=============================

| Symbols in Windbg |

=============================

TOC:

----

1.) Setting Symbol Paths

2.) Getting symbols for offline use

3.) Troubleshooting Symbol Issues

----

1.) Setting Symbol Paths

------------------------

a.) By default, Windbg will attempt to

download symbols from Microsoft's symbol

server. This works well in situations where

internet access is available, and bandwidth

isn't particularly limited. In other cases,

however, (such as the classroom environment),

getting it to work properly can be a bit

challenging (without large delays, at least).

b.) You can set the symbol server paths in Windbg

several ways:

\* File -> Symbol File Path -> (add symbol path here)

\* Windbg also checks the \_NT\_SYMBOL\_PATH to try and find symbols.

Setting it in the following fashion:

\_NT\_SYMBOL\_PATH=SRV\*C:\Users\sample\Symbols\*http://msdl.microsoft.com/download/symbols;

will cause it to try using C:\Users\sample\Symbols before Microsoft's symbol server.

------------------------

2.) Getting Symbols for Offline Use

-----------------------------------

a.) The symchk tool (bundled with the Windows Debugging Tools) can be used

to download symbols for a system. It can typically be located by looking

in the same area Windbg itself is installed at (NOTE: ensure that the symchk

you use matches the architecture of the system you are currently operating on,

as using the x86 symchk to download symbols \*may\* result in an incomplete set,

due to WoW64). There is an OSR NT-Insider article that speaks to this in a bit

more detail at: https://www.osr.com/nt-insider/2015-issue1/fix-offline-symbols/

i.) On the system you wish to download symbols for, create an empty directory, and

run the following command:

symchk /om output.txt /ie \* /s \path\to\empty\folder

ii.) Once that is accomplished, copy output.txt to a location that has internet access, and run:

symchk /im output.txt /s SRV\*\path\to\symbol\directory\*http://msdl.microsoft.com/download/symbols

b.) Another option is to configure caching with Windbg by adding cache\*<location>\* entries to your \_NT\_SYMBOL\_PATH

environment variable, which will cause symbols downloaded from Microsoft's symbol server to be stored at that

location.

-----------------------------------

3.) Troubleshooting Symbol Issues

---------------------------------

a.) If things change while running Windbg, and symbols need to be reloaded, execute the following command:

.reload

b.) Additional output for troubleshooting purposes can be obtained by running:

!sym noisy

prior to .reload (which will increase the verbosity of output)