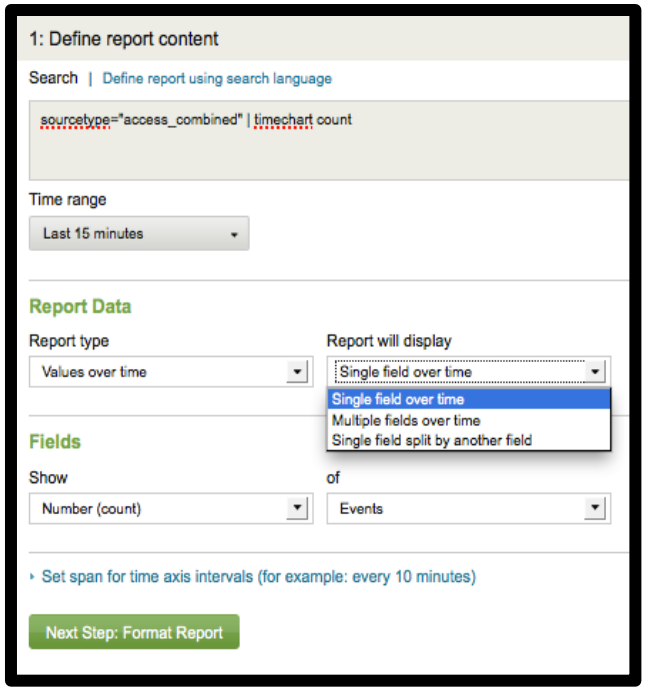
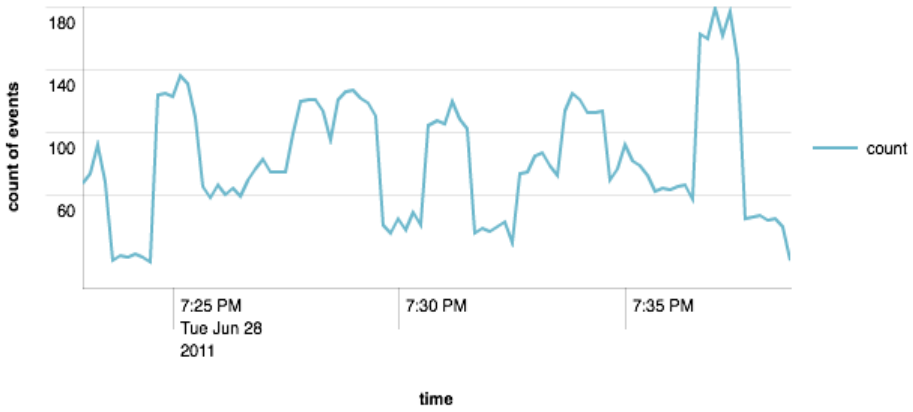
Build a Graph Over Time: Single Field Over Time

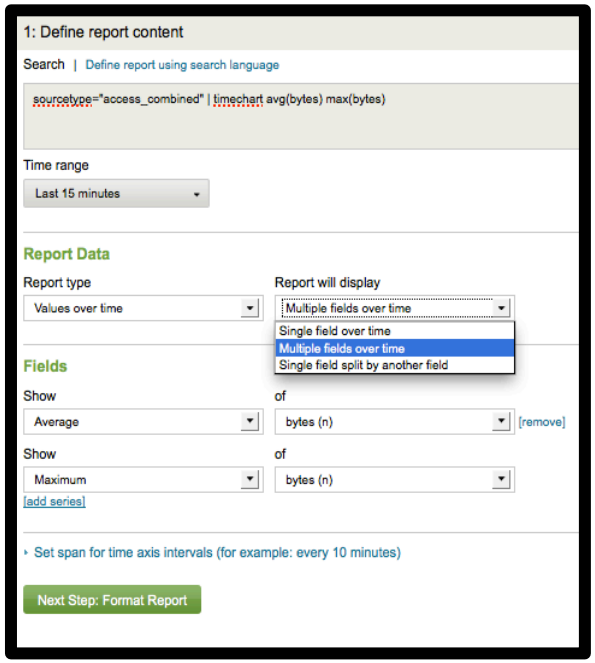
Example: sourcetype=access_combined | timechart count

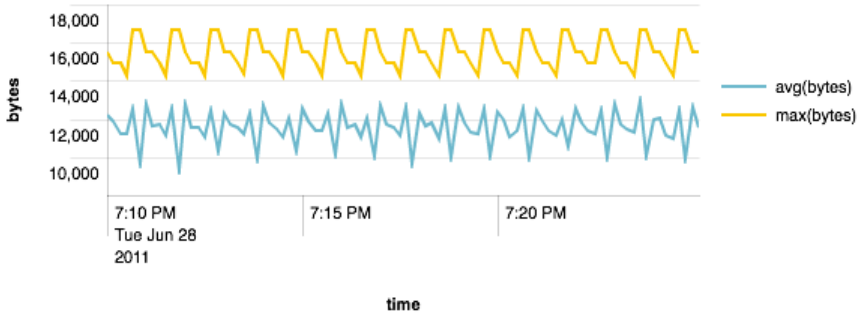




Build a Graph Over Time: Multiple Fields Over Time

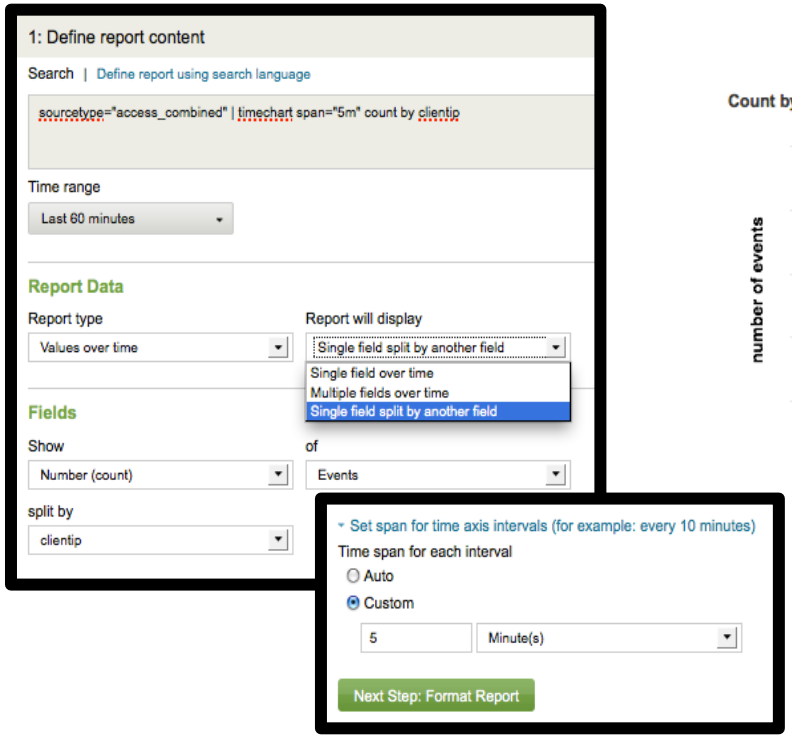
Example: sourcetype=access_combined | timechart avg(bytes) max(bytes)

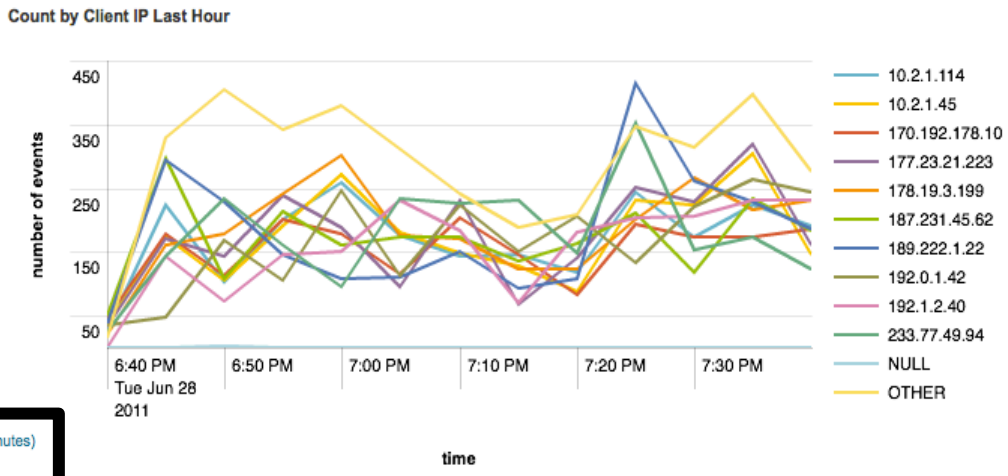




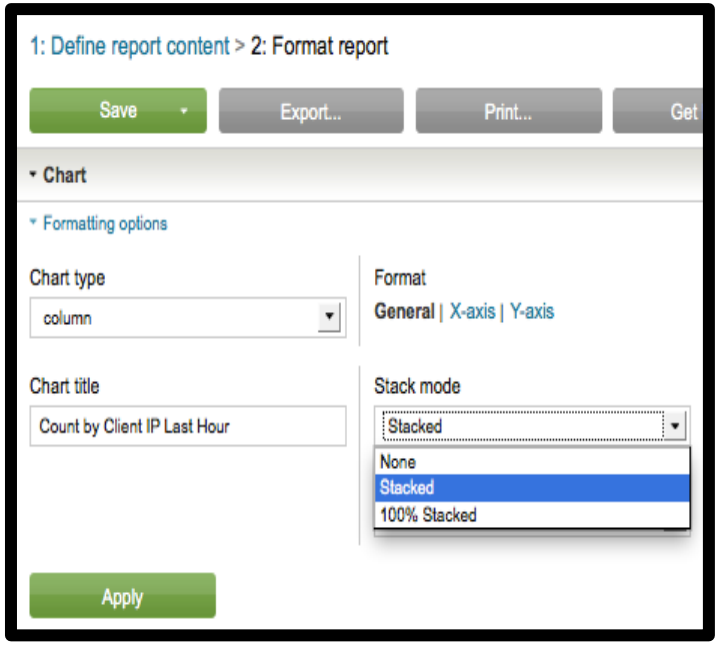
Build a Graph Over Time: Single Field Split by Another Field

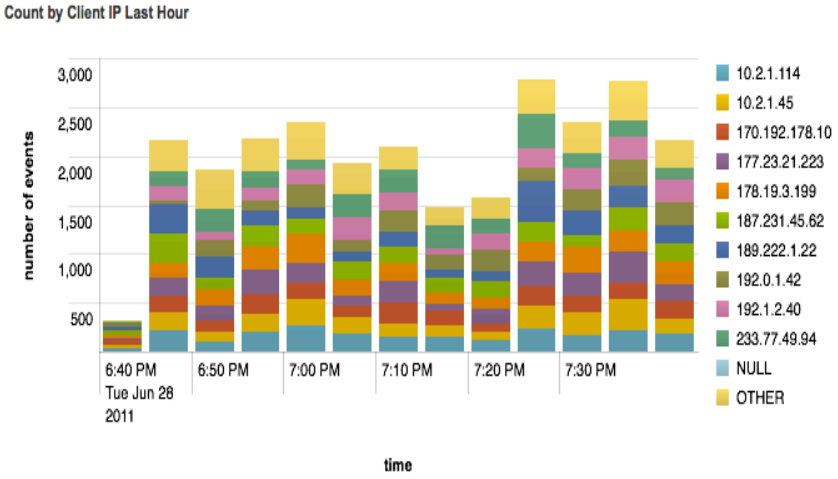
Example: sourcetype=access_combined | timechart span=5m count by clientip





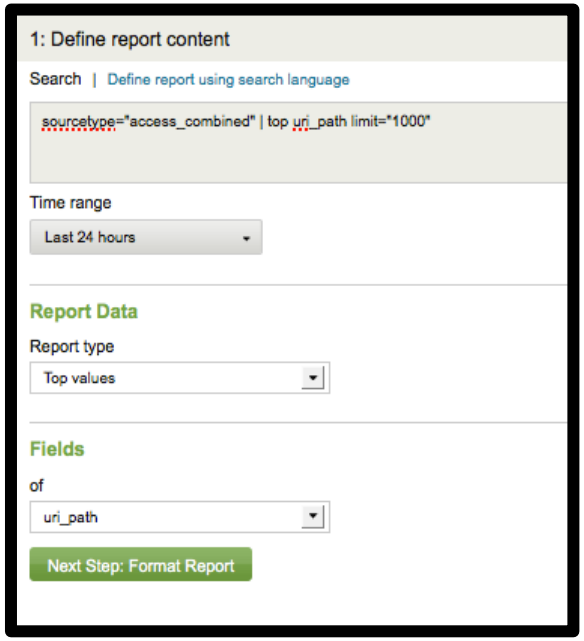
Stack Values

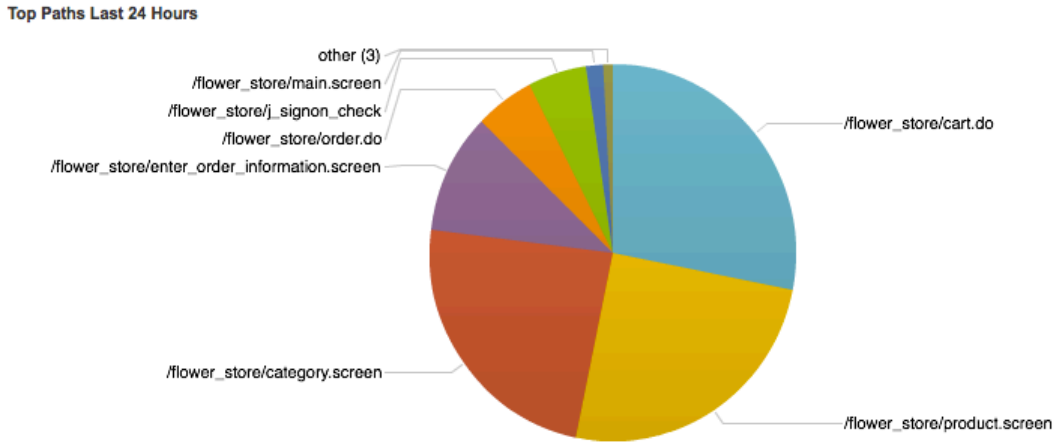




Build a Graph on Values

Example: sourcetype=access_combined | top uri_path

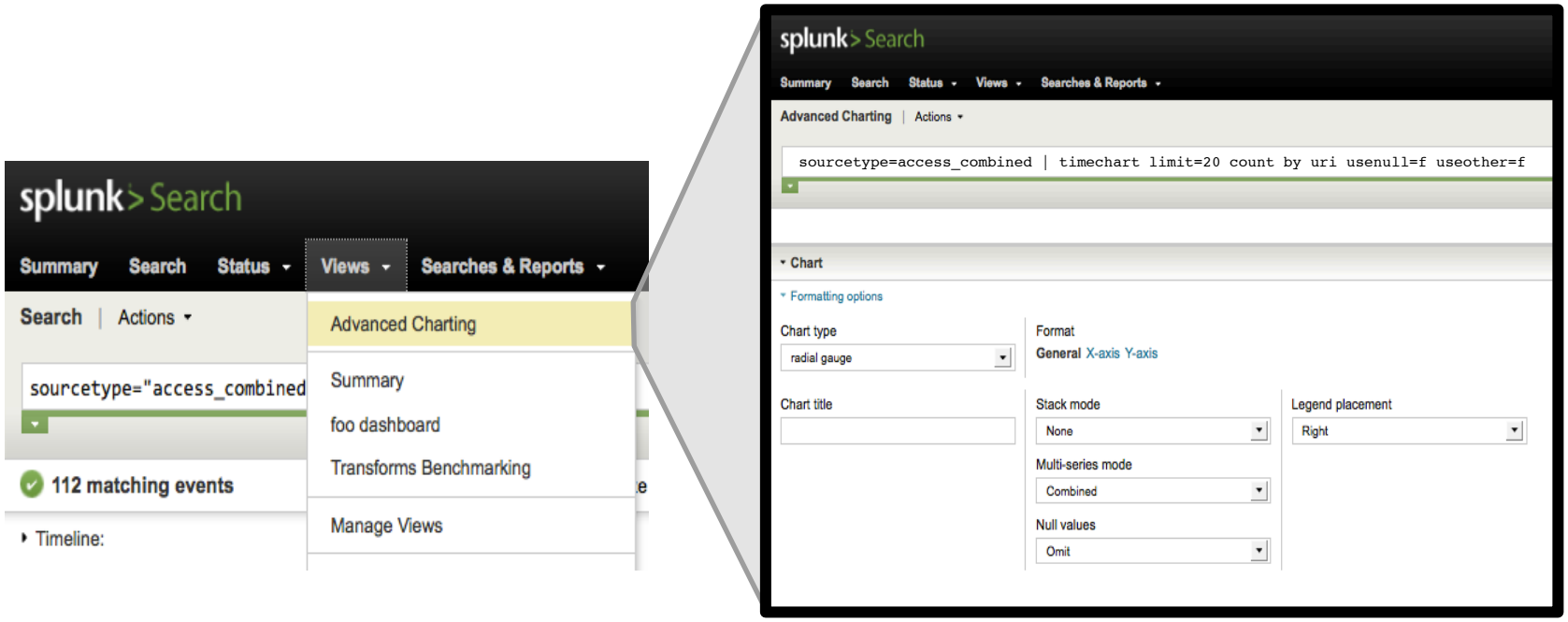




Use the Advanced Charting (AC) View

Define reports and toggle options in the search bar

Example: sourcetype=access_combined |
timechart **limit=20** count by uri **usenull=f useother=f**



Build Gauges

Set thresholds via search + make gauge type selections in UI

Example: sourcetype=access_combined | stats count | gauge count 0 25 50 100 150