OverFlow: An Overview Visualization for Network Analysis

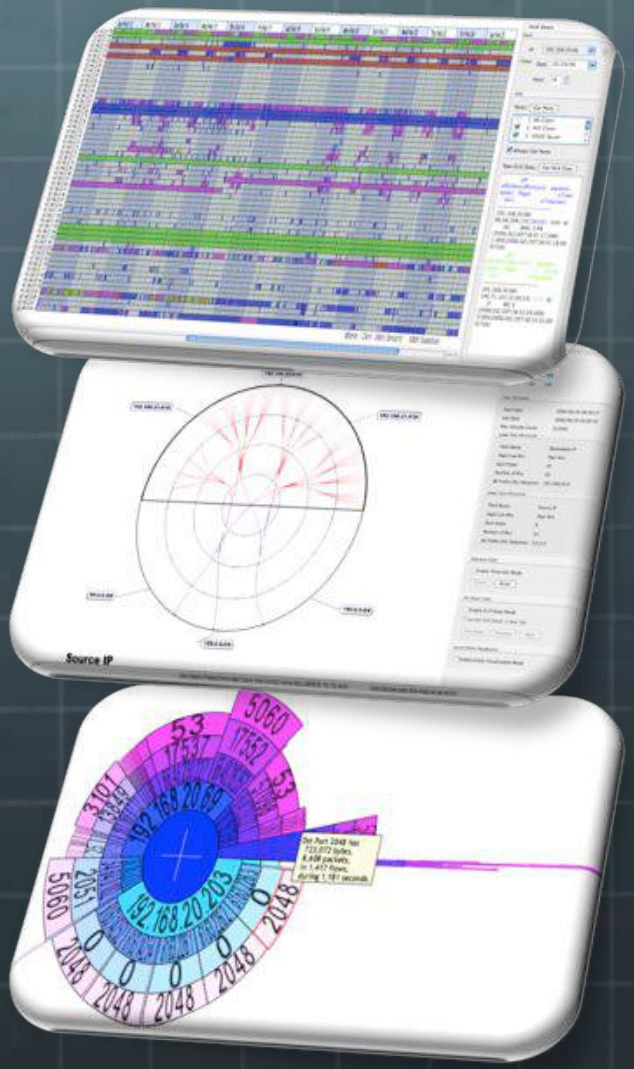
J. Glanfield, S. Brooks, T. Taylor, D. Paterson, C. Smith, C. Gates, J. McHugh

Outline

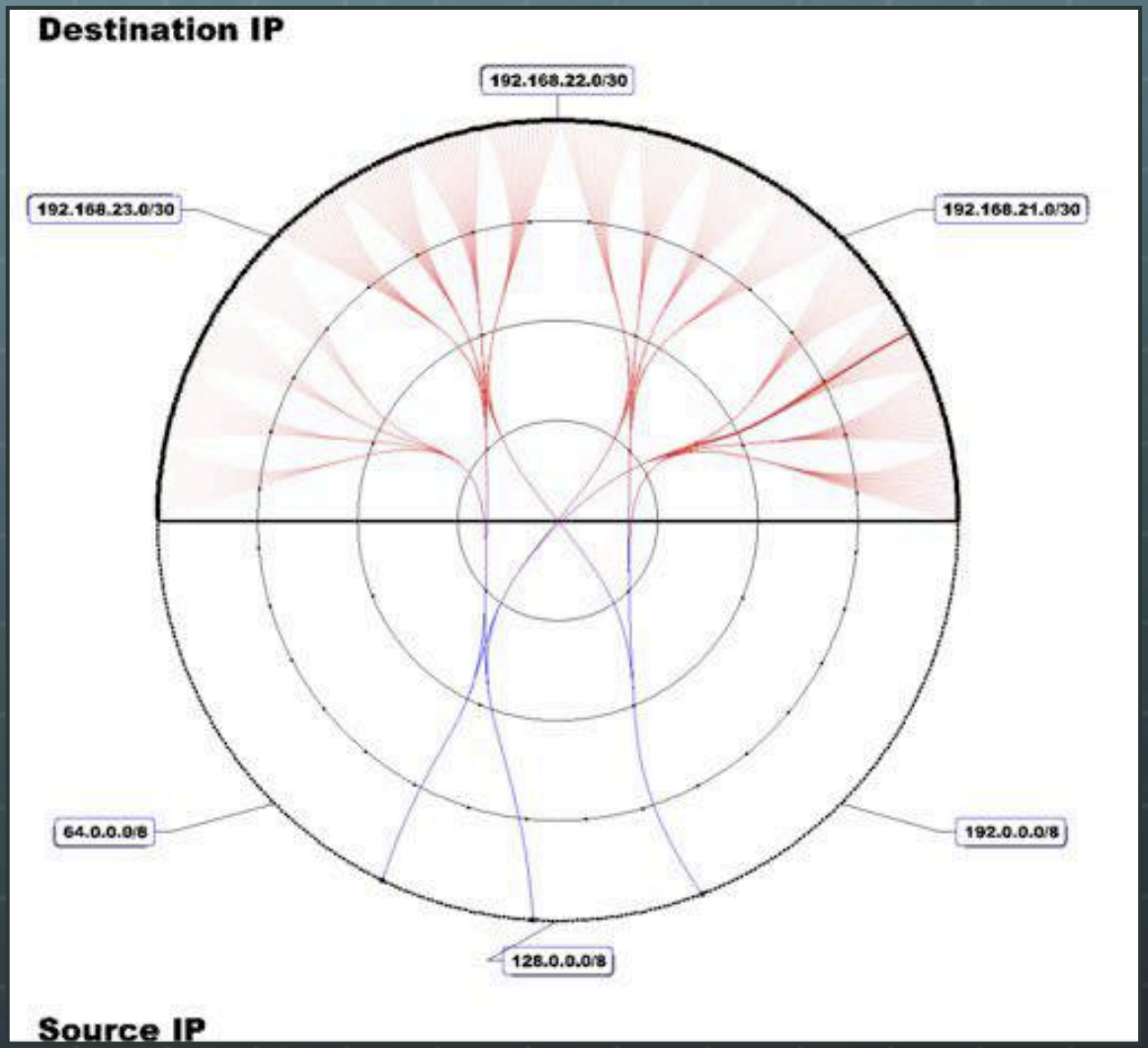
- FloVis: crash course
- OverFlow
  - Motivation
  - Description
  - Case Study
- Future Work & Conclusions

FloVis: Crash Course

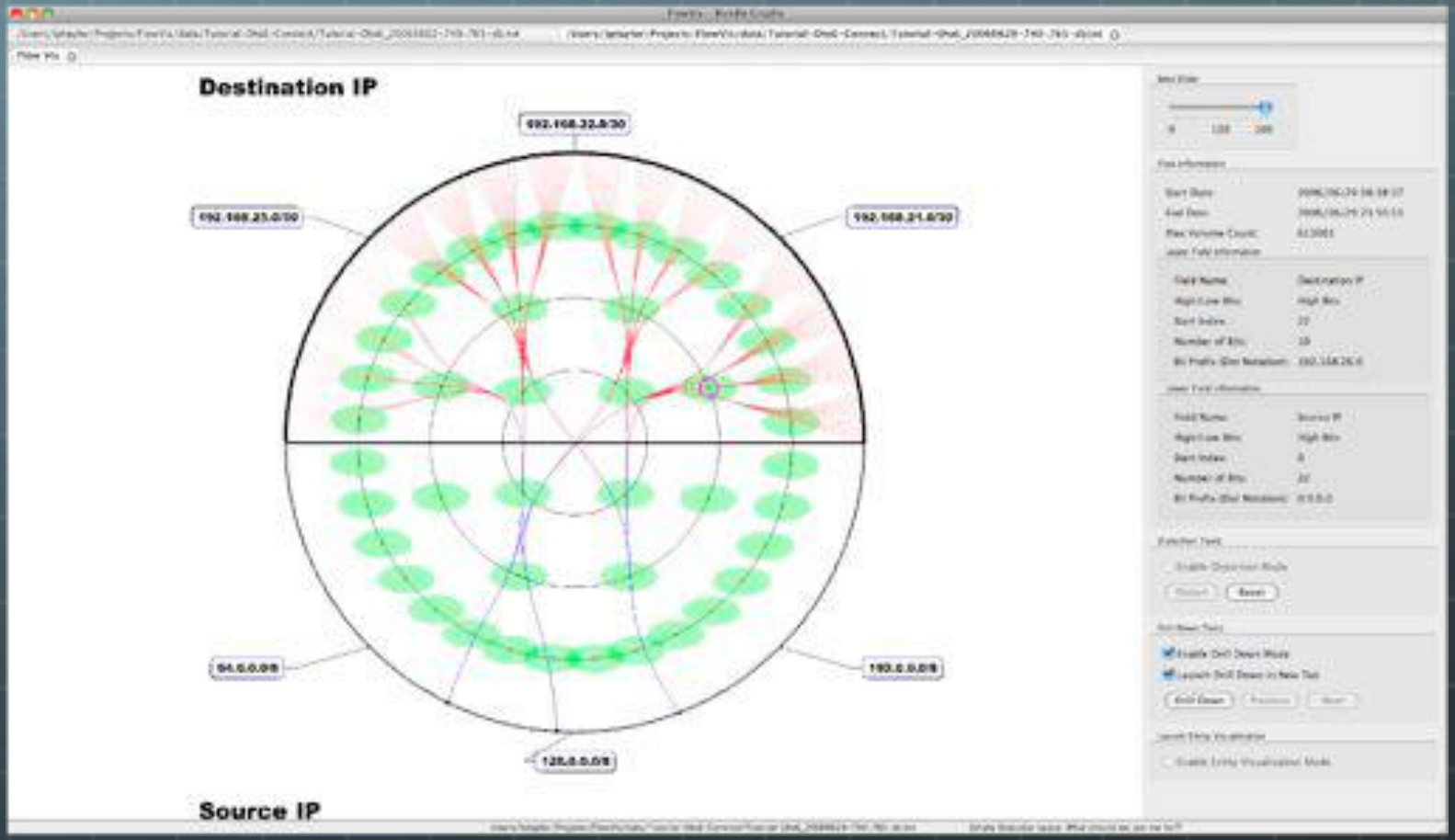
- Network Visualization Framework
  - Promotes extensibility
    - Users create plug-ins
  - Supports transitioning/pivoting
    - Viz-to-viz communication
    - Currently in progress…



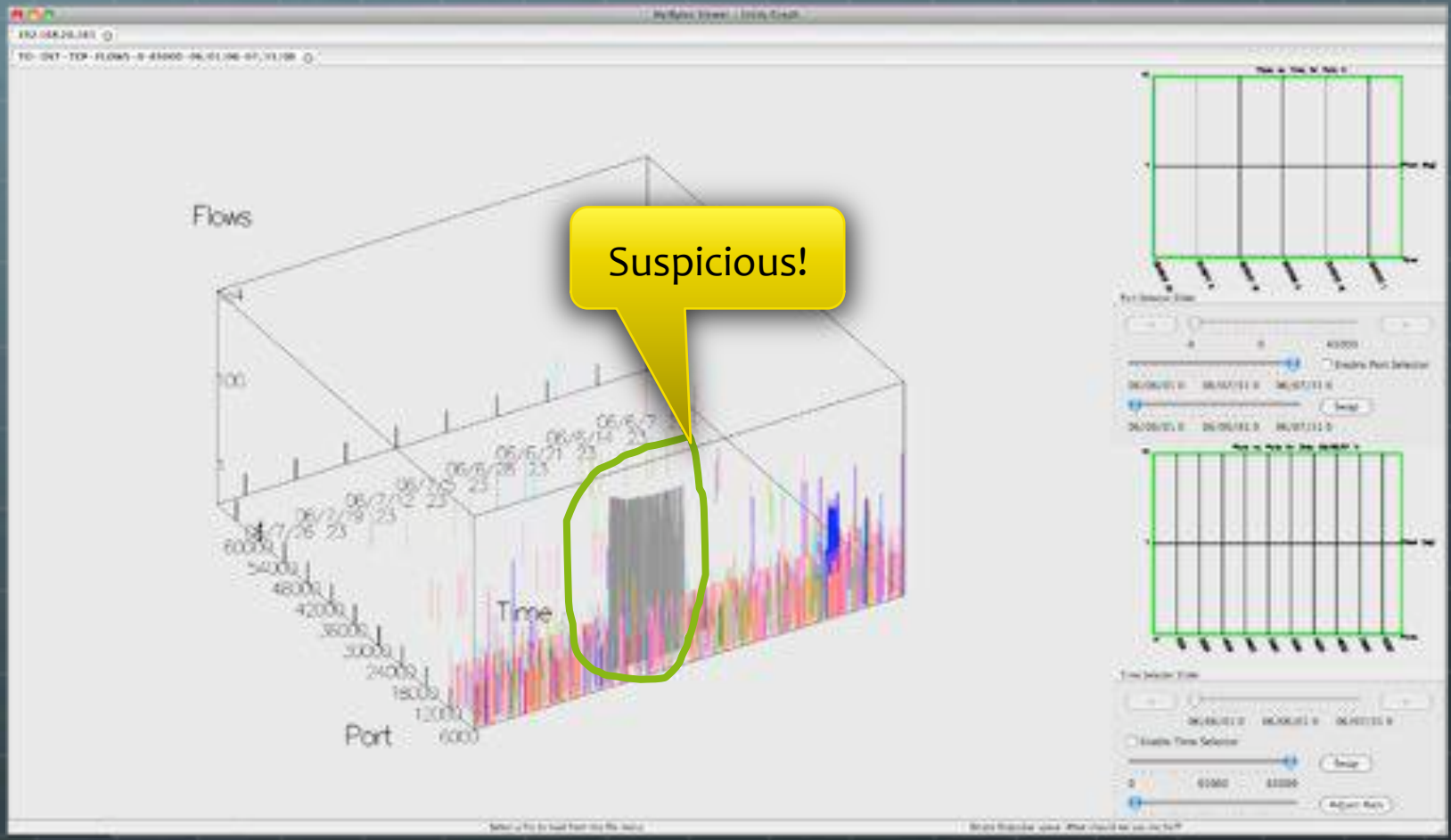
Example: FlowBundle



FlowBundle: Drill down

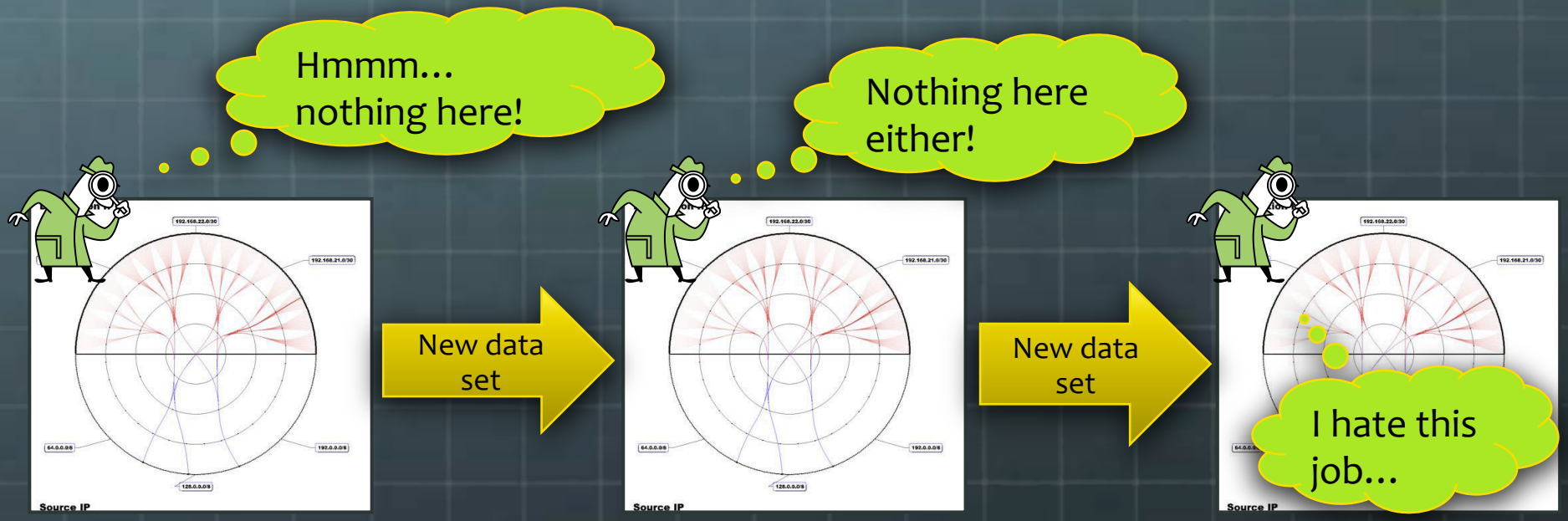


Drill down: continued



Question!

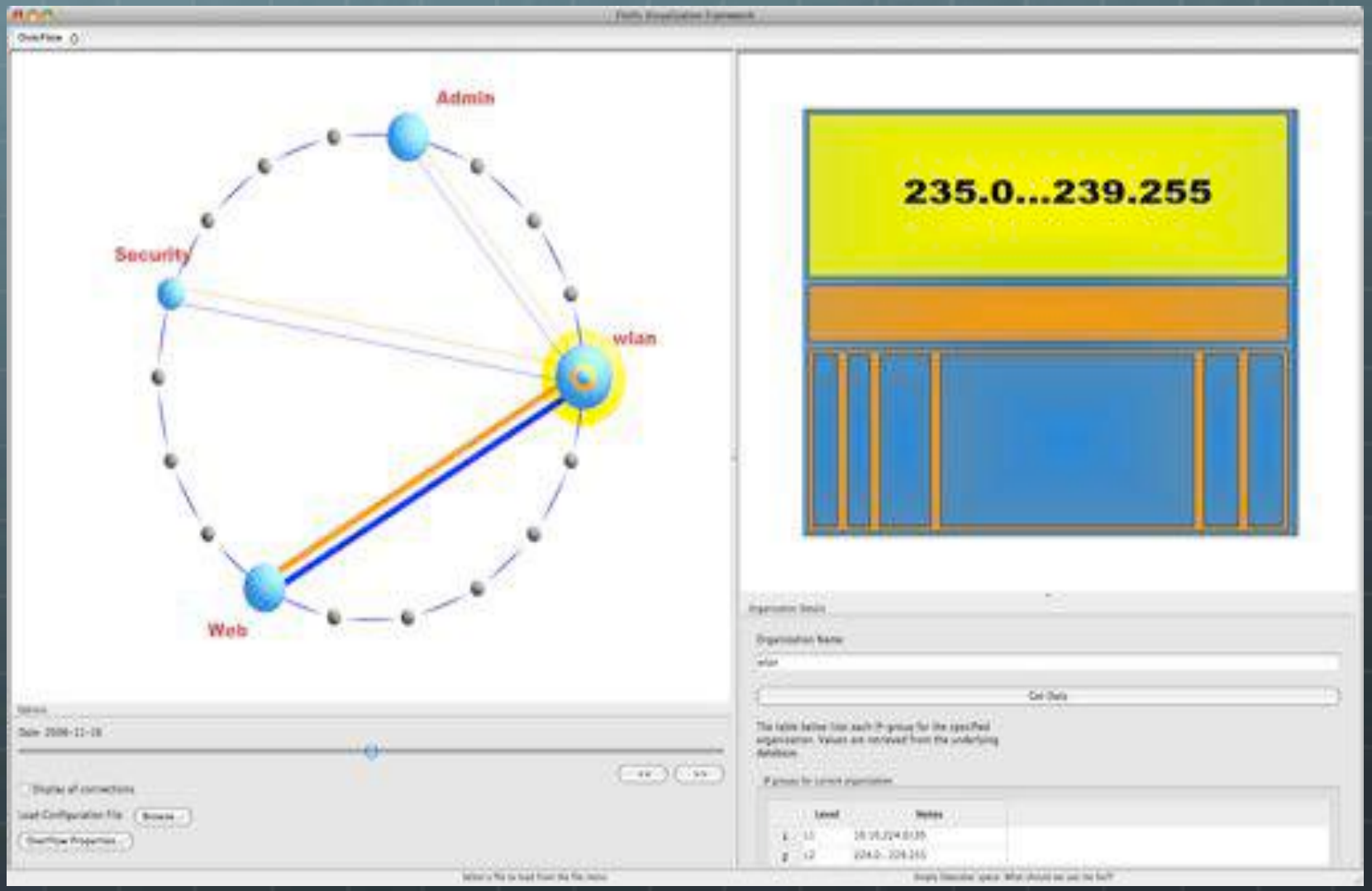
- What motivated the original query?
  - trial-and-error?



OverFlow: Motivation

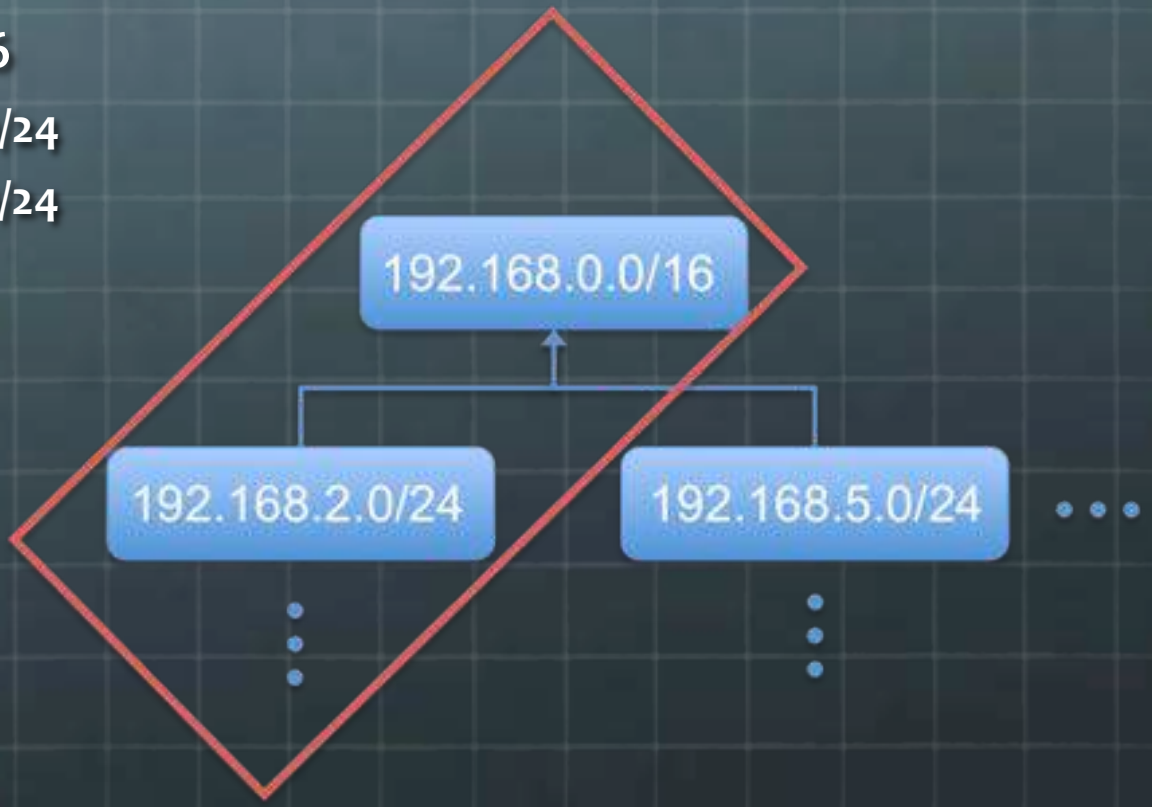
- We need a starting point
- We don't want to go back to the data every time nothing is found worth investigating
  - (reduce "cognitive load" or "cognitive burden")
- FloCon 2009: analysts described need to group IPs
  - Organizational groupings
  - Top-N lists
  - Etc.

OverFlow

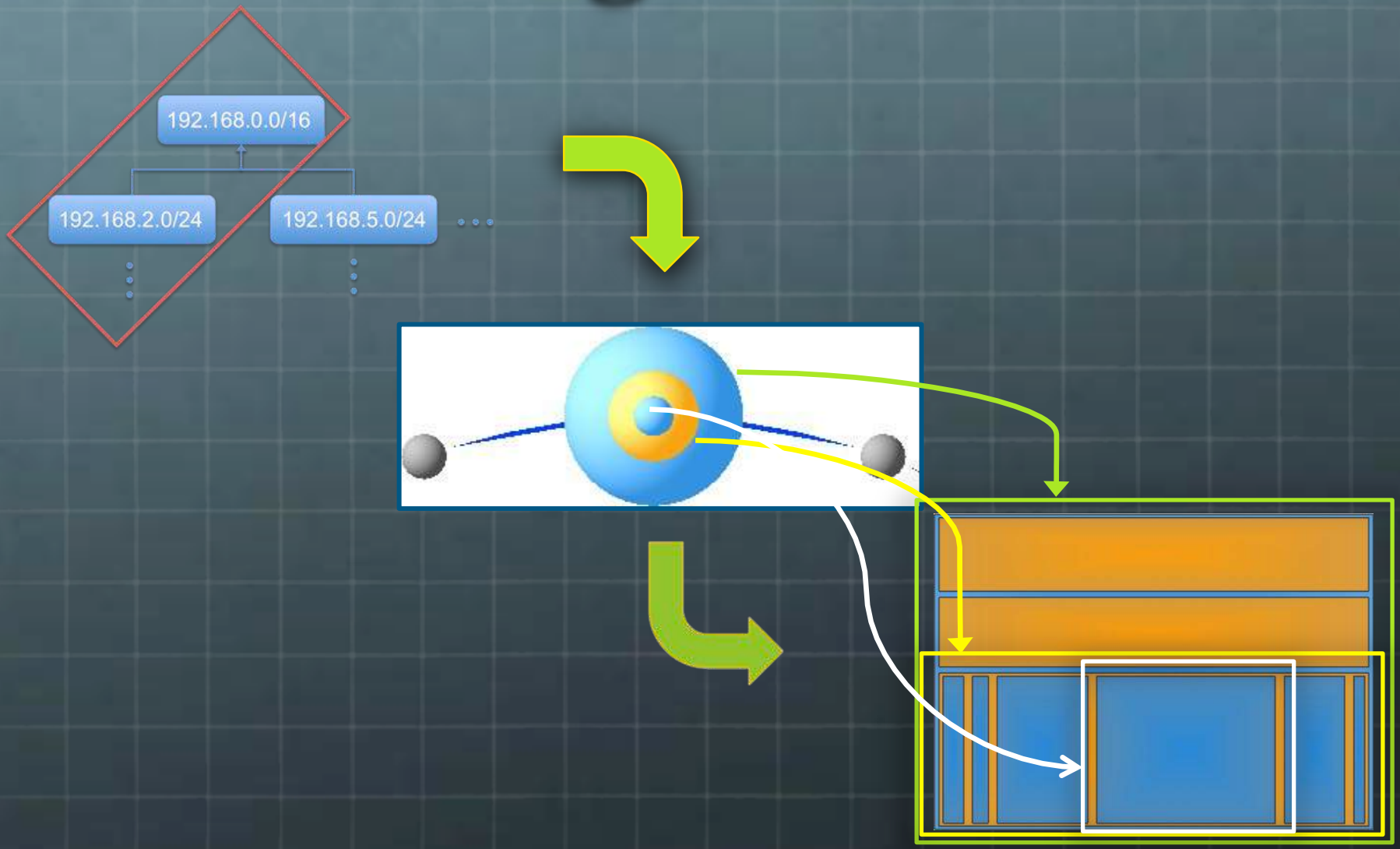


Data Representation

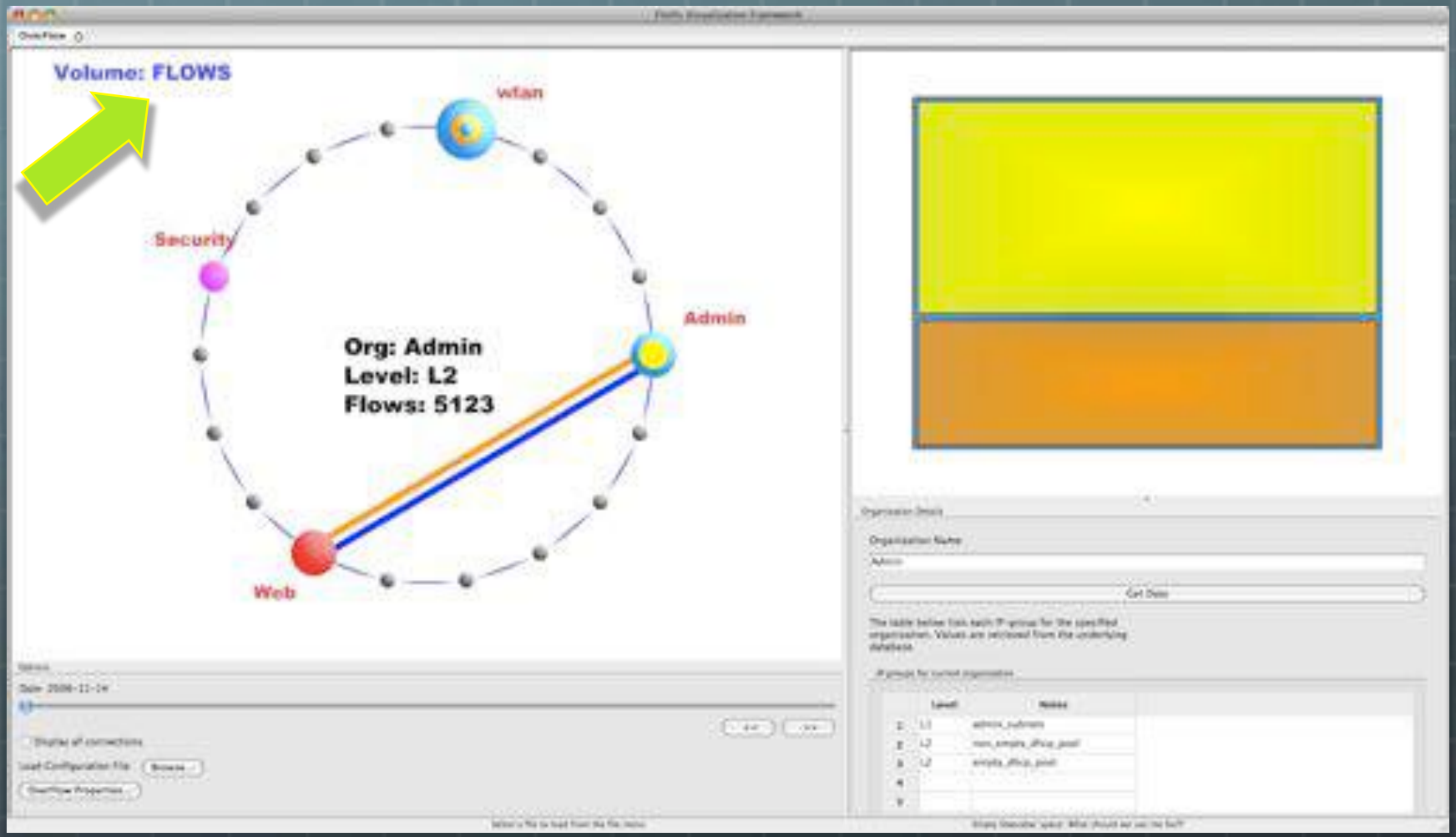
- Organize arbitrary network hierarchies:
  - By hand:
    - 192.168.0.0/16
      - 192.168.2.0/24
      - 192.168.5.0/24
  - Or:



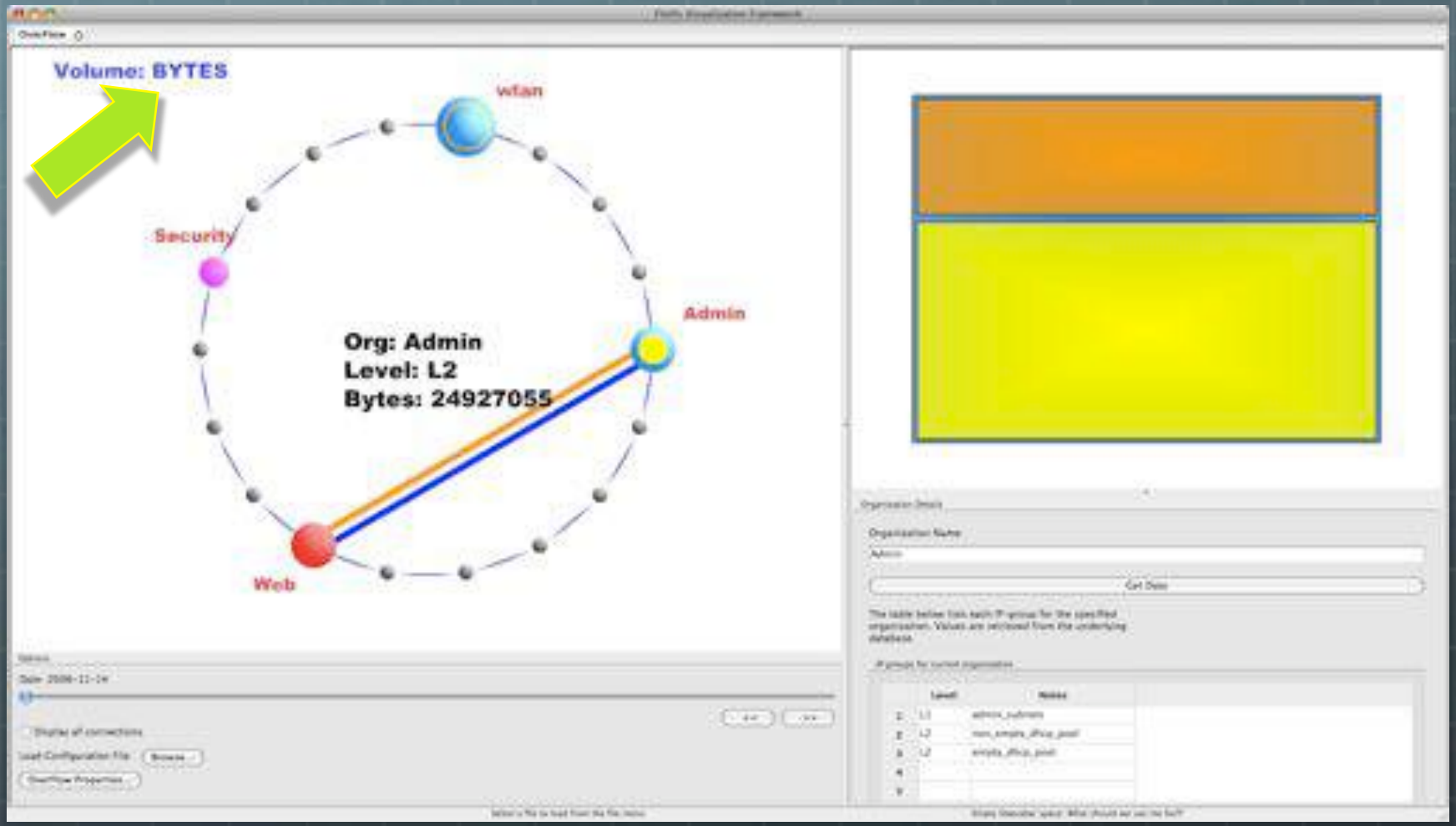
Visualizing Hierarchies



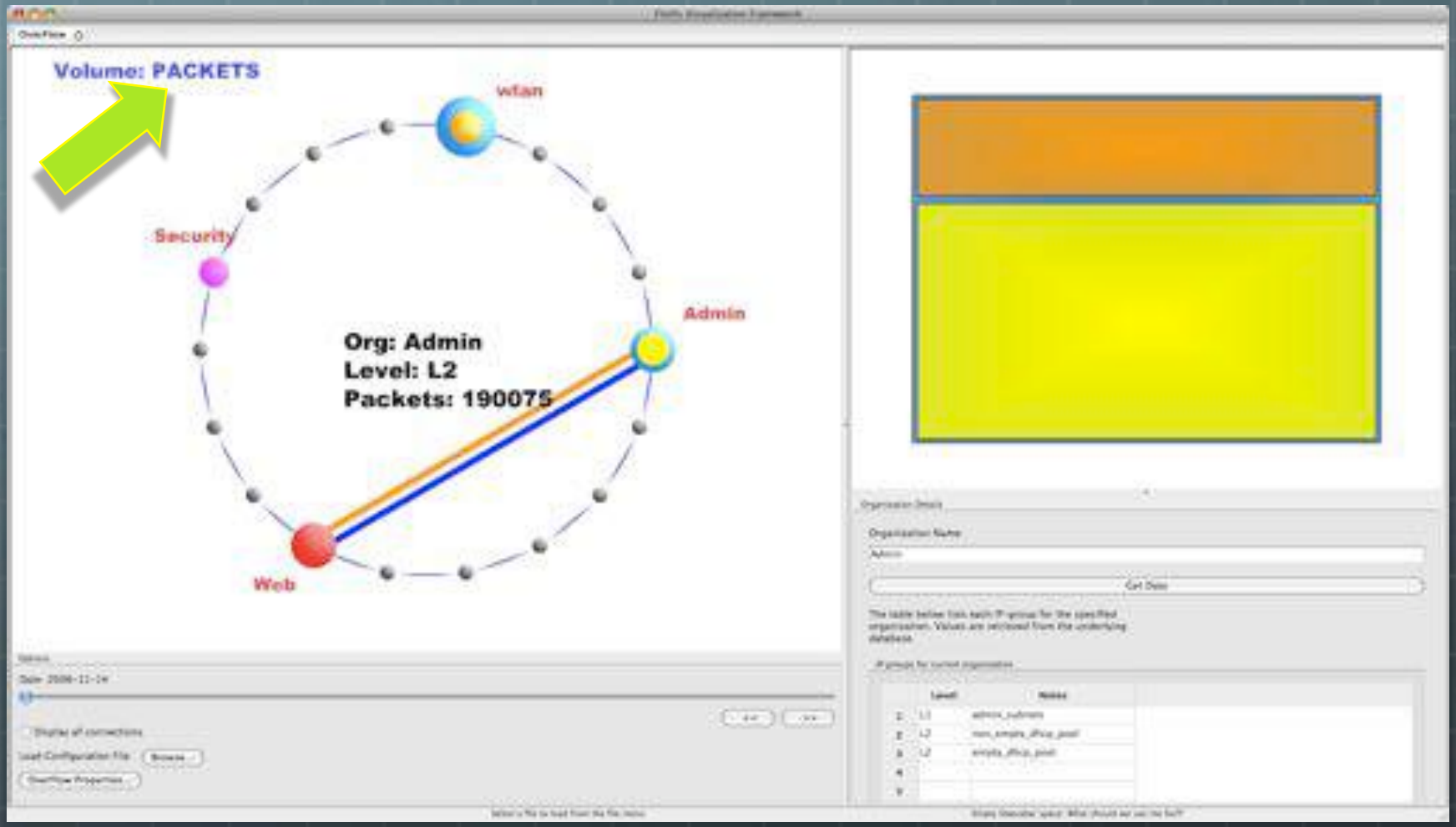
Visualizing Volumes



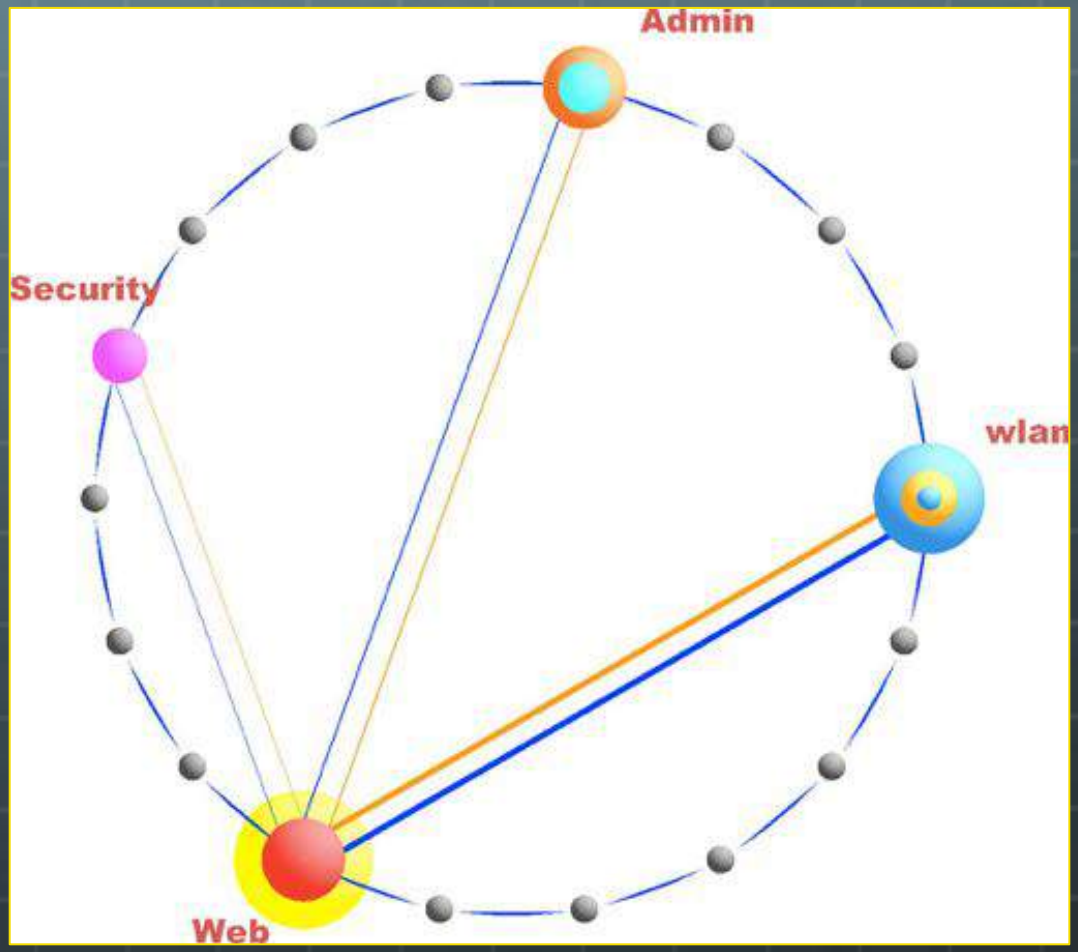
Visualizing Volumes



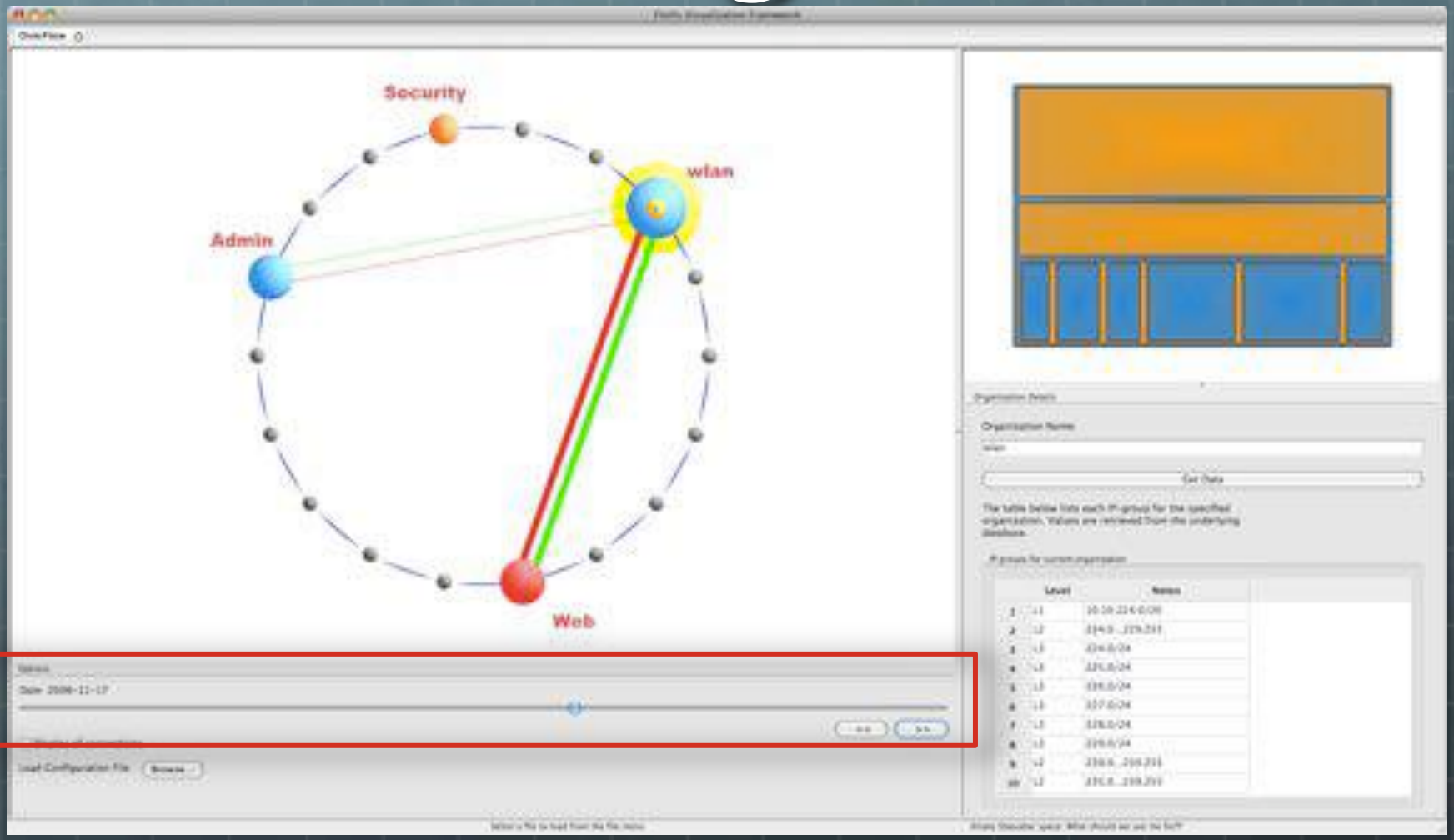
Visualizing Volumes



Visualizing Communications



Transitioning Over Time

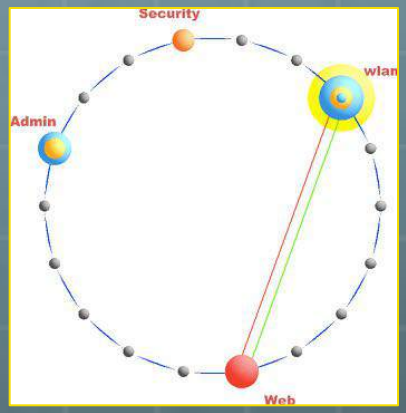


Case Study

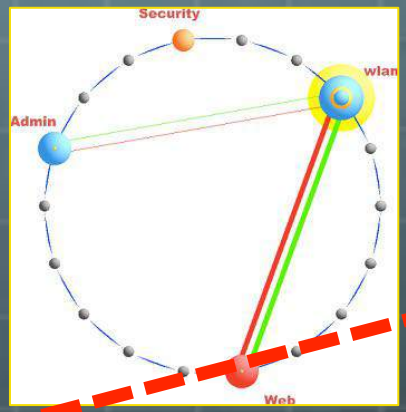
- Network:
  - /17
  - Separated into 3 hierarchies:
    - Admin, Security, and wlan (public access)
    - 1 other group introduced for ‘outside’ IPs
- Data
  - Protocol/volume aggregates
    - SiLK tools used to generate protocol bags

Case Study

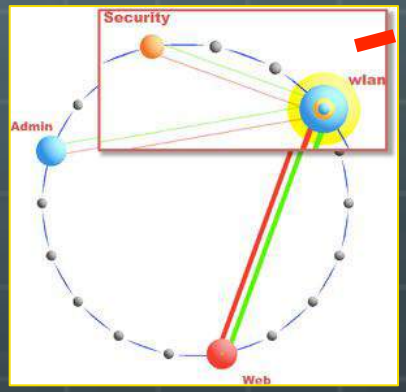
Day 1



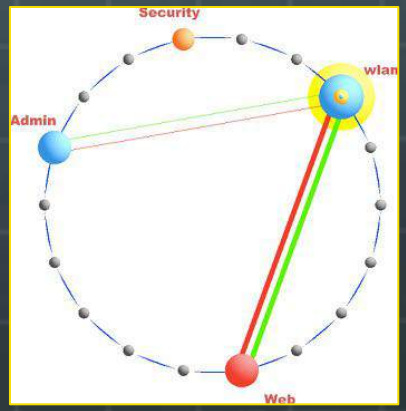
Day 2

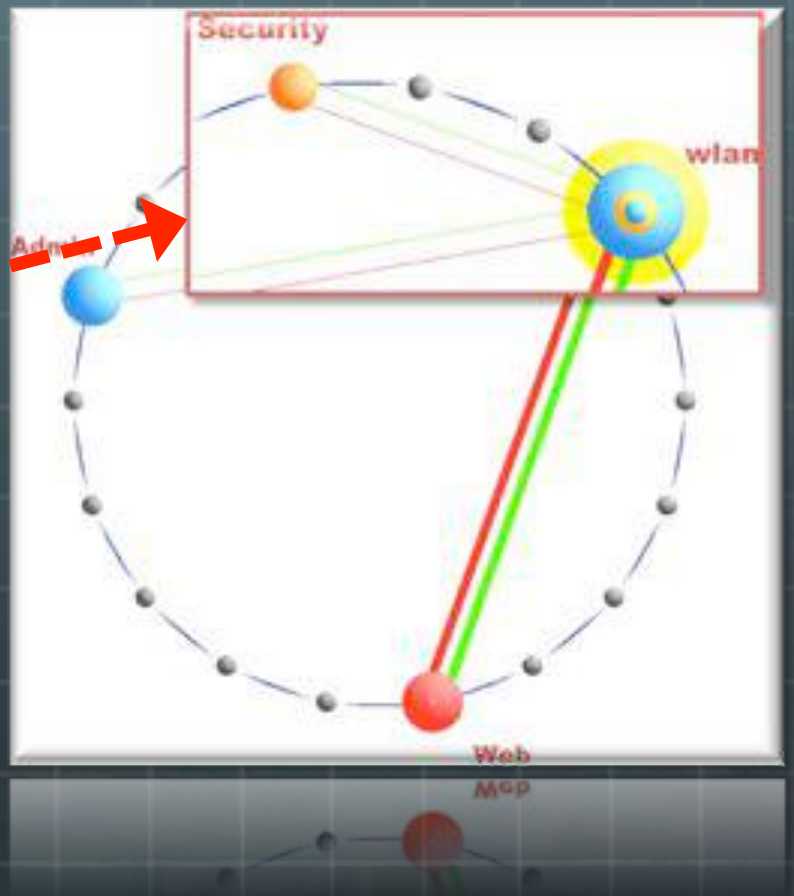


Day 3

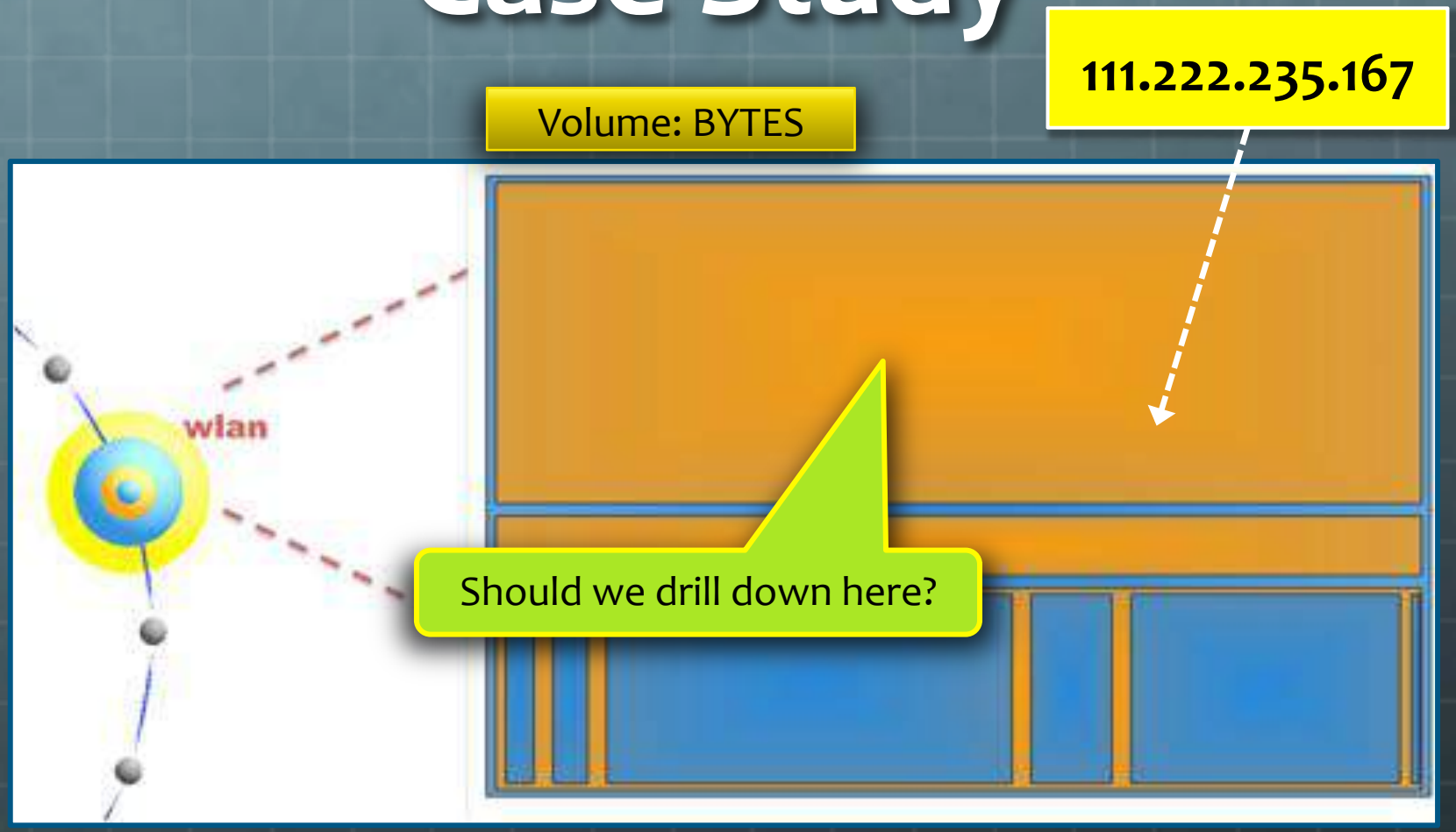


Day 4

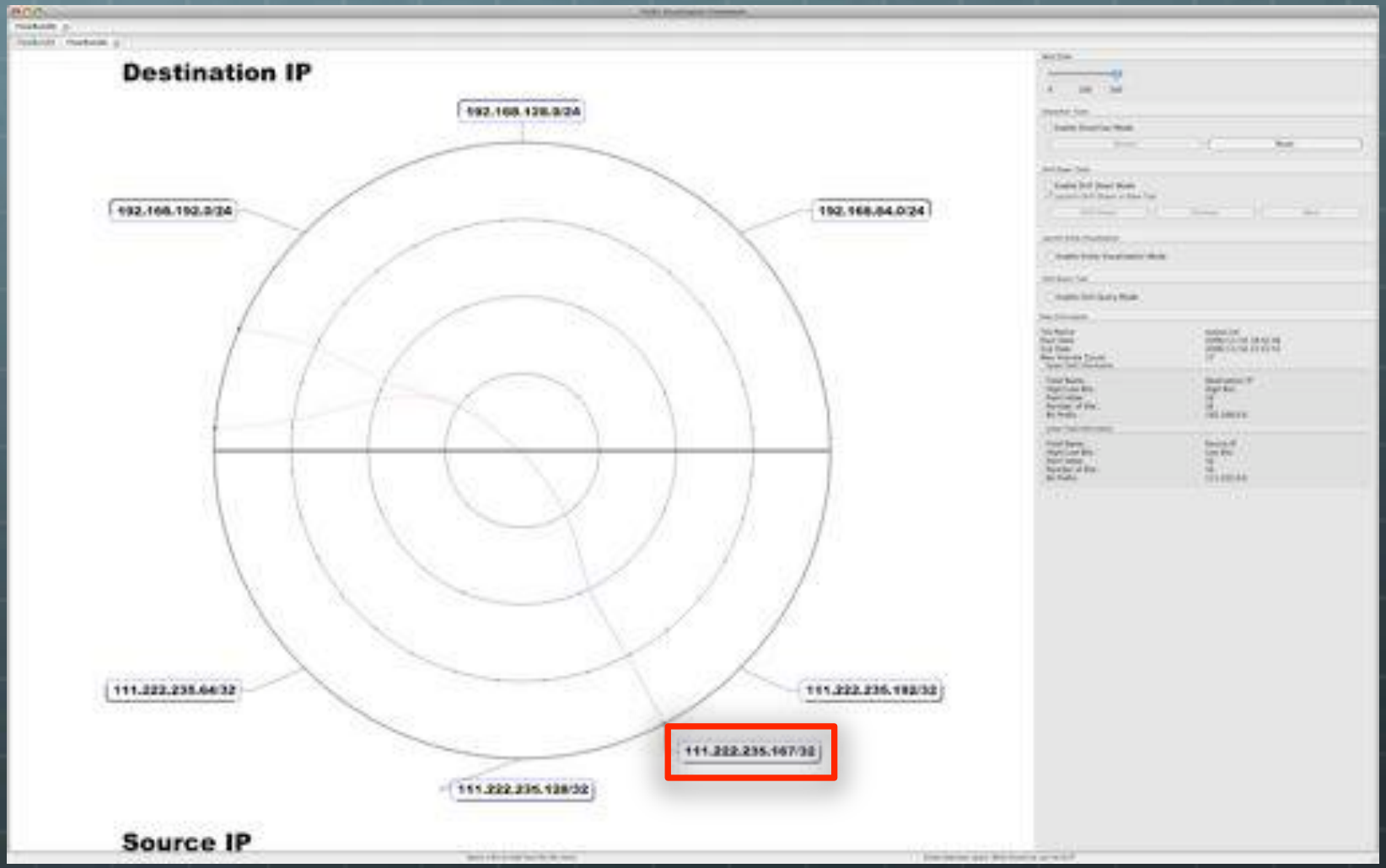




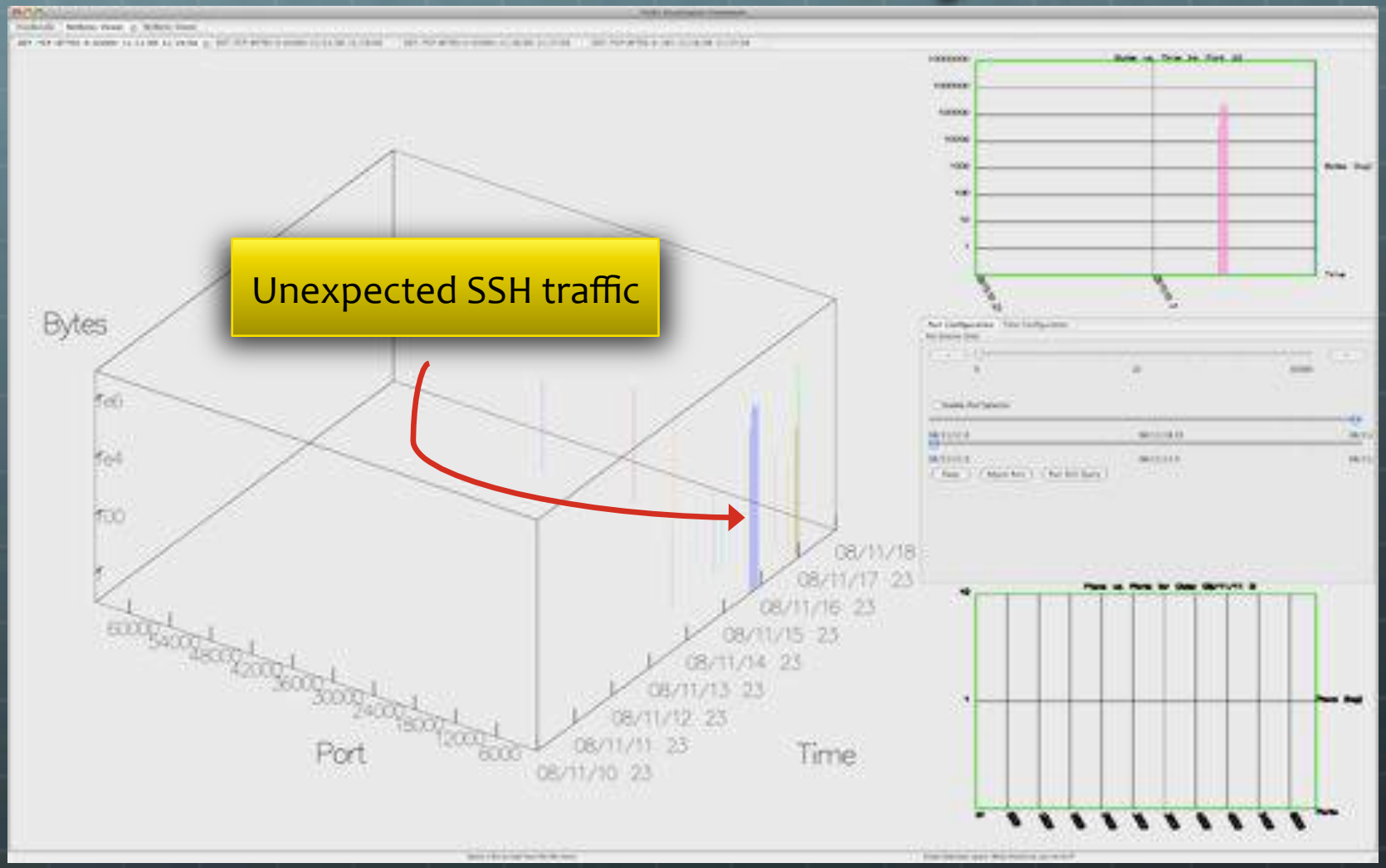
Case Study



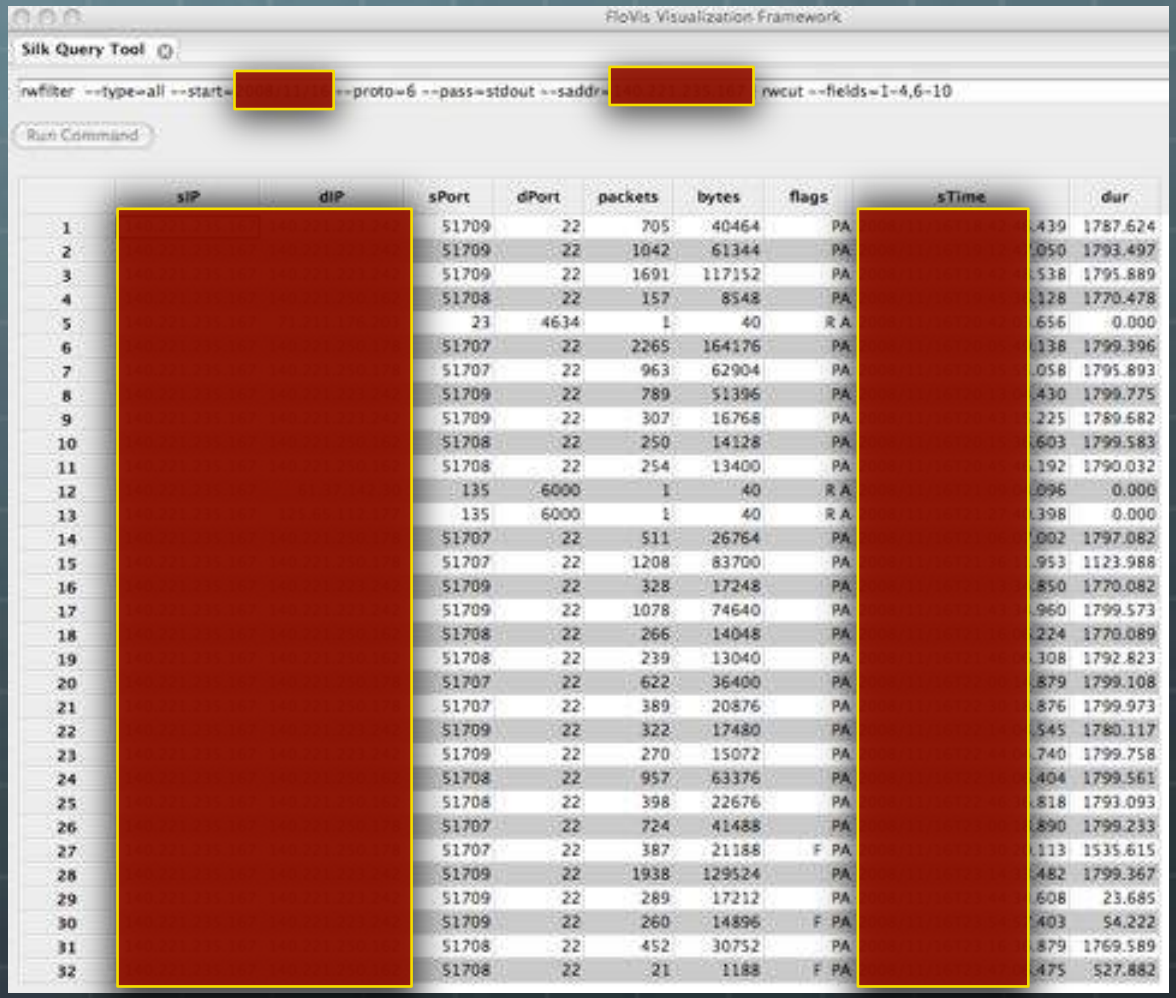
Case Study


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

Case Study

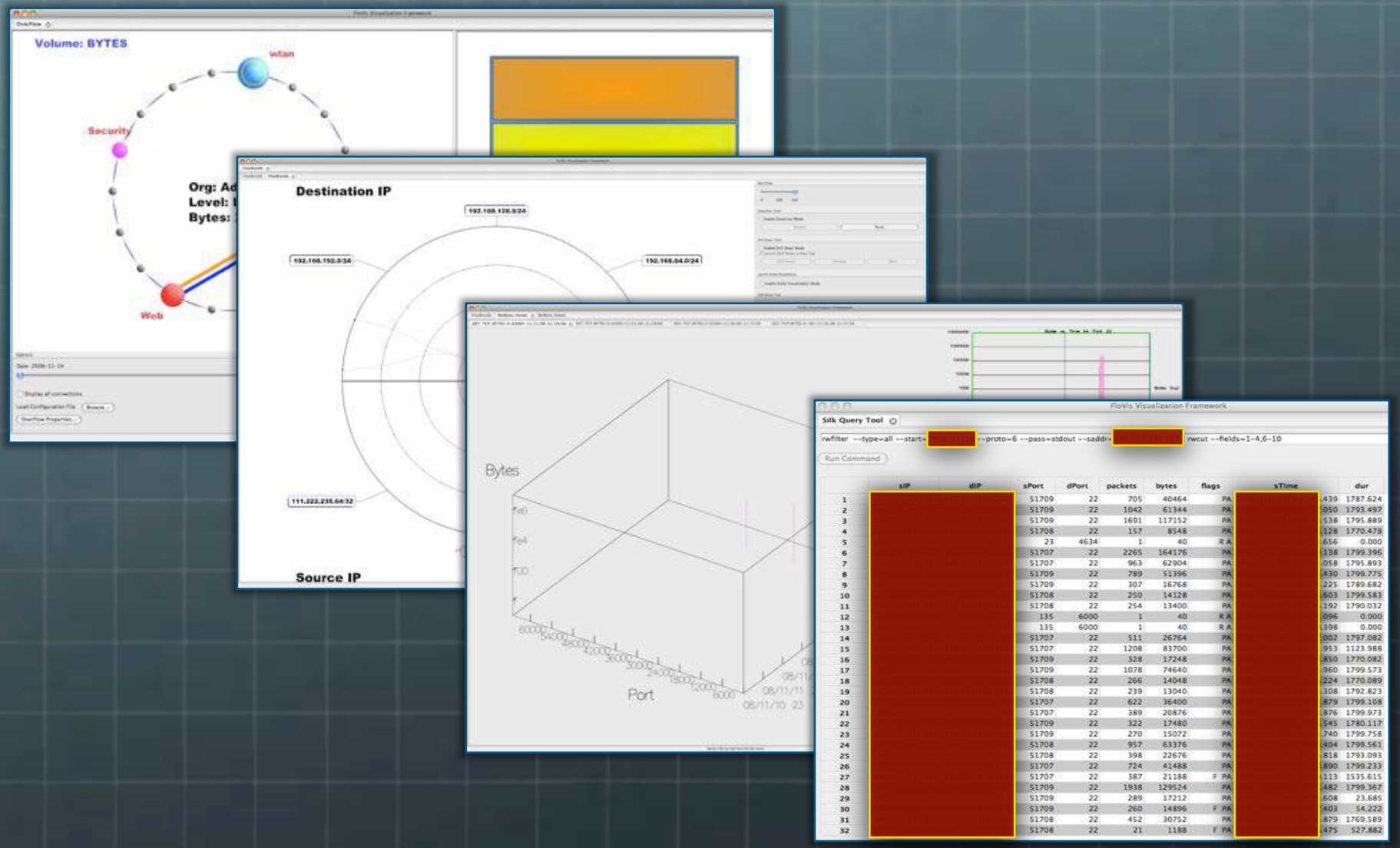

Unexpected SSH traffic
Bytes
Port
Time
08/11/18
08/11/17 23
08/11/16 23
08/11/15 23
08/11/14 23
08/11/13 23
08/11/12 23
08/11/11 23
08/11/10 23

Case Study

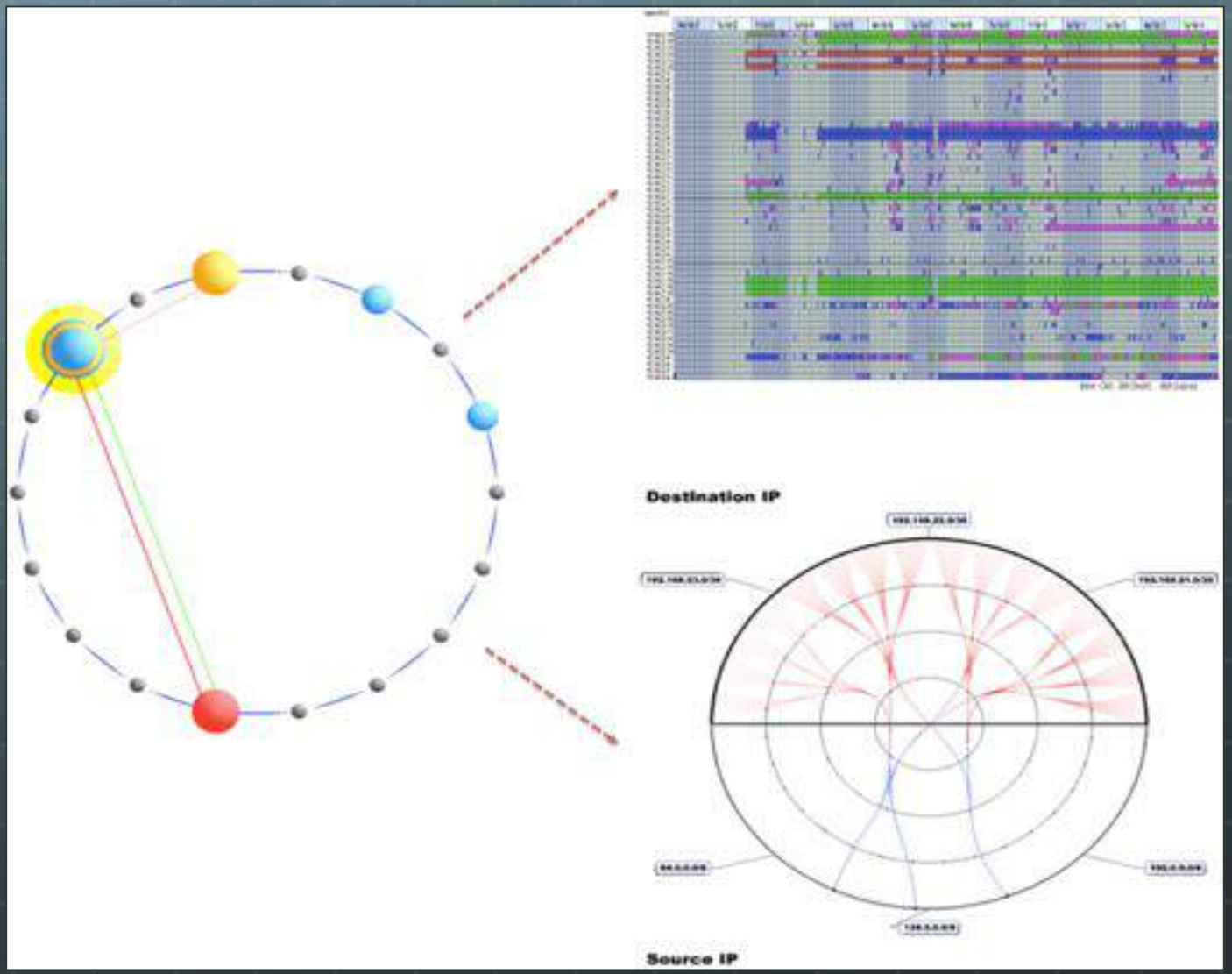


	sIP	dIP	sPort	dPort	packets	bytes	flags	sTime	dur
1	[redacted]	[redacted]	51709	22	705	40464	PA	[redacted].439	1787.624
2			51709	22	1042	61344	PA	.050	1793.497
3			51709	22	1691	117152	PA	.538	1795.889
4			51708	22	157	8548	PA	.128	1770.478
5			23	4634	1	40	R A	.656	0.000
6			51707	22	2265	164176	PA	.138	1799.396
7			51707	22	963	62904	PA	.058	1795.893
8			51709	22	789	51396	PA	.430	1799.775
9			51709	22	307	16768	PA	.225	1789.682
10			51708	22	250	14128	PA	.603	1799.583
11			51708	22	254	13400	PA	.192	1790.032
12			135	6000	1	40	R A	.096	0.000
13			135	6000	1	40	R A	.398	0.000
14			51707	22	511	26764	PA	.002	1797.082
15			51707	22	1208	83700	PA	.953	1123.988
16			51709	22	328	17248	PA	.850	1770.082
17			51709	22	1078	74640	PA	.960	1799.573
18			51708	22	266	14048	PA	.224	1770.089
19			51708	22	239	13040	PA	.108	1792.823
20			51707	22	622	36400	PA	.879	1799.108
21			51707	22	389	20876	PA	.876	1799.973
22			51709	22	322	17480	PA	.545	1780.117
23			51709	22	270	15072	PA	.740	1799.758
24			51708	22	957	63376	PA	.404	1799.561
25			51708	22	398	22676	PA	.818	1793.093
26			51707	22	724	41488	PA	.890	1799.233
27			51707	22	387	21188	F PA	.113	1535.615
28			51709	22	1938	129524	PA	.482	1799.367
29			51709	22	289	17212	PA	.608	23.685
30			51709	22	260	14896	F PA	.403	54.222
31			51708	22	452	30752	PA	.879	1769.589
32			51708	22	21	1188	F PA	.475	527.882

FloVis: Context



Future Work



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?