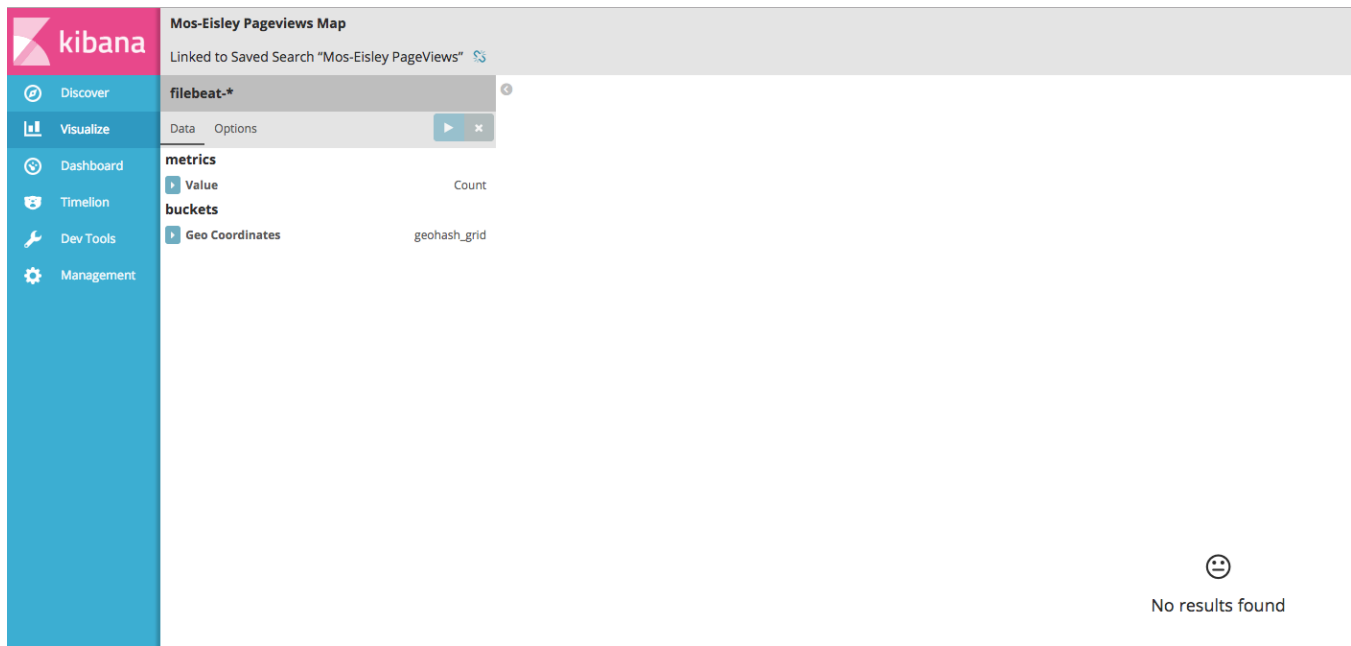


# Wrong GeoIP mapping

As nothing came on the "Tile Maps, all looking like:



I found out the mapping for the geo.location field was wrong (look here: <http://stackoverflow.com/questions/29661372/tile-map-geo-location-field-not-present-under-geohash-aggregation-in-kibana-4-0>)

```
root@elkserver1:/etc/logstash/conf.d# curl http://localhost:9200/filebeat-2016.12.28/_mapping/apache/field/geoip.location?pretty
{
  "filebeat-2016.12.28" : {
    "mappings" : {
      "apache" : {
        "geoip.location" : {
          "full_name" : "geoip.location",
          "mapping" : {
            "location" : {
              "type" : "float"
            }
          }
        }
      }
    }
  }
}
```

root@elkserver1:/etc/logstash/conf.d#

This should (according to the article not be:

```
"mapping" : {"location" : {"type" : "float"}}
```

but

```
"mapping":{"location":{"type":"geo_point"}}
```



This is for sure because I use "filebeat" as index for apache logs, and not "logstash" as is default (if logstash ships directly to Elasticsearch). The filebeat template in /etc/filebeat/filebeat.template.json has no geo/location mappings, and I am not sure its even used; as Elasticsearch just creates the index upon getting data in..

In /etc/logstash/conf.d/10-beats-input.conf I do have:

```
geoip {
  source => "clientip"
  target => "geoip"
  database => "/etc/logstash/GeoLite2-City.mmdb"
  add_field => [ "[geoip][coordinates]", "%{[geoip][longitude]}" ]
  add_field => [ "[geoip][coordinates]", "%{[geoip][latitude]}" ]
}
mutate {
  convert => [ "[geoip][coordinates]", "float" ]
}
```

but that seems to be "not enough" 😞 - possibly because I have no output template defined in /etc/logstash/conf.d/30-elasticsearch-output.conf

....so we need to change this:



TBD...

<http://www.pipebug.com/elasticsearch-logstash-kibana-4-mapping-4.html>



As a test, I changed the Logstash config, so the type=apache went into the Logstash index, and the Geomapping just worked...