

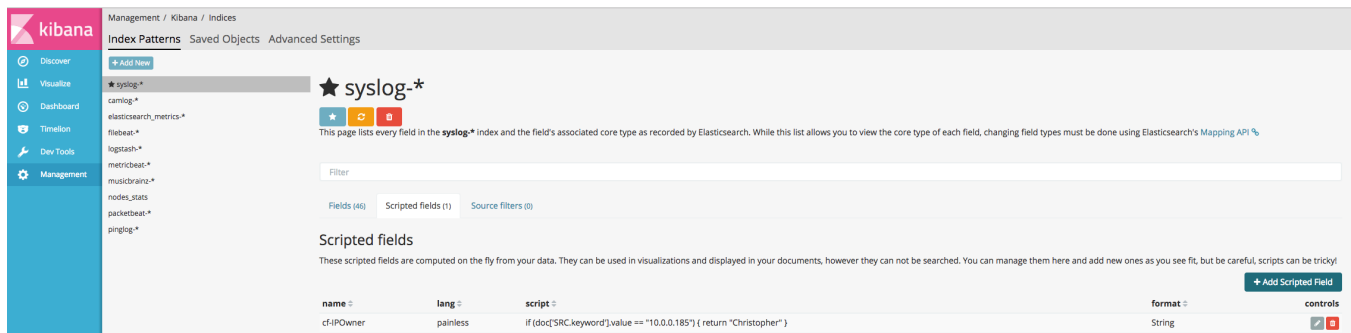
Scripting Fields in Kibana

On my first attempts to create a "replica" of the Splunk Home Monitor, where syslogs from my Asus Router are parsed, I used Logstash for translating IP Addresses to the Owner and Device type in my 10-beats-input.conf file:

```
if [type] == "syslog" {
  if [SRC] == "10.0.0.185" {
    mutate
    {
      add_field => { "IPOwner" => "Christopher" "Device" => "Galaxy" "Interface" => "Wifi" }
    }
  }
  if [SRC] == "10.0.0.190" {
    mutate
    {
      add_field => { "IPOwner" => "Device" "Device" => "Skur Cam" "Interface" => "Cable" }
    }
  }
}
...
...
```

the problem her, is that the data is persistent in Elasticsearch, and Changes to IP's and Devices are not reflected. In Splunk I solved this with a lookup, but now we can do it in Kibana with scripted fields in the new "[Painless](#)" language that also states : *The Painless syntax is similar to [Groovy](#).*

Scripted fields are found in the Management section:



The screenshot shows the Kibana Management interface. On the left is a sidebar with navigation links: Discover, Visualize, Dashboard, Tinnellon, Dev Tools, and Management (selected). The main content area is titled 'Management / Kibana / Indices' and shows the 'Index Patterns' section. The selected index pattern is 'syslog-*'. Below this, there's a list of fields (64), scripted fields (1), and source filters (0). The 'Scripted fields' section is expanded, showing a table with one field: 'cf-IPOwner'. The field is of type 'painless' and uses the script 'if (doc['SRC.keyword'].value == '10.0.0.185') { return 'Christopher' }'. The format is 'String' and the controls are visible.

So, my field in the first successful attempt looks like:

```
if (doc['SRC.keyword'].value == "10.0.0.185") {
  return "Christopher"
}
```

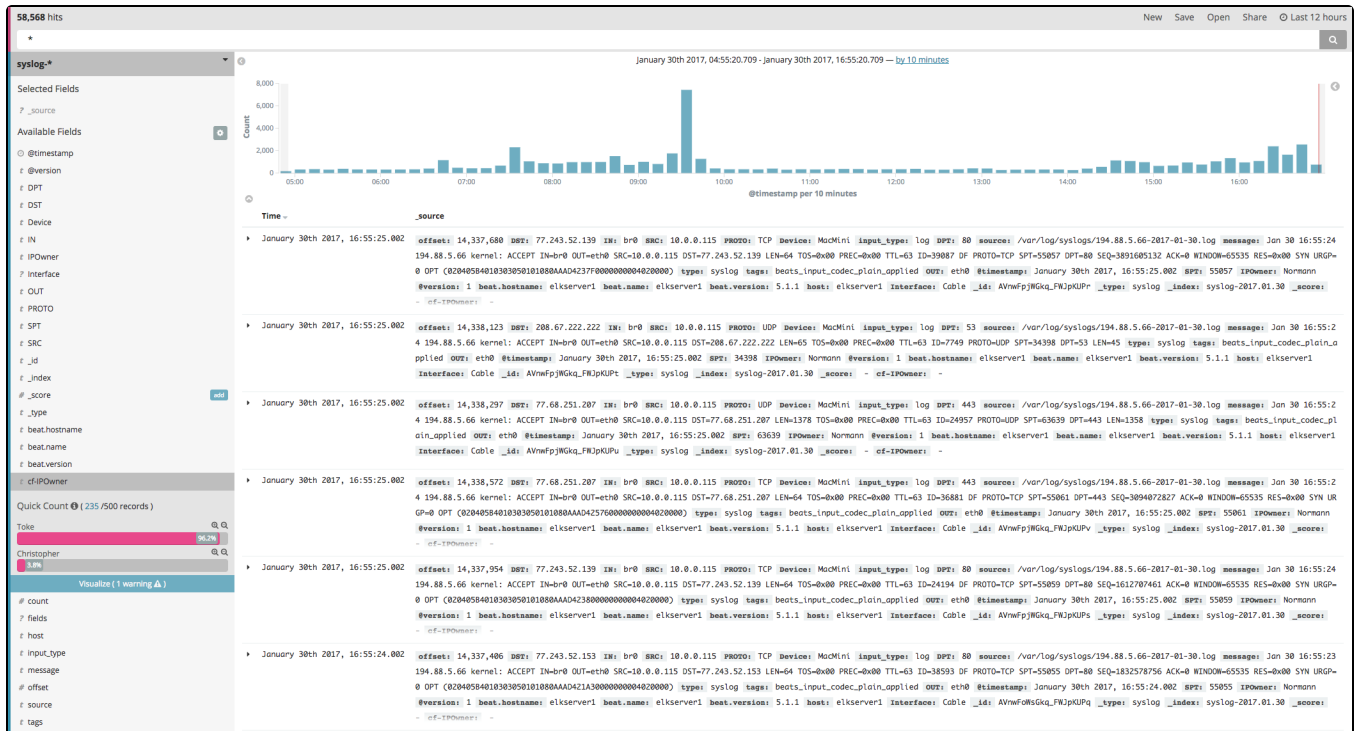
But, the docs also state: "Java's [control flow statements](#) are supported, with the exception of the `switch` statement.", so we can't use the switch, hence I will base it on if's:

```

if (doc['SRC.keyword'].value == "10.0.0.104") {
  return "Toke"
}
if (doc['SRC.keyword'].value == "10.0.0.185") {
  return "Christopher"
}
...
...
...
...
if (doc['SRC.keyword'].value == "10.0.0.196") {
  return "Toke"
}

```

And the success is eminent:



In Logstash I had the possibility to return 3 fields in one bulk (IPOwner, Device and Interface), but I assume that with Scripted fields I need to make a scripted field pr. field.