

This is a ?work? in progress and is not complete. I have only made it available because a few people requested to see it.

What the Deuce LNKs!

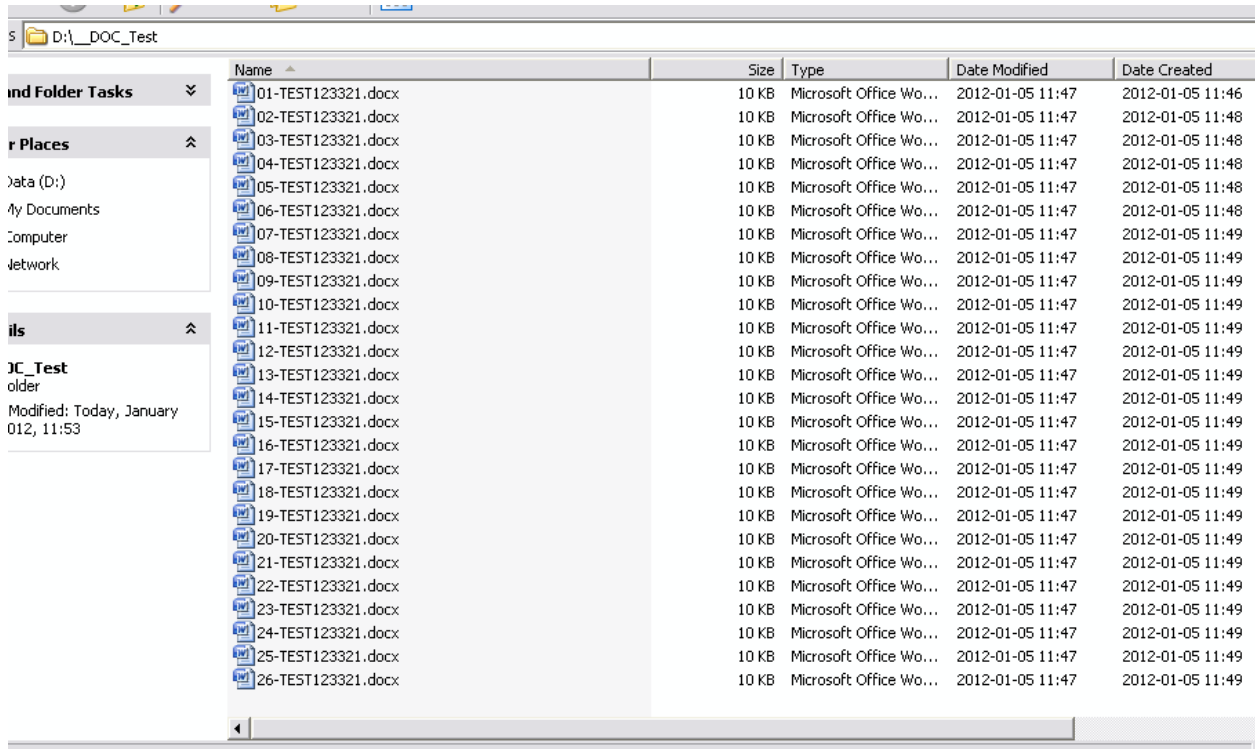
This write-up is not done in an official white-paper capacity, it was done as I am talking to myself, and answering myself. This was tested on 2003 server, Office 2007, and Acrobat 8. I highly recommend you test LNK data with the exact OS and softwares to which you have questions about.

This is not a write-up about the internals of LNK files there are already excellent write-ups about that in papers such as “TheMeaningofLIFE”.

I was looking at my recent files folder on a 2003 server laptop on and was wondering what caused “straggler” LNK files. I noted going back as far as the history of the Recent folder went there were a few PDF and DOC (MS Word .doc and .docx) LNKs here and there 33 and 41 (not including the yesterday or current day) for the past 6 months. Certainly I have reviewed more PDFs and DOCs than that in the past 6 months, so where are the rest of the LNKs? Why do some remain while some are replaced or deleted?

The biggest thing is always test the same version of Software on the same OS as your examination is or will be, to ensure you get the proper results. What I have learned here is LNK files are specific to how a files was accessed with a particular program. It makes a difference in LNK and MRU if you double click on a file like a PDF file as opposed to File | Open in Acrobat Reader.

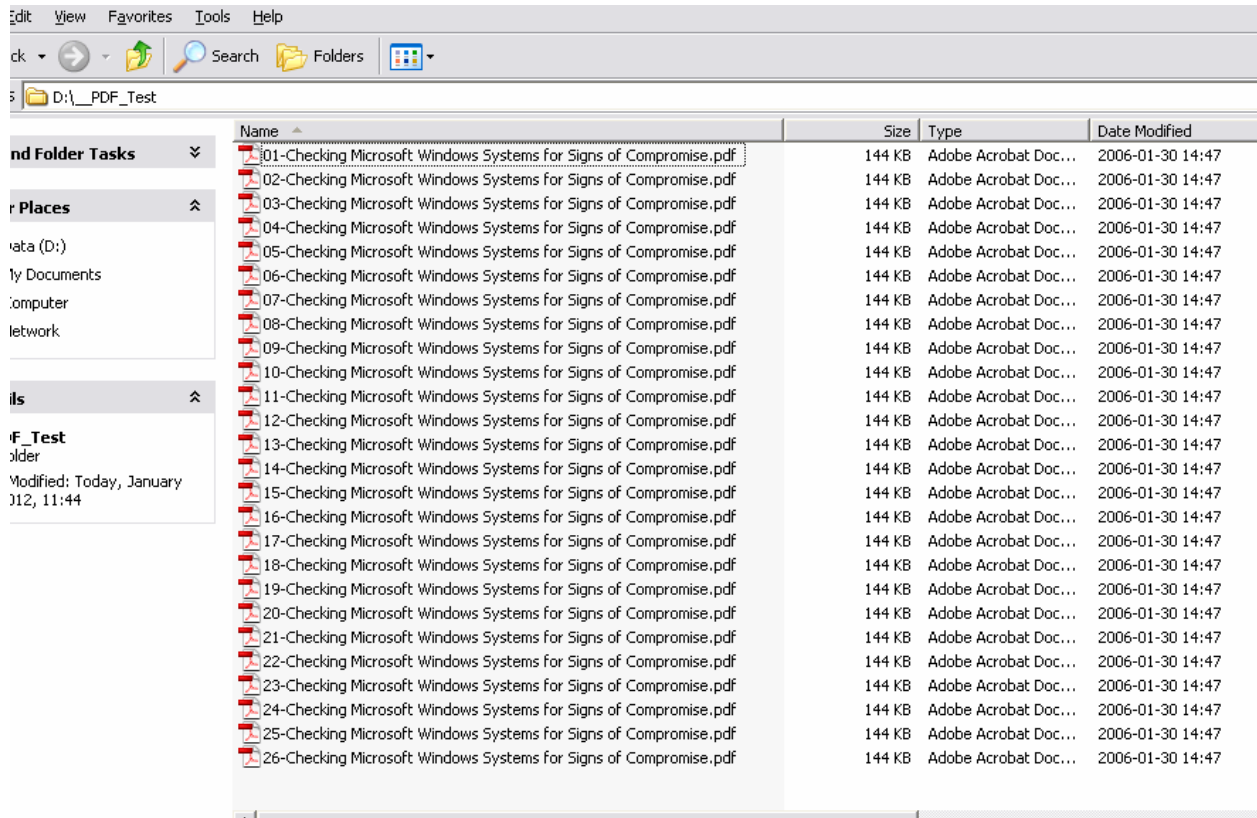
To test the theories here I created to test folders “_DOC_Test” and “_PDF_Test “ in each of the folders I placed 26 DOCs and PDFs respectively numbered 01-26 for each file extension.



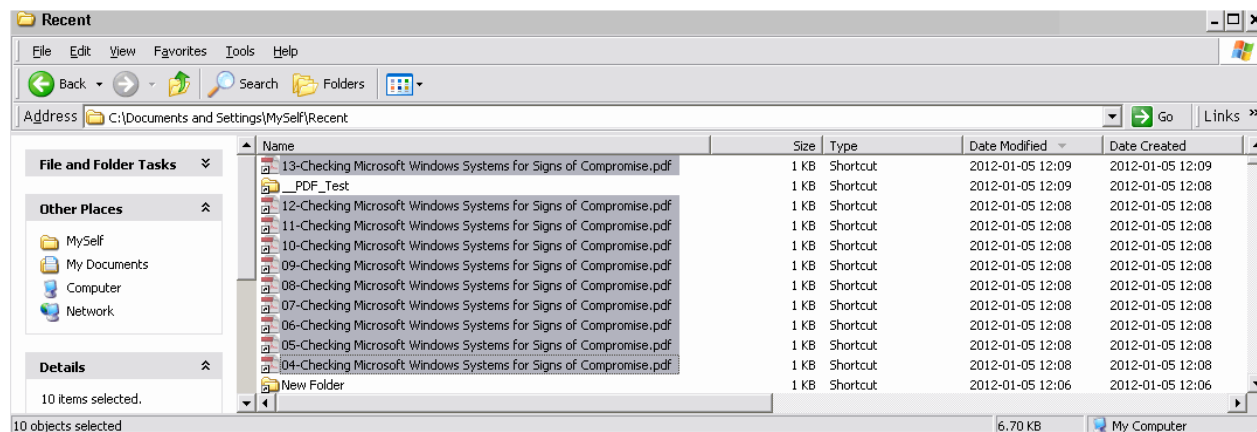
Name	Size	Type	Date Modified	Date Created
01-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:46
02-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:48
03-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:48
04-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:48
05-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:48
06-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:48
07-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:49
08-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:49
09-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:49
10-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:49
11-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:49
12-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:49
13-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:49
14-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:49
15-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:49
16-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:49
17-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:49
18-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:49
19-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:49
20-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:49
21-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:49
22-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:49
23-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:49
24-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:49
25-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:49
26-TEST123321.docx	10 KB	Microsoft Office Wo...	2012-01-05 11:47	2012-01-05 11:49

This is a ?work? in progress and is not complete. I have only made it available because a few people requested to see it.

What the Deuce LNKs!



First test: Open 1-13 of the PDFs by double clicking each one. We check the Recent folder while the 13 PDFs are open, and we see only 10 (04-13) LNK files. We close the 13 PDFs and the Recent folder shows the same 10 LNK files.

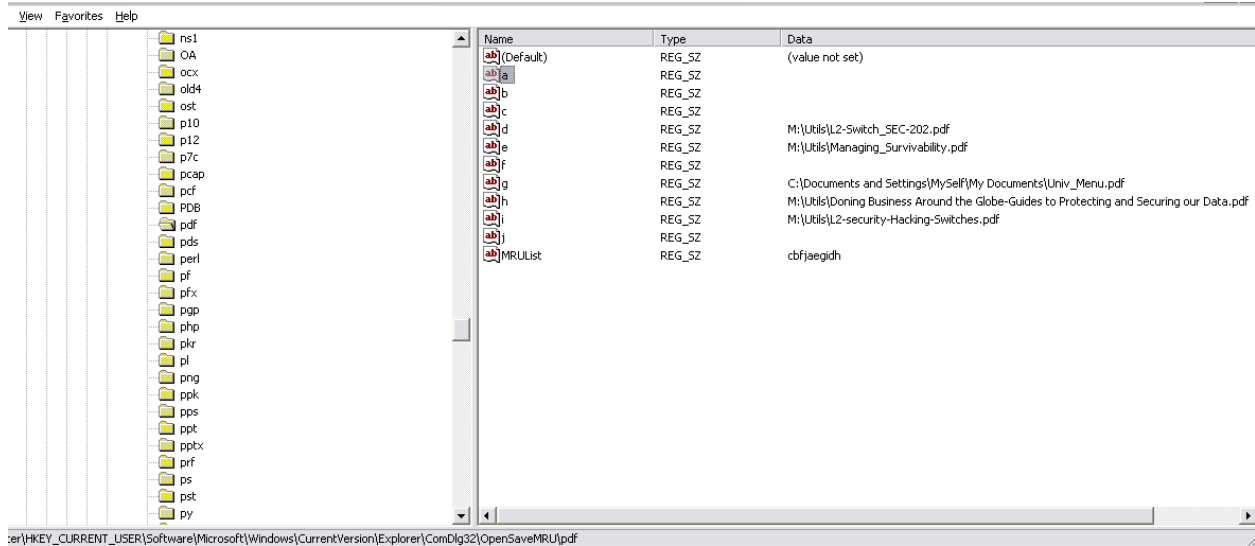


This is a ?work? in progress and is not complete. I have only made it available because a few people requested to see it.

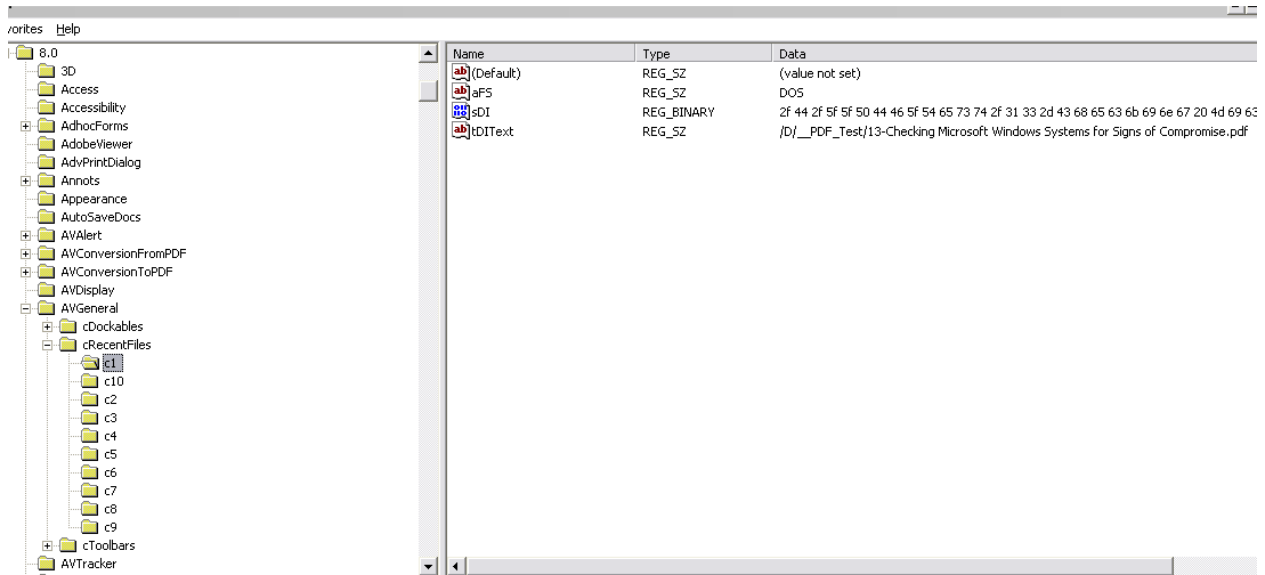
What the Deuce LNKs!

So we check the MRU for the PDF extension at HKCU

\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\pdf and we find 10 references to stuff I opened the day before. Now why is that? (NOTE: I removed several entries here manually as they were client specific documents)



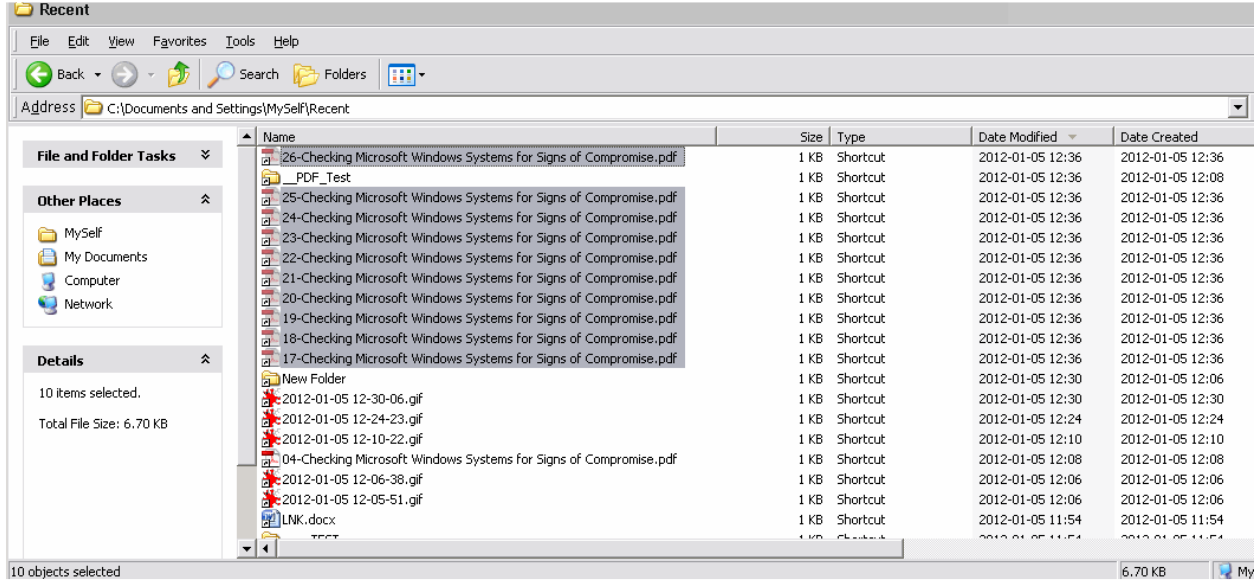
However, if we check HKCU \Software\Adobe\Adobe Acrobat\8.0\AVGeneral\cRecentFiles\ c-1-10 we find reference to the last 10 PDFs we opened by double clicking. And under the File menu in Adobe we see the same 10 references,



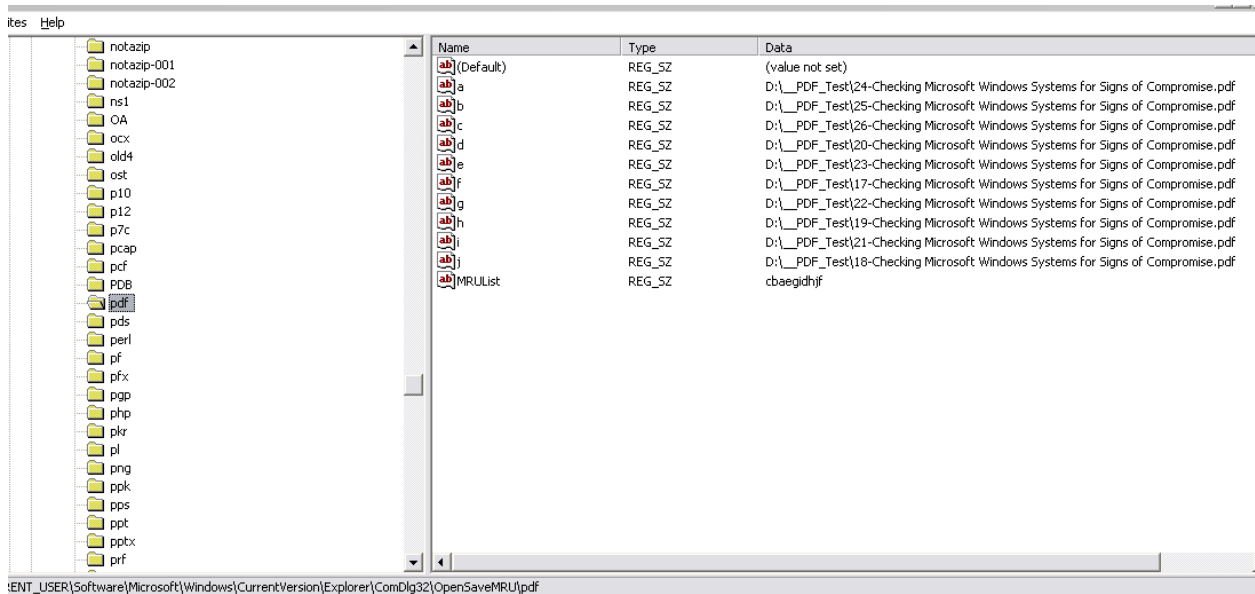
This is a ?work? in progress and is not complete. I have only made it available because a few people requested to see it.

What the Deuce LNKs!

So how do we update the OpenSaveMRU? I know let us use the File | Open menu inside Adobe and open files 14-26. We check the Recent folder while the files are open and we see only 10 (17-26). But wait what is that just a few lines down number 04, that we opened early by double clicking on the PDF files, but where are the other from before?



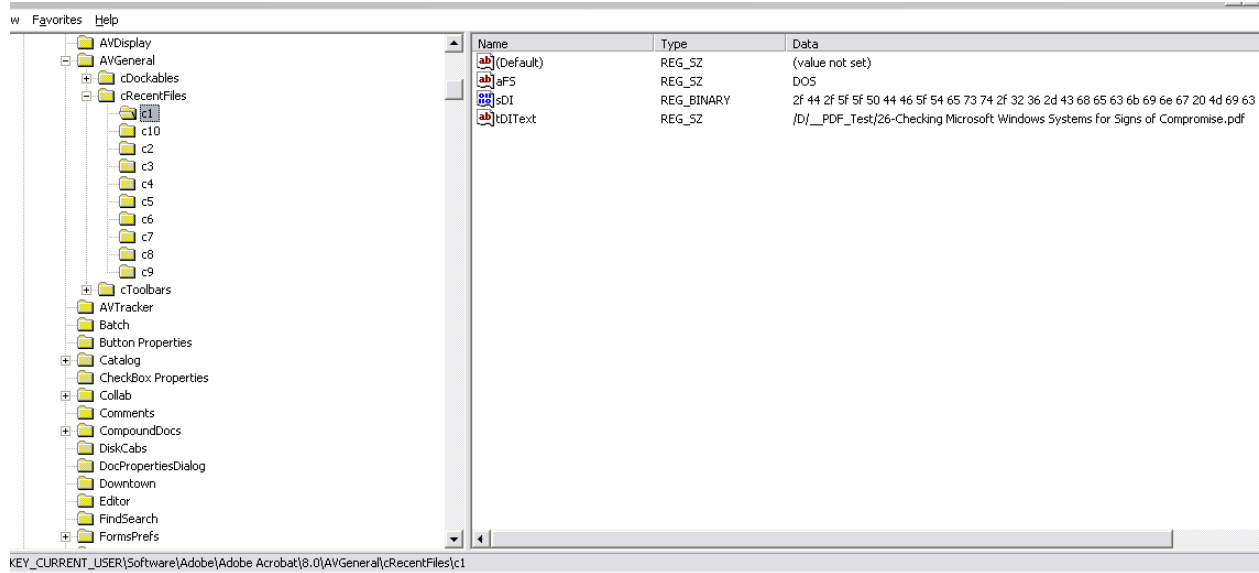
We once again check the MRU for the PDF extension and viola we see the 10 references to the files we just opened.



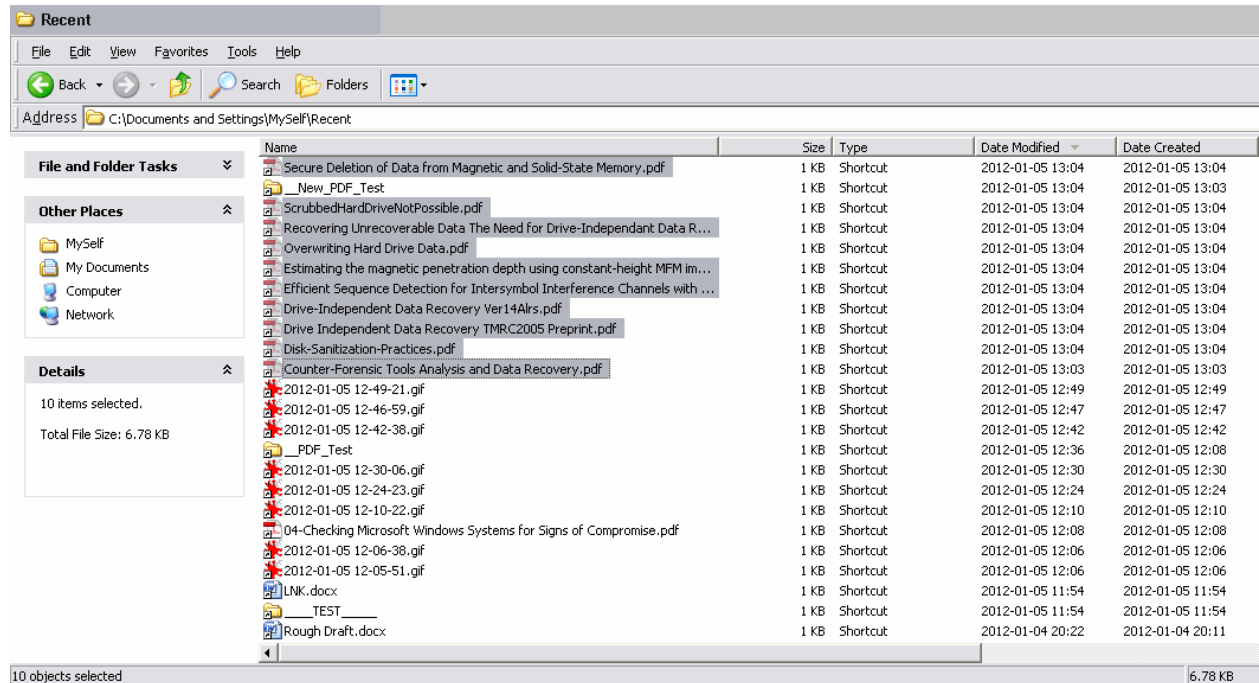
This is a ?work? in progress and is not complete. I have only made it available because a few people requested to see it.

What the Deuce LNKs!

How about the Adobe Recent files? Same 10 references as the PDF MRU. So what about the number 04 LNK file? Is it a “straggler”? Why does it stay and none of the other previous PDF LNK files? It makes 11 LNK files not 10. There is no reference to it in the MRU for PDFs or Adobe Recent files in the Registry.



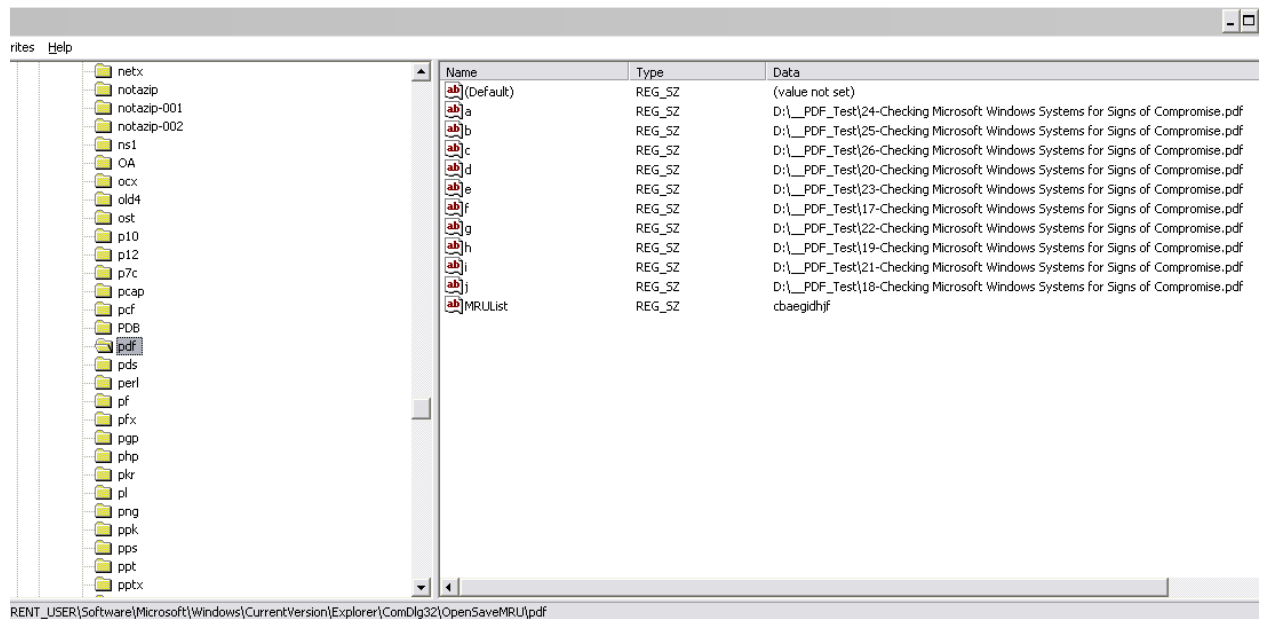
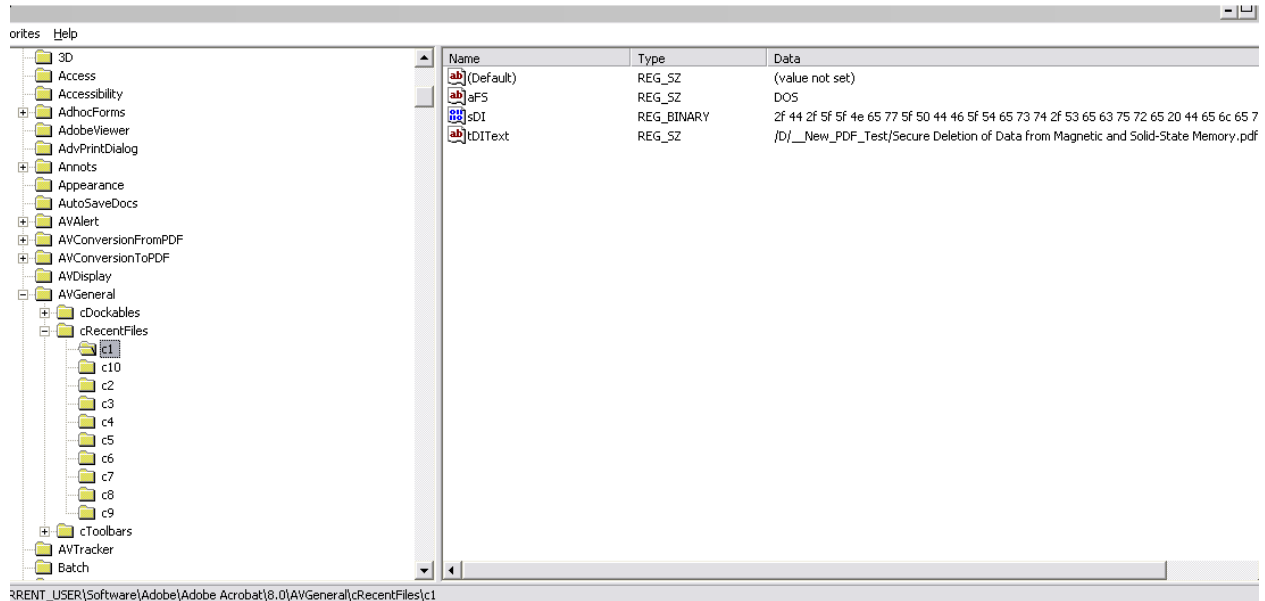
I created a new folder and put 10 different PDFs in it, let us see if we can figure out what keeps the straggler. We open these 10 PDFs, well now 04 is still there.



This is a ?work? in progress and is not complete. I have only made it available because a few people requested to see it.

What the Deuce LNKs!

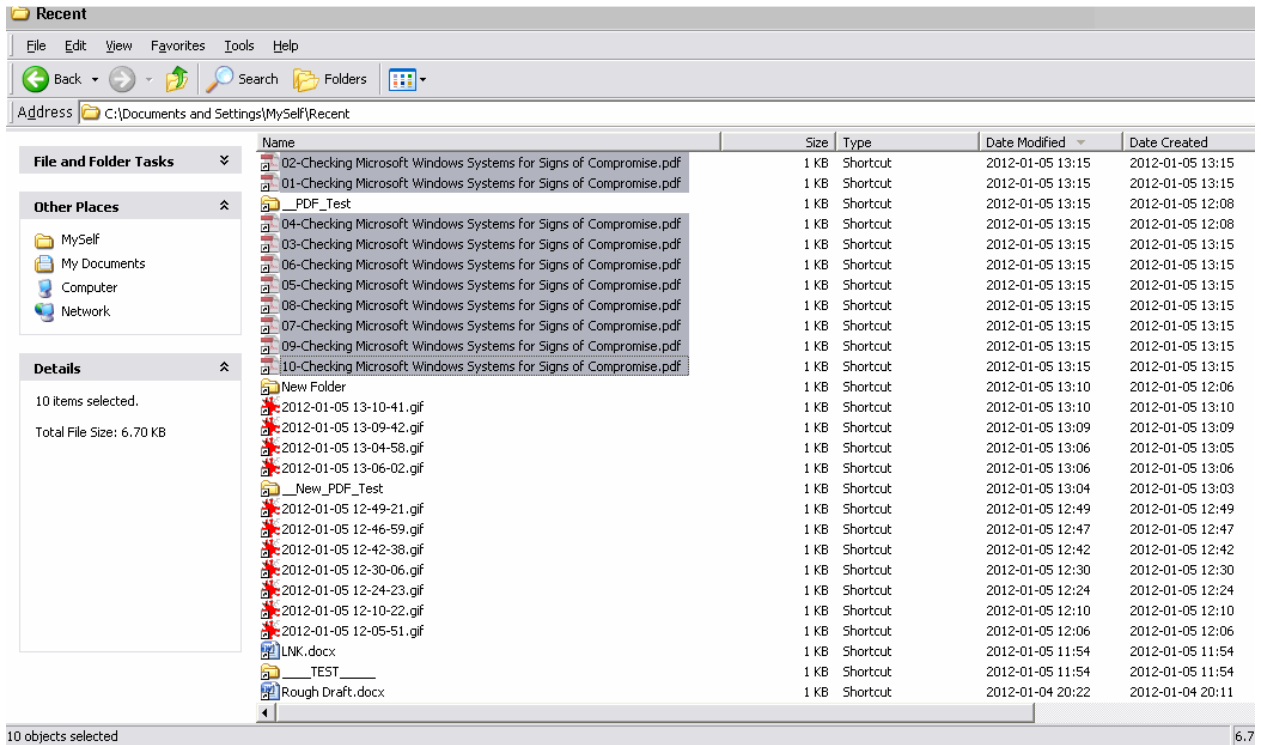
Let us check the Registry. The Adobe Recent files show the 10 files from the New_PDF_Test folder. MRU for PDF extension still shows the number 17-26 file, because I double clicked each PDF, and we have already discovered that only updates when we access File | Open menu inside Acrobat.



Can we consistently create straggler LNK files? I think we will try opening the 26 files again. This time in reverse order 13-01 and 26-14. Ok know we see 01-10 in the Recent folder and 04 is gone, because we have reused the 04 LNK. You will see it is the only one with an earlier creation time. The Adobe recent registry entries update and the PDF MRU stays the same because of the method we opened the files.

This is a ?work? in progress and is not complete. I have only made it available because a few people requested to see it.

What the Deuce LNKs!



We open 26-14 using the File | Open method and we see the 10 number 14-23 references. And we have picked up a new straggler number 09. Both registry entries update accordingly.

This is a ?work? in progress and is not complete. I have only made it available because a few people requested to see it.

What the Deuce LNKs!

The screenshot shows a Windows Explorer window titled 'Recent' with the address bar set to 'C:\Documents and Settings\MySelf\Recent'. The main pane displays a list of files with columns for Name, Size, Type, Date Modified, and Date Created. The list includes 23 PDF files named 'Checking Microsoft Windows Systems for Signs of Compromise.pdf' (numbered 14-23), a 'New Folder', and several GIF files with names like '2012-01-05 13-17-07.gif' through '2012-01-05 12-05-51.gif'. There are also two LNK files: 'LNK.docx' and 'TEST'. The status bar at the bottom indicates '10 objects selected' and a total file size of '6.70 KB'.

Name	Size	Type	Date Modified	Date Created
14-Checking Microsoft Windows Systems for Signs of Compromise.pdf	1 KB	Shortcut	2012-01-05 13:27	2012-01-05 13:27
__PDF_Test	1 KB	Shortcut	2012-01-05 13:27	2012-01-05 12:08
15-Checking Microsoft Windows Systems for Signs of Compromise.pdf	1 KB	Shortcut	2012-01-05 13:27	2012-01-05 13:27
16-Checking Microsoft Windows Systems for Signs of Compromise.pdf	1 KB	Shortcut	2012-01-05 13:27	2012-01-05 13:27
17-Checking Microsoft Windows Systems for Signs of Compromise.pdf	1 KB	Shortcut	2012-01-05 13:27	2012-01-05 13:27
18-Checking Microsoft Windows Systems for Signs of Compromise.pdf	1 KB	Shortcut	2012-01-05 13:27	2012-01-05 13:27
19-Checking Microsoft Windows Systems for Signs of Compromise.pdf	1 KB	Shortcut	2012-01-05 13:27	2012-01-05 13:27
20-Checking Microsoft Windows Systems for Signs of Compromise.pdf	1 KB	Shortcut	2012-01-05 13:27	2012-01-05 13:27
21-Checking Microsoft Windows Systems for Signs of Compromise.pdf	1 KB	Shortcut	2012-01-05 13:27	2012-01-05 13:27
22-Checking Microsoft Windows Systems for Signs of Compromise.pdf	1 KB	Shortcut	2012-01-05 13:27	2012-01-05 13:27
23-Checking Microsoft Windows Systems for Signs of Compromise.pdf	1 KB	Shortcut	2012-01-05 13:27	2012-01-05 13:27
New Folder	1 KB	Shortcut	2012-01-05 13:17	2012-01-05 12:06
2012-01-05 13-17-07.gif	1 KB	Shortcut	2012-01-05 13:17	2012-01-05 13:17
09-Checking Microsoft Windows Systems for Signs of Compromise.pdf	1 KB	Shortcut	2012-01-05 13:15	2012-01-05 13:15
2012-01-05 13-10-41.gif	1 KB	Shortcut	2012-01-05 13:10	2012-01-05 13:10
2012-01-05 13-09-42.gif	1 KB	Shortcut	2012-01-05 13:09	2012-01-05 13:09
2012-01-05 13-04-58.gif	1 KB	Shortcut	2012-01-05 13:06	2012-01-05 13:06
2012-01-05 13-06-02.gif	1 KB	Shortcut	2012-01-05 13:06	2012-01-05 13:06
__New_PDF_Test	1 KB	Shortcut	2012-01-05 13:04	2012-01-05 13:03
2012-01-05 12-49-21.gif	1 KB	Shortcut	2012-01-05 12:49	2012-01-05 12:49
2012-01-05 12-46-59.gif	1 KB	Shortcut	2012-01-05 12:47	2012-01-05 12:47
2012-01-05 12-42-38.gif	1 KB	Shortcut	2012-01-05 12:42	2012-01-05 12:42
2012-01-05 12-30-06.gif	1 KB	Shortcut	2012-01-05 12:30	2012-01-05 12:30
2012-01-05 12-24-23.gif	1 KB	Shortcut	2012-01-05 12:24	2012-01-05 12:24
2012-01-05 12-05-51.gif	1 KB	Shortcut	2012-01-05 12:06	2012-01-05 12:06
LNK.docx	1 KB	Shortcut	2012-01-05 11:54	2012-01-05 11:54
TEST	1 KB	Shortcut	2012-01-05 11:54	2012-01-05 11:54

Ok wait a second. Does this mean as long as I do not open number 09 it will remain a "straggler"? I went ahead and looked at yesterdays LNKs and we can see 12 PDF LNKs . Does this mean they will remain in the Recent folder until it is cleared or if that LNK is used again? I guess only time will tell, and I will have to report back in mo nth on those LNKs. But why those 12? I assure you yesterday when I was pondering this I opened no less than 50-100 PDFs. And, as I stated before not including today and yesterday I have 33 PDF LNKs in my recent for the entire past 6 months. Knowing that there are days I do research I spend some days doing nothing but reading PDF after PDF, 33 might not even cover one of those research days.

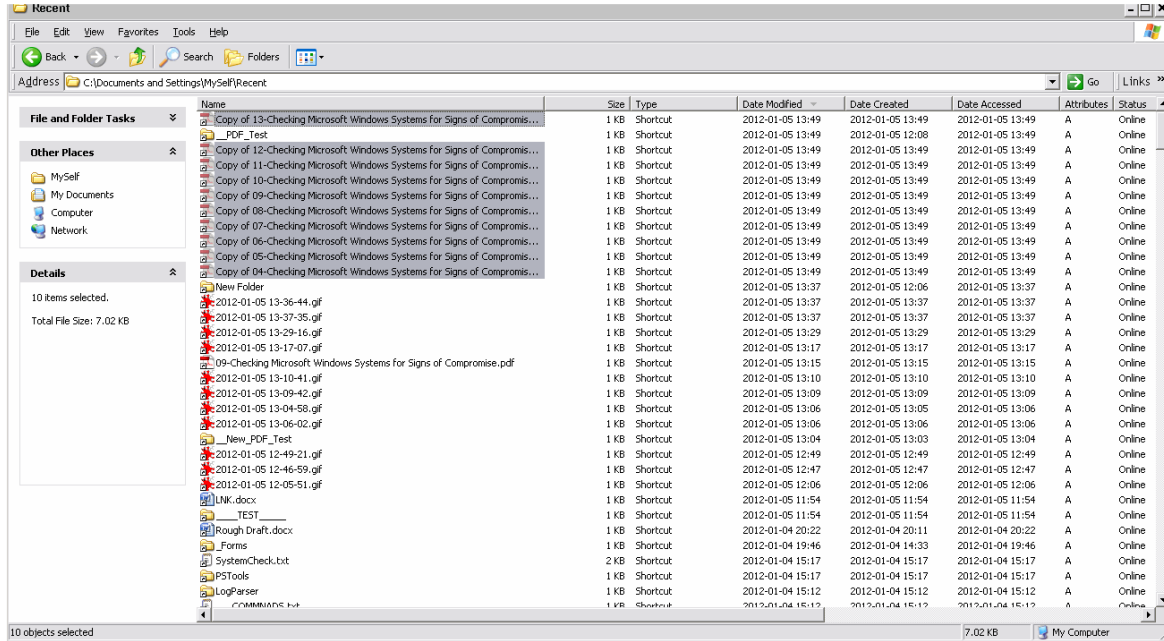
The screenshot shows a Windows Explorer window titled 'Recent' with the address bar set to 'C:\Documents and Settings\MySelf\Recent'. The main pane displays a list of files with columns for Name, Size, Type, Date Modified, and Date Created. The list includes files like 'Utils', 'L2-Switch_SEC-202.pdf', 'Attack_5250_terminal_emulations_from_I_Series_server.pdf', 'Privacy Pays- Making Privacy part of the Coroprate Culture.pdf', 'networksecurityguide.pdf', 'carnivore_draft_1.pdf', 'EvidentData Remote Desktop with Secure Tunnel V1.pdf', 'cert.at-the_wow_effect.pdf', '64-Bit', 'New Microsoft Office Word Document.docx', '001.jpg', 'wedthurs.txt', 'Evidence_of_Folder_Renaming.pdf', 'PCGuide - Ref - Clusters (Allocation Units).pdf', 'PCGuide - Ref -File Deletion and Undeletion.pdf', and '2012-01-04 12-40-38.gif'. The status bar at the bottom indicates '12 objects selected' and a total file size of '6.74 KB'.

Name	Size	Type	Date Modified	Date Created
Utils	1 KB	Shortcut	2012-01-04 14:04	2012-01-04 09:39
L2-Switch_SEC-202.pdf	1 KB	Shortcut	2012-01-04 14:00	2012-01-04 14:00
Attack_5250_terminal_emulations_from_I_Series_server.pdf	1 KB	Shortcut	2012-01-04 13:57	2012-01-04 13:57
Privacy Pays- Making Privacy part of the Coroprate Culture.pdf	1 KB	Shortcut	2012-01-04 13:57	2012-01-04 13:56
networksecurityguide.pdf	1 KB	Shortcut	2012-01-04 13:56	2012-01-04 13:56
carnivore_draft_1.pdf	1 KB	Shortcut	2012-01-04 13:55	2012-01-04 13:55
EvidentData Remote Desktop with Secure Tunnel V1.pdf	1 KB	Shortcut	2012-01-04 13:54	2012-01-04 13:54
cert.at-the_wow_effect.pdf	1 KB	Shortcut	2012-01-04 13:54	2012-01-04 13:54
64-Bit	1 KB	Shortcut	2012-01-04 13:54	2012-01-04 01:11
New Microsoft Office Word Document.docx	1 KB	Shortcut	2012-01-04 13:46	2012-01-04 13:46
001.jpg	1 KB	Shortcut	2012-01-04 13:46	2012-01-04 13:46
wedthurs.txt	1 KB	Shortcut	2012-01-04 13:43	2012-01-04 13:43
Evidence_of_Folder_Renaming.pdf	1 KB	Shortcut	2012-01-04 12:50	2012-01-04 12:50
PCGuide - Ref - Clusters (Allocation Units).pdf	1 KB	Shortcut	2012-01-04 12:50	2012-01-04 12:50
PCGuide - Ref -File Deletion and Undeletion.pdf	1 KB	Shortcut	2012-01-04 12:50	2012-01-04 12:50
2012-01-04 12-40-38.gif	1 KB	Shortcut	2012-01-04 12:40	2012-01-04 12:40

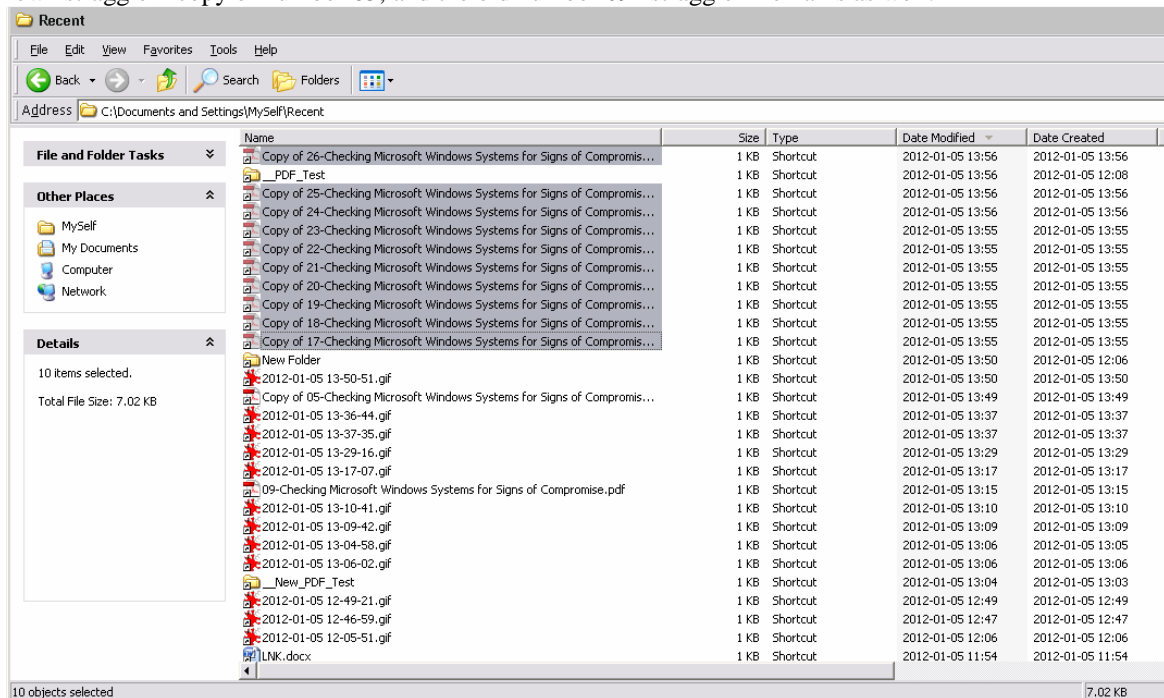
This is a ?work? in progress and is not complete. I have only made it available because a few people requested to see it.

What the Deuce LNKs!

How about if we try something like make a copy of those 26 PDFs and opening those in the same method. From here forth with respect to the PDF Registry entries unless something different happens I will forego those screenshots. We open Copy of 01-13 by double clicking each and the 10 number 04-13 LNK files appear in the Recent folder. The Adobe Recent files registry entry updates and the MRU PDF registry entry does not.



Now we open the Copy of 14-26 and Recent files show the 10 copy of number 17-26 LNK files. But now we have a new “straggler” copy of number 05, and the old number 09 “straggler” remains as well.

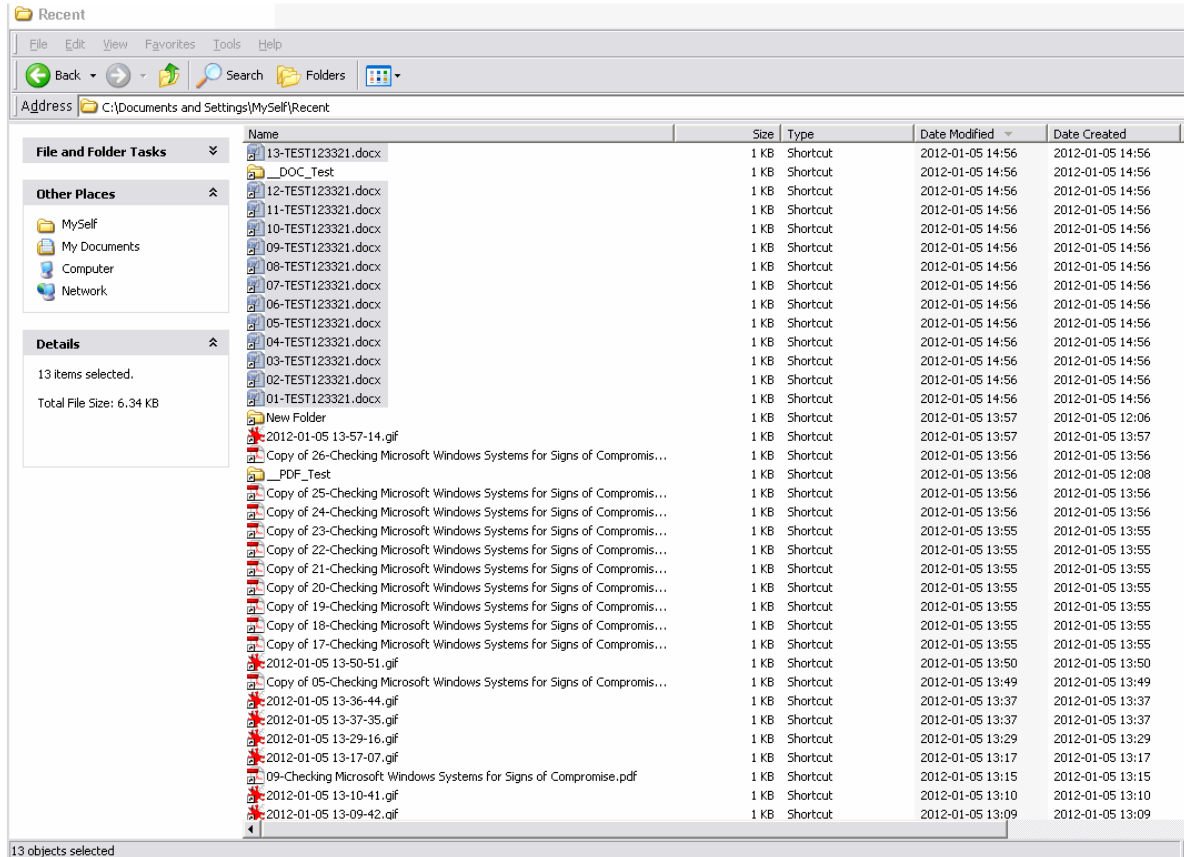


This is a ?work? in progress and is not complete. I have only made it available because a few people requested to see it.

What the Deuce LNKs!

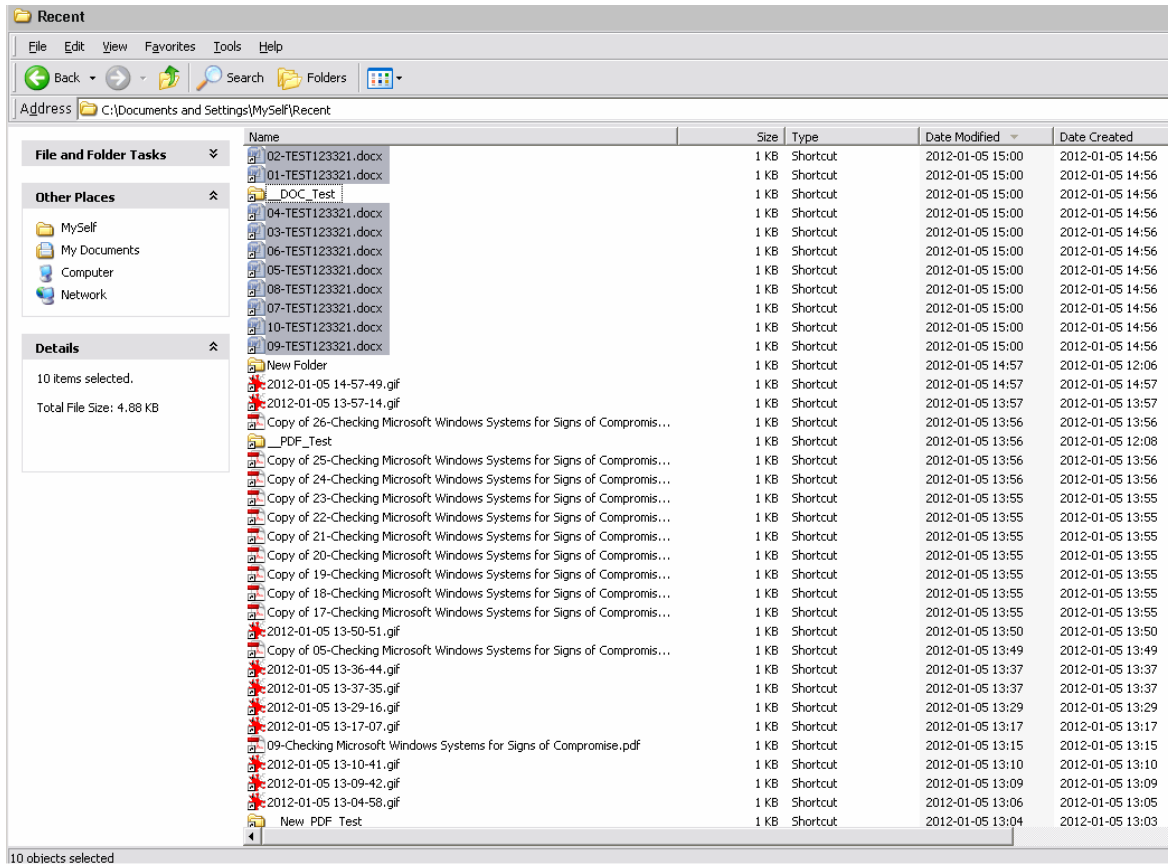
Well I guess we will wait until tomorrow to see what happens with the current PDF LNKs. On to DOCs.

We would we think the DOC LNKs would show the same behavior, for the most part they do. Here we see while we have DOCs number 01-13 open there are 13 LNK files in the Recent folder, unlike only showing 10 with the PDF LNKs.. However, when we close the DOCs we so only 10 number 01-10 LNKs remain. (NOTE: files were opened 01-13 sequentially and closed 13-01 sequentially.)

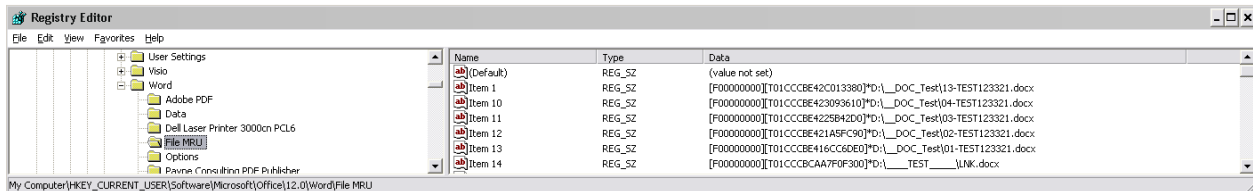


This is a ?work? in progress and is not complete. I have only made it available because a few people requested to see it.

What the Deuce LNKs!



In the Registry at HKCU \Software\Microsoft\Office\12.0\Word\File MRU we find the Word File MRU list has the last 50 entries, and are files 01-13 are listed as 1-13. (NOTE screen shot does not show all 50 items or all 13 of the test docs) .

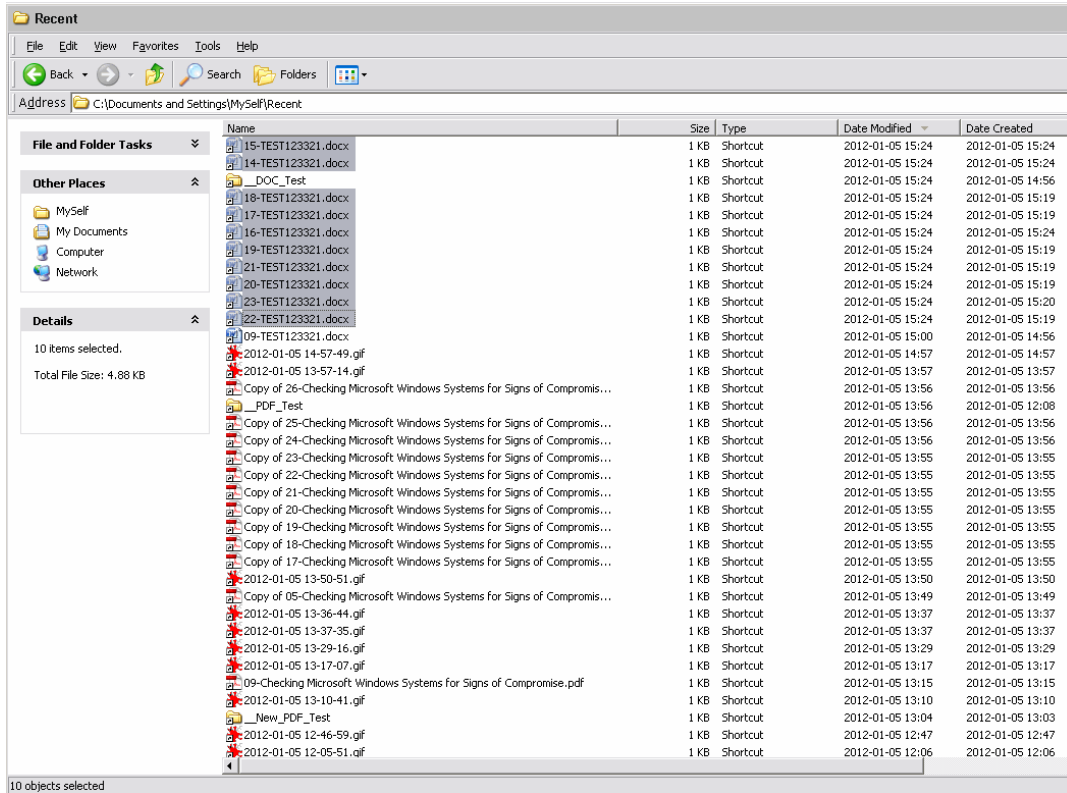


At the DOCX extension specific MRU located at HKCU \Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\docx we find it is not updated

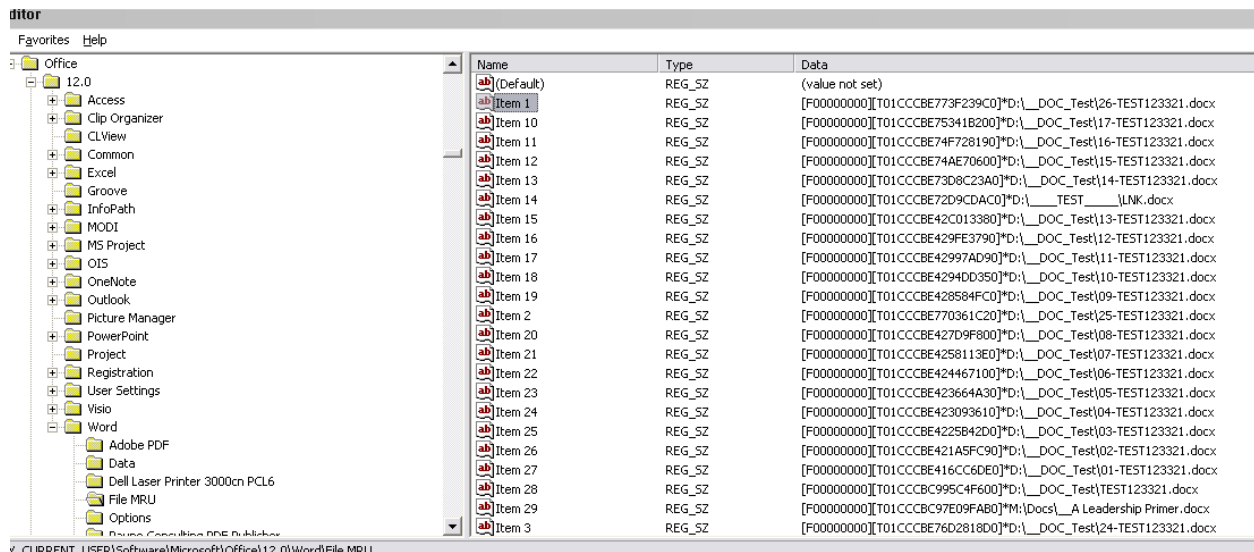
This is a ?work? in progress and is not complete. I have only made it available because a few people requested to see it.

What the Deuce LNKs!

Now we open DOCs 14-26 using the FILE | Open method from within Word. While the files are open we can see now only 10 LNK files (17-26) appear in the Recent folder, and the same when the files are closed.



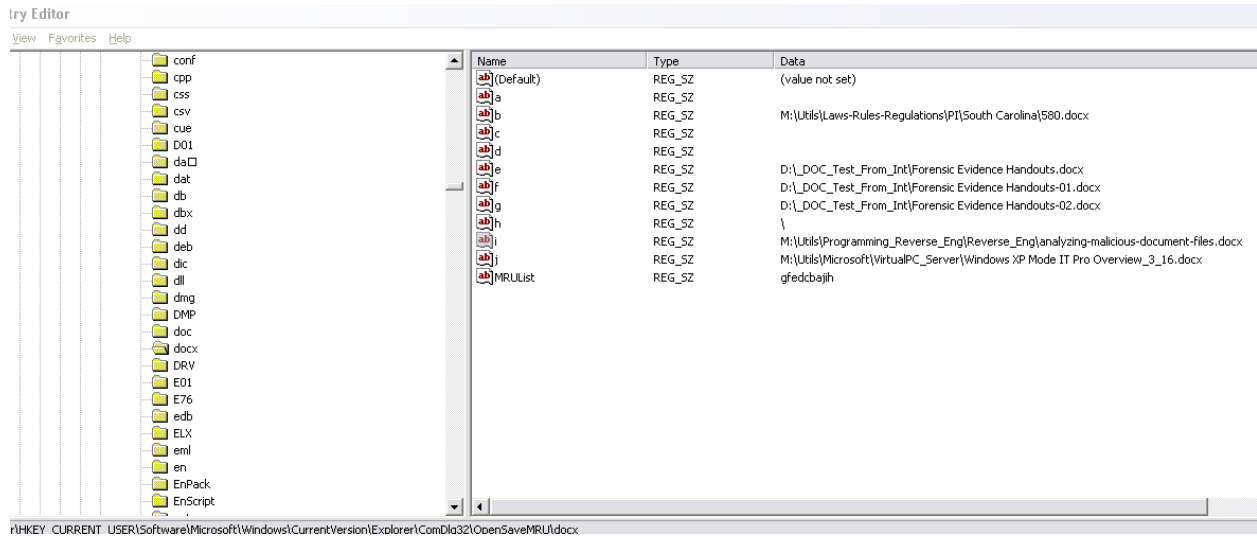
The Word File MRU list has the files 14-26 listed as well as files 01-13 because it holds 50 entries



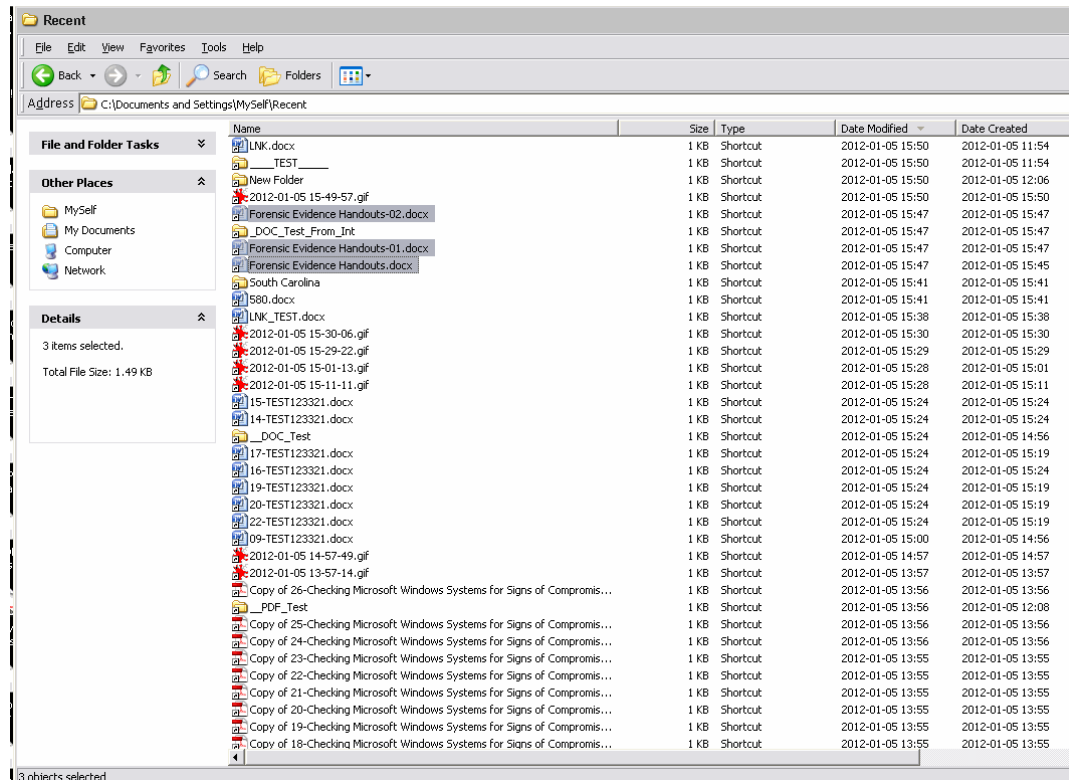
This is a ?work? in progress and is not complete. I have only made it available because a few people requested to see it.

What the Deuce LNKs!

However the DOCX extension specific MRU, still did not update? I MUST KNOW THE SECRET! I looked carefully at the list and noted that the documents seem to reference documents I downloaded from the Internet. I used FireFox, went to a website with a DOCX, downloaded it 3 times and sure enough there were 3 brand new entries in the DOCX extension specific MRU.



And there were 3 brand new LNK files, but wait, I thought LNK files were created “when a file is opened” .



This is a ?work? in progress and is not complete. I have only made it available because a few people requested to see it.

What the Deuce LNKs!

Taking a look at the metadata of the LNK we see that it references the Folder where the file was downloaded, but there is no actual target metadata

Lnk Metadata

Path: C:\Documents and Settings\MySelf\Recent\Forensic Evidence Handouts-01.docx lnk

Flags:

Attributes:

Show Command: SW_SHOWNORMAL

Name:

Relative Path:

Working Path: D:_DOC_Test_From_Int

Arguments:

Icon Location:

Target Metadata

Created Timestamp: 0001-01-01 00:00:00

Accessed Timestamp: 0001-01-01 00:00:00

Written Timestamp: 0001-01-01 00:00:00

File Size: 0

Icon Index: 0

Volume Id

Drive Type: DRIVE_FIXED

Serial No: XXXXXXXX

Name: XXXXXXXX

TrackerDataBlock

MachineId:

NewVolumeId:

NewObjectId:

NewObjectId Timestamp: 0001-01-01 00:00:00

NewObjectId Sequence Number: 0

NewObjectId MAC Address:

BirthVolumeId:

BirthObjectId:

BirthObjectId Timestamp: 0001-01-01 00:00:00

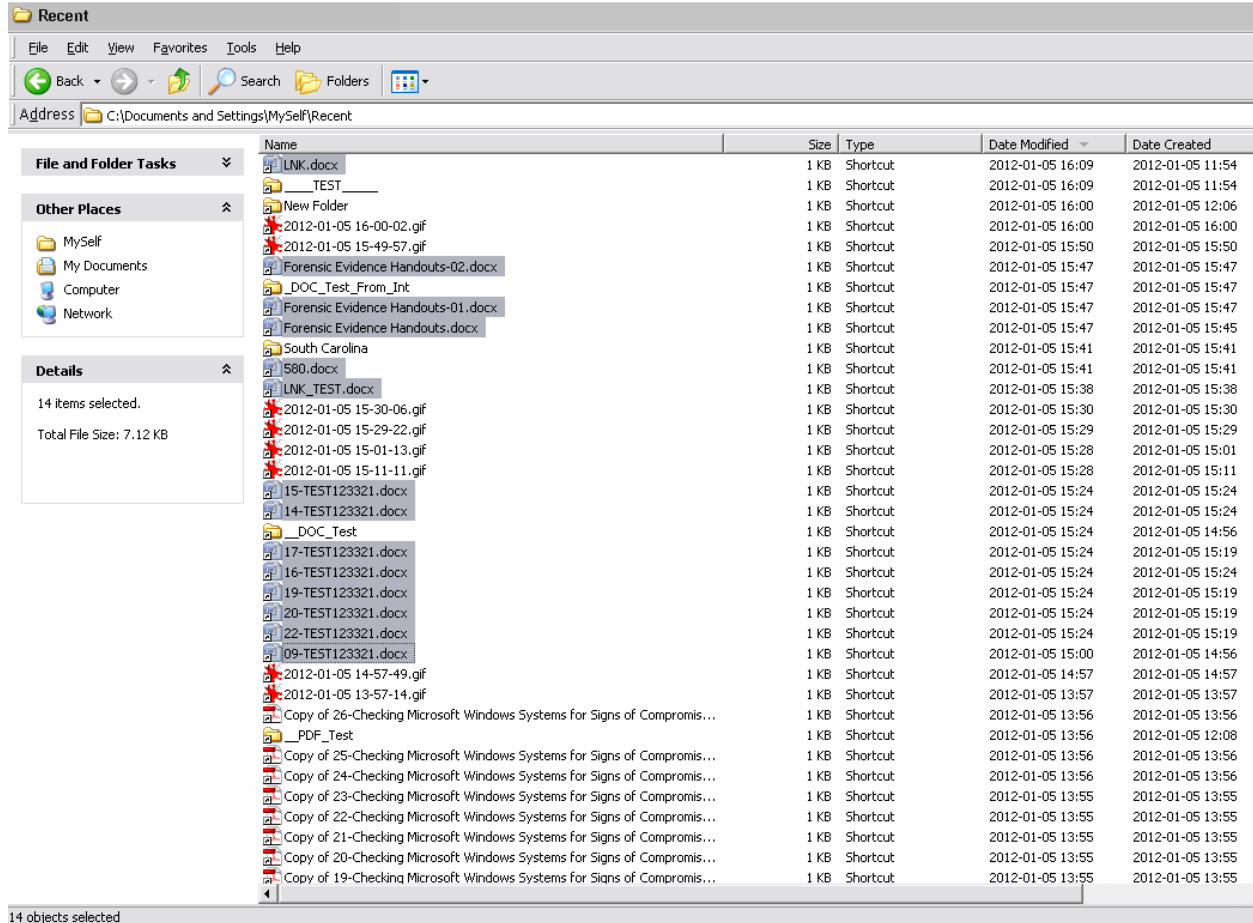
BirthObjectId Sequence Number: 0

BirthObjectId MAC Address:

This is a ?work? in progress and is not complete. I have only made it available because a few people requested to see it.

What the Deuce LNKs!

In addition, as we can see below there are now 14 DOCX LNK files in the Recent folder with no open DOCX files.



We will conclude today's (05 Jan 2012) work and open it back up tomorrow with test on time for the LNK files.

It is 07 Jan 2012 and right now from the past 6 months (through 03 Jan 2013) there are only 31 PDF LNKs and 37 DOC LNKs As opposed to 33 and 41 when we started. None of the LNKs for the 05 Jan - 07 Jan have creation dates prior to the 4th, thus it cannot be from a LNK being reused...so where did they go?

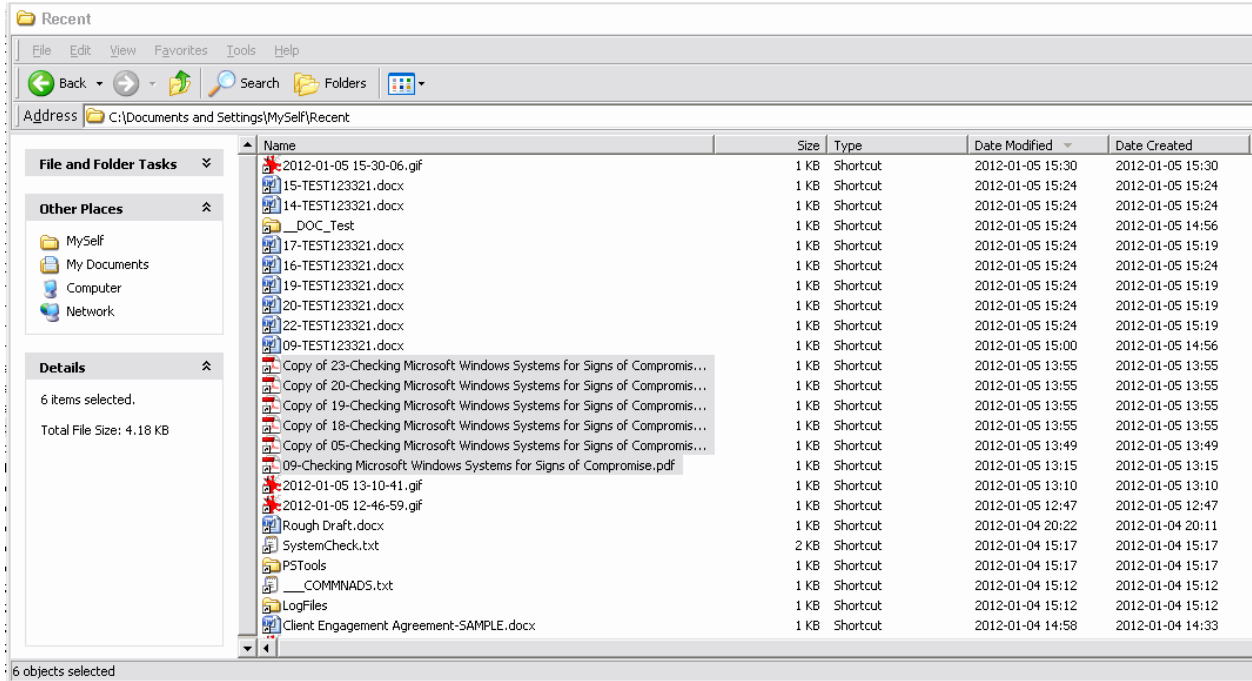
There were 92 LNKs total for 04 Jan when we were finished working on 05 Jan, today there are only 18. There were 94 LNKs total for 05 Jan when we conclude on 05 Jan, today there are only 34.

I now have 64 LNKs for the 6th 31 are MS Excel LNKs (CSV and XLSX), 17 are .SQL (I was log parsing) the rest are ZIP RAR and TXT LNKs. The point is there are no DOCX or PDF LNKs. I opened 10 PDFs this morning by the double click method, they all show in the Recent folder.

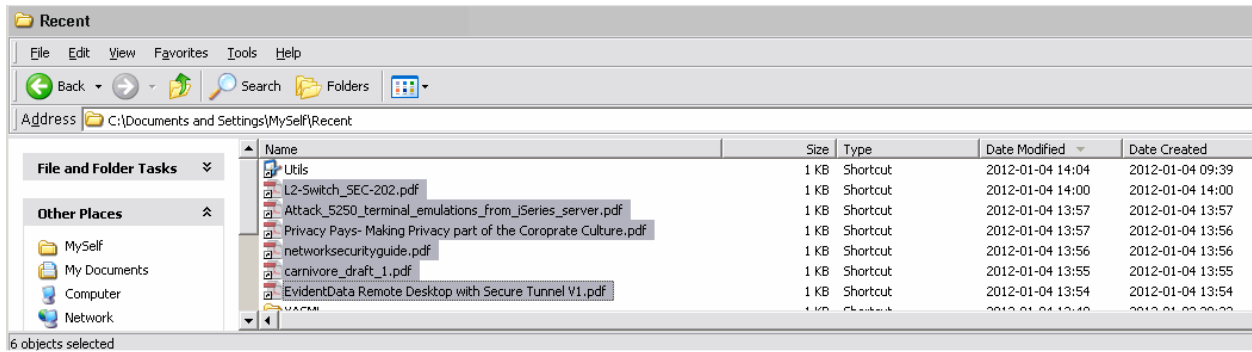
This is a ?work? in progress and is not complete. I have only made it available because a few people requested to see it.

What the Deuce LNKs!

Let us take a look at the LNKs from 4th and the 5th. For the PDF LNKs we have 6 on the 5th, the 2 “stragglers” 09 and copy of 05, and 4 others. Why did the 4 others now remain? I clearly opened 10 PDFs today it should have cleared the rest, at least I would have thought.



How about from the 4th? Here we have 6 as well? WHAT THE DEUCE!



This is a ?work? in progress and is not complete. I have only made it available because a few people requested to see it.

What the Deuce LNKs!

Note to Self:

Explain printing documents to PDF.

Explain the folder shortcuts

Explain how copy and moving a file when opening updates a LNK but makes new Reg entries.