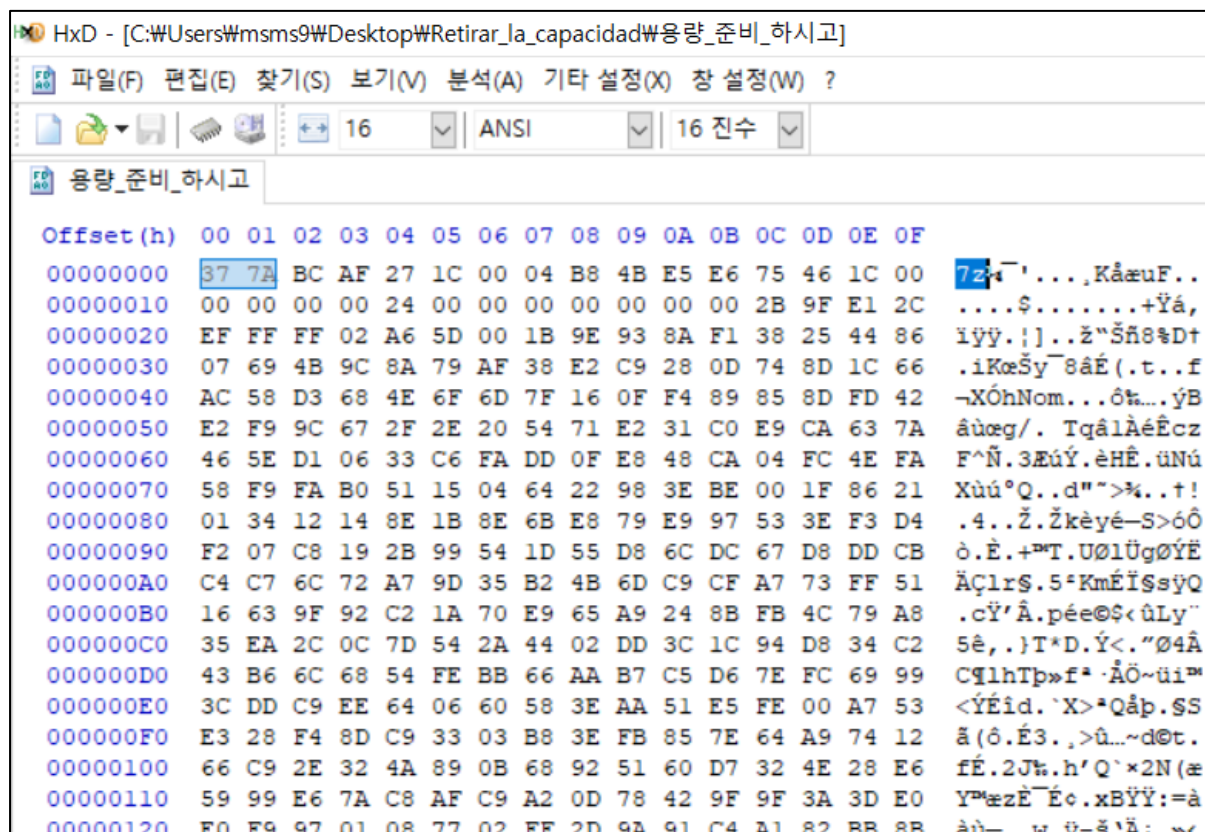
2.2 상세 풀이



[그림 1 - 문제 확인]

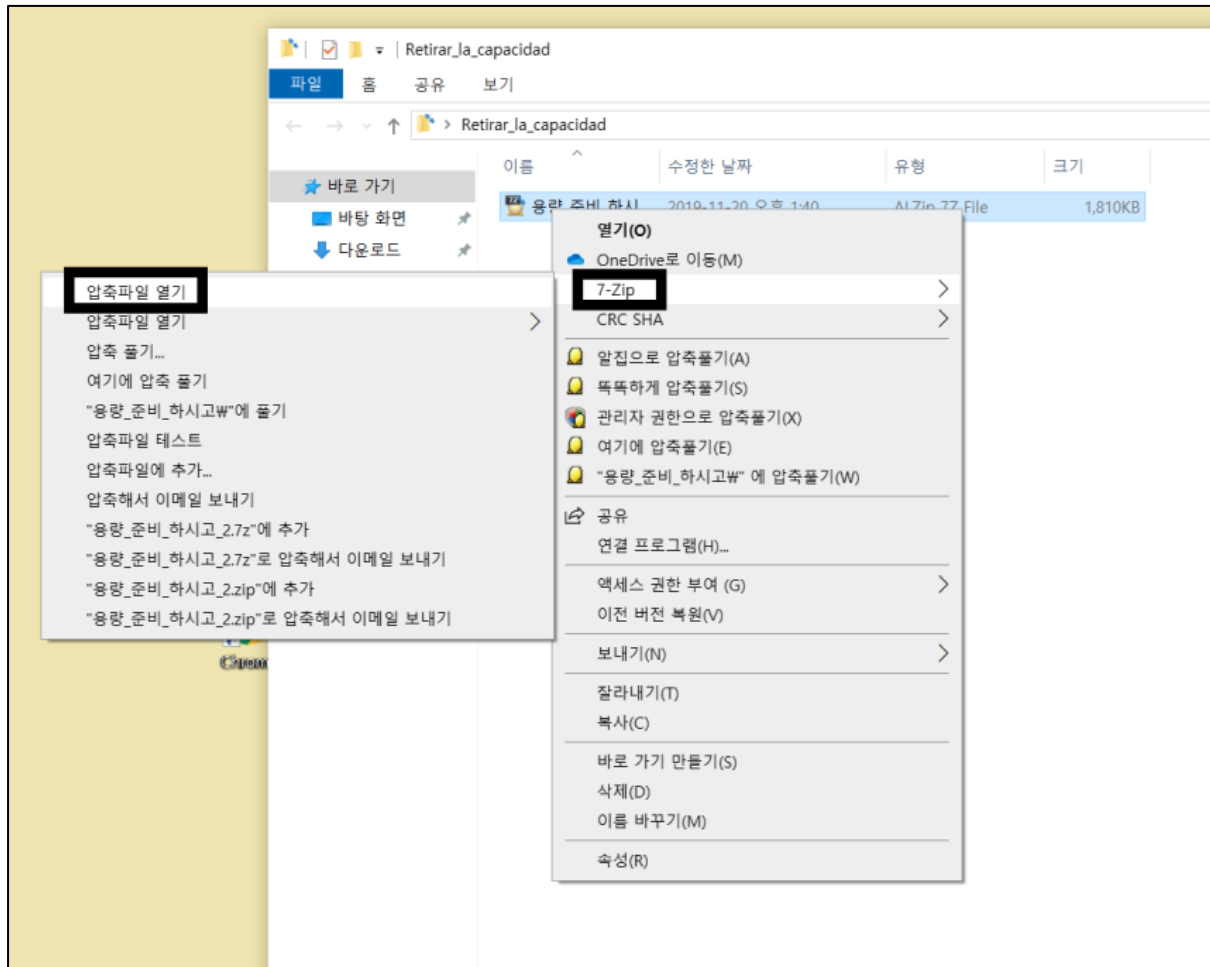
첫 문제화면은 압축 해제로 시작된다.

용량을 풀면, 확장자가 없는 파일이 있다.



[그림 2 - 문제파일 HxD 확인]

“용량_준비_하시고” 파일의 hex 를 확인하니 확장자가 7z 임을 확인 할 수 있었다.



[그림 3 - 문제 파일 확인]

확장자를 7z 으로 변경해준 뒤, 파일을 우측 클릭하여 7-zip 의 압축파일 열기를 클릭한다.

이름	크기	CRC	압축된 크기	속...	암호화	압축 방식
46.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
47.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
48.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
49.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
50.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
51.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
52.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
53.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
54.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
55.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
56.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
57.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
58.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
59.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
60.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
61.7z	13 148 522	CEFEBCBA	303 230	AC	-	LZMA2:24
62.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
63.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
64.7z	13 166 380	BF34AEA1	86 850	AC	-	LZMA2:24
65.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
66.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
67.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
68.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
69.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
70.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
71.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
72.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
73.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
74.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
75.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
76.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
77.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
78.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
79.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24
80.7z	13 148 522	CEFEBCBA		AC	-	LZMA2:24

[그림 4 - 문제 파일 목록]

7-zip 으로 연 파일의 목록을 살펴보던 중, 유일하게 CRC 값이 다른 파일이 하나 존재함을 발견하였다.

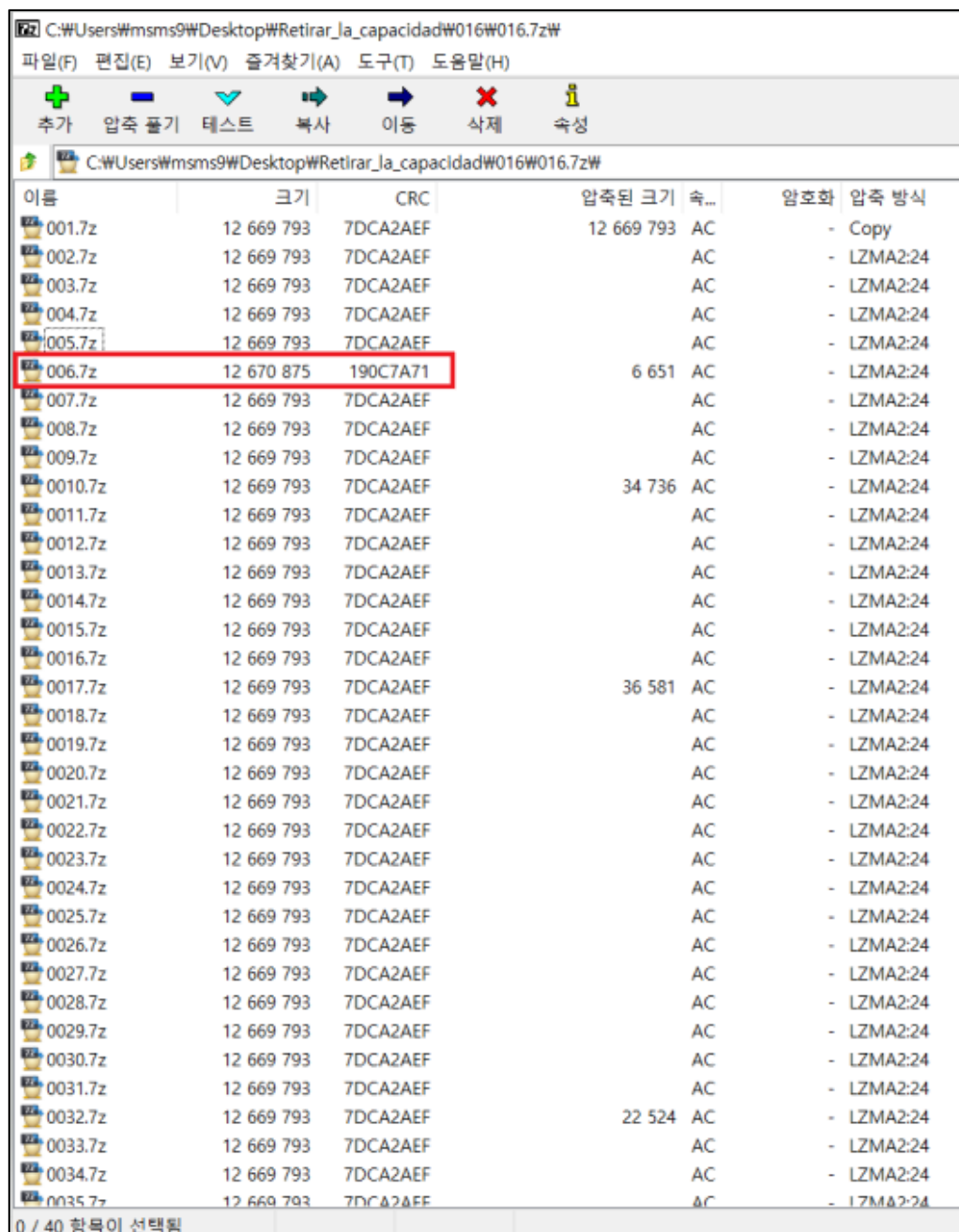
64.7z 파일의 압축을 푼다.

이름	크기	CRC	압축된 크기	속...	암호화	압축 방식	블록	폴더
044.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	6	
045.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	6	
046.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	6	
047.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	6	
048.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	6	
049.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	6	
050.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	6	
051.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	6	
052.7z	12 770 582	F921495C	19 690	AC	-	LZMA2:24	8	
053.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	6	
054.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	6	
055.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	6	
056.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	6	
057.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	6	
058.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	6	
059.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	6	
060.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	6	
061.7z	12 768 692	6D6FD1D3	88 902	AC	-	LZMA2:24	7	
062.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	7	
063.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	7	
064.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	7	
065.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	7	
066.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	7	
067.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	7	
068.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	7	
069.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	7	
070.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	7	
071.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	7	
072.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	7	
073.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	7	
074.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	7	
075.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	7	
076.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	7	
077.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	7	
078.7z	12 768 692	6D6FD1D3		AC	-	LZMA2:24	7	

[그림 5 - 64.7z 파일 목록]

64.7z 압축파일의 목록을 확인하던 중에, 또 다시 CRC 값이 다른 파일을 발견하였다.

052.7z 파일의 압축을 해제해준다.

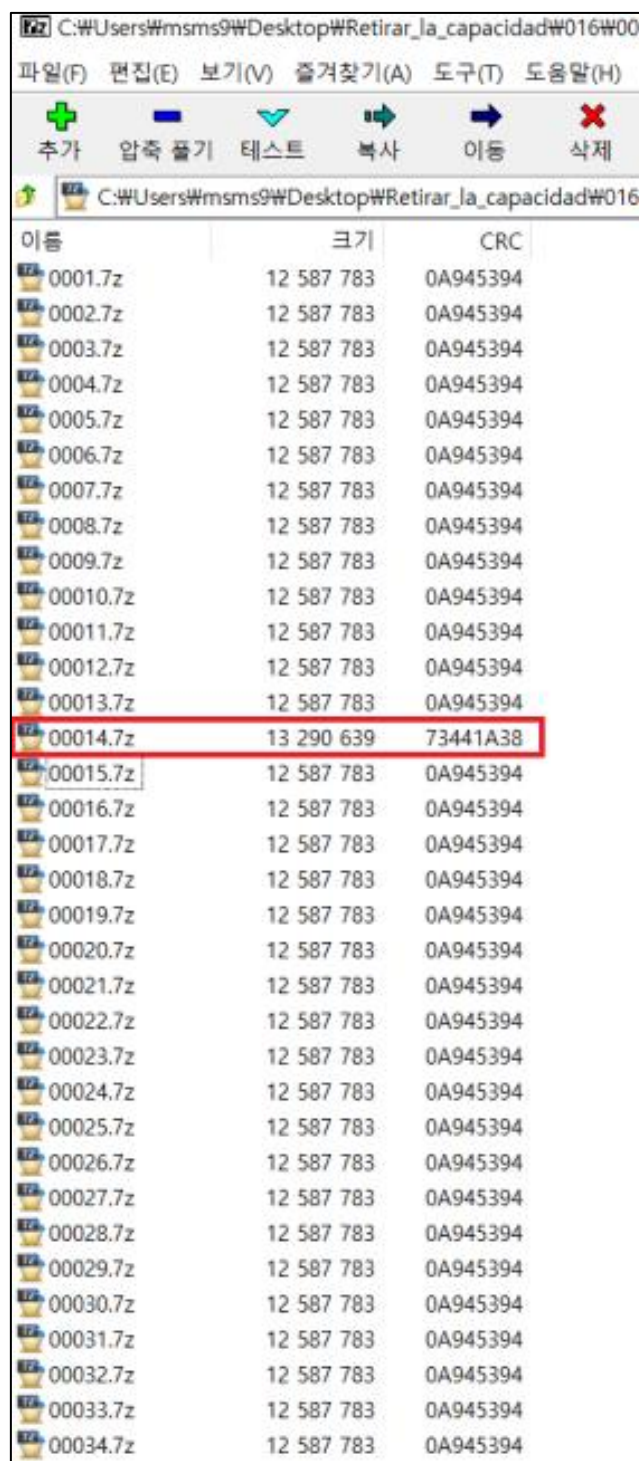


이름	크기	CRC	압축된 크기	속...	암호화	압축 방식
001.7z	12 669 793	7DCA2AEF	12 669 793	AC	-	Copy
002.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
003.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
004.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
005.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
006.7z	12 670 875	190C7A71	6 651	AC	-	LZMA2:24
007.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
008.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
009.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
0010.7z	12 669 793	7DCA2AEF	34 736	AC	-	LZMA2:24
0011.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
0012.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
0013.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
0014.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
0015.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
0016.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
0017.7z	12 669 793	7DCA2AEF	36 581	AC	-	LZMA2:24
0018.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
0019.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
0020.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
0021.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
0022.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
0023.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
0024.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
0025.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
0026.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
0027.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
0028.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
0029.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
0030.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
0031.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
0032.7z	12 669 793	7DCA2AEF	22 524	AC	-	LZMA2:24
0033.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
0034.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24
0035.7z	12 669 793	7DCA2AEF		AC	-	LZMA2:24

[그림 6 - 052.7z 파일 목록]

052.7z 압축파일의 목록을 확인하던 중에, 또 다시 CRC 값이 다른 파일을 발견하였다.

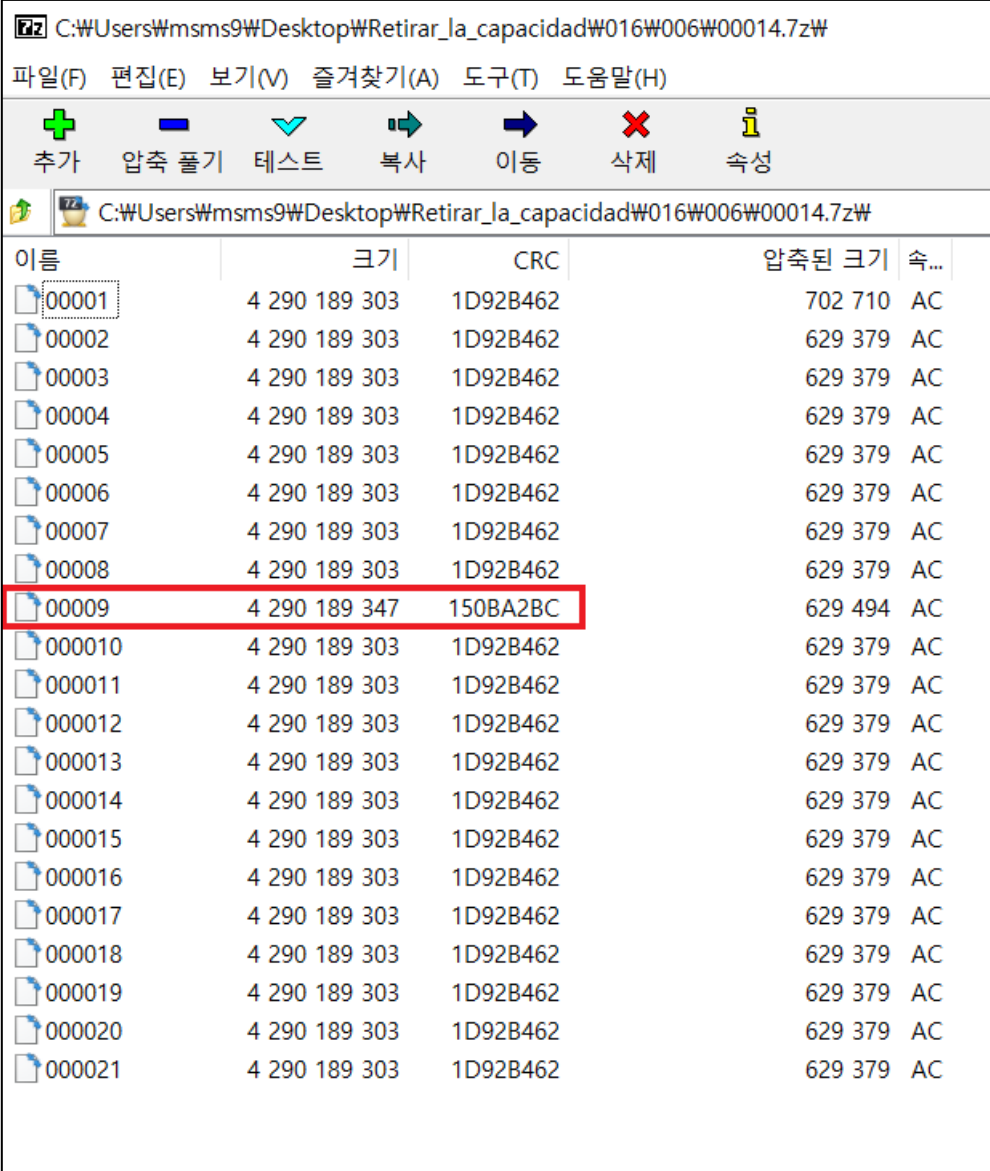
006.7z 파일의 압축을 해제해준다.



이름	크기	CRC
0001.7z	12 587 783	0A945394
0002.7z	12 587 783	0A945394
0003.7z	12 587 783	0A945394
0004.7z	12 587 783	0A945394
0005.7z	12 587 783	0A945394
0006.7z	12 587 783	0A945394
0007.7z	12 587 783	0A945394
0008.7z	12 587 783	0A945394
0009.7z	12 587 783	0A945394
00010.7z	12 587 783	0A945394
00011.7z	12 587 783	0A945394
00012.7z	12 587 783	0A945394
00013.7z	12 587 783	0A945394
00014.7z	13 290 639	73441A38
00015.7z	12 587 783	0A945394
00016.7z	12 587 783	0A945394
00017.7z	12 587 783	0A945394
00018.7z	12 587 783	0A945394
00019.7z	12 587 783	0A945394
00020.7z	12 587 783	0A945394
00021.7z	12 587 783	0A945394
00022.7z	12 587 783	0A945394
00023.7z	12 587 783	0A945394
00024.7z	12 587 783	0A945394
00025.7z	12 587 783	0A945394
00026.7z	12 587 783	0A945394
00027.7z	12 587 783	0A945394
00028.7z	12 587 783	0A945394
00029.7z	12 587 783	0A945394
00030.7z	12 587 783	0A945394
00031.7z	12 587 783	0A945394
00032.7z	12 587 783	0A945394
00033.7z	12 587 783	0A945394
00034.7z	12 587 783	0A945394

[그림 7 - 006.7z 파일 목록]

006.7z 압축파일의 목록 중, CRC 값이 다른 파일을 발견하였다면,
00014.7z 파일의 압축을 해제해준다.

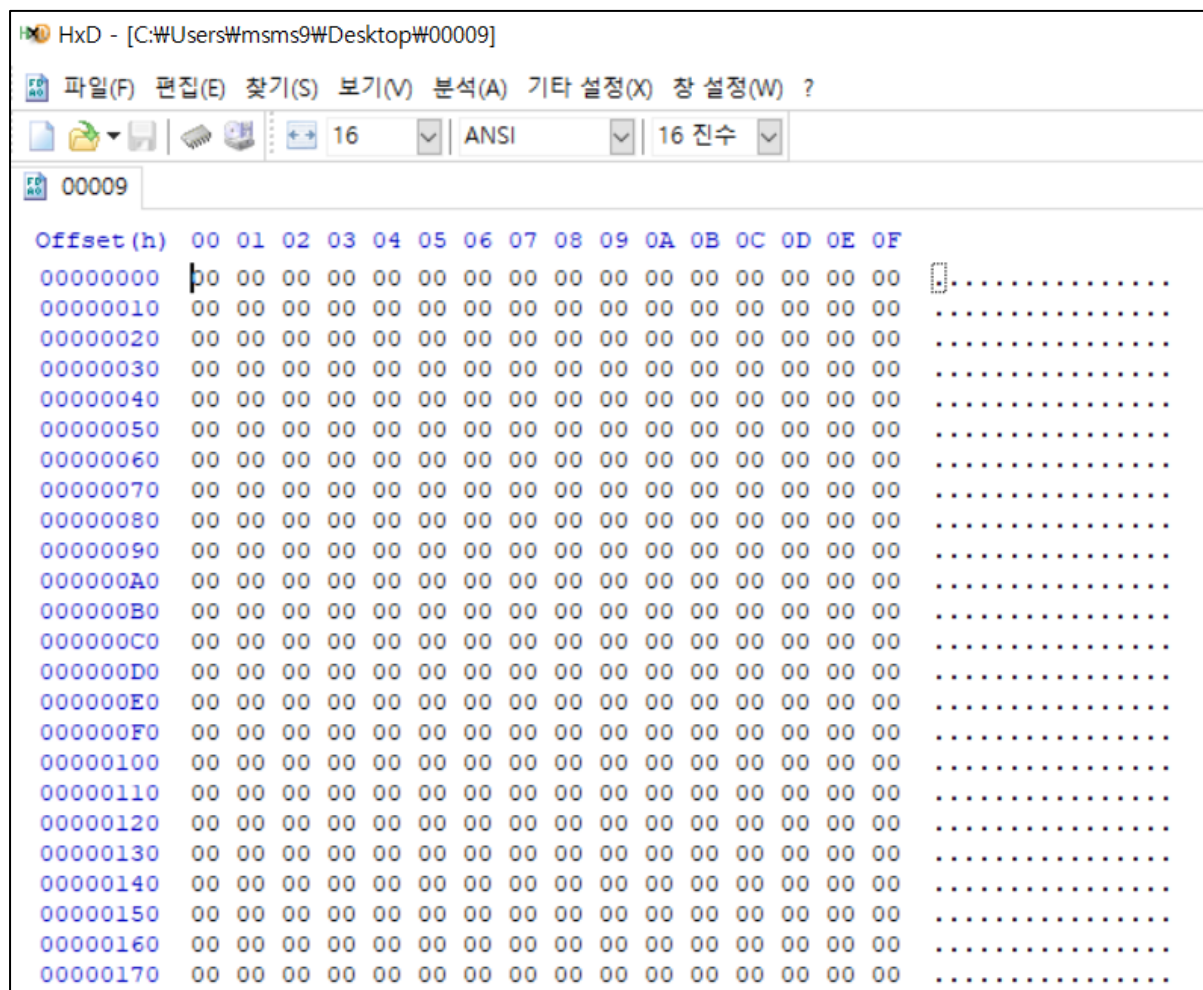


이름	크기	CRC	압축된 크기	속...
00001	4 290 189 303	1D92B462	702 710	AC
00002	4 290 189 303	1D92B462	629 379	AC
00003	4 290 189 303	1D92B462	629 379	AC
00004	4 290 189 303	1D92B462	629 379	AC
00005	4 290 189 303	1D92B462	629 379	AC
00006	4 290 189 303	1D92B462	629 379	AC
00007	4 290 189 303	1D92B462	629 379	AC
00008	4 290 189 303	1D92B462	629 379	AC
00009	4 290 189 347	150BA2BC	629 494	AC
000010	4 290 189 303	1D92B462	629 379	AC
000011	4 290 189 303	1D92B462	629 379	AC
000012	4 290 189 303	1D92B462	629 379	AC
000013	4 290 189 303	1D92B462	629 379	AC
000014	4 290 189 303	1D92B462	629 379	AC
000015	4 290 189 303	1D92B462	629 379	AC
000016	4 290 189 303	1D92B462	629 379	AC
000017	4 290 189 303	1D92B462	629 379	AC
000018	4 290 189 303	1D92B462	629 379	AC
000019	4 290 189 303	1D92B462	629 379	AC
000020	4 290 189 303	1D92B462	629 379	AC
000021	4 290 189 303	1D92B462	629 379	AC

[그림 8 - 00014.7z 파일 목록]

00014.7z 파일의 목록 중에 CRC 값이 다른 00009 파일을 확인하였다.

이 파일을 추출하여 HxD 툴로 확인해보자.



[그림 9 - 00009 파일 HxD 확인]

파일이 전부 0으로 가득 차 있다.

확장자 역시 확인 할 수 없는 상황임으로 안에 키 값의 포맷을 검색해 보자.

06483390	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
064833A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
064833B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
064833C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
064833D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
064833E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
064833F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
06483400	00 00 00 00 69 4B 65 65 00 00 00 00 00 00 00 00	...iKee.....
06483410	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
06483420	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
06483430	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
06483440	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
06483450	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
06483460	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

[그림 10 - key format 발견]

Key 의 포맷이 검색되었다.

하지만 일부만이 검색되는 것을 보아하니 키 값이 파일 안에 있음을 짐작할 수 있다.

Strings.exe 을 사용하여 문자열을 뽑아내보자.

```

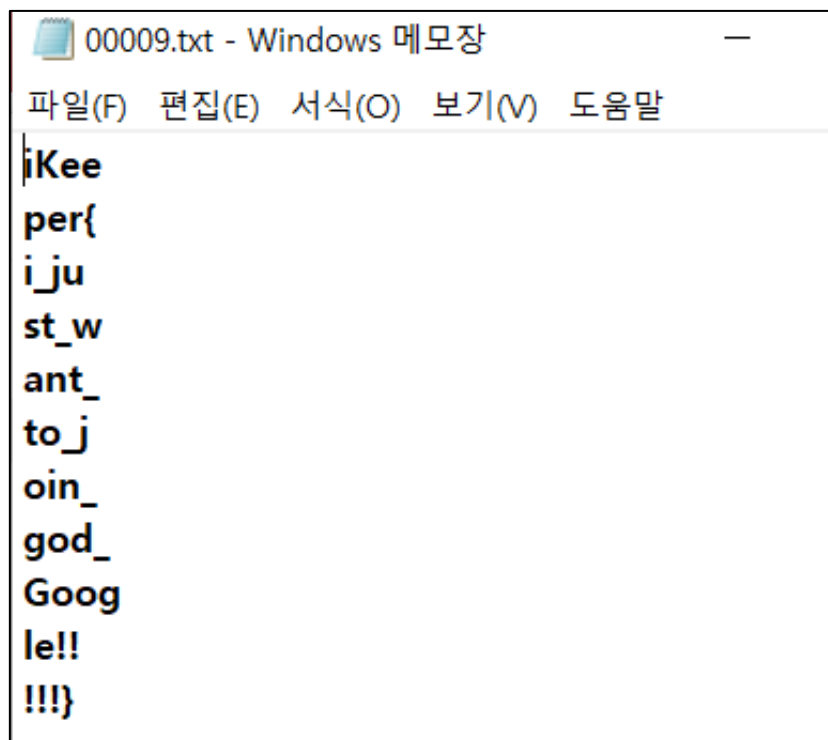
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.18362.476]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\msms9\Desktop\문제 풀이\Retirar_la_capacidad>strings.exe 00009 >> 00009.txt
C:\Users\msms9\Desktop\문제 풀이\Retirar_la_capacidad>

```

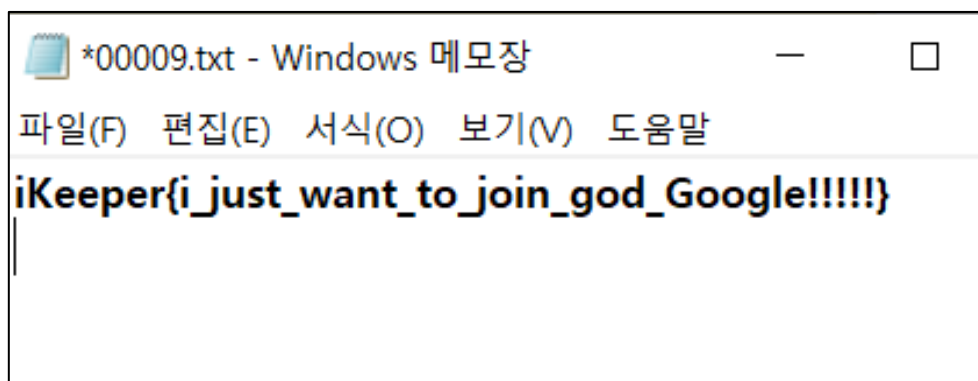
[그림 11 - Key 값 추출]

00009 파일의 string 을 .txt 파일로 뽑아낸다.



[그림 13 - 00009.txt]

문자열이 추출되었다.



[그림 13 - 00009.txt]

Flag 는 iKeeper{i_just_want_to_god_Google!!!!} 이다.