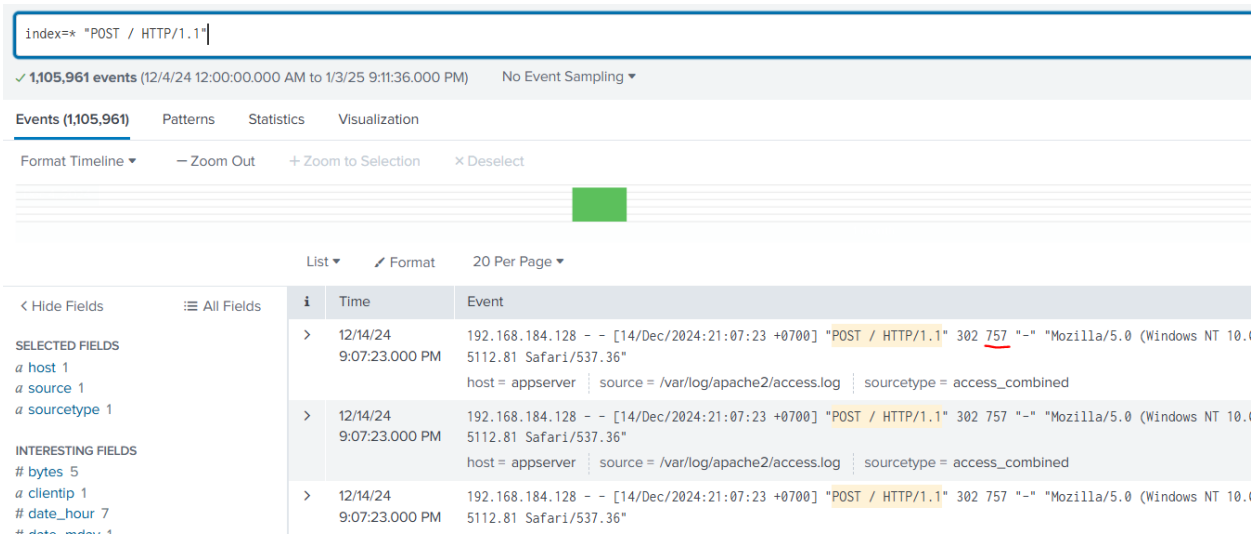
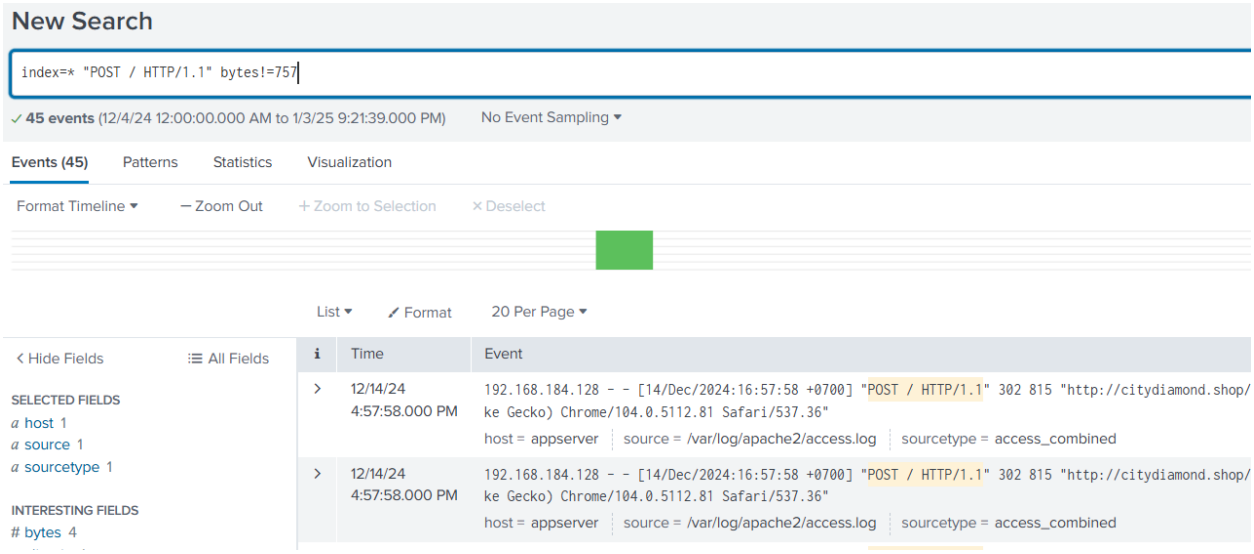
Tier 3.2

Hướng tiếp cận của nhóm tập trung vào phát hiện các event brute-force có vẻ bất thường trong các response trả về.

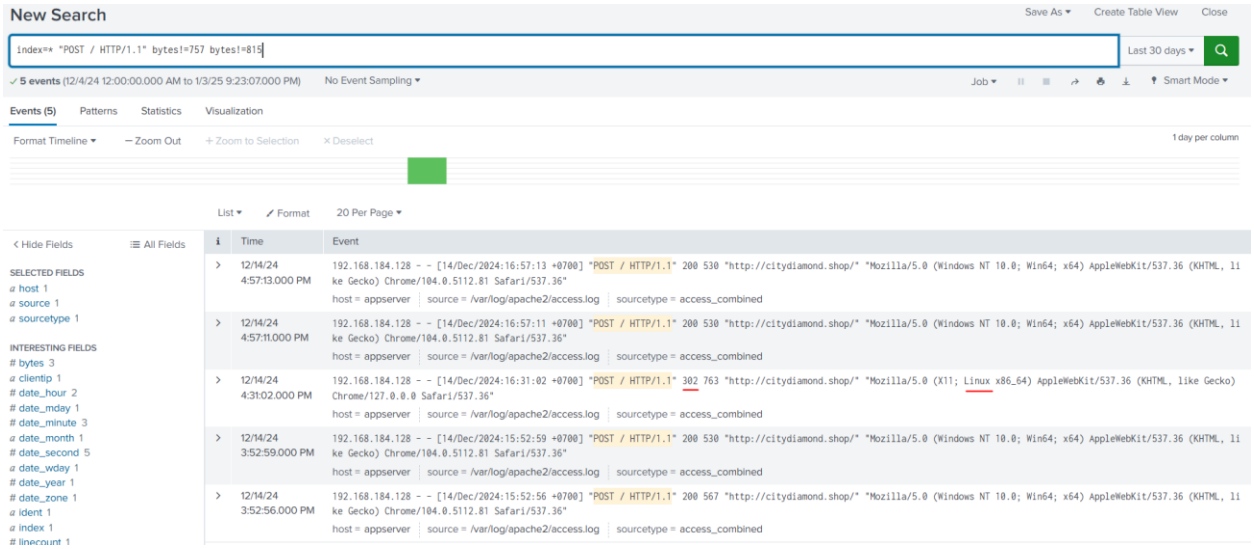
Sau khi query các event thực hiện brute-force bằng các qua giao thức POST đến /:



Nhận thấy rằng hầu hết các event đều có trường bytes (kích thước response) là 757. Tiến hành lọc trường này:



Lần này ta lại thấy hàng loạt các event có bytes 815. Lọc các event này:



Lúc này ta chỉ cần tập trung chỉ yếu vào 5 event trên. Đặc biệt ở event thứ 3 có mã trả về khác với các event còn lại. Ngoài ra để dễ tìm kiếm bên trong file pcap ta nhận thấy chỉ có request này có user-agent Linux.

Sau khi tra cứu chỉ có duy nhất 1 lệnh POST có user-agent có “Linux”:

No.	Time	Source	Destination	Protocol	Length	Value	User-Agent	Info
4948662	3718.145	192.168.184.128	192.168.184.132	HTTP	741	adm,capricorn2,	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/5	POST / HTTP/1.1 (application/x-www-form-urlencoded)

Có username và password tiến hành hash bằng MD5: