301 – Hidden Message

Team Information

Team Name : ISEGYE_IDOL

Team Member : Eungchang Lee, Sojeong Kim, Mingyu Seong, Donghyun HA

Email Address : dfc-isegyeidol@googlegroups.com

Instructions

Description An industrial spy trying to sell important semiconductor technology was arrested. During the investigation, suspicious image files sent through his e-mail were found. Investigators suspect that information about contact with the buyer (date, place, and password) may be hidden in the image files.

Target	Hash (MD5)
images.zip	3b30d77ed8fffcce2315cdbe2bd0b167

Questions

1. What date is the spy supposed to meet the buyer? (from 'cosmos.bmp' file) (75 points)
2. Where is the spy supposed to meet with the buyer? (from 'nightview.png' file) (100 points)
3. What is the password? (from 'white.gif' file) (125 points)

Teams must:

- Develop and document the step-by-step approach used to solve this problem to allow another examiner to replicate team actions and results.
- Specify all tools used in deriving the conclusion(s).

Tools used:

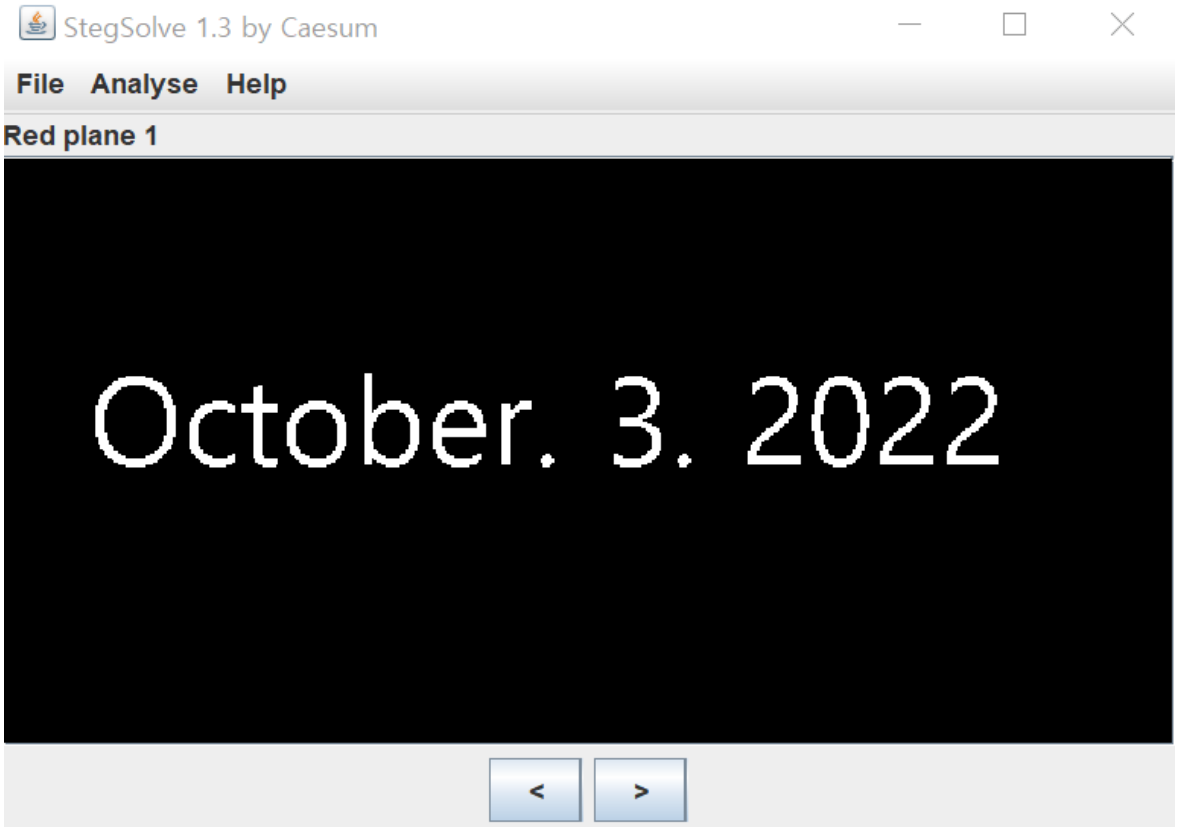
Name:	Stegsolve.jar	Publisher:	caesum
Version:	1.3		
URL:	http://www.caesum.com/handbook/Stegsolve.jar		

Name:	TweakPNG	Publisher:	Jason Summers
Version:	1.4.6		
URL:	http://entropymine.com/jason/tweakpng/		

Name:	HxD	Publisher:	Maël Hörz
Version:	2.5.0.0		
URL:	https://www.mh-nexus.de		

Step-by-step methodology:

1. What date is the spy supposed to meet the buyer? (from 'cosmos.bmp' file)
'cosmos.bmp' 파일을 stegsolve.jar을 사용하여 분석하였다.



[그림 1] stegsolve.jar, Red plane 1

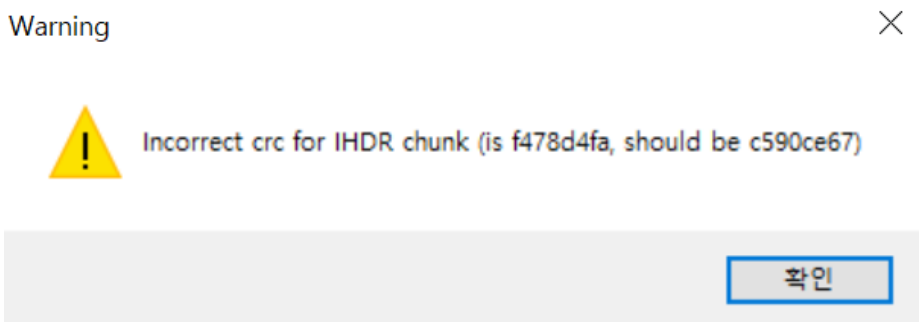
Red plane 1에서 날짜 정보를 확인할 수 있다.

October. 3. 2022.

2. Where is the spy supposed to meet with the buyer? (from 'nightview.png' file)

'nightview.png' 파일을 tweakpng.exe 도구로 분석하였다.

tweakpng.exe에서 nightview.png을 처음 불러올 때 아래와 같은 경고창이 표시된다.



[그림 2] tweakpng.exe에서 nightview.png 파일을 처음 불러올 때 표시되는 경고 창

IHDR chunck에 대한 CRC값이 잘못되어 있는 것을 확인할 수 있다.

IHDR에는 이미지 width, height, bit depth, color 값이 포함되어 있는데, 이 중 이미지 크기 값이 수정되어 누락된 이미지 부분에 스파이가 바이어를 만나는 장소에 대한 정보가 숨겨져 있을 것으로 보았다. 따라서 현재 CRC 값인 0xf478d4fa로 계산되어 나오는 올바른 이미지 크기를 찾는 파이썬 코드를 작성하여 실행하였다.

```
import binascii
import struct

misc = open("./nightview.png","rb").read()

for i in range(3000):
    for j in range(3000):
        data = misc[12:16] + struct.pack('>i',i)+ struct.pack('>i',j)+ misc[24:29]
        crc32 = binascii.crc32(data) & 0xffffffff
        if crc32 == 0xf478d4fa:
            print(i,j)
```

[그림 3] 올바른 이미지 크기 값을 찾기 위한 코드, bf_crc.py

```
mandu@mandu-VirtualBox:~/Desktop/p/PNG$ python3 bf_crc.py
512 512
```

[그림 4] 실행 결과

그 결과 512 * 512라는 결과가 나왔으며 tweakpng.exe를 사용하여 이미지 크기를 수정해 주었다.

이후 이미지 뷰어를 사용하여 nightview.png 파일을 확인해보면, 하단 부분에서 정보를 획득할 수 있다.

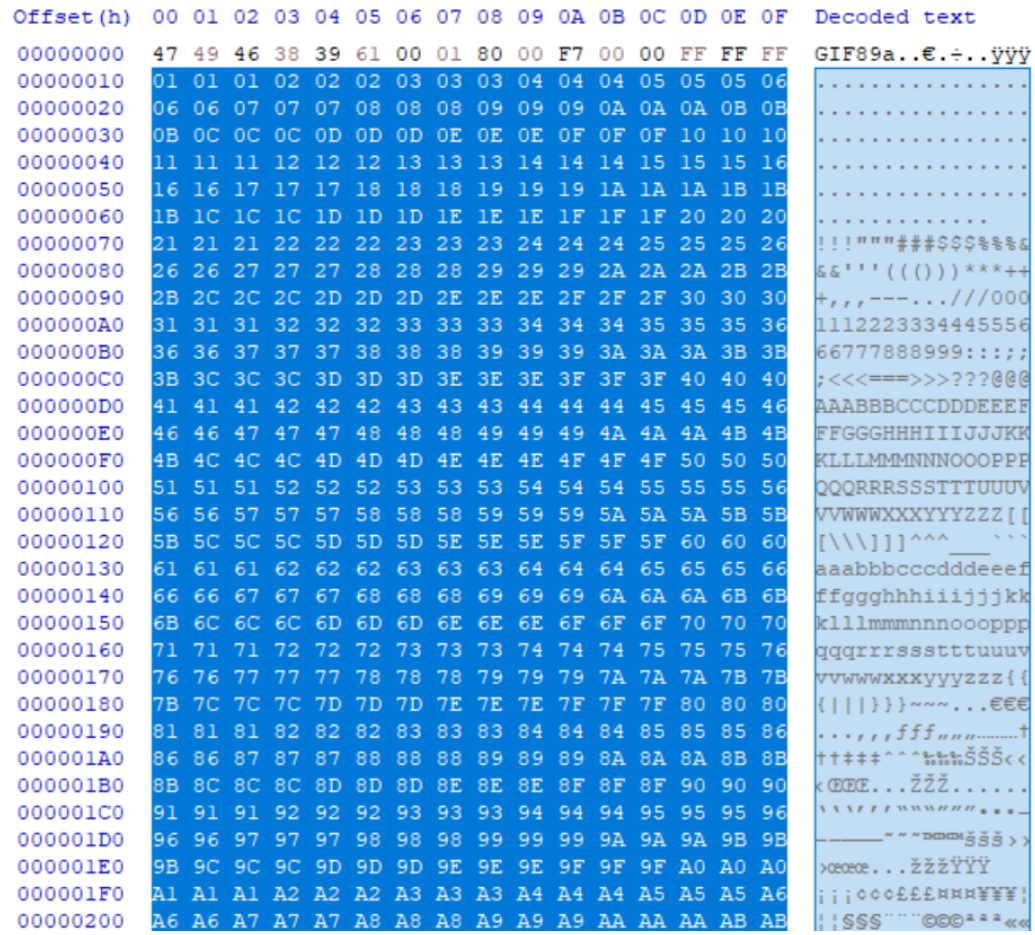
Nara Hotel, Seoul

[그림 5] 이미지 크기가 수정된 이미지

Nara Hotel, Seoul

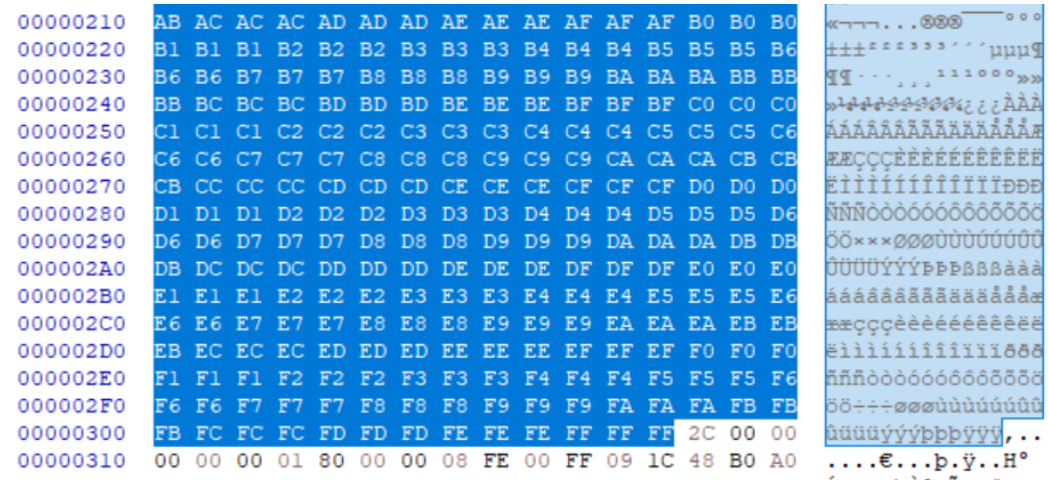
3. What is the password? (from 'white.gif' file)

'white.gif' 파일을 HxD를 사용하여 분석하였다.



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	47	49	46	38	39	61	00	01	80	00	F7	00	00	FF	FF	FF	GIF89a..€.÷..ÿÿÿ
00000010	01	01	01	02	02	02	03	03	03	04	04	04	05	05	05	06	.....
00000020	06	06	07	07	07	08	08	08	09	09	09	0A	0A	0A	0B	0B	.....
00000030	0B	0C	0C	0C	0D	0D	0D	0E	0E	0E	0F	0F	0F	10	10	10	.....
00000040	11	11	11	12	12	12	13	13	13	14	14	14	15	15	15	16	.....
00000050	16	16	17	17	17	18	18	18	19	19	19	1A	1A	1A	1B	1B	.....
00000060	1B	1C	1C	1C	1D	1D	1D	1E	1E	1E	1F	1F	1F	20	20	20	.....
00000070	21	21	21	22	22	22	23	23	23	24	24	24	25	25	25	26	!!!"""###$$$%%%&
00000080	26	26	27	27	27	28	28	28	29	29	29	2A	2A	2A	2B	2B	&&'''((()))***++
00000090	2B	2C	2C	2C	2D	2D	2D	2E	2E	2E	2F	2F	2F	30	30	30	+,,,---.../// 000
000000A0	31	31	31	32	32	32	33	33	33	34	34	34	35	35	35	36	111222333444555 6
000000B0	36	36	37	37	37	38	38	38	39	39	39	3A	3A	3A	3B	3B	66777888999:::;;
000000C0	3B	3C	3C	3C	3D	3D	3D	3E	3E	3E	3F	3F	3F	40	40	40	;<<<===>>>???@@@
000000D0	41	41	41	42	42	42	43	43	43	44	44	44	45	45	45	46	AAABBBCCCDDDEEEF
000000E0	46	46	47	47	47	48	48	48	49	49	49	4A	4A	4A	4B	4B	FFGGGHHHIIIJJJKK
000000F0	4B	4C	4C	4C	4D	4D	4D	4E	4E	4E	4F	4F	4F	50	50	50	KLLLMMMNNNOOOPPP
00000100	51	51	51	52	52	52	53	53	53	54	54	54	55	55	55	56	QQQRRRSSSTTTUUUV
00000110	56	56	57	57	57	58	58	58	59	59	59	5A	5A	5A	5B	5B	VVWWWXXXYYYZZZ[[
00000120	5B	5C	5C	5C	5D	5D	5D	5E	5E	5E	5F	5F	5F	60	60	60	[\\\]]]^^^___```
00000130	61	61	61	62	62	62	63	63	63	64	64	64	65	65	65	66	aaabbbcccdddeeef
00000140	66	66	67	67	67	68	68	68	69	69	69	6A	6A	6A	6B	6B	ffgggghhhiiijjjkk
00000150	6B	6C	6C	6C	6D	6D	6D	6E	6E	6E	6F	6F	6F	70	70	70	klllmmmnnnooopppp
00000160	71	71	71	72	72	72	73	73	73	74	74	74	75	75	75	76	qqqrrrssstttuuuv
00000170	76	76	77	77	77	78	78	78	79	79	79	7A	7A	7A	7B	7B	vvwwwxxxyyyzzz{{
00000180	7B	7C	7C	7C	7D	7D	7D	7E	7E	7E	7F	7F	7F	80	80	80	{|||}}}~~~...€€€
00000190	81	81	81	82	82	82	83	83	83	84	84	84	85	85	85	86	...,,,fff„„„……†
000001A0	86	86	87	87	87	88	88	88	89	89	89	8A	8A	8A	8B	8B	††‡‡‡ˆˆˆ‰‰‰ŠŠŠ‹‹
000001B0	8B	8C	8C	8C	8D	8D	8D	8E	8E	8E	8F	8F	8F	90	90	90	‹ŒŒŒ...ŽŽŽ.....
000001C0	91	91	91	92	92	92	93	93	93	94	94	94	95	95	95	96	‘‘‘’’’“““”””•••–
000001D0	96	96	97	97	97	98	98	98	99	99	99	9A	9A	9A	9B	9B	––—˜˜˜™™™šššsss››
000001E0	9B	9C	9C	9C	9D	9D	9D	9E	9E	9E	9F	9F	9F	A0	A0	A0	›œœœ...žžžŸŸŸ
000001F0	A1	A1	A1	A2	A2	A2	A3	A3	A3	A4	A4	A4	A5	A5	A5	A6	¡¡¡¢¢¢£££¤¤¤¥¥¥¦
00000200	A6	A6	A7	A7	A7	A8	A8	A8	A9	A9	A9	AA	AA	AA	AB	AB	¦¦§§§¨¨¨©©©ª ª ª««

[그림 6] white.gif 0x0 ~ 0x200 영역



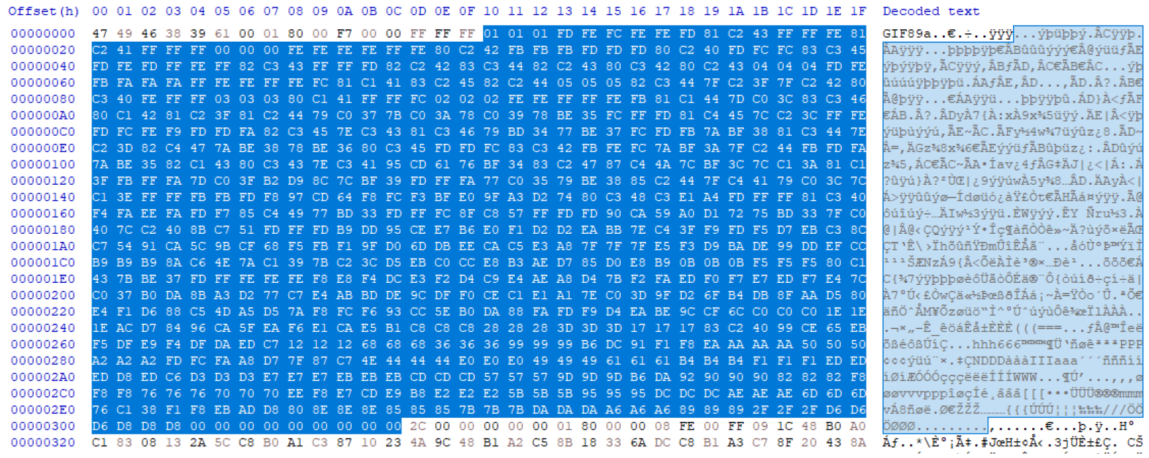
00000210	AB	AC	AC	AC	AD	AD	AD	AE	AE	AE	AF	AF	AF	B0	B0	B0	«¬¬¬...®®®¯¯¯°°°
00000220	B1	B1	B1	B2	B2	B2	B3	B3	B3	B4	B4	B4	B5	B5	B5	B6	±±±²²²³³³´´´µµµ¶
00000230	B6	B6	B7	B7	B7	B8	B8	B8	B9	B9	B9	BA	BA	BA	BB	BB	¶¶···¸¸¸¹¹¹ººº»»
00000240	BB	BC	BC	BC	BD	BD	BD	BE	BE	BE	BF	BF	BF	C0	C0	C0	»¼¼¼½½½¾¾¾¿¿¿ÀÀÀ
00000250	C1	C1	C1	C2	C2	C2	C3	C3	C3	C4	C4	C4	C5	C5	C5	C6	ÁÁÁÂÂÂÃÃÃÄÄÄÅÅÅÆ
00000260	C6	C6	C7	C7	C7	C8	C8	C8	C9	C9	C9	CA	CA	CA	CB	CB	ÆÆÇÇÇÈÈÈÉÉÉÊÊÊËË
00000270	CB	CC	CC	CC	CD	CD	CD	CE	CE	CE	CF	CF	CF	D0	D0	D0	ËÌÌÌÍÍÍÎÎÎÏÏÏÐÐÐ
00000280	D1	D1	D1	D2	D2	D2	D3	D3	D3	D4	D4	D4	D5	D5	D5	D6	ÑÑÑÒÒÒÓÓÓÔÔÔÕÕÕÖ
00000290	D6	D6	D7	D7	D7	D8	D8	D8	D9	D9	D9	DA	DA	DA	DB	DB	ÖÖ×××ØØØÙÙÙÚÚÚÛÛ
000002A0	DB	DC	DC	DC	DD	DD	DD	DE	DE	DE	DF	DF	DF	E0	E0	E0	ÛÜÜÜÝÝÝÞÞÞßßßààà
000002B0	E1	E1	E1	E2	E2	E2	E3	E3	E3	E4	E4	E4	E5	E5	E5	E6	áááâââãããäääåååæ
000002C0	E6	E6	E7	E7	E7	E8	E8	E8	E9	E9	E9	EA	EA	EA	EB	EB	æææçççèèèéééêêêëë
000002D0	EB	EC	EC	EC	ED	ED	ED	EE	EE	EE	EF	EF	EF	F0	F0	F0	ëìììíííîîîïïïðððð
000002E0	F1	F1	F1	F2	F2	F2	F3	F3	F3	F4	F4	F4	F5	F5	F5	F6	ñññòòòóóóôôôõõõö
000002F0	F6	F6	F7	F7	F7	F8	F8	F8	F9	F9	F9	FA	FA	FA	FB	FB	öö÷÷÷øøøùùùúúúûû
00000300	FB	FC	FC	FC	FD	FD	FD	FE	FE	FE	FF	FF	FF	2C	00	00	ûüüüýýýþþþÿÿÿ,..
00000310	00	00	00	01	80	00	00	08	FE	00	FF	09	1C	48	B0	A0	....€...þ.ÿ..H°

[그림 7] white.gif 0x210 ~ 0x31F 영역

GIF의 color table 영역의 일부인 0x10 ~ 0x30c 영역이 0x01, 0x01, 0x01 ~ 0xff, 0xff, 0xff 의 형태로

덮어 쓰여진 것으로 보인다.

해당 영역을 복구하기 위해서 정상 gif의 동일한 영역을 덮어썼다.



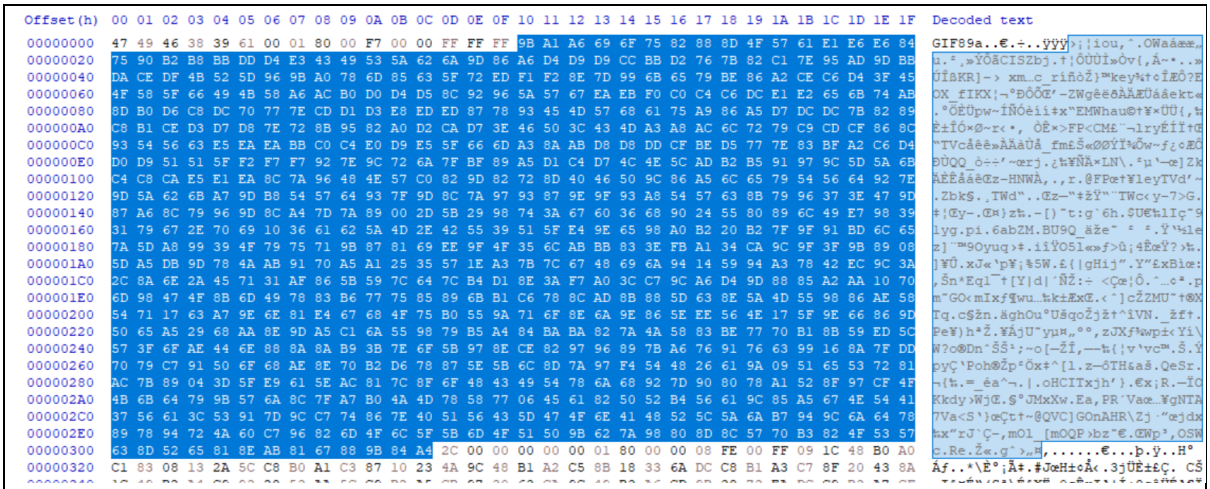
[그림 8] 정상 데이터로 복구한 영역

[그림 9] 이미지 확인

그 결과, PW를 확인할 수 있었다.

P/W : GeKE102

다른 정상 gif의 color table을 영역을 가져와 덮어 쓴 경우에도 배경의 색상만 다를 뿐 PW를 식별하는 데에는 문제가 없음을 확인했다.



```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F  Decoded text
00000000   47 49 46 38 39 61 00 01 80 00 F7 00 00 FF FF FF 9B A1 A6 69 6F 75 82 88 8D 4F 57 61 E1 E6 E6 84  GIF89a..€.÷..ÿÿÿ›¡¦iou‚ˆ.OWaáææ„
00000020   75 90 B2 B8 BB DD D4 E3 43 49 53 5A 62 6A 9D 86 A6 D4 D9 D9 CC BB D2 76 7B 82 C1 7E 95 AD 9D BB  u.²¸»ÝÔãCISZbj.†¦ÔÙÙÌ»Òv{‚Á~•..»
00000040   DA CE DF 4B 52 5D 96 9B A0 78 6D 85 63 5F 72 ED F1 F2 8E 7D 99 6B 65 79 BE 86 A2 CE C6 D4 3F 45  ÚÎßKR]–› xm…c_ríñòŽ}™key¾†¢ÎÆÔ?E
00000060   4F 58 5F 66 49 4B 58 A6 AC B0 D0 D4 D5 8C 92 96 5A 57 67 EA EB F0 C0 C4 C6 DC E1 E2 65 6B 74 AB  OX_fIKX¦¬°ÐÔÕŒ'–ZWgêëðÀÄÆÜáâekt«
00000080   8D B0 D6 C8 DC 70 77 7E CD D1 D3 E8 ED ED 87 78 93 45 4D 57 68 61 75 A9 86 A5 D7 DC DC 7B 82 89  .°ÖÈÜpw~ÍÑÓèíi‡x"EMWhau©†¥×ÜÜ{‚‰
000000A0   C8 B1 CE D3 D7 D8 7E 72 8B 95 82 A0 D2 CA D7 3E 46 50 3C 43 4D A3 A8 AC 6C 72 79 C9 CD CF 86 8C  È±ÎÓ×Ø~r‹•‚ ÒÊ×>FP<CM£¨¬lryÉÍÏ†Œ
000000C0   93 54 56 63 E5 EA EA BB C0 C4 E0 D9 E5 5F 66 6D A3 8A AB D8 DD CF BE D5 77 7E 83 BF A2 C6 D4  "TVcåêê»ÀÄàÙå_fm£Š«ØÝÏ¾Õw~ƒ¿¢ÆÔ
000000E0   D0 D9 51 51 5F F2 F7 F7 92 7E 9C 72 6A 7F BF 89 A5 D1 C4 D7 4C 4E 5C AD B2 B5 91 97 9C 5D 5A 6B  ÐÙQQ_ò÷÷'~œrj.¿‰¥ÑÄ×LN\.²µ'—œ]Zk
00000100   C4 C8 CA E5 E1 EA 8C 7A 96 48 4E 57 C0 82 9D 82 72 8D 40 46 50 9C 86 A5 6C 65 79 54 56 64 92 7E  ÄÈÊåáêŒz–HNWÀ‚.‚r.@FPœ†¥leyTVd'~
00000120   9D 5A 62 6B A7 9D B8 54 57 64 93 7F 9D 8C 7A 97 93 87 9E 9F 93 A8 54 57 63 8B 79 96 37 3E 47 9D  .Zbk§.¸TWd"..Œz—"‡žŸ"¨TWc‹y–7>G.
00000140   87 A6 8C 79 96 9D 8C A4 7D 7A 89 00 2D 5B 29 98 74 3A 67 60 36 68 90 24 55 80 89 6C 49 E7 98 39  ‡¦Œy–.Œ¤}z‰.-[)˜t:g`6h.$U€‰lIç˜9
00000160   31 79 67 2E 70 69 10 36 61 62 5A 4D 2E 42 55 39 51 5F E4 9E 65 98 A0 B2 20 B2 7F 9F 91 BD 6C 65  1yg.pi.6abZM.BU9Q_äže˜ ² ².Ÿ‘½le
00000180   7A 5D A8 99 39 4F 79 75 71 9B 87 81 69 EE 9F 4F 35 6C AB BB 83 3E FB A1 34 CA 9C 9F 3F 9B 89 08  z]¨™9Oyuq›‡.iîŸO5l«»ƒ>û¡4ÊœŸ?›‰.
000001A0   5D A5 DB 9D 78 4A AB 91 70 A5 A1 25 35 57 1E A3 7B 7C 67 48 69 6A 94 14 59 94 A3 78 42 EC 9C 3A  ]¥Û.xJ«'p¥¡%5W.£{|gHij".Y"£xBìœ:
000001C0   2C 8A 6E 2A 45 71 31 AF 86 5B 59 7C 64 7C B4 D1 8E 3A F7 A0 3C C7 9C A6 D4 9D 88 85 A2 AA 10 70  ,Šn*Eq1¯†[Y|d|´ÑŽ:÷ <Çœ¦Ô.ˆ…¢ª.p
000001E0   6D 98 47 4F 8B 6D 49 78 83 B6 77 75 85 89 6B B1 C6 78 8C AD 8B 88 5D 63 8E 5A 4D 55 98 86 AE 58  m˜GO‹mIxƒ¶wu…‰k±ÆxŒ.‹ˆ]cŽZMU˜†®X
00000200   54 71 17 63 A7 9E 6E 81 E4 67 68 4F 75 B0 55 9A 71 6F 8E 6A 9E 86 5E EE 56 4E 17 5F 9E 66 86 9D  Tq.c§žn.äghOu°UšqoŽjž†^îVN._žf†.
00000220   50 65 A5 29 68 AA 8E 9D A5 C1 6A 55 98 79 B5 A4 84 BA BA 82 7A 4A 58 83 BE 77 70 B1 8B 59 ED 5C  Pe¥)hªŽ.¥ÁjU˜yµ¤„ºº‚zJXƒ¾wp±‹Yí\
00000240   57 3F 6F AE 44 6E 88 8A 8A B9 3B 7E 6F 5B 97 8E CE 82 97 96 89 7B A6 76 91 76 63 99 16 8A 7F DD  W?o®Dnˆ‰Š¹;~o[—ŽÎ‚—–‰{¦v'vc™.Š.Ý
00000260   70 79 C7 91 50 6F 68 AE 8E 70 B2 D6 78 87 5E 5B 6C 8D 7A 97 F4 54 48 26 61 9A 09 51 65 53 72 81  pyÇ'Poh®Žp²Öx‡^[l.z—ôTH&aš.QeSr.
00000280   AC 7B 89 04 3D 5F E9 61 5E AC 81 7C 8F 6F 48 43 49 54 78 6A 68 92 7D 90 80 78 A1 52 8F 97 CF 4F  ¬{‰.=_éa^¬.|.oHCITxjh'}.€x¡R.—ÍO
000002A0   4B 6B 64 79 9B 57 6A 8C 7F A7 B0 4A 4D 78 58 77 06 45 61 82 50 52 B4 56 61 9C 85 A5 67 4E 54 41  Kkdy›WjŒ.§°JMxXw.Ea‚PR´Vaœ…¥gNTA
000002C0   37 56 61 3C 53 91 7D 9C C7 74 86 7E 40 51 56 43 5D 47 4F 6E 41 48 52 5C 5A 6A B7 94 9C 6A 64 78  7Va<S'}œÇt†~@QVC]GOnAHR\Zj·"œjdx
000002E0   89 78 94 72 4A 60 C7 96 82 6D 4F 6C 5F 5B 6D 4F 51 50 9B 62 7A 98 80 8D 8C 57 70 B3 82 4F 53 57  ‰x"rJ`Ç–‚mOl_[mOQP›bz˜€.ŒWp³‚OSW
00000300   63 8D 52 65 81 8E AB 81 67 88 9B 84 A4 2C 00 00 00 00 00 01 80 00 00 08 FE 00 FF 09 1C 48 B0 A0  c.Re.Ž«.g^›„¤,.....€...þ.ÿ..H°
00000320   C1 83 08 13 2A 5C C8 B0 A1 C3 87 10 23 4A 9C 48 B1 A2 C5 8B 18 33 6A DC C8 B1 A3 C7 8F 20 43 8A  Áƒ..*\È°¡Ã‡.#JœH±¢Å‹.3jÜȱ£Ç. CŠ
```

[그림 9] 다른 정상 gif의 color table로 복구

[그림 10] 이미지 식별