Why:

I created **pi-hole Visualiser** because I had installed pi-hole but wanted to know more about what the clients on my home network were doing.

Acknowledgements:

- The Raspberry Pi Foundation: For creating a REALLY easy way to experiment with and learn Linux, programming and computing in general.
- Jacob Salmela the creator of pi-hole: If you haven't donated yet, given you have downloaded this Splunk App you probably should.
- The Ninjas @ Splunk: For creating Splunk, The Universal forwarder for Linux ARM (Raspberry Pi) and the Splunk 6.x Dashboard Examples App used as a guide for visualisations.

Disclaimer:

- **pi-hole Visualiser** is provided as-is with no warranty expressed or implied.
- The use of **pi-hole Visualiser** on your Splunk infrastructure is entirely at your own risk.
- **pi-hole Visualiser** is in no way associated with Jacob Salmela, The RaspberryPi Foundation or Splunk.
- Any trade marks used in this app belong to their respective owners, they know who they are.
- Licensed under the MIT License (Refer to License section at the bottom of this page for details).

Things you will need:

Raspberry Pi

It must be capable of running both pi-hole and the splunk forwarder Agent. The Raspberry Pi 2, Model B, 1GB RAM is ideal.
Refer to: https://raspberrypi.org for resellers.

pi-hole

Refer to: https://pi-hole.net for instructions on how to install pi-hole onto your Raspberry Pi.

Splunk Universal Forwarder for ARM

Refer to: https://splunkbase.splunk.com/app/1611/ on how to download and install the forwarder on your Raspberry Pi.

Splunk Enterprise

pi-hole Visualiser was built and tested and deployed on Splunk Enterprise 6.3.2 using Deployment Server
Some visualisations used by **pi-hole Visualiser** may not supported older versions.
Refer to: http://www.splunk.com/en_us/download.html for download and install instructions.

How to install and configure pi-hole Visualiser:

These instructions assume you have the **Splunk Universal Forwarder for ARM** installed on your Raspberry Pi and you have a compatible Splunk Enterprise system available.

Note: $SPLUNK_HOME$ is the location where your Splunk searchhead instance is installed.

- Install the **pi-hole Visualiser** (**piholeVis**) app into Splunk.
  Use either the Splunk GUI to install the app, or download and extract the **piholeVis** archive directly to **$SPLUNK_HOME$/etc/apps** on your searchhead. Restart Splunk to complete the install.

- **VERY IMPORTANT - Do not Skip these steps.**

  Copy **pi-holeCollector.tar.gz** archive upto the Raspberry Pi to **/tmp** using scp (or other file transfer program, I use puTTY pscp). SSH must be enabled on your Raspberry Pi for this to work.

  ```
  pscp $SPLUNK_HOME$/etc/apps/piHoleVis/resources/pi-holeCollector.tar.gz pi@nnn.nnn.nnn.nnn:/tmp
  ```

  Where **nnn.nnn.nnn.nnn** is the IP address of your Raspberry Pi.

  Log into your Raspberry Pi as "pi" and elevate your session to root.

  ```
  pi@RaspberryPi ~ $ sudo -s
  ```

  cd to **/tmp** and extract the **pi-holeCollector** app into the **Splunk Universal Forwarder for ARM**.

  ```
  root@RaspberryPi:/home/pi# cd /tmp
  root@RaspberryPi:/tmp# tar -xvf pi-holeCollector.tar.gz -C /opt/splunkforwarder/etc/apps
  ```

  Using **nano** edit **/opt/splunkforwarder/etc/apps/pi-holeCollector/default/outputs.conf** of the **pi-holeCollector** app update the [tcpout] stanza to where you want the **Splunk Universal Forwarder for ARM** to send the Log/Event data.

  ```
  root@RaspberryPi:/tmp# nano /opt/splunkforwarder/etc/apps/pi-holeCollector/default/outputs.conf
  ```

  ```
  [tcpout]
  defaultGroup=indexer
  # default
  [tcpout:indexer]
  server=xxx.xxx.xxx.xxx:9997
  ```

  Where **xxx.xxx.xxx.xxx** is the IP of your indexer/heavy forwarder. It is assumed you are using the standard port of TCP 9997. If not, change this too.

- Reboot your Raspberry Pi to end your session. The **Splunk Universal Forwarder for ARM** should start automatically and the **pi-holeCollector** app along with it.

  ```
  reboot
  ```

- Log into your Splunk Enterprise System and access **pi-hole Visualiser**. and discover what your network clients are upto.

Troubleshooting

- **Is pi-hole running and configured?**

  Refer to: https://pi-hole.net for advice.

  Confirm that your client machines are using pi-hole as their DNS Server.

  For Windows run **nslookup** from the commandline.

```
nslookup
Default Server: Pi-Hole.IsWorking.OK
Address: yyy.yyy.yyy.yyy
```

yyy.yyy.yyy.yyy should be the IP of your Raspberry Pi running pi-hole. If it isn't then your clients are not using pi-hole form DNS.

Log into your Raspberry Pi and run the following command to tail the pi-hole log and review its content.

```
pi@RaspberryPi ~ $ tail -f /var/log/pihole.log
```

On your client machine generate some web traffic (i.e. DNS lookups)
If the pi-hole is running and you are pointing to it for DNS correctly you should see fresh log entries being written to the pihole.log.

- **I am not seeing anything in Splunk?**

Refer to: https://splunkbase.splunk.com/app/1611/ to make sure you have installed the Splunk Universal Forwarder correctly.

Check that the pi-holeCollector app is installed correctly, your Splunk server is referenced correctly in **outputs.conf** and that the **pi-hole** index exists.

log into your Raspberry Pi and run the following command.

```
pi@RaspberryPi ~ $ ls -l /opt
```

If the **Splunk Universal forwarder for ARM** is installed you should see a directory called **splunkforwarder**.

```
pi@RaspberryPi ~ $ ls -l /opt/splunkforwarder/etc/apps
```

Check that you have installed the **pi-holeCollector** app correctly.
Check that splunk can execute the shell scripts.

```
pi@RaspberryPi ~ $ sudo -s
root@RaspberryPi:/home/pi# ls -l /opt/splunkforwarder/etc/apps/pi-holeCollector/bin
total 20
4 -rwxr-xr-x 1 root root 39 Jan 30 20:39 clock.sh
4 -rwxr-xr-x 1 root root 23 Jan 30 20:39 df.sh
4 -rwxr-xr-x 1 root root 34 Jan 30 20:39 temp.sh
4 -rwxr-xr-x 1 root root 79 Jan 30 20:39 top.sh
4 -rwxr-xr-x 1 root root 35 Jan 30 20:39 volts.sh
```

Confirm that all the shell scripts are executable (as shown above). If not resolve this by running the following command.

```
root@RaspberryPi:/home/pi# chmod +x /opt/splunkforwarder/etc/apps/pi-holeCollector/bin/*.sh
```

Exit your root session when finished.

Check the splunk server that pi-holeVis is sending logs to that it is configured to recieve splunk events on TCP 9997.
Log into your Raspberry Pi and run the following command (You may need to install a telnet client first).
xxx.xxx.xxx.xxx is the IP you are sending Splunk events too.

```
root@RaspberryPi:/home/pi# telnet xxx.xxx.xxx.xxx 9997
Trying xxx.xxx.xxx.xxx...
Connected to xxx.xxx.xxx.xxx.
Escape character is '^]'.
```

If the port is open and the IP address is correct you will see the valid connection.

Log into your Raspberry Pi and run the following command.

```
root@RaspberryPi:/home/pi# top | grep splunkd
1746 root      20   0   88400  40644  17208 S   5.8  4.3   7:53.31 splunkd
1746 root      20   0   88400  40644  17208 S   0.7  4.3   7:53.33 splunkd
```

```
1747 root      20   0   25212   5980   4876 S   0.3  0.6   0:41.08 splunkd
```

If the **Splunk Universal Forwarder for ARM** is running it will appear in the output. If it doesn't appear after a few seconds the forwarder isn't running. Refer to Splunk's documentation to resolve. control-break to exit.

Is the **Splunk Universal forwarder for ARM** is running but you still aren't seeing any data in **pi-hole Visualiser** run the following command.

```
root@RaspberryPi:/home/pi# tail -f /opt/splunkforwarder/var/log/splunk/splunkd.log
```

If the **Splunk Universal Forwarder for ARM** is running OK the log will be relatively quiet. If you are seeing ERRORS they will need to be addressed.

Change Log

Version	Release Date	Comments
1.0	25/01/2016	First Release
1.1	31/01/2016	Added "Pi Health" dashboard, other dashboard tweaks, documentation improvements.
1.1.1	31/01/2016	pi-hole Visualiser now creates its own index, squashed bugs introduced in 1.1

License