Visual Support for Analyzing Network Traffic and Intrusion Detection Events using TreeMap and Graph Representations

Florian Mansmann[1] Fabian Fischer[1] Daniel A. Keim[1] Stephen C. North[2]

[1] University of Konstanz, Germany

[2] AT&T Research, Florham Park, NJ, U.S.A.

Symposium on Computer-Human Interaction for Management of Information Technology, Baltimore, MD, 2009

Introduction

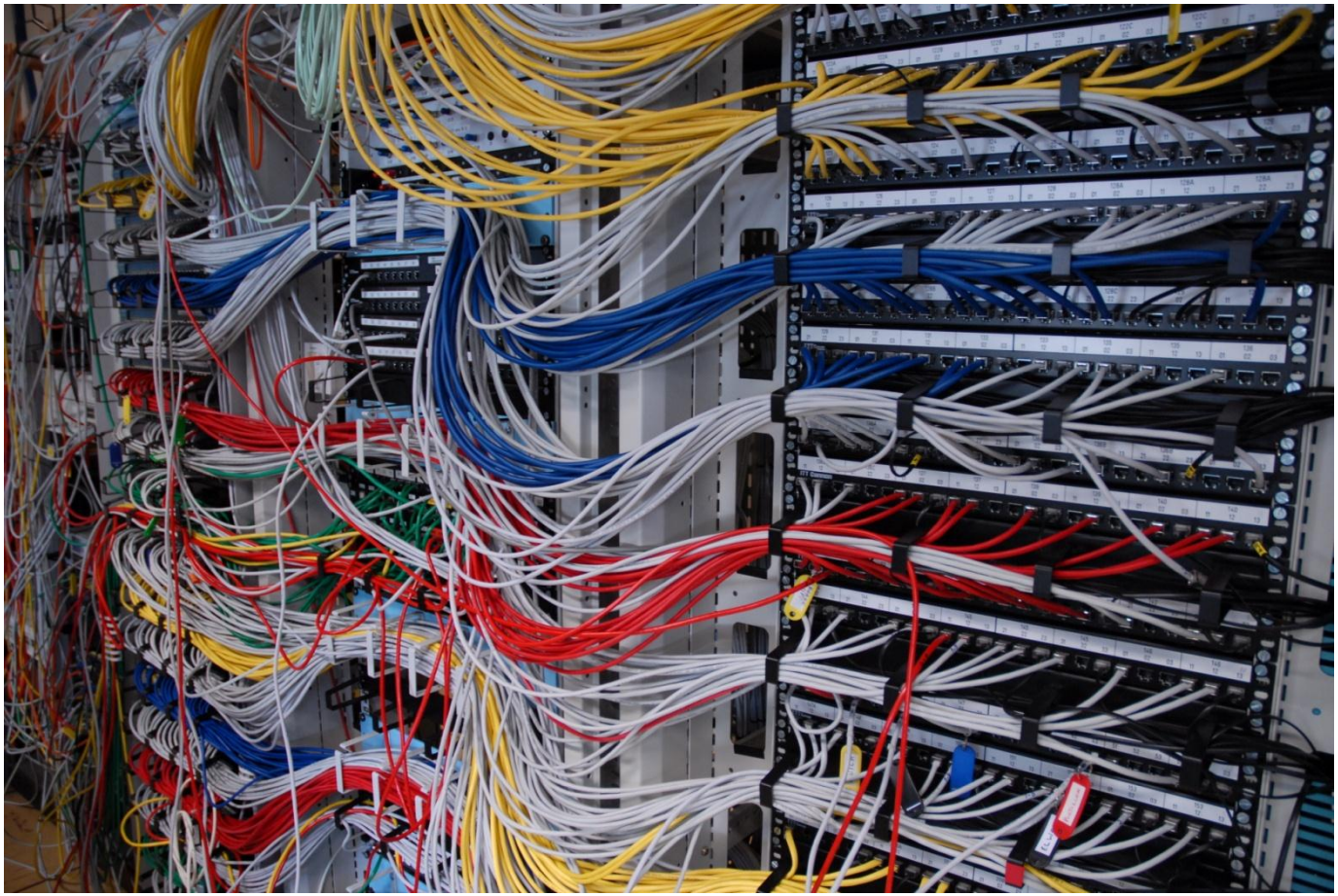


Photo by Guillaume Paumier / Wikimedia Commons, CC-by-sa-3.0

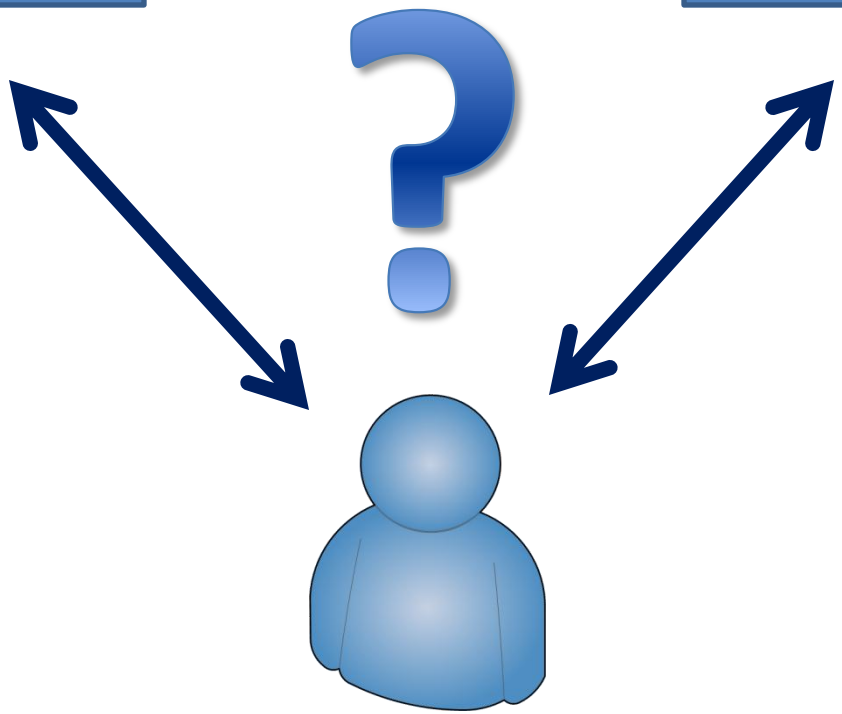
Introduction

Photo by Guillaume Paumier / Wikimedia Commons, CC-by-sa-3.0

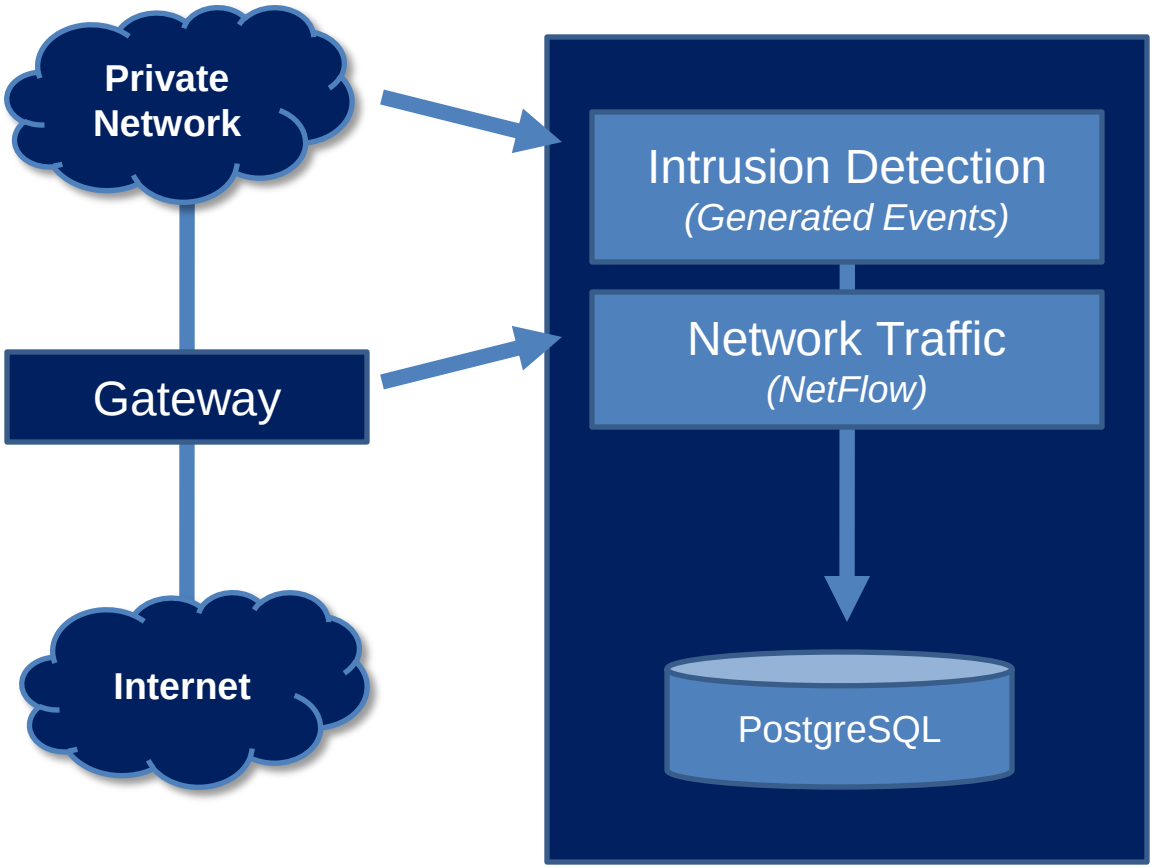
How to combine all the data?

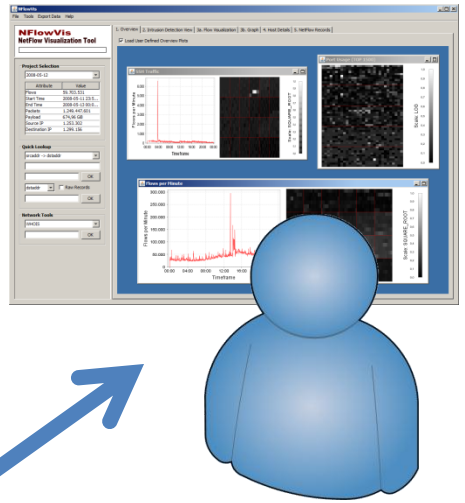
Intrusion Detection
e.g. Generated IDS Events, Firewall Logs

Network Traffic
e.g. NetFlow connections, Bandwidth data,…

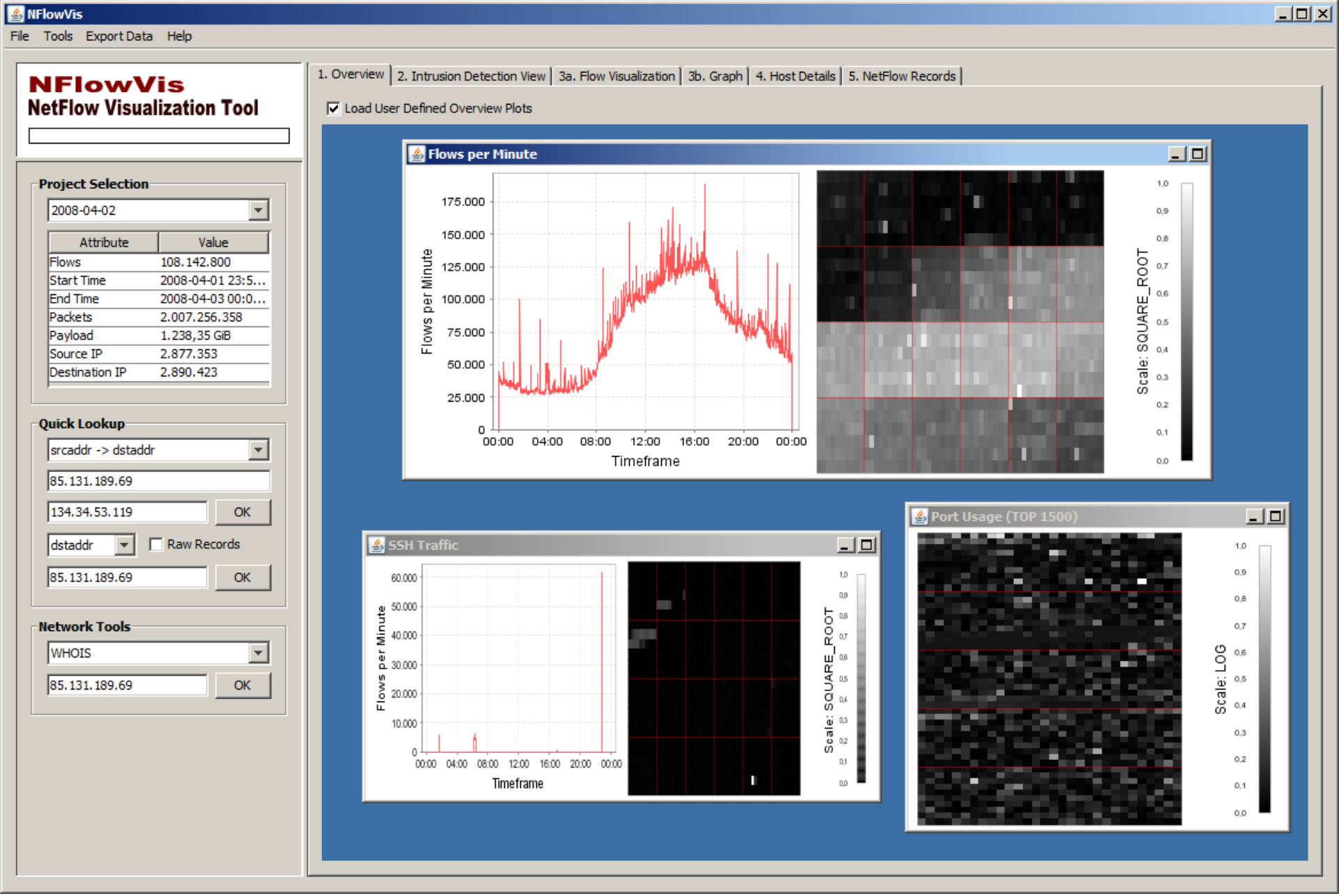


Visual Analytics with NFlowVis

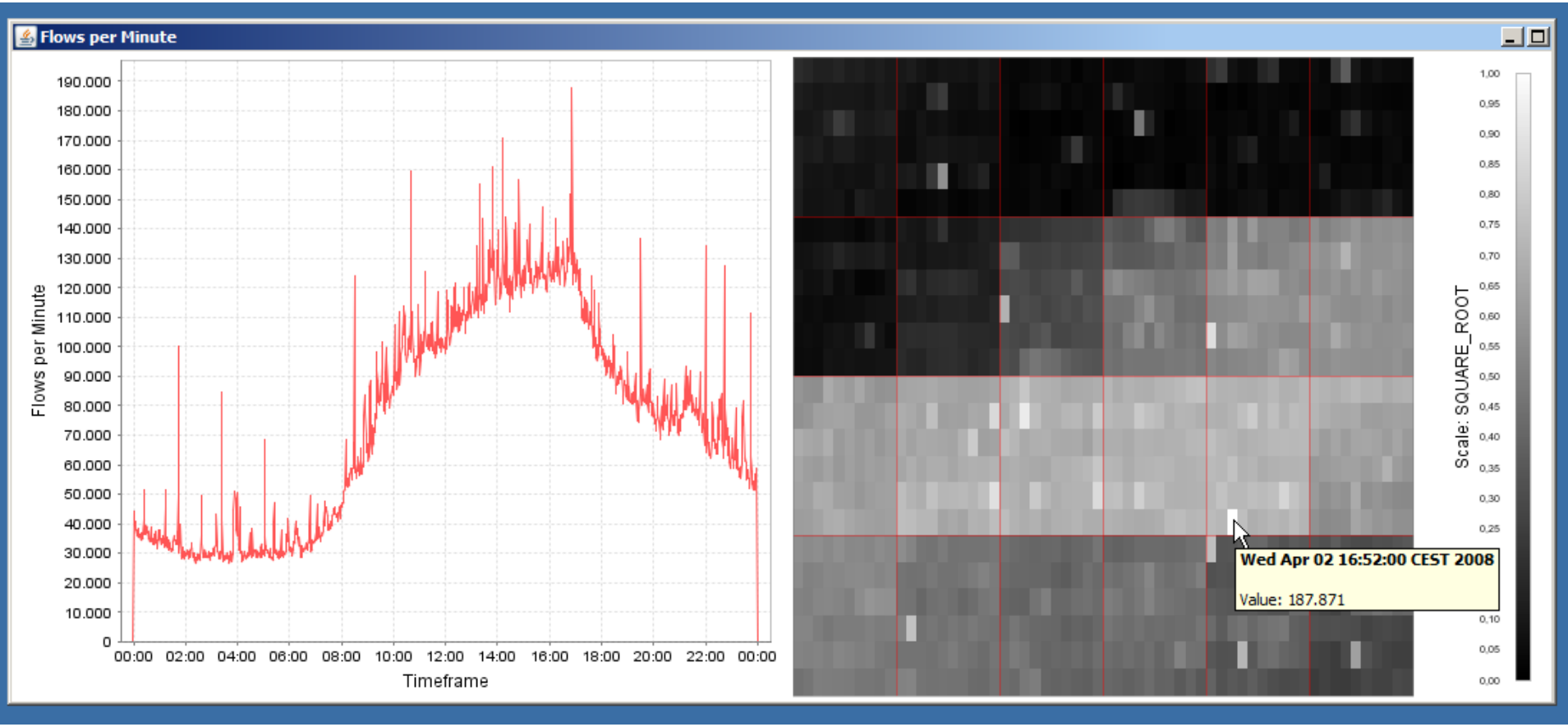




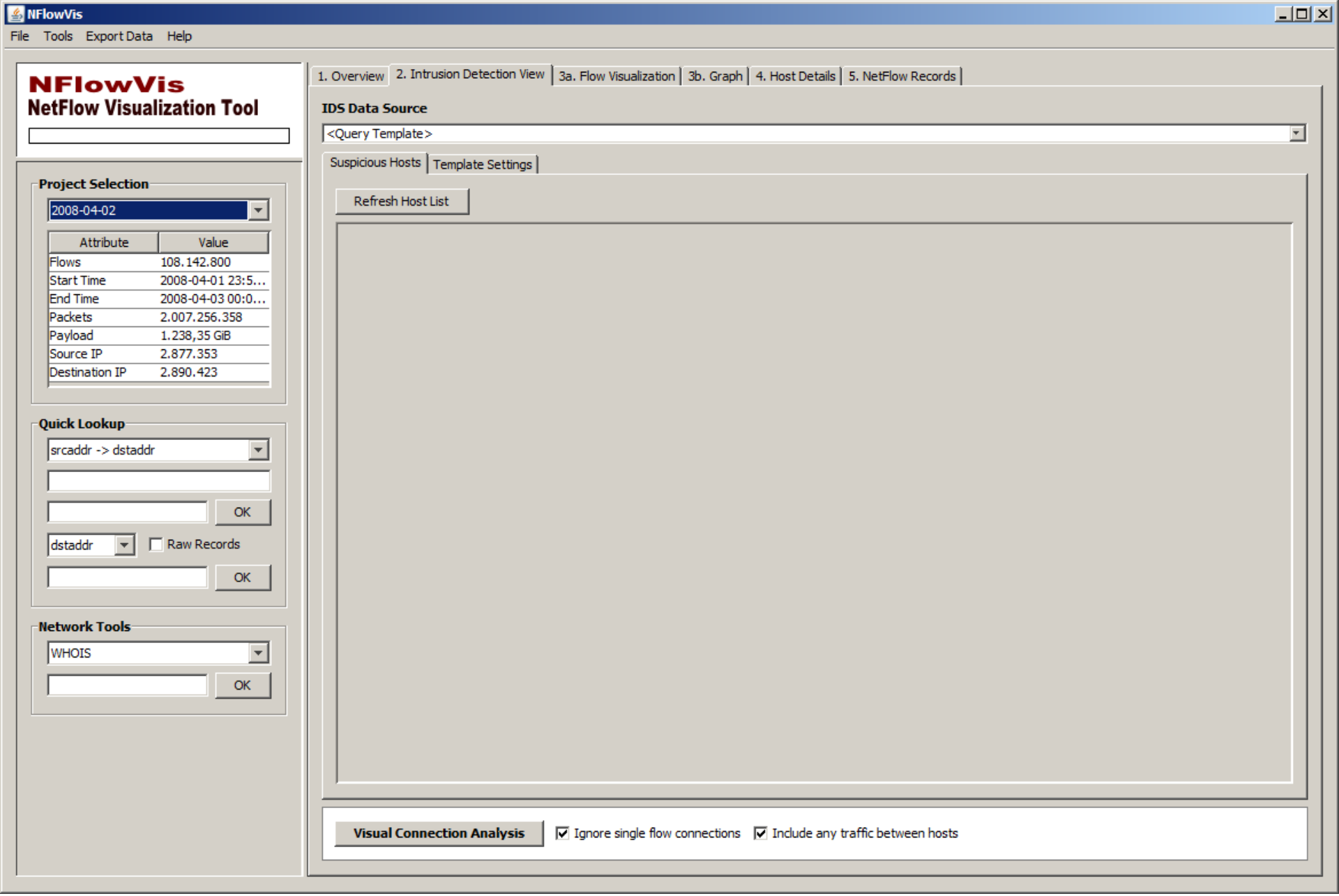
CHIMIT 09
Symposium on Computer-Human Interaction for Management of Information Technology
November 7-8, 2009
Baltimore, MD



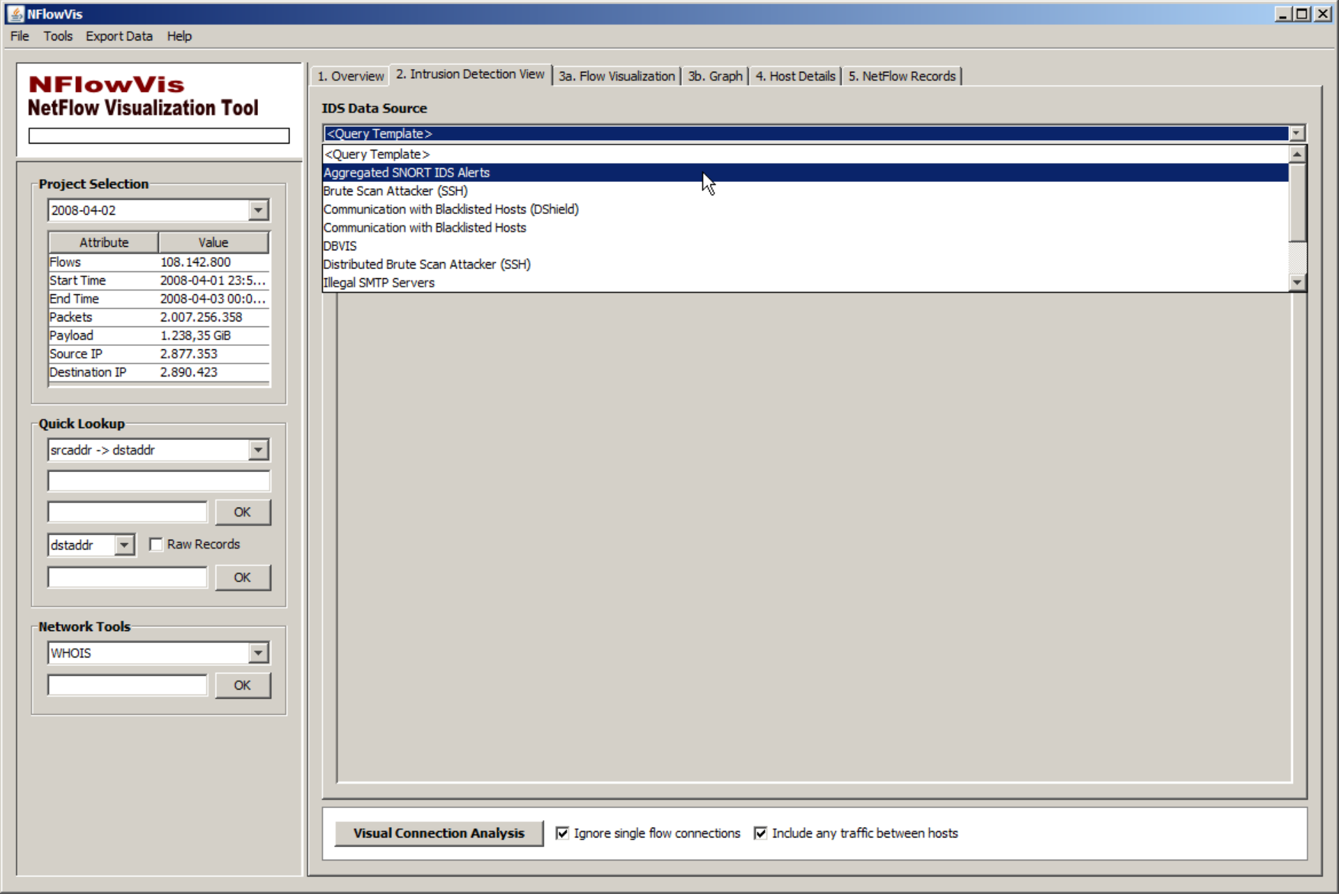
Daily Traffic Overview



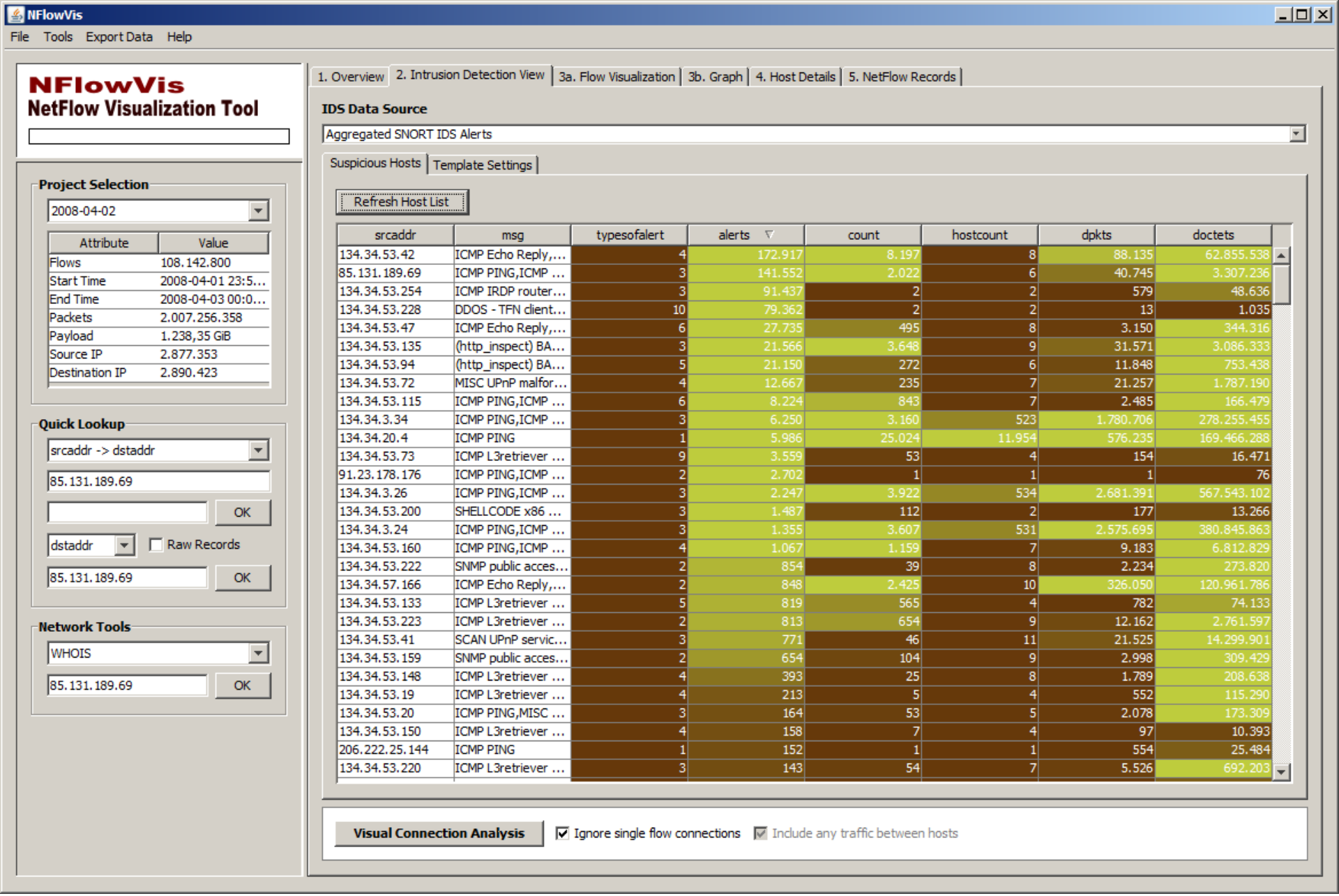
Daily Traffic Overview (Flows per Minute Widget)



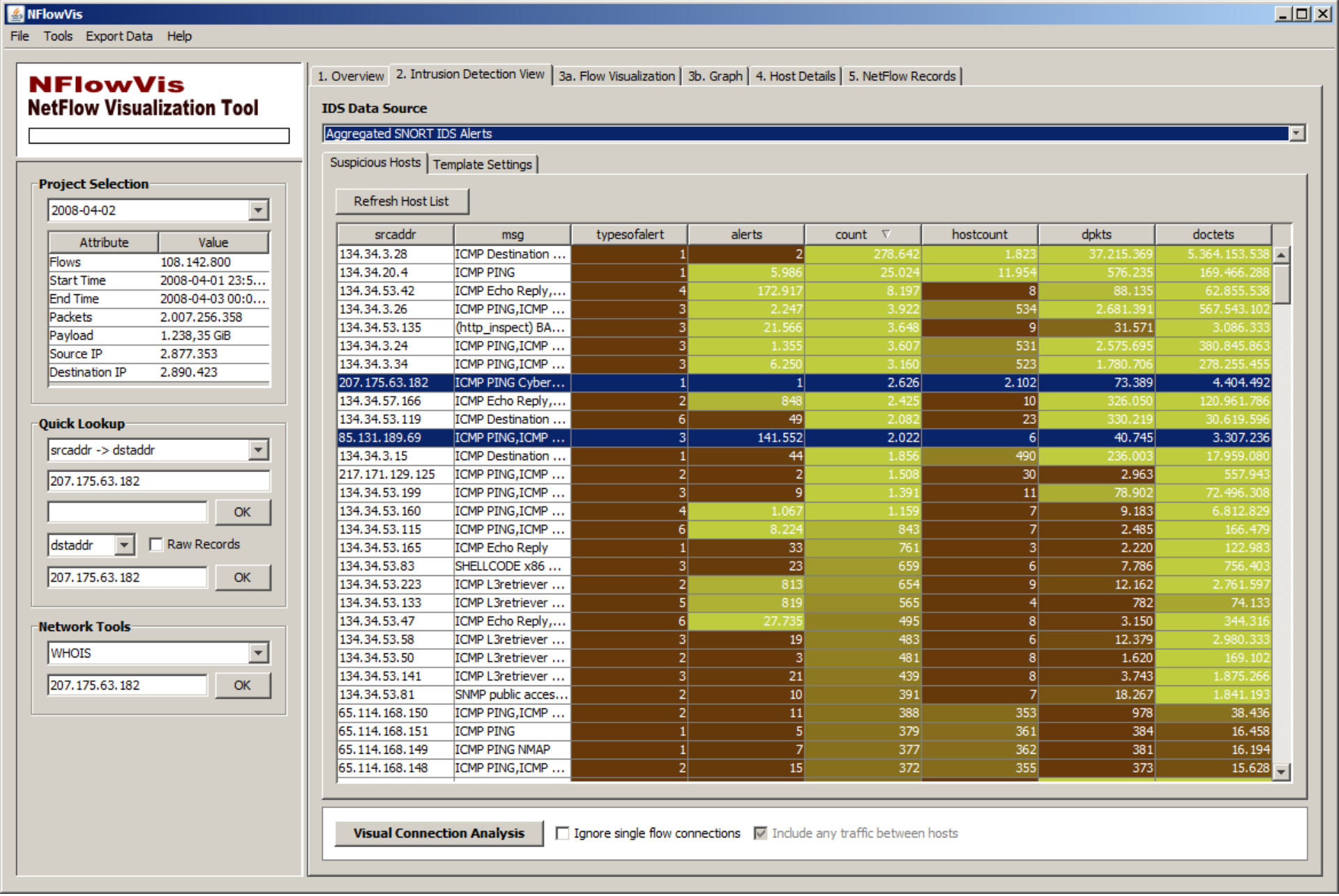
Intrusion Detection View



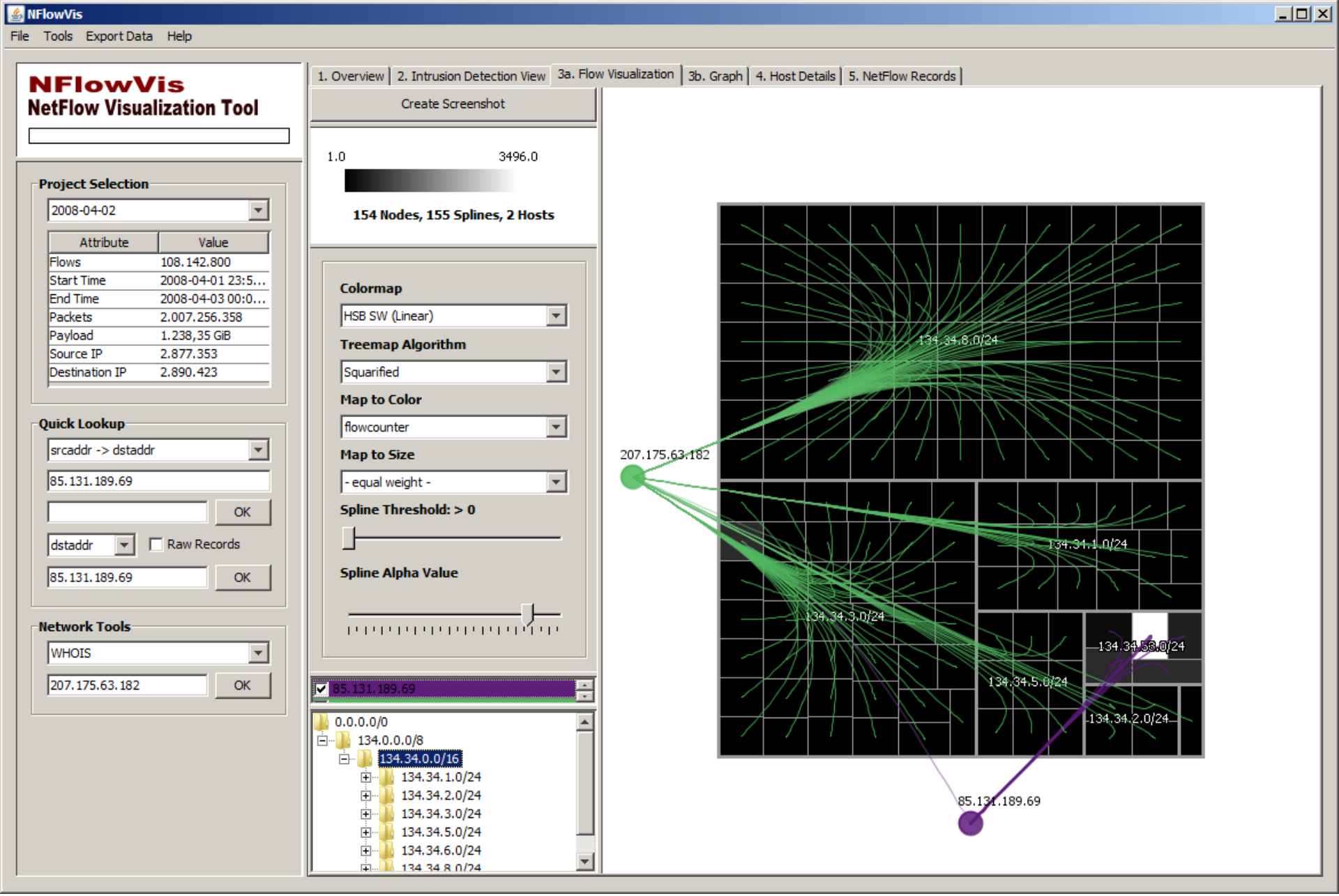
Intrusion Detection View – Select IDS Data Source



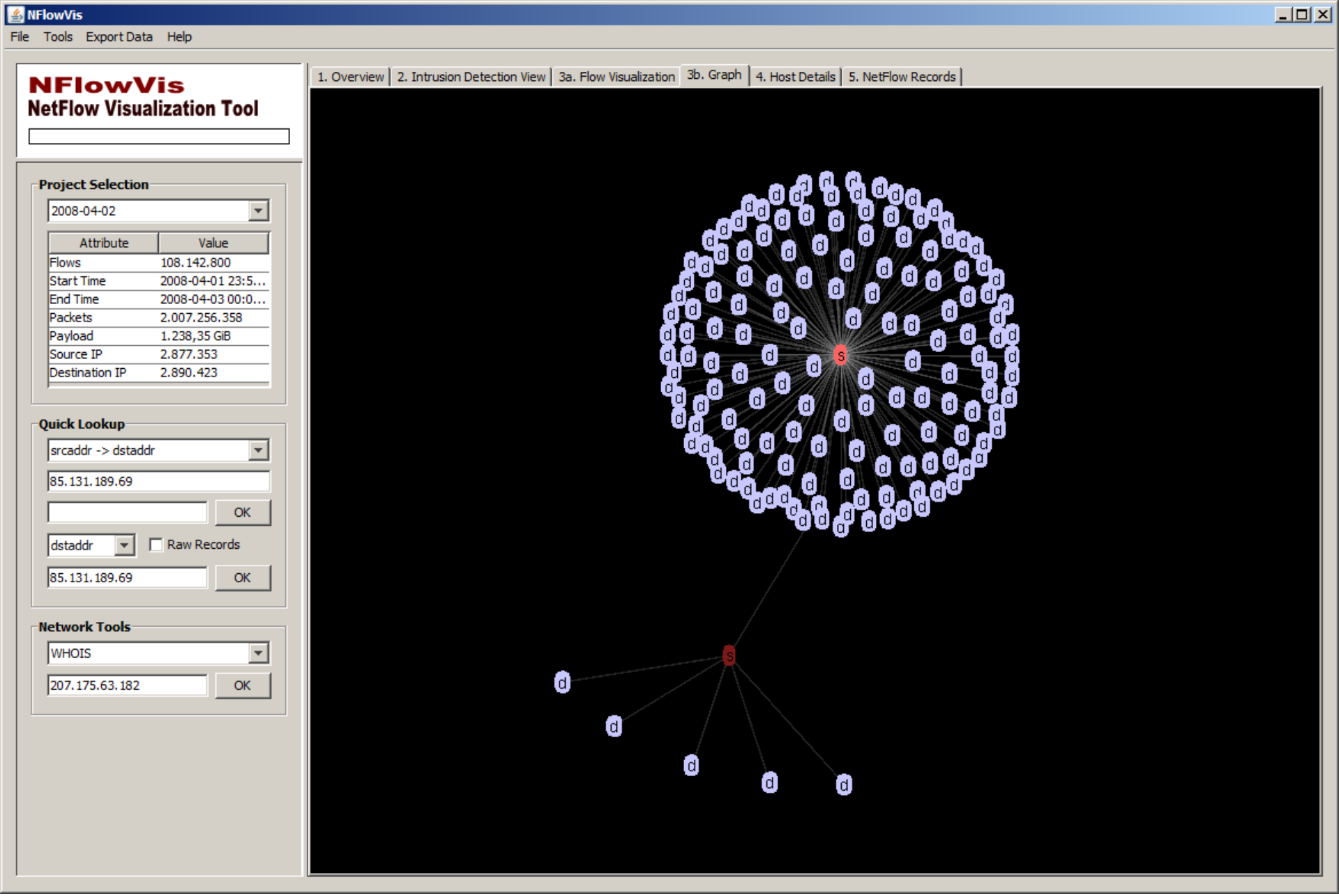
Intrusion Detection View – Suspicious Hosts



Intrusion Detection View – Suspicious Hosts



Home-Centric Network Visualization



Graph Visualization

NFlowVis

File Tools Export Data Help

NFlowVis
NetFlow Visualization Tool

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

Project Selection

2008-04-02

Attribute	Value
Flows	108.142.800
Start Time	2008-04-01 23:5...
End Time	2008-04-03 00:0...
Packets	2.007.256.358
Payload	1.238,35 GiB
Source IP	2.877.353
Destination IP	2.890.423

Quick Lookup

srcaddr -> dstaddr

85.131.189.69

134.34.53.119 OK

dstaddr Raw Records

85.131.189.69 OK

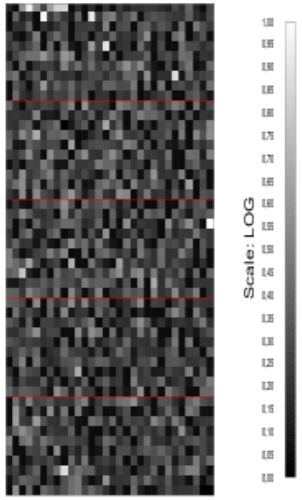
Network Tools

WHOIS

207.175.63.182 OK

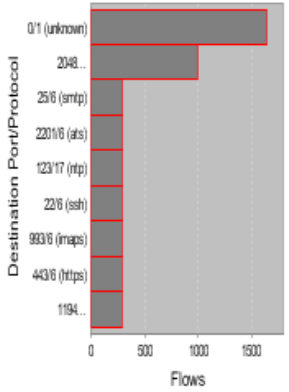
Details for 134.34.53.119

Port Fingerprint (TOP 1500)



Details for Remote Hosts

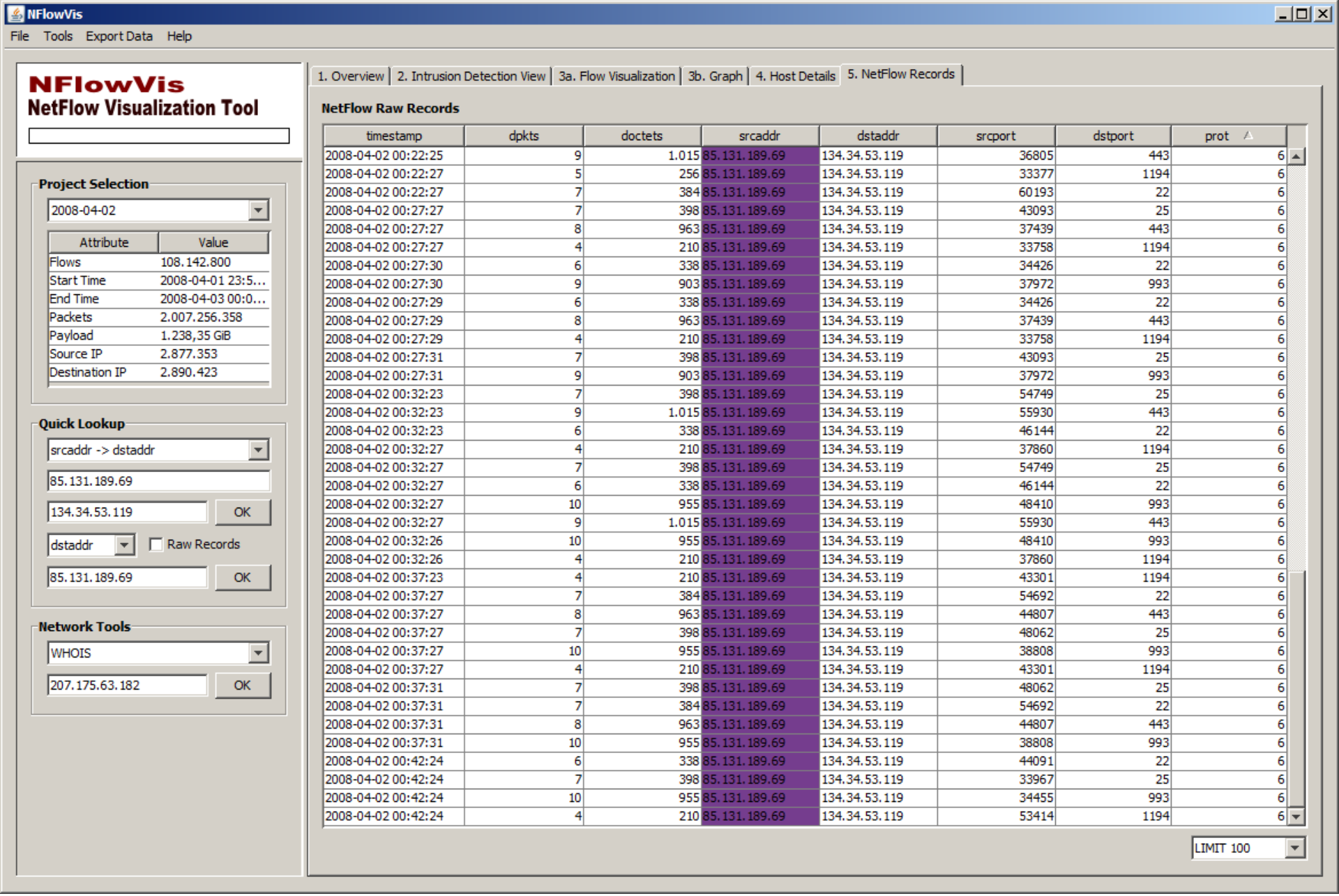
Destination Ports (TOP 10)



Aggretated 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	6	32780	1194	10	512	2
85.131.189.69	134.34.53.119	6	32781	22	12	676	2
85.131.189.69	134.34.53.119	6	32804	1194	10	512	2
85.131.189.69	134.34.53.119	6	32814	1194	8	420	2
85.131.189.69	134.34.53.119	6	32827	993	20	1.910	2
85.131.189.69	134.34.53.119	6	32859	25	16	900	2
85.131.189.69	134.34.53.119	6	32882	443	18	2.030	2
85.131.189.69	134.34.53.119	6	32901	22	12	676	2
85.131.189.69	134.34.53.119	6	32911	993	20	1.910	2
85.131.189.69	134.34.53.119	6	33006	22	14	768	2
85.131.189.69	134.34.53.119	6	33060	22	12	676	2
85.131.189.69	134.34.53.119	6	33090	443	18	2.030	2
85.131.189.69	134.34.53.119	6	33130	22	12	676	2
85.131.189.69	134.34.53.119	6	33146	22	12	676	2
85.131.189.69	134.34.53.119	6	33163	993	20	1.910	2
85.131.189.69	134.34.53.119	6	33176	1194	8	420	2
85.131.189.69	134.34.53.119	6	33178	443	16	1.926	2
85.131.189.69	134.34.53.119	6	33205	25	16	924	2
85.131.189.69	134.34.53.119	6	33210	1194	10	512	2
85.131.189.69	134.34.53.119	6	33242	22	12	676	2
85.131.189.69	134.34.53.119	6	33259	1194	8	420	2
85.131.189.69	134.34.53.119	6	33287	22	12	676	2
85.131.189.69	134.34.53.119	6	33314	25	12	692	2
85.131.189.69	134.34.53.119	6	33317	22	12	676	2
85.131.189.69	134.34.53.119	6	33332	443	18	2.030	2
85.131.189.69	134.34.53.119	6	33340	993	18	1.806	2
85.131.189.69	134.34.53.119	6	33377	993	20	1.910	2
85.131.189.69	134.34.53.119	6	33377	1194	10	512	2
85.131.189.69	134.34.53.119	6	33389	993	20	1.910	2
85.131.189.69	134.34.53.119	6	33428	22	12	676	2
85.131.189.69	134.34.53.119	6	33443	1194	10	512	2
85.131.189.69	134.34.53.119	6	33542	22	14	768	2
85.131.189.69	134.34.53.119	6	33544	443	16	1.926	2
85.131.189.69	134.34.53.119	6	33561	993	20	1.910	2
85.131.189.69	134.34.53.119	6	33572	993	20	1.910	2
85.131.189.69	134.34.53.119	6	33587	1194	8	420	2
85.131.189.69	134.34.53.119	6	33595	1194	10	512	2

Host Details View

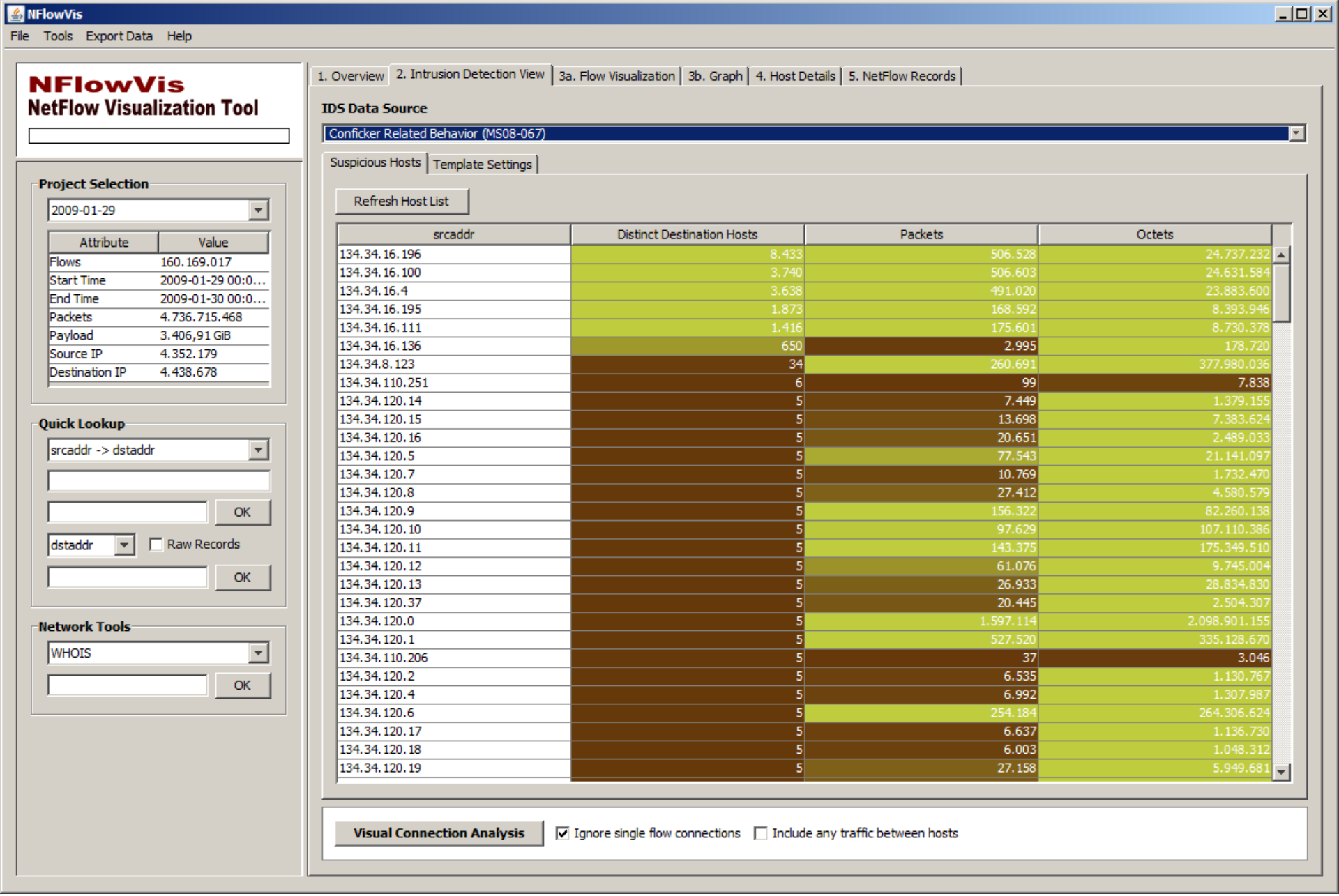


NetFlow Records

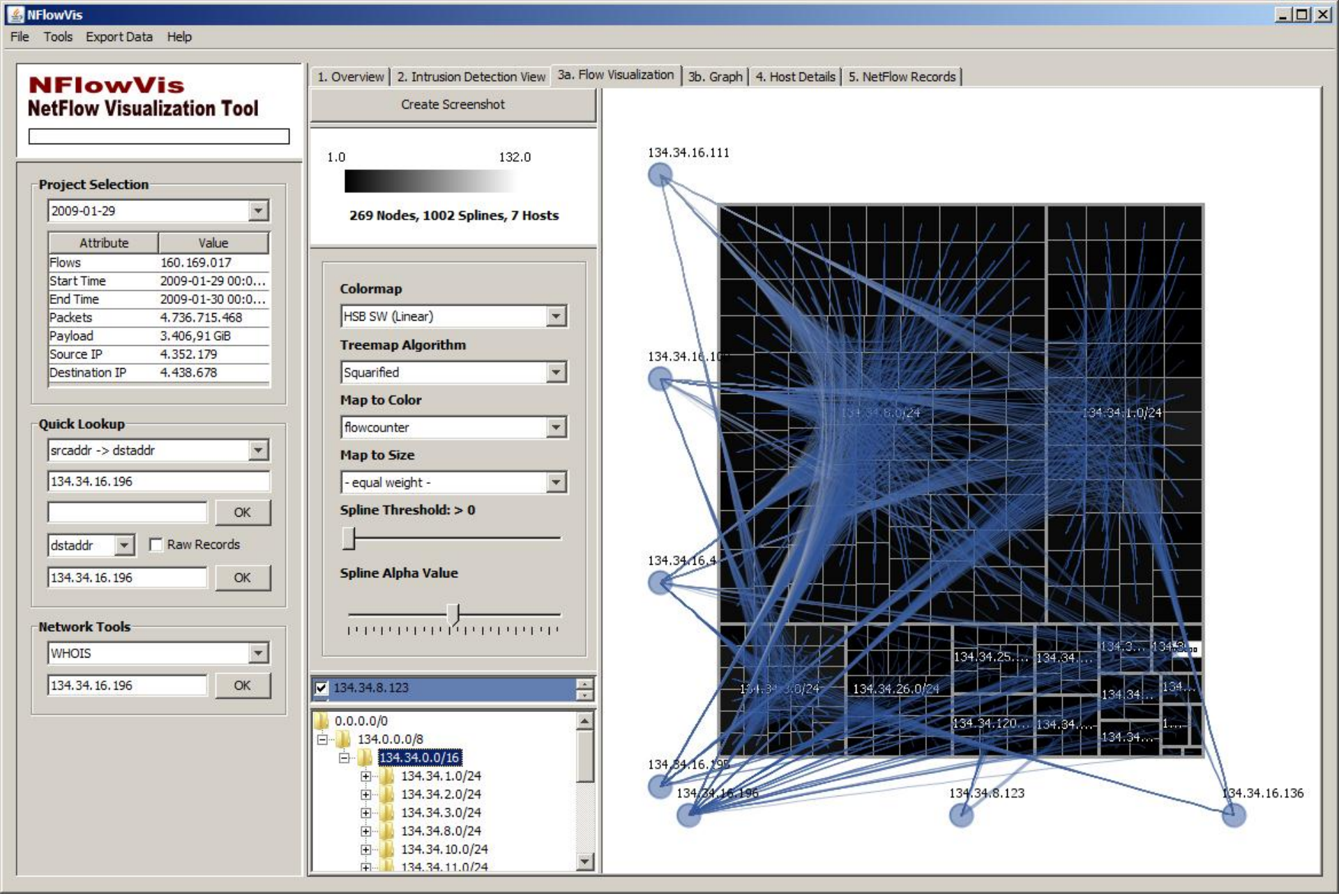
Service Monitoring with NFlowVis

- Example: Conficker Worm (11/2008)
- Exploits MS08-067 vulnerability
- RPC over Port 445/TCP

- **Are there any compromised hosts in my network?**



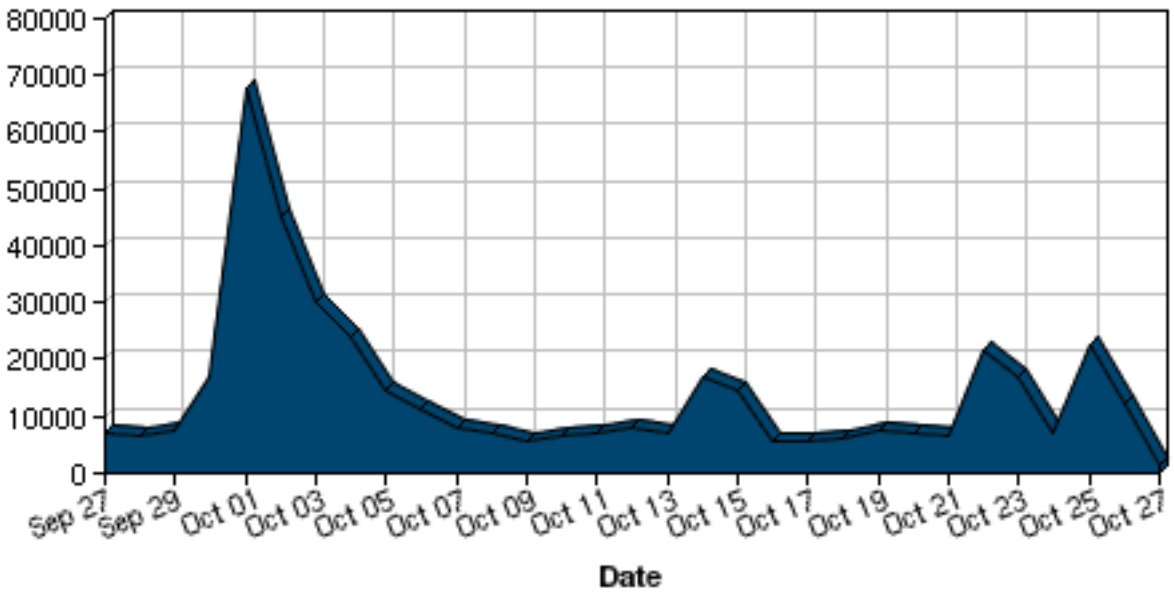
Intrusion Detection View – Suspicious Hosts



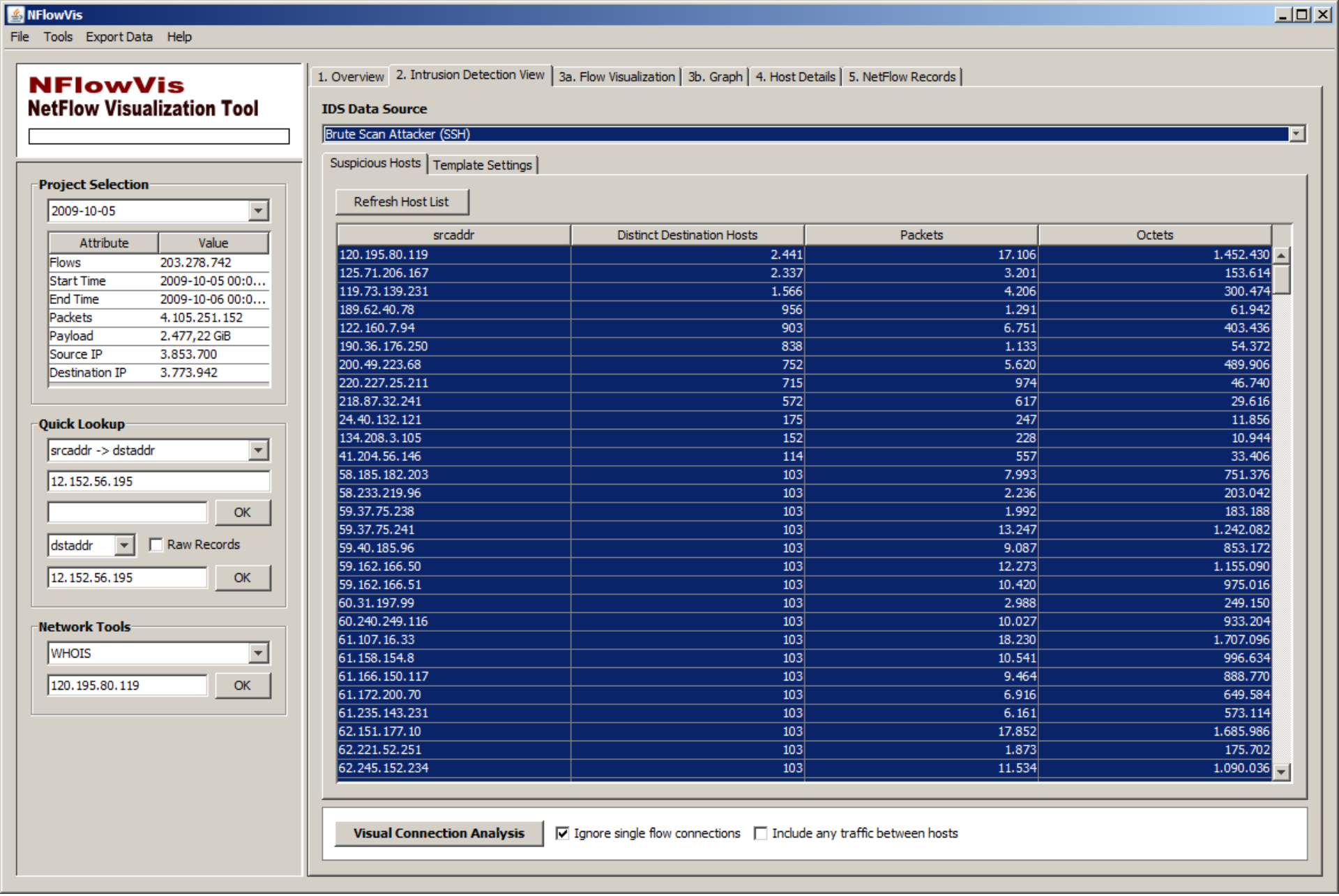
Home-Centric Network Visualization

Analyzing SSH Attacks with NFlowVis

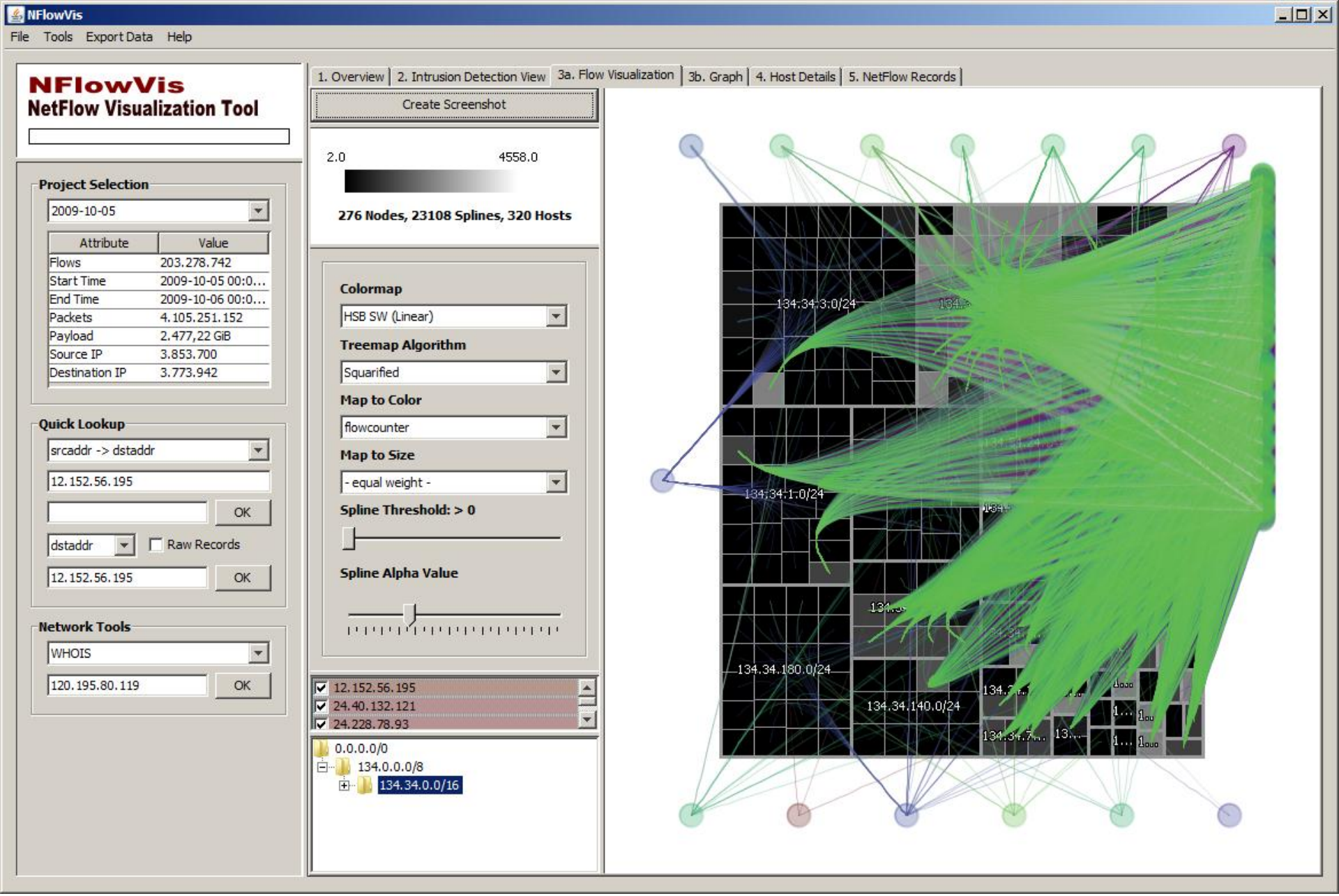
http://stats.denyhosts.net/stats.html



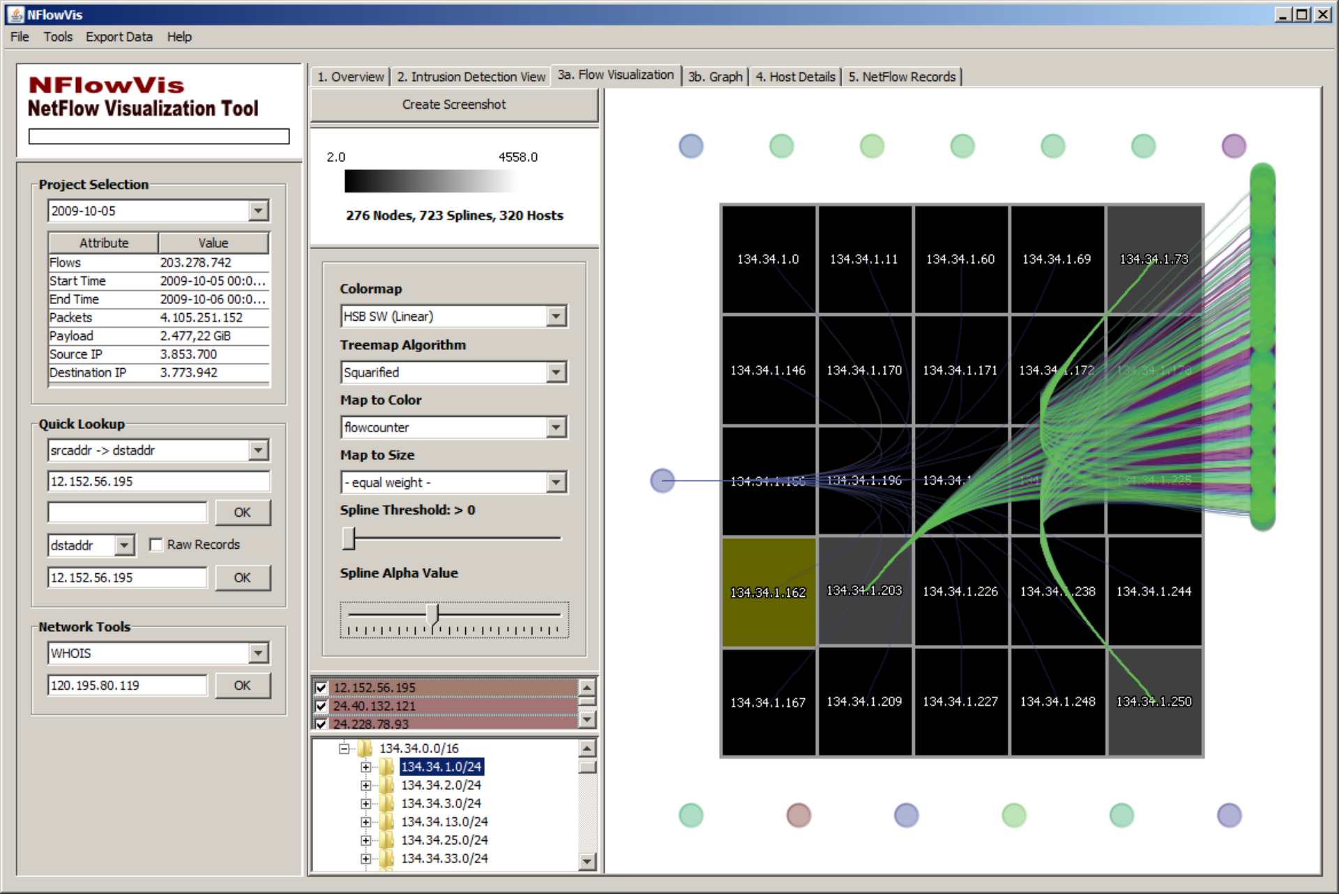
- How was our network affected by these attacks?



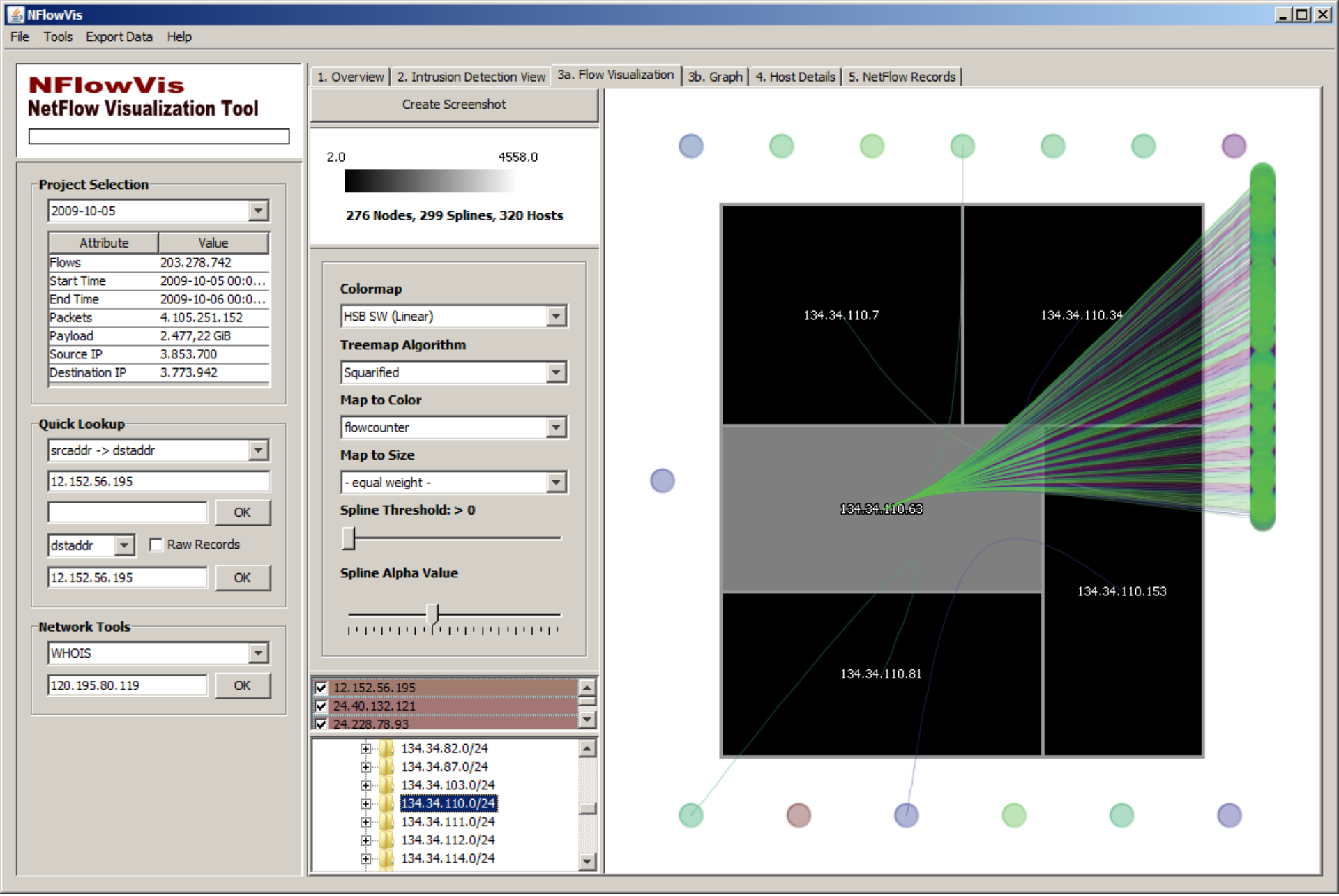
Remote Hosts with SSH connections (5th October 2009)



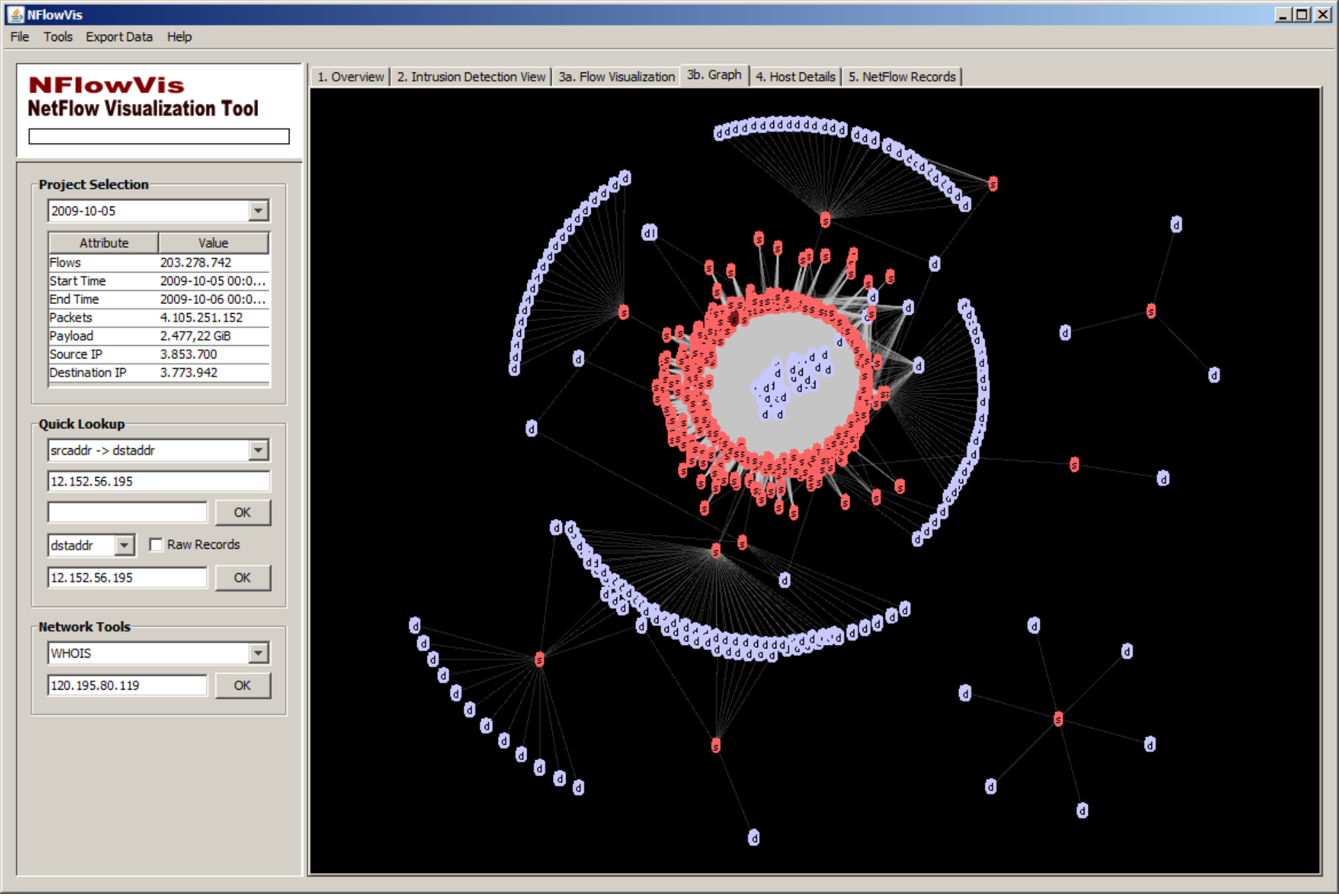
Home-Centric Network Visualization



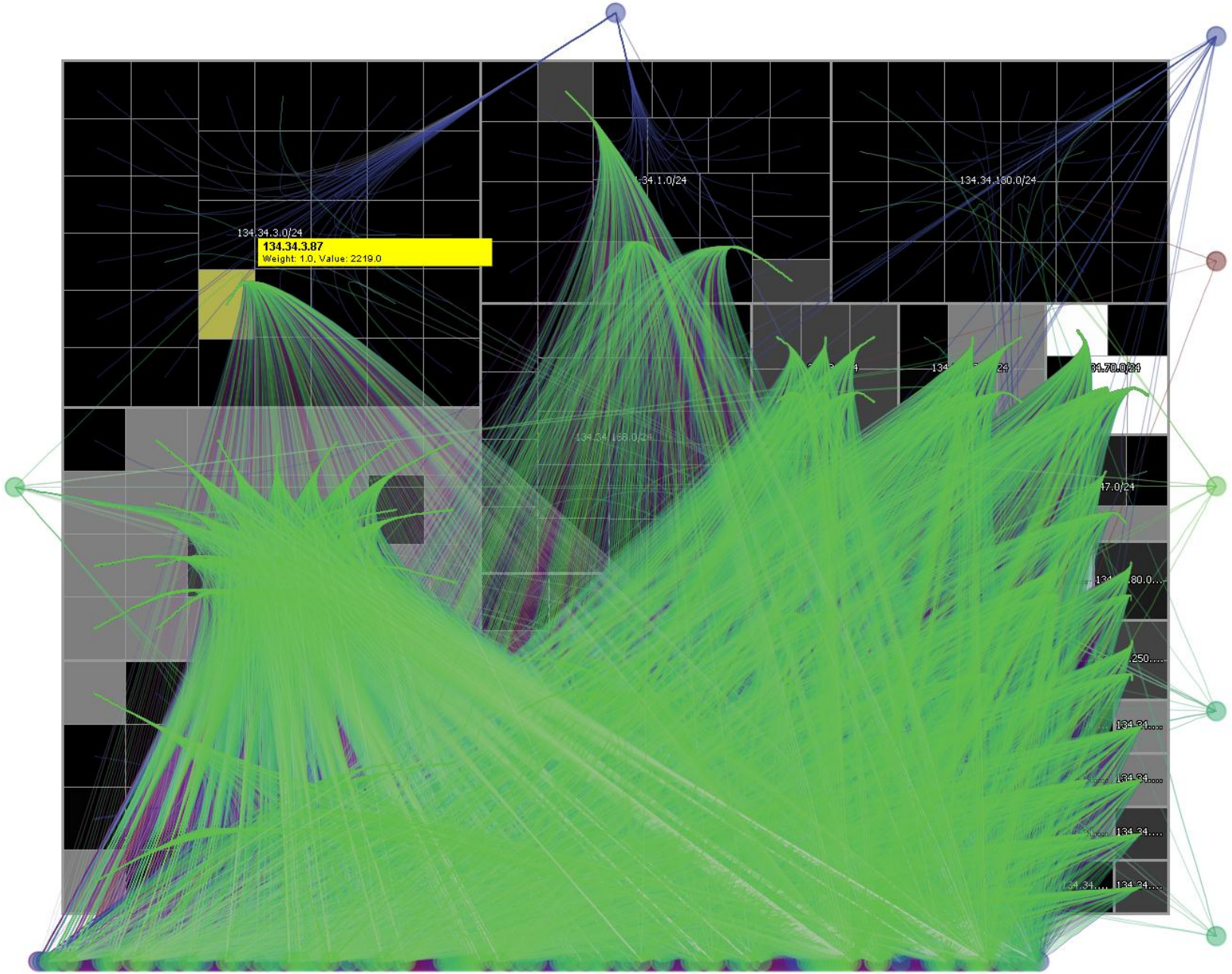
Home-Centric Network Visualization (Drill-Down)



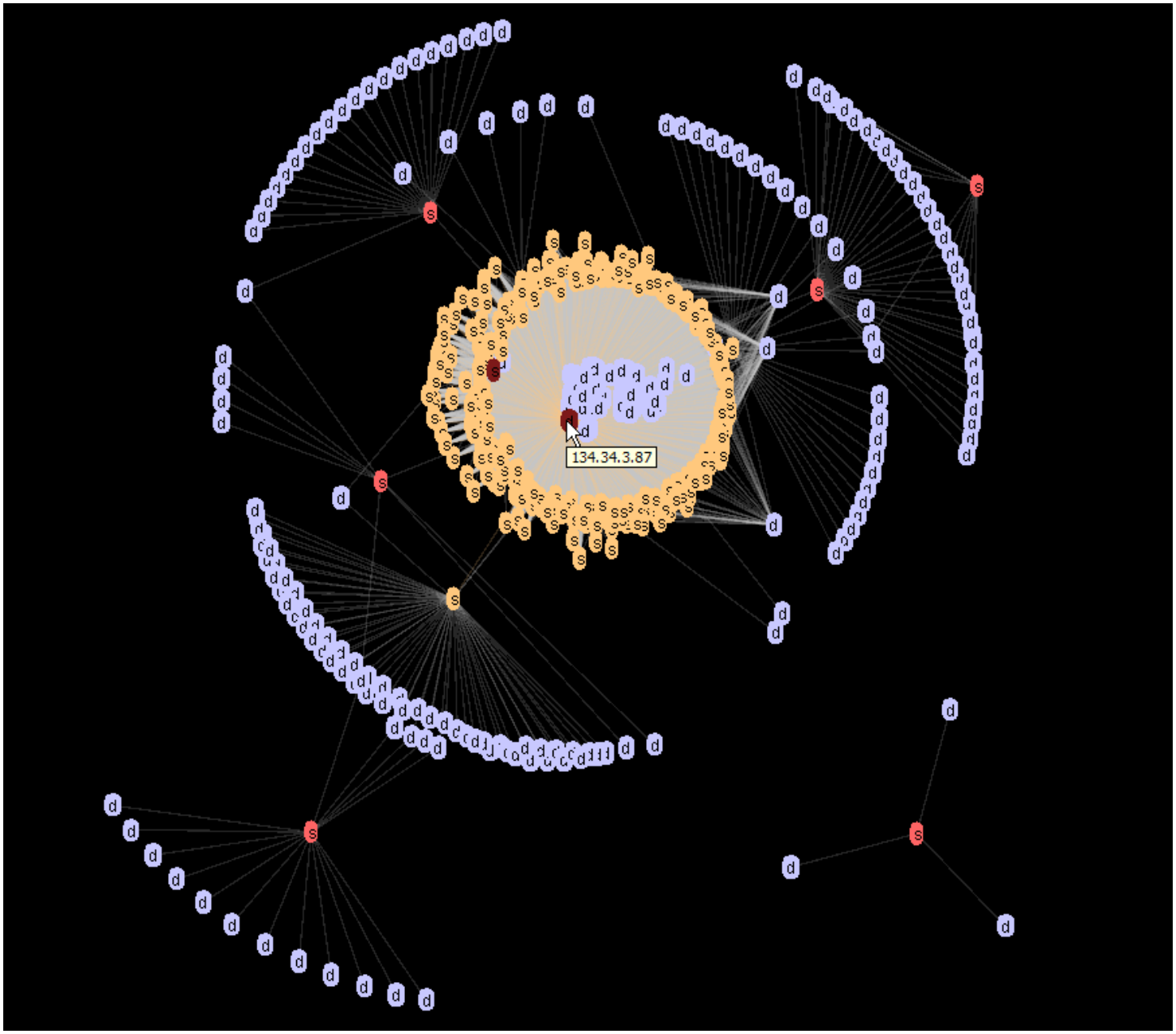
Home-Centric Network Visualization (Drill-Down)



Graph Visualization



Home-Centric Network Visualization (SSH Attacks on 5th October 2009)



Graph Visualization (SSH Attacks on 5th October 2009)

Conclusions

- Intrusion Detection and Network Monitoring combined
- Automated Analysis combined with Interactive Exploration

- **NFlowVis is a Visual Analytics System for Network Data**

Thank you very much for your attention!

Questions?

For further information about this work please contact

Fabian Fischer
Tel. +49 7531 88-2780
Fabian.Fischer@uni-konstanz.de

http://nflowvis.dbvis.de/

References I

Ball, R., Fink, G., and North, C. (2004).
Home-centric visualization of network traffic for security administration.
Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, pages 55–64.

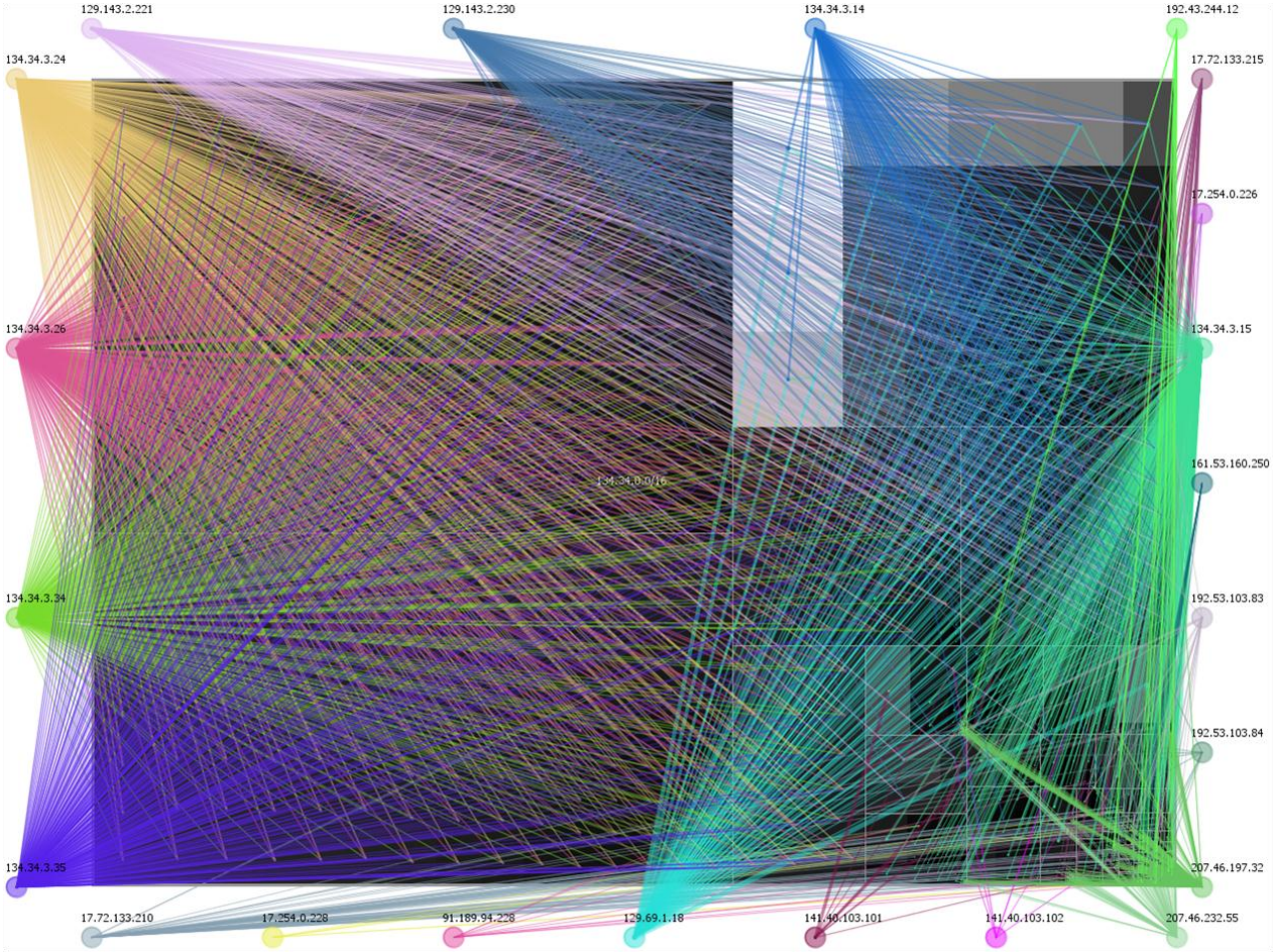
Holten, D. (2006).
Hierarchical Edge Bundles: Visualization of Adjacency Relations in Hierarchical Data.
IEEE Trans. Vis. Comput. Graph., 12(5):741–748.

References II

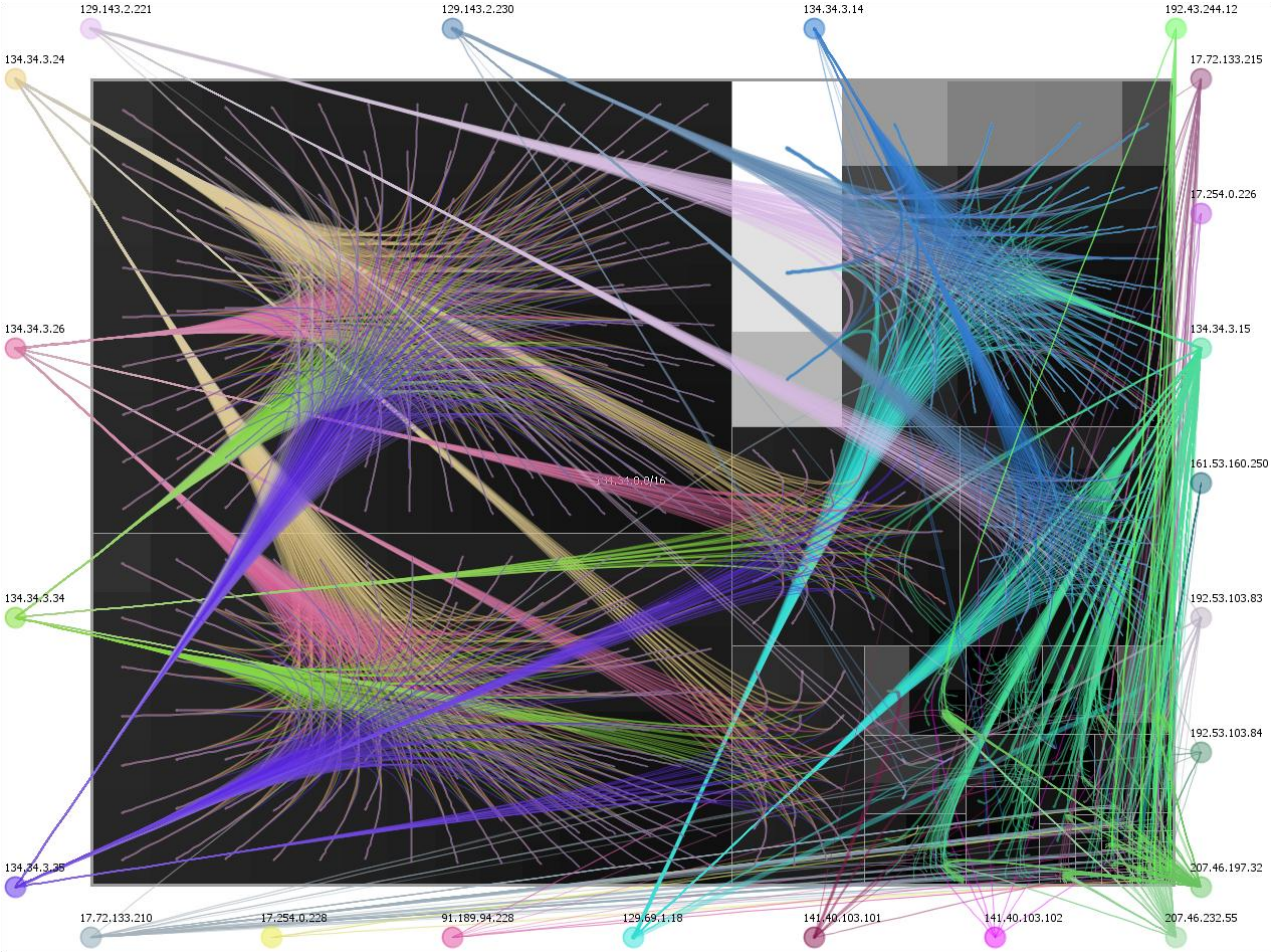
Ellson, J., Gansner, E., Koutsofios, L., North, S., and Woodhull, G. (2002).
Graphviz-Open Source Graph Drawing Tools.
Lecture Notes in Computer Science, pages 483–484.

Shneiderman, B. (1992).
Tree visualization with tree-maps: 2-d space-filling approach.
ACM Trans. Graph., 11(1):92–99.

Hierarchical Edge Bundling



Hierarchical Edge Bundling



CHIMIT 09
Symposium on Computer-Human Interaction for Management of Information Technology
November 7-8, 2009
Baltimore, MD