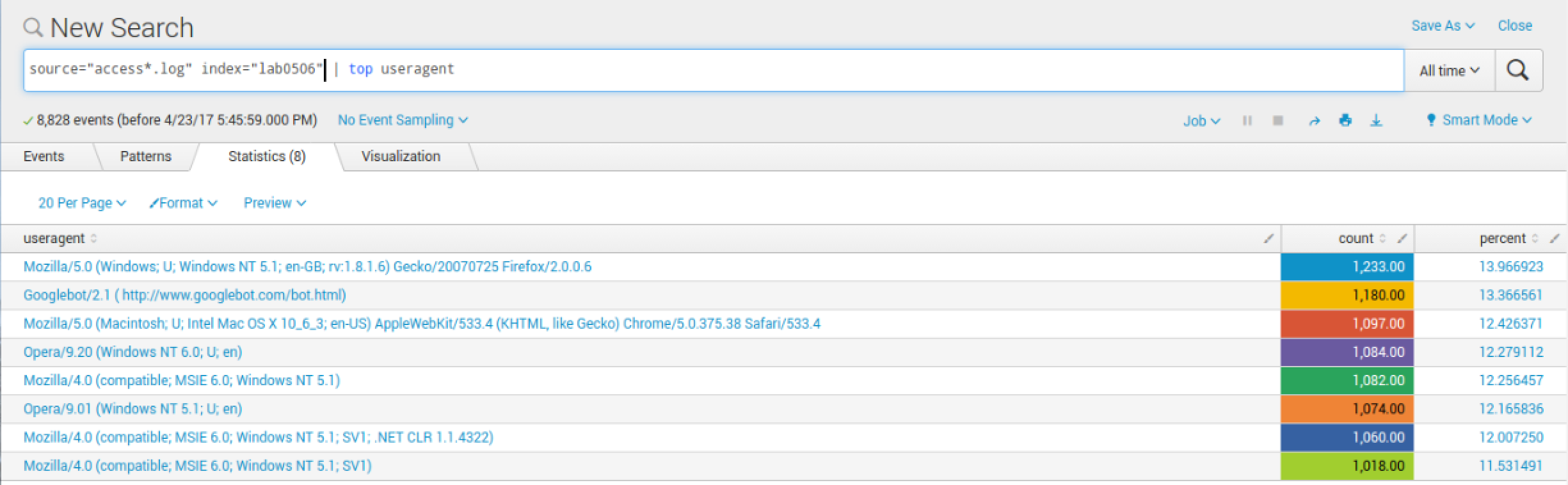
# Introduction

1. Perform all the searches in your text from pages 44 – 50
2. Submit a screen shot of your search results WITH the query statement you used to produce the results.

## Searches

### Top Browsers

source=”access\*.log” index=”lab0506” sourcetype=”access\_combined\_wcookie” | top useragent



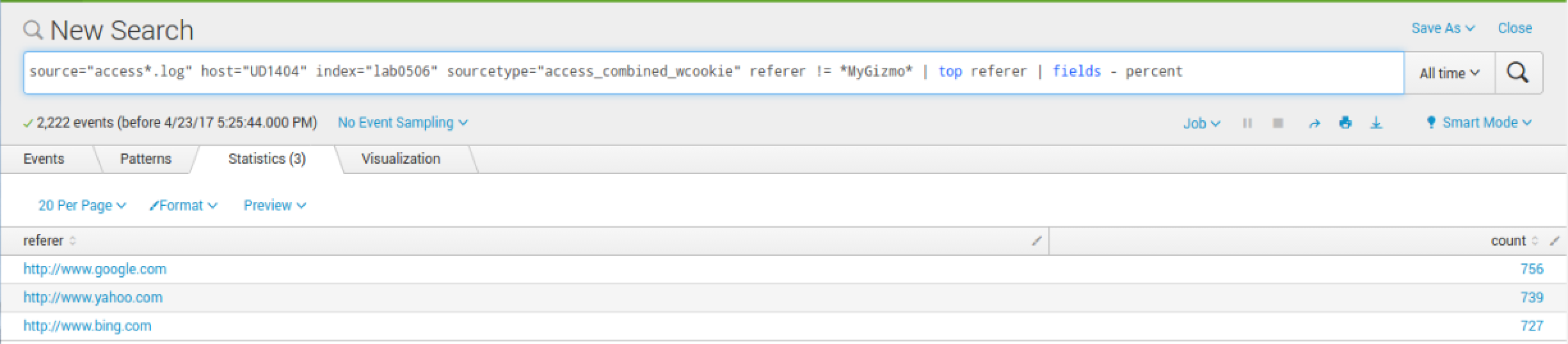
### Top 5 IP Addresses

source=”access\*.log” host=”UD1404” index=”lab0506” sourcetype=”access\_combined\_wcookie” | limit=5 clientip

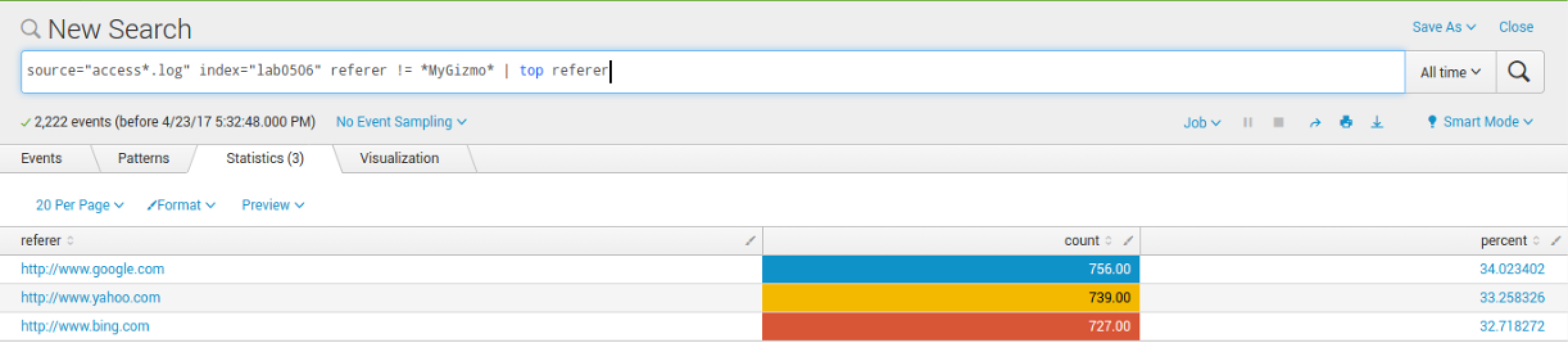
### 

### Top Referral Web Sites

source=”access\*.log” index=”lab0506” referer != \*MyGizmo\* | top referer | fields – percent



source=”access\*.log” index=”lab0506” referer != \*MyGizmo\* | top referer

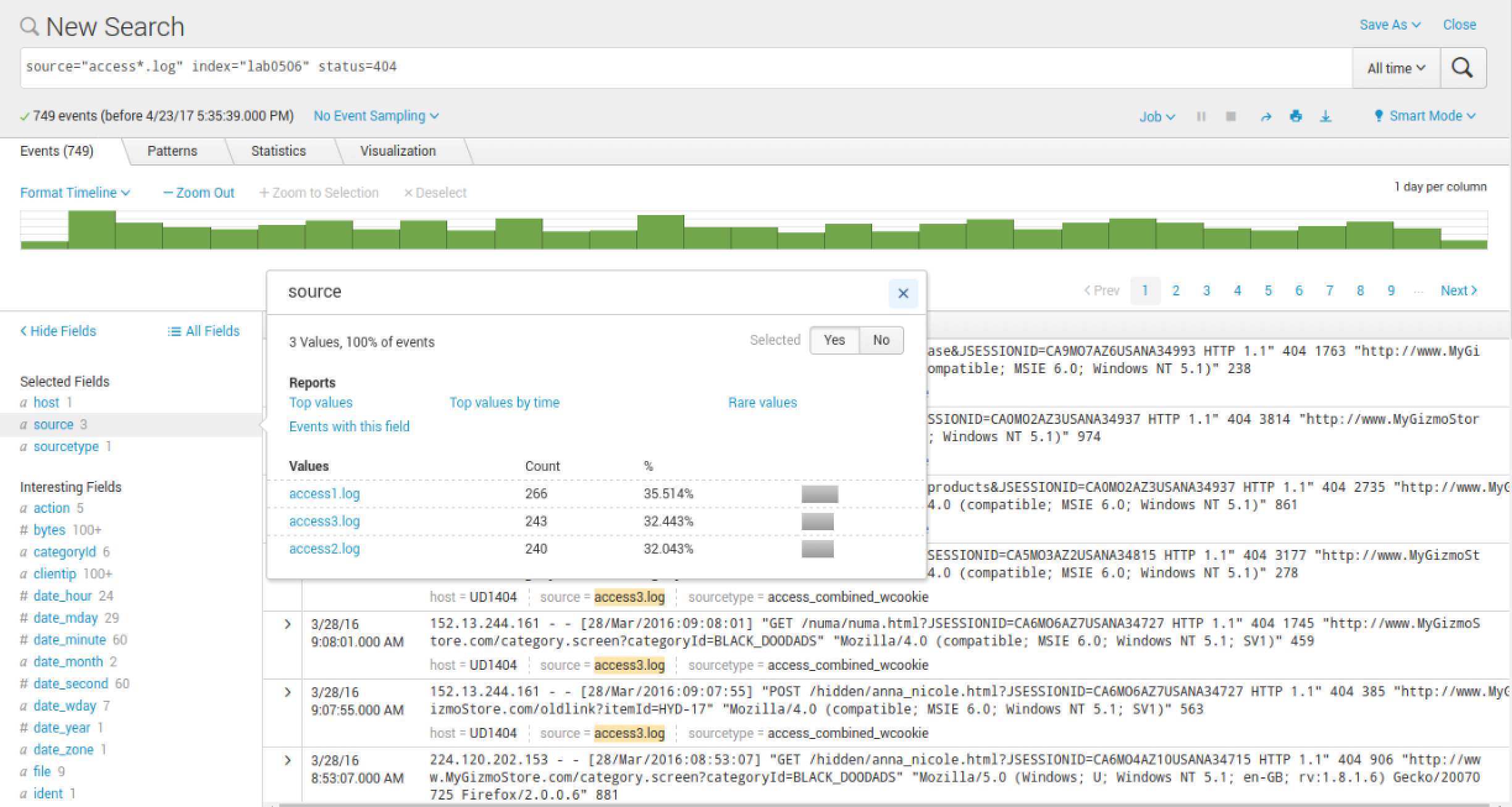


### How Many Events have HTTP 404 Status

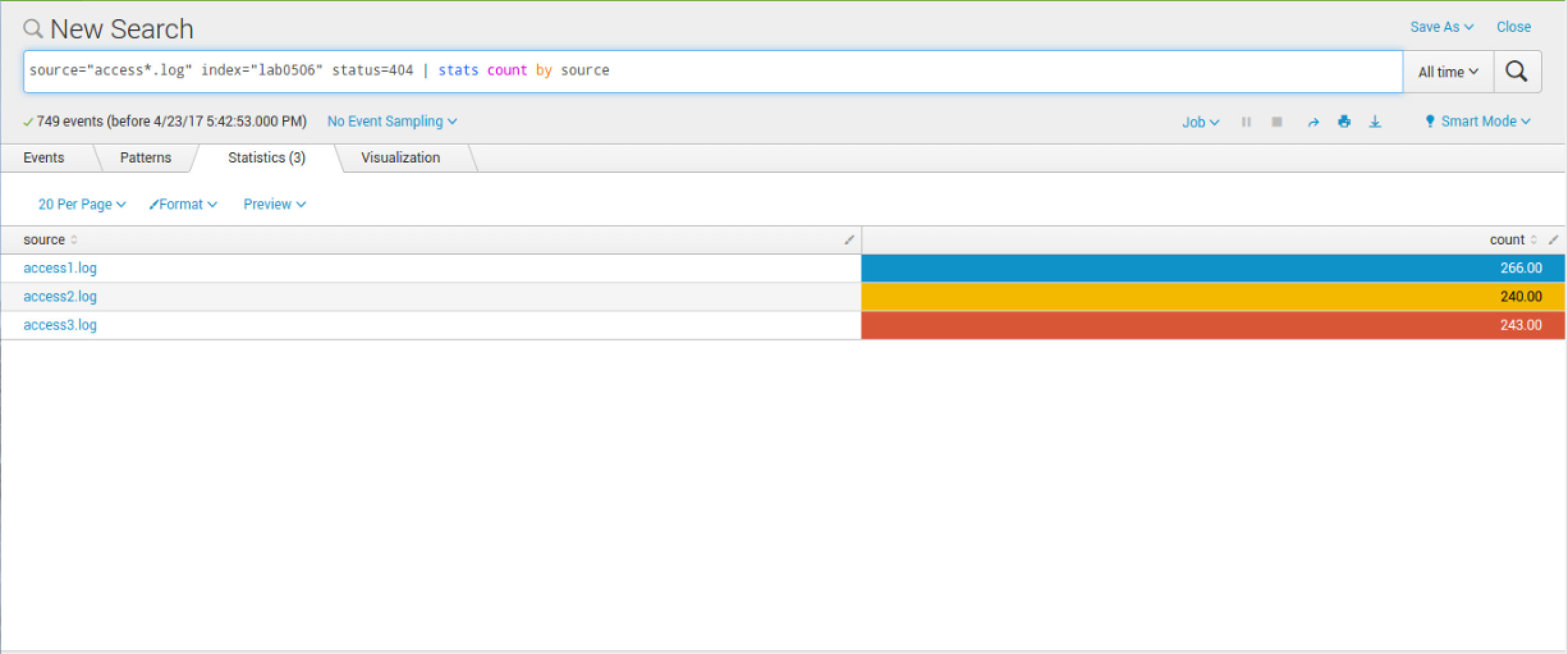
source=”access\*.log” index=”lab0506” referer != \*MyGizmo\* | top referer

### 

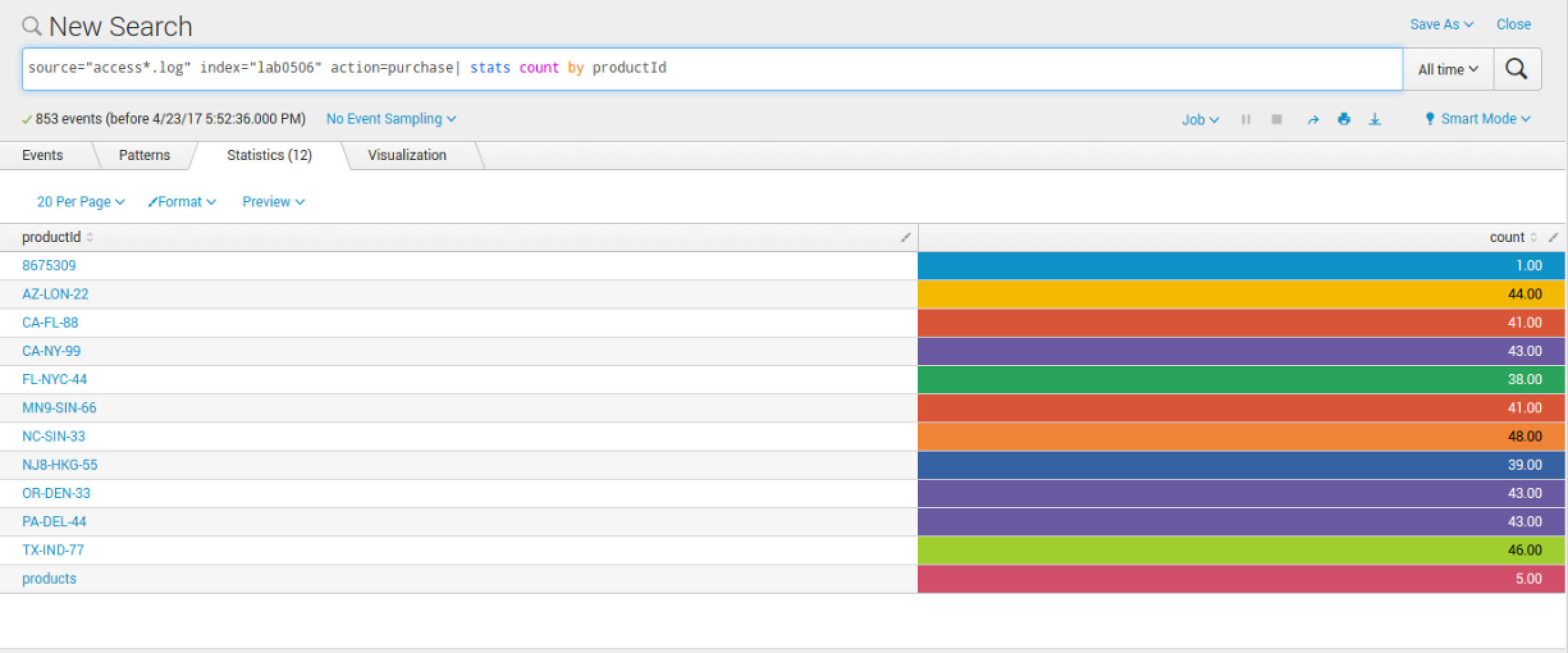
Searching by source (Web Server) – click on the source hyperlink



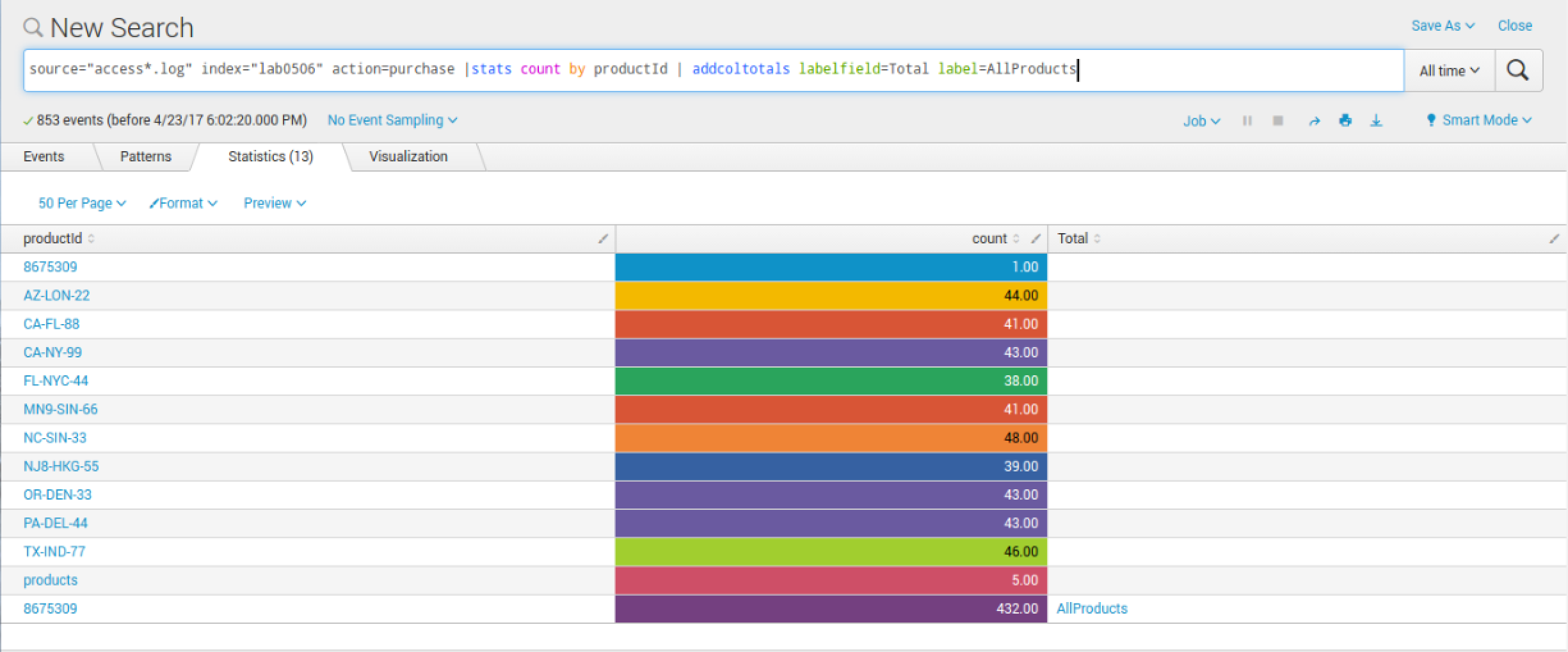
source=”access\*.log” index=”lab0506” status=404 | stats count by host (source)[[1]](#footnote-1)



source=”access\*.log” index=”lab0506” action=purchase | stats count by productId



source=”access\*.log” index=”lab0506” action=purchase | stats count by productId | addtotals labelfield=Total label=AllProducts



1. If you did not load the files as a separate host you will need to use a different method to differentiate the three data sources. [↑](#footnote-ref-1)