

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.

```
18 "542e4cff-e99c-4399-b60e-06b3950d210b",1,"Network activity","ip-src","2.38.41.213","",1,1412320511,"", "", "", "", ""
19 "542e4cff-989c-429a-9549-06b3950d210b",1,"Network activity","ip-src","2.97.3.104","",1,1412320511,"", "", "", "", ""
20 "542e4cff-af30-4059-acc8-06b3950d210b",1,"Network activity","ip-src","2.99.33.207","",1,1412320511,"", "", "", "", ""
21 "542e4cff-f684-4c0b-b778-06b3950d210b",1,"Network activity","ip-src","2.99.243.74","",1,1412320511,"", "", "", "", ""
22 "542e4cff-a264-44c6-95ea-06b3950d210b",1,"Network activity","ip-src","2.100.214.95","",1,1412320511,"", "", "", "", ""
```

- `^(?:.+?){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)