Sarah Lowman 2012

Link Files Cheat Sheet

Background

The Windows Shortcut file has the extension .lnk. It is a metadata file, specific for the Microsoft Windows platform and is interpreted by the Windows Shell. The file format indicates that these files contain a specific signature, `0x4C (4C 00 00 00)` at offset 0 within the file.

My Recent Documents Locations

`C:\Documents and Settings\UserName\Recent` and

`C:\Documents and Settings\UserName\Application Data\Microsoft\Office\Recent`

My Recent Documents Listed?

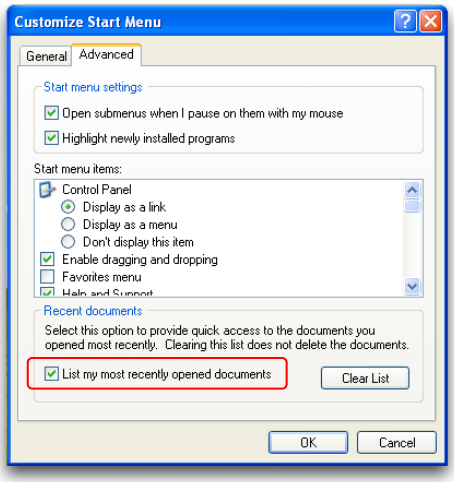
`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced`

`Start_ShowRecentDocs = 0` indicates the option to list Recent Documents is unchecked

`Start_ShowRecentDocs = 2` indicates the option is checked

A registry setting can be used to prevent members of a file class being added to the Recent Items list. An `EditFlags` value `0x00100000` can be set for the file association ProgID key in `HKEY_CLASSES_ROOT`.

Name	Type	Data
(Default)	REG_SZ	Microsoft Common Console Document
EditFlags	REG_DWORD	0x00100000 (1048576)
FriendlyTypeName	REG_EXPAND_SZ	@%SystemRoot%\system32\mmcbase.dll,-130



Time Stamps

As well as Created, Accessed and Modified dates of the link file; at the time a target file is opened, the Created, Accessed and Modified dates of the target file are read and **stored within the associated link file** at offset `0x1C`. Each date is recorded in the FILETIME data type in 8 bytes.

Link file Creation Date	When a target file is opened and a link file is created, the created date of the link file remains the date that target file was first accessed during the lifetime of that link file.
Link file Modified Date	The Modified Date of the link file represents the time when the related target file was last opened (as opposed to when it was closed).
Link file Accessed Date	Where the Created, Accessed and Modified dates of the link file are the same, this indicates that the target file has not been opened since that time.
No Embedded Dates	Where a new file has been created in an application and then saved from it, and a link file has been created, the link file will not contain any embedded dates relating to the target file.
Embedded Modified Date	The Link File internal Modified and Accessed Dates reflect the Target File properties at the time the Target File was last opened.

Note

Once a link file has been created for a target file with a given filename, during the lifetime of that link file, if **another target file of the same name** is accessed from a different location, the **original link file** for that given filename is updated

The exception is in the case of files saved by Microsoft Office applications (2003 & 2007). When a file is created in an Office application and it is first saved, a link file is created in both the user's Recent folder and Office Recent folder. The link file in the Office Recent folder appears to always contain embedded dates when it is first created but the one in the Recent folder contains no embedded dates.

Other data in Link files

- The Shell Item list of the target [Path of target]
- The size of the target when it was last accessed
- Serial number of the volume where the target was stored
- Network volume share name
- Read-only, hidden, system, volume label, encryption, sparse, compressed, offline and several other target attributes
- MAC address of the host computer (sometimes)
- Distributed link tracking information

Sources and Further Reading

http://computerforensics.parsonage.co.uk/downloads/TheMeaningofLIFE.pdf

http://www.forensicswiki.org/wiki/LNK

http://www.forensicfocus.com/link-file-evidentiary-value

http://forensicsfromthesausagefactory.blogspot.co.uk/2009/07/link-files-within-system-restore-points.html