What's multimedia Forensics?

2019.07.22
(Y.M.Jeon)

Multimedia Forensics?

Multimedia Forensics?

- 디지털 비디오, 오디오, 이미지 등의 멀티미디어 데이터에서 증거 획득 & 분석
- CCTV, 블랙박스 등의 영상 및 통화 녹음 등의 사운드, 사진 등에 대한 이미지 파일에 대한 분야로 나뉨

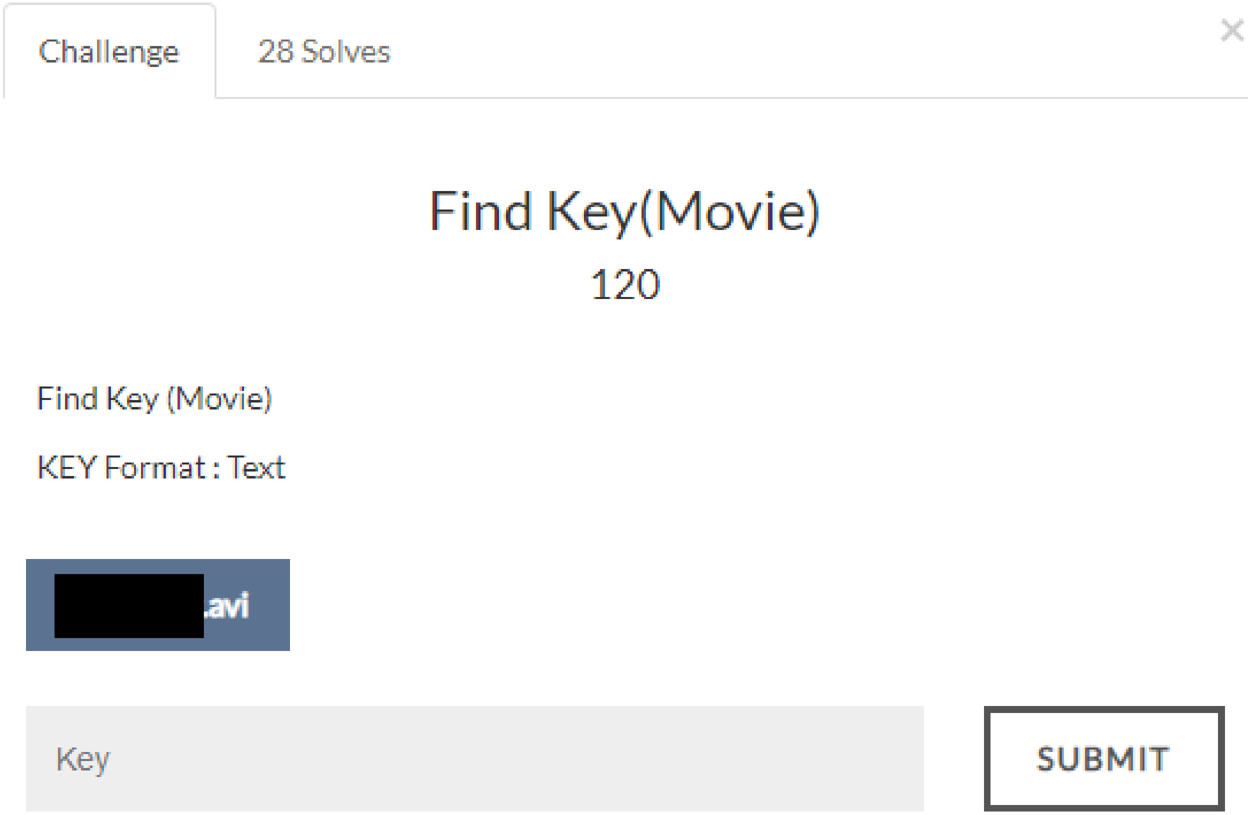
Analysis method?

- 화질 및 음질 개선 작업과 데이터 변조에 대한 검증 및 분석
- 기본적으로 이미지를 이루는 기본 단위인 픽셀 속의 디지털 정보에서 위조나 변조 흔적을 찾을 수 있다.

Request type?

- 증거인멸 시도 복구 : 영상 데이터를 삭제했거나 에러 발생 시 영상 복구 프로그램으로 복구가 불가한 경우
- 화질 개선 : 저해상도, 손실 압축, 동작 흐림, 조명 부족 또는 노이즈 등으로 인하여 판독이 불가한 경우
- 위변조 분석 : 영상 또는 이미지 데이터가 위조 또는 변조가 의심되는 경우 정확한 분석을 원할 경우

Video problem



Find Key(Movie)

120

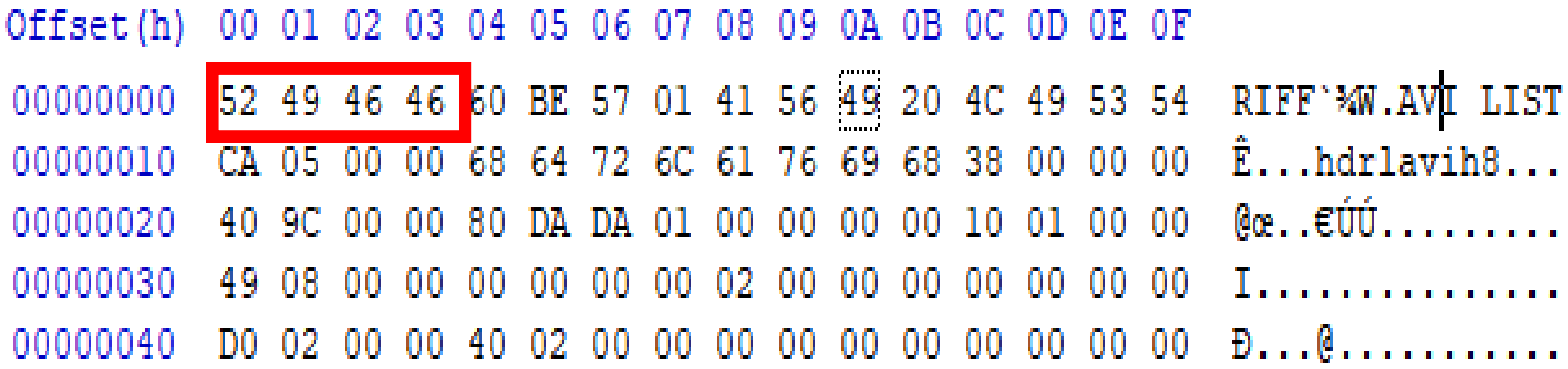
Find Key (Movie)

KEY Format : Text

[redacted].avi

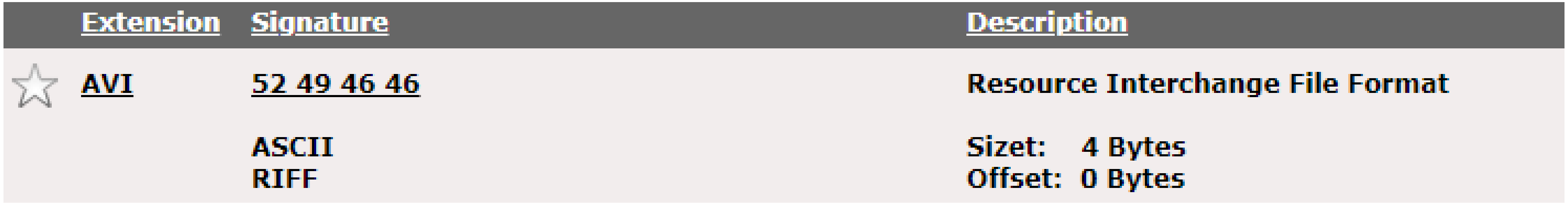
Video problem

avi???



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

00000000  52 49 46 46 60 BE 57 01 41 56 49 20 4C 49 53 54  RIFF`¾W.AVI LIST
00000010  CA 05 00 00 68 64 72 6C 61 76 69 68 38 00 00 00  Ê...hdrlavih8...
00000020  40 9C 00 00 80 DA DA 01 00 00 00 00 10 01 00 00  @œ..€ÚÚ.........
00000030  49 08 00 00 00 00 00 00 02 00 00 00 00 00 00 00  I...............
00000040  D0 02 00 00 40 02 00 00 00 00 00 00 00 00 00 00  Ð...@...........
```



Extension	Signature	Description
☆ AVI	52 49 46 46	Resource Interchange File Format
	ASCII RIFF	Sizet: 4 Bytes Offset: 0 Bytes

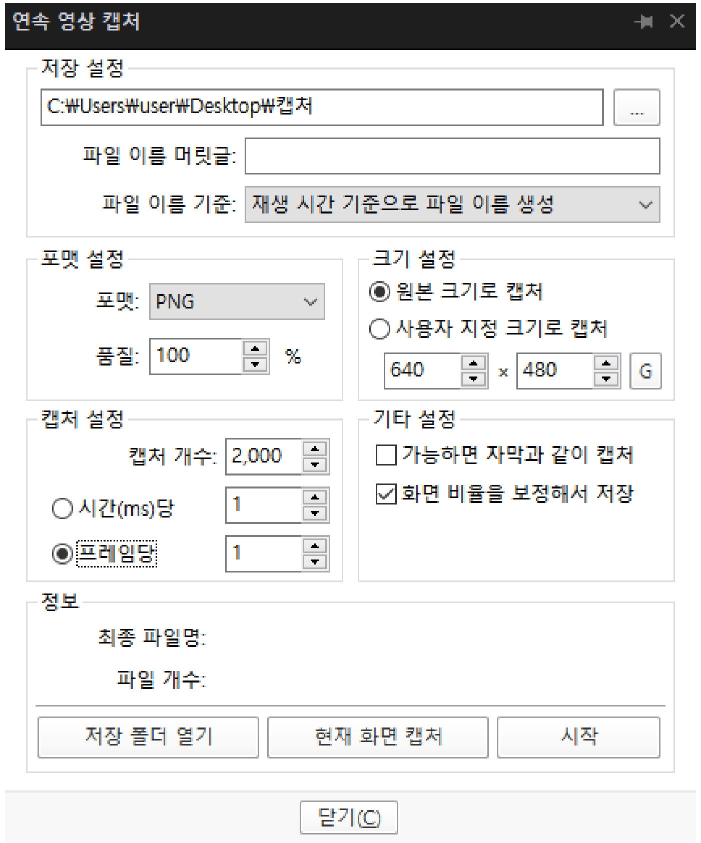
DAT,WAV,AVI = 52 49 46 46

Video problem

동영상

- 사진을 연속적으로 보여주는 것
- 한 장, 한 장의 사진들이 초당 어느 속도로 빠르게 바뀌면서 움직이는 하나의 동영상을 만든다.
- 동영상의 한 장, 한 장의 사진을 프레임이라 한다.

POT Player



연속 영상 캡처

저장 설정

C:₩Users₩user₩Desktop₩캡처

파일 이름 머릿글:

파일 이름 기준: 재생 시간 기준으로 파일 이름 생성

포맷 설정

포맷: PNG

품질: 100 %

크기 설정

● 원본 크기로 캡처

○ 사용자 지정 크기로 캡처

640 x 480

캡처 설정

캡처 개수: 2,000

○ 시간(ms)당 1

● 프레임당 1

기타 설정

□ 가능하면 자막과 같이 캡처

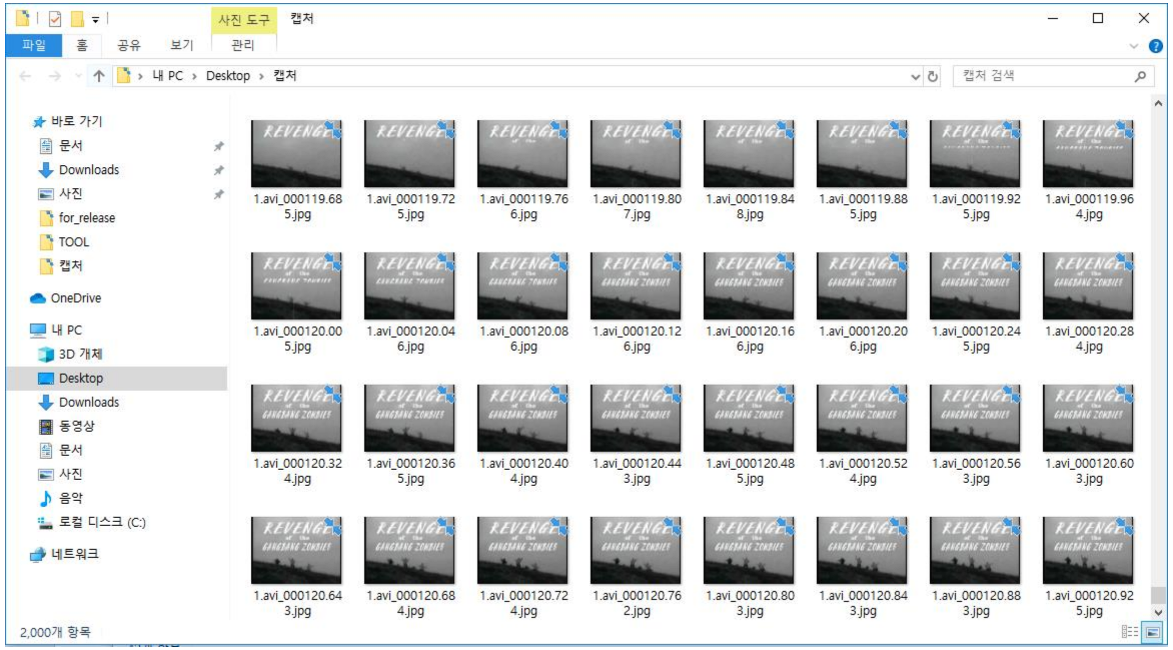
☑ 화면 비율을 보정해서 저장

정보

최종 파일명:

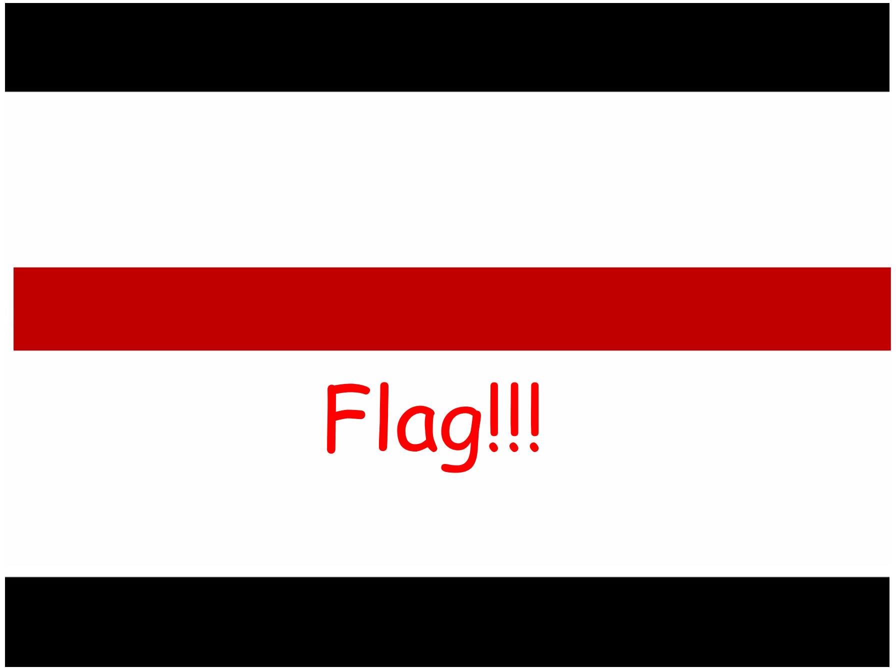
파일 개수:

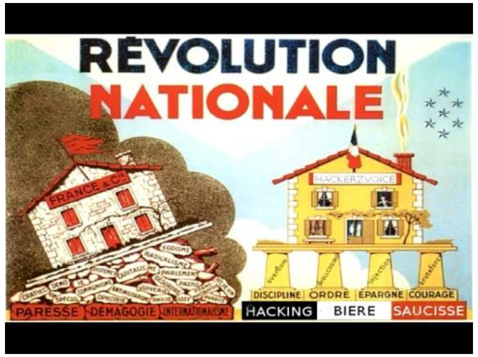
Video problem



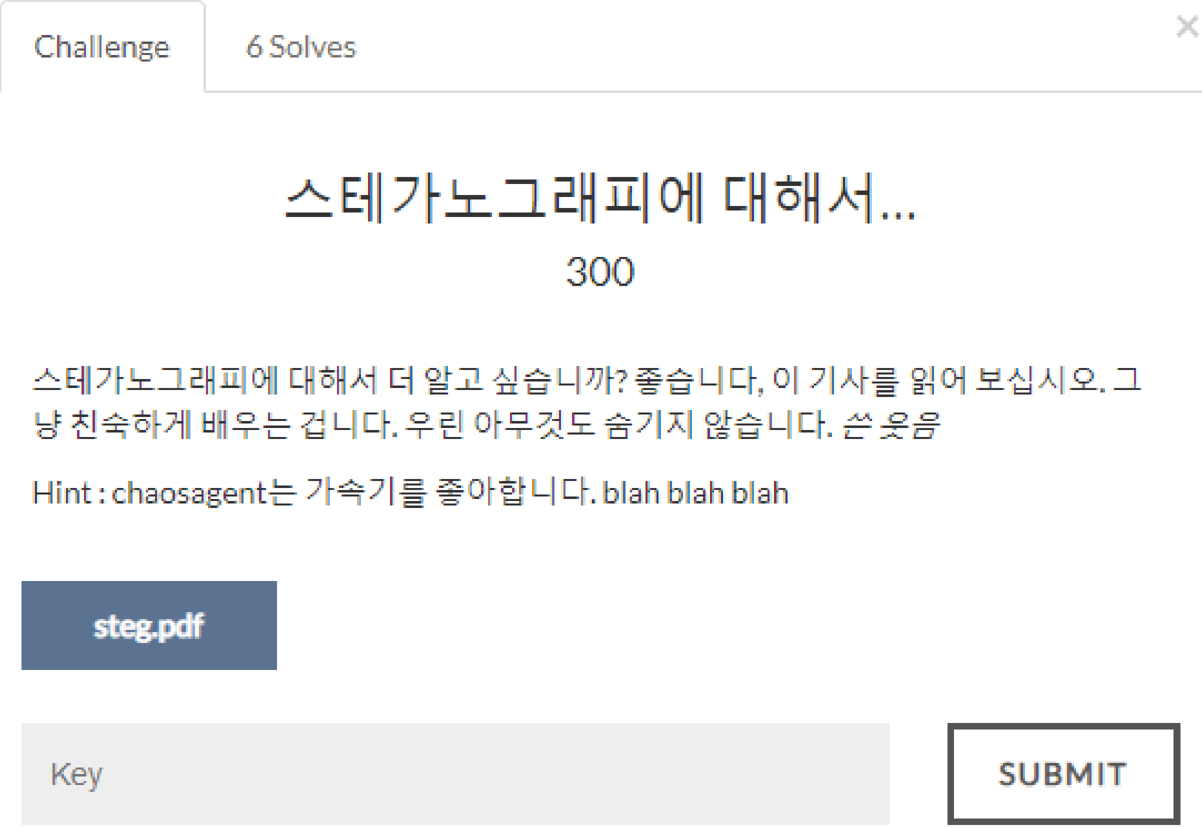
1.avi_000119.685.jpg
1.avi_000119.725.jpg
1.avi_000119.766.jpg
1.avi_000119.807.jpg
1.avi_000119.848.jpg
1.avi_000119.885.jpg
1.avi_000119.925.jpg
1.avi_000119.964.jpg
1.avi_000120.005.jpg
1.avi_000120.046.jpg
1.avi_000120.086.jpg
1.avi_000120.126.jpg
1.avi_000120.166.jpg
1.avi_000120.206.jpg
1.avi_000120.245.jpg
1.avi_000120.284.jpg
1.avi_000120.324.jpg
1.avi_000120.365.jpg
1.avi_000120.404.jpg
1.avi_000120.443.jpg
1.avi_000120.485.jpg
1.avi_000120.524.jpg
1.avi_000120.563.jpg
1.avi_000120.603.jpg
1.avi_000120.643.jpg
1.avi_000120.684.jpg
1.avi_000120.724.jpg
1.avi_000120.762.jpg
1.avi_000120.803.jpg
1.avi_000120.843.jpg
1.avi_000120.883.jpg
1.avi_000120.925.jpg

2,000개 항목




RÉVOLUTION
NATIONALE
HACKERZVOICE
DISCIPLINE ORDRE EPARGNE COURAGE
PARESSE DÉMAGOGIE INTERNATIONALISME
HACKING BIERE SAUCISSE

Audio problem



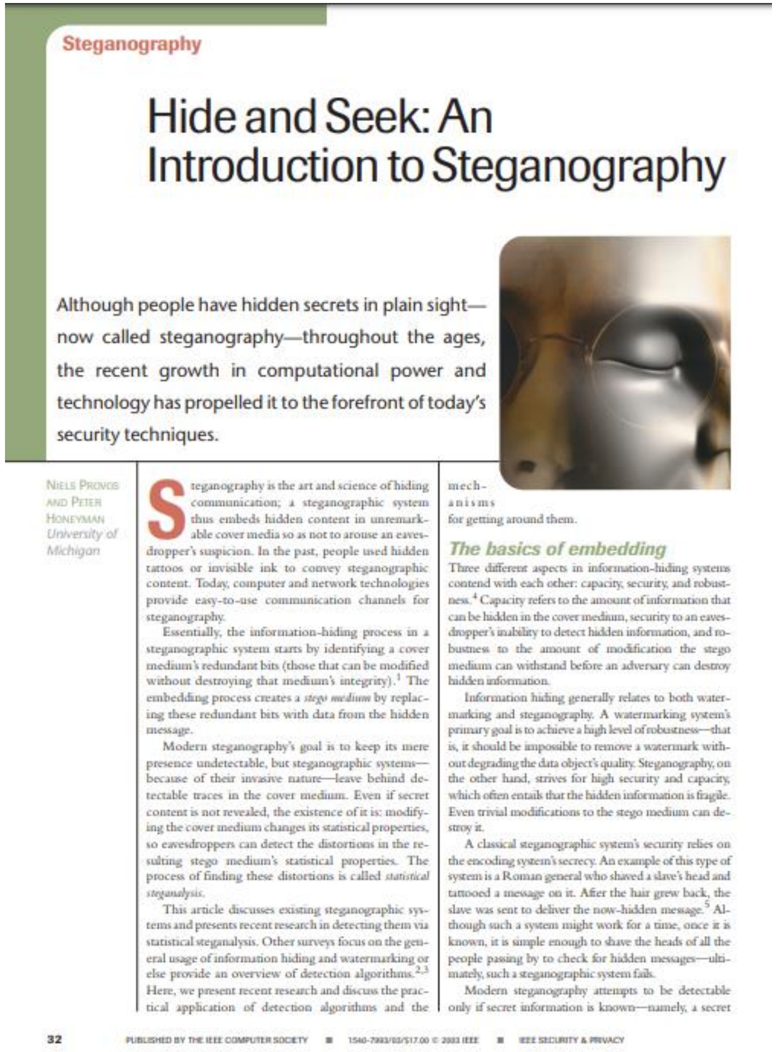
스테가노그래피에 대해서...

300

스테가노그래피에 대해서 더 알고 싶습니까? 좋습니다, 이 기사를 읽어 보십시오. 그냥 친숙하게 배우는 겁니다. 우린 아무것도 숨기지 않습니다. 쓴 웃음

Hint : chaosagent는 가속기를 좋아합니다. blah blah blah

Audio problem



Steganography

Hide and Seek: An Introduction to Steganography

Although people have hidden secrets in plain sight—now called steganography—throughout the ages, the recent growth in computational power and technology has propelled it to the forefront of today's security techniques.

Niels Provos and Peter Honeyman
University of Michigan

Steganography is the art and science of hiding communication; a steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion. In the past, people used hidden tattoos or invisible ink to convey steganographic content. Today, computer and network technologies provide easy-to-use communication channels for steganography.

Essentially, the information-hiding process in a steganographic system starts by identifying a cover medium's redundant bits (those that can be modified without destroying that medium's integrity).[1] The embedding process creates a *stego medium* by replacing these redundant bits with data from the hidden message.

Modern steganography's goal is to keep its mere presence undetectable, but steganographic systems—because of their invasive nature—leave behind detectable traces in the cover medium. Even if secret content is not revealed, the existence of it is: modifying the cover medium changes its statistical properties, so eavesdroppers can detect the distortions in the resulting stego medium's statistical properties. The process of finding these distortions is called *statistical steganalysis*.

This article discusses existing steganographic systems and presents recent research in detecting them via statistical steganalysis. Other surveys focus on the general usage of information hiding and watermarking or else provide an overview of detection algorithms.[2,3] Here, we present recent research and discuss the practical application of detection algorithms and the mechanisms for getting around them.

The basics of embedding

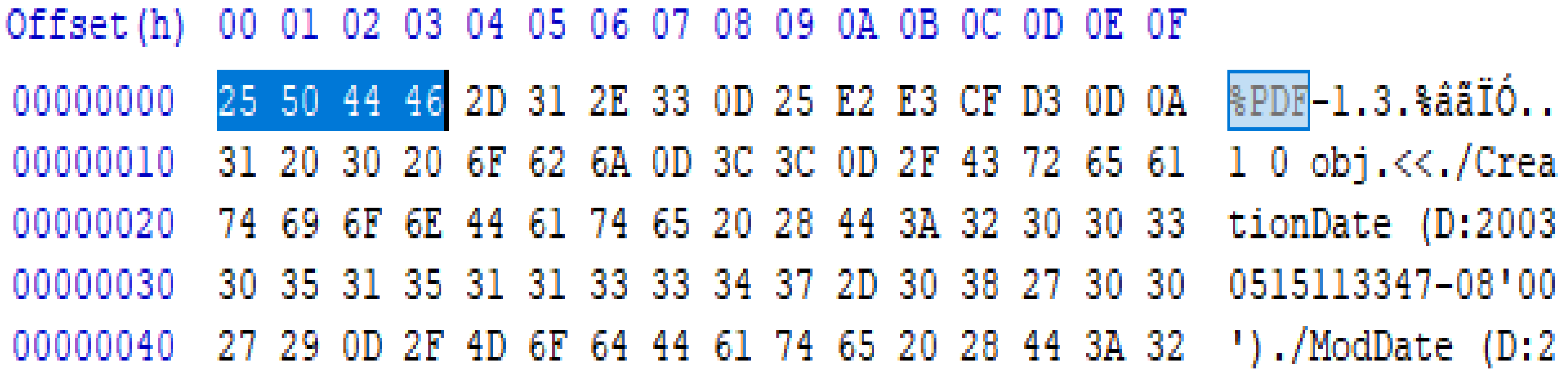
Three different aspects in information-hiding systems contend with each other: capacity, security, and robustness.[4] Capacity refers to the amount of information that can be hidden in the cover medium, security to an eavesdropper's inability to detect hidden information, and robustness to the amount of modification the stego medium can withstand before an adversary can destroy hidden information.

Information hiding generally relates to both watermarking and steganography. A watermarking system's primary goal is to achieve a high level of robustness—that is, it should be impossible to remove a watermark without degrading the data object's quality. Steganography, on the other hand, strives for high security and capacity, which often entails that the hidden information is fragile. Even trivial modifications to the stego medium can destroy it.

A classical steganographic system's security relies on the encoding system's secrecy. An example of this type of system is a Roman general who shaved a slave's head and tattooed a message on it. After the hair grew back, the slave was sent to deliver the now-hidden message.[5] Although such a system might work for a time, once it is known, it is simple enough to shave the heads of all the people passing by to check for hidden messages—ultimately, such a steganographic system fails.

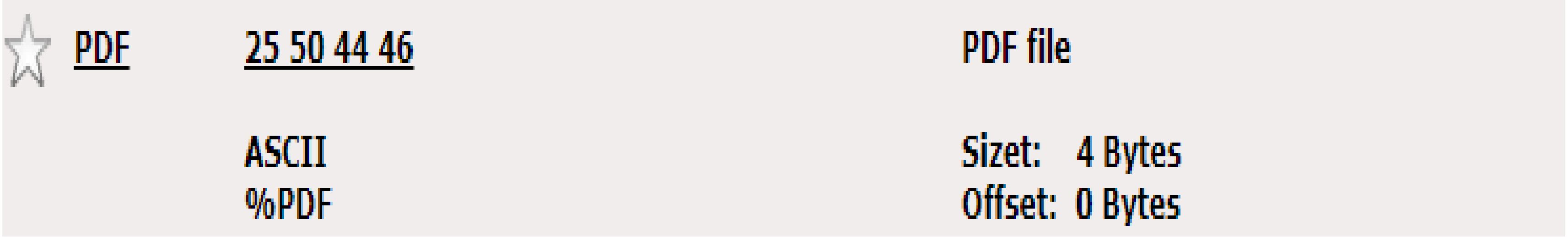
Modern steganography attempts to be detectable only if secret information is known—namely, a secret

32 PUBLISHED BY THE IEEE COMPUTER SOCIETY ■ 1540-7993/03/$17.00 © 2003 IEEE ■ IEEE SECURITY & PRIVACY



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

00000000  25 50 44 46 2D 31 2E 33 0D 25 E2 E3 CF D3 0D 0A  %PDF-1.3.%âãÏÓ..
00000010  31 20 30 20 6F 62 6A 0D 3C 3C 0D 2F 43 72 65 61  1 0 obj.<<./Crea
00000020  74 69 6F 6E 44 61 74 65 20 28 44 3A 32 30 30 33  tionDate (D:2003
00000030  30 35 31 35 31 31 33 33 34 37 2D 30 38 27 30 30  0515113347-08'00
00000040  27 29 0D 2F 4D 6F 64 44 61 74 65 20 28 44 3A 32  ')./ModDate (D:2
```

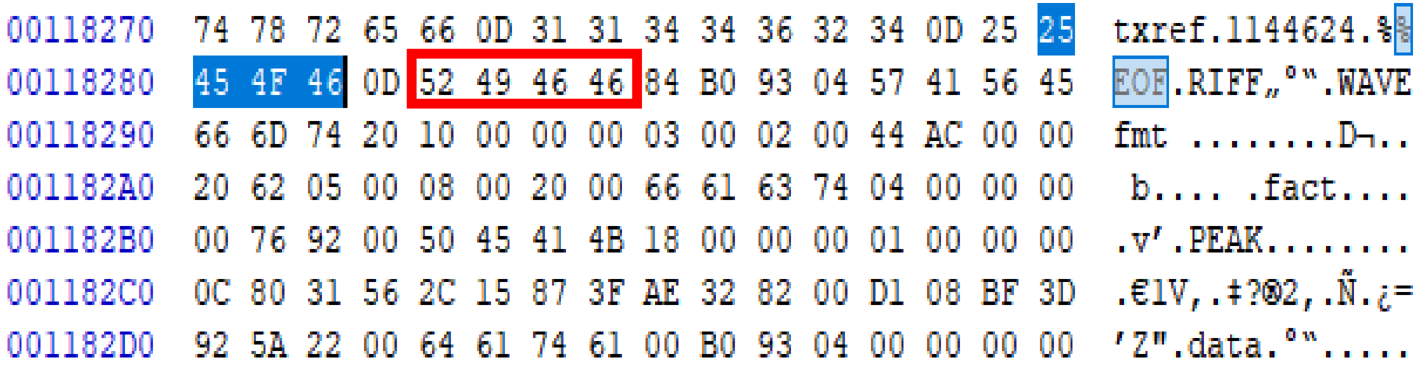


PDF	25 50 44 46	PDF file
	ASCII %PDF	Sizet: 4 Bytes Offset: 0 Bytes

Page 13 ??

Audio problem

PDF FILE: %PDF ~ %EOF

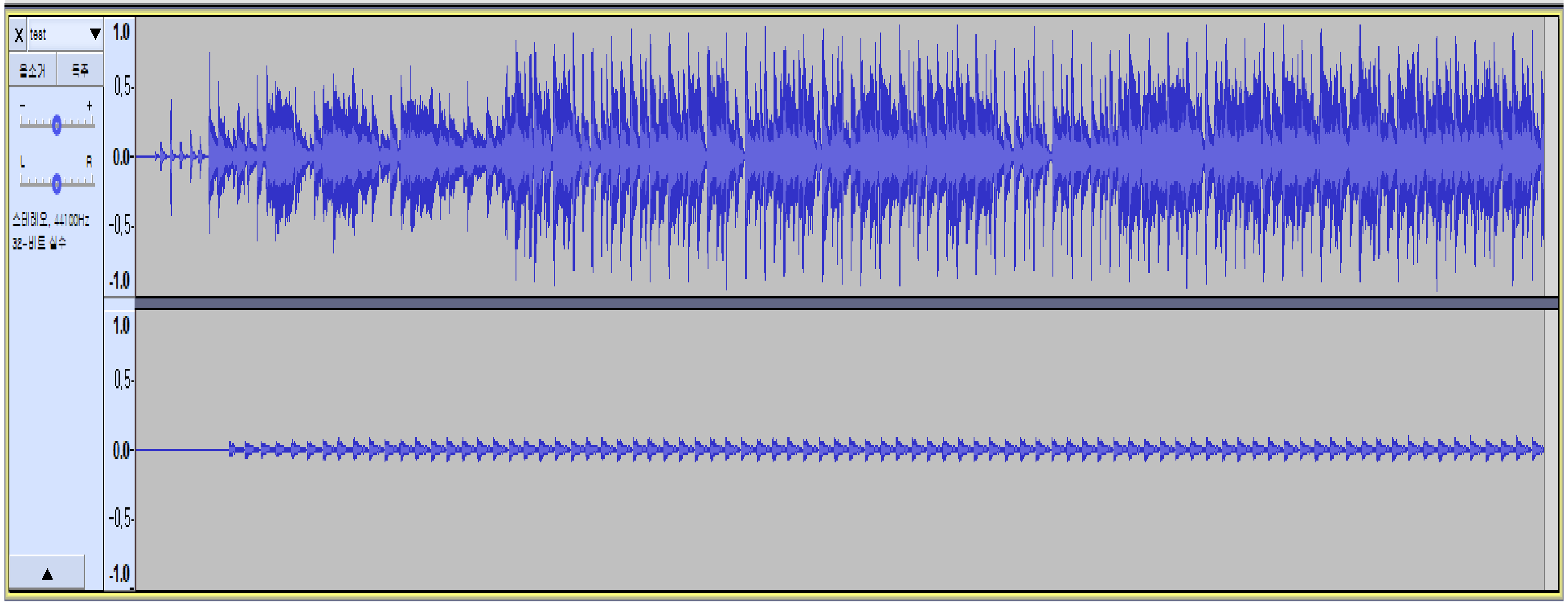


```
00118270  74 78 72 65 66 0D 31 31 34 34 36 32 34 0D 25 25  txref.1144624.%%
00118280  45 4F 46 0D 52 49 46 46 84 B0 93 04 57 41 56 45  EOF.RIFF„°".WAVE
00118290  66 6D 74 20 10 00 00 00 03 00 02 00 44 AC 00 00  fmt ........D¬..
001182A0  20 62 05 00 08 00 20 00 66 61 63 74 04 00 00 00   b.... .fact....
001182B0  00 76 92 00 50 45 41 4B 18 00 00 00 01 00 00 00  .v'.PEAK........
001182C0  0C 80 31 56 2C 15 87 3F AE 32 82 00 D1 08 BF 3D  .€1V,.‡?®2,.Ñ.¿=
001182D0  92 5A 22 00 64 61 74 61 00 B0 93 04 00 00 00 00  'Z".data.°".....
```

WAV FILE???

Audacity

Audio problem



불규칙한 음

높은 음 : 1 , 낮은 음: 0

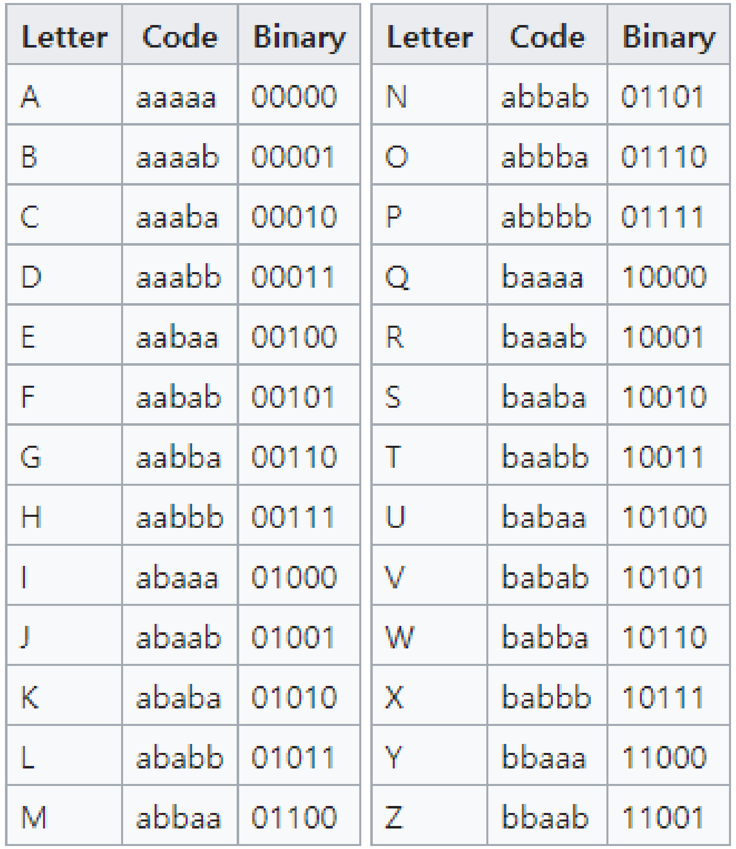
1001100111001000010101011000000011001000100100000100000000100111001101011100110110011

Audio problem

1001100111001000010101011000000011001000100100000100000000100111001101011100110110011

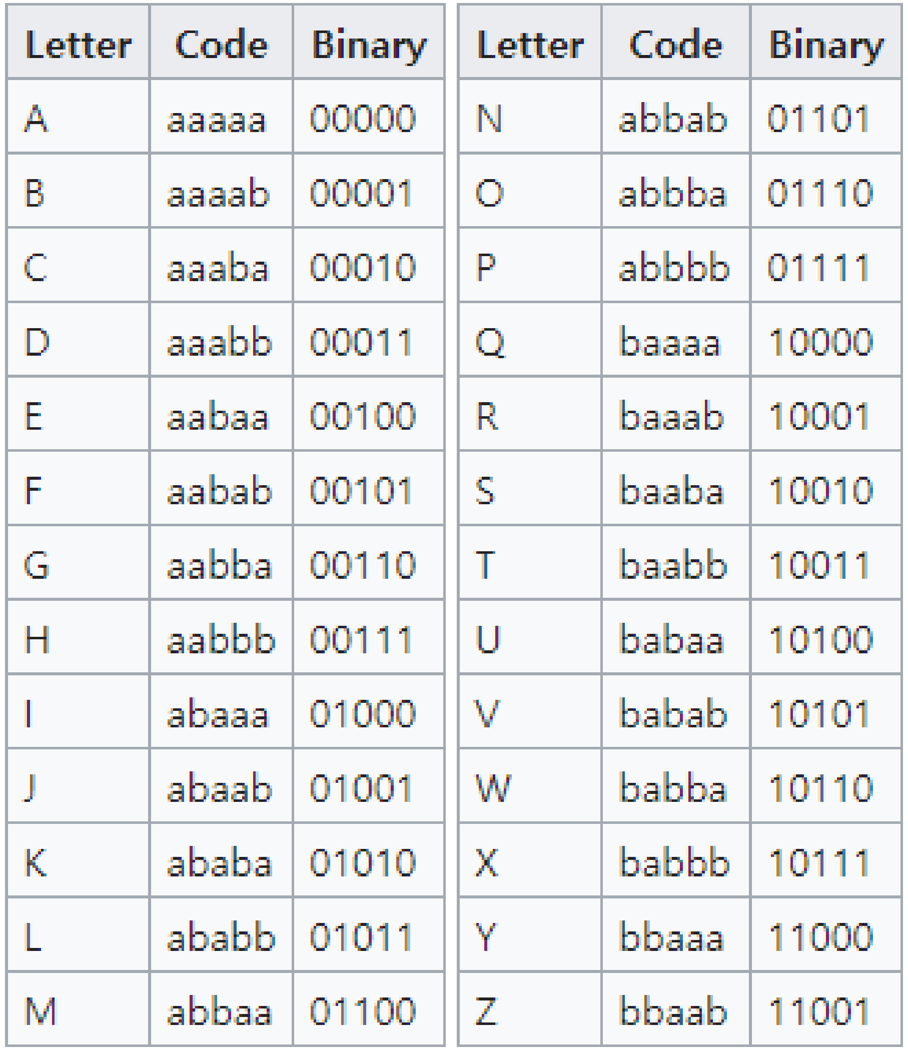
Bacon's cipher ? (Baconian Cipher)

- 스테가노그래피 암호화 방식
- A나 B로 이루어진 5글자의 코드를 문자로 대체하는 방식



Letter	Code	Binary	Letter	Code	Binary
A	aaaaa	00000	N	abbab	01101
B	aaaab	00001	O	abbba	01110
C	aaaba	00010	P	abbbb	01111
D	aaabb	00011	Q	baaaa	10000
E	aabaa	00100	R	baaab	10001
F	aabab	00101	S	baaba	10010
G	aabba	00110	T	baabb	10011
H	aabbb	00111	U	babaa	10100
I	abaaa	01000	V	babab	10101
J	abaab	01001	W	babba	10110
K	ababa	01010	X	babbb	10111
L	ababb	01011	Y	bbaaa	11000
M	abbaa	01100	Z	bbaab	11001

Audio problem



Letter	Code	Binary	Letter	Code	Binary
A	aaaaa	00000	N	abbab	01101
B	aaaab	00001	O	abbba	01110
C	aaaba	00010	P	abbbb	01111
D	aaabb	00011	Q	baaaa	10000
E	aabaa	00100	R	baaab	10001
F	aabab	00101	S	baaba	10010
G	aabba	00110	T	baabb	10011
H	aabbb	00111	U	babaa	10100
I	abaaa	01000	V	babab	10101
J	abaab	01001	W	babba	10110
K	ababa	01010	X	babbb	10111
L	ababb	01011	Y	bbaaa	11000
M	abbaa	01100	Z	bbaab	11001

10011 = T

00111 = H

00100 = E

00101 = F

01011 = L

00000 = A

00110 = G

... FLAG!!!

QnA