DFIR Review

Windows 10 Jump List and Link File Artifacts - Saved, Copied and Moved

Larry Jones

Published on: Sep 25, 2020

License: [Creative Commons Attribution 4.0 International License \(CC-BY 4.0\)](https://creativecommons.org/licenses/by/4.0/)

Synopsis

Forensic question: Are link file and jump list artifacts changed for Windows 10?
OS: Windows 10 Pro version 1903
Tools: Magnet Forensics AXIOM version 4.0.1.19617	

Background

Since Windows 7, Jump Lists and LNK Files have been a valuable source for computer user activity to forensic investigators.

Windows users can create shortcut files on the systems they use. A shortcut file is a small file which has information used to access or point to another file (Lee, FOR500 Windows Forensic Analysis Textbook, Volume 3 Core Windows Forensics II: USB Devices and Shell Items 2018, 8). Shortcut files are most often referred to as **Link** files by forensic analysts based on their **.lnk** file extension. In addition to user created LNK files, the Windows operating system automatically creates LNK files when a user opens a non-executable file or document. Windows creates these LNK files on a frequent basis and their creation is performed in the background without the explicit knowledge of the user. Within a LNK file, Windows records several pieces of information about the **target file** of which the LNK file is designed to access (13Cubed 2017). Some of these pieces of information include:

- The original file system path where the target file is stored.
- Timestamps for both the target file and the LNK file itself.
- The size of the target file.
- The Attributes associated with the target file (i.e. read-only, hidden, archive, etc.).

- The system name, volume name, volume serial number, and sometimes the MAC address of the system where the target is stored.
- Whether the target is stored on a local or remote system.

LNK files are user profile specific in that LNK files are recorded per user on the system. Windows generated LNK files are stored in the folder C:\Users\
<username>\AppData\Roaming\Microsoft\Windows\Recent.

The information contained in LNK files are invaluable to forensic analysts in investigating user file activity (FOR500 Windows Forensic Analysis Textbook, Volume 3 Core Windows Forensics II: USB Devices and Shell Items 2018, 13) including:

- A USB investigation to identify files opened from a specific removable USB device but never saved locally to the system.
- The user knowledge of specific files opened whether those files were stored on the local system, attached removable devices, or network storage.
- The identification of files which no longer exist on a local machine. While a deleted file which was previously opened (generating a LNK file) on the system no longer exists, the system may retain the LNK file recorded to access the deleted file.

Jump Lists were introduced with the release of Windows 7. Jump Lists are automatically created by Windows to allow users to 'jump to' or access items they frequently or recently accessed. Jump Lists are software application specific in that they record files opened from a specific software application. To access a Jump List, the user would right-click the software application from the task bar (i.e. Microsoft Word) and a list of recent documents associated with the software application would be displayed (SANS Forensics 408 Windows Forensic Analysis Volume 4, Core Windows Forensics Part III 2014, 25). There are two variations of Jump Lists – Automatic Destinations and Custom Destinations.

Automatic Destinations contain features which are common across all software applications. Automatic Destinations contain the file extension .automaticDestinations-ms. Automatic Destinations are compound files which contain multiple data streams within the single file. Within Automatic Destinations, each stream contains an embedded LNK entry which can be extracted and parsed. The **DestList** stream acts as a Most Recent Used (MRU) list for files opened from the software application (13Cubed 2017).

Custom Destinations have application specific features which can vary based on the developer's decision to implement the features. Custom Destinations have the file extension .customDestinations-ms. Custom Destinations can also contain a series of LNK entries for files opened using the software application (13Cubed 2017).

Jump Lists are associated with software applications through Application IDs (**App IDs**). AppIDs are unique identifiers which are universal across all Windows systems (SANS Forensics 408 Windows Forensic Analysis Volume 4, Core Windows Forensics Part III 2014, 27-28). All that is required of the forensic analyst is to determine the software application associated with a Jump List AppID. For example, Microsoft Excel 2010 is associated with AppID 9839aec31243a928. The Automatic Destinations Jump List for Microsoft Excel 2010 would be 9839aec31243a928.automaticDestinations-ms.

Jump Lists are also user specific and are valuable to forensic analysts to identify user file activity. Jump Lists are stored in sub-folders of the user's Recent folder previously identified as storing LNK files (C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Recent). Automatic Destinations are stored in the sub-folder AutomaticDestinations and Custom Destinations are stored in the sub-folder CustomDestinations.

Since the inception of Jump Lists in Windows 7, the behavior of LNK files and the DestList stream within Jump Lists have been similar. When a user opened a file such as MyDoc.docx using Microsoft Word, a LNK File was recorded (or updated if previously opened) for the opened file, and the Jump List DestList stream for Microsoft Word would record an entry (or update the entry if previously opened) for the opened file. Forensic analysts could use these two Windows generated artifacts to document user file activity. Generally, LNK Files and the Jump List DestList stream contained similar data, especially for recent user file activity. LNK files did have a maximum number of files which could be stored in the Recent folder (FOR500 Windows Forensic Analysis Textbook, Volume 3 Core Windows Forensics II: USB Devices and Shell Items 2018, 12). Once this maximum number was reached, newly created LNK files would replace the oldest LNK files within the user's Recent folder. The Jump List DestList stream had the capacity to store LNK entries beyond the LNK file maximum file limit. By comparison, the LNK file maximum file storage limit caused LNK files to potentially store less user file activity than Jump Lists. This limitation only effected older LNK files since they were removed from the Recent folder once the maximum file limitation was reached.

In some of my recent digital forensic investigations involving user file activity, my investigations have focused on systems where the Windows 10 operating system was installed. In these user file activity investigations, I began noticing a disparity in the number of LNK files when compared to the Jump List DestList entries. As previously stated, the analysis of LNK files and Jump List entries on Windows 7 systems produced very similar results. My recent Windows 10 investigations of user file activity were beginning to identify a higher number of Jump List entries when compared to the LNK files found on the system. My initial assumption and explanation to this disparity was that the LNK files had reached their maximum capacity in the user's Recent folder. Upon further comparison of Jump List DestList timestamps with LNK file timestamps, this assumption proved inaccurate. Analysis matched the active LNK files on the system with corresponding entries within the various Jump Lists; however, Jump List

entries were present where there was not a corresponding LNK file, and the timestamps for the Jump List entries post-dated the timestamps of the LNK files. Four commonalities were identified in the Jump List entries where there was no corresponding LNK file:

1. Many of the Jump List entries were contained in the Windows Explorer Jump List (AppID f01b44d95cf55d32a);
2. Almost exclusively, the Windows Explorer Jump List entries identified folders and not files; and
3. The MRU timestamps for the Jump List entries were in close proximity – within one or two minutes.
4. Jump List entries were identified for an AppID previously not seen – 5f7b5f1e01b83767. As seen later in the testing results, this AppID was associated with the new Windows 10 feature Quick Access.

Research

Based on the observed changes for LNK files and Jump Lists between Windows 7 and Windows 10, I began research to identify the source of these changes. I consulted several previously published papers concerning the forensic value of LNK files and Jump Lists. Some of these papers include The Meaning of Linkfiles In Forensic Examinations (Parsonage Updated July 2010); Jump List Forensics (Antonovich April 2014); and A Forensic Insight Into Windows 10 Jump Lists (Singh 2016). Several of the sources used in my research were informative and described in detail the structure of Jump Lists and LNK files; however, some of these papers predated the release of the Windows 10 operating system. I also consulted on-line videos like YouTube Channel 13Cubed video titled, LNK FILES AND JUMP LISTS – Introduction to Windows Forensics Series released in 2017. While these sources were recognized as forensic testaments concerning LNK Files and Jump Lists, they did not provide a specific answer to the question – What behavioral changes had evolved for LNK files and Jump Lists in Windows 10?

The only partial explanation for these changes was found in the SANS Windows Forensic Analysis course textbooks. The SANS FOR408 Windows Forensic Analysis course textbook identifies both LNK files and Jump Lists as important forensic artifacts to identify non-executable files *opened/accessed* by a user on a Windows based operating system. However, since this textbook was published in 2014, it predated the release of the Windows 10 operating system. The SANS FOR408 Windows Forensics Analysis course and textbook was later updated in the SANS FOR500 Windows Forensic Analysis course which included an updated course textbook. With the release to Windows 10, the SANS FOR500 course textbook identified two notable changes in the way LNK files were handled. First, when a file is **created**, a LNK file for that target file will also be created. Prior to Windows 10, only a user's opening/accessing a target file would result in a LNK File creation. Secondly, when a target file was **created**, a LNK file would be created for the folder and parent folder where the created target file was created. (Lee, FOR500 Windows Forensic Analysis Textbook, Volume 3 Core Windows Forensics II: USB Devices and Shell Items 2018, 17). While the SANS FOR500 textbook expanded the definition and behavior of Windows 10 LNK files, it was not clear whether created files referred to just newly created

files, files copied from one volume to another, or files moved from one volume to another. The SANS FOR500 course textbook further identified Jump Lists as another source forensic investigators could use for verification of non-executable file opening and/or **creation** inside the Windows 10 operating system (FOR500 Windows Forensic Analysis Textbook, Volume 3 Core Windows Forensics II: USB Devices and Shell Items 2018, 29). While no further explanation was provided, this reference to Jump Lists as a potential source of user file activity expanded to include created files.

Since I was unable to find a complete answer to the question through research, I began testing LNK File and Jump List behavior on a Windows 10 system.

Testing

Testing Setup

Three devices were used in the Windows 10 LNK files and Jump Lists testing. A Dell XPS 8930 desktop with the Windows 10 Pro operating system installed (Build 1903) was used as the primary device to record Jump Lists and LNK files for analysis. The user 'ldjones' was the logon user for the testing sessions on the Dell XPS, and this user profile would be used to analyze data from the Recent folder.

A Lexar USB thumb drive was used as the removable device. The Lexar thumb drive was given the volume name JUMP_TEST. During the Session One test performed on February 5, 2020, the Lexar thumb drive assigned drive letter K after being inserted into the Dell XPS. During the later Sessions Two through Five, the Lexar thumb drive was assigned drive letter L after re-insertion into the Dell XPS.

A Synology Disk Station, model DS218+ was used as the network server. Access to the DS218+ was established as a mapped network drive. The mapped DS218+ was assigned drive letter Z, and it was given the name LJONES-CFA-Admin.

The three devices would be used during the testing process to create, copy, and move various files and folders. The testing was split into five different sessions with each session having a different testing objective based on the user file and folder activity performed during the session. After each session, the analysis of LNK files and Jump Lists was performed to access the effect on LNK file and Jump List behavior for each of the testing session objectives. The following analysis steps were performed during each testing session:

1. Using FTK Imager, a custom content image was created which included the Users\ldjones\AppData\Roaming\Microsoft\Windows\Recent folder.
2. Magnet AXIOM was used to process the custom content image. Artifacts selected for processing were customized to include only Jump Lists and LNK Files from the Operating System artifact

category.

3. Once processing and analysis was complete, AXIOM was used to export LNK File and Jump List reports in the form of Exhibits included with this paper.

The five sessions of user file and folder activities included:

1. Session One focused on the copying and moving of individual files and folders from one device to another.
2. Session Two focused on the simultaneous copying and moving of multiple files and folders from one device to another.
3. Session Three focused on the opening of existing files from one device, and then saving the opened file to a different device using a different file name.
4. Session Four focused on the creation of individual files on each of the devices.
5. Session Five copied and renamed Microsoft Office files without opening any of the copied or renamed files.

Session One: Single File and Folder Testing

Session One testing included the user activity of copying or moving individual files or individual folders between the three devices. On February 5, 2020, the following user file and folder activity took place:

Original Device	File/Folder Name	Receiving Device	Action Taken
DS218+	CV_Resume Folder	Lexar	Copied folder without opening the folder
DS218+	Monthly Mileage Report.docx	Lexar	<ul style="list-style-type: none"> • Opened parent folder Forms • Opened file using Microsoft Word • Saved opened file using Save As and the same file name
DS218+	SecOfStateCertificateGood Standing.pdf	Lexar	<ul style="list-style-type: none"> • Opened parent folder LA Secretary of State • Copied file to the thumb drive without opening file

DS218+	R v Reeves_Supreme Court of Canada.pdf	Lexar	<ul style="list-style-type: none"> Opened parent folder Legal Rulings Moved file (cut & paste) without opening file
DS218+	Logos_Badges Folder	XPS	Copied folder without opening the folder
DS218+	LJONES CFA LetterHead.docx	XPS	<ul style="list-style-type: none"> Opened parent folder Forms Opened file using Microsoft Word Saved opened file using Save As and the same file name
DS218+	2018 LJONES CFA Profit and Loss Statement.pdf	XPS	<ul style="list-style-type: none"> Opened parent folder Financial Statements Moved file without opening the file
DS218+	X-Ways_Cleverbridge Invoice.pdf	XPS	<ul style="list-style-type: none"> Opened grandparent folder Expenses Opened parent folder Software Copied file without opening the file
XPS	MoveDesktop2TDTest.rtf	Lexar	Moved (cut & paste) file without opening the file
XPS	Downloads Folder	Lexar	Copied folder without opening folder
XPS	Desktop2TDTest.docx	Lexar	<ul style="list-style-type: none"> Opened file using Microsoft Word Edited the file and saved the edited version using Save As

XPS	Desktop2Server_Test.txt	DS218+	<ul style="list-style-type: none"> • Opened file using Notepad • Edited the file and saved the edited file using Save As
Lexar	TD2ServerTest.txt	DS218+	<ul style="list-style-type: none"> • Opened file using Notepad • Edited the file & saved the edited file using Save As
Lexar	LSU Tickets Folder	DS218+	Copied folder without opening the folder
Lexar	Coins.docx	DS218+	Moved (cut & paste) file without opening the file

Single File and Folder Results – LNK Files

The linked *Exhibit 1: Windows 10 LNK Files for Single File and Single Folder Test* in PDF format at the end of this paper details the LNK files generated from the Session One test. To begin summation of the LNK file analysis for Session One, LNK files were **not created** or updated in the following circumstances:

- When individual folders were copied from one device to another without first opening the folder. Examples of this activity in the Session One test included the folders CV_Resume, Logos_Badges, and LSU Tickets.
- When individual files were copied from one device to another without first opening the file. Examples of this activity in the Session One test included the files SecOfStateCertificateGoodStanding.pdf and X-Ways_Cleverbridge Invoice.pdf.
- When individual files were moved (cut & paste) from one device to another. Examples of this activity in the Session One test included 2018 LJONES CFA Profit and Loss Statement.pdf, MoveDesktop2TDTest.rtf, and Coins.docx.

These behaviors were consistent with the established pre-Windows 10 LNK file behavior since neither the original source file/folder nor the destination file/folder were opened.

User activity for Session One included the opening of a previously established file, and then that file was saved to another device location using the Save As feature of the software application used to open

the previously established file. It was interesting to note that the **LNK files were created for the newly saved file location, but not for the original file location**. This LNK file behavior for the newly saved file was anticipated since the newly saved file was also open within the software application at the time it was saved. What was not anticipated was the absence of a LNK file for the original file opened from the original location.

An inconsistency was noted in the LNK file behavior for folders opened to access files within those folders. The opening of the folder 'Forms' from the DS218+ server caused a LNK file to be created. This folder was opened initially to access the file Monthly Mileage Report.docx and it was later used to access LJONES CFA LetterHead.docx. This behavior was anticipated since this folder was opened/accessed. The inconsistent behavior occurred when the folders 'LA Secretary of State', 'Legal Rulings', 'Financial Statements', and 'Expenses\Software' were also opened from the DS218+ server to access other files, but no LNK files were created when those folders were opened/accessed.

Another inconsistency occurred in the creation of the LNK files for Session One. Of the five files for which LNK files were created, only one of those LNK file recorded the target file size. Only the target file size of Desktop2Server_Test.txt was recorded in its respective LNK file.

Single File and Folder Results – Jump Lists

The linked *Exhibit 2: Windows 10 Jump List Test for Single Files and Folders* in PDF format at the end of this paper was created to detail the Jump List entries generated from the Session One test. When comparing Exhibit 1 with Exhibit 2 for the Session One test, significantly more Jump List data was recorded in Session One. To summarize the Jump List analysis for Session One:

- Windows Explorer Jump List entries were created for the destination folder when a single folder was copied from the original device to a new device. Examples of this behavior include CV_Resume (Lexar), Logos_Badges (Dell XPS), Downloads (Lexar), and LSU Tickets (DS218+). No entries were created or modified for the original folder location, and this behavior was expected since the original folder location was not opened/accessed. **This behavior of creating Windows Explorer Jump List entries for a single copied folder is the first identified user activity in Windows 10 not previously recorded in prior operating system versions.** In older versions of Windows, these Jump List entries would not have been recorded since the copied folder was not opened/accessed. This also documented a user folder activity within the Windows Explorer Jump List which was undocumented in LNK files.
- The Windows Explorer Jump List entries were inconsistent when recording opened/accessed folders. Examples of accessed folders documented in the Jump List entries include Z:\\Forms, Z:\\LA Secretary of State and Z:\\Expenses\\Software. These Jump List entries for opened single folders documented additional detail not provided by LNK files. The inconsistent Jump List

documentation was based on the folders 'Legal Rulings' and 'Financial Statements' being opened/accessed with no Windows Explorer Jump List entry created or updated.

- The Microsoft Word Jump List entries were created or updated (Last Access Date/Time) when the original file was opened from its original location, and when the newly saved file to the new device location was saved. This behavior was expected since the original file was opened/accessed, and the newly saved file remained open in the software application after being saved to the new location. The Microsoft Word Jump List entries also record the target file size for both files. This detail recorded in the Jump List entries was not recorded in the corresponding LNK files.
- The Quick Access¹ Jump List entries were consistently created each time a file was saved to a new device location, and most often created when the original file was opened from its original location. When a Quick Access Jump List entry was created from the original file location, the Last Access timestamp of the target file was updated and the target file size was recorded. Quick Access Jump List entries for the newly saved file location recorded different data based on the file type:
 - For Microsoft Word files, the target file created timestamp, modified timestamp, and the target file size were not recorded.
 - For text (Notepad) file types, the target file timestamps and the target file size were recorded.
- Notepad Jump List entries were created for both the original file location and the newly saved device location, but each entry recorded differing data.
 - For the originally opened Desktop2Server_Test.txt, only the Last Accessed timestamp was updated and no target file size was recorded.
 - For the newly saved Desktop2Server_Test.txt saved on the DS218+ server, all timestamps were updated and the target file size was recorded.
 - For the originally opened TD2ServerTest.txt, only the Last Accessed timestamp was updated and the target file size was recorded.
 - For the newly saved TD2ServerTest.txt saved on the DS218+ server, only the Last Accessed timestamp was updated and no target file size was recorded.
- As with LNK files, no Jump List entries were created when:
 - Individual files were moved (cut and paste) from one device to another, and
 - Individual files were copied from one device to another without first opening the file.

Session Two: Multiple File and Folder Testing

Session Two testing focused on the user activity of simultaneously copying or moving multiple files or folders between the three devices. On February 8, 2020, the following user activity was performed:

Original Device	File/Folder Name	Receiving Device	Action Taken
-----------------	------------------	------------------	--------------

-----	XWF Program folder	Lexar	Created folder on Lexar thumb drive to accept copied data
Dell XPS	~ 600 files including folders MPlayer, viewer, and x64 (with sub-folders) from within X-Ways Forensics folder on Dell XPS Desktop	Lexar	After opening X-Ways Forensics folder on Dell XPS, copied all files, folders, and sub-folders to the Lexar thumb drive.
DS218+	9 folders named 18-*	Lexar	After accessing the Z drive, copied 9 folders with folder names beginning 18-*
DS218+	4 folders named 19-*	Lexar	Moved (cut/paste) 4 folders with the folder names beginning 19-*

Multiple File and Folder Results – LNK Files

The linked *Exhibit 3: LNK Files Test for Multiple Files/Folders* in PDF format at the end of this paper was created from the Session Two LNK file artifacts. As a result of the Session Two testing, only two LNK Files were created. A LNK File was created for accessing the Lexar thumb drive (Drive L), and a LNK file was created for the new folder 'XWF Program' on the Lexar thumb drive. Creation of these LNK files were expected since those items were accessed to accept data. Windows 10 did not create LNK Files for any of the following user activities:

- The opening of folders 'X-Ways Forensics 19.9' from the Dell XPS desktop and access to the Z: drive (DS218+ server). It was expected that LNK files would have been created for these user activities since these folders were opened/accessed; however, as in Session One LNK file results, LNK files were not always created when folders were opened/accessed.
- The simultaneous copy of multiple files and sub-folders without the files or folders first being opened/accessed.
- The simultaneous copy of multiple folders without the folders first being opened/accessed.
- The simultaneous move (cut and paste) of folders.

Multiple File and Folder Results – Jump Lists

The attached *Exhibit 4: Windows 10 Jump List Test for Multiple Files and Folders* was created to document the Jump List entries for the Session Two testing. As observed from a comparison of Exhibit 3 (LNK

files) with Exhibit 4 (Jump Lists), Jump List entries from the Session Two user file and folder activities contained more detail than LNK file artifacts. In summary,

- Windows Explorer Jump List entries were created for the destination folder locations when the user simultaneously copied multiple folders from one device location to another. ***The Windows Explorer Jump List entries created during the user's simultaneous folder copy operation for multiple folders identified a second new artifact behavior for Windows 10 Jump Lists.***
- It was noted that while the simultaneous copying of multiple folders created Jump List entries, the simultaneous copying of files did not produce Jump List entries.
- Also, no Jump List entries were created for the simultaneous moving (cut & paste) of folders from one device to another.

Session Three: Save As & Renamed Files Testing

Session Three testing involved opening a previously saved file using its default software application and then saving the file with a different file name on a different device. Some of the opened and renamed files were edited while some were saved un-edited in their original data form. On April 15, 2020, the following user actions were taken:

Original Device	Original File Name	Receiving Device	Action Taken
Lexar	SecOfStateCertificateGood Standing.pdf	Dell XPS	Original File opened using Foxit Reader File saved as CertGoodStand.pdf without editing file
Lexar	Monthly Mileage Report.docx	Dell XPS	Original file opened using Microsoft Word File edited & saved as April-Mileage.docx
Lexar	TD2ServerTest.txt	DS218+	Original file opened using Notepad File edited & saved as Lexar-DS218+.txt

Lexar	R v Reeves_Supreme Court of Canada.pdf	DS218+	Original file opened using Foxit Reader File saved as Reeves-Court.pdf without editing
DS218+	Critical Equipment List.xls	Lexar	Original file opened using Microsoft Excel File edited & saved as Write-Blockers.xls
DS218+	USA v Chris Dumas Subpoena.pdf	Lexar	Original file opened using Foxit Reader File saved as Shreveport-Travel.pdf without editing
DS218+	High Tech Interview Questions.docx	Dell XPS	Original file opened using Microsoft Word File edited & saved as Interview.docx
DS218+	LDJPhoto_7-7-19.jpg	Dell XPS	Original file opened using Microsoft Photo Editor File saved as coat-tie.jpg without editing
Dell XPS	2018 LJONES CFA Profit & Loss Statement.pdf	Lexar	Original file opened using Foxit Reader File saved as 2018 Loss.pdf without editing the file
Dell XPS	LJONES CFA LetterHead.docx	Lexar	Original file opened using Microsoft Word File edited & saved as Header.docx

Dell XPS	DCode Image.jpg	DS218+	<p>Pictures folder opened on Dell XPS</p> <p>Original file opened using Microsoft Photo Editor</p> <p>File saved as Test-Image.jpg without editing file</p>
----------	-----------------	--------	---

Single Renamed File Results – LNK Files

The linked *Exhibit 5: Windows 10 LNK File Test for Renamed Files* in PDF format at the end of this paper documented the LNK file artifacts from the Session Three test results. In each instance of user file activity performed in Session Three, Windows created or updated a LNK file for both the original file location and for the new saved file location. This behavior was expected since the original file was opened and the newly saved file remained open after being saved in a new file location. The Session Three LNK file artifacts appeared to differ when compared to the Session One LNK file results. In Session One, original files were opened and then saved to a different device location using the same filename. Session One testing identified LNK files created for the files saved in the new device location with no LNK files created or updated for the original file location.

Inconsistencies were observed from the data recorded within the LNK files created during Session Three. The Session Three LNK files were somewhat inconsistent in their recording of the target file created timestamp, the target file modified timestamp, and the target file size for newly created files.

- The target created timestamp, target modified timestamp, and the target file size data were not recorded for PDF, JPG, and Microsoft Excel file types.
- The target timestamps and target file sizes were recorded for the single newly created text file.
- For Microsoft Word files, a mixture of results was observed:
 - The target timestamps and target file size were recorded for the newly saved file April-Mileage.docx.
 - The target timestamps and target file sizes were not recorded for the newly saved files Interview.docx, and Header.docx

The cause for the inconsistent recording of data for Microsoft Word file types within the LNK files is unknown and may require more testing.

Single Renamed File Results – Jump Lists

The linked *Exhibit 6: Windows 10 Jump List Test for Edited and Renamed Files* at the end of this paper was generated to document the Session Three Jump List analysis. In the Session Three test, the analysis of LNK files and Jump List entries reflect those two artifacts report similar data for files which are opened and then saved using a different name on a different device. Depending on the Jump List, slight variations were observed in the data recorded by the Jump List. A summary for each Jump List recording Session Three user file activity is detailed below:

- The Foxit Reader Jump List was the most consistent in its behavior. It recorded entries for both original file location as well as the newly saved location.
 - For the original file, the entries consistently recorded the target file size with the target creation and modified timestamps unchanged.
 - For the newly saved file, the target created timestamp, the target modified timestamp, and the target file size were not recorded.
- For the Quick Access Jump List, separate entries were created for the original file location and the newly saved file location.
 - For the original file, the entry consistently recorded the target file size with the target creation and target modification timestamps left unchanged.
 - Except when the newly saved file was a text file, the Quick Access Jump List entry did not record the target created timestamp, the target modified timestamp or the target file size. When the newly saved file was a text file, the Quick Access Jump List recorded the target file timestamps and the target file size. It is unknown why the Quick Access Jump List entry recorded data for a newly saved text file was different from the other file types tested.
- The Notepad Jump List recorded separate entries for both the original file location and the newly saved file location.
 - For the original file, the created and modified timestamps remained unchanged and the target file size was recorded.
 - For the newly saved location, no timestamps or target file size were recorded.
- The Microsoft Photo Jump List only recorded entries for the original file location (a Quick Access Jump List entry was created for both locations). These entries kept the target created and modified timestamps unchanged, and the entry recorded the target file size.
- The Microsoft Excel and Microsoft Word Automatic Jump Lists created separate entries for both the original file location and the newly saved file location.
 - For the original location, the target file created and modified timestamps remain unchanged while the target file size was recorded.
 - For the newly saved location, the target created and target modified timestamps recorded when the date and time the new file was saved. Also, the new target file size was recorded for the newly saved location entries.

The Jump List behavior as recorded in Session Three was expected since the original file was opened/accessed and the newly saved file remained open after the file was saved to the new location.

Session Four: Newly Created Files Testing

Session Four testing involved the creation of new files without copying or moving the files from an original location. These newly created files were saved to one of the three devices using during testing. On May 14, 2020, the following user actions were taken:

Software Application	Saved Filename	Saved Device	Description
Microsoft Word	Server_Word_SaveAs.docx	DS218+	Microsoft Word was opened and a blank, new file was opened New file was saved using Save As
Microsoft Word	Server_PDF_MicrosoftPrint.pdf	DS218+	With Server_Word_SaveAs.docx still open, used Microsoft PDF Print to save new file
Notepad	Server_Notepad_SaveAs.txt	DS218+	Notepad was opened with no file specified. Saved the new file using Save As
Microsoft Excel	Desktop_Excel_SaveAs.xlsx	Dell XPS	Opened a blank spreadsheet using Excel Saved the new file using Save As
Foxit Printer	Desktop_PDF_FoxitPrinter	Dell XPS	With Desktop_Excel_SaveAs.xlsx still open, printed the file using Foxit PDF Printer

Notepad++	Desktop_Notepad++_Save As.txt	Dell XPS	Opened Notepad++ to a blank file Saved the file using Save As
7-Zip	Desktop_7Zip_Archive.7z	Dell XPS	Used 7-Zip to create a new archive file
Microsoft PowerPoint	TD_PP_SaveAs.pptx	Lexar	Opened a blank presentation using Power Point Saved the new file using Save As
Microsoft OneNote	TD_OneNote_MicrosoftPDF.pdf	Lexar	Using OneNote, created a note entry Printed the note entry using Microsoft PDF Printer
7-Zip	TD_7Zip_FromServer.7z	Lexar	Using 7-Zip, created a new archive including files from the DS218+ server. Saved the archive to the Lexar thumb drive

Single Newly Created File Results - LNK Files

The linked *Exhibit 7: Windows 10 LNK Files for Newly Created Files* at the end of this paper documented the Session Four test results. A comparison with Exhibit 7 and Exhibit 1 (LNK file results for single copied file test) reflects similar results concerning saved files. Session Four testing included the creation of ten new files. Of the ten new files, eight LNK files were created - The two files which no LNK file was created were both 7-Zip archive files.

Similar to the Session One test results, seven of the eight created LNK files in Session Four did not record target file timestamps or the target file size. The only LNK file which recorded target file timestamps and target file size was a Microsoft Word file (Server_Word_SaveAs.docx). LNK files in Exhibit 1 did not record target file timestamps or target file size for any of the saved Microsoft Word files, and Exhibit 5 was inconsistent in its treatment of LNK files for Microsoft Word file types.

Single Newly Created File Results – Jump Lists

The linked *Exhibit 8: Windows 10 Jump List Entries for Newly Created Files* at the end of this paper was generated to record Jump List entries resulting from the Session Four testing. As with LNK files in Exhibit 7, eight of the ten created files in Session Four testing had corresponding Jump List entries, although not all software application Jump Lists recorded entries. Also similar to LNK files, the two created files which did not have a corresponding Jump List entry were 7-Zip archive files.

The Jump List entries for Microsoft Office file types (Word, Excel, and PowerPoint) recorded the same data categories within the Jump List entries. They each recorded the created and modified timestamps as well as the target file sizes for each of the newly created files. The data recorded for these Microsoft Jump List entries are similar to the Jump List entries recorded in Session One (Exhibit 2) and Session Three (Exhibit 6) testing results.

The Notepad Jump List entry created from Session Four did not record target file created or modified timestamps, and it did not record the target file size. This behavior matched the Notepad Jump List entry from Exhibit 6 (Session Three) for newly saved Notepad files. As the reader may also recall, the Exhibit 2 (Session One) Notepad Jump List entries recorded conflicting data; one file recorded target file timestamps and target file size while a second entry did not record timestamps and target file size.

No software application Jump List entries were created for newly created PDF files or files created with Notepad++ in Session Four testing. Comparing Session Three Jump List entries from Exhibit 6 showed Foxit Reader Jump List entries for newly saved files where the newly saved file was saved from an original file. In Session Four, PDF files were created by using the Microsoft and Foxit print features to create the files, and were not just renamed from an original file.

Finally, eight saved files from Session Four testing generated a Quick Access Jump List entry with the data categories saved within these Quick Access Jump List entries varying. The Quick Access Jump List entries for file types .docx (Microsoft Word), .txt (Notepad), and Notepad++ recorded the target file timestamps and target file size. The target file created timestamp, the target file modified timestamp and the target file size were not recorded for the file types .pdf, .xlsx (Microsoft Excel), and .pptx (Microsoft PowerPoint). Just like the LNK files created in Session Four, no Quick Access Jump List entries were created for the 7-Zip saved files.

Session Five: Copying and Renaming Microsoft Office Files Without Opening

Session Five testing involved the copying of individual files, the simultaneous copying of files, and the renaming of individual files without opening any of the files. All files copied or renamed in Session

Five were Microsoft Office files. On May 28, 2020, the following user actions were taken:

Original Device	Original File	Saved Device	Actions Taken
			Opened This PC on Dell XPS Desktop
XPS Desktop	April-Mileage.docx	Lexar	Right-click > Copy April-Mileage.docx from Dell XPS Desktop Right-click > Paste file on JUMP_TEST from This PC
XPS Desktop	LJONES CFA LetterHead.docx	Lexar	Right-click > Copy LJONES CFA LetterHead.docx from Dell XPS Desktop Right-click > Paste file on JUMP_TEST from This PC
XPS Desktop	Windows 10 Jump List and Link File Artifacts - Saved, Copied & Moved.docx	XPS Desktop	Slow double-click Windows 10 Jump List and Link File Artifacts - Saved, Copied & Moved.docx to access file name. Retyped filename as Old_Jump List and LNK Testing.docx
XPS Desktop	Interview.docx Desktop_Excel_SaveAs.xlsx	Lexar	Control-Enter to select Interview.docx and Desktop_Excel_SaveAs.xlsx files. Right-click > Copy the selected files Right-click > Paste selected files to JUMP_TEST using This PC

			Opened JUMP_TEST (drive L)
Lexar	Desktop2TDTest.docx	XPS Desktop	Right-click > Copy Desktop2TDTest.docx from Lexar Right-click > Paste file on XPS Desktop
Lexar	Header.docx	XPS Desktop	Right-click > Copy Header.docx from Lexar Right-click > Paste file on XPS Desktop
Lexar	Monthly Mileage Report.docx	Lexar	Slow double-click Monthly Mileage Report.docx to access file name Retyped filename as Mileage.docx
Lexar	TD_PP_SaveAs.pptx Write Blockers.xlsx	XPS Desktop	Control-Enter to select TD_PP_SaveAs.pptx and Write Blocker.xlsx from Lexar Right-click > Copy the selected files Right-click > Paste selected files on XPS Desktop

Results: Copied & Renamed Microsoft Office Files Without Opening Files – LNK & Jump Lists

After processing and analyzing the processed Recent folder upon completion of Session Five testing, no created (or updated) LNK files or Jump List entries were identified. After testing and analysis was completed, a review of the Quick Access list using This PC from the Dell XPS failed to contain any files included in the user file activity for Session Five.

Conclusions

Windows 10 Jump List and LNK Files continue to be a source for forensic analysts to document user file and folder activity. Due to some changes in the Windows 10 LNK file and Jump List behaviors, analysts should understand these new behaviors to fully benefit from the analysis of user file and folder activity on a system. In addition to the traditional user file and folder access, Windows 10 has expanded, in limited circumstances, the documenting of user file and folder activity.

For LNK files, the following unique behaviors were observed during testing:

1. When files were opened using their default software application, and then saved to a different device location with the same filename using the software's Save As feature, LNK files were created for the file in the newly saved location (Session One).
2. When an original file was opened using its default software application, then the Save As feature of the software was used to save the file using a different name on a different device, LNK files were created. This user file activity created or modified LNK files for both the original file location and the newly saved file location (Session Three).
3. When a software application was used to create a new file using the Save As or PDF Print features of the software, a LNK file was created for the newly saved file. An exception to this behavior was when the 7-Zip software was used to create a new 7-Zip archive (Session Four).
4. LNK files were not created when an individual folder or simultaneous multiple folders were copied from one device to another (Session One).

For Jump Lists, the following unique behaviors were observed during testing:

1. A Windows Explorer Jump List entry was created for a destination folder when either an individual folder or multiple folders were simultaneously copied from one device to another. This represents a new behavior for the Windows Explorer Jump List in Windows 10. This new behavior has the potential for Jump List entries to be significantly higher when compared to LNK files (Session One and Session Two).
2. Quick Access, a new feature to Windows 10 has its own dedicated Jump List. The Quick Access Jump List consistently recorded entries when a file was saved to a new device location. This newly saved file could have resulted either from the opening of an original file and re-saving the file to a new location; or from the creation of a new file with no interaction with an original file. Quick Access Jump List entries were created irrespective of any software application Jump Lists which may have additionally recorded entries for the same user file activity. Quick Access, as a new feature of Windows 10 caused Jump List entries to be significantly higher when compared to LNK files. While the Quick Access Jump List consistently recorded entries for newly saved files, the recording of entries for original file locations was varied (Session One, Session Three, and Session Four).

3. When an original file was opened using its default software application, and the Save As feature of the software was used to save the file using either the same filename to a different location or a different filename to a different file location, the following software application Jump Lists² recorded entries for both the original file location and the newly saved device location³ (Session One and Session Three):
 1. Foxit Reader
 2. Quick Access
 3. Notepad
 4. Microsoft Excel
 5. Microsoft Word
4. When a software application was used to create a new file with no interaction with an existing file using its Save As feature, the software application Jump List recorded an entry for this newly saved file. The single exception was when a new 7-zip archive was created – No 7-zip Jump List was identified in the testing (Session Four).
5. When a software application's PDF Print feature was used to create a new PDF file type from the an originally opened file, no Jump List entry was created within the software application Jump List. A Quick Access Jump List entry was created for the newly saved PDF file (Session Four).

For both LNK files and Jump Lists, the following common observations were made from testing:

- No LNK file or Jump List entry was created or modified when an individual file was copied, an individual file was renamed, or the simultaneous multiple copying of files from one device to another without the files first being opened (Session One, Session Two and Session Five).
- No LNK file or Jump List entry was created or modified when an individual file or simultaneous multiple files were moved from one device to another (Session One and Session Two).
- The creation or modification of LNK files and the creation/modification of Jump List entries was inconsistently applied when existing folders were opened. At times LNK files and Jump List entries were created when folders were opened, while at other times no LNK file or Jump List entry was created. Based on this inconsistency, other forensic artifacts such as ShellBags⁴ should be used to analyze the opening of folders on a system under examination (Session One, Session Two).

Finally, data recorded in LNK files and Jump List entries were not always consistent as to the target file timestamps and the target file size were recorded. This inconsistency seemed to be based on the application used to open/save the target file (Session One, Session Three, and Session Four).

References

13Cubed, YouTube Channel. 2017. *LNK FILES AND JUMP LISTS - Introduction to Windows Forensics Series*. November 6.

Antonovich, Chris. April 2014. *Jump List Forensics*. Burlington, VT: Leahy Center for Digital Investigation at Champlain College.

Lee, Rob. 2018. *FOR500 Windows Forensic Analysis Textbook, Volume 3 Core Windows Forensics II: USB Devices and Shell Items*. Maryland: SANS Institute.

Lee, Rob, and Chad Tillbury. 2014. *SANS Forensics 408 Windows Forensic Analysis Volume 4, Core Windows Forensics Part III*. The SANS Institute.

Parsonage, Harry. Updated July 2010. *The Meaning of Linkfiles In Forensic Examinations*. Research, computerforensics@parsonage.co.uk.

Patrick Leahy Center for Digital Investigation. April 2015. *Windows 10 Forensics*. Research, Burlington, VT: Champlain College.

Singh, Bhupendra and Sing, Upasna. 2016. *A Forensic Insight Into Windows 10 Jump Lists*. Research, Elsevier.

Trent, Rod. 2015. *How To: Use Quick Access in Windows 10's File Explorer*. July 23. Accessed March 30, 2020. <http://itprotoday.com/windows-server/how-to-use-quick-access-windows-10s-file-explorer>.

Links to Exhibits

Exhibit 1: Windows 10 LNK Files for Single File and Single Folder Test:

[Exhibit 1 - Win10 LNK Single File & Folder Test.pdf](#)

431 KB

Exhibit 2: Windows 10 Jump List Test for Single Files and Folders:

[Exhibit 2 - Win10 Jump Single File & Folder.pdf](#)

448 KB

Exhibit 3: LNK Files Test for Multiple Files/Folders:

[Exhibit 3-Win10 LNK For Multiple Files & Folders.pdf](#)

421 KB

Exhibit 4: Windows 10 Jump List Test for Multiple Files and Folders:

[Exhibit 4 - Win10 Jump Multiple Files & Folders.pdf](#)

442 KB

Exhibit 5: Windows 10 LNK File Test for Renamed Files:

[Exhibit 5 - LNK Test Renamed Files.pdf](#)

448 KB

Exhibit 6: Windows 10 Jump List Test for Edited and Renamed Files:

[Exhibit 6 - Jump Lists Test - Renamed.pdf](#)

459 KB

Exhibit 7: Windows 10 LNK Files for Newly Created Files:

[Exhibit 7 Link Files For Newly Created Files.pdf](#)

429 KB

Exhibit 8: Windows 10 Jump List Entries for Newly Created Files: [Exhibit 8 Jump List Entries For Newly Created Files.pdf](#)

434 KB

DFIR Review

This paper provides valuable information on Windows jump list and link file artifacts. The research is helpful in understanding the new, and sometimes unexpected, behavior of link files and jump lists in Windows 10. It is important to note that the testing procedures and results are expected on Windows 10 version 1903, but there could potentially be variations between previous and future versions of Windows 10. It is important to note that link files may also be stored in other locations, not just in the “C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Recent” folder. The paper indicates that there is a maximum number of link files that can be stored in the “Recent” folder, but the actual number is not indicated.

Future Work

Additional research should be conducted on future versions of Windows 10. We’re unaware of what changes will be made in future versions, and those changes could impact the results one would get by performing these same procedures on jump list and link files. A concise chart indicating how link files and jump lists are affected by each action (copying, moving, opening) would be helpful.

Research into how link files and jump list entries are affected by the deletion of target files and folders in Windows 10 would also be useful. Finally, further analysis is needed to reconcile the inconsistencies found for the embedded target file timestamps within the LNK files.

Reviewers

Ryan Wesley (Methodological Review and Validated Review using Reviewer Generated Datasets)

Ali Hadi (Methodological Review)

Lisa Brown (Methodological Review)

Footnotes

1. Quick Access is a new feature of File Explorer introduced in Windows 10. It is similar to the Favorites section in older versions of Windows. By default, the logged in user will enter Quick Access directly when they open File Explorer (or This PC if displayed on the user’s desktop). Quick Access is similar to a software application Jump List (i.e. Microsoft Word), but Quick Access is not software

application specific. Quick Access lists all file types recently opened and is not restricted to files opened by a specific software application. [↵](#)

2. The Microsoft Photos Jump List only created an entry for the original file location and not the newly saved file location based on this user file activity. [↵](#)

3. This behavior was in contrast to LNK file creation since LNK files were created for only the newly saved file location given the same user file activity. Since two Jump List entries are created for this user file activity, this is another example of Windows 10 Jump Lists creating more entries when compared to the LNK files created. [↵](#)

4. ShellBags are a set of Windows Registry keys which store details about viewed folders. [↵](#)