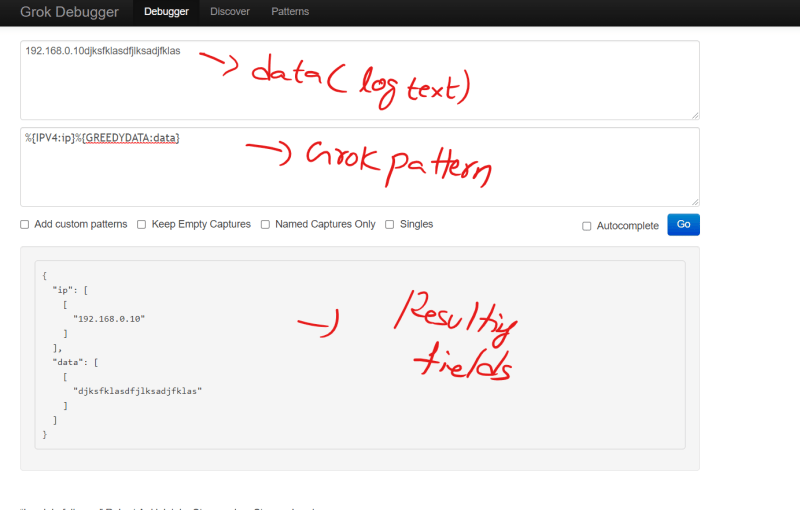
**What is GROK**

* grok is a way to match a line against regular expression, map specific parts of line into dedicated fields
* The basic format of a logstash grok filter

%{SYNTAX:SEMANTIC}

%{PATTERN:FieldName}

* Elastic search has defined around 200 patterns <https://github.com/logstash-plugins/logstash-patterns-core>
* GROK Extracts fields when we write grok patterns which can be use logstash-grok filter 
* Core grok patterns: <https://github.com/logstash-plugins/logstash-patterns-core/blob/main/patterns/ecs-v1/grok-patterns>