The tool used to export data from elasticsearch

es2csv (A CLI tool for exporting data from elasticsearch)

First step:

The command to get source

pip install git+https://github.com/taraslayshchuk/es2csv.git

The command to install es2csv

pip install es2csv

Usage (you can mix all the options together):

run es2csv in query DSL syntax (-q defining query)

es2csv -r -q '{"query": {"match": {"host": "localhost"}}}' -o filename.csv

if you run long queries, you can save query in a json file as shown below (-r defining raw query)

es2csv -r -q @'file.json' -o filename.csv

on custom elasticsearch host or using secure elasticsearch with nginx (-u defining url)

es2csv -u my.cool.host.com:9200 -q 'host: localhost' -o filename.csv

with authorization (-a defining authorization)

es2csv -a login:password -u http://my.cool.host.com:6666/es/ -q 'host: localhost' -o filename.csv

specifying index (-i defining index)

es2csv -i logstash-2015-07-07 -q 'host: localhost' -o filename.csv

More indexes

es2csv -i logstash-2015-07-07 logstash-2015-08-08 -q 'host: localhost' -o filename.csv

Collecting all data on all indices

es2csv -i \_all -q '\*' -o filename.csv

selecting all field

es2csv -f \_all -q 'host: localhost' -o filename.csv

selecting some fields based upon request

es2csv -f host status date -q 'host: localhost' -o filename.csv

selecting nested fields

es2csv -f comments.comment comments.date comments.name -q '\*' -i twitter -o filename.csv

(or you could using es2csv -h to check all other options in detail that you might need)