Collegiate Cyber Defense Competitions

Inject Name	Explain REGEX Coding
Inject ID	SOCS18T

<table>
<tr><td><b>Description</b></td><td>A security consultant wrote a Python script that searches the central syslog repository for common messages that an analyst would want to review or investigate. One of those filters is coded as a regular expression as follows:
[r”(?:iptables|netfilter).*DROP.*SRC=(?P<src>\d{1,3}(?:\.\d{1,3}){3})",]
What does this expression look for ? Explain the REGEX tokens used and what they represent in the message. Provide an example message that this filter would find.</td></tr>
<tr><td><b>Deliverables</b></td><td>Respond with a business memo that explains the regular expression example, and provide an example message that this filter would find.</td></tr>
</table>