

Tool #2: Log Investigator

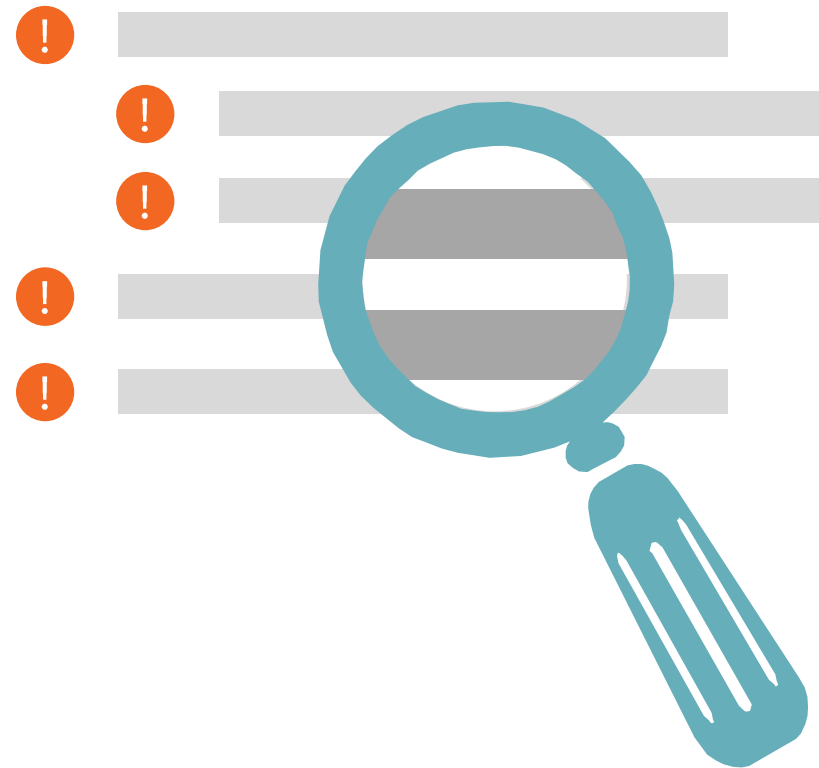


Adam Bertram

adamtheautomator.com | Twitter: [@adbertram](https://twitter.com/adbertram)

Tool Overview

TROUBLESHOOTING



Prerequisites

PowerShell v4



Admin Control over
remote machine

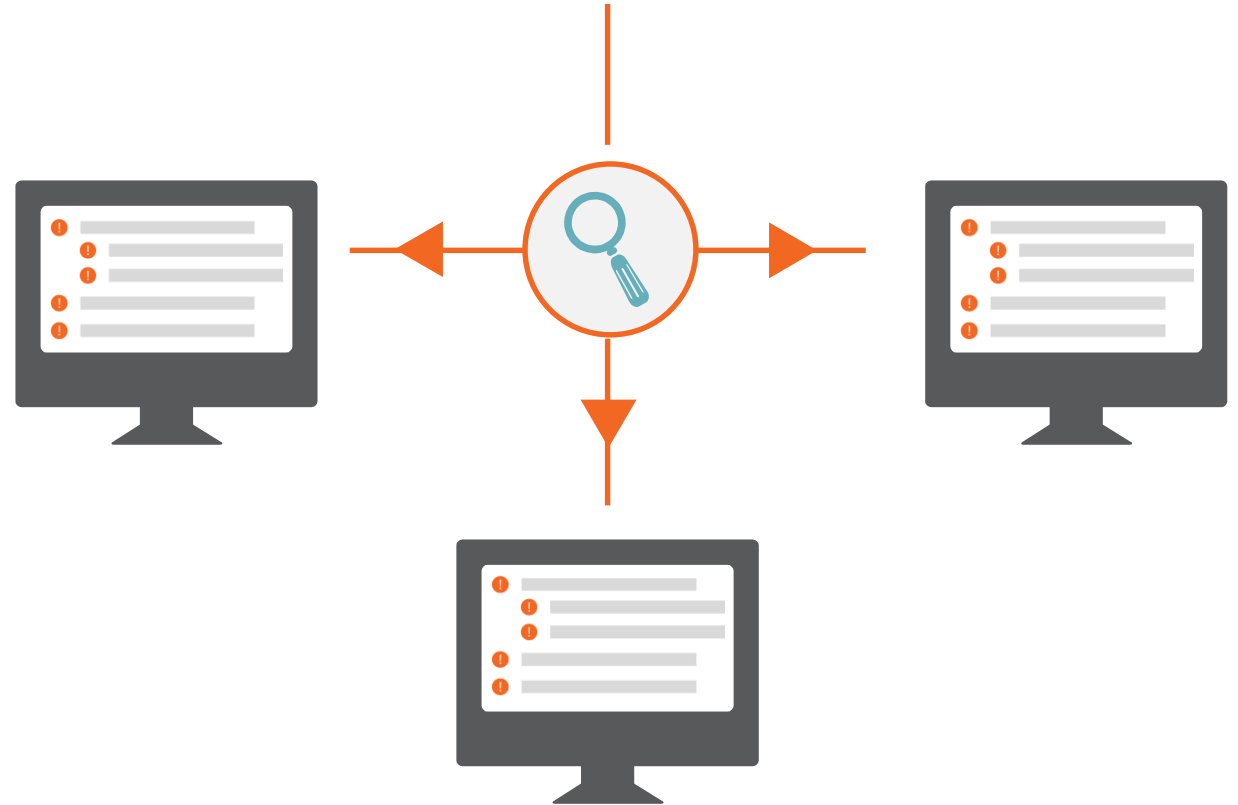


Interrogating Windows Event Logs

Get-EventLog cmdlet



Log Investigator tool










Interrogating Text Logs

Text logs

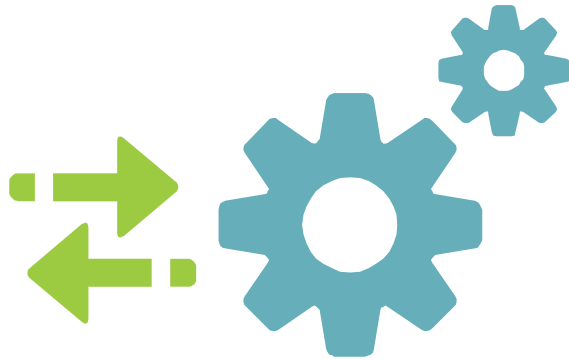


search for log files that were last
written to within the specified time
period



Name	Last Modified ▼
 #####.log	#####
 #####.log	#####
 #####.log	#####
 #####.log	#####
 #####.log	#####
 #####.log	#####
 #####.log	#####

Building the Tool Set



Each tool has different
inputs, outputs and
processing methodologies

- ✓ Move everything into a set of functions
- ✓ Tool can be easily reused at a later time
- ✓ Combine all these functions into a module later

Takeaways

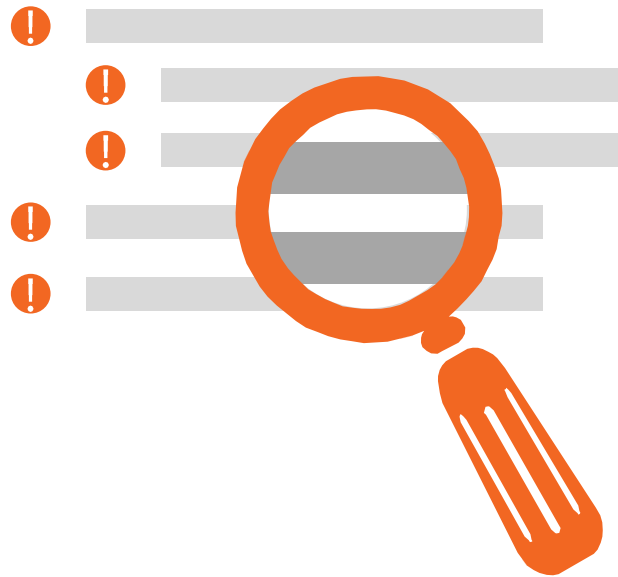


More than 1 way to get
stuff done in
PowerShell

Get-EventLog cmdlet is more common than the
Get-WinEvent cmdlet

Get-WinEvent has a drastic performance
improvement over Get-EventLog.

Summary



Created the Log Investigator tool



Scan Multiple Log sources

Get Logs with in a specified timeframe