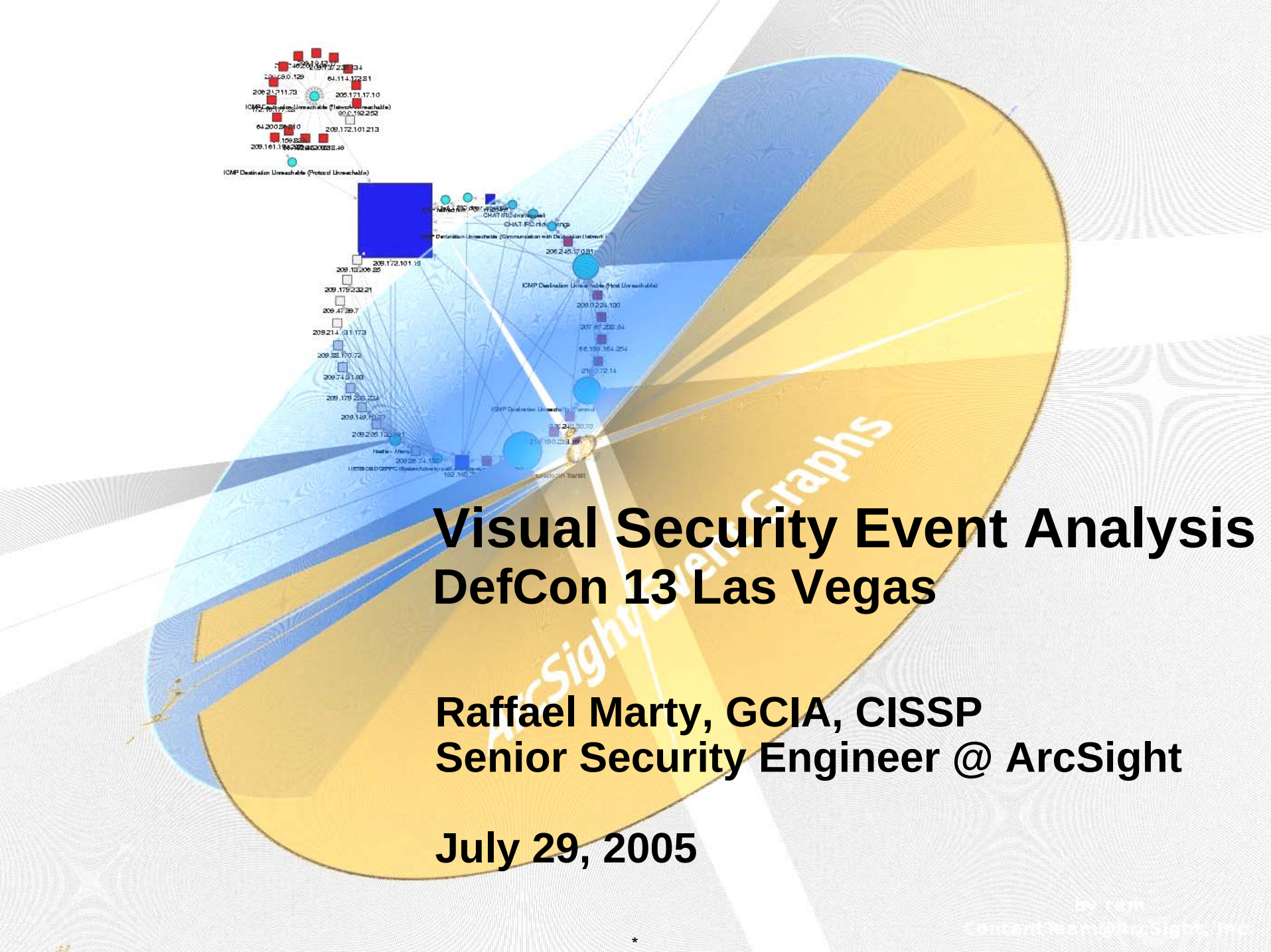
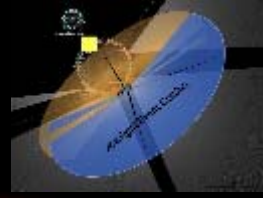


Visual Security Event Analysis
DefCon 13 Las Vegas

Raffael Marty, GCIA, CISSP
Senior Security Engineer @ ArcSight

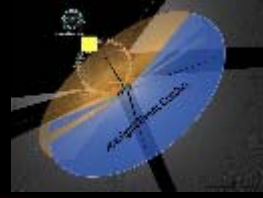
July 29, 2005

Raffael Marty



- Enterprise Security Management (ESM) specialist
- OVAL Advisory Board
  (Open Vulnerability and Assessment Language)
- ArcSight Research & Development
- IBM Research
  - Thor - http://thor.cryptojail.net
  - Log analysis and event correlation research
  - Tivoli Risk Manager

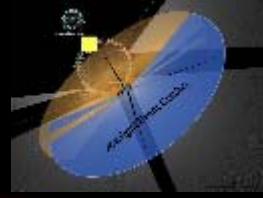
Table Of Contents



- Introduction
- Related Work
- Basics
- Situational Awareness
- Forensic and Historical Analysis
- AfterGlow

Introduction

Disclaimer

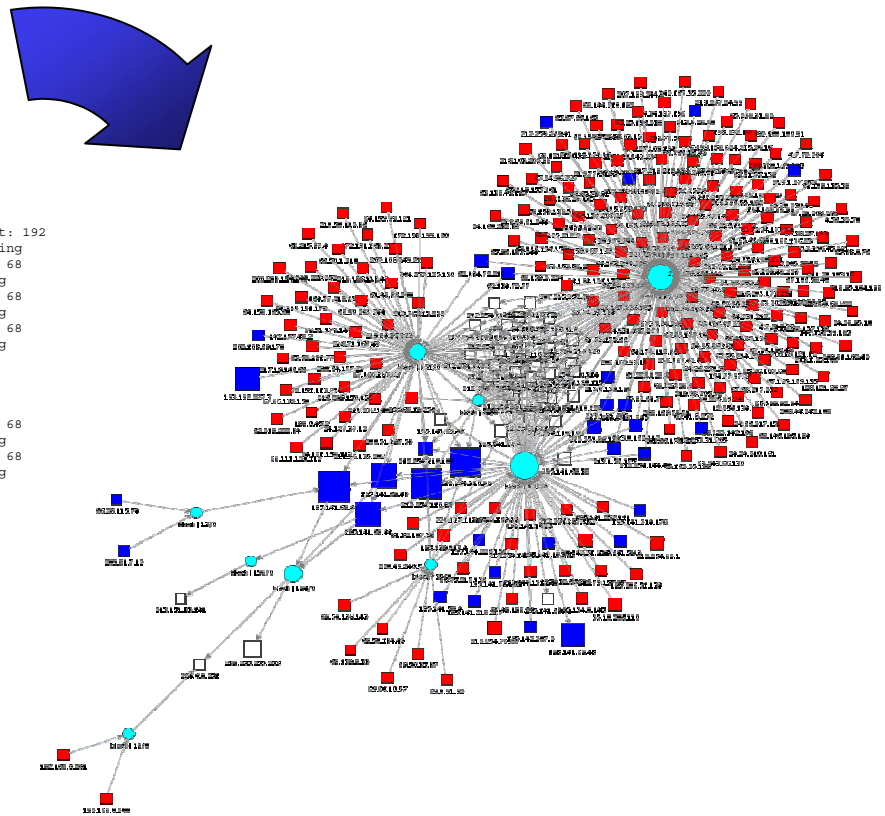


> **IP addresses and host names showing up in event graphs and descriptions were obfuscated/changed. The addresses are completely random and any resemblance with well-known addresses or host names are purely coincidental.**

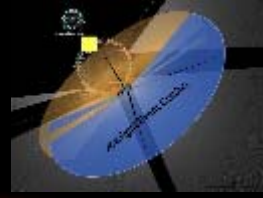
Text or Visuals?

- What would you rather look at?

```
Jun 17 09:42:30 rmarty ifup: Determining IP information for eth0...
Jun 17 09:42:35 rmarty ifup:  failed; no link present.  Check cable?
Jun 17 09:42:35 rmarty network: Bringing up interface eth0:  failed
Jun 17 09:42:38 rmarty sendmail: sendmail shutdown succeeded
Jun 17 09:42:38 rmarty sendmail: sm-client shutdown succeeded
Jun 17 09:42:39 rmarty sendmail: sendmail startup succeeded
Jun 17 09:42:39 rmarty sendmail: sm-client startup succeeded
Jun 17 09:43:39 rmarty vmnet-dhcpd: DHCPINFORM from 172.16.48.128
Jun 17 09:45:42 rmarty last message repeated 2 times
Jun 17 09:45:47 rmarty vmnet-dhcpd: DHCPINFORM from 172.16.48.128
Jun 17 09:56:02 rmarty vmnet-dhcpd: DHCPDISCOVER from 00:0c:29:b7:b2:47 via vmnet8
Jun 17 09:56:03 rmarty vmnet-dhcpd: DHCPOFFER on 172.16.48.128 to 00:0c:29:b7:b2:47 via vmnet8
Jun 17 09:56:03 rmarty vmnet-dhcpd: DHCPREQUEST for 172.16.48.128 from 00:0c:29:b7:b2:47 via vmnet8
Jun 17 09:56:03 rmarty vmnet-dhcpd: DHCPACK on 172.16.48.128 to 00:0c:29:b7:b2:47 via vmnet8
Jun 17 10:00:03 rmarty crond(pam_unix)[30534]: session opened for user root by (uid=0)
Jun 17 10:00:10 rmarty crond(pam_unix)[30534]: session closed for user root
Jun 17 10:01:02 rmarty crond(pam_unix)[30551]: session opened for user root by (uid=0)
Jun 17 10:01:07 rmarty crond(pam_unix)[30551]: session closed for user root
Jun 17 10:05:02 rmarty crond(pam_unix)[30567]: session opened for user idabench by (uid=0)
Jun 17 10:05:05 rmarty crond(pam_unix)[30567]: session closed for user idabench
Jun 17 10:13:05 rmarty portsentry[4797]: attackalert: UDP scan from host: 192.168.80.19/192.168.80.19 to UDP port: 192
Jun 17 10:13:05 rmarty portsentry[4797]: attackalert: Host: 192.168.80.19/192.168.80.19 is already blocked Ignoring
Jun 17 10:14:09 rmarty portsentry[4797]: attackalert: UDP scan from host: 192.168.80.8/192.168.80.8 to UDP port: 68
Jun 17 10:14:09 rmarty portsentry[4797]: attackalert: Host: 192.168.80.8/192.168.80.8 is already blocked Ignoring
Jun 17 10:14:09 rmarty portsentry[4797]: attackalert: UDP scan from host: 192.168.80.8/192.168.80.8 to UDP port: 68
Jun 17 10:14:09 rmarty portsentry[4797]: attackalert: Host: 192.168.80.8/192.168.80.8 is already blocked Ignoring
Jun 17 10:21:30 rmarty portsentry[4797]: attackalert: UDP scan from host: 192.168.80.8/192.168.80.8 to UDP port: 68
Jun 17 10:21:30 rmarty portsentry[4797]: attackalert: Host: 192.168.80.8/192.168.80.8 is already blocked Ignoring
Jun 17 10:28:40 rmarty vmnet-dhcpd: DHCPDISCOVER from 00:0c:29:b7:b2:47 via vmnet8
Jun 17 10:28:41 rmarty vmnet-dhcpd: DHCPOFFER on 172.16.48.128 to 00:0c:29:b7:b2:47 via vmnet8
Jun 17 10:28:41 rmarty vmnet-dhcpd: DHCPREQUEST for 172.16.48.128 from 00:0c:29:b7:b2:47 via vmnet8
Jun 17 10:28:45 rmarty vmnet-dhcpd: DHCPACK on 172.16.48.128 to 00:0c:29:b7:b2:47 via vmnet8
Jun 17 10:30:47 rmarty portsentry[4797]: attackalert: UDP scan from host: 192.168.80.8/192.168.80.8 to UDP port: 68
Jun 17 10:30:47 rmarty portsentry[4797]: attackalert: Host: 192.168.80.8/192.168.80.8 is already blocked Ignoring
Jun 17 10:30:47 rmarty portsentry[4797]: attackalert: UDP scan from host: 192.168.80.8/192.168.80.8 to UDP port: 68
Jun 17 10:30:47 rmarty portsentry[4797]: attackalert: Host: 192.168.80.8/192.168.80.8 is already blocked Ignoring
Jun 17 10:35:28 rmarty vmnet-dhcpd: DHCPINFORM from 172.16.48.128
Jun 17 10:35:31 rmarty vmnet-dhcpd: DHCPINFORM from 172.16.48.128
Jun 17 10:38:51 rmarty vmnet-dhcpd: DHCPREQUEST for 172.16.48.128 from 00:0c:29:b7:b2:47 via vmnet8
Jun 17 10:38:52 rmarty vmnet-dhcpd: DHCPACK on 172.16.48.128 to 00:0c:29:b7:b2:47 via vmnet8
Jun 17 10:42:35 rmarty vmnet-dhcpd: DHCPINFORM from 172.16.48.128
Jun 17 10:42:38 rmarty vmnet-dhcpd: DHCPINFORM from 172.16.48.128
```

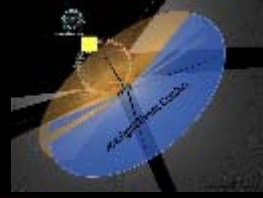


Why Using Event Graphs?



- Visual representation of textual information (logs and events)
- Visual display of most important properties
- Reduce analysis and response times
  - Quickly visualize thousands of events
  - A picture tells more than a thousand log lines
- Situational awareness
  - Visualize status of business posture
- Facilitate communication
  - Use graphs to communicate with other teams
  - Graphs are easier to understand than textual events

When To Use Event Graphs

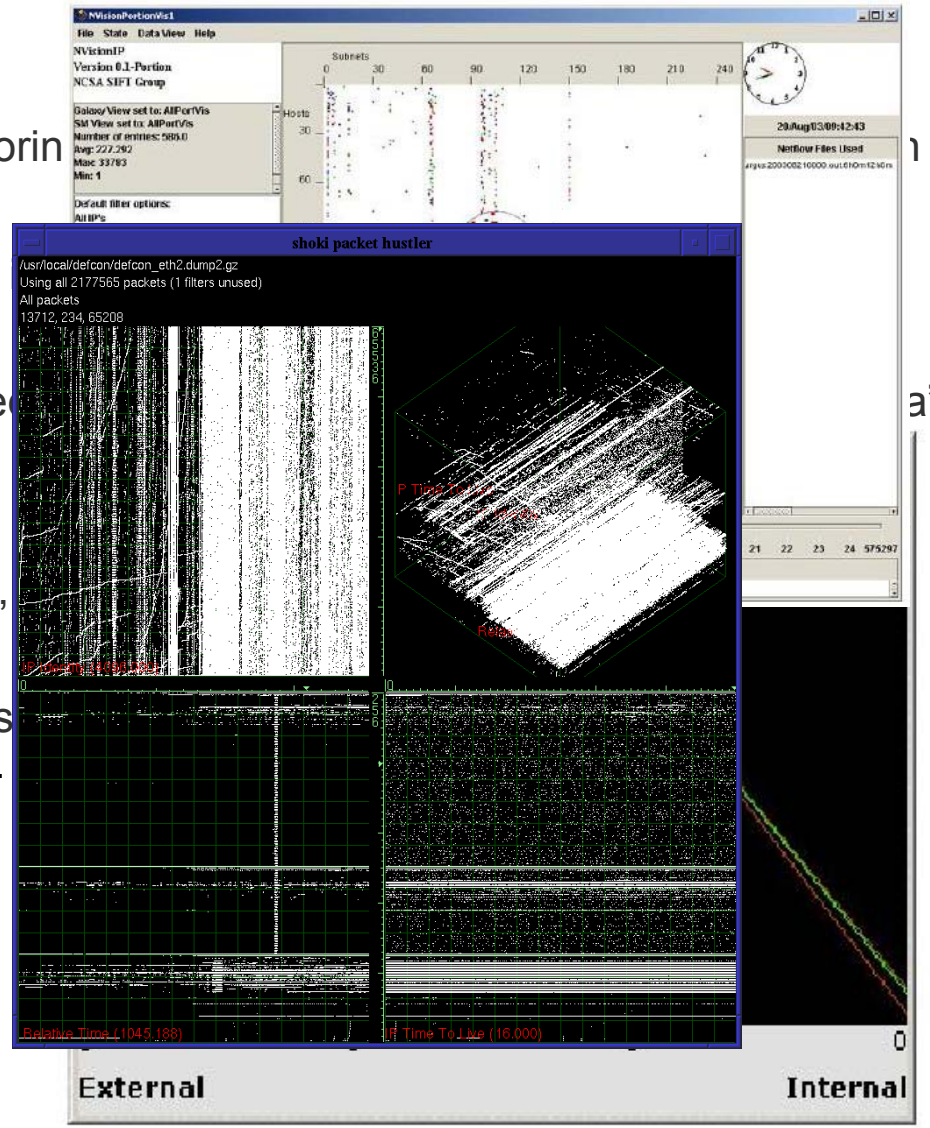


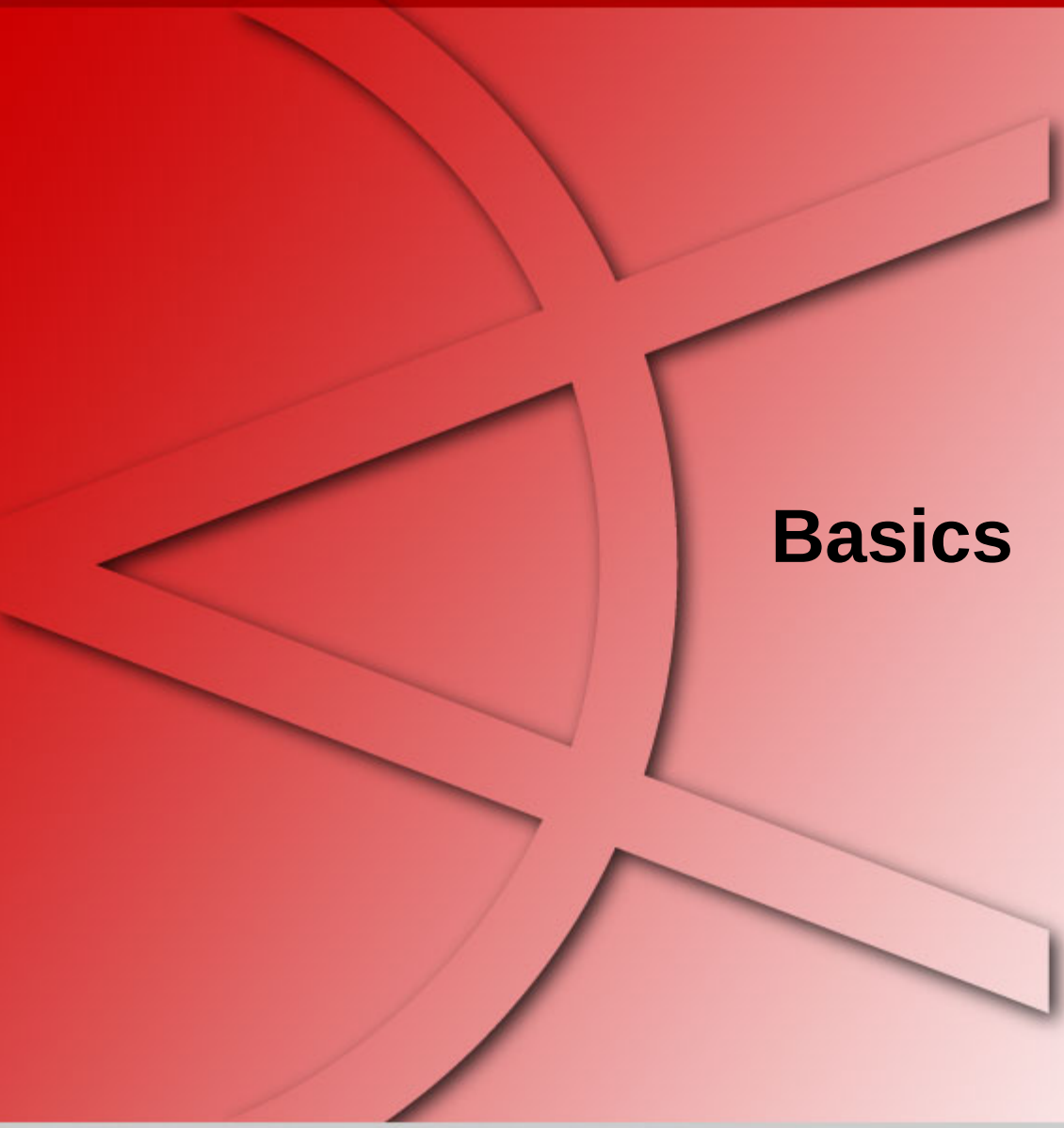
- Real-time monitoring
  - What is happening in a specific business area (e.g., compliance monitoring)
  - What is happening on a specific network
  - What are certain servers doing
  - Look at specific aspects of events
- Forensics and Investigations
  - Selecting arbitrary set of events for investigation
  - Understanding big picture
  - Analyzing relationships

Related Work

Related Work

- Classics
  - Girardin Luc, “A visual Approach for Monitorin … Conference
  - Erbacher: “Intrusion and Misuse Detection … Graphics and Applications
  - Sheng Ma, et al. “EventMiner: An integrate… a”
- Tools
  - Greg Conti, “Network Attack Visualization”, Defcon 2004.
  - NVisionIP from SIFT (Security Incident Fus… Tools), http://www.ncassr.org/projects/sift/.
  - Stephen P. Berry, “The Shoki Packet Hustler”, http://shoki.sourceforge.net.

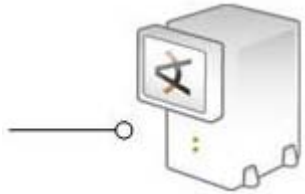




Basics

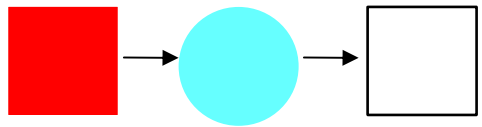
How To Draw An Event Graph?

... | Normalization | ...



Device **Parser** **Event Analyzer / Visualizer**

```
Jun 17 09:42:30 rmarty ifup: Determining IP information for eth0...
Jun 17 09:42:35 rmarty ifup:  failed; no link present.  Check cable?
Jun 17 09:42:35 rmarty network: Bringing up interface eth0:  failed
Jun 17 09:42:38 rmarty sendmail: sendmail shutdown succeeded
Jun 17 09:42:38 rmarty sendmail: sm-client shutdown succeeded
Jun 17 09:42:39 rmarty sendmail: sendmail startup succeeded
Jun 17 09:42:39 rmarty sendmail: sm-client startup succeeded
Jun 17 09:43:39 rmarty vmnet-dhcpd: DHCPINFORM from 172.16.48.128
Jun 17 09:45:42 rmarty last message repeated 2 times
Jun 17 09:45:47 rmarty vmnet-dhcpd: DHCPINFORM from 172.16.48.128
Jun 17 09:56:02 rmarty vmnet-dhcpd: DHCPDISCOVER from 00:0c:29:b7:b2:47 via vmnet8
Jun 17 09:56:03 rmarty vmnet-dhcpd: DHCPOFFER on 172.16.48.128 to 00:0c:29:b7:b2:47 via vmnet8
NH
```



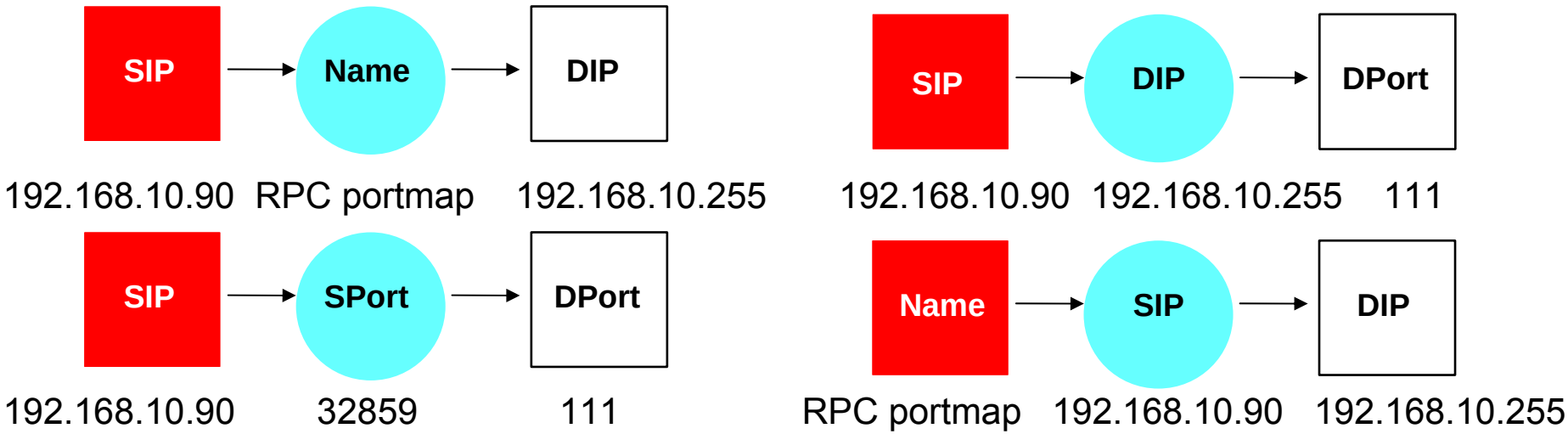
Log File **Event Graph**

Different Node Configurations

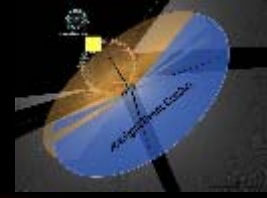
Raw Event:

```
[**] [1:1923:2] RPC portmap UDP proxy attempt [**]
[Classification: Decode of an RPC Query] [Priority: 2]
06/04-15:56:28.219753 192.168.10.90:32859 ->
192.168.10.255:111
UDP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:148 DF
Len: 120
```

Different node configurations:



AfterGlow – Peak Preview



- AfterGlow is not a SIM - there are no parsers (well, tcpdump and sendmail are there).

- Demo of the … e Jacuzzi.

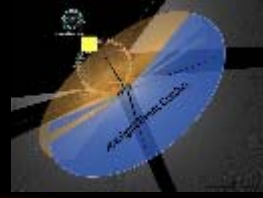
```
cat input.c…                                  …r.properties
| neato –Tg…
```

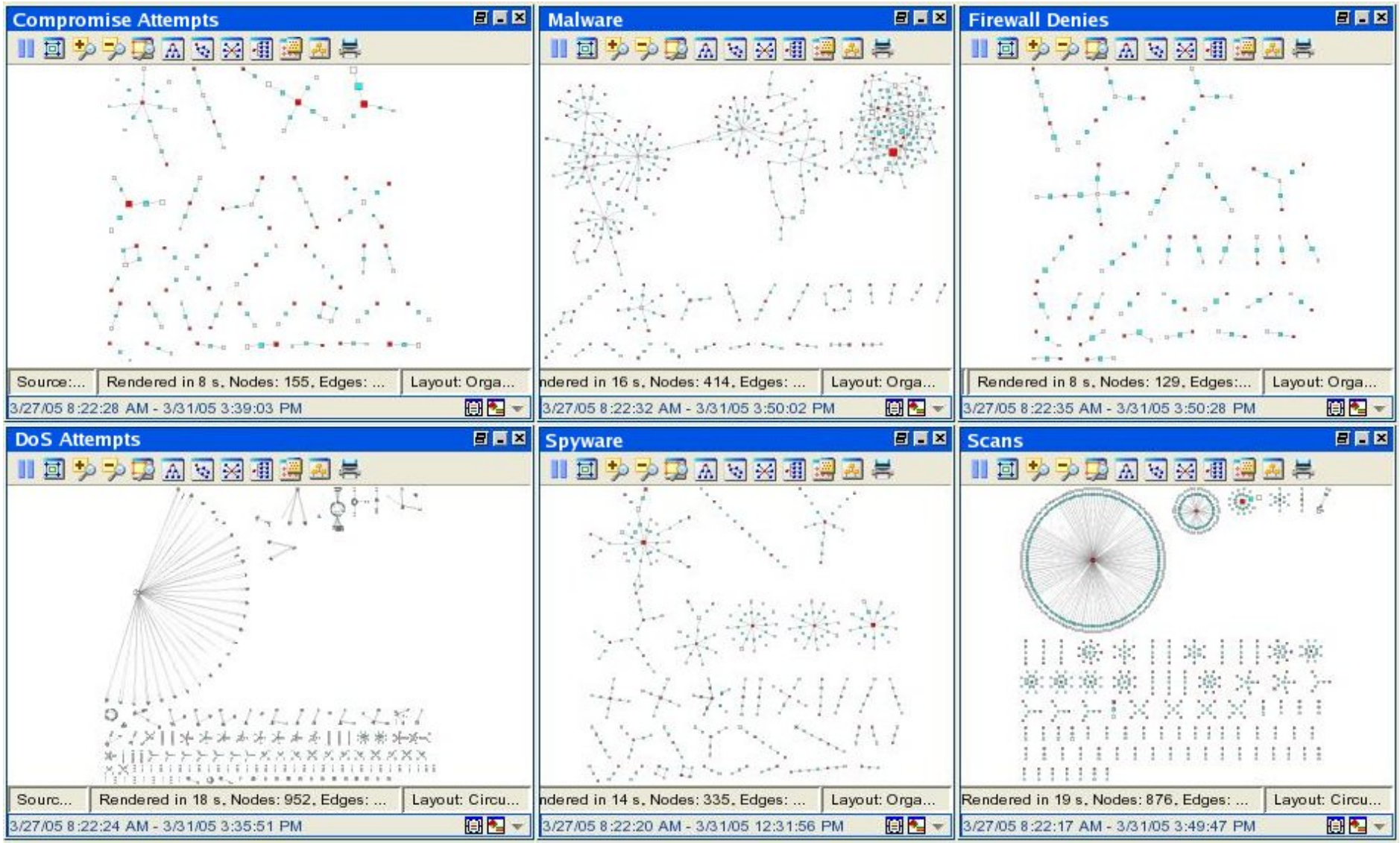
```
color.properties:

color.source="red"
color.event="green"
color.target="blue"
```

Thanks to Christian @ ArcSight!

Situational Awareness

Real-time Monitoring With A Dashboard

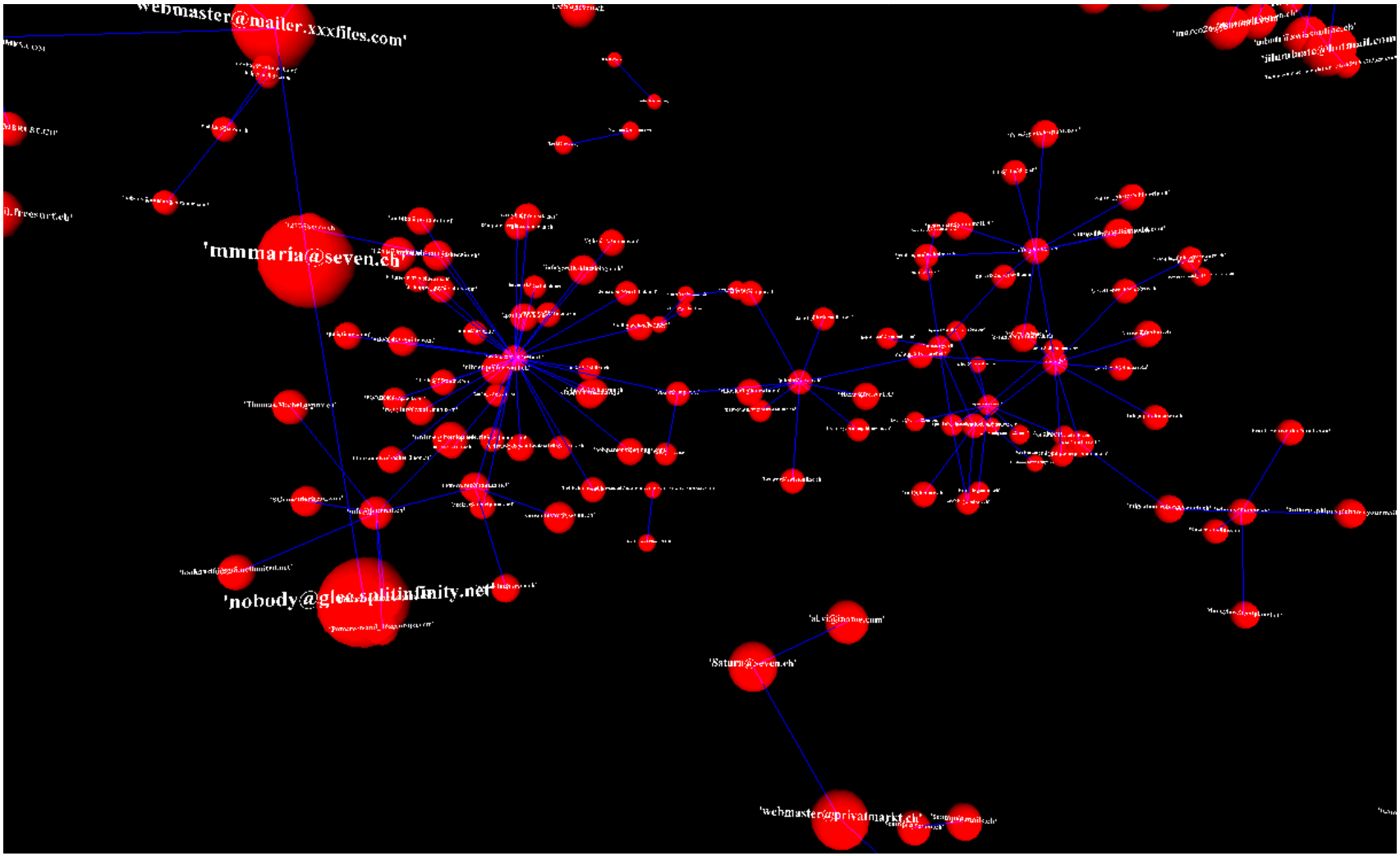




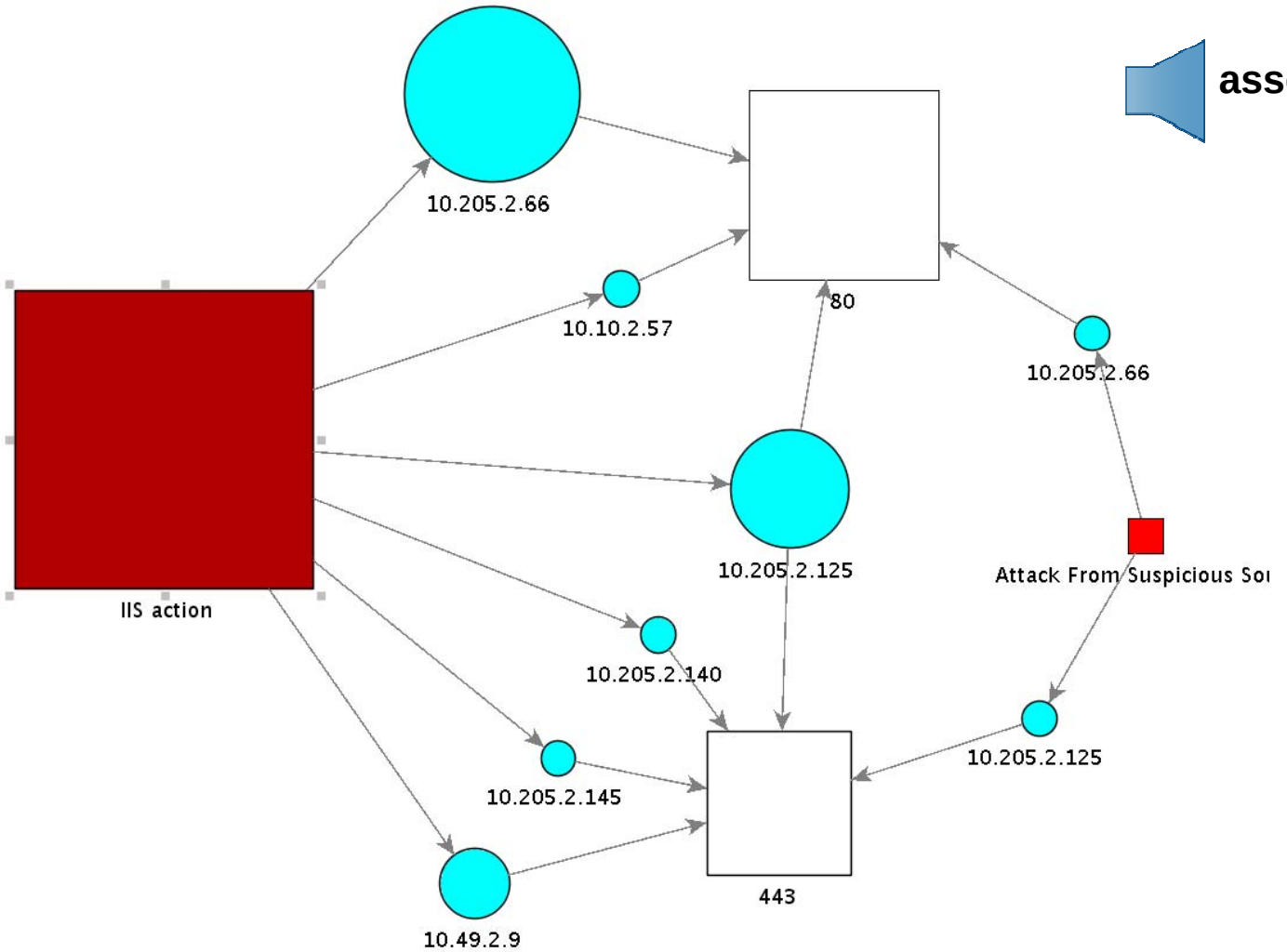
Forensic and Historical Analysis

A 3D Example

- An LGL example:

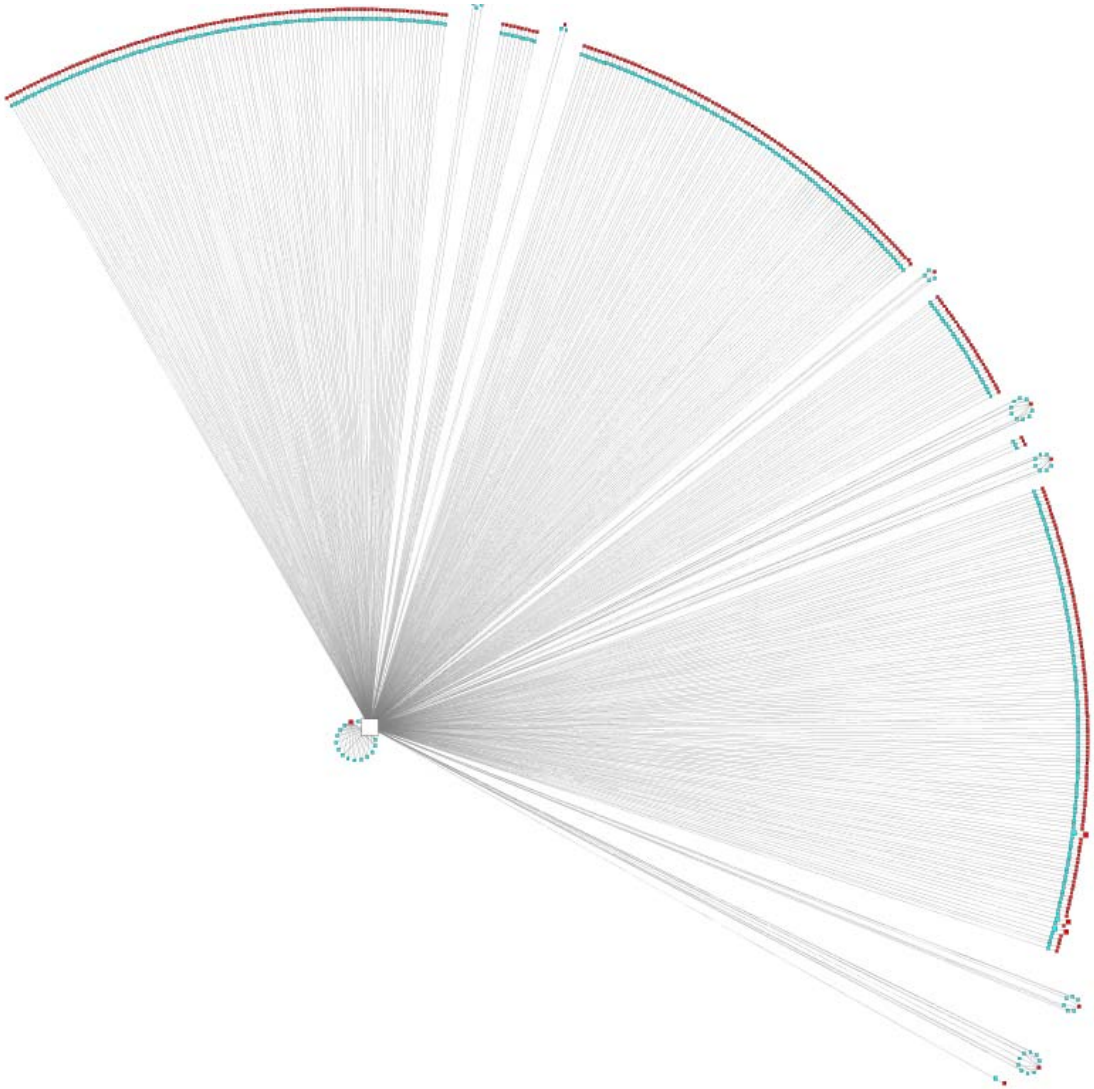


Monitoring Web Servers

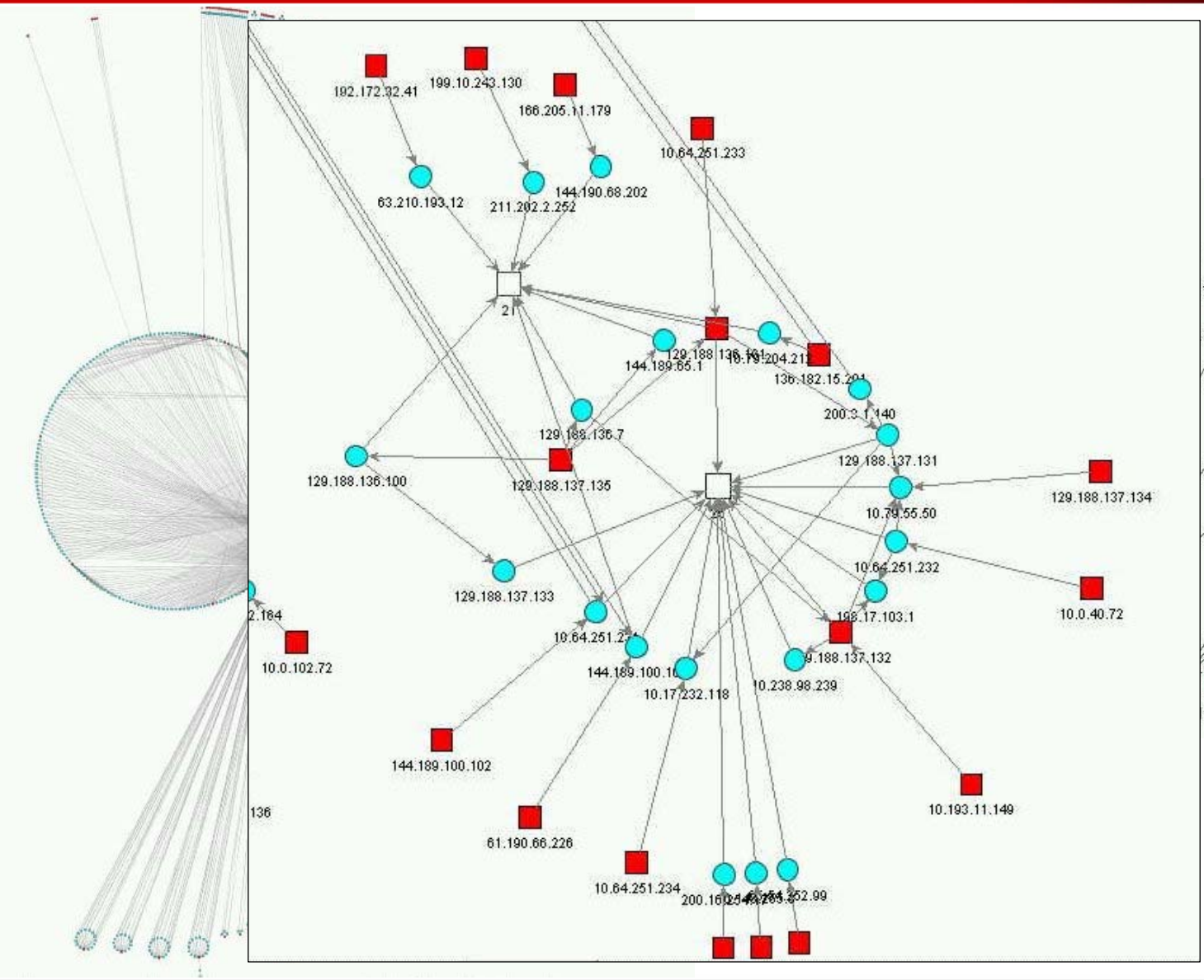


assetCategory(DestIP)= WebServer

Network Scan

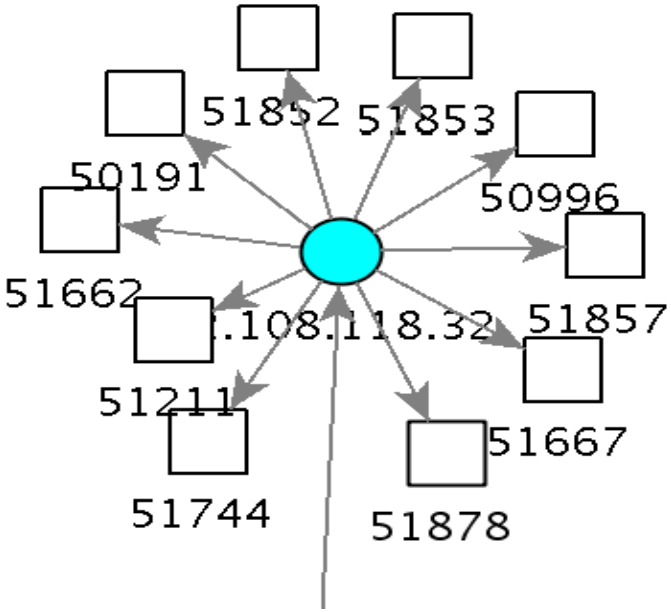


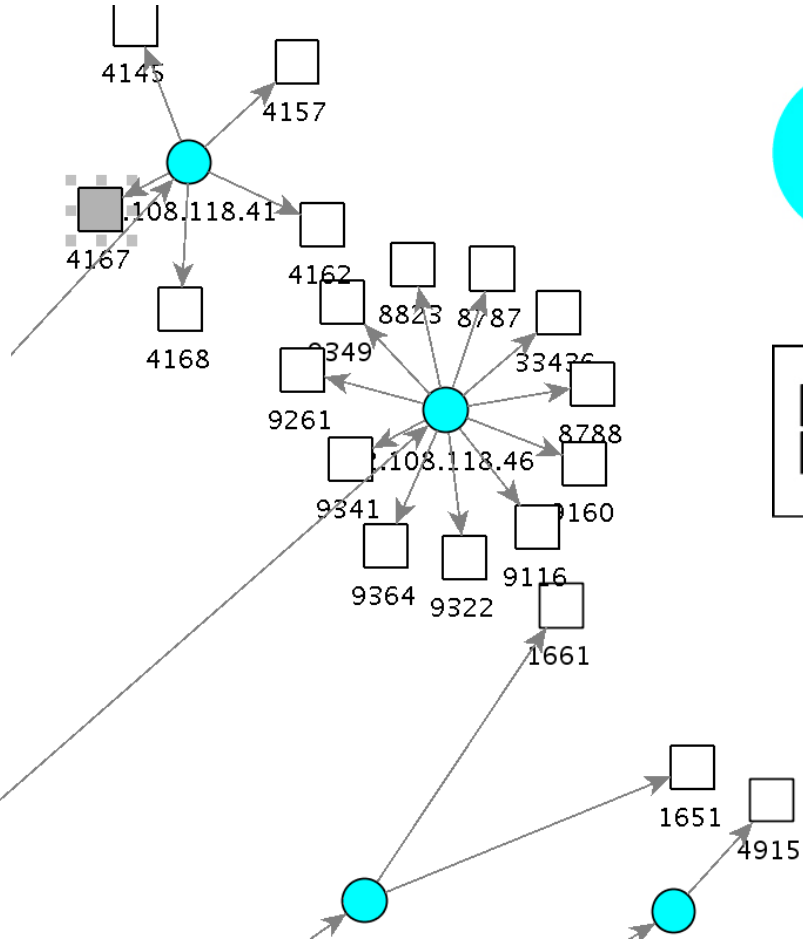
Suspicious Activity?



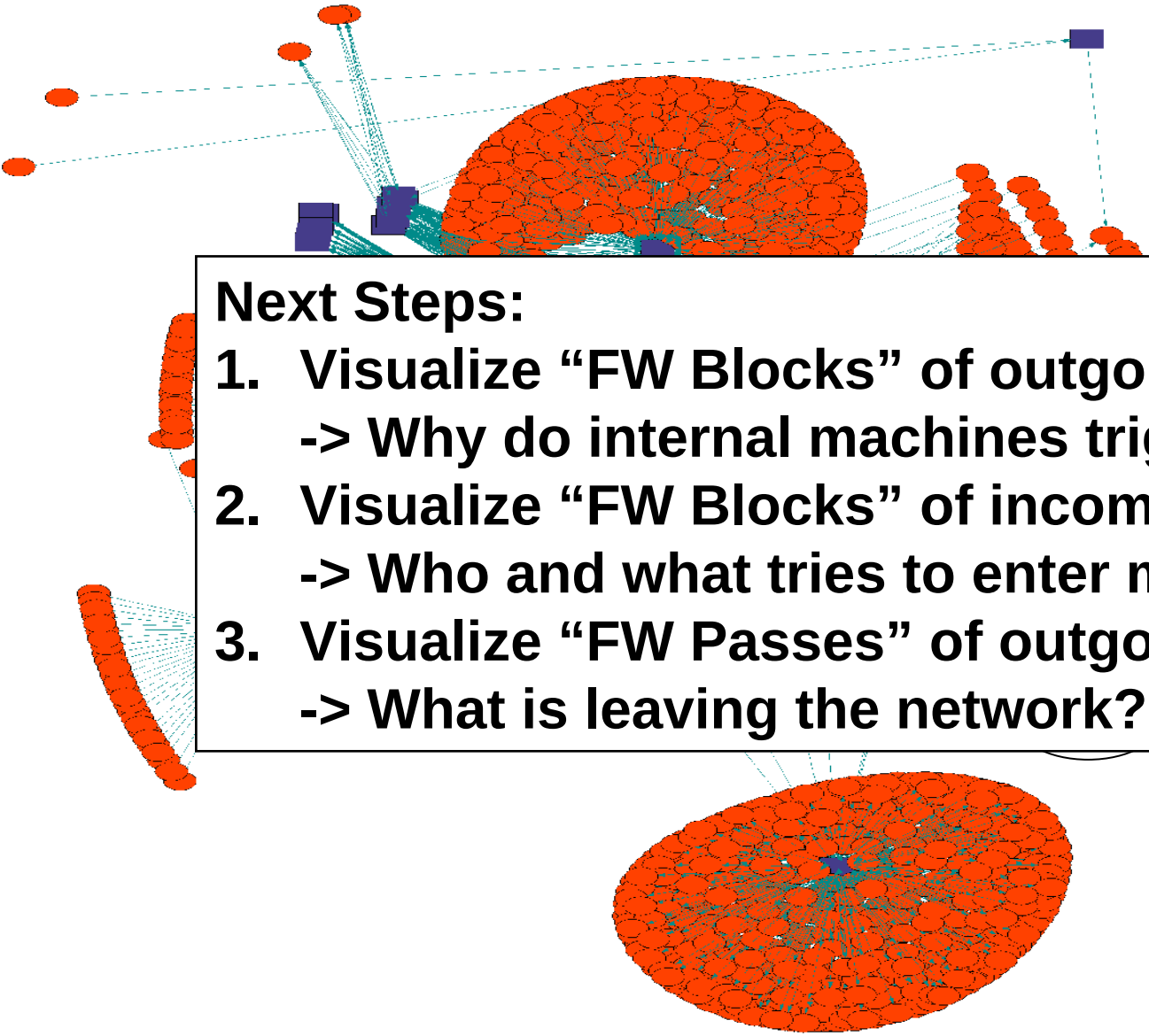
Port Scan

- Port scan or something else?





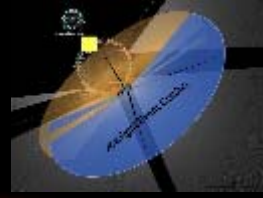
Firewall Activity

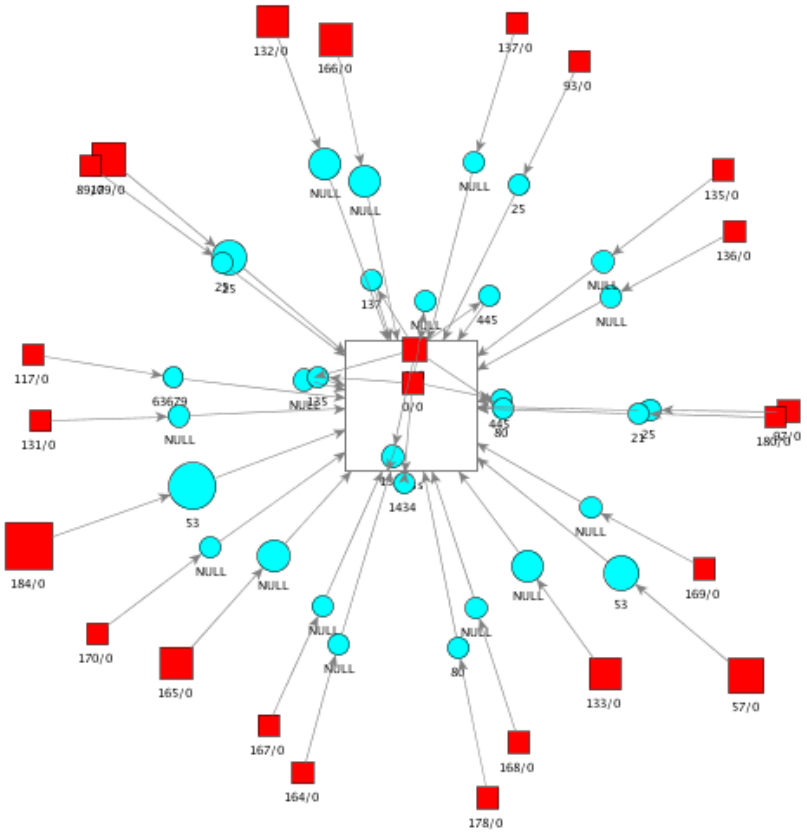


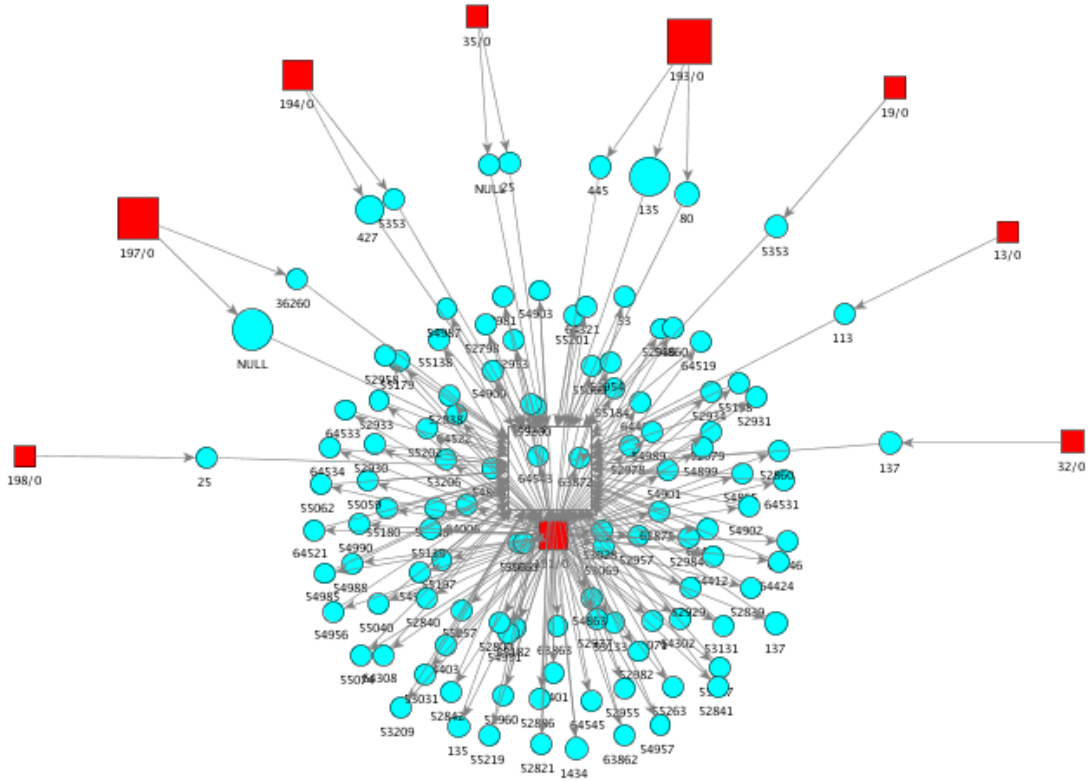
Next Steps:

1. **Visualize "FW Blocks" of outgoing traffic**
   -> Why do internal machines trigger blocks?
2. **Visualize "FW Blocks" of incoming traffic**
   -> Who and what tries to enter my network?
3. **Visualize "FW Passes" of outgoing traffic**
   -> What is leaving the network?

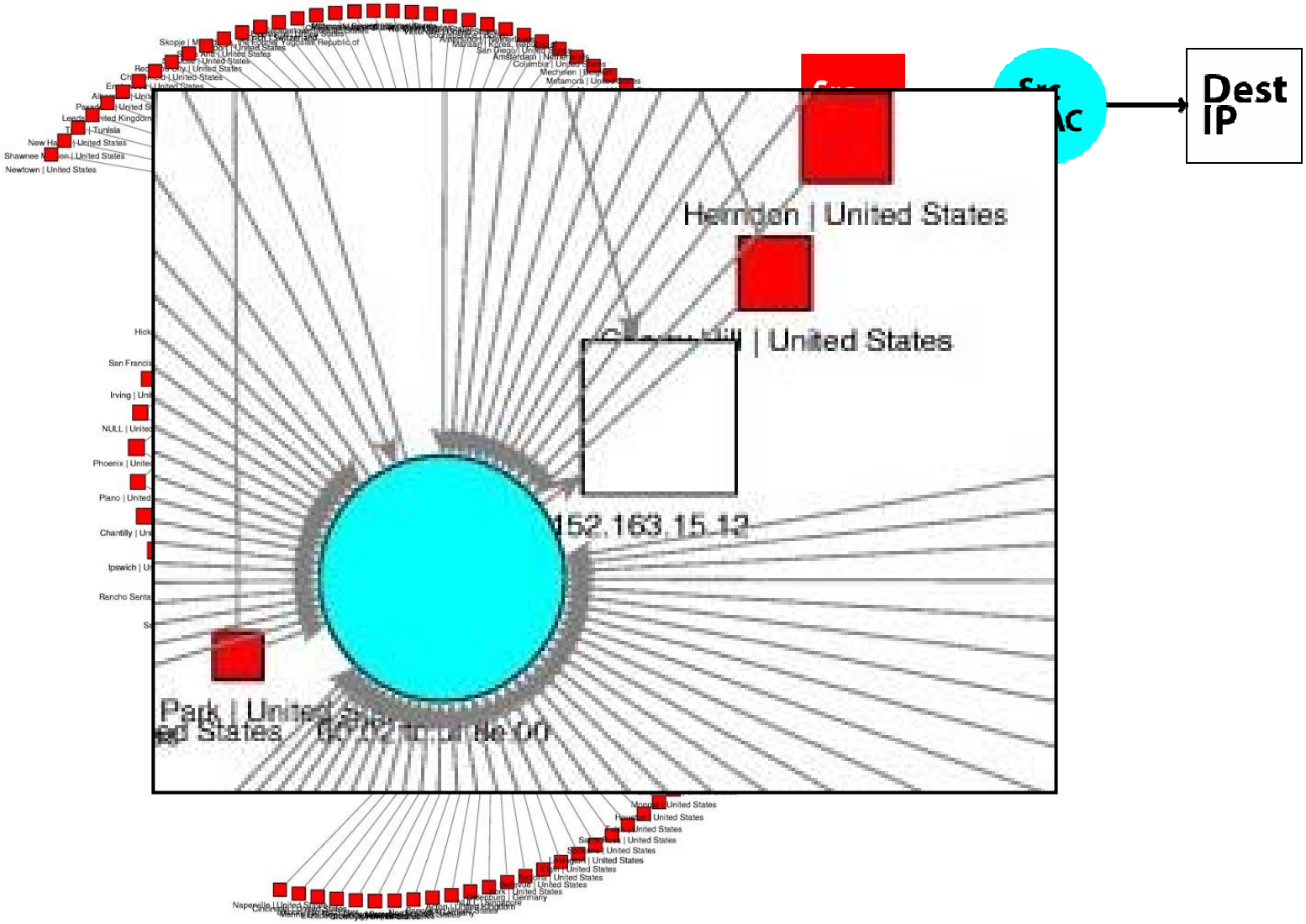
Firewall Rule-set Analysis



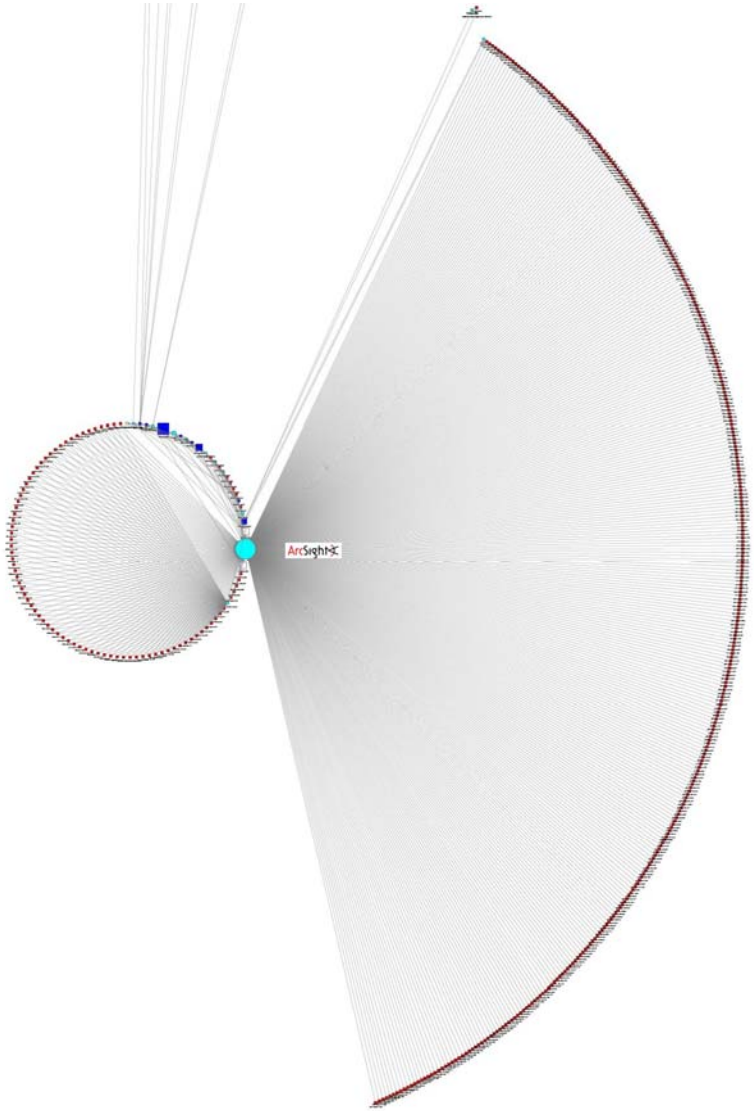




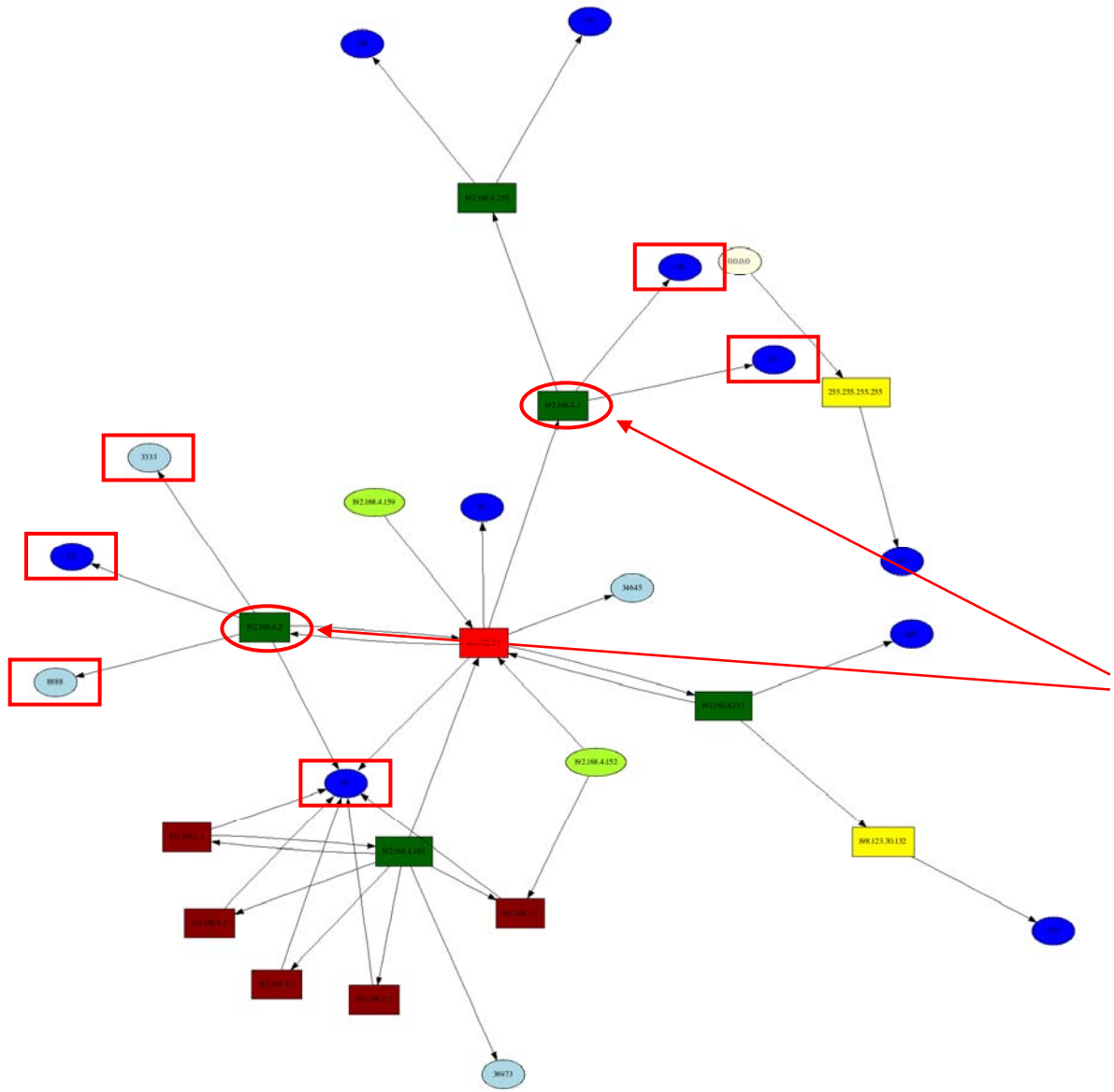
Load Balancer



Worms



DefCon 2004 Capture The Flag



DstPort < 1024

DstPort > 1024

Source Of Evil

Internal Target

Other Team's Target

Internal Source

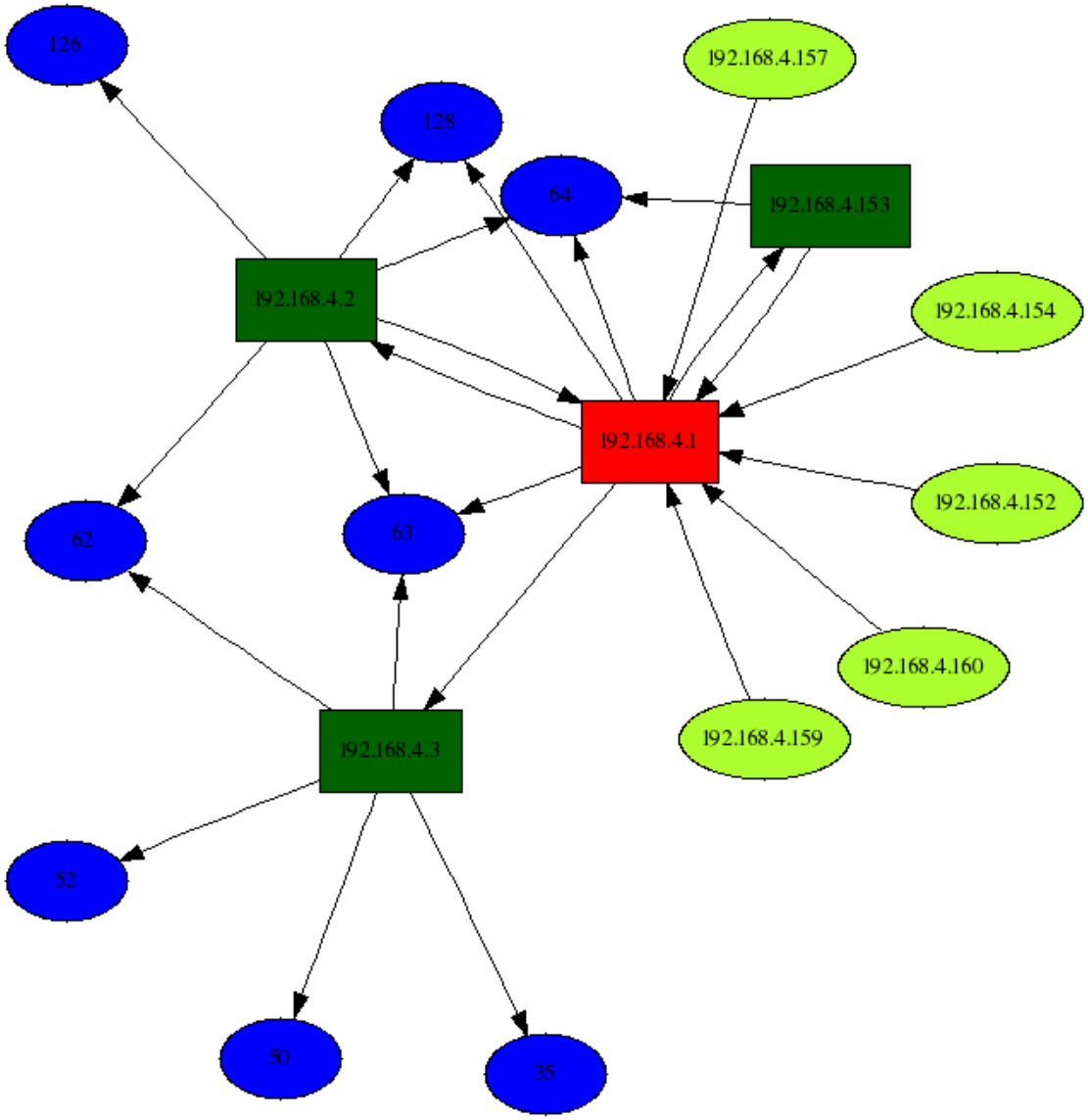
Internet Target

Exposed Services

Our Servers

SIP → DIP → DPort

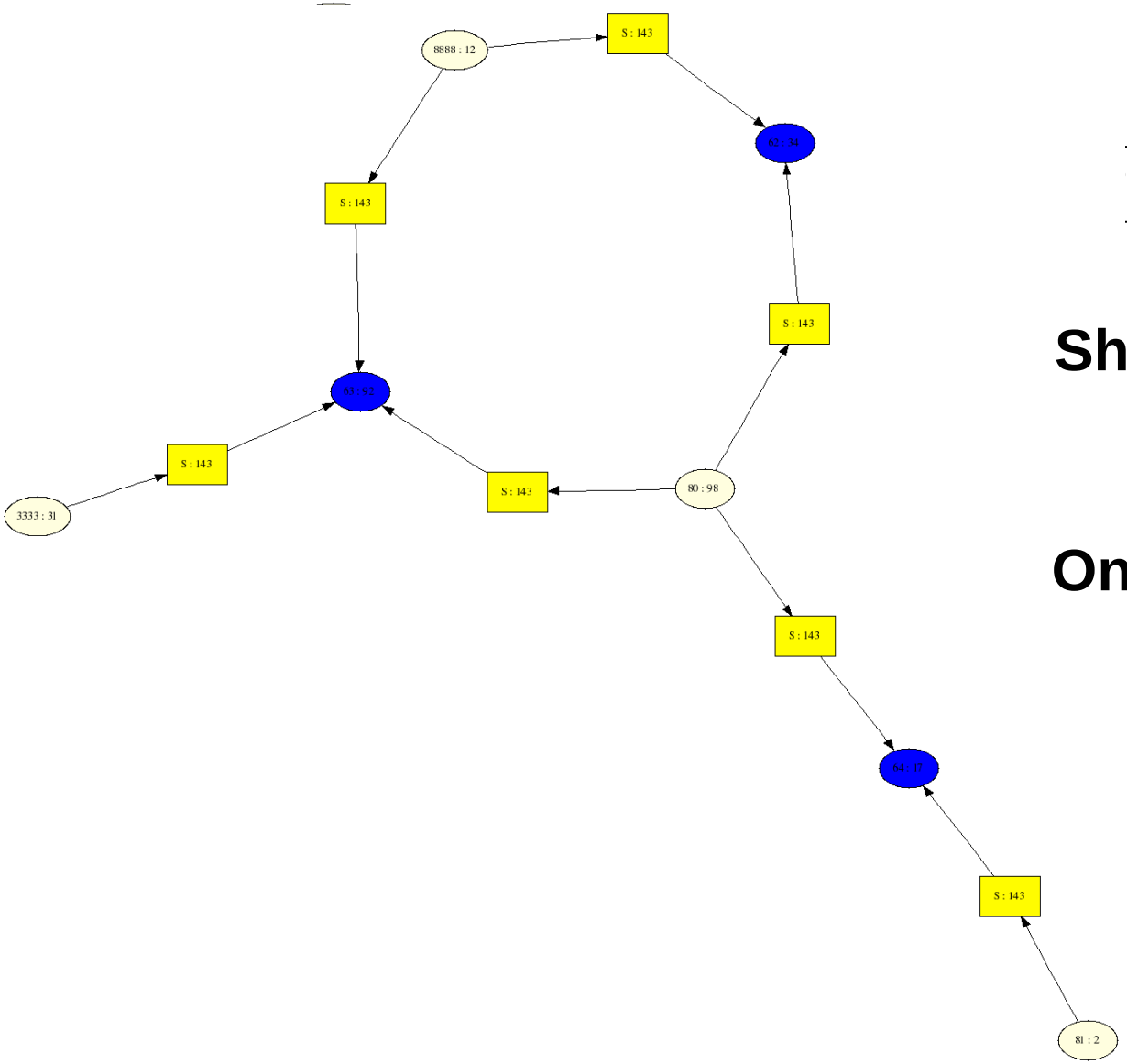
DefCon 2004 Capture The Flag – TTL Games



TTL
Source Of Evil
Internal Target
Internal Source

SIP → DIP → TTL

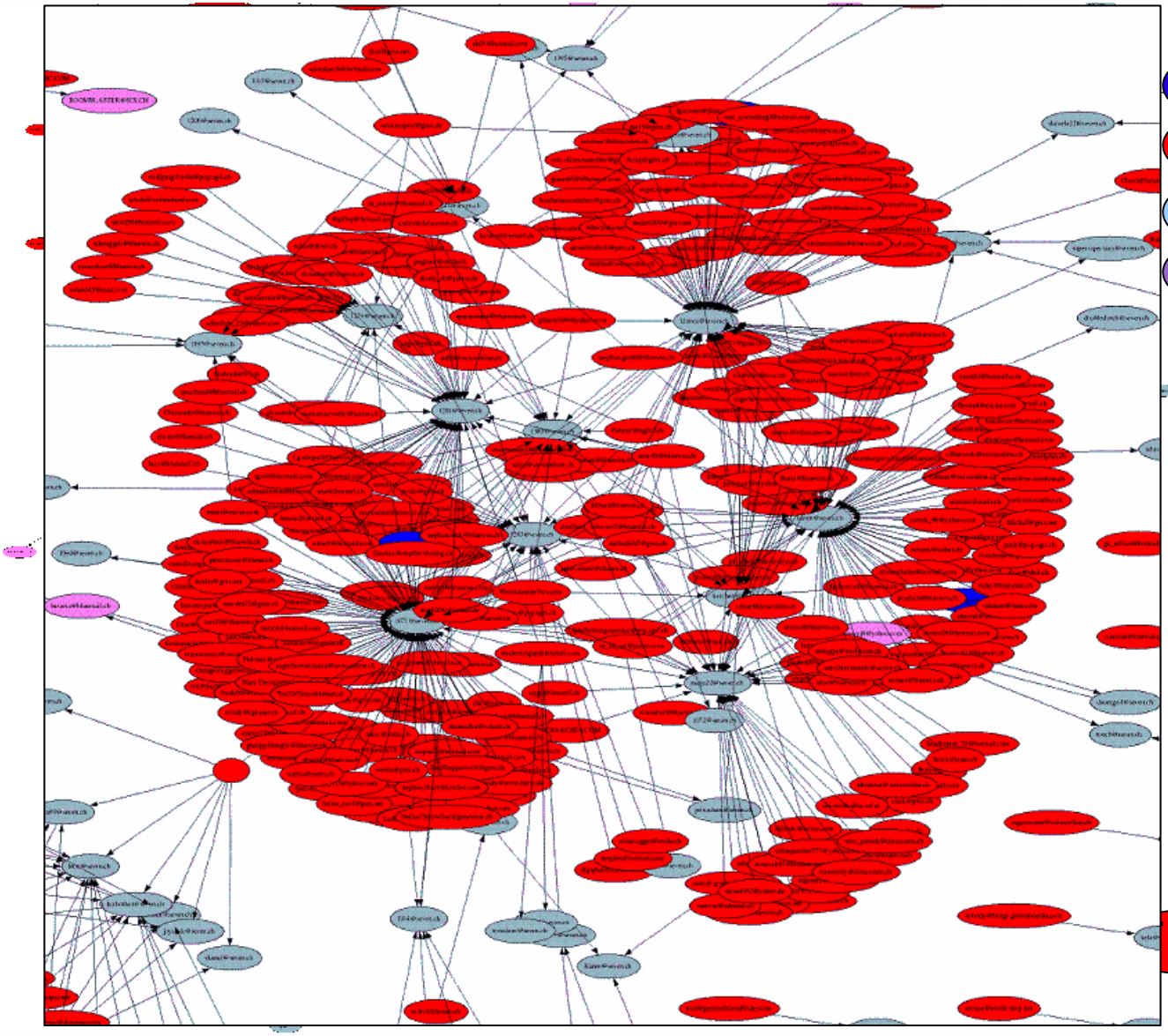
DefCon 2004 Capture The Flag – The Solution



Show Node Counts

Only show SYNs

Email Cliques



From: My Domain

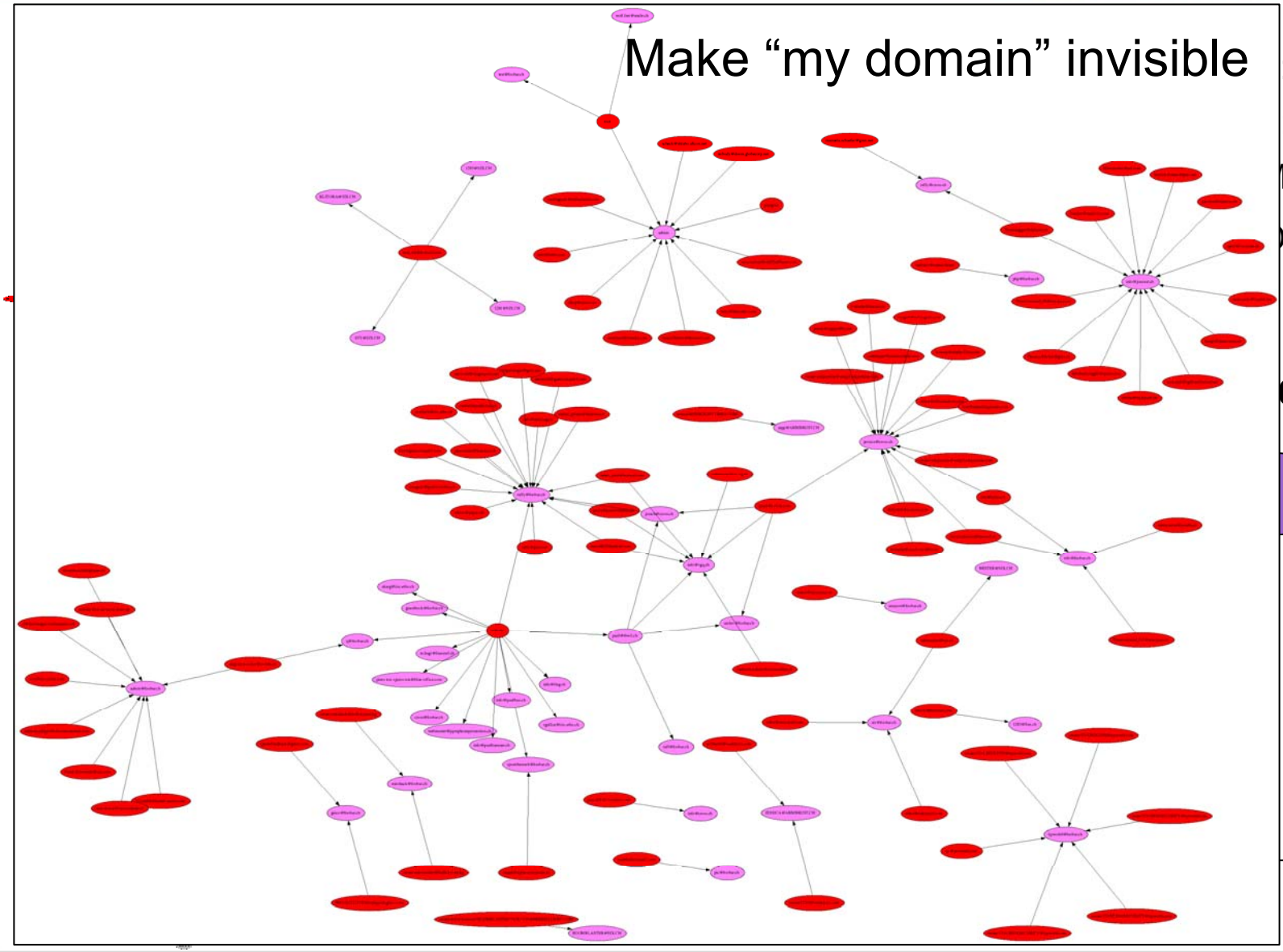
From: Other Domain

To: My Domain

To: Other Domain

rom → To

Email Relays



: My Domain

: Other Domain

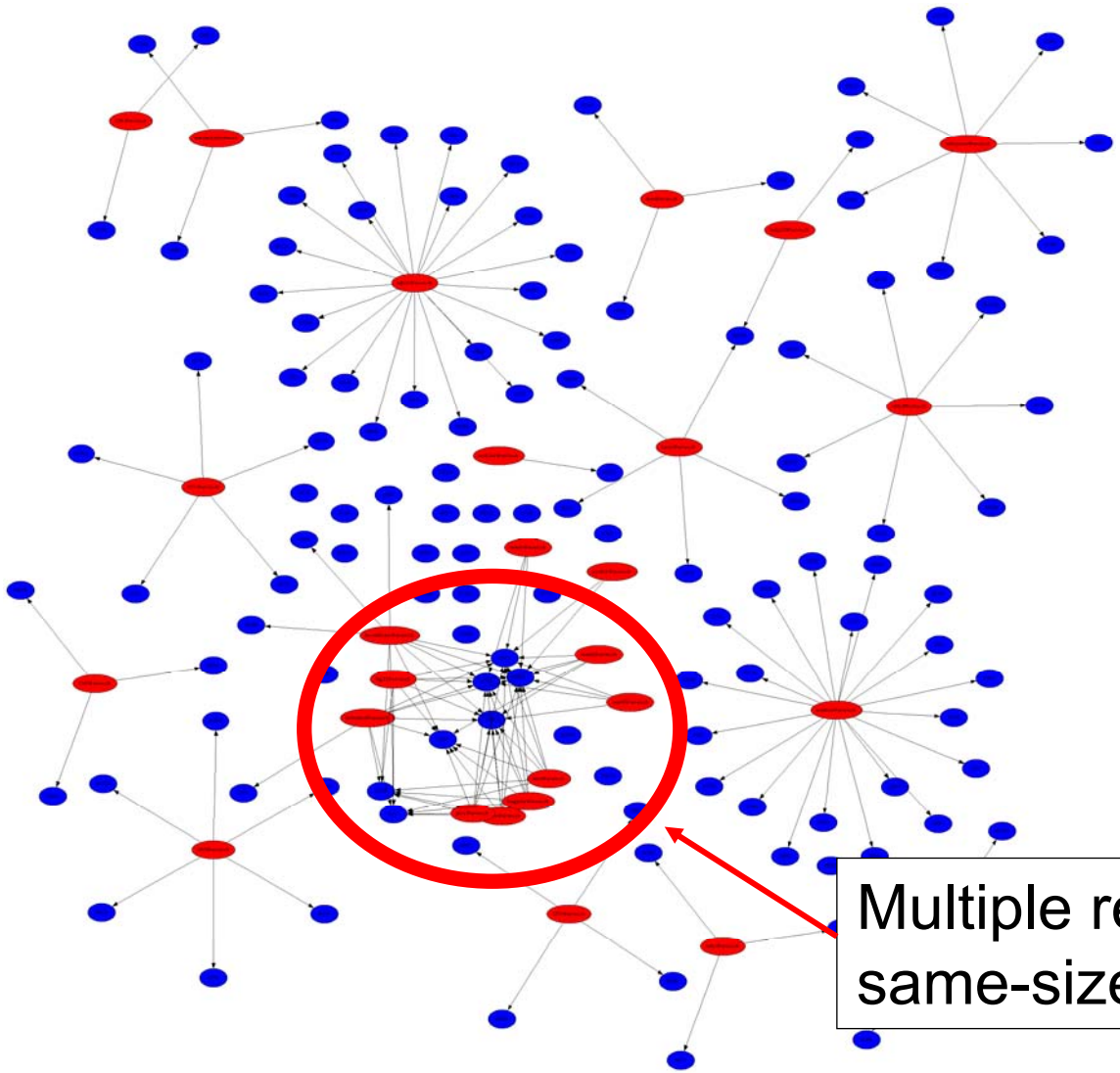
My Domain

Other Domain

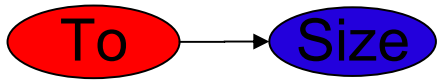
en relay?

To

Email SPAM?

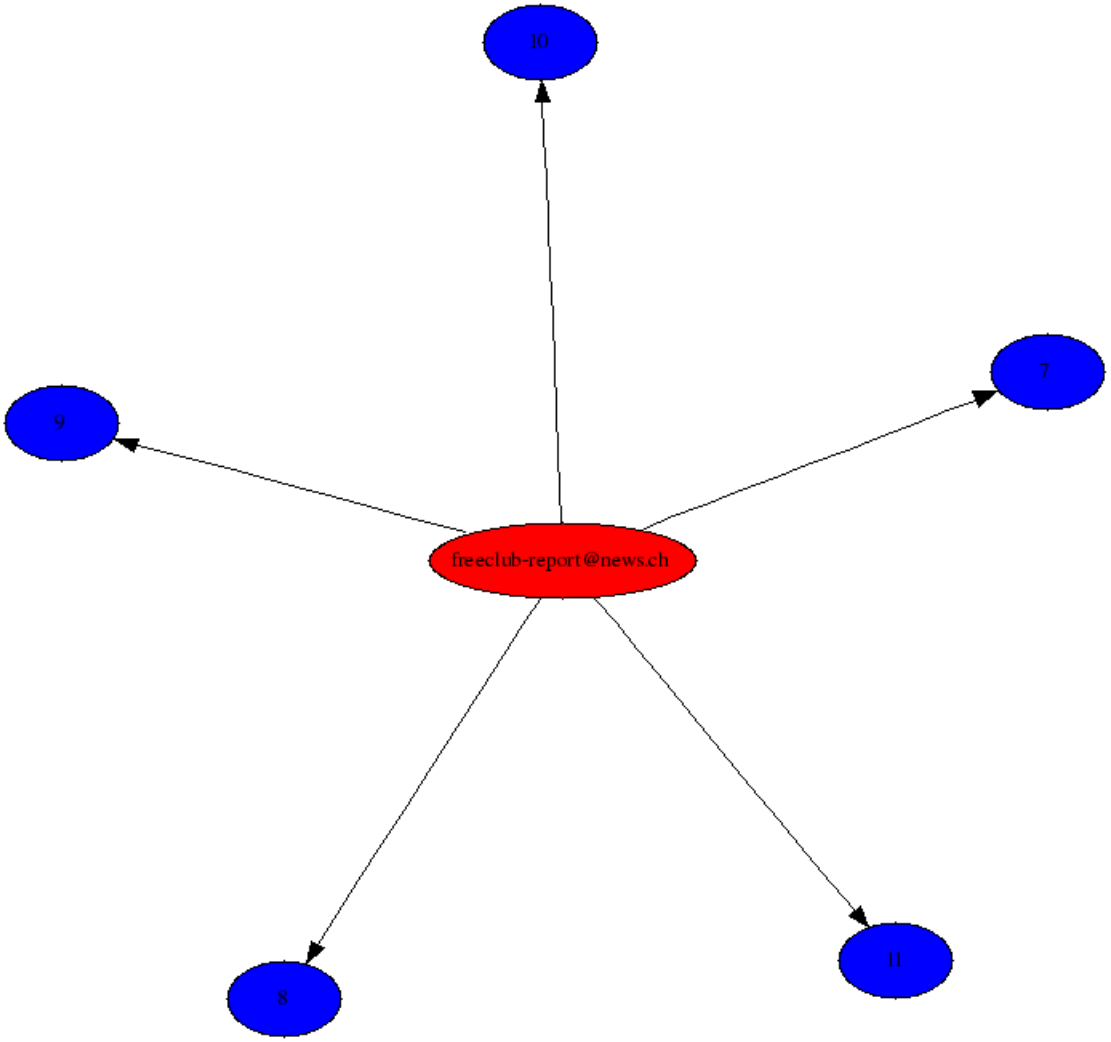


Size > 10.000
Omit threshold = 1

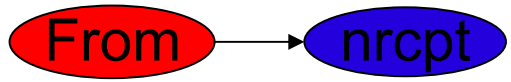


Multiple recipients with same-size messages

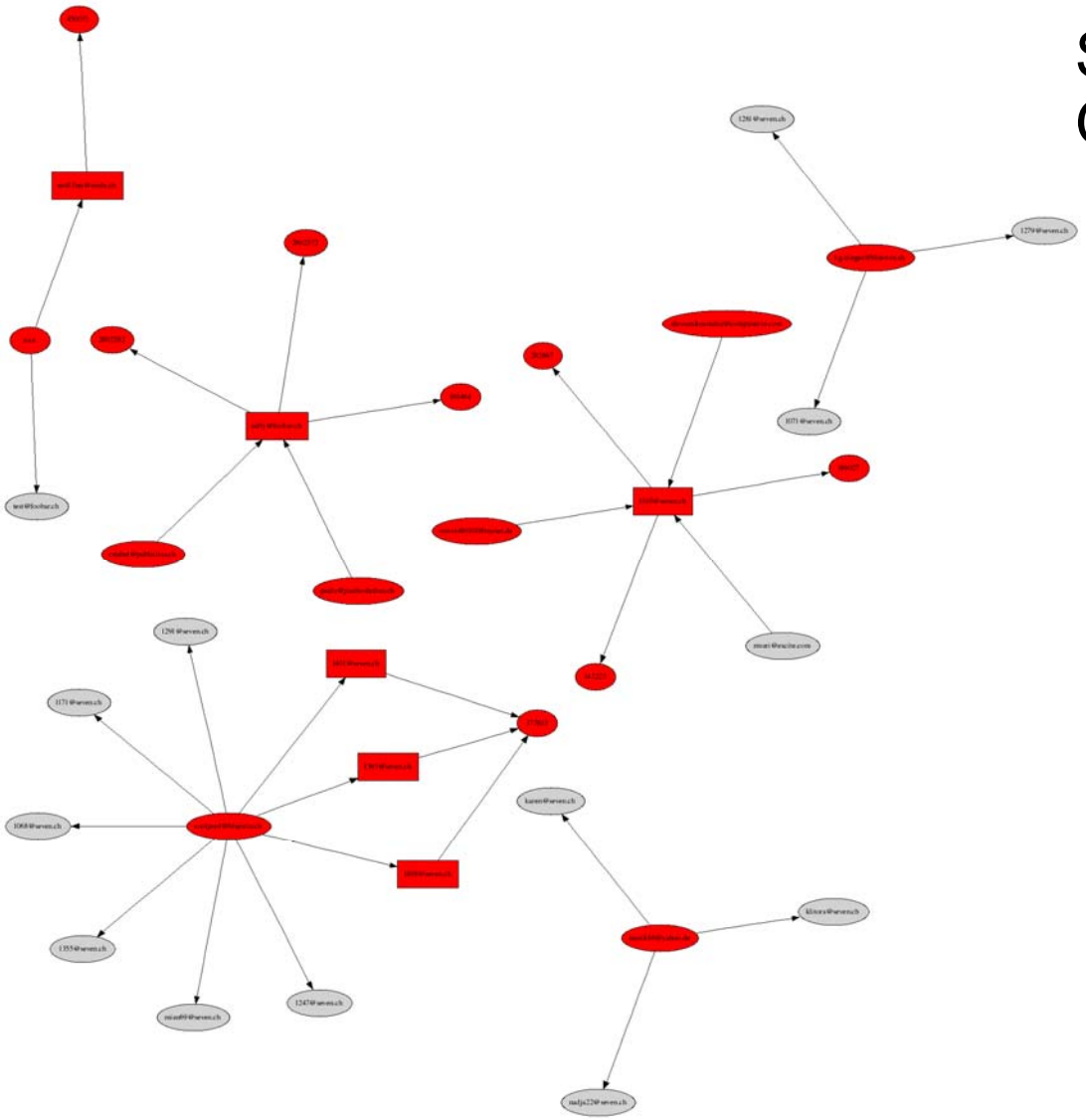
Email SPAM?



nrcpt => 2
Omit threshold = 1



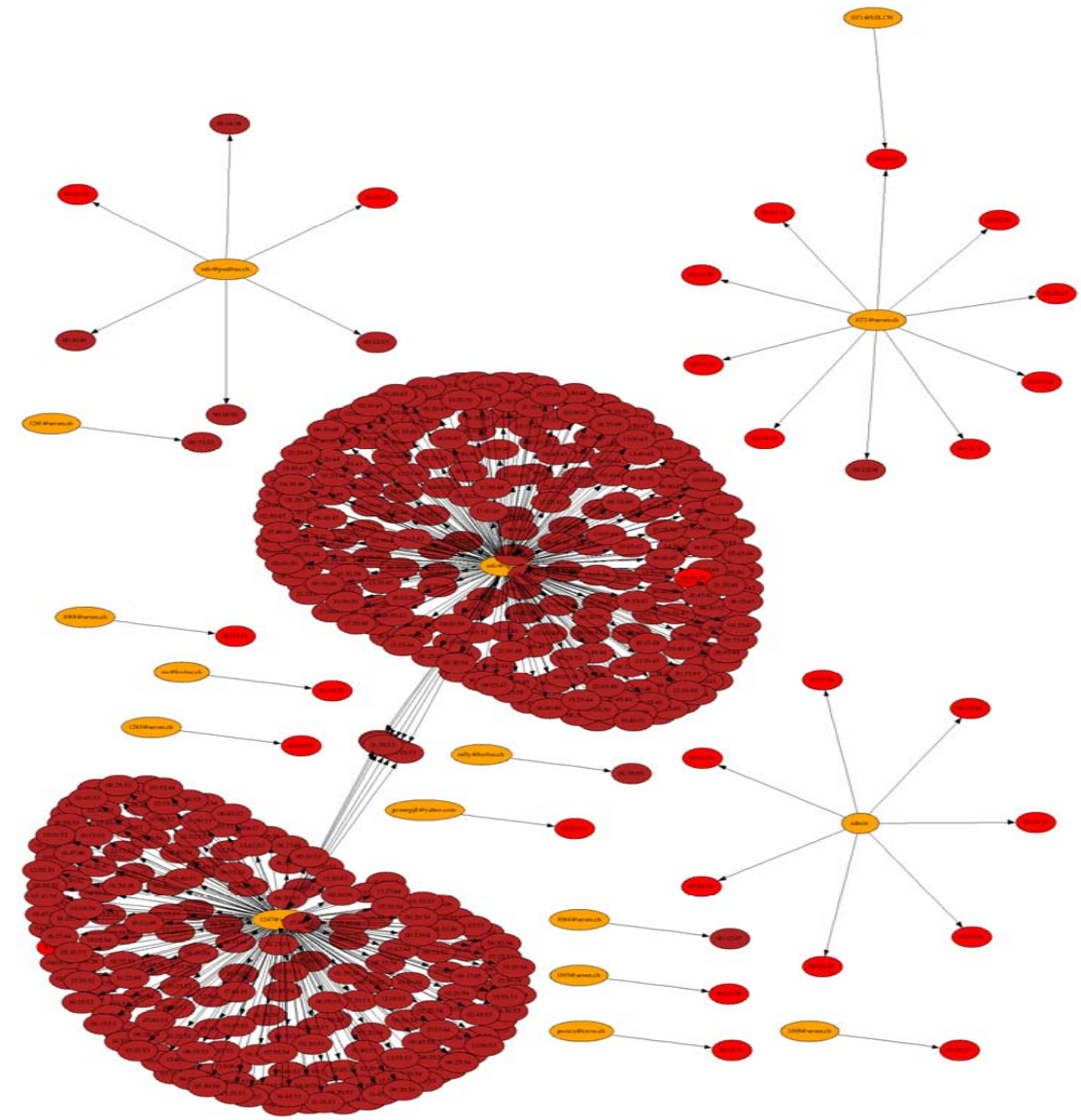
BIG Emails



Size > 100.000
Omit Threshold = 2

Documents leaving the network?

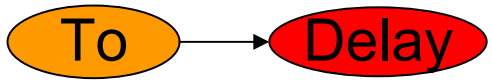
Email Server Problems?



2:00 < Delay < 10:00

Delay > 10:00

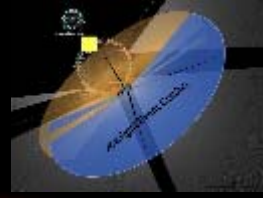
To



AfterGlow

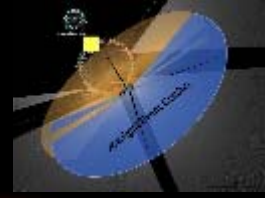
afterglow.sourceforge.net

AfterGlow



- http://afterglow.sourceforge.net
- Supported graphing tools:
  - GraphViz from AT&T (dot and neato)
    http://www.research.att.com/sw/tools/graphviz/
  - LGL (Large Graph Layout) by Alex Adai
    http://bioinformatics.icmb.utexas.edu/lgl/

AfterGlow – Command Line Parameters



- Some command line parameters:

  -h : help

  -t : two node mode

  -d : print count on nodes

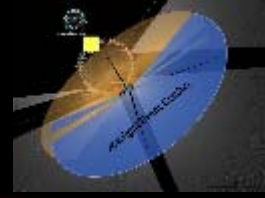
  -e : edge length

  -n : no node labels

  -o threshold : omit threshold (fan-out for nodes to be displayed)

  -c configfile : color configuration file

AfterGlow – color.properties



```
color.[source|event|target|edge]=
    <perl expression returning a color name>
```

- Array `@fields` contains input-line, split into tokens:

```
color.event="red" if ($fields[1] =~ /^192\..*)
```

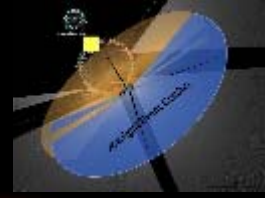
- Special color "`invisible`":

```
color.target="invisible" if ($fields[0] eq
    "IIS Action")
```

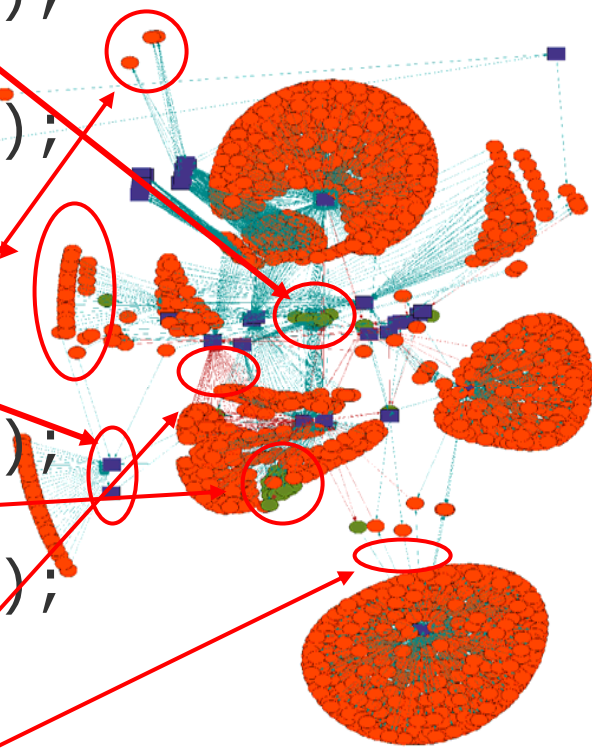
- Edge color

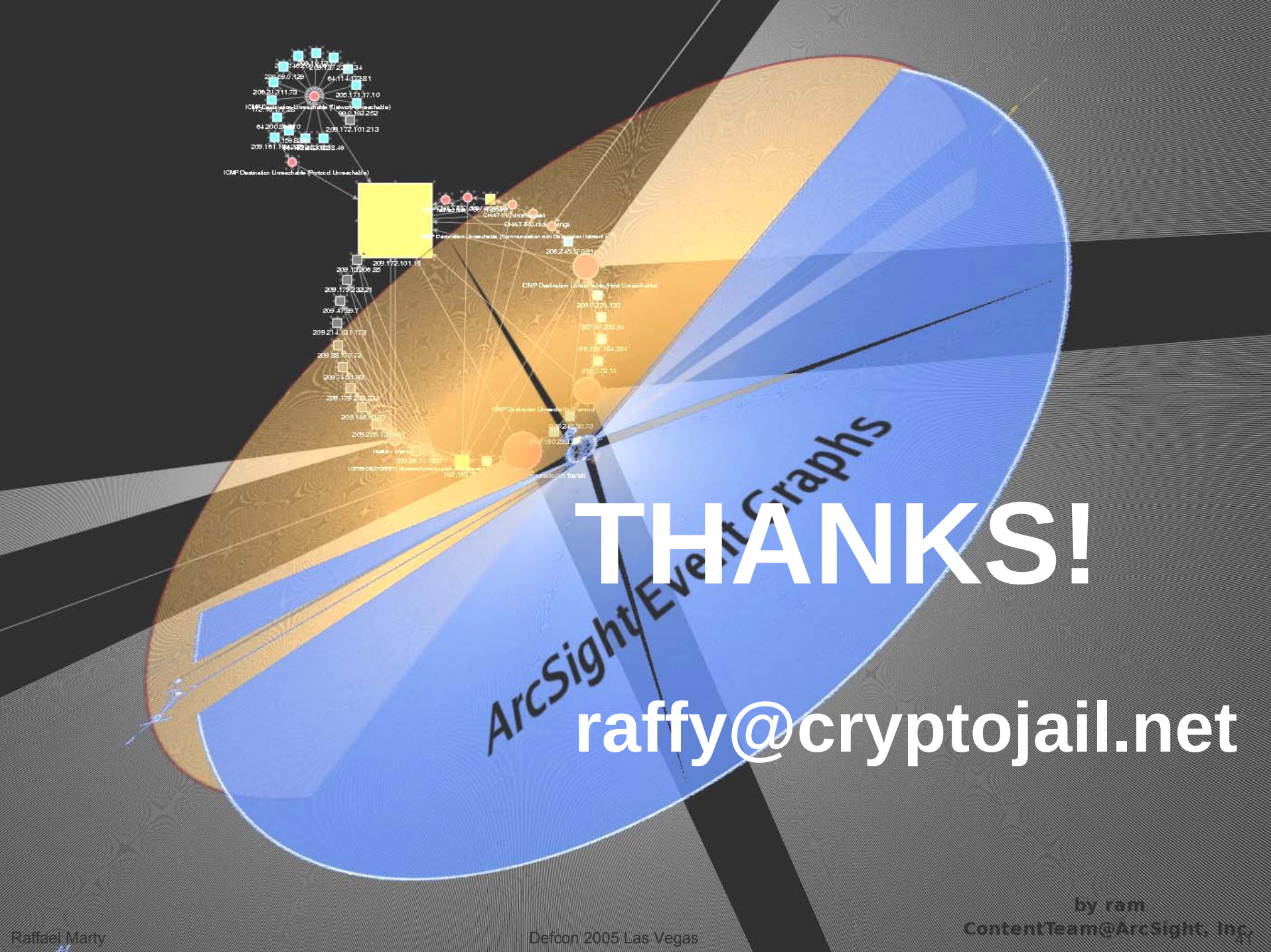
```
color.edge="blue"
```

AfterGlow – color.properties - Example



```
color.source="olivedrab"
  if ($fields[0]=~/191\.141\.69\.4/);
color.source="olivedrab"
  if ($fields[0]=~/211\.254\.110\./);
color.source="orangered1"
color.event="slateblue4"
color.target="olivedrab"
  if ($fields[2]=~/191\.141\.69\.4/);
color.target="olivedrab"
  if ($fields[2]=~/211\.254\.110\./);
color.target="orangered1"
color.edge="firebrick"
  if (($fields[0]=~/191\.141\.69\.\.4/) or
  ($fields[2]=~/191\.141\.69\.4/))
color.edge="cyan4"
```





THANKS!

raffy@cryptojail.net

by ram
ContentTeam@ArcSight, Inc