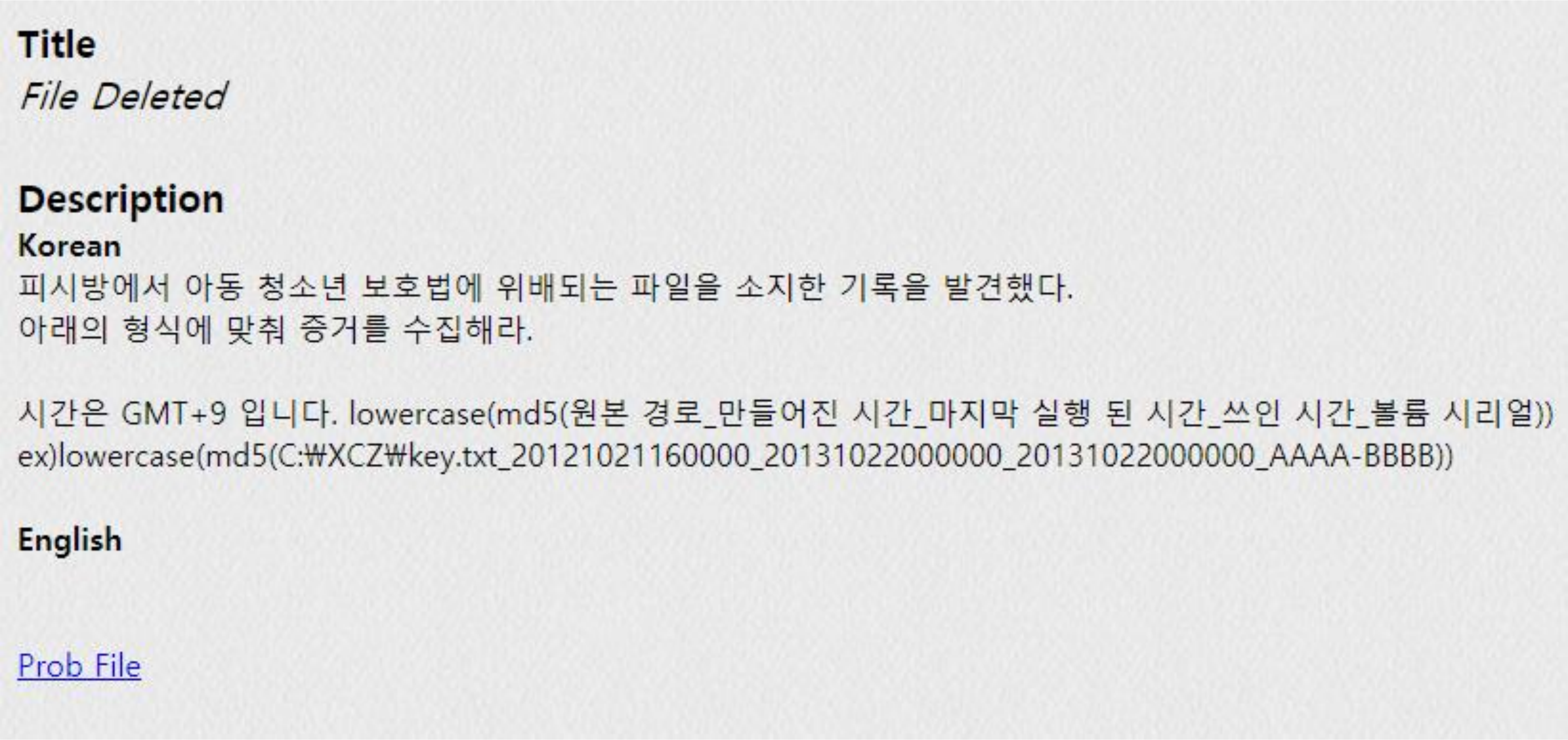
File Deleted?

SCP
전유민
(Y.M.Jeon)



Title

File Deleted

Description

Korean

피시방에서 아동 청소년 보호법에 위배되는 파일을 소지한 기록을 발견했다.
아래의 형식에 맞춰 증거를 수집해라.

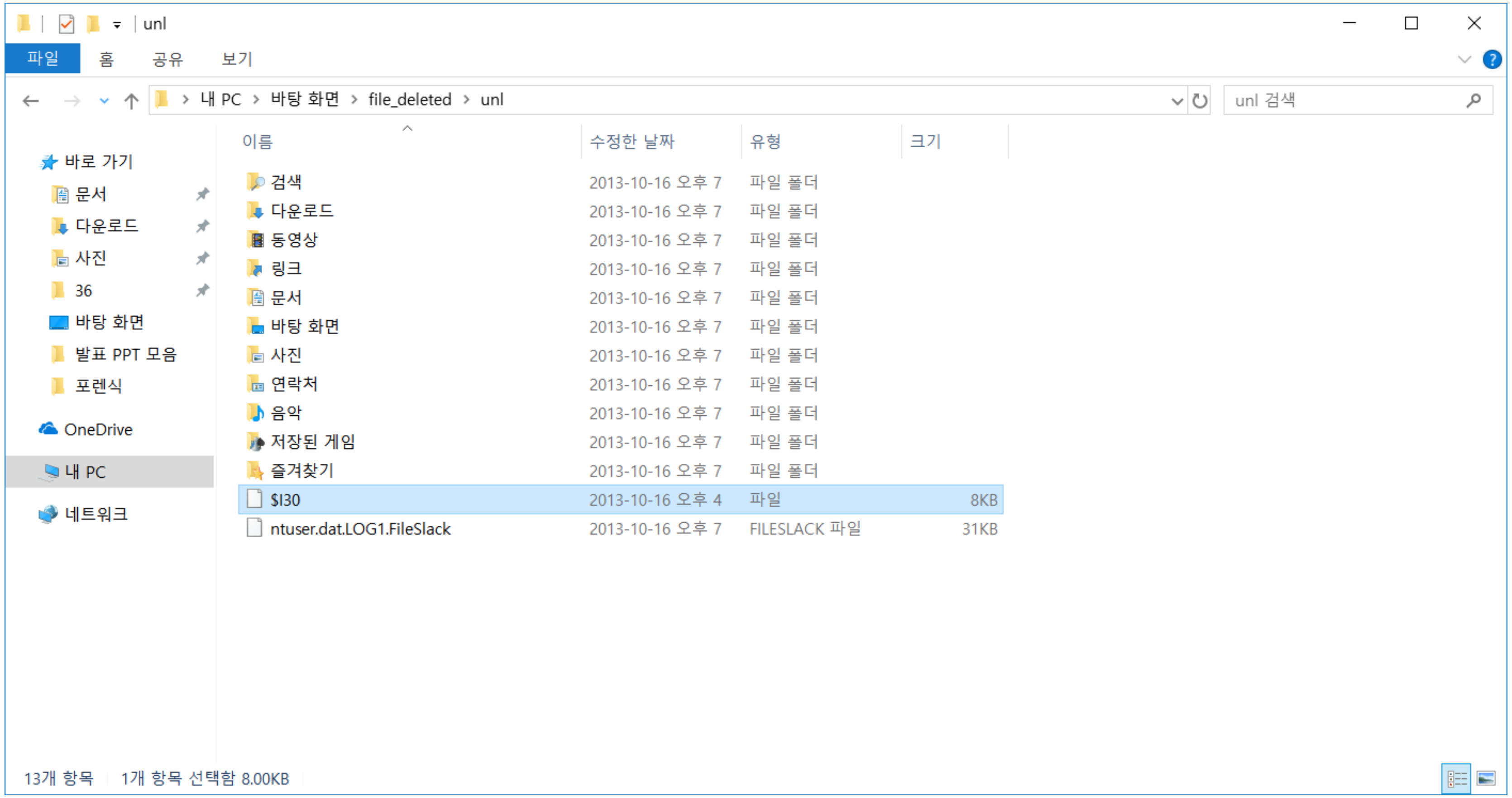
시간은 GMT+9 입니다. lowercase(md5(원본 경로_만들어진 시간_마지막 실행 된 시간_쓰인 시간_볼륨 시리얼))
ex)lowercase(md5(C:₩XCZ₩key.txt_20121021160000_20131022000000_20131022000000_AAAA-BBBB))

English

Prob File

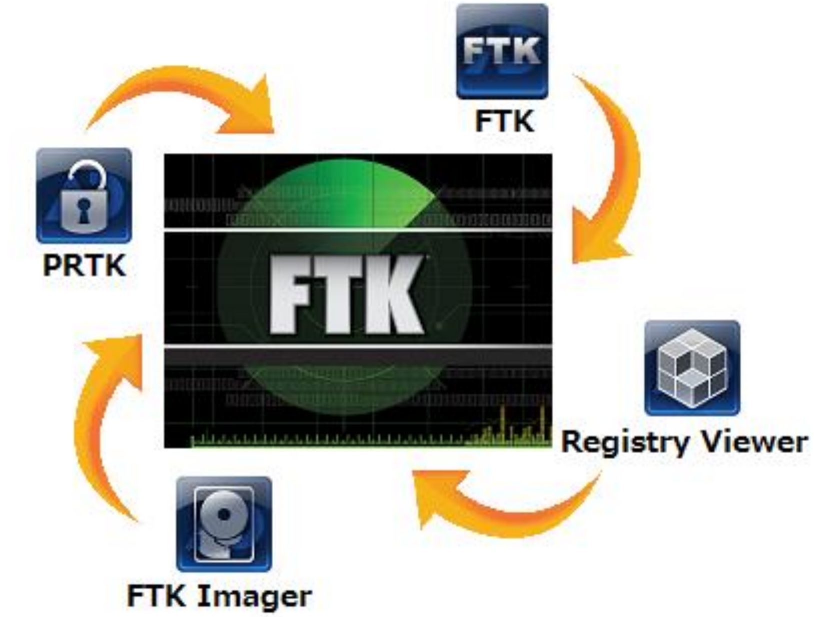
XCZ.KR Prob 36 (Digital Forensic)

Prob file

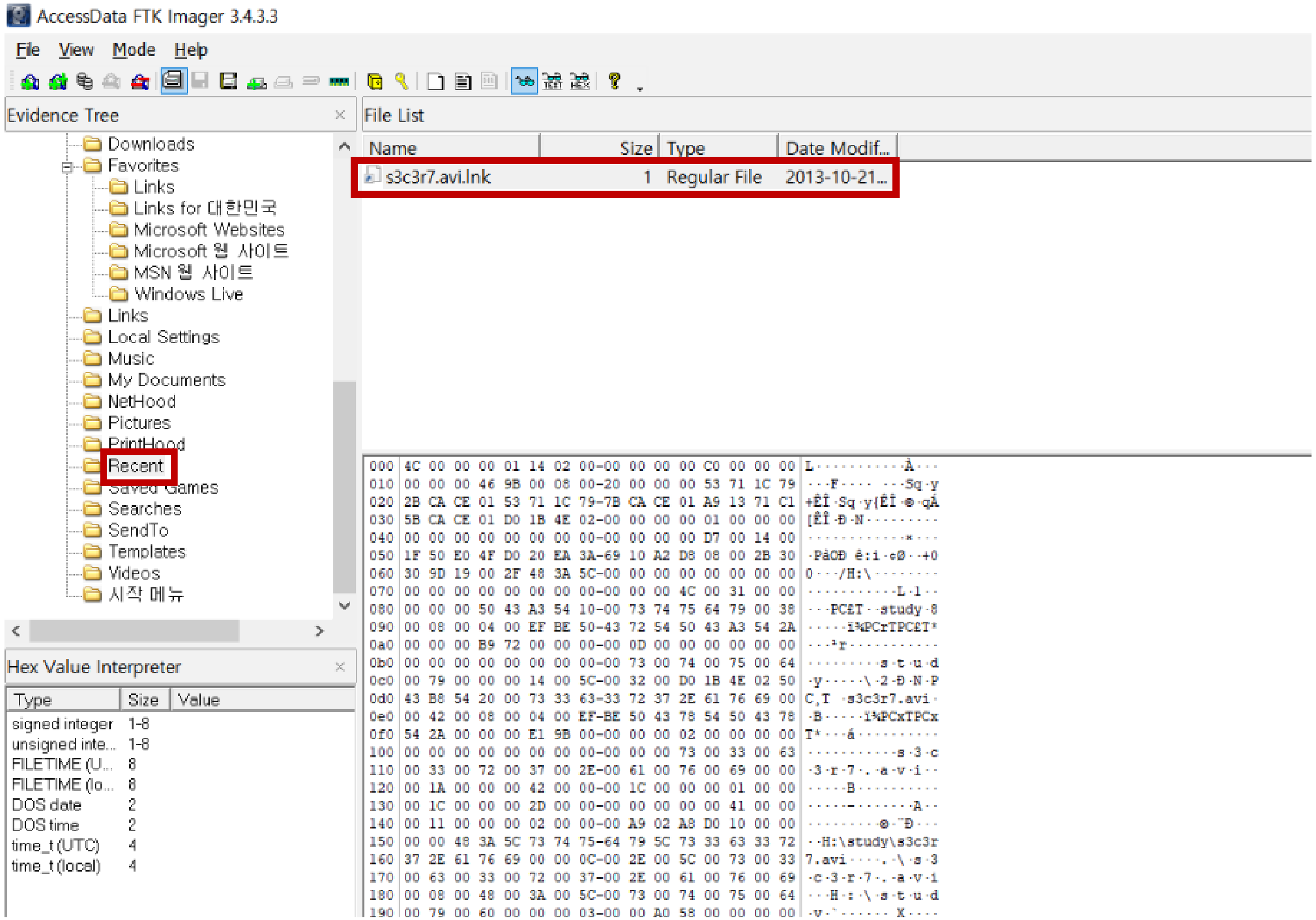


이름	수정한 날짜	유형	크기
검색	2013-10-16 오후 7	파일 폴더	
다운로드	2013-10-16 오후 7	파일 폴더	
동영상	2013-10-16 오후 7	파일 폴더	
링크	2013-10-16 오후 7	파일 폴더	
문서	2013-10-16 오후 7	파일 폴더	
바탕 화면	2013-10-16 오후 7	파일 폴더	
사진	2013-10-16 오후 7	파일 폴더	
연락처	2013-10-16 오후 7	파일 폴더	
음악	2013-10-16 오후 7	파일 폴더	
저장된 게임	2013-10-16 오후 7	파일 폴더	
즐겨찾기	2013-10-16 오후 7	파일 폴더	
$I30	2013-10-16 오후 4	파일	8KB
ntuser.dat.LOG1.FileSlack	2013-10-16 오후 7	FILESLACK 파일	31KB

13개 항목 1개 항목 선택함 8.00KB



FTK Imager



Evidence Tree

- Downloads
- Favorites
  - Links
  - Links for 대한민국
  - Microsoft Websites
  - Microsoft 웹 사이트
  - MSN 웹 사이트
  - Windows Live
- Links
- Local Settings
- Music
- My Documents
- NetHood
- Pictures
- PrintHood
- Recent
- Saved Games
- Searches
- SendTo
- Templates
- Videos
- 시작 메뉴

File List

Name	Size	Type	Date Modif...
s3c3r7.avi.lnk	1	Regular File	2013-10-21...

Hex Value Interpreter

Type	Size	Value
signed integer	1-8	
unsigned inte...	1-8	
FILETIME (U...	8	
FILETIME (lo...	8	
DOS date	2	
DOS time	2	
time_t (UTC)	4	
time_t (local)	4	

```
000  4C 00 00 00 01 14 02 00-00 00 00 00 C0 00 00 00  L···········À···
010  00 00 00 46 9B 00 08 00-20 00 00 00 53 71 1C 79  ···F····  ···Sq·y
020  2B CA CE 01 53 71 1C 79-7B CA CE 01 A9 13 71 C1  +ÊÎ·Sq·y{ÊÎ·©·qÁ
030  5B CA CE 01 D0 1B 4E 02-00 00 00 01 00 00 00 00  [ÊÎ·Ð·N·········
040  00 00 00 00 00 00 00 00-00 00 00 D7 00 14 00 00  ···········×····
050  1F 50 E0 4F D0 20 EA 3A-69 10 A2 D8 08 00 2B 30  ·PàOÐ ê:i·¢Ø··+0
060  30 9D 19 00 2F 48 3A 5C-00 00 00 00 00 00 00 00  0···/H:\········
070  00 00 00 00 00 00 00 00-00 00 4C 00 31 00 00 00  ··········L·1···
080  00 00 00 50 43 A3 54 10-00 73 74 75 64 79 00 38  ···PC£T··study·8
090  00 08 00 04 00 EF BE 50-43 72 54 50 43 A3 54 2A  ·····ï¾PCrTPC£T*
0a0  00 00 00 B9 72 00 00 00-00 0D 00 00 00 00 00 00  ···¹r···········
0b0  00 00 00 00 00 00 00 00-00 73 00 74 00 75 00 64  ·········s·t·u·d
0c0  00 79 00 00 00 14 00 5C-00 32 00 D0 1B 4E 02 50  ·y·····\·2·Ð·N·P
0d0  43 B8 54 20 00 73 33 63-33 72 37 2E 61 76 69 00  C¸T ·s3c3r7.avi·
0e0  00 42 00 08 00 04 00 EF-BE 50 43 78 54 50 43 78  ·B·····ï¾PCxTPCx
0f0  54 2A 00 00 00 E1 9B 00-00 00 00 02 00 00 00 00  T*···á··········
100  00 00 00 00 00 00 00 00-00 00 73 00 33 00 63     ···········s·3·c
110  00 33 00 72 00 37 00 2E-00 61 00 76 00 69 00 00  ·3·r·7·.·a·v·i··
120  00 1A 00 00 00 42 00 00-00 1C 00 00 00 01 00 00  ·····B··········
130  00 1C 00 00 00 2D 00 00-00 00 00 00 00 41 00 00  ·····-·······A··
140  00 11 00 00 00 02 00 00-00 A9 02 A8 D0 10 00 00  ·········©·¨Ð···
150  00 00 48 3A 5C 73 74 75-64 79 5C 73 33 63 33 72  ··H:\study\s3c3r
160  37 2E 61 76 69 00 00 0C-00 2E 00 5C 00 73 00 33  7.avi····.·\·s·3
170  00 63 00 33 00 72 00 37-00 2E 00 61 00 76 00 69  ·c·3·r·7·.·a·v·i
180  00 08 00 48 00 3A 00 5C-00 73 00 74 00 75 00 64  ···H·:·\·s·t·u·d
190  00 79 00 60 00 00 00 03-00 00 A0 58 00 00 00 00  ·y·`······ X····
```

ShellLinkHeader

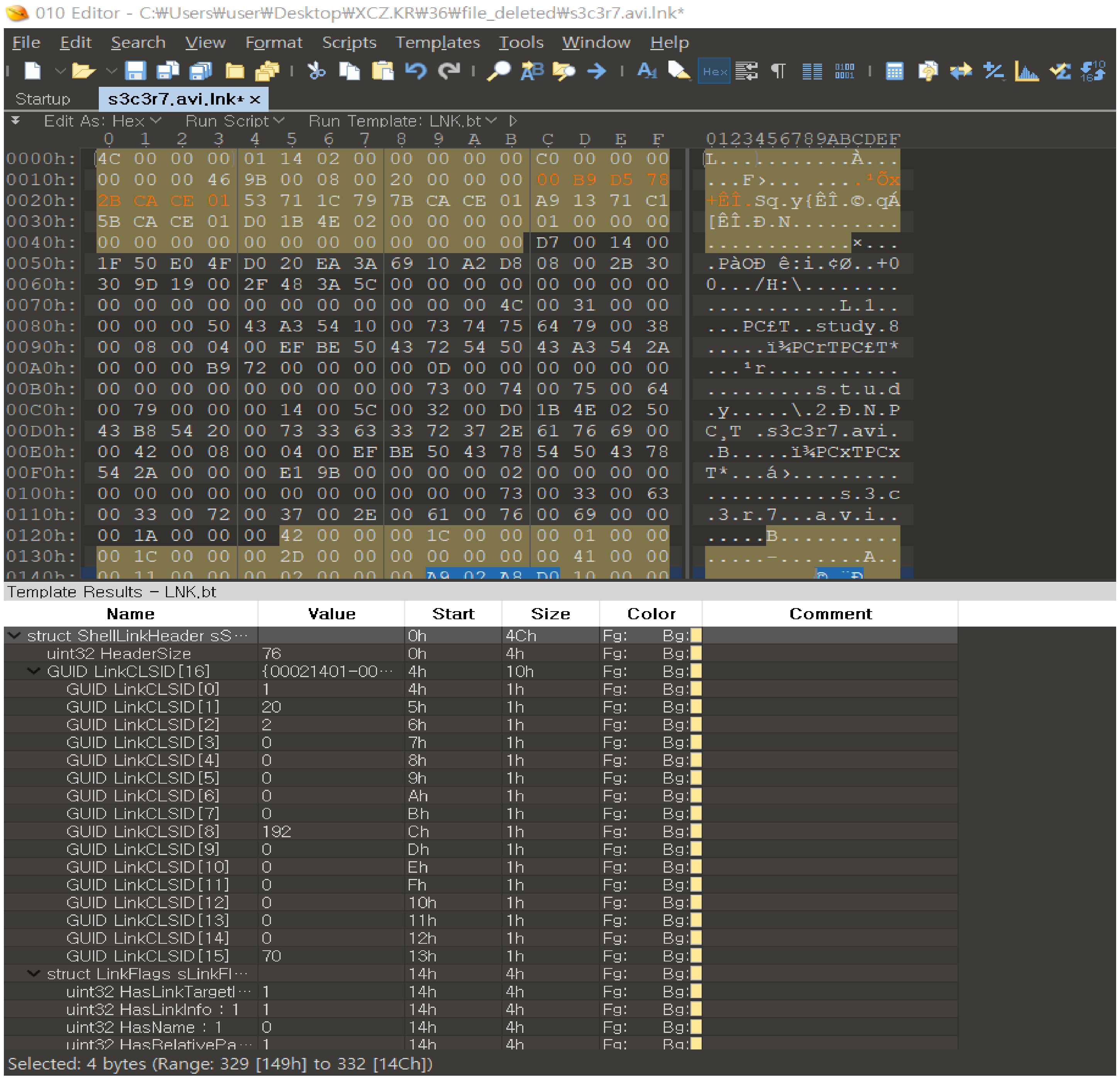
LinkTargetIDList

LinkInfo

StringData

ExtraData

010 Editor


010 Editor - C:₩Users₩user₩Desktop₩XCZ.KR₩36₩file_deleted₩s3c3r7.avi.lnk*
File Edit Search View Format Scripts Templates Tools Window Help
Startup
s3c3r7.avi.lnk* ×
Edit As: Hex
Run Script
Run Template: LNK.bt

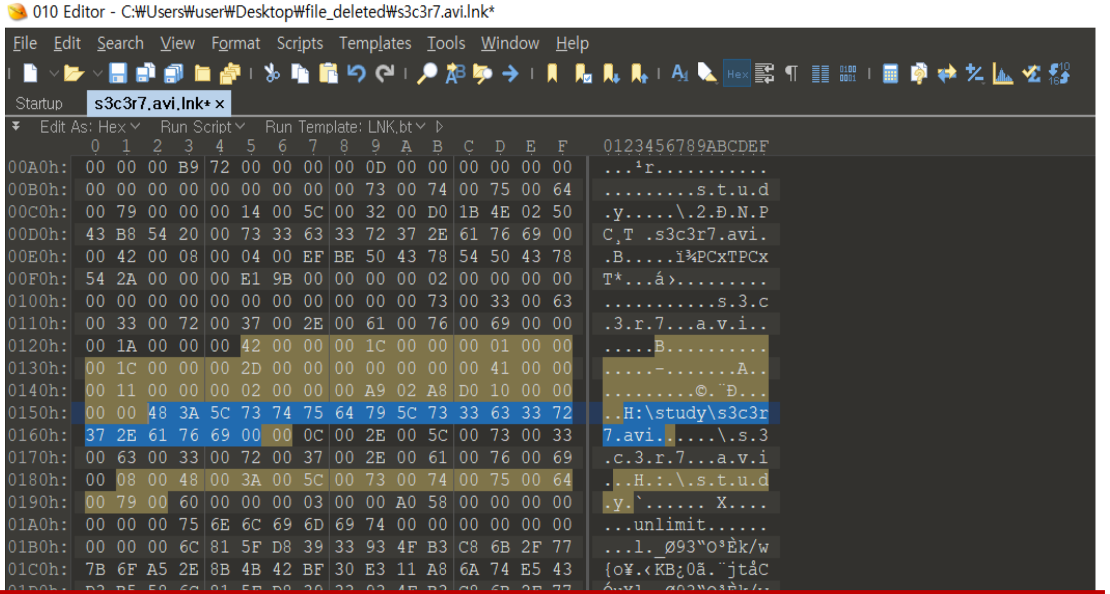
```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 4C 00 00 00 01 14 02 00 00 00 00 00 C0 00 00 00  L...........À...
0010h: 00 00 00 46 9B 00 08 00 20 00 00 00 00 B9 D5 78  ...F›... ....¹Õx
0020h: 2B CA CE 01 53 71 1C 79 7B CA CE 01 A9 13 71 C1  +ÊÎ.Sq.y{ÊÎ.©.qÁ
0030h: 5B CA CE 01 D0 1B 4E 02 00 00 00 00 01 00 00 00  [ÊÎ.Ð.N.........
0040h: 00 00 00 00 00 00 00 00 00 00 00 00 D7 00 14 00  ............×...
0050h: 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30  .PàOÐ ê:i.¢Ø..+0
0060h: 30 9D 19 00 2F 48 3A 5C 00 00 00 00 00 00 00 00  0.../H:\........
0070h: 00 00 00 00 00 00 00 00 00 00 00 4C 00 31 00 00  ...........L.1..
0080h: 00 00 00 50 43 A3 54 10 00 73 74 75 64 79 00 38  ...PC£T..study.8
0090h: 00 08 00 04 00 EF BE 50 43 72 54 50 43 A3 54 2A  .....ï¾PCrTPC£T*
00A0h: 00 00 00 B9 72 00 00 00 00 0D 00 00 00 00 00 00  ...¹r...........
00B0h: 00 00 00 00 00 00 00 00 00 73 00 74 00 75 00 64  .........s.t.u.d
00C0h: 00 79 00 00 00 14 00 5C 00 32 00 D0 1B 4E 02 50  .y.....\.2.Ð.N.P
00D0h: 43 B8 54 20 00 73 33 63 33 72 37 2E 61 76 69 00  C¸T .s3c3r7.avi.
00E0h: 00 42 00 08 00 04 00 EF BE 50 43 78 54 50 43 78  .B.....ï¾PCxTPCx
00F0h: 54 2A 00 00 00 E1 9B 00 00 00 00 02 00 00 00 00  T*...á›.........
0100h: 00 00 00 00 00 00 00 00 00 00 00 73 00 33 00 63  ...........s.3.c
0110h: 00 33 00 72 00 37 00 2E 00 61 00 76 00 69 00 00  .3.r.7...a.v.i..
0120h: 00 1A 00 00 00 42 00 00 00 1C 00 00 00 01 00 00  .....B..........
0130h: 00 1C 00 00 00 2D 00 00 00 00 00 00 00 41 00 00  .....-.......A..
0140h: 00 11 00 00 00 02 00 00 00 A9 02 A8 D0 10 00 00
```

Template Results - LNK.bt

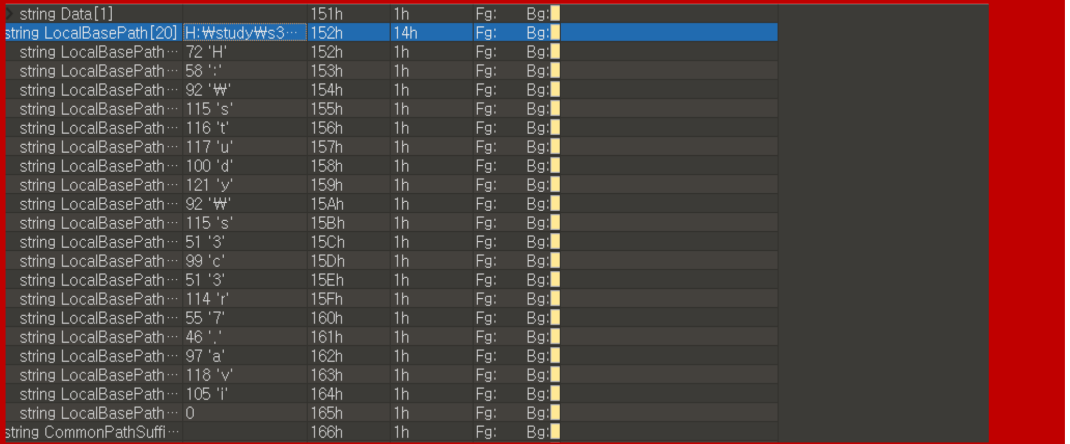
Name	Value	Start	Size	Color	Comment
struct ShellLinkHeader sS···		0h	4Ch	Fg: Bg:🟨	
uint32 HeaderSize	76	0h	4h	Fg: Bg:🟨	
GUID LinkCLSID[16]	{00021401-00···	4h	10h	Fg: Bg:🟨	
GUID LinkCLSID[0]	1	4h	1h	Fg: Bg:🟨	
GUID LinkCLSID[1]	20	5h	1h	Fg: Bg:🟨	
GUID LinkCLSID[2]	2	6h	1h	Fg: Bg:🟨	
GUID LinkCLSID[3]	0	7h	1h	Fg: Bg:🟨	
GUID LinkCLSID[4]	0	8h	1h	Fg: Bg:🟨	
GUID LinkCLSID[5]	0	9h	1h	Fg: Bg:🟨	
GUID LinkCLSID[6]	0	Ah	1h	Fg: Bg:🟨	
GUID LinkCLSID[7]	0	Bh	1h	Fg: Bg:🟨	
GUID LinkCLSID[8]	192	Ch	1h	Fg: Bg:🟨	
GUID LinkCLSID[9]	0	Dh	1h	Fg: Bg:🟨	
GUID LinkCLSID[10]	0	Eh	1h	Fg: Bg:🟨	
GUID LinkCLSID[11]	0	Fh	1h	Fg: Bg:🟨	
GUID LinkCLSID[12]	0	10h	1h	Fg: Bg:🟨	
GUID LinkCLSID[13]	0	11h	1h	Fg: Bg:🟨	
GUID LinkCLSID[14]	0	12h	1h	Fg: Bg:🟨	
GUID LinkCLSID[15]	70	13h	1h	Fg: Bg:🟨	
struct LinkFlags sLinkFl···		14h	4h	Fg: Bg:🟨	
uint32 HasLinkTargetI···	1	14h	4h	Fg: Bg:🟨	
uint32 HasLinkInfo : 1	1	14h	4h	Fg: Bg:🟨	
uint32 HasName : 1	0	14h	4h	Fg: Bg:🟨	
uint32 HasRelativePa···	1	14h	4h	Fg: Bg:🟨	

Selected: 4 bytes (Range: 329 [149h] to 332 [14Ch])

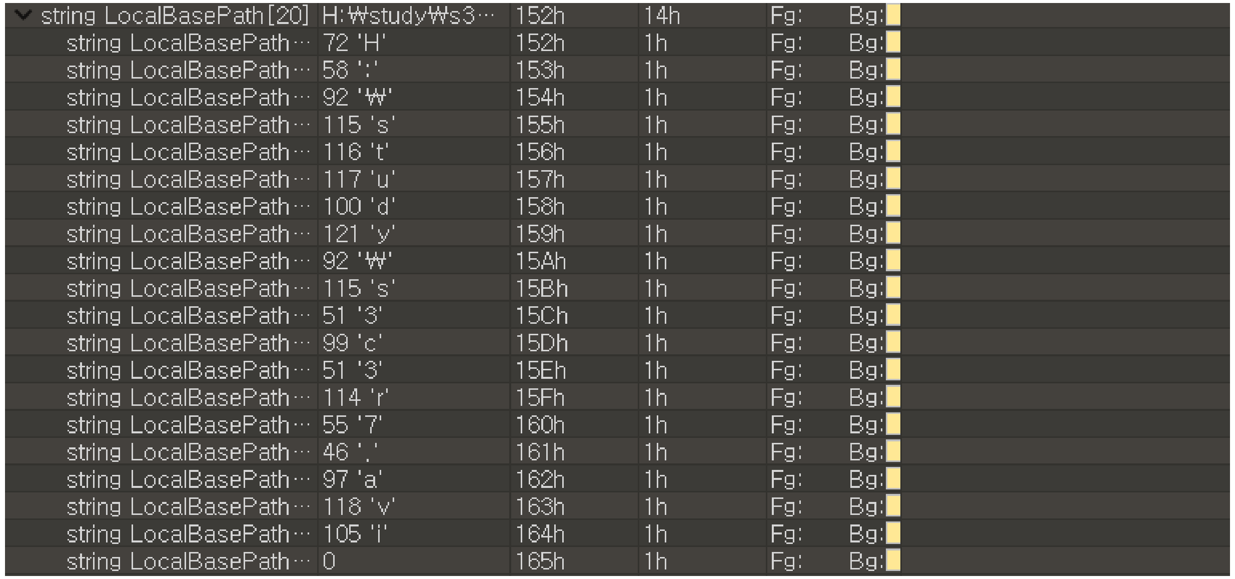
원본 경로???


010 Editor - C:₩Users₩user₩Desktop₩file_deleted₩s3c3r7.avi.lnk*
File Edit Search View Format Scripts Templates Tools Window Help
Startup
s3c3r7.avi.lnk* ×
Edit As: Hex
Run Script
Run Template: LNK.bt

```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
00A0h: 00 00 00 B9 72 00 00 00 00 0D 00 00 00 00 00 00  ...¹r...........
00B0h: 00 00 00 00 00 00 00 00 00 73 00 74 00 75 00 64  .........s.t.u.d
00C0h: 00 79 00 00 00 14 00 5C 00 32 00 D0 1B 4E 02 50  .y.....\.2.Đ.N.P
00D0h: 43 B8 54 20 00 73 33 63 33 72 37 2E 61 76 69 00  C¸T .s3c3r7.avi.
00E0h: 00 42 00 08 00 04 00 EF BE 50 43 78 54 50 43 78  .B.....ï¾PCxTPCx
00F0h: 54 2A 00 00 00 E1 9B 00 00 00 00 02 00 00 00 00  T*...á›.........
0100h: 00 00 00 00 00 00 00 00 00 00 00 73 00 33 00 63  ...........s.3.c
0110h: 00 33 00 72 00 37 00 2E 00 61 00 76 00 69 00 00  .3.r.7...a.v.i..
0120h: 00 1A 00 00 00 42 00 00 00 1C 00 00 00 01 00 00  .....B..........
0130h: 00 1C 00 00 00 2D 00 00 00 00 00 00 00 41 00 00  .....-.......A..
0140h: 00 11 00 00 00 02 00 00 00 A9 02 A8 D0 10 00 00  .........©.¨Đ...
0150h: 00 00 48 3A 5C 73 74 75 64 79 5C 73 33 63 33 72  ..H:\study\s3c3r
0160h: 37 2E 61 76 69 00 00 0C 00 2E 00 5C 00 73 00 33  7.avi......\.s.3
0170h: 00 63 00 33 00 72 00 37 00 2E 00 61 00 76 00 69  .c.3.r.7...a.v.i
0180h: 00 08 00 48 00 3A 00 5C 00 73 00 74 00 75 00 64  ...H.:.\.s.t.u.d
0190h: 00 79 00 60 00 00 00 03 00 00 A0 58 00 00 00 00  .y.`...... X....
01A0h: 00 00 00 75 6E 6C 69 6D 69 74 00 00 00 00 00 00  ...unlimit......
01B0h: 00 00 00 6C 81 5F D8 39 33 93 4F B3 C8 6B 2F 77  ...l._Ø93“O³Èk/w
01C0h: 7B 6F A5 2E 8B 4B 42 BF 30 E3 11 A8 6A 74 E5 43  {o¥.‹KB¿0ã.¨jtåC
```



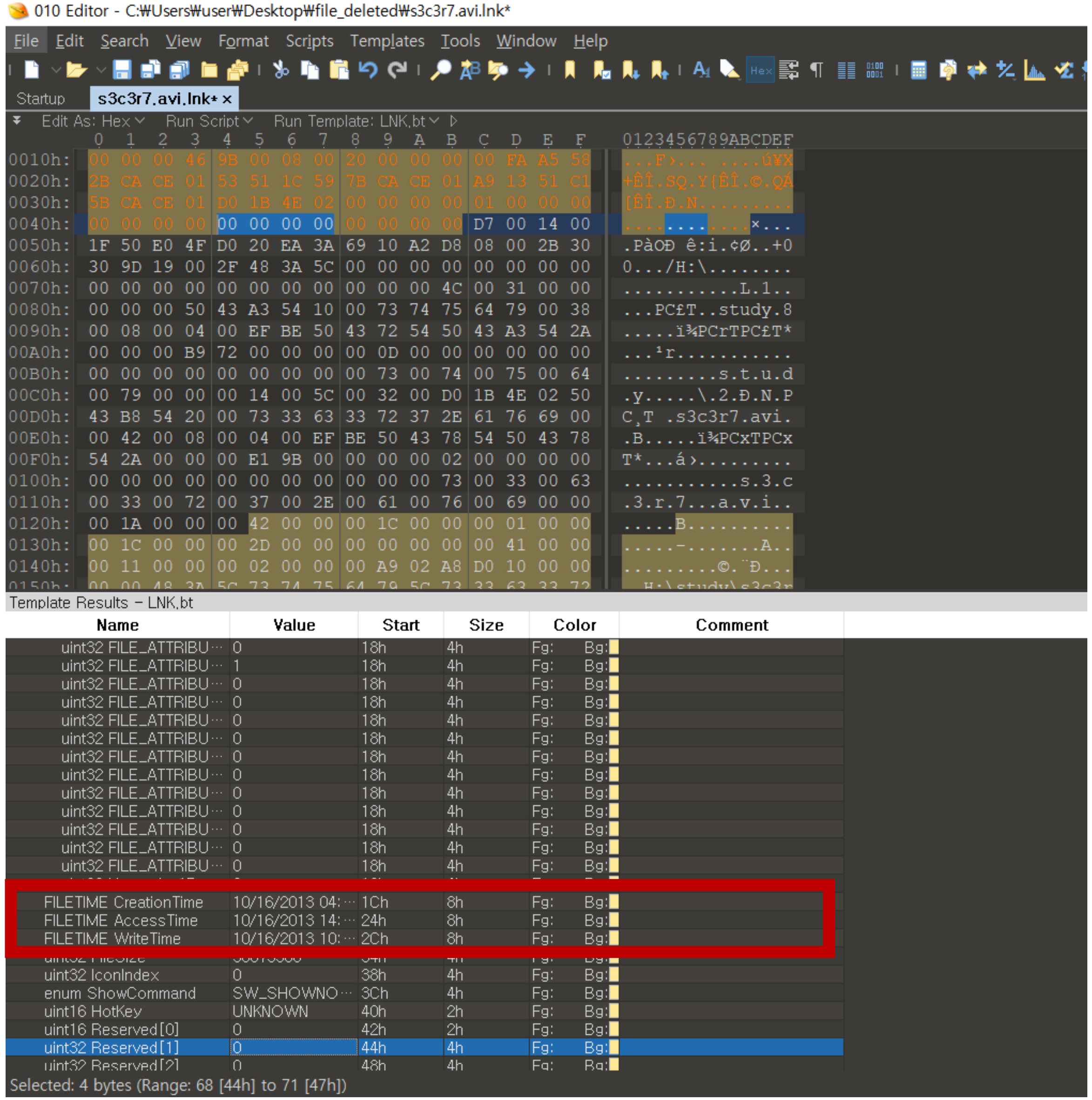
string Data[1]		151h	1h	Fg:	Bg:
string LocalBasePath[20]	H:₩study₩s3···	152h	14h	Fg:	Bg:
string LocalBasePath···	72 'H'	152h	1h	Fg:	Bg:
string LocalBasePath···	58 ':'	153h	1h	Fg:	Bg:
string LocalBasePath···	92 '₩'	154h	1h	Fg:	Bg:
string LocalBasePath···	115 's'	155h	1h	Fg:	Bg:
string LocalBasePath···	116 't'	156h	1h	Fg:	Bg:
string LocalBasePath···	117 'u'	157h	1h	Fg:	Bg:
string LocalBasePath···	100 'd'	158h	1h	Fg:	Bg:
string LocalBasePath···	121 'y'	159h	1h	Fg:	Bg:
string LocalBasePath···	92 '₩'	15Ah	1h	Fg:	Bg:
string LocalBasePath···	115 's'	15Bh	1h	Fg:	Bg:
string LocalBasePath···	51 '3'	15Ch	1h	Fg:	Bg:
string LocalBasePath···	99 'c'	15Dh	1h	Fg:	Bg:
string LocalBasePath···	51 '3'	15Eh	1h	Fg:	Bg:
string LocalBasePath···	114 'r'	15Fh	1h	Fg:	Bg:
string LocalBasePath···	55 '7'	160h	1h	Fg:	Bg:
string LocalBasePath···	46 '.'	161h	1h	Fg:	Bg:
string LocalBasePath···	97 'a'	162h	1h	Fg:	Bg:
string LocalBasePath···	118 'v'	163h	1h	Fg:	Bg:
string LocalBasePath···	105 'i'	164h	1h	Fg:	Bg:
string LocalBasePath···	0	165h	1h	Fg:	Bg:
string CommonPathSuffi···		166h	1h	Fg:	Bg:



string LocalBasePath[20]	H:₩study₩s3···	152h	14h	Fg:	Bg:
string LocalBasePath···	72 'H'	152h	1h	Fg:	Bg:
string LocalBasePath···	58 ':'	153h	1h	Fg:	Bg:
string LocalBasePath···	92 '₩'	154h	1h	Fg:	Bg:
string LocalBasePath···	115 's'	155h	1h	Fg:	Bg:
string LocalBasePath···	116 't'	156h	1h	Fg:	Bg:
string LocalBasePath···	117 'u'	157h	1h	Fg:	Bg:
string LocalBasePath···	100 'd'	158h	1h	Fg:	Bg:
string LocalBasePath···	121 'y'	159h	1h	Fg:	Bg:
string LocalBasePath···	92 '₩'	15Ah	1h	Fg:	Bg:
string LocalBasePath···	115 's'	15Bh	1h	Fg:	Bg:
string LocalBasePath···	51 '3'	15Ch	1h	Fg:	Bg:
string LocalBasePath···	99 'c'	15Dh	1h	Fg:	Bg:
string LocalBasePath···	51 '3'	15Eh	1h	Fg:	Bg:
string LocalBasePath···	114 'r'	15Fh	1h	Fg:	Bg:
string LocalBasePath···	55 '7'	160h	1h	Fg:	Bg:
string LocalBasePath···	46 '.'	161h	1h	Fg:	Bg:
string LocalBasePath···	97 'a'	162h	1h	Fg:	Bg:
string LocalBasePath···	118 'v'	163h	1h	Fg:	Bg:
string LocalBasePath···	105 'i'	164h	1h	Fg:	Bg:
string LocalBasePath···	0	165h	1h	Fg:	Bg:

H:₩study₩s3c3r7.avi

만들어진 시간? 마지막 실행 된 시간? 쓰인 시간?



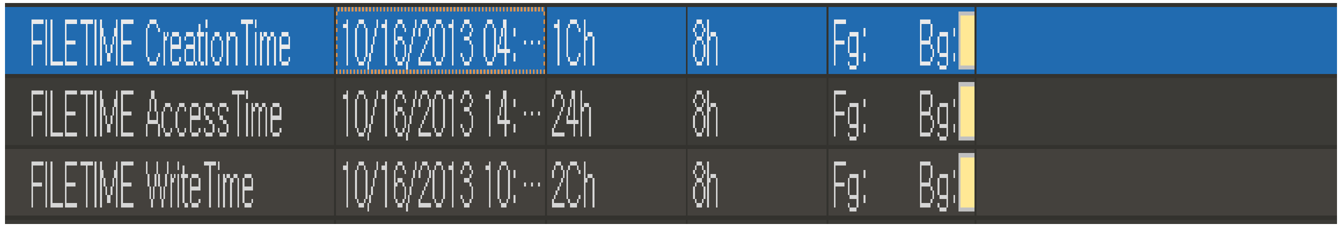
010 Editor - C:₩Users₩user₩Desktop₩file_deleted₩s3c3r7.avi.lnk*

```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0010h: 00 00 00 46 9B 00 08 00 20 00 00 00 00 FA A5 58  ...F›... ....ú¥X
0020h: 2B CA CE 01 53 51 1C 59 7B CA CE 01 A9 13 51 C1  +ÊÎ.SQ.Y{ÊÎ.©.QÁ
0030h: 5B CA CE 01 D0 1B 4E 02 00 00 00 00 01 00 00 00  [ÊÎ.Đ.N.........
0040h: 00 00 00 00 00 00 00 00 00 00 00 00 D7 00 14 00  ............×...
0050h: 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30  .PàOĐ ê:i.¢Ø..+0
0060h: 30 9D 19 00 2F 48 3A 5C 00 00 00 00 00 00 00 00  0.../H:\........
0070h: 00 00 00 00 00 00 00 00 00 00 00 4C 00 31 00 00  ...........L.1..
0080h: 00 00 00 50 43 A3 54 10 00 73 74 75 64 79 00 38  ...PC£T..study.8
0090h: 00 08 00 04 00 EF BE 50 43 72 54 50 43 A3 54 2A  .....ï¾PCrTPC£T*
00A0h: 00 00 00 B9 72 00 00 00 00 0D 00 00 00 00 00 00  ...¹r...........
00B0h: 00 00 00 00 00 00 00 00 00 73 00 74 00 75 00 64  .........s.t.u.d
00C0h: 00 79 00 00 00 14 00 5C 00 32 00 D0 1B 4E 02 50  .y.....\.2.Đ.N.P
00D0h: 43 B8 54 20 00 73 33 63 33 72 37 2E 61 76 69 00  C¸T .s3c3r7.avi.
00E0h: 00 42 00 08 00 04 00 EF BE 50 43 78 54 50 43 78  .B.....ï¾PCxTPCx
00F0h: 54 2A 00 00 00 E1 9B 00 00 00 00 02 00 00 00 00  T*...á›.........
0100h: 00 00 00 00 00 00 00 00 00 00 00 73 00 33 00 63  ...........s.3.c
0110h: 00 33 00 72 00 37 00 2E 00 61 00 76 00 69 00 00  .3.r.7...a.v.i..
0120h: 00 1A 00 00 00 42 00 00 00 1C 00 00 00 01 00 00  .....B..........
0130h: 00 1C 00 00 00 2D 00 00 00 00 00 00 00 41 00 00  .....-.......A..
0140h: 00 11 00 00 00 02 00 00 00 A9 02 A8 D0 10 00 00  .........©.¨Đ...
0150h: 00 00 48 3A 5C 73 74 75 64 79 5C 73 33 63 33 72  ..H:\study\s3c3r
```

Template Results – LNK.bt

Name	Value	Start	Size	Color	Comment
uint32 FILE_ATTRIBU···	0	18h	4h	Fg: Bg:	
uint32 FILE_ATTRIBU···	1	18h	4h	Fg: Bg:	
uint32 FILE_ATTRIBU···	0	18h	4h	Fg: Bg:	
uint32 FILE_ATTRIBU···	0	18h	4h	Fg: Bg:	
uint32 FILE_ATTRIBU···	0	18h	4h	Fg: Bg:	
uint32 FILE_ATTRIBU···	0	18h	4h	Fg: Bg:	
uint32 FILE_ATTRIBU···	0	18h	4h	Fg: Bg:	
uint32 FILE_ATTRIBU···	0	18h	4h	Fg: Bg:	
uint32 FILE_ATTRIBU···	0	18h	4h	Fg: Bg:	
uint32 FILE_ATTRIBU···	0	18h	4h	Fg: Bg:	
uint32 FILE_ATTRIBU···	0	18h	4h	Fg: Bg:	
uint32 FILE_ATTRIBU···	0	18h	4h	Fg: Bg:	
uint32 FILE_ATTRIBU···	0	18h	4h	Fg: Bg:	
FILETIME CreationTime	10/16/2013 04:···	1Ch	8h	Fg: Bg:	
FILETIME AccessTime	10/16/2013 14:···	24h	8h	Fg: Bg:	
FILETIME WriteTime	10/16/2013 10:···	2Ch	8h	Fg: Bg:	
uint32 FileSize	[illegible]	34h	4h	Fg: Bg:	
uint32 IconIndex	0	38h	4h	Fg: Bg:	
enum ShowCommand	SW_SHOWNO···	3Ch	4h	Fg: Bg:	
uint16 HotKey	UNKNOWN	40h	2h	Fg: Bg:	
uint16 Reserved[0]	0	42h	2h	Fg: Bg:	
uint32 Reserved[1]	0	44h	4h	Fg: Bg:	
uint32 Reserved[2]	0	48h	4h	Fg: Bg:	

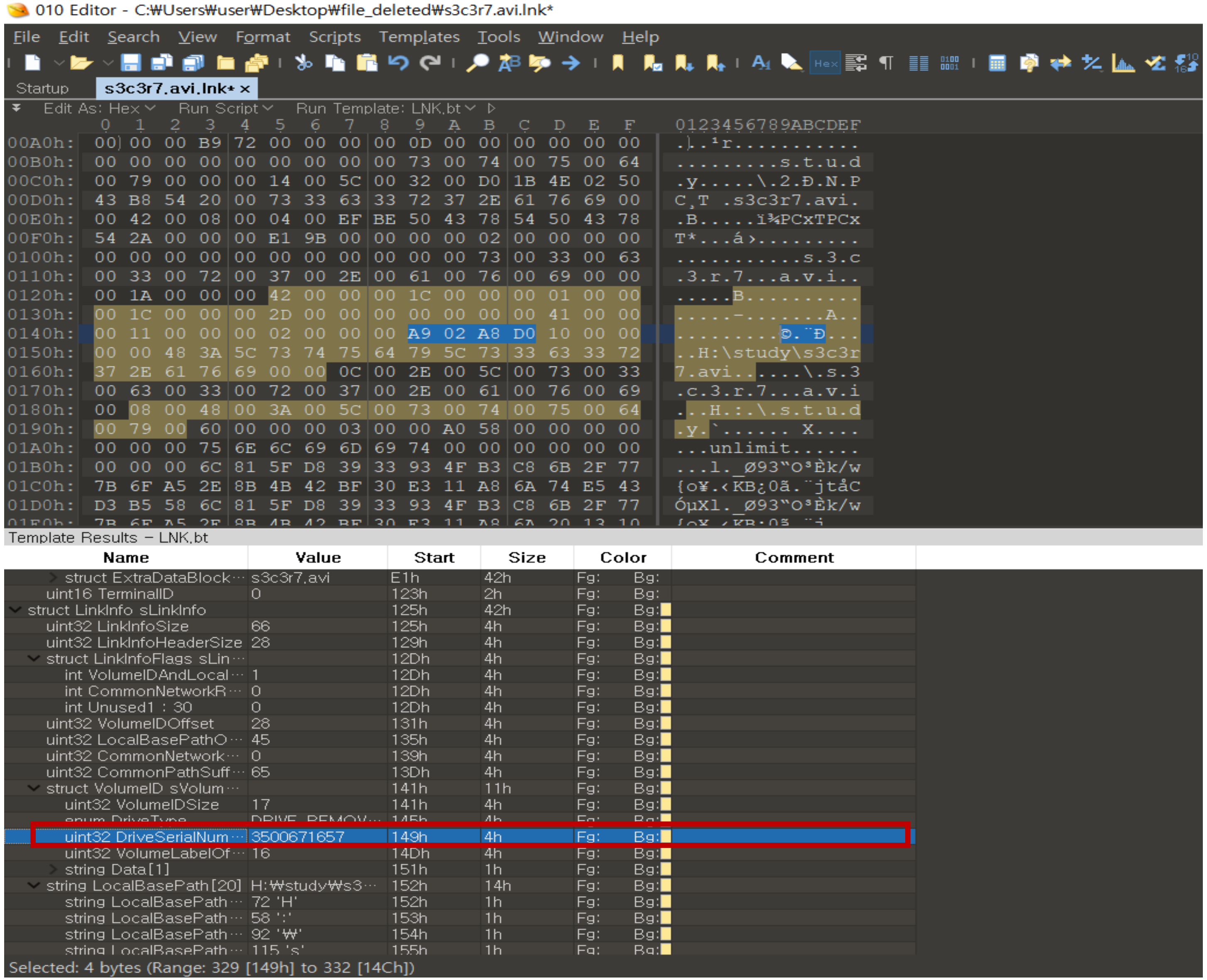
Selected: 4 bytes (Range: 68 [44h] to 71 [47h])



FILETIME CreationTime	10/16/2013 04:···	1Ch	8h	Fg:	Bg:
FILETIME AccessTime	10/16/2013 14:···	24h	8h	Fg:	Bg:
FILETIME WriteTime	10/16/2013 10:···	2Ch	8h	Fg:	Bg:

만들어진 시간 (FILETIME Creation Time)
= 10/16/2013 04:52:10
마지막 실행 된 시간 (FILETIME Access Time)
= 10/16/2013 14:24:50
쓰인 시간 (FILETIME Write Time)
= 10/16/2013 10:37:47

볼륨 시리얼?

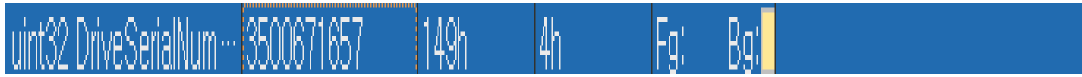

010 Editor - C:₩Users₩user₩Desktop₩file_deleted₩s3c3r7.avi.lnk*
File Edit Search View Format Scripts Templates Tools Window Help
Startup
s3c3r7.avi.lnk* ×
Edit As: Hex
Run Script
Run Template: LNK.bt

```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
00A0h: 00 00 00 B9 72 00 00 00 00 0D 00 00 00 00 00 00  ...¹r...........
00B0h: 00 00 00 00 00 00 00 00 00 73 00 74 00 75 00 64  .........s.t.u.d
00C0h: 00 79 00 00 00 14 00 5C 00 32 00 D0 1B 4E 02 50  .y.....\.2.Ð.N.P
00D0h: 43 B8 54 20 00 73 33 63 33 72 37 2E 61 76 69 00  C¸T .s3c3r7.avi.
00E0h: 00 42 00 08 00 04 00 EF BE 50 43 78 54 50 43 78  .B.....ï¾PCxTPCx
00F0h: 54 2A 00 00 00 E1 9B 00 00 00 00 02 00 00 00 00  T*...á›.........
0100h: 00 00 00 00 00 00 00 00 00 00 00 73 00 33 00 63  ...........s.3.c
0110h: 00 33 00 72 00 37 00 2E 00 61 00 76 00 69 00 00  .3.r.7...a.v.i..
0120h: 00 1A 00 00 00 42 00 00 00 1C 00 00 00 01 00 00  .....B..........
0130h: 00 1C 00 00 00 2D 00 00 00 00 00 00 00 41 00 00  .....-.......A..
0140h: 00 11 00 00 00 02 00 00 00 A9 02 A8 D0 10 00 00  .........©.¨Ð...
0150h: 00 00 48 3A 5C 73 74 75 64 79 5C 73 33 63 33 72  ..H:\study\s3c3r
0160h: 37 2E 61 76 69 00 00 0C 00 2E 00 5C 00 73 00 33  7.avi......\.s.3
0170h: 00 63 00 33 00 72 00 37 00 2E 00 61 00 76 00 69  .c.3.r.7...a.v.i
0180h: 00 08 00 48 00 3A 00 5C 00 73 00 74 00 75 00 64  ...H.:.\.s.t.u.d
0190h: 00 79 00 60 00 00 00 03 00 00 A0 58 00 00 00 00  .y.`...... X....
01A0h: 00 00 00 75 6E 6C 69 6D 69 74 00 00 00 00 00 00  ...unlimit......
01B0h: 00 00 00 6C 81 5F D8 39 33 93 4F B3 C8 6B 2F 77  ...l._Ø93“O³Èk/w
01C0h: 7B 6F A5 2E 8B 4B 42 BF 30 E3 11 A8 6A 74 E5 43  {o¥.‹KB¿0ã.¨jtåC
01D0h: D3 B5 58 6C 81 5F D8 39 33 93 4F B3 C8 6B 2F 77  ÓµXl._Ø93“O³Èk/w
01E0h: 7B 6F A5 2E 8B 4B 42 BF 30 E3 11 A8 6A 20 13 10
```

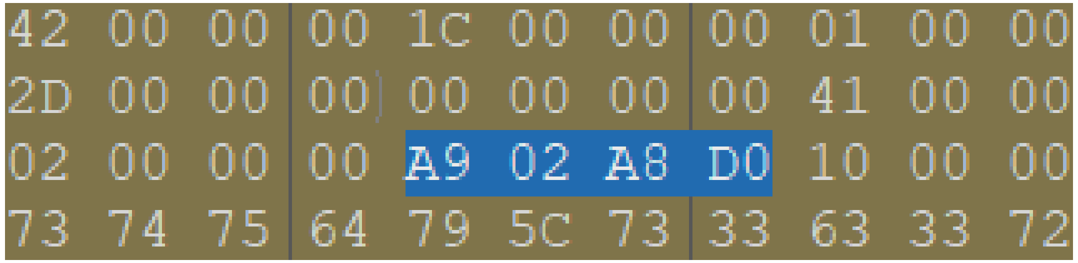
Template Results – LNK.bt

Name	Value	Start	Size	Color	Comment
struct ExtraDataBlock···	s3c3r7.avi	E1h	42h	Fg: Bg:	
uint16 TerminalID	0	123h	2h	Fg: Bg:	
struct LinkInfo sLinkInfo		125h	42h	Fg: Bg:	
uint32 LinkInfoSize	66	125h	4h	Fg: Bg:	
uint32 LinkInfoHeaderSize	28	129h	4h	Fg: Bg:	
struct LinkInfoFlags sLin···		12Dh	4h	Fg: Bg:	
int VolumeIDAndLocal···	1	12Dh	4h	Fg: Bg:	
int CommonNetworkR···	0	12Dh	4h	Fg: Bg:	
int Unused1 : 30	0	12Dh	4h	Fg: Bg:	
uint32 VolumeIDOffset	28	131h	4h	Fg: Bg:	
uint32 LocalBasePathO···	45	135h	4h	Fg: Bg:	
uint32 CommonNetwork···	0	139h	4h	Fg: Bg:	
uint32 CommonPathSuff···	65	13Dh	4h	Fg: Bg:	
struct VolumeID sVolum···		141h	11h	Fg: Bg:	
uint32 VolumeIDSize	17	141h	4h	Fg: Bg:	
enum DriveType	DRIVE_REMOV···	145h	4h	Fg: Bg:	
uint32 DriveSerialNum···	3500671657	149h	4h	Fg: Bg:	
uint32 VolumeLabelOf···	16	14Dh	4h	Fg: Bg:	
string Data[1]		151h	1h	Fg: Bg:	
string LocalBasePath[20]	H:₩study₩s3···	152h	14h	Fg: Bg:	
string LocalBasePath···	72 'H'	152h	1h	Fg: Bg:	
string LocalBasePath···	58 ':'	153h	1h	Fg: Bg:	
string LocalBasePath···	92 '₩'	154h	1h	Fg: Bg:	
string LocalBasePath···	115 's'	155h	1h	Fg: Bg:	

Selected: 4 bytes (Range: 329 [149h] to 332 [14Ch])



uint32 DriveSerialNum···	3500671657	149h	4h	Fg: Bg:

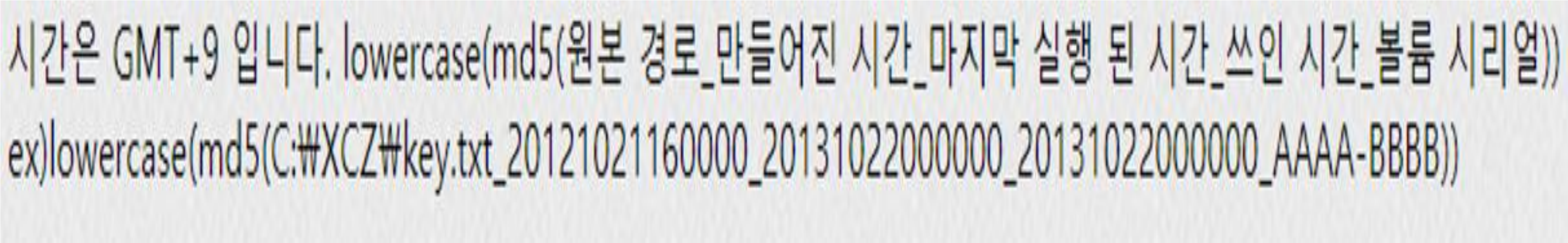


```
42 00 00 00 1C 00 00 00 01 00 00
2D 00 00 00 00 00 00 00 41 00 00
02 00 00 00 A9 02 A8 D0 10 00 00
73 74 75 64 79 5C 73 33 63 33 72
```

볼륨 시리얼 = A9 02 A8 D0???

리틀엔디언 방식으로~

볼륨 시리얼 = D0 A8 02 A9



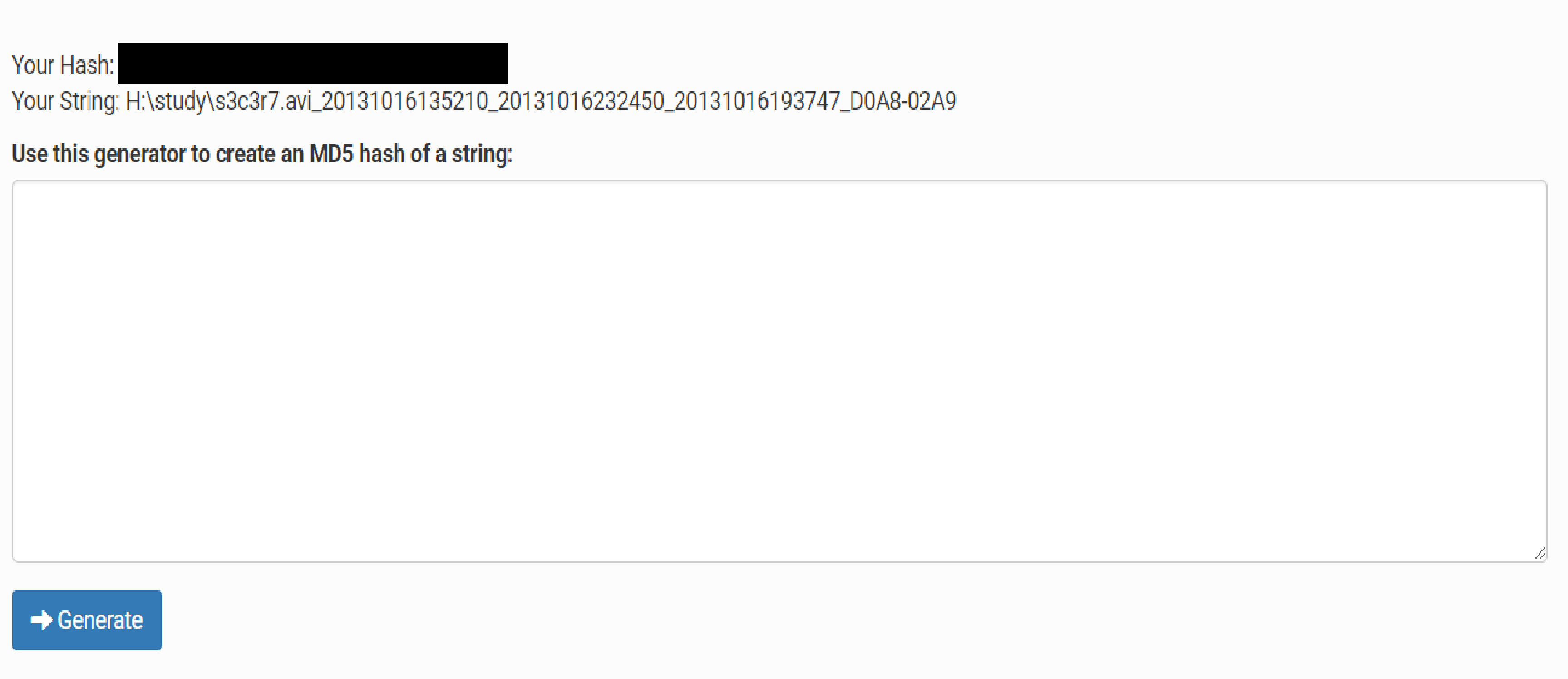
시간은 GMT+9 입니다. lowercase(md5(원본 경로_만들어진 시간_마지막 실행 된 시간_쓰인 시간_볼륨 시리얼))

ex)lowercase(md5(C:₩XCZ₩key.txt_20121021160000_20131022000000_20131022000000_AAAA-BBBB))

H:₩study₩s3c3r7.avi_20131016045210_20131016142450_
20131016103747_D0A8-02A9

GMT+9 ⬇

H:₩study₩s3c3r7.avi_20131016135210_20131016232450_
20131016193747_D0A8-02A9



Your Hash: [redacted]

Your String: H:\study\s3c3r7.avi_20131016135210_20131016232450_20131016193747_D0A8-02A9

Use this generator to create an MD5 hash of a string:

해결~

QnA...?

감사합니다~