lnkanalyser

Info

Windows shortcut (LNK) files hold a wealth of useful information for forensic investigators. There are a number of LNK file parsers out there, and most are ok, some are incorrect and some just don't get enough information extracted e.g. UUID parsing. Microsoft have now released the binary file format (see below) which makes it a lot easier to get things right.

Another key source of information I have used is Harry Parsonage's The Meaning of Life presentation/research. The research explains some of the more obscure information stored in LNK files, such as being able to detect whether a file has been moved from one volume to another, including sometimes the MAC address of primary network card of the host computer, along with an incrementing boot sequence number, so you can use it to check the order that LNK files are created.

Links

- MS LNK Binary Format: https://msdn.microsoft.com/en-us/library/dd871305(PROT.10).aspx
- Harry Parsonage: http://computerforensics.parsonage.co.uk/downloads/TheMeaningofLIFE.pdf

Download

- v1.0.1