



Large-scale Network Monitoring for Visual Analysis of Attacks

Fabian Fischer, Florian Mansmann, Daniel A. Keim, Stephan Pietzko, Marcel Waldvogel
University of Konstanz, Germany

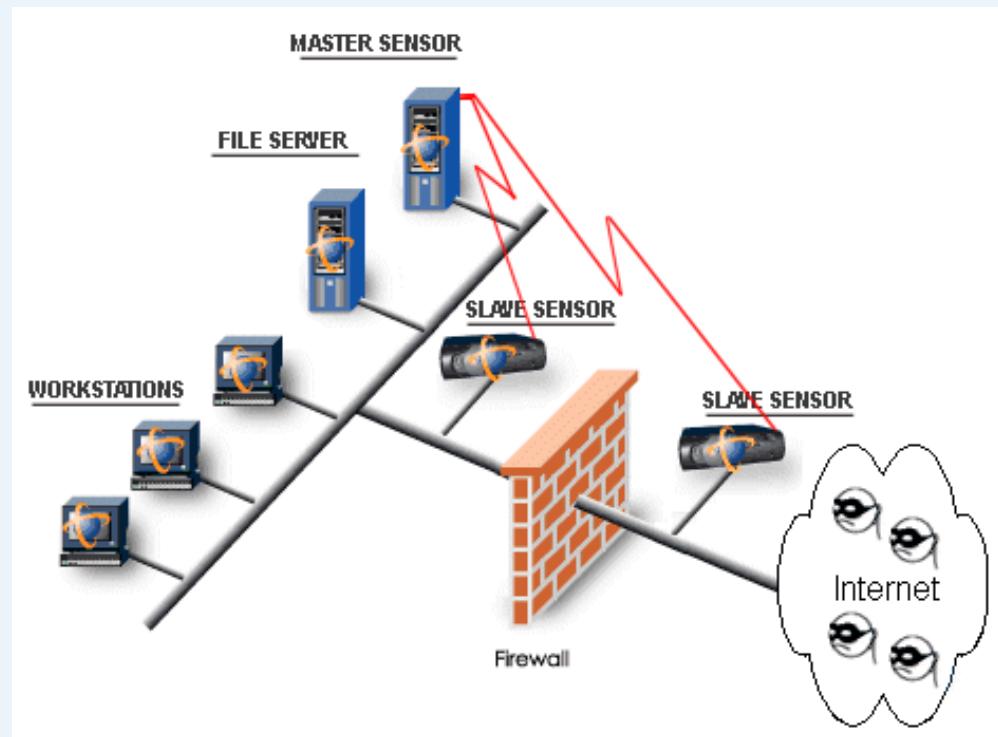
Presenter: Robin Berthier, University of Maryland, College Park

VizSec 2008 - Workshop on Visualization for Computer Security



Intrusion Detection and Network Monitoring

- Network protection by
 - Firewalls
 - Intrusion Detection
 - Network Monitoring
- Problem:
Intrusion Detection and Network Monitoring lead to *very large* number of alerts



How can we support the users of Intrusion Detection System and Network Monitoring Systems to understand the threat situation?







NFlowVis Project

2008-05-11

| Attribute | Value |
|----------------|-----------------------|
| Flows | 61.123.671 |
| Start Time | 2008-05-10 23:59:51.0 |
| End Time | 2008-05-12 00:00:00.0 |
| Packets | 850.117.587 |
| Payload | 408,51 GiB |
| Source IP | 1.295.531 |
| Destination IP | 1.324.219 |

Anonymized NetFlow Traffic

IANA Assignments | Network Tools
Host Details Lookup | Communication Lookup

Quick Host Details Lookup

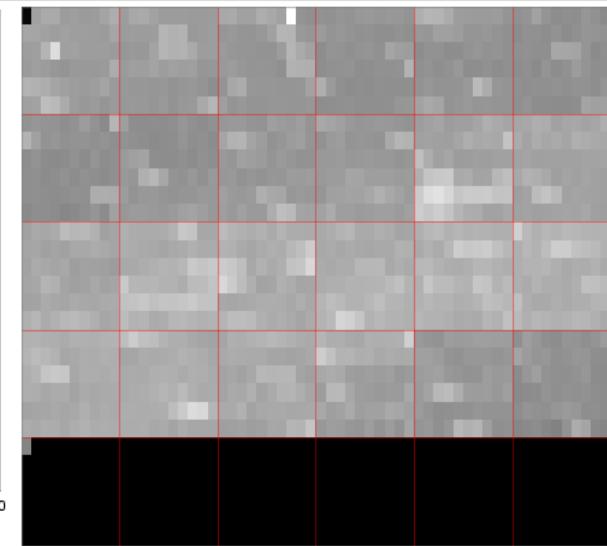
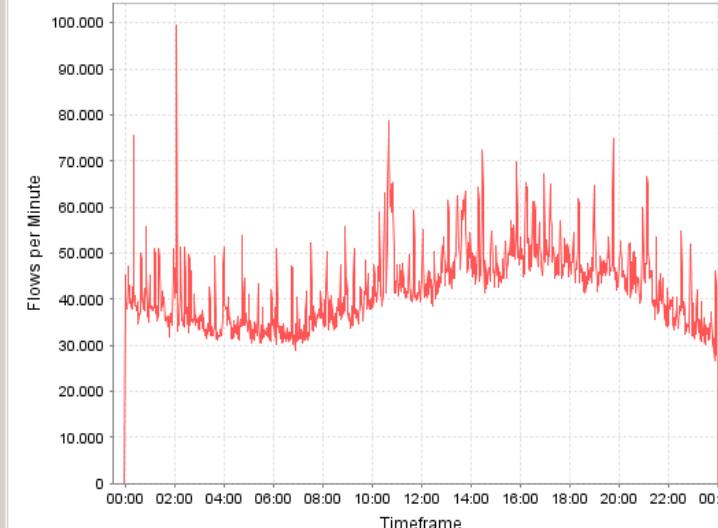
dstaddr

Raw Records

1. Overview | 2. Intrusion Detection View | 3. Flow Visualization | 4. Host Details | 5. NetFlow Records |

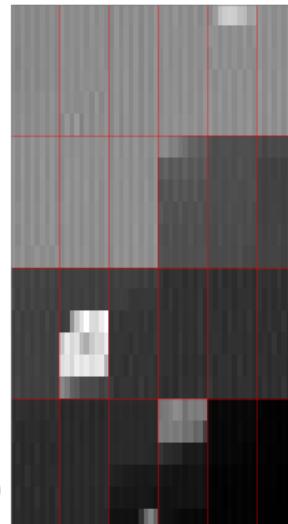
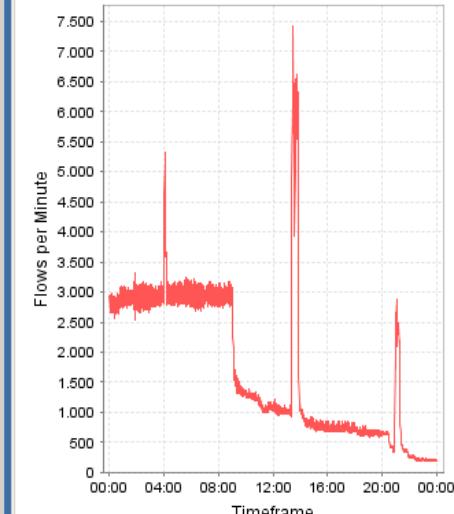
Load User Defined Overview Plots

Flows per Minute

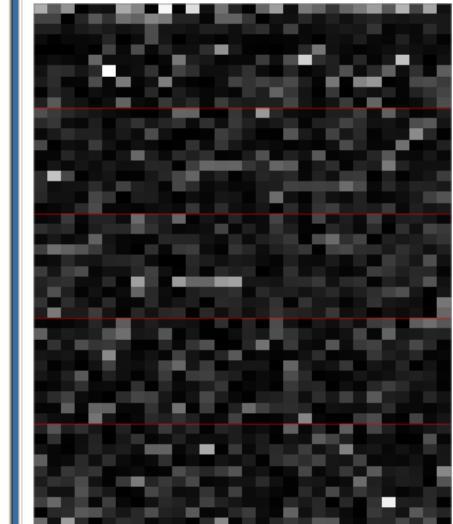


Scale: SQUARE_ROOT

SSH Traffic



Port Usage (TOP 1500)



Scale: LOG



NFlowVis Project

2008-04-02

| Attribute | Value |
|----------------|-----------------------|
| Flows | 108.142.800 |
| Start Time | 2008-04-01 23:59:55.0 |
| End Time | 2008-04-03 00:00:00.0 |
| Packets | 2.007.256.358 |
| Payload | 1.238,35 GB |
| Source IP | 2.877.353 |
| Destination IP | 2.890.423 |

| Anonymized NetFlow Traffic | |
|--------------------------------------|----------------------|
| IANA Assignments | Network Tools |
| Host Details Lookup | Communication Lookup |
| Quick Host Details Lookup | |
| dstaddr | |
| <input type="text"/> | |
| <input type="checkbox"/> Raw Records | |
| | Lookup |

1. Overview | 2. Intrusion Detection View | 3. Flow Visualization | 4. Host Details | 5. NetFlow Records |

IDS Data Source

Aggregated SNORT IDS Alerts

Suspicious Hosts | Template Settings |

Refresh Host List

| srcaddr | msg | typesofalert | alerts | count | hostcount | dpkts | doctets |
|-----------------|----------------------------|--------------|--------|---------|-----------|------------|---------------|
| 134.34.20.4 | ICMP PING | 1 | 5.986 | 25.024 | 11.954 | 576.235 | 169.466.288 |
| 207.175.63.182 | ICMP PING CyberKit 2.... | 1 | 1 | 2.626 | 2.102 | 73.389 | 4.404.492 |
| 134.34.3.28 | ICMP Destination Unreac... | 1 | 2 | 278.642 | 1.823 | 37.215.369 | 5.364.153.538 |
| 134.34.3.26 | ICMP PING,ICMP PING ... | 3 | 2.247 | 3.922 | 534 | 2.681.391 | 567.543.102 |
| 134.34.3.24 | ICMP PING,ICMP PING ... | 3 | 1.355 | 3.607 | 531 | 2.575.695 | 380.845.863 |
| 134.34.3.34 | ICMP PING,ICMP PING ... | 3 | 6.250 | 3.160 | 523 | 1.780.706 | 278.255.455 |
| 134.34.3.15 | ICMP Destination Unreac... | 1 | 44 | 1.856 | 490 | 236.003 | 17.959.080 |
| 65.114.168.149 | ICMP PING NMAP | 1 | 7 | 377 | 362 | 381 | 16.194 |
| 65.114.168.151 | ICMP PING | 1 | 5 | 379 | 361 | 384 | 16.458 |
| 65.114.168.148 | ICMP PING,ICMP PING ... | 2 | 15 | 372 | 355 | 373 | 15.628 |
| 65.114.168.150 | ICMP PING,ICMP PING ... | 2 | 11 | 388 | 353 | 978 | 38.436 |
| 128.9.160.71 | ICMP PING,ICMP PING ... | 2 | 11 | 334 | 322 | 337 | 14.386 |
| 128.9.160.144 | ICMP PING,ICMP PING ... | 2 | 19 | 320 | 307 | 323 | 13.634 |
| 88.170.221.149 | ICMP Echo Reply | 1 | 3 | 154 | 154 | 168 | 15.456 |
| 195.188.216.34 | ICMP PING | 1 | 2 | 84 | 81 | 86 | 3.788 |
| 196.28.58.116 | ICMP PING,ICMP PING ... | 2 | 2 | 72 | 67 | 74 | 5.242 |
| 196.28.58.114 | ICMP PING,ICMP PING ... | 2 | 2 | 65 | 62 | 475 | 31.258 |
| 193.87.127.158 | ICMP PING | 1 | 2 | 51 | 49 | 51 | 2.220 |
| 209.77.220.12 | ICMP PING,ICMP PING ... | 2 | 4 | 48 | 46 | 49 | 4.508 |
| 194.176.105.29 | ICMP PING,ICMP PING ... | 2 | 3 | 113 | 37 | 336 | 29.179 |
| 203.127.16.49 | ICMP PING CyberKit 2.... | 1 | 3 | 37 | 36 | 37 | 3.404 |
| 128.9.160.145 | ICMP PING | 1 | 6 | 37 | 36 | 37 | 1.540 |
| 64.90.198.25 | ICMP PING,ICMP PING ... | 2 | 3 | 37 | 35 | 40 | 3.548 |
| 67.130.40.130 | ICMP PING CyberKit 2.... | 1 | 1 | 32 | 30 | 34 | 3.128 |
| 217.171.129.125 | ICMP PING,ICMP PING ... | 2 | 2 | 1.508 | 30 | 2.963 | 557.943 |
| 134.34.57.27 | ICMP redirect host | 1 | 87 | 50 | 30 | 3.532 | 222.776 |
| 67.62.129.4 | ICMP PING CyberKit 2.... | 1 | 3 | 27 | 27 | 27 | 2.484 |
| 74.59.15.127 | ICMP PING NMAP | 1 | 1 | 43 | 24 | 49 | 2.438 |
| 134.34.53.119 | ICMP Destination Unreac... | 6 | 49 | 2.082 | 23 | 330.219 | 30.619.596 |
| 129.143.1.2 | ICMP Time-To-Live Exc... | 1 | 6 | 24 | 23 | 251 | 18.322 |
| 203.116.51.147 | ICMP PING,ICMP PING ... | 2 | 5 | 22 | 22 | 22 | 2.024 |
| 207.250.107.244 | ICMP PING CyberKit 2.... | 1 | 1 | 23 | 22 | 23 | 2.116 |
| 72.163.216.33 | ICMP PING,ICMP PING ... | 2 | 5 | 23 | 22 | 23 | 2.116 |
| 168.226.40.79 | ICMP PING CyberKit 2.... | 1 | 2 | 24 | 21 | 229 | 21.068 |
| 134.34.3.27 | ICMP Destination Unreac... | 1 | 9 | 259 | 21 | 1.861 | 355.846 |
| 8.7.69.224 | ICMP PING,ICMP PING ... | 2 | 2 | 26 | 20 | 30 | 3.695 |
| 194.24.158.236 | ICMP PING,ICMP PING ... | 2 | 4 | 193 | 20 | 614 | 75.733 |
| 129.143.47.162 | ICMP Time-To-Live Exc... | 1 | 9 | 23 | 20 | 7.600 | 736.680 |
| 75.2.197.81 | ICMP PING CyberKit 2.... | 1 | 2 | 21 | 20 | 21 | 1.932 |

Visual Connection Analysis

 Ignore single flow connections Include any traffic between hosts



NFlowVis Project

2008-04-02

| Attribute | Value |
|----------------|-----------------------|
| Flows | 108.142.800 |
| Start Time | 2008-04-01 23:59:55.0 |
| End Time | 2008-04-03 00:00:00.0 |
| Packets | 2.007.256.358 |
| Payload | 1.238,35 GB |
| Source IP | 2.877.353 |
| Destination IP | 2.890.423 |

Anonymized NetFlow Traffic

[IANA Assignments](#) | [Network Tools](#)
[Host Details Lookup](#) | [Communication Lookup](#)

Quick Host Details Lookup

dstaddr

 Raw Records
Lookup
[1. Overview](#) | [2. Intrusion Detection View](#) | [3. Flow Visualization](#) | [4. Host Details](#) | [5. NetFlow Records](#)

Colormap

HSB SW (Linear)

2.0 1603.0

Treemap Algorithm

Squarified

Value

flowcounter

Weight

Value Attribut (mapped to color and spline width)

flowcounter

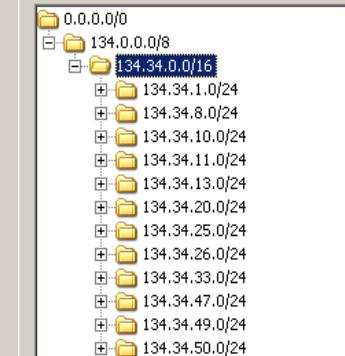
Spline Threshold: > 0

Remote Hosts

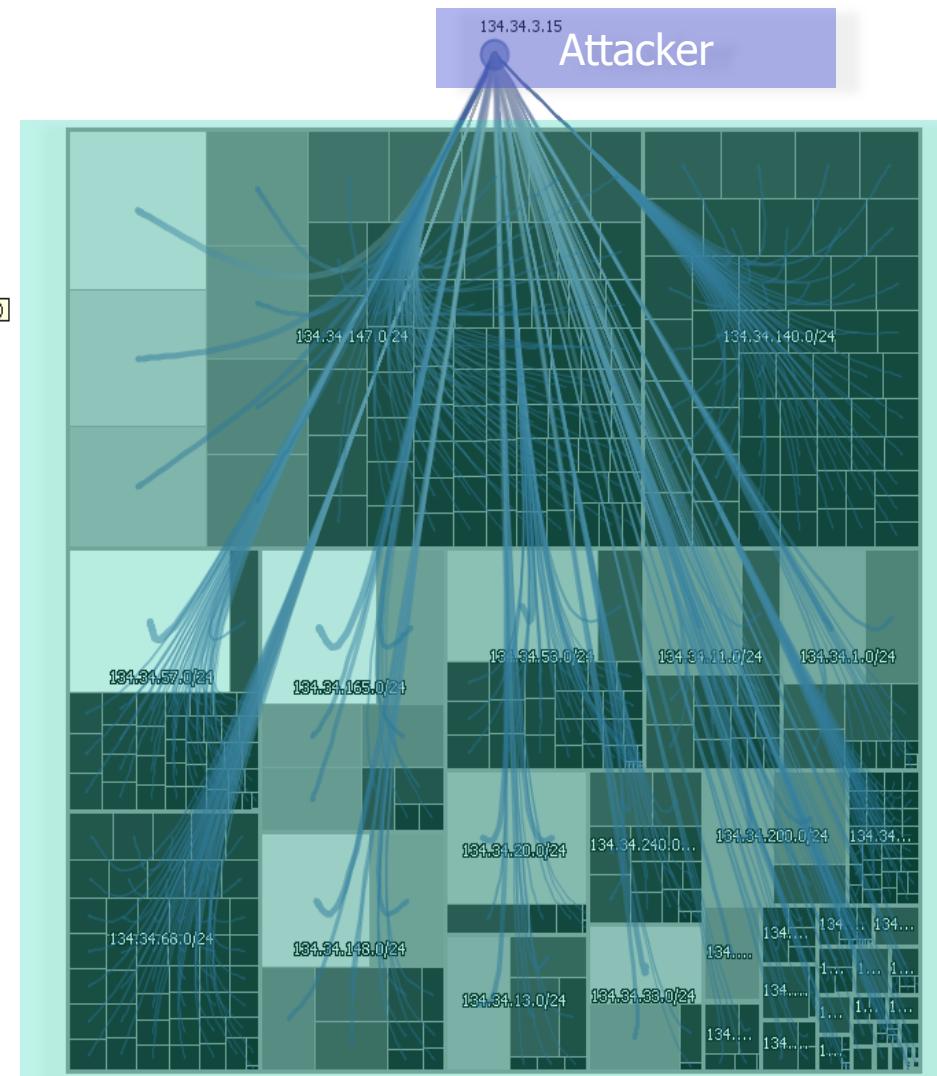
 134.34.3.15

Spline Alpha Value

Local Destination Subnets & Hosts



445 Nodes, 425 Splines, 1 Hosts



Monitored LAN (subdivided into subnets)

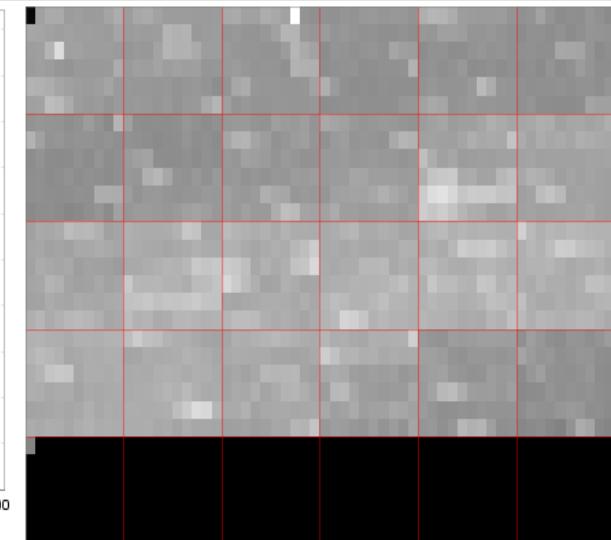
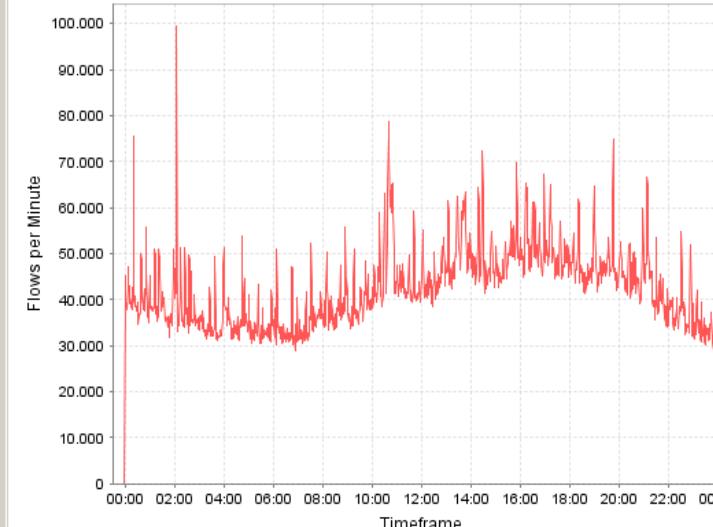


NFlowVis Project

[1. Overview](#) | [2. Intrusion Detection View](#) | [3. Flow Visualization](#) | [4. Host Details](#) | [5. NetFlow Records](#)

Load User Defined Overview Plots

Flows per Minute



IANA Assignments | Network Tools

Host Details Lookup | Communication Lookup

Quick Host Details Lookup

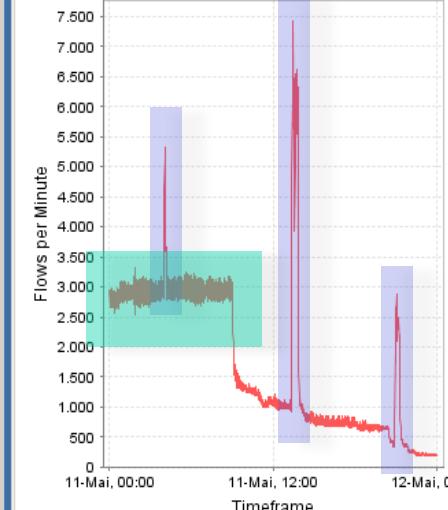
dstaddr

88.191.24.94

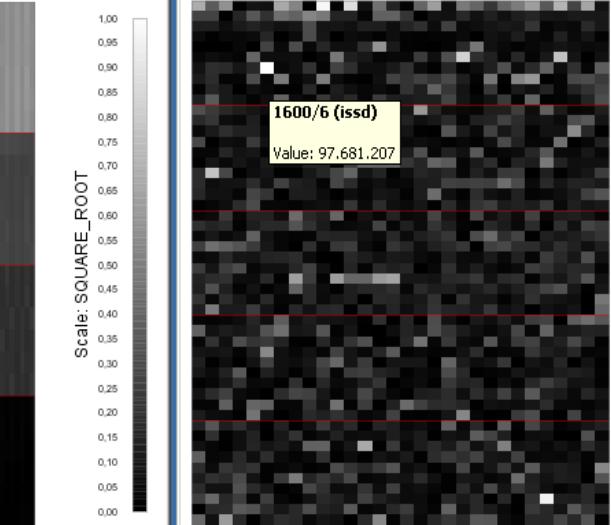
Raw Records

Lookup

SSH Traffic



Port Usage (TOP 1500)



1. Overview | 2. Intrusion Detection View | 3. Flow Visualization | 4. Host Details | 5. NetFlow Records



NFlowVis Project

| 2008-05-11 | |
|----------------|-----------------------|
| Attribute | Value |
| Flows | 61.123.671 |
| Start Time | 2008-05-10 23:59:51.0 |
| End Time | 2008-05-12 00:00:00.0 |
| Packets | 850.117.587 |
| Payload | 408.51 GB |
| Source IP | 1.295.531 |
| Destination IP | 1.324.219 |

| Anonymized NetFlow Traffic | |
|----------------------------|---------------|
| IANA Assignments | Network Tools |

| | |
|---|---|
| IANA Assignments | Network Tools |
| Host Details Lookup | Communication Lookup |
| Quick Host Details Lookup | |
| <input style="width: 100px; border: 1px solid black; padding: 2px; margin-right: 10px;" type="text" value="dstaddr"/> 141.24.32.1 | <input style="margin-right: 10px;" type="checkbox" value="Raw Records"/> Raw Records <input style="border: 1px solid black; padding: 2px; width: 100px;" type="button" value="Lookup"/> |

1. Overview | 2. Intrusion Detection View | 3. Flow Visualization | 4. Host Details | 5. NetFlow Records |

IDS Data Source

Brute Scan Attacker (SSH)

[Suspicious Hosts](#) | [Template Settings](#) |

| srcaddr | Distinct LAN Hosts | Packets | Octets |
|----------------|--------------------|------------|---------------|
| 141.24.32.1 | 59,417 | 946,729 | 86,462,138 |
| 81.5.209.67 | 16,512 | 402,077 | 37,270,034 |
| 75.30.242.48 | 10,162 | 45,458 | 3,833,076 |
| 157.1.129.19 | 129 | 26,382,276 | 2,509,479,374 |
| 12.25.93.200 | 47 | 3,932 | 354,512 |
| 60.19.28.237 | 47 | 1,700 | 163,608 |
| 61.125.195.220 | 47 | 2,656 | 252,100 |
| 62.72.101.21 | 47 | 1,704 | 164,424 |
| 62.97.204.105 | 47 | 2,453 | 237,756 |
| 62.112.222.238 | 47 | 859 | 82,576 |
| 62.118.68.64 | 47 | 1,722 | 166,536 |
| 62.159.113.126 | 47 | 1,341 | 127,626 |
| 62.167.18.238 | 47 | 2,804 | 260,128 |
| 62.233.185.119 | 47 | 1,098 | 105,968 |
| 66.134.26.39 | 47 | 1,890 | 181,684 |
| 66.159.198.247 | 47 | 3,464 | 335,192 |
| 66.193.161.225 | 47 | 4,478 | 432,564 |
| 67.125.255.167 | 47 | 2,445 | 236,288 |
| 68.112.226.152 | 47 | 1,719 | 164,596 |
| 69.60.118.182 | 47 | 1,941 | 188,264 |
| 69.67.164.201 | 47 | 2,605 | 252,332 |
| 69.104.213.18 | 47 | 2,570 | 248,540 |
| 69.159.224.175 | 47 | 1,886 | 181,158 |
| 80.22.111.130 | 47 | 1,706 | 163,164 |
| 80.53.126.251 | 47 | 2,594 | 249,072 |
| 80.152.135.192 | 47 | 2,691 | 259,922 |
| 80.161.109.221 | 47 | 1,702 | 164,016 |
| 80.177.241.225 | 47 | 850 | 81,804 |
| 80.201.241.43 | 47 | 861 | 83,268 |
| 81.45.223.94 | 47 | 849 | 82,074 |
| 81.73.179.127 | 47 | 883 | 86,172 |
| 81.183.215.67 | 47 | 859 | 82,860 |
| 81.210.83.14 | 47 | 1,702 | 164,016 |
| 81.219.193.229 | 47 | 1,701 | 164,296 |
| 82.73.18.83 | 47 | 1,702 | 164,016 |
| 82.106.69.133 | 47 | 852 | 82,012 |
| 82.119.244.210 | 47 | 963 | 91,944 |
| 82.127.35.88 | 47 | 1,828 | 175,156 |
| 82.186.188.210 | 47 | 2,209 | 213,152 |
| 82.200.66.250 | 47 | 8,553 | 7,547,374 |

Visual Connection Analysis

Ignore single flow connections

Include any traffic between hosts



NFlowVis Project

2008-04-02

| Attribute | Value |
|----------------|-----------------------|
| Flows | 108,142,800 |
| Start Time | 2008-04-01 23:59:55.0 |
| End Time | 2008-04-03 00:00:00.0 |
| Packets | 2,007,256,358 |
| Payload | 1,238,35 GB |
| Source IP | 2.877.353 |
| Destination IP | 2.890.423 |

Anonymized NetFlow Traffic

IANA Assignments | Network Tools

Quick Host Details Lookup

| | |
|--------------------------------------|---------------------------------------|
| dstaddr | <input type="button" value="Lookup"/> |
| 220.177.248.87 | |
| <input type="checkbox"/> Raw Records | |

1. Overview | 2. Intrusion Detection View | 3. Flow Visualization | 4. Host Details | 5. NetFlow Records |

Colormap

HSB SW (Linear)

2.0 44.0

Treemap Algorithm

Squarified

Value

flowcounter

Weight

packetcounter

Spline Threshold: > 0



Remote Hosts

 88.191.24.94 91.64.37.160 220.177.248.87

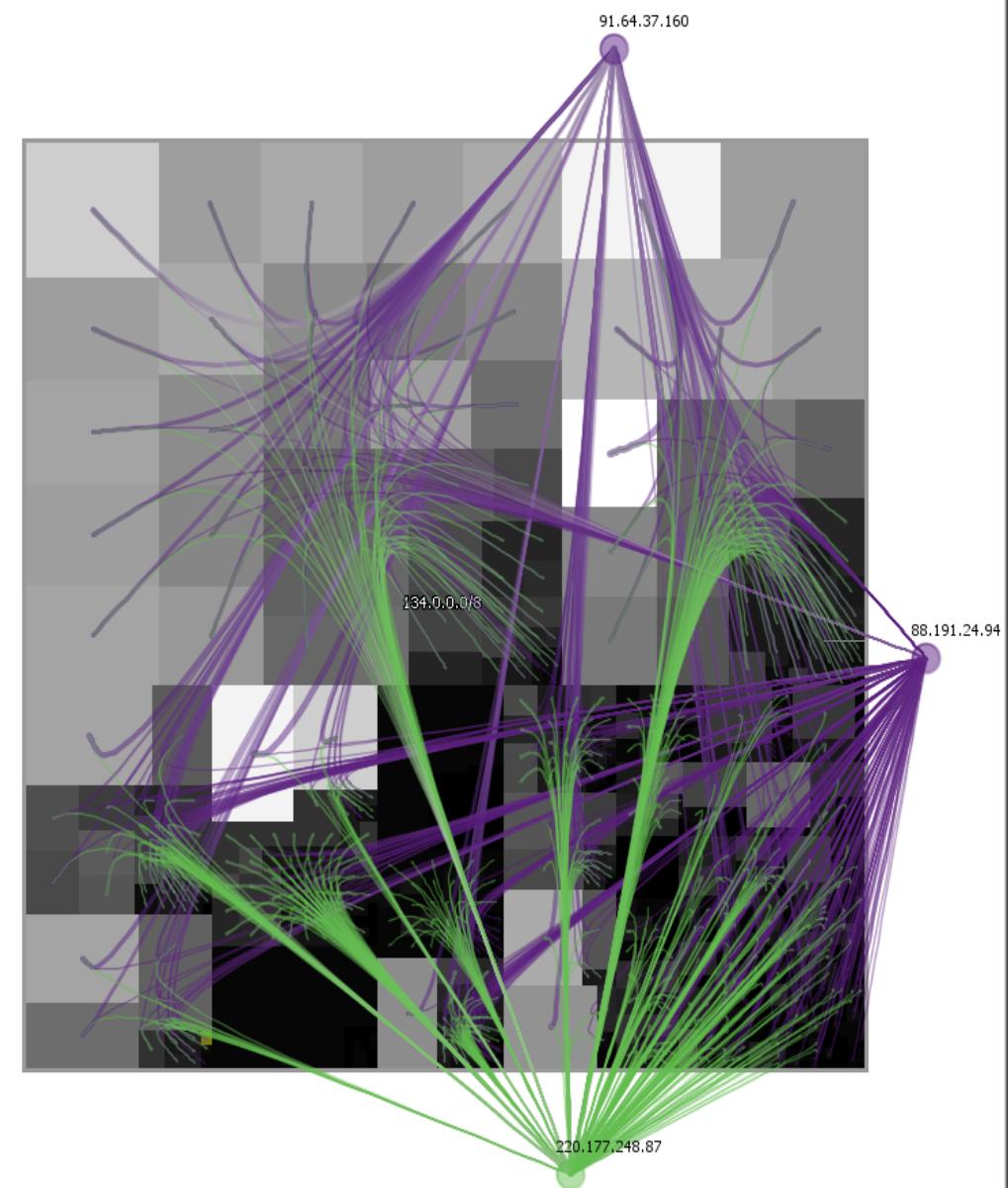
Spline Alpha Value



Local Destination Subnets & Hosts

- 📁 0.0.0.0/0
- +📁 134.0.0.0/8

1510 Nodes, 1164 Splines, 3 Hosts





NFlowVis Project

| 2008-05-11 | |
|----------------|-----------------------|
| Attribute | Value |
| Flows | 61.123.671 |
| Start Time | 2008-05-10 23:59:51.0 |
| End Time | 2008-05-12 00:00:00.0 |
| Packets | 850.117.587 |
| Payload | 408.51 GB |
| Source IP | 1.295.531 |
| Destination IP | 1.324.219 |

| Anonymized NetFlow Traffic | |
|----------------------------|---------------|
| IANA Assignments | Network Tools |

| | |
|--|---------------------------------------|
| IANA Assignments | Network Tools |
| Host Details Lookup | Communication Lookup |
| Quick Host Details Lookup | |
| <input type="button" value="dstaddr"/> <input type="text" value="141.24.32.1"/> <input type="checkbox"/> Raw Records | <input type="button" value="Lookup"/> |

1. Overview | 2. Intrusion Detection View | 3. Flow Visualization | 4. Host Details | 5. NetFlow Records |

IDS Data Source

Brute Scan Attacker (SSH)

[Suspicious Hosts](#) | [Template Settings](#) |

| srcaddr | Distinct LAN Hosts | Packets | Octets |
|----------------|--------------------|------------|---------------|
| 141.24.32.1 | 59.417 | 946.729 | 86.462.138 |
| 81.5.209.67 | 16.512 | 402.077 | 37.270.034 |
| 75.30.242.48 | 10.162 | 45.458 | 3.833.076 |
| 157.1.129.19 | 129 | 26.382.276 | 2.509.479.374 |
| 12.25.93.200 | 47 | 3.932 | 354.512 |
| 60.19.28.237 | 47 | 1.700 | 163.608 |
| 61.125.195.220 | 47 | 2.656 | 252.100 |
| 62.72.101.21 | 47 | 1.704 | 164.424 |
| 62.97.204.105 | 47 | 2.453 | 237.756 |
| 62.112.222.238 | 47 | 859 | 82.576 |
| 62.118.68.64 | 47 | 1.722 | 166.536 |
| 62.159.113.126 | 47 | 1.341 | 127.626 |
| 62.167.18.238 | 47 | 2.804 | 260.128 |
| 62.233.185.119 | 47 | 1.098 | 105.968 |
| 66.134.26.39 | 47 | 1.890 | 181.684 |
| 66.159.198.247 | 47 | 3.464 | 335.192 |
| 66.193.161.225 | 47 | 4.478 | 432.564 |
| 67.125.255.167 | 47 | 2.445 | 236.288 |
| 68.112.226.152 | 47 | 1.719 | 164.596 |
| 69.60.118.182 | 47 | 1.941 | 188.264 |
| 69.67.164.201 | 47 | 2.605 | 252.332 |
| 69.104.213.18 | 47 | 2.570 | 248.540 |
| 69.159.224.175 | 47 | 1.886 | 181.158 |
| 80.22.111.130 | 47 | 1.706 | 163.164 |
| 80.53.126.251 | 47 | 2.594 | 249.072 |
| 80.152.135.192 | 47 | 2.691 | 259.922 |
| 80.161.109.221 | 47 | 1.702 | 164.016 |
| 80.177.241.225 | 47 | 850 | 81.804 |
| 80.201.241.43 | 47 | 861 | 83.268 |
| 81.45.223.94 | 47 | 849 | 82.074 |
| 81.73.179.127 | 47 | 883 | 86.172 |
| 81.183.215.67 | 47 | 859 | 82.860 |
| 81.210.83.14 | 47 | 1.702 | 164.016 |
| 81.219.193.229 | 47 | 1.701 | 164.296 |
| 82.73.18.83 | 47 | 1.702 | 164.016 |
| 82.106.69.133 | 47 | 852 | 82.012 |
| 82.119.244.210 | 47 | 963 | 91.944 |
| 82.127.35.88 | 47 | 1.828 | 175.156 |
| 82.186.188.210 | 47 | 2.209 | 213.152 |
| 82.200.22.250 | 47 | 8.553 | 215.312 |

Visual Connection Analysis

Ignore single flow connections Include any traffic between hosts



NFlowVis Project

2008-05-11

| Attribute | Value |
|----------------|-----------------------|
| Flows | 61.123.671 |
| Start Time | 2008-05-10 23:59:51.0 |
| End Time | 2008-05-12 00:00:00.0 |
| Packets | 850.117.587 |
| Payload | 408,51 GB |
| Source IP | 1.295.531 |
| Destination IP | 1.324.219 |

Anonymized NetFlow Traffic

 IANA Assignments | Network Tools
 Host Details Lookup | Communication Lookup

Quick Host Details Lookup

| | |
|--------------------------------------|---|
| dstaddr | <input type="text" value="200.80.203.252"/> |
| <input type="checkbox"/> Raw Records | |

Lookup

1. Overview | 2. Intrusion Detection View | 3. Flow Visualization | 4. Host Details | 5. NetFlow Records

Colormap

HSB SW (Linear)

221.0 760.0

Treemap Algorithm

Squarified

Value

flowcounter

Weight

flowcounter

Spline Threshold: > 0



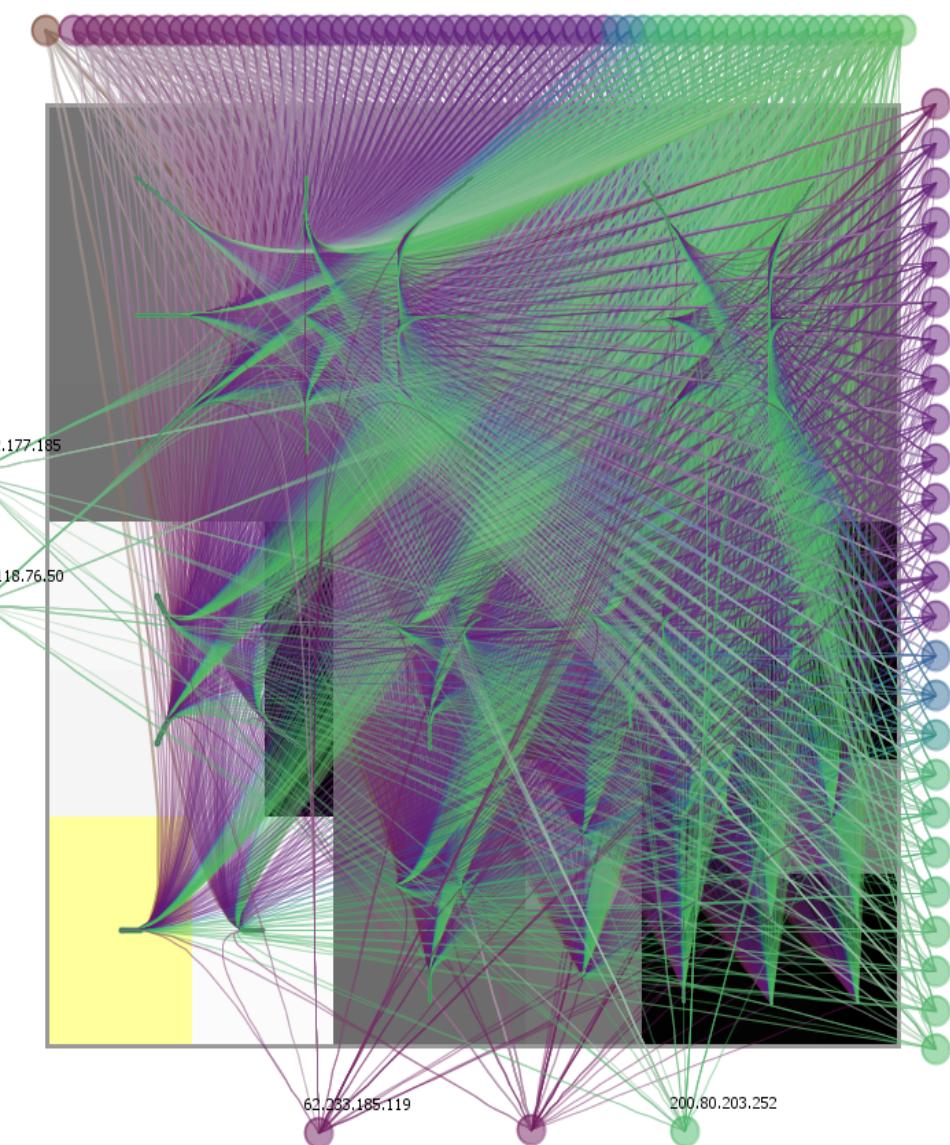
Remote Hosts

- 12.25.93.200
- 60.19.28.237
- 61.125.195.220
- 62.72.101.21
- 62.97.204.105
- 62.112.222.236
- 62.118.68.64

Spline Alpha Value



Local Destination Subnets & Hosts





NFlowVis Project

2008-05-11

| Attribute | Value |
|----------------|-----------------------|
| Flows | 61.123.671 |
| Start Time | 2008-05-10 23:59:51.0 |
| End Time | 2008-05-12 00:00:00.0 |
| Packets | 850.117.587 |
| Payload | 408.51 GB |
| Source IP | 1.295.531 |
| Destination IP | 1.324.219 |

Anonymized NetFlow Traffic

IANA Assignments | Network Tools
 Host Details Lookup Communication Lookup

Quick Host Details Lookup

| | |
|--------------------------------------|--|
| dstaddr | <input type="text" value="202.118.76.50"/> |
| <input type="checkbox"/> Raw Records | |

Lookup

[1. Overview](#) | [2. Intrusion Detection View](#) | [3. Flow Visualization](#) | [4. Host Details](#) | [5. NetFlow Records](#) |

Colormap

HSB SW (Linear)

221.0 760.0

Tremap Algorithm

Squarified

Value

flowcounter

Weight

flowcounter

Spline Threshold: > 0



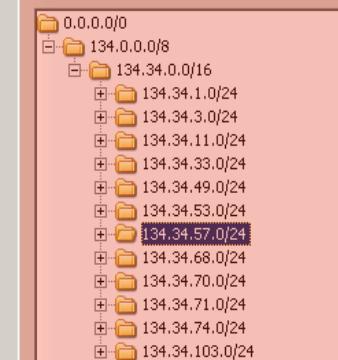
Remote Hosts

- 12.25.93.200
- 60.19.28.237
- 61.125.195.220
- 62.72.101.21
- 62.97.204.105
- 62.112.222.238
- 62.118.68.64

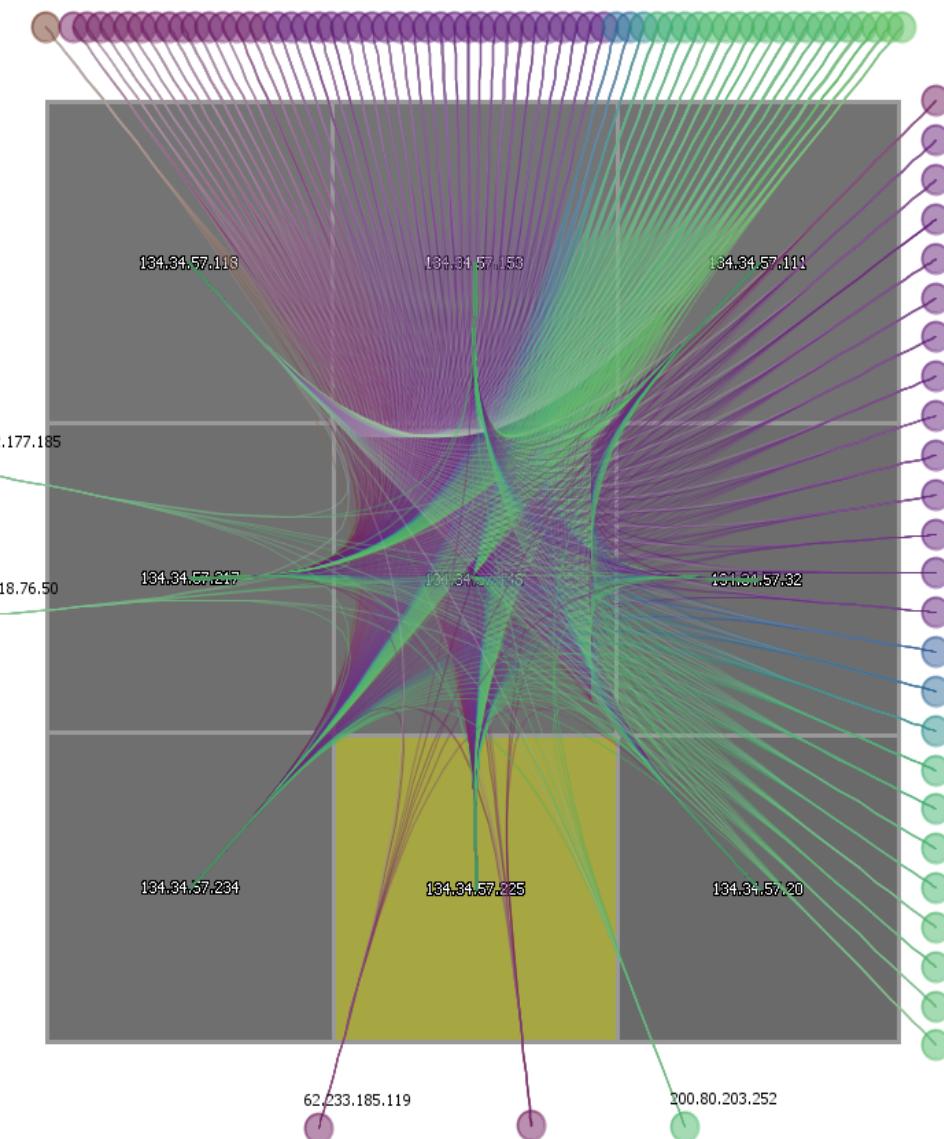
Spline Alpha Value



Local Destination Subnets & Hosts



45 Nodes, 837 Splines, 93 Hosts





NFlowVis Project

2008-05-11

| Attribute | Value |
|----------------|-----------------------|
| Flows | 61.123.671 |
| Start Time | 2008-05-10 23:59:51.0 |
| End Time | 2008-05-12 00:00:00.0 |
| Packets | 850.117.587 |
| Payload | 408.51 GB |
| Source IP | 1.295.531 |
| Destination IP | 1.324.219 |

Anonymized NetFlow Traffic

[IANA Assignments](#) | [Network Tools](#)
[Host Details Lookup](#) | [Communication Lookup](#)

Quick Host Details Lookup

dstaddr

 Raw Records
[1. Overview](#) | [2. Intrusion Detection View](#) | [3. Flow Visualization](#) | [4. Host Details](#) | [5. NetFlow Records](#)

Colormap

HSB SW (Linear)

221.0 760.0

Treemap Algorithm

Squarified

Value

flowcounter

Weight

flowcounter

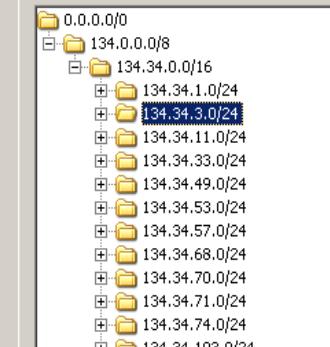
Spline Threshold: > 0

Remote Hosts

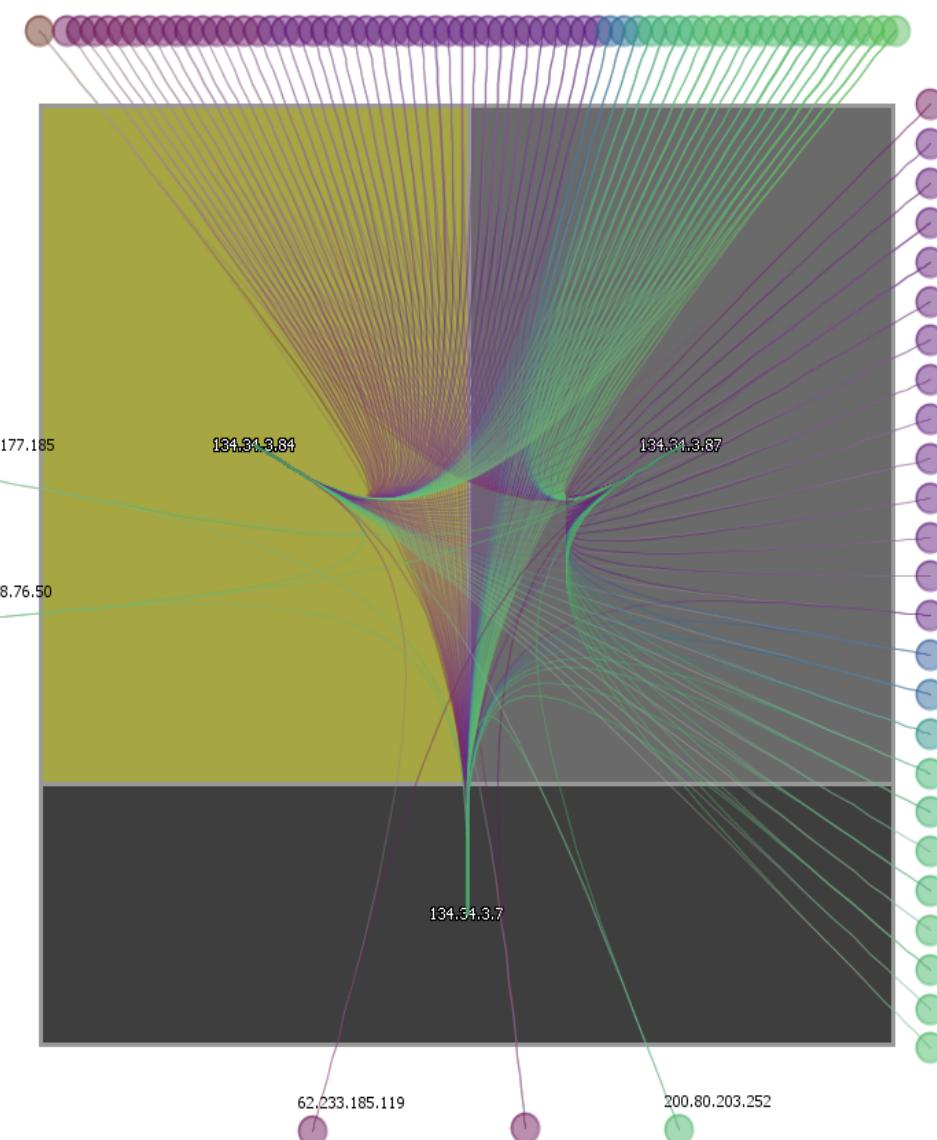
- 12.25.93.200
- 60.19.28.237
- 61.125.195.220
- 62.72.101.21
- 62.97.204.105
- 62.112.222.236
- 62.118.68.64

Spline Alpha Value

Local Destination Subnets & Hosts



45 Nodes, 263 Splines, 93 Hosts





NFlowVis Project

2008-05-11

| Attribute | Value |
|----------------|-----------------------|
| Flows | 61.123.671 |
| Start Time | 2008-05-10 23:59:51.0 |
| End Time | 2008-05-12 00:00:00.0 |
| Packets | 850.117.587 |
| Payload | 408.51 GB |
| Source IP | 1.295.531 |
| Destination IP | 1.324.219 |

Anonymized NetFlow Traffic

IANA Assignments | Network Tools
 Host Details Lookup | Communication Lookup

Quick Host Details Lookup

| | |
|--------------------------------------|--|
| dstaddr | <input type="text" value="202.118.76.50"/> |
| <input type="checkbox"/> Raw Records | |

Lookup

[1. Overview](#) | [2. Intrusion Detection View](#) | [3. Flow Visualization](#) | [4. Host Details](#) | [5. Netflow Records](#)

Colormap

HSB SW (Linear)

221.0 760.0

Treemap Algorithm

Squarified

Value

flowcounter

Weight

flowcounter

Spline Threshold: > 0

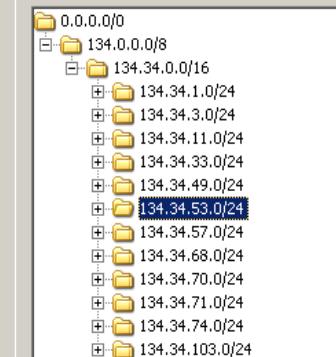
<

Remote Hosts

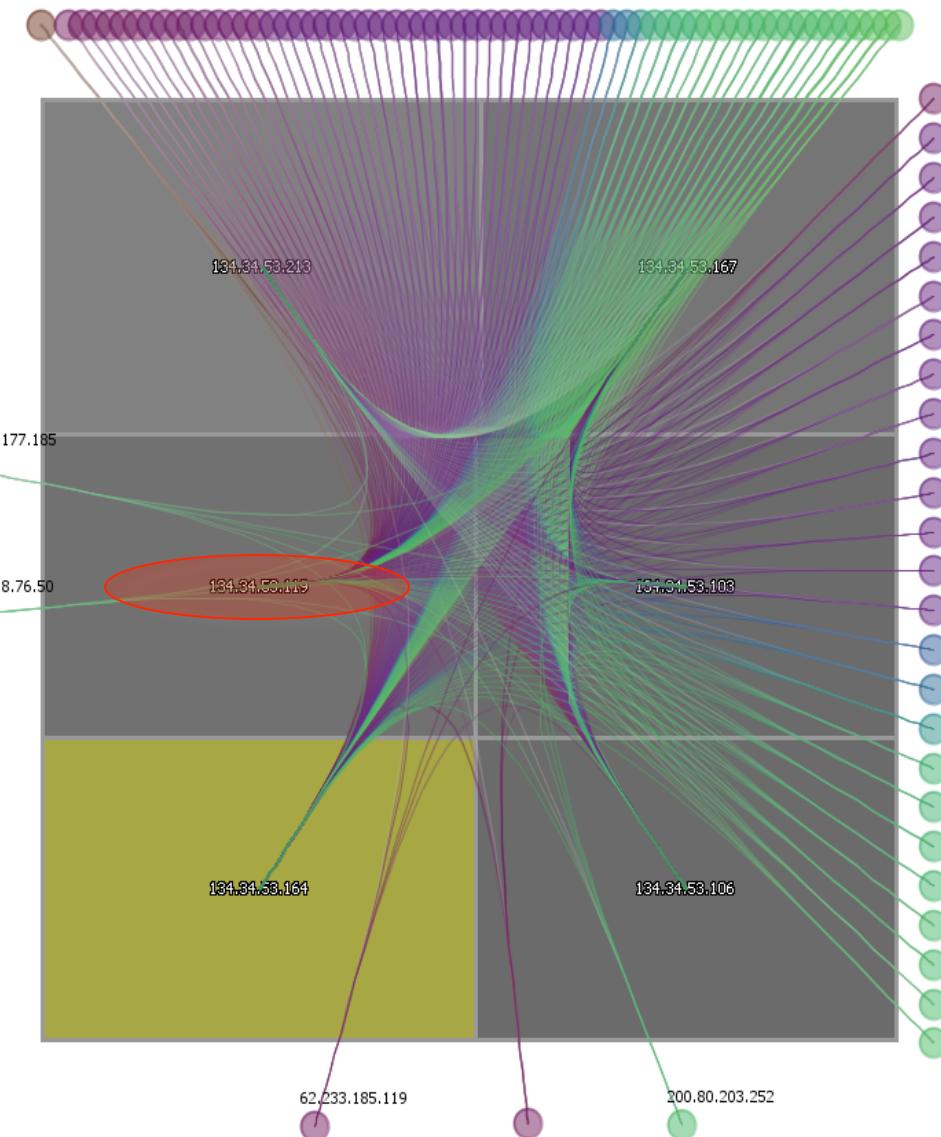
- 12.25.93.200
- 60.19.28.237
- 61.125.195.220
- 62.72.101.21
- 62.97.204.105
- 62.112.222.236
- 62.118.68.64

Spline Alpha Value

Local Destination Subnets & Hosts



45 Nodes, 558 Splines, 93 Hosts



NFlowVis Project

2008-05-20

| Attribute | Value |
|----------------|-----------------------|
| Flows | 96,890,302 |
| Start Time | 2008-05-19 23:59:53.0 |
| End Time | 2008-05-20 23:59:59.0 |
| Packets | 2,281,253,947 |
| Payload | 1,568,99 GB |
| Source IP | 2.534.519 |
| Destination IP | 2.587.215 |

Anonymized NetFlow Traffic

[IANA Assignments](#) | [Network Tools](#)
[Host Details Lookup](#) | [Communication Lookup](#)

Quick Host Details Lookup

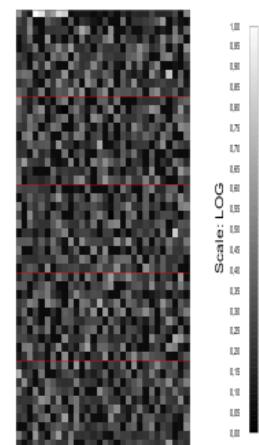
dstaddr

Raw Records

[1. Overview](#) | [2. Intrusion Detection View](#) | [3. Flow Visualization](#) | [4. Host Details](#) | [5. NetFlow Records](#) | [Help](#)

Details for 134.34.53.119

Port Fingerprint (TOP 1500)



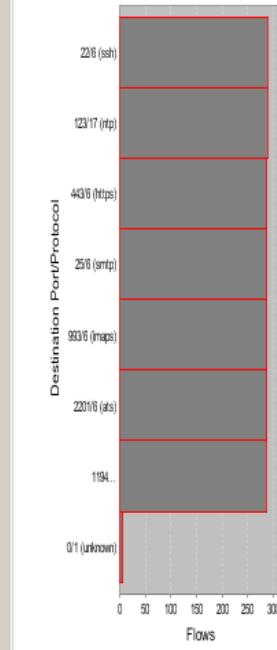
Aggregated Connections (Remote Hosts => 134.34.53.119)

 Ignore single flow connections

| srcaddr | dstaddr | prot | srcport | dstport | packetcounter | octetcounter | flowcounter |
|---------------|---------------|------|---------|---------|---------------|--------------|-------------|
| 85.131.189.69 | 134.34.53.119 | 1 | 8 | 0 | 2,885 | 242,340 | 577 |
| 85.131.189.69 | 134.34.53.119 | 6 | 32788 | 25 | 12 | 692 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 32845 | 1194 | 10 | 512 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 32850 | 993 | 20 | 1,910 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 32869 | 1194 | 8 | 420 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 32870 | 22 | 14 | 768 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 32870 | 25 | 14 | 796 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 32881 | 22 | 14 | 768 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 32929 | 443 | 18 | 2,030 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 32938 | 443 | 20 | 2,134 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 32939 | 993 | 20 | 1,910 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 32970 | 22 | 14 | 768 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33012 | 443 | 18 | 2,030 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33034 | 22 | 12 | 676 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33071 | 22 | 12 | 676 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33090 | 443 | 16 | 1,926 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33098 | 443 | 16 | 1,926 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33099 | 1194 | 10 | 512 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33106 | 25 | 12 | 692 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33147 | 22 | 14 | 768 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33194 | 22 | 12 | 676 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33222 | 25 | 14 | 796 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33246 | 25 | 12 | 692 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33266 | 1194 | 10 | 512 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33269 | 25 | 14 | 796 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33333 | 25 | 14 | 796 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33337 | 443 | 16 | 1,926 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33360 | 25 | 12 | 692 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33382 | 1194 | 8 | 420 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33395 | 22 | 14 | 768 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33429 | 993 | 20 | 1,910 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33434 | 22 | 14 | 768 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33446 | 22 | 12 | 676 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33472 | 25 | 12 | 692 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33509 | 1194 | 10 | 512 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33526 | 1194 | 12 | 604 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33564 | 1194 | 12 | 604 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33591 | 1194 | 8 | 420 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33594 | 25 | 12 | 692 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33604 | 993 | 20 | 1,898 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33605 | 443 | 16 | 1,926 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33607 | 993 | 20 | 1,910 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33642 | 25 | 14 | 796 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33646 | 25 | 12 | 692 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33646 | 1194 | 10 | 512 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33656 | 1194 | 10 | 512 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33677 | 1194 | 34 | 1,628 | 8 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33768 | 1194 | 8 | 420 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33769 | 993 | 20 | 1,910 | 2 |
| 85.131.189.69 | 134.34.53.119 | 6 | 33770 | 9979 | 14 | 796 | 2 |

Details for Remote Hosts

Destination Ports (TOP 10)



NFlowVis Project

2008-05-11

| Attribute | Value |
|----------------|-----------------------|
| Flows | 61.123.671 |
| Start Time | 2008-05-10 23:59:51.0 |
| End Time | 2008-05-12 00:00:00.0 |
| Packets | 850.117.587 |
| Payload | 408.51 GiB |
| Source IP | 1.295.531 |
| Destination IP | 1.324.219 |

Anonymized NetFlow Traffic

| | |
|---------------------|----------------------|
| IANA Assignments | Network Tools |
| Host Details Lookup | Communication Lookup |

Quick Host Details Lookup

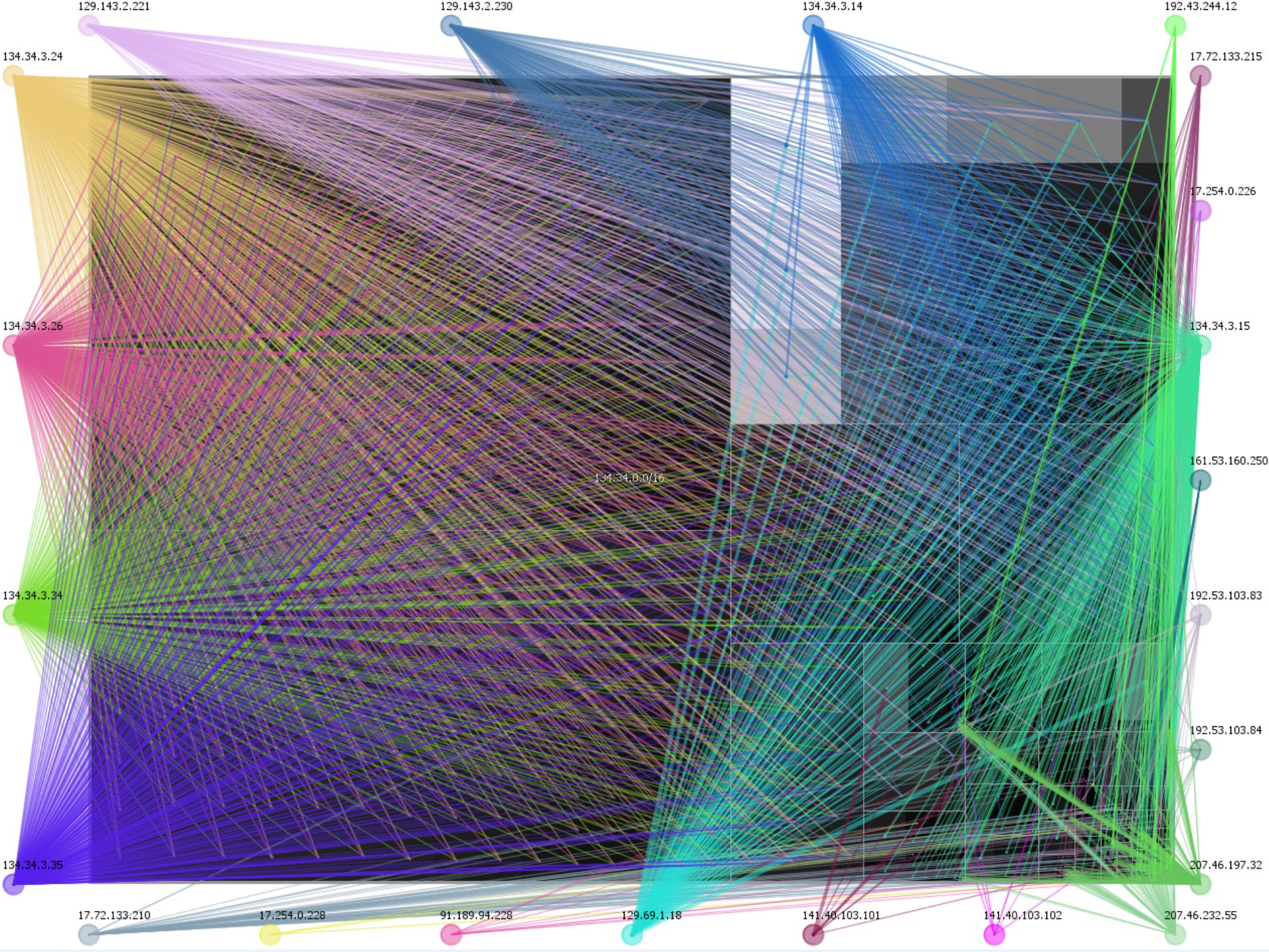
| | |
|---------------------------------------|----------------------------------|
| dstaddr | <input type="button" value="▼"/> |
| 134.34.3.15 | |
| <input type="checkbox"/> Raw Records | |
| <input type="button" value="Lookup"/> | |

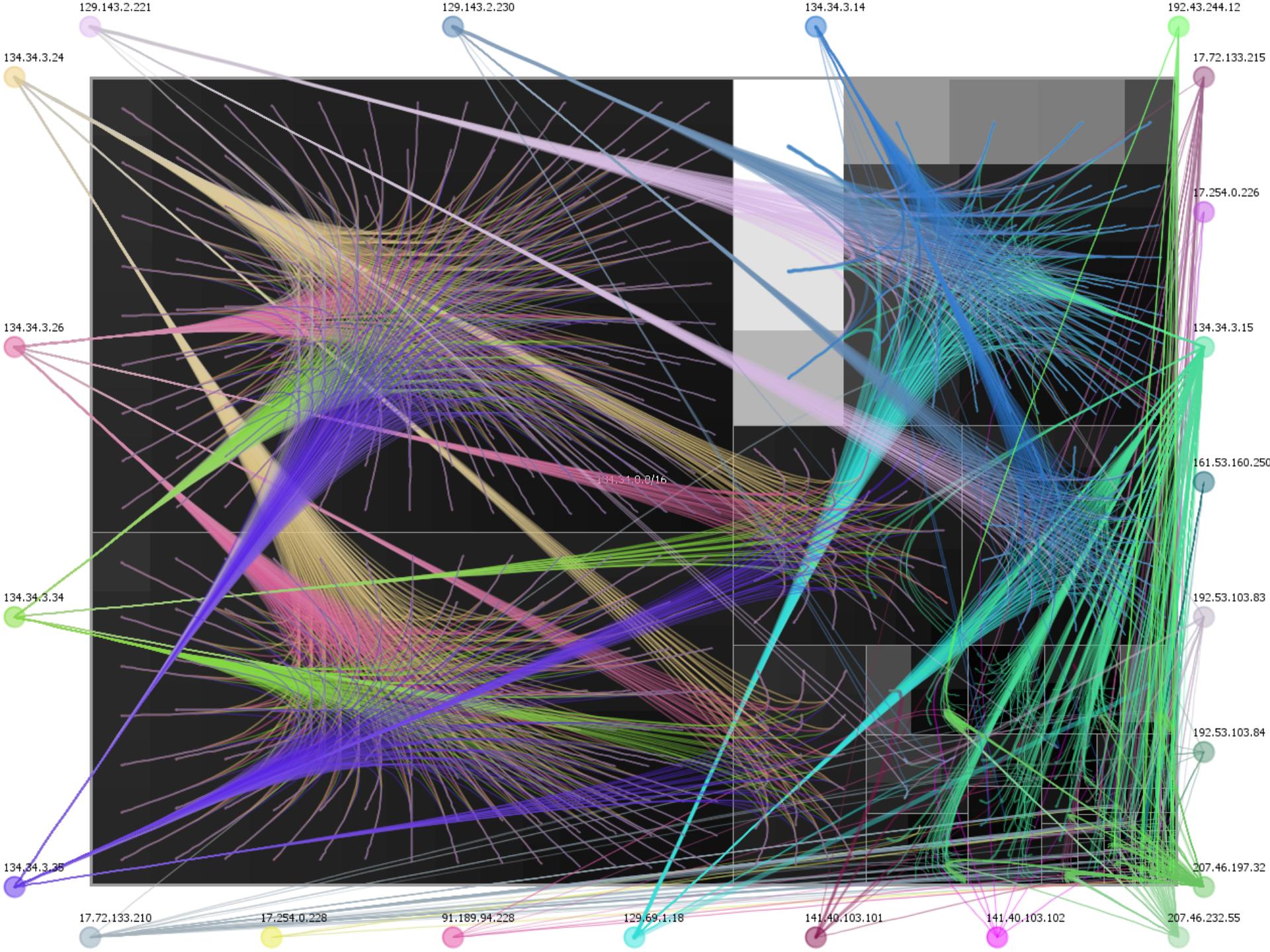
1. Overview | 2. Intrusion Detection View | 3. Flow Visualization | 4. Host Details | 5. NetFlow Records |

NetFlow Raw Records

| timestamp | dpkts | doctets | srcaddr | dstaddr | srcport | dstport | prot |
|---------------------|-------|---------|-------------|---------------|---------|---------|------|
| 2008-05-11 00:11:26 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 00:28:32 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 00:45:33 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 01:02:39 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 01:19:44 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 01:36:45 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 01:53:51 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 02:10:57 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 02:27:58 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 02:45:03 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 03:02:09 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 03:19:10 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 03:36:16 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 03:53:21 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 04:10:22 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 04:27:28 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 04:44:34 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 05:01:35 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 05:18:40 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 05:35:46 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 05:52:47 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 06:09:53 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 06:26:58 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 06:44:00 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 07:01:05 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 07:18:07 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 07:35:12 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 07:52:18 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 08:09:19 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 08:26:25 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 08:43:30 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 09:00:36 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 09:17:37 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 09:34:42 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 09:51:44 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 10:08:49 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 10:25:55 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 10:43:00 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 11:00:02 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 11:17:07 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 11:34:12 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 11:51:14 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 12:08:19 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 12:25:25 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 12:42:26 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 12:59:32 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 13:16:37 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 13:33:39 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 13:50:44 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |
| 2008-05-11 14:07:50 | 1 | 76 | 134.34.3.15 | 134.34.13.154 | 123 | 123 | 17 |

LIMIT 100







Thank you for your attention!

For further information about the tool please contact

Florian Mansmann

Tel. +49 7531 883070

Florian.Mansmann@uni-konstanz.de

References:

- [1] Danny Holten. **Hierarchical Edge Bundles: Visualization of Adjacency Relations in Hierarchical Data.** *IEEE Transactions on Visualization and Computer Graphics*, vol. 12, no. 5, pp. 741-748, September-October, 2006.
- [2] Shneiderman, B.: Tree visualization with tree-maps: 2-d space-filling approach. *ACM Trans. Graph.* 11(1) (1992) 92–99