

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

Carnegie Mellon University

HeinzCollege

PITTSBURGH



...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







About the City

- Org Structure
 - Politicians
 - IT
- Network Structure



Carnegie Mellon University
HeinzCollege



CITY OF PITTSBURGH

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



Carnegie Mellon University
HeinzCollege



Adding Flow

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



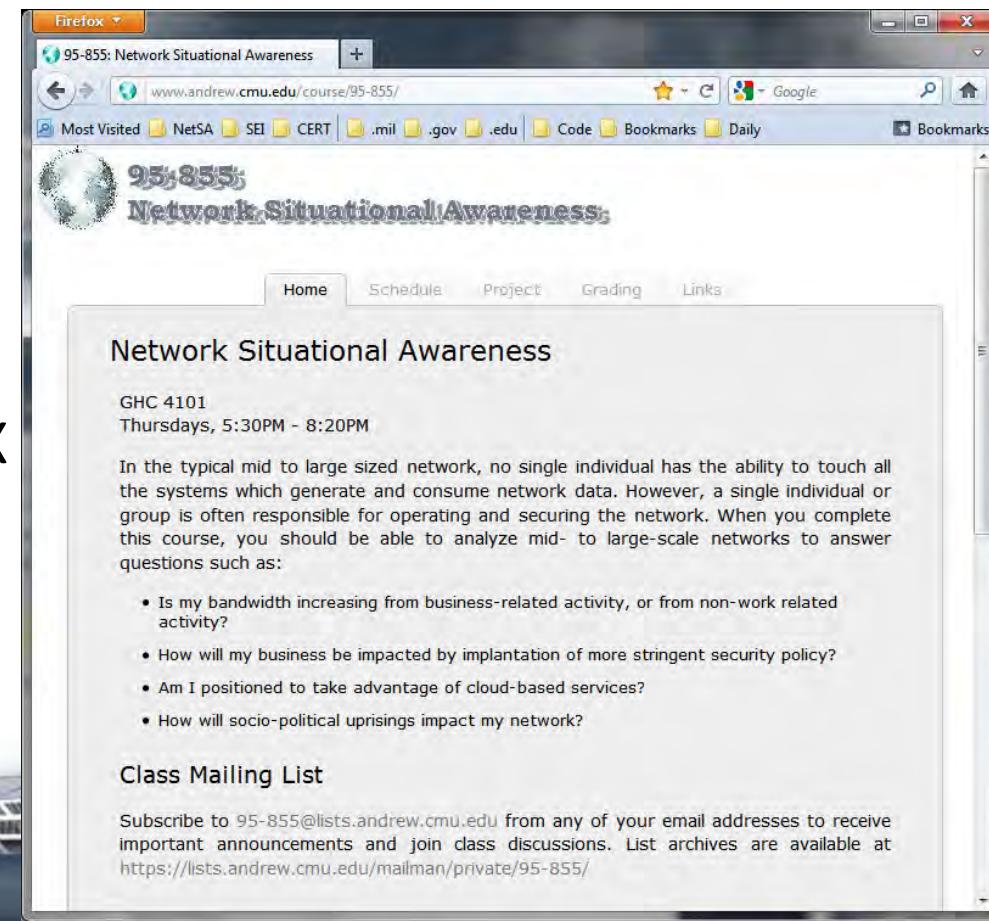
Carnegie Mellon University
HeinzCollege



CITY OF PITTSBURGH

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 title bar "95-855: Network Situational Awareness". The address bar displays the URL "www.andrew.cmu.edu/course/95-855/". The page content is as follows:

95:855: Network Situational Awareness

Home Schedule Project Grading Links

Network Situational Awareness

GHC 4101
Thursdays, 5:30PM - 8:20PM

In the typical mid to large sized network, no single individual has the ability to touch all the systems which generate and consume network data. However, a single individual or group is often responsible for operating and securing the network. When you complete this course, you should be able to analyze mid- to large-scale networks to answer questions such as:

- Is my bandwidth increasing from business-related activity, or from non-work related activity?
- How will my business be impacted by implantation of more stringent security policy?
- Am I positioned to take advantage of cloud-based services?
- How will socio-political uprisings impact my network?

Class Mailing List

Subscribe to 95-855@lists.andrew.cmu.edu from any of your email addresses to receive important announcements and join class discussions. List archives are available at <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



Carnegie Mellon University
HeinzCollege



CITY OF PITTSBURGH



Discussions

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



Carnegie Mellon University
HeinzCollege



CITY OF PITTSBURGH



Results

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



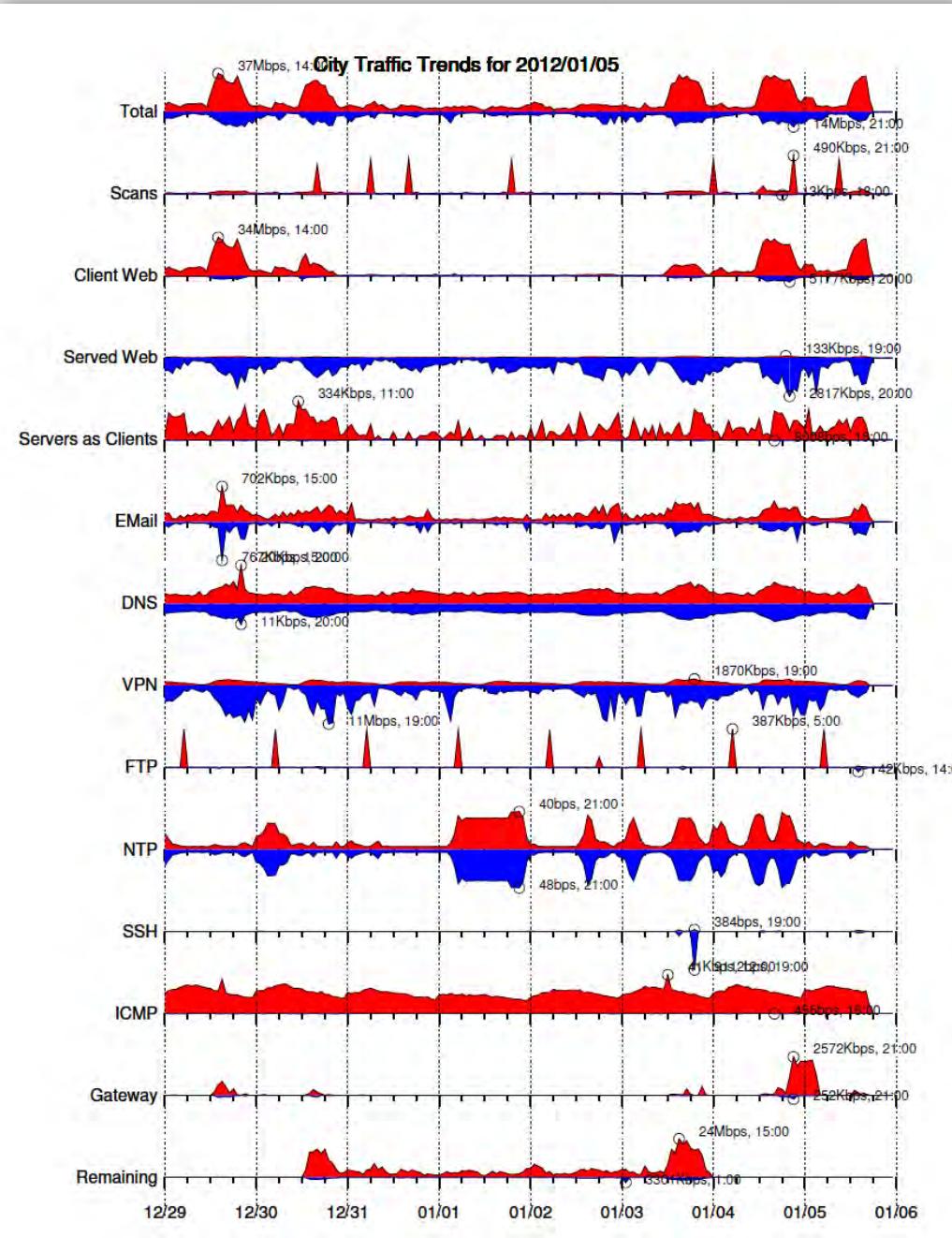
Carnegie Mellon University
HeinzCollege

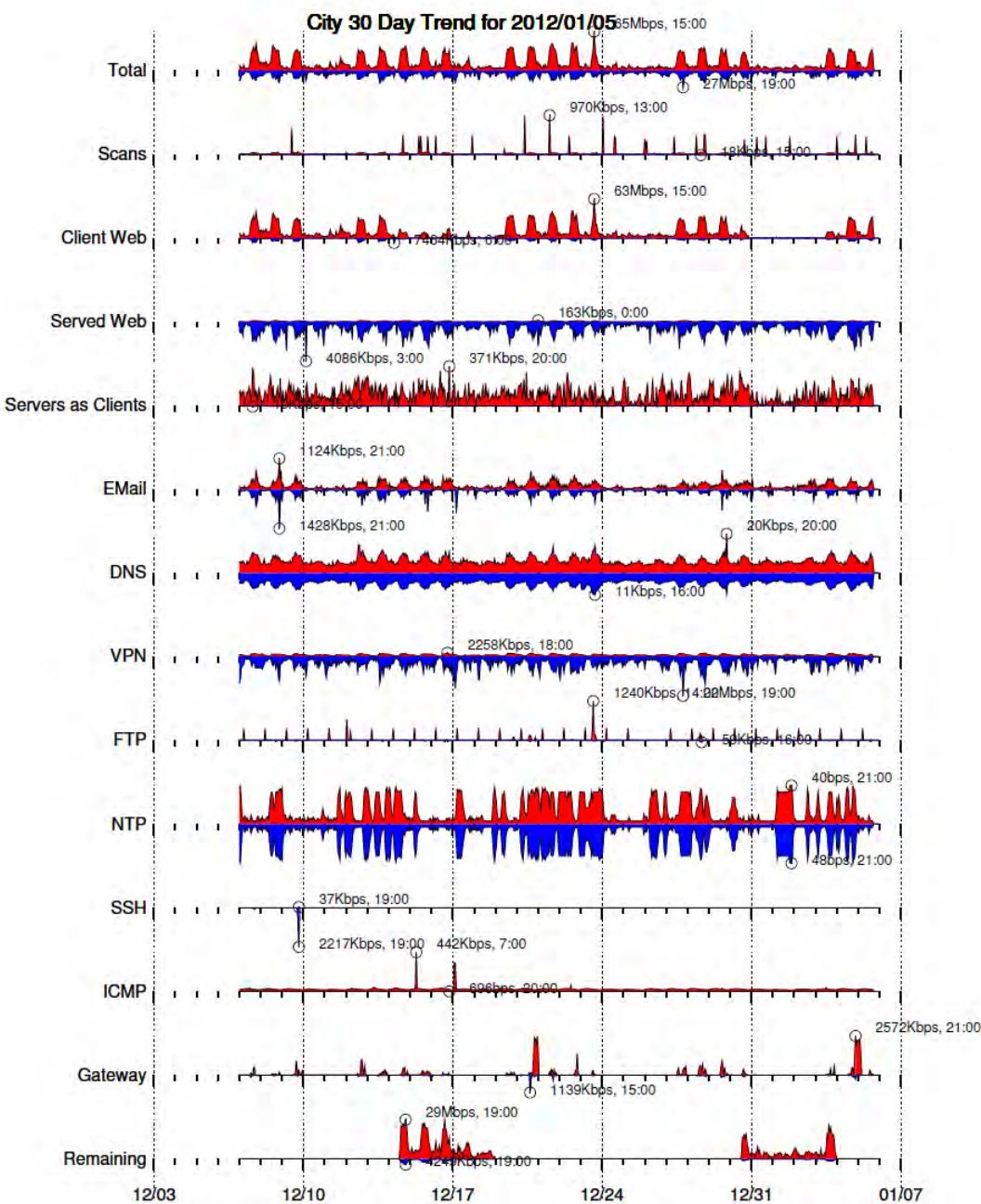
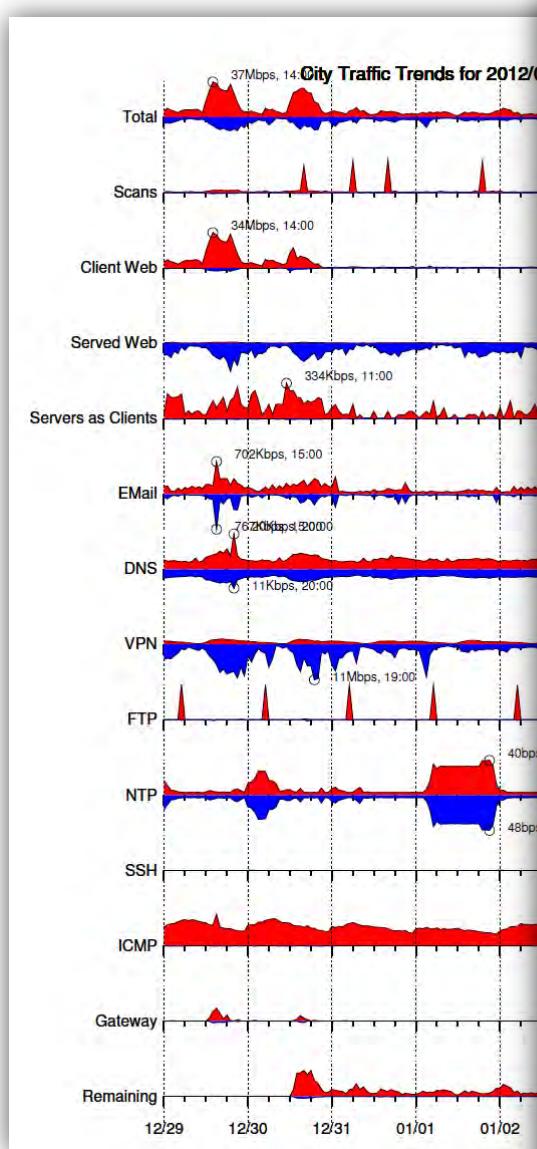


CITY OF PITTSBURGH



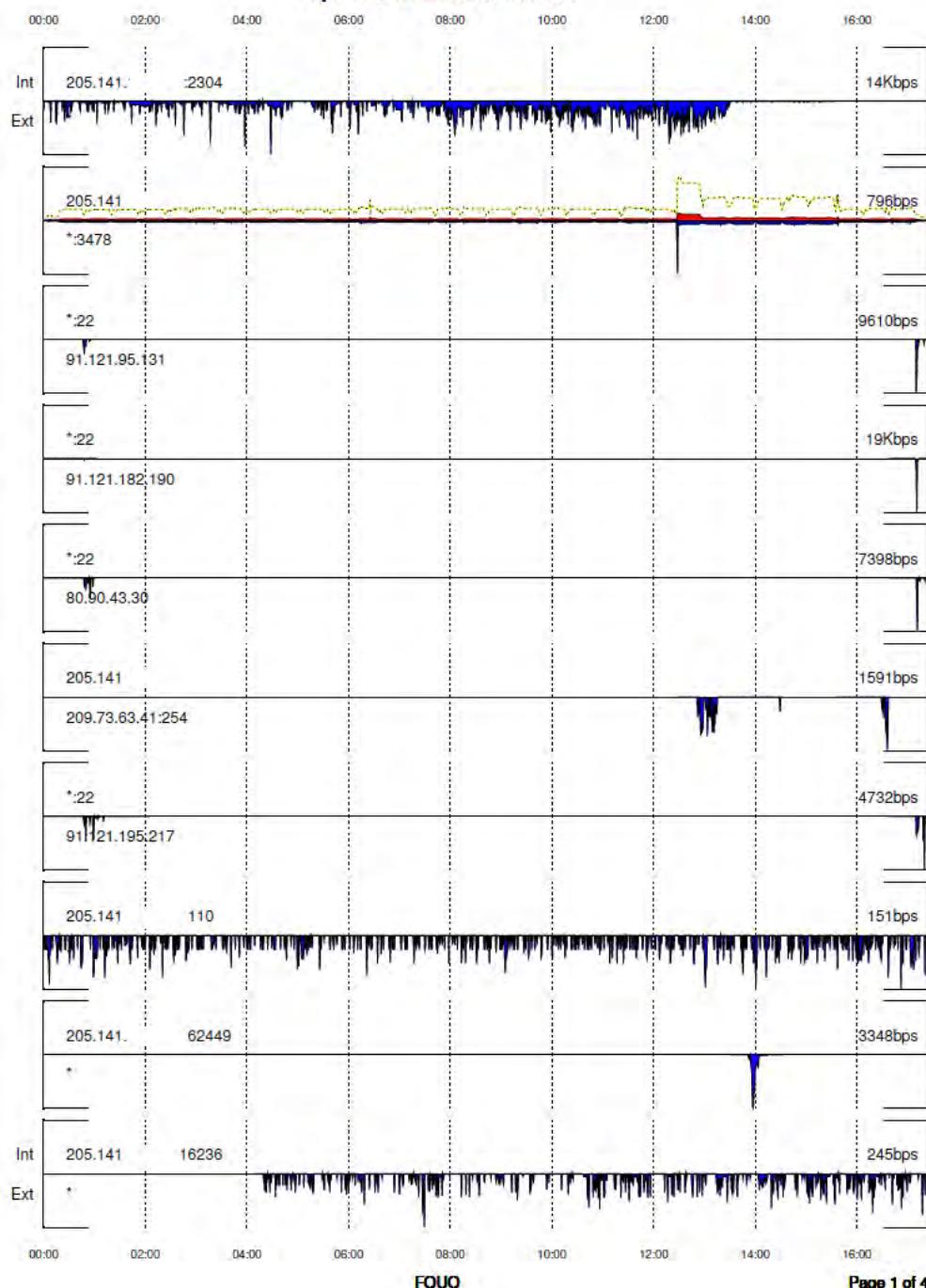
Carne
He





Carnegie Mellon University
Heinz College

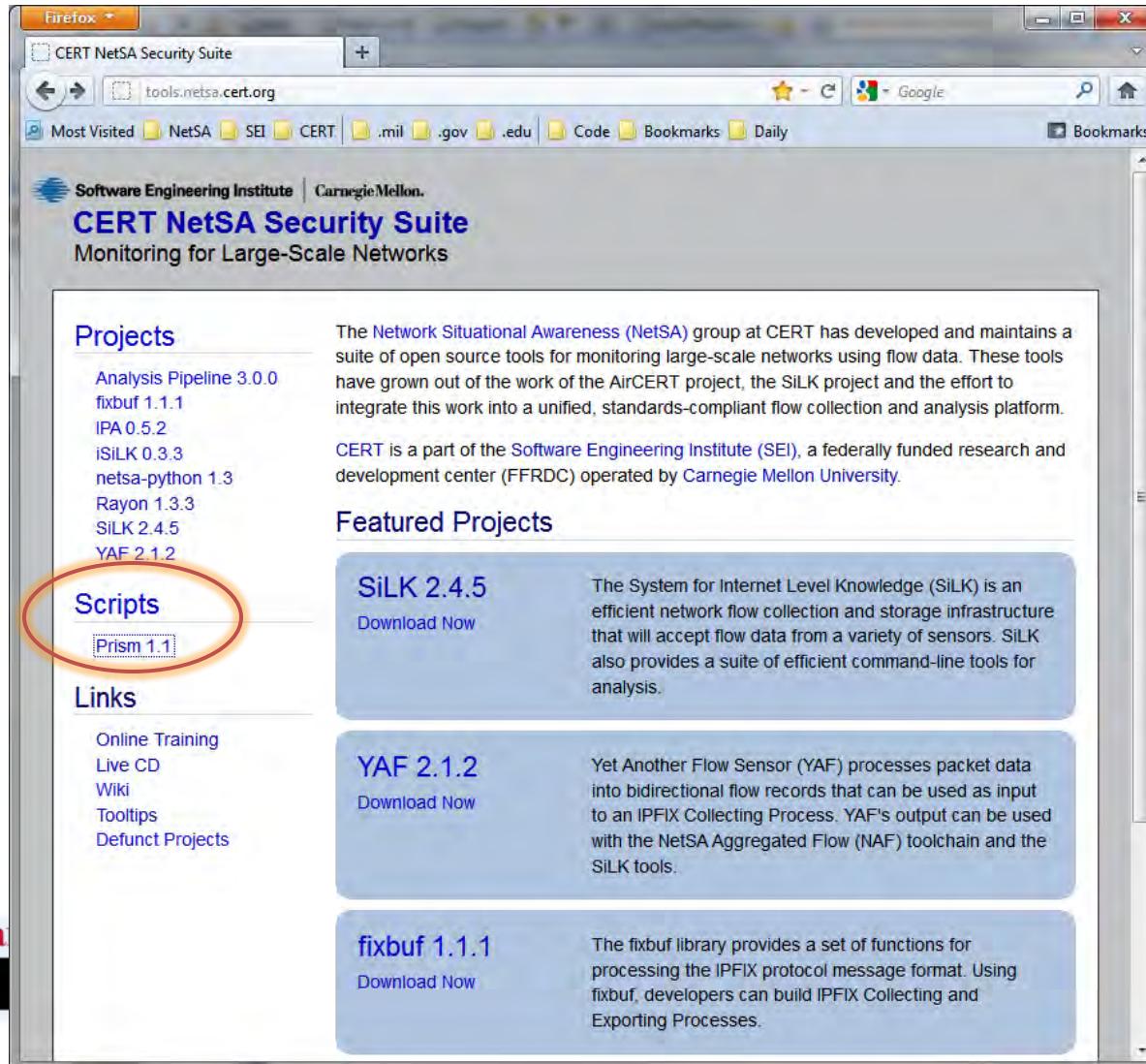
Unprofiled Traffic for 2012/01/05



Carnegie
Hein



Shameful Advertisement: Prism



The Network Situational Awareness (NetSA) group at CERT has developed and maintains a suite of open source tools for monitoring large-scale networks using flow data. These tools have grown out of the work of the AirCERT project, the SiLK project and the effort to integrate this work into a unified, standards-compliant flow collection and analysis platform.

CERT is a part of the Software Engineering Institute (SEI), a federally funded research and development center (FFRDC) operated by Carnegie Mellon University.

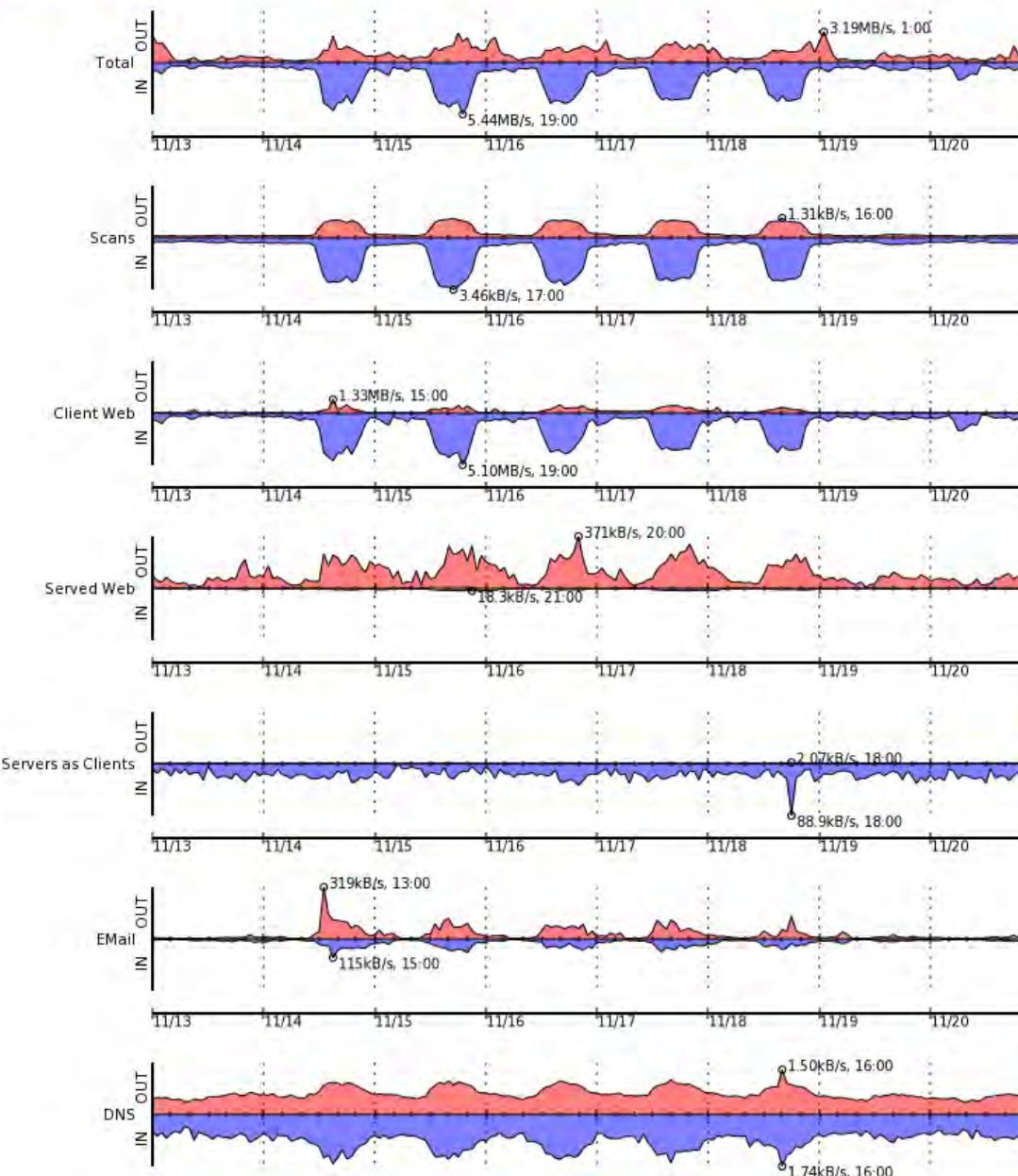
Featured Projects

- SiLK 2.4.5**
Download Now
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**
Download Now
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**
Download Now
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





City Comments

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





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
HeinzCollege



CITY OF PITTSBURGH

Future

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



Carnegie Mellon University
Heinz College



CITY OF PITTSBURGH

Thank You

Alex Musicante, City of Pittsburgh

John Dwyer, Student, Carnegie Mellon University

Sid Faber, Adjunct Faculty, Carnegie Mellon University

Carnegie Mellon University

HeinzCollege

PITTSBURGH