Frequently Asked Questions

What is PFDump?

PFDump is a command line forensic tool that extracts important forensic metadata from a Windows prefetch file.

What is a prefetch file?

A prefetch file is created by a mechanism Windows uses to increase the performance of the program loader. If you look on your Windows XP or higher system you will see a *\Windows\Prefetch* folder. Inside this folder is a series of files with a '.pf' extension. These files have unusual names similar to IEXPLORE.EXE-4B6C9213.pf. **Note:** The prefetch mechanism is *enabled* by default on Windows workstation operating systems starting with XP and *disabled* on Windows server operating systems.

These files contain important program loader information such as DLL dependencies, module sizes, file paths, last run date, run count, etc. When a program is loaded for the first time, the Windows OS does a close analysis of the executable and what it needs to successfully run. This profiling information is optimized and stored in a prefetch file. The next time the program runs, the loader will look for the program's prefetch file. It will then use the information in the file to efficiently load the application. The end result is that the prefetch mechanism significantly reduces the load time of applications.

The value of prefetch files to an investigator is significant. Windows keeps up to 128 files in the prefetch folder. If a user-mode application runs – a prefetch file is created. Savvy investigators can determine what programs have run on a system, the last run time, run count, and the full path to the application.

What problem are you trying to solve?

Unfortunately, most commercial forensic tools do not provide an easy way to examine this treasure of forensic evidence. So, like any other problem - instead of complaining about it I did something about it. I researched existing prefetch publications, deeply studied the internal structure of prefetch files, then wrote a fast and easy to use tool to extract prefetch metadata and put it in a format investigators can use.

What does the tool do?

The main purpose of this tool is to provide prefetch file metadata in a flexible format. *PFDump* extracts the critical metadata from a prefetch file to tab delimited text, html, or xml formats. The tool will examine a single prefetch file, a whole folder of prefetch files, and even the prefetch folder on a live system. This makes the tool useful to incident responders who need to examine systems that cannot be taken offline.

What operating systems are supported?

I have tested the tool with prefetch files from Windows XP, Vista, and 7. It also runs on all these platforms.

What programming language is the tool written in?

The tool is written in C++ and compiled with Microsoft Visual Studio 2008. It is object oriented (e.g. C++ classes) and contains optimized C code for speed. It uses the open source cross-platform *wxWidgets* framework. It is a self-contained executable and has no other dependencies.

How do I use the tool?

The tool is very simple to use. Simply extract the prefetch files from a forensic image and provide the filename or folder containing multiple prefetch files as a parameter when you run the tool. You can also examine the prefetch files on a live system by using the /l parameter. Depending on the command line switches you choose, the tool will dump the output report to stdout, a tab delimited text file, an html file, or an xml file.

Is there a fee for using this tool?

No. I build a lot of tools for incident response work. In the spirit of giving back to the digital community that provides us so many incredible free tools, I provide this tool at no cost to anyone that finds it useful.

Who created this tool?

My name is Michael Spohn. I am a professional incident response consultant based in the Los Angeles area. You can email me at mspohn@malware-hunters.net.

Where can I learn more about this tool?

There tool is well documented. The documents are included in the tool zip file. You can download the tool at www.malware-hunters.net.