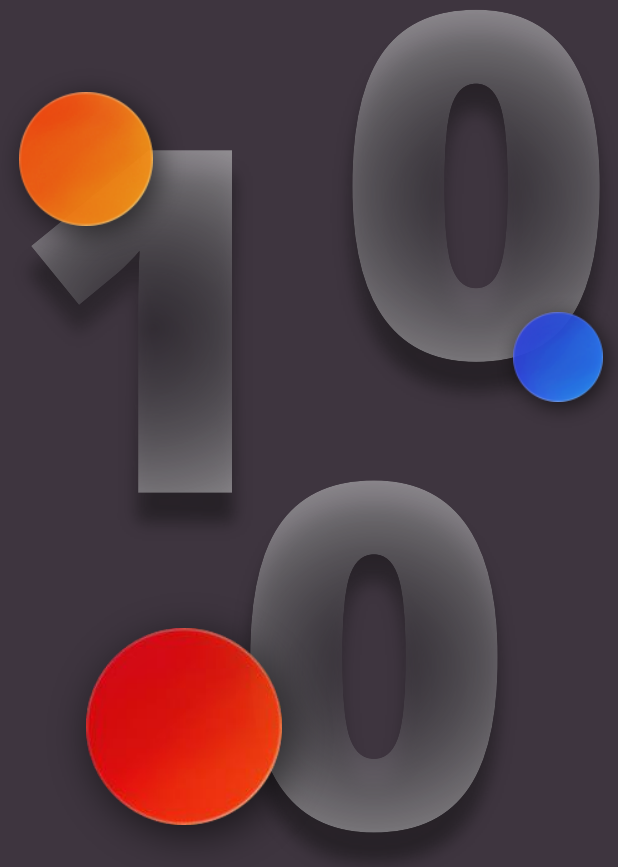
JumpList Template

S.C.P 이유경, 장혜선

2022-01-27

CONTENTS



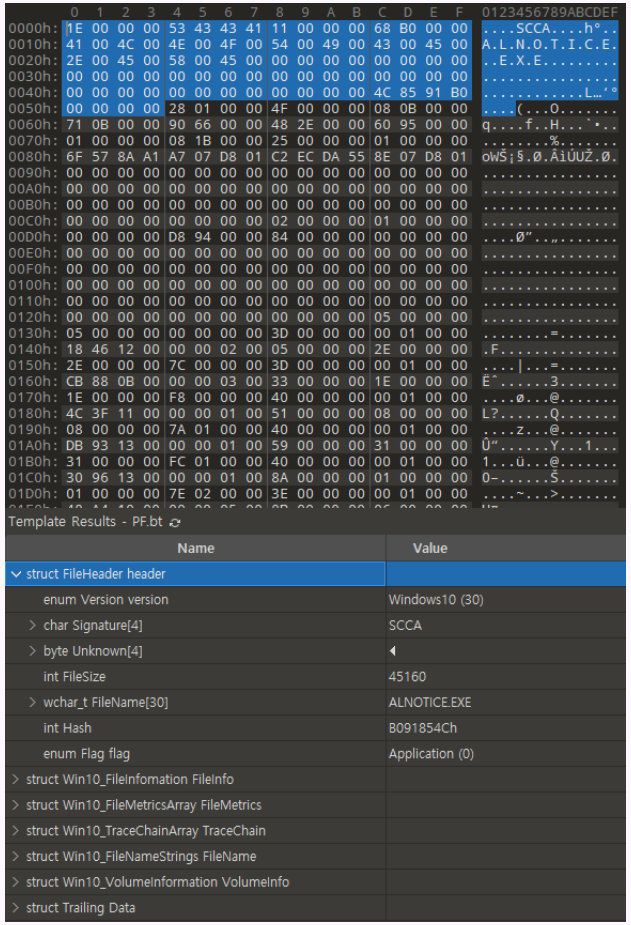
프로젝트 개요

e.g., Prefetch(PF.bt)

[그림 4 - Win 7의 프리패치 파일 구조 offset]

[그림 5 - Win XP의 프리패치 파일 구조 offset]

출처: https://maj3sty.tistory.com/857 [maj3sty]



프로젝트 수행 과정

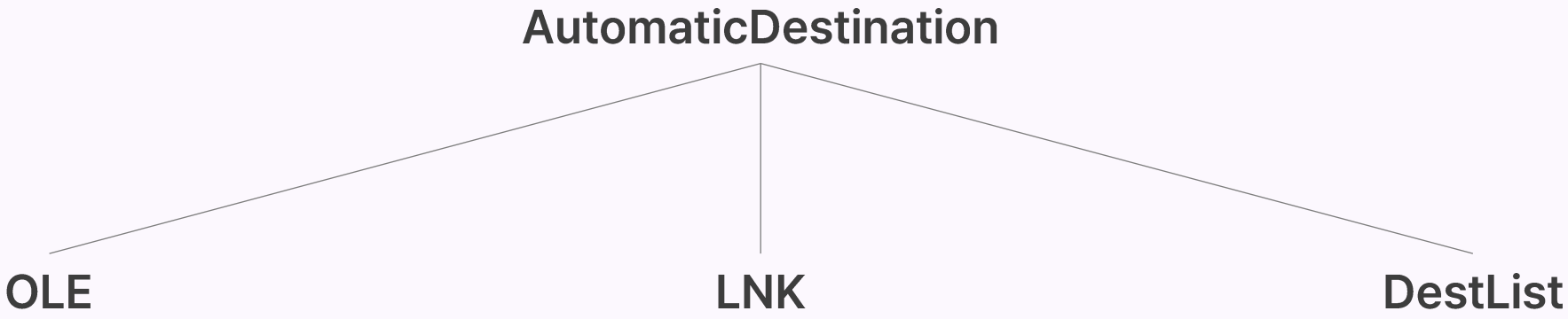
1 분석

AutomaticDestination

CustomDestination

프로젝트 수행 과정

1 분석



프로젝트 수행 과정

1 분석

OLE

- 헤더, Data 영역
- 헤더
  - File Signature, Sector Count, Sector Size, Start Sector ID
- 데이터 영역
  - Storage, stream
  - 테이블 정보

LNK

- ShellLinkHeader
  - 식별 정보, 시간 정보, 대상 파일 크기, 대상 파일 특성 등
- LinkTargetIDList
  - 링크 대상에 대한 정보
- LinkInfo
  - 링크 대상을 분석하기 위해 필요한 데이터
- String Data
  - 사용자 인터페이스 경로의 식별 정보 전달
- Extra Data

DestList

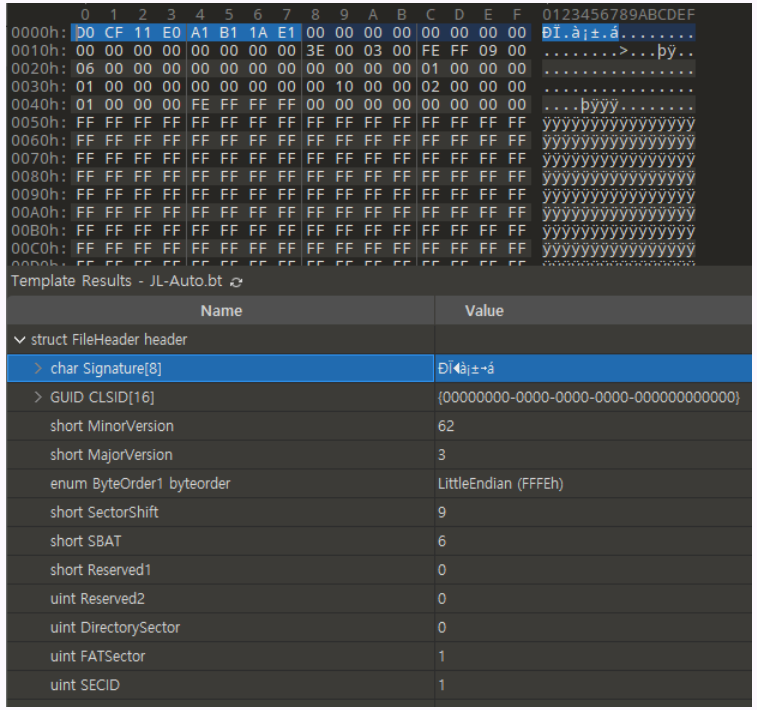
- 점프리스트 파일에 대한 간략한 정보 포함
  - Checksum
  - 마지막 수정 시간 등
- 파일 헤더와 스트림으로 구성

Size	Description	Windows 7/8	Windows 10
4	Version	value 1	value 4
4	Total number of current Entries		
4	Total number of poinned Entries		
4		Floating point value, some kind of counter	Unkown value
8	Last issue Entry ID number		
8		Number of add/delete actions	Number of add/delete/re-open actions

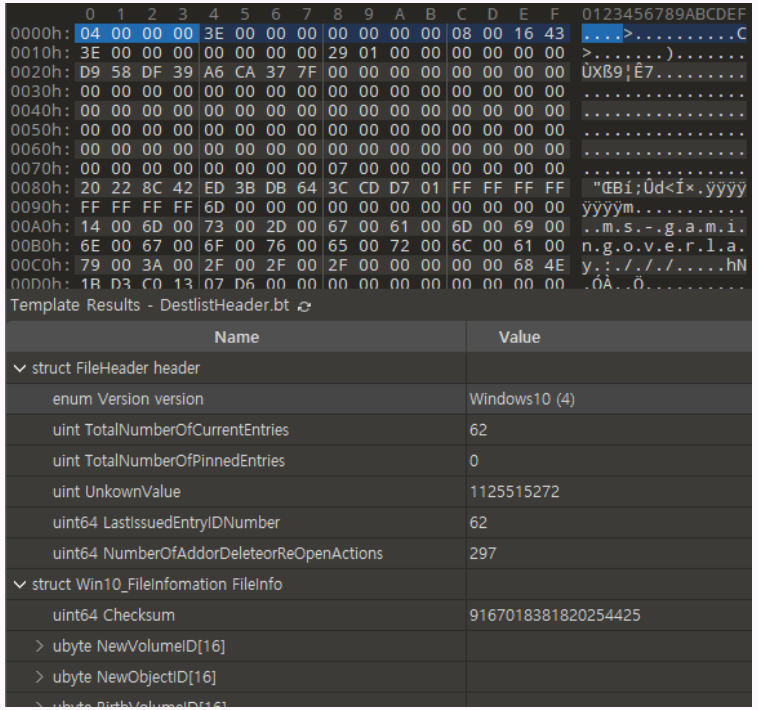
프로젝트 수행 과정

2 템플릿

OLE

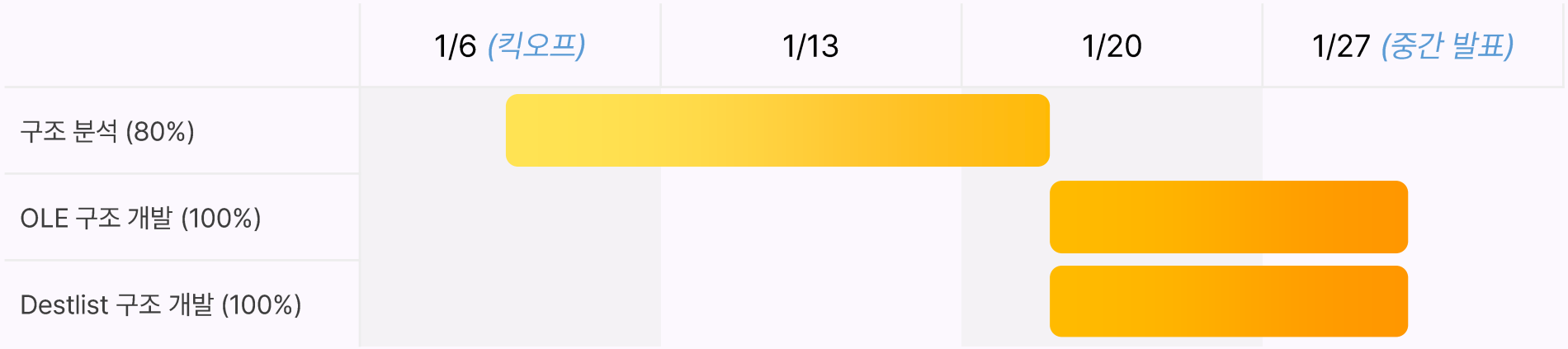


DestList



프로젝트 수행 과정

3 개발 진행 정도



향후 계획

Destlist 위치 찾기

LNK 반복하기

END

010 EDITOR

Question