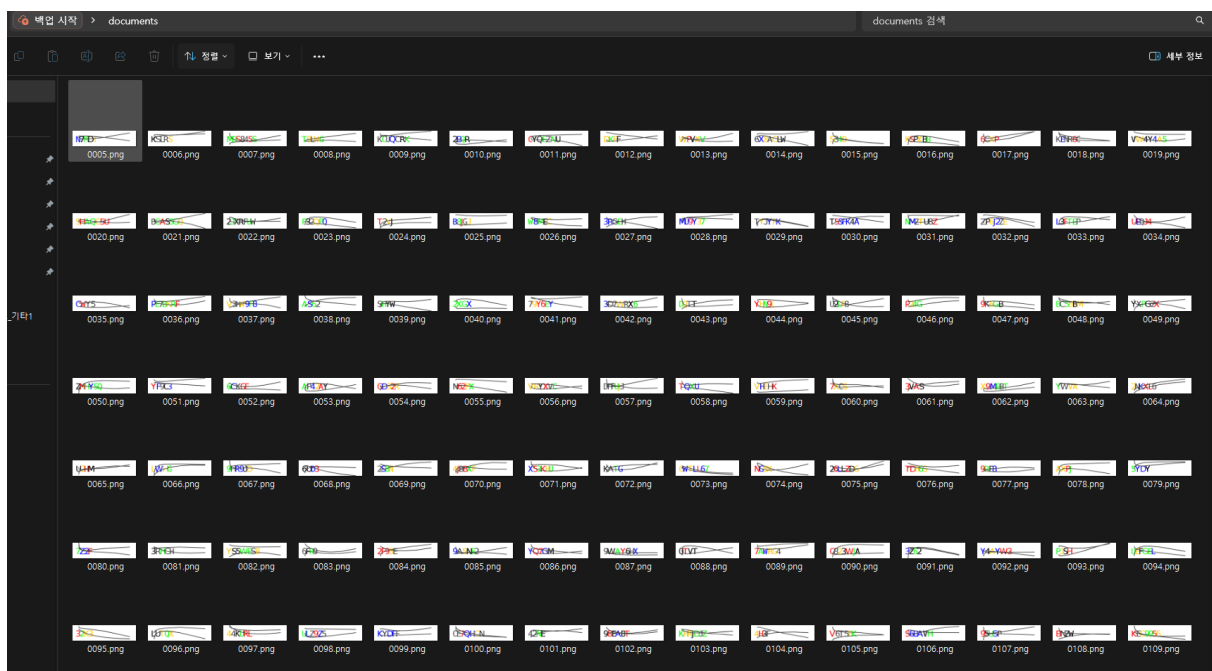


Leaked

≡ 문제 분류	forensic
≡ poc 작성자	김재환
≡ 문제 개발자	김재환

1. 문제

문제에서 제공하는 파일을 열어보면, 엄청난 양의 사진이 존재합니다.



여기서 뭘 찾으려고 하는지 알아야 합니다. 문제를 잘 읽어보겠습니다.

챌린지

0명 해결함



Leaked 1000

산업 스파이는 설계도면이나 파일등에 무언갈 숨겨서 내부자료를 탈취하려고 합니다.

이번에 SOTI에서도 산업 스파이 사건이 발생했다는데요!!
LLM 학습 모델 파일에 숨겨서 내부자료를 밖으로 빼려고 했던 것 같습니다.

과연 산업 스파이가 빼내려고 했던 자료는 무엇일까요?

↓ documents...

플래그
















































제출

- 산업 스파이가 LLM 학습 모델이 내부자료를 숨겼다고 합니다.
- 해당 자료를 찾으면 되는 문제인 것 같습니다.

2. 풀이

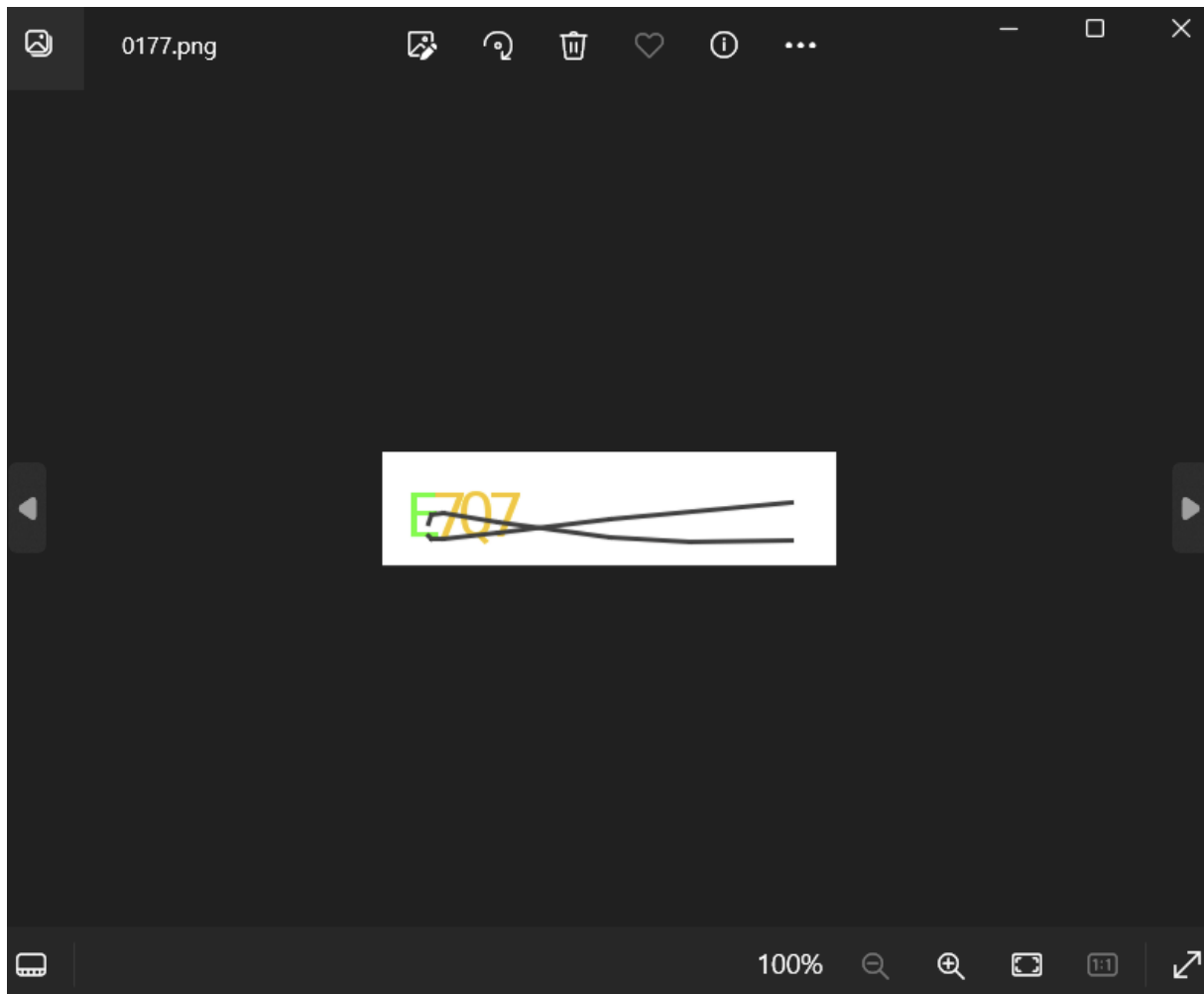
2.1 파일 크기 확인

파일에 무언가를 숨겼다면, 파일 크기가 다른 학습 모델 사진에 비해서 클 확률이 높습니다.

rw-rwxrwx	1	jalnik	jalnik	4 KiB	Tue Feb 6 23:42:04 2024		0155.png
rw-rwxrwx	1	jalnik	jalnik	2 KiB	Tue Feb 6 23:42:06 2024		0156.png
rw-rwxrwx	1	jalnik	jalnik	4 KiB	Tue Feb 6 23:42:06 2024		0157.png
rw-rwxrwx	1	jalnik	jalnik	3 KiB	Tue Feb 6 23:42:08 2024		0158.png
rw-rwxrwx	1	jalnik	jalnik	4 KiB	Tue Feb 6 23:42:08 2024		0159.png
rw-rwxrwx	1	jalnik	jalnik	4 KiB	Tue Feb 6 23:42:08 2024		0160.png
rw-rwxrwx	1	jalnik	jalnik	4 KiB	Tue Feb 6 23:42:10 2024		0161.png
rw-rwxrwx	1	jalnik	jalnik	5 KiB	Tue Feb 6 23:42:10 2024		0162.png
rw-rwxrwx	1	jalnik	jalnik	4 KiB	Tue Feb 6 23:42:12 2024		0163.png
rw-rwxrwx	1	jalnik	jalnik	5 KiB	Tue Feb 6 23:42:12 2024		0164.png
rw-rwxrwx	1	jalnik	jalnik	3 KiB	Tue Feb 6 23:42:14 2024		0165.png
rw-rwxrwx	1	jalnik	jalnik	2 KiB	Tue Feb 6 23:42:14 2024		0166.png
rw-rwxrwx	1	jalnik	jalnik	3 KiB	Tue Feb 6 23:42:16 2024		0167.png
rw-rwxrwx	1	jalnik	jalnik	4 KiB	Tue Feb 6 23:42:16 2024		0168.png
rw-rwxrwx	1	jalnik	jalnik	5 KiB	Tue Feb 6 23:42:16 2024		0169.png
rw-rwxrwx	1	jalnik	jalnik	3 KiB	Tue Feb 6 23:42:18 2024		0170.png
rw-rwxrwx	1	jalnik	jalnik	4 KiB	Tue Feb 6 23:42:18 2024		0171.png
rw-rwxrwx	1	jalnik	jalnik	3 KiB	Tue Feb 6 23:42:20 2024		0172.png
rw-rwxrwx	1	jalnik	jalnik	4 KiB	Tue Feb 6 23:42:20 2024		0173.png
rw-rwxrwx	1	jalnik	jalnik	5 KiB	Tue Feb 6 23:42:22 2024		0174.png
rw-rwxrwx	1	jalnik	jalnik	3 KiB	Tue Feb 6 23:42:22 2024		0175.png
rw-rwxrwx	1	jalnik	jalnik	4 KiB	Tue Feb 6 23:42:24 2024		0176.png
rw-rwxrwx	1	jalnik	jalnik	12 KiB	Fri May 3 17:17:15 2024		0177.png
rw-rwxrwx	1	jalnik	jalnik	5 KiB	Tue Feb 6 23:42:24 2024		0178.png
rw-rwxrwx	1	jalnik	jalnik	3 KiB	Tue Feb 6 23:42:26 2024		0179.png
rw-rwxrwx	1	jalnik	jalnik	4 KiB	Tue Feb 6 23:42:26 2024		0180.png
rw-rwxrwx	1	jalnik	jalnik	5 KiB	Tue Feb 6 23:42:28 2024		0181.png
rw-rwxrwx	1	jalnik	jalnik	4 KiB	Tue Feb 6 23:42:28 2024		0182.png
rw-rwxrwx	1	jalnik	jalnik	4 KiB	Tue Feb 6 23:42:30 2024		0183.png
rw-rwxrwx	1	jalnik	jalnik	4 KiB	Tue Feb 6 23:42:30 2024		0184.png
rw-rwxrwx	1	jalnik	jalnik	2 KiB	Tue Feb 6 23:42:30 2024		0185.png
rw-rwxrwx	1	jalnik	jalnik	4 KiB	Tue Feb 6 23:42:32 2024		0186.png
rw-rwxrwx	1	jalnik	jalnik	4 KiB	Tue Feb 6 23:42:32 2024		0187.png
rw-rwxrwx	1	jalnik	jalnik	3 KiB	Tue Feb 6 23:42:34 2024		0188.png
rw-rwxrwx	1	jalnik	jalnik	3 KiB	Tue Feb 6 23:42:34 2024		0189.png
rw-rwxrwx	1	jalnik	jalnik	3 KiB	Tue Feb 6 23:42:36 2024		0190.png
rw-rwxrwx	1	jalnik	jalnik	4 KiB	Tue Feb 6 23:42:36 2024		0191.png
rw-rwxrwx	1	jalnik	jalnik	3 KiB	Tue Feb 6 23:42:36 2024		0192.png
rw-rwxrwx	1	jalnik	jalnik	4 KiB	Tue Feb 6 23:42:38 2024		0193.png
rw-rwxrwx	1	jalnik	jalnik	3 KiB	Tue Feb 6 23:42:38 2024		0194.png
rw-rwxrwx	1	jalnik	jalnik	3 KiB	Tue Feb 6 23:42:40 2024		0195.png
rw-rwxrwx	1	jalnik	jalnik	4 KiB	Tue Feb 6 23:42:40 2024		0196.png
rw-rwxrwx	1	jalnik	jalnik	4 KiB	Tue Feb 6 23:42:42 2024		0197.png
rw-rwxrwx	1	jalnik	jalnik	4 KiB	Tue Feb 6 23:42:42 2024		0198.png
rw-rwxrwx	1	jalnik	jalnik	3 KiB	Tue Feb 6 23:42:44 2024		0199.png
rw-rwxrwx	1	jalnik	jalnik	4 KiB	Tue Feb 6 23:42:44 2024		0200.png
rw-rwxrwx	1	jalnik	jalnik	4 KiB	Tue Feb 6 23:42:44 2024		0201.png

- 아니나 다를까 177번 사진의 파일의 크기가 다른 파일에 비해 2배 이상 큼니다

육안으로 볼때는 별 차이가 없어 보입니다..



일단 파일을 숨겼다고 했으니, 파일의 시그니처가 남아있을 것입니다. 파일 카빙을 진행해 볼 수 있습니다.

파일 카빙

파일 카빙(file carving)은 디스크 이미지, 메모리 덤프 등에서 파일을 추출하는 과정을 의미합니다.

- binwalk를 사용하면 쉽게 카빙할 수 있습니다.

카빙 결과

```

> /mnt/c/Users/silmu/Desktop/documents
binwalk -e ./0177.png

```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 300 x 75, 8-bit/color RGB, non-interlaced
41	0x29	Zlib compressed data, best compression
3785	0xEC9	PNG image, 400 x 513, 8-bit/color RGBA, non-interlaced
3876	0xF24	Zlib compressed data, compressed

- 오! 두개의 PNG가 한개의 파일에 겹쳐 있는 것을 볼 수 있습니다.

이제 다시 binwalk를 이용하여 파일을 추출해 보도록 하겠습니다.

파일 추출

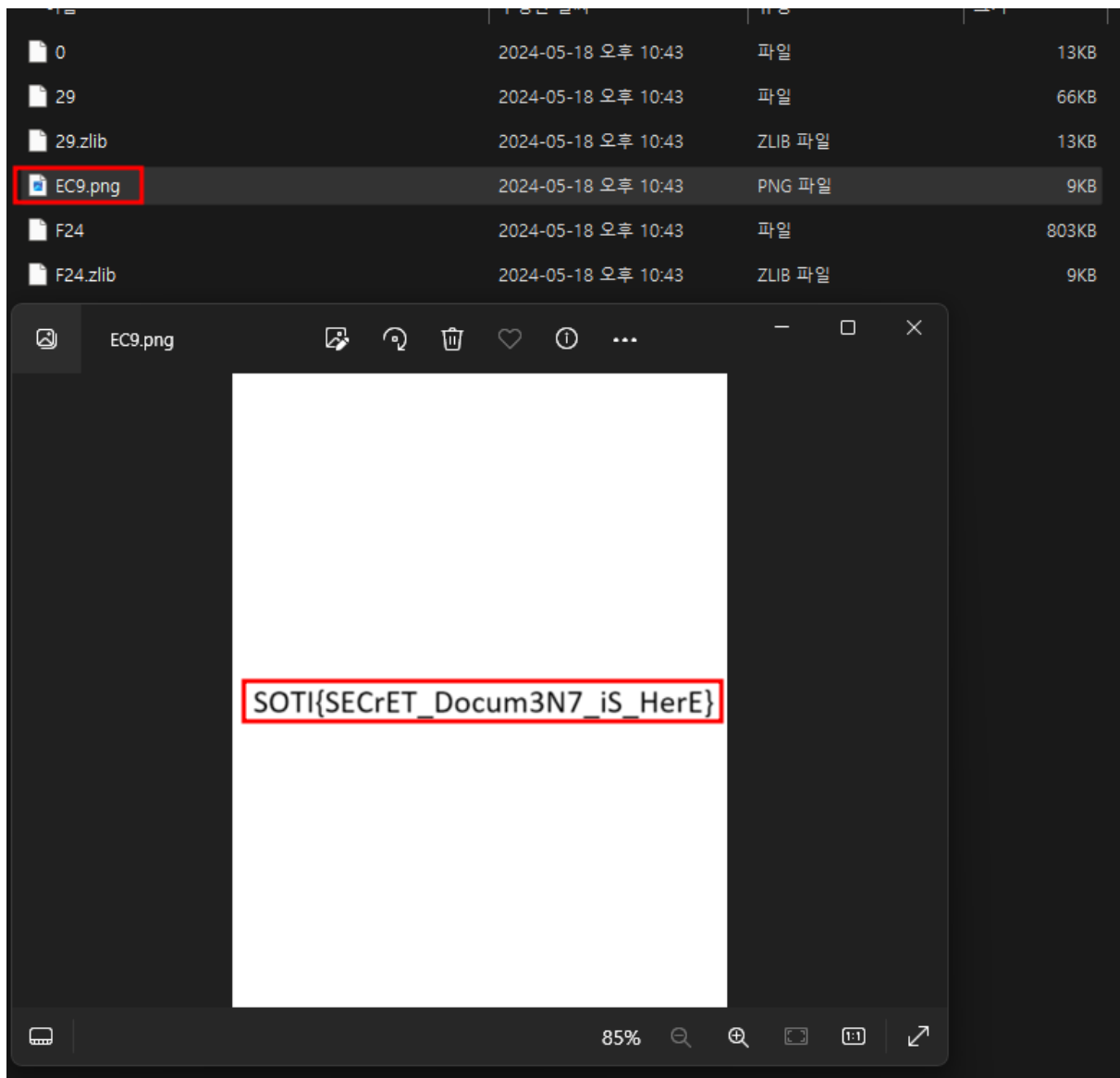
```

> /mnt/c/Users/silmu/Desktop/documents
binwalk --dd ".*" 0177.png

```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 300 x 75, 8-bit/color RGB, non-interlaced
41	0x29	Zlib compressed data, best compression
3785	0xEC9	PNG image, 400 x 513, 8-bit/color RGBA, non-interlaced
3876	0xF24	Zlib compressed data, compressed

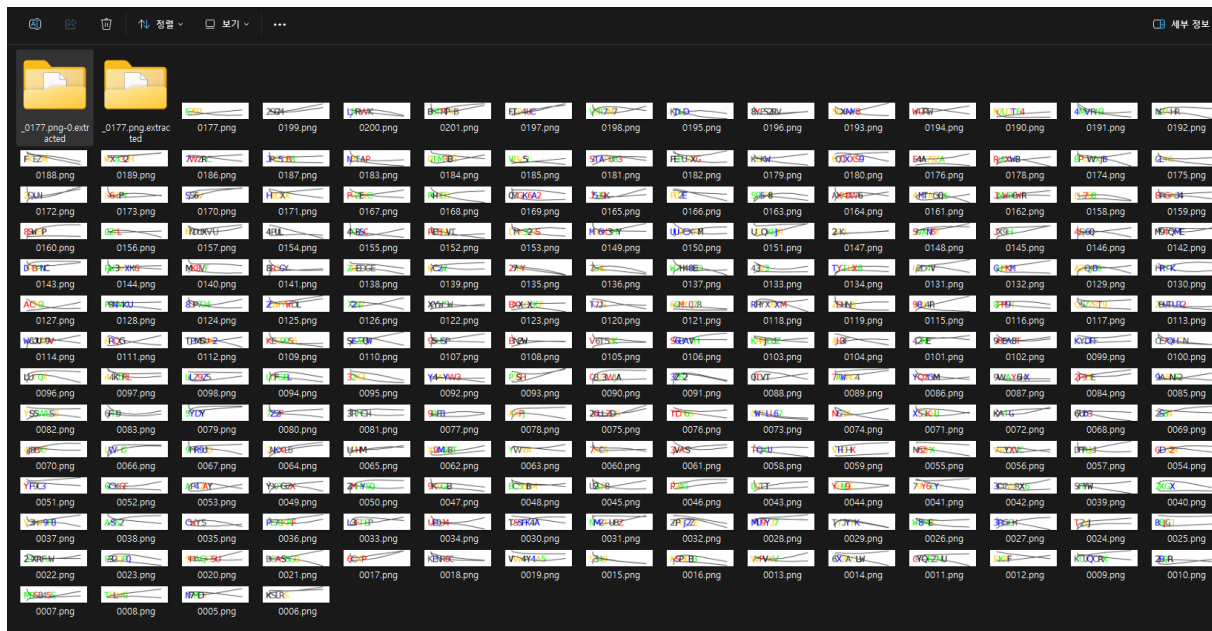
결과



- 이런 비밀 문서가 숨겨져 있었군요!

2.2 수정 시간

이렇게 생각해 볼 수 있습니다. 문제를 낸 사람이 그림이야 어디서 퍼왔겠고... flag를 숨겨야 했을텐데 그렇다면 최근에 수정된 파일을 보면 되는게 아닐까??? 라구요



- 수정 시간으로 조회하면 **0177.png** 가 최근에 수정된 것을 볼 수 있습니다.
- 이후 풀이는 같습니다.



HxD로 파일 시그니처를 탐색하면 안되나요?

- 그래도 됩니다. 하지만 **binwalk** 를 먼저 사용하여, 시그니처 탐색을 하고 하는 것이 더 바람직합니다.