Jump List

01.13 장혜선

목차

첫번째 JumpList

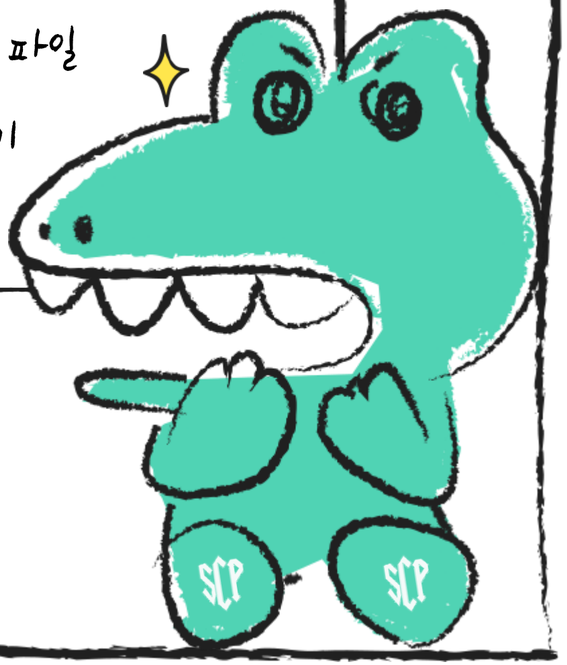
두번째 Auto/Custom

1. Jump List

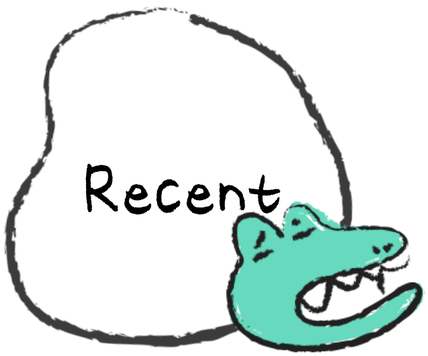
- ✓ 최근 실행한 응용 프로그램 및 링크 정보를 응용 프로그램별로 관리하는 아티팩트
- ✓ Windows 7 version 부터 도입
- ✓ 사용자 편의성을 향상
- ✓ 기본 활성화

이전.

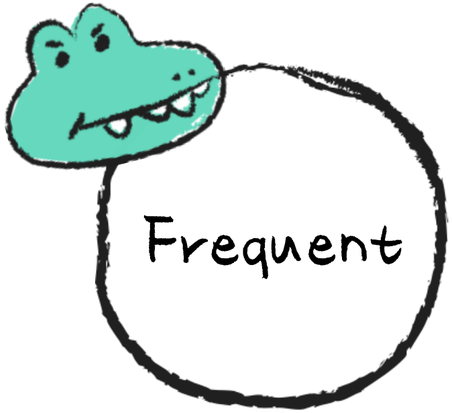
- ✓ 관리
  - "Recent"에 링크 파일
  - "UserAssist" 키



1. Jump List - 종류

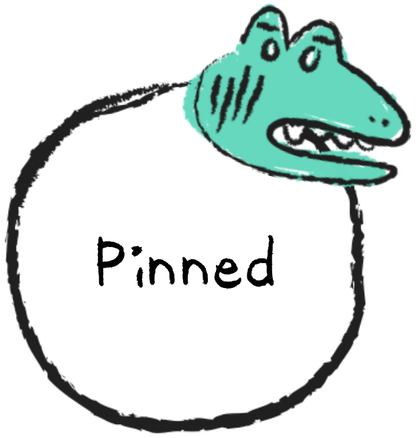


사용자가 **최근** 접근한
파일이나 폴더



사용자가 **자주** 접근한
파일이나 폴더

응용 프로그램에서
지원하는 **작업**



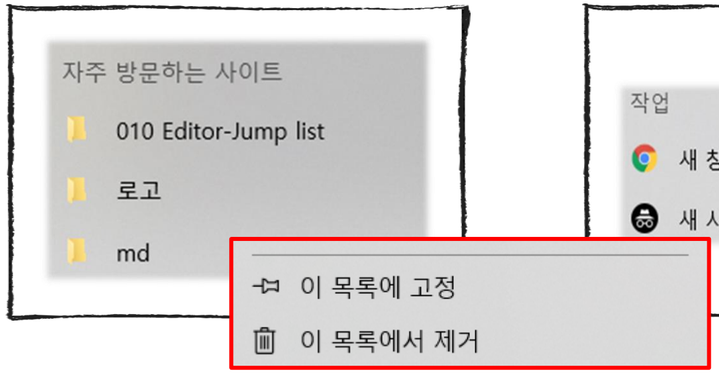
사용자가 **고정**시킨
작업 목록

1. Jump List - 종류

작업표시줄에 있는 응용프로그램 우클릭

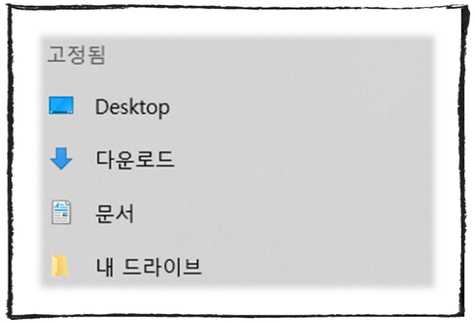
✓ Recent

✓ Frequent



✓ Task

✓ Pinned



1. Jump List - 중요 이유

✓ Recent 폴더, UserAssist 키보다 더 많은 정보를 포함

✓ 사용자가 직접 삭제하지 않는 이상 운영체제 설치부터 누적해서 로그 저장

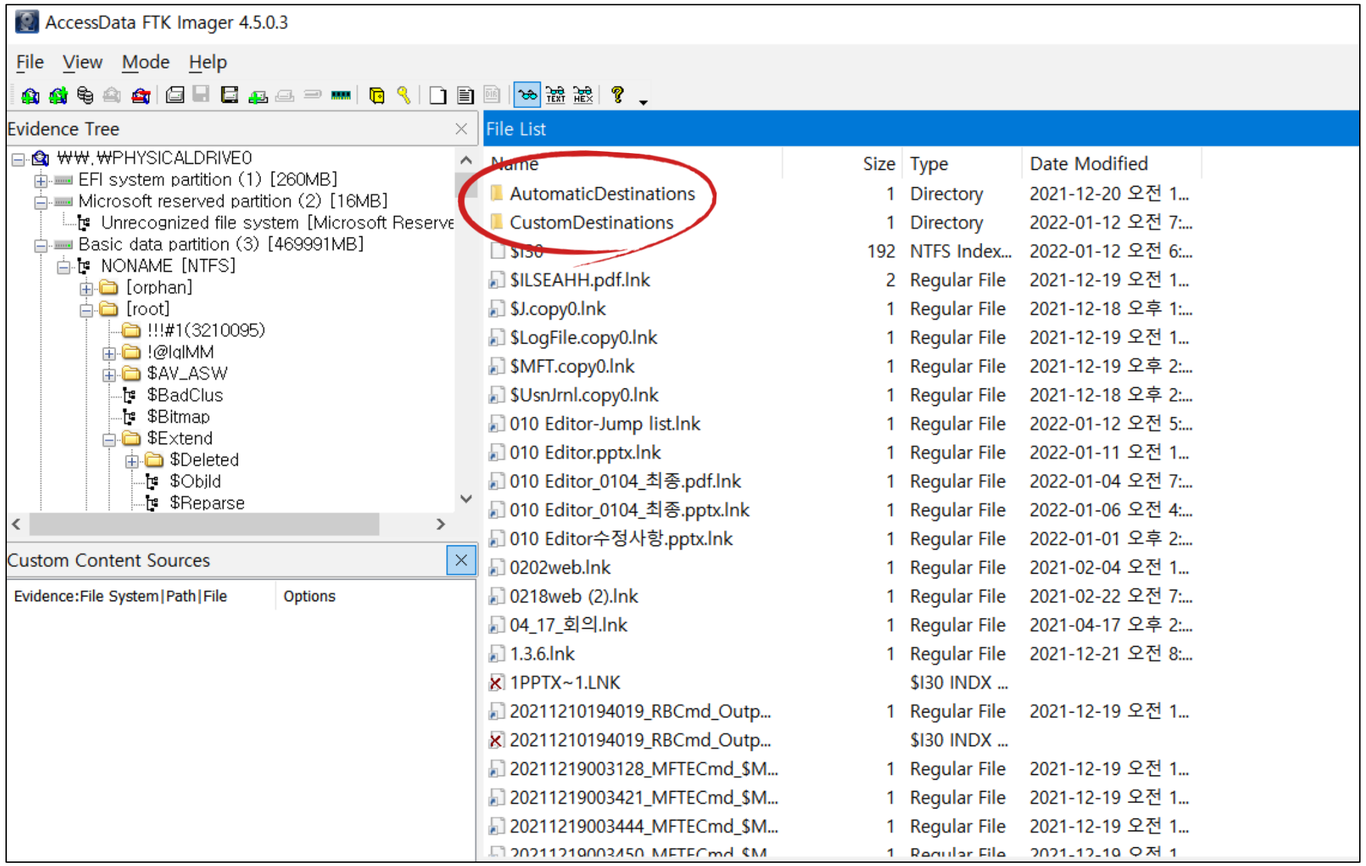
✓ 사용자의 컴퓨터 사용 습관 파악 가능

✓ 사용자와 컴퓨터의 상호작용을 확인 할 수 있는 아티팩트

✓ 사용자의 행위를 파악/추적 가능해 정보 유출 사건 분석에 큰 역할을 함

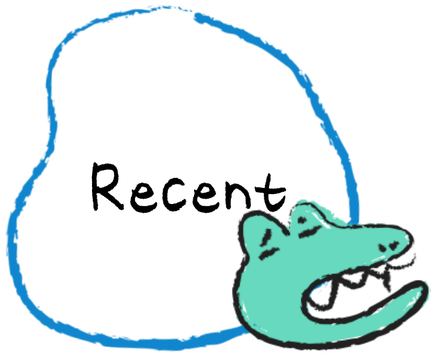
1. Jump List - 혁EH

C:₩Users₩[username]₩AppData₩Roaming₩Microsoft₩Windows₩Recent

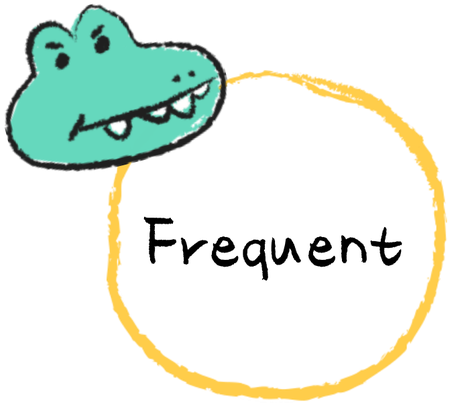


2. Auto/Custom

Automatic
Custom

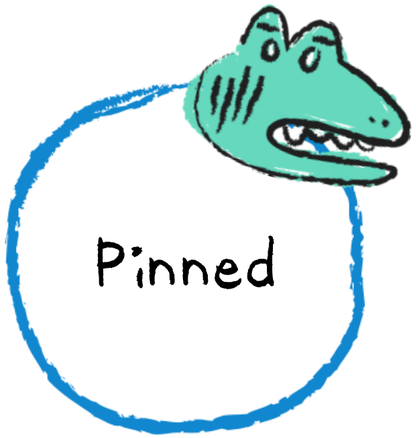


사용자가 **최근** 접근한
파일이나 폴더



사용자가 **자주** 접근한
파일이나 폴더

응용 프로그램에서
지원하는 **작업**

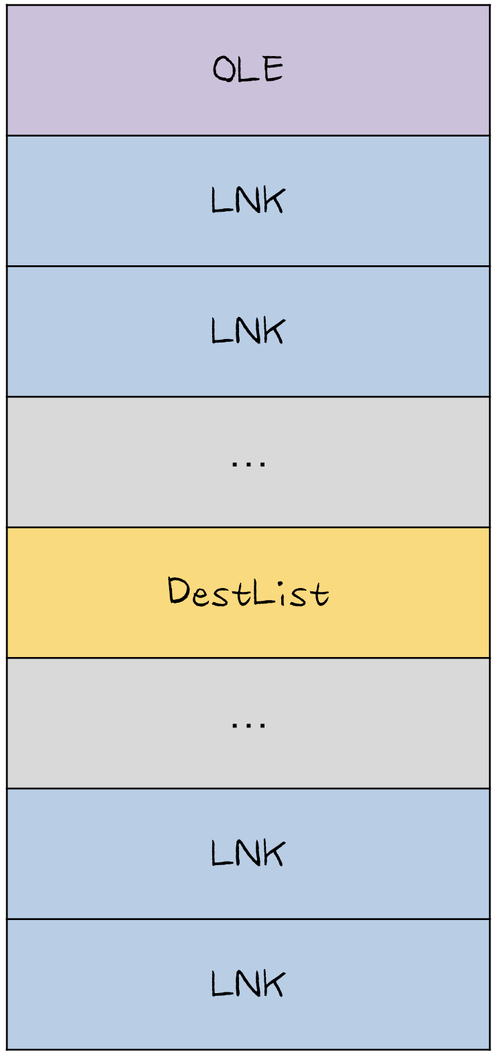


사용자가 **고정**시킨
작업 목록

2. Auto/Custom - Auto

- 사용자가 파일이나 응용 프로그램으로 작업 수행 시 운영체제가 **자동**으로 생성
- OLE 구조
- N개의 LNK
- 1개의 DestList -> 여러 LNK의 간략한 정보 저장

AutomaticDestinations



2. Auto/Custom - Auto

DestList Stream 구조가 깨져 있을 시 확인하는 방법은?

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	f
00	Check Sum								New Volume ID							
10	New Volume ID								Birth Volume ID							
20	Birth Volume ID								Object ID 1							
30	Object ID 2								Machine ID							
40	Machine ID								Entry ID				File Access Count			
50	Last Record Time								Pin				Unicode String Length		Unicode String	
60	Unicode String															
70																

존재 여부

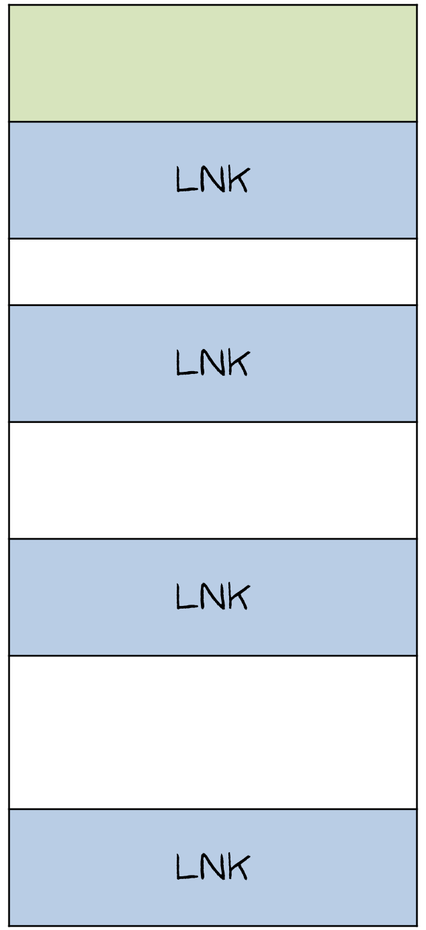
항상 0xffffffff

DestList Stream

2. Auto/Custom - Custom

- 사용자가 파일이나 응용 프로그램을 **자주** 사용할 때 발생
- 알려지지 않은 헤더 뒤에 LNK 구조 나열
- 불규칙적이고 연속적임
- LNK 파일 추출 가능

CustomDestinations

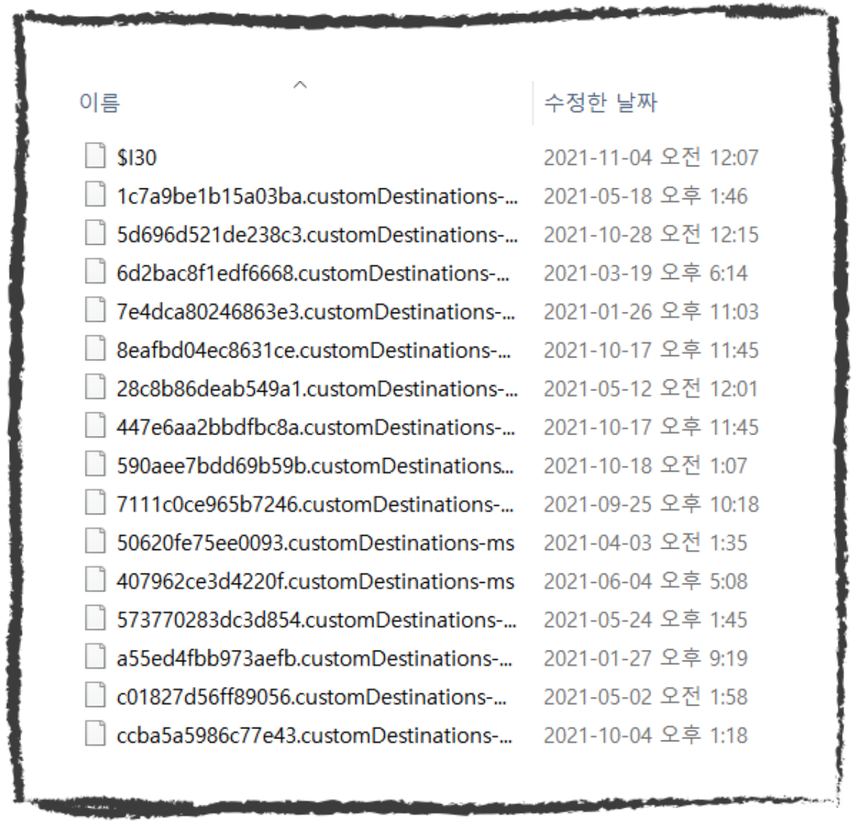


2. Auto/Custom - AppID

✓ 파일명 = APPID ✓ 자동 생성됨

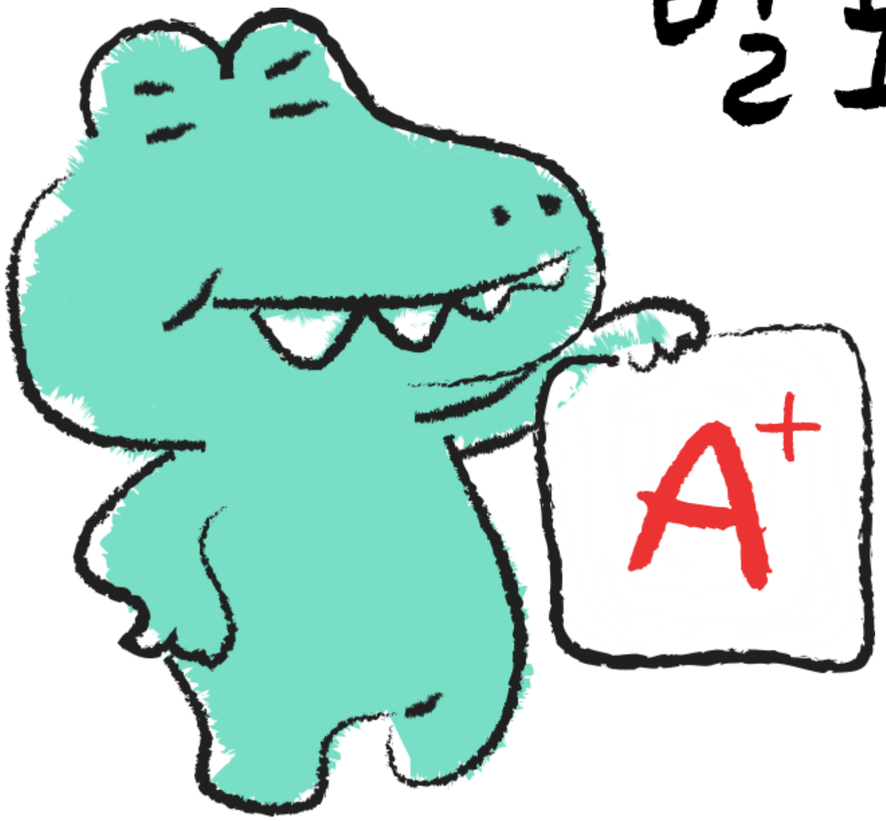
이름	수정한 날짜
$I30	2021-10-28 오전 12:02
1bc392b8e104a00e.automaticDestinatio...	2021-08-18 오전 11:14
1c7a9be1b15a03ba.automaticDestinatio...	2021-05-18 오후 1:46
2c9c22f1faf51072.automaticDestinations...	2021-06-13 오후 10:56
2fea857555875784.automaticDestinatio...	2021-10-28 오전 12:01
3c355482cb54f75b.automaticDestinatio...	2021-01-30 오후 3:52
3ea974195bc3c05d.automaticDestinatio...	2021-06-13 오후 10:58
5b1060ea9c2933ba.automaticDestinatio...	2021-10-17 오후 11:42
5bb830f67194431a.automaticDestinatio...	2021-09-17 오전 1:32
5c5e4638f6459826.automaticDestination...	2021-04-02 오후 11:58
5cc37aeaf0dc09a4.automaticDestination...	2021-05-16 오후 11:45
6d2bac8f1edf6668.automaticDestination...	2021-04-23 오후 8:04
6df4f6af495e5535.automaticDestination...	2021-05-12 오전 12:18
7b99ab6c3d3b551d.automaticDestinatio...	2021-05-24 오후 3:34
7c75dd02f00fdef7.automaticDestination...	2021-06-13 오후 10:58
7e4dca80246863e3.automaticDestinatio...	2021-10-08 오전 1:42

AutomaticDestinations



이름	수정한 날짜
$I30	2021-11-04 오전 12:07
1c7a9be1b15a03ba.customDestinations-...	2021-05-18 오후 1:46
5d696d521de238c3.customDestinations-...	2021-10-28 오전 12:15
6d2bac8f1edf6668.customDestinations-...	2021-03-19 오후 6:14
7e4dca80246863e3.customDestinations-...	2021-01-26 오후 11:03
8eafbd04ec8631ce.customDestinations-...	2021-10-17 오후 11:45
28c8b86deab549a1.customDestinations-...	2021-05-12 오전 12:01
447e6aa2bbdfbc8a.customDestinations-...	2021-10-17 오후 11:45
590aee7bdd69b59b.customDestinations...	2021-10-18 오전 1:07
7111c0ce965b7246.customDestinations-...	2021-09-25 오후 10:18
50620fe75ee0093.customDestinations-ms	2021-04-03 오전 1:35
407962ce3d4220f.customDestinations-ms	2021-06-04 오후 5:08
573770283dc3d854.customDestinations-...	2021-05-24 오후 1:45
a55ed4fbb973aefb.customDestinations-...	2021-01-27 오후 9:19
c01827d56ff89056.customDestinations-...	2021-05-02 오전 1:58
ccba5a5986c77e43.customDestinations-...	2021-10-04 오후 1:18

CustomDestinations



발표를 들어주셔서 감사합니다

Ref. 1 2