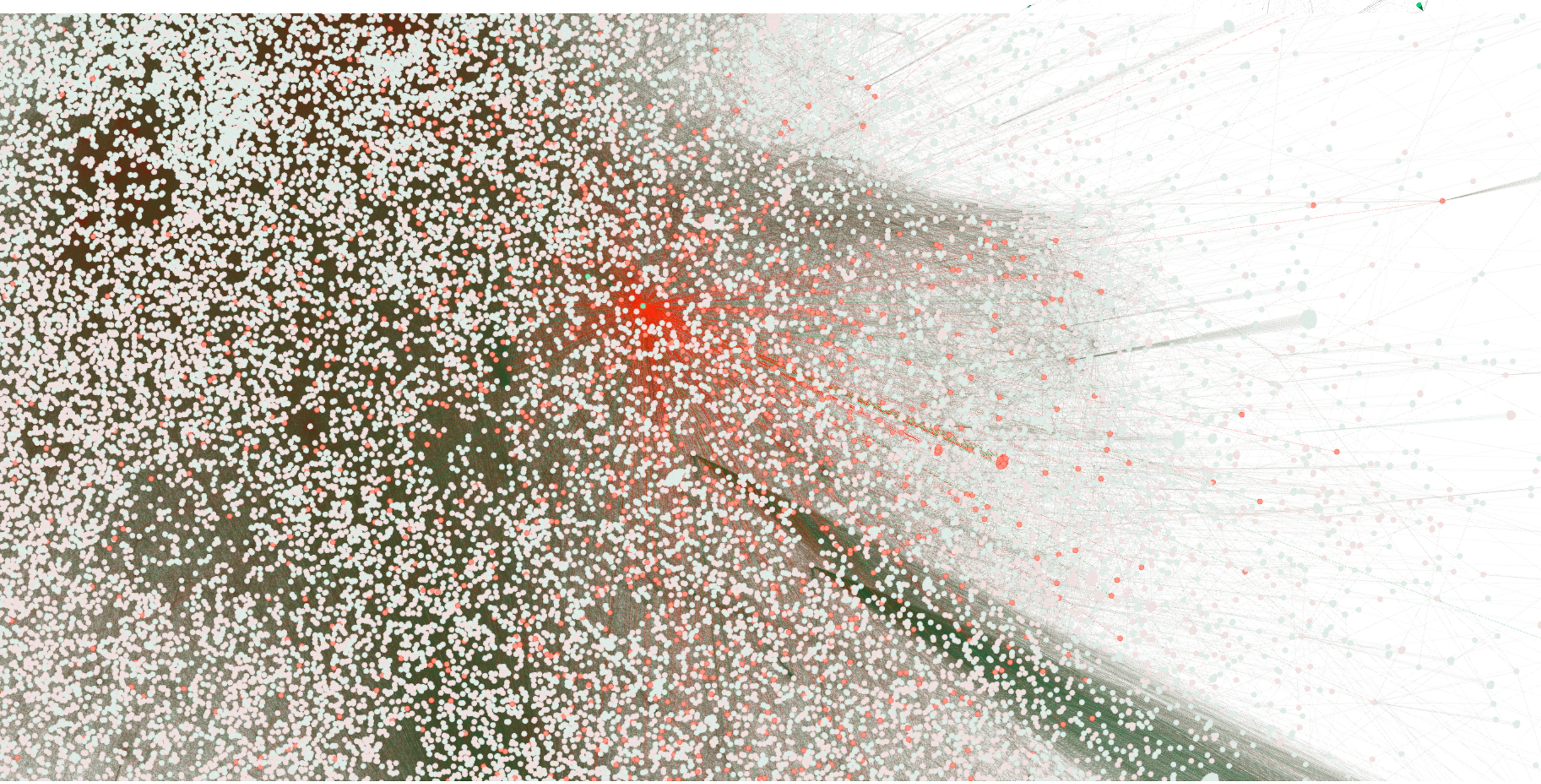
1

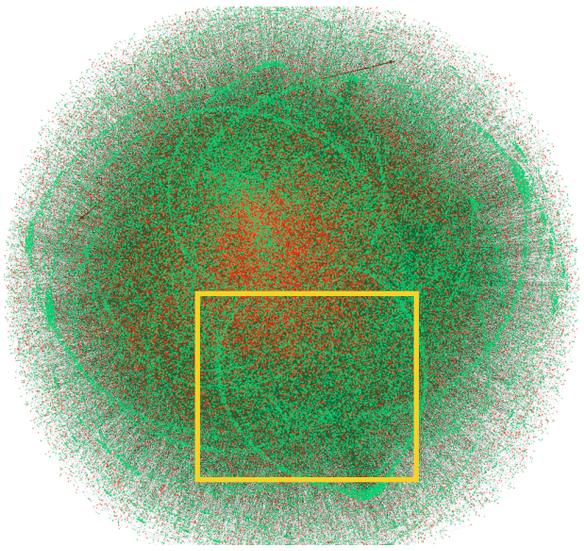
directed network of src-dest IP addresses
internal = red, external = green
1,000,000 flows - 100,000 IP’s - 400,000 edges
zooming in on graph & selecting a node below

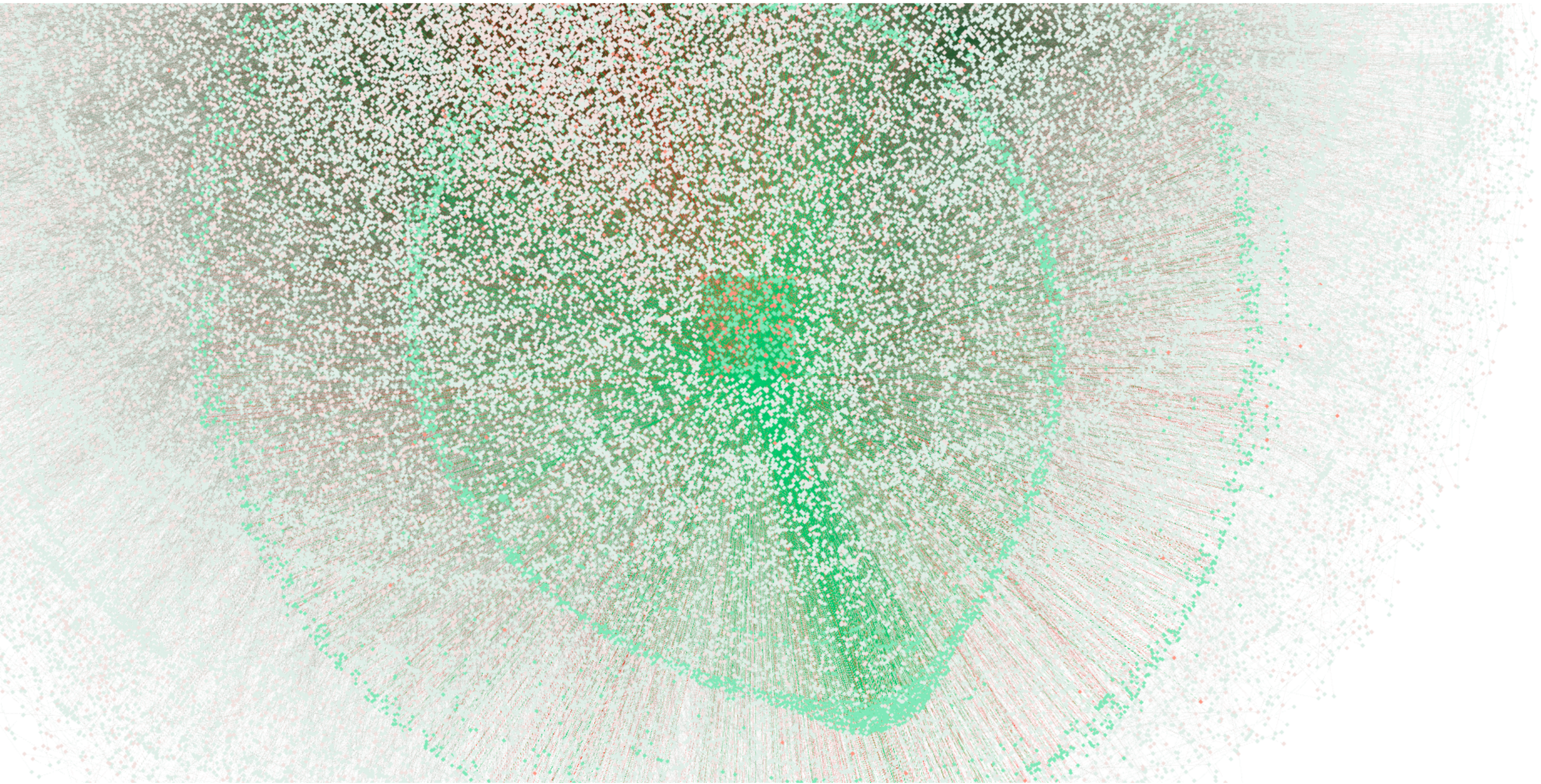


2

I

directed network of src-dest IP addresses
same as before, but new layout
zoomed-in, selecting a group of nodes

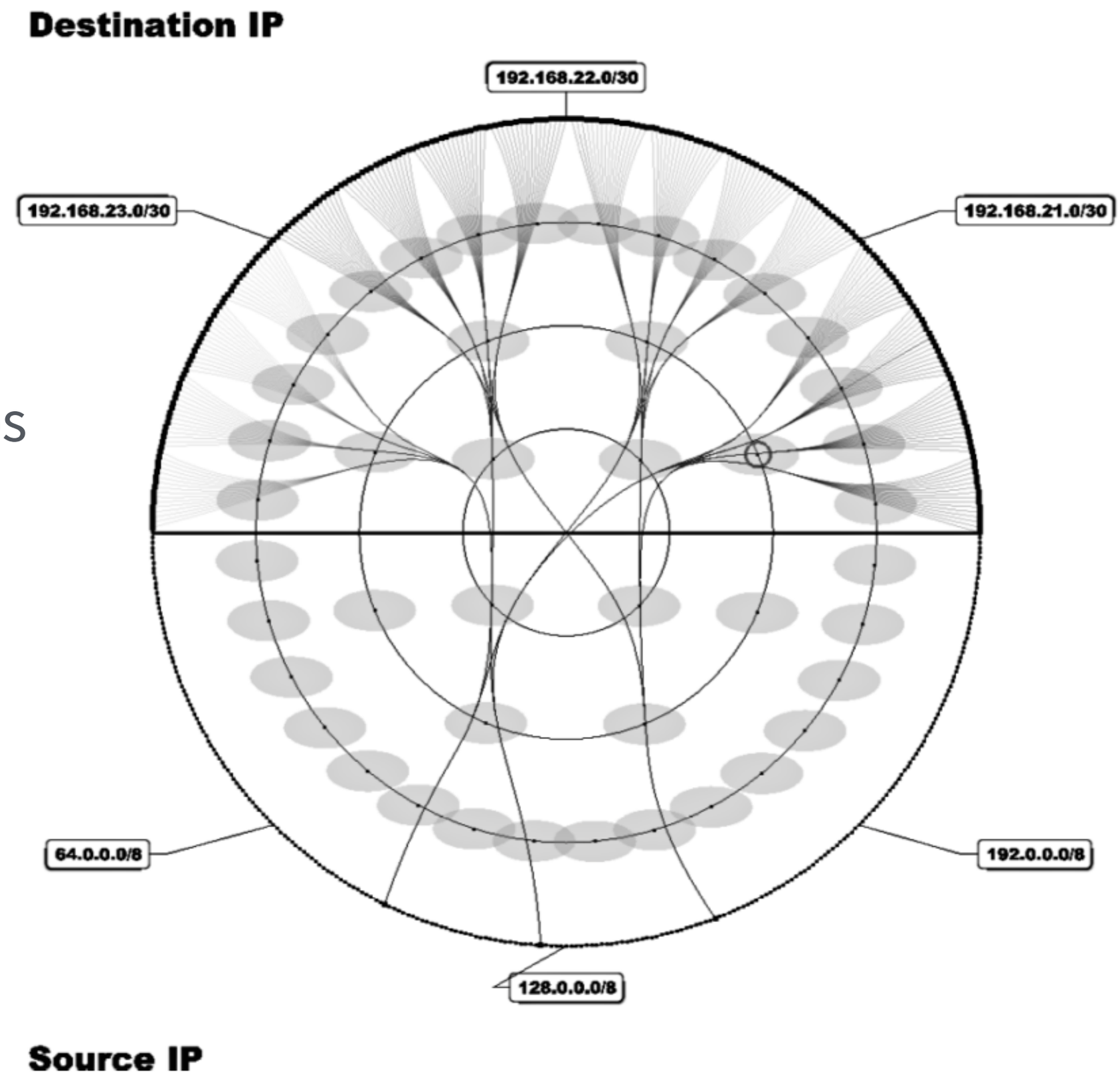




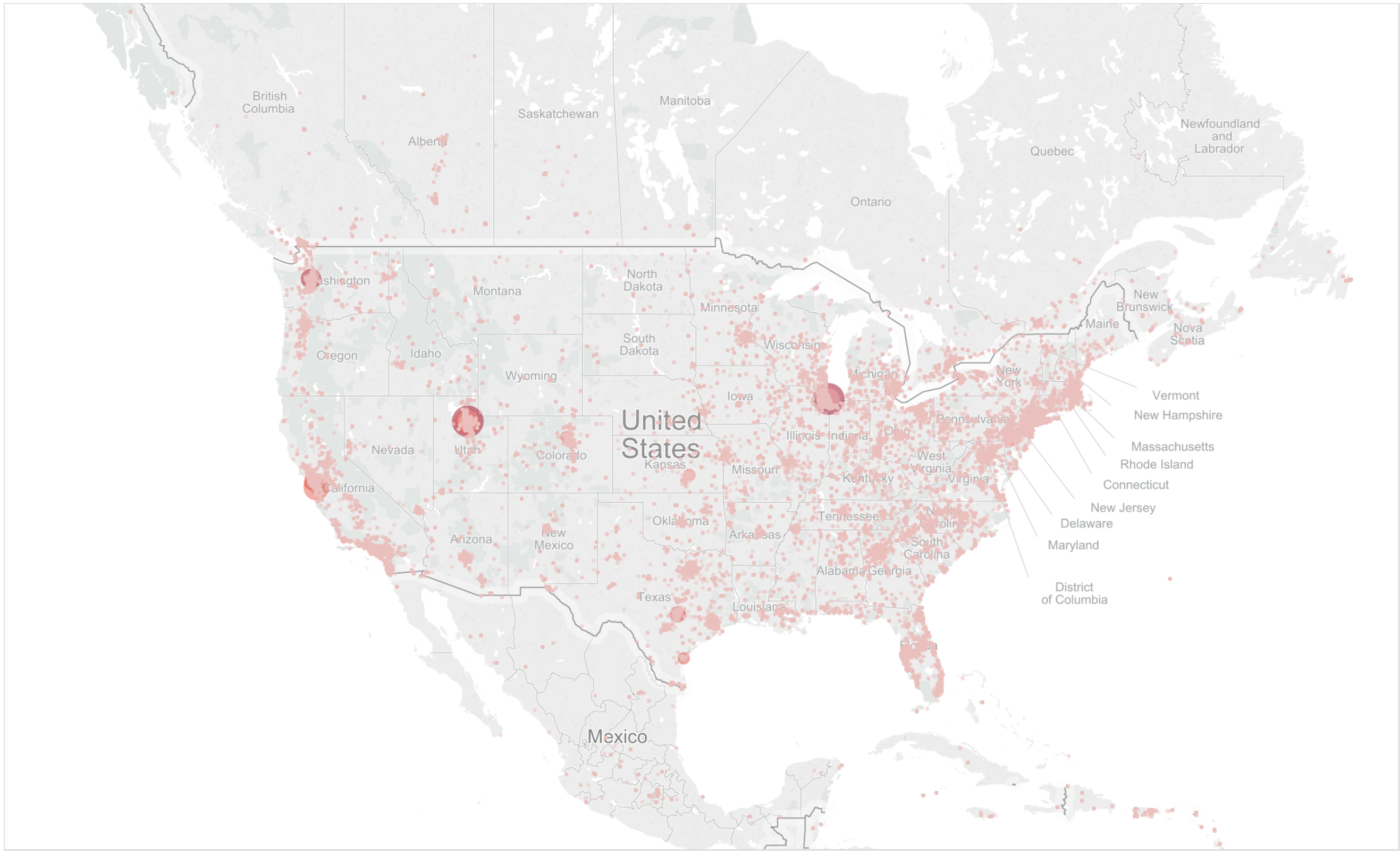
network of src-dest
(not your data)

arranged on circle
bundled by IP groups

would get messy
fast with real data…



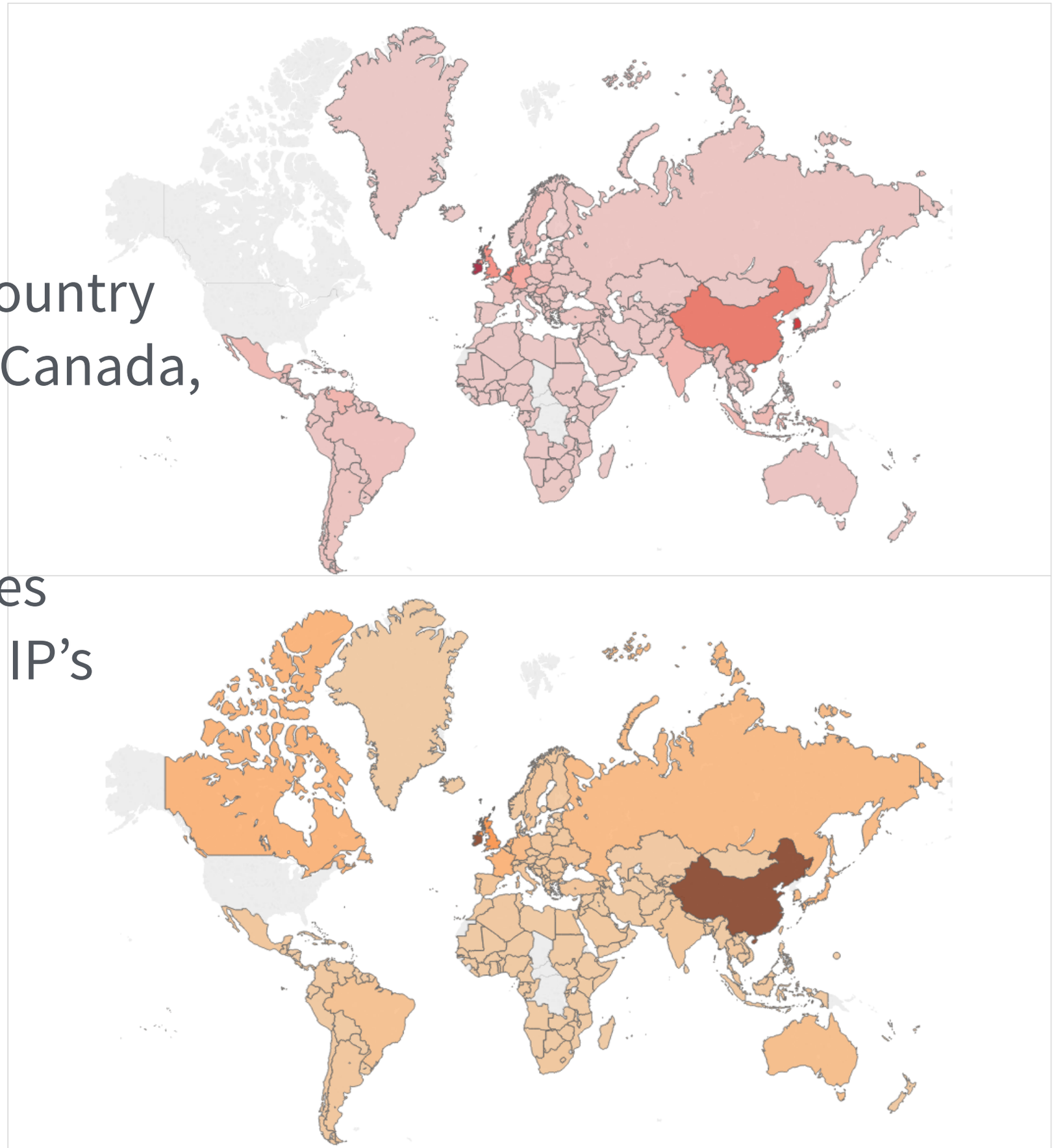
plotting IP addresses as points on a map sized by # packets, colored by # bytes



plotting IP address source & destination as lines on a map centered on Utah; over-plotted for entire dataset…

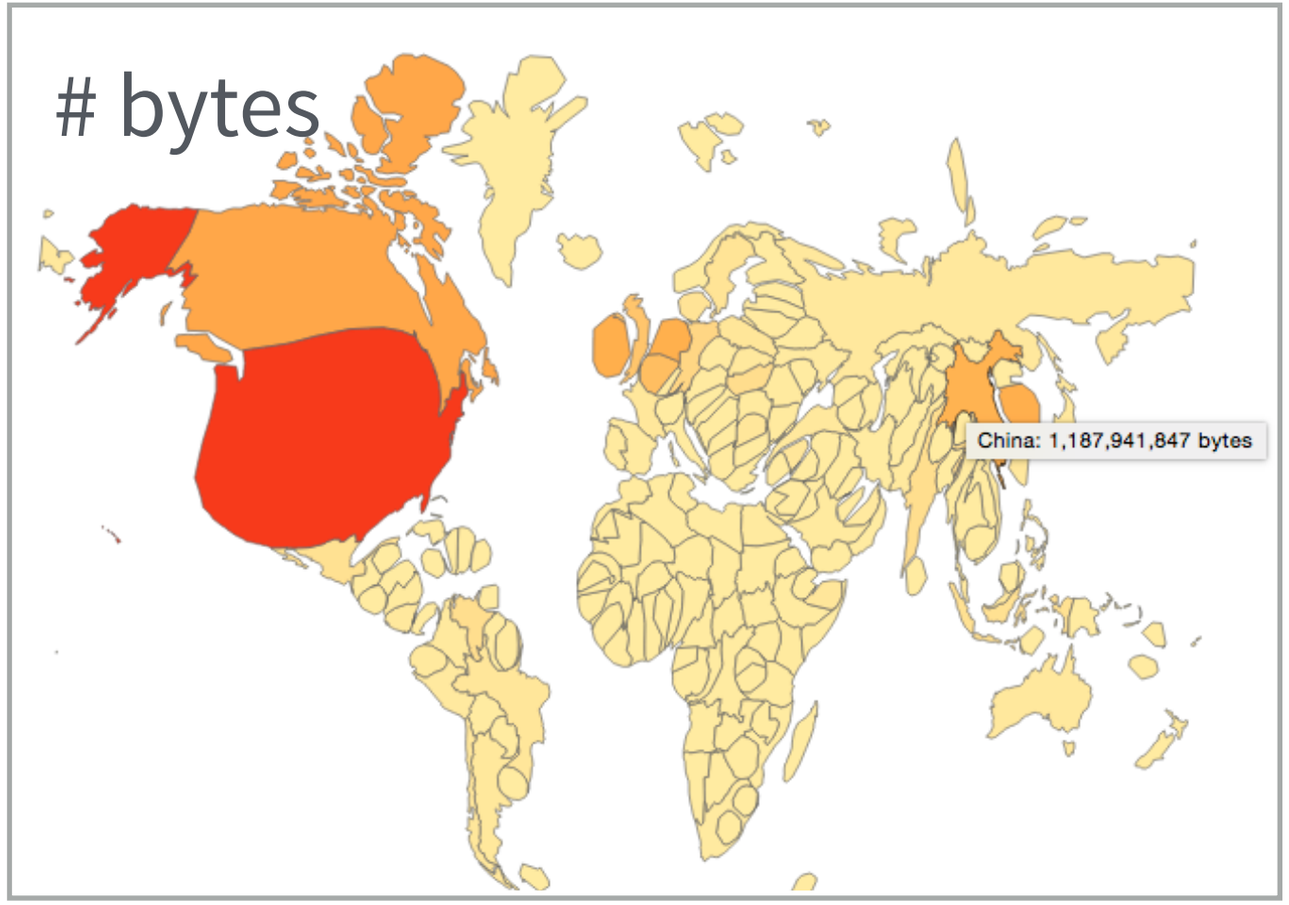
IP address,
aggregated by country
(excluding US & Canada,
since too large)

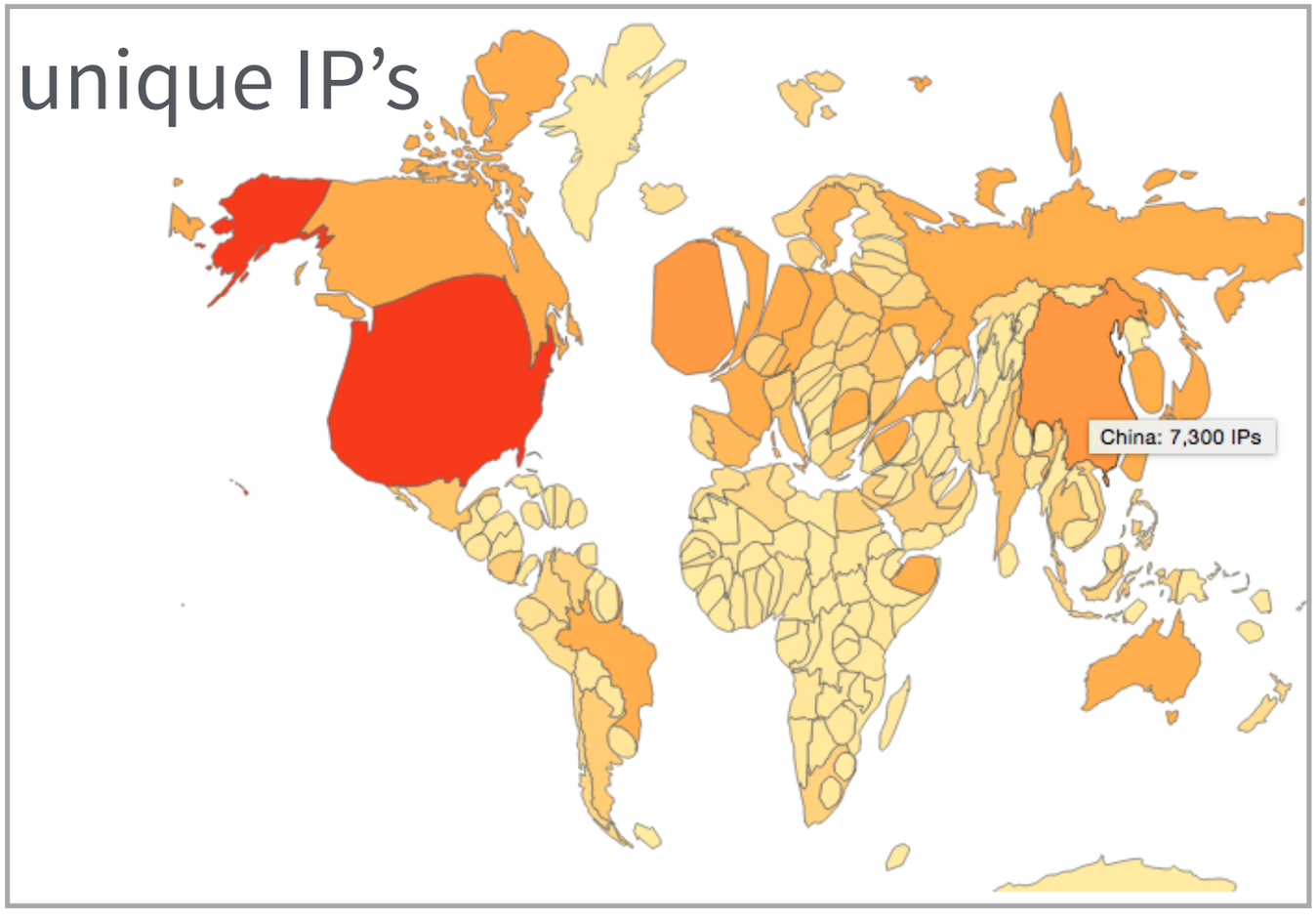
colored by # bytes
and also unique IP’s

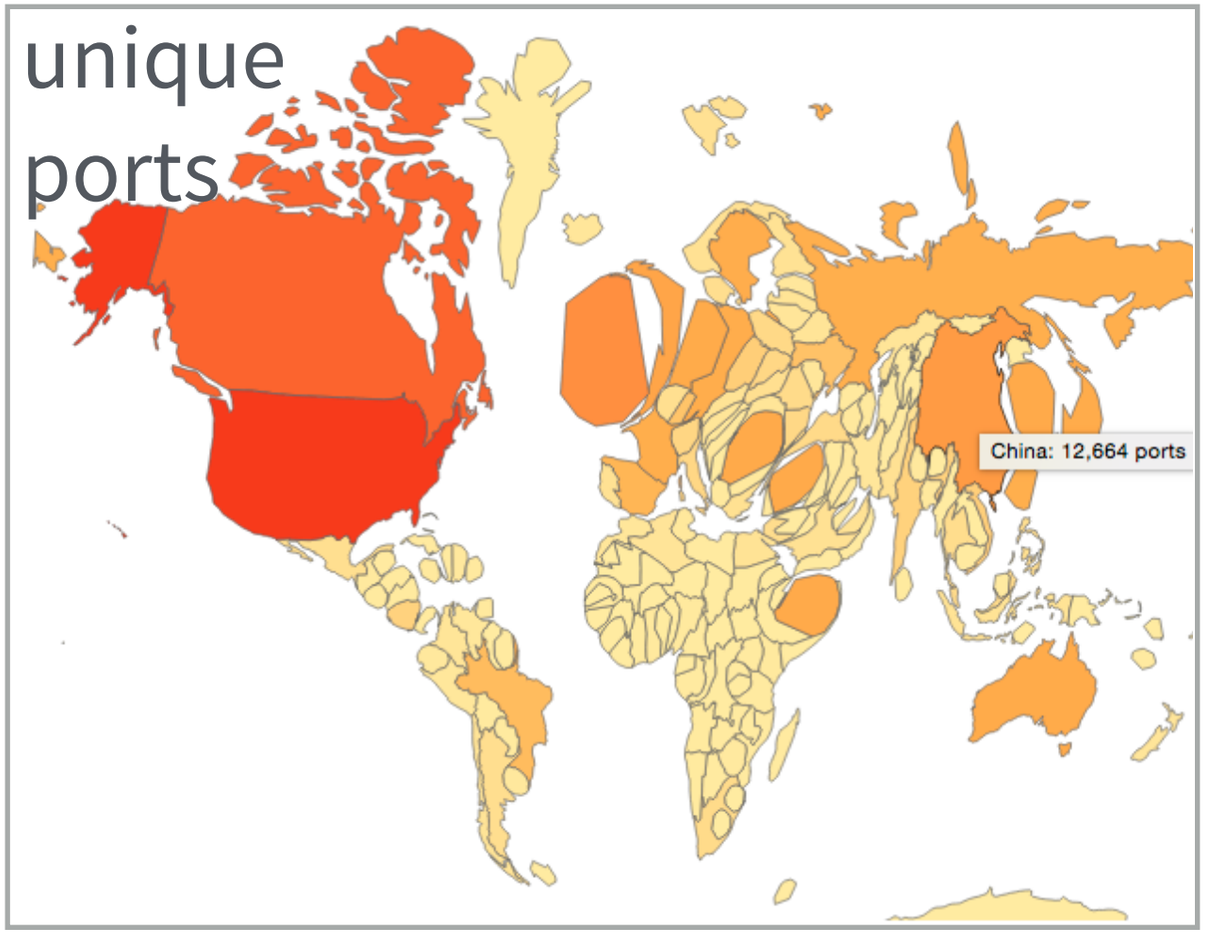


IP address,
aggregated by country

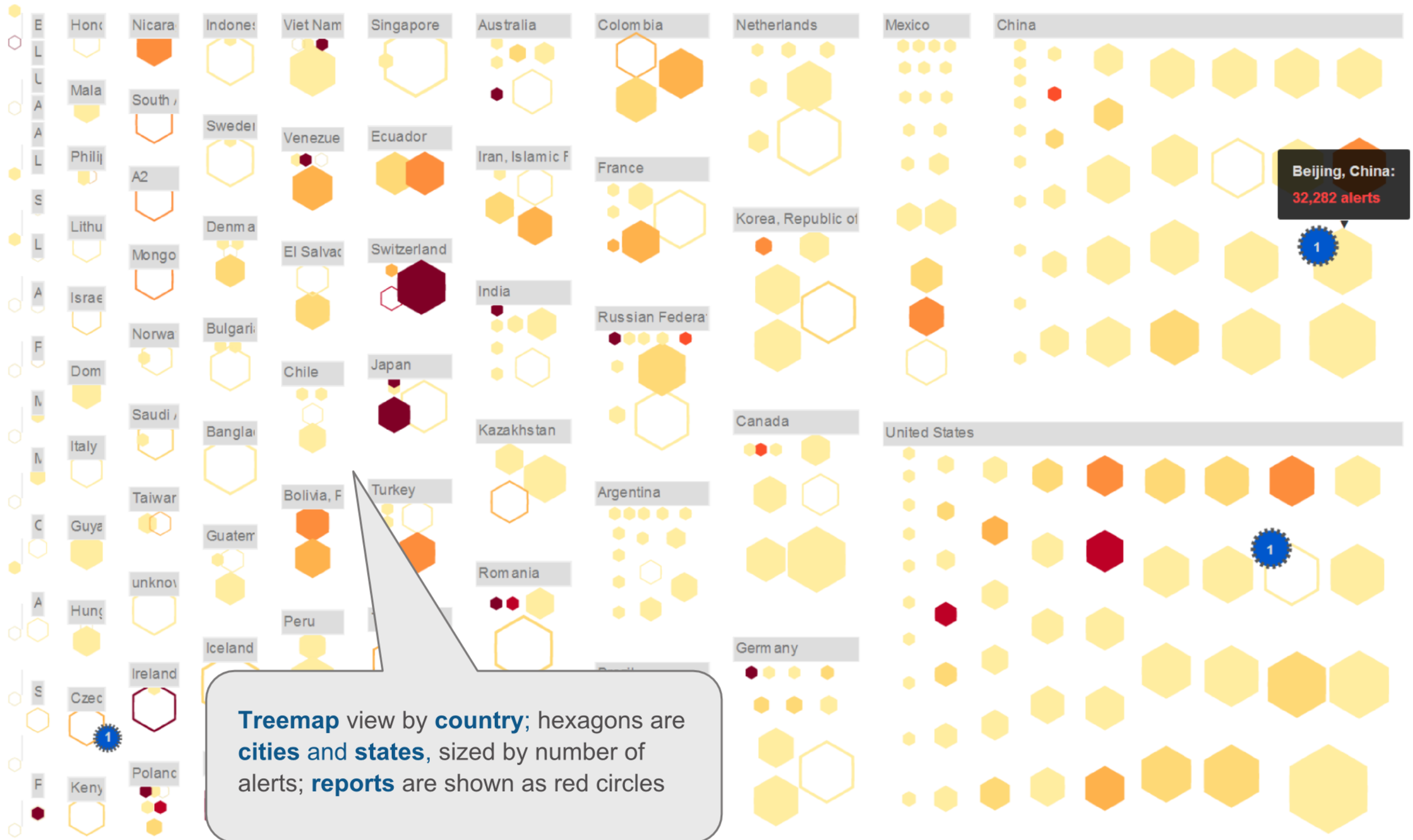
colored & sized by:







IP’s aggregated by both region & country *(not your data)* can correspond approximately to locations on a map colored & sized by choice (activity level, most recent)

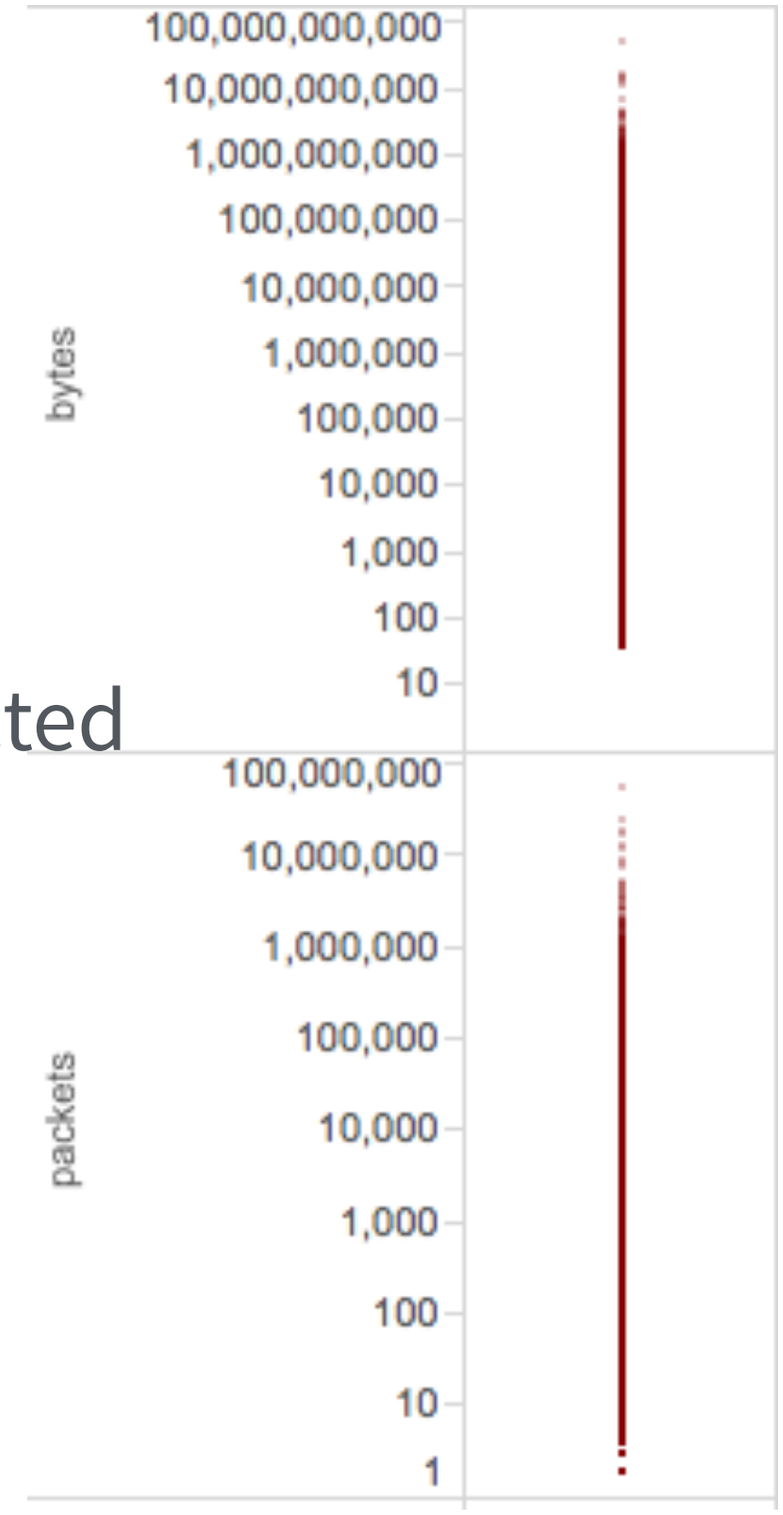


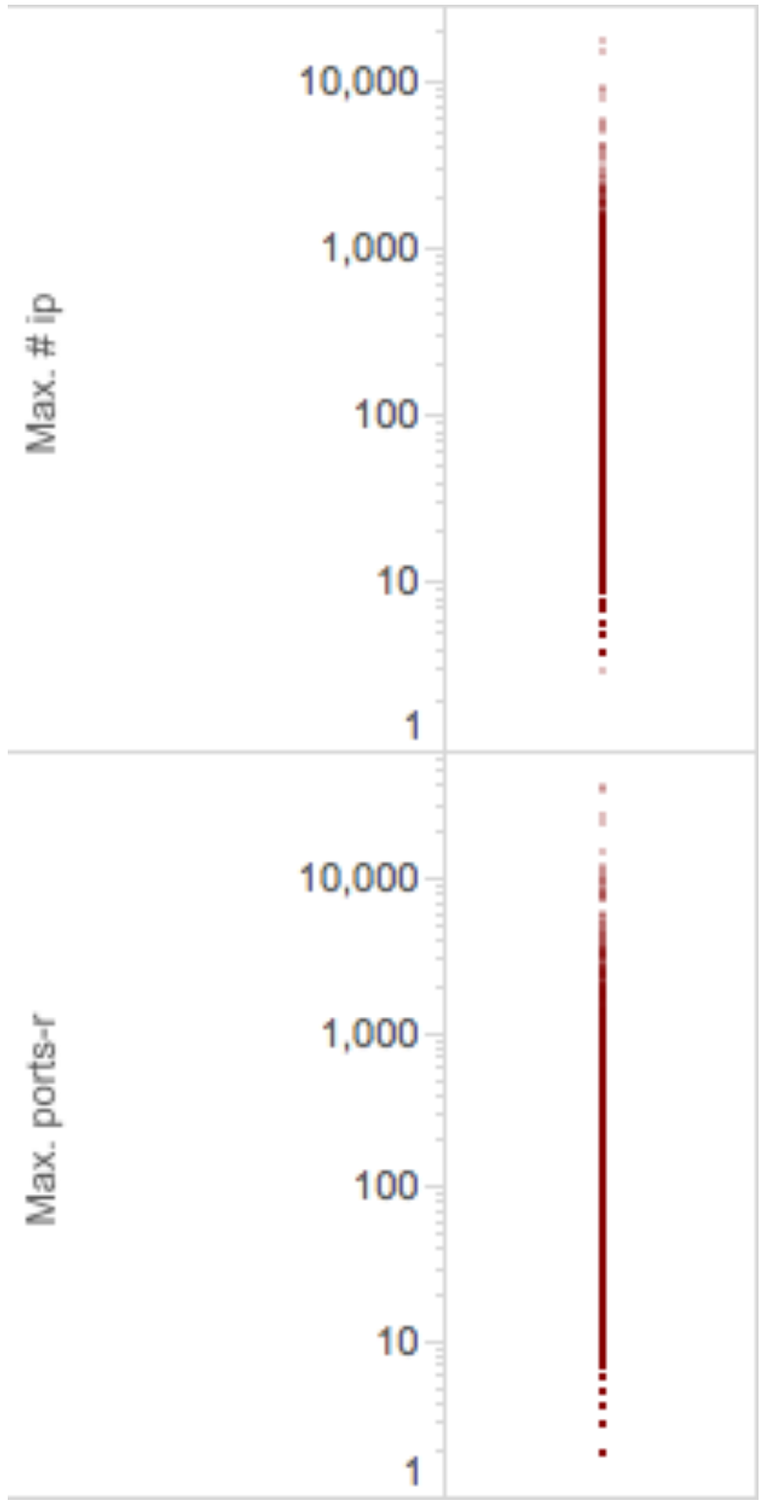
circle for each /24

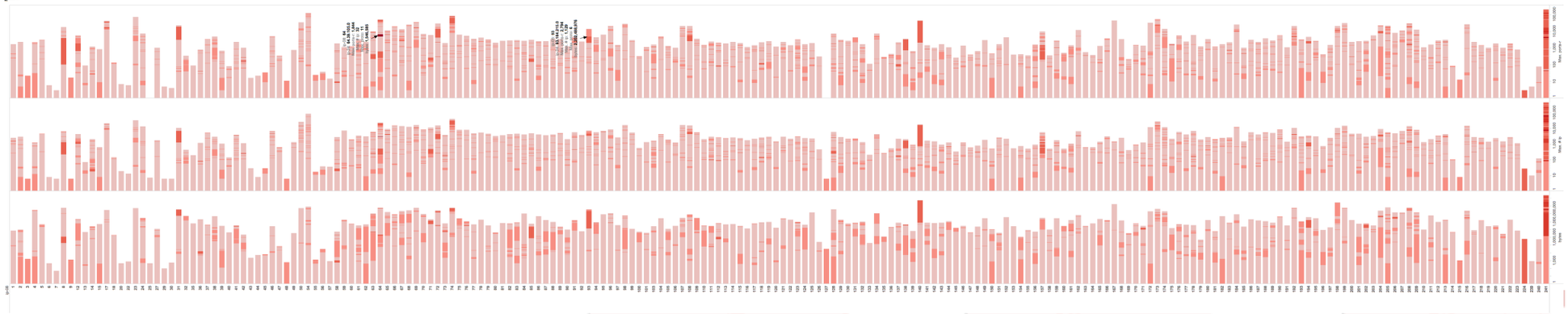
note the log scales

circles can be selected

useful as a legend







three bar charts

bytes, unique IP's, and unique ports

each bar is a /8

bars break into /24

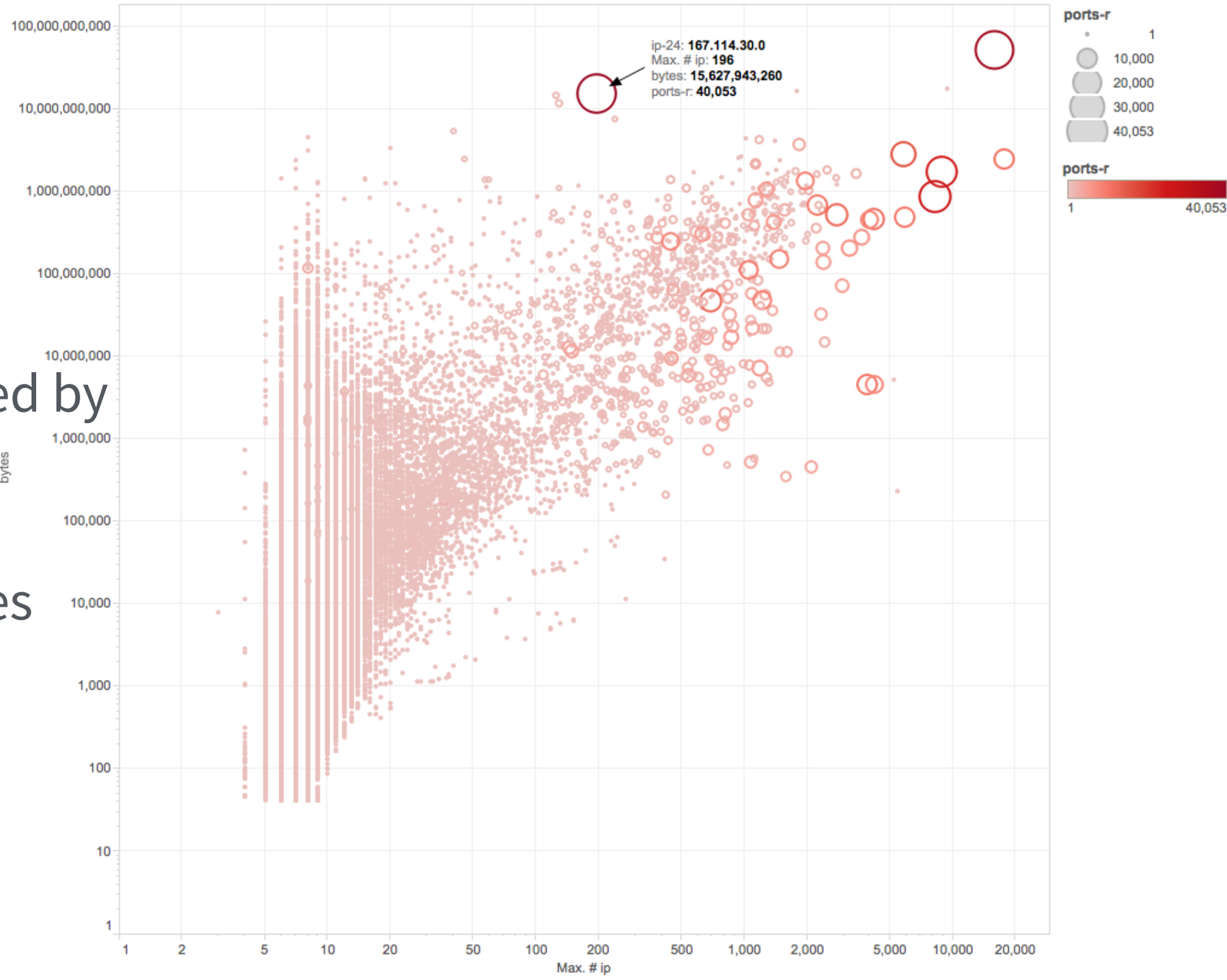
colored by # protocols

note the log scales

scatterplot
  points = /24
  unique IP's
  vs # bytes

sized & colored by
unique ports

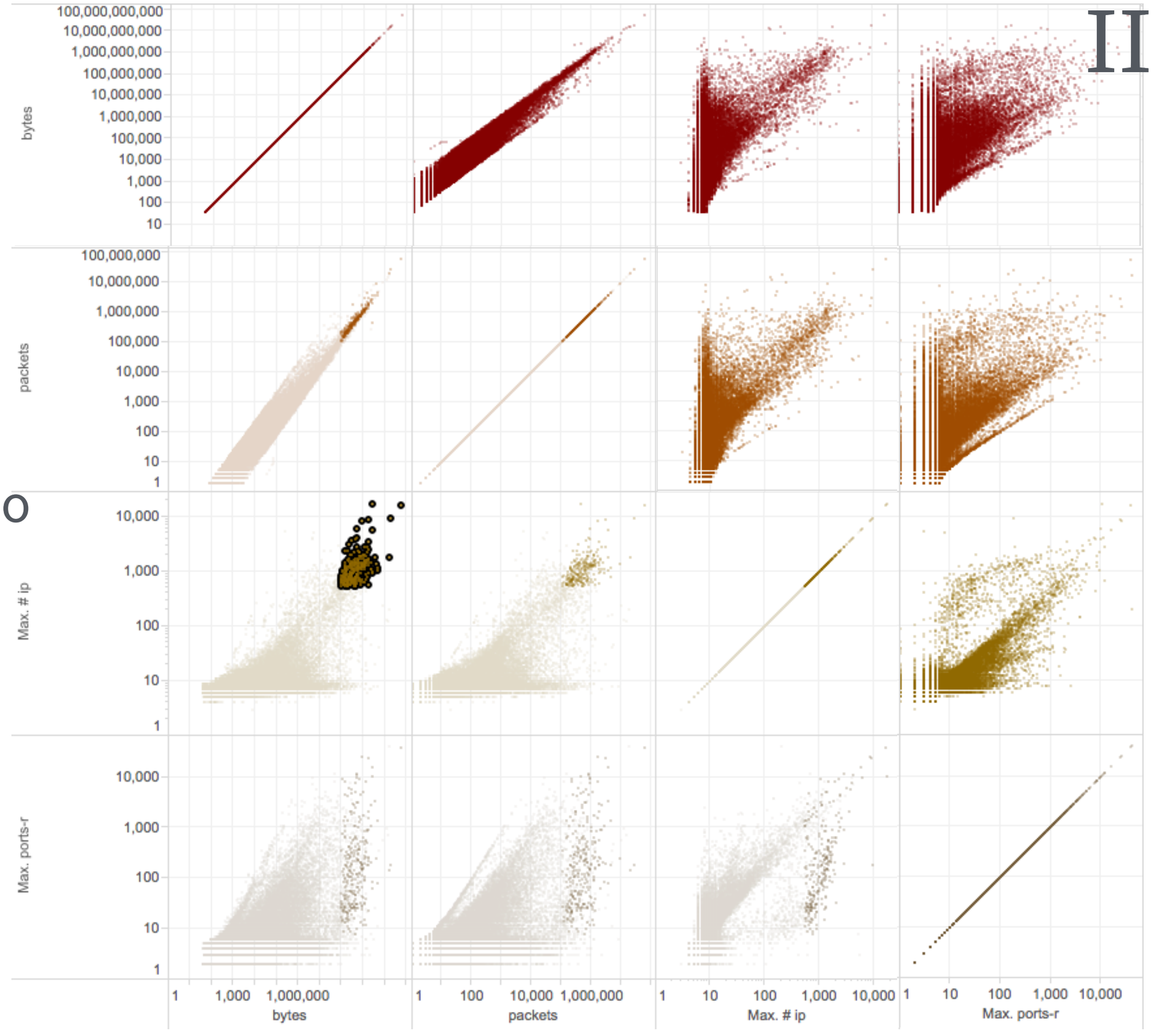
note log scales



multiple scatterplots

points = /24

can select, too

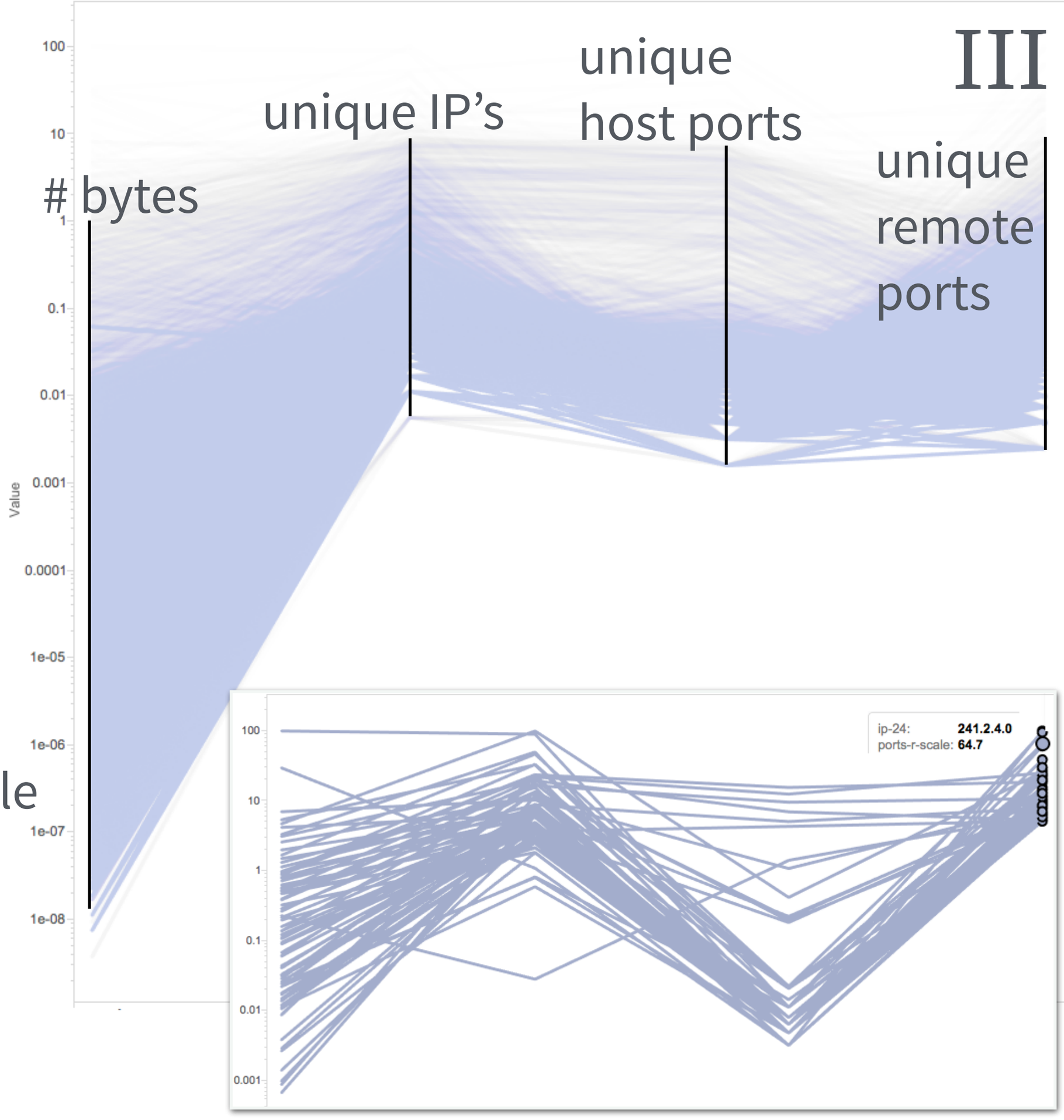


axes are all vertical, can fit 3+

line = /24

can select lines as seen below

note strange scale



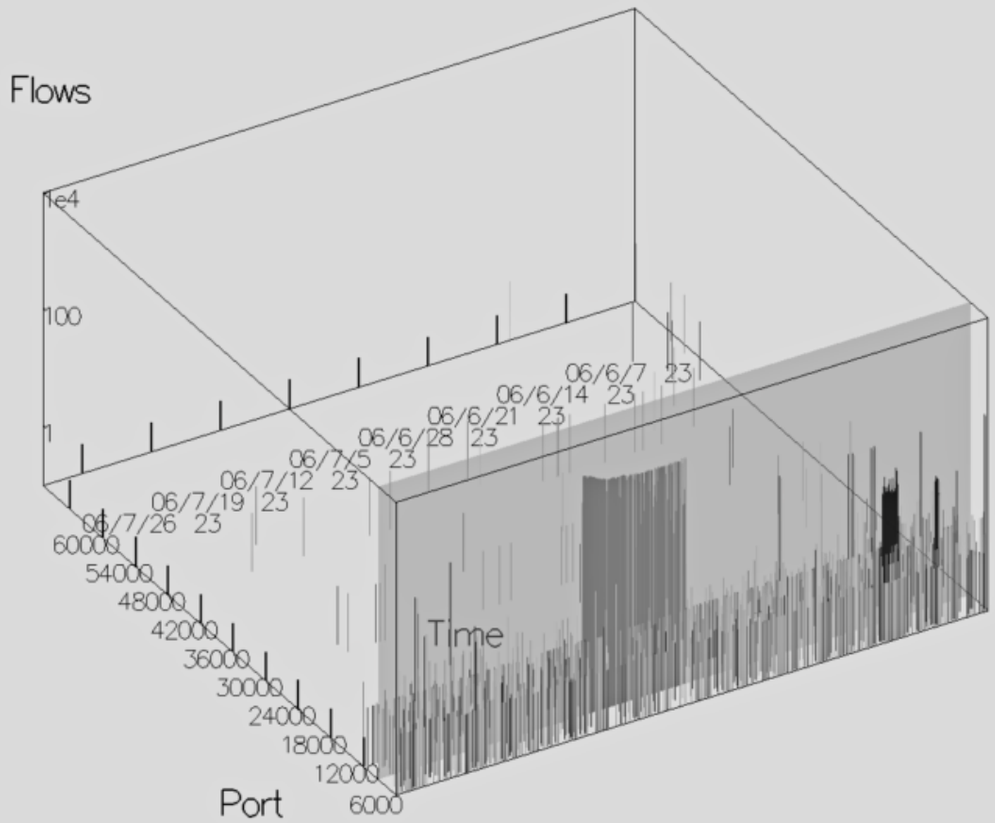
(not your data)

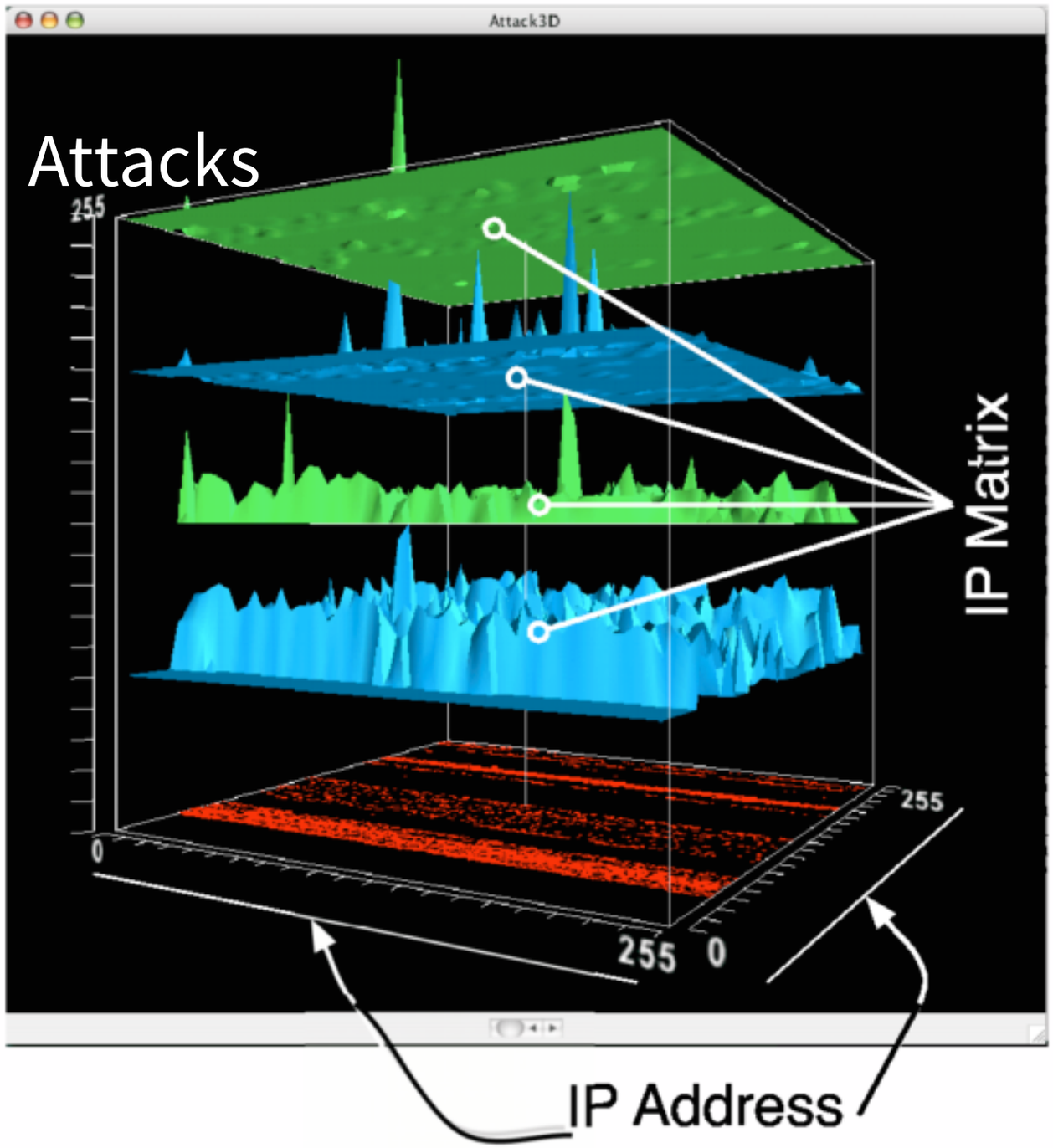
3D graph examples

con:

humans are bad with 3D

thus usually avoided

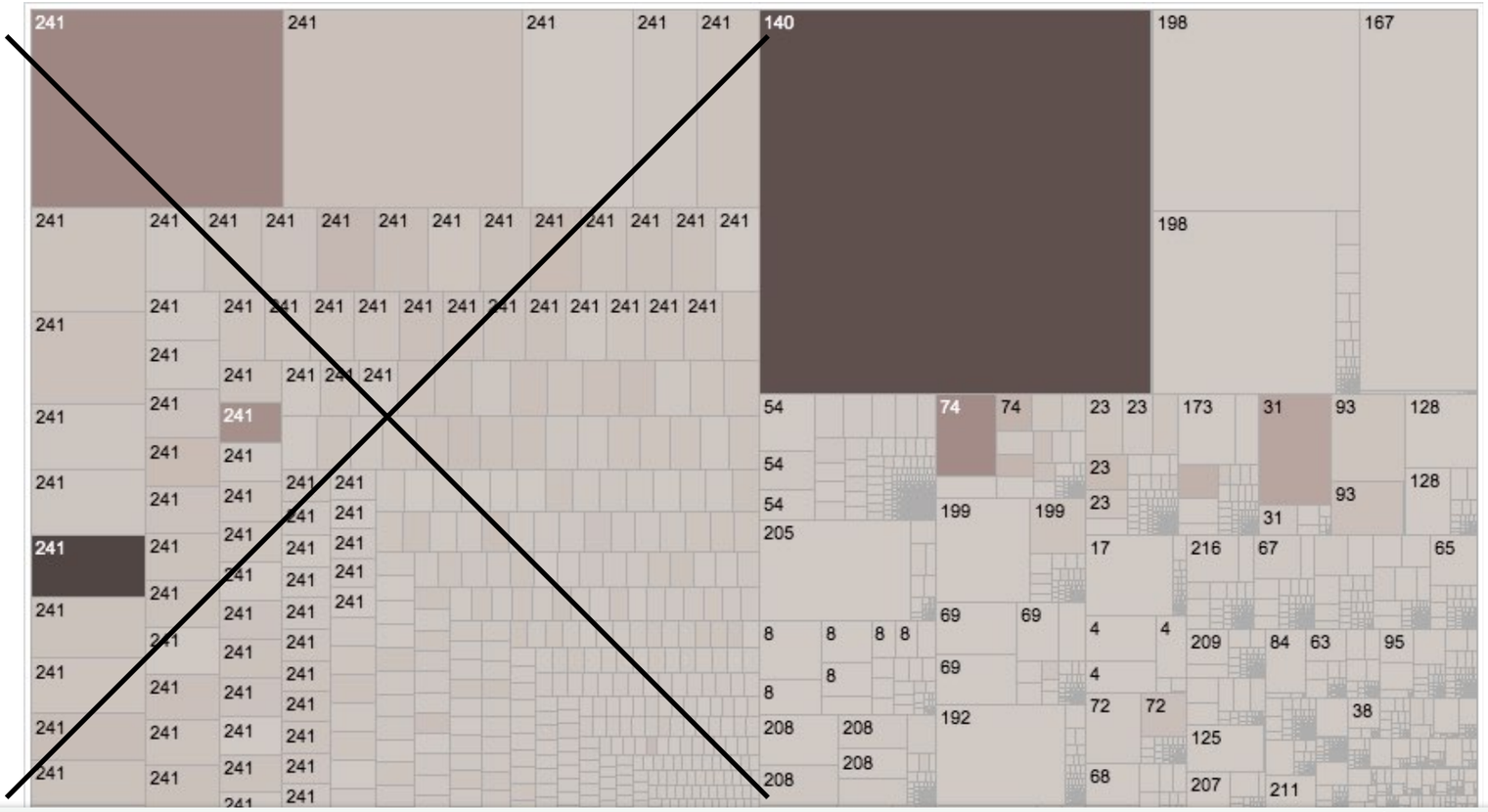


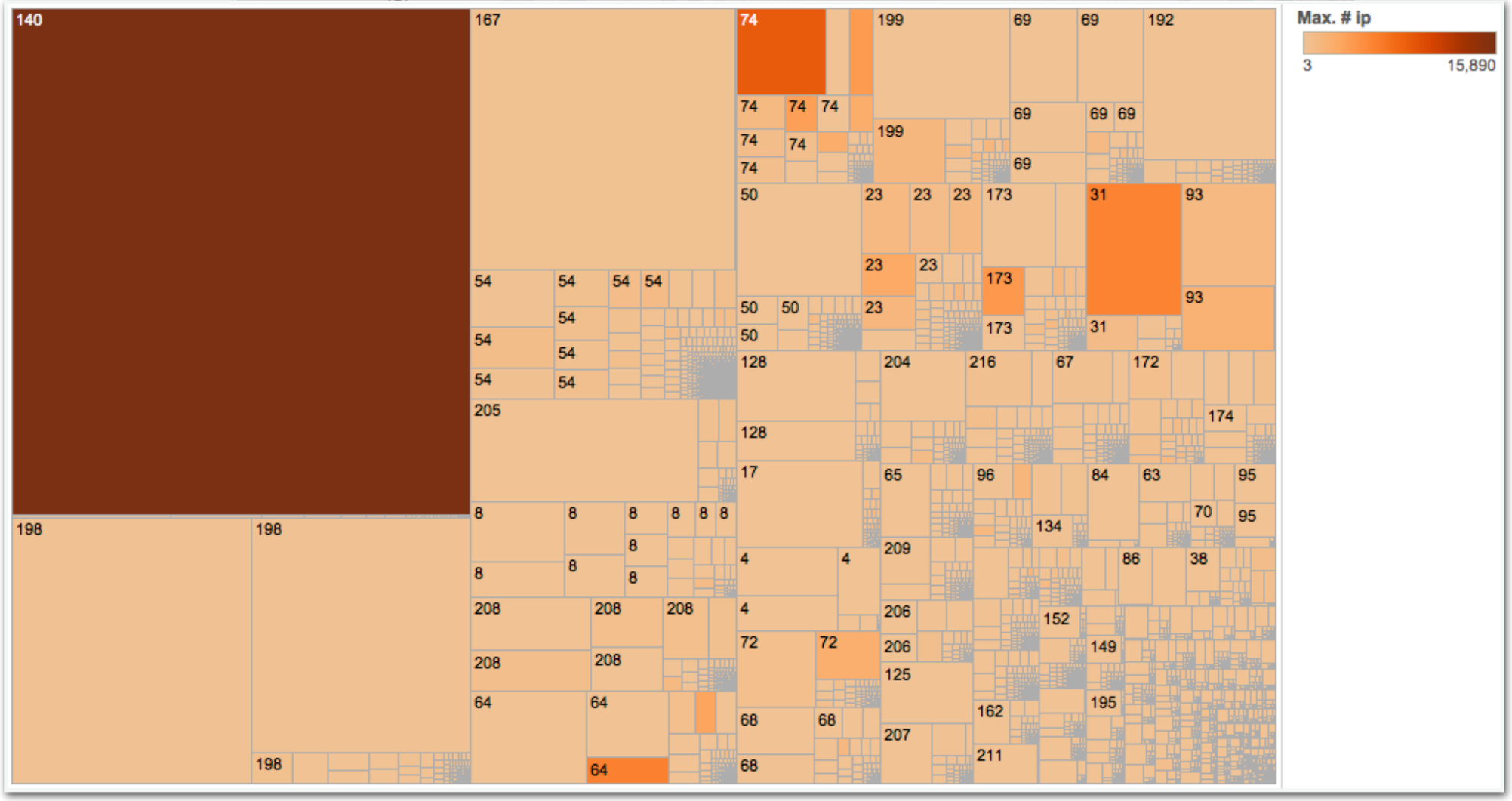


boxes, broken from /8 into /24

colored & sized by unique IP’s

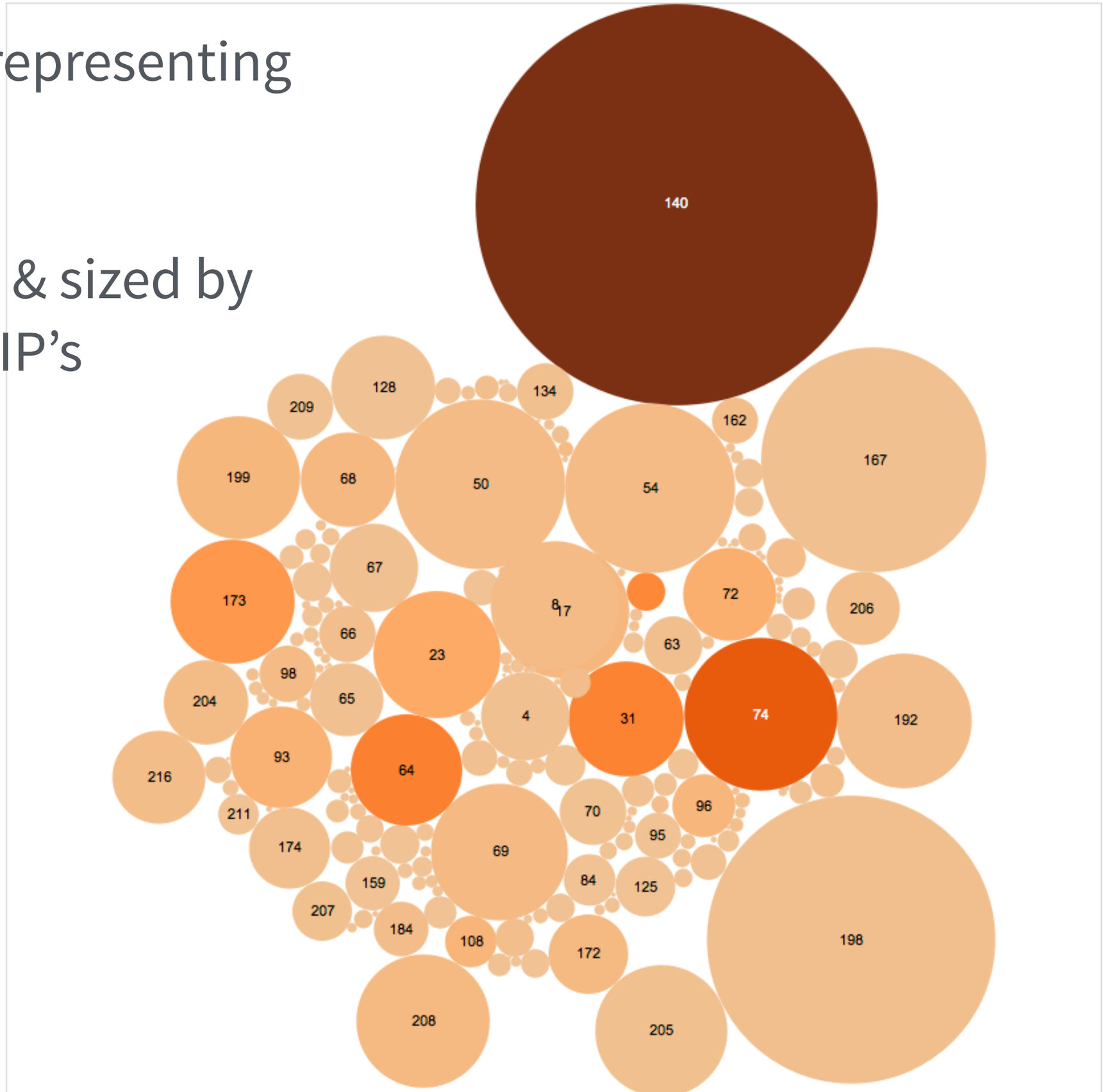
can separate internal vs. external IP’s



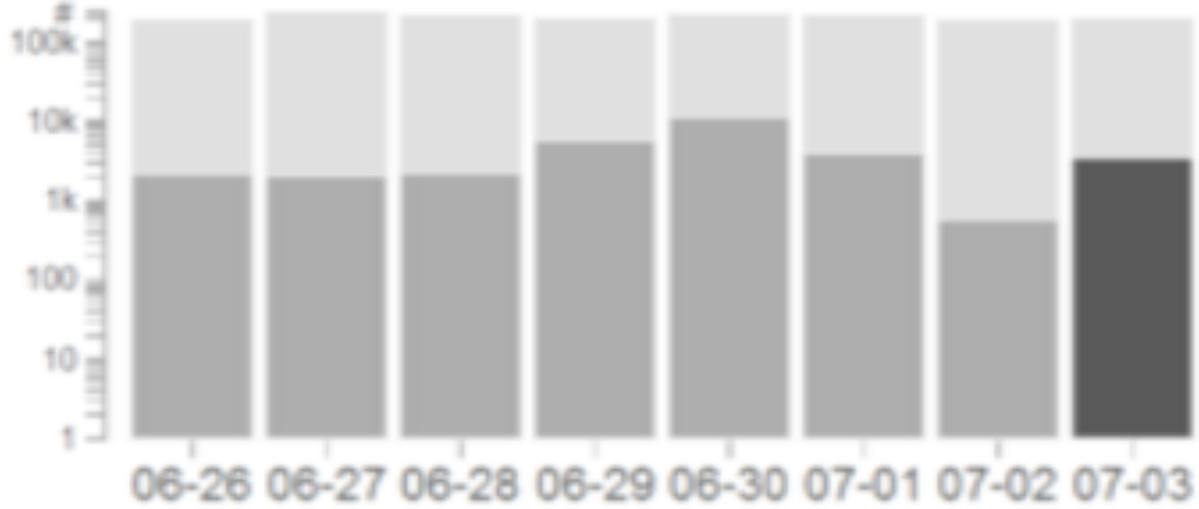


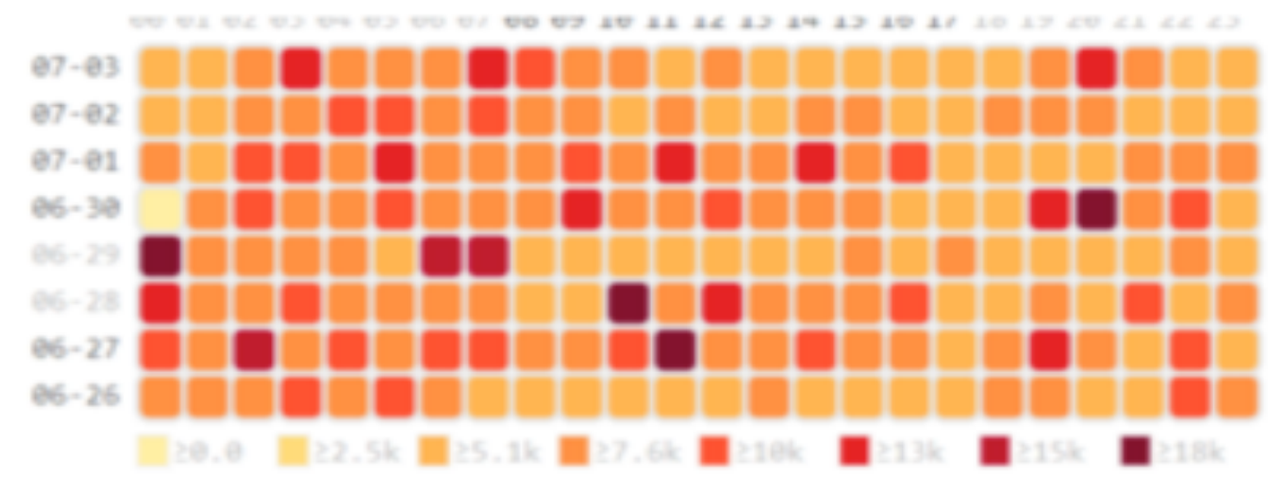
circles representing each /8

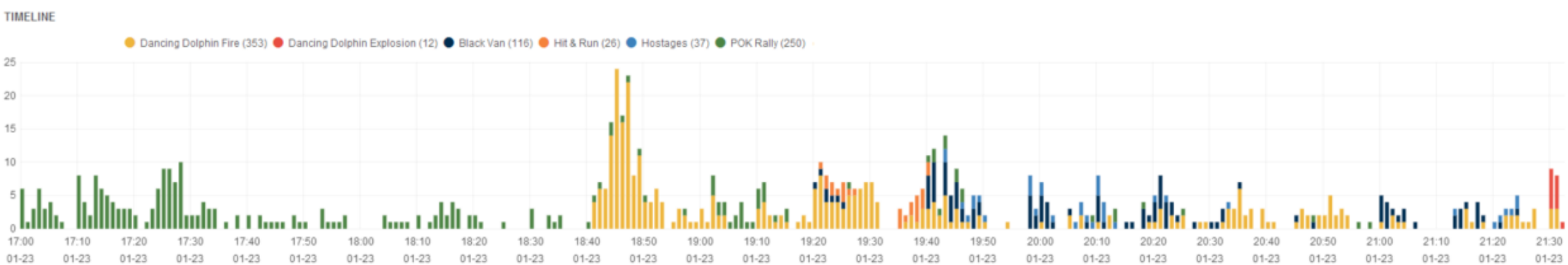
colored & sized by unique IP’s



timelines
(not your data)

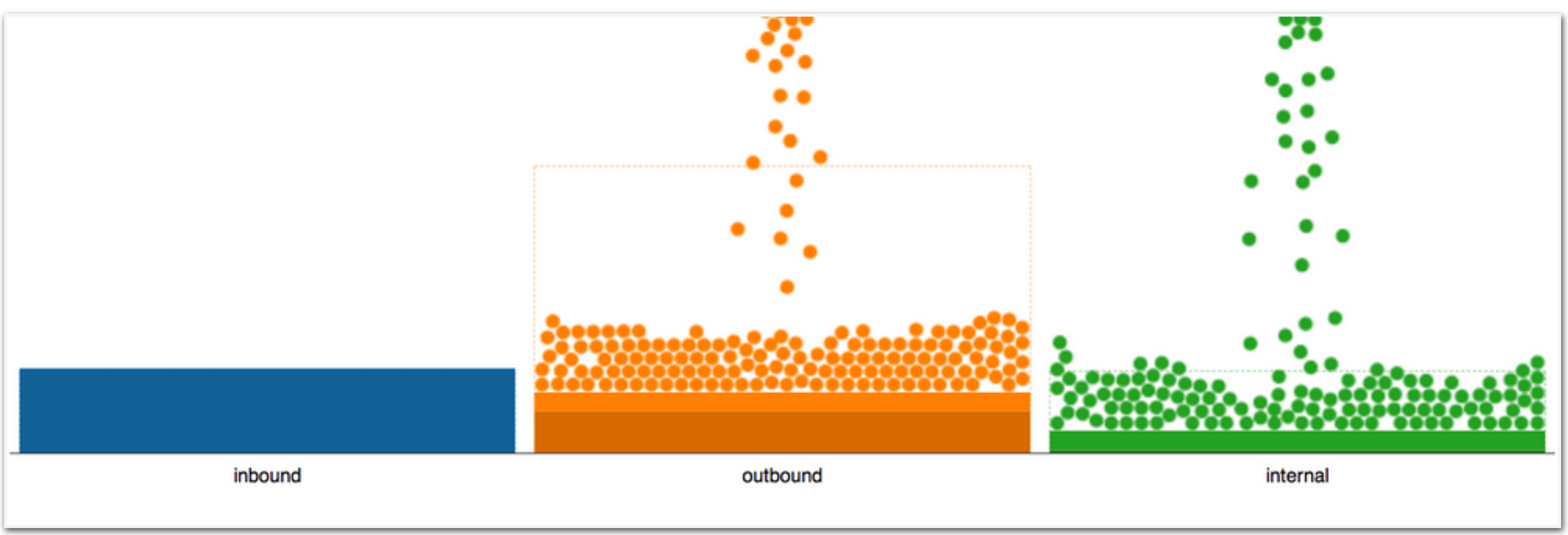






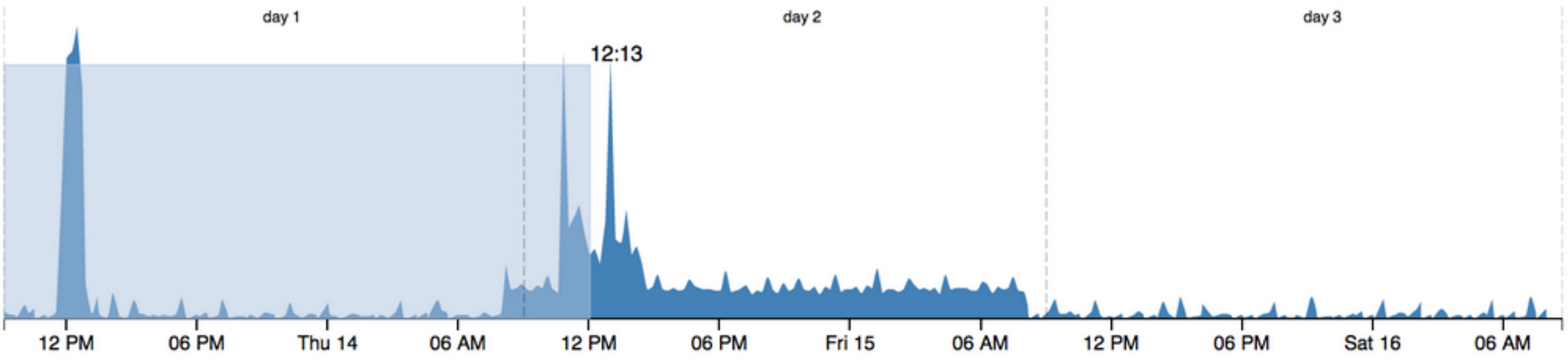
animation
(not your data)

imagine little bubbles falling down, aggregating into bars



interaction
(not your data)

selecting a range of time to visualize
updates other views accordingly…



aggregation
(not your data)

summarizing regions of time
similar to earlier ideas (aggregated into 5 mins)