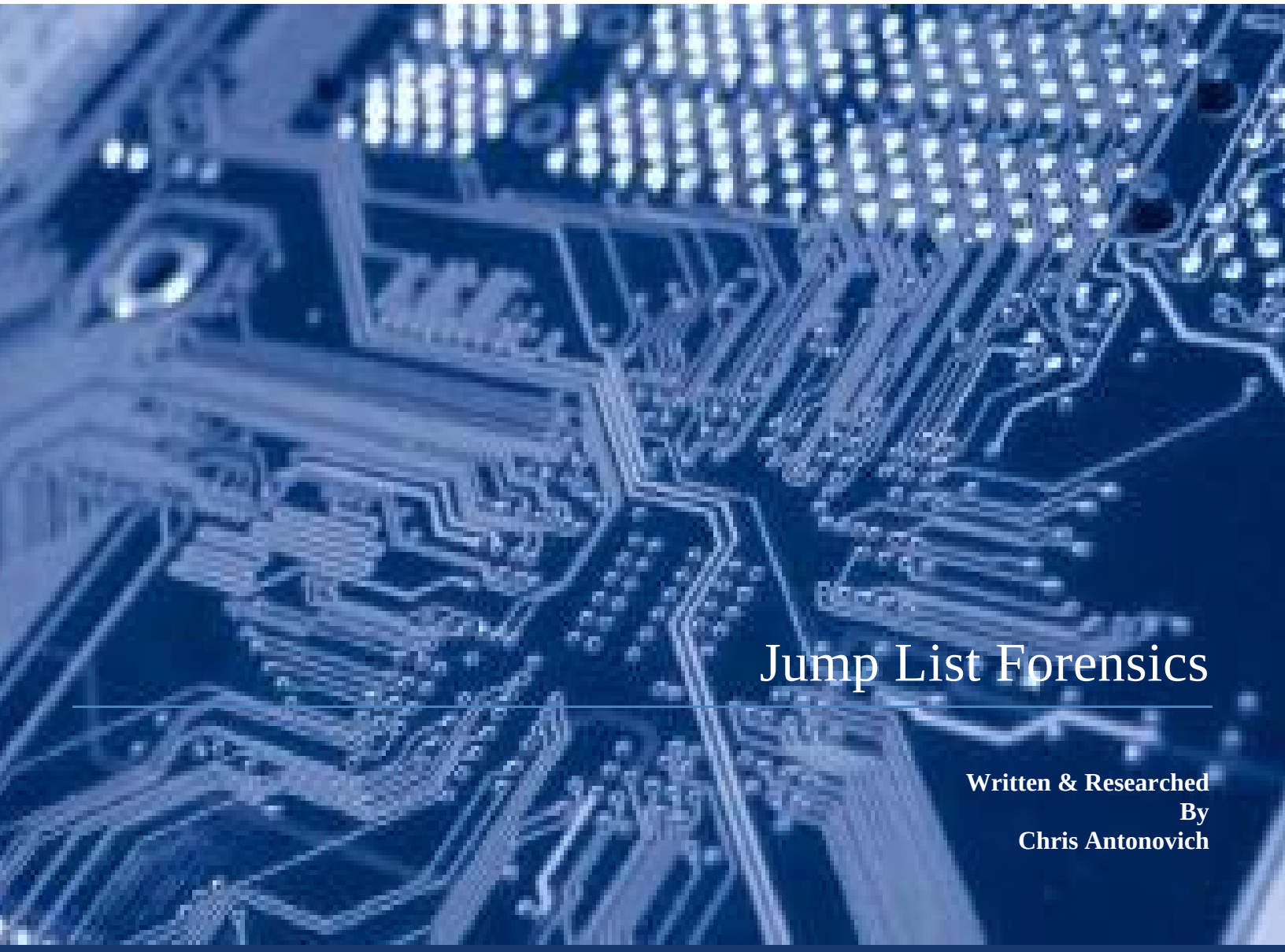
CHAMPLAIN COLLEGE | LCDI Leahy Center for Digital Investigation



Jump List Forensics

Written & Researched By
Chris Antonovich

175 Lakeside Ave, Room 300A
Phone: 802/865-5744
Fax: 802/865-6446
http://www.lcdi.champlin.edu

4/28/14

Disclaimer:

This document contains information based on research that has been gathered by employee(s) of The Senator Patrick Leahy Center for Digital Investigation (LCDI). The data contained in this project is submitted voluntarily and is unaudited. Every effort has been made by LCDI to assure the accuracy and reliability of the data contained in this report. However, LCDI nor any of our employees make no representation, warranty or guarantee in connection with this report and hereby expressly disclaims any liability or responsibility for loss or damage resulting from use of this data. Information in this report can be downloaded and redistributed by any person or persons. Any redistribution must maintain the LCDI logo and any references from this report must be properly annotated.

Contents

Introduction

Jump Lists are a new, unique taskbar feature introduced by Windows 7 and included in Windows 8. Jump Lists are created by certain user actions, such as saving a file using Microsoft Word or going to a website using Firefox, which automatically saves as an *.automaticDestination-ms or a *.customDestination file. This feature gives the user quick and easy access to recently opened application files. By default, Windows applications are typically saved in the "autodest" directory while other applications are saved into the "custdest" file. We believe that this is a nest for holding information during a forensic examination. "The records maintained by [Jump Lists] have the potential to provide the forensic computing examiner with a rich source of evidence during examinations of computers running the Microsoft Windows 7 Operating System" (articles.forensicfocus.com).

Background:

The location of Jump Lists on Windows 7 s:C:\Users\LCDI\AppData\Roaming\Microsoftg\Windows\Recent\... Jump Lists will filter into the two sub-directories, *\AutomaticDestinations and *\CustomDestinations. The automatic sub-directory includes autodest (*.automaticDestination-ms) files created by the operating system and other default applications. The autodest files are in the OLE Compound File structure containing the DestList stream. "The 'DestList' stream acts as a most recently/frequently used (MRU/MFU) list. This stream consists of a 32-byte header, followed by the various structures that correspond to each of the individual numbered streams" with the automatic destinations acting as streams (forensicswiki.org). The "custdest" files use a structure similar to a MS-SHLLINK binary format running together consecutively.

Purpose and Scope:

This experiment may help the forensics community because looking at Jump Lists seldom make a forensic appearance when establishing a time line of events. This project will help members of the LCDI and other members of the forensic community to see how Jump Lists can be very helpful in establishing a timeline of events on a suspect's computer. One of the key aspects of Jump Lists is that they last even after an application has been deleted. (windowsir.blogspot.com)

Research Questions:

Can Jump Lists data that has been deleted be retrieved?

What is the nature of certain application's creation of Jump Lists?

What kind of relevant data from Jump Lists can be acquired?

Terminology:

Autodest – Abbreviation for *.automaticDestinations-ms.

Custdest – Abbreviation for *.customDestinations-ms.

DestList Stream – "The "DestList" stream acts as a most recently/frequently used (MRU/MFU) list. This stream consists of a 32-byte header, followed by the various structures that correspond to each of the individual numbered streams. Each of these structures is 114 bytes in size, followed by a variable length Unicode string." (forensicswiki.org)

EnCase – EnCase is a digital forensic tool suite created by Guidance Software designed for forensic, cybersecurity, and e-discovery.

Forensic Tool Kit – Forensic Tool Kit, or FTK, is forensic software made by AccessData.

JumpLister – A forensic program created by *woanware* that "is designed to open one or more Jump List files, parse the Compound File structure, then parse the link file streams that are contained within." (woanware.co.uk)

Jump Lists – "Jump Lists are a new Windows 7 Taskbar feature that gives the user quick access to recently accessed application files and actions." (forensicswiki.org)

MS-SHLLINK – "The Shell Link Binary File Format specifies a structure called a shell link. That structure is used to store a reference to a location in a link target namespace, which is referred to as a link target. The most important component of a link target namespace is a link target in the form of an item IDlist."(Microsoft)

OLE container – "A technology for transferring and sharing information between applications by inserting a file or part of a file into a compound document. The inserted file can be either linked or embedded. An embedded item is stored as part of the compound document that contains it; a linked item stores its data in a separate file."(Microsoft)

Virtual Machine/VM – A virtual environment being run a on a physical machine that allows an OS to operate.

VMWare Workstation – A hypervisor that allows the creation of multiple VMs to be run simultaneously.

Methodology and Methods

We created Virtual Machines for both Windows 7 and Windows 8 using VMWare Workstation 10.0.0. We wanted to include Windows 8 to see if there are any differences in the way that Jump Lists are created on the new OS as compared to Windows 7. Next, we made a data generation sheet in Microsoft Word listing the steps needed to create Jump Lists for each application and action (See Appendix A). After designing the data generation process, we started the Windows 7 VM. We recorded every action within the VM into an Excel Sheet with time logs for each. We were careful to go through the same array of websites for each web browser application to compare the amount of data each leftbehind in Jump Lists. Then for documents, we used Libre Office Writer, an open source free writing processor, that could create more *.customDestinations files than Windows Office. Using Windows Media Player, we played the three sample video files and sample audio file. After doing so for the Windows 8 VM, we created clones of the two VMs to see if deleting the Jump Lists manually would make them harder to find.

Equipment Used:

Table 1: Equipment

Item	Identifier	Description
Workstation	*Workstation*	*OS: Microsoft Windows 7 Enterprise (64 bit); v6.1.7601; Service Pack 1 Build 7601. Motherboard: ASRock Z77 Extreme6/TB4. Processor: Intel® Core ™ i7-3770k CPU 3.50GHz. RAM: 16.0 GB*
VMWare Workstation v10.0.0	*VMWare*	*Creates VMs for Windows 7 and Windows 8*
FTK® Imager v3.1.0.1514	*FTK Imager*	*Images VMs*
EnCase Imager v7.08.00.137	*EnCase*	*Images VMs*
Forensic Toolkit® v4.1.0.165	*FTK*	*Opens the Image to collect data in comparison to EnCase*
EnCase Imager v7.08.00.137	*EnCase Imager*	*Opens the Image to collect data in comparison to the Forensic Tool Kit*
Jump Lister v1.1.0	*Jump Lister*	*A custom program created for parsing jump list data*

Table 2: Data Generation Software

Item(versions varies with OS)	Identifier	Description/Use
Notepad	*Notepad*	*Default Windows text editor*
Internet Explorer	*Internet Explorer*	*Default Windows Internet Browser*
Firefox Mozilla	*Firefox*	*Internet Browser, distributed by Mozilla*
Libre Office Writer	*Libre Office Writer*	*Open Source, free word processor*
Google Chrome	*Chrome*	*Internet Browser, distributed by Google*
Windows Media Center	*Windows Media Center*	*Media Player, Plays .mp3, .wmv in the experiment*

Data Collection:

After generating data in the VMs, we used FTK Imager to image the files. Unfortunately, FTK Imager could not produce a readable image, causing us to switch to Encase Imager (Figure 1 & 2). We used FTK, EnCase, and Jump Lister to look at the Jump List data, as well as to compare the Windows 7 and 8 VMs.

Figure 1:

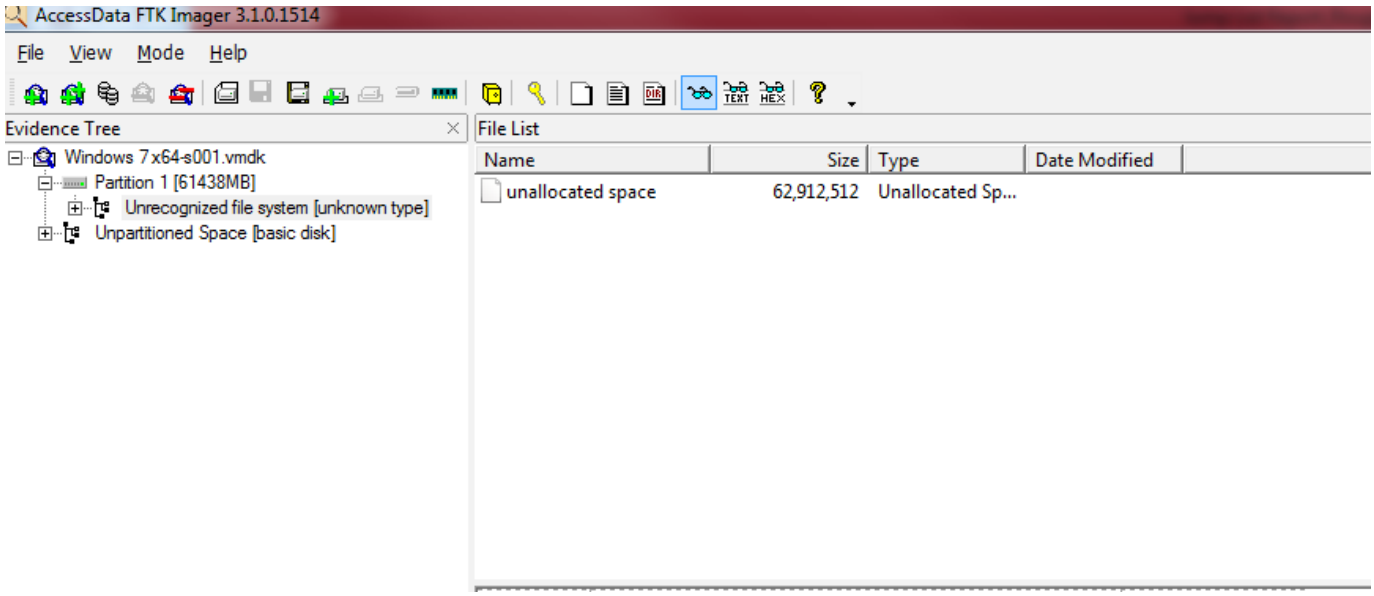
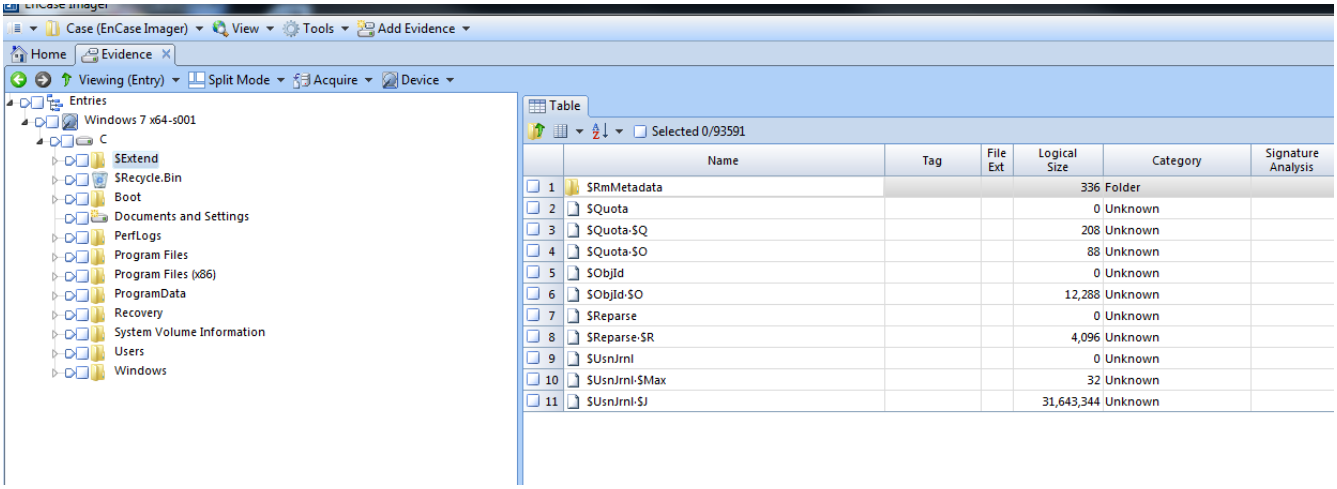


Figure 2:



Analysis

After generating the data, we used forensic tools to export and parse the data from the Jump Lists. When we added the images into Encase and FTK, we selected the Data Carve options to process the evidence. We used FTK and Encase again to look at the hex of the data. We put the Jump List files with JumpLister to assess its usefulness. JumpLister is commonly regarded as the most user-friendly way of managing Jump List Data. According to our research, there should be 10 or less Jump Lists for each application, as well as timestamps of each of the files.

Results

Jump List Data:

According to our findings, Jump Lists carry important pieces of information such as timestamps, applications used, and files recently accessed along with their file paths (See below).

Windows 7:

Figure 3

AutomaticDestinations	Application	File Content
9b9cdc69c124e3b.automaticDestinations-ms	*Notepad*	*Filepaths of accessed files, Timestamps*
1b4dd67f29cb1962.automaticDestinations-ms	*Windows Explorer*	*Filepaths, Timestamps*
7e4dca80246863e3.automaticDestinations-ms	--	*Windows Settings, Timepstamps*
d38a3ea7ec79fbed.automaticDestinations-ms	*Libre Office Writer*	*Filepaths of accessed files, Timestamps*
74d7f43c1561fc1e.automaticDestinations-ms	*Windows Media Player*	*Filepaths(video)*

Figure 4

CustomDestinations	Application	File Content
1b4dd67f29cb1962.customDestinations-ms	---	---
7e4dca80246863e3.customDestinations-ms	---	---
5afe4de1b92fc382.customDestinations-ms	*GettingStarted.exe*	*Filepaths, Timestamps*
28c8b86deab549a1.customDestinations-ms	*Internet Explorer*	*Web History,Timestamps Filepaths of accessed files, etc.*
969252ce11249fdd.customDestinations-ms	*Mozilla Firefox*	*Web History, Timestamps, Filepaths of accessed files, etc.*
74d743c1561c1e.customDestinations-ms	*Windows Media Player*	*Filepaths(Music),*

Windows 8

Figure 5

AutomaticDestinations	Application	File Content
ae6df75df512bd06.automaticDestinations-ms	*Windows Media Player*	*Filepaths of accessed files(music), Timestamps*
4cb9c5750d51c07f automaticDestinations-ms	*Windows Media Player*	*Filepaths of accessed files(video), Timestamps,*
c9533998e1308d73.automaticDestinations-ms	*Windows Photo Viewer*	*Filepaths of accessed files(photos), Timestamps*
f01b4d95cf55d32a.automaticDestinations-ms	*Windows Explorer*	*Filepaths, Timestamps*
9b9cdc69c124e3b.automaticDestinations-ms	*Notepad*	*Filepaths of accessed files, Timestamps*
7e4dca80246863e3.customDestinations-ms	--	*System Settings*
d38a3ea7ec79fbed.automaticDestinations-ms	*Libre Office Writer*	*Filepaths of accessed files, Timestamps*

Figure 6

CustomDestinations	Application	File Content
f01b4d95cf55d32a.customDestinations-ms	--	--
7e4dca80246863e3.customDestinations-ms	--	--
28c8b86deab549a1.customDestinations-ms	*Internet Explorer*	*Web History, TimeStamp, Filepaths of accessed files, etc.*
969252ce11249dd.customDestinations-ms	*Firefox Mozilla*	*Web History, TimeStamp, Filepaths of accessed files, Firefox cache data, etc.*

One of the most useful pieces of information that we gathered from the Jump Lists was the timestamp date associated with each Jump List. This data is important for a forensic examiner when he or she is establishing a timeline of events. This does not work with every application, as some Jump Lists show recently closed websites and files while others will show most frequently visited. Another important piece of information can be found in the Jump List hex, the directory of the Jump Listed file. Another thing to keep in mind is that Windows, by default, limits the amount of Jump Lists there can be, typically at 10. The websites that were in the Internet Explorer and Firefox Jump Lists seemed to differ but contained the same amount of information. The nature in which Jump Lists are created appeared to vary depending on the operating system being used.

The only shared names were two autodest Jump Lists, the jump List for Libre Office Writer, and the Jump List for Notepad. We believe that the two Jump Lists share the same AppID because the programs are both from the same directory. The *7e4dca80246863e3.automaticDestinations-ms* file was shared in both VMs, as well as being in the AutomaticDestinations and CustomDestinations folders (Figure 6 & 7).

7e4dca80246863e3.automaticDestinations-ms

Figure 7(Windows 7):

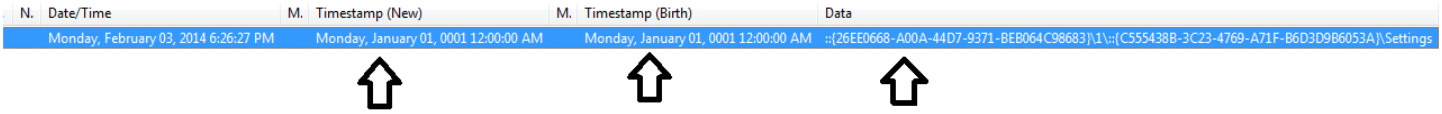
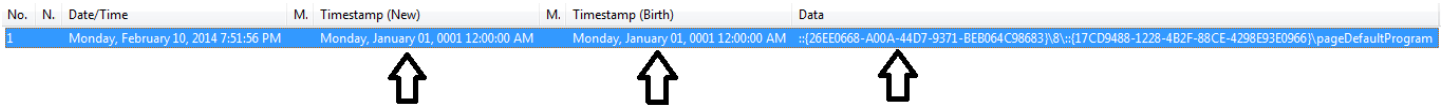


Figure 8(Windows 8):



Besides these exceptions, there were only two common Jump Lists between the two operating systems. The second common Jump List was for the Libre Office Writer. Looking at the data from JumpLister, we could see each of the file paths that were accessed with the application. We found that JumpLister was the best at finding information for the autodest Jump Lists. Though the application could not decipher the AppID, we could see that at least 8 documents were created, although two versions were saved of the same document. The discrepancy in document types is due to the files being saved as both a .docx and a .odt (Figure 9 & 10).

Figure 9(Windows 7):

No.	N...	Date/Time	MAC (New)	Timestamp (New)	MAC (Birth)	Timestamp (Birth)	Data
1	lcdi	Monday, February 10, 2014 8:28:33 PM	00:0c:29:92:a7:24	Monday, February 10, 2014 6:36:22 PM	00:0c:29:92:a7:24	Monday, February 10, 2014 6:36:22 PM	C:\Users\JumpLists\Documents\HelloWorld4.odt
2	lcdi	Monday, February 10, 2014 8:28:44 PM	00:0c:29:92:a7:24	Monday, February 10, 2014 6:36:22 PM	00:0c:29:92:a7:24	Monday, February 10, 2014 6:36:22 PM	C:\Users\JumpLists\Documents\HelloWorld4.docx
3	lcdi	Monday, February 10, 2014 8:27:47 PM	00:0c:29:92:a7:24	Monday, February 10, 2014 6:36:22 PM	00:0c:29:92:a7:24	Monday, February 10, 2014 6:36:22 PM	C:\Users\JumpLists\Documents\HelloWorld.docx
4	lcdi	Monday, February 10, 2014 8:27:48 PM	00:0c:29:92:a7:24	Monday, February 10, 2014 6:36:22 PM	00:0c:29:92:a7:24	Monday, February 10, 2014 6:36:22 PM	C:\Users\JumpLists\Documents\HelloWorld3.docx
5	lcdi	Monday, February 10, 2014 8:27:46 PM	00:0c:29:92:a7:24	Monday, February 10, 2014 6:36:22 PM	00:0c:29:92:a7:24	Monday, February 10, 2014 6:36:22 PM	C:\Users\JumpLists\Documents\HelloWorld2.docx
6	lcdi	Monday, February 10, 2014 8:27:46 PM	00:0c:29:92:a7:24	Monday, February 10, 2014 6:36:22 PM	00:0c:29:92:a7:24	Monday, February 10, 2014 6:36:22 PM	C:\Users\JumpLists\Documents\HelloWorld5.docx
7	lcdi	Monday, February 10, 2014 8:28:13 PM	00:0c:29:92:a7:24	Monday, February 10, 2014 6:36:22 PM	00:0c:29:92:a7:24	Monday, February 10, 2014 6:36:22 PM	C:\Users\JumpLists\Documents\HelloWorld6.odt
8	lcdi	Monday, February 10, 2014 8:28:24 PM	00:0c:29:92:a7:24	Monday, February 10, 2014 6:36:22 PM	00:0c:29:92:a7:24	Monday, February 10, 2014 6:36:22 PM	C:\Users\JumpLists\Documents\HelloWorld6.docx

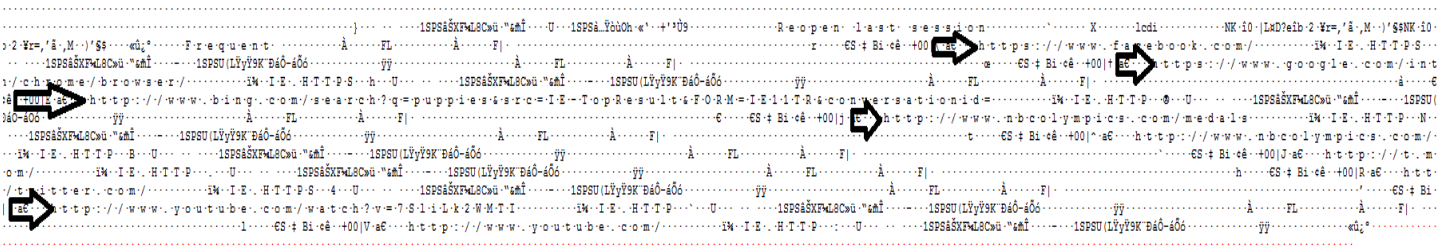
Figure 10(Windows 8):

No.	NetBIOS Name	Date/Time	MAC (New)	Timestamp (New)	MAC (Birth)	Timestamp (Birth)	Data
1	win-upafa6odmqu	Monday, February 03, 2014 8:12:56 PM	00:0c:29:25:57:e4	Monday, February 03, 2014 6:16:28 PM	00:0c:29:25:57:e4	Monday, February 03, 2014 6:16:28 PM	C:\Users\LCDI\Documents\HelloWorld1.docx
2	win-upafa6odmqu	Monday, February 03, 2014 8:06:29 PM	00:0c:29:25:57:e4	Monday, February 03, 2014 6:16:28 PM	00:0c:29:25:57:e4	Monday, February 03, 2014 6:16:28 PM	C:\Users\LCDI\Documents\HelloWorld2.odt
3	win-upafa6odmqu	Monday, February 03, 2014 8:06:10 PM	00:0c:29:25:57:e4	Monday, February 03, 2014 6:16:28 PM	00:0c:29:25:57:e4	Monday, February 03, 2014 6:16:28 PM	C:\Users\LCDI\Documents\HelloWorld3.odt
4	win-upafa6odmqu	Monday, February 03, 2014 8:06:21 PM	00:0c:29:25:57:e4	Monday, February 03, 2014 6:16:28 PM	00:0c:29:25:57:e4	Monday, February 03, 2014 6:16:28 PM	C:\Users\LCDI\Documents\HelloWorld4.odt
5	win-upafa6odmqu	Monday, February 03, 2014 8:06:53 PM	00:0c:29:25:57:e4	Monday, February 03, 2014 6:16:28 PM	00:0c:29:25:57:e4	Monday, February 03, 2014 6:16:28 PM	C:\Users\LCDI\Documents\HelloWorld5.odt
6	win-upafa6odmqu	Monday, February 03, 2014 8:12:57 PM	00:0c:29:25:57:e4	Monday, February 03, 2014 6:16:28 PM	00:0c:29:25:57:e4	Monday, February 03, 2014 6:16:28 PM	C:\Users\LCDI\Documents\HelloWorld3.docx
7	win-upafa6odmqu	Monday, February 03, 2014 8:12:57 PM	00:0c:29:25:57:e4	Monday, February 03, 2014 6:16:28 PM	00:0c:29:25:57:e4	Monday, February 03, 2014 6:16:28 PM	C:\Users\LCDI\Documents\HelloWorld4.docx
8	win-upafa6odmqu	Monday, February 03, 2014 8:12:57 PM	00:0c:29:25:57:e4	Monday, February 03, 2014 6:16:28 PM	00:0c:29:25:57:e4	Monday, February 03, 2014 6:16:28 PM	C:\Users\LCDI\Documents\HelloWorld2.docx
9	win-upafa6odmqu	Monday, February 03, 2014 8:12:57 PM	00:0c:29:25:57:e4	Monday, February 03, 2014 6:16:28 PM	00:0c:29:25:57:e4	Monday, February 03, 2014 6:16:28 PM	C:\Users\LCDI\Documents\HelloWorld5.docx

Chrome did not create any Jump Lists, but we were able to acquire the most recently accessed websites by both Internet Explorer and Mozilla Firefox. The Jump Lists for the web browsers included exact URLs, as well as access times. Using JumpLister to look at the custom destination files showed little information pertaining to the actual websites that were in the Jump List. While examining the hex we can see the exact websites that were

Jump Listed, however. This is the same for Mozilla Firefox, as both Jump Lists were able to show a number of the websites that were accessed (Figure 11).

Figure 11(Windows 8):



For Windows Media Player and Photo Viewer, we were able to easily distinguish what files were viewed with Windows 8. However, one noticeable difference, is that we did not find the Windows photo viewer Jump List in Windows 7. Examing the hex of the data proved very buseful to see what files were accessed, while JumpLister is a good tool to provide the timestamp of when each of the files was accessed.

EnCase v FTK

When we finished the data generation, we used FTK imager to image VMs. When the imaging process was done, we opened the images in FTK to find that the entire image was listed as unallocated space. After comparing the opening the VM files with EnCase Imager, we realized that FTK could not read the file system, which is why the image was empty.(See Figure 1 and 2) we had to restart the process in EnCase Imager which we had not planned to do originally. We reopened the .vmdk file in EnCase Imager and restarted the process which produced readable data. The problem seemed to be that FTK imager could not understand the .vmdk data structure and only showed the file as unallocated space. In order to parse the data we used the EnCase and FTK to look at the data. Unfortunately, FTK was not able to read the data on the file. Figure 1 shows that FTK imager was unable to read the data structure of the file, while EnCase Imager was able to read the same exact file. We have never encountered a situation where FTK Imager was unable to read a .vmdk file. As a result, we only used EnCase Imager to image the rest of the files

Jump List Deletion:

When examining the VMS with deleted Jump Lists, we found that we could not locate any of the deleted Jump Lists data on the Windows 7 VM. FTK and EnCase showed the same results for both VMs; however, we were able to find a portion of the deleted Jump Lists on the Windows 8 VM. For reasons we are unsure of, Encase and FTK only found 4 of the 7 Jump Lists in the *AutomaticDestinations* folder.

Figure 12(Windows 8):

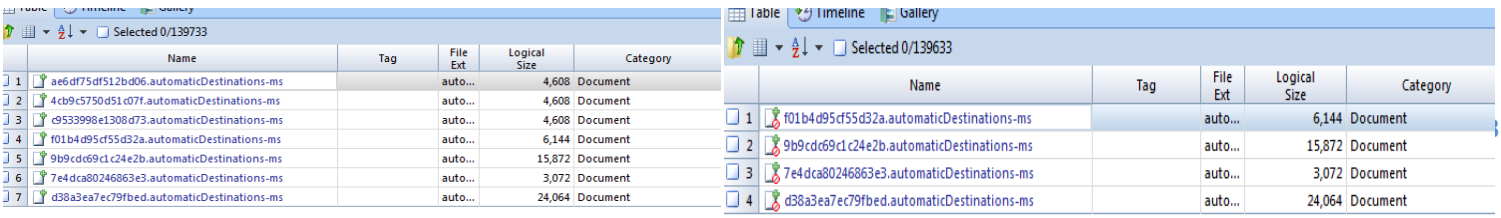
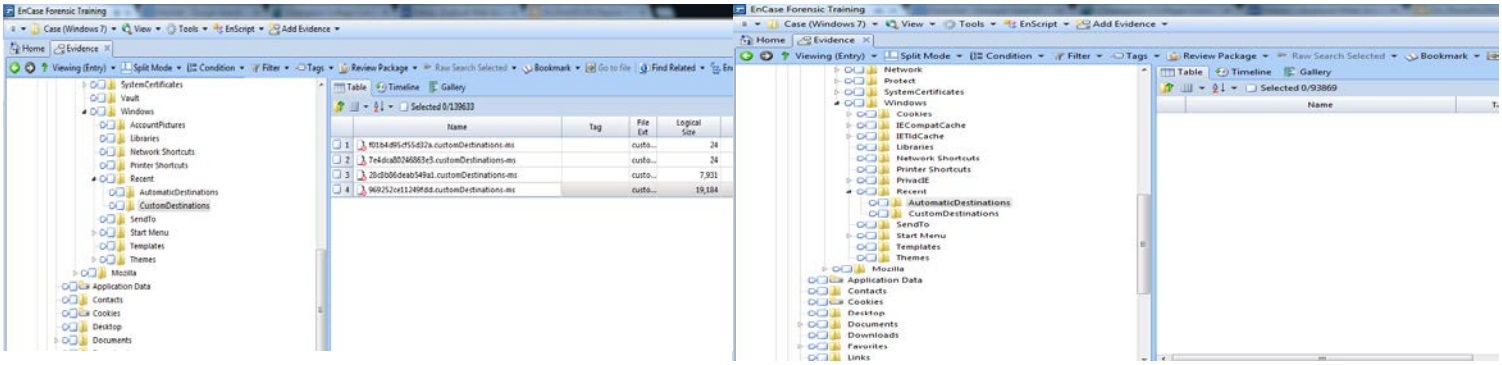


Figure 13(Windows 7):



Conclusion

Overall, we found that Jump List data holds important forensic information, such as time stamps, file paths, and the applications used to create those Jump Lists. According to our findings, the nature of Jump Lists is largely unpredictable as it varies with each application. For example, even though we used Chrome as much as the other web browsers, there were no Jump Lists for the application. We thinkthis might be tied to logging into an account repeatedly as compared to on one single occassion. As for word processors and text editors, we found that they are most likely to create Jump Lists when the feature is turned on. The word processor Libre Office Writer created 8 Jump Lists, showing what files were recently accessed (Figure 3 & 4). In a forensic investigation, this could be useful for an examiner to determine if suspicious documents had been recently accessed. Another important aspect of Jump Lists to note is that they still remain on the computer after an application is deleted (Lyness). When dealing with other default applications such as Windows Media Player and Windows Photo Viewer, I found that Jump Lists were easily located and housed in the automatic destinations folder.

In comparing Windows 8 and Windows 7, the only difference would be the creation of the Windows Photo Viewer Jump Lists. Jump List data also varied between browsers. In terms of the nature of the Jump Lists being created, we found that there were no differences in how information was stored or the file structure of the Jump Lists themselves. The only differences we saw really were that the AppIDs were different because the applications were run from a different file path. Windows 8 did appear to be more avid in creating Jump Lists for each default windows action than Windows 7.

Jump Lists can be very hit or miss in terms of valuable evidence. When an examiner is looking to establish a user's activity, this is a quick and easy way of looking through the hex of each Jump List to see the most recent user activity. Jump Lists may be the most valuable when a user has quickly deleted an application to hide his or her activity.

Further Work

To further research Jump Lists, we might advise to examine applications run from Removable Media Devices to see what differences there may be in Jump Lists, as well as opening documents from Removable Media Devices to see if they have been used.

Appendix A

Table 1: Windows 7 Data Generation

Time	Action	
1:15	*Logged In*	
1:17	*Opened Notepad*	
1:23	*Created 6 .txt files*	Test1, Test2, Test3, Test4, Test5, Test6
1:24	*Opened IE*	
1:25	*Went To Facebook/Logged in*	
1:26	*nbc.com*	
1:27	*Clicked Link to www.nbcolympics.com*	
1:28	*nbcolympics.com/medals*	
1:31	*nbcolympics.com/news/zach-parise-named-united-states-hockey-captain?ctx=team-usa*	
1:34	*bbc.com/news*	
1:36	*www.bbc.co.uk/news/world-europe-26014387*	
1:37	*europa.eu/rapid/press-release_MEMO-14-67_en.html*	
1:41	*www.bbc.co.uk/news/world-europe-26019790*	
1:44	*www.bbc.co.uk/news/world-europe-25925372*	
1:48	*walmart.com*	
1:48	*trending now*	
1:49	*http://www.walmart.com/ip/Sceptre-X505BV-FMDR-50-1080p-60Hz-LED-HDTV/27678567?povid=P1262-TBS-27678567*	
1:50	*Continue shopping*	
1:50	*cnn.com*	
1:51	*http://www.cnn.com/US/?hpt=sitenav*	
1:52	*bing(yahoo mail)*	
1:53	*login.yahoo.com/config/login_verify2?&.src-ym&.intl=us*	
1:54	*bing: puppies*	

1:56	*save picture in images tab*	Saved to Pictures Library
1:59	*bing download chrome*	
1:59	*youtube.com*	
2:00	*http://www.youtube.com/watch?v=7SlILk2WMTI*	
2:03	*twitter.com*	
2:04	*http://www.youtube.com/watch?v=7SlILk2WMTI*	
2:08	*Opened Google Chrome*	
2:08	*Went To Facebook/Logged in*	
2:10	*Clicked Link to www.nbcolympics.com*	
2:11	*nbcolympics.com/medals*	
2:12	*nbcolympics.com/news/zach-parise-named-united-states-hockey-captain?ctx=team-usa*	
2:11	*bbc.com/news*	
2:11	*www.bbc.co.uk/news/world-europe-26014387*	
2:12	*europa.eu/rapid/press-release_MEMO-14-67_en.html*	
2:12	*www.bbc.co.uk/news/world-europe-26019790*	
2:13	*www.bbc.co.uk/news/world-europe-25925372*	
2:13	*walmart.com*	
2:13	*trending now*	
2:13	*http://www.walmart.com/ip/Sceptre-X505BV-FMDR-50-1080p-60Hz-LED-HDTV/27678567?povid=P1262-TBS-27678567*	
2:13	*Continue shopping*	
2:14	*cnn.com*	
2:15	http://www.cnn.com/US/?hpt=sitenav	
2:15	*bing.com/bing(yahoo mail)*	
2:16	*login.yahoo.com/config/login_verify2?&.src-ym&.intl=us*	
2:17	*bing.com/bing: puppies*	
2:42	*save picture in images tab*	http://fascinatingly.com/wp-content/gallery/animals---dogs/puppy-lab-HD-wallpaper.jpg
2:20	*google download Firefox*	
2:20	*youtube.com*	
2:21	*http://www.youtube.com/watch?v=7SlILk2WMTI*	
2:21	*twitter.com*	
2:23	*Opened Firefox*	
2:28	*facebook.com/nbc.com*	

2:30	*Clicked Link to www.nbcolympics.com*	
2:30	*nbcolympics.com/medals*	
2:30	*nbcolympics.com/news/zach-parise-named-united-states-hockey-captain?ctx=team-usa*	
2:30	*bbc.com/news*	
2:31	*www.bbc.co.uk/news/world-europe-26014387*	
2:31	*europa.eu/rapid/press-release_MEMO-14-67_en.html*	
2:31	*www.bbc.co.uk/news/world-europe-26019790*	
2:32	*www.bbc.co.uk/news/world-europe-25925372*	
2:35	*walmart.com*	
2:35	*trending now*	
2:36	*http://www.walmart.com/ip/Sceptre-X505BV-FMDR-50-1080p-60Hz-LED-HDTV/27678567?povid=P1262-TBS-27678567*	
2:37	*cnn.com*	
2:38	*http://www.cnn.com/US/?hpt=sitenav*	
2:38	*bing(yahoo mail)*	
2:38	*login.yahoo.com/config/login_verify2?&.src-ym&.intl=us*	
2:39	*bing: puppies*	
2:40	*save picture in images tab*	http://www.bing.com/images/search?q=puppies&qpvt=puppies&FORM=IGRE#view=detail&id=6A9C71F63307F5D73D062933278F297F098934BB&selectedIndex=7
2:43	*youtube.com*	
2:43	*http://www.youtube.com/watch?v=7SlILk2WMTI*	
2:43	*twitter.com*	
	Chrome	
2:46	*facebook.com*	
2:46	*www.champlain.edu/current-students*	
2:47	*youtube.com*	
2:48	*gmail.com*	logged in, clicked a couple of emails.
2:50	*http://www.imdb.com/?licb=0.8102899217046797*	
2:52	*http://www.imdb.com/name/nm0279545/?ref_=hm_brn_t1*	
2:52	*hulu.com*	
2:53	*reddit.com*	
2:54	www.weather.com/weather/today/Burlington+VT_USVT0033:1:US	
2:55	*engadget.com*	

2:56	*http://www.libreoffice.org/features/writer/*	
2:57	*http://www.libreoffice.org/download*	
2:58	*http://donate.libreoffice.org/home/dl/win-x86/4.2.0/en-US/LibreOffice_4.2.0_Win_x86.msi*	
3:02	*Opened Libre Office Writer*	
3:07	*Saved 5 docs 5 as .odt/.docx*	
3:10	*played kalimba*	Windows Media player
3:10	*Opened "awesomepuppy" "cute puppies" "puppy"*	Windows Photo Viewer
3:11	*Watched Video "wildlife*	Windows Media Player

Table 2: Windows 8 Data Generation

Time	Action	Other
1:50	*Logged In*	
1:54	*Opened Notepad*	
1:58	*Created 6 .txt files*	Test1, Test2, Test3, Test4, Test5, Test6
2:00	*Opened IE*	
2:01	*Went To Facebook/Logged in*	
2:02	*nbc.com*	
2:02	*Clicked Link to www.nbcolympics.com*	
2:02	*nbcolympics.com/medals*	
2:02	*nbcolympics.com/news/zach-parise-named-united-states-hockey-captain?ctx=team-usa*	
2:03	*bbc.com/news*	
2:20	*www.bbc.co.uk/news/world-europe-26014387*	
2:20	*europa.eu/rapid/press-release_MEMO-14-67_en.html*	
2:21	*www.bbc.co.uk/news/world-europe-26019790*	
2:24	*www.bbc.co.uk/news/world-europe-25925372*	
2:25	*walmart.com*	
2:25	*trending now*	
2:26	*http://www.walmart.com/ip/Sceptre-X505BV-FMDR-50-1080p-60Hz-LED-HDTV/27678567?povid=P1262-TBS-27678567*	
	Continue shopping	
2:26	*cnn.com*	
2:26	*http://www.cnn.com/US/?hpt=sitenav*	
2:26	*Bing(yahoo mail)*	
2:27	*login.yahoo.com/config/login_verify2?&.src-ym&.intl=us*	
2:28	*Bing: puppies*	

2:28	*save picture in images tab*	Saved to Pictures Library
2:28	*Bing download chrome*	
2:30	*youtube.com*	
2:32	http://www.youtube.com/watch?v=7ILk2WMTI	
2:33	*twitter.com*	
2:33	*http://www.youtube.com/watch?v=7SlILk2WMTI*	
	Opened Google Chrome	
2:35	*Went To Facebook/Logged in*	
2:37	*Clicked Link to www.nbcolympics.com*	
2:37	*nbcolympics.com/medals*	
2:37	*nbcolympics.com/news/zach-parise-named-united-states-hockey-captain?ctx=team-usa*	
2:38	*bbc.com/news*	
2:39	*www.bbc.co.uk/news/world-europe-26014387*	
2:40	*europa.eu/rapid/press-release_MEMO-14-67_en.html*	
2:40	*www.bbc.co.uk/news/world-europe-26019790*	
2:42	*www.bbc.co.uk/news/world-europe-25925372*	
2:43	*walmart.com*	
2:43	*trending now*	
2:45	*http://www.walmart.com/ip/Sceptre-X505BV-FMDR-50-1080p-60Hz-LED-HDTV/27678567?povid=P1262-TBS-27678567*	
	Continue shopping	
2:45	*cnn.com*	
2:46	http://www.cnn.com/US/?hpt=sitenav	
2:47	*bing.com/bing(yahoo mail)*	
2:47	*login.yahoo.com/config/login_verify2?&.src-ym&.intl=us*	
2:48	*bing.com/bing: puppies*	
2:48	*save picture in images tab*	http://fascinatingly.com/wp-content/gallery/animals---dogs/puppy-lab-HD-wallpaper.jpg
2:49	*google download firefox*	
2:49	*youtube.com*	
2:49	*http://www.youtube.com/watch?v=7SlILk2WMTI*	
2:50	*twitter.com*	
2:51	*Opened Firefox*	
2:52	*facebook.com/nbc.com*	
2:52	*Clicked Link to www.nbcolympics.com*	
2:52	*nbcolympics.com/medals*	
2:53	*nbcolympics.com/news/zach-parise-named-united-states-hockey-captain?ctx=team-usa*	
2:55	*bbc.com/news*	
2:57	*www.bbc.co.uk/news/world-europe-26014387*	
2:57	*europa.eu/rapid/press-release_MEMO-14-67_en.html*	

2:58	*www.bbc.co.uk/news/world-europe-26019790*	
2:58	*www.bbc.co.uk/news/world-europe-25925372*	
2:58	*walmart.com*	
	trending now	
2:58	*http://www.walmart.com/ip/Sceptre-X505BV-FMDR-50-1080p-60Hz-LED-HDTV/27678567?povid=P1262-TBS-27678567*	
3:01	*cnn.com*	
3:01	*http://www.cnn.com/US/?hpt=sitenav*	
3:02	*bing(yahoo mail)*	
3:02	*login.yahoo.com/config/login_verify2?&.src-ym&.intl=us*	
3:02	*bing: puppies*	
3:03	*save picture in download*	3
3:04	*youtube.com*	
3:04	*http://www.youtube.com/watch?v=7SlILk2WMTI*	
2:05	*twitter.com*	
3:00	*Chrome*	
3:06	*facebook.com*	
3:07	*www.champlain.edu/current-students*	
3:09	*youtube.com*	
3:10	*gmail.com*	logged in, clicked a couple of emails.
3:10	*http://www.imdb.com/?licb=0.8102899217046797*	
3:11	*http://www.imdb.com/name/nm0279545/?ref_=hm_brn_t1*	
3:11	*hulu.com*	
3:12	*reddit.com*	
3:12	www.weather.com/weather/today/Burlington+VT_USVT0033:1:US	
3:12	*engadget.com*	
3:13	*http://www.libreoffice.org/features/writer/*	
3:14	*http://www.libreoffice.org/download*	
3:15	*http://donate.libreoffice.org/home/dl/win-x86/4.2.0/en-US/LibreOffice_4.2.0_Win_x86.msi*	
3:16	*Opened Libre Office Writer*	
	Saved 5 docs 5 as .odt/.docx	

References

Carvey, H. (2011, December 28). Windows Incident Response. Jump List Analysis. Retrieved from http://windowsir.blogspot.com/2011/12/jump-list-analysis.html

Carvey, H. (2011, September 8). Jump List Analysis, Pt III. Retrieved from http://windowsir.blogspot.com/2011/09/jump-list-analysis-pt-iii.html

Cowen, D. (2013, August 20). Hacking Exposed Computer Forensics Blog: Daily Blog #58: Understanding the artifacts Jump Lists. Retrieved from http://hackingexposedcomputerforensicsblog.blogspot.com/2013/08/daily-blog-58-understanding-artifacts.html

Hexacorn | Blog. (2013, April 20). Retrieved from http://www.hexacorn.com/blog/2013/04/30/jumplists-file-names-and-appid-calculator/

Jump Lists. (n.d.). *Forensics Wiki*. Retrieved from www.forensicswiki.org/wiki/Jump_Lists

JumpLister. (n.d.). *Woanware*. Retrieved from http://www.woanware.co.uk/forensics/jumplister.html Carvey, H. (2011, August 24). Jump List Analysis, pt II. Retrieved from http://windowsir.blogspot.com/2011/08/jump-list-analysis-pt-ii.html

Lyness, R. (2012, October 30). Forensic Analysis of Windows 7 Jump Lists. *Forensic Focus Articles*. Retrieved from http://articles.forensicfocus.com/2012/10/30/forensic-analysis-of-windows-7-jump-lists/

Microsoft. (2011). Application User Model IDs (AppUserModelIDs). Retrieved from http://msdn.microsoft.com/en-us/library/dd378459%28v=vs.85%29.aspx

Microsoft. (n.d.). [MS-SHLLINK]: Shell Link (.LNK) Binary File Format. Retrieved from http://msdn.microsoft.com/en-us/library/dd871305.aspx

Pullega, D. (2013, September 7). 4n6k: Jump List Forensics: AppIDs Part 1. Retrieved from http://www.4n6k.com/2011/09/jump-list-forensics-appids-part-1.html