Florida Institute of Technology

Harris Institute for Assured Information

C3E Challenge Problem

Marco Carvalho, Ph.D.

Associate Professor and Executive Director,
Harris Institute for Assured Information

Harris Chair for Assured Information

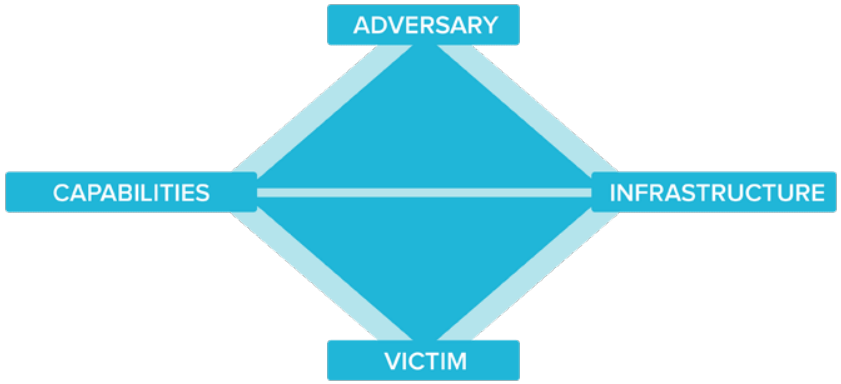
Florida Institute of Technology

Florida Institute of Technology

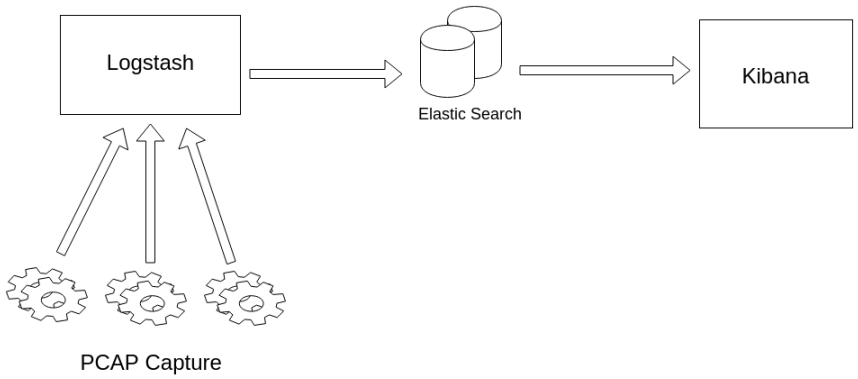
Harris Institute for Assured Information

Two approaches

- Correlating Events across different target networks
  - Source, type, time
- Correlating Patterns across different target networks
  - Looking for Common Data Structures: Generalized Structures or cycles in data that may be repeatable across different target networks
- Visual Analytics
  - Building Visual queries to investigate possible relationships between events in the data
  - Exploring the use of the Diamond model



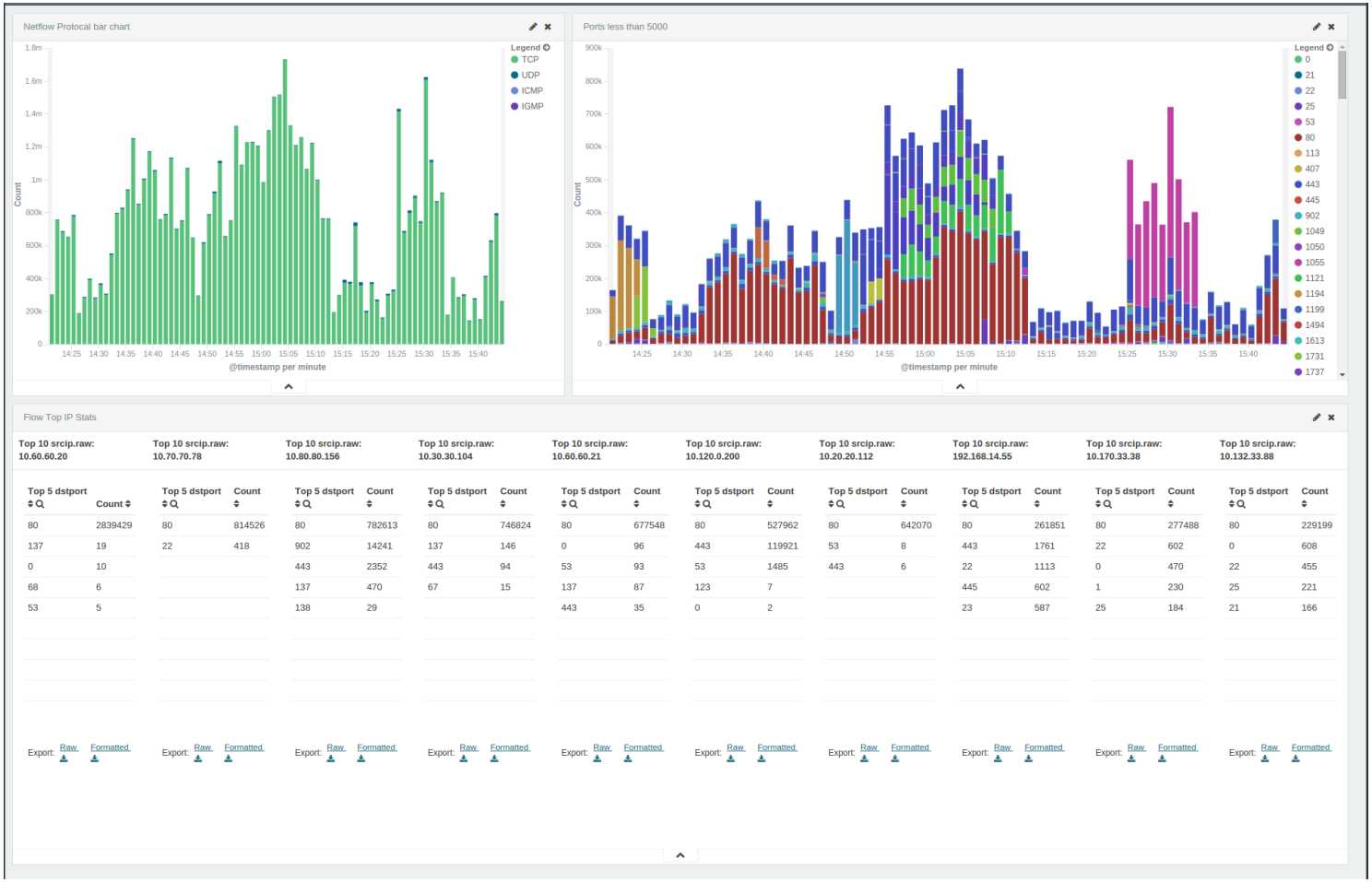
Data Overview and Characterization



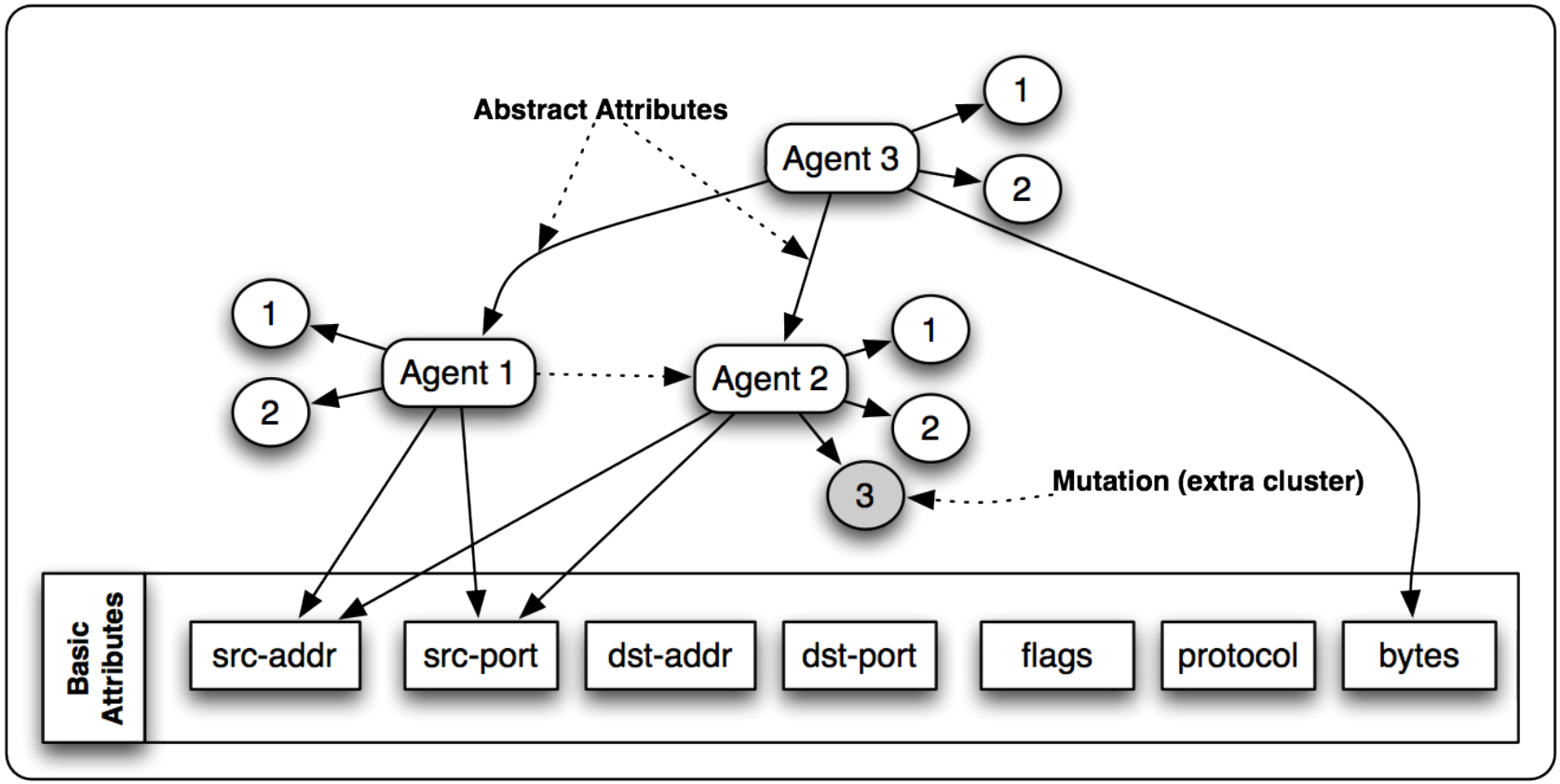
Data Processing

a) Generated Flows from the pcaps
b) Parsed the data on Logstash, and
c) Loaded the data on Elasticsearch for analysis

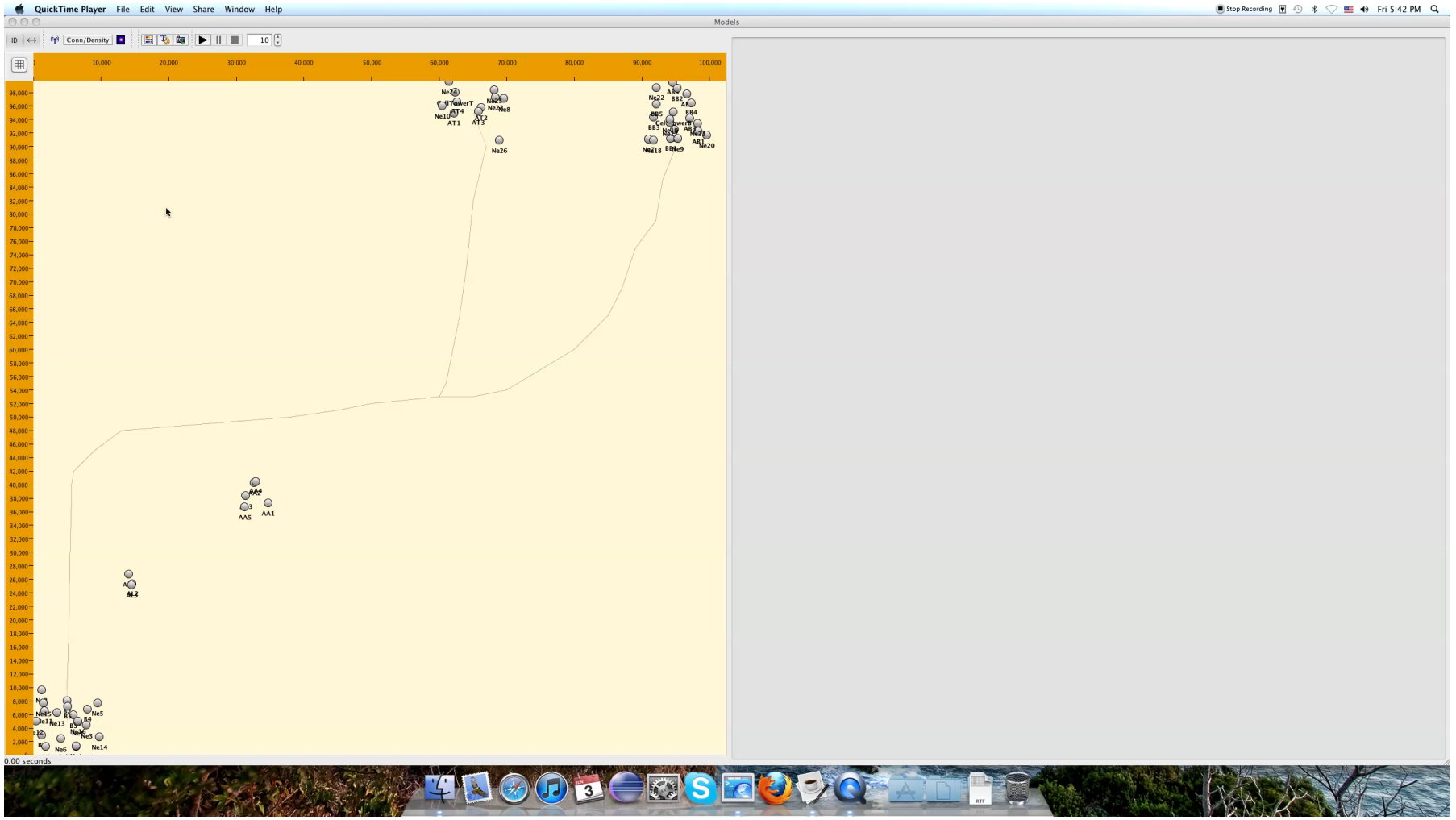
Preliminary overview (1 hour/D1)



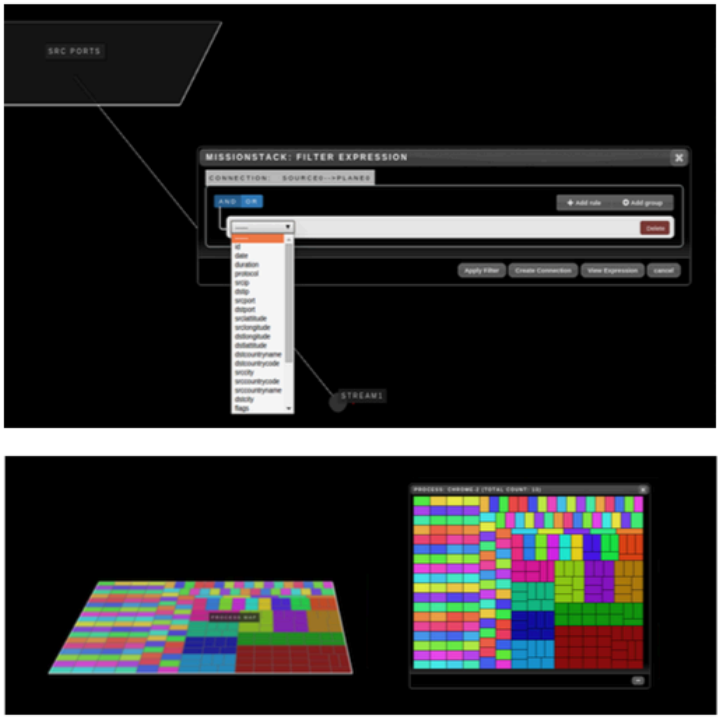
Learning Hierarchical Temporal Models

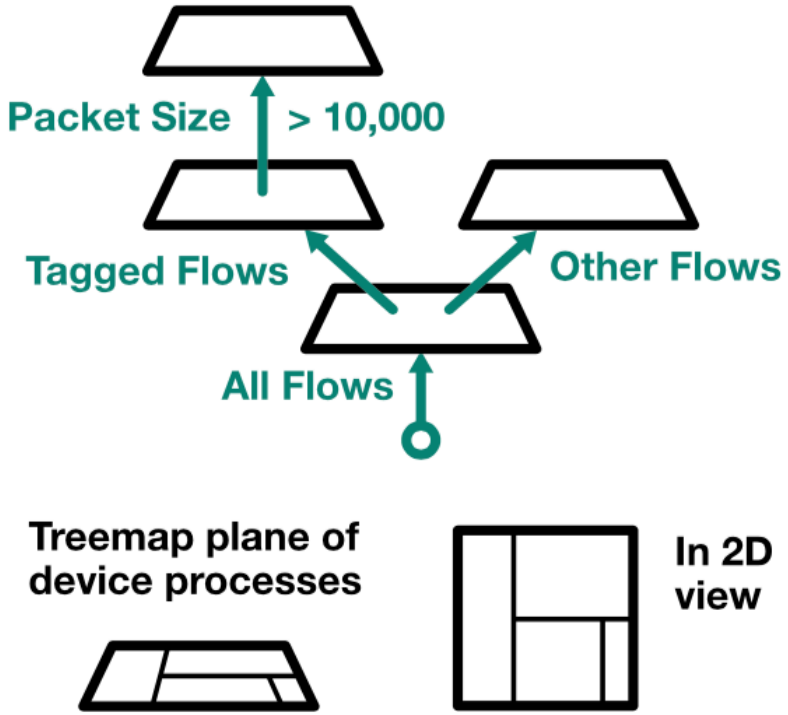


Learning Clusters of Behavior (C2) Models



Flow Visualization

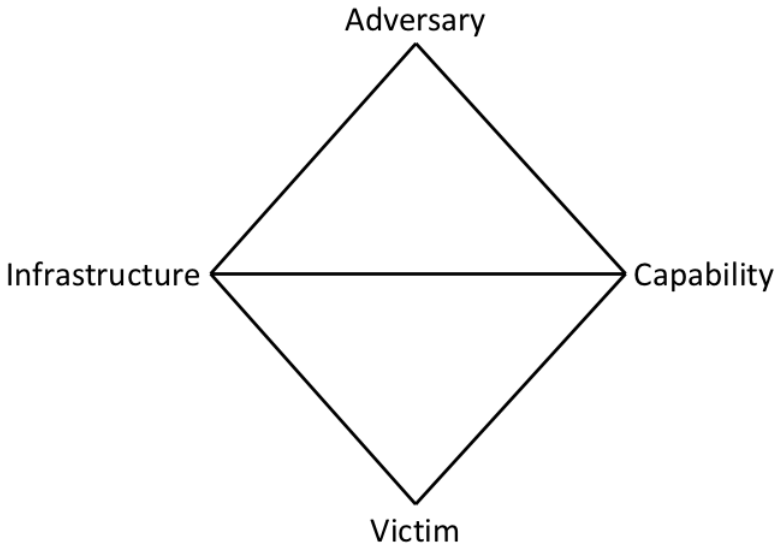


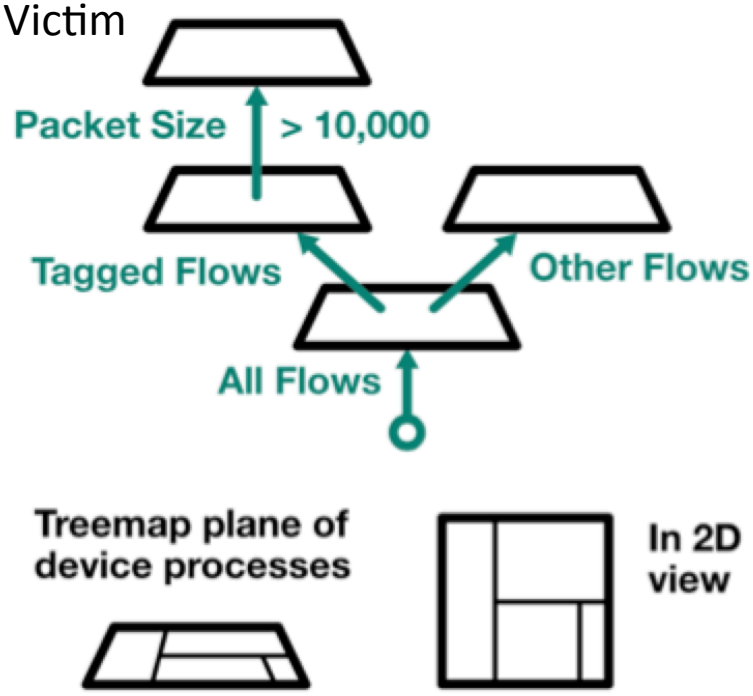


Pivoting the Diamond Model

Adversary >> Infrastructure >> Capability >> Victim

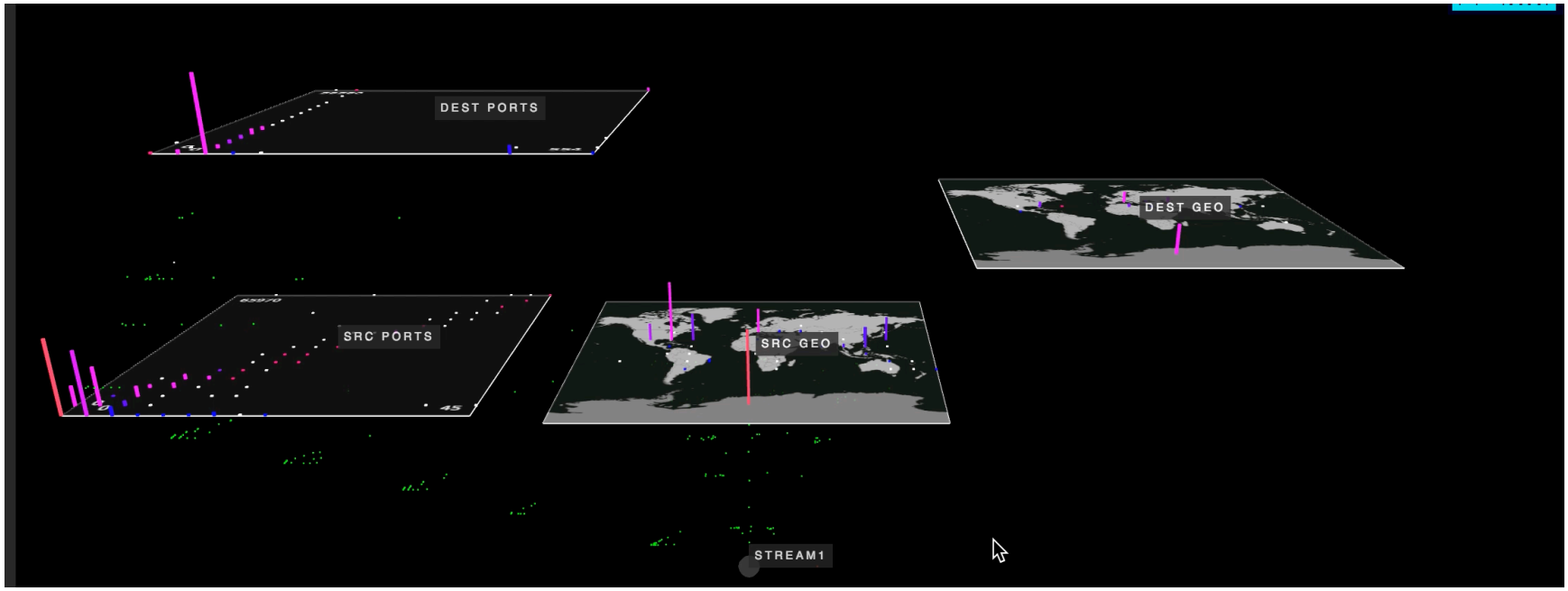
Infrastructure >> Adversary >> Capability >> Victim





Data Modifications/Enrichment

A: Allocating Geographical Positions for Data Sources
B: Identify specific threats from flows (IDS)
C: Define infrastructure and capabilities for the dataset



Progress so far…

Next Steps

- Complete the data import into the analysis framework
- Annotate the flows with indicators for "capabilities" (specific IDS events)
- Complete the visualization to allow for the interactive analysis
- Ground truth?

Marco Carvalho
mcarvalho@fit.edu
(321) 674-8767