# 151 – Layers of Secrecy

## Team Information

**Team Name : HUNTR/X**

**Team Member : Hyeonseo Shin, Seungyeon Lim, Sugyung Lee**

**Email Address : huntrix@googlegroups.com**

Teams must:

- Provide a detailed, step-by-step description of their problem-solving approach to ensure reproducibility by another examiner.
- List all tools used to arrive at their conclusions.

## Tools used:

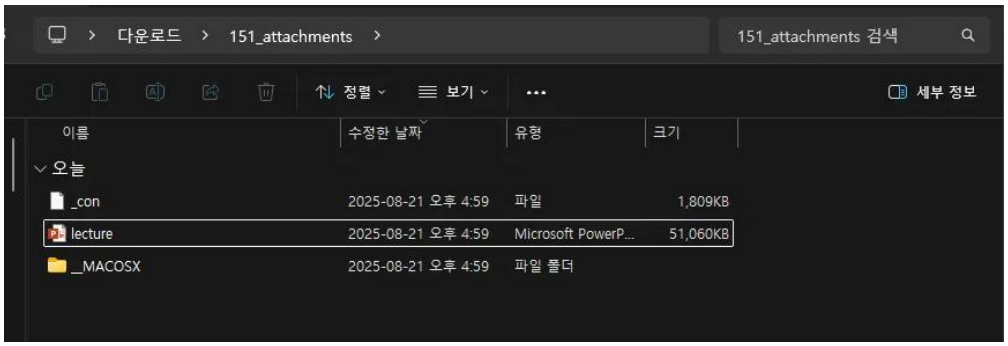
| | | | |
|---|---|---|---|
| Name: | 7-Zip | Publisher: | Igor Pavlov |
| Version: | 23.01 | | |
| URL: | https://www.7-zip.org/ | | |

| | | | |
|---|---|---|---|
| Name: | HxD Hex Editor | Publisher: | Maël Hörz |
| Version: | 2.5.0 | | |
| URL: | https://mh-nexus.de/en/hxd/ | | |

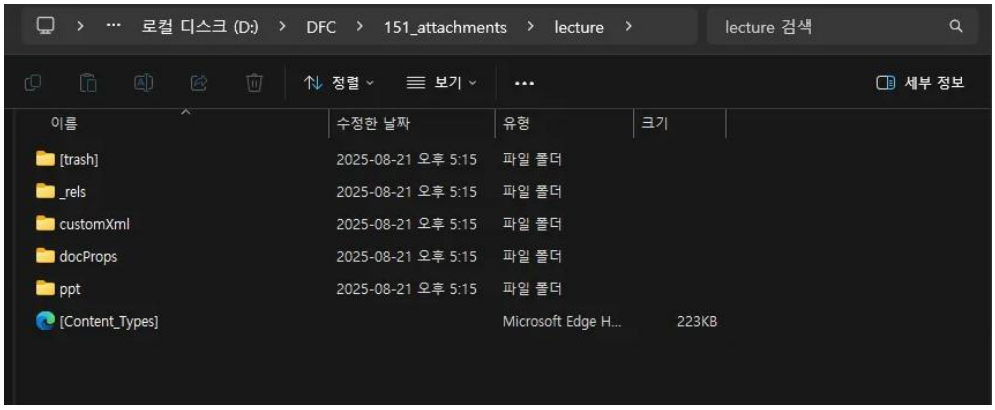
| | | | |
|---|---|---|---|
| Name: | oletools | Publisher: | Decalage |
| Version: | 0.60.2 | | |
| URL: | https://github.com/decalage2/oletools | | |

| | | | |
|---|---|---|---|
| Name: | TINA-TI | Publisher: | Texas Instruments |
| Version: | 9.3 | | |
| URL: | https://www.ti.com/tool/TINA-TI | | |

## Step-by-step methodology:

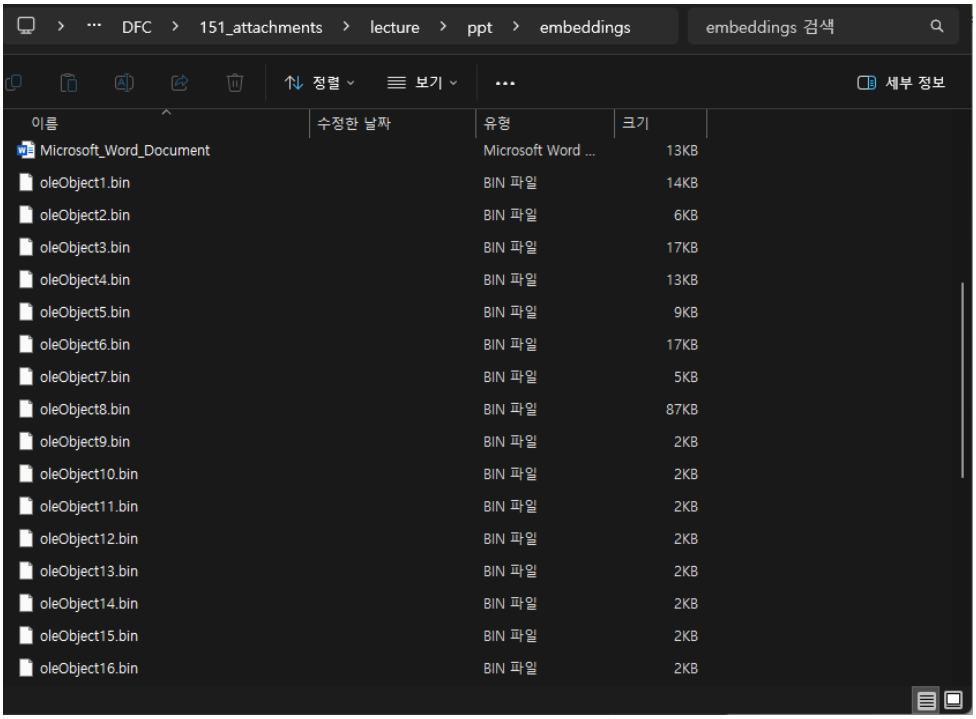



### 1) PPTX 내부 구조 분석




PPTX는 OOXML 구조이므로 압축을 해제하여 내부를 확인.

- 경로: ppt/embeddings/ 에서 OLE 객체(oleObject*.bin) 발견.



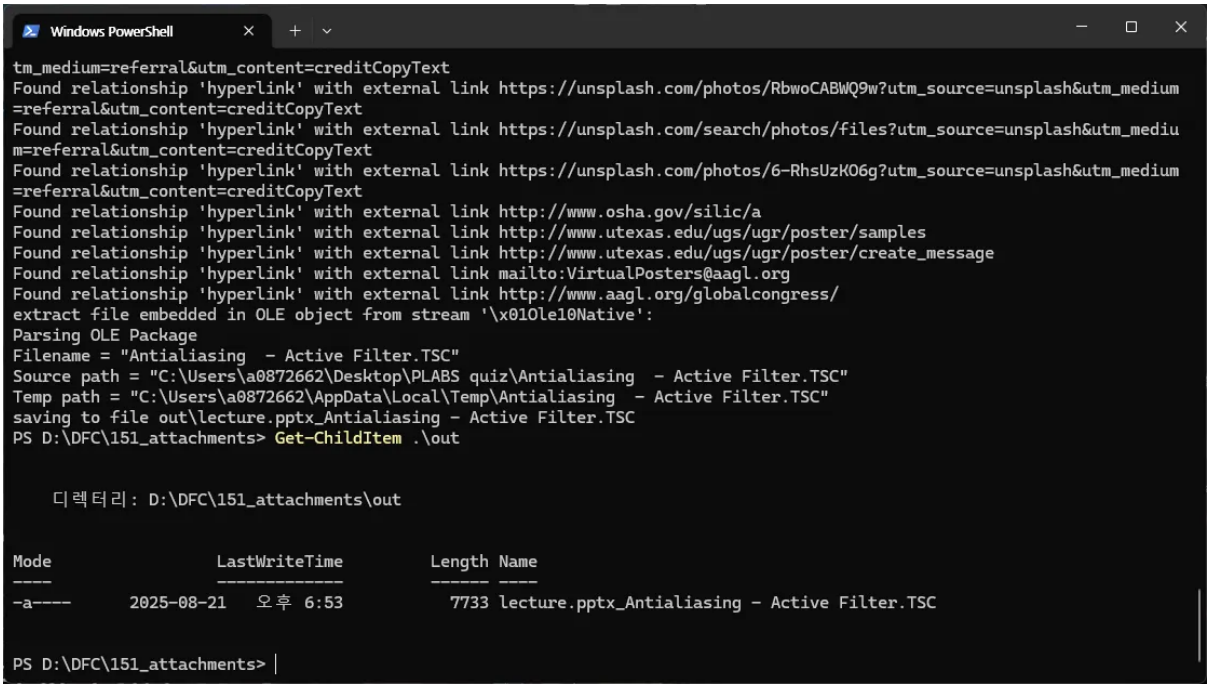

**2) 임베디드 파일 추출**

oletools 사용:

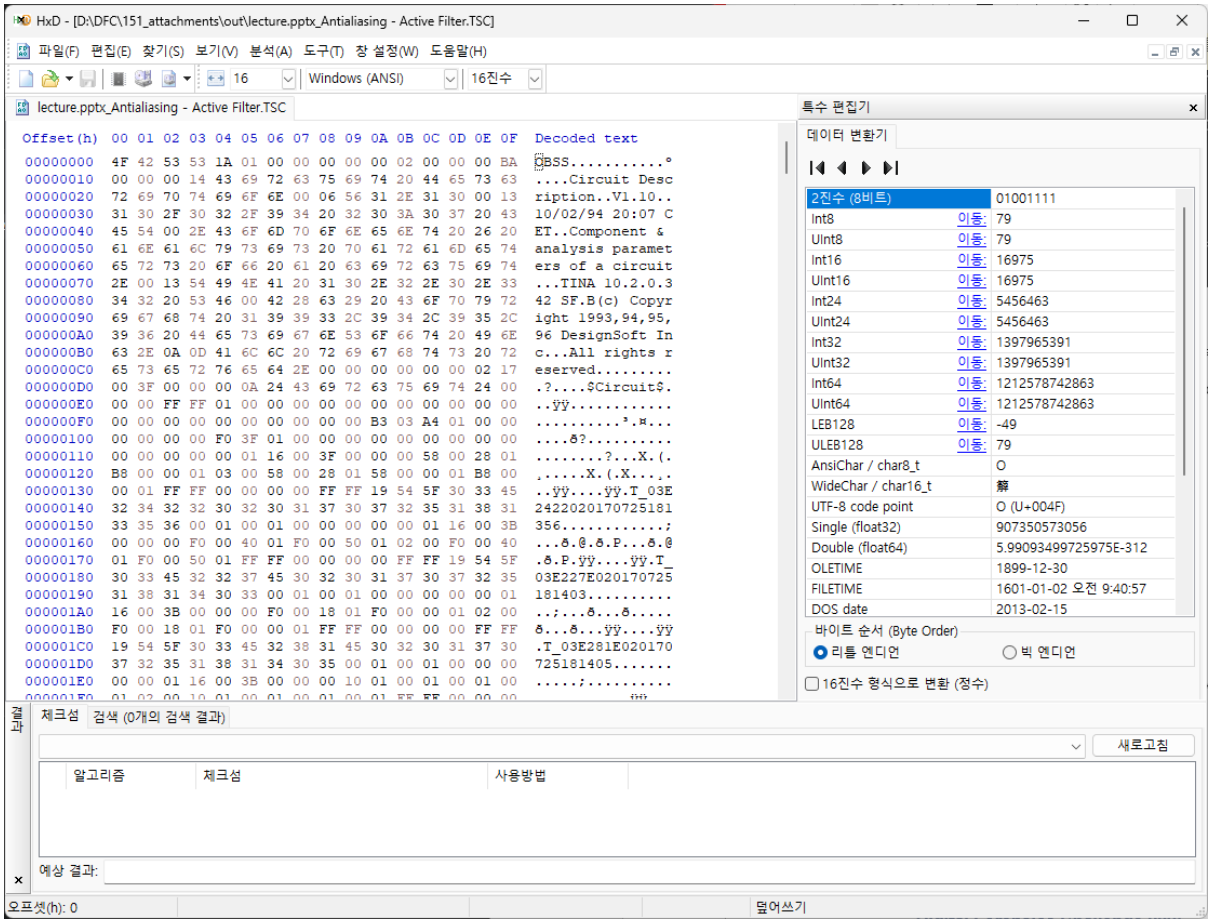
```
PS D:\DFC\151_attachments> python -m oletools.oleobj -d out lecture.pptx
oleobj 0.60.1 - http://decalage.info/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

-------------------------------------------------------------------------------
File: 'lecture.pptx'
Found relationship 'oleObject' with external link Workbook2
```

- 결과: lecture.pptx_Antialiasing - Active Filter.TSC 파일 추출.

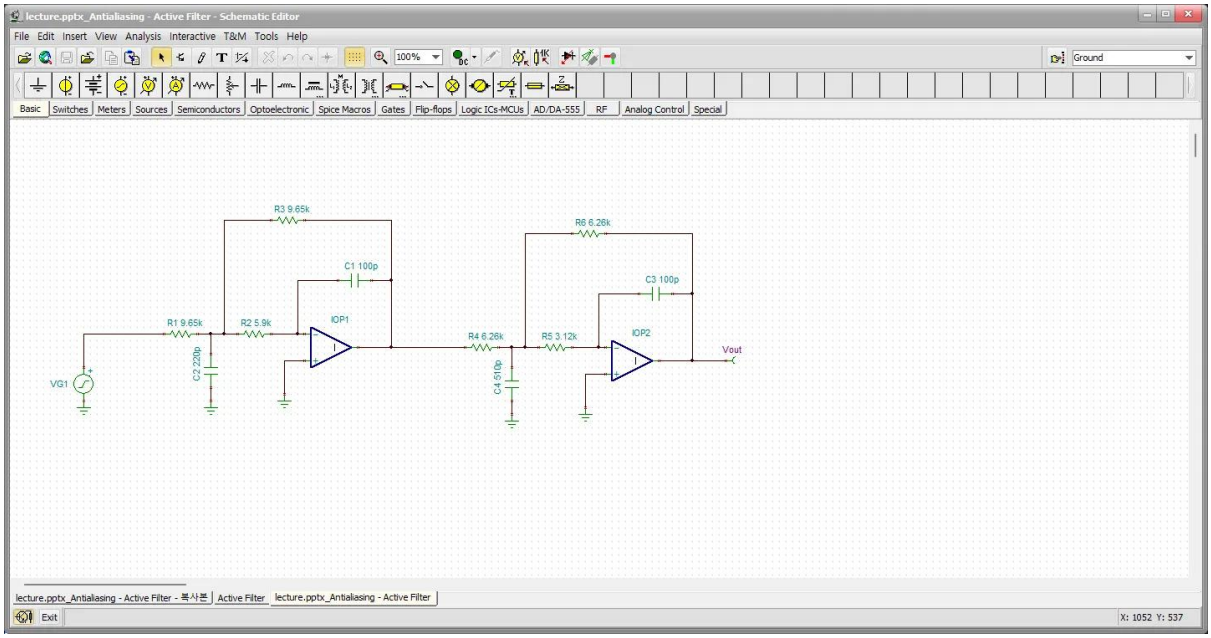



### 4) 추출 파일 분석




- Hex 및 strings로 확인: Circuit Description, TINA 10.2.0.342, R/C 부품 정의 등 존재.

- 해당 파일은 TINA 시뮬레이터에서 열리는 회로 스키매틱(.tsc)임이 확인됨.




### 5) 해시 계산

PowerShell에서 MD5 계산:

```
PS D:\DFC\151_attachments> CertUtil -hashfile '.\out\lecture.pptx_Antialiasing - Active Filter.TSC' md5
MD5의 .\out\lecture.pptx_Antialiasing - Active Filter.TSC 해시:
d71bbecc88b72bd869d841bb3bf60d7e
CertUtil: -hashfile 명령이 성공적으로 완료되었습니다.
PS D:\DFC\151_attachments>
```

- 해시값(MD5): d71bbecc88b72bd869d841bb3bf60d7e

### 결과

_con 파일은 낚시용 무의미한 데이터로 추측 (랜덤성, 시그니처 불일치). 실제 유출 대상은 PPTX 내부 임베디드 .tsc 파일. 해당 파일은 **전자 회로 설계도**이며, 기밀 자료에 해당.

- 유출 대상 파일: ActiveFilter_extracted.tsc
- 해시값(MD5): **d71bbecc88b72bd869d841bb3bf60d7e**