

Alternate Data Stream

이경식

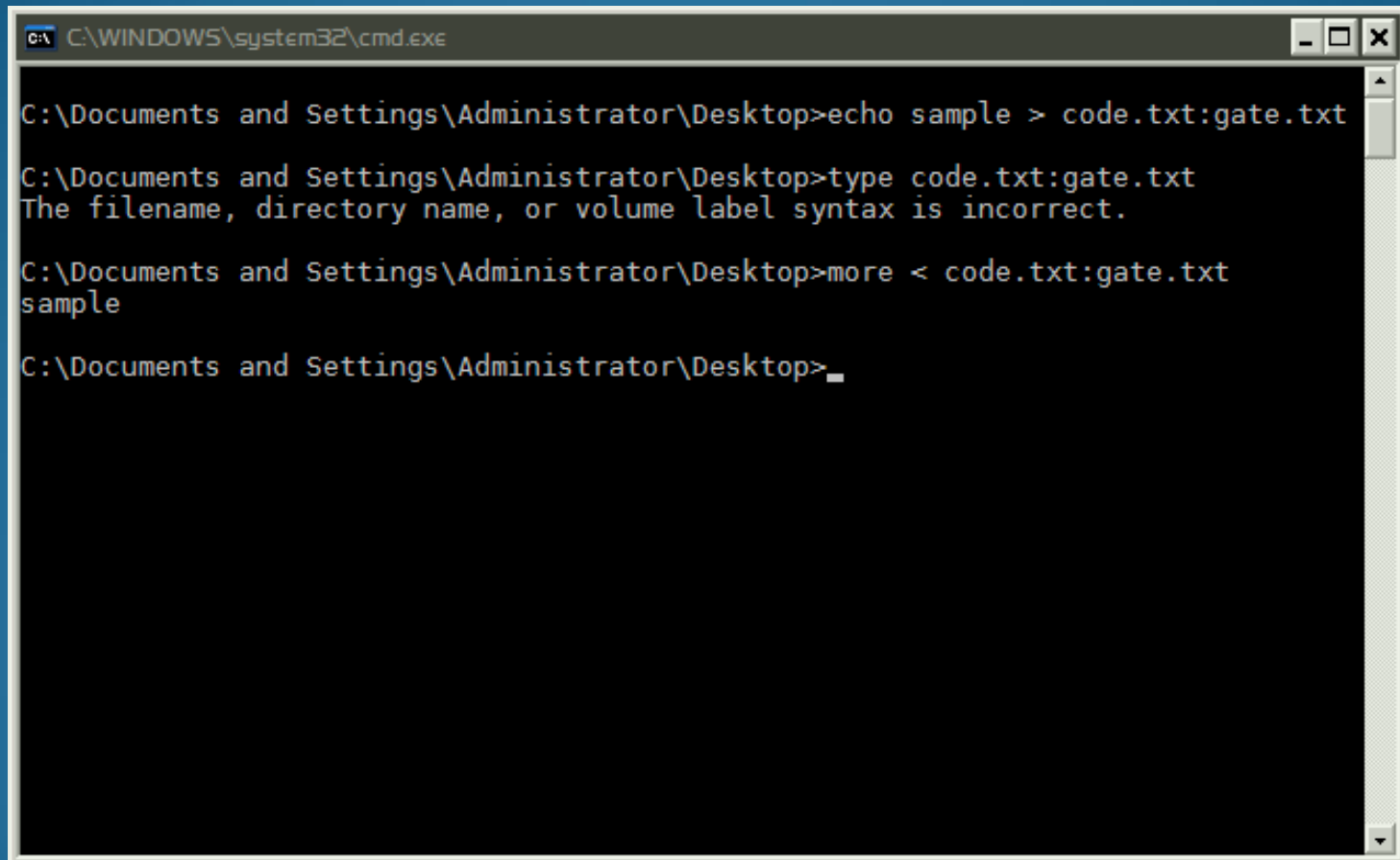
목차

- ADS?
- ADS생성, 내용보기
- \$DATA
- 실험
- Streams.exe

ADS?

- NTFS상의 데이터 속성(\$DATA)은 여러 개 올 수 있음
- 하나 외에 추가적으로 존재하는 \$DATA속성을 말함
- ADS는 Attr Type ID을 필요로 함.
 - 요소가 0xFFFFFFFF로 설정된 경우,
 - WinHex, Encase는 해당 내용이 삭제된 것으로 처리

ADS 생성, 내용보기



```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrator\Desktop>echo sample > code.txt:gate.txt

C:\Documents and Settings\Administrator\Desktop>type code.txt:gate.txt
The filename, directory name, or volume label syntax is incorrect.

C:\Documents and Settings\Administrator\Desktop>more < code.txt:gate.txt
sample

C:\Documents and Settings\Administrator\Desktop>_
```

\$DATA(ADS)

첫 번째 \$DATA의 크기

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
142B1900	2E	00	74	00	78	00	74	00	80	00	00	00	28	00	00	00	. t x t (
142B1910	00	00	18	00	00	00	01	00	0C	00	00	00	18	00	00	00	
142B1920	77	74	66	21	21	21	20	58	28	20	0D	0A	00	00	00	00	wtf!!! X(
142B1930	80	00	00	00	80	00	00	00	00	0C	18	00	00	00	03	00	
142B1940	4F	00	00	00	30	00	00	00	70	00	61	00	73	00	73	00	0 p a s s
142B1950	77	00	6F	00	72	00	64	00	2E	00	74	00	78	00	74	00	w o r d . t x t
142B1960	70	61	73	73	77	6F	72	64	20	69	73	20	61	61	31	31	password is aa11
142B1970	31	38	36	61	62	64	65	33	66	65	34	63	39	64	66	39	186abde3fe4c9df9
142B1980	63	35	64	62	34	66	65	65	36	37	35	37	37	35	65	38	c5db4fee675775e8
142B1990	35	37	64	61	34	36	64	34	35	62	39	64	37	32	34	63	57da46d45b9d724c
142B19A0	37	63	36	64	32	64	66	37	38	63	37	66	20	0D	0A	00	7c6d2df78c7f

두 번째 \$DATA의 크기

					Attr Type ID	Len of Attr		
Non-Res Flag	Len of Name	Offset to Name	Flags	Attr ID	Size of Content	Offset of Cont	Index Flag	Padding

\$DATA(ADS)

Offset Of Cont와 Size Of Contents는
실제 파일 내용의 크기와 Offset을
가짐

Offset Of Cont

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
142B1900	2E	00	74	00	78	00	74	00	80	00	00	00	28	00	00	00	. t x t (
142B1910	00	00	18	00	00	00	01	00	0C	00	00	00	18	00	00	00	
142B1920	77	74	66	21	21	21	20	58	28	20	0D	0A	00	00	00	00	wtf!!! X(
142B1930	80	00	00	00	80	00	00	00	00	0C	18	00	00	00	03	00	
142B1940	4F	00	00	00	30	00	00	00	70	00	61	00	73	00	73	00	0 pass
142B1950	77	00	6F	00	72	00	64	00	2E	00	74	00	78	00	74	00	word . t x t
142B1960	70	61	73	73	77	6F	72	64	20	69	73	20	61	61	31	31	pas word is aa11
142B1970	31	38	36	61	62	64	65	33	66	65	34	63	39	64	66	39	186ab e3fe4c9df9
142B1980	63	35	64	62	34	66	65	65	36	37	35	37	37	35	65	38	c5db4fe 675775e8
142B1990	35	37	64	61	34	36	64	34	35	62	39	64	37	32	34	63	57da46d45 9d724c
142B19A0	37	63	36	64	32	64	66	37	38	63	37	66	20	0D	0A	00	6d2df78c71

Size of Cont

Offset of Cont

Contents

					Attr Type ID	Len of Attr		
Non-Res Flag	Len of Name	Offset to Name	Flags	Attr ID	Size of Content	Offset of Cont	Index Flag	Paddi ng

실험

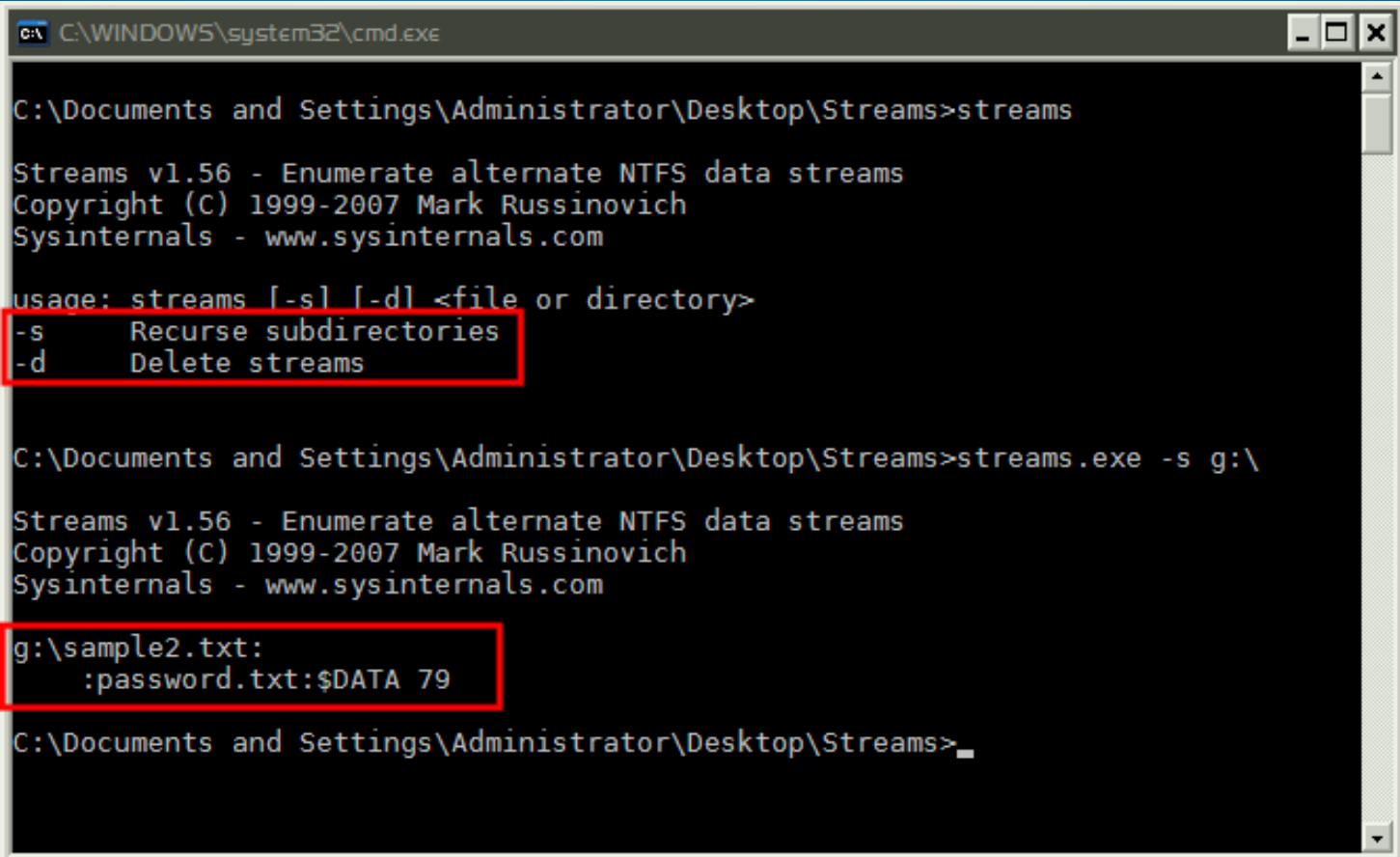
- 원본 파일을 갱신하였을 경우
 - 원본파일 내용 삽입 → 끝에 Attribute 종결자를 삽입
 - ADS정보는 따로 처리하지 않음

Attribute 종결자

142B2100	2E 00 74 00 78 00 74 00	80 00 00 00 40 00 00 00	. t x t @
142B2110	00 00 18 00 00 00 07 00	26 00 00 00 18 00 00 00	&
142B2120	74 72 69 70 6C 65 73 74	72 65 61 6D 44 61 61 61	triplestreamDaaa
142B2130	61 61 61 61 61 61 61 61	61 61 61 61 61 61 61 61	aaaaaaaaaaaaaaaa
142B2140	61 61 61 20 0D 0A 74 00	FF FF FF FF 82 79 47 11	aaa t yyyylyG
142B2150	00 0A 18 00 00 00 06 00	10 00 00 00 30 00 00 00	0
142B2160	70 00 61 00 73 00 73 00	77 00 64 00 2E 00 74 00	p a s s w d . t
142B2170	78 00 74 00 00 00 00 00	74 72 69 70 6C 65 73 74	x t triplest
142B2180	72 65 61 6D 44 20 0D 0A	FF FF FF FF 82 79 47 11	reamD yyyylyG

ADS정보는 그대로 유지

Streams.exe



```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrator\Desktop\Streams>streams

Streams v1.56 - Enumerate alternate NTFS data streams
Copyright (C) 1999-2007 Mark Russinovich
Sysinternals - www.sysinternals.com

usage: streams [-s] [-d] <file or directory>
-s      Recurse subdirectories
-d      Delete streams

C:\Documents and Settings\Administrator\Desktop\Streams>streams.exe -s g:\

Streams v1.56 - Enumerate alternate NTFS data streams
Copyright (C) 1999-2007 Mark Russinovich
Sysinternals - www.sysinternals.com

g:\sample2.txt:
    :password.txt:$DATA 79

C:\Documents and Settings\Administrator\Desktop\Streams>
```