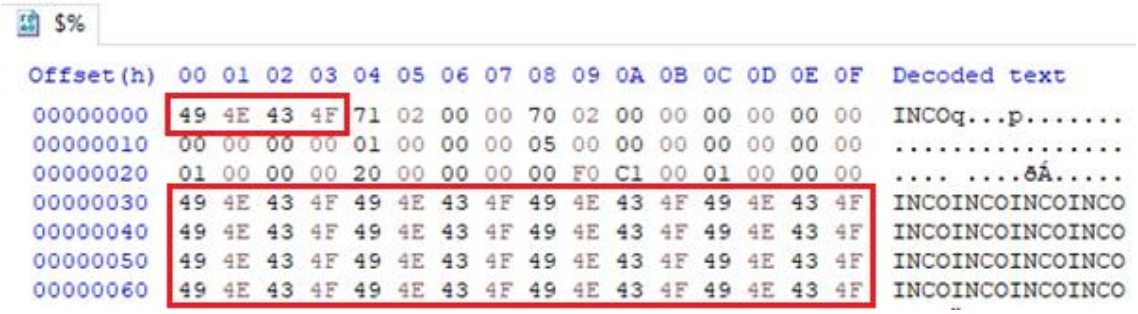
INCOGNITO CTF Write-up

작성자: Team CodeCure – 박의준

HS (Forensics)

이동식 저장장치의 Serial Number를 구하시오

주어진 레지스트리 하이브 파일의 Base Block을 살펴보면 파일의 Signature와 File Name Field가 "INCO" 문자열로 Overwrite 되어있다.

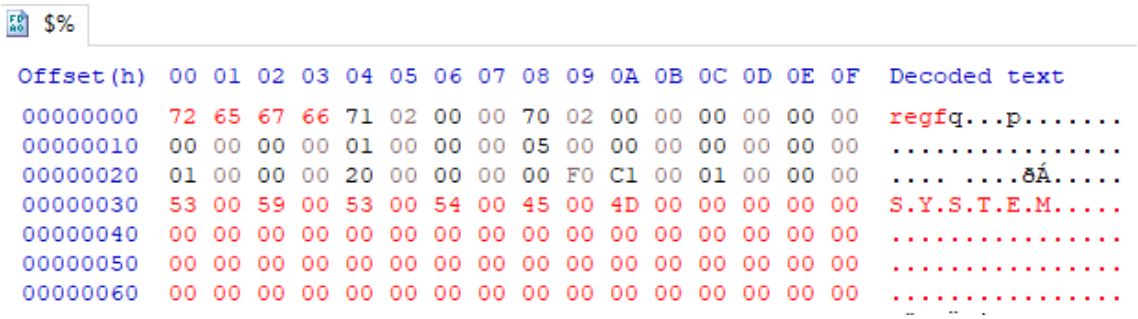


Overwrite

정상 하이브 파일의 Base Block 구조를 참고하여 Offset(0), Length(4), Field("regf") 형식으로 Signature Field를 채워넣으면 레지스트리 도구에서 정상적으로 인식한다.

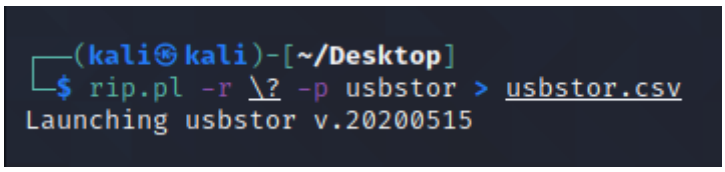
USB 정보가 담긴 하이브 파일 – SYSTEM / type: UTF-16LE

(File Name Field는 다른 값으로 overwrite 되어도 분석에 지장 없음)

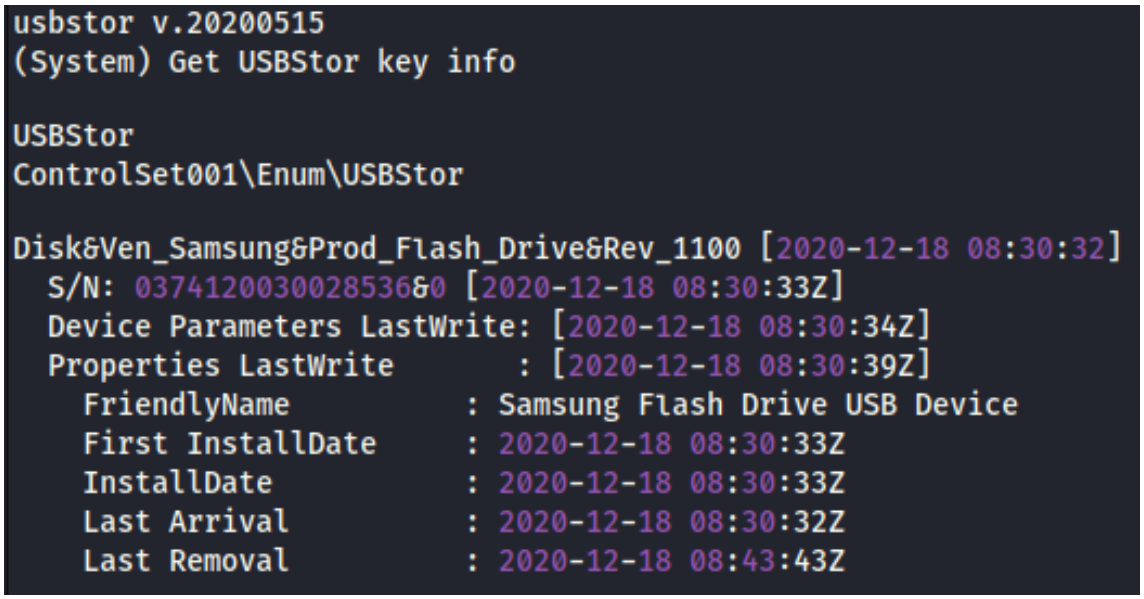


Original Field

RegRipper3.0, USBSTOR 플러그인을 활용하여 하이브 파일을 분석하여 이동식 저장장치의 정보를 추출할 수 있고 Serial Number를 얻을 수 있다.



RegRipper3.0 – USBSTOR



Usbstor.csv

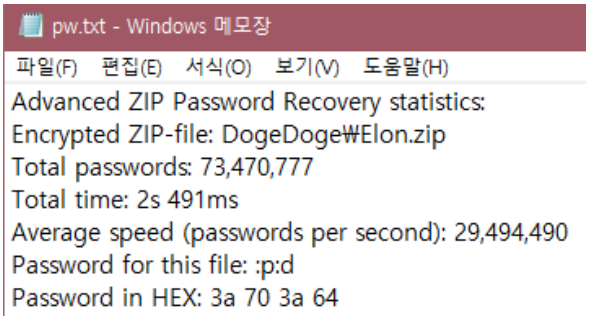
분석 결과의 Serial Number 값으로 "03741200300285360"로 기록되었더라도 실질적인 Serial Number는 '&' 문자를 기준으로 앞부분의 "0374120030028536"이고 뒷부분의 '0'는 PnP Manager로부터 받아오는 Random Number(USB 장치 연결 번호, Port 번호)를 의미하기 때문에 FLAG를 인증할 때 유의해야한다.

INCO{0374120030028536}

DogeDoge (Forensics)

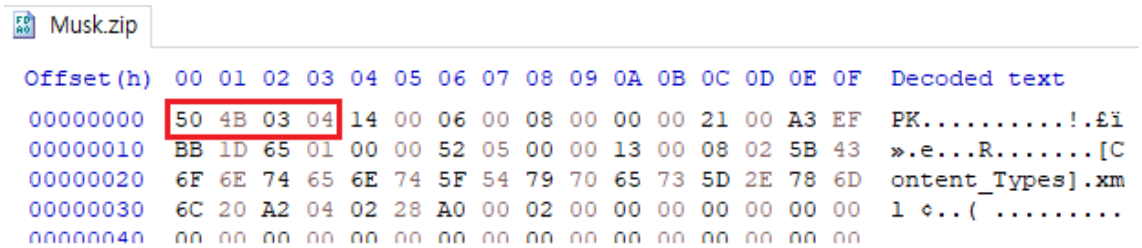
숨겨진 이미지를 찾으시오

주어진 Elon.zip 파일의 암호를 Brute-force 도구를 활용하여 풀어낸다



AZPR 4.00

Elon.zip 을 압축 해제하여 얻은 Musk.zip 파일의 바이너리를 확인하면 Signature Field가 Microsoft Office Open XML Format Signature 값을 가지고 있고 ".docx" 확장자였음을 확인할 수 있다.

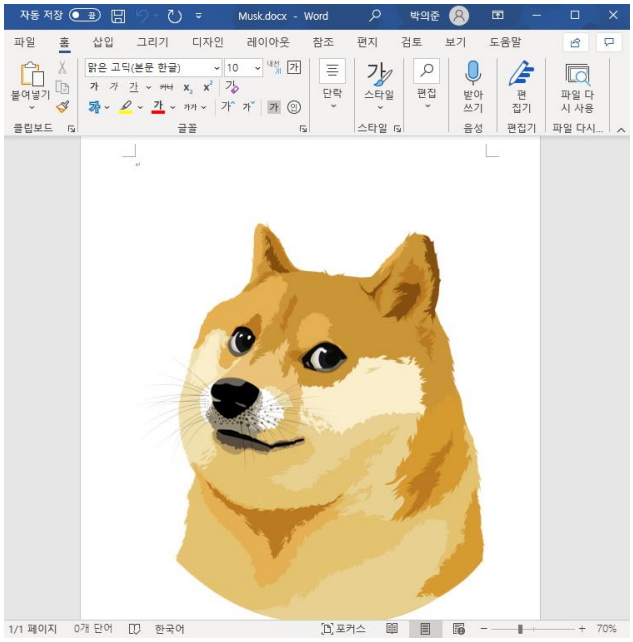


.docx Signature

Extension	Signature	Description
DOCX	50 4B 03 04	MS Office Open XML Format Document
	ASCII PK••	Sizet: 4 Bytes Offset: 0 Bytes

It's same.

Musk.docx를 실행하면 Doge 이미지가 존재하지만 문제의 조건은 "숨겨진" 이미지를 찾는 것이기 때문에 다시 한번 바이너리를 확인한다.



Doge

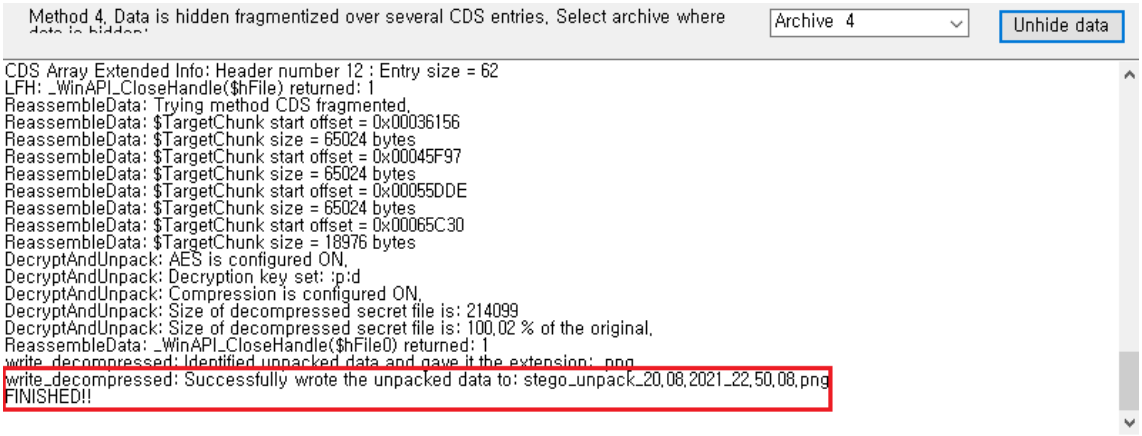
Musk.docx

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	06	00	08	00	00	00	21	00	A3	EF	PK.....!.£ï
00000010	BB	1D	65	01	00	00	52	05	00	00	13	00	08	02	5B	43	».e...R.....[C
00000020	6F	6E	74	65	6E	74	5F	54	79	70	65	73	5D	2E	78	6D	ontent_Types].xm
00000030	6C	20	A2	04	02	28	A0	00	02	00	00	00	00	00	00	00	l ¢..(.....
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
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	.....

Extra Field

Extra Field가 존재하는 것으로 보아 OOXML Steganography를 활용하여 이미지를 은닉한 것으로 추정할 수 있다. ooXML_Steganography_v4의 ooXML_Steganography_UnHider 도구를 활용하고 "Elon.zip" 파일의 패스워드인 ":p:d" 문자열이 AES Descryption Key 라는 것을 Guessing, 숨겨진 이미지를 추출할 수 있다.

Input decryption key



UnHider Finished

DogeDoge.png (FLAG)

FLAG: INCO{M4R5_GAZUA}