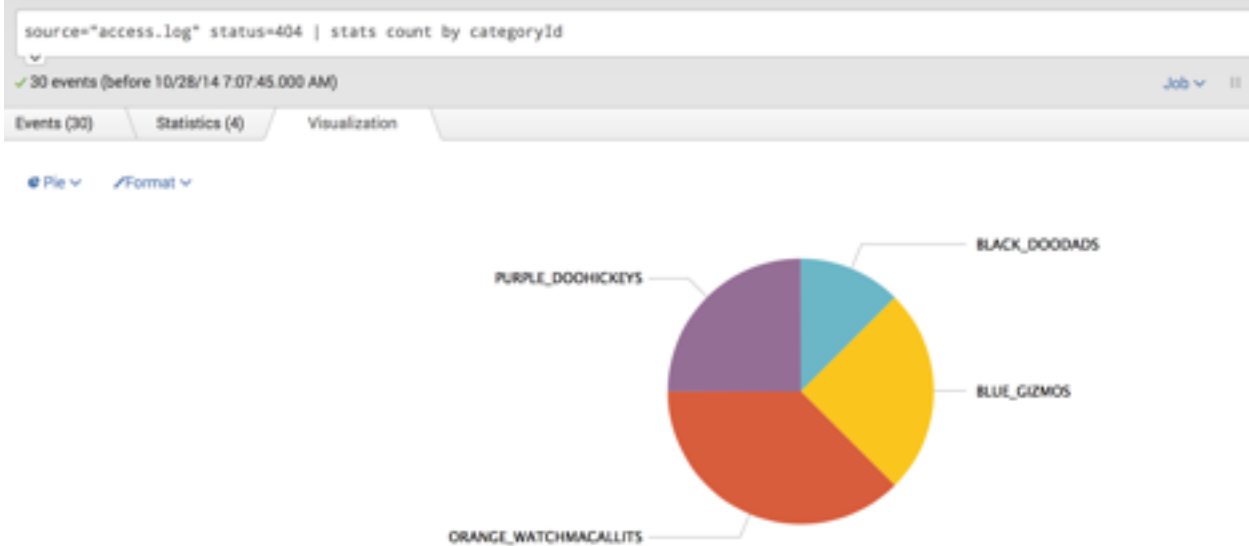


Assignment #3: Using Splunk – Basic and Advanced

In this assignment, we will be using the data provided by *Big Data Analytics Using Splunk* (Zadrozny and Kodali, 2013) – the log data “access.log” from MyGizmoStore.com.

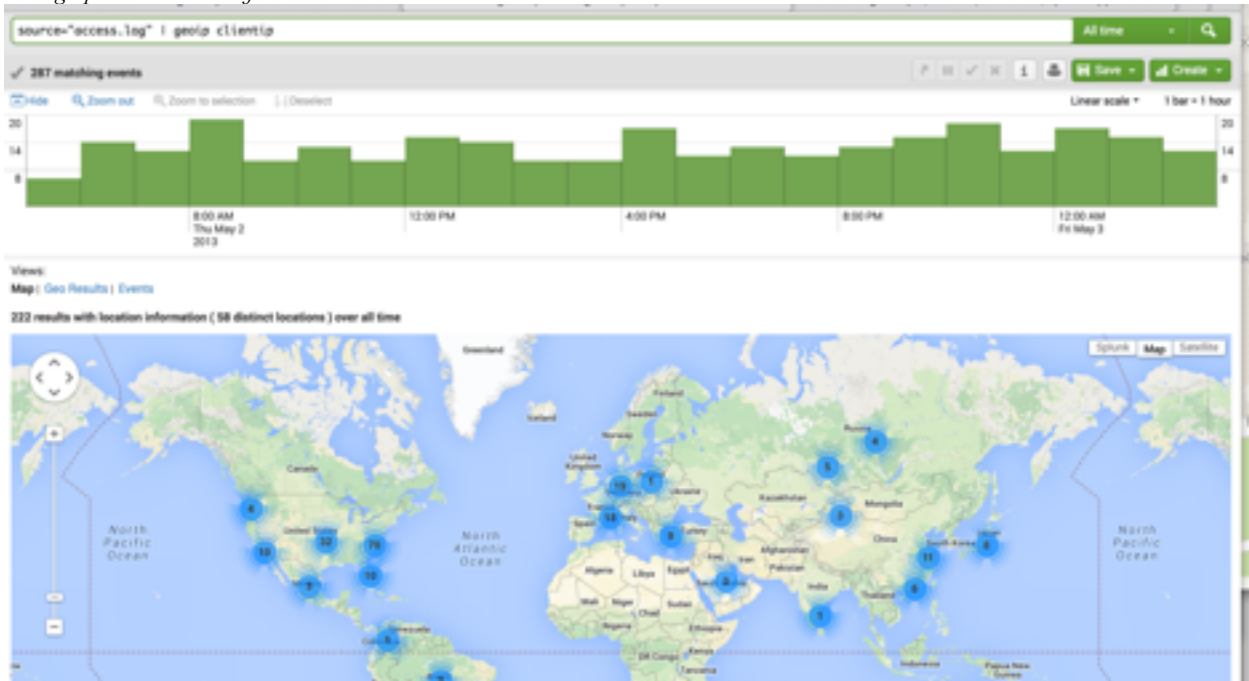
Question 1

Product categories affected by HTTP 404 errors



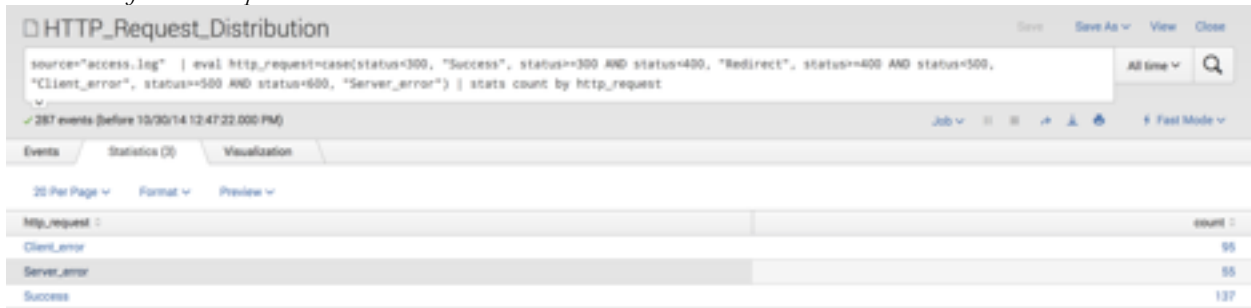
Question 2

Demographic distribution of all clients



Question 3

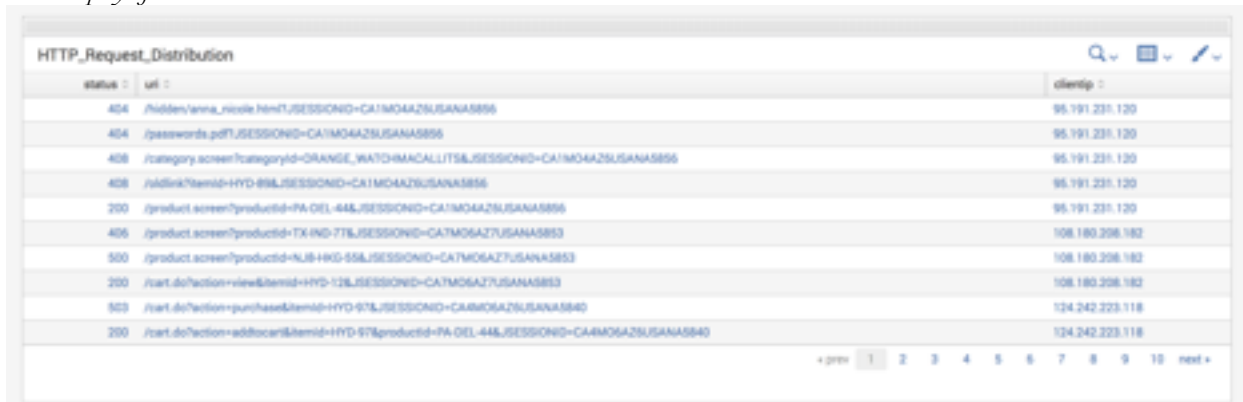
Distribution of HTTP requests



The screenshot shows a Splunk search interface for 'HTTP_Request_Distribution'. The search query is: `source="access.log" | eval http_request=case(status=300, "Success", status=300 AND status=400, "Redirect", status=400 AND status=500, "Client_error", status=500 AND status=600, "Server_error") | stats count by http_request`. The results table shows the following counts:

http_request	count
Client_error	95
Server_error	95
Success	137

Table display of search results

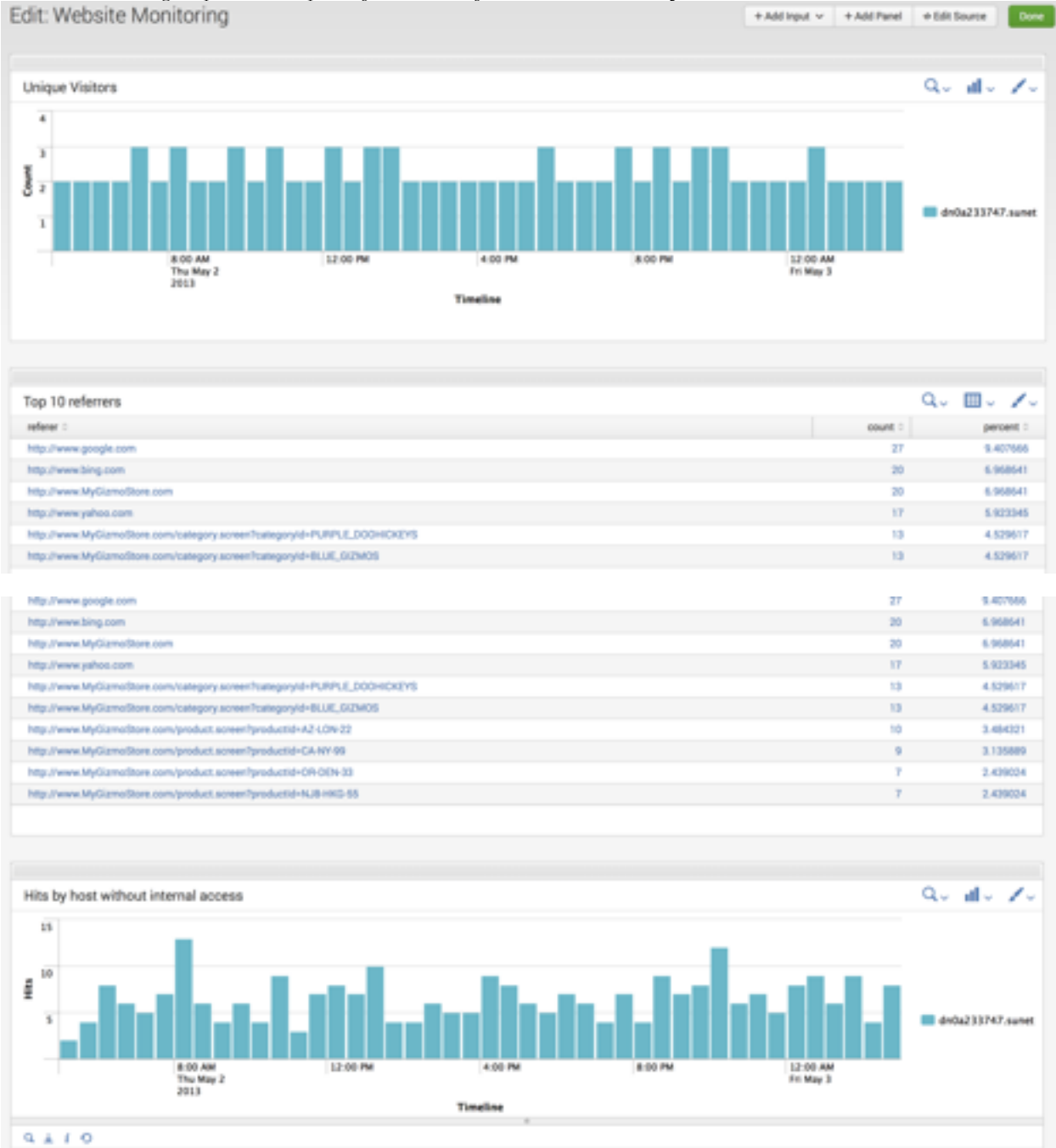


The screenshot shows a table display of search results for 'HTTP_Request_Distribution'. The table has columns for 'status', 'url', and 'clientip'. The results are as follows:

status	url	clientip
404	/hidden/anna_nicole.html?SESSIONID=CA1M04A29USANA5856	95.191.231.120
404	/passwords.pdf?SESSIONID=CA1M04A29USANA5856	95.191.231.120
408	/category.screen?categoryId=ORANGE_WA70HMACALLITS&SESSIONID=CA1M04A29USANA5856	95.191.231.120
408	/addlink?itemid=HYD-89&SESSIONID=CA1M04A29USANA5856	95.191.231.120
200	/product.screen?productId=PA-DEL-44&SESSIONID=CA1M04A29USANA5856	95.191.231.120
406	/product.screen?productId=TX-IND-77&SESSIONID=CA1M06A27USANA5853	108.180.208.182
500	/product.screen?productId=NJB-HKG-55&SESSIONID=CA1M06A27USANA5853	108.180.208.182
200	/cart.do?action=view&itemid=HYD-12&SESSIONID=CA1M06A27USANA5853	108.180.208.182
503	/cart.do?action=purchaseItem&HYD-97&SESSIONID=CA1M06A29USANA5840	124.242.223.118
200	/cart.do?action=addtocart&itemid=HYD-97&productId=PA-DEL-44&SESSIONID=CA1M06A29USANA5840	124.242.223.118

Question 4

Dashboard monitoring unique visitors, top 10 referer addresses for the website, and hits by host without internal access



Question 5

Page "views" per hour



Alert if views drop below 100

The screenshot shows the configuration for an alert titled "Page views under 100 in an hour". The alert is currently disabled. The configuration details are as follows:

- Enabled: Yes. [Disable](#)
- Alert Type: Scheduled. Hourly, at 45 minutes past the hour. [Edit](#)
- Trigger Condition: Number of Results is < 100. [Edit](#)
- Actions: List in Triggered Alerts. [Edit](#)
- App: search
- Permissions: Shared in App. Owned by admin. [Edit](#)

At the bottom, there is a message: **!** There are no fired events for this alert.