

Windows 10 (ELK 스택) (Elastic Stack)에 ElasticSearch Logstash 및 Kibana 설치

https://www.youtube.com/watch?v=8iXZTS7f_hY

이 유튜브를 보고 똑같이 따라하면 Logstash 설치가 가능하다!

개인적으로 너무 친절하고 자세한 사이트이다.

<https://www.elastic.co/kr/downloads/logstash>

elasticsearch Logstash 공식사이트이다.


다운로드 파일와 `logstash -f logstash.conf` 코드가 적혀있다.

- 웬만하면 logstash파일은 D드라이브 혹은 C드라이브에 압축풀기를 하는 것이 좋다.
(파일명이 지나치게 길어서 압축풀기가 안되는 경우도 있다.)
- logstash.conf 코드는 반드시 D:\logstash-7.16.0-windows-x86_64\logstash-7.16.0\bin 밑에 있을 필요가 없다. 어느 곳에 있어도 전혀 상관없다.
- 파일명을 "kmh.conf"라고 설정했으면 `logstash -f kmh.conf` 코드 입력을 한다.
- Input / filter / output 으로 구성되어 있다.

```
logstash.conf X
D: > logstash-7.16.0-windows-x86_64 > logstash-7.16.0 > bin > logstash.conf
1  input {
2    |   stdin {}
3  }
4
5  output {
6    |   elasticsearch {
7    |     |   hosts => ["localhost:9200"]
8    |     |   index => "indexforlogstash"
9    |     |   }
10 }
```

에서 `stdin {}` 는 `cmd`창에 직접 값을 집어넣는다는 이야기이다.

- 한국어를 넣으면 오류가 생긴다.

 관리자: 명령 프롬프트 - `logstash -f logstash.conf`

```
:ecs_compatibility=>:disabled}
[2021-12-13T14:49:00,598][INFO ][logstash.javapipe
kers"=>8, "pipeline.batch.size"=>125, "pipeline.bat
:/logstash-7.16.0-windows-x86_64/logstash-7.16.0/b
[2021-12-13T14:49:01,232][INFO ][logstash.javapipe
=>0,63}
WARNING: An illegal reflective access operation has
WARNING: Illegal reflective access by com.jrubystd
-x86_64/logstash-7.16.0/vendor/bundle/jruby/2.5.0/g
n_channel.jar) to field java.io.FilterInputStream.i
WARNING: Please consider reporting this to the main
WARNING: Use --illegal-access=warn to enable warnin
WARNING: All illegal access operations will be deni
[2021-12-13T14:49:01,292][INFO ][logstash.javapipe
The stdin plugin is now waiting for input:
[2021-12-13T14:49:01,328][INFO ][logstash.agent
non_running_pipelines=>[]}
배가고픕니다., 그래서 꿀을 먹었습니다., 역시나 맛있군
[2021-12-13T15:24:20,172][WARN ][logstash.codecs.l
d40a1c26a8] Received an event that has a different
C7퀸 求D9., B1u05F7A1BCAD B1DB
B8C0C0儼BABFxE4.r", :expected_c
I am hungry, maybe you feel like that
Wow, Minhyoung is the greastest data engineer!
```

```
14 GET indexforlogstash/_search|
```

```
{
  "timestamp" : "2021-12-13T06:24:20.184Z",
  "host" : "DESKTOP-G9DVJ1H",
  "@version" : "1"
},
{
  "_index" : "indexforlogstash",
  "_type" : "_doc",
  "_id" : "H7d3sn0B_FKBD1GTU7IX",
  "_score" : 1.0,
  "_source" : {
    "message" : """"I am hungry, maybe you feel like that""""
  }
},
{
  "timestamp" : "2021-12-13T06:25:04.150Z",
  "host" : "DESKTOP-G9DVJ1H",
  "@version" : "1"
},
{
  "_index" : "indexforlogstash",
  "_type" : "_doc",
  "_id" : "ILe1sn0B_FKBD1GTEbIh",
  "_score" : 1.0,
  "_source" : {
    "message" : """"Wow, Minhyoung is the greastest data engineer!""""
  }
},
{
  "timestamp" : "2021-12-13T07:11:45.301Z",
  "host" : "DESKTOP-G9DVJ1H",
  "@version" : "1"
},
{
  "_index" : "indexforlogstash",
  "_type" : "_doc",
  "_id" : "H7d3sn0B_FKBD1GTU7IX",
  "_score" : 1.0,
  "_source" : {
    "message" : """"I am hungry, maybe you feel like that""""
  }
}
]
```

원하는 데로 데이터가 이쁘게 들어갔다.

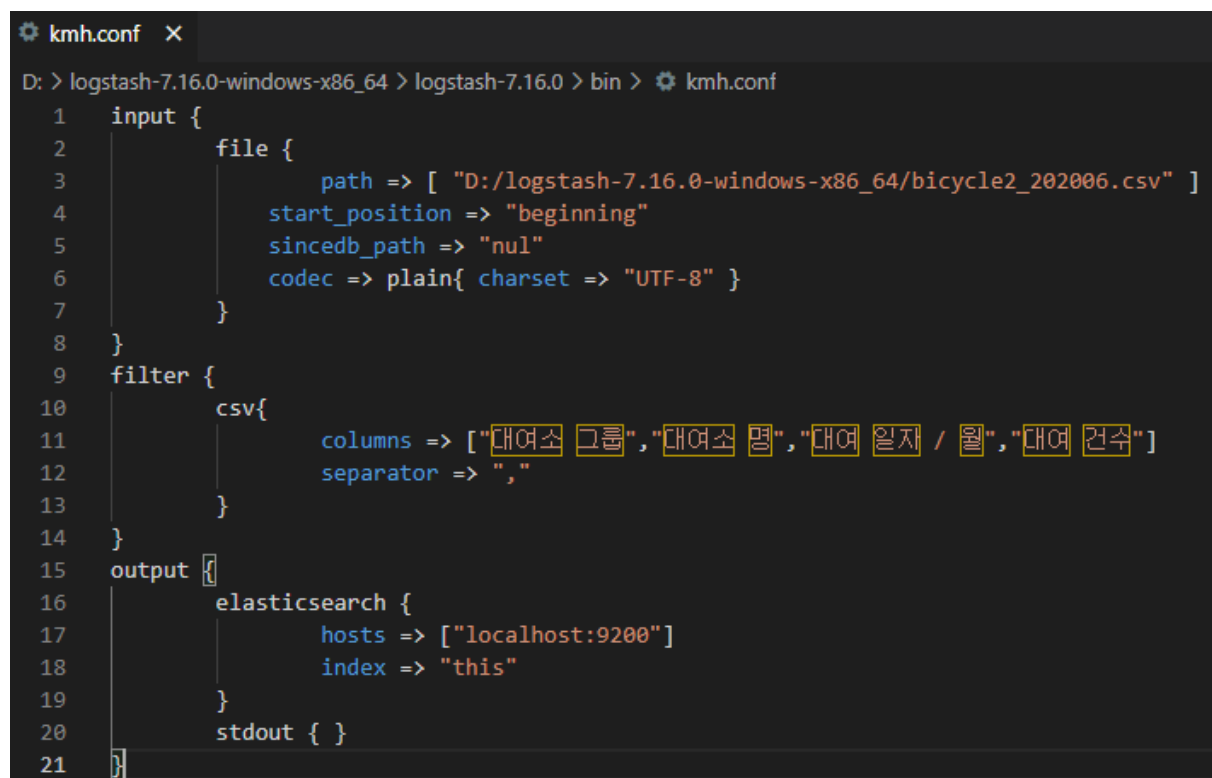
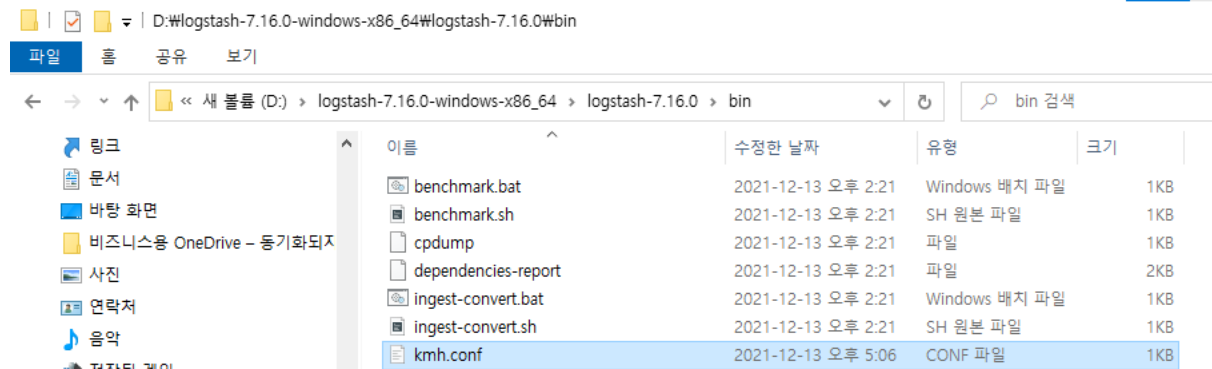
```
[2021-12-13T16:30:27,223][WARN ][logstash.runner] SIGINT received. Shutting down.
[2021-12-13T16:30:27,464][INFO ][logstash.javapipeline] [main] Pipeline terminated {"pipeline.id"=>"main"}
[2021-12-13T16:30:28,357][INFO ][logstash.runner] Logstash shut down.
일괄 작업을 끝내시겠습니까 (Y/N)? y
```

Ctrl+c를 누르고 y를 누르면 작업이 끝이 난다.

이번에는 csv파일을 집어넣어보자.

<https://peanut159357.tistory.com/27>

위의 사이트를 참고하여 엑셀파일을 다운받아보자.



(참고하면 좋은 사이트 : <https://horae.tistory.com/entry/logstash-with-python>)

관리자: 명령 프롬프트 - logstash -f kmh.conf

```
"대여소 그룹" => "종로구",
"대여 건수" => "37",
"host" => "DESKTOP-G9DVJ1H",
"대여소 명" => "3418.창신역2번 출구",
"대여 일자 / 월" => "202006",
"@version" => "1"

"message" => "종로구,3419.국립어린이과학관,202006,145₩r",
"@timestamp" => 2021-12-13T08:07:16.874Z,
"path" => "D:/logstash-7.16.0-windows-x86_64/bicycle2_202006.csv",
"대여소 그룹" => "종로구",
"대여 건수" => "145",
"host" => "DESKTOP-G9DVJ1H",
"대여소 명" => "3419.국립어린이과학관",
"대여 일자 / 월" => "202006",
"@version" => "1"

"message" => "종로구,342.대학로 마로니에공원,202006,2557₩r",
"@timestamp" => 2021-12-13T08:07:16.874Z,
"path" => "D:/logstash-7.16.0-windows-x86_64/bicycle2_202006.csv",
"대여소 그룹" => "종로구",
"대여 건수" => "2557",
"host" => "DESKTOP-G9DVJ1H",
"대여소 명" => "342.대학로 마로니에공원",
"대여 일자 / 월" => "202006",
"@version" => "1"
```

8 GET this/_search

```
16   "max_score" : 1.0,
17   "hits" : [
18     {
19       "_index" : "this",
20       "_type" : "_doc",
21       "_id" : "ObfUsn0B_FKBD1GT7bMv",
22       "_score" : 1.0,
23       "_source" : {
24         "message" : ""강남구,2306.
          압구정역 2번 출구 옆,202006
          ,1310
25       """,
26       "@timestamp" : "2021-12-13T08:07
          :16.442Z",
27       "path" : "D:/logstash-7.16.0
          -windows-x86_64
          /bicycle2_202006.csv",
28       "대여소 그룹" : "강남구",
29       "대여 건수" : "1310",
30       "host" : "DESKTOP-G9DVJ1H",
31       "대여소 명" : "2306. 압구정역
          2번 출구 옆",
32       "대여 일자 / 월" : "202006",
33       "@version" : "1"
34     },
35     {
36       "_index" : "this",
37       "_type" : "_doc",
38       "_id" : "KbfUsn0B_FKBD1GT7bIu",
39       "_score" : 1.0,
40       "_source" : {
41         "message" : ""강남구,2312.
          청담역 13번 출구 앞,202006,673
42       """,
43       "@timestamp" : "2021-12-13T08:07
          :16.442Z",
44       "path" : "D:/logstash-7.16.0
          -windows-x86_64
          /bicycle2_202006.csv",
45       "대여소 그룹" : "강남구",
46       "대여 건수" : "673",
47       "host" : "DESKTOP-G9DVJ1H",
48       "대여소 명" : "2312. 청담역
          13번 출구 앞",
49       "대여 일자 / 월" : "202006",
50       "@version" : "1"
51     }
52   ]
53 }
```