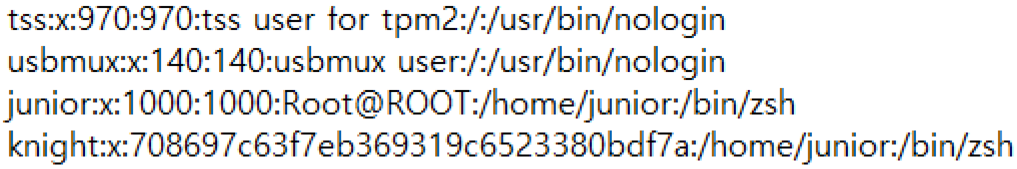
[KnightCTF2022]

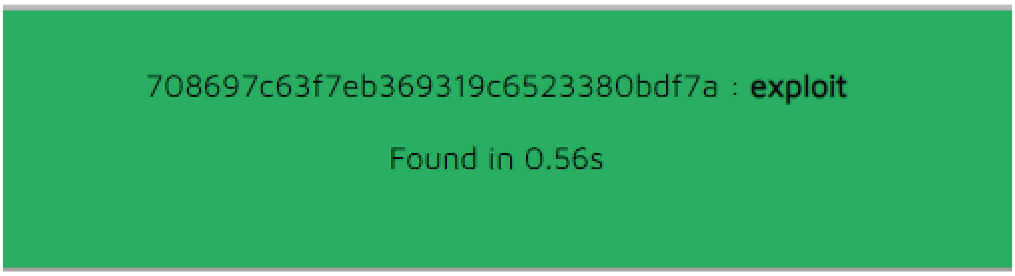
Cryptography

- Passwd



```
tss:x:970:970:tss user for tpm2:/:/usr/bin/nologin
usbmux:x:140:140:usbmux user:/:/usr/bin/nologin
junior:x:1000:1000:Root@ROOT:/home/junior:/bin/zsh
knight:x:708697c63f7eb369319c6523380bdf7a:/home/junior:/bin/zsh
```

knight user의 password 옆에 인코딩된 값을 MD5 Decrypt해보니



708697c63f7eb369319c6523380bdf7a : **exploit**

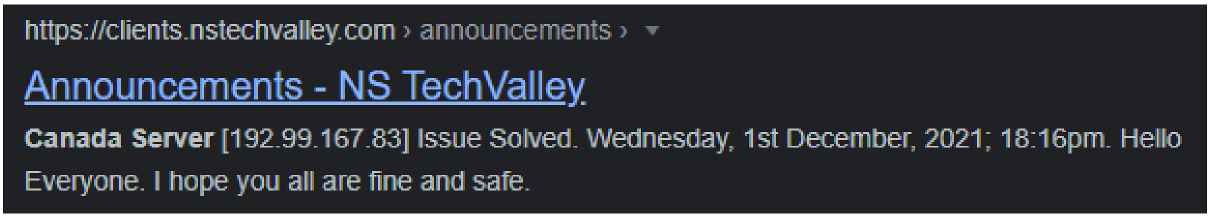
Found in 0.56s

knight user의 password로 exploit임을 알아냈다.

OSINT

- Canada Server

NS TechValley의 Canada server의 IP 주소를 얻기 위해 구글링해보았다.



https://clients.nstechvalley.com › announcements ›

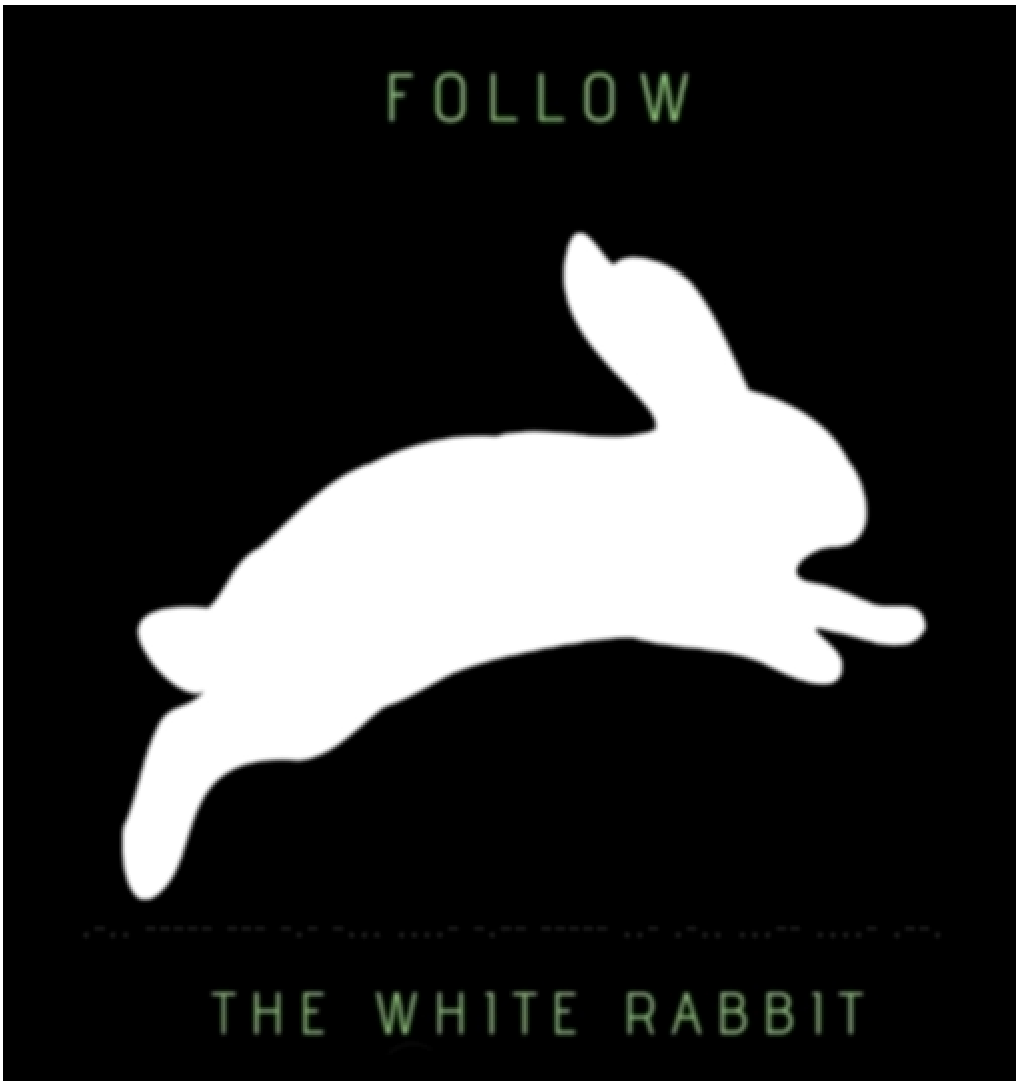
Announcements - NS TechValley

Canada Server [192.99.167.83] Issue Solved. Wednesday, 1st December, 2021; 18:16pm. Hello Everyone. I hope you all are fine and safe.

첫번째 검색 결과로 바로 알 수 있다.

■ Steganography

- Follow The White Rabbit

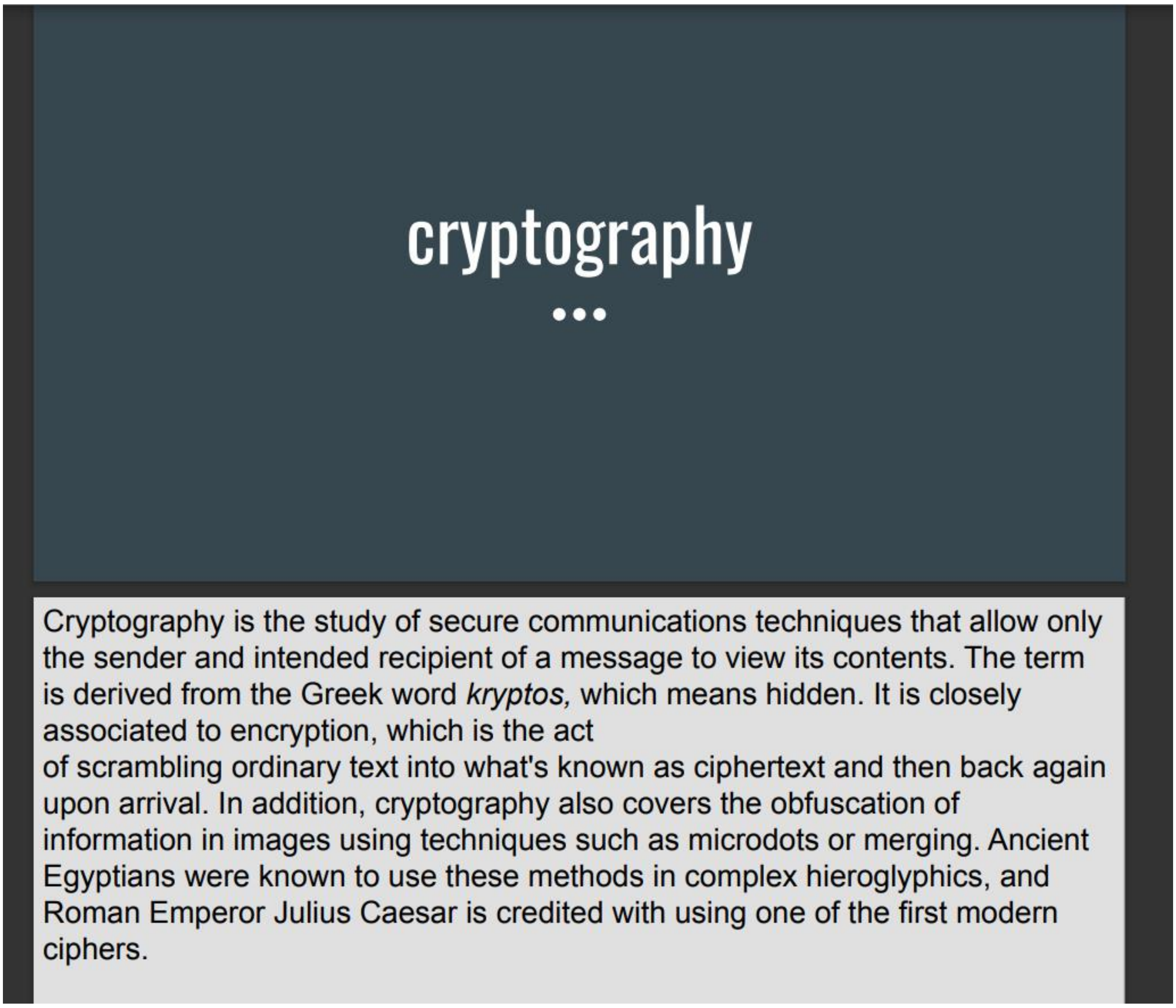


토끼 그림 바로 밑에 있는 모스 부호를 해석해본 결과

L0OKB4Y0UL34P로 나온다.

flag : KCTF{L0OKB4Y0UL34P}

- Follow



Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents. The term is derived from the Greek word *kryptos,* which means hidden. It is closely associated to encryption, which is the act
of scrambling ordinary text into what's known as ciphertext and then back again upon arrival. In addition, cryptography also covers the obfuscation of information in images using techniques such as microdots or merging. Ancient Egyptians were known to use these methods in complex hieroglyphics, and Roman Emperor Julius Caesar is credited with using one of the first modern ciphers.

문제에 주어진 pdf의 글에 이상하게 텅 빈 부분이 있어서 글 내용을 복붙해보니

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents. The term is derived from the Greek word kryptos, which means hidden. It is closely associated to encryption, which is the act KCTF{This_is_the_real_flag}
of scrambling ordinary text into what's known as ciphertext and then back again upon arrival. In addition, cryptography also covers the obfuscation of information in images using techniques such as microdots or merging. Ancient Egyptians were known to use these methods in complex hieroglyphics, and Roman Emperor Julius Caesar is credited with using one of the first modern ciphers

빈 부분에 flag가 숨겨져 있다.

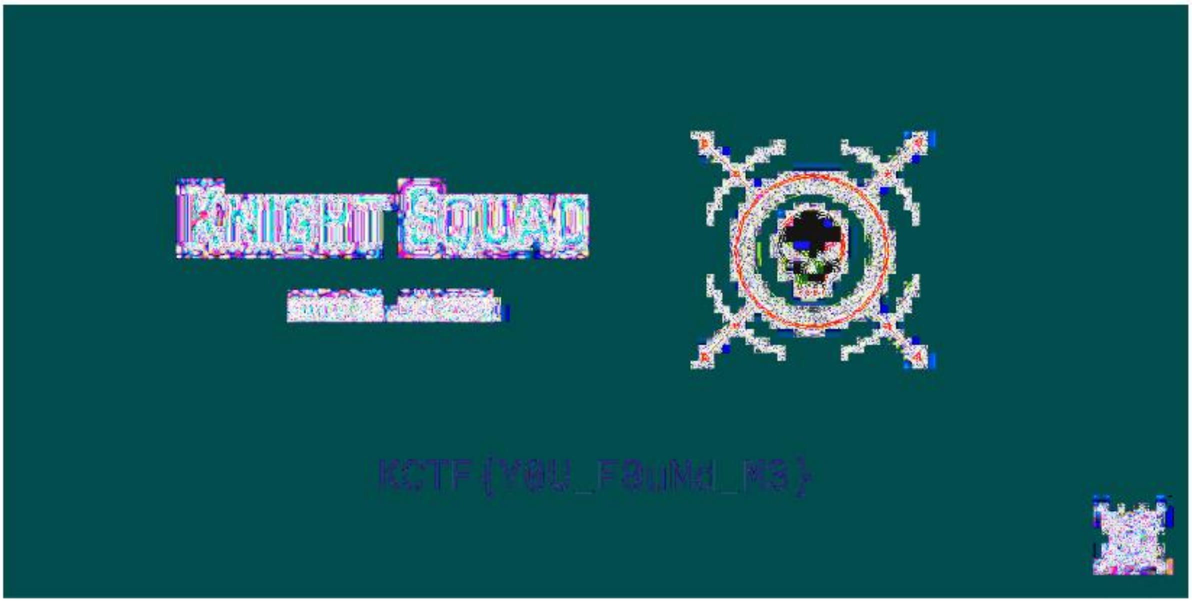
flag : KCTF{This_is_the_real_flag}

■ Digital Forensics

- The Lost Flag

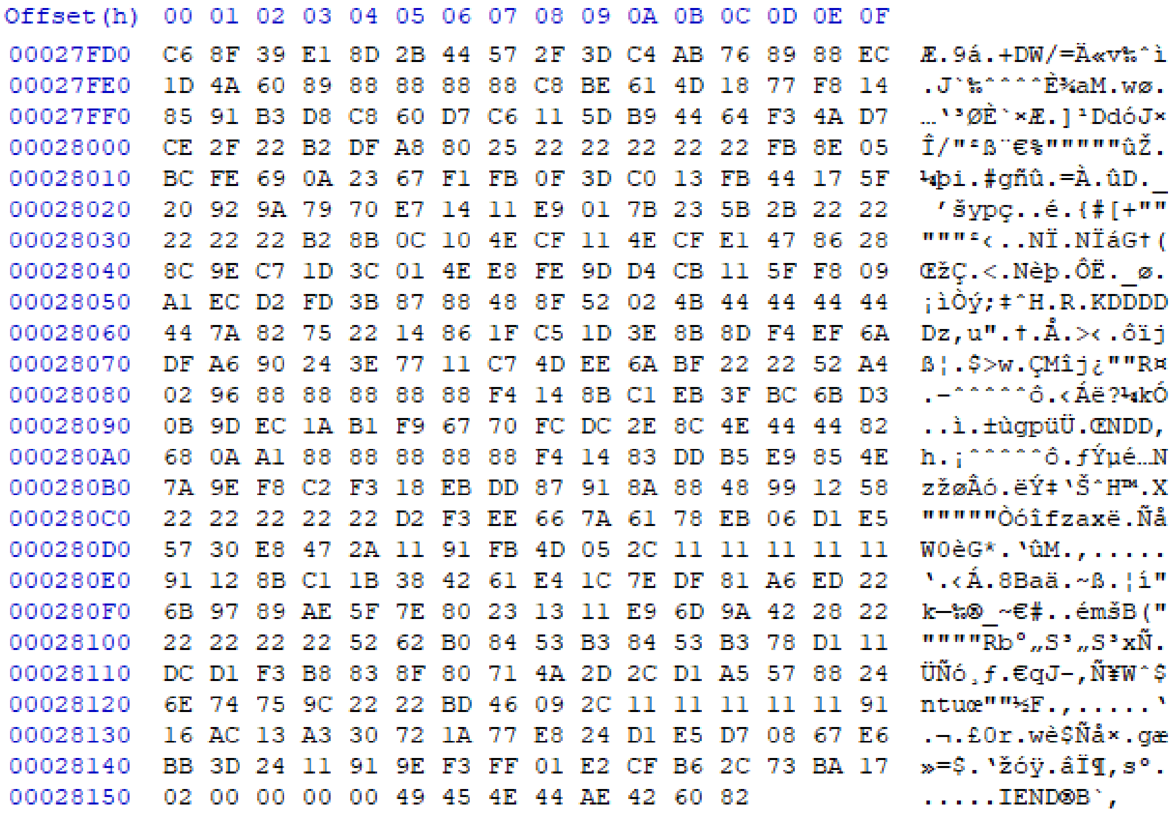
KNIGHT SQUAD
SINCE 28 JAN 2020

이미지 포렌식 사이트를 통해 위 그림을 Error Level Analysis(magnifier enhancement -Auto Contrast)하여 숨겨진 flag를 구해냈다.



flag : KCTF{Y0U_F0uNd_M3}

- Unknown File



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00027FD0  C6 8F 39 E1 8D 2B 44 57 2F 3D C4 AB 76 89 88 EC  Æ.9á.+DW/=Ä«v‰ˆì
00027FE0  1D 4A 60 89 88 88 88 88 C8 BE 61 4D 18 77 F8 14  .J`‰ˆˆˆˆÈ¾aM.wø.
00027FF0  85 91 B3 D8 C8 60 D7 C6 11 5D B9 44 64 F3 4A D7  …'³ØÈ`×Æ.]¹DdóJ×
00028000  CE 2F 22 B2 DF A8 80 25 22 22 22 22 22 FB 8E 05  Î/"²ß¨€%"""""ûŽ.
00028010  BC FE 69 0A 23 67 F1 FB 0F 3D C0 13 FB 44 17 5F  ¼þi.#gñû.=À.ûD._
00028020  20 92 9A 79 70 E7 14 11 E9 01 7B 23 5B 2B 22 22   'šypç..é.{#[+""
00028030  22 22 22 B2 8B 0C 10 4E CF 11 4E CF E1 47 86 28  """²‹..NÏ.NÏáG†(
00028040  8C 9E C7 1D 3C 01 4E E8 FE 9D D4 CB 11 5F F8 09  ŒžÇ.<.Nèþ.ÔË._ø.
00028050  A1 EC D2 FD 3B 87 88 48 8F 52 02 4B 44 44 44 44  ¡ìÒý;‡ˆH.R.KDDDD
00028060  44 7A 82 75 22 14 86 1F C5 1D 3E 8B 8D F4 EF 6A  Dz‚u".†.Å.>‹.ôïj
00028070  DF A6 90 24 3E 77 11 C7 4D EE 6A BF 22 22 52 A4  ß¦.$>w.ÇMîj¿""R¤
00028080  02 96 88 88 88 88 88 F4 14 8B C1 EB 3F BC 6B D3  .–ˆˆˆˆˆô.‹Áë?¼kÓ
00028090  0B 9D EC 1A B1 F9 67 70 FC DC 2E 8C 4E 44 44 82  ..ì.±ùgpüÜ.ŒNDD‚
000280A0  68 0A A1 88 88 88 88 88 F4 14 83 DD B5 E9 85 4E  h.¡ˆˆˆˆˆô.ƒÝµé…N
000280B0  7A 9E F8 C2 F3 18 EB DD 87 91 8A 88 48 99 12 58  zžøÂó.ëÝ‡'ŠˆH™.X
000280C0  22 22 22 22 22 D2 F3 EE 66 7A 61 78 EB 06 D1 E5  """""ÒóîfzaxëÑå
000280D0  57 30 E8 47 2A 11 91 FB 4D 05 2C 11 11 11 11 11  W0èG*.'ûM.,.....
000280E0  91 12 8B C1 1B 38 42 61 E4 1C 7E DF 81 A6 ED 22  '.‹Á.8Baä.~ß.¦í"
000280F0  6B 97 89 AE 5F 7E 80 23 13 11 E9 6D 9A 42 28 22  k—‰®_~€#..émšB("
00028100  22 22 22 22 52 62 B0 84 53 B3 84 53 B3 78 D1 11  """"Rb°„S³„S³xÑ.
00028110  DC D1 F3 B8 83 8F 80 71 4A 2D 2C D1 A5 57 88 24  ÜÑó¸ƒ.€qJ-,Ñ¥Wˆ$
00028120  6E 74 75 9C 22 22 BD 46 09 2C 11 11 11 11 11 91  ntuœ""½F.,.....'
00028130  16 AC 13 A3 30 72 1A 77 E8 24 D1 E5 D7 08 67 E6  .¬.£0r.wè$Ñå×.gæ
00028140  BB 3D 24 11 91 9E F3 FF 01 E2 CF B6 2C 73 BA 17  »=$.'žóÿ.âÏ¶,sº.
00028150  02 00 00 00 00 49 45 4E 44 AE 42 60 82           .....IEND®B`‚
```

다운받은 파일을 HxD로 보는데 맨 끝에 PNG 시그니처가 표시되어 있으므로, 앞에 PNG 시그니처로 바꾼 후에 파일을 열어보았다.

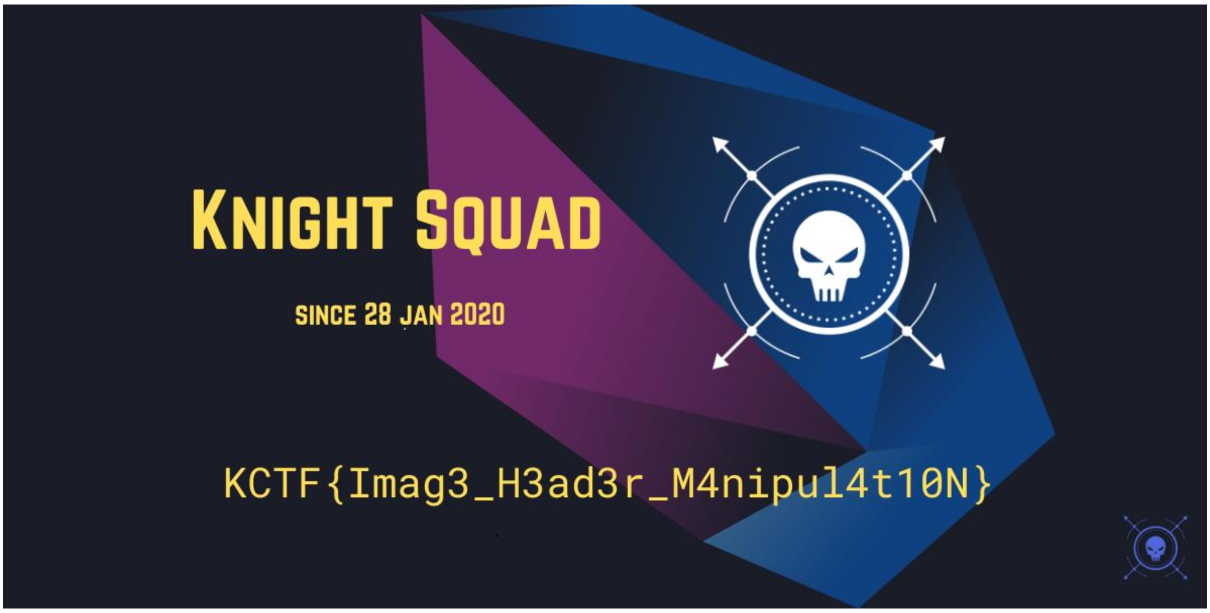


그림 밑에 flag가 KCTF{Imag3_H3ad3r_M4nipul4t10N}로 나와있다.