

# Teaching Flow Analysis with Live Flow Data

*Alex Musicante, City of Pittsburgh*

*John Dwyer, Student, Carnegie Mellon University*

*Sid Faber, Adjunct Faculty, Carnegie Mellon University*



...or

# Pittsburgh's Three Rivers of Flow

*Alex Musicante, City of Pittsburgh*

*John Dwyer, Student, Carnegie Mellon University*

*Sid Faber, Adjunct Faculty, Carnegie Mellon University*





**Robert Morris University**  
nonprofit organizations - communication and information - human resources management - continuing education - doctoral programs

# Geography

**University of Pittsburgh** ★★★★★ 65  
cathedral of learning - department of medicine - department of pathology - forbes avenue - national institutes of health

**Carnegie Mellon University** ★★★★★ 84  
artificial intelligence - tepper school of business - department of psychology - mechanical engineering - software engineering institute

**Duquesne University** ★★★★★☆ 15  
speech language pathology - mary pappert school of music - occupational therapy - administration bldg - graduate school of business

**Carlow University**  
school of nursing - school of education - social services - liberal arts - degree center

**Pittsburgh Bartending School**  
alcohol management - job placement assistance - active job - training program





# About the City

- Org Structure
  - Politicians
  - IT
- Network Structure



Carnegie Mellon University  
**Heinz College**



# Partnership

- History of projects between CMU and the City
  - Heinz College
  - Information Systems & Management
  - Public Policy and Management
- “Penetration Test” project last year
  - Technical exercise
  - Policy assessment and recommendations



# Adding Flow

- Initiated discussions with the CIO
- Review & approval by City Legal, CMU Legal, others
- Volunteers installed a sensor at the primary internet connection

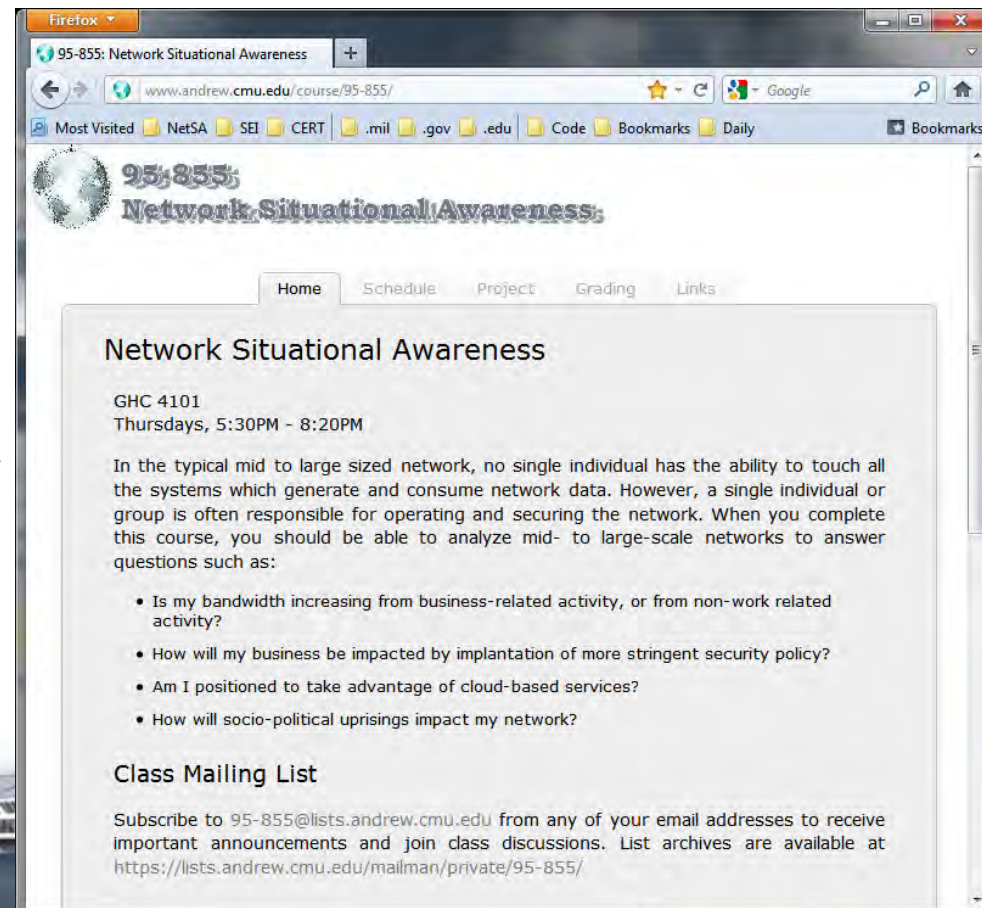


Carnegie Mellon University  
**Heinz College**



# The Class

- Network Situational Awareness class
  - <http://www.andrew.cmu.edu/course/95-855/>
  - Instructors:
    - Tim Shimeall\*
    - Sid Faber
  - Anonymized data
    - MAWI, Internet 2, CDX



The screenshot shows a Firefox browser window with the address bar displaying [www.andrew.cmu.edu/course/95-855/](http://www.andrew.cmu.edu/course/95-855/). The page title is "95-855: Network Situational Awareness". The page content includes a navigation menu with "Home", "Schedule", "Project", "Grading", and "Links". The main heading is "Network Situational Awareness". Below this, the course is identified as "GHC 4101" and "Thursdays, 5:30PM - 8:20PM". A paragraph describes the course's focus on analyzing mid- to large-scale networks. A bulleted list of questions is provided, such as "Is my bandwidth increasing from business-related activity, or from non-work related activity?". At the bottom, there is a "Class Mailing List" section with a subscription link: [95-855@lists.andrew.cmu.edu](mailto:95-855@lists.andrew.cmu.edu) and a link to the list archives: <https://lists.andrew.cmu.edu/mailman/private/95-855/>.



# The Project

- Gain Network Situational Awareness
- Provide information back to the city
- Done in the blind



Carnegie Mellon University  
**Heinz College**



CITY OF PITTSBURGH



# The Process

- Find Heavy Hitters
- Create a profile
- Eliminate bogons
- Monitor over time



# Discussions

- ACL / Least Privilege
- DNS
- Policy Validation
  - Remote Access (Gotomypc)
  - Streaming Video

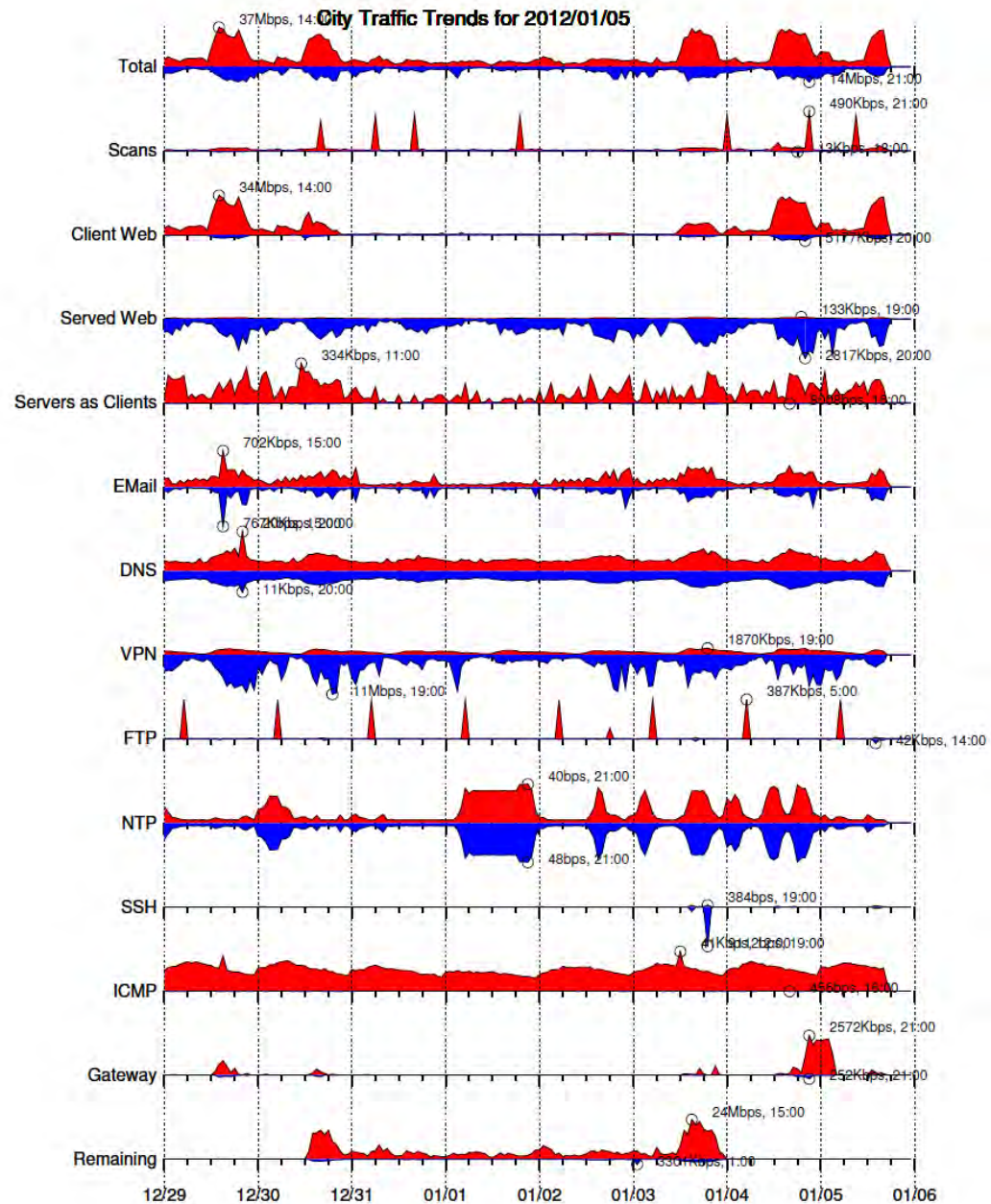


# Results

- Network Profile
  - Scans
  - Client Web, Served Web
  - Servers as Clients
  - Email
  - DNS
  - NTP
  - Etc.

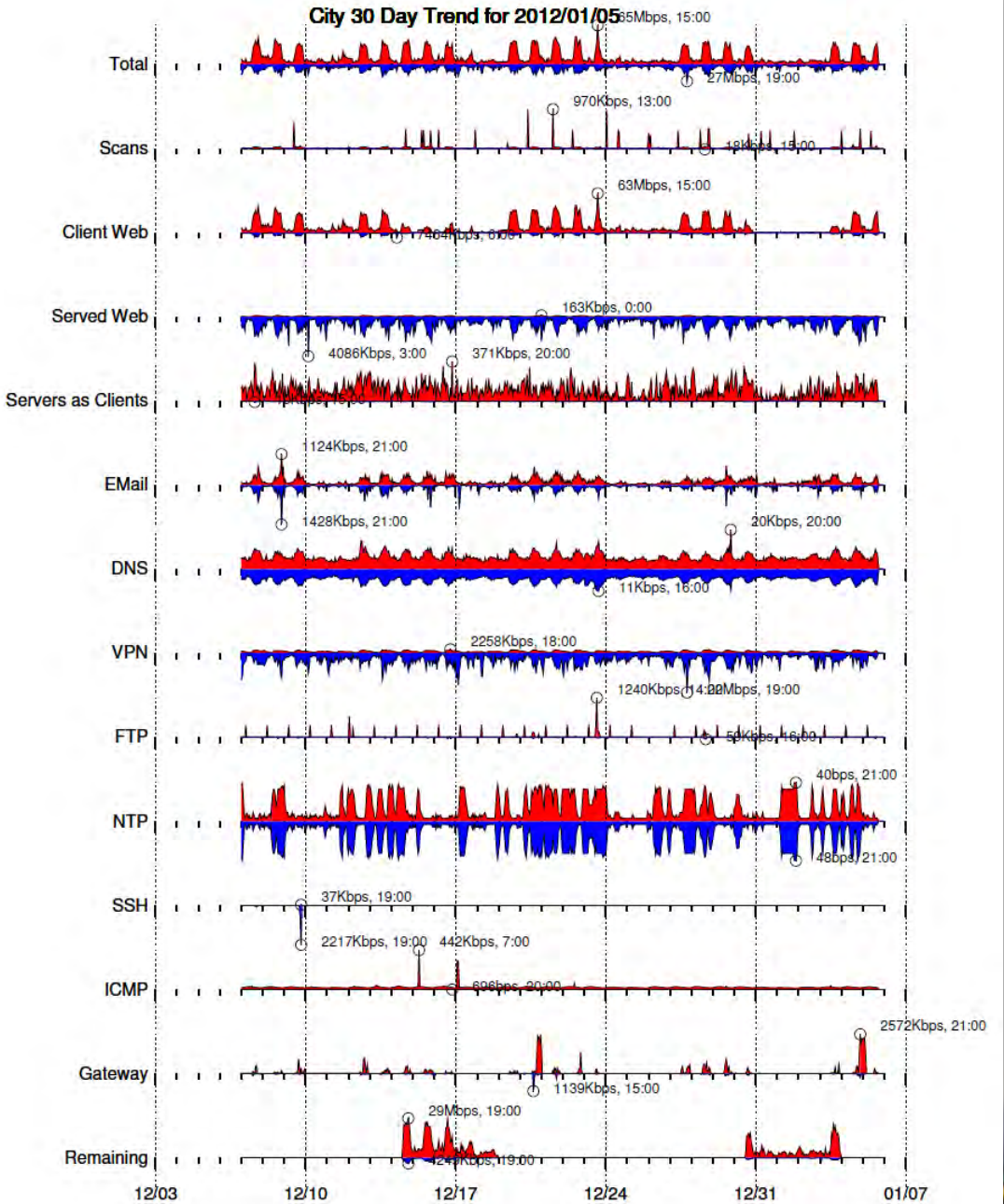
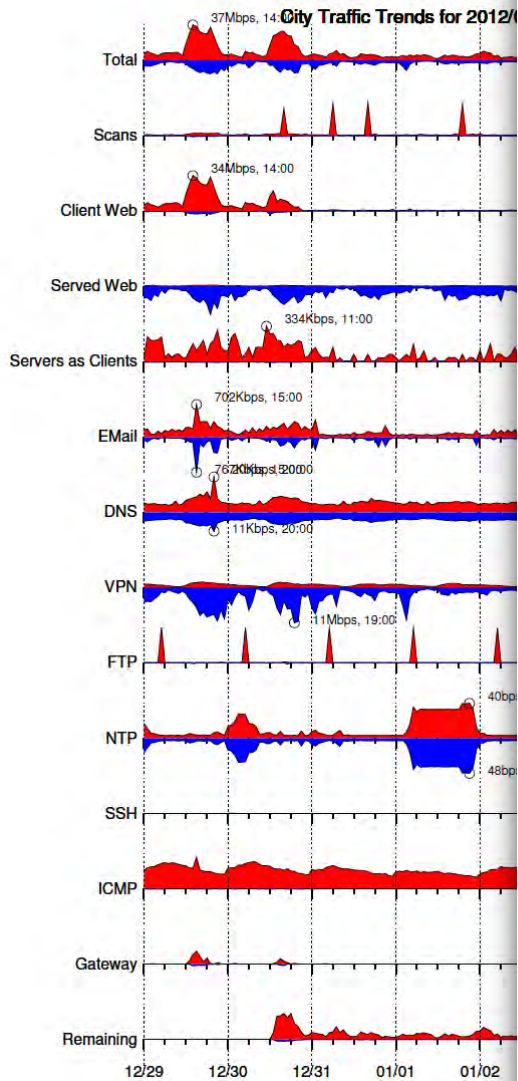






Carnegie  
He

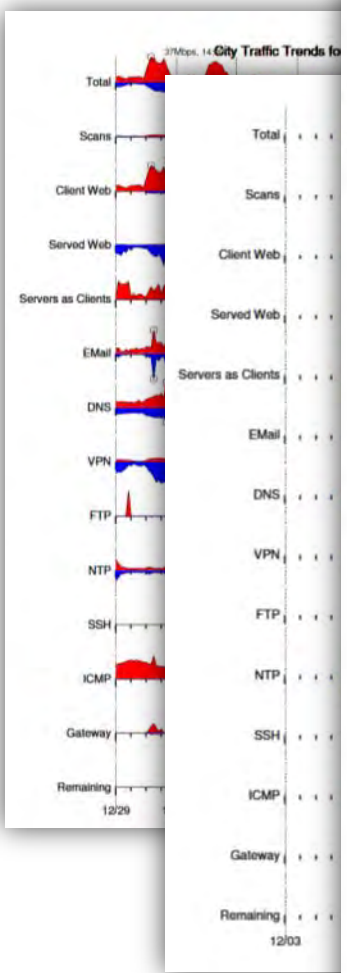
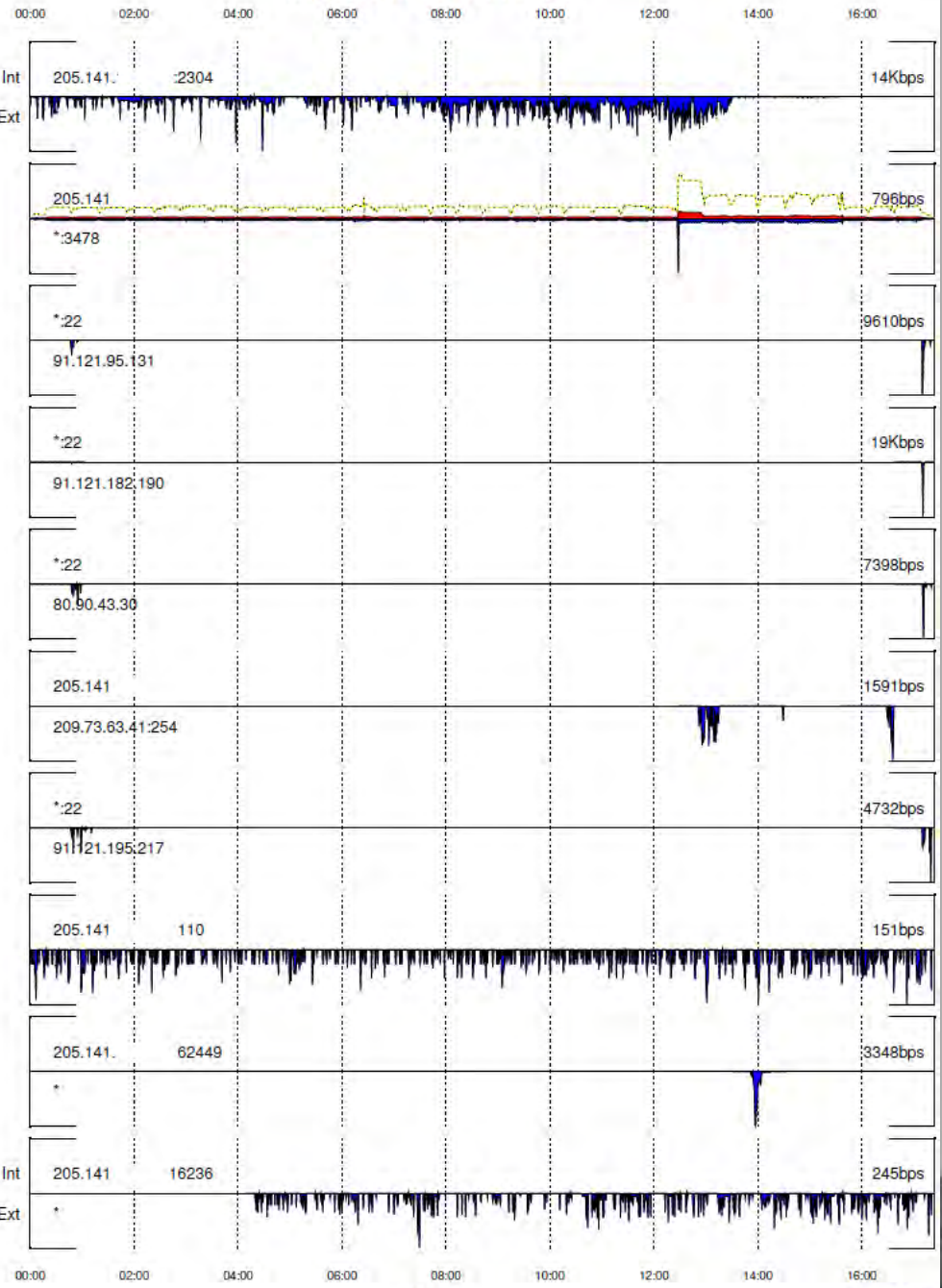




Carnegie Mellon University  
Heinz College



# Unprofiled Traffic for 2012/01/05





# Shameful Advertisement: Prism

The screenshot shows a Firefox browser window displaying the CERT NetSA Security Suite website. The browser's address bar shows the URL `tools.netsa.cert.org`. The website header includes the Software Engineering Institute (SEI) and Carnegie Mellon University logos, along with the title "CERT NetSA Security Suite" and the subtitle "Monitoring for Large-Scale Networks".

The main content area is divided into several sections:

- Projects:** A list of project versions including Analysis Pipeline 3.0.0, fixbuf 1.1.1, IPA 0.5.2, iSiLK 0.3.3, netsa-python 1.3, Rayon 1.3.3, SiLK 2.4.5, and YAF 2.1.2.
- Scripts:** A section containing a link for "Prism 1.1", which is circled in red in the image.
- Links:** A list of resources including Online Training, Live CD, Wiki, Tooltips, and Defunct Projects.
- Featured Projects:** Three highlighted boxes for SiLK 2.4.5, YAF 2.1.2, and fixbuf 1.1.1, each with a "Download Now" link and a brief description.

The "Featured Projects" section contains the following details:

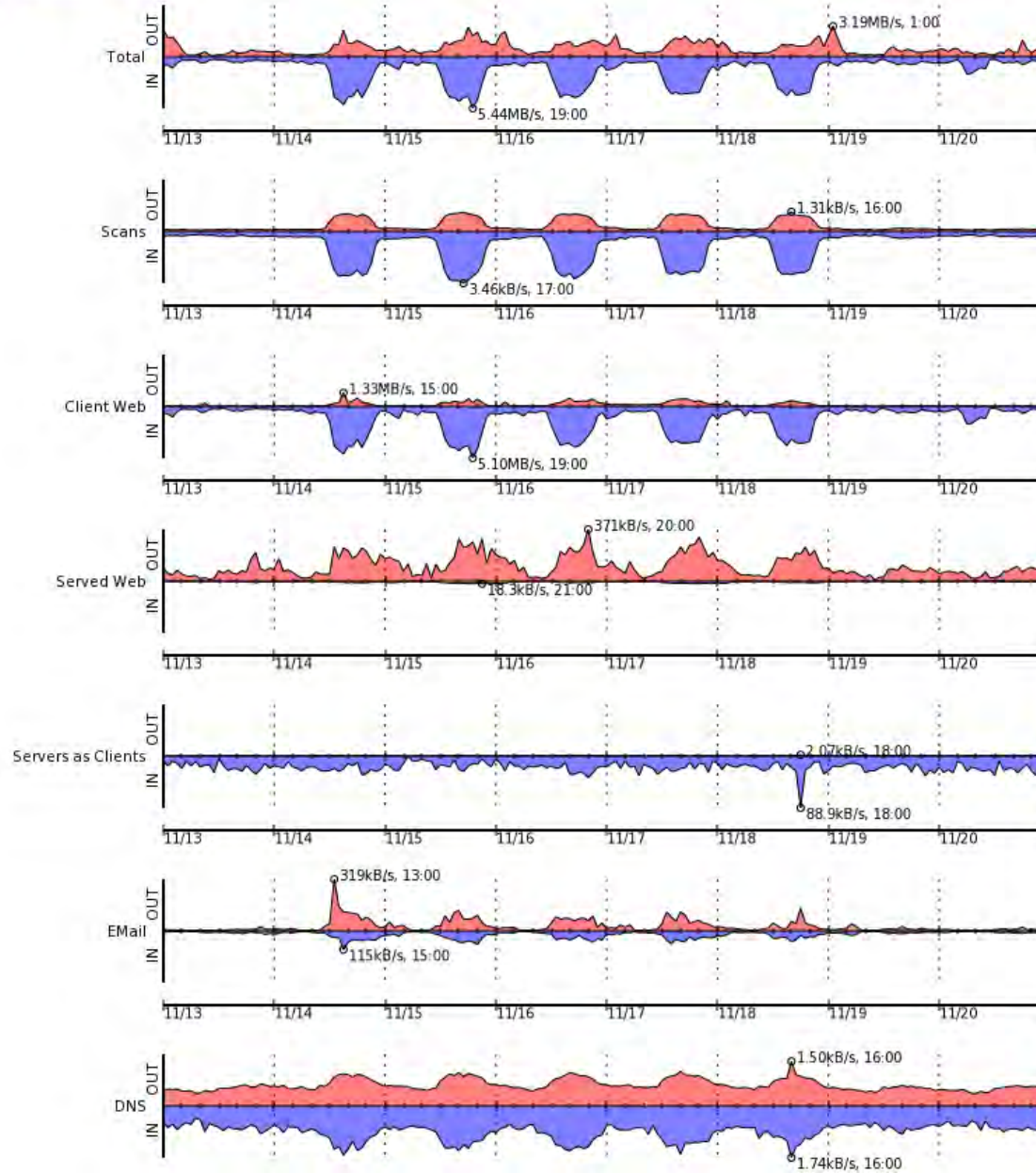
- SiLK 2.4.5:** The System for Internet Level Knowledge (SiLK) is an efficient network flow collection and storage infrastructure that will accept flow data from a variety of sensors. SiLK also provides a suite of efficient command-line tools for analysis.
- YAF 2.1.2:** Yet Another Flow Sensor (YAF) processes packet data into bidirectional flow records that can be used as input to an IPFIX Collecting Process. YAF's output can be used with the NetsA Aggregated Flow (NAF) toolchain and the SiLK tools.
- fixbuf 1.1.1:** The fixbuf library provides a set of functions for processing the IPFIX protocol message format. Using fixbuf, developers can build IPFIX Collecting and Exporting Processes.



# Traffic Volume by Port/Service (bytes)

mB/s =  $10^{-3}$  bytes per second  
 kB/s =  $10^3$  bytes per second  
 MB/s =  $10^6$  bytes per second  
 GB/s =  $10^9$  bytes per second

bytes [packets](#) [flows](#)



# Instructor Comments

- Network Situational Awareness:
  - Perceive: Network flow sensor
  - Comprehend: Network profile, leftovers
  - Project: What does this mean to me?





# Instructor Comments (2)

- All packets are innocent until proven guilty
  - Profile by country
  - Scan traffic, inbound traffic



Carnegie Mellon University  
**Heinz College**



CITY OF PITTSBURGH



# City Comments

- Leveraging university, Limited resources
- External validation
  - Support for external auditors



Carnegie Mellon University  
**Heinz College**



CITY OF PITTSBURGH

# Student Comments

- Initial impression: too much data
- Dividing traffic led to identifying patterns
- Couldn't really be done with full packet data



Carnegie Mellon University  
**Heinz College**



CITY OF PITTSBURGH



# Future

- Improve the sensor
  - Instrument the cold spare
  - Instrument internally
  - Add metadata
- Add a security focus
- Add a geopolitical focus



# Thank You

*Alex Musicante, City of Pittsburgh*

*John Dwyer, Student, Carnegie Mellon University*

*Sid Faber, Adjunct Faculty, Carnegie Mellon University*

