

JumpList Template

S.C.P 이유경, 장혜선

2022-01-27



CONTENTS

01 프로젝트 개요

02 프로젝트 수행 과정

- ¹ 분석
- ² 템플릿
- ³ 개발 진행 정도

03 향후 계획





프로젝트 개요

e.g., Prefetch(PF.bt)

00000000 17 00 00 00 53 43 43 41 11 00 00 00 56 50 02 00SCCA....fP..
 00000010 43 00 48 00 52 00 4F 00 4D 00 45 00 2E 00 45 00 C.H.R.O.M.E...E..
 00000020 58 00 45 00 00 00 FF FF 00 00 00 00 00 00 00 00 X.E...y...
 00000030 54 00 00 00 80 FA FF FF 00 00 00 00 00 00 00 00 T...öüyy...
 00000040 00 00 00 00 00 00 00 00 6E 6D 6E 03 02 9A 23 FFnmn...š#y
 00000050 00 00 00 00 F0 00 00 00 A8 00 00 00 F0 15 00 008...
 00000060 A3 26 00 00 94 E5 01 00 F2 5B 00 00 58 40 02 00 Éä..."[...@..
 00000070 02 00 00 00 AE 0F 00 00 1A 00 00 00 01 00 00 00
 00000080 B4 96 43 A1 C1 D0 CC 01 00 8C 86 47 00 00 00 00 -C;ādi...G+G...
 00000090 00 8C 86 47 00 00 00 00 7B 05 00 00 06 00 00 00 .G+G...{.....

프리패치 버전 시그니처(SCCA) 프리패치 서비스 버전(0x00000011) 프리패치 파일 크기

실행파일 이름 실행파일의 이름이 58byte를 넘길 경우 0x0000으로 설정

실행파일의 전체경로(명령 옵션 포함)의 MD5 해쉬 값

언제나 0x00000000 섹션정보의 offset 섹션 개수

페이지파일 정보의 offset 페이지 파일 개수

파일이름정보의 offset 파일이름정보의 크기

디스크 볼륨 정보 디스크 볼륨 개수 디스크 볼륨 크기

최종실행 시각 언제나 0x00000000 언제나 0x00000000

실행회수

[그림 4 - Win 7의 프리패치 파일 구조 offset]

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

00000000 11 00 00 00 53 43 43 41 DF 00 00 00 EE 2F 00 00SCCA...i/..
 00000010 43 00 4D 00 44 00 2E 00 45 00 58 00 45 00 00 00 C.M.D...E.X.E..
 00000020 06 00 00 00 48 B4 13 82 20 60 0A 82 00 00 00 00 ...H'., '.,...
 00000030 00 00 00 00 90 B3 13 82 40 9D 0E B2 FC 9C 0E B2*,@...äæ.*
 00000040 18 9C 0E B2 60 6B E2 81 40 9D 0E B2 01 40 7B 08 .æ.*`ká.@...@{..
 00000050 00 00 00 00 98 00 00 00 21 00 00 00 2C 03 00 00!.....
 00000060 36 02 00 00 B4 1D 00 00 24 0E 00 00 08 2B 00 00 6.....\$...ø+..
 00000070 01 00 00 00 16 04 00 00 40 B0 C7 D1 50 CF CC 01@°ÇÑPii..
 00000080 00 8C 86 47 00 00 00 00 8C 86 47 00 00 00 00 .G+G...G+G...
 00000090 4A 00 00 00 02 00 00 00 00 00 00 36 00 00 00 J.....6...

프리패치 버전 시그니처 프리패치 서비스 버전

프리패치 파일 크기 실행파일 이름

실행파일 이름의 길이가 58byte를 넘어가는 경우 0x0000으로 설정 됨

실행파일 전체경로(명령 옵션 포함)의 MD5 해쉬 값

언제나 0x00000000 섹션정보 offset 섹션 개수

페이지 파일 정보 offset 페이지파일 개수 파일이름 정보 offset

파일이름 정보 크기 디스크 볼륨 정보 디스크 볼륨 개수

디스크 볼륨 크기 최종 실행 시간 실행 회수

[그림 5 - Win XP의 프리패치 파일 구조 offset]

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	1E	00	00	00	53	43	43	41	11	00	00	00	68	80	00	00SCCA....h'.
0010h:	41	00	4C	00	4E	00	4F	00	54	00	49	00	43	00	45	00	A.L.N.O.T.I.C.E.
0020h:	2E	00	45	00	58	00	45	00	00	00	00	00	00	00	00	00	...E.X.E.....
0030h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00L'.
0040h:	00	00	00	00	00	00	00	00	00	00	00	00	00	4C	85	91	B0
0050h:	00	00	00	00	28	01	00	00	4F	00	00	00	08	08	00	00O.....
0060h:	71	0B	00	00	90	66	00	00	48	2E	00	00	60	95	00	00	q....f...H....
0070h:	01	00	00	00	08	1B	00	00	25	00	00	00	01	00	00	00
0080h:	6F	57	8A	A1	A7	07	D8	01	C2	EC	DA	55	8E	07	D8	01	owS;\$.ø.Å10U2.ø.
0090h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00A0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00B0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00C0h:	00	00	00	00	00	00	00	00	02	00	00	00	01	00	00	00
00D0h:	00	00	00	00	D8	94	00	00	84	00	00	00	00	00	00	00ø"
00E0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00F0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0100h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0110h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0120h:	00	00	00	00	00	00	00	00	00	00	00	00	05	00	00	00
0130h:	05	00	00	00	00	00	00	00	3D	00	00	00	00	01	00	00=.....
0140h:	18	46	12	00	00	02	05	00	00	00	00	00	2E	00	00	00F.....
0150h:	2E	00	00	00	7C	00	00	00	3D	00	00	00	00	01	00	00=.....
0160h:	CB	88	0B	00	00	03	00	00	33	00	00	00	1E	00	00	00	E'.....3.....
0170h:	1E	00	00	00	F8	00	00	00	40	00	00	00	00	01	00	00ø...e.....
0180h:	4C	3F	11	00	00	00	01	00	51	00	00	00	08	00	00	00	L?...Q.....
0190h:	08	00	00	00	7A	01	00	00	40	00	00	00	00	01	00	00Z...@.....
01A0h:	DB	93	13	00	00	00	01	00	59	00	00	00	31	00	00	00	0.....Y...1...
01B0h:	31	00	00	00	FC	01	00	00	40	00	00	00	00	01	00	00	1...0...@.....
01C0h:	30	96	13	00	00	00	01	00	8A	00	00	00	01	00	00	00	0-...S.....
01D0h:	01	00	00	00	7E	02	00	00	3E	00	00	00	00	01	00	00~...>.....

Template Results - PF.bt ↗

Name	Value
struct FileHeader header	
enum Version version	Windows10 (30)
char Signature[4]	SCCA
byte Unknown[4]	◀
int FileSize	45160
wchar_t FileName[30]	ALNOTICE.EXE
int Hash	B091854Ch
enum Flag flag	Application (0)
struct Win10_FileInformation Fileinfo	
struct Win10_FileMetricsArray FileMetrics	
struct Win10_TraceChainArray TraceChain	
struct Win10_FileNameStrings FileName	
struct Win10_VolumeInformation Volumeinfo	
struct Trailing Data	



프로젝트 수행 과정

¹ 분석

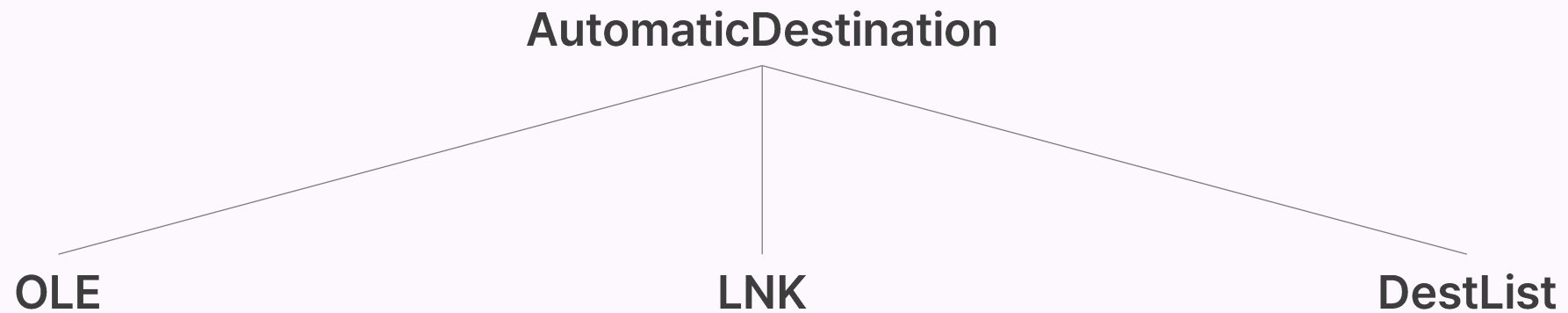
AutomaticDestination

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 pinned 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

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	D0	CF	11	E0	A1	B1	1A	E1	00	00	00	00	00	00	00	00	DI.aj±.ā.....
0010h:	00	00	00	00	00	00	00	00	3E	00	03	00	FE	FF	09	00>...pÿ..
0020h:	06	00	00	00	00	00	00	00	00	00	00	00	01	00	00	00
0030h:	01	00	00	00	00	00	00	00	00	10	00	00	02	00	00	00
0040h:	01	00	00	00	FE	FF	FF	FF	00	00	00	00	00	00	00	00pyyy.....
0050h:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy
0060h:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy
0070h:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy
0080h:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy
0090h:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy
00A0h:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy
00B0h:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy
00C0h:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy
00D0h:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy

Template Results - JL-Auto.bt

Name	Value
▼ struct FileHeader header	
> char Signature[8]	DI4aj±.ā
> GUID CLSID[16]	{00000000-0000-0000-0000-000000000000}
short MinorVersion	62
short MajorVersion	3
enum ByteOrder1 byteorder	LittleEndian (FFFEh)
short SectorShift	9
short SBAT	6
short Reserved1	0
uint Reserved2	0
uint DirectorySector	0
uint FATSector	1
uint SECID	1

DestList

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	04	00	00	00	3E	00	00	00	00	00	00	00	08	00	16	43>.....C
0010h:	3E	00	00	00	00	00	00	00	29	01	00	00	00	00	00	00	>.....).>
0020h:	D9	58	DF	39	A6	CA	37	7F	00	00	00	00	00	00	00	00	UXB9!É7.....
0030h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0040h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0050h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0060h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0070h:	00	00	00	00	00	00	00	00	07	00	00	00	00	00	00	00
0080h:	20	22	8C	42	ED	3B	DB	64	3C	CD	D7	01	FF	FF	FF	FF	"@B1;Üd<I×.yyyy
0090h:	FF	FF	FF	FF	6D	00	00	00	00	00	00	00	00	00	00	00	yyym.....
00A0h:	14	00	6D	00	73	00	2D	00	67	00	61	00	6D	00	69	00	..m.s.-.g.a.m.i.
00B0h:	6E	00	67	00	6F	00	76	00	65	00	72	00	6C	00	61	00	n.g.o.v.e.r.l.a.
00C0h:	79	00	3A	00	2F	00	2F	00	2F	00	00	00	00	00	68	4E	y.:/././....hN
00D0h:	1B	D3	C0	13	07	D6	00	00	00	00	00	00	00	00	00	00	.0A..0.....

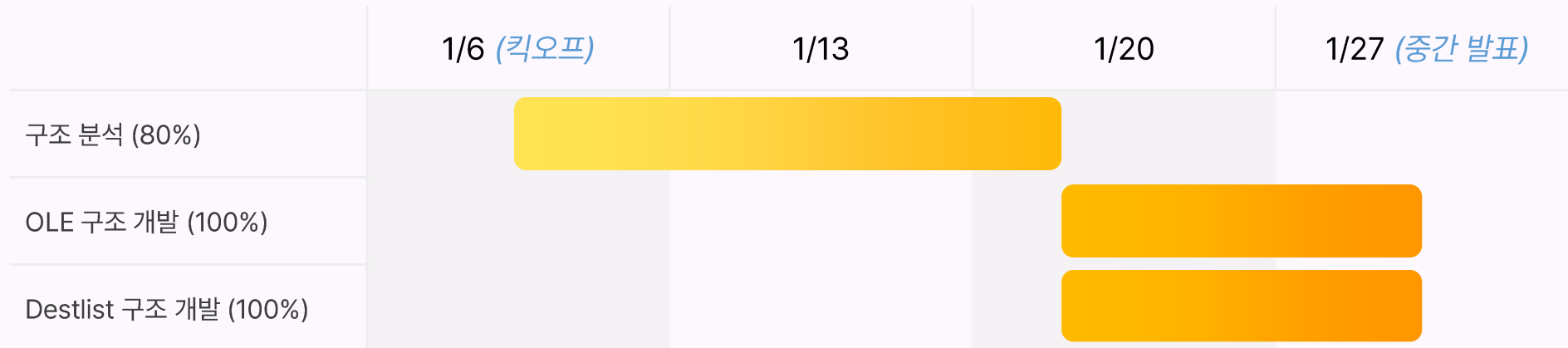
Template Results - DestlistHeader.bt

Name	Value
▼ struct FileHeader header	
enum Version version	Windows10 (4)
uint TotalNumberOfCurrentEntries	62
uint TotalNumberOfPinnedEntries	0
uint UnknownValue	1125515272
uint64 LastIssuedEntryIDNumber	62
uint64 NumberOfAddorDeleteorReOpenActions	297
▼ struct Win10_FileInformation FileInfo	
uint64 Checksum	9167018381820254425
> ubyte NewVolumeID[16]	
> ubyte NewObjectID[16]	
> ubyte BirthVolumeID[16]	



프로젝트 수행 과정

3 개발 진행 정도





향후 계획

Destlist 위치 찾기

LNK 반복하기



END

010 EDITOR



Question