Visualizing Network Security Events using Compound Glyphs from a Service-Oriented Perspective

Jason Pearlman, Henggeler Consulting

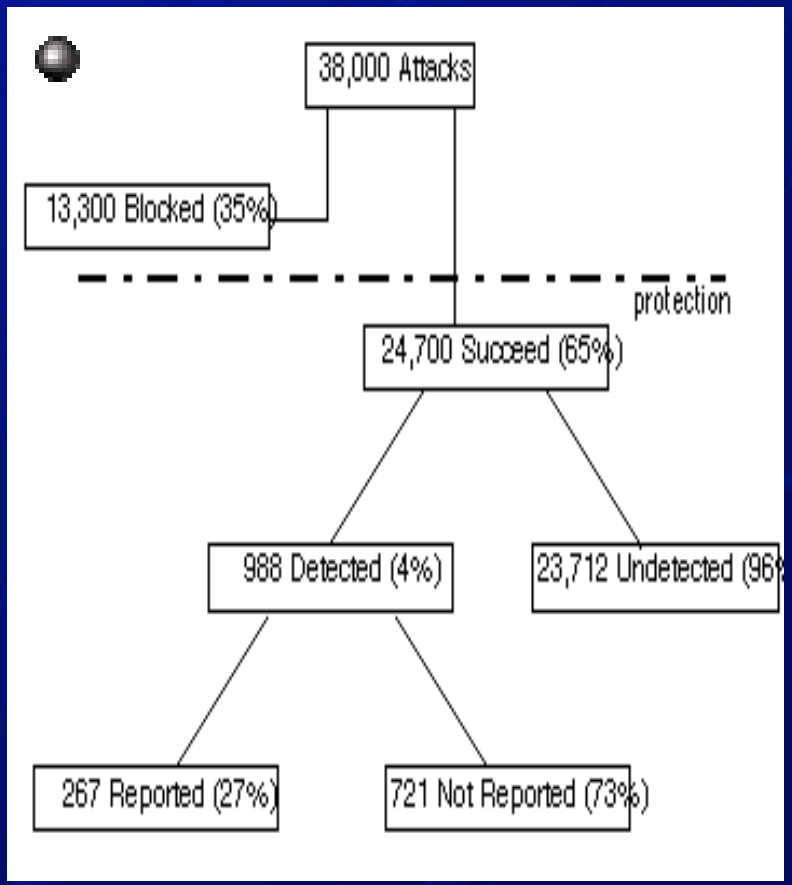
Penny Rheingans, UMBC

Outline

- Problem and Motivation
- Network Attack Background
- Related Work
- Approach
- Results
- Evaluation
- Conclusions/Questions

Problem and Motivation

- Network attacks are a serious problem
  - Network attacks cost businesses estimated 666 million in 2003 [Ball04]
  - DISA (Defense Information Systems Agency) study [Howard]:
    - Approximately 44 million network attacks occur per year
    - 0.7% of network attacks are reported
    - 2.6% are detected

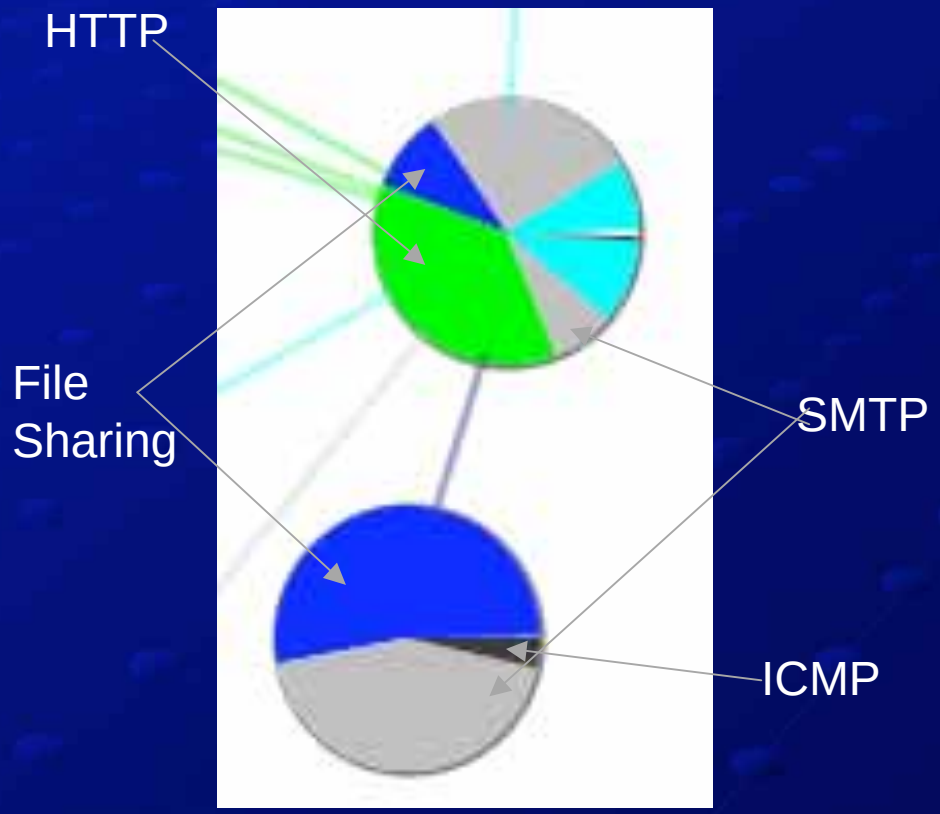


Network Attack Background

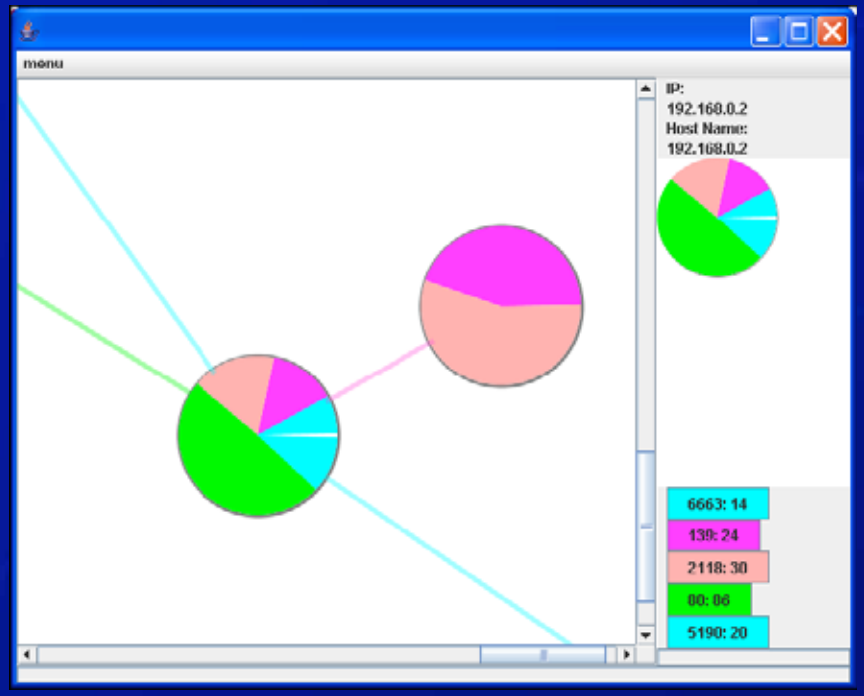
- Some Attack Types
  - Denial of Service (DoS)
    - Overload a service with more load than it can handle
  - Distributed Denial of Service (DDoS)
    - Overload from multiple sources
  - Network Trojan
    - Install itself on a system, propagate to related systems
- Nework Security Data comes in various forms
  - Raw data
  - System and application logs
  - Network routing
  - Port status

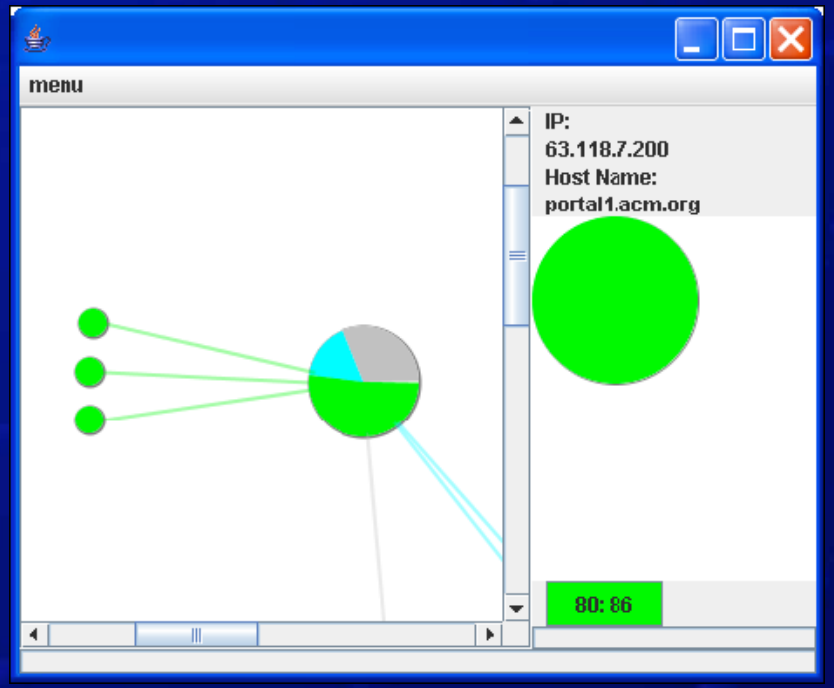
Basic Approach

- Graph of compound glyphs
  - Home-centric
  - Service-oriented
- Pie glyph
  - Size of wedge based on relative activity of service
  - Managed nodes larger than unmanaged
  - Unmanaged node size corresponds to amount of activity



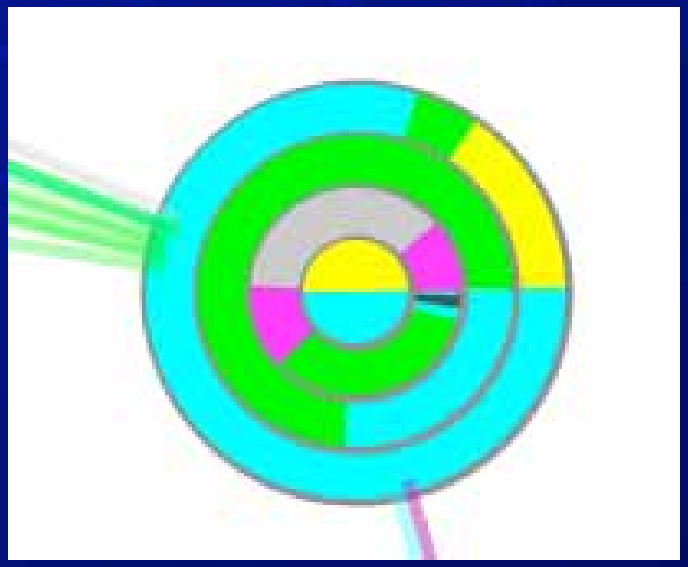
Network Node Glyph



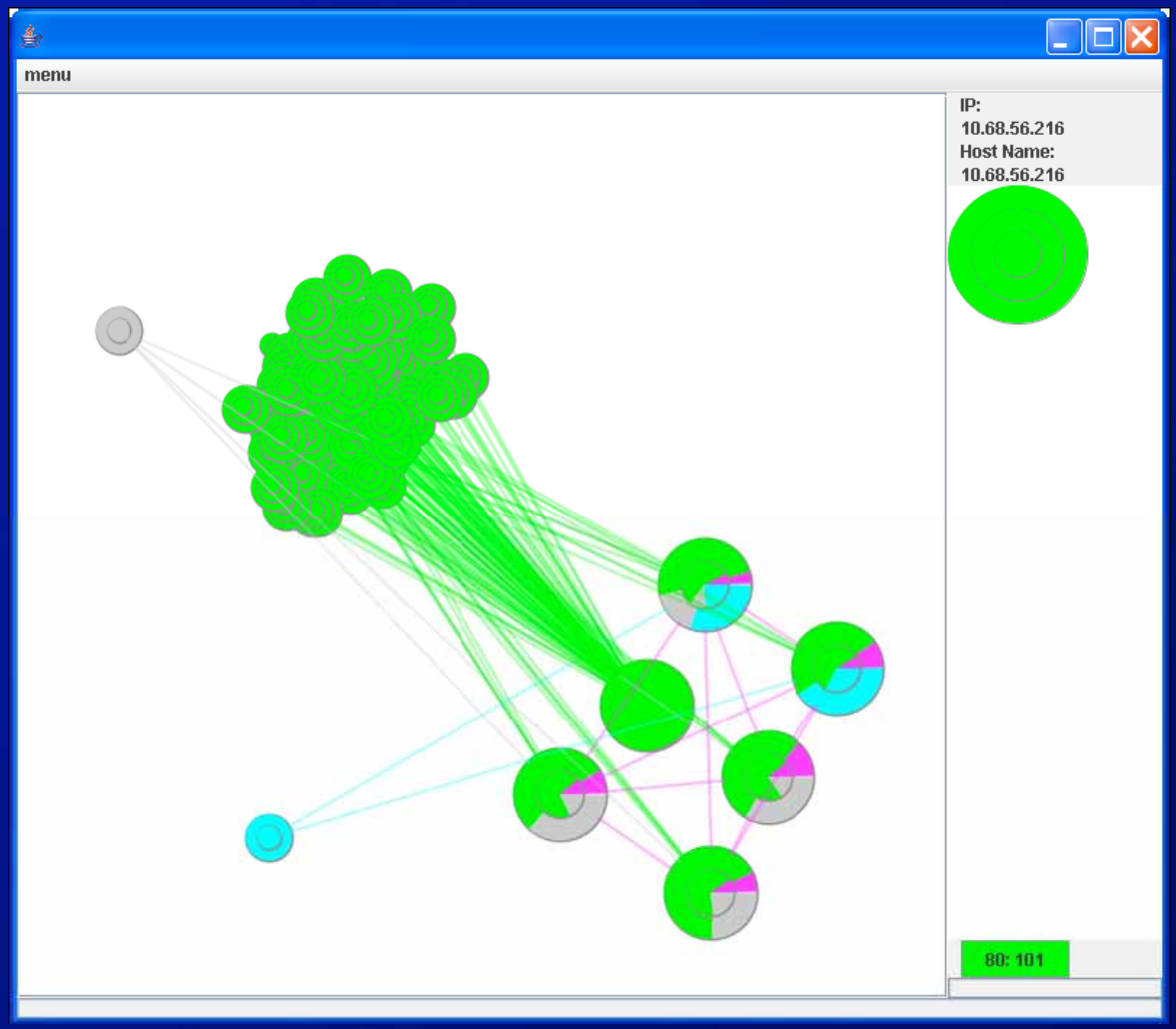


Time Slicing

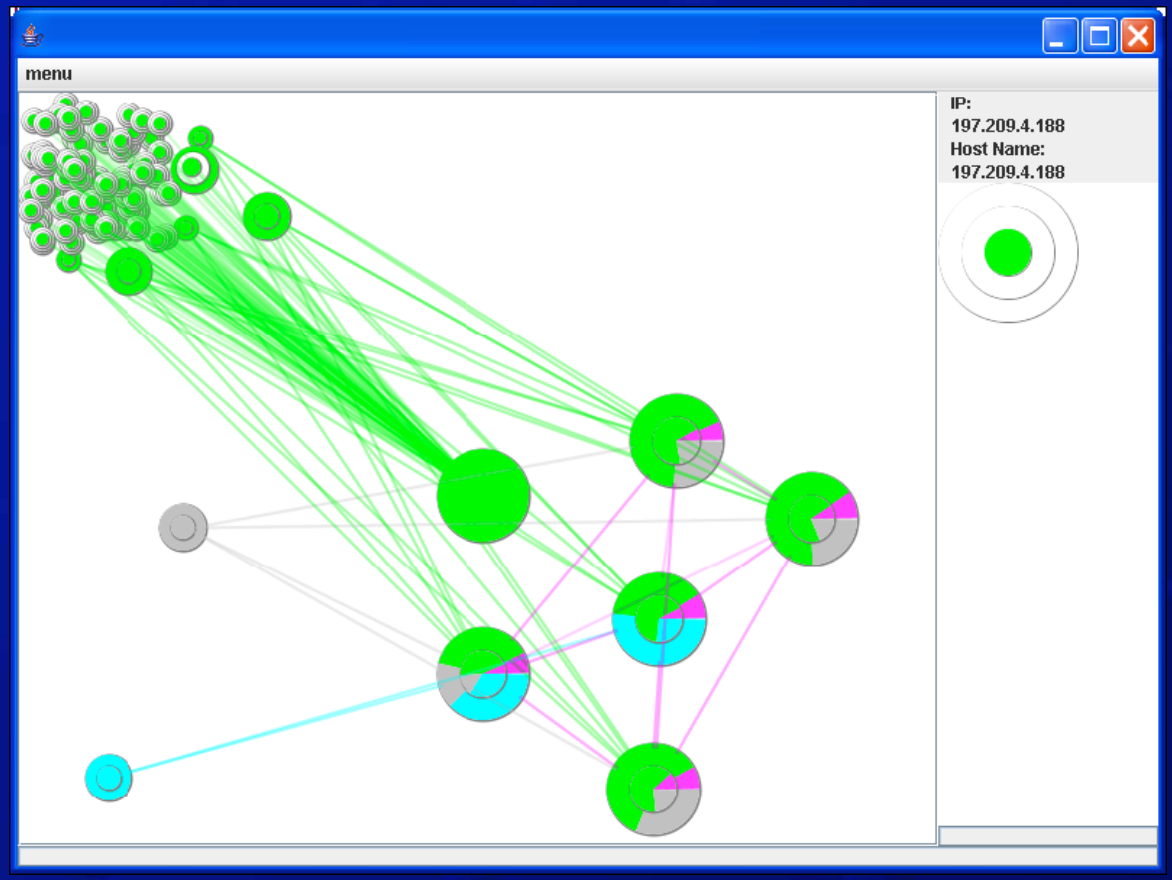
- Temporal visualization technique applied to glyphs
- Inner slice represents activity furthest in the past
- Outer is most recent



Results (Guess What)

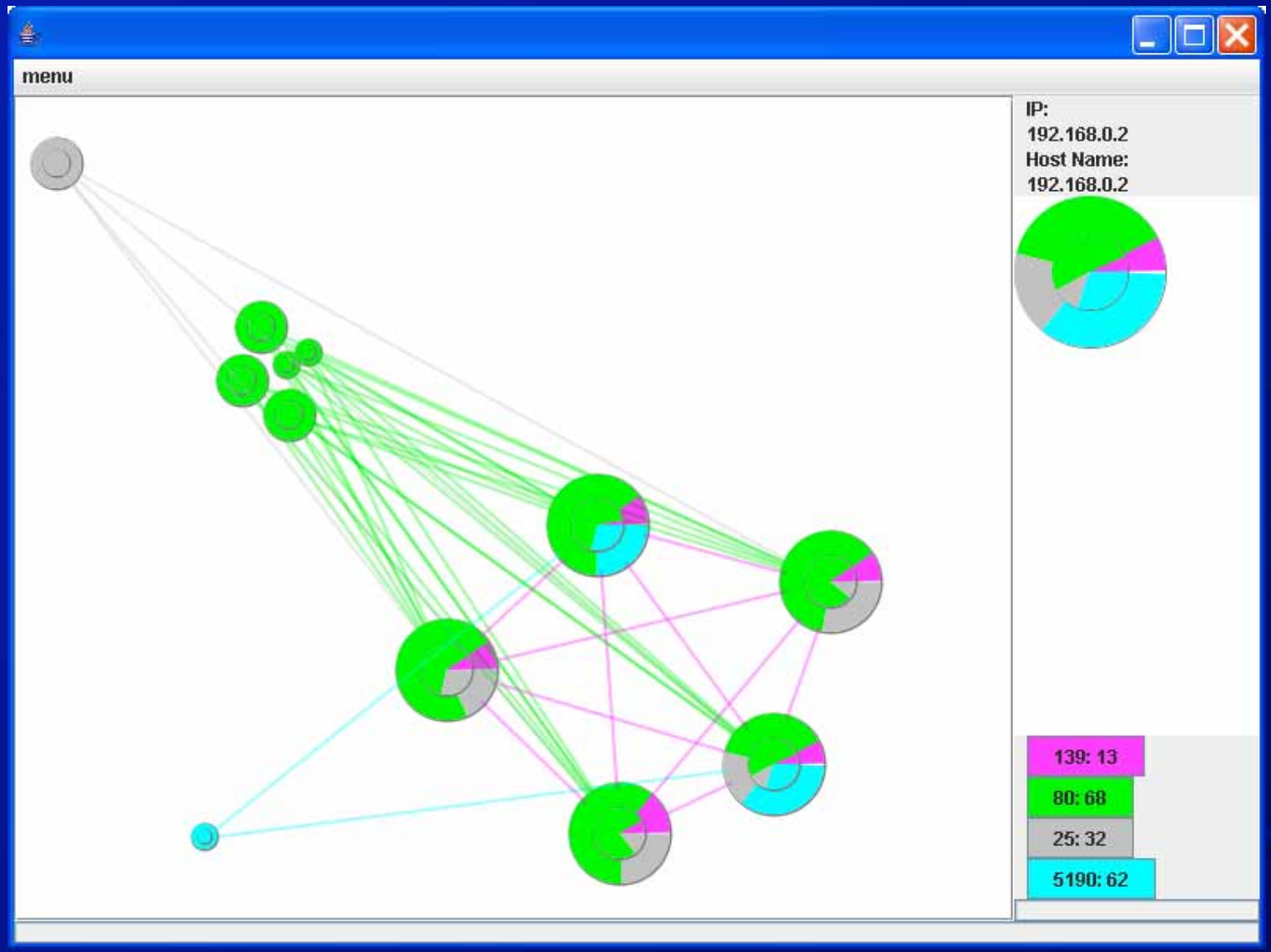


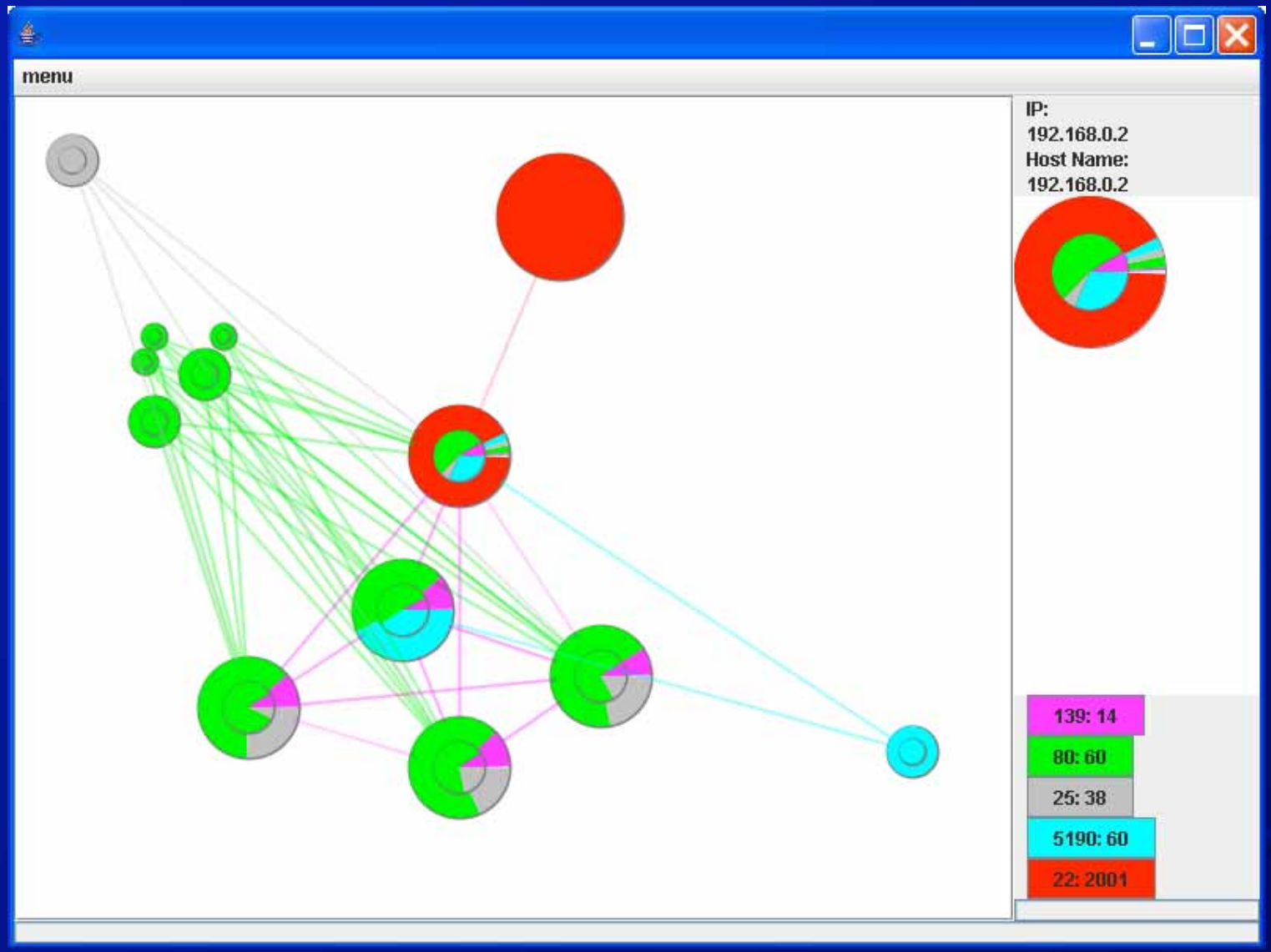
Results, not your initial reaction…

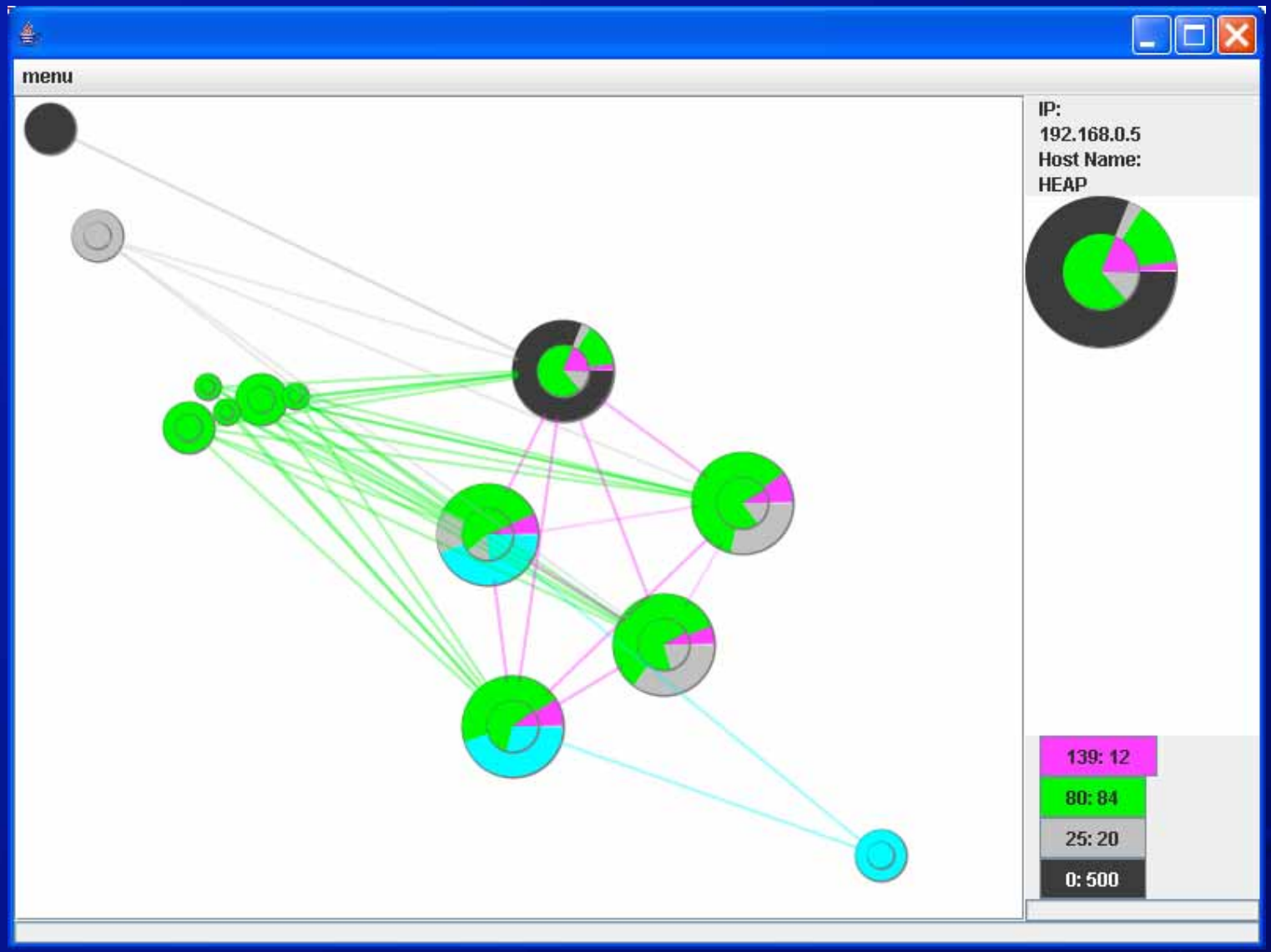


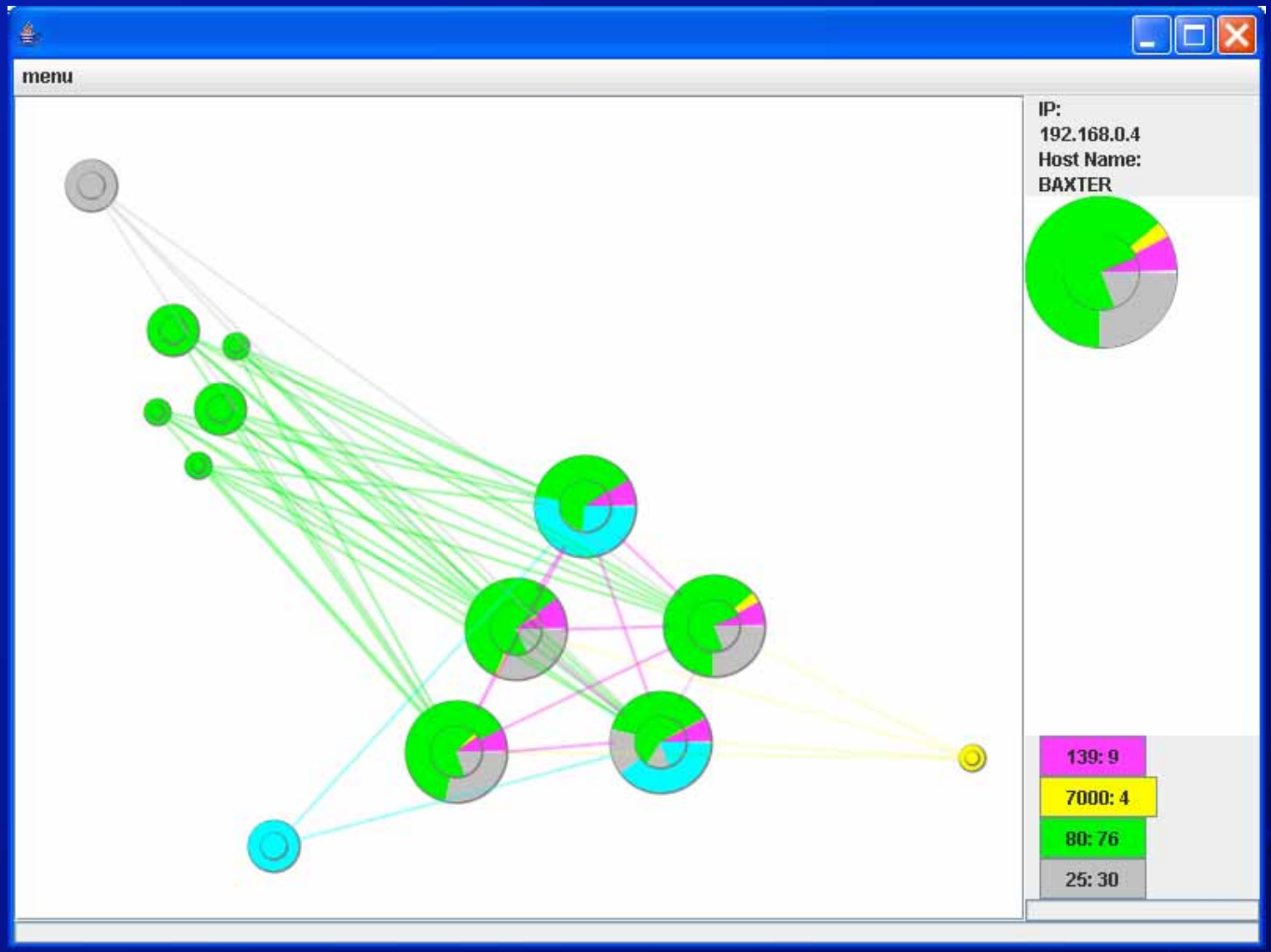
Evaluation

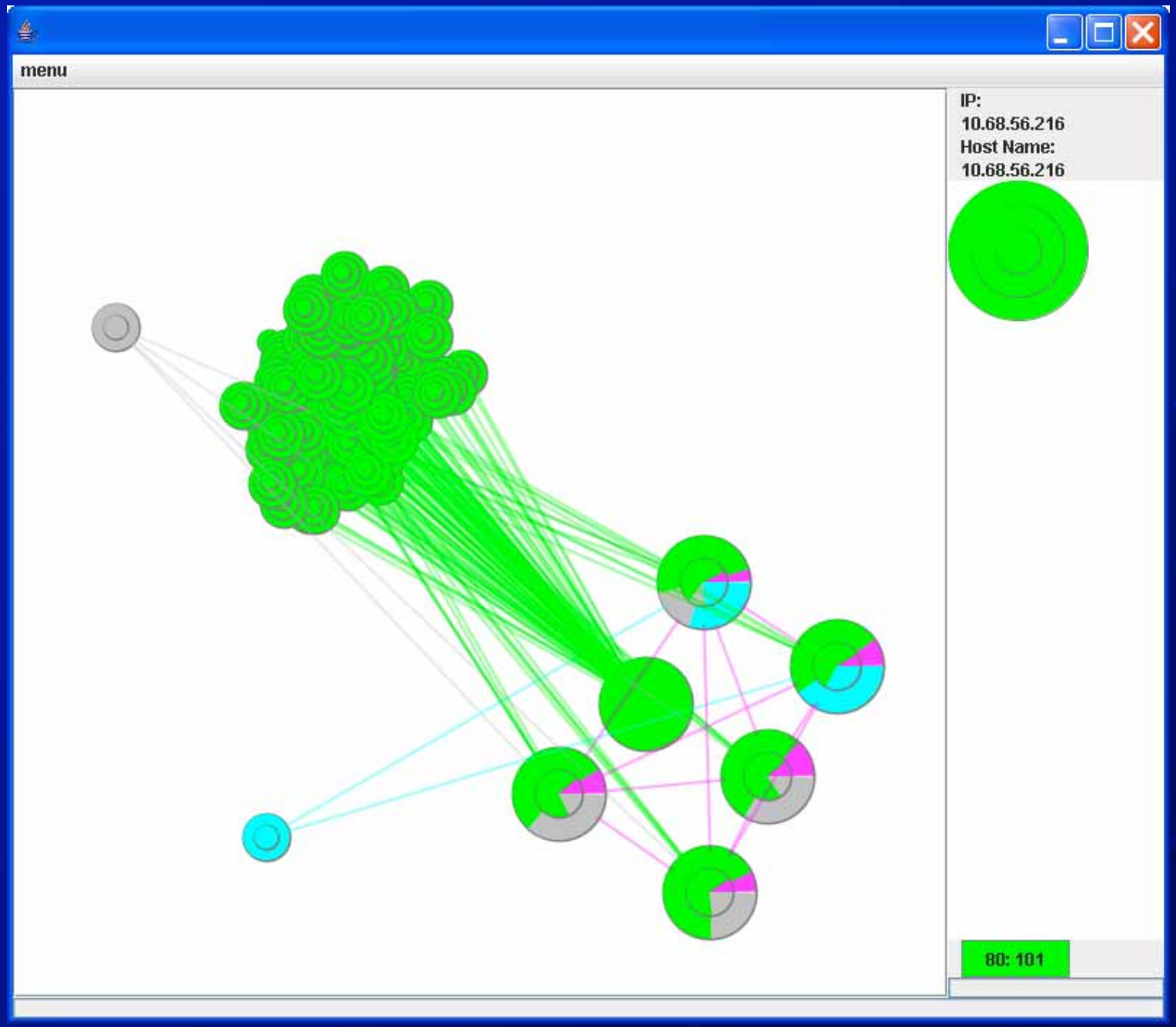
- Several resulting images were shown to a group of five network administrators
- They were asked to explain what they see and choose which attack fits the image best from the following choices
  - Distributed Denial of Service
  - Denial of Service
  - Compromised Network using Trojans
  - Session Hijacking
  - No attack present

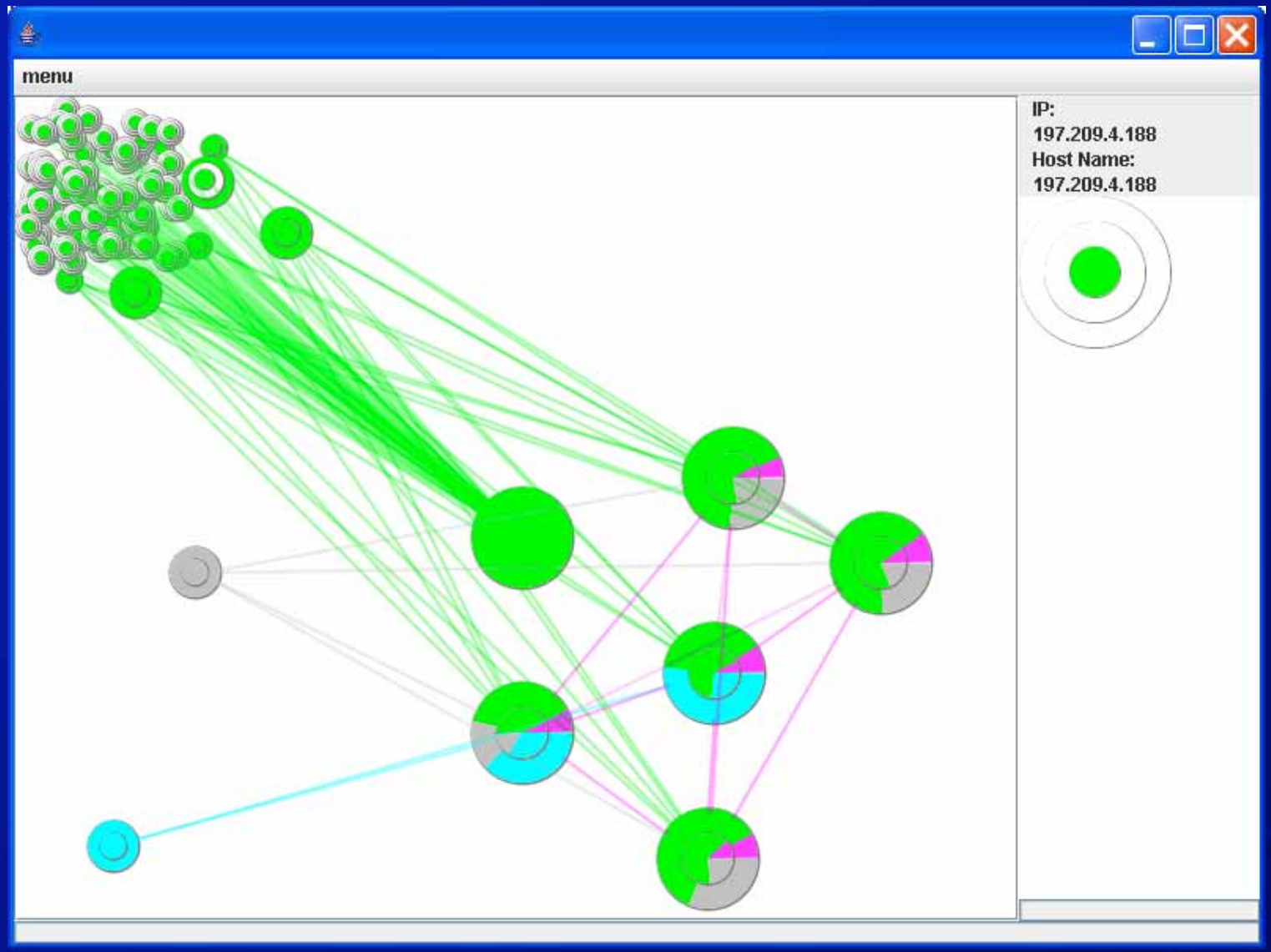

menu
IP:
192.168.0.2
Host Name:
192.168.0.2
139: 13
80: 68
25: 32
5190: 62


menu
IP:
192.168.0.2
Host Name:
192.168.0.2
139: 14
80: 60
25: 38
5190: 60
22: 2001


menu
IP:
192.168.0.5
Host Name:
HEAP
139: 12
80: 84
25: 20
0: 500


menu
IP:
192.168.0.4
Host Name:
BAXTER
139: 9
7000: 4
80: 76
25: 30


menu
IP:
10.68.56.216
Host Name:
10.68.56.216
80: 101

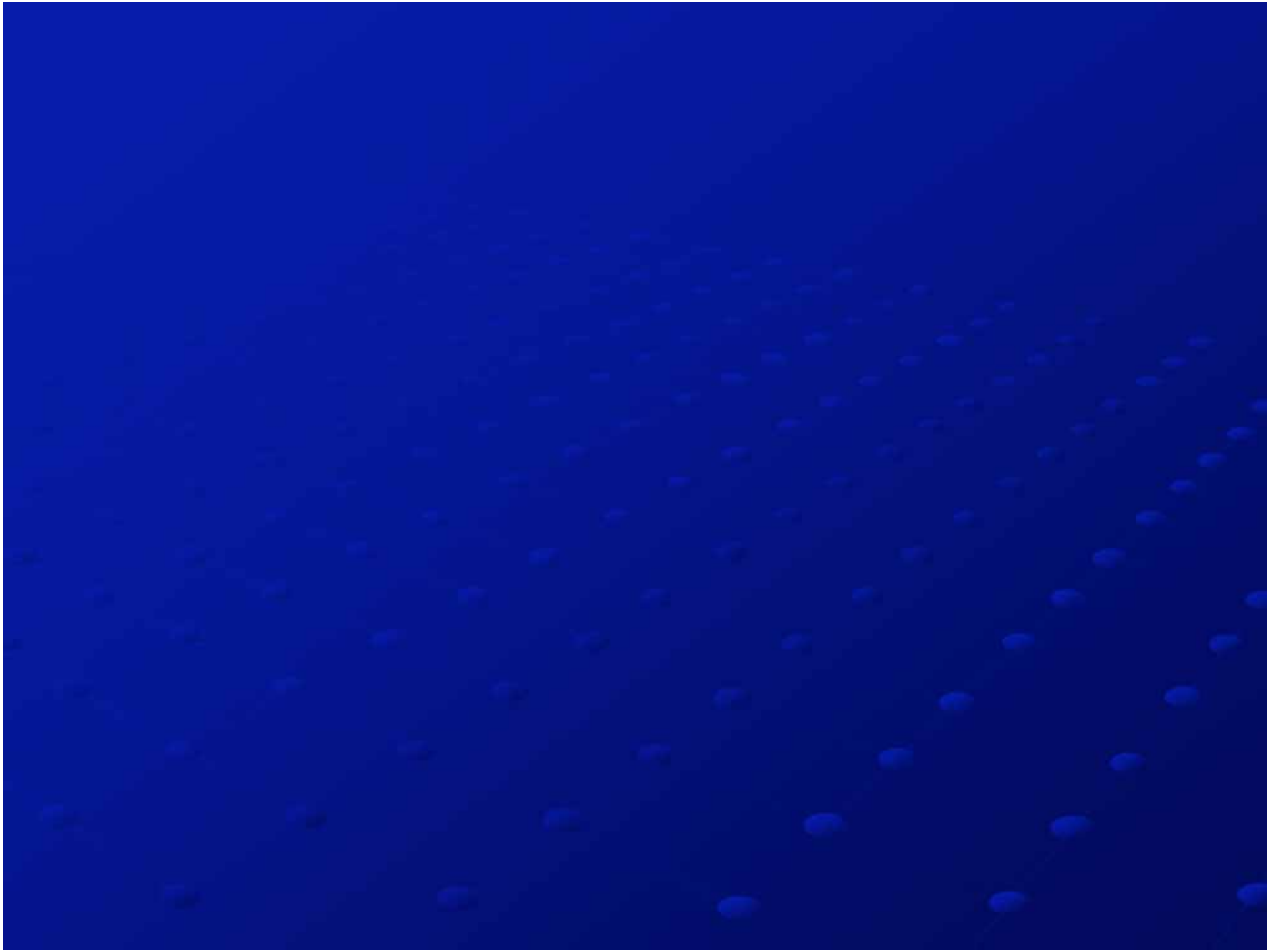

menu
IP:
197.209.4.188
Host Name:
197.209.4.188

Conclusion

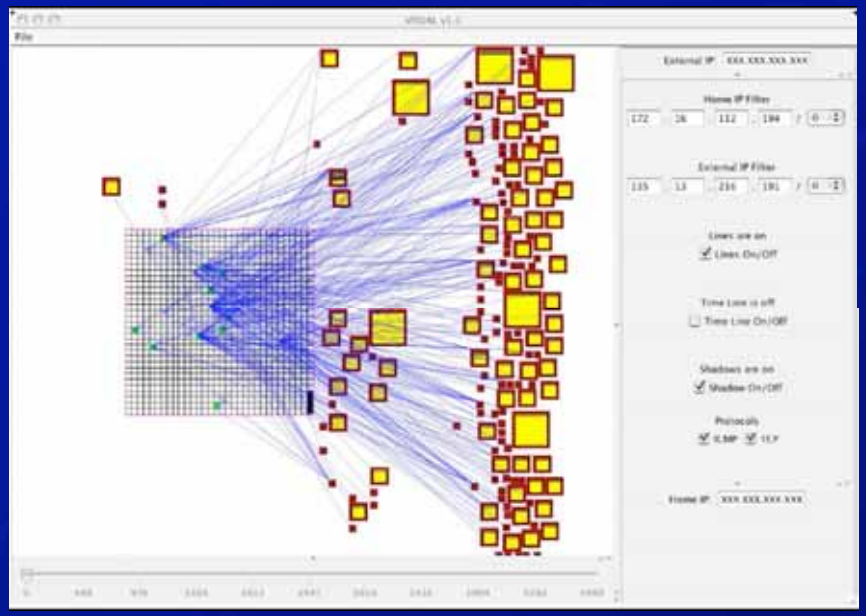
- Four out of five network administrators felt this approach would add additional value in identifying network security events when compared with their current approaches.
- This research provides an application using a combination of visualization techniques applied a network traffic data set in order to better detect the type, severity, and presence of a network attack.

The end

Questions/Comments?



Related Work

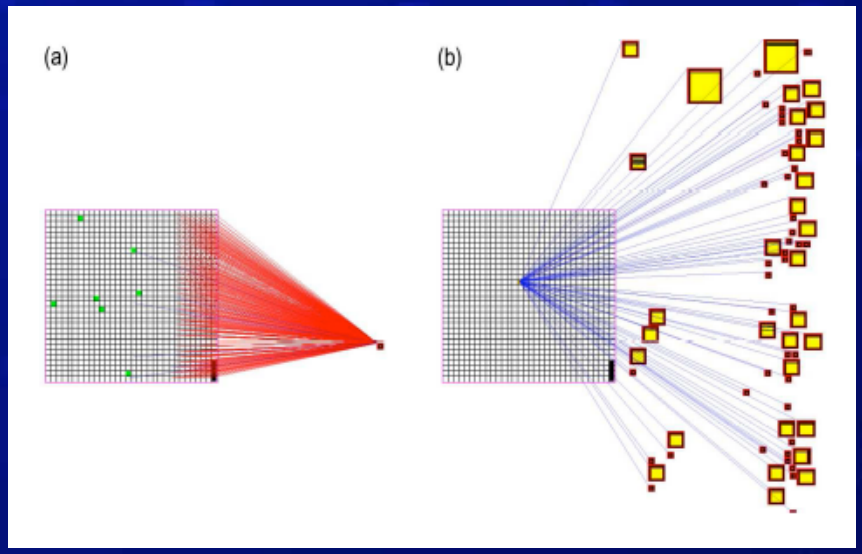


- Home-centric approach
- Embedded activity information into glyph
- Shading
- Filtering

Source: Ball, R., Fink, G. A., and North, C. 2004. Home-centric visualization of network traffic for security administration. In *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining For Computer Security* (Washington DC, USA, October 29 - 29, 2004). VizSEC/DMSEC '04. ACM Press, New York, NY, 55-64

Related Work

- B in the image shows an example of a server on the managed network
- How much activity is happening?
- What kind of activity is the server producing?



Source: Ball, R., Fink, G. A., and North, C. 2004. Home-centric visualization of network traffic for security administration. In *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining For Computer Security* (Washington DC, USA, October 29 - 29, 2004). VizSEC/DMSEC '04. ACM Press, New York, NY, 55-64