SANS DFIR Regex Cheat Sheet

Saturday, August 6, 2022 1:56 PM

Regex - Links

- https://regex101.com/ - Learn / build / test
- SANS SEC 455 Regex Cheat Sheet - https://github.com/sans-blue-team/sec455-wiki/blob/master/Resources/regular-expressions-cheat-sheet-v1.pdf
- MIT Regex Cheat Sheet - https://web.mit.edu/hackl/www/lab/turkshop/slides/regex-cheatsheet.pdf
- Cheatography Regex Cheat Sheet - https://cheatography.com/davechild/cheat-sheets/regular-expressions/

Regex - (Non) Capturing Groups

Capturing (and non-capturing) groups are a good way to identify and re-use regex matches

- ^(.+?,)(.+?,)(.+?,)(.+?,)(.+?,)$ -- Break line into multiple capture groups
- ^(.+?,){2} -- Start at the beginning of the line, and match (twice) the smallest possible group of characters followed by a comma.

- ^(?:.+?,){2}(.+?,) -- Start at the beginning of the line, and match (twice) -- *but don't capture!* -- the smallest possible group of characters followed by a comma. Find -- and capture for reuse! -- the third group of characters followed by a comma.

- (?:^(.+?,){2})(.+?$) -- Non-capturing group (beginning of the line) and capturing group (the rest of the line)