DAVIX Visualization Workshop

Jan P. Monsch
jan.monsch@iplosion.com

About

- Jan P. Monsch
  - Currently
    - Senior Security Analyst 🇨🇭
    - Technical Reviewer @ Pearson Education 🇺🇸
    - DAVIX Project Initiator & Lead Engineer 🇨🇭
    - On program committee for the International Workshop on Visualization for Cyber Security
  - Just finished post-grad school. Hurray!
    - M.Sc. in Security and Forensic Computing @ Dublin City University 🇮🇪

Workshop Preparation

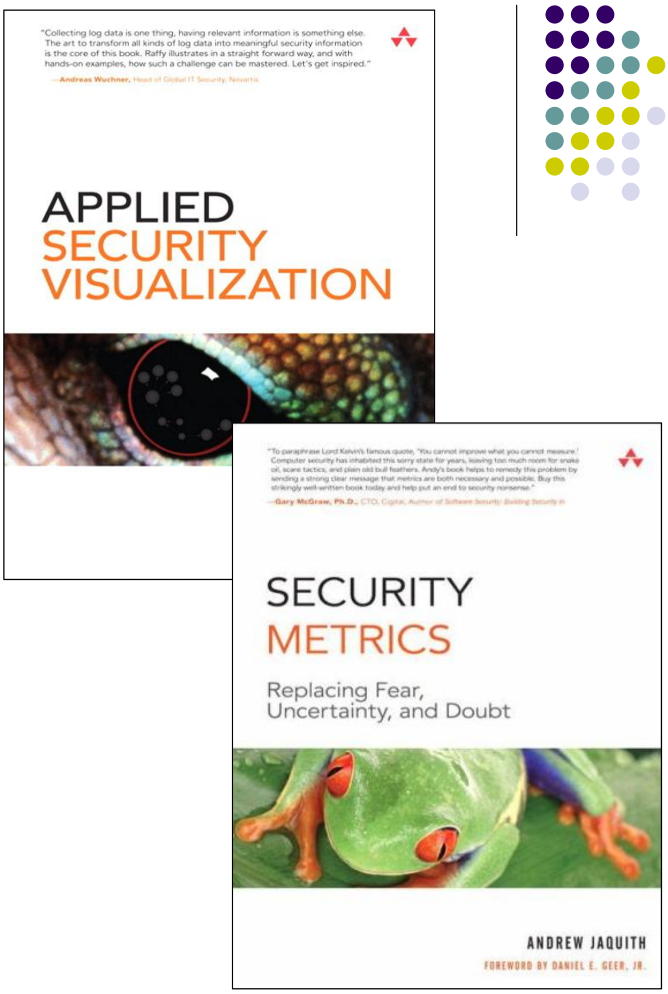
- Recommended setup
  - VMware Player 6.5 or VMware Fusion
- Get DAVIX VMware image
  - Requires 4 GB of disk and 1 GB of RAM
  - USB Stick, DVD
- On some media the image is zipped
  - Directly unzip from the DVD
- Boot, login (root:toor), run X (xconf; startx)

Agenda

- Security Visualization
- Introduction DAVIX
- Walk-Through DAVIX
- Hands-on Lab
- Visualization Contest

Prizes

- 1st prize
  - 1x Applied Security Visualization Book
  - 1x Security Metrics Book
- 2nd prize
  - 1x Applied Security Visualization Book


APPLIED SECURITY VISUALIZATION
SECURITY METRICS
Replacing Fear, Uncertainty, and Doubt
ANDREW JAQUITH
FOREWORD BY DANIEL E. GEER, JR.

Contest Task

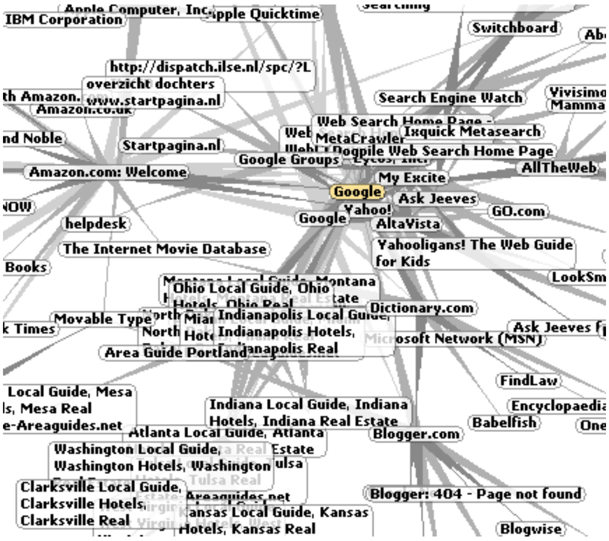
- Analyze the attack(s) in the
  - Jubrowska capture and
  - spty database
- Use any visualization technique you like to document the a particular the attacks
  - Not limited to DAVIX
- Document the case (Text, images, video, …)
  - Tell a story in your submission
  - Make it an interesting read / view

Agenda

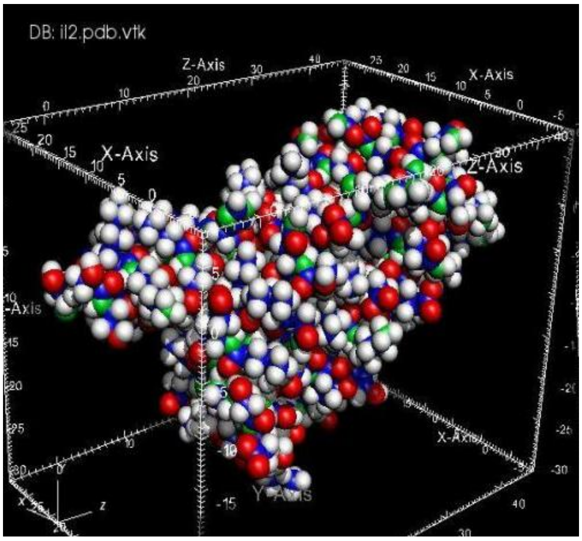
- Security Visualization
- Introduction DAVIX
- Walk-Through DAVIX
- Hands-on Lab
- Visualization Contest

Information vs. Scientific Visualization [1]

- Information visualization
  - visualize large collections of abstract data



- Scientific visualization
  - representation of data with geometric structure

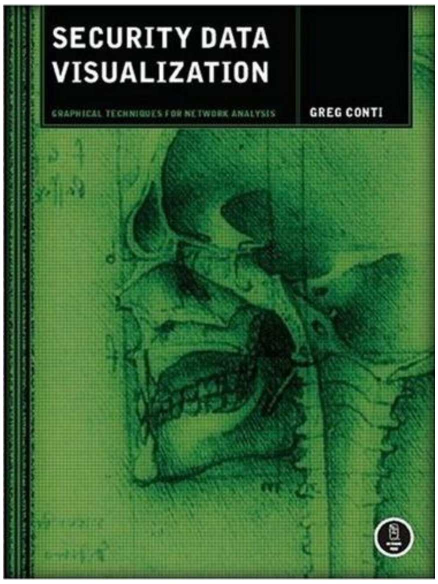


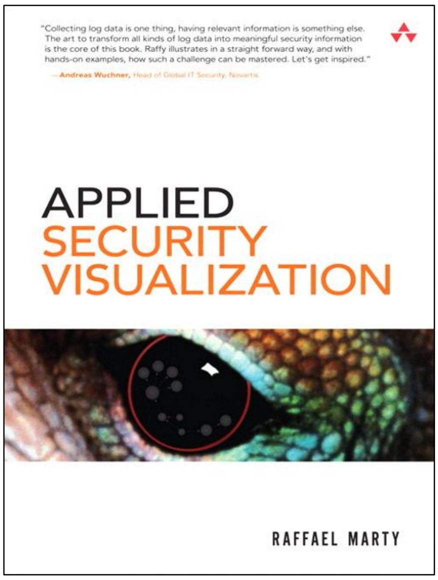
Visualization

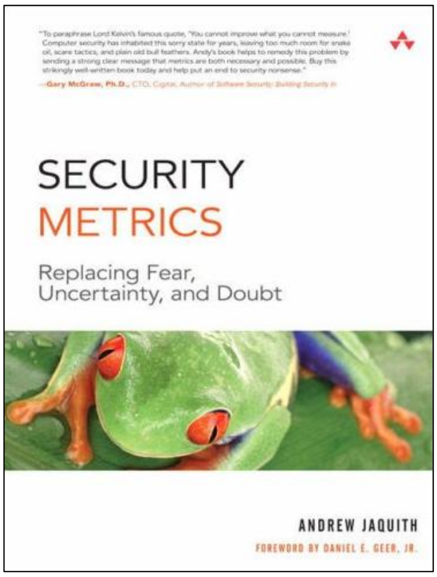
- Ben Shneiderman
  - “The purpose of viz is insight, not pictures.” [2]

Security Visualization Resources

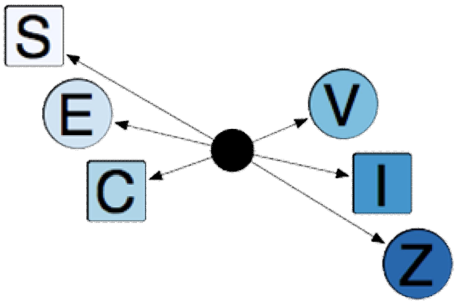
- Security visualization is quite a new field [3, 4, 5]
- Applied part of information visualization

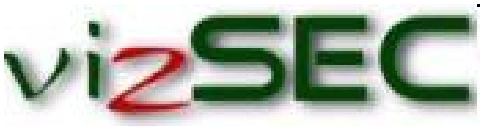

SECURITY DATA VISUALIZATION
GRAPHICAL TECHNIQUES FOR NETWORK ANALYSIS
GREG CONTI




SECURITY METRICS
Replacing Fear, Uncertainty, and Doubt
ANDREW JAQUITH
FOREWORD BY DANIEL E. GEER, JR.

Security Visualization Community



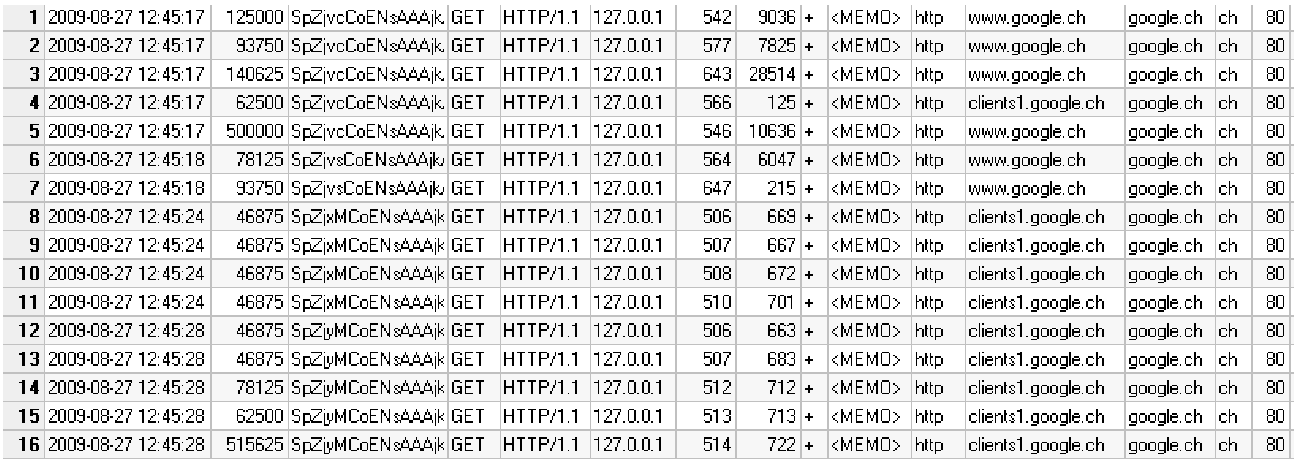


www.secviz.org

www.vizsec.org

Visualization

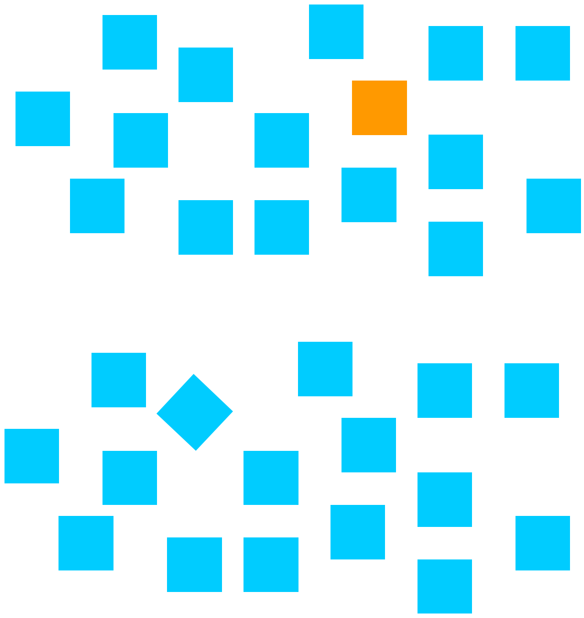
- Analyzing floods of data in tabular or textual form is tedious
- Humans must sequentially scan such data [6,7]



1	2009-08-27 12:45:17	125000	SpZjvcCoENsAAAjk	GET	HTTP/1.1	127.0.0.1	542	9036	+	<MEMO>	http	www.google.ch	google.ch	ch	80
2	2009-08-27 12:45:17	93750	SpZjvcCoENsAAAjk	GET	HTTP/1.1	127.0.0.1	577	7825	+	<MEMO>	http	www.google.ch	google.ch	ch	80
3	2009-08-27 12:45:17	140625	SpZjvcCoENsAAAjk	GET	HTTP/1.1	127.0.0.1	643	28514	+	<MEMO>	http	www.google.ch	google.ch	ch	80
4	2009-08-27 12:45:17	62500	SpZjvcCoENsAAAjk	GET	HTTP/1.1	127.0.0.1	566	125	+	<MEMO>	http	clients1.google.ch	google.ch	ch	80
5	2009-08-27 12:45:17	500000	SpZjvcCoENsAAAjk	GET	HTTP/1.1	127.0.0.1	546	10636	+	<MEMO>	http	www.google.ch	google.ch	ch	80
6	2009-08-27 12:45:18	78125	SpZjvsCoENsAAAjk	GET	HTTP/1.1	127.0.0.1	564	6047	+	<MEMO>	http	www.google.ch	google.ch	ch	80
7	2009-08-27 12:45:18	93750	SpZjvsCoENsAAAjk	GET	HTTP/1.1	127.0.0.1	647	215	+	<MEMO>	http	www.google.ch	google.ch	ch	80
8	2009-08-27 12:45:24	46875	SpZjxMCoENsAAAjk	GET	HTTP/1.1	127.0.0.1	506	669	+	<MEMO>	http	clients1.google.ch	google.ch	ch	80
9	2009-08-27 12:45:24	46875	SpZjxMCoENsAAAjk	GET	HTTP/1.1	127.0.0.1	507	667	+	<MEMO>	http	clients1.google.ch	google.ch	ch	80
10	2009-08-27 12:45:24	46875	SpZjxMCoENsAAAjk	GET	HTTP/1.1	127.0.0.1	508	672	+	<MEMO>	http	clients1.google.ch	google.ch	ch	80
11	2009-08-27 12:45:24	46875	SpZjxMCoENsAAAjk	GET	HTTP/1.1	127.0.0.1	510	701	+	<MEMO>	http	clients1.google.ch	google.ch	ch	80
12	2009-08-27 12:45:28	46875	SpZjyMCoENsAAAjk	GET	HTTP/1.1	127.0.0.1	506	663	+	<MEMO>	http	clients1.google.ch	google.ch	ch	80
13	2009-08-27 12:45:28	46875	SpZjyMCoENsAAAjk	GET	HTTP/1.1	127.0.0.1	507	683	+	<MEMO>	http	clients1.google.ch	google.ch	ch	80
14	2009-08-27 12:45:28	78125	SpZjyMCoENsAAAjk	GET	HTTP/1.1	127.0.0.1	512	712	+	<MEMO>	http	clients1.google.ch	google.ch	ch	80
15	2009-08-27 12:45:28	62500	SpZjyMCoENsAAAjk	GET	HTTP/1.1	127.0.0.1	513	713	+	<MEMO>	http	clients1.google.ch	google.ch	ch	80
16	2009-08-27 12:45:28	515625	SpZjyMCoENsAAAjk	GET	HTTP/1.1	127.0.0.1	514	722	+	<MEMO>	http	clients1.google.ch	google.ch	ch	80

Visualization [6,7]

- Visualization exploits the human's visual perceptive capabilities and parallel processing
  - Size
  - Shape
  - Distance
  - Color
- Easy to spot
  - patterns
  - irregularities

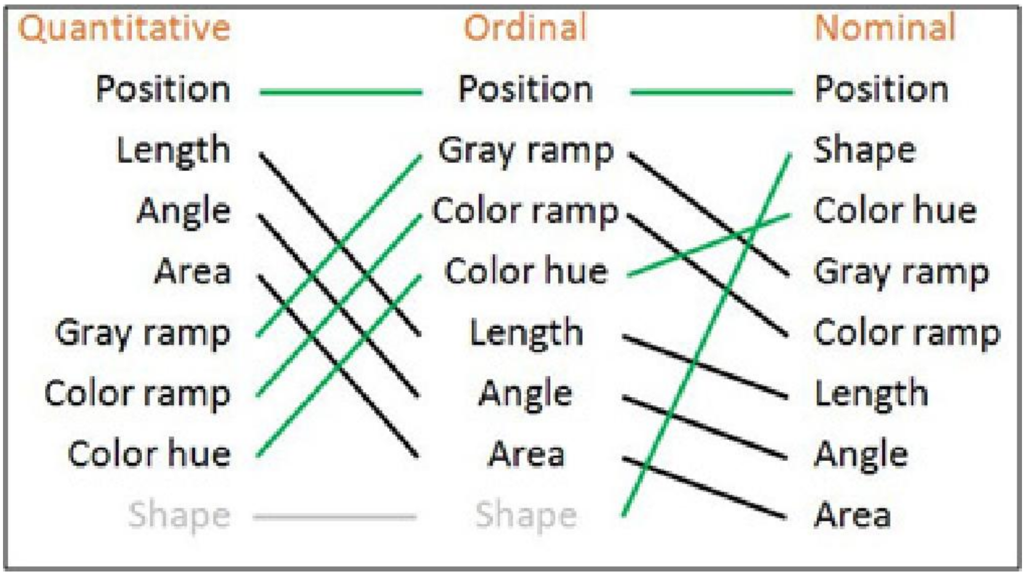


Data Types [7]

- Data types
  - Ordinal
    - Has a sequence
    - e.g. day of week
  - Nominal
    - Has no sequence
    - e.g. types of fishes
  - Quantitative
    - Can be measured
    - e.g. length, time, weight, temperature, speed, …

Visualization Effectiveness [7]

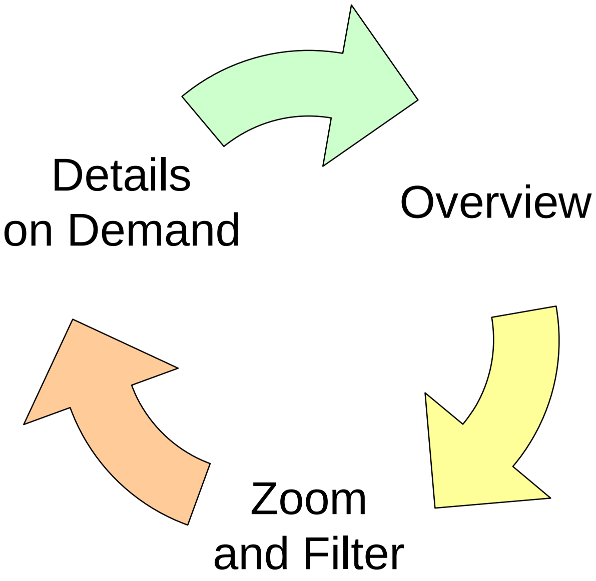
- Each data type has its most effective way of visualization



Quantitative	Ordinal	Nominal
Position	Position	Position
Length	Gray ramp	Shape
Angle	Color ramp	Color hue
Area	Color hue	Gray ramp
Gray ramp	Length	Color ramp
Color ramp	Angle	Length
Color hue	Area	Angle
Shape	Shape	Area

Information Seeking Mantra [8]

- Ben Shneiderman's information seeking mantra
  - *"Overview, Zoom and Filter – Details on Demand.*
  - *Overview, Zoom and Filter – Details on Demand.*
  - *Overview, Zoom and Filter – Details on Demand..."*

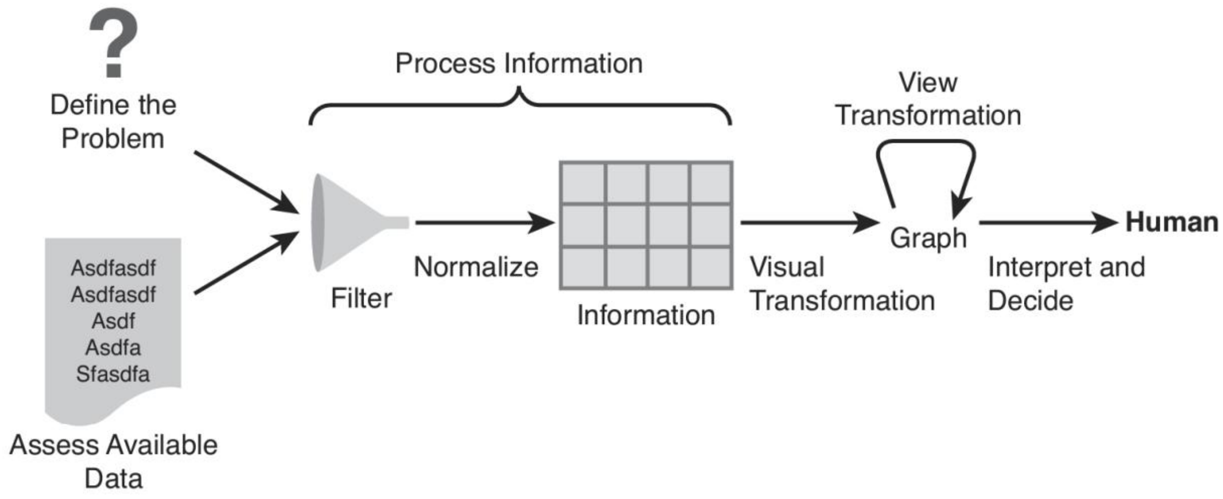


Details on Demand

Overview

Zoom and Filter

Information Visualization Process [4]



Agenda

- Security Visualization
- Introduction DAVIX
- Walk-Through DAVIX
- Hands-on Lab
- Visualization Contest

Initial Situation

- Many free visualization tools
  - But installation is often cumbersome
    - Compiler version and library issues
    - Code difficult to build or broken
    - Diverse runtime environments:
      Java, Perl, Ruby, Python, Windows Applications
- Huge hurdle for people to get start with security visualization

Mission Statement

- DAVIX shall
  - provide the audience with a workable and integrated tools set,
  - enable them to immediately start with security visualization and
  - motivate them to contribute to the security visualization community.

Inside the DAVIX Live CD

- Live Linux CD system based on SLAX 6 [3]
  - Software packages are modularized
  - Easy customizable
  - Runs from CD/DVD, USB stick or hard drive
- Collection of free tools for processing & visualization
  - Tools work out of the box
  - No compilation or installation of tools required
- Comes with documentation [9]
  - Quick start description for the most important tools
  - Links to manuals and tutorials

DAVIX 1.0.1 Tools

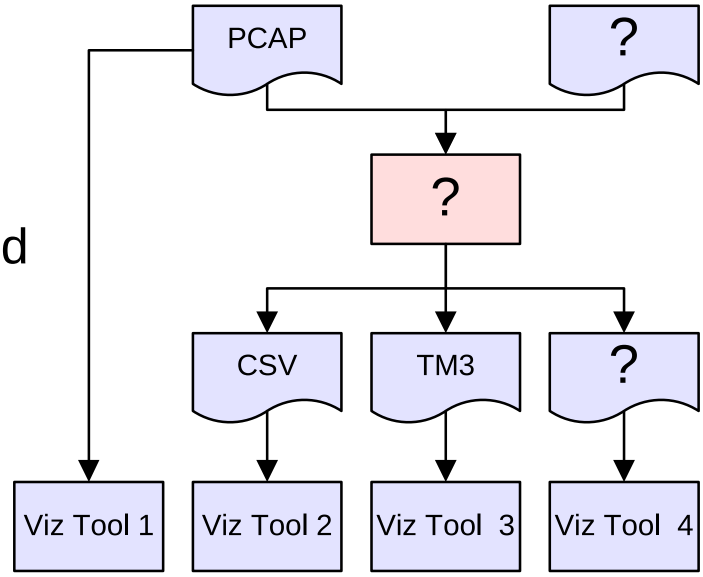
- Capture
  - Network Tools
    - Argus
    - Snort
    - Wireshark
  - Logging
    - syslog-ng
  - Fetching Data
    - wget
    - ftp
    - scp

- Processing
  - Shell Tools
    - awk, grep, sed
  - Visualization Preprocessing
    - AfterGlow
    - LGL
  - Extraction
    - Chaosreader
  - Data Enrichment
    - geoiplookup
    - whois, gwhois

- Visualization
  - Network Traffic
    - EtherApe
    - InetVis
    - tnv
  - Generic
    - AfterGlow
    - Cytoscape
    - Graphviz
    - LGL Viewer
    - Mondrian
    - R Project
    - Treemap

Interface Issue

- Each visualization tool has its own file format interfaces
- Data must be converted to match the import interfaces
- These adapters are mostly self-written snippets of code

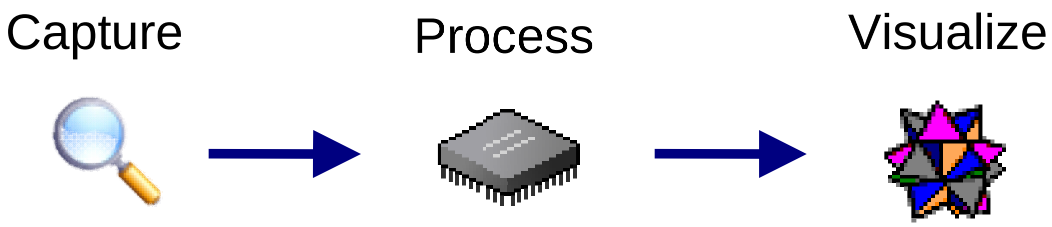


Agenda

- Security Visualization
- Introduction DAVIX
- Walk-Through DAVIX
- Hands-on Lab
- Visualization Contest

User Interface

- Menu organized around Info Viz Process



Capture

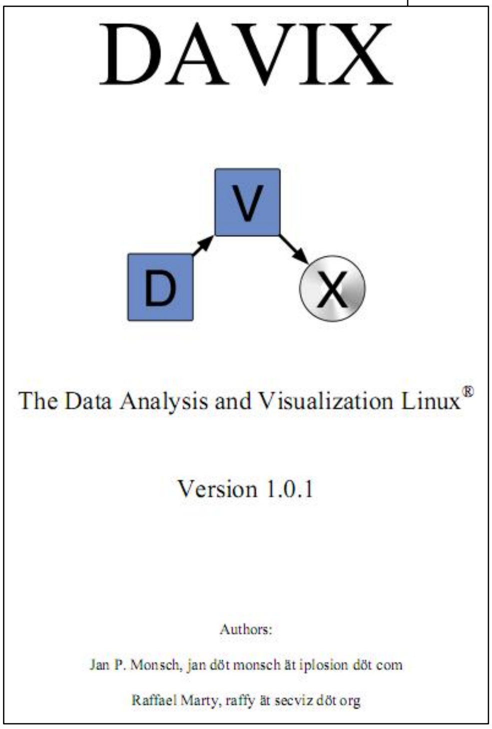
Process

Visualize

- Tools often cover more than one category
  - Afterglow à Process, Visualize
- Additional tools/services
  - Apache, MySQL, NTP

PDF User Manual [9]

- Content
  - Quick start guide
  - Network setup information
  - Tool usage examples
  - Links to online resource
  - Customizing DAVIX



DAVIX

The Data Analysis and Visualization Linux®

Version 1.0.1

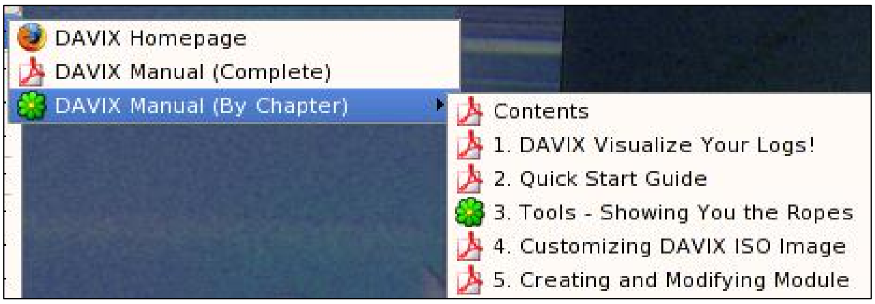
Authors:

Jan P. Monsch, jan döt monsch ät iplosion döt com

Raffael Marty, raffy ät secviz döt org

User Manual in the Menu

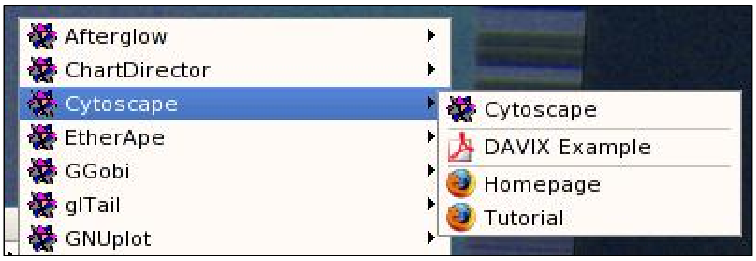
- The manual is browsable by chapter …



DAVIX Homepage
DAVIX Manual (Complete)
DAVIX Manual (By Chapter)

Contents
1. DAVIX Visualize Your Logs!
2. Quick Start Guide
3. Tools - Showing You the Ropes
4. Customizing DAVIX ISO Image
5. Creating and Modifying Module

- … or individual tool chapters



Afterglow
ChartDirector
Cytoscape
EtherApe
GGobi
glTail
GNUplot

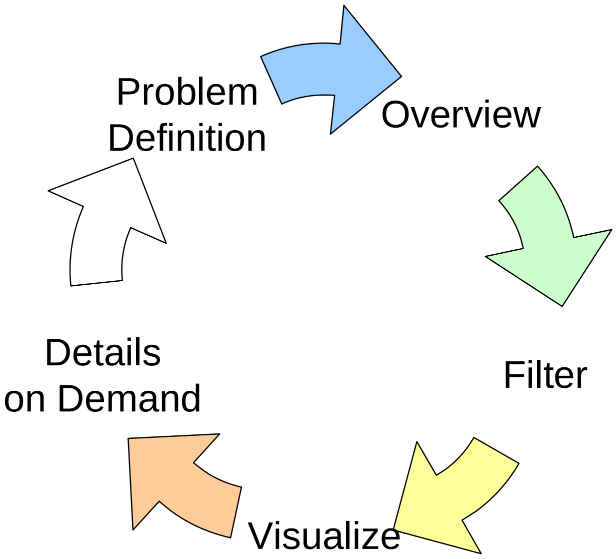
Cytoscape
DAVIX Example
Homepage
Tutorial

Agenda

- Security Visualization
- Introduction DAVIX
- Walk-Through DAVIX
- Hands-on Lab
- Visualization Contest

Overview

- Lab built around Info Viz Process
- DAVIX Tools
  - Processing
    - Wireshark / tshark [10]
    - awk [11], sed, uniq
    - p0f [12], Snort [13]
  - Visualization
    - AfterGlow [14]
    - Graphviz [15]
    - Treemap [16]
    - Cytoscape [17]
    - R Project [18]
    - GGobi [19]



Problem Definition

- Type of Traffic?
- Network Topology?
  - Gateway?
  - Team Server?
  - Other Team Systems?
- Activities?
  - Communication Pattern?
  - Attacks?

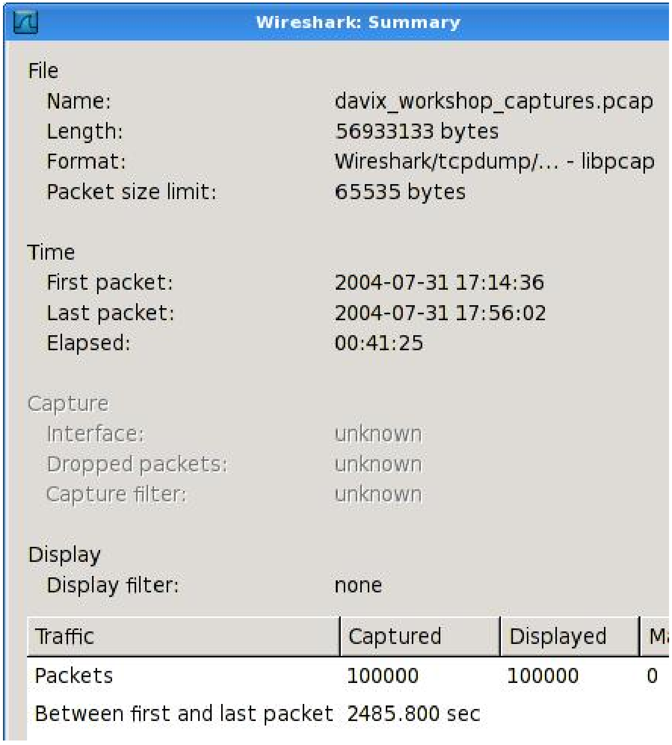
Type of Traffic

Overview: Background

- CTF DEFCON 12
  - PCAP File
- 6 teams
  - 1 server per team with vulnerable services
  - Many team member systems
- Symmetrical setup for all teams.

Overview - Wireshark

- Basic statistics
  - 54 MB PCAP file
  - Date 31.07.2004
  - 41 min of traffic
  - 100’000 packets



Wireshark: Summary

File

Name:	davix_workshop_captures.pcap
Length:	56933133 bytes
Format:	Wireshark/tcpdump/... - libpcap
Packet size limit:	65535 bytes

Time

First packet:	2004-07-31 17:14:36
Last packet:	2004-07-31 17:56:02
Elapsed:	00:41:25

Capture

Interface:	unknown
Dropped packets:	unknown
Capture filter:	unknown

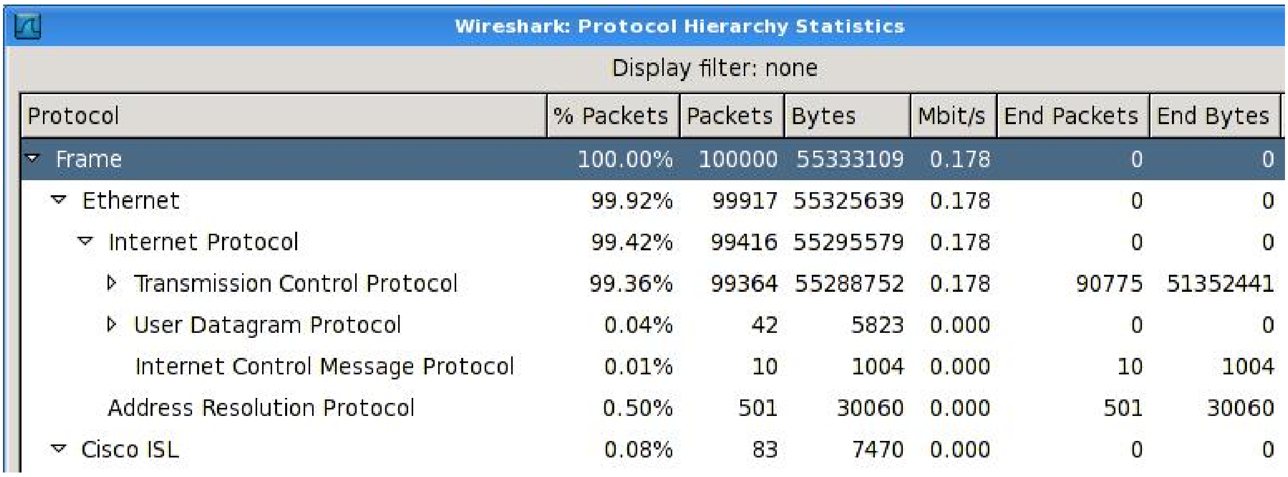
Display

Display filter:	none

Traffic	Captured	Displayed	M
Packets	100000	100000	0
Between first and last packet	2485.800 sec		

Overview: Wireshark

- Packets Protocols
  - Mostly IP
    - Mostly TCP
    - Some UDP
- Traffic Volume
  - Mostly TCP



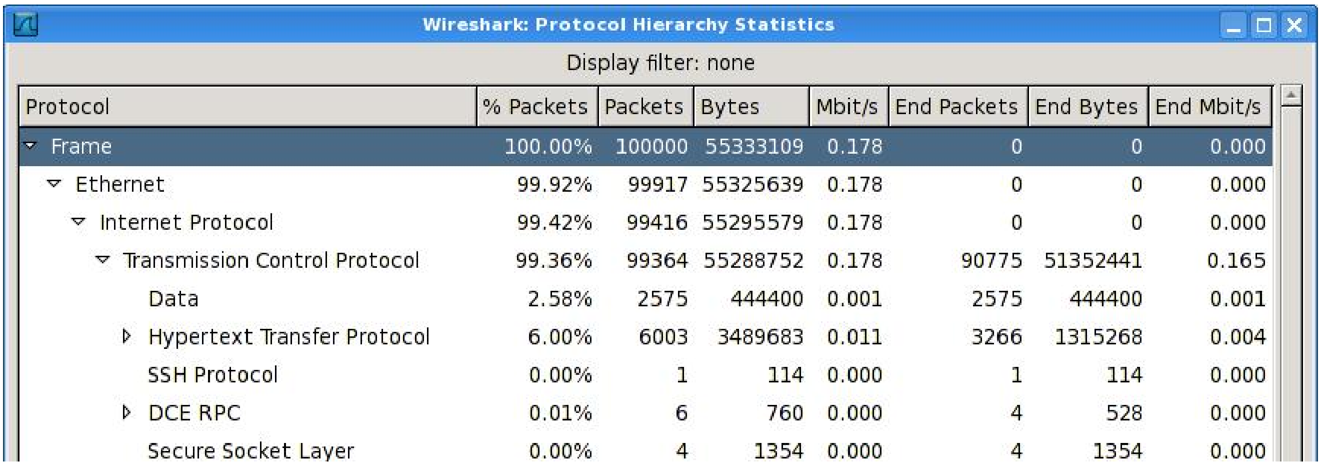
Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes
Frame	100.00%	100000	55333109	0.178	0	0
Ethernet	99.92%	99917	55325639	0.178	0	0
Internet Protocol	99.42%	99416	55295579	0.178	0	0
Transmission Control Protocol	99.36%	99364	55288752	0.178	90775	51352441
User Datagram Protocol	0.04%	42	5823	0.000	0	0
Internet Control Message Protocol	0.01%	10	1004	0.000	10	1004
Address Resolution Protocol	0.50%	501	30060	0.000	501	30060
Cisco ISL	0.08%	83	7470	0.000	0	0

Overview: Wireshark

- TCP
  - Mostly HTTP
  - Some DCE RPC à Windows



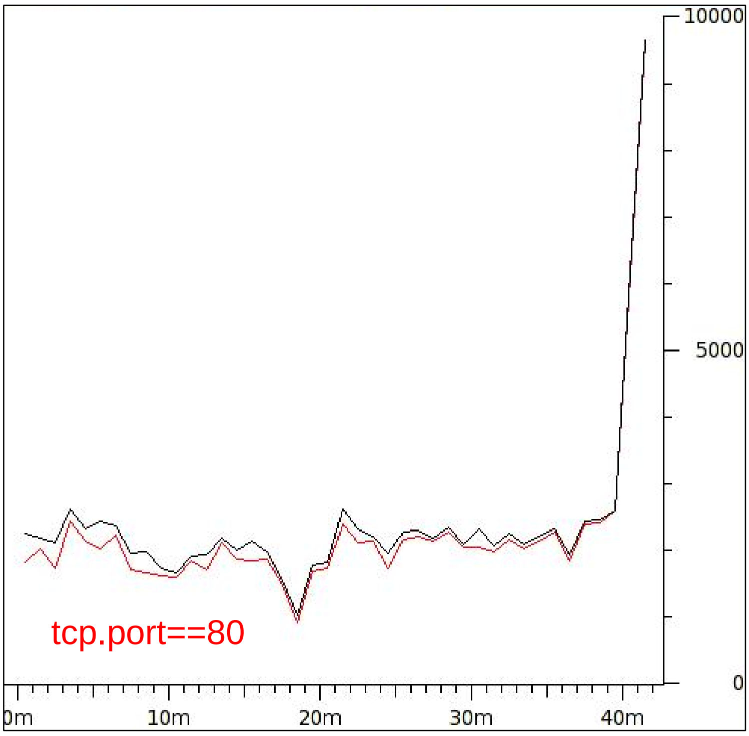
Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00%	100000	55333109	0.178	0	0	0.000
Ethernet	99.92%	99917	55325639	0.178	0	0	0.000
Internet Protocol	99.42%	99416	55295579	0.178	0	0	0.000
Transmission Control Protocol	99.36%	99364	55288752	0.178	90775	51352441	0.165
Data	2.58%	2575	444400	0.001	2575	444400	0.001
Hypertext Transfer Protocol	6.00%	6003	3489683	0.011	3266	1315268	0.004
SSH Protocol	0.00%	1	114	0.000	1	114	0.000
DCE RPC	0.01%	6	760	0.000	4	528	0.000
Secure Socket Layer	0.00%	4	1354	0.000	4	1354	0.000

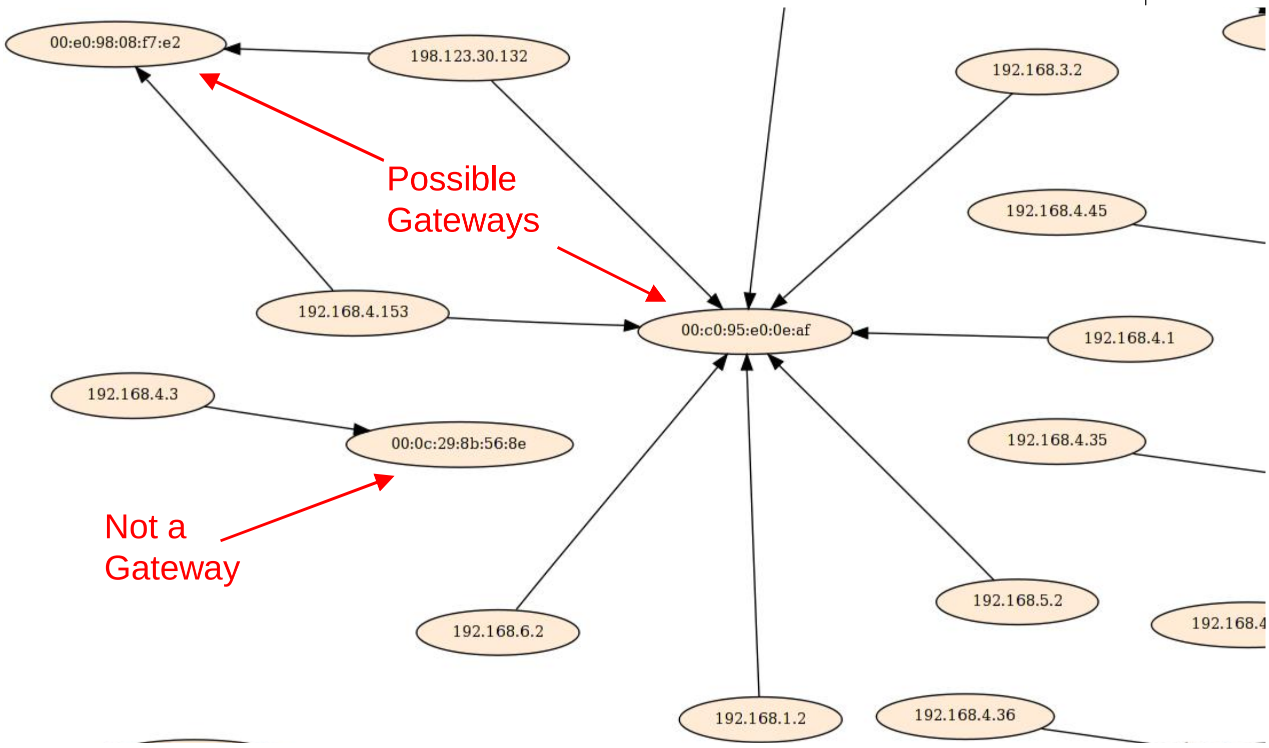
Overview: Wireshark

- Traffic Shape
  - Constant at begin
  - Massive increase towards the end.



Network Topology

Visualize: AfterGlow / Graphviz



Possible Gateways

Not a Gateway

001_network_topology_gateway.sh

Zoom & Filter: tshark

- CSV of source/destination IP to source/destination MAC addresses

  -
    ```
    0.0.0.0,00:00:86:5b:e9:6a
    0.0.0.0,00:04:5a:a2:d4:08
    192.168.1.2,00:c0:95:e0:0e:af
    192.168.3.2,00:c0:95:e0:0e:af
    192.168.4.1,00:c0:95:e0:0e:af
    192.168.4.152,00:09:6b:53:8a:81
    192.168.4.153,00:c0:95:e0:0e:af
    ...
    ```

001_network_topology_gateway.sh

Zoom & Filter: tshark

- Extract IP addresses and their MAC addresses

  -
    ```
    tshark -r davix_workshop_captures.pcap
    -e ip.src -e eth.src –T fields
    -E separator=, -R ip > d_ip_mac.csv
    ```

  -
    ```
    tshark -r davix_workshop_captures.pcap
    -e ip.dst -e eth.dst –T fields
    -E separator=, -R ip >> d_ip_mac.csv
    ```

  -
    ```
    cat d_ip_mac.csv | sort | uniq >
    d_ip_mac_distinct.csv
    ```

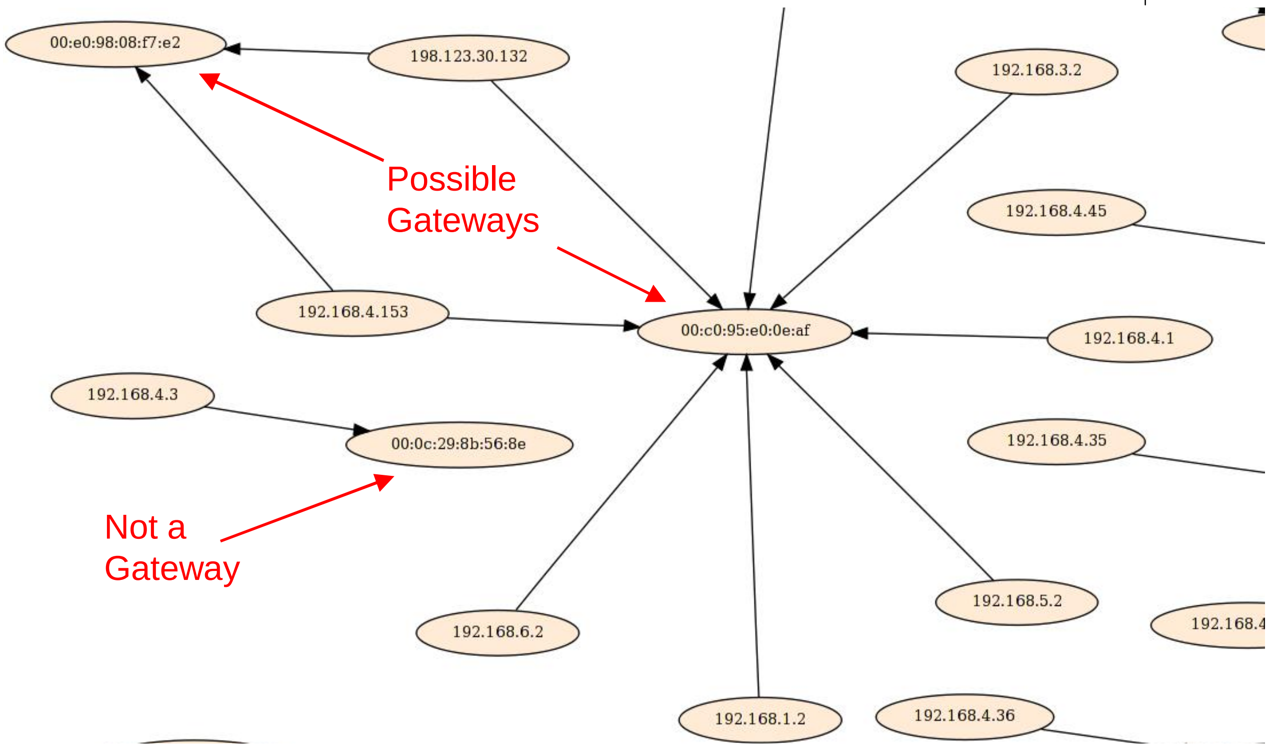
001_network_topology_gateway.sh

Visualize: AfterGlow / Graphviz

- Visualize CSV file using AfterGlow
  - `cat d_ip_mac_distinct.csv | afterglow.pl –t > v_ip_mac.dot`
  - `neato –T png -o v_ip_mac.png v_ip_mac.dot`
- View resulting image
  - `gqview`

001_network_topology_gateway.sh

Visualize: AfterGlow / Graphviz



Possible Gateways

Not a Gateway

002_network_topology_operating_system.sh

Overview: p0f

Other teams come through NAT

- Results

```
192.168.4.1,FreeBSD 4.7-5.2
             (or MacOS X 10.2-10.4)
192.168.4.1,FreeBSD 4.8-5.1
             (or MacOS X 10.2-10.3)
192.168.4.1,Linux 2.4-2.6
192.168.4.1,OpenBSD 3.0-3.9
192.168.4.1,Windows 2000 SP4, XP SP1+
192.168.4.1,Windows XP SP1+, 2000 SP3
192.168.4.152,Linux 2.4-2.6
192.168.4.153,Linux 2.4-2.6
192.168.4.154,Linux 2.4-2.6
192.168.4.157,Linux 2.4-2.6
192.168.4.159,Linux 2.4-2.6
192.168.4.160,Linux 2.4-2.6
192.168.4.45,Linux 2.4-2.6
```

002_network_topology_operating_system.sh

Overview: p0f

- Identify Involved Operating Systems

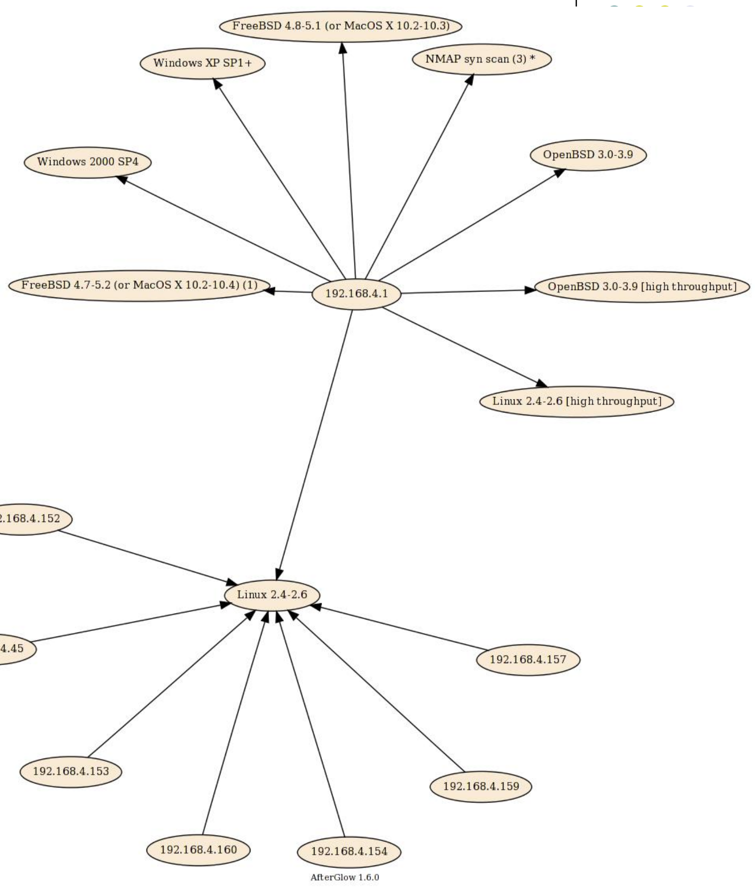
```
p0f -f /etc/p0f/p0f.fp -s
davix_workshop_captures.pcap -N |
sed "s/ (up.*$//" |
sed "s/:[0-9]* - /,/" |
sort | uniq > d_ip_ostype.csv
```

```
cat d_ip_ostype.csv
```

- However, be aware that not ever host's OS can be detected.

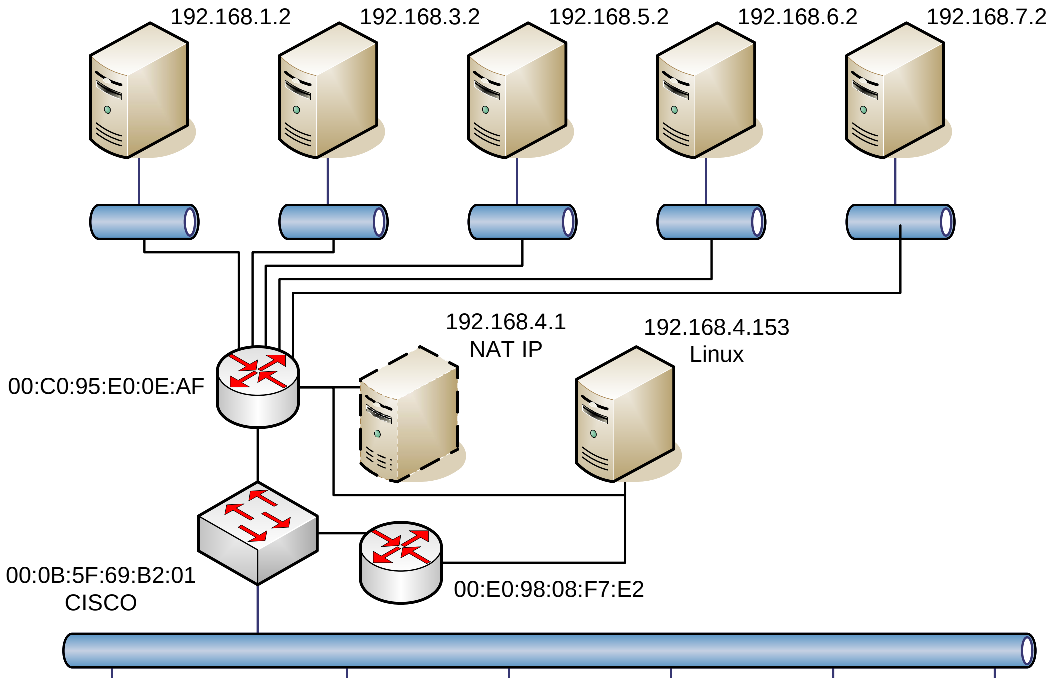
Exercise

- Visualize the OS detection results with Afterglow and neato



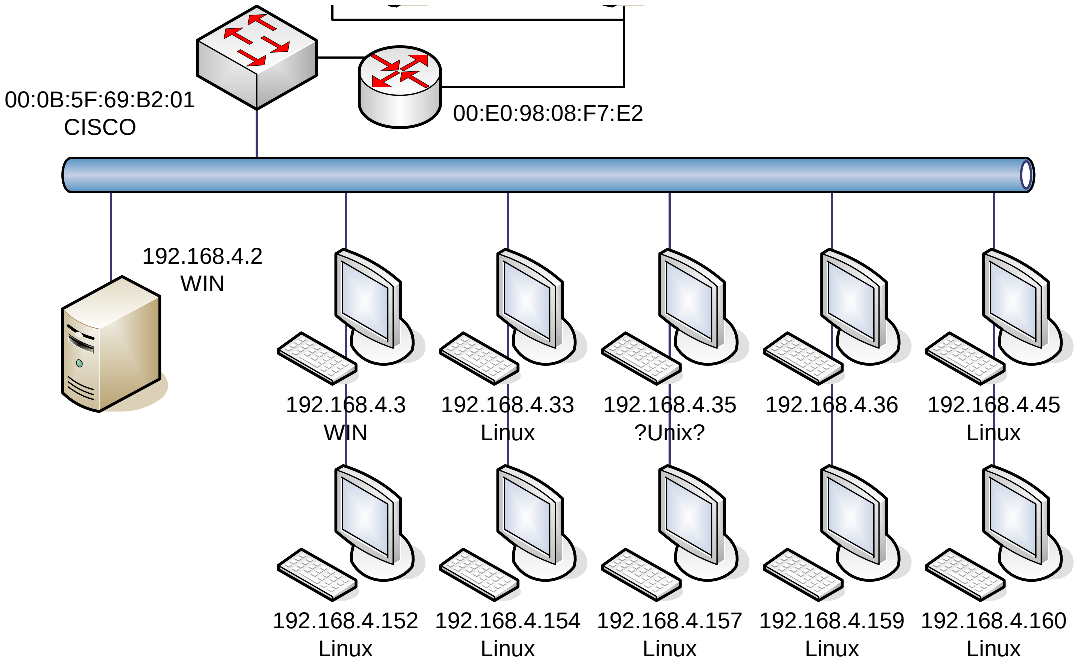
Visualize: Visio ;-)

- Topology Opponents



Visualize: Visio ;-)

- Our Team



Activities

Linked Graphs

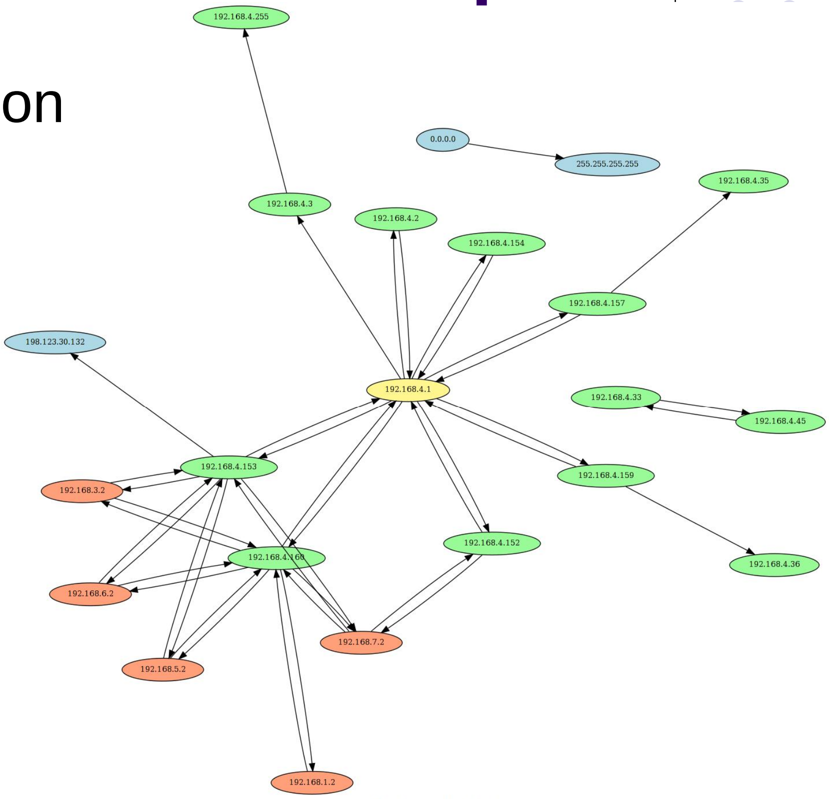
Afterglow / Graphviz

003_activity_connections.sh

Visualize: AfterGlow / Graphviz

- IP communication between hosts.

- Legend
  - 🟩 Our team
  - 🟧 Other teams
  - 🟨 NAT IP
  - 🟦 Neutral



AfterGlow 1.6.0 - Property File: color.properties

003_activity_connections.sh

Zoom & Filter - tshark

- Extract source & destination IP addresses

  -
    ```
    tshark -r davix_workshop_captures.pcap
    -e ip.src -e ip.dst -Tfields -E separator=,
    -R ip > d_ipsrc_ipdst.csv
    ```

- Remove duplicate lines

  -
    ```
    cat d_ipsrc_ipdst.csv | sort -u >
    d_ipsrc_ipdst_distinct.csv
    ```

003_activity_connections.sh

Visualize: AfterGlow / Graphviz

- Visualize CSV file using AfterGlow
  - `cat d_ipsrc_ipdst.csv | afterglow.pl -c color1.properties -t > v_ipsrc_ipdst.dot`
  - `neato –T png -o v_ipsrc_ipdst.png v_ipsrc_ipdst.dot`
- View resulting image
  - `gqview`

003_activity_connections.sh

Visualize: AfterGlow / Graphviz

- AfterGlow p_ipsrc_ipdst.properties

```
color.source="khaki1" if ($fields[0]=~/^192\.168\.4\.1$/);
color.source="palegreen" if ($fields[0]=~/^192\.168\.4\..*/);
color.source="lightblue" if ($fields[0]=~/^0\.0\.0\.0$/);
color.source="lightblue" if ($fields[0]=~/^255\.255\.255\.255$/);
color.source="lightblue" if ($fields[0]=~/^198\.123\.30\.132$/);
color.source="lightsalmon"
```

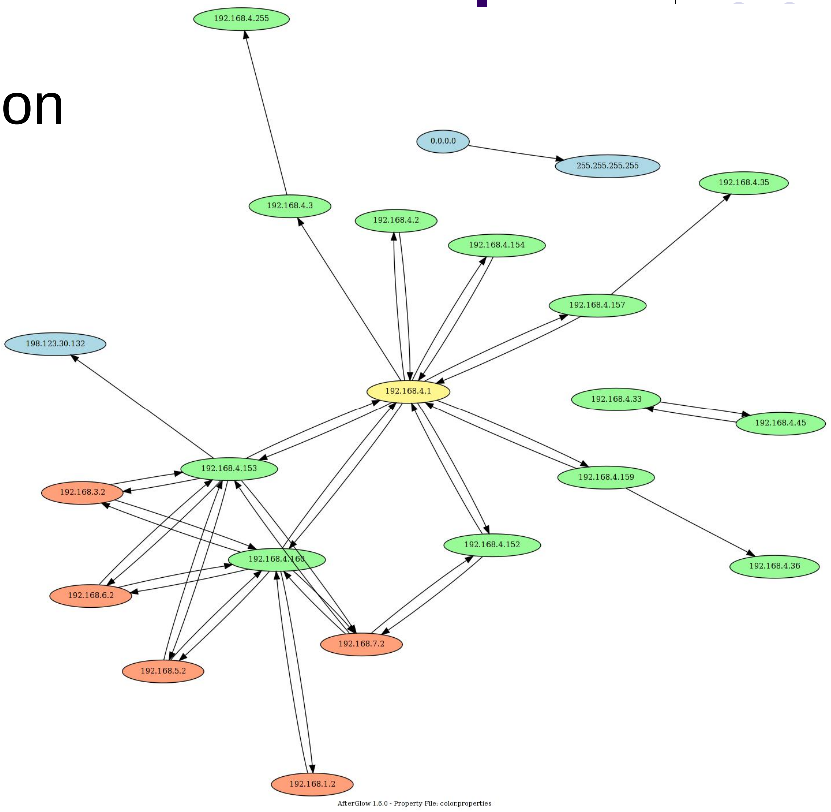
```
color.target="khaki1" if ($fields[1]=~/^192\.168\.4\.1$/);
color.target="palegreen" if ($fields[1]=~/^192\.168\.4\..*/);
color.target="lightblue" if ($fields[1]=~/^0\.0\.0\.0$/);
color.target="lightblue" if ($fields[1]=~/^255\.255\.255\.255$/);
color.target="lightblue" if ($fields[1]=~/^198\.123\.30\.132$/);
color.target="lightsalmon"
```

003_activity_connections.sh

Visualize: AfterGlow / Graphviz

- IP communication between hosts.

- Legend
  - 🟩 Our team
  - 🟧 Other teams
  - 🟨 NAT IP
  - 🟦 Neutral

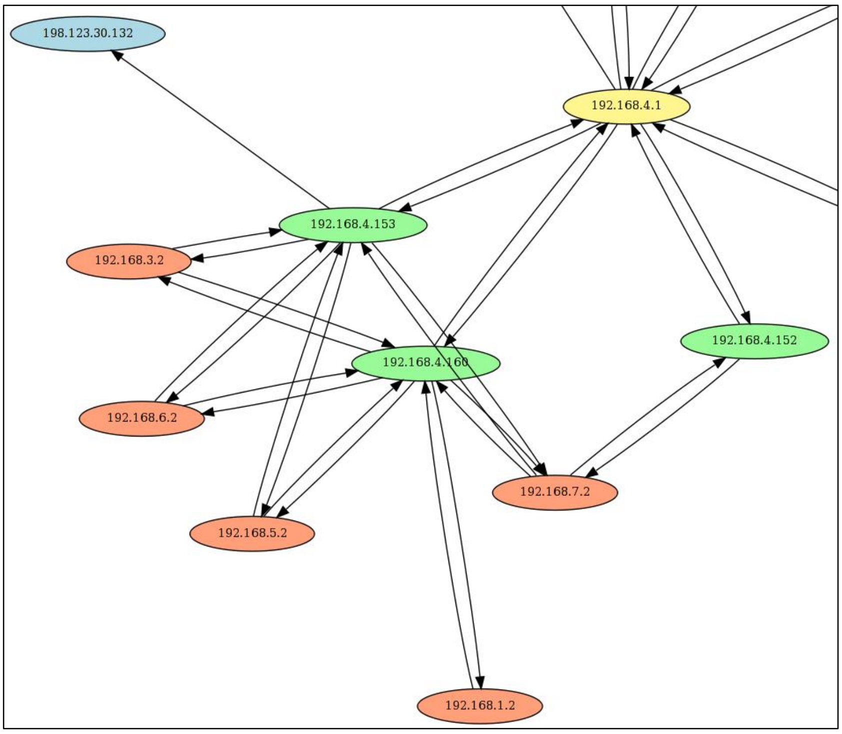


003_activity_connections.sh

Visualize: AfterGlow / Graphviz

- Zoom Image

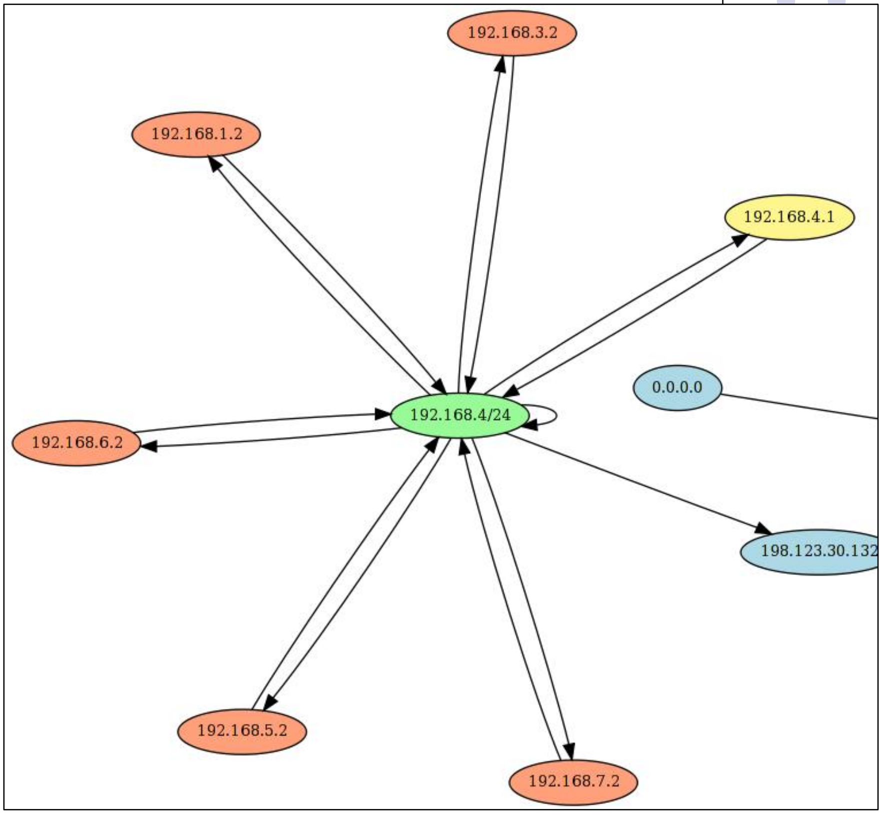
- 192.168.4.0/24 attacking other teams



004_activity_connections_cluster.sh

Visualize: AfterGlow / Graphviz

- Clustering nodes to unclutter the graph



004_activity_connections_cluster.sh

Visualize: AfterGlow / Graphviz

- AfterGlow p_ipsrc_ipdst_cluster.properties

Tweak pattern

```
color.source="khaki1" if ($fields[0]=~/^192\.168\.4\.1$/);
color.source="palegreen" if ($fields[0]=~/^192\.168\.4/);
color.source="lightblue" if ($fields[0]=~/^0\.0\.0\.0$/);
color.source="lightblue" if ($fields[0]=~/^255\.255\.255\.255$/);
color.source="lightblue" if ($fields[0]=~/^198\.123\.30\.132$/);
color.source="lightsalmon"
```

```
color.target="khaki1" if ($fields[1]=~/^192\.168\.4\.1$/);
color.target="palegreen" if ($fields[1]=~/^192\.168\.4/);
color.target="lightblue" if ($fields[1]=~/^0\.0\.0\.0$/);
color.target="lightblue" if ($fields[1]=~/^255\.255\.255\.255$/);
color.target="lightblue" if ($fields[1]=~/^198\.123\.30\.132$/);
color.target="lightsalmon"
```

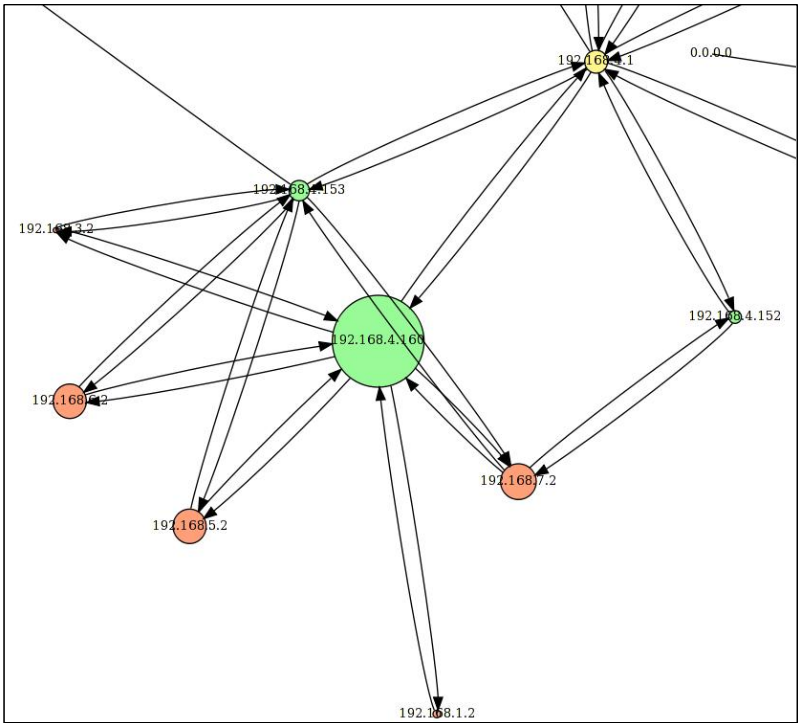
```
cluster.source=regex_replace("(\\d\+\\.\\d\+\\.\\d\+)")."/24" if
( match("^(192\.168\.4\.|xxxx)") && !(field() =~
/^192\.168\.4\.1$/) );
cluster.target=regex_replace("(\\d\+\\.\\d\+\\.\\d\+)")."/24" if
( match("^(192\.168\.4\.|xxxx)") && !(field() =~
/^192\.168\.4\.1$/) );
```

Add cluster instruction

005_activity_connections_volume.sh

Visualize: AfterGlow / Graphviz

- But who is the most active IP?
- Size of nodes dependent on packet volume to represent activity.



005_activity_connections_volume.sh

Visualize: AfterGlow / Graphviz

- AfterGlow p_ipsrc_ipdst_volume.properties

```
color.source="khaki1" if ($fields[0]=~/^192\.168\.4\.1$/);
color.source="palegreen" if ($fields[0]=~/^192\.168\.4\..*/);
color.source="lightblue" if ($fields[0]=~/^0\.0\.0\.0$/);
color.source="lightblue" if ($fields[0]=~/^255\.255\.255\.255$/);
color.source="lightblue" if ($fields[0]=~/^198\.123\.30\.132$/);
color.source="lightsalmon"
size.source=$sourceCount{$sourceName};
maxnodesize=1;
```

```
color.target="khaki1" if ($fields[1]=~/^192\.168\.4\.1$/);
color.target="palegreen" if ($fields[1]=~/^192\.168\.4\..*/);
color.target="lightblue" if ($fields[1]=~/^0\.0\.0\.0$/);
color.target="lightblue" if ($fields[1]=~/^255\.255\.255\.255$/);
color.target="lightblue" if ($fields[1]=~/^198\.123\.30\.132$/);
color.target="lightsalmon"
size.target=$targetCount{$targetName};
```

005_activity_connections_volume.sh

Visualize: AfterGlow / Graphviz

- Visualize CSV file using AfterGlow

  -
    ```
    cat d_ipsrc_ipdst.csv |
    afterglow.pl -t -c
    p_ipsrc_ipdst_volume.properties >
    v_ipsrc_ipdst_volume.dot
    ```

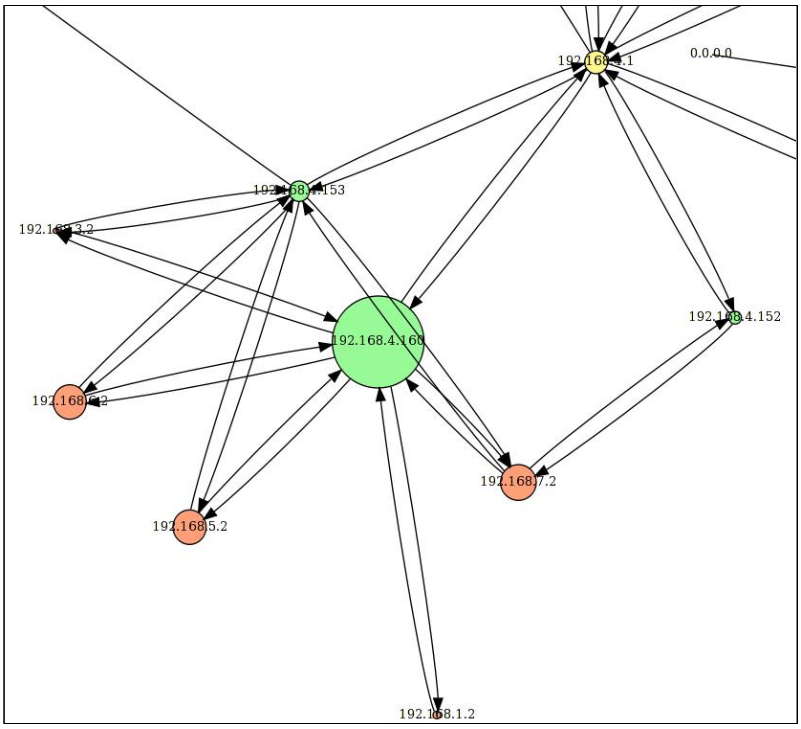
  -
    ```
    neato –T png -o v_ipsrc_ipdst_volume.dot
    v_ipsrc_ipdst_volume.png
    ```
- View resulting image

  -
    ```
    gqview
    ```

004_activity_connections_volume.sh

Visualize: AfterGlow / Graphviz

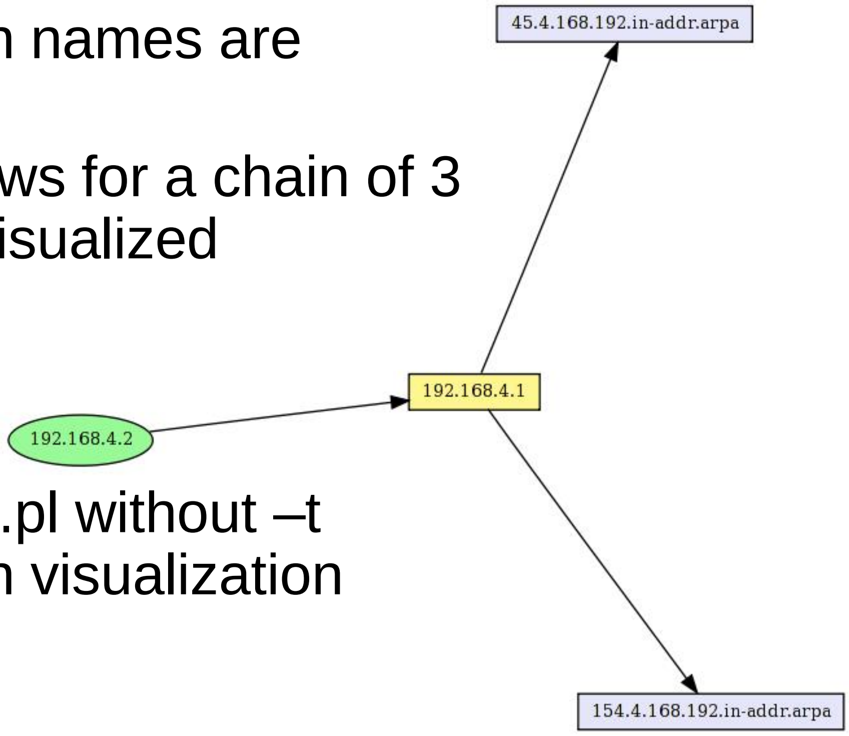
- Most active talker is
  - 192.168.4.160



007_activity_dnsquery.sh

Visualize: AfterGlow / Graphviz

- Which domain names are resolved?
- Afterglow allows for a chain of 3 nodes to be visualized
  - Source
  - Event
  - Target
- Call afterglow.pl without –t for a 3 column visualization



007_activity_dnsquery.sh

Visualize: AfterGlow / Graphviz

- AfterGlow p_ipsrc_ipdst_dnsqryname.properties

```
color.source="khaki1" if ($fields[0]=~/^192\.168\.4\.1$/);
color.source="palegreen" if ($fields[0]=~/^192\.168\.4\..*/);
color.source="lightblue" if ($fields[0]=~/^0\.0\.0\.0$/);
color.source="lightblue" if ($fields[0]=~/^255\.255\.255\.255$/);
color.source="lightblue" if ($fields[0]=~/^198\.123\.30\.132$/);
color.source="lightsalmon";
shape.source="ellipse";
```

```
color.event="khaki1" if ($fields[1]=~/^192\.168\.4\.1$/);
color.event="palegreen" if ($fields[1]=~/^192\.168\.4\..*/);
color.event="lightblue" if ($fields[1]=~/^0\.0\.0\.0$/);
color.event="lightblue" if ($fields[1]=~/^255\.255\.255\.255$/);
color.event="lightblue" if ($fields[1]=~/^198\.123\.30\.132$/);
color.event="lightsalmon";
shape.event="ellipse";
```

```
color.target="lavender";
shape.target="box";
```

Node shape: box, ellipse, diamond, triangle, …

Node types: source, event, target

Exercise

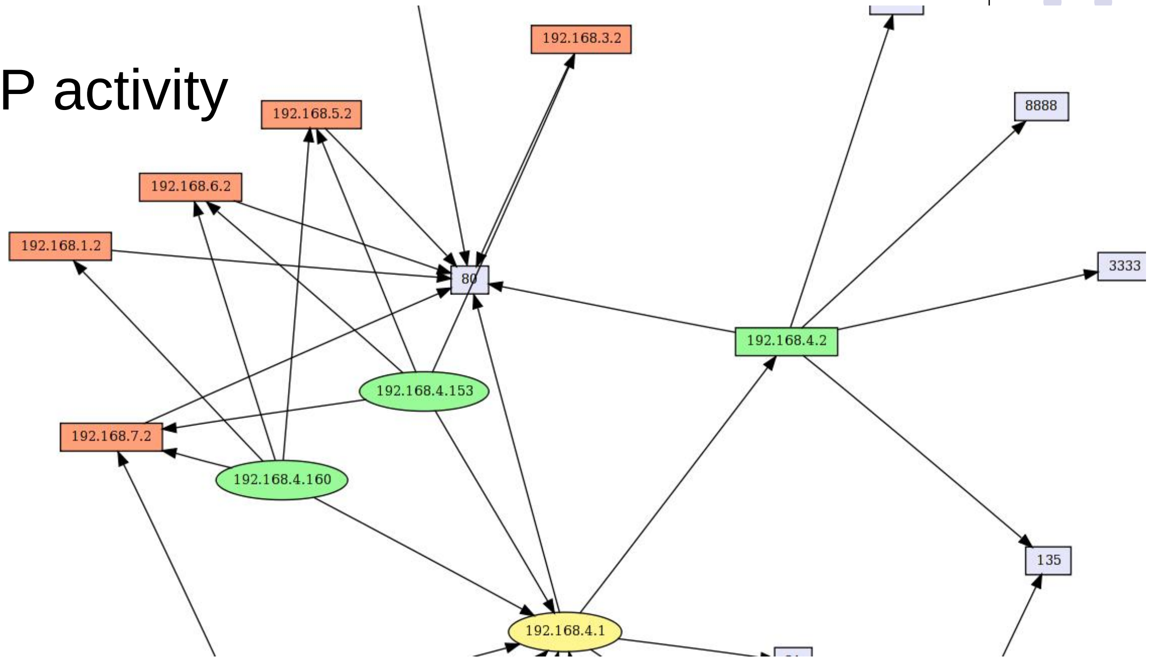
- Analyze TCP activity
  - ip.src à ip.dst à tcp.dstport
  - ip.src à tcp.dstport à ip.dst

- Analyze HTTP request activity
  - ip.src à ip.dst à http.request.method | http.request.uri
  - ip.src à http.request.method | http.request.uri à ip.dst
  - ip.dst à tcp.dstport à http.request.method | http.request.uri

006_activity_connections_tcp_ports.sh

Visualize: AfterGlow / Graphviz

- TCP activity



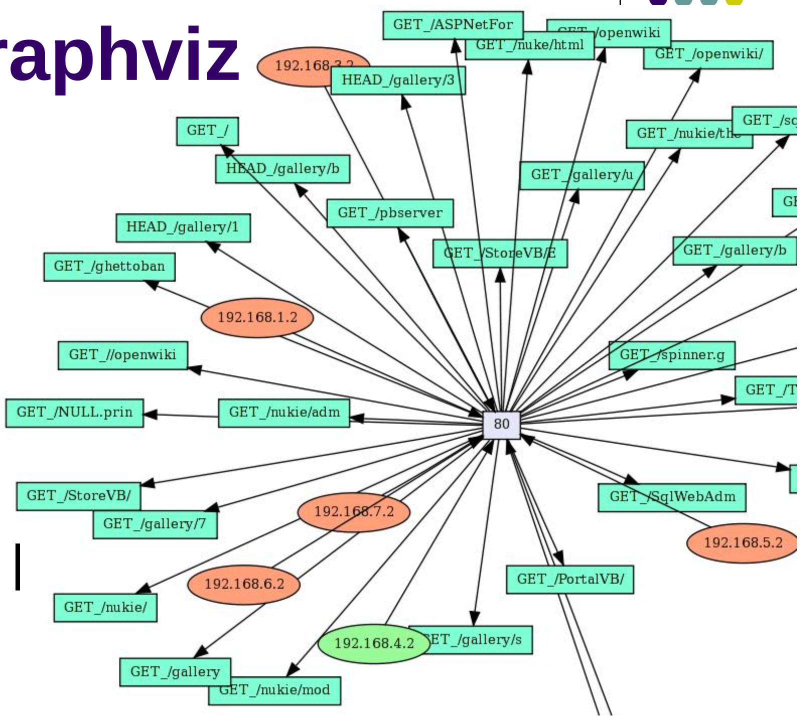
- Prevent port confusion

```
tshark… -R "tcp.flags.syn==1 and tcp.flags.ack==0"
```

Visualize: AfterGlow / Graphviz

008_activity_connections_http.sh

- HTTP activity



- ip.dst à tcp.dstport à http.request.method | http.request.uri

- Assemble & trim request method and URI
- `awk -F, '{print $2 "," $3 "," $4 "_" substr($5,0,10)}'`

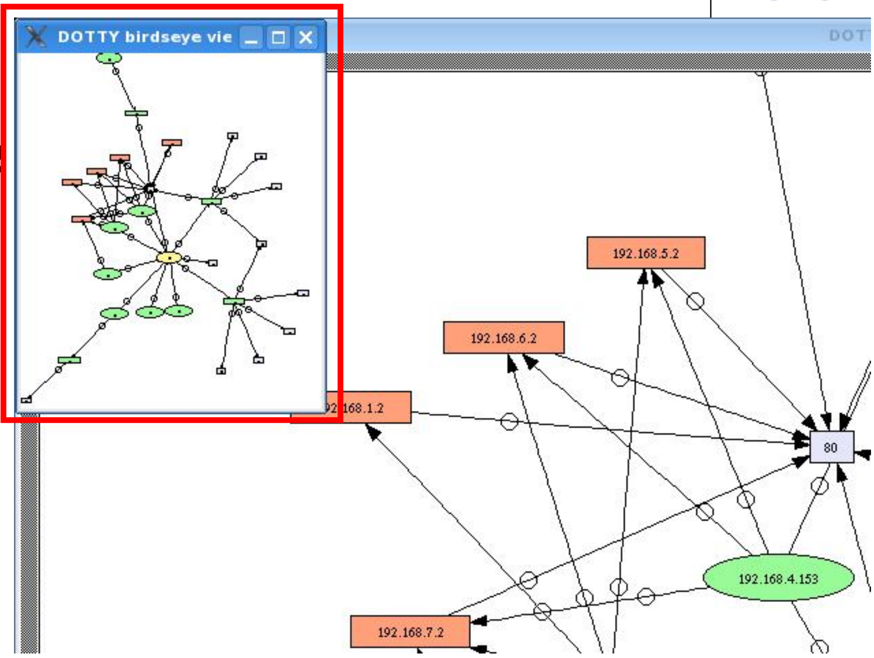
Activities

Linked Graphs

Graphviz lneato / Cytoscape

Visualize: Graphviz lneato

- With *lneato* graphs can be viewed and manipulated interactively.



Birdseye View

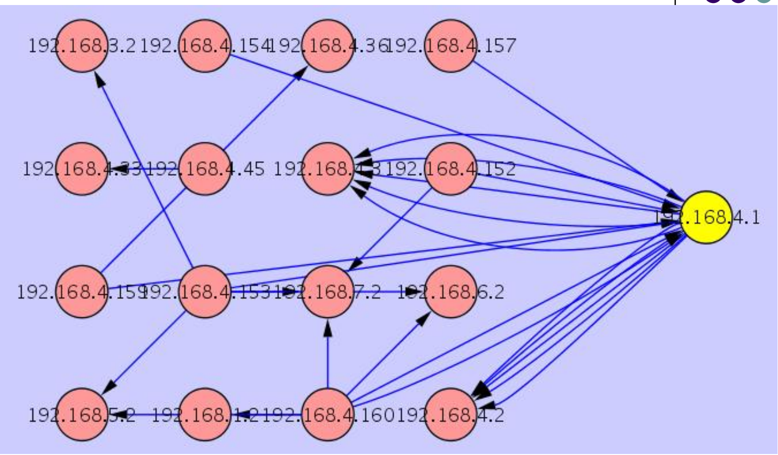
- Command line
- `lneato v_ipsrc_ipdst_tcpport_syn1_ack0.dot`

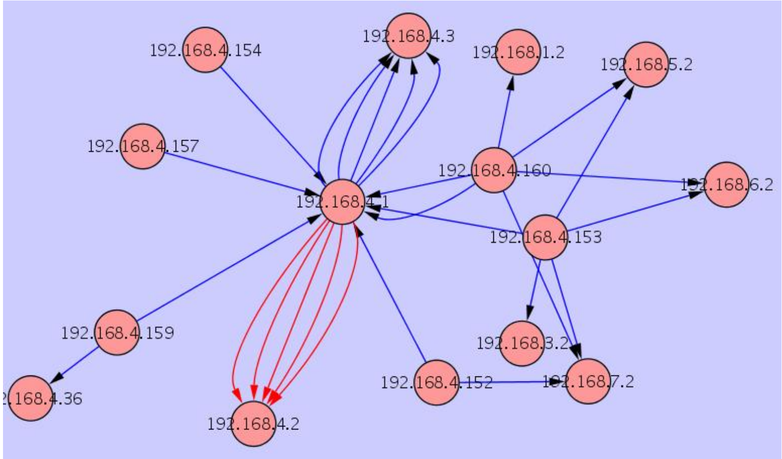
Visualize: Graphviz lneato

- Important commands and short cuts
  - Right click for menu
    - Birdseye view
  - u à undo operation
  - select node + d à delete node
  - l (lowercase L) à layout modified graph
  - L à load and layout original graph
  - z à zoom out
  - Z à zoom in

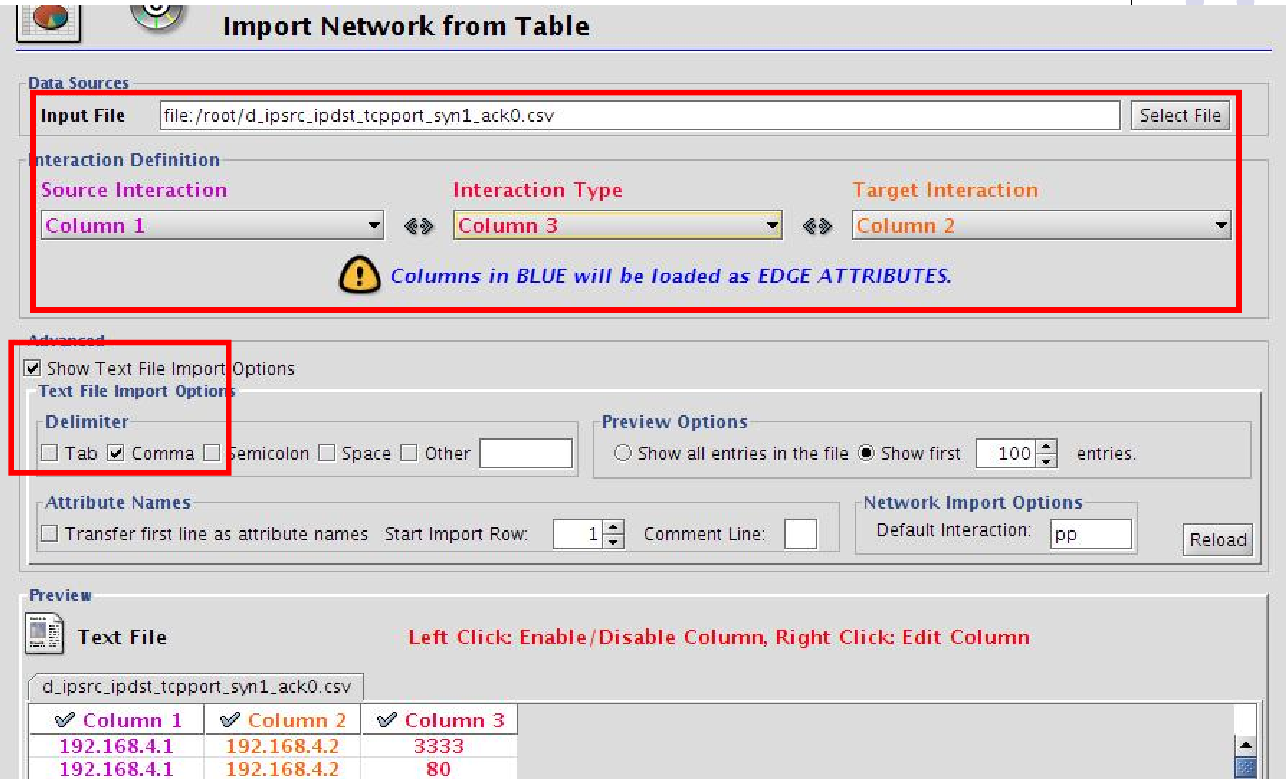
Visualize: Cytoscape

- Bioinformatics Visualization Tool
- Supports different layout algorithms
- Graph merging





Visualize: Cytoscape



Import Network from Table

Data Sources

Input File: file:/root/d_ipsrc_ipdst_tcpport_syn1_ack0.csv

Interaction Definition

Source Interaction: Column 1

Interaction Type: Column 3

Target Interaction: Column 2

Columns in BLUE will be loaded as EDGE ATTRIBUTES.

Advanced

☑ Show Text File Import Options

Text File Import Options

Delimiter: □ Tab ☑ Comma □ Semicolon □ Space □ Other

Preview Options: ○ Show all entries in the file ● Show first 100 entries.

Attribute Names: □ Transfer first line as attribute names Start Import Row: 1 Comment Line:

Network Import Options: Default Interaction: pp

Preview

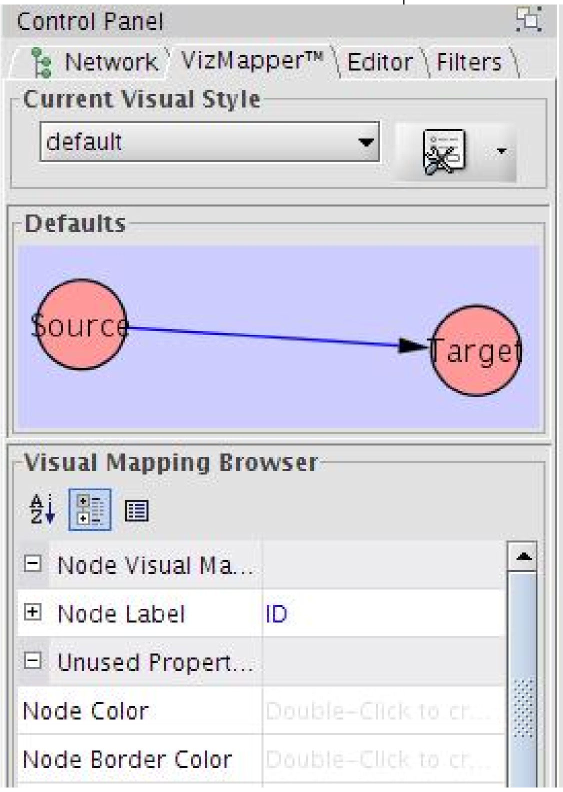
Text File Left Click: Enable/Disable Column, Right Click: Edit Column

d_ipsrc_ipdst_tcpport_syn1_ack0.csv

✓ Column 1	✓ Column 2	✓ Column 3
192.168.4.1	192.168.4.2	3333
192.168.4.1	192.168.4.2	80

Visualize: Cytoscape

- Important functions
  - File\Import\Network from (Text/MS Excel)…
  - Layout\yFiles\...
  - Layout\Cytoscape Layouts
- VizMapper^{TM} tab in control panel
  - Modify graph presentation



Current Visual Style

default

Defaults

Visual Mapping Browser

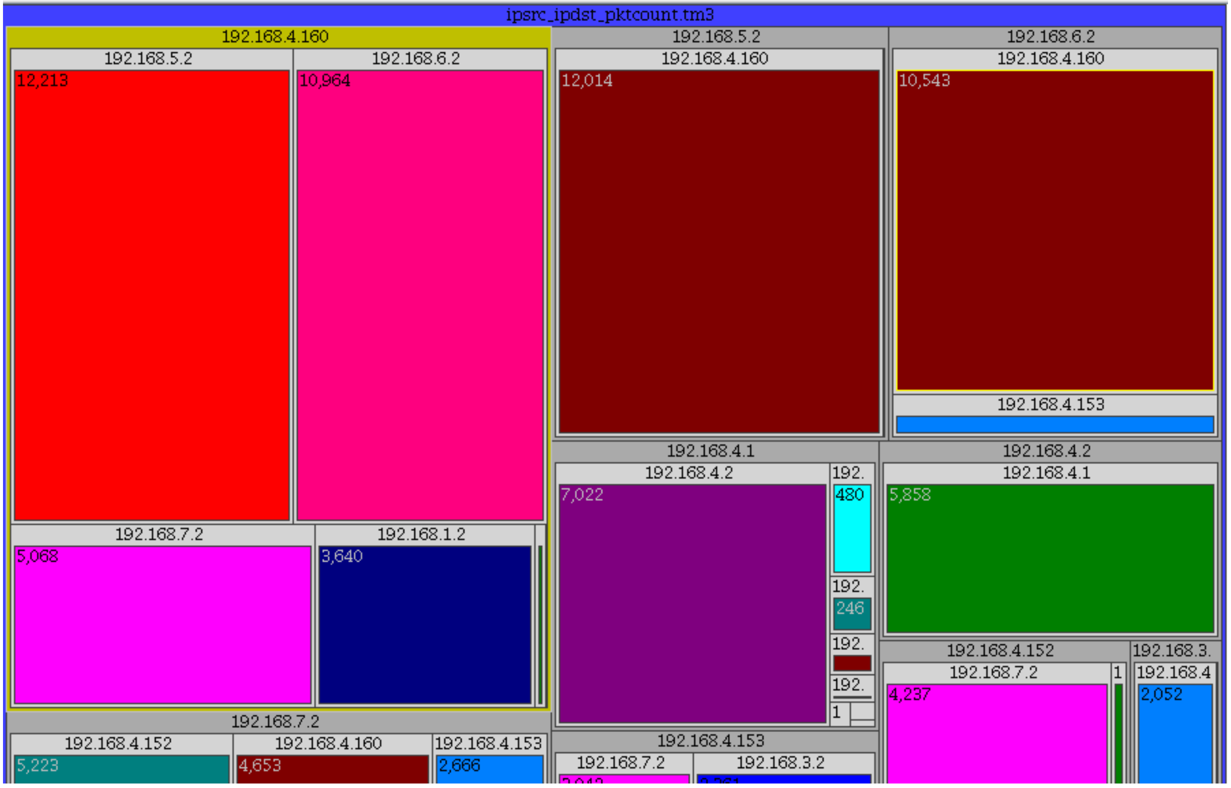
⊟ Node Visual Ma...	
⊞ Node Label	ID
⊟ Unused Propert...	
Node Color	Double-Click to cr...
Node Border Color	Double-Click to cr...

Activities

Treemap

009_activity_connections_treemap.sh

Visualize: Treemap



009_activity_connections_treemap.sh

Visualize: Treemap

- TM3 formatted file

IP Src	IP Dest	Count
STRING	STRING	INTEGER
0.0.0.0	255.255.255.255	4
192.168.1.2	192.168.4.160	2833
192.168.3.2	192.168.4.153	2052
192.168.3.2	192.168.4.160	2
192.168.4.1	192.168.4.152	246
192.168.4.1	192.168.4.153	115
192.168.4.1	192.168.4.154	45
192.168.4.1	192.168.4.157	15
192.168.4.1	192.168.4.159	480
192.168.4.1	192.168.4.160	174
192.168.4.1	192.168.4.2	7022
192.168.4.1	192.168.4.3	39
192.168.4.152	192.168.4.1	273

009_activity_connections_treemap.sh

Zoom & Filter: tshark

- Extract source/destination IP & packet count

  ```
  tshark -r davix_workshop_captures.pcap
  -e ip.src -e ip.dst –T fields
  –E separator=/t -R "ip" |
  sort | uniq -c |
  awk '{print $2 "," $3 "," $1}'
  > d_ipsrc_ipdst_pktcount.csv
  ```

009_activity_connections_treemap.sh

Visualize: Treemap

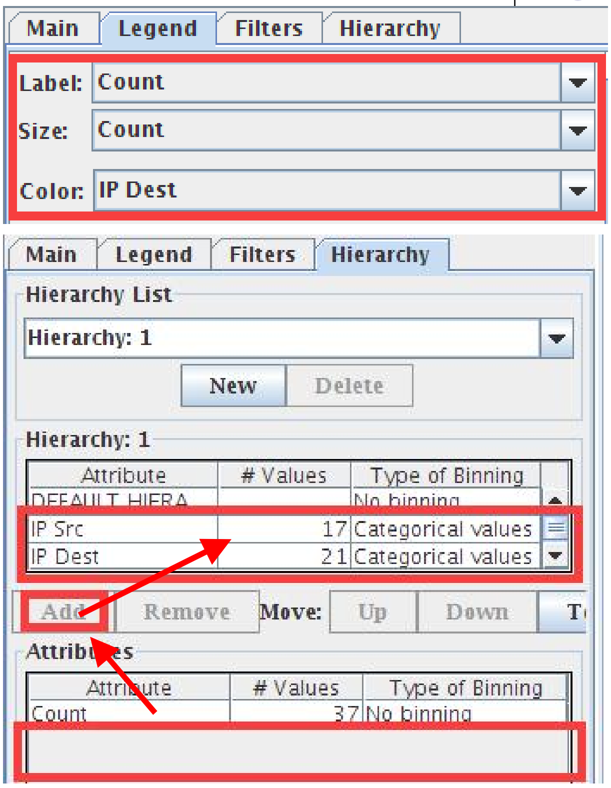
- Convert CSV to TM3 format

  ```
  cat d_ipsrc_ipdst_pktcount.csv |
  awk -F, 'BEGIN
  {
       print "IP Src\tIP Dest\tCount";
       print "STRING\tSTRING\tINTEGER"
  }
  {
       print $1 "\t" $2 "\t" $3
  }' > v_ipsrc_ipdst_pktcount.tm3
  ```

009_activity_connections_treemap.sh

Visualize: Treemap

- Open TM3 file in Treemap
- In *Legend* tab
  - Set *Label* to *count*
  - Set *Size* to *count*
  - Set *Color* to *IP Dest*
- In *Hierarchy* tab
  - Add IP Src to Hierarchy
  - Add IP Dest to Hierarchy



Label: Count

Size: Count

Color: IP Dest

Hierarchy: 1

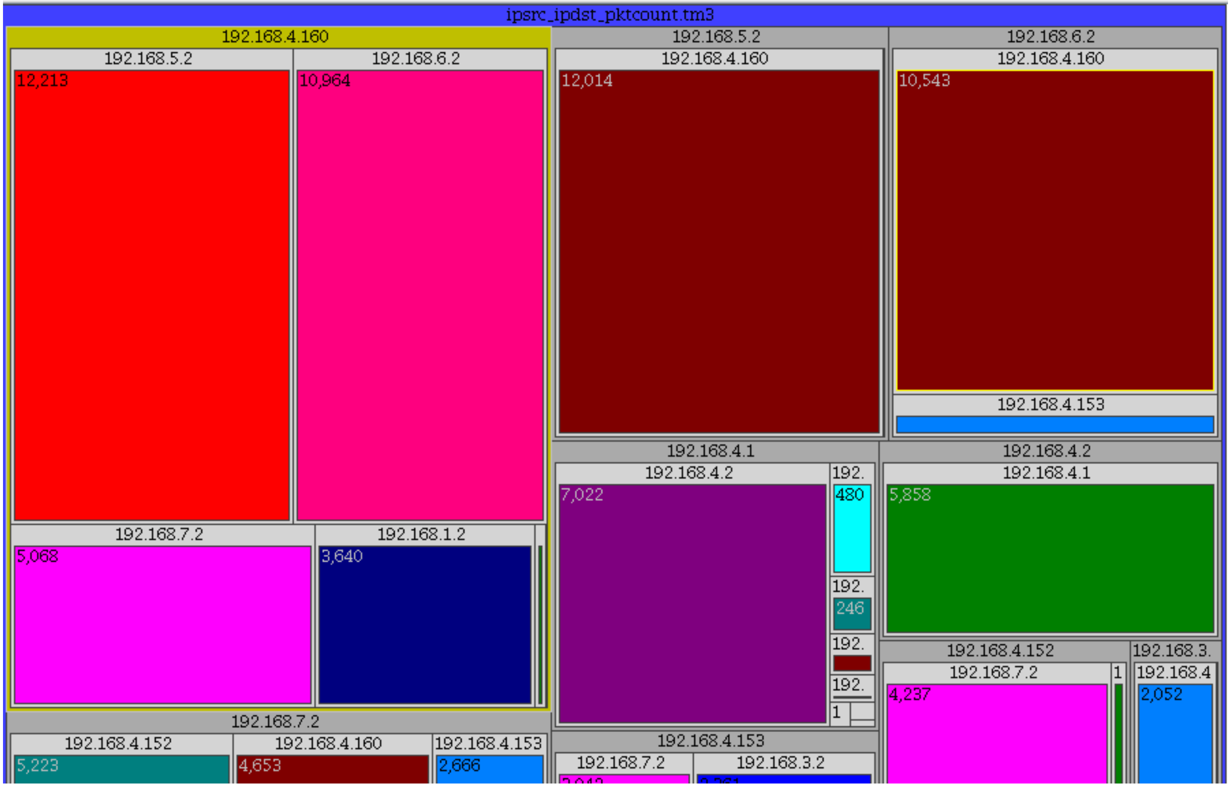
Attribute	# Values	Type of Binning
DEFAULT HIERA...		No binning
IP Src	17	Categorical values
IP Dest	21	Categorical values

Attributes

Attribute	# Values	Type of Binning
Count	37	No binning

009_activity_connections_treemap.sh

Visualize: Treemap



Exercise

- Analyze TCP activity with Treemap
  - ip.src, ip.dst, tcp.dstport, count per tcp port
- Interesting questions
  - Most called TCP port per source IP?
  - Most called TCP port per destination IP?

Attacks

Snort

011_activity_attacks.sh

Zoom & Filter: Snort

- Extract Snort alerts

  -
    ```
    snort -c /etc/snort/snort.bleeding.conf
    -r davix_workshop_captures.pcap
    ```
- Convert Snort alerts to CSV file

  -
    ```
    cat /var/log/snort/alert |
    snortalert2csv.pl "sip dip name" |
    sort –u >
    d_ipsrc_ipdst_attackname_distinct.csv
    ```

011_activity_attacks.sh

Zoom & Filter: Snort

- Snort CSV file

```
192.168.4.1,192.168.4.2,(http_inspect) BARE BYTE UNICODE ENCODING
192.168.4.1,192.168.4.2,BLEEDING-EDGE PHPNuke general SQL injection
attempt
192.168.4.1,192.168.4.2,BLEEDING-EDGE WEB-MISC Poison Null Byte
192.168.4.1,192.168.4.3,(http_inspect) OVERSIZE CHUNK ENCODING
192.168.4.1,192.168.4.3,BLEEDING-EDGE SCAN NMAP -sA (1)
192.168.4.152,192.168.7.2,(http_inspect) OVERSIZE CHUNK ENCODING
192.168.4.152,192.168.7.2,(http_inspect) WEBROOT DIRECTORY
TRAVERSAL
192.168.4.152,192.168.7.2,BLEEDING-EDGE PHPNuke general SQL
injection attempt
192.168.4.152,192.168.7.2,BLEEDING-EDGE SCAN NMAP -sA (1)
192.168.4.152,192.168.7.2,BLEEDING-EDGE WEB-MISC Poison Null Byte
```

Activities

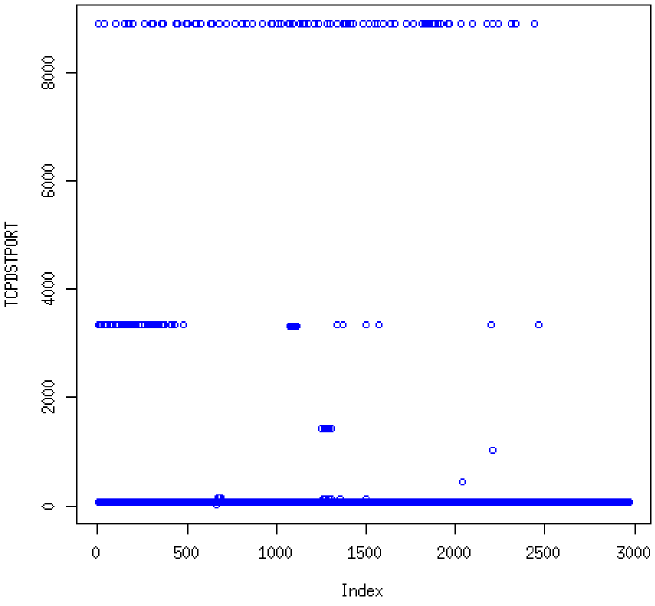
Statistics based Tools

R Project / GGobi

012_activity_tcpdstport_r.sh

Visualization: R

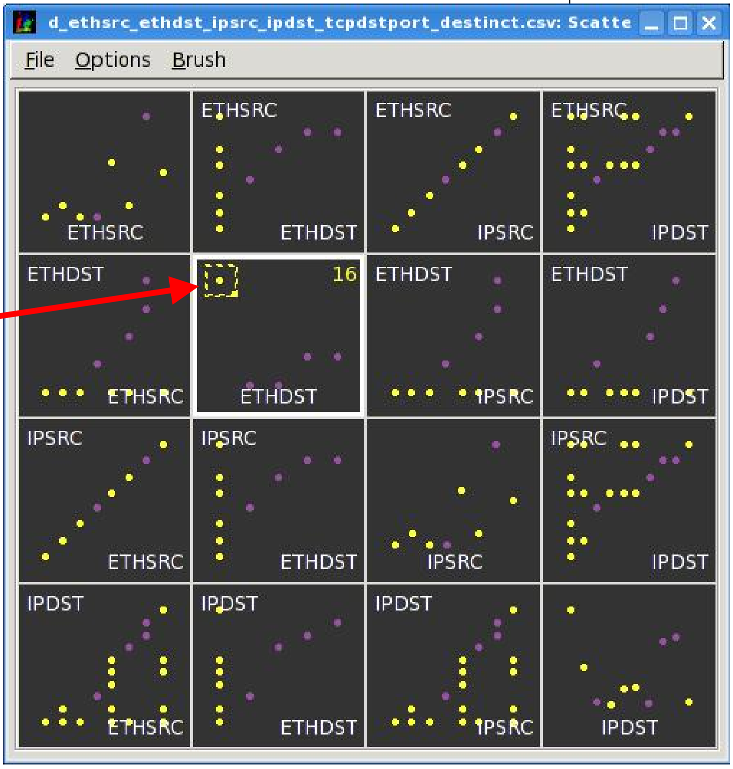
- R is an open source statistics suite
- Lots of features for
  - statistic analysis
  - charting
- Example scatter plot
  - sequence of TCP SYN packets against TCP destination port



013_activity_multivariate_connections_ggobi.sh

Visualization: GGobi

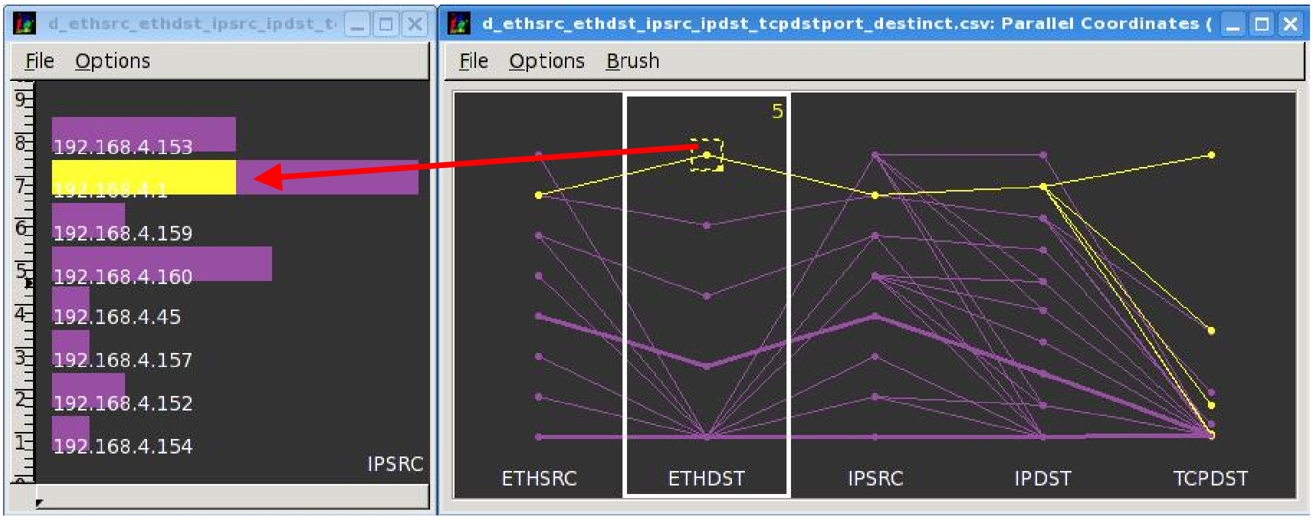
- Visualization tool for multi-dimensional data analysis.
  - Linked views
  - Brushing
- Visualizations
  - Bar charts
  - Scatter plots
  - Parallel coordinates



013_activity_multivariate_connections_ggobi.sh

Visualization: GGobi

- Parallel coordinates
  - Compact visualization of multiple variables

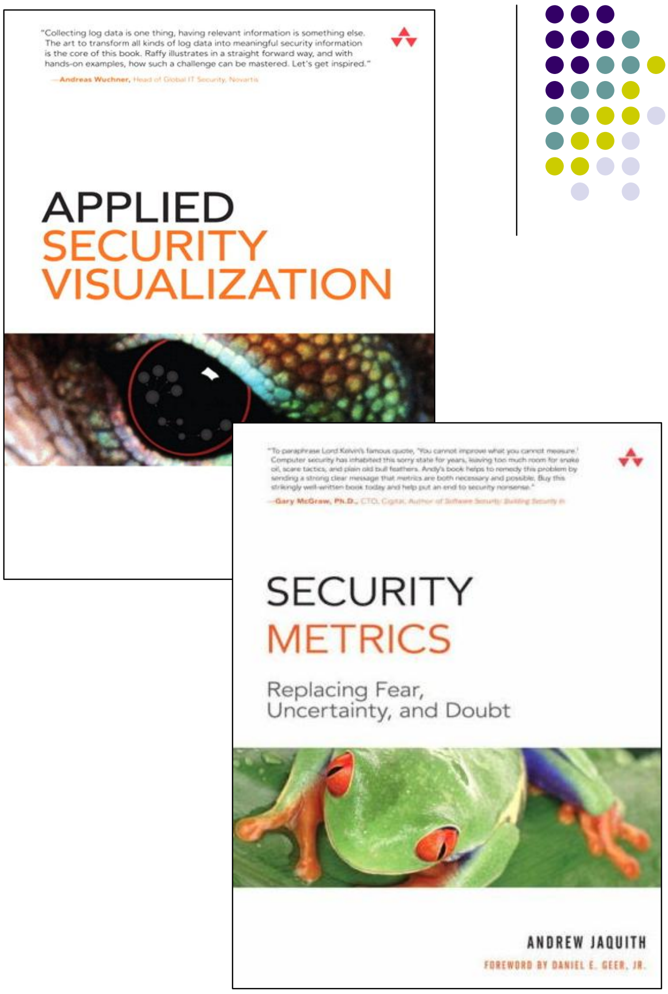


Agenda

- Security Visualization
- Introduction DAVIX
- Walk-Through DAVIX
- Hands-on Lab
- Visualization Contest

Prizes

- 1st prize
  - 1x Applied Security Visualization Book
  - 1x Security Metrics Book
- 2nd prize
  - 1x Applied Security Visualization Book


"Collecting log data is one thing, having relevant information is something else. The art to transform all kinds of log data into meaningful security information is the core of this book. Raffy illustrates in a straight forward way, and with hands-on examples, how such a challenge can be mastered. Let's get inspired."
—Andreas Wuchner, Head of Global IT Security, Novartis
APPLIED
SECURITY
VISUALIZATION
"To paraphrase Lord Kelvin's famous quote, 'You cannot improve what you cannot measure.' Computer security has inhabited this sorry state for years, leaving too much room for snake oil, scare tactics, and plain old bull feathers. Andy's book helps to remedy this problem by sending a strong clear message that metrics are both necessary and possible. Buy this strikingly well-written book today and help put an end to security nonsense."
—Gary McGraw, Ph.D., CTO, Cigital, Author of Software Security: Building Security In
SECURITY
METRICS
Replacing Fear, Uncertainty, and Doubt
ANDREW JAQUITH
FOREWORD BY DANIEL E. GEER, JR.

Task

- Analyze the attack(s) in the
  - Jubrowska capture and
  - spty database
- Use any visualization technique you like to document the a particular the attacks
  - Not limited to DAVIX
- Document the case (Text, images, video, …)
  - Tell a story in your submission
  - Make it an interesting read / view

Submission Details

- Submission conditions
  - deadline: Friday, October 30 12:00 (noon) CET
  - submit to: jan.monsch@iplosion.com
  - single submission by multiple persons possible
  - released under
    - text, images, …: creative commons license: BY-SA
    - code: BSD, MIT or GPL license
- Winner announcement and prize handover
  - Friday, October 30 around 17:00 CET
- Legal recourse is excluded

Contest Kick Start

- The DAVIX VM contains a copy of the Jubrowska capture split up in 14 files
  - /root/jubrowska/jubrowska-capture_1_part*
- The most important fields were extracted with
  - /root/jubrowska/extract.sh
- Most extracts are compressed
  - Use zcat to read the d_*.csv files
- In case you require the original files
  - http://2009.hack.lu/index.php/InfoVisContest

Contest Kick Start

- Clever filtering and clustering is a must
  - Most visualization tools do not scale that well!
- Tools which might be interesting to use
  - Processing (part of DAVIX) [20], code_swarm [25]
  - SIMILE Timeline & Timeplot Widget [21, 22]
  - Google Maps [23]
  - Open Flash Chart [24]
- If you have tool related questions, please approach me at the conference venue.
- Good Luck!

Q & A

Customized visualization workshops are available as in-house training!

Contact:

jan.monsch@iplosion.com

References I

1. Visualization (Computer Graphics). Wikipedia. http://en.wikipedia.org/wiki/Visualization_(computer_graphics).
2. Shneiderman B. *Keynote VizSec*. 2008.
3. Conti G. *Security Data Visualization*. No Starch Press, 2007.
4. Marty R. *Applied Security Visualization*. Pearson Education, 2008.
5. Jaquith A. Security Metrics. Pearson Educatoin, 2007.
6. Few S. Now You See It: Simple Visualization Techniques for Quantitative Analysis. Analytics Press, 2009.
7. Mackinlay J.D., Winslow K. Designing Great Visualizations. Tableau Software, 2009.
8. Shneiderman B. The Eyes Have It: A Task by Data Type Taxonomy for Information Visualization. IEEE Visual Languages. pp. 336 – 343. 1996.
9. Monsch J. P., Marty R. DAVIX Manual 1.0.1. 2008. http://82.197.185.121/davix/release/davix-manual-1.0.1.pdf

References II

10. Wireshark / tshark Manual
    http://www.wireshark.org/docs/wsug_html/
11. awk Tutorial
    http://www.grymoire.com/Unix/Awk.html
12. p0f
    http://lcamtuf.coredump.cx/p0f.shtml
13. Snort Manual
    http://www.snort.org/docs/snort_htmanuals/htmanual_282/
14. AfterGlow Manual
    http://afterglow.sourceforge.net/manual.html
15. Graphviz Documentation
    http://www.graphviz.org/Documentation.php
16. Treemap Manual
    http://www.cs.umd.edu/hcil/treemap/doc4.1/toc.html
17. Cytoscape Online Tutorials
    http://cytoscape.org/cgi-bin/moin.cgi/Presentations

References III

18. The R Manuals
    http://cran-r.project.org/manuals.html
19. GGobi Manual, 2006
    http://www.ggobi.org/docs/manual.pdf
20. Processing
    http://processing.org
21. SIMILE Timeline Widget
    http://www.simile-widgets.org/timeline/
22. SIMILE Timeplot Widget
    http://www.simile-widgets.org/timeplot/
23. Google Maps API
    http://code.google.com/apis/maps/
24. Open Flash Chart
    http://teethgrinder.co.uk/open-flash-chart/
25. code_swarm
    http://code.google.com/p/codeswarm/