

[xcz.kr] Prob1 - End Of Image

문제 풀이

중부대 SCP 정보보안 동아리
92113566 1학년 부원 노무승

목차

1. 문제 풀이

2. 개념 확장

1. 문제 풀이

1-1. 문제 다운로드

Title

End Of Image

Description



새 탭에서 이미지 열기


이미지를 다른 이름으로 저장...

이미지 복사

이미지 주소 복사

이 이미지의 QR 코드 생성

Google에서 이미지 검색

 구성 요소 차단

검사

Ctrl+Shift+I

1-2. 헤더 시그니처 탐색

HxD - [D:\Setting\whysoserious.png]

16 Windows (ANSI) 16진수

파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 도구(T) 창 설정(W) 도움말(H)

whysoserious.png

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG.....IHDR
00000010	00	00	02	BC	00	00	01	5E	08	02	00	00	00	E8	BC	5B	...^.....è[
00000020	00	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00sRGB.®.é..
00000030	00	04	67	41	4D	41	00	00	B1	8F	0B	FC	61	05	00	00	..gAMA...±...üa...
00000040	00	09	70	48	59	73	00	00	0E	C3	00	00	0E	C3	01	C7	..pHYs...Ä...Ä.Ç
00000050	6F	A8	64	00	00	FF	A5	49	44	41	54	78	5E	EC	FD	85	o`d...ÿIDATx^ìý...
00000060	9F	1C	E7	B5	EE	8B	DF	7F	E1	77	3F	BF	7B	EE	D9	67	ÿ.çûî<ß.áw?ç{îÛg

파일의 바이너리를 열어보면 PNG 파일의 **헤더 시그니처**가 보인다.

1-3. PNG 파일 시그니처

PNG	89 50 4E 47 0D 0A 1A 0A P N G	49 45 4E 44 AE 42 60 82 I E N D B `	Portable Network Graphics Format
-----	-------------------------------------	---	-------------------------------------



FORENSIC-PROOF

*Incident Investigation
and Response*

PNG 파일의 헤더 시그니처와 푸터 시그니처를 보자.

1-3. PNG 파일 시그니처

PNG	89 50 4E 47 0D 0A 1A 0A P N G	49 45 4E 44 AE 42 60 82 I E N D B `	Portable Network Graphics Format
-----	-------------------------------------	---	-------------------------------------

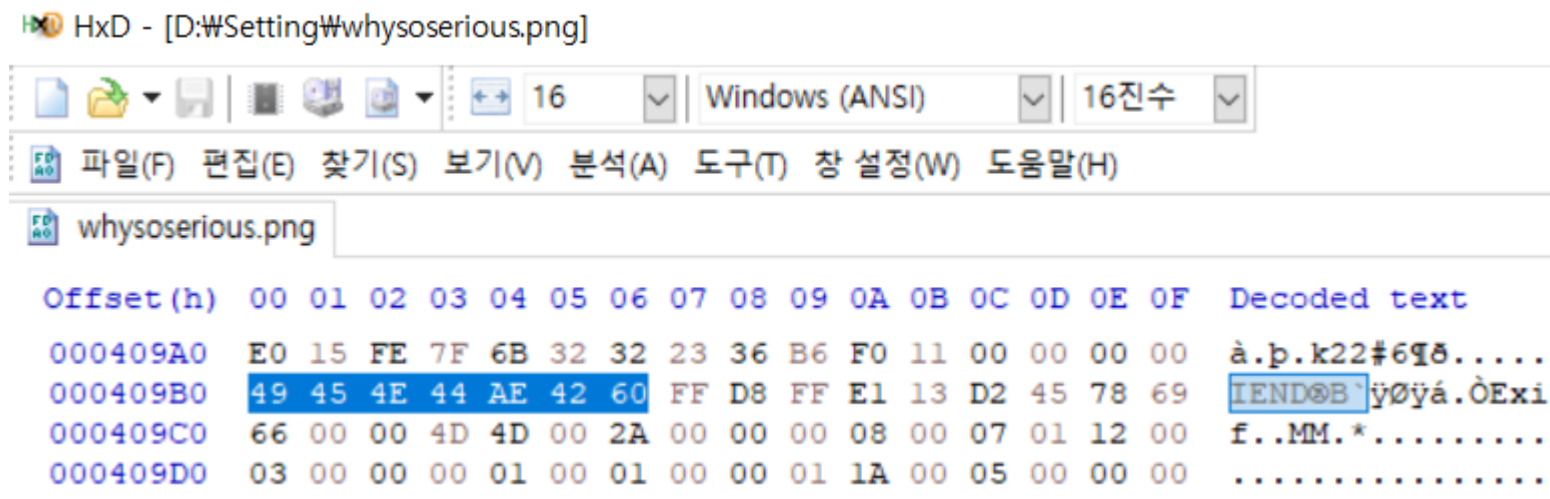


FORENSIC-PROOF

*Incident Investigation
and Response*

PNG 파일의 헤더 시그니처와 푸터 시그니처를 보자.

1-4. 푸터 시그니처 탐색



PNG 파일의 푸터 시그니처를 보면 뒤에 뭔가 데이터가 더 있다.

1-5. JPG 파일 시그니처

FF D8 FF E1

×

전체

동영상

이미지

뉴스

쇼핑

더보기

도구

검색결과 약 28,600,000개 (0.43초)

도움말: [한국어](#) 검색결과만 검색합니다. 환경설정에서 검색 언어를 지정할 수 있습니다.

<http://forensic-proof.com> > archives ▾

[파일 시그니처 모음 \(Common File Signatures\) - FORENSIC ...](#)

2009. 10. 23. — JPEG의 경우 디지털카메라로 캡처한 파일과 구분하기 위해 “FF D8 FF E1” 시그니처도 사용한다. 파일 시그니처는 파일의 처음에만 존재하는 파일 포맷도 ...

JPEG/JFIF	FF D8 FF E0 xx xx 4A 46 49 46	FF D9	JPEG/JFIF Format
JPEG/EXIF	FF D8 FF E8 xx xx 45 78 69 66	FF D9	JPEG/Exif Format – Digital Camera Exchangeable File Format

JPG 파일의 헤더 시그니처와 푸터 시그니처를 보자.

1-6. 해석

아 저 파일은 PNG 파일 뒤에
JPG 파일이 또 있는 구조구나.

앞에 있는 파일이 표면적으로 보이는 이미지이기 때문에
뒤에 있는 이미지를 가져와보자.

1-7. 010 Editor을 이용한 방법

whysoserious.png ×

0123456789ABCDEF

0000h: 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 %PNG.....IHDR

0010h: 00 00 02 BC 00 00 01 5E 08 02 00 00 00 E8 BC 5B ...¼...^.....è¼[

0020h: 00 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00sRGB.ëĬ.é..

0030h: 00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00 ..gAMA...±...üa...

0040h: 00 09 70 48 59 73 00 00 0E C3 00 00 0E C3 01 C7 ..pHYs...Ä...Ä.C

0050h: 6F A8 64 00 00 FF A5 49 44 41 54 78 5E EC FD 85 o"d...ÿ¥IDATx^ìý...

0060h: 9F 1C E7 B5 EE 8B DF 7F E1 77 3F BF 7B EE D9 67 Ÿ.çµî<ß.áw?¿{îÛg

0070h: 43 12 C7 20 8B 59 C3 CC CC 3C 23 66 66 18 69 C4 C.Ç <YÄÏì<#ff.iÄ

0080h: 30 D2 48 1A 66 6A 66 EE 21 49 96 21 71 D0 89 19 00H.fjfi!I-!qĐ%.

0090h: C4 D2 48 1A 49 86 BD F7 39 49 6C B1 EE F7 AD 77 Ä0H.I†½÷9Il±î÷-w

00A0h: A6 3D 92 21 0E 38 60 77 67 A5 5C 5D 5D 5D DD 5D '= '!.8`wg¥\]]]Ý]

00B0h: FA F9 F5 D4 B3 9F F5 AC FF FB 91 FF F6 3F 03 FF âóôô3žö-ÿö'ÿn? h

Template Results - PNG.bt ↗

Name	Value	Start	Size	Color	Comment
> struct PNG_SIGNATURE sig		0h	8h	Fg: Bg:	
> struct PNG_CHUNK chun...	IHDR (Critical, ...	8h	19h	Fg: Bg:	
> struct PNG_CHUNK chun...	sRGB (Ancillar...	21h	Dh	Fg: Bg:	

010 Editor을 이용한 분석 방법도 존재.

1-8. 010 Editor을 이용한 방법

4:09A0h: E0 15 FE 7F 6B 32 32 23 36 B6 F0 11 00 00 00 00

4:09B0h: 49 45 4E 44 AE 42 60 FF D8 FF E1 13 D2 45 78 69

4:09C0h: 66 00 00 4D 4D 00 2A 00 00 00 08 00 07 01 12 00

4:09D0h: 03 00 00 00 01 00 01 00 00 01 1A 00 05 00 00 00

4:09E0h: 01 00 00 00 62 01 1B 00 05 00 00 00 01 00 00 00

4:09F0h: 6A 01 28 00 03 00 00 00 01 00 02 00 00 01 31 00

4:0A00h: 02 00 00 00 1F 00 00 00 72 01 32 00 02 00 00 00

à.þ.k22#6¶ð.

IEND@B`ÿøÿá.ÏExi

f..MM.*

.....

....b.....

j.(.....1.

r ?

Template Results - PNG.bt ↻

Name	Value	Start	Size	Color	Comment
> struct PNG_CHUNK chunk[3]	pHYs (Anc...	3Eh	15h	Fg: Bg:	
> struct PNG_CHUNK chunk[4]	IDAT (Criti...	53h	FFB1h	Fg: Bg:	
> struct PNG_CHUNK chunk[5]	IDAT (Criti...	10004h	10000h	Fg: Bg:	
> struct PNG_CHUNK chunk[6]	IDAT (Criti...	20004h	10000h	Fg: Bg:	
> struct PNG_CHUNK chunk[7]	IDAT (Criti...	30004h	10000h	Fg: Bg:	
> struct PNG_CHUNK chunk[8]	IDAT (Criti...	40004h	9A8h	Fg: Bg:	
> struct PNG_CHUNK chunk[9]	IEND (Crit...	409ACh	Ch	Fg: Bg:	

파일의 구조체를 보여줘서 분석이 쉬움.

1-9. 두 번째 이미지, 데이터 복사


The screenshot shows the HxD hex editor interface. The title bar indicates the file path is [D:\Setting\whyserious.png]. The menu bar includes File (F), Edit (E), Search (S), View (V), Analysis (A), Tools (T), Window (W), and Help (H). The toolbar shows icons for file operations and a status bar indicating 16 bytes per line and Windows (ANSI) encoding. The main display shows a hex dump of the file 'whyserious.png'. The 'Decoded text' column shows the following string: 'à.p.k22#698..... IEND' followed by a BOM (EF BB BF) and the Korean text 'yöyá.ÖExi'. The 'IEND' string is highlighted in blue.


Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
000409A0	E0	15	FE	7F	6B	32	32	23	36	B6	F0	11	00	00	00	00	à.p.k22#698.....
000409B0	49	45	4E	44	AE	42	60	FF	D8	FF	E1	13	D2	45	78	69	IEND' followed by a BOM and the Korean text 'yöyá.ÖExi'
000409C0	66	00	00	4D	4D	00	2A	00	00	00	08	00	07	01	12	00	f..MM.*.....
000409D0	03	00	00	00	01	00	01	00	00	01	1A	00	05	00	00	00
000409E0	01	00	00	00	62	01	1B	00	05	00	00	00	01	00	00	00b.....
000409F0	6A	01	28	00	03	00	00	00	01	00	02	00	00	01	31	00	j.(.....l.
00040A00	02	00	00	00	1E	00	00	00	72	01	32	00	02	00	00	00r.2.....
00040A10	14	00	00	00	90	87	69	00	04	00	00	00	01	00	00	00#i.....
00040A20	A4	00	00	00	D0	00	0A	FC	80	00	00	27	10	00	0A	FC	µ...Đ...ü€...'...ü
00040A30	80	00	00	27	10	41	64	6F	62	65	20	50	68	6F	74	6F	€...'.'Adobe Photo
00040A40	73	68	6F	70	20	43	53	36	20	28	57	69	6E	64	6F	77	shop CS6 (Window
00040A50	73	29	00	32	30	31	32	3A	31	30	3A	31	34	20	31	32	s).2012:10:14 12
00040A60	3A	32	32	3A	31	31	00	00	03	A0	01	00	03	00	00	00	:22:11... ..

헤더 시그니처(FF D8 ..) 부터
푸터 시그니처(FF D9)까지 긁어옴.

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00047980	25	29	24	92	49	4A	49	24	92	52	92	49	24	94	A4	92	%)' IJIS' R' IS" "x'
00047990	49	25	29	24	92	49	4A	49	24	92	52	92	49	24	94	A4	I%)' IJIS' R' IS" "x'
000479A0	92	49	25	29	24	92	49	4A	49	24	92	52	92	49	24	94	' I%)' IJIS' R' IS" "x'
000479B0	A4	92	49	25	29	24	92	49	4A	49	24	92	53	FF	D9		x' I%)' IJIS' S YU

1-9. 두 번째 이미지, 추출


whysoserious.png


flag.jpg

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	FF	D8	FF	E1	13	D2	45	78	69	66	00	00	4D	4D	00	2A	ÿøÿá.òExif..MM.*
00000010	00	00	00	08	00	07	01	12	00	03	00	00	00	01	00	01
00000020	00	00	01	1A	00	05	00	00	00	01	00	00	00	62	01	1Bb..
00000030	00	05	00	00	00	01	00	00	00	6A	01	28	00	03	00	00j.(....
00000040	00	01	00	02	00	00	01	31	00	02	00	00	00	1E	00	00l.....
00000050	00	72	01	32	00	02	00	00	00	14	00	00	00	90	87	69	.r.2.....#i
00000060	00	04	00	00	00	01	00	00	00	A4	00	00	00	D0	00	0A¸...Ð..
00000070	FC	80	00	00	27	10	00	0A	FC	80	00	00	27	10	41	64	ü€...'...ü€...'Ad
00000080	6F	62	65	20	50	68	6F	74	6F	73	68	6F	70	20	43	53	obe Photoshop CS
00000090	36	20	28	57	69	6E	64	6F	77	73	29	00	32	30	31	32	6 (Windows).2012
000000A0	3A	31	30	3A	31	34	20	31	32	3A	32	32	3A	31	31	00	:10:14 12:22:11.

새로운 JPG 파일을 하나 만들고,
파일 바이너리 데이터를 삽입.

1-10. flag 획득



2. 개념 확장

2-1. 문제 유형

포렌식 유형의 문제

but.. very easy

MISC (기타)

~~포렌식 유형의 문제 뿐만 아니라~~ 대체적으로 포렌식 문제가
너무 쉽거나, 이론적 지식 보다는 계성 위주의 문제는 이 분야로 판단.

2-2. 문제 의도

1. 파일 시그니처를 알고 있냐, 없냐
2. 스테가노그래피에 대한 개념이 있냐, 없냐



2-3. 더배워볼것(1)

1. 다양한 파일 시그니처

그래픽 파일 시그니처 (Graphic File Signatures)

by PRONEER on 2009-11-23 · 2 COMMENTS

이전에 파일 시그니처에 대해서 포스팅한적이 있다. 하지만 이번에 새로운 프로젝트를 하면서 급하게 그래픽 파일 포맷에 대한 시그니처가 필요해서 자주 사용하는 그래픽 파일 시그니처를 따로 정리해 보았다.

File Type	Header Signature	Footer Signature	Description
ICO	00 00 01 00	-	Windows Icon Format
CUR	00 00 02 00	-	Windows Cursor Format
BMP, DIB	42 4D B M	-	Windows Bitmap Format
GIF	47 49 46 38 37 61 G I F 8 7 a	00 3B ;	Graphics Interchange Format
GIF	47 49 46 38 39 61 G I F 8 9 a	00 3B ;	Graphics Interchange Format
TIF, TIFF	49 49 2A I I *	-	Tagged Image File Format (little endian)
TIF, TIFF	4D 4D 2A M M *	-	Tagged Image File Format (big endian)
PNG	89 50 4E 47 0D 0A 1A 0A P N G	49 45 4E 44 AE 42 60 82 I E N D B `	Portable Network Graphics Format
JPEG/JFIF	FF D8 FF E0 xx xx 4A 46 49 46	FF D9	JPEG/JFIF Format
JPEG/EXIF	FF D8 FF E8 xx xx 45 78 69 66	FF D9	JPEG/Exif Format - Digital Camera Exchangeable File Format
WMF	D7 CD C6 9A	-	Windows Metafile Format
EMF	01 00 00 00	-	Extended(Enhanced) Windows Metafile Format Printer Spool File

파일 시그니처 모음 (Common File Signatures)

by PRONEER on 2009-10-23 · 21 COMMENTS

Header Signature (Hex)	File Type	Description
xx xx xx xx AF 11	FLI	Graphics - Autodesk Animator
xx xx xx xx AF 12	FLC	Graphics - Autodesk 3D Studio
xx xx 2D 6C 68 35 2D - 1 h 5 -	LZH	Archive - LHA Compressed Archive File
00	PIF	Windows - Program Information File
	PIC	Graphics - IBM Storyboard Bitmap File
	YTR	IRIS OCR Data File
00 00 00 02	MAC	Graphics - MAC Picture Format
00 00 00 nn 66 74 79 70 f t y p 33 67 70 3 g p	3GG 3G2	3rd Generation Partnership Project 3GPP (nn=0x14) 3GPP2 (nn=0x20) Multimedia File
00 00 00 18 66 74 79 70 f t y p 33 67 70 35 3 g p 5	MP4	MPEG-4 Video File

2-4. 더배워볼것(2)

2. 파일 구조

JPEG 파일 구조 요약

[고정] SOI(Start of Image)

[고정] APP Marker (APP0 ~ APP15)

[고정] 추가 APP Marker(APP0 ~ APP15)

[유동] DQT (Define Quantization Tables)

[유동] SOF (Start Of Frame)

[유동] DHT (Define Huffman Tables)

[고정] SOS (Start Of Scan)

[고정] Scan Data

[고정] EOI (End Of Image)

▼ struct JPGFILE jpgfile		0h	7008h	Fg:	Bg:	
enum M_ID SOIMarker	M_SOI (FF...	0h	2h	Fg:	Bg:	
> struct APP1 app1[0]		2h	13D4h	Fg:	Bg:	
> struct APP13 app13		13D6h	1CFAh	Fg:	Bg:	
> struct APP1 app1[1]		30D0h	DD8h	Fg:	Bg:	
> struct APP2 app2		3EA8h	C5Ah	Fg:	Bg:	
> struct APP14 app14		4B02h	10h	Fg:	Bg:	
> struct DQT dqt		4B12h	86h	Fg:	Bg:	
> struct SOF sof0		4B98h	13h	Fg:	Bg:	
> struct DRI dri		4BABh	6h	Fg:	Bg:	
> struct DHT dht		4BB1h	141h	Fg:	Bg:	
> struct SOS scanStart		4CF2h	Eh	Fg:	Bg:	
> char scanData[8966]		4D00h	2306h	Fg:	Bg:	
enum M_ID EOIMarker	M_EOI (FF...	7006h	2h	Fg:	Bg:	

여기서 유동으로 표시한 구조의 경우, 위치 순서가 유동적으로 바뀔 수 있음을 말합니다. 예를 들면 DQT가 먼저 올 수도, SOF가 먼저 올 수도 있는 것이죠.

2-5. 더배워볼것(3)

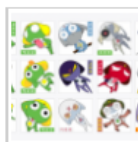
3. 다양한 스테가노그래피 기술



[HackCTF]_[Forensic] [Let'S get it ! \(BMP 스테가노그래피\)](#) | HackCTF

2019/09/03 17:57

24비트 bmp 파일인걸로 봐서는, LSB 나 MSB 스테가노그래피가 적용되어 있을 확율이 크네요. StegSolve...



[xcz.kr] [Prob16 - Mountains beyond mountains \(LSB 스테가노그래피\)](#) | xcz.kr

2016/10/06 03:37

php) 드라마 유령에도 나왔던 기술인 스테가노그래피(Steganography)라는 기술은 MP3파일, 이미지 파일...



[xcz.kr] [Prob12 - Steganography \(MP3 스테가노그래피\)](#) | xcz.kr

2016/09/26 01:18

시키면 에러가 납니다 스텝 항목을 잘 펴보면 이런 항목이 있습니다 Step (3): wrong bits selection...



[A0V3R]_[Forensics] [Extend \(BMP 크기 변환\)](#) | A0V3R

2019/07/09 11:39

bmp의 사진 모습 (이 사진은 문제 파일이 아님) 처음에 문제 제목을 Extract로 보고 스테가노그래피인줄...

Q & A

「
감사합니다
」