# Queries used in the demo

```
index=main | stats count by source sourcetype host
```

```
index=main "Failed password"
| rex "Failed password for (?<user>\S+) from (?<ip>\d+\.\d+\.\d+\.\d+)"
| stats count by ip user
| sort -count
```

```
index=main "203.0.113.45"
| table _time sourcetype source host _raw
| sort _time
```

```
index=main source="webserver.log" "203.0.113.45"
| rex field=_raw "^(?<ip>\d+\.\d+\.\d+\.\d+).*\"(?<method>[A-Z]+) (?<uri>[^ ]+) HTTP"
| stats count by status uri
```

```
index=main source="app.log" (WARN OR ERROR OR "Repeated suspicious")
| table _time _raw
| sort -_time
```

alert :

```
index=main "Failed password"
| rex "from (?<ip>\d+\.\d+\.\d+\.\d+)"
| stats count by ip
| where count > 5
```