JumpList Template

S.C.P 이유경, 장혜선

2022-02-17

CONTENTS

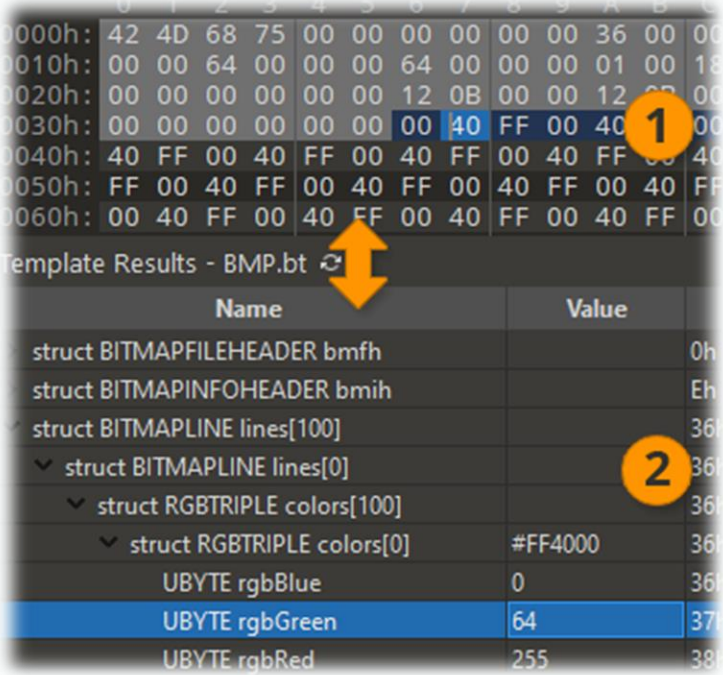
01 프로젝트 개요

[1] 소개

010 Editor

검찰, 경찰 등 국가 주요 기관에서 높은 인지도를 가진 도구
Text/Hex/Disk/Process 데이터를 편집하고 분석할 수 있게 해준다.

HxD와 유사하지만, 010 Editor는 템플릿 기능이 존재하기 때문에 포맷 구조를 손쉽게 파악하여 분석 시간을 단축할 수 있다.
현재 010 Editor는 JumpList의 템플릿을 갖고 있지 않아, 이를 개발하고자 한다



01 프로젝트 개요

[2] 역할 분담

- 이유경

구조 분석

Destlist File Structure

- 장혜선

구조 분석

OLE File Structure

LNK File Structure

01 프로젝트 개요

3 기대 효과

아티팩트 활용도

포렌식 및 침해사고 대응 관점에서 JumpList의 활용도를 파악할 수 있다.

분석 실력 향상

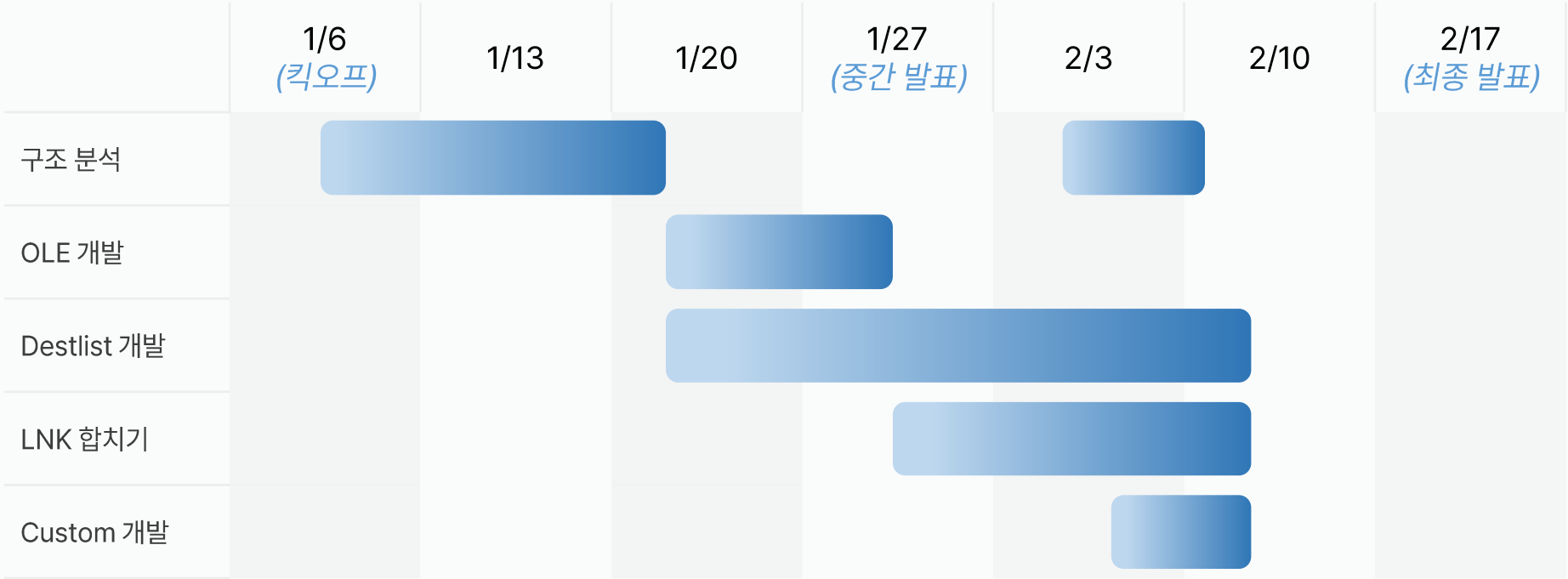
아티팩트의 구조 분석 실력과 개발 기술을 향상시킬 수 있다.

JumpList 분석 시간 단축

템플릿을 이용하면 JumpList 아티팩트 분석 시간이 단축된다.

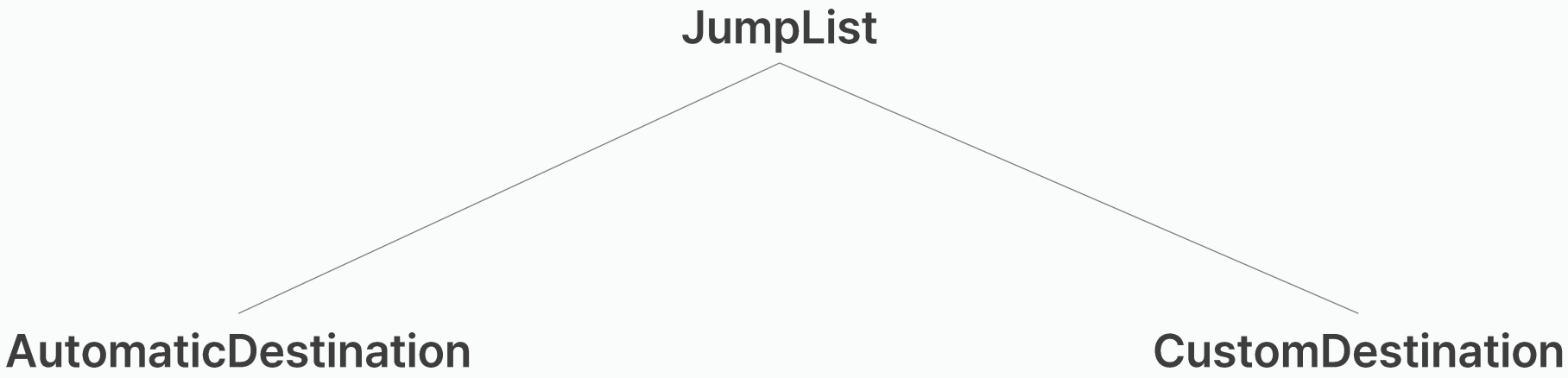
02 프로젝트 수행 과정

1 수행 절차



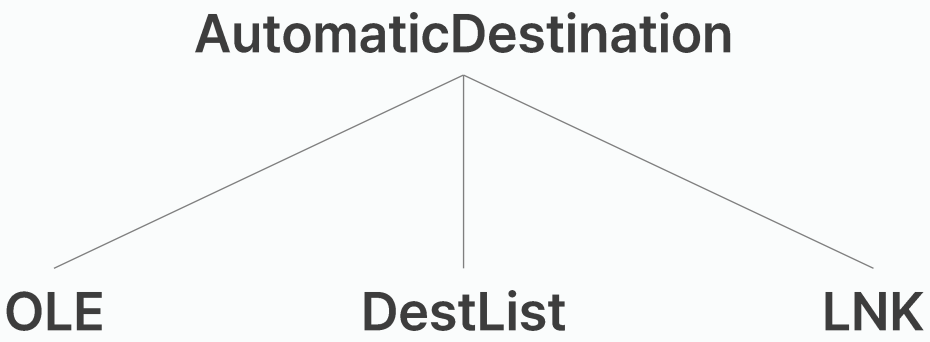
02 프로젝트 수행 과정

[2] 분석



02 프로젝트 수행 과정

[2] 분석



OLE File Structure
LNK File Structure
00 00 00 ···
Destlist File Structure
LNK File Structure
LNK File Structure
...
LNK File Structure

Offset 800

02 프로젝트 수행 과정

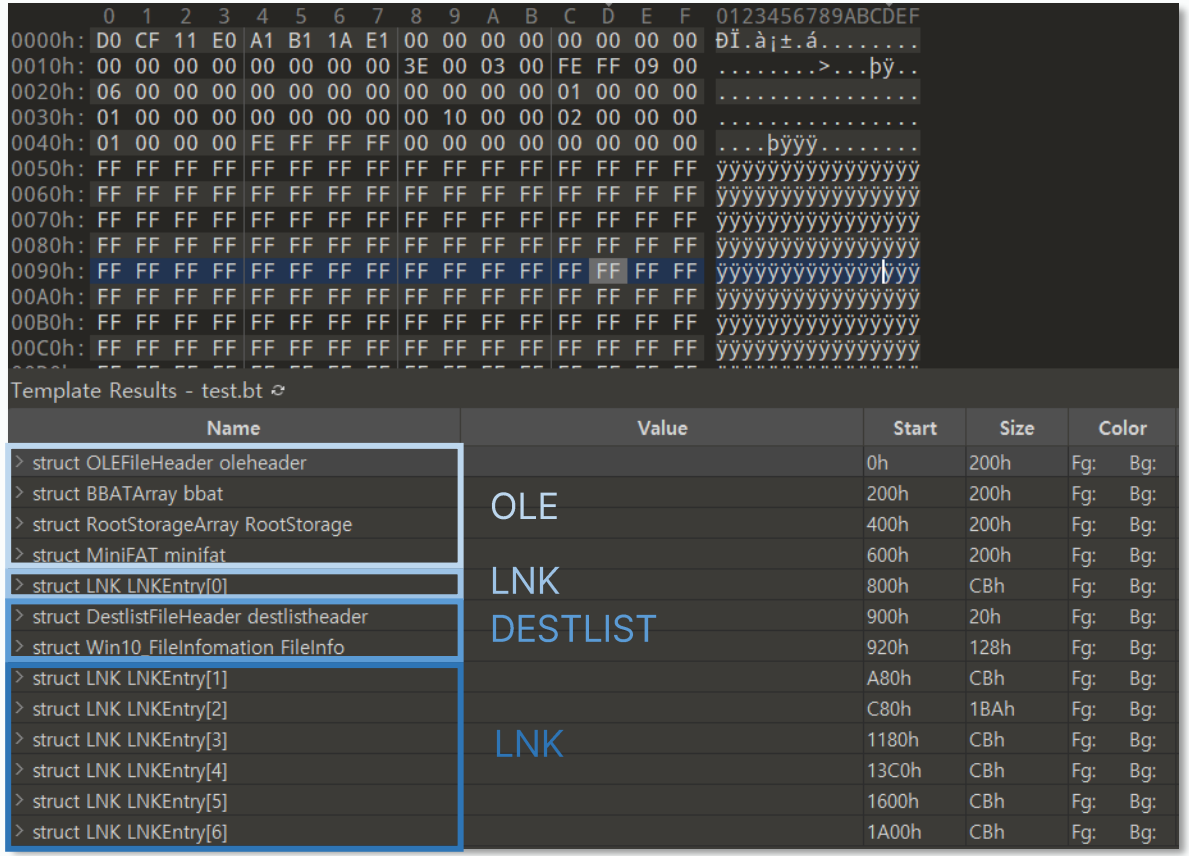
[2] 분석

Unknown Header
LNK File Structure
LNK File Structure
...
LNK File Structure
...
LNK File Structure

02 프로젝트 수행 과정

3 결과물

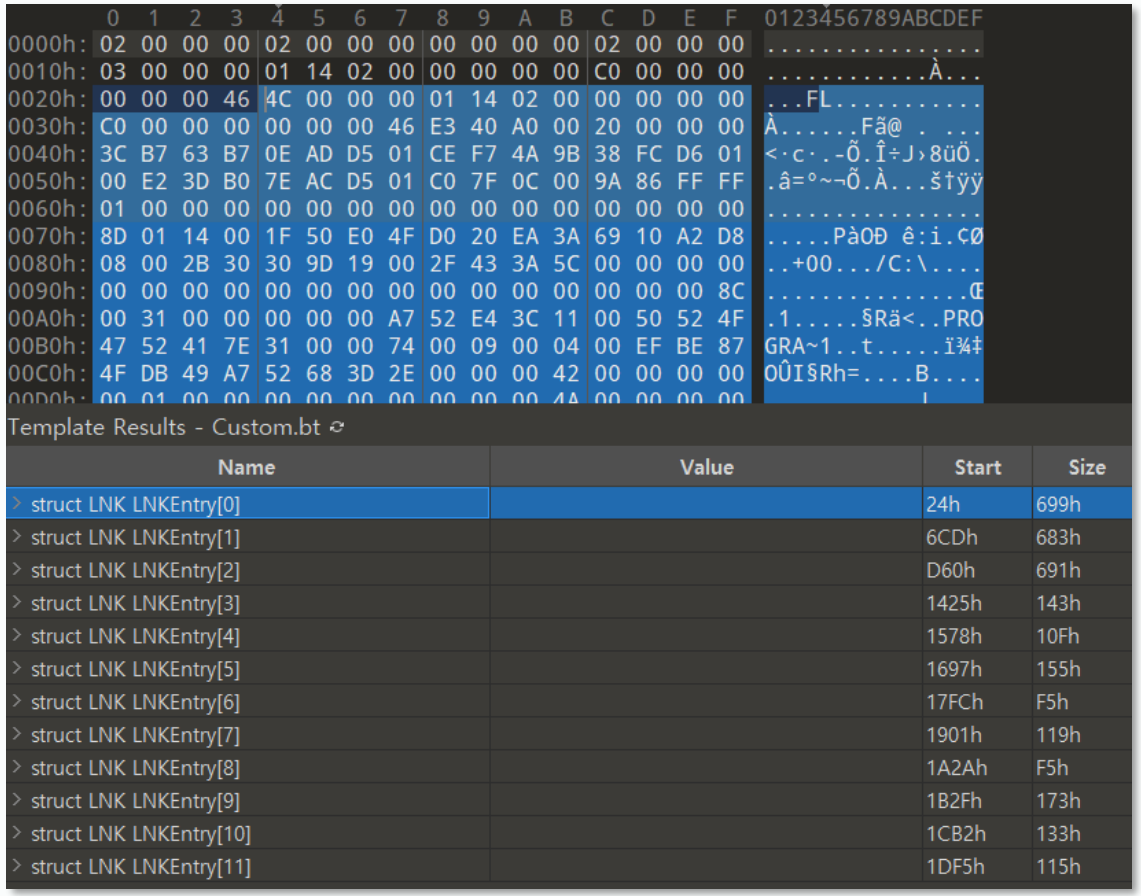
- automatic



02 프로젝트 수행 과정

3 결과물

- custom



03 향후 계획

010 Editor 공식 템플릿 등록

Jumplist 논문

END

010 EDITOR

Question