

CAL POLY

California Cybersecurity
Institute

Computer Forensics CCIC Training

Chapter 6: Recent Files

Lauren Pixley, Cassidy Elwell, and James Poirier

May 2019 (Version 2)



This work by [California Cybersecurity Institute](#) is licensed under a [Attribution-NonCommercial-NoDerivatives 4.0 International License](#).

6

Recent Files

Introduction

From an investigative standpoint, you usually want to determine what files a user recently accessed. It gives you a perspective on how the user used the computer, and it also associates file activity back to the suspect. This will help demonstrate their knowledge about the existence of the files and show that they opened and viewed it. In this chapter, we will focus on link files and jump lists. Both of these artifacts will show you what files the user opened.

Link Files

You are going to first look in Craig's Recent folder. This is located in the following path for versions 7-10 of Windows:

`C:\Users\Craig\AppData\Roaming\Microsoft\Windows\Recent`

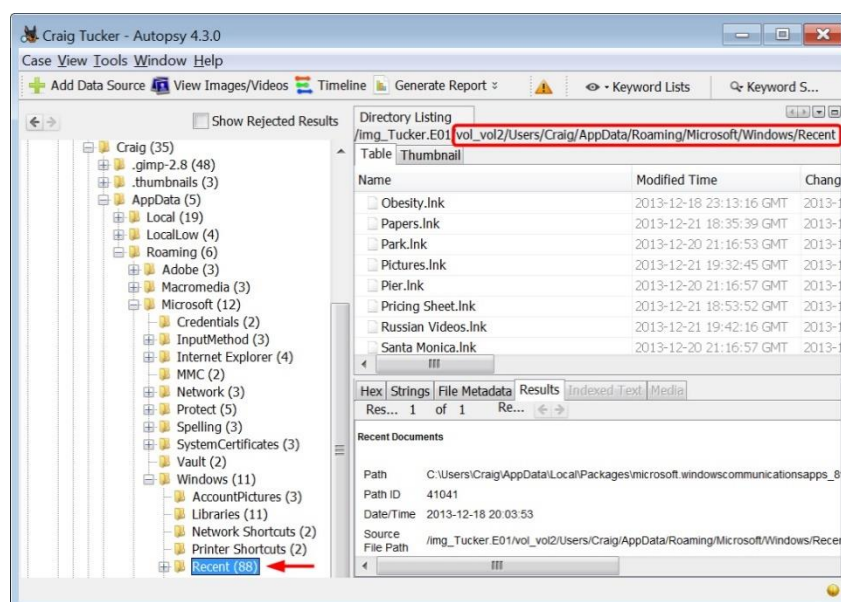


Figure 6-1 – Craig's Link Files in Recent Folder

This folder contains the user's link files. A link file, or LNK, is a Windows shortcut that points back to an original file. A link file is generally created when a file is first opened. Link files are important during analysis, because they show where files were located, when they were opened, and they contain date and time stamps associated with the file. If you look at Windows Explorer and go to the Recent folder, you can see your own link files.

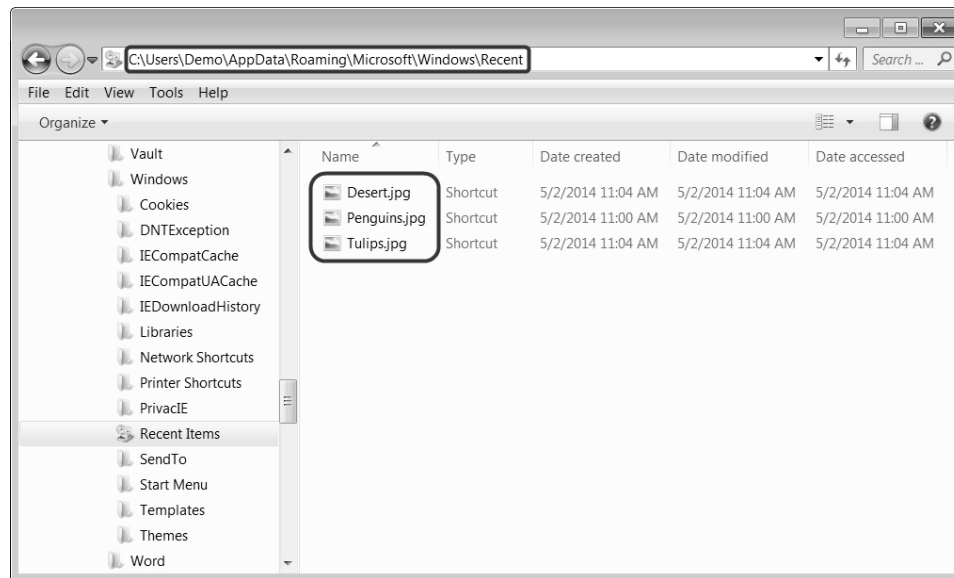


Figure 6-2 – Link Files in Windows Explorer

Note: To view the AppData folder since it is hidden, open Windows Explorer and click Organize ► Folder and Search Options. Check Show Hidden Files, Folders, and Drives under the View tab. If you are on a Windows 8 or 10 machine, click the View tab on Windows Explorer and check Hidden Items.

If you right-click one of the link files and select properties, you can see the information about the link file (see Figure 6-3).

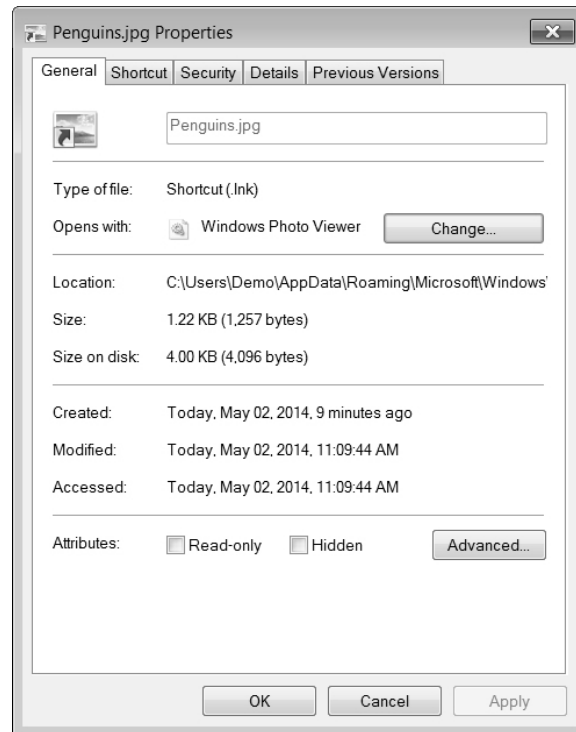


Figure 6-3 – Link File Properties

This link file is merely a pointer back to the actual file. It contains date and time stamps, the size of the file, and if you look at the Shortcut tab, you can even see where the file was located when it was opened.

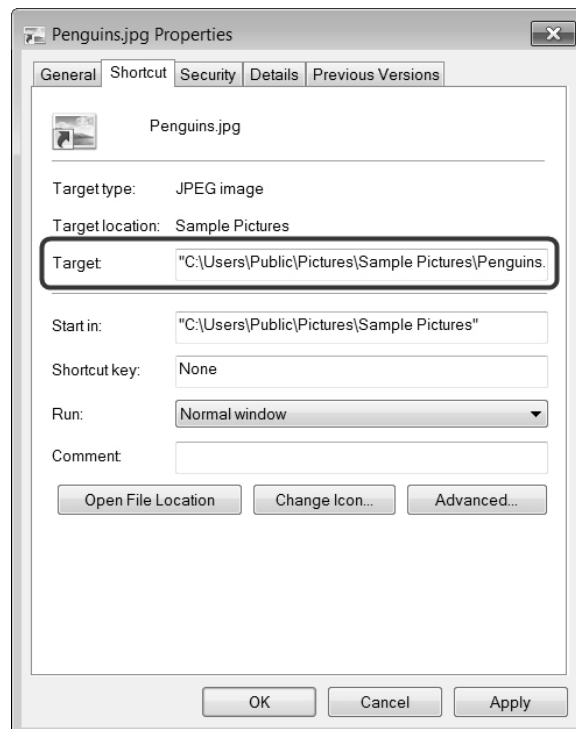


Figure 6-4 - Link File Pointing to Actual File's Location

Example 1 (File Opened Once)

Back in Autopsy, look at the link file called Pier.lnk and click on the Results view. Autopsy will show you the path of where Pier.jpg was stored when it was opened.

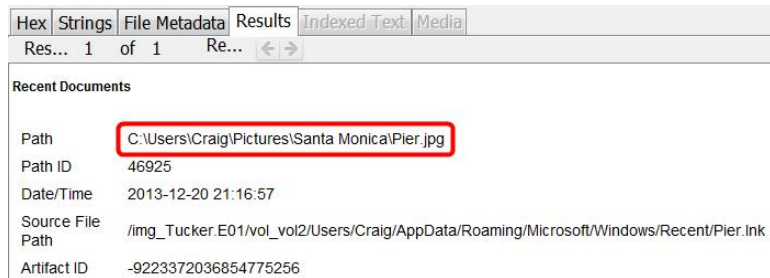


Figure 6-5 – Link File Shows Path of Pier.jpg

If you view Pier.lnk in Hex view, you can see that inside this link there is embedded data that points back to the original file that was opened.

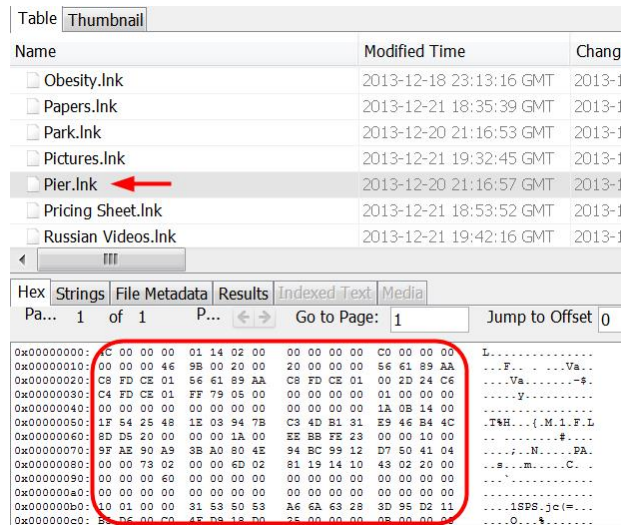


Figure 6-6 – Embedded Data in Pier.lnk

There are three date and time stamps EMBEDDED within the link file. The time stamps you see in the Hex view refer back to the file “Pier.jpg”.

Embedded Time Stamps	Description
Creation Time (Yellow)	This is the time that the file (Pier.jpg) was created in that local path. If the file had been copied to that location, then the Creation date/time is when it was copied.
Last Access Time (Green)	Last access times have been disabled since Windows Vista. It keeps the same date as the Creation time (UTC), but there are some variables that can change or update it.
Last Write Time (Blue)	This is the time that the file (Pier.jpg) was last modified. This is not necessarily the last time it was opened.

Hex	Strings	File Metadata	Results	Indexed Text	Media
Pa...	1	of 1	P...	Go to Page: 1	Jump to Offset 0
0x00000000:	4C 00 00 00	01 14 02 00	00 00 00 00	C0 00 00 00	L.....
0x00000010:	00 00 00 46	9B 00 20 00	20 00 00 00	56 61 89 AA	...F...Va..
0x00000020:	C8 FD CE 01	56 61 89 AA	C8 FD CE 01	00 2D 24 C6	...Va.....-
0x00000030:	C4 FD CE 01	FF 79 05 00	00 00 00 00	01 00 00 00	...y.....
0x00000040:	00 00 00 00	00 00 00 00	00 00 00 00	1A 0B 14 00	...T...{.M.I.F.L
0x00000050:	1F 84 25 48	1E 03 94 7B	C3 4D B1 31	E9 46 B4 4C	...T...{.M.I.F.L
0x00000060:	8D D5 20 00	00 00 1A 00	EE BB FE 23	00 00 10 00	...T...{.M.I.F.L
0x00000070:	9F AE 90 A9	3B A0 80 4E	94 BC 99 12	D7 50 41 04	...T...{.M.I.F.L
0x00000080:	00 00 79 02	00 00 6D 02	81 19 14 10	43 02 20 00	...T...{.M.I.F.L
0x00000090:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	...T...{.M.I.F.L
0x000000a0:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	...T...{.M.I.F.L
0x000000b0:	10 01 00 00	31 53 50 53	A6 6A 63 28	3D 95 D2 11	...T...{.M.I.F.L
0x000000c0:	B5 D6 00 C0	4F D9 18 D0	25 00 00 00	0B 00 00 00	...T...{.M.I.F.L

Figure 6-7 – Embedded Creation, Last Access, and Last Write Times of Pier.jpg

To decode these time stamps, you are going to use the tool called DCode (Version 4.02a). You can download this tool at:

<http://www.digital-detective.net/digital-forensic-software/free-tools/>

Once you have DCode up and running, you need to copy the time stamps out Pier.lnk in hex view and paste them into Notepad.

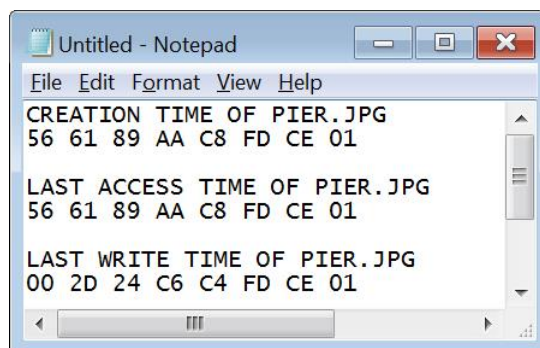


Figure 6-8 – Copy and Paste Embedded Time Stamps of Pier.lnk

In DCode, set the Decode Format to Windows: 64 bit Hex Value – Little Endian. Next, past the first time stamp (creation time of pier.jpg) into the Value to Decode. Hit the Decode button in the bottom right corner and you should see the decoded embedded creation time stamp (see Figure 6-9).

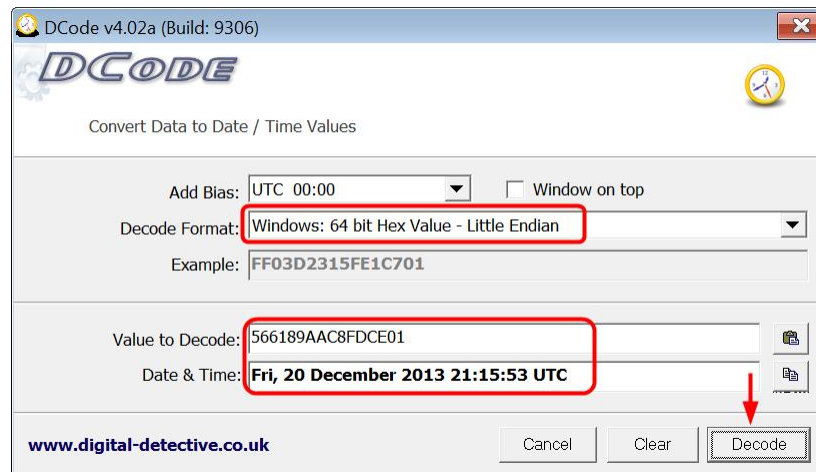


Figure 6-9 – Embedded Creation Time Stamp Decoded

Repeat this for the other two time stamps, and you should have the following date and time stamps:

Embedded Creation Time (UTC): Fri, 20 December 2013 21:15:53 UTC

Embedded Access Time (UTC): Fri, 20 December 2013 21:15:53 UTC

Embedded Last Write Time (UTC): Fri, 20 December 2013 20:48:02 UTC

Next, you need to look at the date and time stamps of the link file itself.

Table Thumbnail			
Name	Created Time	Modified Time	Access Time
Pictures.Ink	2013-12-21 19:32:38 GMT	2013-12-21 19:32:45 GMT	2013-12-21 19:32:45 GMT
Pier.Ink	2013-12-20 21:16:57 GMT	2013-12-20 21:16:57 GMT	2013-12-20 21:16:57 GMT
Pricing Sheet.Ink	2013-12-21 18:53:52 GMT	2013-12-21 18:53:52 GMT	2013-12-21 18:53:52 GMT
Russian Videos.Ink	2013-12-21 19:42:16 GMT	2013-12-21 19:42:16 GMT	2013-12-21 19:42:16 GMT
Santa Monica.Ink	2013-12-20 21:16:53 GMT	2013-12-20 21:16:57 GMT	2013-12-20 21:16:57 GMT
School.Ink	2013-12-20 21:16:19 GMT	2013-12-20 21:16:19 GMT	2013-12-20 21:16:19 GMT

Figure 6-10 - Date and Time Stamps of the Link File

The time stamps in the table pane are about the link file itself and are separate from the time stamps embedded within the link file.

Link File Time Stamps	Description
Created Time	When a file is first opened, it creates a link file. The link file's Created time stamp is when the file (Pier.jpg) was FIRST opened.
Modified Time	This is the time when the file (Pier.jpg) was LAST opened. If this is the same as the Created time stamp, then you know that the file was only opened once.
Access Time	Once again, the accessed time is disabled in Windows Vista, 7, and 8. Accessed will be the same date and time as Modified.

As you can see in Figure 6-10, the Created and Modified time of the link file are the same. This means that the file (Pier.jpg) was only opened once.

Here is a timeline of the file Pier.jpg (All UTC):

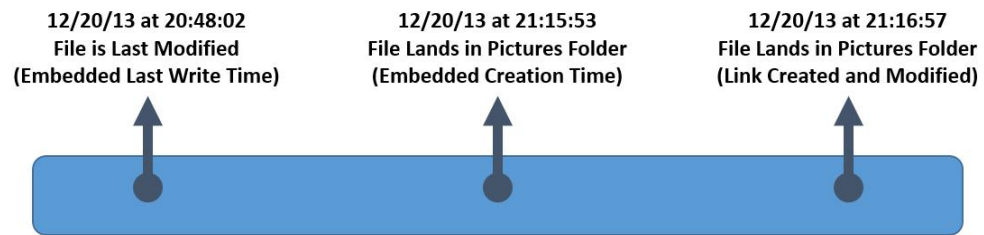


Figure 6-11 - Timeline of Pier.jpg Based on Link File

Since the last time this picture was modified is BEFORE the time it was created in that folder, it is likely that this file was copied to the Pictures folder.

Example 2 (Files Opened More than Once)

Take a look at the file called Cheetos.Ink and click on the Results view. Autopsy will show that this link file is pointing to a “Cheetos.jpg” in E:\Coupons. This is important to note, because this could mean that Craig had plugged in and used an external drive since it is found on something other than the C: drive.



Figure 6-12 - Link File Shows Path of Cheetos.jpg

Next, take a look at the embedded date and time stamps in the Cheetos.Ink file.

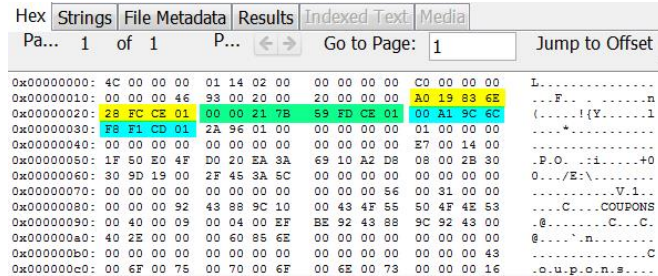


Figure 6-13 - Embedded Creation, Last Access, and Last Write Times of Cheetos.jpg

Use the DCode tool to decode the embedded time stamps. You should have the following time stamps:

Embedded Creation Time (UTC): Wed, 18 December 2013 19:36:22 UTC

Embedded Access Time (UTC): Fri, 20 December 2013 08:00:00 UTC

Embedded Last Write Time (UTC): Mon, 14 January 2013 01:42:34 UTC

Note: You can tell a device is FAT32 based on the Last Access Time embedded in the link file. FAT32 does not track the time of the last accessed activity, only the date. In, DCode is reporting a last accessed date of 12/20/2013 and the time is 8:00 AM (UTC). DCode is attempting to report UTC by adding 8 hours to a field that by default reports 12:00 AM.

Next, take a look at the time stamps of the link file itself.

Table Thumbnail			
Name	Created Time	Modified Time	Access Time
ALL COUPONS.Ink	2013-12-18 20:07:21 GMT	2013-12-18 20:07:21 GMT	2013-12-18 20:07:21 GMT
AWESOME COUPON	2013-12-20 21:43:07 GMT	2013-12-20 21:43:32 GMT	2013-12-20 21:43:32 GMT
Biology and Aggressi	2013-12-18 23:15:30 GMT	2013-12-18 23:17:33 GMT	2013-12-18 23:17:33 GMT
Cheetos.Ink	2013-12-18 19:42:32 GMT	2013-12-20 21:17:12 GMT	2013-12-20 21:17:12 GMT
Coca- Cola.Ink	2013-12-20 21:17:27 GMT	2013-12-20 21:17:27 GMT	2013-12-20 21:17:27 GMT
Coupons (2).Ink	2013-12-18 19:42:16 GMT	2013-12-21 01:09:58 GMT	2013-12-21 01:09:58 GMT

Figure 6-14 - Date and Time Stamps of the Link File

The link file's Modified date and time is different from the Created date and time. This means that Craig opened the file more than once.

Here is a timeline for the file "Cheetos.jpg" (All UTC):

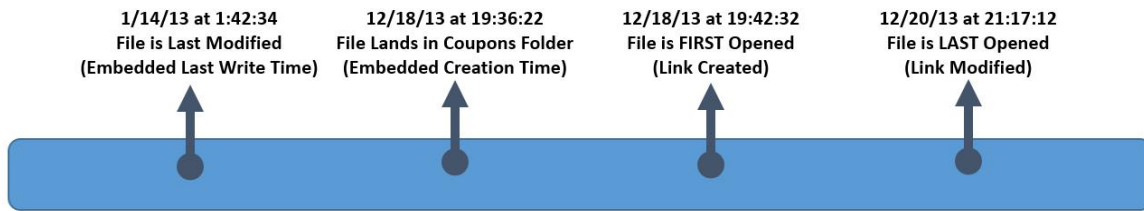


Figure 6-15 - Timeline of Cheetos.jpg Based on Link File

If a file has been opened more than two times, you will only know the FIRST time it was opened (Link Created) and the LAST time it was opened (Link Modified). Without other information, you will not know what the date and time stamps were when it was opened in between. The computer does not track the times in between,

Example 3 (No Embedded Date/Time)

Another example you will want to look at is the MileyCyrus_tongue.lnk. If you look at the link file in Hex view, you will see that there aren't any date and time stamps embedded in the link file.

Table Thumbnail			
Name	Created Time	Modified Time	Access Time
<input type="checkbox"/> http--mail.live.com-.lnk	2013-12-17 23:42:05 GMT	2013-12-17 23:42:05 GMT	2013-12-17 23:42:05
<input type="checkbox"/> iPad - Edited 2013.lnk	2013-12-21 01:01:41 GMT	2013-12-21 01:09:52 GMT	2013-12-21 01:09:52
<input type="checkbox"/> Leaf Transmutation.lnk	2013-12-18 19:42:59 GMT	2013-12-18 19:42:59 GMT	2013-12-18 19:42:59
<input checked="" type="checkbox"/> MileyCyrus_tongue.lnk	2013-12-27 07:41:31 GMT	2013-12-27 07:41:31 GMT	2013-12-27 07:41:31
<input type="checkbox"/> Monster Drink Coupon.lnk	2013-12-17 23:32:34 GMT	2013-12-17 23:32:34 GMT	2013-12-17 23:32:34
<input type="checkbox"/> Multiple Intelligences Theor	2013-12-18 19:45:00 GMT	2013-12-21 18:35:39 GMT	2013-12-21 18:35:39
<input type="checkbox"/> My Stuff.lnk	2013-12-17 23:35:04 GMT	2013-12-18 00:48:30 GMT	2013-12-18 00:48:30

Hex	Strings	File Metadata	Results	Indexed Text	Media
Pa...	1	of 1	P...	Go to Page: 1	Jump to Offset 0
0x00000000: 4C 00 00 00 01 14 02 00 00 00 00 00 00 00 00 00 00 00 00 00					
0x00000010: 00 00 00 46 9B 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00					
0x00000020: 00					
0x00000030: 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00					
0x00000040: 00 00 00 00 00 00 00 00 00 00 00 00 96 06 14 00 00 00 00 00					
0x00000050: 1F 54 25 48 1E 03 94 7B C3 4D B1 31 E9 46 B4 4C 00 00 00 00					
0x00000060: BD D5 20 00 00 00 1A 00 EE BB FE 23 00 00 10 00 00 00 00 00 00 00					
0x00000070: 9F AE 90 A9 3B A0 80 4E 94 BC 99 12 D7 50 41 04 00 00 00 00					
0x00000080: 00 00 73 02 00 00 6D 02 81 19 14 10 43 02 20 00 00 00 00 00					
0x00000090: 00 00 00 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00					
0x000000a0: 00					
0x000000b0: 10 01 00 00 31 53 50 53 A6 6A 63 28 3D 95 D2 11 00 00 00 00					
0x000000c0: B5 D6 00 C0 4F D9 18 D0 25 00 09 00 08 00 00 00 00 00 00 00 00					

Figure 6-16 - No Embedded Time Stamps in Link File for MileyCyrus_tongue.jpg

There are a few situations that can cause this to occur. If the user uses the function “Save as” on a picture when viewing a site using Internet Explorer, a link file will be created with no embedded date and time stamps. Once the user opens the file, embedded date and time stamps will be added in the link file. A link file is also created when a user does a “Save Image as” in Mozilla Firefox and Google Chrome. If the file isn't opened after it has been saved, there won't be any embedded date and time stamps as well.

With certain applications, if the user creates a file in an application and saves it, but never opens it, there won't be any embedded date and time stamps. Once they do open the file, embedded date and time stamps will be added to the link file.

If a user saves an email attachment but does not open it, there will be a link file with no embedded date and time stamps. This only applies to certain email client software programs, such as Windows Live Mail. Once the user actually opens the file, embedded date and time stamps will be added.

The Created time stamp of the link file shows when the picture was saved or created in an application. The Modified time stamp matches the Created time stamp because it was never opened.

If the file had been opened after it was saved, it would create date and time stamps embedded within the link file. The link file's Modified time stamp would show when the file was LAST opened.

So, if a link file has no embedded date and time stamps it means the user could have:

- 1) Used Save as on a picture in a website, but never opened the file
- 2) Created the file in an application, but never opened it
- 3) Saved an attachment through an email client software, but never opened the file

A link file with no embedded date and time stamps merely gives you an idea of where the file might have come from. Later, you will go through the user's email and Internet history. If you see the file as an email attachment or in their download history, you will know exactly where it came from.

Example 4 (File is Moved, Link File is Updated)

Now that you have an understanding of link files, let's take a look at how these can help in an investigation. Look at the link file called Underage_lolita_r@ygold_001.lnk and click on the Results view.

Hex	Strings	File Metadata	Results	Indexed Text	Media
Res...	1	of 1	Re...	← →	
Path	C:\Users\Craig\Pictures\Underage_lolita_r@ygold_001.jpg				
Path ID	-1				
Date/Time	2013-12-21 19:32:38				
Source					
File Path	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Roaming/Microsoft/Windows/Recent/Underage_lolita_r@ygold_001.lnk				
Artifact ID	-9223372036854775249				

Figure 6-17 – Path of Underage_lolita_r@ygold_001.jpg

This link file shows that when the picture was opened, it was located in:

C:\Users\Craig\Pictures

If you go to that location, you will see that the picture is no longer there. Go back to the link file and look at the date and time stamps embedded in the link file.

Hex	Strings	File Metadata	Results	Indexed Text	Media
Pa...	1	of 1	P...	← →	Go to Page: 1 Jump to Offset (
0x00000000:	4C 00 00 00	01 14 02 00	00 00 00 00	C0 00 00 00	L.....
0x00000010:	00 00 00 46	9B 00 20 00	20 00 00 00	72 01 DA 73	...F...E..S
0x00000020:	83 FE CE 01	72 01 DA 73	83 FE CE 01	60 9C EA 85	...E...S...
0x00000030:	10 FE CE 01	B5 93 08 00	00 00 00 00	01 00 00 00	...M...
0x00000040:	00 00 00 00	00 00 00 00	00 00 00 00	4E 07 14 00	.T&H...{.M.1.F.L
0x00000050:	1F 54 25 48	1E 03 94 7B	C3 4D B1 31	E9 46 B4 4C	...N...PA...
0x00000060:	8D D5 20 00	00 00 1A 00	EE BB FE 23	00 00 10 00	...S...m...C...
0x00000070:	9F AE 90 A9	3B A0 80 4E	94 BC 99 12	D7 50 41 04	...N...PA...
0x00000080:	00 00 73 02	00 00 6D 02	81 19 14 10	43 02 20 00	...S...m...C...
0x00000090:	00 00 00 60	00 00 00 00	00 00 00 00	00 00 00 00	...S...m...C...
0x000000A0:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	...S...m...C...
0x000000B0:	10 01 00 00	31 53 50 53	A6 6A 63 28	3D 95 D2 11	...ISPS.jc(=...
0x000000C0:	B5 D6 00 C0	4F D9 18 D0	25 00 00 00	0B 00 00 00	...O...\$.....

Figure 6-18 - Embedded Creation, Last Access, and Last Write Times of Underage_lolita_r@ygold_001.jpg

Use the DCode tool to decode the embedded time stamps. You should have the following time stamps:

Embedded Creation Time (UTC): Sat, 21 December 2013 19:32:57 UTC

Embedded Access Time (UTC): Sat, 21 December 2013 19:32:57 UTC

Embedded Last Write Time (UTC): Sat, 21 December 2013 05:50:16 UTC

Next, take a look at the date and time stamps of the link file itself.






Table	Thumbnail			
Name		Created Time	Modified Time	Access Time
 SonyPSP.lnk		2013-12-21 01:02:46 GMT	2013-12-21 01:14:07 GMT	2013-12-21 01:14:07 GMT
 The Evolutionary Steps of Fish.lnk		2013-12-18 19:45:47 GMT	2013-12-18 19:45:47 GMT	2013-12-18 19:45:47 GMT
 underage daughter R@ygold.lnk		2013-12-21 19:42:16 GMT	2013-12-21 19:43:21 GMT	2013-12-21 19:43:21 GMT
 Underage_lolita_r@ygold_001.lnk		2013-12-21 19:32:38 GMT	2013-12-21 19:33:05 GMT	2013-12-21 19:33:05 GMT
 Underage_lolita_r@ygold_002.lnk		2013-12-21 19:32:45 GMT	2013-12-21 19:33:10 GMT	2013-12-21 19:33:10 GMT

Figure 6-19 - Date and Time Stamps of the Link File

The link file's Modified date and time is different from the Created date and time. This means that Craig opened the file more than once.

Here is a timeline for the file “Underage_lolita_r@ygold_001.jpg” (All UTC):

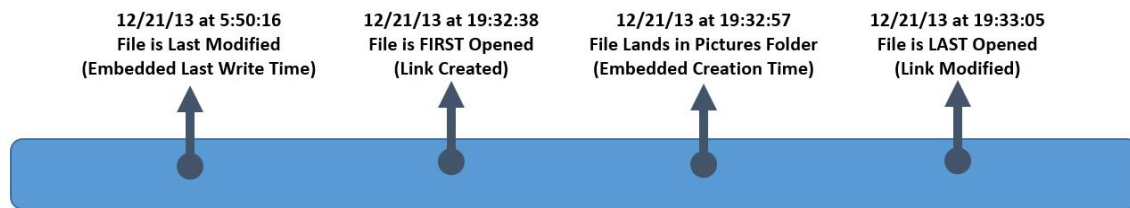


Figure 6-20 - Timeline of Underage_lolita_r@ygold_001.jpg Based on Link File

The embedded Last Write Time tells us that the file was last modified BEFORE the creation time. This indicates that the embedded Creation Time was when the picture was copied, not when it was actually created.

The link file was FIRST opened several seconds before the embedded Creation Time, which means it could have been opened on external media or in another folder before it was copied over.

When a file is opened in one location, it creates a link file. This is important to note that if a suspect then copies that same file to a different location and opens it there, a new link file is not created. The original link file is merely updated.

In this case, a link file was first created for the underage picture when it was opened in another location. When it was copied and opened in the Pictures folder, that same link file’s embedded data was updated. The local path displays where it was last opened, and its embedded Creation Time is updated to when the file was copied to the Pictures folder.

You were able to determine the picture was opened somewhere else because the FIRST time it was opened was before the embedded Creation Time. In the next section, you will learn how jump lists can sometimes show other locations a file was opened in.

Note: This type of file naming is an indicator of child pornography. Searching for child pornography on this suspect’s computer would be out of the scope of your original search warrant, which was just to search for coupons. In a normal investigation, you should obtain another search warrant to further investigate and see if the suspect had child pornography.

Jump Lists

Jump Lists were a new feature added to Windows 7. They are similar to the Windows shortcuts (link files) because they are designed to take a user directly to a specific file or directory used frequently or recently.

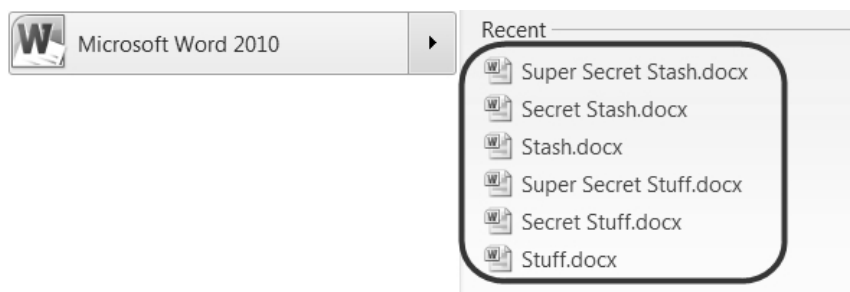


Figure 6-21 - Jump List for Microsoft Word

Jump lists are important to look at because they may contain information of file activity that is no longer present in the link files. However, you may also find file activity in link files but not in a jump list. It is important to note that these are two separate artifacts and will not always match up.

There are two sets of jump lists, which are called Destination files:

automaticDestinations, which are created and maintained by the operating system.

customDestinations, which are maintained by the specific application.

A jump list is basically a catalog of one or more link files associated with a specific application. This catalog stores the data in compound file binary (CFB) format. The jump lists are located in the following subdirectories for all versions of Windows:

`C:\[username]\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations`

`C:\[username]\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations`

There are various tools that you can use to review the contents of these files:

JumpLister from WoanWare: <https://github.com/woanware/JumpLister>

Windows Jump List Parser from TZWorks: <http://www.tzworks.net>

For this case, use JumpLister from WoanWare. To use this tool you need to first export the jump lists. Navigate to the folder in the Tucker image that contains them.

Each jump list file name starts with a hex value prefix. This prefix is the Application ID. A resource for looking up AppID's is located at:

http://forensicswiki.org/wiki/List_of_Jump_List_IDs

Go ahead and highlight all the jump list files in the AutomaticDestinations folder, right-click one, and select Extract File(s) (see Figure 6-22).

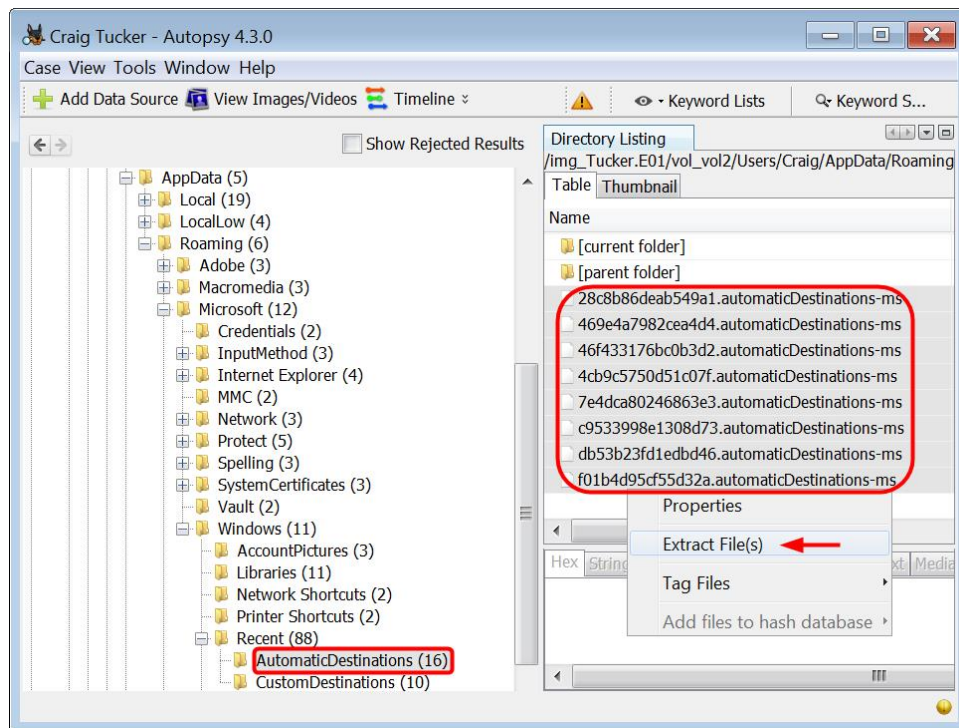


Figure 6-22 – Highlight Jump Lists in AutomaticDestinations, Right-Click and Select Extract File(s)

Extract these files to your case Export folder. Open up the JumpLister tool where you downloaded it, and then select File►Load.

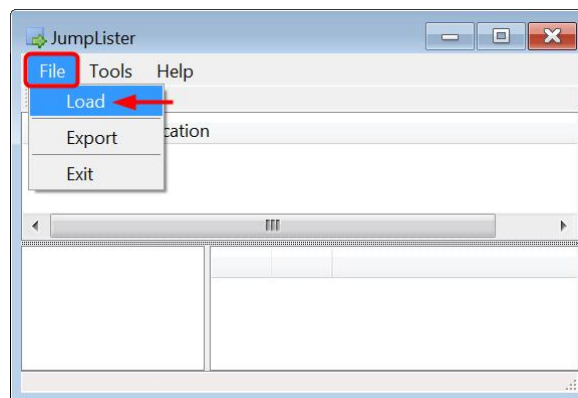


Figure 6-23 – Click Load in JumpLister

Navigate to your export folder that contains the jump list files. Highlight and select each jump list file and click Open.

If you click the jump list 46507-c9533998e1308d73.automaticDestinations-ms in JumpLister, you can see what pictures have been opened (see Figure 6-24).

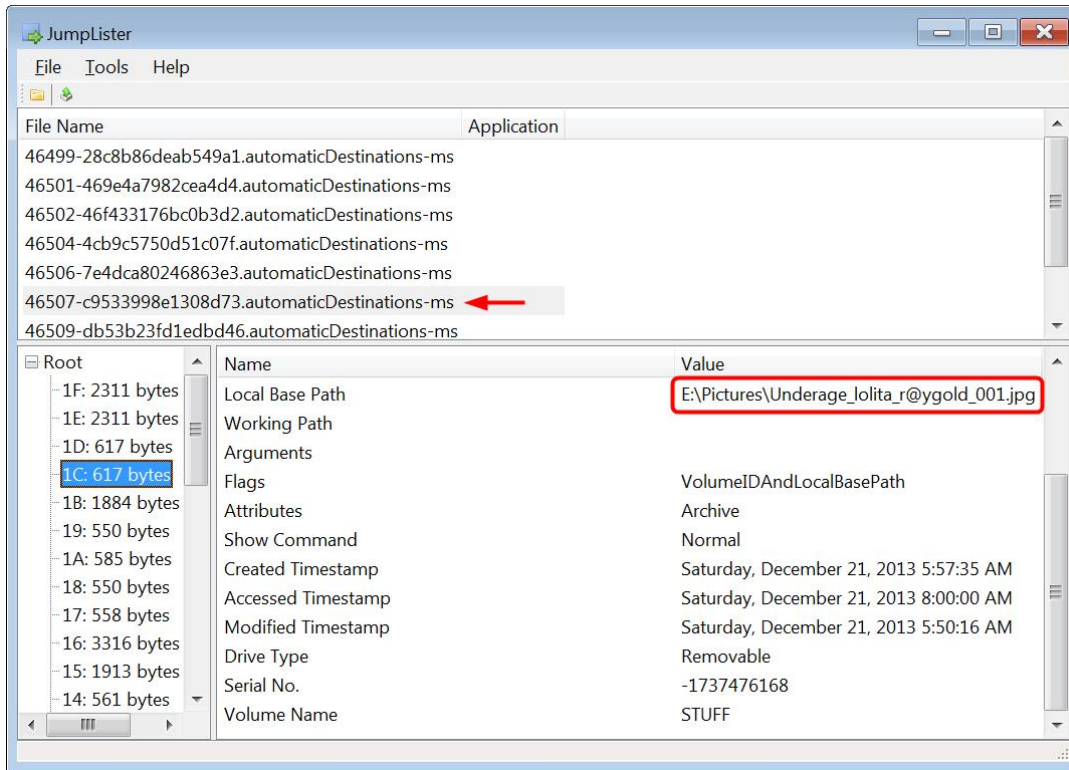


Figure 6-24 - Individual Entries in Photos App Jump List

Note: This version of Jumplister does not display what application goes with the jump list c9533998e1308d73. This application is the Windows 8 “Photos” app and it is the default photo viewer in Windows 8. This application is also present in Windows 10.

In the bottom left pane, there are entries for individual files that have been opened. These entries are equivalent to a link file because they show where the file was located and it has the embedded date and time stamps.

The bottom left pane also has an entry called DestList (Destination List). This list is a summary of each entry (see Figure 6-25). There are three key fields that you want to focus your attention:

- Number:** This number will be associated with the entry number in the bottom left pane
- Date/Time:** This is the last time the file was accessed with the program
- Data:** This is the file location and filename

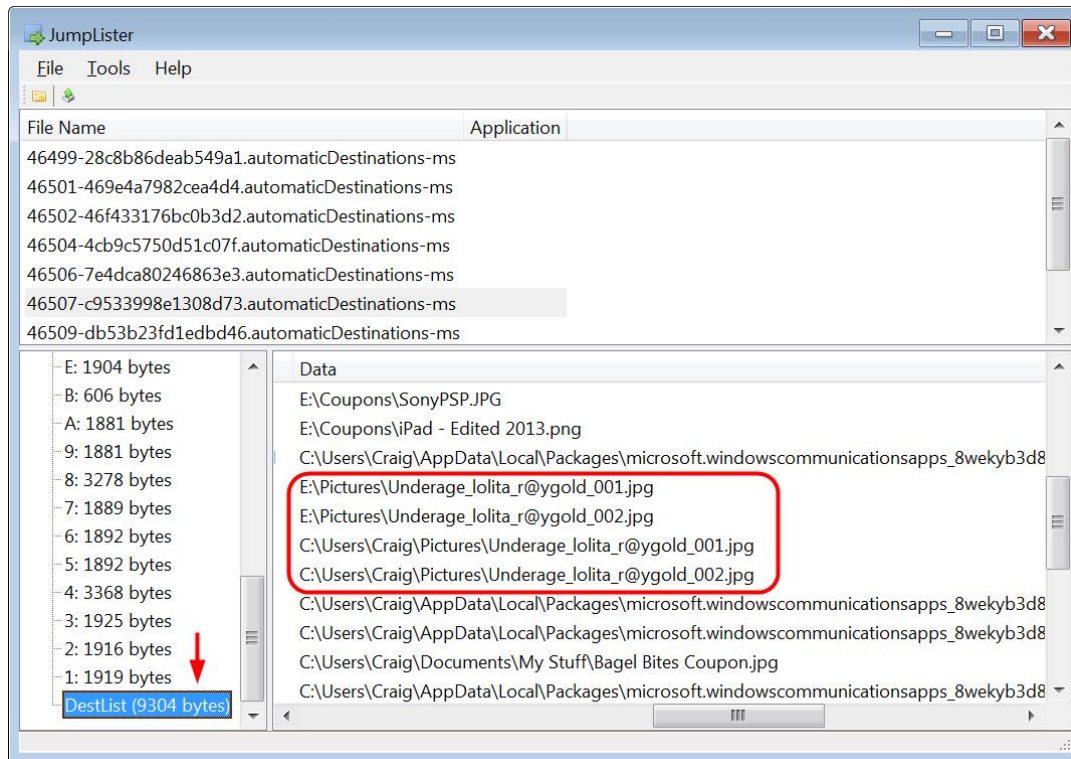


Figure 6-25 - DestList in Jumplist

As you can see in Figure 6-25, the jump list shows the underage pictures that were opened on the E: drive. You did not have this information in the link files because the link files were updated.

You can see in the column Date/Time that the pictures Underage_lolita_r@ygold_001.jpg and Underage_lolita_r@ygold_002.jpg were opened on the E:\ drive and in the Pictures folder on the following dates:

Underage_lolita_r@ygold_001.jpg (E: Drive):	12/21/13 7:32:38 PM (UTC)
Underage_lolita_r@ygold_002.jpg (E: Drive):	12/21/13 7:32:45 PM (UTC)
Underage_lolita_r@ygold_001.jpg (Pictures Folder):	12/21/13 7:33:05 PM (UTC)
Underage_lolita_r@ygold_002.jpg (Pictures Folder):	12/21/13 7:33:10 PM (UTC)

Note: There are two other timestamps called Timestamp (New) and Timestamp (Birth). These are related to Object IDs, which is a more advanced topic. For now, just use the Date/Time stamp to determine when the file was first opened.

You can export out this jump list information to a CSV file by clicking File►Export

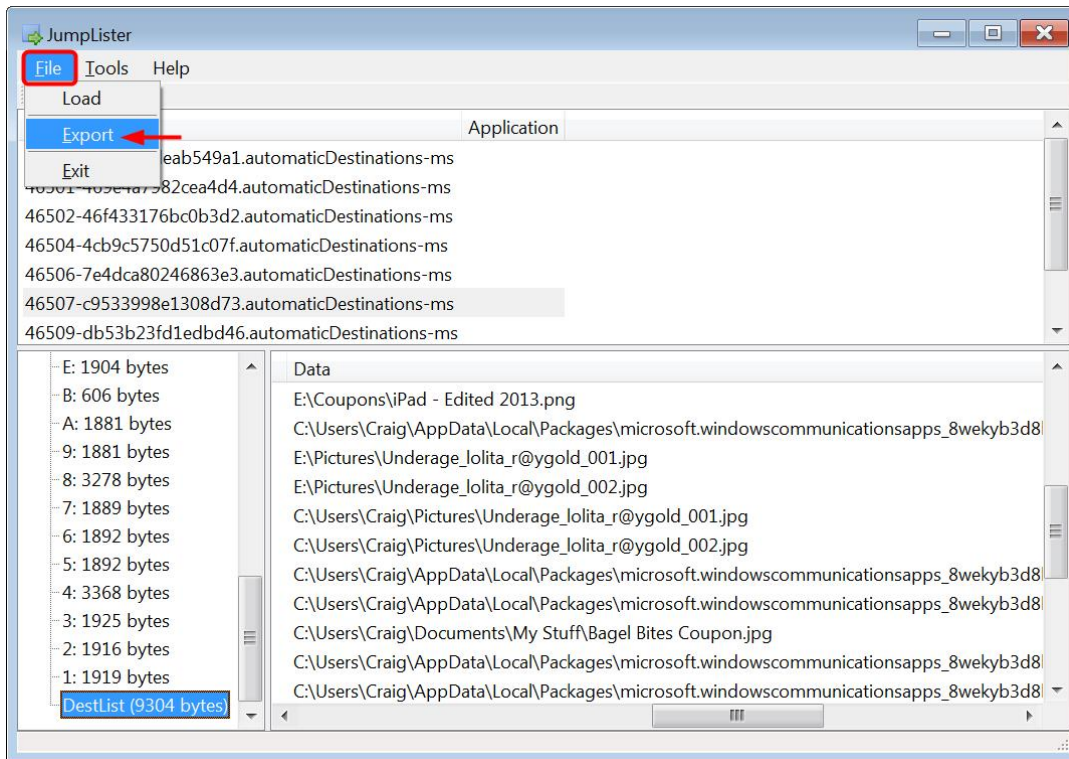


Figure 6-26 - Export Jump List Information to CSV File

Export the files to your case's Export Folder. Now, open up Excel and go to the Data tab. Click "From Text" under "Get External Data".

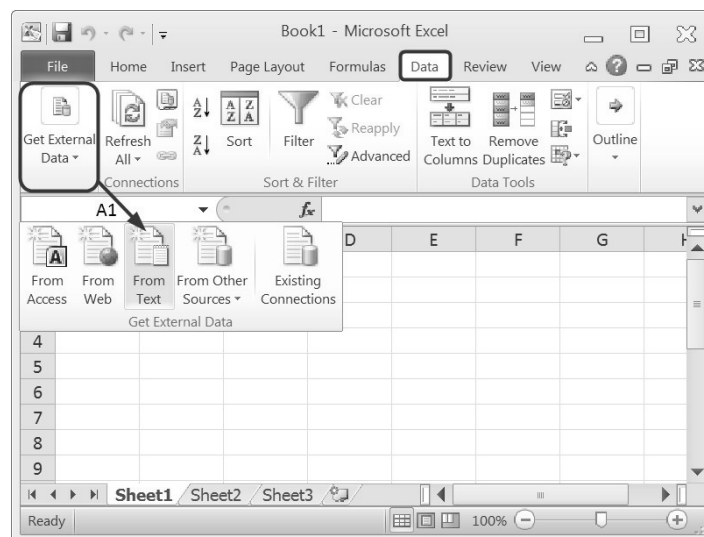


Figure 6-27 - Get External Data from Text to Open CSV File

Navigate to your Tucker Export\Jumplist folder and open the file DestList.csv. A window will open and prompt you to choose your text import options. Pick Delimited and click Next (see Figure 6-28).

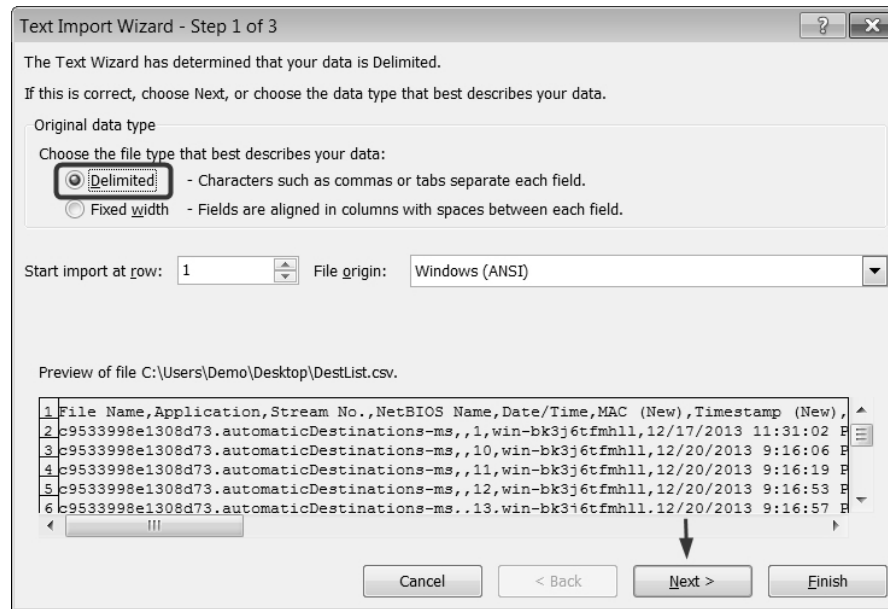


Figure 6-28 - Import DestList.csv as Delimited

Check the Comma delimiter and hit Finish.

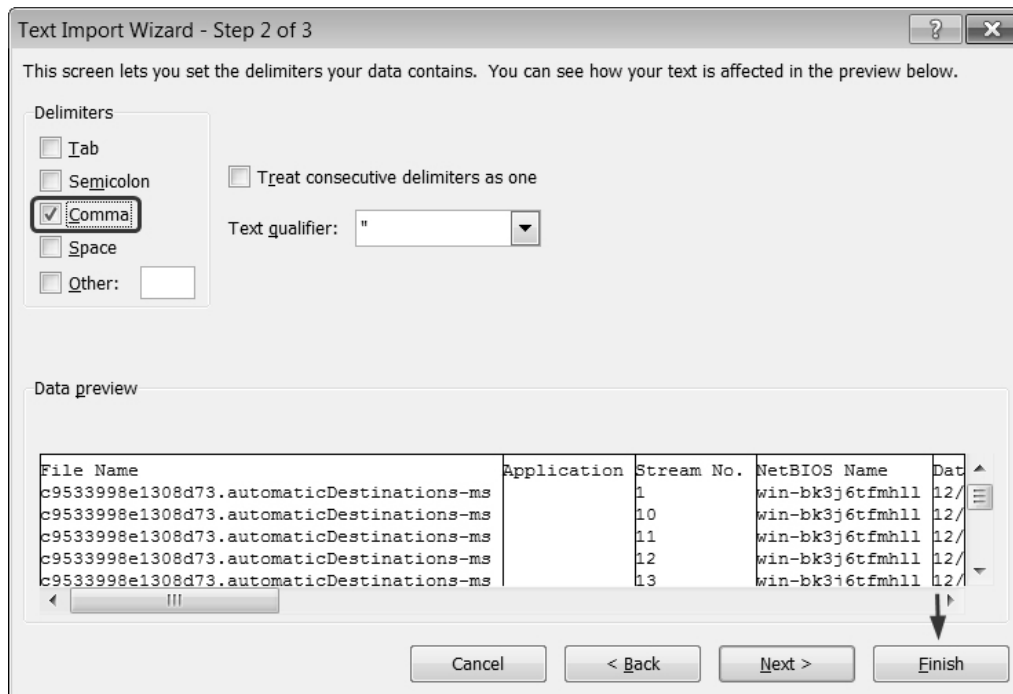


Figure 6-29 - Set Comma as Delimiter

This will give you a clean report of the jump list information (see Figure 6-30).

File Name	Date/Time	Data
c9533998e1308d73.automaticDestinations-ms	12/17/2013 23:31	C:\Users\Craig\AppData\Local\Packages\microsoft.windowscom
c9533998e1308d73.automaticDestinations-ms	12/20/2013 21:16	C:\Users\Craig\Pictures\desk_setup.jpg
c9533998e1308d73.automaticDestinations-ms	12/20/2013 21:16	C:\Users\Craig\Pictures\School\SMC_Library.jpg
c9533998e1308d73.automaticDestinations-ms	12/20/2013 21:16	C:\Users\Craig\Pictures\Santa Monica\Park.jpg
c9533998e1308d73.automaticDestinations-ms	12/20/2013 21:16	C:\Users\Craig\Pictures\Santa Monica\Pier.jpg
c9533998e1308d73.automaticDestinations-ms	12/20/2013 21:17	E:\Coupons\Coca- Cola.jpg
c9533998e1308d73.automaticDestinations-ms	12/20/2013 21:26	C:\Users\Craig\AppData\Local\Packages\microsoft.windowscom
c9533998e1308d73.automaticDestinations-ms	12/20/2013 21:28	C:\Users\Craig\Documents\Guides\HowtoMakeCoupons.jpg
c9533998e1308d73.automaticDestinations-ms	12/21/2013 0:55	E:\Coupons\GiftCards.jpg

Figure 6-30 - CSV of Jump List Information

If you click on one of the cells in the top row and then click the Filter button under the Data tab, you can easily filter for specific text or sort the columns.

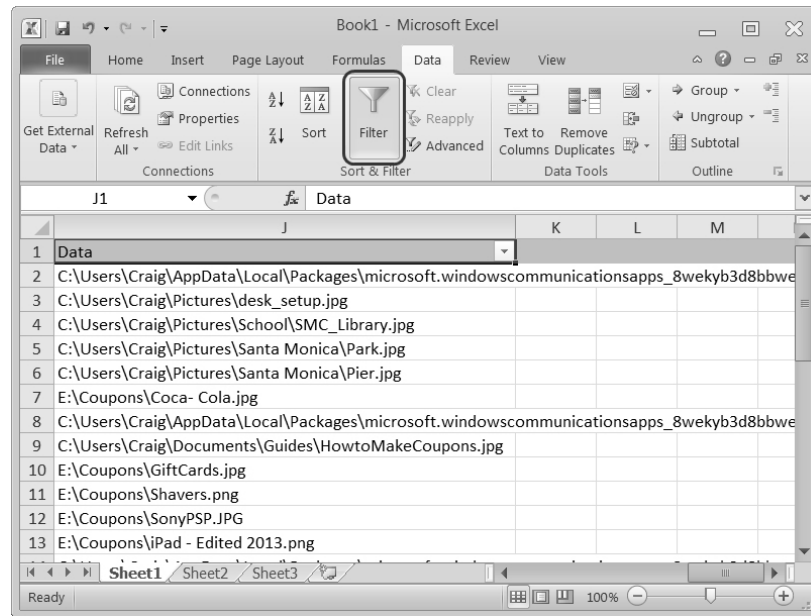


Figure 6-31 - Filter Function in Excel under Data Tab

By clicking the arrow at the end of each column header, you can select filters such as Text Filters► Begins With. These are helpful if you want to only view files on external media or just on the C: drive.

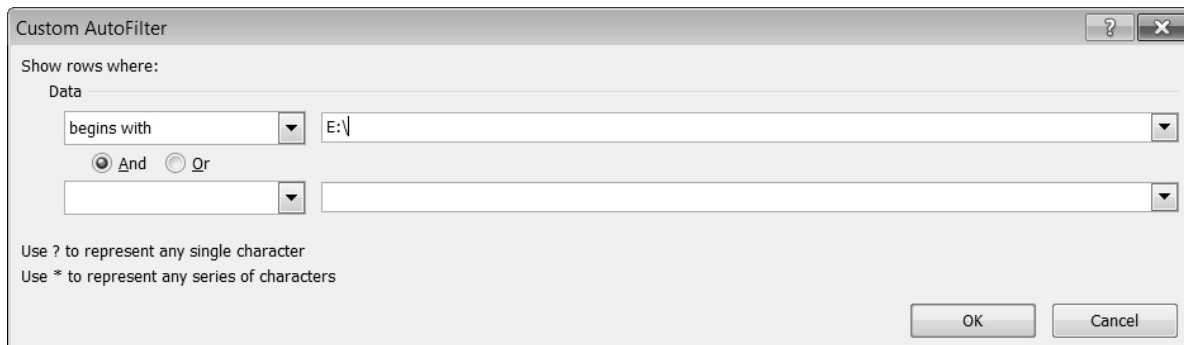


Figure 6-32 - Text Filter Begins with E:\