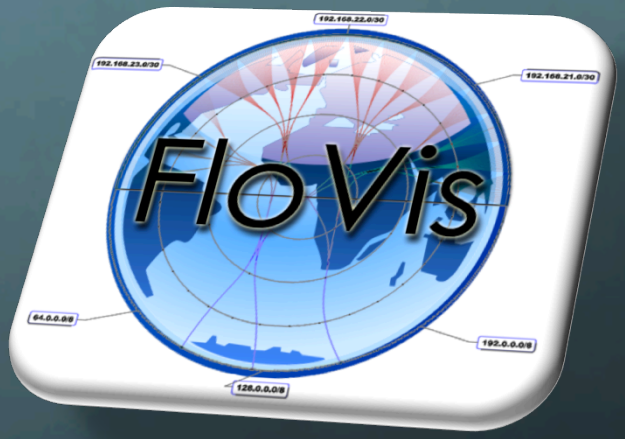


OverFlow: An Overview Visualization for Network Analysis

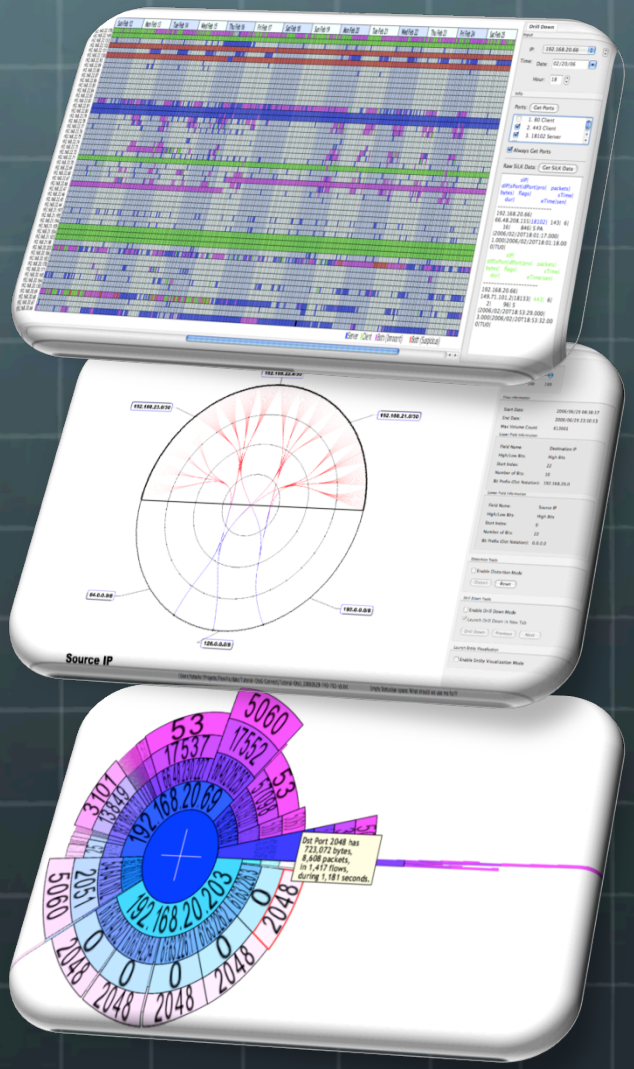
J. Glanfield, S. Brooks, T. Taylor, D. Paterson, C. Smith, C. Gates, J. McHugh

Outline

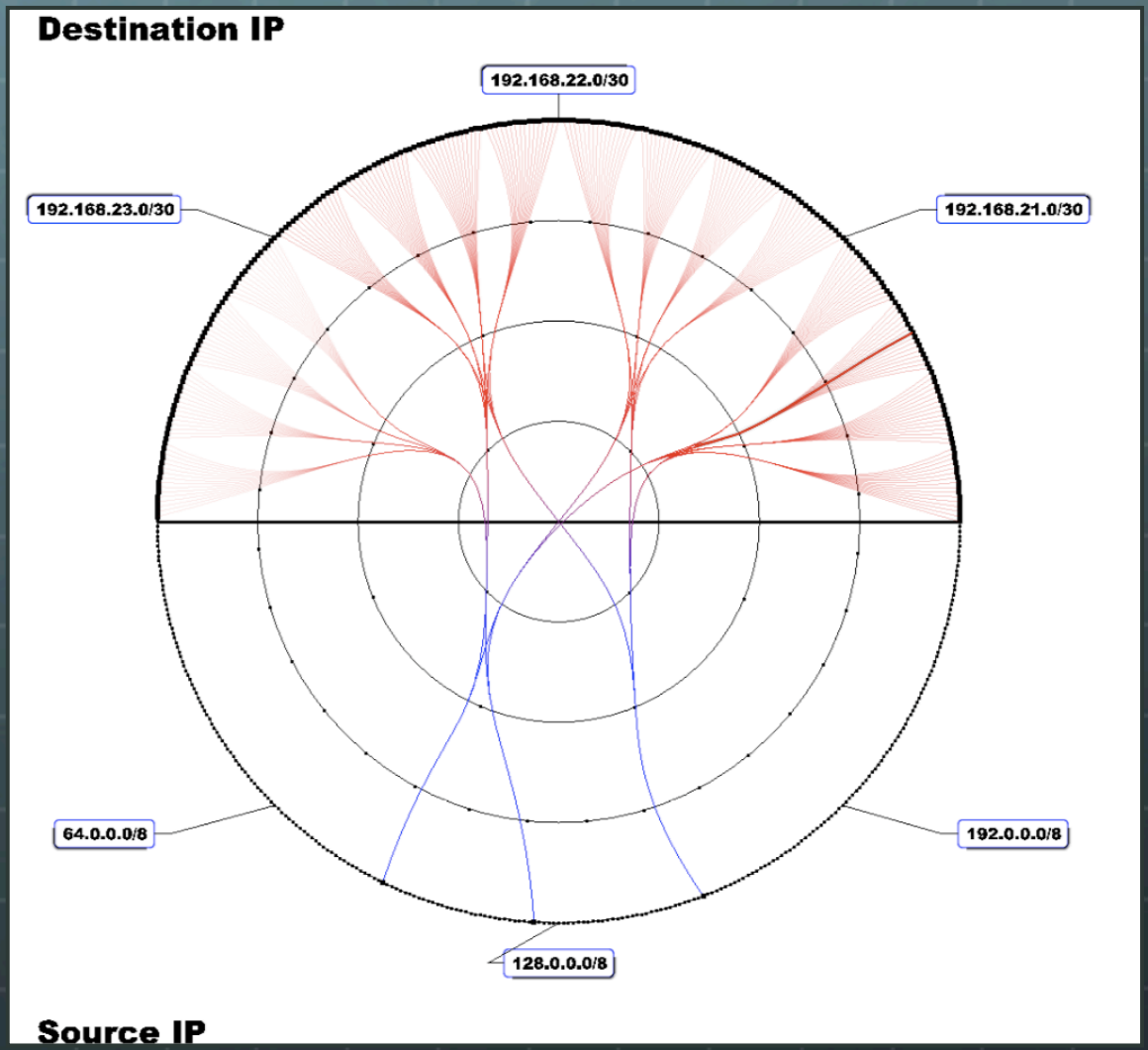
- FloVis: crash course
- OverFlow
  - Motivation
  - Description
  - Case Study
- Future Work & Conclusions

FloVis: Crash Course

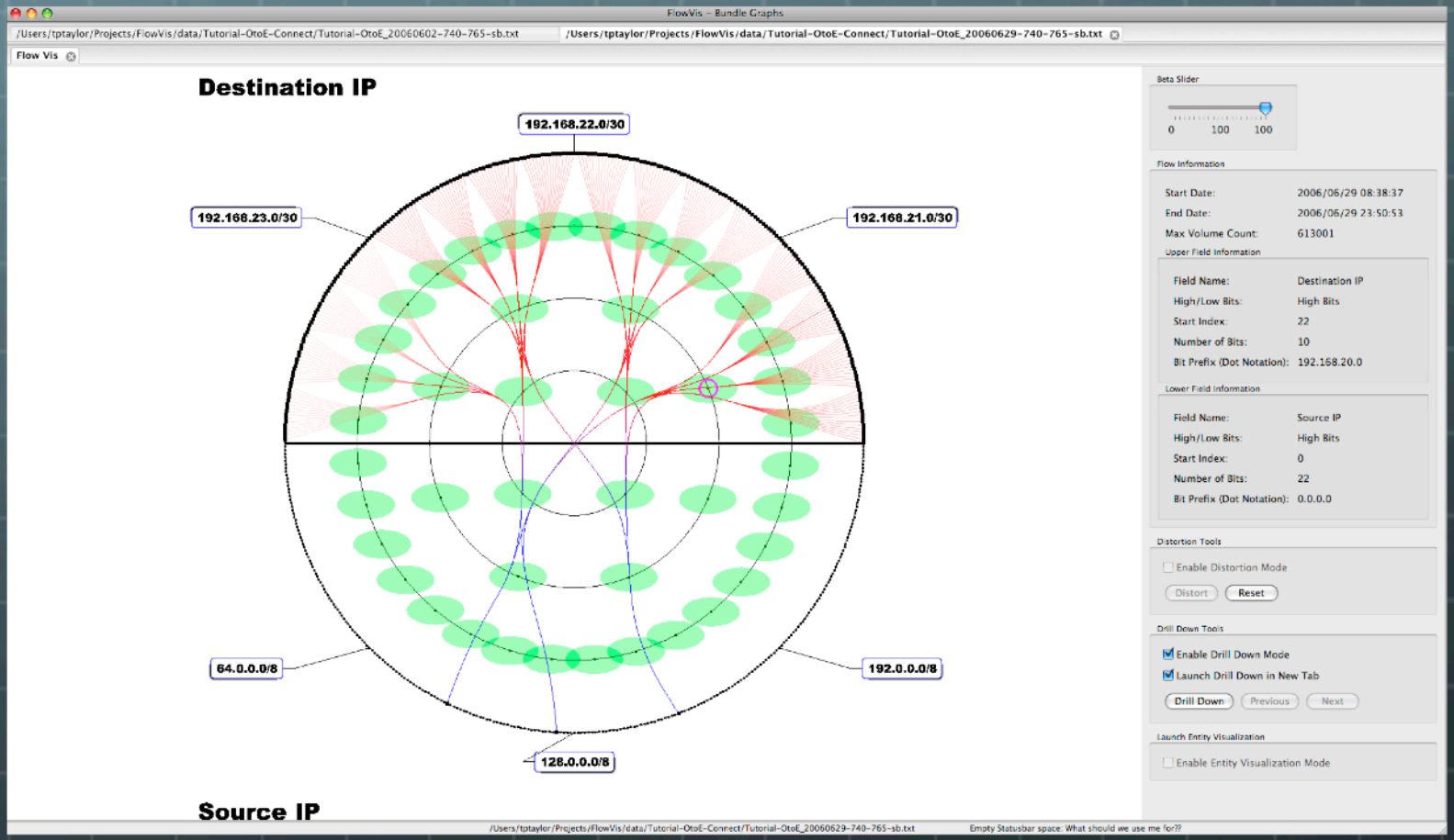
- Network Visualization Framework
  - Promotes extensibility
    - Users create plug-ins
  - Supports transitioning/pivoting
    - Viz-to-viz communication
    - Currently in progress…



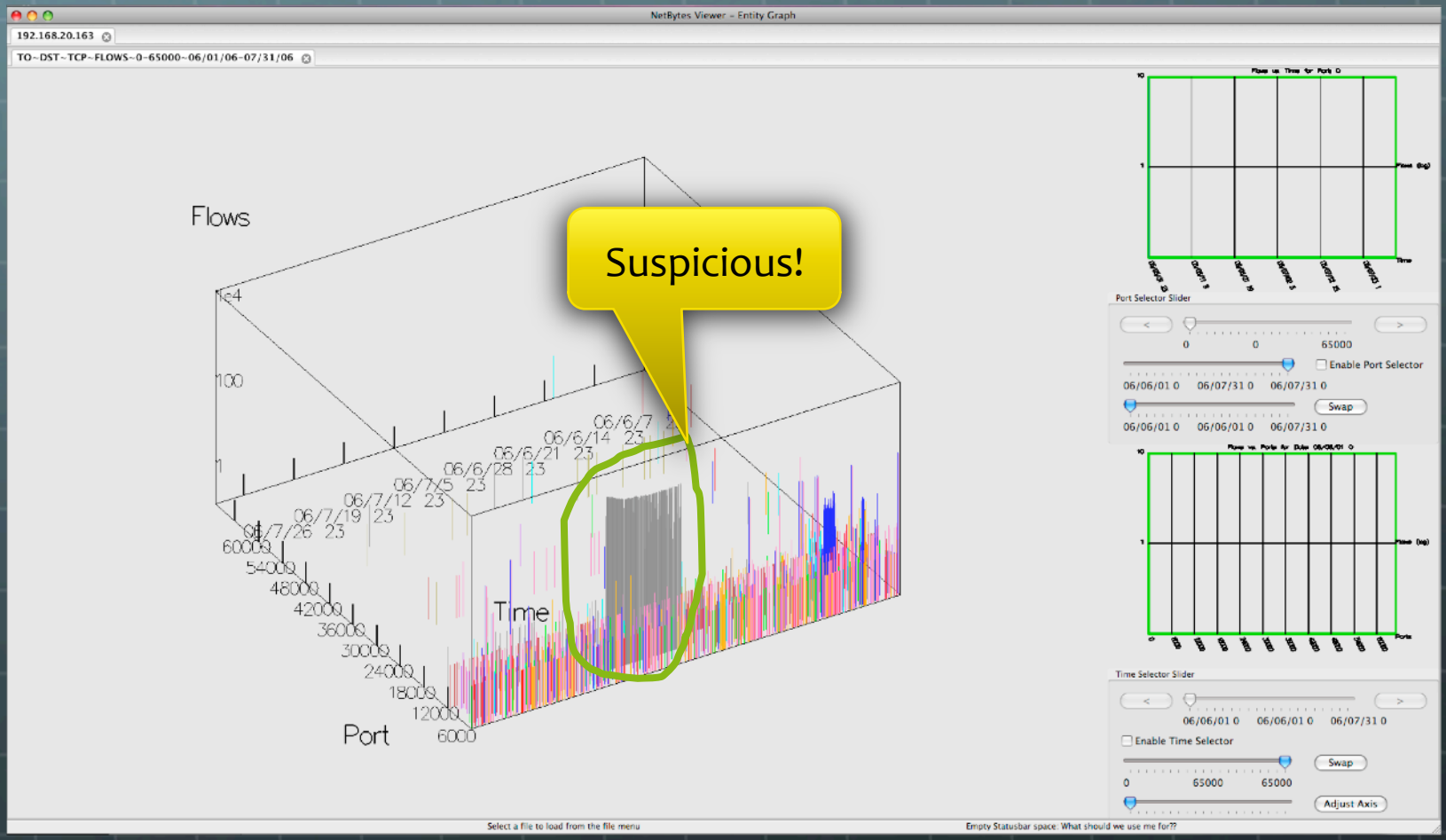
Example: FlowBundle



FlowBundle: Drill down

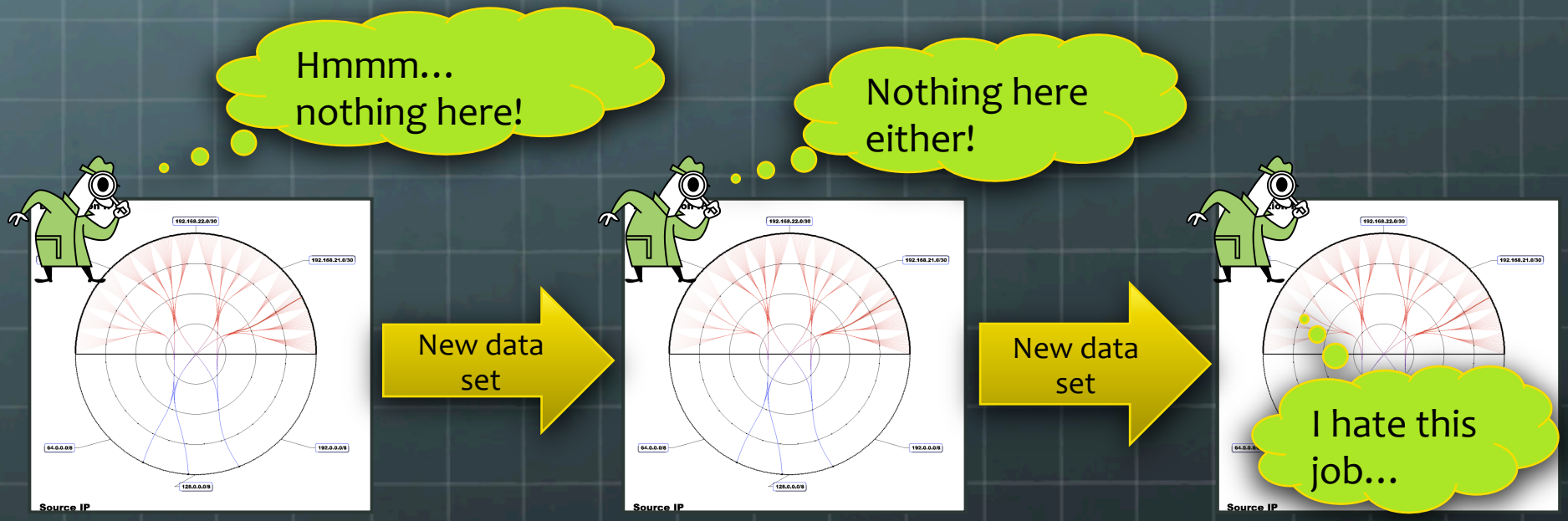


Drill down: continued



Question!

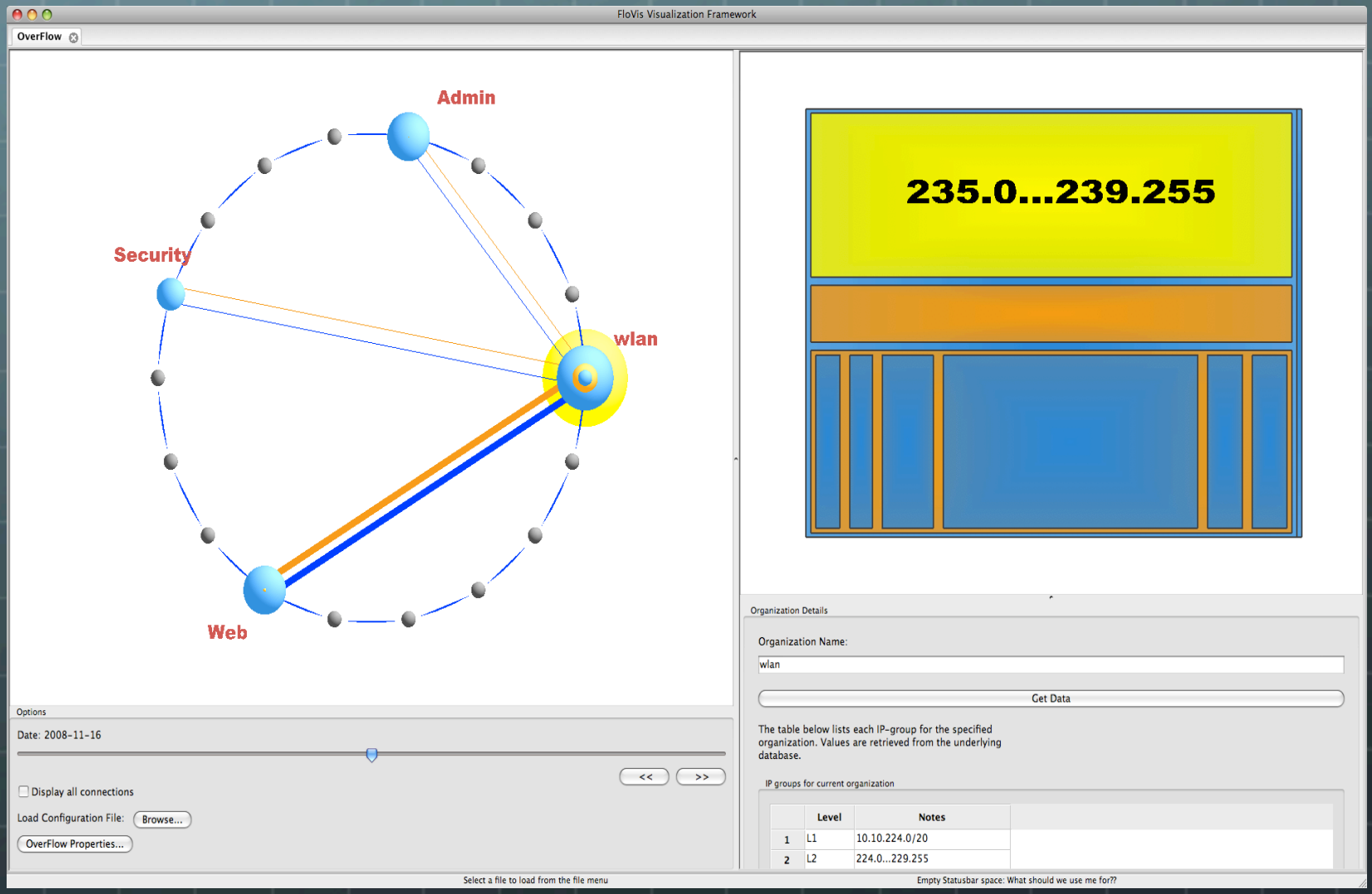
- What motivated the original query?
  - trial-and-error?



OverFlow: Motivation

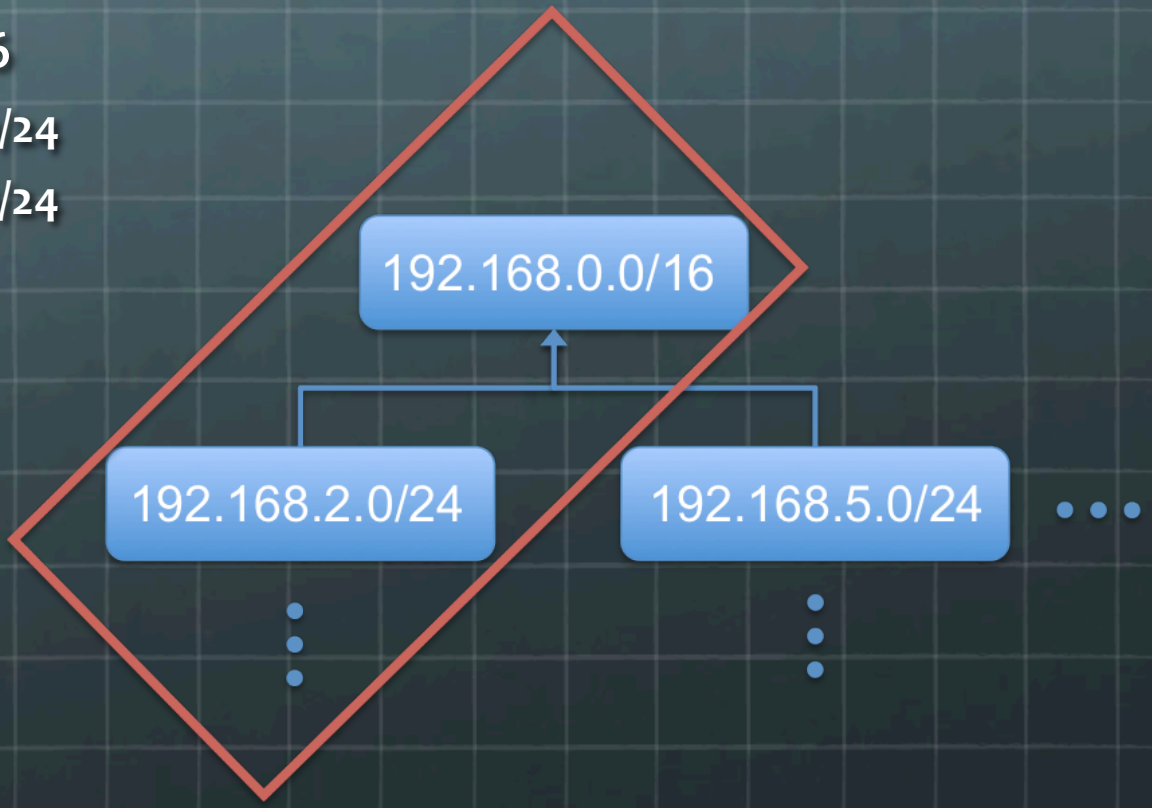
- We need a starting point
- We don't want to go back to the data every time nothing is found worth investigating
  - (reduce "cognitive load" or "cognitive burden")
- FloCon 2009: analysts described need to group IPs
  - Organizational groupings
  - Top-N lists
  - Etc.

OverFlow

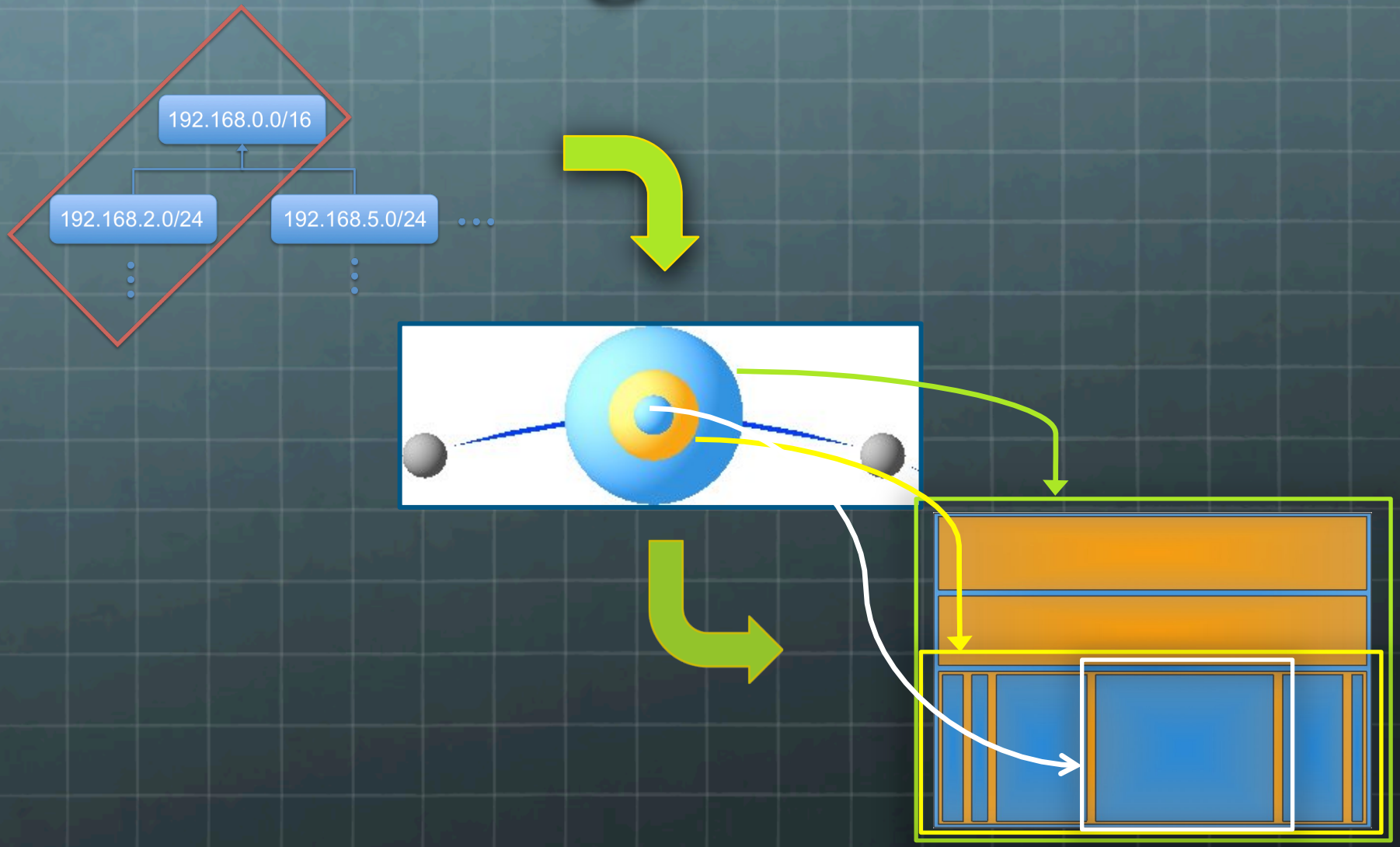

FloVis Visualization Framework
OverFlow
Admin
Security
wlan
Web
235.0...239.255
Options
Date: 2008-11-16
<<
>>
Display all connections
Load Configuration File:
Browse...
OverFlow Properties...
Organization Details
Organization Name:
wlan
Get Data
The table below lists each IP-group for the specified organization. Values are retrieved from the underlying database.
IP groups for current organization
Level
Notes
1
L1
10.10.224.0/20
2
L2
224.0...229.255
Select a file to load from the file menu
Empty Statusbar space: What should we use me for??

Data Representation

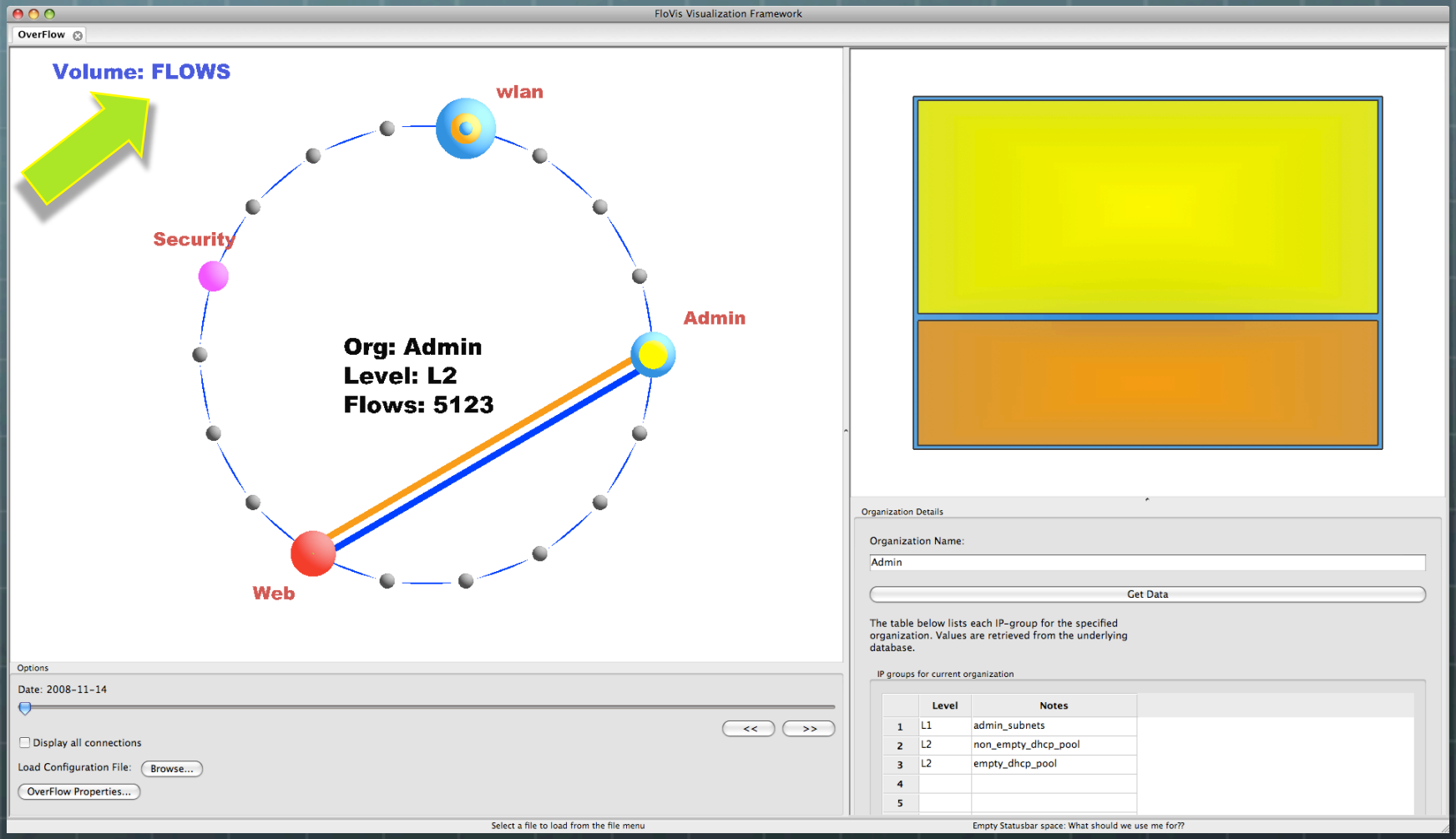
- Organize arbitrary network hierarchies:
  - By hand:
    - 192.168.0.0/16
      - 192.168.2.0/24
      - 192.168.5.0/24
  - Or:



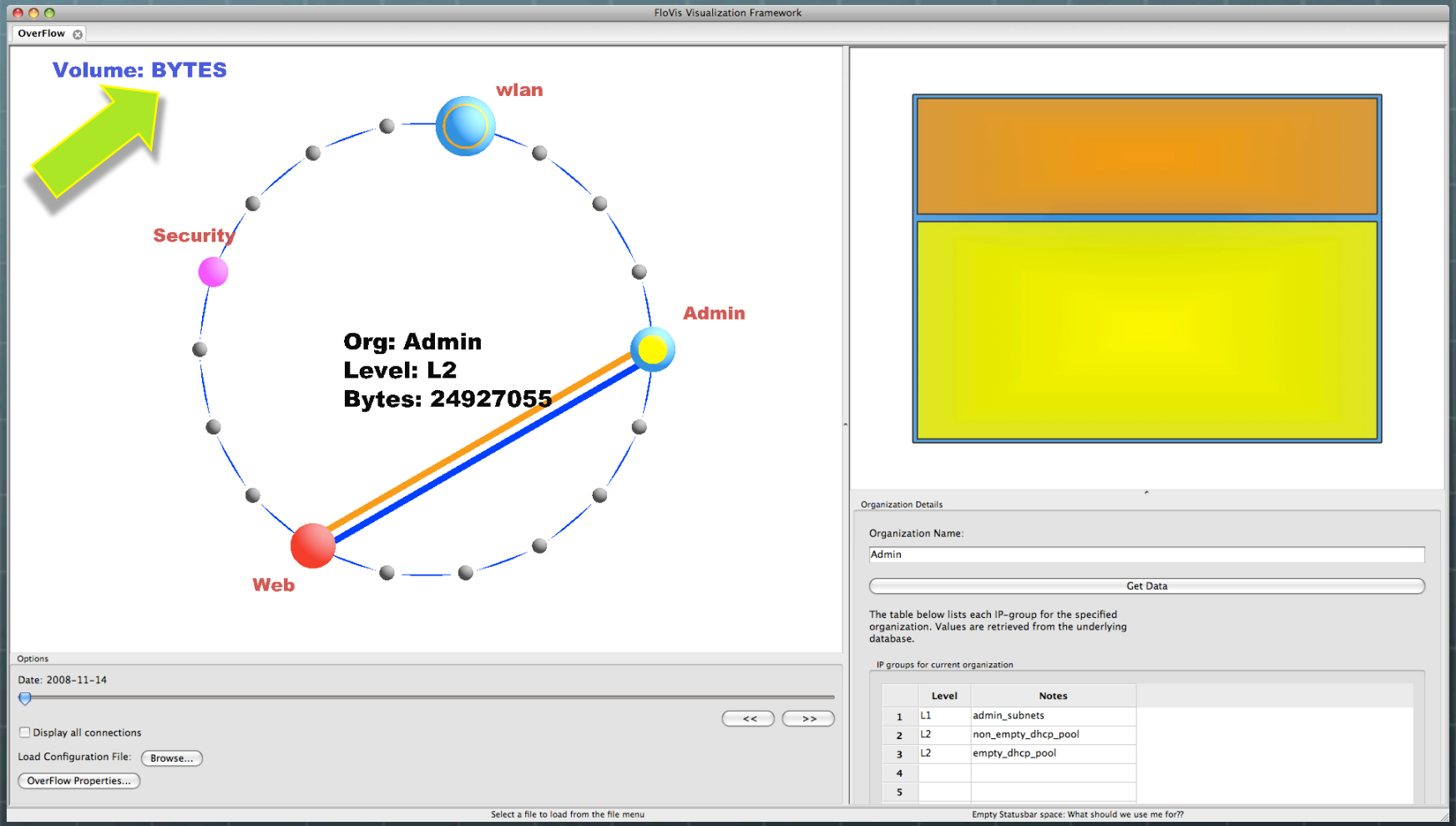
Visualizing Hierarchies



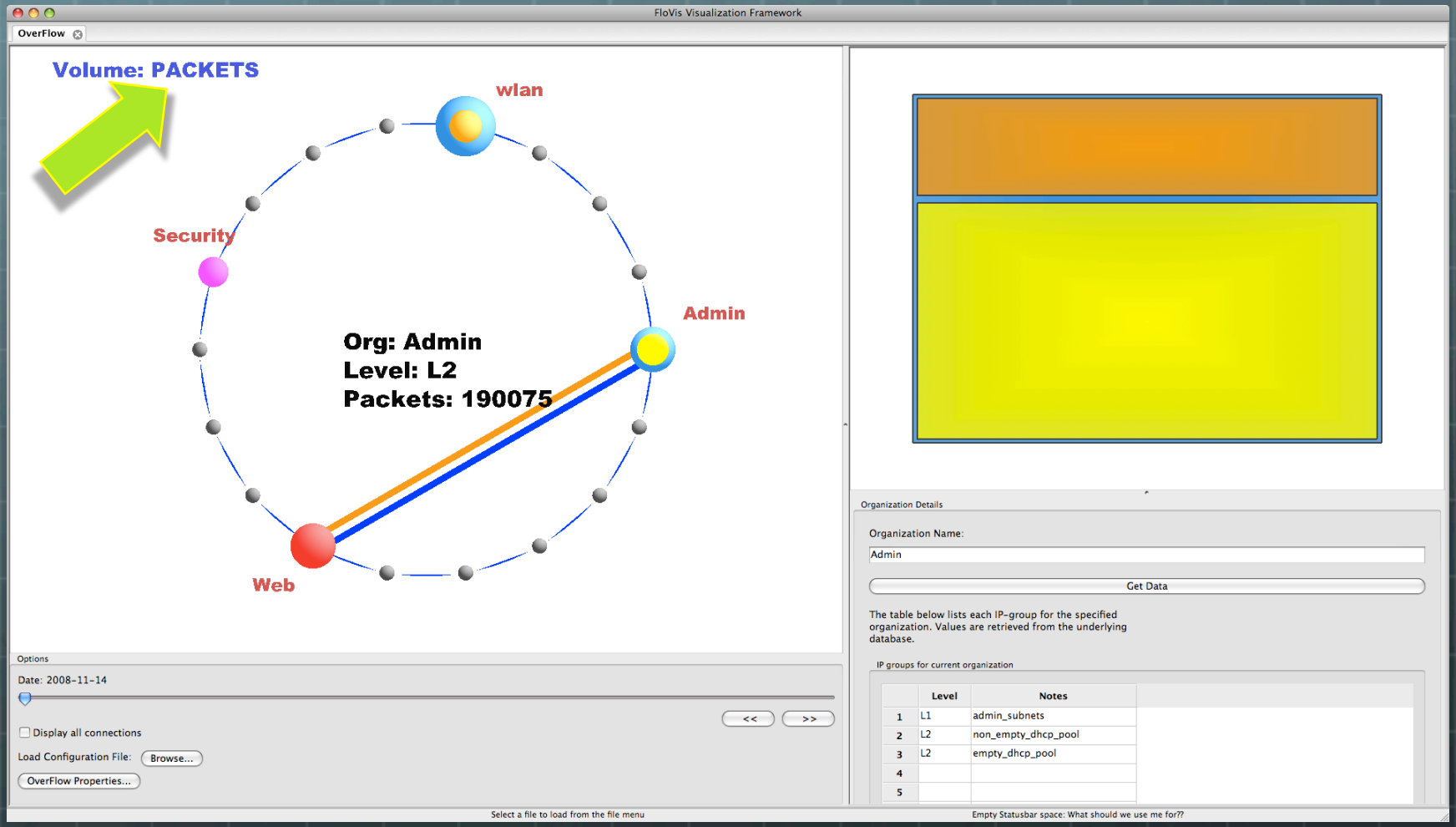
Visualizing Volumes



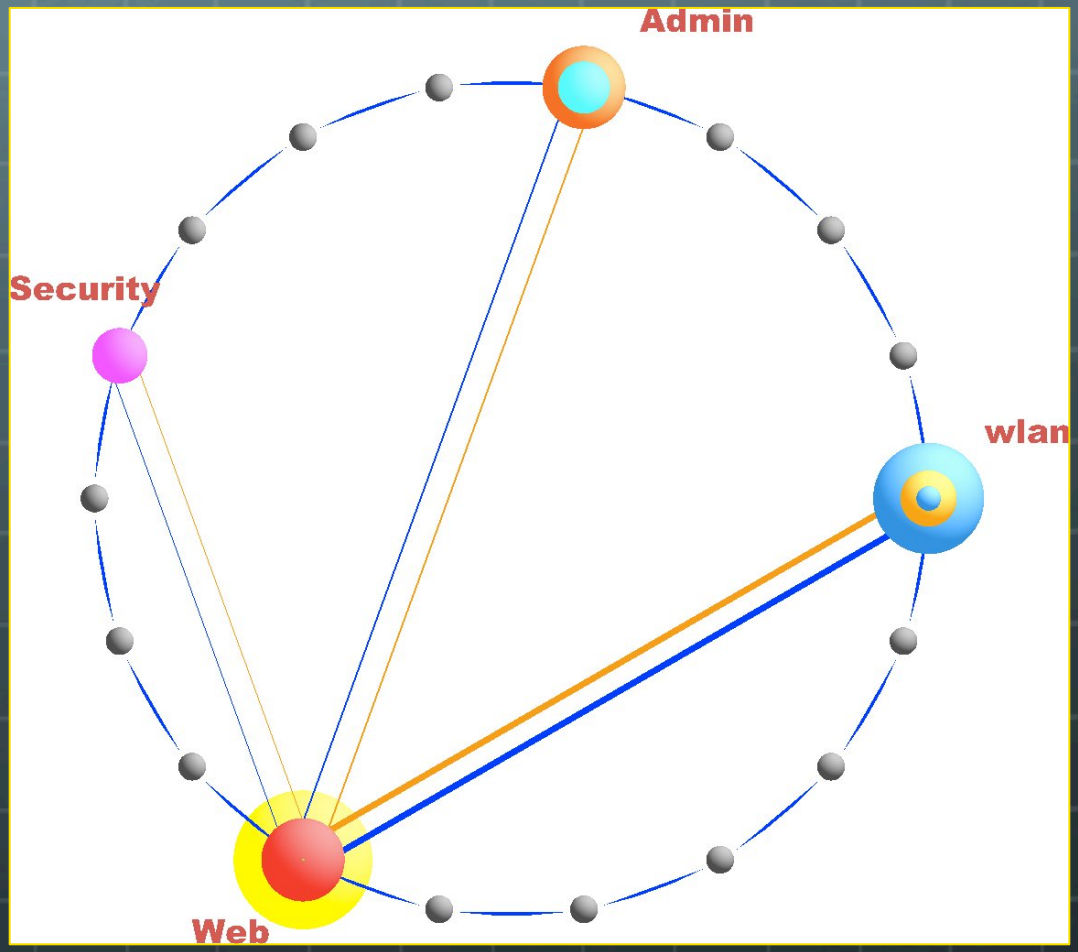
Visualizing Volumes



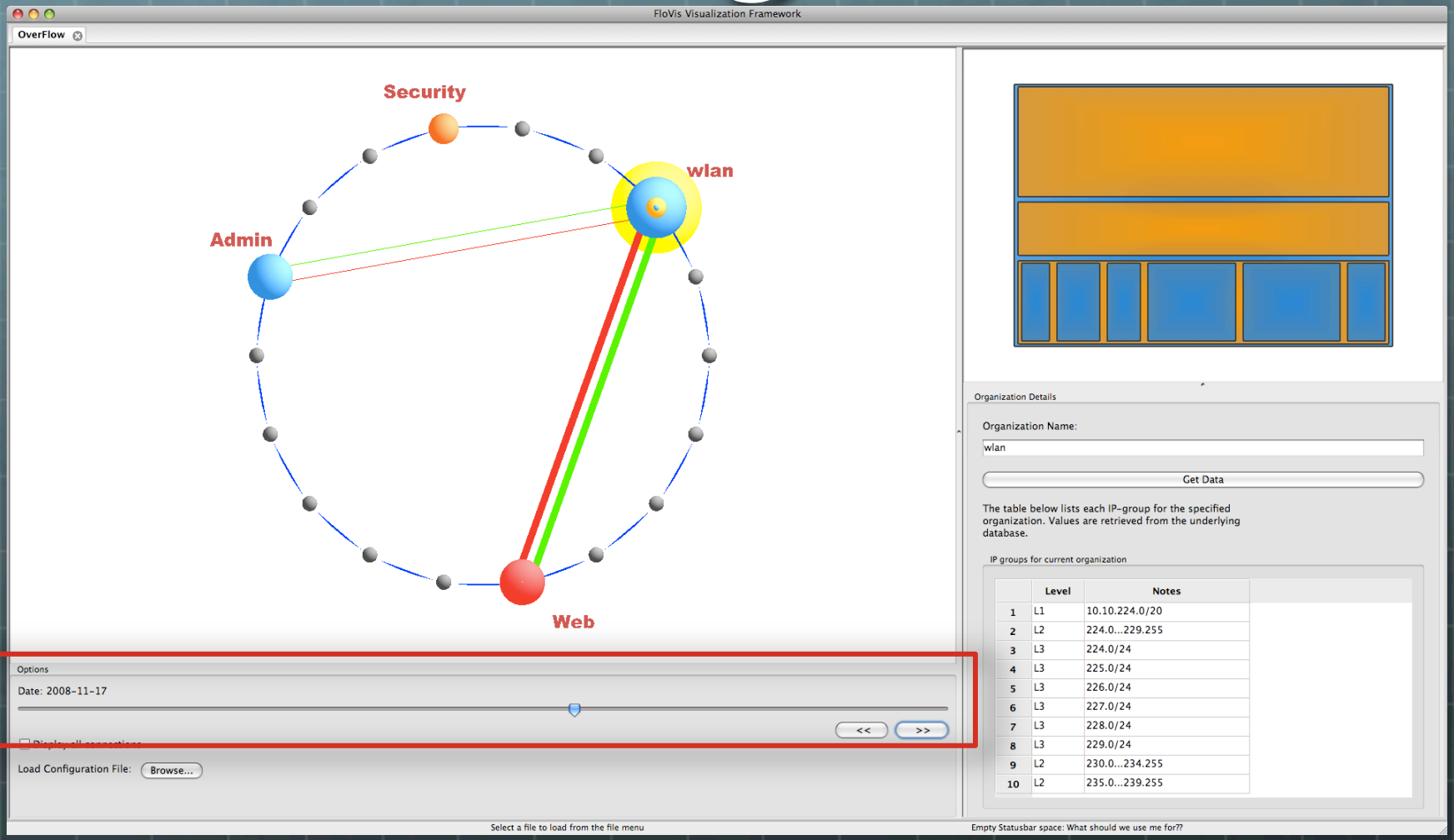
Visualizing Volumes



Visualizing Communications



Transitioning Over Time

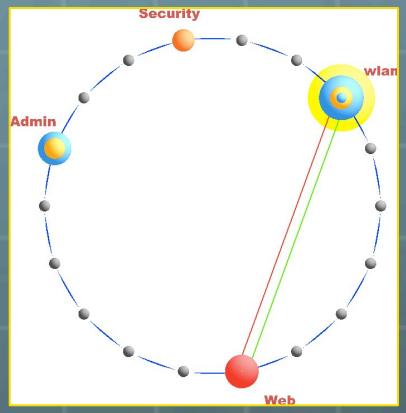


Case Study

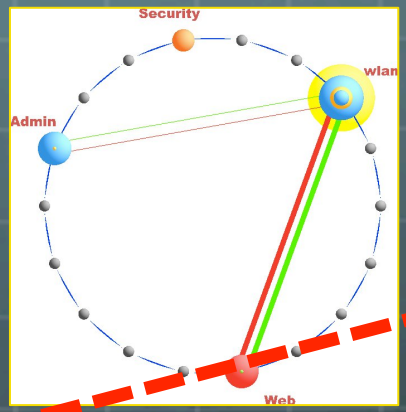
- Network:
  - /17
  - Separated into 3 hierarchies:
    - Admin, Security, and wlan (public access)
    - 1 other group introduced for ‘outside’ IPs
- Data
  - Protocol/volume aggregates
    - SiLK tools used to generate protocol bags

Case Study

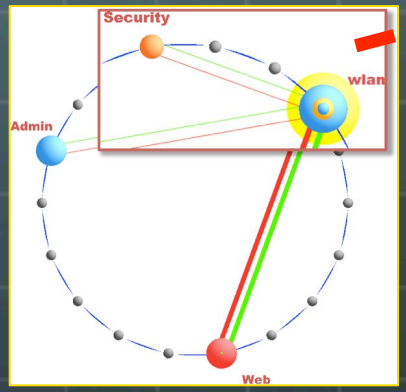
Day 1



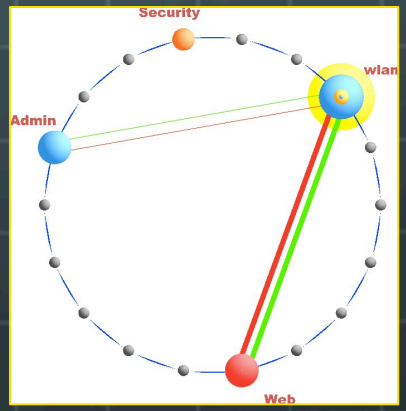
Day 2

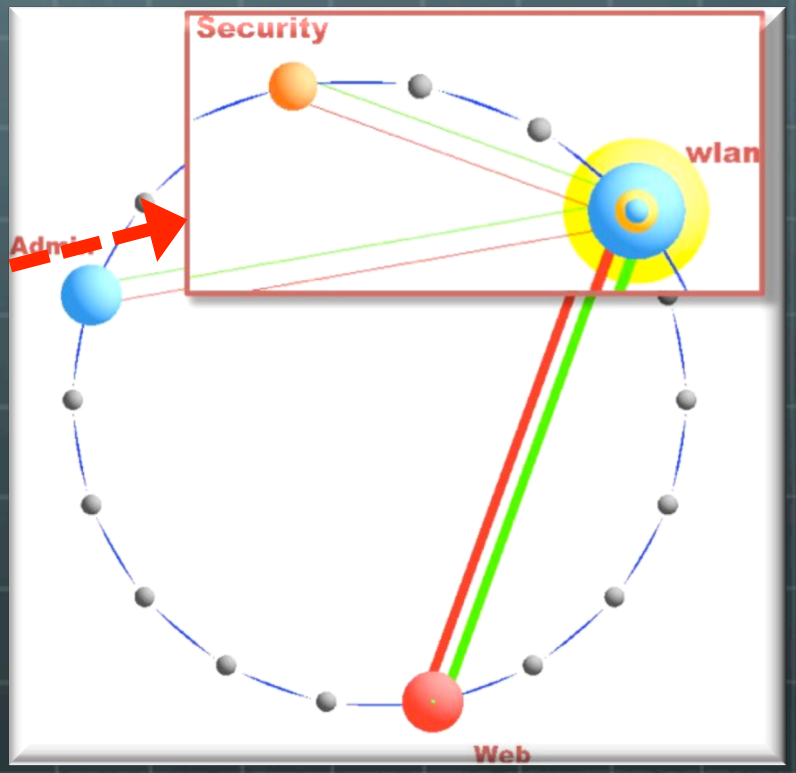


Day 3

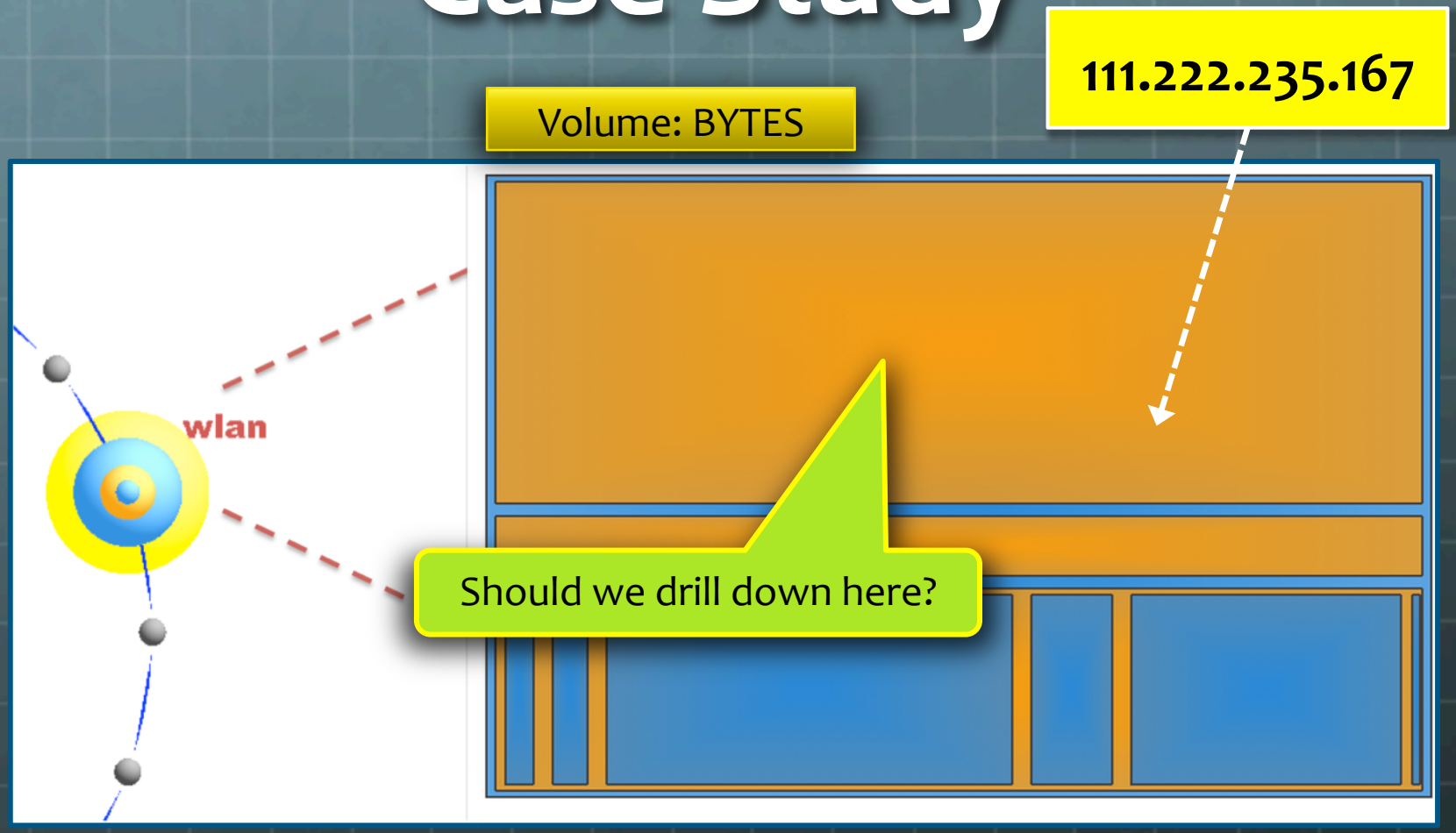


Day 4

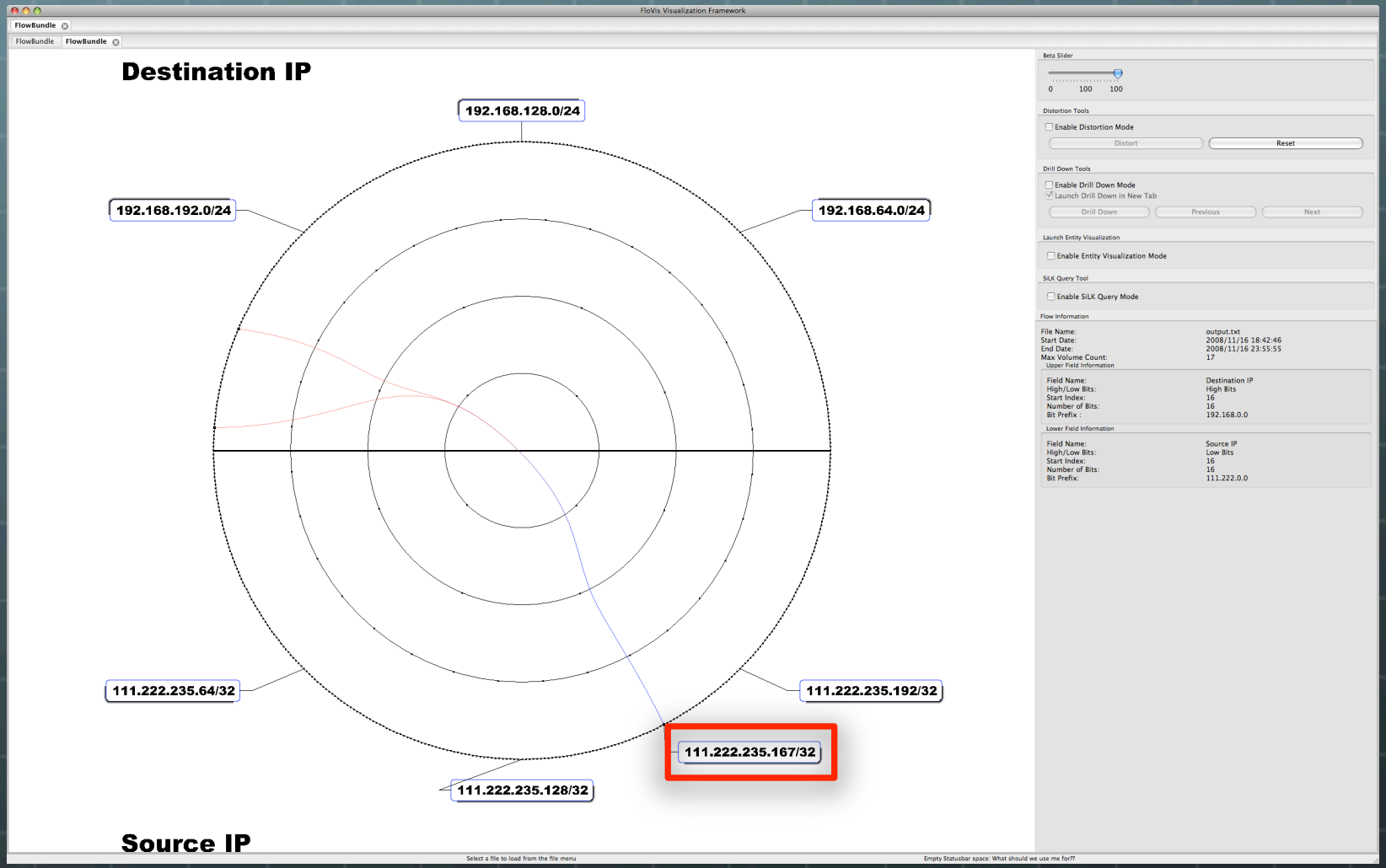




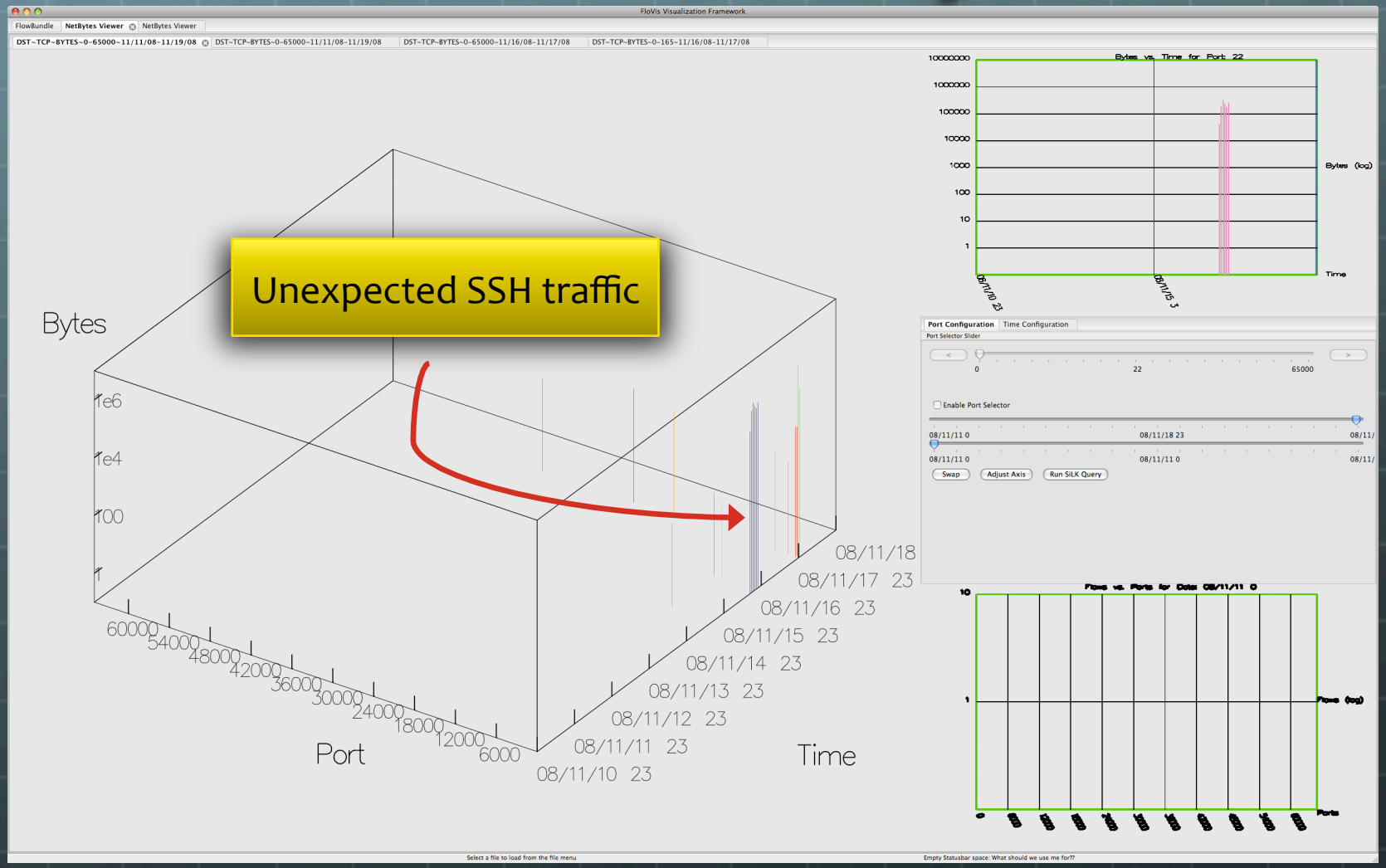
Case Study



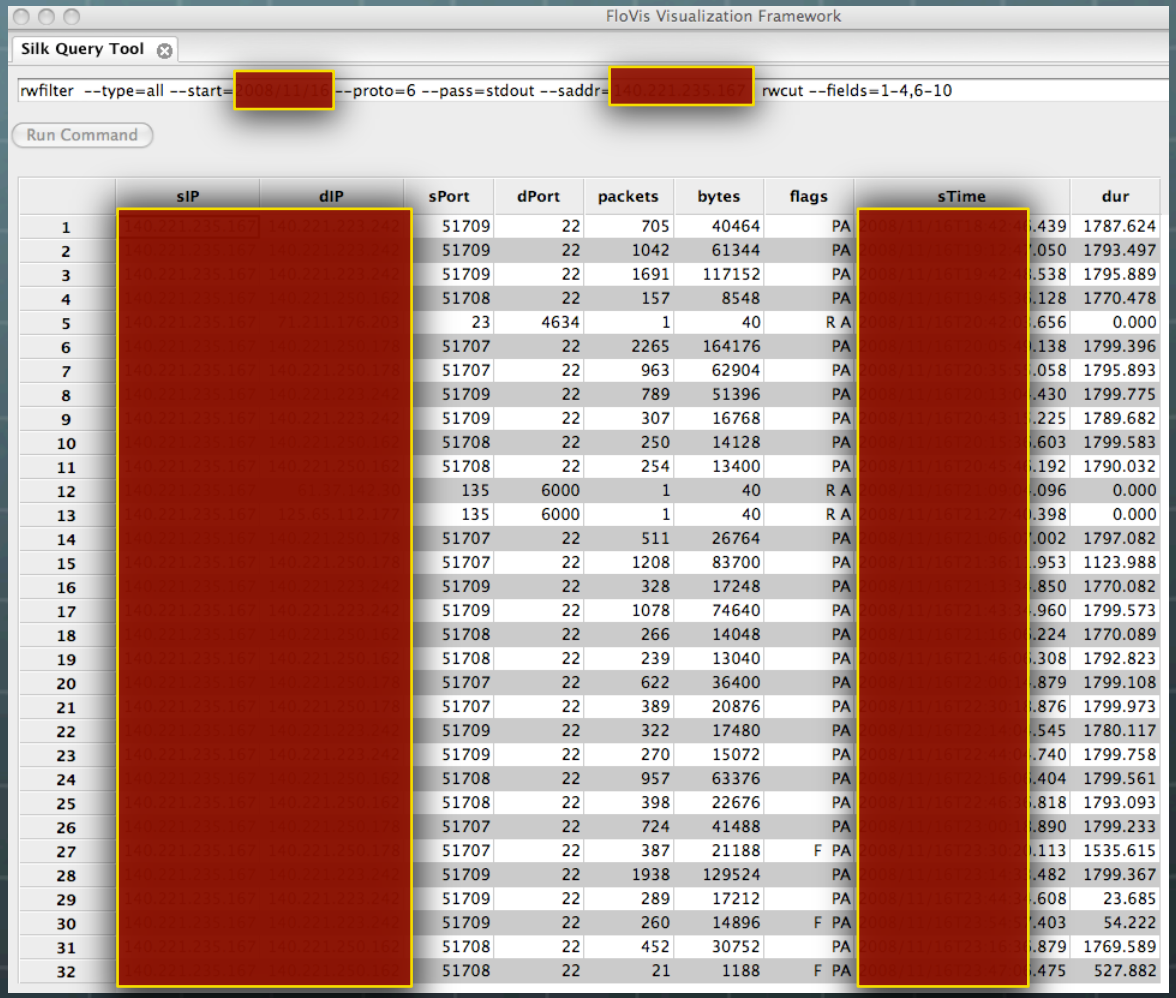
Case Study


FloVis Visualization Framework
FlowBundle
FlowBundle
FlowBundle
Destination IP
192.168.128.0/24
192.168.192.0/24
192.168.64.0/24
111.222.235.64/32
111.222.235.192/32
111.222.235.167/32
111.222.235.128/32
Source IP
Beta Slider
0
100
100
Distortion Tools
Enable Distortion Mode
Distort
Reset
Drill Down Tools
Enable Drill Down Mode
Launch Drill Down in New Tab
Drill Down
Previous
Next
Launch Entity Visualization
Enable Entity Visualization Mode
SiLK Query Tool
Enable SiLK Query Mode
Flow Information
File Name: output.txt
Start Date: 2008/11/16 18:42:46
End Date: 2008/11/16 23:55:55
Max Volume Count: 17
Upper Field Information
Field Name: Destination IP
High/Low Bits: High Bits
Start Index: 16
Number of Bits: 16
Bit Prefix : 192.168.0.0
Lower Field Information
Field Name: Source IP
High/Low Bits: Low Bits
Start Index: 16
Number of Bits: 16
Bit Prefix: 111.222.0.0
Select a file to load from the file menu
Empty Statusbar space: What should we use me for??

Case Study

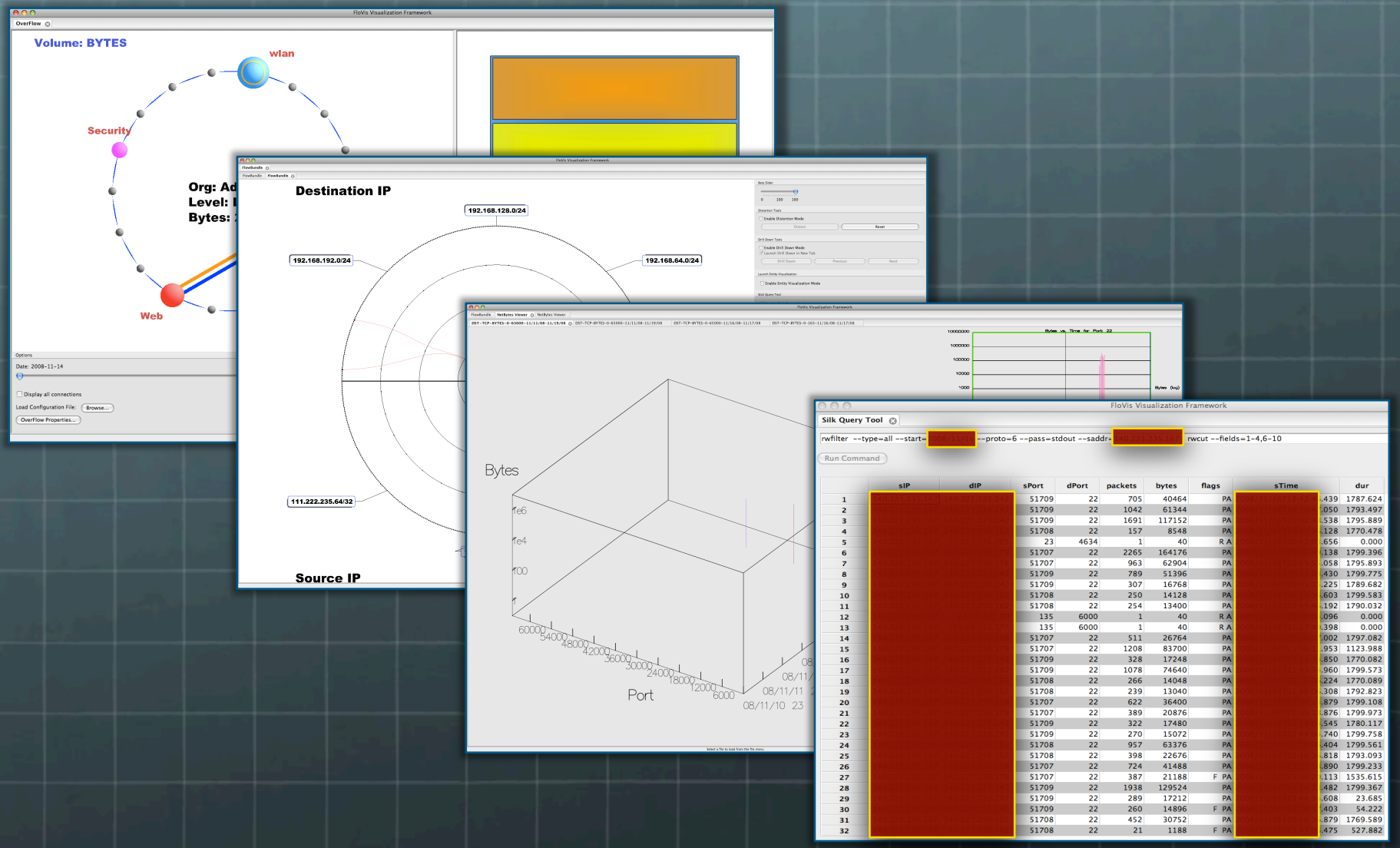

FloVis Visualization Framework
FlowBundle
NetBytes Viewer
NetBytes Viewer
DST~TCP~BYTES~0~65000~11/11/08~11/19/08
DST~TCP~BYTES~0~65000~11/11/08~11/19/08
DST~TCP~BYTES~0~65000~11/16/08~11/17/08
DST~TCP~BYTES~0~165~11/16/08~11/17/08
Unexpected SSH traffic
Bytes
1e6
1e4
100
1
60000
54000
48000
42000
36000
30000
24000
18000
12000
6000
Port
08/11/10 23
08/11/11 23
08/11/12 23
08/11/13 23
08/11/14 23
08/11/15 23
08/11/16 23
08/11/17 23
08/11/18
Time
Bytes vs. Time for Port 22
10000000
1000000
100000
10000
1000
100
10
1
Bytes (log)
Time
08/11/10 23
08/11/15 1
Port Configuration
Time Configuration
Port Selector Slider
0
22
65000
Enable Port Selector
08/11/11 0
08/11/18 23
08/11/
08/11/11 0
08/11/11 0
08/11/
Swap
Adjust Axis
Run SiLK Query
10
1
Flows (log)
Ports
Select a file to load from the file menu
Empty Statusbar space: What should we use me for??

Case Study

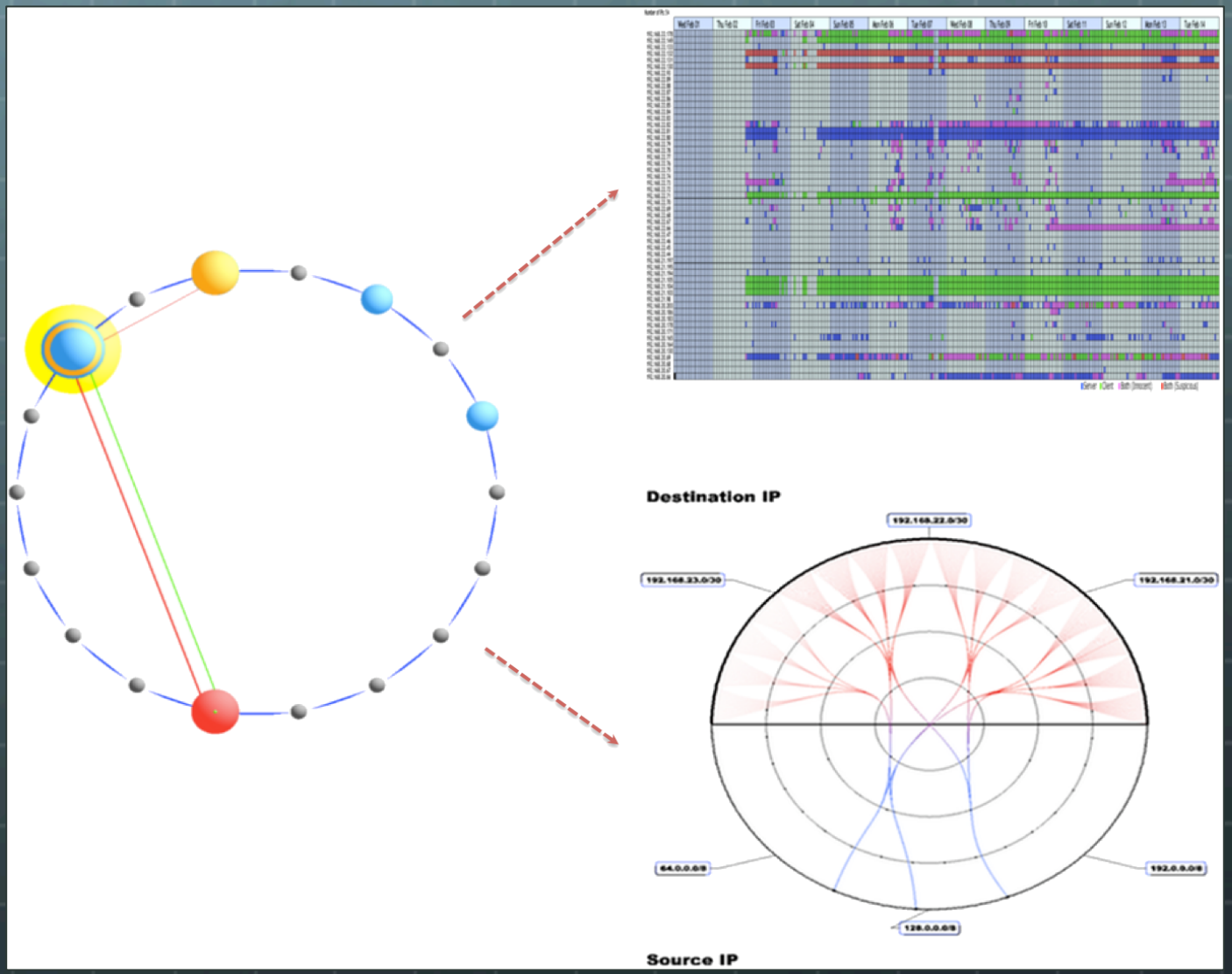


	sIP	dIP	sPort	dPort	packets	bytes	flags	sTime	dur
1	[redacted]		51709	22	705	40464	PA		1787.624
2			51709	22	1042	61344	PA		1793.497
3			51709	22	1691	117152	PA		1795.889
4			51708	22	157	8548	PA		1770.478
5			23	4634	1	40	R A		0.000
6			51707	22	2265	164176	PA		1799.396
7			51707	22	963	62904	PA		1795.893
8			51709	22	789	51396	PA		1799.775
9			51709	22	307	16768	PA		1789.682
10			51708	22	250	14128	PA		1799.583
11			51708	22	254	13400	PA		1790.032
12			135	6000	1	40	R A		0.000
13			135	6000	1	40	R A		0.000
14			51707	22	511	26764	PA		1797.082
15			51707	22	1208	83700	PA		1123.988
16			51709	22	328	17248	PA		1770.082
17			51709	22	1078	74640	PA		1799.573
18			51708	22	266	14048	PA		1770.089
19			51708	22	239	13040	PA		1792.823
20			51707	22	622	36400	PA		1799.108
21			51707	22	389	20876	PA		1799.973
22			51709	22	322	17480	PA		1780.117
23			51709	22	270	15072	PA		1799.758
24			51708	22	957	63376	PA		1799.561
25			51708	22	398	22676	PA		1793.093
26			51707	22	724	41488	PA		1799.233
27			51707	22	387	21188	F PA		1535.615
28			51709	22	1938	129524	PA		1799.367
29			51709	22	289	17212	PA		23.685
30			51709	22	260	14896	F PA		54.222
31			51708	22	452	30752	PA		1769.589
32			51708	22	21	1188	F PA		527.882

FloVis: Context



Future Work


Destination IP
192.168.22.0/30
192.168.23.0/30
192.168.21.0/30
64.0.0.0/8
192.0.0.0/8
128.0.0.0/8
Source IP

Conclusions

- Two accomplishments:
  - 1. Overview of network hierarchies
    - User-defined
  - 2. High-level view of simple communication characteristics (e.g., volumes, connections)
    - Assists the analyst in focusing attention

Learn more…

- T. Taylor, D. Paterson, J. Glanfield, C. Gates, S. Brooks, J. McHugh (2009) FloVis: Flow Visualization System. In *Proceedings of the Cybersecurity Applications and Technologies Conference for Homeland Security* (CATCH). Washington, DC. March 3-4, 2009.
- Teryl Taylor, Stephen Brooks and John McHugh. NetBytes Viewer: An Entity-based NetFlow Visualization Utility for Identifying Intrusive Behavior. In Goodall et al. (eds.), *Mathematics and Visualization (Proceedings of VizSEC)*, Springer-Verlag, August, 2008
- http://www.flovis.net

QUESTIONS?