Using Sigflow on Windows

# 1) Ruby and TShark installation

Both Ruby and TShark are required for Sigflow to run. We are going to install Ruby version 1.9.3-p551 and TShark version 1.10.2 because Sigflow has been tested and works well with these versions. Other versions of Ruby and Wireshark might work (probably not). It’s highly recommended to use these specific versions.

## Downloading and installing Ruby 1.9.3-p551

1. Download the Ruby installer through this link: <http://dl.bintray.com/oneclick/rubyinstaller/rubyinstaller-1.9.3-p551.exe>
2. Run the installer and continue through the wizard until you get to the *Installation Destination and Optional Tasks* page.
3. On this page, make sure you check the *Add Ruby executables to your PATH* checkbox.
4. Continue through the wizard and finish the installation.
5. Ruby should now be properly installed! You can test this by typing *ruby -v* in a Command Prompt.

## Downloading and installing TShark 1.10.2

1. Both 32-bit and 64-bit installers are available for download. Download either the 32-bit or 64-bit installer from from one of these links: <https://www.wireshark.org/download/win32/all-versions/Wireshark-win32-1.10.2.exe> (32-bit) or <https://www.wireshark.org/download/win64/all-versions/Wireshark-win64-1.10.2.exe> (64-bit). Download the 32-bit installer if you are unsure of which version to choose.
2. Run the installer and continue through the wizard until you get to the *Choose Components* page.
3. On this page, make sure that the *TShark* checkbox is checked. All other checkboxes are optional and you may uncheck them.
4. Continue through the wizard and on the *Choose Install Location* page, take note of the installation path.
5. Finish the installation. Note that installing WinPcap isn’t necessary for Sigflow to work and is therefore optional.
6. Now you have to add your tshark installation path (the one you took note of earlier, usually something similar to: *C:\Program Files\Wireshark*) to the Path system variable. This can be done by opening a Command Prompt as administrator (search for *cmd*, right click the *cmd.exe* file and select *Run as administrator*) by writing the command: *setx /M PATH “<installation\_path>;%PATH%”*. Simply replace *<installation\_path>* with your installation path.
7. TShark should now be properly installed! You can test this by typing *tshark -v* in a Command Prompt.

# 2) Extracting Sigflow

Now that both Ruby and TShark have been installed, you should extract Sigflow from the *Sigflow\_on\_windows.zip* archive. This can be done by opening the archive with the File Explorer in windows and extracting the Sigflow folder from there. You can extract the Sigflow folder to any location you want.

# 3) Adding Sigflow to path

Adding sigflow to the path system variable is easily done by running the *Add Sigflow to path.cmd* file as administrator in the extracted Sigflow folder. Doing this will allow you to easily run sigflow from any location.

# 4) Running Sigflow

When run, Sigflow will generate a diagram consisting of html pages at the location it’s run from. To view the generated diagram, simply open the html file with a web browser.

There are three batch scripts to help running Sigflow on Windows. Place the scripts in the same folder as where you store pcap/log files to analyze. It is recommended that you create shortcuts to these scripts on your desktop.

## “Sigflow help.cmd”

This script will when run output Sigflow help information including all the options Sigflow can be run with.

## “Run Sigflow from here.cmd”

This is the recommended script to use for running Sigflow on Windows.

When running the script (“double-click”) it will first ask for the pcap/log file to analyze. The ‘TAB’-key can be used to autocomplete the pcap/log filename. An alternative file will be presented matching the initial letters for each TAB click. At the last the script will ask what Sigflow options to use in the analysis. The script will then run Sigflow and automatically open the diagram with Internet Explorer.

## “sigflow.cmd”

This script can be used to run Sigflow from the Command Prompt. Simply run it from the Command Prompt and pass your options as parameters to it. Example use through Command Prompt: *sigflow.cmd -f my\_pcap\_file.pcap -m -c -s*