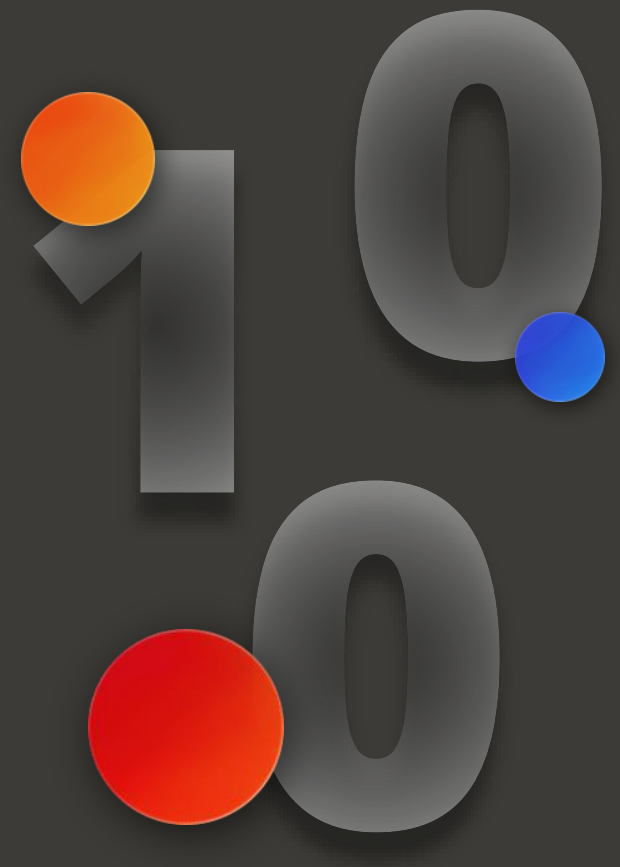
JumpList Template

S.C.P 이유경, 장혜선

2022-01-06

CONTENTS



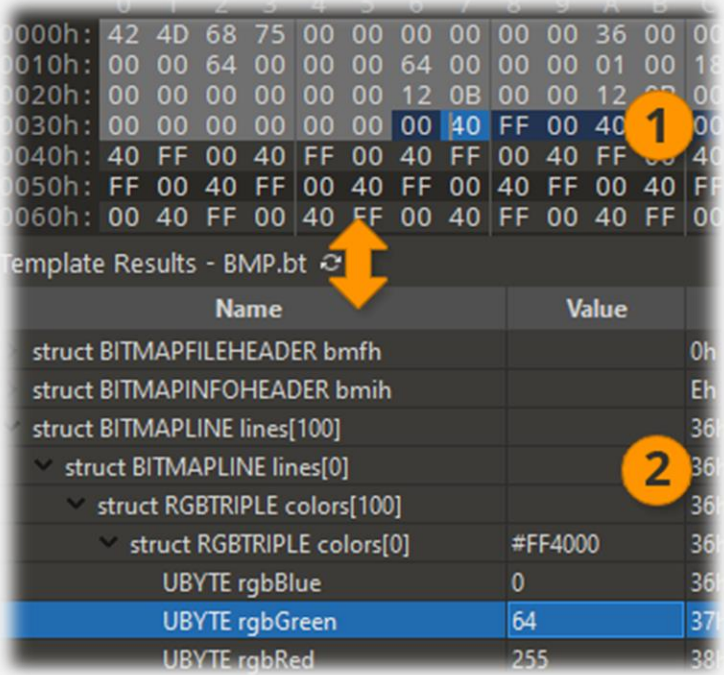
프로젝트 소개

01 프로젝트 개요

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.



프로젝트 소개

01 프로젝트 개요

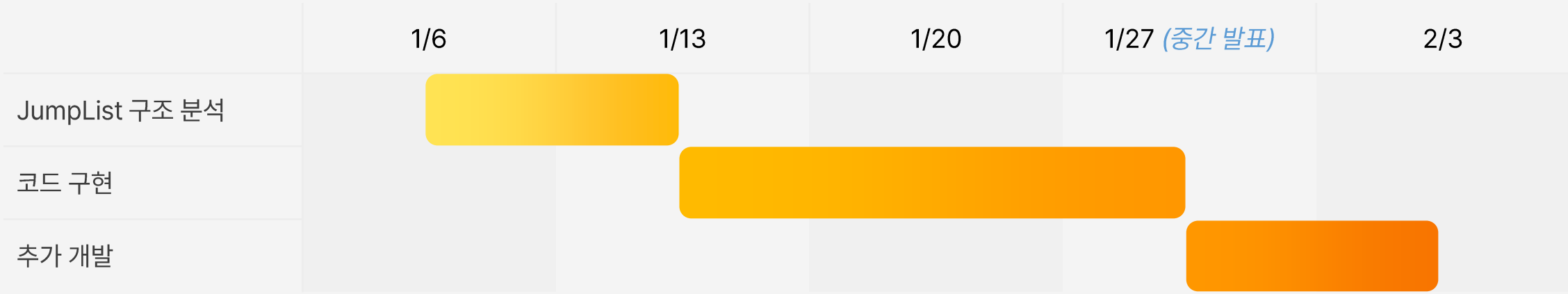
JumpList

최근 실행한 파일에 대한 링크 및 정보를 응용프로그램별로 그룹화하여 관리하는 아티팩트

포렌식 관점에서 보면 사용자가 일부로 삭제하지 않는 이상, 관련 로그를 계속 저장한다는 점에서 중요한 아티팩트가 된다.
운영체제 설치 시부터 지속적으로 저장되어,사용자의 행위를 파악 및 정보 유출 사건 분석에 도움이 된다.

프로젝트 일정

01 프로젝트 개요



역할 분담

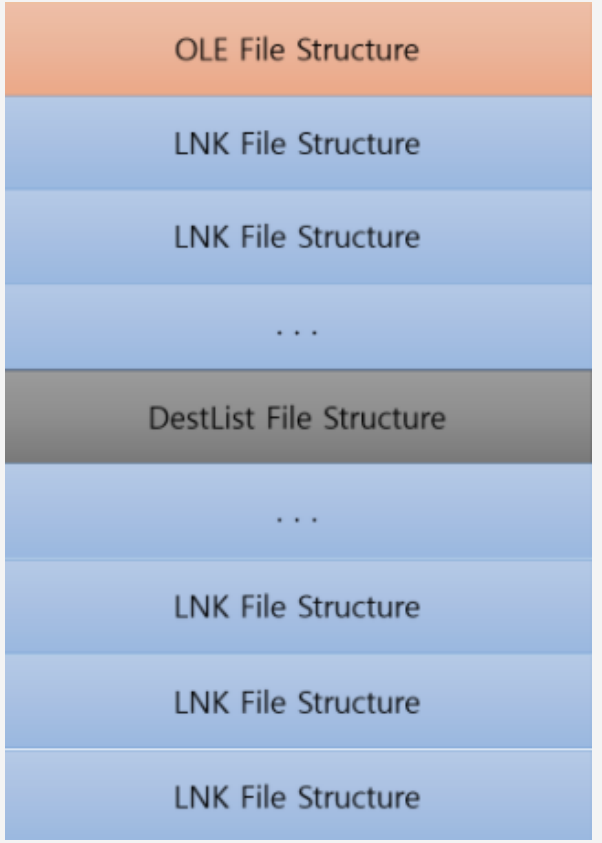
01 프로젝트 개요

이유경

- 분석 및 구현
  - OLE File Structure
  - LNK File Structure

장혜선

- 분석 및 구현
  - OLE File Structure
  - DestList File Structure



기대 효과

02 프로젝트 목표

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

템플릿이 제공됨으로써 JumpList 아티팩트를 분석하는 시간이 단축된다.

공식 템플릿 등록

010 Editor에서 해당 템플릿을 승인한다면 공식 템플릿으로 사용할 수 있다.

최종 목표

02 프로젝트 목표

JumpList Template Development

1. JumpList 구조 분석

2. JumpList 아티팩트 구조에 맞는 코드 구현

3. 010 Editor Template 등록

END

010 EDITOR

Question