



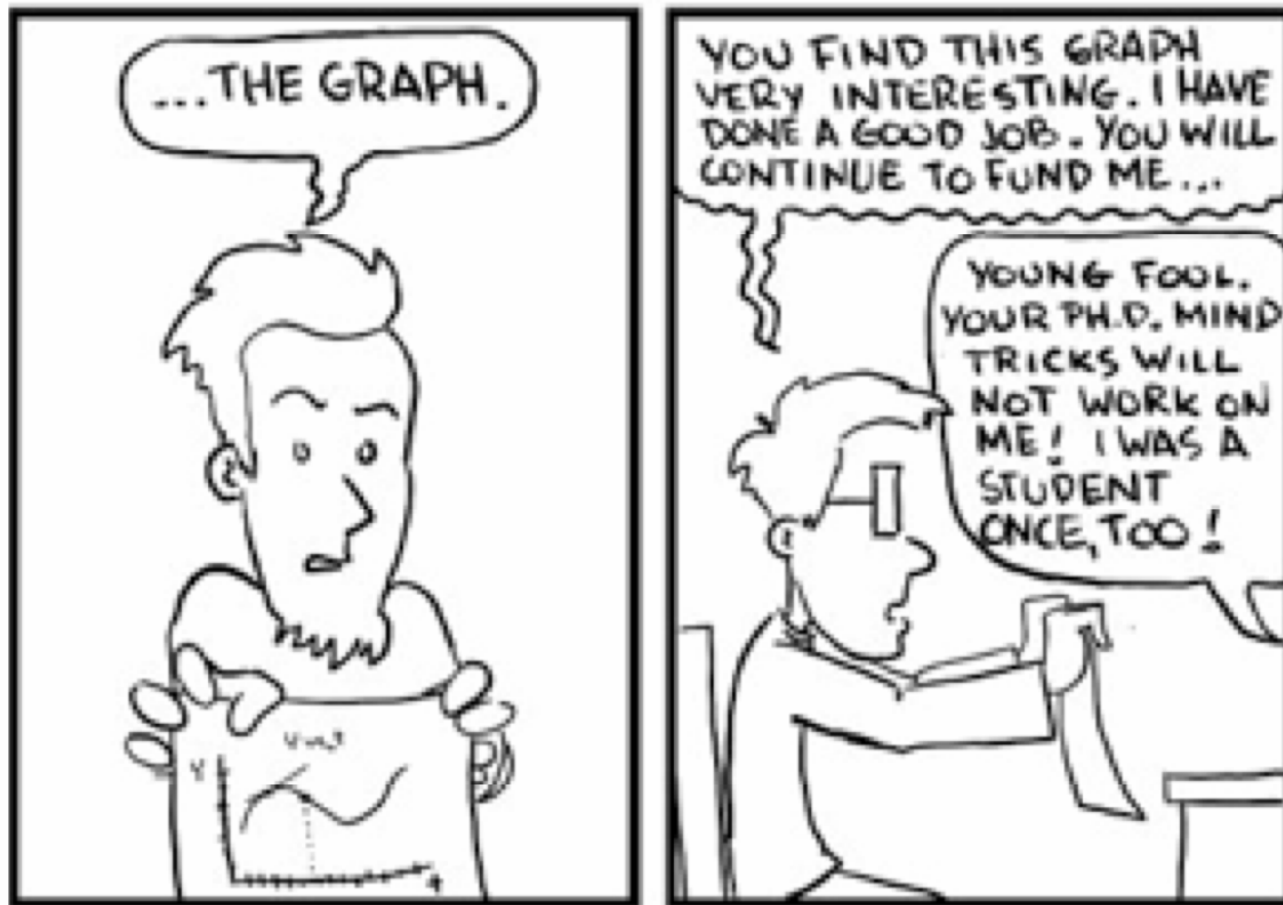
Visualizations of Flow and Analytical Results

**Presentation by: Phil Groce and
Jeff Janies**

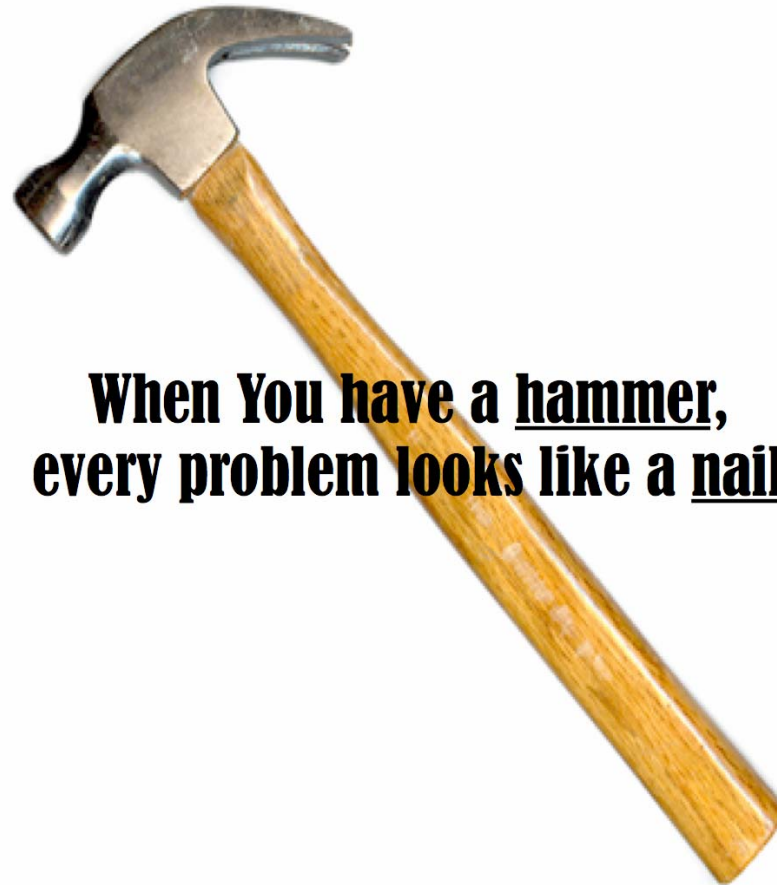
**Network Situational Awareness
group SEI/CERT**



Visualizations are Tools



Visualizations are Tools



**When You have a hammer,
every problem looks like a nail**

Visualizations are Tools



>



Visualizations are Tools



=

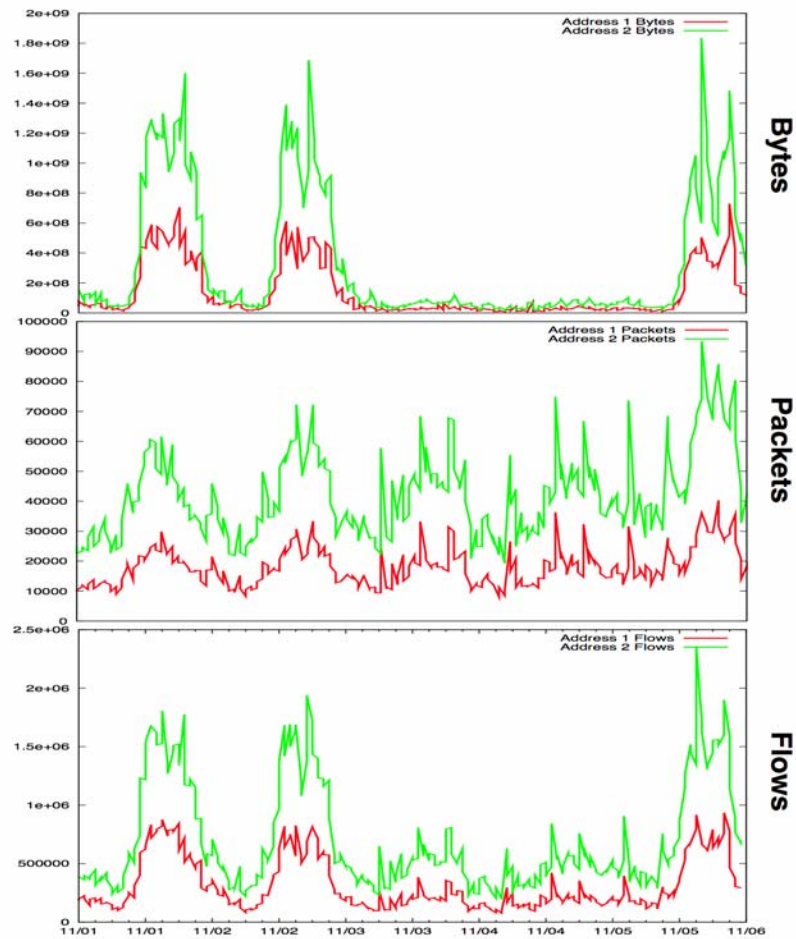




Time Series:

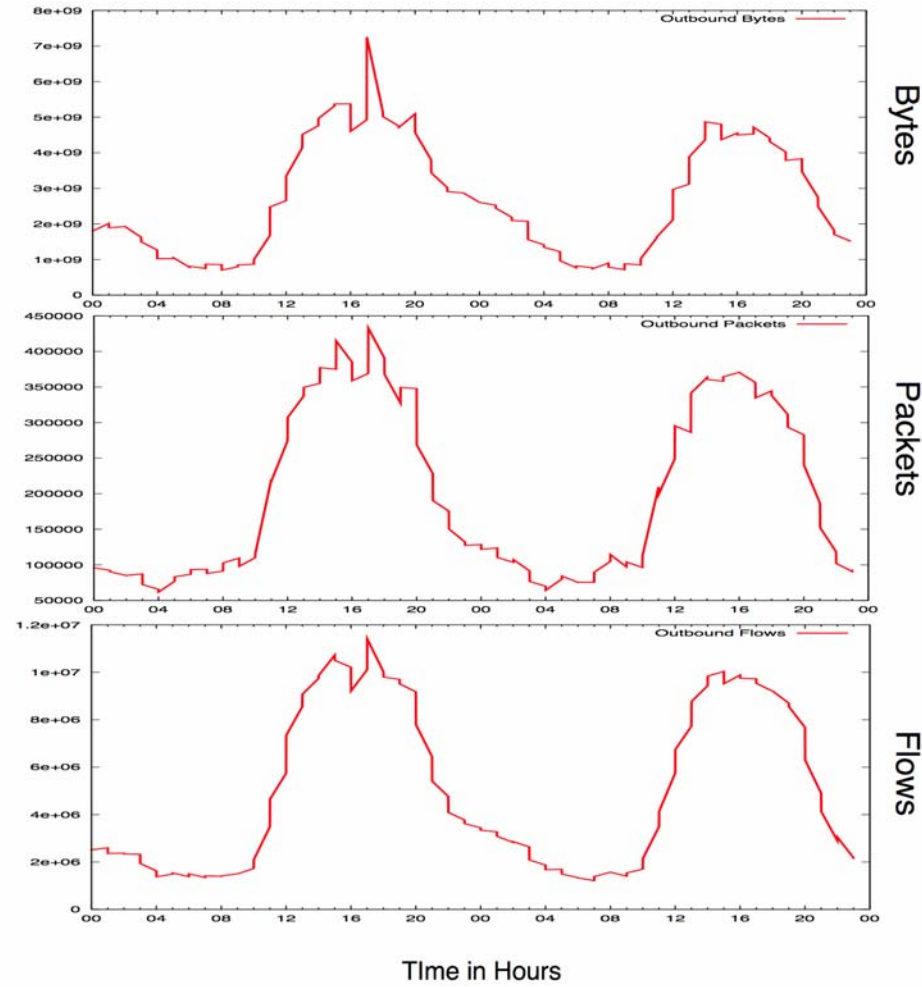
The Tried and True Hammer

Time Series

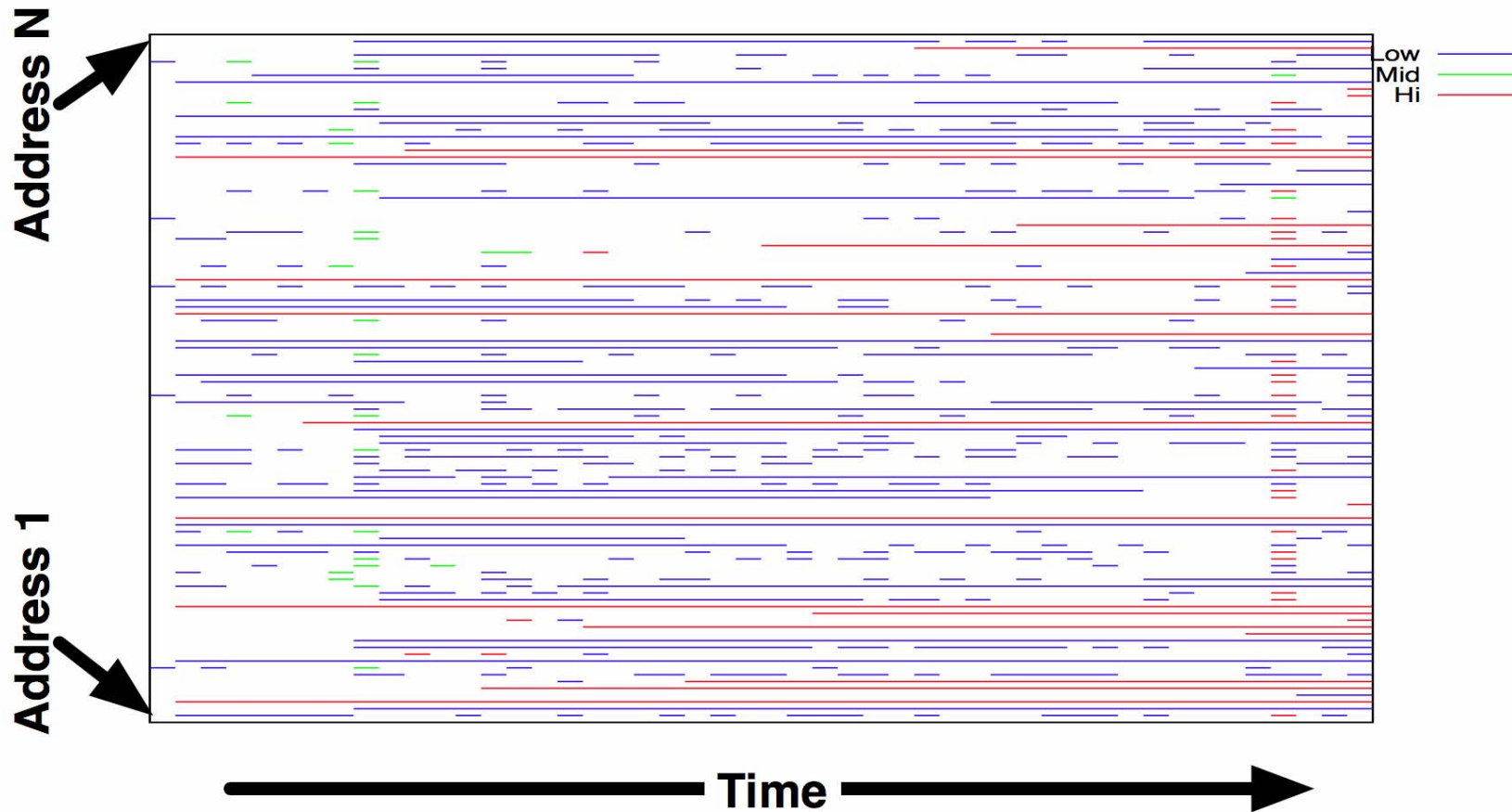


Time Series

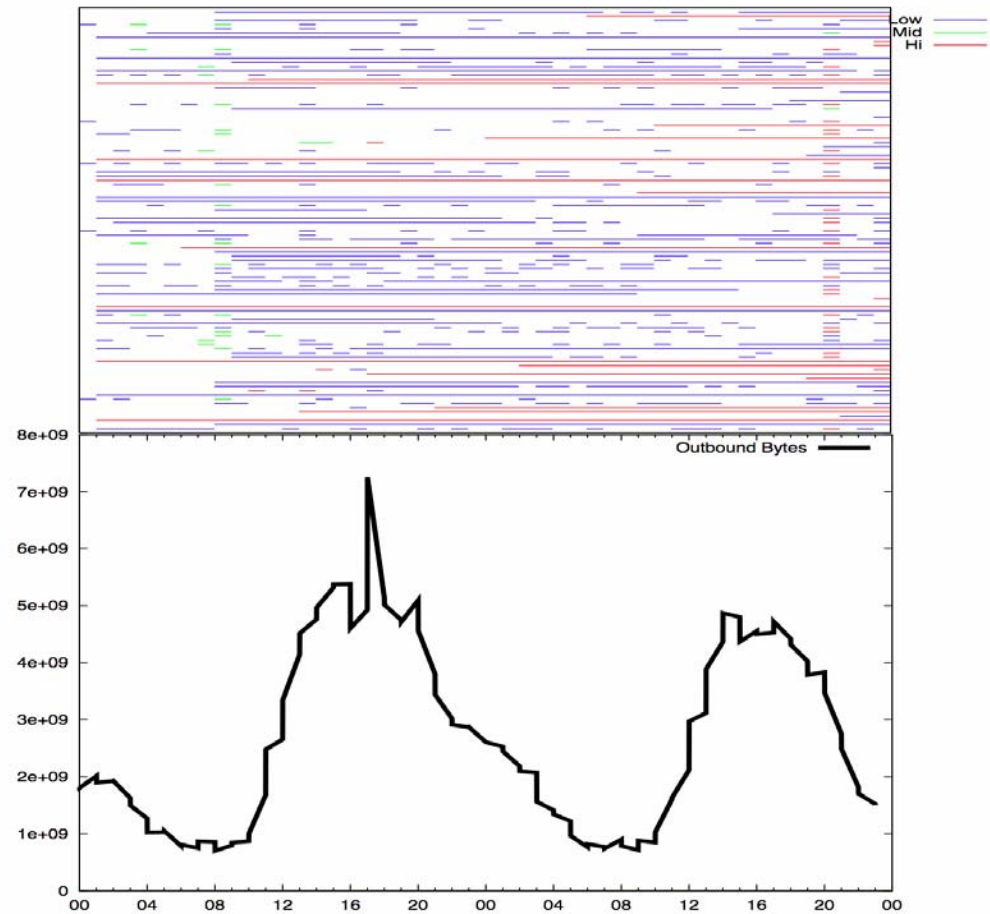
Total Activity For All 100 Hosts



Existence Plots



Existence Plots





Plotting Relationships

Plotting Relationships

US commercial paper and Treasury bills

3-month rates (%)

- Treasury Bills
- Nonfinancial A2/P2 rated
- Financial (asset backed) AA rated

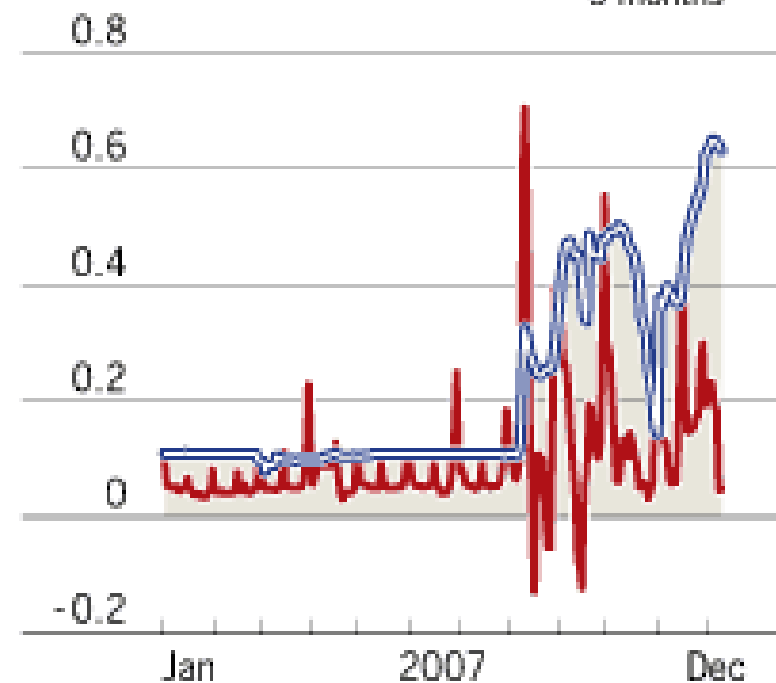


Source: Thomson Datastream

Dollar libor spreads

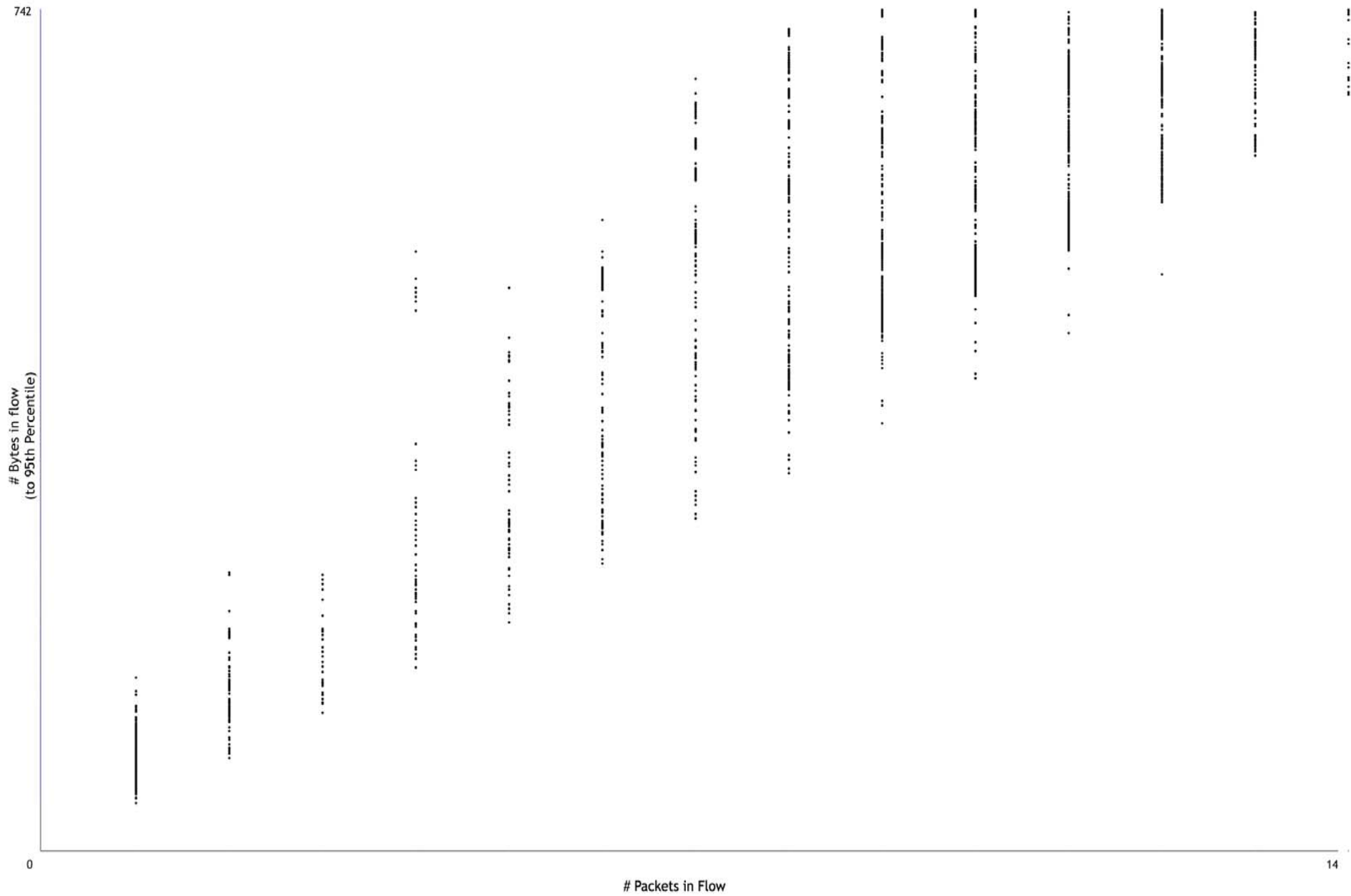
Over Fed Funds target rate
(% points)

- Overnight
- 3 months



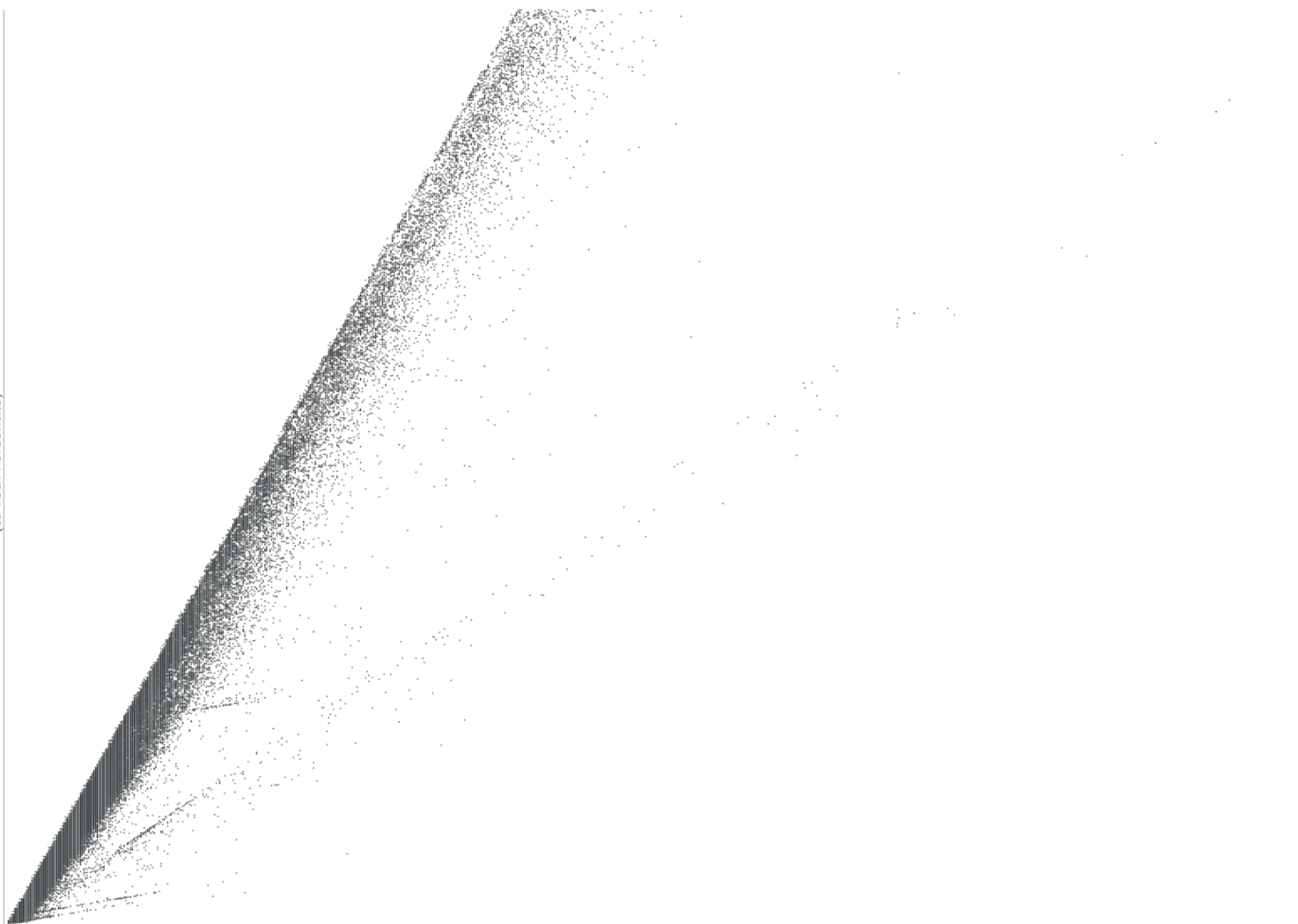
Source: Thomson Datastream

smtp.example.com - Bytes Against Packets
12/01/2007



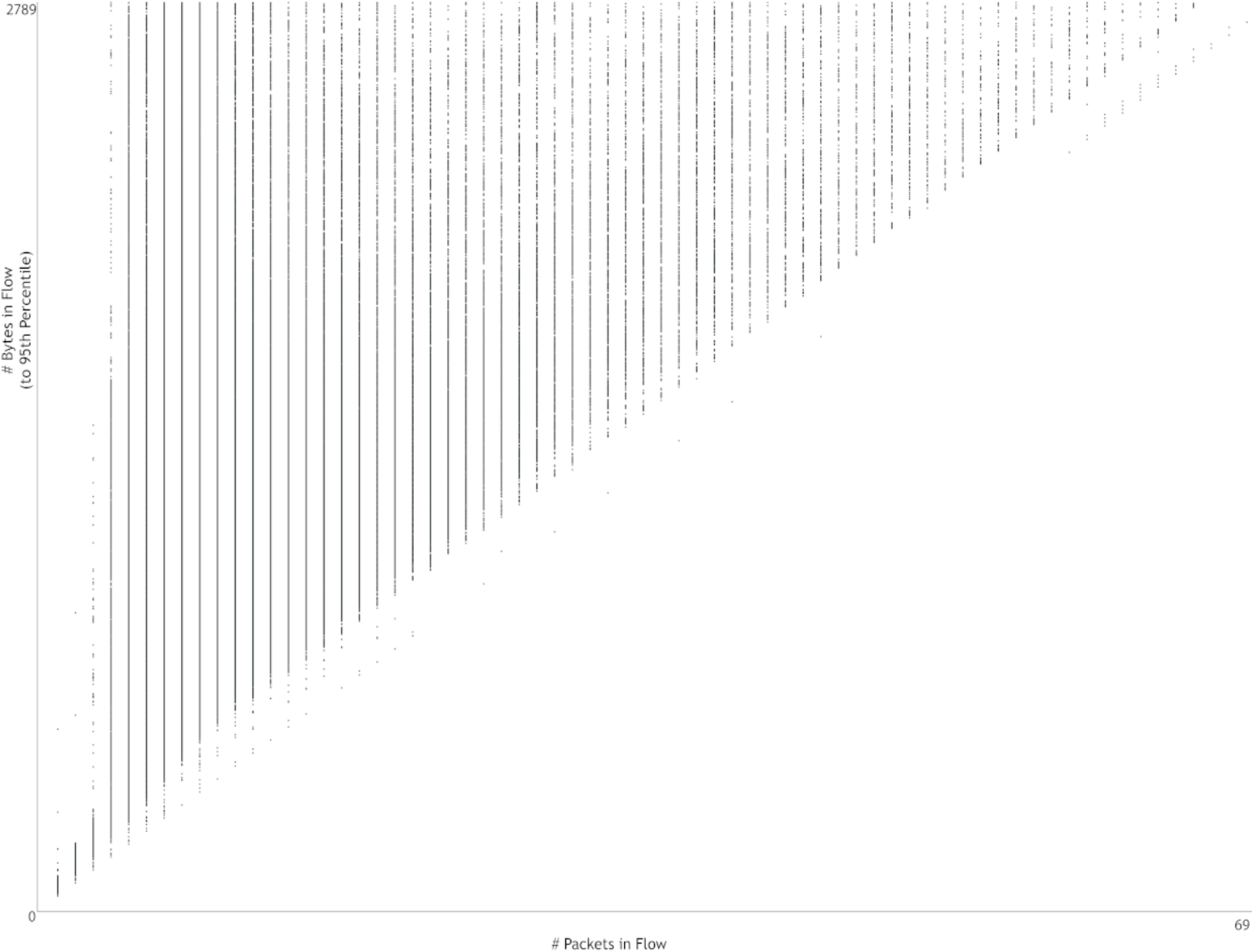
450095

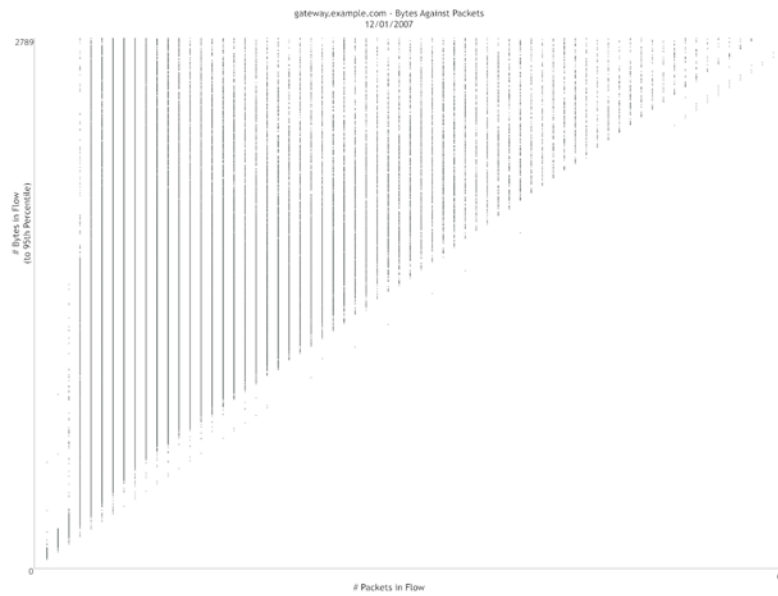
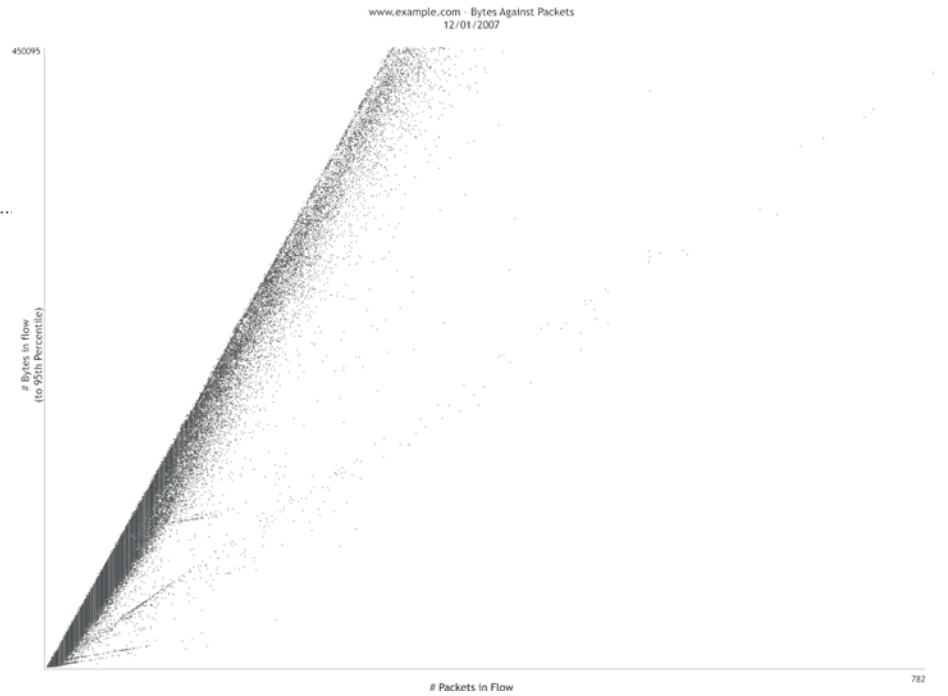
Bytes in flow
(to 95th Percentile)

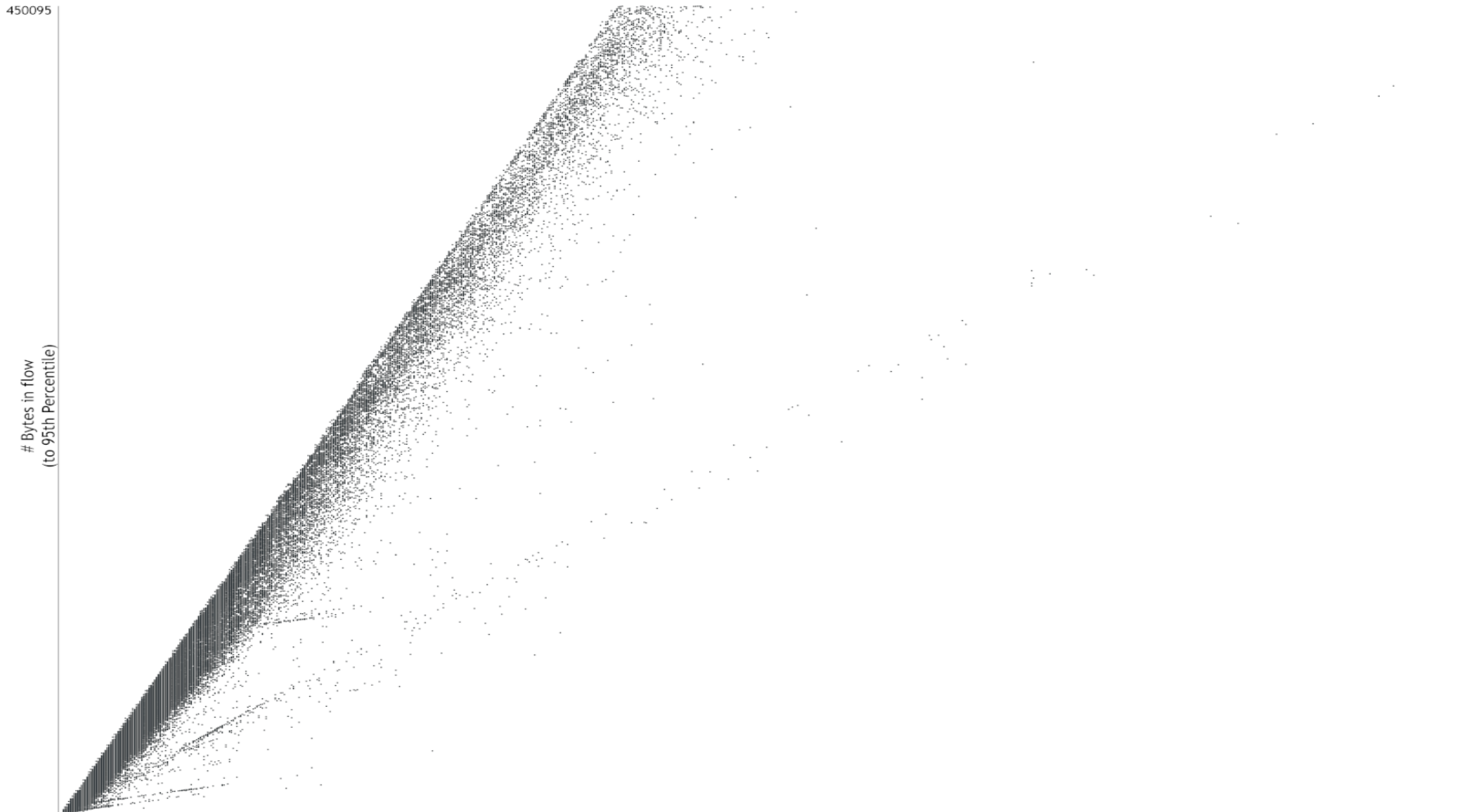


Packets in Flow

782





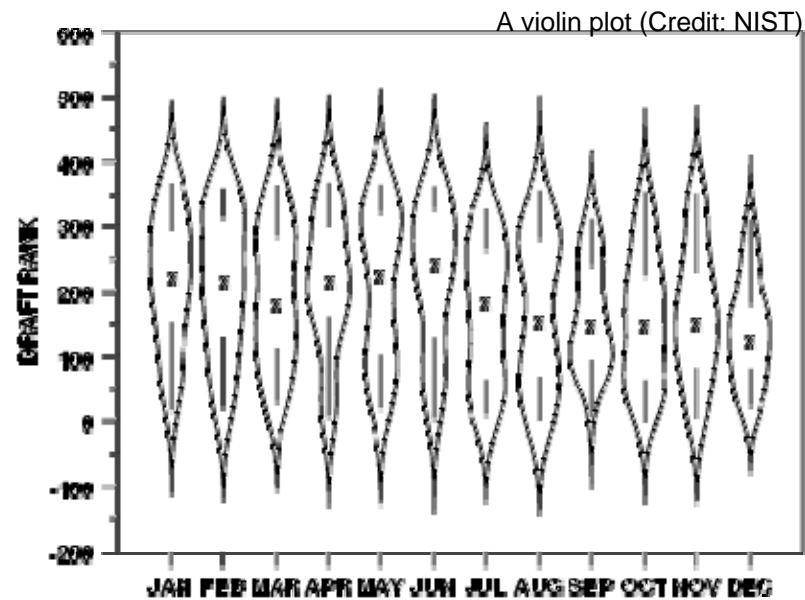
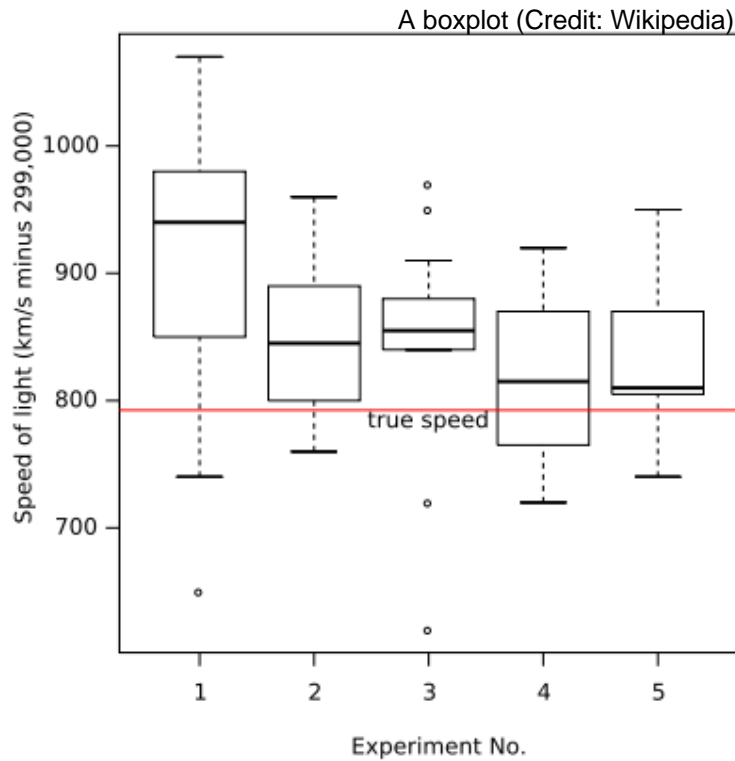




Plotting Distributions:

How a variable relates to itself

Box and Violin Plots

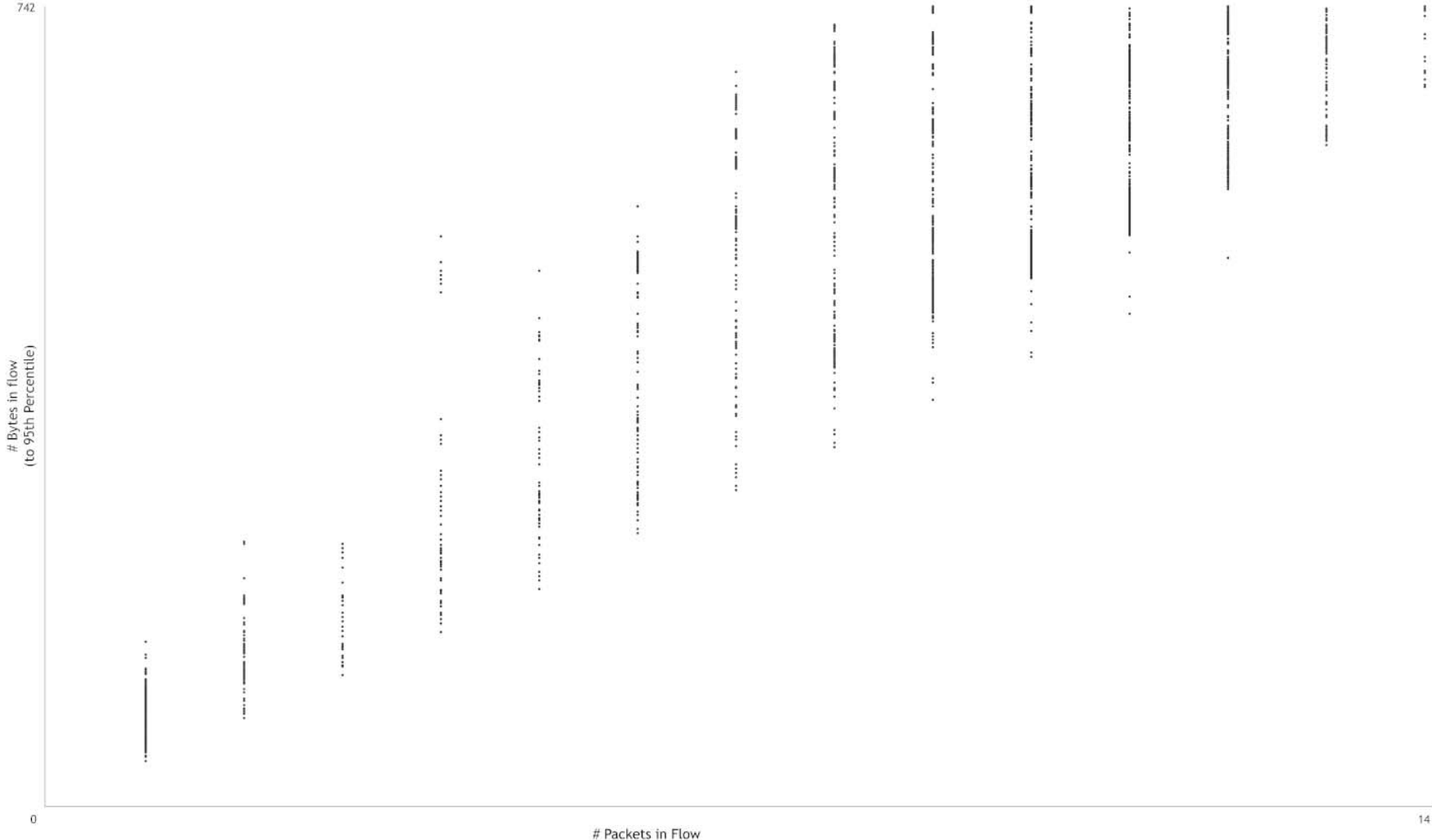


example.com Flow Volume, Binned by Bytes per Packet
2007/12/01



The X axis is bytes per packet in 5-byte increments. The Y axis shows the quantity of flows in each bin. Red indicates flow activity by known scanners.

smtp.example.com - Bytes Against Packets
12/01/2007

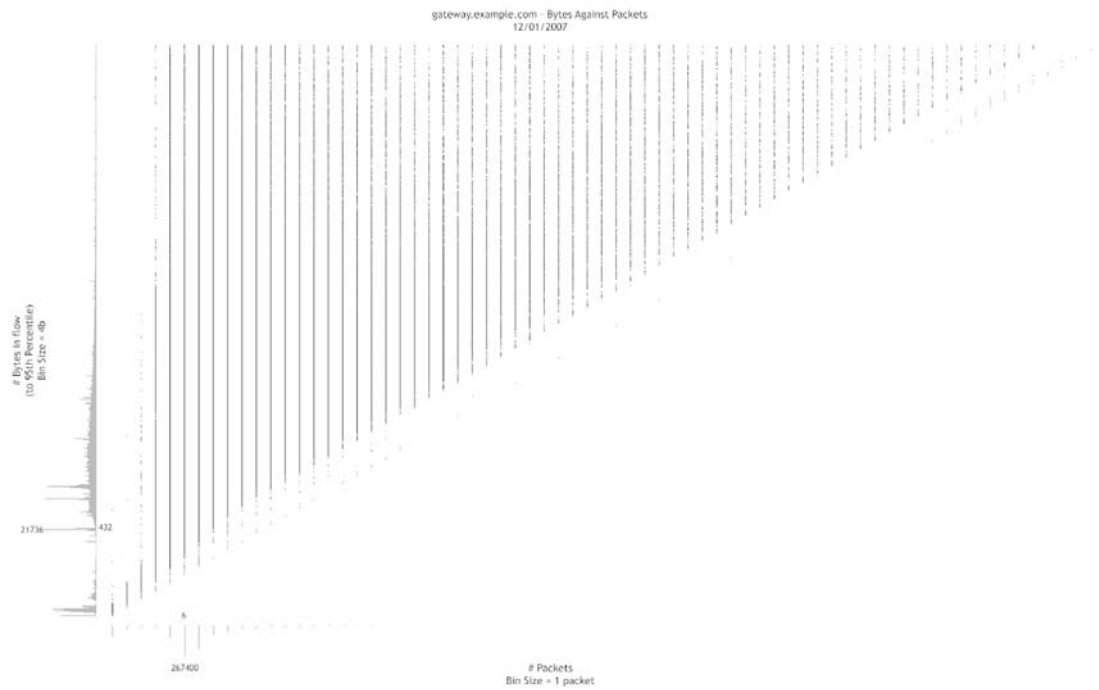
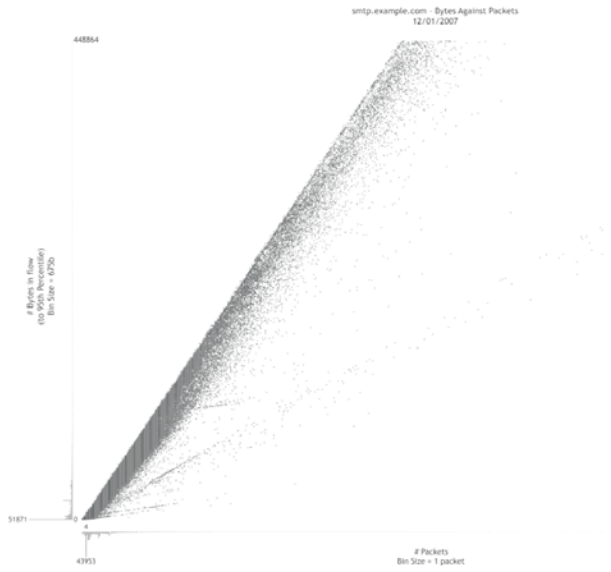


smtp.example.com - Bytes Against Packets
12/01/2007



smtp.example.com - Bytes Against Packets
12/01/2007







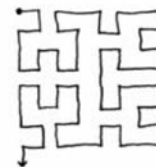
Hilbert Curve:

Broad Scale Visualization

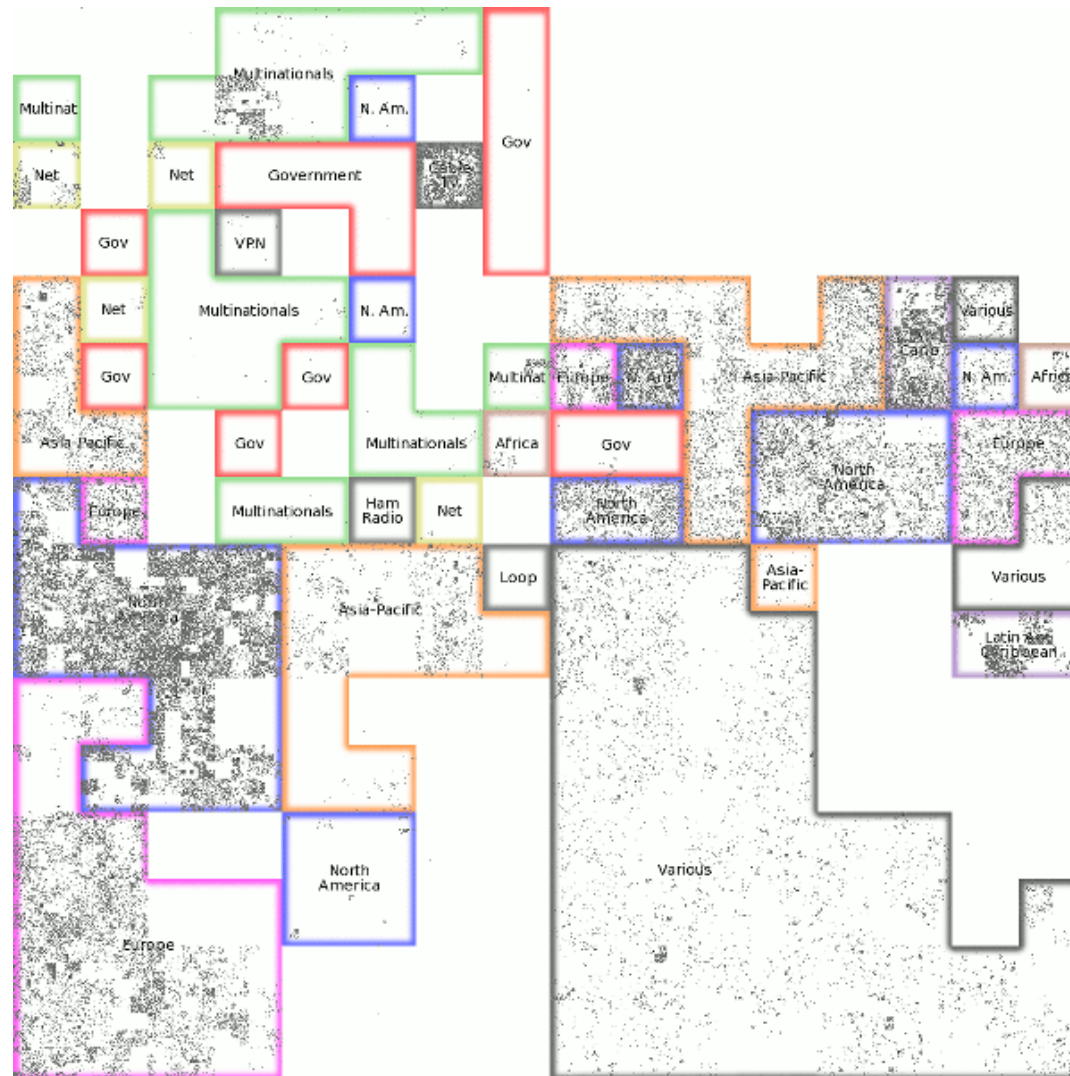
Hilbert Curve



0 1 14 15 16 19 →
3 2 13 12 17 18
4 7 8 11
5 6 9 10



Hilbert Curve (The Movie)



Additional Resources

The R Project. *Introduction to R*. Chapter 13: Graphics. <http://cran.r-project.org/doc/manuals/R-intro.html#Graphics>

Tufte, E. R. *The Visual Display of Quantitative Information*. Cheshire, CT: Graphics Press, 1983.

Tufte, E. R. *Envisioning Information*. Cheshire, CT: Graphics Press, 1990.

Tufte, E. R. *Visual Explanations: Images and Quantities, Evidence and Narrative*. Cheshire, CT: Graphics Press, 1997.

Tufte, E. R. *Beautiful Evidence*. Cheshire, CT: Graphics Press, 2006.

Wilkinson, L., et al. *The Grammar of Graphics*. New York: Springer-Verlag, 1999.