Windows Shortcut File format specification

Analysis of the Windows Shortcut File (LNK) format

By Joachim Metz <joachim.metz@gmail.com>

Summary

A Windows Shortcurt File is used by Microsoft Windows to link to files. This specification is based on earlier work on the format, the Shell Link Binary File Format specification [MS-SHLLINK] and was complimented by reverse engineering.

This document is intended as a working document for the Windows Shortcut File (LNK) format specification. Which should allow existing Open Source forensic tooling to be able to process this file type.

Document information

Author(s): Joachim Metz <joachim.metz@gmail.com>

Abstract: This document contains information about the Windows Shortcut File format.

Classification: Public

Keywords: Windows Shortcut File, LNK

License

Version

Version	Author	Date	Comments
0.0.1	J.B. Metz	September 2009	Initial version.
0.0.2	J.B. Metz	September 2009	Changes obtained by reversing the file format for the liblnk implementation.
0.0.3	J.B. Metz	June 2010	Moved Shell Items information to separate document.
0.0.4	J.B. Metz	July 2010	Changes regarding the extra data blocks.
0.0.5	J.B. Metz	September 2010	Fixed some typos.
0.0.6	J.B. Metz	September 2010	Textual changes
0.0.7	J.B. Metz	July 2011	License update
0.0.8	J.B. Metz	May 2012	Updates for Windows 8.
0.0.9	J.B. Metz	August 2012	Email change.
0.0.10	J.B. Metz	November 2012	Applied updates.
0.0.11	J.B. Metz	February 2013	Additional information about Windows 95 shortcut files.
0.0.12	J.B. Metz	March 2013	Fixed some typos.

Table of Contents

1. Overview

A Windows Shortcut File (LNK) is used by Microsoft Windows to link to files. The Windows Shortcut File format is also known as:

- The Shell Link Binary File format

A LNK consist of the following distinguishable elements:

- file header
- shell item identifiers list
- location information
- data strings
  - description
  - relative path
  - working directory
  - command line arguments
  - icon location
- extra data blocks
  - console properties
  - console codepage
  - Darwin properties
  - environment variables location
  - icon location
  - known folder location
  - metadata property store
  - shim layer properties
  - special folder location
  - distributed link tracker properties
  - vista (and later) shell item identifiers list properties

Characteristics	**Description**
Byte order	little-endian
Date and time values	in both UTC and local time
Character string	ASCII strings are stored in extended ASCII with a codepage. Unicode strings are stored in UTF-16 little-endian without the byte order mark (BOM).

1.1. Test version

The following version of programs were used to test the information within this document:

- Windows 95
- TODO: Windows 98
- TODO: Windows Me
- TODO Windows NT4
- Windows 2000
- Windows XP
- Windows 2003
- Windows Vista
- TODO: Windows 2008
- Windows 7

- Windows 8

2. File header

The file header is 76 bytes of size and consists of:

offset	size	value	description
0	4	0x0000004c (76)	The header size
4	16		The LNK class identifier GUID: {00021401-0000-0000-00c0-000000000046}
20	4		Data flags
24	4		File attribute flags See section: 7.1 File attribute flags
28	8		Creation date and time Filetime
36	8		Last access date and time Filetime
44	8		Last modification date and time Filetime
52	4		File size in bytes
56	4		Icon index value
60	4		ShowWindow value See section: 7.2 Show Window definitions
64	2		Hot key See section: 7.3 Hot Key definitions
66	2	0	Reserved
68	4	0	Reserved
72	4	0	Reserved

2.1. Data flags

The data flags consist of the following values:

Value	Identifier	Description
0x00000001	HasTargetIDList	The LNK file contains a link target identifier
0x00000002	HasLinkInfo	The LNK file contains location information
0x00000004	HasName	The LNK file contains a description data string
0x00000008	HasRelativePath	The LNK file contains a relative path data string
0x00000010	HasWorkingDir	The LNK file contains a working directory data string
0x00000020	HasArguments	The LNK file contains a command line arguments

Value	Identifier	Description
		data string
0x00000040	HasIconLocation	The LNK file contains a custom icon location
0x00000080	IsUnicode	The data strings in the LNK file are stored in Unicode (UTF-16 little-endian) instead of ASCII
0x00000100	ForceNoLinkInfo	The location information is ignored
0x00000200	HasExpString	The LNK file contains environment variables location data block
0x00000400	RunInSeparateProcess	A 16-bit target application is run in a separate virtual machine.
0x00000800		Reserved
0x00001000	HasDarwinID	The LNK file contains a Darwin (Mac OS-X) properties data block
0x00002000	RunAsUser	The target application is run as a different user.
0x00004000	HasExpIcon	The LNK file contains an icon location data block
0x00008000	NoPidlAlias	The file system location is represented in the shell namespace when the path to an item is parsed into the link target identifiers contains a known folder location data block ?
0x00010000		Reserved
Windows Vista and later?		
0x00020000	RunWithShimLayer	The target application is run with the shim layer. The LNK file contains shim layer properties data block.
0x00040000	ForceNoLinkTrack	The LNK does not contain a distributed link tracking data block
0x00080000	EnableTargetMetadata	The LNK file contains a metadata property store data block
0x00100000	DisableLinkPathTracking	The environment variables location block should be ignored
0x00200000	DisableKnownFolderTracking	Unknown
0x00400000	DisableKnownFolderAlias	
0x00800000	AllowLinkToLink	
0x01000000	UnaliasOnSave	
0x02000000	PreferEnvironmentPath	
0x04000000	KeepLocalIDListForUNCTarget	

Note that LNK files in Windows XP and earlier do not use the ForceNoLinkTrack flag.

3. Link target identifier

The link target identifier contains a (shell) item identifier list.

The data flags define if the link target identifier is present or not.

The link target identifier is variable of size and consists of:

offset	size	value	description
0	2		The size of the link target identifier shell item identifiers list
2	...		The shell item identifiers list See [LIBFWSI]

4. Location information

The data flags define if the (link) location information is present or not.

The location information is variable of size and consists of:

offset	size	value	description
0	4		The size of the location information including the 4 bytes of the size itself
Location information header			
4	4		Location information header size
8	4		Location flags
12	4		Offset to the volume information The offset is relative to the start of the location information
16	4		Offset to the local path The offset is relative to the start of the location information
20	4		Offset to the network share information The offset is relative to the start of the location information
24	4		Offset to the common path The offset is relative to the start of the location information
If location information header size > 28			
			Offset to the Unicode local path
If location information header size > 32			
			Offset to the Unicode common path
Location information data			
...	...		The volume information
...	...		The local path string

offset	size	value	description
			ASCII string terminated by an end-of-string character
...	...		The network share information
...	...		The common path ASCII string terminated by an end-of-string character
If location information header size > 28			
...	...		The Unicode local path string Unicode string terminated by an end-of-string character
If location information header size > 32			
...	...		The Unicode common path Unicode string terminated by an end-of-string character

The full filename can be determined by:

- combining the local path and the common path
- combining the network share name (in the network share information) with the common path

Note that the network share name is not necessarily terminated by a path separator. Currently it is assumed that the same applies to the local path. Also the file can contain an empty common path where the local path contains the full path.

Although [MS-SHLLINK] states that when the CommonNetworkRelativeLinkAndPathSuffix location flag is not set the offset to the network share information should be zero, the value can still be set, but is not necessarily valid. This behavior was seen on Windows95.

4.1. Location flags

The location flags consist of the following values:

Value	Identifier	Description
0x0001	VolumeIDAndLocalBasePath	The linked file is on a volume If set the volume information and the local path contain data
0x0002	CommonNetworkRelativeLinkAndPathSuffix	The linked file is on a network share If set the network share information and common path contain data

4.2. Volume information

The volume information is variable of size and consists of:

offset	size	value	description
Volume information header			

offset	size	value	description
0	4		The size of the volume information including the 4 bytes of the size itself
4	4		Drive type
8	4		Drive serial number
12	4		Offset to the volume label The offset is relative to the start of the volume information
Offset to the volume label > 16			
16	4		Offset to the Unicode volume label The offset is relative to the start of the volume information
Volume information data			
...	...		The volume label ASCII string terminated by an end-of-string character
...	...		The Unicode volume label Unicode string terminated by an end-of-string character

4.2.1. Drive types

This drive type consist of one of the following values:

Value	Identifier	Description
0	DRIVE_UNKNOWN	Unknown
1	DRIVE_NO_ROOT_DIR	No root directory
2	DRIVE_REMOVABLE	Removable storage media (floppy, usb)
3	DRIVE_FIXED	Fixed storage media (harddisk)
4	DRIVE_REMOTE	Remote storage
5	DRIVE_CDROM	Optical disc (CD-ROM, DVD, BD)
6	DRIVE_RAMDISK	RAM drive

4.3. Network share information

The network share information is variable of size and consists of:

offset	size	value	description
Network share information header			
0	4		The size of the network share information
4	4		Network share flags
8	4		Offset to the network share name The offset is relative to the start of the

offset	size	value	description
			network share information
12	4		Offset to the device name The offset is relative to the start of the network share information
16	4		Network provider type
Offset to the network share name > 20			
20	4		Offset to the Unicode network share name The offset is relative to the start of the network share information
24	4		Offset to the Unicode device name The offset is relative to the start of the network share information
Network share information data			
...	...		The network share name ASCII string terminated by an end-of-string character
...	...		The device name ASCII string terminated by an end-of-string character
...	...		The Unicode network share name Unicode string terminated by an end-of-string character
...	...		The Unicode device name Unicode string terminated by an end-of-string character

Note that the network share name is not necessarily terminated by a path separator.

4.3.1. Network share flags

The network share flags consist of the following values:

Value	Identifier	Description
0x0001	ValidDevice	If set the device name contains data
0x0002	ValidNetType	If set the network provider type contains data

4.3.2. Network provider types

The network provider types consist of one of the following values:

Value	Identifier	Description
0x001a0000	WNNC_NET_AVID	

Value	Identifier	Description
0x001b0000	WNNC_NET_DOCUSPACE	
0x001c0000	WNNC_NET_MANGOSOFT	
0x001d0000	WNNC_NET_SERNET	
0x001e0000	WNNC_NET_RIVERFRONT1	
0x001f0000	WNNC_NET_RIVERFRONT2	
0x00200000	WNNC_NET_DECORB	
0x00210000	WNNC_NET_PROTSTOR	
0x00220000	WNNC_NET_FJ_REDIR	
0x00230000	WNNC_NET_DISTINCT	
0x00240000	WNNC_NET_TWINS	
0x00250000	WNNC_NET_RDR2SAMPLE	
0x00260000	WNNC_NET_CSC	
0x00270000	WNNC_NET_3IN1	
0x00290000	WNNC_NET_EXTENDNET	
0x002a0000	WNNC_NET_STAC	
0x002b0000	WNNC_NET_FOXBAT	
0x002c0000	WNNC_NET_YAHOO	
0x002d0000	WNNC_NET_EXIFS	
0x002e0000	WNNC_NET_DAV	
0x002f0000	WNNC_NET_KNOWARE	
0x00300000	WNNC_NET_OBJECT_DIRE	
0x00310000	WNNC_NET_MASFAX	
0x00320000	WNNC_NET_HOB_NFS	
0x00330000	WNNC_NET_SHIVA	
0x00340000	WNNC_NET_IBMAL	
0x00350000	WNNC_NET_LOCK	
0x00360000	WNNC_NET_TERMSRV	
0x00370000	WNNC_NET_SRT	
0x00380000	WNNC_NET_QUINCY	
0x00390000	WNNC_NET_OPENAFS	
0x003a0000	WNNC_NET_AVID1	
0x003b0000	WNNC_NET_DFS	
0x003c0000	WNNC_NET_KWNP	
0x003d0000	WNNC_NET_ZENWORKS	

Value	Identifier	Description
0x003e0000	WNNC_NET_DRIVEONWEB	
0x003f0000	WNNC_NET_VMWARE	
0x00400000	WNNC_NET_RSFX	
0x00410000	WNNC_NET_MFILES	
0x00420000	WNNC_NET_MS_NFS	
0x00430000	WNNC_NET_GOOGLE	

5. Data strings

Dependent on the flags in the file header the following data strings are present or not. They are stored in the following order directly after the location information:

- description
- relative path
- working directory
- command line arguments
- icon location

A data string is variable of size and consists of:

offset	size	value	description
0	2		The number of characters in the string
2	...		The string ASCII or Unicode string

6. Extra data

The extra data is variable of size and consists of:

offset	size	value	description
0	...		Extra data blocks
...	4	0	Terminal block Signifies the end of the extra data blocks

The extra data consist of extra data blocks terminated by the terminal block (an empty extra data block).

The extra data blocks are stored in the following order directly after the last data string:

- console properties
- console codepage
- Darwin properties
- environment variables location
- icon location
- known folder location
- metadata property store
- shim layer properties

- special folder location
- distributed link tracker properties
- Vista (and later) shell item identifiers list properties

Note that not all extra data blocks are controlled by the data flags in the file header.

6.1. The environment variables location data block

The environment variables location data block is 788 bytes of size and consists of:

offset	size	value	description
0	4	0x00000314 (788)	Size of the data Includes 4 bytes of the size
4	4	0xa0000001	The extra block signature
8	260		Environment variables location ASCII string terminated by an end-of-string character Unused bytes can contain remnant data
268	520		Unicode environment variables location Unicode string terminated by an end-of-string character Unused bytes can contain remnant data

The environment variables location contains the path to the environment variables information.

6.2. The console properties data block

The console properties data block is 204 bytes of size and consists of:

offset	size	value	description
0	4	0x000000cc (204)	Size of the data Includes 4 bytes of the size
4	4	0xa0000002	The extra block signature
8	2		Color flags
10	2		Pop-up fill attributes
12	2		Screen width buffer size
14	2		Screen height buffer size
16	2		Window width
18	2		Window height
20	2		Window origin x-coordinate
22	2		Window origin y-coordinate
24	4	0	Reserved
28	4	0	Reserved
32	4		Font size

offset	size	value	description
36	4		Font family value
40	4		Font weight value < 700 (regular) value >= 700 (bold)
44	64		Face name Unicode string terminated by an end-of-string character
108	4		Cursor size value <= 25 (small) [26, 50] (normal) [51, 100] (large)
112	4		Full screen A value of 0 represents windowed-mode another value full screen mode
116	4		Insert mode A value of 0 represents insert mode is disabled another value enabled
120	4		Automatic positioning A value of 0 represents automatic positioning is disabled another value enabled. When automatic positioning is off the window origin x and y-coordinates are used to position the window.
124	4		History buffer size
128	4		Number of history buffers
132	4		Duplicates allowed in history A value of 0 represents that duplicates are not allowed in the history another value otherwise.
136	64		Color table

6.2.1. Console color flags

The console color flags consist of the following values:

Value	Identifier	Description
0x0001	FOREGROUND_BLUE	The color of the text is blue
0x0002	FOREGROUND_GREEN	The color of the text is green
0x0004	FOREGROUND_RED	The color of the text is red
0x0008	FOREGROUND_INTENSITY	The color of the text is intensified
0x0010	BACKGROUND_BLUE	The color of the background is blue
0x0020	BACKGROUND_GREEN	The color of the background is green

Value	Identifier	Description
0x0040	BACKGROUND_RED	The color of the background is red
0x0080	BACKGROUND_INTENSITY	The color of the background is intensified

6.2.2. Console font family value

The console font family value consist of the following values:

Value	Identifier	Description
0x0000	FF_DONTCARE	Unknown font
0x0010	FF_ROMAN	Variable-width font with serifs
0x0020	FW_SWISS	Variable-width font without serifs
0x0030	FF_MODERN	Fixed-width font with or without serifs
0x0040	FF_SCRIPT	Handwriting like font
0x0050	FF_DECORATIVE	Novelty font

6.3. The distributed link tracker properties data block

The distributed link tracker properties data block is 96 bytes of size and consists of:

offset	size	value	description
0	4	0x00000060 (96)	Size of the data Includes 4 bytes of the size
4	4	0xa0000003	The extra block signature
8	4	88	Size of the distributed link tracker data
12	4	0	Version of the distributed link tracker data
16	16		Machine identifier string ASCII string terminated by an end-of-string character Unused bytes are set to 0
32	16		Droid volume identifier GUID containing an NTFS object identifier
48	16		Droid file identifier GUID containing an NTFS object identifier
64	16		Birth droid volume identifier GUID containing an NTFS object identifier
80	16		Birth droid file identifier GUID containing an NTFS object identifier

The droid volume identifier can be found in the NTFS $OBJECT_ID attribute of the $Volume file system metadata file. The LSB in the droid volume identifier contains the cross volume move flag. This flag is set if a file is moved across volumes.

The droid file identifier can be found in the NTFS $OBJECT_ID attribute of the corresponding file.

6.4. The console codepage data block

The console codepage data block is 12 bytes of size and consists of:

offset	size	value	description
0	4	0x0000000c (12)	Size of the data Includes 4 bytes of the size
4	4	0xa0000004	The extra block signature
8	4		Codepage

6.4.1. Console codepage value

The console codepage value consist of the following values:

Value	Identifier	Description

TODO

6.5. The special folder location data block

The special folder location data block is 16 bytes of size and consists of:

offset	size	value	description
0	4	0x00000010 (16)	Size of the data Includes 4 bytes of the size
4	4	0xa0000005	The extra block signature
8	4		Special folder identifier
12	4		First child segment offset

The first child segment offset refers to the location of the (shell) item identifier of the first child segment of the (shell) item identifiers list specified by the known folder identifier. The offset contains the number of bytes relative from the start of the (shell) item identifiers list.

6.6. The Darwin properties data block

The Darwin properties data block is 788 bytes of size and consists of:

offset	size	value	description
0	4	0x00000314 (788)	Size of the data Includes 4 bytes of the size

offset	size	value	description
4	4	0xa0000006	The extra block signature
8	260		Darwin application identifier ASCII string terminated by an end-of-string character Unused bytes are set to 0
268	520		Unicode Darwin application identifier Unicode string terminated by an end-of-string character Unused bytes are set to 0

6.7. The icon location data block

The icon location data block is 788 bytes of size and consists of:

offset	size	value	description
0	4	0x00000314 (788)	Size of the data Includes 4 bytes of the size
4	4	0xa0000007	The extra block signature
8	260		Icon location ASCII string terminated by an end-of-string character Unused bytes can contain remnant data
268	520		Unicode icon location Unicode string terminated by an end-of-string character Unused bytes can contain remnant data

The icon location contains the path to the icon information which includes the use of environment variables.

6.8. The shim layer properties data block

The shim is an intermediate layer and was added in Windows Vista.

The shim layer properties data block is variable of size and consists of:

offset	size	value	description
0	4		Size of the data Includes 4 bytes of the size Value => 136
4	4	0xa0000008	The extra block signature
8	...		Name of the shim layer Unicode string terminated by an end-of-string character Unused bytes are set to 0

6.9. The metadata property store data block

The metadata property store data block is variable of size and consists of:

offset	size	value	description
0	4		Size of the data Includes 4 bytes of the size Value >= 12
4	4	0xa0000009	The extra block signature
8	...		Property store

6.9.1. Property store (aka shell property sheet list)

The property store is variable of size and consists of:

offset	size	value	description
0	4		Size of the property store
4	...		The serialized property storages
...	4	0	Terminal identifier Signifies the end of the property store

The last serialized property storage should be of size 0 to terminate the property store.

6.9.2. Serialized property storage (aka Shell property sheet)

The serialized property storage is variable of size and consists of:

offset	size	value	description
0	4		Size of the serialized property storage
4	4	“1SPS” 0x53505331	Version (Serialized property storage version 1)
8	16		Format class identifier GUID
24	...		Serialized property value
...	4	0	Terminal identifier Signifies the end of the serialized property storage

The last serialized property value should be of size 0 to terminate the serialized property storage.

A format class identifier of {d5cdd505-2e9c-101b-9397-08002b2cf9ae} signifies all the serialized property values are serialized named property values otherwise all values should be serialized numeric property values.

6.9.3. Serialized numeric property value (aka numeric shell property)

The serialized numeric property value is variable of size and consists of:

offset	size	value	description
0	4		Size of the serialized property value
4	4		Identifier
8	1	0x00	Reserved
9	...		Typed property value

6.9.4. Serialized name property value (aka named shell property)

The serialized name property value is variable of size and consists of:

offset	size	value	description
0	4		Size of the serialized property value
4	4		Name size
8	1	0x00	Reserved
9	...		Name string Unicode string terminated by an end-of-string character
...	...		Typed property value

6.9.5. Typed property value

See document containing OLE property type (PROPVARIANT) definition.

6.10. The known folder location data block

The known folder data block is 28 bytes of size and consists of:

offset	size	value	description
0	4	0x0000001c (28)	Size of the data Includes 4 bytes of the size
4	4	0xa000000b	The extra block signature
8	16		Known folder identifier Contains a GUID
24	4		First child segment offset

The first child segment offset refers to the location of the (shell) item identifier of the first child segment of the (shell) item identifiers list specified by the known folder identifier. The offset contains the number of bytes relative from the start of the (shell) item identifiers list.

6.11. The shell item identifiers list data block

The shell item identifiers list data block was added in Windows Vista.

The shell item identifiers list data block is variable of size and consists of:

offset	size	value	description
0	4		Size of the data Includes 4 bytes of the size Value >= 10
4	4	0xa000000c	The extra block signature
8	...		The shell item identifiers list See [LIBFWSI]

7. Windows definitions

7.1. File attribute flags

The file attribute flags consist of the following values:

Value	Identifier	Description
0x00000001	FILE_ATTRIBUTE_READONLY	Is read-Only
0x00000002	FILE_ATTRIBUTE_HIDDEN	Is hidden
0x00000004	FILE_ATTRIBUTE_SYSTEM	Is a system file or directory
0x00000008		Reserved, not used by the LNK format Is a volume label
0x00000010	FILE_ATTRIBUTE_DIRECTORY	Ia s directory
0x00000020	FILE_ATTRIBUTE_ARCHIVE	Should be archived
0x00000040	FILE_ATTRIBUTE_DEVICE	Reserved, not used by the LNK format Is a device
0x00000080	FILE_ATTRIBUTE_NORMAL	Is normal None of the other flags should be set
0x00000100	FILE_ATTRIBUTE_TEMPORARY	Is temporary
0x00000200	FILE_ATTRIBUTE_SPARSE_FILE	Is a sparse file
0x00000400	FILE_ATTRIBUTE_REPARSE_POINT	Is a reparse point or symbolic link
0x00000800	FILE_ATTRIBUTE_COMPRESSED	Is compressed
0x00001000	FILE_ATTRIBUTE_OFFLINE	Is offline The data of the file is stored on an offline storage.
0x00002000	FILE_ATTRIBUTE_NOT_CONTENT_INDEXED	Do not index content The content of the file or directory should not be indexed by the indexing service.
0x00004000	FILE_ATTRIBUTE_ENCRYP	Is encrypted

Value	Identifier	Description
	TED	
0x00008000		Unknown (seen on Windows 95 FAT)
0x00010000	FILE_ATTRIBUTE_VIRTUAL	Currently reserved for future use, not used by the LNK format Is virtual

7.2. Show Window definitions

The Show Window value contains a value used by the ShowWindow function. This value consist of one of the following values:

Value	Identifier	Description
0	SW_HIDE	Hides the window and activates another window.
1	SW_NORMAL SW_SHOWNORMAL	Activates and displays the window. The window is restored to its original size and position if the window is minimized or maximized.
2	SW_SHOWMINIMIZED	Activates and minimizes the window.
3	SW_MAXIMIZE SW_SHOWMAXIMIZED	Activates and maximizes the window.
4	SW_SHOWNOACTIVATE	Display the window in its most recent position and size without activating it.
5	SW_SHOW	Activates the window and displays it in its current size and position.
6	SW_MINIMIZE	Minimizes the window and activates the next top-level windows (in order of depth (Z order))
7	SW_SHOWMINNOACTIVE	Display the window as minimized without activating it.
8	SW_SHOWNA	Display the window in its current size and position without activating it.
9	SW_RESTORE	Activates and displays the window. The window is restored to its original size and position if the window is minimized or maximized.
10	SW_SHOWDEFAULT	Set the show state based on the ShowWindow values specified during the creation of the process.
11	SW_FORCEMINIMIZE	Minimizes a window, even if the thread that owns the window is not responding.
0xcc	SW_NORMALNA	Undocumented according to wine project

7.3. Hot Key definitions

The Hot Key values consists of 2 bytes each bytes contains part of the corresponding hot key.

7.3.1. Lower HotKey byte value

Value	Identifier	Description
0x30 – 0x39		Numeric keys 0 - 9
0x41 – 0x5a		Upper case alphabetical keys A- Z
0x70	VK_F1	Function key 1
0x71	VK_F2	Function key 2
0x72	VK_F3	Function key 3
0x73	VK_F4	Function key 4
0x74	VK_F5	Function key 5
0x75	VK_F6	Function key 6
0x76	VK_F7	Function key 7
0x77	VK_F8	Function key 8
0x78	VK_F9	Function key 9
0x79	VK_F10	Function key 10
0x7a	VK_F11	Function key 11
0x7b	VK_F12	Function key 12
0x7c	VK_F13	Function key 13
0x7d	VK_F14	Function key 14
0x7e	VK_F15	Function key 15
0x7f	VK_F16	Function key 16
0x80	VK_F17	Function key 17
0x81	VK_F18	Function key 18
0x82	VK_F19	Function key 19
0x83	VK_F20	Function key 20
0x84	VK_F21	Function key 21
0x85	VK_F22	Function key 22
0x86	VK_F23	Function key 23
0x87	VK_F24	Function key 24
0x90	VK_NUMLOCK	Num lock key
0x91	VK_SCROLL	Scroll lock key

7.3.2. Upper HotKey byte value

Value	Identifier	Description
0x01	HOTKEYF_SHIFT	The shift key
0x02	HOTKEYF_CONTROL	The control key
0x04	HOTKEYF_ALT	The alt key

Appendix A. References

[PARSONAGE08]
Title: The Meaning of Linkfiles In Forensic Examinations
Author(s): Harry Parsonage
Date: September 2008
URL: http://computerforensics.parsonage.co.uk/downloads/TheMeaningofLIFE.pdf

[HAGER]
Title: The Windows Shortcut File Format
Author(s): Jesse Hager
URL: http://www.i2s-lab.com/Papers/The_Windows_Shortcut_File_Format.pdf

[MSDN]
Title: Microsoft Developer Network
URL: http://msdn.microsoft.com/

[MS-PROPERTSTORE]
Title: [MS-PROPERTSTORE] Property Store Binary File Format
URL: http://msdn.microsoft.com/
Date: August 12, 2009

[MS-SHLLINK]
Title: [MS-SHLLINK] Shell Link (.LNK) Binary File Format
URL: http://msdn.microsoft.com/
Date: August 12, 2009

[LIBFWSI]
Title: Windows Shell Item format
Author(s): Joachim Metz
URL: http://code.google.com/p/liblnk/downloads/detail?name=Windows%20Shell%20Item%20format.pdf
Date: June 2010

Appendix B. GNU Free Documentation License

Version 1.3, 3 November 2008

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of

transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The "publisher" means any person or entity that distributes copies of the Document to the public.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the

Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

- N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS
A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION
Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION
You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. FUTURE REVISIONS OF THIS LICENSE
The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. RELICENSING

"Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.