Chapter 24 Lab

Make no mistakes about it, regular expressions can make your head spin so don’t try to create complex regex’s right off the bat. Start simple and here are a few exercises to ease you into it. Use regular expressions and operators to complete the following:

1. Get all files in your Windows directory that have a 2 digit number as part of the name.  
     
   dir c:\windows | where {$\_.name -match "\d{2}"}
2. Find all processes running on your computer that are from Microsoft and display the process ID, name and company name. Hint: Pipe Get-Process to Get-Member to discover property names.  
     
   get-process | where {$\_.company -match "^Microsoft"} | Select Name,ID,Company
3. In the Windows Update log, usually found in C:\Windows, you want to display only the lines where the agent began installing files. You may need to open the file in Notepad to figure out what string you need to select.

get-content .\WindowsUpdate.log | Select-string "Start[\w+\W+]+Agent: Installing Updates"