

## Lecture 14: Extract fields and add knowledge to data

---

Regular expressions using online tool:

Tool	<a href="https://regex101.com/">https://regex101.com/</a>
Sample log line	192.168.219.1 - - [07/Jul/2020:11:01:31 -0400] "GET /splunkbasicscourse HTTP/1.1" 404 493 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36"
Regular expression (Regex) for Apache access logs	^(?<clientip>\S+) (?<identity>\S+) (?<username>\S+) \[(?<timestamp>[^\]]*\)] \"(?<method>\S+) (?<uri>\S+) (?<version>[^\"]*)\" (?<status>\S+) (?<request_size>\S+) \"(?<referrer>[^\"]*)\" \"(?<useragent>[^\"]*)\"
Link to access created regex directly	<a href="https://regex101.com/r/7BvT6j/1">https://regex101.com/r/7BvT6j/1</a>