woanware

JumpLister

About

woanware is the name for a set of tools and applications I have written. The majority of the tools/applications are related to networking, network security, application security or digital forensic tasks.

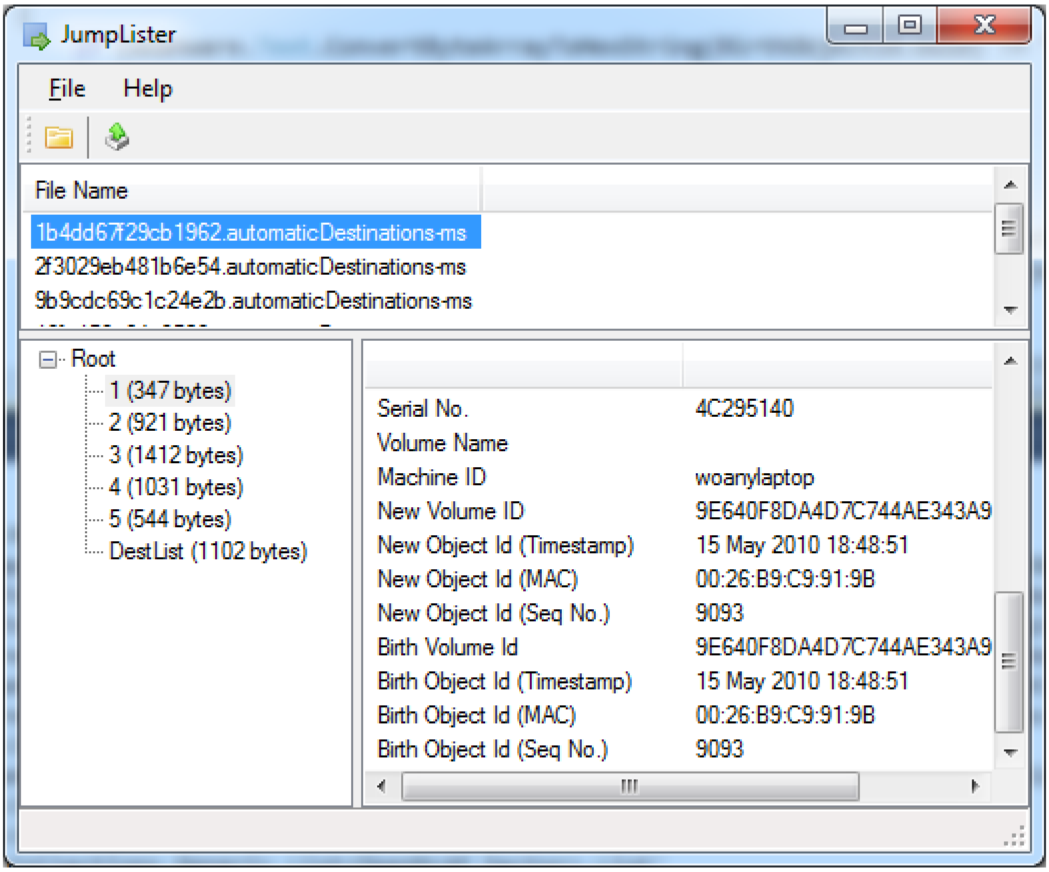
Introduction

Jump Lists have been widely discussed within the forensic community, in particular on the win4n6 mailing list. Jump lists from a forensic perspective have been described as follows (Troy Larson):

```
“put a MS-CFB (compound file binary file format) parser in front of the
link file parser, you will have a tool that opens Windows 7 Jump lists”
```

So that means they are a MS-CFB with N... MS-SHLLINK, so that’s what this application does.

JumpLister 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. It uses the LNK parser I wrote so stuff like object ID’s and MAC addresses are handled.



File Name
1b4dd67f29cb1962.automaticDestinations-ms
2f3029eb481b6e54.automaticDestinations-ms
9b9cdc69c1c24e2b.automaticDestinations-ms

Serial No.	4C295140
Volume Name	
Machine ID	woanylaptop
New Volume ID	9E640F8DA4D7C744AE343A9
New Object Id (Timestamp)	15 May 2010 18:48:51
New Object Id (MAC)	00:26:B9:C9:91:9B
New Object Id (Seq No.)	9093
Birth Volume Id	9E640F8DA4D7C744AE343A9
Birth Object Id (Timestamp)	15 May 2010 18:48:51
Birth Object Id (MAC)	00:26:B9:C9:91:9B
Birth Object Id (Seq No.)	9093

Opening

- To parse a jump list file, use the File->Open menu item, an Open File dialog will be displayed. Select one or more files. The application will parse each file and display the file names in the top list.

It appears that entries can exist in the DestList streams, and not have a matching LNK structure within the JumpList. JumpLister can detect this and if any are identified then it will prompt the user once the loading has finished to save an error log, which will detail the file, stream no. and DestList info.

Viewing

To view a particular file's details, just select the appropriate file name from the top list, the available streams will be displayed in the tree view, located in the bottom left hand corner.

By selecting a particular stream the LNK details will then be displayed in the list view, located in the bottom right hand corner

Export

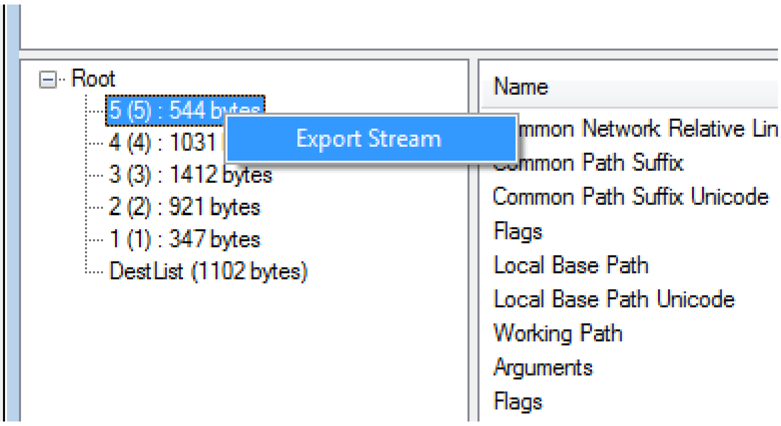
The export works on which ever files are selected in the upper list, so if you want to export more than one file's details at once, then use the SHIFT click or CTRL click method to select each required file.

- Select each file that you want to export
- Click the Export toolbar button or use the File->Export menu item, a folder selection dialog will be displayed
- Select the output folder, click the OK button
- Each file will be output in the format FILENAME.STREAM_NO.txt
-

Stream Export

The individual streams can be exported via the tree view located in the bottom right of the main window.

- To export a stream, select the stream then right click to display a context menu, use the Export Stream menu item
- A Save As dialog will be displayed, choose the export file name/path, click the Ok button. The stream will be exported to the choose file.



Version History

v1.1.0

- Updated OpenMCDF to 1.5.4. R2
- Removed ComponentFactory.Krypton.Toolkit dependency
- Updated the AppIds.txt file from Phill Moore (https://github.com/randomaccess3/4n6_stuff/blob/master/AppID.txt)
- Updated to use shellify LNK parsing library rather than my own
- Updated shellify library to search for LNK structures
- Updated shellify library to parse UUID V1 structures
- Updated the DestList parsing using Rob Lyness's analysis:

http://articles.forensicfocus.com/2012/10/30/forensic-analysis-of-windows-7-jump-lists/

- Added MAC address and timestamps (New and Birth) columns to the DestList list
- Updated the DestList export to include the new DestList fields
- Updated the LinkInfo export to include the new DestList fields

v1.0.6

- Modified the list view output when viewing the DestList to output to decimal. Note this only applies if you have set the appropriate option. Thanks JimmyW
- Added the ability to export the individual streams from the jump list files e.g. the LNK streams or the DestList stream. The functionality can be used by right clicking on the stream in the treeview, located in the bottom right.

v1.0.5

- Added the stream no. to the link info reports (both CSV and txt). Thanks JimmyW
- Modified to allow the representation of HEX values as decimal. Configured via the Tools->Options menu item. The decimal represents occur both in the UI and in the exports. Thanks JimmyW
- Corrected toolbar tooltips! Woo!

v1.0.4

- Fixed an issue where the DestList data was concatenated in each export file. Thanks JimmyW
- Modified the DestList parsing to remove nulls from the NetBIOS value

v1.0.3

- Fixed issue where the DestList stream numbers need to be used as a HEX value to extract the main LNK stream/structure. Thanks JimmyW

v1.0.2

- Added extra error handling around the streams opened via prior identification in the DestLists, since it appears that the DestList can contain StreamNo. entries/data that don't exist as LNK structures/streams. Thanks to StewardD for the sample files.

v1.0.1

- Added ability to parse the DestList data (http://www.forensicswiki.org/wiki/Jump_Lists).
- Added AppId lookup. Thanks StewardD for suggestion. Also thanks for the research performed by various people for the Forensics Wiki (http://www.forensicswiki.org/wiki/List_of_Jump_List_IDs)
- Modified the export to create "AppIds.txt" file, which lists the filenames and the related application
- Modified the export to create "AppIds.csv" file, which lists the filenames and the related application
- Modified the export to create "LinkInfo.csv" file, which lists all of the LNK data from each of the streams, plus the DestList data for each of the streams identified
- Modified the export to create "DestList.csv" file, which lists all of the DestList data

v1.0.0

- Initial public release