

## Using the Volatility –d option for Pretty Process Mapping

(This document is targeted to Windows users of Volatility. The aim of this document is to illustrate to the end user how to use and view the dot image format that can be generated using the PSLIST, PSSCAN2 Volatility commands.)

If you've been playing around with Volatility on your Windows machine, you've more than likely run either PSLIST or PSSCAN2 command to generate a list of processes found in a memory image:

```
"PSSCAN2"
```

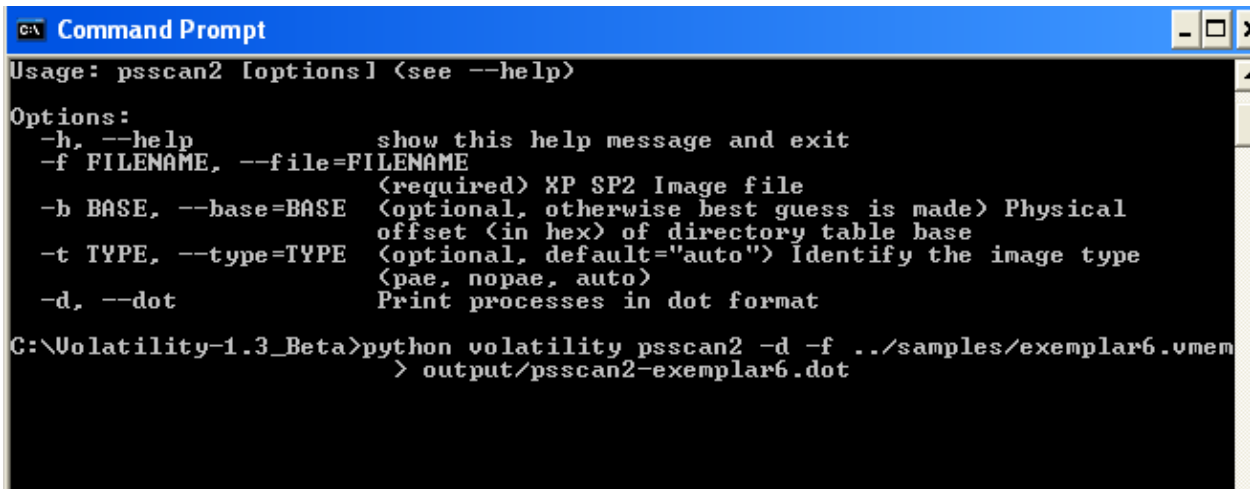
PID	PPID	Time created	Time exited	Offset	PDB	Remarks
648	656	Thu Jan 08 01:53:43 2009		0x0166f7b0	0x03800300	tdctxte.exe
1928	2000	Thu Jan 08 01:49:12 2009		0x01690920	0x03800220	explorer.exe
1232	656	Thu Jan 08 01:47:55 2009		0x016aa3c0	0x03800160	svchost.exe
336	984	Thu Jan 08 01:49:00 2009	Thu Jan 08 01:54:04 2009	0x016cf728	0x03800200	wuauclt.exe
1516	656	Thu Jan 08 01:47:56 2009		0x016e3020	0x038001a0	spoolsv.exe
668	612	Thu Jan 08 01:46:59 2009		0x016ee9a0	0x038000a0	lsass.exe
1656	872	Thu Jan 08 01:53:43 2009	Thu Jan 08 01:53:43 2009	0x016fb4b8	0x03800320	sopidkc.exe
472	872	Thu Jan 08 01:53:42 2009	Thu Jan 08 01:53:43 2009	0x016fdc48	0x038002e0	tdctxte.exe
412	656	Thu Jan 08 01:49:22 2009		0x017df020	0x03800240	msiexec.exe
464	1928	Thu Jan 08 01:52:57 2009		0x017f7020	0x03800140	dw8.exe
1932	656	Thu Jan 08 01:53:41 2009		0x017f96c0	0x038002c0	afisicx.exe
1056	872	Thu Jan 08 01:53:30 2009		0x017fc678	0x038000c0	dxonool32.sys
984	656	Thu Jan 08 01:47:02 2009		0x018068b0	0x03800100	svchost.exe
516	4	Thu Jan 08 01:46:50 2009		0x0180f600	0x03800020	smss.exe
888	656	Thu Jan 08 01:47:02 2009		0x0183c388	0x038000e0	svchost.exe
656	612	Thu Jan 08 01:46:59 2009		0x01859b38	0x03800080	services.exe
796	872	Thu Jan 08 01:53:41 2009	Thu Jan 08 01:53:41 2009	0x01869020	0x03800280	afisicx.exe
1048	984	Thu Jan 08 01:49:13 2009		0x018bc988	0x03800260	wscntfy.exe
1876	656	Thu Jan 08 01:53:43 2009		0x019aa3d0	0x03800340	sopidkc.exe
1020	656	Thu Jan 08 01:47:02 2009		0x019db628	0x03800120	svchost.exe
408	656	Thu Jan 08 01:48:23 2009		0x01a3d020	0x038001e0	alg.exe
224	1020	Thu Jan 08 01:48:17 2009		0x01a41860	0x038001c0	wmiprvse.exe
1304	656	Thu Jan 08 01:47:56 2009		0x01b0cd50	0x03800180	svchost.exe
588	516	Thu Jan 08 01:46:56 2009		0x01b12170	0x03800040	csrss.exe
872	464	Thu Jan 08 01:53:00 2009		0x01b13b40	0x038002a0	atsxyzd.sys
612	516	Thu Jan 08 01:46:56 2009		0x01b2d2d8	0x03800060	winlogon.exe
4	0			0x01bcc7f8	0x007d0000	system

Notice that this list presents both the PID process id and the PPID (Parent PID). You can manually map PPID to PID to determine what process spawned another process...for example see PID 872 (atsxyzd.sys) has a PPID of 464? Now look up the list at PID 464(dw8.exe)...From this we can tell that running dw8.exe created a child process called atsxyzd.sys...Look again at the PPID list and you can also determine that PID 872(atsxyzd.sys) is the PPID of other processes such as PID 1656(sopidkc.exe), PID 472(tdctxte.exe), PID 1056 (dxonool32.sys) and PID 796(afisicx.exe).

Now you either mentally map this process tree or draw it out physically if that helps you, but there IS another way to visualize this process mapping.....

Have you taken a look at the options for the Volatility PSSCAN2 command? If you type “python volatility psscan2 –help”, you’ll see a list of supported options for that Volatility command (and any other Volatility command)

Notice the –d option (“Print processes in dot format”)? Lets run PSSCAN2 with the –d option and output the results to a file....



```
C:\> Usage: psscan2 [options] (see --help)

Options:
-h, --help          show this help message and exit
-f FILENAME, --file=FILENAME
                    (required) XP SP2 Image file
-b BASE, --base=BASE (optional, otherwise best guess is made) Physical
                    offset (in hex) of directory table base
-t TYPE, --type=TYPE (optional, default="auto") Identify the image type
                    (pae, nopae, auto)
-d, --dot           Print processes in dot format

C:\Volatility-1.3_Beta>python volatility psscan2 -d -f ../samples/exemplar6.vmem
> output/psscan2-exemplar6.dot
```

By itself this output file is not going to be much good to you. In fact, if you’re running Office, the output file might even be identified as a WORD DOT file type....it is NOT. It is a DOT IMAGE FORMATED file. In order to view the output of the dot format file, on Windows you will need download and install GraphViz-2.24 (stable) : [www.graphviz.org/download\\_windows.php](http://www.graphviz.org/download_windows.php)



- About
- Download
- source
- fedora
- rhel
- ubuntu
- solaris
- macos
- windows
- News
- Gallery
- Documentation

## Graphviz - Graph Visualization Softw

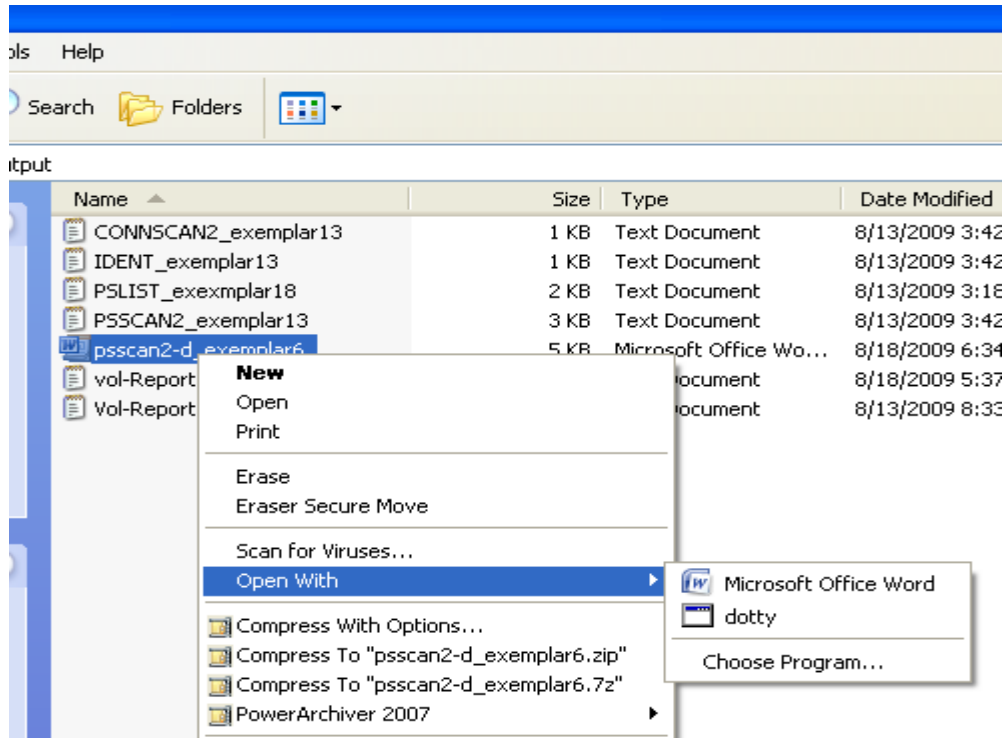
If a package name contains 'mingw', that indicates the package MinGW. Otherwise, the package was built with Visual Studio.

**Warning:** If you plan to use Graphviz as a library, make sure y: the version compatible with your compiler. MinGW binaries will with Visual Studio code. Also, note that the Visual Studio pack only the Release version. If you link these in with a program usin mode, your program will crash.

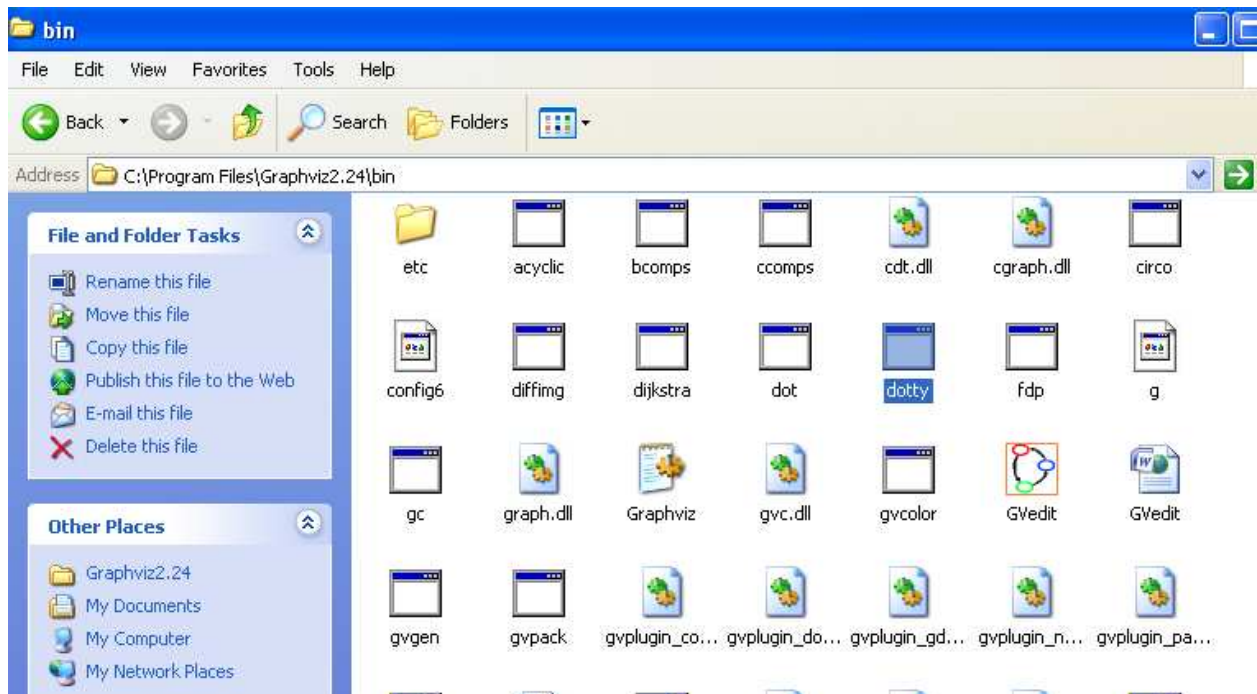
graphviz	current stable release	development sna
Windows	<a href="#">graphviz-2.24.msi</a>	<a href="#">graphviz-2.25.20090818_044</a> <a href="#">graphviz-bin-2.25.20090818</a>

If you encounter problems running or building the Windows ver [bug report](#) or contact [Arif Bilgin](#).

Once installed, right click your psscan2.dot output file and choose to OPEN WITH....and CHOOSE PROGRAM.....

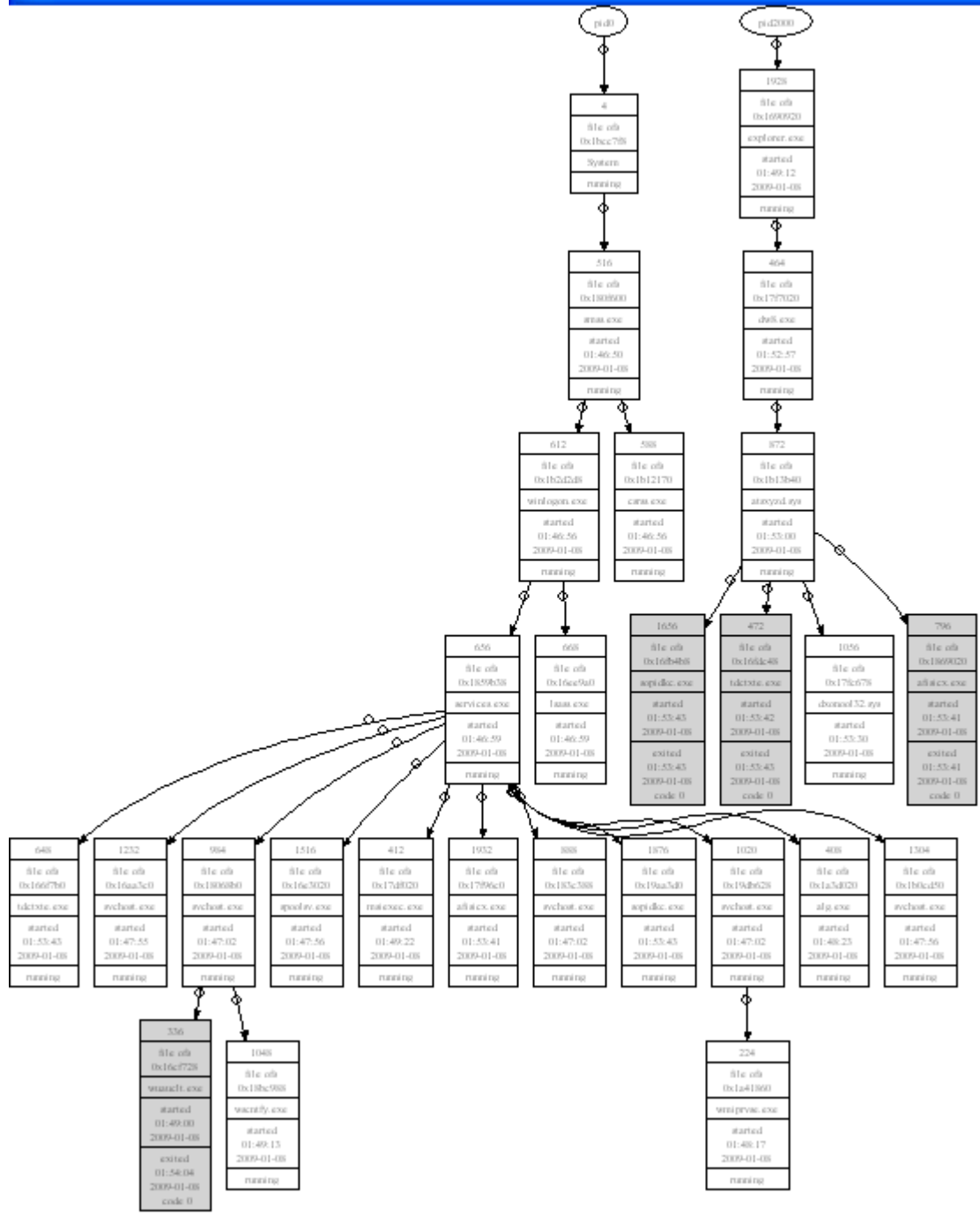


Now Browse to the GraphViz/bin folder and select "dotty"



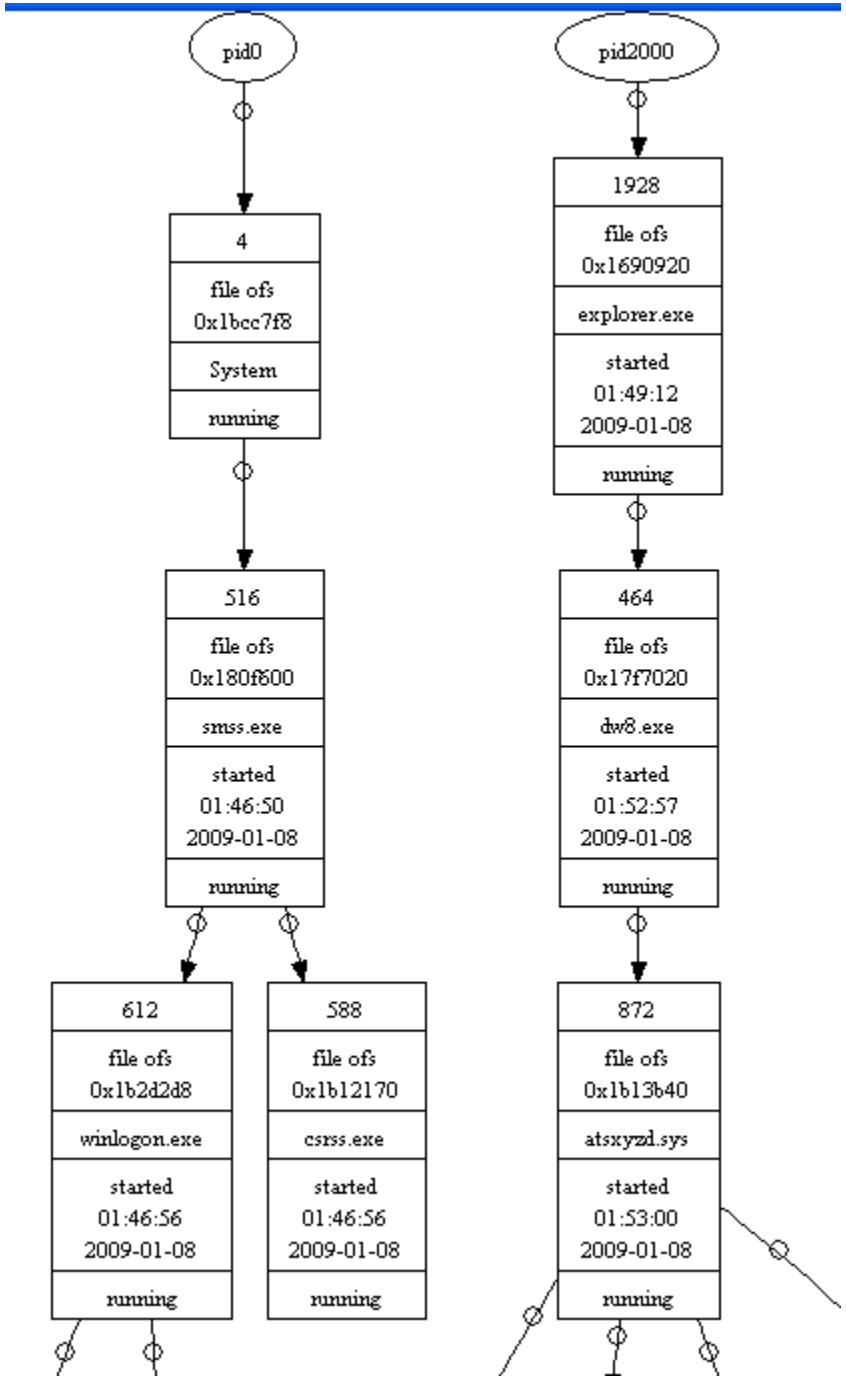
Dotty will now display your DOT image PSSCAN2 output file....

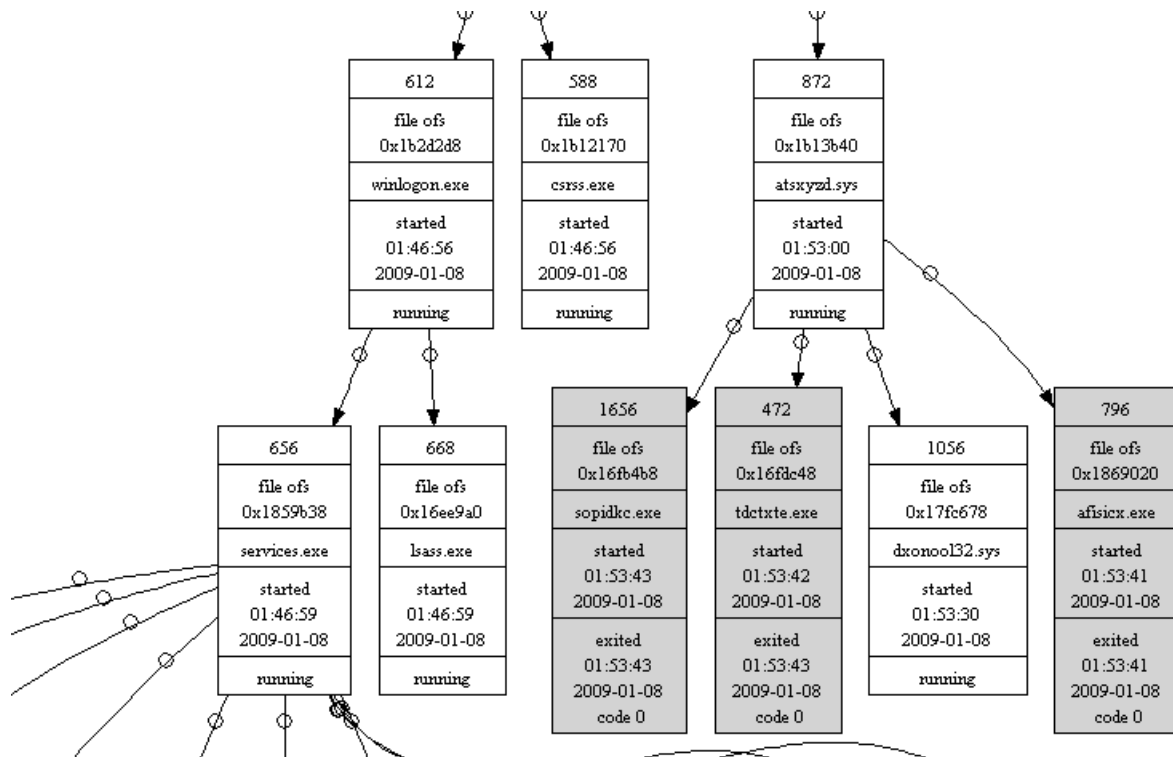
**DOTTY**



By right clicking within the Dotty program, you can see different option such as Zoom in, Zoom Out, Print, etc.... If we zoom in we can much more clearly see the relationships between PPID

and PIDs: such as below where we see PPID 2000 (explorer.exe), which begat PID 464 (dw8.exe), which begat PID 872(atsxyzd.sys)...





Above we can see a clear illustration of PID 872 and its spawned child PIDs 1656, 472, 1056 and 796. Remember when we were trying this with just the text output?

Using the Volatility `-d` option for the PSSCAN2 or PSLIST output offers a Volatility user another way to quickly identify relationships of process artifacts found in memory.