This is a Technology Addon that adds basic search knowledge to supported events generated by p0f Passive Fingerprinting tool.

This TA has no UI views and requires the Splunk administrator to manually set appropriate sourcetypes on the p0f log file monitor to sourcetype=p0f or assure p0f writes it's log to a file named "p0f.log. Please see the README for details.

This TA has been tested with p0f v3.x. Input requirements: p0f output should use the -o switch to output the p0f logfile in greppable format.

The p0f eventtypes that are included in this TA are:

p0f_link - p0f fingerprinting of linktypes communicating on the network
p0f_os - p0f fingerprinting of host platforms communicating on the network
p0f_hostchange - p0f picks up on portchanges of applications
p0f_uptime - p0f detects some uptime stats of communicating hosts
p0f_app - p0f fingerprinting of webservers and other browser type utilities