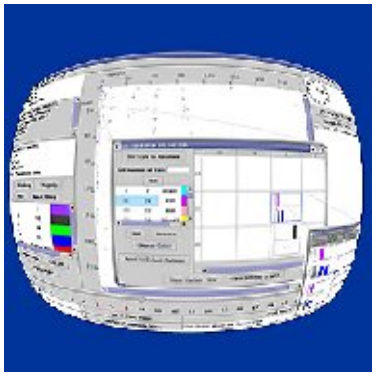
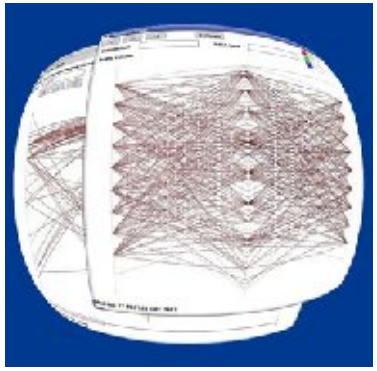
NVisionIP and VisFlowConnect-IP:
Two Tools for Visualizing NetFlows for Security





William Yurcik
<byurcik@ncsa.uiuc.edu>

National Center for Supercomputing Applications (NCSA)
University of Illinois at Urbana-Champaign

NANOG36
Dallas Texas, February 2006

Overview

- **Project Motivation**
- **NetFlows for Security**
- **Two Visualization Tools**
  - ***NVisionIP***
  - ***VisFlowConnect-IP***
- **Summary**

Project Motivation

Internet Security:
N-Dimensional Work Space

large

complex

time dynamics

Visualization can help!

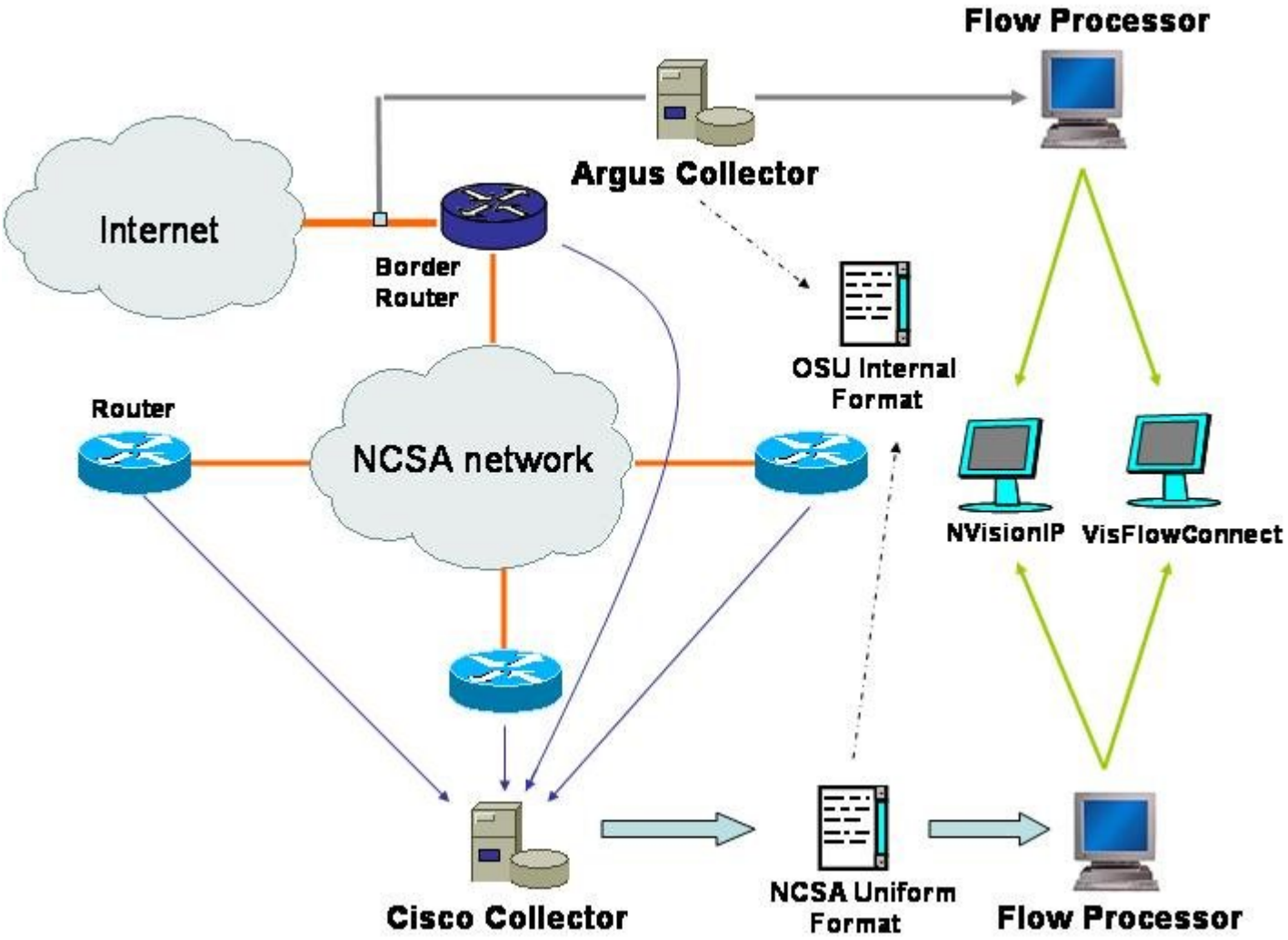
- **in near-realtime**
- **overview – browse – details on-demand**

NetFlows for Security

NetFlows for Security

- **NetFlows can identify connection-oriented attacks like DoS, DDoS, malware distribution, worm scanning, etc…**
- **How many users are on the network at any given time? (upgrades)**
- **Who are my top N talkers?**
- **How long do my users surf?**
- **Where do they go? Where did they come from?**
- **Are users following the security policy?**
- **What are the top N Destination ports?**
- **Is there traffic to vulnerable hosts?**
- **Can you identify and block scanners/bad guys?**

NCSA's NetFlows Architecture



Two NetFlows Visualization Tools

Tool 1: NVisionIP

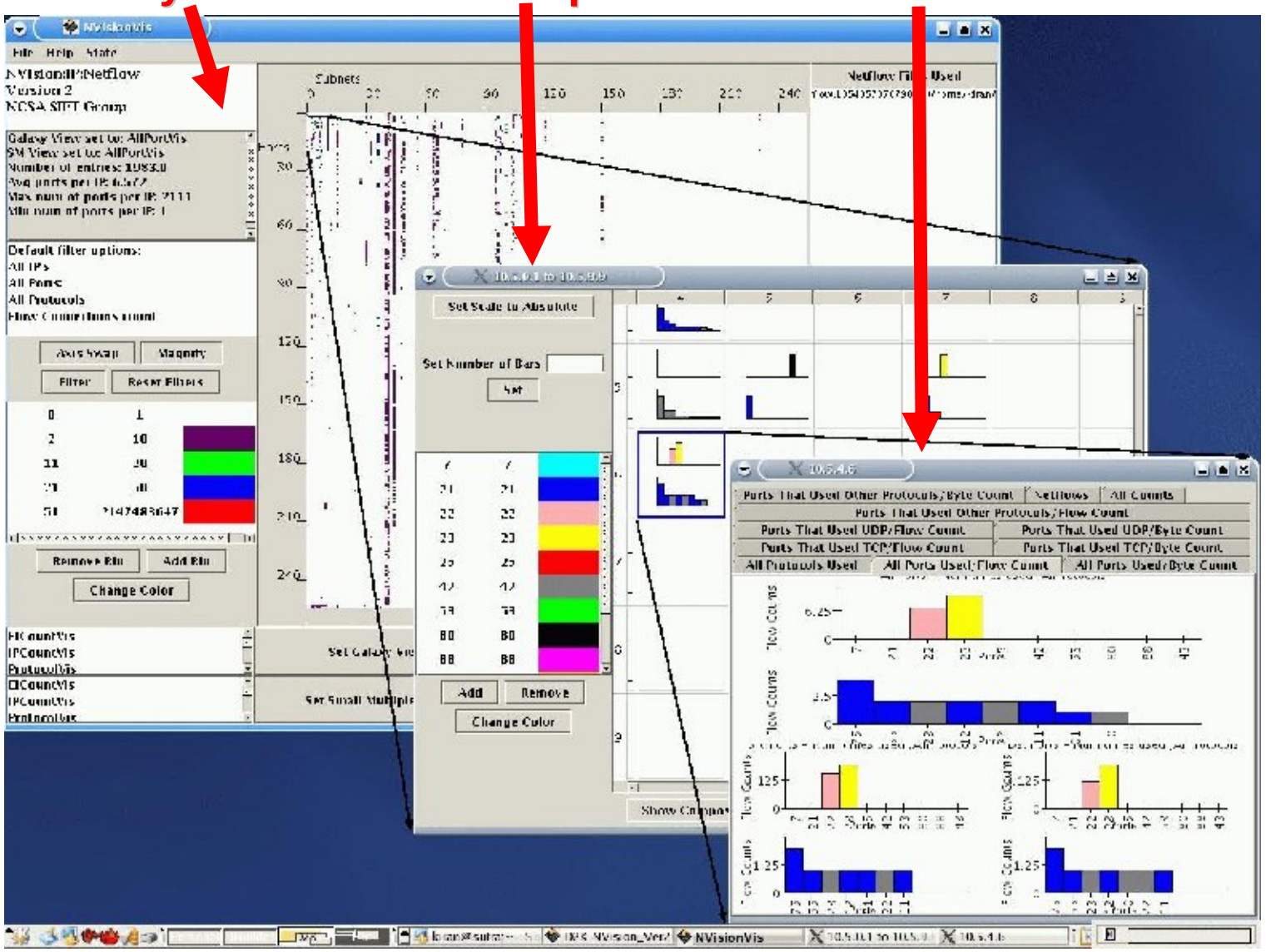
Tool 2: VisFlowConnect-IP

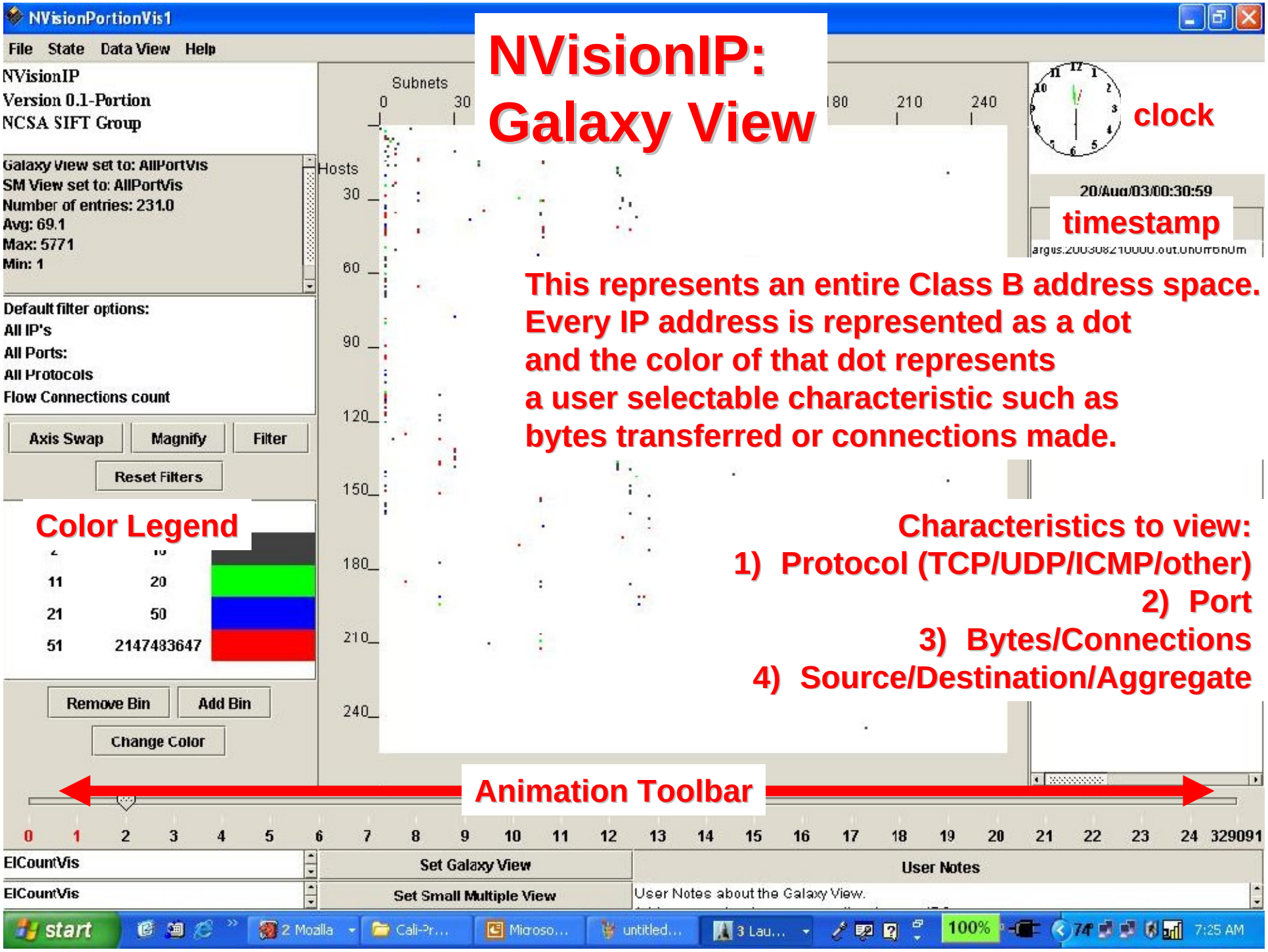
http://security.ncsa.uiuc.edu/distribution/NVisionIPDownLoad.html

NVisionIP: 3-Level Hierarchical Views Designed for

Overview – Browse – Details on Demand

Galaxy View / Small Multiple View / Machine View





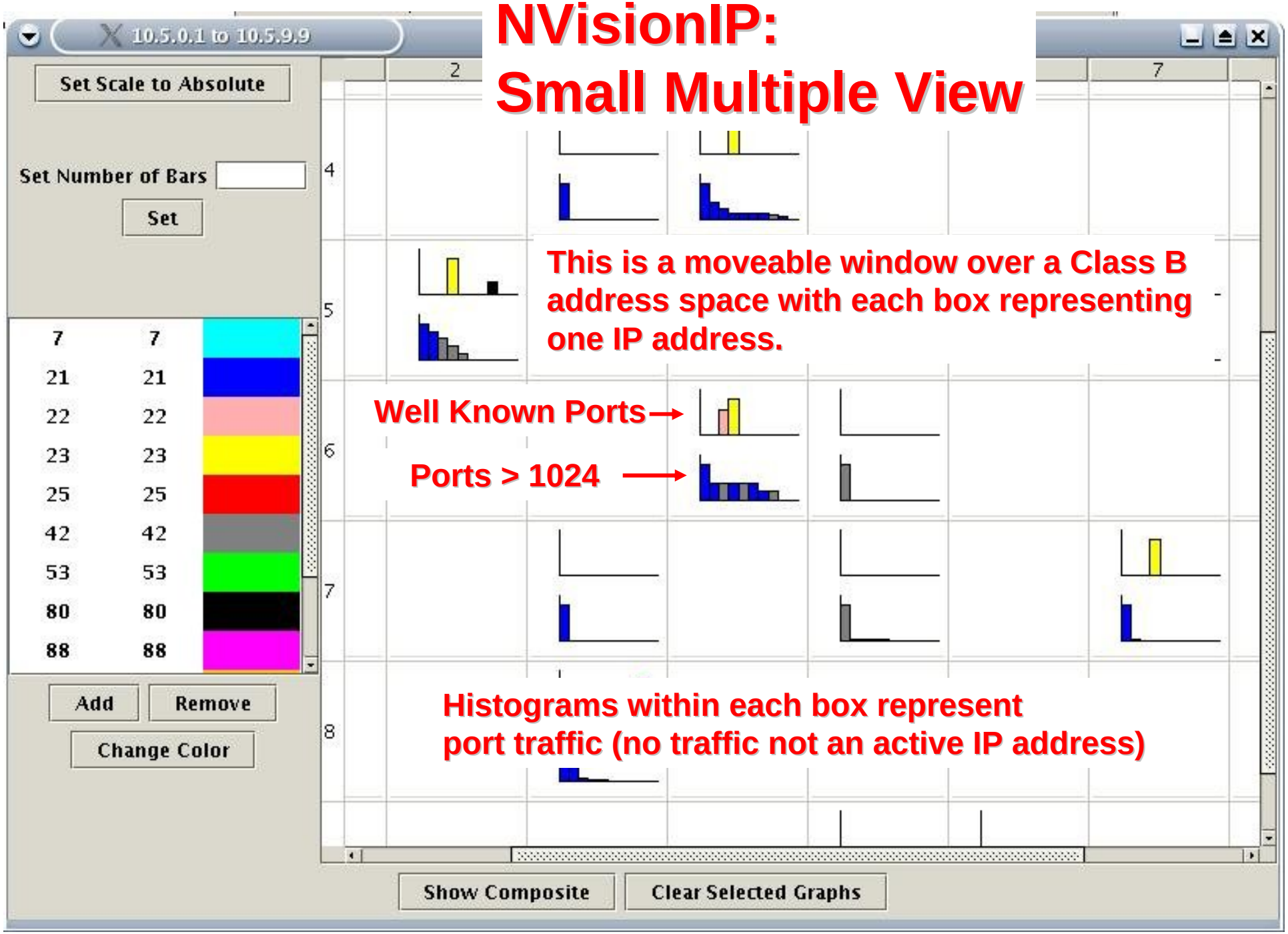
NVisionIP: Galaxy View

This represents an entire Class B address space. Every IP address is represented as a dot and the color of that dot represents a user selectable characteristic such as bytes transferred or connections made.

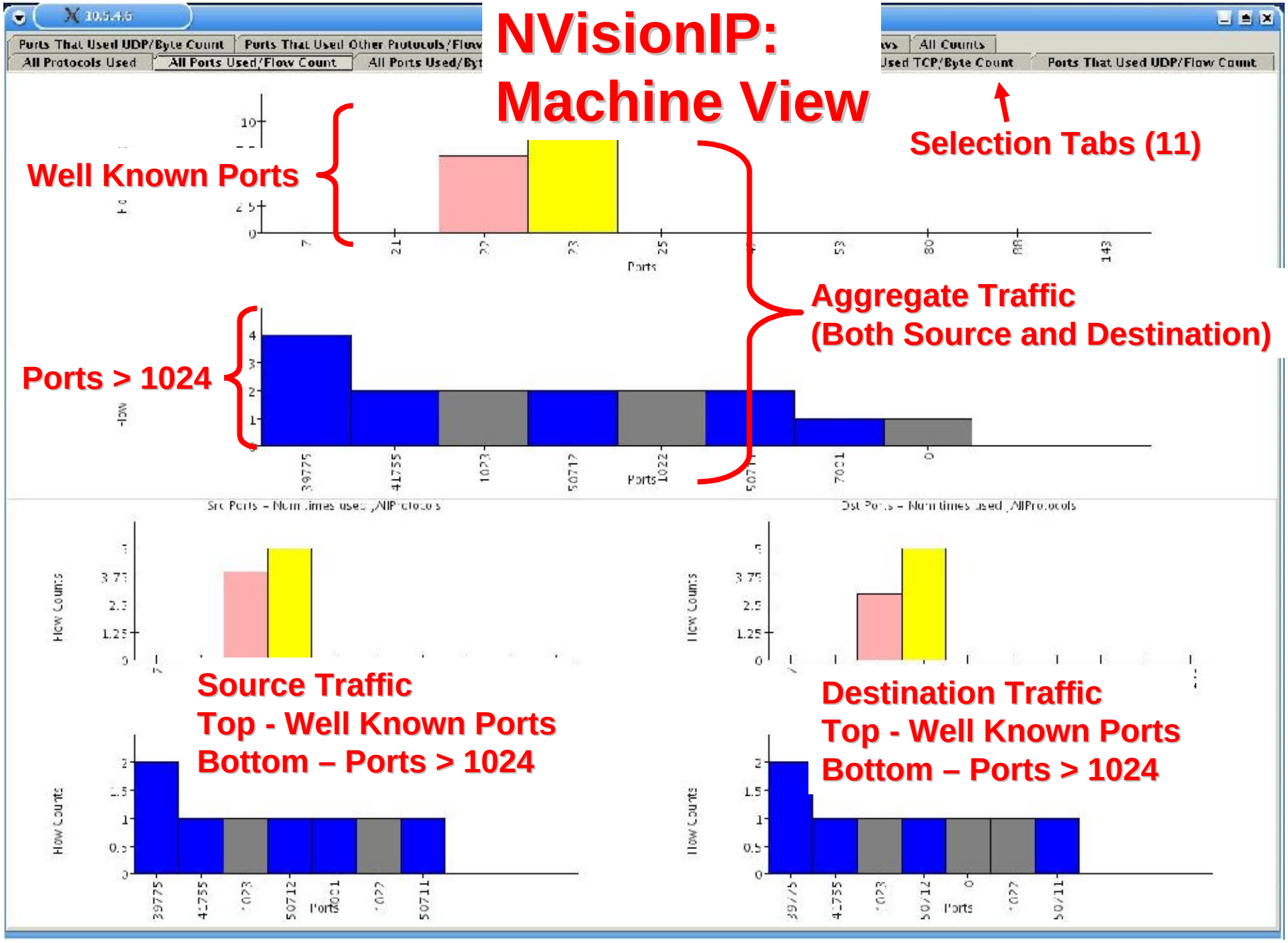
Characteristics to view:

1) Protocol (TCP/UDP/ICMP/other)
2) Port
3) Bytes/Connections
4) Source/Destination/Aggregate

NVisionIP: Small Multiple View



NVisionIP: Machine View



Selection Tabs (11)

Well Known Ports

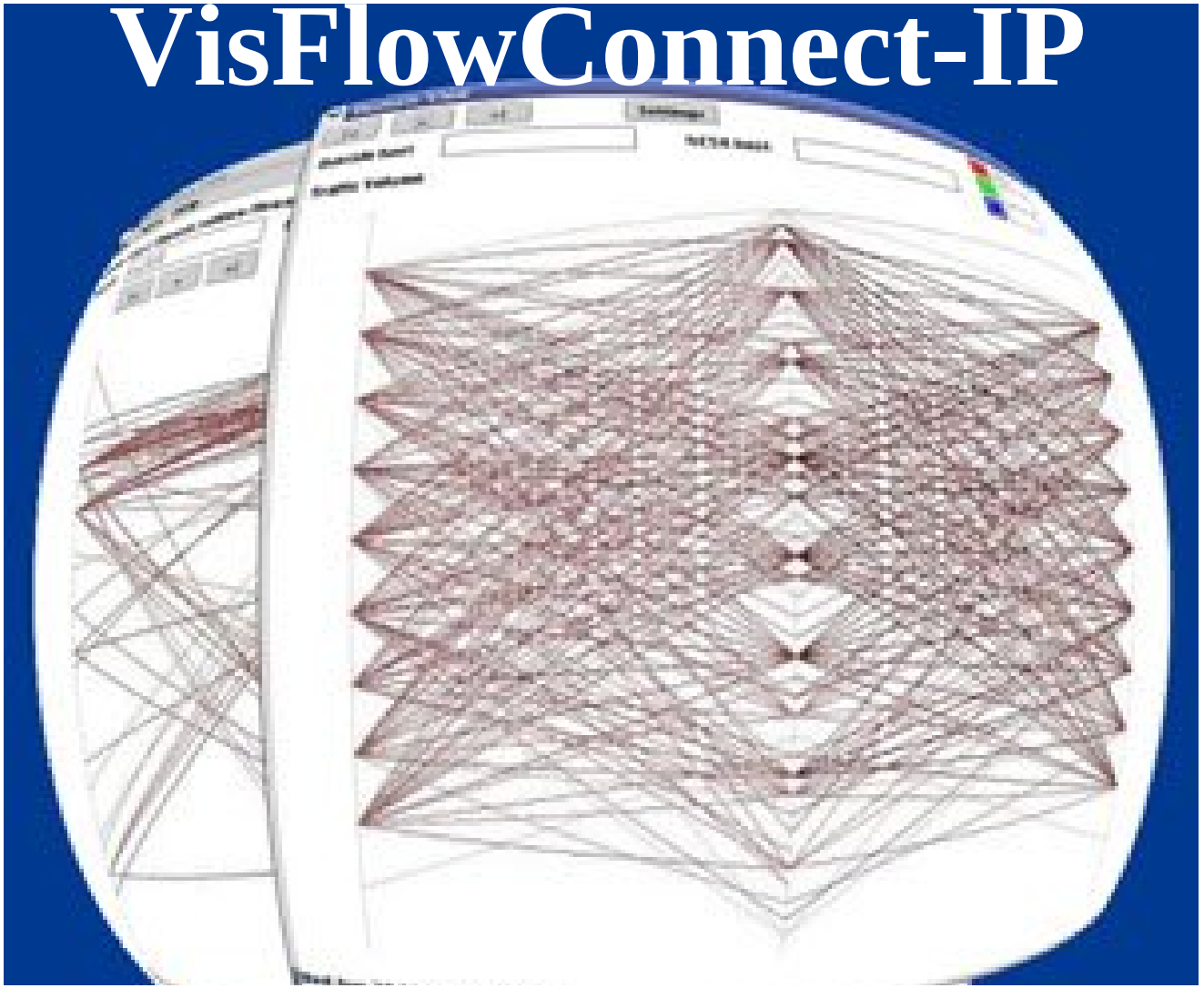
Ports > 1024

Aggregate Traffic
(Both Source and Destination)

Source Traffic
Top - Well Known Ports
Bottom – Ports > 1024

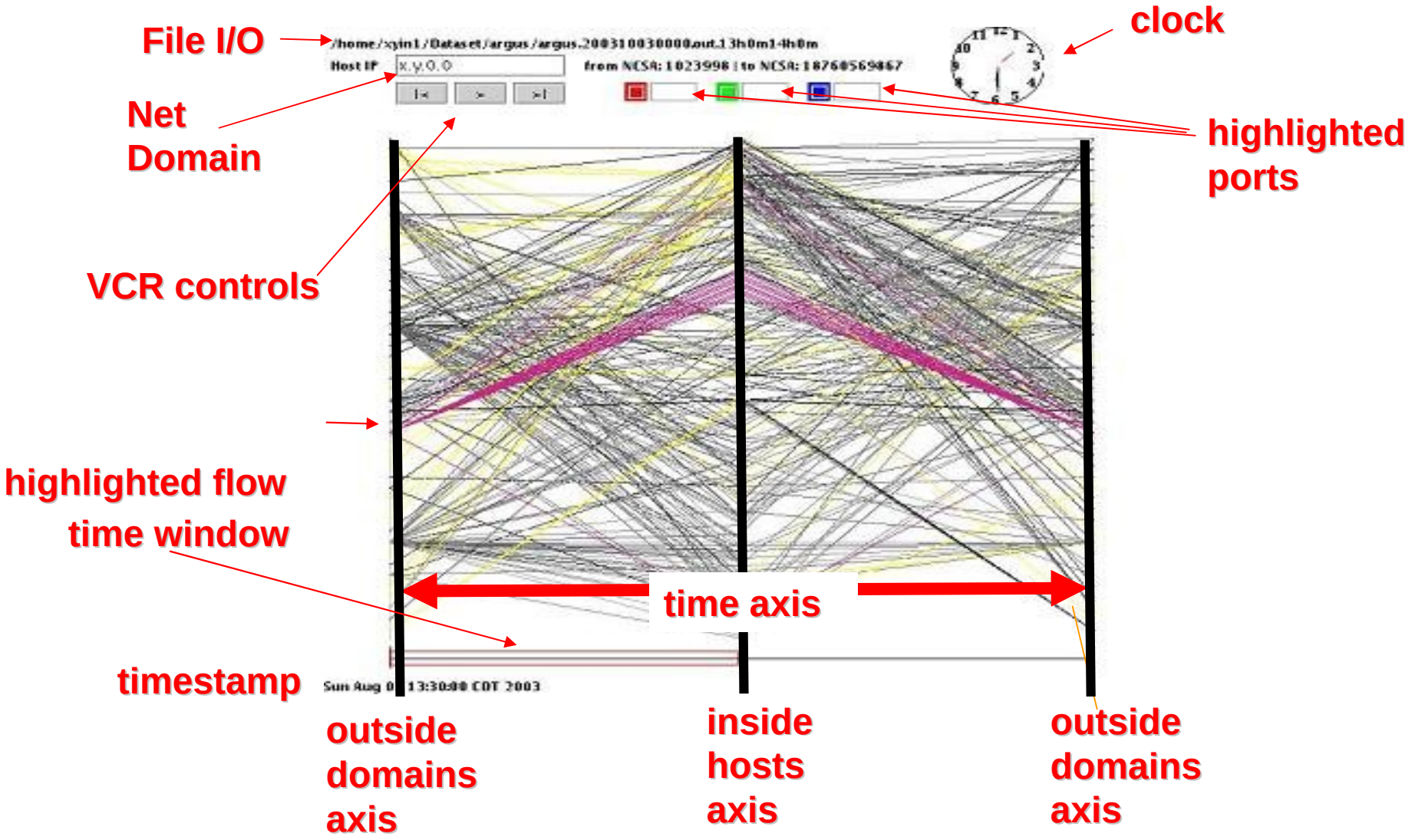
Destination Traffic
Top - Well Known Ports
Bottom – Ports > 1024

VisFlowConnect-IP

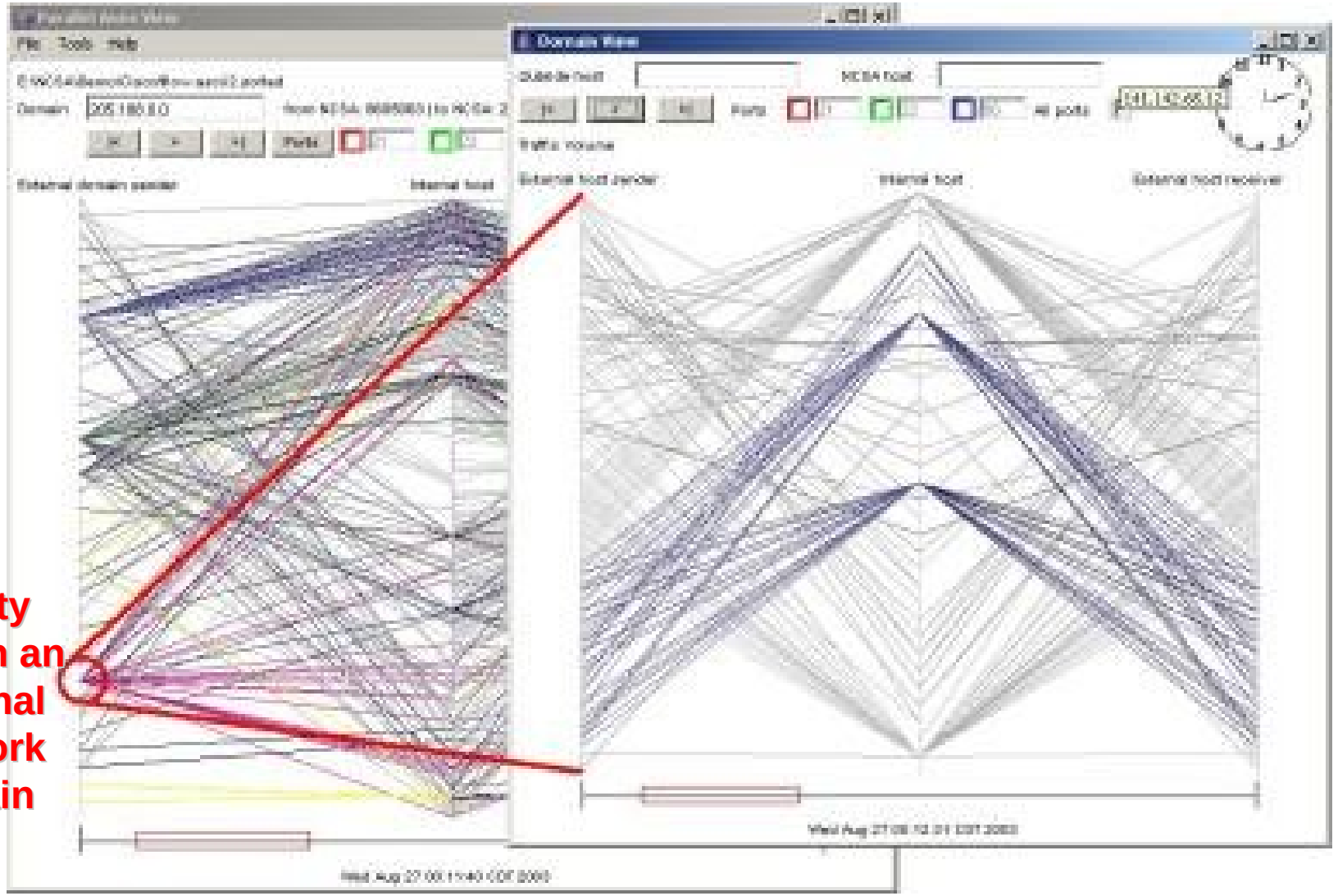


http://security.ncsa.uiuc.edu/distribution/VisFlowConnectDownLoad.html

VisFlowConnect-IP

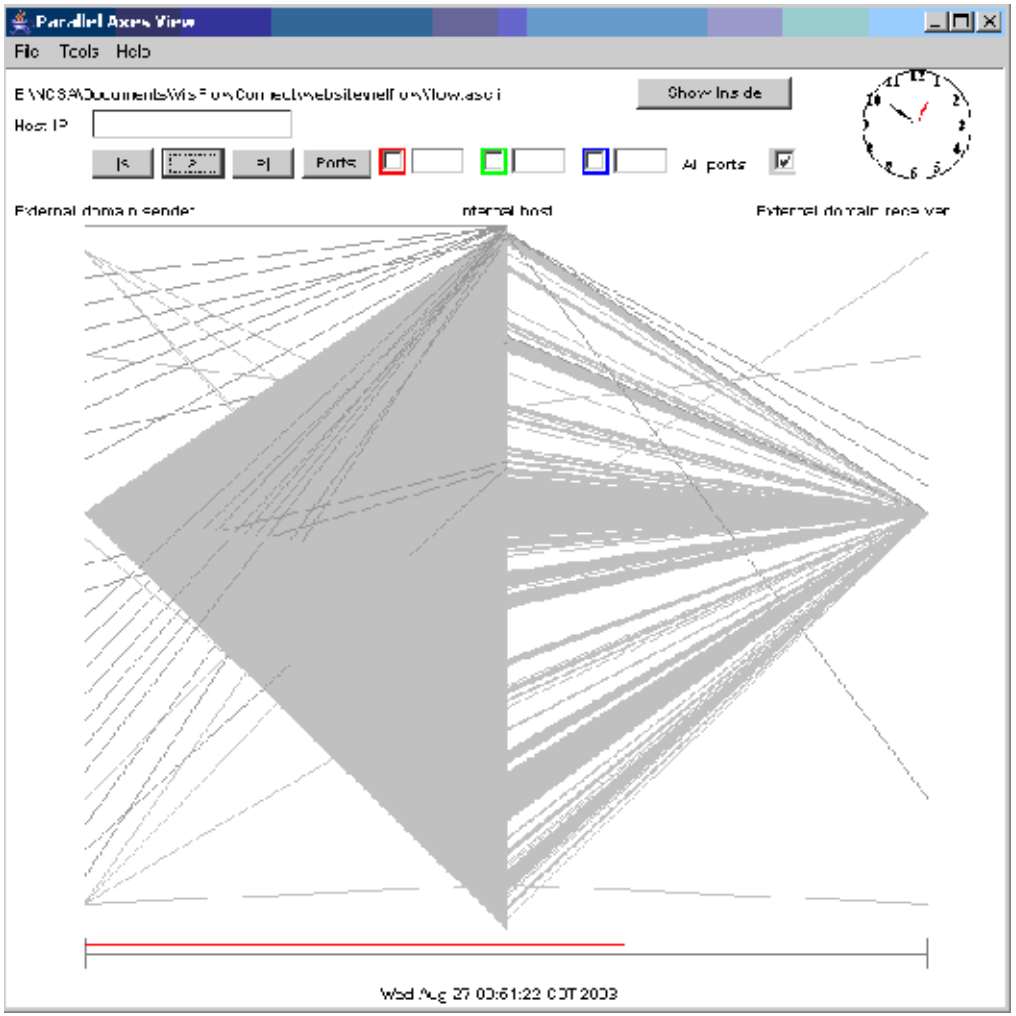


VisFlowConnect-IP
Domain View



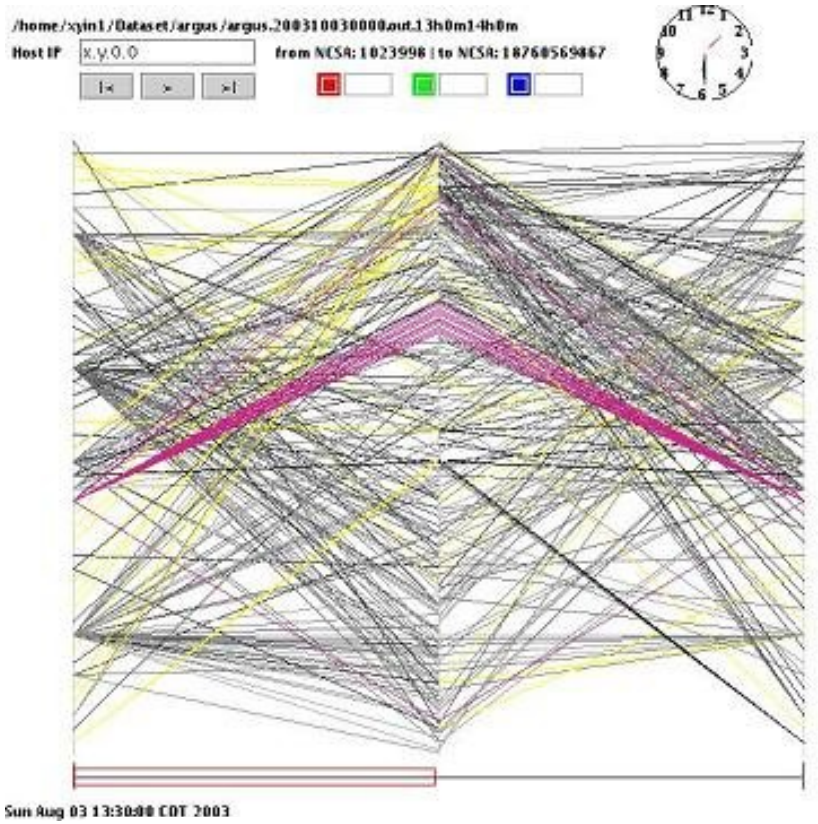
Example 1: MS Blaster

- MS Blaster virus causes machines to send out packets of size 92 to many machines



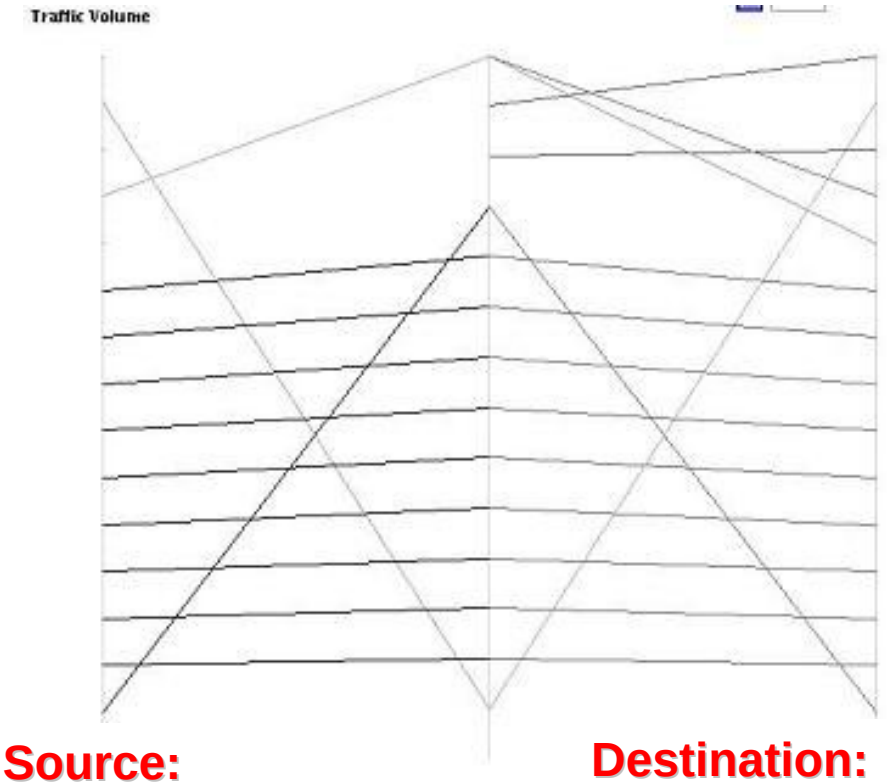
Example 2: Grid Networking

cluster-to-cluster communications



multiple connections to NCSA cluster from same domain

(scan?, DoS?)



Source:

consecutive IP addresses

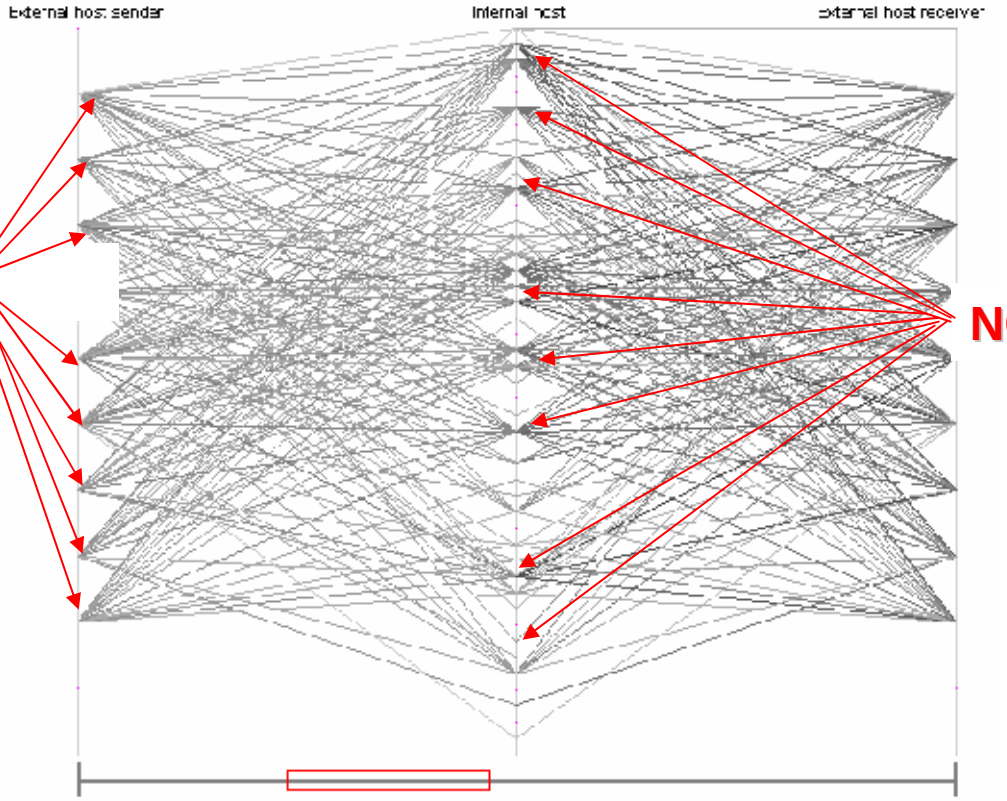
Destination:

consecutive IP addresses

Example 3: Web Crawlers

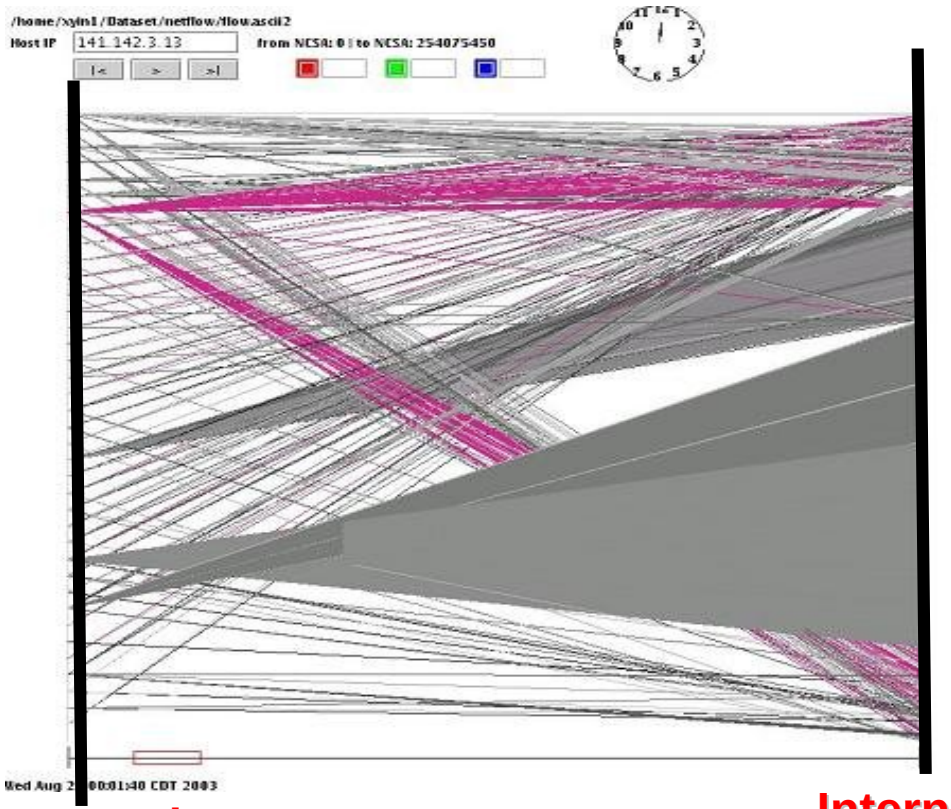
muitiple crawlers indexing NCSA web server content

Web crawlers



NCSA web servers

VisFlowConnect-IP Internal View



Internal network sources

Internal network receivers

Summary

- **NetFlows analysis is non-trivial, however, the potential payoff is large**

  Flow-Analysis Community Homepage

<http://www.ncassr.org/projects/sift/flow-analysis/>

- **Go with the Flow (NetFlows)**

  1.NVisionIP

  2.VisFlowConnect-IP

NVisionIP

<http://security.ncsa.uiuc.edu/distribution/NVisionIPDownLoad.html>

References

- William Yurcik, " **Visualizing NetFlows for Security at Line Speed: The SIFT Tool Suite** ," *19th Usenix Large Installation System Administration Conference (LISA)* , San Diego, CA USA, December 2005.
- Kiran Lakkaraju, Ratna Bearavolu, Adam Slagell, and William Yurcik " **Closing-the-Loop in NVisionIP: Integrating Discovery and Search in Security Visualizations** ," *2nd International Workshop on Visualization for Computer Security (VizSEC)* , held in conjunction with IEEE Vis 2005 and IEEE InfoVis 2005, October 2005.
- Ratna Bearavolu, Kiran Lakkaraju, and William Yurcik, " **NVisionIP: An Animated State Analysis Tool for Visualizing NetFlows** ," *FLOCON - Network Flow Analysis Workshop (Network Flow Analysis for Security Situational Awareness)* , Sept. 2005.
- Kiran Lakkaraju, Ratna Bearavolu, Adam Slagell, and William Yurcik, " **Closing-the-Loop: Discovery and Search in Security Visualizations** ," *6th IEEE Information Assurance Workshop (The West Point Workshop)* , United States Military Academy at West Point, New York USA, June 2005.
- Kiran Lakkaraju, William Yurcik, Adam J. Lee, Ratna Bearavolu, Yifan Li, and Xiaoxin Yin, " **NVisionIP: NetFlow Visualizations of System State for Security Situational Awareness** ," *CCS Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC)* held in conjunction with the *11th ACM Conference on Computer and Communications Security*, 2004.
- Kiran Lakkaraju, William Yurcik, Ratna Bearvolu, and Adam J. Lee, "**NVisionIP: An Interactive Network Flow Visualization Tool for Security**," *IEEE International Conference on Systems, Man and Cybernetics (SMC)* , 2004.
- Cristina Abad, Yifan Li, Kiran Lakkaraju, Xiaoxin Yin, and William Yurcik, " **Correlation Between NetFlow System and Network Views for Intrusion Detection** ," *Workshop on Link Analysis, Counter-terrorism, and Privacy* held in conjunction with the *SIAM International Conference on Data Mining (ICDM)* , 2004.
- William Yurcik, Kiran Lakkaraju, James Barlow, and Jeff Rosendale, " **A Prototype Tool for Visual Data Mining of Network Traffic for Intrusion Detection** ," *3rd IEEE International Conference on Data Mining (ICDM) Workshop on Data Mining for Computer Security (DMSEC)* , 2003.
- Ratna Bearavolu, Kiran Lakkaraju, William Yurcik, and Hrishikesh Raje, " **A Visualization Tool for Situational Awareness of Tactical and Strategic Security Events on Large and Complex Computer Networks** ," *IEEE Military Communications Conference (Milcom)* , 2003.
- Kiran Lakkaraju, Ratna Bearavolu, and William Yurcik, " **NVisionIP - A Traffic Visualization Tool for Security Analysis of Large and Complex Networks** ," *International Multiconference on Measurement, Modelling, and Evaluation of Computer-Communications Systems (Performance TOOLS)* , 2003.
- William Yurcik, James Barlow, and Jeff Rosendale, " **Maintaining Perspective on Who Is The Enemy in the Security Systems Administration of Computer Networks**," *ACM CHI Workshop on System Administrators Are Users, Too: Designing Workspaces for Managing Internet-Scale Systems* , 2003.
- William Yurcik, James Barlow, Kiran Lakkaraju, and Mike Haberman, "**Two Visual Computer Network Security Monitoring Tools Incorporating Operator Interface Requirements**," *ACM CHI Workshop on Human-Computer Interaction and Security Systems (HCISEC)*, 2003.

VisFlowConnect-IP

<http://security.ncsa.uiuc.edu/distribution/VisFlowConnectDownLoad.html>

References

- William Yurcik, " **Visualizing NetFlows for Security at Line Speed: The SIFT Tool Suite** ," *19th Usenix Large Installation System Administration Conference (LISA)* , San Diego, CA USA, December 2005.

- Xiaoxin Yin, William Yurcik, and Adam Slagell, " **VisFlowConnect-IP: An Animated Link Analysis Tool for Visualizing Netflows** ," *FLOCON - Network Flow Analysis Workshop (Network Flow Analysis for Security Situational Awareness)* , Sept. 2005.

- Xiaoxin Yin, William Yurcik, and Adam Slagell, " **The Design of VisFlowConnect-IP: a Link Analysis System for IP Security Situational Awareness** ," *Third IEEE International Workshop on Information Assurance (IWIA)* University of Maryland, 2005.

- Xiaoxin Yin, William Yurcik, Michael Treaster, Yifan Li, and Kiran Lakkaraju " **VisFlowConnect: NetFlow Visualizations of Link Relationships for Security Situational Awareness** ," *CCS Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC)* held in conjunction with the *11th ACM Conference on Computer and Communications Security*, 2004.

- Xiaoxin Yin, William Yurcik, Yifan Li, Kiran Lakkaraju, Cristina Abad, " **VisFlowConnect: Providing Security Situational Awareness by Visualizing Network Traffic Flows** ", *23rd IEEE International Performance Computing and Communications Conference(IPCCC)* , 2004.

- Cristina Abad, Yifan Li, Kiran Lakkaraju, Xiaoxin Yin, and William Yurcik, " **Correlation Between NetFlow System and Network Views for Intrusion Detection** ," *Workshop on Link Analysis, Counter-terrorism, and Privacy* held in conjunction with the *SIAM International Conference on Data Mining (ICDM)* , 2004.

Q & A

NVisionIP

<http://security.ncsa.uiuc.edu/distribution/NVisionIPDownLoad.html>

VisFlowConnect-IP

<http://security.ncsa.uiuc.edu/distribution/VisFlowConnectDownLoad.html>