

# JumpList Template

S.C.P 이유경, 장혜선

2022-02-17



# CONTENTS

## 01 프로젝트 개요

- <sup>1</sup> 소개
- <sup>2</sup> 역할 분담
- <sup>3</sup> 기대효과

## 02 프로젝트 수행 과정

- <sup>1</sup> 수행 절차
- <sup>2</sup> 분석
- <sup>3</sup> 결과물

## 03 향후 계획





# 01 프로젝트 개요

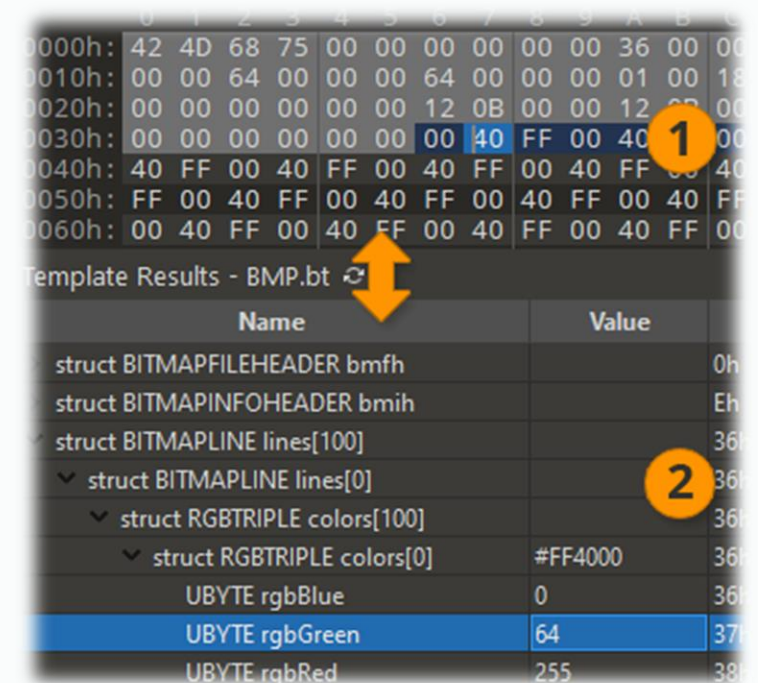
## 1 소개

### 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

<sup>2</sup> 역할 분담

- 이유경

구조 분석

Destlist File Structure

- 장혜선

구조 분석

OLE File Structure

LNK File Structure



# 01 프로젝트 개요

## <sup>3</sup> 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.



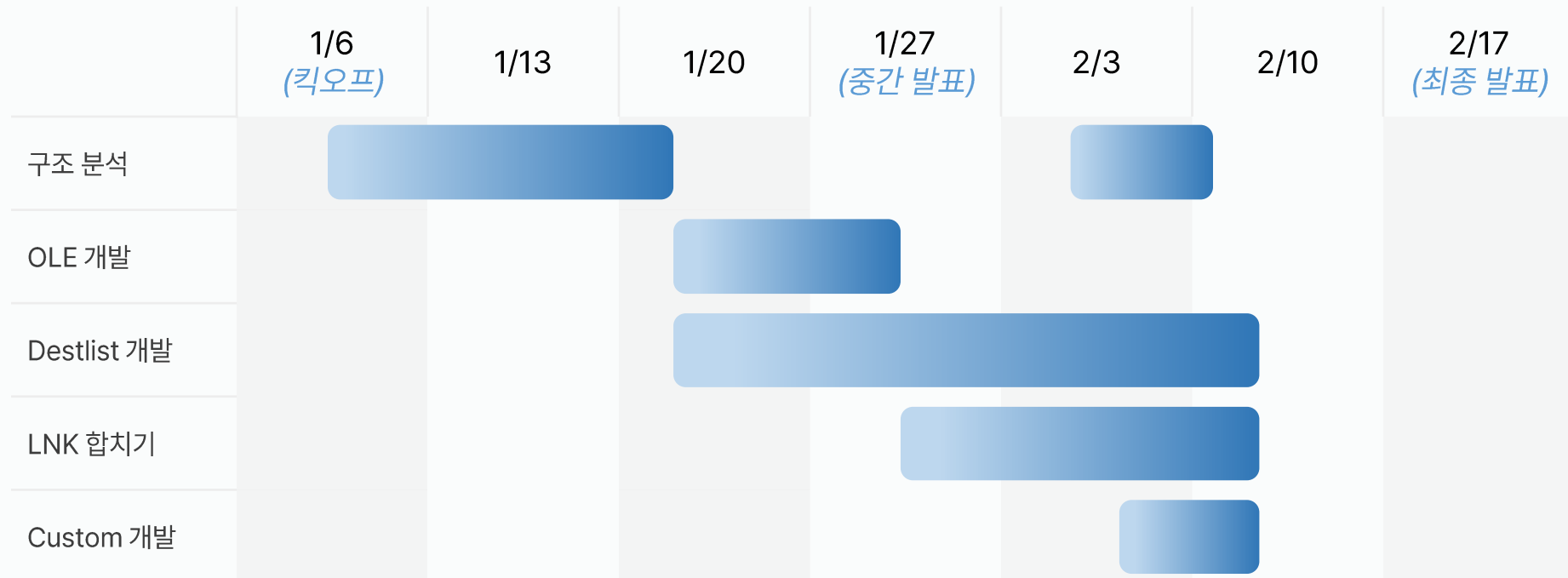
### JumpList 분석 시간 단축

템플릿을 이용하면 JumpList 아티팩트 분석 시간이 단축된다.



# 02 프로젝트 수행 과정

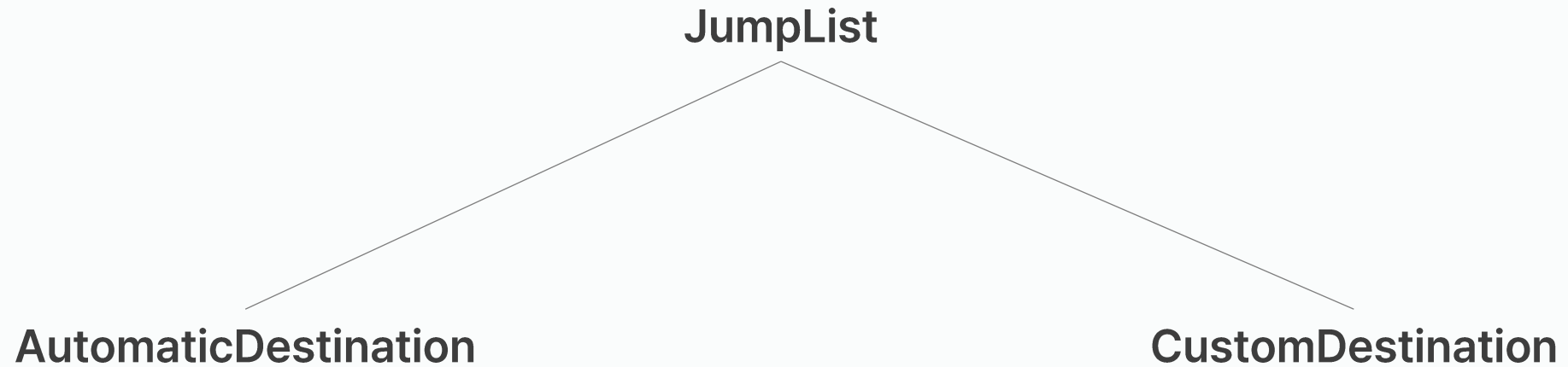
## 1 수행 절차





# 02 프로젝트 수행 과정

<sup>2</sup> 분석





# 02 프로젝트 수행 과정

<sup>2</sup> 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

<sup>2</sup> 분석



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



# 02 프로젝트 수행 과정

## 3 결과물

- automatic

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	D0	CF	11	E0	A1	B1	1A	E1	00	00	00	00	00	00	00	00	01.à±.á.....
0010h:	00	00	00	00	00	00	00	00	3E	00	03	00	FE	FF	09	00	.....>...bÿ..
0020h:	06	00	00	00	00	00	00	00	00	00	00	00	01	00	00	00	.....
0030h:	01	00	00	00	00	00	00	00	00	10	00	00	02	00	00	00	.....
0040h:	01	00	00	00	FE	FF	FF	FF	00	00	00	00	00	00	00	00	...bÿÿ.....
0050h:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy
0060h:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy
0070h:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy
0080h:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy
0090h:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy
00A0h:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy
00B0h:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy
00C0h:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy

Template Results - test.bt ↻

Name	Value	Start	Size	Color
> struct OLEFileHeader oleheader	OLE	0h	200h	Fg: Bg:
> struct BBATArray bbat		200h	200h	Fg: Bg:
> struct RootStorageArray RootStorage		400h	200h	Fg: Bg:
> struct MiniFAT minifat		600h	200h	Fg: Bg:
> struct LNK LNKEntry[0]	LNK	800h	CBh	Fg: Bg:
> struct DestlistFileHeader destlistheader		900h	20h	Fg: Bg:
> struct Win10_FileInfomation FileInfo	DESTLIST	920h	128h	Fg: Bg:
> struct LNK LNKEntry[1]		A80h	CBh	Fg: Bg:
> struct LNK LNKEntry[2]	LNK	C80h	1BAh	Fg: Bg:
> struct LNK LNKEntry[3]		1180h	CBh	Fg: Bg:
> struct LNK LNKEntry[4]		13C0h	CBh	Fg: Bg:
> struct LNK LNKEntry[5]		1600h	CBh	Fg: Bg:
> struct LNK LNKEntry[6]		1A00h	CBh	Fg: Bg:



# 02 프로젝트 수행 과정

## 3 결과물

- custom

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	02	00	00	00	02	00	00	00	00	00	00	00	02	00	00	00	.....
0010h:	03	00	00	00	01	14	02	00	00	00	00	00	C0	00	00	00	.....Ä...
0020h:	00	00	00	46	4C	00	00	00	01	14	02	00	00	00	00	00	...FL.....
0030h:	C0	00	00	00	00	00	00	46	E3	40	A0	00	20	00	00	00	Ä.....Fä@ . . .
0040h:	3C	B7	63	B7	0E	AD	D5	01	CE	F7	4A	9B	38	FC	D6	01	<·c·.-Ö.Î÷J,8üÖ.
0050h:	00	E2	3D	B0	7E	AC	D5	01	C0	7F	0C	00	9A	86	FF	FF	.â=°~-Ö.Ä...štÿÿ
0060h:	01	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0070h:	8D	01	14	00	1F	50	E0	4F	D0	20	EA	3A	69	10	A2	D8	.....Pà0Ð ê:i.çØ
0080h:	08	00	2B	30	30	9D	19	00	2F	43	3A	5C	00	00	00	00	..+00.../C:\....
0090h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	8C	.....Ë
00A0h:	00	31	00	00	00	00	00	A7	52	E4	3C	11	00	50	52	4F	.1.....šRä<..PRO
00B0h:	47	52	41	7E	31	00	00	74	00	09	00	04	00	EF	BE	87	GRA~1..t.....i¼‡
00C0h:	4F	DB	49	A7	52	68	3D	2E	00	00	00	42	00	00	00	00	00IšRh=...B....
00D0h:	00	01	00	00	00	00	00	00	00	00	00	4A	00	00	00	00	.....I

Template Results - Custom.bt ↗

Name	Value	Start	Size
> struct LNK LNKEntry[0]		24h	699h
> struct LNK LNKEntry[1]		6CDh	683h
> struct LNK LNKEntry[2]		D60h	691h
> struct LNK LNKEntry[3]		1425h	143h
> struct LNK LNKEntry[4]		1578h	10Fh
> struct LNK LNKEntry[5]		1697h	155h
> struct LNK LNKEntry[6]		17FCh	F5h
> struct LNK LNKEntry[7]		1901h	119h
> struct LNK LNKEntry[8]		1A2Ah	F5h
> struct LNK LNKEntry[9]		1B2Fh	173h
> struct LNK LNKEntry[10]		1CB2h	133h
> struct LNK LNKEntry[11]		1DF5h	115h



# 03 향후 계획

010 Editor 공식 템플릿 등록

JumpList 논문



**END**

**010 EDITOR**

0110 EDITOR

**Question**

0110 EDITOR