

SuperFetch Tools: SuperFetchTree and SuperFetchList

Source:

TMurgent website at www.turgent.com/Tools.aspx (free)

Purpose:

These two tools were written to investigate the information that SuperFetch stores in its database files. As of this printing, these are still investigative tools as we do not yet fully know the format of these files. Microsoft does not document the format currently, but these tools represent the best efforts to date to extract information about them.

As explained in the book “*Windows System Performance Through Caching*”, recent versions of the Microsoft Windows operating systems record file read patterns from system usage and then prepares scenarios for certain events and stores them in a series of “DB” files in the Windows\Prefetch folder.. The contents of these files contain information such that when an implemented event occurs, the SuperFetch service will pre-cache certain files into the standby lists cache in RAM, in anticipation of their being needed.

Microsoft has suggested these scenarios include user logon and coming out of hibernation, but they have not been clear about all of the scenarios, nor how the choice is made as to if a file should be included.

These DB files are of an undocumented format and compressed. Thanks to some insight by others we now have a clue about the format of at least parts of some of these files. Using this information, I have created these two tools to parse the information from the DB files for display.

This information may be used to better understand how SuperFetch operates. It may also be of interest to the computer forensics community that wants to learn more about particular application use on a computer.

Usage:

These tools provide insight into the files that SuperFetch thinks are interesting. Not all of the files listed will be pre-fetched, however, they only appear in a DB file if they have been read in from disk.

SuperFetchList

SuperFetchList is a command line tool that dumps contents of a SuperFetch DB file. It is an updated version of ReWolf's SuuperFetch Dumper program. For the most part, I have added command line switches to control the detail level, and added an option to parse all of the db files instead of just one.

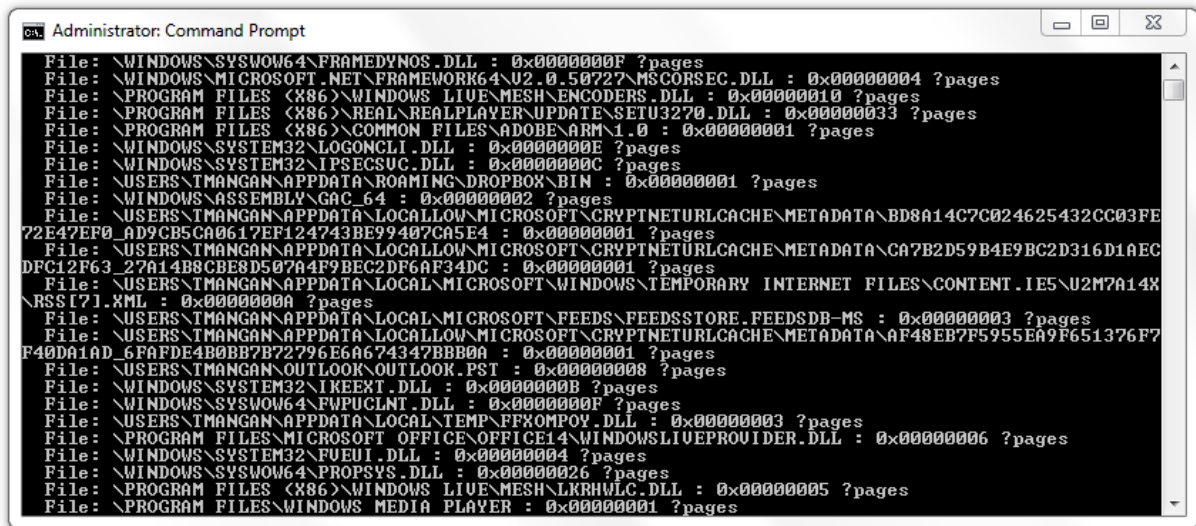
Access to the db files requires administrative access, so start a cmd prompt with "Run as Administrator" option. The command syntax is as follows:

```
Superfetchlist [-v | /v] [-a | /a | DBfile ]
```

The `-v` or `/v` (verbose) option turns on additional detail of information. You may either use the `-a` (or `/a`) option to scan all DB files located in the `C:\Windows\Prefetch` folder, or you can provide a path to a specific DB file.

If you select the all option, each file is separately processed. Output is to stdout, so you should redirect to a file, such as

```
"superfetchlist /a > output.txt"
```

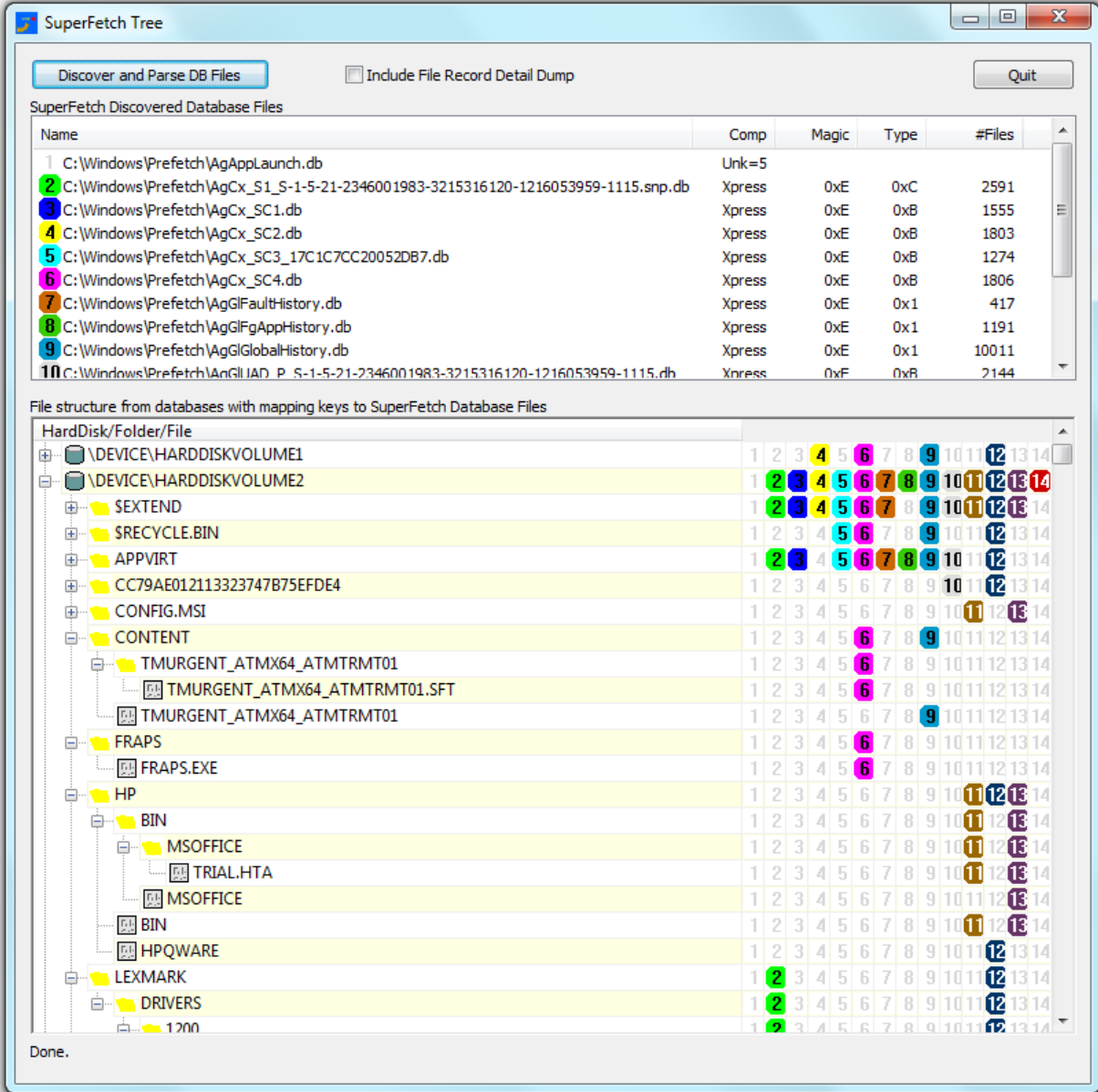


```
Administrator: Command Prompt
File: \WINDOWS\SYSWOW64\FRAMEDYNOS.DLL : 0x0000000F ?pages
File: \WINDOWS\MICROSOFT.NET\FRAMEWORK64\U2.0.50727\MSCORSEC.DLL : 0x00000004 ?pages
File: \PROGRAM FILES (X86)\WINDOWS LIVE\MESH\ENCODERS.DLL : 0x00000010 ?pages
File: \PROGRAM FILES (X86)\REAL\REALPLAYER\UPDATE\SETU3270.DLL : 0x00000033 ?pages
File: \PROGRAM FILES (X86)\COMMON FILES\ADOBE\ARM\1.0 : 0x00000001 ?pages
File: \WINDOWS\SYSTEM32\LOGONCLI.DLL : 0x0000000E ?pages
File: \WINDOWS\SYSTEM32\IPSECSUC.DLL : 0x0000000C ?pages
File: \USERS\TMANGAN\APPDATA\ROAMING\DROPBOX\BIN : 0x00000001 ?pages
File: \WINDOWS\ASSEMBLY\GAC_64 : 0x00000002 ?pages
File: \USERS\TMANGAN\APPDATA\LOCAL\MICROSOFT\CRYPTNETURLCACHE\METADATA\BD8A14C7C024625432CC03FE72E47EF0AD9CB5CA0617EF124743BE99407CA5E4 : 0x00000001 ?pages
File: \USERS\TMANGAN\APPDATA\LOCAL\MICROSOFT\CRYPTNETURLCACHE\METADATA\CA7B2D59B4E9BC2D316D1AECDFC12F63_27A14B8CBE8D507A4F9BEC2DF6AF34DC : 0x00000001 ?pages
File: \USERS\TMANGAN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET FILES\CONTENT.IE5\U2M7A14X\nRSSI?].XML : 0x0000000A ?pages
File: \USERS\TMANGAN\APPDATA\LOCAL\MICROSOFT\FEEDS\FEEDSSTORE.FEEDSDB-MS : 0x00000003 ?pages
File: \USERS\TMANGAN\APPDATA\LOCAL\MICROSOFT\CRYPTNETURLCACHE\METADATA\AF48EB7F5955EA9F651376F7F40DA1AD_6FAFDE4B0BB7B72796E6A674347BBB0A : 0x00000001 ?pages
File: \USERS\TMANGAN\OUTLOOK\OUTLOOK.PST : 0x00000008 ?pages
File: \WINDOWS\SYSTEM32\IKEEXT.DLL : 0x0000000B ?pages
File: \WINDOWS\SYSWOW64\FWPUCLNT.DLL : 0x0000000F ?pages
File: \USERS\TMANGAN\APPDATA\LOCAL\TEMP\FXOMPOY.DLL : 0x00000003 ?pages
File: \PROGRAM FILES\MICROSOFT OFFICE\OFFICE14\WINDOWS\LIVEPROVIDER.DLL : 0x00000006 ?pages
File: \WINDOWS\SYSTEM32\FVEUI.DLL : 0x00000004 ?pages
File: \WINDOWS\SYSWOW64\PROPSYS.DLL : 0x00000026 ?pages
File: \PROGRAM FILES (X86)\WINDOWS LIVE\MESH\LKRHWLC.DLL : 0x00000005 ?pages
File: \PROGRAM FILES\WINDOWS MEDIA PLAYER : 0x00000001 ?pages
```

SuperFetchTree

SuperFetchTree is a GUI tool. It locates and parses all of the SuperFetch db files (that we understand today) and displays a combined list with color coded information about what files reference this list. If you check the details checkbox, it will show additional detail from each entry (we don't understand the format of that detail at present).

This tool will automatically locate all of the db files in the C:\Windows\Prefetch folder and parse them when you click on the button. If you want to see the extra detail for files in the tree view, check the detail dump checkbox before clicking the Discover and Parse button. An example output is shown below.



The screenshot shows the SuperFetch Tree application window. At the top, there is a "Discover and Parse DB Files" button and an "Include File Record Detail Dump" checkbox. Below this is a table of discovered database files.

Name	Comp	Magic	Type	#Files
1 C:\Windows\Prefetch\AgAppLaunch.db	Unk=5			
2 C:\Windows\Prefetch\AgCx_S1_S-1-5-21-2346001983-3215316120-1216053959-1115.snp.db	Xpress	0xE	0xC	2591
3 C:\Windows\Prefetch\AgCx_SC1.db	Xpress	0xE	0xB	1555
4 C:\Windows\Prefetch\AgCx_SC2.db	Xpress	0xE	0xB	1803
5 C:\Windows\Prefetch\AgCx_SC3_17C1C7CC20052DB7.db	Xpress	0xE	0xB	1274
6 C:\Windows\Prefetch\AgCx_SC4.db	Xpress	0xE	0xB	1806
7 C:\Windows\Prefetch\AgGIFaultHistory.db	Xpress	0xE	0x1	417
8 C:\Windows\Prefetch\AgGIFgAppHistory.db	Xpress	0xE	0x1	1191
9 C:\Windows\Prefetch\AgGIGlobalHistory.db	Xpress	0xE	0x1	10011
10 C:\Windows\Prefetch\AnGIIAD_P_S-1-5-21-2346001983-3215316120-1216053959-1115.db	Xpress	0xF	0xB	2144

Below the table is a section titled "File structure from databases with mapping keys to SuperFetch Database Files". It shows a tree view of the file system with mapping keys (1-14) indicating which database files reference each file or folder.

Done.