



2020 JBU-CTF

Forensic

문승재

문제목록

Forensic

Find image

100

Flag in Moon

200

Problem PPTX

200

Forensic

Find image

100

Find image

100

디지털 포렌식 수사관인 당신에게 피의자의 컴퓨터를 수사하라는 명령이 떨어졌다.

피의자의 컴퓨터를 보니 의심이 가는 파일이 있다.

주어진 툴로 확인해보자!!

Find_image.zip

FTK Imager




scpCTF{...}

Submit

Problem PPTX

200

문제풀이

 Find_image	2020-09-09 오후 6:00	파일	1,535,949KB
 Find_image.E02	2020-09-09 오후 6:00	E02 파일	1,141,440KB
 Find_image.txt	2020-09-09 오후 6:07	텍스트 문서	2KB

Find_image.txt

Image Information:

Acquisition started: Wed Sep 9 17:59:35 2020

Acquisition finished: Wed Sep 9 18:00:29 2020

Segment list:

E:\Forensic_challenge\Find_image\E01

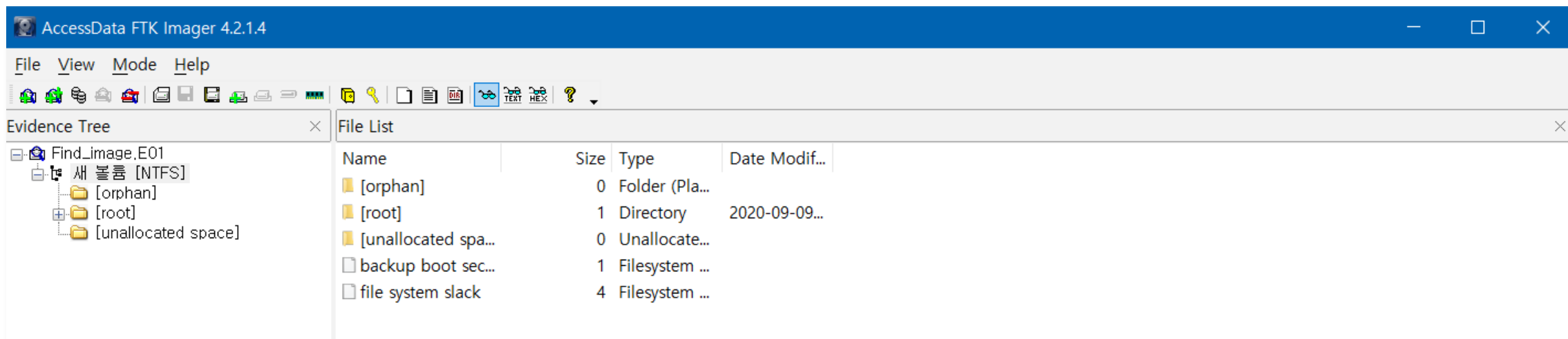
E:\Forensic_challenge\Find_image.E02

Find_image.E01



FTK Imager

문제풀이



문제풀이

Evidence Tree

Find_Image.E01

새 볼륨 [NTFS]

[orphan]

[root]

!@Gxpd

\$BadClus

\$Extend

\$RECYCLE.BIN

\$Secure

\$UpCase

Flag.png

System Volume Information

[unallocated space]

File List

Name	Size	Type	Date Modif...
\$LogFile	6,960	Regular File	2020-09-09...
\$MFT	256	Regular File	2020-09-09...
\$MFTMirr	4	Regular File	2020-09-09...
\$Secure	1	Regular File	2020-09-09...
\$TXF_DATA	1	NTFS Logg...	2020-09-09...
\$UpCase	128	Regular File	2020-09-09...
\$Volume	0	Regular File	2020-09-09...
20160525_21511...	661	Regular File	2020-06-03...
Flag.png	3,564	Regular File	2020-09-09...


Custom Content Sources

Evidence:File System|Path|File

Options

< >

New Edit Remove Remove All Create Image



문제풀이

Evidence Tree

Find_Image.E01

새 볼륨 [NTFS]

[orphan]

[root]

!@Gxpd

\$BadClus

\$Extend

\$RECYCLE.BIN

S-1-5-21-502940310-996

\$Secure

\$UpCase

Flag.png

System Volume Information

[unallocated space]

File List

Name	Size	Type	Date Modif...
\$I27VCIL.png	1	Regular File	2020-09-09...
\$IUXCQJ9.png	1	Regular File	2020-09-09...
\$R27VCIL.png	3,561	Regular File	2020-09-09...
\$RUXCQJ9.png	1,122	Regular File	2020-09-09...
desktop.ini	1	Regular File	2020-09-09...

Custom Content Sources

Evidence:File System|Path|File

Options

scpCTF{w3lc0m3_F0r3n5ic!!}

문제목록

Forensic

Find image

100

Flag in Moon

200

Problem PPTX

200

Forensic

Find image

100

Challenge

0 Solves



Flag in Moon

200

전에 찍은 달 사진을 보고 있다.

오?!?!?! 달 사진이 뭔가 이상하다.

빈 공간을 잘 보면 Flag가 있을지도...?

flag_in_moon.jpg

scpCTF{...}

Submit

Problem PPTX

200

문제풀이



Hex Editor

문제풀이

[illegible]

문제풀이

[illegible]

문제풀이

VIEW

Text ▼

```
c2NwQ1RGe1RoatVfaTVfaEAXZl9NMDBufQ=
```

ENCODE **DECODE****Base64** ▼

VARIANT

Base64 (RFC 3548, RFC 4648) ▼

→ Decoded 25 bytes

VIEW

Text ▼

```
scpCTF{Thi5_i5_h@1f_M00n}
```

문제목록

Forensic

Find image

100

Flag in Moon

200

Problem PPTX

200

Forensic

Find image

100

Challenge

0 Solves



Problem PPTX

200

팀 프로젝트를 하는 나에게 팀원이 PPT를 보내왔다.

어...라....??? PPT가 이상하다.

PPT를 고쳐 문제를 해결하자.

Problem.pptx

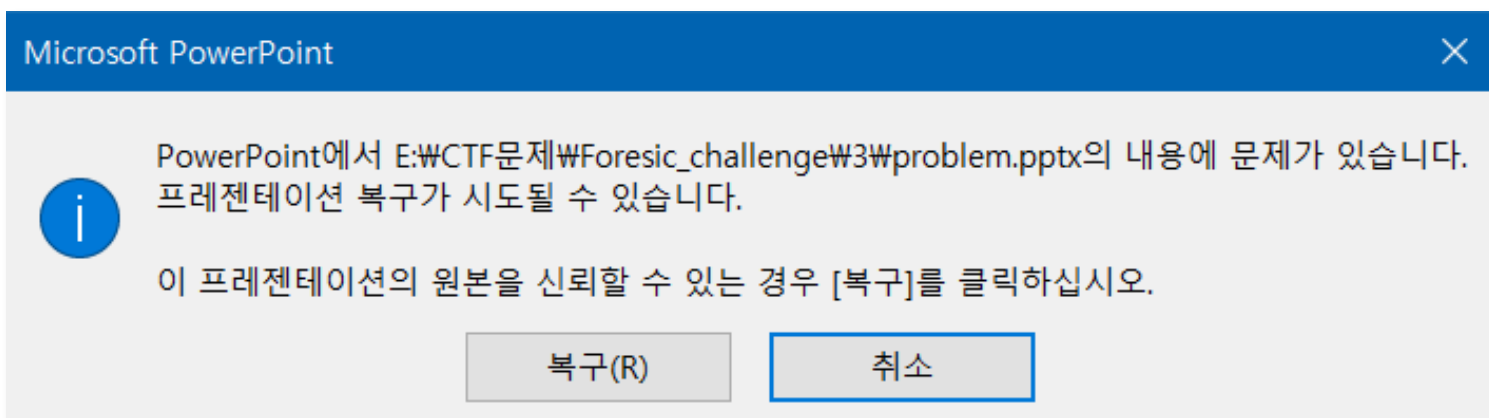
scpCTF{...}

Submit

Problem PPTX

200

문제풀이



문제풀이



PowerPoint

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	50	4B	03	04	14	00	00	00	08	00	0C	02	2D	51	12	C0	PK.....-Q.À
00000010	A0	07	C0	F6	2E	00	37	0F	2F	00	05	00	00	00	31	2E	.Àö..7./.....l.
00000020	70	6E	67	EC	5A	F5	57	94	EF	12	A7	97	5E	10	A4	C3	pngizÖW"i.\$-^..µÃ
00000030	A0	1B	49	A9	15	90	EE	10	E9	46	40	5A	A4	59	42	62	.I@..i.éF@ZµYBb
00000040	11	A5	41	4A	BA	44	9A	95	EE	EE	12	29	89	A5	43	3A	.¥AJ°Dš•ii.)%¥C:
00000050	97	85	8D	EB	F7	DE	FB	4F	DC	73	EE	2F	73	E6	BC	E7	-....ë÷þûÖÜsî/sæ¼ç
00000060	7D	9F	79	67	9E	99	CF	CC	33	F3	7C	D4	D5	56	21	23	}ÿygž™İİ3ó ÔÖV!#
00000070	66	20	C6	C2	C2	22	53	53	7D	A9	8F	85	85	5F	8E	85	f ÅÅÅ"SS)@..... Ž...
00000080	05	08	23	24	F8	FB	A4	3F	7A	99	19	0B	1B	0B	4B	ED	..#šøûµ?z™....Kí
00000090	A5	BC	A1	FF	EF	23	14	3C	C5	E1	00	0C	0B	E8	4C	00	¥¼;ÿi#.<Åá...èL.
000000A0	ED	05	A6	48	80	DF	38	04	CC	AE	E5	33	C6	29	F7	25	í. HÉB8.İöå3Æ)÷%
000000B0	E1	A9	25	FD	4C	7C	5A	65	44	A2	B7	19	AF	1C	AB	17	á@%ýL ZeDc.~.«.
000000C0	59	6C	E5	FB	F4	8D	F8	2E	70	91	95	43	5C	81	91	97	Ylâûô.ø.p`•C\.'-
000000D0	5F	A5	AE	28	C3	22	96	61	F2	AD	72	1F	73	AC	62	0C	¥@ (Å"-aò.r.s~b.
000000E0	C1	7B	AC	99	38	77	AC	63	AD	80	F4	35	0B	8F	F8	D0	Ã{-™8w~c.€ô5...øÐ
000000F0	1B	88	77	3D	0F	6F	5B	6B	DB	F4	EA	A3	17	9B	F7	B1	.^w=.o[kûôê£.>÷±
00000100	CD	49	26	69	12	A7	1D	01	13	CF	A7	2E	9F	C3	2E	C1	ÍI&i.\$...İ\$.ŸÃ.Á
00000110	2F	08	1F	47	52	28	FC	9F	FC	9F	FC	9F	FC	8F	11	10	/..GR(üŸüŸüŸü...
00000120	91	68	00	F1	BF	F9	10	DB	41	F0	6F	DC	78	FC	06	40	`h.ñ¿ù.ÔAðoÜxü.@
00000130	7B	87	8E	02	2A	0C	64	80	50	92	BE	F0	F8	CF	8B	FD	{÷Ž.*.d€P'¼ðøİ<ý

문제풀이



PowerPoint



Word

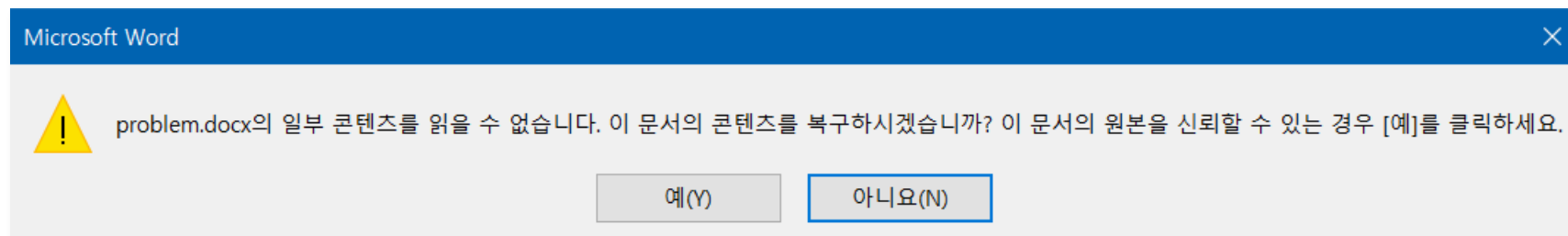


ZIP

문제풀이



Word



문제풀이



ZIP

problem.zip - 알집

파일	흥	편집	도구	보기	도움말				
폴더	필터	검색	×	파일명	압축크기	원본크기	압축률		
.....ZIP problem.zip				1.png	3,077,824	3,084,087	0%	F	
				2.jpg	170,634	187,858	9%	J	
				3.png	2,024,627	2,034,720	0%	F	
				4.jpg	170,634	187,858	9%	J	
				5.jpg	121,092	136,634	11%	J	
				6.jpg	110,146	125,478	12%	J	
				7.png	15,271	20,556	26%	F	
				8.jpg	170,634	187,858	9%	J	
				9.png	129,774	137,866	6%	F	
				10.png	663,782	676,009	2%	F	
				11.png	1,127,773	1,141,753	1%	F	
				12.png	1,077,621	1,091,968	1%	F	
				13.png	267	1,197	78%	F	
				14.png	2,024,627	2,034,720	0%	F	
				15.png	2,024,627	2,034,720	0%	F	
				16.png	293,961	304,863	4%	F	
				17.jpg	140,828	158,520	11%	J	
				18.png	267	1,197	78%	F	
				19.png	259,234	264,115	2%	F	
				20.png	416,096	434,897	4%	F	
				21.png	3,053,267	3,055,701	0%	F	

문제풀이



1.png



2.jpg



3.png



4.jpg



5.jpg



6.jpg



7.png



8.jpg



9.png



10.png



11.png



12.png



13.png



14.png



15.png



16.png



17.jpg



18.png



19.png



20.png



21.png



22.png



23.png



24.png



25.png



26.png



27.png



28.png

문제목록

Forensic

Find image

100

Flag in Moon

200

Problem PPTX

200



감사합니다.