NetBytes Viewer: An Entity-based Netflow Visualization Utility for Identifying Intrusive Behavior

Presented By: Teryl Taylor

Joint Work With: Dr. Stephen Brooks
and
Dr. John McHugh

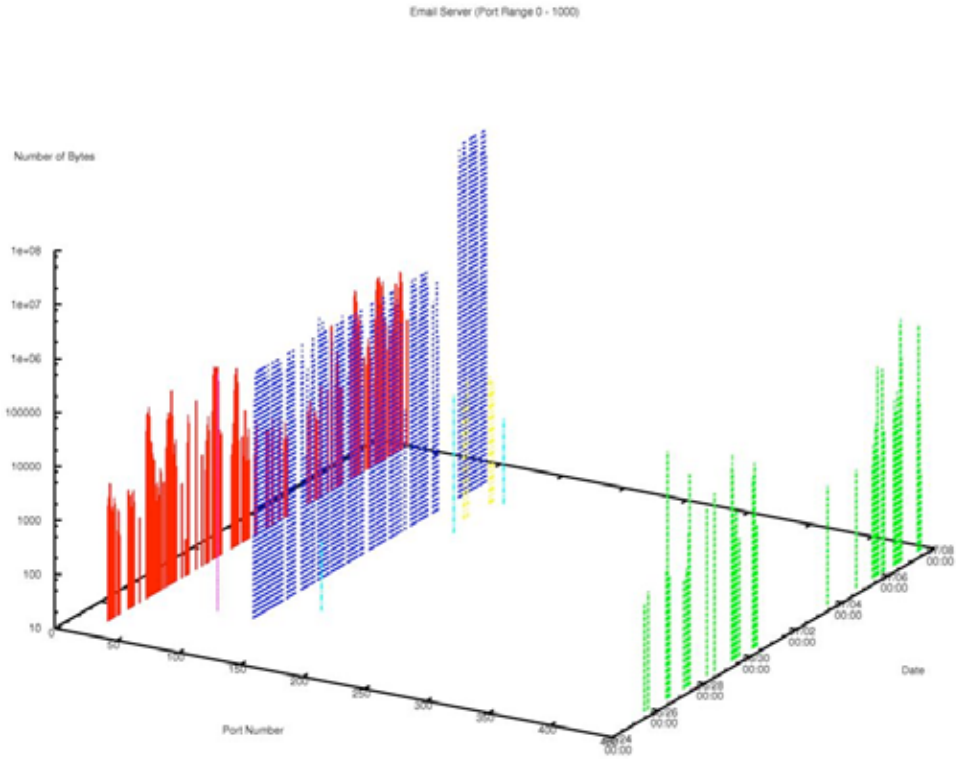
Dalhousie University, Halifax, Nova Scotia Canada

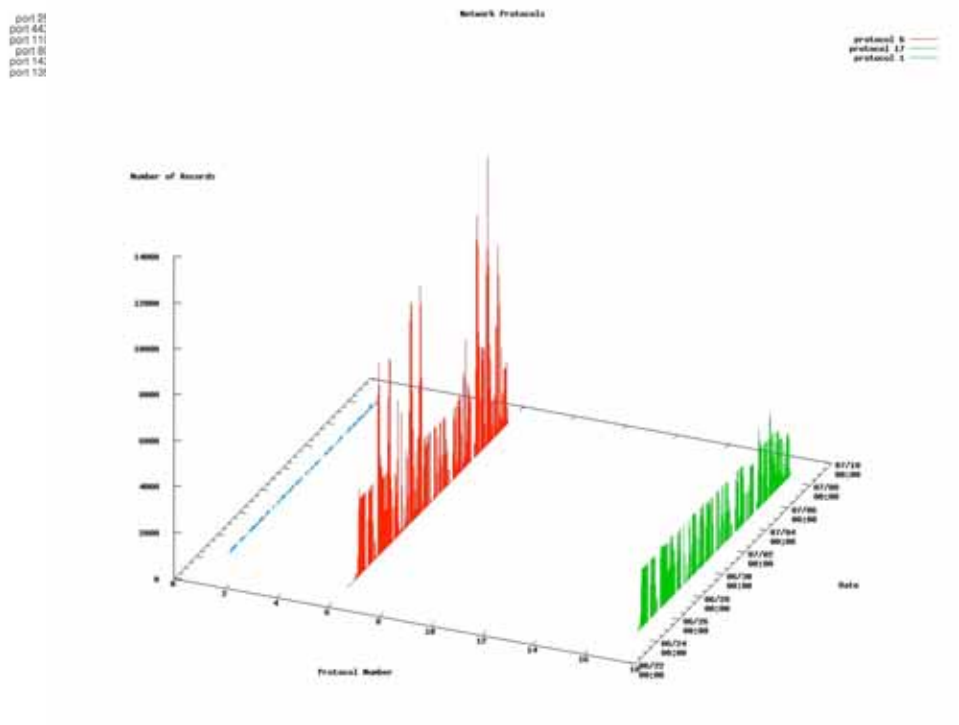
Agenda

- Introduction
- Related Work
- NetBytes Viewer Features
- Architecture
- Case Study
- Future Work

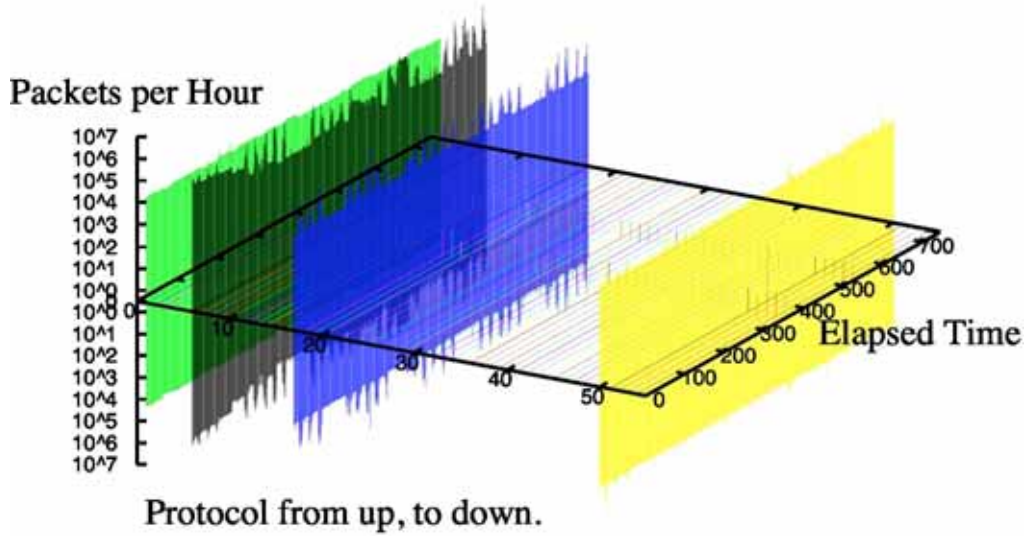
Introduction

- NetBytes Viewer: new interactive visualization tool
- Visualizes Netflow traffic using an entity-based approach
- Provides network administrators insight into what's going on in the network
  - Spotting intrusive behavior
  - See general network patterns



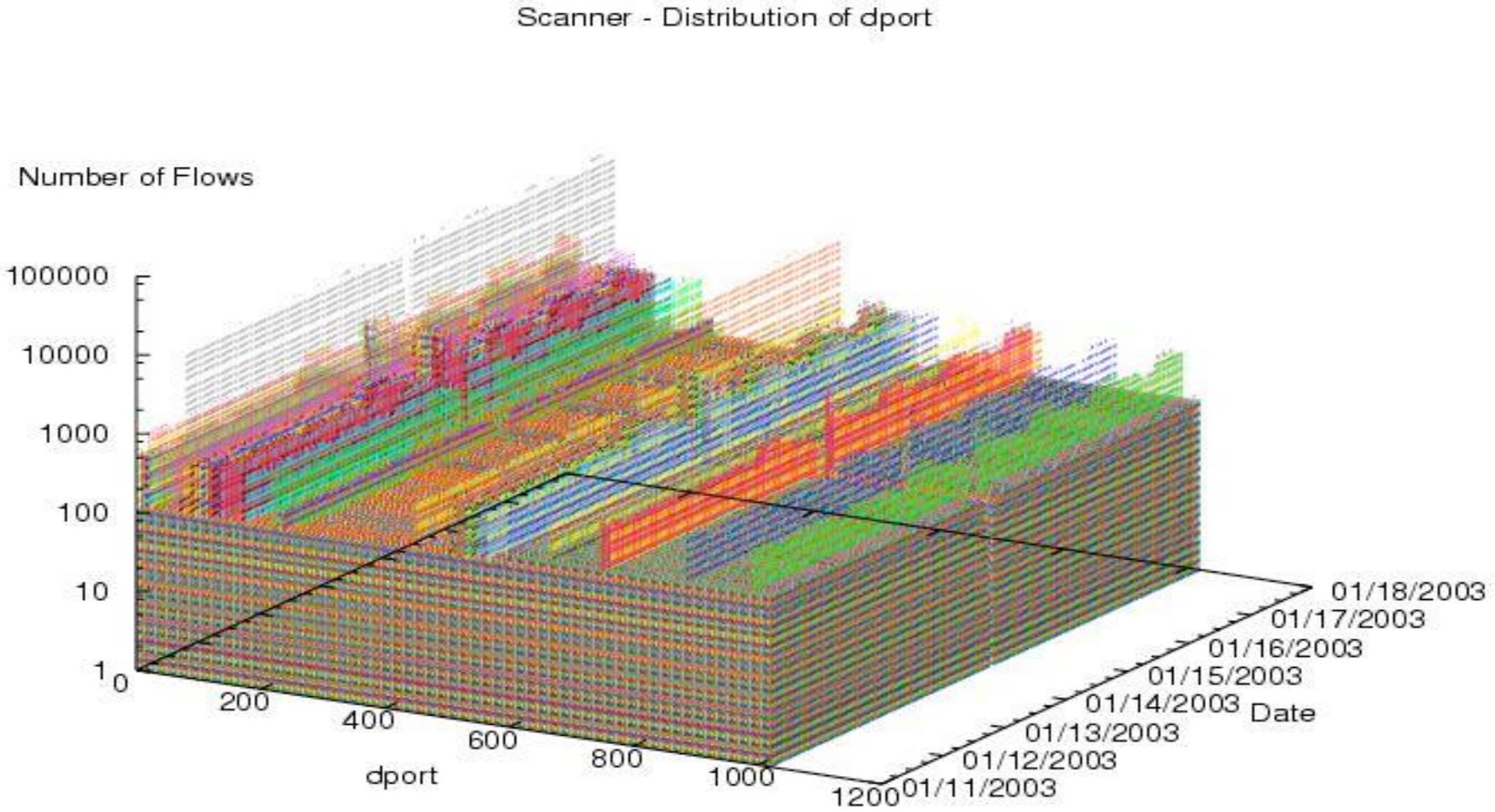


Subnet 10.0.64.0/22: 2006/03/01T00 to 2006/03/31T23
Per protocol traffic from/to subnet up/down



Protocol from up, to down.

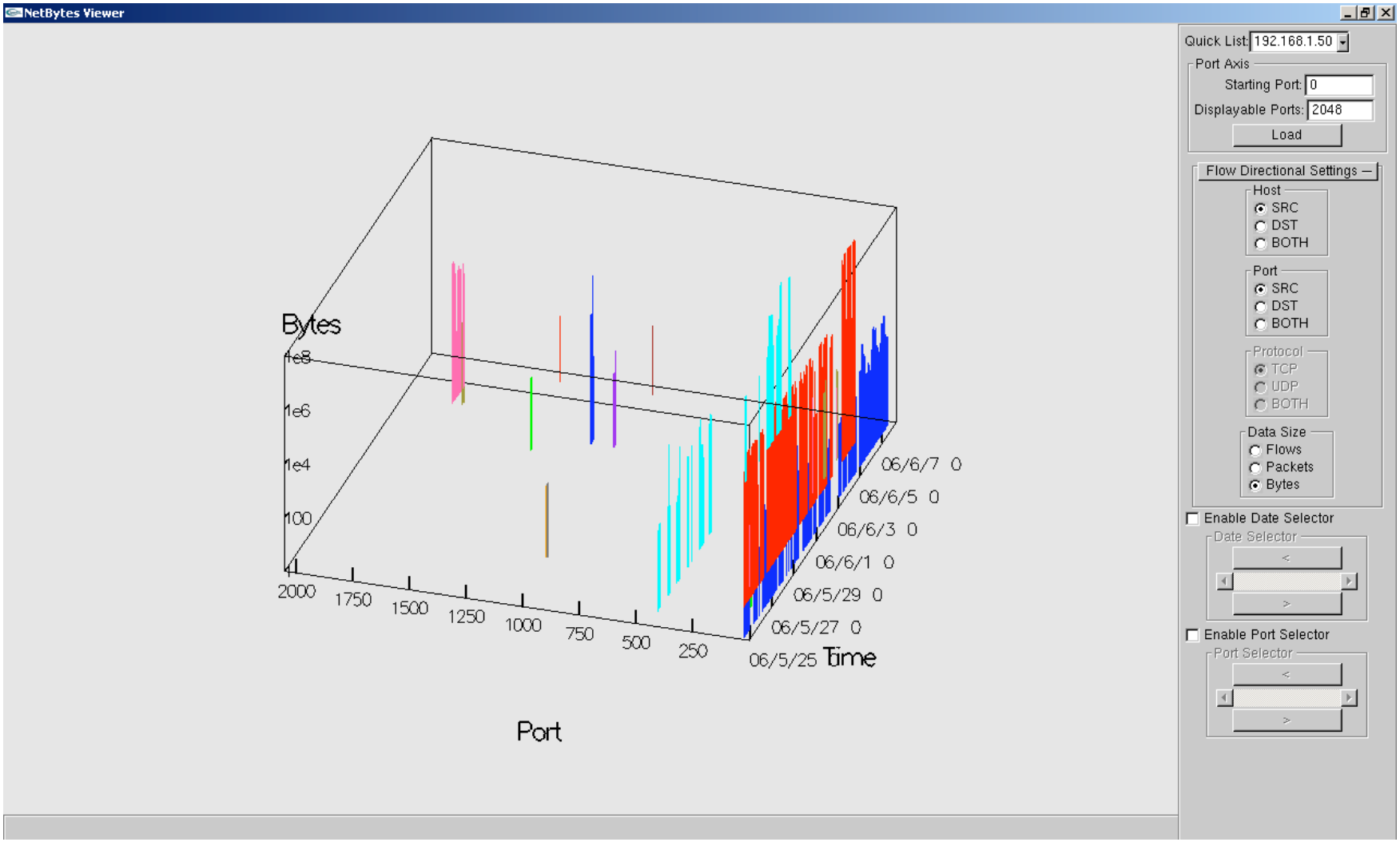
Horizontal/Vertical Scanner



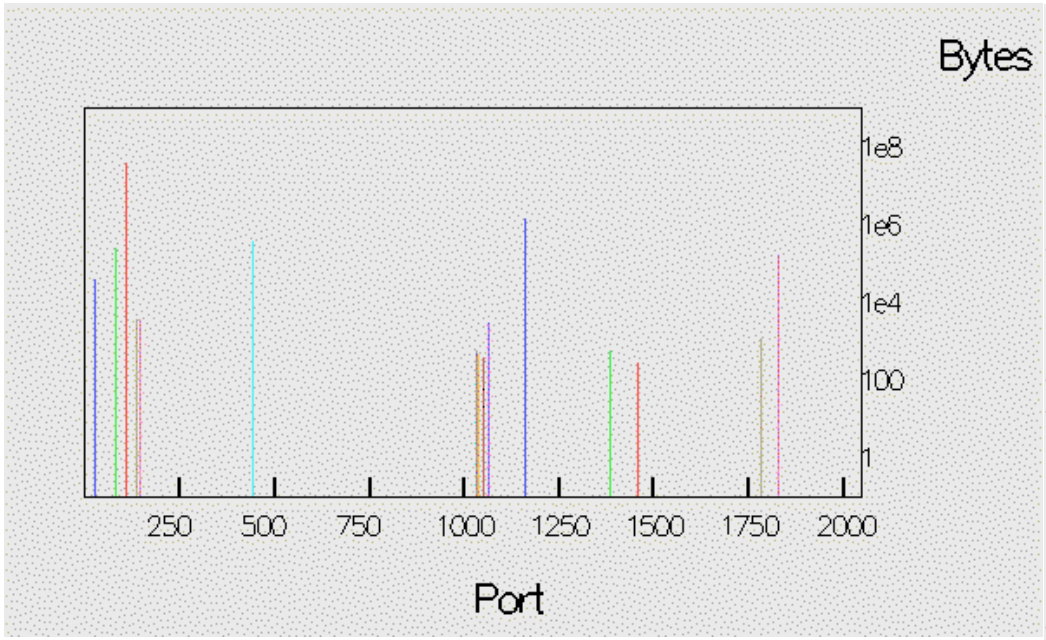
Related Work

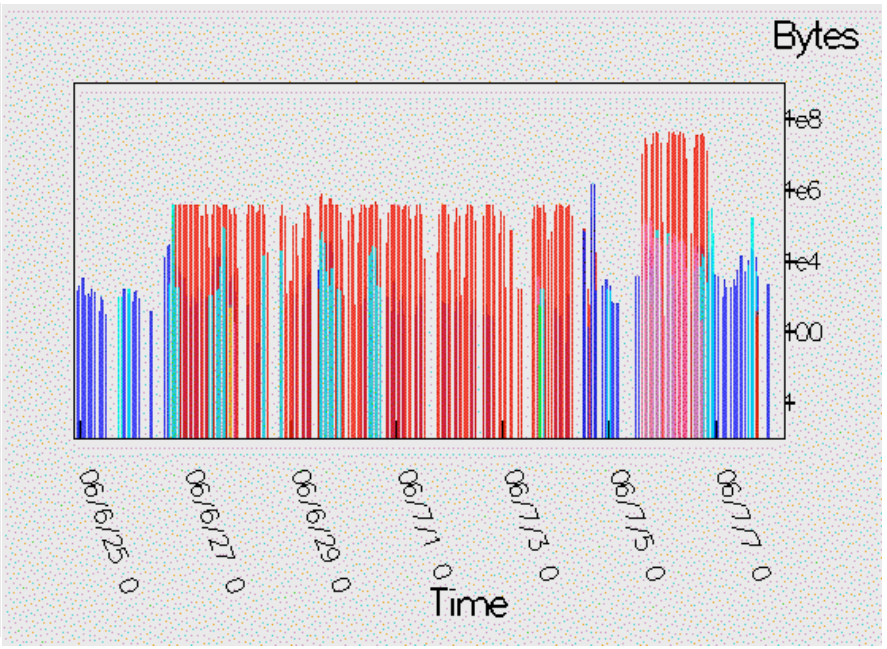
- VISUAL, VisFlowConnect, Flamingo: Focus mainly on network connections and direction of traffic
- Portall which correlates traffic flow with the processes that generate the traffic
- Portvis takes a 2D approach to visualizing port-based temporal traffic

NetBytes Viewer

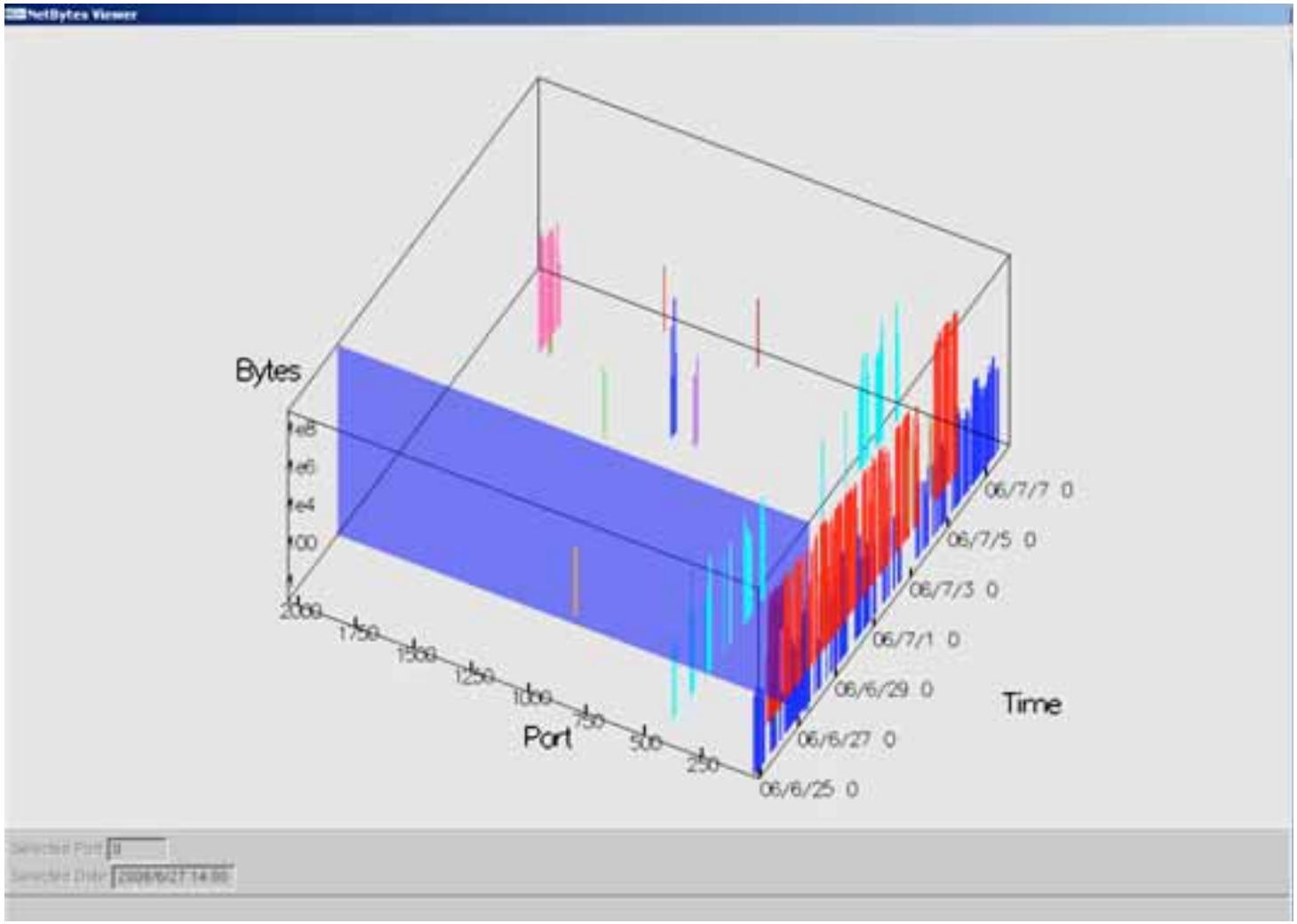


Orthogonal Views

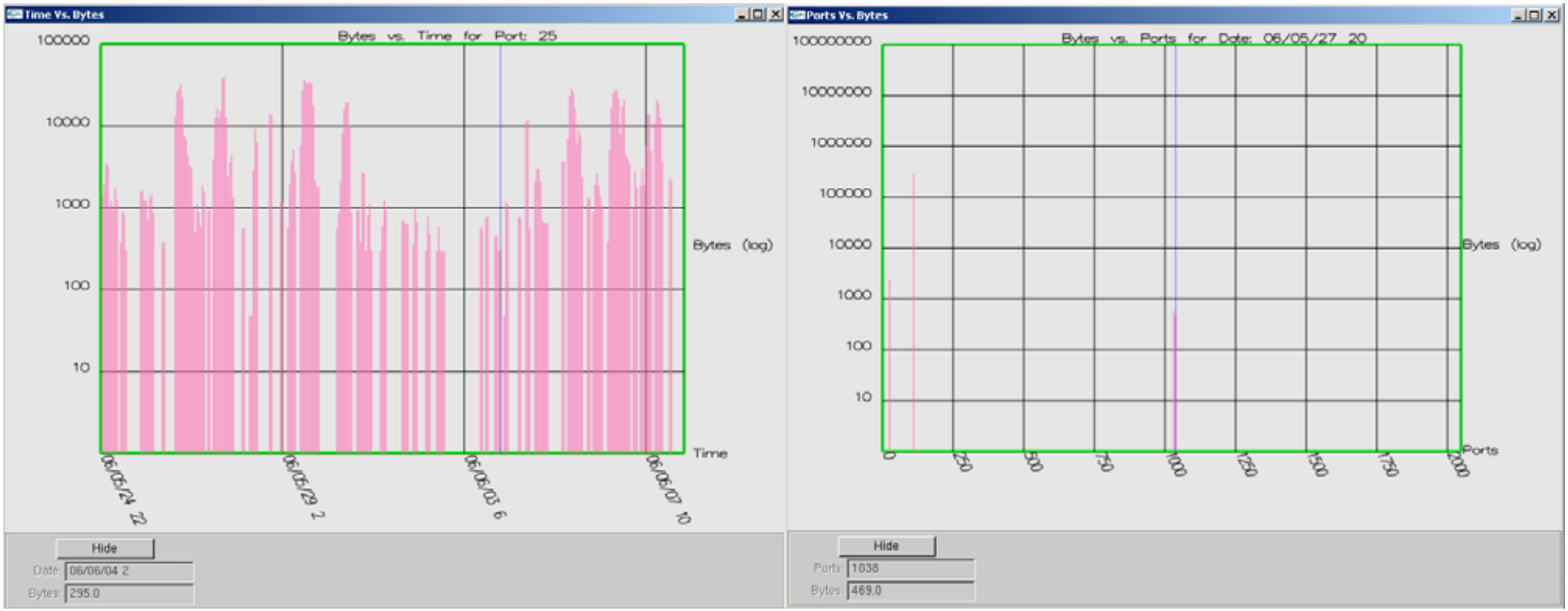




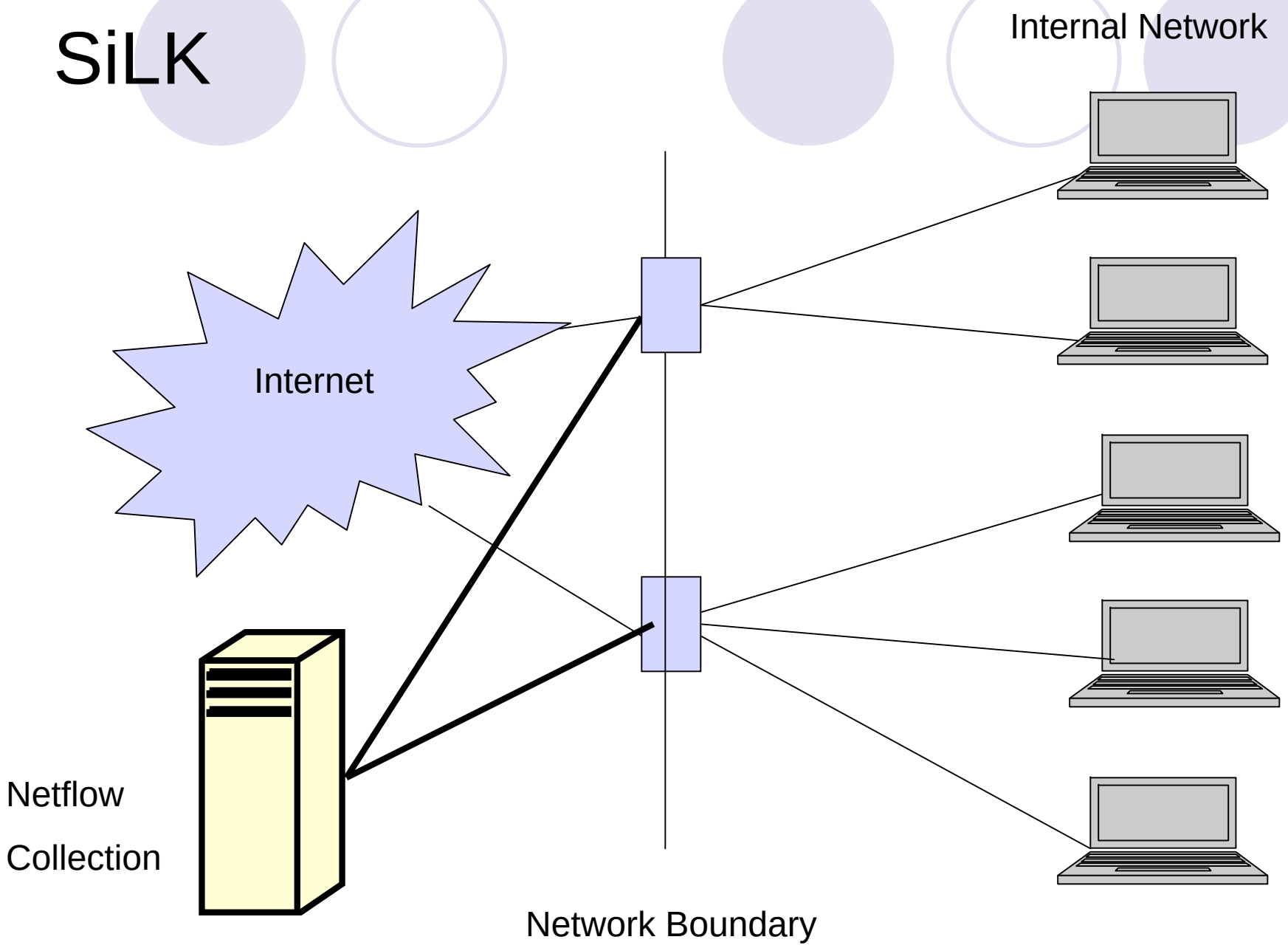
NetBytes Selectors

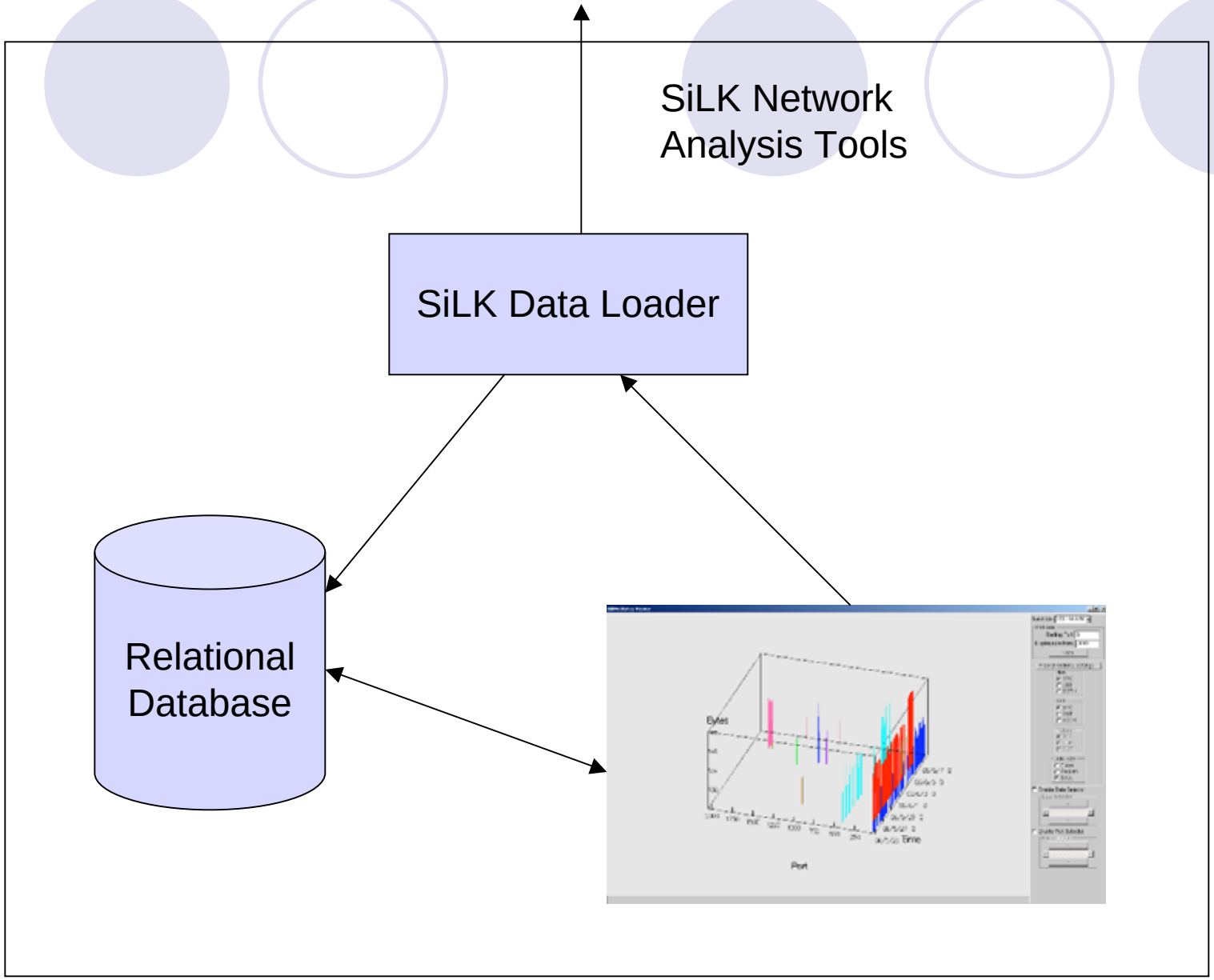


NetBytes Viewer Selection Mode

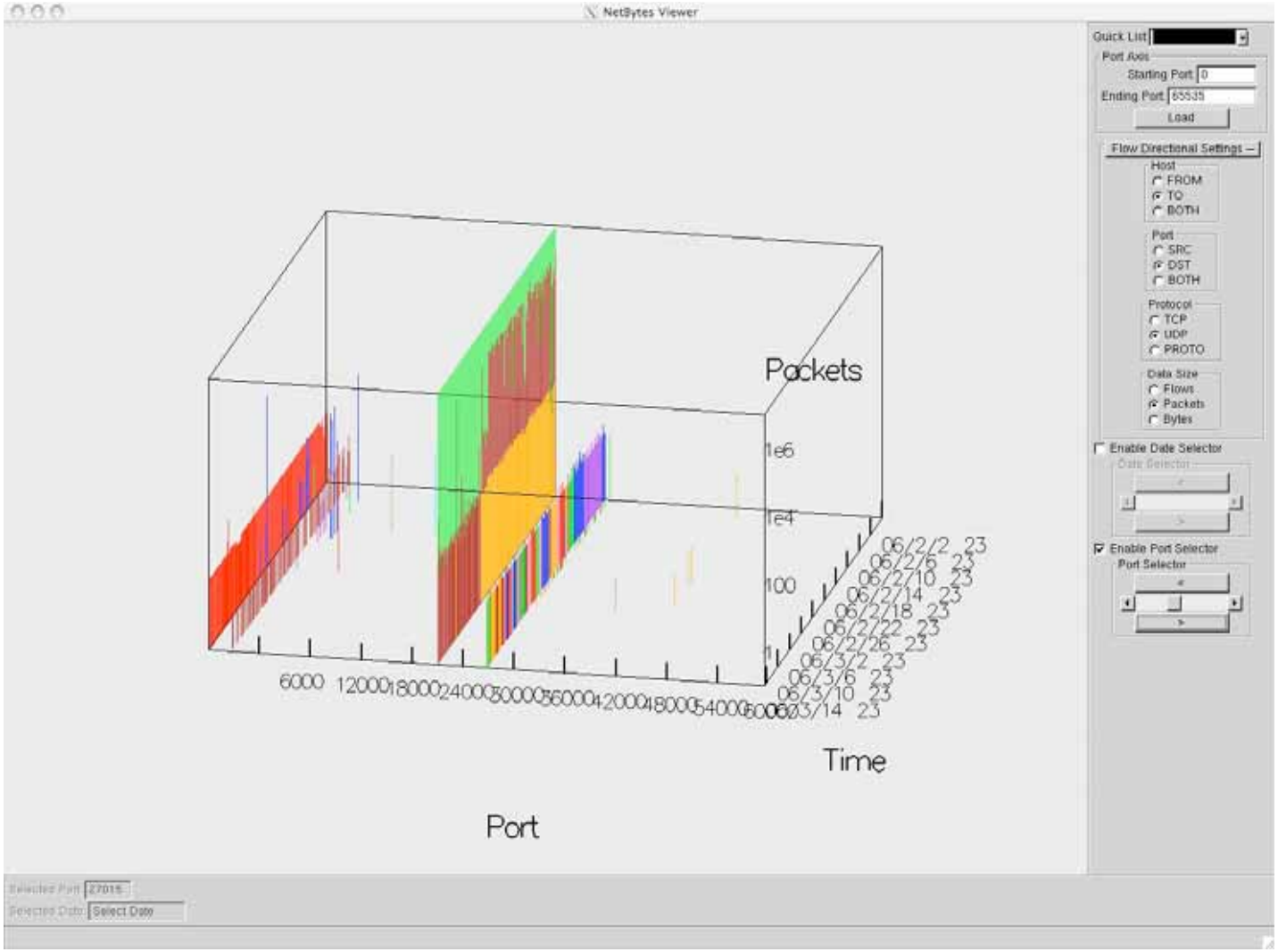


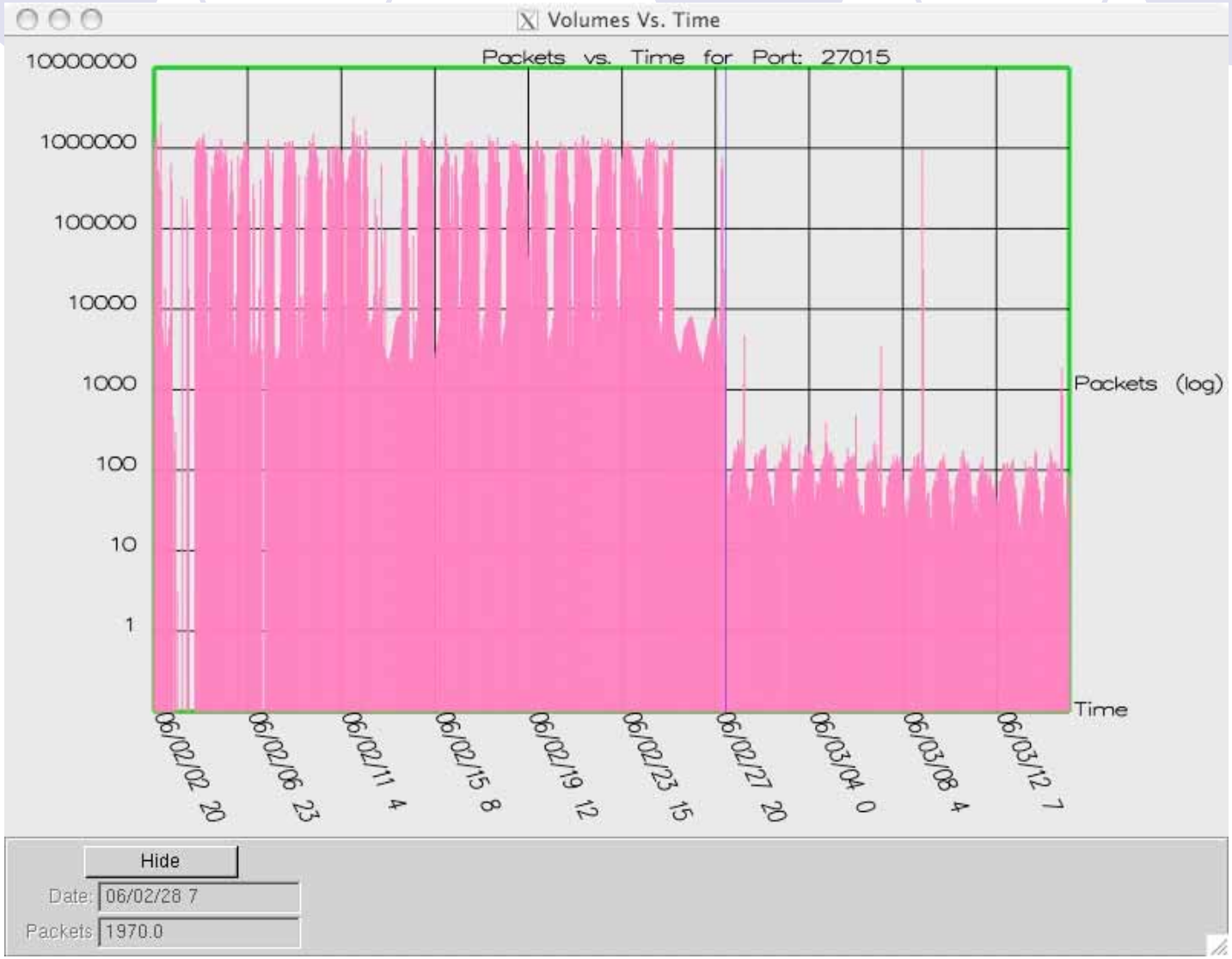
SiLK

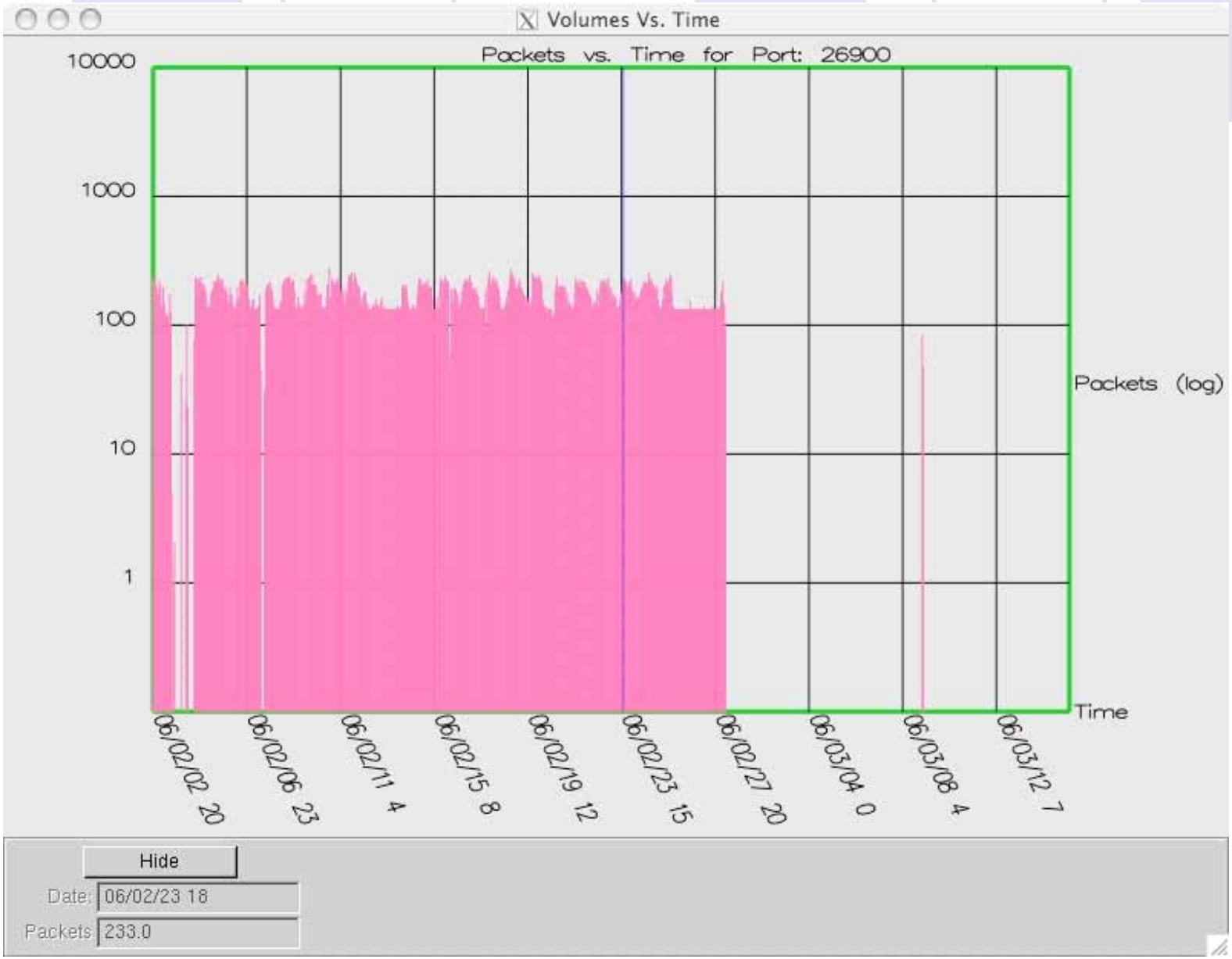

Internal Network
Internet
Netflow
Collection
Network Boundary


SiLK Network
Analysis Tools
SiLK Data Loader
Relational
Database

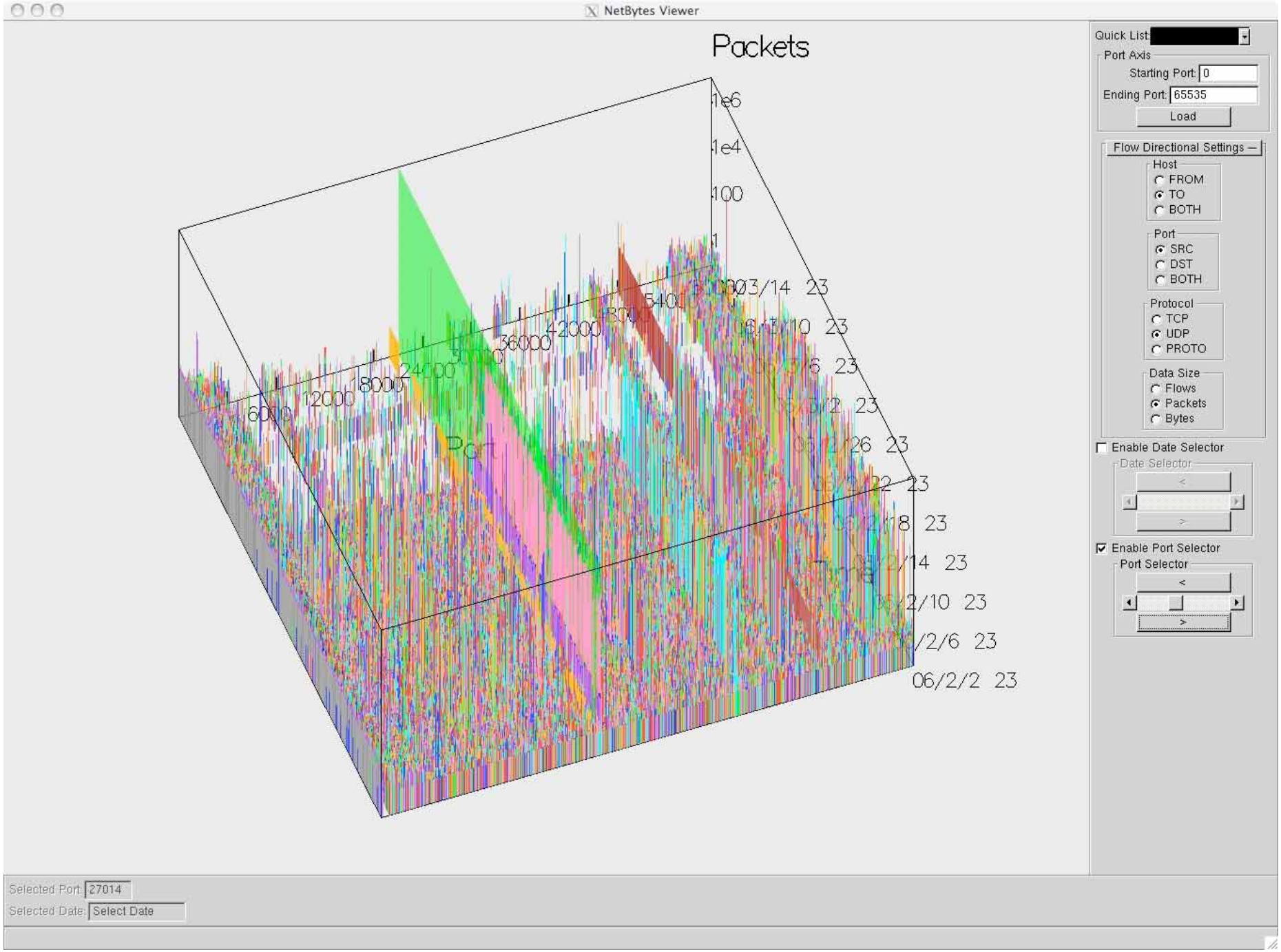
Case Study: Compromised Host




Volumes Vs. Time
Packets vs. Time for Port: 27015
10000000
1000000
100000
10000
1000
100
10
1
Packets (log)
Time
06/02/02 20
06/02/06 23
06/02/11 4
06/02/15 8
06/02/19 12
06/02/23 15
06/02/27 20
06/03/04 0
06/03/08 4
06/03/12 7
Hide
Date: 06/02/28 7
Packets 1970.0


Volumes Vs. Time
Packets vs. Time for Port: 26900
10000
1000
100
10
1
Packets (log)
Time
06/02/02 20
06/02/06 23
06/02/11 4
06/02/15 8
06/02/19 12
06/02/23 15
06/02/27 20
06/03/04 0
06/03/08 4
06/03/12 7
Hide
Date: 06/02/23 18
Packets 233.0


Volumes Vs. Time
Packets vs. Time for Port: 123
10000
1000
100
10
1
Packets (log)
Time
06/02/02 20
06/02/06 23
06/02/11 4
06/02/15 8
06/02/19 12
06/02/23 15
06/02/27 20
06/03/04 0
06/03/08 4
06/03/12 7
Hide
Date: 06/02/23 14
Packets 9.0


NetBytes Viewer
Packets
1e6
1e4
100
1
Port
6000
12000
18000
24000
30000
36000
42000
06/2/2 23
06/2/6 23
06/2/10 23
06/2/14 23
06/2/18 23
06/2/22 23
06/2/26 23
06/3/2 23
06/3/6 23
06/3/10 23
06/3/14 23
Quick List:
Port Axis
Starting Port: 0
Ending Port: 65535
Load
Flow Directional Settings
Host
FROM
TO
BOTH
Port
SRC
DST
BOTH
Protocol
TCP
UDP
PROTO
Data Size
Flows
Packets
Bytes
Enable Date Selector
Date Selector
Enable Port Selector
Port Selector
Selected Port: 27014
Selected Date: Select Date


Volumes Vs. Time
Packets vs. Time for Port: 54020
10000
1000
100
10
1
Packets (log)
Time
06/02/02 20
06/02/06 23
06/02/11 4
06/02/15 8
06/02/19 12
06/02/23 15
06/02/27 20
06/03/04 0
06/03/08 4
06/03/12 7
Hide
Date: 06/02/20 13
Packets 36.0

Future Work

- Drill down component of larger overall network visualization tool
- Selectable Date/Port Ranges
- Nonlinear distortion
- Displaying remote hosts (Volume vs. Host vs. Time)
- Bi-directional graphs
- Generate PDF and JPG
- More Integration with SiLK

Conclusions

- NetBytes Viewer provides a technique for visualizing network traffic using an entity-based framework
- Provides network administrators with insight into what is happening on their networks
- Initial stage of a more comprehensive network visualization project