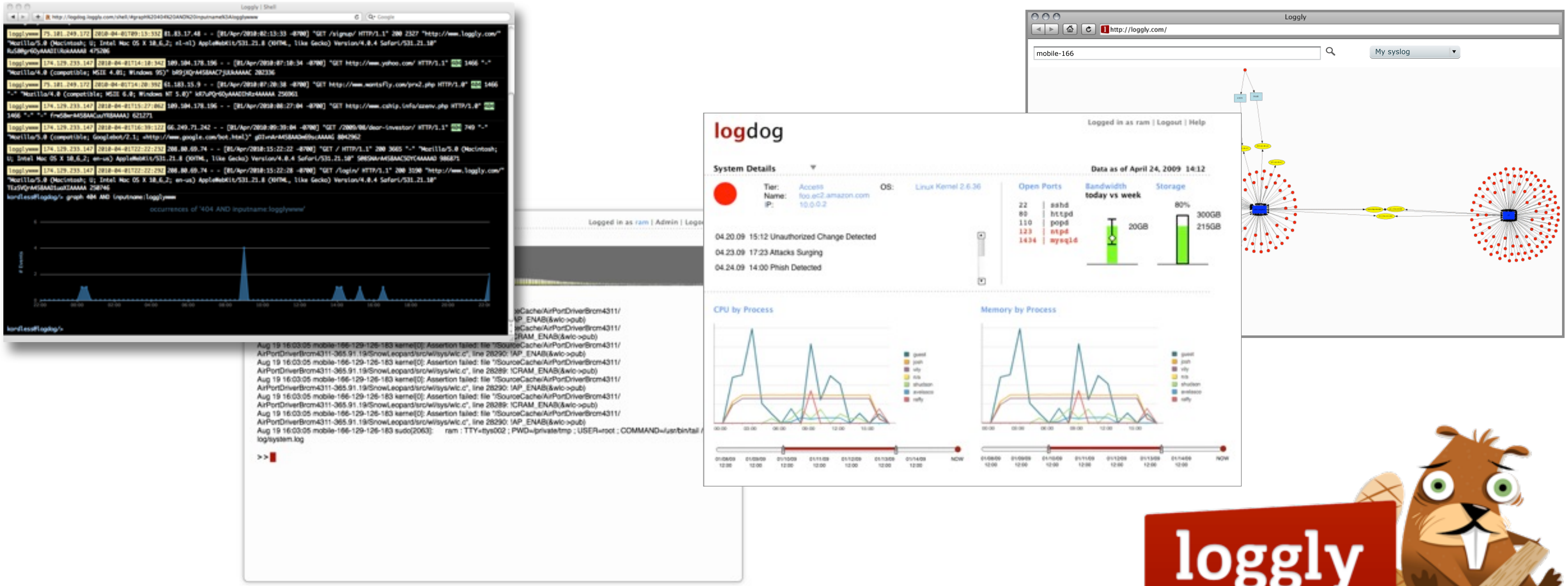
Cloud-based Log Analysis and Visualization

RMLL 2010, Bordeaux, France



Loggly | Shell
http://logdog.loggly.com/shell/#graph%20404%20AND%20inputname%3Alogglywww
Google

```
logglywww 75.101.249.172 2010-04-01T09:13:33Z 81.83.17.48 - - [01/Apr/2010:02:13:33 -0700] "GET /signup/ HTTP/1.1" 200 2327 "http://www.loggly.com/"
"Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_2; nl-nl) AppleWebKit/531.21.8 (KHTML, like Gecko) Version/4.0.4 Safari/531.21.10"
RuS0Wgr6DyAAADIIUkAAAAAB 475206
logglywww 174.129.233.147 2010-04-01T14:10:34Z 109.104.178.196 - - [01/Apr/2010:07:10:34 -0700] "GET http://www.yahoo.com/ HTTP/1.1" 404 1466 "-"
"Mozilla/4.0 (compatible; MSIE 4.01; Windows 95)" bR9jXQrA4SBAAC7jUUkAAAAC 202336
logglywww 75.101.249.172 2010-04-01T14:20:39Z 61.183.15.9 - - [01/Apr/2010:07:20:38 -0700] "GET http://www.wantsfly.com/prx2.php HTTP/1.0" 404 1466
"-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)" k07uPQr6DyAAADIhRz4AAAAA 250061
logglywww 174.129.233.147 2010-04-01T15:27:06Z 109.104.178.196 - - [01/Apr/2010:08:27:04 -0700] "GET http://www.cship.info/azenv.php HTTP/1.0" 404
1466 "-" "-" frw58wr4ASBAACuuYRBAAAAJ 621271
logglywww 174.129.233.147 2010-04-01T16:39:12Z 66.249.71.242 - - [01/Apr/2010:09:39:04 -0700] "GET /2009/08/dear-investor/ HTTP/1.1" 404 749 "-"
"Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)" gDIvnArA4SBAADm09scAAAAG 8042962
logglywww 174.129.233.147 2010-04-01T22:22:23Z 208.80.69.74 - - [01/Apr/2010:15:22:22 -0700] "GET / HTTP/1.1" 200 3665 "-" "Mozilla/5.0 (Macintosh;
U; Intel Mac OS X 10_6_2; en-us) AppleWebKit/531.21.8 (KHTML, like Gecko) Version/4.0.4 Safari/531.21.10" SWdSNArA4SBAAC5DYC4AAAAD 986871
logglywww 174.129.233.147 2010-04-01T22:22:29Z 208.80.69.74 - - [01/Apr/2010:15:22:28 -0700] "GET /login/ HTTP/1.1" 200 3190 "http://www.loggly.com/"
"Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_2; en-us) AppleWebKit/531.21.8 (KHTML, like Gecko) Version/4.0.4 Safari/531.21.10"
TEzSVQrA4SBAADluaXIAAAAA 250746
kordless@logdog/> graph 404 AND inputname:logglywww
```

```
kordless@logdog/>
```

```
…eCache/AirPortDriverBrcm4311/
…AP_ENAB(&wlc->pub)
…eCache/AirPortDriverBrcm4311/
…CRAM_ENAB(&wlc->pub)
Aug 19 16:03:05 mobile-166-129-126-183 kernel[0]: Assertion failed: file "/SourceCache/AirPortDriverBrcm4311/
AirPortDriverBrcm4311-365.91.19/SnowLeopard/src/wl/sys/wlc.c", line 28290: !AP_ENAB(&wlc->pub)
Aug 19 16:03:05 mobile-166-129-126-183 kernel[0]: Assertion failed: file "/SourceCache/AirPortDriverBrcm4311/
AirPortDriverBrcm4311-365.91.19/SnowLeopard/src/wl/sys/wlc.c", line 28289: !CRAM_ENAB(&wlc->pub)
Aug 19 16:03:05 mobile-166-129-126-183 kernel[0]: Assertion failed: file "/SourceCache/AirPortDriverBrcm4311/
AirPortDriverBrcm4311-365.91.19/SnowLeopard/src/wl/sys/wlc.c", line 28290: !AP_ENAB(&wlc->pub)
Aug 19 16:03:05 mobile-166-129-126-183 kernel[0]: Assertion failed: file "/SourceCache/AirPortDriverBrcm4311/
AirPortDriverBrcm4311-365.91.19/SnowLeopard/src/wl/sys/wlc.c", line 28289: !CRAM_ENAB(&wlc->pub)
Aug 19 16:03:05 mobile-166-129-126-183 kernel[0]: Assertion failed: file "/SourceCache/AirPortDriverBrcm4311/
AirPortDriverBrcm4311-365.91.19/SnowLeopard/src/wl/sys/wlc.c", line 28290: !AP_ENAB(&wlc->pub)
Aug 19 16:03:05 mobile-166-129-126-183 sudo[2063]:      ram : TTY=ttys002 ; PWD=/private/tmp ; USER=root ; COMMAND=/usr/bin/tail /
log/system.log

>>
```

logdog
Logged in as ram | Logout | Help
System Details
Data as of April 24, 2009 14:12

Tier: Access
Name: foo.ec2.amazon.com
IP: 10.0.0.2
OS: Linux Kernel 2.6.36

04.20.09 15:12 Unauthorized Change Detected

04.23.09 17:23 Attacks Surging

04.24.09 14:00 Phish Detected

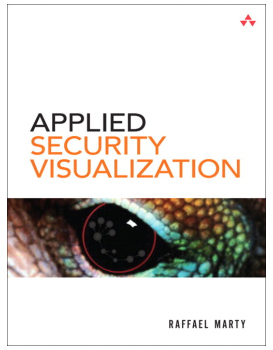
Open Ports

22	sshd
80	httpd
110	popd
123	ntpd
1434	mysqld

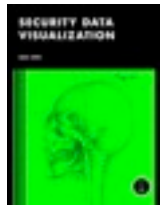
Raffael Marty - @zrlram

Raffael (Raffy) Marty

- Founder @ loggly
- Chief Security Strategist and Product Manager @ Splunk
- Manager Solutions @ ArcSight
- Intrusion Detection Research @ IBM Research
- IT Security Consultant @ PriceWaterhouse Coopers



Applied Security Visualization
Publisher: Addison Wesley (August, 2008)
ISBN: 0321510100



SECVIZ

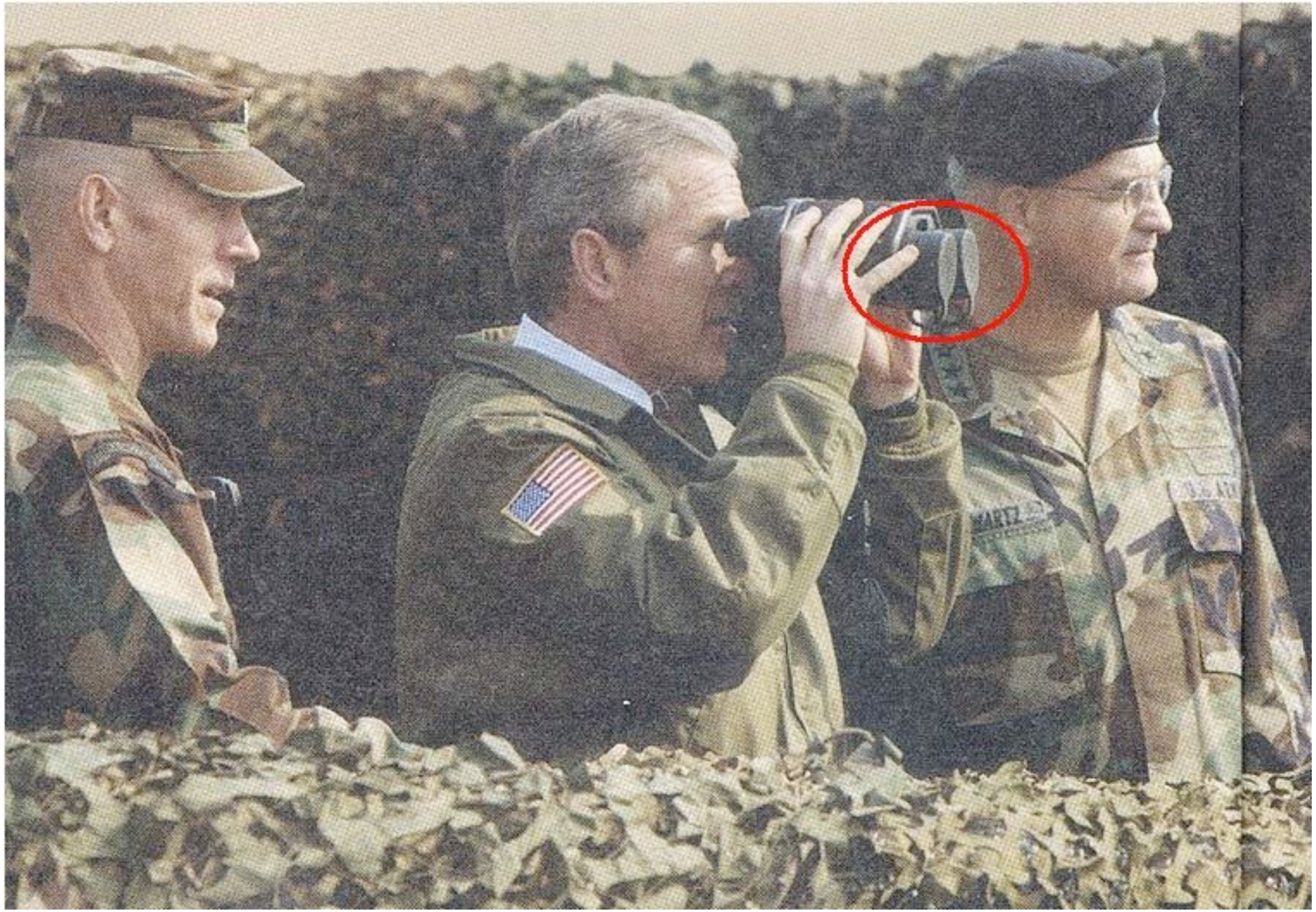
afterglow

DAVIX

Agenda

- Introduction
- Visualization
- InfoViz Process
- Visualization **Tools**
- The Cloud
- Loggly
- Do it Yourself
  - AfterGlow
  - Google Visualization API
- Visualization **Use-Cases**
- Visualization **Resources**

Open Your Eyes



Security Is About Seeing

Goals

- Learn how you can
  - use **visualization** to help solve security problems
  - leverage the **cloud** to build security visualization tools

Information Visualization?

A picture is worth a thousand log records.

Explore and Discover

Answer a Question

Pose a New Question

Increase Efficiency

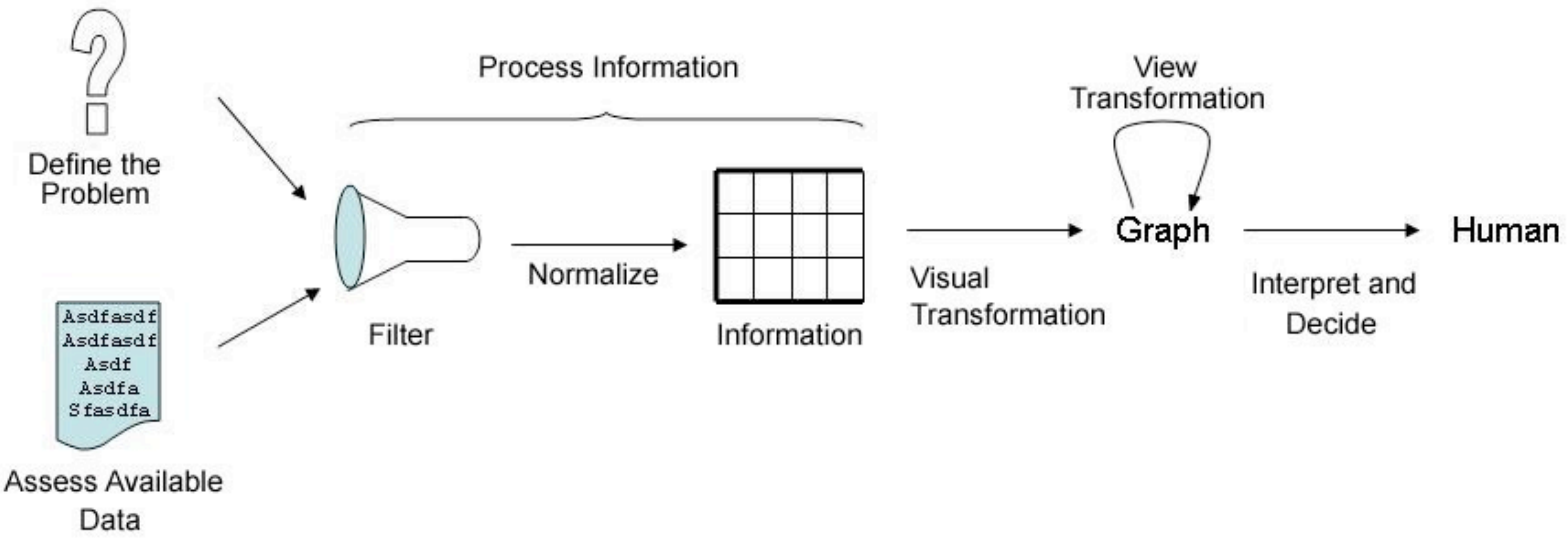
Communicate Information

Support Decisions

Inspire

Visualization and The Cloud

InfoViz Process



Collect

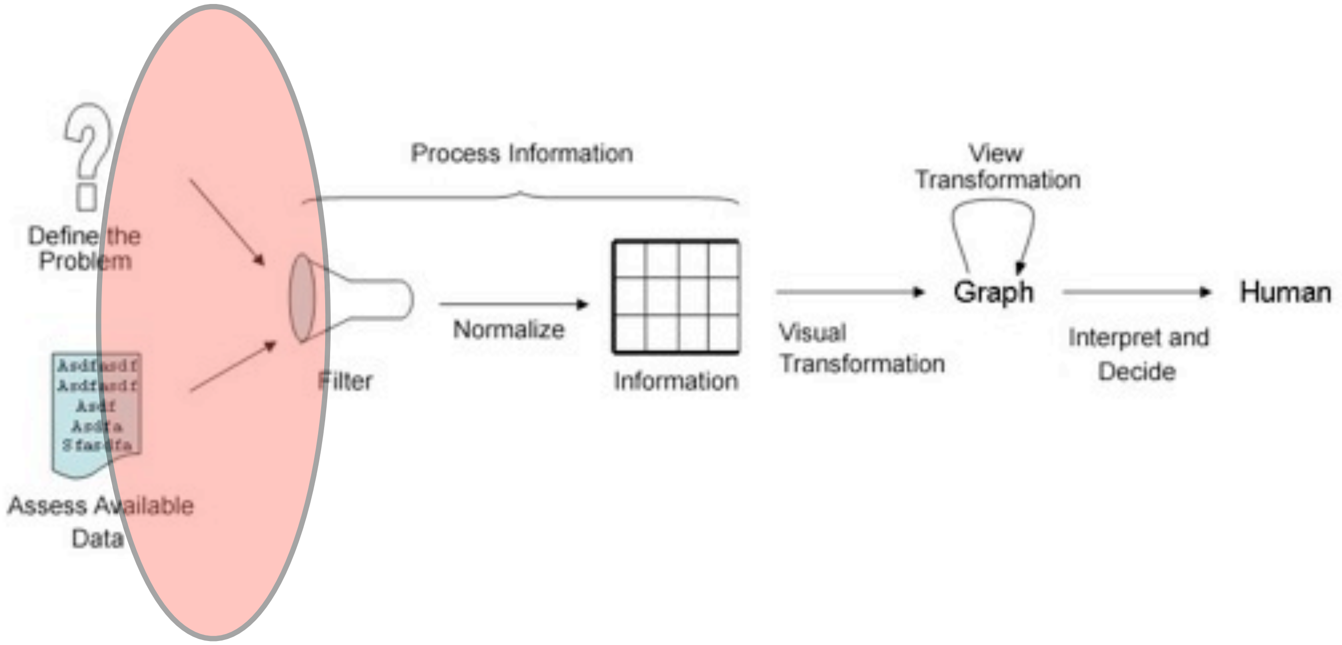
- large-scale data collection
- and processing

Process

- Your parsers
- Standard formats

Visualize

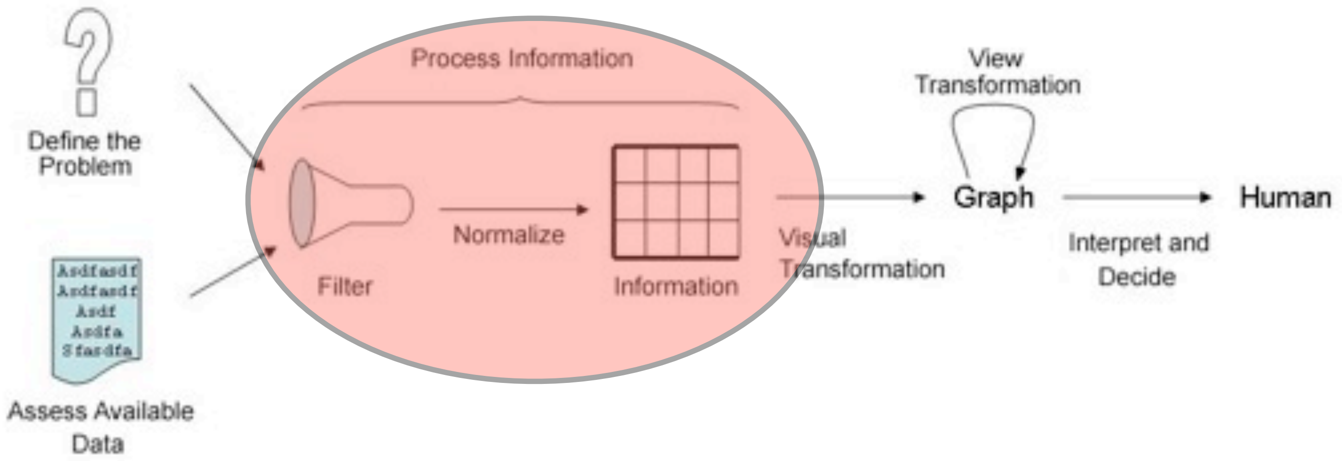
- Visualization Tools
- and Libraries


Define the Problem
Asdfasdf
Asdfasdf
Asdf
Asdfa
Sfasdfa
Assess Available Data
Process Information
Filter
Normalize
Information
View Transformation
Visual Transformation
Graph
Interpret and Decide
Human

Collect

Log Management

- Log Collection and Centralization
- Log Storage
- Log Filtering
- Log Aggregation
- Log Search and Extraction
- Log Retention and Archiving


Define the Problem
Assess Available Data
Asdfasdf
Asdfasdf
Asdf
Asdfa
Sfasdfa
Process Information
Filter
Normalize
Information
Visual Transformation
View Transformation
Graph
Interpret and Decide
Human

Process

Standard Formats

- Multiple formats

```
Oct 13 20:00:43.874401 rule 193/0(match): block in on xl0: 212.251.89.126.3859 >: S
1818630320:1818630320(0) win 65535 <mss 1460,nop,nop,sackOK> (DF)

Oct 13 20:00:43 fwbox local4:warn|warning fw07 %PIX-4-106023: Deny tcp src
internet: 212.251.89.126/3859 dst 212.254.110.98/135 by access-group
"internet_access_in"

Oct 13 20:00:43 fwbox kernel: DROPPED IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:0f:cc:
81:40:94:08:00 SRC=212.251.89.126 DST=212.254.110.98 LEN=576 TOS=0x00 PREC=0x00
TTL=255 ID=8624 PROTO=TCP SPT=3859 DPT=135 LEN=556
```

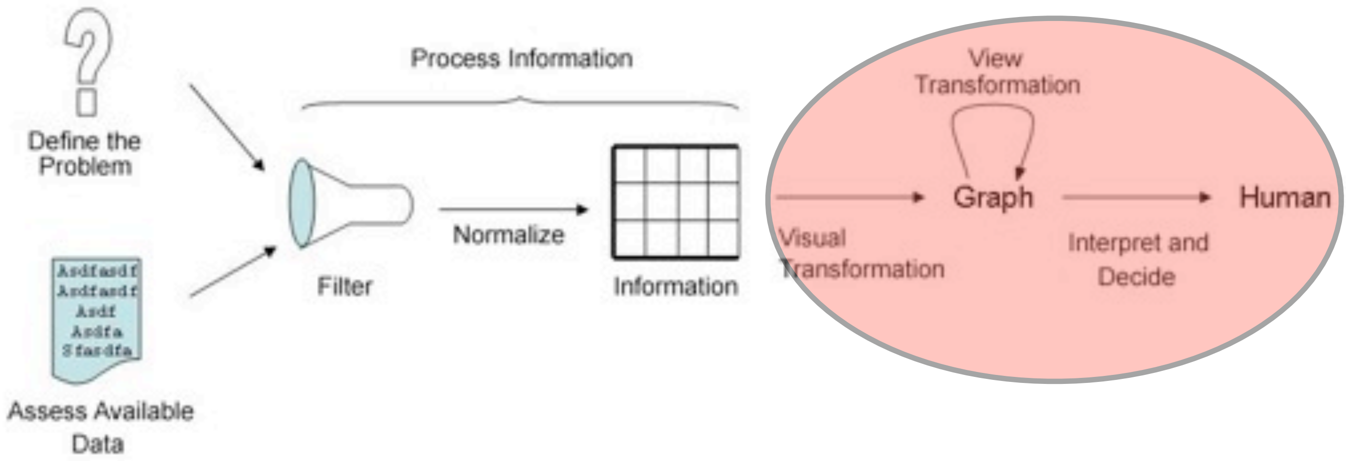
- Log Standards
  - CEE (cee.mitre.org)
  - IDMEF
  - SDEE
  - CBE
  - WELF
  - XDAS

Normalization

- **Parsers**

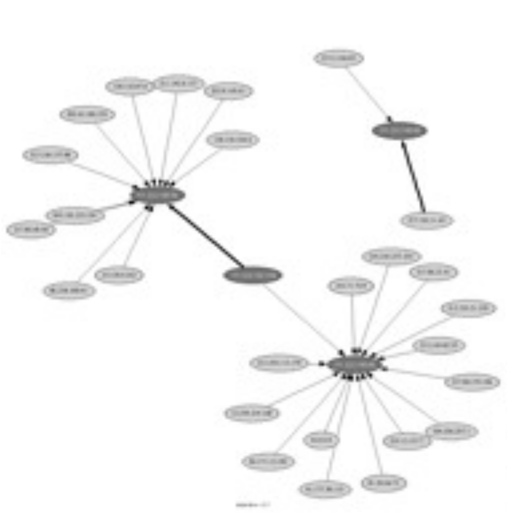
  "To analyze or separate (input, for example) into more easily processed components." (answers.com)

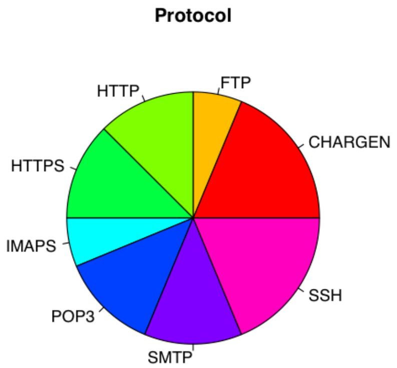
- Generate a common output format for vis-tools (e.g., CSV)
- For example
  - Regex /(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/g
  - http://secviz.org/content/parser-exchange


Define the Problem
Assess Available Data
Process Information
Filter
Normalize
Information
View Transformation
Graph
Visual Transformation
Interpret and Decide
Human
Asdfasdf
Asdfasdf
Asdf
Asdfa
Sfasdfa

Visualize

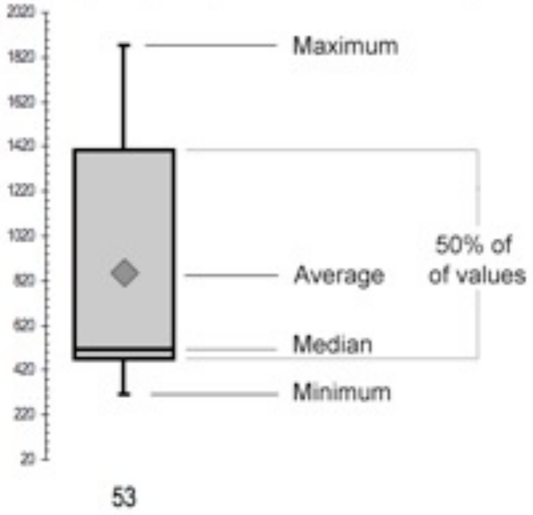
Choose Your Poison

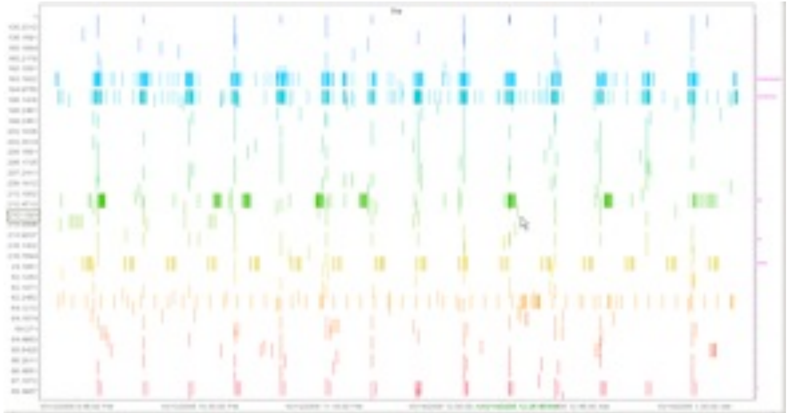


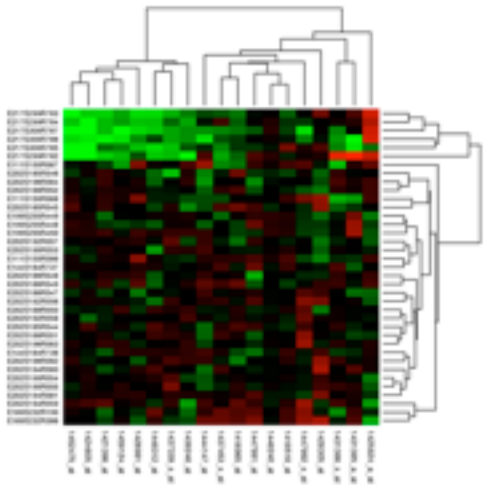


Mon
Tue
Wed
Thu
Fri
Sat
Sun
Mon

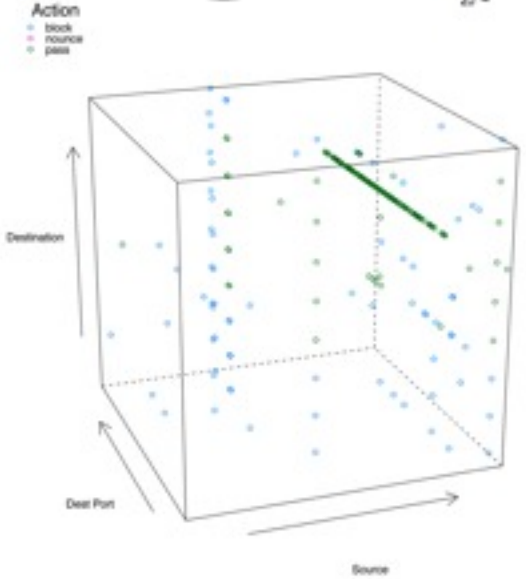
HP DEC
GE
Xerox AT&T Apple MIT
DISA
Multicast
Reserved
IBM
APNIC
ARIN
RIPE
US-DOD
LACNIC
Unallocated
Various Registries

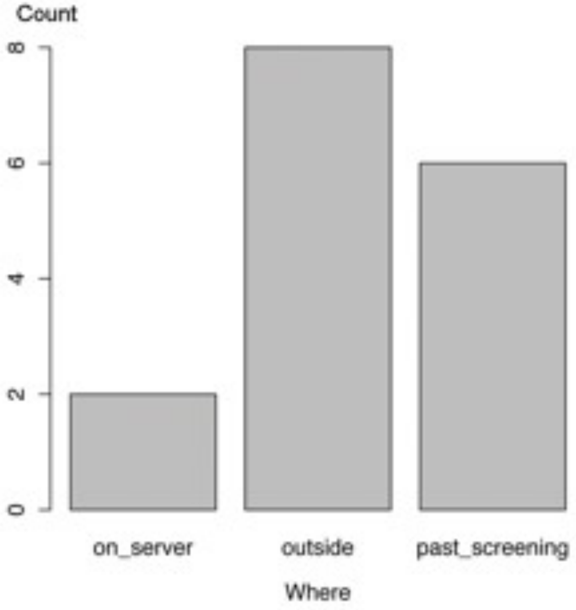


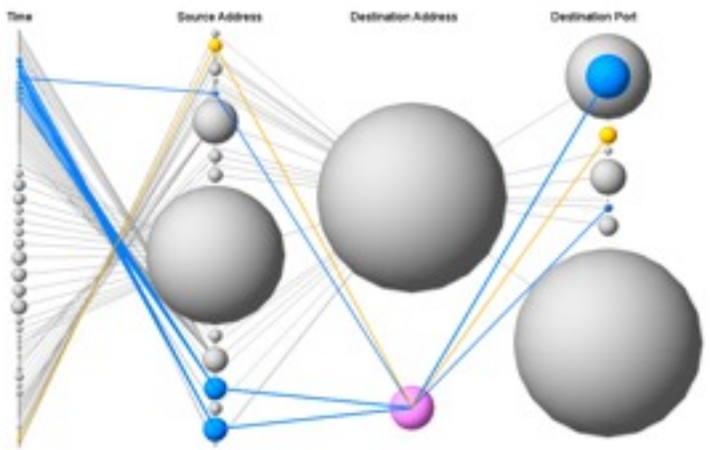


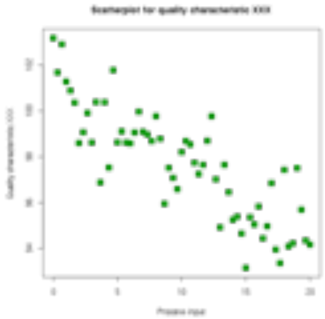


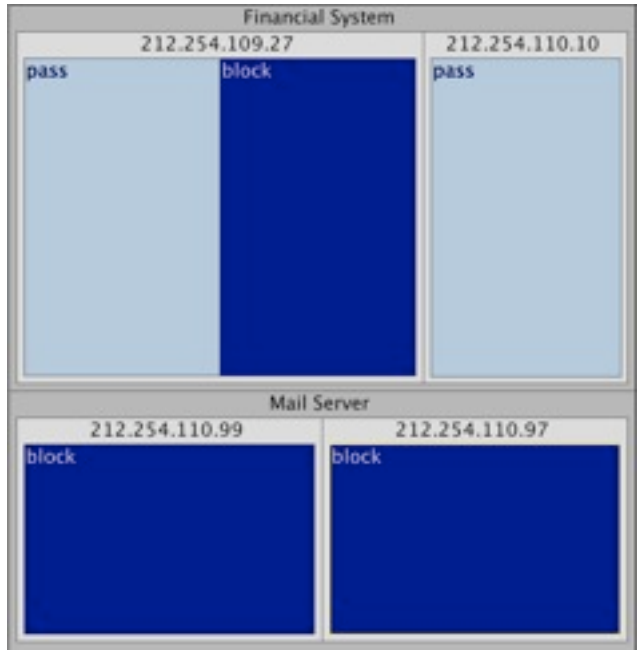
Maroc
famille
sociale
traditions
républicaines
francophones
Portugal
Maghreb
Algérie











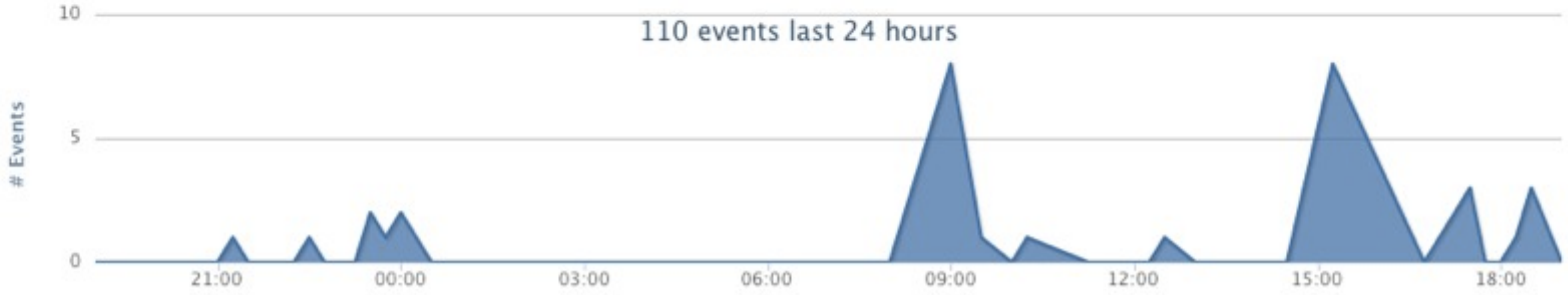
Reporting vs. Visualization

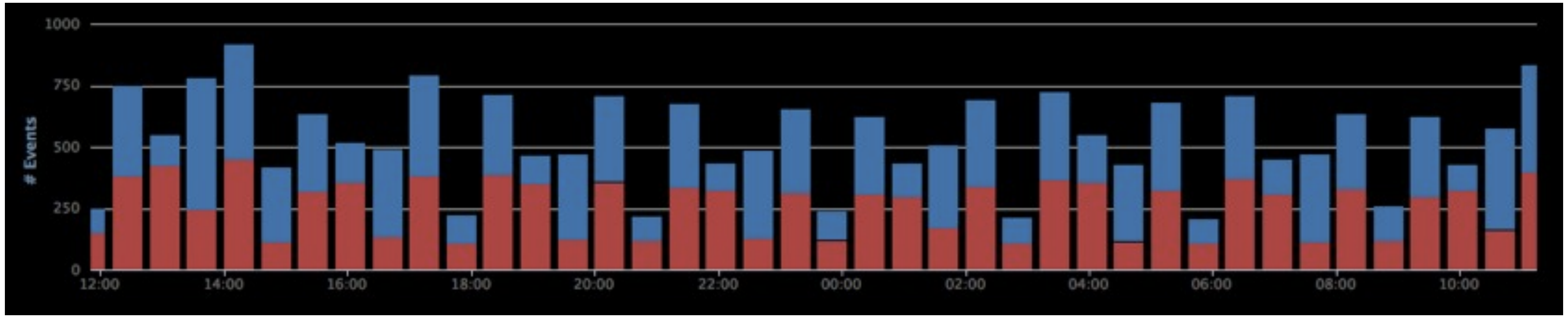
- Reporting Libraries
  - HighCharts
  - Flot
  - Google Chart API
  - Open Flash Chart

- Visualization Libraries
  - TheJIT
  - Graphael
  - Protovis
  - ProcessingJS
  - Flare

JavaScript vs. Flash vs. XYZ

HighCharts



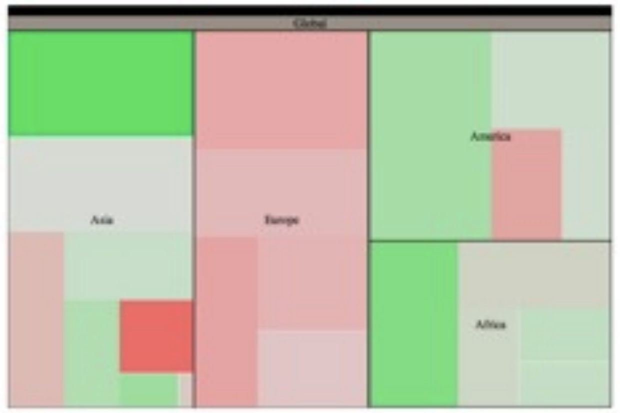


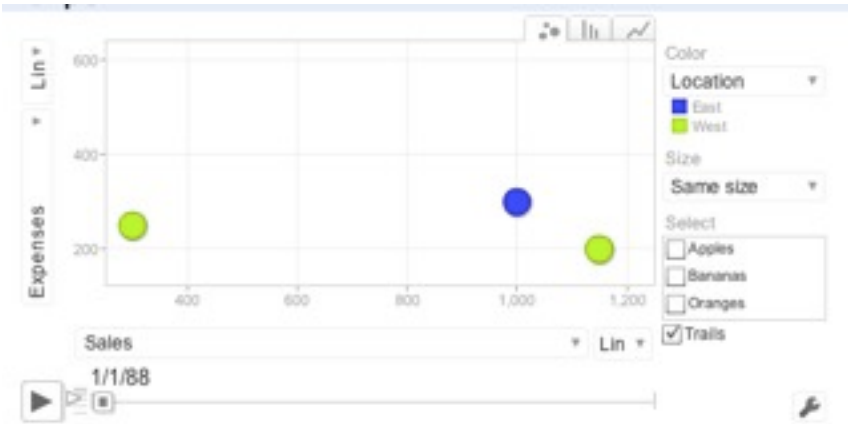
- Click-Through
- On load
  - near real-time updates
- Zoom

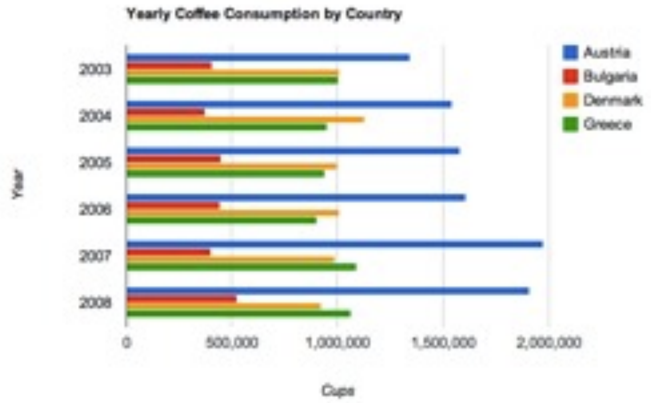
- AJAX data input via JSON

http://www.highcharts.com/

Google Visualization API



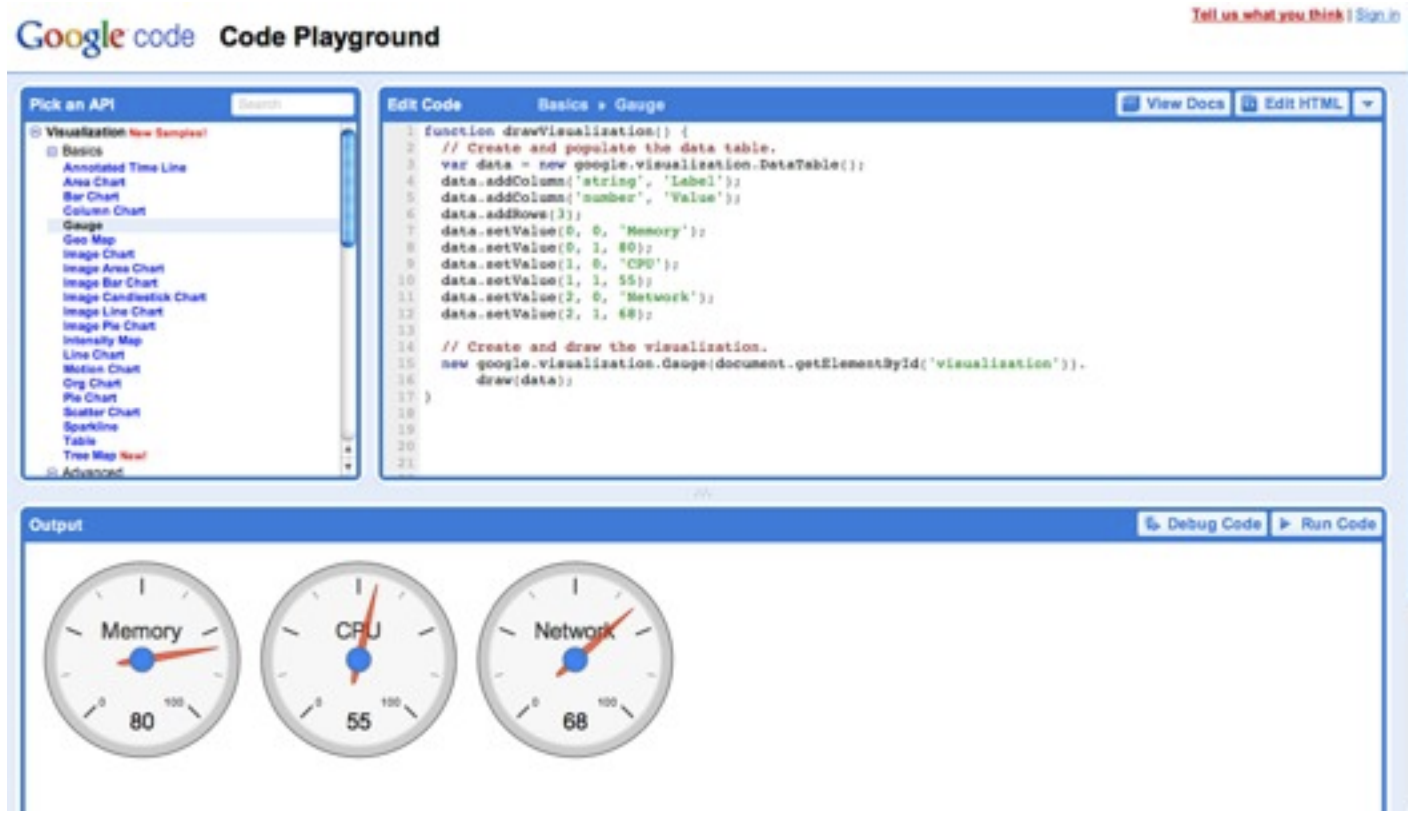




Memory
80
CPU
55
Network
68

http://code.google.com/apis/visualization/interactive_charts.html

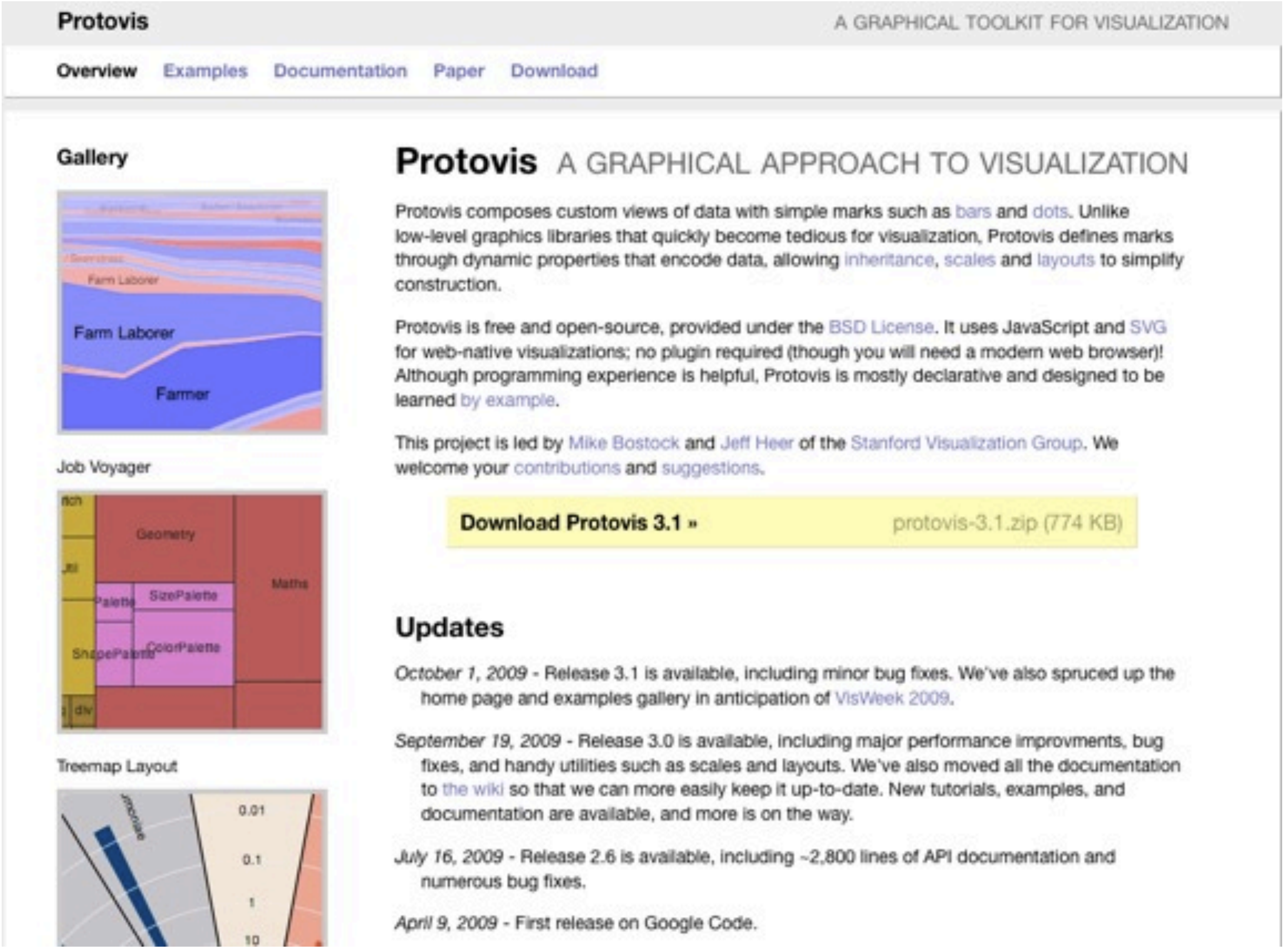
- JavaScript
- Based on DataTables()
- Many graphs
- Playground
  - http://code.google.com/apis/ajax/playground



```
function drawVisualization() {
  // Create and populate the data table.
  var data = new google.visualization.DataTable();
  data.addColumn('string', 'Label');
  data.addColumn('number', 'Value');
  data.addRows(3);
  data.setValue(0, 0, 'Memory');
  data.setValue(0, 1, 80);
  data.setValue(1, 0, 'CPU');
  data.setValue(1, 1, 55);
  data.setValue(2, 0, 'Network');
  data.setValue(2, 1, 68);

  // Create and draw the visualization.
  new google.visualization.Gauge(document.getElementById('visualization')).
      draw(data);
}
```

ProtoVis

- JavaScript based visualization library
- Charting
- Treemaps
- BoxPlots
- Parallel Coordinates
- etc.



Protovis A GRAPHICAL APPROACH TO VISUALIZATION

Protovis composes custom views of data with simple marks such as bars and dots. Unlike low-level graphics libraries that quickly become tedious for visualization, Protovis defines marks through dynamic properties that encode data, allowing inheritance, scales and layouts to simplify construction.

Protovis is free and open-source, provided under the BSD License. It uses JavaScript and SVG for web-native visualizations; no plugin required (though you will need a modern web browser)! Although programming experience is helpful, Protovis is mostly declarative and designed to be learned by example.

This project is led by Mike Bostock and Jeff Heer of the Stanford Visualization Group. We welcome your contributions and suggestions.

Download Protovis 3.1 » protovis-3.1.zip (774 KB)

Updates

October 1, 2009 - Release 3.1 is available, including minor bug fixes. We've also spruced up the home page and examples gallery in anticipation of VisWeek 2009.

September 19, 2009 - Release 3.0 is available, including major performance improvments, bug fixes, and handy utilities such as scales and layouts. We've also moved all the documentation to the wiki so that we can more easily keep it up-to-date. New tutorials, examples, and documentation are available, and more is on the way.

July 16, 2009 - Release 2.6 is available, including ~2,800 lines of API documentation and numerous bug fixes.

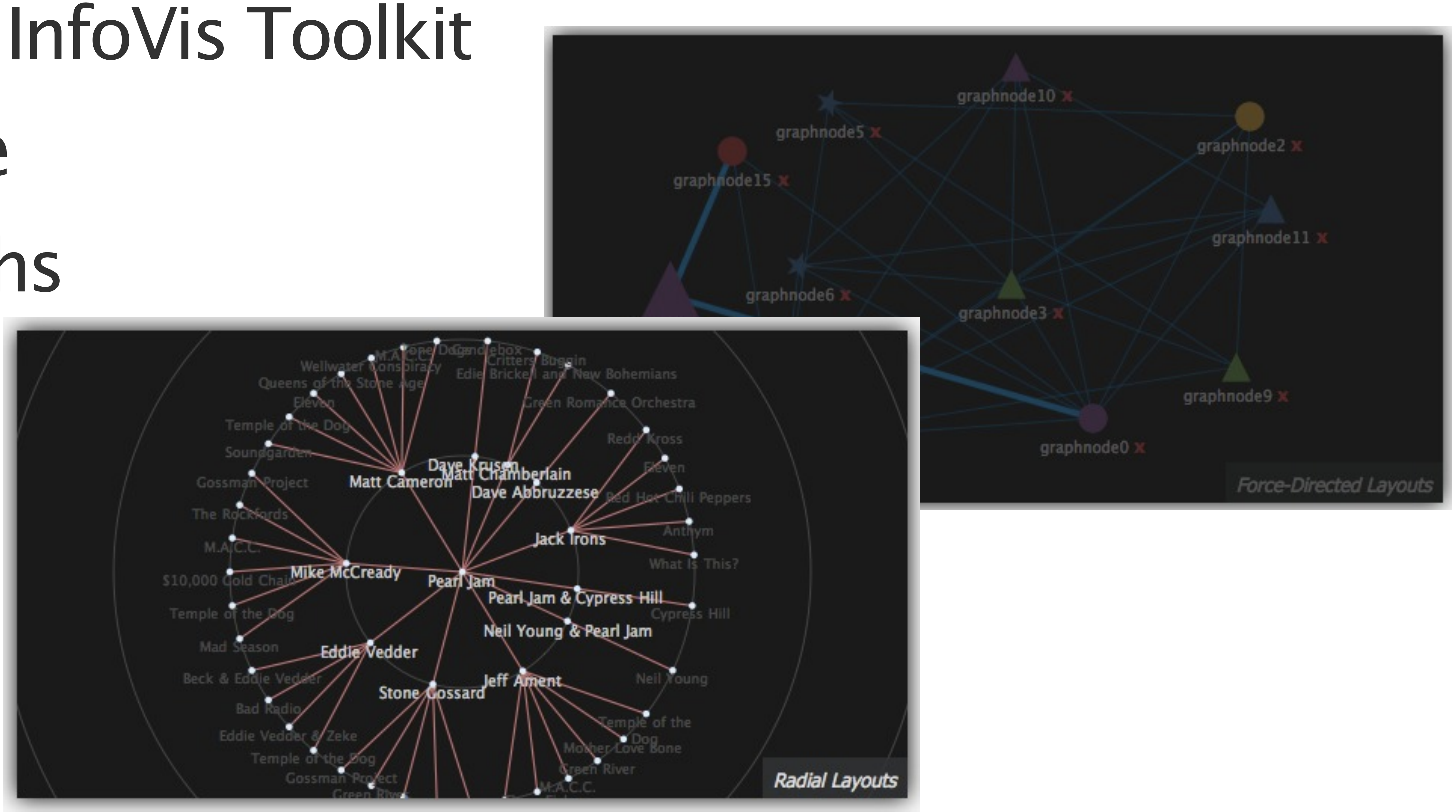
April 9, 2009 - First release on Google Code.

http://vis.stanford.edu/protovis/

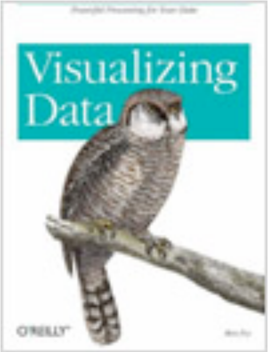
TheJIT

http://thejit.org/

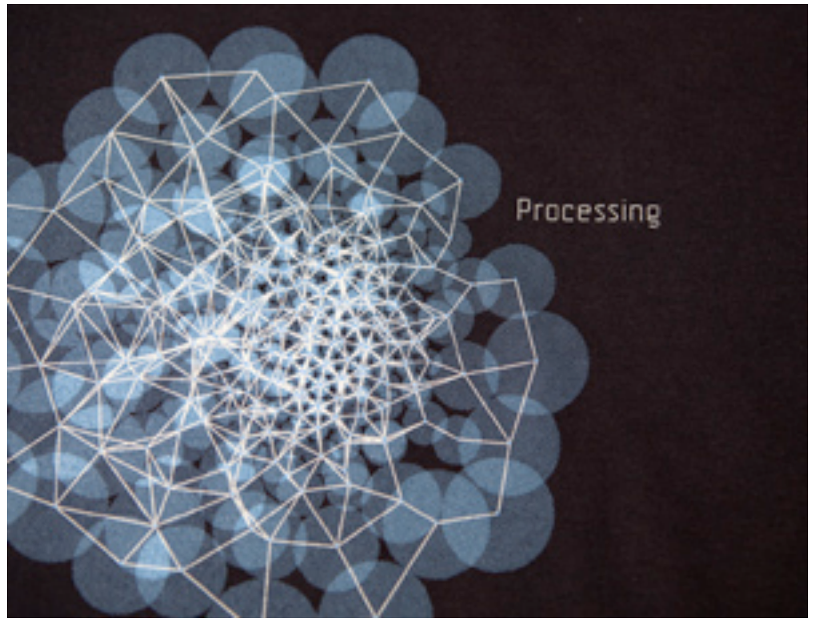
- JavaScript InfoVis Toolkit
- Interactive
- Link Graphs

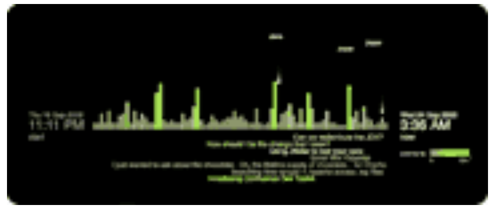


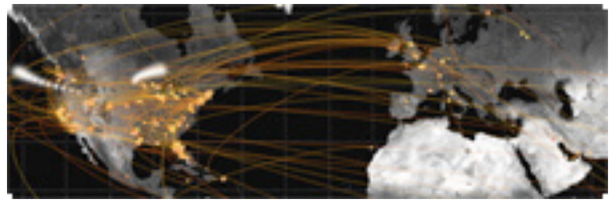
Processing

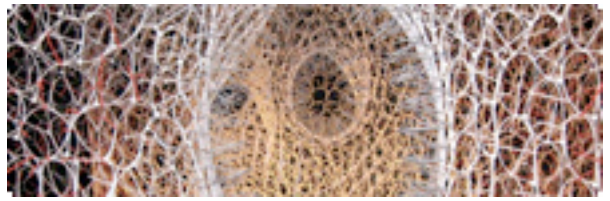


- Visualization library
- Java based
- Interactive (event handling)
- Number of libraries to
  - draw in OpenGL
  - read XML files
  - write PDF files
- Processing JS
  - JavaScript
  - HTML 5 Canvas
  - Web IDE







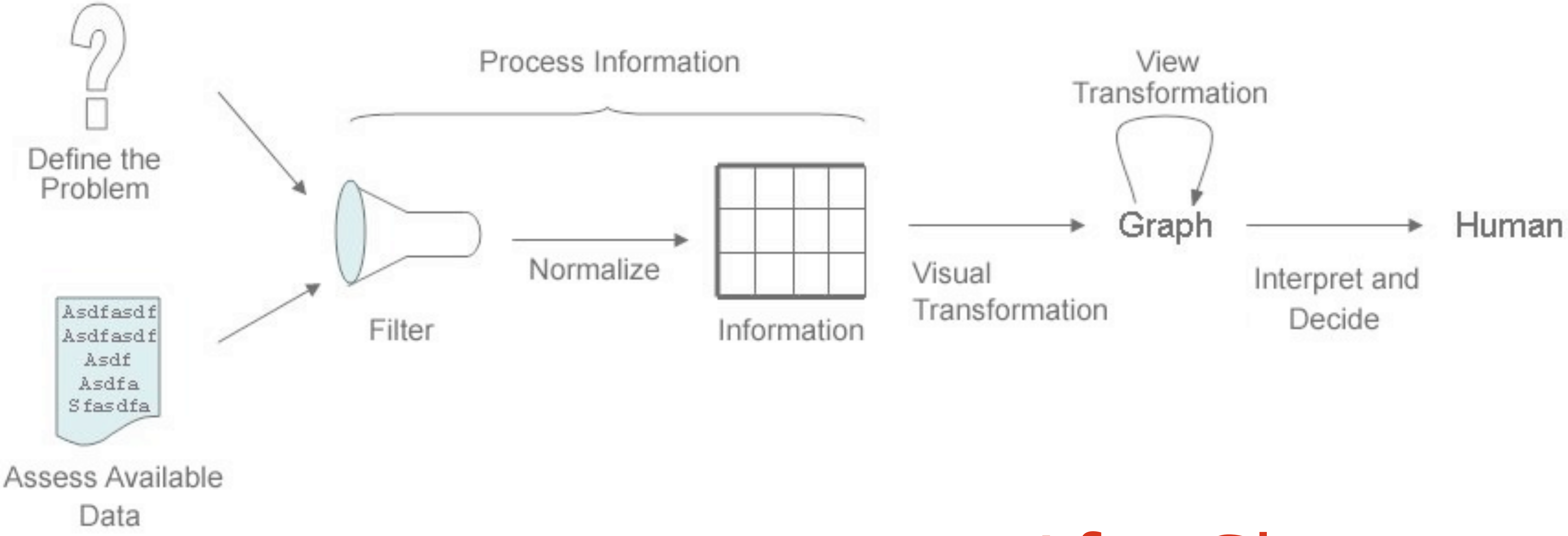


http://processingjs.org/

http://processing.org/

Building Your Own

Build Your Own



Loggly

Regexes

AfterGlow
Google Vis

Data Collection in the Cloud

The (public) Cloud

What it is

- multi-tenancy
- elastic
- “infinite” resources
- pay as you go
- self provisioning

It’s not

- private data center
- virtualization

Types

- SaaS – Software
- PaaS – Platform
- IaaS – Infrastructure

Benefits

- No installation
- No elaborate configurations
- No maintenance
- Great scalability
- 7x24 availability

rackspace

terremark Worldwide, Inc.

GOGRID Control in the Cloud™

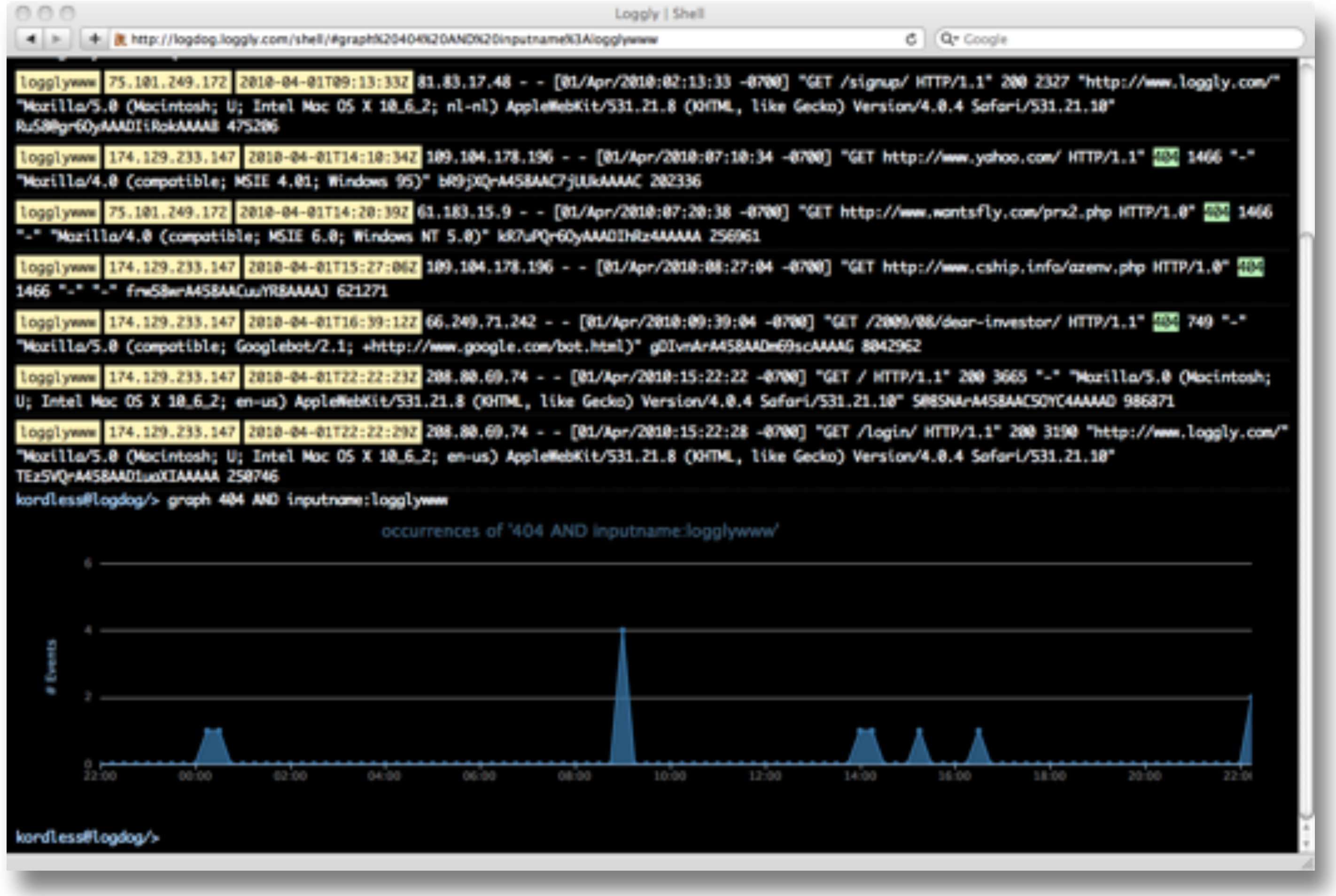
Azure

Google App Engine

amazon webservices™

LaaS – Logging as a Service

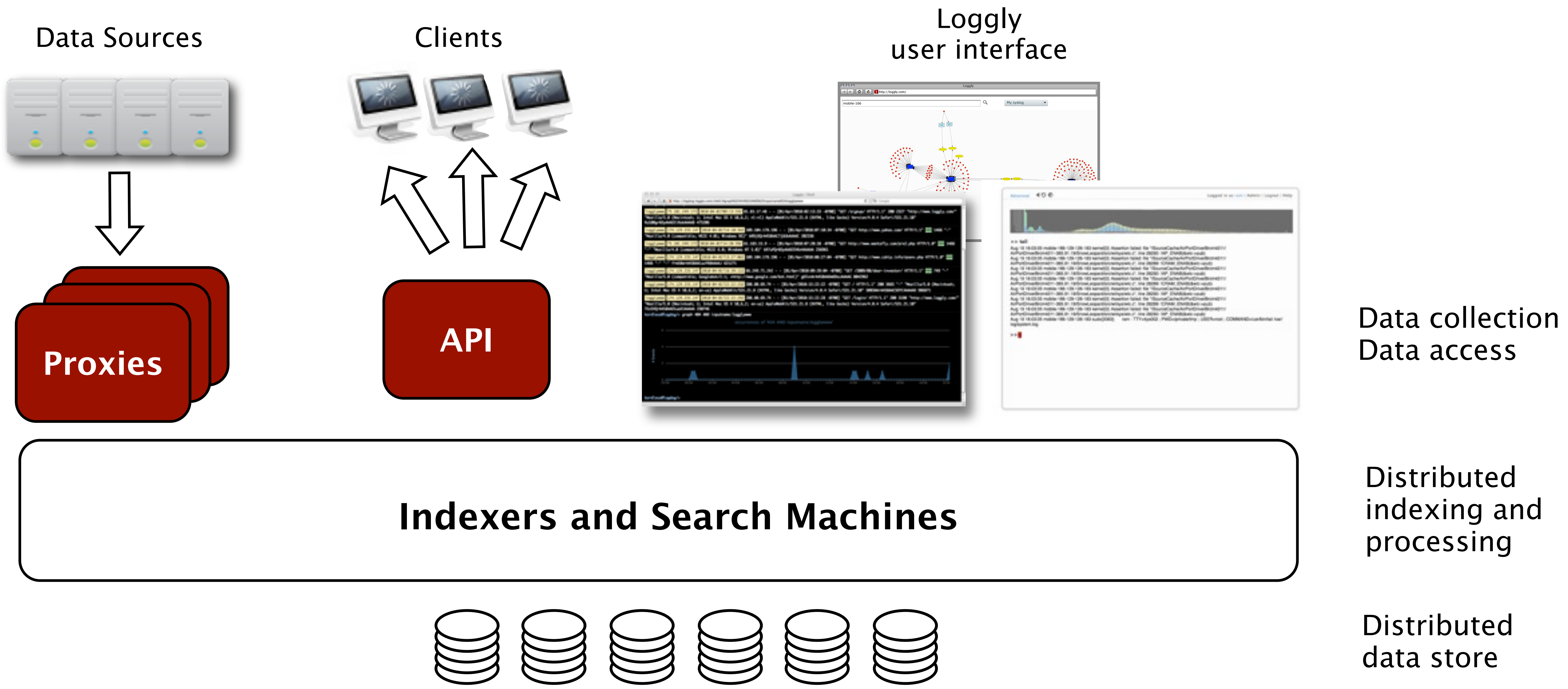
- **All your data in one place**
  - Loggly manages your data (index, store, archive, etc.)
- **Extremely fast search across all your data**
  - Data source agnostic (no parsers)
- **Data management**
  - access control
  - data segregation
  - data overview and summaries
- **API access**


Loggly | Shell
http://logdog.loggly.com/shell/#graph%20404%20AND%20inputname%3Alogglywww
Google

```
logglywww 75.101.249.172 2010-04-01T09:13:33Z 81.83.17.48 - - [01/Apr/2010:02:13:33 -0700] "GET /signup/ HTTP/1.1" 200 2327 "http://www.loggly.com/"
"Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_2; nl-nl) AppleWebKit/531.21.8 (KHTML, like Gecko) Version/4.0.4 Safari/531.21.10"
RuS0@gr6OyAAADIiRokAAAAB 475206
logglywww 174.129.233.147 2010-04-01T14:10:34Z 109.104.178.196 - - [01/Apr/2010:07:10:34 -0700] "GET http://www.yahoo.com/ HTTP/1.1" 404 1466 "-"
"Mozilla/4.0 (compatible; MSIE 4.01; Windows 95)" bR9jXQrA4S8AAC7jUUkAAAAC 202336
logglywww 75.101.249.172 2010-04-01T14:20:39Z 61.183.15.9 - - [01/Apr/2010:07:20:38 -0700] "GET http://www.wantsfly.com/prx2.php HTTP/1.0" 404 1466
"-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)" kR7uPQr6OyAAADIhRz4AAAAA 256961
logglywww 174.129.233.147 2010-04-01T15:27:06Z 109.104.178.196 - - [01/Apr/2010:08:27:04 -0700] "GET http://www.cship.info/azenv.php HTTP/1.0" 404
1466 "-" "-" frw58wrA4S8AACuuYR8AAAAJ 621271
logglywww 174.129.233.147 2010-04-01T16:39:12Z 66.249.71.242 - - [01/Apr/2010:09:39:04 -0700] "GET /2009/08/dear-investor/ HTTP/1.1" 404 749 "-"
"Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)" gDIvnArA4S8AADm69scAAAAG 8042962
logglywww 174.129.233.147 2010-04-01T22:22:23Z 208.80.69.74 - - [01/Apr/2010:15:22:22 -0700] "GET / HTTP/1.1" 200 3665 "-" "Mozilla/5.0 (Macintosh;
U; Intel Mac OS X 10_6_2; en-us) AppleWebKit/531.21.8 (KHTML, like Gecko) Version/4.0.4 Safari/531.21.10" S08SNArA4S8AACSOYC4AAAAD 986871
logglywww 174.129.233.147 2010-04-01T22:22:29Z 208.80.69.74 - - [01/Apr/2010:15:22:28 -0700] "GET /login/ HTTP/1.1" 200 3190 "http://www.loggly.com/"
"Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_2; en-us) AppleWebKit/531.21.8 (KHTML, like Gecko) Version/4.0.4 Safari/531.21.10"
TEzSVQrA4S8AAD1uoXIAAAAA 250746
kordless@logdog/> graph 404 AND inputname:logglywww
```

```
kordless@logdog/>
```

Loggly Architecture



Data Sources

Clients

Loggly user interface

Proxies

API

Data collection
Data access

Indexers and Search Machines

Distributed indexing and processing

Distributed data store

Loggly APIs

http://wiki.loggly.com/api-documentation

- URL format:

http://<***subdomain***>.loggly.com/api/<**resource**>

- RESTful API
  - Access through: /api/<**resource**>
  - JSON, XML, JSONP output
- Authentication
  - Basic auth
  - oAuth

HTTP Based

- **GET** – read
- **POST** – create
- **PUT** – update
- **DELETE** – delete

http://**loggly**.loggly.com/api/**search**/?q=error
User: guest / Password: loggly

syslog to:
logs.loggly.com:514

Search

http://[domain].loggly.com/api/search?q=404

```
{
    "data": [
        {
            "indexed": "2010-07-03T17:17:38.909Z",
            "ip": "75.101.249.172",
            "text": "Oct 13 20:00:38.018152 rule 57/0(match): pass in on xl1: 195.141.69.45.1030 > 62.2.32.250.53:  34388 [1au]
[|domain] (DF)",
            "inputname": "logglyweb",
            "timestamp": "2010-07-03 10:17:38"
        },
        {
            "indexed": "2010-07-03T17:17:37.879Z",
            "ip": "75.101.249.172",
            "text": "Oct 13 20:00:38.115862 rule 57/0(match): pass in on xl1: 195.141.69.45.1030 > 192.134.0.49.53:  49962 [1au]
[|domain] (DF)",
            "inputname": "logglyapp",
            "timestamp": "2010-07-03 10:17:37"
        },

        ...
```

Parser

Raw

```
Oct 13 20:00:38.018152 rule 57/0(match): pass in on xl1: 195.141.69.45.1030 > 62.2.32.250.53:  34388 [1au][|domain] (DF)
Oct 13 20:00:38.115862 rule 57/0(match): pass in on xl1: 195.141.69.45.1030 > 192.134.0.49.53:  49962 [1au][|domain] (DF)
Oct 13 20:00:38.157238 rule 57/0(match): pass in on xl1: 195.141.69.45.1030 > 194.25.2.133.53:  14434 [1au][|domain] (DF)
```

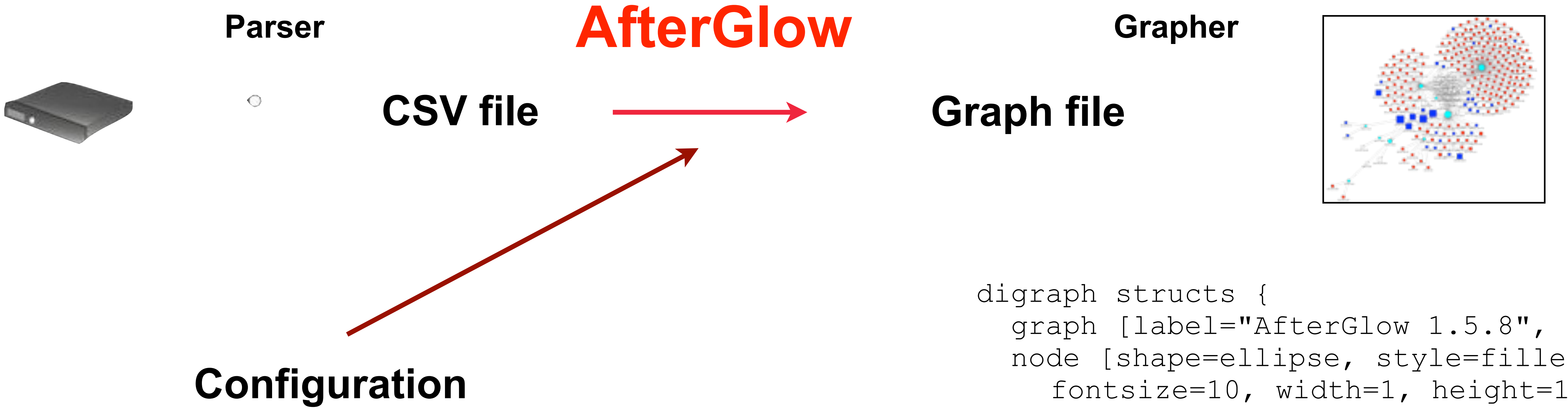
Regex / Parser

```
(.*) rule ([-\d]+\/\d+)\(.*?\): (pass|block) (in|out) on (\w+):
(\d+\.\d+\.\d+\.\d+)\.?(\d*) [<>]
(\d+\.\d+\.\d+\.\d+)\.?(\d*): (.*)
```

Normalized (CSV)

```
Oct 13 20:00:38.018152,57/0,match,pass,in,xl1,195.141.69.45,1030,62.2.32.250,53,34388 [1au][|domain] (DF)
Oct 13 20:00:38.115862,57/0,match,pass,in,xl1,195.141.69.45,1030,192.134.0.49,53,49962 [1au][|domain] (DF)
Oct 13 20:00:38.157238,57/0,match,pass,in,xl1,195.141.69.45,1030,194.25.2.133,53,14434 [1au][|domain] (DF)
```

Visualize



Parser

AfterGlow

Grapher

CSV file

Graph file

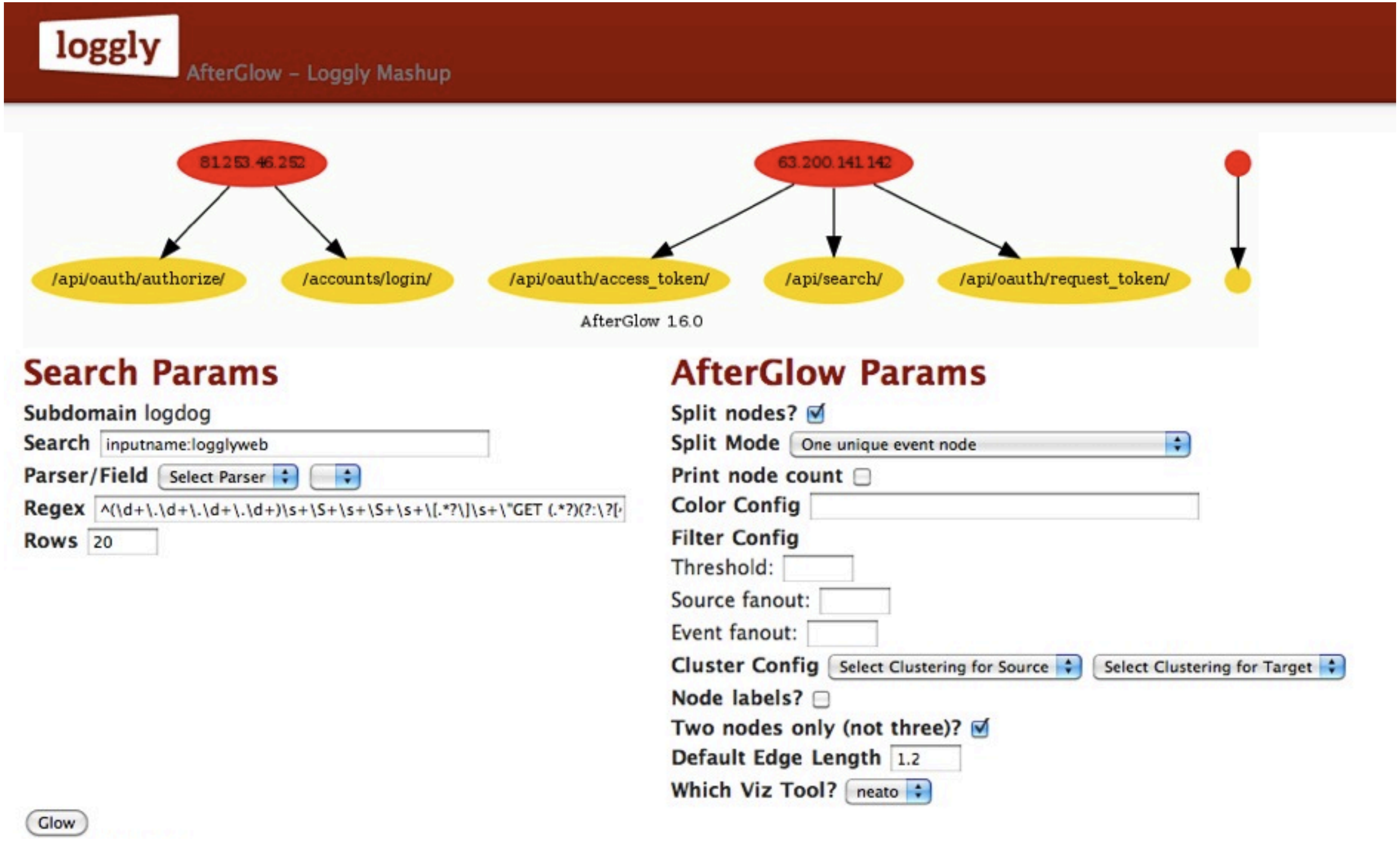
Configuration

```
color.source="green" if ($fields[0] ne "d")
cluster.target=regex_replace("(\\d\+)\\.")."/8"
threshold.event=5
size.target=$fields[1]
```

```
digraph structs {
  graph [label="AfterGlow 1.5.8",  fontsize=8];
  node [shape=ellipse, style=filled,
    fontsize=10, width=1, height=1,
    fixedsize=true];
  edge [len=1.6];

  "aaelenes" -> "Printing Resume" ;
  "abbe" -> "Information Encryption" ;
  "aanna" -> "Patent Access" ;
  "aatharuv" -> "Ping" ;
}
```

http://afterglow.sf.net

AfterGlow Cloud



Search Params

Subdomain logdog

Search inputname:logglyweb

Parser/Field Select Parser

Regex `^(\d+\.\d+\.\d+\.\d+)\s+\S+\s+\S+\s+\[.*?\]\s+\"GET (.*?)(?:\?[`

Rows 20

AfterGlow Params

Split nodes? ☑

Split Mode One unique event node

Print node count □

Color Config

Filter Config

Threshold:

Source fanout:

Event fanout:

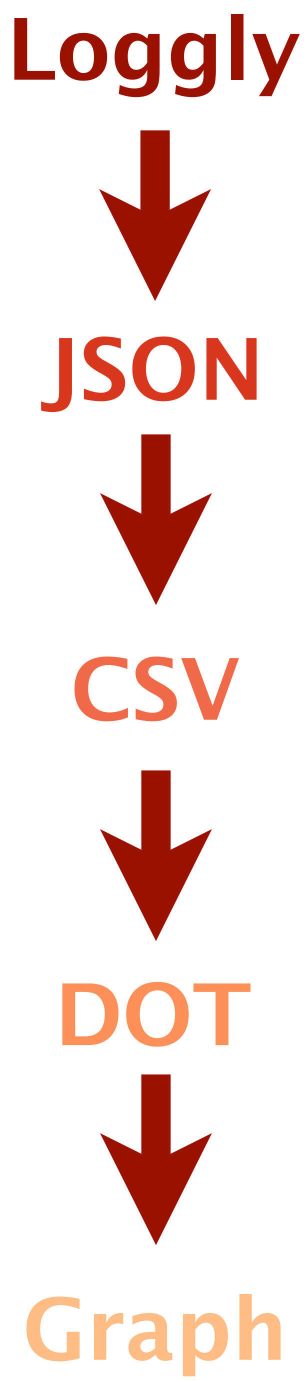
Cluster Config Select Clustering for Source | Select Clustering for Target

Node labels? □

Two nodes only (not three)? ☑

Default Edge Length 1.2

Which Viz Tool? neato



Loggly

JSON

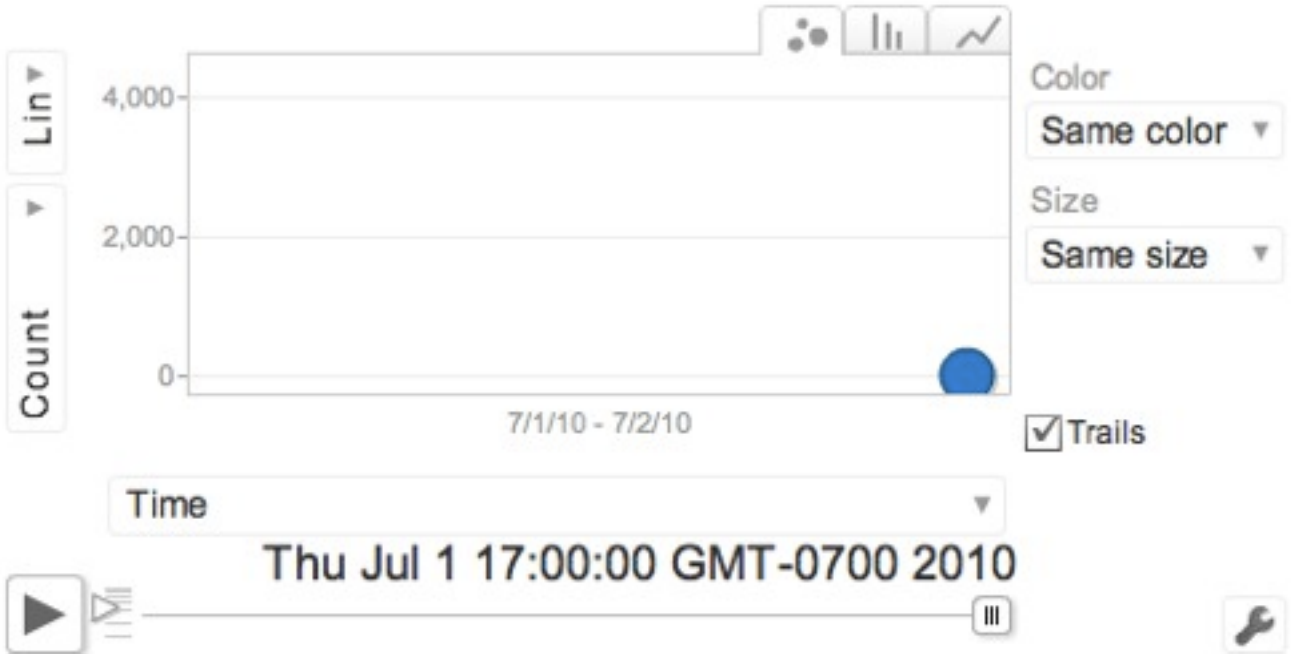
CSV

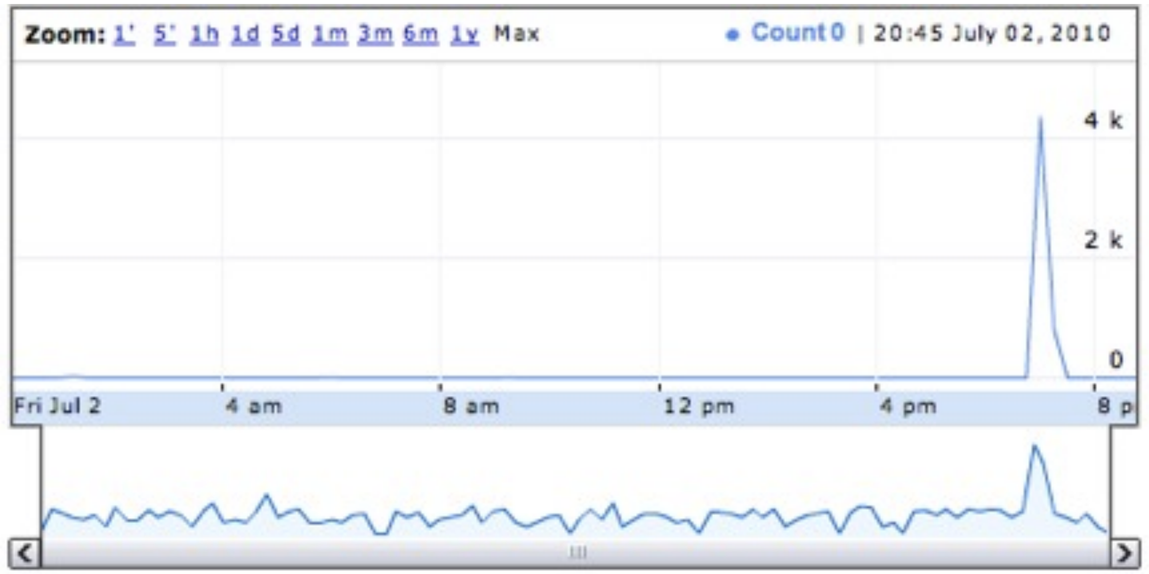
DOT

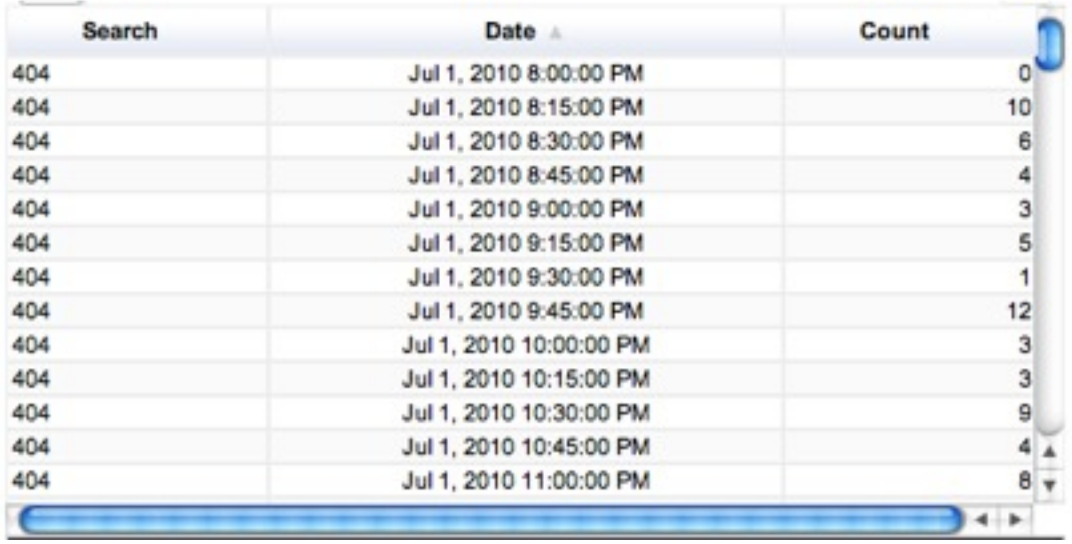
Graph

Google Vis

- JSON to Graphs
- DataTable
  - used among all charts
- Interactivity through events





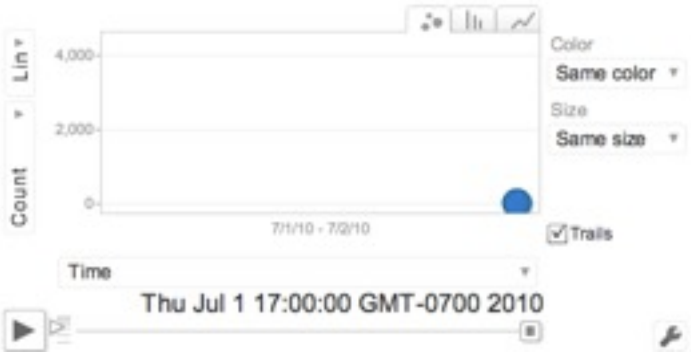


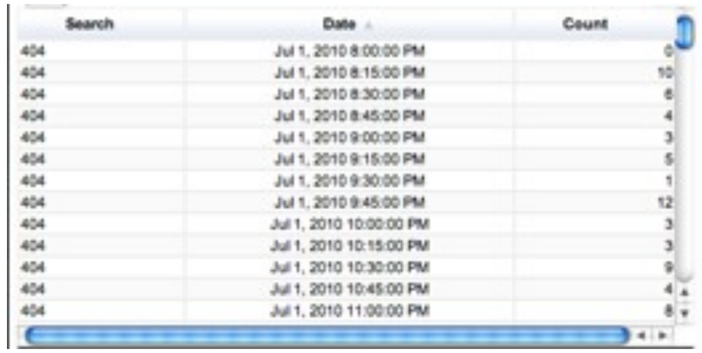
Search	Date	Count
404	Jul 1, 2010 8:00:00 PM	0
404	Jul 1, 2010 8:15:00 PM	10
404	Jul 1, 2010 8:30:00 PM	6
404	Jul 1, 2010 8:45:00 PM	4
404	Jul 1, 2010 9:00:00 PM	3
404	Jul 1, 2010 9:15:00 PM	5
404	Jul 1, 2010 9:30:00 PM	1
404	Jul 1, 2010 9:45:00 PM	12
404	Jul 1, 2010 10:00:00 PM	3
404	Jul 1, 2010 10:15:00 PM	3
404	Jul 1, 2010 10:30:00 PM	9
404	Jul 1, 2010 10:45:00 PM	4
404	Jul 1, 2010 11:00:00 PM	8

Google Vis Code

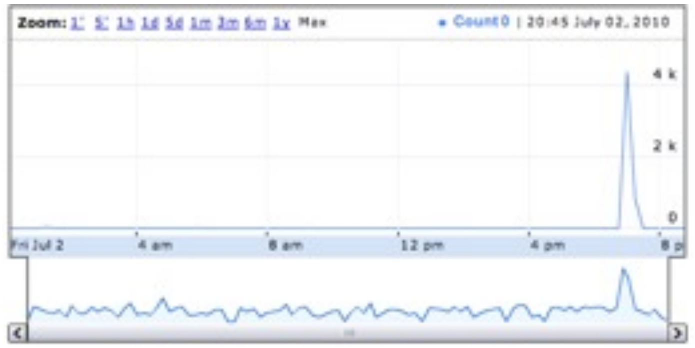
```
<script type="text/javascript">
      google.load('visualization', '1', {'packages':['motionchart', 'table', 'annotatedtimeline']});
      google.setOnLoadCallback(call);
      var trends = new Array();
      function call() {
          $.ajax({ url: "http://logdog.loggly.com/api/search/?q=404&facets=True&buckets=100",
                type:'GET',  dataType: 'jsonp', username: 'xxxxx', password: 'xxxxxx',
                success: function(data) {
                    trends = data.data
                    drawChart();
                }
          });
      }
      function drawChart() {
        var data = new google.visualization.DataTable();
        data.addColumn('string', 'Search');
        data.addColumn('datetime',   'Date');
        data.addColumn('number', 'Count');
        data.addRows(trends);

        var chart = new google.visualization.MotionChart(document.getElementById('chart_div'));
        chart.draw(data, {width: 600, height:300, state:state});

        var view = new google.visualization.DataView(data);
        view.setRows(view.getFilteredRows([{column: 1, minValue: new Date(2007, 0, 1)}]));
        var table = new google.visualization.Table(document.getElementById('test_dataview'));
        table.draw(view, {sortColumn: 1});

        var time = new google.visualization.AnnotatedTimeLine(document.getElementById('timeline'));
        time.draw(timedata, {displayAnnotations: true});
      }
</script>
```

THIS CODE IS NOT FUNCTIONAL!





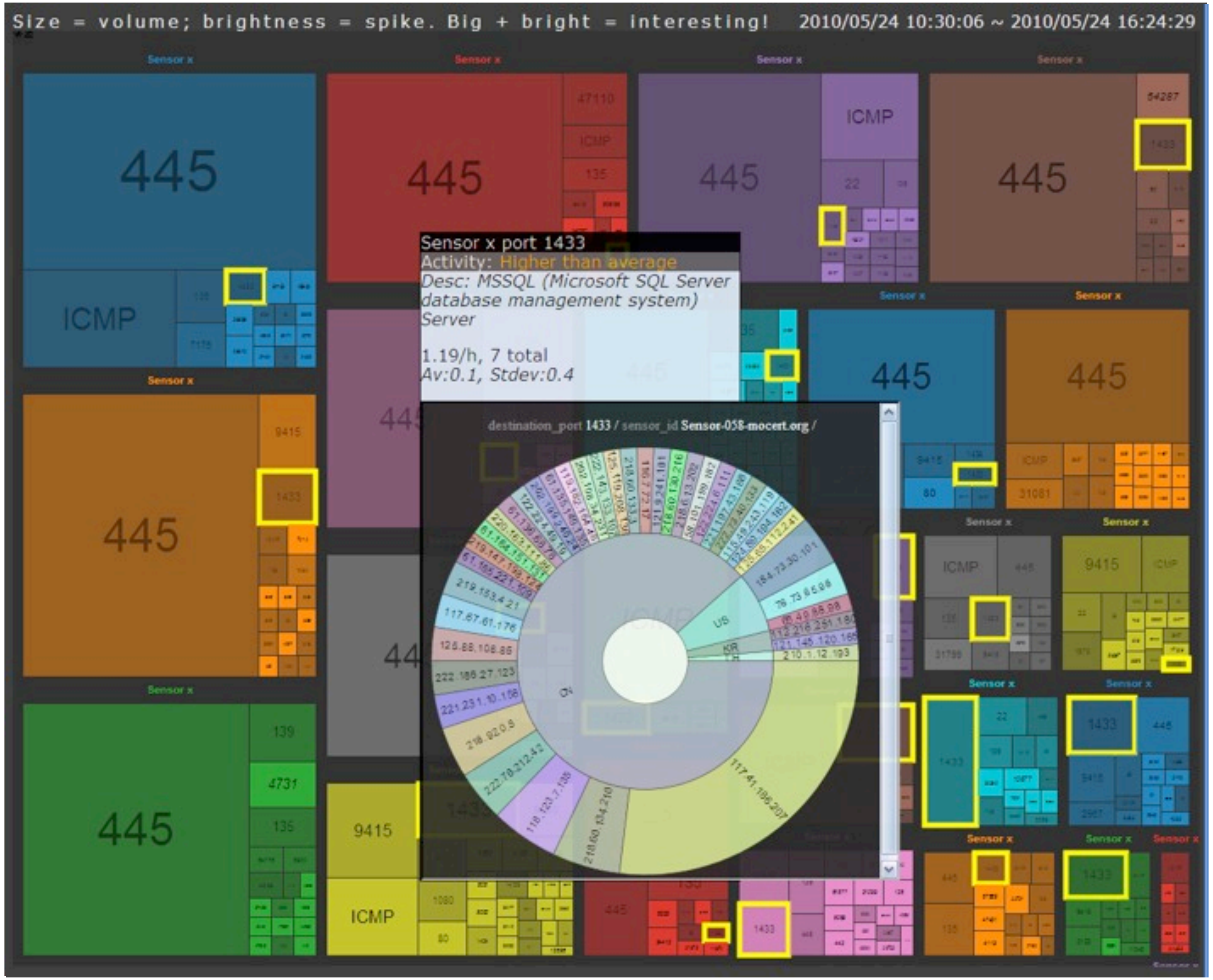
Search	Date	Count
404	Jul 1, 2010 8:00:00 PM	0
404	Jul 1, 2010 8:15:00 PM	10
404	Jul 1, 2010 8:30:00 PM	6
404	Jul 1, 2010 8:45:00 PM	4
404	Jul 1, 2010 9:00:00 PM	3
404	Jul 1, 2010 9:15:00 PM	5
404	Jul 1, 2010 9:30:00 PM	1
404	Jul 1, 2010 9:45:00 PM	12
404	Jul 1, 2010 10:00:00 PM	3
404	Jul 1, 2010 10:15:00 PM	3
404	Jul 1, 2010 10:30:00 PM	9
404	Jul 1, 2010 10:45:00 PM	4
404	Jul 1, 2010 11:00:00 PM	8


Zoom: 1' 5' 1h 1d 5d 1m 3m 6m 1y Max
● Count0 | 20:45 July 02, 2010
4 k
2 k
0
Fri Jul 2
4 am
8 am
12 pm
4 pm
8 p

Visualization Use-Cases

NetFlow Visualization

- Treemap
- Protovis.JS
- Size: Amount
- Brightness: Variance
- Color: Sensor
- Shows: Scans – bright spots



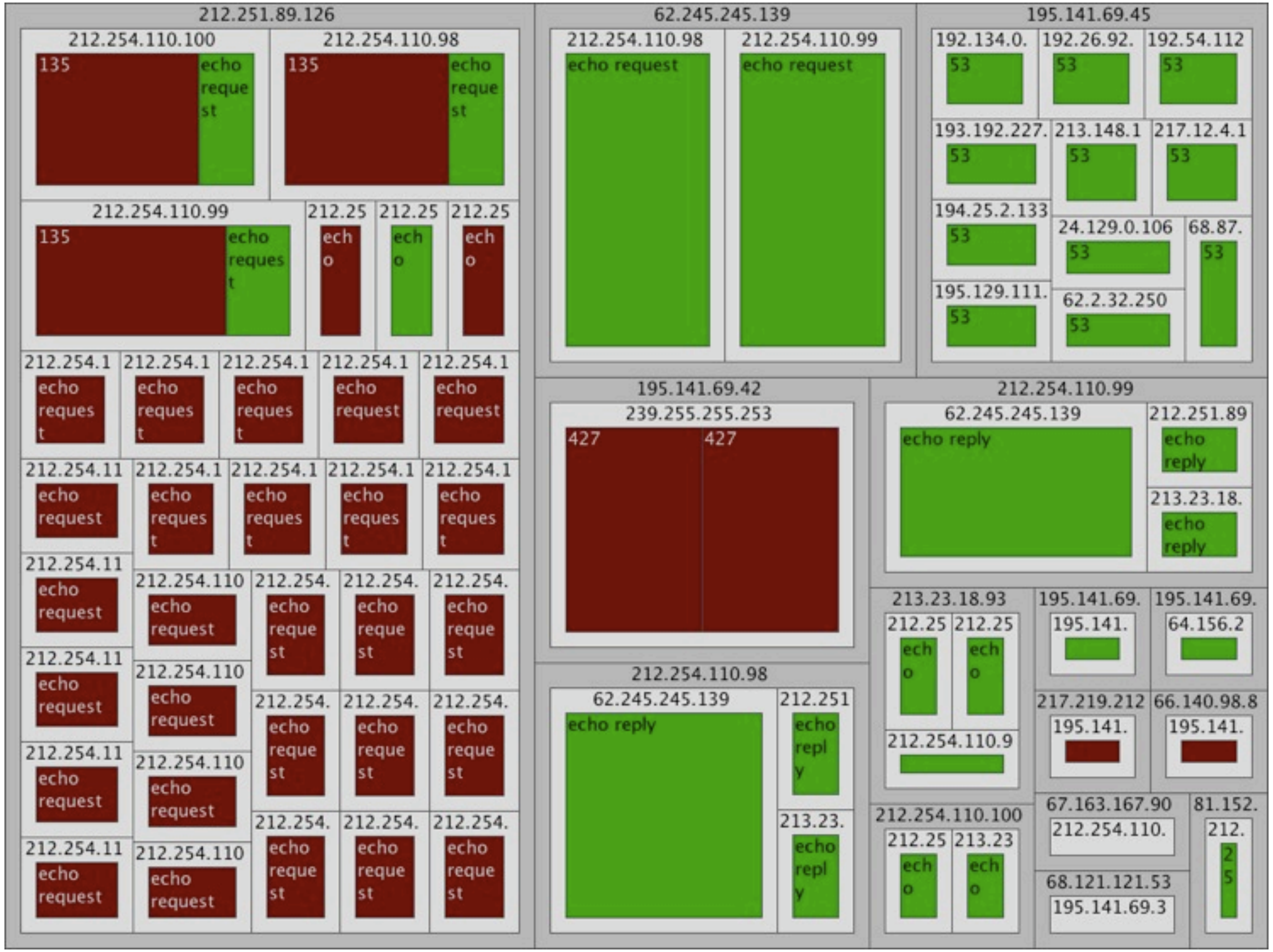
Size = volume; brightness = spike. Big + bright = interesting! 2010/05/24 10:30:06 ~ 2010/05/24 16:24:29

Sensor x port 1433
Activity: Higher than average
Desc: MSSQL (Microsoft SQL Server database management system) Server

1.19/h, 7 total
Av:0.1, Stdev:0.4

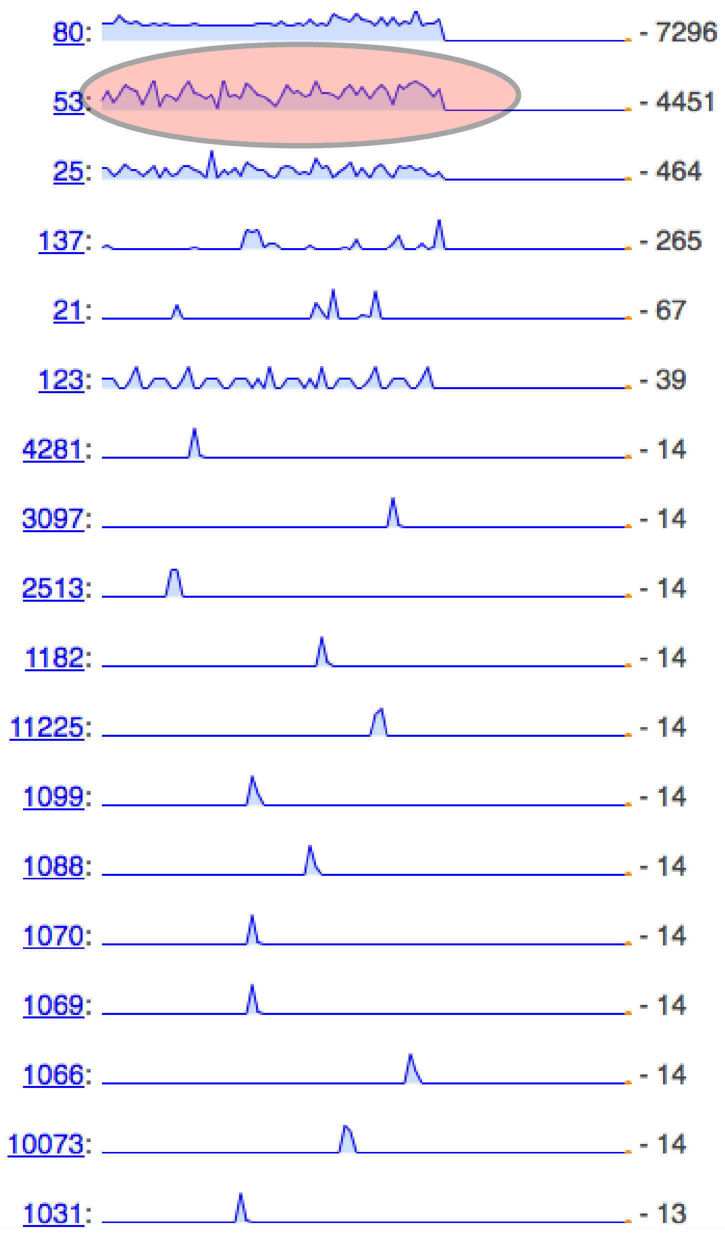
- Thanks to Chris Horsley

Firewall Treemap



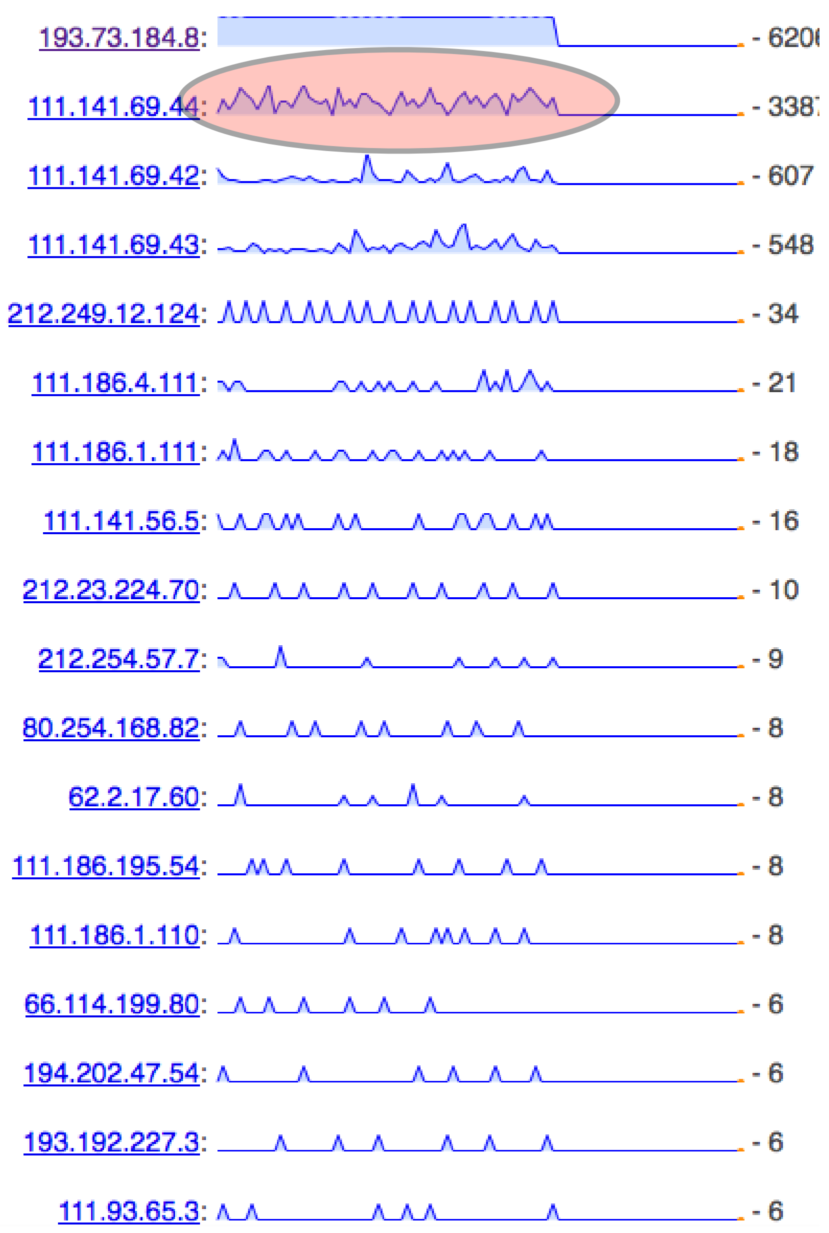
Firewall Log

Port



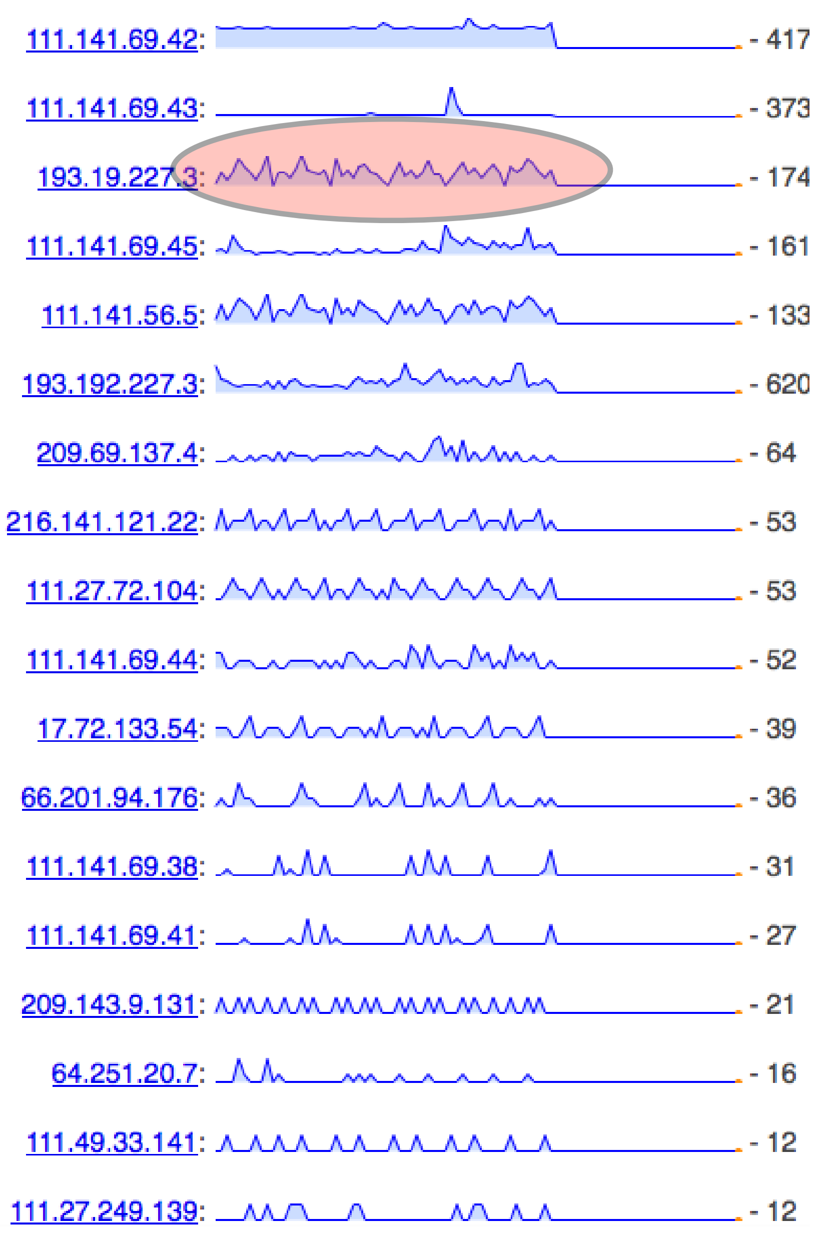
80:	- 7296
53:	- 4451
25:	- 464
137:	- 265
21:	- 67
123:	- 39
4281:	- 14
3097:	- 14
2513:	- 14
1182:	- 14
11225:	- 14
1099:	- 14
1088:	- 14
1070:	- 14
1069:	- 14
1066:	- 14
10073:	- 14
1031:	- 13

Source IP



193.73.184.8:	- 620
111.141.69.44:	- 338
111.141.69.42:	- 607
111.141.69.43:	- 548
212.249.12.124:	- 34
111.186.4.111:	- 21
111.186.1.111:	- 18
111.141.56.5:	- 16
212.23.224.70:	- 10
212.254.57.7:	- 9
80.254.168.82:	- 8
62.2.17.60:	- 8
111.186.195.54:	- 8
111.186.1.110:	- 8
66.114.199.80:	- 6
194.202.47.54:	- 6
193.192.227.3:	- 6
111.93.65.3:	- 6

Destination IP



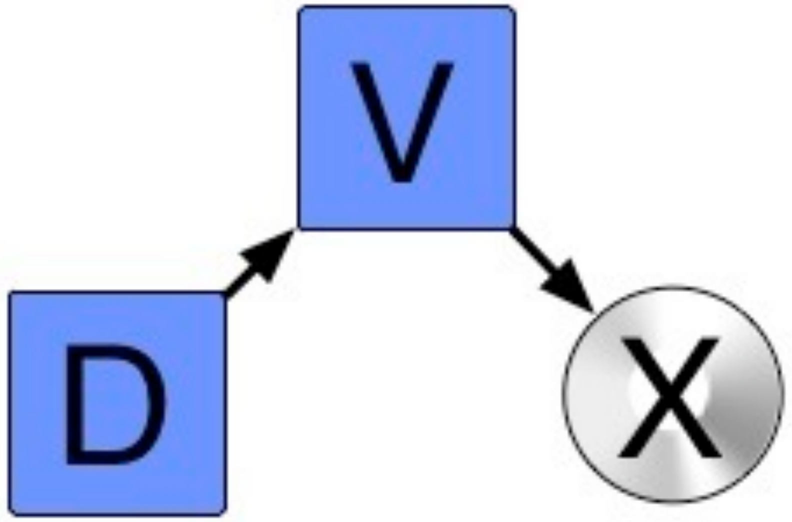
111.141.69.42:	- 417
111.141.69.43:	- 373
193.19.227.3:	- 174
111.141.69.45:	- 161
111.141.56.5:	- 133
193.192.227.3:	- 620
209.69.137.4:	- 64
216.141.121.22:	- 53
111.27.72.104:	- 53
111.141.69.44:	- 52
17.72.133.54:	- 39
66.201.94.176:	- 36
111.141.69.38:	- 31
111.141.69.41:	- 27
209.143.9.131:	- 21
64.251.20.7:	- 16
111.49.33.141:	- 12
111.27.249.139:	- 12

Visualization Resources

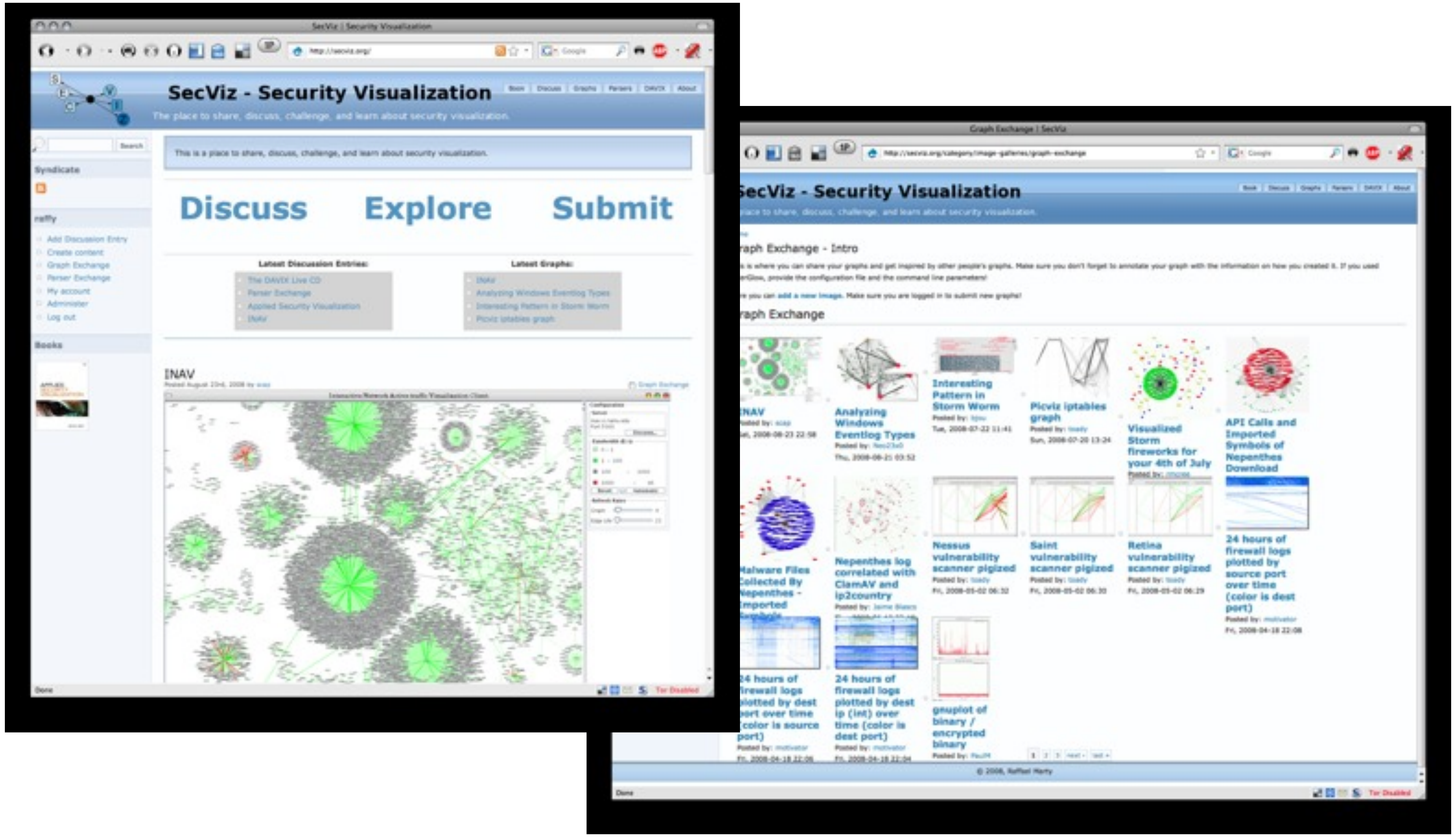
http://secviz.org

Share, discuss, challenge, and learn about security visualization.

- List: secviz.org/mailinglist
- Twitter: @secviz



davix.secviz.org


SecViz | Security Visualization
http://secviz.org/
Google
Book | Discuss | Graphs | Parsers | DAVIX | About
Search
Syndicate
raffy
Books
Done
Tor Disabled
Graph Exchange | SecViz
http://secviz.org/category/image-galleries/graph-exchange

SecViz - Security Visualization

The place to share, discuss, challenge, and learn about security visualization.

This is a place to share, discuss, challenge, and learn about security visualization.

Discuss Explore Submit

- Add Discussion Entry
- Create content
- Graph Exchange
- Parser Exchange
- My account
- Administer
- Log out

Latest Discussion Entries:

- The DAVIX Live CD
- Parser Exchange
- Applied Security Visualization
- INAV

Latest Graphs:

- INAV
- Analyzing Windows Eventlog Types
- Interesting Pattern in Storm Worm
- Picviz iptables graph

INAV

Posted August 23rd, 2008 by scap

Graph Exchange

Interactive Network Active-traffic Visualization Client

ecViz - Security Visualization

ace to share, discuss, challenge, and learn about security visualization.

raph Exchange - Intro

s is where you can share your graphs and get inspired by other people's graphs. Make sure you don't forget to annotate your graph with the information on how you created it. If you used erGlow, provide the configuration file and the command line parameters!

e you can add a new image. Make sure you are logged in to submit new graphs!

raph Exchange

INAV Posted by: scap Sat, 2008-08-23 22:58

Analyzing Windows Eventlog Types Posted by: Neo23x0 Thu, 2008-08-21 03:52

Interesting Pattern in Storm Worm Posted by: bjou Tue, 2008-07-22 11:41

Picviz iptables graph Posted by: toady Sun, 2008-07-20 13:24

Visualized Storm fireworks for your 4th of July Posted by: ohnoes

API Calls and Imported Symbols of Nepenthes Download

Malware Files Collected By Nepenthes - Imported Symbols

Nepenthes log correlated with ClamAV and ip2country Posted by: Jaime Blasco

Nessus vulnerability scanner pigized Posted by: toady Fri, 2008-05-02 06:32

Saint vulnerability scanner pigized Posted by: toady Fri, 2008-05-02 06:30

Retina vulnerability scanner pigized Posted by: toady Fri, 2008-05-02 06:29

24 hours of firewall logs plotted by source port over time (color is dest port) Posted by: motivator Fri, 2008-04-18 22:08

24 hours of firewall logs plotted by dest port over time (color is source port) Posted by: motivator Fri, 2008-04-18 22:06

24 hours of firewall logs plotted by dest ip (int) over time (color is dest port) Posted by: motivator Fri, 2008-04-18 22:04

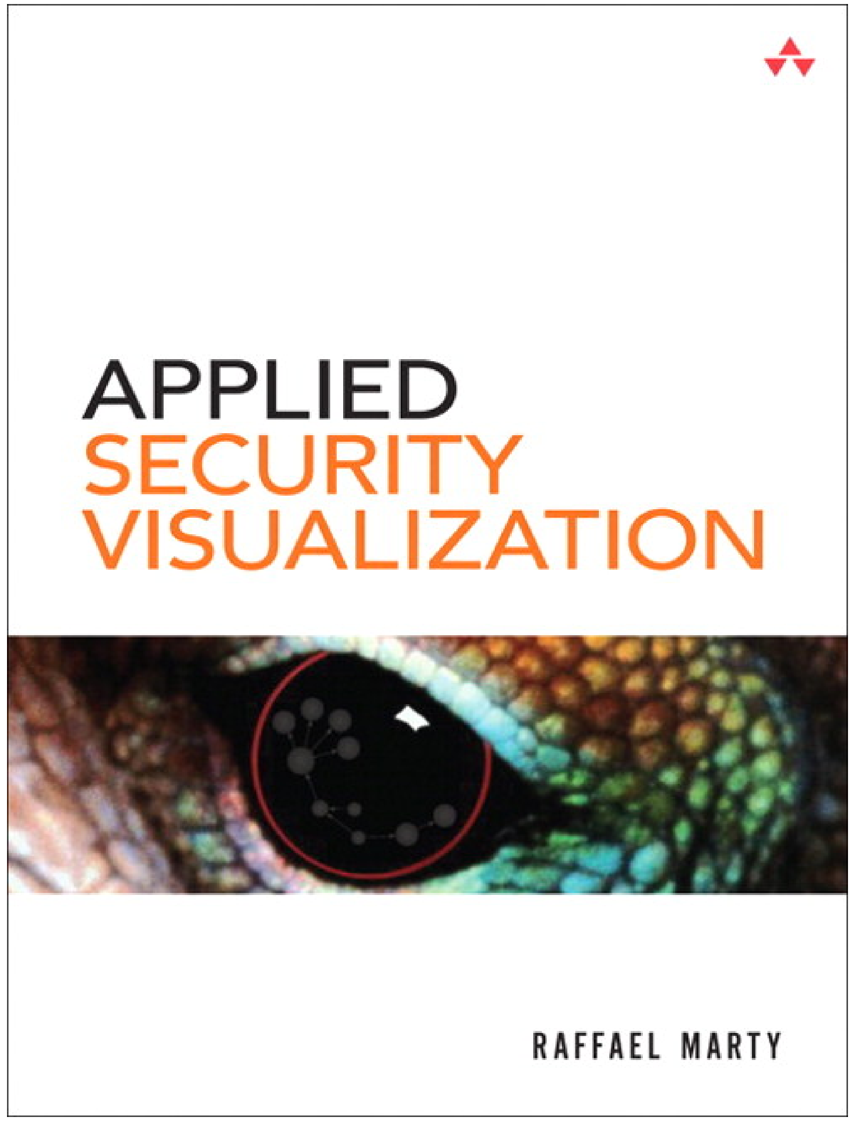
gnuplot of binary / encrypted binary Posted by: PaulM

1 2 3 next › last »

© 2008, Raffael Marty

Applied Security Visualization

- Bridging the gap between security and visualization
- Hands-on, end to end examples
- Data processing and analysis



Chapters

- Visualization
- Data Sources
- From Data to Graphs
- Perimeter Threat
- Compliance
- Insider Threat
- Visualization Tools

Addison Wesley (August, 2008)
ISBN: 0321510100

Thank You!

loggly

raffael.marty@loggly.com
@zrlram