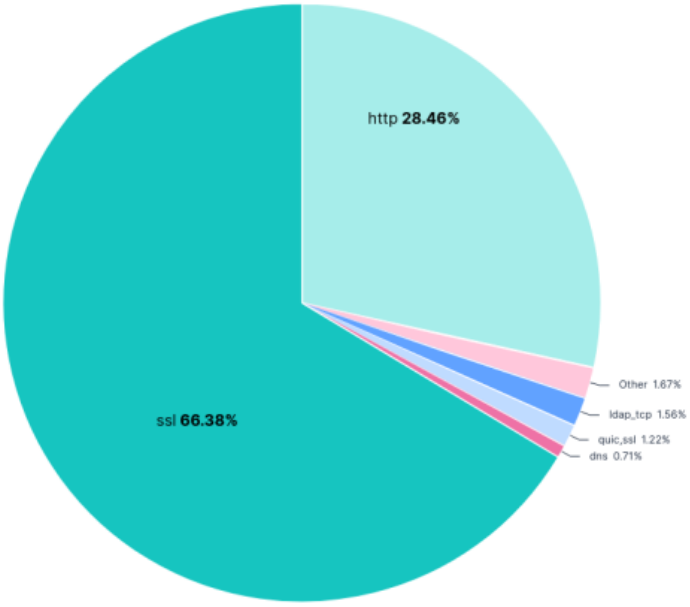
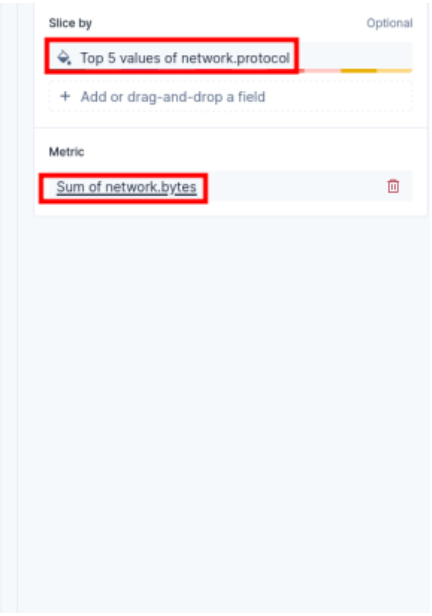
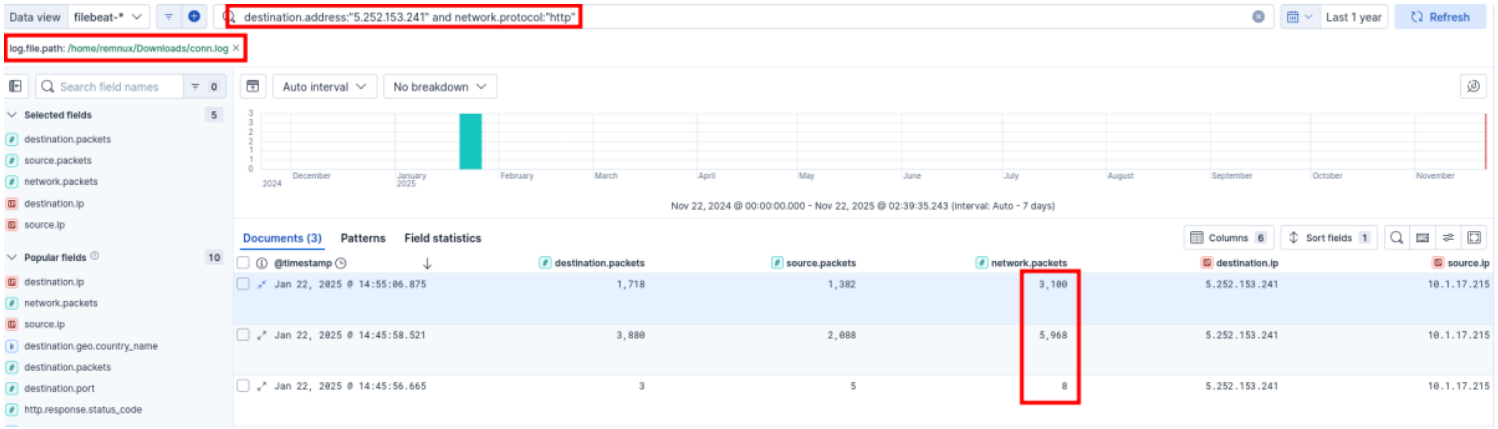
1. 가장 많은 양의 데이터를 주고 받은 프로토콜을 찾고 싶을 때 사용하는 로그는?



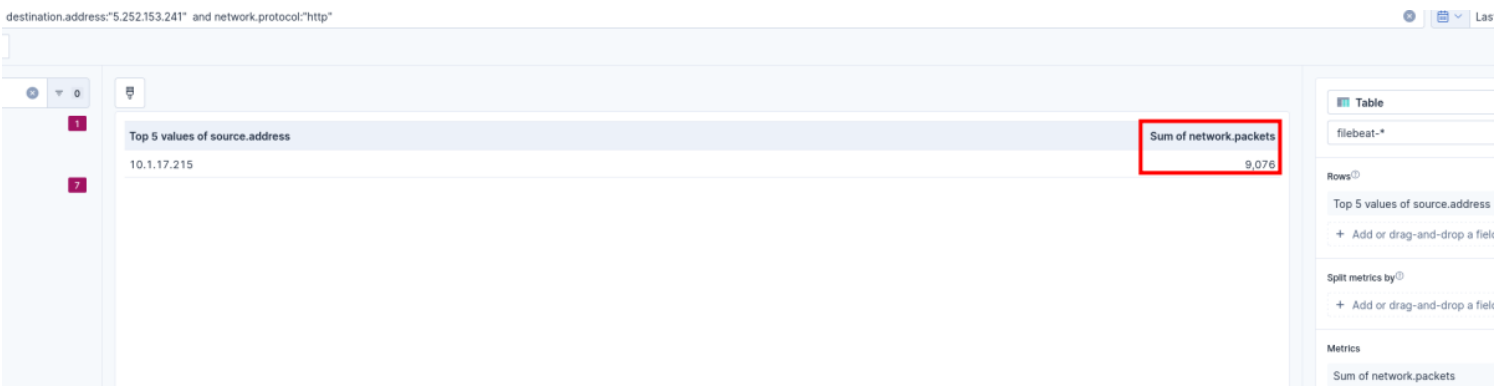


=> conn.log

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

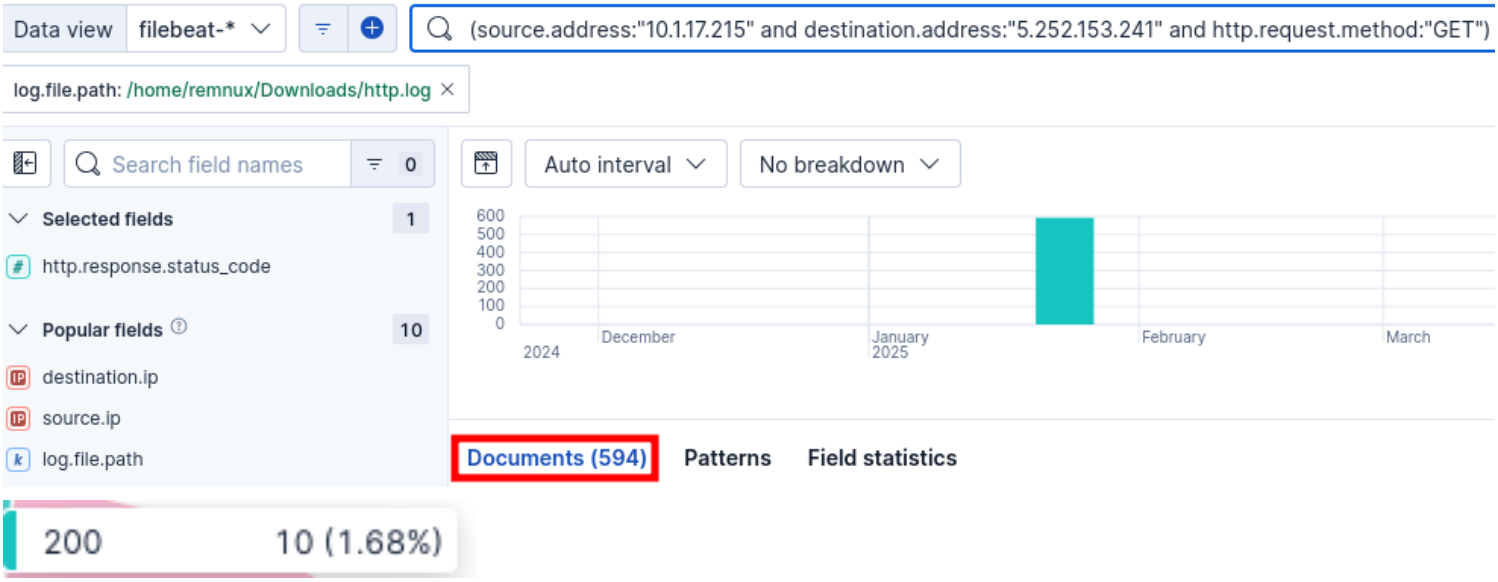


or

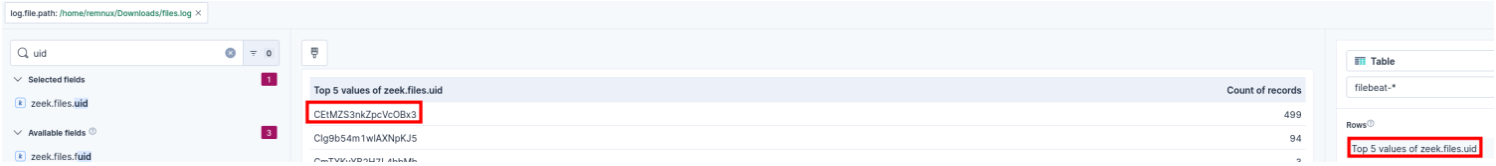


9076

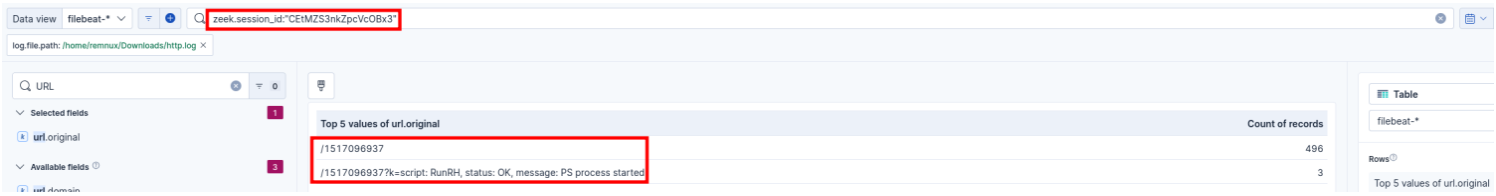
3. http.log를 사용해서 10[.]1[.]17[.]215가 5[.]252[.]153[.]241에 보낸 GET 요청의 수와 그 중 응답 코드가 200인 이벤트의 수를 구하시오



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



file.log


Data view
filebeat-*
zeek.session_id:"CEtMZS3nkZpcVcOBx3"
log.file.path: /home/remnux/Downloads/http.log
URL
Selected fields
1
url.original
Available fields
3
Top 5 values of url.original
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