점프 목록 포렌식

JK Kim

@pr0neer

forensic-proof.com

proneer@gmail.com

개요

1. 점프 목록 소개
2. 점프 목록 구조
3. 점프 목록 카빙
4. 점프 목록 분석

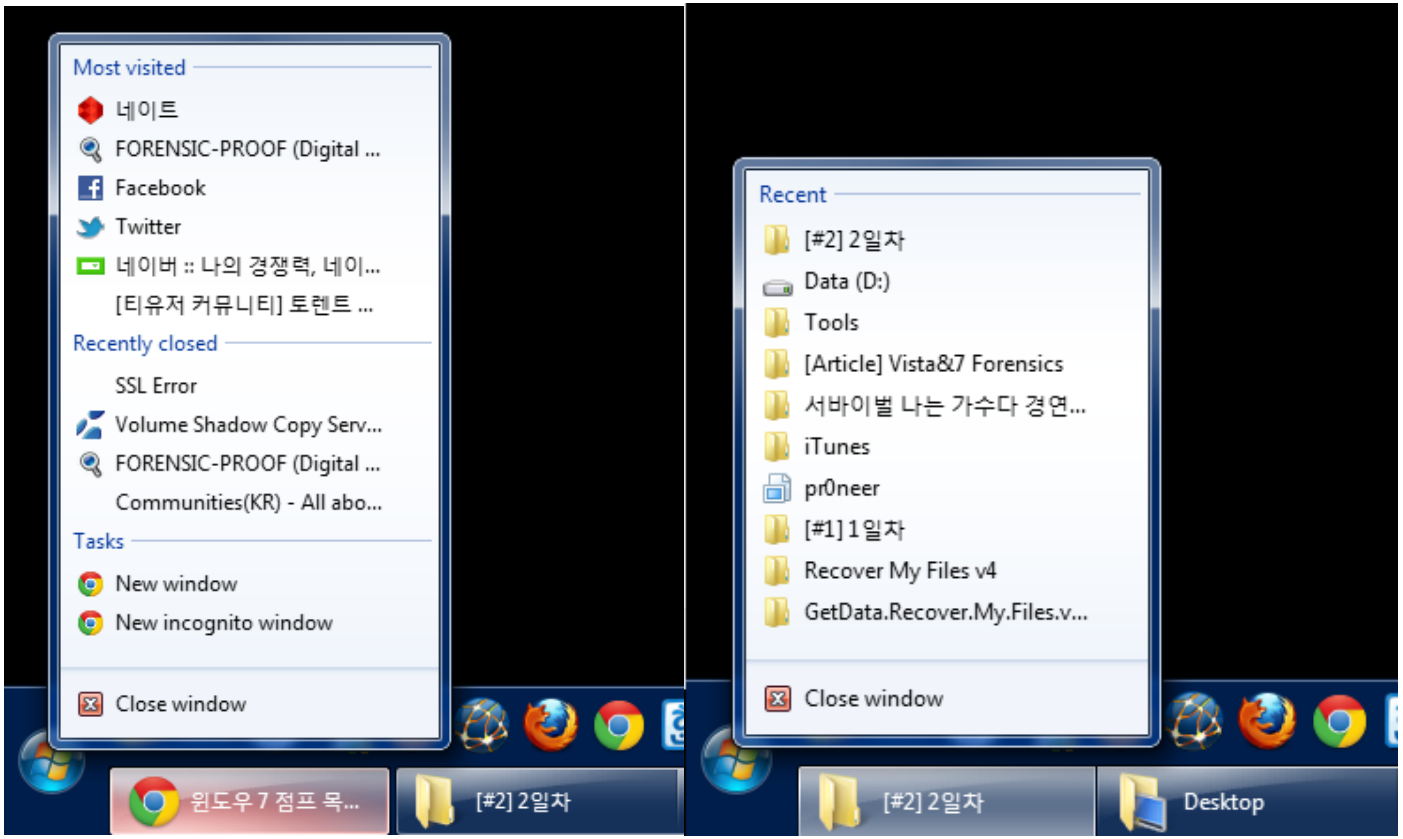
점프 목록 소개

점프 목록 (Jump List)

- **윈도우 7에서 새롭게 추가된 기능**
- **응용프로그램 사용 로그**
  - 최근 접근 문서 (Recent) 폴더와 RecentDocs 레지스트리 키
  - UserAssist 레지스트리 키
  - 점프 목록!!!

점프 목록 확인

- 작업표시줄의 마우스 우클릭으로 점프 목록 확인



점프 목록 종류

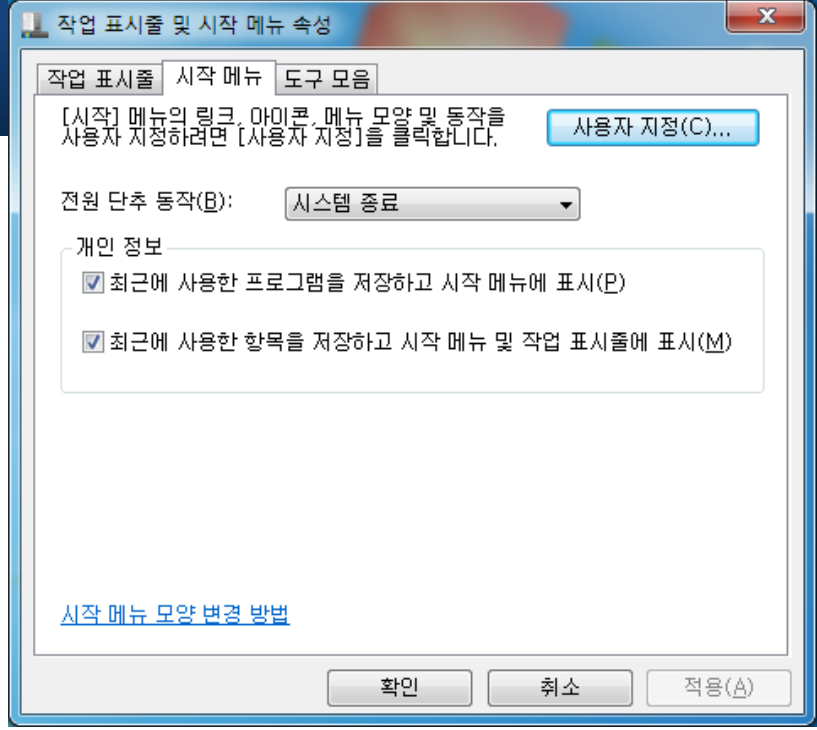
- **Recent**
  - 사용자가 최근 접근한 파일이나 폴더
- **Frequent**
  - 사용자가 빈번히 접근한 파일이나 폴더
- **Tasks**
  - 응용프로그램에서 지원하는 작업 목록
- **Pinned**
  - 사용자가 고정 시킨 작업 목록

점프 목록의 활용

- **포렌식적 의미**
  - 사용자의 응용프로그램 사용 흔적 및 패턴을 파악
  - 윈도우 7에서 기본 활성화
  - 최근 접근 문서(Recent)나 UserAssist 키보다 더 많은 정보 포함
  - 사용자가 직접 삭제하지 않는 이상 운영체제 설치 시부터 지속적으로 로그 저장
  - 사용자의 행위를 파악하거나 정보 유출 사건 분석에 큰 역할

점프 목록 소개

점프 목록 설정



- **[제어판] ➔ [작업표시줄 및 시작메뉴]**
  - **첫 번째 체크박스**
    - ✓ 최근 사용한 프로그램 시작 메뉴에 표시 여부
    - ✓ 체크 해제한 후 적용을 누르면 시작 메뉴 항목 제거
  - **두 번째 체크박스**
    - ✓ 점프 목록에 관한 설정
    - ✓ 체크 해제한 후 적용을 누르면 이전에 기록된 모든 점프 목록 삭제
    - ✓ 고정된(pinned) 점프 목록은 삭제되지 않음
  - **사용자 지정 버튼**
    - ✓ 시작 메뉴와 점프 목록에 지정할 프로그램 지정이나 목록 수 설정

점프 목록 구조

저장 경로

- **Recent 폴더 하위에 저장**
  - %UserProfile%₩AppData₩Roaming₩Microsoft₩Windows₩Recent

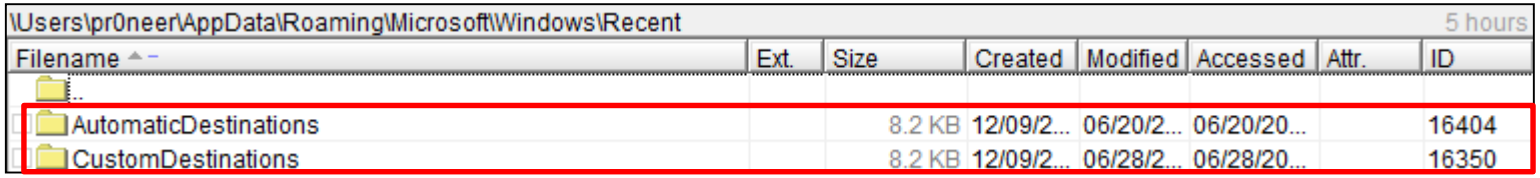
\Users\pr0neer\AppData\Roaming\Microsoft\Windows\Recent — 5 hours

Filename	Ext.	Size	Created	Modified	Accessed	Attr.	ID
..							
AutomaticDestinations		8.2 KB	12/09/2...	06/20/2...	06/20/20...		16404
CustomDestinations		8.2 KB	12/09/2...	06/28/2...	06/28/20...		16350
#1.lnk	lnk	474 bytes	06/20/2...	06/20/2...	06/20/20...	A	214865
#7 Resume.lnk	lnk	0.5 KB	06/20/2...	06/24/2...	06/24/20...	A	226305
[#1] 1일차 (레지스트리, 파일시스템, 파일 복구).lnk	lnk	0.8 KB	06/20/2...	06/20/2...	06/20/20...	A	227446
[#1] 1일차.lnk	lnk	0.7 KB	06/20/2...	06/27/2...	06/27/20...	A	41141
[#10-1] OS Artifacts - Event Logs.pptx.lnk	lnk	1.1 KB	06/27/2...	06/27/2...	06/27/20...	A	213929
[#2-6] File System Forensic Analysis.pdf.lnk	lnk	0.9 KB	06/21/2...	06/21/2...	06/21/20...	A	214837
[#2-7] Data Recovery Techniques.pdf.lnk	lnk	0.9 KB	06/21/2...	06/21/2...	06/21/20...	A	219680
[#2] 2일차.lnk	lnk	0.7 KB	06/20/2...	06/28/2...	06/28/20...	A	57701
[#3-1] File System Forensic Analysis.pdf.lnk	lnk	0.9 KB	06/22/2...	06/22/2...	06/22/20...	A	239334
[#3-2] Data Recovery Techniques.pdf.lnk	lnk	0.9 KB	06/22/2...	06/22/2...	06/22/20...	A	243716
[#3-3] Windows 7 File System.pdf.lnk	lnk	0.9 KB	06/22/2...	06/22/2...	06/22/20...	A	215444
[#3-4] Windows 7 Folder Structure.pdf.lnk	lnk	0.9 KB	06/22/2...	06/22/2...	06/22/20...	A	241208
[#3-5] OS Artifacts - Prefetch & Superfetch.pptx.lnk	lnk	1.0 KB	06/27/2...	06/27/2...	06/27/20...	A	214426
[#3-5] OS Artifacts - Prefetch,Superfetch,ReadyBoost.pptx.lnk	lnk	1.0 KB	06/27/2...	06/27/2...	06/27/20...	A	216571
[#3-5] Windows 7 Artifacts.pptx.lnk	lnk	0.9 KB	06/27/2...	06/27/2...	06/27/20...	A	214003
[#3] 3일차.lnk	lnk	0.7 KB	06/21/2...	06/27/2...	06/27/20...	A	58175
[#9-2] OS Artifacts - Shortcut(LNK).pptx.lnk	lnk	1.1 KB	06/27/2...	06/27/2...	06/27/20...	A	89764
[#FP] Data Recovery Techniques.pdf.lnk	lnk	1.8 KB	06/27/2...	06/27/2...	06/27/20...	A	243912

점프 목록 구조

저장 경로

- **Recent 폴더 하위에 저장**



- **AutomaticDestinations**
  - 운영체제가 자동으로 남기는 항목
  - 최근 사용한 목록(Recent)이나 자주 사용되는 목록(Frequent)

- **CustomDestinations**
  - 응용프로그램이 자체적으로 관리하는 항목
  - 작업(Task) 목록

App ID

- **파일명**
  - 각 응용프로그램 별로 고유한 16자리 사용
    - ✓ http://www.forensicswiki.org/wiki/List_of_Jump_List_IDs
    - ✓ http://forensicartifacts.com/tag/jump-lists/

\Users\pr0neer\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

Filename	Ext.	Size	Created	Modified	Accessed	Attr.	ID
..							
12dc1ea8e34b5a6.automaticDestinations-ms	autom	53.0 KB	06/15/2...	06/22/2...	06/15/20...	A	61095
1b4dd67f29cb1962.automaticDestinations-ms	autom	83.1 KB	06/15/2...	06/28/2...	06/15/20...	A	58662
20f18d57e149e379.automaticDestinations-ms	autom	8.0 KB	06/15/2...	06/25/2...	06/15/20...	A	59221
2d61cccb4338dfc8.automaticDestinations-ms	autom	17.0 KB	06/18/2...	06/26/2...	06/18/20...	A	210248
44a3621b32122d64.automaticDestinations-ms	autom	4.0 KB	06/15/2...	06/19/2...	06/15/20...	A	58696
458f7bc92ebd65ec.automaticDestinations-ms	autom	4.5 KB	06/15/2...	06/27/2...	06/15/20...	A	62186
4d8bdacf5265a04f.automaticDestinations-ms	autom	31.0 KB	06/15/2...	06/27/2...	06/15/20...	A	92035

\Users\pr0neer\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations

Filename	Ext.	Size	Created	Modified	Accessed	Attr.	ID
..							
28c8b86deab549a1.customDestinations-ms	custon	6.3 KB	12/09/2...	06/27/2...	06/27/20...	A	218887
29db278f507c92bb.customDestinations-ms	custon	3.7 KB	02/07/2...	06/15/2...	06/15/20...	A	16196
337ed59af273c758.customDestinations-ms	custon	1.6 KB	06/20/2...	06/20/2...	06/20/20...	A	89006
5afe4de1b92fc382.customDestinations-ms	custon	18.3 KB	12/09/2...	06/15/2...	06/15/20...	A	16353
5d696d521de238c3.customDestinations-ms	custon	23.3 KB	12/09/2...	06/28/2...	06/28/20...	A	190438
5d6f13ed567aa2da.customDestinations-ms	custon	8.8 KB	12/10/2...	06/15/2...	06/15/20...	A	16531
5df4765359170e26.customDestinations-ms	custon	5.6 KB	05/19/2...	06/15/2...	06/15/20...	A	16533

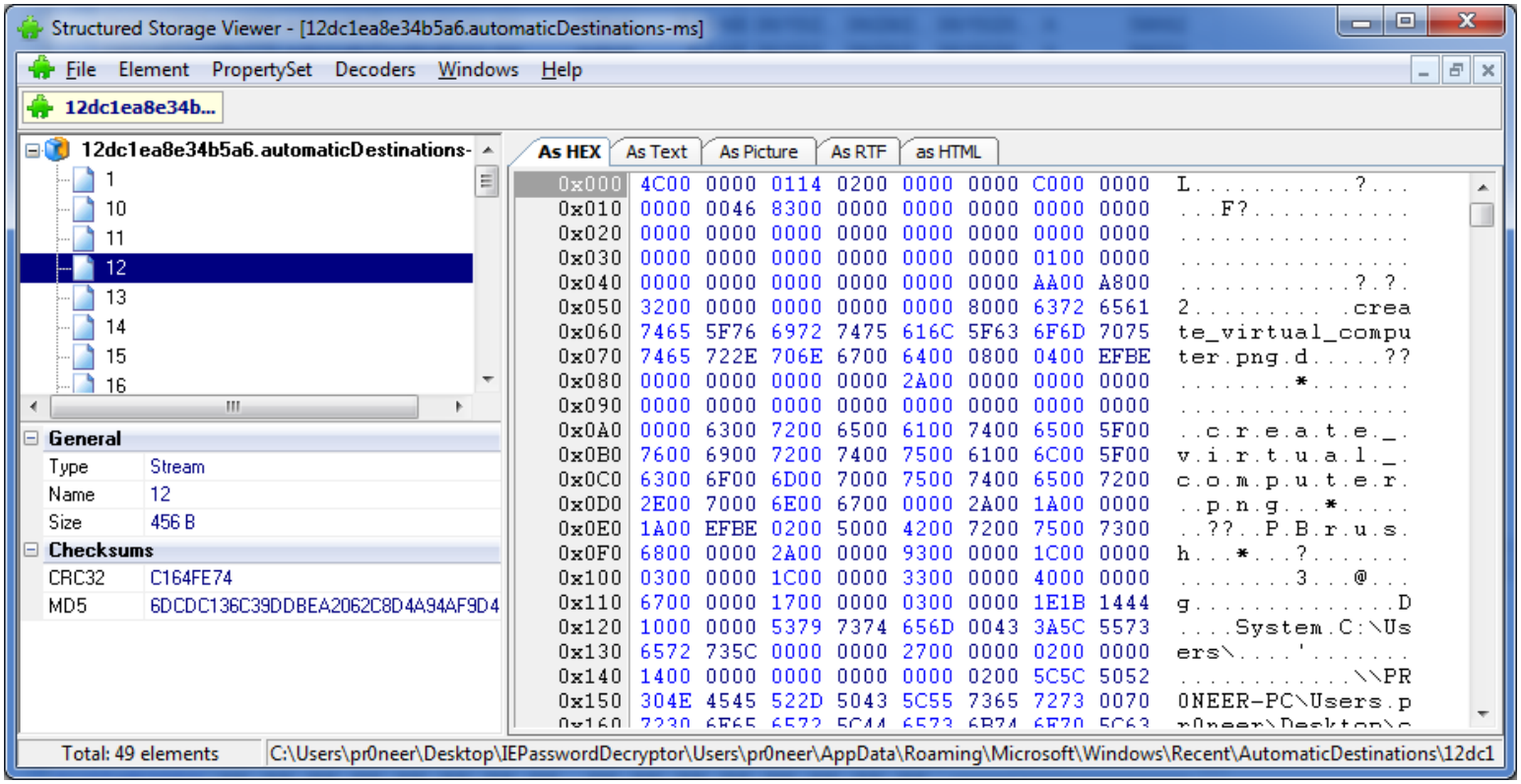
App ID

응용프로그램	점프 목록 파일 이름
Windows Explorer	1b4dd67f29cb1962
Microsoft Word 2003	a8c43ef36da523b1
Microsoft Word 2007	adecfb853d77462a
Microsoft Word 2010	44a3621b32122d64
Internet Explorer 8	28c8b86deab549a1
Notepad	918e0ecb43d17e23
Microsoft Powerpoint 2007	f5ac5390b9115fdb
Adobe Reader 8, 9	23646679aaccfae0
Adobe Acrobat 8 Professional	6807f6e0bc8d4ca7
Paint 6.1	12dc1ea8e34b5a6
Firefox	5c450709f7ae4396
Media Center	b91050d8b077a4e8
Windows Live Mail	d7528034b5bd6f28
Hanword (HWP) 2010	20f18d57e149e379
Gom Audio	458f7bc92ebd65ec
KMPlayer	4d8bdacf5265a04f

점프 목록 구조

구조

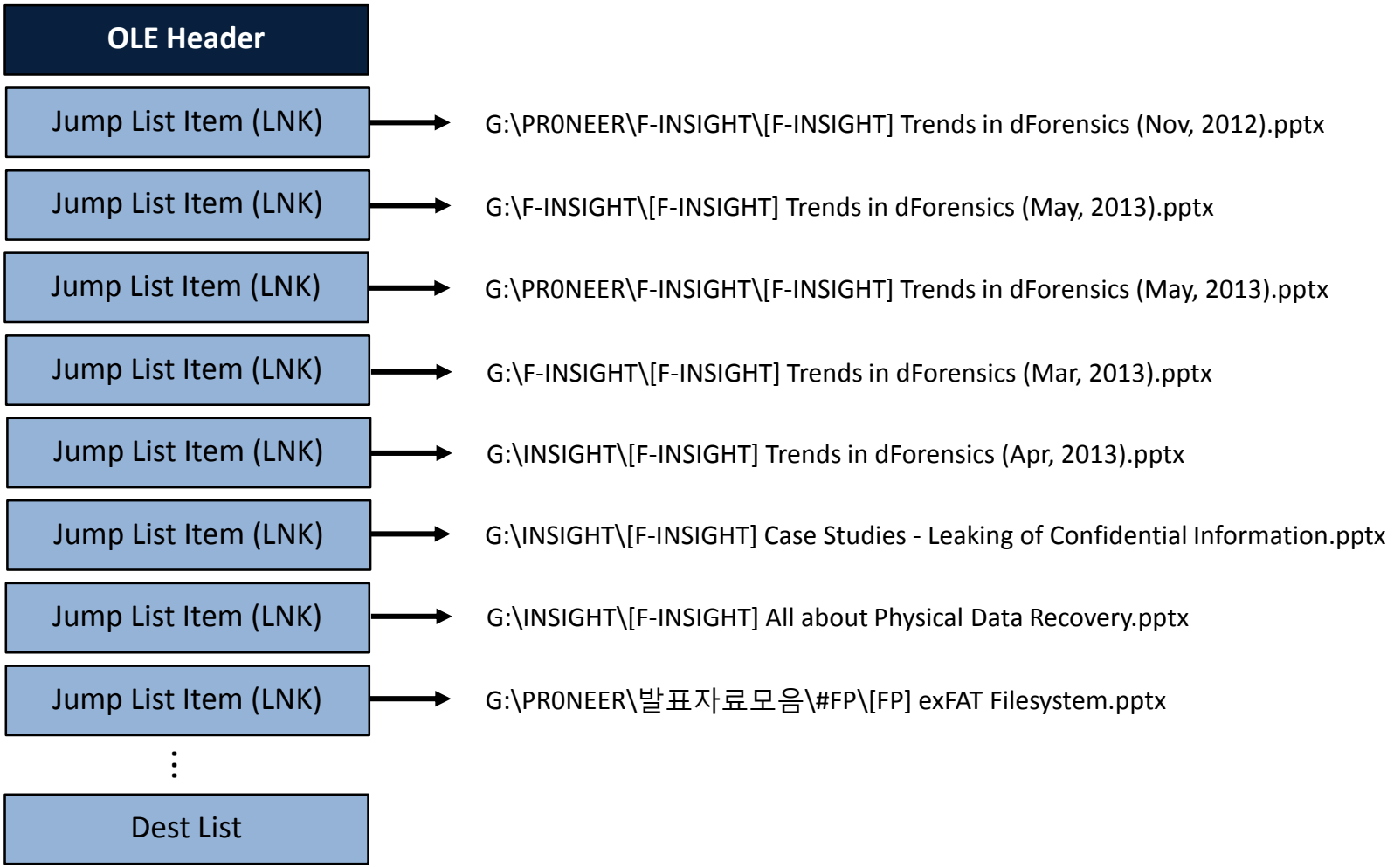
- **점프 목록 파일 구조**
  - OLE Compound 파일 구조를 사용
  - 점프 목록 각 아이템을 OLE 스트림(바로가기 파일)으로 저장



점프 목록 구조

구조

- **점프 목록 파일 구조**



점프 목록 구조

실습 #1

- JumpListsView로 라이브 상태에서 점프 목록 확인하기!!!

점프 목록 구조

실습 #2

- Jmp로 수집한 점프 목록 분석하기!!!

점프 목록 구조

실습 #3

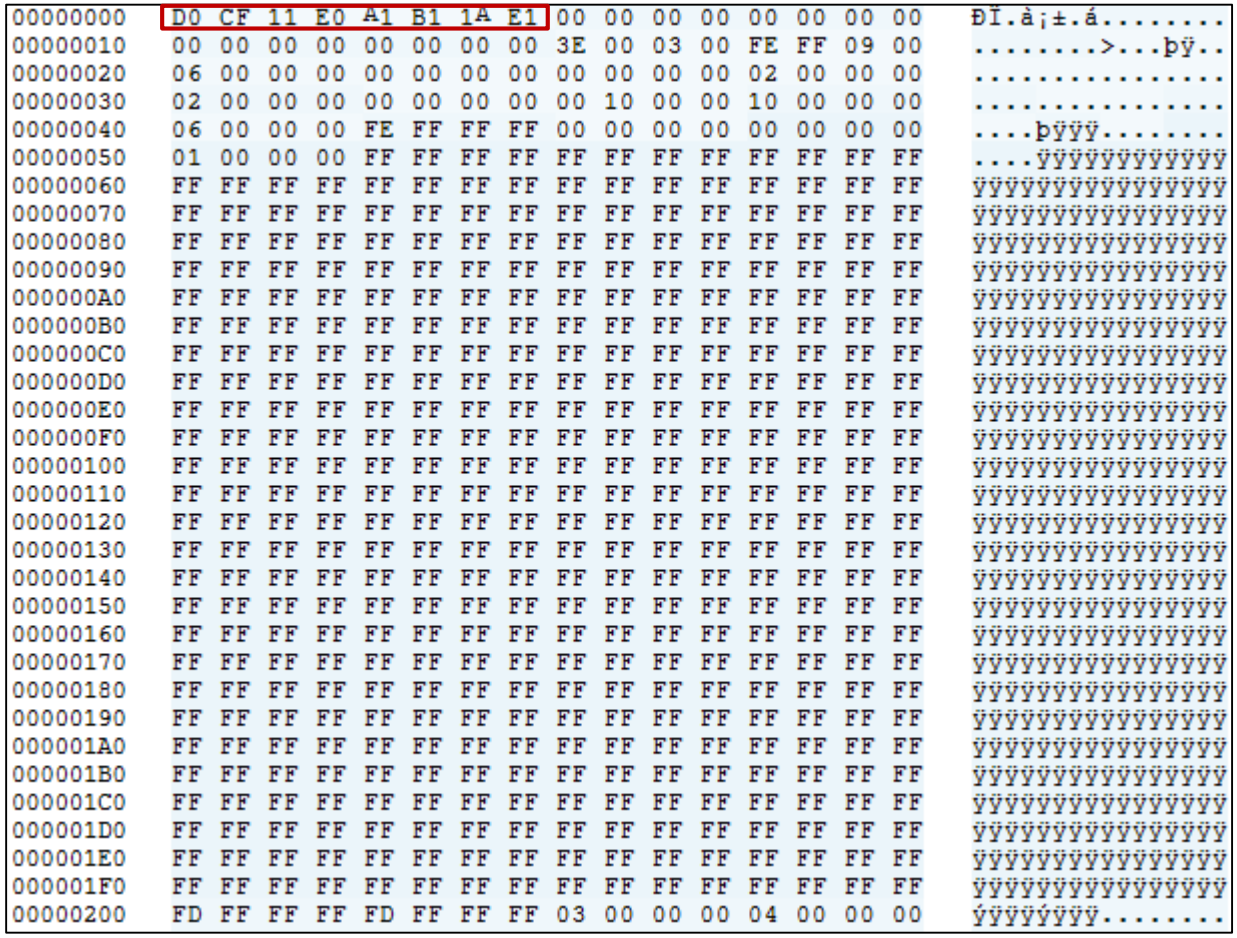
- 점프 목록 항목 삭제 시 변화 살펴보기!!!

점프 목록 카빙

점프 목록 카빙

OLE

- **카빙 방법**
  - 먼저, 8바이트 시그니처를 통해 OLE 문서 파일 카빙

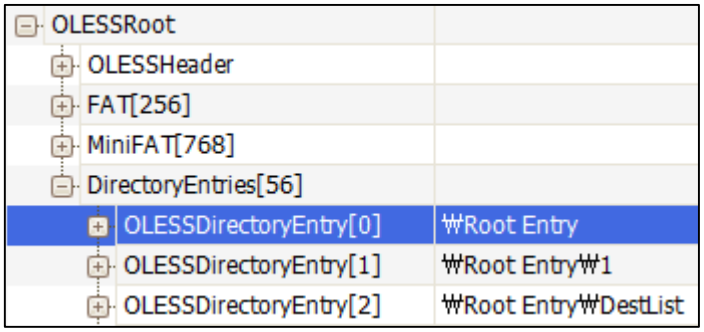


```
00000000  D0 CF 11 E0 A1 B1 1A E1 00 00 00 00 00 00 00 00  ÐÏ.à¡±.á........
00000010  00 00 00 00 00 00 00 00 3E 00 03 00 FE FF 09 00  ........>...þÿ..
00000020  06 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00  ................
00000030  02 00 00 00 00 00 00 00 00 10 00 00 10 00 00 00  ................
00000040  06 00 00 00 FE FF FF FF 00 00 00 00 00 00 00 00  ....þÿÿÿ........
00000050  01 00 00 00 FF FF FF FF FF FF FF FF FF FF FF FF  ....ÿÿÿÿÿÿÿÿÿÿÿÿ
00000060  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000070  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000080  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000090  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000A0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000B0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000C0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000D0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000E0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000F0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000100  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000110  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000120  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000130  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000140  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000150  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000160  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000170  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000180  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000190  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000001A0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000001B0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000001C0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000001D0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000001E0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000001F0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000200  FD FF FF FF FD FF FF FF 03 00 00 00 04 00 00 00  ýÿÿÿýÿÿÿ........
```

점프 목록 카빙

OLE

- **카빙 방법**
  - 카빙된 문서 파일에서 점프 목록 분리
  - 점프 목록 OLE 형식은 모두 기본 3개의 스트림을 가짐 ➔ 초기 3개의 스트림 검증
    - ✓ Root Entry
    - ✓ Root Entry₩1
    - ✓ Root Entry₩DestList



점프 목록 카빙

실습 #4

- 비할당 영역에서 점프 목록 파일 카빙하기!!!

질문 및 답변