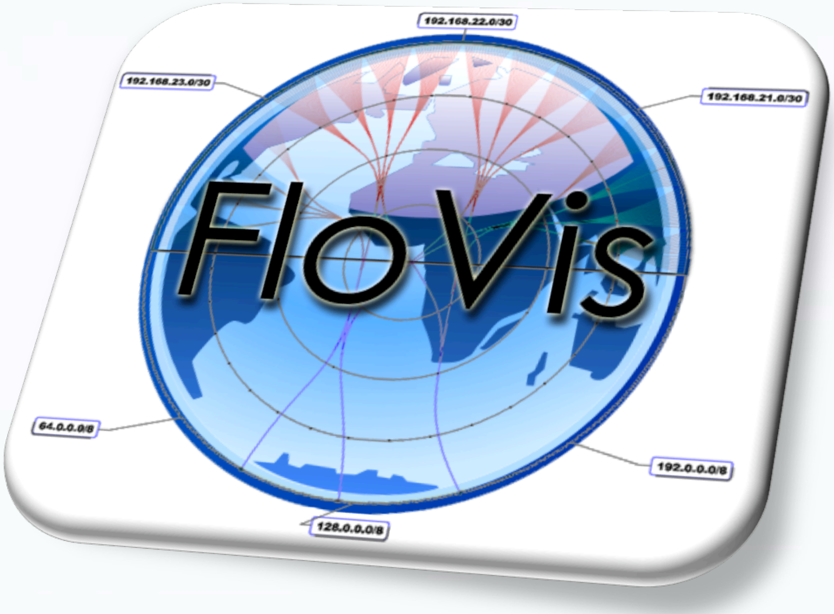
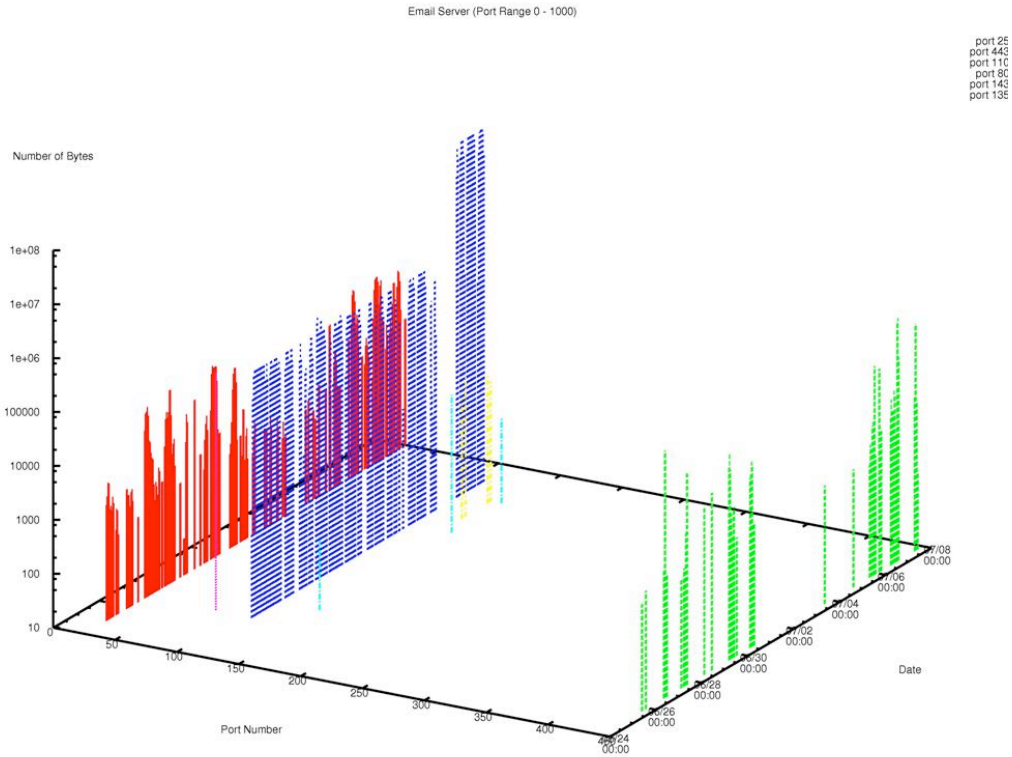


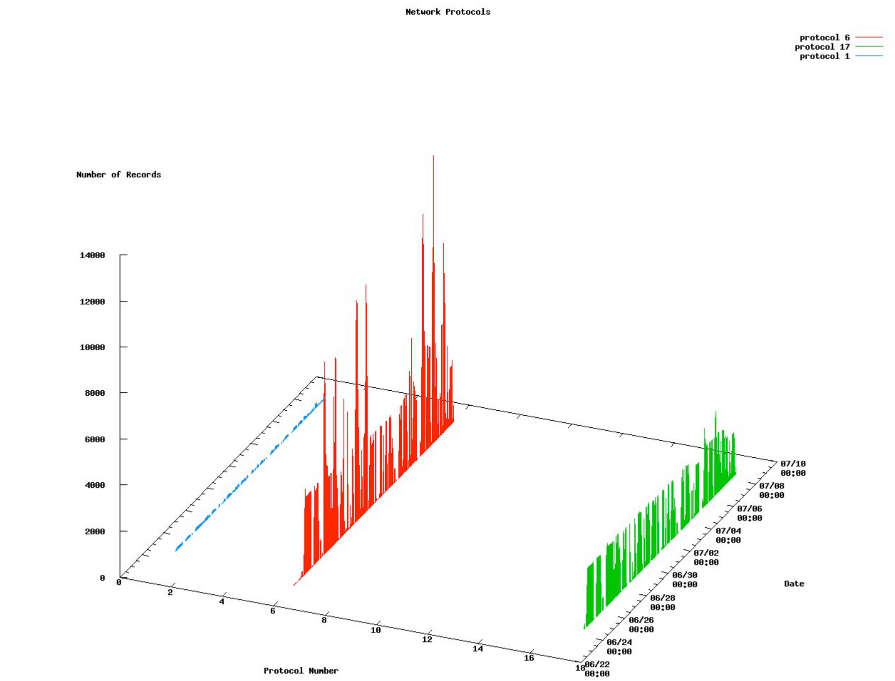
NetBytes Viewer

Joel Glanfield

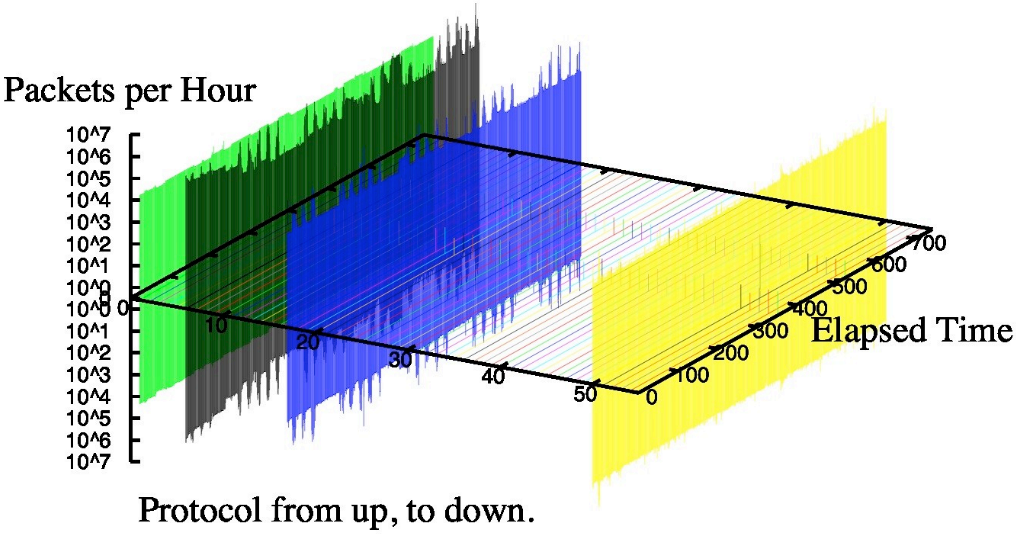
Purpose

- Interactive visualization.
- Part of the FloVis framework along with the Activity Viewer and FlowBundle.
- Visualizes Netflow traffic using an entity-based approach.
- Focuses on volumes (bytes, flows, packets).
- Provides a historical context to traffic volume patterns using a 3D graph.

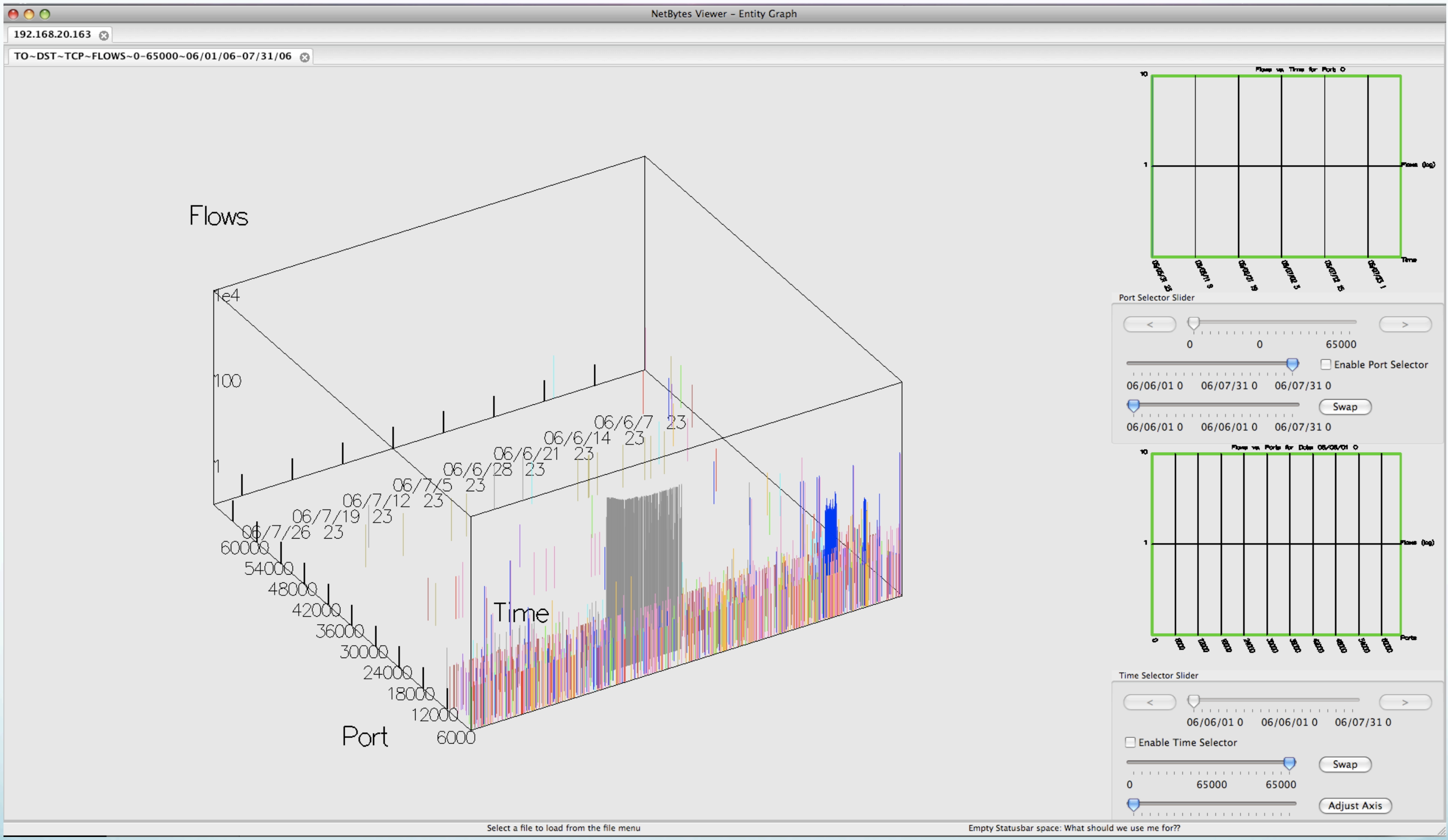




Subnet 10.0.64.0/22: 2006/03/01T00 to 2006/03/31T23
Per protocol traffic from/to subnet up/down



NetBytes Viewer



NetBytes Viewer – Entity Graph

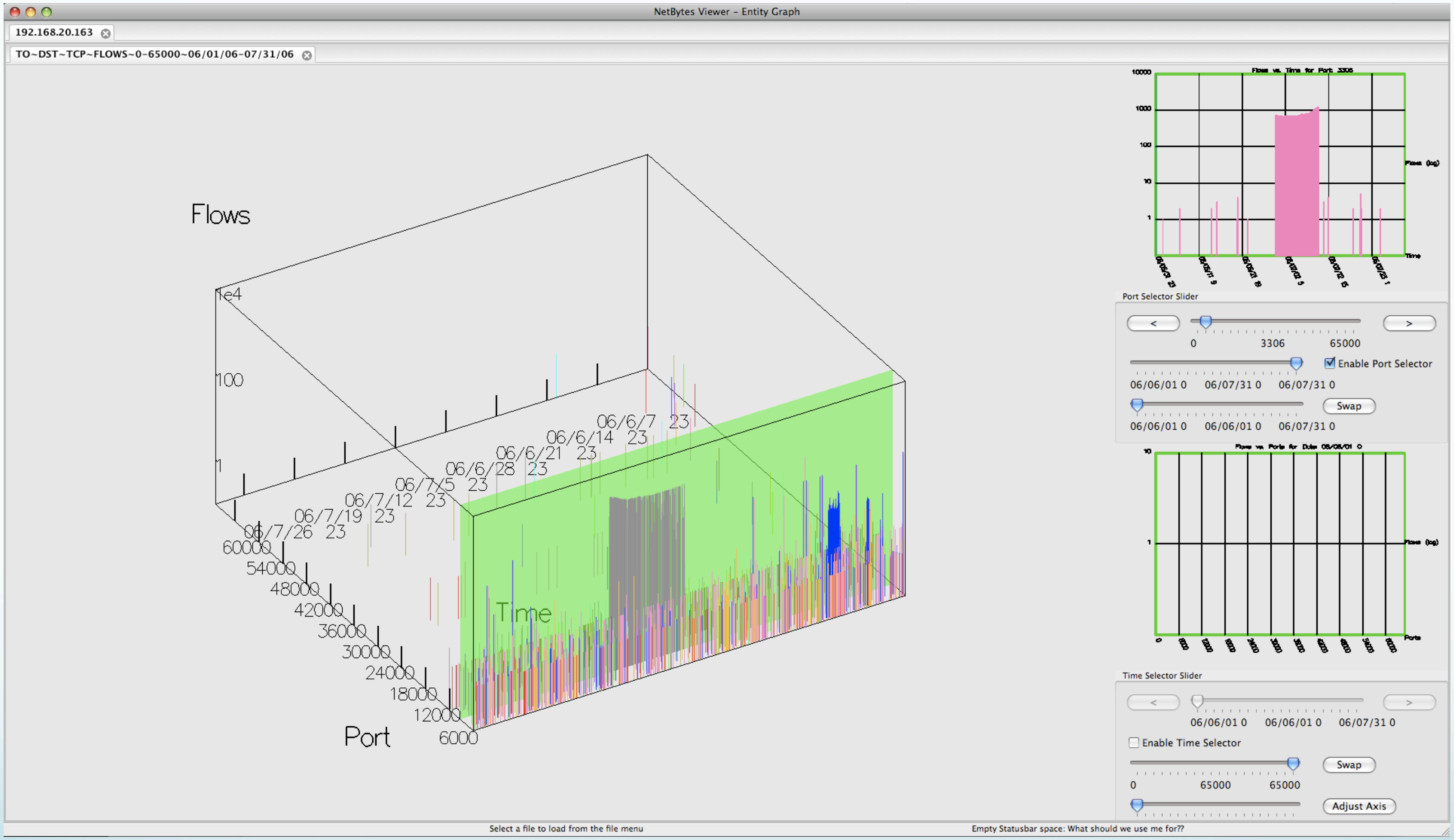
192.168.20.163

TO~DST~TCP~FLOWS~0~65000~06/01/06-07/31/06

Select a file to load from the file menu

Empty Statusbar space: What should we use me for??

Selection Mode



NetBytes Viewer – Entity Graph

192.168.20.163

TO~DST~TCP~FLOWS~0~65000~06/01/06~07/31/06

Port Selector Slider

☑ Enable Port Selector

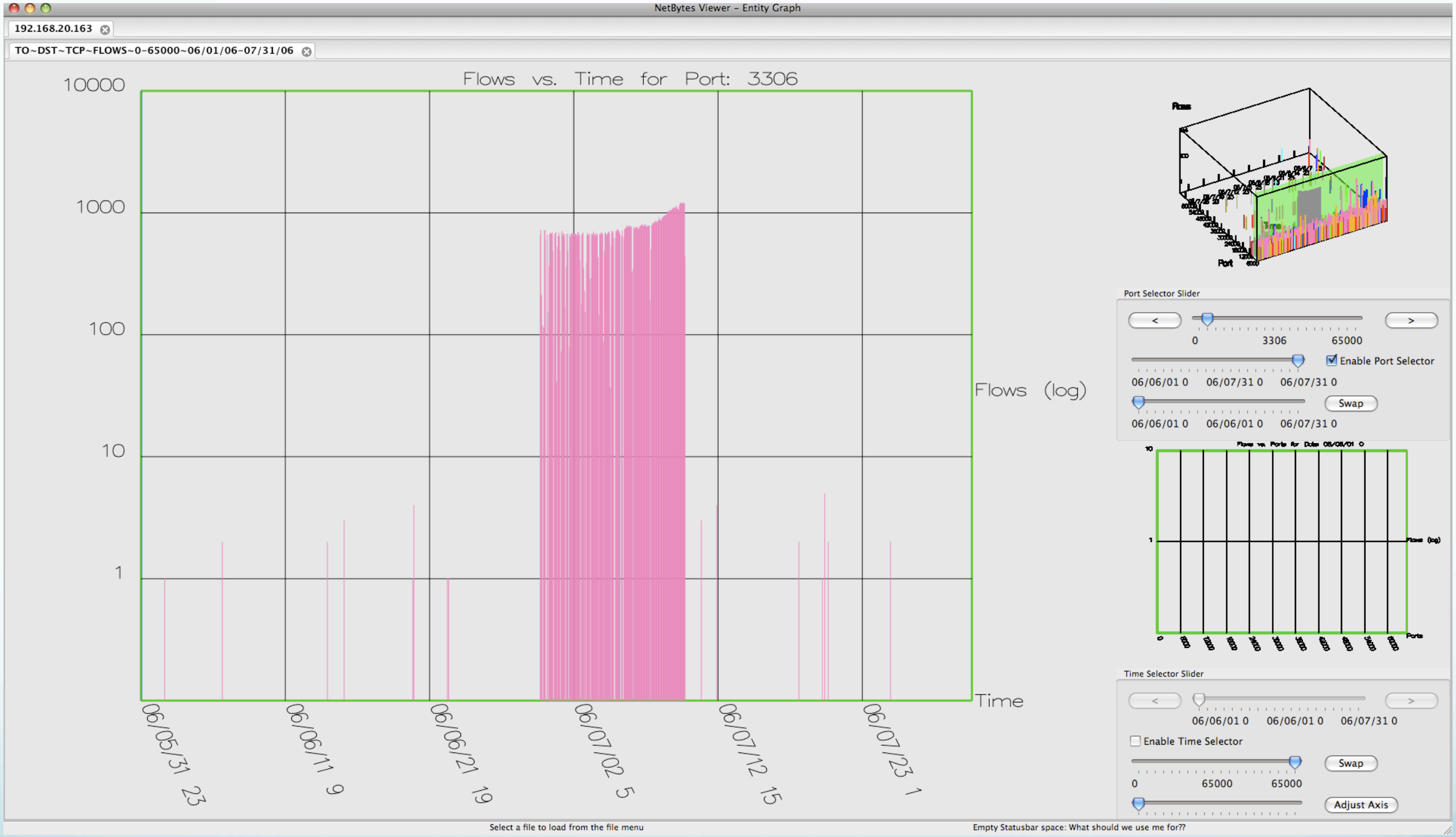
Time Selector Slider

☐ Enable Time Selector

Select a file to load from the file menu

Empty Statusbar space: What should we use me for??

Swapping the Main View



NetBytes Viewer – Entity Graph

192.168.20.163

TO~DST~TCP~FLOWS~0~65000~06/01/06-07/31/06

Port Selector Slider

< 0 3306 65000 >

☑ Enable Port Selector

06/06/01 0 06/07/31 0 06/07/31 0

06/06/01 0 06/06/01 0 06/07/31 0 Swap

Time Selector Slider

< 06/06/01 0 06/06/01 0 06/07/31 0 >

□ Enable Time Selector

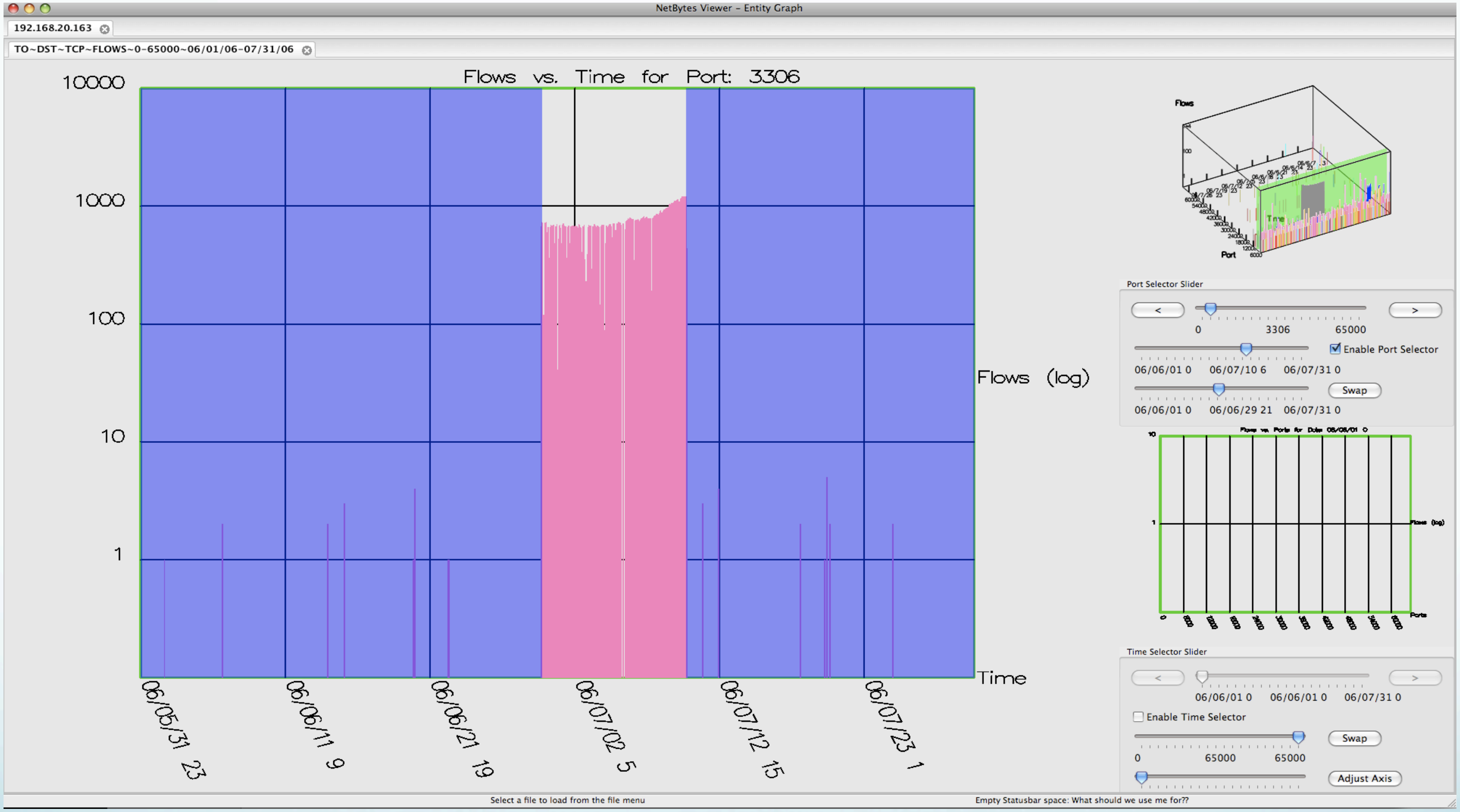
0 65000 65000 Swap

Adjust Axis

Select a file to load from the file menu

Empty Statusbar space: What should we use me for??

Adjust the Axis



NetBytes Viewer – Entity Graph

192.168.20.163

TO~DST~TCP~FLOWS~0~65000~06/01/06~07/31/06

Port Selector Slider

< 0 3306 65000 >

☑ Enable Port Selector

06/06/01 0 06/07/10 6 06/07/31 0

Swap

06/06/01 0 06/06/29 21 06/07/31 0

Time Selector Slider

< 06/06/01 0 06/06/01 0 06/07/31 0 >

☐ Enable Time Selector

Swap

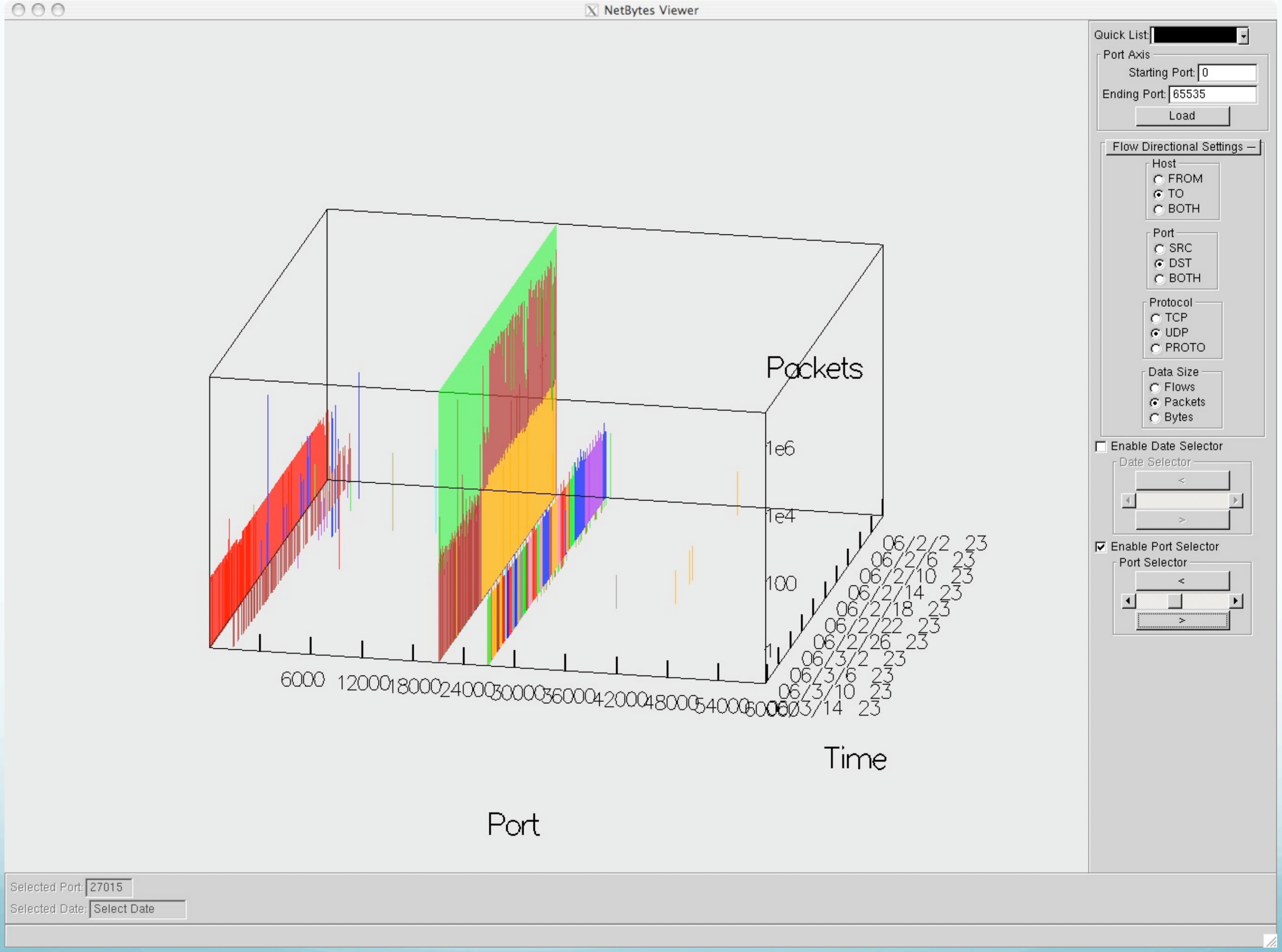
0 65000 65000

Adjust Axis

Select a file to load from the file menu

Empty Statusbar space: What should we use me for??

Case Study: Compromised Host



Quick List:

Port Axis

Starting Port: 0

Ending Port: 65535

Flow Directional Settings

Host
○ FROM
● TO
○ BOTH

Port
○ SRC
● DST
○ BOTH

Protocol
○ TCP
● UDP
○ PROTO

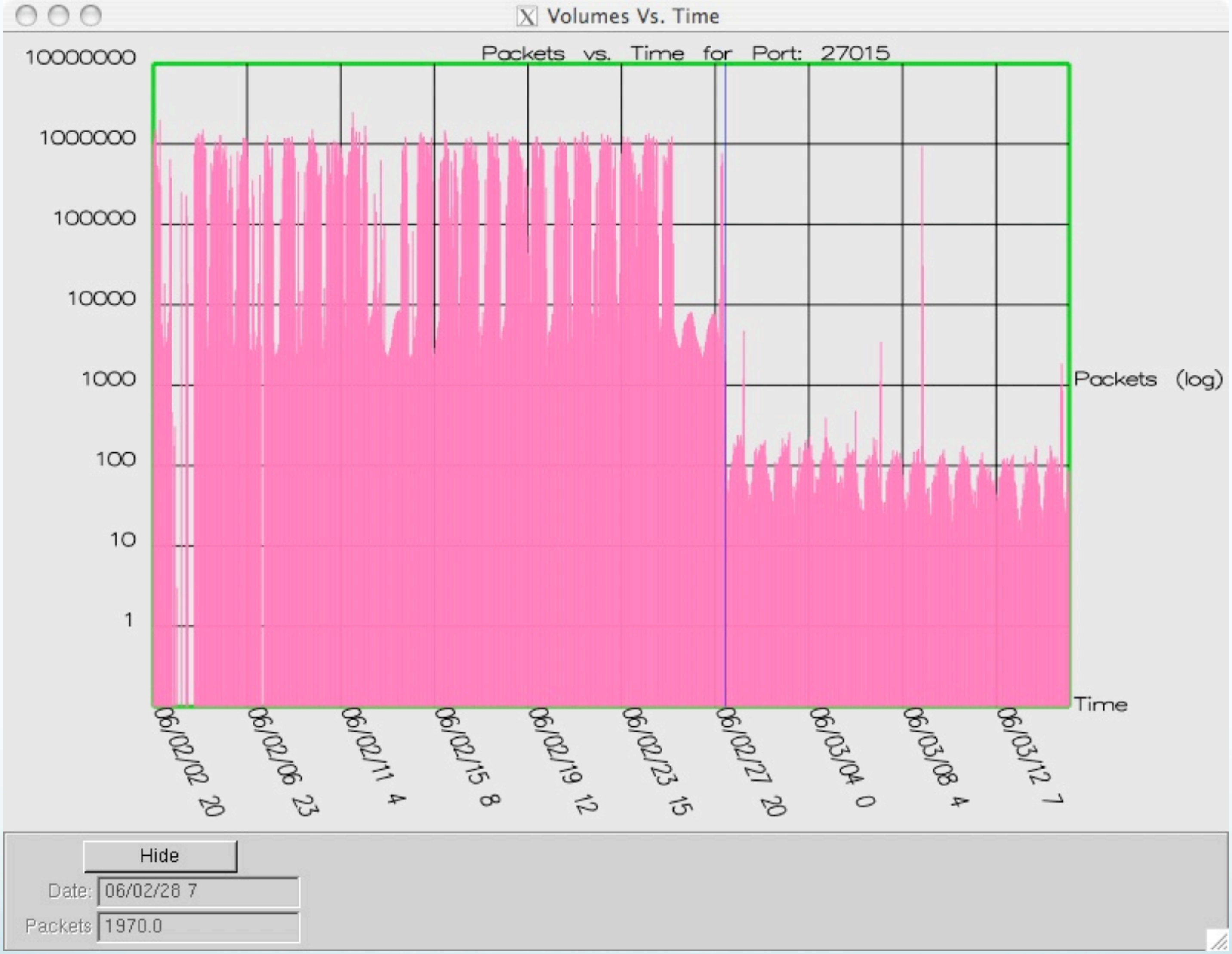
Data Size
○ Flows
● Packets
○ Bytes

☐ Enable Date Selector

☑ Enable Port Selector

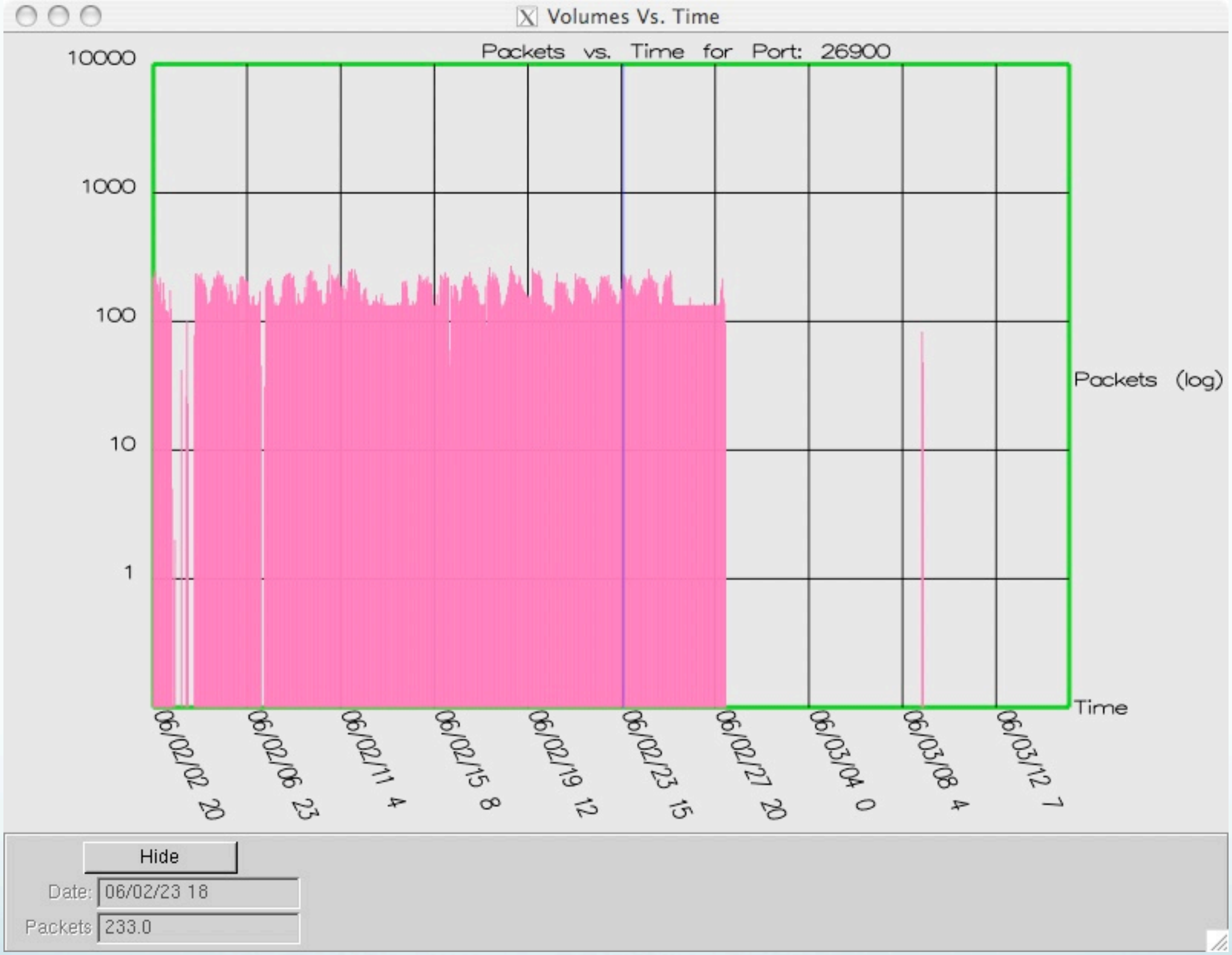
Selected Port: 27015

Selected Date: Select Date



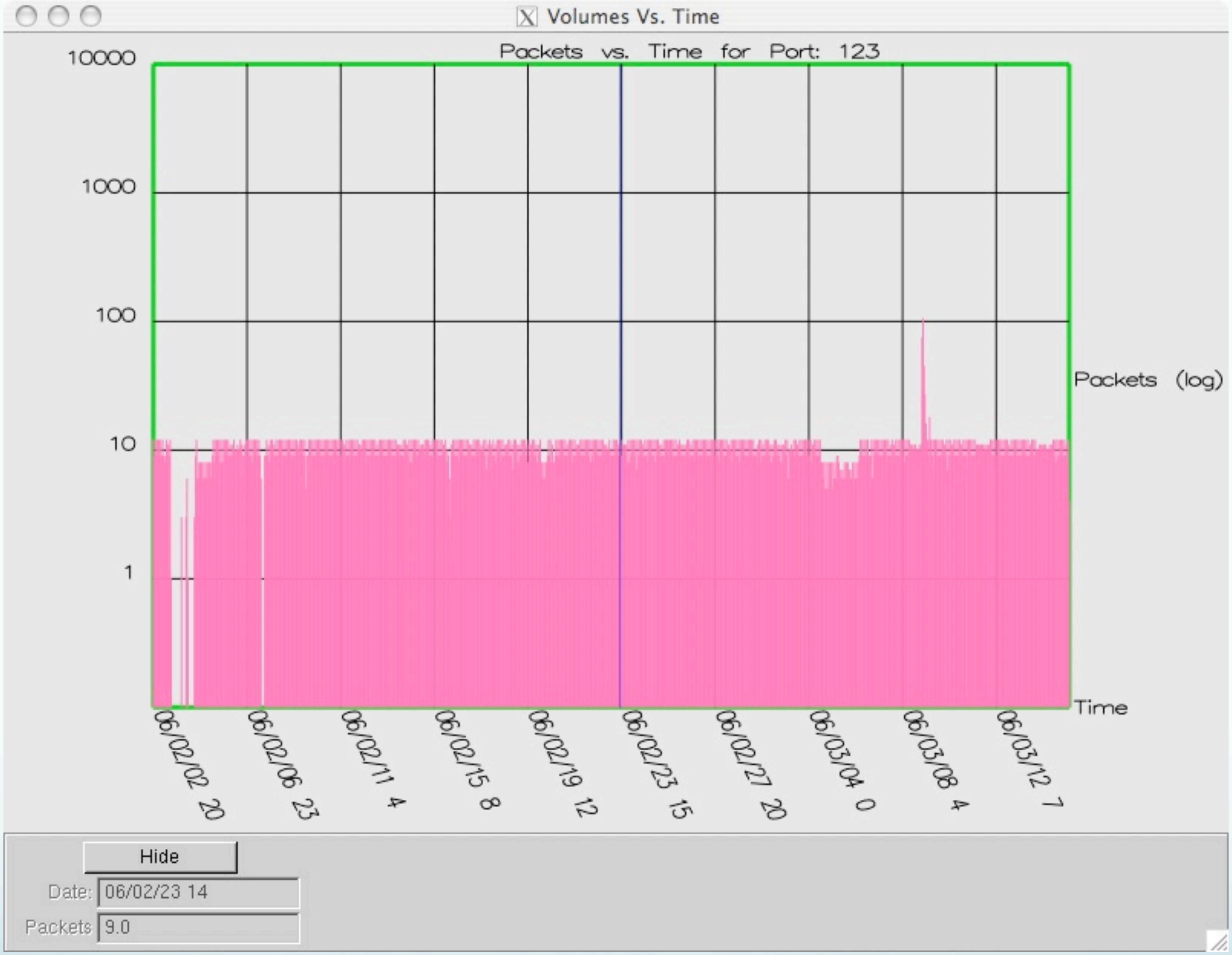
Date: 06/02/28 7

Packets 1970.0



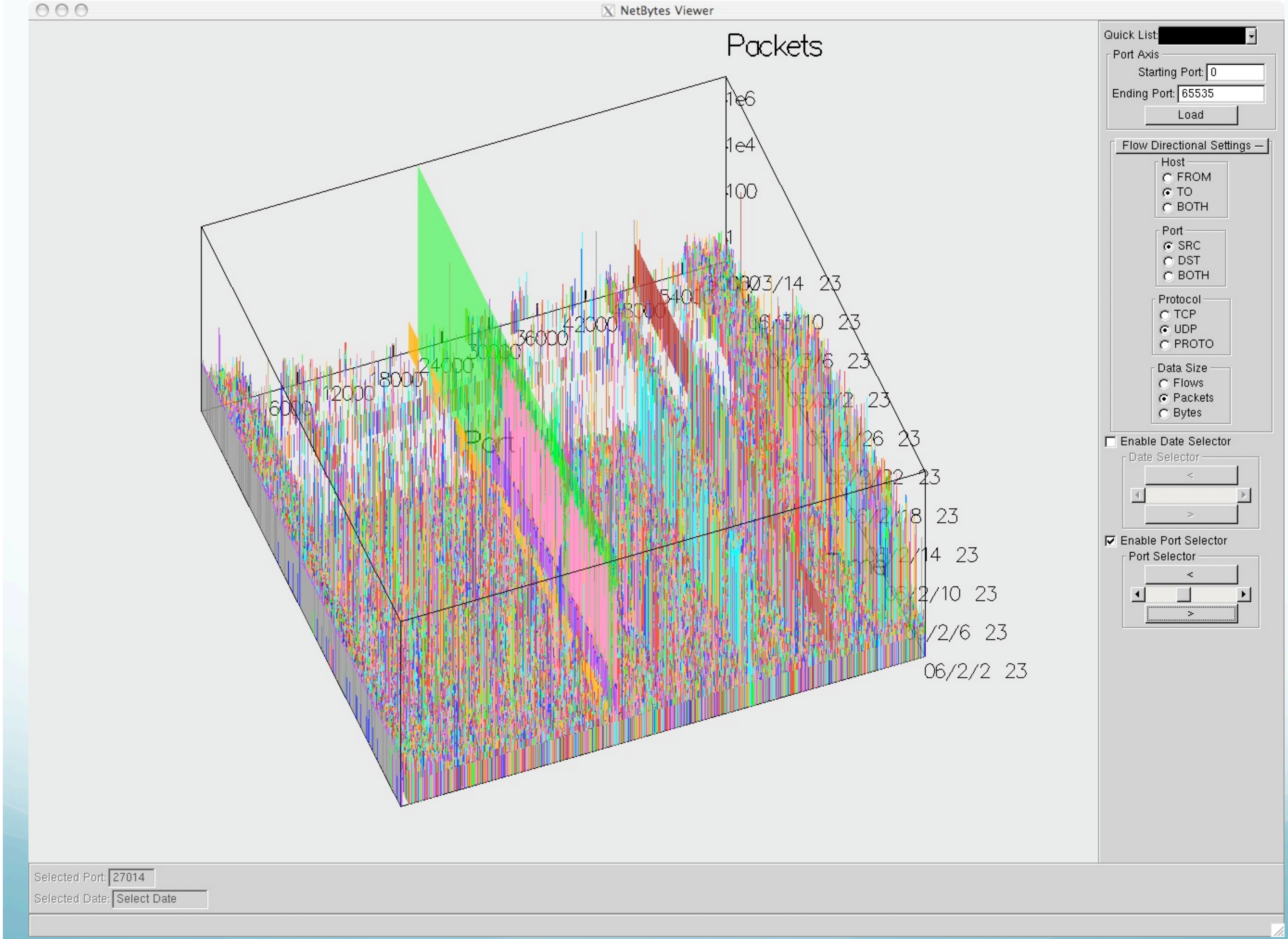
Date: 06/02/23 18

Packets 233.0



Date: 06/02/23 14

Packets 9.0



Quick List:

Port Axis

Starting Port: 0

Ending Port: 65535

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