

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:

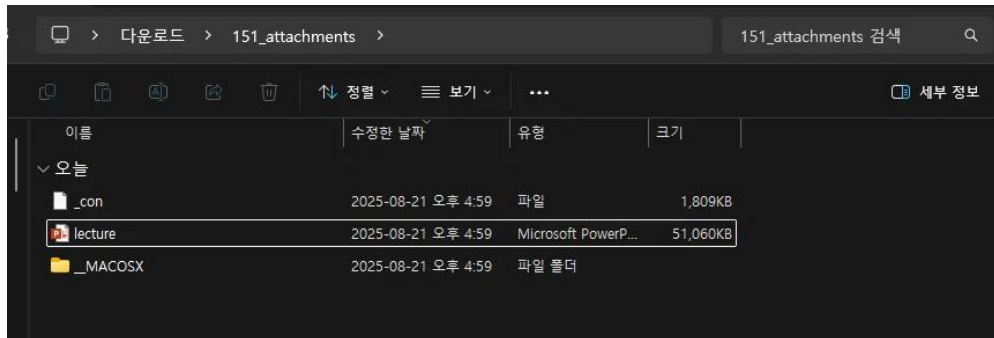
Name:	7-Zip	Publisher:	Igor Pavlov
Version:	23.01		
URL:	https://www.7-zip.org/		

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

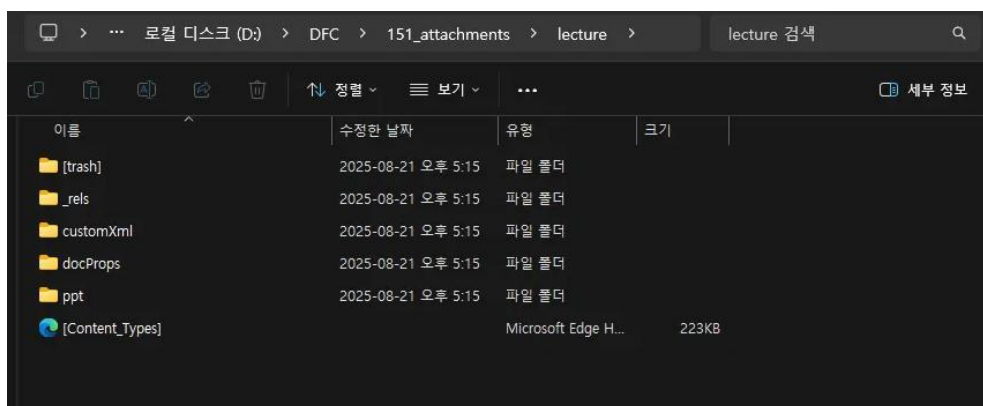
Name:	oletools	Publisher:	Decalage
Version:	0.60.2		
URL:	https://github.com/decalage2/oletools		

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.

DFC > 151_attachments > lecture > ppt > embeddings embeddings 검색

정렬 보기

이름	수정한 날짜	유형	크기
Microsoft_Word_Document		Microsoft Word ...	13KB
oleObject1.bin		BIN 파일	14KB
oleObject2.bin		BIN 파일	6KB
oleObject3.bin		BIN 파일	17KB
oleObject4.bin		BIN 파일	13KB
oleObject5.bin		BIN 파일	9KB
oleObject6.bin		BIN 파일	17KB
oleObject7.bin		BIN 파일	5KB
oleObject8.bin		BIN 파일	87KB
oleObject9.bin		BIN 파일	2KB
oleObject10.bin		BIN 파일	2KB
oleObject11.bin		BIN 파일	2KB
oleObject12.bin		BIN 파일	2KB
oleObject13.bin		BIN 파일	2KB
oleObject14.bin		BIN 파일	2KB
oleObject15.bin		BIN 파일	2KB
oleObject16.bin		BIN 파일	2KB

세부 정보

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.

```

tm_medium=referral&utm_content=creditCopyText
Found relationship 'hyperlink' with external link https://unsplash.com/photos/RbwoCABWQ9w?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText
Found relationship 'hyperlink' with external link https://unsplash.com/search/photos/files?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText
Found relationship 'hyperlink' with external link https://unsplash.com/photos/6-RhsUzK06g?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText
Found relationship 'hyperlink' with external link http://www.osha.gov/silic/a
Found relationship 'hyperlink' with external link http://www.utexas.edu/ugs/ugr/poster/samples
Found relationship 'hyperlink' with external link http://www.utexas.edu/ugs/ugr/poster/create_message
Found relationship 'hyperlink' with external link mailto:VirtualPosters@aagl.org
Found relationship 'hyperlink' with external link http://www.aagl.org/globalcongress/
extract file embedded in OLE object from stream '\x0101e10Native':
Parsing OLE Package
Filename = "Antialiasing - Active Filter.TSC"
Source path = "C:\Users\A0872662\Desktop\PLABS quiz\Antialiasing - Active Filter.TSC"
Temp path = "C:\Users\A0872662\AppData\Local\Temp\Antialiasing - Active Filter.TSC"
saving to file out\lecture.pptx_Antialiasing - Active Filter.TSC
PS D:\DFC\151_attachments> Get-ChildItem .\out

디렉터리: D:\DFC\151_attachments\out

Mode                LastWriteTime         Length Name
----                -
-a-----         2025-08-21 오후 6:53           7733 lecture.pptx_Antialiasing - Active Filter.TSC

PS D:\DFC\151_attachments>

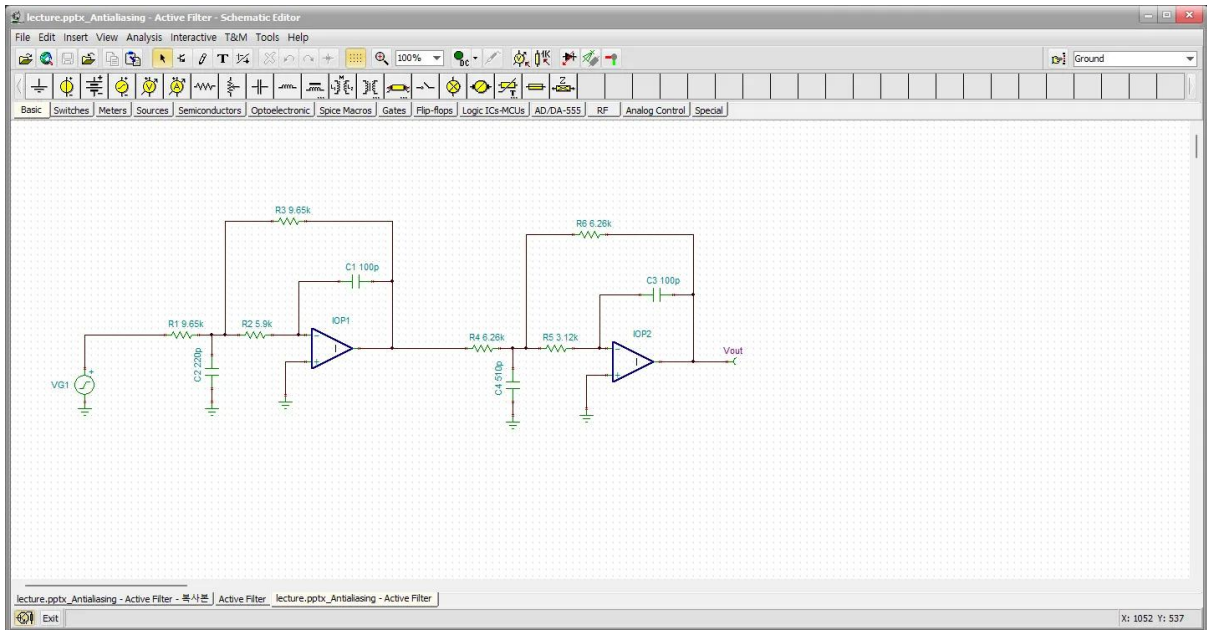
```

4) 추출 파일 분석

Hex editor (HxD) showing the extracted file 'lecture.pptx_Antialiasing - Active Filter.TSC'. The hex view displays the file's content, including a BSS section. The right pane shows a list of memory addresses and their corresponding values, including Int8, UInt8, Int16, UInt16, Int24, UInt24, Int32, UInt32, Int64, UInt64, LEB128, and ULEB128. The bottom pane shows a search results table with columns for address, value, and usage.

- 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 설계도이며, 기밀 자료에 해당.

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