2025 Ping! 정기 세미나 1차

삭제된 파일을 복구해보자

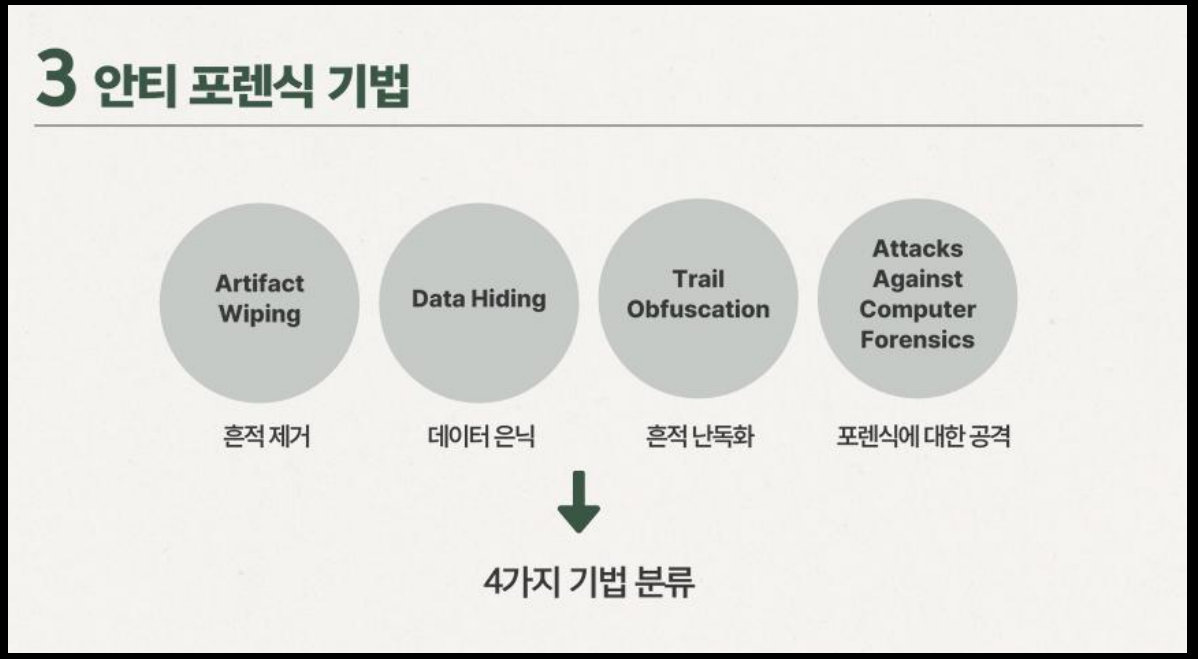
PRESENTER | 임승연 EMAIL | Insndus@gmail.com TEL. | 010-3349-5496

INDEX

1 Intro.

왜 주제를 '삭제된 파일을 복구해보자' 로 정했을까?

1. 진입 장벽을 낮출 수 있을 것
2. 재미있는 주제일 것



안티 포렌식에 대해 알아보자 中

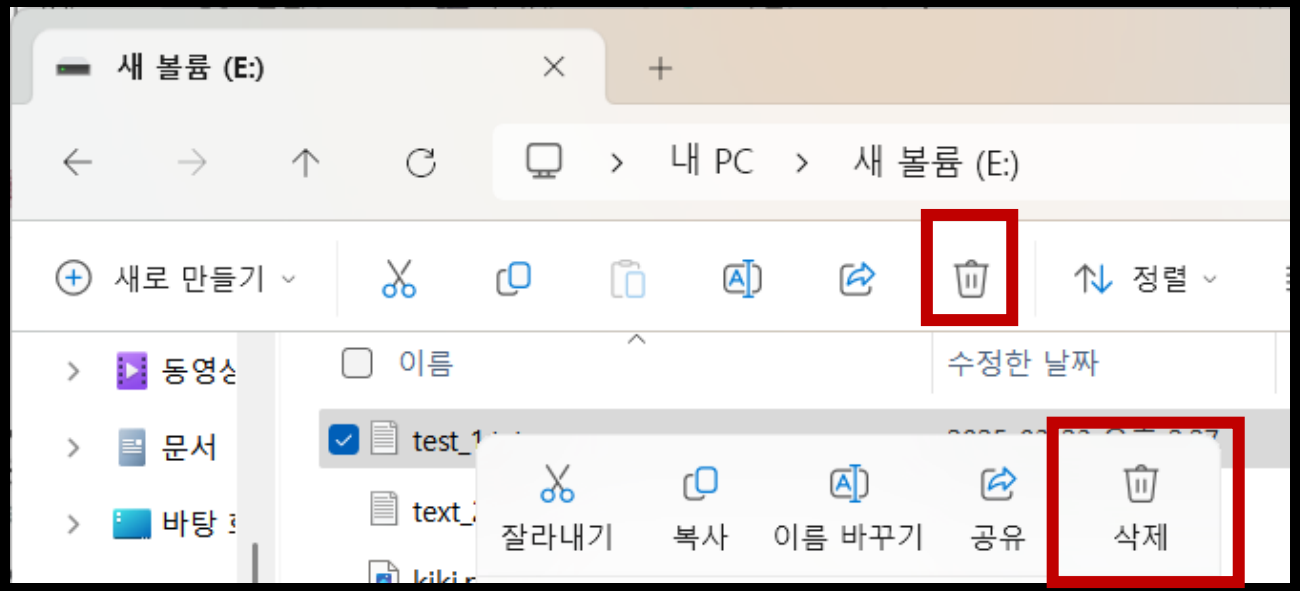
- 디지털 포렌식이란? 디지털 증거를 수집.보존.분석.현출하는데 적용되는 과학기술 및 절차
- 안티 포렌식이란 ? 자신에게 불리하게 작용할 가능성이 있는 증거물을 훼손하거나 차단하는 행위
- 4가지 기법 : 흔적 제거, 데이터 은닉, 흔적 난독화, 포렌식에 대한 공격
- 흔적 제거의 방법 : 파일 및 폴더 삭제 → 파일 카빙 복구 가능 ⇒ 안티-안티 포렌식

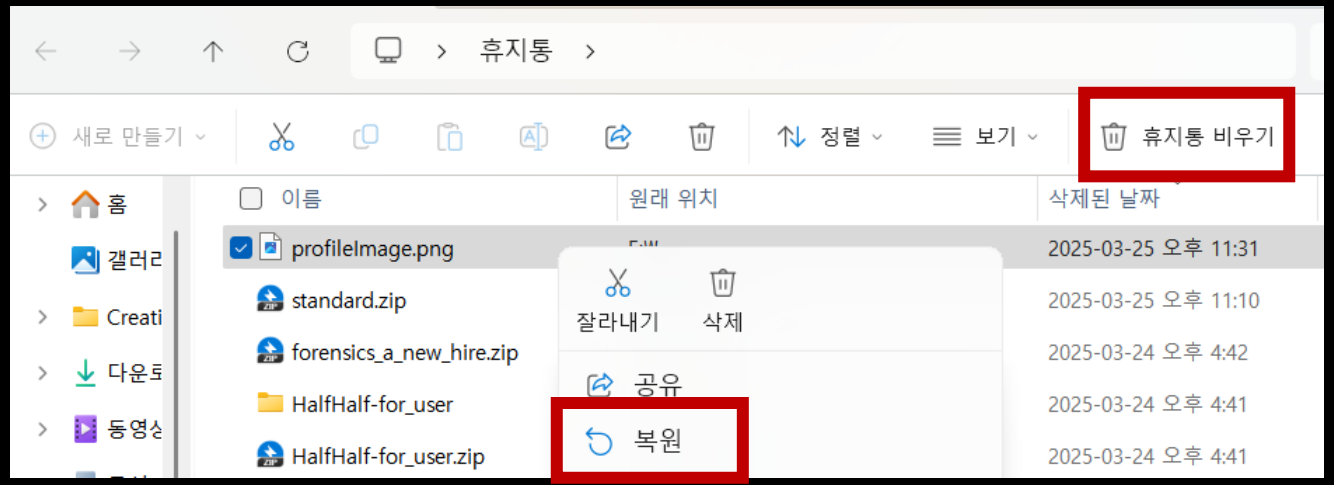
1 Intro.

파일 삭제의 유형

- 일반 삭제 (Delete만)
  - 휴지통에서 복구 가능
  - 파일의 메타데이터를 기반으로 복구 가능

  ⇒ 복원 가능성 GOOD
- 완전 삭제 (SHIFT+DEL)
  - 휴지통을 거치지 않는 경우, 휴지통 비우기와 마찬가지
  - 원본의 흔적 외에는 흔적을 찾기 힘듦





1 Intro.

삭제된 파일 복구 유형

- 파일 메타데이터를 이용한 복구
  - 파일의 메타 정보가 존재하는 경우

- 데이터 카빙
  - 파일의 메타 정보가 덮어쓰여진 경우

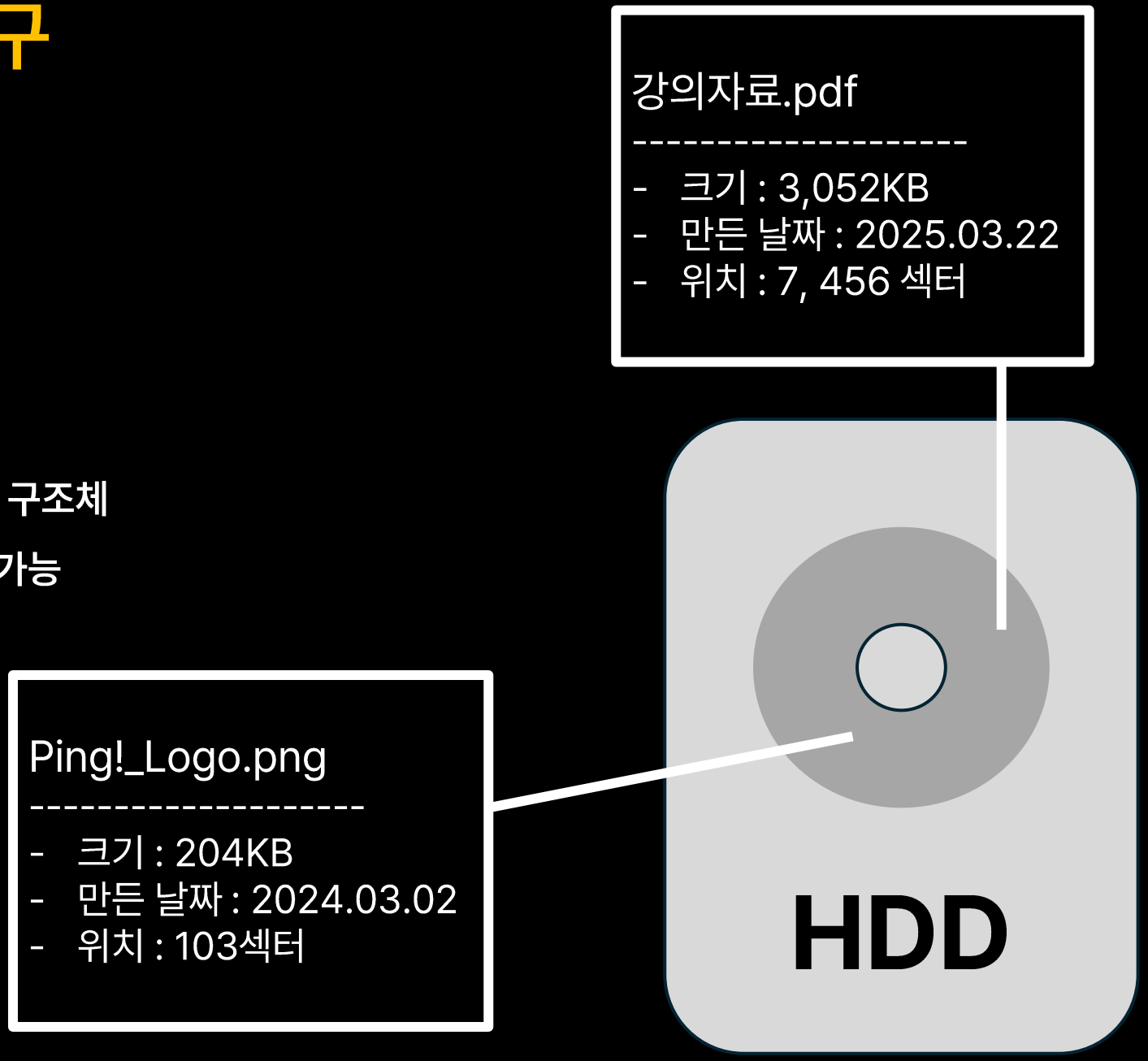
- 덮어쓰여진 파일 복구
  - 파일 데이터가 덮어쓰여진 경우

2 파일 Metadata 기반 복구

용어 정리

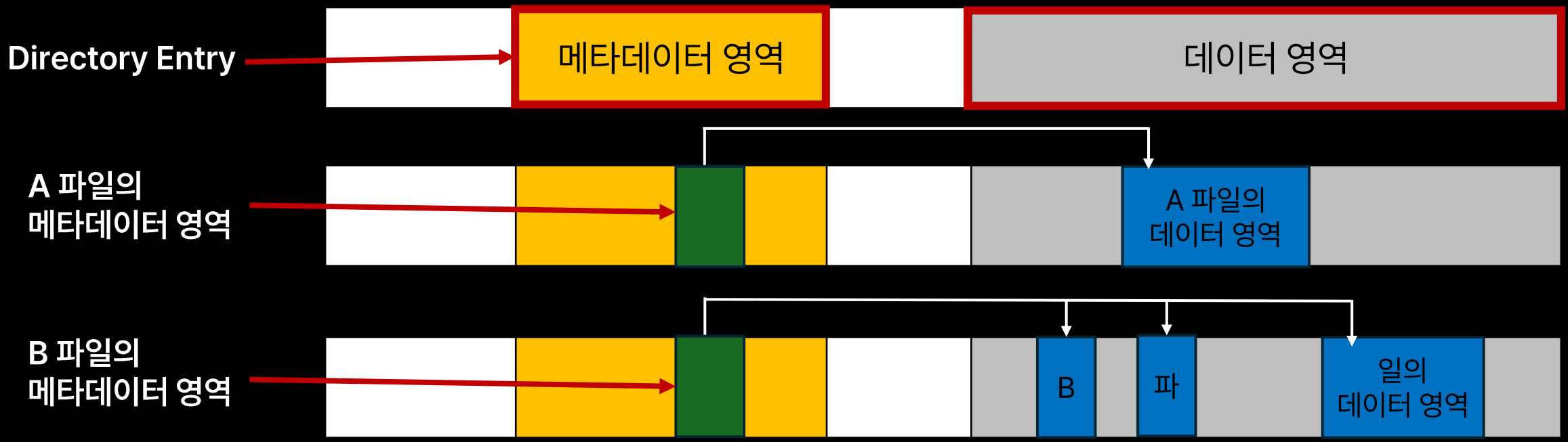
- 메타데이터 (Metadata)
  - 파일의 내용을 정의하고 설명해주는 데이터

- 디렉토리 엔트리 (Directory Entry)
  - 파일의 메타데이터를 저장하는 일정한 크기의 구조체
  - 지워지지 않았다면, 삭제된 파일의 내용 복구 가능



2 파일 Metadata 기반 복구

파일 메타데이터 기반 복구

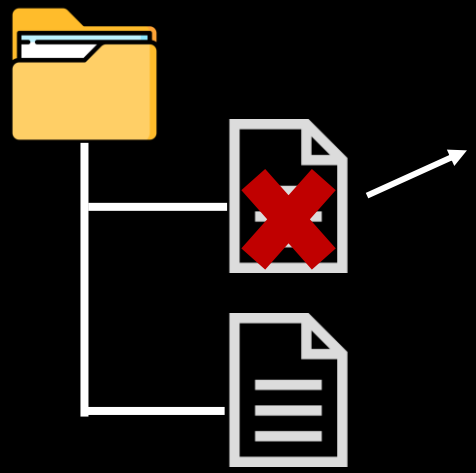


- 복구하고자 하는 파일의 메타 정보와 데이터가 온전하다면 100% 복구

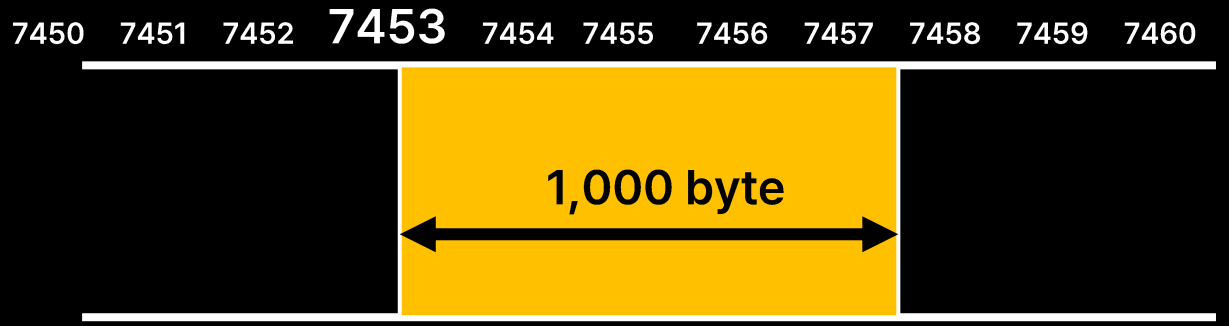
2 파일 Metadata 기반 복구

파일 메타데이터 기반 복구

- 지워지지 않은 Directory Entry를 활용하여 파일 내용을 복구
  - 파일을 완전 삭제해도 파일의 디렉토리 엔트리와 파일 내용은 삭제되지 않음
  - 파일 내용만이 아니라 파일 이름도 복원 가능



- 이름 : test.pdf
- 크기 : 1,000 byte
- 위치 : 7, 453 섹터
- 삭제 여부 : O



2 파일 Metadata 기반 복구

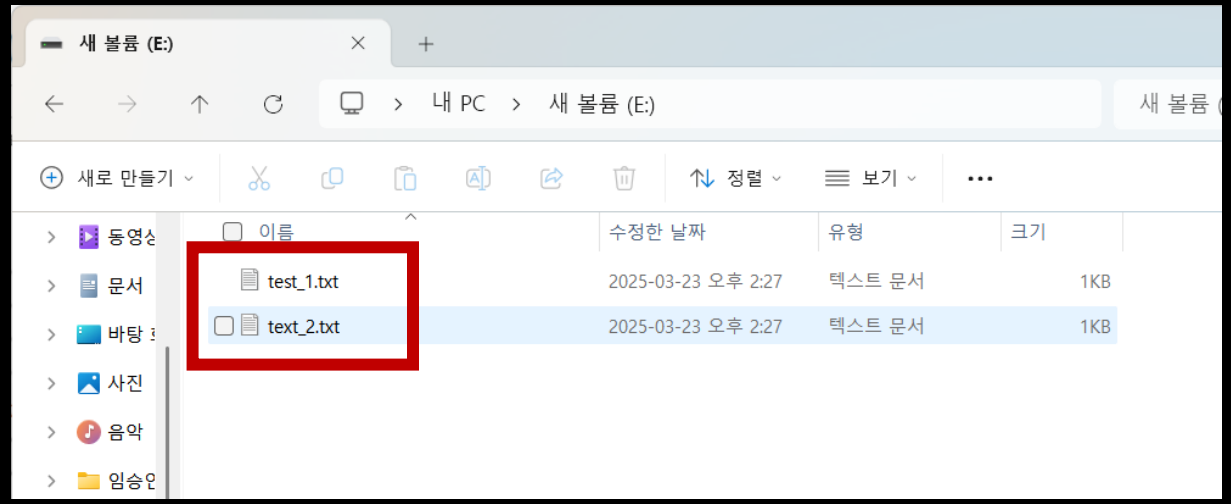
메타데이터 기반 복구 도구

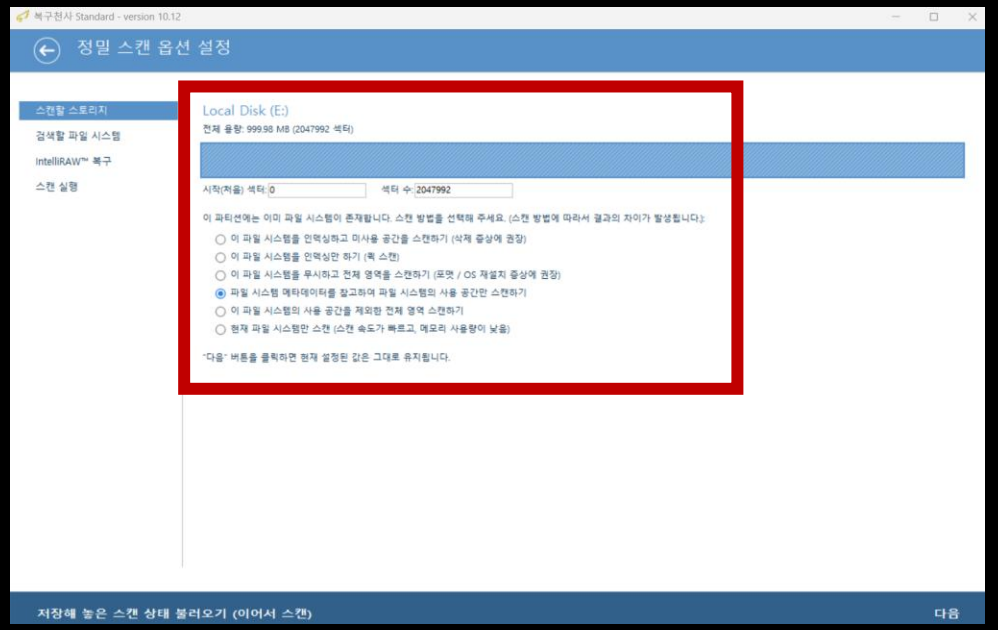
- 복구천사
  - FAT/exFAT에 한해 사용자에게 무료로 복구 도구 제공
- Autopsy
  - 오픈소스 통합 디지털포렌식 분석 도구, 입력된 디스크로부터 삭제된 파일을 별도로 표시
- FTK Imager
  - 디스크 포렌식 도구로써 메타데이터 기반 삭제된 파일 복구 기능 제공
- EnCase
  - 가장 널리 사용되는 디스크 포렌식 도구, 메타데이터 기반 파일 복구 기능 제공

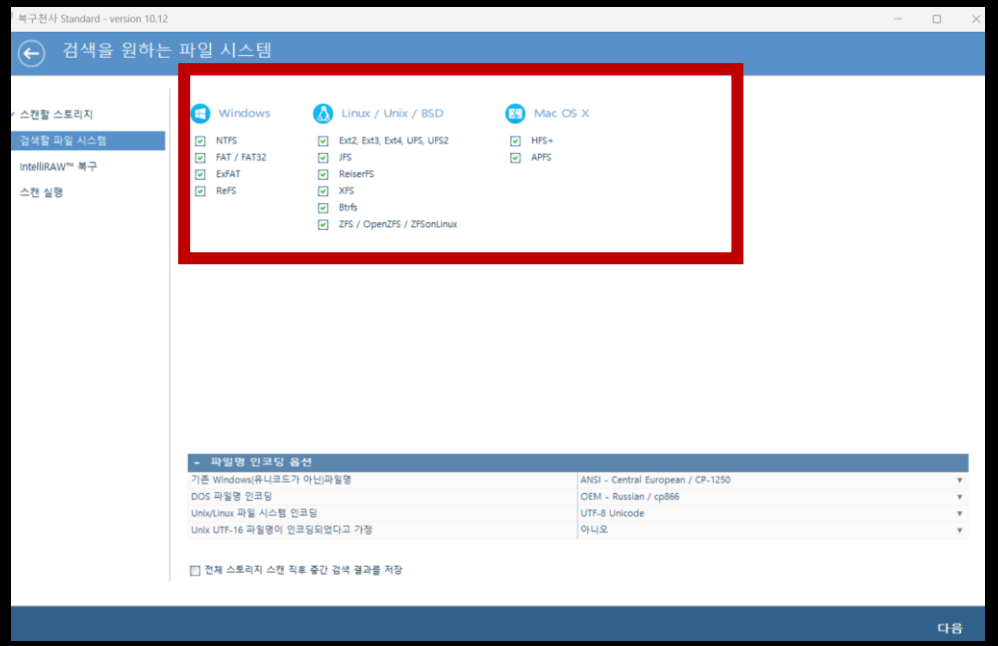
2 파일 Metadata 기반 복구

메타데이터 기반 복구 도구

- 복구천사



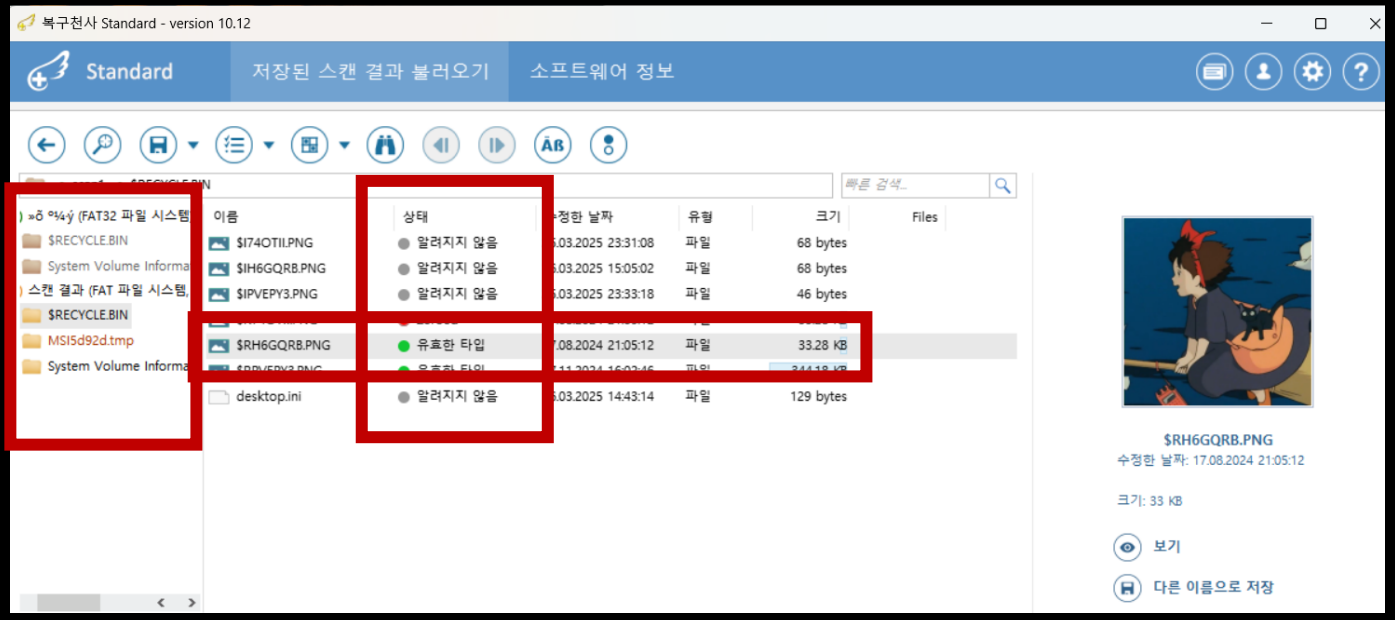


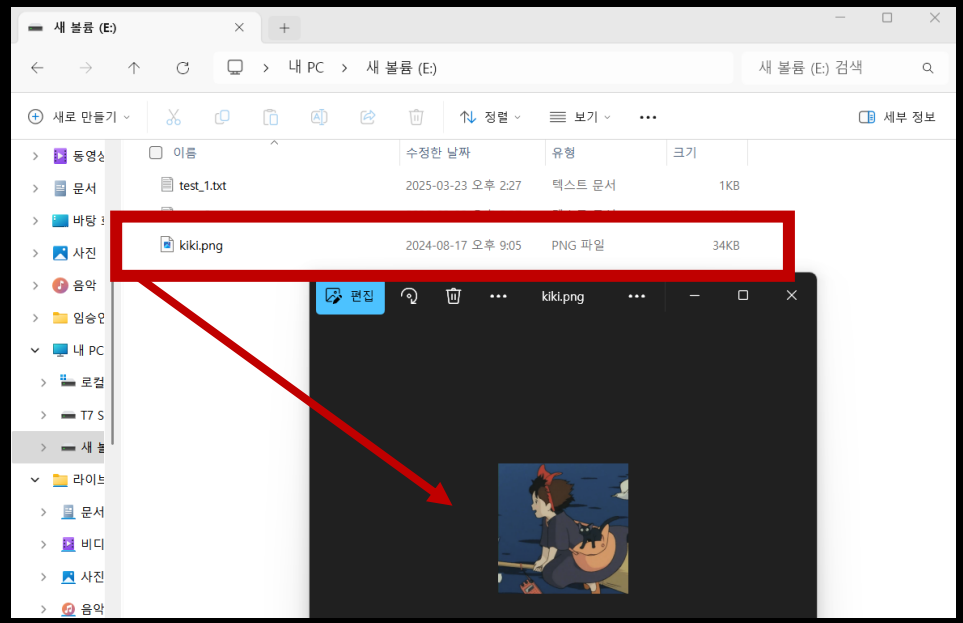


- 볼륨 E에 txt 파일 2개 존재
- 복구천사로 스캔 시작 – 어떤 방법으로 할 지?
- 검색을 원하는 파일 시스템 유형

2 파일 Metadata 기반 복구

메타데이터 기반 복구 도구





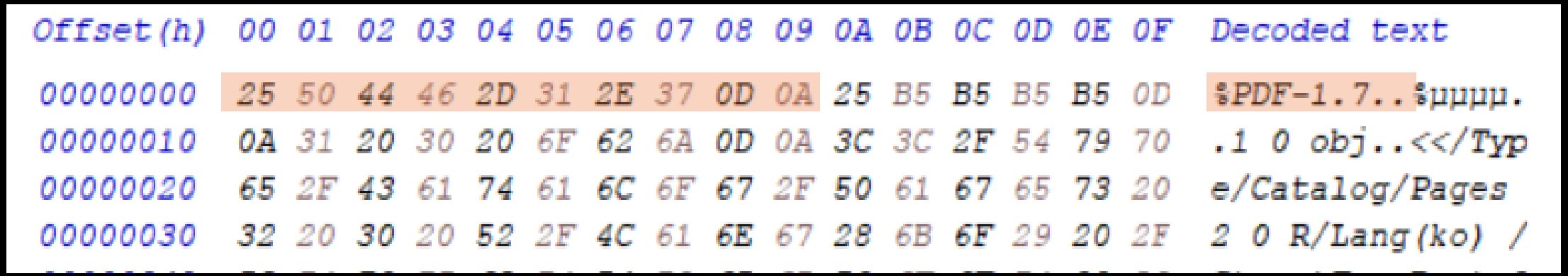
- 스캔 완료 후, $RECYCLE.BIN에서 삭제된 파일을 찾아볼 수 있음.
- [다른 이름으로 저장] – 저장 경로 설정 – 볼륨 E

- 복구 완료 !
- 복구된 사진 확인 가능

3 파일 카빙 기법

용어 정리

- 파일 시그니처 (File Signature)
  - 해당 파일이 어떤 파일 포맷을 가지고 있는지 알려주는 식별자 또는 패턴
- 파일 헤더 (File Header)
  - 파일의 시작 부분에 나타나는 시그니처
- 파일 푸터 (File Footer)
  - 파일의 끝 부분에 나타나는 시그니처, 파일의 끝을 검사할 때 사용

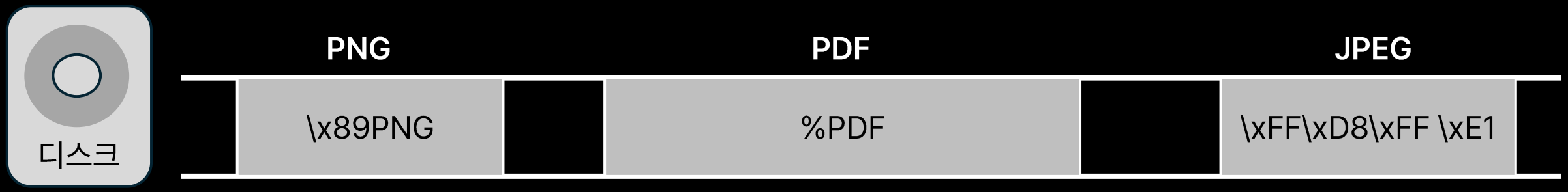


Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	25	50	44	46	2D	31	2E	37	0D	0A	25	B5	B5	B5	B5	0D	%PDF-1.7..%µµµµ.
00000010	0A	31	20	30	20	6F	62	6A	0D	0A	3C	3C	2F	54	79	70	.1 0 obj..<</Typ
00000020	65	2F	43	61	74	61	6C	6F	67	2F	50	61	67	65	73	20	e/Catalog/Pages
00000030	32	20	30	20	52	2F	4C	61	6E	67	28	6B	6F	29	20	2F	2 0 R/Lang(ko) /

3 파일 카빙 기법

파일 카빙 (File Carving)

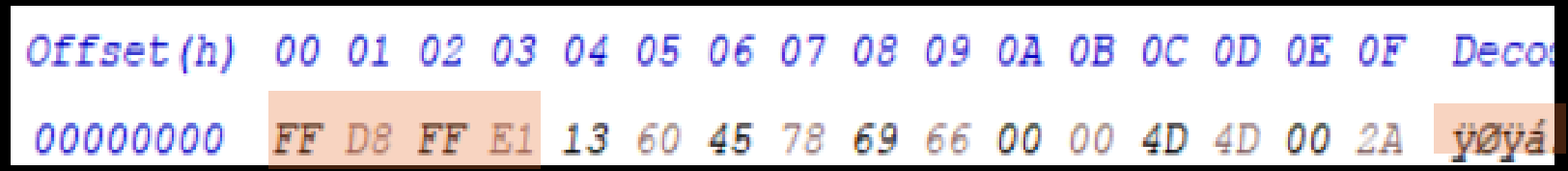
- 파일 시그니처를 기반으로 파일 내용을 복구하는 기술
  - 디렉토리 엔트리 없이 파일 내용 복구 가능
  - 파일 이름은 복원 X
- 작업 수행 시간이 길고, 단편화가 일어난 파일은 온전히 복구할 가능성 ↓
- 단편화된 파일 : 여기저기 흩어져 저장된 데이터들
- 전문 복구 도구를 사용하는 것이 일반적



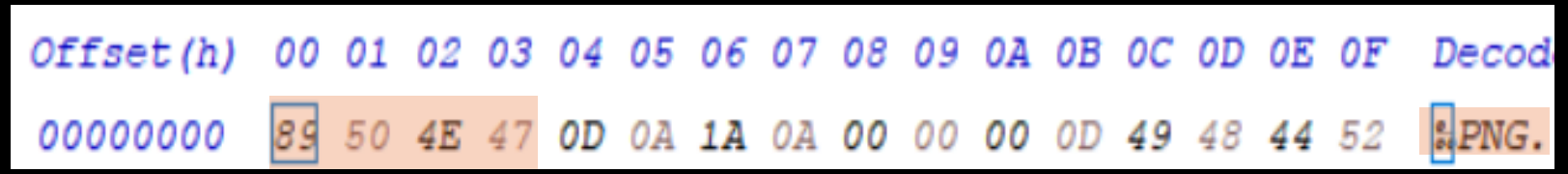
3 파일 카빙 기법

데이터 카빙 (Data Carving)

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Deco
00000000	25	50	44	46	2D	31	2E	37	0D	0A	25	B5	B5	B5	B5	0D	%PDF



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Deco
00000000	FF	D8	FF	E1	13	60	45	78	69	66	00	00	4D	4D	00	2A	ÿØÿá



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decod
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	‰PNG.

- 메타 정보가 없는 경우, 개별 파일 구조에 기반해 복구 → 데이터 카빙 (Data Carving)
- 바이너리 스트림에서 의미 있는 정보를 획득하는 기법

3 파일 카빙 기법

파일 카빙 기반 복구 도구

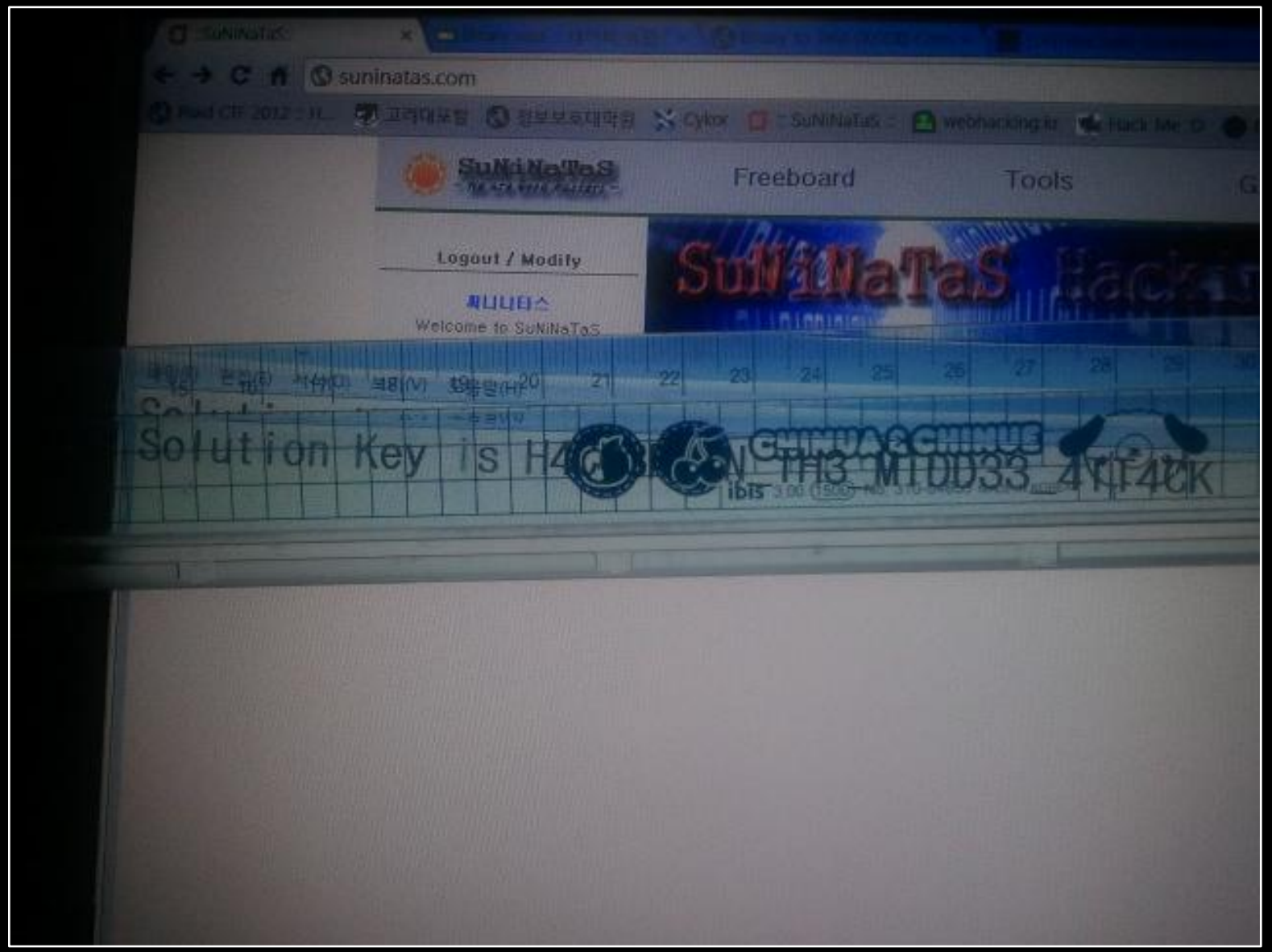
- PhotoRec
  - 오픈소스 데이터 복구 도구로 300개 이상의 파일 유형을 카빙 가능, GUI 제공
- Bulk Extractor
  - 오픈 소스 카빙 도구로 파일 뿐만 아니라 이메일, 신용카드 번호 등 다양한 유형의 데이터를 추출
- X-Ways Forensics
  - 상용 디지털포렌식 도구로 성능이 가장 좋음
- Recuva
  - Ccleaner를 제작한 개발사가 만든 파일 카빙 프로그램
- foremost
  - 파일 헤더와 푸터를 사용하여 할당되지 않은 공간에서 파일을 복구, Kali에서 기본 제공되는 도구

3 파일 카빙 기법

메타데이터 기반 복구 도구

- foremost
  - kali에서 실행
  - suninatas의 21번 문제

  - Flag 값으로 의심되는 부분을 완성시켜야겠다!!



3 파일 카빙 기법

메타데이터 기반 복구 예제

monitor.jpg

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	FF	D8	FF	E1	29	7E	45	78	69	66	00	00	49	49	2A	00	ÿØÿá)~Exif..II*
00000010	08	00	00	00	0B	00	0E	01	02	00	14	00	00	00	92	00	..............’
00000020	00	00	0F	01	02	00	14	00	00	00	A6	00	00				
00000030	02	00	0A	00	00	00	BA	00	00	00	12	01	03				

오프셋	잘라내기 (16진수)
0	FF D8 FF E1 29 7E 45 78 69 66 00 00 49 49 2A 00 08 00 00 00
17D8E	04 1E A0 D5 66 74 0C 09 60 0E 31 8A 5B 12 D7 43 FF D8 FF E1
2FE5A	EE E5 99 B7 83 80 38 6E 73 FE 7A 50 85 28 BB 1F FF D8 FF E1 2
47CF5	39 52 A3 04 7F 78 64 7F 85 34 AC 35 15 17 76 7F FF D8 FF E1
5FA83	04 1E A0 D5 66 74 0C 09 60 0E 31 8A 5B 12 D7 43 FF D8 FF E1
77B4F	EE E5 99 B7 83 80 38 6E 73 FE 7A 50 85 28 BB 1F FF D8 FF E1 2
8F9EA	39 52 A3 04 7F 78 64 7F 85 34 AC 35 15 17 76 7F FF D8 FF E1
A7778	04 1E A0 D5 66 74 0C 09 60 0E 31 8A 5B 12 D7 43 FF D8 FF E1
BF844	EE E5 99 B7 83 80 38 6E 73 FE 7A 50 85 28 BB 1F FF D8 FF E1 2
D76DF	39 52 A3 04 7F 78 64 7F 85 34 AC 35 15 17 76 7F FF D8 FF E1
EF46D	04 1E A0 D5 66 74 0C 09 60 0E 31 8A 5B 12 D7 43 FF D8 FF E1
107539	EE E5 99 B7 83 80 38 6E 73 FE 7A 50 85 28 BB 1F FF D8 FF E1 2
11F3D4	39 52 A3 04 7F 78 64 7F 85 34 AC 35 15 17 76 7F FF D8 FF E1
137162	04 1E A0 D5 66 74 0C 09 60 0E 31 8A 5B 12 D7 43 FF D8 FF E1
14F22F	EE E5 99 B7 83 80 38 6E 73 FE 7A 50 85 28 BB 1F FF D8 FF E1 2

- 접근 방법
  - HxD에서 monitor.jpg 분석
  - jpg 파일 시그니처 : FF D8 FF E1
  - 파일 시그니처를 검색
  - jpg가 여러 개인가? 의심

3 파일 카빙 기법

메타데이터 기반 복구 도구

- foremost

- 접근 방법
  - ls : 현재 디렉토리 목록 확인
  - file로 파일의 확장자명과 정보를 간단하게 조회
  - exiftool : jpg임을 알았으니, 이미지의 메타 데이터 조회
  - 수상한 부분 발견 !! → 왜 일시가 다 다르지? 수정된 파일인가?
  - foremost –i [filename] : 분석할 [filename] 지정 후 분석
  - ls : foremost 분석 결과가 output 디렉토리에 생성

```
┌──(kali㉿kali)-[~/Downloads/wargame]
└─$ ls
monitor.jpg

┌──(kali㉿kali)-[~/Downloads/wargame]
└─$ file monitor.jpg
monitor.jpg: JPEG image data, Exif standard: [TIFF image
    , manufacturer=SAMSUNG                , model=SHW-M110S,
utionunit=2, software=fw 49.1 prm 49.104, datetime=2012

┌──(kali㉿kali)-[~/Downloads/wargame]
└─$ exiftool monitor.jpg
ExifTool Version Number         : 13.10
File Name                       : monitor.jpg
Directory                       : .
File Size                       : 1471 kB
File Modification Date/Time     : 2025:02:21 11:17:08-05:00
File Access Date/Time           : 2025:03:26 08:35:51-04:00
File Inode Change Date/Time     : 2025:03:26 08:35:51-04:00
```

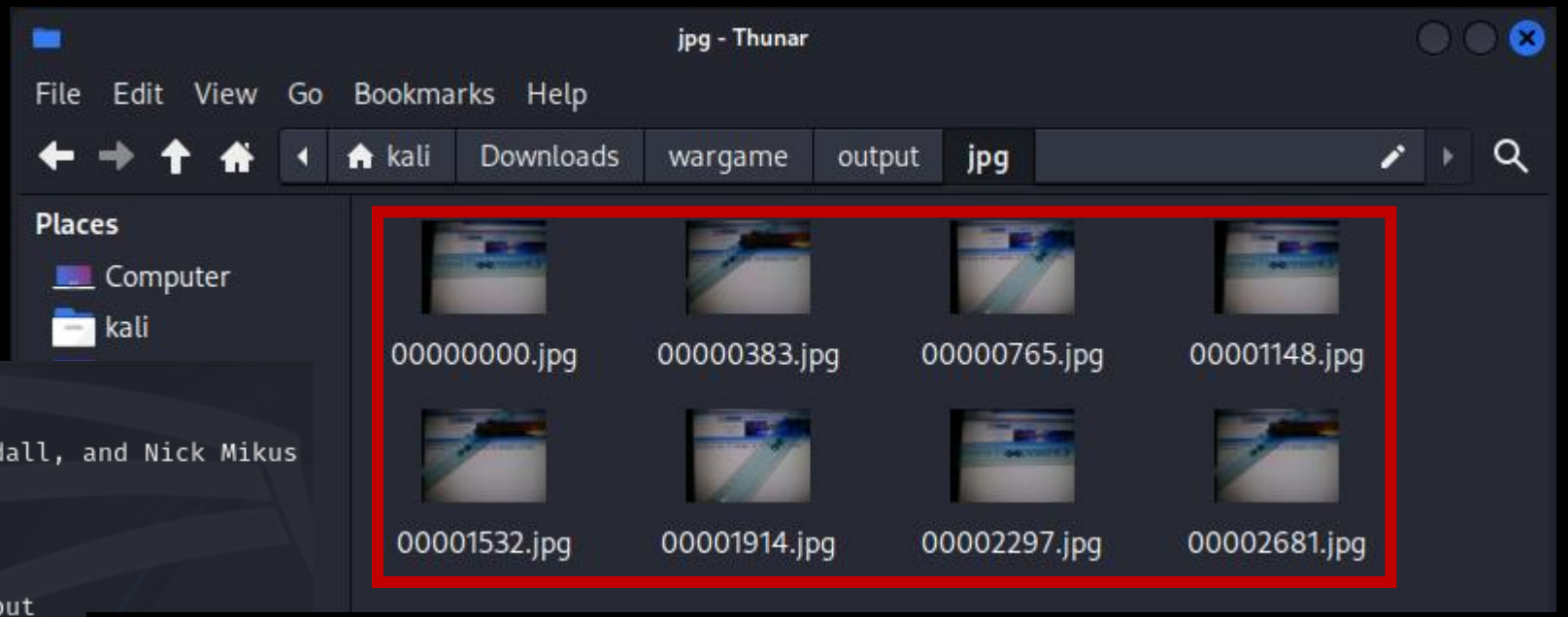
```
┌──(kali㉿kali)-[~/Downloads/wargame]
└─$ foremost -i monitor.jpg
Processing: monitor.jpg
|*|

┌──(kali㉿kali)-[~/Downloads/wargame]
└─$ ls
monitor.jpg  output
```

3 파일 카빙 기법

메타데이터 기반 복구 도구

- foremost




```
┌──(kali㉿kali)-[~/Downloads/wargame/output]
└─$ cat audit.txt
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Wed Mar 26 08:40:07 2025
Invocation: foremost -i monitor.jpg
Output directory: /home/kali/Download/wargame/output
Configuration file: /etc/foremost.con
------------------------------------------------------------------
File: monitor.jpg
Start: Wed Mar 26 08:40:07 2025
Length: 1 MB (1470667 bytes)

Num      Name (bs=512)         Size      File Offset

0:      00000000.jpg          105 KB             0
1:      00000383.jpg          105 KB        196186
2:      00000765.jpg          106 KB        391811
3:      00001148.jpg          105 KB        588266
4:      00001532.jpg          105 KB        784452
5:      00001914.jpg          106 KB        980077
6:      00002297.jpg          105 KB       1176532
7:      00002681.jpg           95 KB       1372718
Finish: Wed Mar 26 08:40:08 2025
```

- 접근 방법
  - cat audit.txt : 생성된 output 디렉토리 안의 audit.txt 를 통해 숨겨져 있거나 복구된 목록을 조회 가능
  - wargame/output/jpg 에서 숨겨져 있던 이미지들을 확인 가능
  - 파일명은 복구되지 않음을 확인 가능
  - 복구된 파일들의 File Offset == HxD에서 확인한 파일 헤더 시그니처

4 마무리

메타데이터 복구 기술 vs 파일 카빙 기술

비교 항목	메타데이터 기반 복구	파일 카빙
속도	빠름	느림
파일 복구 정확도	높음	낮음
오탐 빈도	거의 없음	매우 많음
파일 이름 복구	가능	불가능
포맷 시 복구	저장장치를 포맷할 경우 복구 불가	파일 시그니처 기반이기 때문에 저장장치를 포맷해도 복구 가능
단편화된 파일 복구	정확히 복구 가능	온전한 복구 어려움

Reference

- DFRC [디지털포렌식시리즈] 삭제 파일 복구 기술
  https://youtu.be/60FtdnBey-E?si=IUnewZVINfF5MITF
- https://github.com/proneer/Slides/blob/master/Advanced/
  (FP) 데이터 복구의 거의 모든 것 (Almost Everything for Data Recovery).pdf
- http://suninatas.com/ Forensic 21번 문제