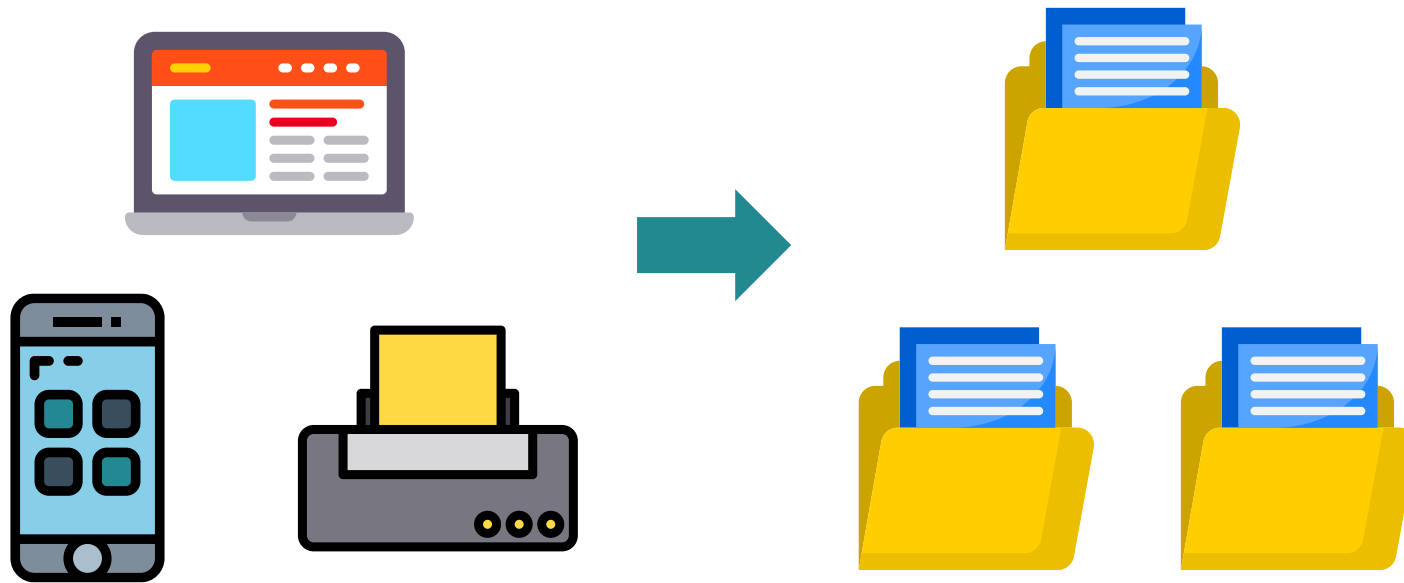


# What Is **Digital Forensics**?

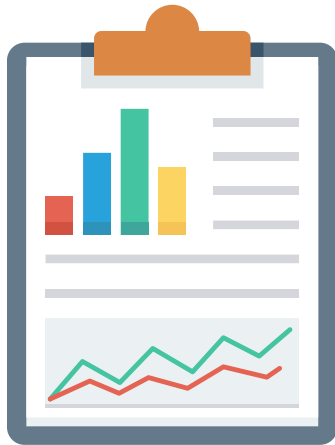
SCP 이다영



# 디지털 포렌식이란?



# 디지털 포렌식이란?



## 디지털 포렌식

**디지털 기기에 남아 있는 자료와 삭제된 자료를 복원해  
수사에 활용하고 법정에서 증거로 활용할 수 있게 하는 것**

# 디지털 포렌식 기술 유형

- (1) **디스크** 포렌식
- (2) **네트워크** 포렌식
- (3) **모바일** 포렌식
- (4) **멀티미디어** 포렌식
- (5) **안티** 포렌식

## (1) 디스크 포렌식

하드디스크, USB, SSD 등 물리적 저장매체에서  
삭제/변경된 데이터를 복원하고 분석하는 기법

## (1) 디스크 포렌식

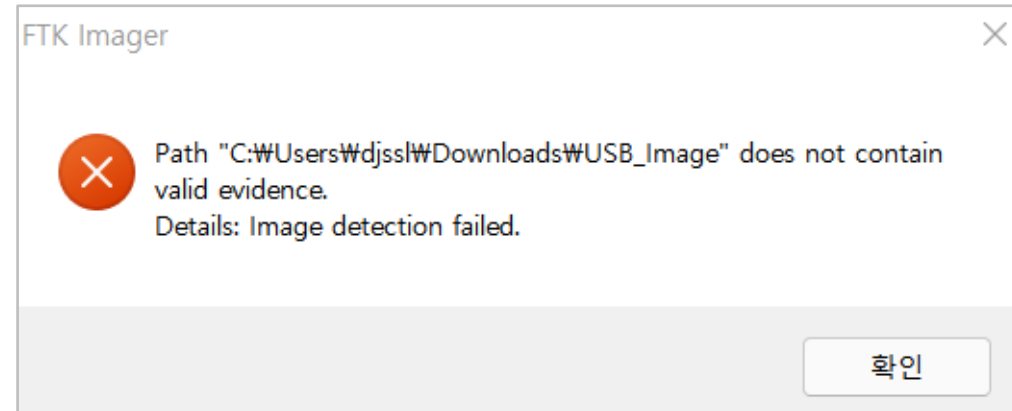


FTK Imager

img_.E01	!IMG2.E01	1,535,876	Regular File
Partition 1 [15263MB]	!IMG2.E02	1,535,933	Regular File
NONAME [FAT32]	!IMG2.E02.FileSlack	4	File Slack
[root]	!IMG2.E03	1,535,934	Regular File
!IMG	!IMG2.E04	1,535,941	Regular File
!IMG2	!IMG2.E04.FileSlack	12	File Slack
SanDiskSecureAccess	!IMG2.E05	1,535,948	Regular File
System Volume Information	!IMG2.E06	1,535,932	Regular File
새 폴더	!IMG2.E06.FileSlack	5	File Slack
새 폴더	!IMG2.E07	1,535,954	Regular File
[redacted]	!IMG2.E07.FileSlack	15	File Slack
[redacted]	!IMG2.E08	1,535,960	Regular File
[redacted]	!IMG2.E08.FileSlack	9	File Slack
[unallocated space]			
Unpartitioned Space [basic disk]			

## (1) 디스크 포렌식

**손상된 USB 이미지를  
복구시켜보자**





# 디지털 포렌식 기술 유형

## (1) 디스크 포렌식

USB_Image																	
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	EB	58	90	4D	53	44	4F	53	35	2E	30	00	02	08	80	11	ëX.MSDOS5.0...€.
00000010	02	00	00	00	00	F8	00	00	3F	00	FF	00	02	00	00	00	.....ø...?.ÿ.....
00000020	80	1D	1D	00	40	07	00	00	00	00	00	00	02	00	00	00	€...@.....
00000030	01	00	06	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000040	80	00	29	0A	E0	96	DE	4E	4F	20	4E	41	4D	45	20	20	€.) .à-PNO NAME
00000050	20	20	46	41	54	33	32	20	20	20	33	C9	8E	D1	BC	F4	FAT32 3ÉŽÑ*ô
00000060	7B	8E	C1	8E	D9	BD	00	7C	88	4E	02	8A	56	40	B4	41	{ŽÁŽÛ*. ^N.ŠV@`A
00000070	BB	AA	55	CD	13	72	10	81	FB	55	AA	75	0A	F6	C1	01	»^Uí.r...ûU^u.ôÁ.
00000080	74	05	FE	46	02	EB	FF	81	C3	00	02	66	40	49	75	94	t.pF.ëÿ.Ã..f@Iu"
00000090	C3	42	4F	4F	54	4D	47	52	20	20	20	20	00	00	00	00	ÃBOOTMGR ....
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000D0	00	00	00	00	0D	0A	52	65	6D	6F	76	65	20	64	69	73	.....Remove dis
000000E0	6B	73	20	6F	72	20	6F	74	68	65	72	20	6D	65	64	69	ks or other medi
000000F0	61	2E	FF	0D	0A	44	69	73	6B	20	65	72	72	6F	72	FF	a.ÿ..Disk errorÿ
00000100	0D	0A	50	72	65	73	73	20	61	6E	79	20	6B	65	79	20	..Press any key
00000110	74	6F	20	72	65	73	74	61	72	74	0D	0A	00	00	00	00	to restart.....
00000120	00	AC	CB	D8	00	00	55	AA	52	52	61	41	00	00	00	00	..-Ëø..U^RRaA....
00000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

['USB\_Image' 파일 구조]

## (1) 디스크 포렌식

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	EB	58	90	4D	53	44	4F	53	35	2E	30	00	02	08	80	11	ëX.MSDOS5.0...€.
00000010	02	00	00	00	00	F8	00	00	3F	00	FF	00	02	00	00	00	.....ø...?.ÿ.....
00000020	80	1D	1D	00	40	07	00	00	00	00	00	00	02	00	00	00	€...@.....
00000030	01	00	06	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000040	80	00	29	0A	E0	96	DE	4E	4F	20	4E	41	4D	45	20	20	€.) .à-ÞNO NAME
00000050	20	20	46	41	54	33	32	20	20	20	33	C9	8E	D1	BC	F4	FAT32 3ÉŽŇ*ó
00000060	7B	8E	C1	8E	D9	BD	00	7C	88	4E	02	8A	56	40	B4	41	{ŽÁŽŮ%. ^N.ŠV@'A
00000070	BB	AA	55	CD	13	72	10	81	FB	55	AA	75	0A	F6	C1	01	»²Uí.r...ûU²u.öÁ.
00000080	74	05	FE	46	02	EB	FF	81	C3	00	02	66	40	49	75	94	t.þF.ëÿ.Ä...f@Iu"
00000090	C3	42	4F	4F	54	4D	47	52	20	20	20	20	00	00	00	00	ÄBOOTMGR ....
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000D0	00	00	00	00	0D	0A	52	65	6D	6F	76	65	20	64	69	73	.....Remove dis
000000E0	6B	73	20	6F	72	20	6F	74	68	65	72	20	6D	65	64	69	ks or other medi
000000F0	61	2E	FF	0D	0A	44	69	73	6B	20	65	72	72	6F	72	FF	a.ÿ..Disk errorÿ
00000100	0D	0A	50	72	65	73	73	20	61	6E	79	20	6B	65	79	20	..Press any key
00000110	74	6F	20	72	65	73	74	61	72	74	0D	0A	00	00	00	00	to restart.....
00000120	00	AC	CB	D8	00	00	55	AA	52	52	61	41	00	00	00	00	.-Ëø..U²RRaA....
00000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

### 파일 시스템

: 컴퓨터에서 파일이나 자료를 쉽게 발견 할 수 있도록  
유지, 관리하는 방법

### 윈도우 주요 파일 시스템

NTFS / **FAT**

File System	Jump command to Boot Code
FAT12 / 16	0x903CEB
<b>FAT32</b>	<b>0x9058EB</b>
NTFS	0x9052EB

# 디지털 포렌식 기술 유형

## (1) 디스크 포렌식

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000200	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000210	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000220	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000230	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Lead Signature	52 52 61 41	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	RRaA.....
000008010	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
000008020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
000008030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
000008040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
000008050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
000008060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
000008070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
000008080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
000008090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
0000080A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
0000080B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
0000080C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
0000080D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
0000080E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
0000080F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
000008100	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
000008110	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
000008120	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
000008130	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
000008140	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
000008150	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
000008160	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
000008170	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
000008180	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
000008190	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
0000081A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
0000081B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
0000081C0	Structure Signature	Free Cluster Count	Next Free Cluster
0000081D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
0000081E0	00 00 00 00 72 72 41 61 4C FB 07 00 04 00 00 00	.....rrAaLû.....	
0000081F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA	.....U^	
	Reserved	Trail Signature	←



# 디지털 포렌식 기술 유형

## (1) 디스크 포렌식

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	EB	58	90	4D	53	44	4F	53	35	2E	30	00	02	08	80	11	ëX.MSDOS5.0...ë.
00000010	02	00	00	00	00	F8	00	00	3F	00	FF	00	02	00	00	00	.....ø...?.ÿ.....
00000020	80	1D	1D	00	40	07	00	00	00	00	00	00	02	00	00	00	ë...@.....
00000030	01	00	06	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000040	80	00	29	0A	E0	96	DE	4E	4F	20	4E	41	4D	45	20	20	ë.) .à-ÞNO NAME
00000050	20	20	46	41	54	33	32	20	20	20	33	C9	8E	D1	BC	F4	FAT32 3ÉŽN46
00000060	7B	8E	C1	8E	D9	BD	00	7C	88	4E	02	8A	56	40	B4	41	{ŽÁŽŮs.   ^N.ŠV@'A
00000070	BB	AA	55	CD	13	72	10	81	FB	55	AA	75	0A	F6	C1	01	»*UÍ.r..ûU*u.ôÁ.
00000080	74	05	FE	46	02	EB	FF	81	C3	00	02	66	40	49	75	94	t.þF.ëÿ.Ă..f@Iu"
00000090	C3	42	4F	4F	54	4D	47	52	20	20	20	20	00	00	00	00	ĂBOOTMGR .....
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000D0	00	00	00	00	0D	0A	52	65	6D	6F	76	65	20	64	69	73	.....Remove dis
000000E0	6B	73	20	6F	72	20	6F	74	68	65	72	20	6D	65	64	69	ks or other medi
000000F0	61	2E	FF	0D	0A	44	69	73	6B	20	65	72	72	6F	72	FF	a.ÿ..Disk errorÿ
00000100	0D	0A	50	72	65	73	73	20	61	6E	79	20	6B	65	79	20	..Press any key
00000110	74	6F	20	72	65	73	74	61	72	74	0D	0A	00	00	00	00	to restart.....
00000120	00	AC	CB	D8	00	00	55	AA	52	52	61	41	00	00	00	00	..-Ëø..U*RRaA....
00000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000200	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000210	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	EB	58	90	4D	53	44	4F	53	35	2E	30	00	02	08	80	11	ëX.MSDOS5.0...ë.
00000010	02	00	00	00	00	F8	00	00	3F	00	FF	00	02	00	00	00	.....ø...?.ÿ.....
00000020	80	1D	1D	00	40	07	00	00	00	00	00	00	02	00	00	00	ë...@.....
00000030	01	00	06	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000040	80	00	29	0A	E0	96	DE	4E	4F	20	4E	41	4D	45	20	20	ë.) .à-ÞNO NAME
00000050	20	20	46	41	54	33	32	20	20	20	33	C9	8E	D1	BC	F4	FAT32 3ÉŽN46
00000060	7B	8E	C1	8E	D9	BD	00	7C	88	4E	02	8A	56	40	B4	41	{ŽÁŽŮs.   ^N.ŠV@'A
00000070	BB	AA	55	CD	13	72	10	81	FB	55	AA	75	0A	F6	C1	01	»*UÍ.r..ûU*u.ôÁ.
00000080	74	05	FE	46	02	EB	FF	81	C3	00	02	66	40	49	75	94	t.þF.ëÿ.Ă..f@Iu"
00000090	C3	42	4F	4F	54	4D	47	52	20	20	20	20	00	00	00	00	ĂBOOTMGR .....
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0D 0A 52 65	.....Re
000001B0	6D	6F	76	65	20	64	69	73	6B	73	20	6F	72	20	6F	74	move disks or ot
000001C0	68	65	72	20	6D	65	64	69	61	2E	FF	0D	0A	44	69	73	her media.ÿ..Dis
000001D0	6B	20	65	72	72	6F	72	FF	0D	0A	50	72	65	73	73	20	k errorÿ..Press
000001E0	61	6E	79	20	6B	65	79	20	74	6F	20	72	65	73	74	61	any key to resta
000001F0	72	74	0D	0A	00	00	00	00	00	AC	CB	D8	00	00	55	AA	rt.....-Ëø..U*
00000200	52	52	61	41	00	00	00	00	00	00	00	00	00	00	00	00	RRaA.....
00000210	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

## (1) 디스크 포렌식

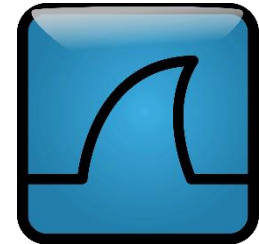
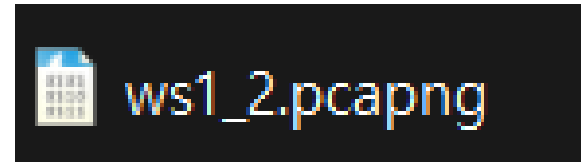
Evidence Tree		File List			
		Name	Size	Type	Date Modified
		관광지	4	Directory	2016-05-30 오전 1:...
		대학교	4	Directory	2016-05-30 오전 1:...
		중앙부처	4	Directory	2016-05-30 오전 1:...
		2차 테러 계획.hwp	10	Regular File	2016-05-30 오전 2:...
		Terrorism Report-2013-North K...	42	Regular File	2016-05-30 오전 1:...
		Terrorism Report-2013-North K...	3	File Slack	
		Terrorism Report-2013-South K...	43	Regular File	2016-05-30 오전 1:...
		Terrorism Report-2013-South K...	2	File Slack	

## (2) 네트워크 포렌식

네트워크 트래픽과 전송 데이터를 수집하여  
증거를 추출하고 분석하는 기법

## (2) 네트워크 포렌식

**패킷 캡처 파일을 분석해  
주고받은 데이터를 확인해보자**



WireShark

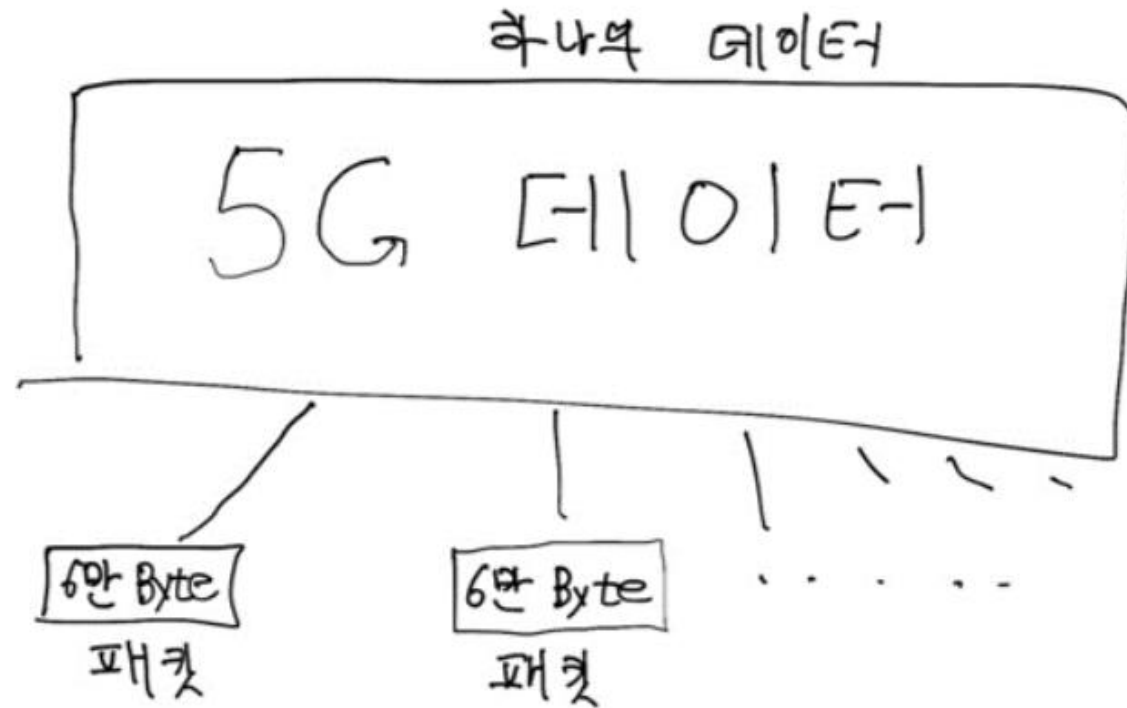
## (2) 네트워크 포렌식

### 패킷

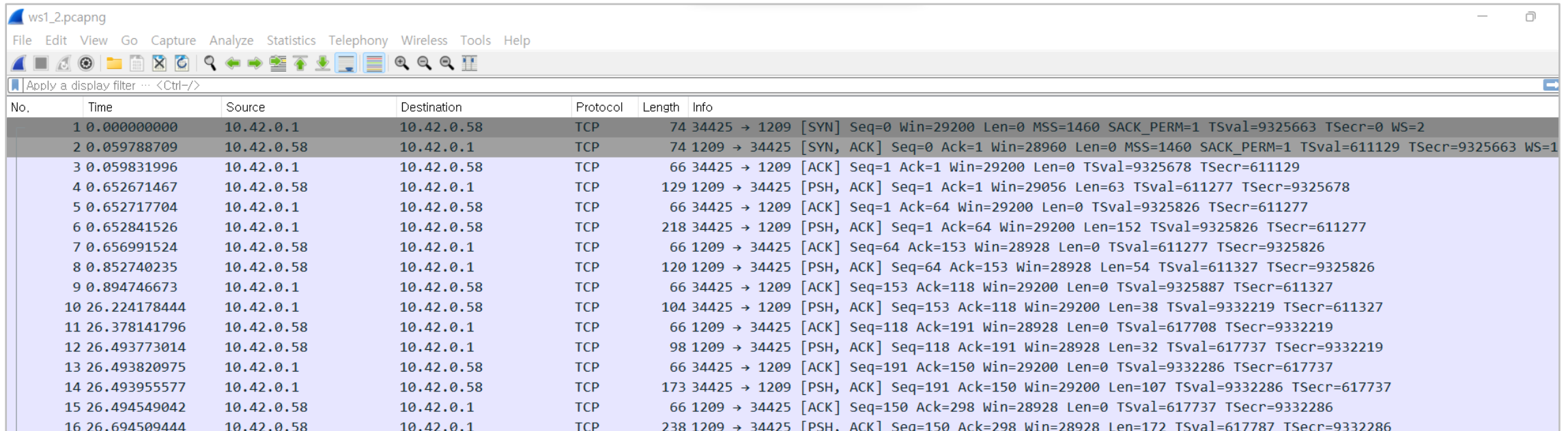
네트워크를 통해 전송되는 데이터의 작은 조각(=블록)



## (2) 네트워크 포렌식



## (2) 네트워크 포렌식



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.42.0.1	10.42.0.58	TCP	74	34425 → 1209 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=9325663 TSecr=0 WS=2
2	0.059788709	10.42.0.58	10.42.0.1	TCP	74	1209 → 34425 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=611129 TSecr=9325663 WS=1
3	0.059831996	10.42.0.1	10.42.0.58	TCP	66	34425 → 1209 [ACK] Seq=1 Ack=1 Win=29200 Len=0 TSval=9325678 TSecr=611129
4	0.652671467	10.42.0.58	10.42.0.1	TCP	129	1209 → 34425 [PSH, ACK] Seq=1 Ack=1 Win=29056 Len=63 TSval=611277 TSecr=9325678
5	0.652717704	10.42.0.1	10.42.0.58	TCP	66	34425 → 1209 [ACK] Seq=1 Ack=64 Win=29200 Len=0 TSval=9325826 TSecr=611277
6	0.652841526	10.42.0.1	10.42.0.58	TCP	218	34425 → 1209 [PSH, ACK] Seq=1 Ack=64 Win=29200 Len=152 TSval=9325826 TSecr=611277
7	0.656991524	10.42.0.58	10.42.0.1	TCP	66	1209 → 34425 [ACK] Seq=64 Ack=153 Win=28928 Len=0 TSval=611277 TSecr=9325826
8	0.852740235	10.42.0.58	10.42.0.1	TCP	120	1209 → 34425 [PSH, ACK] Seq=64 Ack=153 Win=28928 Len=54 TSval=611327 TSecr=9325826
9	0.894746673	10.42.0.1	10.42.0.58	TCP	66	34425 → 1209 [ACK] Seq=153 Ack=118 Win=29200 Len=0 TSval=9325887 TSecr=611327
10	26.224178444	10.42.0.1	10.42.0.58	TCP	104	34425 → 1209 [PSH, ACK] Seq=153 Ack=118 Win=29200 Len=38 TSval=9332219 TSecr=611327
11	26.378141796	10.42.0.58	10.42.0.1	TCP	66	1209 → 34425 [ACK] Seq=118 Ack=191 Win=28928 Len=0 TSval=617708 TSecr=9332219
12	26.493773014	10.42.0.58	10.42.0.1	TCP	98	1209 → 34425 [PSH, ACK] Seq=118 Ack=191 Win=28928 Len=32 TSval=617737 TSecr=9332219
13	26.493820975	10.42.0.1	10.42.0.58	TCP	66	34425 → 1209 [ACK] Seq=191 Ack=150 Win=29200 Len=0 TSval=9332286 TSecr=617737
14	26.493955577	10.42.0.1	10.42.0.58	TCP	173	34425 → 1209 [PSH, ACK] Seq=191 Ack=150 Win=29200 Len=107 TSval=9332286 TSecr=617737
15	26.494549042	10.42.0.58	10.42.0.1	TCP	66	1209 → 34425 [ACK] Seq=150 Ack=298 Win=28928 Len=0 TSval=617737 TSecr=9332286
16	26.694509444	10.42.0.58	10.42.0.1	TCP	238	1209 → 34425 [PSH, ACK] Seq=150 Ack=298 Win=28928 Len=172 TSval=617787 TSecr=9332286

**TCP는 웹이나 이메일과 같이 데이터가 정확하게 전달되어야 하는 통신에서 사용된다 !**

## (2) 네트워크 포렌식



```
Wireshark · Follow TCP Stream (tcp.stream eq 0) · ws1_2.pcapng

$Lock EXTENDEDPROTOCOLXUa`cq;KGq_Xkk3=jf0HOL3B0xUnix Pk=PtokaX|$Supports UserCommand NoGetINFO NoHello UserIP2 TTHSearch
ZPipe0 TLS|$Key .....A .....0A.C.0!...c.p3/%DCN000%/...u..pp0..'...p.|$ValidateNick codelec|$Supports ZPipe0 NoHello
UserCommand UserIP2|$GetPass|$MyPass BITSCTF{such_s3cure_much_w0w}$|Hello codelec|$LoggedIn codelec|$Version 1,0091|
$GetNickList|$MyINFO $ALL codelec <EiskaltDC++ V:2.2.9,M:A,H:0/1/0,S:3>$ $100 KiB/s.$14$|$ZOn|x.=.K..@.F...hQP...D!
1...Nyq....#.....9..Y]..&..C.....O. R|(...[...p..."`.... .W
..MK.P..I4..=...yD%.../0...,.....`..$A.u=Vj....1..B..Y$.0(..B...M.o./..@..$ZOn|x.S....s.WPq..Q...O ..O.V.,Q/
VHT..H.....<...n.....d..99..%E..

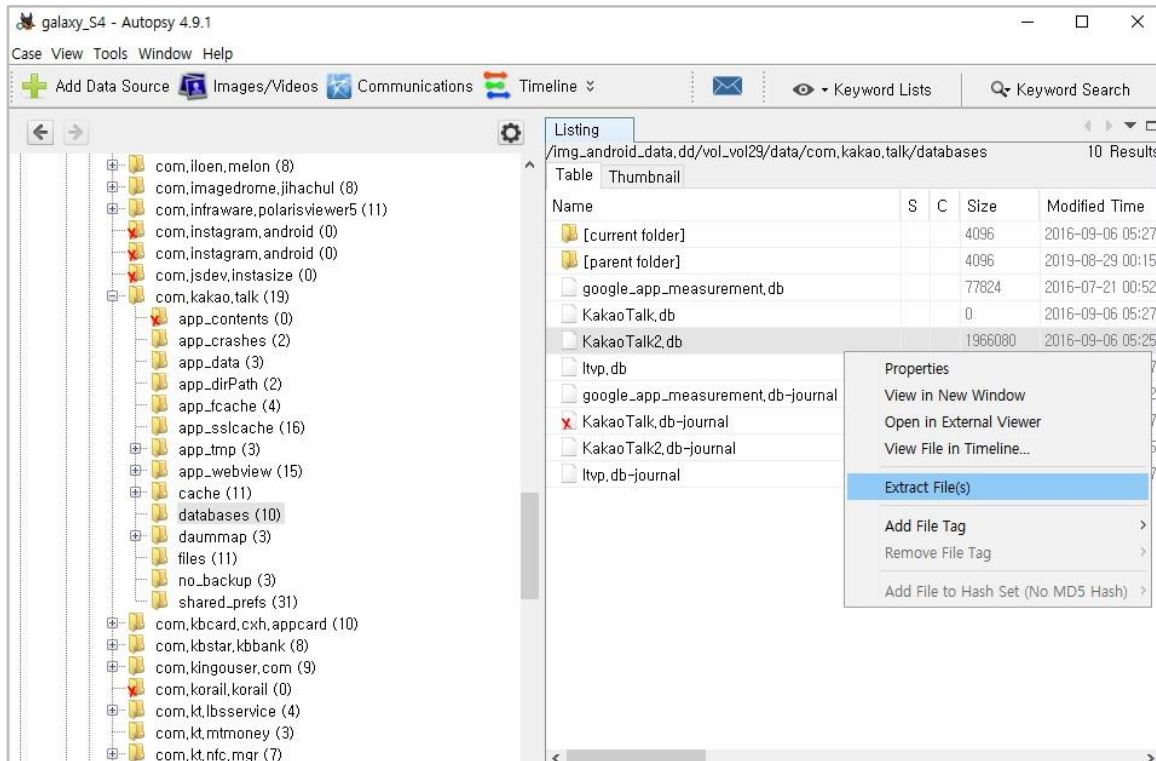
6.....9%....
aVFzFz.:.V.:.V.....:V.v@C...UT..L.L.,.,.
..LL.OI.IM&`.....<c.y...
..N..@C
MTj...7b$MyINFO $ALL Moshpit Get a Permit, Bitch !!!$ $.$$$|$OpList WoodStock$$illustris$$codelec$$Moshpit$$|$UserIP
illustris 127.0.0.1$$codelec 10.42.0.1$$|$ZOn|x..TM..0.=o ...rh...B..Pz.,J.lS.R(.=.E$......4 e..&:.C...h40.....{....p.
1.....-!2R....~....m ,....B....n..[.W..R).v!.^r..q....!....#}.....6@.^....*W..".F.. ...@..
+.*..x.N....#.R..<ML&X.Z.....&..'....g.Z0...|..5?(M3 ..#04...v.J..Q.....I. u.\.].}.;. ....r..
{...^...q.fz1...]s...<r.W..3..+..._.Io.u...F...q...#.Rn.../..h.V....D.Ci.....BSz.../..=.t..). ....^..F....]-.@.....y0.t3Enu.
..**N\Jm3Xm.&.....7...n6....6...#....>...E.R.-..Z...>...@.<zI.....}_..+....(..]WxUK.,....w!.H..}.:....
uEsW$MyINFO $ALL codelec <EiskaltDC++ V:2.2.9,M:A,H:0/0/1,S:3>$ $100 KiB/s.$14$|$MyINFO $ALL codelec <EiskaltDC++ V:
2.2.9,M:A,H:0/0/1,S:3>$ $100 KiB/s.$14$|$ConnectToMe codelec 127.0.0.1:3000|<illustris> codelec|<illustris> pm|$To: codelec
From: illustris $<illustris> I have the flag|$To: codelec From: illustris $<illustris> get it from my share|$MyINFO $ALL
illustris <EiskaltDC++ V:2.2.9,M:A,H:0/0/1,S:8>$ $20A$1329274863$|$ConnectToMe codelec 127.0.0.1:3000|$To: codelec From:
illustris $<illustris> fl3g.txt|$ConnectToMe illustris 10.42.0.1:3000|$ConnectToMe illustris 10.42.0.1:3000|$To: codelec
From: illustris $<illustris> Looks like your share|$To: codelec From: illustris $<illustris> has the flag too|$To: illustris
From: codelec $<codelec> looks like i do|$To: codelec From: illustris $<illustris> Damn... I don't want to start this pcap
over|$To: illustris From: codelec $<codelec> Lite. This will do |$To: codelec From: illustris $<illustris> If you say so|
```

TCP Stream : TCP Packet의 데이터 부분만 모아서 보기 쉽게 출력해준다

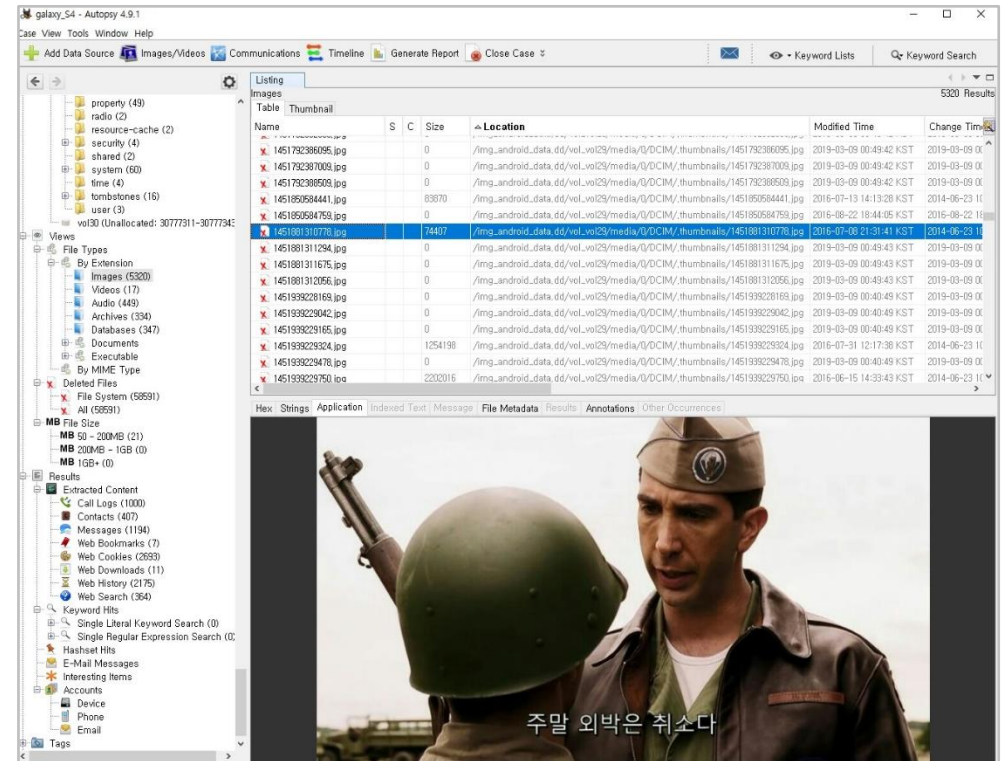
### (3) 모바일 포렌식

**모바일 기기**에 설치된 어플을 사용함으로써  
저장된 데이터를 수집 및 분석하는 기법

## (3) 모바일 포렌식



[카카오톡 데이터 추출]

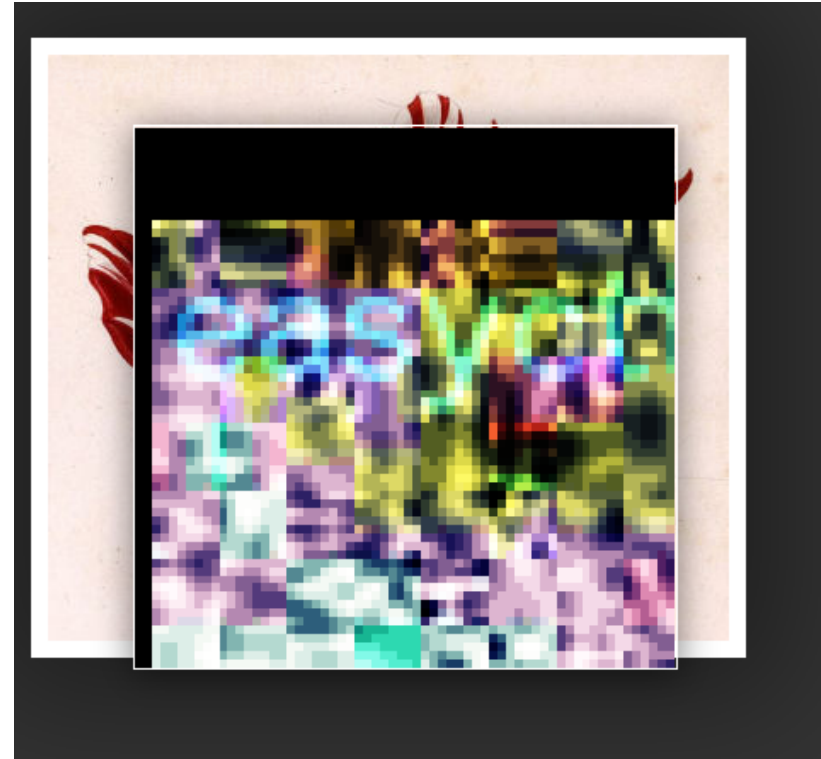


[삭제된 파일 복구]

### (4) 멀티미디어 포렌식

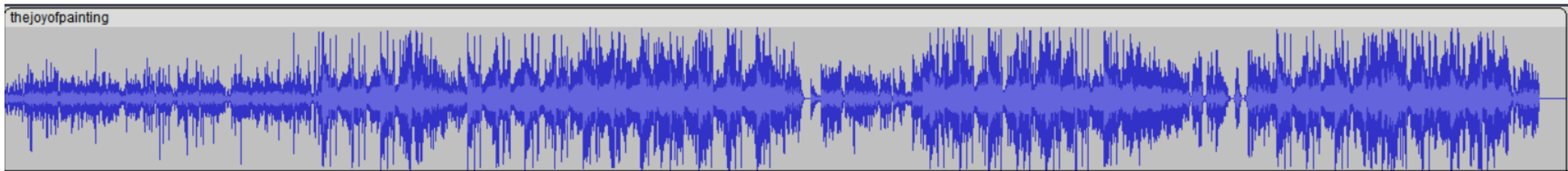
디지털 비디오, 오디오, 이미지 등의  
멀티미디어 데이터를 분석하는 기법

### (4) 멀티미디어 포렌식





## (4) 멀티미디어 포렌식





### (5) 안티 포렌식

디지털 포렌식 기술에 대응하여 자신에게 불리하게 작용할 가능성이 있는  
중요 데이터를 삭제하거나 파괴하는 기법

### (5) 안티 포렌식

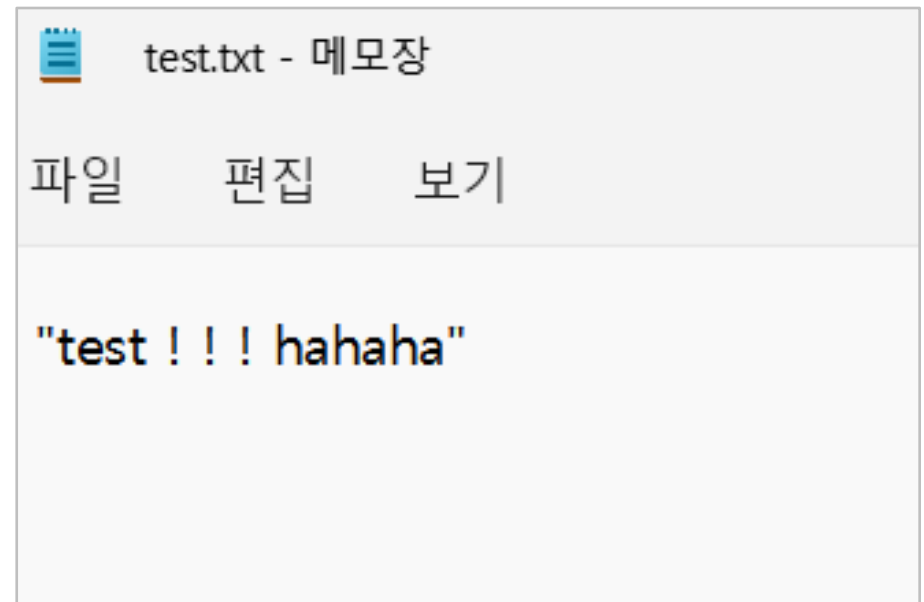
스테가노그래피 (Steganography)

: 일반적인 파일 안에 텍스트나 파일을 숨기는 기법

## (5) 안티 포렌식



[hacking.jpg]



[test.txt]

## (5) 안티 포렌식

The screenshot shows the OpenStego application window. The title bar reads 'OpenStego' with standard window controls. The menu bar contains 'File' and 'Help'. The interface is divided into two main sections: 'Data hiding' and 'Digital watermarking (Beta)'. The 'Data hiding' section has two buttons: 'Hide data' and 'Extract data'. The 'Digital watermarking (Beta)' section has three buttons: 'Generate signature', 'Embed watermark', and 'Verify watermark'. The 'Hide data' button is selected, and the 'Hide data in harmless looking files' panel is active. This panel contains three text input fields: 'Message file' (C:\Users\Wdjssl\OneDrive\바탕 화면\stegano\test.txt), 'Cover file' (C:\Users\Wdjssl\OneDrive\바탕 화면\stegano\hacking.jpg), and 'Output stego file' (C:\Users\Wdjssl\OneDrive\바탕 화면\stegano\hide). Below these is an 'Options' section with a dropdown for 'Encryption algorithm' set to 'AES128', and two password fields labeled 'Password' and 'Confirm password', both containing five black dots. A 'Hide data' button is at the bottom right.

Data hiding	Hide data in harmless looking files
Hide data	Message file C:\Users\Wdjssl\OneDrive\바탕 화면\stegano\test.txt
Extract data	Cover file (Select multiple files or provide wildcard (*, ?) to embed same message in multiple files) C:\Users\Wdjssl\OneDrive\바탕 화면\stegano\hacking.jpg
<b>Digital watermarking (Beta)</b>	Output stego file C:\Users\Wdjssl\OneDrive\바탕 화면\stegano\hide
Generate signature	Options
Embed watermark	Encryption algorithm AES128
Verify watermark	Password ●●●●●
	Confirm password ●●●●●
	Hide data

## (5) 안티 포렌식

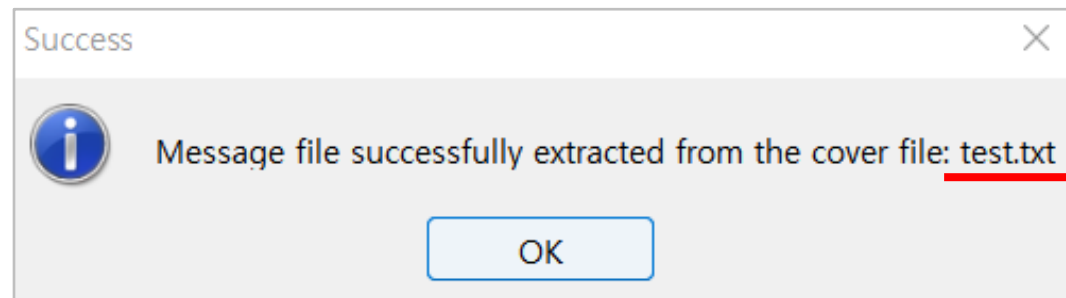
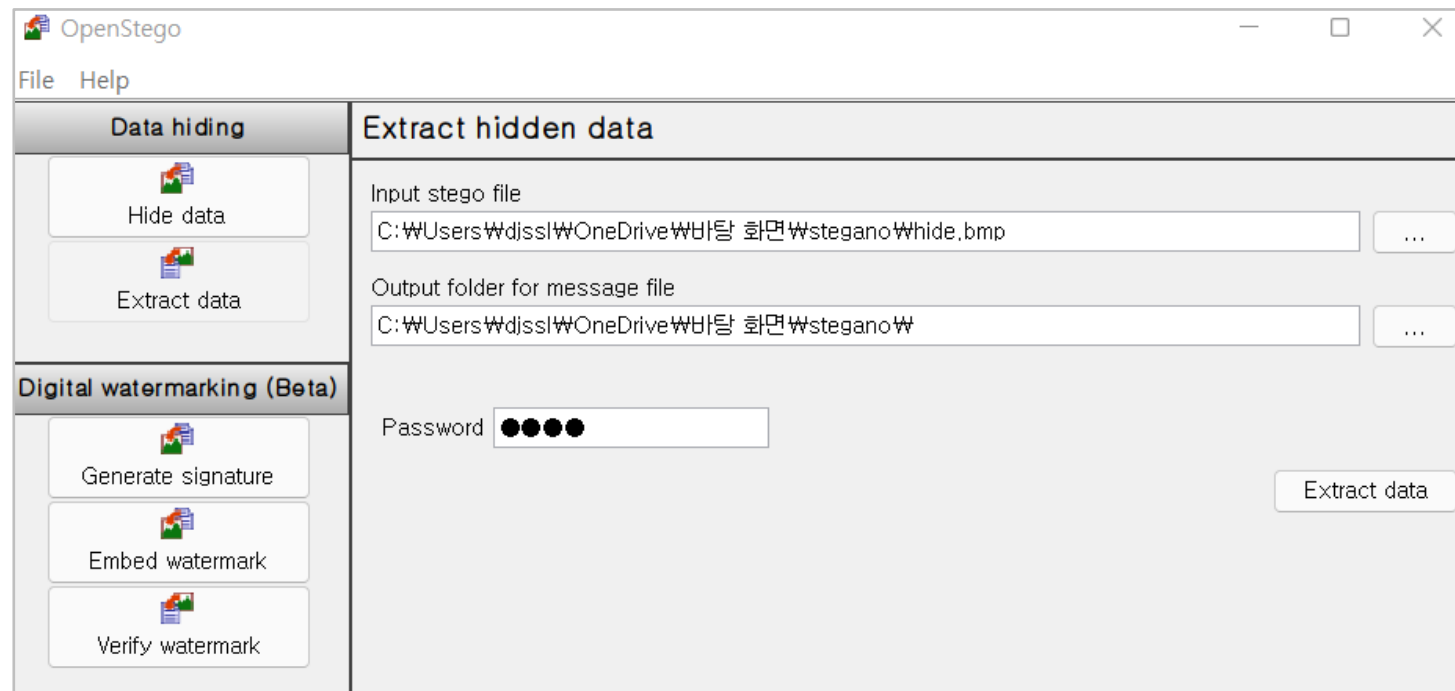


[hacking.jpg]



[hide.bmp]

## (5) 안티 포렌식



감사합니다 😊

SCP 이다영

An illustration of a hand holding a black smartphone. The screen of the phone displays the letters 'SCP' in a white, stylized, gothic-style font. The hand is light-skinned and is positioned on the left side of the phone, with fingers wrapped around it. The background is a solid blue color.

SCP