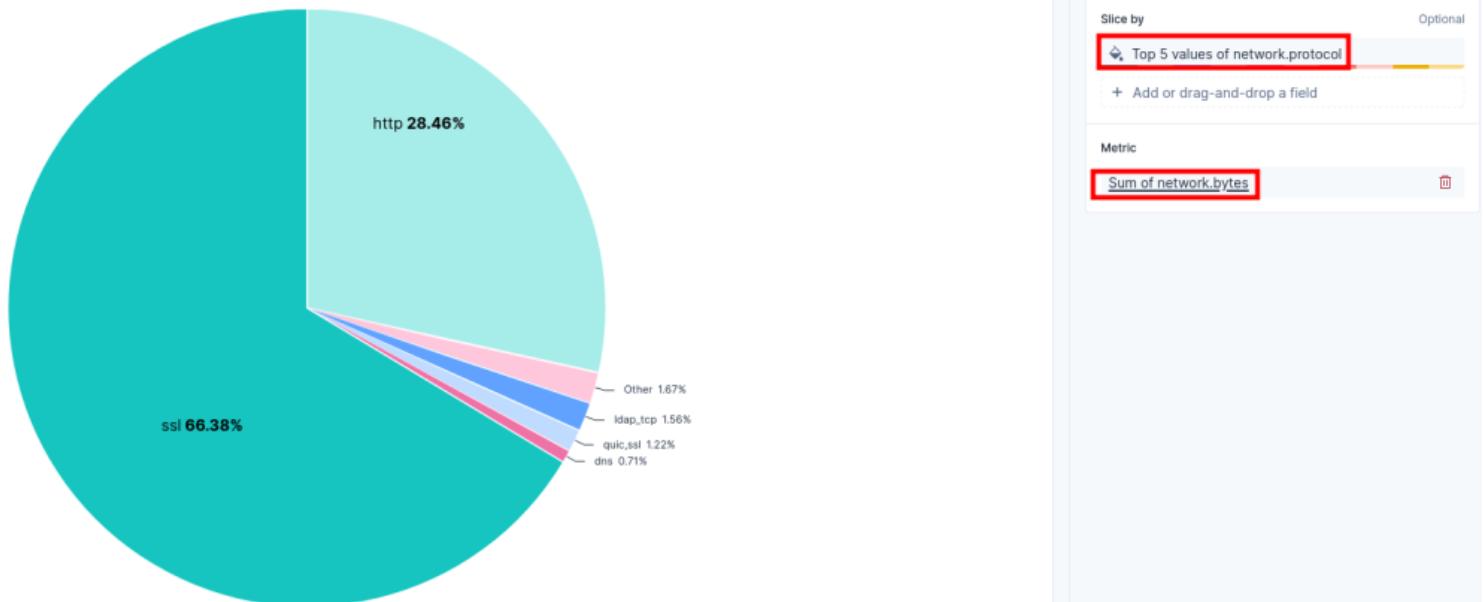
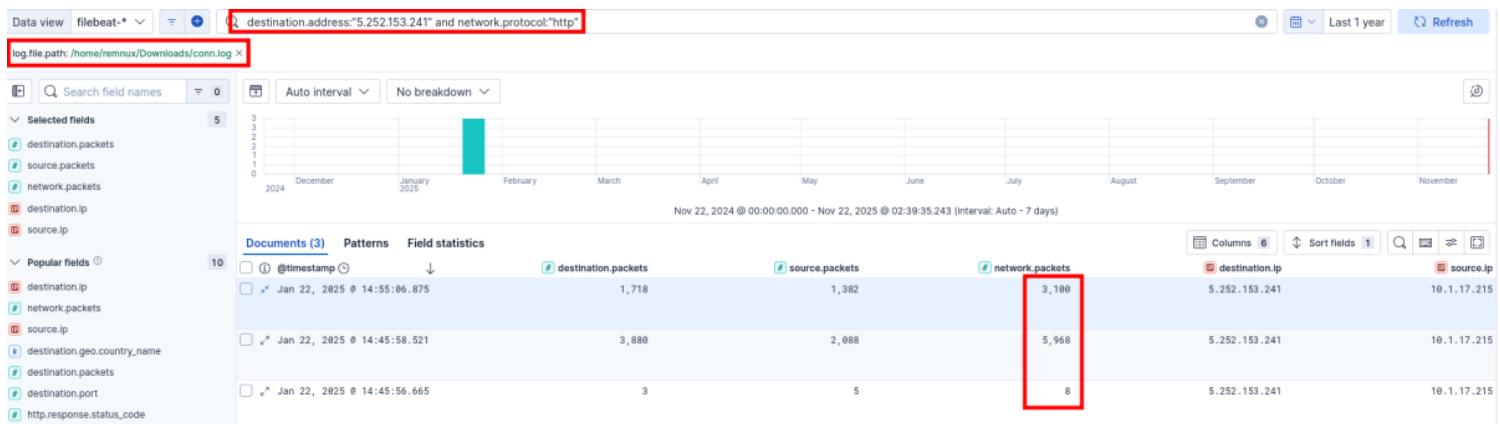


1. 가장 많은 양의 데이터를 주고 받은 프로토콜을 찾고 싶을 때 사용하는 로그는?



=> conn.log

2. conn.log를 사용해서 10[.]1[.]17[.]215와 5[.]252[.]153[.]241가 주고 받은 패킷의 수를 구하시오



or

destination.address:"5.252.153.241" and network.protocol:"http"

Top 5 values of source.address

10.1.17.215

Sum of network.packets
9,076

Rows
Top 5 values of source.address
+ Add or drag-and-drop a field

Metrics
Sum of network.packets

9076

3. http.log를 사용해서 10[.]1[.]17[.]215가 5[.]252[.]153[.]241에 보낸 GET 요청의 수와 그 중 응답 코드가 200인 이벤트의 수를 구하시오

Data view filebeat-* ▾

log.file.path: /home/remnux/Downloads/http.log ×

Selected fields: http.response.status_code

Popular fields: destination.ip, source.ip, log.file.path

Auto interval: No breakdown

Documents (594) Patterns Field statistics

200 10 (1.68%)

4. 가장 많은 수의 파일을 주고 받은 세션의 source ip, destination ip, 요청한 URL을 구하시오 (힌트: file.log, http.log를 둘 다 사용)

log.file.path: /home/remnux/Downloads/file.log ×

Selected fields: zeek.files.uid

Available fields: zeek.files.uid

Count of records: 499
94

Top 5 values of zeek.files.uid
CE1MZS3mkZpcVcOBx3
Clg9b54m1wIAxNpKJS

Rows
Top 5 values of zeek.files.uid

file.log

2/3

Data view filebeat-* log_file.path:/home/remnux/Downloads/http.log

Q URL Selected fields url.original Available fields url.anomalous

Top 5 values of url.original

Value	Count of records
/1517096937	496
/1517096937?k=script:RunRH, status:OK, message:PS process started	3

Table filebeat-* Rows Top 5 values of url.original

http.log