International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 03, March-2015

Forensic Analysis of Jump Lists in Windows Operating System

Kritarth Y. Jhala
Digital Forensics Analyst
eSF Labs Ltd.
Hyderabad , India

A. Anisetti
Digital Forensics Analyst
eSF Labs Ltd.
Hyderabad , India

***Abstract*— The release of Microsoft Windows 7 introduceing a new interesting feature which known as Jump Lists that present the user with links to recently used or accessed files grouped on a application basis. Windows 7 Jump Lists are a new interesting artifacts of the system usage which may have some significant values during forensic analysis where user's different activities are of interest.**

Keywords—Windows Jump Lists Analysis, Windows Forensics, Windows Recent View items analysis,

I. INTRODUCTION

The Jump Lists are the feature of Windows 7 & above provides the user with a graphical interface that associated with each & every installed application files which lists that have been previously accessed by that particular user.

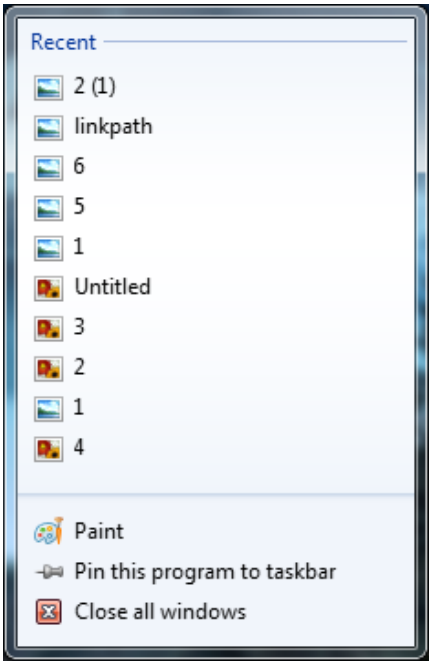


Fig 1. Jump List example associated with MS Paint.

As shown in Fig. 1, it is possible for a user to pin the different types of items.

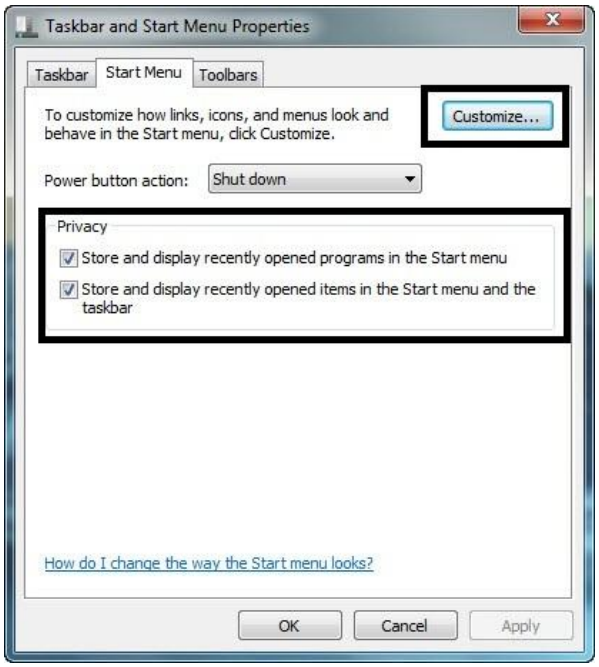


Fig 2. Taskbar and Start Menu Properties Dialog box.

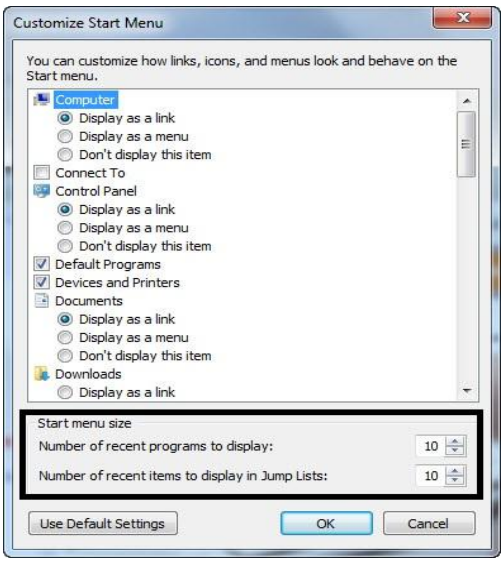
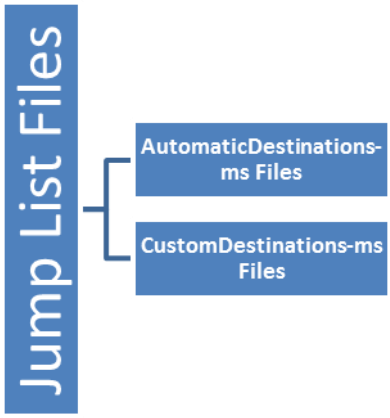


Fig 3. Customize Start Menu Dialog Box.

In this paper, Section 2 gives an overview of actual backend information of the jump lists in the windows operating system. Section 3 is described the AppID of the diferent windows applications.Section 5 presents the forensically evaluation of the solution.

II. Background Information

When the application performs un certain actions, two types of files are genrated that are as below :



A. *AutomaticDestinations-ms files*

- C:\User\(username)\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
- automaticDestinations-ms (autodest) filesare created by the operating systems. When the user performs different uncertain actions like opening files, using the remote desktop connection tools etc. The Jump Lists Appear to be associated produced through file extension analysis.

B. *CustomDestinations-ms files*

- C:\Users\(username)\AppData\Microsoft\Windows\Recent\CustomDestinations
- customDestinations-ms (customdest) files are created when the user pins a file to an application via taskbar These files are appear to consist of stacked segments.

*** Remark : These all directories are hidden. ***
(You have to type full folder path in the address bar to see the contents)

III. Application ID

Calculates the Windows operating system the AppID of an application, knowing as an application's AppID can help identify the identity of any given applications,when user activity is consist a special importance in an investigation. The different files are named with 16 hexadecimal digits, that known as the AppID and that AppID can be followed by the file extension automaticDestinations-ms.These AppIDs can be set by the application or operating system at application runtime.

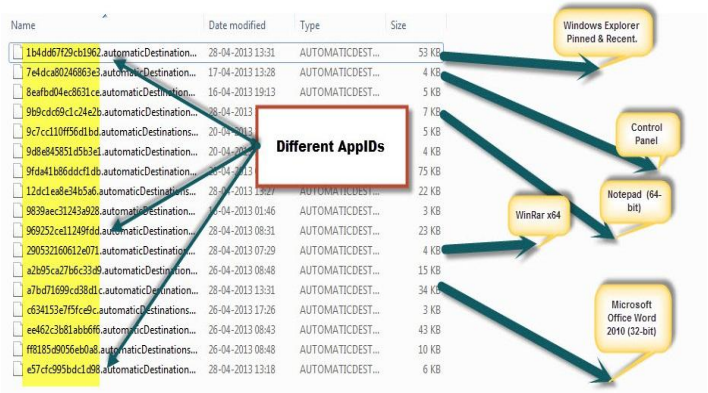


Fig 4 Different AppIds

AppIds:

TABLE I. INTERNET BROWSERS

AppID	Application Description
5d696d521de238c3	Chrome Versions 9.0.597.84 / 12.0.742.100 / 13.0.785.215
cfb56c56fa0f0a54	Mozilla Version 0.9.9
5c450709f7ae4396	Firefox Version 1.0 to 3.0
5df4765359170e26	Firefox Version 4.0.1
1eb796d87c32eff9	Firefox Version 5.0
1461132e553e2e6c	Firefox Version 6.0
28c8b86deab549a1	Internet Explorer Versions 8 or 9
16ec093b8f51508f	Opera Version 8.54 /9.64 /11.50
8a1c1c7c389a5320	Safari Version 3.2.3 (525.29)
1da3c90a72bf5527	Safari Version 4.0.5 (531.22.7) to 5.1 (7534.50)

TABLE II. IMAGE/DOCUMENTS VIEWERS

AppID	Application Description
f0468ce1ae57883d	Adobe Reader Version 7.1.0
c2d349a0e756411b	Adobe Reader Version 8.1.2
ee462c3b81abb6f6	Adobe Reader Version 10.1.0
386a2f6aa7967f36	EyeBrowse Version 2.7
e31a6a8a7506f733	image AXS Pro Version 4.1
b3f13480c2785ae	Paint Version 6.1
7cb0735d45243070	CDisplayVersion 1.8.1.0
3594aab44bca414b	Windows Photo Viewer
169b3be0bc43d592	Fast Picture Viewer Pro. 1.6
d33ecf70f0b74a77	Picasa Version 2.2.0
83b03b46dcd30a0e	iTunes Version 10
271e609288e1210a	MS Office Access 2010 x86
a7bd71699cd38d1c	MS Office Word 2010 x86
cdf30b95c55fd785	MS Office Excel 2007
9839aec31243a928	MS Office Excel 2010 x86
3094cdb43bf5e9c2	MS Office OneNote 2010 x86
be71009ff8bb02a2	MS Office Outlook x86
f5ac5390b9115fdb	MS Office PowerPoint 2007
9c7cc110ff56d1bd	MS Office Powerpoint 2010 x86
adecfb853d77462a	MS Office Word 2007 pinned & recently used
12dc1ea8e34b5a6	Paint 6.1
918e0ecb43d17e23	Notepad (32-bit)
e70d383b15687e37	Notepad++Version 5.6.8 x86

TABLE III. MEDIA PLAYERS

AppID	Application Description
d22ad6d9d20e6857	ALLPlayer Version 4.7
817bb211c92fd254	GOM Player Versions 2.0.12.3375 to 2.1.28.5039
6bc3383cb68a3e37	iTunes version 7.6.0.29 to 8.0.0.35
83b03b46dcd30a0e	iTunes version 9.0.0.70 and 9.2.1.5 and 10.4.1.10
7593af37134fd767	RealPlayer Version 6.0.6.99 and 7 and 8 and 10.5
37392221756de927	RealPlayer Speacial Pack 12
f92e607f9de02413	RealPlayer Version 14.0.6.666
4acae695c73a28c7	VLC Version 0.3.0 and Version 0.4.6

TABLE IV.SYSTEM CLEANERS

AppID	Application Description
ed7a5cc3cca8d52a	CCleanerVersions 1.32.345, 1.41.544, 2.36.1233 &3.10.1525

TABLE V. UTILITIES (32-BIT)

AppID	Application Description
3dc02b55e44d6697	7-Zip version 3.13 /4.20 /4.65/9.20
337ed59af273c758	Sticky Notes
290532160612e071	WinRAR version 2.90 / 3.60 / 4.01
b74736c2bd8cc8a5	WinZip version 15.5
bc0c37e84e063727	cmd.exe for 32-bit

IV. EXPERIMENTAL SETUP

All experiments were conducted in a virtual environment, this was achieved by using virtual environment in VMWare Workstation 9.0 and a merchandise copy of Windows 7 Ultimate 64bit operating system with no service packs.

A virtual environment was created with two virtual disks attached with the file system that consist NTFS format, the first task to hold the OS and the second task to store a series of different specimen texts, pictures, musics and videos files.

Different date & time settings of the virtual environment and all differnt clones are made from it were deliberately maintained in GMT+5.5. in order to assist in how differnt dates and times are captured by jump lists.

Conducted experiments designed for a specific points with that a view to understanding the full architecture of the records maintained by windows operating system jump lists and were broken down into particular objectives.

A. Identifying the initial Jump List data.

The initial stage of this processes were to carry out a fresh installation of OS & that was Windows 7. The virtualisation environment was used to capture a snippets at the completion of the installation and than after an account was created. End of the process was allowed to complete by the newly created user logging on for the first time after that the virtual environment was shut down without accessing any files.

All further experimentats was based upon counterfeit of the virtual environment where the password was applied to the user accounts and various tests were done to change the configuration of the different feature and update the records that maintained by it.

B. Modification in Config. Settings

The modification was achieved by accessing the customize start menu dialog box and that dialog box was resulted in the creation of the registry key value

HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Startjumplistitems

After the deselecting that particular option to store and display different afreshly seen items in the start menu.Further experiments identified that the data. In this either value is '0 'when the feature is disabled or '1' when enabled.

The next step was to use the regedit application of the windows operating systems to access the value of the registry and that is

HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Start JumpListI tems

before changing the data of the value of jumplists start items to 25 before closing regedit application and by accessing the relevant dialog box again to displayed values. None of these values were present at the time of first login.

C. Open files

A number of different sample files are held on the another virtual hard disk were opened using differnt applications included with Windows Operating System like Notepad and WordPad for text,Windows Media Player and Windows Media Center Windows Photo Viewer and Paint for image & picture files,,VLC player,Real Players for video, sound and pictures etc.

D. Data present at first login.

The different functional areas of the different files and folder structures and the windows operating system registries that are generally used to store relevant data to the jump lists that has been created within a current user account at the point that account logs in first.

A fresh install of windows oprating system resulted in the applications like Internet Explorer, Windows Explorer, Windows Media Player, Snipping Tool etc. are automatically being pinned to the taskbar without interaction with the user.

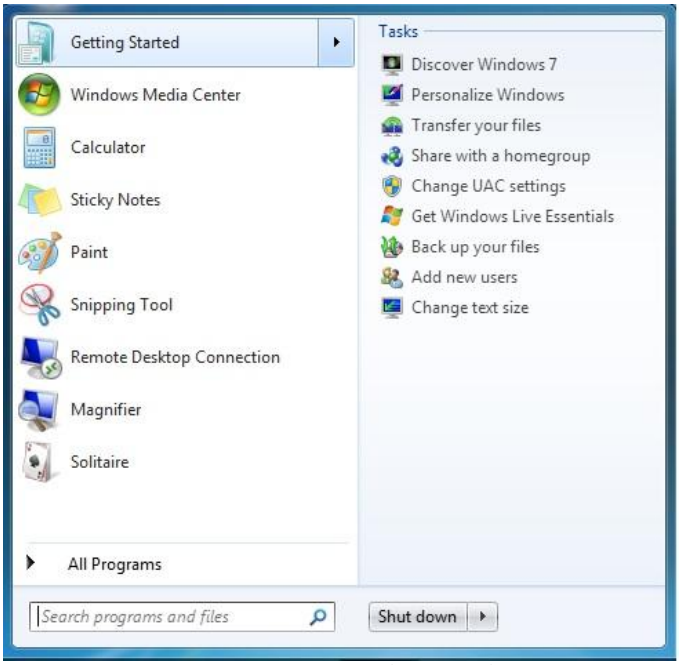


Fig. 5 Start Menu and Taskbar at first login of Windows OS

The directory path of the file is :
(username)\appdata\roaming\microsoft\explorer\quick launch\userpinned\taskBar
found to containing three different shortcut files relating to those three applications.

According to that different application was pinned and found in the windows registry value too.
HKLM>Software>Microsoft>Windows>CurrentVersion> explorer>taskband>favorites & favorites Resolve.

The windows registry value did not exist at this stage.that can be shown in the path of

HKLM>Software>Microsoft>Windows>CurrentVersion> Explorer >Advanced>start JumpList Items

When the system was configured as to showing the different hidden files and folders or not, the automatic destinations directory couldn't be seen when user attempt to navigate to hidden files through the windows explorer.

Suppose however users were entered the full files & folder path into the address bar, the content of the directories could be seen by the user. Navigating to it from a cmd & that had no such problems.

Once jump lists b4dd67f29cb1962.automatic are named, Destinations-ms '1 'exists within the AutomaticDestinations at first login that directory contains different four entries which relating to the different libraries that are available through Windows Explorer.

E. Deleted date of Jump List.

A no. of approaches that applied for deleting the entries from a Jump Lists were tested by different tecniques that are as :

- Manually selecting each and every entry through a right mouse click> remove it from the list.
- When option is deselecting it is to store and display recently used or opened items in the start menu of windows operatin system.
- Navigate to the AutomaticDestinations directory and deleting the compound binary files from the windows explorer

V. Forensics Analysis

A further entry entitled with DestList and it is also present and due to this element is structured, the little information is available relating to that the information contained within these jumplists elements.

A. DestList Structure

A DestList Structure appeared as the first 8 bytes of an entry were kind of hash of the data. Minimal experiment was conducted where a mono byte in each of the easily identified byte sequence in each & every entry was ambeded in a hex editor. As to finding the following observations were made :

- Any change occure in the data entry between the starting point of the unidentified 8 byte value before the data file path would result in any entries within the list after altered entry of data does not appearing in the jump list.
- By changing the path of the files & folders had no effects and the targeted file was opened when the entry was clicked. The jump list was rewritten to amend the file path to show the correct information once again.
- The findings are supported that the entry which consist of first 8 bytes that is kind of hash .

Structure of the DestList elements are available in table header and header entry below

TABLE VI. STRUCTURE OF DESTLIST HEADER AND HEADER ENTRY FORMAT

Offset	Characteristic
0 to 3	First Issued entry ID. Naturally appears & value is always be 1
4 to 7	Shows several number of current entries in jumplist
8 to 11	Shows total number of pinned entries
12to15	Describe floating point value. Some kind of counter.
16to23	Shows last issued entry ID number
24to31	Describe number of add or delete actions Increments as entries are incleded. it increments as individual entries are deleted too.
Structure of 'DestList' Header Entry Format	
0 to 7	Shows as a checksum or hash of the entry.
8 to 23	Describes new volume ID
24to39	Shows Object ID
40to55	Shows birth Volume ID
56to71	Describes object ID
72to87	Shows NetBIOS name of volume where target file is stored.
88to95	Shows entry ID number
96to99	Shows floating point counter to record each and every time the files are accessed or not .
100 to 107	Describes MSFILETIME of last recorded access
108to 111	Shows the entry 'pin' status.
112 to 113	Describes Length of Unicode entry string data
114	Entry string data

B. Accessing File

Most of the created jump lists are record the paths of the files to their respective target files in plain text with unique unicode encoding. The figure shows an encrypted view of windowsmedia file. Windows media player did not follow this trend but instead of this it uses a series of alphanumeric characters to document this information as shown in fig below:

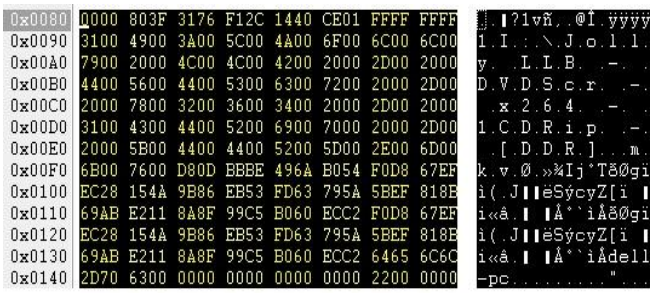


Fig. 6 Hex Value of Media file

The link file of elements in windows media player also are different but in some point to the different executable itself with the different path of the target files recorded as a key during the execution of program.

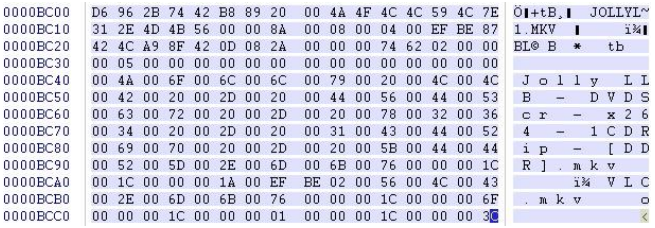


Fig. 7 Example of file path recorded by Media Player

It has been noted windows media player that had recorded two entries for each and every file accessed.One stored with the file path as describe in figure and the other one with the full path. The respective file link elements replicated this with a point to the executable files and the other following the more convenient format with the different link associated files.

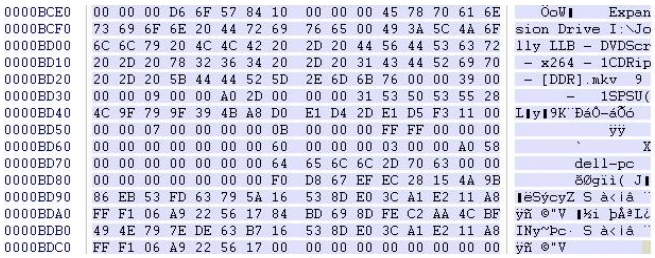


Fig. 8 Example of Link File by Media Player

Not all applications that use all of the different fields that are available in a DestList entry.Below figure shows the difference between the amount of data recoded within the two different entries taken from the same DestList.

When the target files are moved on different drives between the registered machines.Files that have been removed from the recycle bin on drives within the same location & the user who is given an opportunity to restoring a targets to original its location or removed the entry from the jump lists.

For which have been moved files to a drive with the registered type removable such as USB devices any venture to re open a file subjected to such a deletion or move results in an error message is displayed on user screen.

C. Access Order

The list that shown on screen to the user and it stored in the 'DestList' element in LIFO (Last In First Out) manner , with each & everu subsequent entry being append to the list above the preceding entry.

D. Pinning/Unpinning Items

Accurate files & folders can be pinned to the jump lists but not to the taskbar.

The initial item was pinned to the start menu as a new sub directory that known as start menu is created within the path

C:\Users\(username)\AppData\Roaming\Microsoft\ Internet Explorer\Quick Launch\User Pinned

That is used to store a shortcut files relating to that item. Unpinning from the start menu of taskbar results in the shortcut file being removed from the start menu sub directory.

A programs are pin to the start menu or and .lnk file is created and stored in sub-directory

C:\Users\(username)\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned \

Record of these items were pointed to the taskbar is added to the data in the different values favorites and Favorites Resolve too. Within the windows registry

HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Taskband

If shortcut of those files are removed from the respective venues Either manually or during an application uninstallation action the corresponding traces within the folder structure & windows registry values are removed too but any jump lists created it from the use of that programs that remaining intact.

The testing conducted showed that the overall number of items that pinned to the jump lists and that is recorded within the header of the DestList.

Pinning an entry to the jump list results in an update to 4 bytes in sequence in the DestList's and that record behave like a counter and changes from the default hexadecimal numeric value.That occurred as a results of pinning a single entry to jump lists are shown at below figure :

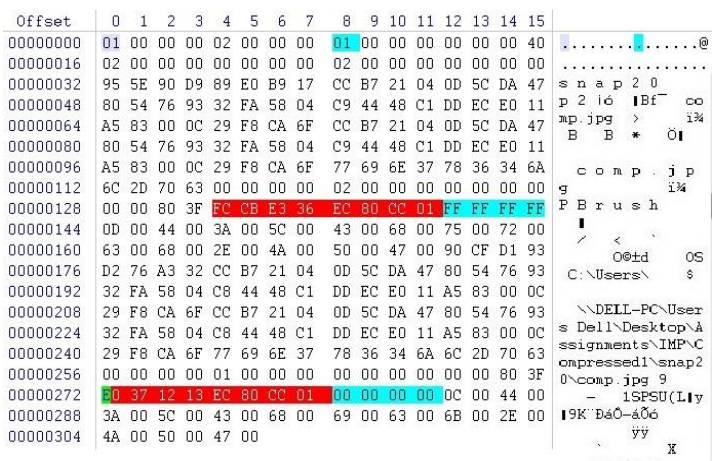


Fig. 9 Changes to 'DestList' element of MSPaint Jump Lists after pinning a single entry

E. Deleting Files Of Jump List

Input at the Command Prompt of the

C:\Users\Win7\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\

resulted in entertained by the contents of the AutomaticDestinations.

Expanding of files of the jump list and manuall the entries are deleted by using the remove from this list option the following tasks were noted:

- A pinned data or entry would not removed until it had been unpinned form the jump list.
- Whenever the last entry was removed from the list, entertained by the Jump List file was deleted from the AutomaticDestinations directory.

The task of removing an entry within the jump list may change the header of the DestList element as a depicted in figure below that provides the elaboration into the structure of that part of that particular element.

List before Deletion-2 Entries

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13
00000000	01	00	00	00	02	00	00	00	01	00	00	00	00	00
00000016	02	00	00	00	00	00	00	00	02	00	00	00	00	00

List after Deletion-1 Entry

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13
00000000	01	00	00	00	01	00	00	00	01	00	00	00	00	00
00000016	02	00	00	00	00	00	00	00	03	00	00	00	00	00

Fig. 10 Changes to DestList element after deleting an entry via the Jump List

After the deselecting the option to store and display recently used as well as opened items in the start menu as well as the taskbar from the dialog box the was noted as follow :

- All the files of Jump List contained no pinned that elements were removed from the automatic destinations directory.
- Jump Lists for those that contain pinned items and all different entries were removed from that list and having only records that are relating to the pinned elements.
- The binary files of the jump lists can be fetched from the Automatic Destinations directory and running on a machine without changing the data that containing by them.

VI. CHALLENGES

Jump Lists are newly introduced feature although windows operating system has been out for a while now some of the issues have already come up. Initial concurrence indicated that at least one jump list record may has been recovered from unallocated space of disk but it turned out that the different three problems of jump lists were from a live acquisition of an images and the applications in question could have been open on the system at a time of the acquisition

This may represents an interesting valid problem that how do user deal with jump lists from live acquisition of images in the case of the apps were open during the acquisition ?

The answer is that user need to understand the binary structure of the jump lists because that is the only way to solve these types of issues. When the tools are not working we need to either have the understand the formats to troubleshoot the issue ourself.

VII. CONCLUSION

From an analyst's point of view Jump Lists are a newly introduced technology and artifact in the windows operating systems that need to be understood better.

At this point we have considerable information which clearly indicates that these artifacts of windows operating system have value and should be parse in timelines for analysis.

There are different ways for jump lists to containing analytic attributes similar to the registry and registry values and also to prefetch files that bound specific user actions.

In addition the research area is necessary but that appears recently that jump lists also representing a persistent artifact which remains after deleted different files, folders and applications.

ACKNOWLEDGMENT

This work was supported by eSF Labs Ltd, Hydreabad,India, that provided the technical conditions and the machines used for the development and testing of the solution.

REFERENCES

[1] The hidden power of Windows Jump Lists : http://www.pcworld.com/article/2858321/the-hidden-power-of-windows-jump-lists.html
[2] Take full advantage of Jump Lists in Windows 7 with these tips : http://www.techrepublic.com/blog/windows-and-office/take-full-advantage-of-jump-lists-in-windows-7-with-these-tips/
[3] AccessData Registry Quick Find Chart: http://accessdata.com/media/en_us/print/papers (July 2011).
[4] Jumplists : http://www.forensicswiki.org/wiki/Jump_Lists
[5] AppID : http://en.wikipedia.org/wiki/Apple_ID
[6] Carvey, H.,Jump List DestList Structure. Windows Incident Response : http://windowsir.blogspot.com/2011/06/meetup–tools–and–other–stuff.html (8 Sep 2011).
[7] Windows Forensics And Security : http://articles.forensicfocus.com/2014/04/14/windows-forensics-and-security/ (April 2014)