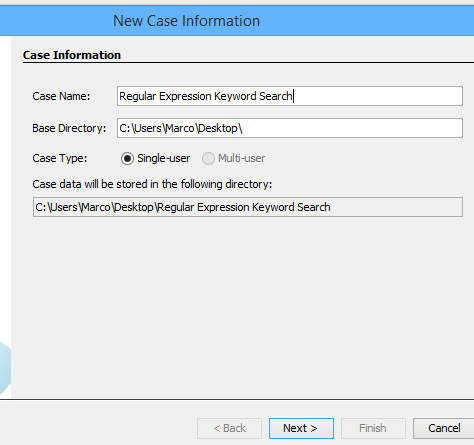
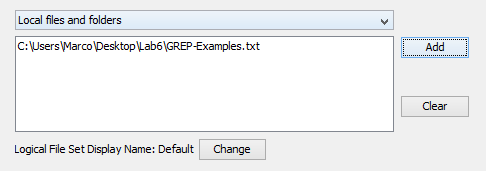
Lab 6 by Marco Seman & Jason Lu

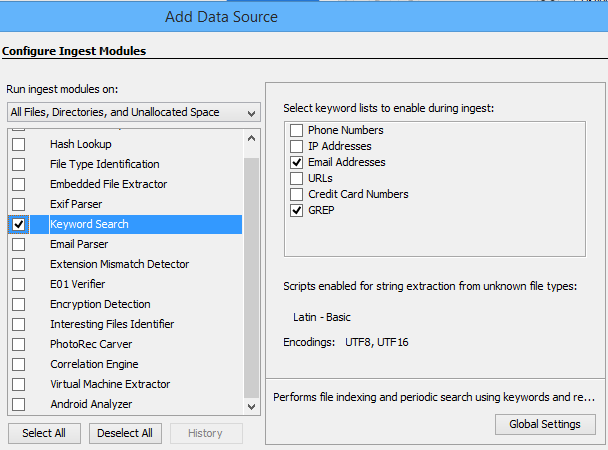
1. Launch Autopsy and create a case, Create New Case and name it as “Regular Expression Keyword Search”.



2. Add data source type: choose Logical Files; browse and select the path to "GREP-Examples.txt".

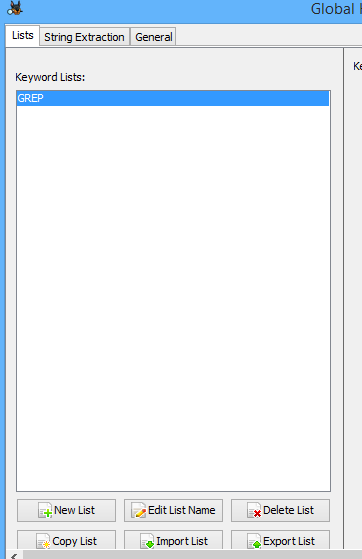


3. In the Ingest (processing) modules window, uncheck all modules except the “Keyword Search”;

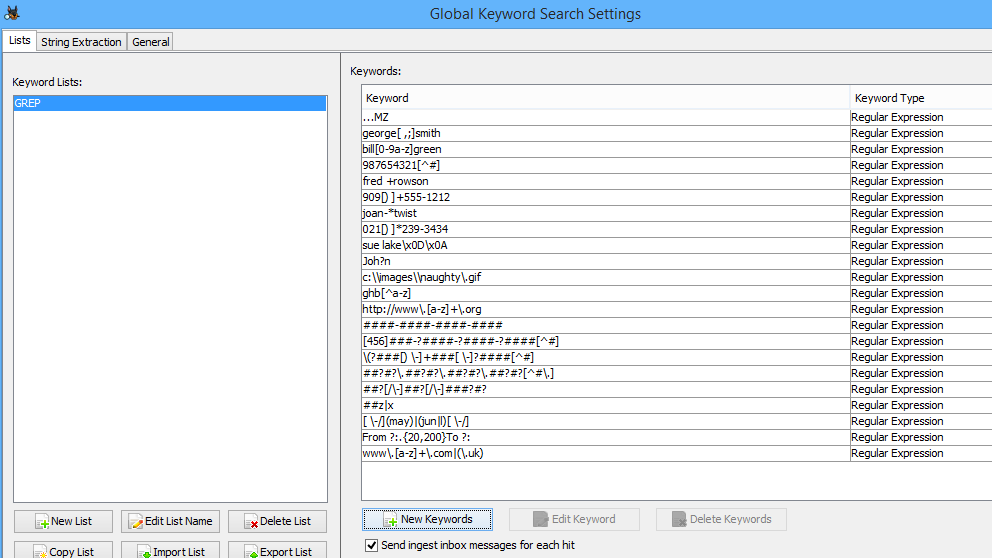


4. Click “Keyword Search” and then click Global Setting.

5. At the Global Keyword Search Setting window, click “new list” and input the “GREP” as the list name.

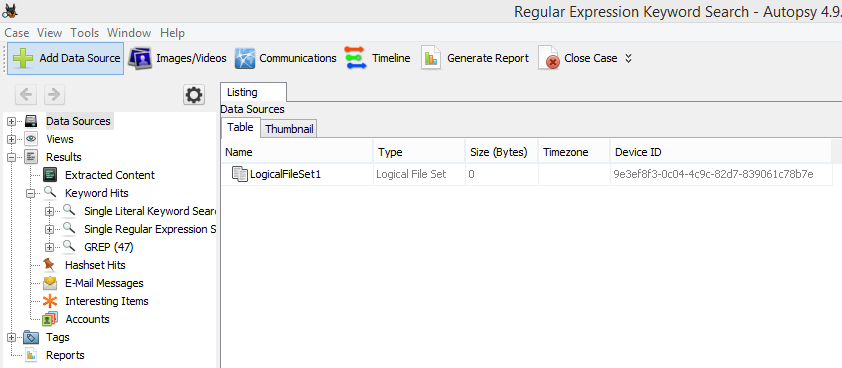


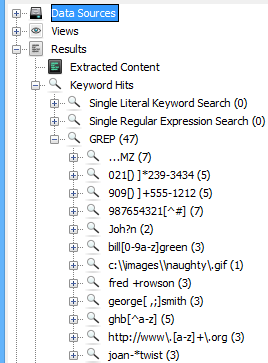
6. Click “New Keywords” and then copy and paste the keyword list from the “GREP-keyword-list.txt” file, and check “regular expression” button.



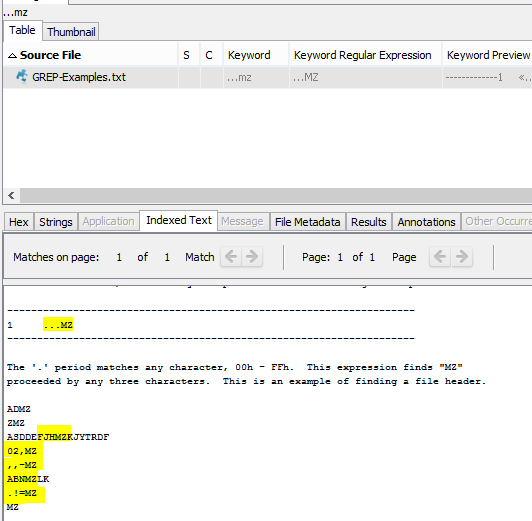
7. Click “OK” twice; click Next and then click Finish.

8. Review the search results under Results > Keyword Hits > GREP, and find all the matches.



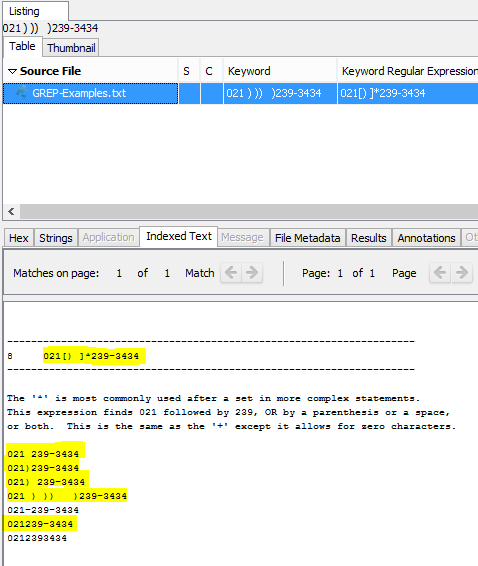


Regular Expression for ..MZ



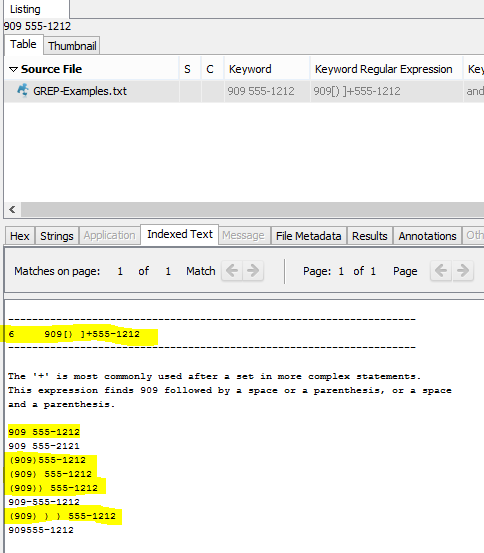
For ...MZ the three periods represent that there must be three digits before the letters MZ

Regular Expression for 021[) ]\*239-3434



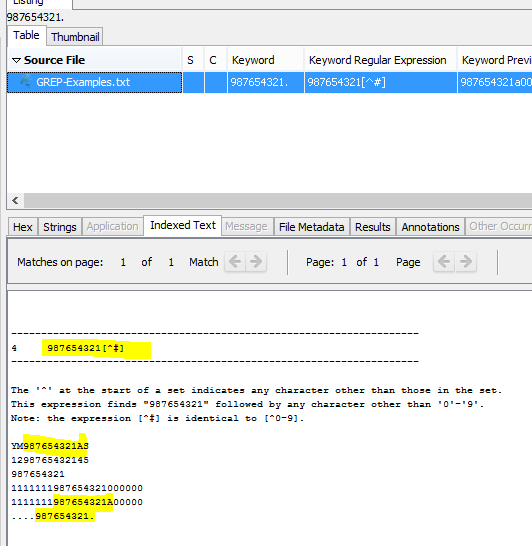
For this, the \* represents that the digit can be repeated 0 or more times.

Regular Expression for 909[) ]+555-1212



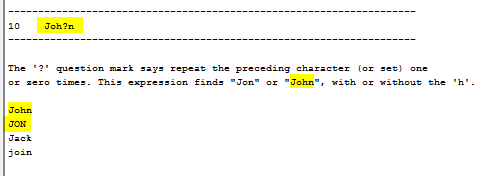
909[) ]+555-1212 - this scenario, the, the 909 is counted as well as repeating “) “ as many times times the user chooses.

Regular Expression for 987654321[^#]



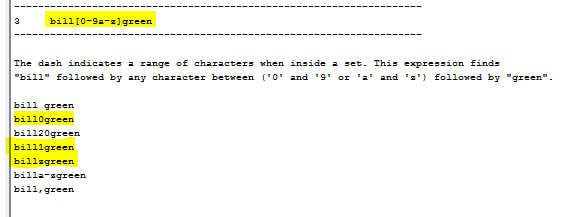
Here, the [^#] is identical to 0-9

Regular Expression for Joh?n



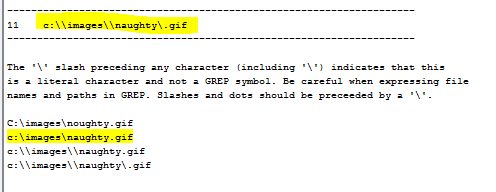
The ? represents 0 or more times after the value

Regular Expression for Bill[0-9a-z]green



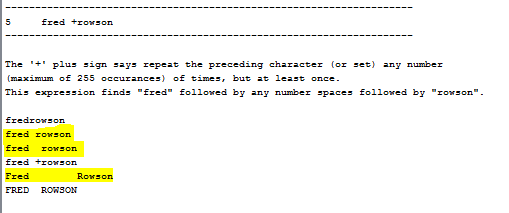
The [0-9a-z] represents any character that is within those ranges followed by green

Regular Expression for C:\\images\\naughty\.gif



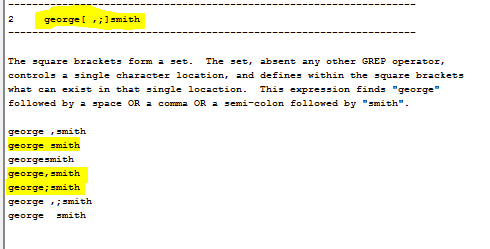
For this scenario, the \\ indicates that it must be exactly one backslash.

Regular expression for fred +rowson



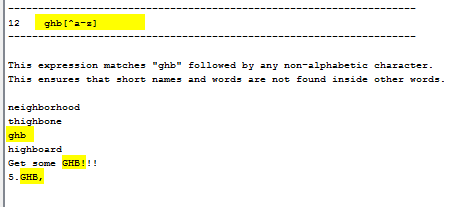
The + before rowson represent one or more space

Regular expression for george[ , ;]smith



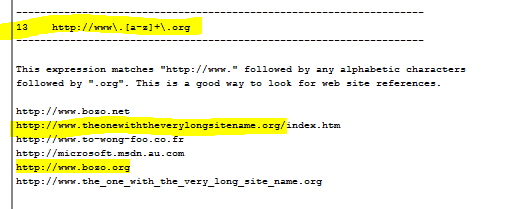
The [ , ;] represent an or function

Regular expression for ghb[^a-z]



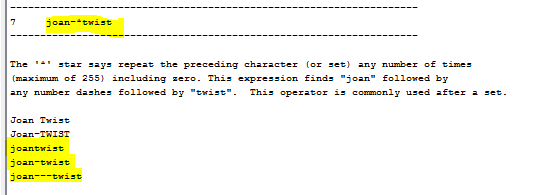
The [^a-z] represents anything besides what’s in an alphabet

Regular expression for [http://www\.[a-z]+\.org](about:blank)



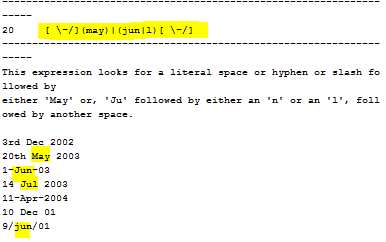
Searches any website between www. (website) . org. Must be between a-z

Regular Expression for joan-\*twist



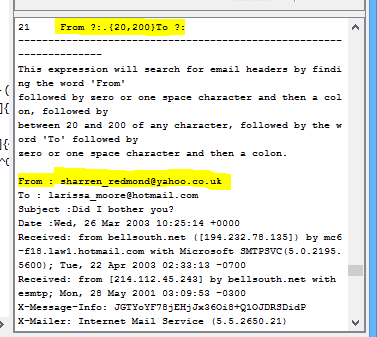
The \* represent zero one or many

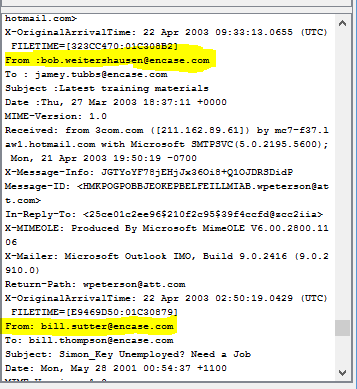
Regular Expression for ((may)|(ju(n|)))



The (\-/] represents that there can be a space, forward slash (/) or dash(-) before may or jun. the “|” expression represents an or option

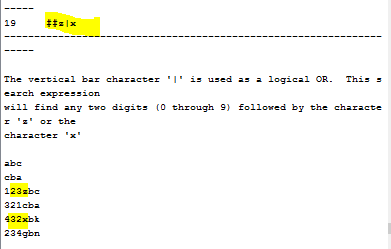
Regular Expression for from ?:. {20,200} To?:





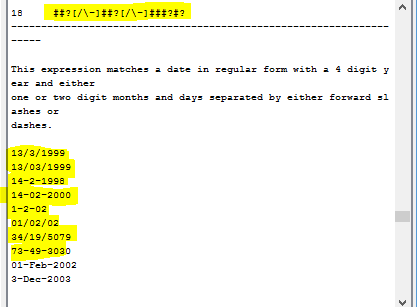
The ?: means that “:” can be repeated zero or more times

Regular expression for [0-9][0-9](z|x)

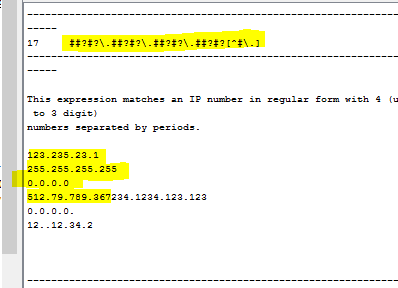


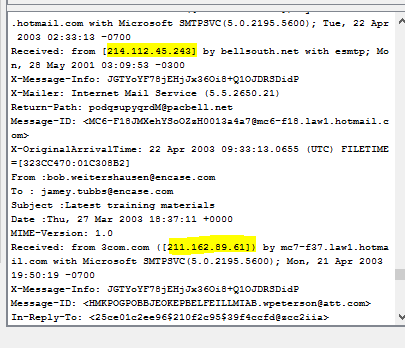
Represent that there can be any two numbers before either z or x

Regular expression for ##?[/\-]##?[/\-]###?#?

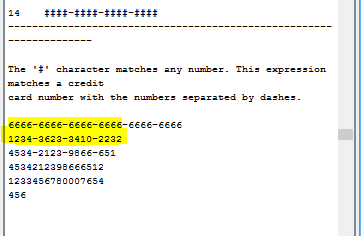


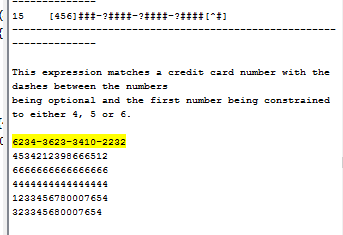
Regular expression for ##?#?\.##?#.##?#?[^#\.]



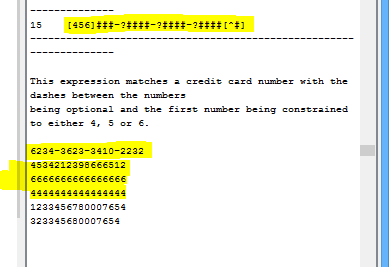


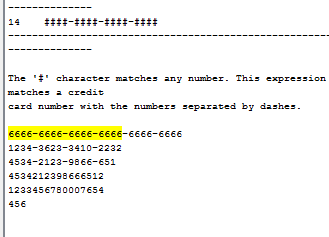
Regular expression for [0-9]{4}-[0-9]{4}-[0-9]{4}-[0-9]{4}



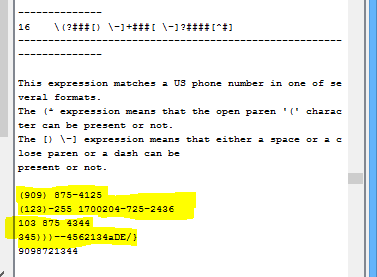


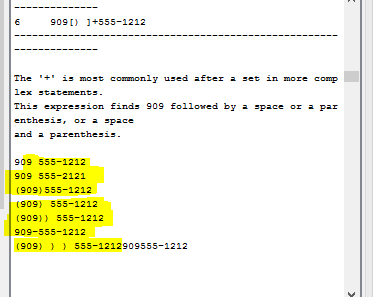
Regular Expression for [456][0-9]{3}-?[0-9]{4}-?[0-9]{4}-?[0-9]{4}





Regular expression for \(?[0-9]{3}[) \-]+[0-9]{3}[ \-]?[0-9]{4}[^0-9]:





Regular Expression for www\.[a-z]+\.co(m|(\.uk))



What we learned:

For lab 6, we learned a how to take an input file with a variety of texts and search for any regular expression from our keyword list. Using the regular expression feature in autopsy, we learned a variety of techniques of how regular expression is implemented. We learned features such as [a-z],[1-9],[A-Z] searches for any values or letters between those set of numbers. We also learned some features such as \* = (zero or many), ? = (zero or one), . = (single character) and much more. Being that we had a little experience with regular expressions during our course in Discrete Structures II, it is interesting to see how it can be useful in the digital forensics field.