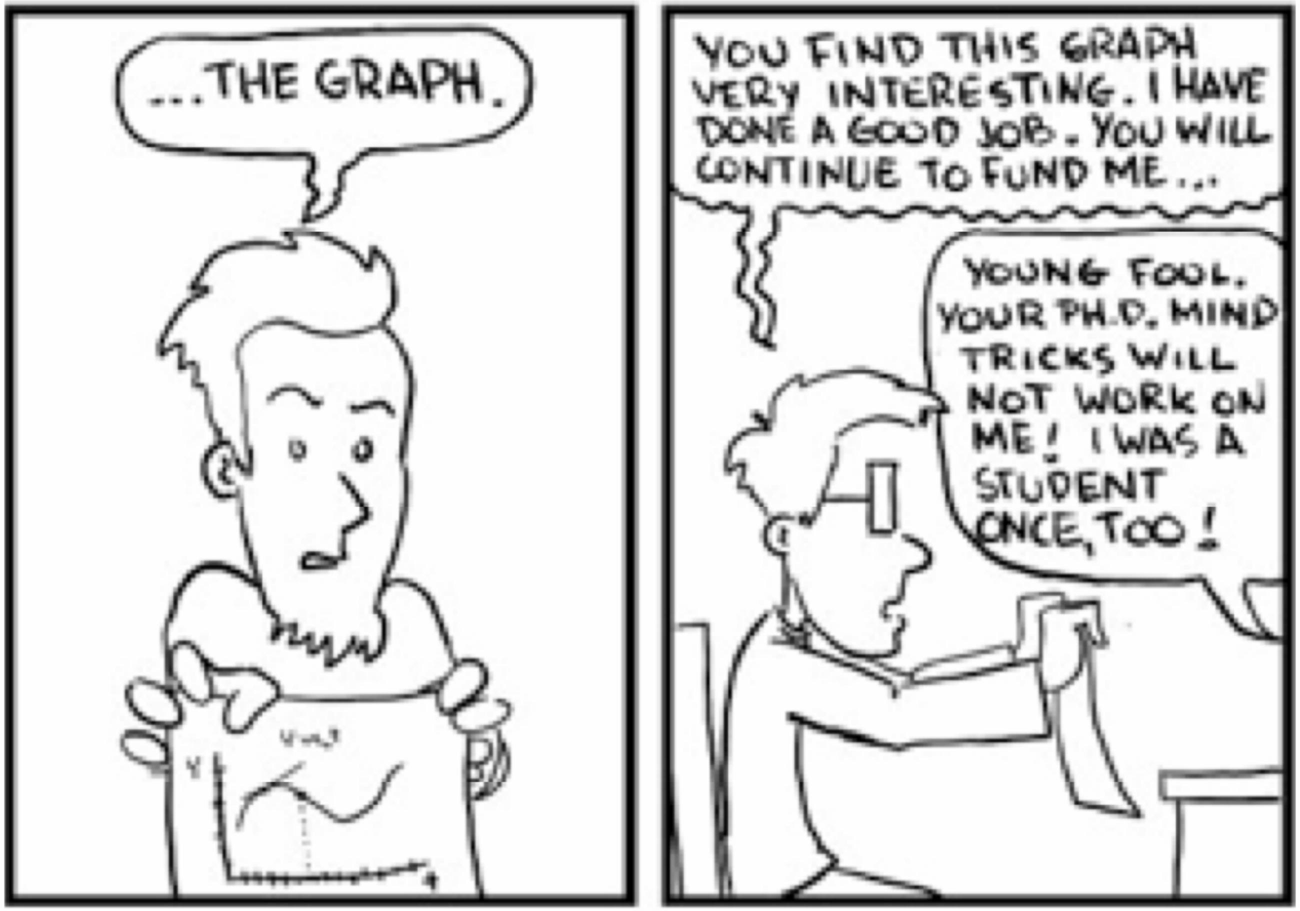
Visualizations of Flow and Analytical Results

Presentation by: Phil Groce and
Jeff Janies
Network Situational Awareness group SEI/CERT

Visualizations are Tools


...THE GRAPH.
YOU FIND THIS GRAPH VERY INTERESTING. I HAVE DONE A GOOD JOB. YOU WILL CONTINUE TO FUND ME...
YOUNG FOOL. YOUR PH.D. MIND TRICKS WILL NOT WORK ON ME! I WAS A STUDENT ONCE, TOO!

Visualizations are Tools

Visualizations are Tools

>

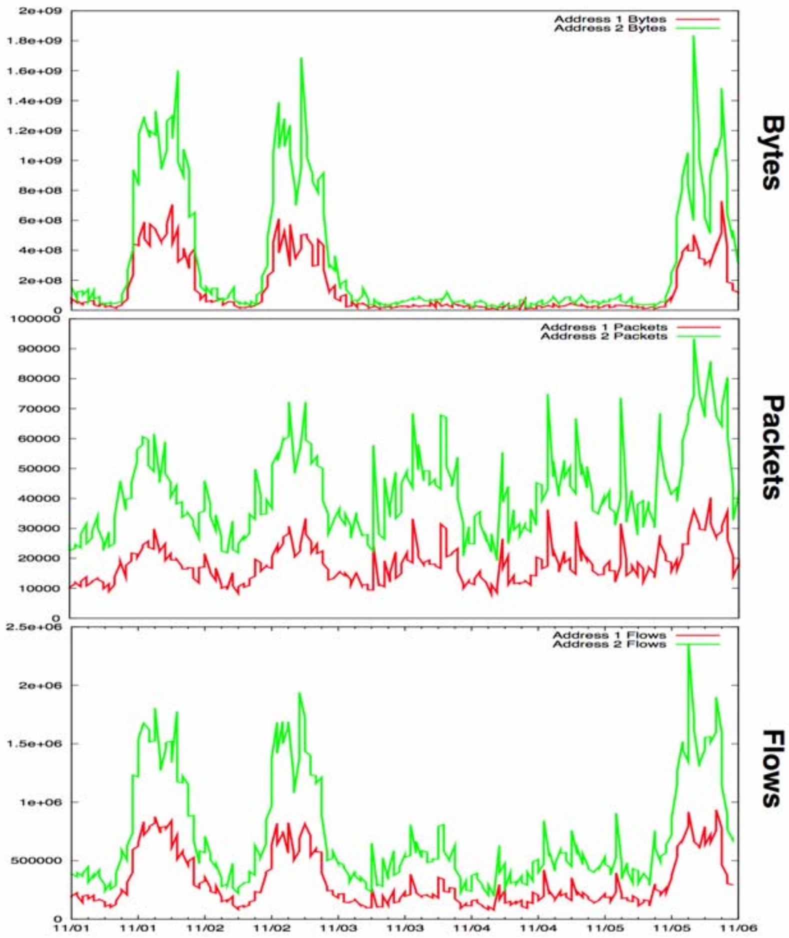
Visualizations are Tools

∈

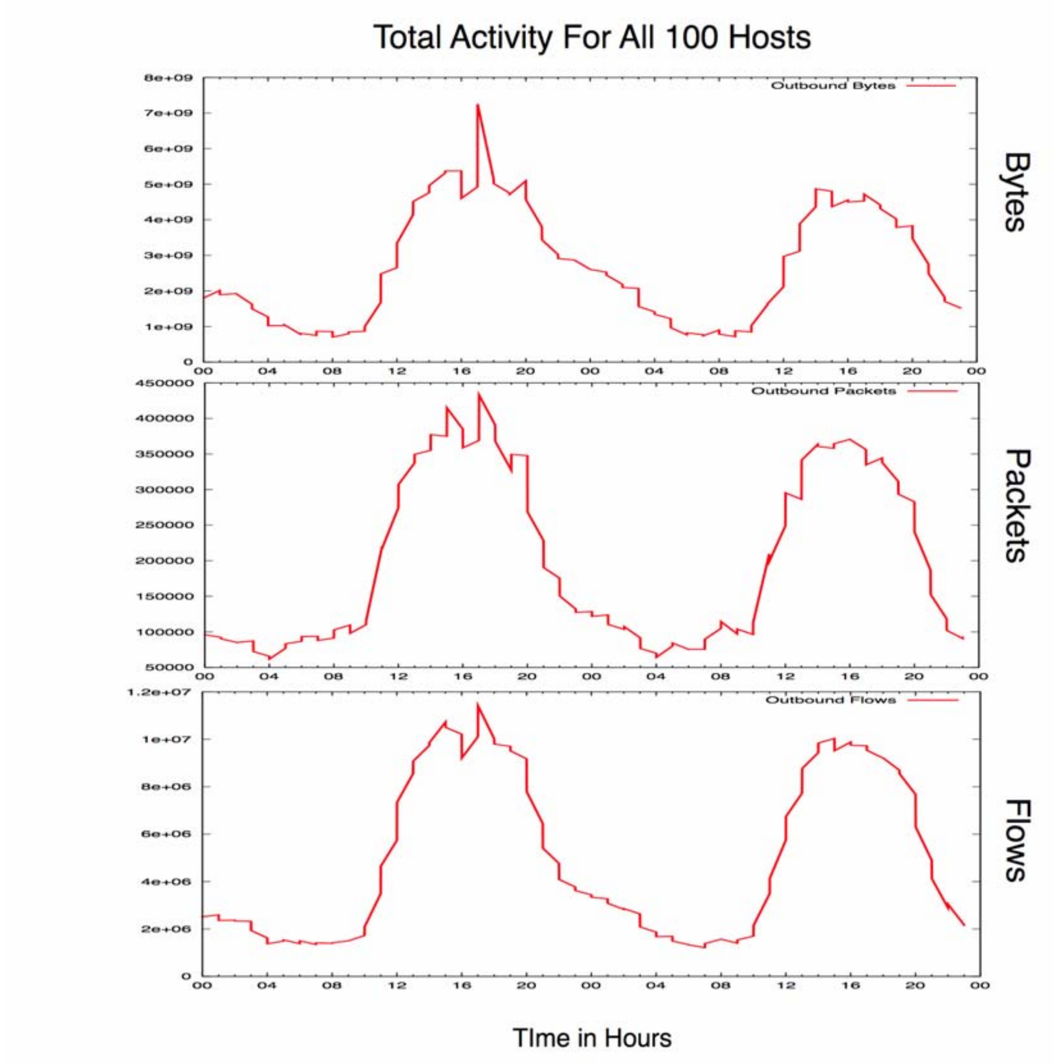
Time Series:

The Tried and True Hammer

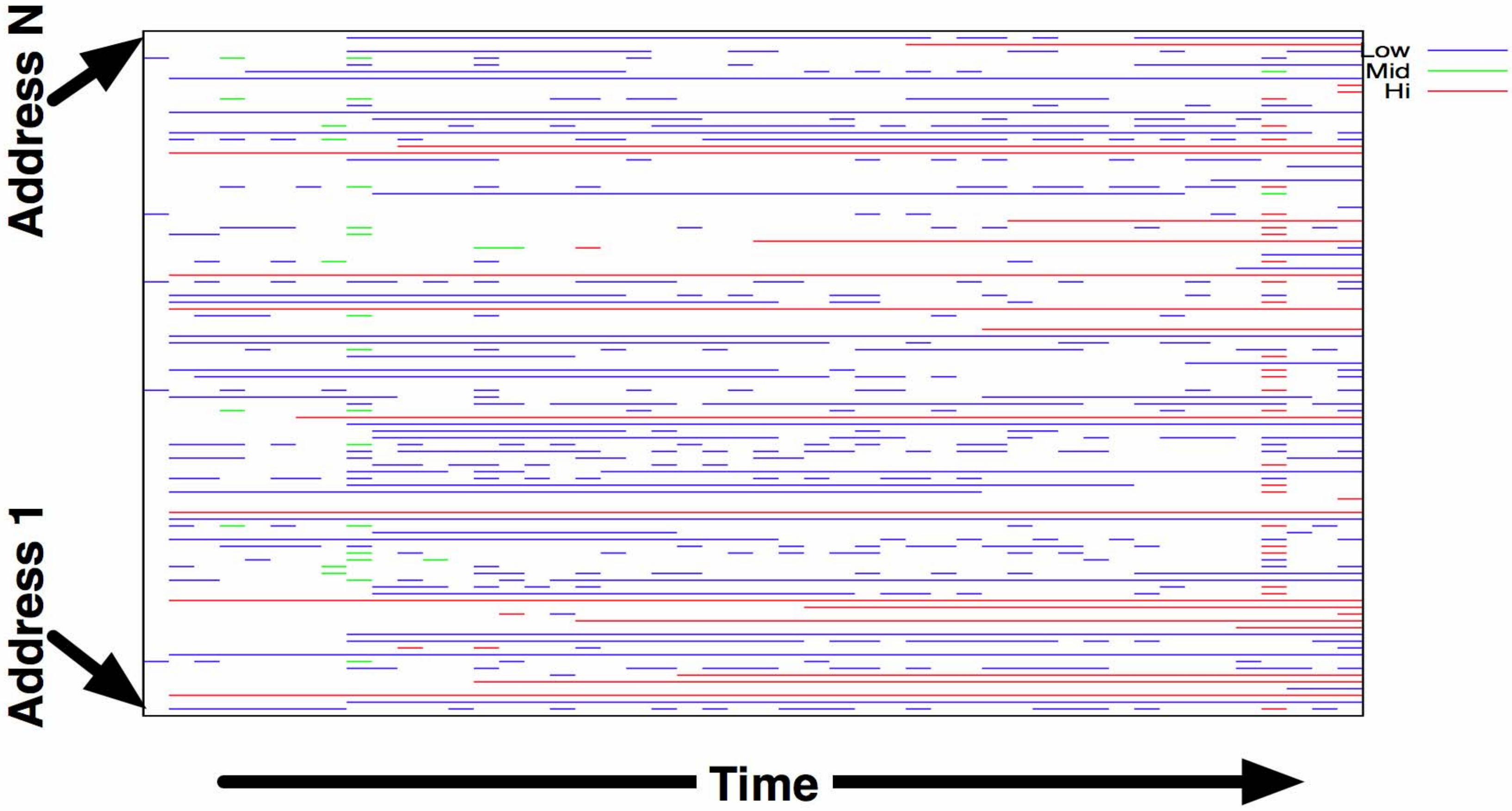
Time Series


Address 1 Bytes
Address 2 Bytes
2e+09
1.8e+09
1.6e+09
1.4e+09
1.2e+09
1e+09
8e+08
6e+08
4e+08
2e+08
0
Bytes
Address 1 Packets
Address 2 Packets
100000
90000
80000
70000
60000
50000
40000
30000
20000
10000
0
Packets
Address 1 Flows
Address 2 Flows
2.5e+06
2e+06
1.5e+06
1e+06
500000
0
Flows
11/01
11/01
11/02
11/02
11/03
11/03
11/04
11/04
11/05
11/05
11/06

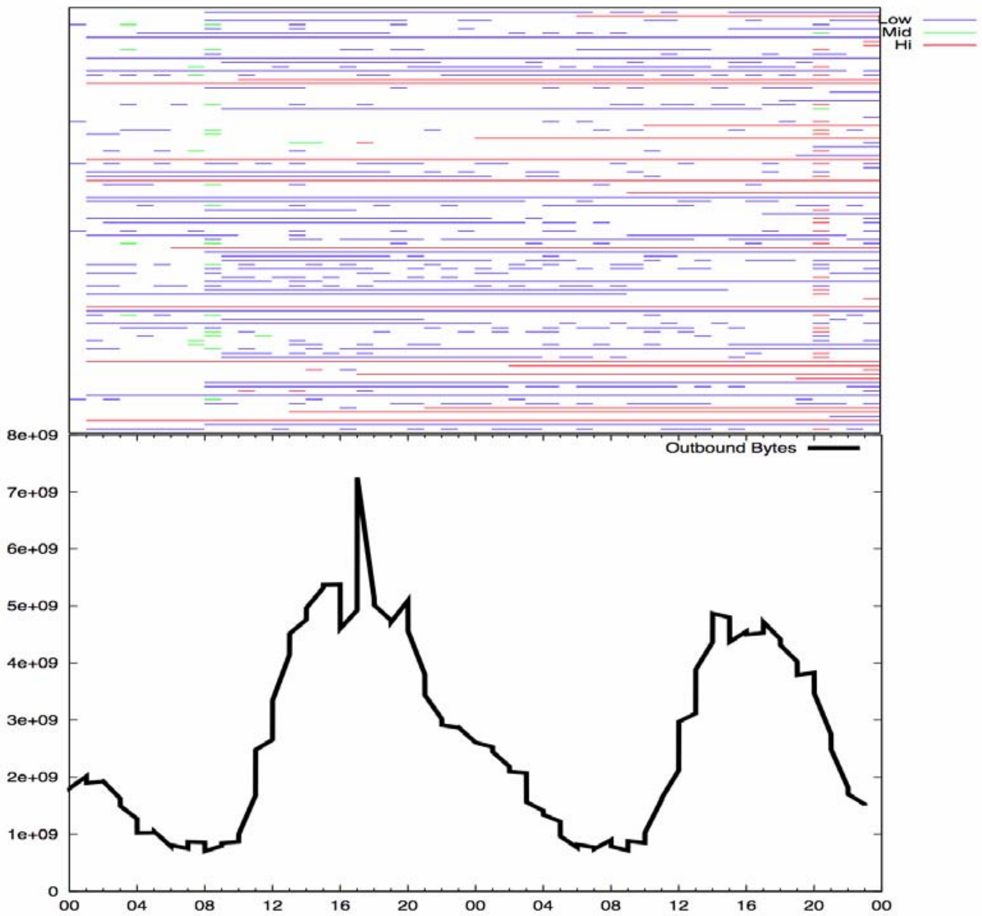
Time Series


Total Activity For All 100 Hosts
Outbound Bytes
Bytes
8e+09
7e+09
6e+09
5e+09
4e+09
3e+09
2e+09
1e+09
0
Outbound Packets
Packets
450000
400000
350000
300000
250000
200000
150000
100000
50000
Outbound Flows
Flows
1.2e+07
1e+07
8e+06
6e+06
4e+06
2e+06
0
00
04
08
12
16
20
00
04
08
12
16
20
00
TIme in Hours

Existence Plots

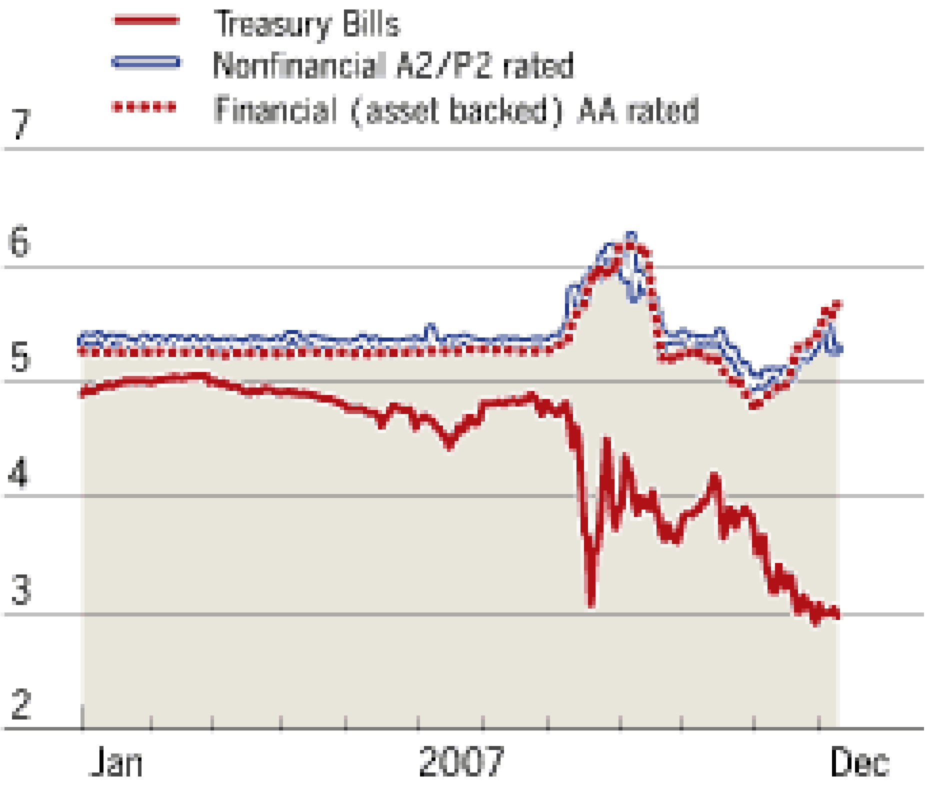


Existence Plots



Plotting Relationships

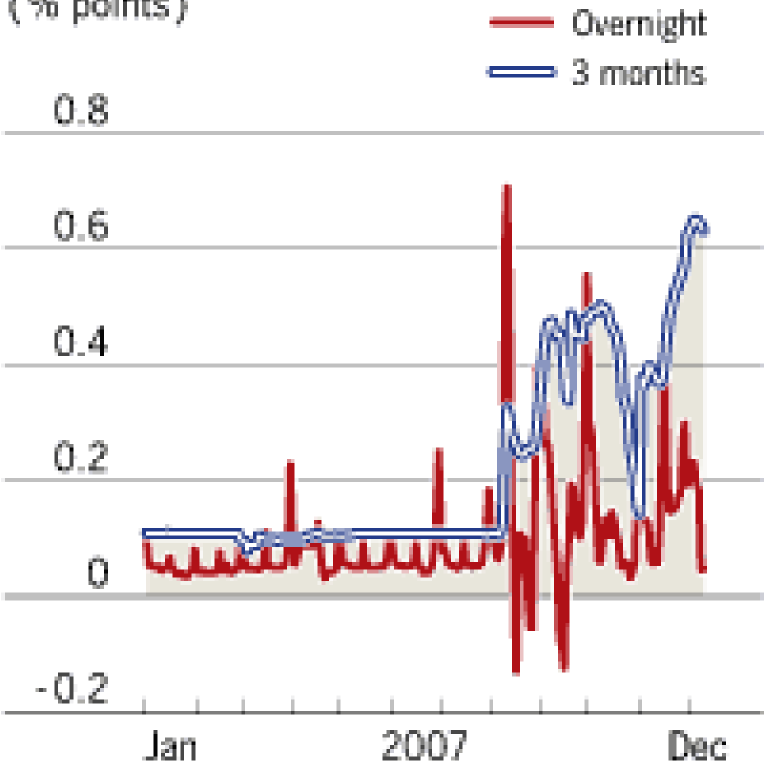
Plotting Relationships



US commercial paper and Treasury bills

3-month rates (%)

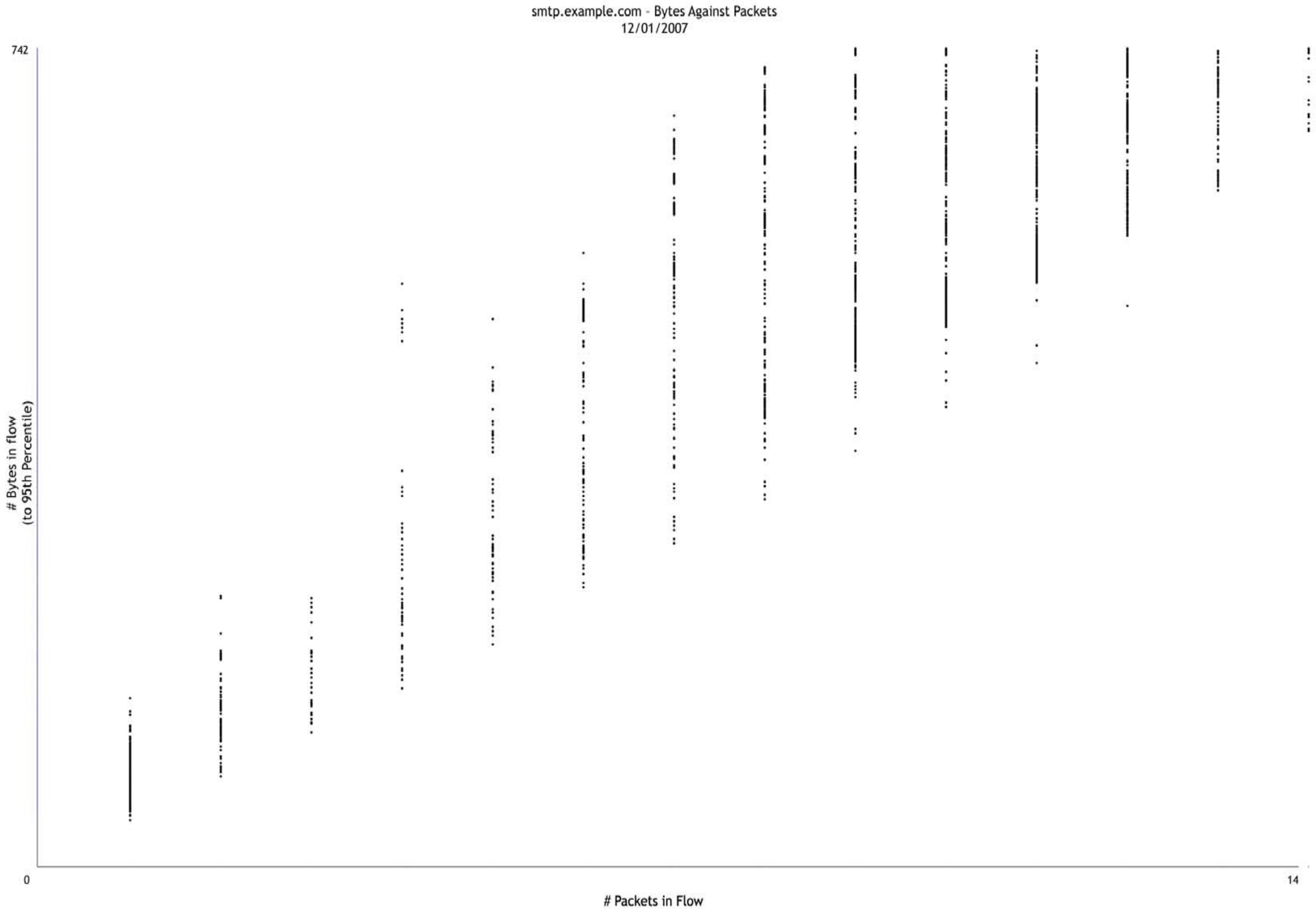
Source: Thomson Datastream

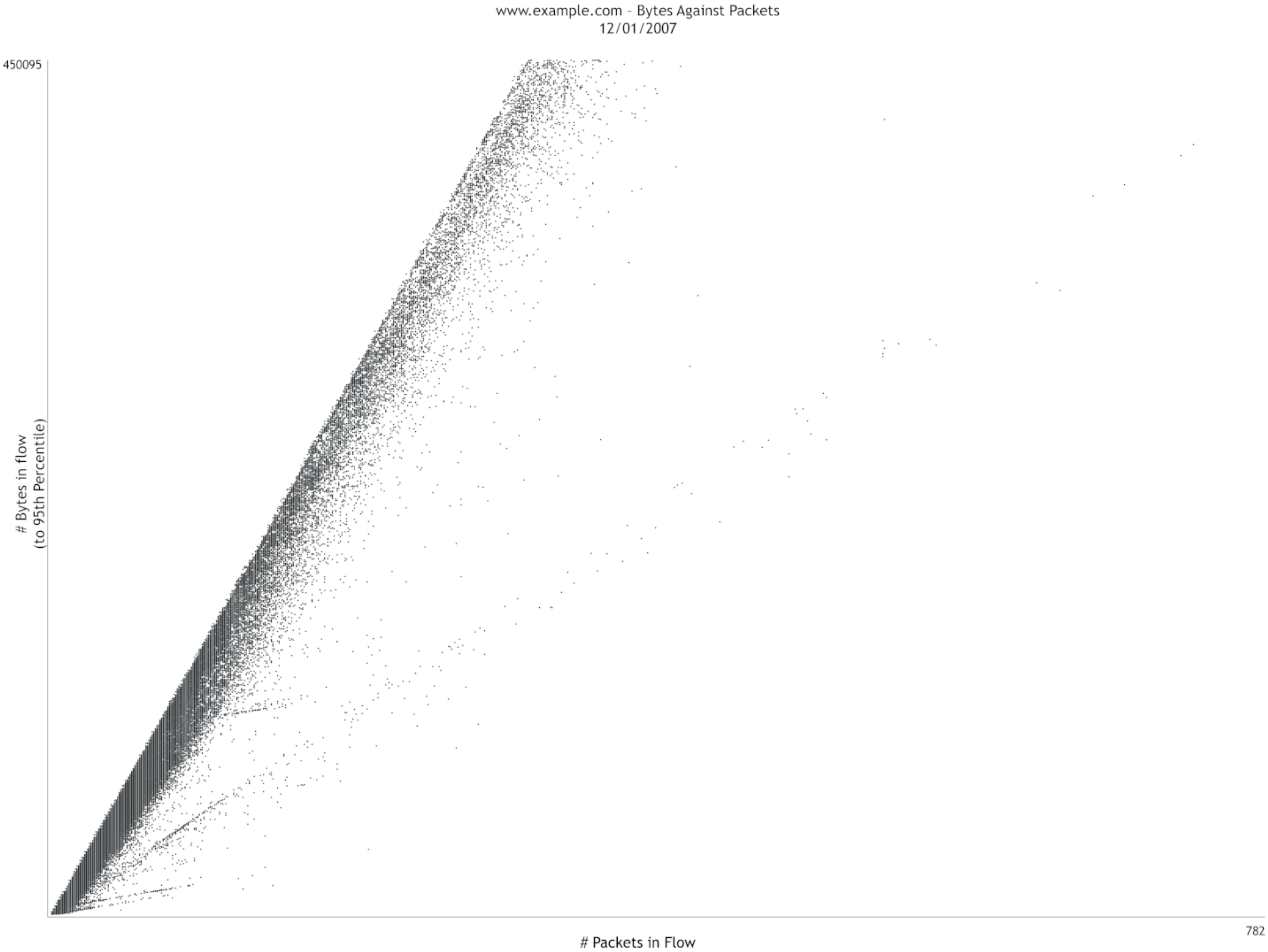


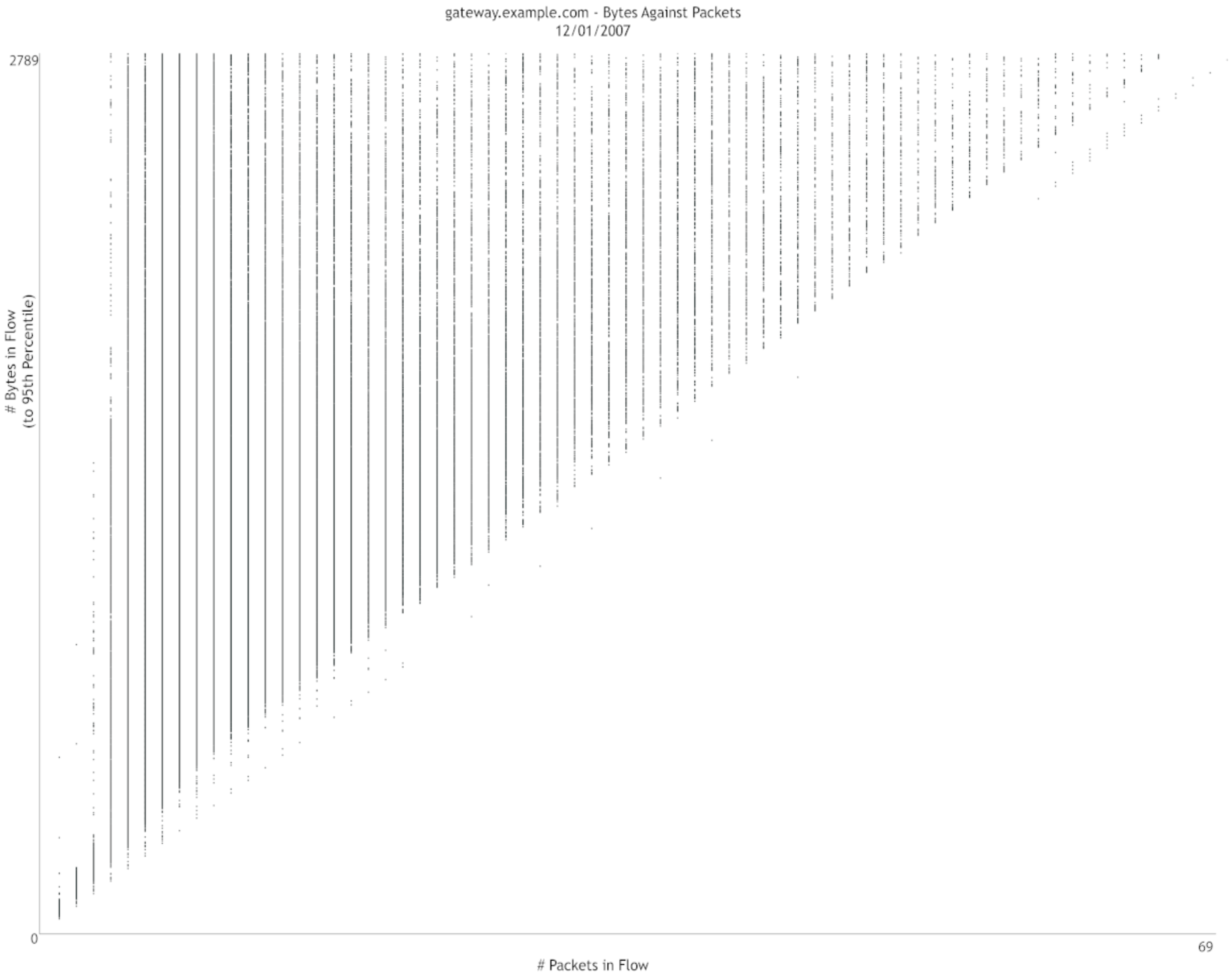
Dollar libor spreads

Over Fed Funds target rate (% points)

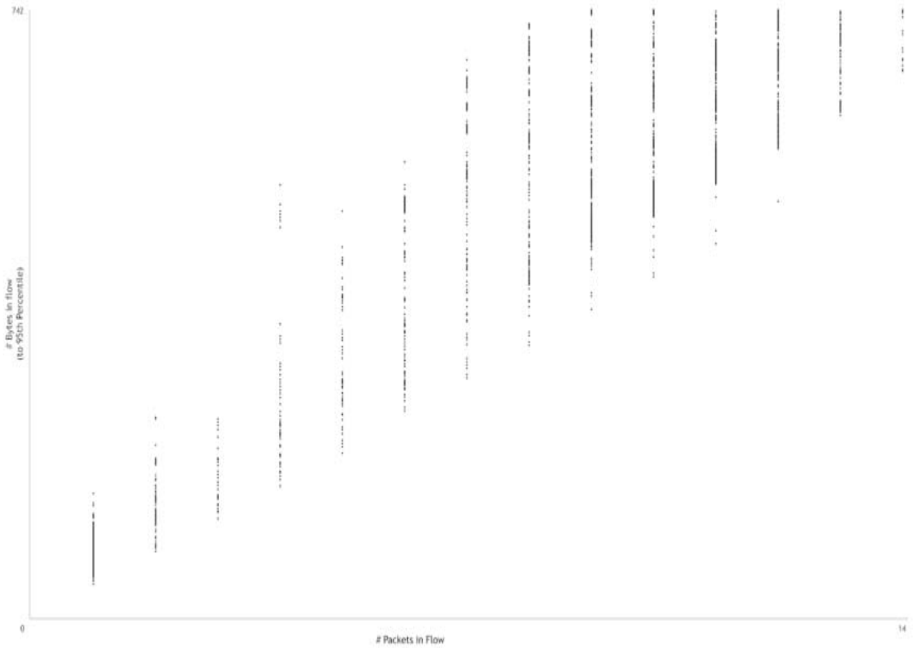
Source: Thomson Datastream


smtp.example.com - Bytes Against Packets
12/01/2007
742
0
# Bytes in flow
(to 95th Percentile)
14
# Packets in Flow

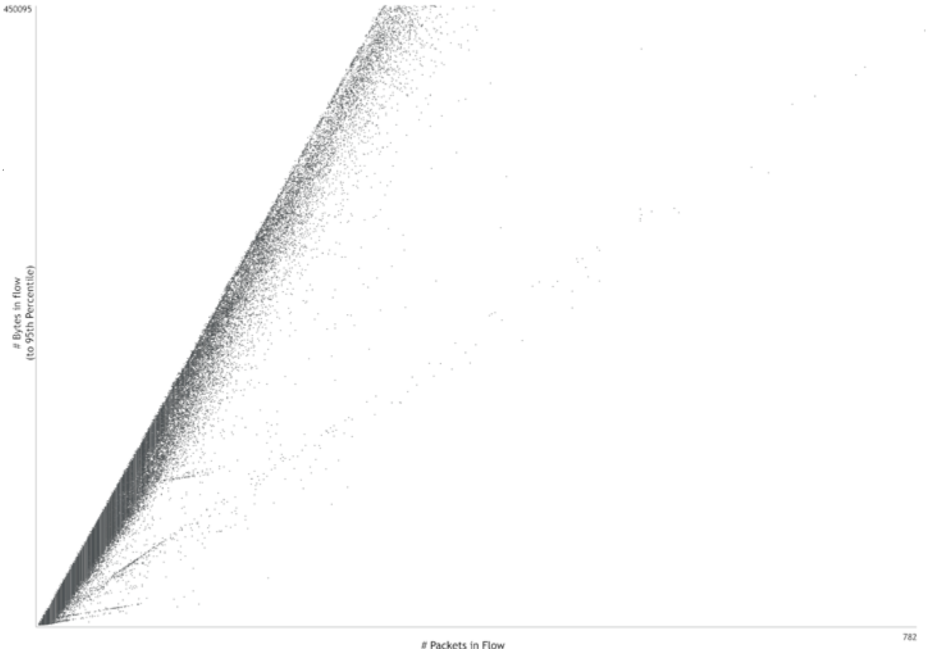

www.example.com – Bytes Against Packets
12/01/2007
450095
# Bytes in flow
(to 95th Percentile)
782
# Packets in Flow


gateway.example.com - Bytes Against Packets
12/01/2007
2789
# Bytes in Flow
(to 95th Percentile)
0
69
# Packets in Flow

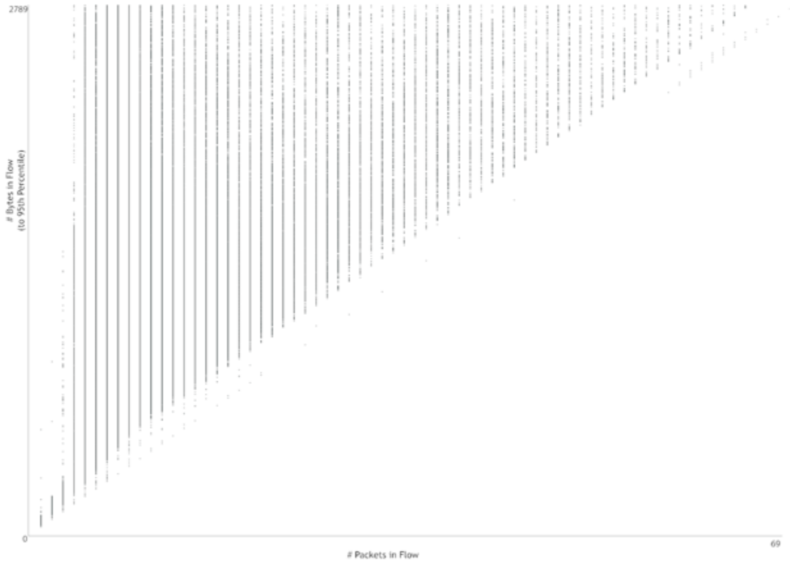
smtp.example.com - Bytes Against Packets
12/01/2007



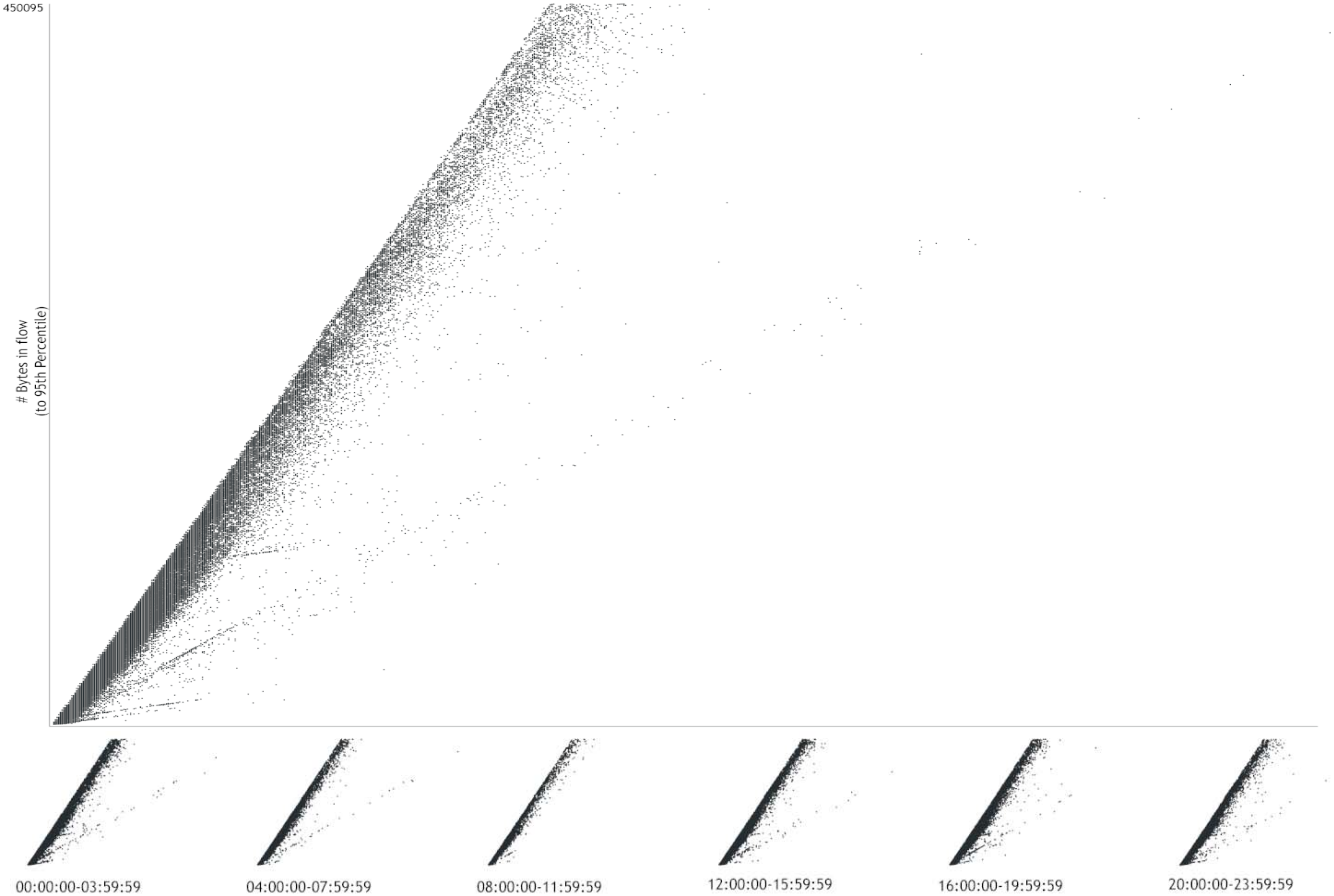
www.example.com - Bytes Against Packets
12/01/2007



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



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

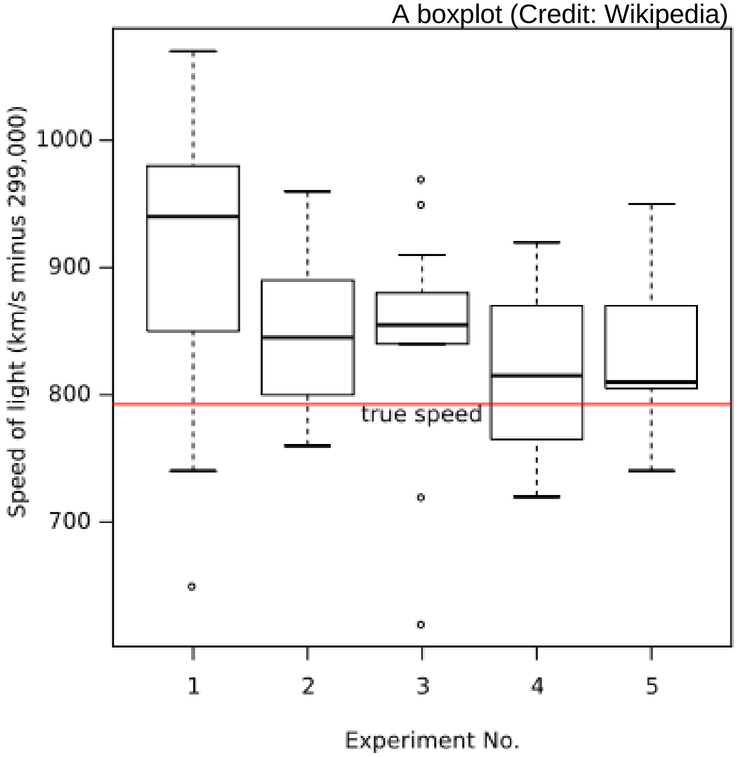


Plotting Distributions:

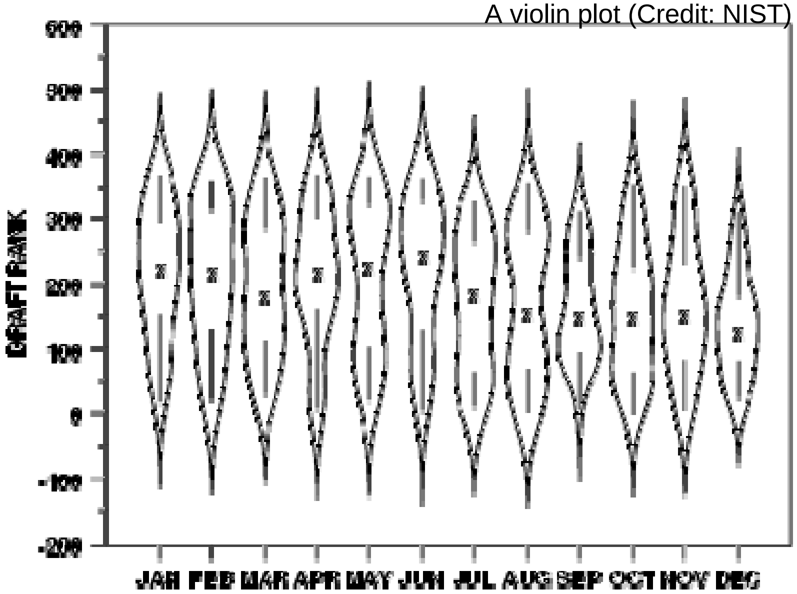
How a variable relates to itself

Box and Violin Plots

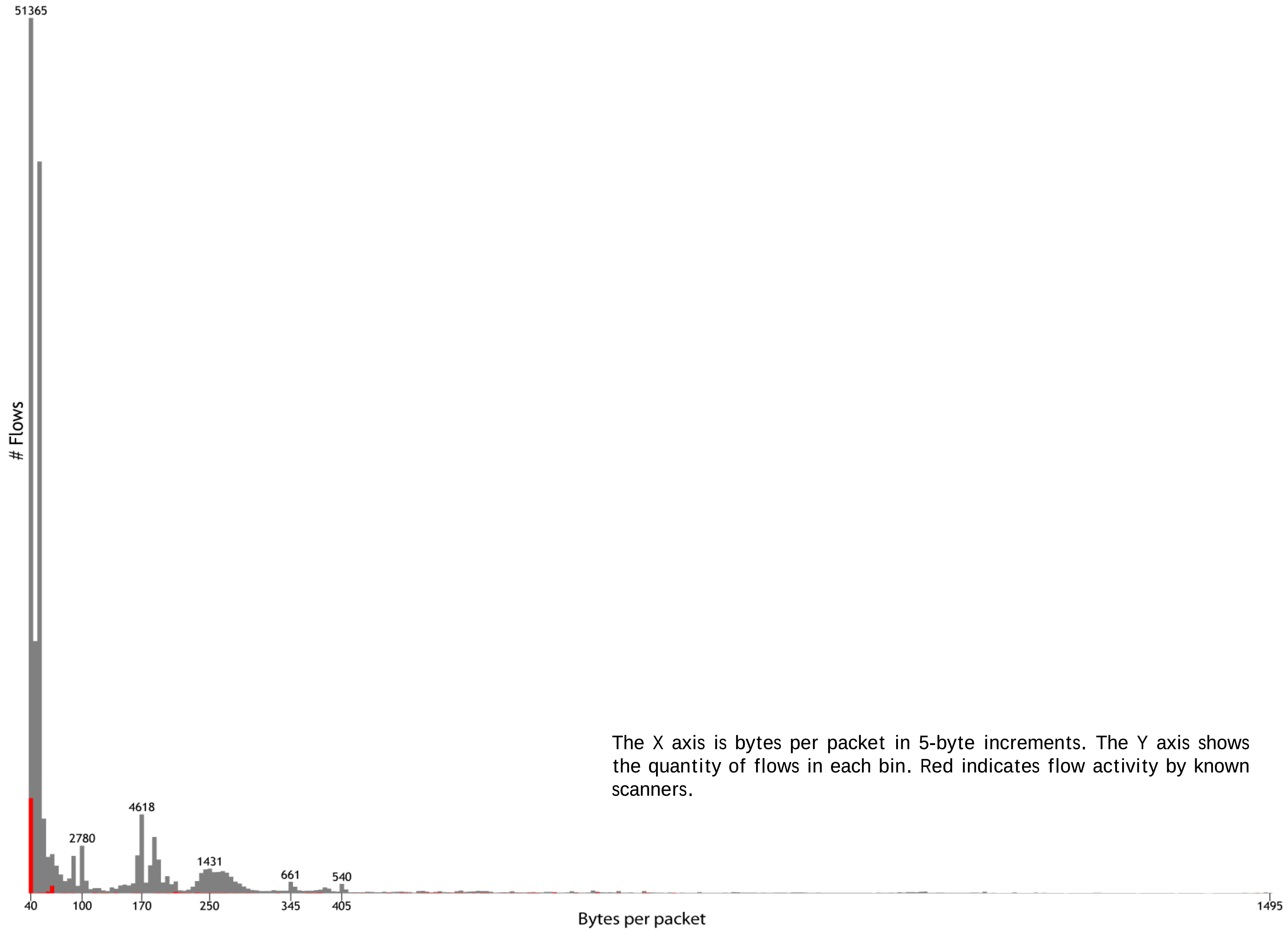
A boxplot (Credit: Wikipedia)



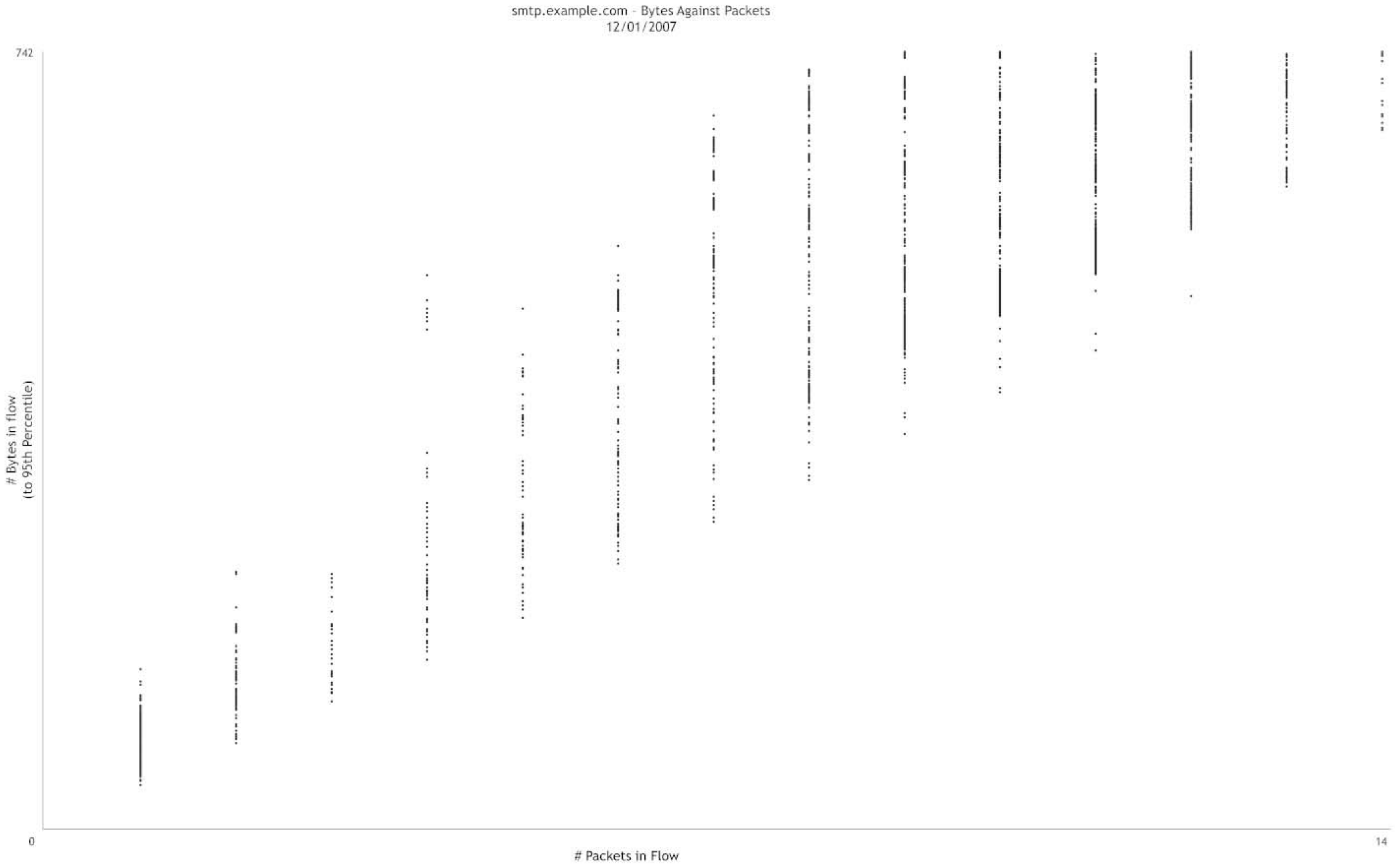
A violin plot (Credit: NIST)

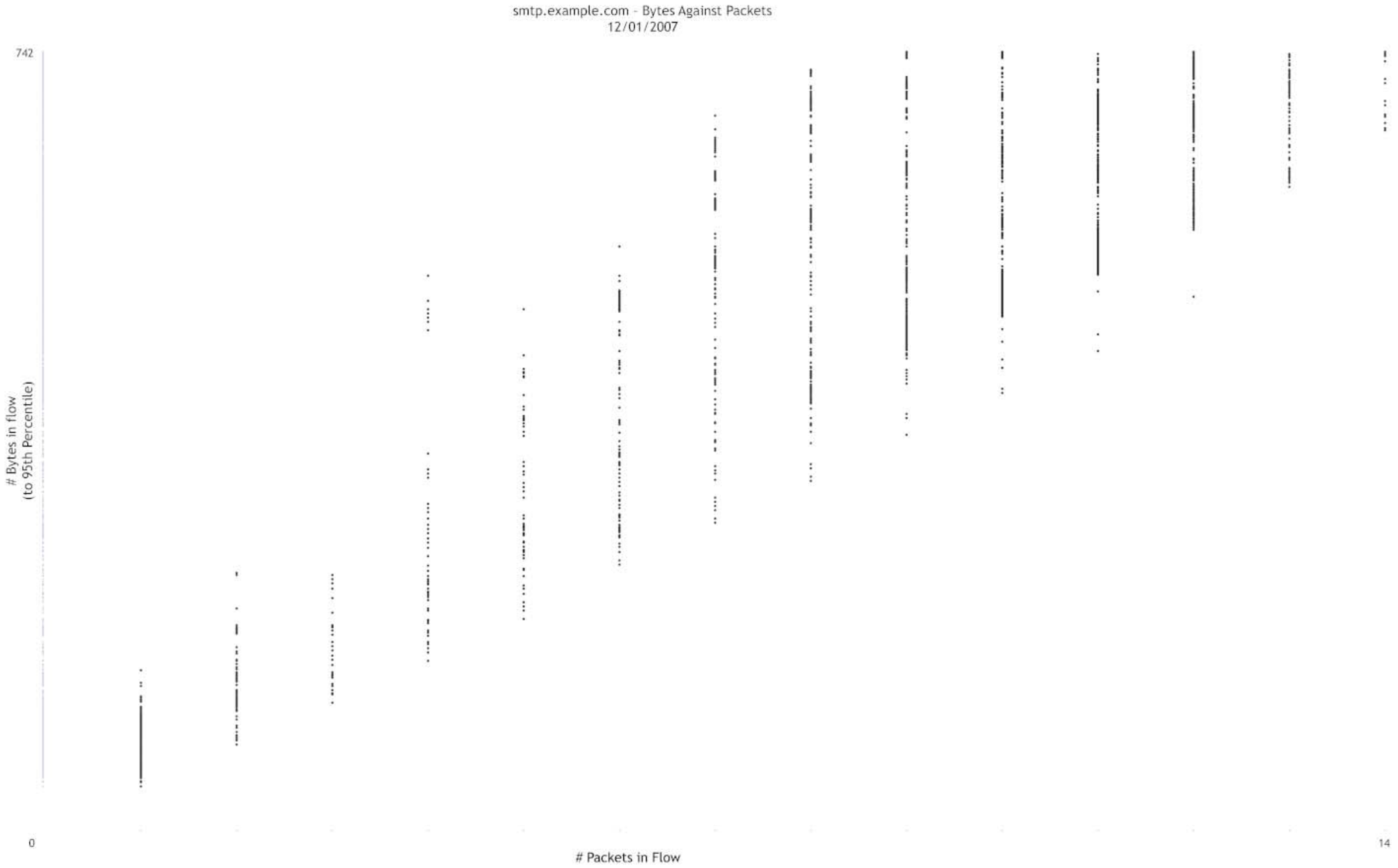


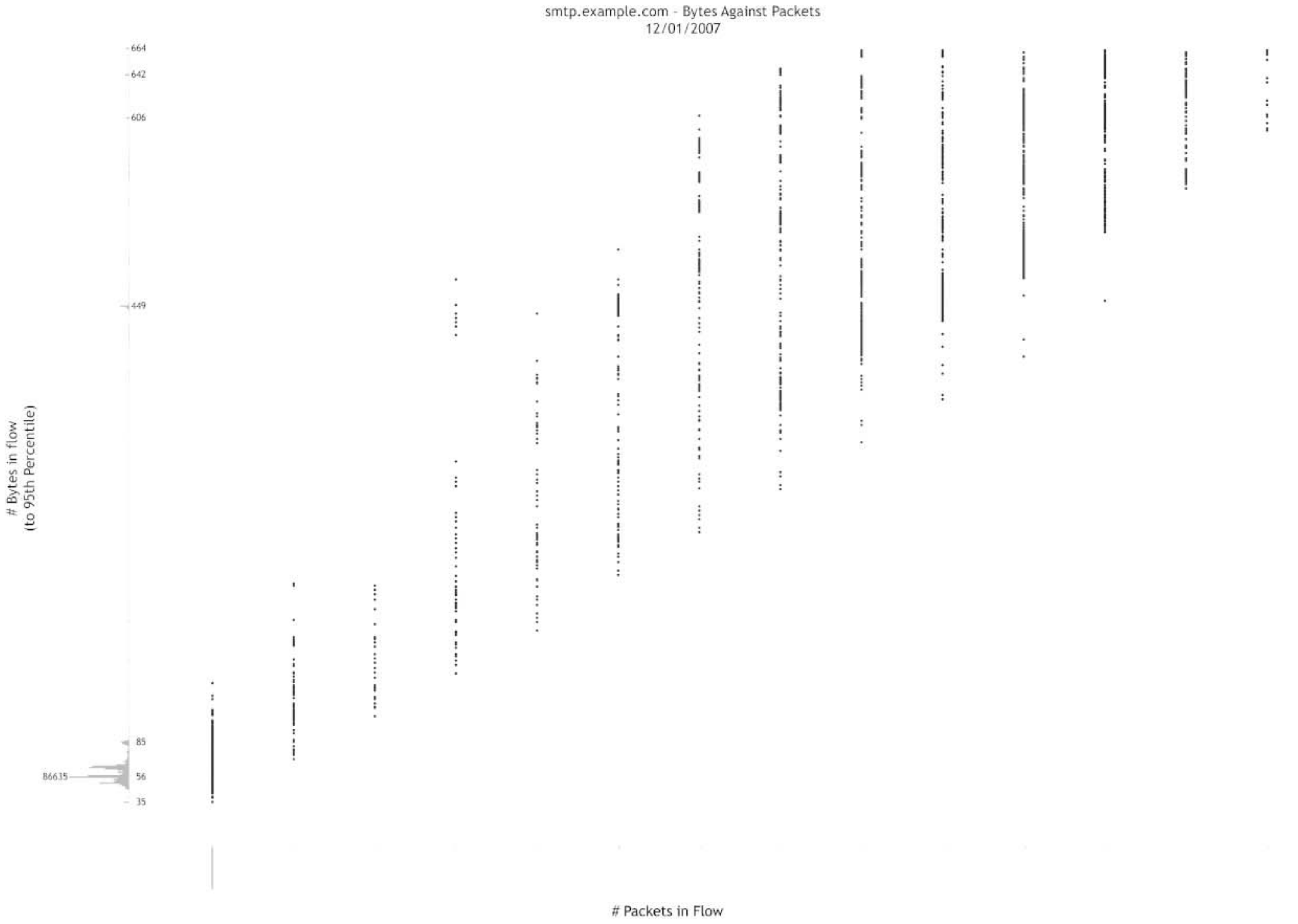
example.com Flow Volume, Binned by Bytes per Packet
2007/12/01

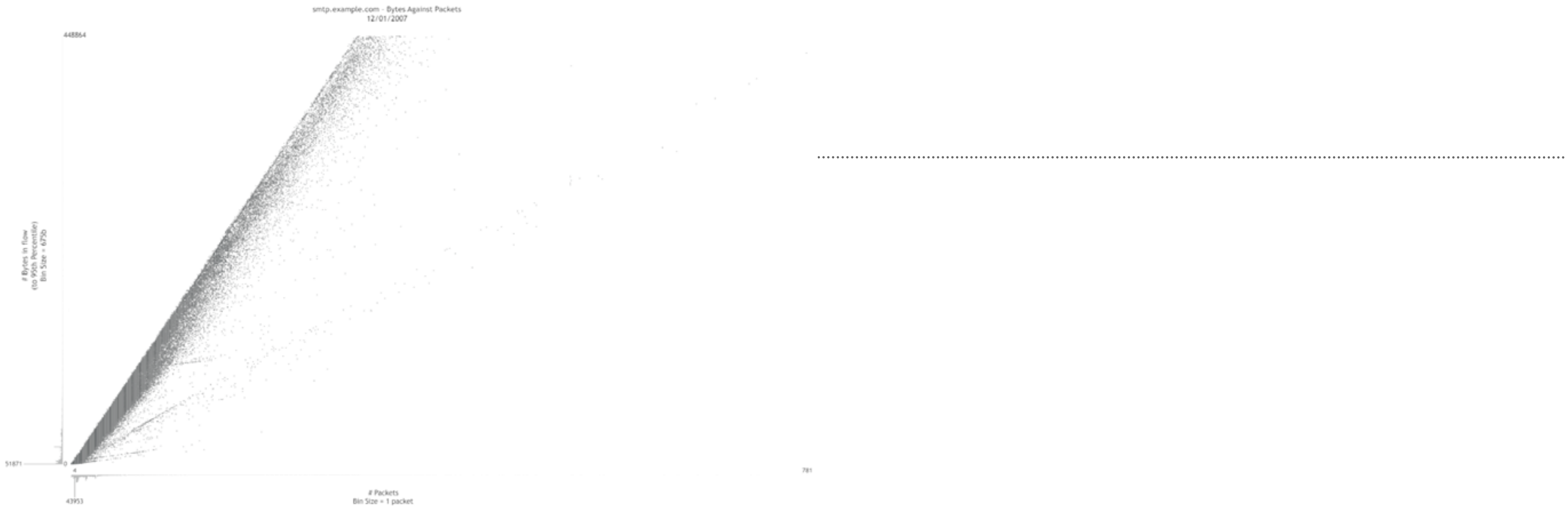


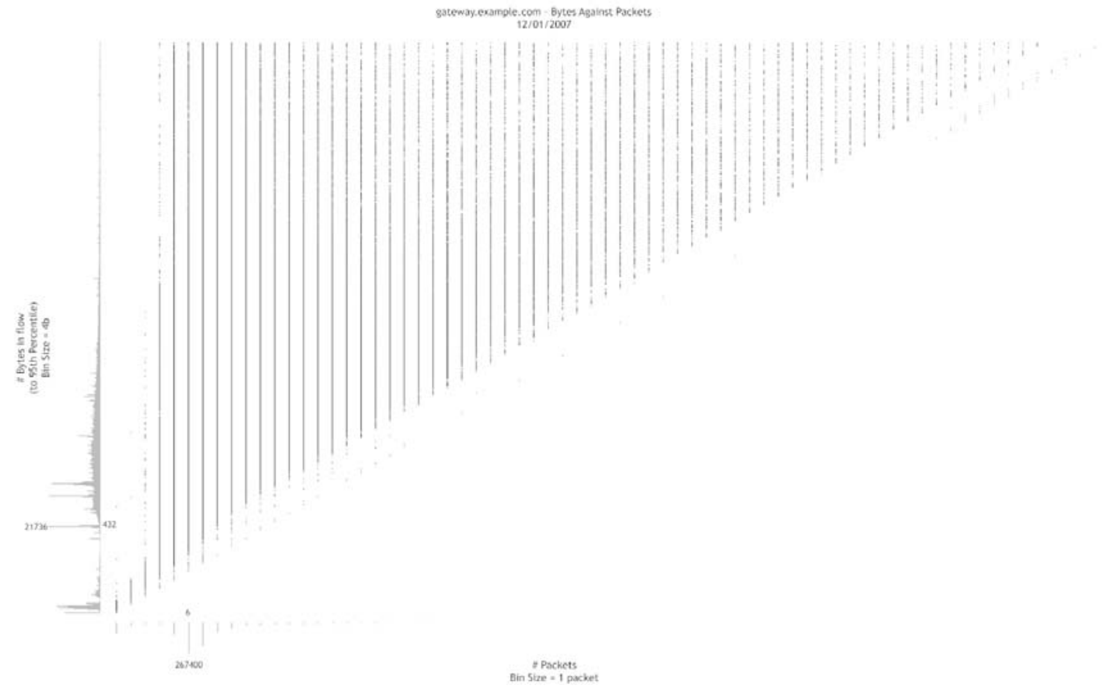
The X axis is bytes per packet in 5-byte increments. The Y axis shows the quantity of flows in each bin. Red indicates flow activity by known scanners.


smtp.example.com - Bytes Against Packets
12/01/2007
742
0
# Bytes in flow
(to 95th Percentile)
14
# Packets in Flow


smtp.example.com - Bytes Against Packets
12/01/2007
742
# Bytes in flow
(to 95th Percentile)
0
# Packets in Flow
14


smtp.example.com - Bytes Against Packets
12/01/2007
# Bytes in flow
(to 95th Percentile)
664
642
606
449
85
86635
56
35
# Packets in Flow

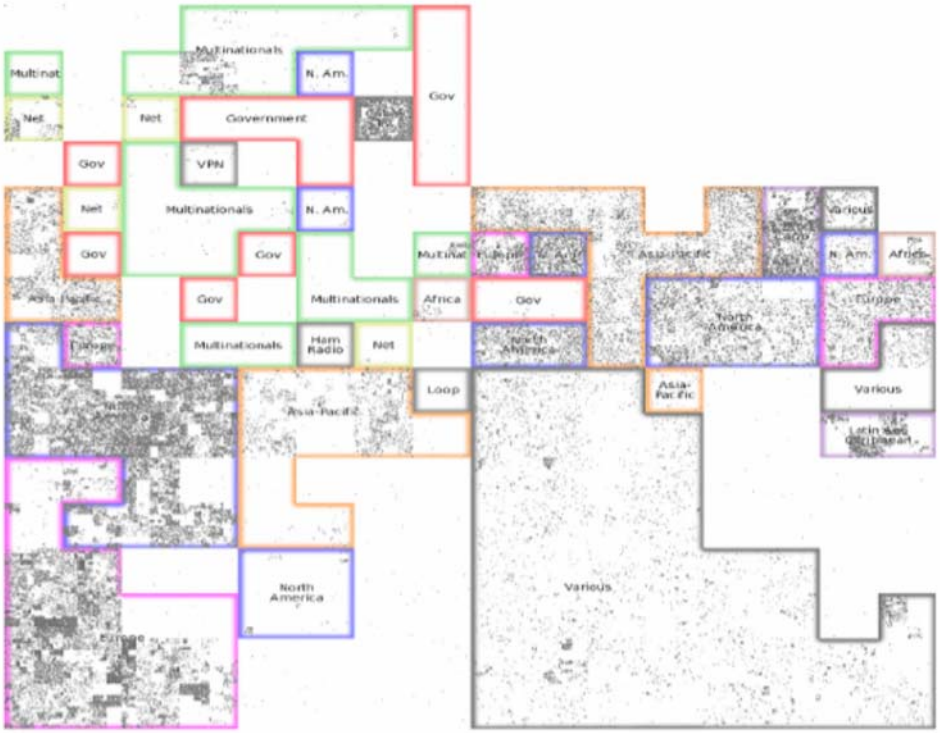

smtp.example.com - Bytes Against Packets
12/01/2007
448864
# Bytes in flow
(to 95th Percentile)
Bin Size = 675b
51871
0
4
781
43953
# Packets
Bin Size = 1 packet


gateway.example.com - Bytes Against Packets
12/01/2007
# Bytes in flow
(to 95th Percentile)
Bin Size = 4b
21736
432
6
267400
# Packets
Bin Size = 1 packet

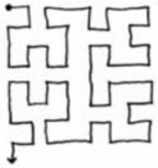
Hilbert Curve:

Broad Scale Visualization

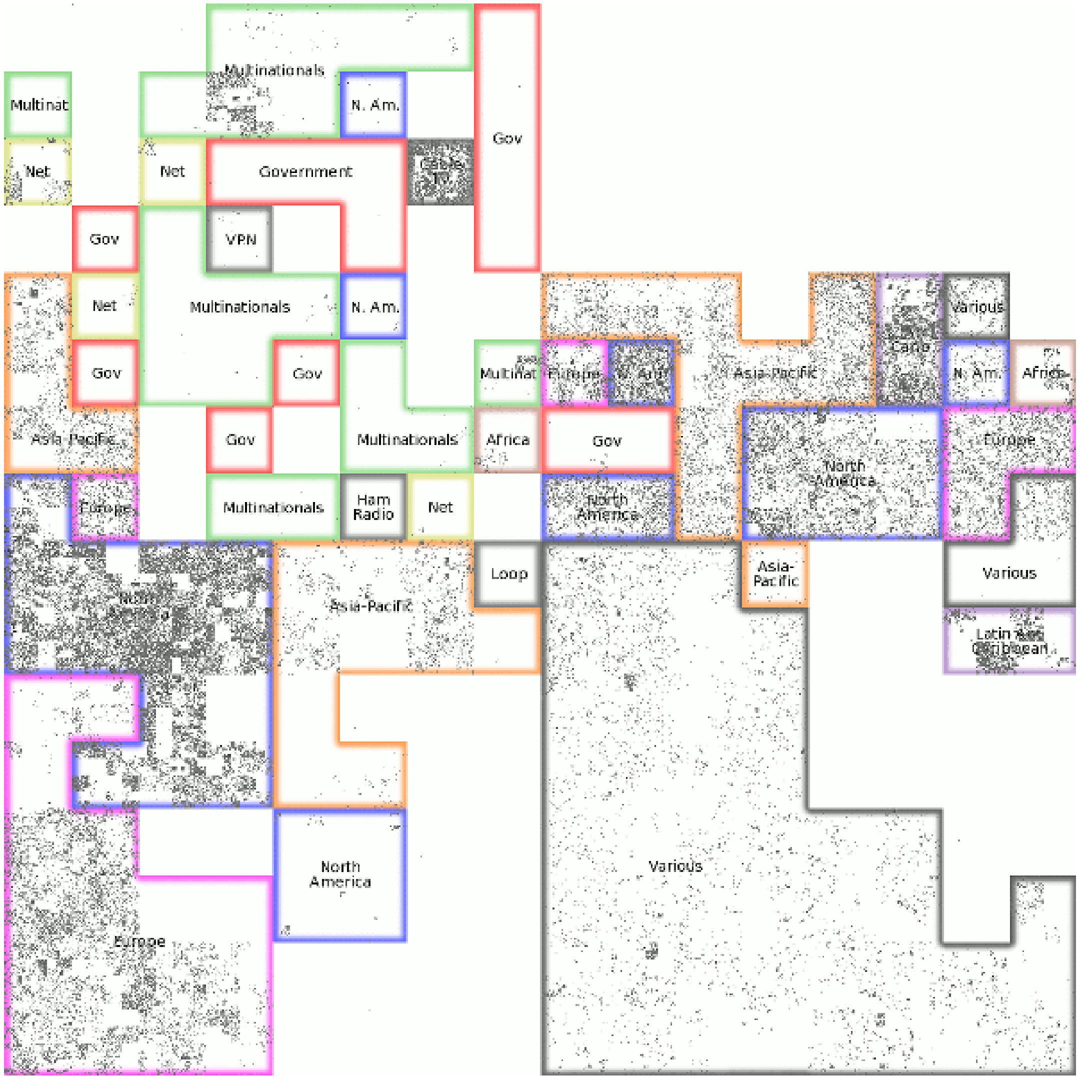
Hilbert Curve



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.