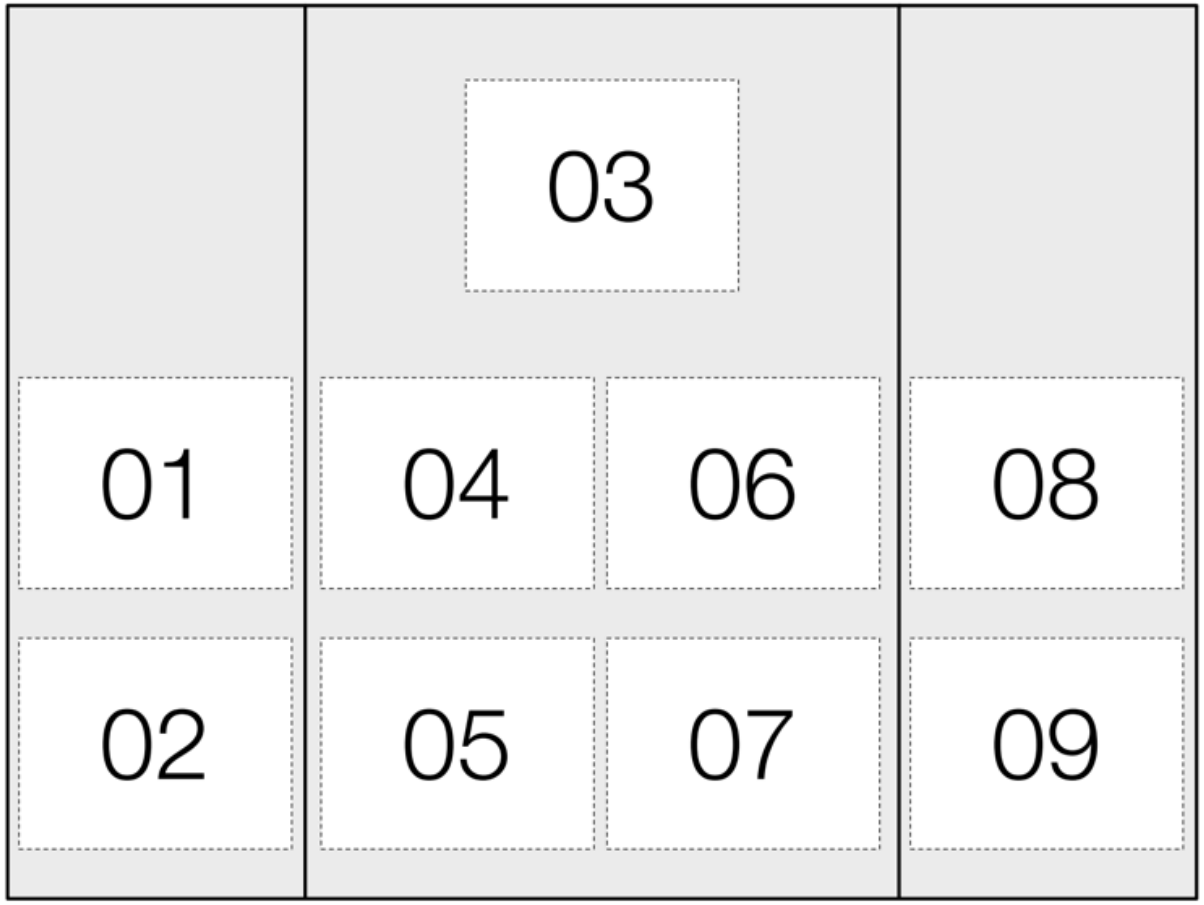


delete the number before printing out！ ！ ！

Visualizations of Dell SonicWALL firewall data

This project is for CS690 Master Project course during the semester fall 2014.

We use primarily d3.js and p5.js to build stand-alone visualizations of Dell SonicWALL firewall data that could be integrated into their Dell SonicWALL Analyzer product.

Team members: Wanzhang Sheng  Kaiming Yang 

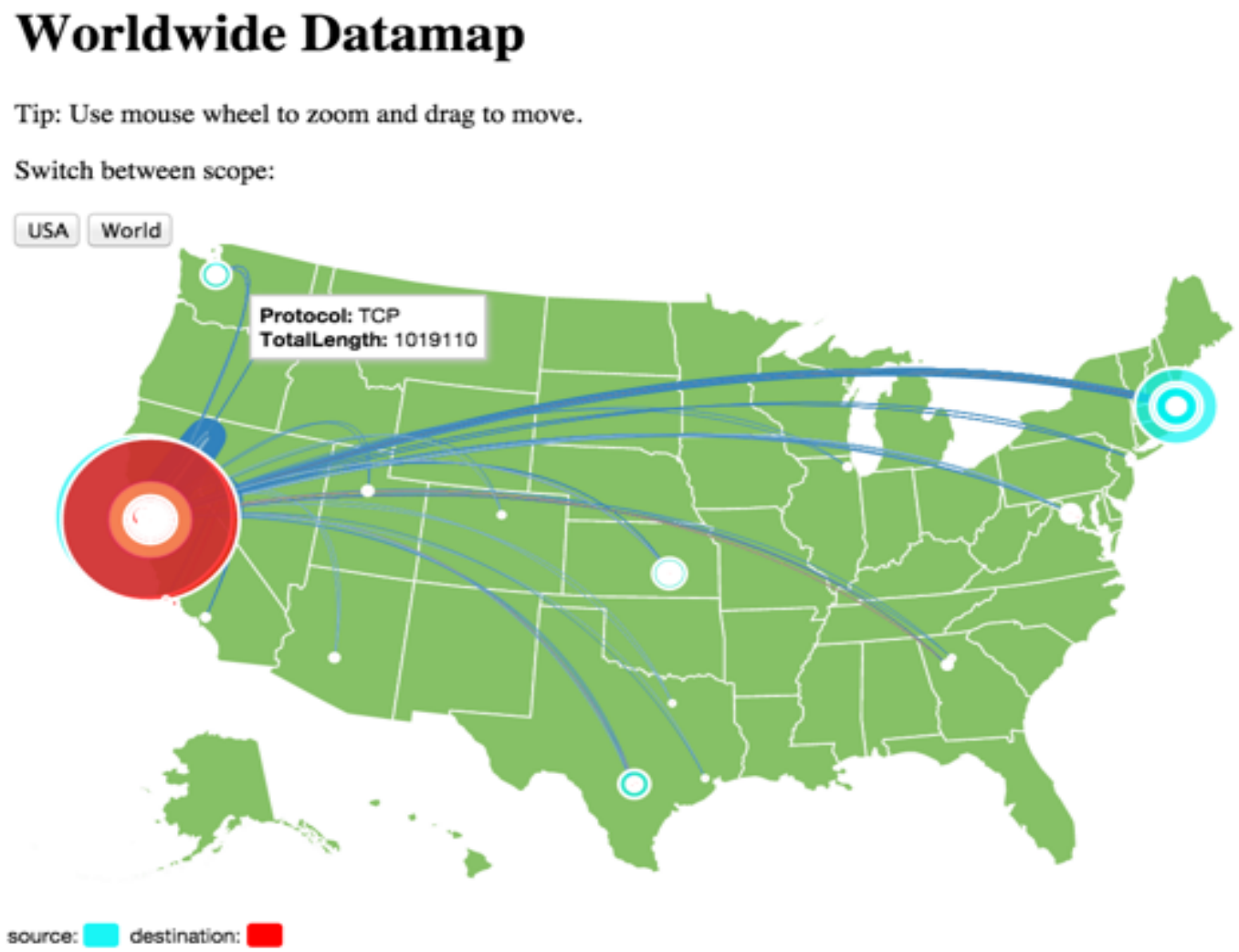
Jie Gao  Xi Han 

We build a website shell using Bootstrap 3.0, sjengle.cs.usfca.edu/cs690-sonicwall/

Sponsors: Sophie Engle, University of San Francisco

Carrie Gates, Dell Research

Our Visualization



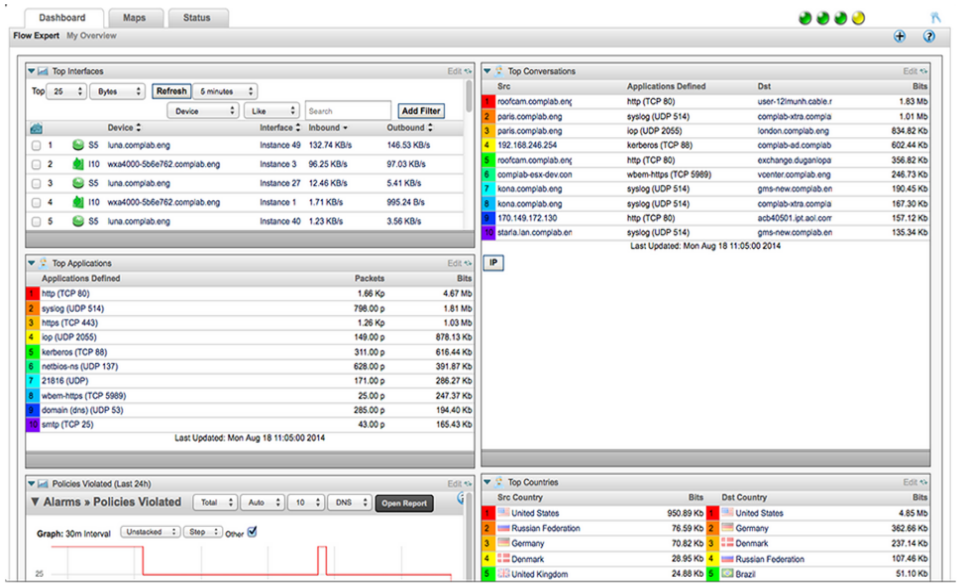
Dataset:

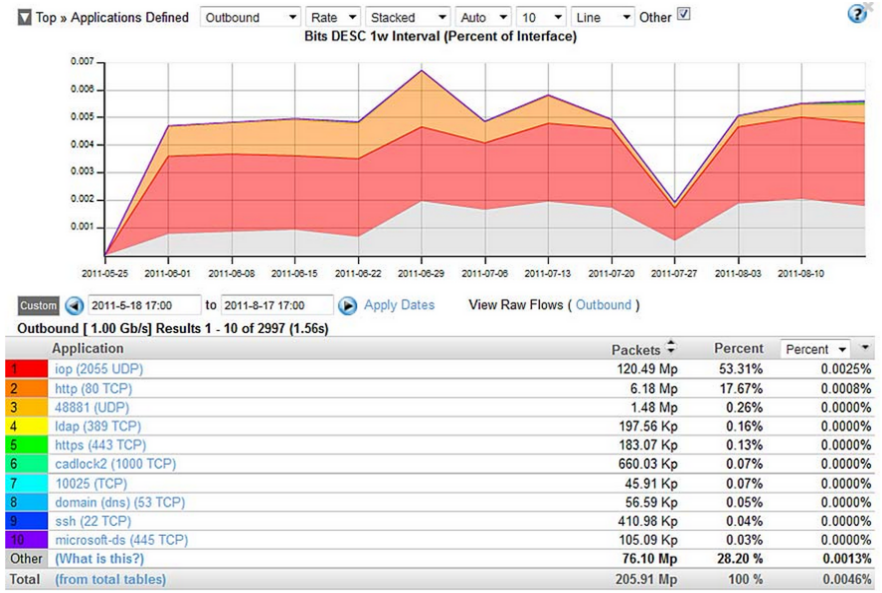
{"Source":"184.84.222.144","Destination":"24.6.173.220","Protocol":"TCP","TotalLength":4769916,"SourceCity":"Redwood City","DestinationCity":"Milpitas","SourceCountry":"United States","DestinationCountry":"United States","SourceLatitude":"37.4852","SourceLongitude":"-122.2364","DestinationLatitude":"37.4404","DestinationLongitude":"-121.8705"}

Dell SonicWALL's products

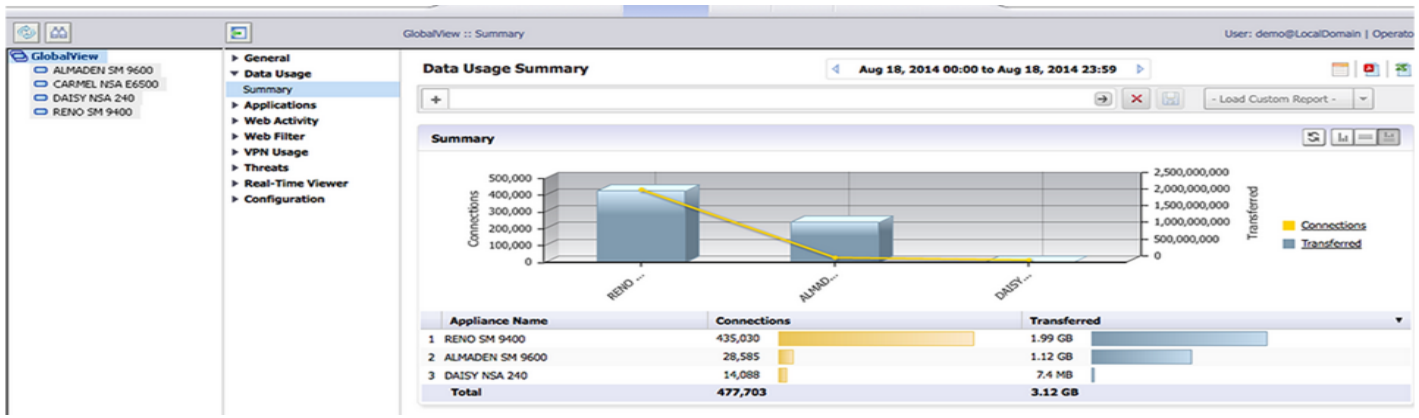
Dell SonicWALL Scrutinizer's Dashboard

Our goal is to build visualizations to be integrated into these products:



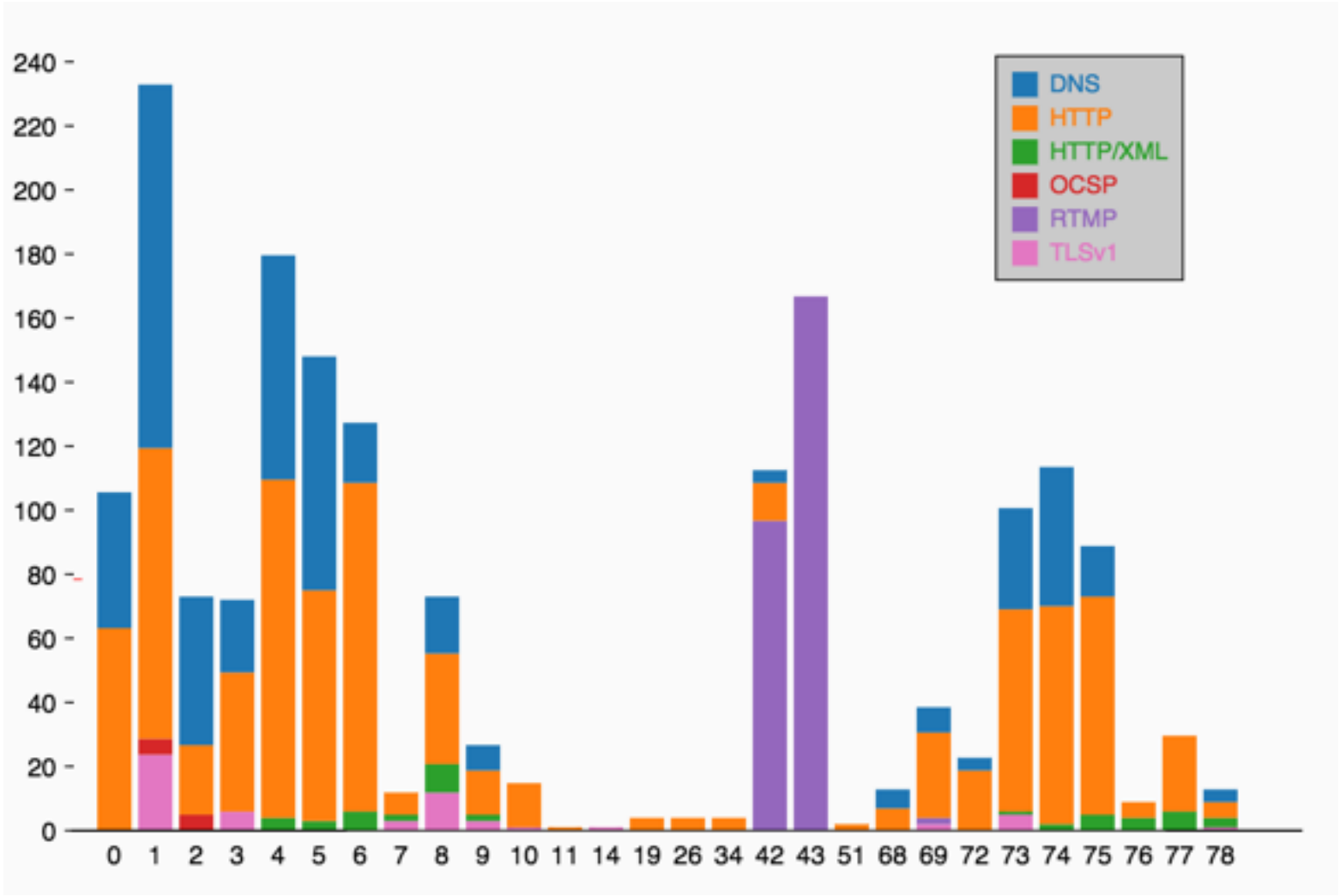


Dell SonicWALL Analyzer

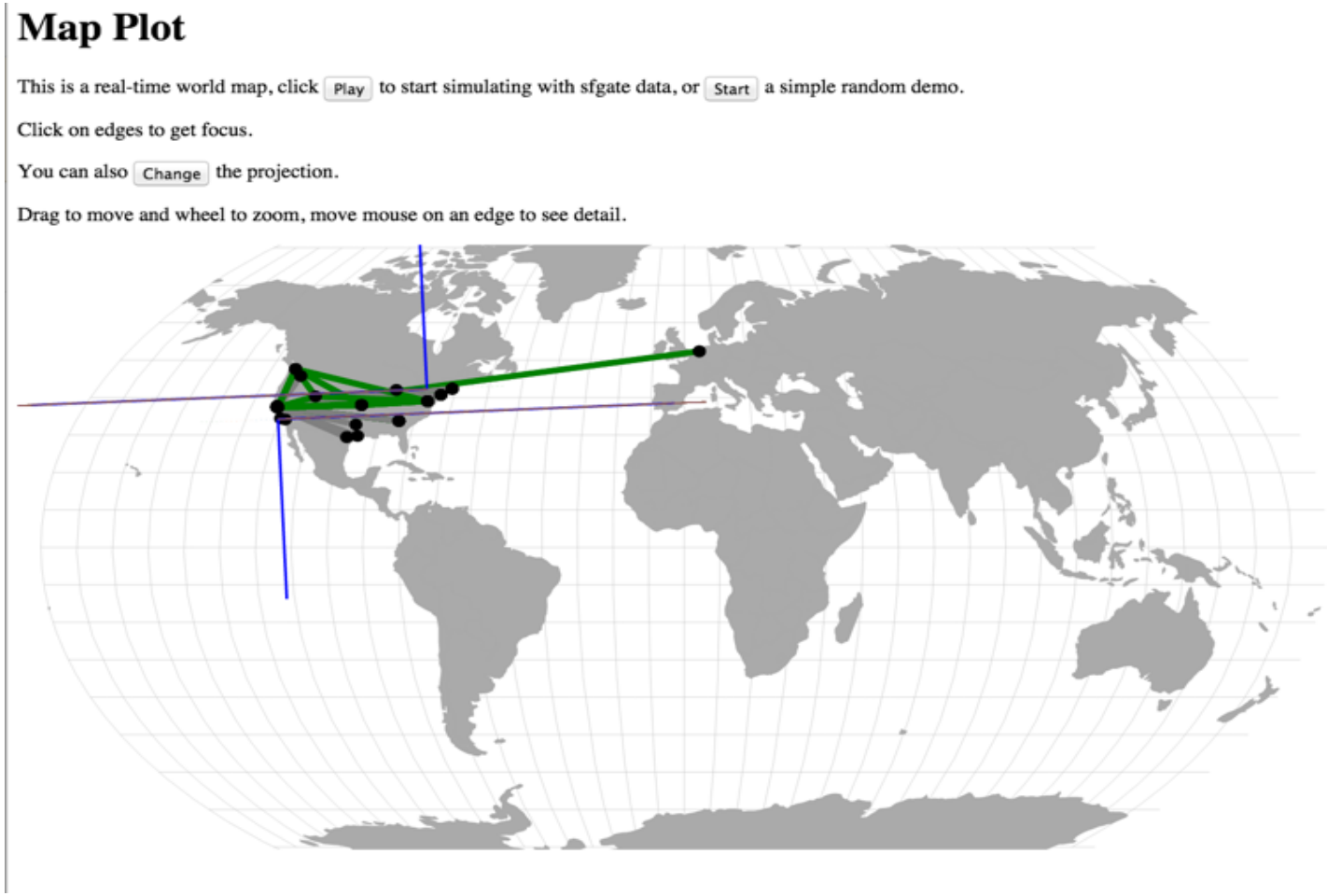


Our Visualizations

Different protocol usage (P5.js)



Our Visualizations (05)

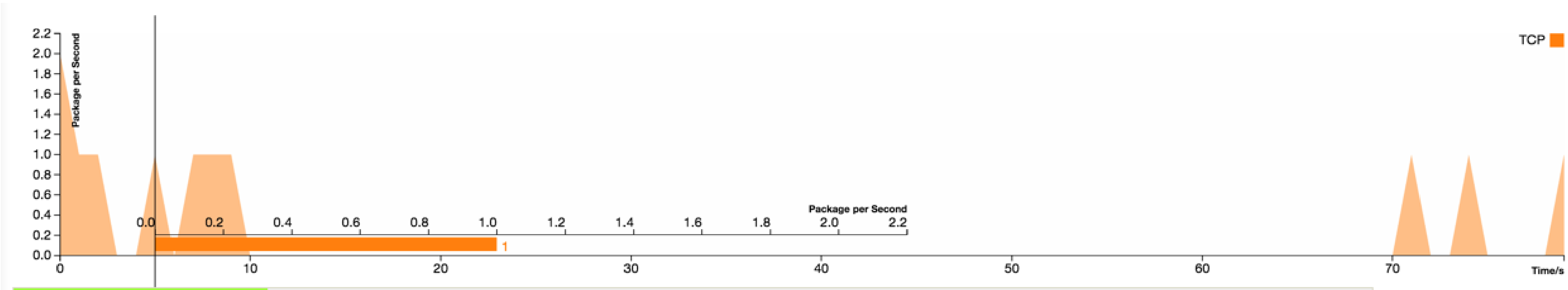


Dataset

No	Time	Source	Destination	Protocol	Length	Info
1	0	24.6.173.220	75.75.75.75	DNS	74	Standard query 0x5285 A www.sfgate.com

IP	Country Code	Country	Region Code	Region	City	Zip Code	Latitude	Longitutde	Area Code	Metro
24.6.173.220	US	United States	CA	California	Milpitas	95035	37.4404	-121.871	807	408

Our Visualizations (04)



Source	SourceCountry	Destination	DestinationCountry	Protocol	Bytes over Time	Total bytes
208.93.137.180	United States, San Jose	c-24-6-173-220.hsd1.ca.comcast.net	United States, Milpitas	TCP		
208.93.137.180	United States, San Jose	c-24-6-173-220.hsd1.ca.comcast.net	United States, Milpitas	HTTP		
67.192.92.227	United States, San Antonio	c-24-6-173-220.hsd1.ca.comcast.net	United States, Milpitas	TCP		
74.217.78.141	United States, San Mateo	c-24-6-173-220.hsd1.ca.comcast.net	United States, Milpitas	TCP		
93.184.216.169	United States,	c-24-6-173-220.hsd1.ca.comcast.net	United States, Milpitas	TCP		
93.184.216.229	United States,	c-24-6-173-220.hsd1.ca.comcast.net	United States, Milpitas	TCP		
a184-84-222-129.deploy.static.akamaitechnologies.com	United States, Redwood City	c-24-6-173-220.hsd1.ca.comcast.net	United States, Milpitas	TCP		
a184-84-222-144.deploy.static.akamaitechnologies.com	United States, Redwood City	c-24-6-173-220.hsd1.ca.comcast.net	United States, Milpitas	TCP		
a184-84-222-89.deploy.static.akamaitechnologies.com	United States, Redwood City	c-24-6-173-220.hsd1.ca.comcast.net	United States, Milpitas	TCP		
a23-62-228-24.deploy.static.akamaitechnologies.com	United States, Cambridge	c-24-6-173-220.hsd1.ca.comcast.net	United States, Milpitas	TCP		
a23-62-228-27.deploy.static.akamaitechnologies.com	United States, Cambridge	c-24-6-173-220.hsd1.ca.comcast.net	United States, Milpitas	TCP		
a96-17-110-102.deploy.akamaitechnologies.com	United States, Cambridge	c-24-6-173-220.hsd1.ca.comcast.net	United States, Milpitas	TCP		
a96-17-110-102.deploy.akamaitechnologies.com	United States, Cambridge	c-24-6-173-220.hsd1.ca.comcast.net	United States, Milpitas	RTMP		

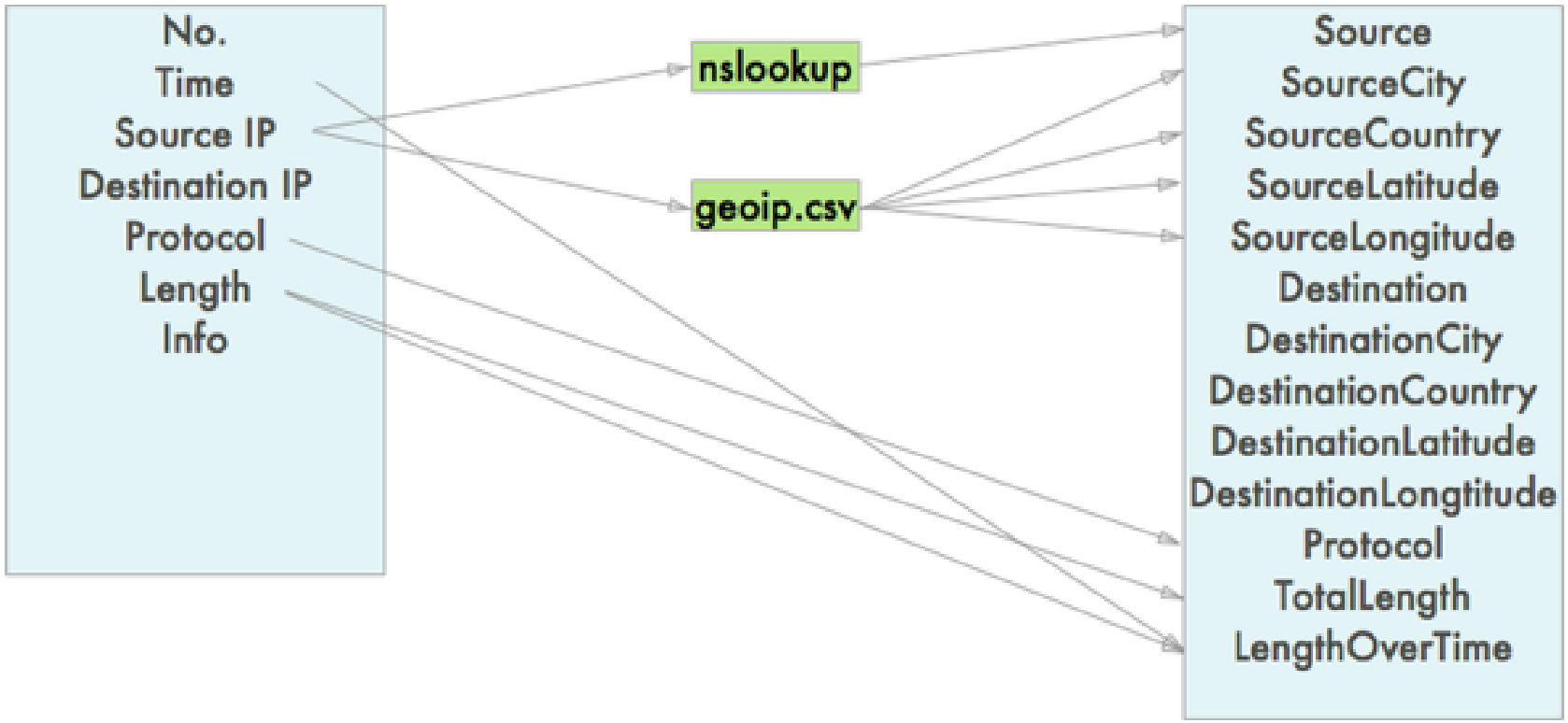
Dataset:

{"Time":0,"Source":"208.93.137.180","Destination":"c-24-6-173-220.hsd1.ca.comcast.net","Protocol":"HTTP","TotalLength":23339}

{"Source":"a184-84-222-144.deploy.static.akamaitechnologies.com","Destination":"c-24-6-173-220.hsd1.ca.comcast.net","Protocol":"TCP","TotalLength":4769916,"SourceCity":"Redwood City","DestinationCity":"Milpitas","SourceCountry":"United States","DestinationCountry":"UnitedStates","SourceLatitude":"37.4852","SourceLongitude":"-122.2364","DestinationLatitude":"37.4404","DestinationLongitude":"-121.8705","LengthOverTime":[0,0,0,0,0,0,0,0,91148,3130952,1547816,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]}

DataSet

The transformation of data structure and impact on visualization



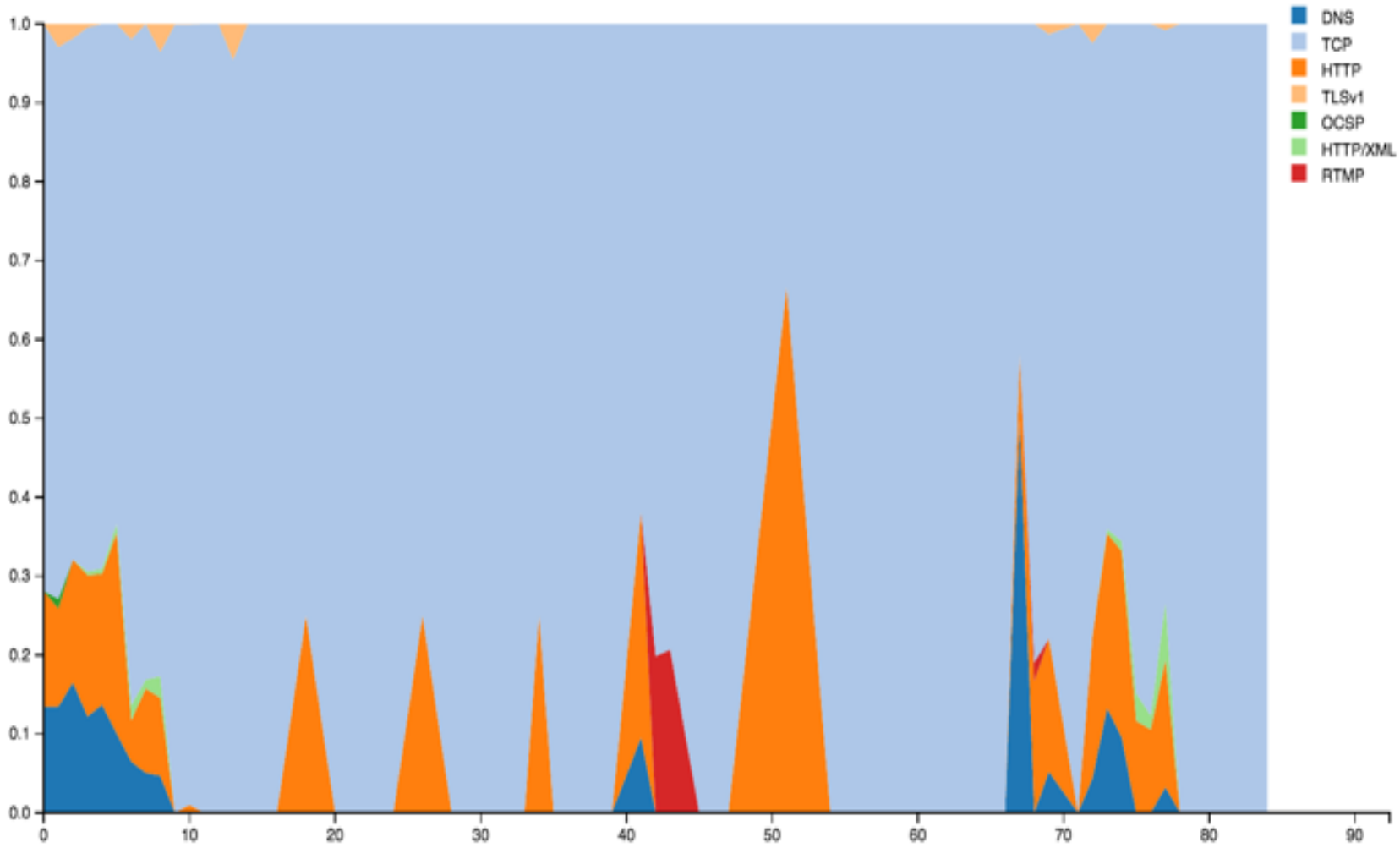
By this, we reduce the data file from 1.4MB to 5.8KB. This will significantly improve the network performance.The file is JSON rather than CSV. JSON is super easy to manipulate in JavaScript.

The structure is just as what we will use in D3, so much less preprocess in user's browser, which means it's faster.

Find more on :http://sjengle.cs.usfca.edu/cs690-sonicwall/

Our Visualizations

The percentage of protocol usage



Dataset: (Wireshark data)

TIME_SPAN	DNS	TCP	HTTP	TLSv1	OCSP	HTTP/XML	RTMP
1	110	573	102	24	10	0	0