

JumpList

made by 임승연

INDEX

1. 개요

2. 구조

3. 분석 방법

1 개요

JumpList

- Windows 7에서 새롭게 추가된 아티팩트
- 응용프로그램별로 그룹화
- 사용자가 자주 사용하거나 최근 사용한 문서 또는 프로그램을 관리하는 링크 파일

디지털 포렌식적 관점

- 문서, 프로그램 실행 유무 판단
- 자주 사용하는 문서, 프로그램 정보 확인
- 최근에 사용한 문서, 프로그램 정보 확인
- 사용자의 행위 파악
- 정보 유출 사건 분석
- 사용자가 최근에 열람, 수정, 생성한 파일에 대한 정보를 얻을 수 있음

1 개요

JumpList 유형 및 생성 규칙

- Windows 10과 11 기준, 기본적으로 활성화 되어 있음
- [개인 설정] - [시작] 에서 비활성화 설정 가능
- Recent [최근 항목]
 - 응용프로그램을 통해 최근 열람한 파일
 - 직접 확인할 수 있는 점프 목록의 개수는 Default값 기준 최대 10개
- Frequent [자주 사용하는/방문하는 항목]
 - 응용프로그램을 통해 자주 열람하는 파일
 - 시스템이 사용자가 주로 사용한다고 판단
 - '최종 실행/수정 시각', '프로그램 실행 횟수', '실행 시간' 과 같은 변수 활용
- Tasks [작업 항목]
 - 특정 프로그램에 대해서 수행할 수 있는 동작을 미리 지정
 - 경우에 따라 미디어 재생, 새 문서 작성 등의 기능을 빠르게 이용하기 위한 파일
 - 예시) 새 창 열기, 이전 창 복원하기 등의 기능을 Tasks라고 함
- Pinned [고정됨]
 - 사용자가 직접 고정한 항목
 - 응용 프로그램의 사용이 종료되어도 작업 표시줄에 응용프로그램의 아이콘을 남겨두기 위한 기능

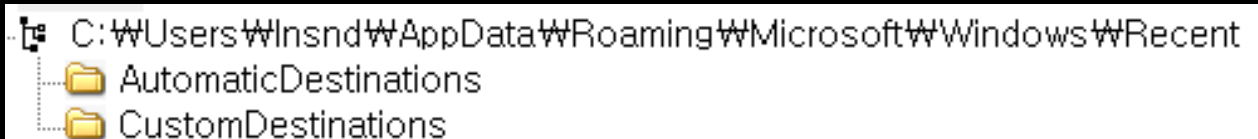
1 개요

JumpList 경로

- Recent 디렉토리의 하위 경로에 위치
- 사용자가 특정 작업 수행 시, OS 또는 애플리케이션에 의해 [UserProfile] 내에 생성
- AutomaticDestinations 하위 디렉토리
 - AutoDestinations-ms (autoDest) 파일 존재
- CustomDestinations 하위 디렉토리
 - CustomDestinations-ms (custDest) 파일 존재

JumpList의 전체 경로

- AutoDest
 - %UserProfile%AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
- CustDest
 - %UserProfile%AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations
- 위의 두 가지 파일들은 숨겨진 파일로, Windows 탐색기를 사용하여 디렉토리 구조를 클릭해도 파일들을 확인할 수 없음
- FTK Imager를 통해 확인 가능



C:\Users\Wnsnd\AppData\Roaming\Microsoft\Windows\Recent

- AutomaticDestinations
- CustomDestinations

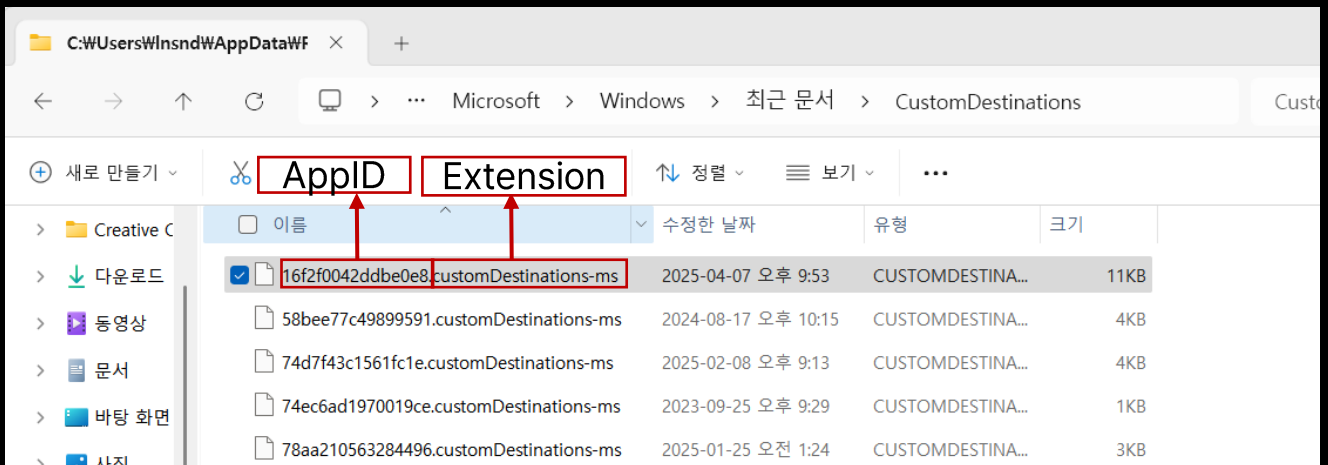
1 개요

JumpList 저장 경로

- AutomaticDestinations
 - 최근 사용한 목록(Recent)이나 자주 사용되는 목록(Frequent)
- CustomDestinations
 - 작업(Task) 목록

JumpList 구조

- App ID
 - 파일명 : 고유한 16자리 사용
- Extension



Properties	
AppId	16f2f0042ddbe0e8
AppId description	Windows Terminal
Entries count	1

2 구조

AutomaticDestinations

- .automaticDestinations-ms 확장자를 가짐
- 파일 이름
 - Hex값
 - 16바이트
 - 시작 바이트가 0인 경우, 15바이트 HexString으로 표시
- HexString은 전체 경로를 CRC 환산식으로 계산한 Hex값
- Path 자체는 Unicode로 변환된 후 계산
- 파일 형식
 - OLECF (Object Linking and Embedding Compound)
 - DestList 파일 이름과 같은 HexString을 사용
 - DestList : 32바이트 헤더와 다수의 DestList 엔트리로 구성
- automaticDestinations-ms에 포함되는 주요 정보
 - 파일의 GUID
 - Hostname
 - 파일 수정 시각
 - 파일 경로

2 구조

AutoDest – DestList structure

DestList Stream 구성

- DestList Header
 - JumpList 전체에 대한 메타 정보
- DestList Entry 배열
 - 사용자가 실행한 개별 파일이나 문서에 대한 정보가 담긴 항목들

DestList Header (32bytes)

오프셋	크기	Windows 7/8 설명	Windows 10 설명
0x00	4	Version number (value 1)	Version number (value 3)
0x04	4	전체 엔트리 수	전체 엔트리 수
0x08	4	고정된 엔트리 수	고정된 엔트리 수
0x0C	4	Floating Point value, some kind of counter	Unknown
0c10	8	최근 사용된 항목	최근 사용된 항목
0x18	8	Number of add/delete actions – increments as Entries are added and deleted	Number of add/delete actions – increments as Entries are added and deleted

2 구조

AutoDest – DestList structure

DestList Entry : Version 1 (Windows 7/8)

오프셋	크기	필드명	설명
0x00	8	Entry checksum or hash	
0x08	16	Droid Volume ID	대상 파일의 Volulme GUID
0x18	16	Droid File ID	대상 파일의 File GUID
0x28	16	Birth Droid Volume ID	생성 당시의 Volume GUID
0x38	16	Birth Droid File ID	생성 당시의 File GUID
0x48	16	Hostname (ASCII, 0-padding)	접근한 컴퓨터 이름
0x58	8	Entry ID Number	항목 식별 번호
0x60	4	Float counter (file access count?)	Floating point counter to record each time the file is accessed not necessarily opened
0x64	8	Last access time	MSFILETIME of last recorded access
0x6C	4	Pin status	0xFFFFFFFF: unpinned, others: pinned count
0x70	2	Length of Unicode string data	
0x72	-	Entry string data	

2 구조

AutoDest – DestList structure

DestList Entry : Version 3 (Windows 10)

오프셋	크기	필드명	설명
0x00	8	Entry checksum or hash	
0x08	16	Droid Volume ID	대상 파일의 Volulme GUID
0x18	16	Droid File ID	대상 파일의 File GUID
0x28	16	Birth Droid Volume ID	생성 당시의 Volume GUID
0x38	16	Birth Droid File ID	생성 당시의 File GUID
0x48	16	Hostname (ASCII, 0-padding)	접근한 컴퓨터 이름
0x58	4	Entry ID Number	항목 식별 번호
0x5C	8	In all test '0x00000000'	
0x64	8	Last access time	MSFILETIME of last recorded access
0x6C	4	Pin status	0xFFFFFFFF: unpinned, others: pinned count
0x70	4	In all test '0xFFFFFFFF'	
0x74	4	Access counter	A counter that consistently increases as files are re-opened (access count)
0x78	8	In all test '0x00000000'	
0x80	2	Length of Unicode string data	
0x82	-	Entry string data	followed by '0x00000000'

2 구조

Custom-Destinations

- .customDestinations-ms 확장자를 가짐
- 파일 이름
 - Hex값
 - 16바이트
 - 시작 바이트가 0인 경우, 15바이트 HexString으로 표시
- 파일 구성
 - 파일 헤더
 - 32바이트로 구성
 - 해당 파일이 몇 개의 엔트리로 구성되었는지 확인 가능
 - 링크 파일 엔트리 (LNK file)
 - LNK 파일에서 확인할 수 있는 GUID 값
 - LNK 파일에서 사용하는 Data Stream
 - Checksum 값
 - 파일 푸터
 - 0xbabffbab
 - 추가적인 데이터
 - LNK 파일에서 확인할 수 있는 GUID 값
 - LNK 파일에서 사용하는 Data Stream

2 구조

CustDest – File Structure

구성요소

- File Header
- Category Structure

File Header (12 bytes)

오프셋	크기	필드명	설명
0x00	4	Format Version	일반적으로 2
0x04	4	Number of categories	포함된 카테고리 개수
0x08	4	Unknown (empty values)	

Category Structure

오프셋	크기	필드명	설명
0x00	4	Category Type	Type 0 : Custom Type 1 : Known Type 2 : User Tasks

- Type 0 – Custom Category (사용자 정의)

오프셋	크기	필드명	설명
0x04	2	문자열 길이	UTF-16 문자열의 문자 수
0x06	...	Category 이름 문자열	UTF-16LE, null 종료 없음
...	4	Entry 개수	포함된 항목 수
...	...	Entries	Shell Object entry 배열
마지막	4	Footer Signature	0xbabffbab

2 구조

CustDest – File Structure

- Type 1 – Known Category (시스템 내장)

오프셋	크기	필드명	설명
...	4	Category ID	1 : Frequent, 2 : Recent
마지막	4	Footer Signature	0xbabffbab

- Type 2 – User Tasks (사용자 작업)

오프셋	크기	필드명	설명
...	4	Number of entries	포함된 작업 수
...	...	Entries	Shell object entry 배열
마지막	4	Footer Signature	0xbabffbab

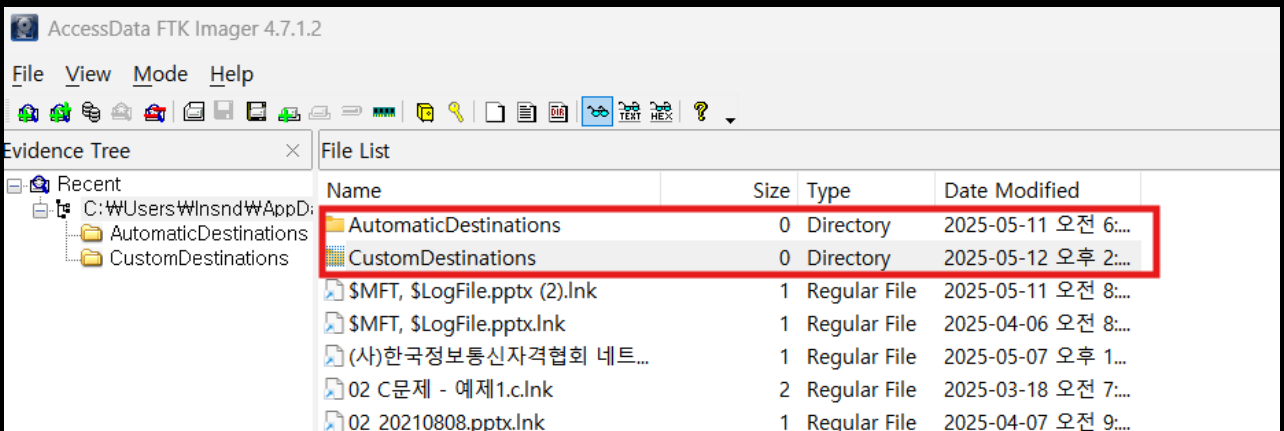
Shell object Entry 구조

오프셋	크기	필드명	설명
0x00	16	Class Identifier	LNK GUID
0x10	...	Shell Object Data	LNK 형식 경로, 아이콘 등

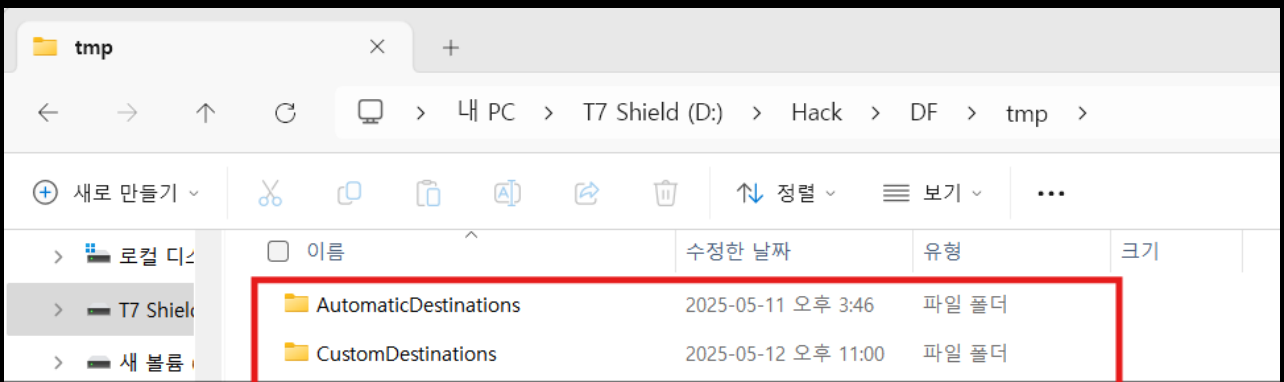
3 분석 방법

JumpList Explorer

- FTK Imager에서
C:\Users\Insnd\AppData\Roaming\Microsoft\Windows\Recent
하위의 AutomaticDestinations, CustomDestinations 폴더를 Export



- 아티팩트 분석을 위해 추출



3 분석 방법

JumpList Explorer

Source File Name	Jump List Type	App ID	App ID Description	Lnk File Count	File Size
D:\Hack\WDFWtmp\AutomaticDestinations\W5...	Automatic	5d696d521de238c3	Google Chrome 9.0.597.84 / ...	555	803,840
D:\Hack\WDFWtmp\AutomaticDestinations\W5...	Automatic	5f7b5f1e01b83767	Quick Access	1,338	2,939,392
D:\Hack\WDFWtmp\AutomaticDestinations\W5...	Automatic	5fd40d254d00899		0	2,560
D:\Hack\WDFWtmp\AutomaticDestinations\W6...	Automatic	6c9c4f36660efd83		21	34,816
D:\Hack\WDFWtmp\AutomaticDestinations\W6...	Automatic	6d2bac8f1edf6668	Microsoft Outlook 2016 64-bit	1	3,584
D:\Hack\WDFWtmp\AutomaticDestinations\W6...	Automatic	6dc04f5ccc522861	Microsoft.Windows.ShellExp...	2	4,608
D:\Hack\WDFWtmp\AutomaticDestinations\W6...	Automatic	6dcad003123a22fe	Android Studio	20	48,128
D:\Hack\WDFWtmp\AutomaticDestinations\W6...	Automatic	6e7c22fc8d19c095		1	3,072
D:\Hack\WDFWtmp\AutomaticDestinations\W6...	Automatic	6fac1b1908485d3	Windows Font Viewer	10	19,968
D:\Hack\WDFWtmp\AutomaticDestinations\W7...	Automatic	7b99ab6c3d3b551d		0	1,536
D:\Hack\WDFWtmp\AutomaticDestinations\W7...	Automatic	7e4dca80246863e3	Control Panel - Settings	9	10,240

- 얻을 수 있는 정보
 - 소스 파일의 경로
 - Jump List 타입 (Automatic / Custom)
 - App ID
 - APP ID 설명 (파일명)
 - 링크 파일 클릭한 횟수
 - 파일의 크기

Name	Entry Number	Target Created On	Target Modified On	Target Accessed ...	Absolute Path	Extra Block Count	Interaction Count
5d696d521de238c3.automaticDestinations-ms							
Entry #: 0560 - This PC\WDWU\4학년\Wwebsevice\W강의자...	560				This PC\WDW...	1	1
Entry #: 0559 - This PC\WDWU\4학년\Wwebsevice\W강의자...	559				This PC\WDW...	1	1
Entry #: 0558 - This PC\WDWU\4학년\Wwebsevice\W강의자...	558				This PC\WDW...	1	1
Entry #: 0557 - This PC\WDWU\4학년\Wwebsevice\W강의자...	557				This PC\WDW...	1	1
Entry #: 0003 - Internet Folder\http://www.msftconnecttest...	3				Internet Folder\...	1	44
Entry #: 0556 - This PC\WDWU\4학년\Wwebsevice\W강의자...	556				This PC\WDW...	1	1
	555				UsersLibraries\WD...	1	1
	554	2025-03-30 12:1...	2025-04-08 11:1...	2025-04-08 11:1...	This PC\WDW...	1	1
	553	2025-04-21 07:4...	2025-04-16 14:3...	2025-04-21 07:4...	This PC\WDW...	1	1
	552	2025-04-21 07:4...	2025-04-16 13:5...	2025-04-21 07:4...	This PC\WDW...	1	1
	551				This PC\WDW...	1	1
	547	2025-04-29 08:3...	2025-04-30 06:5...	2025-04-30 06:5...	This PC\WDW...	1	2

- 얻을 수 있는 정보
 - 엔트리에 부여된 고유 번호
 - 최초 생성 시간 / 마지막 수정 시간 / 마지막으로 접근된 시간
 - 전체 경로
 - Extra 블록의 수 : 고정된 구조 외에 추가 정보를 저장하기 위한 블록
 - 실제 클릭해서 실행한 횟수

References

- <http://www.forensic-artifact.com/windows-forensics/jumplist>
- <https://www.forensic-cheatsheet.com/KR/Artifact/Jumplist>
- Singh, Bhupendra & Singh, Upasna. (2016). A forensic insight into Windows 10 Jump Lists. Digital Investigation. 17. 1-13.
10.1016/j.diin.2016.02.001.
- https://forensics.wiki/jump_lists/
- <https://psmths.gitbook.io/windows-forensics/artifacts-by-type/filesystem-artifacts/automatic-destinations>
- <https://github.com/libyal/dtformats/blob/main/documentation/Jump%20lists%20format.asciidoc>
- <https://binaryforay.blogspot.com/2016/02/jump-lists-in-depth-understand-format.html>