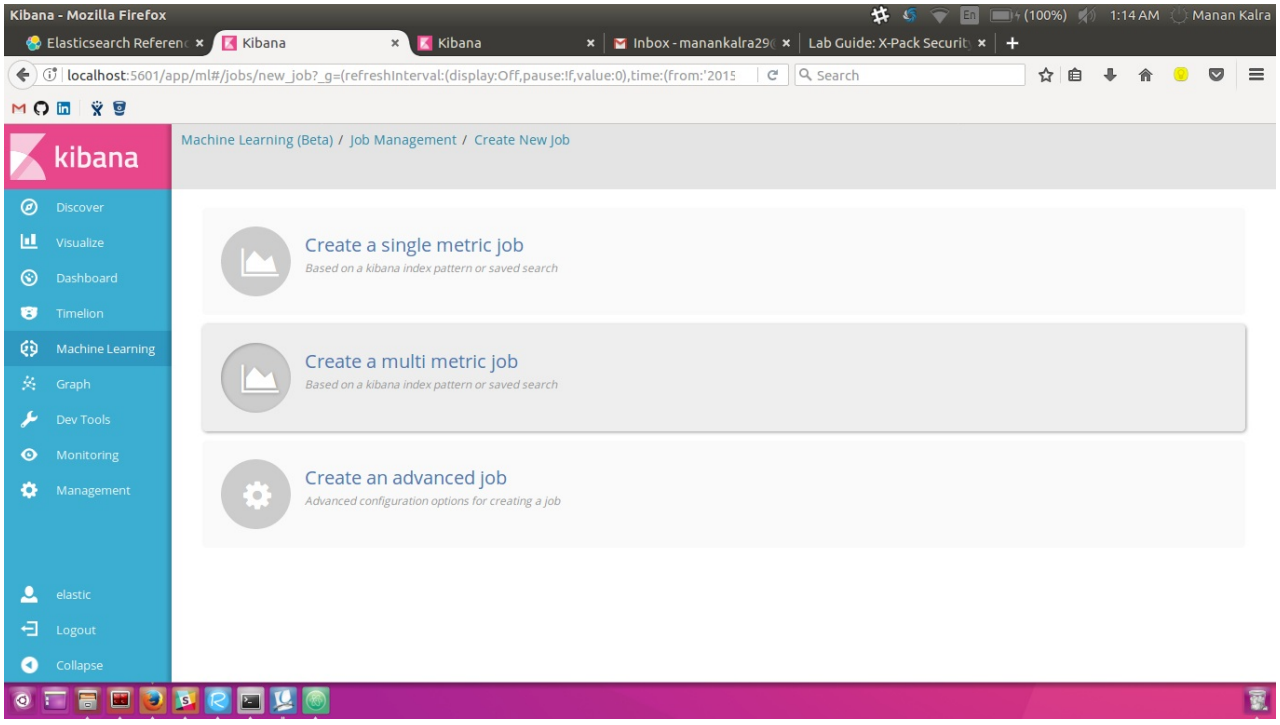
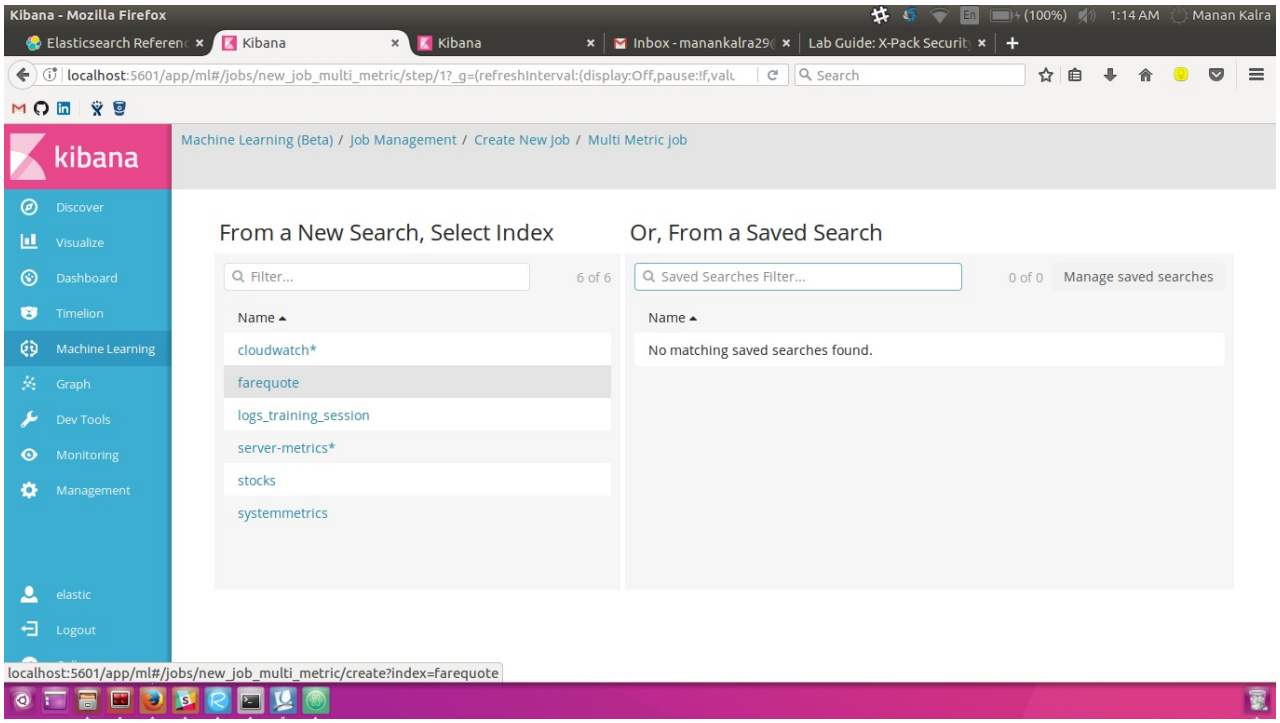
X-Pack: Machine Learning

Multi Metric Job

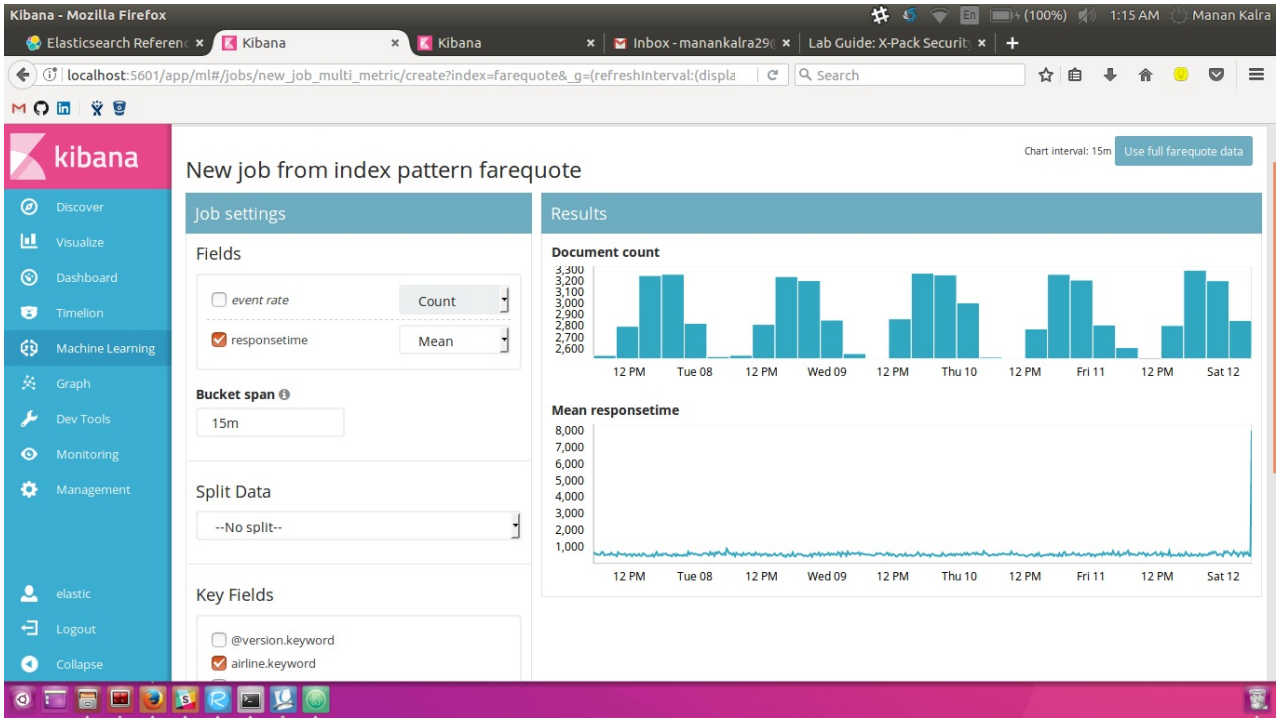
Farequote: Airline Data

- Start the Elasticsearch cluster.
- Start Kibana.
- Create an index via Logstash:
  - Redirect to the directory where Logstash is installed.
  - Copy the provided CSV and configuration file to this location.
  - Make changes in the configuration files, if required.
  - Execute `cat farequote.csv | ./bin/logstash/farequote.conf`.
- Create an index pattern in the Managemet tab of the Kibana console to view the loaded data.
- Click on the *Machine Learning* tab and then on *Create a new job*.
- Select *Multi Metric Job* and choose the *stocks* index.

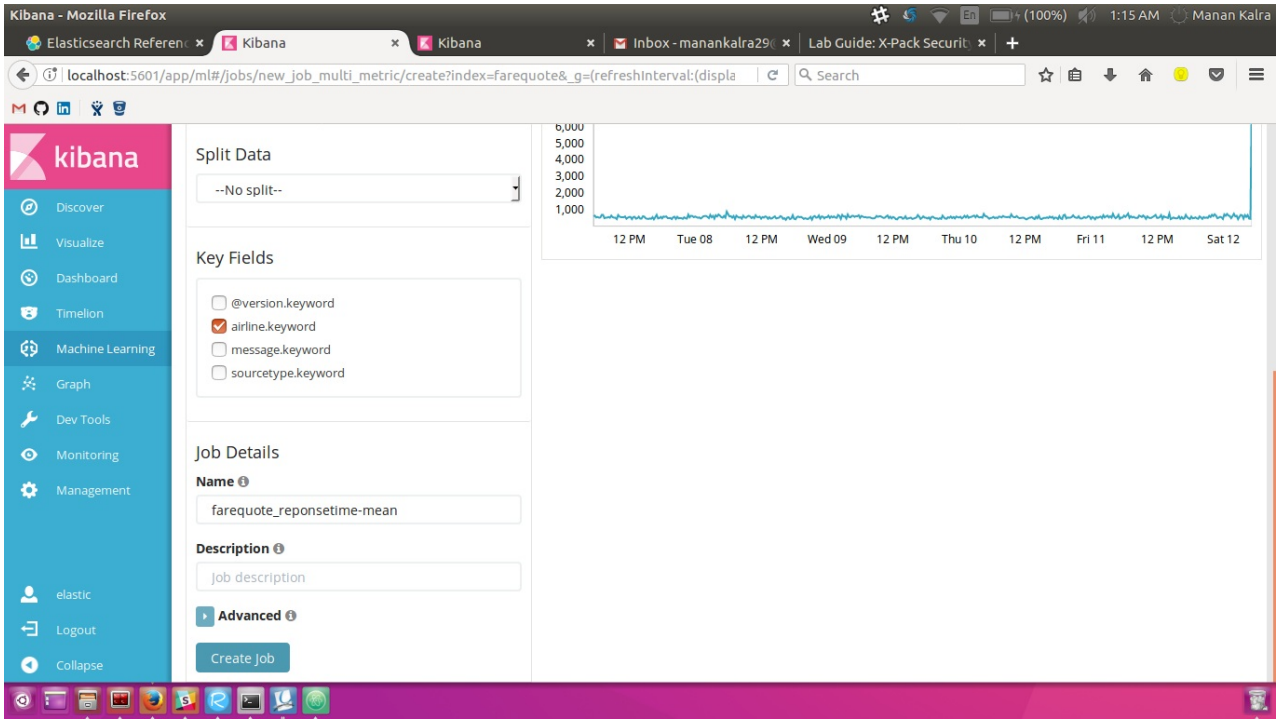




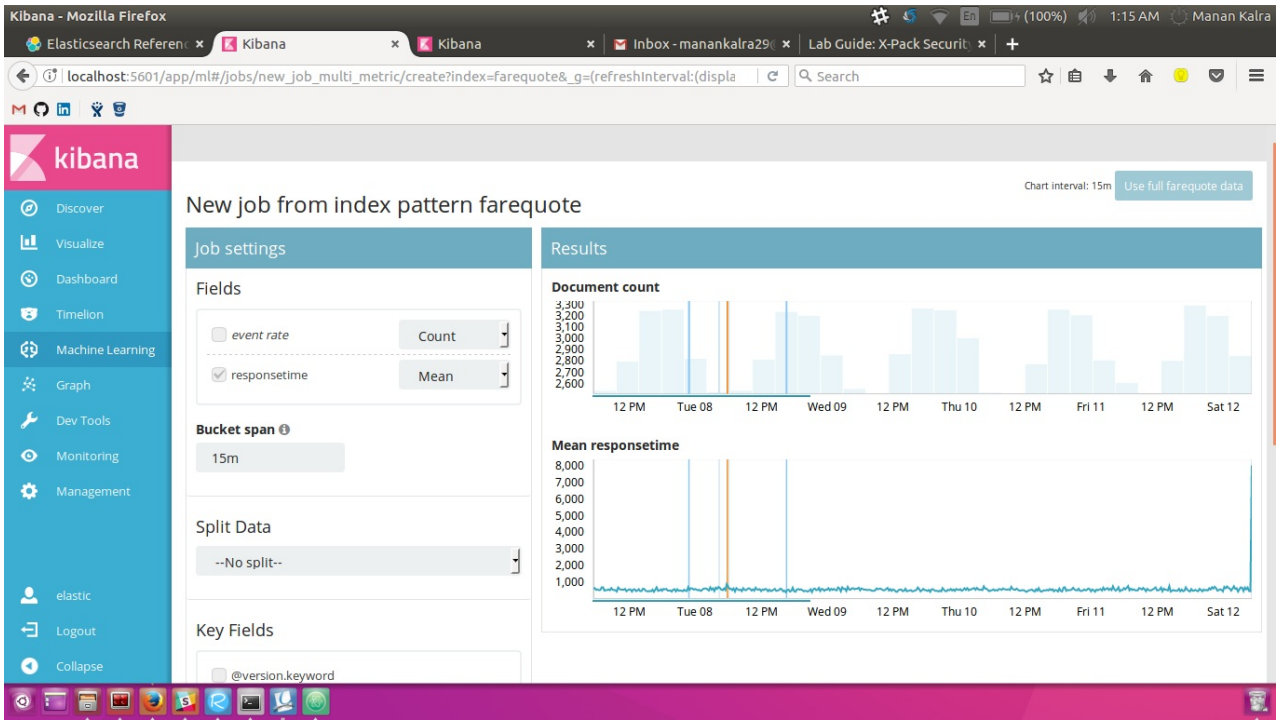
- Click on *Use full farequote data* as the data we are using is static.
- Select the field you want to analyze (responsetime) and a corresponding aggregation, for example: *Mean*.
- Use an appropiate bucket span, for example: 15m.



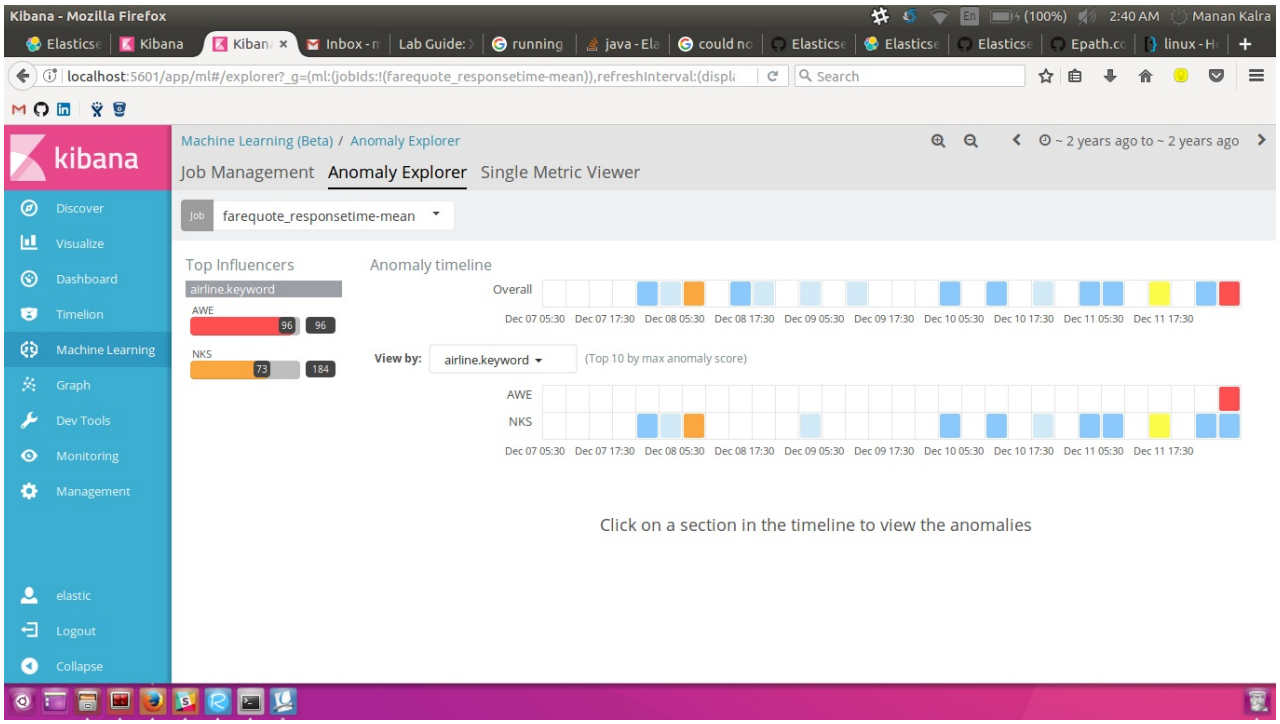
- Select Influencers, which you think can prove to be reponsible for an anomaly, for example: *airline.keyword*.
- Give your job a name. You can create a dedicated index for this job under the *Advanced* drop-down, if required.



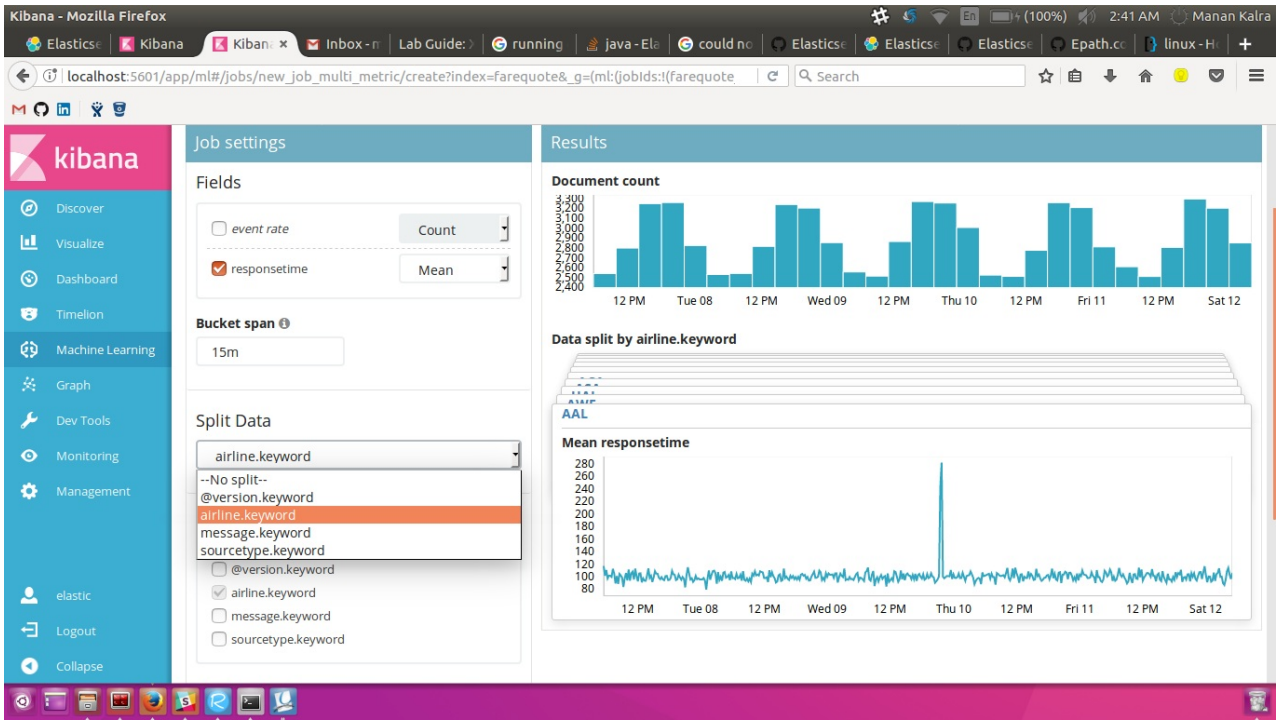
- Click on *Create Job*.

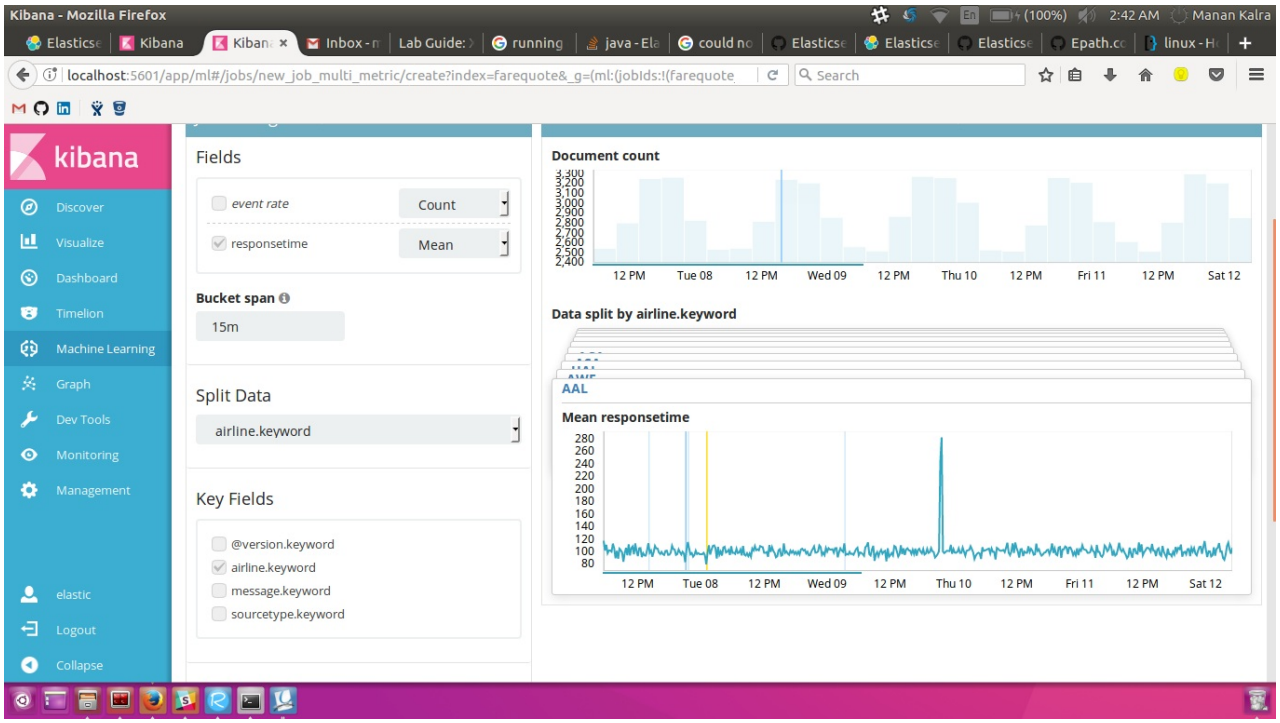


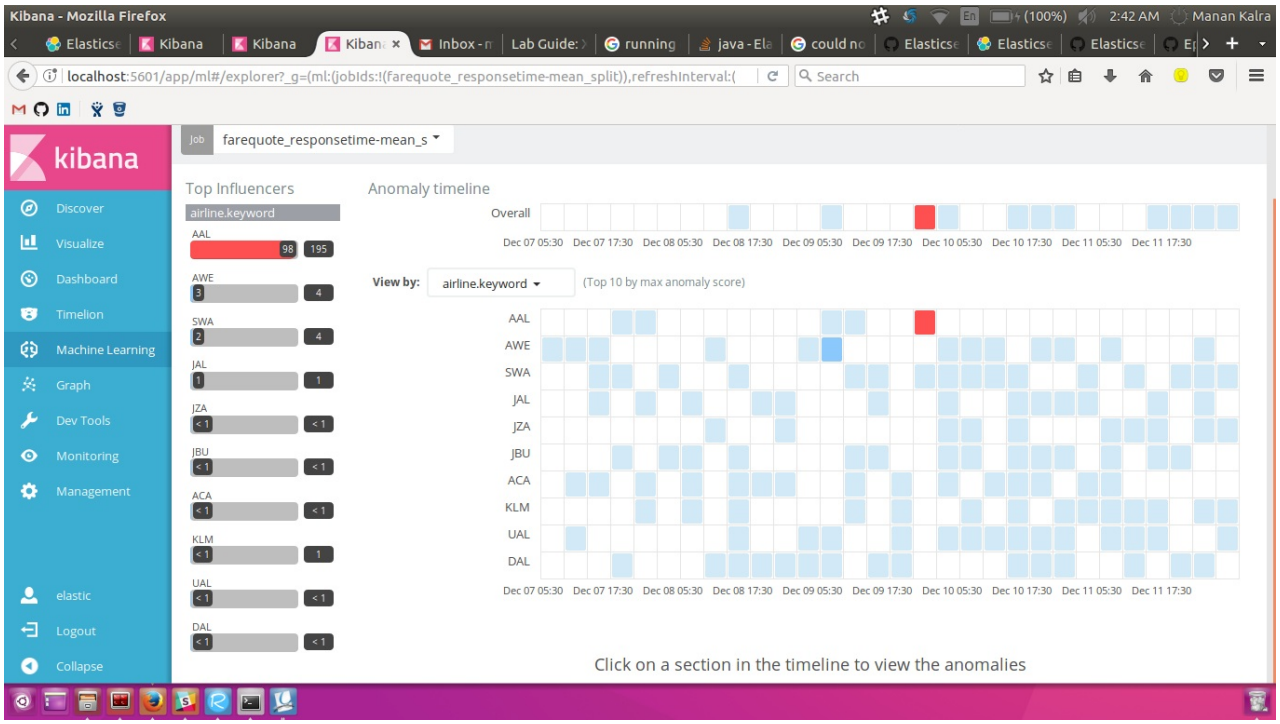
- To view the results of the analytical task, click on *View Results*.
- Allow pop-ups. Results will appear in the Anomaly Explorer tab. You can even click on a timeline ite to view more details.

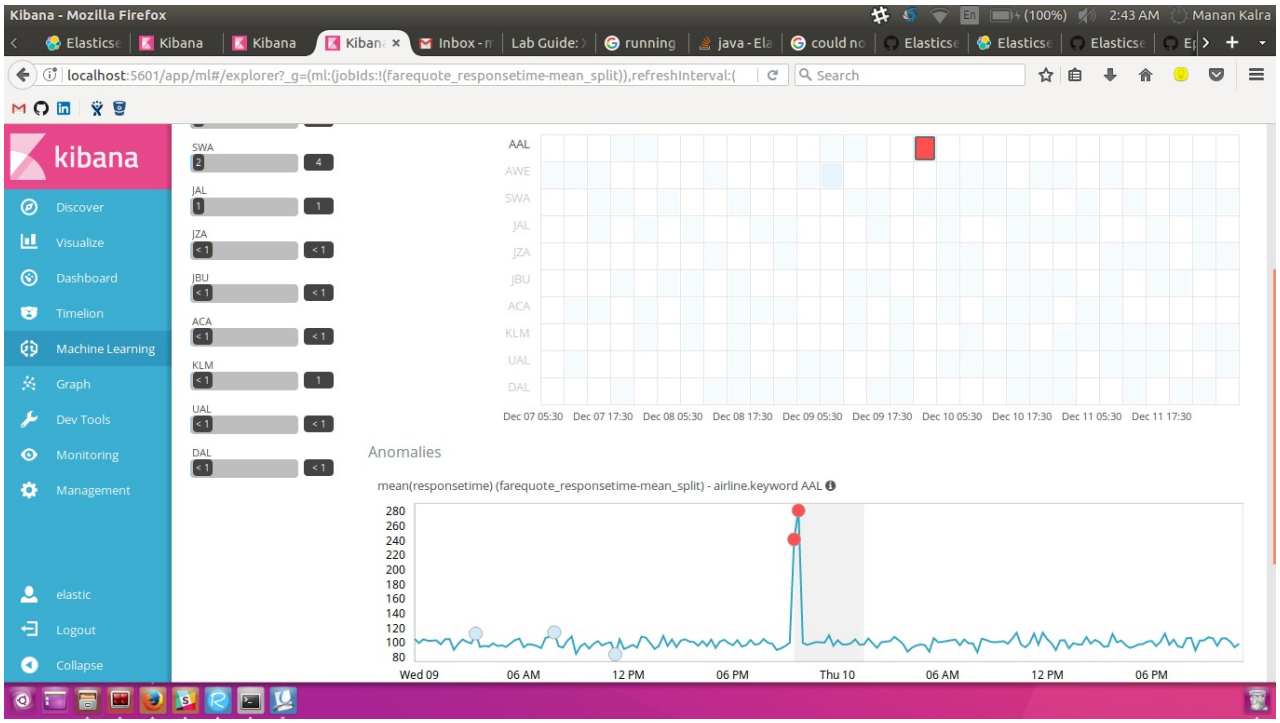


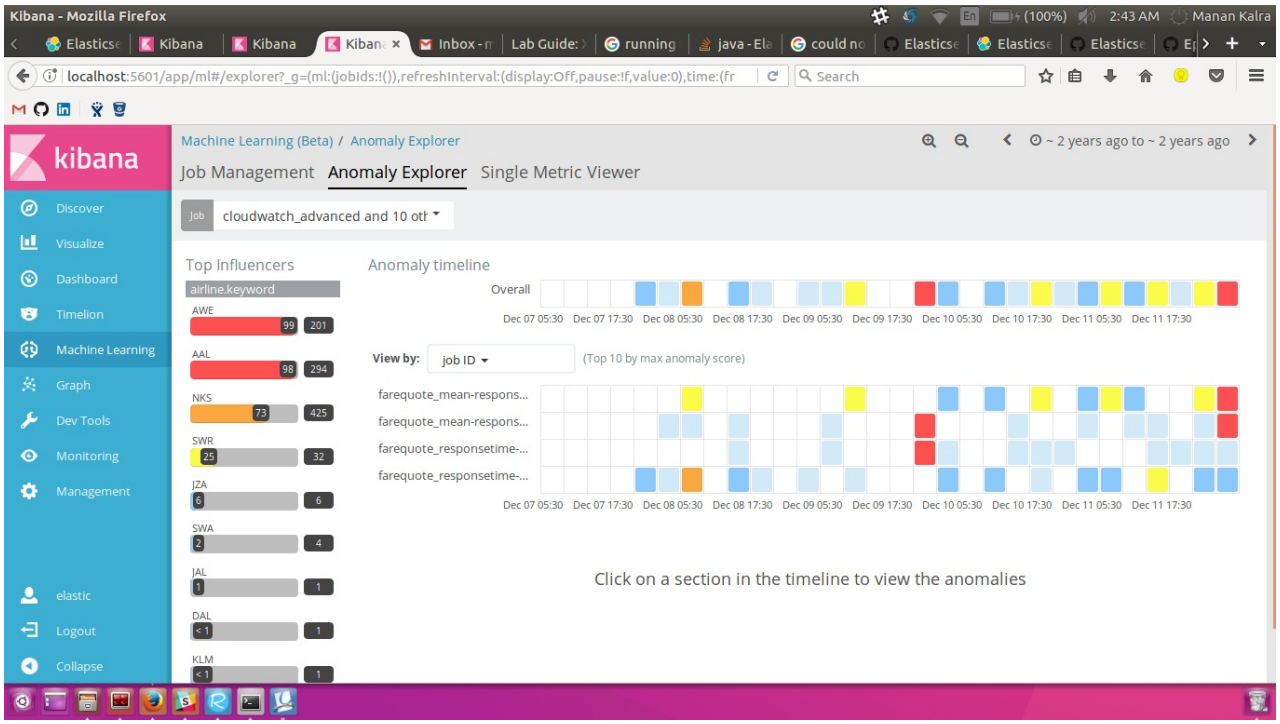
- The above listed method was a kind of individual analysis. Population analysis is also an option. This can be done by splitting the data on a particular field.




Kibana - Mozilla Firefox
localhost:5601/app/ml#/jobs/new_job_multi_metric/create?index=farequote&_g=(ml:(jobIds:!(farequote
kibana
Discover
Visualize
Dashboard
Timelion
Machine Learning
Graph
Dev Tools
Monitoring
Management
elastic
Logout
Collapse
Fields
event rate
Count
responsetime
Mean
Bucket span
15m
Split Data
airline.keyword
Key Fields
@version.keyword
airline.keyword
message.keyword
sourcetype.keyword
Document count
12 PM
Tue 08
Wed 09
Thu 10
Fri 11
Sat 12
Data split by airline.keyword
AAL
Mean responsetime


Kibana - Mozilla Firefox
localhost:5601/app/ml#/explorer?_g=(ml:(jobIds:!(farequote_responsetime-mean_split)),refreshInterval:(
kibana
Job
farequote_responsetime-mean_s
Top Influencers
airline.keyword
AAL
AWE
SWA
JAL
JZA
JBU
ACA
KLM
UAL
DAL
Anomaly timeline
Overall
View by:
airline.keyword
(Top 10 by max anomaly score)
Dec 07 05:30
Dec 07 17:30
Dec 08 05:30
Dec 08 17:30
Dec 09 05:30
Dec 09 17:30
Dec 10 05:30
Dec 10 17:30
Dec 11 05:30
Dec 11 17:30
Click on a section in the timeline to view the anomalies


Kibana - Mozilla Firefox
2:43 AM
Manan Kalra
localhost:5601/app/ml#/explorer?_g=(ml:(jobIds:!(farequote_responsetime-mean_split)),refreshInterval:(
Search
kibana
Discover
Visualize
Dashboard
Timelion
Machine Learning
Graph
Dev Tools
Monitoring
Management
elastic
Logout
Collapse
SWA
JAL
JZA
JBU
ACA
KLM
UAL
DAL
AAL
AWE
Dec 07 05:30
Dec 07 17:30
Dec 08 05:30
Dec 08 17:30
Dec 09 05:30
Dec 09 17:30
Dec 10 05:30
Dec 10 17:30
Dec 11 05:30
Dec 11 17:30
Anomalies
mean(responsetime) (farequote_responsetime-mean_split) - airline.keyword AAL
280
260
240
220
200
180
160
140
120
100
80
Wed 09
06 AM
12 PM
06 PM
Thu 10
06 AM
12 PM
06 PM


Kibana - Mozilla Firefox
2:43 AM
Manan Kalra
localhost:5601/app/ml#/explorer?_g=(ml:(jobIds:!()),refreshInterval:(display:Off,pause:!f,value:0),time:(fr
Search
kibana
Machine Learning (Beta) / Anomaly Explorer
~ 2 years ago to ~ 2 years ago
Job Management
Anomaly Explorer
Single Metric Viewer
Job
cloudwatch_advanced and 10 oth
Top Influencers
airline.keyword
AWE
99
201
AAL
98
294
NKS
73
425
SWR
25
32
JZA
6
6
SWA
2
4
JAL
1
1
DAL
<1
1
KLM
<1
1
Anomaly timeline
Overall
Dec 07 05:30
Dec 07 17:30
Dec 08 05:30
Dec 08 17:30
Dec 09 05:30
Dec 09 17:30
Dec 10 05:30
Dec 10 17:30
Dec 11 05:30
Dec 11 17:30
View by:
job ID
(Top 10 by max anomaly score)
farequote_mean-respons...
farequote_mean-respons...
farequote_responsetime-...
farequote_responsetime-...
Click on a section in the timeline to view the anomalies