바로가기 파일 포렌식

JK Kim

@pr0neer

forensic-proof.com

proneer@gmail.com

개요

1. 바로가기 파일 소개
2. 바로가기 파일 구조
3. 바로가기 파일 카빙
4. 바로가기 파일 분석

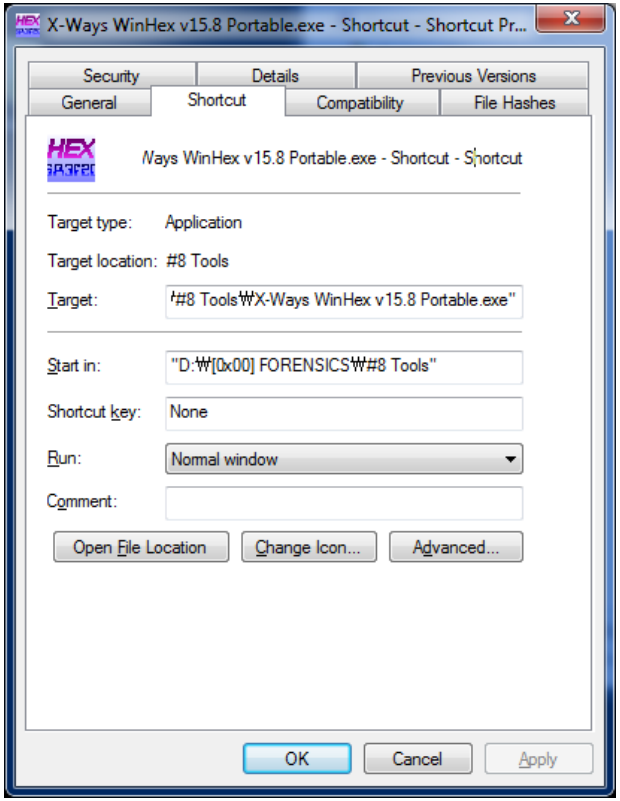
바로가기 파일 소개

Security is a people problem…

바로가기 파일 소개

바로가기 (링크파일)

- **바로가기 파일은?**
  - 링크 파일이라고도 불리며 영문 명칭은 "Windows Shortcut", 공식 명칭은 "Shell Link"
  - 윈도우에만 존재하는 기능으로 응용프로그램, 디렉터리, 파일 등의 객체를 참조하는 파일
  - 명령줄이 아닌 GUI에서만 동작
  - .lnk 확장자를 가짐



바로가기 파일 소개

바로가기 생성

- **윈도우 설치 시**
  - **시작 메뉴**
    - **XP** : C:₩Documents and Settings₩All Users₩Start Menu
    - **Vista/7** : C:₩Users₩Default₩AppData₩Roaming₩Microsoft₩Windows₩Start Menu
  - **관리자의 내 음악(My Music), 내 그림(My Pictures), 내 비디오(My Videos) 폴더**
    - **XP** : C:₩Documents and Settings₩Administrator₩My Documents₩ ➔ "All Users" 폴더를 링크
    - **Vista/7** : C:₩Users₩<username> ➔ "Public" 폴더를 링크

바로가기 생성

- **사용자 생성과 활동 (1)**
  - **시작 메뉴**
    - **XP** : C:₩Documents and Settings₩<username>₩Start Menu
    - **Vista/7** : C:₩Users₩<username>₩AppData₩Roaming₩Microsoft₩Windows₩Start Menu
  - **사용자의 내 음악(My Music), 내 그림(My Pictures), 내 비디오(My Videos) 폴더**
    - **XP** : C:₩Documents and Settings₩<username>₩Documents → "All Users" 폴더를 링크
    - **Vista/7** : C:₩Users₩<username> → "Public" 폴더를 링크
  - **최근 문서**
    - **XP** : C:₩Documents and Settings₩<username>₩Recent
    - **Vista/7** : C:₩Users₩<username>₩AppData₩Roaming₩Microsoft₩Windows₩Recent

바로가기 생성

- **사용자 생성과 활동 (2)**
  - **사용자별 바탕화면**
    - **XP** : C:₩Documents and Settings₩<username>₩Desktop
    - **Vista/7** : C:₩Users₩<username>₩Desktop
  - **Send To 폴더**
    - **Vista/7** : C:₩Users₩<username>₩AppData₩Roaming₩Microsoft₩Windows₩SendTo
  - **빠른 실행 (Quick Launch) 폴더**
    - **XP** : C:₩Documents and Settings₩<username>₩Application Data₩Microsoft₩Internet Explorer₩Quick Launch
    - **Vista/7** : C:₩Users₩<username>₩AppData₩Roaming₩Microsoft₩Internet Explorer₩Quick Launch

바로가기 파일 소개

바로가기 생성

- **응용프로그램 설치 시**
  - 응용프로그램 설치 시 **바탕화면, 시작 메뉴, 빠른 실행 폴더, 설치 폴더**에 바로가기 생성

- **사용자 직접 생성**
  - 사용자들도 필요에 따라 바로가기 생성

바로가기 파일 구조

Security is a people problem…

바로가기 구조

- **Shell Link Binary File Format**
  - **MS 공식 문서** - http://msdn.microsoft.com/en-us/library/dd871305(v=prot.13).aspx
  - **바로가기 파일 기본 구조**

구조 이름	설명
SHELL_LINK_HEADER (default)	식별 정보, 타임스탬프, 선택적인 구조의 존재 유무 플래그
LINKTARGET_IDLIST (optional)	ShellLinkHeader의 HasLinkTargetIDList 플래그가 설정되어 있을때만 존재하는 구조로, 링크 대상의 다양한 정보를 리스트 형태로 구성해놓은 구조
LINKINFO (optional)	ShellLinkHeader의 HasLinkInfo 플래그가 설정되어 있을때만 존재하는 구조로 링크 대상을 참조하기 위한 정보를 가진 구조
STRING_DATA (optional)	링크 대상의 문자열 정보(이름, 상대경로, 작업디렉터리 등)를 저장하는 구조로 ShellLinkHeader에 관련된 플래그가 설정되어 있을 때만 존재
EXTRA_DATA (optional)	링크 대상의 화면 표시 정보, 문자열 코드페이지, 환경 변수와 같은 추가적인 정보 저장을 위한 구조

바로가기 구조

- **SHELL_LINK_HEADER**

범위	크기	이름	설명
0 – 3	4 bytes	HeaderSize	헤더의 크기로 항상 0x0000004C(76) 값
4 – 19	16 bytes	LinkCLSID	클래스 식별자(class identifier)로 항상 00021401-0000-0000-C000-000000000046 값 (고정값)
20 – 23	4 bytes	LinkFlags	링크 대상의 다양한 정보에 대한 플래그
24 – 27	4 bytes	FileAttributes	링크 대상의 파일 속성 정보
28 – 35	8 bytes	CreationTime	링크 대상의 생성 시간
36 – 43	8 bytes	AccessTime	링크 대상의 접근 시간
44 – 51	8 bytes	WriteTime	링크 대상의 쓰기 시간
52 – 55	4 bytes	FileSize	링크 대상의 크기
56 – 59	4 bytes	IconIndex	아이콘 인덱스
60 – 63	4 bytes	ShowCommand	링크가 실행될 때응용프로그램 동작 모드
64 – 65	2 bytes	HotKey	응용프로그램을 바로 실행하기 위한 키보드 조합(핫키 정보)
66 – 75	10 bytes	Reserved	예약된 영역 (항상 0)

바로가기 구조

- **LINKTARGET_IDLIST**
  - 링크 대상의 정보를 리스트 형태로 구성해 놓은 구조
  - **IDList**
    - ItemIDSize
    - Data

struct LinkTargetIDList sLinkTargetIDList	
WORD IDListSize	387
struct IDList sIDList[0]	CLSID_MyComputer
WORD ItemIDSize	20
BYTE Type	31
BYTE Unknown	80 'P'
BYTE GUID[16]	àOÐ ê:i┼¢Ø
struct IDList sIDList[1]	
WORD ItemIDSize	25
BYTE Data[23]	/C:\
struct IDList sIDList[2]	
struct IDList sIDList[3]	
struct IDList sIDList[4]	
WORD TerminalID	0

바로가기 구조

- **LINKINFO**

범위	크기	이름	설명
0 – 3	4 bytes	LinkInfoSize	LinkInfo 구조체 크기
4 – 7	4 bytes	LinkInfoHeaderSize	LinkInfo Header section 크기, 보통 0x0000001C (28)
8 – 11	4 bytes	LinkInfoFlags	LinkInfo 플래그, 좌측 2비트만 사용
12 – 15	4 bytes	VolueIDOffset	VolumeID 위치
16 – 19	4 bytes	LocalBasePathOffset	LocalBasePath 위치 (링크 대상 경로)
20 – 23	4 bytes	CommonNetworkRelativeLinkOffset	Network volume info 위치
24 - 27	4 bytes	CommonPathSuffixOffset	CommonPathSuffix 위치
…	…	…	…

바로가기 구조

- **LINKINFO**

범위	크기	이름	설명
0 – 3	4 bytes	LinkInfoSize	LinkInfo 구조체 크기
4 – 7	4 bytes	LinkInfoHeaderSize	LinkInfo Header section 크기, 보통 0x0000001C (28)
8 – 11	4 bytes	LinkInfoFlags	LinkInfo 플래그, 좌측 2비트만 사용
12 – 15	4 bytes	VolueIDOffset	VolumeID 위치
…	…	…	…

  - **Volume ID**

범위	크기	이름	설명
0 – 3	4 bytes	VolumeIDSize	VolumeID 크기
4 – 7	4 bytes	DriveType	드라이브 형식 (이동형, 고정형, 네트워크 드라이브, CD-ROM, RAM Disk)
8 – 11	4 bytes	DriveSerialNumber	드라이브 시리얼 번호
12 – 15	4 bytes	VolumeLabelOffset	볼륨 레이블 위치
16 – 19	4 bytes	VolumeLabelOffsetUnicode	볼륨 레이블 위치 (유니코드)
20 -	가변	VolumeLabel	볼륨 레이블

바로가기 구조

- **STRING_DATA**
  - 바로가기 설명, 링크 대상까지의 상대 경로, 바로가기 활성화 시 작업 디렉터리 위치 저장

- **EXTRA_DATA**
  - 링크 대상에 대한 추가 정보
    - 콘솔에서 실행될 경우 디스플레이 설정 값
    - 코드 페이지 정보
    - 환경 변수 정보
    - 아이콘 위치 주소
    - NetBIOS 이름
    - MAC 주소
    - …

바로가기 구조

- **바로가기 파일의 디지털 포렌식적 의미**
  - **SHELL_LINK_HEADER**
    - 링크 대상 파일의 속성 (읽기 전용, 숨긴 파일, 시스템, 볼륨 레이블, 암호화, 압축 등)
    - 링크 대상 파일의 생성, 수정, 접근 시간
  - **LINKINFO**
    - 링크 대상 파일의 크기
    - 링크 대상 파일이 위치한 드라이브 형식
    - 링크 대상 파일이 위치한 드라이브 시리얼 번호
    - 링크 대상 파일의 경로
  - **EXTRA_DATA**
    - NetBIOS 이름
    - MAC 주소

바로가기 파일 카빙

Security is a people problem…

바로가기 파일 카빙

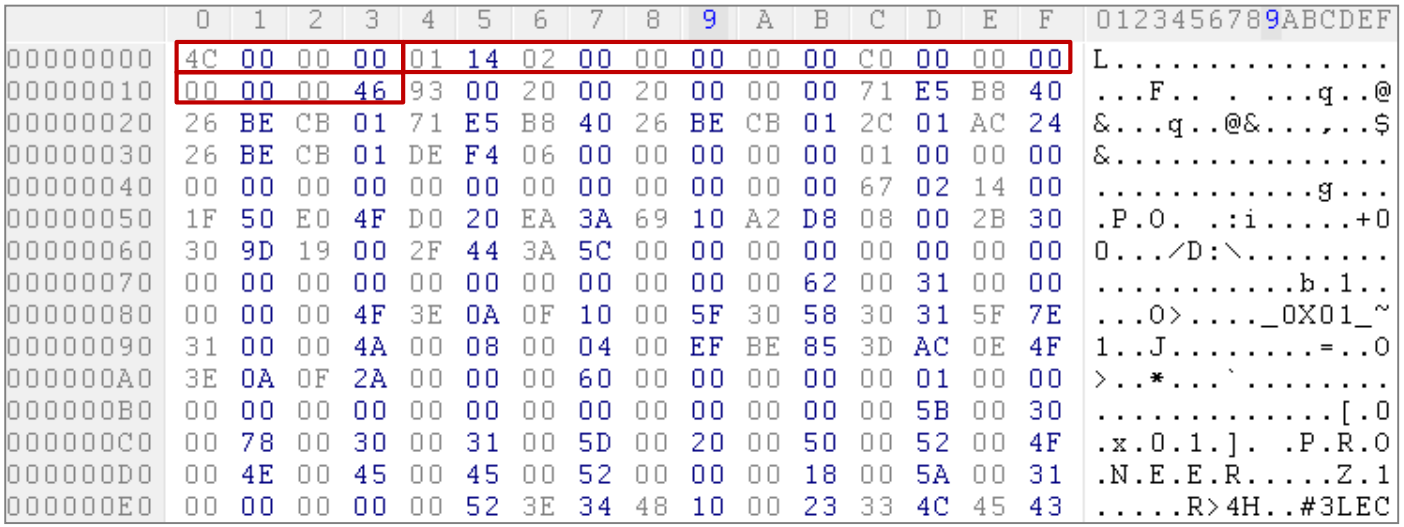
시그니처 카빙

- **카빙의 필요성**
  - 사용자의 필요에 의해 삭제 가능성
  - 최근 문서(Recent)의 경우 바로가기 파일 수 제한
    - **XP** : ??
    - **Vista/7** : 150개
  - 비할당 영역에 존재할 가능성이 많음

바로가기 파일 카빙

시그니처 카빙

- **SHELL_LINK_HEADER**
  - **HeaderSize** : 항상 0x0000004C
  - **LinkCLSID** : 바로가기 파일의 고정된 식별자로 값 동일
    - 00021401-0000-0000-C000-000000000046



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00000000	4C	00	00	00	01	14	02	00	00	00	00	00	C0	00	00	00	L.....
00000010	00	00	00	46	93	00	20	00	20	00	00	00	71	E5	B8	40	...F.. . ...q..@
00000020	26	BE	CB	01	71	E5	B8	40	26	BE	CB	01	2C	01	AC	24	&...q..@&...,..$
00000030	26	BE	CB	01	DE	F4	06	00	00	00	00	00	01	00	00	00	&.....
00000040	00	00	00	00	00	00	00	00	00	00	00	00	67	02	14	00	.....g...
00000050	1F	50	E0	4F	D0	20	EA	3A	69	10	A2	D8	08	00	2B	30	.P.O. .:i.....+0
00000060	30	9D	19	00	2F	44	3A	5C	00	00	00	00	00	00	00	00	0.../D:\.....
00000070	00	00	00	00	00	00	00	00	00	00	00	62	00	31	00	00	.....b.1..
00000080	00	00	00	4F	3E	0A	0F	10	00	5F	30	58	30	31	5F	7E	...O>...._0X01_~
00000090	31	00	00	4A	00	08	00	04	00	EF	BE	85	3D	AC	0E	4F	1..J.....=..O
000000A0	3E	0A	0F	2A	00	00	00	60	00	00	00	00	00	01	00	00	>..*...`.....
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	5B	00	30	.....[.0
000000C0	00	78	00	30	00	31	00	5D	00	20	00	50	00	52	00	4F	.x.0.1.]. .P.R.O
000000D0	00	4E	00	45	00	45	00	52	00	00	00	18	00	5A	00	31	.N.E.E.R.....Z.1
000000E0	00	00	00	00	00	52	3E	34	48	10	00	23	33	4C	45	43	.....R>4H..#3LEC

바로가기 파일 분석

Security is a people problem…

바로가기 파일 분석

바로가기 분석 도구

- **Windows LNK Parsing Utility (lp) –** https://tzworks.net/download_links.php
- **Lnkanalyser –** http://www.woanware.co.uk/forensics/lnkanalyser.html
- **Windows File Analyzer –** http://www.mitec.cz/wfa.html
- **010Editor – LNK Template –** http://www.sweetscape.com/010editor/
- **Lnk Analyzer –** http://www.tarasco.org/security/Lnk_Analyzer/

질문 및 답변