



SCA

Created by Unbbal

Digital Forensics

101



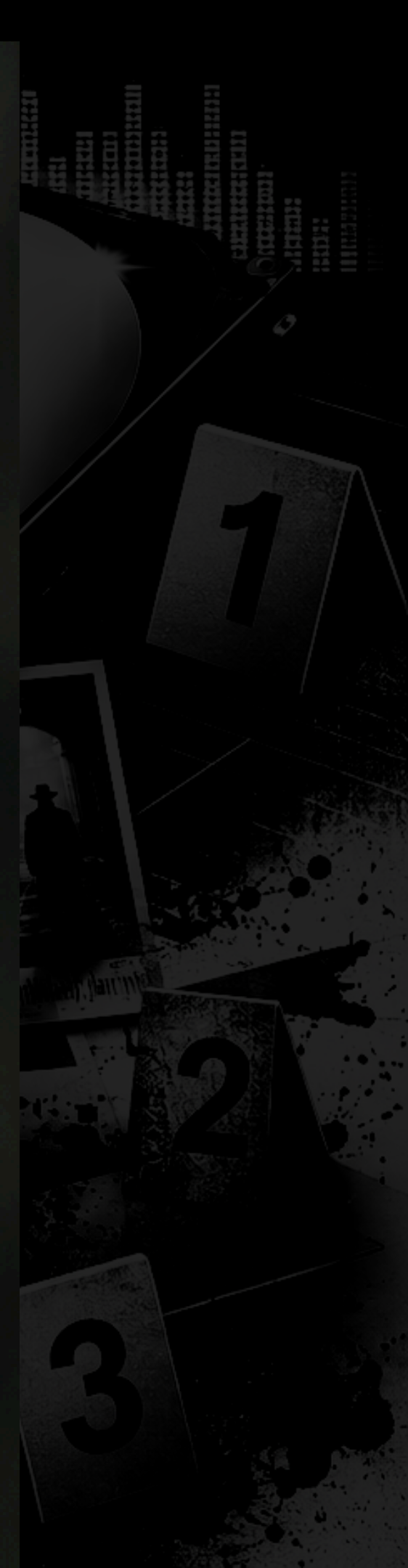
TOC

- 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 파일의 숨겨진 이야기
- 6 수사관의 디지털 탐정
- 7 미션: 디지털 증거 찾기
- 8 모든 것의 시작과 끝

사실은?

것들

- 5 파일의 지문: 해시값
- 6 수사 도구를 열어봅시다
- 7 미션: 숨겨진 단서를 찾아라
- 8 모든 디지털 흔적은 이야기를 남긴다



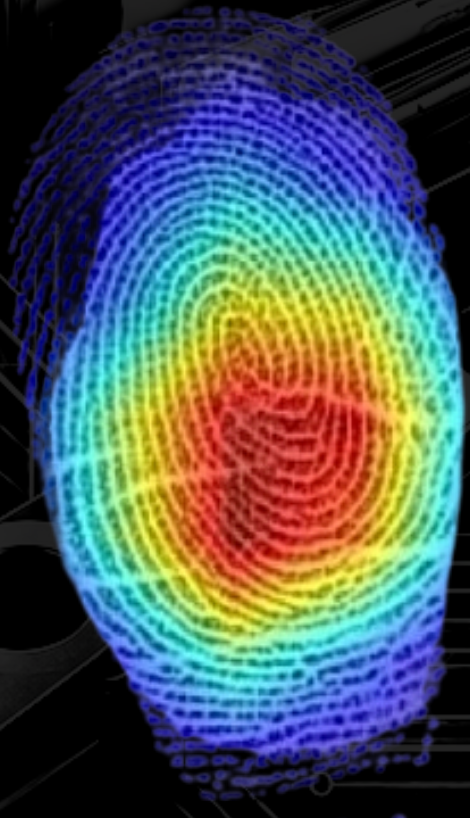


SCA

이름은 어렵운데, 사실은 흔적 찾기입니다

포렌식

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



지문



발자국



CCTV



SCA

이름은 어렵운데, 사실은 흔적 찾기입니다

디지털 포렌식

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

Tue Aug 23 15:54	-	15:54	(00:00)
Tue Aug 23 15:54	-	15:54	(00:00)
Tue Aug 23 15:54	-	15:54	(00:00)
Tue Aug 23 15:54	-	15:54	(00:00)
Tue Aug 23 15:54	-	15:54	(00:00)
Tue Aug 23 15:54	-	15:54	(00:00)
Tue Aug 23 15:54	-	15:54	(00:00)
Tue Aug 23 15:53	-	15:53	(00:00)
Tue Aug 23 15:53	-	15:53	(00:00)
Tue Aug 23 15:53	-	15:53	(00:00)
Tue Aug 23 15:53	-	15:53	(00:00)
Tue Aug 23 15:53	-	15:53	(00:00)
Tue Aug 23 15:53	-	15:53	(00:00)
Tue Aug 23 15:53	-	15:53	(00:00)
Tue Aug 23 15:53	-	15:53	(00:00)
Tue Aug 23 15:52	-	15:52	(00:00)
Tue Aug 23 15:52	-	15:52	(00:00)
Tue Aug 23 15:52	-	15:52	(00:00)
Tue Aug 23 15:51	-	15:51	(00:00)
Tue Aug 23 15:51	-	15:51	(00:00)
Tue Aug 23 15:51	-	15:51	(00:00)
Tue Aug 23 15:51	-	15:51	(00:00)

Log

No.	Time	Source	Destination	Protocol	Info
40	139.931107	wistron_07:07:ee	broadcast	ARP	who has 192.168.1.254? tell 192.168.1.00
47	139.931463	ThomsonT_08:35:4f	Wistron_07:07:ee	ARP	192.168.1.254 is at 00:90:d0:08:35:4f
48	139.931466	192.168.1.68	192.168.1.254	DNS	Standard query A www.google.com
49	139.975406	192.168.1.254	192.168.1.68	DNS	Standard query response CNAME www.l.google.com A 66.102.9.99
50	139.976811	192.168.1.68	66.102.9.99	TCP	62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
51	140.079578	66.102.9.99	192.168.1.68	TCP	http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
52	140.079583	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
53	140.080278	192.168.1.68	66.102.9.99	HTTP	GET /complete/search?hl=en&client=suggest&js=true&q=&cp=1 H
54	140.086765	192.168.1.68	66.102.9.99	TCP	62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
55	140.086921	192.168.1.68	66.102.9.99	TCP	62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
56	140.197484	66.102.9.99	192.168.1.68	TCP	http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
57	140.197777	66.102.9.99	192.168.1.68	TCP	http > 62216 [FIN, ACK] Seq=1 Ack=805 Win=7360 Len=0
58	140.197811	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0

Packet

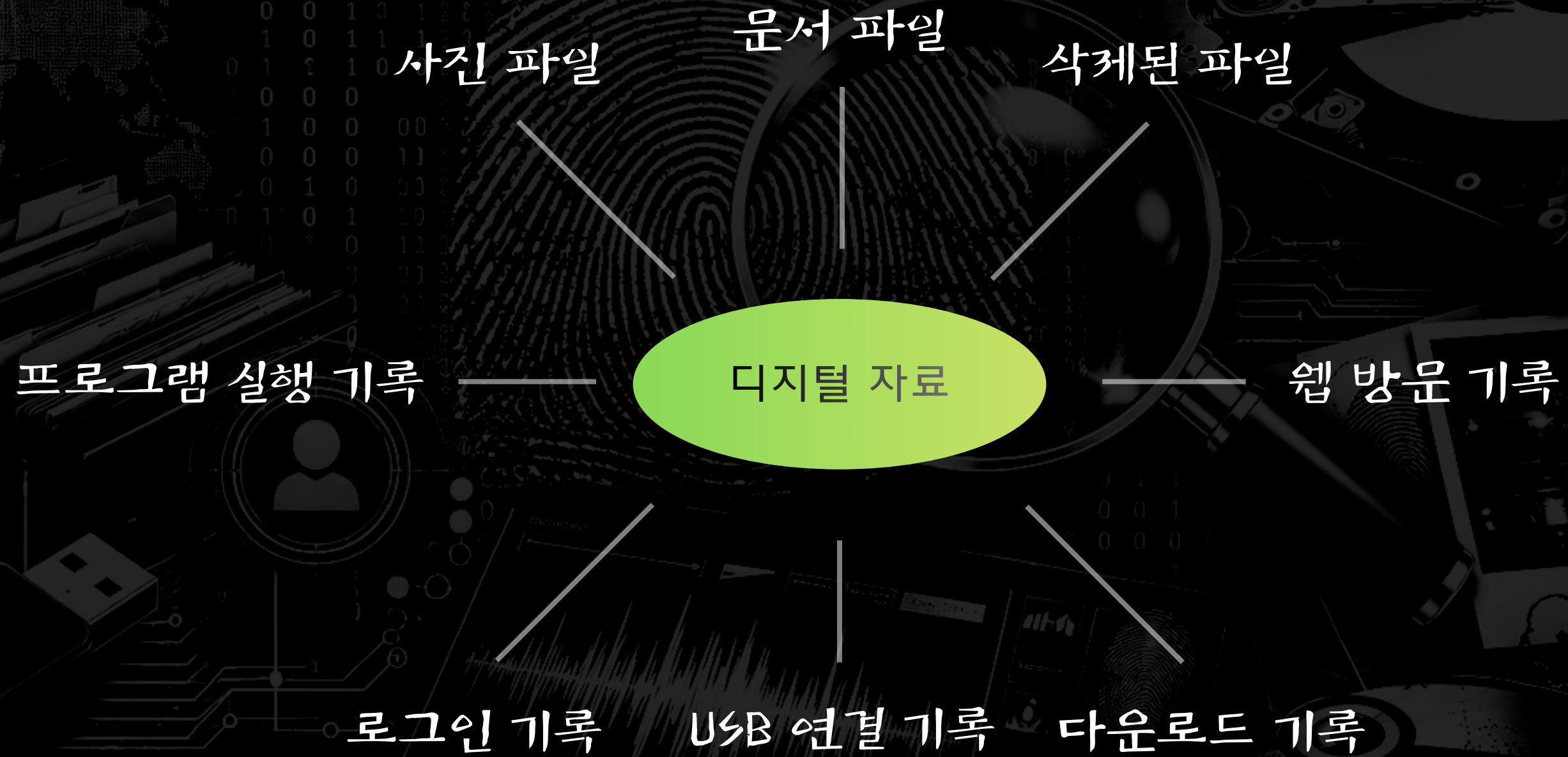
Name	Size	Type	Date Modified
DEFAULT.LOG2	0	Regular File	2009-07-14 오전 2:03:40
SAM	256	Regular File	2020-02-20 오후 2:53:47
SAM.LOG	1	Regular File	2011-04-12 오후 9:08:34
SAM.LOG1	53	Regular File	2020-02-20 오후 2:53:12
SAM.LOG1.FileSla...	3	File Slack	
SAM.LOG2	0	Regular File	2009-07-14 오전 2:03:40
SECURITY	256	Regular File	2020-02-20 오후 2:53:47
SECURITY.LOG	1	Regular File	2011-04-12 오후 9:08:34
SECURITY.LOG1	21	Regular File	2020-02-20 오후 2:53:47
SECURITY.LOG1	\$I30 INDX ...		
SECURITY.LOG2	0	Regular File	2009-07-14 오전 2:03:40
SOFTWARE	24,320	Regular File	2020-02-20 오후 2:53:47
SOFTWARE.LOG	1	Regular File	2011-04-12 오후 9:08:39
SOFTWARE.LOG1	256	Regular File	2020-02-20 오후 2:53:47
SOFTWARE.LOG2	0	Regular File	2009-07-14 오전 2:03:40
SYSTEM	10,240	Regular File	2020-02-20 오후 2:53:47
SYSTEM.LOG	1	Regular File	2011-04-12 오후 9:08:29
SYSTEM.LOG1	256	Regular File	2020-02-20 오후 2:53:47
SYSTEM.LOG2	0	Regular File	2009-07-14 오전 2:03:40

File



SCA

이름은 어렵운데, 사실은 흔적 찾기입니다





SCA

이름은 어렵운데, 사실은 흔적 찾기입니다

디지털 자료가 어떻게 증거가 되나요?

관련성

사건과 관련이 있는가?

무결성

중간에 바뀌지 않았는가?

해석 가능성

어떤 의미를 가지는가?



SCA

이름은 어렵운데, 사실은 흔적 찾기입니다

디지털 자료가 어떻게 증거가 되나요?



사진 파일



분석



증거



SCA

이름은 어렵운데, 사실은 흔적 찾기입니다

잠깐, 이거 아무 데나 써도 되나요?



허가 없는 분석은 수사가 아닙니다



SCA

이름은 어렵운데, 사실은 흔적 찾기입니다

분석해도 되는 것

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

하면 안 되는 것

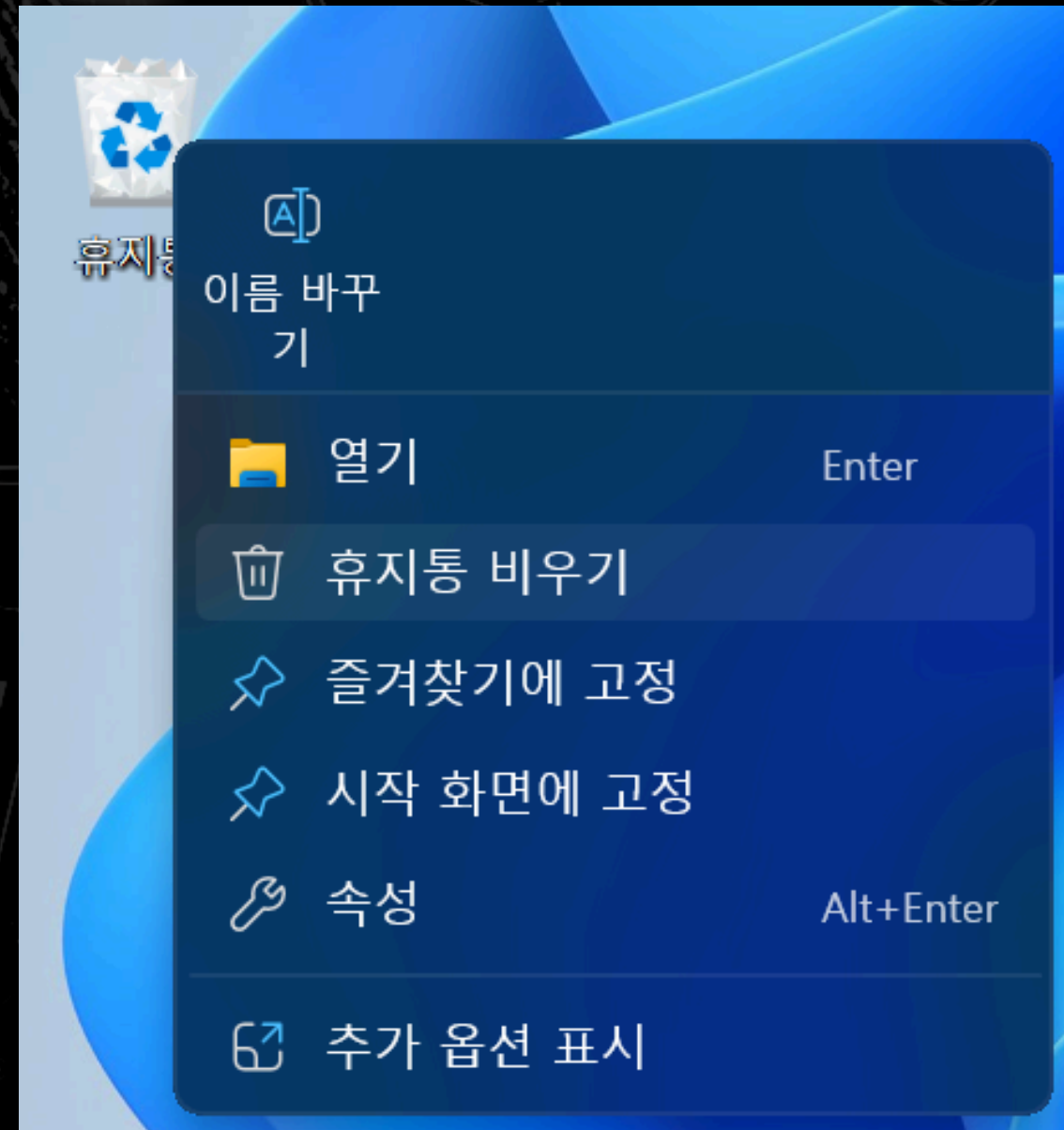
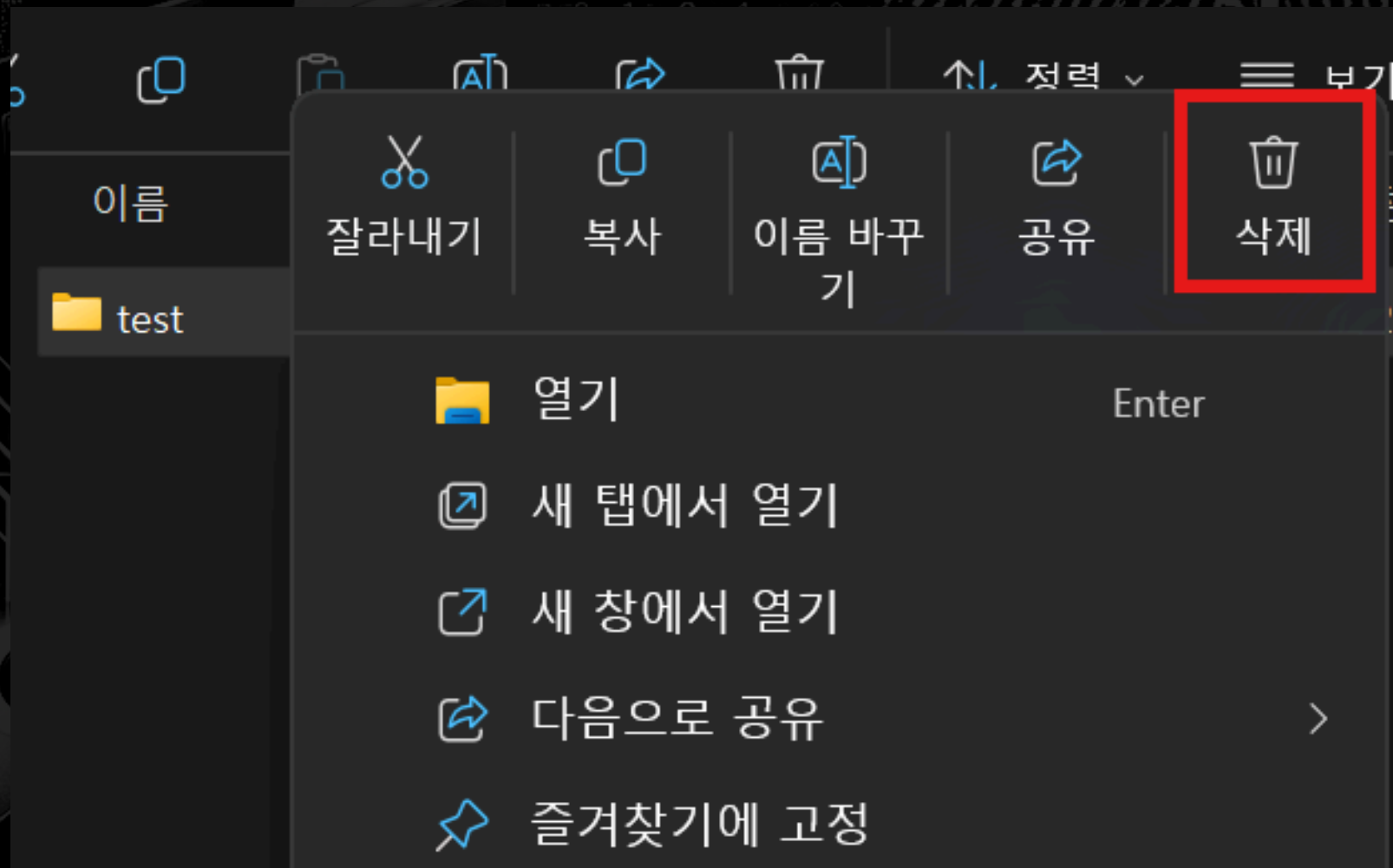
친구 파일 몰래 분석
타인의 스마트폰 확인
허가 없는 계정 접근
개인정보 무단 열람



SCA

삭제 버튼은 만능이 아닙니다

삭제된 파일은 정말 사라졌을까?





SCA

삭제 버튼은 만능이 아닙니다

삭제된 파일은 정말 사라졌을까?



책의 목차에서 제목만 지운 것과 비슷하다.

BOOK

= 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

1m 21s 동안 생각함 >

EXIF만 보면 서울특별시 은평구 쪽, 더 좁히면 연신내역 북쪽 ~ 구파발역 남동쪽 사이, 대략 갈현동/진관동 경계 근처로 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 `GPSPositioningError` 가 **13.4m**라서, 실제 촬영 위치는 이 좌표 주변 반경 **10~20m** 정도로 꽤 정확합니다.

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



SCA

파일에도 지문이 있다고요?



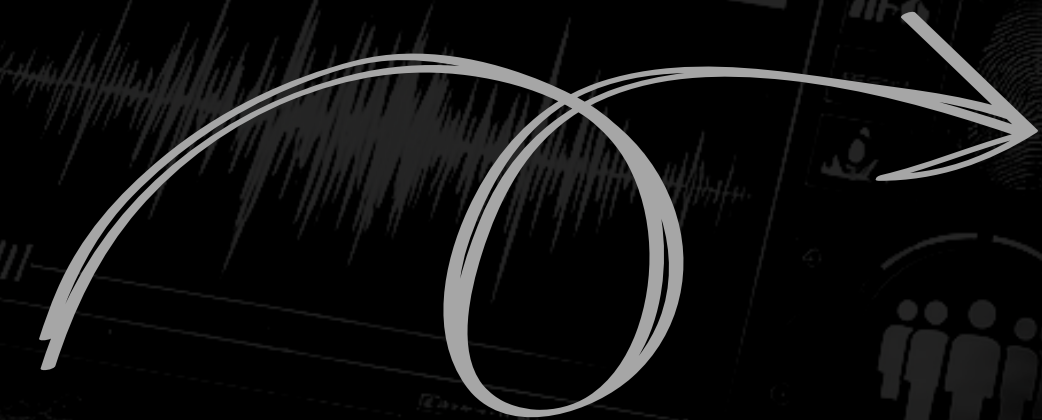
사람



파일



지문



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

Data Format:	Data:
File	phill\OneDrive\Desktop\SCA_CTF\author\test.txt
<input type="checkbox"/> HMAC	Key: Text string
<input checked="" type="checkbox"/> MD5	65a8e27d8879283831b664bd8b7f0ad4
<input type="checkbox"/> MD4	
<input checked="" type="checkbox"/> SHA1	0a0a9f2a6772942557ab5355d76af442f8f65e01
<input checked="" type="checkbox"/> SHA256	dfd6021bb2bd5b0af676290809ec3a53191dd81c7f70a4b2868e
<input type="checkbox"/> SHA384	
<input type="checkbox"/> SHA512	
<input checked="" type="checkbox"/> RIPEMD160	527a6a4b9a6da75607546842e0e00105350b1aaf
<input type="checkbox"/> PANAMA	
<input type="checkbox"/> TIGER	
<input type="checkbox"/> MD2	
<input type="checkbox"/> ADLER32	
<input checked="" type="checkbox"/> CRC32	ec4ac3d0
<input type="checkbox"/> eDonkey/eMule	

SlavaSoft Calculate Close Help



SCA

파일에도 지문이 있다고요?



test.txt

파일 편집 보기

Hello, World!!

한 글자만 바뀌어도
해시값은 바뀐다.

HashCalc

Data Format:	Data:
File	phill\OneDrive\Desktop\SCA_CTF\author\test.txt
<input type="checkbox"/> HMAC	Key: Text string
<input checked="" type="checkbox"/> MD5	d66305ee66a6afc5b7ef7c6810a6f467
<input type="checkbox"/> MD4	
<input checked="" type="checkbox"/> SHA1	5c9c921d4a6ab4603d1640180892a15af46bf873
<input checked="" type="checkbox"/> SHA256	037f927830c3530bf9af08610e4aece368c76f9be724709972c4
<input type="checkbox"/> SHA384	
<input type="checkbox"/> SHA512	
<input checked="" type="checkbox"/> RIPEMD160	f6328ac33a20c25c85363d7cacfa0b1519a4418c
<input type="checkbox"/> PANAMA	
<input type="checkbox"/> TIGER	
<input type="checkbox"/> MD2	
<input type="checkbox"/> ADLER32	
<input checked="" type="checkbox"/> CRC32	185467c4
<input type="checkbox"/> eDonkey/ eMule	

SlavaSoft

Calculate Close Help



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

...



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



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



SCA

수사 가방을 열어봅시다

파일 분석 도구

HxD

binwalk

파일 속성 창

CyberChef

FTK Imager

WinPrefetchView

Wireshark

Steganography Online

grep

Audacity



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



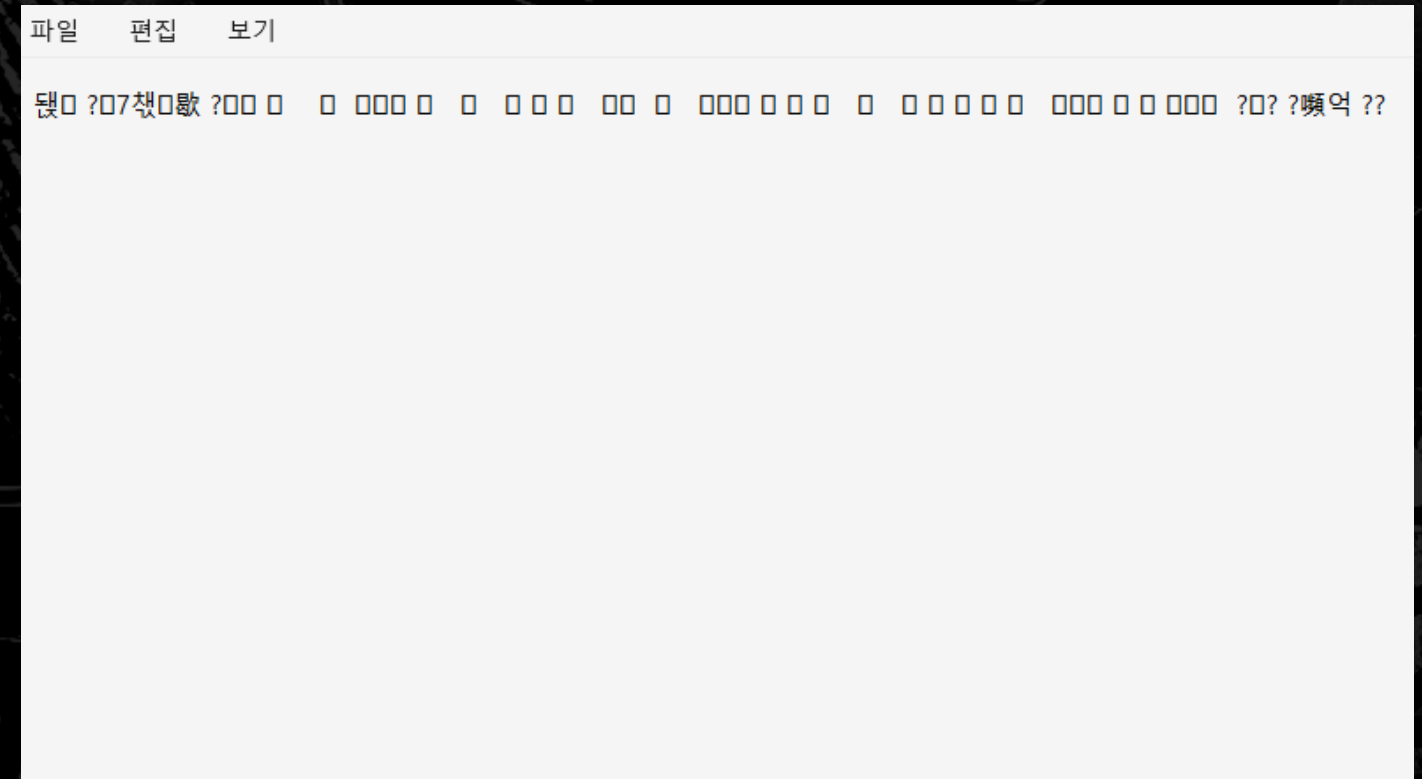
SCA

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	À..â~.7*Upíúí.™
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.€...i.Ð.*i.Àÿi

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?



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	À..â~.7*Upíúí.™
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.Ð.*i.Àÿi

메모장으로 보지 못했던 내용들을 확인할 수 있다.



SCA

수사 가방을 열어봅시다

파일 분석 도구

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)

HxD

binwalk

파일 속성 창

CyberChef

FTK Imager

WinPrefetchView

Wireshark

Steganography Online

grep

Audacity



SCA

수사 가방을 열어봅시다

파일 분석 도구

HxD

binwalk

파일 속성 창

CyberChef

FTK Imager

WinPrefetchView

Wireshark

Steganography Online

grep

Audacity

```
ph111p@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

```
ph111p@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

binwalk 사용

```
ph111p@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.

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



SCA

수사 가방을 열어봅시다

파일 분석 도구

binwalk 사용
추출하고 싶다면 -e 사용

```
ph11lp@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

_binwalk_practice_firmware.bin.extracted

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



SCA

수사 가방을 열어봅시다

파일 분석 도구

_binwalk_practice_firmware.bin.extracted

오늘				
129	2026-06-07 오전 2:24	파일		1KB
129.zlib	2026-06-07 오전 2:24	ZLIB 파일		2KB
300	2026-06-07 오전 2:24	파일		1KB
600.zip	2026-06-07 오전 2:24	압축(ZIP) 파일		1KB
어제				
readme.txt	2026-06-06 오후 2:41	텍스트 문서		1KB
secret.txt	2026-06-06 오후 2:41	텍스트 문서		1KB

flag{BINWALK_FINDS_EMBEDDED_FILES}

This ZIP was embedded inside a fake firmware image.

HxD

binwalk

파일 속성 창

CyberChef

FTK Imager

WinPrefetchView

Wireshark

Steganography Online

grep

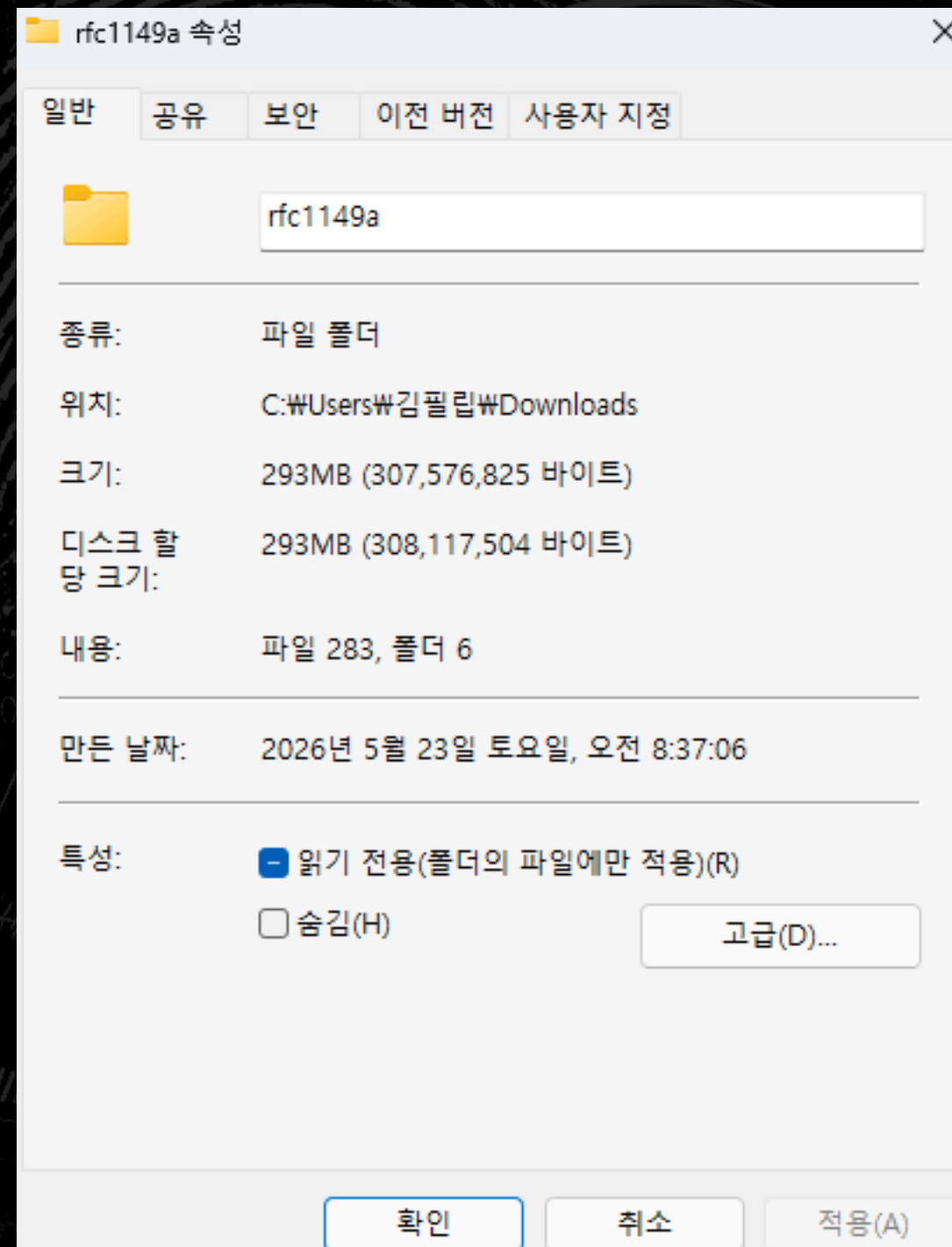
Audacity



SCA

수사 가방을 열어봅시다

메타데이터 도구



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

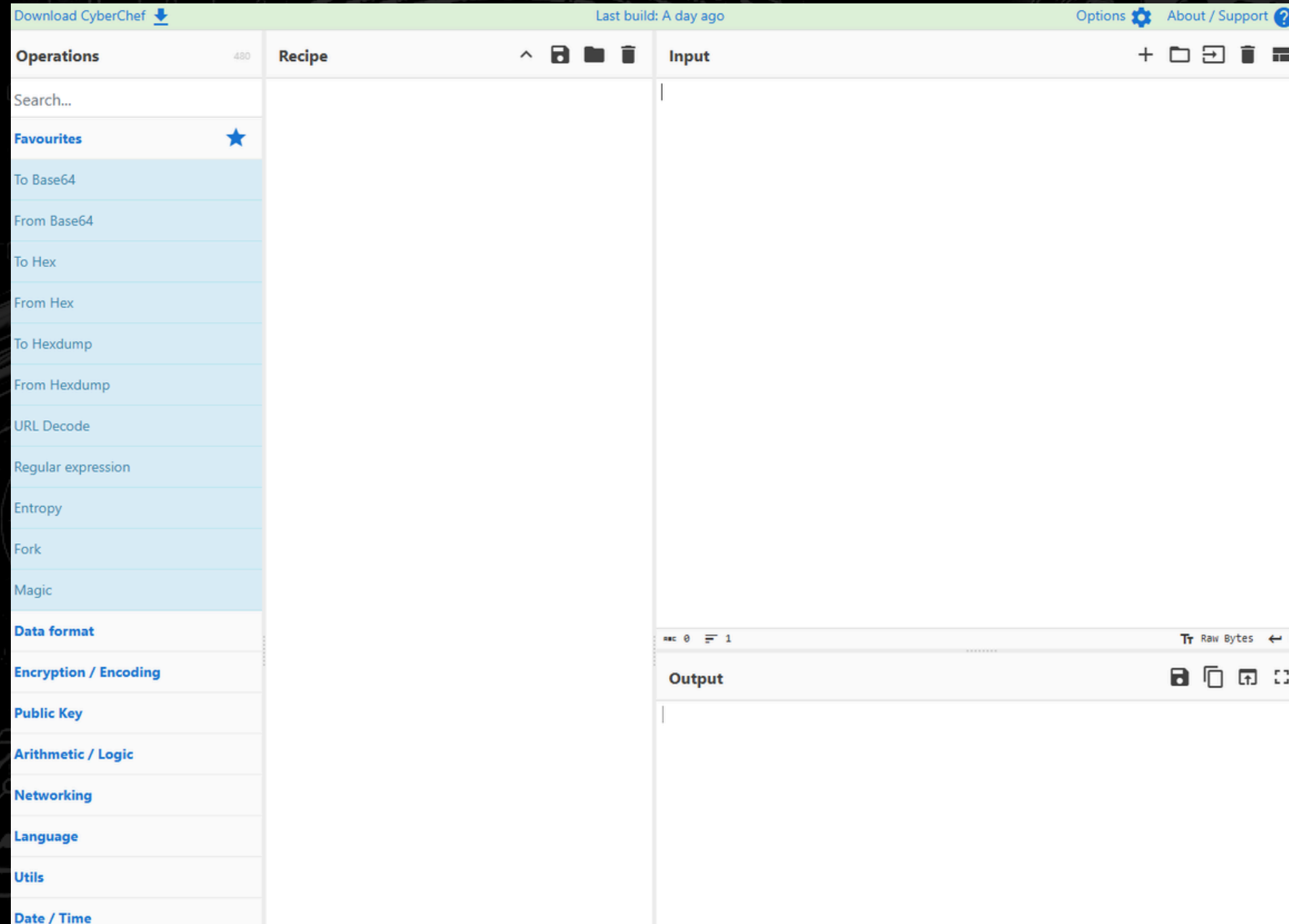
- HxD
- binwalk
- 파일 속성 창
- CyberChef
- FTK Imager
- WinPrefetchView
- Wireshark
- Steganography Online
- grep
- Audacity



SCA

수사 가방을 열어봅시다

디코딩/변환 도구



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

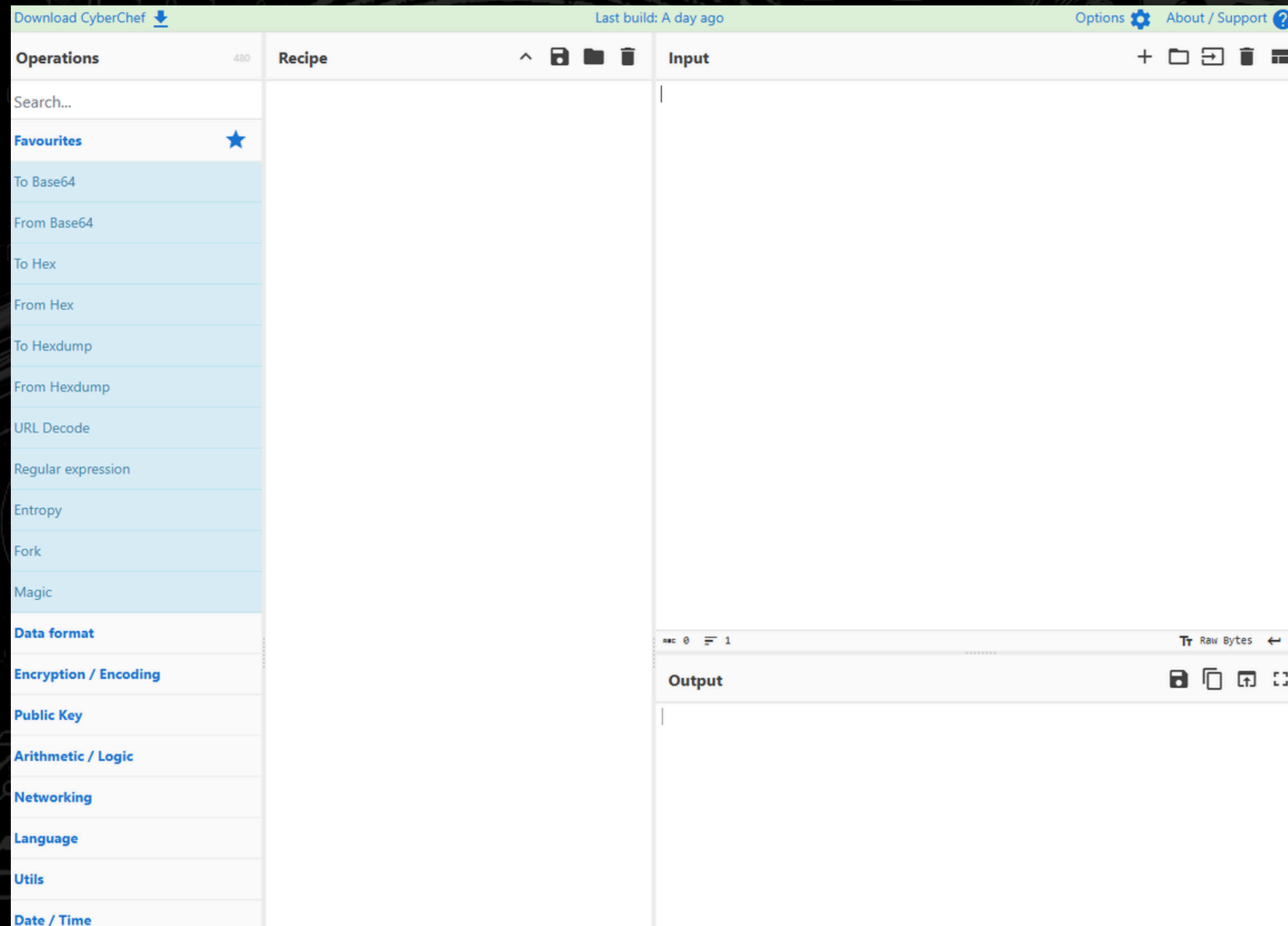
데이터 디코딩, 인코딩, 변환, 압축 해제, 해시 계산, 암호화/복호화 분석 등에 사용할 수 있는 웹 기반 도구



SCA

수사 가방을 열어봅시다

디코딩/변환 도구



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

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



SCA

수사 가방을 열어봅시다

디스크 분석 도구



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

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



SCA

수사 가방을 열어봅시다

디스크 분석 도구

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

HxD

binwalk

파일 속성 창

CyberChef

FTK Imager

WinPrefetchView

Wireshark

Steganography Online

grep

Audacity

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



SCA

수사 가방을 열어봅시다

디스크 분석 도구

AccessData FTK Imager 3.4.2.6

File View Mode Help

Evidence Tree

- WanaCry.E01
 - NONAME [NTFS]
 - [orphan]
 - [root]
 - \$BadClus
 - \$Extend
 - \$Recycle.Bin
 - \$Secure
 - Documents and Settings
 - MSOCache
 - PerfLogs
 - Program Files
 - Common Files
 - DVD Maker
 - Internet Explorer
 - Microsoft Analysis Services
 - Microsoft Games
 - Microsoft Office
 - Microsoft SQL Server
 - Microsoft.NET
 - MSBuild
 - Notepad++
 - Reference Assemblies

Evidence Tree

- WanaCry.E01
 - NONAME [NTFS]
 - [orphan]
 - [root]
 - \$BadClus
 - \$Extend
 - \$Recycle.Bin
 - \$Secure
 - Documents and Settings
 - MSOCache
 - PerfLogs
 - Program Files
 - Common Files
 - DVD Maker
 - Internet Explorer
 - Microsoft Analysis Services
 - Microsoft Games
 - Microsoft Office
 - Microsoft SQL Server
 - Microsoft.NET
 - MSBuild
 - Notepad++
 - Reference Assemblies
 - Uninstall Information
 - VMware
 - Windows Defender
 - Windows Journal

File List

Name	Size	Type	Date Modified
Chess	1	Directory	2017-10-10 ...
FreeCell	1	Directory	2009-07-14 ...
Hearts	1	Directory	2009-07-14 ...
Mahjong	1	Directory	2017-10-10 ...
Minesweeper	1	Directory	2009-07-14 ...
More Games	1	Directory	2009-07-14 ...
Multiplayer	1	Directory	2009-07-14 ...
Purple Place	1	Directory	2009-07-14 ...
Solitaire	1	Directory	2009-07-14 ...
SpiderSolitaire	1	Directory	2009-07-14 ...
\$I30	4	NTFS Index All...	2009-07-14 ...
\$TXF_DATA	1	NTFS Logged ...	2009-07-14 ...

```

00 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00 0
10 10 00 00 00 28 00 00 00-28 00 00 00 01 00 00 00
20 00 00 00 00 00 00 00 00-18 00 00 00 03 00 00 00
30 00 00 00 00 00 00 00 00-
  
```

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



SCA

수사 가방을 열어봅시다

디스크 분석 도구

Evidence Tree

- NONAME [NTFS]
 - [orphan]
 - [root]
 - \$BadClus
 - \$Extend
 - \$Recycle.Bin
 - \$Secure
 - Documents and Settings
 - MSOCache
 - PerfLogs
 - Program Files
 - Common Files
 - DVD Maker
 - Internet Explorer
 - Microsoft Analysis Services
 - Microsoft Games
 - Chess
 - FreeCell
 - Hearts
 - Mahjong
 - Minesweeper
 - ko-KR
 - More Games
 - Multiplayer
 - Purple Place
 - Solitaire
 - SpiderSolitaire

File List

Name	Size	Type	Date Modified
Minesweeper.exe.mui	30	Regular File	2009-07-14 ...

Hex Dump:

```

0000 4D 5A 90 00 03 00 00 00-04 00 00 00 FF FF 00 00 MZ .....ÿÿ..
0010 B8 00 00 00 00 00 00 00-40 00 00 00 00 00 00 00 , .....@.....
0020 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
0030 00 00 00 00 00 00 00 00-00 00 00 00 B8 00 00 00 .....
0040 0E 1F BA 0E 00 B4 09 CD-21 B8 01 4C CD 21 54 68 ..°...í!,-Lí!Th
0050 69 73 20 70 72 6F 67 72-61 6D 20 63 61 6E 6E 6F is program canno
0060 74 20 62 65 20 72 75 6E-20 69 6E 20 44 4F 53 20 t be run in DOS
0070 6D 6F 64 65 2E 0D 0D 0A-24 00 00 00 00 00 00 00 mode...$.....
0080 01 75 F5 D9 45 14 9B 8A-45 14 9B 8A 45 14 9B 8A -uöÜE...E...E...
0090 4C 6C 0F 8A 44 14 9B 8A-4C 6C 0A 8A 44 14 9B 8A L1..D...L1..D...
  
```

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





SCA

수사 가방을 열어봅시다

디스크 분석 도구

File List

Name	Size	Type	Date Modified
amd64_agp.inf.resour...	1	Directory	2017-10-10
amd64_battery.inf.res...			
amd64_battery.inf.res...			
amd64_battery.inf.res...			
amd64_battery.inf.res...			
amd64_battery.inf.res...			
amd64_battery.inf.res...			
amd64_battery.inf.res...			
amd64_battery.inf.res...			
amd64_battery.inf.res...			
amd64_battery.inf.res...			
amd64_battery.inf.res...			
amd64_battery.inf.res...			
amd64_battery.inf.res...			

Name	Size	Type	Date Modified
\$I30	4	NTFS Index All...	2017-10-10 ...
agp.inf_loc	3	Regular File	2009-07-13 ...
gagp30kx.sys.mui	3	Regular File	2010-11-19 ...
uagp35.sys.mui	3	Regular File	2009-07-13 ...

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

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



SCA

수사 가방을 열어봅시다

디스크 분석 도구

WinPrefetchView

File Edit View Options Help

Filename	Created Time	Modified Time	File Size	Process EXE
ACCESSDATA_FTK...	2021-01-20 ...	2021-01-20 ...	48,099	ACCESSDATA_F...
ACCESSDATA_FTK...	2021-01-20 ...	2021-01-20 ...	39,871	ACCESSDATA_F...
ACCESSDATA_FTK...	2021-01-20 ...	2021-01-20 ...	39,881	ACCESSDATA_F...
ACRORD32.EXE-F...	2021-01-21 ...	2021-01-21 ...	12,636	ACRORD32.EXE
ACRORD32.EXE-F...	2021-01-21 ...	2021-01-21 ...	16,332	ACRORD32.EXE
ADISO.EXE-1A0A0...	2021-01-20 ...	2021-01-20 ...	6,250	ADISO.EXE

Filename	Full Path	Device Path	Ir
\$MFT	C:\USERS\USER\APPDATA\WL...	\\VOLUME{01d62dfb6778586c...	4
ACCESSDATA_FTK...	C:\Users\USER\DOWNLOAD...	\\VOLUME{01d62dfb6778586c...	8
ACCESSDATA_FTK...	C:\USERS\USER\APPDATA\WL...	\\VOLUME{01d62dfb6778586c...	4
ACCESSDATA_FTK...	C:\USERS\USER\APPDATA\WL...	\\VOLUME{01d62dfb6778586c...	4
ADVAPI32.DLL	C:\Windows\SysWOW64\adv...	\\VOLUME{01d62dfb6778586c...	2
APPHELP.DLL	C:\Windows\SysWOW64\app...	\\VOLUME{01d62dfb6778586c...	1

223 Files, 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>

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

컴퓨터에서의 아이콘, 경로, 실행횟수 등을 알 수 있다.

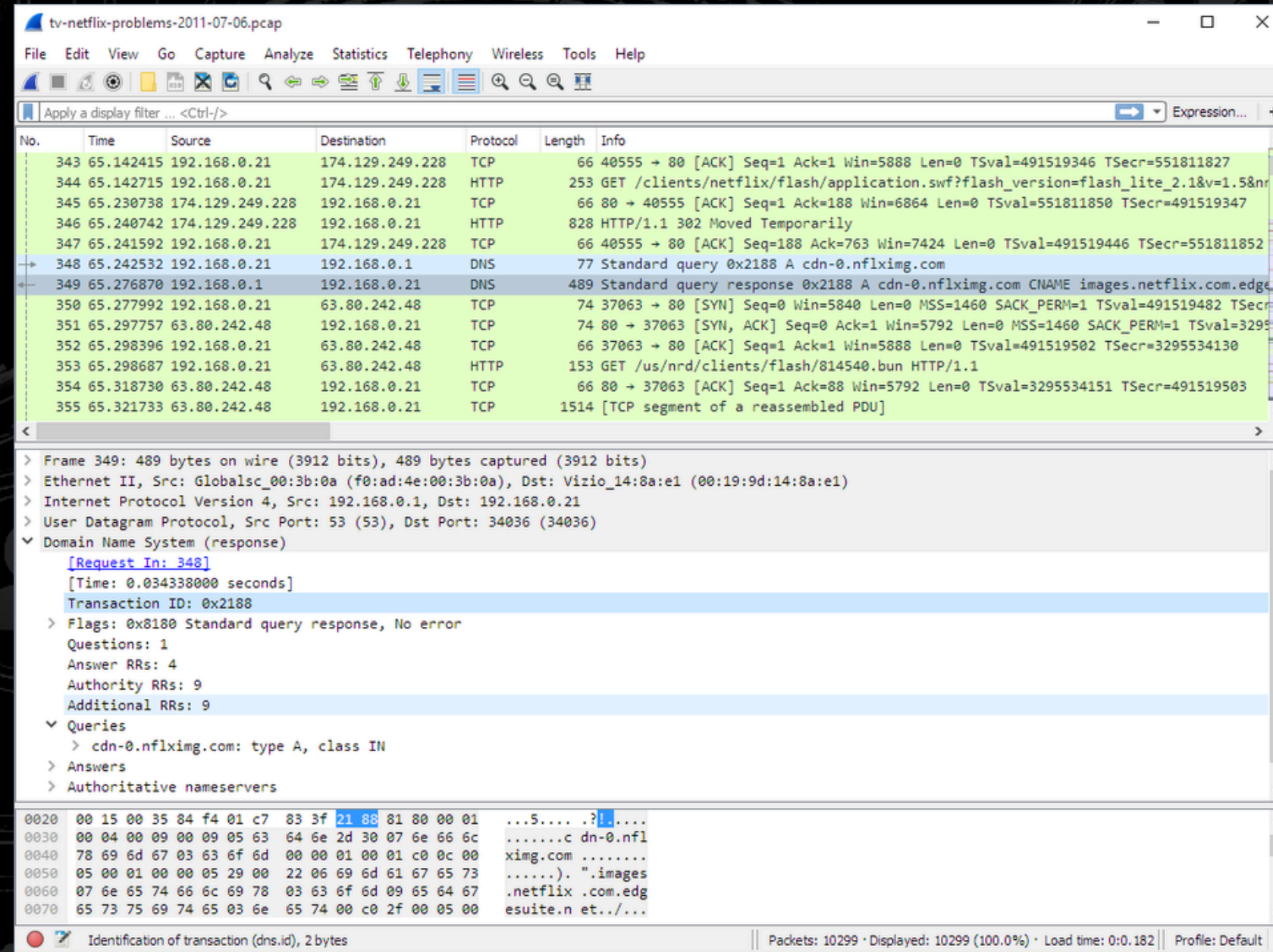
- HxD
- binwalk
- 파일 속성 창
- CyberChef
- FTK Imager
- WinPrefetchView
- Wireshark
- Steganography Online
- grep
- Audacity



SCA

수사 가방을 열어봅시다

네트워크 분석 도구



HxD

binwalk

파일 속성 창

CyberChef

FTK Imager

WinPrefetchView

Wireshark

Steganography Online

grep

Audacity

네트워크에서 오가는 데이터를 패킷 단위로 캡처하고 분석하는 도구



SCA

수사 가방을 열어봅시다

네트워크 분석 도구

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

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

1

2

3



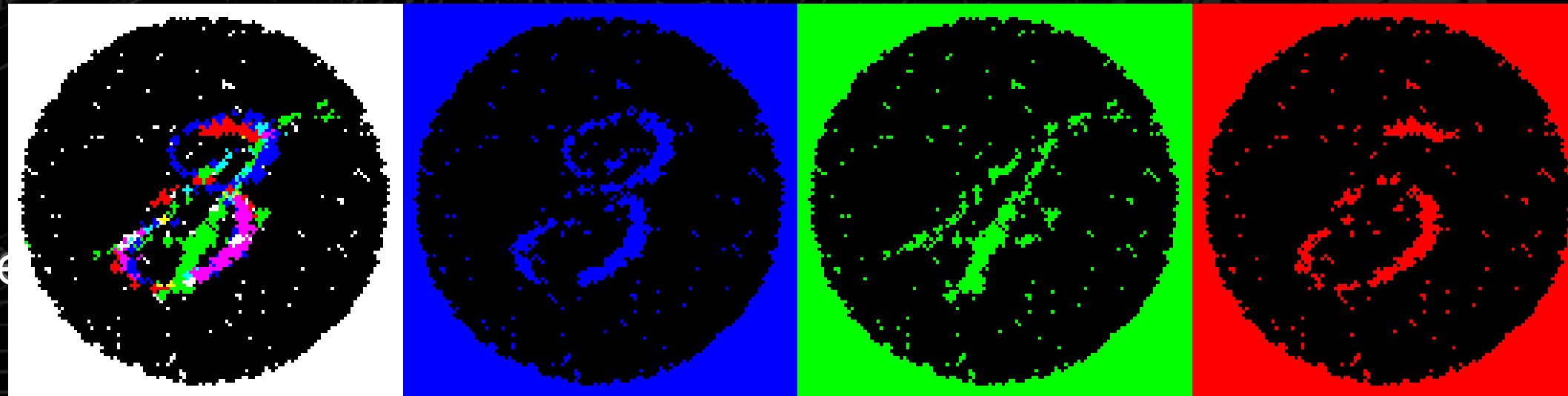
SCA

수사 가방을 열어봅시다

이미지/오디오 포렌식 도구

스테가노그래피란?

데이터를 다른 파일 안에 숨기는 기술



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



SCA

수사 가방을 열어봅시다

이미지/오디오 포렌식 도구

Steganography Online

이미지나 오디오 파일 안에 숨겨진 데이터를 확인

Steganography Online

Encode Decode

Decode image

To decode a hidden message from an image, just choose an image and hit the **Decode** button.

Neither the image nor the message that has been hidden will be at any moment transmitted over the web, all the magic happens within your browser.

파일 선택 선택된 파일 없음

Decode

© 2014 by stylesuxx

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

HxD

binwalk

파일 속성 창

CyberChef

FTK Imager

WinPrefetchView

Wireshark

Steganography Online

grep

Audacity



SCA

수사 가방을 열어봅시다

로그 분석 도구

grep

파일의 내용에서 특정 문자열을 찾고자할 때 사용하는 명령어

```
ph11lp@Phillip: ~
```

```
ph11lp@Phillip:~$ grep [옵션] [패턴] [파일명]
```

HxD

binwalk

파일 속성 창

CyberChef

FTK Imager

WinPrefetchView

Wireshark

Steganography Onl

grep

Audacity



SCA

수사 가방을 열어봅시다

로그 분석 도구

grep

파일의 내용에서 특정 문자열을 찾고자할 때 사용하는 명령어

```
phl1lp@Phillip:/mnt/c/Users/phill/Downloads/Hefty Image/test$ grep "flag" test.txt  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAflagAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
phl1lp@Phillip:/mnt/c/Users/phill/Downloads/Hefty Image/test$ |
```

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

1

2

3



SCA

수사 가방을 열어봅시다

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** : 최대 표시될 수 있는 결과를 제한한다.
- **-E** : 찾을 패턴을 정규 표현식으로 찾는다.
- **-F** : 찾을 패턴을 문자열로 찾는다.

HxD

binwalk

파일 속성 창

CyberChef

FTK Imager

WinPrefetchView

Wireshark

Steganography Online

grep

Audacity



SCA

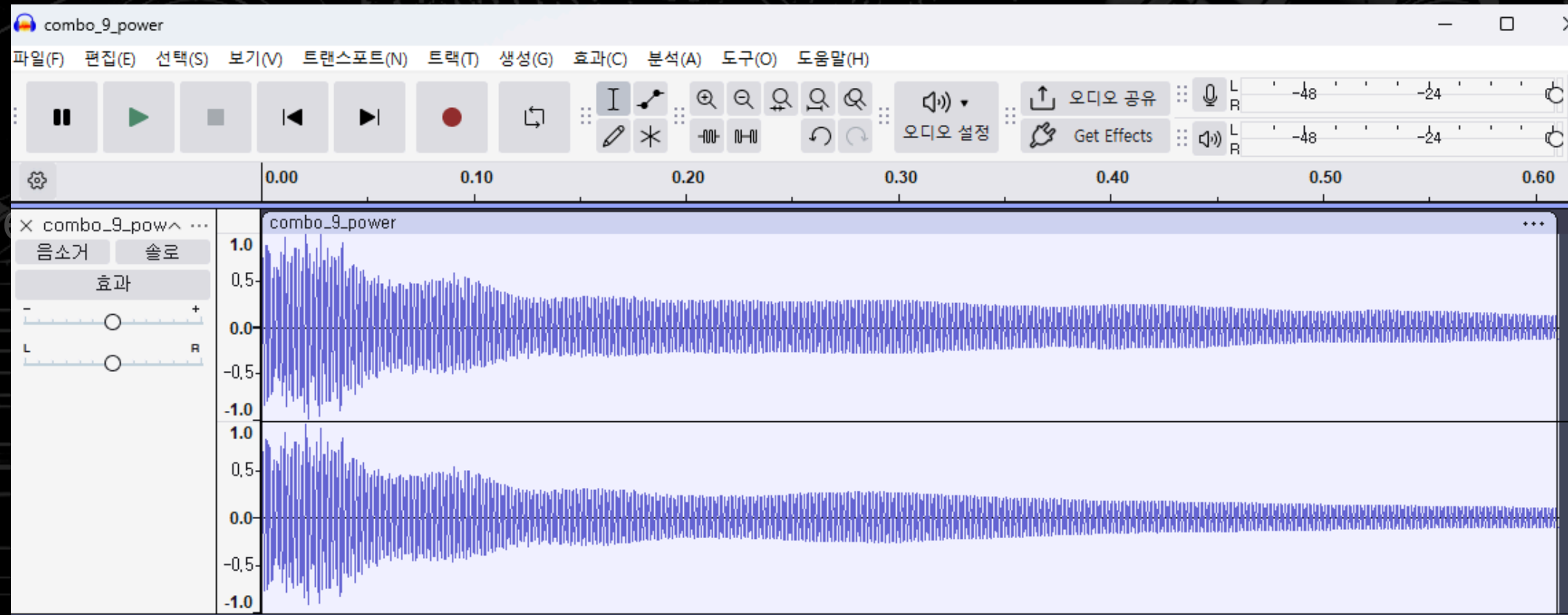
수사 가방을 열어봅시다

이미지/오디오 포렌식 도구

Audacity

무료 오픈소스 오디오 편집·녹음 프로그램

오디오 파일의 파형과 주파수 정보를 시각적으로 분석하는 도구



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

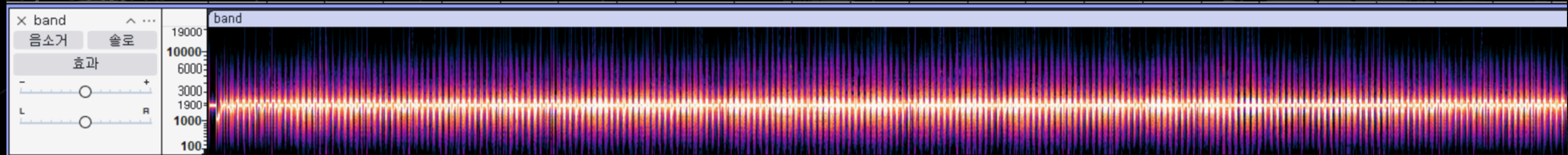
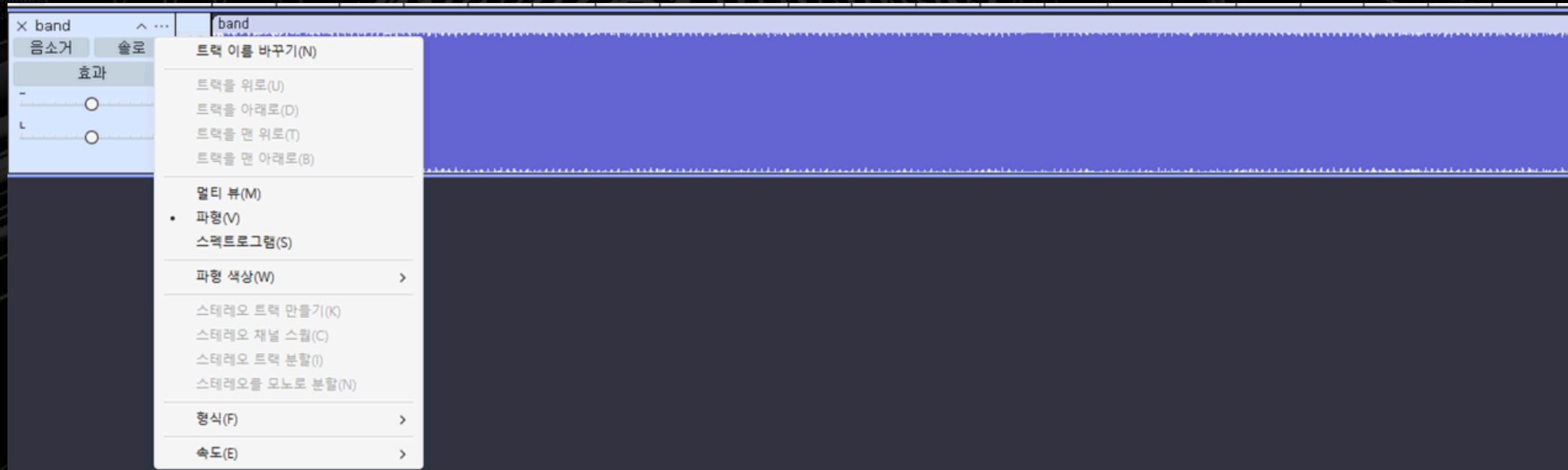


SCA

수사 가방을 열어봅시다

이미지/오디오 포렌식 도구

Audacity



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

1

2

3



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>



SCA

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>



SCA

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

