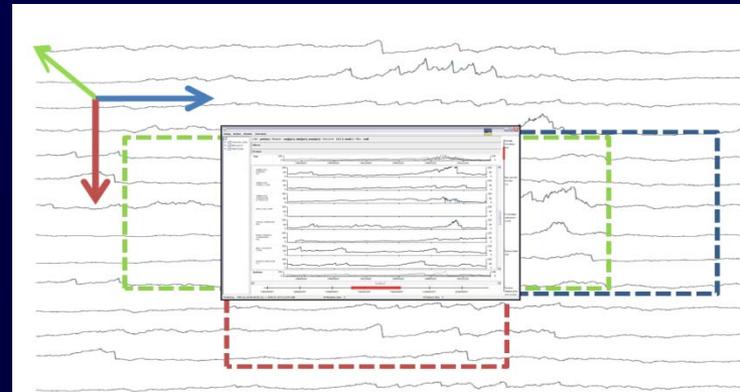


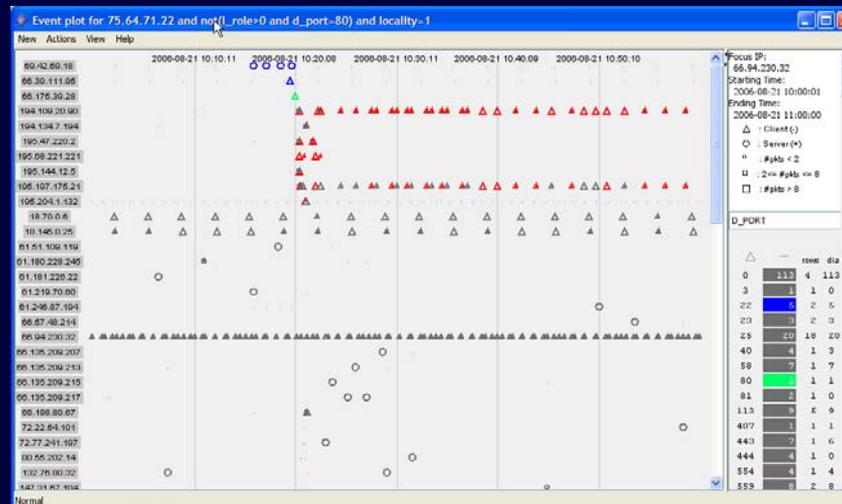
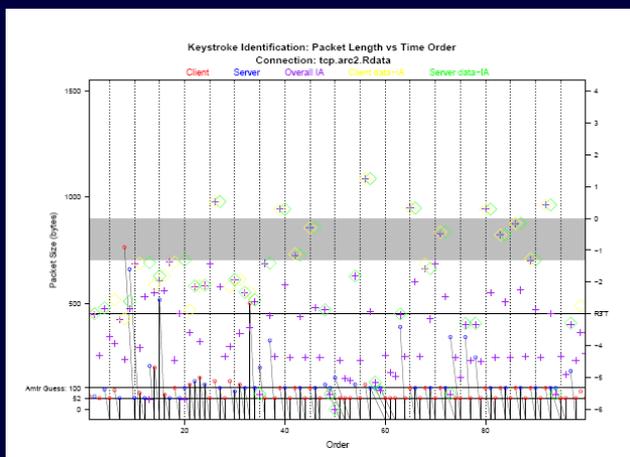
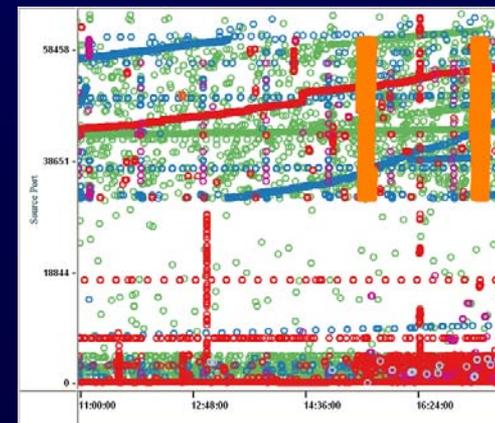
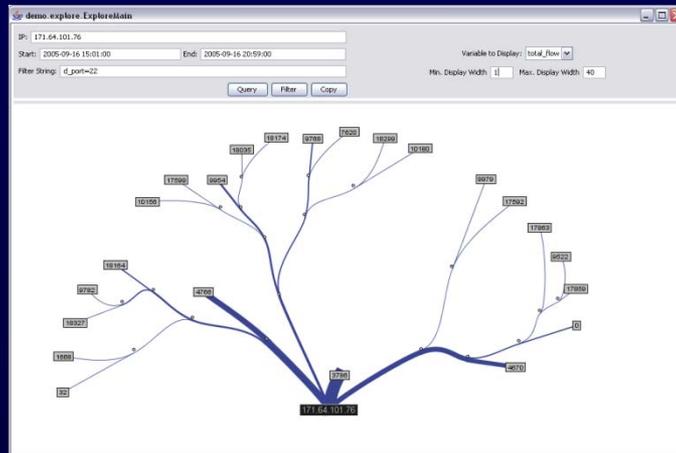
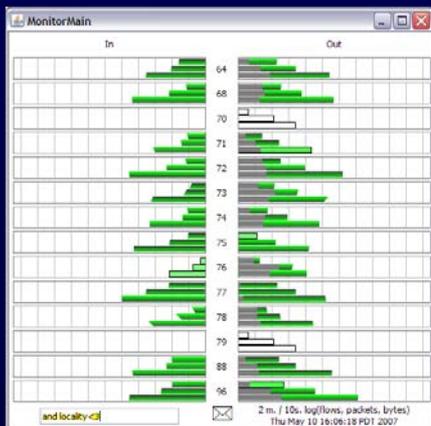
# Stanford/Purdue: Cybersecurity Analytics

- **Branch of Transactional analytics**
  - Focus on network cybersecurity
  - Support interactive analysis of large datasets
- **Visual tool development**
  - Seeing each visualization as a hypothesis test
  - Allowing analysts to create new displays
  - Understanding what makes effective displays
- **Apply analytics and tools at multiple scales**
  - Analyzing traffic at a fine scale
  - Determining the right summaries
  - Supporting forensic investigations





# What have we tried ?



# What have we learned ?

## Humility

- Use simple displays
- Let the data lead you
- Keep history/allow backtrack
- Design for interoperation
- Push analytics upstream
- Support presentation of findings
- Plan on evolution

