
SCA
Created by Unbbal
Digital Forensics
101

SCA

ToC

1 사건 발생: 디지털 흔적이 남았다

2 디지털 포렌식, 이름은 어려운데 사실은?

3 삭제된 파일은 정말 사라졌을까?

4 사진, 문서, 로그가 숨기고 있는 것들

5 파일

6 수사

7 미션

8 모든

사실은?

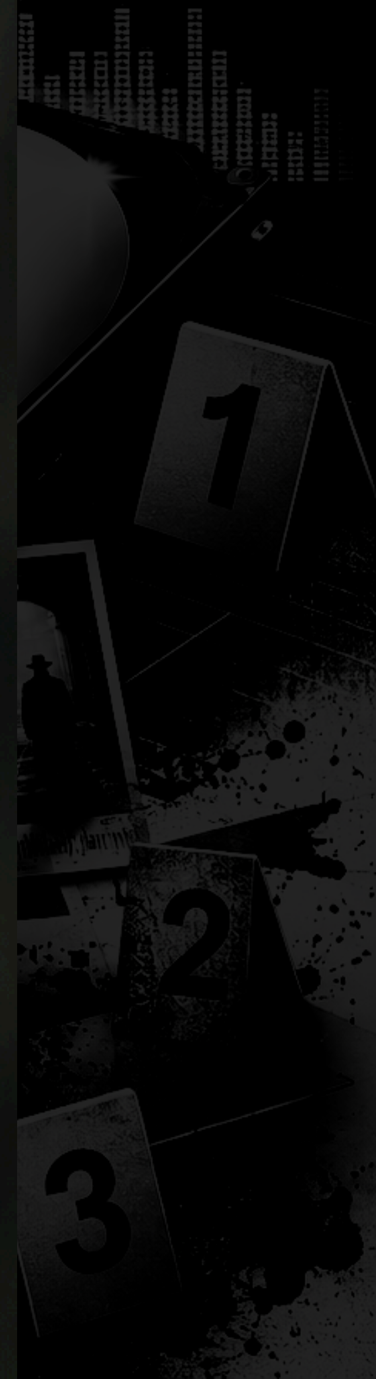
선들

5 파일의 지문: 해시값

6 수사 도구를 열어봅시다

7 미션: 숨겨진 단서를 찾아라

8 모든 디지털 흔적은 이야기를 남긴다

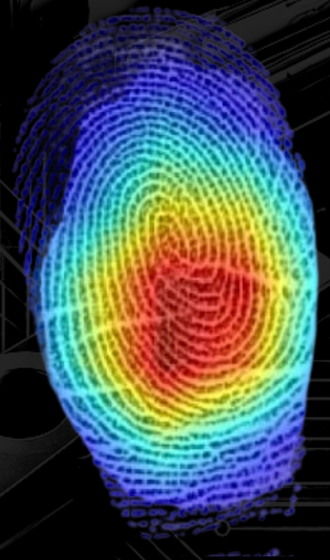


SCA

이름은 어려운데, 사실은 흔적 찾기입니다

포렌식

범죄 과학 수사나 법적 분쟁에서 사용되는
과학적 증거 수집 및 분석 기술



지문



발자국



CCTV

SCA

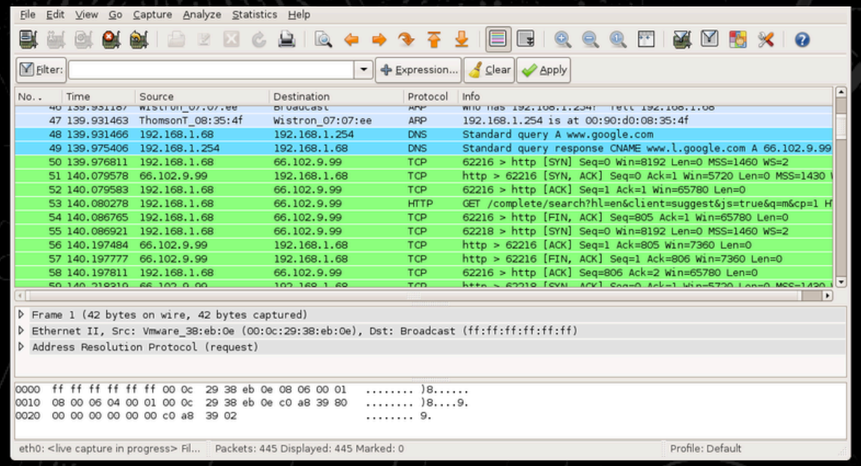
이름은 어려운데, 사실은 흔적 찾기입니다

디지털 포렌식

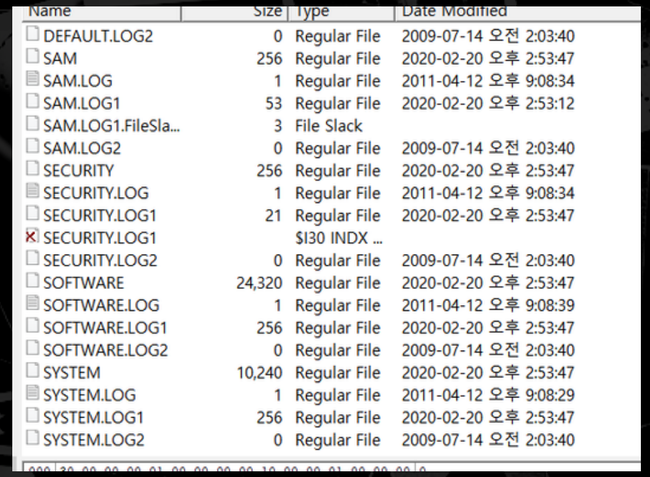
PC, 스마트폰 등 각종 디지털 기기에 남아 있는 데이터를
수집·분석하여 범죄의 단서와 증거를 찾는 과학 수사 기법



Log



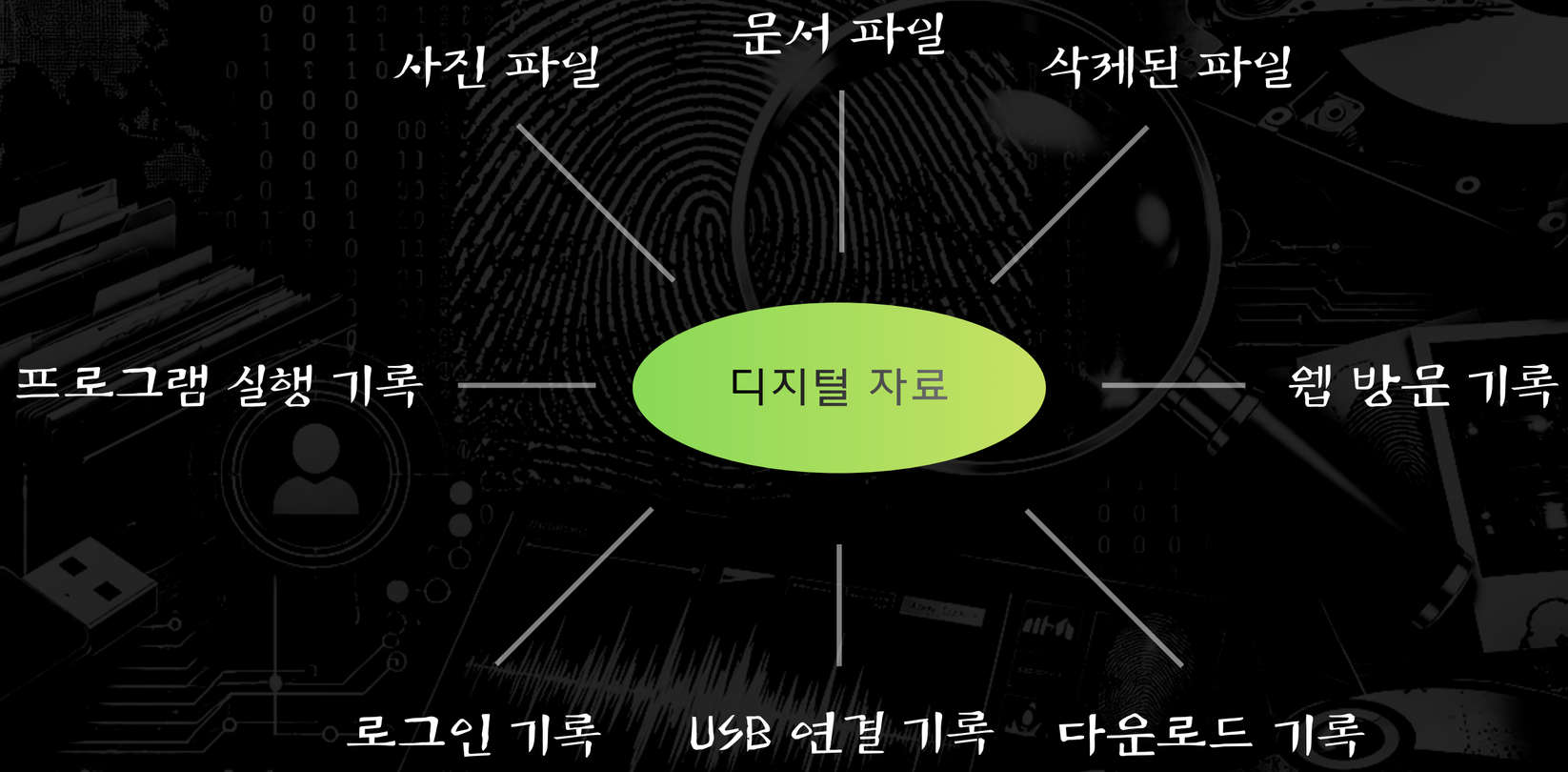
Packet



File

SCA

이름은 어려운데, 사실은 흔적 찾기입니다



SCA

이름은 어려운데, 사실은 흔적 찾기입니다

디지털 자료가 어떻게 증거가 되나요?

관련성

사건과 관련이 있는가?

무결성

중간에 바뀌지 않았는가?

해석 가능성

어떤 의미를 가지는가?

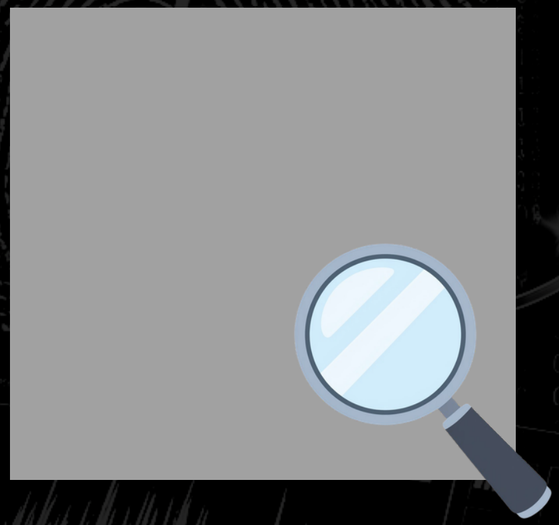
SCA

이름은 어려운데, 사실은 흔적 찾기입니다

디지털 자료가 어떻게 증거가 되나요?



사진 파일



분석

증거

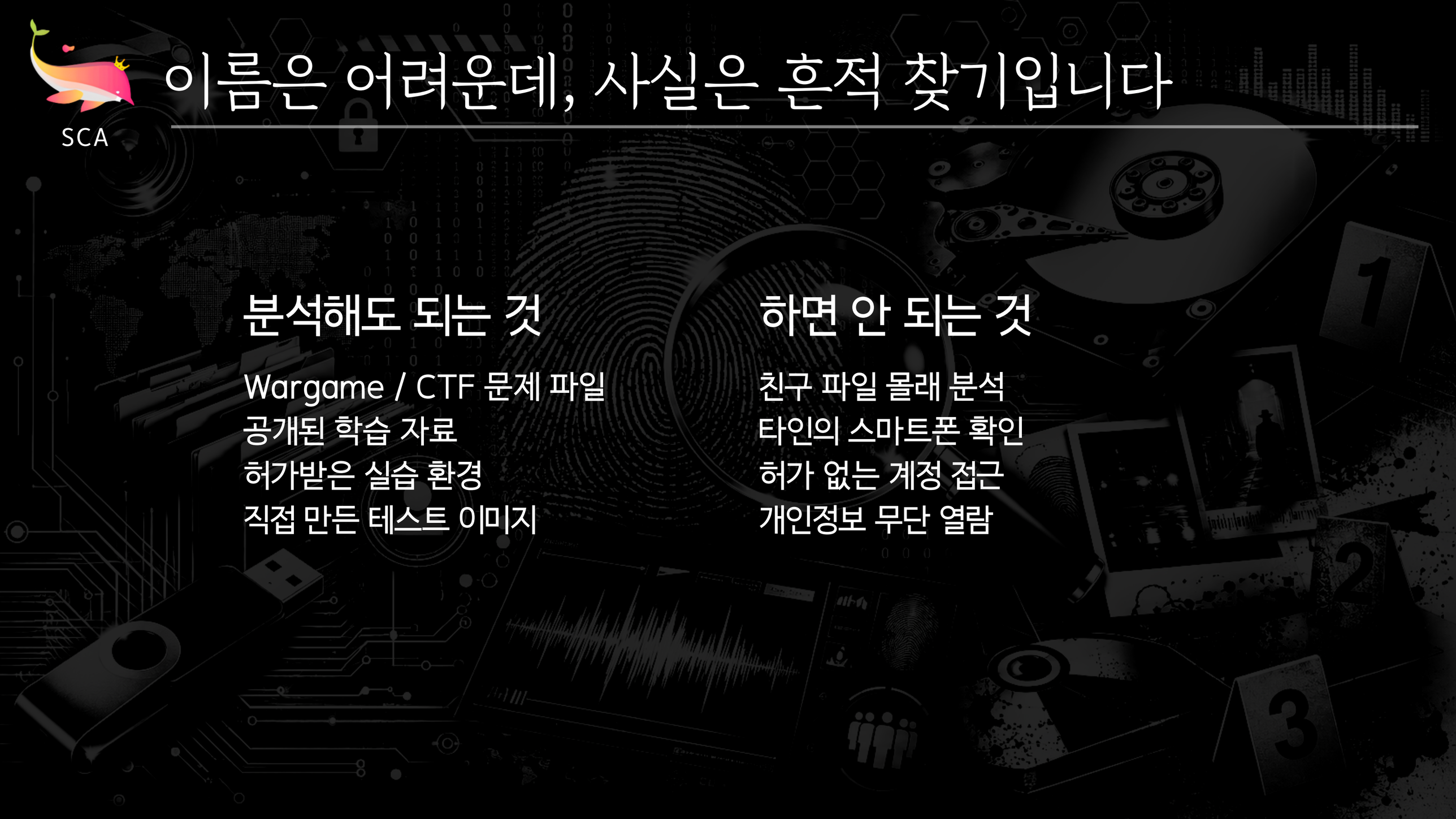
SCA

이름은 어려운데, 사실은 흔적 찾기입니다

잠깐, 이거 아무 데나 써도 되나요?



허가 없는 분석은 수사가 아닙니다



이름은 어려운데, 사실은 흔적 찾기입니다

분석해도 되는 것

Wargame / CTF 문제 파일
공개된 학습 자료
허가받은 실습 환경
직접 만든 테스트 이미지

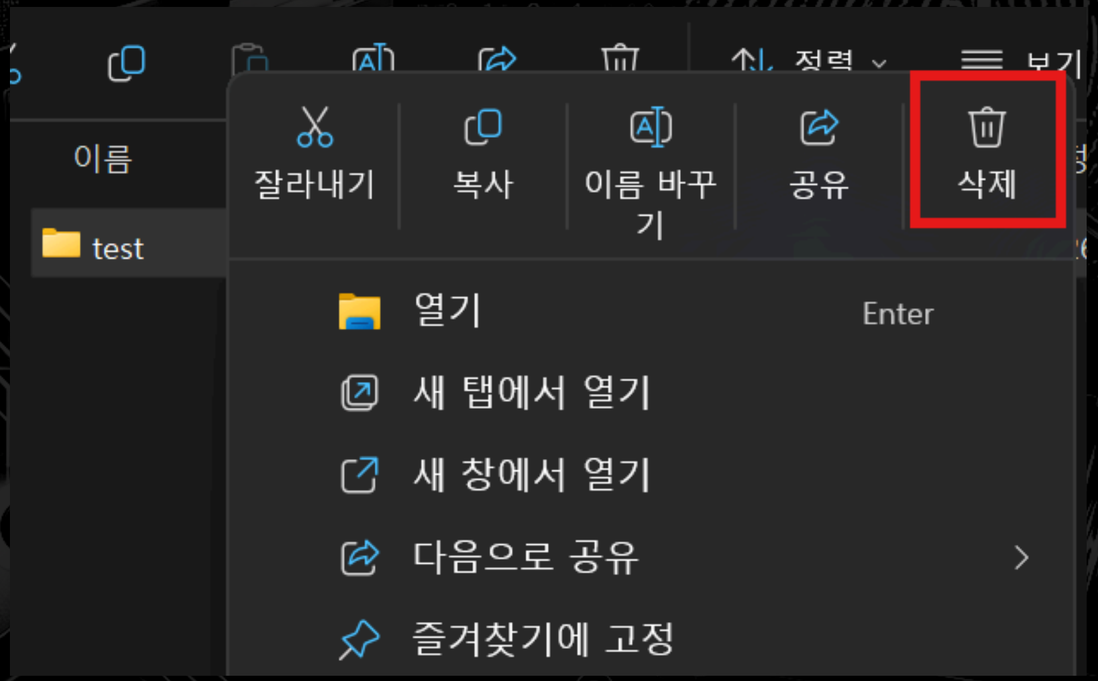
하면 안 되는 것

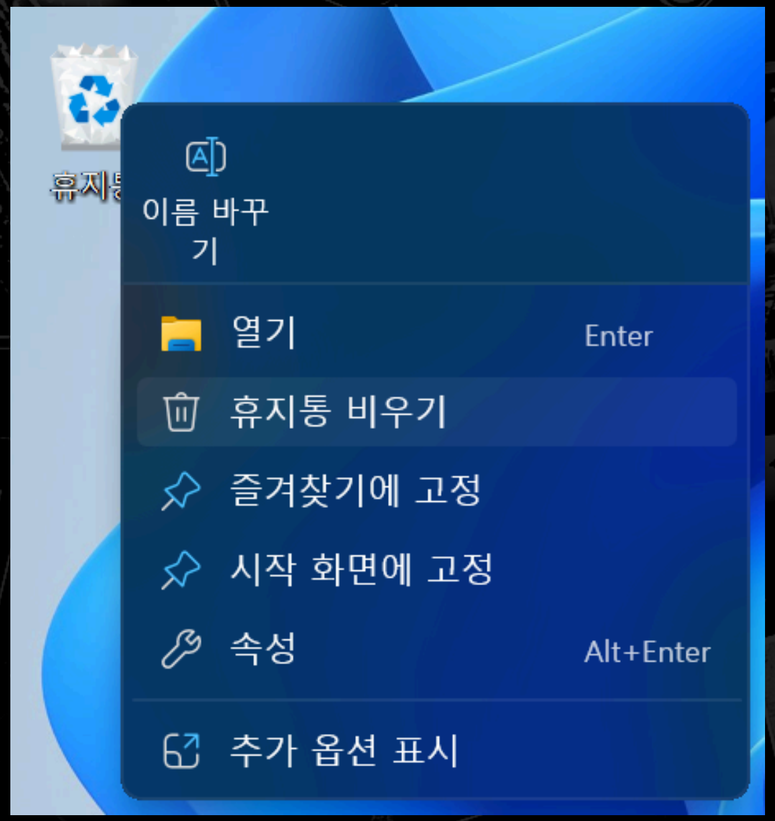
친구 파일 몰래 분석
타인의 스마트폰 확인
허가 없는 계정 접근
개인정보 무단 열람

SCA

삭제 버튼은 만능이 아닙니다

삭제된 파일은 정말 사라졌을까?





SCA

삭제 버튼은 만능이 아닙니다

삭제된 파일은 정말 사라졌을까?

책의 목차에서 제목만 지운 것과 비슷하다.



= 사라진 게 아니라 안 보이는 상태

SCA

파일은 생각보다 수다쟁이입니다



Make	Apple
Model	iPhone 14 Plus
Orientation	6
XResolution	72
YResolution	72
ResolutionUnit	2
Software	26.5
ModifyDate	Mon Jun 01 2026 18:14:42 GMT+0900 (한국 표준시)
HostComputer	iPhone 14 Plus
YCbCrPositioning	1
GPSLatitudeRef	N
GPSLatitude	37.6278
GPSLongitudeRef	E
GPSLongitude	126.9242
GPSAltitudeRef	0
GPSAltitude	83.4394
GPSTimeStamp	0,14,42
GPSSpeedRef	K
GPSSpeed	0
GPSImgDirectionRef	T
GPSImgDirection	71.7303
GPSDestBearingRef	T
GPSDestBearing	71.7303
GPSDateStamp	2026:06:01
GPSHPositioningError	13.4047
ExposureTime	0.0167
FNumber	1.5000
ExposureProgram	2
ISO	250
DateTimeOriginal	Mon Jun 01 2026 18:14:42 GMT+0900 (한국 표준시)

메타데이터: 파일 안의 숨은 설명서

SCA

파일은 생각보다 수다쟁이입니다

Make	Apple
Model	iPhone 14 Plus
Orientation	6
XResolution	72
YResolution	72
ResolutionUnit	2
Software	26.5
ModifyDate	Mon Jun 01 2026 18:14:42 GMT+0900 (한국 표준시)
HostComputer	iPhone 14 Plus
YCbCrPositioning	1
GPSLatitudeRef	N
GPSLatitude	37.6278
GPSLongitudeRef	E
GPSLongitude	126.9242
GPSAltitudeRef	0
GPSAltitude	83.4394
GPSTimeStamp	0,14,42
GPSSpeedRef	K
GPSSpeed	0
GPSImgDirectionRef	T
GPSImgDirection	71.7303
GPSDestBearingRef	T
GPSDestBearing	71.7303
GPSDateStamp	2026:06:01
GPSHPositioningError	13.4047
ExposureTime	0.0167
FNumber	1.5000
ExposureProgram	2
ISO	250
DateTimeOriginal	Mon Jun 01 2026 18:14:42 GMT+0900 (한국 표준시)

촬영 시간
사용 기기
이미지 크기
편집 프로그램
위치 정보 여부
...



SCA

파일은 생각보다 수다쟁이입니다

1m 21s 동안 생각함 ›

EXIF만 보면 **서울특별시 은평구 쪽**, 더 좁히면 **연신내역 북쪽 ~ 구파발역 남동쪽 사이**, 대략 **갈현동/진관동 경계 근처**로 보입니다.

근거는 여기입니다:

- GPS 좌표: **37.6278, 126.9242**
- 연신내역 좌표가 약 **37.61889, 126.92139**라서, 사진 위치는 연신내역에서 **북쪽으로 약 1km** 떨어진 지점입니다. 위키백과
- 구파발역 좌표가 약 **37.6367, 126.9188**이라서, 사진 위치는 구파발역에서 **남동쪽으로 약 1.1km** 정도입니다. Observable
- EXIF의 `GPSHPositioningError`가 **13.4m**라서, 실제 촬영 위치는 이 좌표 주변 **반경 10~20m 정도**로 꽤 정확합니다.

결론: **서울 은평구 갈현동 북쪽, 진관동/구파발 방면으로 올라가는 쪽**에서 찍힌 사진일 가능성이 큽니다.
건물명까지는 지도 없이 확정하긴 어렵지만, 동네 단위로는 거의 이쪽입니다.

SCA

파일에도 지문이 있다고요?



사람



지문



파일



해시값

SCA

파일에도 지문이 있다고요?

Hash의 종류

MD5
MD4
SHA1
SHA256
SHA384
SHA512
RIPEMD 160
PANAMA
TIGER
MD2
ADLER32
CRC32
...

대표적인 해시 알고리즘

SCA

파일에도 지문이 있다고요?

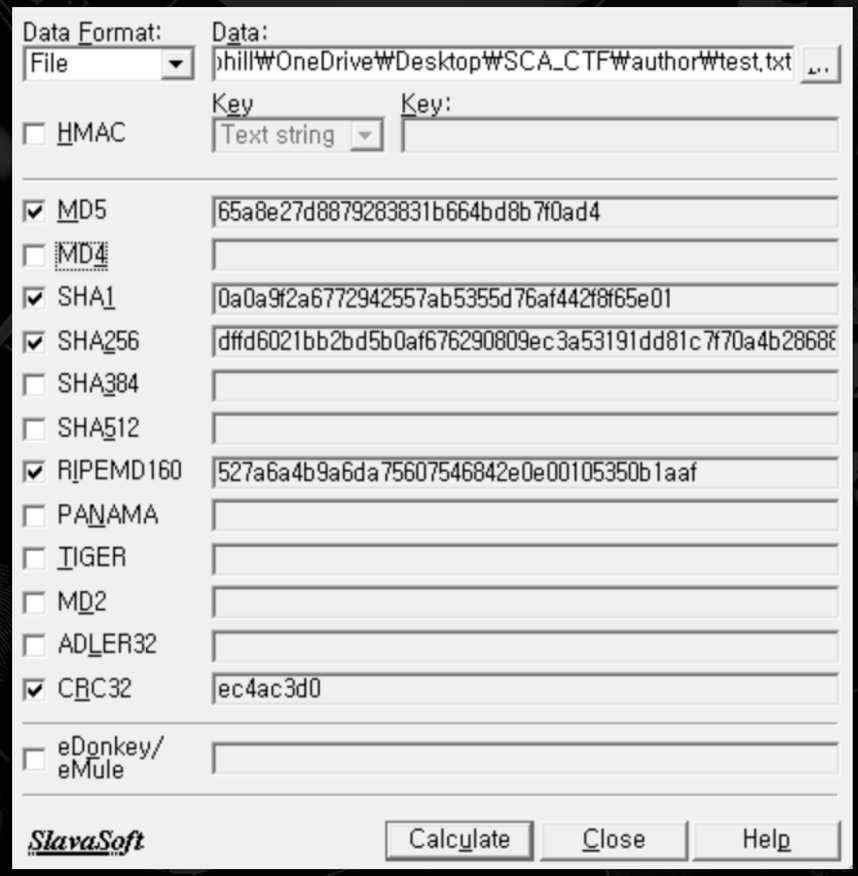


test.txt

파일 편집 보기

Hello, World!

HashCalc

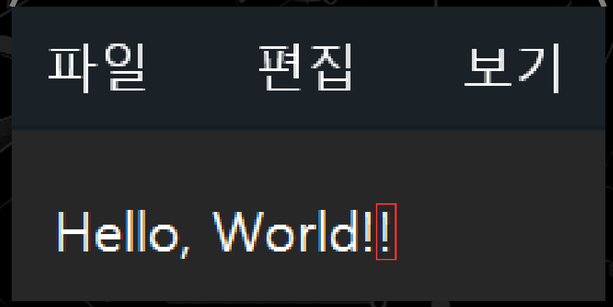


SCA

파일에도 지문이 있다고요?

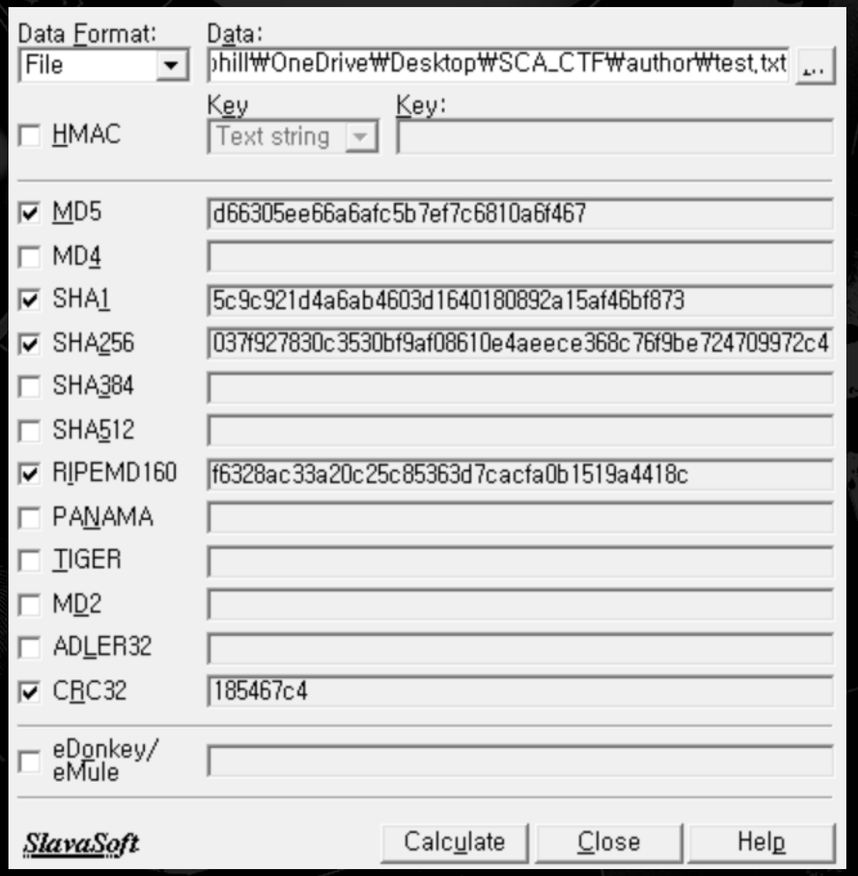


test.txt



한 글자만 바뀌어도
해시값은 바뀐다.

HashCalc

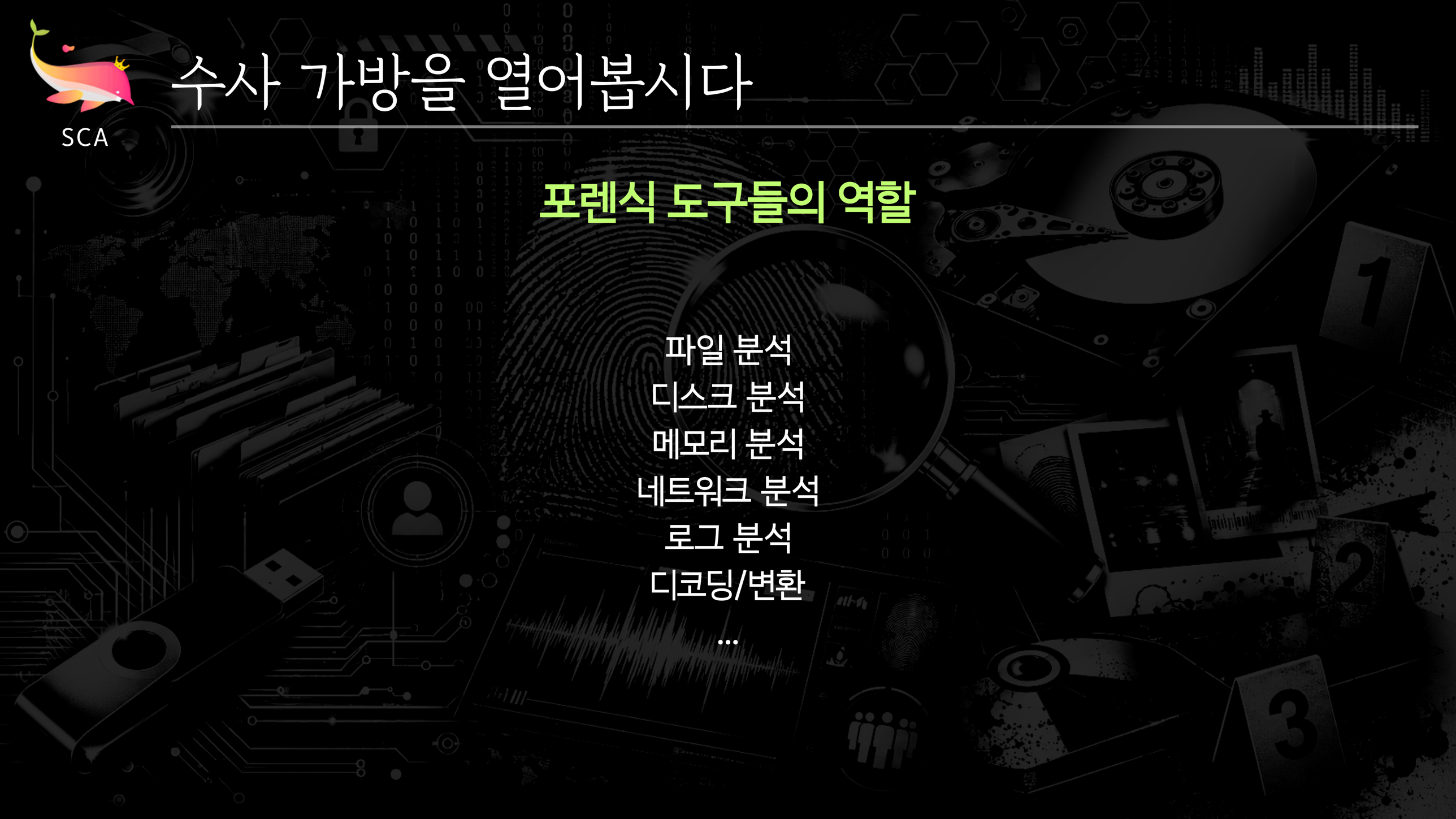


SCA

파일에도 지문이 있다고요?

해시값을 사용하는 이유와 특징

- 변조 탐지 (파일이 바뀌었는지 확인)
- 고정된 길이 (큰 데이터를 고정된 크기로 압축)
- 단방향성 (해시값으로 원래 데이터가 무엇이였는지 역추적 불가)
- 눈사태 효과 (1글자만 바뀌어도 값이 아예 달라짐)


SCA
수사 가방을 열어봅시다
포렌식 도구들의 역할
파일 분석
디스크 분석
메모리 분석
네트워크 분석
로그 분석
디코딩/변환
...
1
2
3

SCA

수사 가방을 열어봅시다

포렌식 도구들의 종류

파일 분석 도구
HxD
xxd
strings
binwalk

메타데이터 도구
exiftool
Metadata2Go
파일 속성 창

디코딩/변환 도구
CyberChef

디스크 분석 도구
FTK Imager
Autopsy
PhotoRec
TestDisk
WinPrefetchView

메모리 분석 도구
Volatility 3
MemProcFS
strings

네트워크 분석 도구
Wireshark
NetworkMiner
tcpdump
tshark

로그 분석 도구
Event Viewer
EvtxECmd
Timeline Explorer
grep
jq

이미지/오디오 포렌식 도구
Steganography Online
Audacity
zsteg



수사 가방을 열어봅시다

포렌식 도구들의 종류

파일 분석 도구
HxD
xxd
strings
binwalk

메타데이터 도구
exiftool
Metadata2Go
파일 속성 창

디코딩/변환 도구
CyberChef

디스크 분석 도구
FTK Imager
Autopsy
PhotoRec
TestDisk
WinPrefetchView

메모리 분석 도구
Volatility 3
MemProcFS
strings

네트워크 분석 도구
Wireshark
NetworkMiner
tcpdump
tshark

로그 분석 도구
Event Viewer
EvtxECmd
Timeline Explorer
grep
jq

이미지/오디오 포렌식 도구
Steganography Online
Audacity
zsteg

SCA

수사 가방을 열어봅시다

파일 분석 도구

HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography Online
grep
Audacity



- 대표적인 무료 헥사 에디터 소프트웨어
- JPG, PNG 등의 파일 등을 헥사 단위로 분석 및 변경 가능

SCA

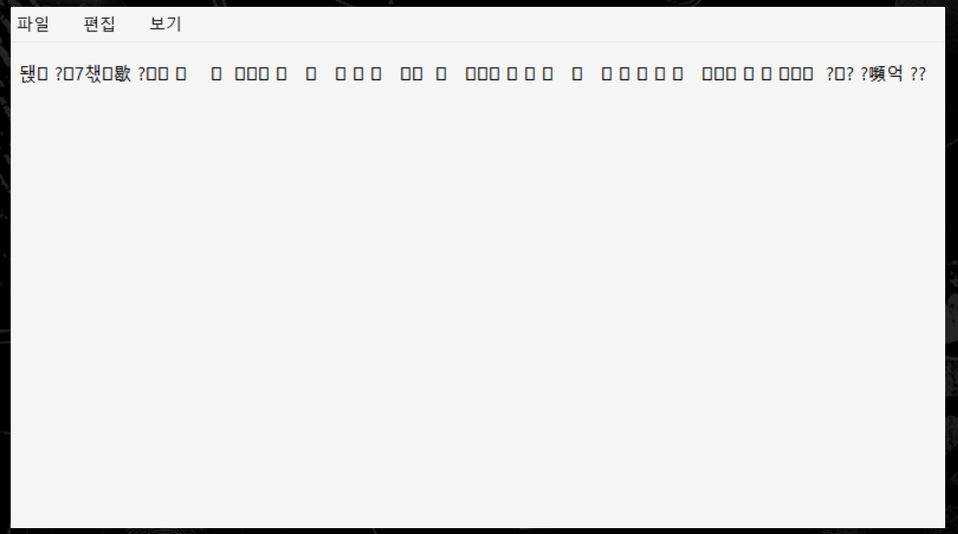
수사 가방을 열어봅시다

파일 분석 도구

HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography Online
grep
Audacity

이런 파일을 메모장으로 열면?





글자가 깨져서 보인다.

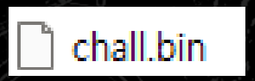
SCA

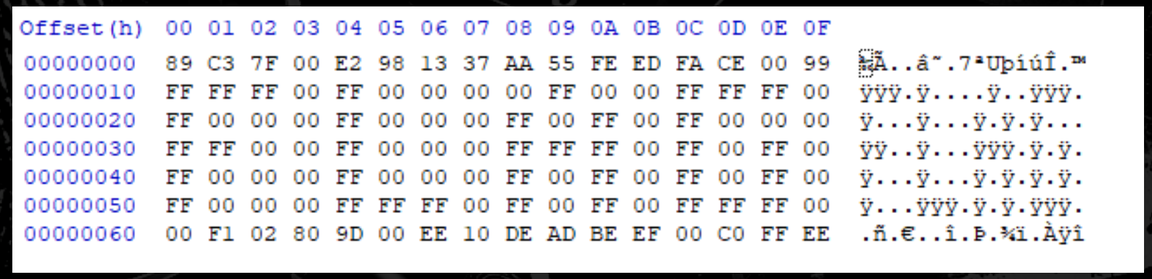
수사 가방을 열어봅시다

파일 분석 도구

HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography Online
grep
Audacity

이런 파일을 HxD으로 열면?





Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	89	C3	7F	00	E2	98	13	37	AA	55	FE	ED	FA	CE	00	99	‰Ã..â˜.7ªUþíúÎ.™
00000010	FF	FF	FF	00	FF	00	00	00	00	FF	00	00	FF	FF	FF	00	ÿÿÿ.ÿ....ÿ..ÿÿÿ.
00000020	FF	00	00	00	FF	00	00	00	FF	00	FF	00	FF	00	00	00	ÿ...ÿ...ÿ.ÿ.ÿ...
00000030	FF	FF	00	00	FF	00	00	00	FF	FF	FF	00	FF	00	FF	00	ÿÿ..ÿ...ÿÿÿ.ÿ.ÿ.
00000040	FF	00	00	00	FF	00	00	00	FF	00	FF	00	FF	00	FF	00	ÿ...ÿ...ÿ.ÿ.ÿ.ÿ.
00000050	FF	00	00	00	FF	FF	FF	00	FF	00	FF	00	FF	FF	FF	00	ÿ...ÿÿÿ.ÿ.ÿ.ÿÿÿ.
00000060	00	F1	02	80	9D	00	EE	10	DE	AD	BE	EF	00	C0	FF	EE	.ñ.€..î.Þ.¾ï.Àÿî

메모장으로 보지 못했던 내용들을 확인할 수 있다.

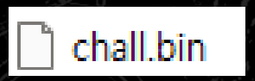
SCA

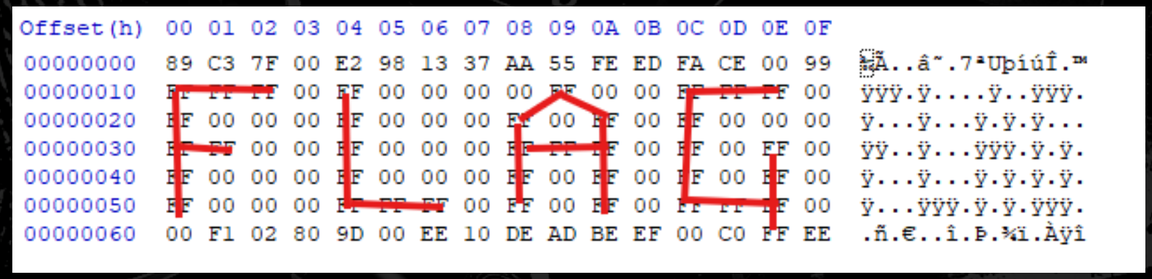
수사 가방을 열어봅시다

파일 분석 도구

HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography Online
grep
Audacity

이런 파일을 HxD으로 열면?





메모장으로 보지 못했던 내용들을 확인할 수 있다.

SCA

수사 가방을 열어봅시다

파일 분석 도구

HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography Online
grep
Audacity

평소 사용 용도

- 바이트 단위로 분석
- 파일 형식 확인
- 숨겨진 문자열이나 특정 hex 패턴을 찾아내기
- 오프셋을 이용해 데이터의 정확한 위치를 확인
- 바이트 수정 (깨져있는 파일 복구, 이미지 크기 조정 등)

SCA

수사 가방을 열어봅시다

파일 분석 도구

HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography Online
grep
Audacity

```
ph1l1lp@DESKTOP-3LHD5Q:/mnt/c/Users/김필립/Downloads$ binwalk firmware.bin
```

- 파일 안에 숨겨져 있거나 끼워 넣어진 파일 구조를 찾아주는 분석 도구

SCA

수사 가방을 열어봅시다

파일 분석 도구

HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography Online
grep
Audacity

```
ph1l1lp@DESKTOP-3LHD5Q:/mnt/c/Users/김필립/Downloads$ binwalk firmware.bin
```

- 파일 안에 숨겨져 있거나 끼워 넣어진 파일 구조를 찾아주는 분석 도구

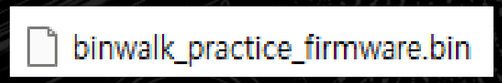
SCA

수사 가방을 열어봅시다

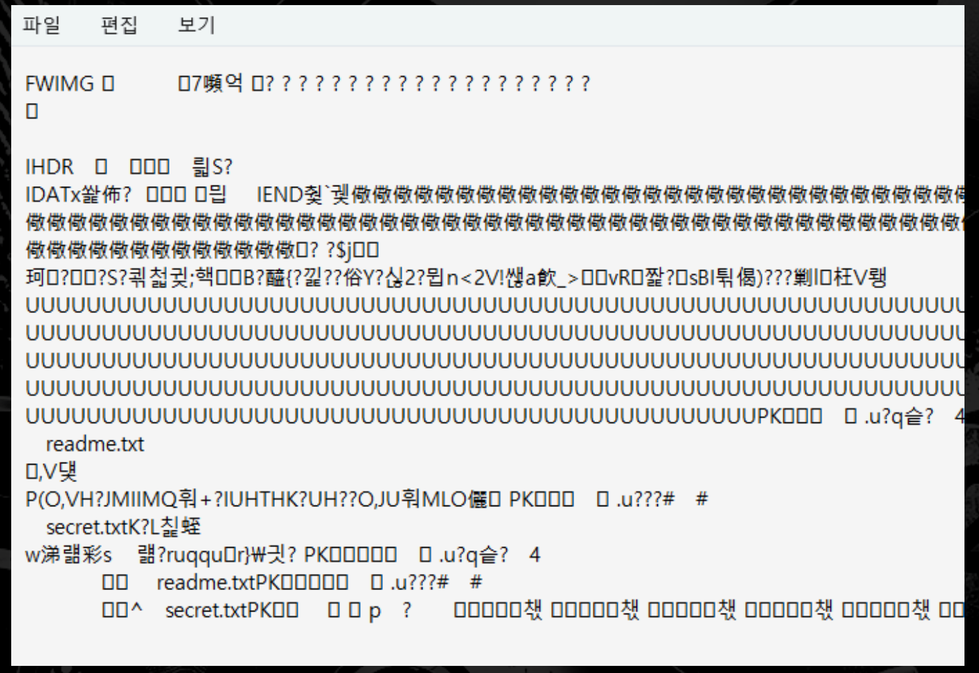
파일 분석 도구

HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography Online
grep
Audacity

메모장으로 열면?







SCA

수사 가방을 열어봅시다

파일 분석 도구

HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography Or
grep
Audacity

binwalk 사용

```
ph1l1lp@DESKTOP-3LHD5Q:/mnt/c/Users/김필립/Downloads$ binwalk firmware.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
256           0x100           PNG image, 1 x 1, 8-bit/color RGB, non-interlaced
297           0x129           Zlib compressed data, default compression
768           0x300           gzip compressed data, maximum compression, last modified: 2026-06-06
14:41:29
1536          0x600           Zip archive data, at least v2.0 to extract, compressed size: 54,
uncompressed size: 52, name: readme.txt
1630          0x65E           Zip archive data, at least v2.0 to extract, compressed size: 35,
uncompressed size: 35, name: secret.txt
1817          0x719           End of Zip archive, footer length: 22
```

png 파일 및 zip파일이 숨겨져 있는걸 확인할 수 있음.

SCA

수사 가방을 열어봅시다

파일 분석 도구

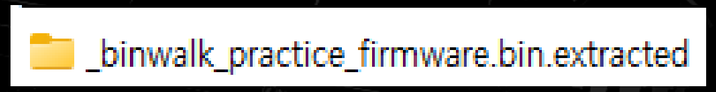
HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography Online
grep
Audacity

binwalk 사용
추출하고 싶다면 -e 사용

```
ph1l1lp@DESKTOP-3LHD5Q:/mnt/c/Users/김필립/Downloads$ binwalk -e firmware.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
256           0x100           PNG image, 1 x 1, 8-bit/color RGB, non-interlaced
297           0x129           Zlib compressed data, default compression
768           0x300           gzip compressed data, maximum compression, last modified: 2026-06-06
14:41:29

WARNING: Extractor.execute failed to run external extractor 'jar xvf '%e'': [Errno 13] Permission denied:
'jar', 'jar xvf '%e'' might not be installed correctly
1536          0x600           Zip archive data, at least v2.0 to extract, compressed size: 54,
uncompressed size: 52, name: readme.txt
1630          0x65E           Zip archive data, at least v2.0 to extract, compressed size: 35,
uncompressed size: 35, name: secret.txt
1817          0x719           End of Zip archive, footer length: 22
```

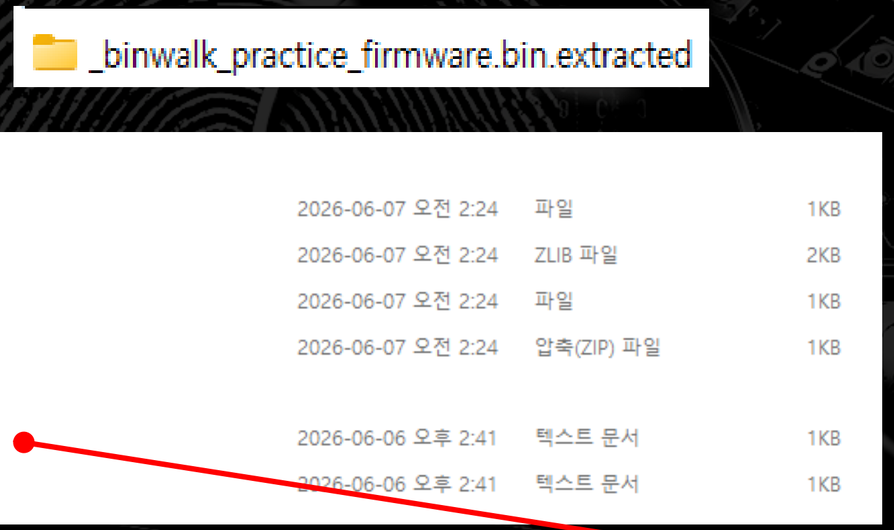


SCA

수사 가방을 열어봅시다

파일 분석 도구

- HxD
- binwalk
- 파일 속성 창
- CyberChef
- FTK Imager
- WinPrefetchView
- Wireshark
- Steganography Online
- grep
- Audacity



flag{BINWALK_FINDS_EMBEDDED_FILES}

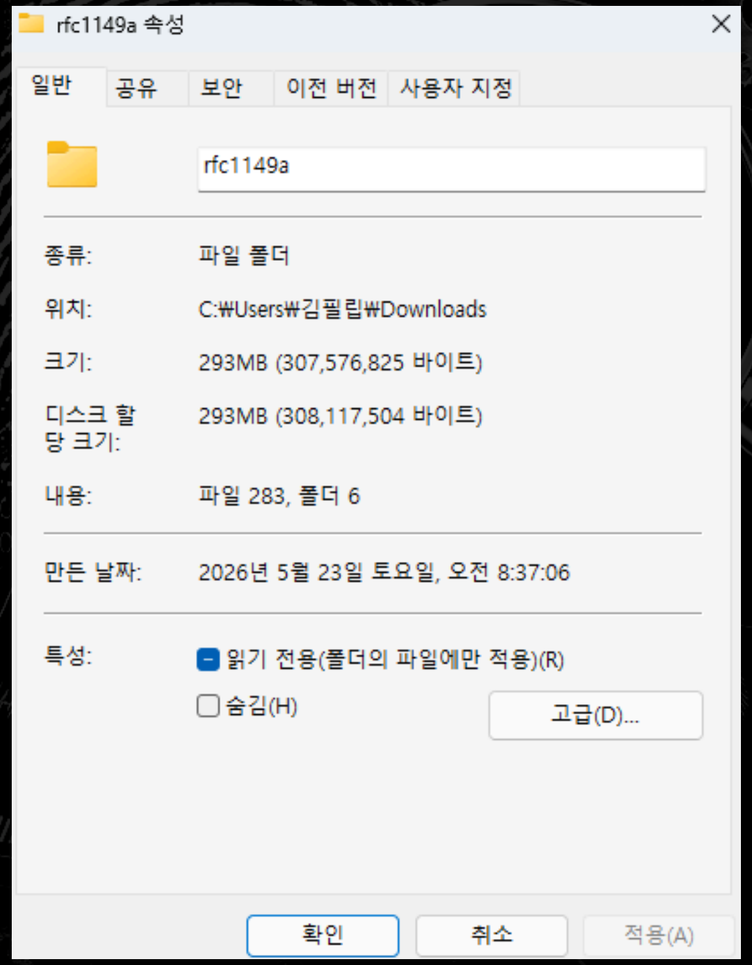
This ZIP was embedded inside a fake firmware image.

SCA

수사 가방을 열어봅시다

HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography Online
grep
Audacity

메타데이터 도구



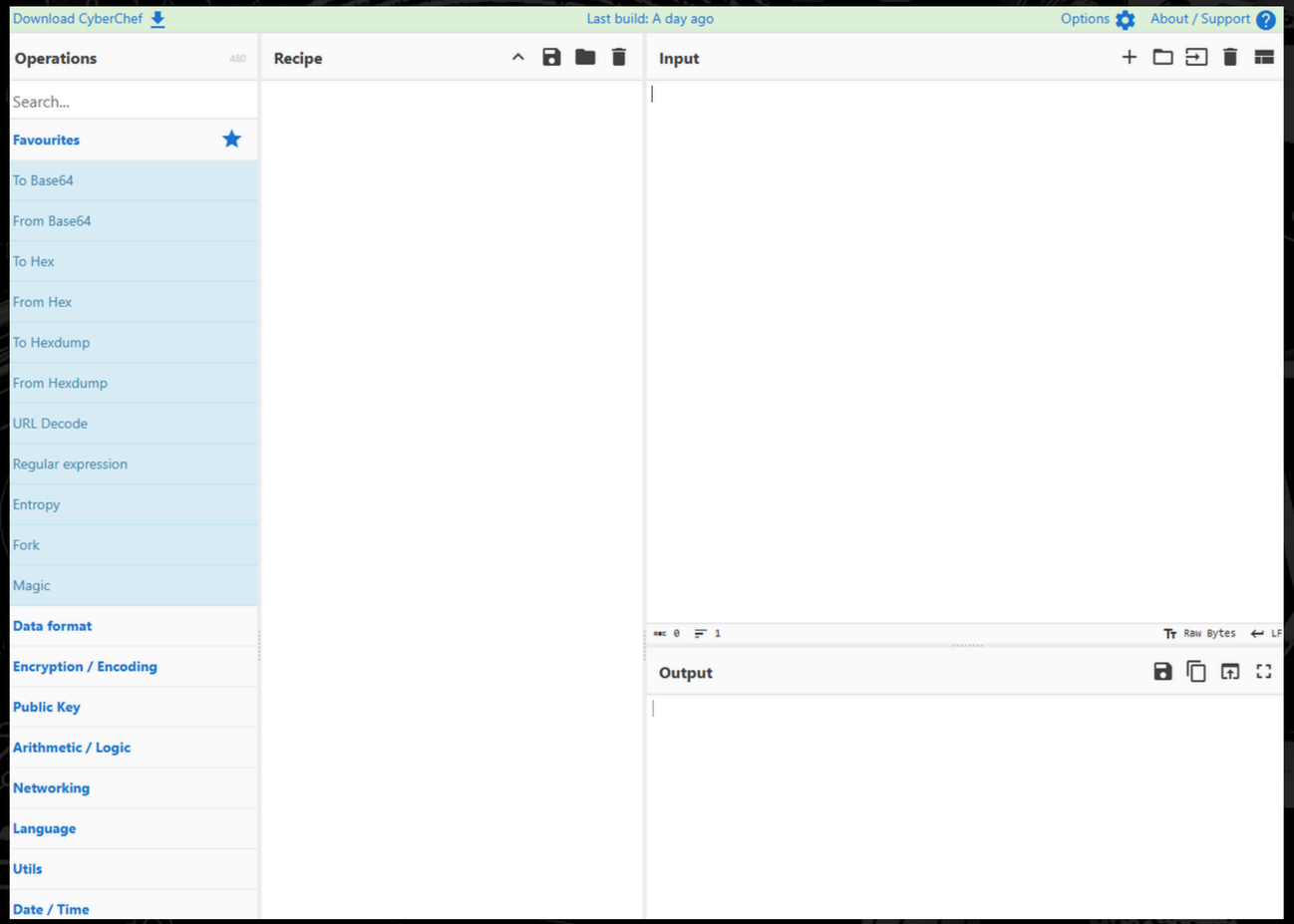
파일 이름
파일 형식
파일 크기
생성 날짜
수정 날짜
마지막 접근 날짜
파일 위치
권한 정보
작성자 정보
사진 촬영 정보

SCA

수사 가방을 열어봅시다

HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography Online
grep
Audacity

디코딩/변환 도구



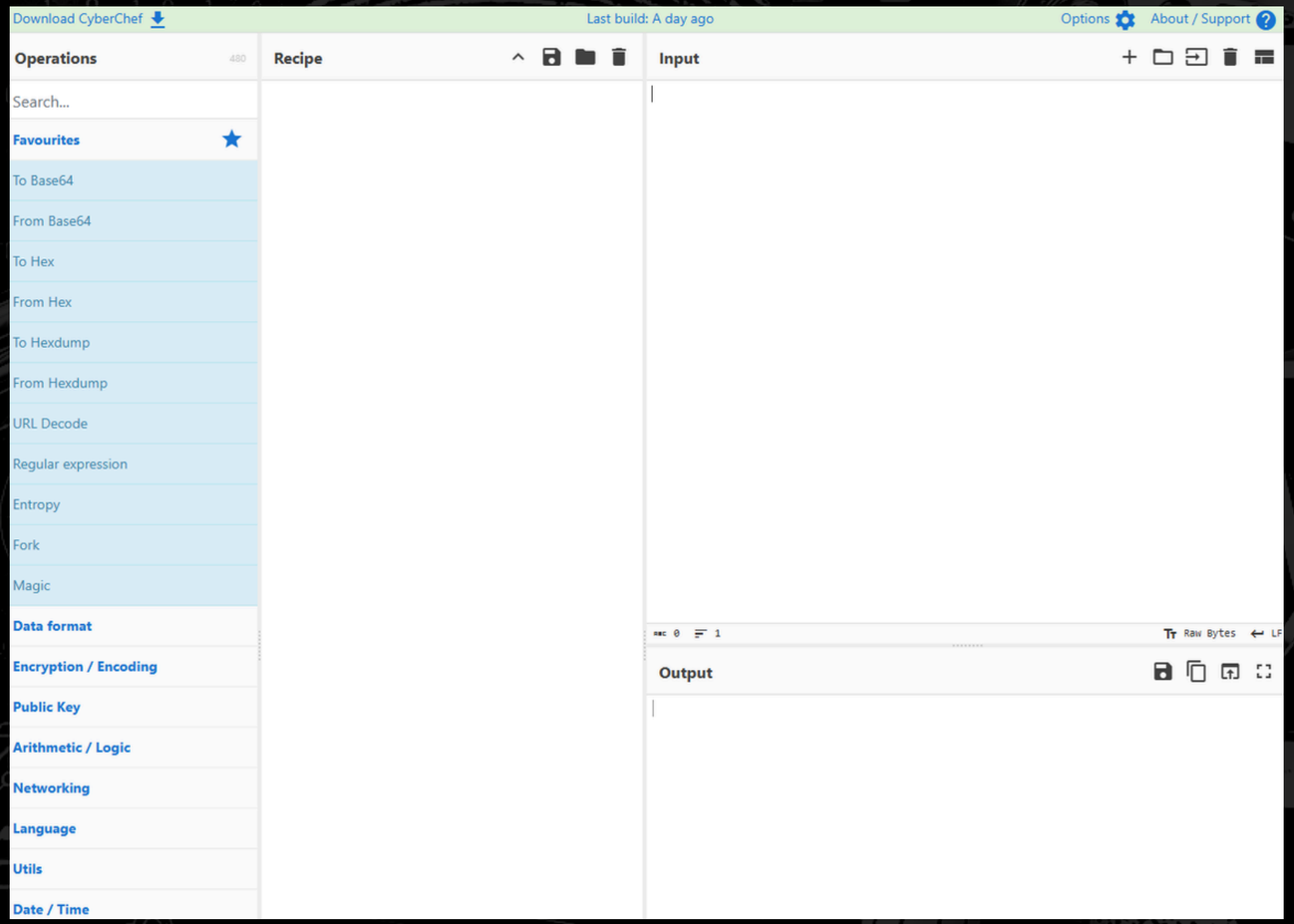
데이터 디코딩, 인코딩, 변환, 압축 해제, 해시 계산, 암호화/복호화 분석 등에 사용할 수 있는 웹 기반 도구

SCA

수사 가방을 열어봅시다

HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography Online
grep
Audacity

디코딩/변환 도구



https://gchq.github.io/CyberChef/

SCA

수사 가방을 열어봅시다

HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography Online
grep
Audacity

디스크 분석 도구



USB, HDD, SSD, 폴더, 파일 등을 원본 그대로 복사한다
→ 복사본을 분석한다
→ 원본 증거가 바뀌지 않았는지 해시값으로 검증한다

SCA

수사 가방을 열어봅시다

디스크 분석 도구

HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography Online
grep
Audacity

저장장치의 포렌식 이미지 생성
원본을 변경하지 않고 파일 미리보기
삭제된 파일 확인
필요한 파일만 추출

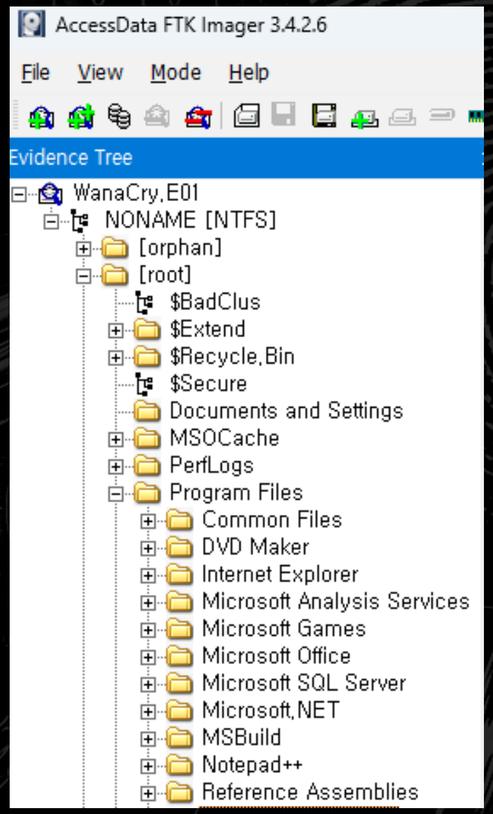
포렌식에서의 이미지: 저장장치를 그대로 복사한 파일
FTK Imager관련 확장자: .E01, .dd, .raw, .img

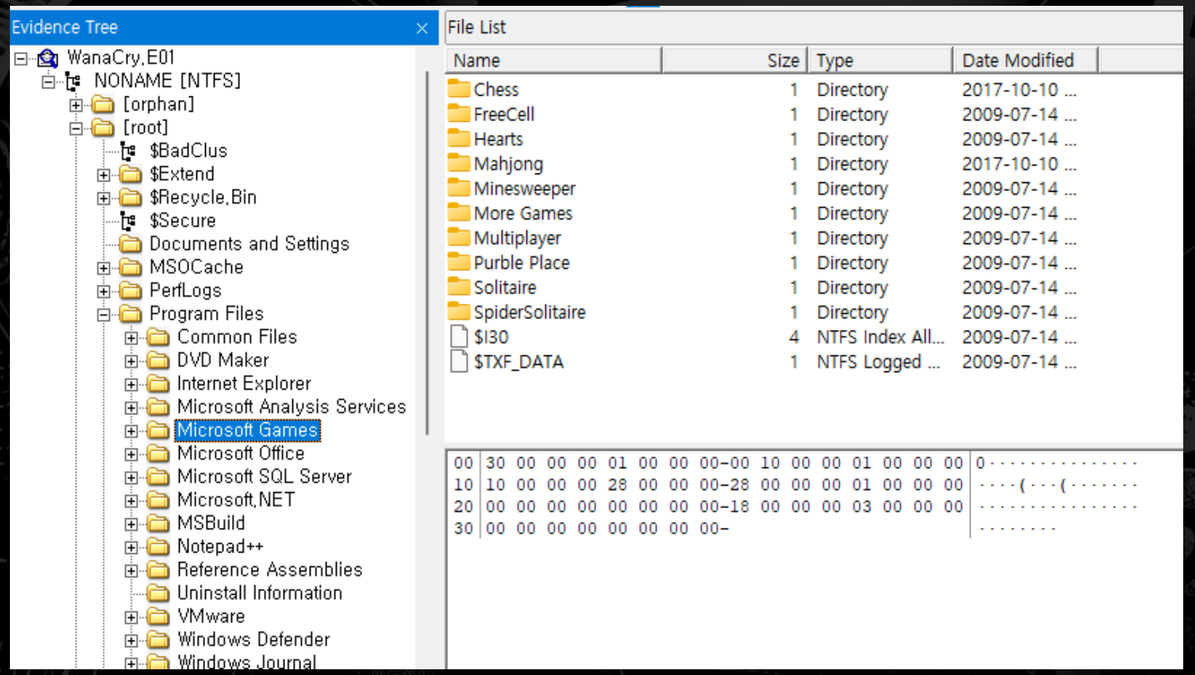
SCA

수사 가방을 열어봅시다

디스크 분석 도구

- HxD
- binwalk
- 파일 속성 창
- CyberChef
- FTK Imager
- WinPrefetchView
- Wireshark
- Steganography Online
- grep
- Audacity



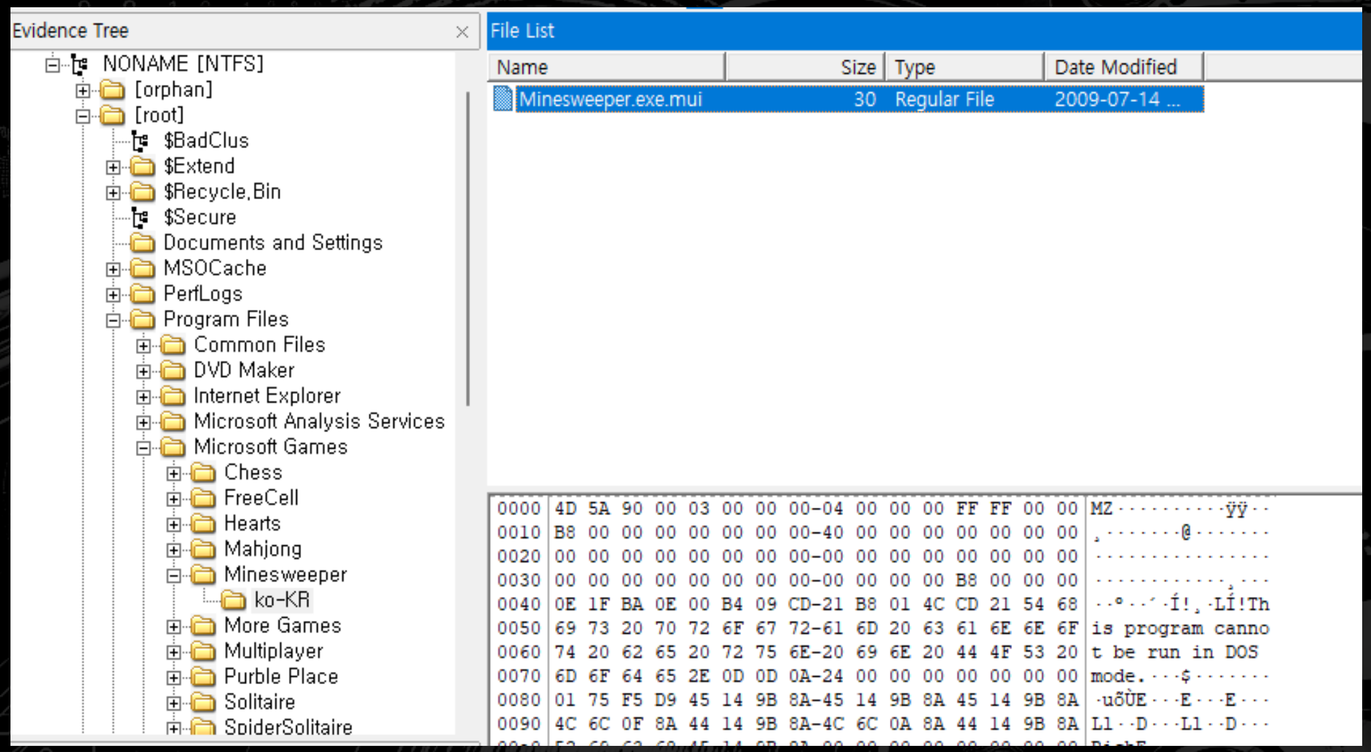


SCA

수사 가방을 열어봅시다

디스크 분석 도구

- HxD
- binwalk
- 파일 속성 창
- CyberChef
- FTK Imager
- WinPrefetchView
- Wireshark
- Steganography Online
- grep
- Audacity

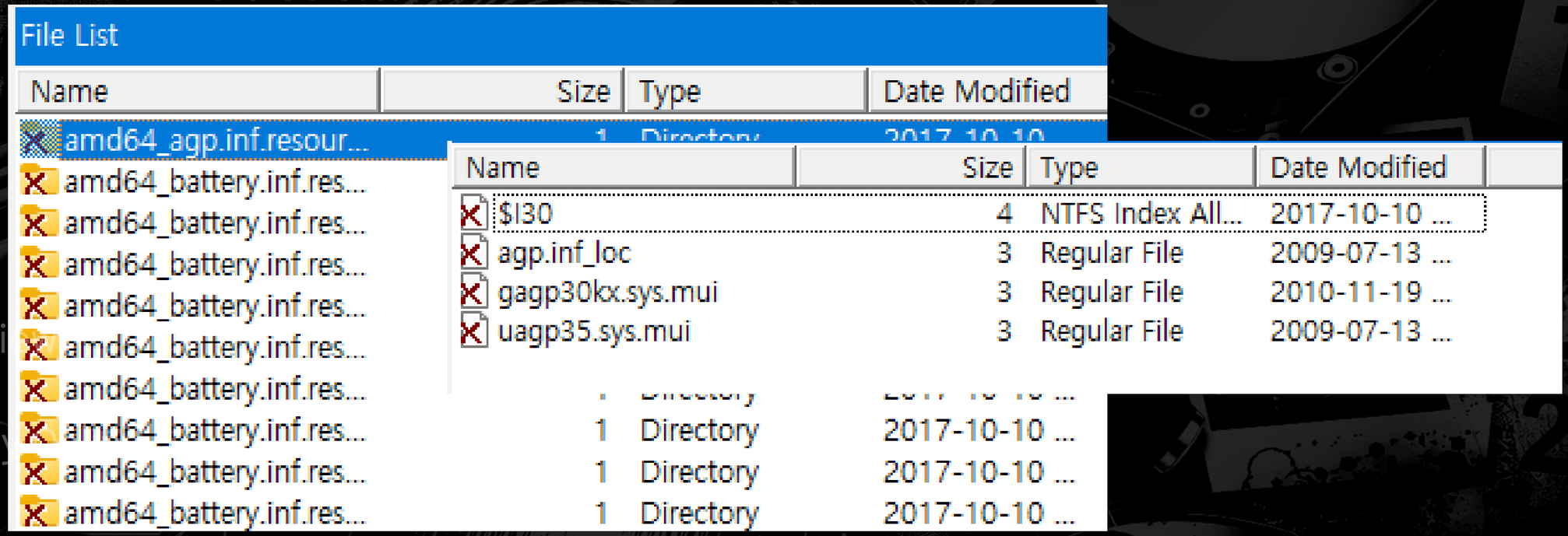


SCA

수사 가방을 열어봅시다

디스크 분석 도구

- HxD
- binwalk
- 파일 속성 창
- CyberChef
- FTK Imager
- WinPrefetchVi
- Wireshark
- Steganography
- grep
- Audacity



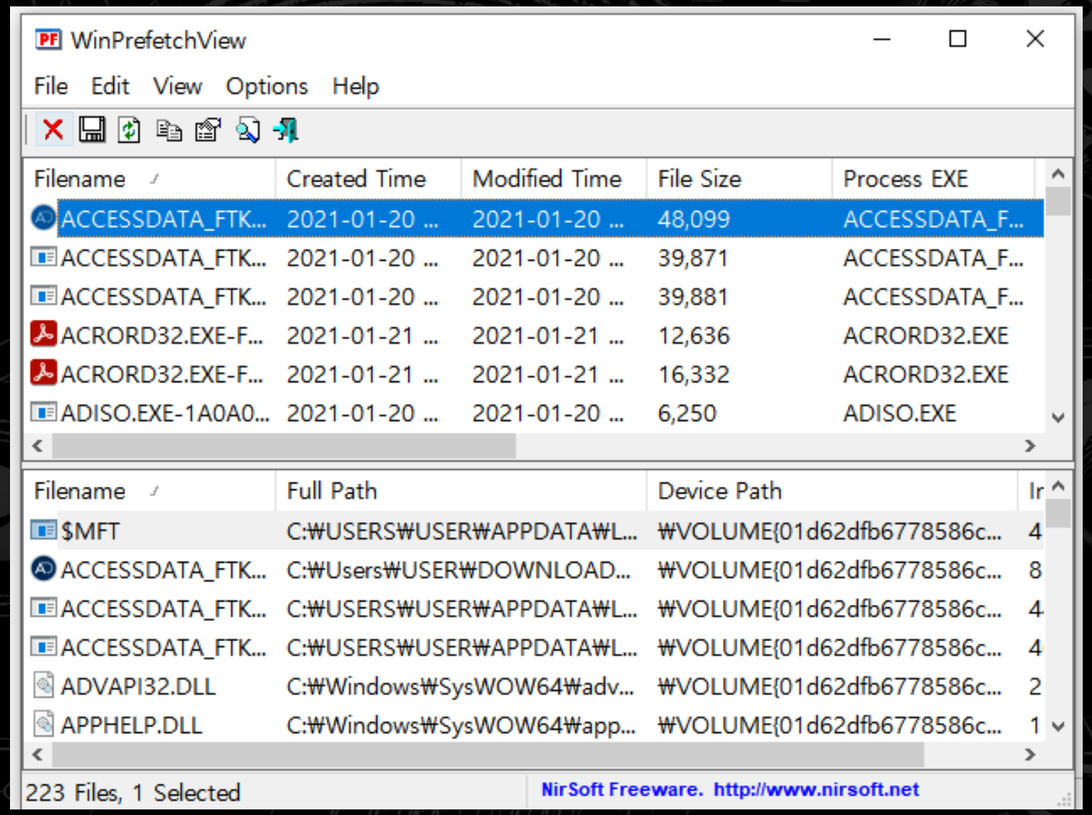
삭제된 파일은 다음과 같이 X표가 쳐져있다.
(우클릭 → Export Files...으로 복구 가능)

SCA

수사 가방을 열어봅시다

디스크 분석 도구

- HxD
- binwalk
- 파일 속성 창
- CyberChef
- FTK Imager
- WinPrefetchView
- Wireshark
- Steganography Online
- grep
- Audacity



https://hey-stranger.tistory.com/62

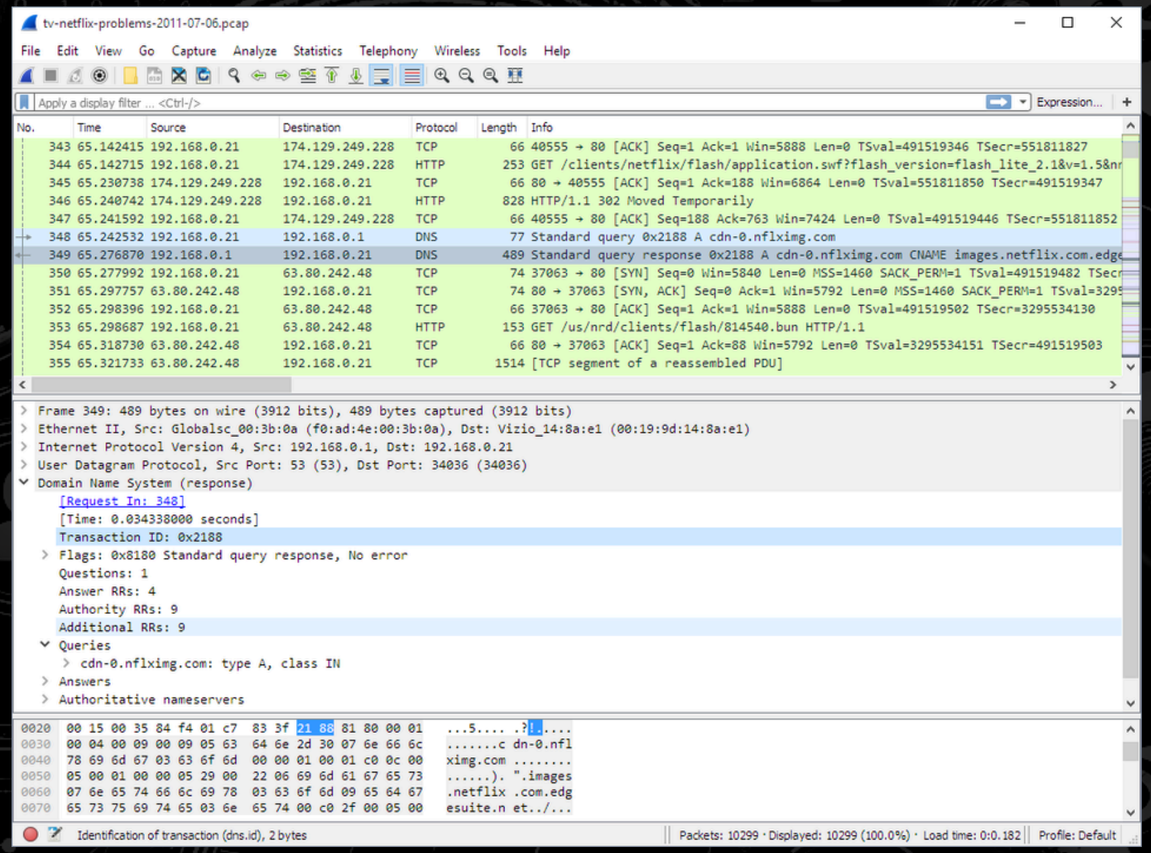
컴퓨터에서의 아이콘, 경로, 실행횟수 등을 알 수 있다.

SCA

수사 가방을 열어봅시다

HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography Online
grep
Audacity

네트워크 분석 도구



네트워크에서 오가는 데이터를 패킷 단위로 캡처하고 분석하는 도구

SCA

수사 가방을 열어봅시다

HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography Online
grep
Audacity

네트워크 분석 도구

어떤 통신이 있었는지 확인
프로토콜 확인
캡처 파일 분석
네트워크 문제 원인 찾기

SCA

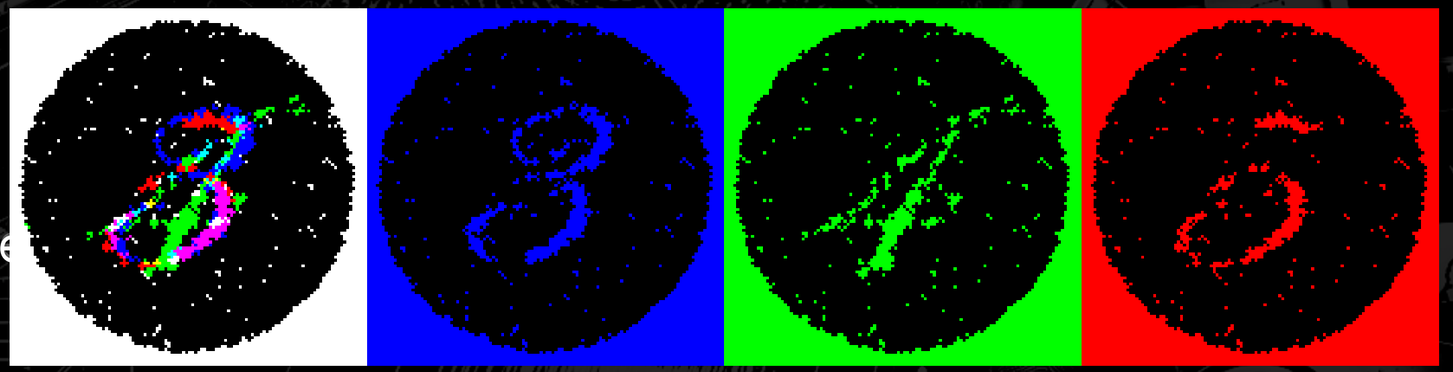
수사 가방을 열어봅시다

이미지/오디오 포렌식 도구

HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography Online
grep
Audacity

스테가노그래피란?

데이터를 다른 파일 안에 숨기는 기술



SCA

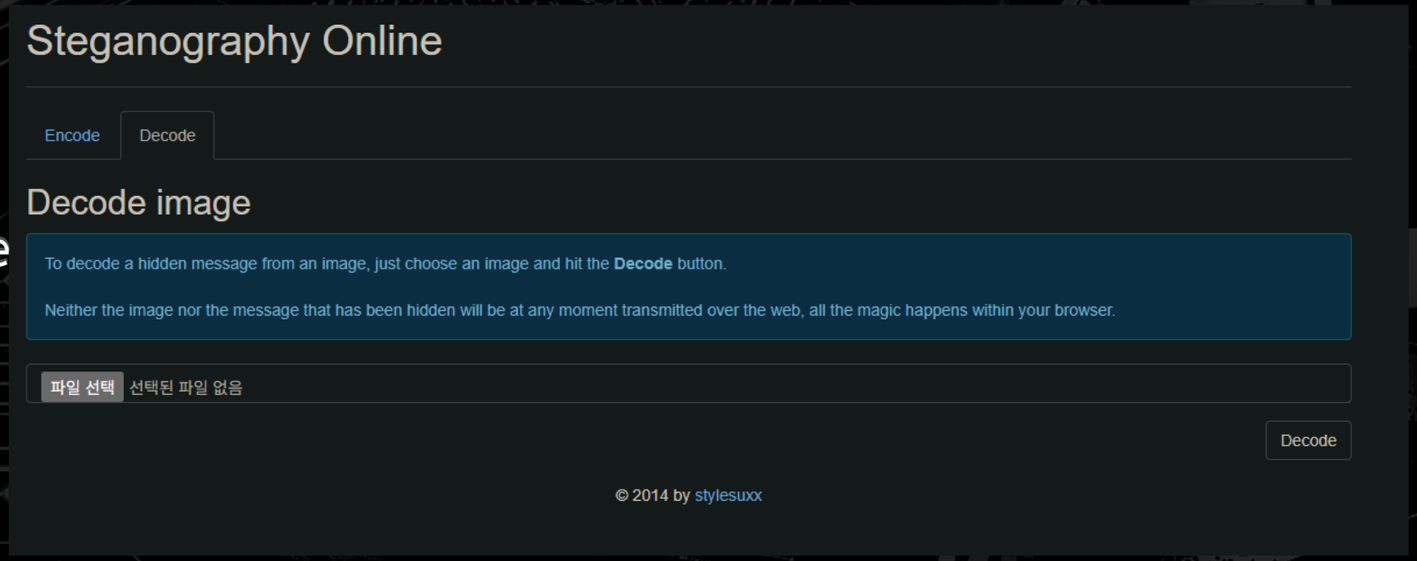
수사 가방을 열어봅시다

이미지/오디오 포렌식 도구

HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography Online
grep
Audacity

Steganography Online

이미지나 오디오 파일 안에 숨겨진 데이터를 확인



https://stylesuxx.github.io/steganography/

SCA

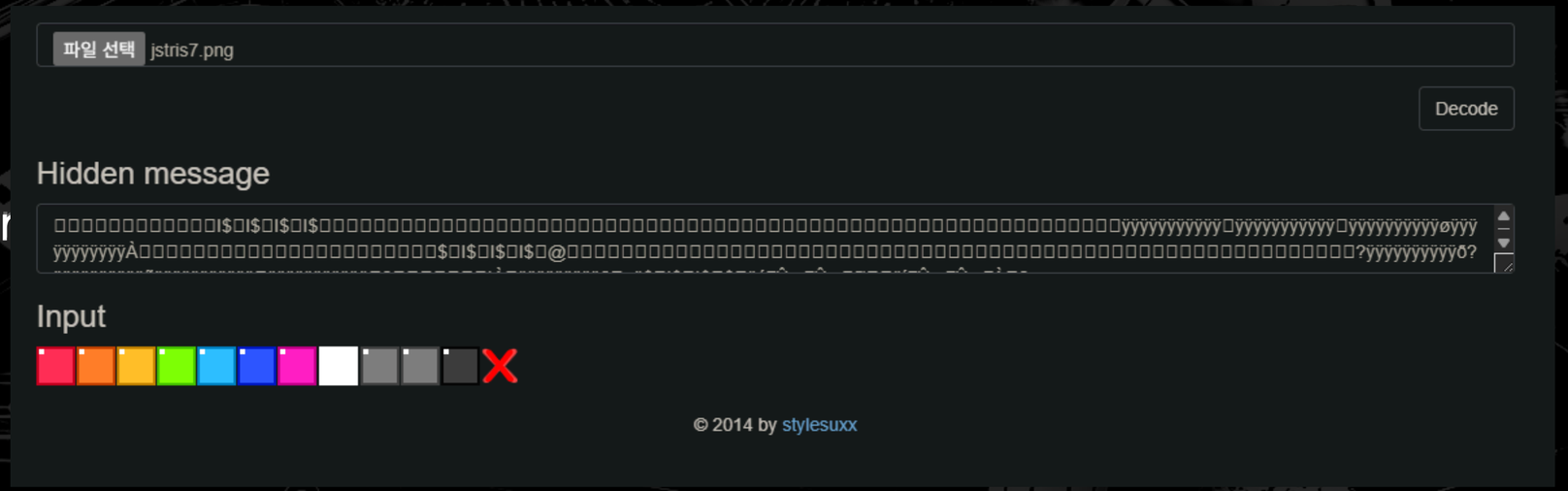
수사 가방을 열어봅시다

이미지/오디오 포렌식 도구

HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography Or
grep
Audacity

Steganography Online

이미지나 오디오 파일 안에 숨겨진 데이터를 확인



https://stylesuxx.github.io/steganography/

SCA

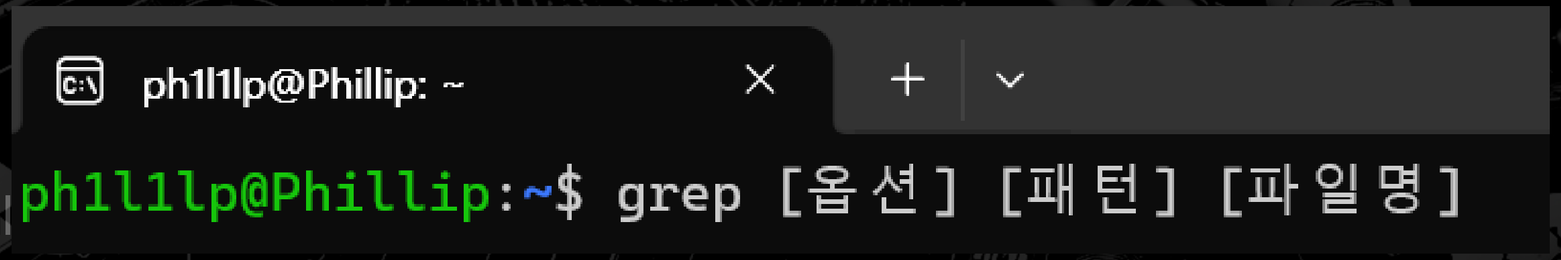
수사 가방을 열어봅시다

로그 분석 도구

HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography Onl
grep
Audacity

grep

파일의 내용에서 특정 문자열을 찾고자할 때 사용하는 명령어



SCA

수사 가방을 열어봅시다

로그 분석 도구

HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography
grep
Audacity

grep

파일의 내용에서 특정 문자열을 찾고자할 때 사용하는 명령어

```
ph1l1p@Phillip:/mnt/c/Users/phill/Downloads/Hefty Image/test$ grep "flag" test.txt
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAflagAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
ph1l1p@Phillip:/mnt/c/Users/phill/Downloads/Hefty Image/test$
```

SCA

수사 가방을 열어봅시다

HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography Online
grep
Audacity

로그 분석 도구

옵션

- **-c :** 일치하는 행의 수를 출력한다.
- **-i :** 대소문자를 구별하지 않는다.
- **-v :** 일치하지 않는 행만 출력한다.
- **-n :** 포함된 행의 번호를 함께 출력한다.
- **-l :** 패턴이 포함된 파일의 이름을 출력한다.
- **-w :** 단어와 일치하는 행만 출력한다.
- **-x :** 라인과 일치하는 행만 출력한다.
- **-r :** 하위 디렉토리를 포함한 모든 파일에서 검색한다.
- **-m 숫자 :** 최대로 표시될 수 있는 결과를 제한한다.
- **-E :** 찾을 패턴을 정규 표현식으로 찾는다.
- **-F :** 찾을 패턴을 문자열로 찾는다.

SCA

수사 가방을 열어봅시다

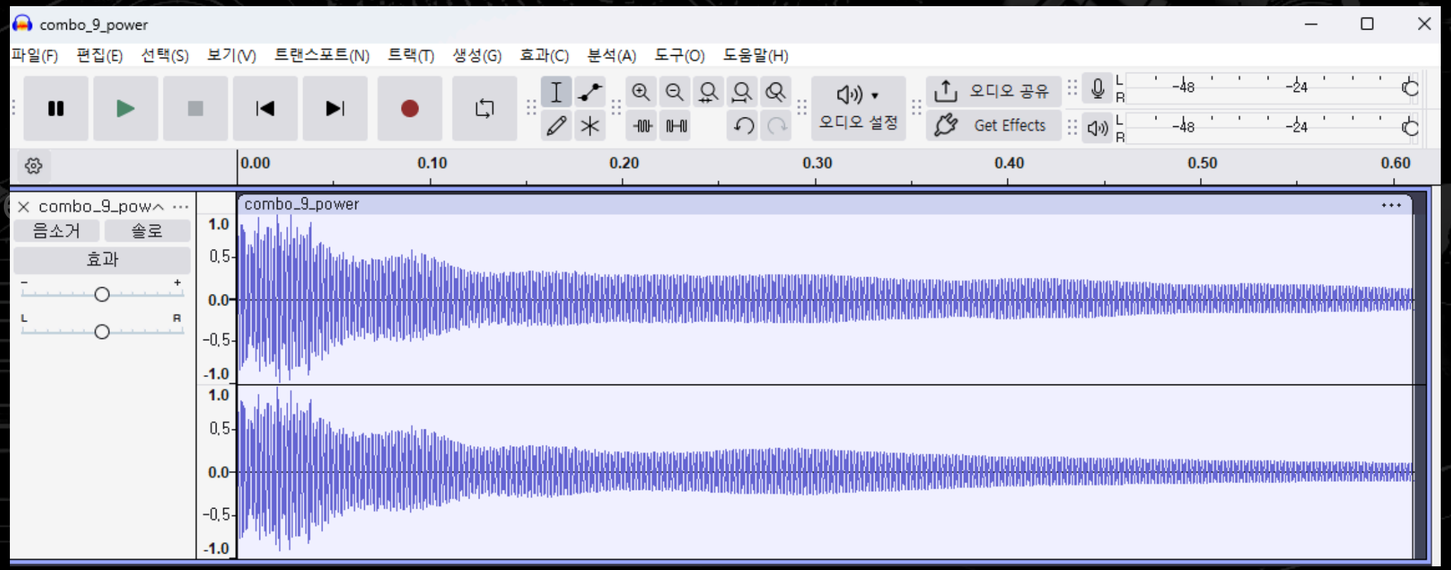
이미지/오디오 포렌식 도구

HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography Online
grep
Audacity

Audacity

무료 오픈소스 오디오 편집·녹음 프로그램

오디오 파일의 파형과 주파수 정보를 시각적으로 분석하는 도구



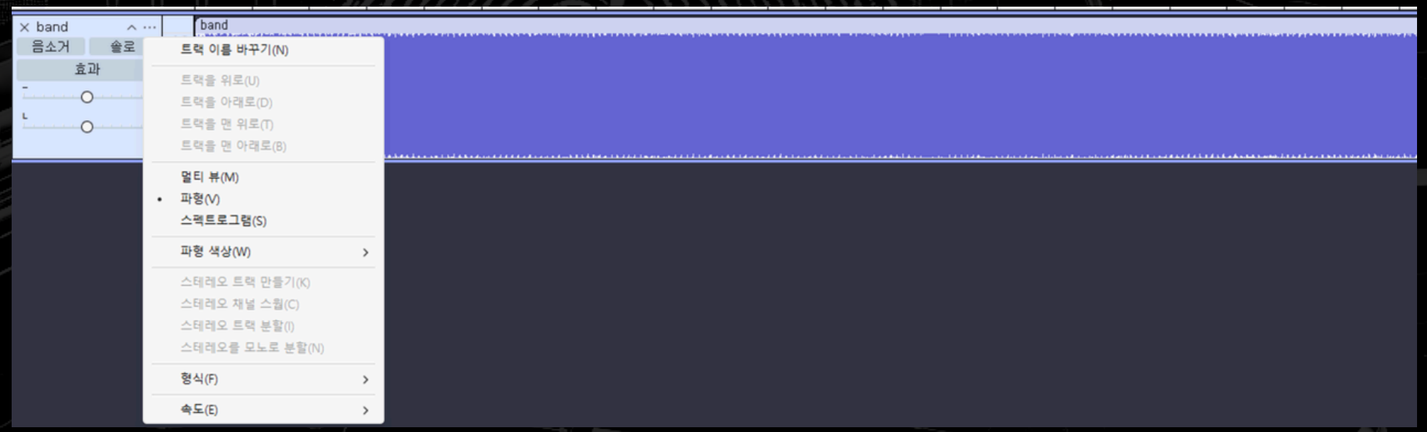
SCA

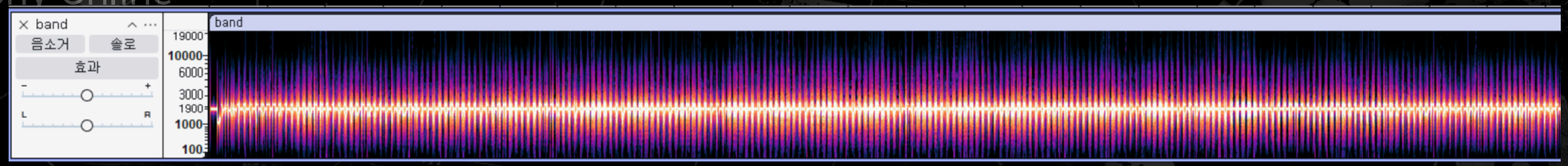
수사 가방을 열어봅시다

이미지/오디오 포렌식 도구

HxD
binwalk
파일 속성 창
CyberChef
FTK Imager
WinPrefetchView
Wireshark
Steganography Online
grep
Audacity

Audacity







SCA

우리도 직접 단서를 찾아봅시다

Basic_Forensics_1

https://dreamhack.io/wargame/challenges/518


SCA
우리도 직접 단서를 찾아봅시다
Steganography Online
Basic_Forensics_1
https://dreamhack.io/wargame/challenges/518



SCA

우리도 직접 단서를 찾아봅시다

Audio Steganography

https://dreamhack.io/wargame/challenges/1660



SCA

우리도 직접 단서를 찾아봅시다

Audacity

Audio Steganography

https://dreamhack.io/wargame/challenges/1660



우리도 직접 단서를 찾아봅시다

Hefty Image

https://dreamhack.io/wargame/challenges/2455



SCA

우리도 직접 단서를 찾아봅시다

binwalk

Hefty Image

https://dreamhack.io/wargame/challenges/2455



SCA

우리도 직접 단서를 찾아봅시다

Steg-Pack

https://dreamhack.io/wargame/challenges/1676



SCA

우리도 직접 단서를 찾아봅시다

binwalk

Steg-Pack

https://dreamhack.io/wargame/challenges/1676



SCA

우리도 직접 단서를 찾아봅시다

Random String

https://dreamhack.io/wargame/challenges/1838



SCA

우리도 직접 단서를 찾아봅시다

grep

Random String

https://dreamhack.io/wargame/challenges/1838



우리도 직접 단서를 찾아봅시다

broken-png

https://dreamhack.io/wargame/challenges/104


SCA
우리도 직접 단서를 찾아봅시다
HxD
broken-png
https://dreamhack.io/wargame/challenges/104


SCA
THE END