



Visualizations of Dell SonicWALL Firewall Data

This project is for CS690 Master Project course during the semester fall 2014. Our goal is to learn SonicWALL data format and build stand-alone visualizations of Dell SonicWALL firewall data that extends what is available in their analysis products. We use primarily d3.js  and p5.js  to create visualizations.

Dell SonicWall Home Visualizations Data Tools Team

Visualization Matters.

Here, we are visualized.

In this project, we will use D3 to build stand-alone prototype visualizations of Dell SonicWALL firewall data that could be integrated into their Dell SonicWALL Analyzer product.

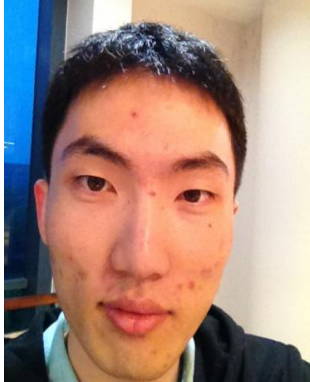
[Learn more on Github](#)

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

Our Team

Team Members(USF graduate students)

Wanzhang Sheng



Kaiming Yang



Jie Gao



Xi Han



Sponsors

Sophie Engle, Assistant Professor,
University of San Francisco



Carrie Gates, Chief Scientist,
Dell Research Center

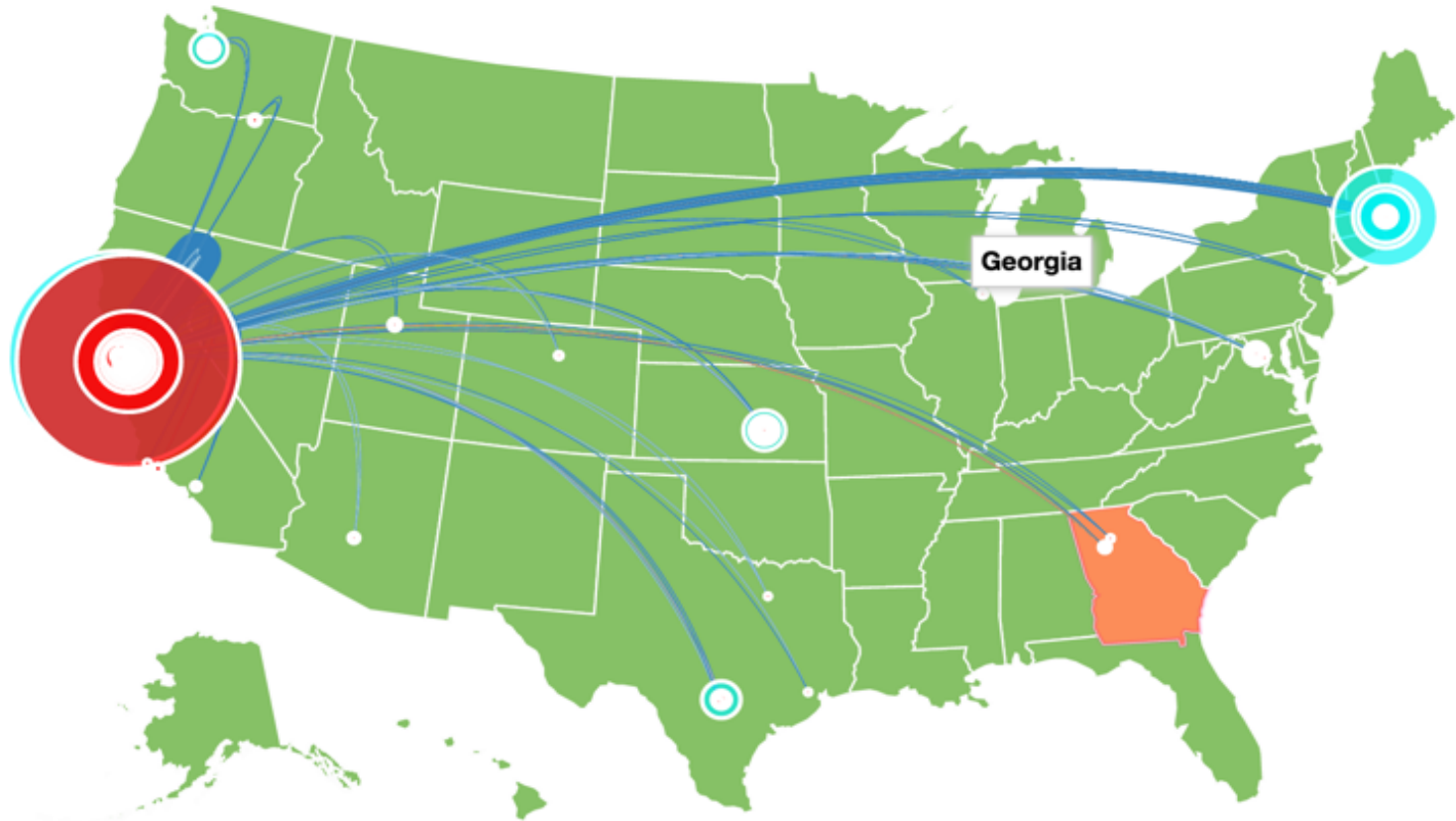


Our Visualizations

Tip: Use mouse wheel to zoom and drag to move.

Switch between scope:

USA World

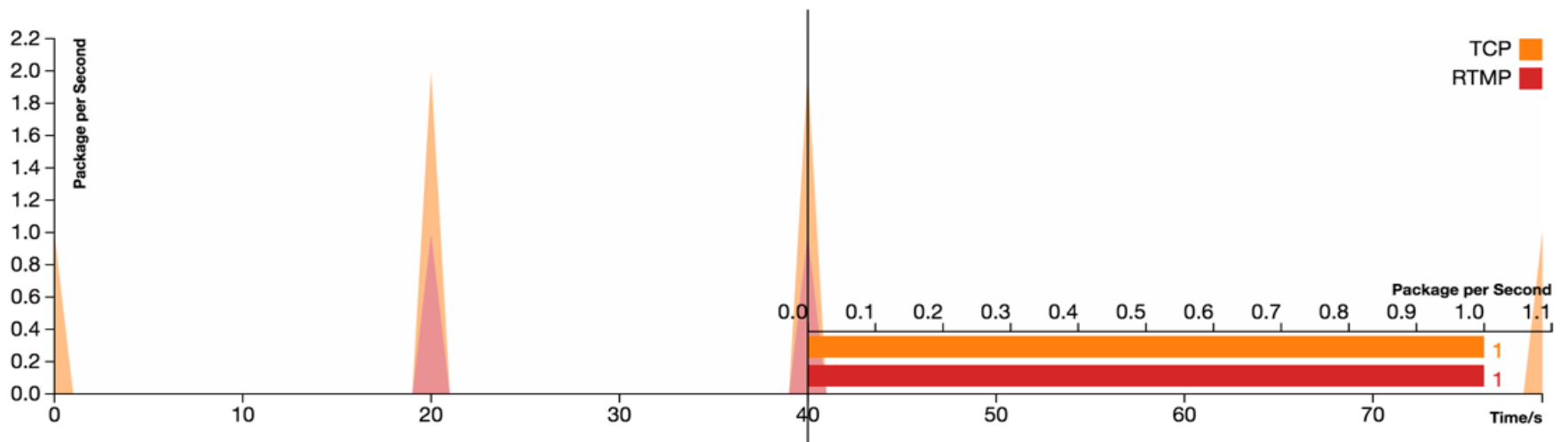


source: ■ destination: ■

Dataset:

```
{"Source": "184.84.222.144", "Destination": "24.6.173.220", "Protocol": "TCP", "TotalLength": 4769916, "SourceCity": "RedwoodCity", "DestinationCity": "Milpitas", "SourceCountry": "UnitedStates", "DestinationCountry": "UnitedStates", "SourceLatitude": "37.4852", "SourceLongitude": "-122.2364", "DestinationLatitude": "37.4404", "DestinationLongitude": "-121.8705"}
```

Dashboard

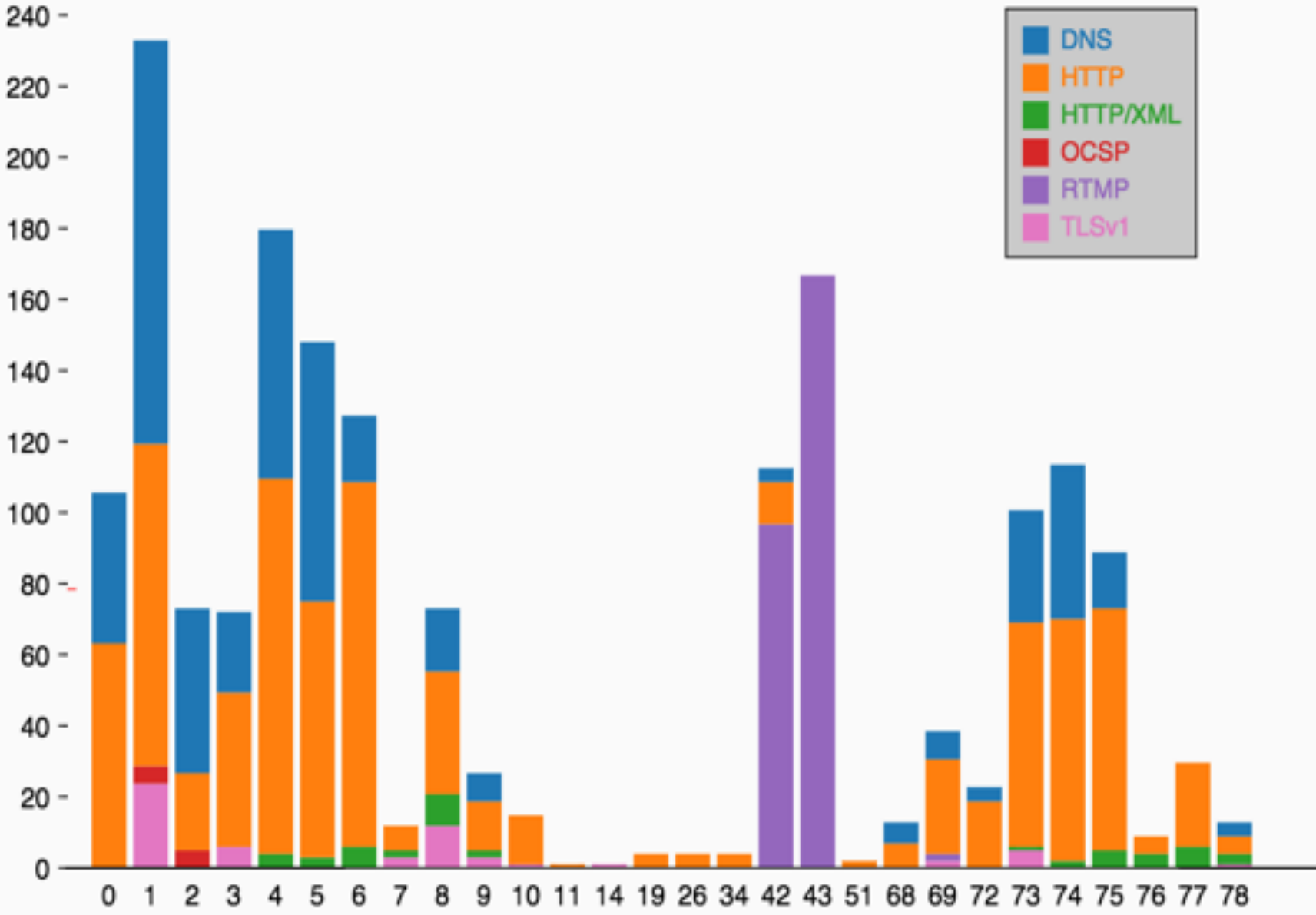


Source	SourceCountry	Destination	DestinationCountry	Protocol	Bytes over Time	Total bytes
a184-84-222-144.deploy.static.akamaitechnologies.com	United States, Redwood City	c-24-6-173-220.hsd1.ca.comcast.net	United States, Milpitas	TCP		
a96-17-110-102.deploy.akamaitechnologies.com	United States, Cambridge	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		
208.93.137.180	United States, San Jose	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		
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		

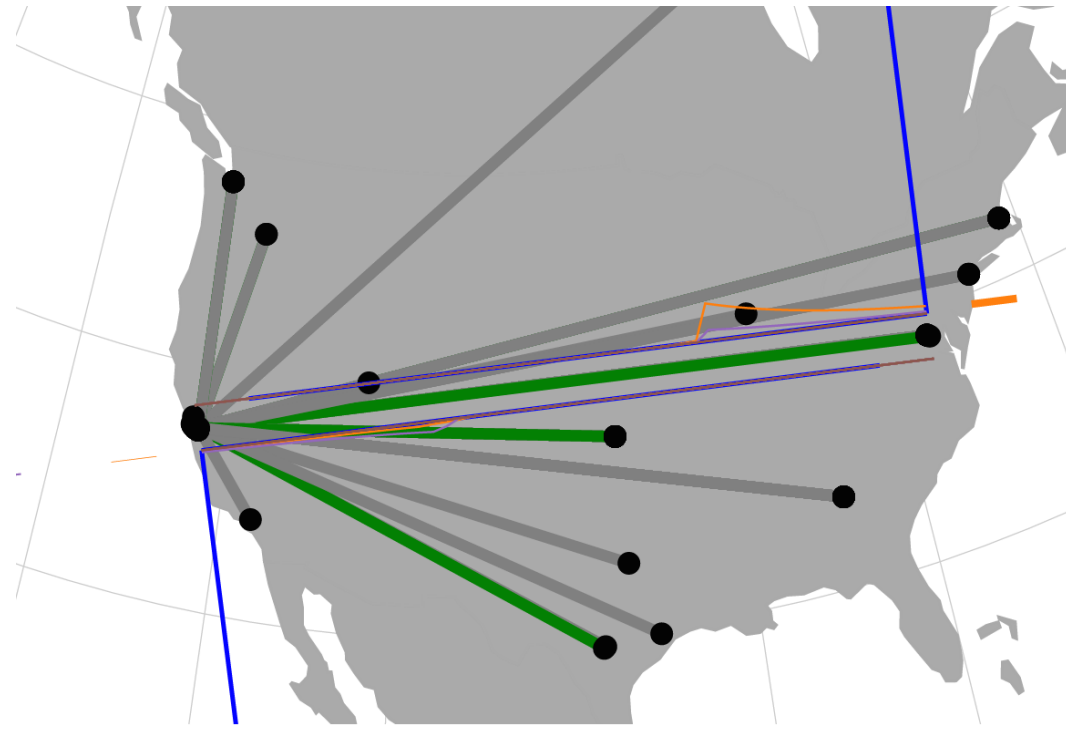
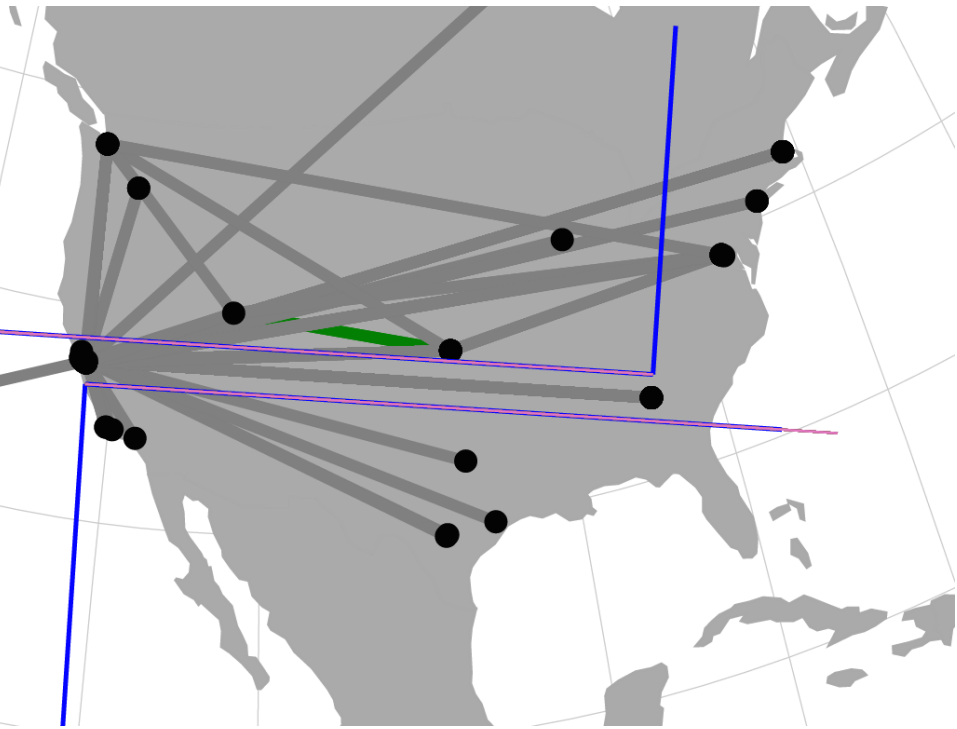
Dataset:

```
{
  "Time":0,
  "Source":"208.93.137.180",
  "Destination":"c-24-6-173-220...",
  "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":"RedwoodCity",
  "DestinationCity":"Milpitas",
  "SourceCountry":"UnitedStates",
  "DestinationCountry":"UnitedStates",
  "SourceLatitude":"37.4852",
  "SourceLongitude":"-122.2364",
  "DestinationLatitude":"37.4404",
  "DestinationLongitude":"-121.8705",
  "LengthOverTime":[0,0,0,0,0 .....]}
```

Different protocol usage (P5.js)



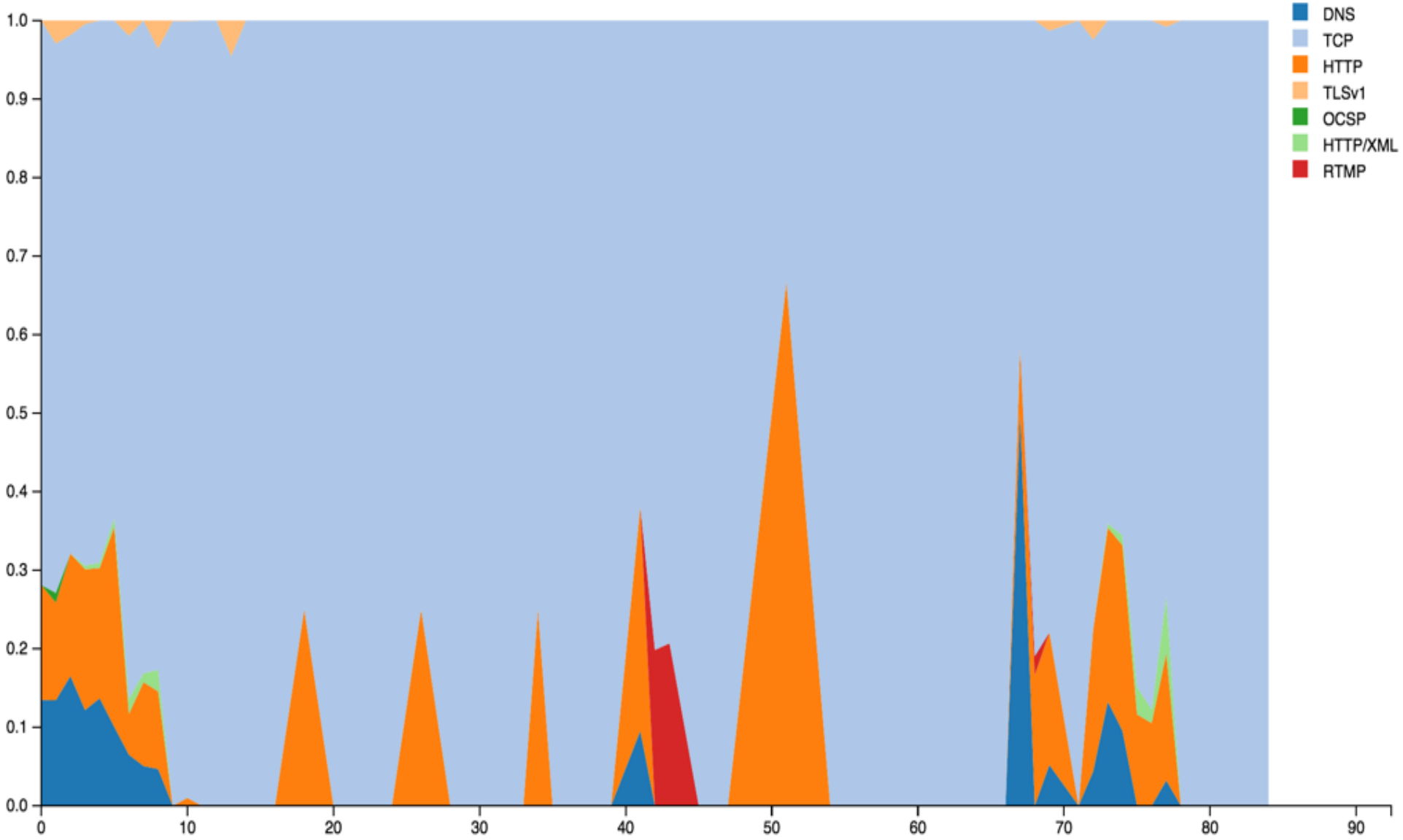
Map plot



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	Lat	Long	Area Code
24.6.173.220	US	USA	CA	California	Milpitas	95035	37.4404	-121.871	807

The percentage of protocol usage

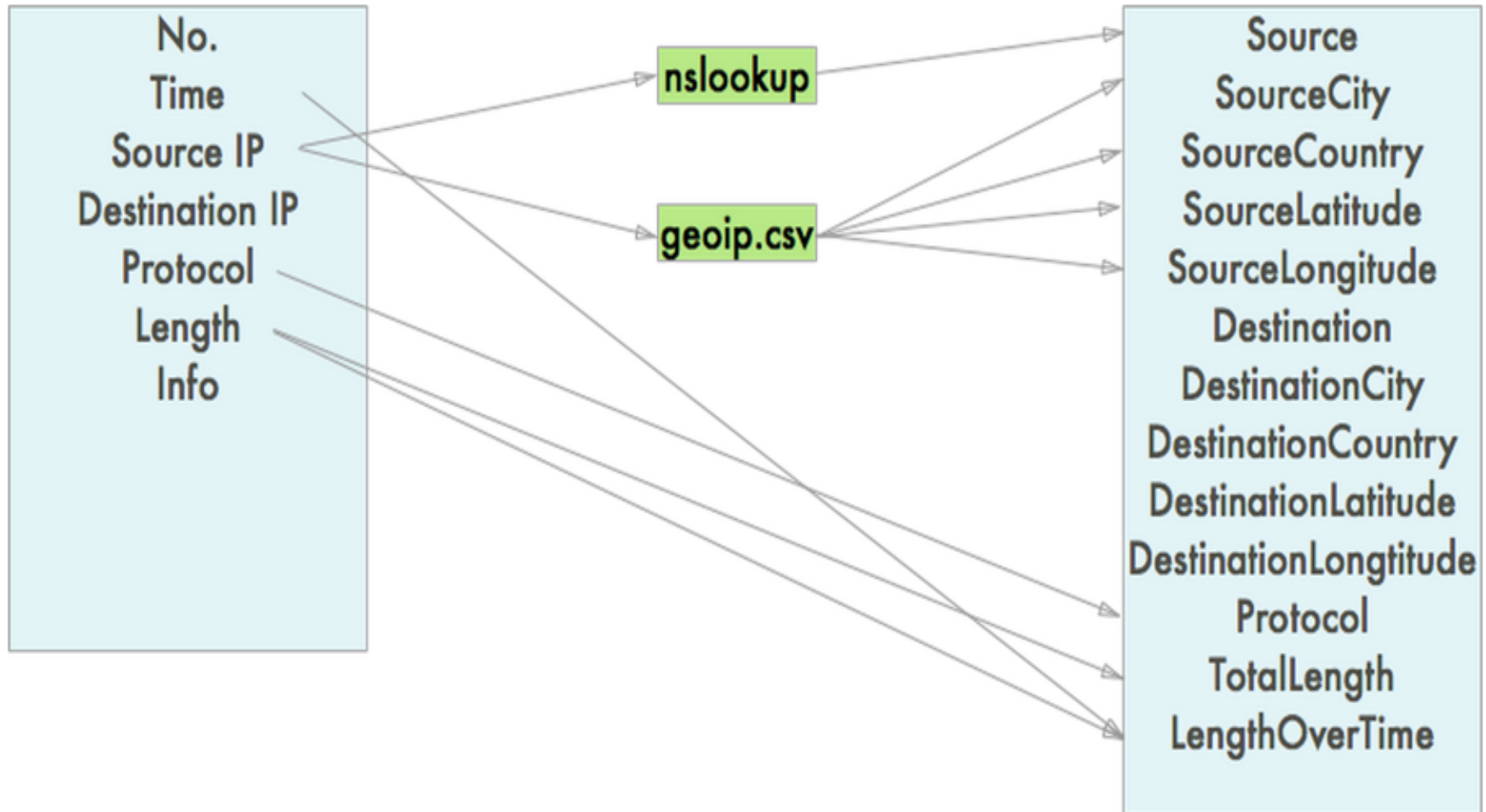


DataSet:(Wireshark Data)

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

DataSet

The transformation of data structure and impact on visualization



By this, we reduce the data file from 1.4MB(left side) to 5.8KB(right side). 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 use in D3, so much less preprocess in user's browser, which means it's faster.

Dell SonicWALL's products

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

Dell SonicWALL Scrutinizer Dashboard

