Applied Regular Expressions using PowerShell

Course Overview

Regular Expressions provide a fast and powerful tool to search data for patterns of information based on a series of functions and literal characters. This specialized one-day workshop provides the knowledge and skills necessary to extract information from a variety of data files including text, logs, code, spreadsheets and other Office type documents. Using a variety of tools and processes, the participant will explore the RegEx language, defining each metacharacters function before applying a structured pattern search across known data. Then using Windows® PowerShell search large data files such as IIS logs to put structure to unstructured data.

This course will first introduce you to the RegEx language and apply the skills learnt across multiple data sets using Windows® PowerShell. This is a hands-on intensive course with multiple instructor led labs and student practicals, followed by a certification exam to demonstrate proficiently in building complex RegEx patterns and applications in PowerShell.

What You Will Learn

- Introduction to Regular Expressions
    o This module will introduce you to the applied use of the Regular Expressions across multiple platforms and demonstrate the powerful application usage this language offers in your daily examinations of data.

- Creating Simple Expressions
    o During this module we will define the use of different command syntax's in a pattern search to located data within data, the following commands will be explored:
        ▪ Literal Characters
        ▪ Meta Characters and their functions
        ▪ Wildcard uses and pitfalls
        ▪ Regular Expression Sets
        ▪ Regular Expression Ranges
        ▪ Use of Function Groups
        ▪ Quantifiers and Repetitions

- Exercises in RegEx pattern searching in PowerShell
    o Applying the skills learnt in the previous modules, we will build and apply pattern searches across multiple data types using PowerShell

- Certification Exam
    o Final course exam using knowledge learnt in the previous exercises across an ISS log

Course Type
Specialized

Course Length
1 day

Course Code
Spec. – RegEx

SPYDER FORENSICS

APPLIED REGULAR EXPRESSIONS USING POWERSHELL
Specialized Level | Participant Guide

Specialist Forensics Curriculum
An introduction to the RegEx language and its use

The Knowledge You Need to Succeed in Digital Investigations

SPYDER FORENSICS